Contingency Planning and Disaster Recovery

Best Practices

Version: 7.3.x

Written by: Product Knowledge, R&D
Date: June 2019

Hyland

© 2015-2019 Hyland Software, Inc. and its affiliates.

Table of Contents

Perceptive Content Contingency Planning 4
Back up your data 4
Back up application files 4
Back up the Perceptive Content database 5
Back up the Perceptive Content OSM 5
Mirror the OSM 6
Select high-availability hardware 6
Use redundant NICs 7
Select reliable object storage hardware 7
Use RAID systems 7
Select DAS, NAS, or SAN technology 7
Use DAS storage 7
Use NAS storage 8
Use a SAN 8
Implement server mirroring and failover 9
Server mirroring to minimize data loss 9
Use failover clusters 9

Perceptive Content Contingency Planning

In all businesses, disaster recovery involves a series of actions to take when an unplanned event occurs that causes data loss, such as a power outage or hardware failure. Companies need to be aware of these issues and develop a contingency plan to determine how to avoid them. Although contingency planning involves hardware and networking that fall beyond the scope of Perceptive Content software, this document provides information about best practices in regards to systems that include products from Perceptive Software, Inc.

There are certain factors to keep in mind when planning your system backup strategy. To reduce the time and dollars spent on recovery, assess and plan for various types of disasters that may occur. For example, you can plan for issues like disk failure, server failure, and a more comprehensive network failure. Your contingency plan may cover everything from day-to-day backups to major disaster recovery.

The following information presents a high-level picture of the tasks associated with disaster recovery – from backing up your data to selecting high availability hardware. Redundancy strategies, such as mirroring and failover, are also covered. As you develop your contingency plan, these topics are provided as background information. This document does not outline specific solutions for your database configuration or business process; it is designed to be a description of the best practices involved in contingency planning.

Back up your data

It is important that your system administrator back up application files, the Perceptive Content database, and the Object Store Manager (OSM) on a routine basis. At a minimum, create nightly routines to back up the Perceptive Content database and OSM. Related information for system redundancy is available on the Product Documentation tab of the Customer Portal on www.perceptivesoftware.com.

Remember that even when you make a backup, test it, and complete it successfully, you can expect a loss of data after a disk, server, or catastrophic failure. You can only recover data that was present at the time the backup was made. If your daily document processing rate is high enough that your company wants to guard against the loss of a day's work, you can set interim backup times throughout the day or, depending on your database and operating system, set up a dynamic backup.

We recommend that you back up your application files, database, and the OSM on a regular basis to keep your data secure. You can create a batch file that runs nightly to back up these folders. You can also use third-party backup and recovery tools. Some database backup and recovery tools are specific enough that they can actually recover single rows and columns within an individual database table.

Back up application files

The application files you need to back up are located in the \inserver6 folder. These files include scanned batches that are not fully processed, configuration files, workflow scripts, LearnMode templates, and executable files. You need these files to recover and recreate your system, as well as the data stored in the database and the OSM.

Back up the entire \inserver6 folder on a daily basis. To conserve space on your backup media, you can choose whether to back up the \inserver6\log and \inserver6\temp folders. Refer to the following documents available on the Product Documentation tab of the Customer Portal on www.perceptivesoftware.com:

- *Oracle Database Best Practices Guide*. Refer to this document for information regarding best practices for backing up data using an Oracle database.
- *Microsoft SQL Server Best Practices Guide*. Refer to this document for information regarding the best practices for backing up data using a Microsoft SQL Server database,

- *Active Passive Failover Cluster Advanced Design Guide*. Refer to this document for information regarding the setup of Perceptive Content in a failover cluster environment.
- *Active-Active and High Availability Advanced Design Guide*. Refer to this document for a high-level overview of setting up Perceptive Content Server in an active-active environment, and in a highly available, clustered environment.

Back up the Perceptive Content database

The location of your Perceptive Content database depends on the type of database you use with the Perceptive Content Server. The Perceptive Content database, named INOW6, contains information about the objects you scan and process.

- If using an external database (such as SQL Server, Oracle, or DB2), back up the INOW6 database using the procedures specified in your database documentation.

In many cases, you cannot back up files that are currently being used. The INOW6 database is always in use by the various processes that are running. As part of your standard backup routine, you must stop all ImageNow Services and make sure that users are not logged on. However, if you need to perform backups during the day, you might consider purchasing third-party backup software, like Veritas, that performs active backups to copy files while they are in use. If you implement a solution that backs up open files, we strongly recommend testing the ability to recover those files.

