Common Luxembourg

News tips and techniques with V5R3 and Power5

IBM

Fabian Michel

Senior IT Specialist
IBM Certified

IBM Belgium s.a.
Avenue du Bourget, 42
B-1130 Bruxelles
Tel. +32 2 225 38 22
Fax +32 2 225 23 68
E-mail: fabian_michel@be.ibm.com

September 28, 2005

Agenda

- Part 1: Security
  - Single sign-on
  - SSL: Secure Socket Layer
  - OpenSSH
  - Firewall and other security enhancements
  - Time synchronization

- Part 2 : Infrastructure management update
  - Virtualization
  - LPAR management facilities
  - TSM: Tivoli Storage Manager

Single Sign-on

September 28, 2005

Single Sign-on

Why ?

Benefit for end users and administrators

- No more “cached” passwords
- Less password resets

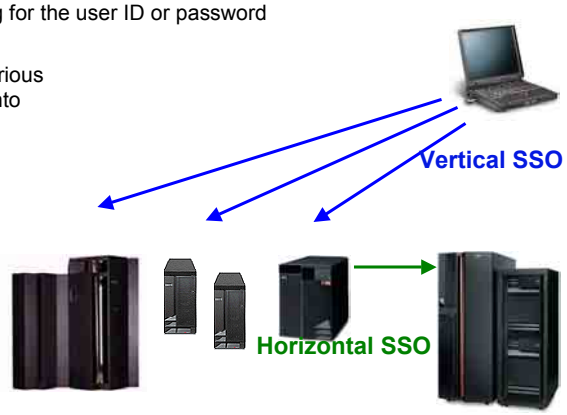
A dream or reality ?

Notes: Single Sign-on

- Simplifies the process for the user; access is controlled under the covers
- Simplifies administration
  - Rely on existing security semantics already in place for existing data
  - **Reduces load** on administrators for "lost" passwords **and** therefore **cost**
  - Reduces client side risks (cached passwords, post-it notes, etc..)
- Makes it easy for customers to associate a user's multiple identities in the enterprise and to manage those associations

Vertical or Horizontal?

- Sign on once to the network using a user ID and password
- Subsequent connection requests to application services and resources are authenticated without prompting for the user ID or password
- Taking different identities for various applications for a single entity into consideration is desirable



Building blocks

How ?

Several components to build a SSO enabled environment

- Authentication source (e.g. Kerberos or LDAP)
- EIM: Enterprise Identity Mapping
- LTPA keys
- Credential vault
- TAM: Tivoli Access Manager

Notes: Building blocks

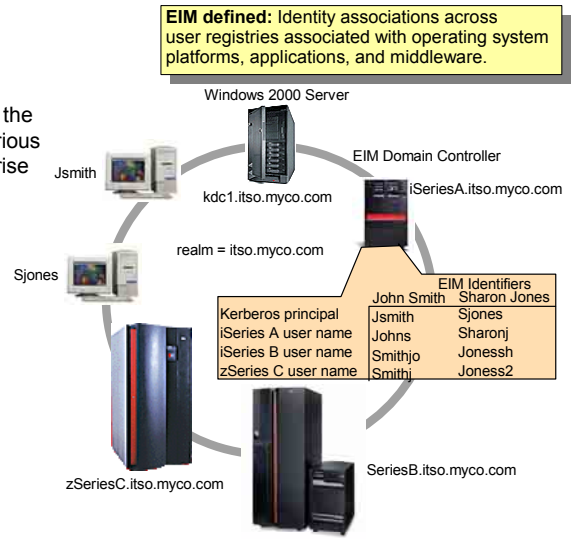
- The term single signon is often misinterpreted or confused with having a single user ID and password to sign on to a system. However, in most cases, users still have to sign on to each application or service individually. With a true SSO solution, a user signs on only once to the network (a central authentication service) and then accesses all participating services without re-entering a user ID or password. Many available SSO solutions, however, only offer a SSO in a Web environment. It is desirable to have a SSO solution that works for both browser-accessible applications and local applications, such as Telnet or DB access.
- With SSO, we distinguish between horizontal and vertical SSO approaches:

  Vertical SSO describes an approach where a client signs on from the client to each individual server using SSO.

  Horizontal SSO involves a client signing on, for example, to a server application, which in turn connects to another server to access a database, signing on on behalf of the user (also with SSO).

EIM

- EIM is a mechanism to map (associate) a person or entity to the appropriate user identities in various registries throughout the enterprise



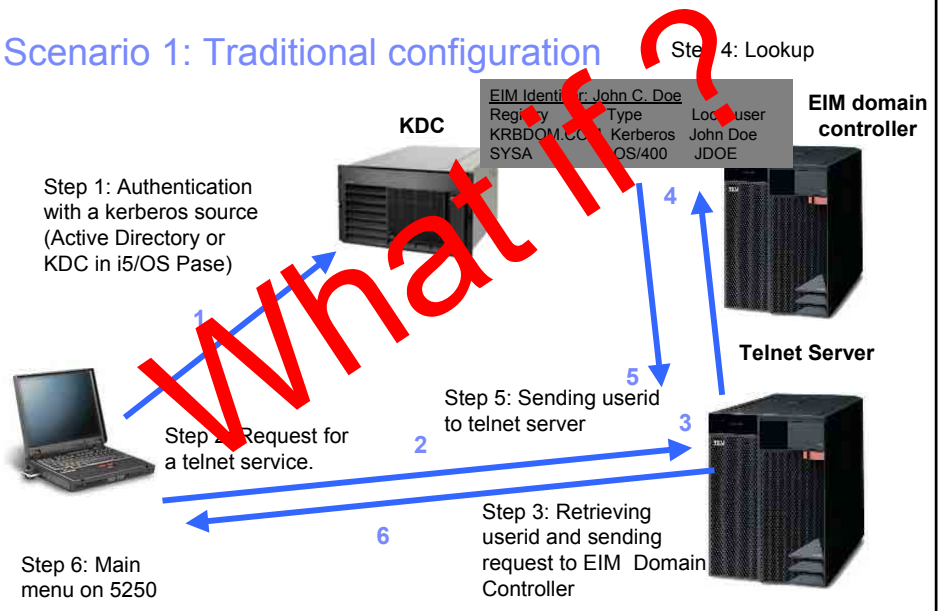
Kerberos and i5/OS enabled applications

- Host servers (used by iSeries Access for Windows)
  - Telnet
  - QFileSrv.400
  - Database Connectivity (DRDA, ODBC, JDBC)
- NetServer
- HTTP Server for iSeries (powered by Apache)
- LDAP
- Windows Integration
- Management Central
- FTP (via Exit program on QIBM_QTMF_SVR_LOGON)

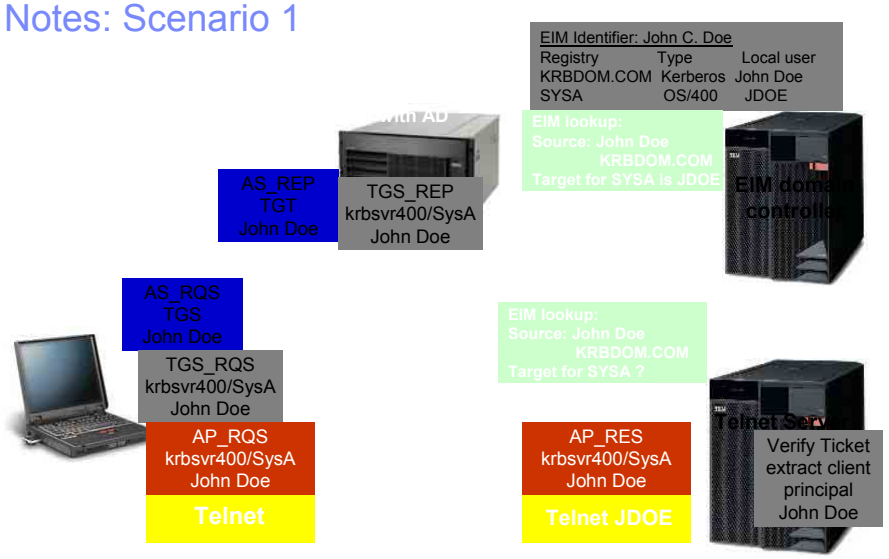
Notes: Kerberos and i5/OS enabled applications

- OS/400 client and server applications that are currently enabled for SSO are:
  - OS/400 Host Servers (5722-SS1 Option 12): Currently used by iSeries Access for Windows and iSeries Navigator.
  - Telnet server: Currently used by PC5250 and IBM WebSphere Host On-Demand Version 8: Web Express Logon feature.
  - Open Database Connectivity (ODBC): Allows SSO access to OS/400 databases through ODBC.
  - Java Database Connectivity (JDBC): Allows SSO access to OS/400 databases through ODBC.
  - Distributed Relational Database Architecture (DRDA): Allows SSO access to OS/400 databases through ODBC.
  - QFileSrv.400
  - LDAP Server: Supports Kerberos authentication only. EIM is not used during the authentication process.
- The following applications were enabled for EIM, Kerberos, or both in V5R3:
  - Management Central for authentication between endpoint systems and the central system.
  - Windows Integration for user enrollment and for submitting network server commands.
  - HTTP Server for iSeries (powered by Apache) when using Microsoft's Internet Explorer 5.0 or later. This support was also added to V5R2 via the HTTP group PTF.
  - The V5R3 enhancement of storing user certificates in LDAP servers also provides the ability for OS/400 applications, such as the FTP server, to use EIM for lookup operation of a target association. This function only pertains to OS/400 applications using digital certificates for client authentication. It is not related to Kerberos at all.

