

Linux & z/VM – Premier Solution Secure and Resilient

Tim Kane,
Linux and Virtualization
PDT Leader



This educational piece is intended for your use in selling. It is NOT a deliverable for your customers

© 2004 IBM Corporation

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: AS/400, DBE, e-business logo, ESCO, eServer, FICON, IBM, IBM Logo, iSeries, MVS, OS/390, pSeries, RS/6000, S/30, VMESA, VSE/ESA, Websphere, xSeries, z/OS, zSeries, z/M

The following are trademarks or registered trademarks of other companies

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
Linux is a registered trademark of Linux Torvalds
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.
Intel is a registered trademark of Intel Corporation
* All other products may be trademarks or registered trademarks of their respective companies.

NOTES:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

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

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

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

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The 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.

Enhance Your Global Fabric by Leveraging Your Most Capable Asset: Your Mainframe

- As our customers understand the IT requirements for on demand they cite a strong synergy to zSeries capabilities

- IBM's vision is to leverage zSeries leadership capabilities around:
 - *OnDemand*
 - *Business Resiliency*
 - *Security*
 - *Business Integration*
 - *Intelligent Workload Management*



Do we really need to worry about Security and Resilience?



Agenda – Security Topics

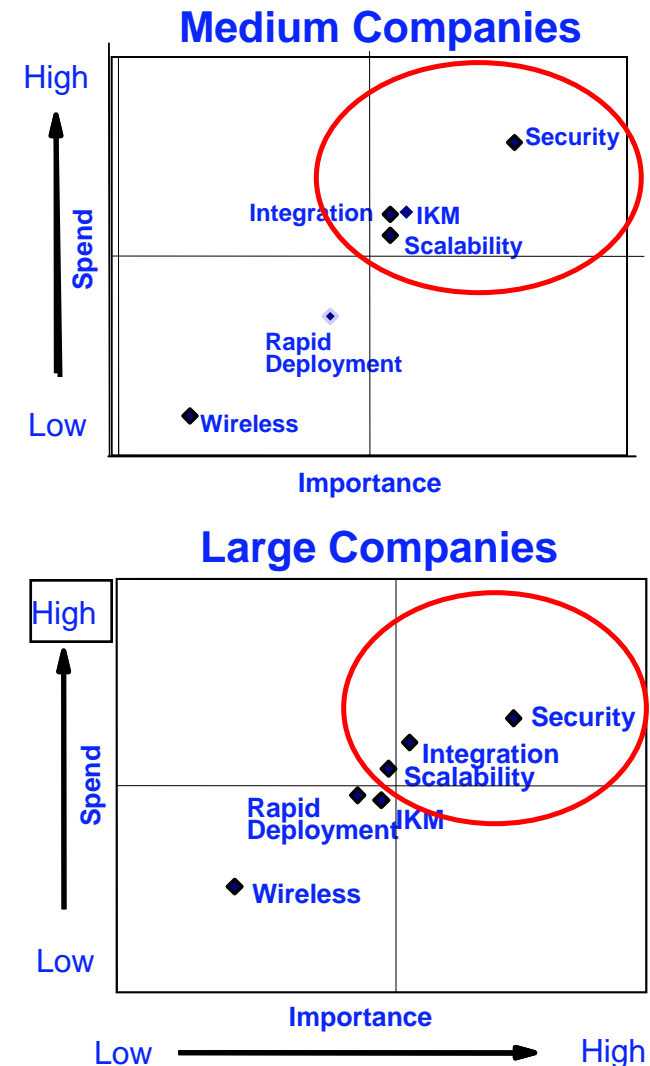
- Growing Emphasis on Security
- Security – The Big Picture
- z/VM System Integrity and Security Functions
- Linux and zSeries Security Topics
- Customer Responsibilities

Is Security Important?

Boardroom level emphasis on Security & Privacy

1. World Wide Political Events
 - ▶ Military Actions, Terrorist concerns, Transportation safety . . .
2. Social and Business Constraints
 - ▶ Corp. Financial Crisis, Brand liability changes, Identity theft . . .
3. Regulatory & Privacy Demands
 - ▶ HIPPA, GLB, Common Criteria, EU & Australian Privacy Act . . .
4. External Attacks
 - ▶ Hacker and System Virus potency in all Industries
 - SoBig.E represented 75% of the email traffic on 8/25/03

Result: More expense just to stay even



Source: 2003 e-business Infrastructure Needs Assessment Research

Assessing the Threat

- Loss of Revenue
- Loss of Customers
- Loss of Intellectual Property
 - ▶ Including customer data
- Loss of Tangible Property
- Loss of Corporate Communications
- Damage to Brand
- Loss of Reputation
- Interruption of Internal/External Communications
- Concern regarding Privacy
 - ▶ Customers
 - ▶ Partners
 - ▶ Employees
- Loss of Data and Source Code

IBM Security Initiatives Based on Interviews & Patterns

Improving current products

- Missing Capabilities
- Better Integration & testing
- Enhance individual products

Enabling New Technology

- Opportunity to improve the Enterprise IT Environment

New End to End Value

- Enabling Security and Privacy permit New enterprise business models

Government Sector

- Common Criteria, FIPS, MLS environments
- Services and Brand Implementation

Secure Alignment within IBM

- Business Security Patterns based product integration
- Across 200+ products and services
- Research leadership and alignment

Enterprise Integrity Go-To-Market

Integration of Physical and Logical security

Web Services Security standards

Linux

Extending the role of Services

- Business Security Patterns based methodology
- Managed Security Services and risk assurance

Integrity Based Computing

- Open Standards for the Enterprise Environment
- Extending IBM's capabilities beyond TCG standards

The Big Picture

Security Management

Security Management covers the policies, processes and tools that:

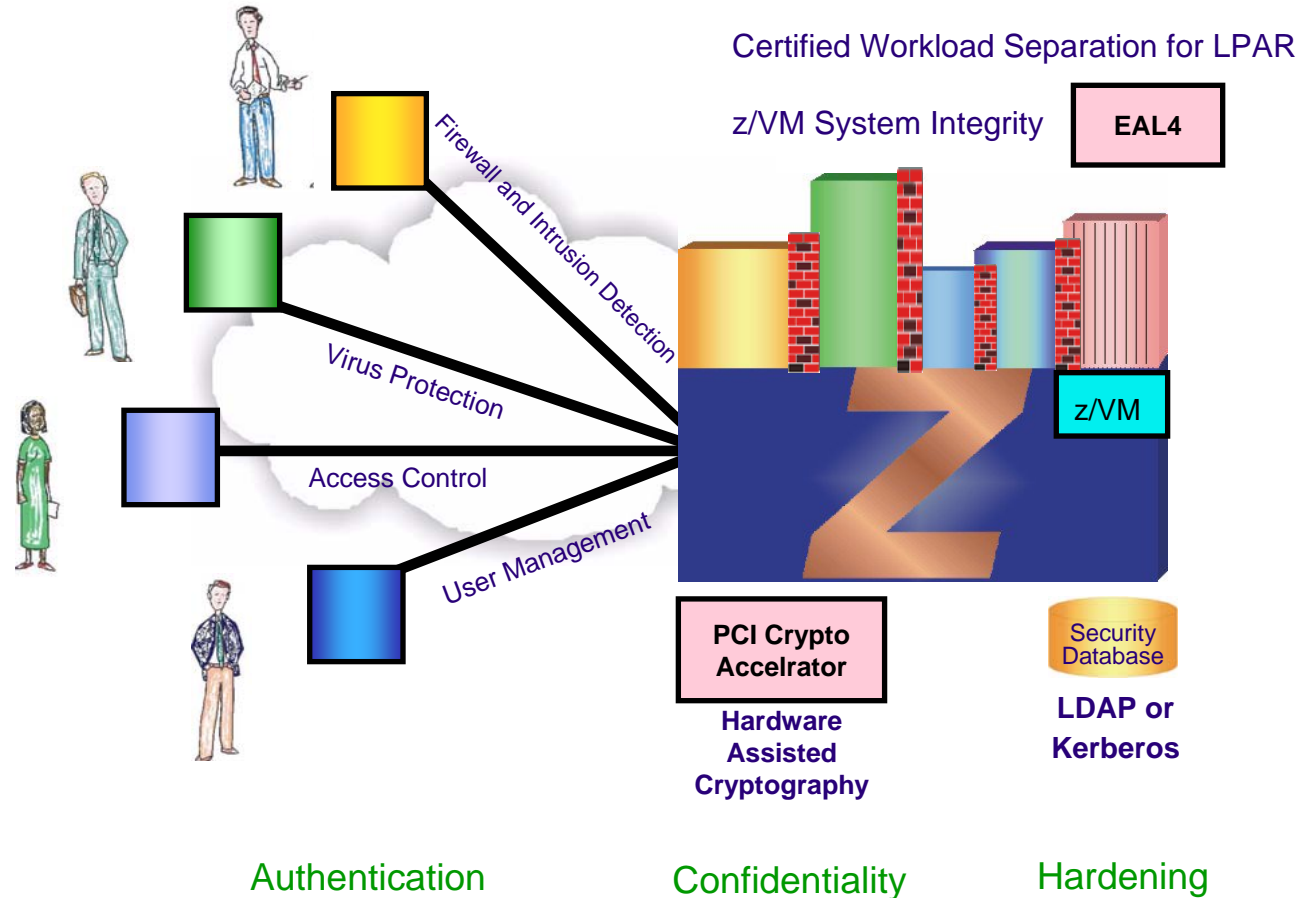
- define users and resources
- control and audit access.

System security is all about risk.

- Human or social risks,
- network risks,
- risk of malicious or accidental application corruption
- data integrity risk

Security policy is ultimately the definition of acceptable risk.

Security – The Big Picture



Addressing the Threat

- 5 key elements of security
 - Identity Lifecycle Management
 - Access Management
 - Threat Management
 - Privacy Management
 - Auditing and Monitoring
- Key operational considerations
 - Providing end-to-end protection
 - Minimizing loss in the event of a security breach
 - Functioning non-intrusively to users

A Comprehensive IT Security Infrastructure

- Firewall
- Virtual Private Network (VPN)
- Virus Protection
- Intrusion Detection
- Authentication and Access Control
- Encryption
- Security Management

Addressing the 5 Security Elements

	Identity lifecycle mgmt	Access mgmt	Threat mgmt	Privacy mgmt	Audit and Monitor
Security Management	X	X	X	X	X
Firewall		X	X		
Virtual Private Network (VPN)		X		X	
Virus protection			X		X
Intrusion Detection System	X	X	X	X	X
Authentication		X			
Encryption				X	

z/VM Integrity And Security Functions

What is z/VM system integrity?