Back up the Perceptive Content OSM

Another critical storage element on Perceptive Content Server is the Object Storage Manager (OSM). The OSM stores three types of information in separate locations, including:

- Perceptive Content documents (image, TXT, PDF, and other files).
- Sub-objects, such as bitmap stamp annotations, embedded OLE annotations, thumbnails, DataCapture data, and worksheets.
- Document batches that have not yet been linked or automatically processed.

The most important storage distinction is that the INOW6 database stores the metadata of each document, and the OSM stores the actual document. You should back up the entire OSM directory structure, including all subdirectories, on a daily basis.

You can use the `list-osm-tree –osm-set <set id>` INTool command to display a list of all OSM sets. Then, you can back up the OSM that contains the documents (OSM_01.00001), the OSM that contains the sub-objects (OSM_02.00001), and the OSM that contains the document batches (OSM_03.00001). By default, the system installs INTool during the Perceptive Content Server installation. For more information about OSM INTool commands, refer to Administrator Topics > Managing Perceptive Content > Administer using Command Line Tools > INTool commands in Administrator Help.

An OSM backup can take several hours to complete. Make sure that you give your backup routine plenty of time to run. If backups take too long, you may need to take measures to speed up the process.

The speed of the backup is directly related to the speed of the backup hardware. If your backups begin taking longer to complete, you may need to switch to higher performance backup hardware and media; for example, digital linear tape (DLT). If the size of the OSM becomes too large to complete a full backup each night, consider a differential backup approach.

Mirror the OSM

If Perceptive Content is a critical application for your enterprise, we recommend you use a third party solution to perform the mirroring on the OSM.

OSM mirroring enables you to create a duplicate OSM for disaster recovery and backup. It provides real-time redundancy of the OSM by placing a copy of the OSM on another path in the file system.

OSM mirroring is accomplished using INTool commands. For more information about OSM INTool commands, refer to Managing Perceptive Content > Administer using Command Line Tools > INTool commands in Administrator Help.

When choosing an OSM mirroring solution, consider the following options.

- Mirroring takes twice as much disk storage space because there is two complete real-time copies of OSM, and slows system performance.
- If the drive where the primary OSM storage fails after you select OSM mirroring, Perceptive Content automatically attempts to read the data from the secondary location.
- While you can read files if your primary OSM location fails, you cannot write any new data, including images.
- Before actions in Perceptive Content are considered complete, the data must write to both the primary and secondary OSM storage locations.
- For the data to store successfully, it must be written to both the primary and secondary storage locations. If one of the data write processes fails, both locations fail to store the data.

If Perceptive Content is a critical application for your enterprise, we recommend you use a third party solution to perform the mirroring on the OSM.

Select high-availability hardware

High-availability means that the system must be available at all times. If your data needs high-availability, consider using one or more of the following hardware solutions. Although there are many high-availability solutions, here is a list of hardware to consider when you develop your contingency plan for the Perceptive Content system.

- Redundant NICs
- Object storage hardware
- RAID systems

You can also choose to replicate hardware within your system to ensure against data loss. There are many types of data loss. While we typically think of catastrophic loss, a contingency plan should account for events such as hardware losses and power failures. For example, you can work around some potential hardware issues by purchasing servers that include multiple hard drives and multiple power supplies.

Use redundant NICs

To protect against faulty network cards, you can add two network interface cards (NICs) to your TCP/IP-based Perceptive Content Server computer. An NIC connects a computer to an Ethernet network, and it usually contains the protocol firmware and controller needed to support the Medium Access Control data link protocol used by Ethernet. You must purchase an Perceptive Content product license for the primary NIC and obtain a failover license agreement for the secondary NIC. Therefore, if you have two NICs for redundancy, make sure that you license both of them so that the secondary card is ready to use when you need it.

Select reliable object storage hardware

You can use a redundant array of independent disks (RAID) level-5 system or an object-specific storage system to store the OSM. The object store needs to be directly accessible by Perceptive Content Server, and you can use a local drive or a network drive using a UNC path. The object store for scanned images and other documents can grow quite large. As a rule, one million scanned pages consume approximately 50 GB of storage.

You can also use a third-party hierarchical storage management (HSM) system to store OSM data. An HSM system stores objects in tiers, based on the frequency of access. Since the main purpose of object storage is to store fixed content in a form that is easy to access, an HSM system works well with the OSM. Be sure to consult with the HSM software documentation for recommendations and requirements on backup strategies.

Use RAID systems

Disk failures comprise a majority of all hardware device failures in server systems. Many companies choose RAID systems for improved performance, data protection, and fault tolerance for disk failures. RAID systems offer high performance, storage capacity, scalability, and survivability, which are the features that lead to high reliability.

Select DAS, NAS, or SAN technology

Certain types of information can be stored on Direct Attached Storage (DAS), Network Attached Storage (NAS), or Storage Area Network (SAN). For example, you can store the Perceptive Content application, database, or OSM in DAS or SAN. In NAS, you can only store the OSM.

