IRON MOUNTAIN®

WHITE PAPER

DOCUMENT MANAGEMENT SOLUTIONS

Digital Record Center® for Images

STORE ELECTRONIC RECORDS WITH CONFIDENCE

Contents

INFORMATION IS... YOUR ADVANTAGE

The Digital Record Center for Images is a Web-based, hosted image repository that is used to store and manage any type of electronic document or record. Users can store electronic documents with confidence, knowing that their important corporate information is always safe and secure, yet quickly accessible by authorized users when needed.

Powered by IBM® Content Manager OnDemand™, a proven system actively used by over 13,000 companies, the Digital Record Center for Images is a Fixed Content Repository that supports COLD data, images, and PDFs. It provides a flexible architecture for scalability and high performance, robust search and retrieval functionality, and rich administrative functionality for system management and self-service administrative capabilities.

WEB-BASED DESIGN

The Digital Record Center for Images is Web-based, providing its functionality to all end users through a Web browser, with no client software to install, update, or configure.

SECURITY FEATURES

The Digital Record Center for Images offers advanced security measures related to data access, transmission,and is located in a secure vault that ensures your data is always protected.

DATA ACCESS SECURITY

Users accessing the Digital Record Center for Images can only access authorized data and are restricted to their document security assignments for functions such as updating metadata and adding annotation notes.

To ease system administration, users are organized into user groups with default group privileges, such as data access or system functions, allowing convenient security settings to be established and assigned to logical organizational groups. When new users are provided system access, their security assignments will be inherited based upon the group that they are in.

Users have no access to or awareness of projects, folders, or documents that they are not authorized to see. This lowers the security risk for the entire system.

Iron Mountain utilizes WORM (Write Once Read Many) tape media to ensure that once customer data is stored it cannot be modified. This option is available upon request.

SECURE SOCKET LAYERS

The Digital Record Center for Images is implemented using Secure Socket Layer (SSL), a protocol for transmitting documents via the Internet using encryption technology. This ensures an extremely high level of data transmission security through 1024-bit encryption technology. As information is transferred between the server and the Web clients, all data is encrypted.

The Digital Record Center for Images uses server-side certificates to encrypt the data using SSL for the Web application. Any Internet traffic that lands on the clear text site using HTTP will be redirected to the secure port for HTTPS. When using Web services integration, a two-way authentication is employed using both client and server-side certificates. All unauthorized requests are rejected. If a customer uses FTP for ingesting assets/documents, access is provided through a secure FTP channel that assigns each customer a unique user name and password. All data is securely and separately stored.

PHYSICAL SECURITY

Within the United States, the Digital Record Center for Images system is housed in Iron Mountain's 15,000 square-foot underground data center in western Pennsylvania. The facility is 220 feet underground and is a Tier 3 data center with multiple active power and cooling distribution paths. With redundant components, the facility provides 99.982 percent availability. The site has emergency power, CCTV, magnetometers, and X-ray machines, all secured by a five-ton gate at its entrance and armed guards on duty 24/7.

The facility is operationally self-sufficient with redundant commercial power feeds and diverse telecom providers as well as full backup power for up to seven days. The facility also has an EPA-certified water treatment plant, an OSHA-certified fire company, 24-hour maintenance, and a 24/7 service operation.

The data center is controlled by electronic access, with CCTV monitoring throughout. It is also protected by a clean agent fire extinguishing system (CAFES) with a preaction (dry pipe) sprinkler system as a backup. Electrical equipment is segregated in a separate room from the computing equipment and all segregating and outside walls and doors are three-hour fire rated. Redundancy is built in throughout the entire facility to provide ultra-reliable service and continuous uptime.

SYSTEM LEVEL SECURITY

The Digital Record Center for Images servers are protected with several layers of system security. The system is deployed in a multi-tier architecture; each tier is protected by multiple firewalls which restrict traffic flows from the Internet as well as between the tiers. For example, a DMZ secures Internet traffic from going directly to the application servers and from the application servers to the data servers. All ports are secured individually between the systems.

Once into the Iron Mountain realm, intrusion detection systems and multiple firewalls at each layer (Web, Application and Data Tier) protect the information by restricting access based on defined policies. Access to the system is also restricted by securing ports and IP addresses.

