

IBM i5/OS keeps your business up and running



IBM i5/OS—Resilient and Secure by Design

Highlights

- *Introducing High Availability Solutions Manager (HASM) for IBM® i5/OS®*
- *i5/OS disk clustering for a complete end-to-end IBM high availability solution offering*
- *Introducing iCluster for i5/OS software replication for disaster recovery*
- *Introducing i5/OS Software Encryption to tape or for data at rest*

Available and secure to help you manage complexity and risk

From an IT perspective, business continuity is all about the availability and security of your core business applications and data. The need to keep mission critical applications in production continuously, the need to recover data, and the need to secure data from both internal and external entities has risen to the top of the IT requirements list. i5/OS V6R1 offers platform resiliency and data protection technologies ensuring that information and systems can be highly available.

i5/OS resiliency solutions

IBM i5/OS V6R1 offers state of the art availability and reliability capabilities. With the introduction of High Availability Solutions Manager (HASM) and IBM DataMirror® iCluster®, IBM now offers a full range of high availability (HA) products for virtually any customer scenario. IBM Cross-Site® Mirroring (XSM) is the i5/OS-based replication solution manager that enables two

systems to have synchronous copies of data which are implemented via IASPs (independent storage pools). This state of the art clustering solution enables operations for managing your high availability environment. HASM may be deployed with XSM using either native disk or SAN-based disk. You may choose to use XSM to manage the i5/OS native replication solution called Geographic Mirroring, or for those customers desiring a SAN-based high availability clustering solution, the HASM cluster integrates the IBM DS8000™ (and the IBM DS6000™) storage replication technology called Metro Mirror. For those clients looking for geographic dispersion for disaster recovery solution deployments, the IBM DS8000 Global Mirror solution may be used or you may choose iCluster, the IBM logical replication solution. iCluster is a software-based data replication solution ideally suited to geographic dispersion and data replication/recovery operations. iCluster may also be extended to support full blown HA operational deployments which are characterized by semi-permanent role swap operations.

Getting started

Business Resiliency is based upon the concept of risk management—managing availability and information security. A corporate policy is the proper starting point for a discussion on business resiliency. At the system level, the policy becomes a specific set of requirements which will ultimately define both your availability and your security solution environment.

Essential IT responsibilities

Asset Availability and integrity

- *Provide for the availability and recoverability of applications and data*
- *Ensure security of applications and data*
- *Provide for application change management*

Compliance

- *Establish an IT policy that supports the corporate policy*
- *Implement and document the policy*
- *Demonstrate conformity to the documented policy*

Availability management

Are your applications available when your customers, partners and employees need to conduct business? High availability is defined as the capability to minimize downtime caused either by planned or unplanned (non-disaster) outage events.

IBM i5/OS business resiliency offerings can provide cost-effective and flexible approaches to enable a redundant system (or systems) to help you deliver on your service level commitments and to help you meet customer expectations for 24x365 availability. Solutions are provided by IBM and also by ISV partners, offering you a wide range of options. The key operational characteristic that distinguishes a high availability shop is that they conduct regular and sustained role swap operations. The primary system becomes the backup and the backup system becomes the primary and remains in this configuration until the next role swap operation.

Disaster recovery refers to your ability to return operations to a user-defined level of capability following a catastrophic event. Generally speaking, a disaster recover solution is primarily focused on the ability to recover operations at a remote location. The primary objective for such a solution is often referred to as geographic dispersion. By creating a disaster recovery environment, you implement a solution that enables recoverability from the occurrence of an extraordinary circumstance such as earthquake, hurricane, flood or fire. The continuous replication of your data to a remote location enables critical data recovery and an eventual resumption of operations. These types of events happen only rarely—but when they do, they have the potential to destroy your business.

Availability management begins with a set of agreements inside an organization on application and data availability metrics. Availability management focuses on single system requirements and extends to clustering solutions which involve multiple

system topologies. In a single system environment, the focus is primarily about backup recovery and disk protection. An implementation will depend on the backup recovery solution and disk protection scheme that best addresses requirements. For clustered system environments, mission critical applications and data must be as close to continuously available as possible. For all clients the most basic requirement is to have a data recovery solution which insures nearly continuous data recoverability.

