



IBM Systems - iSeries  
Systems Management  
Availability roadmap

*Version 5 Release 4*







IBM Systems - iSeries  
Systems Management  
Availability roadmap

*Version 5 Release 4*

**Note**

Before using this information and the product it supports, read the information in "Notices," on page 23.

**Fourth Edition (February 2006)**

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© Copyright International Business Machines Corporation 1998, 2006. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Availability roadmap</b> . . . . .	<b>1</b>	Shorten planned outages . . . . .	12
What's new for V5R4 . . . . .	1	Shorten backup windows. . . . .	13
Availability concepts. . . . .	1	Shorten software maintenance and upgrade windows . . . . .	15
Estimate the value of availability . . . . .	2	Shorten hardware maintenance and upgrade windows . . . . .	15
Decide what level of availability you need . . . . .	3	Availability for multiple systems: Clusters . . . . .	16
Prevent unplanned outages . . . . .	5	Data resilience solutions for i5/OS Clusters. . . . .	17
Prepare for disk failures . . . . .	5	Related information for Availability roadmap . . . . .	19
Plan for power loss . . . . .	7		
Use effective systems management practices. . . . .	8		
Prepare the space for your server . . . . .	8	<b>Appendix. Notices</b> . . . . .	<b>23</b>
Shorten unplanned outages . . . . .	9	Trademarks . . . . .	24
Reduce the time to restart your system . . . . .	9	Terms and conditions . . . . .	25
Recover recent changes after an unplanned outage . . . . .	10		
Recover lost data after an unplanned outage . . . . .	11		
Reduce the time to vary on independent disk   pool. . . . .	12		



---

## Availability roadmap

In today's fast-paced Internet environment, it is crucial that your data and applications be available to you when you need them. If your customers cannot access your Web site because your system is down, they may go to your competitors instead.

*Availability* is the measure of how often your data and applications are ready for you to access when you need them. Different companies have different availability needs. Different systems or different applications within the same company may have different availability needs. The purpose of this topic is to guide you through the world of iSeries™ availability and help you decide which availability tools are right for your business. It is important to note that availability requires detailed planning; these availability tools are only useful if you have implemented them **before** an outage occurs.

Before you can really start to plan for availability on your system, you should become familiar with basic availability concepts, understand the costs and risk associated with outages, and determine your company's needs for availability. Once you have a basic understanding of availability concepts and know what level of availability you need, you can start to plan for that level of availability on a single system or for multiple systems within a cluster environment.

---

## What's new for V5R4

Learn about new function that relates to the Availability roadmap.

### Enhancements to Availability roadmap information

For this release, several updates have been made to the information. These updates include the following topics:

- Descriptions of new disk pool features, such as auxiliary cache IOP and RAID
- New information on data resilience technologies
- New information on saving from a second copy of data
- Enhancements to current information on save window reduction, SMAPP and journaling

---

## Availability concepts

Before you can plan for the availability of your system, it is important for you to understand some of the concepts associated with availability.

Businesses and their IT operations that support them must determine which solutions and technologies will address their business needs. In the case of business continuity requirements, the task is equally daunting. Detailed business continuity requirements must be developed and documented, the solution types identified, and the solution choices evaluated. This is a challenging task due in part to the complexity of the problem.

*Business continuity* is the capability of a business to withstand outages, which are times when the system is unavailable, and to operate important services normally and without interruption in accordance with predefined service-level agreements. To achieve a given desired level of business continuity, a collection of services, software, hardware, and procedures must be selected, described in a documented plan, implemented, and practiced regularly. The business continuity solution must address the data, the operational environment, the applications, the application hosting environment, and the end-user interface. All must be available to deliver a good, complete business continuity solution. Your business continuity plan includes disaster recovery (DR) and high availability (HA).

Disaster recovery (DR) provides a plan in the event of a complete outage at the production site of your business, such as during a natural disaster. DR may provide a set of resources, plans, services, and procedures used to recover important applications and to resume normal operations from a remote site. This *Disaster Recovery Plan* includes a stated disaster recovery goal (for example, resume operations within eight hours) and addresses acceptable levels of degradation.

Another major aspect of business continuity goals for many customers is *high availability*, which is the ability to withstand all outages (planned, unplanned, and disasters) and to provide continuous processing for all important applications. The ultimate goal is for the outage time to be less than .001% of total service time. The differences between high availability and disaster recovery typically include more demanding recovery time objectives (seconds to minutes) and more demanding recovery point objectives (zero end user disruption).

Availability is measured in terms of *outages*, which are periods of time when the system is not available to users. During a *planned outage* (also called a scheduled outage), you deliberately make your system unavailable to users. You might use a scheduled outage to run batch work, back up your server, or apply fixes.

Your *backup window* is the amount of time that your server can be unavailable to users while you perform your backup operations. Your backup window is a scheduled outage that usually occurs in the night or on a weekend when your system has less traffic.

An *unplanned outage* (also called an unscheduled outage) is usually caused by a failure. You can recover from some unplanned outages (such as disk failure, system failure, power failure, program failure, or human error) if you have an adequate backup strategy. However, an unplanned outage that causes a complete system loss, such as a tornado or fire, requires you to have a detailed disaster recovery plan in place in order to recover.

High availability solutions provide fully automated failover to a backup system to ensure continuous operation for end users and applications. These HA solutions must provide an immediate recovery point and ensure that the time of recovery is faster than a non-HA solution.

Unlike with disaster recovery, where entire systems experience an outage, high availability solutions can be customized to individual critical resources within a system, for example a specific application instance. On the i5/OS™ system, the high availability solution is based on cluster technology. You can use i5/OS Clusters as a method to avoid the impacts of both planned and unplanned outages. Even though you still have the outage of the server, the business function will not be impacted by the outage. A *cluster* is a collection of interconnected complete systems used as a single, unified resource. The cluster provides a coordinated, distributed process across the systems to deliver the solution. This results in higher levels of availability, some horizontal growth and simpler administration across the enterprise. For a complete solution, you must address the operational environment, the application hosting environment, application resilience, and the end-user interfaces in addition to providing data resilience mechanisms. Clusters focus on all aspects of the complete solution. The integrated cluster resource services enable you to define a cluster of systems and the set of resources that should be protected against outages. Cluster resource services detect outage conditions and coordinate automatic movement of critical resources to a backup system.

