VERITAS

The Benefits of Inferred Ownership

Available in Veritas Data Insight.

White Paper | April 2022

Contents

Overview

Who is accountable if some important data is deleted, if retention or access privileges are set incorrectly? If you don't know the proper owner and you're a business process owner or in IT, ultimately it falls on your shoulders to ensure proper access management and governance decisions are done across the data within your data infrastructure. Adding to the complexity:

- There can be billions of files spread across the organization
- Users come and go which can lead to files having no valid owner (orphaned)
- Some file systems automatically assign ownership to Administrator or Administrator Group

Instead of being able to make the appropriate people accountable for the data it falls all on IT's shoulders who is challenged to understand the value or risk of individual files. This can lead to things like inappropriate access to sensitive data and keeping data indefinitely resulting in increasing cost and risks.

What you need is a way for IT to distribute responsibility appropriately. This requires knowledge of who should be the owner or custodian of each item of data and should be responsible for effective remediation. Remediation can include setting the proper access privileges, deleting stale data and setting appropriate retention.

Data Insight solves this challenge by determining inferred ownership of data and by providing the ability to assign data custodians on specified paths, shares and files for the purposes of remediation and permission allowance.

Traditionally ownership is assigned to the file creator however, this may no longer be a current employee or an active user of this data. Moreover, it's a tedious job for administrators to maintain correct ownership information on the file system and more often than not, the information is stale. Rather than assigning ownership to the creator, Data Insight uses algorithms that look at user activity and behavior on files as well as accessibility events to infer ownership of files.

Inferred data ownership can be viewed in the Data Insight management console, as seen in Figure 1, or through reporting.

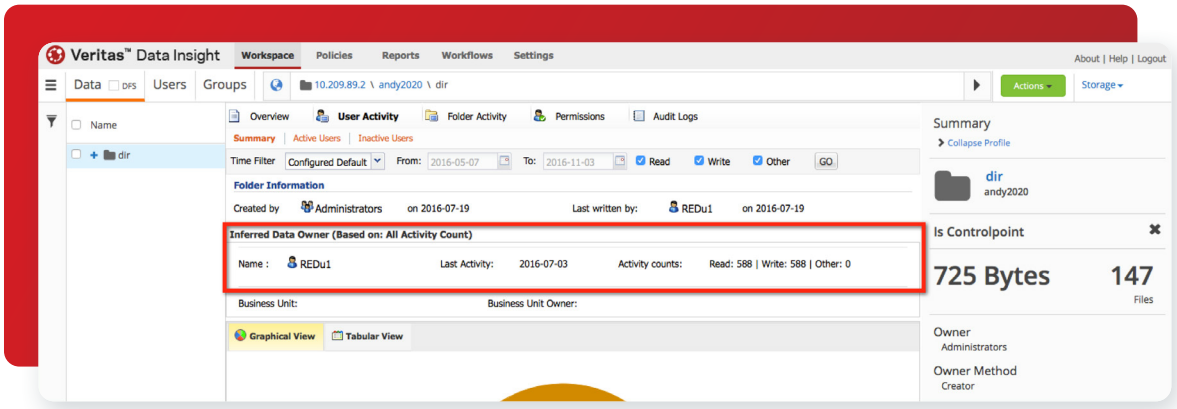


Figure 1 - Management Console View.

Reports

- Access summary for paths report
- Data Aging Report
- Inactive folders report
- Path permissions report
- Consumption by folders report
- Custom report (Inferred owner report)

Custodians and Owners

When determining who should be responsible for managing data this is typically grouped into two main categories, the data custodial and the data owner. A data custodian is a person who is accountable for managing specific data and ensuring it meets business rules for storage and security. The custodian typically owns large sets of data for a number of projects at a database, folder or share level. An inferred owner who is a person that is typically responsible for individual files that they commonly use. The files an inferred owner uses maybe inside folders managed by a data custodian.

Inferred Ownership

By default, Data Insight enables rules-based inference of data owners based on actual usage of the files or folders. Essentially, the most active user on a file or folder is considered the inferred data owner for purposes of efficient remediation and data management. This means the data owner can be a line manager in the business unit, the head of a department, or an information security officer rather than the person who actually created the file. Inferred ownership can also be set by a global policy or by setting a custodian.

Note: Inferred ownership is used solely within Data Insight for remediation purposes, no actual changes are made to the data properties themselves.

Inferred Ownership with Workspace Data Ownership Policy

There is a global workspace data owner policy which infers the most likely owner when configuring workflows and reports.