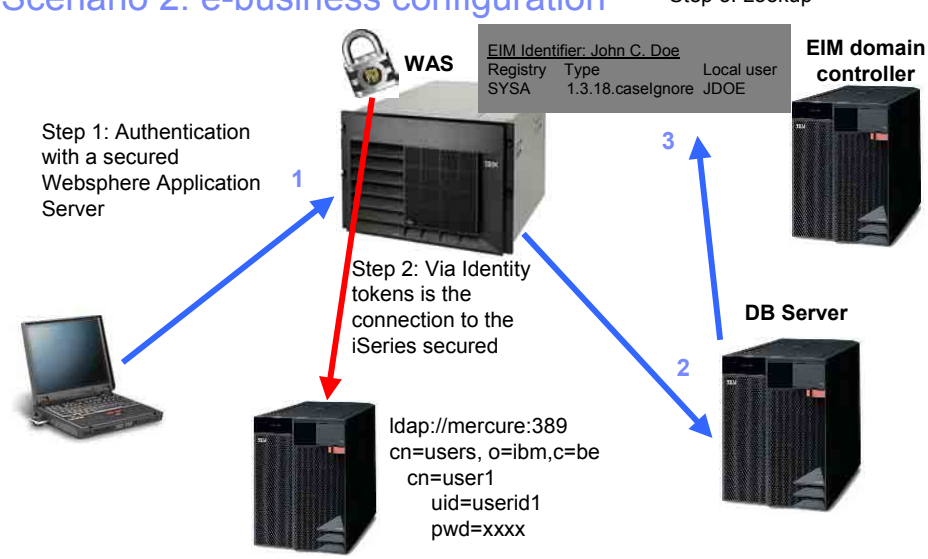
Scenario 1: Traditional configuration



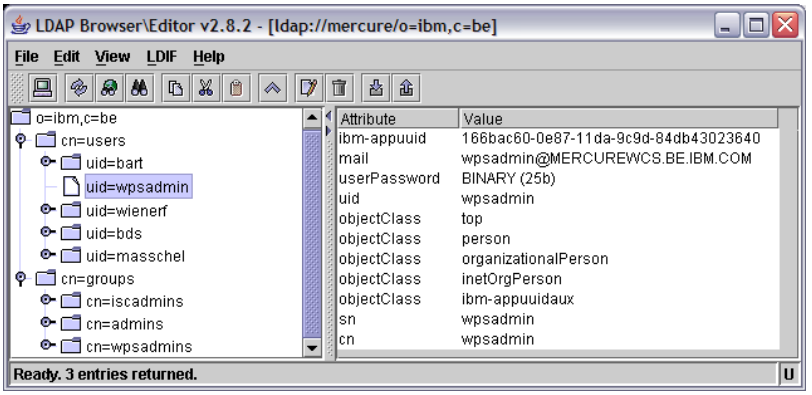
Notes: Scenario 1



Scenario 2: e-business configuration



Scenario 2: LDAP



ldap://mercure:389
DN: uid=wpsadmin,cn=users,o=ibm,c=be

Notes: LDAP

- The Lightweight Directory Access Protocol (LDAP) is an open industry standard that has evolved to meet these needs. LDAP defines a standard method for accessing and updating information in a directory. LDAP has gained wide acceptance as the directory access method of the Internet and is therefore also becoming strategic within corporate intranets. It is being supported by a growing number of software vendors and is being incorporated into a growing number of applications. For example, the two most popular Web browsers, Netscape Navigator/Communicator and Microsoft Internet Explorer, as well as application middleware, such as the IBM WebSphere Application Server or the IBM HTTP server, support LDAP functionality as a base feature.

Scenario 2: e-business configuration

- Identity tokens and LTPA keys
  LTPA is the decriptor of the token
- Identity token together with EIM
- Credential vault (shared or not)
- TAM: Tivoli Access Manger

Where is the standard ?

Notes: Scenario 2

- Identity tokens is one mechanism to authenticate EIM). LTPA keys are also possible (export import), but both the application server must be secured and must refer to the same LDAP server.
- TAM: Tivoli Access Manger. Tivoli has its own product (compared to EIM) to map users.

References:

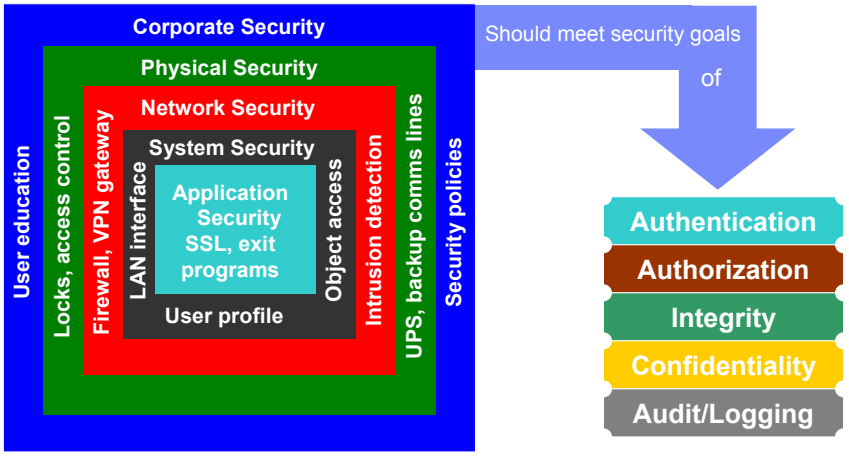
- *Implementation and Practical Use of LDAP on the IBM iSeries™* Server, SG24-6193
- *Using LDAP for Directory Integration*, SG24-6163

SSL: Secure Socket Layer

September 28, 2005

Layered implementation of security

To achieve the highest level of protection, security should be implemented in layers.



Notes: Layered implementation of security

Simply implementing a firewall is not enough to prevent unwanted access to confidential data on your systems. Implementing security in your e-business environment must begin with your corporate security plan. After you determine what the security plan entails, you must tailor it to secure your environment at all layers identified.

The implementation of security in various layers should always meet one or more of the following common security goals:

Authentication: Determine that the users are who they claim to be. The most common technique to authenticate is by user ID and password.

Authorization: Permit a user to access resources and perform actions on them. An example of authorization is the permissions on OS/400 objects.

Confidentiality: Only authorized users can view the data. For data that is transmitted through a network, there are two ways to achieve this goal:

- Make sure that only authorized persons can access the network
- Encrypt the data

Integrity: Only authorized users can modify the data, and they can only modify it in approved ways. The data is not changed either by accident or maliciously. For data that is transmitted over a network, there are two ways to achieve this goal:

- Make sure that only authorized persons can access the network (not easy to achieve in public networks such as the Internet)
- Digitally sign the data

SSL: Secure Socket Layer

- SSL is at no cost on i5/OS
- A lot of services can be secured:
  Telnet, HTTP, Hostservers, Object Signing

Notes: SSL

- Nowadays, security is one of the main topics in the industry. i5/OS is secure because of its outstanding security framework, but it can always be better.
- Sniffer tools are dangerous for password catching ,e.g. Telnet, HTTP and FTP. Netserver uses already encrypted passwords, the http server on i5/OS can be secured via Basic Security … but this is not secure enough (www.google.be and you find already a decriptor)
- SSL or Secure Socket Layer is the mechanism to encrypt ALL your traffic to and from the i5/OS box and is free of charge.

How ?

SSL and Certificates

- Server authentication:
  The certificate to do the encryption is downloaded first to the client and then the SSL connection is started.
- Client authentication
  First: Server authentication
  Second: Client passes his user certificate to the server and gets validated.
  Remark: When installing the user certificate a private key is generated.

Notes: How ?

Certificates are used by SSL to implement much of the encryption/decryption and validation work. These certificates used by SSL are stored in *key databases* (sometimes called *key stores*). There can be several different key databases on each platform (PC, iSeries, and so on). These databases are usually protected by a password. It is very important to have SSL certificates under key database password control on iSeries, because data inside each certificate makes it possible for SSL to establish trust and validation for each connection. It is also very important to track and understand when the certificates you are using will expire, so you can renew them ahead of time. Failures can occur if you use an expired certificate. To view and renew your configured certificates, use Digital Certificate Manager interfaces.

SSL gives some performance overhead, therefore Cryptographic Coprocessors are available.

Common Luxembourg

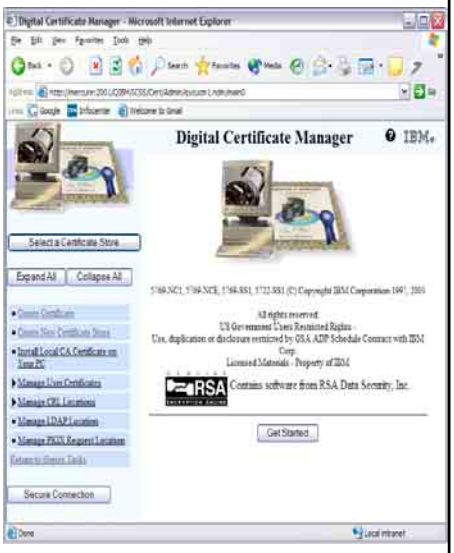
Notes: How ?

- If the iSeries is used to create client certificates, a browser capable of importing/exporting secure PKCS12 files is required. (Currently Microsoft Internet Explorer 5.x and Netscape 4.x or later have this capability.) After the client certificate is created, you need to export it from the browser and import it into the PC SSL key database using IBM Key Management.
- Next to iSeries certificates you can also use Versign certificates (http://www.verisign.com) or Geotrust (http://www.geotrust.com).