---

## Estimate the value of availability

No one would argue the importance of availability. However, when asked to justify the cost of additional hardware to support improved availability, many people do not know how to build a case.

The following steps describe how to estimate the value of your information services:

1. **Develop a list of the major services and solutions that your system provides.** Your system exists so that end users and solutions can accomplish tasks that are critical to the operation of your business.

- | The systems provide solutions to a business function. If the system is unavailable, the business function cannot be completed or is significantly degraded to the point of causing the business lost revenue or increased expenses.
- | 2. **Assess how much it costs you when these services are unavailable.** Each application or service has a direct affect on business functions. You need to determine how these business functions would be affected and what would be the overall cost to your business.
- | 3. **Look at direct costs versus indirect costs.** Direct costs are losses that can be traced directly to a system being unavailable. Indirect costs are those that are incurred by another department or function as a result of an outage.
- | 4. **Consider tangible costs versus intangible costs.** Tangible costs are those that can be measured in currency. However, there are other costs that are not measured with money, such as market share, lost opportunity, and good will.
- | 5. **Analyze fixed costs versus variable costs.** Fixed costs are those that result from a failure and are the same, regardless of the length of the outage. Variable costs are those that vary, based on the length of the outage.

---

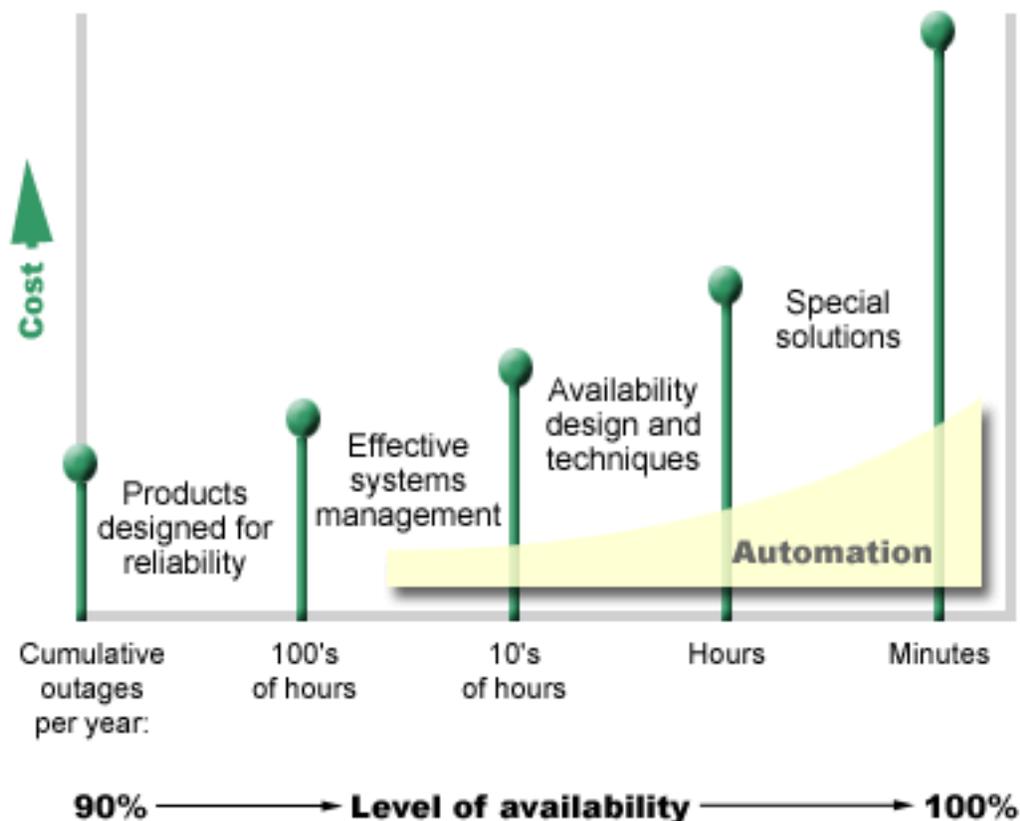
## Decide what level of availability you need

- | After understanding availability at a basic level, it important to assess your individual availability needs.
- | Higher availability is more costly than a lower level availability. You must balance your needs and services with the overall cost of implementing and maintaining these availability solutions.

You want to be sure that you have analyzed your business needs thoroughly in order to decide what level of availability you can afford to maintain. To decide what level of availability you need, consider the following questions:

### Do you have any applications that require 100% availability?

In most cases, you can achieve a high level of availability by implementing sound processes and systems management practices. The closer you need to be to continuous availability, the more of an investment you have to make. Before you make that kind of investment, you should be sure that you require that level of availability. The following figure shows how different techniques can improve availability, but can increase the price you have to pay for it.



- | If your requirements for levels of availability increase, you may want to consider multiple system availability solutions, such as clusters.

### How much downtime is acceptable to you?

It may help you to know what amount of downtime each level of availability represents. The following table shows the amount of downtime you should expect for different levels of availability.

Level of availability	Downtime per year
90%	36.5 days
95%	18.25 days
99%	3.65 days
99.9%	8.76 hours
99.99%	50 minutes
99.999%	5 minutes

Along with knowing how much downtime is acceptable to you, you need to consider how that downtime may occur. For example, you may think that 99% availability is acceptable if the downtime is a series of shorter outages that are distributed over the course of a year. But, you may think differently about 99% availability if the downtime were actually a single outage that lasts 3 days.

- | You also need to consider when a downtime is acceptable and when it is not. For example, your average annual downtime goal per year might be 9 hours. If that downtime were to occur during critical business hours, it could have an adverse affect on the bottom line revenue for your company.

## What level of access do your customers need to your business?

It used to be that customers and business partners accessed your business from 9 a.m. to 5 p.m., so it was realistic to expect that your system only had to be available during those hours. However, the Internet and a diverse global marketplace have changed that expectation; customers and business associates may expect to have access to your company's data at any time of the day or night. Your working hours may be hours or even days different from your global business partner or customer. You have to determine what your customer expectations are, and what is realistic with regard to those expectations, as you determine what level of availability you will maintain.