Inferred ownership can also be defined by a global workspace policy using any of the following criteria:

- The number of read events on the file or folder
- The number of write events on the file or folder
- The cumulative count of all activities
- The file or folder creator
- The user account which last access the file or folder
- The user account which last modified the file or folder
- Owner of the parent folder

A global policy can be defined by any of the criteria above, or combination of criteria, which can be assigned priorities for ownership computations. For example, a policy can be defined to count the number of read events and last modified events to determine the data owner.

If Data Insight is not able to compute the owner based on any of these criteria, the owner of the immediate parent folder is displayed as the owner of the file or folder.

The criteria that is defined in the global workspace data owner policy are also considered for determining the data owner when configuring reports and workflows. However, you can choose to override the policy when you create an Inferred Data Owner report.

Assigning Custodians for Inferred Ownership

As mentioned, the inferred owner can be determined by access patterns of individuals actually working on the files/project. It can also be assigned to a custodian, which is usually a director or leader of a business unit who is in charge of specific data.

Data Insight allows custodian assignments for files in a specific path. To do this, you can define your own set of criteria and priority for Data Insight to infer the appropriate data owner that it will assign as custodian for all files within a selected path. Custodians can be assigned manually, or in bulk by assigning via a csv.

Management Console View of Inferred Ownership

The Workspace Tab of the Data Insight Management Console, seen in Figure 2, allows you to view detailed information about the access patterns for files, folders, and web applications. You can view the attributes of a file or a folder located on a filer, SharePoint site, or web application by clicking the "Expand Profile" link located in the Navigation pane on the right of the screen.

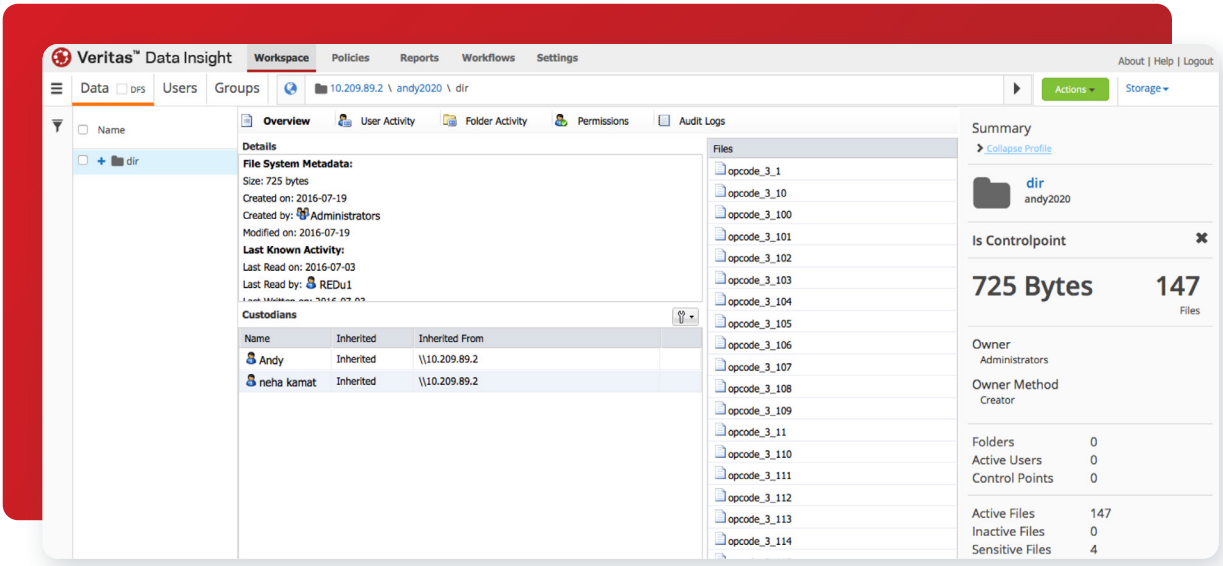


Figure 2 - Workspace View.

This is where you to see the concept of inferred data ownership to give administrators a sense of data ownership. The data may have a "Created By' attribute which is not always indicative of the data's true owner.

By navigating to the User Activity tab, seen in Figure 3, you can see who created the file, who and when it was last written, and finally the inferred owner. The inferred owner's name, last activity and activity counts are displayed.

