



NVIDIA UFM Cyber-AI Documentation v2.6.3

Table of contents

Release Notes	4
Changes and New Features	4
Bug Fixes in This Release	4
Known Issues	4
Software Management	5
Cyber-AI Analytics	13
REST API	34
Session Management	34
User Management	35
UFM Telemetry	39
Cyber-Ai Release Version	42
Configuration	43
Alert Count Summary	49
Suspicious Behavior	53
Link Analysis	73
Resources	86
Telemetry Data	98
Alert Filters	107
CLI Tools	113
High Availability	119
UFM Cyber-AI OS Upgrade	124
Morpheus Integration	131

List of Supported Events	134
Settings and Configuration	140
Appendixes	142
Appendix - Supported Counters	142
Appendix - Cable Information	146
Appendix - Cyber-AI Appliance OS Remanufacture	148
Appendix - Deploying UFM Cyber-AI from an ISO File	165
Document Revision History	181

About This Document

NVIDIA® Unified Fabric Manager (UFM®) Cyber-AI platform determines a data center's unique vital signs and uses them to identify performance degradation, component failures, and abnormal usage patterns.

Downloading Software

To download Cyber-AI software, please visit [NVIDIA's Licensing Portal](#).

Technical Support

Customers who purchased NVIDIA products directly from NVIDIA are invited to contact us through the following methods:

- E-mail: enterprisesupport@nvidia.com
- Enterprise Support page: <https://www.nvidia.com/en-us/support/enterprise>

Customers who purchased NVIDIA M-1 Global Support Services, please see your contract for details regarding technical support.

Customers who purchased NVIDIA products through an NVIDIA-approved reseller should first seek assistance through their reseller.

Document Revision History

For the list of changes made to this document, refer to [Document Revision History](#).

Release Notes

These release notes pages provide information for NVIDIA UFM Cyber-AI software such as changes and new features, bug fixes, and known issues.

Changes and New Features

Feature	Description
UFM Enterprise Version Update	Updated the UFM Enterprise version to 6.15.8-2
UFM OS	Integrated with UFM OS version 25.06.18-2

Bug Fixes in This Release

N/A

Known Issues

N/A

Software Management

This chapter describes how to deploy UFM Cyber-AI on UFM Cyber-AI appliance.

Deploying UFM Cyber-AI

NVIDIA® UFM® Cyber-AI is packaged in a tar file. The tar file consists of several docker images and an installation script. The script will load the docker images and create a UFM Cyber-AI service. UFM Cyber-AI should be installed on UFM Cyber-AI appliance.

To deploy the UFM Cyber-AI:

1. Copy the tar file to the UFM Cyber-AI appliance, for example, to the `/tmp` folder.
2. Copy the license file to the same directory on the UFM Cyber-AI appliance.
3. Connect to the UFM Cyber-AI appliance via SSH.
4. Extract the tar file and install the service. Run:

```
[root@r-ufm ~]# cd /tmp
[root@r-ufm ~]# tar xvf ufm-cyberai-sw-<version>.tar
[root@r-ufm ~]# cd ufm-cyberai-sw-<version>
[root@r-ufm ~]# ./install.sh
```

Installer options:

- `-n|--no-ufm`: By default, UFM Enterprise is installed
- `-q|--quiet`: Upgrade Cyber-AI without a prompt
- `-l|--license`: License file location

Example:

```
./install -u -l <license_file_path>
```

5. If you did not provide the license when running the install script, copy the license file.
Run:

```
[root@r-ufm ~]# cp /tmp/<cyberai-license-file>.lic  
/opt/ufm/cyberai/licenses
```

6. Start the UFM Cyber-AI service. Run:

```
[root@r-ufm ~]# systemctl start ufm-cyberai.service
```

7. Start the UFM Enterprise service. Run:

```
[root@r-ufm ~]# systemctl start ufm-enterprise.service
```

8. Wait 1 minute for the system to come up.

9. Ensure the service health by running the following:

```
[root@r-ufm ~]# ufm-cai-sanity -u <username> -p <password>  
Where the username and password are the default username and  
password for cyberai  
Checking Service...  
Done  
Checking Images...  
Done  
Checking Containers...  
Done
```

```
Checking ufm-cyberai REST server...
Done
Sanity tests completed successfully!
```

10. Set the NVIDIA® UFM® Enterprise connection parameters:

```
[root@ r-ufm ~]# ufm-cai-ufm-params update-i <ufm_ip> -p
<ufm_port> -U <username> -P <password> -s <site_name> -t
<protocol>
```

Options:

```
-h|--help          Show this message
-i|--ip            UFM server IP
-p|--port          UFM REST API connection port
-U|--username      UFM username
-P|--password      UFM password
-s|--site          UFM site name
-t|--protocol      UFM Rest API connection protocol
```

This step can be done also using the web UI. However, it is recommended to set the UFM Enterprise parameters as early as possible, as UFM Cyber-AI needs it to retrieve the fabric topology.

11. To access the UFM Cyber-AI logs, run the following on the UFM Cyber-AI appliance:

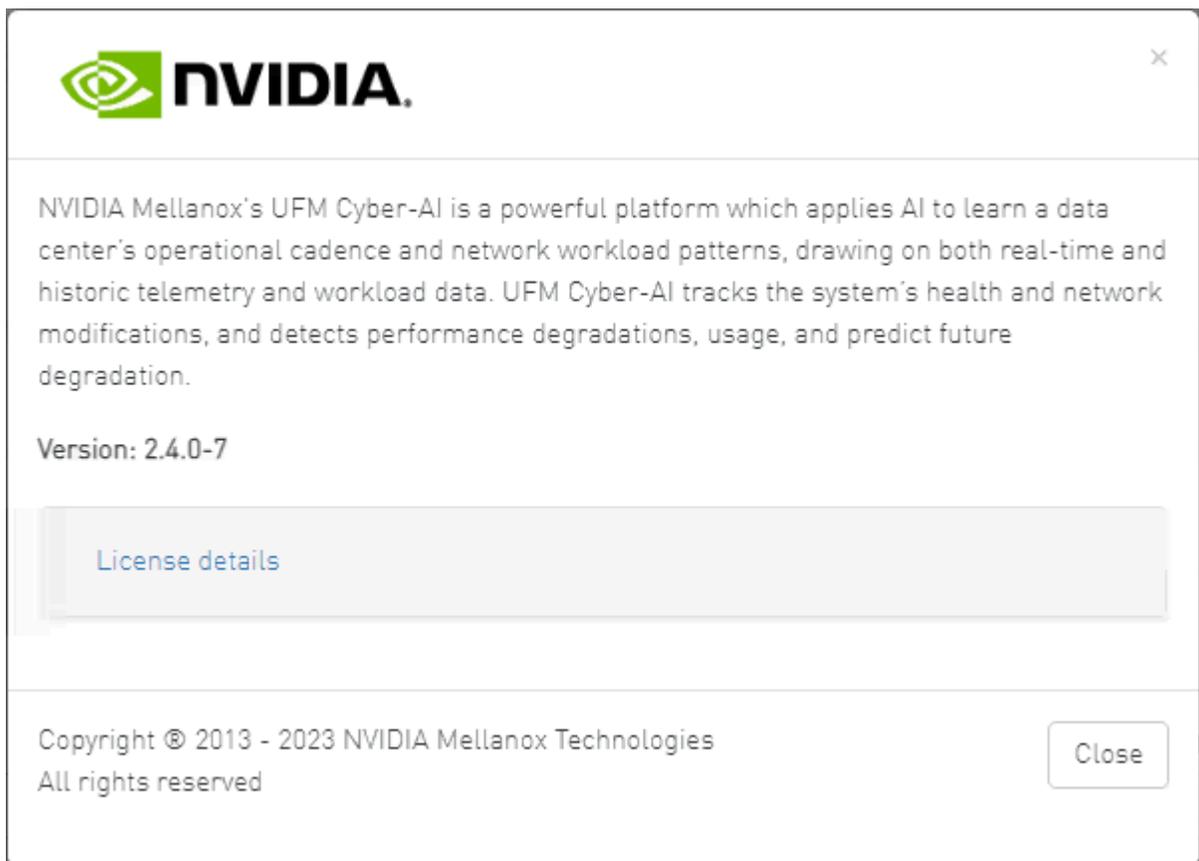
```
[root@r-ufm ~]# ls -la /var/log/cyberai/
total 86160
drwxr-xr-x 2 root root    4096 Mar  6 03:28 .
drwxr-xr-x 3 root root    4096 Mar  5 18:46 ..
-rw-r--r-- 1 root root      0 Mar  5 19:51 access.log
-rw-r--r-- 1 root root 45563430 Mar 12 16:09 console.log
```

```
-rw-r--r-- 1 root root 42646820 Mar 12 16:09 cyberai.log
-rw-r--r-- 1 root root          0 Mar  5 19:53 rest.log
```

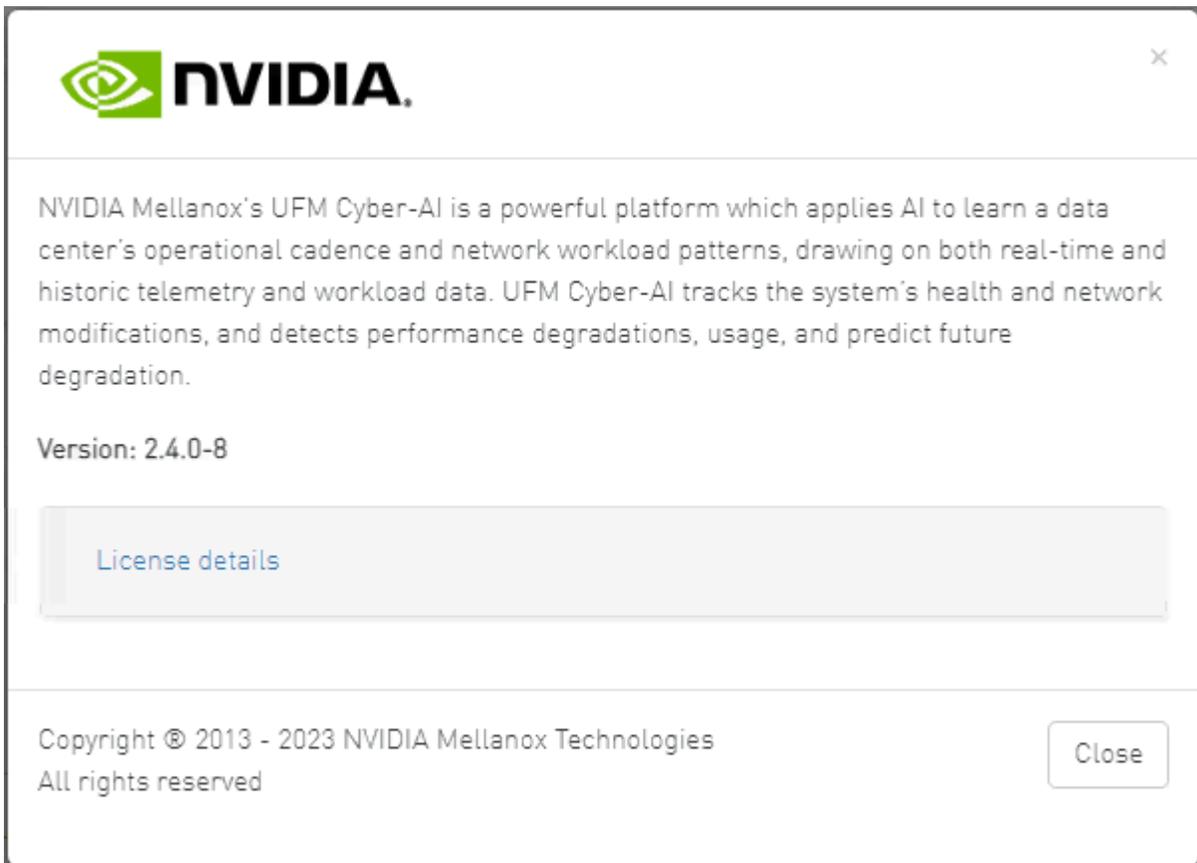
12. For settings and configuration instructions, see [Settings and Configuration](#).

To view the license details:

1. After installing and activating the software, licenses can be viewed in the Web UI by clicking the about icon on the main page.



2. The main about screen displays the current UFM Cyber-AI version and build. To view more information, click "License details".



Upgrading UFM Cyber Software

The first step of upgrading UFM Cyber-AI are similar to the first steps of a fresh installation. The installation process consists of replacing the containers with the new version and upgrading the data according to the new scheme.

1. Copy the tar file to the UFM Cyber-AI appliance, for example, to the `/tmp` folder.
2. Connect to the UFM Cyber-AI appliance via SSH.
3. Stop the UFM Cyber-AI service. Run:

```
[root@r-ufm ~]# systemctl stop ufm-cyberai.service
```

4. Extract the tar file and install the service for upgrade. Run:

```
root@r-ufm ~]# cd /tmp
```

```
[root@r-ufm ~]# tar xvf ufm-cyberai-sw-<version>.tar
[root@r-ufm ~]# cd ufm-cyberai-sw-<version>
[root@r-ufm ~]# ./install.sh
UFM Cyber-AI version <old-version> is installed on this
machine
Would you like to upgrade to version <new-version>? [y|N]:
```

5. Enter 'y' to proceed with the upgrade.

Installer options:

- `-q|--quiet`: Upgrade Cyber-Ai without prompt
- `-n|--no-ufm`: Will not install UFM-Enterprise
- `-l|--license`: The License file location

6. Start the ufm-cyberai service. Run:

```
[root@r-ufm ~]# systemctl start ufm-cyberai.service
```

7. Wait 1 minute for the system to come up.

8. Ensure the service health by running the following:

```
root@r-ufm ~]# ufm-cai-sanity -u <username> -p <password>

Where the username and password are the default username and
password for cyberai
Checking Service...
Done
Checking Images...
Done
Checking Containers...
```

```
Done
Checking ufm-cyberai REST server...
Done
Sanity tests completed successfully!
```

Running Cyber-AI Plugin

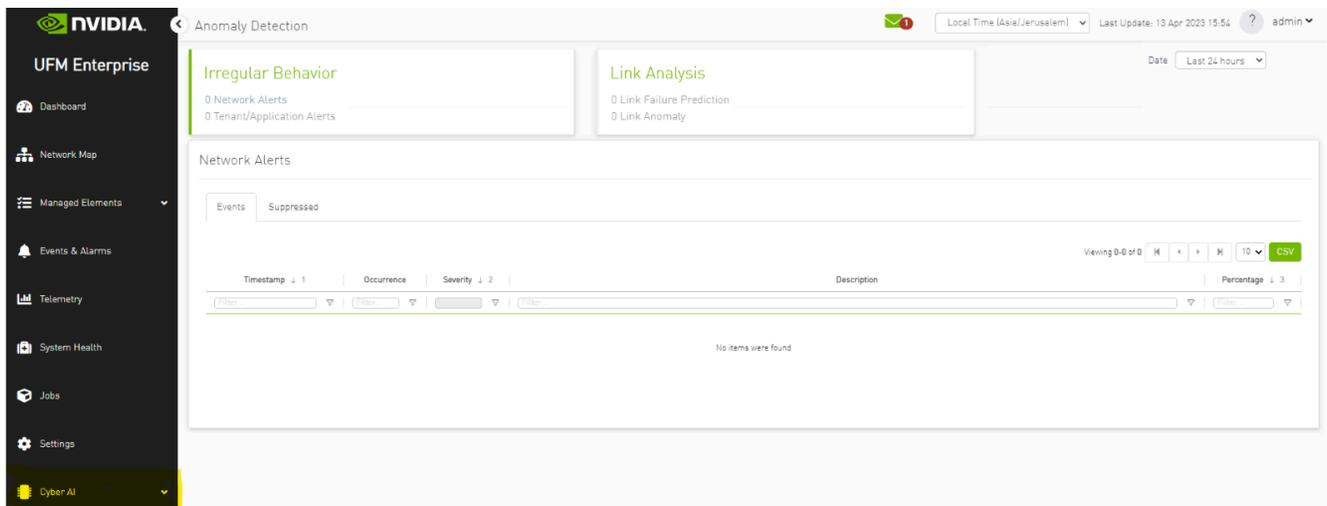
To integrate Cyber-AI with UFM Enterprise, it can be employed as a plugin. To achieve this, follow the below instructions.

1. Download the plugin's docker image to a local host:

```
[root@r-ufm ~]# docker load -i ufm-plugin-
cyberai_<version>.tar.gz
```

2. Load the docker image.

Once the Docker image has been loaded, refer to the UFM Enterprise user manual for instructions on managing the Cyber-AI plugin. It is important to note that when Cyber-AI is executed as a plugin, there will be no direct access to its APIs from remote machines. It will only be accessible locally and without the need for authentication.

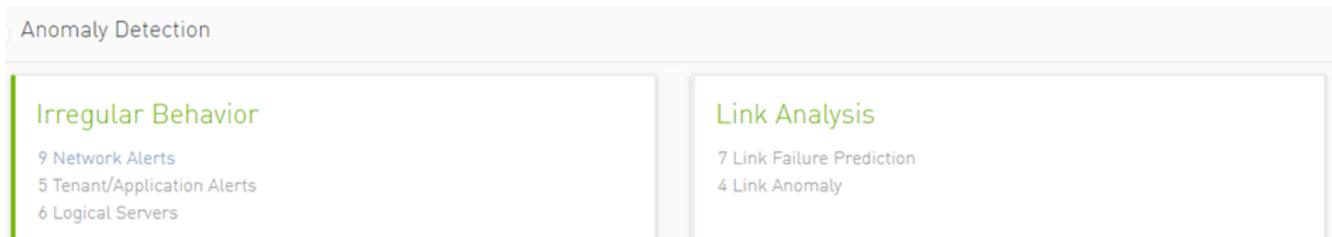


Cyber-AI APIs can be accessed from the remote host via UFM Enterprise using the following URL. You should log in with UFM Enterprise authentication:

https://<host>/ufmRestV2/plugin/cyberai/cyber-ai/analytics/summary?from=-24h&min_probability=85

Cyber-AI Analytics

Anomaly Detection



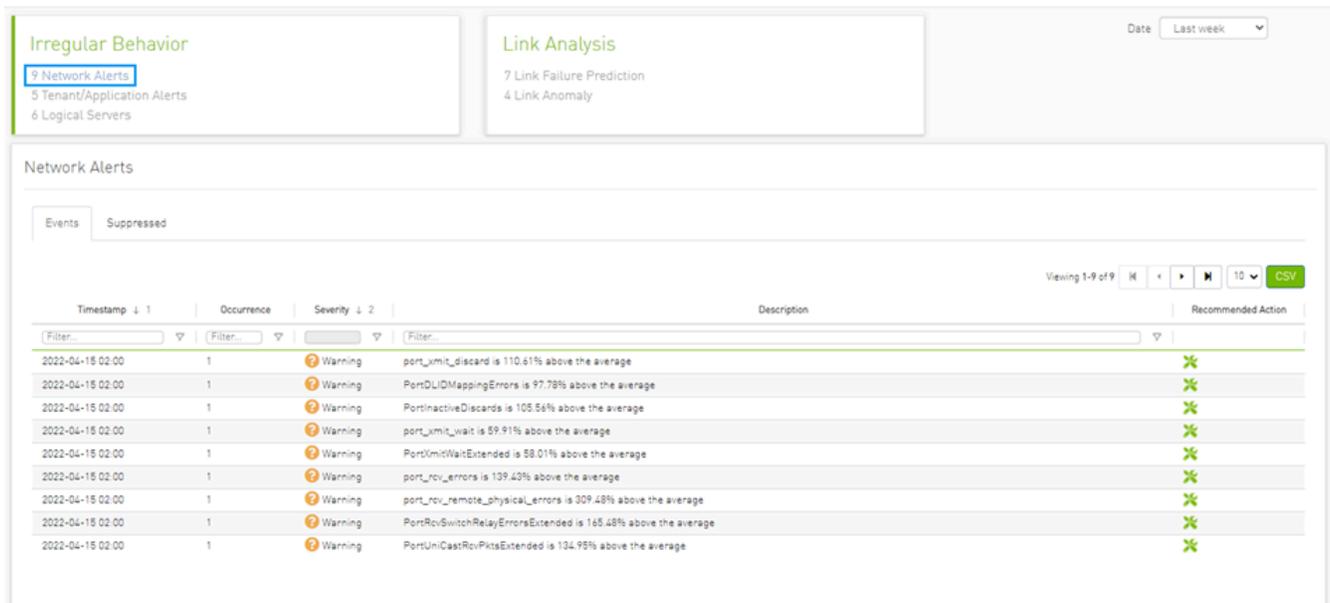
- Network Alerts: Alerts for the entire cluster. The algorithm checks for unusual changes in several important metrics and notifies the user.
- Tenant/Application Alerts: Triggered by PKey monitoring in the cluster. It checks the most congested PKeys for a better understanding of applications' health.
- Link Failure Prediction: Prediction of future link failures 1-to-24 hours in advance using machine learning algorithms with a probability indicator and the counters that influenced the triggering of the alert the most .
- Link Anomaly: Detects anomalous behavior in the cluster with a probability indicator. It detects the most significant influencers on the anomaly notice.

Network Anomalies

The purpose of this tab is to detect abnormal behavior at the level of the entire cluster.

An ETL process runs hourly and calculates network aggregated statistics while another process checks how the current statistics compare to statistics aggregated over the previous month. If over 20% of the difference is detected (default value that can be changed) the system triggers an alert with relevant information. It is also possible to see recommended action by clicking the relevant icon per alert.

The web UI provides a list of alerts as shown in the following:



Clicking any alert provides an additional layer of analysis that shows the anomalous parameter over three different time ranges.



Tenant/Application Alerts

The ETL process of UFM Cyber-AI combines a partitioning key (PKey) topology with network telemetry to monitor PKey performance.

Based on normalized congestion measurements (the default is greater than 70%) the system detects the most congested PKeys. This is done by counting the amount of time when the alert is received.

In addition, a resource allocation pie is available which shows allocated nodes for PKey via free nodes.

Detailed event information is provided to the user regarding PKey alerts, where the user can see PKey details and descriptions of the alert.



Clicking any PKeys alert shows six graphs representing network statistics in general and per selected Pkey.



This way the user can see the impact of a specific PKey throughout the entire network and can see if PKey activity is normal both from a performance and from a duration of usage (if the activity is happening in a reasonable time) point of view.

Viewing 1-10 of 56

Timestamp	Occurrence	Severity	Tenant ID	Description
2022-09-05 20:55	Minor	Minor	Ox1 (2021-09-12 19:59:05)	Tenant Ox1 (2021-09-12 19:59:05) is utilized above 1.53
2022-09-05 20:55	Minor	Minor	Ox2 (2021-09-12 20:02:05)	Tenant Ox2 (2021-09-12 20:02:05) is utilized above 1.64
2022-09-05 20:55	Minor	Minor	Ox3 (2021-09-12 20:02:05)	Tenant Ox3 (2021-09-12 20:02:05) is utilized above 1.48
2022-09-05 20:55	Minor	Minor	Oxe (2021-09-12 19:59:05)	Tenant Oxe (2021-09-12 19:59:05) is utilized above 1.45

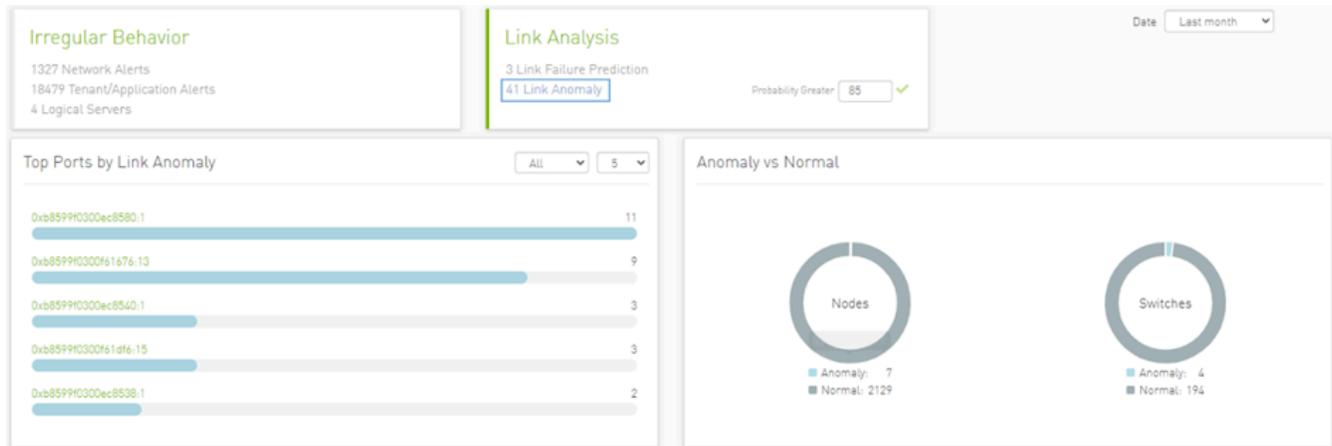
Link Failure Prediction

UFM Cyber-AI trains machine learning algorithms to predict future failures by collecting monitoring information (i.e. training data for the machine learning algorithms) over a time duration (e.g. 1-24 hours) in advance of (retrospectively known) previous failures that

occurred and having the algorithms learn the connection between different parameters over time.

Using the machine learning algorithm, the processor derives the potential failure pattern by, for example, alerting future failure times of components. The processor repeatedly updates the alerted future failure times based on newly collected failures.

The dashboard provides a list of ports with the most Link Failure Predictions alerts raised and the relation between Alerted and the Total number of devices in the cluster.



In the “Top Port by link anomaly” graph, the user can filter the alerts table below by clicking any node name on the graph to add the appropriate filters to the table.

Users may see the detailed events through an event list where alert details like Node Name, Port, Hours to Fail, and alert Description are available.

Timestamp	Occurrence	Severity	Node Guid	Node Name	Port	Hours to Event	Probability ↓	Description
2022-09-11 07:00	5	Suspect	0x1c34da0300d9aaa0	MTL-S-F1-DC-IB-SW160	23	19	91.13	Link Failure Prediction for 0x1c34da0300d9aaa0:23 most ...
2022-09-20 12:00	99	Suspect	0x248a070300e0d4d0	MTL-S-F1-DC-IB-SW121	28	19	84.94	Link Failure Prediction for 0x248a070300e0d4d0:28 most ...
2022-09-11 07:00	8	Suspect	0x1c34da0300d9aaa0	MTL-S-F1-DC-IB-SW160	2	19	83.94	Link Failure Prediction for 0x1c34da0300d9aaa0:2 most d...
2022-09-11 07:00	5	Suspect	0x248a070300e0d4d0	MTL-S-F1-DC-IB-SW215	20	19	83.94	Link Failure Prediction for 0x248a070300e0d4d0:20 most ...

Clicking any alert in the list shows more information and recommended actions related to the alerted node, it will also show any alerts related to the cable that is connected to this node, if there is any, also three graphs representing counters that influenced the triggering of the alert will be shown below. Several time ranges are available.

0x248a070300e0d4d0

Prev Next

Recommended Actions

Site Name MTLX

Time 2022-09-20 12:00

Creation Time 2022-09-15 17:00

Severity ▲ Suspect

Description Link Failure Prediction for 0x248a070300e0d4d0:28 most dominant features ErrorDetectionCounterLane.1: 0.0,x115_dropped: 0.0,phy_raw_errors_lane3: 0.0

Recommended Actions

- Port reset and keep monitoring
- If still getting the alerts, please check if there any related cable alerts via cable anomaly tab
- In addition please check relevant cable measure trend via cable anomaly tab
- If there are alerts for connected cable and/or deprecating trend please consider cable replacement
- If known issue due to maintenance activity please use suppress function do define as known issue

Cable Info

Identifier	SN	GUID	Port Name	Port	Link Partner	Source Type	Source Role	Destination Type	Destination Role	Supported Speed
13	MT2153V503595	0x248a070300e0d4d0	MTL-S-F1-DC-IB-SW121/U1/P28	28	0x1070fd030015da4d:1	switch	tor	host	endpoint	0

Cable Anomalies

Cable Anomalies Events

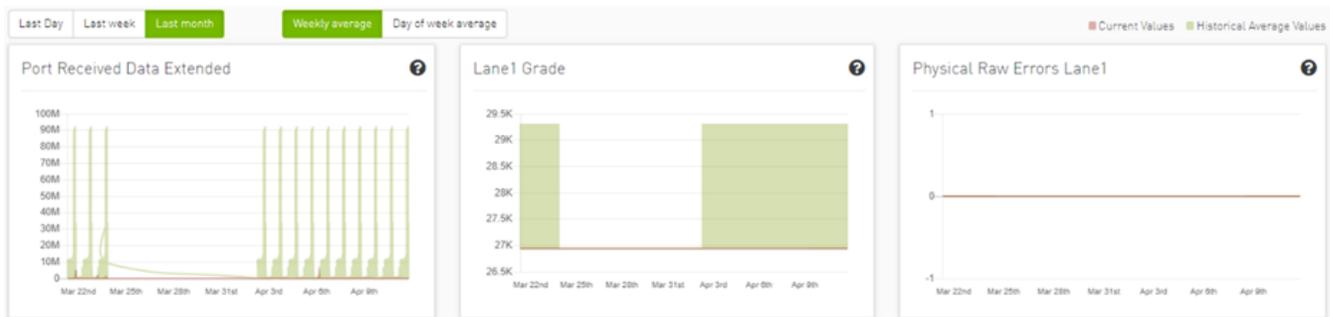
Viewing 0-0 of 0 10 CSV

Timestamp	SN	Node GUID	Port	Influencer	Influencer Value	Severity	Link Partner	Source Type	Source Role	Destination Type	Destination Role	Speed	Length	PN	F
Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...