---

## Prevent unplanned outages

One way to approach availability is to try to prevent unplanned outages. You can use these different methods to ensure that your system experiences as little unplanned downtime as possible.

**Note:** If you have a single system and you cannot achieve the level of availability you need using these strategies, you may want to consider clusters.

## Prepare for disk failures

Because your data is spread across your disks, it is important that you consider how to protect your data in the event that one of those disks fails. Disk protection provides a means to ensure availability of data stored on disks.

Disk storage is the storage that is either internal to your iSeries server or is attached to it. This disk space, together with your server's main memory, is regarded by your system as one large storage area. When you save a file, you do not assign it to a storage location; instead, the system places the file in the location that ensures the best performance. It may spread the data in the file across multiple disk units, if that is the best option. When you add more records to the file, the system assigns additional space on one or more disk units. This way of addressing storage is known as *single-level storage*.

In addition to internal disk storage, you can also use IBM® TotalStorage® Enterprise Storage Server® (ESS) to attach a large volume of external disk units. ESS provides enhanced disk protection, the ability to copy data quickly and efficiently to other ESS servers, and the capability of assigning multiple paths to the same data to eliminate connection failures. For additional information on IBM TotalStorage Enterprise Storage Server (ESS) and its features and to determine if this solution is right for you, see Enterprise disk storage.

## Device parity protection

Device parity protection allows your system to continue to operate when a disk fails or is damaged. When you use device parity protection, the disk input/output adapter (IOA) calculates and saves a parity value for each bit of data. The IOA computes the parity value from the data at the same location on each of the other disk units in the device parity set. When a disk failure occurs, the data can be reconstructed by using the parity value and the values of the bits in the same locations on the other disks. Your system continues to run while the data is being reconstructed.

For an overview of device parity protection, see Device parity protection.

i5/OS supports two types of device parity protection:

### RAID 5

| With RAID 5, the system can continue to operate if one disk fails in a parity set. If more than one disk fails, data will be lost and you must restore the data for the entire system (or only the affected disk pool) from the backup media. Logically, the capacity of one disk unit is dedicated to storing parity data in a parity set consisting of 3 to 18 disk units

#### | **RAID 6**

| With RAID 6, the system can continue to operate if one or two disks fail in a parity set. If more than two disk units fail, you must restore the data for the entire system (or only the affected disk pool) from the backup media. Logically, the capacity of two disk units is dedicated to storing parity data in a parity set consisting of 4 to 18 disk units.

| See Elements of device parity protection for detailed comparison of RAID 5 and RAID 6.

#### | **Write cache and auxiliary write cache IOA**

| When the system sends a write operation, the data is first written to the write cache on the disk IOA and then later written to the disk. If the IOA experiences a failure, the data in the cache may be lost and cause an extended outage to recover the system.

| The auxiliary write cache is an additional IOA that has a one-to-one relationship with a disk IOA. The auxiliary write cache protects against extended outages due to the failure of a disk IOA or its cache by providing a copy of the write cache which can be recovered following the repair of the disk IOA. This avoids a potential system reload and gets the system back on line as soon as the disk IOA is replaced and the recovery procedure completes. However, the auxiliary write cache is not a failover device and cannot keep the system operational if the disk IOA, or its cache, fails.

| See Write cache and auxiliary write cache IOA in Disk management for detailed information on write cache and auxiliary write cache IOA.

### **Mirrored protection**

Disk mirroring is recommended to provide the best system availability and the maximum protection against against disk-related component failures. Data is protected because the system keeps two copies of the data on two separate disk units. When a disk-related component fails, the system may continue to operate without interruption by using the mirrored copy of the data until the failed component is repaired.

| Different levels of mirrored protection are possible, depending on what hardware is duplicated. The level of mirrored protection determines whether the system keeps running when different levels of hardware fail. To understand these different levels of protection, see Determine the level of protection.

| You can duplicate the following disk-related hardware:

- Disk unit
- Disk controllers
- I/O bus unit
- I/O adapter
- I/O processors
- A bus
- | • Expansion towers
- | • HSL ring

For details on mirrored protection, including how it works and how to plan for it, see Mirrored protection.

## Independent disk pools

Independent disk pools (also called independent auxiliary storage pools) enable you to prevent certain unplanned outages because the data on them is isolated from the rest of your server. If an independent disk pool fails, your system can continue to operate on data in other disk pools. Combined with different levels of disk protection, independent disk pools provide more control in isolating the effect of a disk-related failure as well as better prevention and recovery techniques. For detailed information on how to use independent disk pools, see Independent disk pools.

## Geographic mirroring

Geographic mirroring is a function that keeps two identical copies of an independent disk pool at two sites to provide high availability and disaster recovery. The copy owned by the primary node is the production copy and the copy owned by a backup node at the other site is the mirror copy. User operations and applications access the independent disk pool on the primary node, the node that owns the production copy. Geographic mirroring is a sub-function of cross-site mirroring (XSM), which is part of i5/OS Option 41, High Available Switchable Resources.

For details on geographic mirroring, including how it works and how to plan for it, see Geographic mirroring.

## Multipath disk units

You can define up to eight connections from each LUN (Logical Unit) created on the IBM TotalStorage Enterprise Storage Server (ESS) to the IOPs on an iSeries server. If you are using an ESS solution, assigning multiple paths to the same data allows the data to be accessed even though some failures may occur in other connections to the data. Each connection for a multipath disk unit functions independently. Several connections provide availability by allowing disk storage to be used even if a single path fails.

For details on multipath disk units, including its requirements, see Considerations for multipath disk units.

## Plan for power loss

To ensure that your system is available when you need it, you need to make sure that it has an adequate supply of power, and that it is protected in the event that power is lost.

## Power requirements

Part of the planning process for your system is to ensure that you have an adequate power supply. You need to understand your server's requirements and then enlist the aid of a qualified electrician to help install the proper wiring, power cords, plugs and power panels. For details on how to ensure that your system has adequate power, see Plan for power.

## Redundant power supplies

Some IBM Systems are designed with a fully redundant power system. A redundant power supply is a feature that prevents an unplanned outage by providing power if one power supply fails.