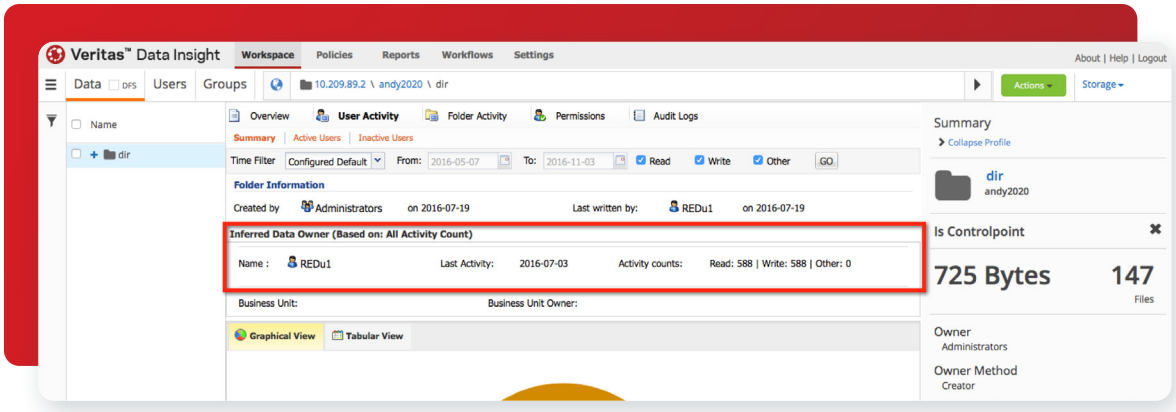


Figure 3 - Inferred Owner.

By navigating to the overview tab of the share or folder, seen in Figure 4, you can see who the custodian of the data is, and you can assign custodians.

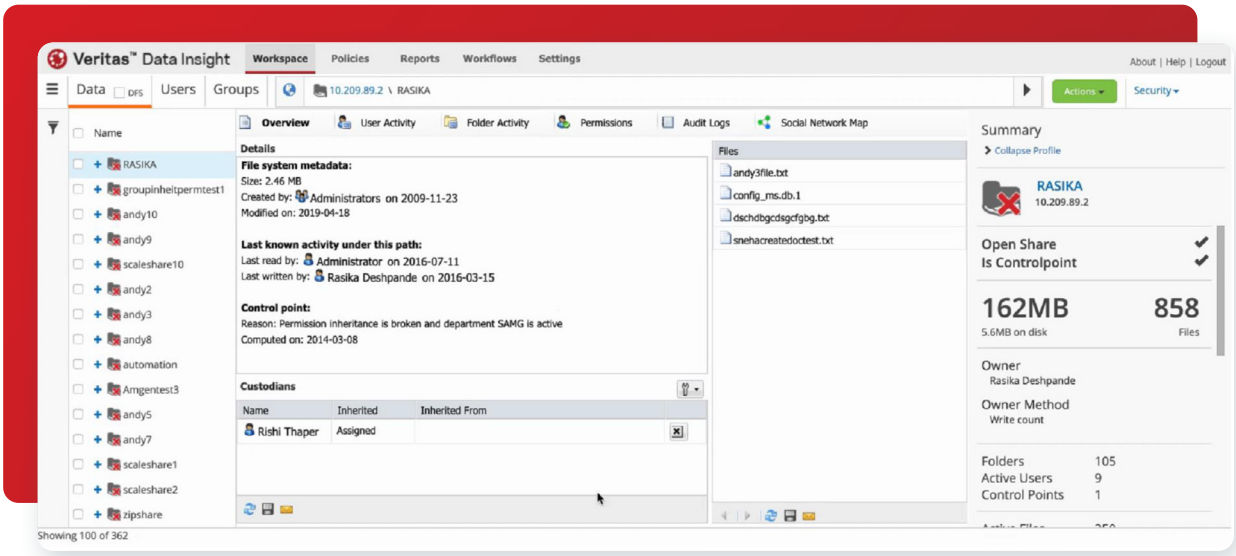


Figure 4 – Custodian.

Ownership Reports

Data Insight includes reporting capabilities to make it simple to see information about users who are responsible for remediation on assigned data locations. There are two default reports included within Data Insight that provide this information, the data custodian summary report and an inferred owner report.

Data Insight also allows users to create their own customized reports if required. Any number of reports can be generated each with different input parameters. Reports can be output in CSV, PDF, and HTML formats.

