Data Insight 5.0 Feature Briefing

Access Change Tracking and Orchestration

This document is about the new access change tracking and orchestration feature in Data Insight 5.0.

This document applies to the following version(s) of Data Insight: 5.0

If you have any feedback or questions about this document please email them to IIG-TFE@symatec.com stating the document title.

VERITAS

Feature Description

Data Insight 5.0 offers new methods to ensure that permissions on CIFS/NTFS-based file systems and SharePoint are configured properly. It also has the ability to audit permission changes. Data Insight can identify permission inconsistencies and help alleviate these issues in the following ways:

- Permissions Search
- Permissions Orchestration
- Permission Delta

Permissions Search

Permissions Search allows users to query access control configurations through metadata collected by Data Insight. Permissions queries can be based on the following parameters:

- Access Control Entry/List
- Path
- Permission Search
- Active Directory Attributes
- Custom Attributes

Creating a query based upon the above-listed parameters allows an administrator to obtain detailed permissions reports on a particular directory or file share.

Permissions Orchestration

After permissions issues have been identified, Data Insight can assist an administrator by correcting problems in the following ways:

- Manage path permissions effectively
- Manage controlled security groups
- Eliminate open access to file shares

Permissions Orchestration is only available for CIFS-based shares and folders.

Permission Delta

Previous versions of Data Insight would collect events on reads, writes, and other events through auditing. However, Data Insight would not audit permission changes. Starting with Data Insight 5.0, permission changes are now collected.

Permission delta enables an administrator with the ability to view permission changes on a specific directory. Changes to the Access Control List (ACL) for a particular folder are now monitored and viewable through the Data Insight console.

Business Value

Permissions Search Business Value

Business value for Permissions Search:

- Customers would like the ability to search permissions that do not abide by best practices or other search criteria based on attributes of an ACE, ACL, or the Trustees. Customers will be able to discover permissions given to Groups based on the attributes of their members. It will also be easy for customers to take permission remediation actions on the results of such queries.
- Customers will be able to easily search and clean-up permissions in order to minimize access risk and maintain permission hygiene.

Permissions Orchestration

Business value for Permissions Orchestration:

- Ensures that the right users have the correct level of access to file shares and folders
- Eliminates identified security loopholes
- Controls access to critical data
- Controls Active Directory group management

Permission Delta

Business value for Permission Delta

- Customers have the ability to view permission changes through auditing to ensure permissions are configured correctly.

Underlying Principles

Permissions Search

The Permission Search feature involves the use of several components. These components include:

- (Ad)Scan (adcli.exe)
- Index (idxwriter.exe)
- Query (report.exe)

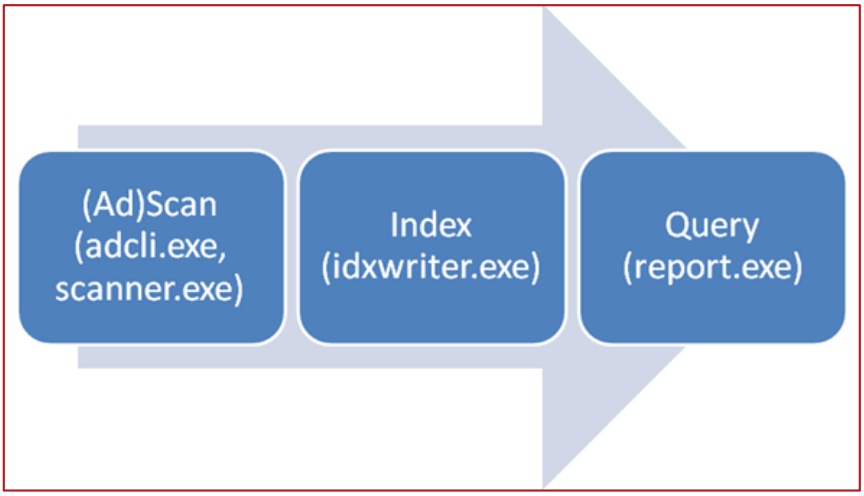


Figure 1 – Permission Search Overview

The (Ad)Scan process collects information about users and user groups from Active Directory. An Active Directory connection must be configured within the Data Insight console. Collected information is stored in a separate Data Insight database.

The Index process indexes collected metadata from monitored file shares and SharePoint sites. The metadata contains Access Control Lists (ACL).

