

Best Practices for Protecting Your IBM FileNet P8 Information

Introduction

There are dozens of articles and white papers outlining the most critical steps organizations can take to minimize the risk of information loss from disasters. There are few, however, that address the most common threats to your enterprise content management (ECM) system information—the logical failures caused by everyday occurrences such as programmatic and user errors, viruses, malfeasance, and corruption.

Working from the assumption that you've already put in place commonly accepted security and disaster recovery best practices, let's explore some additional policies and practices that you must put in place to ensure that the information assets you store in IBM® FileNet® P8 have an adequate level of protection. Here are 10 best practices for P8 backup and recovery.

10 Best Practices

1. Think Granular

Granular recoverability is critical in any ECM implementation. Disaster recovery procedures are not only overkill when it comes to retrieving one, several, or even hundreds of lost documents, they are dangerous—bringing the entire repository offline and rolling it back to an earlier version exposes the entire repository to additional information loss. Don't put yourself in a situation where you must make a devil's choice between recovering one extremely important document and losing updates (and possibly information integrity) for dozens of other documents. Supplement your disaster recover plan with the ability to backup and restore at a granular level.

2. Maintain Your Integrity

Ensuring that P8 information maintains its integrity during the backup process and can be restored to its original state during recovery is critical for meeting compliance and business demands. Taking the entire system offline and performing a "cold" full system backup is an ideal way to ensure that you can fully recover from disasters without compromising information integrity.

However, in the case of logical failures where you need to recover granular information, you're not going to want to take the entire system offline. The only way to recover from these incidents while maintaining information integrity and avoiding application downtime is to enhance your existing repertoire of backup and recovery solutions with an ECM-specific information protection tool. The tool should capture and recover granular information while your ECM system stays online, and should validate the integrity of information during the backup process. Corrupt information should be rejected and flagged for an administrator so that corrective action may be taken. This ensures that only "clean" information is captured during the backup process and that all recovery requests will be successful.

3. Conduct a Regulatory Refresher

Most companies these days are subject to at least several federal and industry-specific regulatory demands, many of which require data preservation and retention. SEC 17a-4, Sarbanes-Oxley, FDA CFR Part 11, and HIPAA are some of the more well-known initiatives but there are numerous others,

including the Federal Rules of Civil Procedure eDiscovery Rules Amendment, which outlines a company's duty to preserve and produce electronically stored information (ESI) in the face of litigation. Non-compliance with these initiatives can result in hefty fines, negative brand exposure, and in extreme cases, business shutdowns.

To avoid these consequences, make sure that you fully understand the regulatory requirements being placed on your company, and look to see what other companies in your industry are doing to address data retention and other compliance mandates. You will also want to ensure that you have an ECM-specific data protection solution that can preserve and recover granular information in its original state so that you don't have to take P8 offline and incur more loss just to restore one document or folder and its associated properties (metadata) such as audit trails.

4. Deploy Application-Aware Backup and Recovery Solutions

“Application-aware backup” is the new catchphrase, but for good reason: it is extremely important to understand the specific requirements of each of your major enterprise applications. When it comes to P8, for example, traditional backup approaches have no awareness of the relationships that an object (e.g., a document) has to other objects in a business process (e.g., another document in a workflow).

Therefore, if you're using your ECM system to route documents through an approval process and one of those documents is accidentally lost, even if you were to restore the document using a traditional recovery solution, you would not be able to restore it back to the specific state in the process it was at before the loss occurred. Your only option would be to route it back through approval process until it reached the stage it was at prior to the deletion – if anyone can remember what stage that was – and suffer the permanent loss of annotations and other properties (metadata), which cannot be recreated. This puts you at compliance risk since the approval process, which specifies who approved what when, is not the original, but a recreation.

By deploying a granular, application-aware backup and recovery solution, you would be able to quickly restore just the affected information back to its original state, with the original metadata intact, avoiding disruptions to critical operations and facilitating compliance.

5. Ensure Continuous Application Availability

While P8 availability isn't always held to the same “five-nines” standards as other applications, quality of service and uptime are still very important metrics for measuring IT and line-of-business performance, particularly in today's global environment where maintaining 24x7 availability is increasingly critical.

