NVIDIA UFM Cyber-AI Documentation

v2.7.0

Table of Contents

You can download a PDF version here.

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.

1 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.

1.1 Changes and New Features in This Release

1.1.1 Changes and New Features in v2.7.0

Feature	Description
Web UI Improvements	Updated Cyber-AI Analytics
REST API	• In Link Analysis: Updated Get Link Failure Prediction History and Get Link Anomaly Prediction History • In Alert Filters: Get Histogram for Link Statu, Link Status and Get Properties for Link Status

1.2 Bug Fixes in This Release

N/A

1.3 Known Issues

N/A

1.4 Changes and New Features History

1.4.1 Changes and New Features in v2.6.0 and 2.6.1

Feature	Description
Job Analytics	Added two job types: "ML Hourly Anomaly" and "ML Hourly Model". For more information, refer to Job Analytics

1.4.2 Changes and New Features in v2.5.0

No changes and new features were introduced this release.

1.4.3 Changes and New Features in v2.4.0

Feature	Description
Cyber-AI plugins	Added Running Cyber-AI Plugin

Feature	Description
Deploying UFM Cyber-AI from an ISO File	Added instructions on deploying UFM Cyber-AI from an ISO file. For more information, refer to Appendix - Deploying UFM Cyber-AI from an ISO File

1.4.4 Changes and New Features in v2.3.0

Feature	Description
DPU telemetry Integration	Accumulate telemetry data from ethtool and sysfs providers.
Cyber-AI Appliance OS Remanufacture	Added instructions on how to remanufacture the Cyber-AI appliance and OS. For more information, refer to Appendix - Cyber-AI Appliance OS Remanufacture.

1.4.5 Changes and New Features in v2.2.0

Feature	Description
Morpheus integration	Included Morpheus Integration in the production level
Cable Anomalities Detection	Added additional properties to the Cable Animalities Detection table
Cable Analysis Improvements	Added the following: • Option to filter by clicking on the bars • Added percentage to bars
Automatic Evaluation License	Generated default evaluation license on first launch
Reorganized Cyber AI Tools	All Cyber AI tools are documented and have the ‘ufm-cai-‘ prefix

1.4.6 Changes and New Features in v2.1.0

Feature	Description
Recommended Actions	Recommended actions for anomalies and alerts were improved to give a recommendation procedure and steps to follow to fix this alert/anomaly
Support SLURM based on UFM Logical-Servers	Aggregate data from devices that belongs to the same logical server, analyze this data and find alerts or anomalies at the logical server level
Combining of Cable info into one tab	Two cable tabs were combined into one tab for better user experience
Filtering Up to Down only for Anomaly View	SanKey graphs are not to be filtered once other objects filtered
Refresh button adding to all UFM Cyber-AI tabs	Added manual and automatic refresh per each dashboard
Adding Version Number to every tab in UFM Cyber-AI	Version number should be available on every tab in UFM Cyber-AI

Feature	Description
Detecting incompatible FW version in UFM Cyber-AI	Sometime the statistics are coming zero due to incompatible version of FW. The comparison of several parameters such as `RX_power <>0` , `TX_bias=0` and `Link_Up=true` will provide with recommended action to upgrade the software.
Morpheus integration	Morpheus Integration was tested in Beta level, but not included
Integrate GPU usage for model training	Using GPU to enhance performance of model training was tested in POC level, but not included
Integration and Infrastructure improvement	• Integrated latest versions of UFM Telemetry and UFM Enterprise • Improved scheduler settings infrastructure

1.4.7 Changes and New Features in v1.1.0

Feature	Description
Cable Anomalies	Added new cable anomalies analysis based on cable attributes trend, a tachometer indication was added also for each anomaly
HA Service (2 nodes)	Added high-availability (HA) support for two Cyber-AI appliances based on DRBD and Pacemaker
Weekly average	Added ability to display weekly average graphs for relevant counters
Data cleanup	Added support for data cleanup, purge, or archiving of old UFM Cyber-AI data files
Anomalies Analysis View	Added new tab for Anomaly Analysis view

1.5 Bug Fixes History

Ref #	Issue
3665932	**Description**: Fixed issue with Anomaly Analysis page
	Keywords: Anomaly, Analysis
	Discovered in release: 2.6.0
3590777	**Description**: After upgrading UFM new telemetry data is not being collected and presented in UI Telemetry tab.
	Keywords: Telemetry, Coredump
	Discovered in release: 2.5.0
3526950	**Description**: Fixed database exception pop-up when inserting link anomaly.
	Keywords: Database, Link Anomaly
	Discovered in Release: 2.4.0
3500018	**Description:** Rectified Analytics job files cleanup issue.

Ref #	Issue
	Keywords: Analytics Job, Cleanup, File
	Discovered in Release: 2.4.0
3467140	**Description**: Added names of stuck jobs to the Cyber-AI status mail.
	Keywords: Status Mail, Stuck Jobs
	Discovered in Release: 2.4.0
3465217	**Description:** Fixed the last-fail-time and last-run displayed in the job status report table.
	Keywords: last-fail-time, Jobs, Status Report
	Discovered in Release: 2.4.0
3459304	**Description**: Fixed Cable daily job failure due to infinity value set in the cable info file.
	Keywords: Cable Daily Job, Infinity Value, Cable Info File
	Discovered in Release: 2.3.0
3448286	**Description**: Fixed issues in Crypto aggregation jobs while generating mining events.
	Keywords: Crypto Aggregation Jobs, Mining Events
	Discovered in Release: 2.4.0
3400002	**Description**: Updating cables telemetry data fails due to negative values from CollectX
	Keywords: Cables, Telemetry, CollectX
	Discovered in Release: 2.3.0
3438034	**Description:** Cyber-AI fails to start on RH as the 'cgroup' file in the container has a different format
	Keywords: Start, RH, Container, Cgroup
	Discovered in Release: 2.3.0
3429609	**Description:** Error in machine learning weekly jobs as the progress must be between 0 and 100, but 102 is given
	Keywords: Machine Learning, job, progress
	Discovered in Release: 2.3.0
3412545	**Description:** Error in Cyber-AI health check when checking log rotate and some archived files were deleted
	Keywords: Health, Log Rotate, Archived
	Discovered in Release: 2.3.0
3332098	**Description**: Error when collecting link failure alerts
	Keywords: Link Failure, Alerts
	Discovered in Release: 2.2.0
3307699	**Description**: The dow analytic job performs unnecessary cleanup of collected system files
	Keywords: Dow, Analytic Job, Cleanup, System Files

Ref #	Issue
	Discovered in Release: 2.2.0
3305254	**Description**: The model column is empty in specific nodes in topology file
	Keywords: Model, Topology File, Empty column
	Discovered in Release: 2.2.0
3282605	**Description**: Dashboard scale represents wrong values on graphs
	Keywords: Dashboard Scale, Graphs
	Discovered in Release: 2.2.0
3272059	**Description**: Delay of weekly jobs schedule due to Cyber-AI restart
	Keywords: Weekly Jobs, Delay
	Discovered in Release: 2.2.0
3242420	**Description**: Cyber-AI scheduler keeps getting stuck
	Keywords: Cyber-AI, Scheduler
	Discovered in Release: 2.2.0
3240067	**Description**: Sorted cable status by length in the "Cable Analysis" page
	Keywords: Cable Analysis, Cable Status by Length
	Discovered in Release: 2.2.0
3254644	**Description**: Removed License Info warning following Cyber-AI start and initial configuration
	Keywords: License Info, Installation, Warning
	Discovered in Release: 2.2.0
3272941	**Description**: Fixed issue with "list index out-of-range" exception in machine-learning-hourly job
	Keywords: List index out-of-range; Machine-learning-hourly job
	Discovered in Release: 2.2.1
3270590	**Description**: Excluded BER counter for distribution compare as its value is very small
	Keywords: BER Counter; Distribution Compare
	Discovered in Release: 2.2.0
3270580	**Description**: Excluded corrupted rows with influencer name "nothing" in the cable alert files
	Keywords: Cable Alert Files
	Discovered in Release: 2.2.0
3270573	**Description**: The default (mixed) model is not used when running the machine-learning-hourly job
	Keywords: Machine-learning-hourly job; Mixed model
	Discovered in Release: 2.2.0

1.6 Known Issues History

Ref #	Issue
3448286	**Description**: Crypto mining events are not being raised
	Workaround: N/A
	Keywords: Crypto Mining Events
3054757/3054735	**Description:** Upgrade of UFM Cyber-AI with UFM Enterprise from 1.1.0 to 2.0.0 does not work.
	Workaround: Uninstall UFM Enterprise and upgrade Cyber-AI.
	Keywords: Upgrade UFM Enterprise HA.
	Discovered in version: 2.0.0
2939711	**Description:** Cable information collection error occurs when running in HA mode.
	Workaround: The operation succeeds when reattempted.
	Keywords: Cables HA
	Discovered in version: 2.0.0
2854289	**Description**: Several ports are open in the UFM Cyber-AI appliance; such as 22, 23, 443, 8443.
	Workaround: N/A
	Keywords: Open ports
	Discovered in version: 1.1
2854289	**Description:** Several ports are open in UFM Cyber-AI appliance such as 22, 23, 443, 8443.
	Workaround: N/A
	Keywords: Open ports
	Discovered in version: 1.1
2903566	**Description**: Anomalies with probability equals to zero will have a “Notice” severity instead of “Warning”.
	Workaround: N/A
	Keywords: Anomaly probability Notice
	Discovered in version: 1.1
2872303	**Description**: HA take-over/fail-over has a stickiness time interval of 15 minutes, if reboot is done on the master during this period it will take ownership once it's up.
	Workaround: Try to avoid rebooting system during the 15 minutes interval.
	Keywords: HA take-over/fail over
	Discovered in version: 1.1

2 Software Management

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

2.1 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.

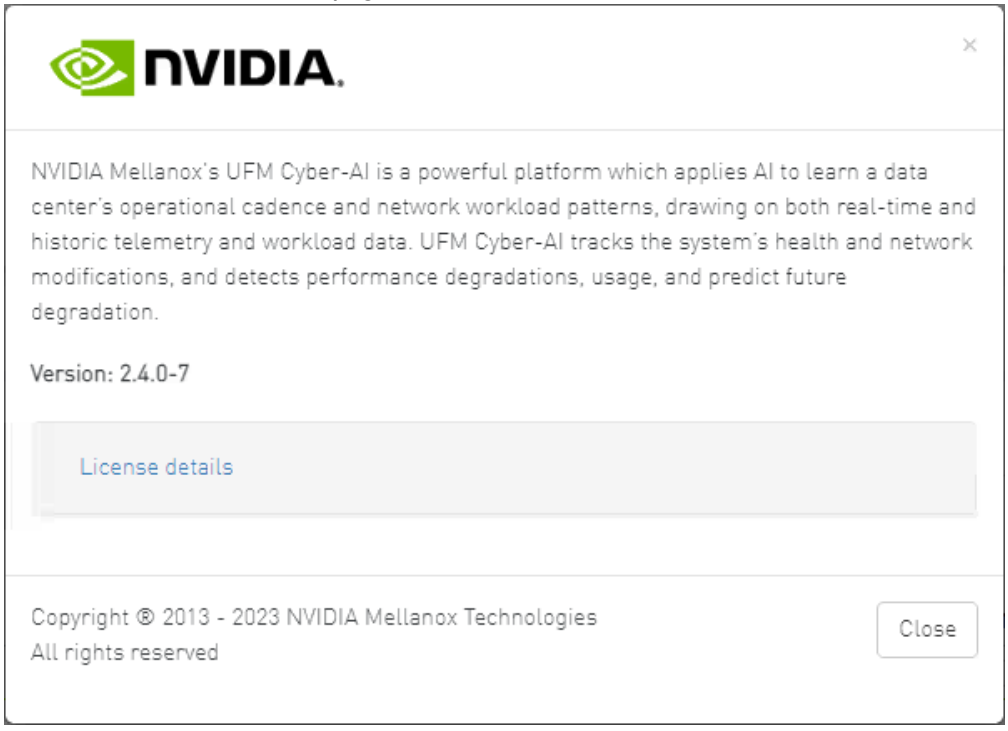
11. To access the UFM Cyber-AI logs, run the following on the UFM Cyber-AI appliance:

```
[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
```

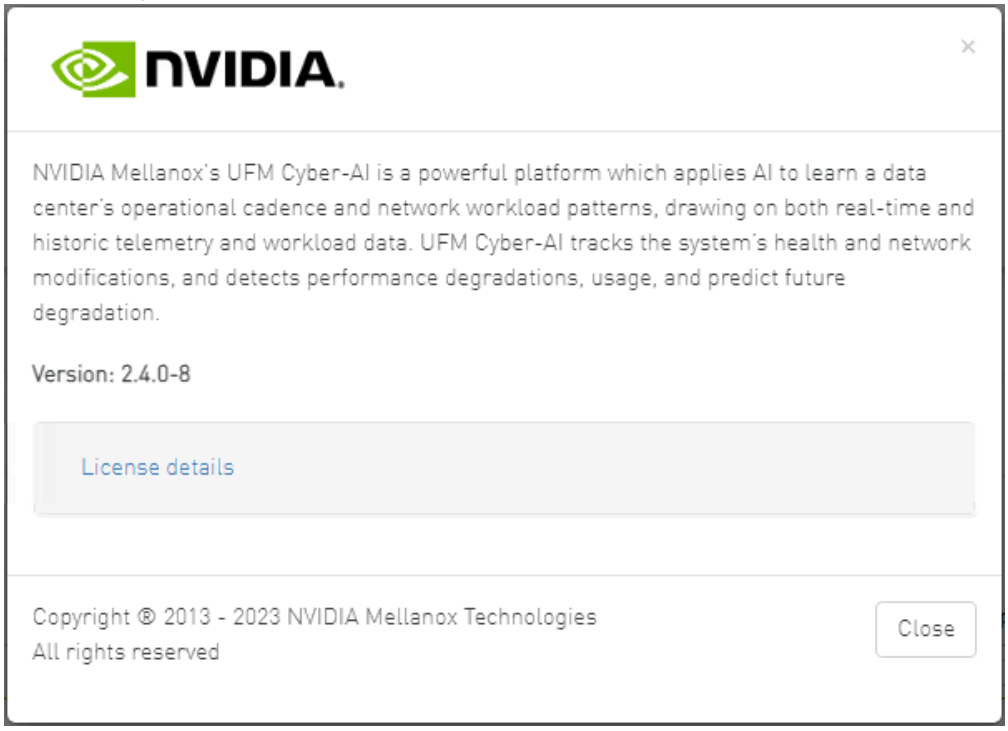
12. For settings and configuration instructions, see Settings and Configuration.

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".