Prerequisites

- Cryptographic Access Provider
- Client Encryption
- DCM: Digital Cerificate Manager

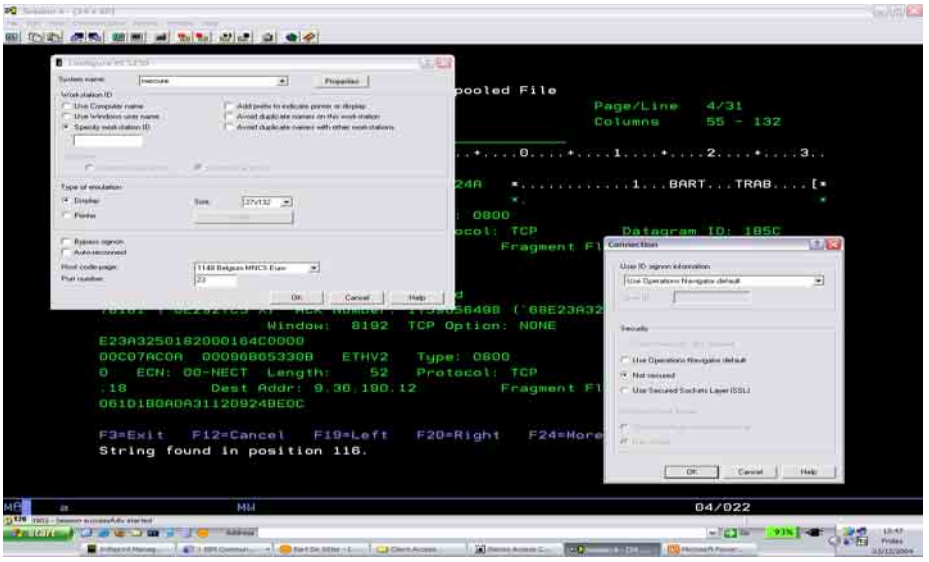
At no charge !

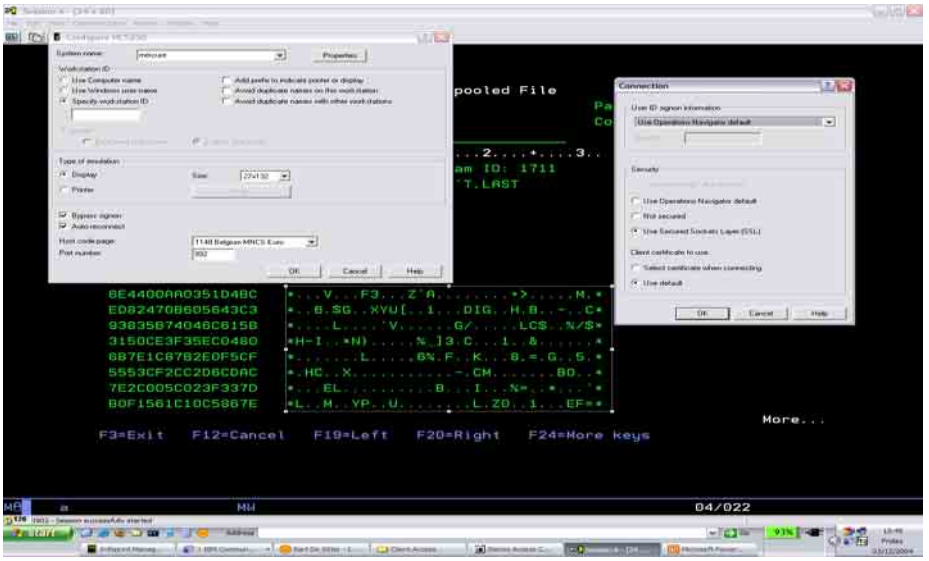


Notes:

- IBM Digital Certificate Manager (DCM), option 34 of OS/400 (5722-SS1).
- TCP/IP Connectivity Utilities for iSeries (5722-TC1).
- IBM HTTP Server for iSeries (5722-DG1). If you are trying to use the HTTP server to use the DCM, be sure you have the IBM Developer Kit for Java (5722-JV1) installed. By default on the iSeries, this product provides the iSeries HTTP Administration Server, which has a link to the Digital Certificate Manager from the administration server's initial page. If you need to start this administration server, enter the following Start TCP Server command from a 5250 session: STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
- The IBM Cryptographic Access Provider product, 5722-AC3 (128-bit). The bit size for this product indicates the maximum size of the secret material within the symmetric keys that can be used in cryptographic operations. The size allowed for a symmetric key is controlled by the export and import laws of each country. A higher bit size results in a more secure connection.
- Client Encryption product, 5722-CE3 (128-bit). iSeries Access for Windows needs this product in order to establish the secure connection.

Demo





Common Luxembourg

OpenSSH

September 28, 2005

Why SSH? (Secure Shell)

Again … normal communication is not secure.

Sniffer tools are dangerous !

What is SSH? (1/2)

- SSH is a program to log into another computer and run commands
- Entire datastream is encrypted
- OpenSSH is the free version of the SSH protocol suite
- Several utilities (ssh – sftp - ...)
- Two protocols are available: SSH1 and SSH2

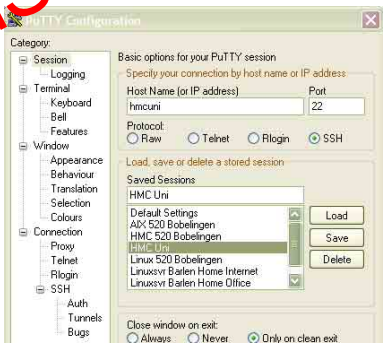
What is SSH? (2/2)

- *ssh* is the client utility used to connect to and run commands on a server running the SSH daemon (sshd)

```
ssh [user@]hostname [command]
```

- The ssh client is also needed to connect to the HMC (cmd)
- A popular ssh client is PuTTY
  - Available for Windows and Unix clients

And now on iSeries ?



Portable Utilities for i5/OS

- Portable Utilities for i5/OS is a license program product (free of charge)
  - LPP number 5733-SC1 (only in 2924)
- Requires i5/OS Portable Application Solution Environment (PASE)
  - 5722-SS1 Option 33

Firewall and other security enhancements

September 28, 2005

Support of Linux-based firewall

- StoneGate Security

FW, VPN & IPS appliances with throughput-based licensing

FW,VPN & IPS software on Intel-based hardware IP-based licensing IBM xSeries

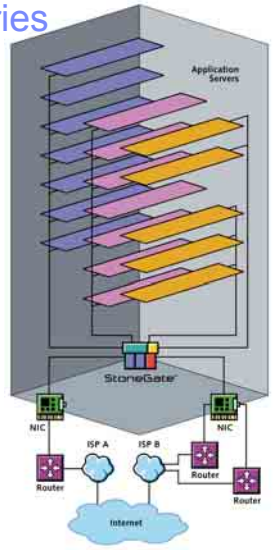
FW & VPN software on **IBM iSeries servers**

FW & VPN software on IBM zSeries Mainframe

STONESOFT
Real World Business Security

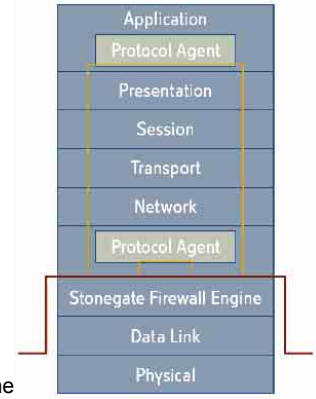
StoneGate Firewall & VPN for iSeries

- When:
  - New workloads, new technologies
  - New iSeries installations
  - Legacy firewall replacement
- What:
  - Linux powered, advanced security inside iSeries
  - Secure server consolidation
  - Secure network virtualization
- Benefits:
  - Best security and availability over the Internet
  - Next-to-application firewall and VPN security
  - Easier to manage and maintain
  - Infrastructure simplification

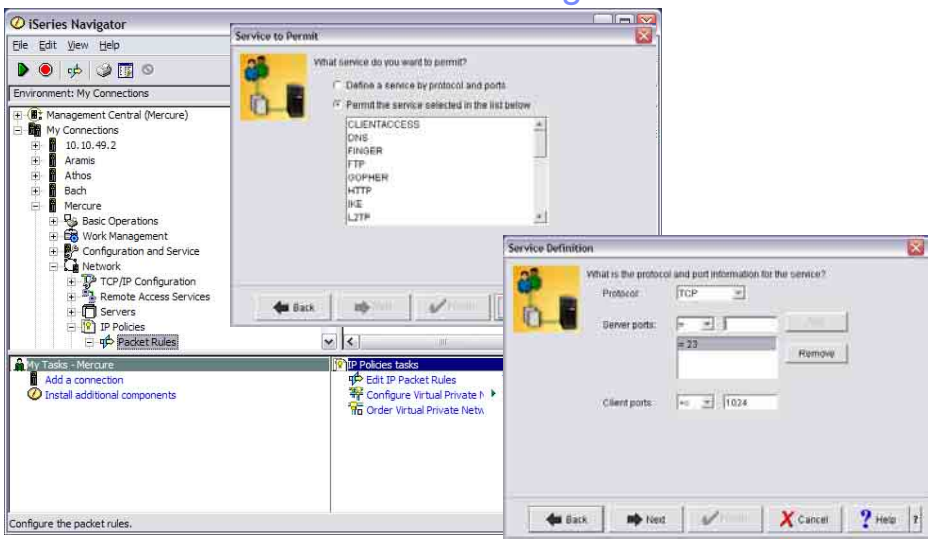


Linux-based firewall

- Provides
  - Multi-Layer Inspection
    - packet filtering
    - stateful inspection
    - application layer inspection
  - Standards compliant VPN
    - IPSec compliant
  - Multi-Link Technology
  - Manageability
- Application layer security with Protocol Agents
- Remote upgradeable
- Operating system hardened for firewall and VPN use
  - Includes only modules needed by StoneGate
  - e.g. sshd included in the standard installation – no telne
  - Read only filesystem (romfs)



Firewall on iSeries: Packet filtering

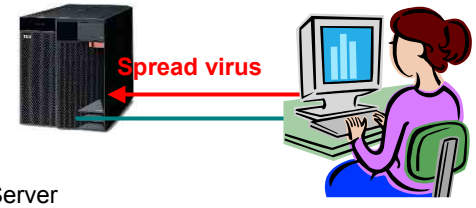


Integrity

Antivirus scanning

Viruses cause significant damage to businesses every year

- Infrastructure support added for enhanced virus scanning for the Integrated File System (IFS)
- Allows third-party vendors to develop antivirus scanning software that plugs into i5/OS (OS/400)
- Scanning support available to scan for any other purpos an object is opened or closed



NetServer
FTP, NFS

W32/BabyBearA

Phantom 1

W32/Cidu-A

Integrity

Antivirus scanning

- OS/400 keeps track of all changes and only calls the scanning software when files or virus definition files change.
  Scanning behavior can be controlled via IFS object attributes and system values.
- Only objects with IFS *TYPE2 in /root, QOpenSys and UDFS file systems are scanned.