- The ability of the Control Program (CP) to operate without interference or harm, intentional or not, from the guest virtual machines
- The inability of a virtual machine to circumvent system security features and access controls
- The ability of CP to protect virtual machines from each other

Linux on zSeries Security

z/VM Guest (virtual machine) Isolation

- **z/VM uses the same facilities for guest separation as LPAR EAL4 certification**
- **Each Linux server image running under z/VM is entirely isolated from other server images**
 - the guest has only access to the processor, when it is active
 - no access to storage
 - any device dedicated to a guest is not accessible by other guests
 - network communication between guest and outside world via physical devices
 - guests may communicate directly to the outside world or
 - through a router (e.g. another Linux guest or the z/VM TCP/IP stack)
 - shared data access and communications through physical pathways or defined VM services
- **z/VM guests may use cryptographic hardware**
 - PCICA is supported by z/VM for Linux guests

What is z/VM System Security

- Authentication: Knowing who is accessing the system or its resources
- Authorization: Enabling a user to only have access to system resources specifically permitted
- Security is only meaningful in the presence of system integrity!
 - ▶ Integrity prevents bypass of security controls

Authentication

- Anyone wishing to access VM resources must provide both the VM user ID and the user password
 - ▶ login
 - ▶ ftp and nfs
 - ▶ rexec

- Or, portal must perform its own authentication and map the authenticated user to a VM user ID
 - ▶ E.g. application which uses Kerberos

- Anonymous access possible, but must be explicitly enabled by system administrator: login, ftp, nfs, rexec

Authorization

- Native CP authorizations can be supplemented by External Security Manager (ESM), e.g. RACF

- Authorization is based on
 - ▶ who you are: your VM user ID
 - ▶ Unix UID/GID
 - ▶ privilege class
 - ▶ directory authorizations
 - ▶ ESM access control list

- what you know: a password
 - ▶ If minidisks not protected by ESM

External Security Manager

- Enhances auditing, authentication, and access controls
- Encrypt user passwords
- Use Access Control List for minidisks instead of minidisk password
- Well-defined programming interfaces
 - ▶ RACROUTE macro
 - ▶ CSL routines
- RACF/VM is a feature of z/VM

Intrusion Detection

- Incorrect passwords
 - ▶ Limit number of attempts
 - ▶ Define actions to be performed
 - ▶ Message to operator
 - ▶ Create an accounting ("journal") record
 - ▶ Lockout for some number of minutes
 - ESM user lockout requires administrator intervention

- Network
 - ▶ Certain denial of service attacks (e.g. blat) are detected and reported on TCPIP console
 - ▶ NETSTAT DOS command

Security

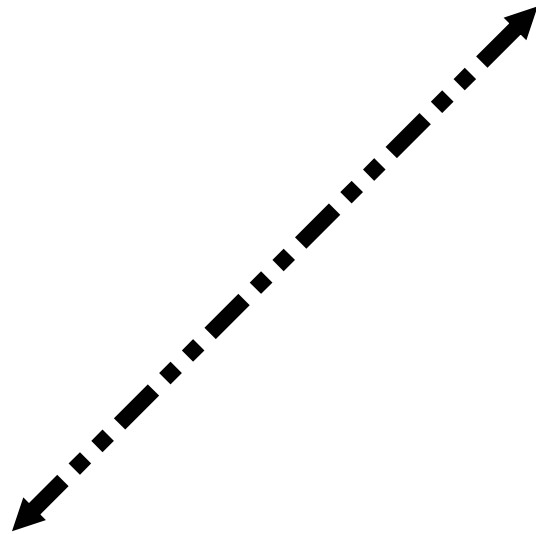
Topics

- ❖ Can Linux really be Secure?
- ❖ Security Certifications for Linux
- ❖ System Hardening
- ❖ Hipersockets – Fast, **and Secure**
- ❖ Encryption
- ❖ Have you considered Open Source Security Products?
- ❖ Commercial Security Products
- ❖ Coordinating Security Management across zSeries

Can Open Source Possibly Be Secure?

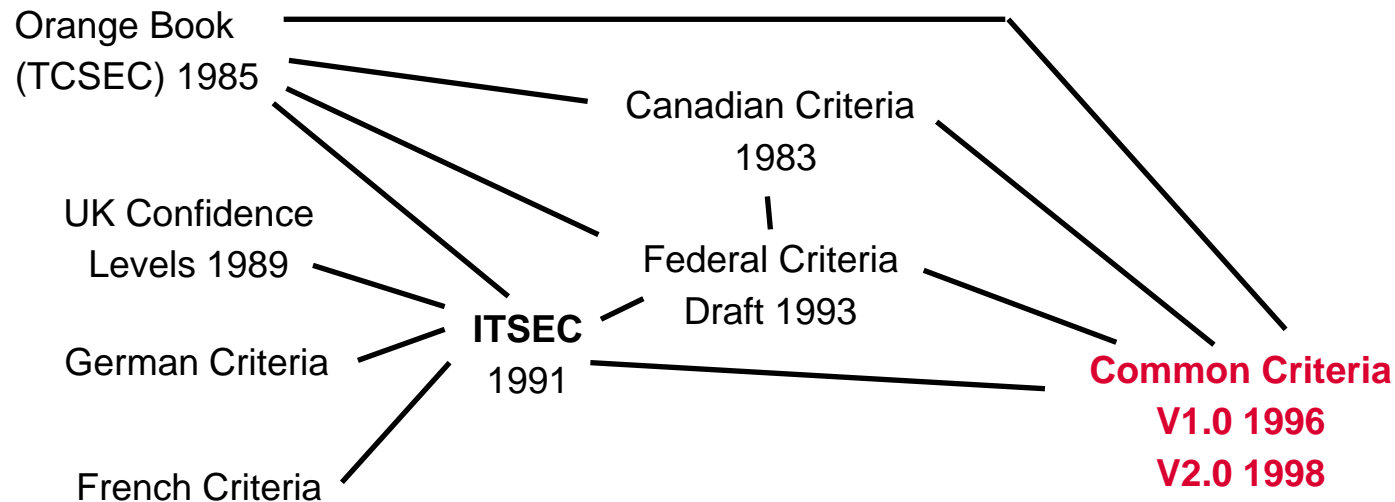
Security through Transparency

- Anyone can analyze the code for flaws and fix them, that is people can scan code for security weaknesses
- Peer review by active developer community increases likelihood of flaws being discovered and fixed
- Fixes appear quickly in response to CERT advisories



Security through Obscurity

Security Certifications



IBM is focusing on working toward:

- ▶ Defense Information Infrastructure Common Operating Environment (DiiCOE) compliance
- ▶ The Common Criteria for Information Technology Security Evaluation (CC) certification

And working to assure Linux initially to EAL2 and eventually to EAL4

Key Government Standards

DII Common Operating Environment (DIICOE)

- ✓ "look + feel+ function"
- ✓ DOD Only, and mandatory
- ✓ New Spec for Linux
 - ✓ Linux Standard Base (LSB)
- ✓ Interoperability via Govt. kernel code operation

+

Common Criteria Security Certification (CC)

- ✓ Criteria for evaluation of IT security
- ✓ International applicability
 - ✓ mandatory / preferred
- ✓ Two independent components:
 - ✓ Function (low to high)
 - ✓ Desired security behavior
 - ✓ "a little, a lot, or somewhere inbetween"
 - ✓ Assurance
 - ✓ Confidence in security claims
 - ✓ Heirarchy of evaluation assurance levels
 - ✓ EAL 1 increasing to EAL 7
- ✓ **Protection Profiles**
 - ✓ **Standardized sets of security requirements: function and assurance**

First things First – Harden That Linux

- Create hardened instances ***and clone them***
- Keep in mind the services that you need and don't need.
- Use tools to help perform Linux hardening:
 - ▶ Bastille
 - Comprehensive System View
 - Educational (Especially for new Linux users)
 - Support from the Linux Community
 - Is now officially available for Linux on zSeries
 - Available from some distributions
 - ▶ Vistalogx
 - Security Auditing Tool (www.vistalogx.com)
 - ▶ NMAP
 - Now with a Windows interface

Nmap Results: Before Hardening

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	open	smtp
37/tcp	open	time
79/tcp	open	finger
80/tcp	open	http
110/tcp	open	pop-3
111/tcp	open	sunrpc
513/tcp	open	login
514/tcp	open	shell
515/tcp	open	printer
767/tcp	open	phonebook
901/tcp	open	samba-swat
2049/tcp	open	nfs

These Ports were all open “out of the box”.

NMAP Results: After Bastille

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	open	smtp
37/tcp	open	time
79/tcp	open	finger
80/tcp	open	http
110/tcp	open	pop-3
765/tcp	open	webster
901/tcp	open	samba-swat
2049/tcp	open	nfs

Ports for:
Sunrpc
Login
Shell
Printer
Phonebook
are gone.

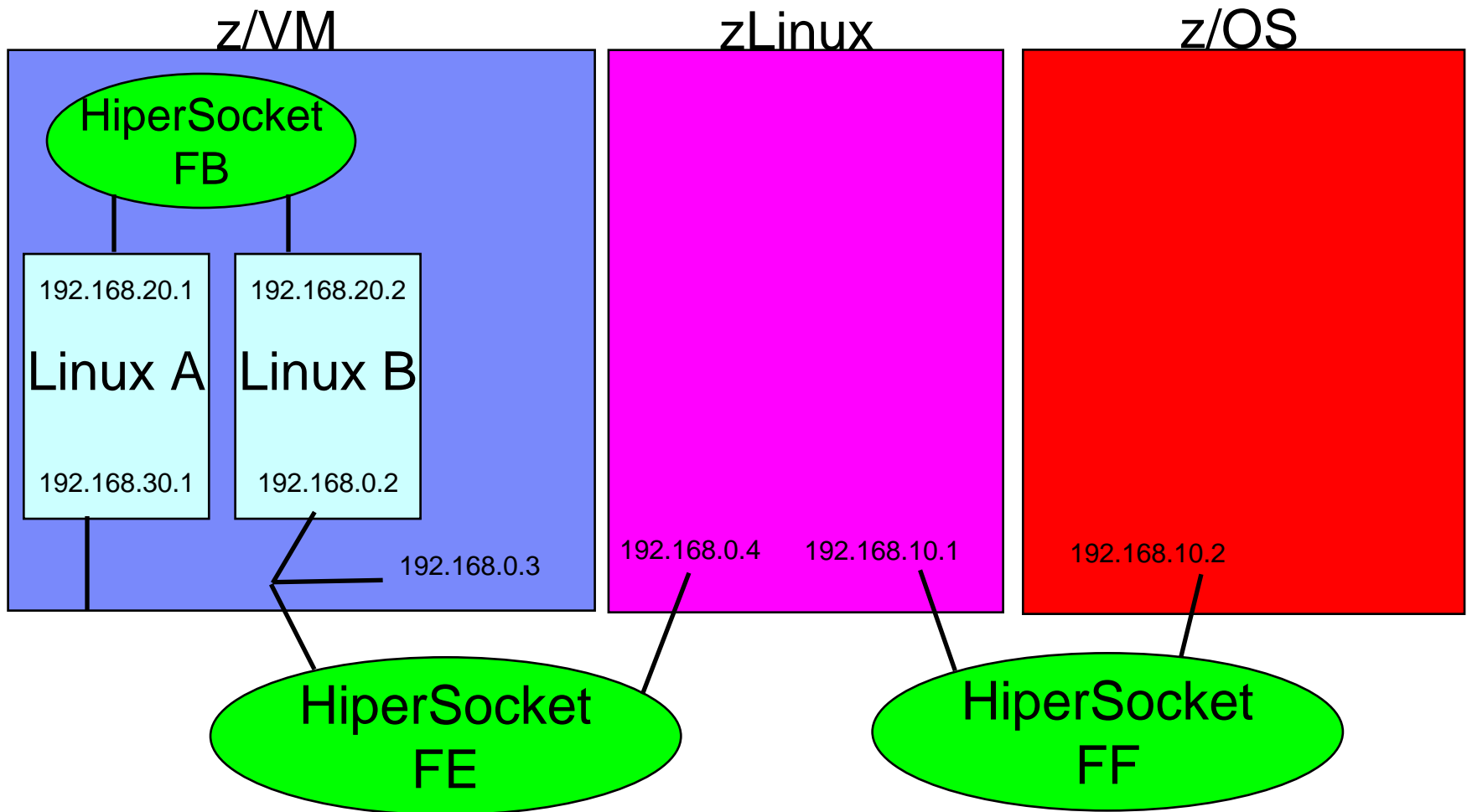
HiperSockets – Just The Facts

- HiperSockets = Internal Queued Direct IO
- Microcode maintained lookup table
- Three devices for each stack
 - ▶ Read Control
 - ▶ Write Control
 - ▶ Data Exchange
- 1024 Devices across all HiperSockets
- Supports Virtual IP Addressing and Dynamic Virtual IP Addressing

VM Guest LAN Support

- Virtual HiperSockets (Virtual Virtual sockets?!?)
- Emulates HiperSockets within a VM image
- Maximum number of unused CHPIDs -1
- 3072 I/O devices per guest LAN
- 1024 guests (TCP/IP stacks)
- Faster communication between Linux images than HiperSockets