The user generates permissions reports through the Query process. Permissions reports are based on the metadata collected by Data Insight, the list of users and groups from the Active Directory scan, and the index processes.

Permissions Orchestration

Permissions Orchestration is part of the overall Permission Remediation workflow available through the Data Insight console. There are two main areas for orchestration: removing permissions from a folder or file share and the ability to remove a user or group from an Active Directory security group. Permissions Orchestration is only available for CIFS-based file shares. Figure 2 provides a high level overview of the remediation process.

Removing Permissions

Permissions can be removed from a file share or folder via two different methods:

- Removing permissions as an action item from the Permissions Search Report
- Removing permissions using the workspace in Data Insight

Once user or group objects have been identified (using one of the above mentioned methods), Data Insight can then facilitate the updating of permissions on the file share or folder.

Removing User or Group Objects

Once an Active Directory user or group object has been identified for removal from an Active Directory security group using the Data Insight user/group centric overview page (accessible from the Data Insight console), Data Insight can then assist with updating Active Directory with the required changes.

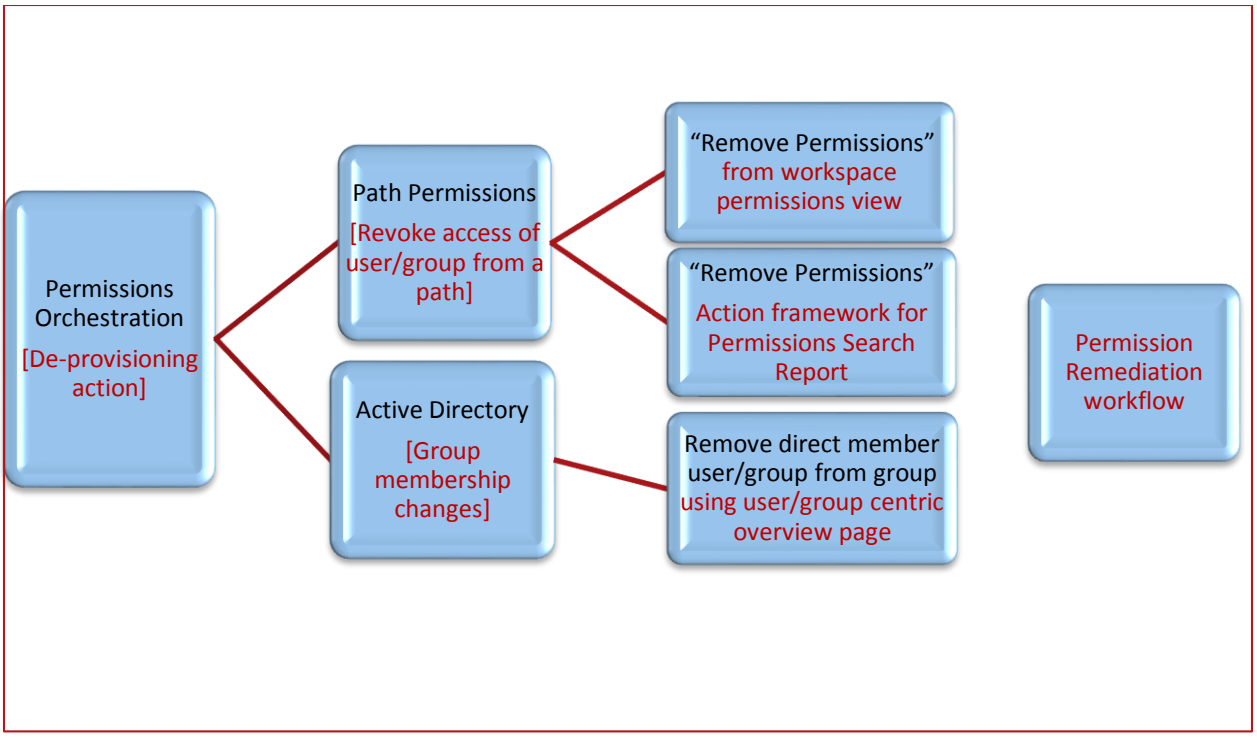


Figure 2 – Permissions Orchestration Overview

Permission Delta

Data Insight 5.0 has a new database to keep track of permission changes called **permdelta**. All permissions changes are recorded to the table. The old and new ACL IDs are stored for each directory that is monitored by Data Insight.