The default view for the graph provides two lines for each graph: One for current data, and another for historical data which is calculated based on average values from the prior week.

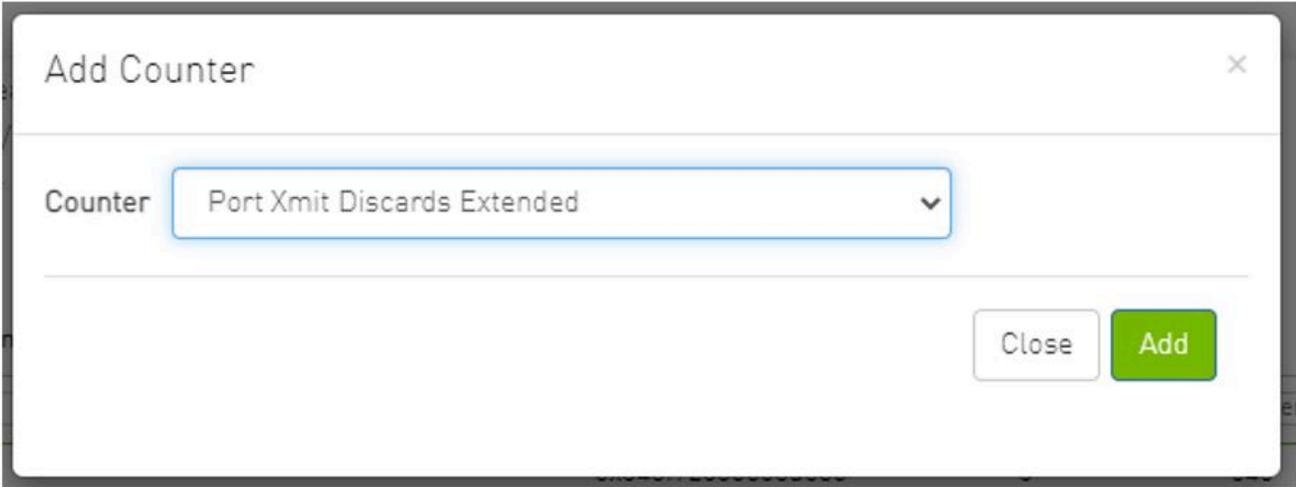
Users can choose to switch between Weekly average (default) to Day of Week average.

Day of Week Average is based on the calculation of the statistics in the same hours and day of the week of the past month. For example The average for 8AM–9AM on Mondays during the past month.



Also, users can add more graphs for more counters by clicking the "Add More" button below the graphs.

Add More



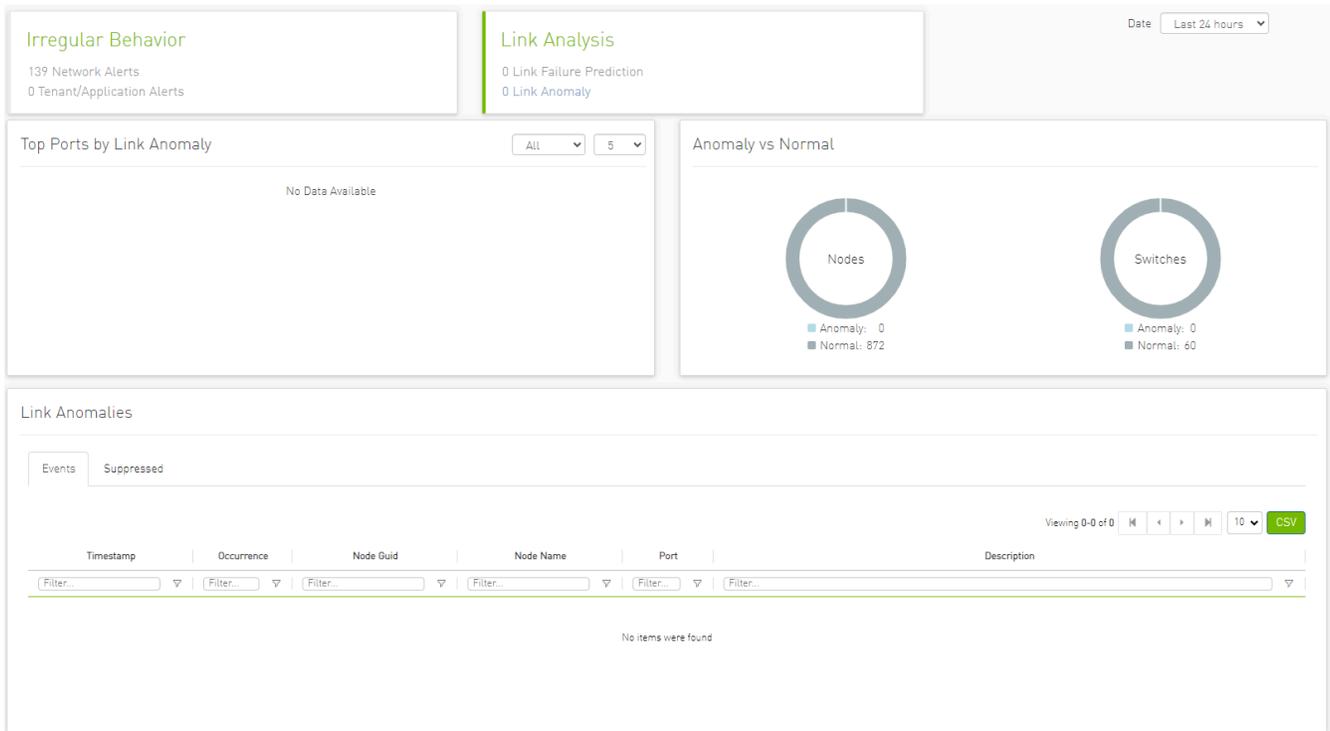
Then a new counter could be chosen, and a new graph for that counter will be added.

Link Anomalies

Port anomaly detection is based on defining composite metrics to reliably detect anomalies, where such metrics dynamically change, for example, according to a baseline that is determined and subsequently updated by a system.

In addition, there is a process for defining an anomaly score that provides a statistical estimation, such as the number of standard deviations, or the number of Mean Absolute Errors (MAEs) from a baseline value of the feature (i.e., metrics value), and assigning a degree of severity according to the number of standard deviations or MAEs.

The dashboard provides a list of top ports reporting link anomalies including the number of times an anomaly is detected and statistics regarding Alerted and the Total number of devices in the cluster.



In the “Top Port by link anomaly” graph, the user can filter the alerts in the table below by clicking any node name on the graph to add the appropriate filters to the table.

Users can also see detailed events in the events list where the alert details such as Node Name, Probability, and Alert Description are available.

Timestamp	Occurrence	Severity	Source	Port	Probability ↓	Description	Recommended Acti...
2022-04-04 04:00	1	Minor	0xb8599f0300f61676	13	90.00	Anomaly detected for 0xb8599f0300f61676:13 regarding phy_raw_errors_lane0_hist2_hist1	✖
2022-04-04 10:00	1	Major	0xb8599f0300f61d56	47	90.00	Anomaly detected for 0xb8599f0300f61d56:47 regarding hist3_phy_raw_errors_lane3_hist1	✖
2022-04-04 21:00	3	Minor	0xb8599f0300f61676	13	90.00	Anomaly detected for 0xb8599f0300f61676:13 regarding hist2_phy_raw_errors_lane0_hist1	✖
2022-04-04 23:00	1	Major	0xb8599f0300ec8580	1	90.00	Anomaly detected for 0xb8599f0300ec8580:1 regarding PortFECCorrectedSymbolCounte...	✖
2022-04-05 17:00	1	Minor	0xb8599f0300f61d56	14	90.00	Anomaly detected for 0xb8599f0300f61d56:14 regarding hist1_hist2_phy_raw_errors_lane3	✖

0xb8599f0300f61df6



Site Name

Local

Time

2022-04-05 17:00

Creation Time

2022-04-05 17:00

Severity

 Minor

Description

Anomaly detected for 0xb8599f0300f61df6:14 regarding hist1,hist2,phy_raw_errors_lane3

Recommended Actions

- Port restart and keep monitoring
- Please check if there any cable alert via cable anomaly tab
- Please check cable measure trend via cable anomaly tab
- Please consider Cable replacement or Suppress as known issue

Clicking any alert in the list shows more information and recommended actions related to the alerted node, it will also show any alerts related to the cable that is connected to this node, if there is any. In addition, three graphs representing counters that influenced the triggering of the alert will be shown below. Several time ranges are available.

0x248a070300e0d4d0

Prev Next

Recommended Actions

Site Name MTLX

Time 2022-09-20 12:00

Creation Time 2022-09-15 17:00

Severity ▲ Suspect

Description Link Failure Prediction for 0x248a070300e0d4d0.28 most dominant features Error:DetectionCounterLane.1:0.0,v115_dropped:0.0,phy_raw_errors_lane3:0.0

Recommended Actions

- Port reset and keep monitoring
- If still getting the alerts, please check if there any related cable alerts via cable anomaly tab
- In addition please check relevant cable measure trend via cable anomaly tab
- If there are alerts for connected cable and/or deprecating trend please consider cable replacement
- If known issue due to maintenance activity please use suppress function do define as known issue

Cable Info

Identifier	SN	GUID	Port Name	Port	Link Partner	Source Type	Source Role	Destination Type	Destination Role	Supported Speed
13	MT2153V503595	0x248a070300e0d4d0	MTL-S-F1-DC-IB-SW121/U1/P28	28	0x1070f030015dad4:1	switch	tor	host	endpoint	0

Cable Anomalies

Cable Anomalies Events

Viewing 0-0 of 0 CSV

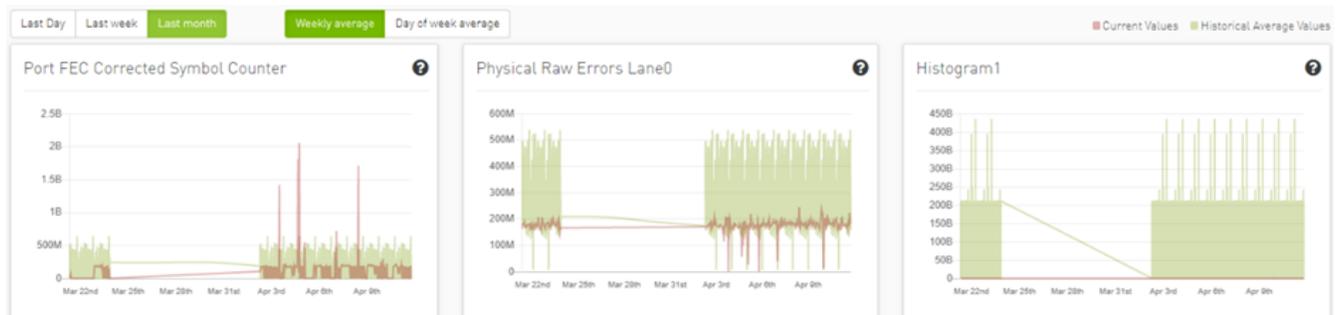
Timestamp	SN	Node GUID	Port	Influencer	Influencer Value	Severity	Link Partner	Source Type	Source Role	Destination Type	Destination Role	Speed	Length	PN
Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...

No items were found

The default view provides two lines for each graph: One for current data, and another for historical data which is calculated based on average values from the prior week.

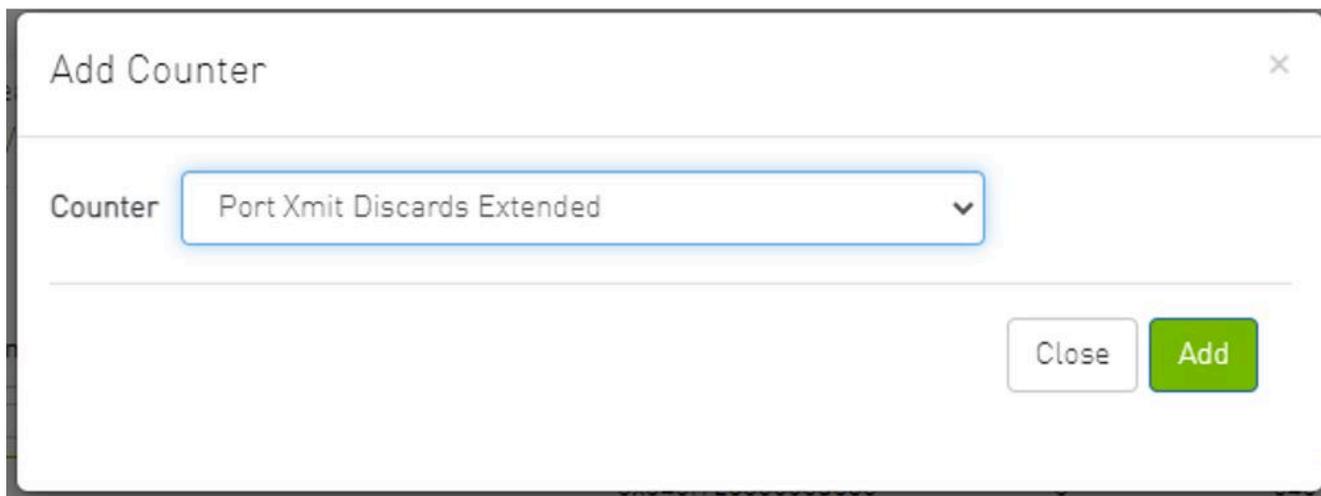
Users can choose to switch between Weekly average (default) to Day of Week average.

Day of Week Average is based on calculating the statistics in the same hours and day of the week of the past month. For example, the average for 8AM–9AM on Mondays during the past month.



Also, users can add more graphs for more counter by clicking the add more button below the graphs.





Then a new counter could be chosen, and a new graph for that counter will be added.

Logical Server Alerts

Logical server data collection and analytic jobs are disabled by default. To enable this, the related flags should be updated in the `scheduler_settings.cfg` file:

```
[analytics_job::logical_server_port_join]
interval = 300
delay = 720
max_input = 12
standard_timeout = 180
enabled = true

[analytics_job::logical_server_aggr]
interval = 300
delay = 780
max_input = 12
standard_timeout = 180
enabled = true

[data_prep_ufm::logical_server]
interval = 60
```

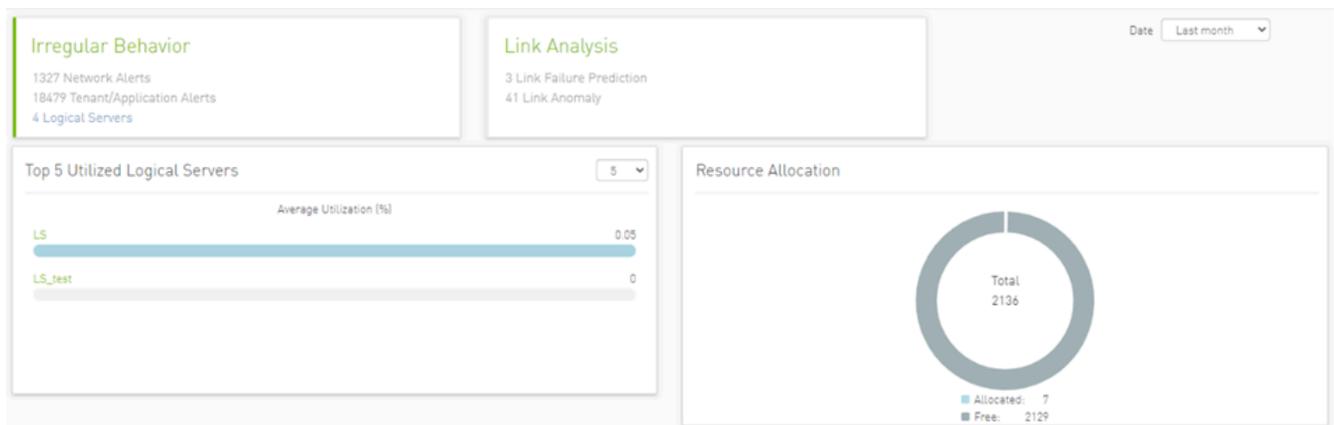
```
delay = 60
skip_collection = false
json_collection = false
```

The ETL process of UFM Cyber-AI combines the topology of the logical server, with network telemetry allowing the monitoring of logical servers' performance.

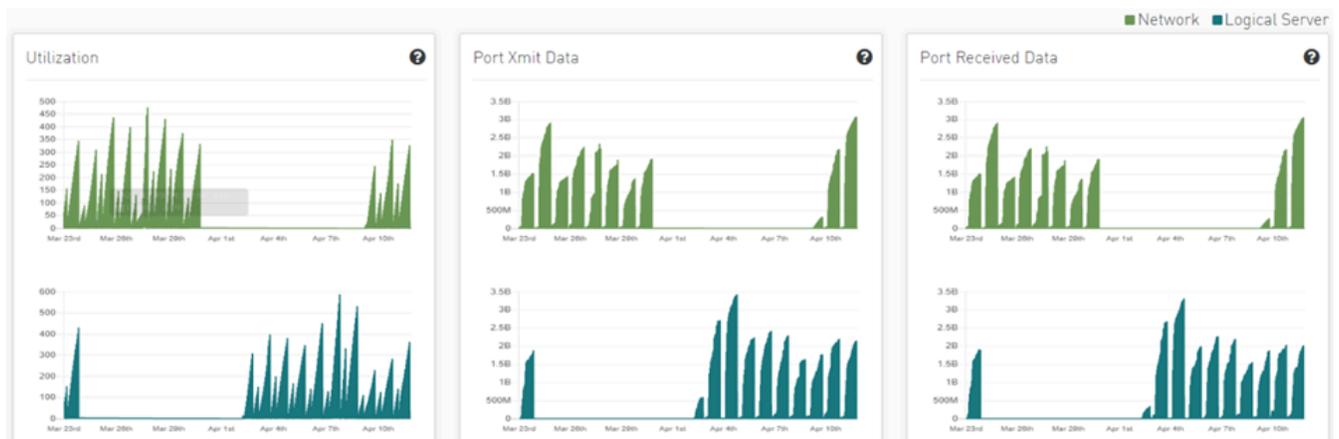
Based on utilization measurements (the default is greater than 70%) the system detects the most utilized logical server. This is done by counting the amount of time when the alert is received.

In addition, a resource allocation pie is available which shows allocated nodes for logical servers compared to free nodes.

Detailed event information is provided to the user regarding logical server alerts, where the user can see logical server details and a description of the alert.



Clicking any logical server alert shows six graphs representing network statistics in general and per selected logical server.



This way the user can see the impact of a specific logical server throughout the entire network and can see if logical server activity is normal both from a performance and from a duration of usage (i.e., if the activity is happening in a reasonable time) point of view.

Timestamp	Occurrence	Severity	Description	Recommended Action
2022-04-17 10:00		Warning	Logical server logical_s is utilized above 84.38%	
2022-04-17 10:00		Minor	Logical server LS is utilized above 0.03	
2022-04-17 10:00		Minor	Logical server LS_test is utilized above 0.01	
2022-04-17 10:00		Critical	Logical server test_ls is utilized above 71.54%	

Recommended Actions

A recommended action is available for all alert types. The user can click on any alert from alerts table in each page to see the recommended actions for the alert.

0x248a070300e7f220 Prev Next

Recommended Actions

Site Name

Time 2022-09-04 09:00

Creation Time 2022-09-02 06:00

Severity Warning

Description Anomaly detected for 0x248a070300e7f220:12 most dominant features raw_ber: 1.4999999999999999e-254,eff_ber: 1.4999999999999999e-254,PortXmitWaitExtended: 0.0

Recommended Actions

- Port reset and keep monitoring
- If still getting the alerts, please check if there any related cable alerts via cable anomaly tab
- In addition please check relevant cable measure trend via cable anomaly tab
- If there are alerts for connected cable and/or deprecating trend please consider cable replacement
- If known issue due to maintenance activity please use suppress function do define as known issue

Cable Info

Identifier	SN	GUID	Port Name	Port	Link Partner	Source Type	Source Role	Destination Type	Destination Role	Supported Speed
13	MT2203V502406	0x248a070300e7f220	MTL-S-F1-DC-IB-SW047/U1/P12	12	0x08c0eb0300ab9c10:1	switch	tor	host	endpoint	SDR/DDR/QDR/FDR/

Anomaly Analysis

Specification Description

The purpose of this module is to analyze the anomalies that were previously found in ML models and to understand possible common ground for the anomalies.

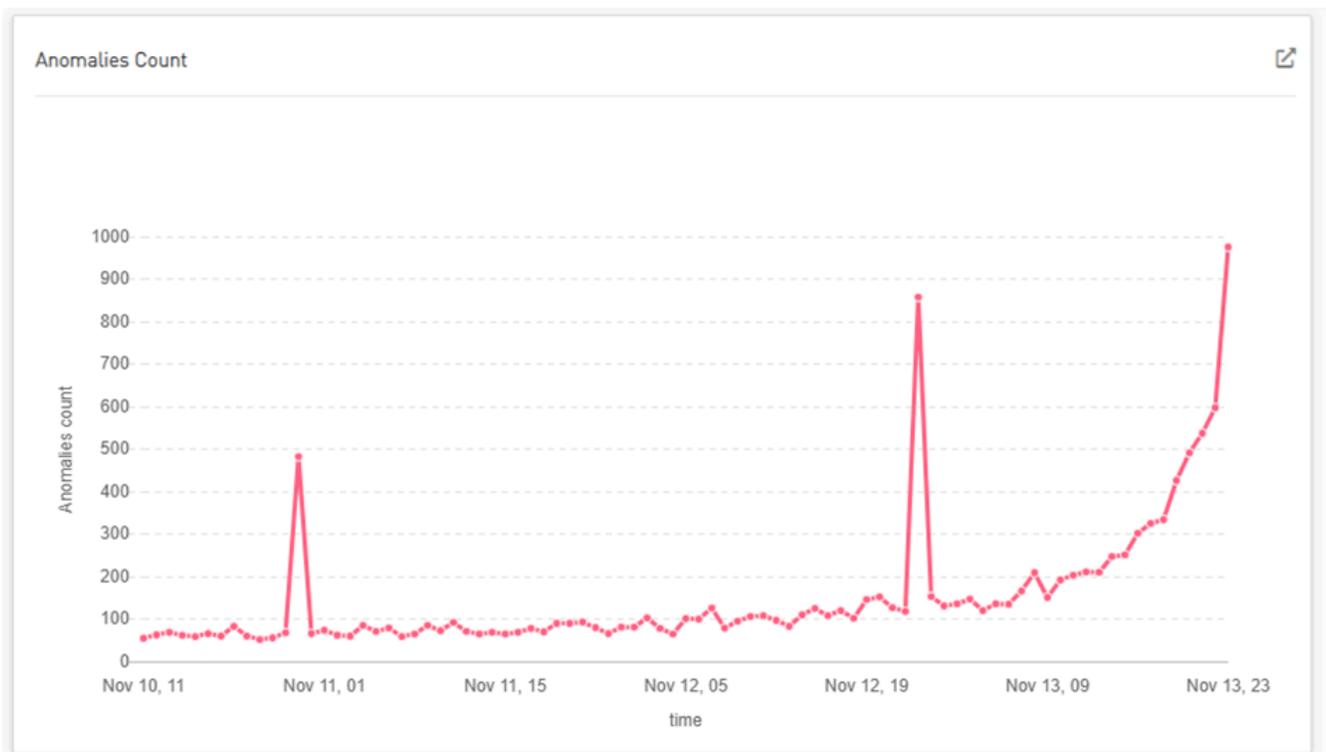
Source Type	Source Role	Destination Type	Destination Role	Length	PN	Rev	FW Version	Type	Width	Source NIC Type	Count of Source Type
host	endpoint	switch	tor	1	N/A	A1	NA	Copper cable- uheq...	4x	Connecti-6	3121
host	endpoint	switch	tor	1	N/A	A1	NA	Copper cable- uheq...	4x	Connecti-6	2554
host	endpoint	switch	tor	2	N/A	A1	NA	Copper cable- uheq...	4x	Connecti-6	97
switch	core	switch	tor	30	N/A	A3	37.50.322	850 nm VCSEL	4x	NA	1851
switch	core	switch	tor	30	N/A	A3	37.51.302	850 nm VCSEL	4x	NA	212
switch	tor	host	endpoint	1	N/A	A1	0.0.0	Copper cable- uheq...	4x	NA	1884
switch	tor	host	endpoint	1	N/A	A1	0.0.0	Copper cable- uheq...	4x	NA	1826
switch	tor	host	endpoint	2	N/A	A1	0.0.0	Copper cable- uheq...	4x	NA	111
switch	tor	switch	core	N/A	N/A	NA	37.50.322	NA - UNKNOWN	4x	NA	15
switch	tor	switch	core	30	N/A	A3	37.50.322	850 nm VCSEL	4x	NA	1404

The table above represents the number of anomalies found by the ML model for each attribute's combination, such as roles for source and destination (endpoint, core, tor), cable parameters (length, Pn, Sn, Version, Type, Width), and Nic type.

Event Flow Charts

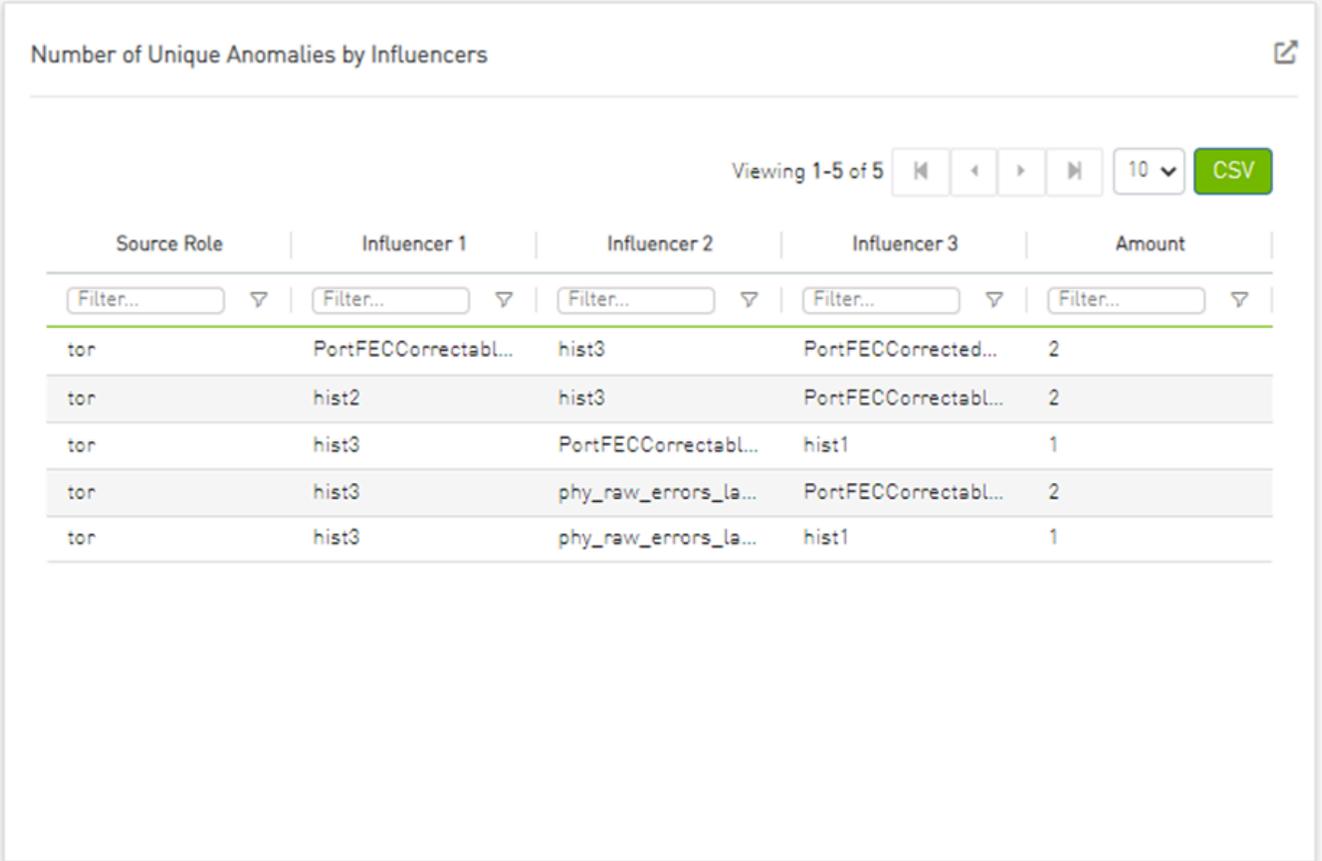
Total Anomalies Over Time

Number of anomalies over time:



Anomalies Influencers

Shows the number of anomalies for each combination of influencers.