Wheels Within Wheels



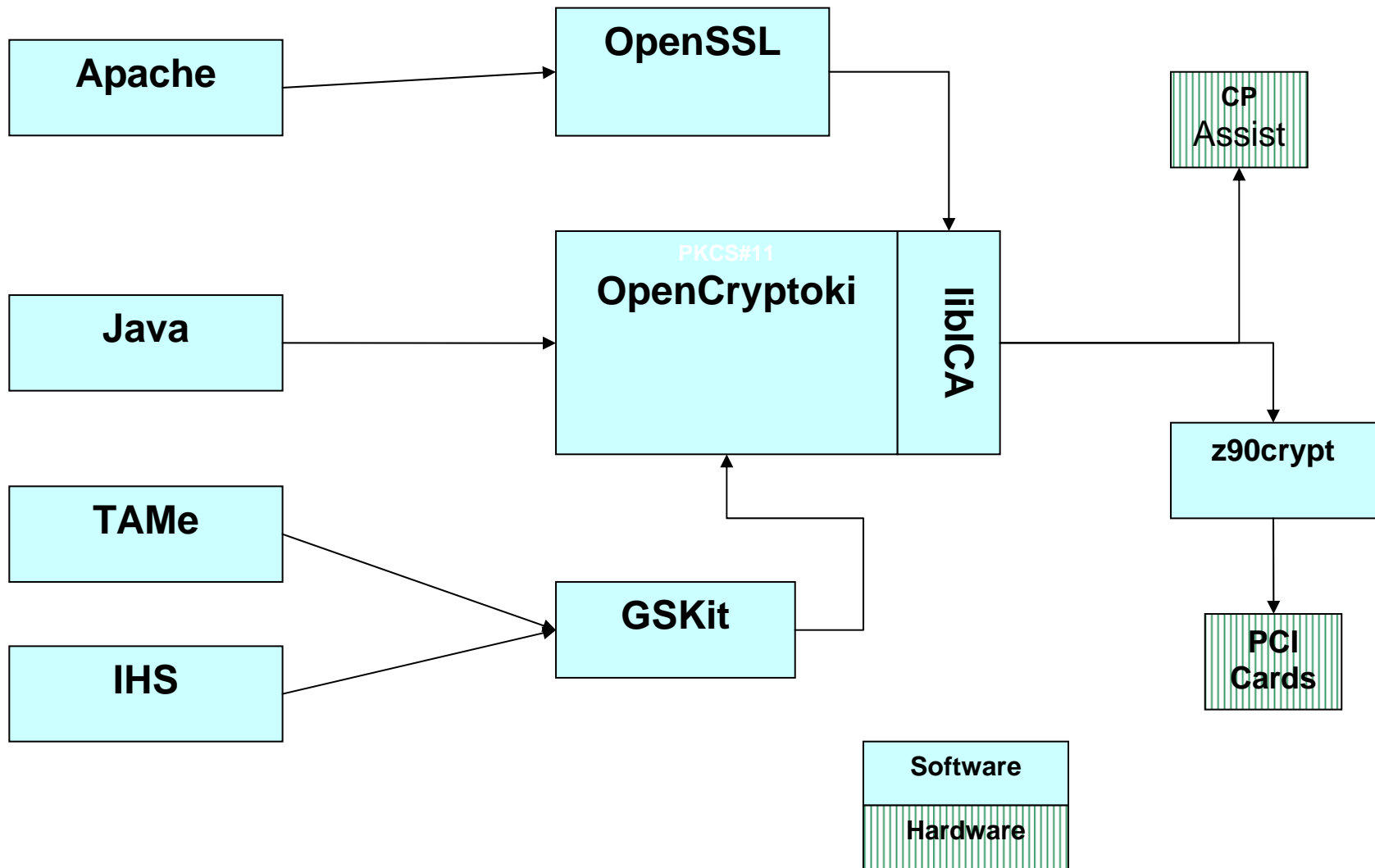
Sockets – Beyond the Hype

- Fast – If you like that kind of thing
- z/VM Guest LANs faster for inter Linux communication
- Don't expect IIOF flows to be faster...
- More secure communication
 - ▶ Unsniffable traffic between connections
 - ▶ Reduces the need for SSL
 - ▶ Lessens the dependency on encryption
 - Real performance benefits

Data Encryption

- Communications between systems
 - Tools to encrypt email, data transfers
 - openSSL (secure socket layer) - encrypt/decrypt data traffic
 - openSSH (secure shell) - for secure communication
 - encrypts all network traffic
 - supports PAM
 - uses openSSL for crypto functions
 - secure remote file copy (scp) based on SSH
 - IPSEC (IP Security Protocol)
 - provides end-to-end cryptographically based security for IPv4 and IPv6
 - Cryptography can be exploited by application and web servers

Encryption



Role of Linux Distributors

- Linux Distributors are taking a more active role in providing a more secure environment right out of the box
- SuSE SLES 9 includes
 - Secure Shell
 - Virtual Private Network
 - Enhanced Audit Capabilities
 - Enhanced Authorization Options
 - Enhanced Firewall Management
 - Intrusion Detection System
 - Cryptographic Libraries and Access to Hardware Accelerators
 - Host and Network Scanning tools

Security Options for Linux on All Platforms

Access Control Lists	LoMac, Best Bits, IBM Tivoli Access Manager & WebSeal, CA's eTrust Access Control & Web Access
Anti-Virus	ClamAV, OpenAntiVirus, AmaViS, MIMEDefrag, CA's eTrust AntiVirus, REA Internet F-PROT
Hardware Acceleration	Asymmetric PCICC, PCICA and PCIXCC from IBM Symmetric DES, TDES, SHA-1
Digital Certificates	Freeware PKI
Firewall	IPTables/NetFilter, zGuard, StoneGate
Intrusion Detection	Snort, Snare, PortSentry, TripWire, LIDS, IPLog, IBM Tivoli Risk Manager, ISS RealSecure, PredatorWatch, SafeZone
Directory Services	OpenLDAP, IBM Directory, CA's eTrust Directory, NIS/NIS+

Vendor Product
Open Source Product

Security Options for Linux on All Platforms

Secure Network Communications	OpenSSH, PGP, GNU PGP, USAGI IPv6, FreeS/WAN, CA's eTrust VPN, StoneSoft's StoneGate VPN
Secure Socket Layer (SSL)	OpenSSL, GSKIT, PKCS#11
System Hardening	Bastille, Tiger, Distributions
Secure Data	CFS, TCFS, ppdd, McAfee's E-Business Server
Distributed Policy Management	IBM Tivoli Access Manager, CA's eTrust Directory
Proxy Server	Proxy Suite from SuSE, IBM Edge Server

Vendor Product
Open Source Product

Open Source Security Tools

- **Authentication:** password checkers check for trivial passwords or given password rules
 - ▶ Cracklib, passwd+, anlpasswd
- **Encryption:** GNU Pretty Good Privacy (GnuPG)
- **Intrusion Detection:**
 - ▶ SNORT (www.snort.org)
 - Network intrusion detection system
 - Analyzes network traffic
 - May perform actions dependent on rules
 - ▶ Tripwire (www.tripwire.org)
 - checks integrity of file system
 - checks gathered information with database

Open Source Security Tools

- **Intrusion Detection:** LIDS - Linux Intrusion Detection System (www.lids.org)
 - ▶ restrict access to security relevant functions for all users
 - ▶ based on "Linux Capabilities" - more granular superuser privileges

 - ▶ intrusion detection options, e.g.
 - logging of violations
 - kernel port scan detector
 - hide system monitoring tools
 - additional read-/append-only options
 - ▶ restrict, e.g.
 - loading of kernel modules
 - raw memory access, raw disk access, raw access to I/O ports
 - access to all files used during boot process
 - ▶ system protection, e.g.
 - using ACLs and Linux Capabilities
 - protection of routing tables and firewall rules
 - protection of mount function
 - protection of daemons against specific signals

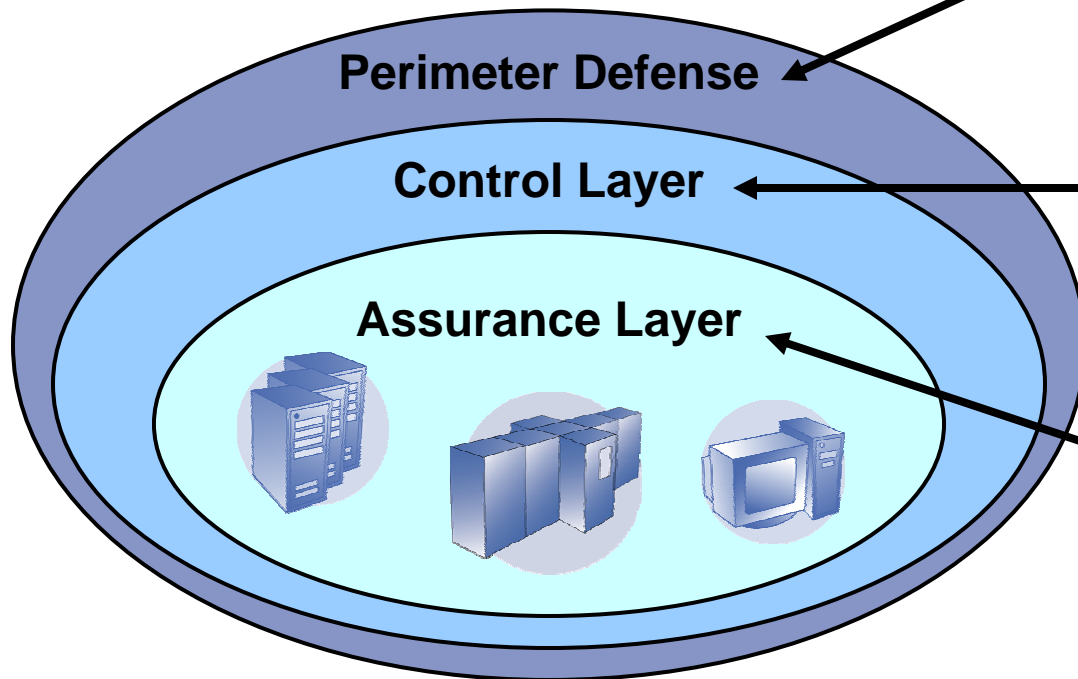
Open Source Security Projects

- Project: Linux Event Logging for Enterprise Class Systems
 - ▶ provides open source event logging facility
 - ▶ offers capabilities and features comparable to event and error logging found in enterprise-class Unix systems
 - ▶ supports logging of events including printk and syslog messages
 - dependent on configuration file
 - ▶ POSIX compliant
 - ▶ more information at evlog.sourceforge.net

- Project: Auditd (www.hert.org/projects/linux/auditd)
 - ▶ logging as part of the Linux kernel.
 - ▶ all processes are affected by auditing
 - ▶ detects security abuses from user land processes
 - ▶ used for security, syslogd should be used for debugging

Organizations Need More Than Just Perimeter Defense

Tivoli solutions provide management for all three layers



Perimeter Defense
 Keep out unwanted with

- Firewalls
- Anti-Virus
- Intrusion Detection, etc.

Control Layer

- Which users can come in?
- What can users see and do?
- Are user preferences supported?
- Can user privacy be protected?

Assurance Layer

- Can I comply with regulations?
- Can I deliver audit reports?
- Am I at risk?
- Can I respond to security events?