2.2 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!
```

2.3 Running Cyber-AI Plugin

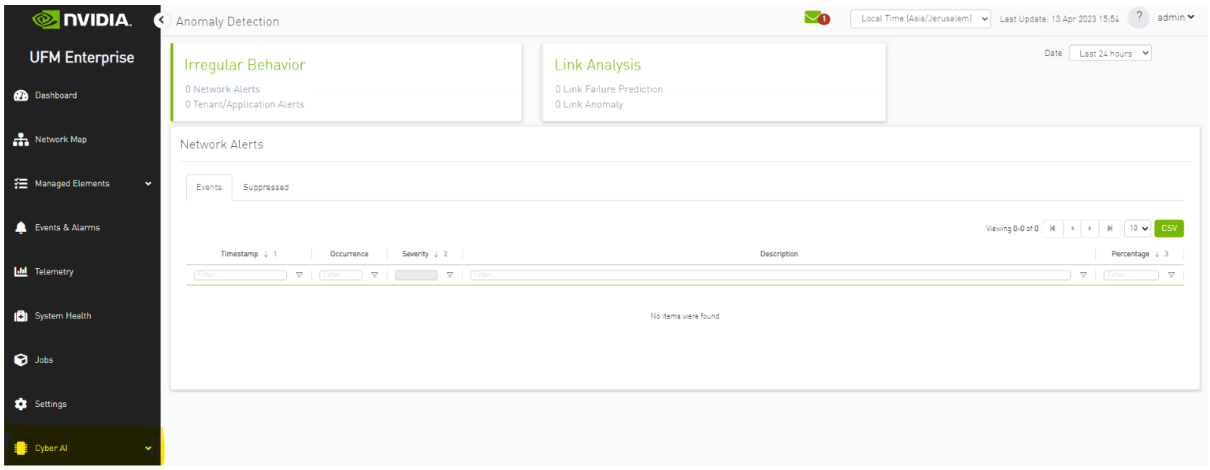
To integrate Cyber-AI with UFM Enterprise, it can be employed as a plugin. To achieve this, follow the below instructions.

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.

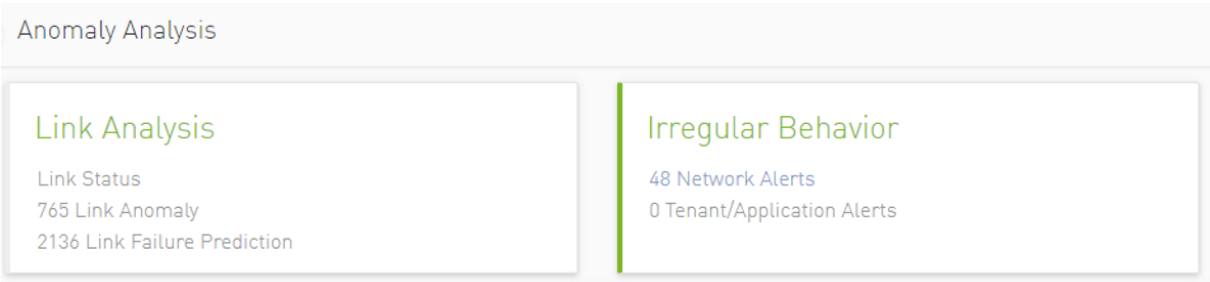


Cyber-AI APIs can be accessed from the remote host via UFM Enterprise using the following URL. You should log in with UFM Enterprise authentication:

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

3 Cyber-AI Analytics

3.1 Anomaly Analysis



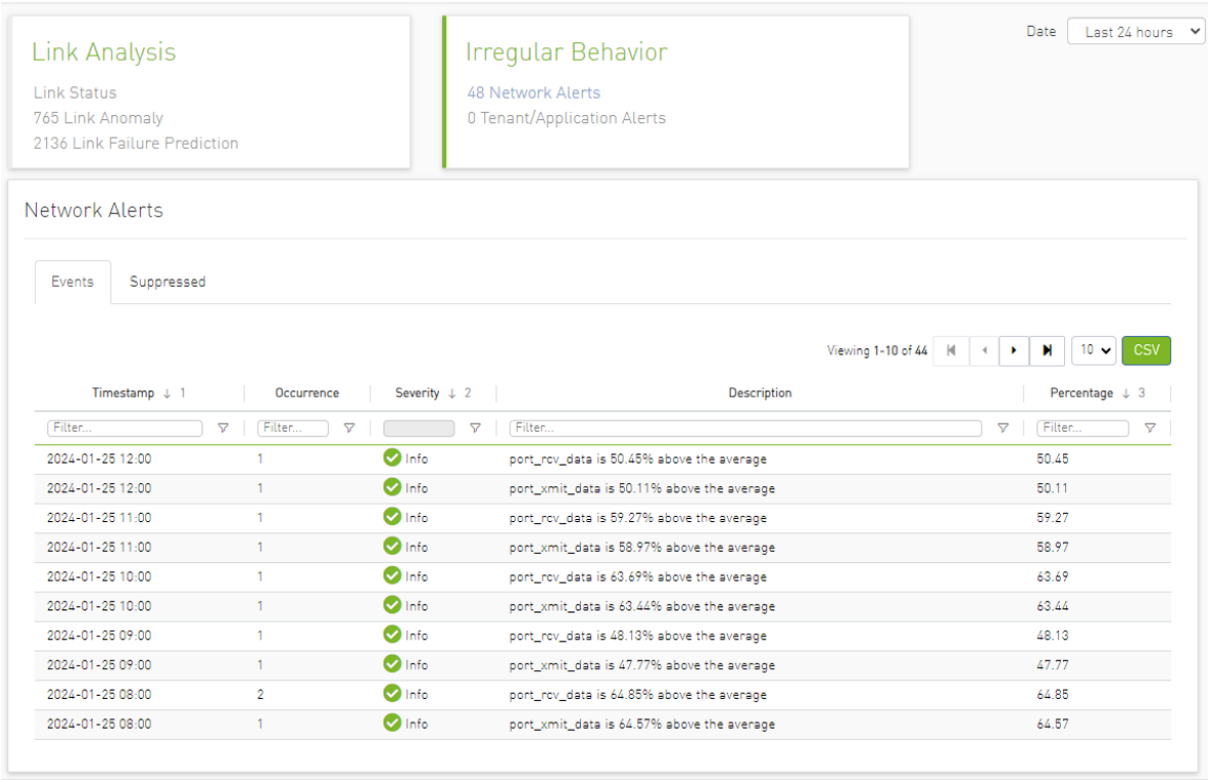
- Link Status: Collects information about the links periodically.
- Link Anomaly: Detects anomalous behavior in the cluster with a probability indicator. It detects the most significant influencers on the anomaly notice.
- Link Failure Prediction: Prediction of future link failures 1-to-24 hours in advance using machine learning algorithms with a probability indicator.
- 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.

3.1.1 Network Alerts

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 recommended actions related to the selected alert anomalous parameter over three different time ranges.

Prev Next

Recommended Actions

Site Name test

Time 2024-01-25 10:00

Creation Time 2024-01-25 10:00

Severity Info

Description port_rcv_data:540330257 is above the average: 330085573

Recommended Actions

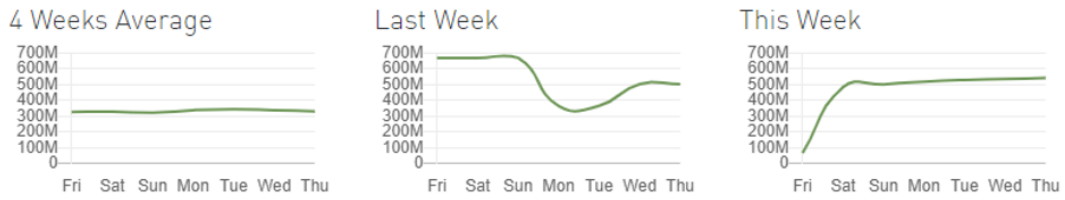
- These steps should be applied on top 5 ports
- Port reset and keep monitoring
- If still getting the alerts, please check if there any related cable alerts via cable anomaly tab
- In addition please check relevant cable measure trend via cable anomaly tab
- If there are alerts for connected cable and/or depredating trend please consider cable replacement
- If known issue due to maintenance activity please use suppress function do define as known issue

Network Members

Node Name	Node GUID	Port	Port Received Data	Role	Type
il-sim-yoks-0382 mlx4_0	0xf4521403007c3a80	1	536870912	endpoint	host
mtlxls04-slv02	0xf4521403006d28e0	2	536870912	endpoint	host
mtlxls04-slv01	0xf4521403006d25b0	2	536870912	endpoint	host
mtlxds01	0xf45214030015751 0	2	536870912	endpoint	host
mtlxls01	0xf45214030001db70	1	536870912	endpoint	host

Top influencers

Average Port Received Data



Add More

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

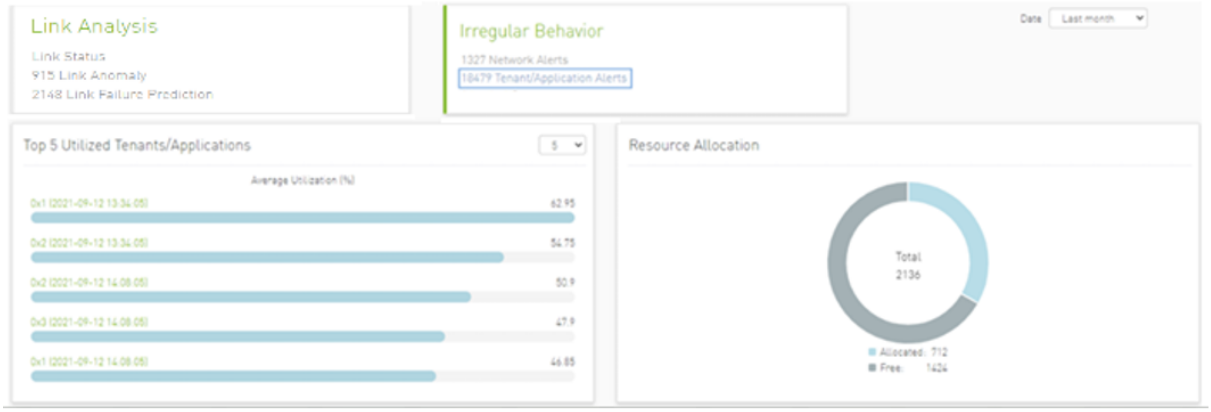
3.1.2 Tenant/Application Alerts

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

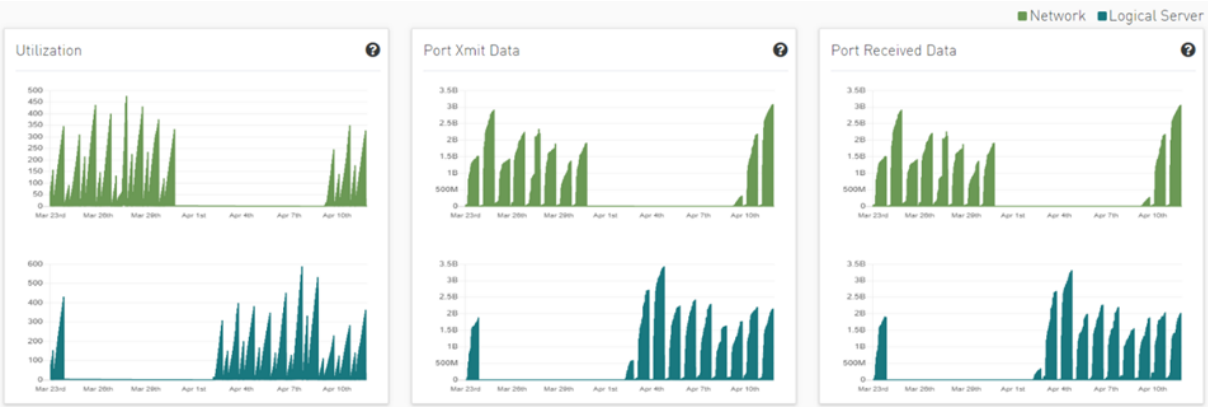
Based on normalized congestion measurements (the default is greater than 70%) the system detects the most congested PKeys. This is done by counting the amount of time when the alert is received.

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

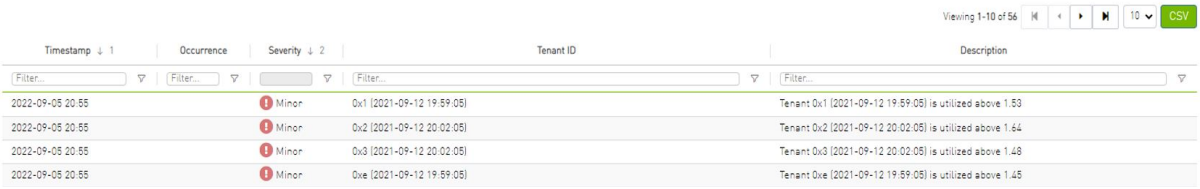
Detailed event information is provided to the user regarding PKey alerts, where the user can see PKey details and descriptions of the alert.



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.

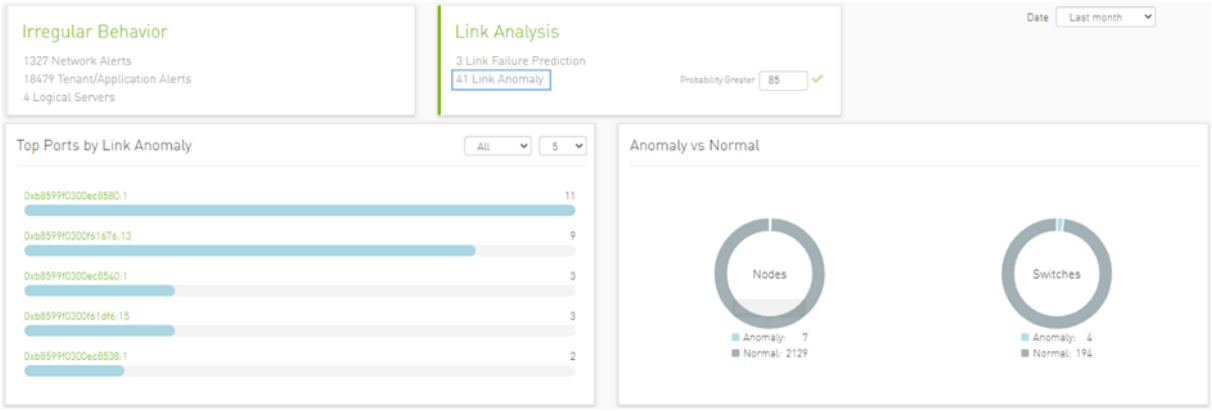


3.1.3 Link Failure Prediction

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.

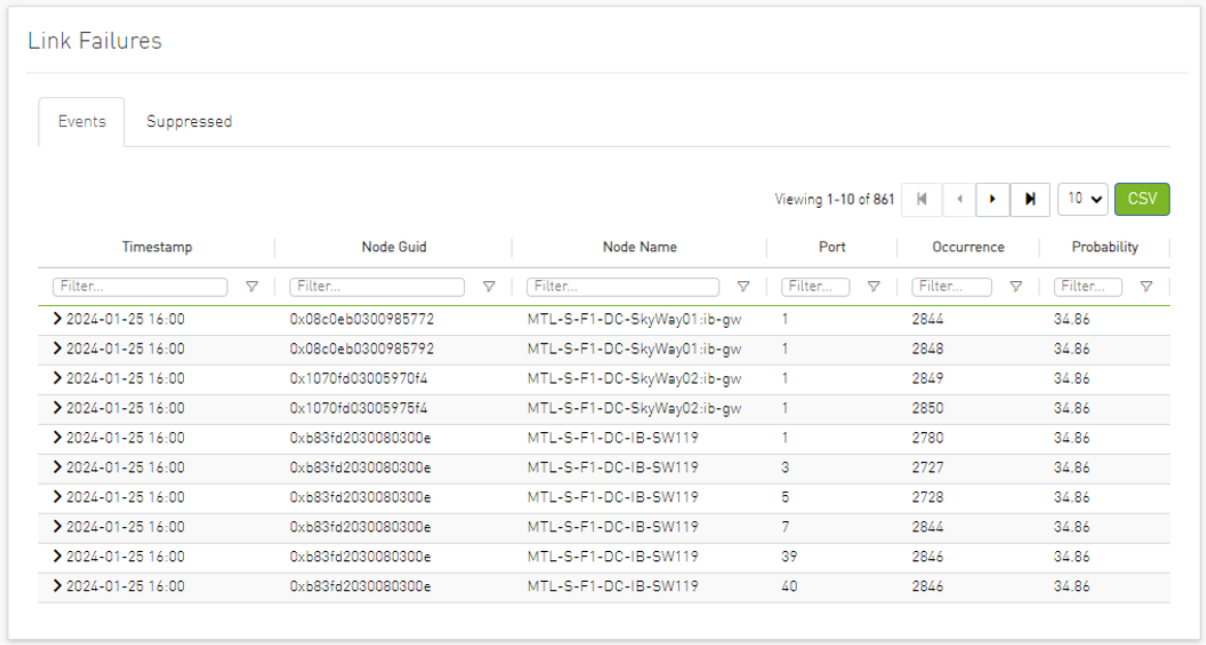
Using the machine learning algorithm, the processor derives the potential failure pattern by, for example, alerting future failure times of components. The processor repeatedly updates the alerted future failure times based on newly collected failures.

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.

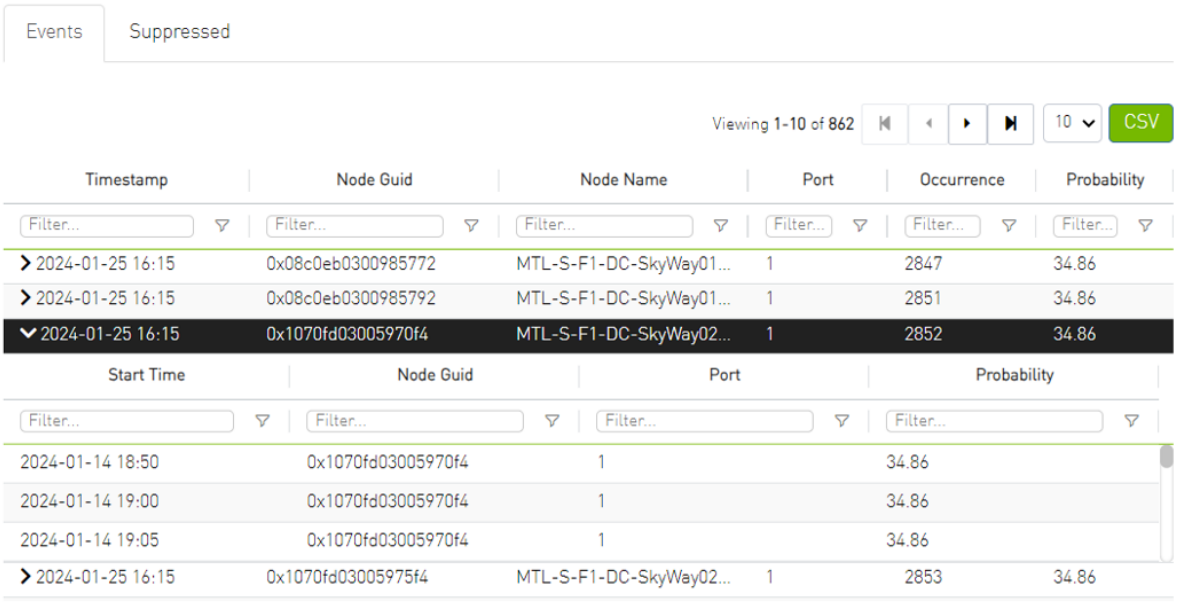


In the “Top Ports by link” graph, the user can filter the alerts table below by clicking any node name on the graph to add the appropriate filters to the table.

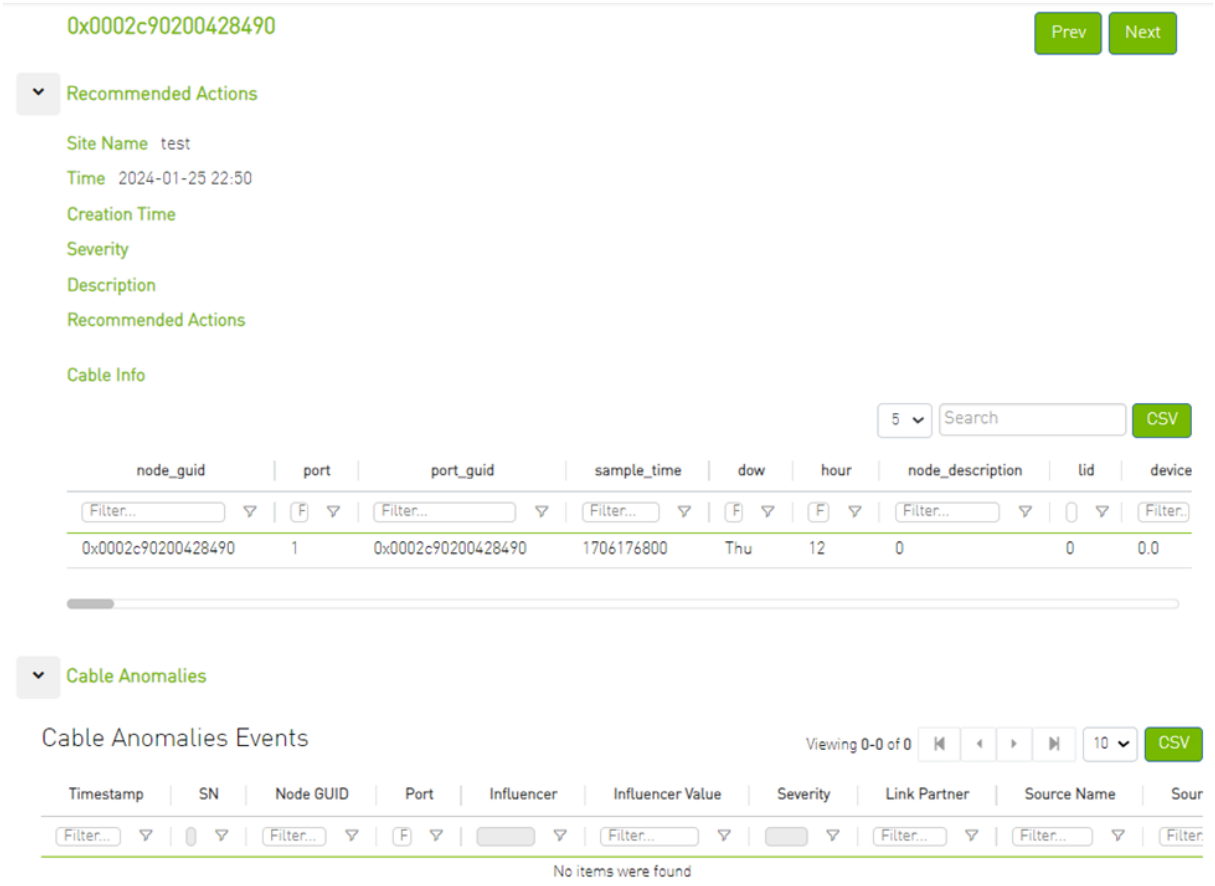
Users may see the detailed events through an event list where alert details like Node Name, Port, Occurrence and Probability are available.



When clicking on the arrow icon in the alert row, the table will expand and will show the history for the specific link.



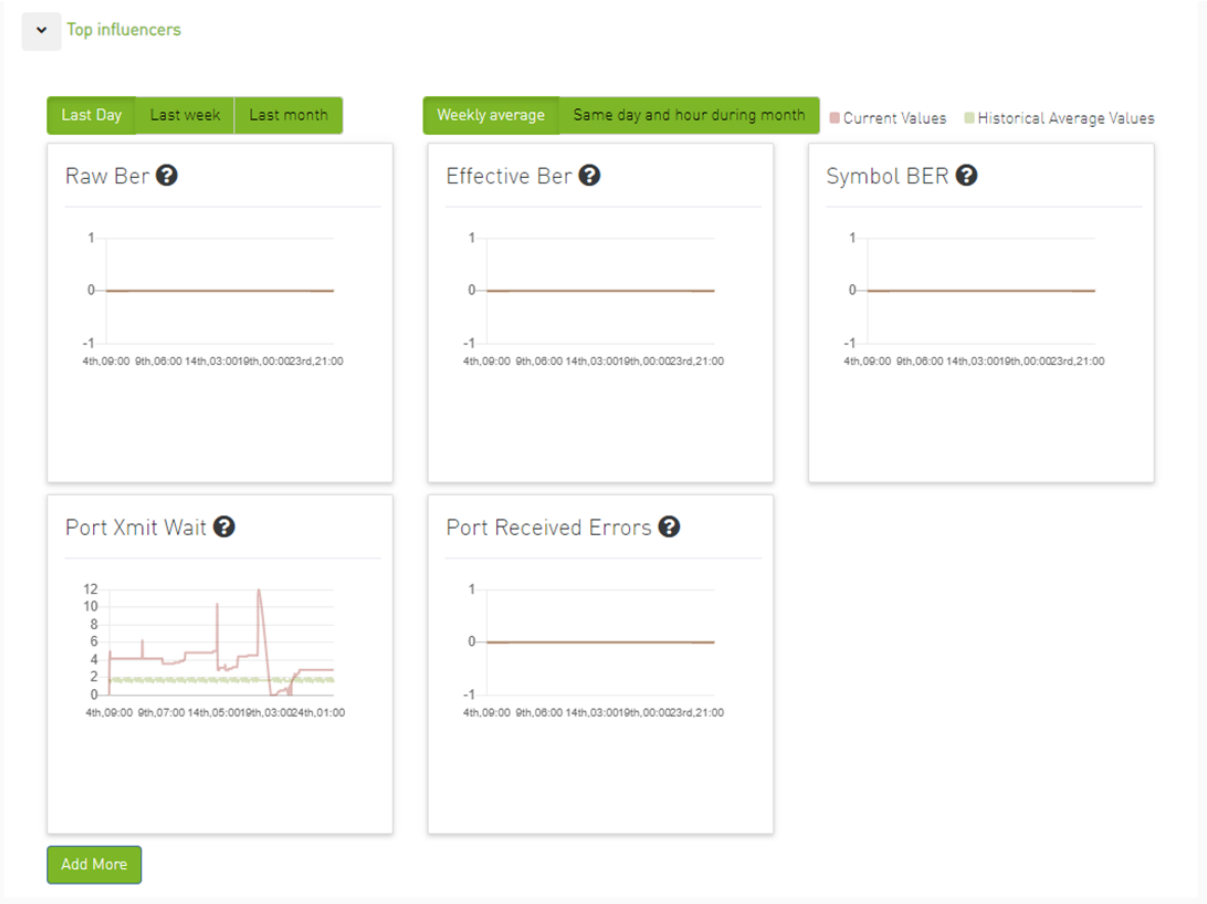
Clicking any alert in the list shows more information and recommended actions related to the alerted node, it will also show any alerts related to the cable that is connected to this node, if there is any, also five graphs representing counters that influenced the triggering of the alert will be shown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



The default view provides two lines for each graph: one for the current data, and another for the calculated historical data 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.

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

3.1.4 Link Anomaly

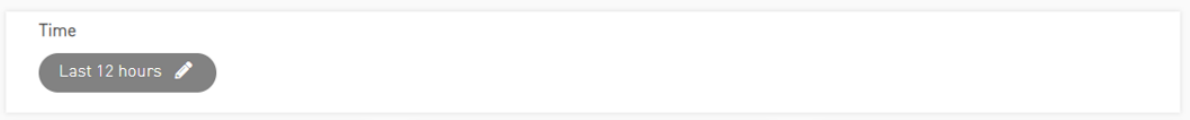
Port anomaly detection is based on defining composite metrics to reliably detect anomalies, where such metrics dynamically change, for example, according to a baseline that is determined and subsequently updated by a system.

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 the following views:

3.1.4.1 Time Filter

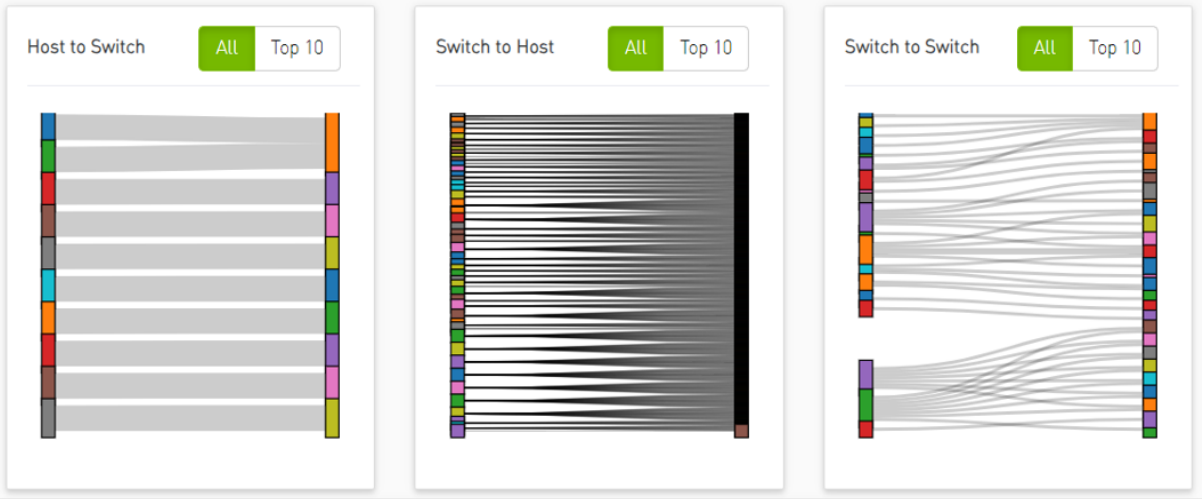
Users can filter link anomaly data by time via searching for either an absolute or relative time.



3.1.4.2 Event Flow Charts

Event flow charts display anomalies between devices, with each link in the chart describing the number of anomalies between two devices.

The width of the link reflects the number of anomalies that occurred between the two devices.



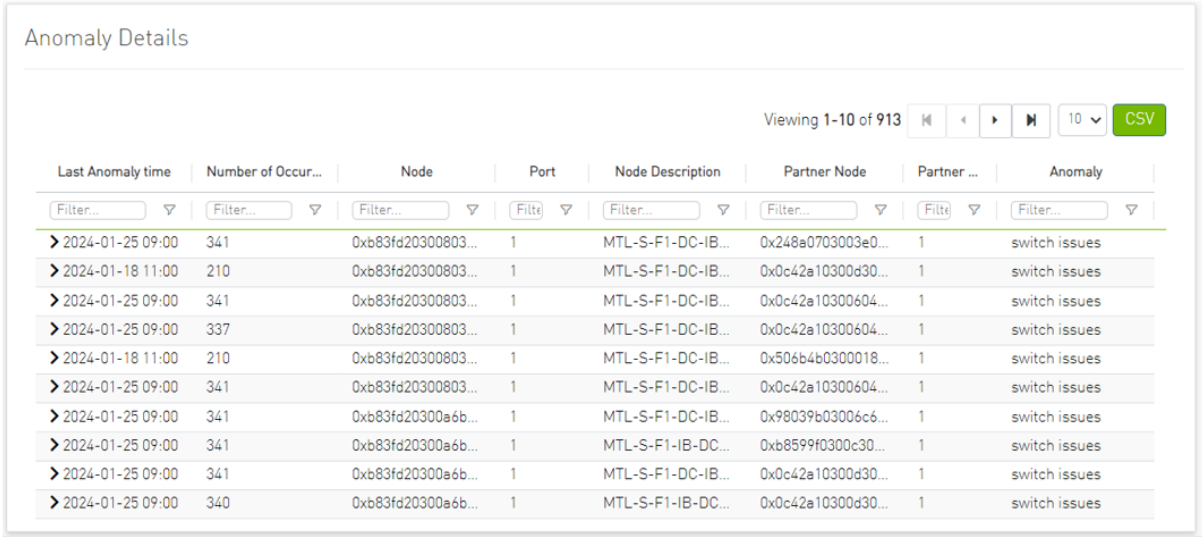
Clicking on the 'Top 10' button will reveal the top 10 devices with the highest occurrences of anomalies.

Clicking on link/device filters the table below.

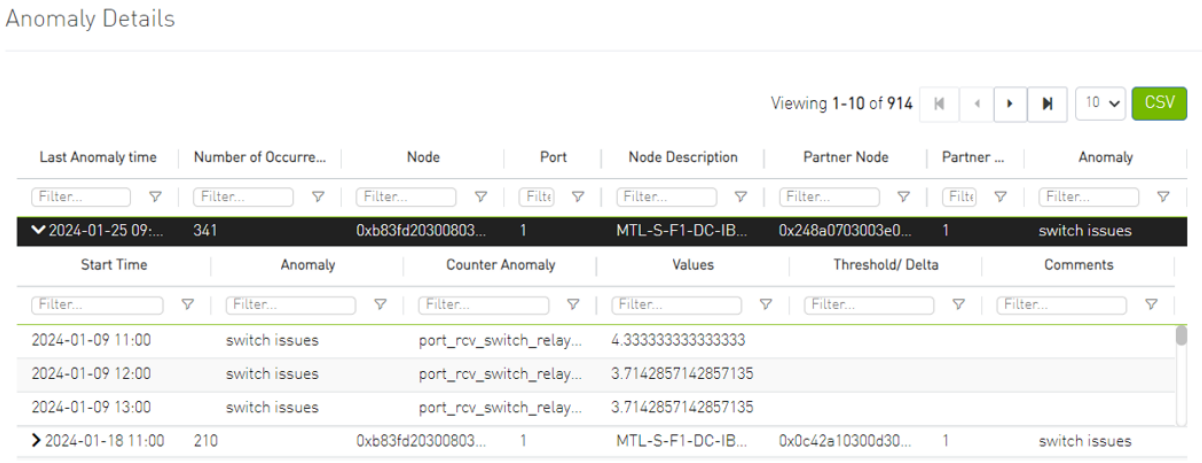
3.1.4.3 Anomaly Details

The table below represents the anomaly details such as Last Anomaly time, Number of Occurrences, Node and Partner Node.

Users can filter the anomaly details table by clicking on either a device or a link in the event flow charts.

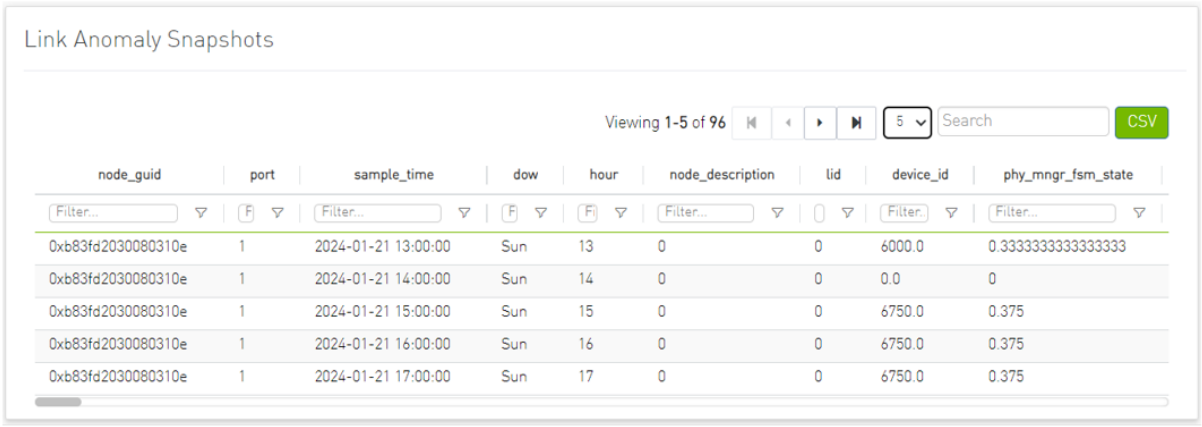


Clicking on the arrow icon in the anomaly node, the table will expand and will show all the history for the specific alert.



3.1.4.4 Link Anomaly Snapshots

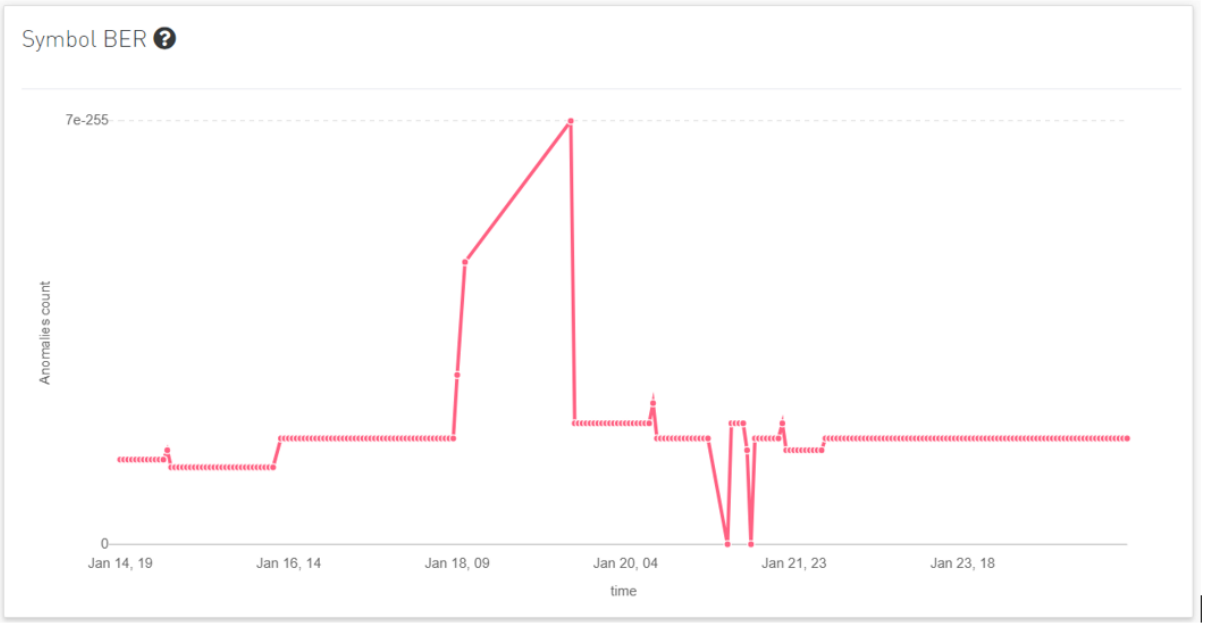
Clicking on the anomaly node will display all telemetry counters for the selected port, starting from the selected time range.



3.1.4.5 Total Anomalies Over Time

When clicking on a counter from the table an overtime graph will appear.

The chart will display the number of anomalies over time, with the time scale corresponding to the selected filter.



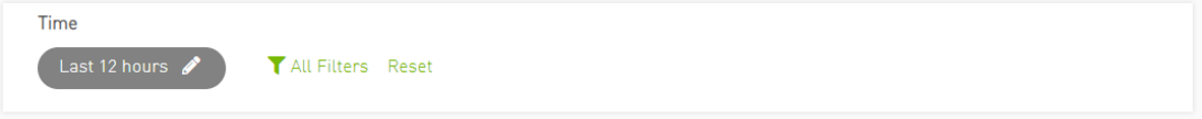
3.1.5 Link Status

Provides information about the links and the distribution of the attributes value according to the selected time range.

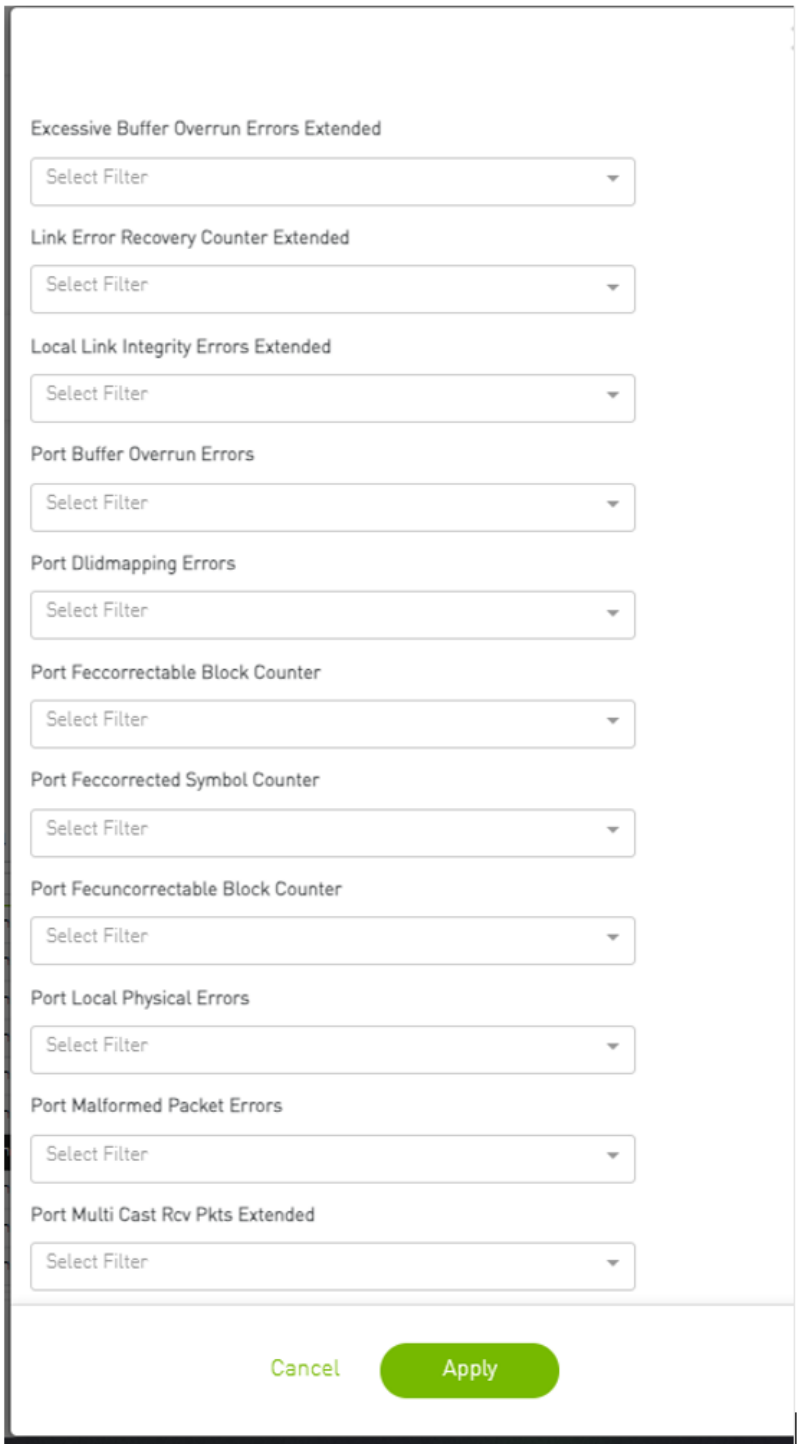
The dashboard provides the following views:

3.1.5.1 Filters

Users can filter link status data by time by searching for either an absolute or relative time, or by link attribute by clicking on the 'All Filters' button.



Clicking on the 'All Filters' button will open the following modal:



This modal filters the link status dashboard by the selected attribute values. Each attribute represents a dropdown containing the available values.

Additionally, clicking on the reset button will reset all filters.

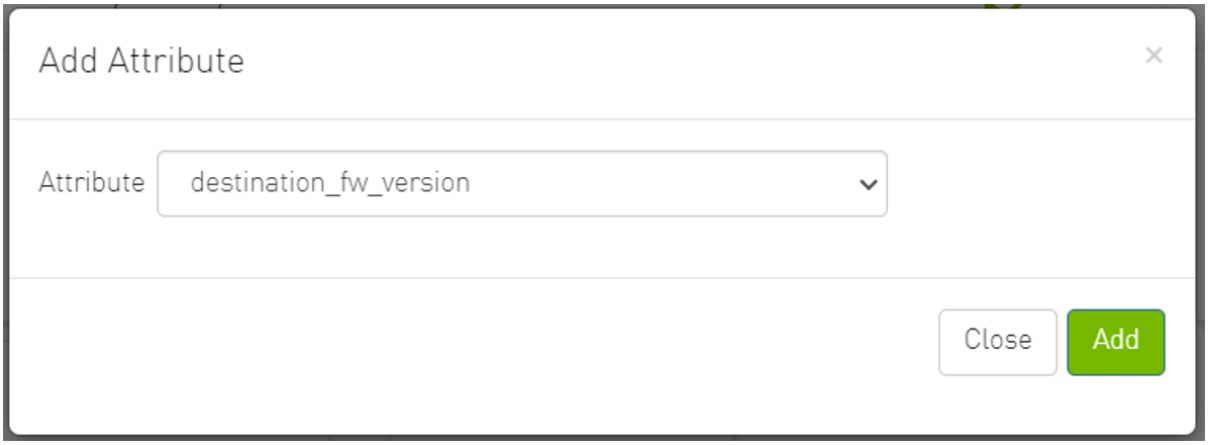
3.1.5.2 Attributes

The most important attributes will be displayed as histograms.

By clicking on a graph, the entire link status dashboard will be filtered based on the selection in the graph.

For example, clicking on "Active" in the "Logical state" graph will filter all the other graphs and tables by this selection.

Users can add more graphs for more attributes by clicking the "Add More" button below the graphs.



3.1.5.3 Counters

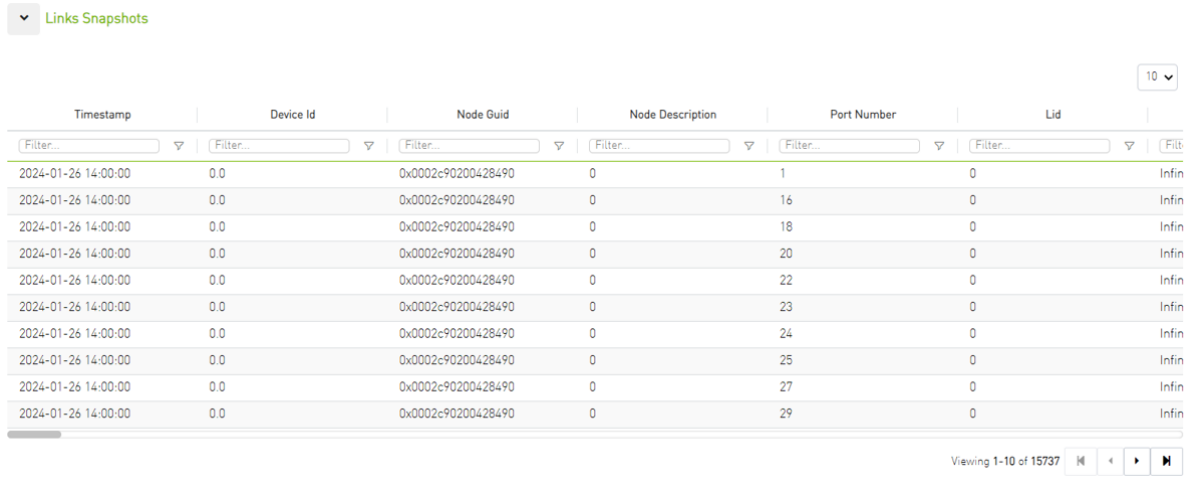
The most important counters will be displayed as histograms.

By clicking on a graph, the entire link status dashboard will be filtered based on the selection in the graph.

Users can add more graphs for more counters by clicking the "Add More" button below the graphs.

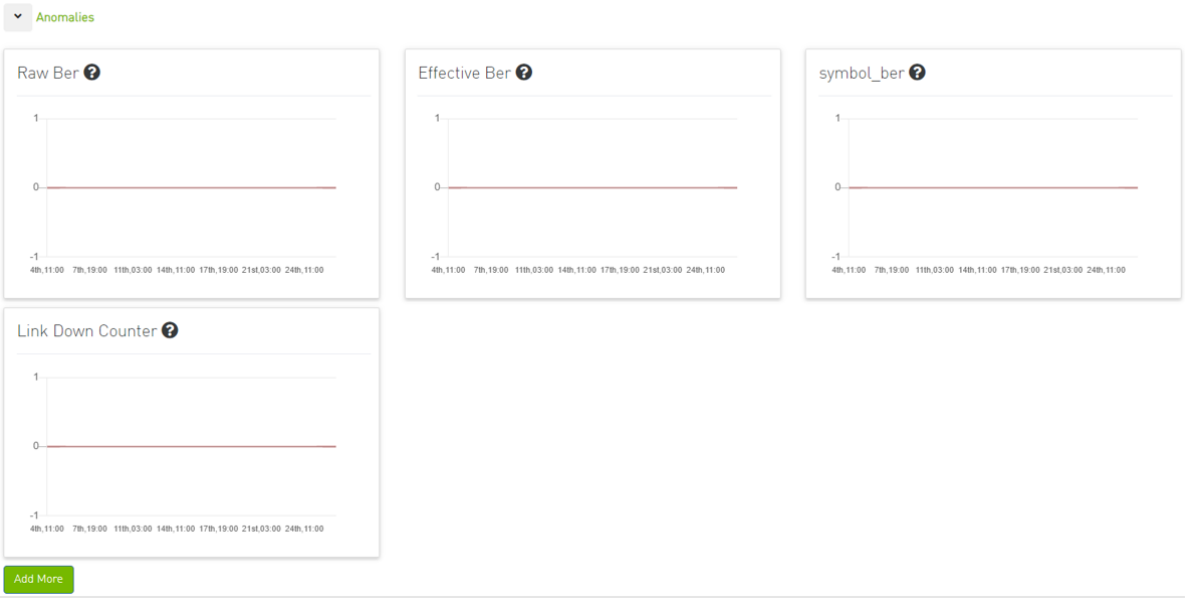
3.1.5.4 Links Snapshots

The table below represents the links snapshots details such as device ID, node GUID, port number and the related counters.

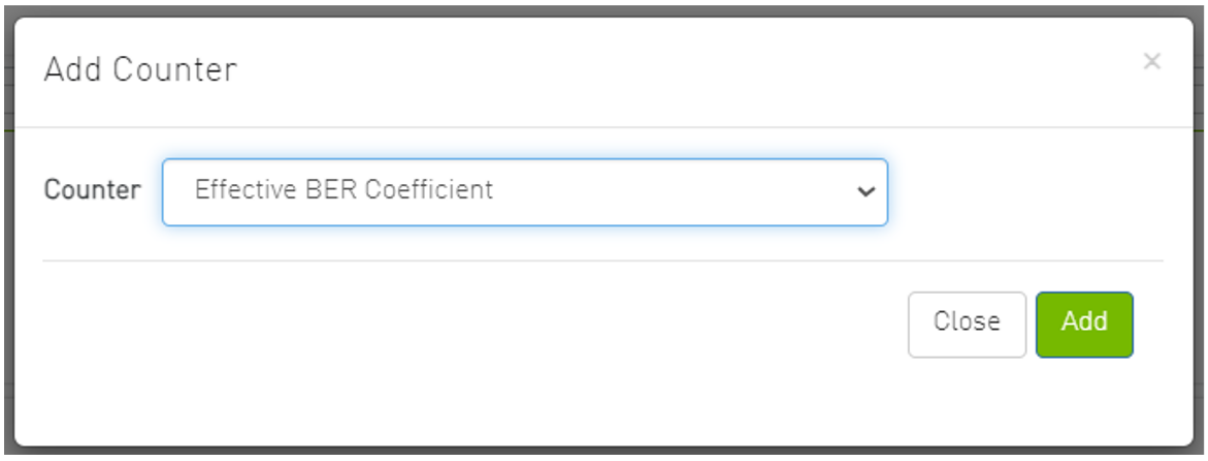


3.1.5.5 Anomalies

Clicking on a snapshot in the Links Snapshots table will display the most important counters as time graphs. These charts will show the counter values over time, with the time scale corresponding to the selected time filter.



Users can add more graphs for more counters by clicking the "Add More" button below the graphs.



3.1.6 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]
```