Some systems support a dual line cord feature. This allows you to provide power to the system from two different external power sources. This can avoid an unplanned outage if one power source fails.

## Uninterruptible power supplies

Even when you have an adequate power supply, there are still times when you may lose power, such as during a storm. To prevent unplanned outages that result from losing power, you may need to invest in

hardware specifically designed to keep your server going when power is lost. One such piece of hardware is an *uninterruptible power supply (UPS)*. You can use a UPS to provide auxiliary power to your processor, disks, system console, and any other devices that you think are necessary. Uninterruptible power supplies provide the following advantages:

- Let you continue operations during brief power outages (brown outs).
- Protect the system from voltage peaks (white outs).
- Provide a normal end of operations in case of an extended power outage, which can reduce your recovery time when you restart your server. For information on how to write a program that will help you control your server's shutdown in these conditions, see *Control system shutdown using a power handling program*.

For information on which uninterruptible power supplies are compatible with your server, see *Uninterruptible power supply systems*

## Generator power

If you think you could experience an extended power failure, you might want to consider purchasing a generator. A generator goes a step further than a UPS in that it enables you to continue normal operations during longer power failures.

## Use effective systems management practices

One of the simplest ways to prevent unplanned outages is to ensure that you are doing everything you can to keep your system running smoothly. This includes performing basic preventive maintenance and systems management tasks that help your system perform at its peak.

Many of these systems management tasks can be automated, which helps you prevent failures that may occur because of human error or an oversight.

One way you can help ensure the availability of your system is to monitor its performance and react promptly to any problems that you encounter. You can use the *Collection Services* and *monitors* functions in *Management Central* to actively monitor and track the performance of your server. You can be notified of any problems that jeopardize the availability of your system in time to react and prevent an unplanned outage. For more information on how to plan for and manage the performance of your server, see *Performance*.

Fixes are also an important systems management component that can help you keep your system available. When problems are discovered in *iSeries* programs, IBM issues a **fix** (also known as a *PTF*, or *program temporary fix*) to correct the problem. You need to be aware of fixes and install them on your system to ensure that your system is operating at its optimal level. You should create a fix management strategy and make checking for and applying fixes part of the routine maintenance for your server. For more information on how to obtain and apply fixes, refer to *Use software fixes*. For help in determining a strategy for preventive maintenance based on your *iSeries* environment and applications, try the *Fix*

*Maintenance Advisor* .

- | In addition, you should also develop a strategy of when and how new applications will be added to your
- | systems. Before adding a new application or updating an existing application, ensure that any software,
- | hardware, or other dependencies are understood and in place. It is also important to plan and test these
- | new or changed applications before introducing them into a production environment to help avoid
- | potential outages or other unexpected impacts.

## Prepare the space for your server

One way to prevent unplanned outages is to ensure that the space where you put your system promotes availability. Many physical and environmental factors contribute to how your system performs.

The first thing you need to do is familiarize yourself with your server. Different system models have different requirements with regard to the conditions they are in, so you should be aware of what your system needs. For more information on the physical characteristics of each model, see *Server specifications*. For information on the physical characteristics of the hardware that you can attach to your server, see *Hardware specification sheets*.

Once you are familiar with the physical characteristics of your server, be sure to consider the following about the space where it resides:

- **Location.** The physical location of your server can have an impact on how available it is. For example, if the room is not secure, your system could be vulnerable to vandalism or even someone accidentally dislodging the power cord. For more details on what precautions you should take with regard to your server's location, see *Physical site planning: Site selection, building and space considerations*.
- **Cables.** Cables are often overlooked, but without them your system would be unusable. You need to ensure that your cables are in good condition and are being used correctly. For more information on how to ensure that your cables do the job you need them to do, see *General cabling considerations*.
- **Environment.** The environment you provide for your server is also crucial to availability. The environment includes such things as temperature, humidity, and other factors that can inhibit the performance of your server. For more detailed information on the environment you need to provide for your server, see *Physical site planning: Site environment, safety, and security*.

---

## Shorten unplanned outages

Unplanned outages do occur, and a key to availability is to ensure that when they do occur you can recover from them as quickly as possible.

The purpose of all recovery strategies is to get back to where you were before the outage occurred.

If you have a single system and you cannot achieve the level of availability you need using these strategies, you may want to consider clusters.

## Reduce the time to restart your system

Unfortunately, systems periodically experience an unplanned outage. Use the availability tools described here to restart your system as quickly as possible after an unplanned outage.

- | Before your system powers down, it performs certain activities to ensure that your data is protected and that jobs are ended in a controlled manner. When you experience an unplanned outage, your system cannot perform these activities. Each of these tools should be used together to quicken the start up times for your system.

For more details on what happens when your system ends abnormally, see *Start and stop the system*.

Use the *Reducing iSeries IPL Time* experience report to learn how to control the time that it takes to start your iSeries server.

## System-managed access-path protection (SMAPP)

An *access path* is the route an application takes through a database file to get to the records it needs. A file can have multiple access paths, if different programs need to see the records in different sequences. When your server ends abnormally, such as during an unplanned outage, the system must rebuild the access paths the next time it starts, which can take a long time. When you use system-managed access-path protection, the system protects the access paths so they do not have to be rebuilt when your system starts after an unplanned outage. This will save you time when you restart your server, which will enable you to get back to your normal business processes as quickly as possible. For detailed information on SMAPP, see *System-managed access-path protection*.

## Journaling access paths

Like SMAPP, journaling access paths can help you to ensure that critical files and access paths are available as soon as possible after you restart your server. However, when you use SMAPP, the system decides which access paths to protect. Therefore, if the server does not protect an access path that you consider critical, you may be delayed in getting your business running again. When you journal access paths, you decide which paths to journal.

For more details on journaling access paths, see [SMAPP and access path journaling](#).

- | SMAPP and journaling access paths can be used separately. However; if you use these tools together, you
- | can maximize their effectiveness for reducing startup time by ensuring that all access paths that are
- | critical to your business operations are protected.
  
- | Protecting your access paths is also important if you plan to use any disk-based copy services, such as
- | cross-site mirroring or IBM TotalStorage Enterprise Storage Solution (ESS) peer-to-peer copy features, to
- | avoid rebuilding access paths when you failover to a backup server.

