21 Access Manager Dashboard

Access Manager Dashboard provides visual analytics of access related data based on the usage, performance, and events of Access Manager. Access Manager dashboard captures and filters the events. For more information, see (https://www.netiq.com/documentation/access-manager-45/product-overview/data/product-overview.html#analytics)"Analytics Server" in the Access Manager Overview.

This dashboard helps in visualizing the access patterns, tuning the policies, and getting insights about the usage of Access Manager in your environment. You can also monitor the real-time data access patterns to decide further actions.

You can use the Access Manager dashboard to perform the following:

- Displays visual analytics based on access patterns, logins, risk-based authentication, and usage of Access Manager. This helps the administrators to tune the system according to their needs.
- The trends of using devices, browsers, or applications in an organization.
- It provides the number of unique users who have logged in to Access Manager.
- It displays the graphs in a full screen (kiosk) mode, which helps in viewing Access Manager Dashboard in a data center. in addition, it does not time-out.
- It can display a snapshot of the historic data graphs based on the query for any specific time.

The Access Manager Dashboard displays the following graphs by default. You can customize the layout of the dashboard based on your requirements.

21.1 Improved Access Manager Dashboard

Following are a few improvisations from the earlier versions of the Access Manager Dashboard:

- Limited hardware requirement
- Updated third party libraries like Java and Tomcat
- Inbuilt geo-location identification capability. Administrator does not have to configure this capability.
- Custom dashboard creation and customizing view of graphs or visualization.

NOTE: The limitation is that user cannot generate or view the Reports. This feature is not supported with this version of Access Manager Dashboard. There is no offline support for dashboard and the existing events cannot be migrated. You also cannot upgrade to this dashboard, it works only as fresh install.

21.2 Access Manager Dashboard Overview

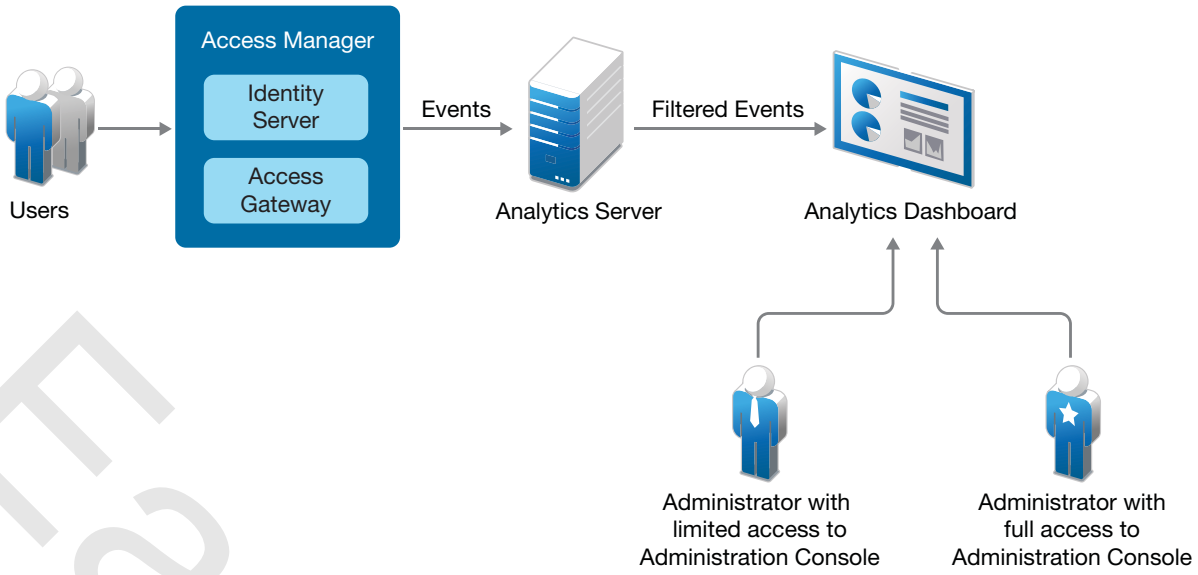
The Access Manager Dashboard comprises of the following sections to help you manage the data:

- **Recently viewed**: Displays the following actions.
  - **New**: Allows you to perform a new search.
  - **Save**: Allows you to save the performed search.
  - **Open**: Allows you to open a saved search.
  - **Share**: Allows you to share the search using **Snapshot** or **Saved objects**.
- **Visualize**: Helps you visualize the captured data in the dashboard using customizing view of the graphs.
- **Dashboard**: Provides visual analytics of access related data based on the usage, performance, and events of Access Manager.
- **Dev Tools**: Provides you the tools to help you interact with the data.
- **Management**: Helps you manage every resource present in the entire dashboard.

For more information about creating customizing views of the graphs, visualizing the content, and for managing and setting preferences, see Section 21.12.7, “Creating a Custom Dashboard,” on page 972.

21.3 Architecture

Access Manager Dashboard filters the events that are required for generating graphs. The following diagram displays the architecture of Access Manager Dashboard.



The Access Manager components generate events based on user access.

21.4 Migration

The current dashboard relies on Sentinel which makes it challenging to upgrade Elasticsearch, Logstash, and Kibana (ELK) components. There is also a limitation of memory and storage space. The re-architect-ed Access Manager dashboard is independent of SIEM server and makes use of logstash, which acts as the aggregator replacing the Analytic Server aggregator. This change means that the events are directly sent to ELK along with the SIEM server. The events are also processed by ELK. Therefore, there is no offline support for dashboard and the existing events cannot be migrated. You also cannot upgrade to this dashboard, it works only as fresh install.

Workflow

The syslog events are redirected to ELK which processes and stores them in Elasticsearch. These events are further visualized in Kibana.

You can also use Access Manager Dashboard along with Sentinel side by side for events to be captured in both. You have to configure two target servers based on the port number and event format to view these events. For more information, see (https://www.netiq.com/documentation/access-manager-45/admin/data/b63kqzr.html#b63kqzr).

21.5 Hardware Requirements for Analytics Server

The following is the minimum hardware requirement for Analytics Server:

For the demonstration purpose:

- CPU: 2 Cores
- Memory: 4 GB
- Hard disk: 50 GB

For a production environment:

- CPU: 4 Cores
- Memory: 16 GB
- Hard disk: Depends on the Access Manager login pattern for a day.

For more information about Analytics Server events, see Section 21.8, “Enabling Events for Each Graph,” on page 963.

	25000 logins per day	500000 logins per day	100000 logins per day
Number of days	**Disk space in GB**	**Disk space in GB**	**Disk space in GB**
1	0.058	0.115	0.23
10	0.575	1.15	2.3
30	1.725	3.45	6.9
60	3.45	6.9	13.8
90	5.175	10.35	20.7
120	6.9	13.8	27.6
180	20.99	41.975	83.95

21.5.1 Analytics Server Data Retention

The data stored in Analytics Server is retained in the local storage depending on the retention policy configured.

The default retention policy retains the audit events for 180 days. After 180 days, all data is purged from Analytics Server.

21.6 Who Can Access the Dashboard

The following users can view and manage Access Manager Dashboard:

- Access Manager administrators
- Users who are added in the configuration store of Administration Console.

NOTE: The policy container administrators (delegated administrators and policy view administrators) do not have access to Access Manager Dashboard.

To create a user in the configuration store, perform the following steps:

1. In Administration Console, click <user name> at the top right of the page and then click **Manage Roles & Tasks > Users > Create User**.
2. Specify the details in the mandatory fields.

3 **Context**: Specify the organization context.

   3a Click the object selector icon. The object selector browser displays the **Browse** and **Search** tabs.

   3b Select the **Browse** tab. Select **novell** from the Contents list.

4 **Password**: Specify and confirm the password.

   If you do not specify a password here, the user will log in without the password.

NOTE: This user can access only Access Manager Dashboard and does not have the rights to make changes in Administration Console.