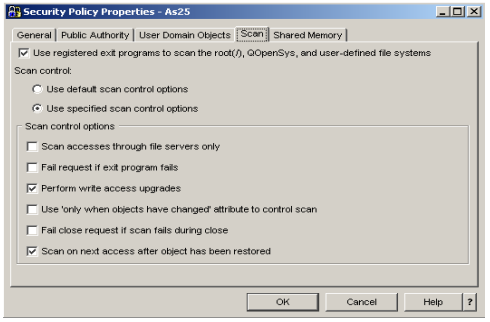
Integrity

Antivirus scanning

- Virus scanning products can register to the following exit points:
  QIBM_QP0L_SCAN_OPEN: Integrated File System Scan on Open Exit Program
  QIBM_QP0L_SCAN_CLOSE: Integrated File System Scan on Close Exit Program
- System-wide behavior controlled via two new

System value QSCANFS

System value QSCANFSCTL



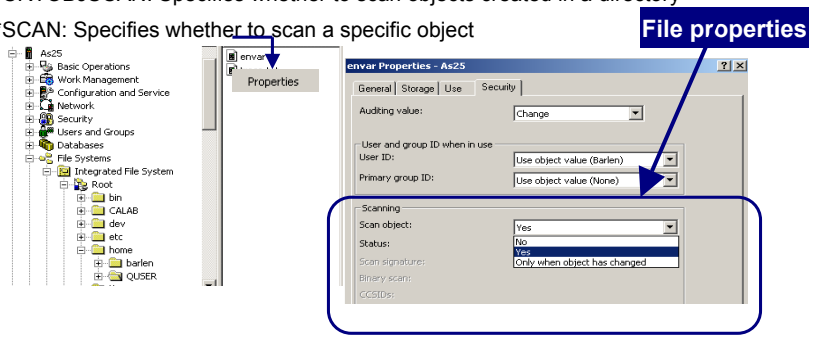
Integrity

Antivirus scanning

- Which files are being scanned can be further controlled via IFS object attributes.
- The following two new attributes were added and can be set via the Change Attribute (CHGATR) command:

  *CRTOBJSCAN: Specifies whether to scan objects created in a directory

  *SCAN: Specifies whether to scan a specific object

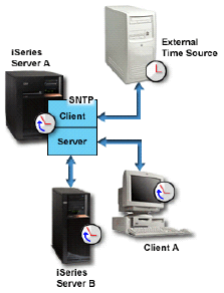



```
CHGATR OBJ('/home/quser/envar') ATR(*SCAN) VALUE(*NO)
```

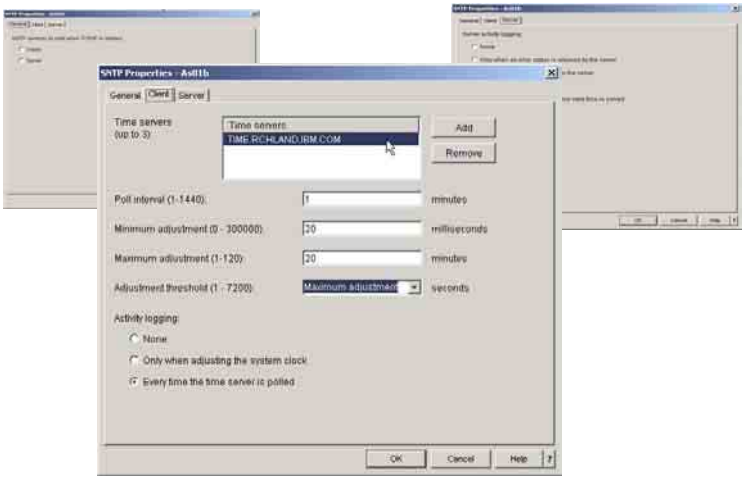

Time Synchronization

What time is it?

- V5R3 SNTP client
  changes system clock instead of software clock
- V5R3 SNTP server support
  iSeries serves time to other clients
- iSeries SNTP client and server can
  run concurrently

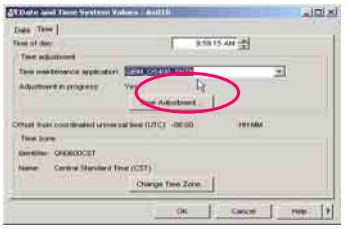


SNTP Configuration in iNav

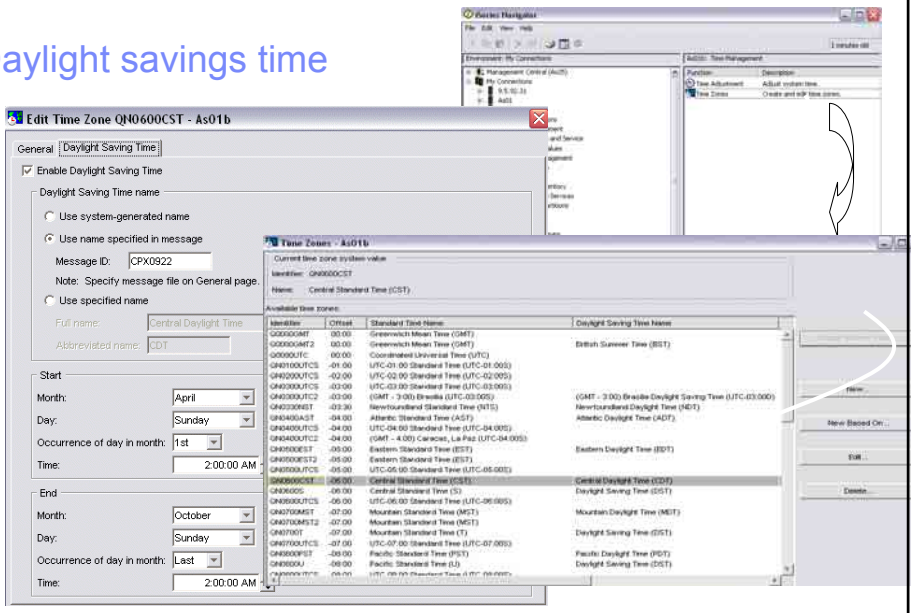


System values

- QDATETIME
  Composed of system values QDATE and QTIME
- QTIMADJ
  Time adjustment system value
  Identify the software to use to adjust system clock
  Keep system clock synchronized with external time source
- QTIMZON
  Central European Time: QP0100CET2



Daylight savings time



Need a break?

COMMON Belgium Infrastructure management

September 28, 2005

IBM

Fabian Michel

Senior IT Specialist
IBM Certified

IBM Belgium s.a.
Avenue du Bourget, 42
B-1130 Bruxelles
Tel. +32 2 225 38 22
Fax +32 2 225 23 68
E-mail: fabian_michel@be.ibm.com

Agenda Part 2

- Virtualization
- LPAR managment facilities
  - WebSM
  - Portable Utilities 5733-SC1 (OpenSSH)
  - Uncapped Partitioning
- Tivoli Storage Manager (TSM)

Virtualization Engine

Virtualization is delivered natively in IBM ^ ® iSeries™ servers. IBM Virtualization Engine - for Systems technologies can be used to help simplify your IT infrastructure, without disruption. You're then able to focus on continued business innovation and growth.

http://www-03.ibm.com/servers/eserver/about/virtualization/systems/iseries.html

Key Technologies

- **DLPAR:** Dynamic logical partitioning increases flexibility, enabling selected system resources like processors, memory and I/O components to be added and deleted from dedicated partitions while they are actively in use. The ability to reconfigure dynamic LPARs enables system administrators to dynamically redefine all available system resources to reach optimum capacity for each partition.
- **Micro-Partitioning™:** The POWER5™ processor introduces an enhanced partitioning model based on established mainframe technologies and LPAR/ DLPAR implementations on POWER4™ and POWER4+™ servers. Micro-Partitioning enables the virtualization of system resources on an extremely granular level. In POWER5 processor-based systems, physical resources can be abstracted into virtual resources that are available to partitions. Resources can be shared easily, and changes in resource allocation are transparent to users.
- **IBM Director Multiplatform:** IBM Director Multiplatform enables monitoring and event management across a heterogeneous IT environment, including Windows®, Intel®, AIX, OS/400 and Linux®, from a single Java-based user interface. From one access point, you can monitor system resources, inventory, events, task management, core corrective actions, distributed commands and hardware control for your servers and storage.
- **IBM Virtualization Engine console:** Many editions of iSeries and i5 servers feature Virtualization Engine console. The console is based on the IBM Integrated Solutions Console framework to provide a consolidated view for managing your virtualized enterprise resources. The Virtualization Engine console works with IBM Director Multiplatform to present a comprehensive view of individual platforms.
- **Virtual Ethernet:** Without requiring any additional hardware, the POWER5™-based iSeries systems provide 1Gb Virtual Ethernet communication paths between multiple operating systems such as i5/OS™, Linux® and AIX® 5L. Virtual Ethernet segments can be dynamically created and access to a virtual LAN segment can be restricted for security or traffic segregation requirements.
- **Virtual I/O:** The Virtual I/O Server is a special-purpose partition that provides virtual I/O resources to client partitions. The Virtual I/O Server owns the resources that are shared with clients. A physical adapter assigned to a partition can be shared by one or more other partitions, enabling administrators to minimize the number of physical adapters they require for individual clients. The Virtual I/O Server can thus reduce costs by eliminating the need for dedicated network adapters, disk adapters and disk drives.

