ZUBIN™

DATA DYNAMICS

Technical Datasheet

Personas and Capabilities

Introduction

This document outlines the various personas supported by Zubin, the specific capabilities available to each persona, and the process for assigning these personas to users via the Control Panel. This ensures that users have the appropriate access and functionalities tailored to their roles.

Personas and Capabilities

Security Officer

Capabilities

1. **Dashboard**
   a. Reviews the overall security posture calculated by weighing against the threshold and scores assigned to the data collected during the various metadata and content-based scans conducted in the product.
   b. Breaks down this security posture into issues raised against Access Control, Data Retention, Data Sensitivity, Data Redundancy.
   c. Provides a geographical view of security risks and a categorized view of sensitivity labels assigned to various files.
   d. Reviews the progress of tasks raised against the risks assigned to various stakeholders.
   e. Updated with risk analysis, remediation, and action.

2. **Alarm Configuration**
   a. Reviews the threshold, weightages, and scores assigned to various security risk categories.

3. **Data Workflow**
   a. Review the data orchestration pipelines created in the product.

4. **Data Policy**
   a. Reviews the various data management policies created in the product.

5. **Data Store**
   a. Reviews the data storage information added in the product.

Infrastructure Officer

Capabilities

1. **Dashboard**
   a. Reviews the overall storage efficiency calculated by weighing against the threshold and scores assigned to the data collected during the various metadata and content-based scans conducted in the product.
   b. Breaks down this efficiency posture into issues raised against Data Retention, Data Redundancy, Cold Data, and Orphaned Data.
   c. Provides a geographical view of accessible data and a categorized view of ROT (Redundant, Obsolete, Trivial) data.
   d. Reviews the progress of tasks raised against the storage optimization activity assigned to various stakeholders.
   e. Updated with data usage analysis, remediation, and action.

2. **Alarm Configuration**
   a. Reviews the threshold, weightages, and scores assigned to various storage inefficiency categories.

3. **Data Workflow**
   a. Reviews the storage optimization pipelines created in the product.

4. **Data Policy**
   a. Reviews the various storage management policies created in the product.

5. **Data Store**
   a. Reviews the data storage information added to the product.

Policy Administrator

Capabilities

1. **Dashboard**
   a. Same as Security Officer

2. **Alarm Configuration**
   a. Reviews and configures the threshold, weightages, and scores assigned to various security risk categories.

Click here for a demo

b. Sets rules, thresholds, notifications, and stakeholders.
c. Creates and executes the Data Workflow.

3. **Data Workflow**
   a. Reviews, configures, shares, deletes, triggers, and schedules data orchestration pipelines created in the product.

4. **Defines data workflows tied to policies.**
   a. Conducts data discovery, metadata analysis, content analysis, statistical sampling, tagging, and labelling.
   b. Implements data minimization, delete, archive, risk remediation, and quarantine.
   c. Manages permissions.
   d. Conducts data migration (Migrate, File to File, Object to Object, File to OneDrive, Transform, File to File, Object to Object).

5. **Data Policy**
   a. Reviews, configures, shares, deletes, triggers, and schedules the various data management policies created in theproduct.

6. **Data Store**
   a. Same as the Security Officer

Storage Administrator

Capabilities

1. **Dashboard**
   a. Same as the Infrastructure Officer

2. **Alarm Configuration**
   a. Same as the Infrastructure Officer

3. **Data Workflow**
   a. Same as the Infrastructure Officer

4. **Data Policy**
   a. Same as the Infrastructure Officer

5. **Data Store**
   a. Reviews, configures, shares, and deletes the data storage information added in the product.
   b. Creates data stores (SMB, NFS, S3, One Drive).

Data Owner

Capabilities

1. **Dashboard**
   a. Views of security and storage for the files where they are either the owners or custodians.
   b. Updated with risk and data usage analysis, remediation, and action.
   c. Overall Risk Score, Access Control, Data Redundancy, Data Sensitivity, Data Retention, Cold Data, Orphan Data, Risk Mitigation, Carbon Footprint Analysis, Data Sensitivity by Department, Location, Datacenter, and Data Owner, File Distribution by Type, Location, and Age.

2. **Self-service data management and actionability**
   a. Conducts data discovery, metadata analysis, content analysis, and statistical sampling.
   b. Implements data minimization, delete, archive, risk remediation, and quarantine.
   c. Manages permissions.
   d. Conducts data migration (Migrate (SMB, NFS, S3, and One Drive), File to File, Object to Object, File to OneDrive, Transform, File to File, Object to Object).