Tivoli Security for the Automation Blueprint



Enables information assets, confidentiality and data integrity to be protected

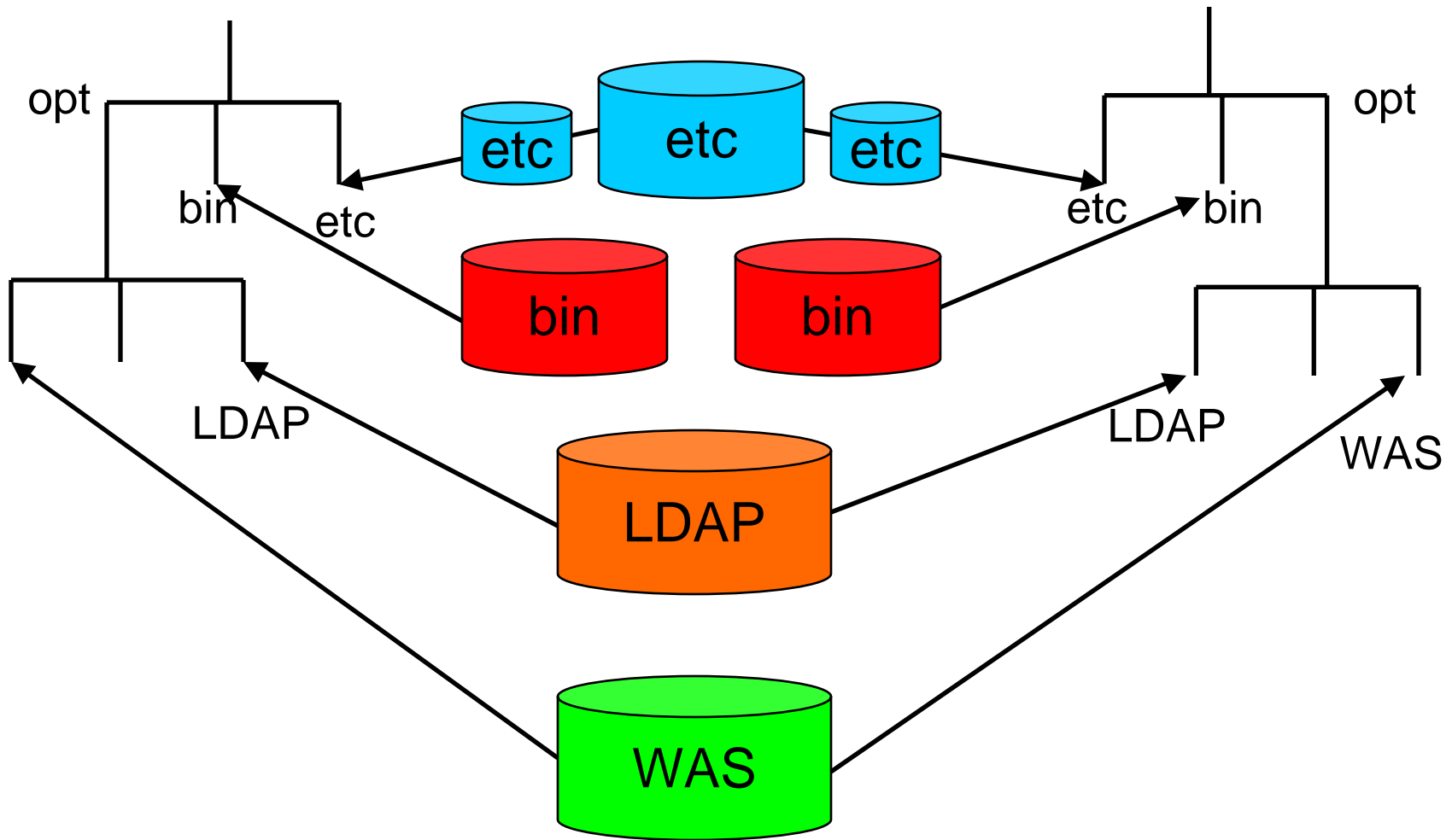
- **Identity Management Solution**
 - ▶ IBM Tivoli Identity Manager
 - ▶ IBM Tivoli Access Manager Family
 - ▶ IBM Tivoli Privacy Manager
 - ▶ IBM Tivoli Directory Server
 - ▶ IBM Tivoli Directory Integrator

- **Security Event Management Solution**
 - ▶ IBM Tivoli Risk Manager

Coordinating Security Management across zSeries

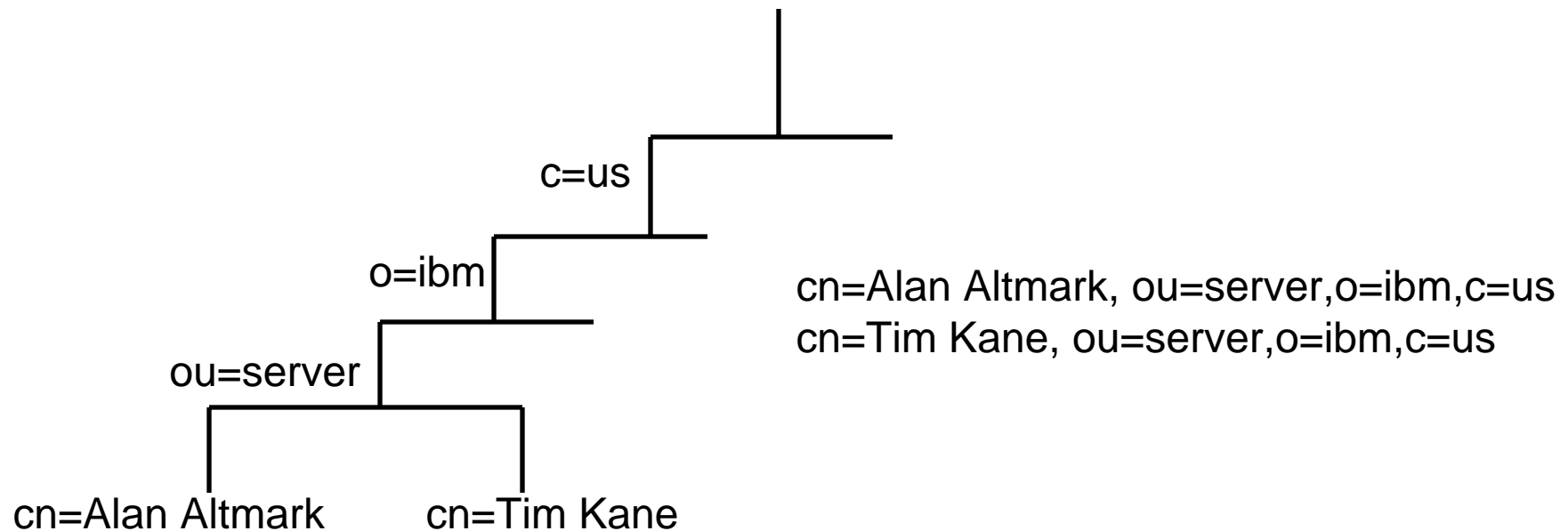


Using z/VM to Clone Linux



LDAP A Security Database

- Lightweight Directory Access Protocol
- Limited function database
- Relatively Static Data
- Based on a Directory (hierarchical) structure

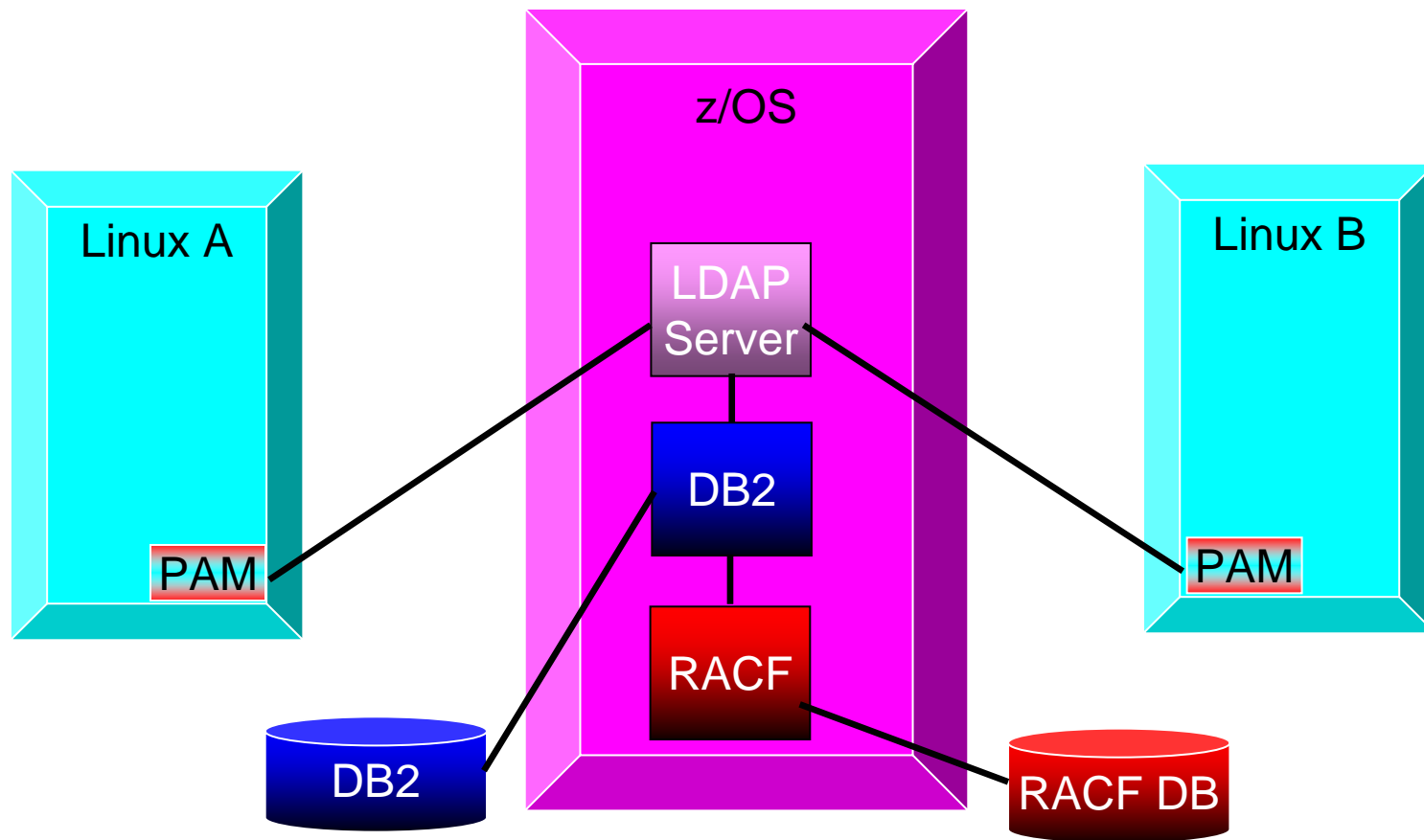


PAM Who?

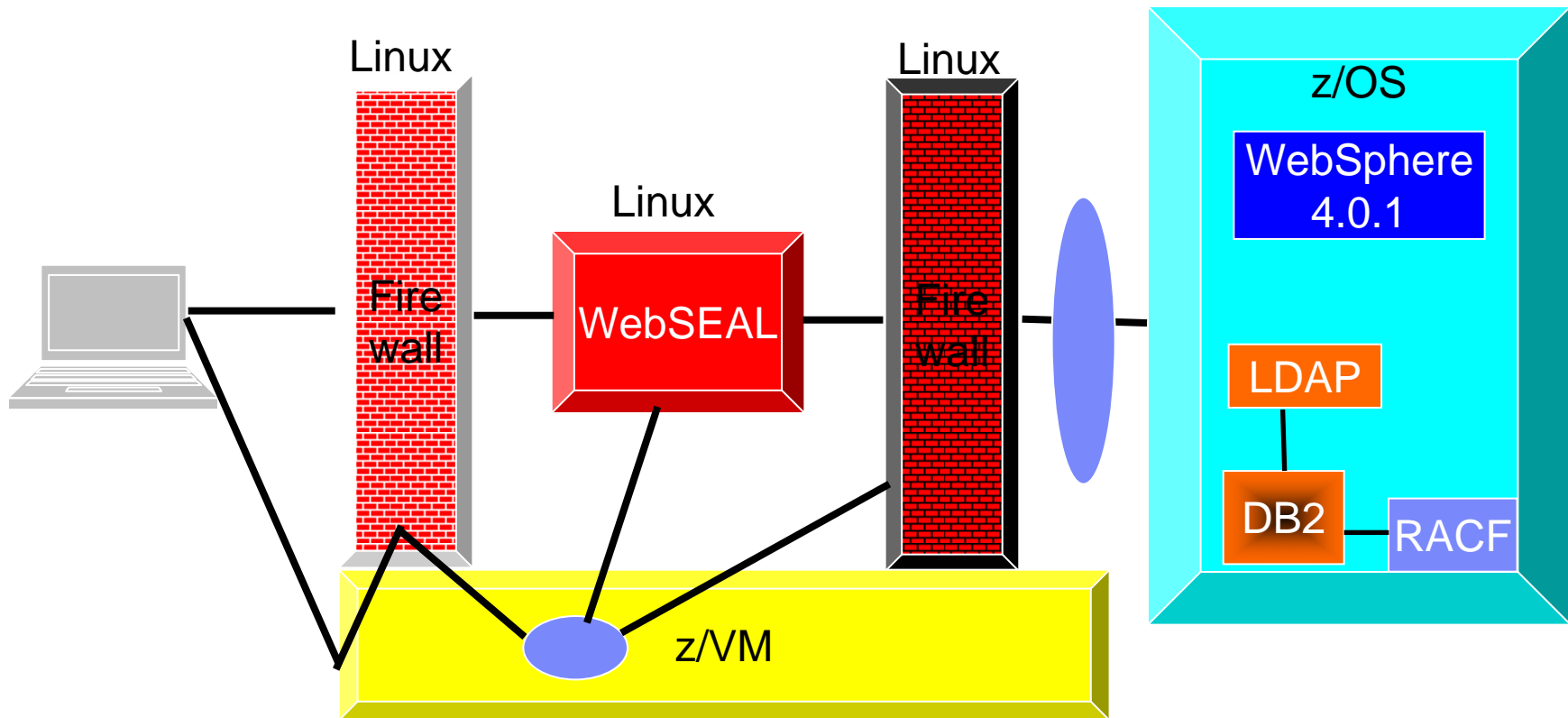
- Pluggable Authentication Module
- Allows you to create security for each service you provide
- This allows you to limit access to services.
- Create layers of security to access certain functions.
- A bunch of different PAMs are available:
 - ▶ PAMSMB – Use NT to authenticate Linux Users
 - ▶ CUECAT – Bar code reader based authentication
 - ▶ PAMAFS – Use AFS to authenticate
 - ▶ LDAPPAM – Use LDAP to authenticate user

But Wait... There's More....