Getting started

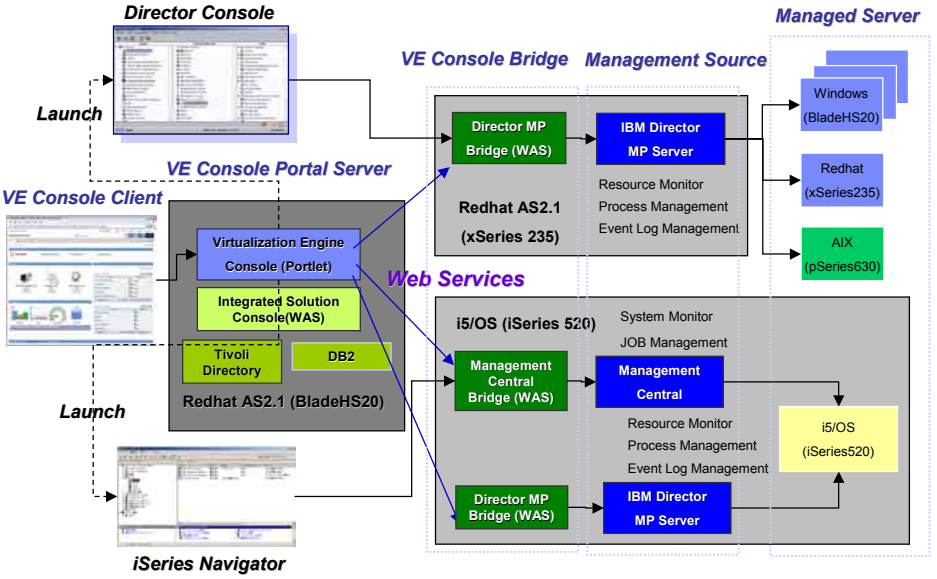
The information center!

http://publib.boulder.ibm.com/infocenter/eserver/v1r1/en_US/index.htm?info/veicinfo/eicarplangeneral.htm

What is the Virtualization Engine Console ?

- Virtualization Engine Console :
  - Integrated system management interface for IBM Virtualization Engine environment
    - Web based interface
    - Portal application for a system administrator who manages server, storage,…
  - Major functions
    - ***Health Center***
      - Provide a system administrator with overall resource health of managed resources in a consistent way
        - Resource Health
        - Monitor
        - Execute Task
      - Integrate and Enhance existing management server (ex. IBM Director)
    - ***Launchpad***
      - Launch system management consoles from single access place
        - Web client , local application client

Virtualization Engine Console implementation



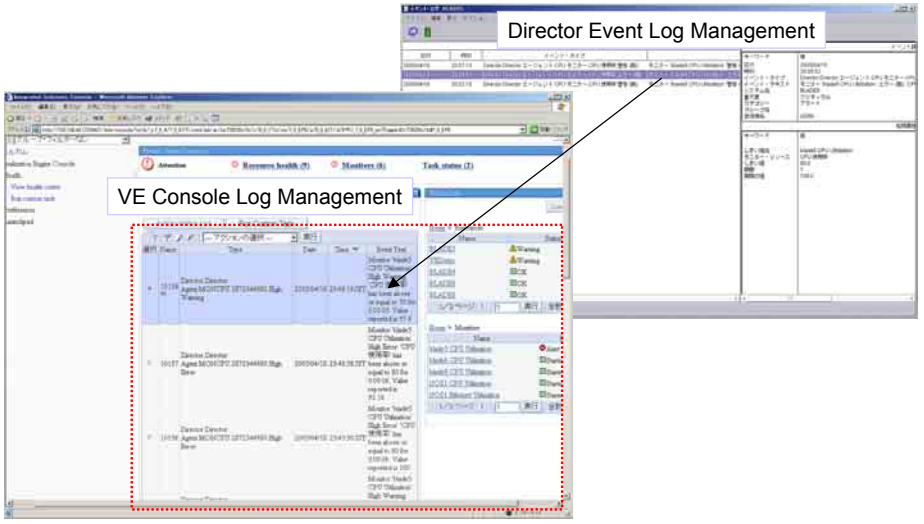
Supported functions of each Management Source

Virtualization Engine Console	Cluster Systems Management	IBM Director Multiplatform or IBM Director 4.20	Management Central	IBM Tivoli Monitoring 5.1.1
Resource	A node or a group of nodes running either AIX or Linux managed by a Cluster Systems Management (CSM) server.	A physical resource or logical group managed by the IBM Director Server.	The health of the Management Central server is checked by verifying the TCP/IP connection. If TCP/IP is up, the heartbeat of the server is reporting in, and the server is considered to be healthy.	not supported
Monitor	A Resource Monitoring and Control (RMC) condition monitoring resources on one or more endpoint systems managed by a CSM management server.	A threshold (individual, group, process monitor) monitoring an attribute on a system or systems managed by an IBM Director Server.	A Management Central server has system, file, job, message, and B2B activity monitors.	Tivoli Monitoring monitors resources at distributed systems. In this context, a resource is anything that affects the operation of a computer system and includes physical and logical disks, processors, memory, printers, as well as the processes and services running.
Custom task	A predefined DCEM task exposed to the Virtualization Engine console through CSM.	A set of custom tasks assisting in Director Multiplatform or IBM Director and console maintenance.	A commonly used command and package definition stored in Management Central.	not supported
Logs	Logs are AIX system logs and error logs	The Director Event Log on the IBM Director Server and the filters that are defined on this log.	Management Central does not map any logs into the Virtualization Engine console.	not supported
Processes	AIX processes and services that are running on the endpoint system.	AIX or Linux processes and services or Windows applications depending on the operating system of the Director Multiplatform or IBM	Management Central maps jobs into processes.	not supported

http://publib.boulder.ibm.com/infocenter/eserver/v1r1/en_US/index.htm

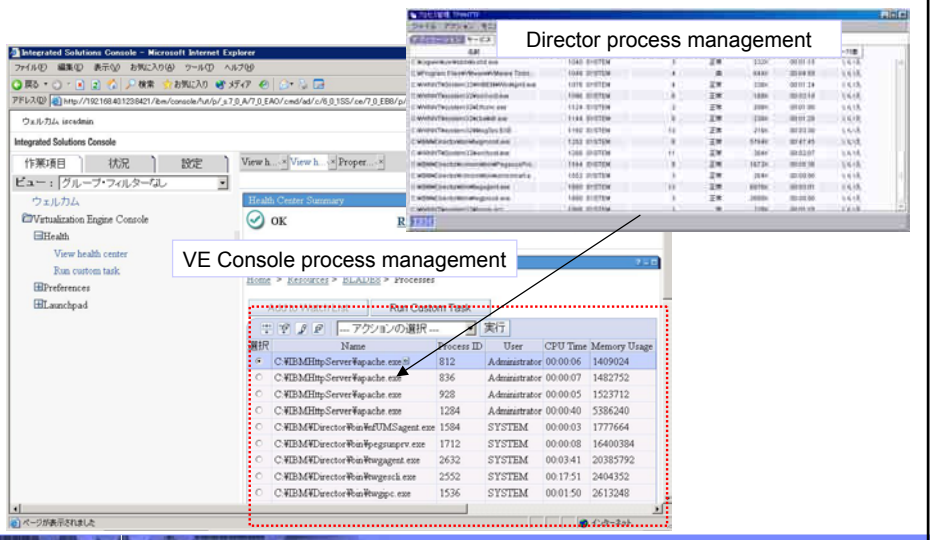
VE Console : Health Center sample1

IBM Director event log (message ,severity,..) is mapped into common VE console event log



