USER GUIDE v1.1

Last Updated: June 2022

Cyral Standard Dashboard: Splunk

TABLE OF CONTENTS

I. Introduction

This Guide accompanies the Cyral Standard Dashboard for Splunk. This dashboard ingests Data Activity Logs from all sidecars registered in your Control Plane. It includes a collection of pre-configured tables and graphs that display patterns in the ways users and applications access your data.

The Cyral Log Detail View accompanies the Standard Dashboard file. This detail view includes a set if pre-configured filters on your raw log data that complement the visualizations in the dashboard, and that make it easy to analyze your data.

II. Pre-Requisites

Many 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. Dashboard Setup Instructions

1. Configure the Splunk Integration in your Control Plane using the instructions provided in Cyral Docs: Send Cyral logs to Splunk.

2. Once logs are being sent to Splunk, install the Cyral App either by uploading the file provided directly by Cyral customer support, or by downloading the app from Splunkbase using one of the below instructions (for a distributed deployment, this app should be installed on Search Heads):

    a. Install an add-on in a single-instance Splunk Enterprise deployment - Splunk Documentation
    b. Install an add-on in a distributed Splunk Enterprise deployment - Splunk Documentation

3. Once the installed, modify the Cyral Logs event type that the Cyral app creates by changing the search string to match whatever search criteria is used to locate Cyral logs in your Splunk environment. Additional details regarding editing event types can be found at the below URLs:

    a. Define event types in Splunk Web - Splunk Documentation
    b. Configure event types in eventtypes.conf - Splunk Documentation

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.
- If you installed the dashboard from Splunkbase, Cyral updates to the Standard Dashboard will be pushed automatically. Any changes you made to the dashboard will be overridden at that time.

V. Guide to Graphs and Tables

NOTE ON FILTERS

Filters applied at the top of the dashboard apply to all tables and graphs in the dashboard.

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 Registered Repository 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.

Average Connections per Timeframe	The Cyral Standard Dashboard uses the Splunk out-of-the-box configuration to calculate this field. The value is calculated differently depending on what value you have for the Timeframe filter. For information on how this field could be adapted to show average connections per hour, broken out by hour, see this resource.
Connection Activity by Geography	Shows IP address location of all connections to all repositories (unless filters are applied).
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.
Recent Access Approvals	Displays all approvals; results are paginated after the 10 most recent approvals.
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.
Activity Category by SSO Group	Displays which query types are used most frequently by various SSO Groups. See **Appendix A** for details on the specific queries grouped into the “Activity Categories” listed.
Trends in User Activity	Displays trends in query usage across various repos.

SECURITY ACTIVITY

Chart or Table Name	Notes
Privileged Commands by Users	See Appendix A for a list of queries categorized as a “privileged command.”
Privileged Commands Trends	Conveys how many users from various SSO groups executed privileged commands/queries.
Access Changes by Users	See Appendix A for a list of queries categorized as an “Access Change.”
Access Changes Trends	Conveys how many users from various SSO groups executed access change commands/queries.
Suspicious Activity	Describes frequency and types of Suspicious Activity happening in each of your repositories. Suspicious Activity includes: • Port Scans • Full Table 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.
Activity Categories with Highest Error Rates	Displays the number of queries with errors across the timeframe specified in your global filters.
Slowest Queries	Displays top ten slowest queries. **Note:** The Data Table/Field only populates if a query was for data registered in your Data Map.

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*