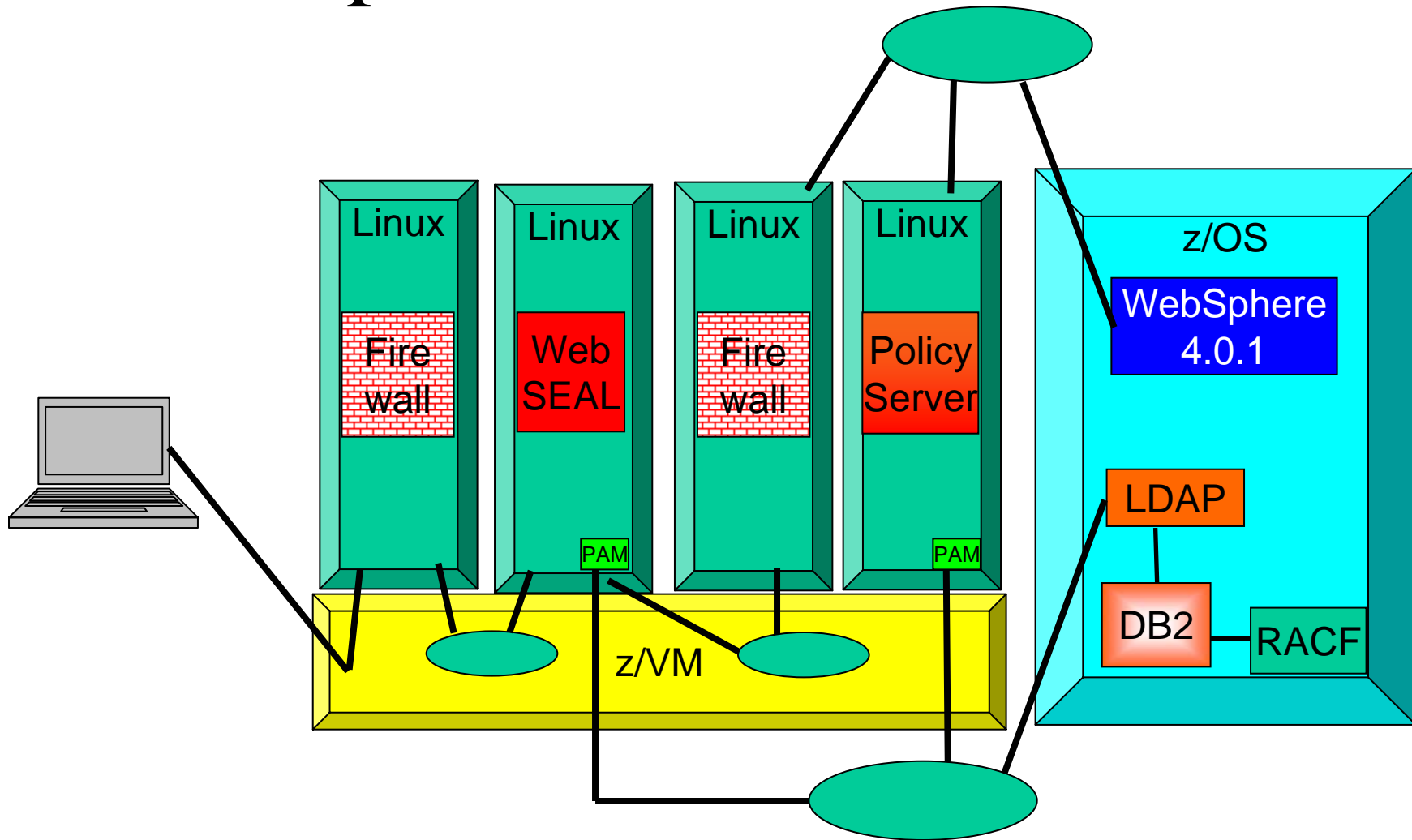
- What if RACF only held the Password?



Putting All your e-business servers on zSeries



Complete e-business Scenario



Customer Responsibilities

***Pay Attention:
This is Important***

Wake Up : This Part is Almost Over!

- Linux on z/Series is the essentially the same as every other Linux
 - ▶ Must be hardened
 - ▶ Vulnerable to network attacks
 - ▶ Must be diligent to ensure that all holes covered
- Linux on z/Series is different from every other Linux
 - ▶ Simple cloning will allow to quickly clone hardened Linux
 - ▶ HiperSockets allow for fast, security-rich communication between images
 - ▶ LDAP TDBM and RACF can be used as a back end for Linux authentication

Summary

- There are customer responsibilities
 - ▶ Define & deploy a security policy and awareness program
 - ▶ Examine audit trails periodically
 - ▶ Apply recommended service
 - ▶ Proactively harden and re-harden your systems
 - ▶ Data integrity must be managed by customer

- A full discussion of z/VM security and integrity features can be found in publication GM13-0145
<http://www.ibm.com/servers/eserver/zseries/library/techpapers/gm130145.html>

- Additional information about Linux Security on zSeries can be found in a new whitepaper
<http://www.ibm.com/servers/eserver/zseries/library/techpapers/pdf/gm130488.pdf>

Agenda: Resilience Topics

- Resilience Technologies
- High Availability
 - ▶ Tivoli System Automation for Linux
- Business Resilience
 - ▶ PPRC/XRC
 - ▶ xDR

Availability Topics

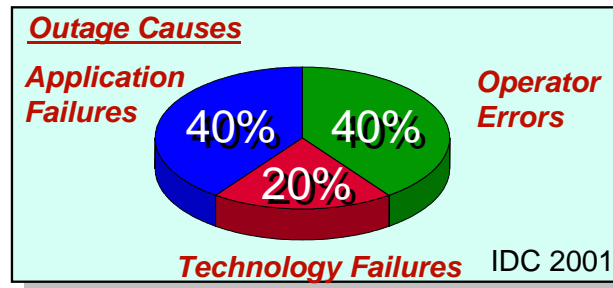
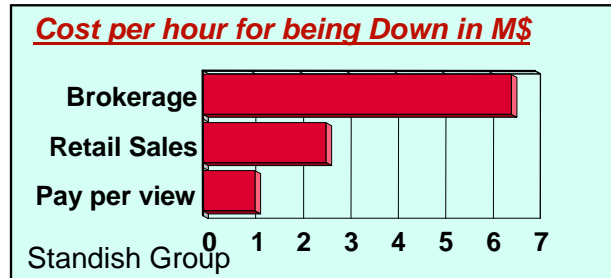
Linux on zSeries

March 2004

***High Availability:
System Automation for Linux***

***Business Continuity:
PPRC/XRC
xDR***

High Availability: Business Issue



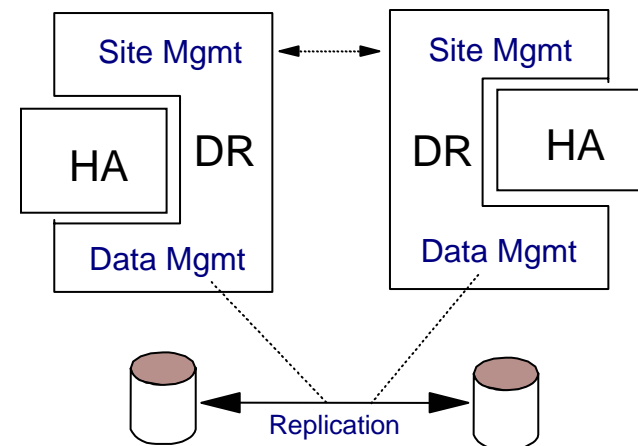
- e-business challenges
 - ▶ Downtime unaffordable
 - ▶ No service window
 - ▶ Is complex to manage

- Customer pressures
 - ▶ Application availability
 - ▶ Increasing complexity and operations costs
 - ▶ Automation implementation and maintenance costs
 - ▶ Education requirements related to automation
 - ▶ Rapid change of I/T infrastructure, new workload

- ▶ **Loss** of business
- ▶ **Loss** of customers – the competition is just a mouse click away
- ▶ **Loss** of creditability, brand image and stock value

Technology Approaches Used for Business Continuity

- “Continuous” Availability (CA)
 - ▶ “Continuous” Operation (addresses planned outages)
 - System, application and network mgmt based on automation technology
 - ▶ High Availability (HA, addresses unplanned outages)
 - Cluster HA
 - Typically one site
 - System, application and network mgmt based on automation technology
 - Availability of data based on shared data access, RAID, local mirroring technology
- Disaster Recovery (DR)
 - ▶ Typically built on top of HA products
 - ▶ At least two dispersed sites
 - Site mgmt based on automation technology
 - Data mgmt with remote mirroring



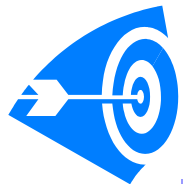
How to achieve High Availability?