System Administrator

Capabilities

1. **User Management**
   a. Adds, removes, and manages user accounts within the system.
   b. Assigns or revokes user roles and permissions.
   c. Integrates with the organization's AD for user synchronization.

2. **Role Management**
   a. Creates, modifies, and deletes roles within the system.
   b. Assign capabilities to roles to tailor access and functionalities.
   c. Maps AD roles to system roles to streamline access control.
   d. Assigns or removes roles assigned to each user. These roles are not auto-assigned based on the information from AD.

3. **Data Engine Management**
   a. Configures and maintains the data engines used for metadata and content scanning.
   b. Monitors performance and optimizes engine configurations.
   c. Manages engine updates and upgrades.

4. **License Management**
   a. Manages license allocation and ensures compliance with license terms.
   b. Generates license usage reports and monitors license consumption.
   c. Handles license renewals and updates.

Persona Assignment from Active Directory

Integration Overview

Zubin integrates with the organization's Active Directory (AD) to automate the sync of users with the product based on AD query. This integration ensures that users receive appropriate access and capabilities based on their roles within the organization.

Click here for a demo

Steps for Persona Assignment

1. **AD Synchronization**
   a. Synchronize user information from the organization's AD to the enterprise product.
   b. New users are added on a 24-hour frequency and updates to existing users are processed every 12 hours.

2. **Role Mapping**
   a. System administrators can assign or remove the roles assigned to each user.
   b. These roles are not auto-assigned based on the information from AD, allowing for manual control over role assignments.

3. **Automatic Assignment**
   a. Implement automatic persona assignment based on the defined mapping rules.
   b. Ensure that changes in AD (e.g., role changes, new hires) are reflected in the enterprise product.

4. **Manual Overrides**
   a. Allow administrators to manually assign or override personas for specific users if necessary.
   b. Ensure that manual changes are logged and audited for compliance.

