Oracle Autonomous Health Framework Fleet Insights User's Guide

F96585-09
November 2025

Oracle Autonomous Health Framework Fleet Insights User's Guide ,

F96585-09

Primary Author: Nirmal Kumar

Contributing Authors: Arjun Upadhyay, Deepak Mecheri , Gareth Chapman , Priyank Mehra , Rishabh Bhardwaj , Sai Chiranjeevi Konapala , Troy Anthony

Contents

Changes in this Release

Changes in Previous Releases

1 Get Started

Changes in this Release

This preface lists changes in the Oracle Autonomous Health Framework Fleet Insights User's Guide 25.2.0.0.

Space Analysis

The Space Analysis dashboard provides a comprehensive overview of disk space utilization across all nodes in the fleet. It enables administrators to proactively detect storage-related issues, identify nodes approaching capacity, and manage disk usage efficiently.

For more information, see Space Analysis.

RPM List

The RPM List dashboard offers a comprehensive matrix view of installed RPM packages and their versions across multiple nodes and clusters. It serves as a critical tool for verifying software consistency and quickly identifying discrepancies across systems.

For more information, see RPM List.

System Changes

The System Changes dashboard provides visibility into system-level modifications — such as database parameter updates and configuration adjustments — across the fleet, over a selected time range.

For more information, see System Changes.

Patch Information

The Patch Information dashboard provides a centralized view of patch compliance across the fleet. It enables administrators to monitor, validate, and track the deployment of software patches—particularly for databases and other critical components.

For more information, see Patch Information.

Detected Problems

The Detected Problems dashboard provides a centralized, real-time view of critical issues identified across database clusters. It helps administrators and engineers quickly assess the nature and impact of system anomalies, facilitating faster root cause analysis and resolution.

For more information, see .Detected Problems

Fleetwide Capacity Analysis

The Fleet Resource Insights dashboard provides a quick view of resource usage across your fleet, helping you identify top and bottom consumers, spot bottlenecks, and uncover underutilized nodes for optimized performance.

Cluster-Wise Usage Trends and Forecast

Get a detailed view of cluster-level resource utilization with current trends and future forecasts to support proactive capacity planning. Visualize usage patterns by metric, track forecast growth, and use historical trends to optimize resource allocation.

Filter Fleet Based on Targets (Cluster and Hosts)

You can now filter fleet data by clusters and hosts, enabling more precise comparisons and analysis.

- Cluster & Node Selection: Select one or more clusters and individual hosts to narrow down the data view.
- Cross-Metric Comparison: Use this feature to compare systems across metrics such as CPU, memory, patch state, and more.
- Helps isolate anomalies, validate consistency, and perform focused health reviews.
- Ideal for multi-cluster environments or segmented monitoring strategies.

Import Diagnostic Collections to Fleet Insights

Fleet Insights now supports importing diagnostic collections manually, even when a direct connection to AHF is unavailable.

How it works:

- Accepts `.zip` diagnostic bundles
- Requires generic user credentials to initiate processing

Benefits:

- Enables offline or air-gapped analysis workflows
- Provides flexibility in environments with strict security or connectivity restrictions

Collection Retention Period

You can now define how long diagnostic collections are retained on the Fleet Insights server.

Previously: Retention was indirectly controlled via disk space usage

Now: You can specify a time-based retention policy (e.g., retain data for 30, 60, or 90 days)

Improves control over:

- Data lifecycle management
- Storage optimization
- Compliance with audit/data retention policies

Purge Disk Utilization Percentage

You can now configure the disk utilization percentage threshold at which purging begins on the Fleet Insights server.

Changes in Previous Releases

AHF Fleet Insights 25.1.0.0

Single-Instance Support

AHF Fleet Insights now supports single-instance systems.

Many organizations use a mix of clustered and single-instance databases. Previously, AHF Fleet Insights supported only clustered environments.

With this release, AHF Fleet Insights expands its capabilities to include the registration and management of single-instance systems.

To register a single-instance system, use the standard registration command:

```
ahf configuration set --type fleet-insights --user-name <registration_user> --
url <ahffi_app_url>
```

Event Time in Events Drilldown Tables

Event analysis and diagnostics have been improved with the introduction of precise timestamps in the Events Drilldown Tables.

Knowing exactly when an event occurred is essential for diagnosing issues and reconstructing system activity timelines. A new Event Time column has been added to the Events Drilldown Tables, offering detailed timing information for each event. This enhancement significantly

improves visibility into system behavior, enabling more accurate diagnostics, auditing, and event correlation.

With this feature, users can more easily identify patterns, understand the sequence of critical events, and gain deeper insights into their system's operational history.

How to View the Event Time:

1. From the Home page, set your desired time range using the filter.
2. Click the Events panel to open the Events page.
3. On the Events page, click any chart or table entry to drill down into a specific event type.
4. The Events Drilldown Table at the bottom of the page now includes the new Event Time column.

Configurable Session Timeout

AHF Fleet Insights now offers configurable session timeouts, providing a balance between enhanced security and improved user experience.

Previously, sessions were limited to a fixed 30-minute timeout, often resulting in users being logged out and needing to re-authenticate. With this update, administrators can now customize session timeout durations based on their organization's security policies and operational requirements—up to a maximum of 24 hours (1440 minutes).

This flexibility ensures uninterrupted access for longer tasks while still allowing organizations to enforce session expiration for security compliance.

How to Set the Session Timeout

You can configure the session timeout either via the command line or the web interface:

- Command Line:

  ```
  ahffi updateproperty -k TIMEOUT -v <minutes>
  ```

- Web Interface:
  1. Click your login name at the top right corner of the Fleet Insights web application.
  2. Select **Admin**.
  3. Go to **Configurations** and set the desired timeout value.

Prioritized Collection Purging

AHF Fleet Insights now features an improved data purging policy that intelligently prioritizes which collections to retain, ensuring more useful data remains available for longer.

Automated purging of older collections is critical for optimizing storage and maintaining system performance. With this enhancement, AHF Fleet Insights refines its approach by assigning higher deletion priority to:

- Older collections
- Collections not actively used by the user interface

This means more recent and relevant data is preserved longer, giving users better access to the information that matters most—especially during troubleshooting or historical analysis.

No configuration is necessary—this enhancement is automatically applied and requires no user action.

Support for Custom Installation Temp Directory

The AHF Fleet Insights installer now supports the `AHFFI_TMP_DIR` environment variable, allowing users to specify a custom directory for storing temporary files during installation.

By default, the installer writes temporary files to the `/tmp` directory. However, this location may not always be suitable—particularly in environments with limited disk space or restrictive permissions.

To address this, users can now redirect temporary file storage to an alternative location by setting the `AHFFI_TMP_DIR` environment variable before running the installer.

Before running the installer, specify a custom temporary directory by exporting `AHFFI_TMP_DIR=<TEMP_DIR_PATH>`.

1

Get Started

- What is AHF Fleet Insights?
  AHF Fleet Insights enables you to efficiently oversee and diagnose a fleet of database systems, ensuring seamless and reliable database services for users. A fleet refers to a collection of database clusters or single-instance systems.
- Prerequisites
  Review the prerequisites to install and use AHF Fleet Insights on various supported platforms.
- Users and Privileges
  Review the list of users and their privileges.
- Supported Platforms
  Review the list of supported platforms.
- Recommended Browsers
  Review the list of recommended browsers.
- Deploy AHF Fleet Insights
  Learn to deploy AHF Fleet Insights.
- Import SSL Certificates
  To import and use custom-SSL certificates other than the default one created during installation, use this procedure.
- Update Properties
  To update a property or a set of properties, use this procedure.
- Diagnose AHF Fleet Insights
  The diagnose tool helps you collect diagnostic data on-demand to debug and maintain AHF Fleet Insights.
- Uninstall AHF Fleet Insights
  Learn to uninstall AHF Fleet Insights.
- Security Best Practices for AHF Fleet Insights
  Review the key security measures to secure the AHF Fleet Insights application, including changing default credentials, managing SSL certificates, enforcing file permissions, and ensuring Nginx FIPS compliance.

1.1 What is AHF Fleet Insights?

AHF Fleet Insights enables you to efficiently oversee and diagnose a fleet of database systems, ensuring seamless and reliable database services for users. A fleet refers to a collection of database clusters or single-instance systems.

Fleet Analytics

AHF Fleet Insights provides an aggregated view of the entire fleet based on various dimensions:

- Topology: Understand the structure of your fleet, including the type of clusters (RAC, ODA, Exadata).

- Server Configurations: Get details on server configurations, such as database versions and hardware models of database and storage servers.
- Insight Dimensions: Analyze insights gathered from different clusters, such as top events, best practice compliance issues, and operating system issues.

These analytics help in:

- Identifying and resolving issues.
- Optimizing performance.
- Improving management and security of the fleet.

Root Cause Analysis

- Observe major issues at the fleet level.
- Drill down to their respective root causes by exploring dashboards.
- Narrow down to specific insight reports as needed.

Diagnostic Data Access

To prevent data loss due to retention period constraints, AHF Fleet Insights:

- Provides a centralized system to store and retain diagnostic insights for an extended period.
- Ensures critical diagnostic information is preserved and accessible when issues arise.

1.2 Prerequisites

Review the prerequisites to install and use AHF Fleet Insights on various supported platforms.

- **Minimum recommended system resources:**
  - 4 Cores
  - 16 GB RAM
  - 4 GB disk space per registered cluster

  A dedicated server is not mandatory, but it would improve performance. Running other applications on the same server could cause interference and impact the performance.
- **Installing necessary software dependencies**
  - Java
    Go to https://www.oracle.com/in/java/technologies/downloads/ and download Java (22 or above).

    For example:

    ```
    sudo yum install https://download.oracle.com/java/23/latest/
    jdk-23_linux-x64_bin.rpm
    ```

  - Instant client and SQL*Plus
    Go to https://www.oracle.com/in/database/technologies/instant-client/linux-x86-64-downloads.html and download the latest version of Basic and SQL*Plus packages for your operating system.

For example if you are running Oracle Linux 8:

```
sudo yum install https://download.oracle.com/otn_software/linux/
instantclient/2340000/oracle-instantclient-
basic-23.4.0.24.05-1.el8.x86_64.rpm
```

```
sudo yum install https://download.oracle.com/otn_software/linux/
instantclient/2340000/oracle-instantclient-
sqlplus-23.4.0.24.05-1.el8.x86_64.rpm
```

For example if you are running Oracle Linux 7:

```
sudo yum install https://download.oracle.com/otn_software/linux/
instantclient/2114000/oracle-instantclient-
basic-21.14.0.0.0-1.x86_64.rpm
```

```
sudo yum install https://download.oracle.com/otn_software/linux/
instantclient/2114000/oracle-instantclient-
sqlplus-21.14.0.0.0-1.x86_64.rpm
```

- **Additional mandatory software dependencies**

> **Note**
>
> Ensure that the following packages are included in your environment, as they are crucial for a successful installation and the smooth operation of the application.

  - `sudo yum install cronie`

    The command `sudo yum install cronie` installs the `Cronie` package, which provides the `cron` daemon on Linux. This daemon allows users to schedule automated tasks, or "`cron jobs`," to run at specified times, useful for routine maintenance, backups, and other recurring tasks.

  - `sudo yum install iproute`

    The command `sudo yum install iproute` installs the `iproute` package on Linux, which provides network management tools like `ip`. These tools are used to configure and control networking features such as IP addresses, routes, network interfaces, and traffic control, essential for network setup and troubleshooting.

  - `sudo yum install hostname`

    The command `sudo yum install hostname` installs the `hostname` package on Linux, which provides tools to view and set the system's hostname. This is essential for identifying the machine on a network, configuring network settings, and managing server or device names.

- **Fleet Insights Database Schema Owner:**

Create a database user dedicated for AHF Fleet Insights using the `create_db_user.sql` script. This script is included in the installer zip file. The default user name is `AHFFI`. Replace the password placeholder in the script with the actual password you want to set and grant the appropriate privileges.

```
CREATE USER AHFFI IDENTIFIED BY <password> DEFAULT TABLESPACE <tablespace>;
GRANT CREATE SESSION TO AHFFI;
GRANT CONNECT, RESOURCE TO AHFFI;
GRANT CREATE TABLE TO AHFFI;
GRANT INSERT ANY TABLE TO AHFFI;
alter user AHFFI quota unlimited on <tablespace>;
```

For more information about updating the password, refer to ahffi.

- **Database connection string:**
  A valid database connection string to connect to Oracle Database (minimum version 19c).
- **Nginx server port:**
  The Nginx server is used to serve the application, and its port is configured during the AHF Fleet Insights installation. The application will run on the port you specify within the range of 1024 to 49151.

> **Note**
>
> If Oracle AI Database 26ai is used as the infrastructure repository database, then it does not require an additional license. For more information, see Special License Rights in the Oracle Database Licensing Information User Manual. Oracle AI Database 26ai can be downloaded from https://www.oracle.com/uk/database/free/

1.3 Users and Privileges

Review the list of users and their privileges.

- **Fleet Admin:** Responsible for managing the fleet of database systems.
- **DBA:** Responsible for maintaining, troubleshooting, and fixing a specific set of database clusters of the fleet.
- **INSTALL_USER:** Any Linux non-root user can install the application.

> **Note**
>
> `sudo` privileges are not required for this user to install the application. The installer will fail if run with `root` privileges.

- **User interface users:**
  - **Admin user:** A default user interface admin user `fleet_admin` is created while installing the application. This user will have access to all data across the fleet.
  - **Cluster manager:** Access is restricted to the data collected from the clusters assigned to the user.
- **Generic Client Registration User:** This user is required for registering client clusters for uploading Oracle Trace File Analyzer / Oracle Exachk / Oracle Orachk collections.

1.4 Supported Platforms

Review the list of supported platforms.

AHF Fleet Insights is supported on the following operating systems:

- Oracle Enterprise Linux (OEL)
- Red Hat Enterprise Linux (RHEL 8 or above)
- Supported architecture: x86_64

1.5 Recommended Browsers

Review the list of recommended browsers.

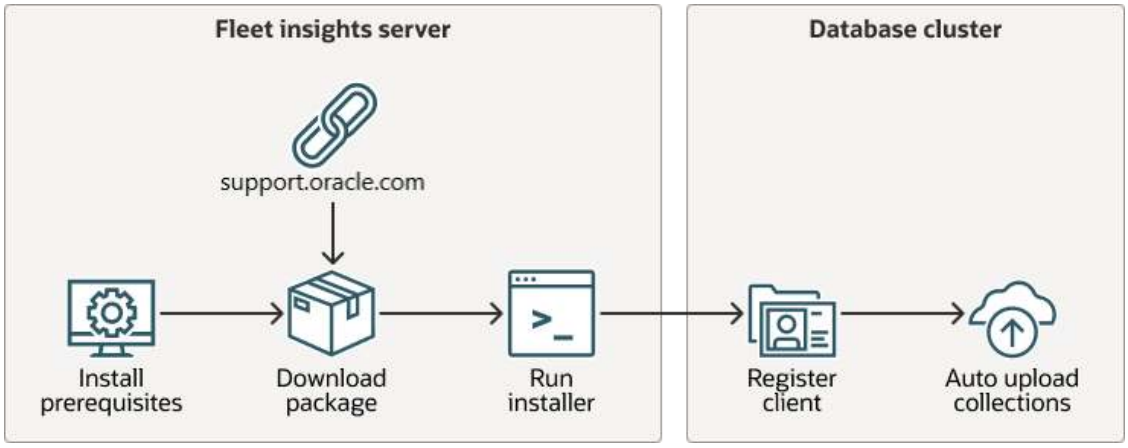
The reports are rendered best in the newest and last 5 prior versions of the following browsers:

- Microsoft Internet Explorer (latest, latest minus 5)
- Microsoft Edge (latest, latest minus 5)
- Google Chrome (latest, latest minus 5)
- Mozilla Firefox (latest, latest minus 5)
- Apple Safari (latest, latest minus 5)

1.6 Deploy AHF Fleet Insights

Learn to deploy AHF Fleet Insights.

Figure 1-1 AHF Fleet Insights deployment process



Deploying AHF Fleet Insights involves the following steps:

1. Install all the Prerequisites.
2. Download the AHF Fleet Insights package `AHFFI-LINUX_v25.2.0.zip`.
3. Run the AHF Fleet Insights installer `ahf_fleet_setup`.

4. Register client clusters to the AHF Fleet Insights server.
5. Set up automatic collection upload from the registered clusters to the AHF Fleet Insights server.

- Install and Patch AHF Fleet Insights
  Learn to install and patch AHF Fleet Insights on various supported platforms.
- Create Generic Registration User
  To create a generic registration user if it was not created during installation, follow these steps:
- Register Client Clusters to AHF Fleet Insights Server
  To automatically upload Oracle Exachk, Oracle Orachk, and Oracle Trace File Analyzer collections to the AHF Fleet Insights server, register AHF client clusters with the AHF Fleet Insights server. AHF Fleet Insights then processes these data collections to provide an organized and insightful summary.
- Deregister Client Clusters from AHF Fleet Insights Server
  Deregister AHF client clusters from the AHF Fleet Insights server to prevent them from automatically uploading Oracle Exachk, Oracle Orachk, and Oracle Trace File Analyzer collections.

1.6.1 Install and Patch AHF Fleet Insights

Learn to install and patch AHF Fleet Insights on various supported platforms.

> **Note**
>
> - Any Linux non-root user can install AHF Fleet Insights.
> - A self-signed SSL certificate (**Key type**: RSA, **key length**: 4096) is dynamically created during install time for securing HTTPS connection.
>   You have an option to substitute the default certificate with your own through the command-line interface. For more information, see ahffi.
> - The default port for installation is 5005, unless specified by the user. The valid port range is 1024 to 49151. If the specified port is not available, the AHF Fleet Insights application will fail to install.

1. Download AHF Fleet Insights binary `AHFFI-LINUX_v25.2.0.zip` from My Oracle Support note 3043060.1.
2. Unzip `AHFFI-LINUX_v25.2.0.zip`.

   ```
   unzip AHFFI-LINUX_v25.2.0.zip
   ```

   Find the following files in the unzipped directory.

   - `README.txt`: Contains commands to validate the binary, setup prerequisites, and install Fleet Insights application.
   - `ahf_fleet_setup_onprem.dat`, `oracle-ahffi.pub`: Files to verify the digital signature of the binary.
   - `ahf_fleet_setup_onprem.zip`: Installer zip.
3. Validate the installer binary using the command mentioned in the `README.txt` file.

4. Unzip `ahf_fleet_setup_onprem.zip`.
   Find the following files in the unzipped directory.
   - `ahf_fleet_setup`: Installer binary.
   - `connectstring.txt`: A template for the database connection string. You can modify this file as needed and pass it as an argument during installation.
   - `create_db_user.sql`: This SQL script creates a new database user (with a default username of AHFFI) and grants the necessary privileges. The user is required to replace the password placeholder with a secure password.
   - `properties.txt`: A template for configuration properties. You can modify this file and pass it as an argument during installation when using the `-quiet` mode.
   - `version.json`: Contains version info. DO NOT edit this file.
   - `installer_utils.sh`: Utility file for the installer. DO NOT edit this file.
5. During installation, you will be prompted to enable or disable ClamAV, open-source antivirus engine used for detecting trojans, viruses, malware, and other malicious threats to sanitize collections. Download ClamAV from https://www.clamav.net/ and set it up.

   > **⚠ Caution**
   >
   > Enabling ClamAV is optional, but doing so will result in increased processing time.

6. To install AHF Fleet Insights, run:

   ```
   ./ahf_fleet_setup -loc <install loc>
   ```

   > **ⓘ Note**
   >
   > By default, the AHFFI installer uses `/tmp` as the staging location during installation. If you prefer to use a different location, you can set the `AHFFI_TMP_DIR` environment variable to the desired path before running the installer.

7. To install AHF Fleet Insights in quiet mode with the property file, run:

   ```
   ./ahf_fleet_setup -quiet <properties file>
   ```

8. To patch AHF Fleet Insights, run:

   ```
   ./ahf_fleet_setup
   ```

For more information about install options, see ahf_fleet_setup.

Properties

Mandatory properties

- `INSTALL_DIR/<install loc>`: Installation directory must be present and accessible by the install user.
- `DB_HOST`: Database hostname.
- `DB_PORT`: Database port.

- `DB_SERVICE`: Database service name.
- `DB_USER`: Database username.
- `DB_PASSWORD`: Database password.
- `INSTANT_CLIENT`: Path to instant client.
- `JAVA_HOME`: Path to Java home.

Optional properties

- `WEBAPP_PORT`: The port on which the application will run (must be within the range of 1024 - 49151). This port must be open to allow the AHF Client to register successfully.
- `DB_WALLET`: DB wallet path if the connection requires it.
- `GENERIC_REGISTRATION_USER`: The API admin username (can be created from the unified command-line interface as well).
- `GENERIC_REGISTRATION_PASSWORD`: The API admin user password. The API admin user password. It must be at least 8 characters long and include at least one numeric digit, one special character, and one uppercase letter.
- `CLAMSCAN`: Path to `clamscan`. If mentioned, collections will be scanned for infected files. Note that scanning for infected files would increase the collection processing time.

> **Note**
>
> - If both `GENERIC_REGISTRATION_USER` and `GENERIC_REGISTRATION_PASSWORD` are provided, the generic registration user will be created automatically at the end of a successful installation.
> - Sensitive data like passwords are removed from the properties file and other files once installation is successfully completed.

