Flyer

opentext™

Protecting Your Documentum System with Data Protector 24.1

OpenText™ Documentum™ content management is a well-established distributed, cloud-native enterprise content platform. As with all software-based solutions a secure backup and recovery strategy is key for protecting your digital assets and regular backups are essential to prevent data loss caused by human errors, cyberattacks, or hardware malfunctions.

Protecting Documentum with Data Protector at a Glance:

- **OpenText Data Protector for Documentum:**
  Protects all digital assets stored within Documentum from intentional and unintentional modifications or attacks.
- **Prevent successful ransomware attacks:**
  Data Protector secures your Documentum system by using advanced backup and recovery technologies and AI/machine learning to assist with the detection of anomalies caused by malware attacks.
- **Prevent internal attacks on your Documentum data:**
  The majority of data loss is caused by internal actions and Data Protector provides powerful restore capabilities to enable the quick recover any lost data.

Organizations of all sizes are grappling with the volume and diversity of content. Managing documents, emails, forms, and process-created data, has never been more challenging. Increased regulations, additional content types and new ways of working can make the task seem overwhelming. Beyond these challenges, however, is the opportunity to transform organizations by extracting value from information while enhancing governance.

OpenText™ Documentum™ provides a broad set of capabilities that manage content across file stores, enterprise applications, such as SAP, and collaborative tools, including Microsoft® SharePoint®. Its extensibility makes custom integrations simple. With Documentum™, organizations ensure information is organized, preserved and easily accessible, while adhering to privacy and security protocols.

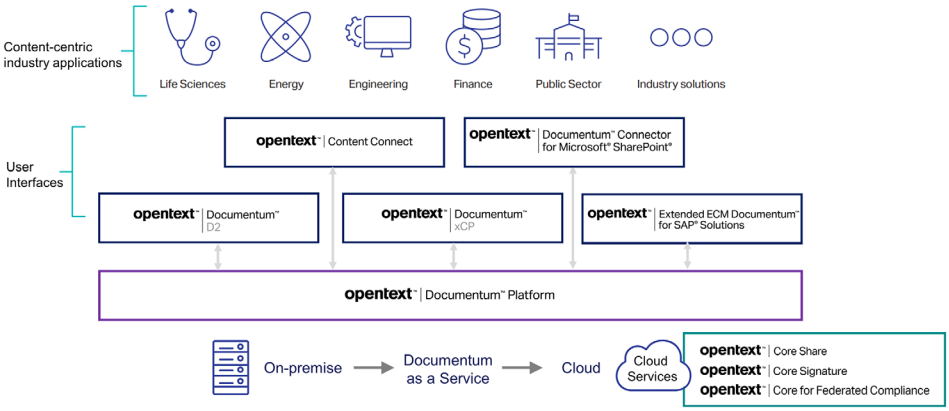

Figure 1. Documentum Platform Components

However, just like any software, Documentum™ is susceptible to human errors, cyberattacks, or hardware malfunctions, which can lead to data loss and disruption. This is why regularly backing up your Documentum™ System is crucial, even if you have data replication or redundancy in place.

Data Replication and Redundancy: Not Enough

Data replication involves creating multiple copies of data across different servers or storage devices. This ensures that if one copy becomes unavailable or corrupted, there are other versions to fall back on. Redundancy, on the other hand, focuses on providing multiple paths for data access in case of hardware failure or network connectivity issues.

While both replication and redundancy can enhance data availability, they don't eliminate the need for backups. Here's why:

1. **Safeguarding Against Human Error:** Even with replication and redundancy in place, human error remains a significant threat to data integrity. A mistaken deletion, accidental overwrite, or incorrect configuration change could render valuable documents inaccessible or even permanently lost. Data Protector Backup Agent for Documentum™ serve as a safety net, enabling you to perform individual restores of files or parts of your database, or even restore Documentum™ to a previous state before the error occurred.
2. **Protecting Against Cyberattacks and Ransomware:** Cyberattacks are becoming increasingly sophisticated, and Document Management Systems are often targeted due to their potential to store sensitive data. Malware infections, phishing scams, and ransomware attacks can compromise your Documentum environment, making data inaccessible or even encrypting it until a ransom is paid. Data Protector Backups provide a lifeline in these situations, allowing you to restore Documentum to a clean state and minimize the impact of the attack.
3. **Enabling Testing and Development:** Backups are not only essential for disaster recovery but also play a crucial role in testing and development. When implementing new features or making changes to your Documentum™ System, you can use a backup copy to test the functionality without affecting your live system. This allows for thorough testing, ensuring that new changes are stable and don't introduce errors or data loss.
4. **Complying with Regulations and Data Governance:** In regulated industries, data security and compliance with data governance policies are paramount. Data Protector Backups provide concrete evidence of data integrity and availability, which can be crucial for audits and compliance checks. Having regular backups demonstrates diligence in data management and helps businesses meet regulatory requirements.
5. **Minimizing Downtime and Ensuring Business Continuity:** Data loss or system downtime due to a hypothetical Documentum outage can have severe consequences for businesses. Lost documents, disrupted workflows, and negative impacts on customer service can significantly impact operations and profitability. Regular backups automatically scheduled by Data Protector ensure that you can quickly restore the system in case of an outage, minimizing downtime and maintaining business continuity.

Syncing Document and Database Backups

Effective backups require synchronization between document backups and the Documentum™ database. This ensures that the backup accurately reflects the current state of the system, including any changes made to documents, versioning, audit trails, workflows, and user rights.