Number of Unique Anomalies by Influencers

Viewing 1-5 of 5

10 CSV

Source Role	Influencer 1	Influencer 2	Influencer 3	Amount
tor	PortFECCorrectabl...	hist3	PortFECCorrected...	2
tor	hist2	hist3	PortFECCorrectabl...	2
tor	hist3	PortFECCorrectabl...	hist1	1
tor	hist3	phy_raw_errors_la...	PortFECCorrectabl...	2
tor	hist3	phy_raw_errors_la...	hist1	1

Global interactive and general filters can be applied by clicking on any entity in the dashboard.

Different times can be chosen by clicking on the last 12 hours.

Source GUID

Destination GUID

Source Role

Destination Role

Destination Type

Source Type

Influencer 1

Influencer 2

Influencer 3

Length

Clicking on reset will clear all of the filters.

Cable Anomalies Detection Specification Description

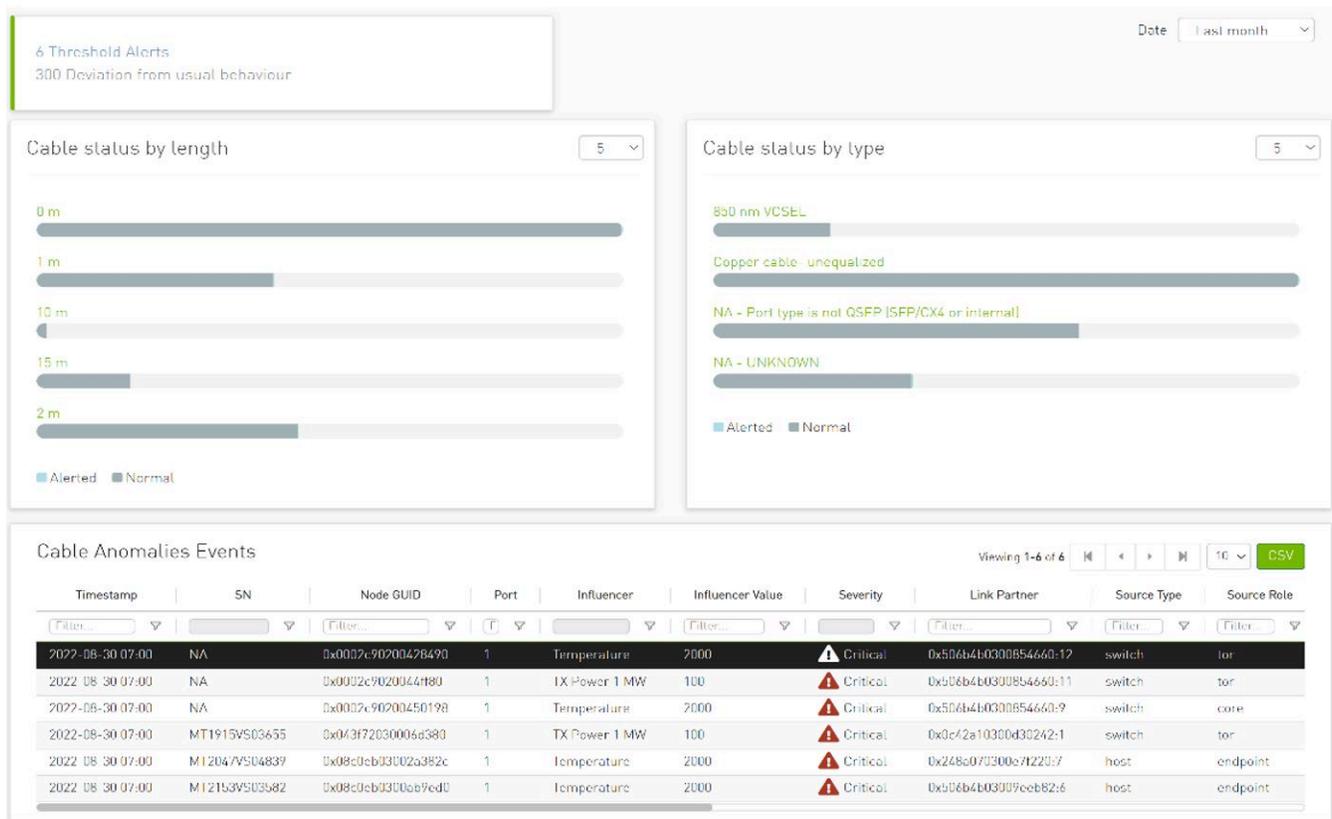
The present invention generally relates to the detection anomaly over cables and understanding degradation mechanisms for improving stability in data centers.

This innovation includes the detection of trends, intrusion, and any abnormal behavior of cables.

Moreover, with analysis of degradation over time we can determine better future performance strategies.

Customer Output

Threshold Alerts Tab



0x0002c90200428490

Prev Next

Recommended Actions

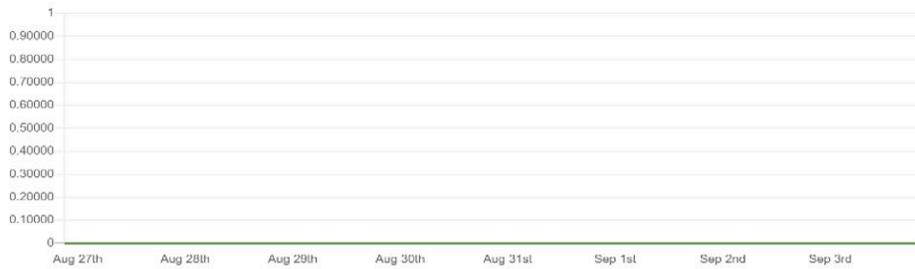
Site Name Local
 Time 2022-08-30 07:00
 Creation Time 2022-08-30 07:00
 Severity ▲ Critical
 Description Cable threshold event for 0x0002c90200428490:1:NA regarding temperature:2000.0

Recommended Actions

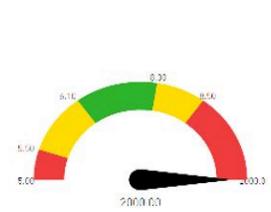
- Please check relevant cable measure trend
- If there are alerts for connected cable and/or deprecating trend please consider cable replacement
- If known issue due to maintenance activity please use suppress function do define as known issue

Trending

Trend over last month



Alert Tachometer



Deviation from Usual Behavior Tab

6 Threshold Alerts

300 Deviation from usual behaviour from 85 to 100

Date Last month

Cable Anomalies Deviation

Viewing 1-10 of 300

Timestamp ↓	Node GUID	Port	SN	Influencer	Influencer Value	Deviation from usual behaviour	Severity	Link Partner
2022-08-30 07:00	0x248a070300c01650	1	MT1712TT02630	TX Bias 1	0	100	● info	0x7cfe900300f73d20:14
2022-08-30 07:00	0x248a070300fb69a0	1	MT1551TT00309	TX Bias 1	0	100	● info	0x7cfe900300f73d20:10
2022-08-30 07:00	0x506b4b03008545a0	1	TW421200015	TX Power 1 MW	0	100	● info	0x7cfe900300b13740:18
2022-08-30 07:00	0x506b4b03009eeb82	1	MT1629FT00864	TX Bias 1	0	100	● info	0x7cfe900300f73e0:3
2022-08-30 07:00	0x506b4b03009eeeb02	1	MT1629FT00856	TX Bias 1	0	100	● info	0x7cfe900300f73e0:4
2022-08-30 07:00	0x7cfe900300a5bae40	1	IW421200017	TX Power 1 MW	0	100	● info	0x506b4b0300854660:9
2022-08-30 07:00	0x7cfe900300a5ba40	1	TW421200016	TX Power 1 MW	0	100	● info	0x506b4b0300854660:10
2022-08-30 07:00	0x7cfe900300b32c0	1	TW011401049	TX Power 1 MW	0	100	● info	0x248a070300e0d490:23
2022-08-30 07:00	0x7cfe900300b33f0	1	IW011401513	TX Power 1 MW	0	100	● info	0x248a070300e7240:16
2022-08-30 07:00	0x7cfe900300b37c0	1	TW421200020	TX Power 1 MW	0	100	● info	0x506b4b0300854660:25



Background Art

Cable Anomaly Detection

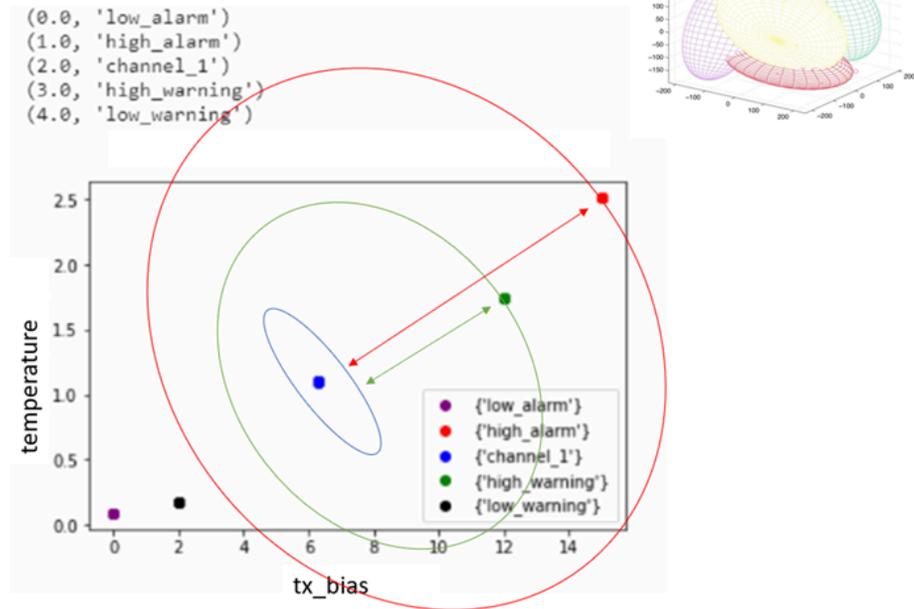
1. There are 5 measurements from the management tool (IB) with four thresholds per measure; see the Ethernet example below.

```

module_voltage
Channel_*_ tx_power
Channel_*_rx_power
Channel_*_tx_bias
      module_temp
  
```

2. There is a 5D (dimensions) GMM model which clusters channel and threshold behavior.

2D example of GMM model



3. To indicate alert: UFM Cyber-AI is calculating for every new data entry its deviation from channel centroid probabilistically per measurement.
4. The system is defining the probability rate for the indication above deviation
5. Each event per measurement is unique to node, port, and SN.
6. For user convenience, there is the representation of the current measure via pre-defined thresholds in the tachometer
7. For every chosen entry in the table, the trend graph is updated
8. The trend graph represents the trend for the chosen measure to detect abnormal behavior over time

Job Analytics

Introduction

Analytic jobs are critical components in CyberAI. Each analytic job has a specific task to accomplish and runs periodically in a docker container. They process raw data collected from UFM Telemetry and generate informative data that can be displayed to the user in a form of alerts that can be used in making decisions. The process of data includes splitting the data into chunks of 5 mins, calculating the delta (difference between counters values), aggregating data (hourly, day of week, topology, and PKey), and inference the data for any alerts.

Job Types

1. File Splitter: This job splits the file if it contains more than one timestamp.
2. Delta Processing: This job calculates the delta from the current sampling and the previous 5 minutes.
3. Hourly Aggregation: This job aggregates all delta files in the previous hour into one csv file.
4. Network Hourly Aggregation: Similar to hourly aggregation but, make average over all network nodes.
5. DOW Aggregation: Collect the CSV files on the same day of the week (DOW), at the same hour, to be aggregated.
6. Network DOW Aggregation: Similar to DOW aggregation but makes average over all network nodes.
7. Network Anomaly: Analyzes the network hourly data with the network DOW aggregation and looks for anomalies.
8. Topology Aggregation: Merges data collected from hourly aggregation, cables, and UFM topology files, and generates a file to be used by ML hourly aggregation.
9. ML hourly Anomaly: Analyzes the topology merged file using ML model files and looks for link anomalies alert
10. ML hourly model: Analyzes the topology merged file using ML model files and looks for link failure prediction Alert
11. ML Weekly Aggregation: Updates the ML model used by ML hourly aggregation based on the weekly collected topology.

12. PKEY Port Join: Merges the delta output files with the PKEY data and generates a file to be input for the PKEY aggregation.
13. PKEY Aggregation: Analyzes the joined PKEY data and looks for PKEY (tenant) alerts.
14. Logical Server Join: Merges the delta output files with the logical server data and generates a file to be input for the logical server aggregation.
15. Logical Servers Aggregation: Analyzes the joint logical servers data and looks for logical servers alerts.
16. Cable Daily: Analysis of cable counters files and looks for cable threshold and deviation alerts.
17. Weekly Aggregation: Makes weekly average on hourly data to be displayed to compare the hourly data with the weekly average of this hour.

Output Sample

The screenshot displays the 'Job Analytics' section of the NVIDIA UFM Cyber AI interface. The table lists various jobs with their configurations and execution details.

Job Name	Type	Frequency (seconds)	Last Run	Last Run Status	Total Runs	Total Successful Runs	Next Run	Dependencies	Summary
file_splitter	File Splitter	300	2021-10-01 16:05:54	Completed			2021-10-01 16:10:54	Port counters	
delta_proc	Delta Processing	300	2021-10-01 16:10:50	New			2021-10-01 16:15:50	File Splitter	
hourly_agg	Hourly Aggregation	3600	2021-10-03 16:06:50	Completed			2021-10-03 17:06:50	Delta Processing	/opt/ufm/cyber-ai/6
con_agg	DDW Aggregation	86400	2021-10-04 16:07:49	Completed			2021-10-05 16:07:49	Hourly Aggregation	/opt/ufm/cyber-ai/6
topology_agg	Topology Aggregation	3600	2021-10-03 21:04:54	Completed			2021-10-03 22:04:54	Hourly Aggregation.T...	
ml_hourly_agg	ML Hourly Aggregation	3600					2021-09-30 17:07:04	Topology Aggregation	
pkey_port_join	Pkey Port Join	300	2021-10-01 16:16:49	Completed			2021-10-01 16:21:49	Delta Processing.PK...	/opt/ufm/cyber-ai/6
pkey_agg	PKEY Aggregation	300	2021-09-30 18:02:49	Completed			2021-09-30 18:07:49	Pkey Port Join	/opt/ufm/cyber-ai/6
ml_weekly_agg	ML Weekly Aggregation	604800					2021-10-07 16:08:04		
network_hourly_agg	Network Hourly Aggregat...	3600	2021-10-02 17:07:07	New			2021-10-02 18:07:07	Delta Processing	/opt/ufm/cyber-ai/6

REST API

- [Session Management](#)
- [User Management](#)
- [System Details](#)
- [Application Details](#)
- [Configuration](#)
- [Analytics](#)
- [Suspicious Behavior](#)
- [Link Analysis](#)
- [Resources](#)
- [Telemetry Data](#)
- [Alert Filters](#)

Session Management

Login

- URL

```
POST /cyber-ai/login
```

- Request Data

```
login=<username>&password=<password>
```

- Response – if successful, a session is created and a cookie with the session data is returned to the client
- Response codes:

Status	Description
302	Found (login success)
401	Unauthorized (login failure)

Logout

- URL

```
POST /cyber-ai/logout
```

- Request Data

```
None
```

- Response codes:

Status	Description
200	Success
401	Unauthorized

User Management

Get User/All Users

- URL

```
GET /cyber-ai/users/  
GET /cyber-ai/users/{username}
```

- Request Data

```
none
```

- Response – for all users, it returns a list, while for single user it returns single object

```
[  
  {  
    "username": "admin",  
    "pwd": "*****",  
    "role": "Admin"  
  }  
]
```

- Response codes:

Status	Description
200	Success
404	Not found

Add User

- URL

```
POST /cyber-ai/users
```

- Request data

```
{  
  "username": "johns",  
  "pwd": "drowssap",  
  "role": "User"  
}
```

Supported Roles: Admin/User

- Response codes:

Status	Description
201	Created
409	Conflicted

Modify User/Change Password

Users can change their own password only. Admins can modify both passwords and roles.

- URL

```
PATCH /cyber-ai/users/{username}
```

- Request data – just `pwd` and/or `role` can be used in the request

```
{  
  "pwd": "drowssap",  
}
```

```
}
```

- Response

```
none
```

- Response codes:

Status	Description
200	Success
400	Bad request
403	Forbidden
404	Not found

Delete User

- URL

```
DELETE /cyber-ai/users/{username}
```

- Request data

```
none
```

- Response

```
none
```

- Response codes:

Status	Description
204	No content (success)
403	Forbidden
404	Not found

UFM Telemetry

- URL

```
GET /cyber-ai/system/ufm-telemetry
```

- Request Data

```
none
```

- Response: number of collected results for port counters and cable information

```
{
  "port_counters": 20,
  "cable_info": 8
}
```

- Response codes

Status	Description
200	Success

UFM Enterprise

- URL

```
GET /cyber-ai/system/ufm-enterprise
```

- Request Data

```
none
```

- Response codes

Status	Description
200	Ok

Run Analytic Job

- URL

```
POST /cyber-ai/system/analytic-jobs
```

- Request Data

```
{  
  "job_type": "delta_proc"  
}
```

- Response details regarding the fabric

```
none
```

- Response codes

Status	Description
201	Created
400	Bad Request (invalid argument)

Get Analytic Jobs statistics

- URL

```
GET /cyber-ai/system/analytic-jobs
```

- Request Data

```
none
```

- Response details regarding the fabric

```
[
  {
    "job_name": "file_splitter",
    "job_type": "File Splitter",
    "frequency": 300,
    "runs": 50,
    "successful_runs": 40,
    "last_run_status": "Success",
    "last_run_time": 1631520596.290813,
    "next_run_time": 1631520596.290813,
    "summary": "",
    "dependencies": "Port counters"
  },
  ...
]
```

```
]
```

- Response codes

Status	Description
200	Ok
400	Bad Request (invalid argument)

Cyber-Ai Release Version

- URL

```
GET /cyber-ai/app/version
```

- Request Data

```
none
```

- Response

```
{  
  "release_version": "0.9.4-6"  
}
```

- Response codes

Status	Description
200	Ok

License Details

- URL

```
GET /cyber-ai/app/license
```

- Request Data

```
none
```

- Response

```
{  
  "license_functionality": "functionality",  
  "customer_num": "123456789",  
  "serial_num": "987654321",  
  "license_type": "type",  
  "expiration_date": "2090-09-08"  
}
```

- Response codes

Status	Description
200	Ok

Configuration

Set UFM Enterprise Connections Parameters

- URL

```
PUT /cyber-ai/config/ufm-params
```

- Request data

```
{  
  "password": "qwerty",  
  "ip": "10.210.4.57",  
  "username": "admin",  
  "protocol": "[http|https]"  
  "port": 443  
}
```

- Response codes

Status	Description
204	Success
400	Bad request

Get UFM Enterprise Connections Parameters

- URL

```
GET /cyber-ai/config/ufm-params
```

- Request data

```
none
```

- Response

```
none
```

- Response codes

Status	Description
200	Success

Alert Count Summary

- URL

```
GET /cyber-ai/analytics/summary
```

- URL filters

- From – retrieve alerts triggered within the last given time period

```
from=-<time>
```

Note

Supported time units: h (for hours), d (for days), w (for weeks), m (for months). For example: from=-6h.

- Probability – returns all alerts with probability equal to, or greater than the given probability

```
min_probability=<0-100>
```

- Request data

```
none
```

- Response

```
{
  "network_alerts": {
    "Critical": 422,
    "Major": 10,
    "Minor": 0,
    "Warning": 0,
    "Suspect": 0,
    "Info": 0,
    "Notice": 0
  },
  "tenant_alerts": {...},
  "link_failures_predictions": {...},
},
"link_anomaly_predictions": {...},
"cable_events": {...},
  "logical_server_alerts": {...},
}
}
```

 **Note**

If successful, the analytics summary will be returned in JSON format.

- Response codes

Status	Description
204	Success
400	Bad request

Cable Distribution Count

Cable Length

- URL

```
GET /cyber-ai/analytics/distribution/cable-length
```

- URL filters
 - `from` – retrieve cable distributions based on cable’s length with alerts counts from a specific time:
 - `to` - retrieve cable distributions based on cable’s length with alerts counts until a specific time
 - `min_probability` – retrieve cable distributions with larger than or equal minimum probability
 - `max_probability` – retrieve cable distributions with less than or equal maximum probability

```
from=-<time>&to=-<time>&min_probability=<[0-100]>&max_probability=<[0-100]>
```

- Request data

```
none
```

- Response

```
{
  "20": {
    "normal": 2090,
    "alerted": 212
  },
  "30": {
    "normal": 968,
    "alerted": 487
  }
}
```

- Response codes

Status	Description
200	Success
400	Bad request

Cable Technology Type

- URL

```
GET /cyber-ai/analytics/distribution/cable-type
```

- URL filters

- from – retrieve cable distributions based on cable’s length with alerts counts from a specific time:
- to - retrieve cable distributions based on cable’s length with alerts counts until a specific time
- `min_probability` – retrieve cable distributions with larger than or equal minimum probability
- `max_probability` – retrieve cable distributions with less than or equal maximum probability

```
from=-<time>&to=-<time>&min_probability=<[0-100]>&max_probability=<[0-100]>
```

- Request data

```
none
```

- Response codes

Status	Description
200	Success
400	Bad request

Alert Count Summary

- URL

```
GET /cyber-ai/analytics/summary
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).
For example: `?from=-6h`.

- Probability – return all alerts with probability equal to, or greater than the given probability

```
?min_probability=<0-100>
```

- Request Data

```
none
```

- Response

```
{
  "network_alerts": {
    "Critical": 422,
    "Major": 10,
    "Minor": 0,
    "Warning": 0,
    "Suspect": 0,
    "Info": 0
  },
  "tenant_alerts": {{...}},
  "Critical": 11,
```

```

    "Major": 10,
    "Minor": 0,
    "Warning": 7
  },
  "link_failures_predictions": {{...}},
  },
  "link_anomaly_predictions": {...},
  "cable_events": {{...}}
}
}

```

(i) Note

If successful, the analytics summary is returned in JSON format.

- Response codes

Status	Description
200	Success
400	Bad Request (invalid argument)

Cables Distribution Counts

Cable Length

- URL

```
GET /cyber-ai/analytics/distribution/cable-length
```

- URL filters:

- From – retrieve cable distributions based on cable’s length with alerts counts from a specific time:

```
?from=-<time>
```

- Request Data

```
none
```

- Response

```
{
  "20" : {
    "normal" : 2090,
    "alerted" : 212
  },
  "30" : {
    "normal" : 968,
    "alerted" : 487
  }
}
```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)

Cable Technology Type

- URL

```
GET /cyber-ai/analytics/distribution/cable-type
```

- URL filters
 - From – retrieve cable distributions based on cable’s technology with alerts counts from a specific time:

```
?from=-<time>
```

- Request Data

```
none
```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)

Suspicious Behavior

Get All Network Alerts

- URL

```
GET /cyber-ai/anomalies/network
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).
For example: `?from=-6h`.

- Severity – retrieve only alerts with a severity included in the list:

```
?severities=<comma-separated list of severities>
```

Supported severity types: Critical, Major, Minor, Warning, Info.

- Request data

```
none
```

- Response

```
{
  [
    "alert_id": 2001,
    "timestamp": "Mon Sep 7 07:54:17 2020",
    "network_name": "default",
    "severity": "Critical",
    "probability": 85,
      "percentage": 60
    "influencers": [
      "infl1",
      "infl2",
      "infl3"
    ]
  ]
}
```

```
    ],
    "description": "Suspicious network behavior is detected
in your cluster",
  ]
}
```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)

Get Specific Network Alert

- URL

```
GET /cyber-ai/anomalies/network/<alert_id>
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).

For example: `?from=-6h`.

- Request data

```
none
```

- Response

```
{
  "alert_id": 39241,
  "occurrence": "1 time during the last 2 hours",
  "severity": "Warning",
  "description": "port_xmit_wait is 2735.23% above the
average",
  "full_description": "port_xmit_wait:132470536 is above the
average: 4672298",
  "influencers": [
    "port_xmit_wait"
  ],
  "recommended_actions": [
    "These steps should be applied on top 5 ports",
    "Port reset and keep monitoring",
    "If still getting the alerts, please check if there any
related cable alerts via cable anomaly tab",
    "In addition, please check relevant cable measure trend
via cable anomaly tab",
    "If there are alerts for connected cable and/or
depredating trend please consider cable replacement",
    "If known issue due to maintenance activity please use
suppress function do define as known issue"
  ],
  "percentage": 2735.23,
  "nodes": [
    {
      "port_guid": "0x24be05ffffc13011",
      "port_xmit_wait": 467264335.5705527,
      "port_name": "HCA-1/1",
      "node_guid": "0x24be05ffffc13010",
      "system_name": "mtlx319",
      "type": "switch",
      "role": "tor"
    }
  ]
}
```

```

    },
    {
      "port_guid": "0x98039b03006c6912",
      "port_xmit_wait": 466359722.25149757,
      "port_name": "1",
      "node_guid": "0x98039b03006c6912",
      "system_name": "mtlx473",
      "type": "host",
      "role": "endpoint"
    }
  ],
  "first_occurrence_timestamp": "2022-09-21 13:00",
  "influencers_display_names": [
    "Port Xmit Wait"
  ],
  "timestamp": "2022-09-21 13:00"
}

```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)
404	Not found

Get All Tenant/Application Alerts

- URL

```
GET /cyber-ai/anomalies/tenant
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).
For example: `?from=-6h`.

- Severity – retrieve only alerts with a severity included in the list:

```
?severities=<comma-separated list of severities>
```

Supported severity types: Critical, Major, Minor, Warning, Suspect, Info.