Example 1-1 Property file

```
# Mandatory
INSTALL_DIR=/scratch/ahfs_local/install_test
DB_HOST=<your hostname.domainname>
DB_PORT=1555
DB_SERVICE=<your DB service URL>
DB_USER=ahffi_testuser
DB_PASSWORD=*******
INSTANT_CLIENT=/usr/lib/oracle/23/client64
JAVA_HOME=/usr/lib/jvm/jdk-23.0.2-oracle-x64

# Optional
WEBAPP_PORT=5000
DB_WALLET=
GENERIC_REGISTRATION_USER=
GENERIC_REGISTRATION_PASSWORD=
CLAMSCAN=
```

1.6.2 Create Generic Registration User

To create a generic registration user if it was not created during installation, follow these steps:

> **Note**
>
> The generic registration user can be created either during installation or after the installation is complete.

To create a generic registration user, follow these steps:

1. Navigate to the AHF installation directory:

   ```
   cd <install_dir>
   ```

   Replace *<install_dir>* with the actual AHF installation path.
2. Run the following command to create the user:

   ```
   ./ahffi create-generic-user <user name>
   ```

   Replace *<username>* with the desired generic user name.

Enter the password when prompted.

> **Note**
>
> The password must be at least 8 characters long and include at least one numeric digit, one special character, and one uppercase letter.

Example 1-2 Registration user

```
./ahffi create-generic-user admin
Generic registration password:
Enter generic registration password again
Generic registration password:

Generic registration user admin created
```

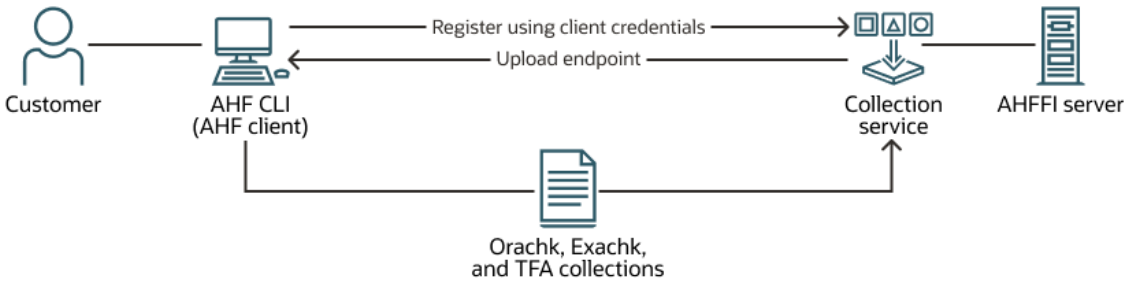
Related Topics

- ahffi
  Use the `ahffi` command to manage AHF Fleet Insights.

1.6.3 Register Client Clusters to AHF Fleet Insights Server

To automatically upload Oracle Exachk, Oracle Orachk, and Oracle Trace File Analyzer collections to the AHF Fleet Insights server, register AHF client clusters with the AHF Fleet Insights server. AHF Fleet Insights then processes these data collections to provide an organized and insightful summary.

Figure 1-2 Register AHFFI Clients



> **Note**
>
> - Ensure that the port where AHF Fleet Insights is set up on the server is open, allowing the AHF client to register successfully.
> - AHF Fleet Insights web application port must be exposed and accessible by the AHF Client system.
> - AHF Client must be running AHF 24.9 or above.
> - AHF Client must be running on a cluster.
> - If you are a Platinum customer and AHF collections/data are being uploaded to the Platinum Gateway, please do not change the upload configurations for the Platinum user.
> - To upload results to AHF Fleet Insights, you can configure the upload as the root user. AHF is capable of uploading data to multiple endpoints.

1. To fetch the registration command, run `ahffi info` from the install directory:

   ```
   ./ahffi info
   Application URL : https://demo.oracle.system.com:5000/ahfservice
   Registration command : ahf configuration set --type fleet-insights --user-
   name <generic_registration_user> --url https://demo.oracle.system.com:5000
   ```

   To create generic registration user, see Create Generic Registration User.

2. To register client clusters to AHF Fleet Insights server tool, run the registration command as `root` on the AHF Client:

   ```
   ahf configuration set --type fleet-insights --user-name
   <generic_registration_user> --url https://demo.oracle.system.com:5000
   ```

   > **Note**
   >
   > Replace the registration user name placeholder.

After successful registration, registered client clusters will automatically upload collections to AHF Fleet Insights. Oracle Trace File Analyzer collections with Insights can also be accessed directly from the AHF Fleet Insights web interface.

1.6.4 Deregister Client Clusters from AHF Fleet Insights Server

Deregister AHF client clusters from the AHF Fleet Insights server to prevent them from automatically uploading Oracle Exachk, Oracle Orachk, and Oracle Trace File Analyzer collections.

1. To deregister a client cluster from the AHF Fleet Insights server, run the following command with `root` privileges on the AHF Client.

```
ahf configuration unset --type fleet-insights
Successfully deregistered.
```

1.7 Import SSL Certificates

To import and use custom-SSL certificates other than the default one created during installation, use this procedure.

> **Note**
>
> A self-signed SSL certificate (**Key type:** RSA, **key length:** 4096) is dynamically created during install time for securing HTTPS connection.
> You have an option to substitute the default certificate with your own through the command-line interface. For more information, see ahffi.

To import SSL certificates, run:

```
./ahffi importcert -cert <cert file> -key <key file>
```

The application restarts automatically after you import custom SSL certificates.

Example 1-3 Import SSL certificates

```
./ahffi importcert -cert /scratch/certs/ahf.crt -key /scratch/certs/ahf.key
2023-08-14 09:44:18 UTC: [testnode] [2832363] [UPDATE_PROPERTIES] [INFO] Path
to the input properties file provided as : /scratch/ahfs_local/install_test/
ahf_service.properties.1692006258
2023-08-14 09:44:22 UTC: [testnode] [2832363] [UPDATE_PROPERTIES] [INFO]
nginx: the configuration file /scratch/ahfs_local/install_test/ahf_service/
third_party/nginx/conf/ahfs_nginx_with_ssl.conf syntax is ok
2023-08-14 09:44:22 UTC: [testnode] [2832363] [UPDATE_PROPERTIES] [INFO]
nginx: configuration file /scratch/ahfs_local/install_test/ahf_service/
third_party/nginx/conf/ahfs_nginx_with_ssl.conf test is successful
Restarting the application...
2023-08-14 09:44:23 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Component
chosen as all
2023-08-14 09:44:23 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Action
chosen as restart
2023-08-14 09:44:23 UTC: [testnode] [2833231] [MANAGE_APP] [INFO]
Successfully removed job(s) for all from crontab
2023-08-14 09:44:28 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Killed the
existing Fleet Insights processes
```

```
2023-08-14 09:44:32 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Killed the
existing collection processing engine processes
2023-08-14 09:44:33 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Killed the
existing ahf_service processes for component(s): all.
2023-08-14 09:44:33 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Starting
Fleet Insights
2023-08-14 09:44:37 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Started
Fleet Insights successfully
2023-08-14 09:44:37 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] The path to
manage_app.log is /scratch/ahfs_local/install_test/ahf_service/log/
manage_app.log
2023-08-14 09:44:37 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] The path to
nginx access.log is /scratch/ahfs_local/install_test/ahf_service/third_party/
nginx/logs/access.log
2023-08-14 09:44:37 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Starting
the collection processing engine
2023-08-14 09:44:38 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Collection
processing engine is running
2023-08-14 09:44:38 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Started the
collection processing engine successfully
2023-08-14 09:44:38 UTC: [testnode] [2833231] [MANAGE_APP] [INFO]
Successfully added job(s) for all from crontab
2023-08-14 09:44:38 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Started the
ahf_service processes for component(s): all.
Successfully imported the certificates
```

1.8 Update Properties

To update a property or a set of properties, use this procedure.

> **Note**
>
> You might need to restart the application for some updates to take effect.

To update a property, run:

```
./ahffi updateproperty -k <key> -v <value>
```

Set of keys that can updated:

- DB_HOST=
- DB_PORT=
- DB_SERVICE=
- DB_USER=
- DB_PASSWORD=
- WEBAPP_PORT=
- DB_WALLET=
- INSTANT_CLIENT=<*path*>
- JAVA_HOME= <*path*>

- CLAMSCAN= <*path to clamscan folder*>
- LOG_RETENTION
  The number of days a log file will be retained after its last edited date.
- MAX_COLLECTION_DIR_SIZE
  Maximum size (GB) for the collections directory. If exceeded, old collections will be deleted.
- CLIENT_KEY_EXPIRY_IN_DAYS
  Client needs to reset password after this (in days) expiry.
- GRACE_PERIOD_IN_DAYS
  Client must reset password before the grace period (in days) ends after expiry to avoid getting deregistered.
- COLLECTION_UPLOAD_LIMIT
  Total collection(s) size (GB) that can be uploaded in an hour.

To update a set of properties, run:

```
./ahffi updateproperty -p <property file>
```

Add a list of properties you want to update to a text file and then use that text file to update the properties.

For example:

```
DB_HOST="<your hostname.domainname>"
DB_PORT="1555"
DB_SERVICE="<your DB service URL>"
DB_USER="ahffi_testuser"
DB_PASSWORD="*******"
JAVA_HOME="/usr/lib/jvm/java-11-openjdk-11.0.19.0.7-4.0.1.el8.x86_64"
INSTANT_CLIENT="/usr/lib/oracle/21/client64"
```

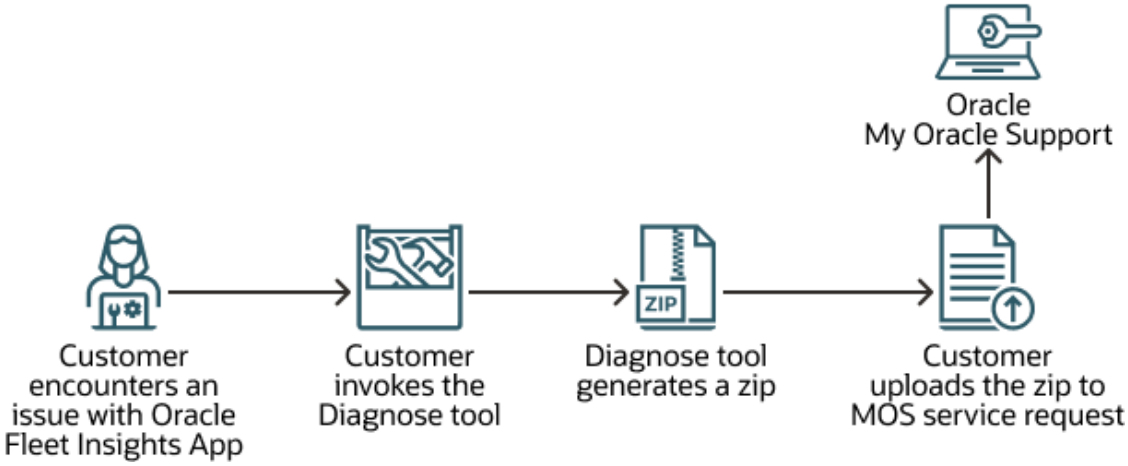
Related Topics

- Install and Patch AHF Fleet Insights
  Learn to install and patch AHF Fleet Insights on various supported platforms.
- ahf_fleet_setup
  Use the `ahf_fleet_setup` command to install or patch AHF Fleet Insights.

1.9 Diagnose AHF Fleet Insights

The diagnose tool helps you collect diagnostic data on-demand to debug and maintain AHF Fleet Insights.

Figure 1-3 Diagnose AHF Fleet Insights



This diagnostic data includes:

- Application logs
- Processing engine logs
- Operating system related details (disk space, #process, and so on)
- Nginx configuration file and logs
- Source environment and properties file
- Plugin logs
- Individual processing stage logs

You can run the diagnostic component through the command-line interface.

- `./ahffi diagnose`

  Collects application logs and packages them into a ZIP file that can be used to diagnose issues in the Fleet Insights application.

- `./ahffi diagnose --collection <collection_id>`

  In addition to the standard application logs, this command includes collection-specific logs —those generated while processing the specified collection.

1.10 Uninstall AHF Fleet Insights

Learn to uninstall AHF Fleet Insights.

Uninstall options:

- `-q`: Uninstalls the application in [q]uiet mode (no prompts, default options are to keep backup).
- `-qc`: Uninstalls the application in [q]uiet mode and [c]leanup all AHF Fleet Insights related files and database entries in quite mode.

- `-qb`: Uninstalls the application in [q]uiet mode and keep a [b]ackup in the database

If you run `./ahffi uninstall` without any options, you will be prompted to enter the following:

```
clean DB object [y/n]
retain backup [y/n]


./ahffi uninstall -qc
Uninstalling AHF service in quiet mode
Database objects will be cleaned as part of this uninstallation
No install directory, considering /scratch/ahfs_local/install_test as the
install directory
Removing installation from /scratch/ahfs_local/install_test/
2023-08-14 10:07:10 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Uninstalling AHF Service
2023-08-14 10:07:10 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Cleaning AHF Service database objects

SQL*Plus: Release 21.0.0.0.0 - Production on Mon Aug 14 10:07:10 2023
Version 21.10.0.0.0

Copyright (c) 1982, 2022, Oracle.  All rights reserved.

Last Successful login time: Mon Aug 14 2023 10:07:10 +00:00

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.17.0.0.0

SQL>   2    3    4    5    6    7    8    9   10   11   12   13   14   15
16   17   18   19   20   21   22   23   24   25   26   27   28   29   30
31   32   33   34
PL/SQL procedure successfully completed.

SQL> Disconnected from Oracle Database 19c Enterprise Edition Release
19.0.0.0.0 - Production
Version 19.17.0.0.0
2023-08-14 10:07:13 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Stopping all running ahfs processes
2023-08-14 10:07:14 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Component
chosen as all
2023-08-14 10:07:14 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Action
chosen as stop
2023-08-14 10:07:14 UTC: [testnode] [3015554] [MANAGE_APP] [INFO]
Successfully removed job(s) for all from crontab
2023-08-14 10:07:20 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Killed the
existing Fleet Insights processes
2023-08-14 10:07:23 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Killed the
existing collection processing engine processes
2023-08-14 10:07:24 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Killed the
existing ahf_service processes for component(s): all.
2023-08-14 10:07:24 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Removing AHF Service backup files
2023-08-14 10:07:24 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Deleting AHF Service application files
```

```
Completing  AHF Service uninstallation
2023-08-14 10:07:26 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Successfully uninstalled AHF service
Successfully uninstalled application
```

Related Topics

- ahf_fleet_setup
  Use the `ahf_fleet_setup` command to install or patch AHF Fleet Insights.
- ahffi
  Use the `ahffi` command to manage AHF Fleet Insights.

1.11 Security Best Practices for AHF Fleet Insights

Review the key security measures to secure the AHF Fleet Insights application, including changing default credentials, managing SSL certificates, enforcing file permissions, and ensuring Nginx FIPS compliance.

Change default user credentials

During installation, a user account is created with a default username and password. Upon first login, the application requires the admin user to change the credentials. The application enforces this password change to secure the UI admin account.

Replace SSL certificates

You can replace expired SSL certificates or use your own custom SSL certificates for the application. The unified CLI offers a simple way to do this using the `importcert` command, allowing you to update certificates seamlessly when needed. For more information, see Import SSL Certificates.

File permissions

All AHF Fleet Insights application files and directories are restricted to the necessary user group, typically just the install user. Files containing credentials are further secured by being set to read-only, ensuring that sensitive information remains protected.

Nginx configuration

Nginx is configured to allow only FIPS-compliant ciphers as listed on NGINX FIPS Compliance. This configuration is enabled by default, so no additional setup is required.

Passwords

Passwords are not stored in any installation files; they are encrypted and removed from the properties and other files once the installation is successfully completed.

Command-Line Interface (CLI)

Only the installation user can run the CLI commands.

2

Command Line Reference

2.1 ahf_fleet_setup

Use the `ahf_fleet_setup` command to install or patch AHF Fleet Insights.

Syntax

```
ahf_fleet_setup [OPTIONS]
```

Option	Description
`-h, --help`	Prints this help message and exits.
`-loc <path>`	Specifies the installation path (not needed for patching).
`-connect_string <file>`	(optional) Specifies DB connection string as a text file.
`-db_wallet_path <path>`	(optional) Specifies DB wallet path.
`-quiet [<property file>]`	Proceeds with installation/patching in quiet mode.

Example 2-1 Connect string

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=*****.<host name>.<domain name>)
(PORT=1**5))(CONNECT_DATA=(SERVICE_NAME=*****.<host name>.<domain name>)))
```

Example 2-2 Installation

```
./ahf_fleet_setup -loc <install location>
```

```
./ahf_fleet_setup -loc <install location> -connect_string <connect string file>
```

```
./ahf_fleet_setup -loc <install location> -db_wallet_path <db wallet path>
```

```
./ahf_fleet_setup -loc <install location> -db_wallet_path <db wallet path> -connect_string <connect string file>
```

```
./ahf_fleet_setup -quiet <properties file>
```

Example 2-3 Patching

```
./ahf_fleet_setup
```

```
./ahf_fleet_setup -quiet
```

```
./ahf_fleet_setup -quiet <properties file>
```

Not something the user would typically run. Only use case is for when a new version introduces a property that requires user to provide a value.

2.2 ahffi

Use the `ahffi` command to manage AHF Fleet Insights.

A binary with the name `ahffi` will be available in the install location once Fleet Insights installation is successful.

Syntax

```
ahffi [OPTIONS]
```

Option	Description
`-h`, `--help`	Prints this help message and exits.
`version`	Prints application version info.
`start`	Starts all Fleet Insight processes.
`stop`	Stops all Fleet Insight processes.
`restart`	Restarts all Fleet Insight processes.
`status`	Gets the running status of Fleet Insight processes.

Option	Description
`info`	Prints the app URL and command used to register clients.
`diagnose`	Runs `ahffi` diagnostics.
`create-generic-user <username>`	Creates generic registration user.
`uninstall [-q] [-c] [-b]`	Uninstalls Fleet Insights application. • `-q`: Uninstall the application in [q]uiet mode (no prompts, default options are to keep backup) • `-c`: [c]leanup all AHF Fleet Insights related files and database entries in quite mode • `-b`: keep a [b]ackup in the database Upon successful run, the uninstaller: • Uninstalls the application. • Deletes the metadata file `~/.ahffi` that contains the install location info.
`update-password {db_user|registration_user}`	Updates password for the specified user.
`updateproperty -k <key> -v <value>`	Updates a single application property.
`updateproperty -p <propery file>`	Updates application properties as read from a specified text file.
`importcert -cert <cert file> -key <key file>`	Use this command option to import your own SSL certificates for running the application instead of using the default certificates. Upon successful run: • Imported certificate is copied to the `ahf_install_loc/ahf_service/certs/` directory. • If the certificate already exists, the existing certificate is backed up with `.default` extension. • The `ahf_install_loc/ahf_service/third_party/nginx/conf/ahfs_nginx_with_ssl.conf` file must have correct configuration for certificates. • Application is automatically restarted.
`import-diagnostics [args]`	Use this option to import and process diagnostic files manually. • `-t`: [t]arget • `-c`: [c]ollection • `-f`: diagnostic zip [f]ile • `-u`: generic [u]sername `ahffi import-diagnostics [-t|--target <target>] [-f|--file <zip_file>] [-u|--user <username>] [-c|--collection <collection_name>]` Where: `-target`, `-file`, and `-user` are required parameters.

Example 2-4 ahffi restart

```
./ahffi restart
2023-06-26 17:54:11 UTC: [testnode] [180200] [MANAGE_APP] [INFO] The
specified component flag: restart is not valid, using the default value 'all'
2023-06-26 17:54:11 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Component
chosen as all
2023-06-26 17:54:11 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Action
chosen as restart
None of the queried jobs are present in crontab
2023-06-26 17:54:12 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Successfully
removed job(s) for all from crontab
2023-06-26 17:54:17 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Killed the
existing Fleet Insights processes
2023-06-26 17:54:20 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Killed the
existing collection processing engine processes
2023-06-26 17:54:21 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Killed the
existing ahf_service processes for componet(s): all.
2023-06-26 17:54:21 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Starting
Fleet Insights
2023-06-26 17:54:22 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Started
Fleet Insights successfully
2023-06-26 17:54:22 UTC: [testnode] [180200] [MANAGE_APP] [INFO] The path to
manage_app.log is /scratch/ahfs_local/install_test/ahf_service/log/
manage_app.log
2023-06-26 17:54:23 UTC: [testnode] [180200] [MANAGE_APP] [INFO] The path to
nginx access.log is /scratch/ahfs_local/install_test/ahf_service/third_party/
nginx/logs/access.log
2023-06-26 17:54:23 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Starting the
collection processing engine
2023-06-26 17:54:24 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Collection
processing engine is running
2023-06-26 17:54:24 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Started the
collection processing engine successfully
All jobs are present in crontab
2023-06-26 17:54:25 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Successfully
added job(s) for all from crontab
2023-06-26 17:54:25 UTC: [testnode] [180200] [MANAGE_APP] [INFO] Started the
ahf_service processes for componet(s): all.
```

Example 2-5 ahffi status