Data Custodian Report

The Data Custodian Report provides detailed information about the assigned custodians including:

- The name of the custodian
- The account name of the custodian, for example, user@domainname.com
- The data source, for example a filer or web application, on which there is a custodian assignment
- Access path - the physical path on which the user is assigned as custodian
- DFS path - the DFS path on which the user is assigned as custodian
- The status of the selected user in the directory service. For example, active, disabled, or deleted
- Information about attribute values

Inferred Owner Report

The Inferred Owner report provides a summary of inferred owners on the specified paths. The owners are determined based on the activity on the files during the specified time period. The Inferred Owner report provides the following information:

- The name of the share or site collection
- DFS path - the DFS path on which the inferred owner is assigned as custodian
- The name of the inferred owner
- The account name of the inferred owner
- The name of the business unit
- The name of the business owner
- The data owner policy through which the data owner is inferred

In addition to these ownership reports, you can also get ownership information for paths in the following reports:

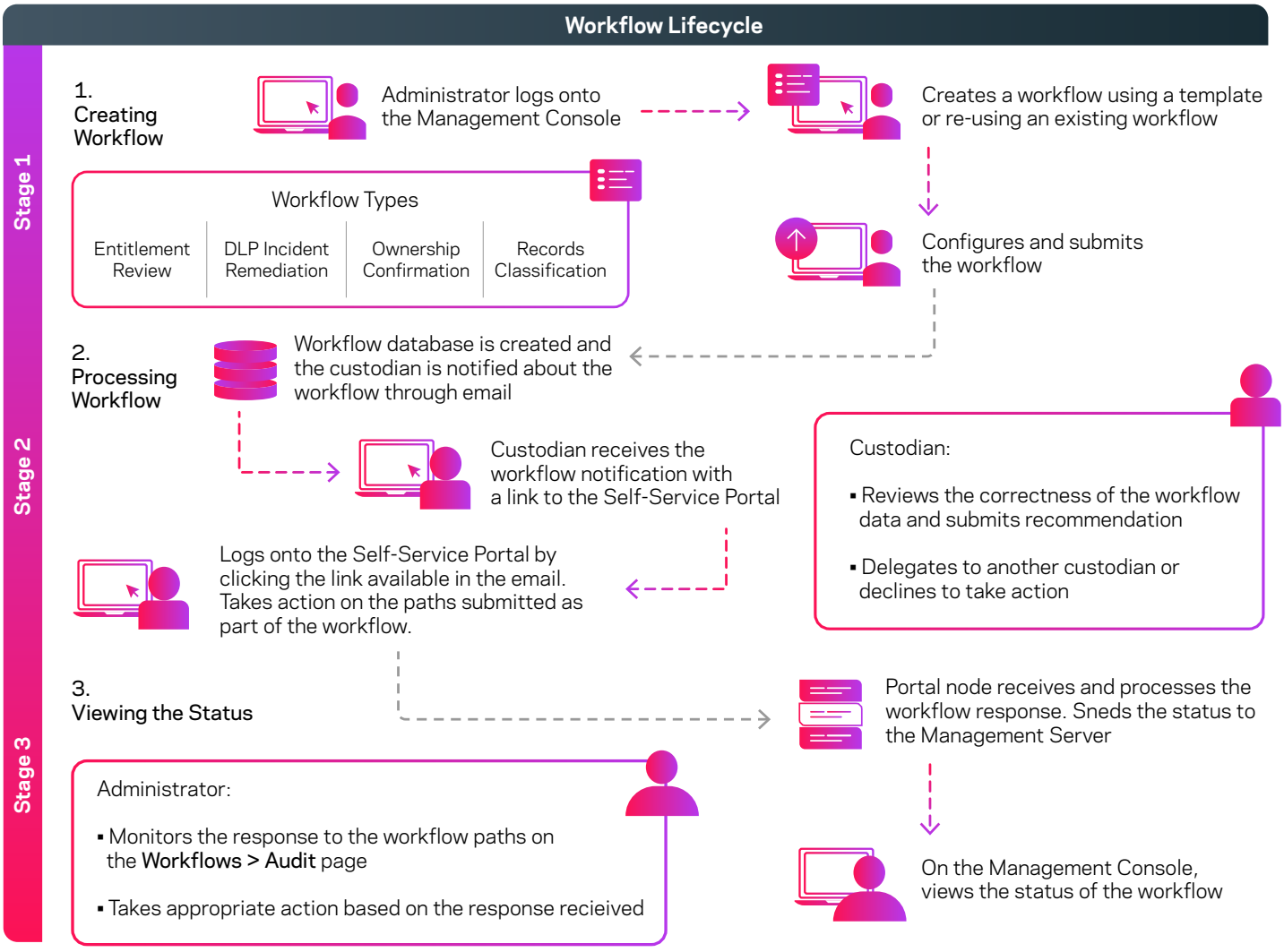
- Activity summary for paths report
- Data aging report
- Inactive folders report
- Path permissions report
- Consumption by folders report

Remediation Workflows

Now that Data Insight has provided you a way to identify who should be responsible for remediation on assigned data locations how do you assign the actual responsibility? It is time consuming to manually inform data owners about issues with resources that they own and track the remediation actions on such resources. To solve this, Data Insight provides remediation workflows that provide an easy automated way to:

- distribute remediation tasks to configured custodians and data owners
- define attributes to be displayed to the owner or custodian and the actions they can take on these resources
- record audit logs

Figure 5 shows a sample remediation workflow.