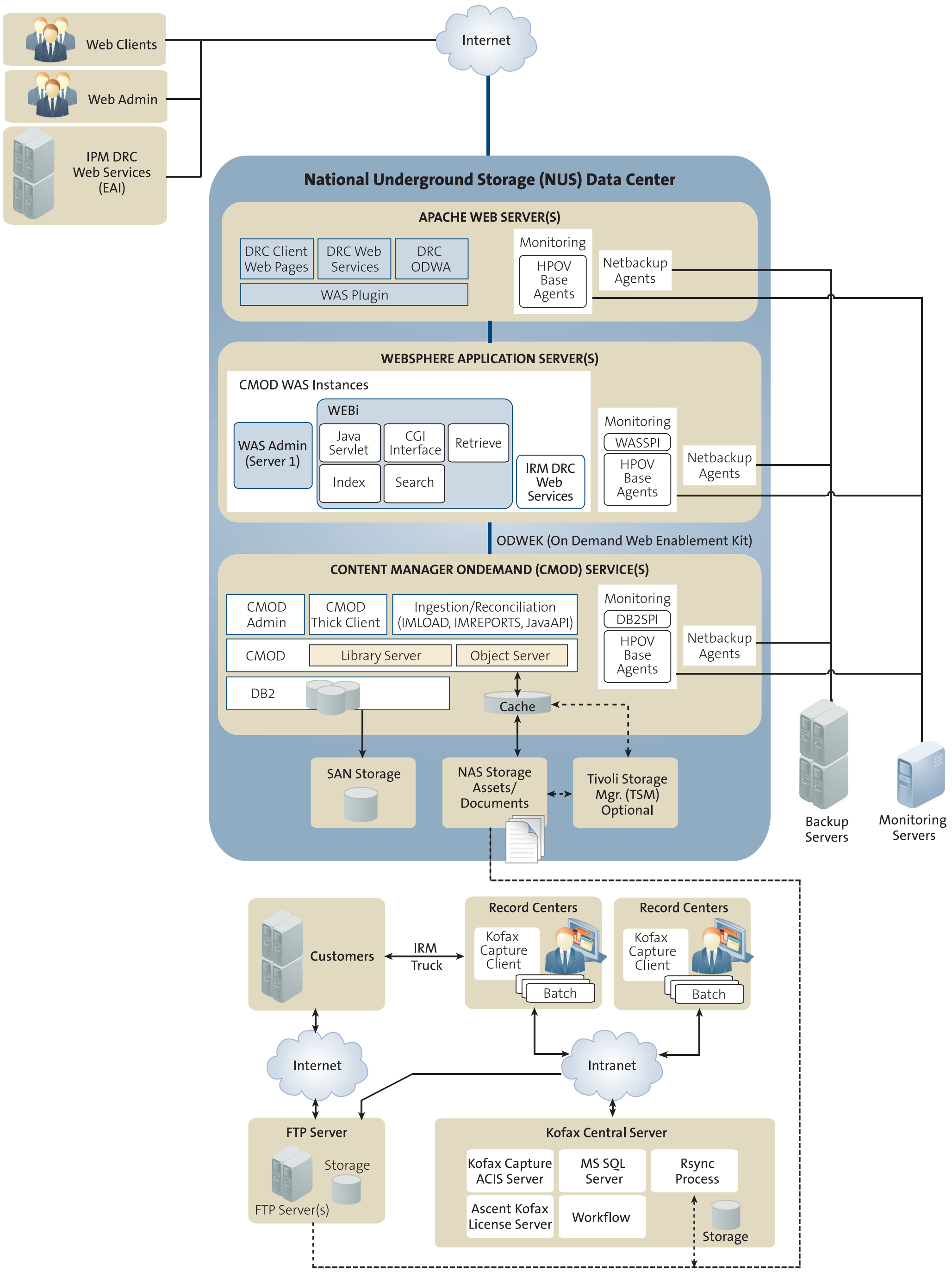
SYSTEM ADMINISTRATION SECURITY

Internal access to system administration functions is restricted to authorized administrators only. Internal audit policies ensure there is no unauthorized access to the Digital Record Center for Images systems.

SECURE PASSWORD PROTECTION

Digital Record Center for Images application authentication is provided by IBM's Tivoli® Directory Server. During implementation, Iron Mountain works with each customer to define authentication attributes that are used to create a unique security policy tailored to their needs. Attributes include password expiration time, minimum length, login failures, and alpha and non-alpha character requirements. By providing a unique security policy for each customer, Iron Mountain can meet both the flexibility and protection demands of every customer.

DIGITAL RECORD CENTER FOR IMAGES – SYSTEM ARCHITECTURE



INGESTION

For inbound assets, the Digital Record Center for Images uses SHA-1, a one-way hash function developed by the National Institute of Standards and Technology (NIST), to ensure file transfer integrity. A one-way hash function takes variable-length input and produces a fixed-length output. This fixed-length output is called the message digest. The hash function ensures that if the information is changed in any way — even by just one bit — an entirely different output value is produced.