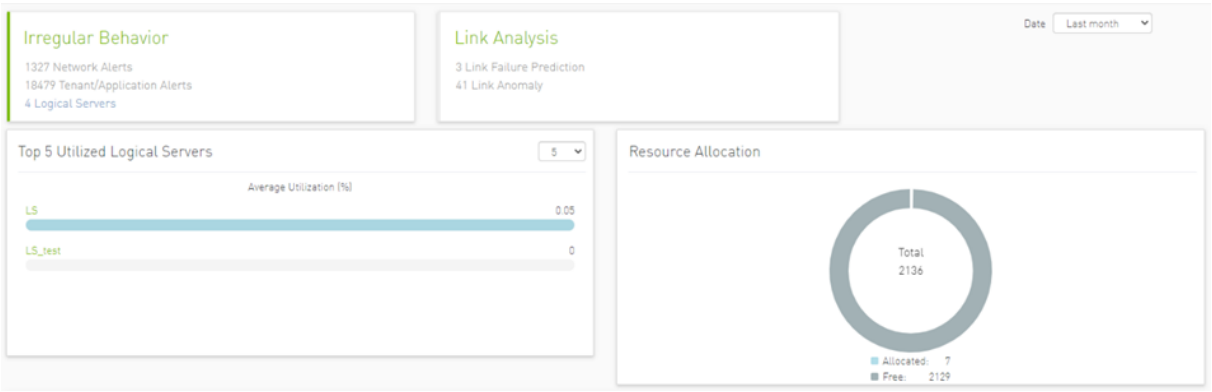
```
interval = 300
delay = 780
max_input = 12
standard_timeout = 180
enabled = true

[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.

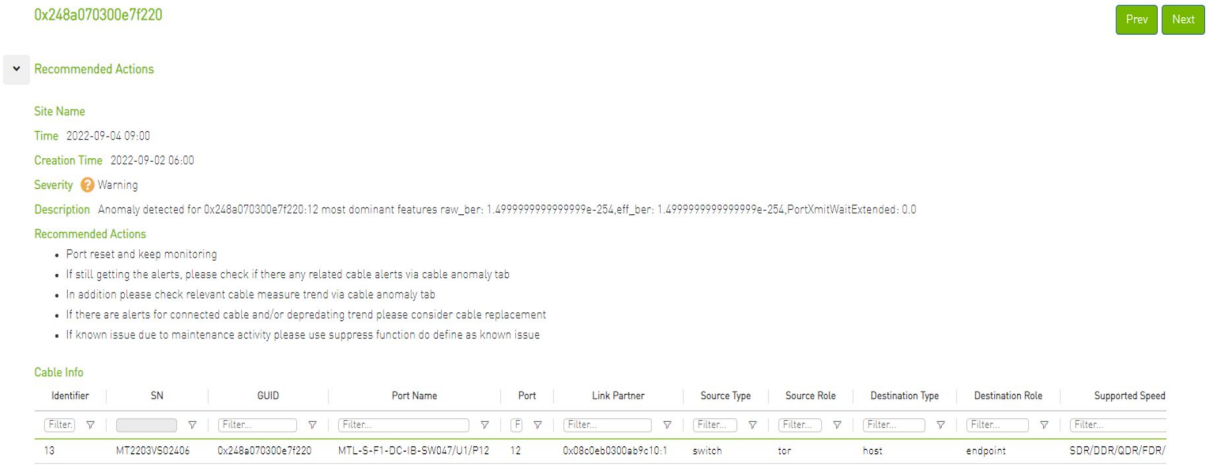


Clicking any logical server alert shows six graphs representing network statistics in general and per selected logical server.

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.

3.1.7 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.



3.2 Cable Anomalies Detection

3.2.1 Specification Description

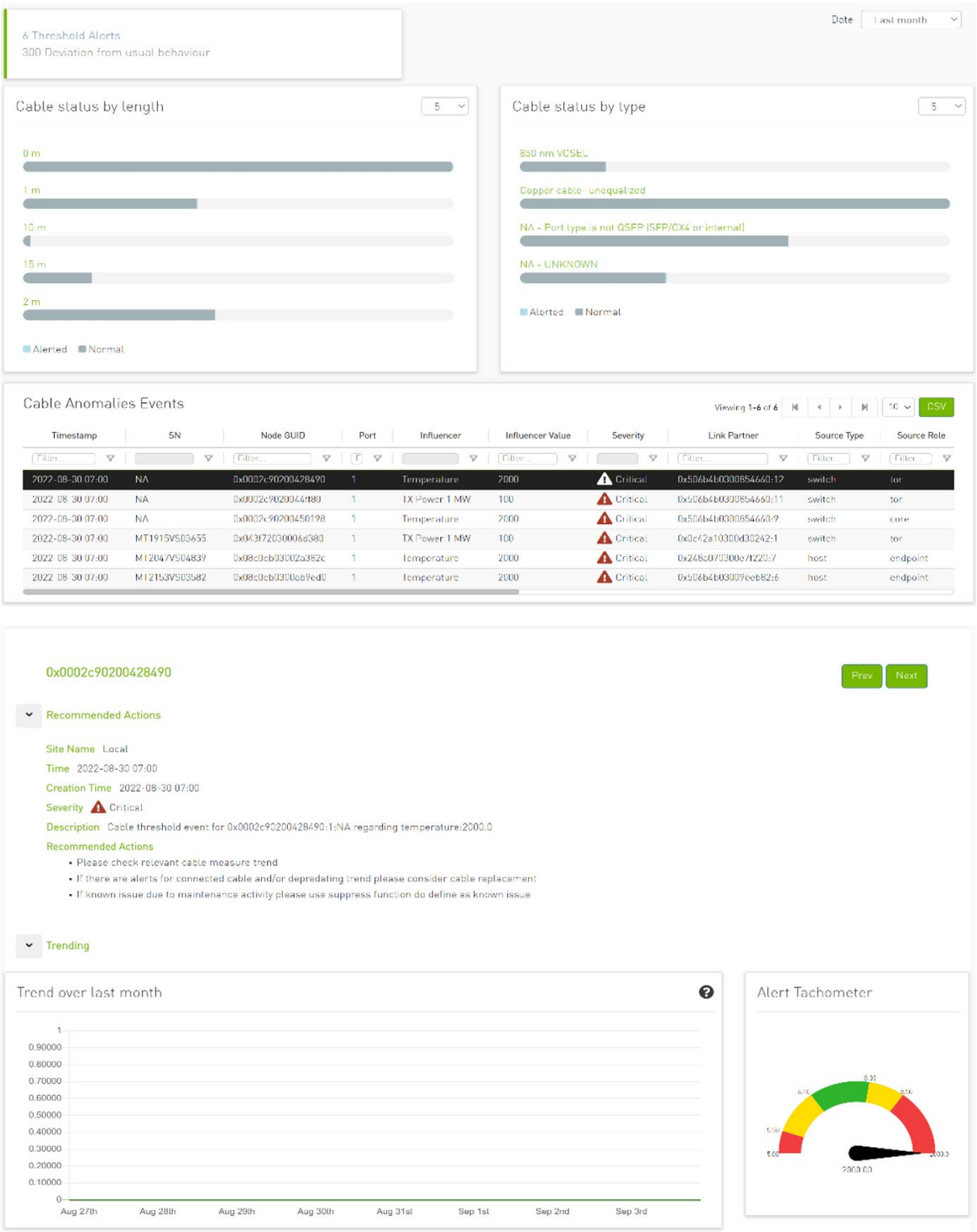
The present invention generally relates to the detection anomaly over cables and understanding degradation mechanisms for improving stability in data centers.

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

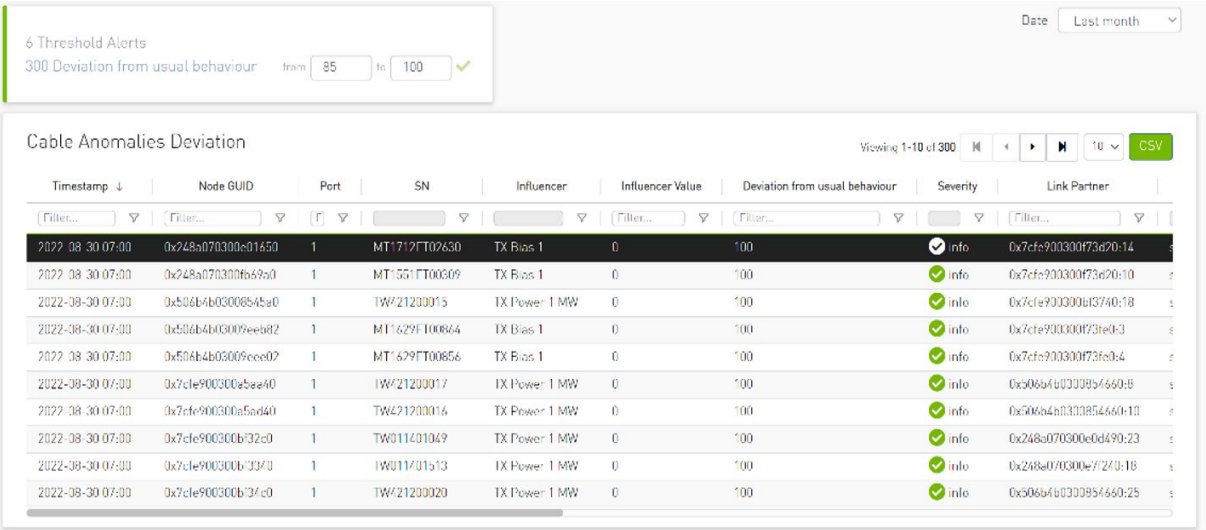
Moreover, with analysis of degradation over time we can determine better future performance strategies.

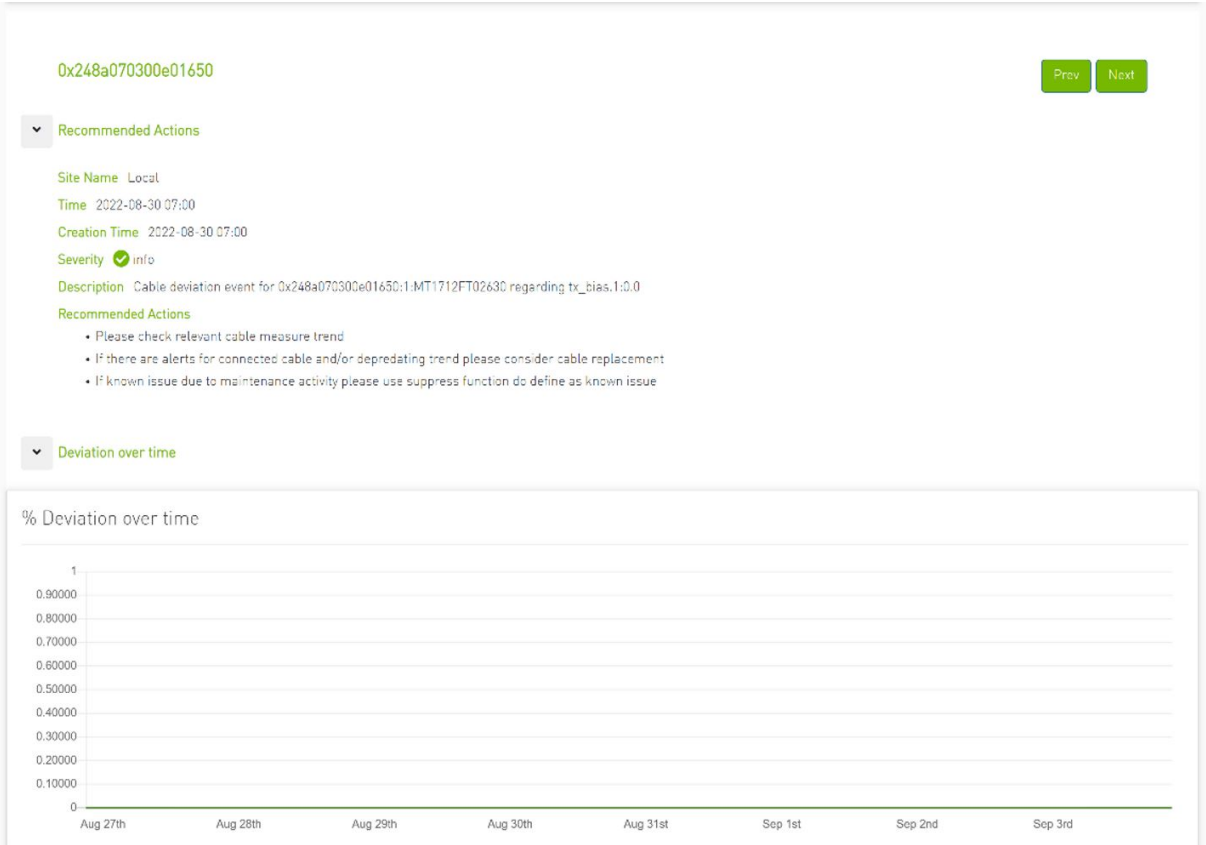
3.2.2 Customer Output

3.2.2.1 Threshold Alerts Tab



3.2.2.2 Deviation from Usual Behavior Tab





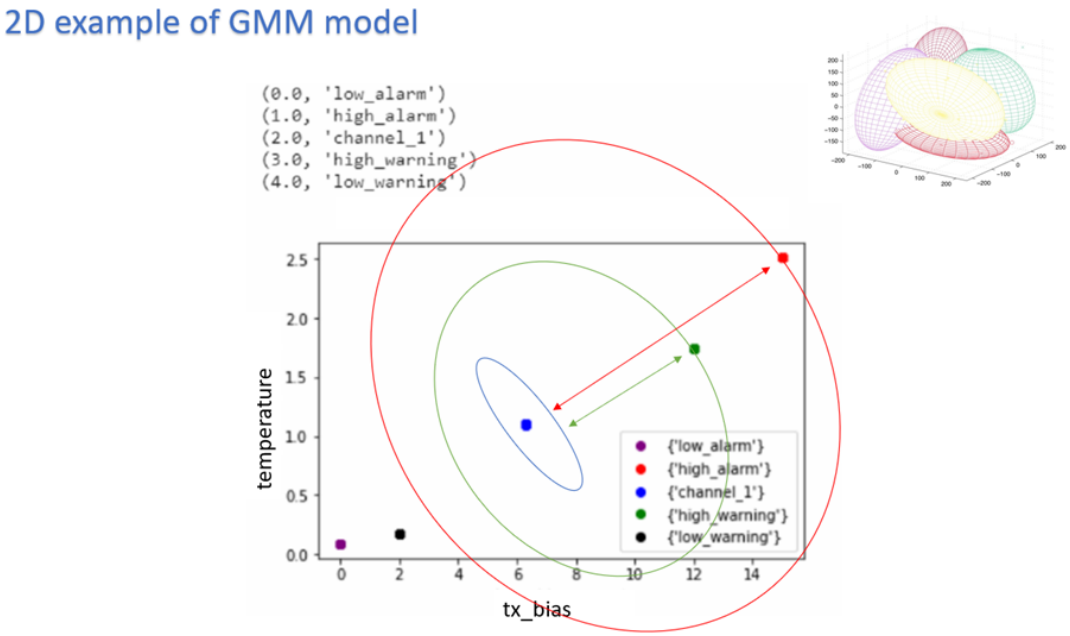
3.2.3 Background Art

3.2.3.1 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.



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

3.3 Job Analytics

3.3.1 Introduction

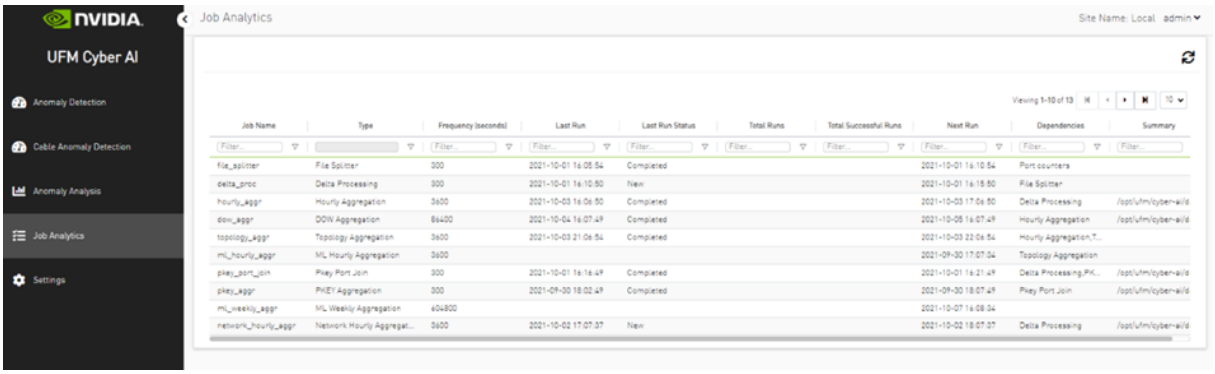
Analytic jobs are critical components in CyberAI. Each analytic job has a specific task to accomplish and runs periodically in a docker container. They process raw data collected from UFM Telemetry

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.

3.3.2 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.

3.3.3 Output Sample



4 REST API

4.1 Session Management

4.1.1 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)

4.1.2 Logout

- URL

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

- Request Data