- high reliability of each component
 - ▶ quality, RAID, ECC,
 - ▶ ESS & zSeries



- small recovery times
 - ▶ fast boot times
 - ▶ no FS check => journaling FS
 - ▶ Linux (ext3fs, ReiserFS, JFS)



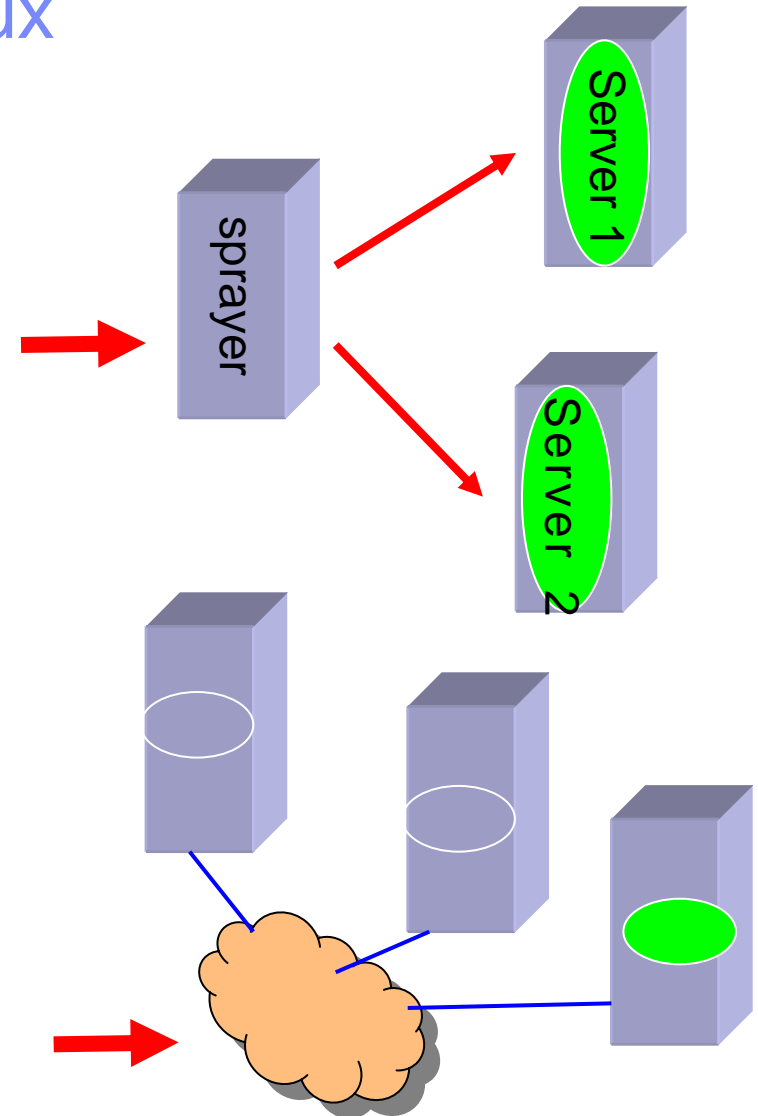
- redundant components
 - ▶ use different copies of a component transparently
 - ▶ avoid single points of failure

- IBM Tivoli System Automation for Linux

High Availability Options for Linux

Options

- ▶ Load Balancing
 - A sprayer intelligently distributes work among available systems
 - Simple services that can be provided by any of multiple instances of a server
 - Linux Virtual Server Project
- ▶ Automated Failover
 - All systems are peers
 - Keep all resources redundant
 - Mutual health monitoring
 - Automation Engine decides where to run which resources
 - Services of arbitrary complexity
 - SA for Linux



System Automation for Linux – A Policy-based HA solution

- IBM's strategic high availability (HA) solution for ~~@platforms~~ running Linux
- System Automation for Linux manages business application availability
 - ▶ “Resource Monitoring”: Fast detection of HW failures and SW failures
 - Processes, IP addresses, file systems, and others...
 - ▶ “Automation”: Quick and consistent recovery of failed resources and/or whole appls
 - Based on a sophisticated knowledge about business applications
- Ease of use: Policy-based HA solution
 - ▶ Describe Requirement in High Level Language
 - ▶ Use concepts similar to administrator thinking - no script programming!
 - ▶ Little effort for
 - complex HA scenarios and
 - Simple scenarios
 - precanned solutions
 - ▶ Flexible: easy to modify requirements
 - ▶ Not error prone

@server Targets

zSeries

- ✓ z/Linux
- ✓ z/OS

*feed back in System Automation for OS/390



xSeries

- ✓ x/Linux



IBM Tivoli
System Automation
for Linux

iSeries

- ✓ i/Linux
- ✓ OS/400

*System Automation for OS/400



BladeCenter

- ✓ x/Linux

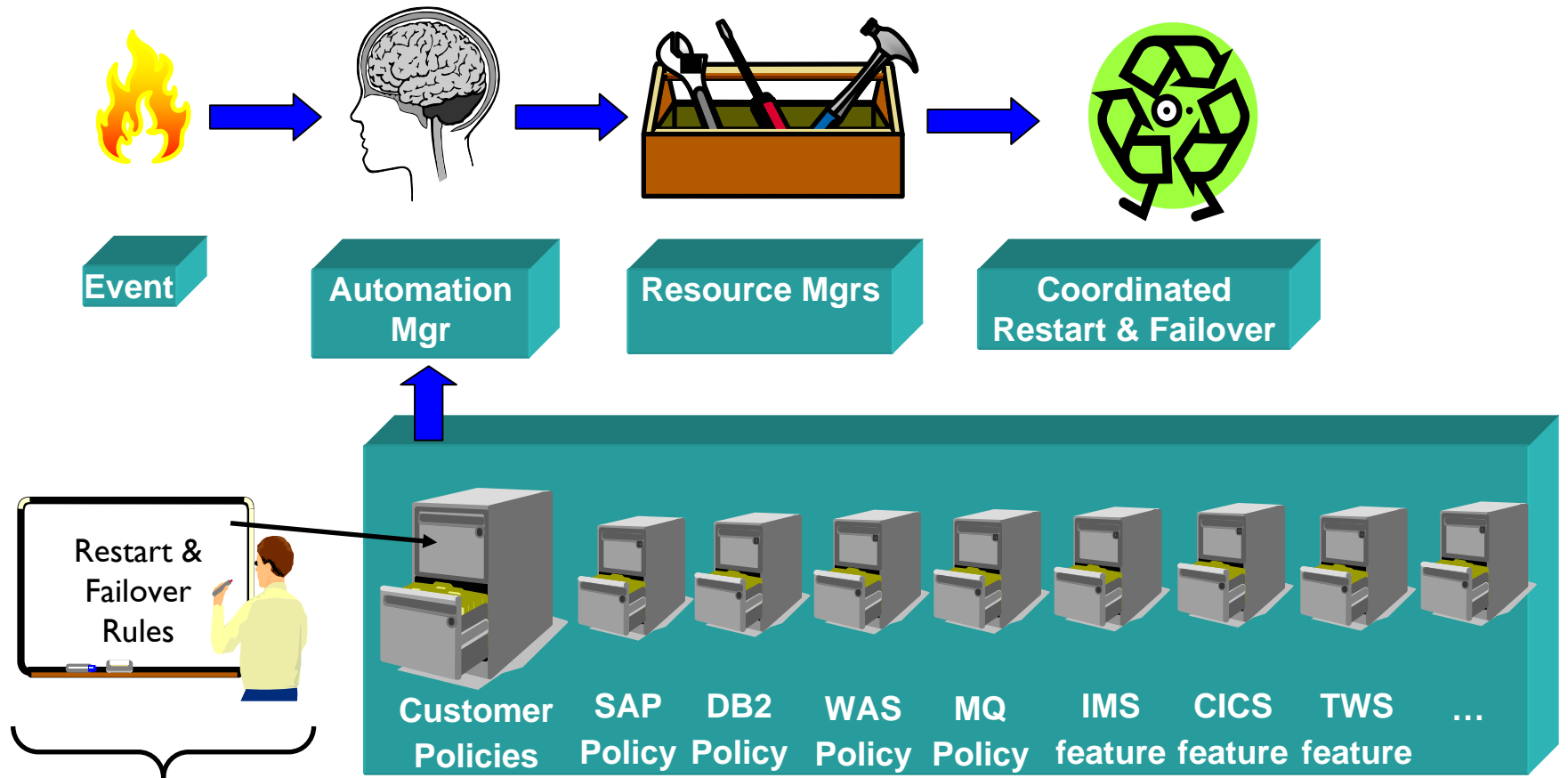


pSeries

- ✓ p/Linux



System Automation: Basic Principles

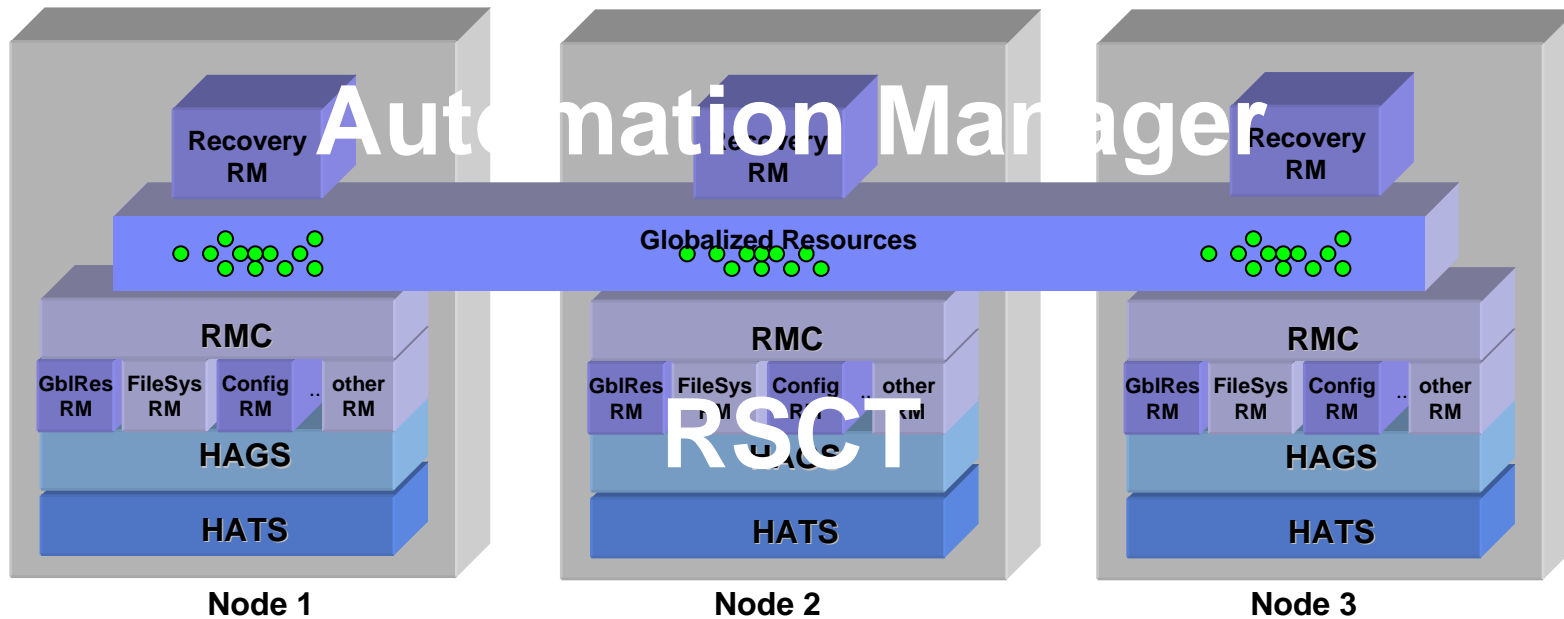


***'Pre-Canned' Scenarios:
out-of-the-box policies and features provided
by System Automation***



Exploits world-class pSeries & zSeries technology:

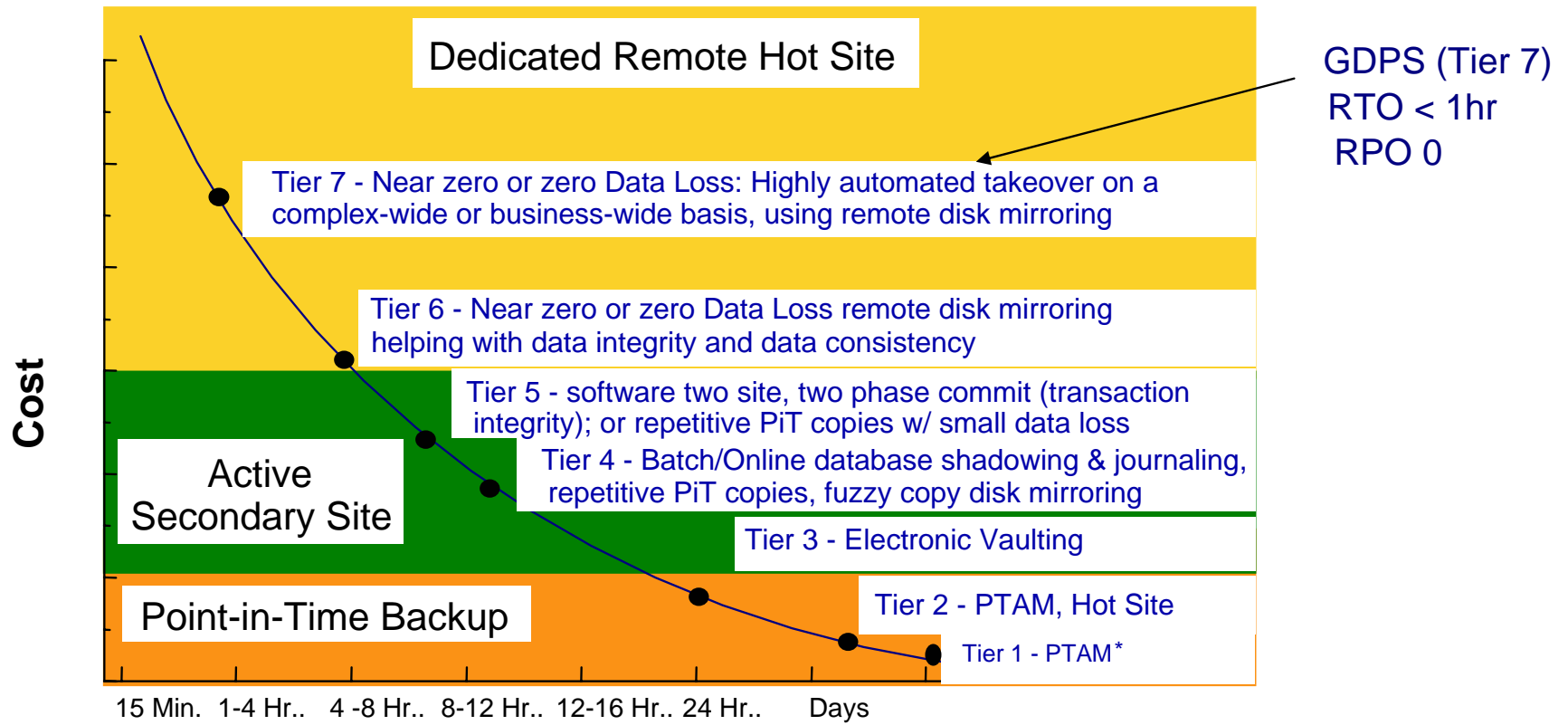
- AIX cluster infrastructure **RSCT (Reliable Scalable Cluster Technology)**
 - ▶ - provides functions like heartbeat, resource monitoring and control, ...
- z/OS' **Automation Manager**
 - ▶ - Expert system (hidden to the user) which drives automation decisions based on an automation policy