When evaluating your P8 backup and recovery policies or plans, ask yourself (and your team) how much P8 downtime and data loss you can tolerate. While traditional backup and recovery solutions are ideal for recovering from disasters, if you need to recover from a logical failure and do not have an ECM-aware recovery solution, you will most likely have to take P8 offline to restore the lost data and incur additional information loss – or suffer the loss and its consequences. Keep in mind that when it comes to e-discovery and compliance requirements, the timeliness of producing information is critical.

6. Perform Proactive Integrity Checks

Because complex relationships between documents, sub-documents, workflows and all the other properties (metadata) surround ECM information, it is especially vulnerable to data corruption. Worse, it can often be difficult to detect this kind of logical data loss. Data corruption often goes undetected until someone unsuccessfully tries to access the data for a business need. It can also, however, rear its ugly head during repository migrations and upgrades, where it can halt migration scripts, causing delays and lost productivity. In order to ensure information integrity, with an ECM-specific solution that performs proactive integrity checks and alerts you to corruptions and other integrity issues.

It's one thing to identify the problem, and another thing entirely to be able to fix it. Correcting corruptions requires extensive knowledge of ECM platforms and their underlying metadata schemas. In many cases, an ECM-specific granular recovery solution can help correct corrupted metadata by recovering it back to its original, uncorrupted state. However, it is also critical to conduct an in-depth analysis of information integrity on a regular basis, and develop and implement a plan with ECM system experts to rectify integrity issues that aren't so easily corrected.

7. Recover to Any Point in Time

To ensure a full recovery from logical failures, you'll want to make sure that you have a granular recovery solution that performs hot (online) captures of your P8 information on a continuous, frequent basis – ideally as often as every 15 minutes. This ensures that you can recover documents back to just about any point in time, and even recover documents that were created or modified as little as 15 minutes ago. And because the captures are “hot,” there's no need to worry about disrupting productivity.

In addition, the captures should be “incremental,” meaning that they capture only the additions or changes that have been made to ECM information, which minimizes any impact on system performance.

8. Minimize Your Data Loss Window

If you follow the earlier advice by capturing P8 data every 15 minutes, you will almost automatically reduce your data loss window by a significant margin—the more frequent you can be in your backup while the system is online, the smaller your window, and the better you are able to meet ever-increasing recovery point objectives (RPOs) and recovery time objectives (RTOs).

Solutions exist that provide cost-effective ways to reduce unplanned downtime, recover quickly from logical failures, facilitate compliance and decrease the frequency with which the ECM system needs to be brought down for backup and recovery. These solutions supplement traditional enterprise backup and recovery solutions and can be easily integrated into existing enterprise continuous data protection (CDP) schemes.

9. Implement Records Management Policies and Enforce Retention Policies.

Organizations should implement and enforce stringent records management and retention policies to mitigate civil and financial risks from regulatory non-compliance. Regulatory non-compliance can result from inconsistent records management, accidental deletions, data corruption and essentially any other event not in accordance with business practices and regulatory guidelines. If these policies already exist in your organization, be sure to review them regularly to make sure they comply with new and changing regulations.

Your P8 backup and recovery solution should be sensitive to your retention policies, consistently capturing, recovering and disposing of information based on retention policies. The solution should ensure that records are recoverable during the specified retention period, and that they are permanently expunged once the retention period has expired.

10. Minimize the Number of Chefs in the Kitchen.

To ensure rapid recovery from logical failures while minimizing required recovery resources, the recovery process should be manageable by a single administrator. There should be no need to convene a data recovery committee meeting to identify the least impactful means of retrieving one, several, or even thousands of lost or corrupt documents.

About CYA Technologies

CYA Technologies, an enChoice® company, provides the only end-to-end portfolio of solutions that optimize enterprise content management (ECM) application efficiency, facilitate compliance, and insure companies against the risks of ECM information loss. CYA solutions support ECM systems including EMC Documentum and IBM FileNet P8, and protect thousands of repositories at more than 275 global organizations including DuPont, Gruenthal, McKinsey & Company, Petro-Canada, Schering-Plough, Standard & Poor's, and the U.S. Army.

For more information about CYA, visit www.cya.com, or call +1.203.513.3111 ext. 501.

CYA Technologies,
an enChoice® company
4 Research Drive
Shelton, CT 06484
+1.203.513.3111
www.cya.com