## Independent disk pools

When a system is started or restarted, you can start each independent disk pools individually. By starting each independent disk pool separately, the system can be made available more quickly. You can prioritize the workload so that critical data becomes available first. You can then vary on independent disk pools in a specific order based on this priority. See [Example: Make independent disk pool available at startup](#) for more information.

## Recover recent changes after an unplanned outage

After an unplanned outage, your goal is to get your system up and running again as quickly as possible. You want to get back to where you were before the outage occurred without having to manually re-enter transactions.

This may involve rebuilding some of your data. There are a few availability tools that you can use that will help you more quickly get back to where you were before the outage occurred.

## Journaling

Journal management prevents transactions from being lost if your system ends abnormally. When you journal an object, the system keeps a record of the changes you make to that object. For detailed information on how to plan for and use journaling, see [Journal management](#).

## Commitment control

Commitment control helps to provide data integrity on your server. It allows you to define and process a group of changes to resources, such as database files or tables, as a single transaction. Then, it ensures that either the entire group of individual changes occur or that none of the changes occur. For example, you lose power just as a series of updates are being made to your database. Without commitment control, you run the risk of having incomplete or corrupt data. With commitment control, the incomplete updates would be backed out of your database when you restart your server.

You can use commitment control to design an application so the system can restart the application if a job, an activation group within a job, or the system ends abnormally. With commitment control, you can have assurance that when the application starts again, no partial updates are in the database due to incomplete transactions from a prior failure.

For detailed information on how to plan for and use commitment control, see [Commitment control](#).

## Recover lost data after an unplanned outage

You may lose data as a result of an unplanned outage, such as a disk failure. The most extreme example of data loss is losing your entire site, such as what might happen as a result of a natural disaster.

There are a few ways that you can prevent your data from being lost in these situations or at least limit the amount of data that is lost.

### Backup and recovery

It is imperative that you have a proven strategy for backing up your server; the time and money you spend creating this strategy is more than recovered should you need to restore lost data or perform a recovery. Once you have created a strategy, you must ensure that it works by testing it, which involves performing a backup and recovery and then validating that your data was backed up and restored correctly. If you change anything on your server, you need to assess whether your backup and recovery strategy needs to change.

Every system and business environment is different, but, ideally, you should try to do a full backup of your system at least once a week. If you have a very dynamic environment, you will also have to back up changes to objects on your system since the last backup. Then, if you have an unexpected outage and need to recover those objects, you can recover the latest version of them.

For guidance on how to create a backup and recovery strategy, see [Plan a backup and recovery strategy](#). For instructions on how to perform backups on your server, see [Back up your server](#). For information on how to restore your server, see [Recover your server](#).

If you would like a solution to help you manage your backup and recovery strategy and your backup media, you can use Backup, Recovery and Media Services (BRMS). BRMS is a program that helps you implement a disciplined approach to managing your backups, and provides you with an orderly way to retrieve lost or damaged data. Using BRMS, you can manage your most critical and complex backups, including online backups of Lotus® servers, simply and easily. You can also recover your system fully in the event of a disaster or failure.

In addition to these backup and recovery features, BRMS enables you to track all of your backup media from creation to expiration. You no longer have to keep track of which backup items are on which volumes, and worry that you will accidentally write over active data. You can also track the movement of your media to and from offsite locations.

For detailed information on the tasks that BRMS can help you perform, see [Backup, Recovery and Media Services](#).

For help in planning and managing your backup and recovery strategy, contact IBM Business Continuity and Recovery Services .

### Limit the amount of data that is lost

You can group your disk drives into logical subsets called *disk pools* (also known as auxiliary storage pools or ASPs). The data in one disk pool is isolated from the data in the other disk pools. If a disk unit fails, you only have to recover the data that was stored in the disk pool that the failed disk unit was a part of.

For detailed information on disk pools, disk pool types, and examples of how to use disk pools for different purposes, see [Disk pools](#). For information on how to configure disk units and disk pools, see [Disk management](#).

**Independent disk pools** are disk pools that can be brought online or taken offline without any dependencies on the rest of the storage on a system. This is possible because all of the necessary system information associated with the independent disk pool is contained within the independent disk pool. Independent disk pools offer a number of availability and performance advantages in both single and multiple system environments. For detailed information, see Independent disk pools.

| **Logical partitions** provide the ability to divide one system into several independent systems. The use of logical partitions is another way that you can isolate data, applications, and other resources. You can use logical partitions to improve the performance of your server, such as by running batch and interactive processes on different partitions. You can also protect your data by installing a critical application on a partition apart from other applications. Then, if another partition fails, that program is protected.

For detailed information on logical partitions and how to use them, see Logical partitions.

### | **Reduce the time to vary on independent disk pool**

| When unplanned outages occur, data stored within independent disk pools is unavailable until they can be restarted. To ensure that the restart occurs quickly and efficiently, you should use recommended strategies for varying on your independent disk pools.

| These strategies provide a means of reducing the vary on time for independent disk pools.

### | **Synchronize user profile name, UID, and GID**

| In a clustered environment, a user profile is considered to be the same across servers if the profile names are the same. The name is the unique identifier in the cluster. However, a user profile also contains a user identification number (UID) and group identification number (GID). To reduce the amount of internal processing that occurs during a switchover, where the independent disk pool is made unavailable on one server and then made available on a different server, the UID and GID values should be synchronized across the recovery domain for the device CRG.

### | **Use recommended structure for independent disk pools**

| The recommended structure for using independent disk pools is to place the majority of your application data objects into independent disk pools and a minimal number of nonprogram objects in SYSBAS, which is the system disk pool and all configured basic disk pools. The system disk pool and basic user disk pools (SYSBAS) would contain primarily operating system objects, licensed program libraries, and few user libraries. This structure yields the best possible protection and performance. Application data is isolated from unrelated faults and can also be processed independently of other system activity. Vary on and switchover times are optimized with this structure.

| This recommended structure does not exclude other configurations. For example, you might start by migrating only a small portion of your data to a disk pool group and keeping the bulk of your data in SYSBAS. This is certainly supported. However, you should expect longer vary-on and switchover times with this configuration since additional processing is required to merge database cross-reference information into the disk pool group.

