

Installing Thunder Observability Agent

April, 2024

© 2024 A10 Networks, Inc. All rights reserved.

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at: a10-virtual-patent-marking.

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting <u>www.a10networks.com</u>.

Table of Contents

Introduction	6
Internal Thunder Observability Agent (iTOA)	
AWS	
Publishing the vThunder Metrics on AWS	10
Publishing the vThunder Logs on AWS	
Sample Cloud Credentials File	
Azure	
Publishing the vThunder Metrics on Azure	
Publishing the vThunder Logs on Azure	21
Sample Cloud Credential File	
VMware	
Publishing the vThunder Metrics on VMware	
Publishing the vThunder Logs on VMware	
Sample Cloud Credential File	
External Thunder Observability Agent (TOA)	
External Thunder Observability Agent (TOA)	
External Thunder Observability Agent (TOA) Download Links Supported Technology	
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics	38
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs	38
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs Supported ACOS Versions	38 39 40 40 40 42 42
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs Supported ACOS Versions Supported Platforms	38 39 40 40 40 42 42 42 42
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs Supported ACOS Versions Supported Platforms Install TOA	38
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs Supported ACOS Versions Supported Platforms Install TOA Python Plugin Installation	38
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs Supported ACOS Versions Supported Platforms Install TOA Python Plugin Installation Prerequisites	38 39 40 40 40 42 42 42 42 42 42 44 44 44
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs Supported ACOS Versions Supported Platforms Install TOA Python Plugin Installation Prerequisites Installation Steps	38 39 40 40 40 42 42 42 42 44 44 44 44 44 45 46
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs Supported ACOS Versions Supported Platforms Install TOA Python Plugin Installation Prerequisites Installation Steps Containerized Installation	38 39 40 40 40 42 42 42 42 44 44 44 44 44 45 46 46 49
External Thunder Observability Agent (TOA) Download Links Supported Technology Supported Thunder Metrics Supported Thunder Logs Supported ACOS Versions Supported Platforms Install TOA Python Plugin Installation Prerequisites Installation Steps Containerized Installation Prerequisites	38 39 40 40 42 42 42 44 44 44 45 46 46 46 49 50

Global Configuration
Main Properties
Logging61
Crontab
Cloud-specific Configuration63
AWS Config64
AWS Credentials64
Azure Credentials65
VMware Credentials
Elasticsearch Credentials
PushGateway Credentials
Splunk Credentials
GCP Credentials
OCI Credentials
Data Collection Configuration
Thunder Credentials
TOA Thunder Configuration Matrix
Data Publish Configuration
Config JSON
Monitor Dashboard
Monitor Metrics
Monitor Logs
Troubleshoot
TOA Logging
Examples
AWS
Azure
VMware
Elasticsearch
Prometheus

Splunk
Google Console Platform
Oracle Cloud Infrastructure
What's New
3.0.0
2.0.0
1.0.0
Appendix
Get Resource ID
Install Python, Crontab, and Syslog221
Uninstall TOA
Import vROps Template
Import a Dashboard
Import an Alert Definition
Import a Notification
Installing vROps and vRLI
Base64 Conversion Examples
Creating Widgets in OCI
Create Policies to Publish Data in OCI
Disclaimer
License

.....

Introduction

The A10 Thunder Observability Agent is a custom plugin to monitor A10 Thunder[®] Application Delivery Agent (ADC) performance metrics and syslogs.

There are two types of A10 Thunder Observability Agent available:

Internal Thunder Observability Agent (iTOA)

This is an in-built Python plugin within ACOS which is configured using ACOS Command Line Interface (CLI) or aXAPI.

You can use iTOA:

- For ACOS v6.0.1 or later.
- For configuring vThunder using aXAPI or CLI to publish the metrics directly on the same AWS, Azure, or VMware platform where the vThunder instance is deployed with outbound internet connectivity.
- For configuring vThunder using aXAPI or CLI to publish the syslogs on:
 - AWS CloudWatch directly from vThunder with outbound internet connectivity.
 - Azure Log Analytics Workspace directly from vThunder with outbound internet connectivity to access '*.*microsoftonline.com*' and '*.*azure.com*'.
 - VMware vRealize Log Insight (vRLI) which is accessible from vThunder.
- For managing the data collection, processing, aggregation, and publishing internally for configured L3V partitions.
- For supporting maximum 20 partitions per vThunder instance.
- For publishing metrics or logs every 1 minute.

To configure the Internal Thunder Observability Agent, see <u>Internal Thunder</u> <u>Observability Agent (iTOA)</u>.

External Thunder Observability Agent (TOA)

This external plugin can be installed on Linux, CentOS, and Ubuntu platforms as a Python Plugin installation package and Docker containerization.



You can use TOA:

- For any ACOS deployment platform.
- For any ACOS software version.
- For a Thunder with outbound internet connectivity restrictions.

In this case, TOA can have outbound internet connectivity. It can collect data from Thunder and then publish the metrics and syslogs on the cloud monitoring tool through internet.

TOA serves as an intermediary for managing Thunder Syslogs and 14 Thunder metrics. Syslogs can be directed to log analysis platforms like AWS, Azure, VMware, Elasticsearch (Kibana), Prometheus (Grafana), Splunk, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure(OCI). Thunder metrics are exclusively sent to the platform where Thunder is deployed, which include AWS, Azure, and VMware. Additionally, TOA can send both logs and metrics to shared platforms like Elasticsearch (Kibana), Prometheus (Grafana), Splunk, GCP, and OCI.

To install the external Thunder Observability Agent, see <u>External Thunder</u> <u>Observability Agent (TOA)</u>.

7

NOTE: It is recommended to configure any one TOA at a time.

The internal Thunder Observability Agent (iTOA) is an in-built capability in ACOS that can be configured for any vThunder device to publish the performance metrics and syslogs on the cloud monitoring tool.

The supported vThunder metrics and logs are listed below:

Supported vThunder Metrics

The following table lists the supported vThunder metrics:

Metric	Description
CPU Usage Percentage (Data)	Average data CPU usage, in percentage, for all data CPU configured within a vThunder instance for the last data collection cycle.
Memory Usage Percentage	Memory (RAM) usage, in percentage, of a vThunder instance for the last data collection cycle.
Disk Usage Percentage	Average disk storage usage, in percentage, for all disks associated with a vThunder instance for the last data collection cycle.
Throughput Rate (Global/BPS)	Total vThunder system global throughput bits per sec from vThunder instance to the server for the last data collection cycle.
Interface Down Count (Data)	Count of the total data network interfaces configured for a vThunder instance which is inactive for the last data collection cycle.
Total New Connection (Sec)	Count of the total new connections sent from vThunder instance to the server for the last data collection cycle per second. This includes L4-conns-per-sec, L7-conns-per-sec, L7- trans-per-sec, ssl-conns-per-sec, and ip-nat-conns-per-sec.
Transactions Rate (Sec)	Count of the total L7 transactions made per second from vThunder instance to the server for the last data collection

Table 1	: SI	upporte	ed vThu	inder	Metrics



Table 1 : Supported vThunder Metrics

Metric	Description
	cycle.
Server Down Count	Count of the total web or app servers configured in the vThunder instance which are not reachable from vThunder for the last data collection cycle.
Server Down Percentage	Percentage of the total web or app servers configured in the vThunder instance which are not reachable from vThunder for the last data collection cycle.
SSL Errors Count	Count of the total errors that occurred during data transmission from vThunder to the server due to SSL connection, negotiate, encrypt, and decrypt for the last data collection cycle.
Server Errors Count	Count of the total errors that occurred during data transmission from vThunder to the server with status codes 4xx and 5xx for that last data collection cycle.
Total Session Count	Count of the total active sessions of the vThunder instance for the last data collection cycle.
Packet Rate (Sec)	Count of the total packets sent from or received at the vThunder instance for the last collection cycle.
Packet Drop Rate (Sec)	Count of the total packets dropped while sending data from or receiving data at the vThunder instance for the last collection cycle.

Supported vThunder Logs

The following table lists the supported vThunder logs:

Table 2 : Support	ed Thunder Logs
-------------------	-----------------

Logs	Description
SysLogs	Thunder internal logs such as:
	 SSL connection, negotiate, encrypt, and decrypt
	Status codes 4xx and 5xx



AWS

iTOA can be configured to publish performance metrics and syslogs of a vThunder deployed on AWS.

The following topics are covered:

Publishing the vThunder Metrics on AWS	10
Publishing the vThunder Logs on AWS	14
Sample Cloud Credentials File	16

Publishing the vThunder Metrics on AWS

If the vThunder instance is deployed on the AWS cloud platform, the vThunder metrics can be published on the AWS CloudWatch.

To publish the vThunder metrics on AWS, perform the following steps:

1. Log in to the vThunder instance deployed on AWS using CLI with the administrative privilege:

ACOS(config)#admin <admin_user>

For example

ACOS(config)#**admin** adminuser2

2. Import the AWS credentials and AWS configuration files:

ACOS(config-admin:<admin_user>)#cloud-cred aws-cred import <file_ transfer_method> ACOS(config-admin:<admin_user>)#cloud-cred aws-config import <file_ transfer_method>

The <file_transfer_method> can be any of the following:



```
use-mgmt-port Use management port as source port
tftp: Remote file path of tftp: file system(Format:
tftp://host/file)
ftp: Remote file path of ftp: file system(Format: ftp://
[user@]host[:port]/file)
scp: Remote file path of scp: file system(Format: scp://
[user@]host/file)
sftp: Remote file path of sftp: file system(Format: sftp://
[user@]host/file)
```

For example

```
ACOS(config-admin:adminuser2)#cloud-cred aws-cred import
tftp://192.168.0.0/credentials.txt
ACOS(config-admin:adminuser2)#cloud-cred aws-config import
tftp://192.168.0.0/configuration.txt
```

For a sample credentials file, see <u>AWS Credentials File</u>.

For a sample configuration file, see <u>AWS Configuration File</u>.

3. Verify if the AWS credentials and AWS configuration files are imported correctly:

```
ACOS(config-admin:<admin_user>)#cloud-cred aws-cred show
aws_access_key_id = XXXX
aws_secret_access_key = XXXX
ACOS(config-admin:<admin_user>)#cloud-cred aws-config show
region = XXXX
output = XXXX
```

 Enable and configure the vThunder metrics.
 By default, all the metrics are disabled. You can enable one or more <u>vThunder</u> <u>Metrics</u>.



ACOS(config)#cloud-services cloud-provider ACOS(config-cloud-provider)#aws ACOS (config-cloud-provider-aws) #metrics ACOS(config-cloud-provider-aws-metrics)#enable ACOS (config-cloud-provider-aws-metrics) #active-partitions name ACOS(config-cloud-provider-aws-metrics)#namespace name ACOS(config-cloud-provider-aws-metrics)#**cps** enable ACOS(config-cloud-provider-aws-metrics)#**cpu** enable ACOS(config-cloud-provider-aws-metrics)#**disk** enable ACOS (config-cloud-provider-aws-metrics) #interfaces enable ACOS(config-cloud-provider-aws-metrics)#memory enable ACOS (config-cloud-provider-aws-metrics) **#packet-drop** enable ACOS (config-cloud-provider-aws-metrics) **#packet-rate** enable ACOS (config-cloud-provider-aws-metrics) #server-down-count enable ACOS (config-cloud-provider-aws-metrics) #server-down-percentage enable ACOS (config-cloud-provider-aws-metrics) #server-error enable ACOS(config-cloud-provider-aws-metrics)#sessions enable ACOS(config-cloud-provider-aws-metrics)#ssl-cert enable ACOS(config-cloud-provider-aws-metrics)#throughput enable ACOS(config-cloud-provider-aws-metrics) #tps enable

NOTE: For better throughput, you must enable only those metrics that are required.

For more information on each CLI parameter, see the *Command Line Interface Reference*.

5. Verify the running configuration:



```
ACOS (config) #show running-config cloud-services cloud-provider
!Section configuration: 473 bytes
cloud-services cloud-provider
  aws
   metrics
      enable
      namespace vThunder
      active-partitions shared
      cpu enable
     memory enable
     disk enable
     throughput enable
     interfaces enable
     cps enable
      tps enable
     server-down-count enable
      server-down-percentage enable
      ssl-cert enable
      server-error enable
      sessions enable
      packet-drop enable
      packet-rate enable
```

6. Verify the thunder-observability-agent.log file:

-bash# tail -f /a10data/log/thunder-observability-agent.log

7. View the vThunder metrics.

To view the Thunder metrics on AWS CloudWatch, perform the following steps:

- a. From the AWS Management Console, go to CloudWatch > Metrics > All metrics.
- b. Select **Browse** > <your_Thunder_metric_namespace>.
- c. Click the required metric to be monitored from the **Metrics** panel.
- d. Select the management IP of the Thunder instance to be monitored.



As the Thunder instances are selected, the metric data gets populated in the **Untitled Graph** panel for the selected the time range. For more information, see <u>Graph a metric</u>.

Publishing the vThunder Logs on AWS

When the vThunder instance is deployed on any AWS, Azure, or VMware cloud platform, the vThunder logs can be published to any one of the cloud platforms such as AWS CloudWatch, Azure Log Analytics Workspace, or VMware vRealize Log Insight (vRLI).

To publish the vThunder logs on AWS, perform the following steps:

1. Log in to the deployed vThunder instance using CLI with the administrative privilege:

ACOS(config)#**admin** <admin user>

For example

ACOS(config) #**admin** adminuser2

2. Import the AWS credentials and AWS configuration files:

```
ACOS(config-admin:<admin_user>)#cloud-cred aws-cred import <file_
transfer_method>
ACOS(config-admin:<admin_user>)#cloud-cred aws-config import <file_
transfer method>
```

The <file_transfer_method> can be any of the following:

```
use-mgmt-port Use management port as source port
tftp: Remote file path of tftp: file system(Format:
tftp://host/file)
ftp: Remote file path of ftp: file system(Format: ftp://
[user@]host[:port]/file)
scp: Remote file path of scp: file system(Format: scp://
[user@]host/file)
sftp: Remote file path of sftp: file system(Format: sftp://
[user@]host/file)
```

For example



```
ACOS(config-admin:adminuser2)#cloud-cred aws-cred import
tftp://192.168.0.0/credentials.txt
ACOS(config-admin:adminuser2)#cloud-cred aws-config import
tftp://192.168.0.0/configuration.txt
```

For a sample credentials file, see <u>AWS Credentials File</u>.

For a sample configuration file, see <u>AWS Configuration File</u>.

3. Verify if the AWS credentials and AWS configuration files are imported correctly:

```
ACOS(config-admin:<admin_user>)#cloud-cred aws-cred show
aws_access_key_id = XXXX
aws_secret_access_key = XXXX
ACOS(config-admin:<admin_user>)#cloud-cred aws-config show
region = XXXX
output = XXXX
```

4. Enable and configure the vThunder logs:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#log
ACOS(config-cloud-provider-aws-log)#enable
ACOS(config-cloud-provider-aws-log)#log-group-name name
ACOS(config-cloud-provider-aws-log)#active-partitions name
```

For more information on each CLI parameter, see the *Command Line Interface Reference*.

5. Verify the running configuration:

```
ACOS(config)#show running-config cloud-services cloud-provider

!Section configuration: 103 bytes

cloud-services cloud-provider

aws

log

enable

log-group-name vThunder

active-partitions shared

!
```



6. Verify the thunder-observability-agent.log file:

-bash# tail -f /a10data/log/thunder-observability-agent.log

- 7. View the vThunder logs on AWS CloudWatch:
 - a. From the AWS Management Console, go to CloudWatch > Logs > Log groups.
 - b. Click <your_ log_group_name>.
 - c. Under the **Log streams** tab, click the required log stream to be monitored.

The log stream format is 'DD/MM/YYYY/Management_IP/<your_ log_group_ name>-<Active_Partition_Name>'.

All logs are displayed in a tabular format with expandable details.

Sample Cloud Credentials File

The AWS cloud-cred files must be a text file and it should have the cloud-specific parameters.

AWS Credentials File

The sample AWS credentials.txt file is as follows:

```
aws_access_key_id = XXXX
aws_secret_access_key = XXXX
```

Table 3 : AWS Credentials File Parameters

Parameter	Description
aws_access_	To get the access key ID and secret access key, perform the
key_id	following steps:
	1. Open the <u>IAM console</u> .
	2. On the navigation menu, select Users .
aws_secret_	3. Select your IAM username.
access_key	 Open the Security credentials tab and select Create access key.
	5. To view the new access key, select Show .



AWS Configuration File

The sample AWS configuration.txt file is as follows:

region = XXXX output = XXXX

Table 4 : AWS Config File Parameters

Parameter	Description
region	Specifies the AWS logged-in user's working region.
	Example
	us-east-1
output	Specify json as the AWS CLI output format.

Azure

iTOA can be configured to publish performance metrics and syslogs of a vThunder deployed on Azure.

The following topics are covered:

Publishing the vThunder Metrics on Azure	
Publishing the vThunder Logs on Azure	
Sample Cloud Credential File	24

Publishing the vThunder Metrics on Azure

If the vThunder instance is deployed on Azure cloud platform, the vThunder metrics can be published on the Azure Application Insights.

To the publish vThunder metrics on Azure, perform the following steps:

1. Log in to the vThunder instance deployed on Azure using CLI with the administrative privilege:

ACOS(config)#admin <admin user>

17



For example

ACOS(config)#**admin** adminuser2

2. Import the Azure credentials file:

```
ACOS(config-admin:<admin_user>)#cloud-cred azure-cred import <file_
transfer method>
```

The <file_transfer_method> can be any of the following:

```
use-mgmt-port Use management port as source port
tftp: Remote file path of tftp: file system(Format:
tftp://host/file)
ftp: Remote file path of ftp: file system(Format: ftp://
[user@]host[:port]/file)
scp: Remote file path of scp: file system(Format: scp://
[user@]host/file)
sftp: Remote file path of sftp: file system(Format: sftp://
[user@]host/file)
```

For example

```
ACOS(config-admin:adminuser2)#cloud-cred azure-cred import
tftp://192.168.0.0/credentials.txt
```

For a sample credentials file, see Azure Credentials File.

3. Verify if the Azure credentials file is imported correctly:

```
ACOS(config-admin:<admin_user>)#cloud-cred azure_cred show
azure_workspace_primary_key = XXXX
azure_client_id = XXXX
azure_secret_id = XXXX
azure_tenant_id = XXXX
azure_location = XXXX
```

 Enable and configure the vThunder metrics.
 By default, all the metrics are disabled. You can enable one or more <u>vThunder</u> <u>Metrics</u>.



ACOS(config)#cloud-services cloud-provider ACOS(config-cloud-provider)#azure ACOS (config-cloud-provider-azure) #metrics ACOS(config-cloud-provider-azure-metrics)#enable ACOS (config-cloud-provider-azure-metrics) #active-partitions name ACOS (config-cloud-provider-azure-metrics) #resource-id ID ACOS(config-cloud-provider-azure-metrics)#**cps** enable ACOS(config-cloud-provider-azure-metrics)#**cpu** enable ACOS(config-cloud-provider-azure-metrics)#**disk** enable ACOS(config-cloud-provider-azure-metrics)#interfaces enable ACOS(config-cloud-provider-azure-metrics) #memory enable ACOS (config-cloud-provider-azure-metrics) #packet-drop enable ACOS(config-cloud-provider-azure-metrics) **#packet-rate** enable ACOS (config-cloud-provider-azure-metrics) #server-down-count enable ACOS (config-cloud-provider-azure-metrics) #server-down-percentage enable ACOS(config-cloud-provider-azure-metrics)#server-error enable ACOS (config-cloud-provider-azure-metrics) #sessions enable ACOS (config-cloud-provider-azure-metrics) #ssl-cert enable ACOS (config-cloud-provider-azure-metrics) #throughput enable ACOS(config-cloud-provider-azure-metrics) **#tps** enable

NOTE: For better throughput, you must enable only those metrics that are required.

To get resource-id value, go to Azure Portal > Azure services > Virtual machine > <your_vThunder_instance> > Setting > Properties and get the Resource ID from the right panel.

For more information on each CLI parameter, see the *Command Line Interface Reference*.

5. Verify the running configuration:



```
ACOS(config)#show running-config cloud-services cloud-provider
!Section configuration: 473 bytes
cloud-services cloud-provider
 azure
   metrics
      enable
      resource-id /subscriptions/07d34b9b-61e3-475a-abbc-
006b16812a3e/resourceGroups/vth-
rg6/providers/microsoft.insights/components/vth-vmss-app-insights
     active-partitions shared
     cpu enable
     memory enable
     disk enable
     throughput enable
     interfaces enable
     cps enable
     tps enable
     server-down-count enable
     server-down-percentage enable
     ssl-cert enable
      server-error enable
     sessions enable
     packet-drop enable
      packet-rate enable
```

6. Verify the thunder-observability-agent.log file:

-bash# tail -f /a10data/log/thunder-observability-agent.log

- 7. View the vThunder metrics on Azure Application Insights.
 - a. From the **Azure Portal**, go to **Azure services** > **Resource Groups** > <your_ resource_group> and click <your_app_insight_name>.

OR



From the **Azure Portal**, go to **Azure services** > **Resource Groups** > <*your_ resource_group* > and click <*your_vThunder_instance_name* > whose metric is to be monitored.

- b. Click **Metrics** from the left **Monitoring** panel.
- c. Select the appropriate resources whose metrics you want to view:

Field Name	Description
Scope	If you are adding the metrics from Application Insight window, the selected app insight name is auto-populated.
	If you are adding the metrics from vThunder instance window, select your app insight name.
Metric Namespace	Select Thunder.
Metric	Select a metric from the drop-down. For the list of available vThunder metrics, see <u>Supported vThunder Metrics</u> .

Table 5 : Azure Application Insight Dashboard

As a metric is selected, the corresponding data is plotted in the chart area for the selected the time range.

d. To view multiple metrics on the same chart, click **Add metric** and repeat the above step. For more information, see <u>Metrics Explorer</u>.

Publishing the vThunder Logs on Azure

When the vThunder instance is deployed on any AWS, Azure, or VMare cloud platform, the vThunder logs can be published to any one of the cloud platforms such as AWS CloudWatch, Azure Log Analytics Workspace, or VMware vRealize Log Insight (vRLI).

To publish the vThunder logs on Azure Log Analytics Workspace, perform the following steps:



1. Log in to the deployed vThunder instance using CLI with the administrative privilege:

ACOS(config) #admin <admin user>

For example

ACOS(config) #**admin** adminuser2

2. Import the Azure credentials file:

```
ACOS(config-admin:<admin_user>)#cloud-cred azure-cred import <file_
transfer method>
```

The <file transfer method> can be any of the following:

```
use-mgmt-port Use management port as source port
tftp: Remote file path of tftp: file system(Format:
tftp://host/file)
ftp: Remote file path of ftp: file system(Format: ftp://
[user@]host[:port]/file)
scp: Remote file path of scp: file system(Format: scp://
[user@]host/file)
sftp: Remote file path of sftp: file system(Format: sftp://
[user@]host/file)
```

For example

```
ACOS(config-admin:adminuser2)#cloud-cred azure-cred import
tftp://192.168.0.0/credentials.txt
```

For a sample credentials file, see <u>Azure Credentials File</u>.

3. Verify if the Azure credentials file is imported correctly:

```
ACOS(config-admin:<admin_user>)#cloud-cred azure-cred show
azure_workspace_primary_key = XXXX
azure_client_id = XXXX
azure_secret_id = XXXX
azure_tenant_id = XXXX
azure_location = XXXX
```

4. Enable and configure the vThunder logs:



```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#azure
ACOS(config-cloud-provider-azure)#log
ACOS(config-cloud-provider-azure-log)#enable
ACOS(config-cloud-provider-azure-log)#resource-id ID
ACOS(config-cloud-provider-azure-log)#workspace-id ID
ACOS(config-cloud-provider-azure-log)#active-partitions name
```

To get resource-id value, go to Azure Portal > Azure services > Virtual machine > <your_vThunder_instance> > Setting > Properties and get the Resource ID from the right panel.

To get workspace-id value, go to Azure Portal > Azure services > Log Analytics workspaces > <your_log_analytics_workspace> > Settings > Agents.

For more information on each CLI parameter, see the *Command Line Interface Reference*.

5. Verify the running configuration:

```
ACOS(config)#show running-config cloud-services cloud-provider

!Section configuration: 103 bytes

cloud-services cloud-provider

azure

log

enable

resource-id /subscriptions/07d34b9b-61e3-475a-abbc-

006b16812a3e/resourceGroups/vth-

rg10/providers/Microsoft.Compute/virtualMachineScaleSets/vth-

vmss/virtualMachines/1

workspace-id dcfd78d5-3a49-425d-8410-e02e281f7991

active-partitions shared
```

6. Verify the thunder-observability-agent.log file:

-bash# tail -f /a10data/log/thunder-observability-agent.log

7. View the vThunder logs on Azure Log Analytics Workspace:



- a. From the **Azure Portal**, go to **Azure services** > **Resource Groups** > <your_ resource_group> and click <your_log_analytics_workspace_name>.
- b. Click Logs from the left General panel.

You can close the **Queries** pop-up window.

- c. From New Query1 > Tables tab, expand Custom Logs.
- d. Double-click THUNDER_SYSLOG_CL.
- e. Click Run.

All logs are displayed in tabular format with expandable details.

The following table lists the Thunder Logs filter options:

Filter	Description
log_data	Specifies the actual log entry.
hostname	Displays the vThunder resource ID.
log_type	Displays the vThunder system logs.
appname	Displays the application name.
ip	Displays the vThunder IP address.
agent	Displays the agent name.
jobid	Displays the JOB ID provided in the thunder- observability-agent.log file.
priority	Displays the Notice, Info, Error, and so on as per actual log entry.
partition	Displays the vThunder partition name.

Table 6 : Log Filters

Sample Cloud Credential File

The Azure cloud-cred file must be a text file and it should have the cloud-specific parameters.

Azure Credentials File

The sample Azure credentials.txt file is as follows:

Internal Thunder Observability Agent (iTOA)



```
azure_workspace_primary_key = XXXX
azure_client_id = XXXX
azure_secret_id = XXXX
azure_tenant_id = XXXX
azure_location = XXXX
```

Table 7 : Azure Credentials File Parameters

Parameter	Description
azure_	To get the workspace primary key, go to Azure Portal > Azure
workspace_	<pre>services > Log Analytics workspaces > <log_analytics_< pre=""></log_analytics_<></pre>
primary_key	workspace> > Settings > Agents.
azure_	To get the client ID, secret ID, and tenant ID, go to Azure Portal
client_id	> Azure services > Azure Active Directory > App Registration >
azure_	Owned applications > <application_name>.</application_name>
secret_id	
azure_	
tenant_id	
azure_	To get the location, go to Azure Portal > Azure services >
location	Resource Groups > <your_resource_group> > Overview ></your_resource_group>
	Essentials > Location.

VMware

iTOA can be configured to publish performance metrics and syslogs of a vThunder instance deployed on VMware.

The following topics are covered:

Publishing the vThunder Metrics on VMware	26
Publishing the vThunder Logs on VMware	
Sample Cloud Credential File	



Publishing the vThunder Metrics on VMware

If the vThunder instance is deployed on the VMware cloud platform, the vThunder metrics can be published on the VMware vRealize Operations Manager (vROps).

To publish the vThunder metrics on VMware, perform the following steps:

1. Log in to the vThunder instance deployed on VMware using CLI with the administrative privilege:

ACOS(config)#**admin** <admin user>

For example

ACOS(config) #**admin** adminuser2

2. Import the VMware credentials file:

```
ACOS(config-admin:<admin_user>)#cloud-cred vmware-cred import <file_
transfer method>
```

The <file transfer method> can be any of the following:

```
use-mgmt-port Use management port as source port
tftp: Remote file path of tftp: file system(Format:
tftp://host/file)
ftp: Remote file path of ftp: file system(Format: ftp://
[user@]host[:port]/file)
scp: Remote file path of scp: file system(Format: scp://
[user@]host/file)
sftp: Remote file path of sftp: file system(Format: sftp://
[user@]host/file)
```

For example

```
ACOS(config-admin:adminuser2)#cloud-cred vmware-cred import
tftp://192.168.0.0/credentials.txt
```

For a sample credentials file, see <u>VMware Credentials File</u>.

3. Verify if the VMware credentials file is imported correctly:



ACOS(config-admin:<*admin_user*>)**#cloud-cred vmware-cred show** vmware_vrops_username = XXXX vmware vrops password = XXXX

 Enable and configure the vThunder metrics.
 By default, all the metrics are disabled. You can enable one or more <u>vThunder</u> <u>Metrics</u>.

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#vmware
ACOS(config-cloud-provider-vmware) #metrics
ACOS(config-cloud-provider-vmware-metrics)#enable
ACOS(config-cloud-provider-vmware-metrics)#active-partitions name
ACOS(config-cloud-provider-vmware-metrics) #resource-id ID
ACOS (config-cloud-provider-vmware-metrics) #vrops-host num
ACOS(config-cloud-provider-vmware-metrics)#cps enable
ACOS(config-cloud-provider-vmware-metrics)#cpu enable
ACOS(config-cloud-provider-vmware-metrics)#disk enable
ACOS (config-cloud-provider-vmware-metrics) #interfaces enable
ACOS(config-cloud-provider-vmware-metrics) #memory enable
ACOS (config-cloud-provider-vmware-metrics) #packet-drop enable
ACOS (config-cloud-provider-vmware-metrics) #packet-rate enable
ACOS (config-cloud-provider-vmware-metrics) #server-down-count enable
ACOS(config-cloud-provider-vmware-metrics)#server-down-percentage
enable
ACOS(config-cloud-provider-vmware-metrics)#server-error enable
ACOS (config-cloud-provider-vmware-metrics) #sessions enable
ACOS(config-cloud-provider-vmware-metrics)#ssl-cert enable
ACOS (config-cloud-provider-vmware-metrics) #throughput enable
ACOS(config-cloud-provider-vmware-metrics)#tps enable
```

NOTE: For better throughput, you must enable only those metrics that are required.

To get resource-id value, go to vRealize Operations Web UI Home > Environment > Object Browser > All Objects > vCenter Adapter > Virtual Machine > vThunder and get the resource ID from the URL.

27



For more information on each CLI parameter, see the *Command Line Interface Reference*.

5. Verify the running configuration:

```
ACOS(config)#show running-config cloud-services cloud-provider
!Section configuration: 473 bytes
cloud-services cloud-provider
  azure
   metrics
      enable
     vrops-host 10.67.4.13
      active-partitions shared
      resource-id 3ae28ba2-c8b9-497f-8b98-76bedc93f31c
     cpu enable
     memory enable
     disk enable
      throughput enable
      interfaces enable
     cps enable
      tps enable
      server-down-count enable
      server-down-percentage enable
      ssl-cert enable
      server-error enable
      sessions enable
      packet-drop enable
      packet-rate enable
```

6. Verify the thunder-observability-agent.log file:

-bash# tail -f /a10data/log/thunder-observability-agent.log

7. View the vThunder metrics.

To view the Thunder metrics on VMware vRealize Operations Manager, perform the following steps:



- a. Ensure the vROps virtual machine is powered on and reachable.
- b. Create a dashboard for vThunder. For more information, see <u>Create a</u> <u>Dashboard</u>.
- c. Create an alert for vThunder. For more information, see Create an Alert.
- d. Create a notification for vThunder. For more information, see <u>Create a</u> <u>Notification</u>.
- e. From the vRealize Operations Web UI, go to Home > Visualize > Dashboard and select your dashboard created for the Thunder metrics.
- f. From **Object List**, double-click your Thunder instance.
- g. From **Metric Picker**, expand **Metrics** > **THUNDER** and double-click the following common metrics:
 - Memory Usage Percentage
 - Disk Usage Percentage

As a metric is selected, the corresponding data gets populated in the **Metric Chart** panel for the selected the time range.

- h. From **Metric Picker**, expand **Metrics** > **THUNDER-SHARED** or **THUNDER-Px** and double-click the following metrics:
 - CPU Usage Percentage (Data)
 - Throughput Rate (Global/BPS)
 - Interface Down Count (Data)
 - Total New Connection (Sec)
 - Transactions Rate (Sec)
 - Server Down Count
 - Server Down Percentage
 - SSL Errors Count
 - Server Errors Count
 - Total Session Count



- Packet Rate (Sec)
- Packet Drop Rate (Sec)

As the metric is selected, the corresponding data gets populated in the **Metric Chart** panel for the selected the time range.

To view multiple metrics data, select each of those metrics. The data corresponding to each metric is displayed in the **Metric Chart** panel.

NOTE: If you encounter any resource ID issues for cross-platform log monitoring, disable the VMware metric monitoring and re-enable it.

Create a Dashboard

To create a dashboard manually, perform the following steps:

- 1. From the vRealize Operations Web UI, go to Home > Visualize > Dashboards and click Create to add a new dashboard.
- 2. Provide a name to the new dashboard and double-click or drag the following widgets:
 - Object List
 - Metric Picker
 - Metric Chart
- 3. Click Show Interactions to create interactions.
- 4. Drag the connectors and create interactions.
- 5. Click **Save** to save the changes.

A dashboard for Thunder metrics is created.

Create an Alert

To create an alert definition manually, perform the following steps:

- 1. From the vRealize Operations Web UI, go to Home > Configure > Alerts and click Alert Definitions.
- 2. Click Add in the Alert Definitions window.
- 3. Enter or select the appropriate values in the following fields:



Table 8 : Alert tab fields

Field Name	Description
Name	Enter the alert name.
	Example
	ThunderAlert
Base Object Type	Select vCenter Adapter > Virtual Machine.
Under the Advanced Settings:	
Impact	Select Health.
Criticality	Select Critical.
Alert Type & Subtype	Select Application : Performance.

- 4. Click Next.
- 5. Click Select Specific Object to select your Thunder instance in the Symptoms / Conditions tab .
- 6. Select your Thunder instance and click **Select** in the **Select Object** window.

The selected Thunder instance is listed under **Conditions**.

- 7. Select **Metrics** > **Thunder** and drag the required metrics to the left-side panel.
- 8. Specify the appropriate alert condition.
- 9. Click Next.
- 10. Add the appropriate recommendations in the **Recommendations** tab, if needed.
- 11. Click Next.
- 12. Select appropriate policy in the **Policies** tab, if needed.
- 13. Click Next.

The **Notification** tab is displayed. The notification can be created after the alert definition is created. For more information, see <u>Create a Notification</u>.

14. Click **Create** in the **Notification** tab.

An alert definition is created and is listed in the **Alert Definition** window.

Create a Notification



To create a notification manually, perform the following steps:

- 1. From the vRealize Operations Web UI, go to Home > Configure > Alerts and click Notifications.
- 2. Click Add in the Notifications window.
- 3. Enter or select the appropriate values in the following fields:

Table 9 : Notifications tab

Field Name	Description
Name	Enter the notification name.
	Example
	ThunderAlertNotification
Notification Status	Select Enable.

- 4. Click Next.
- 5. In the **Criteria** field, select **Object Type** from the drop-down.

A field appears to select the object type.

6. Expand vCenterAdapter and select Virtual Machine from the drop-down.

The selected object type is listed under **Criteria**.

- 7. In the **Category** field, select **Alert Definition** from the drop-down created in the <u>Create an Alert</u>.
- 8. Search your alert definition.
- 9. Select your alert definition and drag it to add as the criteria.
- 10. Click **OK**.

The selected alert definition is listed under Category.

- 11. In the **Status** field under **Notify On**, select the alert status for which you want to receive the notifications.
- 12. Click Next.



- 13. In the **Outbound method** field, select **Standard Email Plugin** from the drop-down list.
- 14. Click **Create New Instance** to create a new instance for corresponding Outbound method.
- 15. Enter or select the appropriate values in the following fields:

Table 10 : Create New Instance

Field Name	Description
Instance Name	Enter the notification instance name.
	Example
	ThunderNotificationInstance
SMTP Host	Enter the URL or IP address of the email host
	server.
SMTP Port	Enter the SMTP port number used to connect with
	the email host server.
Secure Connection Type	Select SSL .
User Name	Enter the username that is used to connect to the
Password	Enter the password for the connection username that appears on the notification message.
Sender Email Address	Enter the email address of the sender.
Sender Name	Enter the display name of the sender email address.
Receiver Email Address	Enter the email address of the receiver that receives the notification.

16. Click **Save** to save the changes.

The new instance is populated in the **Select Instance** field.

- 17. Click Next.
- 18. Enter or select the appropriate values in the following fields for the default



template:

Table 11 : Select Payload Template tab

Field Name	Description
Recipient(s)	Enter the email addresses of the recipient to receive the notification.
Max Notifications	Enter the maximum number of notification to be sent for the active alert.
Delay to notify	Enter the delay time in minutes before sending a notification when a new alert is generated.

19. Click Create.

A new notification is created for the selected alert definition and it is listed in the **Notifications** window.

Publishing the vThunder Logs on VMware

When the vThunder instance is deployed on any AWS, Azure, or VMare cloud platform, the vThunder logs can be published to any one of the cloud platforms such as AWS CloudWatch, Azure Log Analytics Workspace, or VMware vRealize Log Insight (vRLI).

To publish the vThunder logs on VMware vRealize Log Insight, perform the following steps:

1. Log in to the deployed vThunder instance using CLI with the administrative privilege:

ACOS(config)#**admin** <admin_user>

For example

ACOS(config) #**admin** adminuser2

2. Import the VMware credentials file:

```
ACOS(config-admin:<admin_user>)#cloud-cred vmware-cred import <file_
transfer method>
```

The <file transfer method> can be any of the following:



```
use-mgmt-port Use management port as source port
tftp: Remote file path of tftp: file system(Format:
tftp://host/file)
ftp: Remote file path of ftp: file system(Format: ftp://
[user@]host[:port]/file)
scp: Remote file path of scp: file system(Format: scp://
[user@]host/file)
sftp: Remote file path of sftp: file system(Format: sftp://
[user@]host/file)
```

For example

```
ACOS(config-admin:adminuser2)#cloud-cred vmware-cred import
tftp://192.168.0.0/credentials.txt
```

For a sample credentials file, see VMware Credentials File.