Guided Tour

Permissions Search

Permissions Search reports are accessible through the Data Insight console under **Reports -> Permission Reports -> Permissions Search**. Creating a Permissions Search report is similar to creating other reports in Data Insight.

A template will need to be created in order to report on the necessary items. Templates can be based on ACEs or ACLs.

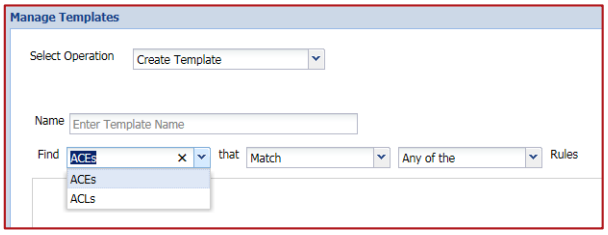


Figure 3 – Creating a template for Permissions Search

Additionally, at least one rule will need to be created. A default rule can be selected (as shown in Figure 4) or a custom rule can be defined (as shown in Figure 5). Multiple rules can be added to the template.

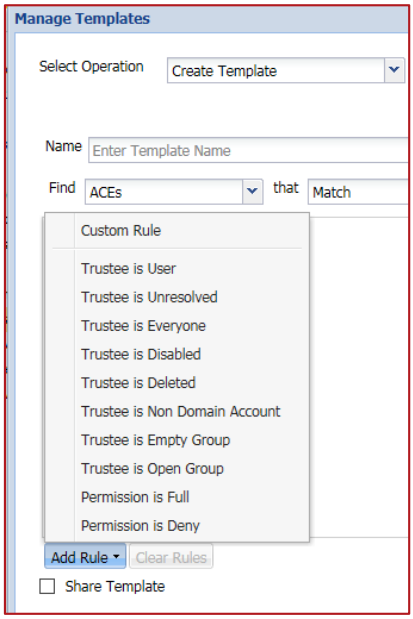


Figure 4 – Selecting a default rule for the template

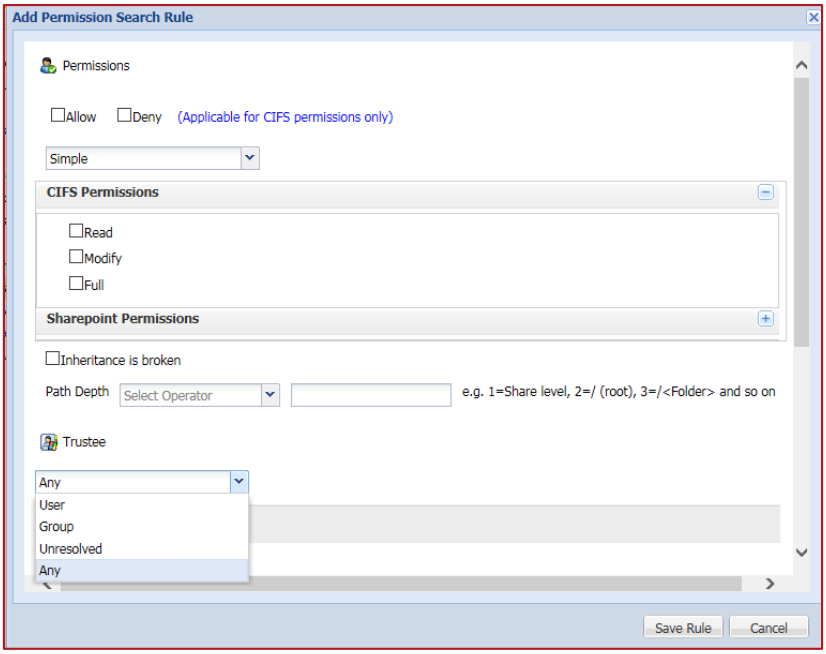


Figure 5 – Creating a custom rule

For more information on Permissions Search, please refer to the Data Insight 5.0 administration guides.

Permissions Orchestration

Before permissions remediation can be performed, it will be necessary to configure remediation by navigating to **Settings -> Remediation -> Permissions** in the Data Insight console. Remediation can be done by either raising a ticket (which requires an SMTP server to be created) or through a custom script. For more information please refer to the Data Insight 5.0 administration guides.