Regular synchronization helps maintain data integrity and facilitates rapid recovery in case of an incident. By syncing backups frequently, organizations can minimize the data loss window and ensure that they can quickly restore Documentum™ to its operational state.

Back Up

Scheduling a backup job for Documentum™ in Data Protector is a breeze. The process is straightforward and can be completed in just a few simple steps:

- **Create a backup specification:** This is the blueprint for your backup job and thanks to the new integration it includes the information for both the content server and the database. The backup specification defines what you want to back up and where you want to back it up to, and can be either scheduled or manually triggered.
- **Choose the backup type:** There are two main types of backups for Documentum™: full and incremental. Full backups back up

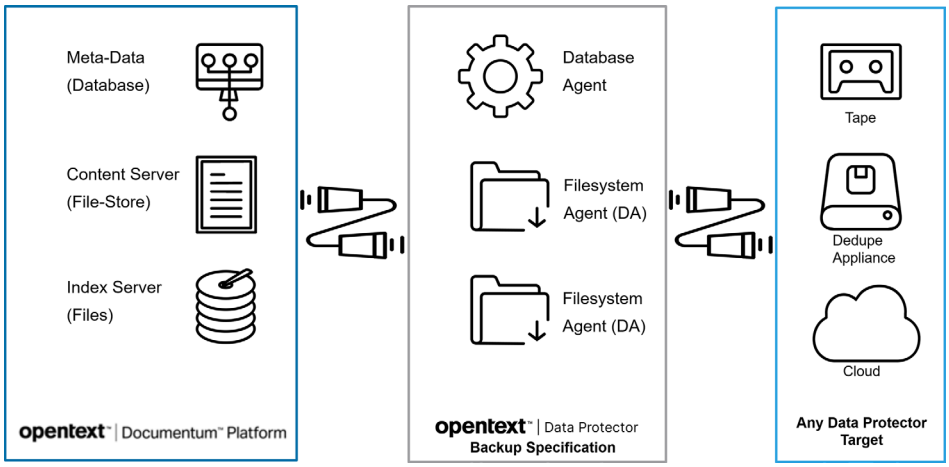

Figure 2. Data Protector integration for Documentum™

the entire Documentum™ repository, while incremental backups only back up the changes that have been made since the last backup.

- **Select the backup destination:** You can back up your Documentum™ repository to a variety of destinations, including disk, deduplication repositories, tape, or the cloud.
- **Set the backup schedule:** You can schedule your backup job to run on a regular basis, such as daily, weekly, or monthly.

Once you have created your backup job, you can start it manually or schedule it to run automatically. Data Protector will take care of the rest, natively integrating with Documentum™ Database and ensuring that the repository is backed up regularly and securely.

Restore

Data Protector backups include all the necessary information to restore a complete Documentum™ system or an individual item at a repository level. This means that you can restore the system to a previous state if it is accidentally deleted or corrupted. You can also restore individual items, and both the backup and the restore can be done without taking the server down.

In conclusion, while replication and redundancy can offer some level of protection, backups remain the foundation of data security for document management systems like Documentum™. By consistently backing up Documentum™, you can safeguard your valuable documents from a variety of threats,

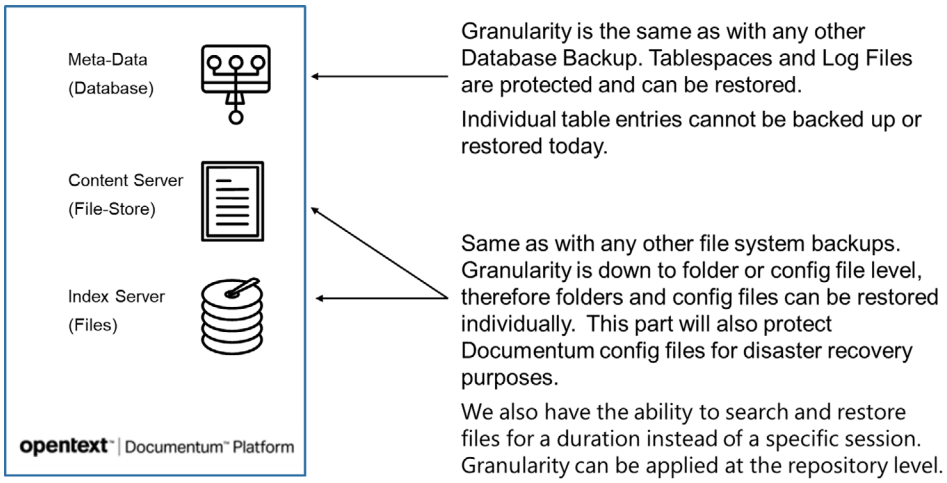

Figure 3. Restore Granularity

including human error, cyberattacks, and testing mishaps. This proactive approach will help maintain data integrity, ensure compliance, and minimize downtime, keeping your organization's operations secure and resilient.

Data Protector

Data Protector is an enterprise grade backup and disaster recovery solution for large, complex, and heterogeneous IT environments. Built on a scalable architecture that combines security and analytics, it enables customers to meet their continuity needs reliably and cost-effectively.

Documentum™

Documentum™ content management is a distributed, cloud-native enterprise content platform that offers a compliant, secure single-source-of-truth for all users. Built on a modular foundation, Documentum™ software integrates into enterprise business applications to enable access from any UI. Documentum™ products scale to meet the high-volume content demands of highly regulated organizations.

Learn more at
www.microfocus.com/dataprotector

www.opentext.com

opentext™