21.7 Prerequisites for Viewing Graphs on the Access Manager Dashboard

To view the required data in Access Manager Dashboard, ensure that you perform the following before launching it:

1. Configure the settings on Administration Console. For more information about configuration settings, see Analytics Server Configuration (https://www.netiq.com/documentation/access-manager-45/admin/data/analytics-server-manageconf.html)
2. Enable the events for the required graphs. For more information about the events required for each graph, see Section 21.8, “Enabling Events for Each Graph,” on page 963.
3. (Conditional) If you want any specific user to view Access Manager Dashboard, then add the user to the configuration store. For more information about adding the user to configuration store, see Section 21.6, “Who Can Access the Dashboard,” on page 962.

21.8 Enabling Events for Each Graph

To view graphs on Access Manager Dashboard, you must enable the required events in Administration Console. The enabled events are sent to dashboard server that generates graphs for Access Manager Dashboard.

NOTE: If the events are not enabled, the graphs do not display any data.

To view the events for Identity Server, perform the following steps on Administration Console:

1 Click **Devices > [*Identity Server cluster name*] > Edit > Auditing and Logging**.

2 In the **Audit Logging** section, select **Enabled**.

To view the events for Access Gateway, click **Devices > [*Access Gateway server]* > Edit > Auditing** on Administration Console.

The following table provides the list of graphs with the required events:

Graph	Events
Unique Users Logged In	◆ Logins Consumed (Identity Server) ◆ Session Created/ Destroyed (Access Gateway)
◆ Identity Server Active Users ◆ Access Gateway Active Users ◆ Access Gateway Uptime ◆ Access Gateway Requests Trend ◆ Access Gateway Cache Utilization	Server Statistics To enable Administration Console to send the server statistics events to dashboard Server., perform the sub-steps of Step 5 of (https://www.netiq.com/documentation/access-manager-45/admin/data/b63kqzr.html).
Access Gateway Accessed Applications	◆ Session Created/ Destroyed ◆ Application Accessed
Access Gateway Logins	Session Created/ Destroyed
Identity Server Accessed Applications	◆ Federation Token Sent ◆ Federation Token Received ◆ Token Issued to Web Service ◆ OAuth and OpenID token Issued
Identity Server Logins	Logins Consumed
Pre Auth Risk Distribution	Risk Based Pre-authentication Action Invoked (Identity Server)
Post Auth Risk Distribution	Risk-based Authentication Action Invoked (Identity Server)
Geolocation of Users Logged In	◆ Logins Consumed (Identity Server) ◆ Session Created/ Destroyed (Access Gateway) ◆ Risk Based Pre-authentication Action Invoked (Identity Server) ◆ Risk-based Authentication Action Invoked (Identity Server)
◆ Most Used Browsers ◆ Most Used Endpoint Devices	◆ Session Created/ Destroyed (Access Gateway) ◆ Logins Consumed (Identity Server) ◆ Risk Based Pre-authentication Action Invoked (Identity Server) ◆ Risk-based Authentication Action Invoked (Identity Server)
Most accessed users	◆ Risk-based Authentication Action Invoked (If risk-based authentication is configured) ◆ Risk Based Pre-authentication Action Invoked (If risk-based authentication is configured) ◆ Logins Consumed (Identity Server)

Graph	Events
Client IP Addresses	◆ Risk-based Authentication Action Invoked (If risk-based authentication is configured) ◆ Risk Based Pre-authentication Action Invoked (If risk-based authentication is configured) ◆ Login Consumed ◆ Login Consumed Failure
Most Used Contracts	◆ Login Consumed ◆ Login Consumed Failure
Failed Authentications	◆ Login Consumed Failure

21.9 Viewing Data in Access Manager Dashboard

Access Manager Dashboard displays all the required Access Manager events in the form of graphs. You can view data in each graph only if the events are enabled for the graphs. For information about enabling events for each graph, see Section 21.8, “Enabling Events for Each Graph,” on page 963. The graphs are displayed based on the default data query and in the following modes:

- Section 21.9.1, “Real-time Data,” on page 965
- Section 21.9.2, “Historic Data,” on page 965

21.9.1 Real-time Data

By default, the real-time data mode displays the graphs with data for the last 7 days. Access Manager 5.0 onwards, the offline mode is not supported. You cannot migrate existing events in real-time and offline indices to this product.