This hash computation occurs twice, once by the sender to establish the message digest and once by the recipient who confirms the message digest. If the digests are not identical, corruption may have occurred during the transfer. The Digital Record Center for Images provides confirmation reports that describe the FTP/SHA-1 transaction results with intelligent messages.

INGESTION PREPROCESSING

All records go through several pre-ingestion processing phases to ensure that they are eligible for ingestion. A batch with files deemed ineligible — it does not pass one of the pre-ingestion processing phases — is sent to a rejected file directory for further investigation, and an email is sent to the system administrator. The following provides an overview of pre-ingestion processing:

- **Unzip/Uncompress Files.** If files have been compressed and bundled in zip files, the zip files must be unzipped before ingestion in order to extract and process each individual file properly.
- **Decryption.** Files sent to Iron Mountain for storage in the Digital Record Center for Images are encrypted to ensure secure data transmission. Once files are transferred, each file must be decrypted to extract the necessary index values (metadata) and other asset information.
- **Data Authentication.** Customers may optionally provide an SHA-1 hash value which is recalculated on receipt of the file to verify a successful FTP transmission. In addition, when assets are moved between capture servers and FTP serves, hash values are created both before and after the transfer so that the original file is removed, but only after the values match. All files are also time/date stamped to help ensure the authenticity of archived assets.
- **Untar Files.** Files created by a .tar program must be processed to obtain full assets. For example, a customer might send a compressed tarball containing multiple assets (assets.tar.gz). The pre-ingestion process uncompresses and untars these files in order to obtain the underlying assets for ingestion.

RECONCILIATION

Iron Mountain has created an exclusive process to improve the standard ingestion process by incorporating the high-level enhancements such as batch validation; data type and field level validation with autocorrect; reconciliation reporting; flexible disposition options; and feedback.

- **Batch Validation.** Prior to attempting to ingest the batch into the Digital Record Center for Images, the content of the batch will be validated to ensure all of the expected files, documents, and pages have been properly received. Validating on the front end of the process alleviates most of the downstream issues. Failed batches will be moved to a review directory for analysis and disposition.
- **Data Type and Field-Level Validation with Autocorrect.** In addition to batch validation, index data types and optionally some field-level validation will be performed in order to:
  - Avoid adding index values that are known to be incorrect.
  - Optionally autocorrect fields in error and mark these corrected records for review.
  - Avoid attempting to process batches the Digital Record Center for Images will reject and subsequently back out.

- **Reconciliation Reporting.** The Digital Record Center for Images's proprietary ingestion process produces reconciliation reports which highlight, and give details on, exceptions to the ingestion process. These reports will contain all the information needed to determine the cause or causes of the problem. Using this approach, the Digital Record Center for Images operations team, the scanning operations teams, and customer administrators are able to look at the same information to quickly identify and resolve any issues.
- **Flexible Disposition Options.** Configuration parameters can be added that allow flexibility regarding the disposition of successfully ingested batches. Options for disposition include:
  - Delete successfully ingested batches, or
  - Move successfully ingested batches to a backup directory.
- **Feedback.** If so configured, an XML file will be created at the conclusion of processing and made available to the upstream process. The upstream process can then use this information to update its own reconciliation process or use it in any other manner. Email notifications are also available, with click-through link to the exception report for easy access. This full feedback loop allows for tracking the chain of custody of the ingested documents.

DESKTOP UPLOAD CAPABILITIES

Desktop Upload allows you to quickly and simply upload digital files from your desktop to the Digital Record Center for Images. This intuitive, web-based application provides the option to store digital and converted files together, in one location, for use by authorized employees in multiple settings. Mandatory metadata fields index each file for simple document retrieval. Desktop Upload ensures the traceability of digital content added to the Digital Records Center for Images by adding User ID's and reference numbers to all uploaded content available for viewing. Additionally, this hosted solution provides user notifications when uploaded content is available for viewing.

ADMINISTRATION TOOL

The Digital Record Center for Images's administration tool is a convenient and simple way for customer administrators to manage their Digital Record Center for Images users. This intuitive Web-based UI enables administrators to perform user administrative tasks such as adding, removing, activating, and deactivating users, adding and removing users from groups, and resetting user passwords. User management is further simplified by automatic email notification to users when their accounts are initially set up and when passwords are reset.

HIGH AVAILIBILITY

The Digital Record Center for Images infrastructure utilizes field-proven IBM hardware and software. It is configured as a redundant, fault-tolerant architecture with no single point of failure which includes all components of hardware and software. IBM's High Availability Cluster Multiprocessing (HACMP) helps protect the Digital Record Center for Images from failures by providing reliable monitoring, failure detection, and automated recovery of the application environment to backup resources, all transparently to the user.

