USER GUIDE v1.2

Last Updated: Sept 2022

Cyral Standard Dashboard: ELK

TABLE OF CONTENTS

I. Introduction

This Guide accompanies the Cyral Standard Dashboard for Elasticsearch Kibana (ELK). This dashboard ingests Data Activity Logs from all sidecars registered in your Control Plane. It includes a collection of pre-configured tables and graphs intended to reveal patterns in user and application access behavior. Note, the dashboard is accompanied by a pre-configured Discover view named 'Log Detail View' that formats your log data in an easy-to-read format.

II. Pre-Requisites

1. Sidecars must be configured to send logs to the relevant ELK instance. Detailed instructions are provided here: https://cyral.com/docs/integrations/siem/elk

2. Some tables and visualizations in the dashboard require SSO User or Group information to display data correctly. To enable this, your IdP provider should be integrated with the Control Plane, and users should be using Cyral to connect to the database(s).

III. Installation Instructions

1. Cyral Customer Support will provide you two exported Kibana files:
    - Standard Dashboard
    - Log Detail View (Discover View)

2. Login to your Kibana instance. Make sure you are logged into the tenant that will be accessible to all users who need access to the dashboard once it's installed.

   For example, if you have the default Kibana tenants of **Private** and **Global**, be sure you are logged into the **Global** tenant when you install the dashboard. To read more about tenants in Kibana, see Kibana Multi-Tenancy.

3. From the navigation menu on the left-hand side, click on Stack Management located under the Management heading.

4. From the resulting menu, click on Saved Objects located under the Kibana heading.

5. On the resulting Saved Objects page, click on the Import link in the upper right corner of the page.

6. On the resulting import saved objects page:
    a. Click to browse and locate the ndjson file provided in Step 1
    b. Make sure that **automatically overwrite all saved objects?** is enabled
    c. Click the Import button
7. You should receive an 'Import Successful' message. Once received, click the Done button.

8. You can confirm that the dashboard is available by navigating to the Dashboards page or validate the Log Detail View by selecting the 'open' button from the Discover page.

IV. How to Customize Your Dashboard

If you'd like to make changes to the dashboard file Cyral provides, clone the dashboard, and make changes to the duplicate file.

- If you installed the dashboard file directly, this guarantees future re-uploads do not override your customized version.

V. Guide to Graphs and Tables

SYSTEM SUMMARY

Chart or Table Name	Notes
Number of Repositories	Conveys how many repositories contributed to data visible in the dashboard. This number does not necessarily reflect the number of repositories registered in your Control Plane.
Number of Sidecars	Conveys how many sidecars contributed to data visible in the dashboard. This number does not necessarily reflect the number of sidecars registered in your Control Plane.
Number of Active Database Accounts	Conveys how many individual repository accounts contributed to data visible in the dashboard. This number does not necessarily reflect the number of database accounts registered in your Control Plane.

Total Connections Over Time Period	Displays count of connections for the time period specified in your filters.
Number of Active Users	Number of unique users captured in the logs. This value reflects individual users who logged in via BI Tools (i.e. Looker, Tableau) if Service Account Resolution has been configured.
Number of Active SSO Groups	Number of unique SSO groups captured in the logs. This value reflects the SSO Groups of individual users who logged in via BI Tools (i.e. Looker, Tableau) if Service Account Resolution has been configured.
Number of Users in each SSO Group	Conveys number of users from each SSO Group that accessed one or more repositories during the time range specified by the dashboard filters.
Repository Connections by SSO Group	Conveys number of unique connections from users--classified by SSO Group—for the time range specified by the dashboard filters.
Approvals by Approver	Displays all approvals; results are paginated after the 10 most recent approvals.
Approvals by Repository	Displays all approvals; results are paginated after the 10 most recent approvals.

DATA ACTIVITY

Chart or Table Name	Notes
Repository Connections	Displays total number of connections and total number of queries to each repository across the timeframe specified. Average Query Size in Bytes calculated based on timeframe filter applied.