- Request data

```
none
```

- Response

```
{
  [
    "alert_id": 3001,
    "timestamp": "Mon Sep 7 07:53:45 2020",
    "tenant_id": "0x0004",
    "severity": "Critical",
    "probability": 85,
    "influencers": [
      "infl1",
      "infl2",
      "infl3"
    ],
  ],
}
```

```
    "description": "Inefficient network utilization for PKey  
0x0004"  
  ]  
}
```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)

Get Specific Tenant Alert

- URL

```
GET /cyber-ai/anomalies/tenant/<alert_id>
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).

For example: `?from=-6h`.

- Request data

```
none
```

- Response

```
[
  "alert_id": 3001,
  "timestamp": "Mon Sep 7 07:54:17 2020",
  "tenant_id": "0x0004",
  "severity": "Critical",
  "probability": 85,
  "influencers": [
    "infl1",
    "infl2",
    "infl3"
  ],
  "description": "Inefficient network utilization for PKey
0x0004",
  "occurrence": "9 times during the last 24 hours",
  "recommended_actions": "It seems that your placement
engine/job scheduler did not allocate the best nodes for this
job",
  "nodes": [
    {
      "node_guid": "0x24be05ffffc13010",
      "system_name": "mtlx319",
      "type": "switch",
      "role": "tor"
    },
    {
      "node_guid": "0x98039b03006c6912",
      "system_name": "mtlx473",
      "type": "host",
      "role": "endpoint"
    }
  ]
}
```

- Response codes

Status	Description
200	Success
404	Not found

Get Logical Server Alerts

- URL

```
GET /cyber-ai/anomalies/ logical-server
```

- URL filters

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).

For example: `?from=-6h`.

- Severity – retrieve only alerts with a severity included in the list:

```
?severities=<comma-separated list of severities>
```

Supported severity types: Critical, Major, Minor, Warning, Suspect, Info and Notice.

- Request data

```
none
```

- Response

```
[
  {
    "alert_id": 1,
    "logical_server": "LS_test",
    "severity": "Critical",
    "description": "Logical server test_ls is utilized above
71.54%",
    "influencers": [
      "utilization",
      "port_xmit_data",
      "port_rcv_data"
    ],
    "influencers_display_names": [
      "Utilization",
      "Port Xmit Data",
      "Port Received Data"
    ],
    "timestamp": "2022-02-21 18:10"
  }
]
```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)

Get Specific Logical Server Alert

- URL

```
GET /cyber-ai/anomalies/logical-server/<alert_id>
```

- Request data

```
none
```

- Response

```
{
  "alert_id": 1,
  "logical_server": "LS_test",
  "severity": "Critical",
  "description": "Logical server test_ls is utilized above
71.54%",
  "influencers": [
    "utilization",
    "port_xmit_data",
    "port_rcv_data"
  ],
  "influencers_display_names": [
    "Utilization",
    "Port Xmit Data",
    "Port Received Data"
  ],
  "timestamp": "2022-02-21 18:10"
}
```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)

Cables Alerts

Cable Alerts Summary

- URL

```
GET /cyber-ai/anomalies/cable/summary
```

- Filters
 - from
 - to
 - min_deviation
 - max_deviation

- Request Data

```
none
```

- Response

```
{
  'cable_threshold_events': {
    'Critical': 6,
    'Major': 0,
    'Minor': 0,
    'Warning': 0,
    'Suspect': 0,
    'Info': 0,
    'Notice': 0
  },
  'cable_deviation_events': {
    'Critical': 0,
```

```
'Major': 0,  
'Minor': 0,  
'Warning': 0,  
'Suspect': 0,  
'Info': 5,  
'Notice': 0  
}  
}
```

- Response Code

Status	Description
200	Success
400	Bad request (invalid argument)

Threshold Events

- URL

```
GET /cyber-ai/anomalies/cable/threshold
```

- Filters
 - from
 - to
 - sn
 - guid
 - severity
 - influencers

- port
- channel
- brief
- Request data

```
none
```

- Response

```
"alert_id": 1,  
"occurrence": 179,  
"node_guid": "0x0010e0000187dce9",  
"port": 1,  
"link_partner": "0x506b4b0300623360:7",  
"source_type": "switch",  
"source_role": "tor",  
"destination_type": "switch",  
"destination_role": "tor",  
"sn": "NA",  
"speed": "NA",  
"cable_info": "850 nm VCSEL",  
"description": "Cable Failure for 0x0010e0000187dce9:1:NA regarding tx_bias.1:0.0",  
"severity": "Critical",  
"influencers": [  
    "tx_bias.1"  
],  
"influencers_values": [  
    0  
],  
"channel": 1,  
"influencers_display_names": [  
    "TX Bias"
```

```
    ],  
    "timestamp": "2022-06-18 00:00"  
  }, ...
```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)

Specific Threshold Event

- URL

```
GET /cyber-ai/anomalies/cable/threshold/<event_id>
```

- Request data

```
none
```

- Response

```
{  
  "alert_id": 1,  
  "occurrence": 179,  
  "node_guid": "0x0010e0000187dce9",  
  "port": 1,  
  "link_partner": "0x506b4b0300623360:7",  
  "source_type": "switch",
```

```

"source_role": "tor",
"destination_type": "switch",
"destination_role": "tor",
"sn": "NA",
"speed": "NA",
"cable_info": "850 nm VCSEL",
"description": "Cable Failure for 0x0010e0000187dce9:1:NA regarding tx_bias.1:0.0",
"severity": "Critical",
"influencers": [
    "tx_bias.1"
],
"influencers_values": [
    0
],
"channel": 1,
"influencers_display_names": [
    "TX Bias"
],
"timestamp": "2022-06-18 00:00"
}

```

- Response codes

Status	Description
200	Success

Threshold Event Tachometer

- URL

```
GET /cyber-ai/anomalies/cable/threshold/<event_id>/meter
```

- Request data

```
none
```

- Response

```
{  
  "high_alarm_range": [8.5, 9],  
  "high_warning_range": [8, 8.5],  
  "normal_range": [6.1, 8],  
  "low_warning_range": [5.5, 6.1],  
  "low_alarm_range": [5, 5.5]  
}
```

- Response codes

Status	Description
200	Success

Deviation Events

- URL

```
GET /cyber-ai/anomalies/cable/deviation
```

- Filters
 - from
 - to

- sn
 - guid
 - severity
 - influencers
 - port
 - channel
 - min_deviation
 - max_deviation
 - brief
- Request data

None

- Response

```
[
{
  "alert_id": 1,
  "occurrence": 179,
  "node_guid": "0x0010e0000187dce9",
  "port": 1,
  "link_partner": "0x506b4b0300623360:7",
  "source_type": "switch",
  "source_role": "tor",
  "destination_type": "switch",
  "destination_role": "tor",
  "sn": "NA",
  "speed": "NA",
```

```

    "cable_info" : "850 nm VCSEL",
    "description" : "Cable Failure for 0x0010e0000187dce9:1:NA regarding tx_bias.1:0.0",
    "deviation" : 69.14892243,
    "severity" : "Critical",
    "influencers" : [
        "tx_bias.1"
    ],
    "influencers_values" : [
        0
    ],
    "channel" : 1,
    "influencers_display_names" : [
        "TX Bias"
    ],
    "timestamp" : "2022-06-18 00:00"
}, ...
]

```

- Response codes

Status	Description
200	Success
400	Bad request (invalid argument)

Specific Deviation Event

- URL

```
GET /cyber-ai/anomalies/cable/deviation/<event_id>
```

- Request data

none

- Response

```
{
  "alert_id": 1,
  "occurrence": 179,
  "node_guid": "0x0010e0000187dce9",
  "port": 1,
  "link_partner": "0x506b4b0300623360:7",
  "source_type": "switch",
  "source_role": "tor",
  "destination_type": "switch",
  "destination_role": "tor",
  "sn": "NA",
  "speed": "NA",
  "cable_info": "850 nm VCSEL",
  "description": "Cable Failure for 0x0010e0000187dce9:1:NA regarding tx_bias.1:0.0",
  "deviation": 69.14892243,
  "severity": "Critical",
  "influencers": [
    "tx_bias.1"
  ],
  "influencers_values": [
    0
  ],
  "channel": 1,
  "influencers_display_names": [
    "TX Bias"
  ],
  "timestamp": "2022-06-18 00:00"
}
```

- Response codes

Status	Description
200	Success

Link Analysis

Get All Link Failure Predictions

- URL

```
GET /cyber-ai/prediction/link-failure
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).

For example: `?from=-6h`.

- Severity – retrieve only alerts with a severity included in the list:

```
?severities=<comma-separated list of severities>
```

Supported severity types: Critical, Major, Minor, Warning, Info.

- Request data

none

- Response

```
[
  {
    "alert_id": 4001,
    "timestamp": "Mon Sep 7 06:52:17 2020",
    "node_guid": "0x44556677adbf0121",
    "node_name": "k11r2n03 HCA-1",
    "port": 1,
    "port_name": "k11r2n03 HCA-1:1",
    "severity": "Critical",
    "probability": 85,
    "influencers": [
      "infl1",
      "infl2",
      "infl3"
    ],
    "description": "Link failure prediction detected on port
k15r1n03 HCA-1"
  }
]
```

- Response codes

Status	Description
200	Success
400	Bad Request

Get Specific Link Failure Prediction

- URL

```
GET /cyber-ai/prediction/link-failure/<alert_id>
```

- URL filters:

- Severity – retrieve only alerts with a severity included in the list:

```
?severities=<comma-separated list of severities>
```

- Probability – return all predictions with probability equal to, or greater than the given probability

```
?min_probability=<0-100>
```

- Request data

```
none
```

- Response

```
{
  "alert_id": 4001,
  "timestamp": "Mon Sep 7 06:52:17 2020",
  "node_guid": "0x44556677adbf0121",
  "node_name": "k11r2n03 HCA-1",
  "port": 1,
  "port_name": "k11r2n03 HCA-1:1",
  "severity": "Critical",
```

```

    "probability": 85,
    "influencers": [
      "infl1",
      "infl2",
      "infl3"
    ],
    "description": "Link failure prediction detected on port
k15r1n03 HCA-1",
    "occurrence": "9 times during the last 24 hours",
    "recommended_actions": "The temperature of the peer switch
is very high. Please check that all fans of the peer switch
are working properly"
  }

```

- Response codes

Status	Description
200	Success
400	Bad Request
404	Not Found

Get All Link Anomaly Predictions

- URL

```
GET /cyber-ai/prediction/link-anomaly
```

- URL filters:
 - From – retrieve predictions triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).
For example: `?from=-6h`.Severity – retrieve only predations with a severity included in the list

- o Probability – return all predictions with probability equal to, or greater than the given probability

```
?min_probability=<0-100>
```

- Request Data

```
none
```

- Response

```
[
  {
    "alert_id": 4001,
    "timestamp": "Mon Sep 7 06:52:17 2020",
    "node_guid": "0x44556677adbf0121",
    "node_name": "k11r2n03 HCA-1",
    "port": 1,
    "port_name": "k11r2n03 HCA-1:1",
    "severity": "Critical",
    "probability": 85,
    "influencers": [
      "infl1",
      "infl2",
      "infl3"
    ]
  }
]
```

```
    ],
    "description": "Link failure prediction detected on port
k15r1n03 HCA-1"
  }
]
```

- Response codes

Status	Description
200	Success
400	Bad Request

Get Specific Link Anomaly Prediction

- URL

```
GET /cyber-ai/prediction/link-anomaly/{alert_id}
```

- URL filters:

- Probability – return all predictions with probability equal to, or greater than the given probability

```
?min_probability=<0-100>
```

- Severity – retrieve only alerts with a severity included in the list:

```
?severities=<comma-separated list of severities>
```

Supported severity types: Critical, Major, Minor, Warning, Info.

- Request Data

```
none
```

- Response

```
{
  "alert_id": 1,
  "occurrence": "1 time during the last 30 days and 14
hours",
  "node_guid": "0xb8599f0300ec8780",
  "node_name": "0xb8599f0300ec8780",
  "node_type": "hca",
  "port": 1,
  "severity": "Warning",
  "description": "Anomaly detected for
0xb8599f0300ec8780:1 regarding hist2,hist1,hist3",
  "full_description": "Anomaly detected for
0xb8599f0300ec8780:1 regarding hist2,hist1,hist3",
  "influencers":[
    "hist2",
    "hist1",
    "hist3"
  ],
  "probability": 9.48048404228375e-05,
  "hours_to_fail": 0,
  "recommended_actions": "Anomaly detected for
0xb8599f0300ec8780:1 regarding hist2,hist1,hist3",
  "port_name": "0xb8599f0300ec8780:1",
  "influencers_display_names":[
    "Histogram 2",
    "Histogram 1",
    "Histogram 3"
  ]
}
```

```
    ],  
    "timestamp": "2021-08-16 00:00"  
  }  
}
```

- Response codes

Status	Description
200	Success
404	Not Found

Events Flows

- URL

```
GET /cyber-ai/prediction/link-anomaly/analysis/events_flow
```

- URL filters:
 - from
 - to
 - min_probability
 - max_probability
 - src
 - guid
 - dst
 - guid
 - src_role
 - dst_role

- dst_type
 - src_type
 - influencer1
 - width
 - cable_type
 - fw_ver
 - rev
 - cable_pn
 - length
 - influencer2
 - influencer3
- Request Data

```
none
```

- Response

```
[[{  
  "src_guid": "0x0c42a1030001f494",  
  "dst_guid": "0xb8599f0300f61696",  
  "src_type": "host",  
  "dst_type": "switch",  
  "count": 8  
}]
```

- Response codes

Status	Description
200	Success
400	Bad request

Elements

- URL

```
GET /cyber-ai/prediction/link-anomaly/analysis/elements
```

- Request data

```
none
```

- Response

```
[{
  "src_type": "host",
  "src_role": "endpoint",
  "dst_type": "switch",
  "dst_role": "tor",
  "length": 1,
  "cable_pn": "0000001PG737",
  "rev": "A1",
  "fw_ver": "NA",
  "cable_type": "Copper cable- unequalized",
  "width": "4x",
  "src_nic_type": "ConnectX-6",
  "count": 2
}]
```

- Response codes

Status	Description
200	Success
400	Bad request

Timeline

- URL

```
GET /cyber-ai/prediction/link-anomaly/analysis/timeline
```

- URL filters:

- from
- to
- src
- guid
- dst
- guid
- src_role
- dst_role
- dst_type
- src_type
- influencer1
- width
- cable_type

- fw_ver
- rev
- cable_pn
- length
- influencer2
- influencer3
- Request Data

```
none
```

- Response

```
[{
  "time": 1638889200,
  "count": 301
}]
```

- Response codes

Status	Description
200	Success
400	Bad request

Influencers

- URL

```
GET /cyber-ai/prediction/link-anomaly/analysis/influencers
```

- URL filters:
 - from
 - to
 - src
 - guid
 - dst
 - guid
 - src_role
 - dst_role
 - dst_type
 - src_type
 - influencer1
 - width
 - cable_type
 - fw_ver
 - rev
 - cable_pn
 - length
 - influencer2
 - influencer3

- Request Data

```
none
```

- Response

```
[{  
  "src_role": "core",  
  "count": 1,  
  "influencer1": "PortFECCorrectableBlockCounter",  
  "influencer2": hist2,  
  "influencer3": hist3  
}]
```

- Response codes

Status	Description
200	Success
400	Bad request

Resources

Get Top 10 Nodes by Link Failure Indication

- URL

```
GET /cyber-ai/resources/nodes/top-link-failure
```

- URL filters:

- `from` – retrieve nodes with triggered link failures within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).
For example: `?from=-6h`.

- `Probability` – return all nodes whose link failures with probability equal to, or greater than the given probability

```
?min_probability=<0-100>
```

- `count` – retrieve specific number of nodes
- `Severity` – retrieve nodes based on the severity of link failures:

```
?severities=<comma-separated list of severities>
```

- `Node Type` – retrieve nodes based on the type (“host”, “switch”)

```
?node_type=<type>
```

- Request

```
none
```

- Response

```
[
  {
    "failure_indications": 1,
    "port_name": "0x506b4b03005c2360:7"
  },
  {
    "failure_indications": 1,
    "port_name": "0x506b4b0300623360:8"
  },
  {
    "failure_indications": 1,
    "port_name": "0x506b4b03006c1f20:13"
  }
]
```

- Response codes

Status	Description
200	Success
400	Bad Request (invalid argument)

Get Anomaly Nodes

- URL

```
GET /cyber-ai/resources/nodes/anomaly
```

- URL filters:
 - From – retrieve nodes whose triggered alerts within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).

For example: `?from=-6h`.

- Probability – return all alerts with probability equal to, or greater than the given probability

```
?min_probability=<0-100>
```

- Severity – retrieve only alerts with a severity included in the list:

```
?severities=<comma-separated list of severities>
```

- Request

```
none
```

- Response

```
{}
```

- Response codes

Status	Description
200	Success

Get Anomaly Cables

- URL

```
GET /cyber-ai/resources/cable/anomaly
```

- URL filters:

- From – retrieve cables whose triggered alerts within the last given time period

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).
For example:

```
?from=-6h.
```

- Request

```
none
```

- Response

```
    "nodes" :
    {
        "anomaly" : 473,
        "normal" : 1663
    },
    "switches" :
    {
        "anomaly" : 31,
```

```
    "normal": 167
  }
}
```

- Response codes

Status	Descriptions
200	Success
400	Bad Request (invalid argument)

Get Tenants Allocation

- URL

```
GET /cyber-ai/resources/tenant/allocation
```

- Request

```
none
```

- Response

```
{
  "allocated": 15,
  "free": 993
}
```

- Response codes

Status	Description
200	Success

Get Tenant Nodes

- URL

```
GET /cyber-ai/resources/tenant/{tenant_id}/nodes
```

- Request

```
none
```

- Response

```
[
  {
    "port_guid": "0xec0d9a03008460a6",
    "port_name": "HCA-2/1",
    "system_name": "nia-m4-bb02",
    "utilization": 15.4
  },
  {
    "port_guid": "0xec0d9a0300845e6a",
    "port_name": "HCA-2/1",
    "system_name": "nia-m4-bb06",
    "utilization": 15.4
  }
]
```

- Response code

Status	Description
200	Success

Get Top Congested Tenants/Applications

- URL

```
GET /cyber-ai/resources/tenant/top-congested
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).

For example: `?from=-6h`.

- Count – retrieve specific number of nodes

```
?count=<integer larger than 0>
```

- Request

```
none
```

- Response

```
[
```

```
{
  "tenant_id": "0x0001",
  "congestion": 4
}{
  "tenant_id": "0x0003",
  "congestion": 3
}{
  "tenant_id": "0x0005",
  "congestion": 2
}
]
```

- Response codes

Status	Description
200	Success
400	Bad Request

Get Logical Servers Allocation

- URL

```
GET /cyber-ai/resources/logical-server/allocation
```

- Request

```
none
```

- Response

```
{
```

```
"allocated": 15,  
"free": 2131  
}
```

- Response codes

Status	Description
200	Success
400	Bad request

Get Top Congested Logical Servers

- URL

```
GET /cyber-ai/resources/logical-server/top-congested
```

- URL filters

- From – retrieve alerts triggered within the latest given time period:

```
?from=-<time>
```

Note

Supported time units: h (for hours), d (for days), w (for weeks) and m (for months). For example: ?from=-6h.

- Count – retrieve a specific number of nodes

```
?count=<integer larger than 0>
```

- Request

```
none
```

- Response

```
[  
  {  
    "logical_server": "LS",  
    "utilization": 0.0315922587555555  
  },  
  {  
    "logical_server": "LS_test",  
    "utilization": 0.0060010954666666  
  }  
]
```

- Response codes

Status	Description
200	Success
400	Bad request

Get Link Anomalies

- URL

```
GET /cyber-ai/resources/link-anomaly
```

- URL filters:

- Influencers:

```
?influencers=<comma-separated list of influencers>
```

- Request

```
none
```

- Response

```
[  
  {  
    "name": "v115_dropped",  
    "description": "Number of incoming VL15 packets  
dropped due to resource limitations (e.g., lack of  
buffers) in the port."  
  }  
]
```

- Response codes

Status	Description
200	Success
400	Bad Request

Get Link Anomalies For influencer

- URL

```
GET /cyber-ai/resources/link-anomaly/{influencer}
```

- Request

```
none
```

- Response

```
{
  "name": "v115_dropped",
  "description": "Number of incoming VL15 packets dropped
due to resource limitations (e.g., lack of buffers) in the
port."
}
```

- Response codes

Status	Description
200	Success
404	Not Found

Telemetry Data

Get the Telemetry Counter list

- URL

```
GET /cyber-ai/telemetry/counters?type=<type>
```

Allowed Types:

- Link
 - Cable
 - Network
 - Tenant
 - Logical-server
- Request Data

```
None
```

- Response

```
{  
  "LinkDownedCounterExtended": "Link Downed Counter Extended",  
  "MaxRetransmissionRate": "Max Retransmission Rate",  
  "PortBufferOverrunErrors": "Port Buffer Overrun Errors",  
  "PortDLIDMappingErrors": "Port DLID Mapping Errors",  
  "PortFECCorrectableBlockCounter": "Port FEC Correctable Block Counter",  
  "PortFECCorrectedSymbolCounter": "Port FEC Corrected Symbol Counter",  
  "PortFECUncorrectableBlockCounter": "Port FEC Uncorrectable Block Counter",  
  ...  
}
```

Get Network Counter's Telemetry Data

- URL

```
GET /cyber-ai/telemetry/network/traffic?period=<period_type>
```

Where `period_type` can be:

- `weekly_average`
- `last_week`
- `current_week`

- Request Data

```
none
```

- Response

```
[  
  {  
    "time": "06:00:00",  
    "DOW": "Wed",  
    "value": 50  
  },  
  {  
    "time": "07:00:00",  
    "DOW": "Wed",  
    "value": 45  
  }  
]
```

Get Tenant Telemetry Data

- URL for tenant

```
GET /cyber-ai/telemetry/tenant/{tenant_id}/{counter}
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).
For example: `?from=-6h`.

- To – retrieve telemetry data for a given time point:

```
?to=-<time>
```

- Request Data

```
none
```

- Response

```
[  
  {  
    "time": "06:00:00",  
    "value": 45  
  },  
  {  
    "time": "07:00:00",
```

```
    "value": 55
  }
]
```

- Response codes

Status	Description
200	Success
400	Bad Request (invalid argument)

Get Tenant Network Telemetry Data

- URL

```
GET /cyber-ai/telemetry/tenant/network/{counter}
```

- URL filters:

- margin – retrieve telemetry data from a given time point:

```
?margin=<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).
For example: `? margin=1d`.

- Time Per Tenant

```
?time_per_tenant=<tenant_id>
```

- Request Data

```
none
```

- Response

```
[  
  {  
    "time": "06:00:00",  
    "value": 45  
  },  
  {  
    "time": "07:00:00",  
    "value": 55  
  }  
]
```

- Response codes

Status	Description
200	Success
400	Bad Request (invalid argument)

Get Logical Servers Telemetry Data

- URL for tenant

```
GET /cyber-ai/telemetry/logical-  
server/<logical_server_id>/{counter}
```

- URL filters
 - From – retrieve telemetry data within the latest given time period

```
?from=-<time>
```

i Note

Supported time units: h (for hours), d (for days), w (for weeks) and m (for months). For example: ?from=-6h.

- To – retrieve telemetry data for any given time point

```
?to=-<time>
```

- Request data

```
none
```

- Response

```
[
  {
    "time": "2022-03-01 14:51:07.000000",
    "value": 1.1666666666666647e-254
  },
  {
    "time": "2022-03-01 15:51:07.000000",
    "value": 1.16668418566647e-182
  }
]
```

- Response codes

Status	Description
200	Success
400	Bad request

Get Link Telemetry Data

- URL

```
GET /cyber-ai/telemetry/link/{node_id}
```

- URL filters:

- From – retrieve alerts triggered within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).

For example: `?from=-1d`.

- Influencers

```
?influencers=<comma-separated list of influencers>
```

- Average, return average data:

```
?average=[ "True" | "False" ]
```

- Request Data

```
none
```

- Response

```
[  
  {  
    "time": "06:00:00",  
    "value": 45  
  },  
  {  
    "time": "07:00:00",  
    "value": 55  
  }  
]
```

Get Cable Telemetry Data

- URL

```
GET /cyber-ai/telemetry/cable/{cable_id}/{influencer}
```

- URL filters:

- From – retrieve telemetry data within the last given time period:

```
?from=-<time>
```

Supported time units: h (for hours), d (for days), w (for weeks), m (for months).

For example: `?from=-6h`.

- Probability – return all alerts with probability equal to, or greater than the given probability

```
?min_probability=<0-100>
```

- Influencers:

```
?influencers=<comma-separated list of influencers>
```

- Request Data

```
none
```

- Response

```
{
  "time": "06:00:00",
  "value": 45
},
{
  "time": "07:00:00",
  "value": 55
}
]
```

Alert Filters

Add Alerts Filter

- URL

```
POST /cyber-ai/alerts/filter
```

- Request Data

```
{
  "filter_type": "link_anomaly",
  "filter_elements": "0x35b286a72f6dc42:15",
  "filter_attributes": "hist1, hist2, hist3",
  "enabled": [
    true|false
  ]
}
```

- Response

```
{
  "filter_id": 100,
}
```

- Response codes

Status	Description
201	Created
400	Bad Request (invalid argument)

Delete Alert Filter

- URL

```
DELETE /cyber-ai/alerts/filter/{filter_id}
```

- Request Data

```
none
```

- Response

```
none
```

- Response codes

Status	Description
200	Successful
404	Not found

Enable Alert Filter

- URL

```
PUT /cyber-ai/alerts/filter
```

- Request Data

```
{  
  "filter_id": 100,  
  "enabled" : [true|false]
```

```
}
```

- Response

```
{  
  "filter_id": 100,  
  "filter_type": "link_anomaly",  
  "filter_elements": "0x35b286a72f6dc42:15",  
  "filter_attributes": "hist1, hist2, hist3",  
  "enabled": [true|false]  
}
```

- Response codes

Status	Description
200	Success
404	Not found

Get Alerts Filter

- URL

```
GET /cyber-ai/alerts/filter
```

- URL filters:
 - Type – retrieve alerts of specific type (or all types if this filter is not used)

```
?type=<alert_type>
```

Supported types: link_failure_prediction, link_anomaly, cable_event, tenant_alert, network_alert and logical_server_alert

- Request Data

```
none
```

- Response

```
[
  {
    "filter_id": 1,
    "filter_type": "link_anomaly",
    "filter_elements": "0x35b286a72f6dc42:15",
    "filter_attributes": "hist1, hist2, hist3",
    "enabled": true
  },
  {
    "filter_id": 2,
    "filter_type": "link_anomaly",
    "filter_elements": "0x35b286a72f6dc42:16",
    "filter_attributes": "hist1, hist2, hist3",
    "enabled": false
  }
]
```

- Response codes

Status	Description
200	Success
400	Bad request

Get Alert Filter

- URL

```
GET /cyber-ai/alerts/filter/{filter_id}
```

- Request Data

```
none
```

- Response

```
{  
  "filter_id": 1,  
  "filter_type": "link_anomaly",  
  "filter_elements": "0x35b286a72f6dc42:15",  
  "filter_attributes": "hist1, hist2, hist3",  
  "enabled": true  
}
```

- Response codes

Status	Description
200	Success
404	Not found

CLI Tools

In addition to the REST API used for Cyber AI management, Cyber AI software provides several command-line tools (CLI) for managing the Cyber AI system.

The CLI tools are installed on the Cyber AI host and can communicate with the Cyber AI containers.

ufm-cai-sanity

This tool is helpful for testing that cyberai is running and the suitable containers were loaded:

Tests

- Checks ufm-cyberai service is running
- Checks Cyber AI images are loaded

```
"cyberai_worker" "cyberai_web" "cyberai_plm" "mellanox/ufm-telemetry"
```

- Check containers are running

```
cyberai-web" "cyberai-plm" "ufm-telemetry"
```

- Checks that REST services are running

Usage

```
ufm-cai-sanity
```

ufm-cai-jobs

This script manages Cyber AI analytics jobs. Commands:

Command	Usage
<code>dump</code>	Dump status of a job if provided, otherwise dump status for all jobs (in json format)
<code>list</code>	List all job names
<code>run</code>	Runs given job
<code>enable</code>	Enables given job (Requires restart to take effect)
<code>disable</code>	Disables given job (Requires restart to take effect)
<code>reset-stats</code>	Resets all previous status (run times)

Usage

```
ufm-cai-jobs [-h] | [-c (dump|list|run|enable|disable|reset-stats) [-j <job-name>]]
```

ufm-cai-ufm-params

This script configures and shows the UFM connection info.

Usage

```
ufm-cai-ufm-params (update|show) <option>
```

Update

Updates UFM configuration.

Option	Description
<code>-i --ip</code>	UFM server IP
<code>-p --port</code>	UFM REST API connection port
<code>-U --username</code>	UFM username
<code>-P --password</code>	UFM password
<code>-s --site</code>	UFM site name
<code>-t --protocol</code>	UFM Rest API connection protocol

Show

Shows current UFM configuration (except password).

ufm-cai-status

This script checks the Cyber AI status, prints it or sends an email. The script runs once a day, using the Linux cron-job.

Usage

```
usage: ufm-cai-status [-h] [-m] [-p
{none,plain,simple,html,json}]
optional arguments:
  -h, --help            show this help message and exit
  -m, --mail            Send an email with the status report
  -p {none,plain,simple,html,json}, --print-report
{none,plain,simple,html,json}
                        Specify how to print the status report to
console
```

Configuration

The configuration file is located in:

```
/opt/ufm/cyber-ai/conf/status_report_config.yaml
```

It should be configured properly in order for Cyber AI to run:

```
site_name: <site>

mail_server:
  # To use local smtp server set server to 127.0.0.1
  server: <server>
  port: <port>
  use_tls: true
  sender: <sender>
  username: <username>
  password: <password>

# report_type: ( html | text )
report_type: html

recipient_list:
# - <name@example.com>
```

Cron Job

```
# crontab -l
30 7 * * * /usr/local/bin/ufm-cyberai_status -m
```

ufm-cai-sysdump

This script collects data and logs from Cyber AI and saves it into a zipped file to be used for debugging and troubleshooting.

Usage

```
ufm-cai-sysdump <options>
```

Options

Option	Description
<code>-v --verbose</code>	explain what is being done
<code>-n --network</code>	collect network counters files
<code>-c --cables</code>	collect cable counters files
<code>-z --archived</code>	collect archived counter files when associated with <code>[-n]</code> or <code>[-c]</code>
<code>-g --aggregated</code>	collect aggregated files
<code>-d --database</code>	collect database file(s)
<code>-t --topology</code>	collect topology files
<code>-m --model</code>	collect model files
<code>-l --log</code>	collect log files
<code>-f --conf</code>	collect configuration files
<code>-a --all</code>	collect all above

Output

Output file is in tgz format:

```
cyberai-sysdump-<date and time>.tgz
```

ufm-cai-weekly-alerts-report

This script generates a csv file for each type of alerts in Cyber-AI according to the given interval and saves it to the specified output directory.

Usage

```
ufm-cai-weekly-alerts-report [-h] [-i IP] [-t TIME] [-o OUT_DIR]
```

Options

Option	Long option	Description
-i	--ip	Cyber-AI IP address
-t	--time	Interval to get the data for. (1 2 3...)(h d w m)
-o	--out-dir	output directory to save the data to

High Availability

Overview

UFM HA supports High-Availability on the host level for UFM products (UFM Enterprise/UFM Appliance/UFM CyberAI) The solution is based on pacemaker to monitor services and DRBD to sync file-system states. The HA package can be used with both bare-metal and Dockerized UFM products.

UFM HA should be installed on two machines, master and standby.

Supported Platforms

1. Ubuntu
2. Centos Master

Prerequisites

Pacemaker packages

1. pacemaker
2. pcs
3. corosync

DRBD Package

- DRBD utils 8.4 or up.

Configuration

ufm_ha_cluster usage

```
ufm_ha_cluster --help
Usage: ufm_ha_cluster [-h|--help] <command> [<options>]
This script manages ufm HA cluster.