You can add filters, or refresh the data after a specific time duration. You can view data from the time dashboard Server is configured till the present time, but the data that is older than 7 days will not be displayed.

For information about the actions that you can perform on a dashboard, see Section 21.12, “Managing Access Manager Dashboard,” on page 969

21.9.2 Historic Data

The historic data mode displays the graphs for the last 6 months or 180 days. The data is displayed for the time duration that you specify in the Access Manager Dashboard date range.

When you require the historic data, click **Access Manager Dashboard** > **Historical Dashboard** and specify the duration in the date range.

To return to the default dashboard to view the real-time data, click **Dashboard** > **Access Manager Dashboard**. For information about the actions that you can perform on the dashboard, see Section 21.12, “Managing Access Manager Dashboard,” on page 969.

21.10 Types of Graphs

The graphs represent the information about the business requirement of an organization. Access Manager Dashboard displays the following graphs in real-time and historic data modes by default:

21.10.1 Unique Users Logged In

This graph displays the user count based on the number of distinct users who are logged in to Identity Server and Access Gateway. This count is irrespective of how often they send login requests.

This graph helps to determine the number of distinct users who are logged in to web applications that are configured to use Access Manager.

21.10.2 Identity Server Active Users

This graph displays the data for the number of users who are logged in to Identity Server and is active at a specific interval.

This graph is helpful in analyzing how many users are authenticated within a specific time interval.

21.10.3 Access Gateway Active Users

This graph displays the data for the number of users who are logged in to Access Gateway and are active within a specific time interval.

This graph is helpful in determining how many users are authorized within a specific time interval.

21.10.4 Geolocation of Users Logged In

This displays the map with number of logged in users in specific geographical location. You can hover the mouse on each region to know the number of users who are accessing applications from that region.

This graph helps in identifying the location from where the most or the least number of users access applications.

NOTE: To display the user count for different countries, Analytics Server uses the IP address that is specified in the geolocation provider database. Hence, the data on the graph is dependent on the configured geolocation provider details.

21.10.5 Pre-Auth Risk Distribution

This graph displays a pie-chart with the distribution of the levels of risk (high, medium, and low). Each portion displays the risk percentage based on the number of sessions and percentage of the risk level that is configured in Identity Server.

These graphs help in determining the risks that are detected before authentication. Based on the risk level, administrators can change the policies to mitigate the risk.

21.10.6 Post-Auth Risk Distribution

This graph displays the pie-chart with the different levels of risk (high, medium, and low). Each portion of the pie-chart displays the risk percentage based on the number of sessions and percentage of the risk level that is configured in Identity Server.

These graphs help in mitigating the risk that are detected after authentication.

21.10.7 Identity Server Accessed Applications

This graph displays the name and the number of times the applications such as, federated applications, OAuth, and WS-Trust are accessed through Identity Server.

This graph helps in determining the most commonly used applications through Identity Server.

21.10.8 Access Gateway Accessed Applications

This graph displays the name of web applications with the number of times any web application is accessed through Access Gateway.

This graph helps in determining the most commonly used applications through Access Gateway.

21.10.9 Most Used Browsers

This graph displays the name of all the browsers with the comparison of their usage in the Access Manager environment.

This graph helps in determining the most commonly used browsers from which the requests are sent to applications that are configured with Access Manager.

21.10.10 Most Used Endpoint Devices

This graph displays the name of all the endpoint devices with the comparison of their usage in the Access Manager environment.

This graph helps in determining the most commonly used devices that users use for sending access requests.

21.10.11 Most Accessed Users

This graph displays the name of the top ten users who have got access by using Access Manager. **Other** includes the names of other users.

This graph helps in determining the users who frequently send requests to get access through Access manager.

21.10.12 Client IP Addresses

This graph displays the IP address of the client machines from which the requests are received frequently.