Perceptive Content Object	DAS	NAS	SAN
Application	X		X
Database	X		X
OSM	X	X	X

Use DAS storage

DAS describes a storage device that is directly attached to a host system. The simplest example of DAS is the internal hard drive of a server computer. Your contingency plan needs to cover what to do when a server goes down. In a DAS environment, a server failure means that the data contained in that server is no longer available to users. You can use DAS storage for the Perceptive Content application, database, and OSM.

Use NAS storage

NAS is a data storage mechanism that uses special devices connected directly to the network. These devices are assigned an IP address which clients access using a server that acts as a gateway to the data. The benefit of a NAS structure is that although it may contain many servers, you can centralize the storage of data. This means that you can centralize the security, management, and backup of your data. A simple example of a NAS system is a CD-ROM tower, which is a stand-alone entity with multiple CD-ROM drives that is connected directly to the network.

A NAS is easy to expand, so if you need more storage space, you can add another NAS device and increase the available storage. You can add fault tolerant measures, such as RAID, to make sure that the NAS device does not become a point of failure. You can use NAS for the OSM. NAS is not recommended for the Perceptive Content application or database.

Use a SAN

A SAN is a dedicated network that is different from standard Local Area Networks (LANs) or Wide Area Networks (WANs). The difference is that a SAN interconnects storage resources using highly scalable architecture. Companies use SANs because of the network's extremely high interconnection data rates between storage peripherals. This type of network includes hardware and specialized management software.

SAN hardware usually includes a variety of information devices, including RAID storage systems, hubs, switches, bridges, servers, backup devices, interface cards, and cabling. A SAN makes it possible for devices to communicate with each other on a separate network. This communication provides many advantages, including the ability to back up every piece of data on your network independently. You can use SAN storage for the Perceptive Content application, database, or OSM.

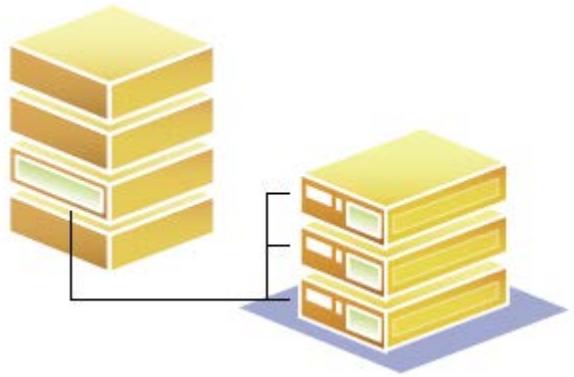
Implement server mirroring and failover

Perceptive Content supports server mirroring and failover technologies. These redundancy features enhance the reliability of your Perceptive Content system. These technologies are often included in high-availability systems.

Server mirroring to minimize data loss

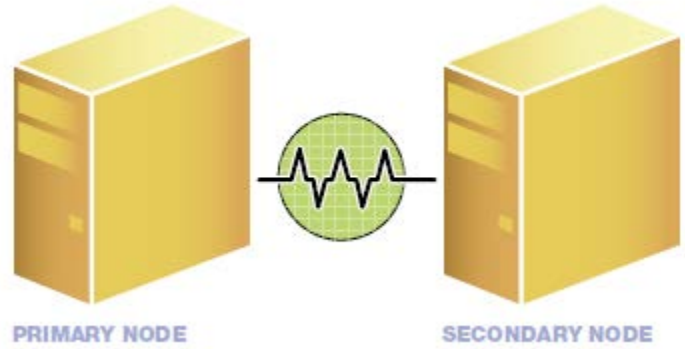
Redundancy through server mirroring lets you minimize data loss or recover data and system information. Redundancy usually involves implementing two systems, which allows you to switch one system to another and quickly resolve hardware or system-loss issues on the original machine. Mirroring ensures that the data is available from multiple sources in near real time. Perceptive Content supports “active mirroring”. Therefore, after the system switch occurs, you must restart ImageNow Services on the new system using a batch file or script.

Traditional mirroring only works over limited distances. Storage area network (SAN) and similar technologies can overcome distance issues, but they are typically costly.



Use failover clusters

In clustering, both servers share the disk array but only one server controls the disks. The clustering service uses a heartbeat to monitor the state of the primary server. In the event that one server fails, the clustering service automatically transfers control of the disk array to the other server, and so the database or file server stays up.



Failover can provide redundancy of the Perceptive Content Server services. A failover server can be particularly beneficial to customers using Perceptive Content across their enterprise in support of critical

business processes such as hospital patient records. This option requires the execution of a failover license agreement to allow a failover setup on an additional server, as well as additional server hardware and a virtual machine or secondary NIC.