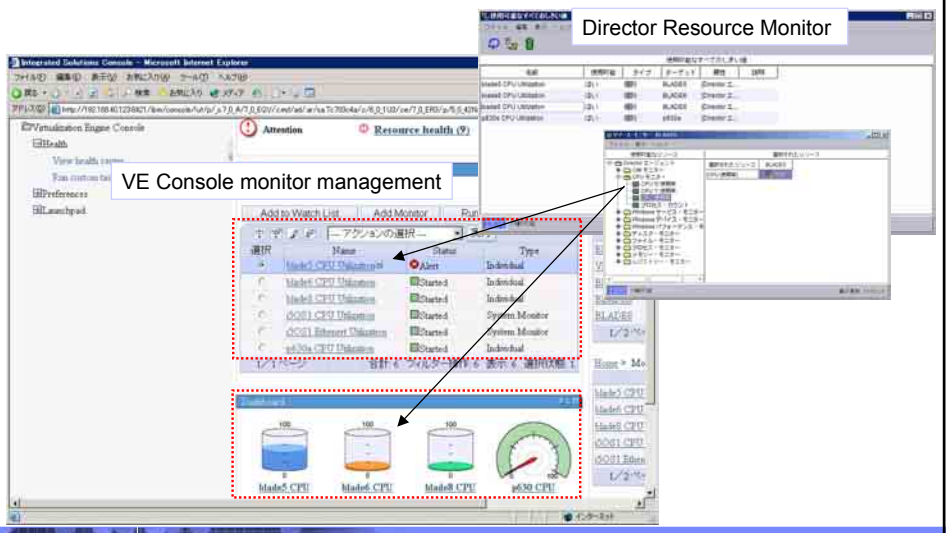
VE Console : Health Center sample2

IBM Director process is mapped into common VE console process



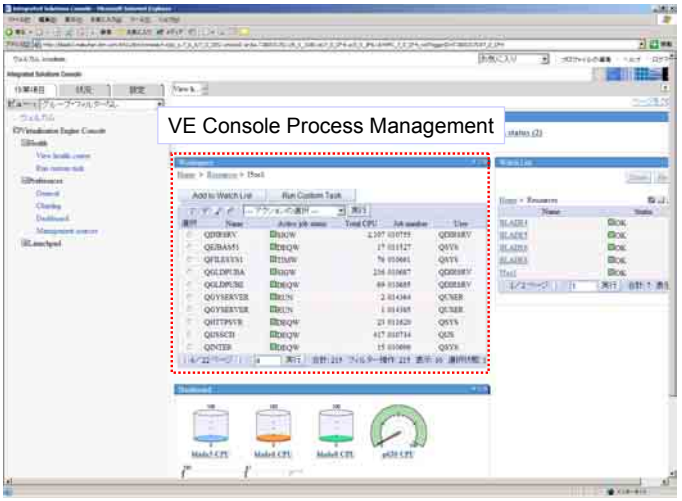
VE Console : Health Center sample3

IBM Director resource monitor is mapped into common VE console monitor



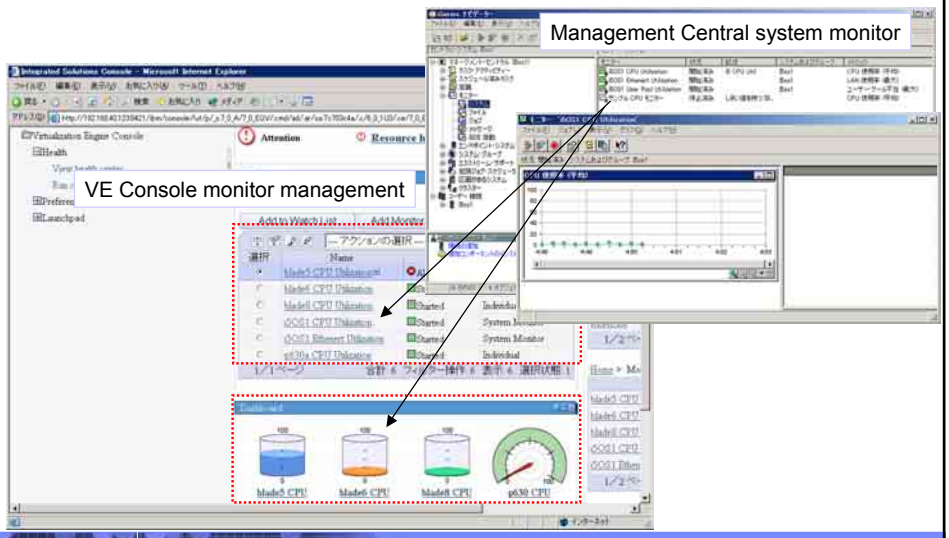
VE Console : Health Center sample4

iSeries Management Central job management is mapped into common VE console process



VE Console : Health Center sample5

iSeries Management Central system monitor is mapped into common VE console monitor



Common Luxembourg

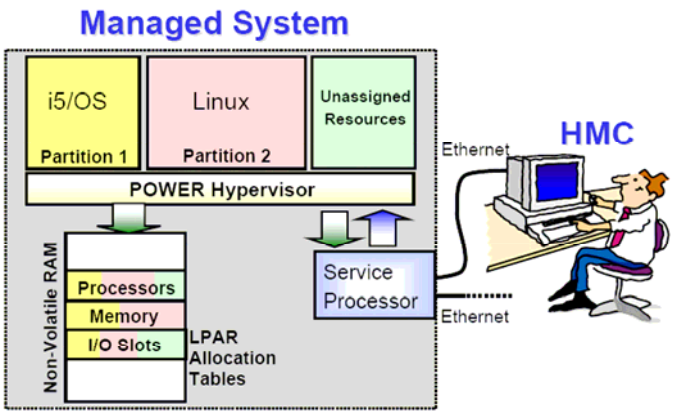
LPAR Management today

WebSM, OpenSSH, Uncapped Partitioning

September 28, 2005

How does LPAR work today?

The Big Picture

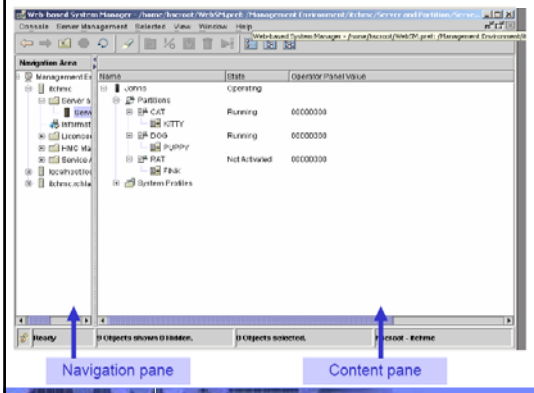


Interface

Desktop
7315-C03

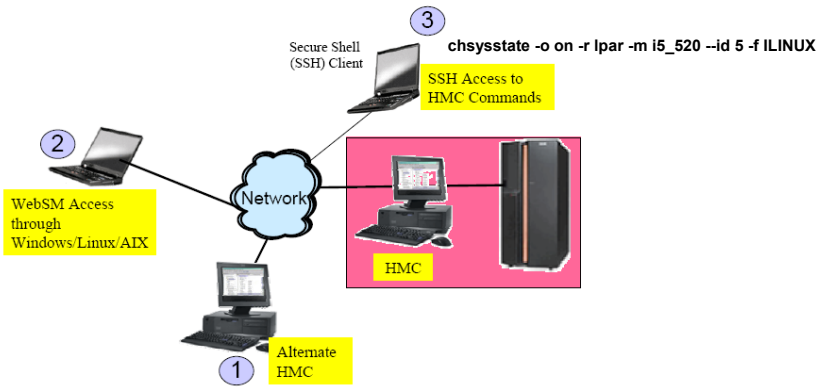
Rack-mount
7316-CR2

HMC Interface



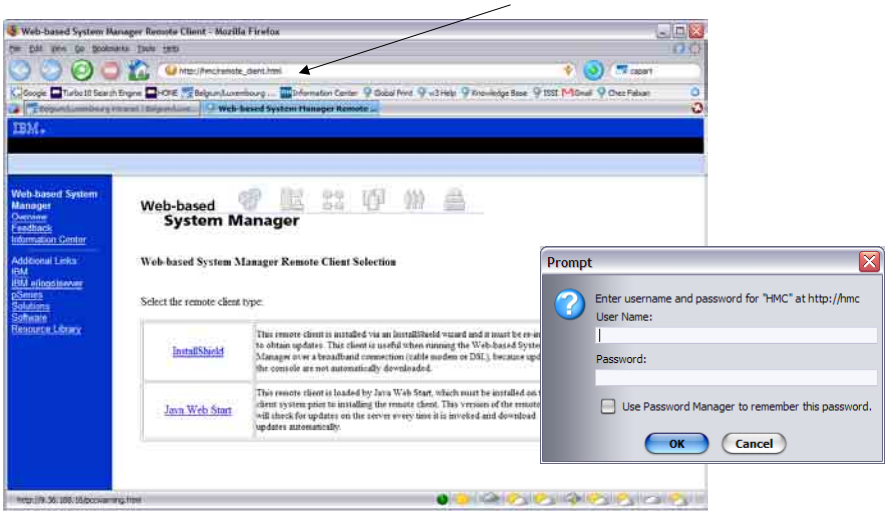
What about remote access?

Remote Access to the HMC



How to install WebSM?

http://hmc/remote_client.html



WebSM live demo!

Demo

What is behind Portable Utilities 5733-SC1?

- Licence Program 5733-SC1 Portable Utilities was introduced at no charge with every V5R3 SW orders since July 2005.
- It contains the OpenSSH(Secure SHell), OpenSSL and zlib open source packages ported to i5/OS using the i5/OS PASE runtime environment.
- The SSH protocol suite is a software solution that provides secure alternatives for telnet and ftp.
- OpenSSH is the open source implementation of the SSH protocol suite. OpenSSH is widely available for use on many other platforms including Linux, AIX and z/OS.
- How to use ssh to remotely manage HMC resources?