21.10.13 Most Used Contracts

This graph displays the name and number of the frequently used contracts.

This graph helps in determining the most commonly used contracts that are used for authentication.

21.10.14 Failed Authentications

This graph displays the number of failed authentications that occurred in a specific interval.

21.10.15 Identity Server Logins

This graph displays the number of login requests that are sent to Identity Server with respect to time.

This graph helps in determining the interval when there are too many user login requests sent to Identity Server.

21.10.16 Access Gateway Logins

This graph displays the number of login requests that are sent to Access Gateway with respect to time.

This graph helps in determining the interval when there are too many user login requests sent to Access Gateway.

21.10.17 Access Gateway Uptime

This graph displays the total time Access Gateway has been running since it was last started.

It helps in determining the time for next reboot.

21.10.18 Access Gateway Requests

This graph displays the number of requests that are sent to Access Gateway at a specific interval.

This graph helps in determining the load on Access Gateway server at each interval.

21.10.19 Access Gateway Cache Utilization

This graph displays the percentage of the used cache from the available cache for Access Gateway.

21.10.20 Access Gateway Devices

This graph displays the list of all Access Gateway servers with the health of each server.

21.10.21 Identity Server Devices

This graph displays the list of all Identity Provider servers with the health of each server.

21.11 Accessing the Dashboard

You can access the Access Manager Dashboard by using any of the following ways:

- **Administration Console Dashboard:** You can access Access Manager Dashboard from Administration Console either by clicking **Devices > Analytics Server > Access Manager Dashboard** or by clicking **Access Manager Dashboard** under **Admin Tasks**.
- **Access Manager Dashboard Web Page:** You can directly access the web page by using the https://<ip address of Analytics Server>:8445/amdashboard/login URL.

21.12 Managing Access Manager Dashboard

Access Manager Dashboard is the default dashboard.

You can modify and save it with a different name. You can create different dashboards as per your requirements.

You can perform the following tasks to manage dashboards:

21.12.1 Managing Layout of the Dashboard

You can customize the layout of a dashboard. Log into **Access Manager Dashboard** > **Create new dashboard** > **Add filter** > **Save**.

21.12.2 Exporting and Importing a Customized Dashboard

You can export the required customized dashboard to any location on the system, and then import it when you require it.

21.12.2.1 Exporting a Customized Dashboard

1. Log in to **Access Manager Dashboard**.
2. Click **Management > Saved Objects**.
3. Select the customized dashboard that you require to export and click export. The exported object is saved in the downloads.

21.12.2.2 Importing a Customized Dashboard

1. Log in to **Access Manager Dashboard**
2. Click **Management** > **Saved Objects**.
3. Click the Import icon.
4. Select the file you want to import.
5. Click **Done**.

21.12.3 Filtering Data to View Required Details

You can choose to view the required details by adding filters to the data that generates the graphs.

The following are the types of the time and data filter:

- Global graph filter. This filter allows you to make and view the changes that impact the whole dashboard. Example: When you add a filter for one graph, it is applied to all the graphs in the dashboard. For example, if you select a specific time range in the **Identity Server Active Users** graph, all the graphs will display the data based on the same time range. In the same way, whenever you select the level of risk, geolocation, or specific interval within a graph, all graphs display the data based on the selected level of risk, location, or time respectively.
- Individual graph filter. This filter allows you to customize the view of a specific graph. Example: For the **Unique Users Logged In** graph, you can click on the **...**at the top right corner to make graph specific changes.

  Using this filter, you can exclude the time graph from the global graph.

You can view the filters under **Access Manager Dashboard** > **Add filter**.

21.12.4 Managing Dashboard

This section covers the actions that you can perform on Access Manager Dashboard.

21.12.5 Adding or Modifying Refresh Time for Real-time Dashboard

The default value of refresh time interval is 30 seconds. You can change this default value and set a custom auto refresh interval. Ensure to save the dashboard after every change. You can disable auto refresh by selecting the **Stop** option against **Refresh every 30 seconds** field.