HACMP monitors, detects, and reacts to conditions, maintaining service availability during random, unexpected system or software problems. In the event of a problem, the system automatically fails over to the passive node with no interruption in service.

All data I/O internal to the Digital Record Center for Images is transmitted using Multipath Input/Output (MPIO) capabilities to the storage devices to maximize throughput and provide efficient routing.

STORAGE SOLUTION

The Digital Record Center for Images uses state-of-the-art storage technologies. Both Storage Area Networks (SAN) and Network Attached Storage (NAS) are used to provide a balance between cost and reliability and efficiency. SAN storage is used for high security, high performance, and throughput for storing metadata in databases. NAS storage is used to keep all the archive data online and on spinning disk which provides a cost-effective way to scale while still having the documents available within seconds for retrieval by the Digital Record Center for Images user.

This solution is completely redundant with multiple hardware solutions that include Fibre Channel adapters, network interface cards, SAN fabric, and switches which are supported by multi-pathed input/output for redundancy and resilience.

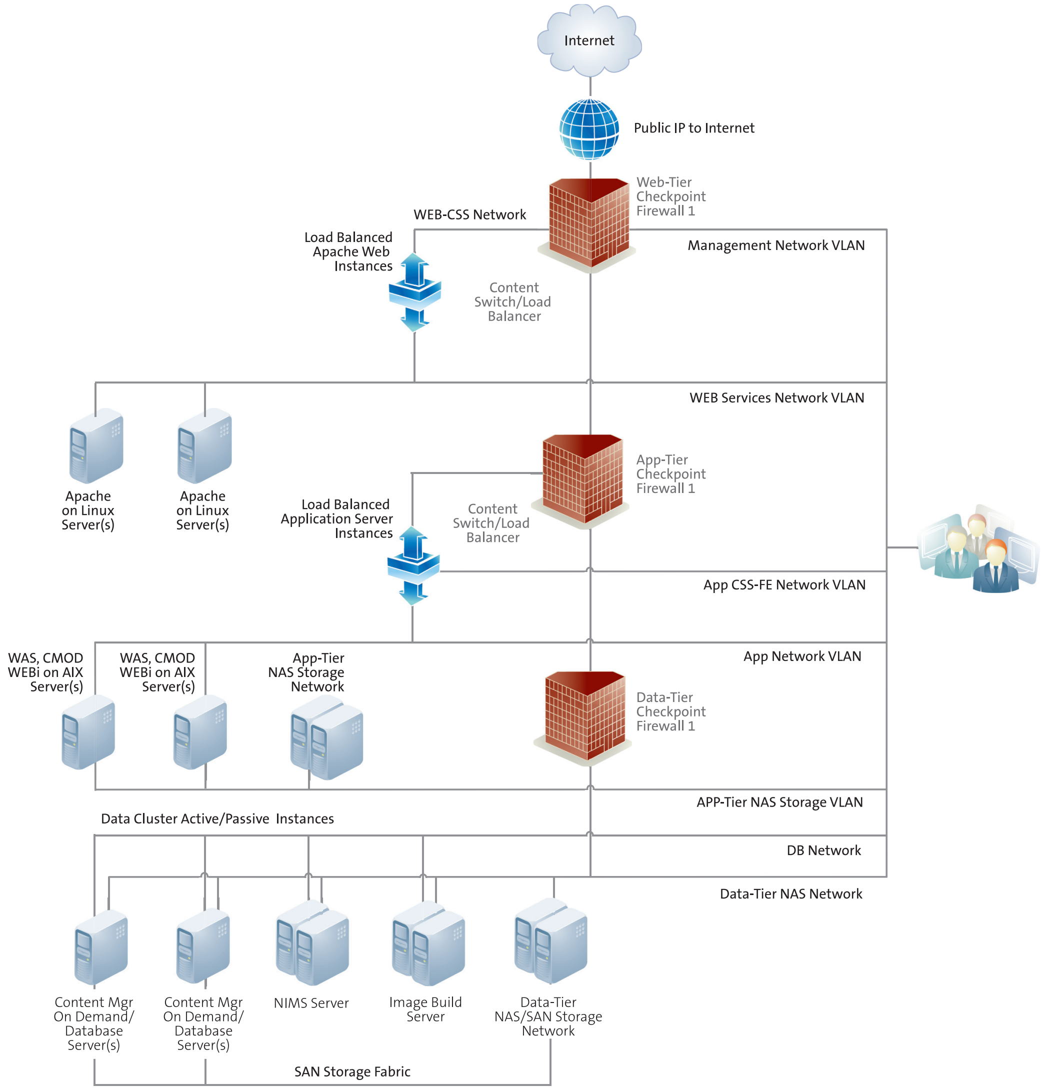
DISASTER RECOVERY

Iron Mountain's Disaster Recovery (DR) site for the Digital Record Center for Images is located in an underground facility that is geographically separated from the primary facility. In the case of a disaster at the primary data center, the Digital Record Center for Images will continue operations from the disaster recovery site.