V6R1 availability capabilities include:

- *HASM clustering solutions that can simplify the management of highly-available environments*
- *Web-based cluster management*
- *Expanded Administration Domain for i5/OS synchronization of Sysbas objects*
- *iCluster software replication optimized for geographic dispersion and/or data replication/recovery*
- *DS8000 storage server solutions; Metro Mirror and Global Mirror are integrated as an extension of the i5/OS HASM/XSM for best of breed SAN clustering topologies.*
- *Significant fiber channel performance and capacity improvements that put DS8000 performance on par with i5/OS native disk storage deployments.*

Security management

The future of security for applications and data is policy driven. Traditional security is often ad-hoc, a collection of technologies that focus on items such as intrusion detection, fire walls, password management and so forth. Modern IT organizations will have natural language policy constructs that allow non-technical staff to create and understand security. Compliance reports will demonstrate compliance to the given policy in natural language. The ultimate goal is to have a solution where by the policy is implemented into the technical configuration without human intervention. This is the future and the future is here with Secure Perspective.

Policy creation and implementation

Given that a security implementation derives from a security policy, an audit will focus on your ability to demonstrate compliance to your policy. IBM Secure Perspective is designed to help you develop a system level, data-centric security policy. Secure Perspective forces you to focus on policy and leaves the implementation of the policy up to the tool. The tool produces a natural language report which demonstrates compliance to the given policy. Secure Perspective is focused on data-centric security—the most fundamental focus and appropriate driving force behind security. Data-centric security is the modern way to implement your core security policy.

Platform technologies

IBM i5/OS is architected and designed to meet stringent security requirements. IBM i5/OS is highly securable by design—from inception its architecture has been object-based. Object-based architecture necessitates precise rules for interaction between users and objects. These rules translate into world-class security properties. Objects have defined interfaces and access rules that are unique for each object type. With the i5/OS object-based architecture, one object type cannot masquerade as another, and only authorized entities may access a given object. This means that the i5/OS architecture can be

secured at the object level versus depending only on exit point security methods. By focusing on object level security, i5/OS can help you to enable a security policy that starts on the inside, at the most fundamental level of information management.

Artful and intelligent integration of hardware, security, systems management and middleware into a robust platform for business computing is the hallmark of i5/OS. V6R1 reinforces the proven ability of i5/OS to help safeguard data, help shield assets from hackers and help keep business applications and data available.

V6R1 security capabilities include:

- *New i5/OS software encryption solutions for backup tapes and data at rest*
- *Hardware storage protection to help prevent “rogue” programs from accessing system objects*
- *Intrusion detection features that administrators can use to readily automate monitoring for intrusion events, such as scanning for open TCP/IP ports as well as intrusion prevention capability*
- *New auditing features to strengthen access control*

Application change management

Application change management is about documented processes and procedures that define who may change an application and how it may be moved from a test environment into a production environment. Change management must ensure both quality control and security. There are industry standard change management policies as well as tools to help enforce the change management process. Digital Certificates are a means of helping ensure that only authorized owners of code have changed the code and that the current level of production code has not been changed by anyone other than the authorized owner.

Compliance

Compliance is the ability of your firm to demonstrate conformity to internal or government regulations and/or industry standards—including those regarding information integrity. These regulations and standards evolve constantly. Their relationship to corporate requirements, internal business controls, auditing procedures and audit evidence are complex. Using the relevant regulations and standards as guides, you can create your data-centric policy using Secure Perspective. Another approach is to utilize the solutions and expertise from i5/OS ISVs, whose offerings take advantage of the rich capabilities of i5/OS. IBM i5/OS can help you assure that your business and its technology infrastructure are meeting these critical compliance demands.



© Copyright IBM Corporation 2008

IBM Corporation
Integrated Marketing Communications
Systems & Technology Group
Route 100
Somers, NY 10589

Published in the United States of America
January 2008
All Rights Reserved

IBM, the IBM logo, Cross-Site, DS6000, DS8000 and i5/OS are trademarks or registered trademarks of International Business Machines Corporation.

DataMirror and iCluster are registered trademarks of DataMirror Corporation, an IBM Company.

Other trademarks and registered trademarks are the properties of their respective companies.

References in this publication to IBM products or services do not imply that IBM intends to make them available in every country in which IBM operates. Consult your local IBM business contact for information on the products, features, and services available in your area.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.

This equipment is subject to all applicable FCC rules and will comply with them upon delivery.

For more information

Contact your IBM representative or IBM Business Partner or visit:

ibm.com/systems/power/software/availability