```
./ahffi status
2023-06-26 18:11:13 UTC: [testnode] [313565] [MANAGE_APP] [INFO] The
specified component flag: status is not valid, using the default value 'all'
2023-06-26 18:11:13 UTC: [testnode] [313565] [MANAGE_APP] [INFO] Component
chosen as all
2023-06-26 18:11:13 UTC: [testnode] [313565] [MANAGE_APP] [INFO] Action
chosen as status
2023-06-26 18:11:14 UTC: [testnode] [313565] [MANAGE_APP] [INFO] Fleet
Insights is running
2023-06-26 18:11:14 UTC: [testnode] [313565] [MANAGE_APP] [INFO] Collection
processing engine is running
2023-06-26 18:11:14 UTC: [testnode] [313565] [MANAGE_APP] [INFO] Container
Manager isn't enabled in this install
```

```
2023-06-26 18:11:14 UTC: [testnode] [313565] [] [INFO] All AHF Service
processes for componet(s): all are running.
```

Example 2-6 ahffi info

```
./ahffi info
Application URL : https://demo.oracle.system.com:5000/ahfservice
Registration command : ahf configuration set --type fleet-insights --user-
name <registration_user> --url https://demo.oracle.system.com:5000
```

Example 2-7 ahffi diagnose

```
./ahffi diagnose
Running diagnose tool
  adding: testnode.06-26-2023-18-25-33-UTC.ahffi_logs/ (stored 0%)
  adding: testnode.06-26-2023-18-25-33-UTC.ahffi_logs/ahffi_log_files.txt
(deflated 85%)
  adding: testnode.06-26-2023-18-25-33-UTC.ahffi_logs/os_detail_file.txt
(deflated 78%)
  adding: testnode.06-26-2023-18-25-33-UTC.ahffi_logs/wallet_utils.err
(deflated 95%)
...
...
...
  adding: testnode.06-26-2023-18-25-33-UTC.ahffi_logs/consumer_daemon.log.1
(deflated 96%)
  adding: testnode.06-26-2023-18-25-33-UTC.ahffi_logs/consumer_daemon.log
(deflated 96%)
/scratch/ahfs_local/install_test
DIAGNOSE_AHFFI ran successfully
Diagnostic info can be found at /scratch/ahfs_local/collections/collections/
testnode.06-26-2023-18-25-33-UTC.ahffi_logs.zip
```

Example 2-8 ahffi create-generic-user

```
./ahffi create-generic-user admin
Generic registration password:
Enter generic registration password again
Generic registration password:

Generic registration user admin created
```

Example 2-9 ahffi importcert

```
./ahffi importcert -cert /scratch/certs/ahf.crt -key /scratch/certs/ahf.key
2023-08-14 09:44:18 UTC: [testnode] [2832363] [UPDATE_PROPERTIES] [INFO] Path
to the input properties file provided as : /scratch/ahfs_local/install_test/
ahf_service.properties.1692006258
2023-08-14 09:44:22 UTC: [testnode] [2832363] [UPDATE_PROPERTIES] [INFO]
nginx: the configuration file /scratch/ahfs_local/install_test/ahf_service/
third_party/nginx/conf/ahfs_nginx_with_ssl.conf syntax is ok
2023-08-14 09:44:22 UTC: [testnode] [2832363] [UPDATE_PROPERTIES] [INFO]
nginx: configuration file /scratch/ahfs_local/install_test/ahf_service/
```

```
third_party/nginx/conf/ahfs_nginx_with_ssl.conf test is successful
Restarting the application...
2023-08-14 09:44:23 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Component
chosen as all
2023-08-14 09:44:23 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Action
chosen as restart
2023-08-14 09:44:23 UTC: [testnode] [2833231] [MANAGE_APP] [INFO]
Successfully removed job(s) for all from crontab
2023-08-14 09:44:28 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Killed the
existing Fleet Insights processes
2023-08-14 09:44:32 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Killed the
existing collection processing engine processes
2023-08-14 09:44:33 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Killed the
existing ahf_service processes for component(s): all.
2023-08-14 09:44:33 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Starting
Fleet Insights
2023-08-14 09:44:37 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Started
Fleet Insights successfully
2023-08-14 09:44:37 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] The path to
manage_app.log is /scratch/ahfs_local/install_test/ahf_service/log/
manage_app.log
2023-08-14 09:44:37 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] The path to
nginx access.log is /scratch/ahfs_local/install_test/ahf_service/third_party/
nginx/logs/access.log
2023-08-14 09:44:37 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Starting
the collection processing engine
2023-08-14 09:44:38 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Collection
processing engine is running
2023-08-14 09:44:38 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Started the
collection processing engine successfully
2023-08-14 09:44:38 UTC: [testnode] [2833231] [MANAGE_APP] [INFO]
Successfully added job(s) for all from crontab
2023-08-14 09:44:38 UTC: [testnode] [2833231] [MANAGE_APP] [INFO] Started the
ahf_service processes for component(s): all.
Successfully imported the certificates
```

Example 2-10 ahffi updateproperty

```
./ahffi updateproperty -k WEBAPP_PORT -v 5001
2023-08-14 09:58:36 UTC: [testnode] [2945846] [UPDATE_PROPERTIES] [INFO] Key
of the property to be updated: WEBAPP_PORT
2023-08-14 09:58:36 UTC: [testnode] [2945846] [UPDATE_PROPERTIES] [INFO]
Value of the property to be updated: 5001
2023-08-14 09:58:36 UTC: [testnode] [2945846] [UPDATE_PROPERTIES] [INFO]
Writing the provided key-value pair to /scratch/ahfs_local/install_test/
ahf_service.properties.1692007116
2023-08-14 09:58:39 UTC: [testnode] [2945846] [UPDATE_PROPERTIES] [INFO]
nginx: the configuration file /scratch/ahfs_local/install_test/ahf_service/
third_party/nginx/conf/ahfs_nginx_with_ssl.conf syntax is ok
2023-08-14 09:58:39 UTC: [testnode] [2945846] [UPDATE_PROPERTIES] [INFO]
nginx: configuration file /scratch/ahfs_local/install_test/ahf_service/
third_party/nginx/conf/ahfs_nginx_with_ssl.conf test is successful
```

Example 2-11 Update DB user password

> **Note**
>
> Before changing the database password, stop the Fleet Insights service.

```
./ahffi update-password db_user
Application needs to be stopped for this action.
Proceed to stop the application? [y/n]: y
2024-06-28 05:34:24 UTC: [testnode] [2746424] [MANAGE_APP] [INFO] Component
chosen as all
2024-06-28 05:34:24 UTC: [testnode] [2746424] [MANAGE_APP] [INFO] Action
chosen as stop
2024-06-28 05:34:25 UTC: [testnode] [2746424] [MANAGE_APP] [INFO]
Successfully removed job(s) for all from crontab
2024-06-28 05:34:30 UTC: [testnode] [2746424] [MANAGE_APP] [INFO] Killed the
existing Fleet Insights processes
2024-06-28 05:34:33 UTC: [testnode] [2746424] [MANAGE_APP] [INFO] Killed the
existing collection processing engine processes
2024-06-28 05:34:34 UTC: [testnode] [2746424] [MANAGE_APP] [SUCCESS] Killed
the existing ahf_service processes for component(s): all.
Please update your DB with new password and only then proceed by pressing
ENTER...
Enter new DB user password:
Enter new DB user password again:
2024-06-28 05:35:18 UTC: [testnode] [2751047] [UPDATE_PROPERTIES] [INFO] Key
of the property to be updated: DB_PASSWORD
2024-06-28 05:35:21 UTC: [testnode] [2751047] [UPDATE_PROPERTIES] [INFO]
Writing the provided key-value pair to /scratch/ahfs_local/install_test/
ahf_service.properties.1719552921
2024-06-28 05:35:32 UTC: [testnode] [2751047] [UPDATE_PROPERTIES] [INFO]
nginx: the configuration file /scratch/ahfs_local/install_test/ahf_service/
third_party/nginx/conf/ahfs_nginx_with_ssl.conf syntax is ok
2024-06-28 05:35:32 UTC: [testnode] [2751047] [UPDATE_PROPERTIES] [INFO]
nginx: configuration file /scratch/ahfs_local/install_test/ahf_service/
third_party/nginx/conf/ahfs_nginx_with_ssl.conf test is successful
DB password changed. Starting Fleet Insights...
2024-06-28 05:35:36 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] Component
chosen as all
2024-06-28 05:35:36 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] Action
chosen as start
2024-06-28 05:35:36 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] Starting
Fleet Insights
2024-06-28 05:35:41 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] Started
Fleet Insights successfully
2024-06-28 05:35:41 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] The path to
manage_app.log is /scratch/ahfs_local/install_test/ahf_service/log/
manage_app.log
2024-06-28 05:35:41 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] The path to
nginx access.log is /scratch/ahfs_local/install_test/ahf_service/third_party/
nginx/logs/access.log
2024-06-28 05:35:41 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] Starting
the collection processing engine
2024-06-28 05:35:42 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] Collection
```

```
processing engine is running
2024-06-28 05:35:43 UTC: [testnode] [2752698] [MANAGE_APP] [INFO] Started the
collection processing engine successfully
2024-06-28 05:35:44 UTC: [testnode] [2752698] [MANAGE_APP] [INFO]
Successfully added job(s) for all from crontab
2024-06-28 05:35:44 UTC: [testnode] [2752698] [MANAGE_APP] [SUCCESS] Started
the ahf_service processes for component(s): all.
```

Example 2-12 ahffi uninstall

```
./ahffi uninstall -qc
Uninstalling AHF service in quiet mode
Database objects will be cleaned as part of this uninstallation
No install directory, considering /scratch/ahfs_local/install_test as the
install directory
Removing installation from /scratch/ahfs_local/install_test/
2023-08-14 10:07:10 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Uninstalling AHF Service
2023-08-14 10:07:10 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Cleaning AHF Service database objects

SQL*Plus: Release 21.0.0.0.0 - Production on Mon Aug 14 10:07:10 2023
Version 21.10.0.0.0

Copyright (c) 1982, 2022, Oracle.  All rights reserved.

Last Successful login time: Mon Aug 14 2023 10:07:10 +00:00

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.17.0.0.0

SQL>   2    3    4    5    6    7    8    9   10   11   12   13   14   15
16   17   18   19   20   21   22   23   24   25   26   27   28   29   30
31   32   33   34
PL/SQL procedure successfully completed.

SQL> Disconnected from Oracle Database 19c Enterprise Edition Release
19.0.0.0.0 - Production
Version 19.17.0.0.0
2023-08-14 10:07:13 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Stopping all running ahfs processes
2023-08-14 10:07:14 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Component
chosen as all
2023-08-14 10:07:14 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Action
chosen as stop
2023-08-14 10:07:14 UTC: [testnode] [3015554] [MANAGE_APP] [INFO]
Successfully removed job(s) for all from crontab
2023-08-14 10:07:20 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Killed the
existing Fleet Insights processes
2023-08-14 10:07:23 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Killed the
existing collection processing engine processes
2023-08-14 10:07:24 UTC: [testnode] [3015554] [MANAGE_APP] [INFO] Killed the
existing ahf_service processes for component(s): all.
2023-08-14 10:07:24 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
```

```
Removing AHF Service backup files
2023-08-14 10:07:24 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Deleting AHF Service application files
Completing  AHF Service uninstallation
2023-08-14 10:07:26 UTC: [testnode] [3014990] [UNINSTALL_AHFS] [INFO]
Successfully uninstalled AHF service
Successfully uninstalled application
```

Example 2-13 ahffi import-diagnostics

```
./ahffi import-diagnostics -t <target> -f <collection.zip> -u
<generic_registration_user>
Enter password for generic user admin:
Trying to queue <collection.zip> for processing...
Queued <collection.zip> for processing..
```

2.3 Managing Exadata Capacity Planning Plugin

The Exadata Capacity Planning Plugin uses `systemd` units to manage the CPU and memory resources consumed by capacity plugin jobs on the Fleet server.

Enabling the Exadata Capacity Planning Plugin

To enable the plugin, run the following script from the installation directory:

```
sudo bash /<install_loc>/collection_processing_engine/util/
configure_cgroups_capacity.sh --enable
```

> **Note**
>
> Root privileges are required to grant the current AHF Linux user permission to manage `systemd` units.

Once the capacity plugin is enabled from the AHFFI server side, enable the weekly capacity collection upload from the cluster side.

Log in to the cluster(s) registered with the Fleet Server and run the following command. This command configures exachk to schedule weekly capacity collections every Sunday at 4:00 a.m.:

```
exachk -set "AUTORUN_SCHEDULE=0 4 * * 0;AUTORUN_FLAGS=-profile workload-
capacity -showpass -tag autostart_client_capacity -
readenvconfig;COLLECTION_RETENTION=2" -id autostart_client_capacity
```

This setup ensures that capacity data is automatically collected and uploaded on a weekly basis.

Default Resource Limits

When enabled with default settings, all running capacity plugin jobs collectively consume:

- 25% of total CPU resources (equivalent to 1 core on a 4-core system)

- 25% of total system memory

These limits help ensure that capacity jobs do not overwhelm the system and can be adjusted as needed.

Modifying Resource Limits

To change the default limits, use the script with the `--reset` option:

```
sudo bash /<install_loc>/collection_processing_engine/util/
configure_cgroups_capacity.sh --reset
```

Viewing Available Options

To list all available configuration options, run:

```
sudo bash /<install_loc>/collection_processing_engine/util/
configure_cgroups_capacity.sh --help
```

Option	Description
`--reset [--cpu <quota>] [--memory <limit>]`	Resets the resource limits to default or provided values (CPU: 25% per core, Memory: 25% of total RAM). **Note** The `--reset` option can only be used if resource limiting is already enabled.
`--enable [--cpu <quota>] [--memory <limit>]`	Enables the resource limits with default or provided settings.
`--disable`	Disables resource limiting and remove `polkit` permissions.
`--status`	Checks if resource limiting is currently enabled.
`-h, --help`	Prints this help message and exits.

3 AHFFI Web Interface

3.1 Get Started with AHF Fleet Insights Web Interface

AHF Fleet Insights web interface is an intuitive and user-friendly interface making it accessible for both technical and non-technical users.

Log in to the application

1. To fetch the application URL, go to the install location, and then run:

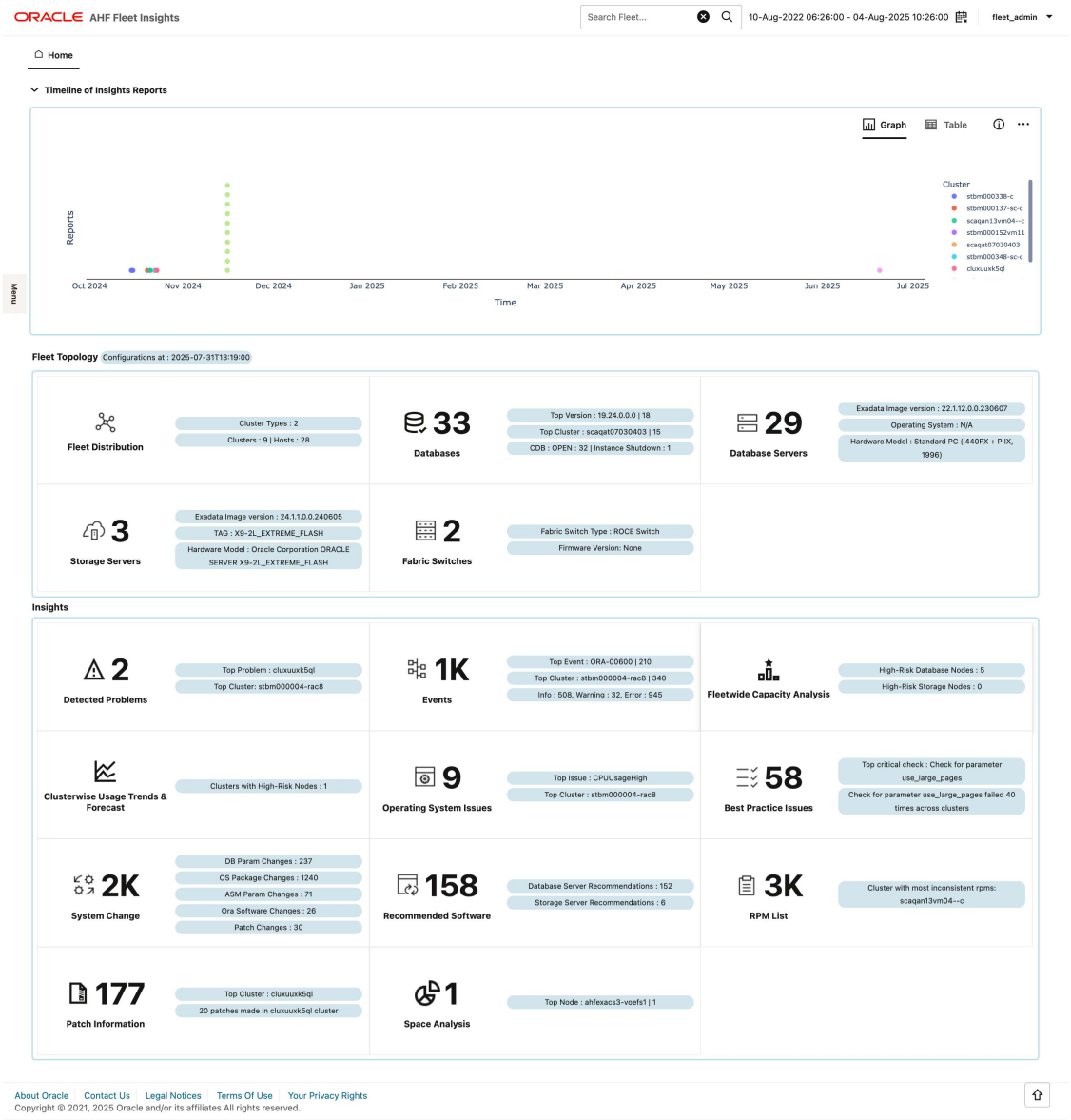
   ```
   ./ahffi info
   ```

2. Open the URL in a recommended browser.
3. Enter the fleet admin credentials in the login screen, and then click **Login**.

> **Note**
>
> - Default login credentials: `fleet_admin/welcome1`
> - During your first login, you will be prompted to update your password.

> **Note**
>
> If you're unable to view data on the dashboard after successful registration, it may be because, for AHF Fleet Insights (AHFFI), AHF collections are scheduled to run every 5th and 17th hour of the day. The corresponding cluster data will only appear in the Fleet Insights dashboard after the scheduled collection has been completed.
> Alternatively, you can trigger an on-demand collection immediately using the `tfactl diagcollect` command with the `-insights` option on the AHF client. For example:
>
> ```
> tfactl diagcollect -insights -last 4h
> ```

Figure 3-1 AHF Fleet Insights - Home



Home

- **Global search and filter**: Search and filter issues by specific cluster or system across the fleet.
- **Global time filter**: Filter issues that occurred within a specific time window.
- **Menu drawer**: Navigate between different sections of the dashboard.
- **Timeline of events**: A chronological view of Insights reports collected across the fleet.
- **Fleet topology**: Statistics for the complete fleet.
  The fleet configuration displayed reflects the current state, regardless of the selected start time.
  - **Fleet Distribution**: Aggregated statistics for the entire fleet.

  - **Databases**: Aggregated metrics and insights about all Oracle Databases deployed across the fleet.
  - **Database Servers**: Provides aggregated information about database servers across the fleet.
  - **Storage Servers**: Provides aggregated information about storage servers across the fleet.
  - **Fabric Switches**: Provides aggregated information about Network Fabric Switches across the fleet.
- **Insights**: Events occurred, Best Practice issues, operating system issues, and software recommendations.
  - **Detected Problems**: Provides detected issues across systems, with insights into causes and resolution.
  - **Events**: Provides details about the events that occurred across the fleet.
  - **Fleetwide Capacity Analysis**: Quickly view resource usage across your fleet to spot top/bottom consumers, bottlenecks, and under utilized nodes for better performance.
  - **Cluster-Wise Usage Trends & Forecast**: Track cluster-level usage trends, forecasts, and history to plan capacity and optimize resource allocation.
  - **Operating System Issues**: Provides details about the metrics collected and a detailed report on operating system anomalies.
  - **Best Practice Issues**: Provides the results of Best Practices Compliance checks across the fleet.
  - **System Changes**: Helps to track system-level changes across the fleet.
  - **Recommended Software**: Lists recommended software-supported versions.
  - **RPM List**: Lists installed RPMs and compare clusters for differences in software packages.
  - **Patch Information**: Provides recommended patches and highlighting systems running outdated database versions.
  - **Space Analysis**: Helps to monitor space utilization across the fleet and identify systems nearing capacity.

3.2 Tasks You Can Perform Using AHF Fleet Insights Web Interface

The use cases are not limited to the ones listed in this section.

- Home
- Fleet Topology
- Insights
- Admin
- File Viewer
- Common User Interface Functionalities

3.2.1 Home

- Keep track of all the Insights reports collected across the fleet
- View the aggregate statistics of a fleet at a glance
- Filter cluster-specific or system-specific issues
- Filter issues that happened during a specific time window
- Move from aggregations to specific Insights report and diagnostic collections

3.2.1.1 Keep track of all the Insights reports collected across the fleet

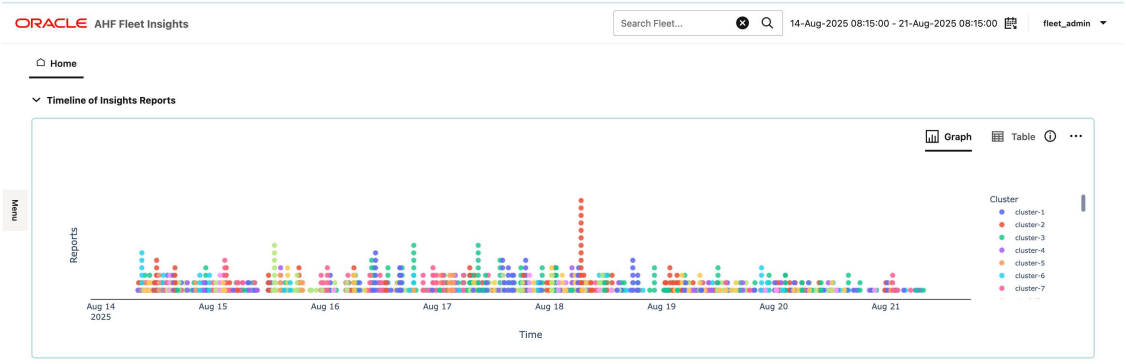
Maintain visibility into the collection and frequency of Insights reports across all clusters in your fleet.

Purpose:

- **View Report Timelines:** Monitor when reports are generated for individual clusters to understand activity patterns.
- **Monitor Report Frequency:** Track how often each cluster generates Insights reports to assess system behavior.
- **Identify Report Bursts:** Detect sudden spikes in report generation, which may point to recurring or urgent issues.
- **Analyze Noise Levels:** Spot clusters producing excessive or frequent reports, helping identify noisy systems or misconfigurations.

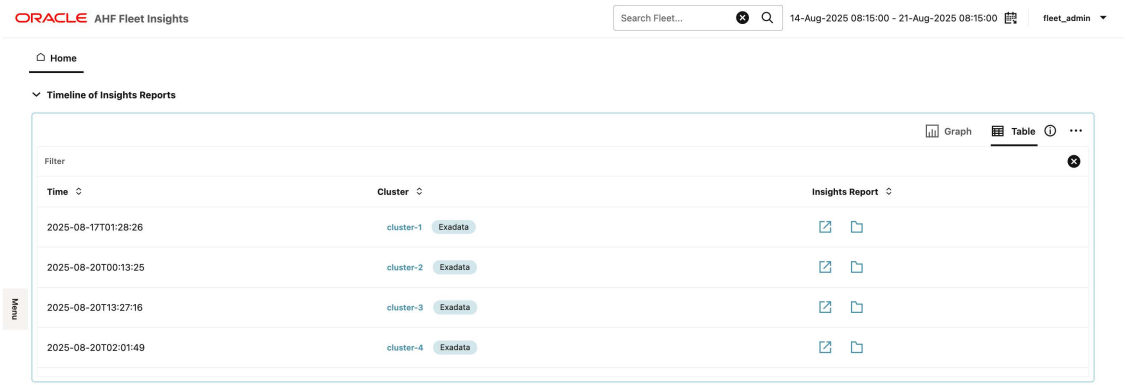
The plot displays the insights reports uploaded from monitored clusters over the selected time period.

Figure 3-2 Timeline of Events - Graph



Click a scatter point to access the corresponding insights report

Figure 3-3 Timeline of Events - Table



1. Click the name of the cluster to view cluster summary and collection details.
2. Click the file viewer to view files in a collection.

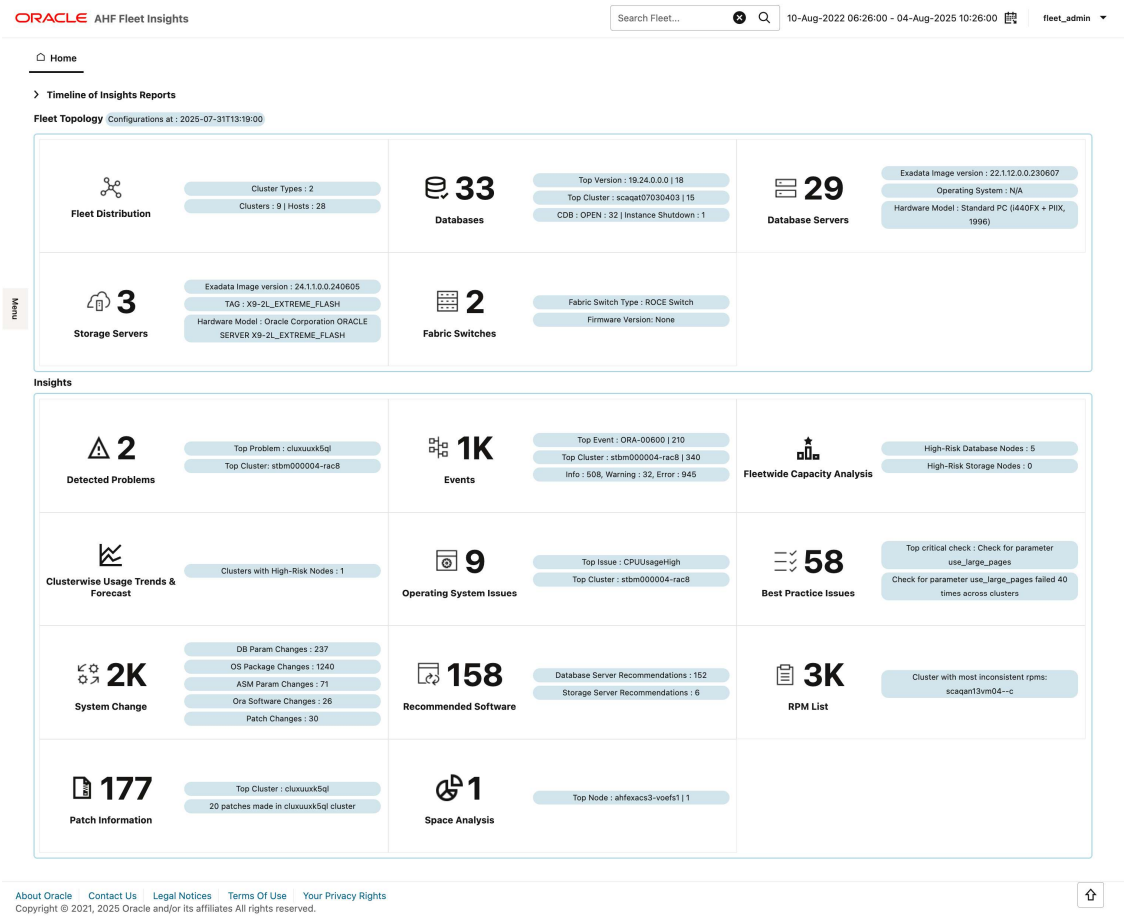
3.2.1.2 View the aggregate statistics of a fleet at a glance

Get a high-level overview of your entire fleet's health and performance from the Home page.

Purpose:

- **Overview of Key Metrics:** Quickly access critical statistics across the entire fleet to assess overall system health.
- **Identify Key Areas:** Easily spot standout sections or anomalies during issue investigation.
- **Focus on Potential Causes:** Pinpoint the areas most likely to contain the root cause, streamlining troubleshooting efforts.

Figure 3-4 Aggregate statistics of a fleet



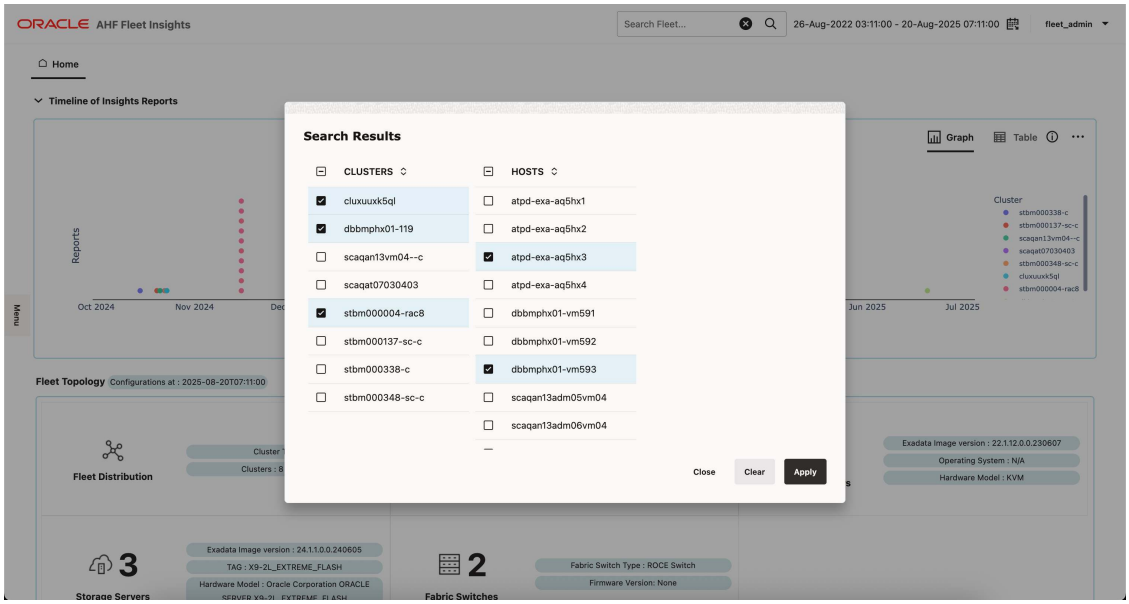
3.2.1.3 Filter cluster-specific or system-specific issues

Use this feature to isolate and analyze issues affecting particular clusters or systems, rather than viewing data at a global level.

Purpose:

- **Detailed Insights:** Access statistics and aggregates specific to individual clusters or hosts to better understand localized behavior and performance.
- **Focused Analysis:** Narrow the scope of investigation to relevant systems or clusters, enabling more efficient and targeted troubleshooting.

Figure 3-5 Filter cluster-specific or system-specific issues



1. In the search field, enter the name of the cluster or host, and then click the search icon.
2. In the resulting Search Results window, click **Apply**.

3.2.1.4 Filter issues that happened during a specific time window

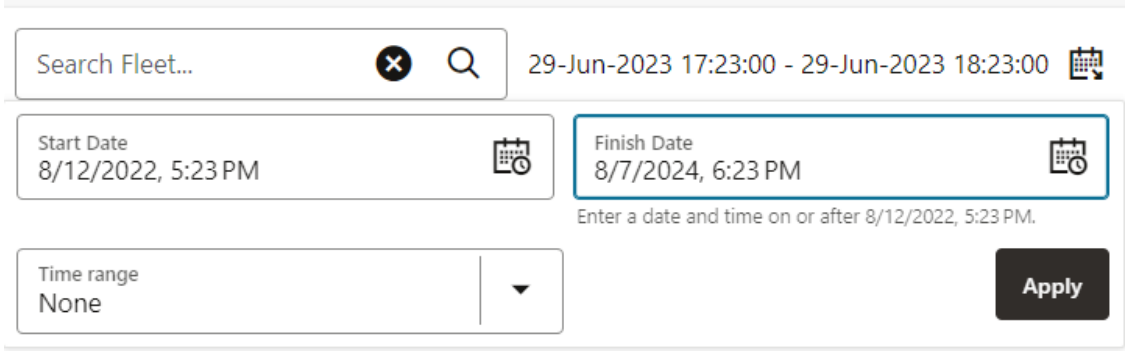
This feature allows you to refine the view of Fleet Insights data based on a selected time range, helping you isolate and investigate issues more effectively.

Purpose:

- **Customized Analysis:** By default, Fleet Insights displays data from a 4-hour window ending at the time of the last report generation. You can adjust this time range to focus on specific periods of interest.
- **Precise Troubleshooting:** Filter statistics and aggregated data to investigate issues that occurred within a defined timeframe, improving diagnostic accuracy and resolution speed.

Select a timeframe from the calendar control, and then click **Apply**.

Figure 3-6 Global Time Filter



3.2.1.5 Move from aggregations to specific Insights report and diagnostic collections