```
None
```

- Response codes:

Status	Description
200	Success
401	Unauthorized

4.2 User Management

4.2.1 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

4.2.2 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

4.2.3 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

4.2.4 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

4.3 System Details

4.3.1 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

4.3.2 UFM Enterprise

- URL

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

- Request Data

```
none
```

- Response codes

Status	Description
200	Ok

4.3.3 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)

4.3.4 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

Status	Description
400	Bad Request (invalid argument)

4.4 Application Details

4.4.1 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

4.4.2 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

4.5 Configuration

4.5.1 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

4.5.2 Get UFM Enterprise Connections Parameters

- URL

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

- Request data

```
none
```

- Response

```
none
```

- Response codes

Status	Description
200	Success

4.5.3 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 – 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": {…},
    }
   }
```

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

- Response codes

Status	Description
204	Success
400	Bad request

4.5.4 Cable Distribution Count

4.5.4.1 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

4.5.4.2 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

4.6 Analytics

4.6.1 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": {{…}
```

```
    }
  }
```

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

- Response codes

Status	Description
200	Success
400	Bad Request (invalid argument)

4.6.2 Cables Distribution Counts

4.6.2.1 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)

4.6.2.2 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)

4.7 Suspicious Behavior

4.7.1 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)

4.7.2 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

4.7.3 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)

4.7.4 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

4.7.5 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)

4.7.6 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)

4.7.7 Cables Alerts

4.7.7.1 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)

4.7.7.2 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)

4.7.7.3 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

4.7.7.4 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

4.7.7.5 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)

4.7.7.6 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

4.8 Link Analysis

4.8.1 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

4.8.2 Get Link Failure Prediction History

- URL

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

- Request data

```
none
```

- Response

```
[
   {
      "alert_id":2,
      "created":1705251000,
      "node_guid":"0x0002c90200428490",
      "port":16,
      "node_name":"Infiniscale-IV Mellanox Technologies",
      "probability":0
   },
   {
      "alert_id":2,
      "created":1705251600,
      "node_guid":"0x0002c90200428490",
      "port":16,
      "node_name":"Infiniscale-IV MellanoxTechnologies",
      "probability":0
   }
]
```

- Response codes

Status	Description
200	Success
400	Bad Request
404	Not Found

4.8.3 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
  - 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

4.8.4 Get Link Anomaly Prediction History

- URL

```
cyber-ai/prediction/link-anomaly/<anomaly_id>
```

- Request Data

```
none
```

- URL filters:
  - Severities – retrieves only alerts with a severity included in the list.

```
Severities:<comma separated list  of severity>
```

- Response


```
[
   {
      "alert_id":165,
      "created":1704790800,
      "node_guid":"0x08c0eb03002a37fc",
      "port":1,
      "dst_guid":"0xb83fd2030080304e",
      "dst_port":11,
      "type":"link_issues",
      "counter":"port_rcv_errors",
      "counter_value":10922.5,
      "comments":""
   },
   {
      "alert_id":165,
      "created":1704794400,
      "node_guid":"0x08c0eb03002a37fc",
      "port":1,
      "dst_guid":"0xb83fd2030080304e",
      "dst_port":11,
      "type":"link_issues",
      "counter":"port_rcv_errors",
      "counter_value":9362.142857142857,
      "comments":""
   }
]
```


4.8.5 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

4.8.6 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

4.8.7 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

4.8.8 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

4.9 Resources

4.9.1 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)

4.9.2 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

4.9.3 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)

4.9.4 Get Tenants Allocation

- URL

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

- Request

```
none
```

- Response

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

- Response codes

Status	Description
200	Success

4.9.5 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

4.9.6 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

4.9.7 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

4.9.8 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>
```

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

4.9.9 Get Link Anomalies

- URL

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

- URL filters:
  - Influencers:

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

  - Request

```
none
```

  - Response

```
[
  {
     "name": "vl15_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

4.9.10 Get Link Anomalies For influencer

- URL

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

- Request

```
none
```

- Response

```
{
     "name": "vl15_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

4.10 Telemetry Data

4.10.1 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",
...
}
```

4.10.2 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
  }
 ]
```

4.10.3 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)

4.10.4 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)

4.10.5 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>
    ```

    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

Status	Description
400	Bad request

4.10.6 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
  }
 ]
```

4.10.7 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
  }
]
```

4.11 Alert Filters

4.11.1 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)

4.11.2 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

4.11.3 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

4.11.4 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

4.11.5 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

4.11.6 Link Status

- URL

```
cyber-ai/telemetry/link-status
```

- Filters

```
From
node_guid
port
port_guid
sample_time
dow
hour
node_description
lid
device_id
phy_mngr_fsm_state
phy_state
logical_state
link_speed_active
link_width_active
fec_mode_active
raw_ber
eff_ber
symbol_ber
phy_raw_errors_lane0
phy_raw_errors_lane1
phy_raw_errors_lane2
phy_raw_errors_lane3
phy_effective_errors
phy_symbol_errors
time_since_last_clear
hist0
hist1
hist2
hist3
hist4
hist5
hist6
hist7
hist8
hist9
hist10
hist11
hist12
hist13
hist14
hist15
fw_version
switch_temperature
switch_voltage
link_down_events
LinkErrorRecoveryCounterExtended
link_partner
destination_port_node_description
destination_guid
destination_port
source_server_operation_mode
source_system_name
source_ip
source_fw_version
source_hw_version
source_nic_type
source_port_dname
source_port_node_description
source_host
source_technology
destination_type
destination_role
destination_model
destination_server_operation_mode
destination_system_name
```

```
destination_ip TEXT,
destination_fw_version
destination_hw_version
destination_nic_type
destination_port_dname
destination_host
destination_technology
```

- Response


```
[
   {
      "node_guid":"0x0002c90200428490",
      "port":1,
      "port_guid":"0x0002c90200428490",
      "sample_time":1706151600,
      "dow":"Thu",
      "hour":5,
      "node_description":"0",
      "lid":0,
      "device_id":"0.0",
      "phy_mngr_fsm_state":0,
      "phy_state":"Phy_up",
      "logical_state":"Active",
      "link_speed_active":0.125,
      "link_width_active":0.5,
      "fec_mode_active":31.875,
      "raw_ber":0,
      "eff_ber":0,
      "symbol_ber":0,
      "phy_raw_errors_lane0":0,
      "phy_raw_errors_lane1":0,
      "phy_raw_errors_lane2":0,
      "phy_raw_errors_lane3":0,
      "phy_effective_errors":0,
      "phy_symbol_errors":0,
      "time_since_last_clear":0,
      "hist0":0,
      "hist1":0,
      "hist2":0,
      "hist3":0,
      "hist4":0,
      "hist5":0,
      "hist6":0,
      "hist7":0,
      "hist8":0,
      "hist9":0,
      "hist10":0,
      "hist11":0,
      "hist12":0,
      "hist13":0,
      "hist14":0,
      "hist15":0,
      "fw_version":"NA",
      "switch_temperature":0,
      "switch_voltage":0,
      "link_down_events":0,
      "LinkErrorRecoveryCounterExtended":0,
      "link_partner":"NA",
      "destination_port_node_description":"MTL-S-F1-DC-IB-SW10:12",
      "destination_guid":"0xb83fd203008031ce",
      "destination_port":12,
      "pn":"NA",
      "sn":"NA",
      "transmitter_technology":"NA",
      "cable_type":"NA",
      "cable_vendor":"NA",
      "length":"NA",
      "cable_identifier":"NA",
      "rev":"NA",
      "diag_supply_voltage":"NA",
      "temperature":"NA",
      "status_opcode":0,
      "down_blame":"Unknown",
      "local_reason_opcode":"No_link_down_indication",
      "remote_reason_opcode":"No_link_down_indication",
      "e2e_reason_opcode":0,
      "PortRcvRemotePhysicalErrorsExtended":0,
      "PortRcvErrorsExtended":0,
      "PortXmitDiscardsExtended":0,
      "PortRcvSwitchRelayErrorsExtended":0,
      "ExcessiveBufferOverrunErrorsExtended":0,
      "LocalLinkIntegrityErrorsExtended":0,
      "PortRcvConstraintErrorsExtended":0,
      "PortXmitConstraintErrorsExtended":0,
      "PortBufferOverrunErrors":0,
      "PortDLIDMappingErrors":0,
      "VL15DroppedExtended":0,
      "PortXmitWaitExtended":0,
      "PortXmitDataExtended":13623112821.5,
      "PortRcvDataExtended":77872769279.5,
      "PortXmitPktsExtended":27879243.625,
      "PortRcvPktsExtended":97167768,
      "PortUniCastXmitPktsExtended":27847241.25,
      "PortUniCastRcvPktsExtended":95548800.375,
      "PortMultiCastXmitPktsExtended":32002.375,
      "PortMultiCastRcvPktsExtended":1618967.625,
      "SyncHeaderErrorCounter":0,
      "PortSwLifetimeLimitDiscards":0,
      "PortSwHOQLifetimeLimitDiscards":0,
```

```
    "PortFECCorrectableBlockCounter":0,
    "PortFECCorrectedSymbolCounter":0,
    "PortFECUncorrectableBlockCounter":0,
    "PortLocalPhysicalErrors":0,
    "PortMalformedPacketErrors":0,
    "rx_power_1_mw":"NA",
    "rx_power_2_mw":"NA",
    "rx_power_3_mw":"NA",
    "rx_power_4_mw":"NA",
    "tx_power_1_mw":"NA",
    "tx_power_2_mw":"NA",
    "tx_power_3_mw":"NA",
    "tx_power_4_mw":"NA",
    "source_type":"switch",
    "source_role":"tor",
    "source_model":"SDR",
    "source_server_operation_mode":"Switch",
    "source_system_name":"Infiniscale-IV Mellanox Technologies",
    "source_ip":"0.0.0.0",
    "source_fw_version":"0.0.0",
    "source_hw_version":"NA",
    "source_nic_type":"NA",
    "source_port_dname":"1",
    "source_port_node_description":"Infiniscale-IV Mellanox Technologies:1",
    "source_host":"0002c90200428490",
    "source_technology":"QDR",
    "destination_type":"switch",
    "destination_role":"tor",
    "destination_model":"MQM8700",
    "destination_server_operation_mode":"Switch",
    "destination_system_name":"MTL-S-F1-DC-IB-SW10",
    "destination_ip":"10.60.130.10",
    "destination_fw_version":"27.2010.4120",
    "destination_hw_version":"NA",
    "destination_nic_type":"NA",
    "destination_port_dname":"12",
    "destination_host":null,
    "destination_technology":"HDR"
},
{
    "node_guid":"0x0002c9020044ff80",
    "port":1,
    "port_guid":"0x0002c9020044ff80",
    "sample_time":1706151600,
    "dow":"Thu",
    "hour":5,
    "node_description":"0",
    "lid":0,
    "device_id":"0.0",
    "phy_mngr_fsm_state":0,
    "phy_state":"Phy_up",
    "logical_state":"Active",
    "link_speed_active":0.125,
    "link_width_active":0.5,
    "fec_mode_active":31.875,
    "raw_ber":0,
    "eff_ber":0,
    "symbol_ber":0,
    "phy_raw_errors_lane0":0,
    "phy_raw_errors_lane1":0,
    "phy_raw_errors_lane2":0,
    "phy_raw_errors_lane3":0,
    "phy_effective_errors":0,
    "phy_symbol_errors":0,
    "time_since_last_clear":0,
    "hist0":0,
    "hist1":0,
    "hist2":0,
    "hist3":0,
    "hist4":0,
    "hist5":0,
    "hist6":0,
    "hist7":0,
    "hist8":0,
    "hist9":0,
    "hist10":0,
    "hist11":0,
    "hist12":0,
    "hist13":0,
    "hist14":0,
    "hist15":0,
    "fw_version":"NA",
    "switch_temperature":0,
    "switch_voltage":0,
    "link_down_events":0,
    "LinkErrorRecoveryCounterExtended":0,
    "link_partner":"NA",
    "destination_port_node_description":"MTL-S-F1-DC-IB-SW10:11",
    "destination_guid":"0xb83fd203008031ce",
    "destination_port":11,
    "pn":"NA",
    "sn":"NA",
    "transmitter_technology":"NA",
    "cable_type":"NA",
    "cable_vendor":"NA",
    "length":"NA",
    "cable_identifier":"NA",
    "rev":"NA",
    "diag_supply_voltage":"NA",
    "temperature":"NA",
    "status_opcode":0,
    "down_blame":"Unknown",
    "local_reason_opcode":"No_link_down_indication",
```

```
      "remote_reason_opcode":"No_link_down_indication",
      "e2e_reason_opcode":0,
      "PortRcvRemotePhysicalErrorsExtended":0,
      "PortRcvErrorsExtended":0,
      "PortXmitDiscardsExtended":0,
      "PortRcvSwitchRelayErrorsExtended":0,
      "ExcessiveBufferOverrunErrorsExtended":0,
      "LocalLinkIntegrityErrorsExtended":0,
      "PortRcvConstraintErrorsExtended":0,
      "PortXmitConstraintErrorsExtended":0,
      "PortBufferOverrunErrors":0,
      "PortDLIDMappingErrors":0,
      "VL15DroppedExtended":0,
      "PortXmitWaitExtended":0,
      "PortXmitDataExtended":273269961.5,
      "PortRcvDataExtended":434894002,
      "PortXmitPktsExtended":1866950.125,
      "PortRcvPktsExtended":2284998.5,
      "PortUniCastXmitPktsExtended":1861369.125,
      "PortUniCastRcvPktsExtended":639736.5,
      "PortMultiCastXmitPktsExtended":5581,
      "PortMultiCastRcvPktsExtended":1645262,
      "SyncHeaderErrorCounter":0,
      "PortSwLifetimeLimitDiscards":0,
      "PortSwHOQLifetimeLimitDiscards":0,
      "PortFECCorrectableBlockCounter":0,
      "PortFECCorrectedSymbolCounter":0,
      "PortFECUncorrectableBlockCounter":0,
      "PortLocalPhysicalErrors":0,
      "PortMalformedPacketErrors":0,
      "rx_power_1_mw":"NA",
      "rx_power_2_mw":"NA",
      "rx_power_3_mw":"NA",
      "rx_power_4_mw":"NA",
      "tx_power_1_mw":"NA",
      "tx_power_2_mw":"NA",
      "tx_power_3_mw":"NA",
      "tx_power_4_mw":"NA",
      "source_type":"switch",
      "source_role":"tor",
      "source_model":"SDR",
      "source_server_operation_mode":"Switch",
      "source_system_name":"Infiniscale-IV Mellanox Technologies",
      "source_ip":"0.0.0.0",
      "source_fw_version":"0.0.0",
      "source_hw_version":"NA",
      "source_nic_type":"NA",
      "source_port_dname":"1",
      "source_port_node_description":"Infiniscale-IV Mellanox Technologies:1",
      "source_host":"0002c9020044ff80",
      "source_technology":"QDR",
      "destination_type":"switch",
      "destination_role":"tor",
      "destination_model":"MQM8700",
      "destination_server_operation_mode":"Switch",
      "destination_system_name":"MTL-S-F1-DC-IB-SW10",
      "destination_ip":"10.60.130.10",
      "destination_fw_version":"27.2010.4120",
      "destination_hw_version":"NA",
      "destination_nic_type":"NA",
      "destination_port_dname":"11",
      "destination_host":null,
      "destination_technology":"HDR"
   }
]
```


4.11.7 Get Histogram for Link Status

- URL:

```
/cyber-ai/telemetry/link-status/ influencer/histogram influencer
```

- Filters:

```
From
To
counter=counters comma separated
```

- Response:


```
{
   "raw_ber":{
      "0":{
         "total":7994
      },
      "1.4999999999999999e-254":{
         "total":6300
      },
```

```
      "2e-18":{
         "total":7
      },
      "3e-17":{
         "total":18
      },
      "4e-17":{
         "total":3
      },
      "1e-16":{
         "total":11
      },
      "2e-16":{
         "total":3
      },
      "4e-16":{
         "total":7
      },
      "2e-15":{
         "total":7
      },
      "3e-15":{
         "total":7
      },
      "5e-15":{
         "total":7
      },
      "1e-14":{
         "total":7
      },
      "8e-13":{
         "total":7
      },
      "5e-12":{
         "total":7
      },
      "7e-12":{
         "total":7
      },
      "3e-11":{
         "total":7
      },
      "2e-07":{
         "total":6
      },
      "3e-07":{
         "total":1
      }
   },
   "eff_ber":{
      "0":{
         "total":7994
      },
      "1.4999999999999999e-254":{
         "total":6374
      },
      "3e-17":{
         "total":10
      },
      "4e-16":{
         "total":7
      },
      "3e-15":{
         "total":7
      },
      "5e-15":{
         "total":7
      },
      "2e-07":{
         "total":6
      },
      "3e-07":{
         "total":1
      }
   },
   "symbol_ber":{
      "0":{
         "total":7994
      },
      "1.8749999999999998e-255":{
         "total":6374
      },
      "1.25e-17":{
         "total":10
      },
      "5e-17":{
         "total":7
      },
      "3.75e-16":{
         "total":7
      },
      "6.25e-16":{
         "total":7
      },
      "2.5e-08":{
         "total":5
      },
      "3.75e-08":{
         "total":1
      },
      "6.25e-08":{
         "total":1
      }
```

```
    }
}
```

4.11.8 Get Properties for Link Status

- URL:

```
/cyber-ai/telemetry/link-status/ properties
```

- Filters:

```
From
To
```

- Response:


```
{"phy_state": [
    "Phy_up"
  ],
  "logical_state": [
    "Active"
  ],
  "link_speed_active": [
    0.0909090909090909,
    2.909090909090909,
    1.4545454545454546,
    0.3636363636363636
  ],
  "link_width_active": [
    0.3636363636363636
  ],
  "fec_mode_active": [
    23.181818181818183,
    0.2727272727272727,
    0,
    0.0909090909090909
  ],
  "raw_ber": [
    0,
    1.4999999999999999e-254,
    7e-13,
    4e-12,
    1e-15,
    4e-15,
    6e-12,
    2e-18,
    1e-14,
    1e-12,
    2e-15,
    1e-16,
    5e-12,
    2e-17,
    4e-17,
    5e-17
  ],
  "eff_ber": [
    0,
    1.4999999999999999e-254,
    4e-12,
    1e-15,
    4e-15,
    1e-17,
    3e-17
  ],
  "symbol_ber": [
    0,
    1.3636363636363634e-255,
    3.636363636363636e-13,
    9.090909090909091e-17,
    3.6363636363636364e-16,
    1.8181818181818186e-18,
    9.090909090909089e-18
  ]
}
```

5 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.