3. Verify if the VMware credentials file is imported correctly:

```
ACOS(config-admin:<admin_user>)#cloud-cred vmware-cred show
vmware_vrops_username = XXXX
vmware vrops password = XXXX
```

4. Enable and configure the vThunder logs:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#vmware
ACOS(config-cloud-provider-vmware)#log
ACOS(config-cloud-provider-vmware-log)#enable
ACOS(config-cloud-provider-vmware-log)#vrli-host IP_address
ACOS(config-cloud-provider-vmware-log)#active-partitions name
```

For more information on each CLI parameter, see the *Command Line Interface Reference*.

5. Verify the running configuration:



```
ACOS(config)#show running-config cloud-services cloud-provider
!Section configuration: 103 bytes
cloud-services cloud-provider
vmware
log
enable
vrli-host 10.67.4.16
active-partitions shared
```

6. Verify the thunder-observability-agent.log file:

```
-bash# tail -f /a10data/log/thunder-observability-agent.log
```

- 7. View the vThunder logs on the VMware vRLI:
 - a. From a the vRealize Log Insight Web UI, go to Home > Explore Logs.
 - b. Click **Add Filter** and add the following filter criteria to search all the logs received from a specific Thunder IP:
 - _index: ip
 - condition: is
 - value: <vThunder_IP>
 - c. Add the following filter criteria to search all logs:
 - _index: source
 - condition: is
 - value: <Source_IP>
 - d. Verify if the logs are generated.

The following table lists the vThunder Logs filter options:

<u> </u>	
Filter	Description
hostname	Displays the vThunder resource ID.
log_type	Displays the vThunder system logs.
appname	Displays the application name.

Table 12 : Log Filters


Table 12 : Log Filters	s	
------------------------	---	--

Filter	Description
ip	Displays the vThunder IP address.
agent	Displays the agent name.
jobid	Displays the JOB ID provided in thunder-observability- agent.log file.
priority	Displays the Notice, Info, Error, and so on as per actual log entry.
partition	Displays the vThunder partition name.

Sample Cloud Credential File

The VMware cloud-cred file must be a text file and it should have the cloud-specific parameters.

VMware Credentials File

The sample VMware credentials.txt file is as follows:

vmware_vrops_username = XXXX
vmware_vrops_password = XXXX

Parameter	Description
vmware_	Specifies your vROps login credentials.
vrops_	
username	
vmware_	
vrops_	
password	

.

The external Thunder Observability Agent (TOA) is a lightweight autonomous data processing engine that can be externally installed and configured for any Thunder device.

The TOA offers the following capabilities for Thunder[®] Application Delivery Controller (ADC):

- Collects, processes, and publishes 14 Thunder metrics. The default data collection frequency is 1 minute. Thunder metrics can be sent to the platform where Thunder is deployed, which includes AWS, Azure, and VMware or can be sent to shared platforms like Elasticsearch (Kibana), Prometheus (Grafana), Splunk, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI). Metrics can be sent to any one platform at a time. For more information on Thunder metrics, see <u>Supported Thunder Metrics</u>.
- Collects, processes, and publishes Thunder Syslogs. The default data collection frequency is 1 minute. The logs can be published on various platforms like AWS, Azure, VMware, Kibana (Elasticsearch), Grafana (Prometheus and Pushgateway), Splunk, GCP, and OCI. Logs can be sent to any one platform at a time. For more information on Thunder logs, see <u>Supported Thunder Logs</u>.
- Manages the data collection, processing, aggregation, and publishing internally.
- Provides multitasking capabilities to collect and process data from multiple Thunder instances and their partitions simultaneously. By default, it collects data from a shared partition.
- TOA supports Shared and L3V partitions. The maximum number of partitions supported per Thunder is 20.
- Installs on any orchestration platform such as public cloud compute instances, private cloud physical or virtual machines, hypervisor VMs, and on-premise physical hardware and is self-driven.
- Installs on Linux, CentOS, and Ubuntu platforms as a Python Plugin installation package and Docker containerization.
- Supports single or multiple Thunder instances.



- Supports Thunder instances running under AWS Auto Scaling Group or Azure Virtual Machine Scale Set (VMSS).
- Collects data from any type of Thunder device installed on public cloud compute instances, private cloud physical or virtual machines, hypervisor VMs, and on-premise physical hardware installation.
- Publishes data to <u>Azure Cloud</u>, <u>AWS Cloud</u>, <u>VMware ESXi</u>, <u>Kibana (Elasticsearch)</u>, Grafana (Prometheus and Pushgateway), <u>Splunk,GCP</u>, and <u>OCI</u>.

Download Links

- Python Central Repository
- Docker Central Repository
- A10 GitHub Repository

The following figure shows the TOA workflow.



Figure 1 : TOA Workflow

.



Supported Technology

The following table provides TOA-supported technologies:

Table 14 : Supported Technologies

Name	Version	License		
Python	3.10	PSF License		
		Python 3.3 license Python.org		
Requests	2.27.1	Apache Software License 2.0		
Boto3	1.24.25	Apache 2.0 (amazon.com)		
google-auth	2.22.0	Apache Software License 2.0,		
		Apache 2.0 (google.com)		
oci	2.121.1	Apache Software License and		
		Universal Permissive License		

Supported Thunder Metrics

The following table lists the TOA-supported Thunder metrics:

Metric	Description
CPU Usage Percentage (Data)	Average data CPU usage, in percentage, for all data CPU configured within a Thunder instance for the last data collection cycle.
Memory Usage Percentage	Memory (RAM) usage, in percentage, of a Thunder instance for the last data collection cycle.
Disk Usage Percentage	Average disk storage usage, in percentage, for all disks associated with a Thunder instance for the last data collection cycle.
Throughput Rate	Total Thunder system global throughput bits per sec from

Table 15 : Supported Thunder Metrics



Table	15 :	gang	orted	Thunder	Metrics
10010	_		0.000	i i i a i i a c i	

Metric	Description		
(Global/BPS)	Thunder instance to the server for the last data collection cycle.		
Interface Down Count (Data)	Count of the total data network interfaces configured for a Thunder instance which is inactive for the last data collection cycle.		
Total New Connection (Sec)	Count of the total new connections sent from Thunder instance to the server for the last data collection cycle per second. This includes L4-conns-per-sec, L7-conns-per-sec, L7- trans-per-sec, ssl-conns-per-sec, and ip-nat-conns-per-sec.		
Transactions Rate (Sec)	Count of the total L7 transactions made per second from Thunder instance to the server for the last data collection cycle.		
Server Down Count	Count of the total web or app servers configured in the Thunder instance that are not reachable from Thunder for the last data collection cycle.		
Server Down Percentage	Percentage of the total web or app servers configured in the Thunder instance that are not reachable from Thunder for the last data collection cycle.		
SSL Errors Count	Count of the total errors that occurred during data transmission from Thunder to the server due to SSL connection, negotiate, encrypt, and decrypt for the last data collection cycle.		
Server Errors Count	Count of the total errors that occurred during data transmission from Thunder to the server with status codes 4xx and 5xx for that last data collection cycle.		
Total Session Count	Count of the total active sessions of the Thunder instance for the last data collection cycle.		
Packet Rate (Sec)	Count of the total packets sent from or received at the Thunder instance for the last collection cycle.		
	NOTE: Applicable for ACOS 5.2.1-P7, ACOS 6.0.0, and higher		

41

.....

•

•



Table	15 :	Sup	norted	Thunder	Metrics
Tuble	тэ.	Jup	porteu	munuci	WICTICS

Metric	Description
Packet Drop Rate (Sec)	Count of the total packets dropped while sending data from or receiving data at the Thunder instance for the last collection cycle.
	NOTE: Applicable for ACOS 5.2.1-P7, ACOS 6.0.0, and higher

Supported Thunder Logs

The following table lists the TOA-supported Thunder logs:

Table 16 : Supported Thunder Logs

Logs	Description
SysLogs	Thunder internal logs such as:
	 SSL connection, negotiate, encrypt, and decrypt
	Status codes 4xx and 5xx

Supported ACOS Versions

The following table provides the TOA-supported ACOS versions:

ACOS Version	TOA Ver- sion	ADC	CGN	SSLi	TPS
64-bit Advanced Core OS (ACOS) version 6.0.3-P1	>=1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 6.0.3	>=1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS)	>=1.0.0	V	Х	Х	Х

Table 17 : Supported ACOS versions



Table 17 : S	Supported	ACOS	versions
--------------	-----------	------	----------

ACOS Version	TOA Ver- sion	ADC	CGN	SSLi	TPS
version 6.0.2					
64-bit Advanced Core OS (ACOS) version 6.0.1	>=1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 6.0.0-P2- SP1	>= 1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 6.0.0-P1	>= 1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 5.2.1-P9	>= 1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 5.2.1-P8	>= 1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 5.2.1-P7	>= 1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 5.2.1-P6	>= 1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 5.2.1-P5	>= 1.0.0	V	Х	Х	Х
64-bit Advanced Core OS (ACOS) version 4.1.4- GR1-x	1.0.0	V	X	Х	X



•



Supported Platforms

The following table provides the TOA supported platforms and monitoring applications:

Cloud Platform	Monitoring Applications
AWS Cloud	CloudWatch
Azure Cloud	Application Insights
	 Log Analytics Workspace
VMware ESXi (On Premise)	 vRealize Operations Manager (vROps)
	 vRealize Log Insight (vRLI)
Elasticsearch	• Kibana
Prometheus	• Grafana
Splunk	 Splunk Analytics
	Splunk Dashboard
Google Cloud Platform (GCP)	Metrics Explorer
	Logs Explorer
Oracle Cloud Infrastructure (OCI)	Metrics Explorer
	Log Search

Table 18 : Supported platforms and monitoring tools

Install TOA

TOA is a standalone software that can be installed on any orchestration platform. The following installation options are available:

• Python Plugin Installation

TOA is installed on Linux/CentOS/Ubuntu platform using a Python plugin.

Figure 2 illustrates the installation of TOA in the Python plugin architecture.

44



Figure 2 : Python Plugin Installation Architecture



<u>Containerized Installation</u>

TOA is installed on the Kubernetes cluster using a docker image.

Figure 3 illustrates the installation of TOA in a containerized architecture.

Figure 3 : Containerized Installation Architecture



Python Plugin Installation

This section describes how to install and configure a Thunder Observability Agent (TOA) on any public cloud, private cloud, hypervisor VM, or on-premise machine using Python plugin.

The following topics are covered:

Prerequisites	46
Installation Steps	46





Prerequisites

The following tables list the prerequisites for installing TOA using the Python plugin:

Hardware Dependencies

Table 19 : Hardware Dependencies

Requirement	Description
Virtual Machine	2 GB RAM, 1 CPU, 4 GB NOTE: The hardware configuration is applicable for one to ten Thunder instances with moderate
	transactions.
Platform	Any public cloud, private cloud, hypervisor VM, or on- premise machine.
Instance Type	Dedicated or Shared.

Software Dependencies

Requirement	Description
Operating System	 <u>CentOS 7</u> or higher
	 <u>Ubuntu 20</u> or higher
Python	3.6 or higher
Access-level	Root

Table 20 : Software Dependencies

Installation Steps

To install TOA using the Python plugin, perform the following steps:

- 1. Log in to the instance where you want to install TOA.
- 2. Depending on your operating system, install Python version, Crontab, and Syslog. For the installation steps, see <u>Install Python, Crontab, and Syslog</u>.

If the Python version, Crontab, and Syslog are already installed, skip this step.

46



3. Create a virtual environment.

```
pip3 install virtualenv
cd /usr
virtualenv toaenv
source toaenv/bin/activate
```

4. Run the following command to install the TOA:

```
pip3 install thunder-observability-agent
```

After the execution, all the following configuration files are available at the default location /usr/toaenv/thunder-observability-agent:

- main.properties
- config.json
- logging.conf
- init.sh
- 5. Run init.sh, a one-time execution script, to enable crontab job for data collection and create credential files for Thunder and cloud providers:

```
cd /usr/toaenv/thunder-observability-agent
sh init.sh
```

After the execution, all the following files are available at the /root/ hidden folder:

- .thunder/credentials
- .aws/config
- .aws/credentials
- .azure/credentials
- .vmware/credentials
- .splunk/credentials
- .elasticsearch/credentials
- .pushgateway/credentials



- .gcp/credentials
- .oci/credentials
- 6. If you want to change the default location of the TOA config files, update the environment variable TOA_CONFIG_PATH and the Logging file.

If you do not want to change the default location, skip this step.

- 7. If you want to change the credentials file location, update the Main Properties file.
- 8. Verify Crontab configuration.
- 9. Verify TOA installation.

The agent.log file is created at the /var/log/thunder-observability-agent path. For the sample agent.log file, see <u>TOA Logging</u>.

10. Edit the configuration files.

Depending on your cloud provider, configure the following files mentioned in Table 21:

- Thunder credentials to collect data from Thunder.
- Cloud credentials to establish a connection with the cloud provider.
- Config.json to publish required metrics or logs.

Table 21 : Cloud specific Configuration Fil	es
---	----

Cloud	File name
AWS	<u>Thunder Credentials</u>
	<u>AWS Config</u>
	<u>AWS Credentials</u>
	<u>Config JSON</u>
Azure	<u>Thunder Credentials</u>
	<u>Azure Credentials</u>
	<u>Config JSON</u>
VMware	<u>Thunder Credentials</u>



Table 21 : Cloud	specific	Configuration	Files
------------------	----------	---------------	-------

Cloud	File name	
	<u>VMware Credentials</u>	
	<u>Config JSON</u>	
Elasticsearch	<u>Thunder Credentials</u>	
	Elasticsearch Credentials	
	<u>Config JSON</u>	
Prometheus	<u>Thunder Credentials</u>	
(PushGateway)	PushGateway Credentials	
	<u>Config JSON</u>	
Splunk	<u>Thunder Credentials</u>	
	Splunk Credentials	
	<u>Config JSON</u>	
GCP	<u>Thunder Credentials</u>	
	<u>GCP Credentials</u>	
	<u>Config JSON</u>	
ОСІ	<u>Thunder Credentials</u>	
	OCI Credentials	
	<u>Config JSON</u>	

11. Monitor Thunder metrics and logs.

For more information, see Monitor Dashboard.

Containerized Installation

This section describes how to install TOA in a single container pod of the Kubernetes cluster using YAML files.

The following topics are covered:

Prerequisites	. 50
Installation Steps	50



Prerequisites

The following are the prerequisites for installing TOA using Containers:

- Kubernetes environment
- Download the <u>Kubernetes TOA manifest files</u> installation files.

Installation Steps

To install the TOA in a container, perform the following steps:

1. Run the following command to create TOA namespace:

kubectl create namespace thunder-observability-agent

2. Run the following command to set TOA as the default Kubernetes namespace:

```
kubectl config set-context --current --namespace=thunder-observability-
agent
```

3. Edit the YAML files.

Depending on your cloud provider, configure the following files mentioned in Table 22:

- Thunder credentials to collect data from Thunder.
- Cloud credentials to establish a connection with the cloud provider.
- configmap.yaml to publish required metrics or logs.

Table 22 : 0	Cloud	specific	Configuration	Files

Cloud	File name	Reference
AWS	aws-configmap.yaml	Main Properties
		<u>Config JSON</u>
		• Logging
	aws-secret.yaml	AWS Config
		AWS Credentials
		• Thunder Credentials
Azure	azure-configmap.yaml	Main Properties
		<u>Config JSON</u>



Table 22 : Cloud specific Configuration Fi	les
--	-----

Cloud	File name	Reference
		 Logging
	azure-secret.yaml	<u>Azure Credentials</u>
		<u>Thunder Credentials</u>
VMware	vmware-configmap.yaml	Main Properties
		<u>Config JSON</u>
		Logging
	vmware-secret.yaml	VMware Credentials
		• Thunder Credentials
Elasticsearch	elasticsearch-	Main Properties
	configmap.yaml	<u>Config JSON</u>
		• Logging
	elasticsearch-secret.yaml	Elasticsearch
		<u>Credentials</u>
		<u>Thunder Credentials</u>
Prometheus	pushgateway-configmap.yaml	Main Properties
		<u>Config JSON</u>
		• Logging
	pushgateway-secret.yaml	PushGateway
		<u>Credentials</u>
		<u>Thunder Credentials</u>
Splunk	splunk-configmap.yaml	<u>Main Properties</u>
		<u>Config JSON</u>
		 Logging
	splunk-secret.yaml	<u>Splunk Credentials</u>
		• Thunder Credentials
Google Cloud (GCP)	gcp-configmap.yaml	Main Properties

••••



Table 22 : Cloud specific Configuration Files

Cloud	File name	Reference
		<u>Config JSON</u>
		• Logging
	gcp-secret.yaml	GCP Credentials
		• Thunder Credentials
		Base64 Conversion
Oracle Cloud	oci-configmap.yaml	Main Properties
Infrastructure		<u>Config JSON</u>
		• Logging
	oci-secret.yaml	OCI Credentials
		• Thunder Credentials
		Base64 Conversion

4. Run the following commands to apply the cloud-specific configuration:

kubectl apply -f <cloud-provider>-configmap.yaml kubectl apply -f <cloud-provider>-secret.yaml

5. Run any of the following commands to apply and create a container:

kubectl apply -f <cloud-provider>-pod.yaml

or

```
kubectl apply -f <cloud-provider>-cronjob.yaml
```

6. Verify TOA installation.

The agent.log file is created at the /var/log/thunder-observability-agent path. For the sample agent.log file, see <u>TOA Logging</u>.

7. Monitor Thunder metrics and logs.

For more information, see Monitor Dashboard.

NOTE: By default, the system works using the default configuration. TOA only supports a single pod installation.

52



Configure TOA

This section lists the global TOA configuration files and cloud-specific configuration files that are required to establish a connection with TOA.

The following topics are covered:

Global Configuration	53
Cloud-specific Configuration	63
Data Collection Configuration	71
Data Publish Configuration	75

Global Configuration

The following files are used for the global TOA configurations:

- Main Properties
- Logging
- <u>Crontab</u>

Main Properties

This file lists the global TOA configuration parameters. If you want to change the configuration file path, this file must be updated with the correct paths.

File Path: /usr/toaenv/thunder-observability-agent/main.properties

Parameter	Description	Default Value
log_ collection_ delay_min	Specifies the latency of log collection in minutes.	0
	The system considers the Thunder logs that are generated from the Start Time until the End	

Table 23 : File Parameters



Table 23 : File Parameters

Parameter	Description	Default Value
	Time as:	
	Start Time = Last data collection time	
	End Time = Current data collection time - <log_ collection_delay_min></log_ 	
	Example	
	If the current data collection time is 10:00:00 AM and the last data collection time is 09:59:00 AM, then:	
	the Start Time is 9:59:00 AM.	
	the End Time is 10:00:00 AM (which is 10:00:00 AM - 0 minutes).	
	So, TOA collects all the logs generated by Thunder instance from 9:59:00 AM to 10:00:00 AM.	
cron_job_ frequency min	Specifies the cron job frequency in minutes.	1
	This parameter should match with the crontab -e job definition. The system considers crontab -e for job scheduling. If the	



Table 23 : File Parameters

Parameter	Description	Default Value
	frequency is changed in this parameter, it should also change in the crontab file.	
	For more information, see <u>Crontab</u> .	
http_ssl_ verify	Disables SSL certificate verification over HTTPS.	False
	If a user wants to enable SSL:	
	 For CA signed certificate configured in Thunder, set the parameter to True. 	



Table 23 : File Parameters

Parameter	Description		Default Value
	NOTE:	For a self-	
		signed	
		certificate	
		configured	
		in	
		Thunder,	
		create a	
		*.pem file,	
		import the	
		Thunder	
		public	
		certificate,	
		and	
		provide	
		the path	
		in place of	
		True.	
		Example	
		/usr/toae	
		nv/thunde	
		r-	
		observabi	
		lity-	
		agent/toa	
		.pem	



Table 23 : File Parameters

Parameter	Description	Default Value
	NOTE: If vROps and vRLI haves self-signed certificate s, then their public certificate s must be imported in *.pem file.	
http_con- nection_ timeout_sec	Specifies the maximum amount of time, in seconds, that the TOA waits to set up an HTTP connection to com- municate with any Thun- der instance.	15
max_threads	Specifies the maximum number of threads to be created at the same time.	2000
config_path	Specifies the configuration file path for publishing logs and metrics.	/usr/toaenv/ thunder-observability-agent/ config.json
thunder_ credentials_ path	Specifies the configuration file path to collect data from any of the following: • <u>Single Thunder</u>	/root/.thunder/ credentials

••••



Table 23 : File Parameters

Parameter	Description	Default Value
	Instance	
	<u>Multiple Thunder</u> <u>Instances</u>	
	<u>Thunder Instances in</u> <u>AWS Auto scaling</u> <u>Group</u>	
	• Thunder Instances in <u>Azure VMSS</u> .	
aws_ credentials_ path	Specifies the AWS credentials file path to establish a connection and publish the data to AWS CloudWatch.	/root/.aws/ credentials
	NOTE: Applicable only if you want to publish the Thunder data to AWS CloudWatch.	
aws_config_ path	Specifies the AWS configuration file path to publish the data.	/root/.aws/ config
	NOTE: Applicable only if you want to publish the Thunder data to AWS CloudWatch.	
azure_ credentials_ path	Specifies the Azure credentials file path to establish the	/root/.azure/ credentials



Table 23 : File Parameters

Parameter	Description	Default Value
	connection and publish the data.	
	NOTE: Applicable only if you want to publish the Thunder data to Azure Application Insights and Azure Log Analytics Workspace.	
vmware_ credentials_ path	Specifies the VMware credentials file path to establish the connection and publish the data. NOTE: Applicable only if you want to publish the	/root/.vmware/ credentials
	Thunder data to VMware vROps.	
elasticsearch_ credentials_ path	Specifies the Elasticsearch credentials file path to establish the connection and publish the data.	/root/.elasticsearch/credentials



Table 23 : File Parameters

Parameter	Description	Default Value
	NOTE: Applicable only if you want to publish the Thunder data to Elasticsearch Kibana.	
pushgateway_ credentials_ path	Specifies the Pushgateway credentials file path to establish the connection and publish the data.	/root/.pushgateway/credentials
	NOTE: Applicable only if you want to publish the Thunder data to Prometheus Grafana.	
<pre>splunk_ credentials_ path</pre>	Specifies the Splunk credentials file path to establish the connection and publish the data. NOTE: Applicable only if you want to publish the Thunder data to Splunk.	/root/.splunk/credentials
gcp_cre- dentials_path	Specifies the GCP credentials file path to establish the connection and publish	/root/.gcp/credentials

••••



Table 23 : File Parameters

Parameter	Description	Default Value
	the data. NOTE: Applicable only if you want to publish the Thunder data to Google Cloud Platform.	
oci_cre- dentials_path	Specifies the OCI credentials file path to establish the connection and publish the data.	/root/.oci/credentials
	NOTE: Applicable only if you want to publish the Thunder data to Oracle Cloud Infrastructure.	

Logging

This file lists the TOA logging configurations.

File Path: /usr/toaenv/thunder-observability-agent/logging.conf

```
[loggers]
keys=root
[handlers]
keys=hand01
[formatters]
keys=form01
[logger_root]
```

••••



```
level=INFO
 handlers=hand01
 [handler_hand01]
 class=logging.handlers.RotatingFileHandler
 # ERROR, INFO
 level=INFO
 formatter=form01
 # logFilePath, append, maxBytes, backupCount
 args=('/var/log/thunder-observability-agent/agent.log', 'a', 5000000,
100)
 [formatter form01]
 format=%(asctime)s - (%(filename)s:%(lineno)d) - %(levelname)s - %
(message)s
 datefmt=
 style=%
 validate=True
 class=logging.Formatter
```

Crontab

By default, TOA creates the crontab configuration file that contains the command to configure the data collection frequency. This command is executed at regular intervals.

To verify the crontab configuration, perform the following steps:

1. Run the following command to verify the Python version:

python3 --version

In case if the version is other than python3.10, then replace in the crontab.

2. Run the following command to open the crontab file:

\$ crontab -e



3. In case if required, edit the Python version as appropriate:

```
*/1 * * * * /usr/toaenv/bin/python3 /usr/toaenv/lib/python3.10/site-
packages/thunder-observability-agent/toa.py
```

NOTE: By default, TOA collects data at a frequency of 1 minute. If you are changing the frequency in the crontab file, you should change the cron_job_frequency_min parameter in the main.properties as well and vice-versa. For more information, see <u>Main Properties</u>.

Cloud-specific Configuration

The following information is required to setup the cloud-specific configuration to publish the Thunder metrics and logs.

- <u>AWS Config</u> (Applicable only if you want to publish the data to AWS CloudWatch)
- <u>AWS Credentials</u> (Applicable only if you want to publish the data to AWS CloudWatch)
- <u>Azure Credentials</u> (Applicable only if you want to publish the data to Azure Application Insights and Azure Log Analytics Workspace)
- <u>VMware Credentials</u> (Applicable only if you want to publish the data to vRealize Operations (vROps))
- Elasticsearch Credentials

(Applicable only if you want to publish the data to Elasticsearch Kibana)

• PushGateway Credentials

(Applicable only if you want to publish the data to Prometheus Grafana)

• Splunk Credentials

(Applicable only if you want to publish the data to Splunk)

GCP Credentials

(Applicable only if you want to publish the data to GCP)



OCI Credentials

(Applicable only if you want to publish the data to OCI)

AWS Config

This file lists the AWS configurations to publish the Thunder metrics or logs to AWS CloudWatch.

File Path: /root/.aws/config

Update the following parameters according to your AWS setup:

[default] region = XXXX output = XXXX

Table 24 : AWS Config File Parameters

Parameter	Description	
region	Specifies the AWS logged-in user's working region.	
	Example	
	us-east-1	
output	Specify json as the AWS CLI output format.	

For sample configuration, see Examples.

AWS Credentials

This file lists the AWS credential configurations to publish the Thunder metrics or logs to AWS CloudWatch.

File Path: /root/.aws/credentials

Update the following parameters according to your AWS setup:

```
[default]
aws_access_key_id = XXXX
aws secret access key = XXXX
```



Table 25 : AWS Credentials File Parameters

Parameter	Description	
aws_access_key_id	To get the access key ID and secret access key, perform the following steps:	
	1. Open the <u>IAM console</u> .	
	2. On the navigation menu, select Users .	
aws_secret_access_key	3. Select your IAM user name.	
	 Open the Security credentials tab, and select Create access key. 	
	5. To view the new access key, select Show .	

For sample configuration, see Examples.

Azure Credentials

This file lists the Azure credential configurations to publish the Thunder metrics or logs to Azure Application Insights and Azure Log Analytics Workspace respectively.

File Path: /root/.azure/credentials

Update the following parameters according to your Azure setup:

```
azure_workspace_primary_key = XXXX
azure_client_id = XXXX
azure_secret_id = XXXX
azure_tenant_id = XXXX
azure_location = XXXX
```

Table 26 : Azure Credentials File Parameters

Parameter	Description
azure_workspace_ primary_key	To get the workspace primary key, go to Azure Portal > Azure services > Log Analytics workspaces > <log_ analytics_workspace=""> > Settings > Agents.</log_>
	Figure 4 : Agents window



Table 26 : Azure Credentials File Parameters

Parameter	Description		
	And region of a constraint of a con		
azure_client_id	To get the client ID, secret ID, and tenant ID, go to Azure Portal > Azure services > Azure Active Directory		
	> App Registration > Owned applications >		
	<application_name>.</application_name>		
azure_secret_id			
	Figure 5 : Azure active directory - App registrations window		
	Home 2 Alb Networks App registrations & -		
	Azarativis Unicology + Heer registration) Induction () Refer. 1 Download () Refer. 2 Downloa		
azure_tenant_id	Review Nationals Provide Nationals Company and color problem Company Compan		
	Manager All applications Detend applications ▲ Users All opplications (2.5 str typing digitary more are particulated Select (0 to ther there r) *********************************		
	Control Identifies Zeplandern Sound Zeplandern Sound Daplay ware 1, Daplay ware 1, Zeplandern Sound Zeplan		
	A Annihestink units Deligned admin parwes 2//002		
azure location	To get the location, go to Azure Portal > Azure		
a_a_o	services > Resource Groups >		
	Services > Resource Groups > <your_resource_group></your_resource_group>		
	> Overview > Essentials > Location. Figure 6 : Resource Group window		
	(e) thereas area → → → → → → → → → → → → → → → → → → →		
	D Sanch ≪ + Cream @ Manageriese ∨ @ Delete resource group () Refeat ½ Exports CDV % Open query Assign tags → More ∨ @ Delete *** However A function		
	Control School Sch		
	Tops		
	Fevera Resources Recommendations (2) Strittons The for any field. The evenant all X: Logarion equals all X: Logarion equals all X: Incerting		
	Deployments Showing 1 to 24 of 24 records.		
	Verset Type 1 Location 1; Name 1; Type 1; Location 1; Verset Verset/second Neme transition		
	In Properties Construction		
	Cost Management III Share Annuales - tok-mail-applicing/sts Simat detector sites toke Global *** 5. Cost analysis IIII Share Annuales - tok-mail-applicing/sts IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		
	Cost dent (preview) C		

For sample configuration, see Examples.



VMware Credentials

This file lists the VMware credential configurations to publish the metrics or logs.

File Path:/root/.vmware/credentials

Update the following parameters according to your VMware setup:

vmware_vrops_username = XXXX
vmware vrops password = XXXX

Table 27 : VM ware Credentials File Parameters

Parameter	Description
vmware_vrops_username	Specifies your vROps login credentials.
vmware_vrops_password	

For sample configuration, see **Examples**.

Elasticsearch Credentials

This file lists the Elasticsearch credential configurations to publish the metrics or logs.

```
File Path: /root/.elasticsearch/credentials
```

Update the following parameters according to your Elasticsearch setup:

```
username = XXXX
password = XXXX
```

Table 28 : Elasticsearch Credentials File Parameters

Parameter	Description
username	Specifies your Elasticsearch login credentials.
password	

For sample configuration, see Examples.

PushGateway Credentials

This file lists the PushGateway credential configurations to publish the metrics or logs.

67



File Path: /root/.pushgateway/credentials

Update the following parameters according to your PushGateway setup:

username = XXXX password = XXXX

Table 29 : PushGateway Credentials File Parameters

Parameter	Description
username	Specifies your PushGateway login credentials.
password	

For sample configuration, see **Examples**.

Splunk Credentials

This file lists the Splunk credential configurations to publish the metrics or logs.

File Path: /root/.splunk/credentials

Update the following parameters according to your Splunk setup:

token_log = XXXX
token metric = XXXX

Table 30 : Splunk Credentials File Parameters

Parameter	Description
token_log	Specifies your Splunk HEC token for logs and metrics.
token_metric	

For sample configuration, see **Examples**.

GCP Credentials

This file lists the GCP credential configurations to publish the metrics or logs.

File Path: /root/.gcp/credentials

Update the following parameters according to your GCP setup:

gcp_project_id = XXXX
gcp service key path = XXXX



Table 31 : GCP	Credentials F	ile Parameters
----------------	---------------	----------------

Parameter	Description
gcp_project_id	Specifies your GCP project ID and path to the service account key file.
	To obtain the GCP project ID and service account key file path, perform the following steps:
	 Open <u>Google Cloud Console</u> and select the project you want to work with.
	2. Navigate to IAM & Admin > Service Accounts.
	 Click Create Service Account and provide the service account details.
	 Click Create and continue, followed by Done. The service account will be created.
	 On the Service Accounts page, select the created service account and click the three dots () on the Action column.
gcp_service_key_path	6. Select Manage Keys.
	The Keys page will be displayed.
	 Click the Add key drop-down menu and select Create new key.
	8. Select the Key type as JSON and click Create.
	The service account key file will be download to your system.
	 Open the file in a text editor and locate the project_id field. The value of this keys represents gcp_project_id in the GCP credentials file.
	 Store the downloaded JSON securely and provide its path as the gcp_service_key_path in the GCP credentials file.

For sample configuration, see Examples.

69

. . : : : : : : : : :



OCI Credentials

This file lists the OCI credential configurations to publish the metrics or logs.

File Path: /root/.oci/credentials

Update the following parameter according to your OCI setup:

oci_api_key_path= XXXXXXXX

Table 32 : OCI Credentials File Parameter

Parameter	Description
oci_api_ key_path	Specifies the path to the private key file used for authenticating the OCI services.
	To obtain the oci_api_key_path, perform the following steps:
	 Log in to the Oracle Cloud Infrastructure console, open the Profile menu, and click My Profile.
	2. In the Resources section, click API Keys .
	3. Click Add API Key.
	The Add API Key dialog will be displayed.
	4. Click Download Private Key.
	The file will be downloaded to your system. Store this file securely.
	5. Click Add.
	The Configuration File Preview page will be displayed. This page allows you to preview the configuration file. This file includes basic authentication information required to create your configuration file.
	 Copy and paste the configuration snippet from the text box into your text editor and save the configuration file without specifying any file extension.
	 After pasting the snippet, update the key_file parameter with the location where the private key file is saved (downloaded and saved previously).



Table 32 : OCI Credentials File Parameter

Parameter	Description
	The newly created configuration file (without any file extension) is considered an OCI API key file.
	8. Provide this API key file path as the oci_api_key_path in the OCI credentials file.

For sample configuration, see <u>Examples</u>.

Data Collection Configuration

In your topology, there can be a single, multiple, or auto scale Thunder instances that are either installed on AWS, Azure, or VMware compute instances. To collect the Thunder metrics or logs, configure the Thunder credentials file depending on the type of Thunder instance/s:

- Single Thunder Instance
- <u>Multiple Thunder Instances</u>
- Thunder Instances in AWS Auto scaling Group
- Thunder Instances in Azure VMSS

For more information on TOA - Thunder configuration with, see <u>TOA Thunder</u> <u>Configuration Matrix</u>.

Thunder Credentials

This file lists the Thunder credential configurations to collect the Thunder metrics, logs, or both.

File Path: /root/.thunder/credentials

Update the Thunder credentials file to provide the credentials of the Thunder instance/s whose metrics or logs are to be monitored as per the type of Thunder instance:

Single Thunder Instance

Provide the details of the Thunder instance running on any platform.



```
{
    "thunders": [{
        "ip": "XXXX",
        "username": "XXXX",
        "password": "XXXX",
        "resource_id": "XXXX",
        "active_partitions": "shared"
    }]
}
```

Multiple Thunder Instances

Provide the details of the Thunder instances running on any platform.

```
{
    "thunders": [{
        "ip": "XXXX",
        "username": "XXXX",
        "password": "XXXX",
        "resource_id": "XXXX",
        "active_partitions": "shared"
     },
        {
        "ip": "XXXX",
        "username": "XXXX",
        "username": "XXXX",
        "password": "XXXX",
        "resource_id": "XXXX",
        "active_partitions": "shared"
     }]
}
```

Thunder Instances in AWS Auto scaling Group

Provide the details of the Thunder instances running in AWS Auto Scaling Group.


```
"autoscale" : 1,
"provider" : "aws",
"thunders": [{
    "username": "XXXX",
    "password": "XXXX",
    "resource_id": "XXXX",
    "active_partitions": "shared"
}]
```

Thunder Instances in Azure VMSS

Provide the details of Thunder instances running in Azure VMSS.

