Top Ten Reasons You Should Upgrade from Storage Manager to File Dynamics

The introduction of File Dynamics by OpenText in 2018 greatly expanded the network data management capabilities that were offered previously in Storage Manager for Active Directory. File Dynamics, with its impressive track record of subsequent product releases and new features, has replaced Storage Manager for Active Directory. Yet some loyal Storage Manager for Active Directory customers have still not upgraded. Here are 10 reasons why you should.

An expanded emphasis on data growth, automation, compliance, security, and protection are all contributing to an evolving definition of network data management. To meet the dynamic demands of today's organizations, OpenText™ offers OpenText™ File Dynamics.

Built on technology that is today managing millions of users and groups in hundreds of organizations around the world, File Dynamics offers dramatic performance and management capabilities over its predecessor – OpenText™ Storage Manager for Active Directory.

At OpenText, we're now working to make happy Storage Manager for Active Directory customers ecstatic File Dynamics customers. These 10 features, only available in File Dynamics, should help.

1. **Enhanced security and protection of high-value targets.** There are some network folders where data loss or unauthorized access would be catastrophic to an organization. In File Dynamics we call these "high-value targets." Through various File Dynamics policies detailed below, you can enhance the security and protection of these folders.

2. **Apportionment of management to data owners.** No one knows the value and sensitivity of data more than the individuals that work with that data. With File Dynamics, you designate data owners from the departments that work with sensitive data located in high-value targets to help establish governing policies. Using the Data Owner Client interface, Data owners can help set policies for data access permissions, be notified when these access permissions have changed, and even recover lost or corrupted data.

3. **Security Notification policies.** There might be times when an IT department worker who is unfamiliar with the sensitivity of a high-value target, will grant access permissions to an unauthorized user. Security Notification polies allow Data Owners to analyze and be notified of any changes in security permissions for a selected target path. Notifications are sent via email and specify the added, modified, or removed permissions for users and groups.

File Dynamics:

- Keeps sensitive data secure
- Empowers those familiar with the data to help manage it
- Controls data access
- Automates routine storage management tasks
- Simplifies data migrations
- Remediates the location of sensitive files
- Enables file management in identity management systems
- And much more

Policies that you define are the means of automating and assuring the proper management of network-stored data, its protection, and the governance of its access.

With File Dynamics, you have the means to not only provision, manage, and dispose of user and group storage, but to secure high-value targets from unauthorized access and protect these high-value targets from data loss or data corruption that can occur from negligence, hardware failure, or even a ransomware attack.

Connect with Us
OpenText CEO Mark Barrenechea's blog

4. **Security Fencing policies.** Some of your high-value targets might be restricted to group membership, whose members might change over time. Security Fencing policies let you set limits on how access permissions can change over time by specifying containers, groups, or users that can be given access permissions and others that should never be given access permissions.

5. **Security Lockdown policies.** Once the proper access permissions for a high-value target have been established, you can set a baseline of access permissions that will be strictly enforced through a Lockdown policy. When unauthorized access permission changes are made to the high-value target, the new permissions are removed and the permissions specified in the Lockdown policy are restored.

6. **Data protection.** Epoch Data Protection policies allow you to maintain nearline archives of high-value targets. Data Owners can view and access the archive of the high-value target as it existed at a selected point in time. In essence, it is a "time machine" for the data and associated permissions on the high-value targets.

7. **Workload policies.** These are policies that provide the ability to import externally-generated files that can be enacted through a Data Owner via the Data Owner Client. For example, reports generated in OpenText™ File Reporter that specify the location of sensitive files can be imported into the Data Owner Client where a designated Data Owner can remediate the location of these files.

8. **Content control policies.** As a Target-Driven policy with a direct association to a folder or share, the data management capabilities that were previously available in Groom operations are now available as Content Control policies, enabling you to groom files from any location on the network.

9. **Data location policies.** These new Target-Driven policies allow you to move and copy data from one location to another.

10. **Scoping.** To alleviate the burden of monitoring non-applicable Active Directory events and non-managed storage areas, File Dynamics lets you specify what types of events and which storage resources are monitored through "scoping."

Learn more at
www.microfocus.com/opentext

opentext™