OPTIONS:
  -h|--help          Show this message

COMMANDS:
  config             Configure HA cluster
  set-password       Change hacluster password
  status             Check HA cluster status
  failover           Master node failover
  takeover           Standby node takeover
  start              Start HA services
  stop               Stop HA services
  attach             attach new standby node from cluster
  detach             detach the old standby to cluster

For more help about each command, type:
ufm_ha_cluster <command> --help
```

Setting HA Cluster Password

HA cluster user is a user used for pacemaker synchronization. the password for the user should be the same on both machines. To set the password, run the following command on both machines (order does not matter).

```
ufm_ha_cluster set-password -p <new-password>
```

Configuring Pacemaker and DRBD

```
ufm_ha_cluster config --help
```

```
Usage: ufm_ha_cluster config [<options>]
```

The config command configures ha add-on for ufm server.

OPTIONS:

-r --role <node role>	Node role (master or standby)
-n --peer-node <node-hostname>	Peer node name. mandatory.
-s --peer-sync-ip <ip address>	Peer node sync ip address mandatory.
-c --sync-interface	Local interface to be used for drbd sync mandatory.
-i --virtual-ip <virtual-ip>	Cluster virtual IP. mandatory.
-f --ha-config-file <file path>	HA configuration file. default: ufm-ha.conf
-p --hacluster-pwd <pwd>	hacluster user password default: default password
-h --help	Show this message

Note

1. You must run configuration script on the standby machine, then on the master machine.
2. Running config command will not start UFM services, you have to run it directly from the master machine.
3. Initial file system sync between master and standby may take few minutes, depending on your sync interface speed.
4. You must wait for the sync process before starting the services. You may use the status command for monitoring the sync.
5. If you are using high-availability for both UFM Cyber-AI and UFM Enterprise you have to change the following line in `ufm-ha.conf` file:

```
systemd_services=ufm-cyberai
systemd_services=ufm-cyberai ufm-ha-
watcher ufm-enterprise
```

Stopping UFM Services

You may stop UFM services using the following stop command.

```
ufm_ha_cluster stop
```

Takeover Services

Takeover command can be executed on the standby machine so it will be the master.

```
ufm_ha_cluster takeover
```

Master Failover

Failover command can be executed on the master machine so it will be the standby.

```
ufm_ha_cluster failover
```

Replace HA Node

To replace old standby, detach the old standby, then configure the new standby, and attach it to the cluster.

On the master, run the detach command:

```
ufm_ha_cluster detach
```

On the new standby, run the config command, for more information, refer to [ufm-cai-jobs](#).

On the master node, run the attach command:

```
Ufm_ha_cluster -n <peer_node> -s <peer_sync_ip> -p <hacluster-  
pwd> -c <sync-interface>
```

UFM Cyber-AI OS Upgrade

This section provides a step-by-step guide for UFM Cyber-AI Operating System upgrade.

Each UFM Cyber-AI Appliance software has an additional tar file with a `-omu.tar` suffix (OMU stands for OS Manufacture and Upgrade). This tar file can be used to re-manufacture the server and to upgrade the operating system/software on the server.

Extracting the Software

1. Copy the `OMU` tar file to a temporary directory on the server.

```
CyberAI - ufm-cyberai-appliance<version>-<revision>-omu.tar
```

2. Extract the contents of the tar file to `/tmp`:

```
tar xf ./ufm-cyberai-appliance-<version>-<revision>-omu.tar -C /tmp/
```

3. Change to the extracted directory:

```
cd /tmp/ufm-cyberai-appliance-<version>-<revision>-omu
```

4. An upgrade script and an ISO file are included in the extracted directory:

```
ls -l ./#ls -l ./
ufm-os-upgrade.sh
ufm-cyberai-appliance-<version>-<revision>.iso
```

The following flags are available in the upgrade script help.

```
# ufm-os-upgrade.sh --help
```

```
ufm-os-upgrade.sh will upgrade and install OS packages.
```

IMPORTANT!!! a reboot is mandatory after the finalization of this script,
kernel and kernel models will not work properly until the server is rebooted.

Additional SW installations will be automatically invoked after reboot,

a message will pop on all open terminals with the installation status:

```
"UFM-OS-FIRSTBOOT-FAILURE" - if installation is failed.
```

```
"UFM-OS-FIRSTBOOT-SUCCESS" - if installation succeeded.
```

additional info will be available in `"/var/log/ufm_os_upgrade_<UFM-OS-VERSION>.log"` log file.

```
syntax: ufm-os-upgrade.sh [options]
```

options

```
--appliance-sw-upgrade    upgrade ufm_appliance SW as well,  
default is to upgrade OS only, P.S. only applicable for  
StandAlone installations.
```

```
-d,--debug                debug info will be visible on the  
screen.
```

```
-r,--reboot              Automatically reboot the server when  
upgrade is finished.
```

```
P.S. if secure boot is enabled and a new  
certificate is enrolled  
the server will not automatically  
reboot even if this flag is set.
```

```
-y, --yes          wont prompt for user acknowledgements.  
-h, --help        print this help message.
```

Warning

IMPORTANT!!! System reboot is mandatory once the upgrade procedure is completed. The `-r` flag can be used to automatically reboot the server at the end of the upgrade. Note that some kernel modules may not work properly until server reboot is performed.

Upgrading in Standalone Mode

1. Stop UFM and CyberAI services.

```
systemctl stop ufm-enterprise.service  
systemctl stop ufm-cyberai.service
```

2. Run the upgrade script:

Note

System reboot is mandatory once the upgrade procedure is completed. The `-r` flag can be used to automatically reboot the server.

To bypass user prompts, use the `-y` flag when executing the command, but note that this flag alone will not trigger an automatic server reboot. If a reboot is desired, use the `-r` flag in combination with `-y`. Additionally, the

`--appliance-sw-upgrade` flag can be used to upgrade both the UFM Enterprise Appliance SW and Cyber-AI SW, but this upgrade is not enabled by default. In the provided example, the server will automatically reboot after the upgrade process is completed.

```
./ufm-os-upgrade.sh -y -r
```

The below is an example with the `--appliance-sw-upgrade` flag. Note that the UFM Enterprise appliance SW will also be upgraded.

```
./ufm-os-upgrade.sh -y -r --appliance-sw-upgrade
```

3. After the reboot procedure is complete, a systemd service (`ufm-os-firstboot.service`) runs the remainder of the upgrade procedure. Once completed, a message is prompted to all open terminals including the status:

"UFM-OS-FIRSTBOOT-FAILURE" - if installation is failed.

"UFM-OS-FIRSTBOOT-SUCCESS" - if installation succeeded.

Example:

```
root@ufm-ai03:~#  
root@ufm-ai03:~#  
Broadcast message from root@ufm-ai03 (somewhere) (Fri Dec 30 18:47:32 2022):  
UFM-OS-FIRSTBOOT-SUCCESS, installation succeeded additional info is available in /var/log/ufm-os-firstboot.log
```

To manually check the status, run

`systemctl status ufm-os-firstboot.service`. If it is already completed, an error message is prompted stating that there is no such service. In that case, the log `/var/log/ufm-os-firstboot.log` can be checked instead.

```
systemctl status ufm-os-firstboot.service
```

Example:

```
root@ufm-ai03:~# systemctl status ufm-os-firstboot
Unit ufm-os-firstboot.service could not be found.
root@ufm-ai03:~#
```

Upgrade in High-Availability Mode

Upgrade on HA should be done first on the stand-by node and after that on the master node, each node upgrade is similar to the SA instructions.

In case the Standby node is unavailable, the upgrade can be run on the Master node only, however, some additional steps will be required after the appliance is upgraded.

1. [On the standby Node]: Copy and extract the OMU tar file to a temporary directory, refer to [Extracting the Software](#).
2. [On master Node]: Run the upgrade script.

Note

System reboot is mandatory once the upgrade procedure is completed. The `-r` flag can be used to automatically reboot the server.

The `--appliance-sw-upgrade` flag CAN NOT !!! be supplied to upgrade the UFM Enterprise Appliance SW in HA and the upgrade will not be performed if provided.

The `-y` flag can be supplied to skip user questions (the flag does not automatically reboot the server on its own. For auto reboot, combine with the `-r` flag).

In the following example the server auto reboots once the upgrade procedure is completed:

```
cd /tmp/ufm-cyberai-appliance-<version>-<revision>-omu
```

```
./ufm-os-upgrade.sh -y -r
```

3. In case the `-r` flag was not included, the server must be manually rebooted if the user selects "No" when prompted with a question on whether to reboot after the script finishes.

```
reboot now
```

4. After the reboot procedure is complete, a systemd service (`ufm-os-firstboot.service`) runs the remainder of the upgrade procedure. Once completed, a message is prompted to all open terminals including the status:

"UFM-OS-FIRSTBOOT-FAILURE" - if installation is failed.

"UFM-OS-FIRSTBOOT-SUCCESS" - if installation succeeded.

Example:

```
root@ufm-ai03:~#  
root@ufm-ai03:~#  
Broadcast message from root@ufm-ai03 (somewhere) (Fri Dec 30 18:47:32 2022):  
UFM-OS-FIRSTBOOT-SUCCESS, installation succeeded additional info is available in /var/log/ufm-os-firstboot.log
```

To verify the status manually, execute "`systemctl status ufm-os-firstboot.service`". If the service has already completed, an error message will be displayed indicating that the service does not exist. In such a scenario, refer to the log file located at `/var/log/ufm-os-firstboot.log` for checking the status.

```
systemctl status ufm-os-firstboot.service
```

Example:

```
root@ufm-ai03:~# systemctl status ufm-os-firstboot  
Unit ufm-os-firstboot.service could not be found.  
root@ufm-ai03:~#
```

5. After the stand-by node have finished the upgrade check the HA cluster status

```
ufm_ha_cluster status
```

```
root@swx-ufm3-11:~# ufm_ha_cluster status
Cluster name: ufmcluster
WARNING: corosync and pacemaker node names do not match (IPs used in setup?)
Stack: corosync
Current DC: swx-ufm3-11 (version 1.1.18-2b07d5c5a9) - partition with quorum
Last updated: Thu Mar 16 18:45:19 2023
Last change: Mon Feb 27 12:40:22 2023 by root via crm_resource on swx-ufm3-11

2 nodes configured
5 resources configured

Online: [ swx-ufm3-09 swx-ufm3-11 ]

Full list of resources:

Master/Slave Set: ha_data_drbd_master [ha_data_drbd]
Masters: [ swx-ufm3-09 ]
Slaves: [ swx-ufm3-11 ]
Resource Group: ufmcluster-grp
  ha_data_file system      (ocf::heartbeat:Filesystem): Started swx-ufm3-09
  ufm-ha-watcher           (systemd:ufm-ha-watcher):   Started swx-ufm3-09
  ufm-enterprise           (systemd:ufm-enterprise):   Started swx-ufm3-09

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
DRBD_RESOURCE: ha_data
DRBD_CONNECTIVITY: Connected
DISK_STATE: UpToDate
DRBD_ROLE: Secondary
PEER_DISK_STATE: UpToDate
PEER_DRBD_ROLE: Primary
```

Every node within the cluster is expected to be operational while the present node remains in a stand-by mode (designated as Secondary in DRBD_ROLE).

6. [On the Master Node]: Initiate a fail-over of UFM to the stand-by node, which will result in the upgraded node taking over as the master and the current node transitioning to a stand-by state.

```
ufm_ha_cluster failover
```

Wait until all the resources of UFM are up and functioning correctly on the upgraded node.

7. Perform the same process on the inactive node that has not been upgraded, and is currently functioning as a standby.

Morpheus Integration

NVIDIA Morpheus is an open AI application framework that provides cybersecurity developers with a highly optimized AI developer framework and pre-trained AI capabilities that, for the first time, allows them to inspect all IP traffic across their data center fabric instantaneously. Bringing a new level of security to data centers, Morpheus provides development capabilities around dynamic protection, real-time telemetry, adaptive policies, and cyber defenses for detecting and remediating cybersecurity threats.

The Morpheus Developer Kit allows developers to quickly and easily set up an example pipeline to run inference models provided by NVIDIA and experiment with the features and capabilities available within the Morpheus framework to address their cybersecurity and information security use cases.

Features

- Built on RAPIDS™
 - Built on the RAPIDS™ libraries, deep learning frameworks, and NVIDIA Triton™ Inference Server, Morpheus simplifies the analysis of logs and telemetry to help detect and mitigate security threats.
- AI Cybersecurity Capabilities
 - Deploy your models using common deep-learning frameworks. Or get a jump-start in building applications to identify leaked sensitive information, detect malware, and identify errors via logs by using one of NVIDIA's pre-trained and tested models.
- Real-Time Telemetry
 - Morpheus can receive rich, real-time network telemetry from every NVIDIA® BlueField® DPU-accelerated server in the data center without impacting performance. Integrating the framework into a third-party cybersecurity offering brings the world's best AI computing to communication networks.
- DPU-Connected
 - The NVIDIA BlueField Data Processing Unit (DPU) can be used as a telemetry agent for receiving critical data center communications into Morpheus. As an

optional addition to Morpheus, BlueField DPU extends static security logging to a sophisticated dynamic real-time telemetry model that evolves with new policies and threat intelligence.

Prerequisites

1. A Cyber AI machine with T4 or V100 GPU, at least 64GB RAM, eight cores CPU, and 100 GB storage.
2. Morpheus tarball which contains Morpheus AI Engine Docker image.
3. Installing Docker engine.

The Integration involves installing and starting the Morpheus AI Engine.

Installing Morpheus AI Engine

Morpheus tarball is available through [this link](#).

Morpheus tarball Components:

- Installer and Uninstaller Scripts.
- The configuration file contains the Morpheus docker image details.
- Morpheus docker image.
- Machine Learning models files.

To Integrate Morpheus with CyberAI, follow the next steps:

- Decompress the morpheus-22.06.tar
- Run the installer script sh.
- Installer script loads the Morpheus docker image and enables Morpheus in cfg
 1. Load Morpheus docker image morpheus-22.06.tar.gz
 2. Set [Morpheus] enabled = true inside cfg
 3. Enable Telemetry GPU counters collection by setting [data_prep_telemetry::gpu_counter] skip_collection = false

4. Copy the models' files under the volumes created for Morpheus.

```
/opt/ufm/cyber-ai/scripts/e2e_model_script.py  
/opt/ufm/cyber-  
ai/datastore/morpheus/output/random_forest_model_crypto_re
```

Starting Morpheus AI Engine

After installing the Morpheus AI Engine, restarting Cyber AI creates a Morpheus docker container, which stores GPU Telemetry in a shared volume accessed by the Morpheus docker container, where you can run the ML model and inference Crypto-Mining activities and generate output files with events.

List of Supported Events

UFM Cyber AI tab	Elements	Counters
Link anomaly/Link Failure Prediction	Node+Port	symbol_error_counter
		local_link_integrity_errors LocalLinkIntegrityErrorsExtended
		SymbolErrorCounterExtended
		UnknownBlockCounter
		SyncHeaderErrorCounter
		phy_symbol_errors
		ErrorDetectionCounterLane.[1-12]
		FECCorrectableBlockCounterLane.[1-12]
		FECCorrectedSymbolCounterLane.[1-12]
		PortFECCorrectableBlockCounter
		PortFECCorrectedSymbolCounter
		phy_corrected_bits
		phy_raw_errors_lane*
		raw_ber_coef
		raw_ber_magnitude
		raw_ber
		FECUncorrectableBlockCounterLane.[1-12]
		PortFECUncorrectableBlockCounter
		effective_ber_coef
		effective_ber_magnitude
eff_ber		
port_xmit_discard		
port_rcv_switch_relay_errors		

UFM Cyber AI tab	Elements	Counters
		excessive_buffer_errors ExcessiveBufferOverrunErrorsExtended
		PortMalformedPacketErrors
		PortDLIDMappingErrors
		PortBufferOverrunErrors
		PortVLMMappingErrors
		PortNeighborMTUDiscards
		PortInactiveDiscards
		PortSwHOQLifetimeLimitDiscards
		PortSwLifetimeLimitDiscards
		port_xmit_wait
		PortXmitWaitExtended
		LinkDownedCounterExtended link_down_counter
		LinkErrorRecoveryCounterExtended link_error_recovery_counter
		port_rcv_constraint_errors
		PortRcvConstraintErrorsExtended
		port_rcv_data
		PortRcvDataExtended
		port_rcv_errors
		PortRcvErrorsExtended
		port_rcv_pkts
		PortRcvPktsExtended
		port_rcv_remote_physical_errors
		PortRcvRemotePhysicalErrorsExtended
		PortRcvSwitchRelayErrorsExtended
		PortUniCastRcvPktsExtended
		PortUniCastXmitPktsExtended

UFM Cyber AI tab	Elements	Counters
		port_xmit_constraint_errors
		PortXmitConstraintErrorsExtended
		port_xmit_data
		PortXmitDataExtended
		PortXmitDiscardsExtended
		port_xmit_pkts
		PortXmitPktsExtended
		phy_received_bits
		RetransmissionPerSec
		hist0
		hist1
		hist2
		hist3
		vl15_dropped
		VL15DroppedExtended
		link_error_recovery_counter
		ExcessiveBufferOverrunErrorsExtended
		GradeID
		Lane0Grade
		Lane1Grade
		Lane2Grade
		Lane3Grade
		MaxRetransmissionRate
		PortLocalPhysicalErrors
		PortLoopingErrors
		PortMultiCastRcvPktsExtended
		PortMultiCastXmitPktsExtended
Network Alerts	NW	raw_ber

UFM Cyber AI tab	Elements	Counters
		eff_ber port_xmit_discard port_rcv_switch_relay_errors PortDLIDMappingErrors PortVLMappingErrors PortNeighborMTUDiscards PortInactiveDiscards port_xmit_wait PortXmitWaitExtended LinkDownedCounterExtended LinkErrorRecoveryCounterExtended port_rcv_data port_rcv_errors port_rcv_pkts port_rcv_remote_physical_errors PortRcvSwitchRelayErrorsExtended PortUniCastRcvPktsExtended PortUniCastXmitPktsExtended port_xmit_constraint_errors port_xmit_data PortXmitDiscardsExtended port_xmit_pkts phy_received_bits RetransmissionPerSec
Tenant/Application Alerts	Pkey	raw_ber eff_ber port_xmit_discard port_rcv_switch_relay_errors

UFM Cyber AI tab	Elements	Counters
		PortDLIDMappingErrors PortVLMappingErrors PortNeighborMTUDiscards PortInactiveDiscards port_xmit_wait PortXmitWaitExtended LinkDownedCounterExtended LinkErrorRecoveryCounterExtended port_rcv_data port_rcv_errors port_rcv_pkts port_rcv_remote_physical_errors PortRcvSwitchRelayErrorsExtended PortUniCastRcvPktsExtended PortUniCastXmitPktsExtended port_xmit_constraint_errors port_xmit_data PortXmitDiscardsExtended port_xmit_pkts phy_received_bits RetransmissionPerSec
Cable Events	Node+Port	temperature_low_th temperature_high_th voltage_low_th voltage_high_th rx_power_low_th rx_power_high_th tx_power_high_th

UFM Cyber AI tab	Elements	Counters
		tx_bias_low_th
		tx_bias_high_th

Settings and Configuration

Inside the container, the directory `/config` contains the configuration files for the UFM Cyber-AI application. The file `launch_ibdiagnet_config.ini` is the main configuration file.

The basic configurations of `launch_ibdiagnet_config.ini` are listed in the following table:

Section	Key	Type	Default	Description
ibdiagnet	ibdiagnet_enabled	Boolean	true	Enable/disable ibdiagnet
	data_dir	String	/data	data_dir: Directory in which logs are placed
	ibdiag_output_dir	String	/tmp/ibd	Directory where ibdiag places files
	sample_rate	Integer	-	Frequency counter divider
	hca	String	mlx5_2	Card to use
	app_name	String	/opt/collectx/bin/ibdiagnet	Full path to the application
	topology_mode	String	discover	Topology mode
	topology_discovery_factor	Integer	0	Every "n" iterations of discovery, result from the last discovery is used
retention	retention_enabled	Boolean	true	Enable/disable retention service
	retention_interval	Time	1d	Interval between running the retention process
	retention_age	Time	100d	Period to keep collected data

Section	Key	Type	Default	Description
compression	compression_enabled	Boolean	true	Enable/disable service
	compression_interval	Time	6h	Interval to running the service
	compression_age	Time	12h	Period to compress
cable_info	cable_info_schedule	csv	-	Weekday/Time to collect data

Appendixes

- [Appendix - Supported Counters](#)
- [Appendix - Cable Information](#)
- [Appendix - Cyber-AI Appliance OS Remanufacture](#)
- [Appendix - Deploying UFM Cyber-AI from an ISO File](#)

Appendix - Supported Counters

Supported InfiniBand Counters

- Counter
- ExcessiveBufferOverrunErrorsExtended
- GradeID
- Lane0Grade
- Lane1Grade
- Lane2Grade
- Lane3Grade
- LinkDownedCounterExtended
- LinkErrorRecoveryCounterExtended
- LocalLinkIntegrityErrorsExtended
- MaxRetransmissionRate
- PortBufferOverrunErrors

- PortDLIDMappingErrors
- PortFECCorrectableBlockCounter
- PortFECCorrectedSymbolCounter
- PortFECUncorrectableBlockCounter
- PortInactiveDiscards
- PortLocalPhysicalErrors
- PortLoopingErrors
- PortMalformedPacketErrors
- PortMultiCastRcvPktsExtended
- PortMultiCastXmitPktsExtended
- PortNeighborMTUDiscards
- PortRcvConstraintErrorsExtended
- PortRcvDataExtended
- PortRcvErrorsExtended
- PortRcvPktsExtended
- PortRcvRemotePhysicalErrorsExtended
- PortRcvSwitchRelayErrorsExtended
- PortSwHOQLifetimeLimitDiscards
- PortSwLifetimeLimitDiscards
- PortUniCastRcvPktsExtended
- PortUniCastXmitPktsExtended
- PortVLMappingErrors
- PortXmitConstraintErrorsExtended

- PortXmitDataExtended
- PortXmitDiscardsExtended
- PortXmitPktsExtended
- PortXmitWaitExtended
- QP1DroppedExtended
- RetransmissionPerSec
- SymbolErrorCounterExtended
- SyncHeaderErrorCounter
- UnknownBlockCounter
- VL15DroppedExtended
- ber_threshold
- eff_ber
- effective_ber_coef
- effective_ber_magnitude
- excessive_buffer_errors
- link_down_counter
- link_error_recovery_counter
- load_avg
- local_link_integrity_errors
- node_guid
- phy_corrected_bits
- phy_raw_errors_lane0
- phy_raw_errors_lane1

- phy_raw_errors_lane2
- phy_raw_errors_lane3
- phy_received_bits
- phy_symbol_errors
- port_guid
- port_num
- port_rcv_constraint_errors
- port_rcv_data
- port_rcv_errors
- port_rcv_pkts
- port_rcv_remote_physical_errors
- port_rcv_switch_relay_errors
- port_xmit_constraint_errors
- port_xmit_data
- port_xmit_discard
- port_xmit_pkts
- port_xmit_wait
- raw_ber
- raw_ber_coef
- raw_ber_magnitude
- symbol_error_counter
- threshold_type
- time_since_last_clear

- vl15_dropped

Supported Per-lane Counters

- ErrorDetectionCounterLane.<1-12>
- FECCorrectableBlockCounterLane.<1-12>
- FECCorrectedSymbolCounterLane.<1-12>
- FECUncorrectableBlockCounterLane.<1-12>

Appendix - Cable Information

Type	Field
power	mw
	dbm
cable	port
	lid
	port_name
	vendor
	oui
	pn
	sn
	rev
	length
	type
	supportedspeed
	temperature
	powerclass
	nominalbitrate
cdrenabletxrx	

Type	Field
	inputeq
	outputamp
	outputemp
	fw_version
	attenuation_2.5_5_7_12
	rx_power_type
	rx_power.1.mw
	rx_power.1.dbm
	rx_power.2.mw
	rx_power.2.dbm
	rx_power.3.mw
	rx_power.3.dbm
	rx_power.4.mw
	rx_power.4.dbm
	tx_bias.1
	tx_bias.2
	tx_bias.3
	tx_bias.4
	tx_power.1.mw
	tx_power.1.dbm
	tx_power.2.mw
	tx_power.2.dbm
	tx_power.3.mw
	tx_power.3.dbm
	tx_power.4.mw
	tx_power.4.dbm
	cdr_tx_rx_loss_indicator
	adaptive_equalization_fault

Type	Field
	tx_rx_lol_indicator
	temperature_alarm_and_warning
	voltage_alarm_and_warning
	rx_power_alarm_warning
	tx_bias_alarm_and_warning
	diag_supply_voltage
	transmitter_technolog
	eth_com_codes_ext
	datacode
	lot
	tx_adaptive_equalization_freeze
	rx_output_disable
	tx_adaptive_equalization_enable

Appendix - Cyber-AI Appliance OS Remanufacture

Warning

This section provides a step-by-step guide for deploying Cyber-AI (CAI) from an ISO file in case of unrecoverable issues. This guide provides instructions on how to remanufacture the Cyber-AI appliance and OS.

Step 1: Extract the TAR file to a temporary directory

Run the following command to extract the `ufm-cyberai-appliance-<version>-omu.tar` to a temporary directory:

```
tar xzf /path/to/ufm-cyberai-appliance-<version>-omu.tar -C /tmp
```

An ISO file and an upgrade script will be present inside the directory.

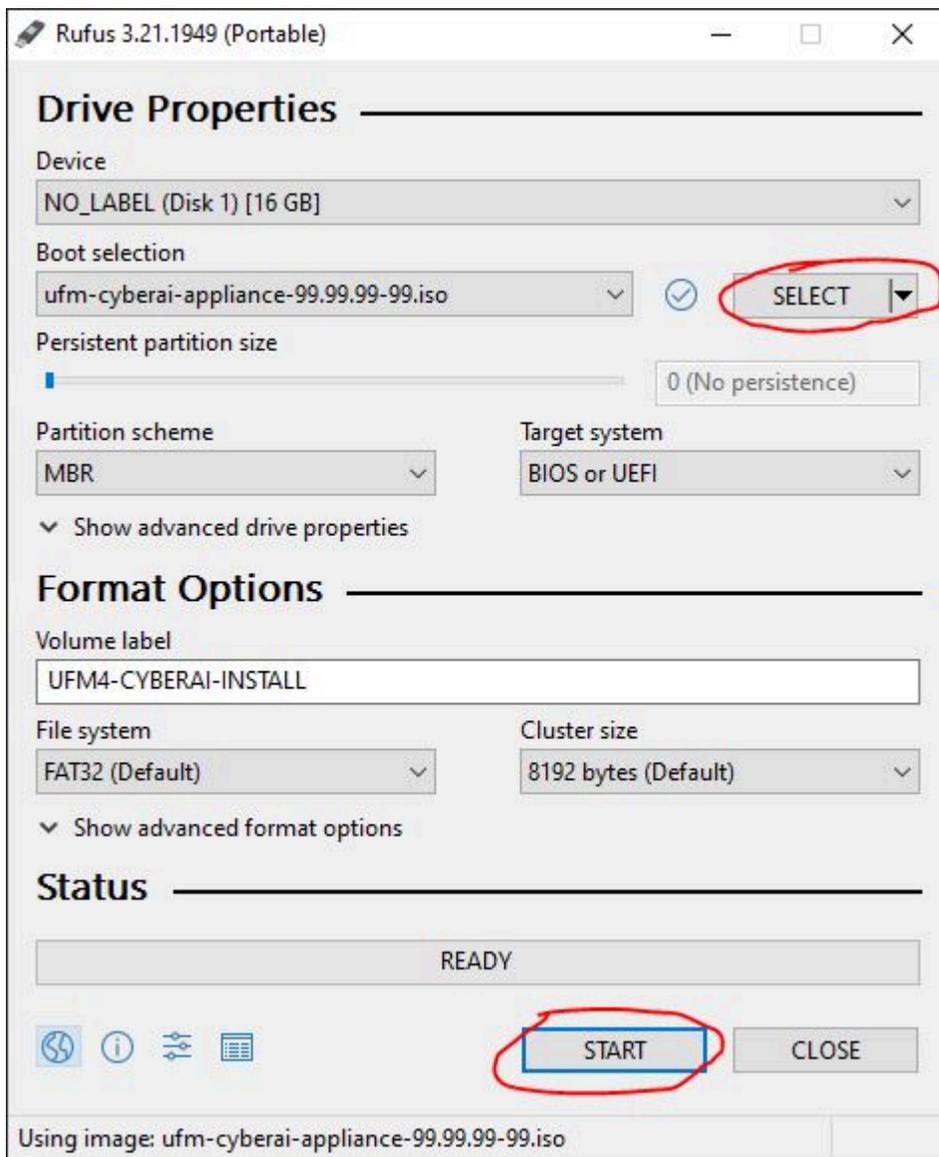
```
ls -ltrh /tmp/ufm-cyberai-appliance-<version>-omu/  
-rw-r--r-- 1 root root 7.5G Dec 31 17:49 ufm-cyberai-appliance-  
<version>.iso  
-rwxr-xr-x 1 root root 11K Dec 31 17:49 ufm-os-upgrade.sh
```

Step: 2 - Burn ISO to USB

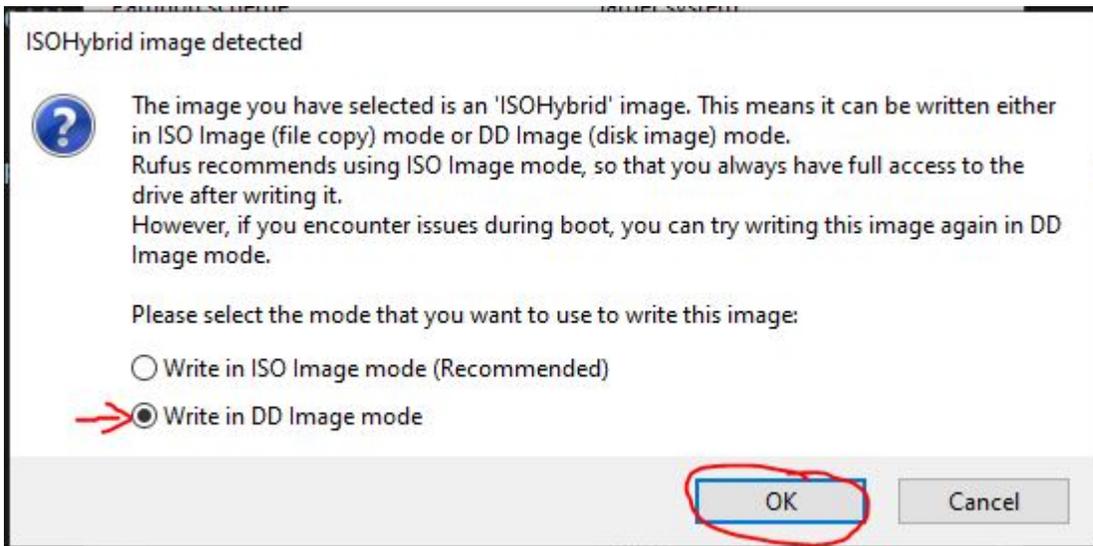
Burning ISO can be performed on Windows or Linux operating systems. Based on the desired installation method, follow the below instructions.

Windows

1. Download and open Rufus. Refer to [Rufus - Create bootable USB drives the easy way](#).
2. Download and open the tar file `ufm-cyberai-appliance-<version>-omu.tar`.
3. On Rufus, click on "SELECT" and from the drop-down menu, select the `ufm-cyberai-appliance-<version>.iso`, then click "START".



4. An "isohybrid image detected" message will pop up. Choose "Write in DD mode" and click "OK".



5. A message will appear stating that all data on the usb device will be lost, click "OK and continue".



6. Wait for Rufus to finish.
7. Unplug the USB device.

Linux

1. Identify the USB drive by running the following command:

 **Warning**

IMPORTANT!!! Ensure you are NOT running the following commands on a hard drive device but only on the USB (in the examples below it will be /dev/sdb).

(i) Note

The USB drive is mapped to sdb in the following command snippet.

```
root@ubuntu18:~# ls -ltrh /dev/disk/by-id/usb*
lrwxrwxrwx 1 root root 9 Jan 2 13:44 /dev/disk/by-id/usb-
SanDisk_Cruzer_Glide_3.0_4C530000040724111091-0:0 ->
../../../../sdb
lrwxrwxrwx 1 root root 10 Jan 2 13:44 /dev/disk/by-id/usb-
SanDisk_Cruzer_Glide_3.0_4C530000040724111091-0:0-part1 ->
../../../../sdb1
```

2. Copy the `ufm-cyberai-appliance-<version>.iso` to the USB using the following dd command:

(i) Note

The USB drive is mapped to /dev/sdb.

```
dd if=/path/to/ufm-cyberai-appliance-<version>.iso of=/dev/sdb
bs=4M status=progress oflag=sync
```

3. Verify that the USB is bootable:

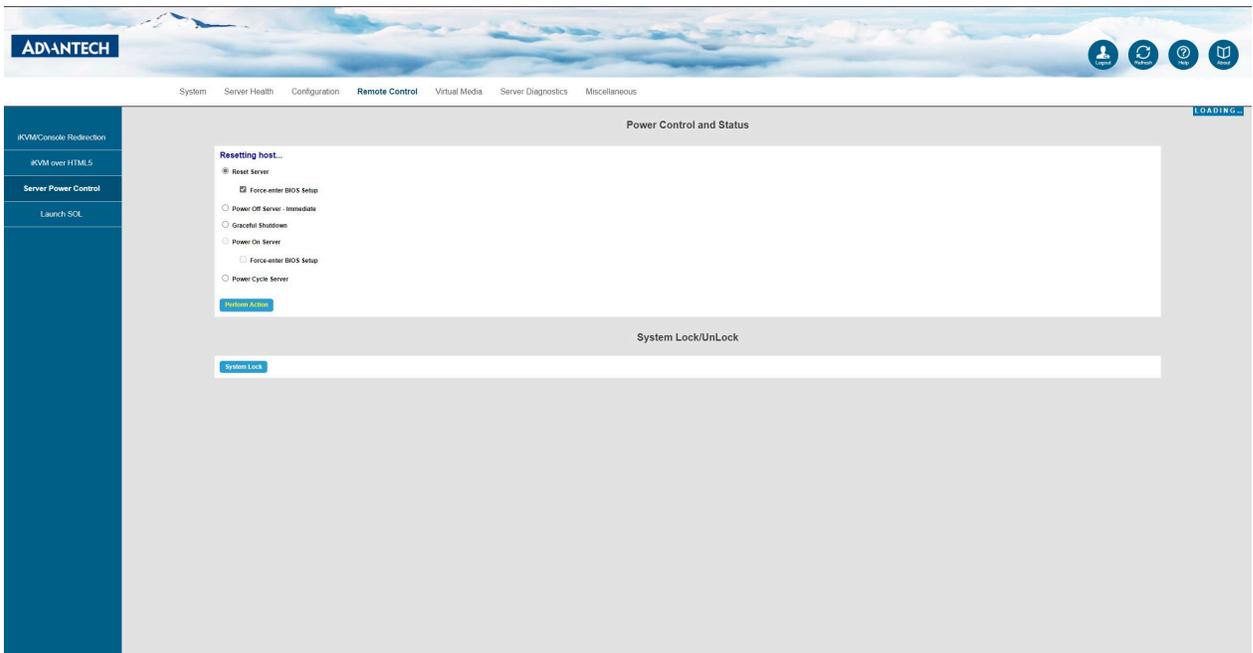
```
root@ubuntu18:~# fdisk -l /dev/sdb
Disk /dev/sdb: 14.9 GiB, 16005464064 bytes, 31260672 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x594ec03e

Device      Boot Start          End  Sectors  Size Id Type
/dev/sdb1   *           64 15679439 15679376  7.5G 17 Hidden
HPFS/NTFS
```

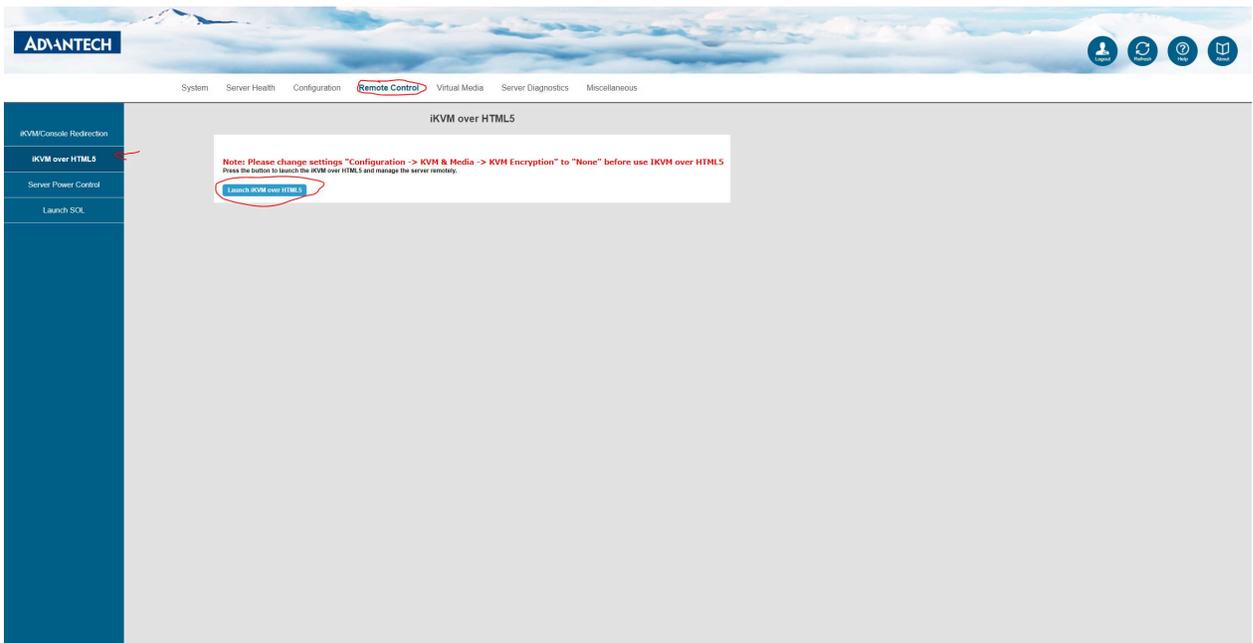
4. Unplug the USB.

Step: 3 - Manufacture Cyber-AI from USB

1. Plug the USB (prepared in the previous step) to one of the Cyber-AI server back USB ports.
2. Login to BMC web UI: https://<BMC_IP_ADDRESS>.
3. Navigate to "Remote Control" → "Server Power Control" and check the "Force-enter BIOS Setup" checkbox under the "Restart Server". Then, click "Perform Action".

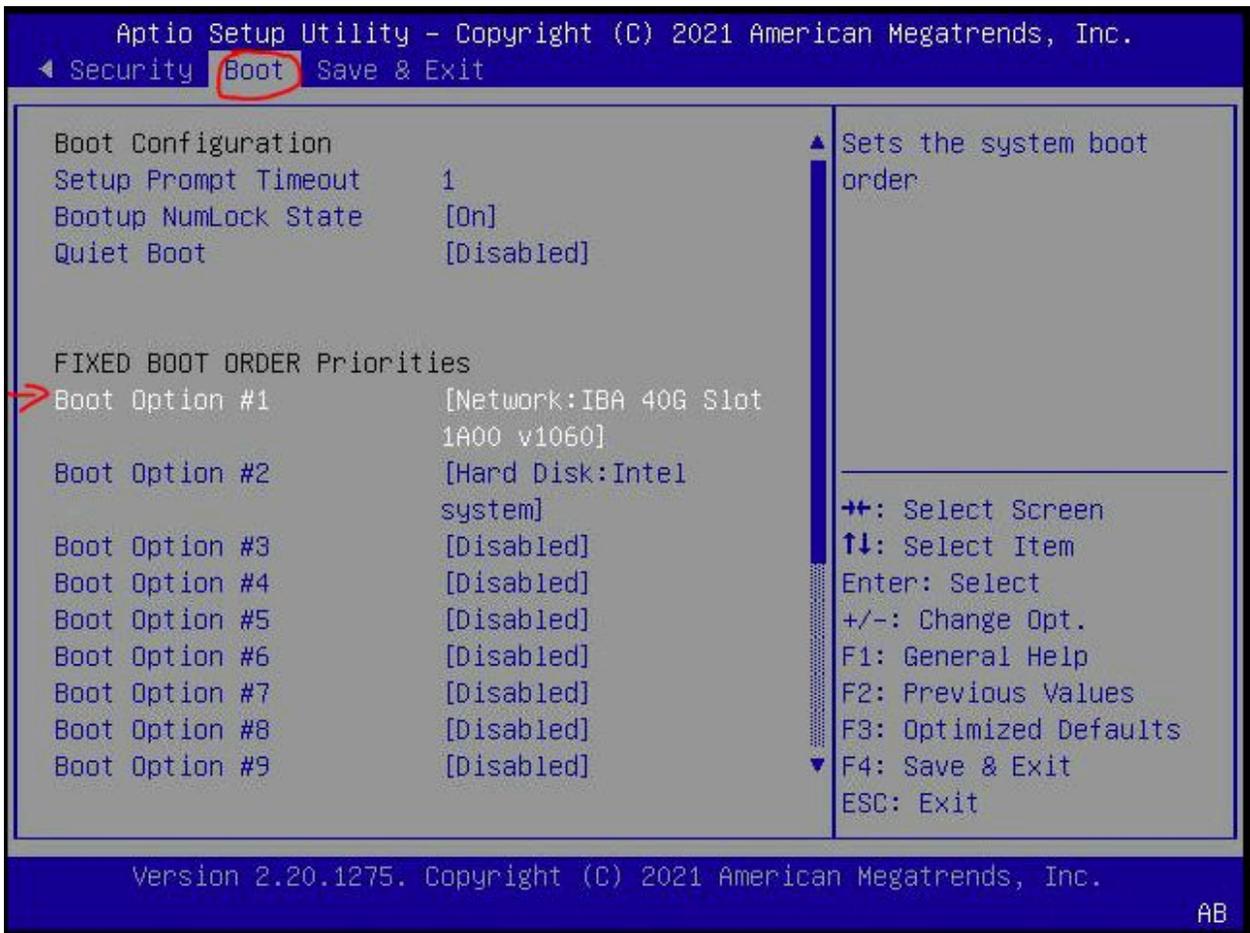


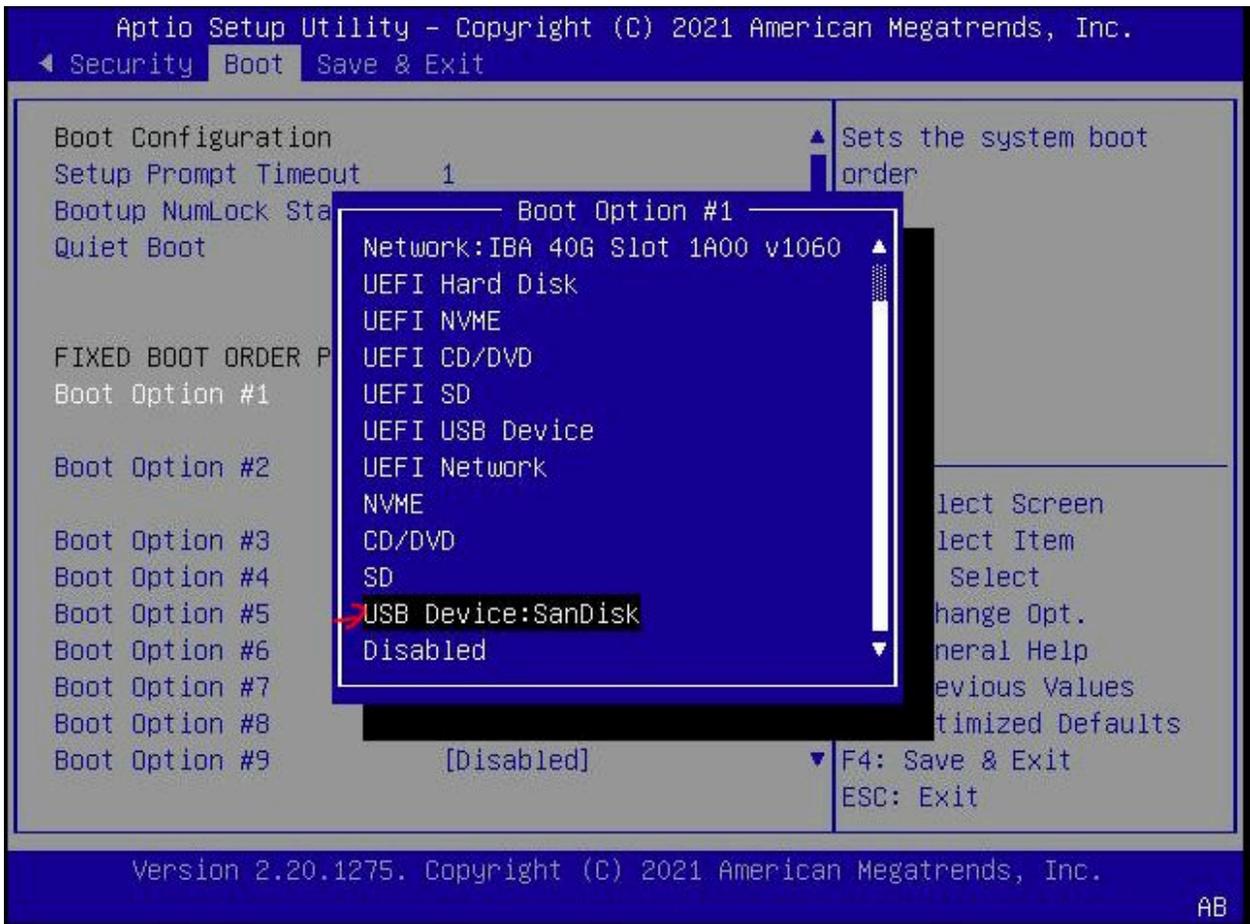
4. Navigate to "Remote Control" → "iKVM over HTML5" and click "Launch iKVM over HTML5" button.



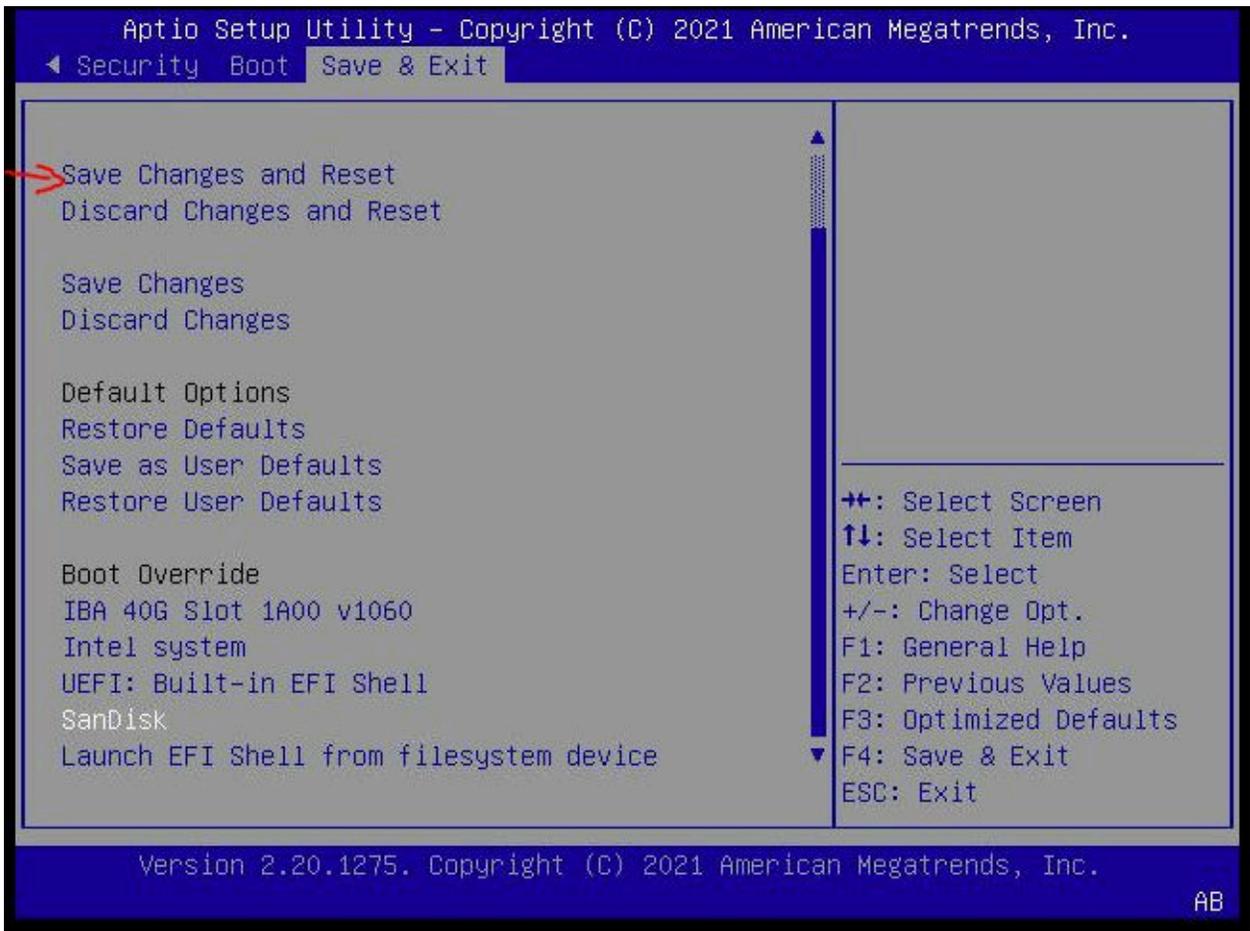
A new window will open.

5. In the BIOS menu, navigate to BOOT → "Boot Option #1" and check "USB Device: <NAME OF USB DEVICE>".

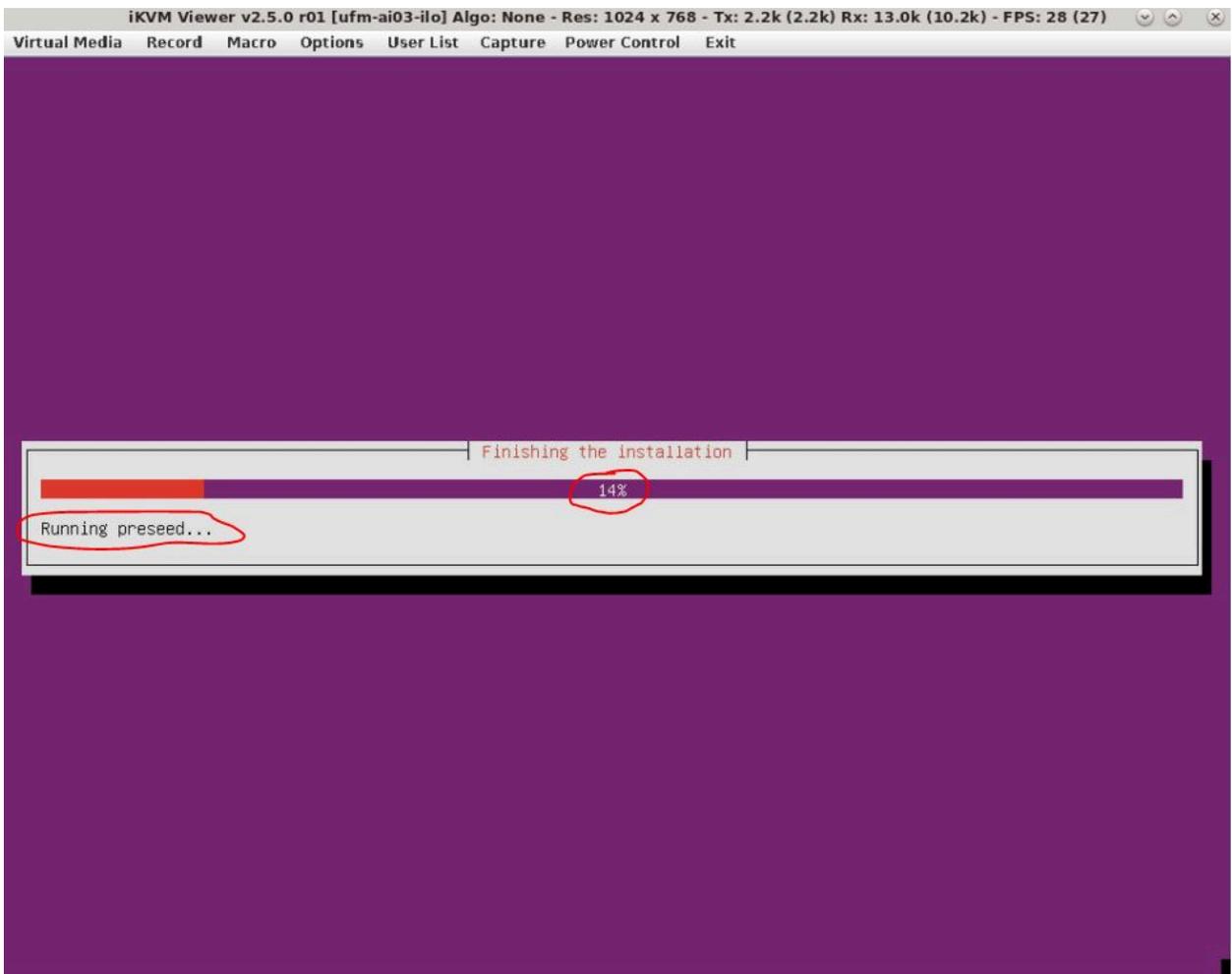




6. Navigate to "Save & Exit" → "Save Changes and Reset" and press enter.



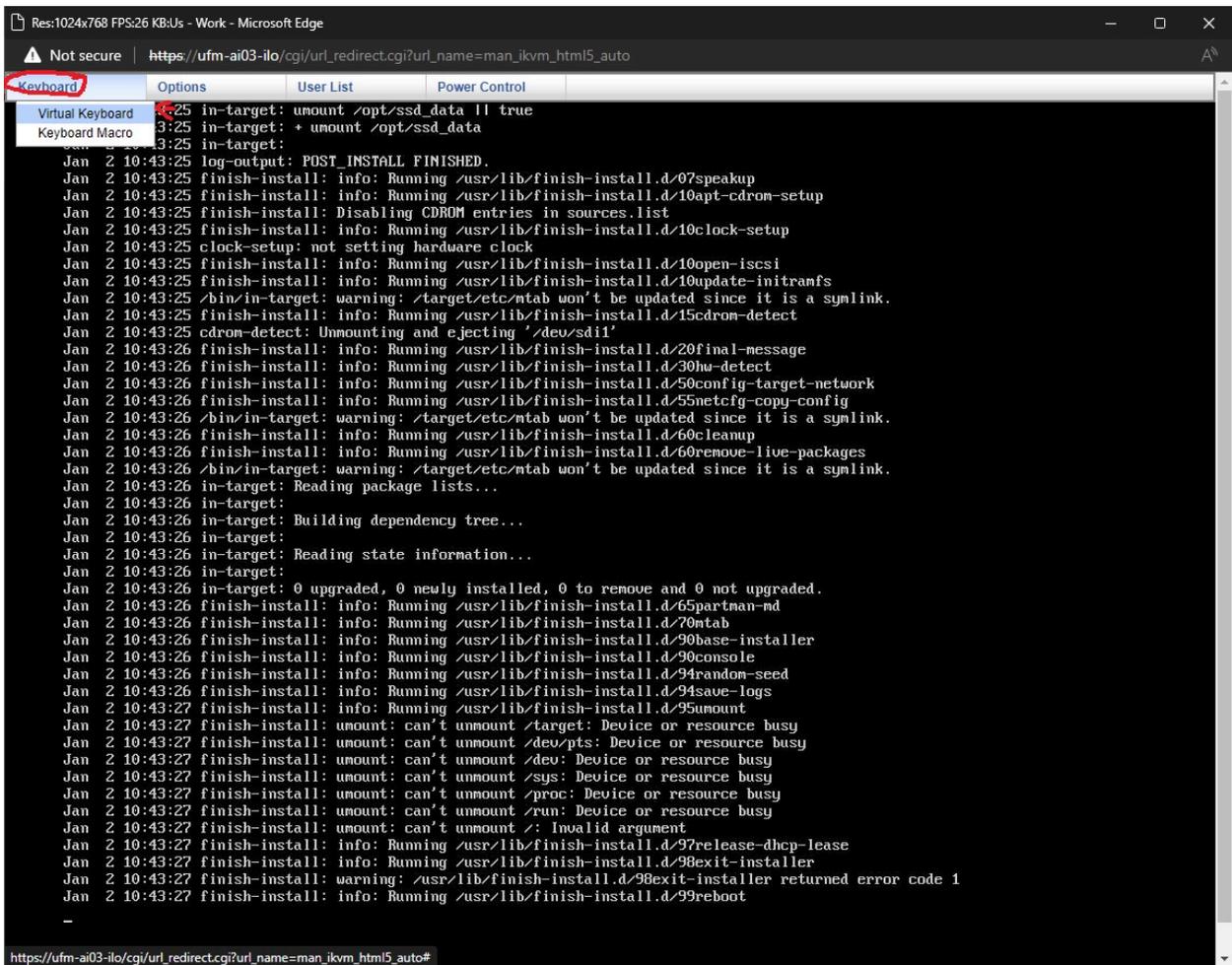
7. At this point Cyber-AI installation should start automatically.



8. The process takes ~50 minutes, "Running preseed..." will show ~14-16 percent and will remain on this percentage for most of the time. This does not mean that the process is stuck.

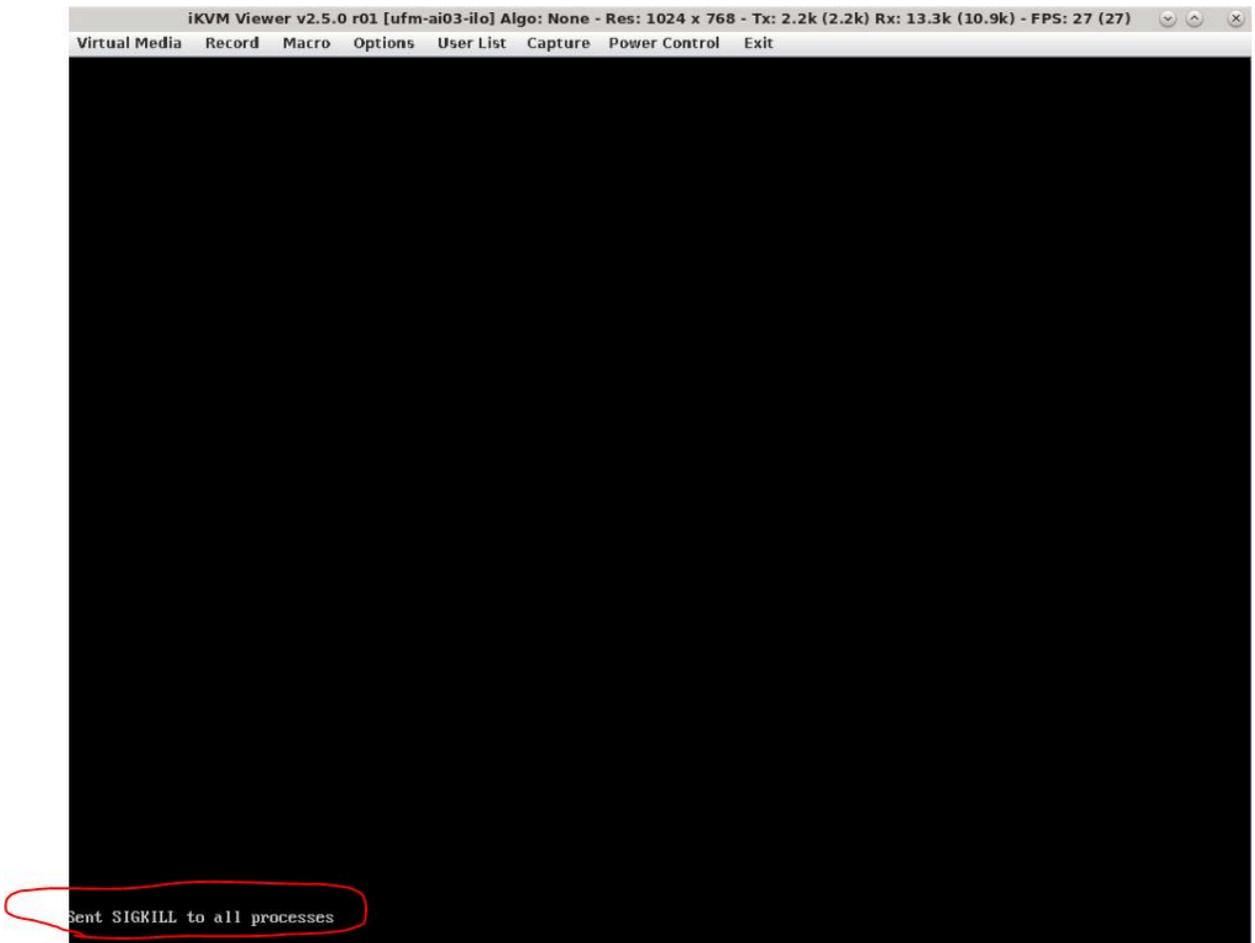
The preseed file runs in the background and will take ~35-40 minutes to complete.

a log can be viewed by switching to tty4 by click on "Virtual Media" → "Virtual Keyboard"



On the virtual keyboard that appears, press ALT+F4 (do this on the **virtual keyboard** to switch to tty4, otherwise the window will close).

9. When the OS installation is complete (if still on tty1 (purple screen)) the screen will be black and a "Sent SIGKILL to all processes" message will appear.

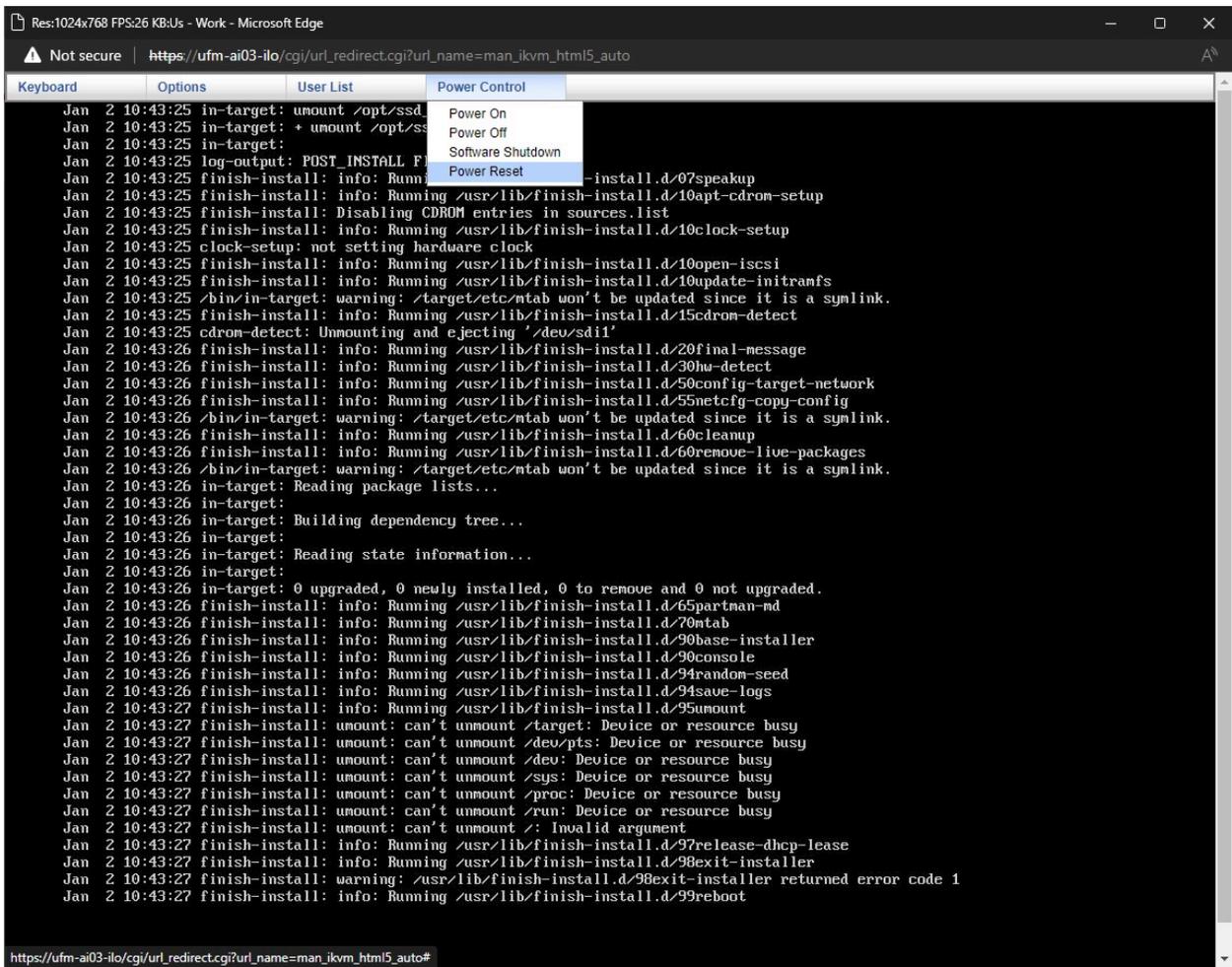


On the tty4 (log screen), a messages with "finish-install:" will appear.