Data Insight allows you to create the following workflows for different remediation tasks:

- Entitlement Review

  Review the user permissions on the folders that the custodians are responsible for and attest the permissions or suggest changes.

  You can send the change request to a ticketing system or Identity and Access Management (IAM) tool or use custom scripts to remediate the permissions.

- Data Loss Prevention (DLP) Incident Remediation

  View policy violations and take action on the files that violate policies. The policy information is pulled into Data Insight from Symantec Data Loss Prevention (DLP). The actions are Smart Response rules defined by DLP administrators. DLP uses the Smart Response rules to remediate the resources that violate configured DLP policies.

  Data Insight uses two DLP Web services for incident remediation - the Response Rules Listing Service and the Response Rule Execution Service. The Response Rule Listing Service provides a list of available response rules in DLP, such as delete or quarantine, for a given incident. The Response Rule Execution Service takes the response rule requests submitted by users from the Self-Service Portal and executes them in DLP.

- Ownership Confirmation

  Confirm the ownership of files and folders in your storage environment.

- Records Classification

  Classify the sensitive files that must be retained for a legally mandated period. The workflow helps you classify files based on their business value and manage the life cycle of sensitive documents by applying data management rules to the classified data.

  You can choose to archive the files that are marked as record and apply retention categories that define how long the files must be stored before being deleted. The files that are marked as record are retained based on the file classification policies that they match.

  You can use the workflow to trigger automatic actions to archive data to Enterprise Vault.

As seen in the workflow, once the Data Insight administrator submits a workflow from the Data Insight console, the custodians receive an email notification with a link to the Self-Service Portal. They can log in to the portal, choose the necessary remediation actions, and submit the changes for execution by the DLP Enforce Server, Enterprise Vault server, or the Data Insight Management Server, depending on the type of workflow.

Depending upon the workflow, the custodian may perform the following actions within the Self-Service Portal:

DLP Incident Remediation

Choose the configured remediation actions and submit the same for execution by the DLP Enforce Server. The steps they would follow include:

- View a snapshot of the number of files that are assigned for their attention
- Filter the list of files based on the severity of the incidents that the files have violated, the recency of the last access date, or the DLP policy that the files violate
- Select one of the available actions, which are DLP Smart Response rules configured in DLP to run which will execute in parallel on multiple files

Entitlement Review

Review the user permissions on folders they own and automatically trigger a permission remediation workflow to execute the changes such as:

- View a snapshot of the users whose permissions are assigned for their review
- Review if the user has the creator owner permission on a path
- Filter the users to be reviewed based on their activity profiles and the assigned paths. As an example, review the entitlements for inactive users
- Make recommendation to grant or revoke user permissions on the specified paths
- Decline the review request or delegate the review work to another user

The Data Insight administrator can allow the custodian to either:

- make suggestion on relevant changes that they can then approve or
- automatically trigger a permission remediation action to distribute the actions to the proper authorities such as, directory server administrators

Ownership Confirmation

The custodian can view all the paths to confirm which you accept the ownership of. Once the custodians confirm or deny the ownership, the status summary is displayed in the Data Insight Management Console. A Data Insight administrator may review the status and take further actions based on it such as assigning a different custodian to paths which the previous custodian denied.

Records Classification

The custodian can select to classify files based on business value of their content. They can apply various filters on the data and select which files they want to be archived using Enterprise Vault™ and have specific post-processing actions (such as retention periods) applied.

Additional Considerations

- The Inferred Data Ownership feature outlined in this document is included in the standard licensing agreement for Veritas Data Insight
    - Additional licensing is required for the Self-Service Portal for remediating data found in reports where the inferred data owner is the owner of the filer or folder
- Active Directory information and global policy considerations are required to show inferred ownership information in Data Insight
- To use Inferred Data Ownership for remediation, a minimum of one remediation workflow must be created

For further information, please refer to the Data Insight Administration guide and User's Guide.

Summary

To summarize, Data Insight allows organizations to simplify the process of ensuring proper access management and governance decisions are done across their data infrastructure. It uses analytics to determine the inferred owner, and also allows administrators to assign a custodian. This ownership/custodian information can then be reviewed in reports and also used in automated remediation workflows. These workflows not only distribute remediation tasks appropriately and maintain audit logs but also tie into actions that the owner or custodian can use. These actions can include permission remediation, ownership confirmation and archiving with records classification.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1011 04/22