Permissions Orchestration is performed using the Data Insight Workspace or as an action item from a permissions search report. When using the Data Insight Workspace, navigate to the folder or share in question and bring up the Profile view. In the Profile window, a user clicks on **Permissions**. File system access control list and share level permissions are viewable (as shown in Figure 6). The user can remove permissions for a particular user or group object by selecting "Remove Permissions" for the selected object. Depending on the method defined for permissions remediation, an email will be sent or a custom script will be executed to remove the user or group object in question.

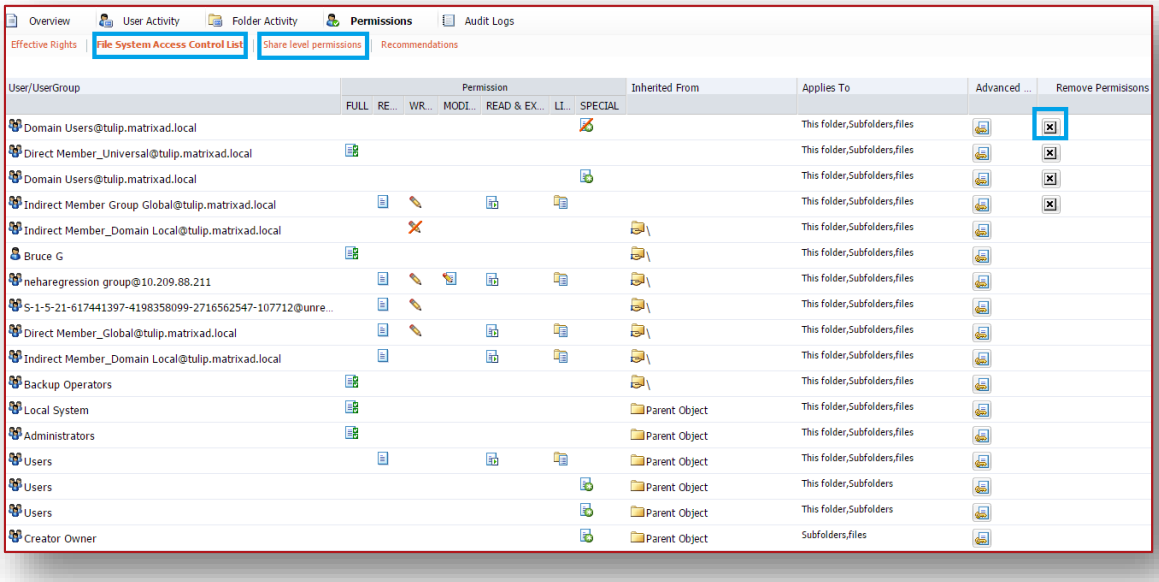


Figure 6 – Permissions Orchestration

Permission Delta

A new audit access named "Permission Change" is now available with Data Insight 5.0 and later. In order to view the permission changes, a user navigates using the Dashboard to the ***Desired Directory Path* -> Audit Logs -> Access -> Permission Changes**. It should be noted that permission deltas are only available for directories and not for files. Share-level permission changes are not supported.