This feature enables you to transition from high-level aggregated views to specific AHF Insights reports or diagnostic collections for in-depth analysis.

Purpose:

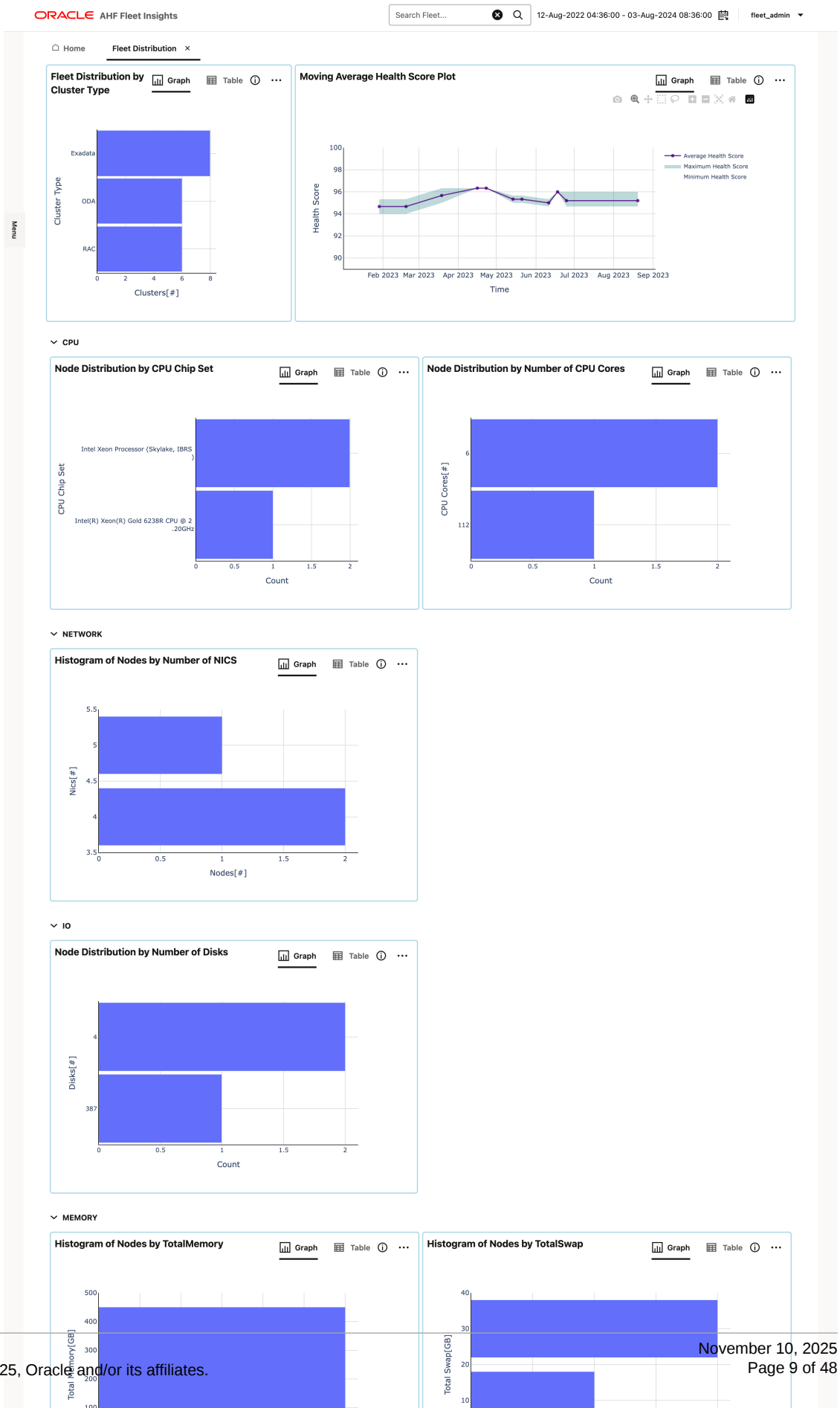
- **Detailed Investigation:** Drill down from summarized metrics to detailed insights reports or diagnostic data for a closer examination of system behavior.
- **Root Cause Analysis:** Review individual records to identify the underlying causes of issues, enabling more accurate and efficient troubleshooting.

3.2.2 Fleet Topology

Fleet Topology provides a real-time view of the current configuration and aggregated statistics for the entire fleet. It offers comprehensive insights into the distribution and status of all components, including databases, database servers, storage servers, and network fabric switches, enabling holistic monitoring and analysis of fleet-wide resources.

3.2.2.1 Fleet Distribution

Figure 3-7 Fleet Distribution



- Observe the distribution of fleet in terms of the type of clusters
- Observe the fleet's compliance health score trend over a period of time
- Observe the distribution of fleet across various system configurations

3.2.2.1.1 Observe the distribution of fleet in terms of the type of clusters

Purpose:

- **Fleet Composition:** Determine the number of systems categorized by type within the fleet.
- **Informed Decisions:** Utilize this distribution to guide decisions related to patching, upgrading, and managing resources based on the type and count of systems.

3.2.2.1.2 Observe the fleet's compliance health score trend over a period of time

Purpose:

- **Health Score Monitoring:** After deploying AHF Fleet Insights and registering client clusters, you will receive a compliance health score for each cluster along with suggested fixes in the Best Practice Issues section.
- **Performance Evaluation:** Track the fleet average health score over time. Ideally, the score should remain constant or improve as you apply recommended patches.
- **Issue Detection:** If the average score begins to decline, this may indicate issues during patching or other problems that require further investigation.

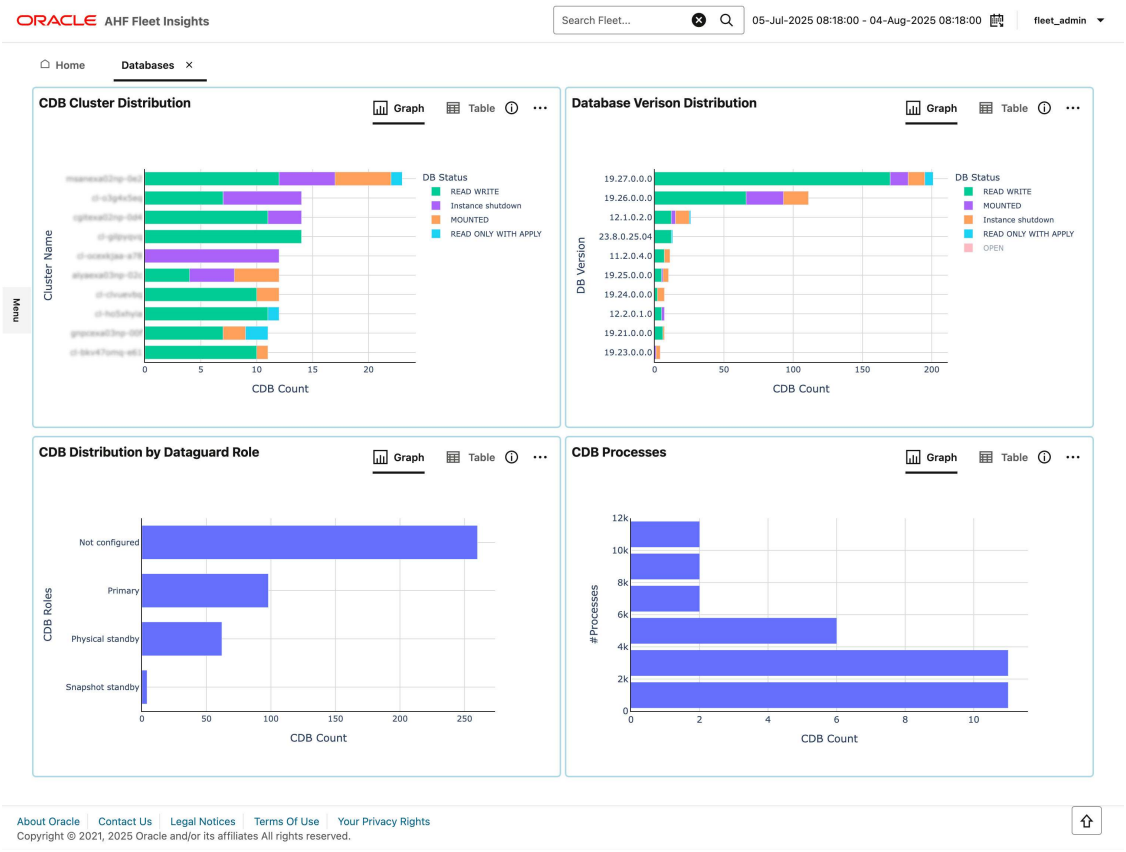
3.2.2.1.3 Observe the distribution of fleet across various system configurations

Purpose:

- **Configuration Overview:** Analyze how your fleet is distributed across different system configurations, as captured by Insights reporting. This includes dimensions such as CPU chipset type, memory size, and other hardware or software configurations.
- **Informed Decisions:** Use this distribution data to make informed decisions about system management, including patching, upgrades, and capacity planning.

3.2.2.2 Databases

Figure 3-8 Databases



- Observe the distribution of databases across the fleet
- Find what versions of databases are extensively used across the fleet

3.2.2.2.1 Observe the distribution of databases across the fleet

Purpose:

- **Database Status Overview:** Determine how databases are distributed across your fleet, including their operational statuses (online, unavailable, etc.).
- **Identify Issues:** Assess which databases or clusters may require attention based on their current status and distribution.
- **Informed Decision-Making:** Use this information to prioritize actions such as maintenance, troubleshooting, or resource reallocation to ensure optimal performance and availability.

3.2.2.2.2 Find what versions of databases are extensively used across the fleet

Purpose:

- **Version Analysis:** Assess which database versions are most prevalent to guide decisions on prioritizing upgrades or patching efforts.
- **Strategic Planning:** Use the version distribution information to align upgrade strategies with fleet-wide requirements and ensure compatibility and performance.

3.2.2.3 Database Servers

Figure 3-9 Database Servers

- Know the distribution of fleet across various database server configurations
- Identify the most commonly used operating system/version across your database servers
- Identify the most common range of memory sizes across your database servers

3.2.2.3.1 Know the distribution of fleet across various database server configurations

Purpose: Understand the distribution of your fleet across different configurations of database servers, such as Exadata Image Version and Hardware Model Distribution. This insight helps in making informed decisions about:

- **Patch and Bug Prioritization:** Target updates and fixes based on the configuration spread within your fleet.
- **Capacity Planning:** Assess current capacity and plan for future needs according to the distribution.
- **Fault Tolerance:** Identify potential vulnerabilities and enhance fault tolerance across configurations.
- **Resource Allocation:** Optimize resource distribution based on the configuration details of your servers.

3.2.2.3.2 Identify the most commonly used operating system/version across your database servers

Purpose:

- **Optimize Performance:** Ensure consistency in the operating system environment to streamline performance tuning and troubleshooting.
- **Enhance System Management:** Standardize configurations across your fleet to simplify management tasks and improve security by addressing specific vulnerabilities related to common operating systems and versions.

3.2.2.3.3 Identify the most common range of memory sizes across your database servers

Purpose:

- **Performance Optimization:** Ensure that memory resources are appropriately allocated to meet the performance requirements of your database operations.
- **Troubleshooting:** Address performance issues by analyzing memory usage patterns and adjusting configurations as needed.
- **Cost Management:** Manage costs by aligning memory allocations with your performance needs and avoiding over-provisioning.

3.2.2.4 Storage Servers

Figure 3-10 Storage Servers

- Know the distribution of fleet across various storage server configurations

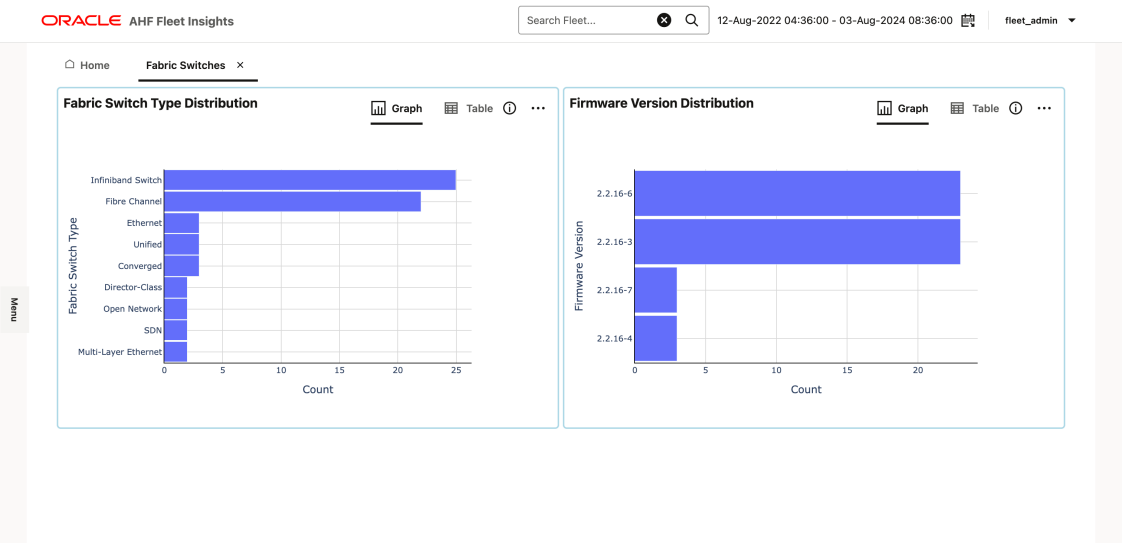
3.2.2.4.1 Know the distribution of fleet across various storage server configurations

Purpose:

- **Understand Configuration Distribution:** Gain insight into how your fleet is distributed across various storage server configurations, such as Exadata Image Version and Hardware Model Distribution.
- **Make Informed Decisions:** Use this information for patch and bug prioritization, capacity planning, fault tolerance, and resource allocation, ensuring that your maintenance and planning strategies are aligned with your infrastructure's configuration.

3.2.2.5 Fabric Switches

Figure 3-11 Fabric Switches



- Know the distribution of fleet across various fabric switch configurations

3.2.2.5.1 Know the distribution of fleet across various fabric switch configurations

Purpose:

- **Understand Configuration Distribution:** Gain insight into how your fleet is distributed across various fabric switch configurations, such as Switch Type and Firmware Version.
- **Optimize Performance and Troubleshoot Issues:** Use this information to optimize performance, streamline troubleshooting, and ensure that your fabric switch configurations are effectively managed.

3.2.3 Insights

Insights centralizes fleet-wide analysis of events, detected problems, and best practice compliance, along with detailed reports on operating system anomalies and software recommendations. It tracks system changes, monitors capacity and usage trends, and highlights patch, RPM, and version discrepancies. By consolidating issues, trends, and recommendations, it supports proactive maintenance, optimization, and resolution across the entire fleet.

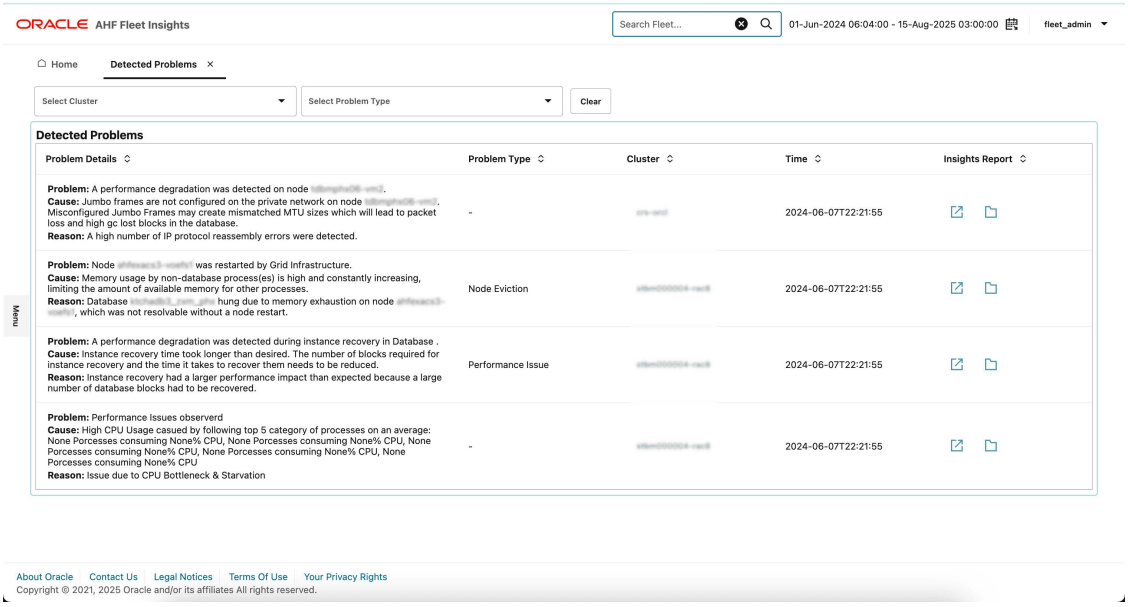
- Detected Problems
- Events
- Fleetwide Capacity Analysis
- Cluster-Wise Usage Trends and Forecast
- Operating System Issues
- Best Practice Issues
- System Changes
- Recommended Software

- RPM List
- Patch Information
- Space Analysis

3.2.3.1 Detected Problems

The Detected Problems dashboard provides a centralized, real-time view of critical issues identified across database clusters. It helps administrators and engineers quickly assess the nature and impact of system anomalies, facilitating faster root cause analysis and resolution.

Figure 3-12 Detected Problems