IBM Tivoli System Automation and Linux for zSeries

- Customers running zLinux have a high demand for HA
 - ▶ Running mission critical applications on zLinux
 - DB2
 - Websphere
 - SAP
 - ▶ Are used to HA (from z/OS) and expect similar tools on Linux
- SA Linux has strong proximity to z/OS
 - ▶ Leveraging z/OS technology in the Linux space
 - ▶ Coordinate applications running on z/OS and applications on zLinux with the same technology
- Enables Disaster Recovery
 - ▶ Coordinated DR for zLinux, z/OS and z/VM
- Competitors of SA (Lifekeeper, Veritas) not running on Linux for zSeries
- Majority of SA Linux licenses for zSeries Linux

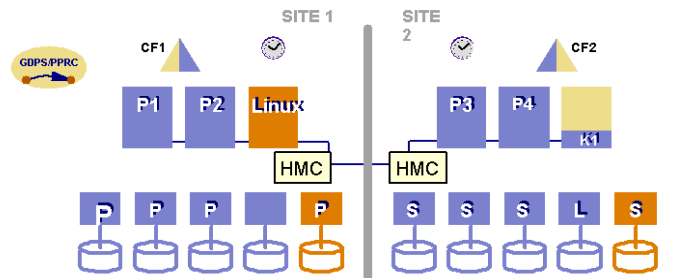
Share Disaster Recovery Tiers



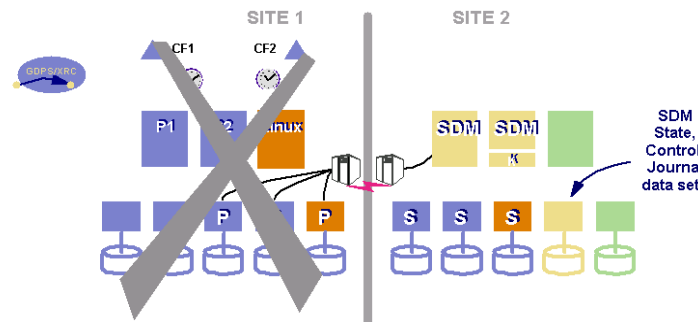
Tiers based on Share Group
*PTAM = Pickup Truck Access Method

zSeries - Tap industry leading business continuity

- Higher Grid infrastructure availability
 - ▶ Flexibility to house or backup critical Grid software Servers and Directories
 - ▶ GDPS Resiliency maintains mission critical data on both Linux and z/OS™ systems
 - ▶ Restarts critical Linux Grid servers in backup configuration
- Minimize downtime of key components
 - ▶ Flexible software maintenance and regression testing platform
 - ▶ Faster maintenance application backouts and/or restarts due to code defects



- Planned and Unplanned reconfigurations
- Unplanned Site Reconfiguration driven by z/OS
 - ▶ Controlling System recovers secondary disks including Linux
 - ▶ Expendable workload stopped
 - ▶ CBU invoked, if applicable
 - ▶ Site 1 production systems restarted including Linux
- GDPS manages PPRC Linux volumes



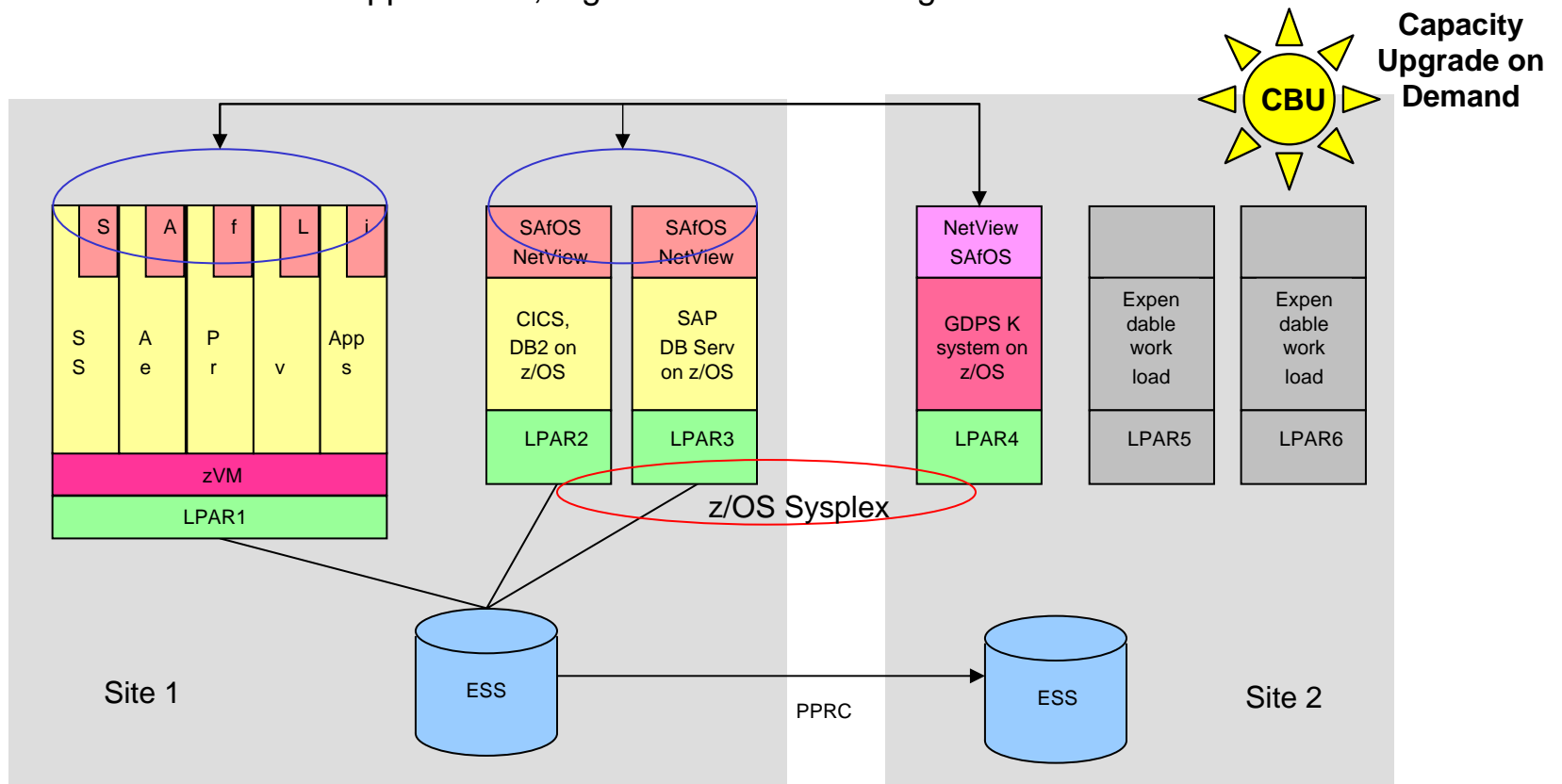
- Unplanned Site Reconfiguration manually initiated by customer
 - ▶ Controlling System recovers secondary disks including Linux
 - ▶ Expendable workload (SDM) stopped
 - ▶ CBU invoked, if applicable
 - ▶ Site 1 production systems restarted including Linux
- GDPS manages XRC Linux volumes
- Linux for zSeries extended to time stamp data
 - ▶ SuSE Linux 8

Cross Platform Disaster Recovery (xDR) Objectives

- Provide near continuous availability for heterogeneous distributed IT business applications
 - ▶ "Recover my business rather than my platform technology"
 - ▶ unplanned outages including disasters
 - ▶ and planned outages
- Provide a common solution for managing multiple platform DR
- Improve recovery time and minimize data loss
- Reduce the total cost of ownership for a two or more site IT topology
- Enable successful recovery with lower skill levels via automated processes

xDR for zSeries Scenarios

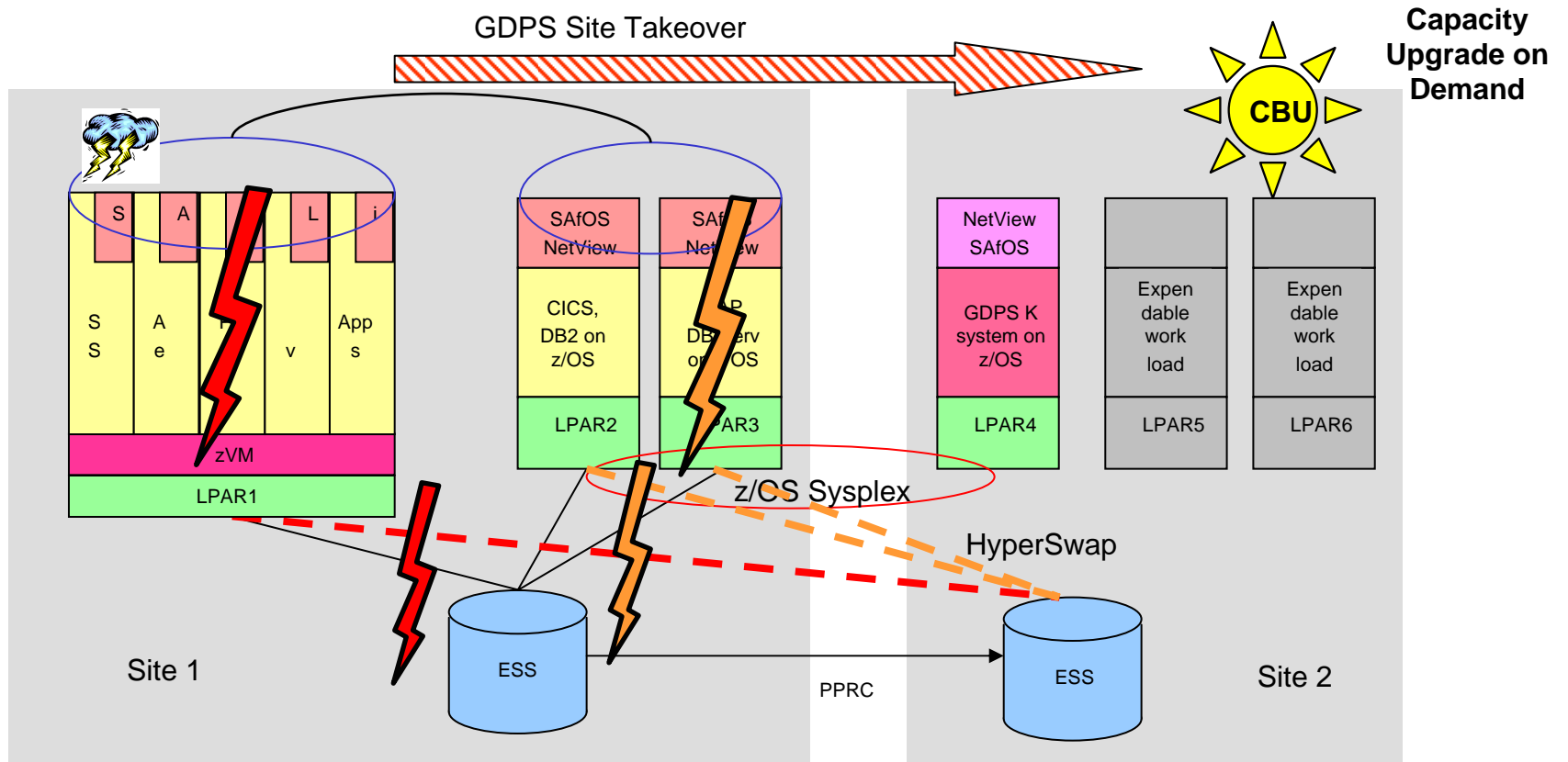
- Examples:
 - ▶ WAS and Portlet servers running on Linux/zSeries under zVM, CICS and DB2 running on z/OS sysplex
 - ▶ SAP application servers running on Linux/zSeries under zVM, SAP DB server running on z/OS
 - ▶ Other Linux/zSeries applications, e.g. mail servers running on Linux/zSeries under zVM