```
"autoscale" : 1,
"provider" : "azure",
"thunders": [{
"username": "XXXX",
"password": "XXXX",
"resource_id": "XXXX",
"active_partitions": "shared"
}]
```

Table 3	33 :	Thunder	Credentials	File	Parameters
---------	------	---------	-------------	------	------------

Parameter	Description
autoscale	Specify 1 if the Thunder instance is in AWS auto scale group or Azure virtual machine scale set.
	By default, it is disabled.
provider	Specifies the cloud provider only if the Thunder instance is in AWS auto scale group or Azure virtual machine scale set (autoscale=1). The following options are available:
	• aws
	• azure



Table 33 : Thunder Credentials File Parameters

Parameter	Description
thunders	Specifies the Thunder instance details. The following parameters are available:
	• ip
	• username
	• password
	• resource_id
ip	Specifies the Thunder instance IP address.
username	Specifies the Thunder instance username.
password	Specifies the Thunder instance password.
resource_id	Specifies the compute instance resource IDS on which Thunder is deployed.
	For more information, see Get Resource ID.
active_partitions	Specifies one or more comma-separated partition/s for which the Thunder metrics or logs are viewed. By default, the active partition is "Shared".
	For example: "SHARED, Px"
	The maximum number of partitions supported per Thunder is 20.
	Only L3V active partitions are supported.
	To view Thunder metrics or logs of all active partitions, specify "*".
	To collect data from one active partition, one session is required through management interface.
	For example : If a user has defined 20 partitions in one Thunder device then 20 concurrent sessions are created in the device while collecting the data.

For sample configuration, see Examples.

74



TOA Thunder Configuration Matrix

The following table provides the TOA Thunder Configuration Matrix.

Table 34 : TOA Thunder Configuration Matrix

Logs	Metrics	Cron Cycle	Partition per Thunder	Maximum Number of Thunder devices
Enabled	Enabled	1 min	Up to 20 Partitions on each Thunder	Up to 05 Thunder Device
Enabled	Enabled	1 min	Up to 08 Partitions on each Thunder	Up to 10 Thunder Device
Enabled	Enabled	1 min	Up to 06 Partitions on each Thunder	Up to 15 Thunder Device

For example: If all logs and all metrics are enabled for every 1 minute of the data collection cycle with 20 active partitions on each Thunder device, ideally up to 5 Thunder devices can be configured per TOA instance.

Data Publish Configuration

The Thunder metrics and logs can be published on the cloud platforms such as AWS, Azure, VMware, Kibana (Elasticsearch), Grafana (Prometheus and Pushgateway), Splunk, Google Cloud Platform (GCP), or Oracle Cloud Infrastructure (OCI). To publish the Thunder metrics or logs, configure the config.json file with the appropriate TOA parameters for the required cloud platform:

- Metrics
 - <u>AWS</u>
 - <u>Azure</u>
 - <u>VMware</u>
 - Elasticsearch
 - PushGateway
 - <u>Splunk</u>



- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI)
- Logs
 - <u>AWS</u>
 - <u>Azure</u>
 - <u>VMware</u>
 - Elasticsearch
 - Prometheus
 - <u>Splunk</u>
 - Google Cloud Platform (GCP)
 - Oracle Cloud Infrastructure (OCI)

Config JSON

This file lists the TOA configurations to collect Thunder metrics or logs and enable the required cloud provider.

File Path: /usr/toaenv/thunder-observability-agent/config.json

Metrics

Depending on your cloud platform, configure the parameters to publish the Thunder metrics.

AWS

Configure the following parameters in the config.json to publish Thunder metrics to the AWS CloudWatch. By default, all the metrics are enabled. You can enable one or more Thunder Metrics.

NOTE: For better throughput, you must enable only those metrics which are required.



• • • •

Table 35 : AWS	Configuration	Parameters
----------------	---------------	------------

Parameter	Description	Default Value
aws_provider	Specify 1 to publish selected metric/s, logs, or both to AWS.	0
	By default, it is disabled and does not send metric to AWS. To publish metric/s it is mandatory to enable AWS as a provider.	
aws_metric	Specify 1 to publish metrics to AWS CloudWatch. It sends the data only if aws_provider is also enabled.	0
	By default, it is disabled.	
aws_cpu	Specify 1 to publish the deployed Thunder instances' average data CPU usage (percentage) on the AWS CloudWatch. If the aws_provider and aws_metrics parameters are enabled, TOA sends this metric to the AWS CloudWatch.	1
	By default, it is enabled.	
aws_memory	Specify 1 to publish the deployed Thunder instances' memory usage (percentage) on the AWS CloudWatch. By default, it is enabled.	1
aws_disk	Specify 1 to publish the deployed Thunder instances' storage disk usage on the AWS CloudWatch. By default, it is enabled.	1
aws_throughput	Specify 1 to publish the deployed Thunder instances' active throughput on the AWS CloudWatch.	1



Table 35 :	AWS	Configuration	Parameters
------------	-----	---------------	------------

Parameter	Description	Default Value
	By default, it is enabled.	
aws_interfaces	Specify 1 to publish the deployed Thunder instances' interface down count on the AWS CloudWatch.	1
	By default, it is enabled.	
aws_cps	Specify 1 to publish the deployed Thunder instances' new connection rate per second on the AWS CloudWatch.	1
	By default, it is enabled.	
aws_tps	Specify 1 to publish the deployed Thunder instances' transaction rate per second on the AWS CloudWatch.	1
	By default, it is enabled.	
aws_server_down_ count	Specify 1 to publish the deployed Thunder instances' server down count on the AWS CloudWatch. By default, it is enabled.	1
aws_server_down_ percentage	Specify 1 to publish the deployed Thunder instances' configured web/app servers down percentage on the AWS CloudWatch. By default, it is enabled.	1
aws_ssl_cert	Specify 1 to publish the deployed Thunder instances' SSL cert error count on the AWS CloudWatch. By default, it is enabled.	1
aws_server_error	Specify 1 to publish the deployed	1

••••

.....



Parameter	Description	Default Value
	Thunder instances web/app servers 4xx, 5xx errors count on the AWS CloudWatch.	
aws_sessions	Specify 1 to publish the deployed Thunder instances' active session count on the AWS CloudWatch. By default, it is enabled.	1
aws_packet_rate	Specify 1 to publish the deployed Thunder instances' packet rate on the AWS CloudWatch. By default, it is enabled.	1
aws_packet_drop	Specify 1 to publish the deployed Thunder instances' packet drop count on the AWS CloudWatch. By default, it is enabled.	1

Azure

Configure the following parameters in the config.json to publish Thunder metrics to the Azure Application Insights. By default, all the metrics are enabled. You can enable one or more Thunder Metrics.

NOTE:	For better throughput, you must enable only those metrics which
	are required.

Table 36 : Azure Configuration Parameters

Parameter	Description	Default Value
azure_provider	Specify 1 to publish selected metric/s, logs, or both to Azure.	0

79





Table 36 : Azure Configuration Parameters

Parameter	Description	Default Value
	By default, it is disabled and does not send metrics to Azure. To publish metric/s it is mandatory to enable Azure as a provider.	
azure_metric	Specify 1 to send metrics to Azure Application Insights. It sends the data only if azure_provider is also enabled.	0
	By default, it is disabled.	
azure_metric_ resource_id	Specifies the Azure Application Insights resource ID.	<azure_ metric_ resource</azure_
	To get this value, go to Azure Portal > Azure services > Application Insights > <your_< td=""><td></td></your_<>	
	Thunder_instance> > Properties > Resource ID.	
	Example	
	<pre>/subscriptions/07dxxxxxxxx/ resourceGroups/ <resource_group_name>/ providers/microsoft.insights/ components/<app-insight-name></app-insight-name></resource_group_name></pre>	
azure_cpu	Specify 1 to publish the deployed Thunder instances' average data CPU usage (percentage) on the Azure Application Insights. If the azure_provider and azure_ metrics parameters are enabled, TOA sends this metric to the Azure Application Insights.	1
		-
azure_memory	Specify 1 to publish the deployed Thunder instances' memory usage (percentage) on the Azure Application Insights.	

••••

.....



Table 36	: Azure	Configuration	Parameters
----------	---------	---------------	------------

Parameter	Description	Default Value
	By default, it is enabled.	
azure_disk	Specify 1 to publish the deployed Thunder instances' storage disk on the Azure Application Insights.	1
	By default, it is enabled.	
azure_ throughput	Specify 1 to publish the deployed Thunder instances' active throughput on the Azure Application Insights.	1
	By default, it is enabled.	
azure_ interfaces	Specify 1 to publish the deployed Thunder instances' interfaces down count on the Azure Application Insights.	1
	By default, it is enabled.	
azure_cps	Specify 1 to publish the deployed Thunder instances' new connection per second on the Azure Application Insights. By default, it is enabled.	1
azure_tps	Specify 1 to publish the deployed Thunder instances' transaction rate per second on the Azure Application Insights. By default, it is enabled	1
azure server	Specify 1 to publish the deployed Thunder	1
down_count	instances' web/app servers down count on the Azure Application Insights.	
	By default, it is enabled.	
azure_server_ down_	Specify 1 to publish the deployed Thunder instances' configured web/app servers down	1

••••

.....



Table 36 : Azure Configuration Parameter
--

Parameter	Description	Default Value
percentage	percentage on the Azure Application Insights.	
	By default, it is enabled.	
azure_ssl_cert	Specify 1 to publish the deployed Thunder instances' SSL error count on the Azure Application Insights.	1
	By default, it is enabled.	
azure_server_ error	Specify 1 to publish the deployed Thunder instances' web/app servers 4xx, 5xx errors count on the Azure Application Insights.	1
	By default, it is enabled.	
azure_sessions	Specify 1 to publish the deployed Thunder instances' active session count on the Azure Application Insights.	1
	By default, it is enabled.	
azure_packet_ rate	Specify 1 to publish the deployed Thunder instances' packet rate on the Azure Application Insights.	1
	By default, it is enabled.	
azure_packet_ drop	Specify 1 to publish the deployed Thunder instances' packet drop count on the Azure Application Insights.	1
	By default, it is enabled.	

VMware

Configure the following parameters in the config.json to publish Thunder metrics to the VMware vROps. By default, all the metrics are enabled. You can enable one or more Thunder Metrics.

.



NOTE: For better throughput, you must enable only those metrics which are required.

Table 37 : VM ware Configuration Parameters

Parameter	Description	Default Value
vmware_provider	Specify 1 to publish selected metric/s, logs, or both to VMware.	0
	By default, it is disabled and does not send metric to VMware. To publish metric/s it is mandatory to enable VMware as a provider.	
vmware_metric	Specify 1 to publish the metrics to VMware vROps. It sends the data only if vmware_provider is also enabled.	0
	By default, it is disabled.	
vmware_vrops_	Specifies the VMware vROps host IP	<vmware_< td=""></vmware_<>
host	address. To get the host, go to ESXI host	vrops_
	Networking > IP Address.	110SC_01_1p>
vmware_cpu	Specify 1 to publish the deployed Thunder instances' average data CPU usage (percentage) on the VMware vROps. If the vmware_provider and vmware_metrics parameters are enabled, TOA sends this metric to the VMware vROps.	1
vmware memory	Specify 1 to publish the deployed	1
	Thunder instances' memory usage (percentage) on the VMware vROps.	
	By default, it is enabled.	
vmware_disk	Specify 1 to publish the deployed	1

••••



Parameter	Description	Default Value
	Thunder instances' storage disk on the VMware vROps.	
	By default, it is enabled.	
vmware_	Specify 1 to publish the deployed	1
throughput	Thunder instances' active throughput on	
	the VMware vROps.	
	By default, it is enabled.	
vmware_	Specify 1 to publish the deployed	1
interfaces	Thunder instances' interfaces down	
	count on the VMware vROps.	
	By default, it is enabled.	
vmware_cps	Specify 1 to publish the deployed	1
	Thunder instances' new connections per	
	second on the VMware vROps.	
	By default, it is enabled.	
vmware_tps	Specify 1 to publish the deployed	1
	Thunder instances' transaction rate per	
	second on the VMware vROps.	
	By default, it is enabled.	
vmware_server_	Specify 1 to publish the deployed	1
down_count	Thunder instances' web/app servers	
	down count on the VMware vROps.	
	By default, it is enabled.	
vmware_server_	Specify 1 to publish the deployed	1
down_percentage	Thunder instances' configured web/app	
	servers down percentage on the VMware	
	By default, it is enabled.	

Table 37 : VM ware Configuration Parameters



	Table 37 :	VMware	Configuration	Parameters
--	------------	--------	---------------	------------

Parameter	Description	Default Value
vmware_ssl_cert	Specify 1 to publish the deployed	1
	Thunder instances' SSL error count on	
	the VMware vROps.	
	By default, it is enabled.	
vmware_server_	Specify 1 to publish the deployed	1
error	Thunder instances' web/app servers 4xx,	
	5xx errors count on the VMware vROps.	
	By default, it is enabled.	
vmware_sessions	Specify 1 to publish the deployed	1
	Thunder instances' active session count	
	on the VMware vROps.	
	By default, it is enabled.	
vmware_packet_	Specify 1 to publish the deployed	1
rate	Thunder instances' packet rate on the	
	VMware vROps.	
	By default, it is enabled.	
vmware_packet_	Specify 1 to publish the deployed	1
drop	Thunder instances' packet drop count on	
	the VMware vROps.	
	By default, it is enabled.	

Elasticsearch

Configure the following parameters in the config.json to publish Thunder metrics to Elasticsearch. By default, all the metrics are enabled. You can enable one or more <u>Thunder Metrics</u>.

NOTE: For better throughput, you must enable only those metrics which are required.

.



Table 38 : Elasticsearch Configuration Parameters

Parameter	Description	Default Value
es_provider	Specify 1 to publish selected metric/s, logs, or both to Elasticsearch.	0
	By default, it is disabled and does not send metric to Elasticsearch. To publish metric/s it is mandatory to enable Elasticsearch as a provider.	
es_metric	Specify 1 to publish the metrics to Elasticsearch. It sends the data only if es_provider is also enabled.	0
	By default, it is disabled.	
es_host	Specify the Elasticsearch host IP address.	<host ip:port=""></host>
es_cpu	Specify 1 to publish the deployed Thunder instances' average data CPU usage (percentage) on Elasticsearch. If the es_provider and es_metrics parameters are enabled, TOA sends this metric to Elasticsearch. By default, it is enabled.	1
es_memory	Specify 1 to publish the deployed Thunder instances' memory usage (percentage) on Elasticsearch. By default, it is enabled.	1
es_disk	Specify 1 to publish the deployed Thunder instances' storage disk on Elasticsearch. By default, it is enabled.	1
es_throughput	Specify 1 to publish the deployed Thunder instances' active throughput	1

••••



Parameter	Description	Default Value
	on Elasticsearch.	
	By default, it is enabled.	
es_interfaces	Specify 1 to publish the deployed Thunder instances' interfaces down count on Elasticsearch.	1
	By default, it is enabled.	
es_cps	Specify 1 to publish the deployed Thunder instances' new connections per second on Elasticsearch.	1
es_tps	Specify 1 to publish the deployed Thunder instances' transaction rate per second on Elasticsearch. By default, it is enabled.	1
es_server_down_ count	Specify 1 to publish the deployed Thunder instances' web/app servers down count on Elasticsearch. By default, it is enabled.	1
es_server_down_ percentage	Specify 1 to publish the deployed Thunder instances' configured web/app servers down percentage on Elasticsearch. By default, it is enabled.	1
es_ssl_cert	Specify 1 to publish the deployed Thunder instances' SSL error count on Elasticsearch. By default, it is enabled.	1
es_server_error	Specify 1 to publish the deployed	1

••••

•

.....



Parameter	Description	Default Value
	Thunder instances' web/app servers 4xx, 5xx errors count on Elasticsearch.	
	By default, it is enabled.	
es_sessions	Specify 1 to publish the deployed Thunder instances' active session count on Elasticsearch.	1
	By default, it is enabled.	
es_packet_rate	Specify 1 to publish the deployed Thunder instances' packet rate on Elasticsearch.	1
	By default, it is enabled.	
es_packet_drop	Specify 1 to publish the deployed Thunder instances' packet drop count on Elasticsearch.	1
	By default, it is enabled.	

Table 38 : Elasticsearch Configuration Parameters

PushGateway

Configure the following parameters in the config.json to publish Thunder metrics to the Pushgateway. By default, all the metrics are enabled. You can enable one or more <u>Thunder Metrics</u>.

NOTE:	For better throughput, you must enable only those metrics which
	are required.

Table 39 : Pushgateway Configuration Parameters

Parameter	Description	Default Value
pushgateway_ provider	Specify 1 to publish selected metric/s, logs, or both to Pushgateway.	0
	By default, it is disabled and does not send metric to Pushgateway. To	

••••



Parameter	Description	Default Value
	publish metric/s it is mandatory to enable Pushgateway as a provider.	
pushgateway_ metric	Specify 1 to publish the metrics to Pushgateway. It sends the data only if pushgateway_provider is also enabled.	0
	By default, it is disabled.	
pushgateway_host	Specify the Pushgateway host IP address.	<host ip:port=""></host>
pushgateway_cpu	Specify 1 to publish the deployed Thunder instances' average data CPU usage (percentage) on Pushgateway. If the pushgateway_provider and pushgateway_metrics parameters are enabled, TOA sends this metric to the Pushgateway.	1
	By default, it is enabled.	
pushgateway_ memory	Specify 1 to publish the deployed Thunder instances' memory usage (percentage) on Pushgateway. By default, it is enabled.	1
pushgateway_disk	Specify 1 to publish the deployed Thunder instances' storage disk on the Pushgateway. By default, it is enabled.	1
pushgateway_ throughput	Specify 1 to publish the deployed Thunder instances' active throughput on Pushgateway.	1

Table 39 : Pushgateway Configuration Parameters



Table 39 :	Pushgateway	/ Configuration	Parameters

Parameter	Description	Default Value
pushgateway_	Specify 1 to publish the deployed	1
interfaces	count on Pushgateway.	
	By default, it is enabled.	
pushgateway_cps	Specify 1 to publish the deployed	1
	Thunder instances' new connections	
	Du default, it is enabled	
pushgateway_tps	Specify 1 to publish the deployed	
	per second on Pushgateway.	
	By default, it is enabled.	
pushgateway_	Specify 1 to publish the deployed	1
server_down_	Thunder instances' web/app servers	
count	down count on Pushgateway.	
	By default, it is enabled.	
pushgateway_	Specify 1 to publish the deployed	1
server_down_	Thunder instances' configured	
percentage	web/app servers down percentage on	
	Pushgateway.	
	By default, it is enabled.	
pushgateway_ssl_	Specify 1 to publish the deployed	1
cert	Thunder instances' SSL error count on	
	Pushgateway.	
	By default, it is enabled.	
pushgateway_	Specify 1 to publish the deployed	1
server_error	Thunder instances' web/app servers	
	4xx, 5xx errors count on Pushgateway.	

••••



Table 39 : Pushgateway	Configuration	Parameters
Tuble 33 . Tubligatema	y conngaration	i urumeters

Parameter	Description	Default Value
	By default, it is enabled.	
pushgateway_ sessions	Specify 1 to publish the deployed Thunder instances' active session count on Pushgateway.	1
	By default, it is enabled.	
pushgateway_ packet_rate	Specify 1 to publish the deployed Thunder instances' packet rate on Pushgateway.	1
pushgateway_ packet_drop	By default, it is enabled. Specify 1 to publish the deployed Thunder instances' packet drop count on Pushgateway.	1
	By default, it is enabled.	

Splunk

Configure the following parameters in the config.json to publish Thunder metrics to the Splunk. By default, all the metrics are enabled. You can enable one or more Thunder Metrics.

NOTE: For better throughput, you must enable only those metrics which are required.

Table 40 : Splunk Configuration Parameters

Parameter	Description	Default Value
splunk_provider	Specify 1 to publish selected metric/s, logs, or both to Splunk.	0
	By default, it is disabled and does not send metric to Splunk. To publish metric/s it is mandatory to enable Splunk as a provider.	



Table 40 : Splunk Configuration Parameters

Parameter	Description	Default Value
splunk_metric	Specify 1 to publish the metrics to Splunk. It sends the data only if splunk_provider is also enabled.	0
	By default, it is disabled.	
splunk_host	Specify the Splunk host IP address.	<host ip:port=""></host>
splunk_cpu	Specify 1 to publish the deployed Thunder instances' average data CPU usage (percentage) on Splunk. If the splunk_provider and splunk_metrics parameters are enabled, TOA sends this metric to the Splunk. By default, it is enabled.	1
splunk_memory	Specify 1 to publish the deployed Thunder instances' memory usage (percentage) on Splunk. By default, it is enabled.	1
splunk_disk	Specify 1 to publish the deployed Thunder instances' storage disk on Splunk. By default, it is enabled.	1
splunk_ throughput	Specify 1 to publish the deployed Thunder instances' active throughput on Splunk. By default, it is enabled.	1
splunk_ interfaces	Specify 1 to publish the deployed Thunder instances' interfaces down count on Splunk. By default, it is enabled.	1



Table 40 :	Splunk	Configuration	Parameters
------------	--------	---------------	------------

Parameter	Description	Default Value
splunk_cps	Specify 1 to publish the deployed Thunder instances' new connections per second on Splunk.	1
	By default, it is enabled.	
splunk_tps	Specify 1 to publish the deployed Thunder instances' transaction rate per second on Splunk. By default, it is enabled.	1
splunk_server_ down_count	Specify 1 to publish the deployed Thunder instances' web/app servers down count on Splunk.	1
	By default, it is enabled.	
splunk_server_ down_percentage	Specify 1 to publish the deployed Thunder instances' configured web/app servers down percentage on Splunk.	1
	By default, it is enabled.	
splunk_ssl_cert	Specify 1 to publish the deployed Thunder instances' SSL error count on Splunk.	1
	By default, it is enabled.	
splunk_server_ error	Specify 1 to publish the deployed Thunder instances' web/app servers 4xx, 5xx errors count on Splunk. By default, it is enabled.	1
splunk_sessions	Specify 1 to publish the deployed Thunder instances' active session count on Splunk.	1



Parameter	Description	Default Value
	By default, it is enabled.	
splunk_packet_ rate	Specify 1 to publish the deployed Thunder instances' packet rate on Splunk.	1
	By default, it is enabled.	
splunk_packet_ drop	Specify 1 to publish the deployed Thunder instances' packet drop count on Splunk.	1
	By default, it is enabled.	

Google Cloud Platform (GCP)

Configure the following parameters in the config.json to publish Thunder metrics to the GCP. By default, all the metrics are enabled. You can enable one or more <u>Thunder Metrics</u>.

NOTE:	For better throughput, you must enable only those metrics which
	are required.

Additionally, you must enable the **Strackdriver Monitoring API** in the Google Cloud console. To do so, navigate to **APIs & Services > Library > Strackdriver Monitoring API**, and click **Enable**.

Table 41 : GCP Configuration Parameters

Parameter	Description	Default Value
gcp_provider	Specify 1 to publish selected metric/s, logs, or both to GCP.	0
	By default, it is disabled and does not send metric to GCP. To publish metric/s it is mandatory to enable GCP as a provider.	
gcp_metric	Specify 1 to publish the metrics to GCP. It	0



.....

Table 41 : 6	SCP Configuration	Parameters
--------------	-------------------	------------

Parameter	Description	Default Value
	sends the data only if gcp_provider is also enabled.	
	By default, it is disabled.	
gcp_cpu	Specify 1 to publish the deployed Thunder instances' average data CPU usage (percentage) on GCP. If the gcp_ provider and gcp_metrics parameters are enabled, TOA sends this metric to the GCP.	1
	By default, it is enabled.	1
gcp_memory	Thunder instances' memory usage (percentage) on GCP.	l
acp disk	Specify 1 to publish the deployed	1
	Thunder instances' storage disk on GCP.	
	By default, it is enabled.	
gcp_throughput	Specify 1 to publish the deployed Thunder instances' active throughput on GCP. By default, it is enabled.	1
gcp_interfaces	Specify 1 to publish the deployed Thunder instances' interfaces down count on GCP.	1
		1
gcb_cb2	Specify 1 to publish the deployed Thunder instances' new connections per second on GCP.	Ţ

gcp_sessions

gcp_packet_rate

Feedback

Parameter	Description	
	By default, it is enabled.	
gcp_tps	Specify 1 to publish the deployed Thunder instances' transaction rate per second on GCP.	1
	By default, it is enabled.	
gcp_server_down_ count	Specify 1 to publish the deployed Thunder instances' web/app servers down count on GCP.	1
	By default, it is enabled.	
gcp_server_down_ percentage	Specify 1 to publish the deployed Thunder instances' configured web/app servers down percentage on GCP. By default, it is enabled.	1
gcp_ssl_cert	Specify 1 to publish the deployed Thunder instances' SSL error count on GCP. By default, it is enabled	1
gcp_server_error	Specify 1 to publish the deployed Thunder instances' web/app servers 4xx, 5xx errors count on GCP.	1

Table 41 : GCP Configuration Parameters



1

1

By default, it is enabled.

By default, it is enabled.

on GCP.

Specify 1 to publish the deployed

Specify 1 to publish the deployed

Thunder instances' active session count

Thunder instances' packet rate on GCP.



Table 41 : GCP Configuration Parameters

Parameter	Description	Default Value
	By default, it is enabled.	
gcp_packet_drop	Specify 1 to publish the deployed Thunder instances' packet drop count on GCP. By default, it is enabled.	1

Oracle Cloud Infrastructure (OCI)

Configure the following parameters in the config.json to publish Thunder metrics to the OCI. By default, all the metrics are enabled. You can enable one or more <u>Thunder Metrics</u>.

NOTE: For better throughput, you must enable only those metrics which are required.

Before publishing metrics in OCI, you must create and manage certain policies that define the necessary permissions. To do the same, see <u>Create Policies to Publish</u> Data in OCI.

Parameter	Description	Default Value
oci_provider	Specify 1 to publish selected metric/s, logs, or both to OCI. By default, it is disabled and does not send metric to OCI. To publish metric/s it is mandatory to enable OCI as a provider.	0
oci_metric	Specify 1 to publish the metrics to OCI. It sends	0

Table 42 : OCI Configuration Parameters



Table 42 : OCI	Configuration	Parameters
----------------	---------------	------------

Parameter	Description	Default Value
	the data only if oci_ provider is also enabled.	
	By default, it is disabled.	
oci_cpu	Specify 1 to publish the deployed Thunder instances' average data CPU usage (percentage) on OCI. If the oci_provider and oci_metrics parameters are enabled, TOA sends this metric to the OCI. By default, it is	1
	enabled.	
oci_memory	Specify 1 to publish the deployed Thunder instances' memory usage (percentage) on OCI. By default, it is	1
	enabled.	
oci_disk	Specify 1 to publish the deployed Thunder instances' storage disk on OCI.	1
	By default, it is enabled.	

.....



.

.....

. .

Table 42 : OCI Co	onfiguration Parameters
-------------------	-------------------------

Parameter	Description	Default Value
oci_ throughput	Specify 1 to publish the deployed Thunder instances' active throughput on OCI.	1
	By default, it is enabled.	
oci_ interfaces	Specify 1 to publish the deployed Thunder instances' interfaces down count on OCI. By default, it is enabled.	1
oci_cps	Specify 1 to publish the deployed Thunder instances' new connections per second on OCI. By default, it is enabled.	1
oci_tps	Specify 1 to publish the deployed Thunder instances' transaction rate per second on OCI. By default, it is enabled.	1
oci_server_ down_count	Specify 1 to publish the deployed Thunder instances' web/app servers down count on OCI.	1



.

.....

•

Parameter	Description	Default Value
	By default, it is enabled.	
oci_server_ down_ percentage	Specify 1 to publish the deployed Thunder instances' configured web/app servers down percentage on OCI.	1
	By default, it is enabled.	
oci_ssl_cert	Specify 1 to publish the deployed Thunder instances' SSL error count on OCI.	1
	By default, it is enabled.	
oci_server_ error	Specify 1 to publish the deployed Thunder instances' web/app servers 4xx, 5xx errors count on OCI.	1
	By default, it is enabled.	
oci_sessions	Specify 1 to publish the deployed Thunder instances' active session count on OCI.	1
	By default, it is enabled.	
oci_packet_ rate	Specify 1 to publish the deployed Thunder	1



Table 42 : OCI Configuration Parameters

Parameter	Description	Default Value
	instances' packet rate on OCI.	
	By default, it is enabled.	
oci_packet_ drop	Specify 1 to publish the deployed Thunder instances' packet drop count on OCI.	1
	By default, it is enabled.	
oci_com- partment_id	Specify the compartment id, also known as Oracle Cloud Identifier (OCID), of your compartment in Oracle Cloud Infrastructure (OCI).	ocid1.compartment.oc1xxxxxxx
	To obtain the OCID, perform the following steps:	
	 Open the OCI console and access the navigation menu. 	
	 Click Identity & Security, and under the Identity section, select Compartments. 	
	A list of	



Table 42 : OCI Co	nfiguration Parameters
-------------------	------------------------

Parameter	Description	Default Value
	compartments that exist within your OCI tenancy will be displayed.	
	 Click the compartment of your choice. 	
	The Instance Information tab will be displayed.	
	 Under General Information, next to OCID, click Show. 	
	The full OCID value will be displayed.	
	 Click Copy to copy the OCID to your clipboard and then paste it into the service request form field. 	

Logs

Depending upon your cloud platform, configure the following parameters to publish the Thunder logs:

AWS

Configure the following parameters in the config.json to publish <u>Thunder Logs</u> to the AWS CloudWatch.



Table 43 : /	AWS Confi	iguration P	Parameters
--------------	-----------	-------------	------------

Parameter	Description	Default Value
aws_provider	Specify 1 to publish selected metric/s, logs, or both to AWS.	0
	By default, it is disabled and does not send logs to AWS. To publish logs it is mandatory to enable AWS as a provider.	
aws_log	Specify 1 to publish the logs to AWS CloudWatch. It sends the data only if aws_ provider is also enabled.	0
	By default, it is disabled.	
aws_log_group_	Specifies the log group name under which	<aws_log_< td=""></aws_log_<>
name	all logs are sent to AWS CloudWatch.	group_name>
	To get this folder, it can be found under AWS Management Console > CloudWatch > Logs > <log_group_name>.</log_group_name>	

For sample configuration, see Examples.

Azure

Configure the following parameters in the config.json to publish <u>Thunder Logs</u> to the Azure Log Analytics Workspace.

Table 44 : Azure Configuration Parameters

Parameter	Description	Default Value
azure_provider	Specify 1 to publish the selected metric/s, logs, or both to Azure.	0
	By default, it is disabled and does not send logs to Azure. To publish logs, it is mandatory to enable Azure as a provider.	
azure_log	Specify 1 to publish the logs to Azure	0



Table 44 : Azure Configuration Parameters

Parameter	Description	Default Value
	Log Analytics Workspace. It sends the data only if azure_provider is also enabled.	
	By default, it is disabled.	
azure_log_ workspace_id	Specifies the Azure Log Analytics Workspace ID.	<azure_log_ workspace_id></azure_log_
	To get this value, go to Azure Portal > Azure services > Log Analytics workspaces > <your_log_analytics_ workspace> > Settings > Agents.</your_log_analytics_ 	

For sample configuration, see <u>Examples</u>.

VMware

Configure the following parameters in the config.json to publish <u>Thunder Logs</u> to the VMware vRLI.

Parameter	Description	Default Value
vmware_provider	Specify 1 to publish the selected metric/s, logs, or both to VMware.	0
	By default, it is disabled and does not send logs to VMware. To publish logs, it is mandatory to enable VMware as a provider.	
vmware_log	Specify 1 to publish the logs to VMware vRLI. It sends the data only if vmware_ provider is also enabled. By default, it is disabled	0
vmware vrli host	Specifies the VMware vBLL host IP	<umuare< td=""></umuare<>
	address. To get the host, go to ESXi host	vrli_host_





Table 45 : VM ware Configuration Parameters

Parameter	Description	Default Value
	<pre>> Virtual Machines > <your_vrli_vm> ></your_vrli_vm></pre>	or_ip>
	Networking > IP Address.	

For sample configuration, see Examples.

Elasticsearch

Configure the following parameters in the config.json to publish <u>Thunder Logs</u> to Elasticsearch.

Table 46 : Elasticsearch Configuration Parameters

Parameter	Description	Default Value
es_provider	Specify 1 to publish the selected metric/s, logs, or both to Elasticsearch. By default, it is disabled and does not send logs to Elasticsearch. To publish logs, it is mandatory to enable Elasticsearch as a provider.	0
es_log	Specify 1 to publish the logs to Elasticsearch. It sends the data only if es_provider is also enabled. By default, it is disabled.	0
es_host	Specify the Elasticsearch host IP address.	<host ip:port=""></host>

For sample configuration, see Examples.

Prometheus

Configure the following parameters in the config.json to publish <u>Thunder Logs</u> to Pushgateway.

Parameter	Description	Default Value
pushgateway_	Specify 1 to publish the selected	0



Parameter	Description	Default Value
provider	metric/s, logs, or both to Pushgateway.	
	By default, it is disabled and does not send logs to Pushgateway. To publish logs, it is mandatory to enable Pushgateway as a provider.	
pushgateway_log	Specify 1 to publish the logs to Pushgateway. It sends the data only if pushgateway_provider is also enabled.	0
	By default, it is disabled.	
pushgateway_host	Specify the Pushgateway host IP address.	<host ip:port=""></host>

For sample configuration, see Examples.

Splunk

Configure the following parameters in the config.json to publish <u>Thunder Logs</u> to Splunk.

Parameter	Description	Default Value
splunk_provider	Specify 1 to publish the selected metric/s, logs, or both to Splunk.	0
	By default, it is disabled and does not send logs to Splunk. To publish logs, it is mandatory to enable Splunk as a provider.	
splunk_log	Specify 1 to publish the logs to Splunk. It sends the data only if splunk_ provider is also enabled.	0

Table 48 : Splunk Configuration Parameters

.



Table 48 : Splunk Configuration Parameters

Parameter	Description	Default Value
	By default, it is disabled.	
splunk_host	Specify the Splunk host IP address.	<host ip:port=""></host>

For sample configuration, see Examples.

Google Cloud Platform (GCP)

Configure the following parameters in the config.json to publish <u>Thunder Logs</u> to GCP.

Table 49 : GCP Configuration Parameters

Parameter	Description	Default Value
gcp_provider	Specify 1 to publish the selected metric/s, logs, or both to GCP.	0
	By default, it is disabled and does not send logs to GCP. To publish logs, it is mandatory to enable GCP as a provider.	
gcp_log	Specify 1 to publish the logs to GCP. It sends the data only if gcp_provider is also enabled.	0
	By default, it is disabled.	

Additionally, you must enable the **Cloud Logging API** in the Google Cloud console. To do so, navigate to **APIs & Services > Library > Cloud Logging API**, and click **Enable**.

For sample configuration, see Examples.

Oracle Cloud Infrastructure (OCI)

Configure the following parameters in the $\tt config.json$ to publish $\underline{\sf Thunder Logs}$ to OCI.

Before publishing logs in OCI, you must create and manage certain policies that define the necessary permissions. To do the same, see <u>Create Policies to Publish</u> <u>Data in OCI</u>.

Parameter	Description	Default Value
oci_provider	Specify 1 to publish the selected metric/s, logs, or both to OCI.	0
	By default, it is disabled and does not send logs to OCI. To publish logs, it is mandatory to enable OCI as a provider.	
oci_log	Specify 1 to publish the logs to OCI. It sends the data only if oci_provider is also enabled.	0
	By default, it is disabled.	
oci_log_id	Specify the Oracle Cloud Identifier (OCID) of your log in OCI. To obtain the OCID, perform the following steps:	ocid1.log.oc1.xxxx.xxxxxx
	 Open the OCI console, access the navigation menu, and click Observability & Management. 	
	 Under Logging, click Log Groups. 	
	 Under List Scope, select the compartment where you have the permissions. 	

. . : : : : : : : : :
External Thunder Observability Agent (TOA)



Table 50 : OCI Configuration Parameters

Parameter	Description	Default Value
	4. On the Log Groups page, click Create Log Group.	
	 Enter a log group name, description (optional), and click Create. 	
	A new log group will be created.	
	 Click on the newly created log group, navigate to the Logs tab within the group and click Create custom log. 	
	 Enter a log name, select the log group created in the previous step and click Create custom log. 	
	 Click Cancel on the Create agent configuration page (if prompted). 	
	A new log will be created.	
	 Click the newly created log. The OCID of the log will be displayed under the Log Information tab. 	
	 Click Copy to copy the OCID to your clipboard and then paste it into the service request form field. 	

.....



For sample configuration, see Examples.

Monitor Dashboard

This section describes how to track and monitor the health, throughput, and performance of your Thunder instances.

The following topics are covered:

Monitor Metrics	110
Monitor Logs	152

Monitor Metrics

Depending on your cloud provider, the steps are provided to monitor the configured metrics.

AWS CloudWatch

To monitor the Thunder metrics on AWS CloudWatch, perform the following steps:



1. From the AWS Management Console, go to CloudWatch > Metrics > All metrics.

aws Services	Q Search	[Alt+S]										
CloudWatch	×	CloudWatch > Metrics Untitled graph I2										
Dashboards	1 ⊘ 0 💬 8	1Your CloudWatch										
► Logs		o.s Select some metri										
Metrics All metrics Explorer		0 14:30 14:45 15:00 15:15 15:30 15:45										
Streams		Browse Query Graphed metrics Options Source										
X-Ray tracesEvents		Metrics (3,538) Info N. Virginia Q. Search for any metric, dimension, resource id or account id										
 Application monito Insights 	oring	▼ Custom namespaces										
Settings New		Avolucensemanager/incenseOsage 56 Inunder 558										
		AWS namespaces										

Figure 7 : AWS All metrics

2. Select **Browse** > <your_Thunder_metric_namespace>.

Figure 8 : Thunder Metrics

				=										
Browse Query Graphed metrics	Options Sou	urce					Add math 🔻	Add query 🔻						
Metrics (338) Info														
N. Virginia 🔻 All > Thunder Q. Search for any metric, dimension, resource id or account id														
CPU Usage Percentage (Data)	31	Disk Usage Percentage	32	Interface Down Count (Data)	18	Memory Usage	Percentage	32						
Packet Drop Rate (Sec)	8	Packet Rate (Sec)	7	SSL Errors Count	32	Server Down Co	ount	9						
Server Down Percentage	9	Server Errors Count	32	Throughput Rate (Global/BPS)	32	Total New Conr	ection (Sec)	32						
Total Session Count	32	Transactions Rate (Sec)	32											

- 3. Click the required metric to be monitored from the **Metrics** panel. For the list of available Thunder metrics, see <u>Supported Thunder Metrics</u>.
- 4. Select the management IP of one or multiple Thunder instance/s to be monitored.

111

Feedback

As the Thunder instances are selected, the metric data gets populated in the **Untitled Graph** panel for the selected the time range. For more information, see <u>Graph a metric</u>.





Azure Application Insight

To monitor the Thunder metrics on Azure Application Insight, perform the following steps:

1. From the **Azure Portal**, go to **Azure services** > **Resource Groups** > <your_ resource_group> and click your app insight name.

The selected app insight - Overview window is displayed.



Figure 10 : Selected app insight - Overview window

	, P Search resources, services, a	nd docs (G+/)	
Home > Microsoft.AppInsights Overview	\rightarrow		
application-insight			
₽ Search «	★ Application Dashboard 🛛 📣 Getting sta	irted 🔎 Search	🧬 Logs 🕈 Monitor resource group 🛛 🔊 Feed
💡 Overview 🔺	∧ Essentials		
Activity log	Resource group (move) : <u>vth-gslb</u>		
Access control (IAM)	Location : East US 2		
🗳 Tags	Subscription (move) : Eng Azure		
🤌 Diagnose and solve problems	Subscription ID : 07d34b9b-61e3-47	5a-abbc-006b16812	Za3e
Investigate	Tags (<u>edit</u>) : <u>Click here to add ta</u>	<u>195</u>	
Application map	Show data for last:		
Smart detection	30 minutes 1 hour 6 hours 12 h	iours 1 day	3 days 7 days 30 days
- Live metrics	Failed requests	\$	Server response time
P Transaction search	100		100ms
🌷 Availability	80		80ms
III Failures	60		_60ms
Performance	40		40ms
Troubleshooting guides (preview)	0 10:30 AM 10:45 AM 11 AM 11:15	AM UTC+05:30	0ms 10:30 AM 10:45 AM 11 AM 11:15 AM UTC+
Monitoring	Failed requests (Count) thunder O		Server response time (Avg) thunder =-
III Alerts			
 Metrics Diagnostic settings 	Availability	\$	

OR

From the **Azure Portal**, go to **Azure services** > **Resource Groups** > <*your_ resource_group* > and click your Thunder instance name whose metric is to be monitored.

Figure 11 : Thunder instance window

Home > vth-rg10 > vth-inst1 vth-inst1 Metrics Virtual machine	* …	Select a scope	
Search Operations	+ New chart 🕐 Refresh 😰 Share 🗸 😳 Feedback 🗸	Resource types	Locations
Sastion Auto-shutdown	ter Add metric * ▼ Add filter St Apply splitting	Search to filter items	
🥔 Backup	Scope Metric Namespace Metric	Scope	Resource type Location
Disaster recovery	vth-inst1 Virtual Machine Host V Select metric	└ ∨ 🕈 Eng Azure	Subscription -
🏶 Updates	100		Resource group -
😹 Inventory		application-insight	Application Insights South Central US
Change tracking		> () emumba-log-ingestion	Resource group -
📮 Automanage	_ 80	> () usama-log-ingestion-rg	Resource group -

2. Click Metrics from the left Monitoring panel.



A scope picker is displayed in the Metric dashboard.

Figure 12 : Scope Picker

application-insight N Application Insights	∕letrics ☆ …			
₽ Search «	– New chart 💍 Refresh 🛛 🛱 Di	agnose 🗸 🖻 Share 🗸 🙂 Feed	eedback 🗸	
🕈 Overview	Chart Title 🧷			
Activity log	😓 Add metric 🔭 Add filter	🛠 Apply splitting		
Access control (IAM)				
🧳 Tags	Scope	Metric Namespace	Metric Aggregation	
Diagnose and solve problems	100		CPU Usage Percentage (Data)	
Investigate			Disk Usage Percentage Vianterface Down Count (Data)	
- Application map			Memory Usage Percentage A Decision Decision	
🗟 Smart detection	30		So Packet Drop Rate (Sec)	
✤ Live metrics			Server Down Count	
P Transaction search	80		Server Down Percentage	
🎈 Availability				
Hat Failures				
Performance	70			

3. Select the appropriate resources whose metrics you want to view:

Table 51 : Thunder Metrics

Field Name	Description
Scope	If you are adding the metric from Application Insight window, the selected app insight name is auto-populated. If you are adding the metric from Thunder instance window, select your app insight name.
Metric Namespace	Select Thunder .
Metric	Select a metric from the drop-down. For the list of available Thunder metrics, see <u>Supported</u> <u>Thunder Metrics</u> .

As the metric is selected, the corresponding data is plotted in the chart area for the selected the time range.



Figure 13 : Plotted metric data

Nev	w chart Refresh 🖻 Sha	are 🗸 🙂 Feedback 🗸			Local Time: Last 24 ho
Avg	g CPU Usage Percentage ((Data) for application-insig	ht 🖉		
52	Add metric 🦙 Add filter	🔀 Apply splitting			🖄 Line chart 🗸 📙 Drill into Logs 🗸 🔱 New alert rule 🔚 Sav
•	Scope application-insight	Metric Namespace thunder	Metric CPU Usage Percentage	Aggregation V Avg V	
	0.70				
	0.60				
	0.40				
	0.30				
	0.20				

4. To view multiple metrics on the same chart, click **Add metric** and repeat the above step. For more information, see <u>Metrics Explorer</u>.

VMware vROps

To monitor the Thunder metrics on vROps, perform the following steps:

- 1. Start vROps VM
- 2. Create a Dashboard
- 3. Create an Alert
- 4. Create a Notification
- 5. View Thunder Metrics

Start vROps VM

To start the vROps virtual machine, perform the following steps:

1. From the VMware ESXi console, go to Navigator > Virtual Machines > <your_ vROps_VM> and click Power on.



Figure 14 : Start vROps VM

📲 Navigator 🗉	🕞 vRopsMgr863
✓ ☐ Host Manage	😴 Console 🔤 Monitor i Power off 🔢 Suspend 💿 Restart i 🦯 Edit i 🧭 Refresh i 🔅 Actions
Monitor	VRopsMgr863 Guer 0S Other 3 x or later Linux (64-bit) 0 MHz
Virtual Machines Virtual Machines VRopsMgr863	Chryster Tools Yes MEMORY CPUs 4 0 B
Monitor Monitor Monitor	Memory 16 GB STORAGE 274 GB
 VMware-vRealize-Log-I More VMs 	* General Information
▼ Storage 2 ▼ □ Data2	

NOTE:

The system may take a few minutes to start the vROps virtual machine.

2. Click **Console** to launch vROps virtual machine.

The vROps virtual machine is powered on and is reachable.

Figure 15 : vRealize Operations Appliance



3. Log in to the vRealize Operations Web UI with your admin credentials.

The vRealize Operations Home page is displayed.

• • •<mark> • • •</mark>



Figure 16 : vRealize Operations - Home page



Create a Dashboard

The dashboard can be created using either of the following options:

• Import a dashboard template

To import a dashboard using JSON file, see Import a Dashboard.

• Create a dashboard manually

To create a dashboard manually, perform the following steps:

1. From the vRealize Operations Web UI, go to Home > Visualize > Dashboards and click Create to add a new dashboard.

The New Dashboard window is displayed.



Figure 17 : New Dashboard window

vn	vm vRealize Operations																																	
		~		Ne	W	Da	asł	hb	oa	rd				СА	NCE	EL		S	AVE				ACI		vs v	,	SH	ow	INT	ER/	АСТ	ION	s	
			Ŀ																															
G ۲	Home																																	
Ď	Data Sources	>																																
																				2	1			1	1		ł	1	•					
līn e	Environment	>															D	rag	g w cr	/idg eat	get ting	s r g y	ror ou	n∙k rd	asł	ow nba	to bar	be d	gir	י ר י				
	Visualize	~																																
	Dashboards																																	
	Views																																	

- 2. Provide a name to the new dashboard and double-click or drag the following widgets:
 - Object List
 - Metric Picker
 - Metric Chart

Figure 18 : Dashboard widgets

»	ļ	Thunder Metrics	CANCEL	E	ACTIONS ~ SHOW	INTERACTIONS				
ŝ	÷	Object List			Metric Picker			Metric Chart		
	Ŀ	Name	Adapter Type	Obje -						
÷,	1	vRealize Operations Manage	vRealize Operations	vR .						
DA >	Ŀ	vrealize-identity-manager	vCenter Adapter	Vir ·						
		vSphere World	vCenter Adapter	vs .						
	Ĵ	VMware Private Cloud	Container	VN .						
2,	÷	Datacantar	Wantar Adaptar	D						
	2	Filter							Views 🔵	Widgets
*//× >	ſ	Otient List	Metric Pricer		Metric Chart		Scoutoard		Frame	
@ ` @ `		Import Apply Gate Apply Gate Apply Gate Chick (State) Coles States Scate Chick (State) Coles States Scate Chick (State) Coles States Scate Scate Coles States Scate Scate Coles States Scate Scate Coles States Scate Scates Coles States Scate Scates Coles States Scates Coles States Scates Scates Coles States Scates Scates				N () N	Vincense 53.19, incense 53.19, incense 53.19, incense 53.19, incense 54.19, incen	eed 89.58 s		
		Object List	Metric Pic	ker	Metric	Chart	Scoreboa	ird	Heatmap	

3. Click **Show Interactions** to create interactions.



Figure 19 : Interactions



- 4. Drag the connectors and create interactions as shown in the Figure 19.
- 5. Click **Save** to save the changes.

A dashboard for Thunder metrics is created.

Create an Alert

The alert definition can be created using either of the following options:

• Import an alert definition template

To import an alert definition using XML file, see Import an Alert Definition.

• Create an alert definition manually