5.1 ufm-cai-sanity

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

5.1.1 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

5.1.2 Usage

```
ufm-cai-sanity
```

5.2 ufm-cai-jobs

This script manages Cyber AI analytics jobs. Commands:

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

5.2.1 Usage

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

5.3 ufm-cai-ufm-params

This script configures and shows the UFM connection info.

5.3.1 Usage

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

5.3.1.1 Update

Updates UFM configuration.

Option	Description
`-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

5.3.1.2 Show

Shows current UFM configuration (except password).

5.4 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.

5.4.1 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
```

5.4.2 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>
```

5.4.3 Cron Job

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

5.5 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.

5.5.1 Usage

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

5.5.1.1 Options

Option	Description
`-v|--verbose`	explain what is being done

Option	Description
`-n|--network`	collect network counters files
`-c|--cables`	collect cable counters files
`-z|--archived`	collect archived counter files when associated with [-n] or [-c]
`-g|--aggregated`	collect aggregated files
`-d|--database`	collect database file(s)
`-t|--topology`	collect topology files
`-m|--model`	collect model files
`-l|--log`	collect log files
`-f|--conf`	collect configuration files
`-a|--all`	collect all above

5.5.1.2 Output

Output file is in tgz format:

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

5.6 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.

5.6.1 Usage

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

5.6.1.1 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

6 High Availability

6.1 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.

6.1.1 Supported Platforms

1. Ubuntu
2. Centos Master

6.1.2 Prerequisites

6.1.2.1 Pacemaker packages

1. pacemaker
2. pcs
3. corosync

6.1.2.2 DRBD Package

- DRBD utils 8.4 or up.

6.2 Configuration

6.2.1 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
```

6.2.2 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>
```

6.2.3 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)
                                        mandatory.
    -n | --peer-node <node-hostname>    Peer node name.
                                        mandatory.
    -s | --peer-sync-ip <ip address>    Peer node sync ip adreess
                                        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
```

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
```

6.2.4 Stopping UFM Services

You may stop UFM services using the following stop command.

```
ufm_ha_cluster stop
```

6.2.5 Takeover Services

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

```
ufm_ha_cluster takeover
```

6.2.6 Master Failover

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

```
ufm_ha_cluster failover
```

6.2.7 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>
```

7 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.

7.1 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 -1 ./# ls -1 ./
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.
```

> 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.

7.1.1 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:

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

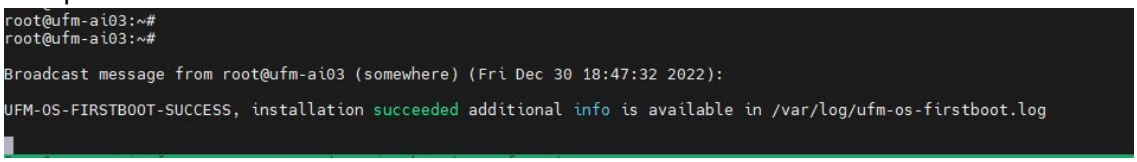
To bypass user prompts, use the `-y` flag when executing the command, but note that this flag alone will not trigger an automatic server reboot. If a reboot is desired, use the `-r` flag in combination with `-y`. Additionally, the `--appliance-sw-upgrade` flag can be used to upgrade both the UFM Enterprise 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
```

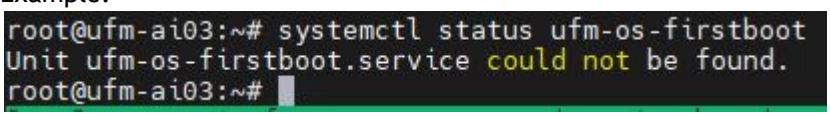
3. After the reboot procedure is complete, a systemd service (`ufm-os-firstboot.service`) runs the remainder of the upgrade procedure. Once completed, a message is prompted to all open terminals including the status:
"UFM-OS-FIRSTBOOT-FAILURE" - if installation is failed.
"UFM-OS-FIRSTBOOT-SUCCESS" - if installation succeeded.
Example:



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:



7.1.2 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.

   > 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.

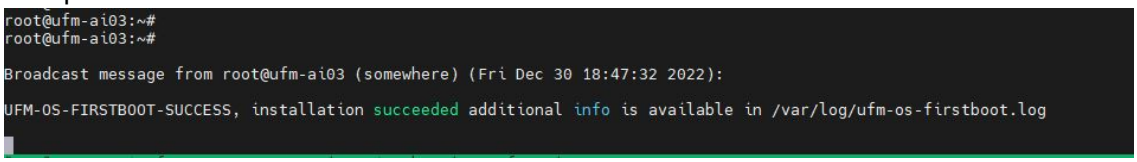
   The `-y` flag can be supplied to skip user questions (the flag does not automatically reboot the server on its own. For auto reboot, combine with the `-r` flag).
   In the following example the server auto reboots once the upgrade procedure is completed:

   ```
   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:

   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.

8 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.

8.1 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.

8.2 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.

8.3 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
    a. Load Morpheus docker image morpheus-22.06.tar.gz
    b. Set [Morpheus] enabled = true inside cfg
    c. Enable Telemetry GPU counters collection by setting [data_prep_telemetry::gpu_counter] skip_collection = false
    d. 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_resnet.pkl
```

8.4 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.

9 List of Supported Events

UFM Cyber AI tab	Elements	Counters
Link anomaly/Link Failure Prediction	Node+Port	symbol_error_counter

UFM Cyber AI tab	Elements	Counters
		local_link_integrity_errors LocalLinkIntegrityErrorsExtended
		SymbolErrorCounterExtended
		UnknownBlockCounter
		SyncHeaderErrorCounter
		phy_symbol_errors
		ErrorDetectionCounterLane.[1-12]
		FECCorrectableBlockCountrLane.[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
		excessive_buffer_errors ExcessiveBufferOverrunErrorsExtended
		PortMalformedPacketErrors
		PortDLIDMappingErrors
		PortBufferOverrunErrors
		PortVLMappingErrors
		PortNeighborMTUDiscards
		PortInactiveDiscards
		PortSwHOQLifetimeLimitDiscards
		PortSwLifetimeLimitDiscards
		port_xmit_wait
		PortXmitWaitExtended

UFM Cyber AI tab	Elements	Counters
		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
		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

UFM Cyber AI tab	Elements	Counters
		Lane1Grade
		Lane2Grade
		Lane3Grade
		MaxRetransmissionRate
		PortLocalPhysicalErrors
		PortLoopingErrors
		PortMultiCastRcvPktsExtended
		PortMultiCastXmitPktsExtended
Network Alerts	NW	raw_ber
		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

UFM Cyber AI tab	Elements	Counters
Tenant/Application Alerts	Pkey	raw_ber
		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
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
		tx_bias_low_th
		tx_bias_high_th

10 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 running ibdiagnet process
	data_dir	String	/data	data_dirString/dataDirectory in which UFM Cyber-AI data is placed
	ibdiag_output_dir	String	/tmp/ibd	Directory in which ibdiagnet places files
	sample_rate	Integer	-	Frequency of collecting port counter data
	hca	String	mlx5_2	Card to use
	app_name	String	/opt/collectx/bin/ibdiagnet	Full path of the ibdiagnet application
	topology_mode	String	discover	Topology policy
	topology_discovery_factor	Integer	0	Every "n" iterations, run discovery, otherwise, use result from last run if 0 or 1
retention	retention_enabled	Boolean	true	Enable/disable retention service
	retention_interval	Time	1d	Interval to wait before running the retention process
	retention_age	Time	100d	Period to reserve the collected data
compression	compression_enabled	Boolean	true	Enable/disable compression service
	compression_interval	Time	6h	Interval to wait before running the compression service
	compression_age	Time	12h	Period to reserve the compressed data
cable_info	cable_info_schedule	csv	-	Weekday/hr:min,hr:hm Time to collect cable info data

11 Appendixes

11.1 Appendix - Supported Counters

11.1.1 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

11.1.2 Supported Per-lane Counters

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

11.2 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
	inputeq
	outputamp
	outputemp
	fw_version
	attentuation_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

Type	Field
	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
	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

11.3 Appendix - Cyber-AI Appliance OS Remanufacture

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.

11.3.1 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.

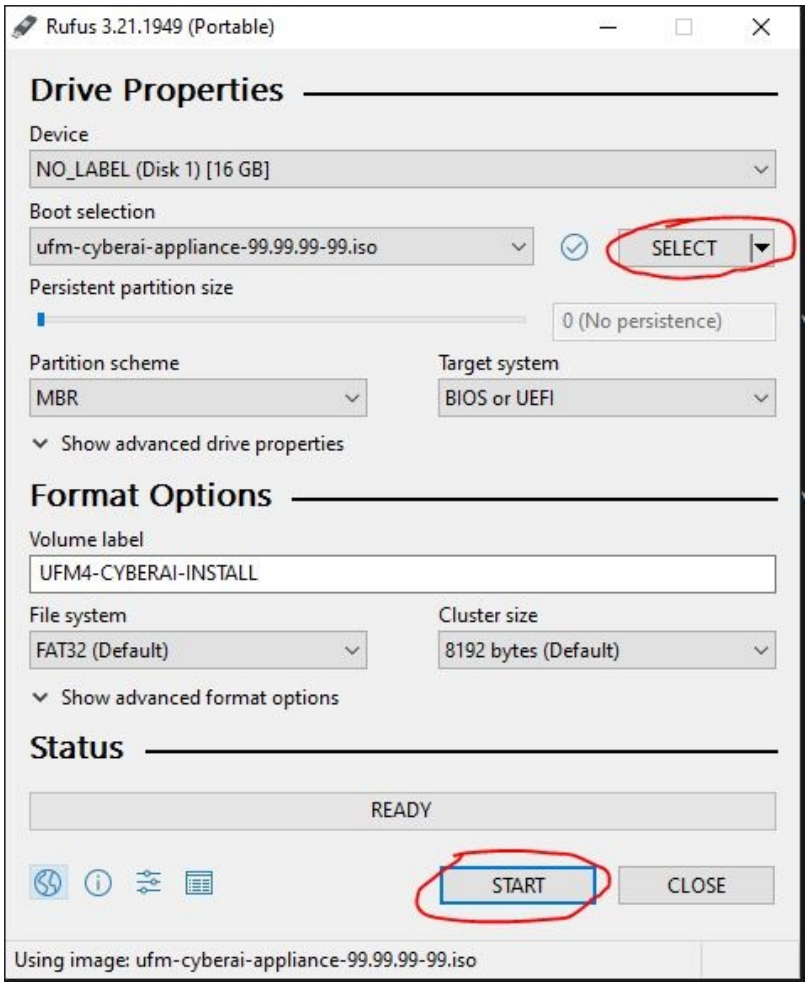
```
ls -ltrh /tmp/ufm-cyberai-appliance-<version>-omu/
-rw-r--r-- 1 root root 7.5G Dec 31 17:49 ufm-cyberai-appliance-<version>.iso
-rwxr-xr-x 1 root root  11K Dec 31 17:49 ufm-os-upgrade.sh
```

11.3.2 Step: 2 - Burn ISO to USB

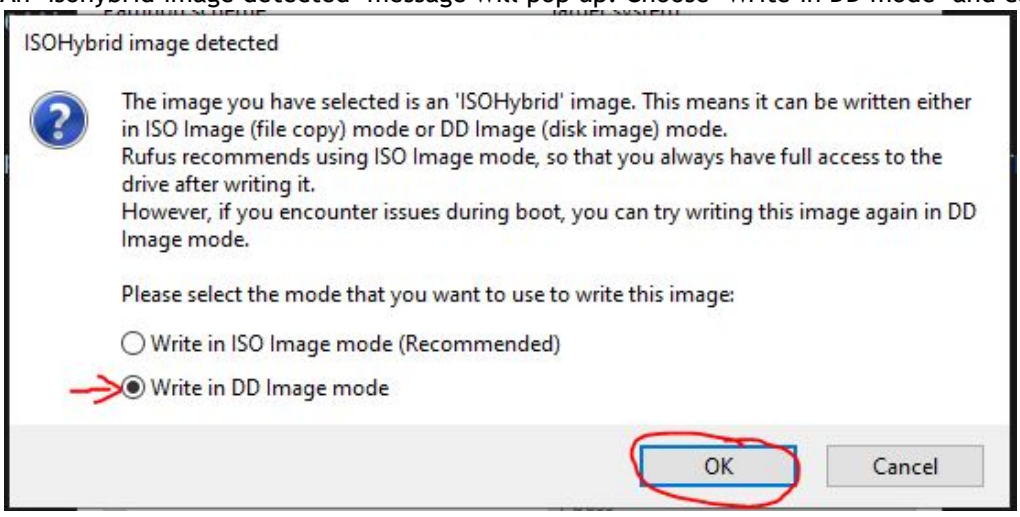
Burning ISO can be performed on Windows or Linux operating systems. Based on the desired installation method, follow the below instructions.

11.3.2.1 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.

11.3.2.2 Linux

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

   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).

   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:

   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
```

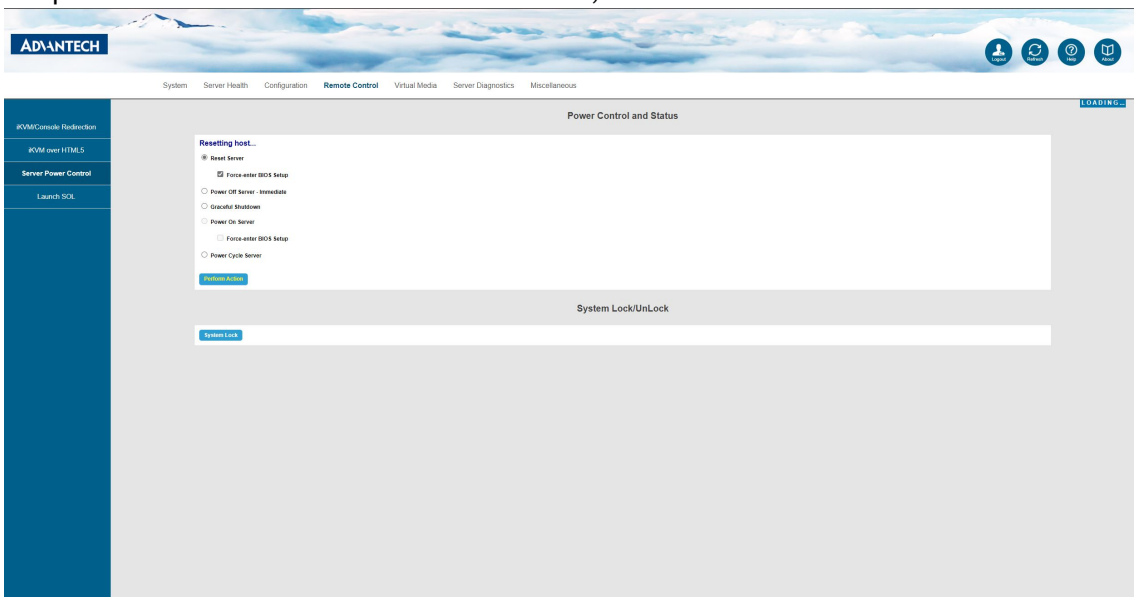
3. Verify that the USB is bootable:

```
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
```

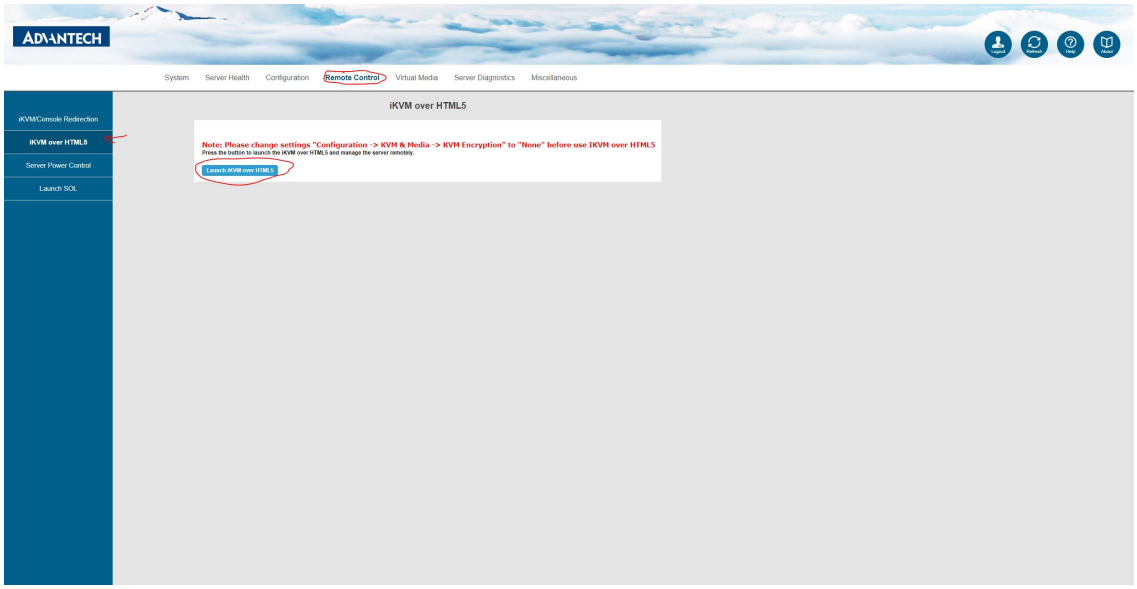
4. Unplug the USB.

11.3.3 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".

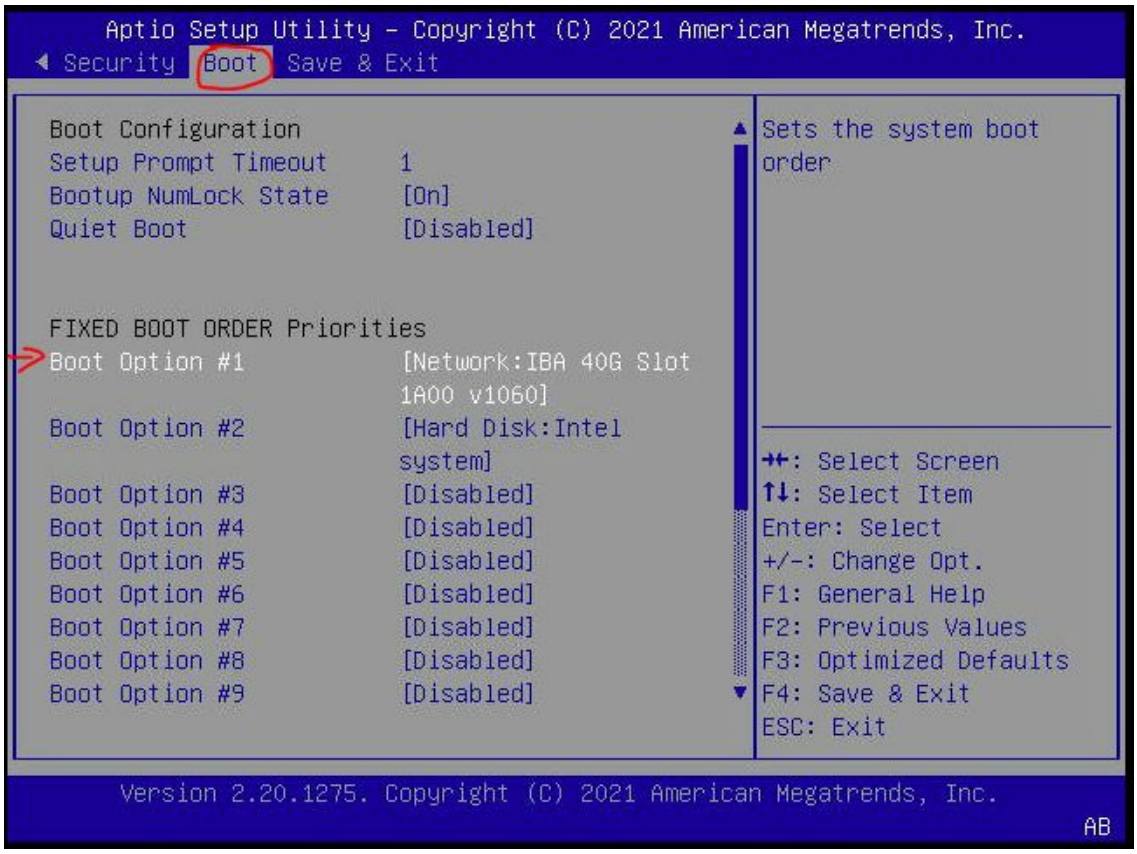


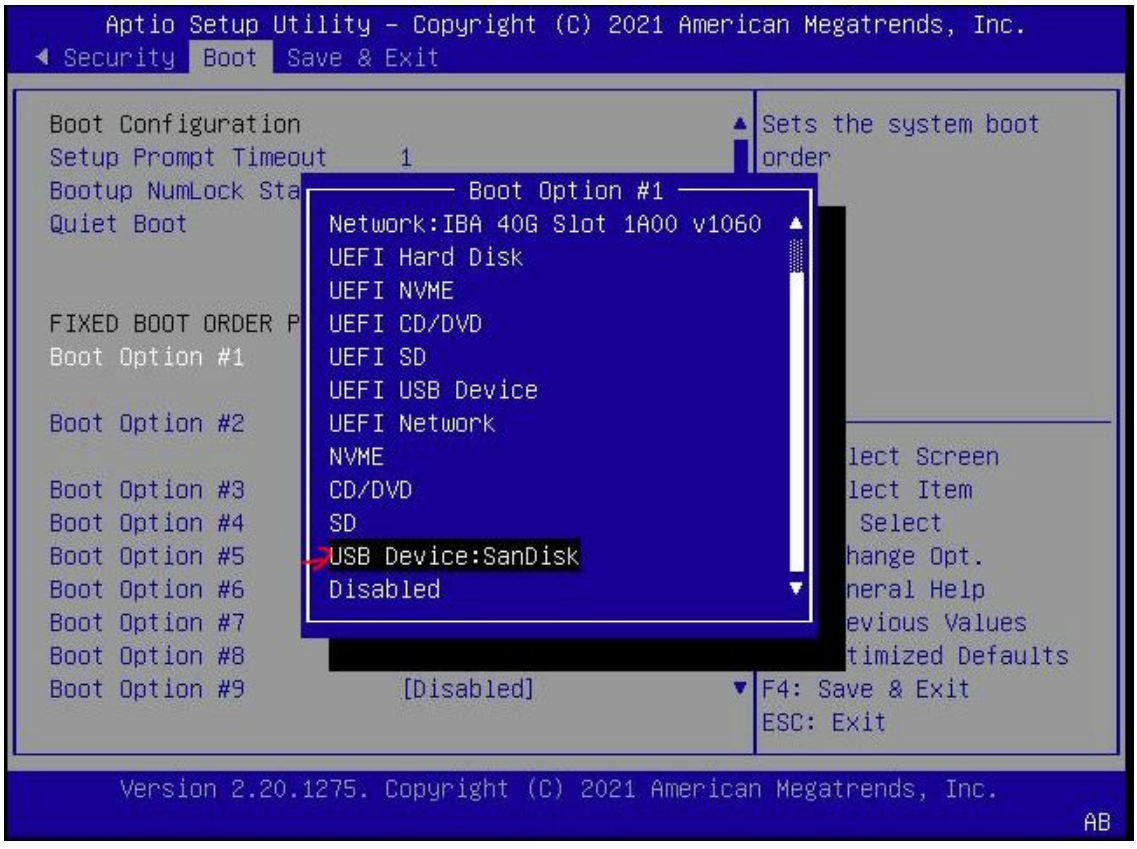
4. Navigate to "Remote Control" → "iKVM over HTML5" and click "Launch iKVM over HTML5" button.