21.12.6 Creating Visualization

You can create a custom dashboard by creating a set of custom visualizations using Kibana and add them to the dashboard.

1. Click the Visualize icon  .
2. Click **Create new visualization**.
3. Select a visualization type. For example, let us use the **Horizontal Bar** chart. You can follow the same procedure for other types of visualization.
4. In the **New Horizontal Bar/Choose a source**, select **historic** or **realtime**.
5. Add a filter from the displayed options. Such as **@timestamp, @version** etc. You can also use the Kibana Query Language (KQL) or the Lucene query syntax for simplified query.
6. Select the dates from **Commonly used or Recently used** date ranges.
7. Set the refresh interval in seconds, minutes, or hours.

A graph is generated based on your selection. You can configure the chart to match your preferences. You can organize your data by using **Metrics** and **Buckets.**

- **Metrics**: This section has options to quantify the data with count, average, sum, max/min, etc.
- **Buckets**: This section has aggregations of data that are sorted according to your search criteria.

8 Click **Update.**You can visualize the created graph.

21.12.6.1 Saving a Visualization

After creating a visualization, click **Confirm Save**. Set a name.

You can also use an existing visualization to create a clone or a copy of that visualization.

1 Click **Visualize**. You can view all existing visualizations.
2 Select the required visualization.
3 Use the edit icon to customize the visualization.
4 Click the slider and **Save as a new visualization** with a different **Title**.
5 Click **Confirm Save**. If you wish to undo changes at this point, click **Cancel**.

21.12.7 Creating a Custom Dashboard

The custom dashboard allows you to view saved data based on the index selection on every visualization.

To create a custom dashboard, create a new and empty dashboard and then add the saved visualization or create a new visualization.

1 Click **Dashboard**.
2 Select **Create new dashboard**.
3 Save the dashboard with a name and description.
4 Click **Confirm Save**.
5 In the newly created dashboard, click **Edit**. The **Add** option is displayed.
6 Select the Visualization using **Add Panels**. This adds the visualization you require based on the options from the already saved visualizations. You get a confirmation that the panels you selected are added.
7 Click **Save**.
8 Set a name and description.
9 Click **Confirm Save**.

21.12.8 Customizing the Views of the Graphs

There are default graphs available in the dashboard. These have already been created using the available data in the elastic search. However, you can create custom visualization. For example instead of a line chart one can create a bar chart. Instead of displaying numbers for a unique user a visualization of Gauge can be created.

You can create custom dashboards by adding default visualization or any custom visualizations you have created. Consider the following sample use cases, to illustrate how you can customize the views of the default graphs available in the dashboard.

21.12.8.1 Use Case: Customizing Unique Users Logged In Graph

Let us consider you want to customize the view.

1. Click **Access Manager Dashboard > Visualize > Create new Visualization**.
2. Click **Edit** from the top page
3. Click **Options** from the right top corner of **Unique Users Logged In** graph.
4. Click **Edit Visualization**.
5. Click **Edit Filter**.
6. Click **Edit as Query DSL**.
7. Copy the **Elasticsearch Query DSL** to a notepad.

   You can also manually note the Metric information
   - Aggregation
   - Field
   - Custom Label
8. Click **New Visualization Gauge**. Select either **Historic** or **Realtime** dashboard.
9. Add the filter you had copied in the notepad using **Edit as Query DSL**.
10. Click **Save**.
11. In the **realtime**/**historic** data **Metrics** field.

    Select the following values:

    11a **Aggregation**: Select Unique Count

    11b **Field**: Select userName.keyword

    11c Apply changes.
12. Click **Save**. Provide the visualization with a title.

21.12.8.2 Use Case: Customizing View for Client IP Address Graph

Let us consider you want to customize the view from Vertical to Horizontal view of the chart.

1. Click **Access Manager Dashboard > Visualize > Create new Visualization**.
2. Click **New/Edit Visualization**
3. Click **Edit** from the top page
4. Click **Options** from the right top corner of **Client IP Address** graph.
5. Click **Edit Filter**.
6. Click **Edit as Query DSL**.
7. Copy the **Elasticsearch Query DSL** to a notepad.