To create an alert definition manually, perform the following steps:

- 1. From the vRealize Operations Web UI, go to Home > Configure > Alerts and click Alert Definitions.
- 2. Click Add in the Alert Definitions window.

The **Create Alert Definition** panel with **Alert** tab is displayed.



Figure 20 : Create Alert Definition window

Create Alert Definition (Virtual Machine)			
⋒ / Alerts / Alert De	efinitions		
1 - Alert		2 - Symptoms / Conditions New	
Name	ThunderAlert		
Description	reate description for alert		
Base Object Type V	irtual Machine	X ¥	
✓Advanced Settings			
Impact	Health	~	
Criticality	Critical	~	
Alert Type & Subtype	Application : Performan	ce 🗸	
Wait Cycle	1 \$		
Cancel Cycle	1		

3. Enter or select the appropriate values in the following fields:

•	Table 52 : Alert tab fields	
	Field Name	Description
	Name	Enter the alert name.
		Example
		In the Figure 20, the alert definition name is
		ThunderAlert.
	Base Object Type	Select vCenter Adapter > Virtual Machine.

External Thunder Observability Agent (TOA)



Table 52 : Alert tab fields

Field Name	Description	
Under the Advanced Settings:		
Impact	Select Health.	
Criticality	Select Critical .	
Alert Type & Subtype	Select Application : Performance.	

4. Click Next.

The Symptoms / Conditions tab is displayed.

Figure 21 : Symptoms / Conditions tab

Create Alert Definition	Create Alert Definition Virtual Machine ?					?
1 - Alert 2 - S	ymptoms / Conditions 🔰 3 - Recommen	dations 4	- Policies		5 - Notifications	
Drag and drop metric to specify it alert here to create a new set	s condition or symptom into your	Defined On:	Self	Symptoms		×
		Select Specific	Object		Filter	
		 Favorites Metrics Properties 	S			

5. Click Select Specific Object to select your Thunder instance.

The **Select Object** window is displayed.

Figure 22 : Select Object window

Select Object				×
Page Size: 50 V			vth-inst1	~
Name	Adapter Type	Object Type	Policy	
vth-inst1	vCenter Adapter	Virtual Machine	vSphere	Solution's D
			CLOSE	SELECT

6. Select your Thunder instance and click Select.



The selected Thunder instance is listed under **Conditions**.

Figure 23 : Selected Thunder instance



7. Select Metrics > Thunder and drag the required metrics to the left-side panel.

.....



Figure 24 : Drag metric

sef-vitual Machine indication indicatio	Alert	2 - Symptoms / Conditions	3 - Recommendations	4 - Policies
conditions X > if "thinder(CU Usage Percentage (Data) > C mark a: ① minow Image and diread symptom / condition in to your set Drag and drop metric to specify its condition or symptom into your alert here to create a new set X X Drag and drop metric to specify its condition or symptom into your alert here to create a new set X X Drag and drop metric to specify its condition or symptom into your alert here to create a new set X X Drag and drop metric to specify its condition or symptom into your alert here to create a new set X X Drag and drop metric to specify its condition or symptom into your alert here to create a new set X X Drag and drop metric to specify its condition or symptom into your alert here to create a new set X X X Drag and drop metric to specify its condition or symptom into your alert here to create a new set X X X X Drag and drop metric to specify its condition or symptom into your alert here to create a new set X <td< td=""><td>Self - Virtual Machine</td><td></td><td></td><td>Defined On: Self V</td></td<>	Self - Virtual Machine			Defined On: Self V
Conditions			×	
A * f TundericPU Usage Percentage (balk) mark as @ mto_v trag an additional symptom / condition in to your set (vti-isst) (onditions			Conditions New Symptoms
ag an additional symptom / condition in to your set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify its condition or symptom into your alert here to create a new set rag and drop metric to specify i	> If Thunder CPU Usage Percentage (Data) > ~ () mark as () info ~		(uth_inet1 v)
ag and drop metric to specify its condition or symptom into your alert here to create a new set ag and drop metric to specify its condition or symptom into your alert here to create a new set ag and drop metric to specify its condition or symptom into your alert here to create a new set b C Cefiguration b C CPU b	ig an additional symptom / condition in to y	pur set		
ag and drop metric to specify its condition or symptom into your alert here to create a new set ag and drop metric to specify its condition or symptom into your alert here to create a new set A Capacity Analytics Generated C CPU Ulitization for Resources C CP				> 🚵 Favorites
ag and drop metric to specify its condition or symptom into your alert here to create a new set				Metrics Analytics Generated
2 d a d oligo intente de gebrain als de la deriverais d'activité de la deriverais d'activité de gebrain als de la deriverais d'activité de la deriverais de la deriverais d'activité de la deriverais	ag and drop metric to specify its con-	Rion or symptom into your alert here to create a new set		> Configuration
 > [2] CPU Utilization for Resources > [3] Datastore > [3] CPU Utilization for Resources > [4] Datastore > [5] Coust > [6] Coust > [6] Coust > [6] Memory Usage on Host > [6] Memory Usage on Host > [7] Memory Usage on Host > [8] Memory Usage on Host > [8] Memory Usage on Host > [9] Memory Usage Processon > [9] Memory Usage Percentage (Data) > [9] Memory Usage Percentage > Interface Down Court (Usa) > Memory Usage Percentage > Packet Drop Rate (Sec) > Sever Down Percentage 	sg and drop metric to specify its cond	adorror symptom into your alert here to create a new set		> CPU
 S Datastore <li< td=""><td></td><td></td><td></td><td>> 🔝 CPU Utilization for Resources</td></li<>				> 🔝 CPU Utilization for Resources
 S. Dirk Space S. Dirk Space Usage on Datastore G. Gust Memory Usage on Host Memory Vage Protectage S. Strape S. Strape S. Strape S. Strape S. Virtual Dirk S. System S. System S. Virtual Dirk S. Wirtual Dirk S. Wirtual Dirk S. Strape Constructions Generated S. Strate Constructions (Section 2) S. Kinder S. Strates Constructions (Section 2) Section 2) Section 2) S. Strates Constructions (Section 2) Section 2) <li< td=""><td></td><td></td><td></td><td>> 🔂 Datastore</td></li<>				> 🔂 Datastore
 S Dick Space Usage on Datastore C Guest Memory Memory Usage on Host Memory Usage on Host Metwork Metwork Metwork Metwork Metwork Metwork Metwork Storage <l< td=""><td></td><td></td><td></td><td>> 🔂 Disk Space</td></l<>				> 🔂 Disk Space
 S Guest S Memory S Memory Usage on Host S Memory Usage on Host S Memory Usage on Host S Petomance S Physical Disk S Physical Disk S Physical Disk S Storage S Storage S Storage S Storage S Storage S System S Virtual Disk S Vesite: Operations Generated If Weite: Operations Generated If Weite: Operations Generated If Weite: Operations Generated S Weite: Operations Generated If Weite: Operations Generated S Memory Usage Percentage Interface Down Count (Disk) Memory Usage Percentage Roket Drop Rate (Sec) Server Down Count Server Down Count Server Down Percentage 				> Disk Space Usage on Datastore
 > Memory Usage on Host > Memory Usage on Host > Memory Usage on Host > Memory Usage Network > Sever Down Count > Sever Down Percentage 				> 🔝 Guest
 > Memory Usage on Host > Metwork > Metwork > Physical Disk > Power > Storage > Metwork > Storage > Metwork > Storage > Metwork > Metwork > Storage > Metwork > Met				> 🔝 Memory
 K Network K Network K Performance R Physical Disk M Power Storage S Storage S Storage S Strimary K System Tunder W Virtual Disk W Virtual Disk W Virtual Disk W Virtual Disk S Virtual Disk S Virtual Disk S Ander Percentage (Data) S Disk Usage Percentage (Data) S Disk Usage Percentage Herdretz Down Court (Data) Memory Usage Percentage Facket Drop Rate (Sec) Facket Drop Rate (Sec) Server Down Court Server Down Court Server Down Court Server Down Percentage 				> 🔝 Memory Usage on Host
 > II Performance > II Performance > II Provide Disk > II Storage > II Vitual Disk >				> 🔝 Network
 > IX Physical Disk > IX Physical Disk > IX Strange > IX Tunder > IX Virtual Disk > IX Virtual Disk > IX Virtual Disk > IX Virtual Disk > IX Tunder > IX Tunder > IX Tunder > IX Strange Percentage (Data) > Status Usage Percentage > Interfere Down Court (Data) > Memory Usage Percentage > Packet Drop Rate (Sec) > Packet Drop Rate (Sec) > Packet Disk Data (Sec) > Sever Down Court > Sever Down Court > Sever Down Percentage 				> 🔝 Performance
 > Ever Power > Storage > Sto				> 🔝 Physical Disk
 > IX Storage > IX Storage > IX Storage > IX Summary > IX System > IX Thunder > IX Visual Disk > IX Visual Disk > IX Visual Disk > IX Visual Disk Usage Percentage > Interfer > Oisk Usage Percentage > Interfer Down Count (Data) > Hermory Usage Percentage > Packet Drop Rate (Sec) > Server Down Count > Server Down Percentage 				> 🔝 Power
 > [K] Summay > [K] System > [K] Thunder > [K] Virtual Dick >				> 🔝 Storage
 > [v] System > [v] Trunder > [v] Virual Dick > [v] Vesilize Oberations Generated ✓ u^A₀ Trunder ● CPU Usage Percentage (Data) ● Dick Usage Percentage ● Interface Down Court (Data) ● Memory Usage Percentage ● Packet Rate (Sec) ● Server Down Court ● Server Down Court ● Server Down Court ● Server Down Percentage 				> 🔝 Summary
> IQ Thunder > IQ Thunder > IQ Virual Disk > IQ Virual Disk IQ Virual Disk IQ Virual Disk IQ Virual Disk IQ Virual Disk IQ Virual Disk <td></td><td></td><td></td><td>> 🔝 System</td>				> 🔝 System
> [k] Virtual Dick > (€) Virtual Dick → (€) Virtual Dick → (±) Thunder → (±) Dick Usage Percentage (Data) ● Dick Usage Percentage ● Interface Down Count (Data) ● Memory Usage Percentage ● Interface Down Count (Data) ● Memory Usage Percentage ● Tacket Dron Data (Sec) ● Tacket Dick Data (Sec) ● Tacket Dick Data (Sec) ● Tacket Dick Data (Sec) ● Server Down Percentage				> 🔝 Thunder
> ∑ Wealize Operations Generated ✓ do Trunder ✓ do Trunder				> 🔝 Virtual Disk
✓				> 🔝 vRealize Operations Generated
CPU Usage Percentage Otal Otal Usage Percentage Instructure Instructure Instructure Instructure Instructure Packet Dron Rate (Sec) Packet Rate (Sec) Packet Rate (Sec) Packet Rate (Sec) Server Down Count Server Down Count				V 🚵 Thunder
Disk Usage Percentage Interface Down Count (Data) Memory Usage Percentage Packet Thoo Rate (Sec) Packet Rate (Sec) Server Down Count Server Down Count				 CPU Usage Percentage (Data)
Interface Down Count (Data) Memory Usage Percentage Packet Drop Rate (Sec) Packet Rate (Sec) Packet Rate (Sec) Server Down Count Server Down Percentage				 Disk Usage Percentage
Memory Usage Percentage Packet Drop Rate (Sec) Packet Rate (Sec) Server Down Percentage Server Down Percentage				 Interface Down Count (Data)
Packet Drop Rate (Sec) Packet Rate (Sec) Server Down Count Server Down Count				 Memory Usage Percentage
Packet Rate (Sec) Server Down Count Server Down Ocurt				 Packet Drop Rate (Sec)
Server Jown Count Server Down Percentage				 Packet Rate (Sec)
Server Down Percentage				Server Down Count
				 Server Down Percentage

8. Specify the appropriate alert condition.

Figure 25 : Alert condition

1 - Alert	2 - Symptoms / Conditions New	3 - Recommendations
1. Self - Virtual Machine		
Conditions		×
> If Thunder CPU Usage Percentage	(Data) > ~ 75 🗘 mark as 🚺 Info ~	
Drag an additional symptom / condition in	to your set	

- 9. Click Next.
- 10. Add the appropriate recommendations in the **Recommendations** tab, if needed.
- 11. Click Next.



- 12. Select appropriate policy in the **Policies** tab, if needed.
- 13. Click Next.

The **Notification** tab is displayed. The notification can be created after the alert definition is created. For more information, see <u>Create a Notification</u>.

Create Alert Definitio	Virtual Machine				?
1 - Alert	2 - Symptoms / Conditions	3 - Recommendations	4 - Policies	5 - Notifications	
	You hat tr	ve no notification rules with m iggers defined by alert definit	otification tion.		
PREVIOUS	CREATE CANCEL				

14. Click **Create** in the **Notification** tab.

An alert definition is created and is listed in the Alert Definition window.

Figure 26 : Verify Alert Definition

Alert Definitions	ons				?
ADD ····		Name :	Thunder ×	ALL FILTERS V	Quick filter
Name 1	Adapt Obj Alert Type	Alert Subtype Critica	lity Impact	Define Last Modified	Modified By
ThunderAlert	vCe Vir Application	Performance 🥼	📄 Health	User 5:31 PM	admin

Create a Notification

The notification can be created using either of the following options:

• Import a notification template

To import a notification using JSON file, see Import a Notification.



• Create a notification manually

To create a notification manually, perform the following steps:

- 1. From the vRealize Operations Web UI, go to Home > Configure > Alerts and click Notifications.
- 2. Click Add in the Notifications window.

The **Notifications** panel with **Notification** tab is displayed.

Figure 27 : Notifications tab

Notifications	itions			?
1 - Notification	2 - Define Criteria	3 - Set Outbound Method	4 - Select Payload Template	
Name	ThunderAlettNotification			
Description	Create description for notification			
Notification Status				
PREVIOUS	CREATE CANCEL			

3. Enter or select the appropriate values in the following fields:

Table 53	•	Notifications	tab
10010 33	•	1 Councations	LUN

Field Name	Description	
Name	Enter the notification name.	
	Example	
	In the Figure 27, notification name is	
	ThunderAlertNotification.	
Notification Status	Select Enable.	

4. Click Next.

The Define Criteria tab is displayed.



Figure 28 : Define Criteria tab

NOULICATIONS					
🞧 / Alerts / No	otifications				
1 - Notification	2 - Define Criteria	3 - Set Outbound	Method 4	- Select Payload	i Template
Object Scope:	Select set of Objects you would like to receive notification	s about.			
Criteria	Object Type × ~	Select an Objec	t Type	× ~	CLEAR
		Tanzu Ku	bernetes cluster		
		vCenter 5	Server		
		Virtual M	achine		
Alert Scope:	Select set of Alerts you would like to receive notifications al	Virtual M	achine Folder		
		vSphere	Distributed Port Group		

5. In the Criteria field, select Object Type from the drop-down.

A field appears to select the object type.

6. Expand vCenterAdapter and select Virtual Machine from the drop-down.

The selected object type is listed under Criteria.

Figure 29 : Criteria defined

3 - Set Outbound Method		- Notification		
	about.	like to receive notifications	Select set of Objects you would like to	bject Scope: S
× ~	Select an Object Type	×	Object Type	Criteria
X	Select an Object Type	× ×	Object Type	Criteria The alert trigge
		ct types:	gers on ANY of the selected object type	The alert trigge

 In the Category field, select Alert Definition from the drop-down created in the <u>Create an Alert</u>.

An Alert Definition pop-up is displayed.



Figure 30 : Alert Definition pop-up

Alert Definitions						** ×
The notification will be sent when ANY of the selected ale	ert de	finitions triggers an alert.			-	
Drag an alert definition to add as criteria.		Name 🕇	Object	ALL FILTERS	Criticality	Modified By
	::	A fatal error occured on a PCI	Host	Hardware (()	admin
Drop aiert deliniuon nere		A fatal memory error was det	Host	Hardware ((!	admin
		A node may be down and it is	vRea	Administrati	<u>/10</u>	admin
	::	A PCIe error occurred during	Host	Hardware (!	admin
			1 - 50 of	530 items 🔇	1 2 3	4 5 11 >
					CANCE	С

8. Search your alert definition.

Figure 31 : Search alert definition

Alert Definitions			e ⁷	\times
The notification will be sent when ANY of the selected ale	ert definitions triggers an alert.			
Drag an alert definition to add as criteria.	Name : Thund	Object Alert Type	Criticality Modified By	_
Drop alert definition here	:: ThunderAlert	Virtu Application	/ admin	
			1 - 1 of 1 item	ns
			CANCEL OK	

9. Select your alert definition and drag it to add as the criteria.

.



Figure 32 : Drag alert definition

Alert Definitions			2 ⁸ ×
The notification will be sent when ANY of the selected	d alert definitions triggers an a	alert. ime : Thunder × ALL FILTERS	▼ Quick filter
Drag an alert definition to add as criteria.	Name 🕇	Object Alert Type	Criticality Modified By
H ThunderAlert X			
Drop alert definition here			
			1 - 1 of 1 items

10. Click **OK**.

The selected alert definition is listed under Category.

Figure 33 : Selected alert definition

Alert Scope: Select set of Alerts you would like to receive notifications about.						
Category	Alert Definition	X v				
The alert is ANY	of the selected (1): 🖉					
ThunderAlert x	Ð					
Criticality	All Criticality	~				
Control State	All States	~				
PREVIOUS	NEXT CREATE CANCEL					

11. In the **Status** field under **Notify On**, select the alert status for which you want to receive the notifications.



External Thunder Observability Agent (TOA)

Figure 34 : Notify On

Notify On:	Select the Alert status change you want to receive notifications on.
Status	All Statuses 🗸

12. Click Next.

The Set Outbound Method tab is displayed.

Figure 35 : Set Outbound Method tab



- 13. In the **Outbound method** field, select **Standard Email Plugin** from the dropdown list.
- 14. Click **Create New Instance** to create a new instance for corresponding Outbound method.

The fields for creating a new instance are displayed.



Figure 36 : Create New Instance fields

Instance Name:	ThunderNotificationInstance	
Use Secure Connection:	0	
Requires Authentication:	0	
SMTP Host:	smtp-mail.outlook.com	
SMTP Port:	587	
Secure Connection Type:	SSL × v	
User Name:	SaaS-Monitor@a10networks.com	
Password:		
Sender Email Address:	SaaS-Monitor@a10networks.com	
Sender Name:	Saas-Monitor	
Receiver Email Address:		
TEST	CANCEL SAVE	

15. Enter or select the appropriate values in the following fields:

Table 54 : Create New Instance

Field Name	Description
Instance Name	Enter the notification instance name.
	Example
	In the Figure 36, the notification instance
	name is ThunderNotificationInstance.
SMTP Host	Enter the URL or IP address of the email host server.
SMTP Port	Enter the SMTP port number used to connect with the email host server.
Secure Connection Type	Select SSL .
User Name	Enter the username that is used to connect to the email server.
Password	Enter the password for the connection username that appears on the notification message.



Table	54:	Create	New	Instance
i ubic		cicate	140.44	motunee

Field Name	Description
Sender Email Address	Enter the email address of the sender.
Sender Name	Enter the display name of the sender email address.
Receiver Email Address	Enter the email address of the receiver that receives the notification.

16. Click **Save** to save the changes.

The new instance is populated in the **Select Instance** field.

Figure 37 : Selected New Instance

1 - Notification	2 - Define Criteria		3 - Set Outbound Method	i	4 - Select Payload Template
Pick the outbound	method you would like to use to send your	r not	ification.		
Outbound method	Standard Email Plugin	v	. ThunderNotificationInstance	v	+ CREATE NEW INSTANCE

17. Click Next.

The Select Payload Template tab is displayed.

Figure 38 : Select Payload Template tab

1 - Notification	2 - Define Criteria	3 - Set Outbound Method	4 - Select Payload Template
> Default Email Ter	nplate		
Recipient(s)			
Cc Recipients	e.g. example@domain.com		
Bcc Recipients	e.g. example@domain.com	(i)	
Notify again	e.g. 15 (Optional)	¢ (1)	
	-	<u>^</u>	
Max Notifications	3	~ (I)	

18. Enter or select the appropriate values in the following fields for the default template:

Table 55 : Select Payload Template tab

Field Name	Description
Recipient(s)	Enter the email addresses of the recipient to

131



Table	55 ·	Select	Pav	/load	Temr	late	tah
Table	55.	Jelect	ra	yiuau	remp	nate	ιab

Field Name	Description
	receive the notification.
Max Notifications	Enter the maximum number of notification to be sent for the active alert.
Delay to notify	Enter the delay time in minutes before sending a notification when a new alert is generated.

19. Click Create.

A new notification is created for the selected alert definition and it is listed in the **Notifications** window.

Figure 39 : Verify Notification

		~	Notifications				
¢	Configure	\sim	$\widehat{\mbox{\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$}\m$				
	Policies		ADD ····				
	Alerts		Rule Name	Description	Instance	Outbound Method	Payload Template
Alerts Super Metrics			ThunderAlertNotification		ThunderNotificationI	Standard Email Plugin	Default Email Template

View Thunder Metrics

To view the Thunder metrics, perform the following steps:

1. From the vRealize Operations Web UI, go to Home > Visualize > Dashboard and select your dashboard created for Thunder metrics.

The selected dashboard is displayed.



Figure 40 : Selected dashboard

Dashboards	Thunder Metrics ACTIONS ~		1H 6H 24H 7D CUS	
☆ Home	Object List		Metric Picker	Metric Chart
Manage	Name	Adapter Type	> 🔝 Favorites	
T Create	Non vSAN Datastores	Container	> A Metrics	
> ☆ Favorites	PoweredOn:vCenter-Server	vCenter Adapte		
✓	vth-inst1	vCenter Adapte		
Thunder Metrics	vRealize LCM Appliance	vCenter Adapte		
Capacity	vSAN World	vSAN Adapter		
Reclaim	vSAN Datastores	Container		
Workload Placement	1 - 50 of 73 item	< <u>1</u> 2 →		
Rightsize				
Compliance				

- 2. From **Object List**, double-click your Thunder instance.
- 3. From Metric Picker, expand Metrics > THUNDER and double-click the following common metrics:
 - Memory Usage Percentage
 - Disk Usage Percentage

As the metric is selected, the corresponding data gets populated in the **Metric Chart** panel for the selected the time range.

Figure 41 : THUNDER Dashboard

vm	vRealize Operations					Q C A A
»	Dashboards	Thunder Metrics ACTIONS -				1H 6H 24H 7D CUSTOM 🏠 😪
÷ ۲	☆ Home ② Manage + Create	Object List Name ↓	Adapter Type	Metric Picker	Metric Charl	t
₪ ›	> ☆ Favorites ~ © Recents	windows WIN2016-DHCP	vCenter Adapter	A capacity Analytics Generated A configuration CPU A CPU CPU	•H: 75.1	70
	Thunder Metrics	vThunderAdaptor_Management Pa vThunderAdaptor (vRealize Operati	vRealize Operations vThunderAdaptor	A Datastore A Disk Space A Disk Space A Disk Space Usage on Datastore	•L: 61.4	200 PM 04:00 PM 06:00 PM
<i>i</i> ¶. r		vthunder_2nic_1vm_demo vth-inst1	vCenter Adapter vCenter Adapter	> 🛃 Guest > 🛃 Guest File System > 🛃 Memory		thrinstl THUNDERIDIsk Usage Percentage
∉ ¢		vthunder-inst1-ha-pd vThunder-File-Upload	vCenter Adapter	 Memory Usage on Host Network Performance 	•H: 36	36
©		vThunder-6-pd vth-agent	vCenter Adapter	> 🛃 Physical Disk > 🛃 Power > 🛃 Storage	•L: 35	33 34.5 2.00 PM 04.00 PM 06.00 PM
ê		vSphere World vSAN World	vCenter Adapter vSAN Adapter	> ♣ Summary > ♣ System > ➡ THUNDER	<u> </u>	X4.00 PM [2]
		vSAN Datastores	Container	 Memory Usage Percentage Disk Usage Percentage 		

4. From Metric Picker, expand Metrics > THUNDER-SHARED or THUNDER-Px and



double-click the following metrics:

- CPU Usage Percentage (Data)
- Throughput Rate (Global/BPS)
- Interface Down Count (Data)
- Total New Connection (Sec)
- Transactions Rate (Sec)
- Server Down Count
- Server Down Percentage
- SSL Errors Count
- Server Errors Count
- Total Session Count
- Packet Rate (Sec)
- Packet Drop Rate (Sec)

As the metric is selected, the corresponding data gets populated in the **Metric Chart** panel for the selected the time range.

Figure 42 : THUNDER-SHARED Dashboard

vm	vRealize Operations				с С Д <u>В</u>
»	Dashboards	Thunder Metrics ACTIONS ~			1H 6H 24H 7D CUSTOM 🔀 🖋
ŵ	☆ Home	Object List		Metric Picker	Metric Chart
	+ Create	Name 🤟	Adapter Type	> 🛃 vRealize Operations Generated	th-inst
5,		wr-dhcp	vCenter Adapter	V 🚵 THUNDER-SHARED	THUNDER-SHARED Server Down Count
IIa >	> ☆ Favorites	windows	vCenter Adapter	CPO Usage Percentage (Data) Interface Down Count (Data)	•H: 1
000	✓	WIN2016-DHCP	vCenter Adapter	Packet Drop Rate (Sec)	
	Thunder Metrics	vThunderådantor, Management Da	vRealize Operations	Packet Rate (Sec) Septer Down Count	411
ο.		vThunderAdaptor (vRealize Operati	vThunderAdaptor	Server Down Count Server Down Percentage	02:00 PM 04:00 PM 06:00 PM
<i>``</i>		vthunder_2nic_1vm_demo	vCenter Adapter	 Server Errors Count SSL Errors Count 	04:00 PM
<i>%</i> ~>		vth-inst1	vCenter Adapter	Throughput Rate (Global/BPS) Total New Connection (Per Sec)	THUNDER-SHARED Server Down Percentage
⊕ >		vthunder-inst1-ha-pd	vCenter Adapter	 Total New Connection (Sec) 	•H: 100
		vThunder-File-Upload	vCenter Adapter	Total Session Count	100
© >		vThunder-6-pd	vCenter Adapter	Transactions Rate (Sec) Properties	•L: 100
m		vth-agent	vCenter Adapter		02:00 PM 04:00 PM 06:00 PM
		vSphere World	vCenter Adapter		04:00 PM

To view multiple metrics data, select each of those metrics. The data corresponding to each metric is displayed in the **Metric Chart** panel. For the list of available Thunder metrics, see <u>Supported Thunder Metrics</u>.

Kibana (Elasticsearch)

134



To monitor the Thunder metrics on Kibana UI, perform the following steps:

1. Import the Kibana dashboard.

To import the Kibana dashboard, perform the following steps:

- a. Download the dashboard-template JSON file.
- b. Log in to Kibana.
- c. Navigate to Menu > Management > Saved Objects > Import.
- d. Select the downloaded Kibana dashboard file and click Import.

Figure 43 : Importing Dashboard File

E D Stack Management	Saved objects					
Security © Users	Saved Objects	1	Import saved objects $\hfill \stackrel{\times}{\longrightarrow}$			
API keys	Manage and share your saved objects. To edit the underlying d object, go to its associated application.	ata of an	Select a file to import			
Kibana ©			ch (
Data Views	Q Search	Тур	export.ndjson			
Saved Objects	Type Title Tags	Spaces	Remove			
Search Sessions	Advanced Settings [8.7.1]	-	Import options			
Spaces Advanced Settings	Rows per page: 50 \vee		Check for existing objects O Automatically overwrite			
Stack [®]			conflicts			
License Management			Request action on conflict			
Upgrade Assistant			Cancel Import			

2. View the Metrics.

To view the metrics, navigate to **Menu** > **Dashboard**. All the metrics are displayed as shown below:



Figure 44 : Thunder Dashboard



3. View the Metric Hits.

To view all the metric hits along with meta field details, navigate to **Menu** > **Discover** > **Thunder-Metrics**.

Grafana (Prometheus)

To monitor the Thunder metrics on Grafana UI, perform the following steps:

- 1. Import the Grafana dashboard.
 - a. Download the dashboard-template JSON file.
 - b. Log in to Grafana.
 - c. Navigate to Menu > Dashboard and click New > Import.

Figure 45 : Dashboards

Home > Dashboards		
器 Dashboards	Dashboards	
Playlists	Q Search for dashboards and folders	New Y
Snapshots		
Library panels	S Filter by tag v Starred D ≔ t≡ Sort	New Dashboard
		Import
	🖻 General	import
	Thunder C General	

. . . .



d. On the Import Dashboard page, click Upload dashboard JSON file.

Figure 46 : Import dashboard

Home > Dashboards > Imp	dashboard	
B Dashboards Playlists Snapshots Library panels	Import dashboard Import dashboard from file or Grafana.com	
	Lpload dashboard JSON file Drag and drop here or click to browse Accepted file types: .json, .txt	
	Import via grafana.com	
	Grafana.com dashboard URL or ID	oad
	Import via panel json	
	Load Cancel	

- e. Browse the downloaded Grafana dashboard file and click Load.
- 2. View the dashboard.

To view the dashboard, navigate to **Menu** > **Dashboard**. All the metrics are displayed as shown below:



Figure 47 : Grafana Metrics Dashboard

6		Q Sear	rch or jump to	. ED ctri+k					+ ~	۲	jh.	4
Home > Dashboards	Thunder 🟠 📽			📣 Add			② Last 15			0		
Disk Usage Percentage				Memory Usage Percentag 63.75 63.5 63.25	e				Refre	sh dasht	board	
0 	00 INT ="TOA", APPNAME="THU INT ="TOA", APPNAME="THU INT ="TOA", APPNAME="THU INT ="TOA", APPNAME="THU INT ="TOA" APPNAME="THU	19:05 DER", HOSTNAME="3cf8#3 DER", HOSTNAME="3cf8#3 DER", HOSTNAME="3cf8#3 INEB", HOSTNAME="3cf8#3	19:10 19c-9b46-47fe 19c-9b46-47fe 19c-9b46-47fe 19c-9b46-47fe	63	19:00 (AGENT = (AGENT = (AGENT = (AGENT =	"TOA", AI "TOA", AI "TOA", A	19 PPNAME="THU PPNAME="THU PPNAME="THU DPNAME="THU	KOS INDER", HOST INDER", HOST INDER", HOST INDER", HOST	TNAME = ". TNAME = ". TNAME = ".	ז 3cf8e39 3cf8e39 3cf8e39 ז-רגביז-ז	19:10 c-964 c-964 c-964 c-964	
Throughput Rate (Global/BF 800 600 400	×s)			Packet Drop Rate (Sec) 100 75 50 25 0								

Splunk

To monitor the Thunder metrics in Splunk Enterprise, perform the following steps:

- 1. Log in to Splunk Enterprise.
- 2. Create an HTTP Event Collector (HEC) for the metrics.

To use HEC, you need to configure at least one token. The token is used to authenticate and send data to Splunk.

- a. Navigate to Settings > Data Inputs > HTTP Event Collector.
- b. Click New Token.
- c. Enter the token name as 'collectorMetric' and click Next.
- d. Select a source type as log2metrics_json from the **Source Type** drop-down list box.
- e. Click Create a new index.
- f. Enter the name as 'thunder_metrics' and select the **Index Data Type** as **Metrics**. Click **Save**.

The index will be add to the Available Items list box.

g. Choose the newly created index ('thunder_metrics') from the **Available Items** list box.



h. Click Review to review the settings and then click Submit.

The token is created.

- i. Store the token generated for later reference.
- **NOTE:** If you have already created this token then ensure that the dashboard xml file contains the same index name.
- 3. Navigate to Apps > Search & Reporting > Dashboard and then click Create New Dashboard.

Figure 48	: Create N	lew Dashboard
1 901 6 10	. or cate r	Cir Dasiisoara

Dashboard Title	Thunder-Metrics		
	thunder-metrics		🖋 Edit ID
Description	Dashboard for the	Dashboard for thunder metrics	
Permissions	🔒 Private	•	
How do you want t	o build your dashboard	?	What's this?

4. On the **Create New Dashboard** form, perform the following steps:



- a. Enter a name for the dashboard in the **Dashboard Title** field.
- b. Enter description in the **Description** field.
- c. Select the appropriate permissions from **Permissions** drop-down menu.
- d. Under How do you want to build your dashboard?, select Classic Dashboard framework, and then click Create.
- 5. On the newly created dashboard, first click **Edit** and then click **Source**.

Figure 49 : Metrics Dashboard

Thunder-Metrics			Edit Export •
Time Range	Time Span		
Last 7 days 🔹	auto 👻	Hide Filters	

- 6. Copy the XML code from the dashboard template file and paste it in the editor.
- 7. Edit the following tags:
 - label It must be same as the Dashboard Title entered in <u>Step-4a</u>.
 - description It must be same as the dashboard Description entered in <u>Step-</u>
 <u>4b</u>.
 - query The index mentioned in this tag must be same as the one in use.
- 8. Click Save.
- 9. Verify if the metrics are displayed.



Figure 50 : Thunder-Metrics Dashboard

splunk-enterprise Apps *	🔕 Administrator * 🔕 Messages * Settings * Activity * Help * 🔍 Find
	🔀 Search & Reporting
Thunder-Metrics	Edit Export •
Deshboard for thunder metrics	
Average Disk Usage	Average Memory Usage 12.5 Average Memory Usage
	a.g., nemory., sage, per: 60.4
41	05
- 109,864,11391,917	65
0.00 PM 0.00 P	7.22 лис. 245.446 5.02 лис. 8.15 лис. 8.20 лис. 8.45 лис. 9.02 лис. 9.15 лис. 9.20 лис. 17 лиц.4 2012
Autorana Sonar Estars Court Autorana Total Sassina Court	Aurona SSI Error Court Q. J. I. O. Mr 100
100 - 100 -	100
Contract of the second s	1
	U
- against -	eq.t. cost
The Aug 1 Wed Aug 2 Thu Aug 1 Ye Aug 4 New Aug 1 Wed Aug 2	Thu Aug 3 Fin Aug 4 Thu Aug 3 Fin Aug 3 Fin Aug 4
2023 مەنقى ئەنتقى	2012 Anti
Average Server Down Percentage Average Server Down Count	Average Transactions Rate (Sec)
10 T	1
Tor Aug 1 Wed Aug 2 Thu Aug 3 Fit Aug 4 Tor Aug 1 Wed Aug 2 2023	Thu Aug 3 Fit Aug 4 Tun Aug 1 Wed Aug 2 Thu Aug 3 Fit Aug 4 2023
ini, ini,	بىر.
Average Interface Down Count (Data)	Average Total New Connection (Sec)
3	
	si
and the second s	- 10,335,444,2594504
000 PM 000 AM 000 PM 000 AM 000 PM 000 AM 000 AM 000 AM 000 AM 000 AM 200 AM 20	2 000 MM 0.00 AM 0.00 MM 0.000 MM 0.000 MM 0.000 MM 0.000 AM MM JUL
	_100
Average CPU Usage Percentage (Data) 100	Average Throughput Rate (Global/BPS) 100
3	5
9 9 9	16 IS
- and the reader for	eq_troughout,rate
1 200 РМ 1 200 АМ 1 200 РМ 1 200 АМ 1 200 РМ 1 200 АМ 200 РМ 200 АМ Мар № 1 200 Ам 1 200 РМ 1 200 АМ 1 200 РМ 1 200 АМ 1 200 РМ 1 200 АМ	200 PM 200 AM 200 PM 200 AM 200 PM 200 AM 200 PM 200 AM
2023	2023

GCP Metrics Explorer

To monitor the Thunder metrics on the GCP Metric Explorer, perform the following steps:

- 1. View the Metric
- 2. Customize the Metric
- 3. Create a Dashboard

View the Metric

- 1. Open Google Cloud Console and select the project you want to work with.
- 2. In the navigation menu, select **Monitoring** and then navigate to **Metrics Explorer**.



- 3. In the **Metric** section, click **Select a metric** to open a drop-down menu.
- 4. Select **Global** to access metrics applicable to your entire project.
- 5. Navigate to **Custom metrics**, scroll through the list of custom metrics and select the metric you want to monitor. For example, to chart the memory utilization, you can select **Memory Usage Percentage** metric as show in Figure 51.

Figure 51 : Select a metric in GCP

\sim	Monitoring	Metrics explorer	RETURN TO OLD QUERY EDITOR	🗉 🖸 🛨	G K 🕓 Last 5	minutes 🗸 IST 🔍 🗲 🐹 SAVE CHART
-	Metrics Scope	Quer Select a met	tric			Reset X
	i project	Filter by	y resource or metric name	✓ ACTIVE METRIC CATEGORIES		➤ ACTIVE METRICS
á	Overview	A Active		Popular metrics	1 metric >	CPU Usage Percentage (Data) custom.googleapis.com/a10networks-public-39
±:	Dashboards	V POPULAR RES	SOURCES	Billing	1 metric >	Disk Usage Percentage
⋺	Integrations	Global	22 metrics >	5		custom.googleapis.com/a10networks-public-39
e°	Services	✓ ACTIVE RESO	URCES	Custom metrics	14 metrics >	Interface Down Count (Data) custom.googleapis.com/a10networks-public-39
- 16	Metrics explorer	Audited Reso	ource 2 metrics >	Logs-based metrics	6 metrics >	Memory Usage Percentage custom.googleapis.com/a10networks-public-39
16	Metrics management	Consumed A	API 4 metrics >	Stats	1 metric >	Packet Drop Rate (Sec) custom.googleapis.com/a10networks-public-39
	Alerting					
<u>+</u>	Uptime checks	Consumer Q	uota 3 metrics >			custom.googleapis.com/a10networks-public-39
٢	Synthetic monitoring	GCS Bucket	9 metrics >			Server Down Count custom.googleapis.com/a10networks-public-39
Ē	Release Notes		·· ·			Server Down Percentage
<1		Selection previe Global > Cus	w stom metrics > Memory Usage Pero	centage		Cancel Apply

6. Click **Apply**.

The metric will be displayed as show in .

Memory usage percentage metric





Feedbad

 Click Save Chart in the Metrics Explorer toolbar to save the chart to an existing dashboard or you can create a new dashboard. To create a new dashboard, see <u>Create Dashboard</u>.

Customize the Metric

To customize and analyze your metrics data effectively, you can employ the following options:

- The **Widget type** drop-down menu within the **Display** pane allows you to choose from a variety of chart types including line charts, stacked area charts, and stacked bar charts.
- The **Threshold line** within the **Display** pane allows you to add a threshold line to the metric. You can also set an alert to receive notifications when the threshold is breached.
- The **Compare to Past** option under the **Display** pane allows you to select a time range from the past for comparing the metrics.
- The **Filter** element allows you to narrow down the metrics data based on specific filtering criteria such as resource labels, metric labels, resource types, and other metadata.



• The **Aggregation** element allows you to apply aggregation functions, using such as sum, average, count, min, max, and percentile to aggregate metric data.

Additionally, to add another metrics to the current chart, you can click **Add Query** and specify the metrics to be monitored. This allows comparing multiple metrics or data series within the same chart.

Create a Dashboard

To create a custom dashboard and monitor a metric, perform the following steps:

- 1. In the navigation panel, select **Monitoring**, and then click **Dashboards**.
- 2. On the **Dashboards Overview** page, click **Create Dashboard**.
- 3. Click the dashboard's title, enter a name for the dashboard and click **Save**.
- 4. Click + Add Widget and select the Metrics widget as shown in Figure 52.
External Thunder Observability Agent (TOA)



Figure 52 : GCP Dashboard - Add Widget

Add widget			×
Data			
Metric	Logs	EQ Log Analytics PREVIEW	Alert policy
Explore metric data	SLO		
Visualization			
Line	Stacked area	Stacked bar	Heatmap
Table	Top List	Gauge	1,337 Scorecard

- 5. Click **Select a metric** and navigate to **Global > Custom metrics**.
- 6. Scroll through the list of metrics, select a metric you want to monitor, and click **Apply**.

The metric will be added to the dashboard as shown in the following images.



Figure 53 : Metrics Dashboard in GCP

COV Events O Group by - T Filter ADD FILTER	Seried 12/12/23, 400 PM 🛛 💩 🔜 Autor
ALO DIDIT	
Mannon Hanas Banastana 1990/	PBHIlipan Berrantan Milel
minut A needla a annead a fanait	0 1
	5
	9
	6
ито-као алёми адёми адёми. • 10.44.25.160 • 10.64.25.181	° 1/170-130 3.1/PM 3.2/PM 3.2/PM 3.2/PM 3.2/PM 3.1/PM 3.1/PM 3.1/PM 3.1/PM 3.1/PM 4.0/PM 4.0
Disk Usage Percentage [SUM]	Interface Down Count [SUM]
	1
	۵
	a
	s , , , <u>, , , , , , , , , , , , , , , ,</u>
UTC-530 3167M 3207M 4007M 4007M	UTC-030 3307M 3307M 3307M 3307M 3307M 3307M 3407M 3407M 3407M 3407M 4007M 4007M 4007M
Packet Drop Rate (Sec) [SUM]	Packet Rate (Sec) [SUM]
	λ. Π
	25
anan saha saha saha saha saha saha saha	interes sine sine sine sine sine sine sine si
000000 200000 200000 200000 200000 200000 200000 200000 200000 200000 200000 000000	
Total Sensico Court (SUM)	Transactions Rate (Sec) (SUM)
4	
170-030 3:587M 3257M 3257M 3257M 3257M 3267M 3:67M 3:67M 3:67M 3:67M 3:67M 4:67M 4:67M 4:67M 4:67M 4:67M 4:67M	UTD-630 3:1974 32974 32974 32974 32974 34974
lerver Down Court [SUM]	Server Down Percentage (SUM)
1	
10-130 3:11/PU 3:21/PU 3:21/PU PI xPI0 +PI1 xPI2 +PI3 xPI6 #PI7 *PI6 #PI7 *PI8 +PI9 *P2 +P3 xP4 +P5 xP6 +P7 xP8 +P9 x 544880	URC+630 3116M 326M 326M 326M 336M 336M 346M 346M 346M 346M 346M 34
erver Errors Count [SUM]	SSL Errors Courr (SUM)
X	
	x
8	
03	x
10-630 ગ્રાંગમ રાગેગમ રાગેગમ રાગેગમ રાગેગમ રાગેગમ IPI ≋PIQ ♦PII ♥PIZ ▲PIB #PIZ ♦PIS #PIG ♥PIS #PIZ ♦PB #PI ♦PZ ♥PB #PI ♦PS #PB ♦PS #DB48ED	υτο-και ακέπει αρίπει
Throughput Rate (Global/UPS) (SUM)	Total New Connection (Sec) [SUM]
22	1
	80
	202
C+630 315PM 325PM 325PM 325PM 325PM 325PM 325PM 325PM 325PM 465PM 465PM 465PM 465PM 465PM 465PM 465PM	บกระนอง 3.15PM 202PM 202PM 202PM 202PM 202PM 202PM 202PM 402PM 402PM

OCI Metrics Explorer

To monitor the Thunder metrics on the OCI Metric Explorer, perform the following steps:

- 1. View the Chart
- 2. Create an Alarm
- 3. Create a Dashboard

146

. . . .



View the Chart

- Log in to the OCI console, open the navigation menu and click Observability & Management.
- 2. Under Monitoring , click Metrics Explorer.

The **Metric Explorer** page will be displayed as shown in Figure 54. This page is divided into two sections, the graph section, where the graphs are displayed and the query section, where you can define a query.

Figure 54 : OCI - Metric Explorer

r	Start time	End time	2024 10 22 43 UTC	Quick selects						Y-Axis Label	Y-Axis Min value	Y-Axis Max value
	1010,1010,000		2024 10 22 03 010	List nour 🗘						Custom y-axis tablet	Custom minimum value	Custom maximum v
												Show Data
	60-						_					
	40-											
	20-											
	2012月											
	09.35	09.40	09.45	09.50	09.55	10.00	10.05	10.10	10.15	10.20	10.25	10.30
						10.00						
	Aquet in exit (whole of data display					tine (of	, 					
	Aquet varie (ontoor of sets open 11.05 Close query editor	55.53	16.15	15.20	15.25	15:30	15.35	15-a0	15.45	1550	15.55	16.00
	Apier versi instan data data Unité Cone query estar	35 [°] 30	15.15	uizo Query 1	15.25	16.30	15.35	15-00	15.45	15.50	1555	1600
	Agut +ent protor of an along stats Close query editor	15 ⁵ 13 4(5 = "(HARDER").rear()	55 5 5	side	15/25	196-30	1938	15-40	19.45	1550	1555	1600
	Agent + ett sunnar + des stops vision Close query editor Closer y 1 menn, lange, three entrops (14) (Web)	15.10 RCE = "PMADER").rean()	si is Add Overy	Query 1 Conditioners	15/25	1530	v 1525 Metric narrespace ⊘ Bunder	15-40	19.45	Resource group	túss Optional ()	1600
	Ager-ser John right	15.10 RCK = "PMADER").rean()	15.15	Guery 1 Congarment CoughtaineCript Homesinade (publiciptingCouchtien	1525 wCmpt	15:30	1525 Metrio namespace ⊘ Brunder	15-40	1645	Resource group C Transer	tiúss Optional @	1600
	Ager - ero sonor ef an atop, siss Close query atoffer Close query atoffer Manay, sage, for entage (sc) events	95 [°] 19 K(K = "PHARDR").ream()	15 15 Add Coery	relation	1525 1625	1530	1535 Maris namespace () Bunder Interval ()	15.40	1645	tidat Resource group Thunder Statistic @	túiss Captionaí 🥥	1600
	Agencies remove data may 1988 Casa away ether Case y away ether Case y 1 Remove Augnore entropy (1) (1989)	15'10 KC = "Inklast"),man()	15:55	Cuery 1 CostativeCost CostativeCost ribercostade reproductive Merrory, Diago, Percentage	tilas wCrap	1630 C	tiús Metric namespace () Brunder Interval () 1 minute	16-40	1948	tião Resource group C) Thunder Statistic ⊙ Mean	túiss Captionaí (j)	sioo
	April 44 million (2014) USA Core Gary and Core American (2014) Marris, Single American (2014)	5553 861 • *19648(8*).seae()	vins	Vide Query 1 Congenier Congenier Conditiencing Conditiencing Merroy, Diago, Percentage	súas	10000000000000000000000000000000000000	tiúss Matric namespace ⊘ thunder Interval © I minute	1540	vies	tilis0 Resource group C Trunder Statistic ⊙ Mean	teles	Told
	Ager an arrows or any arrow of	5553 80(- *156884*),arps()	vi ss	Cuery 1 Coursement Coursement Coursements Coursements Coursements Coursements Coursements Coursements Coursements Course	19/25 seCrapt	1000 C	15.56 Matric narvespace () Bunder Iterval () 1 minute	1510	vies	1500 Resource group O Thunder Sastato O Mean	ssas	tais
	April - an instance of the state Units Come events when Come events when Come events when the state Come events when the state of the state State of the state of the state of the state State of the state of	15 ⁵ 13 80 + "196854").mear()	tá tá Add Overy	User Query 1 Counterform Counterform Counterform Counterform Counterform Counterform Counterform Counterform Counterform Counterform Metric climenisions Dimension name @	tujas 	1530 C	16.55 Natio namespace () Bunder Interval () I minute	1500	1145	1550 Resource group C) Thunder Statistic @ Mean	siste	1600

- 3. In the query section, enter the following:
 - **Compartment** Select a compartment where you want to do the analysis and you have access.
 - Metric namespace Select the metric namespace for querying metric data; thunder in this case. This drop-down lists metric namespaces for the selected compartment.
 - **Resource group** Select a resource group; **Thunder** in this case. Specifying a resource group ensures that only metric data for the resources within that group are returned.
 - Metric Name Select a metric name from the drop-down menu.



- Metric Dimensions (optional) Set dimensions by selecting a dimension name and specifying a dimension value. By selecting appropriate dimensions, you can limit the metric data.
- 4. Click Update Chart.

The updated chart will be displayed in the graph section.

Create an Alarm

1. In the query portion of the **Metric Explorer** page, click **Create Alarm**.

The **Create Alarm** page will be displayed as shown in Figure 55.

Figure 55 : OCI - Create Alarm Page

ORACLE Cloud Search resources, services, documentation, and Marketplace					US West (Phoenix) ~ 🗔 🛕 🧿 (
ate Alarm					
Your alarm is almost complete. Fill in all remaining required fields below					
fine alarm					Switch to Advanced Mor
name			Alam severity ()		
U_Usage_Percentage_Alarm			Critical		0
bedy Detienal ()					
alarm which triggers when the mean of CPU usage percentage is above 50 percent.					
d to 1000 characters (1/1000)					
agar (year-on-ne) gging is a metadata system that allows you to organize and track alarms within your tenancy (newspace None (apply a freeform tag)	+	Tag key Enter a tag key		Value Enfor a lag key first	×
					+ Additional tag
fetric description he metric to evaluate for the atam.					
ompariment		Metric namespace ④		Resource group Optional ()	
CloudNativeCmpt	0	thunder	0	Thunder	0
Inetworkscloud (root) EngOrg/CloudNativeOrpt					
etric name ()		Interval ()		Statistic ()	
CPU_Usage_Percentage_Data	0	1 minute	0	Mean	0
table dimensions					
ieuric dimensions					
inension name @			Dimension value ()		
reditic dimensions. mension name ⊙ felicit a value		•	Dimension value () Select a value		• ×
ettin C uttintensiontas exector name (2) etect a value Aggregate metric atreams (2)		\$	Dimension value (j) Select a value		Additional dimension

- 2. Enter a name for the alarm and select the severity level from the **Alarm Severity** drop-down menu.
- 3. In the **Alarm body** text box, enter a notification message.
- 4. In the Metric description area, enter the following metric details:
 - **Compartment** Select the compartment that contains the resources to generate metrics evaluated by the alarm. This compartment also serves as a storage location for the alarm.



- Metric namespace Select a service that generates the metrics for the resources that you want to monitor; thunder in this case. The drop-down lists all metric namespaces for the selected compartment.
- **Resource group** Select the resource group that the metric belongs to; Thunder in this case.
- Metric name Select a metric name you wish to evaluate for the alarm.
- Interval Select a time-frame or a frequency at which data points are aggregated.
- Statistics Select a statistical function to aggregate data points. The options available are Mean, Rate, Sum, Max, Min, and more.
- 5. In the **Metric Dimensions** area, select a dimension name and specify a dimension value. By selecting appropriate dimensions, you can narrow the metric data to be evaluated.
- 6. In the **Trigger rule** area, specify the condition to be satisfied for the alarm to be triggered. Set the following parameters:
 - **Operator** Select an operator to be used for the condition threshold. For example, **greater than** or **less than** operators.
 - Value Enter the value to be used for the condition threshold.
 - **Trigger delay minutes** Enter the number of minutes before the alarm is triggered.

Figure 56 : Create Alarm - Trigger rule area



7. In the **Destination** area under **Define alarm notifications**, select the destination for alarm notifications.



Figure 57 : OCI - Define Alarm Notifications

Define alarm polifications							
Denne alarmitotilcations							
Destination	Destination						
Destination							
Destination service ④		Compartment ④		Topio	e ()		
Notifications	0	CloudNativeCmpt	0	Sel	elect a value		
	the second and the second s						
Create a new topic and subscription							
Topio name			Topic description Optional				
ThunderMetricsAlarm							
Subscription protocol (2)			Subscription Email ()				
Ernal		0	user@gmail.com				
Create topic and subscription Cancel							
Message grouping							
This alarm applies to 6 metric streams.							
 Group notifications across metric streams Split notifications per metric stream 							
Message Format							
Send formatted messages							
Send Pretty JSON messages (raw text with line break in the break in	ka)						
 Send raw messages 							
Repeat notification? (I alarm cardinues to fire)							
Superass relifications						Q	
) протехности на страници н						
Z Enable this alarm? ()							
Sava alarm Cascal							

Set the following parameters:

- Destination service Select one of the following:
 - **Notifications** Send alarm notifications to a topic. A topic is a communication channel for sending messages.
 - **Streaming** Send alarm messages to a stream. A stream is an append-only log.
- **Compartment** Select the compartment that contains the resources that generate metrics evaluated by the alarm.
- Stream (If Destination service selected is Streaming) Select a stream for alarm notification.
- **Topic** (If **Destination service** selected is **Notifications**) Select a topic to be used for notifications.

You can select an existing topic or create a new one. To create a new topic, click **Create a topic**. Enter a topic name, description, **Subscription Protocol** (Email, SMS, Custom URL, and more) and click **Create topic and subscription**.

8. Select Enable the alarm? checkbox.