---

## **Shorten planned outages**

Planned outages are necessary and are expected; however, because they are planned does not mean they are nondisruptive. Planned outages are often related to system maintenance.

| Clusters can effectively eliminate planned outages by providing application and data availability on a second system or partition during the planned outage.

## Shorten backup windows

By reducing the amount of time it takes to complete your backups, you can also reduce the amount of time your system is unavailable.

A key consideration of any backup strategy is determining your backup window, which is the amount of time that your system can be unavailable to users while you perform your backup operations. The challenge is to back everything up in the window of time that you have. To lessen the impact the backup window has on availability, you can reduce the amount of time a backup takes using one or more of the following techniques.

### Improved tape technologies

Faster and denser tape technologies can reduce the total backup time. See Storage Solutions for more information.

### Parallel saves

Using multiple tape devices concurrently can reduce backup time by effectively multiplying the performance of a single device. See Save to multiple devices to reduce your save window for more details on reducing your backup window.

### Saving to non-removable media

Saving to media that is faster than removable media, for example directly to a disk unit, can reduce the backup window. Data can be migrated to removable media at a later time. See Save to virtual tape media for more information.

### Perform online backups

You can reduce your backup window by saving objects while they are still in use on the system or by conducting online backups.

### Save-while-active

The save-while-active function is an option available through Backup, Recovery and Media Services (BRMS) and on several save commands. Save-while-active can significantly reduce your backup window or eliminate it altogether. It allows you to save data on your system while applications are still in use without the need to place your system in restricted state. Save-while-active creates a checkpoint of the data at the time of the save operation is issued. It saves that version of the data while allowing other operations to continue. For detailed information on save-while-active, see Save your server while it is active.

### Online backups

Another method of backing up objects while they are in use is known as an *online backup*. Online backups are similar to save-while-active backups, except that there are no checkpoints. This means that users can use the objects the whole time they are being backed up. Backup, Recovery, and Media Services (BRMS) supports the online backup of Lotus servers, such as Domino<sup>®</sup> and QuickPlace<sup>®</sup>. You can direct these online backups to a tape device, media library, save files, or a Tivoli<sup>®</sup> Storage Manager (TSM) server. For detailed information on Lotus online backups, see Backup, Recovery and Media Services.

**Note:** It is important that you continue to back up system information in addition to any save-while-active or online backups you do. There is important system information that cannot be backed up using save-while-active or online backups.

## | **Backup from a second copy**

| Several techniques can be implemented to reduce the backup window by conducting backups from a second copy of the data.

| **Note:** If you are saving from a second copy, you should ensure that the contents of the copy are consistent. You may need to quiesce the application.

| These techniques include:

## | **Saving from a second system**

| Some technologies, such as replication, make available a second copy of the data that can be used to shift the save window from the primary copy to the secondary copy. This technique can eliminate the backup window on the primary system. Therefore, it does not affect production since the backup processing is done on a second system.

## | **IBM TotalStorage Enterprise Storage Server (ESS) FlashCopy<sup>®</sup> used with the iSeries Copy Services for ESS toolkit**

| IBM TotalStorage Enterprise Storage Server (ESS) provides enhanced storage capabilities. This technology uses the ESS function of FlashCopy on an independent disk pool. A single ESS server creates a point-in-time version of the independent disk pool where the host is not aware of the copy. The toolkit enables bringing the copy on to the backup system to perform saves or other processing. For information on IBM TotalStorage (ESS) and its features, see IBM TotalStorage website.

## | **Back up less data**

| You can reduce planned outages by backing up smaller amounts of data at different times. There are several ways that you can isolate the data on your system for this type of operation.

| **Note:** You can use Backup, Recovery and Media Services to perform all of these kinds of backups.

## | **Incremental backups**

| Incremental backups enable you to save changes to objects since the last time they were backed up. There are two types of incremental backups: cumulative and changes-only. A *Cumulative backup* specifies a backup that includes all changed objects and new objects since the last full backup." save the changes to an object since the last full backup of that object. This is useful for objects that do not change very often, or do not change greatly between full backups. A *changes-only backup* includes all changed objects and new objects since the last incremental or full backup.

| Incremental backups are especially useful for data that changes frequently. For example, you do a full backup every Saturday night. You have some libraries that are used extensively and so you need to back them up more frequently than once a week. You can use incremental backups on the other nights of the week instead of doing a full backup to capture them. This will shorten your backup window while also ensuring that you have a backup of the latest version of those libraries.

## | **Security data and configuration data**

| You can also reduce planned outages by isolating certain kinds of data and then backing it up separately. Security data includes user profiles, authorization lists, and authority holders. Configuration data includes information about how your server is set up, such as line descriptions, device descriptions, and configuration lists. These types of data are saved as part of a full system backup, but you can also save them separately without having to shut your system down. For details on how to back up these types of data, see Manually save parts of your server.

## | **Omit certain items**

| You can also reduce your backup window by reducing the number of objects you save or preventing objects from being saved more than once. You can do this by choosing to omit certain objects from a backup. For example, you may want to save all user libraries except for temporary libraries. You can choose to omit all temporary libraries from your backup, which will shorten the length of backup processing. Many of the commands that you use to save your system give you the option to omit items from the backup. For details on these commands, see [Commands to save parts of your server](#) and [Commands to save specific object types](#). You can also use Backup, Recovery and Media Services to omit items from a backup.

## | **Data archiving**

| Data that is not needed for normal production can be archived and taken offline. It is brought online only when needed, perhaps for month-end or quarter-end processing. The daily backup window is reduced since the archived data is not included.

## **Shorten software maintenance and upgrade windows**

You can keep your system available by effectively planning and managing fixes and installing new releases.

### **Manage fixes**

To reduce the amount of time your system is unavailable, you should ensure that you have a fix management strategy in place. If you stay current on what fixes are available and install them on a routine basis, you will have fewer problems. Be sure that you apply fixes as frequently as you have decided is appropriate for your business needs. For recommendations on how to create a fix management strategy, see [Plan your fix management strategy](#).