Repository Traffic Across Time (Queries)	Displays trends in total number of queries submitted to each repository. These queries may have been from individual users or applications.
Repository Traffic Across Time (Connections)	Displays trends in total number of connections to each repository. These connections could have been made by individual users or applications.
Data Most Frequently Accessed	Displays data assets registered in your Data Map in order of the most frequently accessed. Results are paginated after ten rows. Notes: • A Data Map is required for this table to populate data. • This table requires a value for the SSO User/Group name. Application access data is excluded from this table.
Data Access Distribution	Shows which data assets registered in your Data Map are accessed the most frequently. This pie chart displays all data assets for all repositories unless filters are applied.

SECURITY ACTIVITY

Chart or Table Name	Notes
Suspicious Activity	Describes frequency and types of Suspicious Activity happening in each of your repositories. Suspicious Activity includes: • Port Scans • Authentication Failures • Cyral Policy Triggers
Suspicious Activity Trends	Conveys frequency of Suspicious Activity for each of your repositories.

REPOSITORY PERFORMANCE

Chart or Table Name	Notes
Summary	Displays statistics based on the timeframe assigned in your global filters. Duration metrics are calculated based on the difference between first query seen and last query seen for a given connection.
Query Error Rates by Repository	Displays the count and percentage of queries with errors.
Trend of Errors Over Time	Displays trends in number of errors across time for each repository.

VI. Appendix A – Data Activity Logs Taxonomy

Cyral maps relevant query language from all logs coming from your various repositories to these central Activity Terms. These terms are then grouped into Activity Categories for ease of analysis and visualization in your dashboards. If you'd like to see the complete mapping between Activity Terms and database query statements, please contact Customer Support.

Activity Category	Activity Term	Notes
Data Reads	Select Data	*Example:* SELECT (PostgreSQL) and FIND (MongoDB) both map to the term Select Data.
	Select Data Bulk	
	Select Data	
	Export Data Bulk	
	Analyze Statistics	
	Explain	

Data Changes	Insert Data	
	Update Data	
	Delete Data	
	Merge Data	
	Copy Data	
	Truncate Data	
View Changes	Create View	
	Alter View	
	Drop View	
Schema Changes	Create Table	
	Alter Table	
	Delete Table	
	Rename Table	
	Create Schema	
	Modify Schema	
	Delete Schema	
	Annotate Schema	
	Create Collection	*Not all Activity Terms are relevant to every repository type.*
	Alter Collection	
	Delete Collection	
	Create Bucket	
	Delete Bucket	
Query Flow Operation	Begin Transaction	
	Cursor Operation	
	Variable Declaration	
	Clear Session State	
	Execute Stored Procedure	
	Listen	
	Notify	
	Prepare Statement	
	Release Savepoint	
	Rollback Transaction	
	Commit Transaction	
	Savepoint	
Repo Changes	Create Database	
	Update Database	

	Annotate Database	
	Delete Database	
Access Changes	Create User Account	
	Modify User Account	
	Delete User Account	
	Create Group	
	Modify Group	
	Delete Group	
	Create Role	
	Modify Role	
	Delete Role	
	Modify Access	*Not relevant for PG repositories*
	Grant Access	
	Revoke Access	
Privileged Commands	Modify Log	
	System Change	
	Functionality Change	
	Alter Trigger	
	Create Trigger	
	Delete Trigger	
	Backup	
	Restore	*Not relevant for PG repositories*
	Create Access Method	
	binlog	*Not relevant for PG repositories*
	Flush	*Not relevant for PG repositories*
	Kill	*Not relevant for PG repositories*
	Deadlock	*Not relevant for PG repositories*
	Load Index Into Cache	*Not relevant for PG repositories*
	Reset	*Not relevant for PG repositories*
	Reset Persist	*Not relevant for PG repositories*
	Startup	*Not relevant for PG repositories*
	Restart	*Not relevant for PG repositories*
	Shutdown	*Not relevant for PG repositories*