When the alarm is enabled, the configured metric is evaluated and alarm messages are sent to the selected destination service when the metric data satisfies a condition and triggers the rule.

9. Click Save Alarm.

You can view the newly created alarm by navigating to **Monitoring** > **Alarm Definitions**. Here, you can enable, disable, and edit the alarm as well.

For more information of Alarms, see Managing Alarms.

Create a Dashboard

To create a dashboard, perform the following steps:

- 1. Log in to the OCI console, open the navigation menu and click **Observability & Management**.
- 2. Under Logging Analytics, click Dashboard.

The **Dashboards** page with a list of existing dashboards will be displayed.

- 3. Click Create dashboard.
- 4. In the About tab, enter a Dashboard name, Dashboard compartment, and Dashboard description.
- 5. In the Widgets tab, click +.

Here you can select one of the following:

- **Create Widget** This option allows you to add a variety of pre-configured widgets to your dashboard. To create a widget, see <u>Create Widget</u>.
- Create Query-Based Widget The option allows you to add widgets based on queries executed against your data. To create a query-based widget, see Create Query-Based Widget.

After creating and saving the widgets, they are automatically added to the dashboard as shown in Figure 58.



Figure 58 : Widgets added to Dashboard

Server Down Count Average ①	Server Down Percentage Average
	8
5 **	2 50
0 40	<u><u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u></u>
30 30	6.30
0 m	5 m
	0.20
8 10	2 10
· · · · · · · · · · · · · · · · · · ·	8 0 <u>x x</u>
01:00 PM 01:05 PM 01:10 PM 01:15 PM 01:20 PM 01:25 PM 01:30 PM 01:35 PM 01:40 PM 01:46 PM 01:60 PM	01:00 PM 01:05 PM 01:10 PM 01:15 PM 01:20 PM 01:25 PM 01:30 PM 01:36 PM 01:36 PM 01:36 PM 01:36 PM
Annu England Annua	
Server Errors Count Average	SSL Error Count Average
60	60
T 50	
Š e	5.0
1 8 C	8.1
E 30	£ 30
4 20	20
5 10	35 10
01:00 PM 01:05 PM 01:10 PM 01:15 PM 01:20 PM 01:28 PM 01:30 PM 01:38 PM 01:40 PM 01:45 PM 01:60 PM	01.00 PM 01.00 PM 01.10 PM 01.15 PM 01.20 PM 01.25 PM 01.30 PM 01.35 PM 01.36 PM 01.40 PM 01.45 PM 01.60 PM PM 01.40 PM
	8 9 9 9 9 9 9 9 9 9 9 9 9 9
Transactions Rate (Sec) Average	Throughput, Rate (Global/Rate) Average
_ 60	1.0K
X 40	A
10. ···	
8 20	
Ť 20	
2 10	<u>₽</u> [∞] 02×
E	
0100 PM 0110 PM 0110 PM 0115 PM 0120 PM 0125 PM 0125 PM 0130 PM 0135 PM 0135 PM 0140 PM 0140 PM	0120 0120 0120 PM 0110 PM 0110 PM 0110 PM 0120 PM 0120 PM 0120 PM 0120 PM 0140 PM 0140 PM 0140 PM 0140 PM
Rah 6 2024	Feb 5, 2024

Monitor Logs

Depending on your cloud provider, the steps are provided to monitor the configured logs.

AWS CloudWatch

To monitor the Thunder logs on the AWS CloudWatch, perform the following steps:

1. From the AWS Management Console, go to CloudWatch > Logs > Log groups.

aws	Services	Q Search	1		[Alt+S]]					2	🔶 🕜 N. Virginia	•	AllowUserToPassCloudWatc	hL	Runge Tener	•
Cloud	Watch	×		CloudWat	ch 🗧 Log groups												
Favorite	s and recents	•		Log	aroups (14)							Ct Actions =	1	View in Long Incidity		ate les group	
Dashbo	ards			By defai	ult, we only load up to 10000 log groups.									view in Logs insights	Cit	race rog group	•
Alarms	۱ 🛆	1 Ø 0 ⊖ 8		Q F	ilter log groups or try prefix search			Exact match								< 1 > @	>
₩ Logs					Log group		Data protection	 Sensitive data count	⊽	Retention	▼	Metric filters	▼	Contributor Insights	v	Subscriptio	v
Log gro	sights				/aws/lambda/nvm-ext-server-lambda-function		⊖ Inactive	-		Never expire		-				-	
					/aws/lambda/nvm-ext-vth-lambda-function		⊖ Inactive	-		Never expire		-				-	
 Metrics All metrics 	rics				/aws/lambda/sachin-test-lambda-function		⊖ Inactive	-		Never expire		-					
Explore	r				/aws/lambda/test-lambda-function		⊖ Inactive	-		Never expire		-					
Streams	5				/aws/lambda/test-nvm-server-lambda-function		⊖ Inactive	-		Never expire		-					
▶ X-Ray t	races				/aws/lambda/test-nvm-vth-lambda-function		⊖ Inactive	-		Never expire		-				-	
Events					/aws/lambda/test1		⊖ Inactive	-		Never expire		-				-	
Applica	ition monitori	ring			/aws/lambda/vth-lambda-function		⊖ Inactive	-		Never expire		-		-		-	
Insights	s				/aws/lambda/vth-pub-lambda-function		⊖ Inactive	-		Never expire		-		-		-	
Setting	s				aws-metrics		⊖ Inactive	-		3 days		-				-	
Getting	Started				new_logs		⊖ Inactive	-		1 day		-				-	
					test		⊖ Inactive	-		1 day						-	
					vThExternalAgent		⊖ Inactive	-		Never expire		-					
					Thunder		⊖ Inactive	-		Never expire		-					

Figure 59 : AWS Log Groups



2. Click **Thunder** log group.

Figure 60 : Thunder Log Group

CloudWatch ×	CloudWatch > Log groups > Thunder		
Favorites and recents	Thunder		Actions v View in Logs Insights Search log group
Dashboards Alarms ▲ 1 ⓒ 0 ⓒ 8	▼ Log group details		
Logs Logs Insights Metrics All metrics Explorer Streams	ARN amawsJogsus-east-1:9398501966822.log-group: • Creation time 14 days ago Retention Never expire Stored bytes 822.2.8	Metric filters o Subscription filters o Contributor Insights rules -	Data protection - new inactive Sensitive data found - new - KMS key ID -
X-Ray traces Events Rules	Log streams Metric filters Subscription filters Contributor	Insights Tags Data protection - <i>new</i>	
Event Buses Application monitoring	Log streams (68) Q. Filter log streams or try prefix search	Exact match Show expired 🕑 Info	C Create log stream Search all log streams < 1 > ∅
Settings	Log stream		•
Getting Started	30/03/2023/[\$LATEST]ghsnvjowgwqxtoy 30/03/2023/[\$LATEST]noihowbksriwyxd	2023-03-30 16:22:28 (UTC+05:3 2023-03-30 14:59:51 (UTC+05:3	(כ
	29/03/2023/[\$LATEST]yiknlhafiabpzzf	2023-03-29 19:42:57 (UTC+05:3	
	29/03/2023/[\$LATEST]vnhqlokmtoaeyuq	2023-03-29 19:36:49 (UTC+05:3	(0

3. Under the **Log streams** tab, click the required log stream to be monitored.

All logs are displayed in tabular format with expandable details.

Figure 61 : Logs events on AWS CloudWatch

CloudWatch ×	CloudWatch > Log groups > 1	hunder > 09/05/2023/10.67.4.25/3ae28ba2-c8b9-497f-8b98-76bedc93f31b		
Favorites and recents	Log events			
Dashboards	You can use the filter bar below	to search for and match terms, phrases, or values in your log events. Learn more about filter patterns 🗹		C Actions V Create metric filter
▶ Alarms 🛕 1 ⊘ 0 💬 8	Q. Filter events		Clear 1m 30m	1h 12h Custom 🗉 Display 🔻 🥥
▼ Logs				
Log groups	Message			
Logs Insights	No older events at this moment	L. Retry		
▼ Metrics	May 09 2023 09:13:36 Notice	[SYSTEM]:A aXAPI session for user "admin" from 10.67.4.12 has been opened. Session ID assigned is 74.		
All metrics	May 09 2023 09:13:36 Notice	[SYSTEM]:A aXAPI session for user "admin" from 10.67.4.12 has been opened. Session ID assigned is 73.		
Explorer	May 09 2023 09:13:36 Info	[SYSTEM]:Session timed out		
Streams	May 09 2023 09:13:36 Info	[SYSTEM]:Session timed out		
X-Ray traces	May 09 2023 09:13:36 Info	[SYSTEM]:Session ID 53 for user "admin" from 10.67.4.12 has timed out		
▼ Events	May 09 2023 09:13:36 Info	[SYSTEM]:Session timed out		
Rules	May 09 2023 09:13:36 Info	[SYSTEM]:Local authentication successful (user: admin).		
Event Buses	May 09 2023 09:13:36 Info	[SYSTEM]:Session ID 52 for user "admin" from 10.67.4.12 has timed out		
Application monitoring	May 09 2023 09:13:36 Info	[SYSTEM]:Local authentication successful (user: admin).		
h losiobte	May 09 2023 09:14:36 Notice	[SYSTEM]:A aXAPI session for user "admin" from 10.67.4.12 has been opened. Session ID assigned is 76.		
P IIBIGIIIS	May 09 2023 09:14:36 Info	[SYSTEM]:Local authentication successful (user: admin).		
Settings	May 09 2023 09:14:36 Notice	[SYSTEM]:A aXAPI session for user "admin" from 10.67.4.12 has been opened. Session ID assigned is 75.		
Getting Started	May 09 2023 09:14:36 Info	[SYSTEM]:Session timed out		
	May 09 2023 09:14:36 Info	[SYSTEM]:Session ID 55 for user "admin" from 10.67.4.12 has timed out		
	May 09 2023 09:14:36 Info	[SYSTEM]:Session timed out		
	Nav. 00 2022 00:14:24 Toto	(EVETEN) Garring TO 54 dec upon "admin" doom 10 57 4 11 bar timed out		

Azure Log Analytics Workspace

To monitor the Thunder logs on the Azure Log Analytics Workspace, perform the following steps:

153



- 1. From the **Azure Portal**, go to **Azure services** > **Resource Groups** > <*your_ resource_group*> and click your log analytics workspace name.
- 2. Click Logs from the left General panel.

You can close the **Queries** pop-up window.

- 3. From New Query1 > Tables tab, expand Custom Logs.
- 4. Double click THUNDER_SYSLOG_CL.

The THUNDER_SYSLOG_CL query window is displayed.

Figure 62 : Custom Logs window

Home > vth-vmss-log-workspace6												
vth-vmss-log-work Log Analytics workspace	space Logs ☆ …											×
P Search «	₽ New Query 1* 🛛 × 🕂									💙 Feedbad	k 🔠 Queries 🍥	• m ~
Cverview	P vth-vmss-log-wor Select scope	Run Time range : Last	30 minutes	Save 🗸 🖻 Share 🗸 🕂 N	iew alert rule	→ Export ∨ 5	Pin to 🗸 🛛 🖀	Format query				
 Activity log 	Tables Oueries Functions ··· «	1 THUNDER_SYSLOG_CL										-
Access control (IAM)												
Tags	,₽ Search :											*
Diagnose and solve problems	🍸 Filter 📔 Group by: Solution 🗸	Results Chart										Q
🧬 Logs	T Collapse all	TimeGenerated [Local Time] ↑↓	JOBID_s	log_data_s	LOG_TYPE_s	APPNAME_s	HOSTNAM	IP_s	AGENT_s	PRIORI	Туре	
Settings	Favorites	 5/9/2023, 1:37:02.212 PM 	20230509080701	May 09 2023 09:05:36 Notice [Syslog	Thunder	10.67.4.25	10.67.4.25	TOA	Info	THUNDER_SYSLOG_C	a de
Tables	You can add favorites by clicking on	Tenantid	dcfd78d5-3a49-	425d-8410-e02e281f7991								ā
Anants	the 🛠 icon	SourceSystem	RestAPI									-1.
Agenis	 LogManagement 	TimeGenerated [UTC]	2023-05-09T084	07:02.2128943Z								- 1
Usage and estimated costs	 Custom Logs 	JOBID_s	2023050908070	1								
🗈 Data export	fluentbit_CL	log_data_s	May 09 2023 09	05:36 Notice [SYSTEM]:A aXAPI session	n for user "admin"	from 10.67.4.12 has	been opened. Sessio	n ID assigned is 5	7.			
Network isolation	▲ Ⅲ THUNDER_SYSLOG_CL	LOG_TYPE_s	Syslog									
Linked storage accounts	t AGENT_s (string)	APPNAME_s	Thunder									
III Properties	t APPNAME_s (string)	HOSTNAME_s	10.67.4.25									
	f Computer (string)	IP_5	10.67.4.25									
Loois	t HOSTNAME s (string)	AGENT_s	TOA									
Classic	t IP s (string)	PRIORITY_5	Info									
Legacy agents management	f log_data_s (string)	Type	THUNDER_SYSU	DG_CL								
Legacy activity log connector	t LOG TYPE s (string)	> 5/9/2023, 1:37:02:212 PM	20230509080701	May 09 2023 09:05:36 Info [SYS	Syslog	Thunder	10.67.4.25	10.67.4.25	TOA	Info	THUNDER_SYSLOG_C	1.
Legacy storage account logs	f PRIORITY s (string)	> 5/9/2023, 1:37:02:212 PM	20230509080701	May 09 2023 09:05:36 Notice [S	Syslog	Thunder	10.67.4.25	10.67.4.25	TOA	Info	THUNDER_SYSLOG_C	1.
Legacy computer groups	t RawData (string)	> 5/9/2023, 1:37:02:212 PM	20230509080701	May 09 2023 09:05:36 Info (\$YS	Syslog	Thunder	10.67.4.25	10.67.4.25	TOA	Info	THUNDER_SYSLOG_C	1
- cogacy compared groups	TimeGenerated (datatime)	> 5/9/2023, 1:37:02:212 PM	20230509080701	May 09 2023 09:05:36 Info [SYS	Syslog	Thunder	10.67.4.25	10.67.4.25	TOA	Info	THUNDER_SYSLOG_C	1.
Legacy solutions	 Innegenerated (datetime) 											

5. Click Run.

All logs are displayed in tabular format with expandable details.

The following table lists the Thunder Logs filter options:

Table 56 : Log Filters

Filter	Description
log_data	Specifies the actual log entry.
hostname	Displays the vThunder resource ID.
log_type	Displays the vThunder system logs.
appname	Displays the application name.



Table 56 : Log Filters

Filter	Description
ip	Displays the vThunder IP address.
agent	Displays the agent name.
jobid	Displays the JOB ID provided in the thunder-observability- agent.log file.
priority	Displays the Notice, Info, Error, and so on as per actual log entry.
partition	Displays the vThunder partition name.

VMware vRLI

To monitor the Thunder logs on the VMware vRLI, perform the following steps:

- 1. Start vRLI VM
- 2. View Logs

Start vRLI VM

To start the vRLI virtual machine, perform the following steps:

1. From the VMware ESXi console, go to Navigator > Virtual Machines > <your_ vRLI_VM> and click Power on.

Figure 63 : Start vRLI VM

Ta Navigator	(VMware-vRealize-Log-Insight-8.8			
* 🛛 Host Manage	Console Monitor > Post	eron 🍙 Shut do	own 🔢 Suspend 🧑 Restart 🥖 Edit 🥑 Refresh	Actions
Montor	Co. Co. Co. Co. Co. Co. Co. Co. Co. Co.	Mware-vRealize uest OS ompatibility Meare Tools PUs	e-Log-Insight-8.8 Cther 3.x or later Linux (64-bit) ESR6 02 without machine Yesi 4	5 GHz
th-agent th-inst1		ost name	a ua localhost	8.06 GB

NOTE:

The system may take a few minutes to start the vRLI virtual machine.

2. Click **Console** to launch vRLI virtual machine.

The vRLI virtual machine is powered on and reachable.

155



Figure 64 : VMware vRealize Log Insight

VMware-vRealize-Log-Insight-8.8	🖬 🗉 💷 🏠 Actions 🛞
VMware vRealize Log Insight 8.8.0 Build 19675011	
Visit VMware vRealize Log Insight:	
metp // 10.07.4.15/	

View Logs

1. From the **vRealize Log Insight Web UI**, go to **Home** > **Explore Logs** to view the logs.

The Logs window is displayed.

Figure 65 : vRealize Log Insight - Overview window

vm	Log Insight	Ø	admin ~
	+ NEW DASHBOARD Custom Dashboards A My Dashboards plore Logs ed Dashboards	Latest 5 minutes of d c Display legend on all widgets ① ① ①	≮ ₽
⊴ > & 83	Content Pack Dashboards	Number of events by _ & i * localitotipe exa. procedent procede	i *-
6 4 () >	Problems Event Types Statistics	gr 00 100	h
†4† >	Log Insight Agents Syslog Agents VMware - vROps 6.7+ VMware - vSAN	Number of error even_ d <i>i</i> *	i *-

- 2. Click **Add Filter** and add the following filter criteria to search all the logs received from a specific Thunder IP:
 - _index: ip
 - condition: is
 - value: <Thunder_IP>



Figure 66 : vRealize Log Insight - Add Filter



- 3. Add the following filter criteria to search all logs received from TOA:
 - _index: source
 - condition: is
 - value: <TOA_IP>
- 4. Verify if the logs are generated.

Figure 67 : Logs on vRealize Log Insight

vm	n Log Insight	
»	May 29, 2022 634 02 PM to 639 22 PM to 639 2	Go to Snapshots 📰 Add to Dashboard 🌰
۵		
M		
ھ >	aba aba aba	1839
*	Count of events + + over time + Acroy Reset	iconds - Chart Type 🖬 Automatic - 🔹
æ.,	Latest 5 minutes of data 🗸 🗸 🖸	👷 📑 🗍 🌲 🖄
Lø	+ ADD FLITER May 29, 2023, 18:34:02.466 to May 29, 2023, 18:39:3	2.852
<u>e</u>	CONTENT PACKS v (Extract all fields)	
(j) >	Events Field Table Event Types Event Trends 1to 50 out of \$1 events View* Sort Never16 First*	Manage Fields 🖋 😕
117 >	8-May 29, 2023 May 29 2023 14:45:57 Info 83302.455 spure agent appname event_type hostname ip jobid kg_type partition promity	
	8-May 29, 2023 May 29 2023 14:05:57 Notice (SISTBQ:).4 adv21 session for user "advin" from 10.44.25.12 has been opened. Session ID assigned is 29. 83:39:02:485 source agent appname event_type hostname ip jobid log_type partition priority	hostname jo jobid
	Hay 29, 2023 Hay 29 2023 14:45:57 Hotice (SHSTB01:Session ID 29 is now closed. Hit 30:02.485 source agent appname event_type hotiname ip jobid log_type partition priority	log_type partition priority
	Wey 29, 2023 Way 29 2023 14:05:57 Info SistB01:Local authentication successful (seer: absis). Bi302.485 source agent appname event_type hostname (p jobid log_type partition priority	E source
	Hug 22, 2023 Hug 25 12425 14-051-57 Notice (SHSTBQ):A JuNPI session for user "admin" from 10, 64, 25 12 has been opened. Session 1D assigned is 30. HIGP 02.485 source agent appname event_type hostname ip polid log_type partition priority	
	Weily 29, 2023 Way 29 XN21 14-051-57 Notice (SHSTBD):Session ID 38 is now classed. HISH 02.485 source agent apprame event_hype hostname ip polid log_type partition priority	
	6+May 29, 2023 May 29 2023 H4-06:55 Info [SYSTBO]:Local authentication successful (user: admin). 10:20:02:401 source agent appname event, yoe hostname to jobid log_type partition priority	

The following table lists the Thunder Logs filter options:



Table 57 : Log Filters

Filter	Description
hostname	Displays the Thunder resource ID.
log_type	Displays the Thunder system logs.
appname	Displays the application name.
ip	Displays the Thunder IP address.
agent	Displays the agent name.
jobid	Displays the JOB ID provided in TOA in the thunder- observability-agent.log file.
priority	Displays the Notice, Info, or Error, and so on as per actual log entry.
partition	Displays the Thunder partition name.

Kibana (Elasticsearch)

To monitor the Thunder logs on Kibana UI, perform the following steps:

1. Import the Kibana dashboard.

To import the Kibana dashboard, perform the following steps:

- a. Download the dashboard-template JSON file.
- b. Log in to Kibana.
- c. Navigate to Menu > Management > Saved Objects > Import.
- d. Select the downloaded Kibana dashboard file and click Import.



Figure 68 : Importing Dashboard File

E D Stack Management	Saved objects	
Security © Users	Saved Objects	Import saved objects $^{ imes}$
Roles API keys	Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.	Select a file to import
Kibana ©		ch
Data Views		
Files	Q Search	p <u>export.ndjson</u> Remove
Saved Objects	Type Title Tags Spaces	
Tags Search Sessions	Advanced Settings [8.7.1]	Import options
Spaces	Davia par para E0 st	• Chack for existing objects
Advanced Settings	Rows per page. 50 V	Check for existing objects
		Automatically overwrite
Stack [®]		conflicts
License Management		C Request action on conflict
Upgrade Assistant		Cancel Import

2. View the Logs.

To view the logs, navigate to **Menu** > **Dashboard**. All the logs are visible below the metrics as shown:

Figure 69 : Logs Dashboard

1	•	elastic	Q. Find app	os, content, an	nd more.				•/		o	6	8× 🔇
=		D Dashboard	Thunder 🗸						Full scree	n Share	Clone	0	Edit
0	gs											12 de	ocume
=	Co	lumns © 1 field sorted	1									13	
		↓ TIMESTAMP 🕙 🗸	message ~	LOG_TYPE ~	PRIORITY ~	HOSTNAME ~	IP v	JOBID ~	APPNAME \sim	partition \sim	NAMESPA	~	AGENT
^		Nov 2, 2023 0 19:11:45.000	Nov 02 2023 13:38:46 Warning [ACOS]:The total unknown unicast packets 6870 per	Syslog	Warning	3cf8e39c- 9b46-47fe- a967	10.64.25.181	20231102134145	THUNDER	SHARED	THUNDER- SHARED		TOA
"		Nov 2, 2023 Ø 19:11:24.000	Nov 02 2023 13:38:46 Warning [ACOS]:The total unknown unicast packets 6870 per	Syslog	Warning	3cf8e39c- 9b46-47fe- a967	10.64.25.181	20231102134124	THUNDER	SHARED	THUNDER- SHARED		TOA
P		Nov 2, 2023 0 13:55:11.000	Nov 02 2023 08:22:13 Notice [SYSTEM]:Session ID 415 is now closed.	Syslog	Notice	3cf8e39c- 9b46-47fe- a967	10.64.25.181	20231102082511	THUNDER	SHARED	THUNDER - SHARED		TOA
7		Nov 2, 2023 0 13:55:11.000	Nov 02 2023 08:22:11 Notice [SYSTEM]:Session ID 414 is now closed.	Syslog	Notice	3cf8e39c- 9b46-47fe- a967	10.64.25.181	20231102082511	THUNDER	SHARED	THUNDER- SHARED		TOA
<i>p</i>		Nov 2, 2023 0 13:55:11.000	Nov 02 2023 08:22:07 Notice [SYSTEM]:A aXAPI session for user "admin" from	Syslog	Notice	3cf8e39c- 9b46-47fe- a967	10.64.25.181	20231102082511	THUNDER	SHARED	THUNDER- SHARED		TOA
2		Nu. 0 0000 A	NULL AR ARRA ARIANIAT T.C.	Cup144	* - f -	A. 60.00.	10 44 06 101	00001100000511	111.007.0	2111 D.C.D.	1110000		-

3. View the Log Hits.

To view all the log hits along with meta field details, navigate to **Menu** > **Discover** > **Thunder-Logs**.

Grafana (Prometheus)

To monitor the Thunder logs on Grafana UI, perform the following steps:



1. Import the Grafana dashboard.

To import the Grafana dashboard, perform the following steps:

- a. Download the dashboard-template JSON file.
- b. Log in to Grafana.
- c. Navigate to Menu > Dashboard and click New > Import.

Figure 70 : Dashboards

Home > Dashboards			^
器 Dashboards	Dashboards		
Playlists			New ~
Snapshots			New Dashboard
Library panels	Starred	t≡ Sort	New Folder
			Import
	Thunder Ci General		

d. On the Import dashboard page, click Upload dashboard JSON file.



Figure 71 : Import dashboard

	rt dashboard
器 Dashboards	Import dashboard Import dashboard from file or Grafana.com
Playlists	
Snapshots	Line databased 1991) file
Library panels	Drag and drop here or click to browse Accepted file types: .json, .txt
	Import via grafana.com
	Grafana.com dashboard URL or ID Load
	Import via panel json
	Load Cancel

- e. Browse the downloaded Grafana dashboard file and click Load.
- 2. View the dashboard.

To view the dashboard, navigate to **Menu** > **Dashboard**. All the logs are visible below the metrics as shown:



Figure 72 : Grafana Logs Dashboard

6	c	Q Search or ju	imp to	🖾 ctri+k			+ ~ 🛛 🛈	» 🖏
⊟ Home → Dashboards	🖘 Thunder 🟠 📽			ed⊳ Add ∽		 Last 15 minutes 	~ @ @	
0.5 0 19:05 — packet_rate_MAGENT="TO — packet_rate_(AGENT="TO — packet_rate_(AGENT="TO — packet_rate_IAGENT="TO	19:10 A", APPNAME="THUNDER", HOSTNAME="3cf8ø39c- A", APPNAME="THUNDER", HOSTNAME="3cf8ø39c- A", APPNAME="THUNDER", HOSTNAME="3cf8ø39c- A", APPNAME="THUNDER", HOSTNAME="3cf8ø39c- a dermame="thunder", HOSTNAME="thunder", HOSTNAME", HOSTNAME="thunde	19:15 9b46-47fe-a96; 9b46-47fe-a96; 9b46-47fe-a96; 9b46-47fe-a96;	25 0 7-98t 55 7-98t 55 7-98t 55 7-089 45	19:05 I.errors.count/ADENT="Tr I.errors.count/ADENT="Tr I.errors.count/ADENT="Tr I.errors.count/ADENT="Tr	DA", APPNAME **T) DA", APPNAME **T) DA", APPNAME **T) DA", APPNAME **T)	19:10 FUNDER", HOSTNAME="3 FUNDER", HOSTNAME="3 FUNDER", HOSTNAME="3 # NOTED" MOSTNAME="3	19:15 icf8e39c-9b46-4; icf8e39c-9b46-4; icf8e39c-9b46-4; icf8e39c-9b46-4;	7fe-a967- 7fe-a967- 7fe-a967- 7fe-a967-
Logs O								
TIMESTAMP	MESSAGE	AGENT	APPNAME	HOSTNAME	IP	JOBID	LOG_TYPE	PARTI
2023-11-02T13:39:46	Nov 02 2023 13:36:02 Critical [SYSTEM]:F	TOA	THUNDER	3cf8e39c-9b46	10.64.25.181	20231102133946	Syslog	SHAR
2023-11-02T13:39:46	Nov 02 2023 13:36:07 Info [SYSTEM]:Loca.	ТОА	THUNDER	3cf8e39c-9b46	10.64.25.181	20231102133946	Syslog	SHAR
2023-11-02T13:39:46	Nov 02 2023 13:36:07 Notice [SYSTEM]:A	тоа	THUNDER	3cf8e39c-9b46	10.64.25.181	20231102133946	Syslog	SHAR
2023-11-02T13:39:46	Nov 02 2023 13:36:09 Critical [SYSTEM]:F	TOA	THUNDER	3cf8e39c-9b46	10.64.25.181	20231102133946	Syslog	SHAR
2023-11-02T13:39:46	Nov 02 2023 13:36:10 Notice [SYSTEM]:S	. TOA	THUNDER	3cf8e39c-9b46	10.64.25.181	20231102133946	Syslog	SHAR
2023-11-02T13:39:46	Nov 02 2023 13:36:11 Info [SYSTEM]:Local.	ТОА	THUNDER	3cf8e39c-9b46	10.64.25.181	20231102133946	Syslog	SHAR
2023-11-02T13:39:46	Nov 02 2023 13:36:11 Notice [SYSTEM]:A	TOA	THUNDER	3cf8e39c-9b46	10.64.25.181	20231102133946	Syslog	SHAR

Splunk

To monitor the configured logs in Splunk Enterprise, perform the following steps:

- 1. Log in to Splunk Enterprise.
- 2. Create an HTTP Event Collector (HEC) for the logs.

To use HEC, you need to configure at least one token. The token is used to authenticate and send data to Splunk.

- a. Navigate to Settings > Data Inputs > HTTP Event Collector.
- b. Click New Token.
- c. Enter the token name as 'collectorLog' and click Next.
- d. Select a source type as _json from the **Source Type** drop-down list box.
- e. Click Create a new index.
- f. Enter the name as 'thunder_log' and select the **Index Data Type** as **Events**. Click **Save**.

The index will be add to the **Available Items** list box.

- g. Choose the newly created index ('thunder_logs') from the **Available Items** list box.
- h. Click Review to review the settings and then click Submit.



The token is created.

i. Store the token generated for later reference.

NOTE: If you have already created this token then ensure that the dashboard xml file contains the same index name.

3. Navigate to Apps > Search & Reporting > Dashboard and then click Create New Dashboard.

Figure 73 : Create New Dashboard

Create New D	ashboard		
Dashboard Title	Thunder-Logs		
	thunder-logs		/ Edit ID
Description	Dashboard for	thunder logs	
Permissions	🔒 Private	•	

- 4. On the **Create New Dashboard** form, perform the following steps:
 - a. Enter a name for the dashboard in the **Dashboard Title** field.
 - b. Enter description in the **Description** field.



- c. Select the appropriate permissions from **Permissions** drop-down menu.
- d. Under How do you want to build your dashboard?, select Classic Dashboard framework, and click Create.
- 5. On the newly created dashboard, first click **Edit** and then click **Source**.

Figure 74 : Logs Dashboard	
Thunder-Logs	Edit Export
Dashboard for thunder logs	

- 6. Copy the XML code from the <u>dashboard template file</u> and paste it in the editor.
- 7. Edit the following tags:
 - label It must be same as the Dashboard Title entered in Step-4a.
 - description It must be same as the dashboard Description entered in <u>Step-</u>
 <u>4b</u>.
 - query The index mentioned in this tag must be same as the one in use.
- 8. Click Save.
- 9. Verify if the logs are displayed.

Figure 75 : Thunder-Logs Dashboard

ylek:	rterprise	Apps =								🖗 Administra 🕈 🚦 Mari	uga t Satings	Anny -	ng+ Q1	
													No.	A Reporting
Thund Institute April In Product	ler-Logs for hunder log	Approve # Tree		lura				-		Newpox All	Pattan		ta tu	•
		•		448 - 144 - 144										
Testing														
						5	5,02	23						
Logitatio														
ALENT 1	1	HOSTMANE I	**	,080 1	101,7195	AMESPACE	AMPENDEN 1	PRORTY 1	796.1	Sec. 1				
	14,403	1470742-5479-4488-5684- 78,98545408	10.04.25.748	30.007-072-0	trig	1+04001+ (s+440)	34403	NUM	1000700001003	3.1 11 202 80:10 42 Mellow	Drotteri deve	en 30 12 (n. marc)	Conel.	
-	14,403	Satter of the sale-sale- factorization	10.04.21.140	2010/10/10	to be	140808- 34980	34482	NULL	10.001000011000	3.1 0 202 80.10.00 Relies 10.00.22.100 Tax Deep agenced	Control + and Section 10 antip	PE section for an ed in 10.	er "scittus" (
ч.	14,400	1410147-5475-468-568- 7839545468	10.04.25.145	2010/14/14	trig	1+04001+ (s+680)	(444)	2476	10007000011003	3.4 31 2023 40:10:42 3454 #West).	(14970PC Geo)	advertication of	scoreful (an	
10	14,403	Satter at the sale-sale- facetorials	10.04.25.140	2010/10/210	tria	10808- 34803	34483	Notice	10.007000011000	3.5 0 202 80.70.02 Rolling 10.01.22.745 has been aprecia	(prompt) + and benine ID amig	PE session for un ed in 14.	er "scillas" (
10	1404030	1400147-5475-468-548- 78,90545408	10.04.25.145	2018/14/14	tyring .	540400- 344400	(444)	NULL	1000700001003	34 10 363 40 10 40 Mellow	CHINE Sea	an 30 14 15 mm c	Crowd.	
10	14,403	1470742-5475-488-568- Factoriae	10.04.25.140	30.001012.00	trig	140808- 34680	34403	NUM	10.007000011001	34 0 303 80.10 K Molec	(1977)PÅ dess	en 30 10 in mar d	losed.	
10	THURSDAY	1470747-5475-668-5484	10.04.25.145	2010/10/210	today	1-04001-	34403	No. of Concession, Name	1000700011003	ALC: NO REPORT OF	DOTES A MARK	At section for up	er famor de	

GCP Logs Explorer

To monitor the configured logs in GCP Logs Explorer, perform the following steps:

164

External Thunder Observability Agent (TOA)



- 1. View Thunder Logs
- 2. Configure Query Parameters
- 3. Create an Alert
- 4. Add Logs to Dashboard

View Thunder Logs

- 1. Open Google Cloud Console and select the project you want to work with.
- 2. In the navigation menu, select **Logging**, and then navigate to **Logs Explorer**.

The Log Explorer interface will be displayed. This interface allows you to retrieve logs, parse and analyze log data, and refine query parameters.

3. Click Log name drop down menu on the toolbar, select the log name thunder (default name of the log generated), and click Apply as shown in .

Logs Explorer - Log name

External Thunder Observability Agent (TOA)



Log name 💌	Severity 👻	SI	how qu
elect log names		Clear	×
	ames		
OTHER			
Thunder			
projects/a10n	etworks-public-	396315/logs/	Thu
	etworks-public- RING API DenEventv1 etworks-public-	396315/logs/	mon
 projects/a10n CLOUD MONITO ViolationOp projects/a10n 	etworks-public- RING API DenEventv1 etworks-public-	396315/logs/ 396315/logs/	/mon
projects/a10n CLOUD MONITO ViolationOp projects/a10n	etworks-public- RING API DenEventv1 etworks-public-	396315/logs/ 396315/logs/	/mon

The log is displayed in the **Query results** pane as shown in Figure 76.



Figure 76 : Logs Explorer Interface

Logs Explorer 🔀 Refine sc	cope 1view	CƏ Share link 🛛 🗢 Learn
Query Recent (37) Saved (0)	Suggested (0) Library	🔟 Clear query 😨 Save Stream logs Run query
© Last 1 hour Q Search all fields		Resource thunder Severity Solver Show query
Cog fields 😑 Histogram		id Create metric A Create alert O Jump to now More actions ▼
Log fields <>	Query results 224 log entries	Find in results Correlate by 👻 Units Correlate by
	SEVERITY TIME IST 🔹 🛧 💌 SUMMARY 🥒 Edit 🤍 Summ	ary fields 🕒 Wrap lines
PROJECT ID	Q [*] 47% of results are similar and can be hidden. Hide similar er	ttries Preview X
a10networks-public-396315 22	24 > 1 2023-12-12 16:00:30.469 Dec 12 2023 10:26:55 Notice	[SYSTEM]:Session ID 311 is now closed.
RESOURCE TYPE	> i 2023-12-12 16:00:30.469 Dec 12 2023 10:26:53 Notice	[SYSTEM]:A aXAPI session for user "admin" from 172.23.20.98 has bee-
Global 22	24 2023-12-12 16:00:30.469 Dec 12 2023 10:26:53 Into	[SYSTEM]:Local authentication successful (user: admin).
SEVERITY	2023-12-12 16:00:56.737 Dec 12 2023 10:26:39 Warning	[ACOS]:Duplicated IP 10:0:3:25 MAC 00:50:56:A4:5E:55 from Port 2 VLA-
i Notice 17	75 > 1 2023-12-12 16:00:56.737 Dec 12 2023 10:26:09 Warning	[ACOS]:Duplicated IP 10.0.3.23 MAC 00:50:56:A4:8E:73 from Port 1 VL-
U Warning 3	> ! 2023-12-12 16:00:56.737 Dec 12 2023 10:26:09 Warning	[ACOS]:Duplicated IP 10.0.2.6 MAC 00:50:56:A4:5F:E5 from Port 2 VLA-
. Wanning S	> ! 2023-12-12 16:04:27.766 Dec 12 2023 10:30:39 Warning	[ACOS]:Duplicated IP 10.0.3.23 MAC 00:50:56:A4:8E:73 from Port 1 VL-
i Info 1	17 > !! 2023-12-12 16:04:27.766 Dec 12 2023 10:30:39 Warning	[ACOS]:Duplicated IP 10.0.2.6 MAC 00:50:56:A4:5F:E5 from Port 2 VLA-
	> (!) 2023-12-12 16:04:27.766 Dec 12 2023 10:30:09 Warning	[ACOS]:Duplicated IP 10.0.3.23 MAC 00:50:56:A4:8E:73 from Port 1 VL-
	> ! 2023-12-12 16:04:27.766 Dec 12 2023 10:30:09 Warning	[ACOS]:Duplicated IP 10.0.2.6 MAC 00:50:56:A4:5F:E5 from Port 2 VLA-
	Shewing loss for lost 1 hour from 12(12/22, 2:10) bit to 12(12/22, 4)	[ACUS]:Duplicated IP 18.8.2.6 MAC 88:58:56:A4:5F:E5 From Port 2 VLA-

Additionally, you can select **Histogram** in the **Results** toolbar to provide a visual representation of log data distribution. This also helps in the identification of patterns, anomalies, and trends within the log data.

Figure 77 : Logs Explorer - Histogram

**	Query Recent (4) Save	ed (0)	Suggested (2) Library			Clear quer	y 🗈 Save Stream logs Run query
E	() Last 15 minutes Q Searc	h all fields			Re	source Thunder	Severity Show query
	1 logName="projects/a10netwo	rks-publi	c-396315/logs/Thunder*				
il.							
Ξ	Log fields 🛛 💙 Histogra	am			Create met	ric 🏨 Create alert	() Jump to now More actions 👻
≡q,	Log fields	<>	Histogram				© ⊕ ≎
÷			<				
	PROJECT ID	100	Mar 14, 2:19:15 PM	2:3	5PM	2:30 PM	Mar 14, 2:34:30 PM
	RESOURCE TYPE	109	Query results 109 log entries		Se Find in res	sults	Correlate by 👻 🛃 Download
ത	Global	109	SEVERITY TIME IST - 1	SUMMARY 🖉 Edit 💽 Summar	fields 🕒 Wrap lines		
69	∧ SEVERITY		> i 2024-03-14 14:34:02.176	Mar 14 2024 09:02:59 Notice	[SYSTEM]:Session ID 21 is now	closed.	
	i Notice	53	> 2024-03-14 14:34:02.176	Mar 14 2024 09:02:59 Notice	[SYSTEM]: A aXAPI session for u	user "admin" from 10.6	4.25.188 has been opened. Session ID-
	(!) Warning	46	i 2024-03-14 14:34:02.176	Mar 14 2024 09:02:59 Notice	[SYSTEM]:A aXAPI session for u	user "admin" from 10.6	4.25.188 has been opened. Ses:
ľ	i Info	10	> (i) 2024-03-14 14:34:02.176	Mar 14 2024 09:02:59 Notice	[SYSTEM]:Session ID 20 is now	closed.	
			> ii 2024-03-14 14:34:02.176	Mar 14 2024 09:02:59 Notice	[SYSTEM]:A aXAPI session for u	iser "admin" from 10.6	4.25.188 has been opened. Session ID

Configure Query Parameters

A query in **Logs Explorer** specifies parameters and conditions to retrieve specific log data, thereby aiding log analysis and troubleshooting. Following are the commonly configured query parameters:

• The **Severity** option in the **Log fields** pane allows you to filter log entries based on their severity level, enabling you to quickly identify and prioritize issues. The



severity levels include DEBUG, INFO, WARNING, ERROR, and CRITICAL, representing varying degrees of importance and urgency.

- The **Time-range selector** in the **Query** pane allows you to specify the time range for which you want to view the log data. You can select predefined time ranges (e.g., last hour, last 24 hours) or define a custom time range by specifying the start time and end time.
- The **Search-text box** in the **Query** pane allows you to perform text-based searches within logs, making it easier to find log entries containing specific information or events of interest. For example, entering **error** in the text box helps pinpoint logs related to errors in the application.

After configuring the query parameters, click **Save** in the **Query** pane to save the query i.e., store the specific set of parameters and conditions for future purpose.

Create an Alert

- 1. On the Results toolbar, click Create alert.
- 2. In the Alert details pane, enter the **policy name**, select an option from the **severity level** drop-down menu, and click **Next**.
- 3. In the **Choose logs to include in the alert** pane, check the configured query and log results by clicking **Preview logs**.

The query for the thunder logs (created in the previous steps by specifying various filtering parameters) will be displayed in this pane. You can also edit the query in this pane. After editing the query, you can check the results by clicking **Preview logs**.

- 4. Click Next.
- 5. In the Set notification frequency and autoclose duration pane, select values for **Time Between Notification** and the **Incident autoclose duration**, and click **Next**.
- 6. In the Who should be notified pane, you can select one or more notification channels for the alert. If you already have an SMS or email notification channel configured, then you can select it from the list. Else, click Manage notification channels and add a notification channel. For more information, see <u>Create and Manage Notification channels</u>.
- 7. Click Save.

168

External Thunder Observability Agent (TOA)





Your log-based alert policy is configured.

For more information, see <u>Configure log-based alerts</u>.

Add Logs to Dashboard

- 1. In the navigation panel, select **Monitoring**, and then click **Dashboards**.
- 2. On the Dashboards Overview page, click Create Dashboard.
- 3. Click the dashboard's title, enter a name for the dashboard, and click **Save**.
- 4. Click + Add Widget and select Logs as shown in Figure 78.



Figure 78 : Dashboard - Add Widget - Log



The Configure Widget page will be displayed.

- 5. On the **Configure Widget** page, click **Log name** drop-down menu, select the log name as **Thunder**, and click **Apply**.
- 6. Click **Severity** drop-down menu , select the severity from the list, and click **Apply**.

The queried log will be added to the dashboard as shown in the following image.

170



.



Figure 79 : GCP Dashboard with Logs

Thunc	ler-Logs		
Sho	w query		
Def	sity 🖉 Eit	ter Search all fields and values	0
EVERITY	TIMESTAMP	SUMMARY	
	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:57 Notice	[SYSTEM]:A aXAPI session for user 'admin' from 172.23.20.98 has been opened. Session ID assigned is 326.
•	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:57 Notice	[SYSTEM]:A aXAPI session for user "admin" from 172.23.20.98 has been opened. Session ID assigned is 325.
	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:57 Notice	[SYSTEM]:A aXAPI session for user 'admin' from 172.23.20.98 has been opened. Session ID assigned is 324.
> ()	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:57 Notice	[SYSTEM]:A aXAPI session for user 'admin' from 172.23.20.98 has been opened. Session ID assigned is 323.
	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:57 Notice	[SYSTEM]:A aXAPI session for user 'admin' from 172.23.20.98 has been opened. Session ID assigned is 322.
	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:57 Notice	[SYSTEM]:A aXAPI session for user "admin" from 172.23.20.98 has been opened. Session ID assigned is 321.
•	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:57 Notice	[SYSTEM]:A aXAPI session for user 'admin' from 172.23.20.98 has been opened. Session ID assigned is 320.
	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:56 Notice	[SYSTEM]:A aXAPI session for user 'admin' from 172.23.20.98 has been opened. Session ID assigned is 319.
	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:56 Info	[SYSTEM]:Local authentication successful (user: admin).
	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:56 Notice	[SYSTEM]:A aXAPI session for user 'admin' from 172.23.20.98 has been opened. Session ID assigned is 318.
> •	2023-12-12 16:00:30.469 UTC+5:30	Dec 12 2023 10:26:56 Notice	[SYSTEM]:A aXAPI session for user "admin" from 172.23.20.98 has been opened. Session ID assigned is 317.

OCI Logs Search

To monitor the configured logs in Oracle Cloud Infrastructure (OCI) Logs Search, perform the following steps:

- 1. View Thunder Logs
- 2. Filter and Search Logs

View Thunder Logs

- 1. Log in to the OCI console, open the navigation menu and click **Observability & Management**.
- 2. Under Logging, click Log Group, and select your log group.
- 3. On the Log Group page, under Resources, click Logs.
- 4. From the list, select the log name for which the logs are being collected i.e., the logs for which OCID is mentioned in the <u>config.json</u> file for publishing purpose.

The log data is displayed in the **Explore Log** area as show in Figure 80.



Figure 80 : OCI - Viewing log details

	Status: 🔶 Active									
Resources	Explore Log									
Contract on	Sort	Filter by time	Start Date	End Date						
Exprore Log	Newest	Custom	C Feb 5, 2024 7:03:31 AM	🗎 Feb 5, 2024 8:00:31 AM 📋	Actions *					
Mencs	100		✓ Number of log events per mit	nute						
	120 60 0 Feb 05, 07.05 Feb 00	. 67.10 Feb 05, 07.15 Feb 05, 07.20 I	reb 05, 07.25 Feb 05, 07.30 Feb 05, 0	17.35 Feb 05, 07.45 Feb 05, 07.45 Feb 05, 07.50 Feb 05, 01	1.55 Feb 05, 08:00					
	datetime	type	×	data.message	×					
	Feb 5, 2024, 08:00:07 UTC	Syslog		(1d1:1336bcda2-8585-4025-97a1-6b3e8926b27c1;1tme1:12024-	02-05T08.0 V					
	Feb 5, 2024, 08:00:07 UTC	Syslog		("id":"7651d4ee-e084-45db.bebb-a7f9a6bc3b74","time":"2024.0	12.05T08:00 🗸					
	Feb 5, 2024, 08 00 07 UTC	Syslog		("id":"358x00b5-09b5-4085-9436-d751879973da","time"."2024-02	05T08.00.0					
	Feb 5, 2024, 08 00 07 UTC	Syslog		("id":"74739dd5-ddb8-4543-84c4-17917ecb06b","time"."2024-0	12-05T08.00 V					
	Feb 5, 2024, 08:00:07 UTC	Syslog		("id":"e0e79d95-d1a0-4cc8-8ef5-4839de07bde2","tme":"2024-0	12-05T08:00 V					
	Feb 5, 2024, 08:00:07 UTC	Syslog		("id":"446a8821-71d7-4e8b-8305-042555eb24db","time":"2024-0	2-05T08.00 V					
	Feb 5, 2024, 08:00:07 UTC	Syslog		("id":"a5x29ctb-5ax3-4989-8876-bc93a7779276","time":"2024-0	2-05T08:00 🗸					

The **Explore Log** area provides various fields to help analyze log data effectively. Some of the common fields are:

- **Sort** This field allows you to arrange the log entries based on their timestamp (newest or oldest entries).
- Filter by Time This field allows you to narrow down log data for a specified time period. You can select a predetermined time range from the list or select Custom to specify a date range using Start Date and End Date fields.
- Actions This drop-down menu has the following options:
 - **Wrap-lines** This option ensures that all content remains visible without the need for horizontal scrolling.
 - **Explore with Log Search** This option allows you to view the log data on the **Search** page directly that provides various search and filtering options.

For more information on options, see <u>Search and Filter logs</u>.

Filter and Search Logs

The **Explore with Log Search** option under **Actions** drop-down menu provides powerful features such as advanced search syntax, aggregation functions, and visualization tools that help you perform complex analysis and investigation related to log data. By clicking this option, the log data can be viewed on the **Search** page as shown in Figure 81.

172



Figure 81 : OCI - Log Search

aire line						Failert ince in search			5E 6	how Advanced Mo
Total associa Maria						Coultable Coult The	w armhunder.inter.min			
ter by time	Start Cale			1	Date					
	U 9665.2	124 / 30/30 AM	C	912	0 5, 2024 0.15 50 A		0		Mo	e search options /
lect regions to search										
/5 Viest (Phoenix)										
								Renet Search	Save search Create conved	Q Search
										Adapted
piore Visualize										OFF
					 Notice of log 	events per minute				
188										
18							la a	de la secolo	dia	
128 128 14							h	dhata.	altu.,	
198 108 08 8		Feb 04, 87 10	Feb 10.	07.38			1011.2.4		altu.	Feb 06, 08 10
198 199 00 1 4m 20,07:00	Bank 5, 2014, 47 48	Fell OL ET 15	Feb 10.	07.34		.11	1	ىيىيىلە	altu.,	Feb 00, 10 10
198 109 00 1 Hels 90, 07:00 Uring \$500 kg event(a) fram.Volum,	Feb 5, 2024, 07.0	Peo 01, 81 15 158 UTC to Mare, Feb 5, 2004, 88 15 58 UTC	Auto 10.	07 JA			Feit, 270	<u>dinata.</u>	altu.,	Fes 06, 58 15 Actions +
102 103 10 10 10 10 10 10 10 10 10 10 10 10 10	Peo 5, 2024, 07 04	An OL ET 15 ISS UTC to Mor, Petr'S, 2004, 08 15 S0 UTC des MCSSAGE X	Aut 10, data JOBIO	07 JA	<	- 11	Feit 210	Analog_1175		Fea 06, 08 19 Actions •
100 100 00 1 1 Ann 30, 07 00 100 kg event(s) from Mon, draw 4, 2024, 30 1001 UTC	Feb 5, 2004, 17 10	Per 05, ET 15 SISUITO to Mar, Feb 5, 2004, 81 15 SISUITO Ana MESSAGE X Part of 2004 05 11:05 Hours, jacObijDu	Feb 20, 6499-20000 200402500-1301	07.38	< des.PRODUTY Viewing	- 11	Pecili 21 de Adat MOSTMARE X Soficilio dolt effectificationado	Ave 10, 1012		Actions +
100 105 00 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Feb 5, 2024, 87 81	Pec 04, 811 10 ISSUIC No Mon, Pach 5, 2004, 08 15 58 U/CC Man MCSAACE X Pack 05 200 No 110 Strategy, Doctor 50 No.469 E Pack 05 200 No 110 Strategy, Doctor 50 No.469 E Pack 05 200 No 110 Strategy Control 100 No.469 E	Feb 20, data J0000 2004020500-1301	07 38	K Gen.FRORTY Varing	- 11	Adda 12 da Adda 12 da Adda 20 da 4% add "Albandidad	An it is it	(00.479005 5.4025	Actions +
188 18 19 19 19 19 19 19 19 19 19 19	Feb 5, 2024, 87 88	Feb 05, 81 10 SSE UTC Is New, Feb 5, 2004, NB 15:58 UTC deax MESIADE March 2014 RE 10:02 Names price 2014 RE 10:02 Names Fill Not 2014 Names Fill Names Fill Names Fill Names Fill Names	Feb 20 64/64-20200 2024/22/800-1001 2024/22/800-1001	07 Ja	x destriction	- 11	An IN CENTRE Adda IN CENTRE In Color-ON-A	An IL LOS		Autors v
198 198 199 199 199 199 199 199 199 199	Feb 5, 2024, 87 00	Feb 03, 8110 559 U/C to Mee, Feb 5, 2004, 88 15580 U/C des 9455002 X Feb 02 200 8 01100 deems () possel 41 02 2004 00 0200 Feb 0429 0 5 hourthy 11/2 000 1000 Feb 0429 0 5 hourthy 11/2 000 1000 Feb 0429 0 6 hourthy 11/2 000 1000 1000 1000 1000 1000 1000	Auto 20, Auto 2000 2019-025509-020 2019-025509-020	07.38	x assumed and a	- Luu I I	An IO (TAUE) X	An LOG_TIPE	C OSATINUE TRADER	Actions +
100 101 102 103 104 105 105 105 105 105 105 105 105	Feb 5, 2024, 87 00	An U.S. 21 10 Sec. VIC 10 10 Sec. VIC 10 10 Sec. VIC 10 10 Anno PEERAGE X Anno 10 2014 11 10 2014 11 X Anno 10 2014 11 10 2014 11 X Anno 10 2014 11 10 2014 11 X Anno 10 2014 11 Anno 10	Fee 81, 6499-J0800 200-020800-001 200-020800-001 200-020800-001	C? 38	< desuffection Varing Into Notion	- 11	An AD COMME X An AD COMME X Jordice 266 4°N ADT Allowshold Jordice 266 4°N ADT Allowshold Jordice 266 4°N ADT Allowshold	An IL ALLA An IL ALLA Demy Demy Dyney		Actions v
102 102 103 104 105 105 105 105 105 105 105 105	Feb 5, 2024, 87 (8	Fact SE ET 11 Fact SE ET 11 Fact SE ET 12 Fact SE Fac	Aut 20, Aut 2000 200-022500-001 200-022500-001 200-022500-001	07.88	 des_FRONTY Varing Into Notos 	- 11	And 216 An USANE X And 266 Point Strendon And 266 Point Strendon And 266 Point Strendon	An IL A IL A		Autors x
100 101 102 103 103 104 105 105 105 105 105 105 105 105	Feb 5, 2024, 87 87	An ULE IF ID All SSE UPG Set Mit 75 ADD ALL All STATE Set Mit 75 ADD ALL And Mit 75 ADD ALL All ALL And ALL All ALL And ALL All ALL And ALL All ALL All ALL All ALL	Ass 20. ass.2080 209422800-001 209422800-001 209422800-001	07.08	Karang Info Notoe	- 11	An INCOMMENT An INCOMMENT And AN AND AN AND AN AND AND AN And AND	An IK SHE	C GRAMMAR NUCCH NUCCH NUCCH	An OL BESS Actions • X
100 100 100 100 100 100 100 100	Feb 5, 2024, 87 87	Ans (K, ET 10) SM UPC for Max, Single AB 11550 UPC Ans Antibiotic X Ans Antibiotic Antib	An II. An II. II.A. III. II.A. III.A. II.A. II.A. II.A. II. II.A. III.A. II.A. III.A. III.A. II.A. II.A. II.A. II.A. III.A. IIII.A. III.A. III.A. III.A. IIII.A. IIII.A. IIII.A. IIII.A. IIIIIIII	07 AB	 des.PROBITY Varing Mo Notes 	- 1 - • • • •	An IOTALE X	An LOL TYPE T	c on.ATTANE TUADER TUADER TUADER TUADER TUADER	Address +
143 143 144 145 145 145 145 145 145 145	Feb 5, 2004, 07 0	An ULE IF ID SHE UPD IN UNA A SIZE IN ITS SUUTO Annotation III and IIII and IIIIIIIIII	An IX An JOBO 20402050-001 20402050-001 20402050-001 20402050-001	07.04	K des/Hookty Varing Pfs Notes	- 11	An INCOMMENT AND	An isk to be An isk to be former former former former former		Autors - Actions - X

The Search page is typically divided into two main parts, the filter section and the display section.

- Filter Section It allows you to specify criteria to narrow down the search results. Some of the common features in this section are:
 - Custom Filters This feature allows you to create custom filters based on attributes such as log source, severity level, specific keywords or phrases within log messages, or custom metadata fields associated with the log entries.

Start typing in the text box to automatically display filtering options, along with the operators. For example, entering a displays filters starting with that letter. Select a filter from the list and use an operator to create a filter. For example, data.JOBID= '<jobid_value>'.

- Filter by Time This field allows you to narrow down log data for a specified time period. You can select a predetermined time range from the list or select Custom to specify a date range using Start Date and End Date fields.
- Select Regions to Search This filter allows you to filter logs based on specific regions. You can choose to include or exclude certain regions from the search scope based on your monitoring requirements.
- **Save search** This option allows you to save the above-mentioned filter settings for future purpose.
- Display Section This section has the Explore and Visualize tabs that present log



data in accordance to the above-mentioned filters and search criteria.

- On the Explore tab, a graph displays the number of log events per minute. This tab displays a maximum of 100 search results. Some other commonly used options under this tab are:
 - Manage log fields under Actions menu allows you to add fields to the Explore tab. The new fields are appended to the right of the first three default fields (datetime, type, data.message). You can add a maximum of six log fields using this option.

Figure 82 : Manage log fields

Filter fields		×
 datetime 		
type		
+ data.AGENT		
+ data.APPNAME		
+ data.HOSTNAME		
🕂 data.IP		
(+) data.JOBID		
(+) data.LOG_TYPE		
(+) data.MESSAGE		
(+) data PARTITION		
data.PRIORITY	Ν	
(+) id	13	
oracle.compartmentid		
oracle.loggroupid		
oracle.logid		
(+) oracle.tenantid		
(+) source		
+ specversion		
+ subject		
(+) time		

••••



- **Export log data (JSON)** under **Actions** menu allows you to export log data to a JSON file that can be downloaded to your local storage.
- JSON tab (available after expanding any entry in the data.message field) allows you to view the log data fields and values, as well as collapse and expand nodes.
- **Before & After** tab (available after expanding any entry in the **data.message** field) provides context around a selected log entry by displaying logs that occur immediately before and after it.

For more information on options in the **Explore** tab, see <u>Viewing Search</u> <u>Results</u>.

 The Visualize tab allows you to visualize the log data as a chart to identify patterns, trends, and anomalies more effectively. For more information on options in this tab, see <u>Visualizing Search Results</u>.



Figure 83 : OCI - Visualize Logs

Troubleshoot

TOA Logging

TOA creates the agent.log file at the default directory /var/log/thunderobservability-agent path when the TOA cron is executed. This file contains the readable system logs from Thunder devices as per the configured frequency. It is used to troubleshoot any encountered issue.



The log file format contains logging level information. The logging level can be changed to DEBUG level for troubleshooting purpose.

A sample log file is shown below:

```
2023-05-29 06:47:01,831 - INFO - ###### TOA ###### All Rights Reserved
@A10 Networks Inc ##### TOA #####
2023-05-29 06:48:02,063 - INFO - Job No
                                                : 20230529104802.
2023-05-29 06:48:02,063 - INFO - Job Start Time : 2023-05-29
10:48:02.006315+00:00.
2023-05-29 06:48:02,064 - WARNING - WARNING
                                                : No log or metric is
enabled. To enable [metric, log set to [1]] in config.json.
2023-05-29 06:48:02,064 - INFO - Job Execution
                                                : 0.058001 seconds.
2023-05-29 06:48:02,064 - INFO - Job End Time
                                                : 2023-05-29
10:48:02.064316+00:00
2023-05-29 06:48:02,064 - INFO - Documentation
                                                : www.al0networks.com or
https://github.com/a10networks/thunder-observability-agent.
2023-05-29 06:48:02,064 - INFO - ##### TOA ###### All Rights Reserved
@A10 Networks Inc ##### TOA #####
2023-05-29 06:49:01,301 - INFO - Job No
                                                : 20230529104901.
2023-05-29 06:49:01,301 - INFO - Job Start Time : 2023-05-29
10:49:01.244429+00:00.
2023-05-29 06:49:01,301 - WARNING - WARNING
                                                : No log or metric is
enabled. To enable [metric, log set to [1]] in config.json.
2023-05-29 06:49:01,301 - INFO - Job Execution
                                                : 0.057536 seconds.
2023-05-29 06:49:01,302 - INFO - Job End Time
                                                : 2023-05-29
10:49:01.301965+00:00
2023-05-29 06:49:01,302 - INFO - Documentation
                                                : www.al0networks.com or
https://github.com/a10networks/thunder-observability-agent.
2023-05-29 06:49:01,302 - INFO - ##### TOA ###### All Rights Reserved
@A10 Networks Inc ##### TOA #####
2023-05-29 06:50:01,533 - INFO - Job No
                                                : 20230529105001.
2023-05-29 06:50:01,533 - INFO - Job Start Time : 2023-05-29
10:50:01.477199+00:00.
2023-05-29 06:50:01,533 - ERROR - Error
                                                 : File not found or
corrupt. Please check file and path: [/usr/toaenv/thunder-observability-
agent/config.json]. Application config not found. Please check [config
path] in main.properties.
```

176



2023-05-29 06:50:01,533 - INFO - Job Execution : 0.056567 seconds. 2023-05-29 06:50:01,533 - INFO - Job End Time : 2023-05-29 10:50:01.533766+00:00 2023-05-29 06:50:01,533 - INFO - Documentation : www.alOnetworks.com or https://github.com/a10networks/thunder-observability-agent. 2023-05-29 06:54:01,462 - INFO - ##### TOA ###### All Rights Reserved @A10 Networks Inc ##### TOA ##### 2023-05-29 06:55:01,738 - INFO - Job No : 20230529105501. 2023-05-29 06:55:01,738 - INFO - Job Start Time : 2023-05-29 10:55:01.680906+00:00. 2023-05-29 06:55:01,738 - INFO - Log Provider : VMWARE. 2023-05-29 06:55:01,738 - INFO - Log : VMWARE LOG. 2023-05-29 06:55:01,738 - INFO - Metric Provider : VMWARE. 2023-05-29 06:55:01,739 - INFO - Metric : VMWARE METRIC. 2023-05-29 06:55:01,739 - INFO - No of Thunders : 1 ['10.64.25.13']. 2023-05-29 06:55:01,739 - WARNING - WARNING : No partitions found for thunder [], setting to default 'SHARED'. Multiple L3V partition can be configured as comma separated for example if we have partition 'P1' and 'P2' then we can define as ['partition' : ' Shared, P1, P2'] upto 20 partitions. 2023-05-29 06:55:01,739 - INFO - No of Partitions : 10.64.25.13 [Count: 1] [shared]. 2023-05-29 06:55:02,068 - INFO - Published Log : 10.64.25.13 THUNDER-SHARED [Count: 3]. 2023-05-29 06:55:02,112 - INFO - Published Metric : 10.64.25.13 THUNDER [Count: 2] [{'Memory Usage Percentage': 63.4, 'Disk Usage Percentage': 36}1. 2023-05-29 06:55:02,151 - INFO - Published Metric : 10.64.25.13 THUNDER-SHARED [Count: 10] [{'Server Errors Count': 0, 'Total Session Count': 0, 'SSL Errors Count': 0, 'Server Down Percentage': 0, 'CPU Usage Percentage (Data)': 0.0, 'Total New Connection (Sec)': 0, 'Interface Down Count (Data)': 0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'Throughput Rate (Global/BPS)': 0}]. 2023-05-29 06:55:02,161 - INFO - Job Execution : 0.480912 seconds. 2023-05-29 06:55:02,161 - INFO - Job End Time : 2023-05-29 10:55:02.161818+00:00 2023-05-29 06:55:02,162 - INFO - Documentation : www.alOnetworks.com or

177



https://github.com/a10networks/thunder-observability-agent. 2023-05-29 07:00:02,016 - INFO - ##### TOA ###### All Rights Reserved @A10 Networks Inc ##### TOA ##### 2023-05-29 07:01:01,258 - INFO - Job No : 20230529110101. 2023-05-29 07:01:01,258 - INFO - Job Start Time : 2023-05-29 11:01:01.201609+00:00. 2023-05-29 07:01:01,259 - INFO - Log Provider : VMWARE. 2023-05-29 07:01:01,259 - INFO - Log : VMWARE LOG. 2023-05-29 07:01:01,259 - INFO - Metric Provider : VMWARE. 2023-05-29 07:01:01,259 - INFO - Metric : VMWARE METRIC. 2023-05-29 07:01:01,259 - INFO - No of Thunders : 1 ['10.64.25.13']. 2023-05-29 07:01:01,259 - INFO - No of Partitions : 10.64.25.13 [Count: 2] [{'shared', 'p1'}]. 2023-05-29 07:01:01,592 - INFO - Published Log : 10.64.25.13 THUNDER-P1 [No Data Found]. 2023-05-29 07:01:01,664 - INFO - Published Metric : 10.64.25.13 THUNDER-P1 [Count: 10] [{'Total Session Count': 0, 'Server Errors Count': 0, 'Server Down Percentage': 0, 'SSL Errors Count': 0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'Interface Down Count (Data)': 1, 'Throughput Rate (Global/BPS)': 0, 'Total New Connection (Sec)': 0, 'CPU Usage Percentage (Data) ': 0.0}]. 2023-05-29 07:01:01,673 - INFO - Published Metric : 10.64.25.13 THUNDER-SHARED [Count: 10] [{'SSL Errors Count': 0, 'Server Down Percentage': 0, 'Server Errors Count': 0, 'Total Session Count': 0, 'Server Down Count': 0, 'Interface Down Count (Data)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Transactions Rate (Sec)': 0, 'Throughput Rate (Global/BPS)': 0, 'Total New Connection (Sec) ': 0}]. 2023-05-29 07:01:01,682 - INFO - Published Metric : 10.64.25.13 THUNDER [Count: 2] [{'Disk Usage Percentage': 36, 'Memory Usage Percentage': 66.8}]. 2023-05-29 07:01:01,701 - INFO - Published Log : 10.64.25.13 THUNDER-SHARED [Count: 10]. 2023-05-29 07:01:01,712 - INFO - Job Execution : 0.51061 seconds. 2023-05-29 07:01:01,712 - INFO - Job End Time : 2023-05-29 11:01:01.712219+00:00 2023-05-29 07:01:01,712 - INFO - Documentation : www.al0networks.com or https://github.com/a10networks/thunder-observability-agent.

178



2023-05-29 05:57:02,553 - INFO - ###### TOA ###### All Rights Reserved @A10 Networks Inc ##### TOA ##### 2023-05-29 05:58:01,786 - INFO - Job No : 20230529095801. 2023-05-29 05:58:01,787 - INFO - Job Start Time : 2023-05-29 09:58:01.730452+00:00. 2023-05-29 05:58:01,787 - INFO - Log Provider : VMWARE. 2023-05-29 05:58:01,787 - INFO - Log : VMWARE LOG. 2023-05-29 05:58:01,787 - INFO - Metric Provider : VMWARE. 2023-05-29 05:58:01,787 - INFO - Metric : VMWARE METRIC. 2023-05-29 05:58:01,787 - INFO - No of Thunders : 1 ['10.64.25.13']. 2023-05-29 05:58:01,787 - INFO - No of Partitions : 10.64.25.13 [Count: 1] [*]. 2023-05-29 05:58:02,848 - INFO - Published Metric : 10.64.25.13 THUNDER [Count: 2] [{'Disk Usage Percentage': 35, 'Memory Usage Percentage': 61.6}]. 2023-05-29 05:58:02,923 - INFO - Published Metric : 10.64.25.13 THUNDER-P1 [Count: 10] [{'Total Session Count': 0, 'Server Errors Count': 0, 'SSL Errors Count': 0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'Total New Connection (Sec)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Server Down Percentage': 0, 'Interface Down Count (Data)': 1, 'Throughput Rate (Global/BPS)': 0}]. 2023-05-29 05:58:03,210 - INFO - Published Log : 10.64.25.13 THUNDER-P5 [No Data Found]. 2023-05-29 05:58:03,216 - INFO - Published Log : 10.64.25.13 THUNDER-P8 [No Data Found]. 2023-05-29 05:58:03,252 - INFO - Published Metric : 10.64.25.13 THUNDER-P7 [Count: 10] [{'Server Errors Count': 0, 'Total Session Count': 0, 'SSL Errors Count': 0, 'Server Down Percentage': 0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'Throughput Rate (Global/BPS)': 0, 'Total New Connection (Sec)': 0, 'Interface Down Count (Data)': 0, 'CPU Usage Percentage (Data)': 0.0}]. 2023-05-29 05:58:03,288 - INFO - Published Log : 10.64.25.13 THUNDER-SHARED [Count: 6]. 2023-05-29 05:58:03,379 - INFO - Published Log : 10.64.25.13 THUNDER-P19 [No Data Found]. 2023-05-29 05:58:03,381 - INFO - Published Metric : 10.64.25.13 THUNDER-P15 [Count: 10] [{'Total Session Count': 0, 'Server Errors Count': 0,

179

'Server Down Percentage': 0, 'SSL Errors Count': 0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Interface Down Count (Data)': 0, 'Throughput Rate (Global/BPS)': 0, 'Total New Connection (Sec)': 0}]. 2023-05-29 05:58:03,422 - INFO - Published Metric : 10.64.25.13 THUNDER-P2 [Count: 10] [{'Server Down Count': 1, 'Server Down Percentage': 100.0, 'Server Errors Count': 0, 'Total Session Count': 0, 'SSL Errors Count': 0, 'Interface Down Count (Data)': 0, 'Transactions Rate (Sec)': 0, 'Total New Connection (Sec)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Throughput Rate (Global/BPS)': 0}]. 2023-05-29 05:58:03,502 - INFO - Published Metric : 10.64.25.13 THUNDER-P11 [Count: 10] [{'SSL Errors Count': 0, 'Total Session Count': 0, 'Server Errors Count': 0, 'Transactions Rate (Sec)': 0, 'Server Down Percentage': 0, 'Server Down Count': 0, 'Total New Connection (Sec)': 0, 'Interface Down Count (Data)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Throughput Rate (Global/BPS)': 0}]. 2023-05-29 05:58:03,547 - INFO - Published Metric : 10.64.25.13 THUNDER-P4 [Count: 10] [{'Total Session Count': 0, 'SSL Errors Count': 0, 'Server Errors Count': 0, 'Total New Connection (Sec)': 0, 'Server Down Percentage': 0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'Throughput Rate (Global/BPS)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Interface Down Count (Data)': 0}]. 2023-05-29 05:58:03,608 - INFO - Published Log : 10.64.25.13 THUNDER-P11 [No Data Found]. 2023-05-29 05:58:03,626 - INFO - Published Log : 10.64.25.13 THUNDER-P1 [No Data Found]. 2023-05-29 05:58:03,620 - INFO - Published Log : 10.64.25.13 THUNDER-P16 [No Data Found]. 2023-05-29 05:58:03,674 - INFO - Published Metric : 10.64.25.13 THUNDER-P5 [Count: 10] [{'SSL Errors Count': 0, 'Server Errors Count': 0, 'Total Session Count': 0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'Server Down Percentage': 0, 'Total New Connection (Sec)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Interface Down Count (Data)': 0, 'Throughput Rate (Global/BPS)': 0}]. 2023-05-29 05:58:03,740 - INFO - Published Metric : 10.64.25.13 THUNDER-P17 [Count: 10] [{'Server Errors Count': 0, 'SSL Errors Count': 0, 'Total Session Count': 0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'Server Down Percentage': 0, 'Throughput Rate (Global/BPS)': 0, 'CPU Usage

Feedbac


Percentage (Data)': 0.0, 'Total New Connection (Sec)': 0, 'Interface Down Count (Data)': 0}]. 2023-05-29 05:58:03,809 - INFO - Published Metric : 10.64.25.13 THUNDER-P8 [Count: 10] [{'Server Down Percentage': 0, 'Server Errors Count': 0, 'SSL Errors Count': 0, 'Total Session Count': 0, 'Transactions Rate (Sec)': 0, 'Server Down Count': 0, 'Total New Connection (Sec)': 0, 'CPU Usage Percentage (Data) ': 0.0, 'Throughput Rate (Global/BPS) ': 0, 'Interface Down Count (Data) ': 0}]. 2023-05-29 05:58:04,082 - INFO - Published Log : 10.64.25.13 THUNDER-P9 [No Data Found]. 2023-05-29 05:58:04,248 - INFO - Published Metric : 10.64.25.13 THUNDER-P19 [Count: 10] [{'Total Session Count': 0, 'Server Down Count': 0, 'Server Errors Count': 0, 'SSL Errors Count': 0, 'Transactions Rate (Sec)': 0, 'Server Down Percentage': 0, 'CPU Usage Percentage (Data)': 0.0, 'Throughput Rate (Global/BPS)': 0, 'Interface Down Count (Data)': 0, 'Total New Connection (Sec)': 0}]. 2023-05-29 05:58:04,250 - INFO - Published Metric : 10.64.25.13 THUNDER-P9 [Count: 10] [{'Server Down Count': 3, 'Server Down Percentage': 100.0, 'Server Errors Count': 0, 'Total Session Count': 0, 'SSL Errors Count': 0, 'Total New Connection (Sec)': 0, 'Transactions Rate (Sec)': 0, 'Interface Down Count (Data)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Throughput Rate (Global/BPS)': 0}]. 2023-05-29 05:58:04,258 - INFO - Published Metric : 10.64.25.13 THUNDER-P3 [Count: 10] [{'Server Down Percentage': 100.0, 'Server Down Count': 2, 'Transactions Rate (Sec)': 0, 'SSL Errors Count': 0, 'Total Session Count': 0, 'Server Errors Count': 0, 'Total New Connection (Sec)': 0, 'Throughput Rate (Global/BPS)': 0, 'CPU Usage Percentage (Data)': 0.0, 'Interface Down Count (Data)': 0}]. 2023-05-29 05:58:04,260 - INFO - Published Log : 10.64.25.13 THUNDER-P12 [No Data Found]. 2023-05-29 05:58:04,267 - INFO - Published Metric : 10.64.25.13 THUNDER-P13 [Count: 10] [{'Total Session Count': 0, 'Server Down Percentage': 0, 'Server Errors Count': 0, 'SSL Errors Count': 0, 'Transactions Rate (Sec)': 0, 'Server Down Count': 0, 'Total New Connection (Sec)': 0, 'CPU Usage Percentage (Data) ': 0.0, 'Interface Down Count (Data) ': 0, 'Throughput Rate (Global/BPS)': 0}]. 2023-05-29 05:58:04,308 - INFO - Published Log : 10.64.25.13 THUNDER-P4 [No Data Found].

181



2023-05-29 05:58:04,377 - INFO - Published Log : 10.64.25.13 THUNDER-P18 [No Data Found]. 2023-05-29 05:58:04,396 - INFO - Published Metric : 10.64.25.13 THUNDER-SHARED [Count: 10] [{'Server Errors Count': 0, 'Total Session Count': 0, 'SSL Errors Count': 0, 'Transactions Rate (Sec)': 0, 'Server Down Count': 0, 'CPU Usage Percentage (Data)': 0.0, 'Throughput Rate (Global/BPS)': 0, 'Server Down Percentage': 0, 'Total New Connection (Sec)': 0, 'Interface Down Count (Data) ': 0}]. 2023-05-29 05:58:04,468 - INFO - Published Log : 10.64.25.13 THUNDER-P7 [No Data Found]. 2023-05-29 05:58:04,469 - INFO - Published Metric : 10.64.25.13 THUNDER-P16 [Count: 10] [{'Server Errors Count': 0, 'SSL Errors Count': 0, 'Total Session Count': 0, 'Server Down Percentage': 0, 'Server Down Count': 0, 'CPU Usage Percentage (Data)': 0.0, 'Throughput Rate (Global/BPS)': 0, 'Interface Down Count (Data)': 0, 'Total New Connection (Sec)': 0, 'Transactions Rate (Sec)': 0}]. 2023-05-29 05:58:04,472 - INFO - Published Log : 10.64.25.13 THUNDER-P2 [No Data Found]. 2023-05-29 05:58:04,474 - INFO - Published Log : 10.64.25.13 THUNDER-P15 [No Data Found]. 2023-05-29 05:58:04,599 - INFO - Published Log : 10.64.25.13 THUNDER-P17 [No Data Found]. 2023-05-29 05:58:04,607 - INFO - Published Log : 10.64.25.13 THUNDER-P10 [No Data Found]. 2023-05-29 05:58:04,624 - INFO - Published Metric : 10.64.25.13 THUNDER-P10 [Count: 10] [{'Transactions Rate (Sec)': 0, 'SSL Errors Count': 0, 'Total Session Count': 0, 'Server Down Percentage': 0, 'Server Down Count': 0, 'Server Errors Count': 0, 'Total New Connection (Sec)': 0, 'Interface Down Count (Data)': 0, 'Throughput Rate (Global/BPS)': 0, 'CPU Usage Percentage (Data) ': 0.0}]. 2023-05-29 05:58:04,742 - INFO - Published Log : 10.64.25.13 THUNDER-P14 [No Data Found]. 2023-05-29 05:58:04,844 - INFO - Published Metric : 10.64.25.13 THUNDER-P18 [Count: 10] [{'SSL Errors Count': 0, 'Total Session Count': 0, 'Server Errors Count': 0, 'Server Down Count': 0, 'Server Down Percentage': 0, 'Throughput Rate (Global/BPS)': 0, 'Interface Down Count (Data)': 0, 'Transactions Rate (Sec)': 0, 'Total New Connection (Sec)': 0, 'CPU Usage Percentage (Data)': 0.0}].

182



2023-05-29 05:58:04,910 - INFO - Published Log : 10.64.25.13 THUNDER-P3 [No Data Found]. 2023-05-29 05:58:04,919 - INFO - Published Log : 10.64.25.13 THUNDER-P13 [No Data Found]. 2023-05-29 05:58:04,922 - INFO - Published Metric : 10.64.25.13 THUNDER-P14 [Count: 10] [{'Server Down Percentage': 0, 'Total New Connection (Sec)': 0, 'Transactions Rate (Sec)': 0, 'Total Session Count': 0, 'Server Errors Count': 0, 'SSL Errors Count': 0, 'Server Down Count': 0, 'CPU Usage Percentage (Data)': 0.0, 'Interface Down Count (Data)': 0, 'Throughput Rate (Global/BPS)': 0}]. 2023-05-29 05:58:04,942 - INFO - Published Log : 10.64.25.13 THUNDER-P6 [No Data Found]. 2023-05-29 05:58:04,978 - INFO - Published Metric : 10.64.25.13 THUNDER-P12 [Count: 10] [{'Server Errors Count': 0, 'Server Down Percentage': 0, 'Total Session Count': 0, 'SSL Errors Count': 0, 'CPU Usage Percentage (Data)': 0.0, 'Server Down Count': 0, 'Transactions Rate (Sec)': 0, 'Interface Down Count (Data)': 0, 'Throughput Rate (Global/BPS)': 0, 'Total New Connection (Sec)': 0}]. 2023-05-29 05:58:05,002 - INFO - Published Metric : 10.64.25.13 THUNDER-P6 [Count: 10] [{'Throughput Rate (Global/BPS)': 0, 'Server Down Percentage': 0, 'Server Errors Count': 0, 'Total New Connection (Sec)': 0, 'SSL Errors Count': 0, 'Transactions Rate (Sec)': 0, 'Total Session Count': 0, 'Server Down Count': 0, 'CPU Usage Percentage (Data)': 0.0, 'Interface Down Count (Data)': 0}]. 2023-05-29 05:58:05,013 - INFO - Job Execution : 3.282716 seconds. 2023-05-29 05:58:05,013 - INFO - Job End Time : 2023-05-29 09:58:05.013168+00:00 2023-05-29 05:58:05,013 - INFO - Documentation : www.al0networks.com or https://github.com/a10networks/thunder-observability-agent.

Examples

The following topics are covered:

<u>AWS</u>	
Azure	
VMware	

Elasticsearch	196
Prometheus	200
<u>Splunk</u>	204
Google Console Platform	208
Oracle Cloud Infrastructure	211

AWS

Borse Inc. is a regular A10 client. The company has purchased multiple instances of Thunder and deployed it on their AWS platform. The instances are configured as an ADC load balancer for their gaming applications named [Pokers]. The company is receiving timeout/failover complaints from their online customers especially when there is a high traffic load caused by an event, festival, or holiday. The client wants a standard way to monitor using AWS CloudWatch and to get an email alert when the aggregated CPU usage crosses 75% so that proper action can be taken on time.

Parameter	Description
Linux Environment IP	10.22.32.51
Hardware	2 GB RAM, 1 CPU, 4 GB memory
Thunder details	
Thunder instance	1
Thunder IP	10.22.32.01
User Name	Online_Pokers_TH
Password	Thunder@Borse@3201
Resource_Name	North_Virginia_Online_Pokers_TH
resource_id	i-1234567890abcdef0
Thunder instance	2
Thunder IP	10.22.32.02
User Name	Online_Pokers_TH2
Password	Thunder@Borse@3202
Resource_Name	North_Virginia_Online_Pokers_TH2

The client has shared the following environment details:

184



Parameter	Description
resource_id	i-1234567890uvwxyz0
Thunder instance	3
User Name	Online_Pokers_TH3
Password	Thunder@Borse@3203
Resource_Name	vth-auto-scale-group
AWS Monitoring details	
aws_log_group_name	Thunder
aws_access_key_id	AKIA5VU3P46JEI7OQU54
aws_secret_access_key	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
region	us-east-1

Solution

A10 Support team will propose to install **Thunder Observability Agent (TOA)** for collecting and publishing logs on AWS CloudWatch:

1. Install Python if the recommended version is not already installed on the shared Linux instance IP 10.22.32.51.