Individual fixes can be **delayed** or **immediate**. Delayed fixes can be loaded and applied in two separate steps. They can be loaded while your system runs and then applied the next time you restart your server. Immediate fixes do not require you to restart your system in order for them to take effect, which eliminates the need for downtime. Immediate fixes may have additional activation steps that are described in full in the cover letter that accompanies the fix. For more information on how to apply fixes, see [Install fixes](#).

### **Upgrade to a new release**

You are required to power down your system when you upgrade to a new version of i5/OS. To minimize the amount of time a software upgrade takes, it is important that you plan your installation carefully. For information on the planning process, see [Upgrading or replacing i5/OS and related software](#).

## **Shorten hardware maintenance and upgrade windows**

By effectively planning hardware maintenance and upgrades, you can greatly reduce and even eliminate the impact of these activities to availability of your server.

There are times when you need to perform routine maintenance on your hardware or increase the capacity of your hardware. These operations can be disruptive to your business.

If you are performing a system upgrade, be sure that you do careful planning before you begin. The more carefully you plan for your new server, the faster the upgrade will go. For more details on the planning process, see [Upgrades](#).

## | **Concurrent maintenance**

| Many hardware components on the iSeries system can be replaced, added, or removed concurrently while the system is operating. For example, the ability to "hot plug" is supported for PCI card slots, disk slots, and redundant fans and power supplies. Concurrent maintenance improves the availability of the system and allows you to perform certain upgrades, maintenance, or repairs without impacting the users of the system.

| For details on concurrent maintenance, see [Concurrent maintenance](#).

## **Capacity on Demand**

With IBM eServer™ Capacity on Demand, you can activate additional processors and pay only for the new processing power as your needs grow. You can increase your processing capacity without disrupting any of your current operations.

Capacity on Demand is a feature that offers the capability to nondisruptively activate one or more central processors of your server. Capacity on Demand adds capacity in increments of one processor, up to the maximum number of stand-by processors built into your model. Capacity on Demand has significant value for installations where you want to upgrade without disruption.

For more information on this feature, see [Capacity on Demand](#).

---

## **Availability for multiple systems: Clusters**

For multiple system environments, you can use clusters as a strategy to maintain a high or continuous availability for your systems and applications.

A *cluster* is a collection or group of multiple systems that work together as a single server. If your business needs high or continuous availability, clustering is the solution that you should consider.

Systems in a cluster work cooperatively to provide a single computing solution. You can have up to 128 systems in a cluster. This allows you to efficiently group your systems together to set up an environment that provides availability that approaches 100 percent for your critical applications and data. This helps ensure that your essential systems and applications are always available. Clusters also provide simplified systems management and increased scalability to seamlessly add new components as your business grows.

You have to weigh the cost of this solution against the cost of downtime on your system to decide whether to implement clusters in your business.

If you do choose to use clusters in your environment, you will have the added benefit of improving application availability. The level of application availability will depend on how well the application integrates with cluster resource services. For more information on these applications, see [Highly available programs](#).

To learn more about clusters, including how it works and how to implement clusters in your business, see [Clusters](#). For more information on clusters in the context of other high availability solutions, see [High availability and clusters](#) .

## **Highly available programs**

Highly available applications provide users continued access to data and application functions despite planned or unplanned outages. i5/OS has provided an application resilience architecture that supports various degrees of highly available application. Applications at the high end of the availability spectrum

are enhanced with integrated functions and provide automation of the environment. These functions are controlled by cluster management utilities. For more information on these topics, see Cluster applications.

## | **iSeries cluster middleware**

| iSeries cluster middleware is a group of competitive third party products which provide cluster management and data replication functions and services. These products make full use of the Cluster Resource Services functions of i5/OS and adhere to the iSeries cluster architecture. For a list of cluster middleware and a description of the criteria these programs must meet, see High Availability and Clusters. 

---

## **Data resilience solutions for i5/OS Clusters**

This topic provides an overview of different data resilience technologies that can be used to with i5/OS Clusters to enhance high availability in multiple system environments.

*Data resilience* is the ability for the data to remain accessible to the application even if the system that originally hosted the data fails. Choosing the correct set of data resilience technologies in the context of your overall business continuity strategy can be complex and difficult. It's important to understand the different data resilience solutions that can be used alone or with clusters to enhance availability in multiple system environments. You can either choose a single solution or use a combination of these technologies to meet your needs.

For more details on these solutions, see Data Resilience Solutions for IBM i5/OS High Availability Clusters. The section called "Comparison characteristics" contains a detailed comparison of the attributes for each of these technologies.

## **Replication**

With replication, changes to an object are copied to a saved version with near real-time accuracy. Replication is one of the most widely used high availability solutions in multiple system environments. On the iSeries, this solution is most often implemented through a business partner.

Consider replication when you have the following requirements:

- You need two or more copies of the data.
- You want concurrent access to the second copy of data.
- You need backup window reduction.
- You need to selectively replicate objects within a library or directory.
- Your IT staff can monitor the state of the replication environment.
- You need geographic dispersion between copies, especially if they need distances greater than what can be achieved by hardware solutions.
- You already have deployed a solution using logical object replication.
- You need a solution that has no special hardware configuration requirements.
- Failover and switchover times should not exceed tens of minutes.
- Transaction level integrity is important for all journaled objects.

## **Switchable disk pools**

Switchable disk pools are storage devices on the operating system that are independent of a particular system. This allows you to "switch" disk pools from one system to another without performing a full IPL. The key benefits to switchable disk pools involve its simple design and maintenance. One copy of the data is always current with no other version to synchronize so there is minimal administration.

Consider switchable disk pools when you have the following requirements:

- Only one copy of the data with hardware protection satisfies your requirement and you have considered or addressed avoiding unplanned outages due to disk subsystem failures.
- You need a simple, low cost and low maintenance solution.
- Disaster recovery (DR) is not needed.
- You only need coverage for planned outages and certain types of unplanned outages.
- The source and target system are at the same site.
- You want consistent failover and switchover times within minutes and that do not depend on transaction volumes.
- Transaction-level integrity is important for all objects.
- You need immediate availability of all object changes with no loss of in flight data.
- Objects not within an independent disk pool either do not need to be replicated or are handled via some other mechanism.
- You need the highest throughput environment.
- Your environment calls for multiple, independent databases that can be moved between systems.