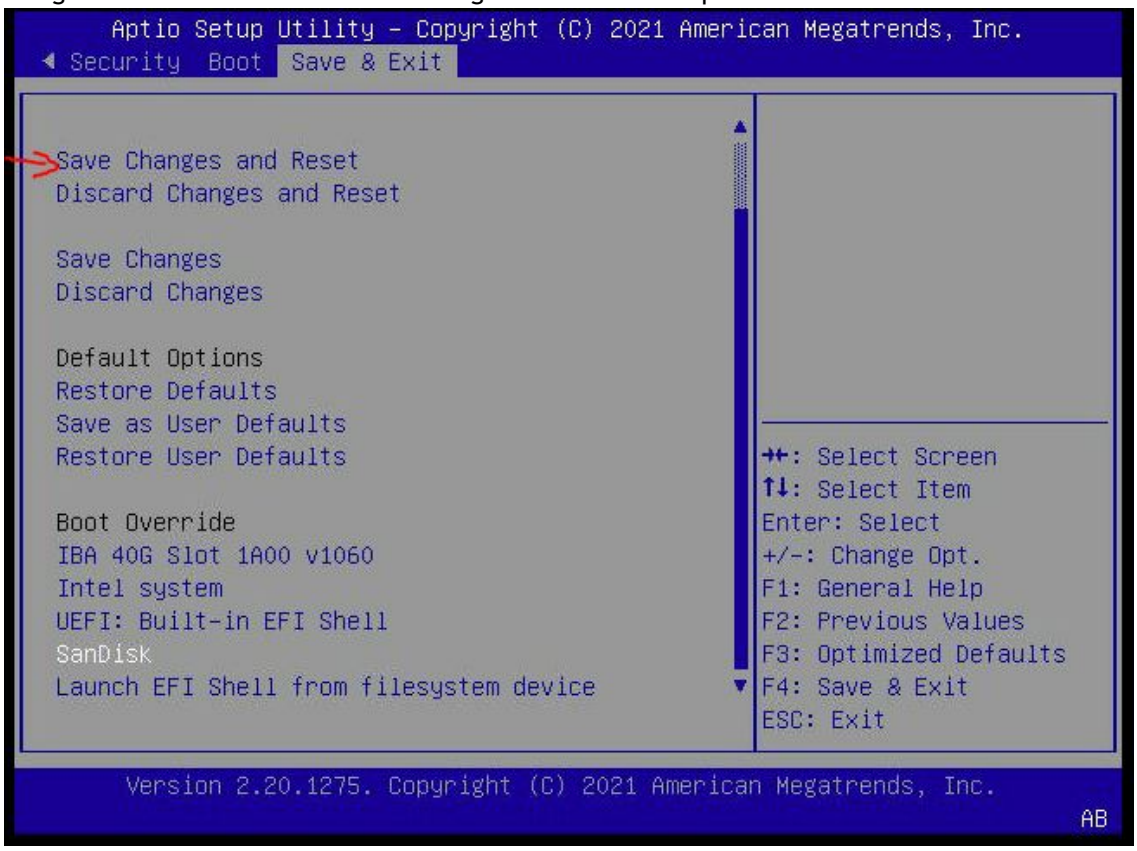
A new window will open.

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

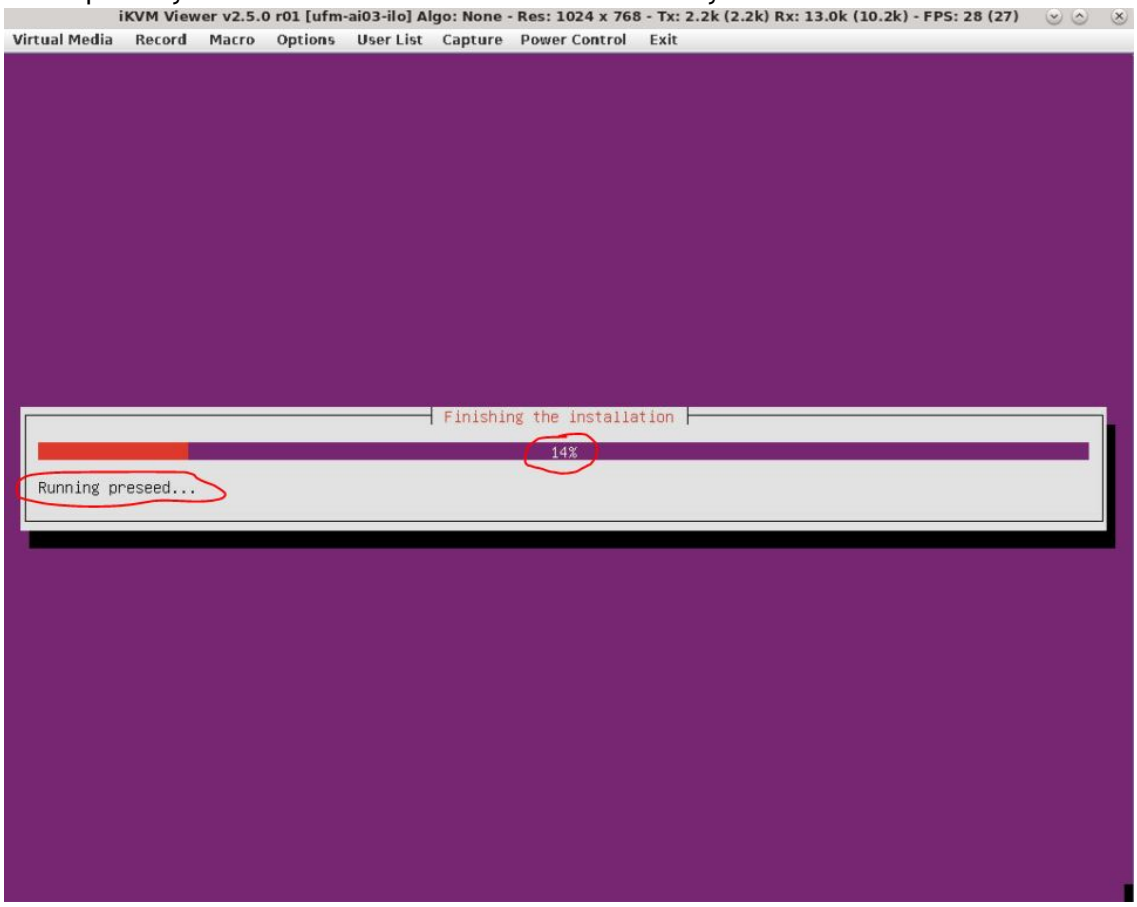

Aptio Setup Utility – Copyright (C) 2021 American Megatrends, Inc.
Security
Boot
Save & Exit
Boot Configuration
Setup Prompt Timeout 1
Bootup NumLock State [On]
Quiet Boot [Disabled]
FIXED BOOT ORDER Priorities
Boot Option #1 [Network:IBA 40G Slot 1A00 v1060]
Boot Option #2 [Hard Disk:Intel system]
Boot Option #3 [Disabled]
Boot Option #4 [Disabled]
Boot Option #5 [Disabled]
Boot Option #6 [Disabled]
Boot Option #7 [Disabled]
Boot Option #8 [Disabled]
Boot Option #9 [Disabled]
Sets the system boot order
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1275. Copyright (C) 2021 American Megatrends, Inc.
AB


Aptio Setup Utility – Copyright (C) 2021 American Megatrends, Inc.
Security
Boot
Save & Exit
Boot Configuration
Setup Prompt Timeout 1
Bootup NumLock Sta
Quiet Boot
FIXED BOOT ORDER P
Boot Option #1
Boot Option #2
Boot Option #3
Boot Option #4
Boot Option #5
Boot Option #6
Boot Option #7
Boot Option #8
Boot Option #9 [Disabled]
Boot Option #1
Network:IBA 40G Slot 1A00 v1060
UEFI Hard Disk
UEFI NVME
UEFI CD/DVD
UEFI SD
UEFI USB Device
UEFI Network
NVME
CD/DVD
SD
USB Device:SanDisk
Disabled
Sets the system boot order
lect Screen
lect Item
Select
hange Opt.
neral Help
evious Values
timized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1275. Copyright (C) 2021 American Megatrends, Inc.
AB

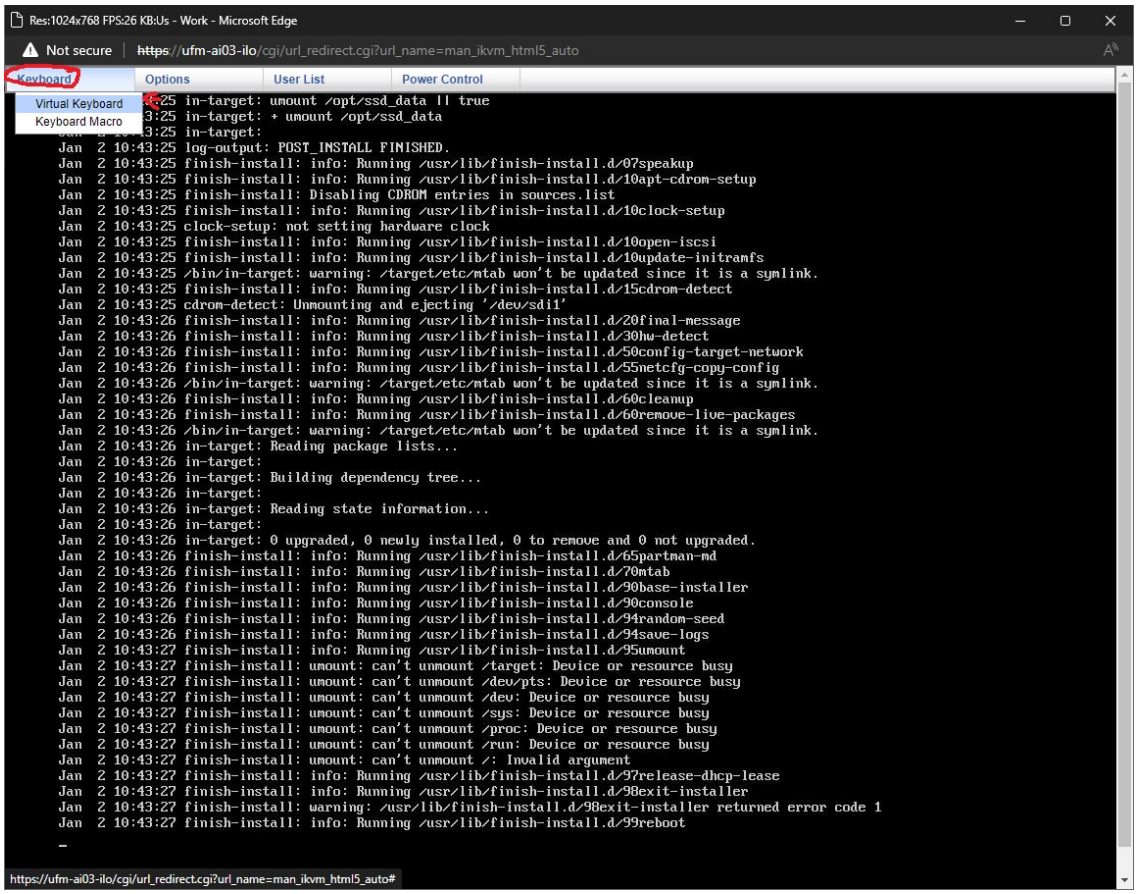
6. Navigate to "Save & Exit" → "Save Changes and Reset" and press enter.



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

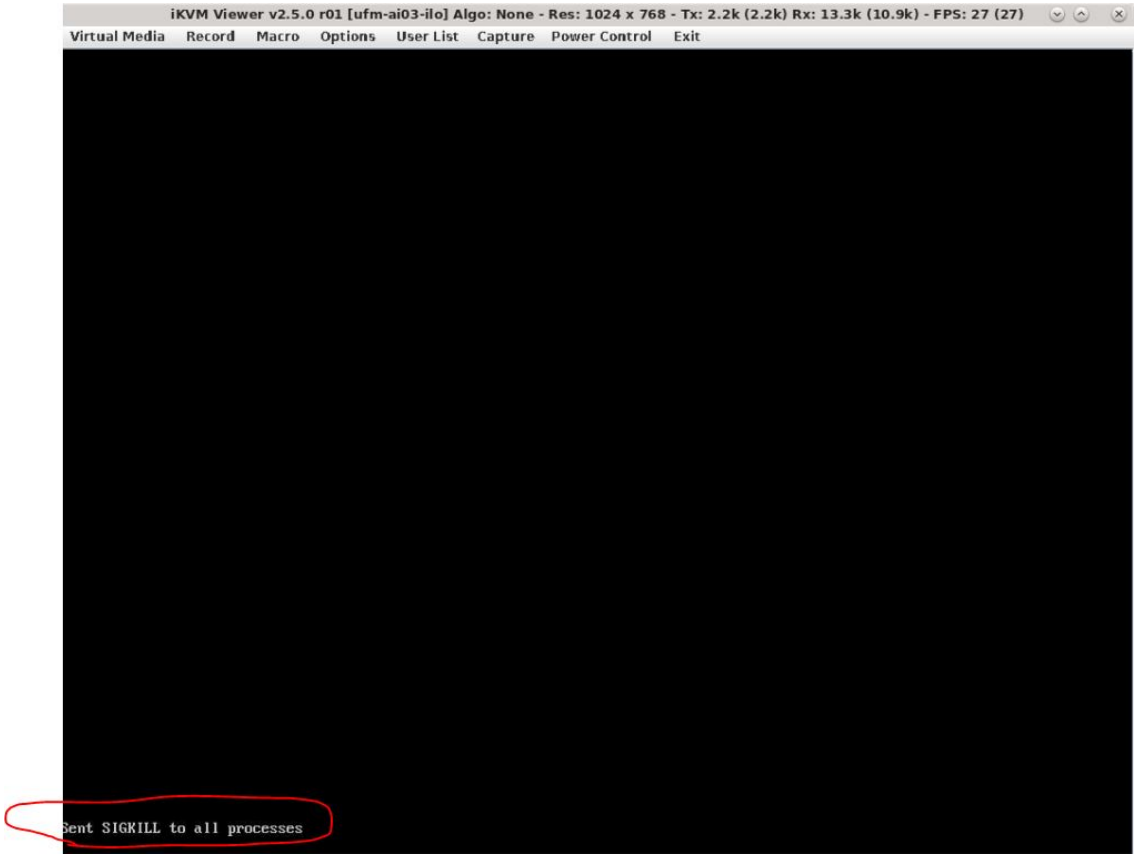


8. The process takes ~50 minutes, "Running preseed..." will show ~14-16 percent and will remain on this percentage for most of the time. This does not mean that the process is stuck.
   The preseed file runs in the background and will take ~35-40 minutes to complete.
   a log can be viewed by switching to tty4 by click on "Virtual Media" → "Virtual Keyboard"

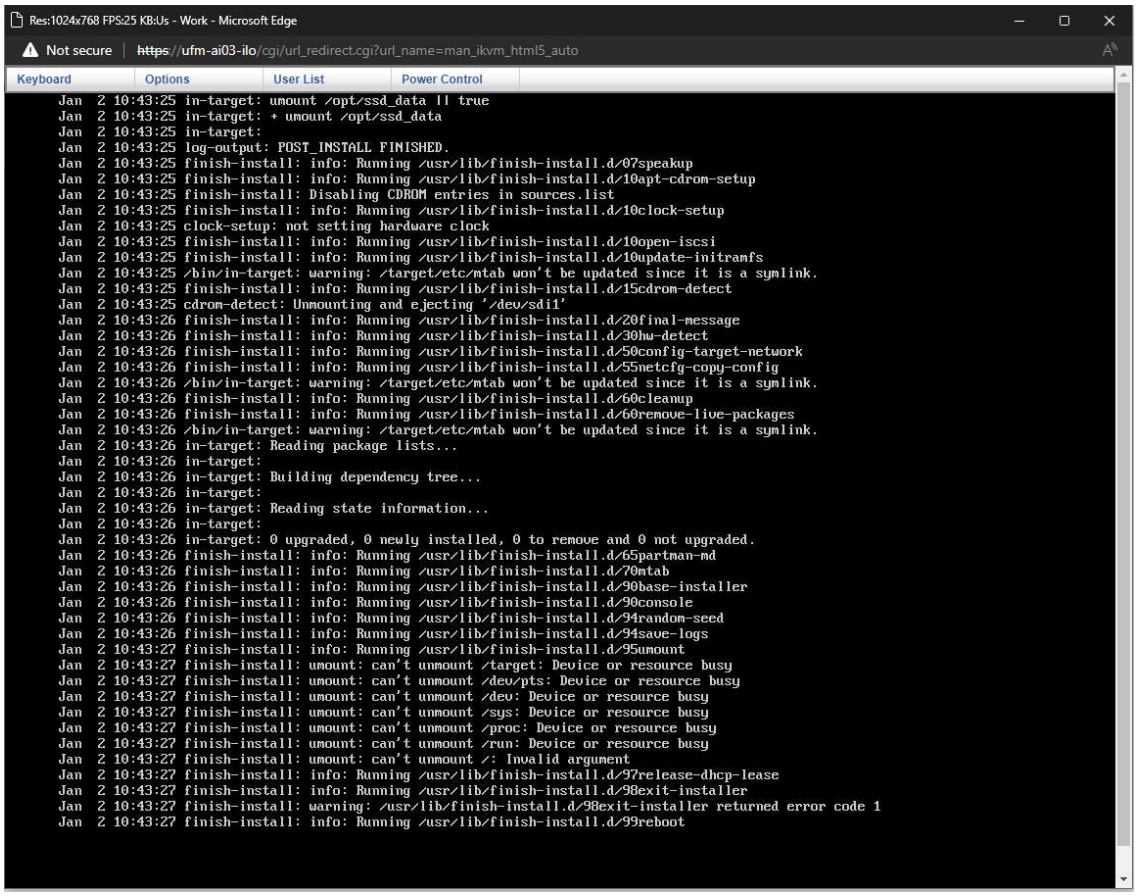


On the virtual keyboard that appears, press ALT+F4 (do this on the virtual keyboard to switch to tty4, otherwise the window will close).

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.

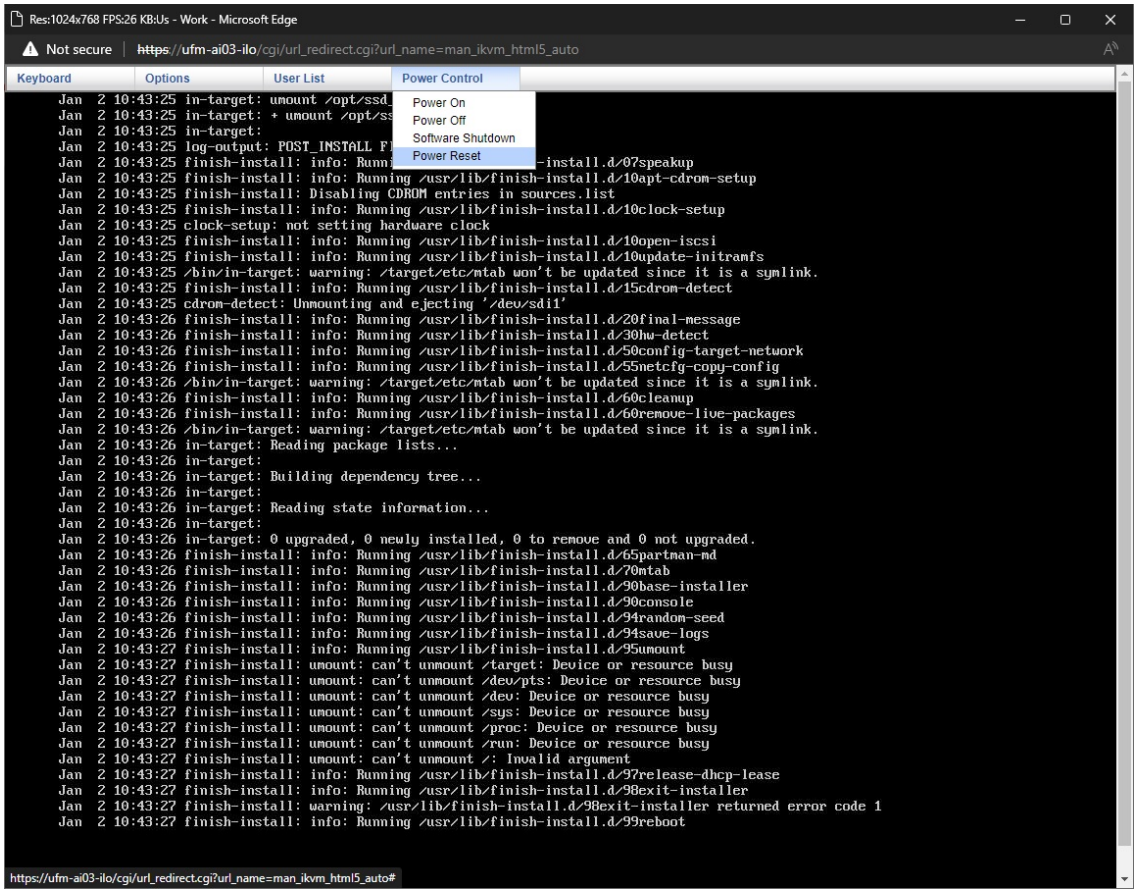


On the tty4 (log screen), a messages with "finish-install:" will appear.

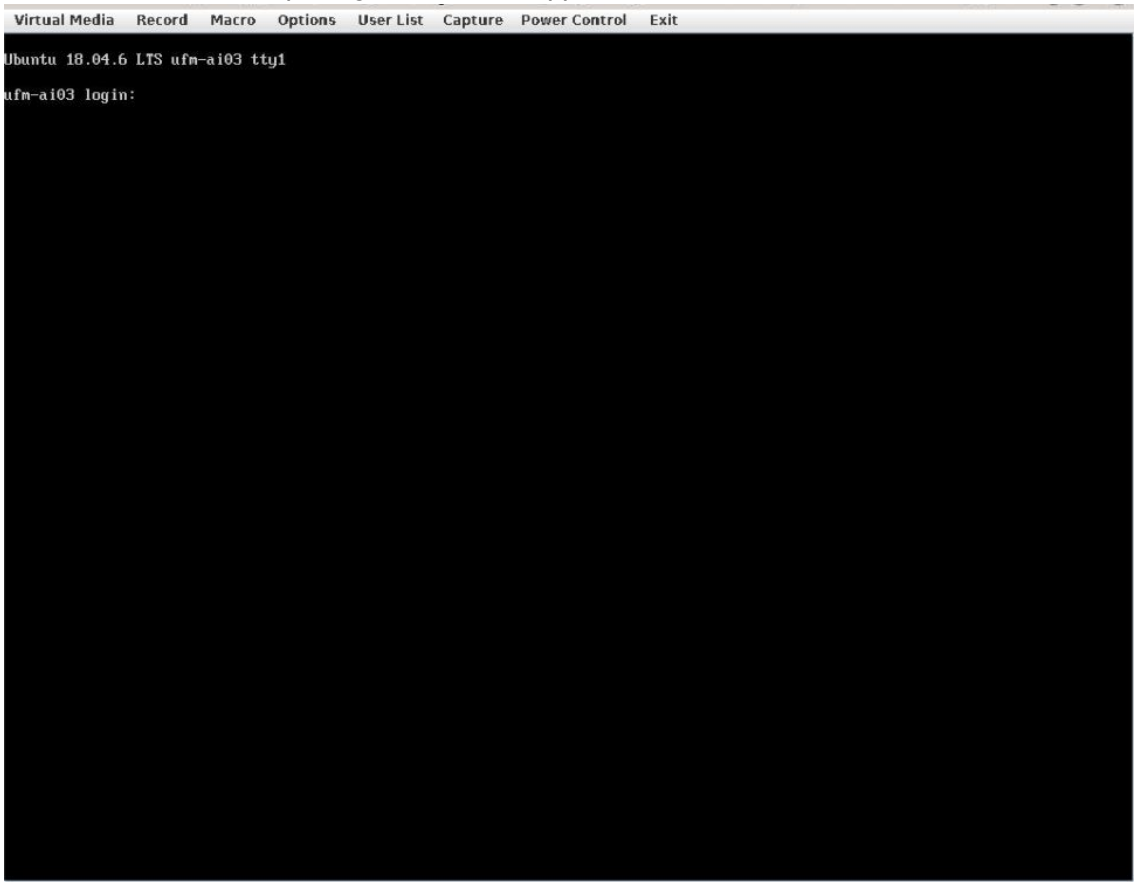


10. At this point, remove the USB from the Cyber-AI server (or reboot to BIOS as seen in step #3 and change the "Boot option #1" which was set to USB earlier to "disabled".