```
apt update
apt-get install python3.10
apt install python3-pip
apt install cron
apt install rsyslog
```

2. Install TOA.

```
pip install virtualenv
virtualenv venv
source venv/bin/activate
pip install thunder_observability_agent
```

- 3. Configure TOA.
 - a. Configure Thunder details in the /root/.thunder/credentials file depending on the type of Thunder instance:



Single instance

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Pokers_TH",
    "password": "Thunder@Borse@3201",
    "resource_id": "i-1234567890abcdef0",
    "active_partitions": "shared"
}]
```

Multiple instances

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online Pokers TH",
    "password": "Thunder@Borse@3201",
    "resource id": i-1234567890abcdef0,
   "active partitions": "shared"
 },
  {
    "ip": "10.22.32.02",
    "username": "Online Pokers TH2",
    "password": "Thunder@Borse@3202",
    "resource id": "i-1234567890uvwxyz0",
    "active partitions": "P1"
 }]
```

Auto Scale instance

{

"autoscale" : 1,



```
"provider" : "AWS",
"thunders": [{
    "username": "Online_Pokers_TH",
    "password": "Thunder@Borse@3201",
    "resource_id": "vth-auto-scale-group-name",
    "active_partitions": "shared"
}]
```

b. Update the following configurations in the /root/.aws/config file.

```
[default]
    region = us-east-1
    output = json
```

c. Update the AWS credentials in the /root/.aws/credentials file.

```
[default]
    aws_access_key_id = AKIA5VU3P46JEI70QU54
    aws_secret_access_key = HsrNj8yZn2sLeHLfxTbG/r6yZCeTGdy3YojRKBg0
```

d. Update AWS configuration properties in the /usr/toaenv/thunderobservability-agent/config.json file.



```
"aws provider": 1,
"aws metric": 1,
"aws cpu": 1,
"aws memory": 1,
"aws disk": 1,
"aws throughput": 1,
"aws interfaces": 1,
"aws cps": 1,
"aws tps": 1,
"aws server down count": 1,
"aws server down percentage": 1,
"aws ssl cert": 1,
"aws server error": 1,
"aws sessions": 1,
"aws packet rate": 1,
"aws_packet_drop": 1,
"aws log": 1,
"aws_log_group_name": "Thunder",
```

4. Check logs at /var/log/thunder-observability-agent/agent.log.

For more examples, see GitHub.

Azure

ABC Corp. is a regular A10 client. The company has purchased multiple instances of Thunder and deployed it on their Azure platform. The instances are configured as an ADC load balancer for their gaming applications named [Football]. The company is receiving timeout/failover complaints from their online customers especially when there is a high traffic load caused by an event, festival, or holiday. The client wants a standard way to monitor using Azure Application Insight and Log Analytics Workspace and to get an email alert when the aggregated CPU usage crosses 75% so that proper action can be taken on time.

The client has shared the following environment details:



.

Parameter	Description	
Linux Environment IP	10.22.32.51	
Hardware	2 GB RAM, 1 CPU, 4 GB memory	
Thunder details	·	
Thunder instance	1	
Thunder IP	10.22.32.01	
User Name	Online_Football_TH	
Password	Thunder@ABC@3201	
Resource_Name	North_Virginia_Online_Football_TH	
resource_id	i-1234567890lmnopq0	
Thunder instance	2	
Thunder IP	10.22.32.02	
User Name	Online_Football_TH2	
Password	Thunder@ABC@3202	
Resource_Name	North_Virginia_Online_Football_TH2	
resource_id	i-1234567890rstuvw0	
Thunder instance	3	
User Name	Online_Football_TH3	
Password	Thunder@ABC@3203	
Resource_Name	vth-auto-scale-group	
Azure Monitoring details		
azure_location	southcentralus	
azure_metric_resource_id	/subscriptions/07d34b9b-61e3-475a-abbc- 006b16812a3e/ resourceGroups/vth-rg6/ providers/microsoft.insights/ components/vth-vmss-app-insights	
azure_workspace_primary_key	tewPsyMYkdGOThRjEyI************************************	



Parameter	Description
azure_client_id	10724xxx-xxx-xxxx-xxxx-xxxx2c14726d
azure_secret_id	9-xxx~jlxxxEVyxxxxHNxxxOwv_xxxxZLxxxTM
azure_tenant_id	91d27xxx-xxxx-xxxx-xxxxf81fcb2f
azure_log_workspace_id	dcfd7xxx-xxxx-xxxx-xxxxf81fc991

Solution

A10 Support team will propose to install **Thunder Observability Agent (TOA)** for collecting and publishing logs on the Azure platform:

1. Install Python if the recommended version is not already installed on the shared Linux instance IP 10.22.32.51.

```
apt update
apt-get install python3.10
apt install python3-pip
apt install cron
apt install rsyslog
```

2. Install TOA.

```
pip install virtualenv
virtualenv venv
source venv/bin/activate
pip install thunder_observability_agent
```

3. Configure TOA.

a. Configure Thunder details in the /root/.thunder/credentials file depending upon the type of Thunder instance:

Single instance

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Football_TH",
    "password": "Thunder@ABC@3201",
```



```
"resource_id": "i-1234567890lmnopq0"
"active_partitions": "shared"
}]
```

Multiple instances

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Football_TH",
    "password": "Thunder@ABC@3201",
    "resource id": "i-12345678901mnopq0"
    "active partitions": "shared"
 },
  {
    "ip": "10.22.32.02",
    "username": "Online Football TH2",
    "password": "Thunder@ABC@3202",
    "resource id": "i-1234567890rstuvw0"
    "active partitions": "shared"
 }]
```

Auto Scale (VMSS) instance

```
{
    "autoscale" : 1,
    "provider" : "Azure",
    "thunders": [{
         "username": "Online_Football_TH3",
         "password": "Thunder@ABC@3203",
         "resource_id": "vth-auto-scale-group"
         "active_partitions": "shared"
    }]
}
```

b. Update the Azure credentials in the /root/.azure/credentials file.



c. Update Azure configuration properties in the /usr/toaenv/thunderobservability-agent/config.json file.

```
"azure provider": 1,
  "azure metric": 1,
  "azure metric resource id": "/subscriptions/07d34b9b-61e3-475a-
abbc-006b16812a3e/resourceGroups/vth-
rg6/providers/microsoft.insights/components/vth-vmss-app-insights",
  "azure cpu": 1,
  "azure memory": 1,
  "azure disk": 1,
  "azure throughput": 1,
  "azure interfaces": 1,
 "azure cps": 1,
 "azure tps": 1,
  "azure server down count": 1,
  "azure server down percentage": 1,
  "azure ssl cert": 1,
  "azure server error": 1,
  "azure sessions": 1,
  "azure packet rate": 1,
  "azure packet drop": 1,
  "azure log": 1,
  "azure_log_workspace_id": "dcfd7xxx-xxxx-xxxx-xxxx+81fc991"
```

4. Check logs at /var/log/thunder-observability-agent/agent.log.

For more examples, see GitHub.

192



VMware

LMQ Corp. is a regular A10 client. The company has purchased multiple instances of Thunder and deployed it on their VMware platform. The instances are configured as an ADC load balancer for their gaming applications named [Baseball]. The company is receiving timeout/failover complaints from their online customers especially when there is a high traffic load caused by an event, festival, or holiday. The client wants a standard way to monitor using VMware vRealize Operations Manager (vROps) and vRealize Log Insight (vRLI) and to get an email alert when the aggregated CPU usage crosses 75% so that proper action can be taken on time.

Parameter	Description
Linux Environment IP	10.22.32.51
Hardware	2 GB RAM, 1 CPU, 4 GB memory
Thunder details	
Thunder instance	1
Thunder IP	10.22.32.01
User Name	Online_Baseball_TH
Password	Thunder@LMQ@3201
Resource_Name	North_Virginia_Online_Baseball_TH
resource_id	i-1234567890lmnopq0
Thunder instance	2
Thunder IP	10.22.32.02
User Name	Online_Baseball_TH2
Password	Thunder@LMQ@3202
Resource_Name	North_Virginia_Online_Baseball_TH2
resource_id	i-1234567890rstuvw0
VMware Monitoring details	
vRLI IP	10.22.32.11
vROPs IP	10.22.32.12

The client has shared the following environment details:



Parameter	Description
vROPs User Name	vROPsAdmin
vROPs Password	vROPs@Borse@3212

Solution

A10 Support team will propose to install **Thunder Observability Agent (TOA)** for collecting and publishing logs on the VMware platform:

1. Install Python if the recommended version is not already installed on the shared Linux instance IP 10.22.32.51.

```
apt update
apt-get install python3.10
apt install python3-pip
apt install cron
apt install rsyslog
```

2. Install TOA.

```
pip install virtualenv
virtualenv venv
source venv/bin/activate
pip install thunder observability agent
```

- 3. Configure TOA.
 - a. Configure Thunder details in the /root/.thunder/credentials file depending upon the type of Thunder instance:

Single instance

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Baseball_TH",
    "password": "Thunder@LMQ@3201",
    "resource_id": "i-1234567890lmnopq0",
    "active_partitions": "shared"
}]
```



Multiple instances

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Baseball_TH",
    "password": "Thunder@LMQ@3201",
    "resource_id": "i-1234567890lmnopq0",
    "active_partitions": "shared"
    },
    {
        "ip": "10.22.32.02",
        "username": "Online_Baseball_TH2",
        "password": "Thunder@LMQ@3202",
        "resource_id": "i-1234567890rstuvw0",
        "active_partitions": "shared"
    }]
```

b. Update the VMware credentials in the /root/.vmware/credentials file.

vmware_vrops_username = vROPsAdmin
vmware_vrops_password = vROPs@Borse@3212

c. Update VMware configuration properties in the /usr/toaenv/thunderobservability-agent/config.json file.



```
"vmware provider": 1,
"vmware metric": 1,
"vmware vrops host": "10.22.32.12",
"vmware cpu": 1,
"vmware memory": 1,
"vmware disk": 1,
"vmware throughput": 1,
"vmware interfaces": 1,
"vmware cps": 1,
"vmware tps": 1,
"vmware server down count": 1,
"vmware server down percentage": 1,
"vmware ssl cert": 1,
"vmware server error": 1,
"vmware sessions": 1,
"vmware packet rate": 1,
"vmware packet drop": 1,
"vmware log": 1,
"vmware vrli host": "10.22.32.11"
```

4. Check logs at /var/log/thunder-observability-agent/agent.log.

For more examples, see GitHub.

Elasticsearch

LMQ Corp. is a regular A10 client. The company has purchased multiple instances of Thunder and deployed it on their Elasticsearch platform. The instances are configured as an ADC load balancer for their gaming applications named [Baseball]. The company is receiving timeout/failover complaints from their online customers especially when there is a high traffic load caused by an event, festival, or holiday. The client wants a standard way to monitor using Elasticsearch and Kibana.

The client has shared the following environment details:



Parameter	Description
Linux Environment IP	10.22.32.51
Hardware	2 GB RAM, 1 CPU, 4 GB memory
Thunder details	
Thunder instance	1
Thunder IP	10.22.32.01
User Name	Online_Baseball_TH
Password	Thunder@LMQ@3201
Resource_Name	North_Virginia_Online_Baseball_ TH
resource_id	i-1234567890lmnopq0
Thunder instance	2
Thunder IP	10.22.32.02
User Name	Online_Baseball_TH2
Password	Thunder@LMQ@3202
Resource_Name	North_Virginia_Online_Baseball_ TH2
resource_id	i-1234567890rstuvw0
Elasticsearch Monitoring details	
Elasticsearch User Name	Elastic
Elasticsearch Password	BWFAN28DOPy8jpxh8tJQ
Elasticsearch Host	127.0.0.0:9200

Solution

A10 Support team will propose to install **Thunder Observability Agent (TOA)** for collecting and publishing logs on Elasticsearch:

1. Install Python if the recommended version is not already installed on the shared Linux instance IP 10.22.32.51.



```
apt update
apt-get install python3.10
apt install python3-pip
apt install cron
apt install rsyslog
```

2. Install TOA.

```
pip install virtualenv
virtualenv venv
source venv/bin/activate
pip install thunder_observability_agent
```

- 3. Configure TOA.
 - a. Configure Thunder details in the /root/.thunder/credentials file depending on the type of Thunder instance:

Single instance

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Baseball_TH",
    "password": "Thunder@LMQ@3201",
    "resource_id": "i-12345678901mnopq0",
    "active_partitions": "shared"
}]
```

Multiple instances

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Baseball_TH",
    "password": "Thunder@LMQ@3201",
```



```
"resource_id": i-1234567890lmnopq0,
"active_partitions": "shared"
},
{
    "ip": "10.22.32.02",
    "username": "Online_Baseball_TH2",
    "password": "Thunder@LMQ@3202",
    "resource_id": "i-1234567890rstuvw0",
    "active_partitions": "shared"
}]
```

b. Update the Elasticsearch credentials in the /root/.elasticsearch/credentials file.

```
username = elastic
password = BWFAN28DOPy8jpxh8tJQ
```

c. Update Elasticsearch configuration properties in the /usr/toaenv/thunderobservability-agent/config.json file.



```
"es provider": 1,
"es_metric": 1,
"es host": "127.0.0.0:9200",
"es cpu": 1,
"es memory": 1,
"es disk": 1,
"es throughput": 1,
"es interfaces": 1,
"es cps": 1,
"es tps": 1,
"es server down count": 1,
"es server down percentage": 1,
"es ssl cert": 1,
"es server error": 1,
"es sessions": 1,
"es packet_rate": 1,
"es packet drop": 1,
"es log": 1
 }
```

4. Check logs at /var/log/thunder-observability-agent/agent.log.

For more examples, see GitHub.

Prometheus

LMQ Corp. is a regular A10 client. The company has purchased multiple instances of Thunder and deployed it on their Prometheus platform. The instances are configured as an ADC load balancer for their gaming applications named [Baseball]. The company is receiving timeout/failover complaints from their online customers especially when there is a high traffic load caused by an event, festival, or holiday. The client wants a standard way to monitor using Prometheus, Pushgateway & Grafana.

The client has shared the following environment details:

Parameter	Description
Linux Environment IP	10.22.32.51



Parameter	Description	
Hardware	2 GB RAM, 1 CPU, 4 GB memory	
Thunder details		
Thunder instance	1	
Thunder IP	10.22.32.01	
User Name	Online_Baseball_TH	
Password	Thunder@LMQ@3201	
Resource_Name	North_Virginia_Online_Baseball_ TH	
resource_id	i-1234567890lmnopq0	
Thunder instance	2	
Thunder IP	10.22.32.02	
User Name	Online_Baseball_TH2	
Password	Thunder@LMQ@3202	
Resource_Name	North_Virginia_Online_Baseball_ TH2	
resource_id	i-1234567890rstuvw0	
Prometheus Monitoring details		
Pushgateway User Name	admin	
Pushgateway Password	pushgateway123	
Pushgateway Host	127.0.0.0:9091	

Solution

A10 Support team will propose to install **Thunder Observability Agent (TOA)** for collecting and publishing logs on Prometheus:

1. Install Python if the recommended version is not already installed on the shared Linux instance IP 10.22.32.51.



```
apt update
apt-get install python3.10
apt install python3-pip
apt install cron
apt install rsyslog
```

2. Install TOA.

```
pip install virtualenv
virtualenv venv
source venv/bin/activate
pip install thunder_observability_agent
```

- 3. Configure TOA.
 - a. Configure Thunder details in the /root/.thunder/credentials file depending on the type of Thunder instance:

Single instance

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Baseball_TH",
    "password": "Thunder@LMQ@3201",
    "resource_id": "i-12345678901mnopq0",
    "active_partitions": "shared"
}]
```

Multiple instances

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Baseball_TH",
    "password": "Thunder@LMQ@3201",
```



```
"resource_id": i-1234567890lmnopq0,
"active_partitions": "shared"
},
{
    "ip": "10.22.32.02",
    "username": "Online_Baseball_TH2",
    "password": "Thunder@LMQ@3202",
    "resource_id": "i-1234567890rstuvw0",
    "active_partitions": "shared"
}]
```

b. Update the Pushgateway credentials in the /root/.pushgateway/credentials file.