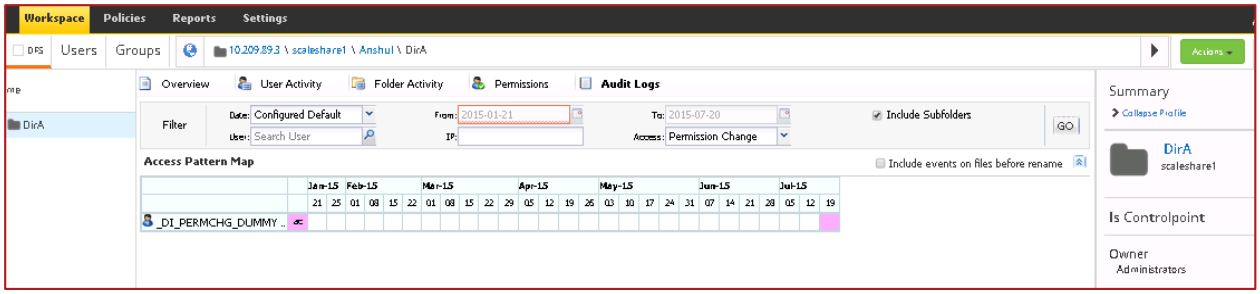
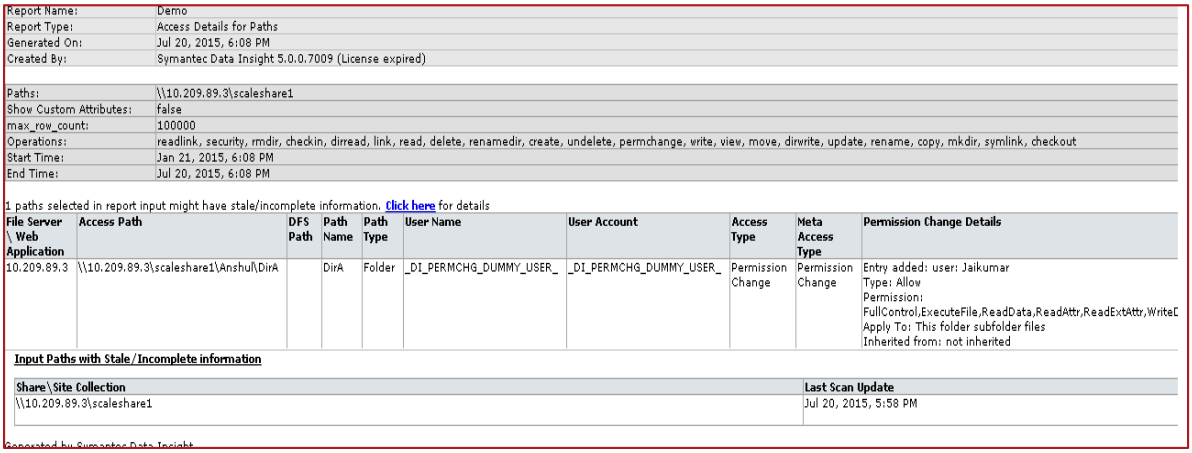


Figure 7 – Viewing permission deltas in the Data Insight Workspace

Permission deltas are also viewable in report format. Under the Reports tab, navigate to **Reports -> Access Detail Reports -> Access Details for Paths**. The report will only list changes when All Users or All Groups are selected for the report.



Report Name:	Demo
Report Type:	Access Details for Paths
Generated On:	Jul 20, 2015, 6:08 PM
Created By:	Symantec Data Insight 5.0.0.7009 (License expired)
Paths:	\\10.209.89.3\scaleshare1
Show Custom Attributes:	false
max_row_count:	100000
Operations:	readlink, security, rmdir, checkin, dirread, link, read, delete, renamedir, create, undelete, permchange, write, view, move, dirwrite, update, rename, copy, mkdir, symlink, checkout
Start Time:	Jan 21, 2015, 6:08 PM
End Time:	Jul 20, 2015, 6:08 PM

1 paths selected in report input might have stale/incomplete information. Click here for details

File Server \ Web Application	Access Path	DFS Path	Path Name	Path Type	User Name	User Account	Access Type	Meta Access Type	Permission Change Details
10.209.89.3	\\10.209.89.3\scaleshare1\Anshul\DirA		DirA	Folder	_DI_PERMCHG_DUMMY_USER_	_DI_PERMCHG_DUMMY_USER_	Permission Change	Permission Change	Entry added: user: Jaikumar Type: Allow Permission: FullControl,ExecuteFile,ReadData,ReadAttr,ReadExtAttr,WriteE Apply To: This folder subfolder files Inherited from: not inherited

Input Paths with Stale / Incomplete information

Share \ Site Collection	Last Scan Update
\\10.209.89.3\scaleshare1	Jul 20, 2015, 5:58 PM

Generated by Symantec Data Insight

Figure 8 – Viewing permission deltas in report format

Licensing and support considerations

Licensing

Licensing for all features described in this document come standard with the license type purchased for Data Insight (such as Box, SharePoint, CIFS, and so on.)

Support Considerations

For Permissions Orchestration:

- Permissions cannot be modified for SharePoint, NFS, or Box
- Only deprovisioning (removal of permissions) is supported. Permissions cannot be added.

For Permission Delta:

- Available only for folders - Changes of permissions on individual files are not supported

About Symantec:
Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.
Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at **www.symantec.com**.

Symantec Corporation

World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA

+1 (650) 527 8000

+1 (800) 721 3934

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**