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

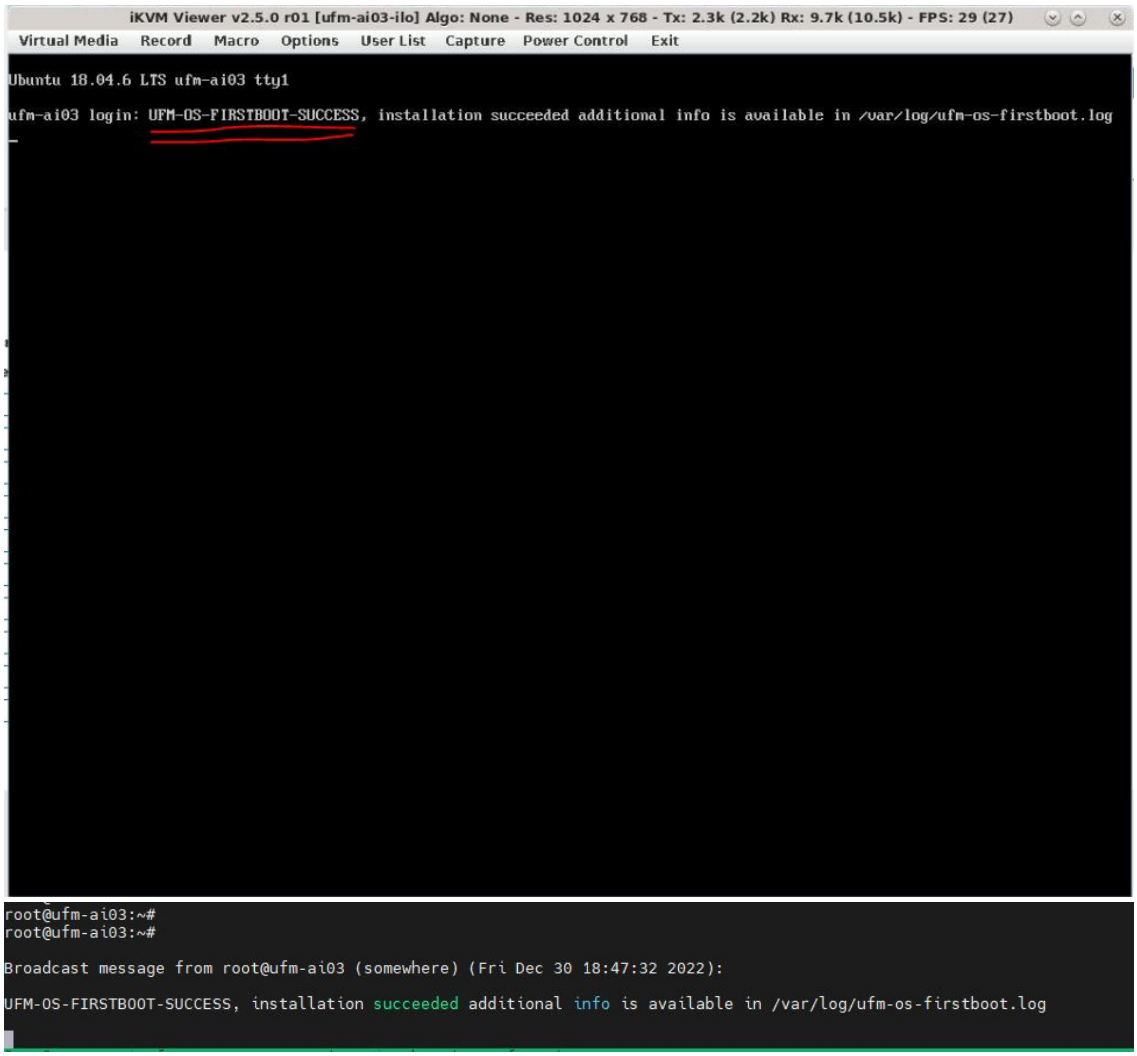


12. After the server boots up a login screen will appear.



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

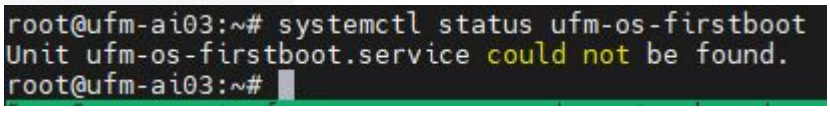
13. Additional software installation is triggered on the server's first boot. Once complete, a message will appear on all the connected terminals "UFM-OS-FIRSTBOOT-SUCCESS" in case of success, and FAILED in case the process failed.



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.



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

11.4 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.

11.4.1 Step 1: Extract the TAR file to a temporary directory

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

Extract TAR file

```
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.

Extract TAR file

```
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
```

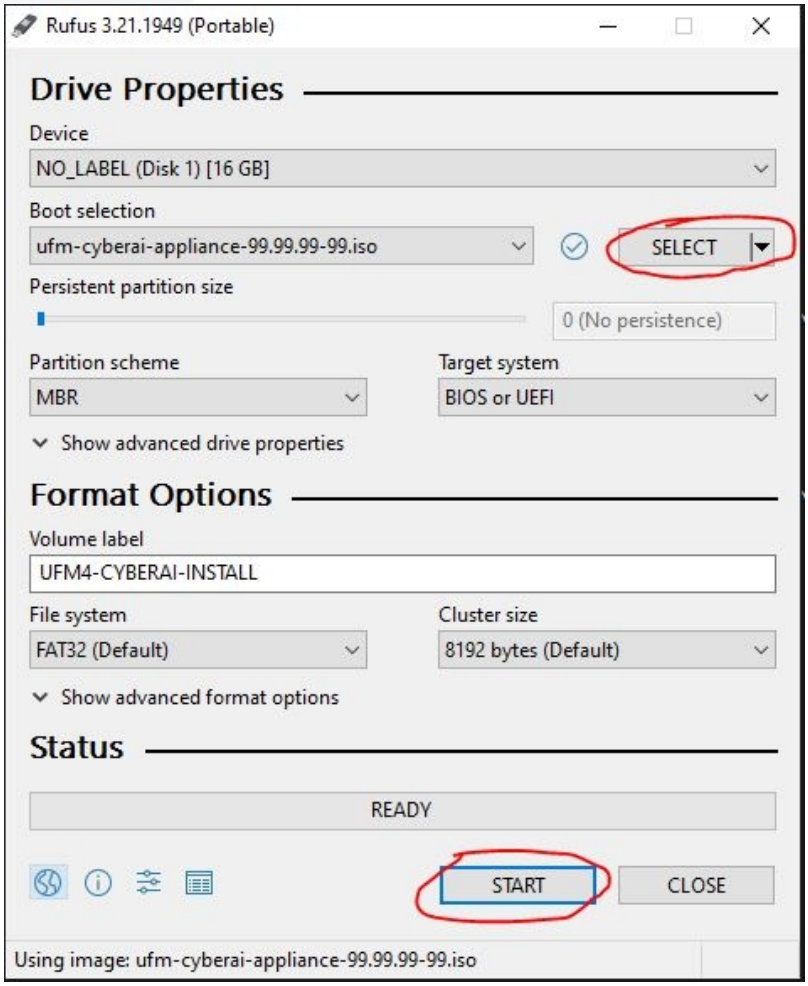
11.4.2 Step: 2 - Burn ISO to USB

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.

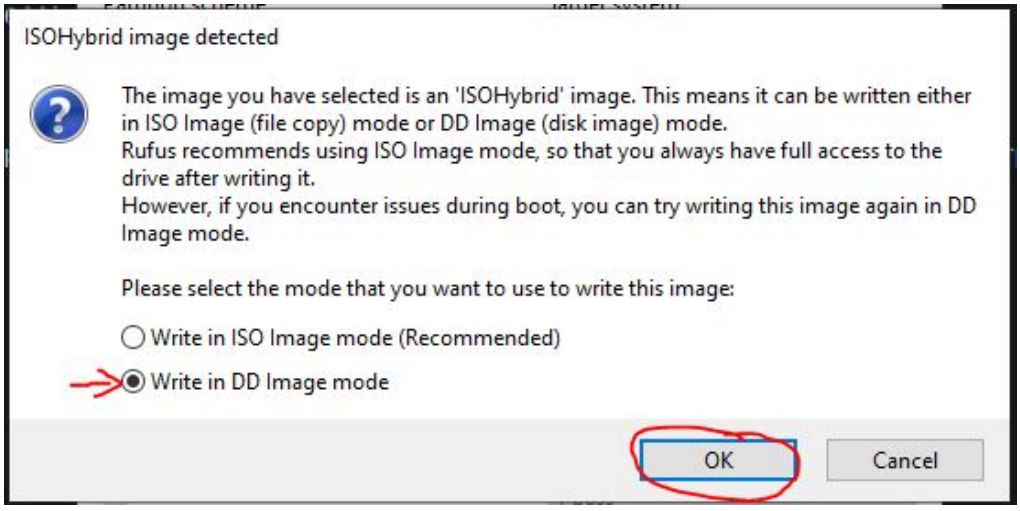
11.4.2.1 Windows

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".



5. You will see a message indicating that all data on the USB device will be erased. Click "OK and continue" to proceed.

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

11.4.2.2 Linux

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

   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).

   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
```

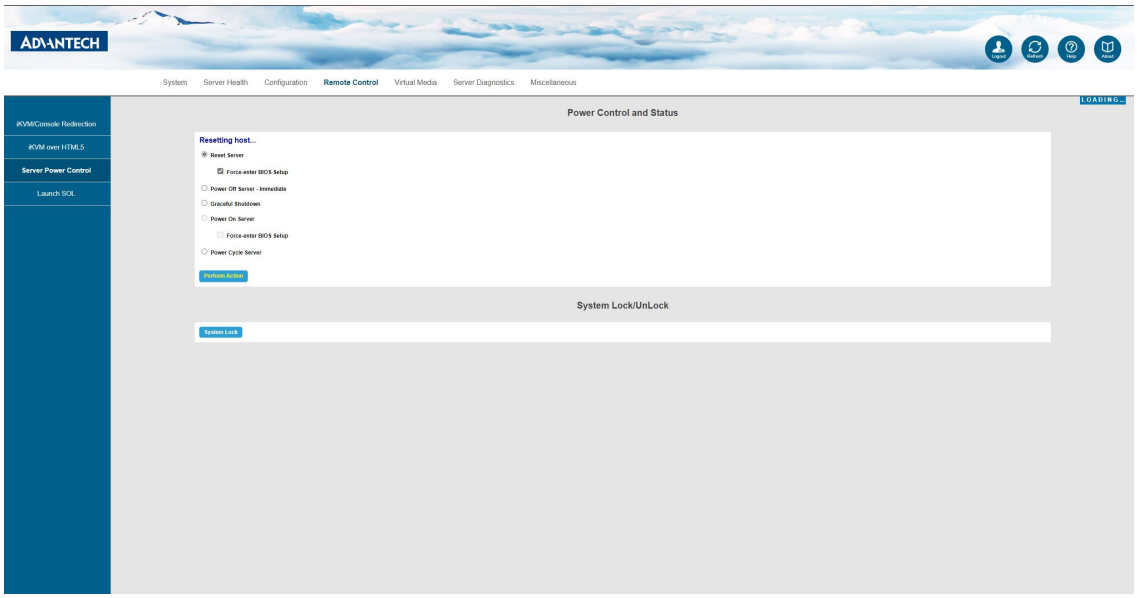
3. Verify that the USB is bootable:

```
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
```

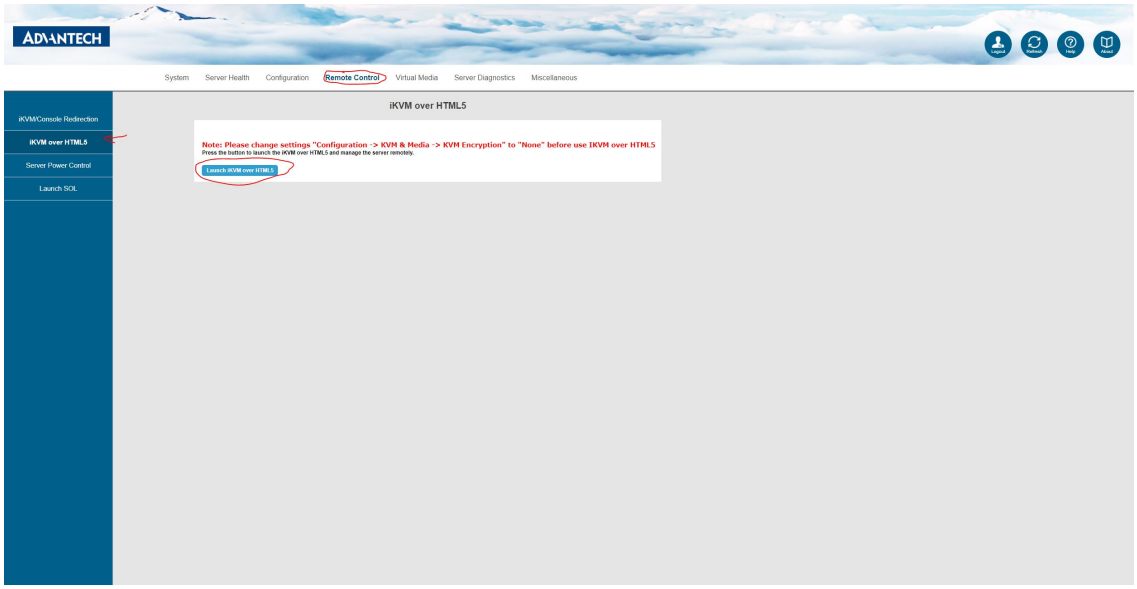
4. Unplug the USB.

11.4.3 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".

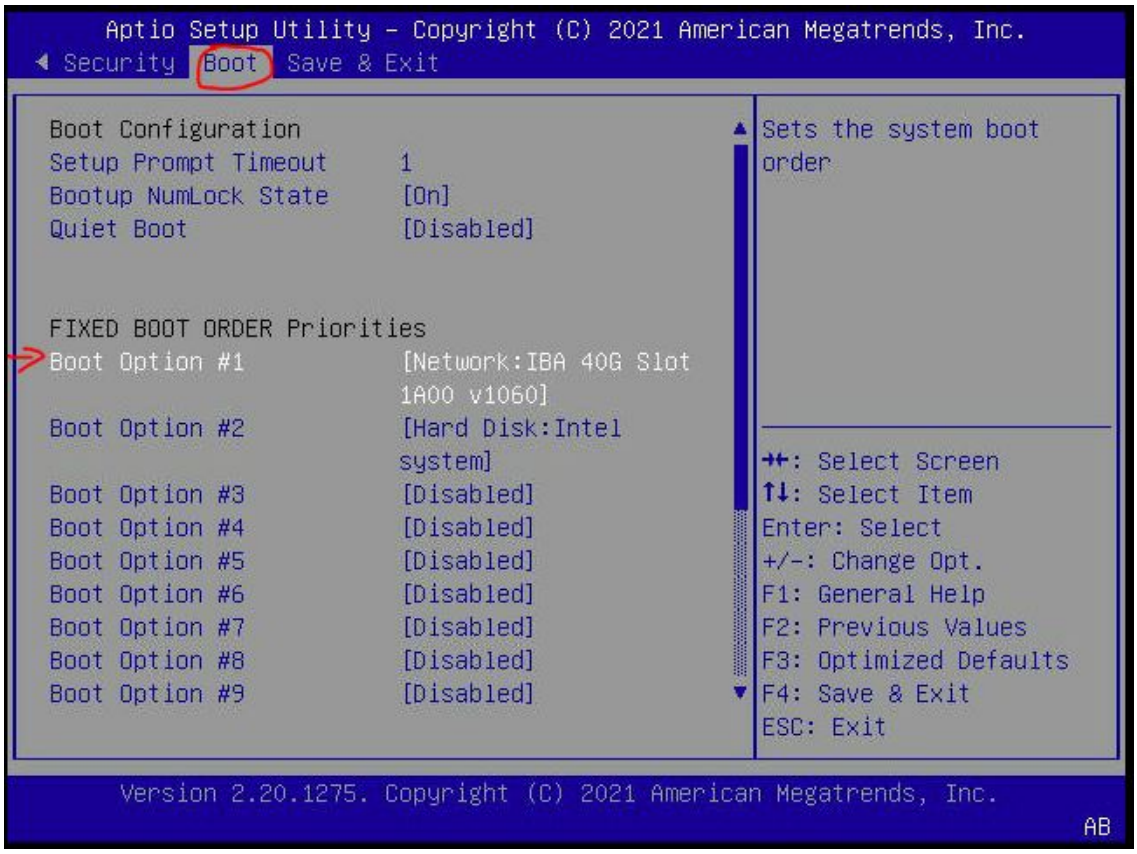


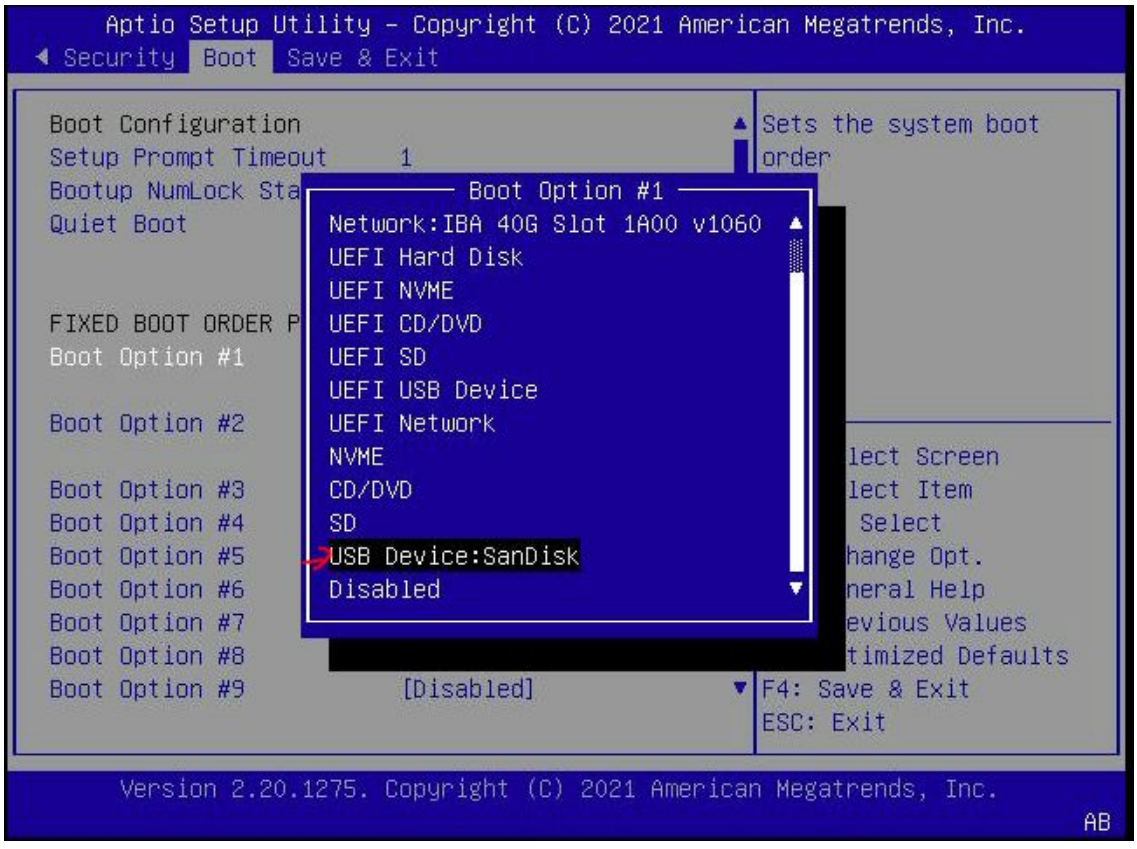
4. Navigate to "Remote Control" → "iKVM over HTML5" and click "Launch iKVM over HTML5" button.



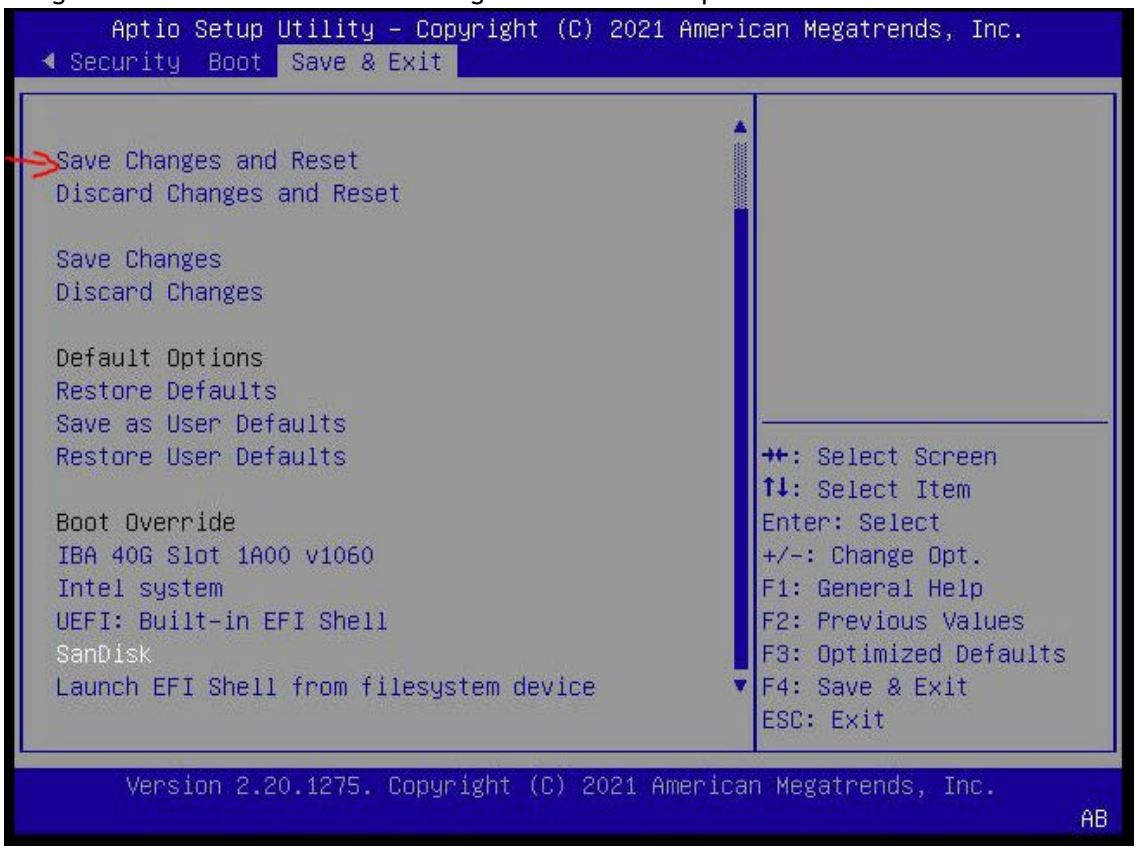
A new window will open.