```
Res:1024x768 FPS:25 KB/s - Work - Microsoft Edge
https://ufm-ai03-ilo/cgi/url_redirect.cgi?url_name=man_ikvm_html5_auto
Keyboard Options User List Power Control
Jan 2 10:43:25 in-target: umount /opt/ssd_data || true
Jan 2 10:43:25 in-target: + umount /opt/ssd_data
Jan 2 10:43:25 in-target:
Jan 2 10:43:25 log-output: POST_INSTALL FINISHED.
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/07speakup
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10apt-cdrom-setup
Jan 2 10:43:25 finish-install: info: Disabling CDRROM entries in sources.list
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10clock-setup
Jan 2 10:43:25 clock-setup: not setting hardware clock
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10open-iscsi
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10update-initramfs
Jan 2 10:43:25 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/15cdrom-detect
Jan 2 10:43:25 cdrom-detect: Unmounting and ejecting '/dev/sd11'
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/20final-message
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/30hw-detect
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/50config-target-network
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/55netcfg-copy-config
Jan 2 10:43:26 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/60cleanup
Jan 2 10:43:26 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:26 in-target: Reading package lists...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: Building dependency tree...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: Reading state information...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/65partman-md
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/70mtab
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/90base-installer
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/90console
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/94random-seed
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/94save-logs
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/95umount
Jan 2 10:43:27 finish-install: umount: can't unmount /target: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /dev/pts: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /dev: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /sys: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /proc: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /run: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /: Invalid argument
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/97release-dhcp-lease
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/98exit-installer
Jan 2 10:43:27 finish-install: warning: /usr/lib/finish-install.d/98exit-installer returned error code 1
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/99reboot
```

10. At this point, remove the USB from the Cyber-AI server (or reboot to BIOS as seen in step #3 and change the "Boot option #1" which was set to USB earlier to "disabled".

11. Reboot the server. Click the "Power Control" menu and select "Power Reset".



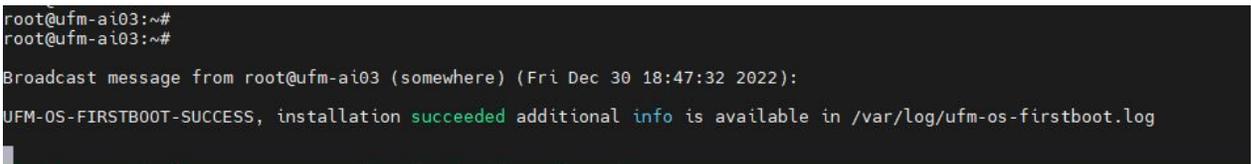
12. After the server boots up a login screen will appear.

```
Virtual Media  Record  Macro  Options  User List  Capture  Power Control  Exit
Ubuntu 18.04.6 LTS ufm-ai03 tty1
ufm-ai03 login:
```

 **Warning**

You can now log in to the server, however, the installation is not finished yet and Cyber-AI cannot be started.

- 13. Additional software installation is triggered on the server's first boot. Once complete, a message will appear on all the connected terminals "UFM-OS-FIRSTBOOT-SUCCESS" in case of success, and FAILED in case the process failed.



14. To manually check the status, run:

```
systemctl status ufm-os-firstboot
```

if the installation is still running, the output provides a status.

if the installation finished, `ufm-os-firstboot` will not be found and the log at `/var/log/ufm-os-firstboot.log` can be viewed.

```
root@ufm-ai03:~# systemctl status ufm-os-firstboot
Unit ufm-os-firstboot.service could not be found.
root@ufm-ai03:~#
```

15. Cyber-AI is now successfully installed and can be started.

Appendix - Deploying UFM Cyber-AI from an ISO File

This section provides a step-by-step guide for deploying Cyber-AI from an ISO file.

Step 1: Extract the TAR file to a temporary directory

Extract the `ufm-cyberai-appliance-<version>-omu.tar` file to a temporary directory.

```
tar xzf /path/to/ufm-cyberai-appliance-<version>-omu.tar -C /tmp
```

There is both an ISO file and an upgrade script located in the directory.

```
ls -ltrh /tmp/ufm-cyberai-appliance-<version>-omu/
-rw-r--r-- 1 root root 7.5G Dec 31 17:49 ufm-cyberai-appliance-
<version>.iso
-rwxr-xr-x 1 root root 11K Dec 31 17:49 ufm-os-upgrade.sh
```

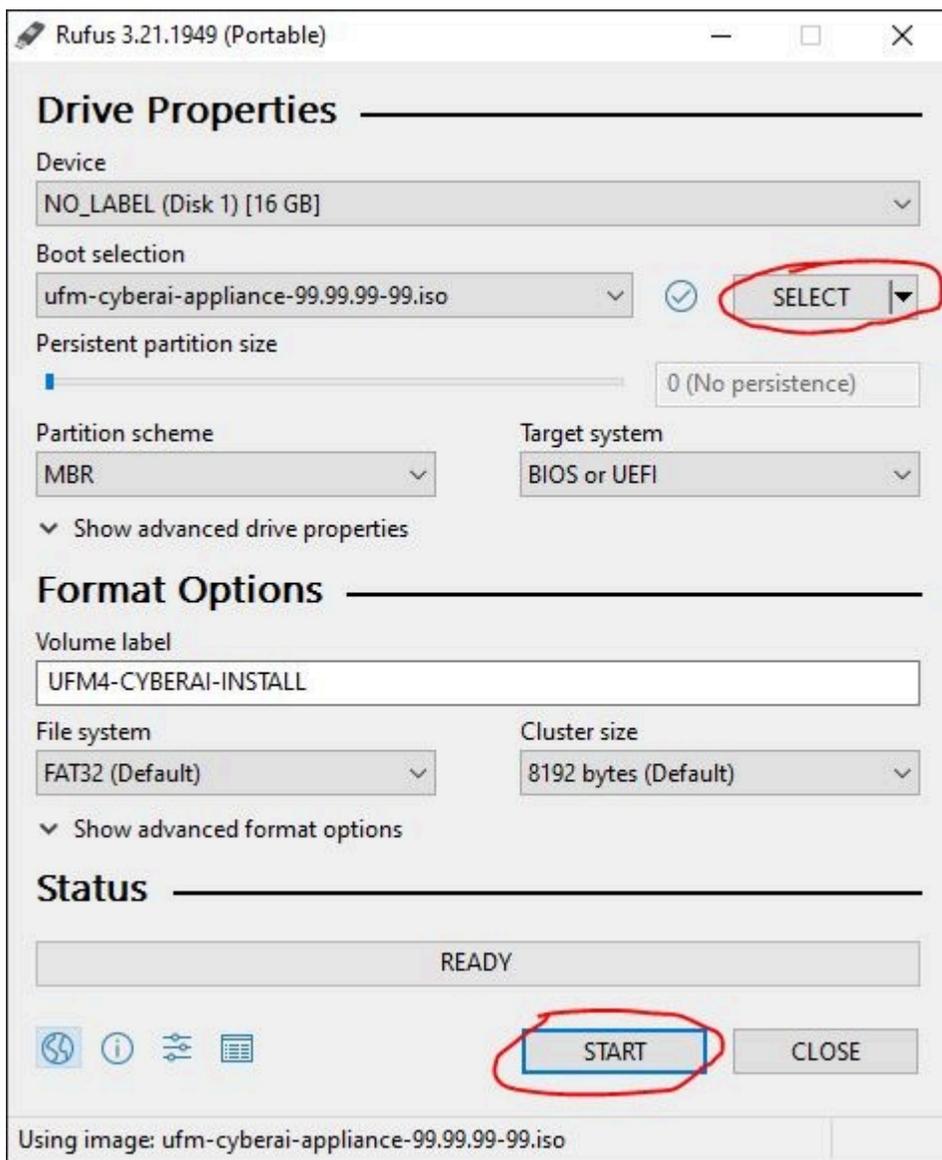
Step: 2 - Burn ISO to USB

To burn the ISO onto a USB device, you can use either a Windows or Linux operating system. Follow the instructions below depending on your preferred installation method.

Windows

1. Download and open Rufus. Refer to [Rufus - Create bootable USB drives the easy way](#).
2. Download and open the tar file `ufm-cyberai-appliance-<version>-omu.tar`.

3. Click on "SELECT" and from the drop-down menu, select the `ufm-cyberai-appliance-<version>.iso`, then click "START".



4. When the "ISOHybrid image detected" message appears, select "Write in DD mode" and then click "OK".<images/download/attachments/4054293205/iso-deployment2-version-1-modificationdate-1751291936893-api-v2.png>
5. You will see a message indicating that all data on the USB device will be erased. Click "OK and continue" to proceed.<images/download/attachments/4054293205/iso-deployment3-version-1-modificationdate-1751291937308-api-v2.png>
6. Wait for Rufus to finish.
7. Unplug the USB device.

Linux

1. Identify the USB drive by running the following command:

Warning

IMPORTANT!!! Ensure you are NOT running the following commands on a hard drive device but only on the USB (in the examples below it will be `/dev/sdb`).

Note

The USB drive is mapped to `sdb` in the following command snippet.

```
root@ubuntu18:~# ls -ltrh /dev/disk/by-id/usb*
lrwxrwxrwx 1 root root 9 Jan 2 13:44 /dev/disk/by-id/usb-
SanDisk_Cruzer_Glide_3.0_4C530000040724111091-0:0 ->
../sdb
lrwxrwxrwx 1 root root 10 Jan 2 13:44 /dev/disk/by-id/usb-
SanDisk_Cruzer_Glide_3.0_4C530000040724111091-0:0-part1 ->
../sdb1
```

2. Copy the `ufm-cyberai-appliance-<version>.iso` to the USB using the following `dd` command:

```
dd if=/path/to/ufm-cyberai-appliance-<version>.iso of=/dev/sdb
bs=4M status=progress oflag=sync
```

3. Verify that the USB is bootable:

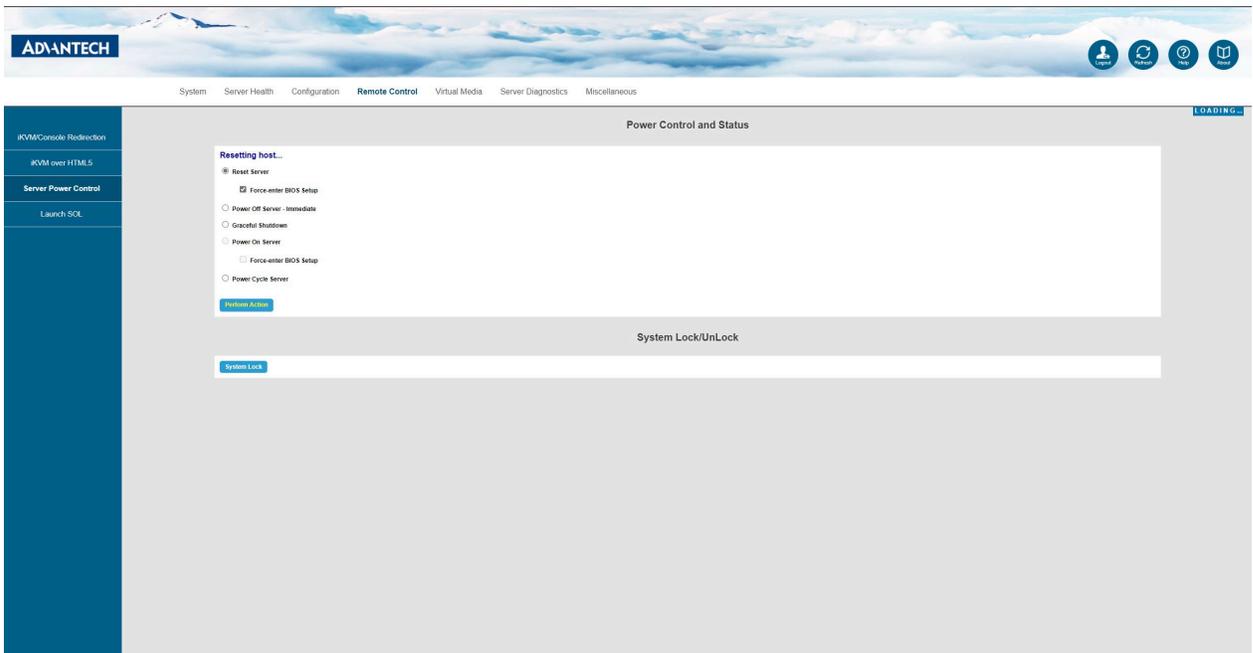
```
root@ubuntu18:~# fdisk -l /dev/sdb
Disk /dev/sdb: 14.9 GiB, 16005464064 bytes, 31260672 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x594ec03e