This dashboard is a key tool for maintaining fleet health, reliability, and performance.

The Detected Problems page offers:

- A summary of active and historical problems detected across clusters and nodes
- Insights into the root cause, impact level, and problem type
- Drilldowns and filters to accelerate issue investigation and remediation

Centralized Problem Table

A sortable, filterable table that lists:

- Problem type (e.g., performance degradation, node eviction)
- Affected node and cluster
- Time of occurrence
- Root cause and resolution status

Filtering options

These filters support targeted analysis during incident response or performance reviews.

- Select Cluster: View problems for a specific cluster
- Select Problem Type: Focus on categories like Performance Issue, Node Eviction, High CPU, etc.
- Clear Button: Quickly reset filters to return to the full problem list

Use cases

- Root cause analysis
  Drill into specific issues to trace back to their root cause and related system events, accelerating resolution.
- Operational monitoring
  Track the frequency and patterns of recurring problems to identify systems needing immediate attention or optimization.
- Capacity and reliability planning
  Surface early warning signs of system stress, such as:
  - High memory/CPU usage
  - Jumbo frame mismatches
  - Recurrent network disconnects

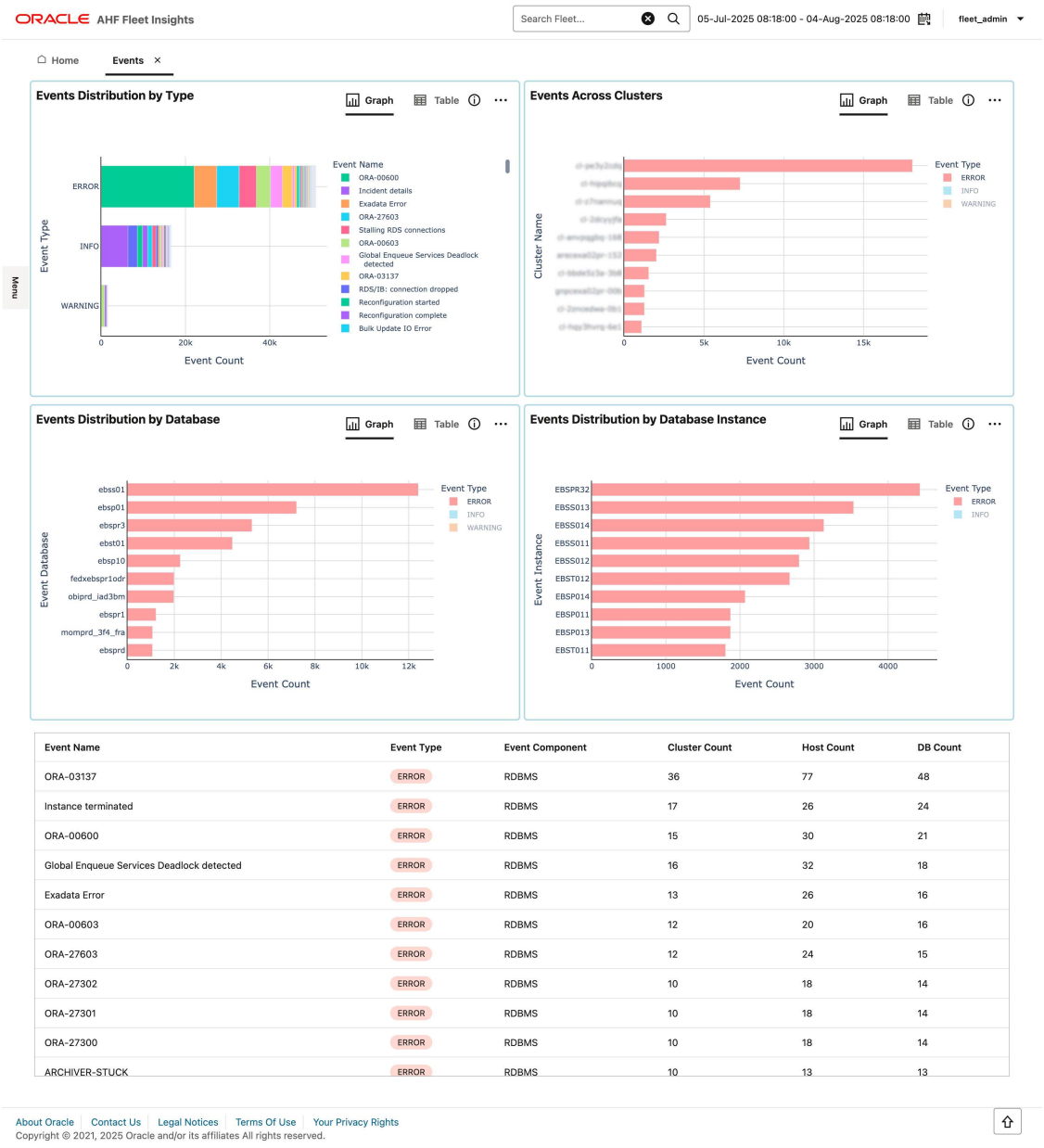
  This allows for preemptive scaling or configuration adjustments.
- Audit and compliance
  Access historical records of issues, including:
  - Timestamps
  - System impact
  - Resolutions applied

  Supports internal audits, incident postmortems, and SLA tracking.

3.2.3.2 Events

The Events dashboard enables you to monitor, investigate, and analyze error occurrences across databases, clusters, and hosts. It helps identify systems with the highest error counts, detect anomalies, investigate recurring or recent issues, and correlate event spikes with system updates. Through filtering and drill-down views, it pinpoints affected resources and links to relevant insight reports for deeper troubleshooting.

Figure 3-13 Events



- Identify databases with the highest number of error events
- Identify clusters with the highest number of error events
- Drill-down flow

3.2.3.2.1 Identify databases with the highest number of error events

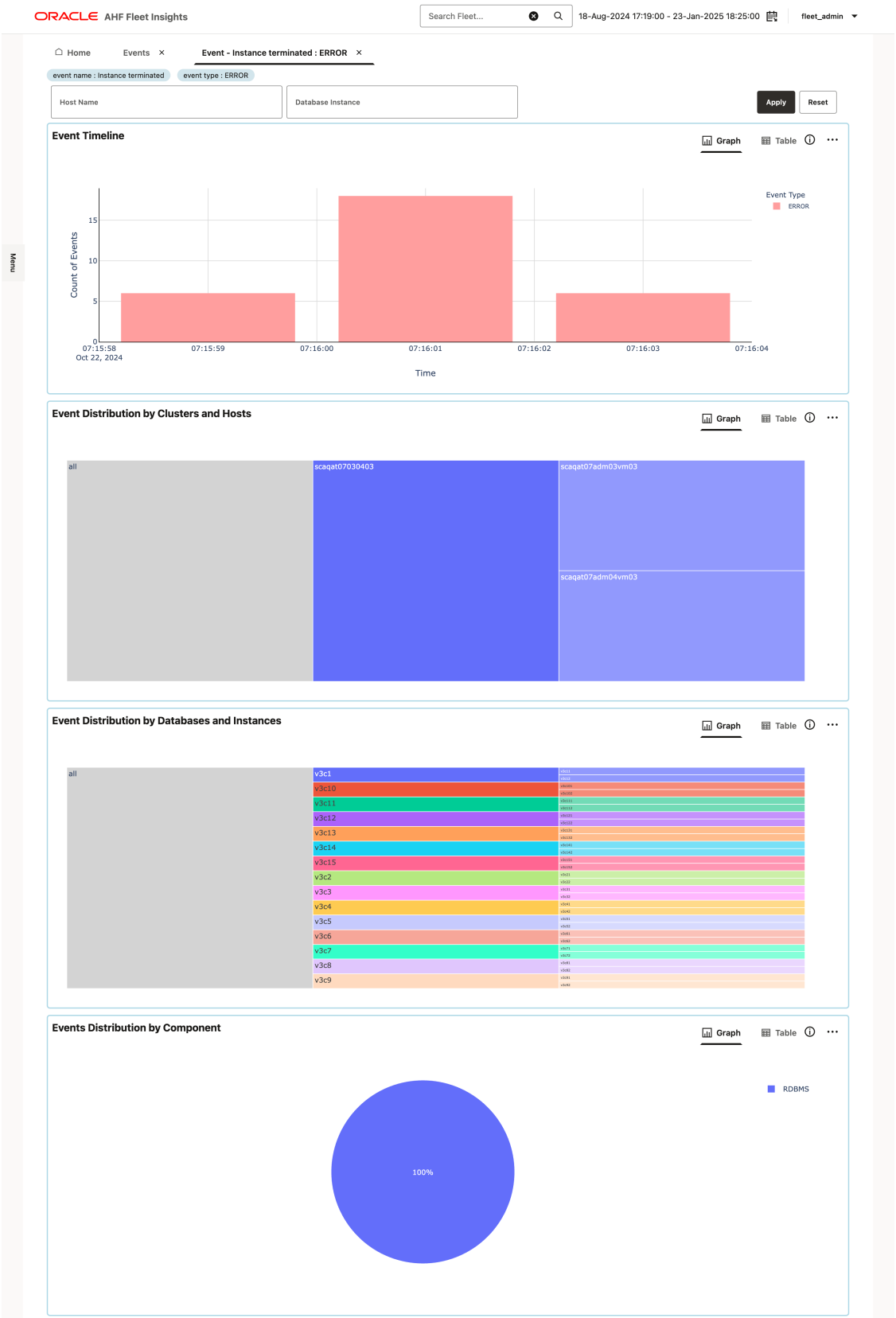
Purpose: Identify the databases having the maximum number of error events.

3.2.3.2.2 Identify clusters with the highest number of error events

Purpose: Identify the clusters having the maximum number of error events.

3.2.3.2.3 Drill-down flow

Figure 3-14 Events drill-down flow



- Investigate a specific error event
- Find the most recent events across the fleet
- Identify anomalies among certain clusters/hosts

3.2.3.2.3.1 Investigate a specific error event

Purpose:

- Find the error that occurred the most and apply it as a filter.
- In the drill-down page, check if there is a spike of occurrence of this event on the timeline chart.
- Filter the hosts on which this event occurred the most.
- Filter the databases on which this event occurred the most.
- Once the filters are applied, pinpoint the insight reports which can be used to further investigate the event.

3.2.3.2.3.2 Find the most recent events across the fleet

Purpose:

- Observe if the new issues occur after a system update.
- Filter by time.
- Monitor events between the last system update and now.

3.2.3.2.3.3 Identify anomalies among certain clusters/hosts

Purpose:

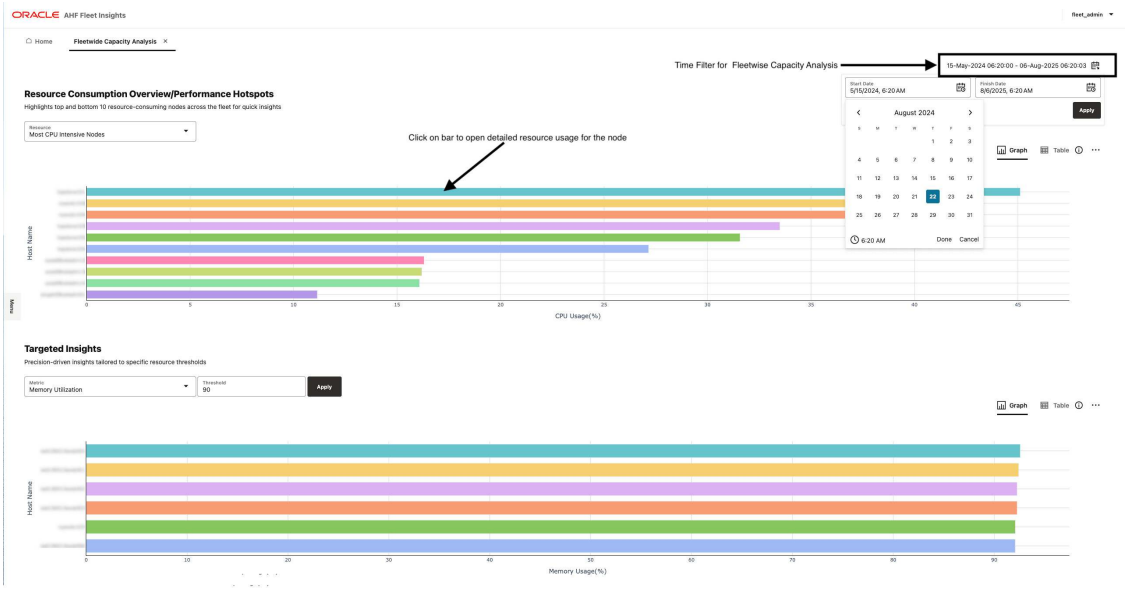
- Analyze if it is more prevalent on certain clusters/hosts.
- Analyze if it is more prevalent on certain databases.
- Filter and go to the corresponding insight report for more granular analysis.

3.2.3.3 Fleetwide Capacity Analysis

The Fleet Resource Insights dashboard provides a quick view of resource usage across your fleet, helping you identify top and bottom consumers, spot bottlenecks, and uncover underutilized nodes for optimized performance.

Refer to Managing Exadata Capacity Planning Plugin.

Figure 3-15 Fleetwide Capacity Analysis



Resource Consumption Overview/Performance Hotspots

- Highlights top and bottom 10 resource-consuming nodes across the fleet for quick insights.
- Investigate high-consuming nodes to identify potential bottlenecks.
- Review low-consuming nodes to identify underutilized resources.

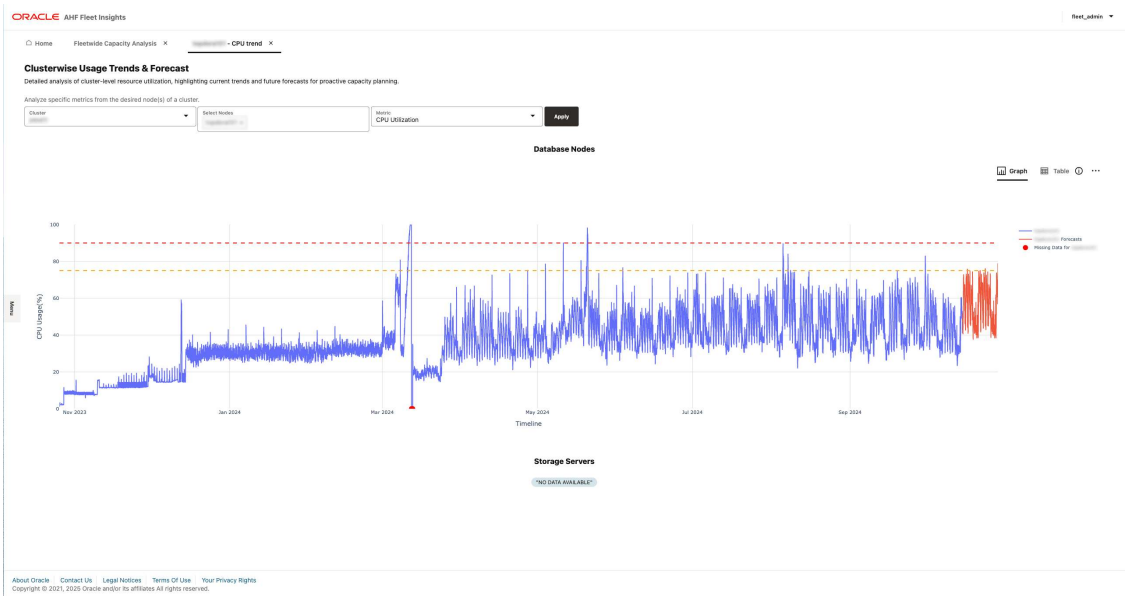
Targeted Insights

- Precision-driven insights tailored to specific resource thresholds.
- Adjust resource thresholds and metric selection to refine the scope of insights.
- Use these insights to proactively address potential performance bottlenecks.

Fleetwide Capacity Analysis drill-down

Click on the bar to open the complete resource usage for selected node and metric. For more information, see Cluster-Wise Usage Trends and Forecast.

Figure 3-16 Fleetwide Capacity Analysis-drilldown



3.2.3.4 Cluster-Wise Usage Trends and Forecast

Get a detailed view of cluster-level resource utilization with current trends and future forecasts to support proactive capacity planning. Visualize usage patterns by metric, track forecast growth, and use historical trends to optimize resource allocation.

Refer to Managing Exadata Capacity Planning Plugin.

Figure 3-17 Cluster-Wise Usage Trends and Forecast

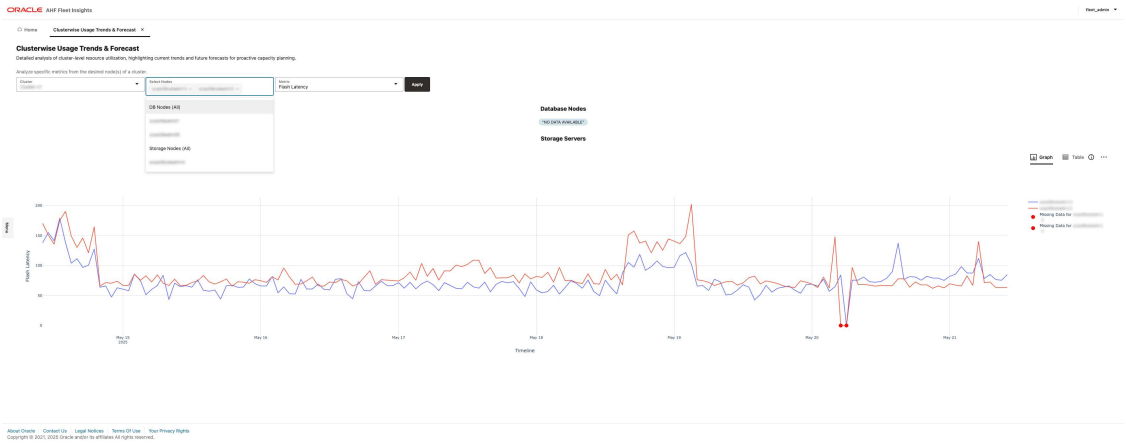


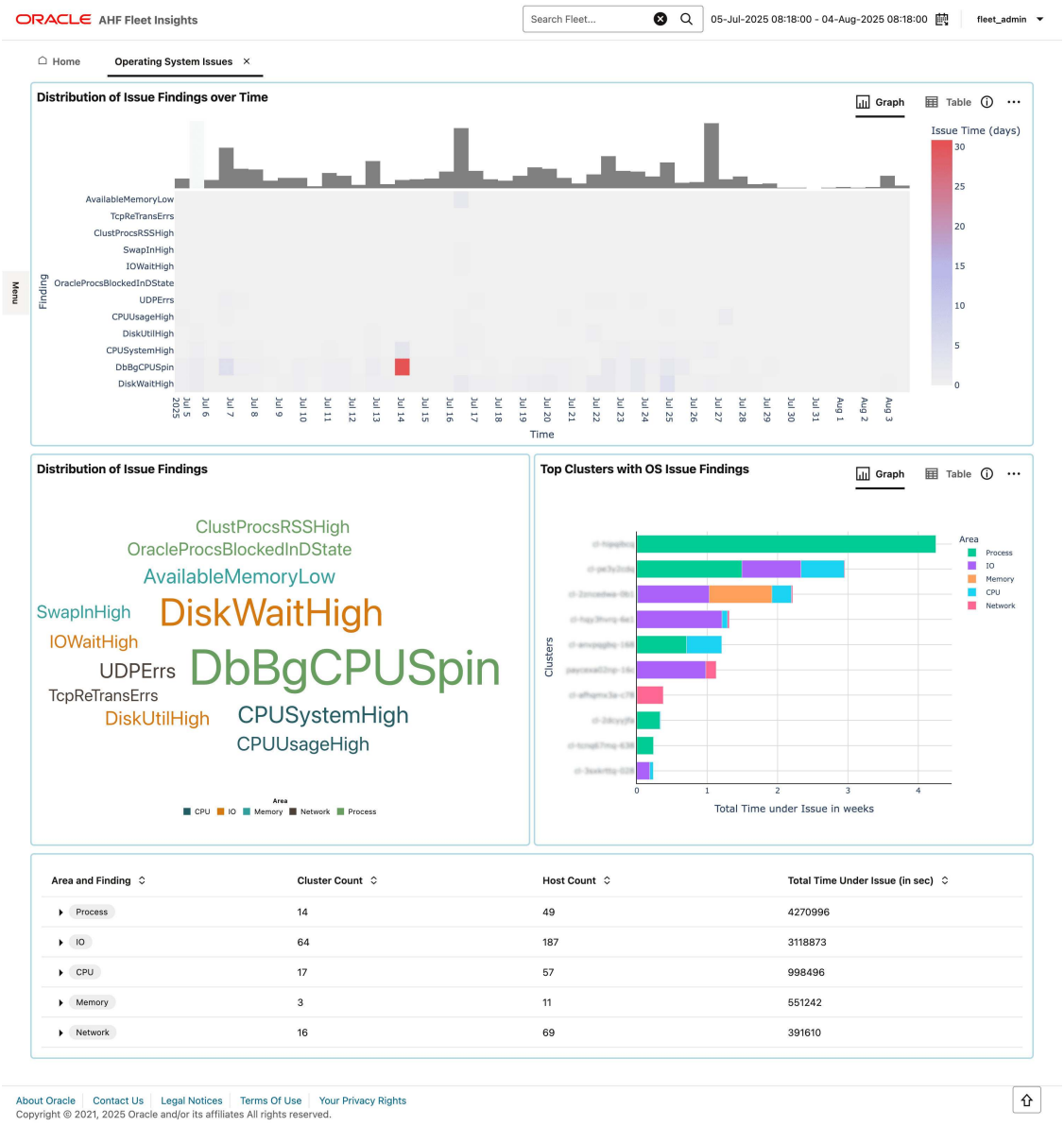
Figure 3-18 Cluster-Wise Usage Trends and Forecast

- Detailed analysis of cluster-level resource utilization, highlighting current trends and future forecasts for proactive capacity planning.
- Visualize resource usage trends across cluster for a specific metric by choosing desired database and storage servers.
- Monitor forecast growth to plan for timely resource scaling
- Use historical trends to identify patterns in cluster usage and optimize allocation.

3.2.3.5 Operating System Issues

The Operating System Issues dashboard provides an overview of operating system–related problems detected within your environment. You can review trends to see which issues have increased over a specific period, identify the cluster most impacted, and check for spikes in reported incidents. From there, you can drill down to see the most affected host and access the OS Issues section in the Insights report for detailed analysis and troubleshooting steps.

Figure 3-19 Operating system issues



- Identify prominent operating system issues in a given period
- Identify which cluster has been most impacted by operating system issues
- Identify if there was a spike in operating system issues reported during a specific timeframe

3.2.3.5.1 Identify prominent operating system issues in a given period

Purpose: Determine which operating system issues have experienced a significant increase in reports and identify the specific time period during which these spikes occurred.

3.2.3.5.2 Identify which cluster has been most impacted by operating system issues

Purpose: Select the most impacted cluster as a Fleet manager and then drill-down for further analysis. And, as a DBA, you can investigate a particular cluster.

3.2.3.5.3 Identify if there was a spike in operating system issues reported during a specific timeframe

Purpose:

- Within the drill-down page, check the timeline to see if there were any spikes for operating system issues in that particular cluster.
- Identify the host that is most impacted by the operating system issues.
- Finally, go to an Insights report, which would take you to the **OS Issues** section of the Insights report to facilitate more granular analysis.

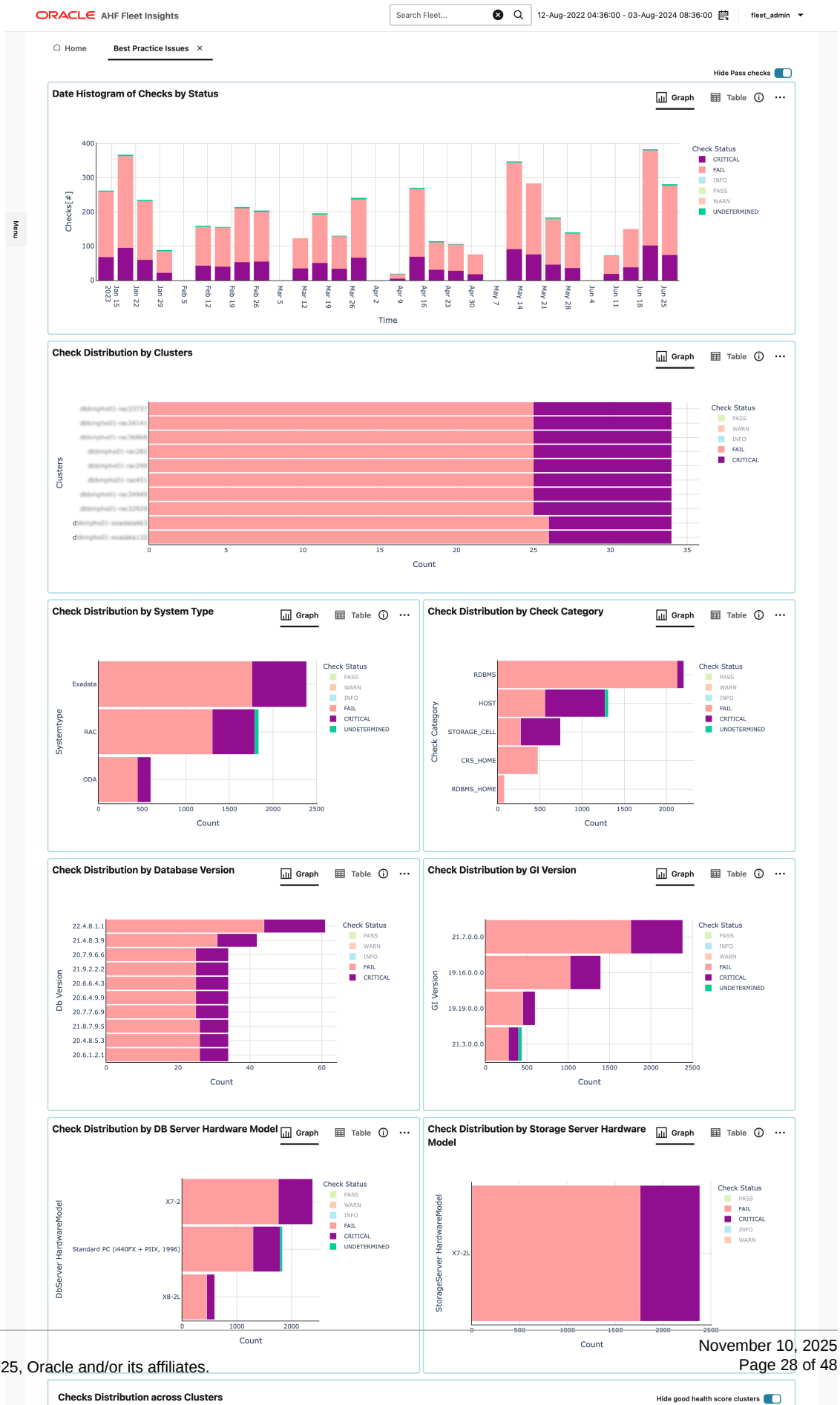
Drill-down flow

1. Investigate a particular operating system issue.
2. Select the time range where there is a spike in operating system issues.
3. Apply cluster and host filters.
4. Once the filters are applied, pinpoint the insight reports, which can be used to investigate the issue further.

3.2.3.6 Best Practice Issues

The Best Practice Issues dashboard helps you identify and analyze critical best practice issues across your environment. You can view the top clusters and database server hardware models with the highest number of issues, then apply filters to focus on specific clusters or hardware types. Drill-down options allow you to refine results by check type, category, and system type, enabling you to pinpoint particular checks. From there, you can explore the Insights report or review diagnostic collections to investigate the root cause and plan corrective actions.