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

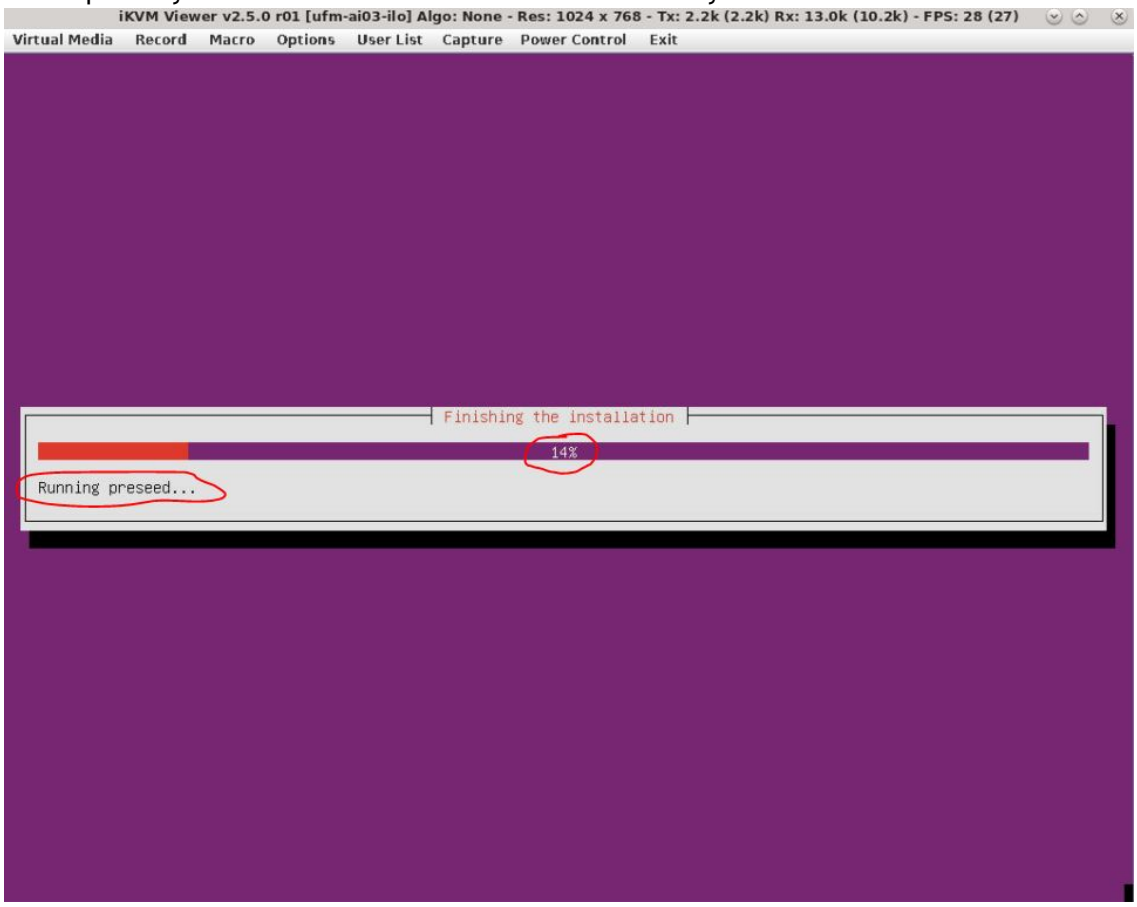

Aptio Setup Utility – Copyright (C) 2021 American Megatrends, Inc.
Security
Boot
Save & Exit
Boot Configuration
Setup Prompt Timeout 1
Bootup NumLock State [On]
Quiet Boot [Disabled]
FIXED BOOT ORDER Priorities
Boot Option #1 [Network:IBA 40G Slot 1A00 v1060]
Boot Option #2 [Hard Disk:Intel system]
Boot Option #3 [Disabled]
Boot Option #4 [Disabled]
Boot Option #5 [Disabled]
Boot Option #6 [Disabled]
Boot Option #7 [Disabled]
Boot Option #8 [Disabled]
Boot Option #9 [Disabled]
Sets the system boot order
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1275. Copyright (C) 2021 American Megatrends, Inc.
AB


Aptio Setup Utility – Copyright (C) 2021 American Megatrends, Inc.
Security
Boot
Save & Exit
Boot Configuration
Setup Prompt Timeout 1
Bootup NumLock Sta
Quiet Boot
FIXED BOOT ORDER P
Boot Option #1
Boot Option #2
Boot Option #3
Boot Option #4
Boot Option #5
Boot Option #6
Boot Option #7
Boot Option #8
Boot Option #9 [Disabled]
Boot Option #1
Network:IBA 40G Slot 1A00 v1060
UEFI Hard Disk
UEFI NVME
UEFI CD/DVD
UEFI SD
UEFI USB Device
UEFI Network
NVME
CD/DVD
SD
USB Device:SanDisk
Disabled
Sets the system boot order
lect Screen
lect Item
Select
hange Opt.
neral Help
evious Values
timized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1275. Copyright (C) 2021 American Megatrends, Inc.
AB

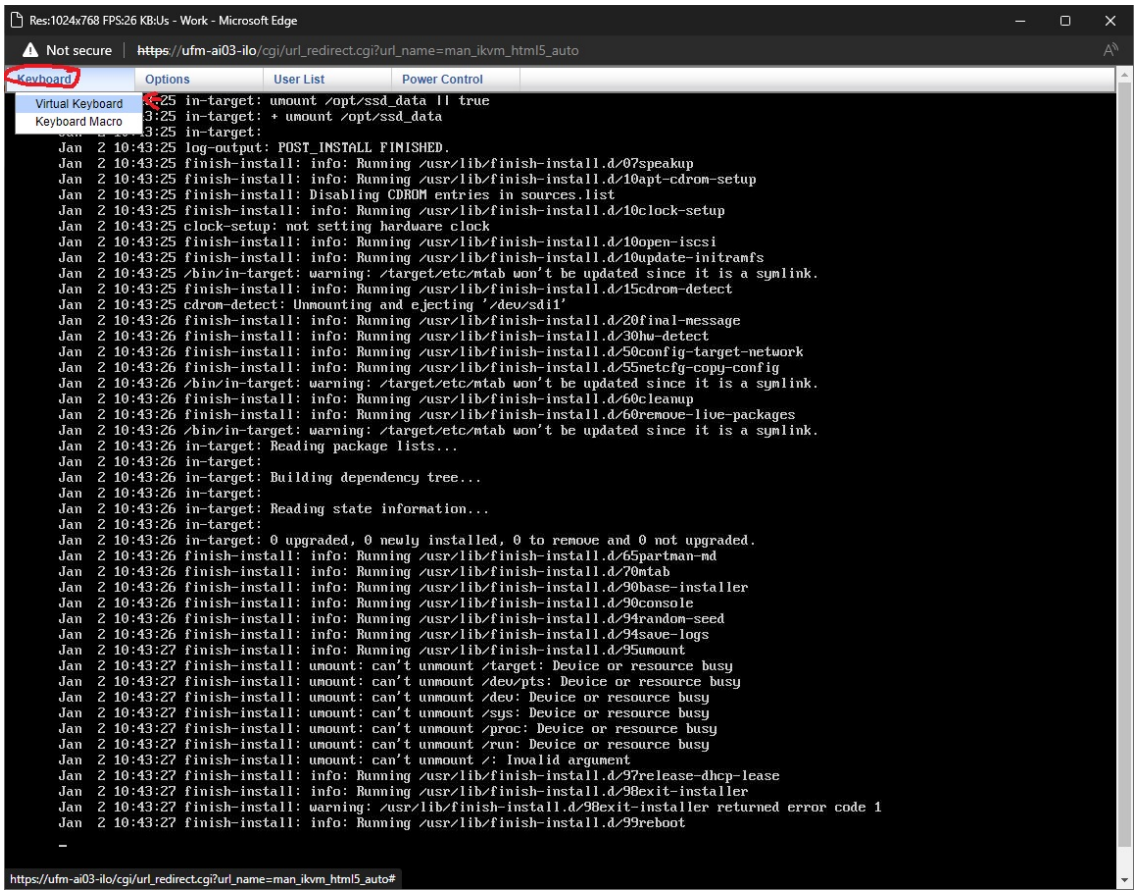
6. Navigate to "Save & Exit" → "Save Changes and Reset" and press enter.



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

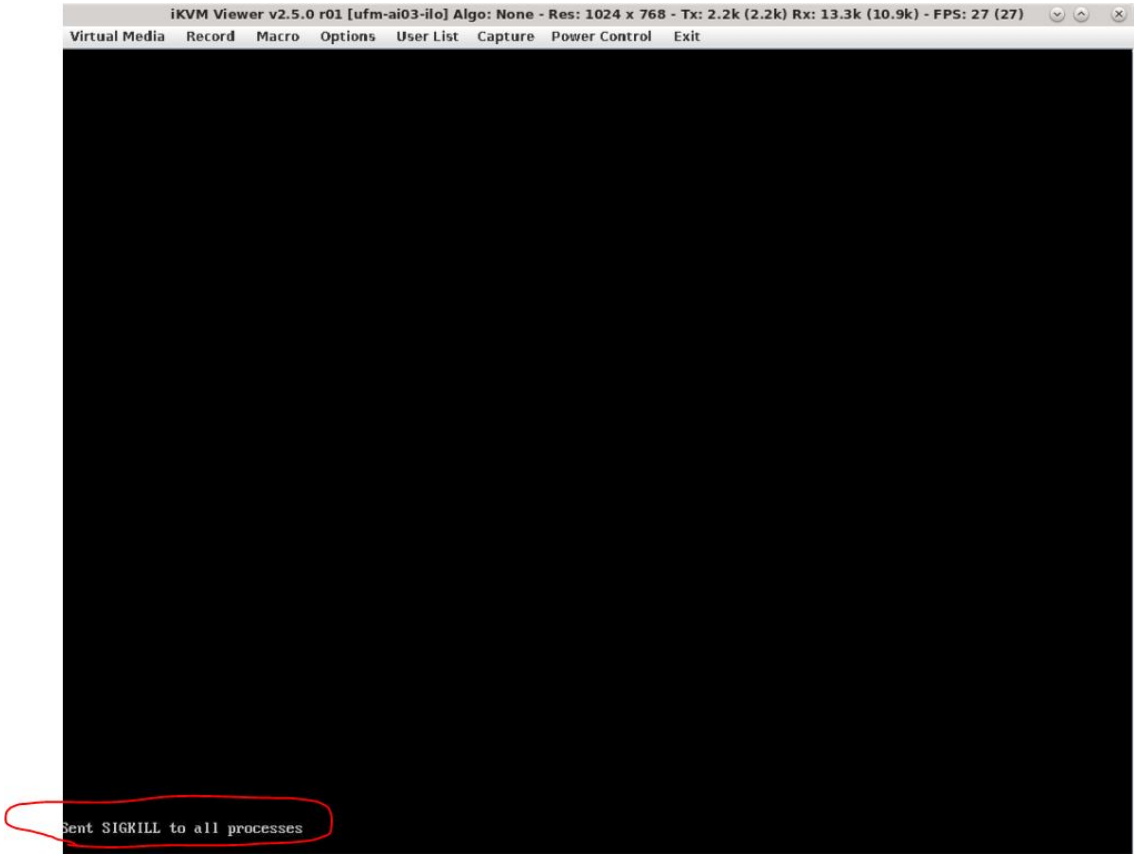


8. The process takes ~50 minutes, "Running preseed..." will show ~14-16 percent and will remain on this percentage for most of the time. This does not mean that the process is stuck.
   The preseed file runs in the background and will take ~35-40 minutes to complete.
   a log can be viewed by switching to tty4 by click on "Virtual Media" → "Virtual Keyboard"

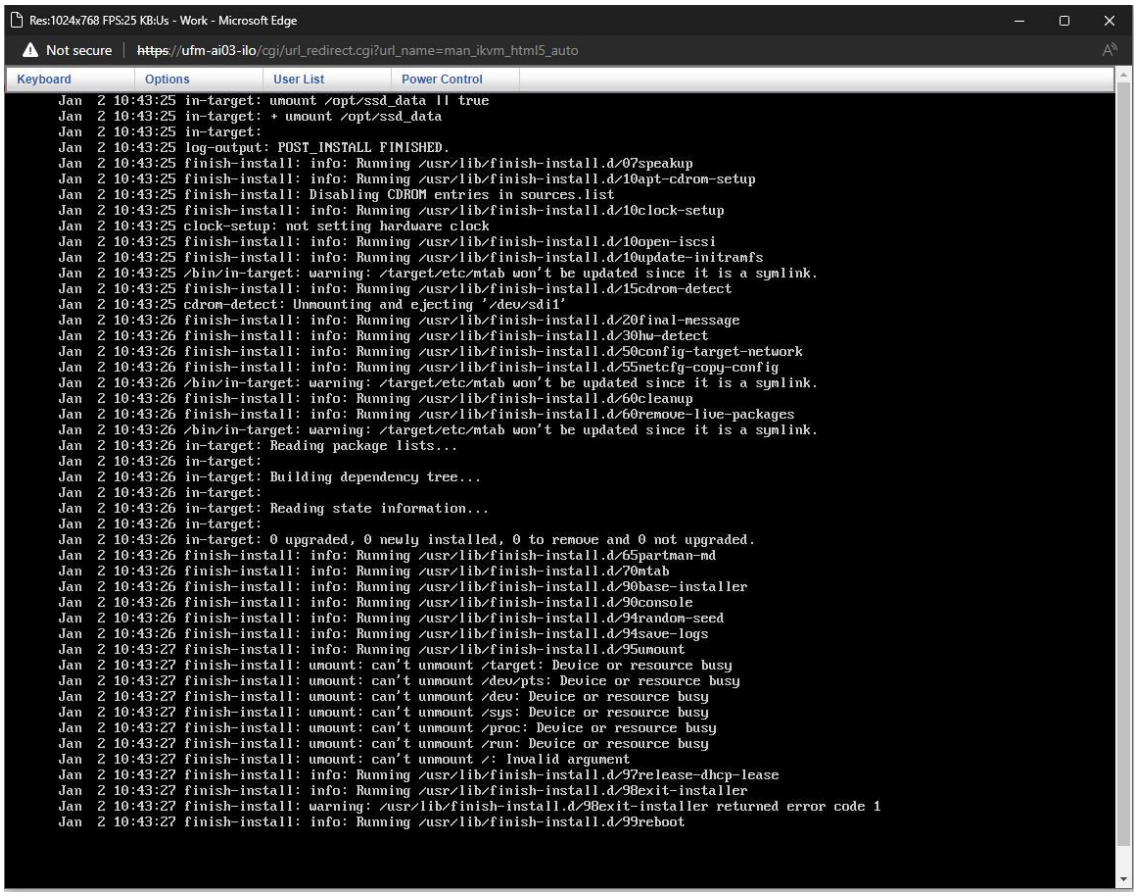


On the virtual keyboard that appears, press ALT+F4 (do this on the virtual keyboard to switch to tty4, otherwise the window will close).

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.

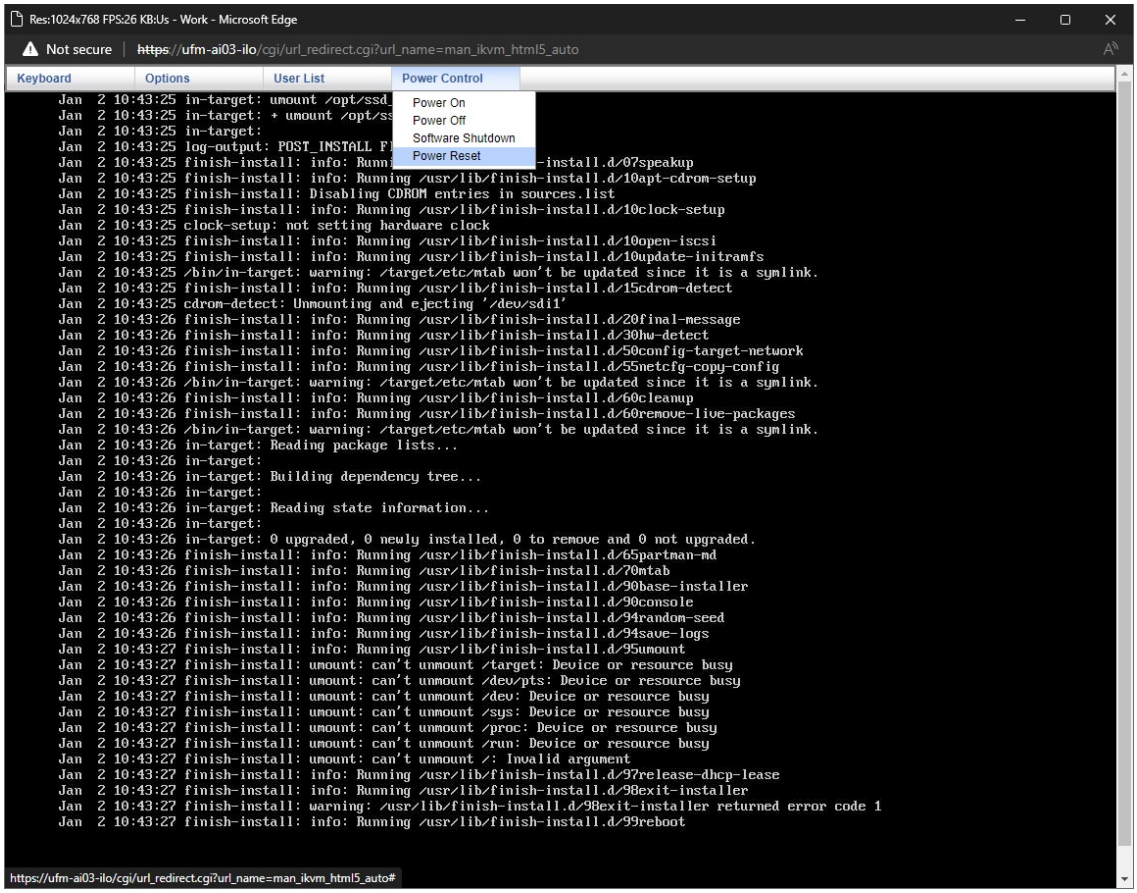


On the tty4 (log screen), a messages with "finish-install:" will appear.

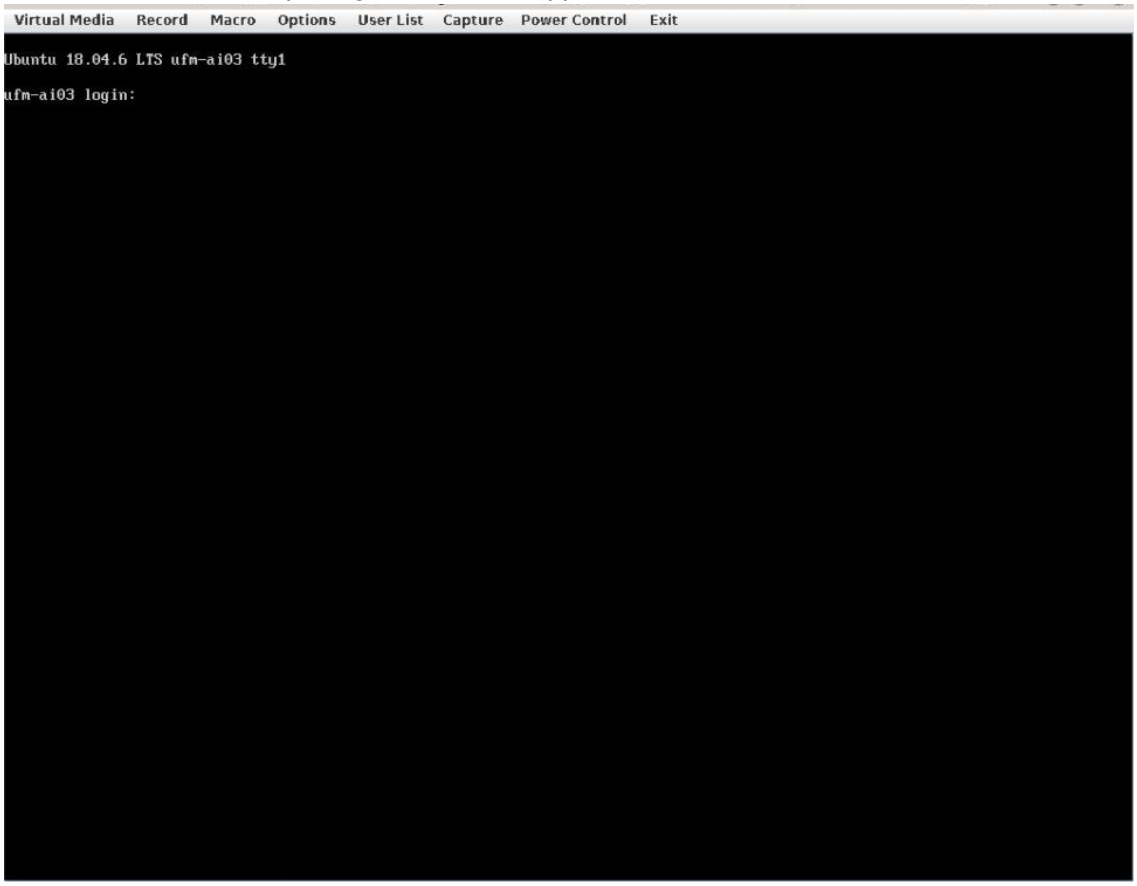


10. At this point, remove the USB from the Cyber-AI server (or reboot to BIOS as seen in step #3 and change the "Boot option #1" which was set to USB earlier to "disabled".

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

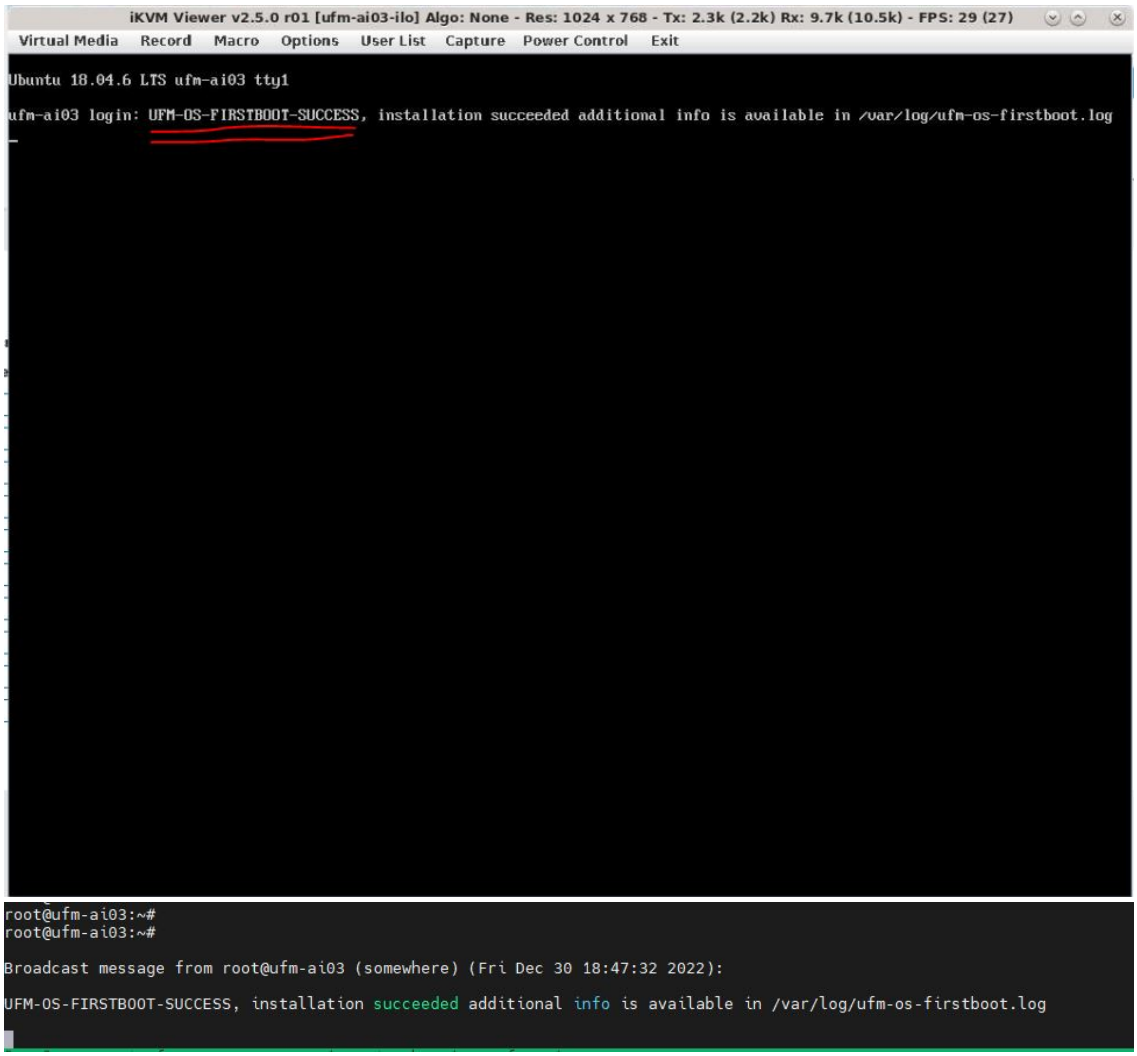


12. After the server boots up a login screen will appear.



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

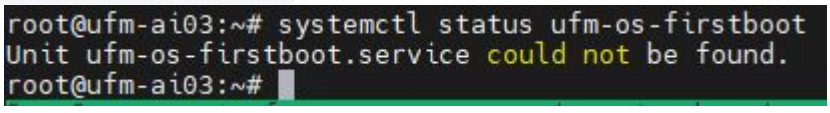
13. Additional software installation is triggered on the server's first boot. Once complete, a message will appear on all the connected terminals "UFM-OS-FIRSTBOOT-SUCCESS" in case of success, and FAILED in case the process failed.



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.



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

12 Document Revision History

Revision	Date	Description
Rev 2.7.0	Feb 8, 2024	Added: • In Link Analysis: Updated Get Link Failure Prediction History and Get Link Anomaly Prediction History • In Alert Filters: Get Histogram for Link Statu, Link Status and Get Properties for Link Status Updated Cyber-AI Analytics
Rev 2.6.1	Dec 12, 2023	Updated: • 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: • 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: • 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: • Changes and New Features in This Release • Bug Fixes in This Release Added: • 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	Added: • Cable Alerts Summary • CLI Tools • Morpheus Integration Updated • Changes and New Features in This Release • Software Management • Cyber-AI Analytics • Get Specific Network Alert • Get Specific Tenant Alert • Threshold Events • High Availability
Rev 2.1	Jul, 2022	Added: • Cables Alerts • Get the Telemetry Counter list Updated: • Cyber-AI Analytics • Suspicious Behavior

Revision	Date	Description
	Aug, 2022	Updated links here.
Rev 2.0	Apr, 2022	Updated: • Software Management • Cyber-AI Analytics • Configuration • Suspicious Behavior • Link Analysis • Resources • Telemetry Data • Alert Filters
Rev 1.1.0	Jan, 2021	Added: • Downloading the Software Updated: • Deploying UFM Cyber-AI • Upgrading UFM Cyber Software • High Availability
Rev 1.0	Dec, 2021	Added: • Anomaly Analysis • Cable Anomalies Detection • Job Analytics • Get Cable Trend • Events Flows • Elements • Timeline • Influencers • 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. Neither NVIDIA Corporation nor any of its direct or indirect subsidiaries and affiliates (collectively: “NVIDIA”) make any 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, the NVIDIA logo, and Mellanox are trademarks and/or registered trademarks of NVIDIA Corporation and/or