Utilities available in Open SSH:

- 1. **ssh** - a secure telnet replacement that allows an i5/OS user to connect as a client to a server running the sshd daemon. An ssh client can also be used to connect to the HMC on the IBM Eserver 5xx iSeries models.
- 2. **sftp** - a secure ftp replacement. As with all implementations of sftp on other platforms, sftp can only transfer data in binary format. Note that sftp also does not provide the enhanced functions available in the i5/OS ftp utility when transferring files in the QSYS.LIB file system nor does it provide the CCSID data conversion options available in the i5/OS ftp utility.
- 3. **scp** - a secure file copy program -- basically an alternative to sftp for copying a single file in the integrated file system (IFS).
- 4. **ssh-keygen** - a public/private key generation and management tool. SSH allows users to authenticate using these public and private keys as an alternative to using their OS signon password.
- 5. **ssh-agent** - an authentication agent that can store private keys. ssh-agent allows a user to load their public/private key pass phrase into memory to avoid needing to retype the pass phrase each time an SSH connection is started.
- 6. **sshd** - The daemon that handles incoming ssh connections. The sshd daemon utility allows users to connect to i5/OS via an ssh client. In contrast to connecting to i5/OS via telnet and being presented with a 5250 screen interface, users that connect via ssh to an i5/OS system running the sshd daemon will be presented with a character interface and an i5/OS PASE command line.
- More details on this utilities found at: http://www.openssh.org/manual.html

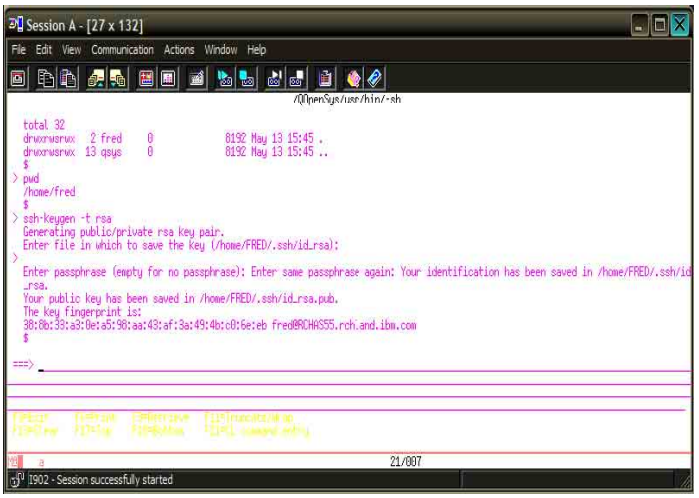
Installing the OpenSSH licence program in i5/OS

- **Install the licence program 5722-SS1 Option 33 -** Portable Application Solutions Environment (PASE).
- **Install the licence program** IBM Portable Utilities for i5/OS **using the command RSTLICPGM LICPGM(5733SC1) DEV(OPTxx) OPTION(*BASE) RSTOBJ(*ALL) LNG(2924).**
- **Install the licence program 5733SC1 Option 1** OpenSSH, OpenSSL, zlib **using the command RSTLICPGM LICPGM(5733SC1) DEV(OPTxx) OPTION(1) RSTOBJ(*PGM).**

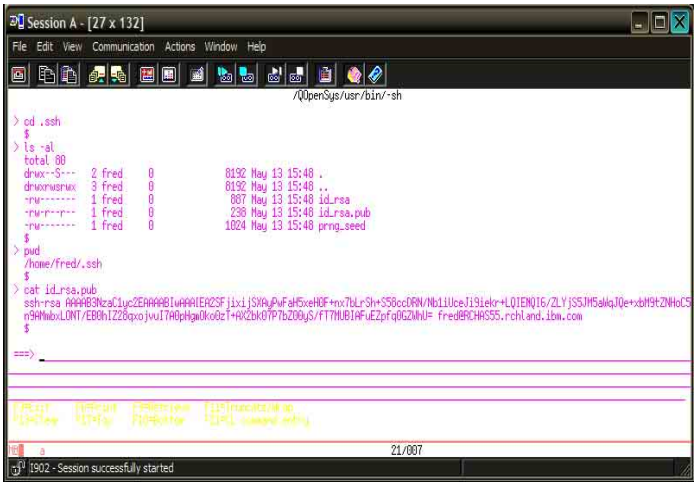
Configuring SSH

1. Create a new HMC *user* (to be performed on the HMC with adequate wizard).
2. Create a corresponding i5/OS *user* profile
3. Signon to i5/OS with this *user* profile and run **call qp2term**
4. Create the directory called *user* under **/home**
5. Change the owner ship of the directory *user* using the command **chown *user user***
6. Go to the directory **cd /home/*user***
7. Generate the ssh key by using the command **ssh-keygen –t rsa**.
8. Go to the directory **cd /home/*user*/.ssh**
9. Run a command **cat id_rsa.pub** and copy the displayed key
10. Establish the connection to HMC from qp2term shell using the command **ssh -T x.x.x.x** (where x.x.x.x is the IP address of the HMC).
11. run the command **mkauthkeys** to authenticate the key which we have generated **mkauthkeys --add** 'paste the key here.
12. Run a command **ssh -T x.x.x.x** to logon to HMC.

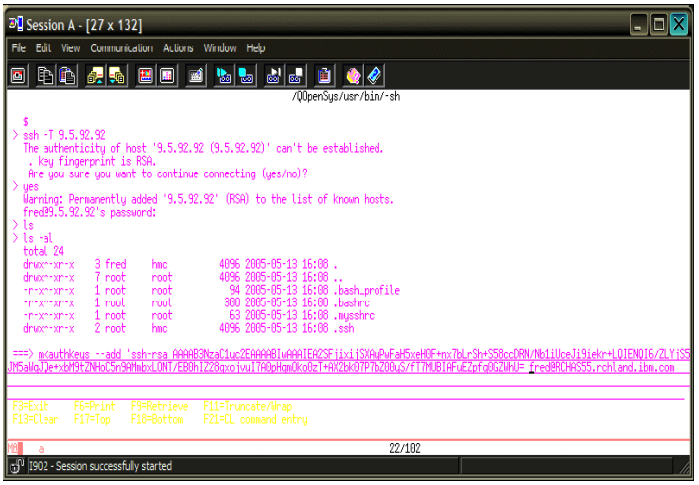
Configuring SSH: generating the public key



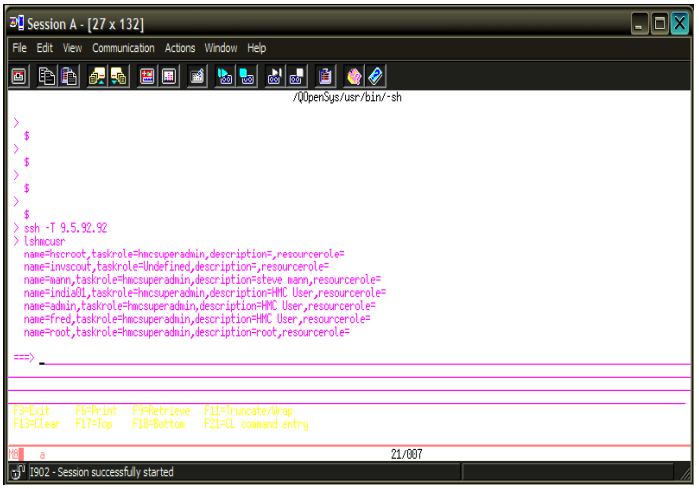
Configuring SSH: copy the rsa public key



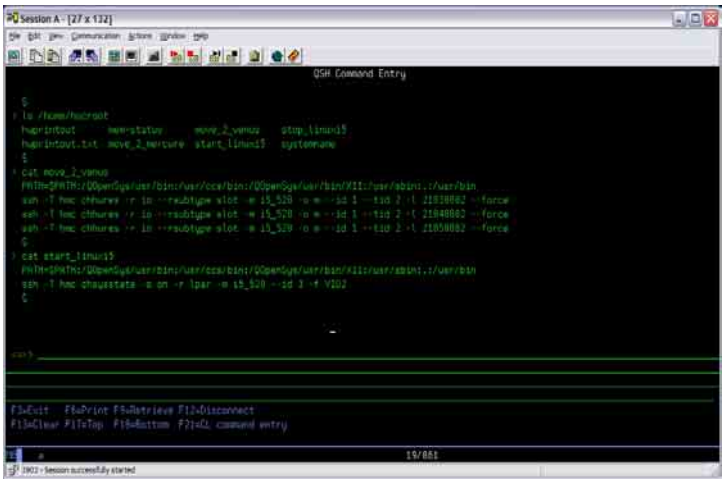
Configuring SSH: key authentication



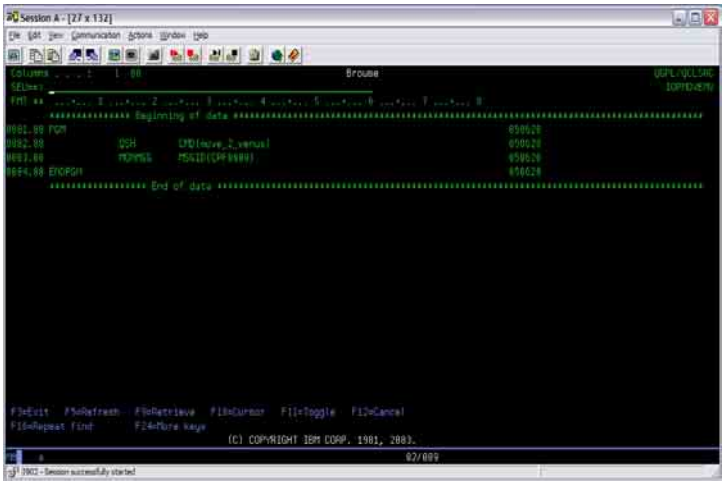
Signon!