```
username = admin
password = pushgateway123
```

c. Update Pushgateway configuration properties in the /usr/toaenv/thunderobservability-agent/config.json file.



"pushgateway provider": 1, "pushgateway metric": 1, "pushgateway host": "127.0.0.0:9091", "pushgateway cpu": 1, "pushgateway memory": 1, "pushgateway disk": 1, "pushgateway throughput": 1, "pushgateway interfaces": 1, "pushgateway cps": 1, "pushgateway tps": 1, "pushgateway server down count": 1, "pushgateway server down percentage": 1, "pushgateway ssl cert": 1, "pushgateway server error": 1, "pushgateway sessions": 1, "pushgateway_packet_rate": 1, "pushgateway packet drop": 1, "pushgateway log": 1

4. Check logs at /var/log/thunder-observability-agent/agent.log.

For more examples, see GitHub.

Splunk

XYZ Corp. is a regular A10 client. The company has purchased multiple instances of Thunder and deployed it on their Splunk platform. The instances are configured as an ADC load balancer for their gaming applications named [Volleyball]. The company is receiving timeout/failover complaints from their online customers especially when there is a high traffic load caused by an event, festival, or holiday. The client wants a standard way to monitor using the Splunk dashboard and Splunk Analytics. Additionally, the client also wants to get an email alert when the aggregated CPU usage exceeds 75% to take an appropriate action.

The client has shared the following environment details:



Parameter	Description	
Linux Environment IP	10.22.32.51	
Hardware	2 GB RAM, 1 CPU, 4 GB memory	
Thunder details		
Thunder instance	1	
Thunder IP	10.22.32.01	
User Name	Online_Volleyball_TH	
Password	Thunder@XYZ@3201	
Resource_Name	North_Virginia_Online_Vol- leyball_TH	
resource_id	i-1234567890lmnopq0	
Thunder instance	2	
Thunder IP	10.22.32.02	
User Name	Online_Volleyball_TH2	
Password	Thunder@XYZ@3202	
Resource_Name	North_Virginia_Online_Vol- leyball_TH2	
resource_id	i-1234567890rstuvw0	
Splunk Monitoring details		
token_log	2acdaae2a-0497-4a6c-97b7- b155e79aa88	
token_metric	f944d49-37f4-4bba-a2f6-df0cd- be86fcbd	
splunk_host	127.0.0.0:8088	

Solution

A10 Support team will propose to install **Thunder Observability Agent (TOA)** for collecting and publishing logs on the Splunk platform:

1. Install Python if the recommended version is not already installed on the shared Linux instance IP 10.22.32.51.



```
apt update
apt-get install python3.10
apt install python3-pip
apt install cron
apt install rsyslog
```

2. Install TOA.

```
pip install virtualenv
virtualenv venv
source venv/bin/activate
pip install thunder_observability_agent
```

- 3. Configure TOA.
 - a. Configure Thunder details in the /root/.thunder/credentials file depending on the type of Thunder instance:

Single instance

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Volleyball_TH",
    "password": "Thunder@XYZ@3201",
    "resource_id": "i-1234567890lmnopq0",
    "active_partitions": "shared"
}]
```

Multiple instances

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Volleyball_TH",
    "password": "Thunder@XYZ@3201",
```



```
"resource_id": i-1234567890lmnopq0,
"active_partitions": "shared"
},
{
    "ip": "10.22.32.02",
    "username": "Online_Volleyball_TH2",
    "password": "Thunder@XYZ@3202",
    "resource_id": "i-1234567890rstuvw0",
    "active_partitions": "shared"
}]
```

b. Update the Splunk credentials in the /root/.splunk/credentials file.

```
token_log=2acdaae2a-0497-4a6c-97b7-b155e79aa88
token metric=f944d49-37f4-4bba-a2f6-df0cdbe86fcbd
```

c. Update Splunk configuration properties in the /usr/toaenv/thunderobservability-agent/config.json file.

```
"splunk provider": 1,
"splunk metric": 1,
"splunk cpu": 1,
"splunk memory": 1,
"splunk disk": 1,
"splunk throughput": 1,
"splunk interfaces": 1,
"splunk cps": 1,
"splunk tps": 1,
"splunk server down count": 1,
"splunk server down percentage": 1,
"splunk ssl cert": 1,
"splunk server error": 1,
"splunk sessions": 1,
"splunk packet rate": 1,
"splunk_packet_drop": 1,
"splunk log": 1,
"splunk host": "127.0.0.0:8088"
```



}

4. Check logs at /var/log/thunder-observability-agent/agent.log.

For more examples, see <u>GitHub</u>.

Google Console Platform

JKQ Corp. is a regular A10 client. The company has purchased multiple instances of Thunder and deployed it on their Google Cloud Platform (GCP). The instances are configured as an ADC load balancer for their gaming applications named [Baseball]. The company is receiving timeout/failover complaints from their online customers especially when there is a high traffic load caused by an event, festival, or holiday. The client wants a standard way to monitor using the GCP Logs Explorer and GCP Metrics Explorer. Additionally, the client also wants to get an email alert in case of error logs to take the appropriate action.

The client has shared the following environment details:

Parameter	Description			
Linux Environment IP	10.22.32.51			
Hardware	2 GB RAM, 1 CPU, 4 GB memory			
Thunder details				
Thunder instance	1			
Thunder IP	10.22.32.01			
User Name	Online_Baseball_TH			
Password	Thunder@JKQ@2828			
Resource_Name	North_Virginia_Online_Baseball_ TH			
resource_id	i-1234567890lmnopq0			
Thunder instance	2			
Thunder IP	10.22.32.02			
User Name	Online_Baseball_TH2			
Password	Thunder@JKQ@2829			
Resource_Name	North_Virginia_Online_Baseball_			



Parameter	Description
	TH2
resource_id	i-1234567890rstuvw0
GCP Monitoring details	
gcp_project_id	jkq-public-396315
gcp_service_key_path	C:/Users/Desktop/keyFolder/jkq- public-396315-db3b0f.json
gcp_log_name	thunder

Solution

A10 Support team will propose to install **Thunder Observability Agent (TOA)** for collecting and publishing logs on the GCP platform:

1. Install Python if the recommended version is not already installed on the shared Linux instance IP 10.22.32.51.

```
apt update
apt-get install python3.10
apt install python3-pip
apt install cron
apt install rsyslog
```

2. Install TOA.

```
pip install virtualenv
virtualenv venv
source venv/bin/activate
pip install thunder_observability_agent
```

- 3. Configure TOA.
 - a. Configure Thunder details in the /root/.thunder/credentials file depending on the type of Thunder instance:

Single instance

```
"autoscale" : 0,
"provider" : "XXXX",
```



```
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Baseball_TH",
    "password": "Thunder@JKQ@2828",
    "resource_id": "i-1234567890lmnopq0",
    "active_partitions": "shared"
}]
```

Multiple instances

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online Baseball TH",
    "password": "Thunder@JKQ@2828",
    "resource id": i-12345678901mnopq0,
    "active partitions": "shared"
 },
  {
    "ip": "10.22.32.02",
    "username": "Online Baseball TH2",
    "password": "Thunder@JKQ@2829",
    "resource id": "i-1234567890rstuvw0",
    "active partitions": "shared"
 }]
```

b. Update the GCP credentials in the /root/.gcp/credentials file.

```
gcp_project_id = jkq-public-396315
gcp_service_key_path = C:/Users/Desktop/keyFolder/jkq-public-
396315-db3b0f.json
```

c. Update GCP configuration properties in the /usr/toaenv/thunderobservability-agent/config.json file.



```
"gcp provider": 1,
"gcp metric": 1,
"gcp cpu": 1,
"gcp memory": 1,
"gcp disk": 1,
"gcp throughput": 1,
"gcp interfaces": 1,
"gcp cps": 1,
"gcp tps": 1,
"gcp server down count": 1,
"gcp server down percentage": 1,
"gcp ssl cert": 1,
"gcp server error": 1,
"gcp sessions": 1,
"gcp packet rate": 1,
"gcp packet drop": 1,
"gcp log": 1
```

4. Check logs at /var/log/thunder-observability-agent/agent.log.

For more examples, see <u>GitHub</u>.

Oracle Cloud Infrastructure

TUV Corp. is a regular A10 client. The company has purchased multiple instances of Thunder and deployed it on their OCI platform. The instances are configured as an ADC load balancer for their gaming applications named [Volleyball]. The company is receiving timeout/failover complaints from their online customers especially when there is a high traffic load caused by an event, festival, or holiday. The client wants a standard way to monitor using the OCI Logs and OCI Metrics Explorer. Additionally, the client also wants to get an email alert in case of error logs to take the appropriate action.

The client has shared the following environment details:

Parameter	Description
Linux Envir-	10.22.32.51
onment IP	

211





. . .

• • • •

Parameter	Description	1
Hardware	2 GB RAM, 1 CPU, 4 GB memory	1
Thunder det	ails	
Thunder instance	1	
Thunder IP	10.22.32.01	
User Name	Online_Volleyball_TH	
Password	Thunder@TUV@2828	
Resource_ Name	North_Virginia_Online_Volleyball_TH	
resource_ id	i-1234567890lmnopq0	
Thunder instance	2	-
Thunder IP	10.22.32.02	
User Name	Online_Volleyball_TH2	
Password	Thunder@TUV@2829	
Resource_ Name	North_Virginia_Online_Volleyball_TH2	
resource_ id	i-1234567890rstuvw0	
OCI Monitor	ing details	
oci_api_ key_path	C:/Users/Desktop/keyFolder/tuvconfig	
oci_com- partment_ id	ocid1 com- partment.oc1amlkjytrnpczhiafkgum6yjjhltv6frnn3wb6y3442fr5tc3j4kl	jhgfsq
oci_log_id	ocid1 log.oc1.phx.am- lkjytrnpczhiafkgfrfvuboum6yjjhltv6frnn3wb6y3442fr5tc3j4sq	

Solution

212



A10 Support team will propose to install **Thunder Observability Agent (TOA)** for collecting and publishing logs on the OCI platform:

1. Install Python if the recommended version is not already installed on the shared Linux instance IP 10.22.32.51.

```
apt update
apt-get install python3.10
apt install python3-pip
apt install cron
apt install rsyslog
```

2. Install TOA.

```
pip install virtualenv
virtualenv venv
source venv/bin/activate
pip install thunder_observability_agent
```

- 3. Configure TOA.
 - a. Configure Thunder details in the /root/.thunder/credentials file depending on the type of Thunder instance:

Single instance

```
"autoscale" : 0,
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Volleyball_TH",
    "password": "Thunder@TUV@2828",
    "resource_id": "i-12345678901mnopq0",
    "active_partitions": "shared"
}]
```

Multiple instances

```
"autoscale" : 0,
```



```
"provider" : "XXXX",
"thunders": [{
    "ip": "10.22.32.01",
    "username": "Online_Volleyball_TH",
    "password": "Thunder@TUV@2828",
    "resource_id": i-1234567890lmnopq0,
    "active_partitions": "shared"
    },
    {
        "ip": "10.22.32.02",
        "username": "Online_Volleyball_TH2",
        "password": "Thunder@TUV@2829",
        "resource_id": "i-1234567890rstuvw0",
        "active_partitions": "shared"
    }]
```

b. Update the OCI credentials in the /root/.oci/credentials file.

```
oci_api_key_path = C:/Users/Desktop/keyFolder/tuvconfig
```

c. Update OCI configuration properties in the /usr/toaenv/thunderobservability-agent/config.json file.

```
{
    "oci_provider": 1,
    "oci_compartment_id":
    "ocidl.compartment.ocl..amlkjytrnpczhiafkgum6yjjhltv6frnn3wb6y3442f
r5tc3j4kljhgfsq",
    "oci_cpu": 1,
    "oci_memory": 1,
    "oci_disk": 1,
    "oci_disk": 1,
    "oci_interfaces": 1,
    "oci_cps": 1,
    "oci_cps": 1,
    "oci_server_down_count": 1,
    "oci_server_down_percentage": 1,
```



```
"oci_ssl_cert": 1,
"oci_server_error": 1,
"oci_sessions": 1,
"oci_packet_rate": 1,
"oci_packet_drop": 1,
"oci_log": 1,
"oci_log_id":
"ocidl.log.ocl.phx.amlkjytrnpczhiafkgfrfvuboum6yjjhltv6frnn3wb6y344
2fr5tc3j4sq"
}
```

4. Check logs at /var/log/thunder-observability-agent/agent.log.

For more examples, see <u>GitHub</u>.

What's New

3.0.0

In this release, the TOA is enhanced to support the following enterprise solutions for data collection and analytics:

- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI)

2.0.0

In this release, the TOA is enhanced to support the following enterprise solutions for data collection and analytics:

- Elasticsearch Kibana
- Prometheus (Pushgateway) Grafana
- Splunk Splunk Analytics and Splunk Dashboard



1.0.0

This release has the following enhancements for Thunder[®] Application Delivery Controller (ADC):

- TOA supports Linux, CentOS, and Ubuntu platforms as a Python Plugin installation package and Docker containerization.
- TOA supports AWS, Azure, and VMware cloud providers.
- Single, multiple, and auto scale Thunder instances can be configured for TOA.
- TOA provides multitasking capabilities to collect and process data from multiple Thunder instances and its partitions simultaneously. By default, it collects data from shared partition.
- TOA supports Shared and L3V partitions. The maximum number of partitions supported per Thunder is 20.
- TOA collects, processes and publishes 14 Thunder metrics. The default data collection frequency is 1 minute. The metrics can be published on the same platform where the Thunder instance is deployed. For more information on Thunder metrics, see <u>Supported Thunder Metrics</u>.
- TOA collects, processes, and publishes Thunder Syslogs. The default data collection frequency is 1 minute. The logs can be published on the same platform where the Thunder instance is deployed or it can also be published to any AWS, Azure, or VMware platforms. For more information on Thunder logs, see <u>Supported Thunder</u> <u>Logs</u>.

Appendix

Get Resource ID

To get the resource ID for single or multiple Thunder instance/s, perform the following steps depending on your cloud provider:

AWS

1. Go to AWS Management Console > EC2 > Instances and select your Thunder


instance.

2. From the **Details** tab, get the **Instance ID**.

Figure 84 : Thunder instance Resource ID

aws Services	Q Search		[Alt+S]]
New EC2 Experience Tell us what you think	×	Instances (1/14) Info	ivito or tao (rasa-sonsitiva)	
EC2 Dashboard EC2 Global View		Name	▼ Instance ID	Instance state ▼ Instance type
Events		vth-server1	i-0ac7627f6cf416d84	⊖ Stopped . @Q t2.micro
Limits		✓ vth-inst1	i-0a718290e6cf3499c	⊖ Stopped . @Q m4.xlarge
 Instances 		centos7	i-0d614024ad00d9659	⊖ Stopped @Q t2.micro
Instances		4		
Instance Types		Instance: i-0a71829	0e6cf3499c (vth-inst1)	
Launch Templates		Details Security	Networking Storage Status	checks Monitoring Tags
Spot Requests	-	Details Security	Networking Storage Status	riecks Monitoring Tags
Savings Plans		 Instance summary Inf 	0	
Reserved Instances		Instance ID		
Dedicated Hosts		□ i-0a718290e6cf3499c	(vth-inst1)	
Scheduled Instances				

Azure

- 1. Go to Azure Portal > Azure services > Virtual machine and select your Thunder instance.
- 2. From the left panel, click **Setting > Properties**.
- 3. Get the **Resource ID** from the right panel.



Figure 85 : Thunder instance Resource ID

vth-inst1 Prope	erties 🛪 >
₽ Search	V1 «
Overview	Agent status
Activity log	Not Ready
Access control (IAM)	Agent version
🗳 Tags	Unknown
Diagnose and solve problems	Ephemeral OS disk N/A
Settings	
Networking Ø Connect	Azure Spot eviction policy N/A
a Disks	Azure Spot eviction type
💶 Size	N/A
Ø Microsoft Defender for Cloud	Host group
Advisor recommendations	None
Extensions + applications	Host
Nailability + scaling	
a Configuration	Proximity placement group
😵 Identity	·
Properties	Resource ID
🔒 Locks	/subscriptions/07c esourceGroups/autoscale_test/providers/Microsoft.Compute/virtualMachines
Operations	
✓ Bastion	Location
Auto-shutdown	East US
🔗 Backup	Availability zone
Disaster recovery	None

VMware

1. Log in to the **vRealize Operations Web UI** with your admin credentials to get the Thunder Resource ID once your vROps virtual machine is powered on.

The vRealize Operations Home page is displayed.





Figure 86 : vRealize Operations - Home page

vm vRealize Ope	rations		Q	С	Ļ	°
	«	Home				
A Home		Quick Start Operations Overview				
Data Sources	>	Optimize Performance		Op	otimize C	Capacit
🕼 Environment	>	DATACENTERS REQUIRING OPTIMIZATION				
🗋 Visualize	>					
🖏 Troubleshoot	>	Workload Optimization Run workload optimization to ensure consistent performance in your datacenters	Ē	20	Assess Ca Determine if capacity in y	there is su our enviro

2. Go to Home > Environment > Object Browser > All Objects > vCenter Adapter > Virtual Machine and click Thunder.

Figure 87 : vRealize Operations - Virtual machine window

\leftarrow	\rightarrow C (A Not secure	https://13/ui/index.action#environment/object-browser/tree/c1df14aa-38e	e8-4cc7-ba10-808869203473, summary
vm	vRealize Operations		
>>	Object Browser 😫 🔹 🔹	Secentos7 ACTIONSY	TROUBLESHOOT
ଳ	> 🦓 Service Discovery Adapter	Summary Alerts Metrics Capacity Compliance Logs Events more	
۵×	> 🖋 vCenter Adapter v 👩 vCenter Adapter	Centos7	Active Alerts
De la	> 🔝 Datacenter	Centos 7 (64-bit)	① Critical
ma -	> 📴 Datastore	IP Address: 10.67.4.12	! Immediate
53.>	> 🛃 Entity Status	Number of virtual CPUs: 4 Memory: 2 08	A Warning
0.1	> 🔝 Host System	Disk Space: 16 GB	 Info
÷.	> 🚱 vCenter Server	Vinite Louis Tools resources and the set	
<i>%</i> >	B Uirtual Machine B Thunder	© Time Remaining	⑦ Capacity Remaining
÷.	> 🚵 VMware vCenter Server	? Days	? (?)
© >	> 🏠 VMware-vRealize-Log-Insight-8.8		I
	> 🍪 vRealize-Operations-Cloud-Proxy-8	Configuration	Ping Statistics
	> 👸 vRopsMgr863	Virtual Hardware CPU: 4 (4 Sockets x 1 vCore)	Ping monitoring is not enabled for this Cloud Account.
	2 Co Vindinaci		

3. Get the resource ID from the URL.



NOTE: This resource ID is necessary only when directing VM metrics data exclusively to vRealize Operations. However, for sending Thunder metrics data to platforms other than VMware, any custom name can be assigned as the resource ID, for example, 'vm-123'. Additionally, for sending Thunder Syslogs to VMware and other platforms, this resource ID is optional, and any custom name, such as 'vm-123', can be assigned as the resource ID.

To get the resource ID for Thunder instance in auto scaling group or in VMSS, perform the following steps depending on your cloud provider:

AWS

- 1. Go to AWS Management Console > EC2 > Auto Scaling Groups and select your Thunder auto scale group instance.
- 2. From the **Details** tab, get the **Auto Scaling group name**.

EC2 > Auto Scaling groups > vth-auto-scale-group vth-auto-scale-group Details Activity Automatic scaling Instance management Monitoring Instance refresh Group details Edit Desired capacity um capacity Wed Dec 21 2022 12:17:54 GMT+0530 (India Standard Time) Amazon Resource Name (ARN) Maximum capacity arn:aws:autoscaling:us-east--1:939850196882:autoScalingGroup:9a9b2d49-81c8-4fa8-a521-186fc206b431:autoScalingGroupName/vth-auto-scale-gr Launch template Edit Launch template AMLID stance type ami-08c40ec9ead489470 nplate-for-auto-scaling 🖸 t2.micro lt-08a22c748b138d0cd Security groups Security group IDs Key pair name Storage (volumes Description ssingh2 Created by

Figure 88 : Thunder Auto Scaling instance Resource ID

Azure

- 1. Go to Azure Portal > Azure services > Virtual machine scale set and select your Thunder VMSS instance.
- 2. From the left panel, click Setting > Properties.
- 3. Get the **Resource Group name** from the right panel.





.

Figure 89 : Thunder VMSS instance Resource ID



Install Python, Crontab, and Syslog

Depending on your operation system, install Python (3.6 or higher), Crontab, and Syslog:

CentOS

To install latest Python from OS repository, perform the following steps:

```
yum install -y python3
```

To install Crontab and Syslog, perform the following steps:

```
yum install cronie
yum install rsyslog
```

Linux/Ubuntu

To install Python, perform the following steps:



```
apt update
apt-get install python3.10
apt install python3-pip
```

To install Crontab and Syslog, perform the following steps:

```
apt install cron
apt install rsyslog
```

Uninstall TOA

To uninstall TOA, perform the following steps:

1. Run the following commands to uninstall TOA:

```
cd /usr
source toaenv/bin/activate
pip uninstall thunder-observability-agent
```

2. Run the following commands to remove the cloud-specific configuration files:

```
cd /root
rm -rf .aws .azure .vmware .thunder
```

3. Run the following commands to remove the TOA configuration files:

```
cd /usr
rm -rf toaenv
```

4. Run the following command to remove the crontab configuration:

```
crontab -e
```

5. Remove the following entry from the crontab file:

```
*/1 * * * * /usr/toaenv/bin/python3 /usr/toaenv/lib/python3.10/site-
packages/thunder-observability-agent/toa.py
```

6. Run the following commands to remove TOA:

```
cd /var/log/
rm -rf thunder-observability-agent
```



Import vROps Template

The vRealize Operations Manager (vROps) creates a dashboard and a notification by importing a JSON files. It also creates alert definition by importing an XML file.

The following topics are covered:

- Import a Dashboard
- Import an Alert Definition
- Import a Notification

Import a Dashboard

To import a dashboard using the JSON file, perform the following steps:

- 1. Download and open the <u>dashboard-template</u> JSON file.
- 2. Edit the following parameter values in the JSON file:
 - id
 - name
- 3. Save the changes in the JSON file.
- From the vRealize Operations Web UI, go to Home > Visualize > Dashboards and click Manage.

The Manage window is displayed.

External Thunder Observability Agent (TOA)



Figure 90 : Manage window

	m vRealize Operati	ons			
		«	Dashboards	Manage	
Ŝ	Data Sources Environment	>	☆ Home⊘ Manage+ Create	ADD Ne V	Import Auto-rotate De Import ds
\sim	Visualize	~	> ☆ Favorites ~ © Recents		Manage Dashboard Folders Manage Dashboard Sharing
	Dashboards		vGautam-Test- Dashboard		
	Views		Metric- Dashboard-PD		

5. Click ... > Import in the Manage panel.

The Import Dashboard window is displayed.

Figure 91 : Import Dashboard window

Import Dashboard		\times
Select a Dashboard ZIP, PAK or JSON file to import		BROWSE
The import process begins when you click on the Import butto	on.	
In case of a conflict:		
Overwrite		
• Rename		
	CANCEL	IMPORT

6. Browse and select the **dashboard-template.json** file.

7. Click Import.

The new dashboard is imported and listed in the **Dashboards** window.



Import an Alert Definition

To import an alert definition using the XML file, perform the following steps:

- 1. Download and open the <u>alert-template</u> XML file.
- 2. Enter the following parameter values in the XML file as appropriate:
 - id
 - name

NOTE:

The id and name must have unique values.

- 3. Save the changes in the XML file.
- 4. From the vRealize Operations Web UI, go to Home > Configure > Alerts and click Alert Definitions.

The **Alert Definitions** window is displayed.

Figure 92 : Alert Definitions window

	m vRealize Operati	ions			
		~	Alert De	efinition	S
¢	Configure	~	命 / Alert	s / Alert I	Definitions
	Policies		ADD]
	Alerts			Delei Expo	te ort
	Super Metrics		□ : v	Impo	ort
	Application Discovery				

5. Click **...** > **Import** in the **Alert Definition** window.

The Import Alert Definition window is displayed.



Figure 93 : Import Alert Definition window

Import Alert Definition	\times
Select an Alert Definition XML file to import.	BROWSE
The import process begins when you click on the Import b	utton.
In case of a conflict: Overwrite existing Alert Definition Skip import	
	CANCEL

- 6. Browse and select the alert-template.json.
- 7. Click Import.

The new alert definition is imported and listed in the **Alert Definitions** window.

Import a Notification

To import a notification using the JSON file, perform the following steps:

- 1. Download and open the notification-template JSON file.
- 2. Update the alert definition id in the following parameter:





NOTE: The AlertDefinitionID must have the same value as provided in the **alert-template.json**.

3. Update the sender and recipient email address values in the following parameter:

- 4. Save the changes in the JSON file.
- 5. From the vRealize Operations Web UI, go to Home > Configure > Alerts and click Notifications.

The **Notifications** window is displayed.

Figure 94 : Notifications window

V	m vRealize Operati	ons					
		«	Notifica	tions			
¢	Configure	~	命 / Alert	s / Notifi	cations		
	Policies		ADD]		
			R	Dele	te		Description
	Alerts		п : т	Disal	ble	tion	
	Super Metrics			Enak Expo	ole ort	lion	
	Application Discovery	- 1		Impo	ort		
	Application Monitoring				Impo	rt Not	ification Settings



6. Click ... > Import in the Notifications panel.

The Import Notification Settings window is displayed.

Figure 95 : Import Notification Settings window

Import Notification Settings	\times
Select a Notification Settings JSON file to import.	BROWSE
The import process begins when you click on the Import butto	n.
In case of a conflict: Overwrite existing Notification Settings Skip import	
	CANCEL

- 7. Browse and select the **notification-template.json** file.
- 8. Click Import.

The new notification is imported and listed in the Notifications window.

Installing vROps and vRLI

vROps

To install vROps on an ESXi host, see vROps Installation.

vRLI

To install vRLI on an ESXi host, see vRLI Installation.

Base64 Conversion Examples

Base64 is an encoding technique used to convert binary data into an ASCII text format. The process of converting a JSON file to Base64 is particularly relevant for

228



cloud platforms like GCP and OCI, primarily due to the presence of private keys structured in the JSON format.

Google Cloud Platform

In this example, the private key contained in **gcpServiceKeyFile.json** is converted to Base64 and then placed in the YAML file.

• Contents of gcpServiceKeyFile.json:

```
{
"type": "service_account",
"project_id": "xxxx",
"private_key_id": "xxxx",
"private_key": "----BEGIN PRIVATE KEY----\xxxxn----END PRIVATE KEY-----\n",
"client_email": "xxxx",
"client_id": "xxxx",
"client_id": "xxxx",
"auth_uri": "xxxx",
"auth_provider_x509_cert_url": "xxxx",
"client_x509_cert_url": "xxxx",
"universe_domain": "xxxx"
}
```

• Encoded output after converting JSON to Base64 :

```
ewogICJ0eXBlIjogInNlcnZpY2VfYWNjb3VudCIsCiAgInByb2plY3RfaWQiOiAiYTEwbmV
0d29ya3Mt
```

NOTE: The curly brackets must also be included during the conversion.

• The encoded Base64 string is placed in the YAML file in the following manner:

```
---
apiVersion: v1
kind: Secret
metadata:
name: gcp-service-key-file-secret
namespace: thunder-observability-agent
type: Opaque
```

Installing Thunder Observability Agent External Thunder Observability Agent (TOA)



data:

```
gcpServiceKeyFile.json: |
ewogICJ0eXBlIjogInNlcnZpY2VfYWNjb3VudCIsCiAgInByb2plY3RfaWQiOiAiYTEwbmV
0d29ya3Mt
```

The Base64 string must follow the pipe character. Ensure that the entire encoded key is indented to align under the **gcpServiceKeyFile.json** field, maintaining the YAML structure.

Oracle Cloud Infrastructure

In this example, the private key contained in **ociPrivateKey.pem** is converted to Base64 and then placed in the YAML file.

• Contents of ociPrivateKey.pem:

```
----BEGIN PRIVATE KEY----
xxxxxxxx
----END PRIVATE KEY----
```

• Encoded output after converting JSON to Base64:

LS0tLS1CRUdJTiBQUk1WQVRFIEtFWS0tLS0tCk1JSUV2Z01CQURBTkJna3Foa21HOXcwQkF RRUZBQVNDQktnd2dnU

• The encoded Base64 string is placed in the YAML file in the following manner:

```
---
apiVersion: v1
kind: Secret
metadata:
name: oci-private-key-file-secret
namespace: thunder-observability-agent
type: Opaque
data:
ociPrivateKey.pem: |
LSOtLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z01CQURBTkJna3Foa21HOXcwQkF
RRUZBQVNDQktnd2dnU
---
```

The Base64 string must follow the pipe character. Ensure that the entire encoded key is indented to align under the **ociPrivateKey.pem** field, maintaining the YAML structure.



Creating Widgets in OCI

You can add widgets to your dashboard within the Oracle Cloud Infrastructure (OCI) Logging Analytics service to visualize and analyze your data effectively.

While creating a dashboard, the **Widget** tab on the dashboard creation page provides the following options to create a widget:

Create Widget

This option allows you to add a variety of pre-configured widgets to your dashboard. To create a widget using this method, perform the following steps:

- 1. On the metric widget creation page, under Data panel, click +.
- 2. The Add Source Data dialog box is displayed as shown in Figure 96.

Figure 96 : Create Widget - Add Source Data

Add source data				
Data source				
All Metric Sources	\$			
Namespace		Resource Group	Optional	
thunder	\$	Thunder	\$	
Metrics				
Throughput_Rate_Global_BF	⊳s ≎			
Add Cancel				

- 3. Enter data source information to generate the metrics:
 - Data Source Select All Metric Sources.
 - Namespace Select the namespace you have access to; in this case thunder.



- **Resource Group** Select the resource group; in this case **Thunder**.
- **Metrics** Based on the previous three selections, this menu gets refreshed with the names of all the metrics available. Select a metric of your choice.
- 4. Click Add.

All the selected metrics will be listed under **Source Data**.

5. Drag and drop the metrics that you want to visualize from **Source Data** section to **Y Axis** section under **Visualization** panel as shown in Figure 97.

(i) (\$\overline\$)									Last 8 Hours Today 07:30 AM - 03:30 PM UTC+05:30
🗗 Data	몇 Visualization	Ø	Apply	Cancel					
~ Source data +	Chart type	Through	put Rate (Glob	al/Rate) Averag	je 🧷				
Throughput_Rate_Global_BPS :	Line chart 🗘	800							
	Y axis								
	Throughput_Rate_Global_B ×	700							
		600							
	X axis Read only	6							
	Time (Auto)	500							
	Y axis title Optional	(Glob							
	Throughput Rate (Global/Rate)	004 H							
	Legend	ndybr							
	Correlated tooltips	0 300							
	Data cursor	200							
	Stacked	200							
		100							
		0 —							
			08:00 AM Feb 5, 2024	09:00 AM	10:00 AM	11:00 AM	12:00 PM	01:00 PM	02:00 PM 03:00 PM
						Throughput_Rate_0	Global_BPS		

Figure 97 : Create Widget

You can see the chart where the selected data is plotted along Y axis. Additionally, you can add more metrics to the Y Axis section and visualize multiple metrics together. You can customize the visualization by specifying or modifying the visualization options. Some of the common options are:

- Time Range Select the time range from the time selector.
- Chart Type You can select the chart type as Area Chart, Line Chart or Bar Chart.
- Y Axis Title Specify a title for the data projected on the Y Axis.
- **Stacked** In case of multiple metrics, you can use this option to stack charts for better viewing.
- 6. Specify the name for the widget in the field provided above the chart.



7. Click **Apply** to save the widget.

The widget will be added to the dashboard as well.

For more information, see <u>Creating Widgets</u>.

Create Query-Based Widget

The option allows you to add widgets based on queries executed on your data. To create a query-based widget, perform the following steps:

- 1. After clicking **Create query-based widget**, the query-based widget builder is displayed.
- 2. Specify the following metric details:
 - Namespace Select the applicable namespace; thunder in this case.
 - **Resource group** Select a resource group; **Thunder** in this case.
 - Query Enter a query, in MQL syntax, to retrieve the metric information you want to display in the widget. For example, CPU_Usage_Percentage_Data [auto].grouping().mean()
- 3. Click Run.

The query is executed and the metric data is displayed in a tabular format.

- 4. In the **About** tab, enter a name for the widget, select a compartment where you want the widget to reside, and add a description.
- 5. In the **Visualization** tab, select a chart type and customize the visualization. You can customize the visualization by specifying or modifying the visualization options. Some of the common options are:
 - X axis Select the data attribute to be projected on the X axis.
 - Y axis Select the data attribute to be projected on the Y axis.
 - Series Select the data attribute to be plotted in a separate series in the chart.
 - **Color by** Select the data attribute for which you want to assign different colors.
 - X Axis Title Specify a title for the data projected on the X Axis.



- Y Axis Title Specify a title for the data projected on the Y Axis.
- **Stacked** In case of multiple metrics, you can use this option to stack charts for better viewing.
- 6. In **Settings** tab, you can review and edit the widget inputs, if needed.
- 7. Click **Save** to save the widget.

The widget will be added automatically to the dashboard as well.

(i) (\$\overline\$)										Last 8 Hours Today 07:36 AM -	03:36 PM UTC+I	15:30 🔻
										{JSON}	Save	Cancel
lamespace	Resource	group Optional	Qu	ery 🕡								
hunder	C Thunder		C Tr	roughput_Rate_Gl	obal_BPS[1m].mean(Run
1.0K									About Visu	alization	Settings (i)	
0.8K					ž I	1			 Configured widge Time* 	et inputs: 3	ashboard Time	1
0.6K			×	}	*	M			Compartment* Region	⊗ Linked with ⊆ ⊗ Linked with ⊆	compartment console Region Add Ir	/ /
0.2K												
0.0		10.00 114		10.00 014	04-00 544	00.00.014	oo oo oo Hido ra	w data				
Feb 5. 2024	namespace	resourceGroup	compartm	entid	01.00 PM	02.00 PM	03.00 PM 110212	n				
Throughput_Rate_Global_BPS	thunder	Thunder	ocid1.comp	ocid1.compartment.oc1aaaaaaaaao6k/dkudnixspu5kckm7hmlznbbmnle42k4oig5vi2ci6nkj6ig								
Throughput_Rate_Global_BPS	put_Rate_Global_BPS thunder Thunder ocid1.compartment.oc1.aaaaaaaaaa6k/dkudnixspu5kckm7hmlznbbmnle42k4oig5v/2ci6nkj6iq T(v											

Similarly, you can add other metrics to the dashboard as shown in Figure 98.
 Figure 98 : OCI Dashboard

nunder-Metrics	000																Taday	01:00 PM - 01:50 PM	итс+оз:зе 📍	Actions
Remory Usage Percentage /	01:10 PM	01:15 PM	0120 PM	01.25 PM	01.30 PM	01:38 PM	01.40 PM	01.45 PM	01:50 PM	Disk Usage Pe 00 00 00 00 00 00 00 00 00 0	01:05 PM	01:10 PM	01:18 PM	01.20 PM	01.25 PM	01:30 PM	01.36 PM	01:40 PM	01.45 PM	01.50
PU Usage Percentage Ave	01:10 PM	01:15 PM	01:20 PM	01:25 PM	01:30 PM	01.35 PM	01:40 PM	01.45 PM	01:50 PM	Interface Down 00 00 00 00 00 00 00 00 00 0	Count Averag	98 01:10 PM	01:18 PM	01:20 PM	01:25 PM	01:30 PM	01.38 PM	01-40 PM	01:45 PM	01.5
*acket Rate (Sec) Average	M V							Γ		Packet Drop R 00 00 00 00 00 00 00 00 00 00 00 00 00	ate (Sec) Aver	age								

For more information of creating query-based widgets, see <u>Creating Query-based</u> Widgets.



Create Policies to Publish Data in OCI

To publish metrics and logs in OCI, you need to create and manage certain policies that define the necessary permissions. These policies specify which groups or users have access to perform certain actions on resources within specific compartments.

To create a policy, perform the following steps:

- 1. Log in to the OCI console and navigate to **Identity & Security > Policies**.
- 2. On the Policies page, click **Create Policy**.
- 3. In the **Create Policy** section, enter a policy name, description, and specify the compartment where you want to create the policy.
- 4. Under **Policy Builder**, click the **Show manual editor**.
- 5. Enter the policy rules based on the data that needs to be published:
 - To publish metrics, enter Policies for Metrics
 - To publish logs, enter Policies for Logs
- 6. Click **Create**.

Policies for Metrics

To publish metrics you need to grant permission to the following policies in OCI:

 Allow group <group_name> to read metrics in compartment <compartment_ name>

This policy allows the specified group to read metrics within the specified compartment.

 Allow group <group_name> to manage alarms in compartment <compartment_ name>

This policy grants the specified group permission to manage alarms within the specified compartment.

 Allow group <group_name> to manage ons-topics in compartment <compartment_name>

235



This policy provides the specified group with permissions to manage Oracle Notification Service (ONS) topics within the specified compartment.

 Allow group <group_name> to use streams in compartment <compartment_ name>

This policy enables the specified group to use streams within the specified compartment. Streams are used for real-time data ingestion, processing, and analysis.

Policies for Logs

To publish logs you need to grant permission to the following policies in OCI:

 Allow group <group_name> to use log-groups in compartment <compartment_ name>

This policy allows the specified group to access and view log-groups within the specified compartment.

 Allow group <group_name> to manage log-groups in compartment <compartment_name>

This policy allows the specified group to create, update, and delete log groups within the specified compartment.

Allow group <group_name> to write logs in compartment <compartment_name>

This policy permits the specified group to write logs to log groups within the specified compartment.

For more information on policies, see Managing Policies.

Disclaimer

IMPORTANT READ CAREFULLY

To use TOA, the user must license and install the following software. All such software is licensed separately by the owner of such software. A10 Networks has no responsibility for such software, nor does it provide any representation, warranty, or other attestation of it. A description of the licenses for such software is provided

236



below for your convenience only, however, it is up to you to confirm the license terms for such software at the time of installation and comply with them.

If you have any questions about the open-source software needed to use the TOA product, please email <u>support@a10networks.com</u>. In the subject line of your email, please reference: 'Open-Source Software'.

Open-Source Licenses and Copyright Notices for Required Software

The following table lists the open-source software which must be licensed and installed in order to use TOA and the open-source license type for each tool.

Tool	License
Python 3.10+	PSF LICENSE AGREEMENT FOR PYTHON 3.10.11
Requests 2.27.1+	Apache Software License 2.0
Boto3 1.23.10+	Apache 2.0 (<u>amazon.com)</u> https://aws.amazon.com/apache-2-0/
Botocore 1.29.121	Apache Software License 2.0
google-auth 2.22.0	Apache Software License 2.0,
	Apache 2.0 (google.com)
oci 2.121.1	Apache Software License,
	Universal Permissive License
certifi 2022.12.7	Mozilla Public License 2.0
charset-normalizer 3.1.0	MIT License
idna 3.4	MIT License
jmespath 1.0.1	MIT License
python-dateutil 2.8.2	Apache Software License 2.0, BSD License
s3transfer 0.6.0	Apache Software License 2.0
Six 1.16.0	MIT License
urllib3 1.26.15	MIT License



License

For TOA License information, see <u>THUNDER OBSERVABILITY AGENT END USER</u> <u>SOFTWARE LICENSE AGREEMENT</u>.



©2024 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/company/legal/trademarks/.