Figure 3-20 Best Practice issues



3.2.3.6.1 Identify critical issues across clusters

Purpose: Find the top cluster having more number of best practice issues. Within the check distribution by cluster plot, select the top cluster as filter.

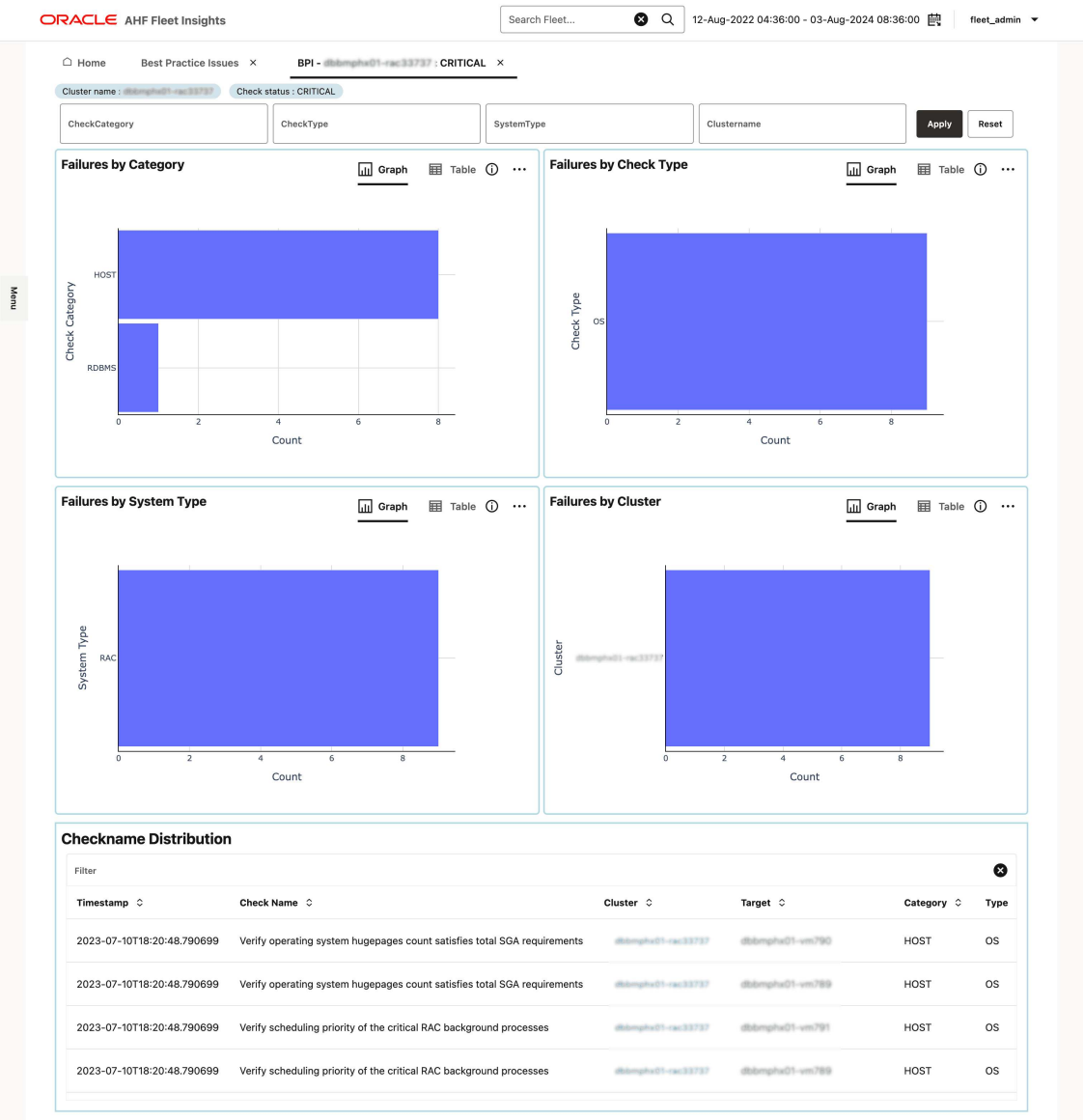
3.2.3.6.2 Identify critical issues across database server hardware models

Purpose:

- Identify the top database server hardware model having more number of best practice issues.
- Filter for the top database server hardware and go on to the next stage of analysis.

3.2.3.6.3 Drill-down flow

Figure 3-21 Best Practice issues drill-down flow



- Identify critical issues in a specific cluster
- Find the distribution of issues on a specific database server hardware model

3.2.3.6.3.1 Identify critical issues in a specific cluster

Audience: DBA

Purpose:

- Select a cluster with more critical checks. Further drill-down is made based on check type, category, system type, and so on. Once the filters are applied on the drill down page, you will end up with a few particular checks.
- Explore the insights report or diagnostic collection for a particular record or drill-down to discover the root cause of an issue.

3.2.3.6.3.2 Find the distribution of issues on a specific database server hardware model

Audience:

- Fleet admin
- DBA

Purpose:

- Select a database server hardware model with more critical checks. Further drill-down is made based on check type, category, system type, and so on. Once the filters are applied on the drill down page, you will end up with a few particular checks.
- Explore the insights report or diagnostic collection for a particular record or drill-down to discover the root cause of an issue.

3.2.3.7 System Changes

The System Changes dashboard provides visibility into system-level modifications — such as database parameter updates and configuration adjustments — across the fleet, over a selected time range.

This dashboard helps administrators:

- Track system modifications over time
- Assess the potential impact of changes on stability, performance, and compliance
- Identify clusters or nodes with unusual or frequent change patterns

Figure 3-22 System Change

Distribution of system changes over time

This plot shows a temporal distribution of system changes across the fleet:

- Y-axis: System change types (e.g., DB config, kernel parameters, file changes)
- X-axis: Time buckets within the selected range (e.g., hourly, daily)
- Margin Plot (above X-axis): Total number of changes per time bucket — useful for spotting change spikes or periods of unusual activity

This view highlights what types of changes occurred, when they occurred, and how frequently — ideal for trend analysis and change audits.

System changes by cluster

This plot summarizes system changes by cluster, providing both breadth and depth:

- X-axis: Clusters in the fleet
- Bars: Total number of changes
- Color breakdown: Specific system change types (e.g., OS-level, DB config, service restarts)

Key capabilities:

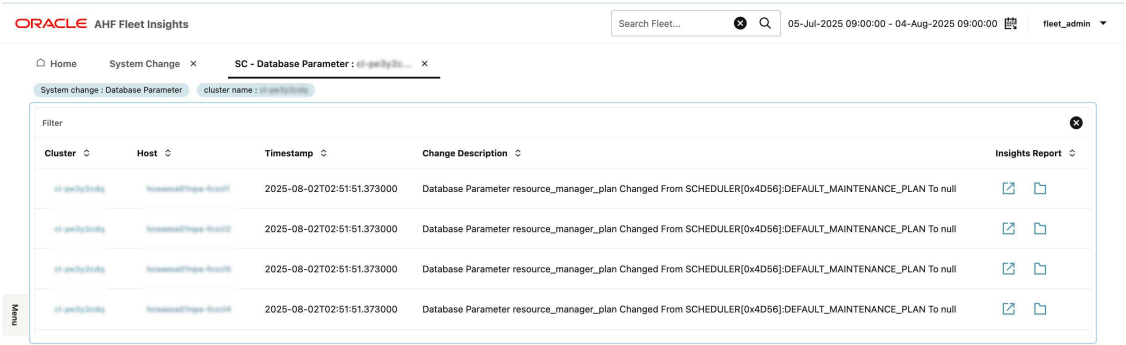
- View which clusters are undergoing frequent or large-scale changes
- Identify anomalies or outliers in change volume
- Select a cluster or system change type for drill-down investigation

Use this dashboard to:

- Monitor configuration drift across systems
- Detect risky or unauthorized changes in high-impact environments
- Align with change control and audit requirements

System Changes drill-down

Figure 3-23 System Changes



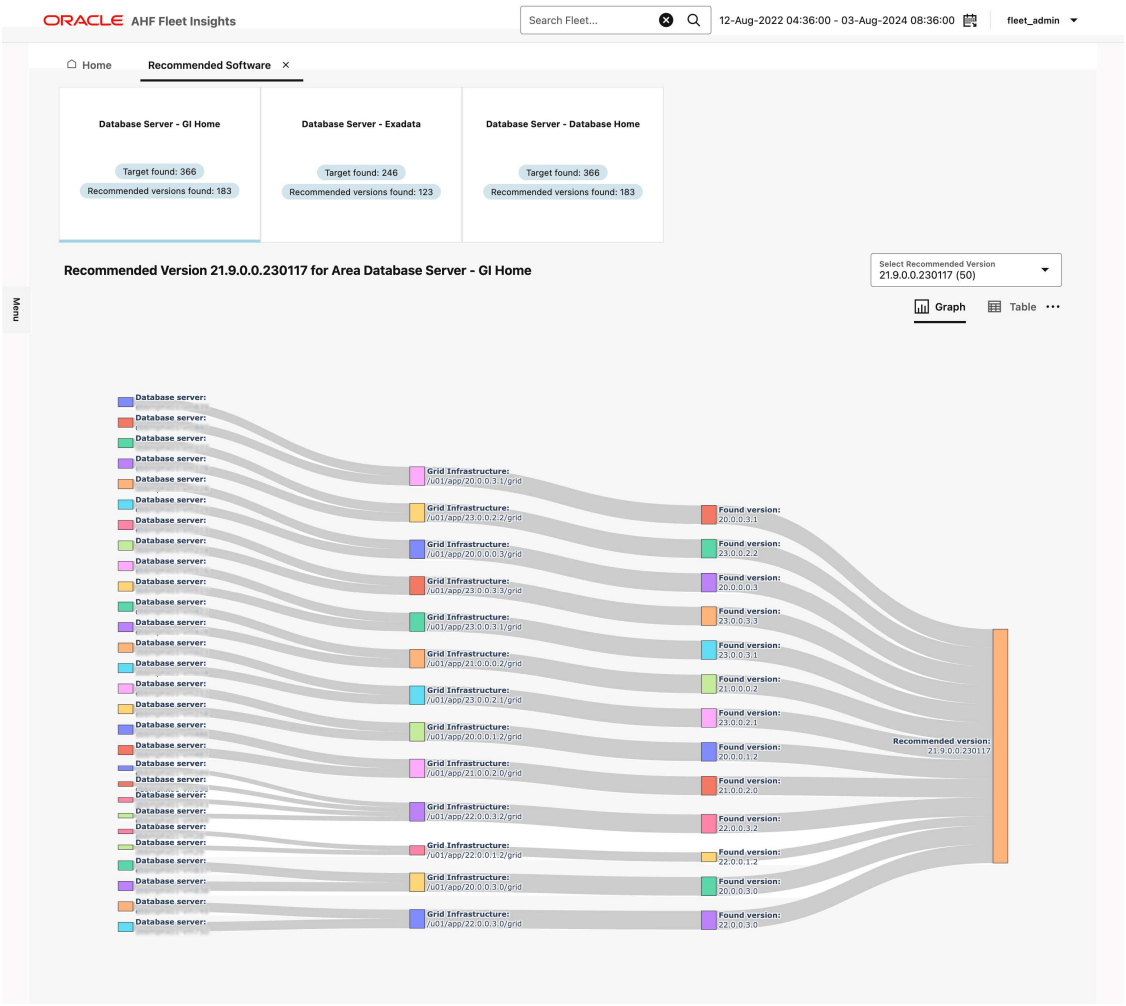
Purpose:

This drill-down page provides a detailed summary of all system changes that occurred based on the selected cluster name, system change type, or time range. From this view, you can navigate to the corresponding Insight report for a more granular analysis.

3.2.3.8 Recommended Software

The Recommended Software dashboard provides MAA-based recommendations for software versions to improve your fleet's compliance. You can view a visual summary of the versions currently in use and the recommended target versions. Use this information to prioritize systems for patch upgrades, focusing first on those that will deliver the greatest improvement in compliance and performance.

Figure 3-24 Recommended software



- Identify recommended software version to improve the compliance of your fleet

3.2.3.8.1 Identify recommended software version to improve the compliance of your fleet

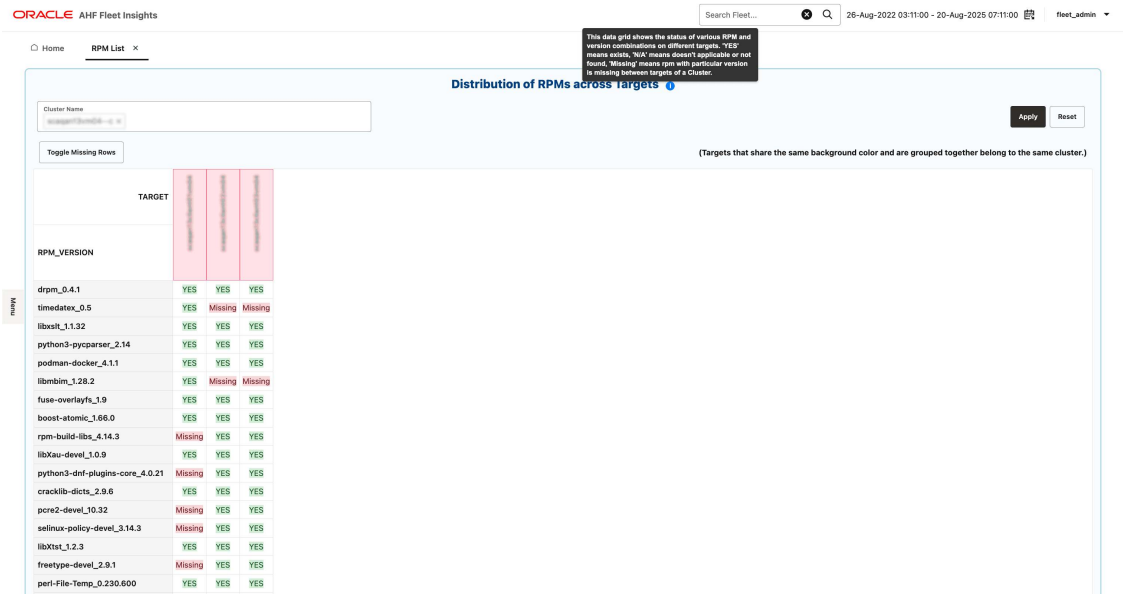
Purpose:

- Review the MAA-based software recommendations.
- Get a visual representations of what versions were found across the fleet and to what version to update.
- Identify what systems to target first for patch upgrades to get maximum benefits.

3.2.3.9 RPM List

The RPM List dashboard offers a comprehensive matrix view of installed RPM packages and their versions across multiple nodes and clusters. It serves as a critical tool for verifying software consistency and quickly identifying discrepancies across systems.

Figure 3-25 RPM List



This page is essential for:

- Identifying missing, inconsistent, or outdated RPMs across servers
- Enforcing standardization and compliance across environments
- Supporting patch readiness and troubleshooting by pinpointing package gaps
- Cluster selection
  Cluster Name Filter: Users can select one or more clusters to analyze and compare RPM package status.
  - Supports multi-cluster comparison
  - Allows side-by-side validation of package presence and versions across nodes
  - Ideal for reviewing fleet-wide consistency

  Use this to:
  - Isolate specific clusters for focused audits
  - Compare development, staging, and production environments

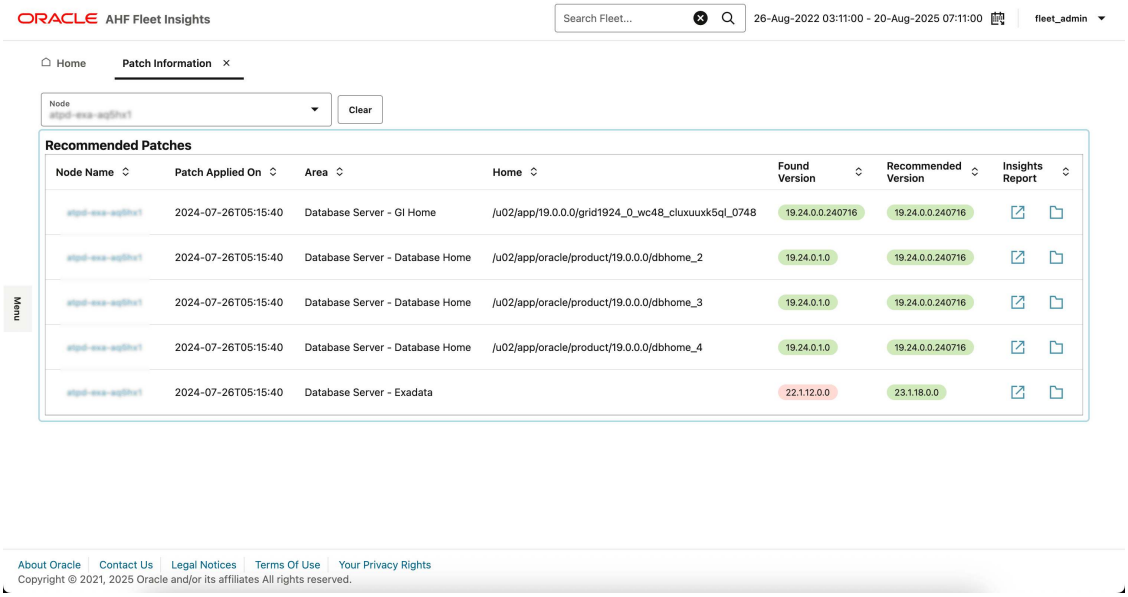
- Toggle missing rows
  Toggle Missing Rows: This button filters the matrix to only show RPMs that are missing on one or more nodes.
  - Helps quickly narrow down inconsistencies
  - Eliminates noise by hiding fully consistent rows
  - Essential for preparing clean, focused patch plans

  Use cases
  - Patch planning
    Identify which RPMs need to be installed or upgraded before applying a patch to ensure smooth execution.
  - Compliance checks
    Verify that critical RPMs are installed consistently across nodes and clusters to meet organizational or regulatory standards.
  - Cluster health review
    Spot RPM mismatches within a cluster that could lead to unpredictable behavior, software failures, or drift from configuration baselines.

3.2.3.10 Patch Information

The Patch Information dashboard provides a centralized view of patch compliance across the fleet. It enables administrators to monitor, validate, and track the deployment of software patches—particularly for databases and other critical components.

Figure 3-26 Patch Information



This dashboard is essential for ensuring systems remain:

- Secure
- Up-to-date

- Compliant with internal and external patching standards

> **Note**
>
> Select a node to view its patch history.

Use cases

- Patch gap identification
  Quickly spot which systems require updates and what patches are missing.
- Compliance validation
  Support internal audits and regulatory compliance by verifying patch levels against policy-defined baselines.
- Patch cycle planning
  Facilitate planning for upcoming patch windows by identifying high-priority systems and estimating required effort.
- Audit and analysis
  Access detailed patch logs, version histories, and exception reports to support root cause analysis or audit reviews.

3.2.3.11 Space Analysis

The Space Analysis dashboard provides a comprehensive overview of disk space utilization across all nodes in the fleet. It enables administrators to proactively detect storage-related issues, identify nodes approaching capacity, and manage disk usage efficiently.

Figure 3-27 Space Analysis

Nodes with space issues (utilization > 90%)

> **Note**
>
> If this section displays "No data available", it means no nodes currently exceed the 90% utilization threshold — a positive indicator.