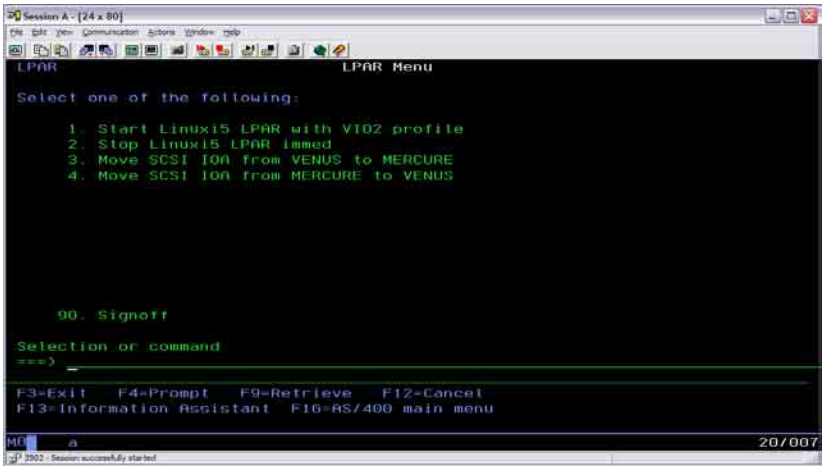
OpenSSH scripting examples in QSHELL:



CL command example to run a QSH script:

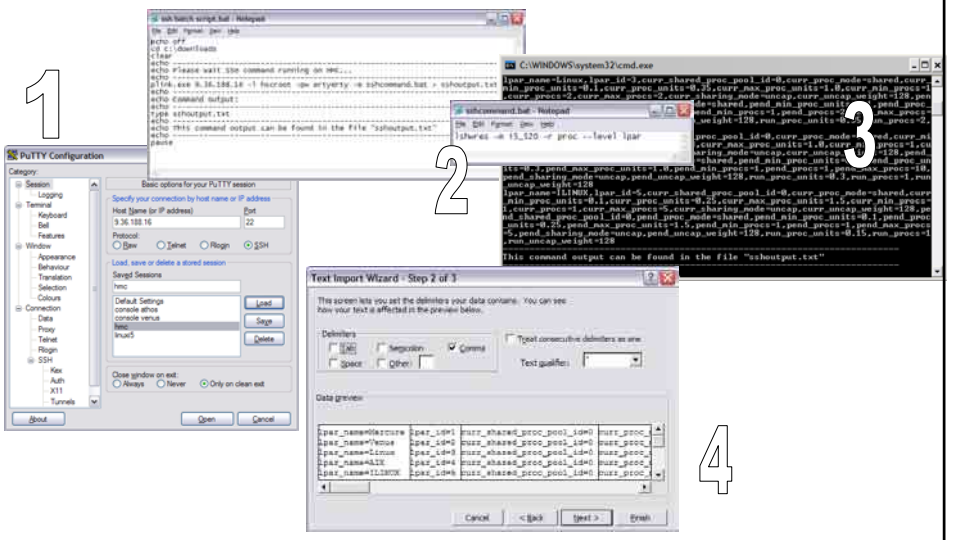


Customize….



Once scripts and commands are working as desired you can easily integrate them to your menus, other CL scripts, scheduled tasks, etc...

SSH from Windows using Putty & Plink.exe



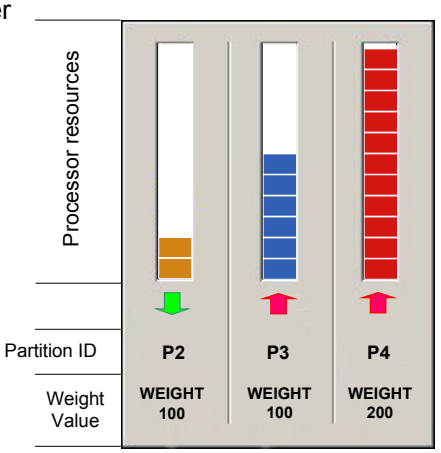
Live Demo!

Uncapped Partitioning

- What is it?
- How does it work?
- How to configure it?
- Licencing consequences?

Capped and Uncapped Partition support

- Automate processing power distribution with uncapped partitions
- Use resources out of a shared processor pool
- Uncapped weight value
- Defined in the Partition Profiles
- Use what is available



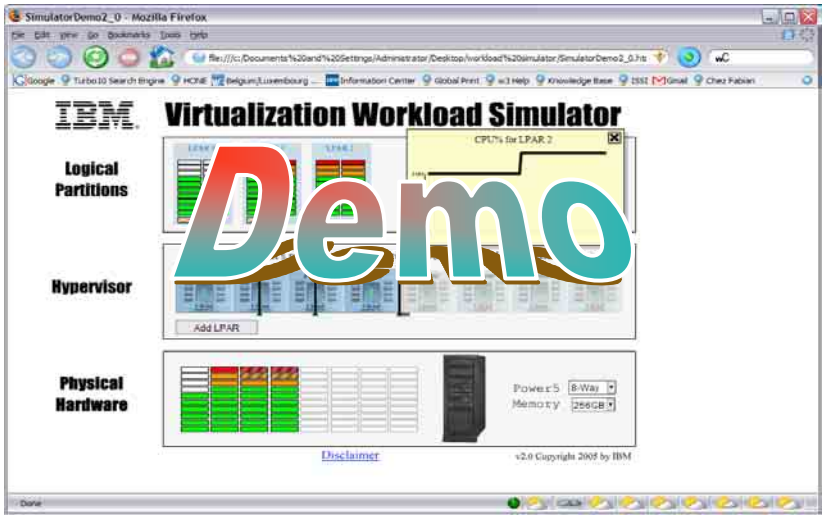
Notes: Capped and Uncapped processor support - 1

When setting up a partition profile, you will need to set up the desired, minimum, and maximum values you want for the profile.
The **desired processing value** is the amount of processing resources that the partition will get if processing power is not overcommitted. If the desired amount of processing units is available, the profile will start with the amount processing units indicated. However, if when processors are overcommitted , the partition will get a value that is between the minimum and desired amount.
If the **minimum processing value** is not met for a partition profile, the profile will not be activated. If there is a processor failure, the system will attempt to accommodate the minimum processor sizes for all partitions. If all minimums are satisfied, the partitions will restart with all available resources distributed proportionately to their allocation.
Partitions in the shared processing pool can have a sharing mode of capped or uncapped.
A **capped partition** indicates that the logical partition will **never exceed its assigned processing capacity**. The capped mode could be used if the user knows a software application would never require more than a certain amount of processing power. Any unused processing resources will only be used by the uncapped partitions in the same shared processing pool.
An **uncapped partition** means that the partition's **assigned current processing capacity may be exceeded**, up to the partition's maximum virtual processors settings, when the shared processing pool has any unused processing power.
As an example, partitions 2, 3, and 4 all had uncapped mode selected. Partition 2 had 3.00 processing units assigned to it, but only 1.00 processing unit was in use. Partition 3 had 1.00 processor processing unit, but had a workload demand that required additional processor resources. Because partition 3 is uncapped, the server allows the unused 2.00 processing units in partition 2 to be used in partition 3. This situation increases the processing power for partition 3 to 3.00 processing units, and the workload demand needed at that particular time finishes.

Notes: Capped and Uncapped processor support - 2

Using the same example, assuming that both partitions 3 and 4 both need additional resources at the same time to complete a job, the server can distribute the unused processing resources to both partitions.
This distribution process is determined by the uncapped weight of each of the partitions.
Uncapped weight is a number in the range of 0 through 255 that you set for each uncapped partition in the shared processing pool. By setting the uncapped weight (255 being the highest weight), any available unused capacity is distributed to contending logical partitions **in proportion to the established weight value** of the uncapped partitions. The default uncapped weight value is 128. Again using the same example, if partition 3 had an uncapped weight of 100 and partition 4 had an uncapped weight of 200, partition 4 would get twice the unused processing resources that partition 3 received.
Finally, when the eServer i5 has partition(s) configured that are using a profile with **dedicated processors** and these partition(s) are in a **power off status**, the processors that then are unused in the server, become available for the uncapped partition processor pool.

Uncapped partitioning simulator tool demo!



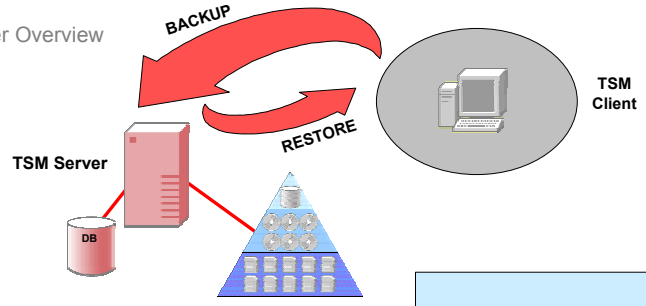
Uncapped partitioning live demo!

An AIX solution at work…

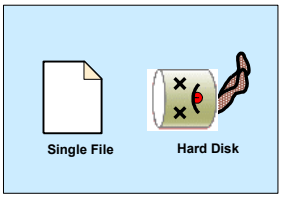
TSM - Tivoli Storage Manager

Backup / Restore

Tivoli Storage Manager Overview



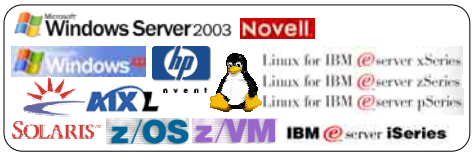
- Progressive / selective / adaptive subfile differencing / point-in-time / volume level
- Multiple versions kept
- Policy managed
- System assisted restore
- Automated scheduling



Data Protection

Tivoli Storage Manager is widely scalable. It supports popular applications, databases, and storage devices…

TSM supports a broad set of operating environments



TSM supports major business applications

TSM supports over 500 storage devices including disk, tape, optical and network storage appliances

In summary, managing storage with IBM Tivoli Storage Manager can substantially benefit your bottom line

Centralized Data Backup and Restore - Providing data protection based on smart-move and smart-store technology, leading to faster backups and restores with less network and storage resources needed
Automated Data Archive and Retrieve – Making it easy to protect and manage documents that need to be kept for a certain period of time
Automated, High Speed Policy-Based Disaster Recovery – Enabling business continuance after disasters, with reduced risk of manual error or need to add additional resources
24x365 Application Protection – Permitting business critical applications to continue operating with little or no interruption

TSM demo infrastructure