## **Cross-site mirroring**

*Cross-site mirroring*, combined with the geographic mirroring function, enables you to mirror data on disks at sites that can be separated by a significant geographic distance. Geographic mirroring provides the ability to replicate changes made to the production copy of an independent disk pool to a mirror copy of that independent disk pool. As data is written to the production copy of an independent disk pool, the operating system mirrors that data to a second copy of the independent disk pool through another system. This process keeps multiple identical copies of the data.

Consider cross-site mirroring when you have the following requirements:

- You want a system-generated second copy of the data (at an IASP level).
- You need two copies of data, but do not need concurrent access to a second copy.
- A relatively low cost and low maintenance solution is desired, but you also need disaster recovery.
- Geographic dispersion between copies is needed, but your distance requirement does not adversely impact your acceptable production performance goals.
- You want consistent failover and switchover times within minutes and that do not depend on transaction volumes.
- Transaction-level integrity is important for all objects.
- You need immediate availability of all object changes with no loss of in flight data.
- Objects not within an independent disk pool either do not need to be replicated or are handled via some other mechanism.
- The second copy that is not available during resynchronization fits within your service level objectives.

## **IBM TotalStorage Enterprise Storage Server PPRC used with the iSeries Copy Services for ESS toolkit**

This solution involves the replication of data at the storage controller level to a second storage system using IBM TotalStorage Enterprise Storage Server (ESS) copy services. An independent disk pool is the basic unit of storage for the ESS peer-to-peer remote copy (PPRC) function. PPRC generates a second copy of the independent disk pool on another ESS. The toolkit comes as part of the iSeries Copy Services for ESS services offering. It provides a set of functions to combine the PPRC, IASP, and i5/OS cluster services for coordinated switchover and failover processing through a cluster resource group.

This solution provides the benefit of the remote copy function and coordinated switching operations, which gives you good data resiliency capability if the replication is done synchronously. The toolkit

enables you to attach the second copy to a backup system without an IPL. No load source recovery is involved in the operations. You also have the ability to combine this solution with other ESS-based copy services functions, such as FlashCopy, for additional benefits such as save window reduction.

Consider IBM TotalStorage Enterprise Storage Server (ESS) peer-to-peer remote copy (PPRC) with IASP and Toolkit when you have the following requirements:

- You desire a storage-based solution for DR, especially if multiple platforms are involved.
- You do not need complete high availability (HA), but seek to cover Disaster recovery and some planned outages for critical application data.
- You want consistent failover and switchover times within minutes and that do not depend on transaction volumes.
- You want two copies of data, but do not need concurrent access to a second copy.
- Geographic dispersion between copies is needed, but your distance requirement does not adversely impact your acceptable production performance goals. Alternatively, consider Peer-to-Peer Remote Copy (PPRC) Global Mirror, which is also known as asynchronous PPRC.
- Transaction-level integrity is important for all objects.
- You need availability of all object changes with no loss of in-flight data.

---

## Related information for Availability roadmap

Several sources relate to Availability roadmap. Use these iSeries manuals, IBM Redbooks™ (in PDF format), and Web sites to learn more about high availability, backup and recovery, clusters, and other related topics. You can view or print any of the PDFs.

### Manuals

- Backup and Recovery 
- Backup, Recovery and Media Services for iSeries 

### IBM Redbooks

- Data Resilience Solutions for IBM i5/OS High Availability Clusters 
- Clustering and IASPs for Higher Availability 
- Striving for Optimal Journal Performance on DB2® Universal Database for iSeries 
- High Availability on the AS/400® System: A System Manager's Guide 
- AS/400 Remote Journal Function for High Availability and Data Replication 
- The System Administrator's Companion to AS/400 Availability and Recovery 
- IBM eServer iSeries Independent ASPs: A Guide to Moving Applications to IASPs 
- Introduction to Storage Area Network, SAN 
- iSeries and Storage Area Networks 
- Domino 6 for iSeries Best Practices Guide 
- IBM WebSphere V5.1 Performance, Scalability, and High Availability 

- Microsoft Windows Server 2003 Integration with iSeries 
- Integrating Backup Recovery and Media Services and IBM Tivoli Storage Manager 
- Planning for IBM eServer i5 Data Protection with Auxiliary Write Cache Solutions 
- Independent ASP Performance Study on the IBM eServer iSeries Server 
- Improve Whole System Backups with the New Save-While-Active Function 
- Choosing the right backup strategy for Domino 6 for iSeries 
- Multipath for IBM iSeries 
- The LTO Ultrium Primer for IBM iSeries Customers 
- Seven Tiers of Disaster Recovery 

### Web sites

- High Availability and Clusters 
- Backup, Recovery and Media Services 
- Capacity on Demand 
- IBM Business Continuity and Recovery Services 
- iSeries for Capacity Backup 
- Logical Partitioning 
- Storage Solutions 
- Implementing PeopleSoft EnterpriseOne ERP 8.0 Using an Independent Auxiliary Storage Pool 
- Performance Management 
- IBM TotalStorage 

### iSeries Information Center topics

- Backup and Recovery
- Clusters
- Commitment control
- Disk management
- Journal management
- Logical partitions
- Storage solutions

### Experience reports

- Backing up the integrated file system
- Reducing iSeries IPL Time

## Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Open the PDF in your browser (click the link above).
2. In the menu of your browser, click **File**.
3. Click **Save As...**
4. Navigate to the directory in which you would like to save the PDF.
5. Click **Save**.

## Downloading Adobe Reader

If you need Adobe Acrobat Reader to view or print these PDFs, you can download a copy from the Adobe Web site ([www.adobe.com/prodindex/acrobat/readstep.html](http://www.adobe.com/prodindex/acrobat/readstep.html))  .



---

## Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106-0032, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N  
Rochester, MN 55901  
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

- | The licensed program described in this information and all licensed material available for it are provided
- | by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement,
- | IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- | AS/400
- | DB2
- | Domino
- | Enterprise Storage Server
- | eServer
- | FlashCopy
- | i5/OS
- | IBM
- | iSeries
- | Lotus
- | QuickPlace
- | Redbooks
- | Tivoli
- | TotalStorage

| Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

| Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

---

## Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

**Personal Use:** You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

**Commercial Use:** You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER

EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.





Printed in USA