Device            Boot  Start          End  Sectors  Size Id Type
/dev/sdb1        *             64 15679439 15679376   7.5G 17 Hidden
HPFS/NTFS
```

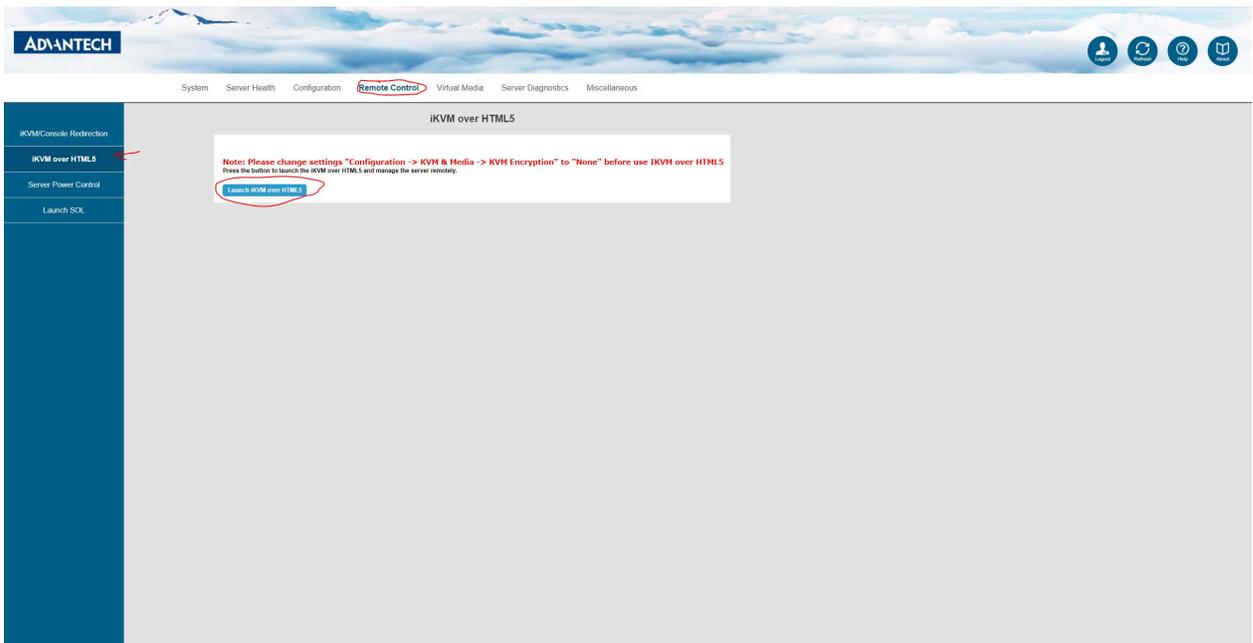
4. Unplug the USB.

Step: 3 - Manufacture Cyber-AI from USB

1. Plug the USB (prepared in the previous step) to one of the Cyber-AI server USB ports on its rear panel.
2. Log in to BMC web UI: https://<BMC_IP_ADDRESS>.
3. Navigate to "Remote Control" → "Server Power Control" and check the "Force-enter BIOS Setup" checkbox under the "Restart Server". Then, click "Perform Action".

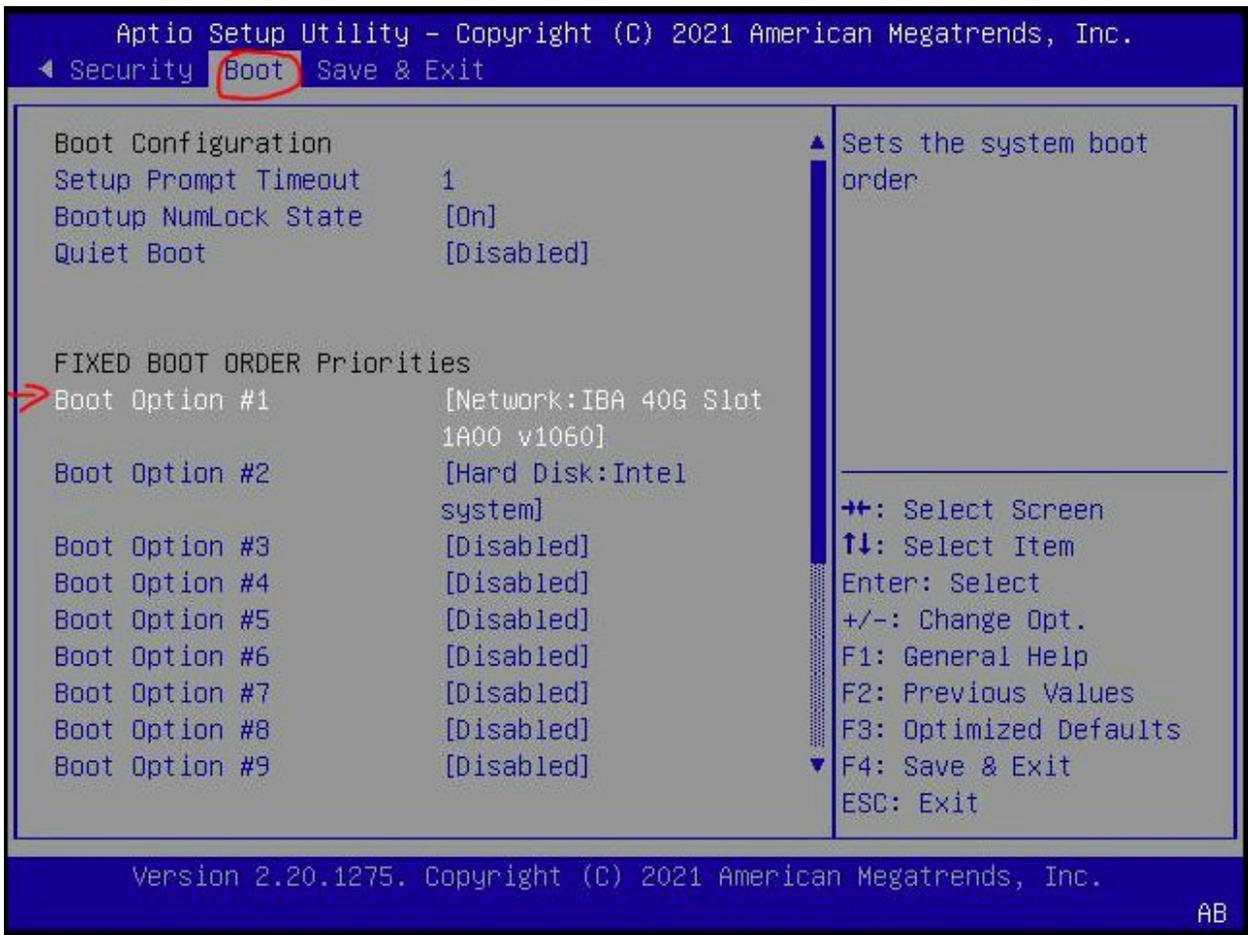


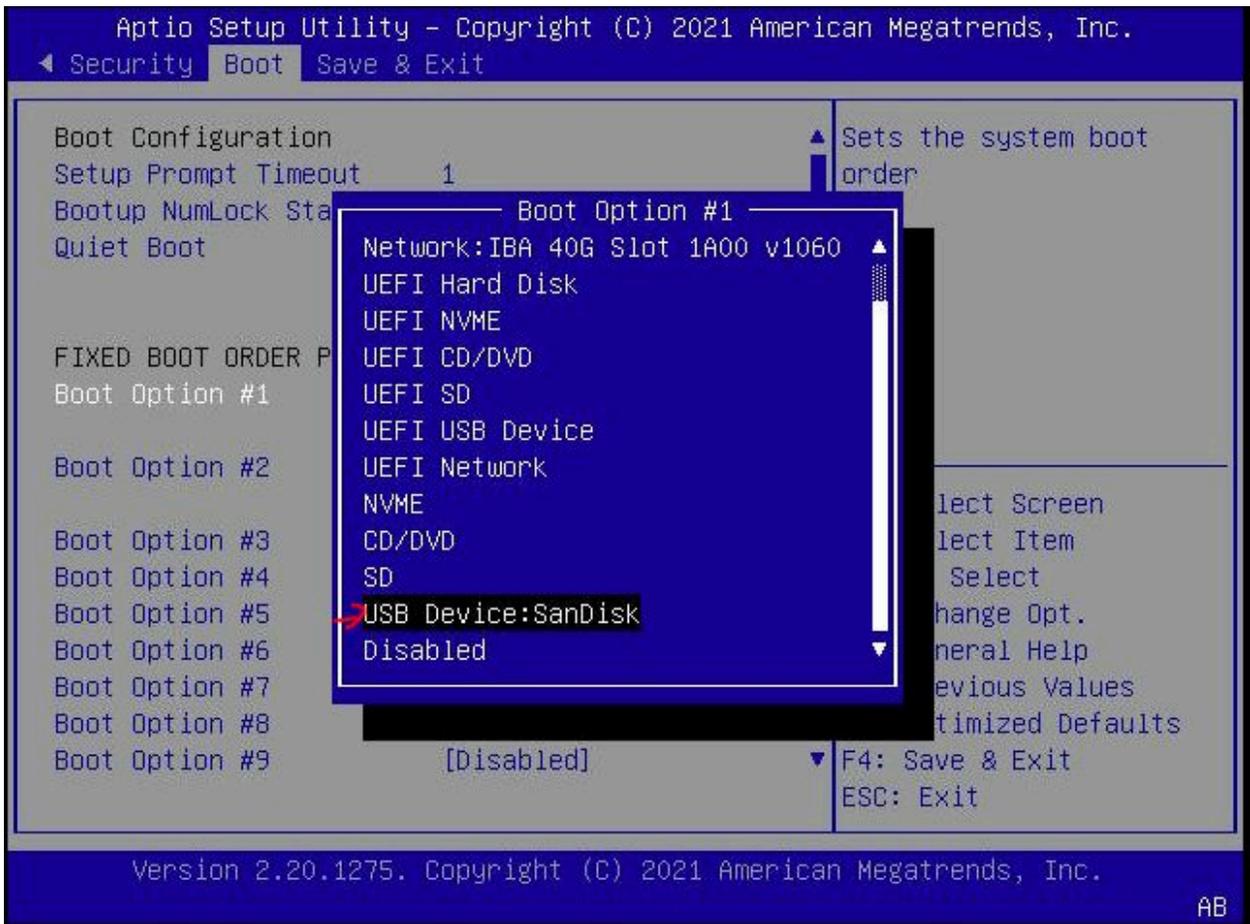
4. Navigate to "Remote Control" → "iKVM over HTML5" and click "Launch iKVM over HTML5" button.



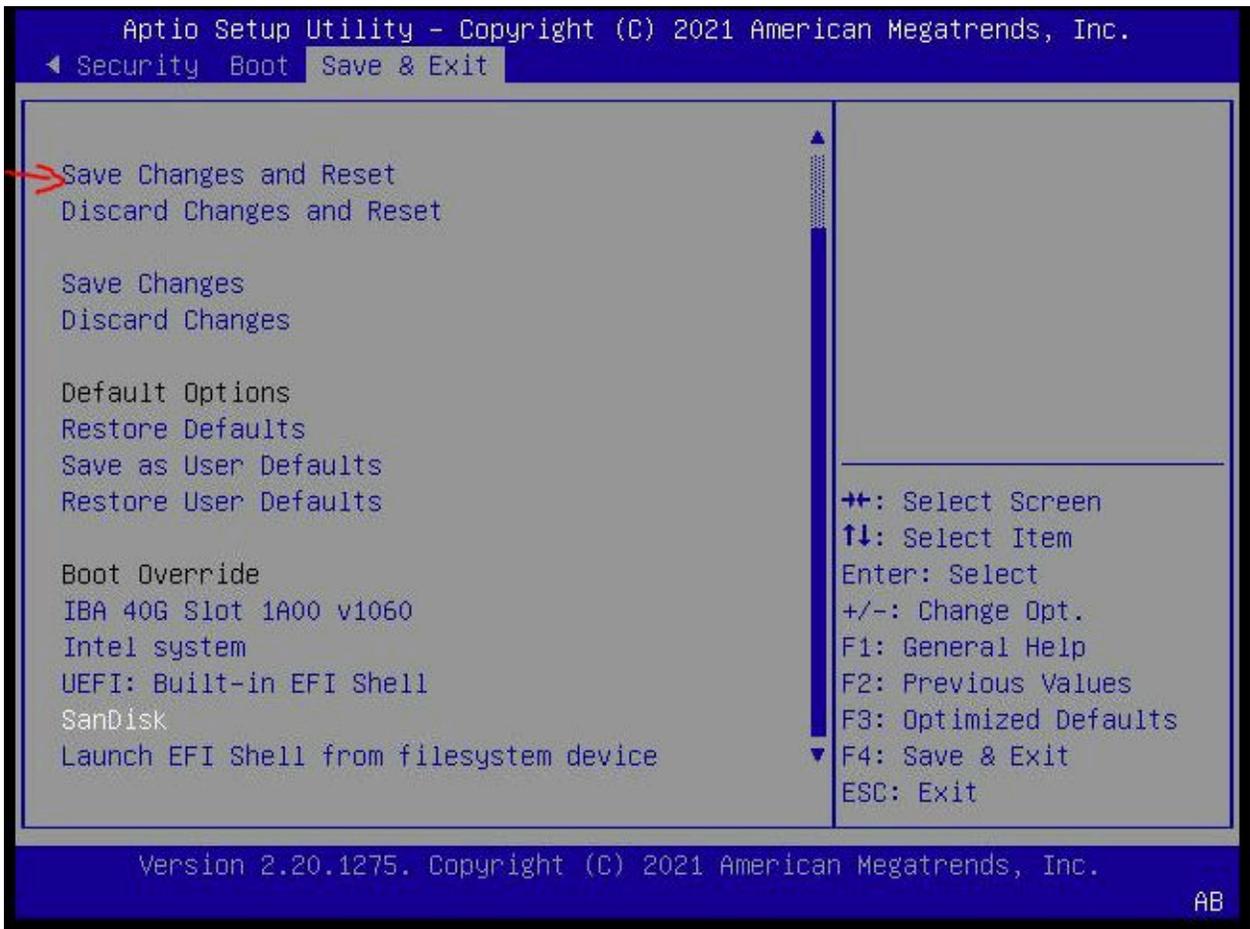
A new window will open.

5. In the BIOS menu, navigate to BOOT → "Boot Option #1" and check "USB Device: <NAME OF USB DEVICE>".

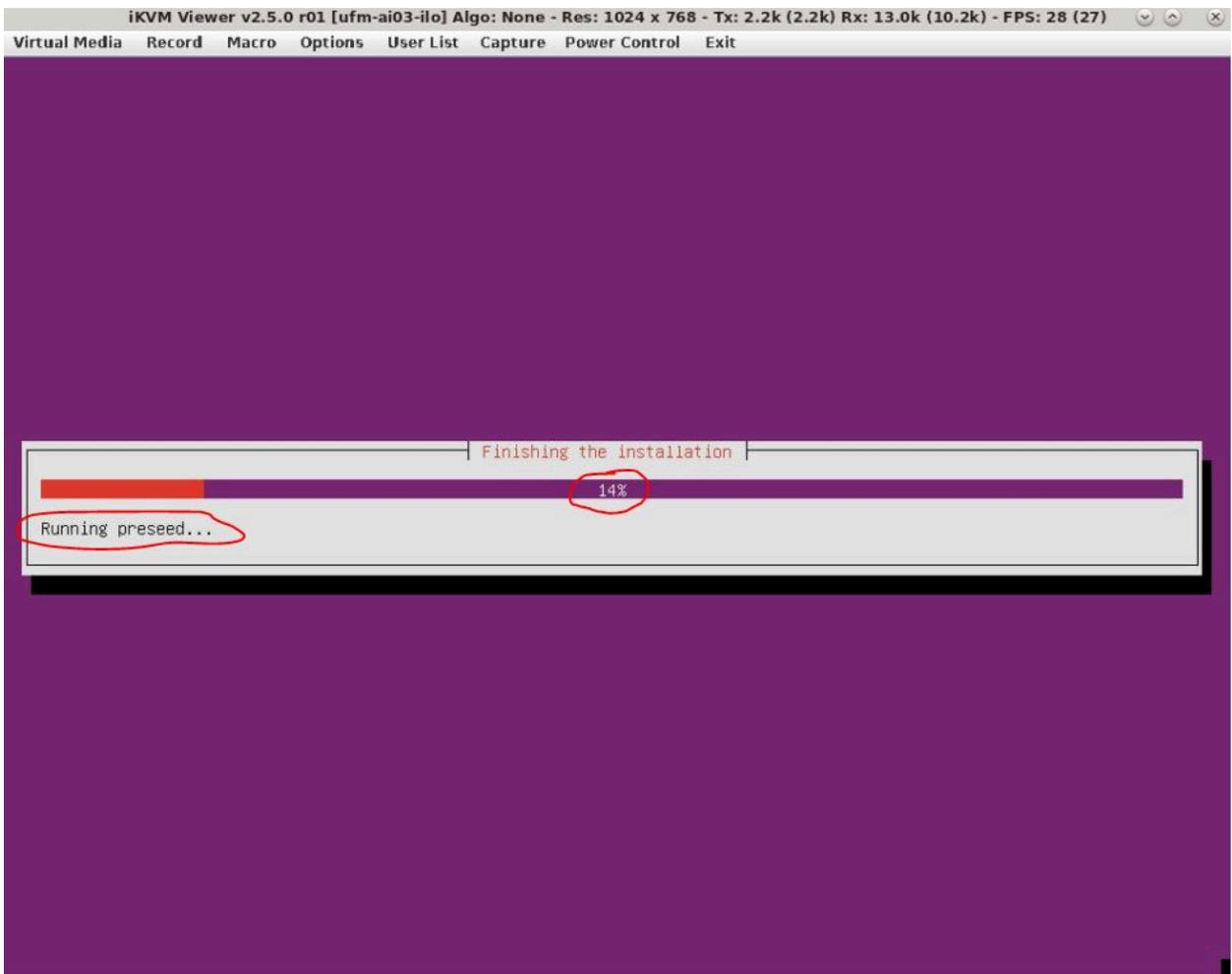




6. Navigate to "Save & Exit" → "Save Changes and Reset" and press enter.



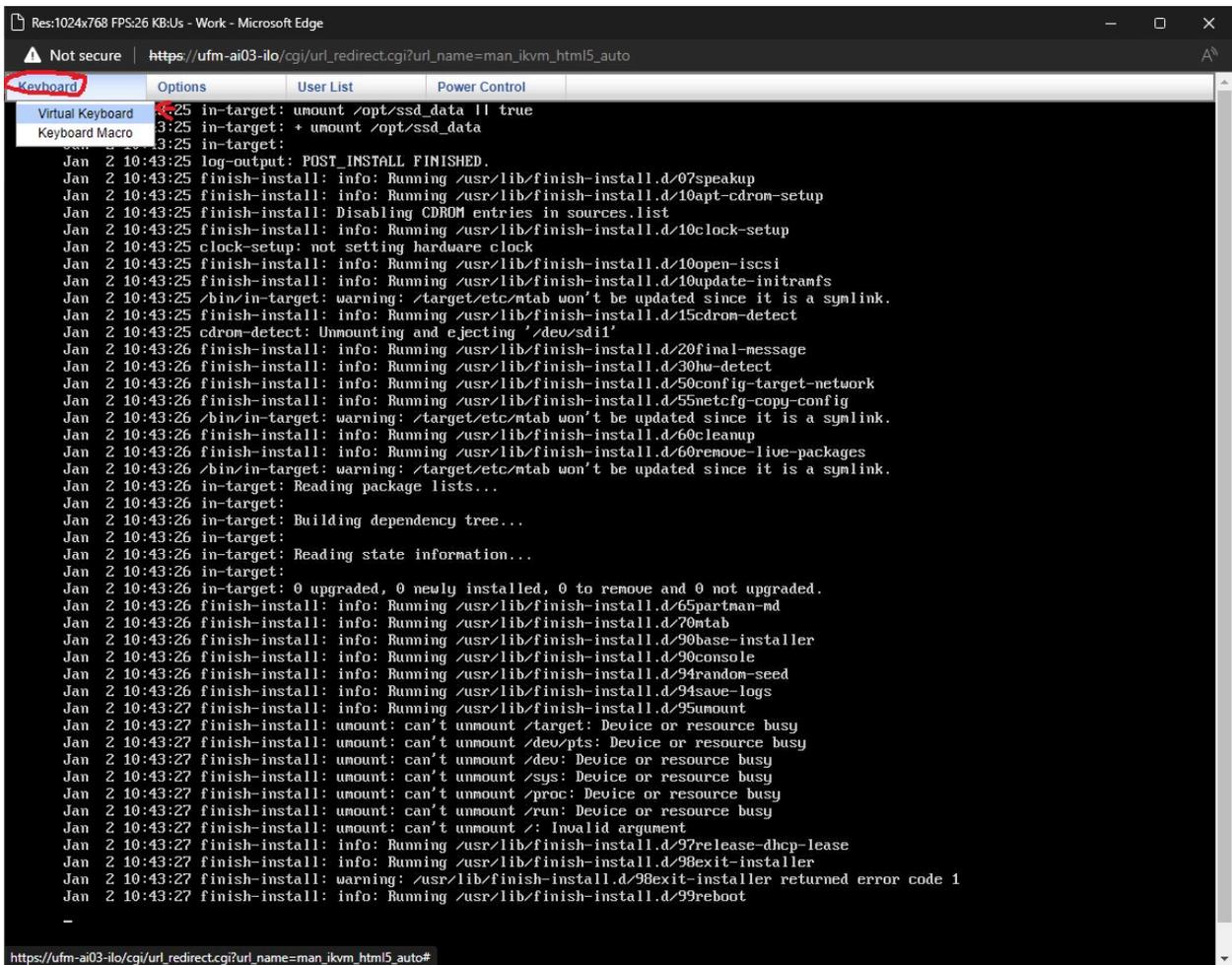
7. At this point Cyber-AI installation should start automatically.



8. The process takes ~50 minutes, "Running preseed..." will show ~14-16 percent and will remain on this percentage for most of the time. This does not mean that the process is stuck.

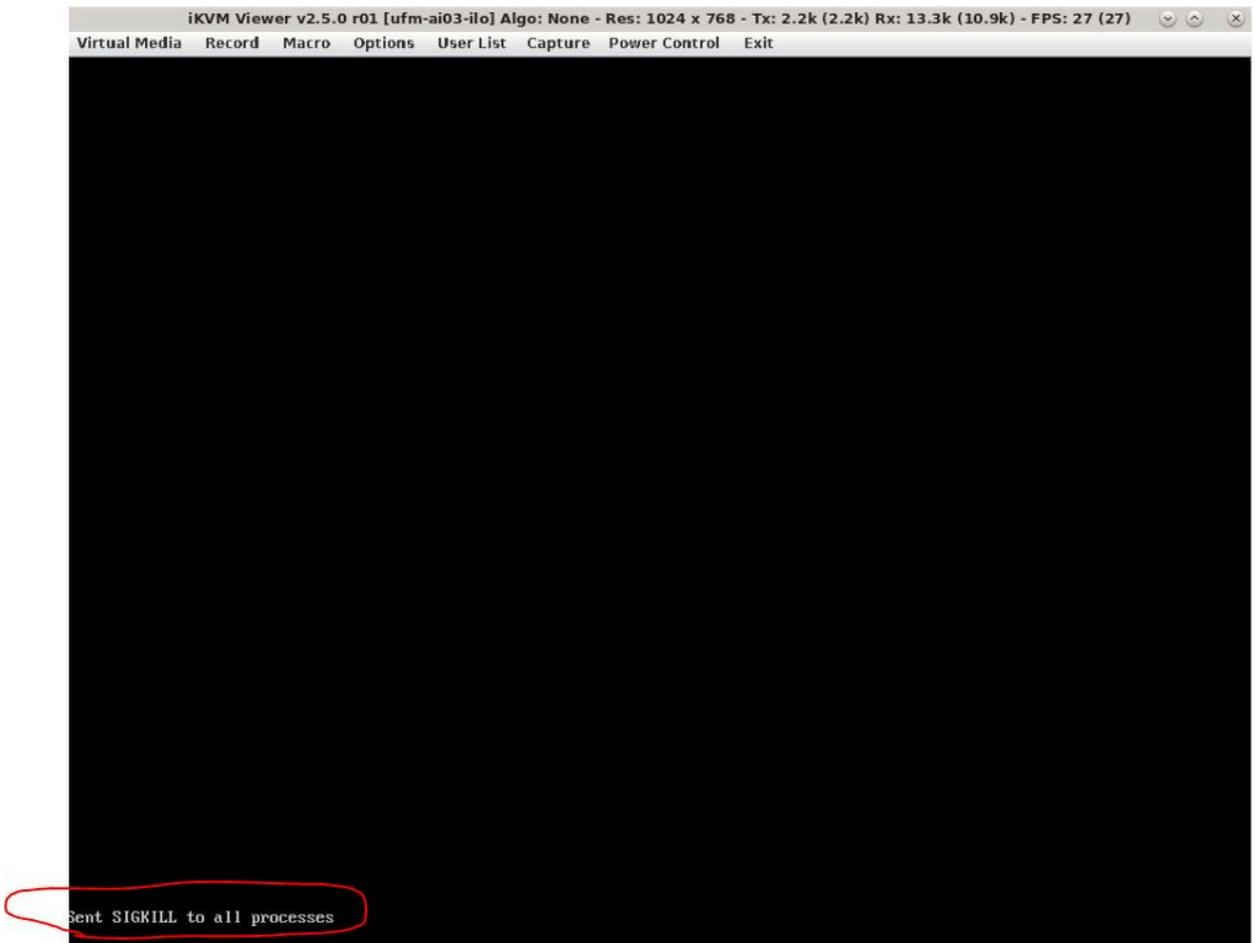
The preseed file runs in the background and will take ~35-40 minutes to complete.

a log can be viewed by switching to tty4 by click on "Virtual Media" → "Virtual Keyboard"



On the virtual keyboard that appears, press ALT+F4 (do this on the **virtual keyboard** to switch to tty4, otherwise the window will close).

9. When the OS installation is complete (if still on tty1 (purple screen)) the screen will be black and a "Sent SIGKILL to all processes" message will appear.



On the tty4 (log screen), a messages with "finish-install:" will appear.

```
Res:1024x768 FPS:25 KB/s - Work - Microsoft Edge
https://ufm-ai03-ilo/cgi/url_redirect.cgi?url_name=man_ikvm_html5_auto
Keyboard Options User List Power Control
Jan 2 10:43:25 in-target: umount /opt/ssd_data || true
Jan 2 10:43:25 in-target: + umount /opt/ssd_data
Jan 2 10:43:25 in-target:
Jan 2 10:43:25 log-output: POST_INSTALL FINISHED.
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/07speakup
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10apt-cdrom-setup
Jan 2 10:43:25 finish-install: info: Disabling CDRROM entries in sources.list
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10clock-setup
Jan 2 10:43:25 clock-setup: not setting hardware clock
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10open-iscsi
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10update-initramfs
Jan 2 10:43:25 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/15cdrom-detect
Jan 2 10:43:25 cdrom-detect: Unmounting and ejecting '/dev/sd11'
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/20final-message
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/30hw-detect
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/50config-target-network
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/55netcfg-copy-config
Jan 2 10:43:26 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/60cleanup
Jan 2 10:43:26 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:26 in-target: Reading package lists...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: Building dependency tree...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: Reading state information...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/65partman-md
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/70mtab
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/90base-installer
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/90console
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/94random-seed
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/94save-logs
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/95umount
Jan 2 10:43:27 finish-install: umount: can't unmount /target: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /dev/pts: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /dev: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /sys: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /proc: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /run: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /: Invalid argument
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/97release-dhcp-lease
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/98exit-installer
Jan 2 10:43:27 finish-install: warning: /usr/lib/finish-install.d/98exit-installer returned error code 1
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/99reboot
```

10. At this point, remove the USB from the Cyber-AI server (or reboot to BIOS as seen in step #3 and change the "Boot option #1" which was set to USB earlier to "disabled").

11. Reboot the server. Click the "Power Control" menu and select "Power Reset".

```
Res:1024x768 FPS:26 KB/s - Work - Microsoft Edge
https://ufm-ai03-ilo/cgi/url_redirect.cgi?url_name=man_ikvm_html5_auto
Keyboard Options User List Power Control
Jan 2 10:43:25 in-target: umount /opt/ssd
Jan 2 10:43:25 in-target: + umount /opt/ssd
Jan 2 10:43:25 in-target:
Jan 2 10:43:25 log-output: POST_INSTALL F
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/07speakup
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10apt-cdrom-setup
Jan 2 10:43:25 finish-install: Disabling CDRROM entries in sources.list
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10clock-setup
Jan 2 10:43:25 clock-setup: not setting hardware clock
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10open-iscsi
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/10update-initramfs
Jan 2 10:43:25 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:25 finish-install: info: Running /usr/lib/finish-install.d/15cdrom-detect
Jan 2 10:43:25 cdrom-detect: Unmounting and ejecting '/dev/sd11'
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/20final-message
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/30hw-detect
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/50config-target-network
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/55netcfg-copy-config
Jan 2 10:43:26 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/60cleanup
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/60remove-live-packages
Jan 2 10:43:26 /bin/in-target: warning: /target/etc/mtab won't be updated since it is a symlink.
Jan 2 10:43:26 in-target: Reading package lists...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: Building dependency tree...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: Reading state information...
Jan 2 10:43:26 in-target:
Jan 2 10:43:26 in-target: 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/65partman-md
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/70ntab
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/90base-installer
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/90console
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/94random-seed
Jan 2 10:43:26 finish-install: info: Running /usr/lib/finish-install.d/94save-logs
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/95umount
Jan 2 10:43:27 finish-install: umount: can't unmount /target: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /dev/pts: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /dev: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /sys: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /proc: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /run: Device or resource busy
Jan 2 10:43:27 finish-install: umount: can't unmount /: Invalid argument
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/97release-dhcp-lease
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/98exit-installer
Jan 2 10:43:27 finish-install: warning: /usr/lib/finish-install.d/98exit-installer returned error code 1
Jan 2 10:43:27 finish-install: info: Running /usr/lib/finish-install.d/99reboot
https://ufm-ai03-ilo/cgi/url_redirect.cgi?url_name=man_ikvm_html5_auto#
```

12. After the server boots up a login screen will appear.

```
Virtual Media  Record  Macro  Options  User List  Capture  Power Control  Exit
Ubuntu 18.04.6 LTS ufm-ai03 tty1
ufm-ai03 login:
```

 **Warning**

You can now log in to the server, however, the installation is not finished yet and Cyber-AI cannot be started.

- 13. Additional software installation is triggered on the server's first boot. Once complete, a message will appear on all the connected terminals "UFM-OS-FIRSTBOOT-SUCCESS" in case of success, and FAILED in case the process failed.

```
iKVM Viewer v2.5.0 r01 [ufm-ai03-ilo] Algo: None - Res: 1024 x 768 - Tx: 2.3k (2.2k) Rx: 9.7k (10.5k) - FPS: 29 (27)
Virtual Media Record Macro Options User List Capture Power Control Exit
Ubuntu 18.04.6 LTS ufm-ai03 tty1
ufm-ai03 login: UFM-OS-FIRSTBOOT-SUCCESS, installation succeeded additional info is available in /var/log/ufm-os-firstboot.log
```

```
root@ufm-ai03:~#
root@ufm-ai03:~#
Broadcast message from root@ufm-ai03 (somewhere) (Fri Dec 30 18:47:32 2022):
UFM-OS-FIRSTBOOT-SUCCESS, installation succeeded additional info is available in /var/log/ufm-os-firstboot.log
```

14. To manually check the status, run:

```
systemctl status ufm-os-firstboot
```

if the installation is still running, the output provides a status.

if the installation finished, `ufm-os-firstboot` will not be found and the log at `/var/log/ufm-os-firstboot.log` can be viewed.

```
root@ufm-ai03:~# systemctl status ufm-os-firstboot
Unit ufm-os-firstboot.service could not be found.
root@ufm-ai03:~#
```

15. Cyber-AI is now successfully installed and can be started.

Document Revision History

Revision	Date	Description
Rev 2.6.3	Jun 30, 2025	Updated Changes and New Features in This Release
Rev 2.6.1-4	Sep 24, 2024	Updated Changes and New Features in This Release
Rev 2.6.1	Dec 12, 2023	Updated: <ul style="list-style-type: none"> • Link Anomalies • Bug Fixes in This Release
Rev 2.6.0	Nov, 2023	Updated Job Analytics
Rev 2.5.1	Aug, 2023	Updated Bug Fixes in This Release
Rev 2.5.0	Aug, 2023	Updated Bug Fixes in This Release
Rev 2.4.0	May, 2023	Updated: <ul style="list-style-type: none"> • Changes and New Features in This Release • Bug Fixes in This Release • Known Issues • Upgrading UFM Cyber Software • ufm-cai-sanity - Updated usage • ufm-cai-status - Updated configuration • ufm-cai-weekly-alerts-report - Updated usage and options Added: <ul style="list-style-type: none"> • Running Cyber-AI Plugin • Appendix - Deploying UFM Cyber-AI from an ISO File • UFM Cyber-AI OS Upgrade
Rev 2.3.0	Jan, 2023	Updated: <ul style="list-style-type: none"> • Changes and New Features in This Release

Revision	Date	Description
		<ul style="list-style-type: none"> • Bug Fixes in This Release <p>Added:</p> <ul style="list-style-type: none"> • Bug Fixes History • ufm-cai-weekly-alerts-report • Appendix - Cyber-AI Appliance OS Remanufacture
Rev 2.2.1	Dec, 2022	Updated Bug Fixes in This Release
Rev 2.2	Oct, 2022	<p>Added:</p> <ul style="list-style-type: none"> • Cable Alerts Summary • CLI Tools • Morpheus Integration <p>Updated</p> <ul style="list-style-type: none"> • Changes and New Features in This Release • Software Management • Cyber-AI Analytics • Get Specific Network Alert • Get Specific Tenant Alert • Threshold Events • High Availability

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation ("NVIDIA") makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

Trademarks

NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

© Copyright 2025, NVIDIA. PDF Generated on 06/30/2025