   You can also manually note the Metric information
   - Aggregation

- Field
- Custom Label

8 Click **Create a New Visualization**. We want to create a **Horizontal Bar** chart instead of the already existing **Vertical Bar** chart

9 Select either **Historic** or **Realtime** dashboard.

10 Paste the filter you had copied in the notepad using **Edit as Query DSL**.

11 In the **Buckets** field of **X -axis**

12 Select the following values:

12a **Aggregation**: Terms

12b **Field**: SourceIP.keyword

NOTE: Add another **Bucket** specifying the above fields.

12c Click **Apply changes**.

13 Click **Save**. Provide the visualization with a title.

21.12.9 Discovering Data

You can explore the data by using Kibana's data discovery feature. This feature gives you access to every document in every index that matches the selected index pattern. You can submit search queries, filter the search results, and view document data for a set time limit.

Setting an index pattern is important to drill down, explore, and visualize the data. You can use both the Kibana Query Language (KQL) and Lucene query syntax for simplified query.

You can also view and share reports of the data search using **Snapshot** or **Saved objects**.

21.12.9.1 Viewing Index Pattern

View an index pattern to explore and visualize the data.

1 Click **Management** > **Kibana** > **Index Patterns**.

2 Select **realtime** or **historic** pattern. You can view all the index patterns along with the associated fields as recorded.

21.12.9.2 Viewing and Sharing Reports

After you create a visualization, click **Share**. This generates an iframe code as a short URL or long URL for saved object. You can share reports by using **Saved object** or by using a **Snapshot**.

To share a report with the data in **Discover** tab, perform the following steps:

1 Click **Discover**.

2 Save the index with a unique name for which you want to generate the data.

3 Click **Share**.

4 Generate the link as **Snapshot** using **Short URL** or **Saved object** to view or share the report.

NOTE: If you have a new and unsaved visualization that uses the snapshot link and you save that visualization and then create a snapshot link, the new snapshot link will be a reference to the initial object also adding the changes made on top of them. Hence, if you delete the object, the snapshot link will not work.

21.12.10 Logging Analytics Server Events

You can set the log level for each component to view the output in the respective log file location. Ensure to restart the service after making any change.

- Elasticsearch

  `/etc/elasticsearch/log4j2.properties`

  ```
  # log action execution errors for easier debugging
    logger.action.name = org.elasticsearch.action
    logger.action.level = debug
  ```

  NOTE: You can restart the service by using `rcnovell-elasticsearch restart` command.

- Logstash

  `/etc/logstash/logstash.yml`

  ```
  # ------------ Debugging Settings --------------
  #
  # Options for log.level:
  #   * fatal
  #   * error
  #   * warn
  #   * info (default)
  #   * debug
  #   * trace
  #
  log.level: info
  path.logs: /var/opt/novell/nam/logs/logstash
  #
  # ------------ Other Settings -------------
  #
  # Where to find custom plugins
  # path.plugins: []
  #
  ```

  NOTE: You can restart the service by using `rcnovell-logstash restart` command.

- Kibana

  `/opt/novell/nam/dashboard/webapps/kibana/config/kibana.yml`

  - Set the value of `logging.silent` to `true` to suppress all logging output.

    ```
    #logging.silent: false
    ```

  - Set the value of `logging.quiet`to `true` to suppress all logging output other than error messages.

```
#logging.quiet: false
```

NOTE: You can restart the service by using `rcnovell-kibana restart` command.

- Set the value of `logging.verbose` to `true` to log all events, including system usage information and all requests.

  ```
  #logging.verbose: false
  ```

Value	Description	Result
`logging.silent`	Boolean	Produces no logging output
`logging.quiet`	Boolean	Only log messages tagged with **error** or **fatal** tags, or errors are recorded by the API.
`logging.verbose`	Boolean	Log all the information including information about system usage and every request.
`logging.events`	Maps log types to the tags of the output. Supports * tag.	Provides access to every possible combination of logging output filtering. Also supports custom logging setup by use of plug-ins.