OFFSITE BACKUP

All data from the Digital Record Center for Images is also backed up on a regular schedule. Incremental backups are performed nightly and full backups are carried out each week with tapes held for 30 days. A full backup is also conducted on a monthly rotation with tapes held for thirteen months. Once created, the tapes are removed from the underground facility and stored in a secure fireproof vault at a separate location.

DIGITAL RECORD CENTER FOR IMAGES – NETWORK ARCHITECTURE


Internet
Public IP to Internet
Web-Tier Checkpoint Firewall 1
WEB-CSS Network
Load Balanced Apache Web Instances
Content Switch/Load Balancer
Management Network VLAN
WEB Services Network VLAN
Apache on Linux Server(s)
Apache on Linux Server(s)
Load Balanced Application Server Instances
Content Switch/Load Balancer
App-Tier Checkpoint Firewall 1
App CSS-FE Network VLAN
WAS, CMOD WEBi on AIX Server(s)
WAS, CMOD WEBi on AIX Server(s)
App-Tier NAS Storage Network
App Network VLAN
Data-Tier Checkpoint Firewall 1
APP-Tier NAS Storage VLAN
Data Cluster Active/Passive Instances
DB Network
Data-Tier NAS Network
Content Mgr On Demand/ Database Server(s)
Content Mgr On Demand/ Database Server(s)
NIMS Server
Image Build Server
Data-Tier NAS/SAN Storage Network
SAN Storage Fabric

SYSTEM MONITORING

Each physical machine in the environment is monitored for up/down status using an enterprise service monitoring solution. The critical system functions that are monitored include system parameters such as CPU, memory, I/O, network, processes and many others. The service monitoring solution is also set up to monitor the applications and the software running on the systems which include Web, application, database, and FTP servers, IBM Content Manager OnDemand, storage volumes, ingestion rates, etc. Threshold values are set up to notify the appropriate teams when action is required.

In addition, a synthetic transaction runs to ensure that all of the components are functioning optimally. This synthetic transaction will monitor how long a transaction takes so system accessibility can be measured. It will also ensure that the system is available for functions such as logging in and searching the archive.

The synthetic transaction is initiated from different geographic locations including California, Massachusetts, Illinois, New York, and Europe to determine the network latency to monitor both internal and external response times.

Should an alert be triggered, an email notification and a phone alert are automatically generated to the emergency personnel on call for the component that failed. The system requires that the alert be acknowledged or it will automatically escalate to the next level.

Support staff at the Network Operating Center (NOC) continuously monitors and responds to these notifications.

SYSTEM SUPPORT

Iron Mountain provides 24/7 support via phone and e-mail for the Digital Record Center for Images, with multiple tiers of support depending on the severity of the issue. As with system monitoring, issues automatically escalate to the next level should that be required.

THE DIGITAL RECORD CENTER FOR IMAGES WEB SERVICES API

A Web services-based Application Programming Interface (API) is available which enables software integration links to be developed between the Digital Record Center for Images and existing information systems such as Enterprise Resource Planning (ERP) Systems, Product Data Management (PDM) Systems, Geographic Information Systems (GIS), or Project Management Systems. By utilizing this API set, customers gain access to a number of convenient integration methods that will directly link important corporate information systems with the Digital Record Center for Images.

SUMMARY

Company policy, industry standards and legal regulations dictate the requirements that must be met when deploying and managing a data center for digital assets. Providing an efficient, scalable, secure environment that meets these standards requires the right mix of the latest technology, extensive industry know-how and tight controls based on proven best practices. With the Digital Record Center for Images, Iron Mountain leverages our technology and expertise to provide organizations with a cost-effective, highly robust solution to their digital storage needs. As this paper describes, Iron Mountain has created a first-class data center and infrastructure based on efficient industry standard platforms. By adding enhancements in the area of security, high availability, reporting and integration, linked with the control of the physical documents and ingestion process through an audited chain of control, Iron Mountain's Digital Record Center for Images can ensure important corporate information is always safe and secure, yet quickly accessible by authorized users when needed.

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at www.ironmountain.com for more information.