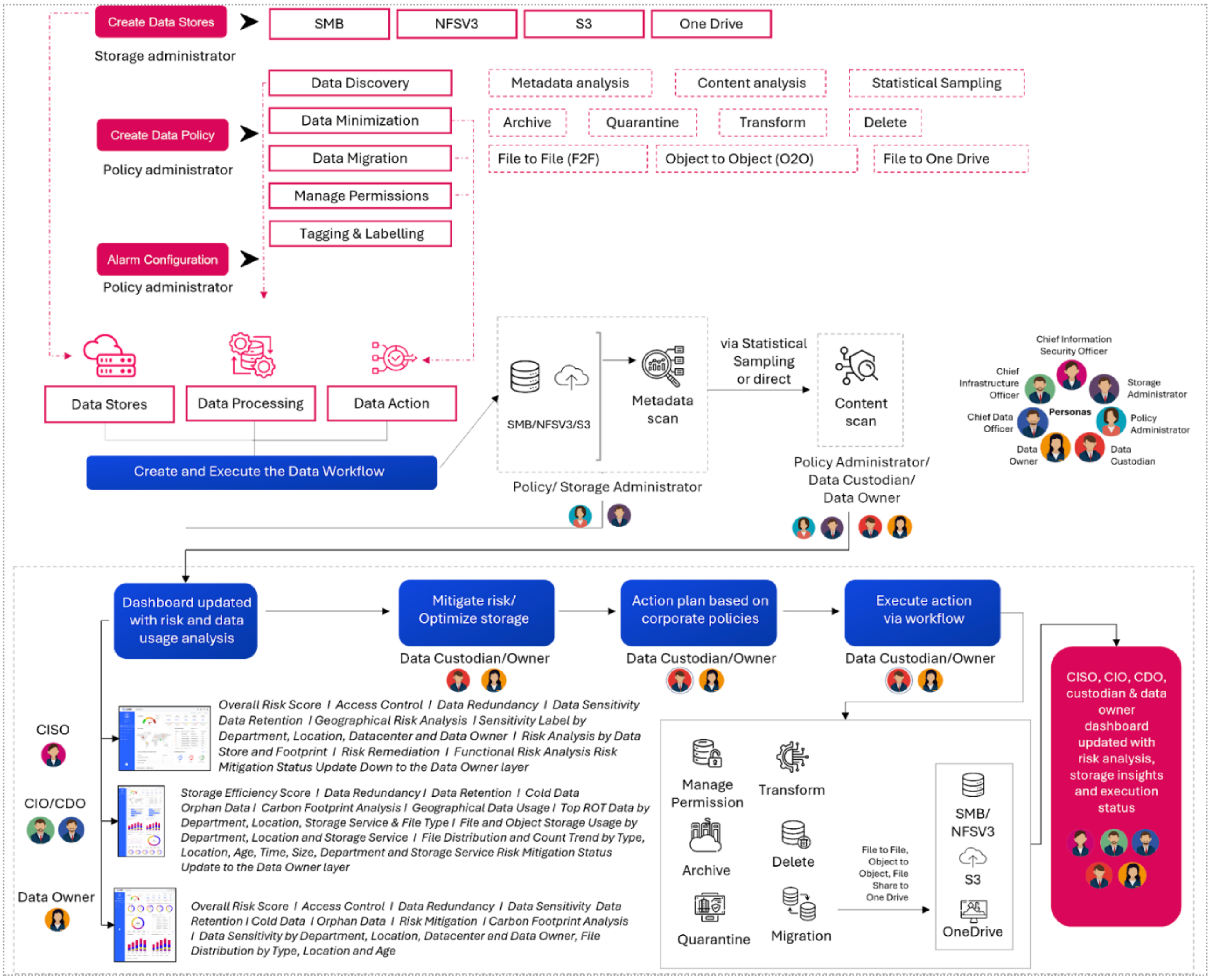
Detailed Workflow

1. **User Login**
   a. When a user logs into the enterprise product, the system checks their AD credentials and retrieves their attributes.

2. **Persona Determination**
   a. Based on the role(s) assigned in the product for the user, related personas and their resulting features are made available.
   b. Users with multiple personas can switch between the personas under the same session without needing to re-login.

3. **Capability Activation**
   a. The system activates the capabilities associated with the assigned persona(s).
   b. Users gain access to the features and functions specific to their role.

4. **Ongoing Synchronization**
   a. Periodically synchronize with AD to ensure that any changes (e.g., role updates, user additions) are reflected in the persona assignments.
   b. Update user capabilities as necessary based on changes in AD attributes.



Create Data Stores
Storage administrator
SMB
NFSV3
S3
One Drive

Create Data Policy
Policy administrator
Data Discovery
Data Minimization
Data Migration
Manage Permissions
Tagging & Labelling
Metadata analysis
Content analysis
Statistical Sampling
Archive
Quarantine
Transform
Delete
File to File (F2F)
Object to Object (O2O)
File to One Drive

Alarm Configuration
Policy administrator

Data Stores
Data Processing
Data Action
Create and Execute the Data Workflow

SMB/NFSV3/S3
Metadata scan
Policy/ Storage Administrator
via Statistical Sampling or direct
Content scan
Policy Administrator/ Data Custodian/ Data Owner

Personas
Chief Information Security Officer
Storage Administrator
Policy Administrator
Data Custodian
Data Owner
Chief Data Officer
Chief Infrastructure Officer

Dashboard updated with risk and data usage analysis
Mitigate risk/ Optimize storage
Data Custodian/Owner
Action plan based on corporate policies
Data Custodian/Owner
Execute action via workflow
Data Custodian/Owner

CISO

Overall Risk Score I Access Control I Data Redundancy I Data Sensitivity Data Retention I Geographical Risk Analysis I Sensitivity Label by Department, Location, Datacenter and Data Owner I Risk Analysis by Data Store and Footprint I Risk Remediation I Functional Risk Analysis Risk Mitigation Status Update Down to the Data Owner layer

CIO/CDO

Storage Efficiency Score I Data Redundancy I Data Retention I Cold Data Orphan Data I Carbon Footprint Analysis I Geographical Data Usage I Top ROT Data by Department, Location, Storage Service & File Type I File and Object Storage Usage by Department, Location and Storage Service I File Distribution and Count Trend by Type, Location, Age, Time, Size, Department and Storage Service Risk Mitigation Status Update to the Data Owner layer

Data Owner

Overall Risk Score I Access Control I Data Redundancy I Data Sensitivity Data Retention I Cold Data I Orphan Data I Risk Mitigation I Carbon Footprint Analysis I Data Sensitivity by Department, Location, Datacenter and Data Owner, File Distribution by Type, Location and Age

Manage Permission
Transform
Archive
Delete
Quarantine
Migration
File to File, Object to Object, File Share to One Drive
SMB/ NFSV3
S3
OneDrive

CISO, CIO, CDO, custodian & data owner dashboard updated with risk analysis, storage insights and execution status

Your next chapter of success awaits; let's write it together with Zubin. Click here for a demo