This horizontal bar chart highlights nodes with one or more file system mounts exceeding 90% disk usage.

- Each bar represents a node.
- Bar length corresponds to the number of problematic mounts on that node.

This visualization helps quickly identify which systems are at risk of running out of space.

Disk usage distribution

A vertical bar chart that shows how file system mounts are distributed across utilization ranges (e.g., 0–10%, 10–20%, etc.).

This helps answer questions like:

- Are most mounts underutilized?
- Is there a concerning cluster of high-usage mounts?

This view helps identify fleet-wide storage trends or imbalances.

Disk usage over time by mount

> **Note**
>
> Select a node to view its historical disk usage.

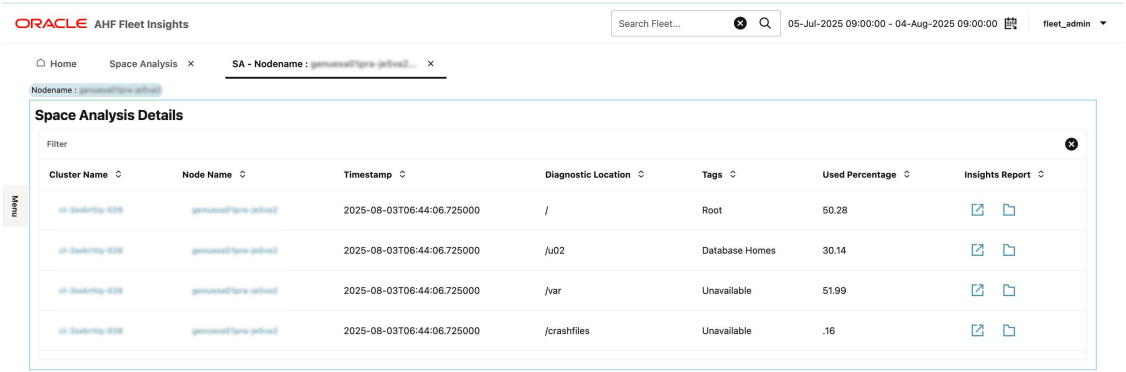
This time-series line chart tracks the percentage of disk usage over time for individual mount points on a selected node.

It enables long-term monitoring of storage growth and helps detect abnormal spikes or trends in disk consumption.

Node Drilldown: Space Analysis Details

Clicking on a node in the Nodes with Space Issues chart opens the Space Analysis Details page for that specific node.

Figure 3-28 Space Analysis Details



Purpose:

This drilldown page offers a granular view of disk usage at the mount level for the selected node. It helps you analyze space utilization with precise location and timestamp details, enabling more accurate diagnostics.

3.2.4 Admin

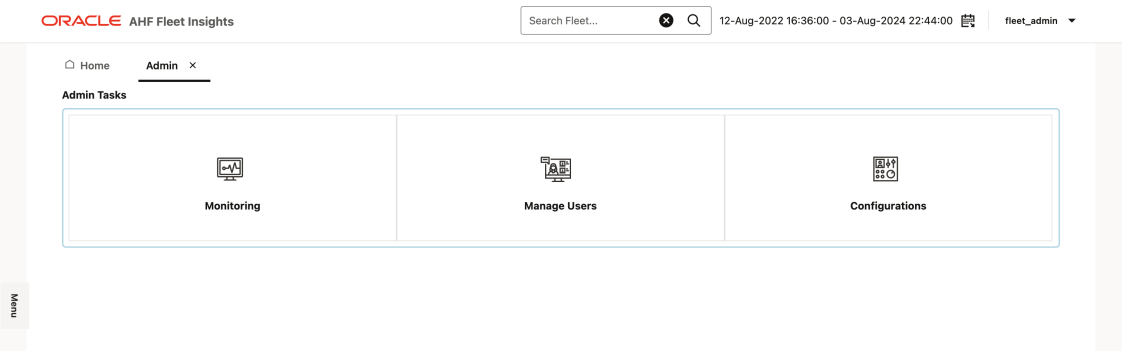
> **Note**
>
> Only Fleet Admin can perform the following administrative tasks.

- Accessing the Admin Dashboard
- Monitoring
- Manage users
- Configurations

3.2.4.1 Accessing the Admin Dashboard

Click the drop-down list at the upper-right corner and select **Admin**.

Figure 3-29 Admin dashboard



The Admin Dashboard provides access to the following key sections:

- **Monitoring**: View the status of uploaded collections and track whether they are being processed successfully.
- **Manage Users**: Allows Fleet Administrators to create new users, assign roles, and control access to data across the fleet.
- **Configurations**: Offers a unified interface for Fleet Administrators to view configuration values across the fleet and make changes as needed.

3.2.4.2 Monitoring

Monitor the performance and health of the Fleet Insights application. Identify and troubleshoot issues related to the processing of uploaded collections.

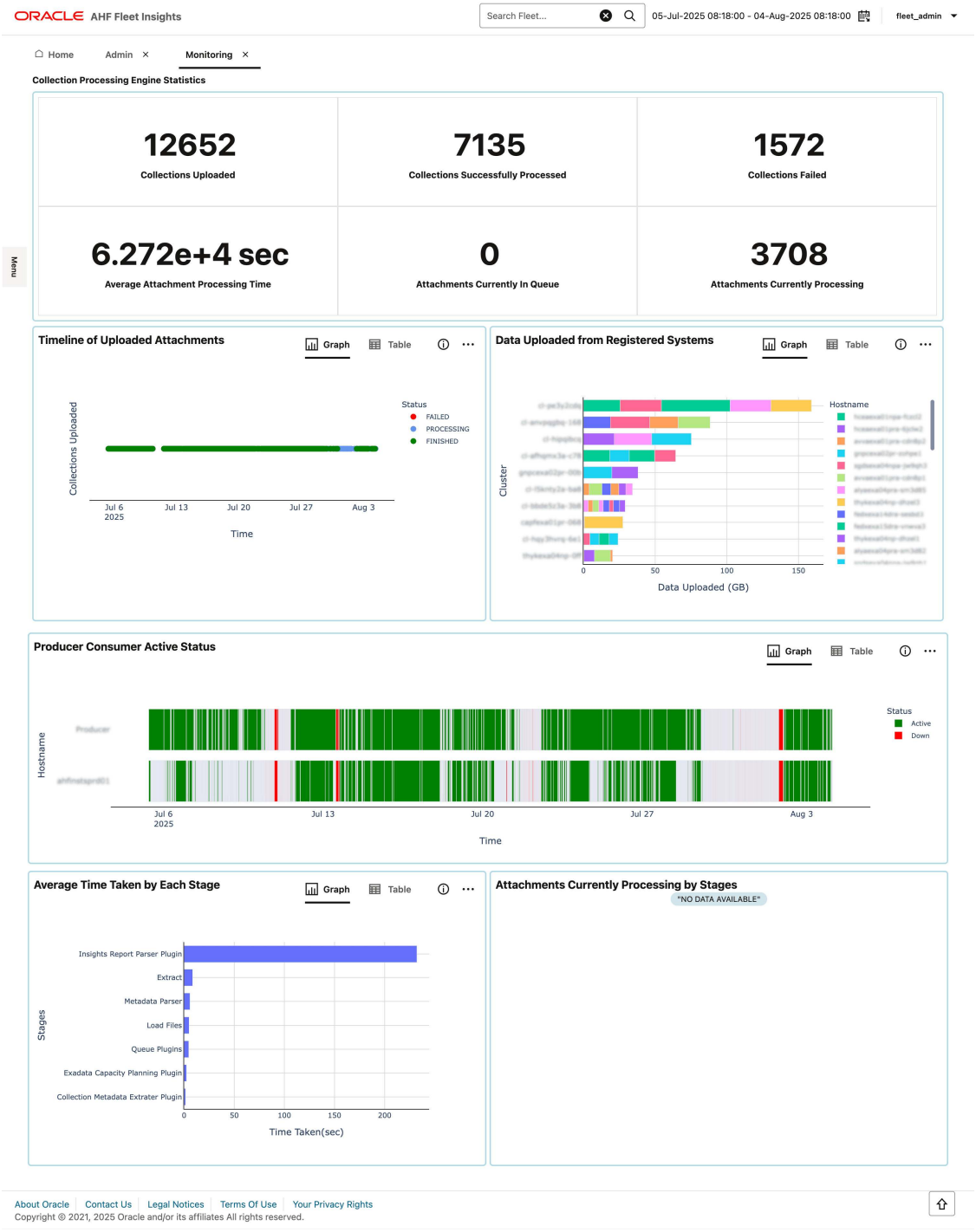
- Keep track of the performance of Fleet Insights application
- Find why was there a failure in processing the collections

3.2.4.2.1 Keep track of the performance of Fleet Insights application

Purpose:

- Check if the collections being uploaded getting processed successfully by the Fleet Insights application.
- Review various stats such as the following for a given time period:
  - Number of collections uploaded
  - Number of collections successfully processed
  - Number of failures
  - Average time to process a collection

Figure 3-30 Track Fleet Insights application performance



3.2.4.2.2 Find why was there a failure in processing the collections

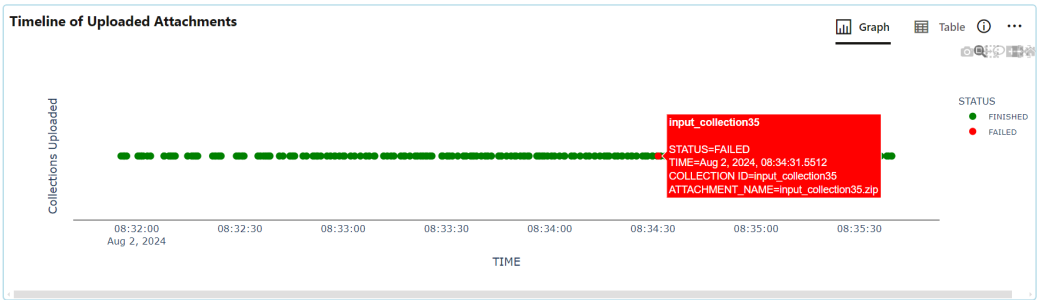
Purpose:

- Search or filter for failed collections.

- Open collection specific drill-down page to check at what stage of processing there was a failure.
- Open logs to see why there was a failure.

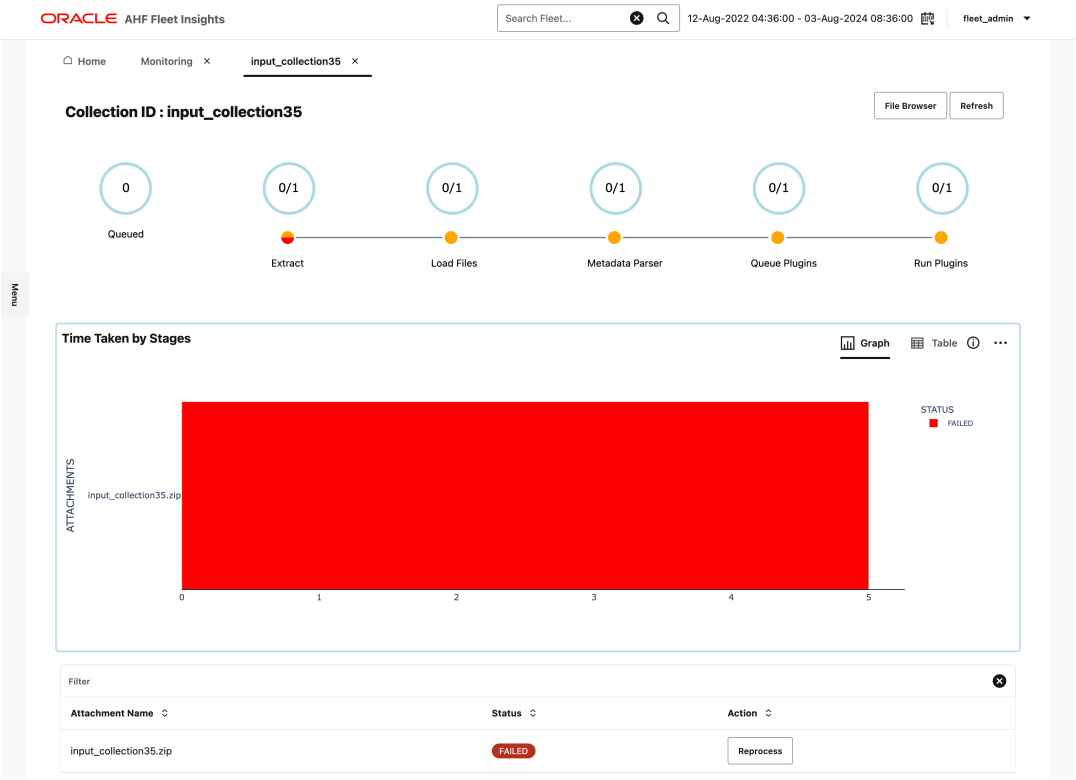
1. Hover the mouse pointer over the failed collections in the **Timeline of Uploaded Collections** section.

Figure 3-31 Timeline of Uploaded Attachments



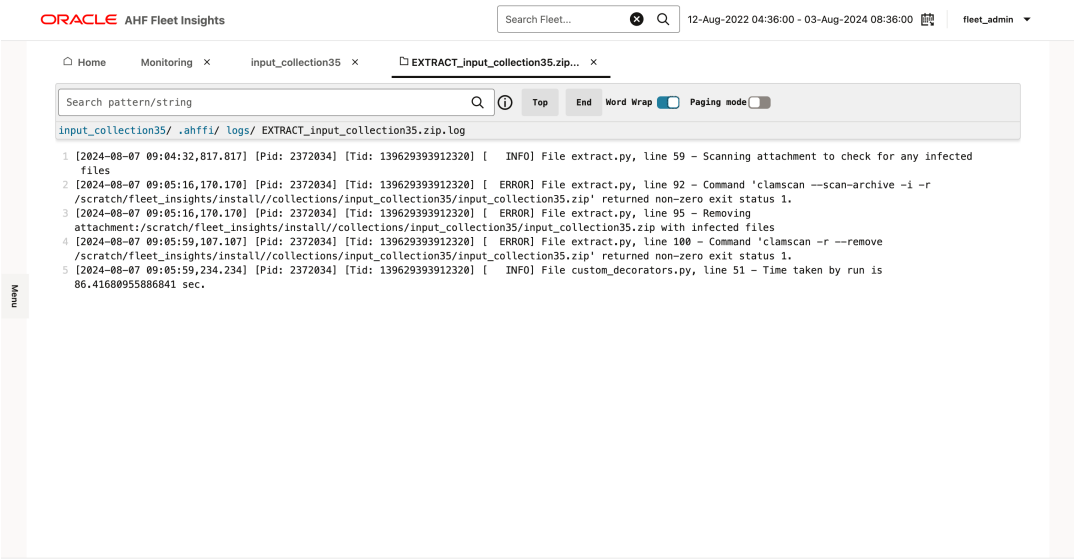
2. Click the scatter points to view details.

Figure 3-32 View collection upload timeline



3. Under **Action**, click **Reprocess** to upload the collection again.
4. In the **Time Taken by Stages** section, click the red bar of the failed attachment to view logs.

Figure 3-33 View failed collection upload logs



3.2.4.3 Manage users

As a fleet manager, create and manage UI users by assigning roles and limiting data access. Enable or disable cluster managers, restrict them to specific clusters, and reset client access when needed.

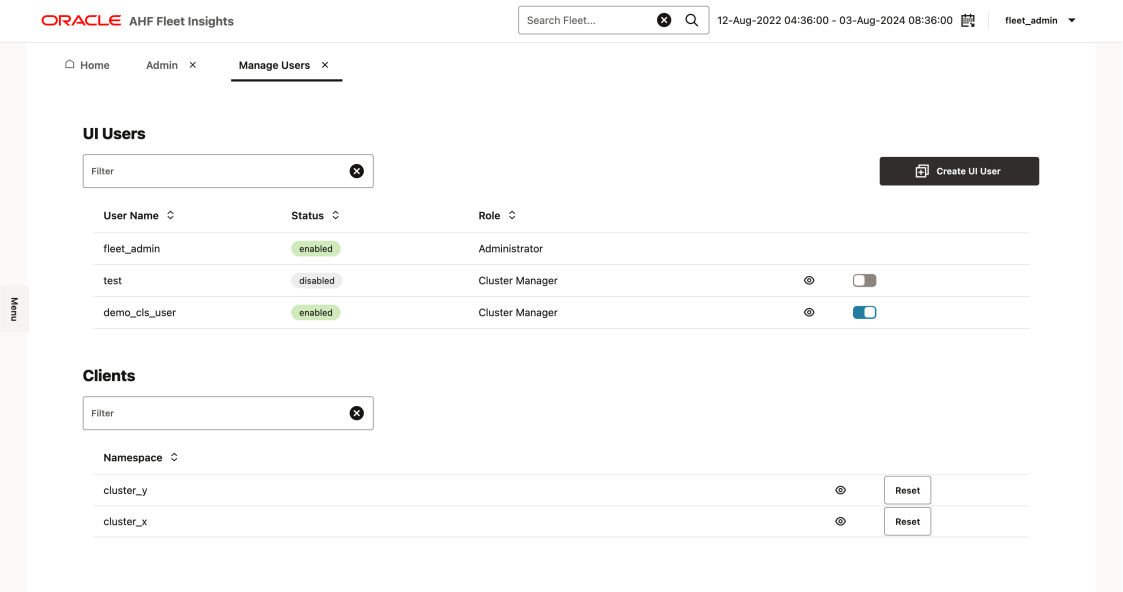
- Manage users as a fleet manager

3.2.4.3.1 Manage users as a fleet manager

Purpose:

- Create user interface users and assign them specific and limited roles and data access.
- Enable or disable cluster managers.
- Restrict cluster managers to their assigned clusters.
- Remove (reset) clients.

Figure 3-34 Manage users



To create a UI user

1. Click **Create UI User**.
2. In the resulting page, enter user name and password, and then select a role (Administrator, Cluster Manager).
3. If you choose to assign Cluster Manager role, **Cluster Access** field is displayed.
4. Click and select the clusters from the list you want to assign to the user.
5. Click **Save**.

To restrict cluster managers to their assigned clusters

1. Slide the toggle button to enable or disable the cluster manager.
2. Click the view icon to the list of cluster assigned to the cluster manager.
3. In the resulting page, click **Edit**, and then add or remove clusters from the list.
4. Click **Save**.

To remove clients

1. Filter the user you want to remove.
2. Click **Reset**.

3.2.4.4 Configurations

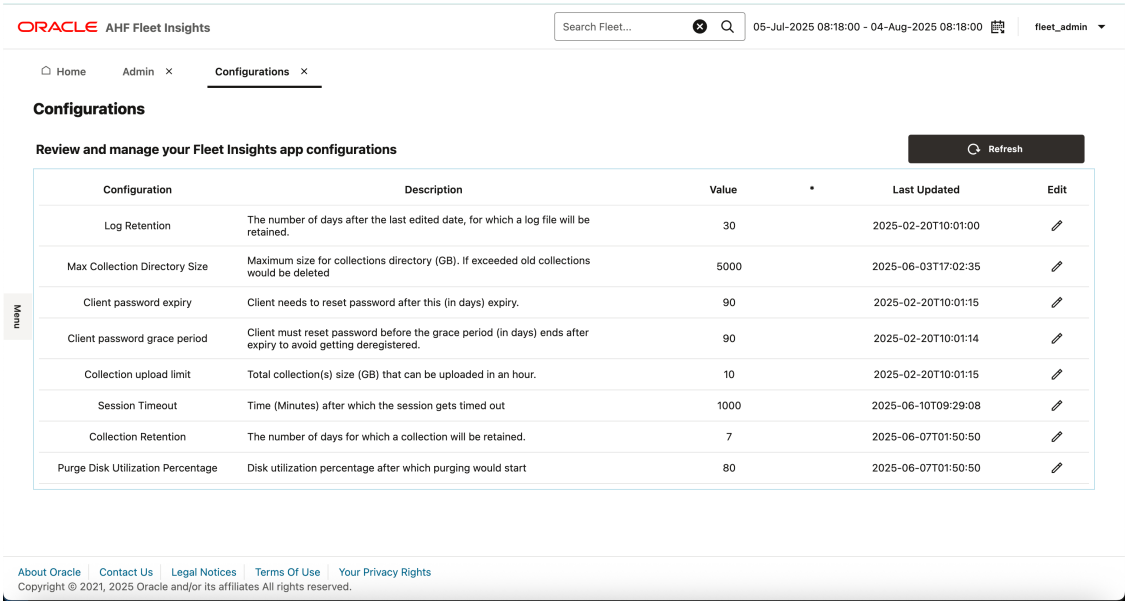
View and manage Fleet Insights configuration settings. Edit specific parameters as needed to align with your fleet's requirements. Simply locate the parameter, click the edit icon, and enter the new value.

- View and edit Fleet Insights configuration

3.2.4.4.1 View and edit Fleet Insights configuration

Purpose: View Fleet Insights configuration details and reconfigure the values when needed.

Figure 3-35 AHF Fleet Insights configuration parameters



Edit configuration parameters

1. Locate the parameter you want to update.
2. Click the Edit icon next to the parameter.
3. Enter the new value in the input field.
4. Click the tick mark to save your changes.

> **Note**
>
> Changes take effect immediately and may impact how insights are generated or processed. Ensure values are updated carefully.

3.2.5 File Viewer

The File Viewer allows you to access and inspect files within a collection directly from the UI. It is integrated into several areas across the platform to support easier troubleshooting and analysis.

You can filter files by name or type to quickly locate relevant information.

Where to Find It

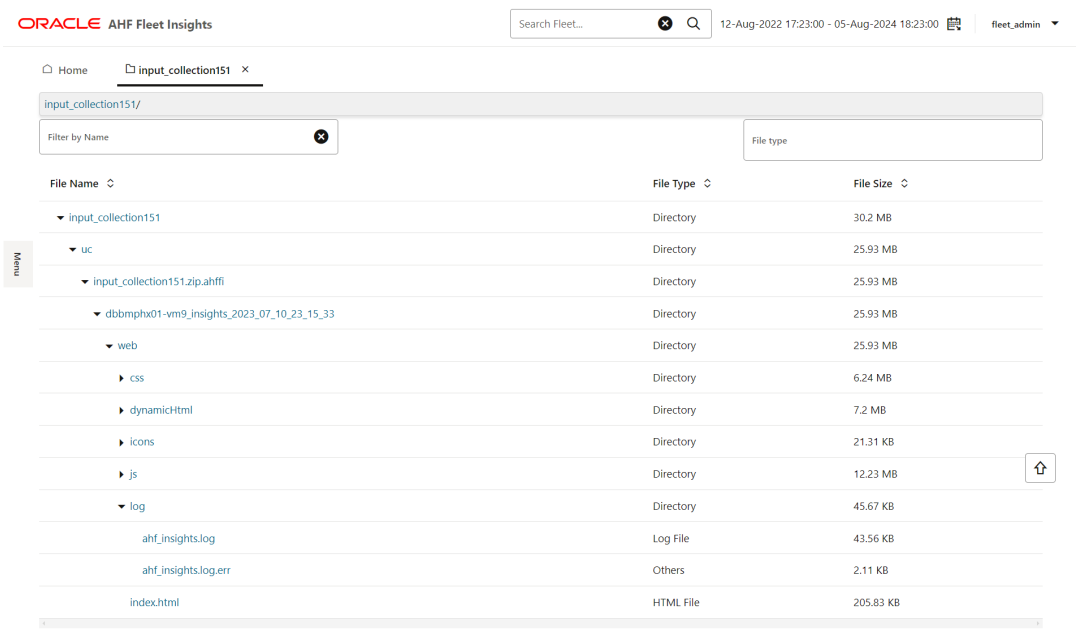
The File Viewer is available in the following areas:

- Timeline of Events (Table View)
- Drill-down pages in the Fleet Topology and Insights sections
- Other pages and sections throughout the platform when drilling down into specific collections or reports

How to Use the File Viewer

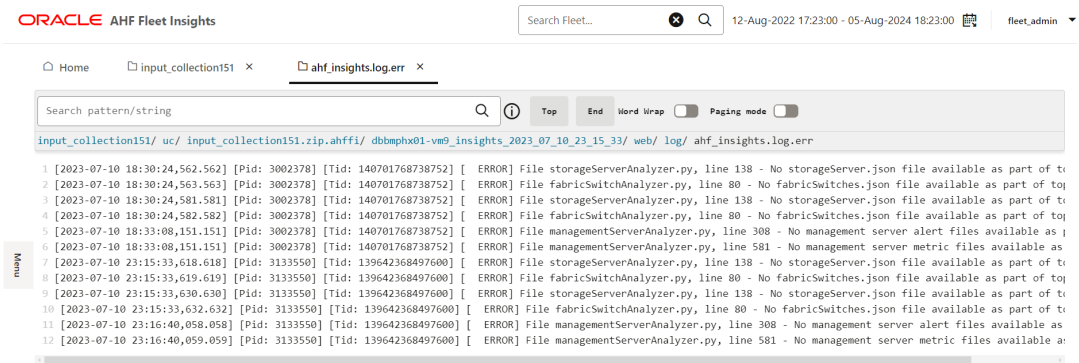
1. Click the Table view to see collection details in a tabular format.
2. Click the File Viewer icon associated with an Insights Report.
3. In the left-hand tree pane, expand the tree to locate an error event or specific log file.

Figure 3-36 File viewer



4. Click the desired error log to open and examine the details of the issue.

Figure 3-37 Error event log



3.2.6 Common User Interface Functionalities

- **Collapsible Menu Drawer:** Navigate to any section from any page using the collapsible menu drawer.
- **Help Page:** Access answers to FAQs on the help page.
  Click the drop-down list at the upper-right corner and select **Help**.
- **Update User Interface Login Password:** Update your user interface login password easily.
  Click the drop-down list at the upper-right corner and select **Update Password**.

Figure 3-38 Menu drawer

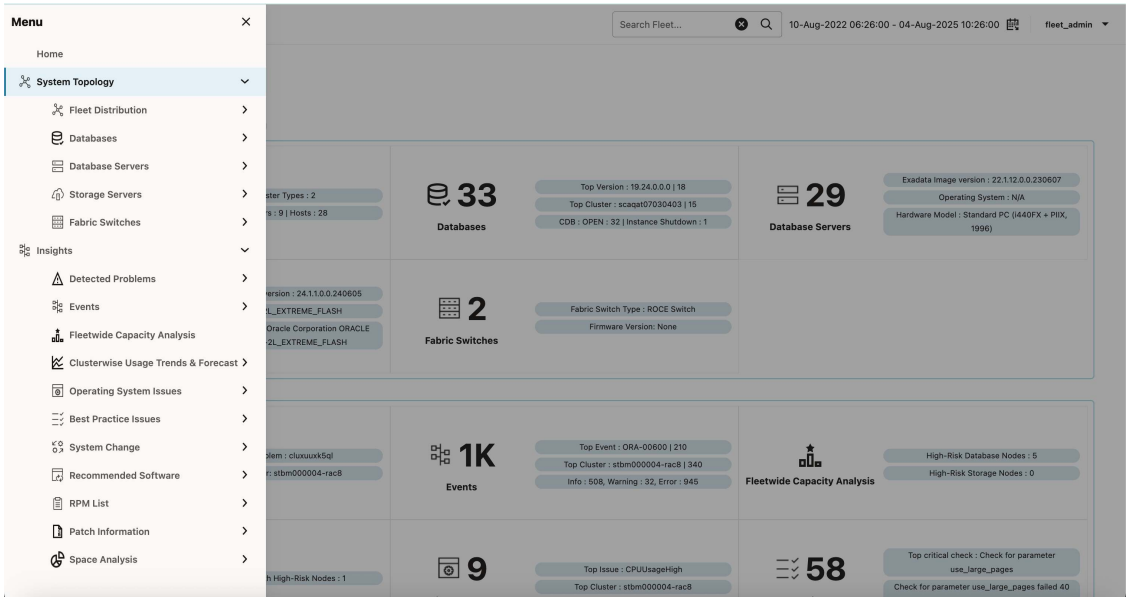
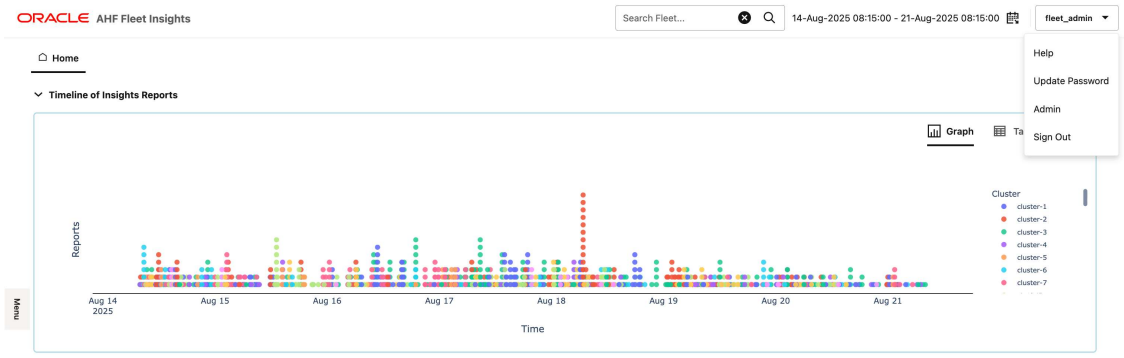


Figure 3-39 AHF Fleet Insights - Home - common functionalities



- **Graph and Table View:** Each section offers both graph and table views for data visualization.
- **Info Icon:** An info icon on each plot provides additional details about the data.
- **CSV Download:** Download the plot data as a CSV file for further analysis.
  Click the Actions menu (three dots) and select **Download CSV**.

Figure 3-40 AHF Fleet Insights - Home - common functionalities