xDR for zSeries Functionality

- GDPS can manage ESS for any platform (z & open)
- GDPS: planned site takeover (IPL OS, reconfig DASD)
- GDPS: unplanned site takeover or re-ipl in place triggered by z/OS

- zSeries DR: unplanned coordinated site failover (or re-ipl in place) triggered by Linux for zSeries
- zSeries DR: planned coordinated HyperSwap
- zSeries DR: unplanned coordinated HyperSwap or site takeover triggered by Linux for zSeries



xDR for zSeries Customer Value

- Industrial Strength DR Solution for Linux for zSeries based on GDPS
 - ▶ Enables lower skilled operators to perform DR if specialists unavailable
 - ▶ Pretested DR solution with highest probability of success
 - ▶ End game: near continuous availability (hyperswap) even in DR case

- High customer value for coordinated Linux for zSeries – z/OS DR
 - ▶ Coordinated HyperSwap
 - E.g. because storage subsystems are used by both, Linux for zSeries and z/OS
 - ▶ Coordinated site takeover
 - ▶ Planned and unplanned support

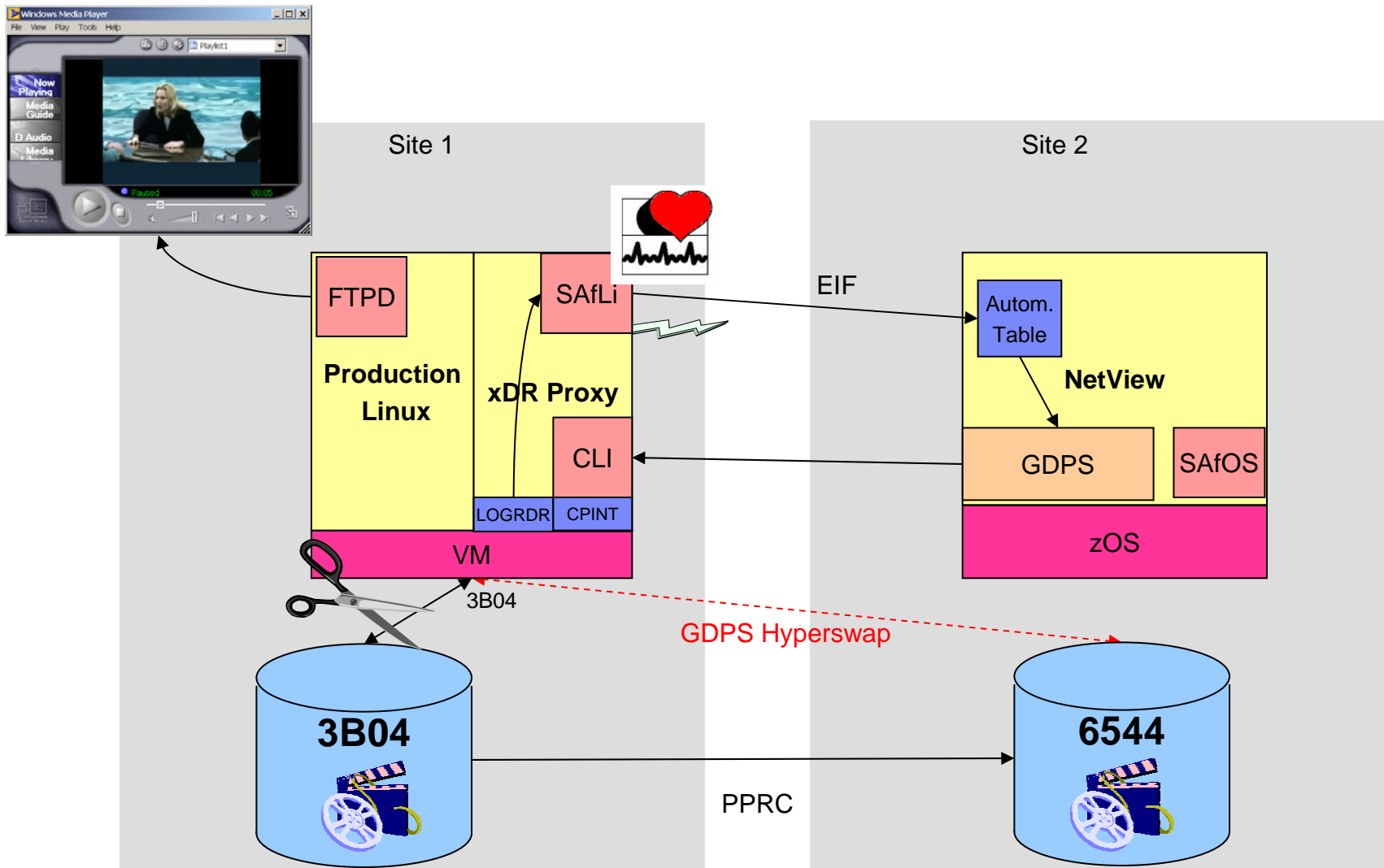
- DR augments the benefits for Server Consolidation on Linux for zSeries

- Fast time to market
 - ▶ Limited Availability 2Q 2004
 - Joint customer study with 3 European customers
 - ▶ GA 9 / 2004

xDR for zSeries Availability Outlook

- xDR for zSeries is not a separate product
- xDR for zSeries consists of the following parts:
 - ▶ Linux for zSeries
 - SuSE SLES 8 refresh
 - Availability date 4 / 2004
 - ▶ zVM
 - V5R1
 - GA 9 / 2004
 - ▶ SAfLi R2
 - Runs on SuSE SLES 8
 - GA 4 / 2004
 - ▶ Service offering GDPS 3.1
 - SPE with xDR for zSeries 9 / 2004

CeBIT Demo: Unplanned Hyperswap Scenario



Demo Setup Overview

The screenshot displays a Windows desktop environment with the following components:

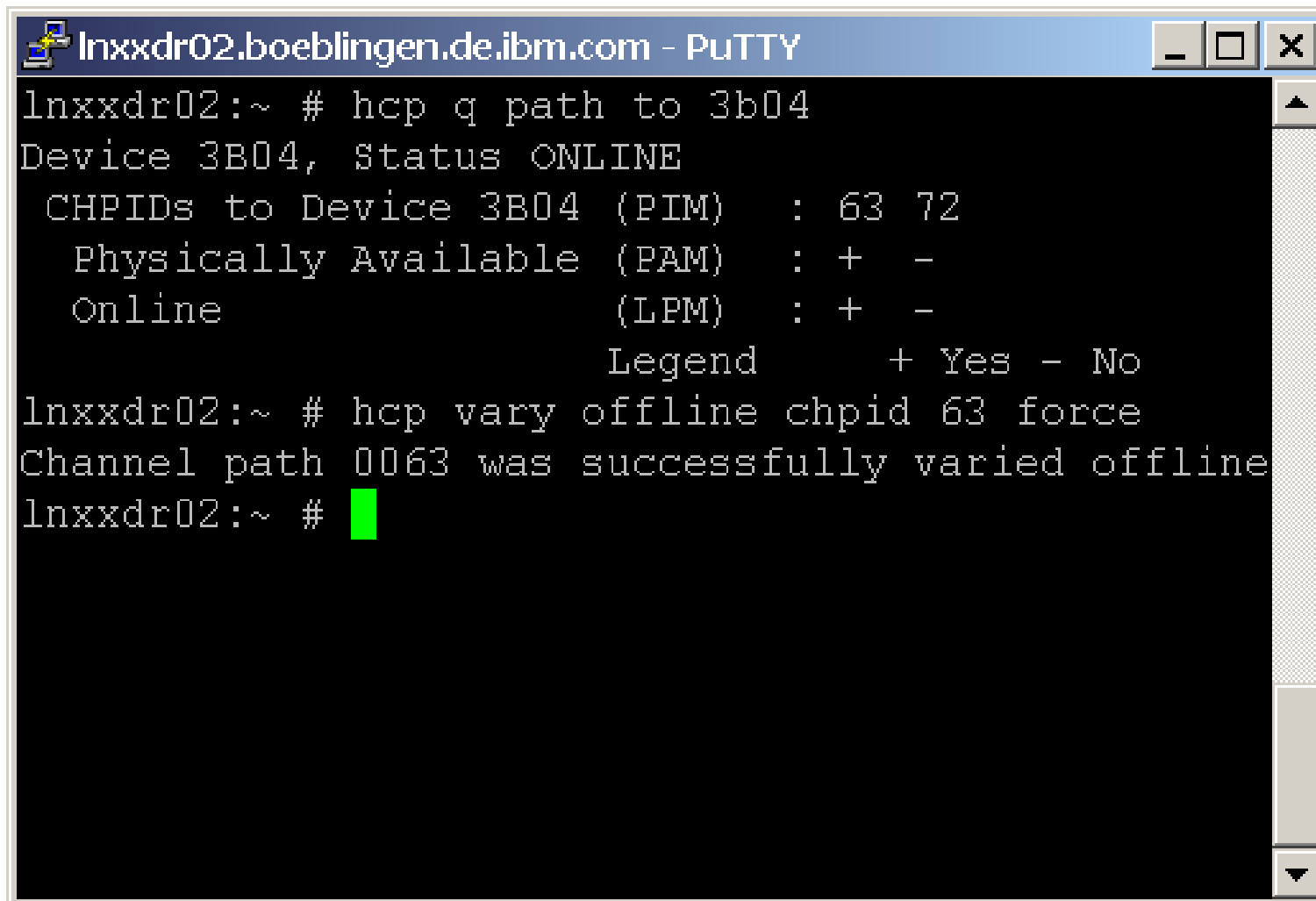
- Windows Media Player:** Located in the top-left, showing a video player interface with a 'Paused' status and a 00:33 timer. An arrow labeled 'Media Player' points to it.
- NetView:** A window in the top-right displaying a list of network heartbeat messages. An arrow labeled 'Netview' points to it.
- Production Linux:** A terminal window in the bottom-left showing the output of a command: 's, 7043 MB', '3b04 (ECKD) at (94: 8)', 's, 7043 MB', and 'Setup completed'. An arrow labeled 'Production Linux' points to it.
- xDR Proxy:** A terminal window in the bottom-middle showing a shell prompt 'lnxxdr02:~ #'. An arrow labeled 'xDR Proxy' points to it.
- Console:** A large terminal window in the bottom-right displaying detailed system logs with columns for time, cylinder, and subchannel. An arrow labeled 'Console' points to it.

DISK 3B04 is mapped to real DASD 3B04

Console

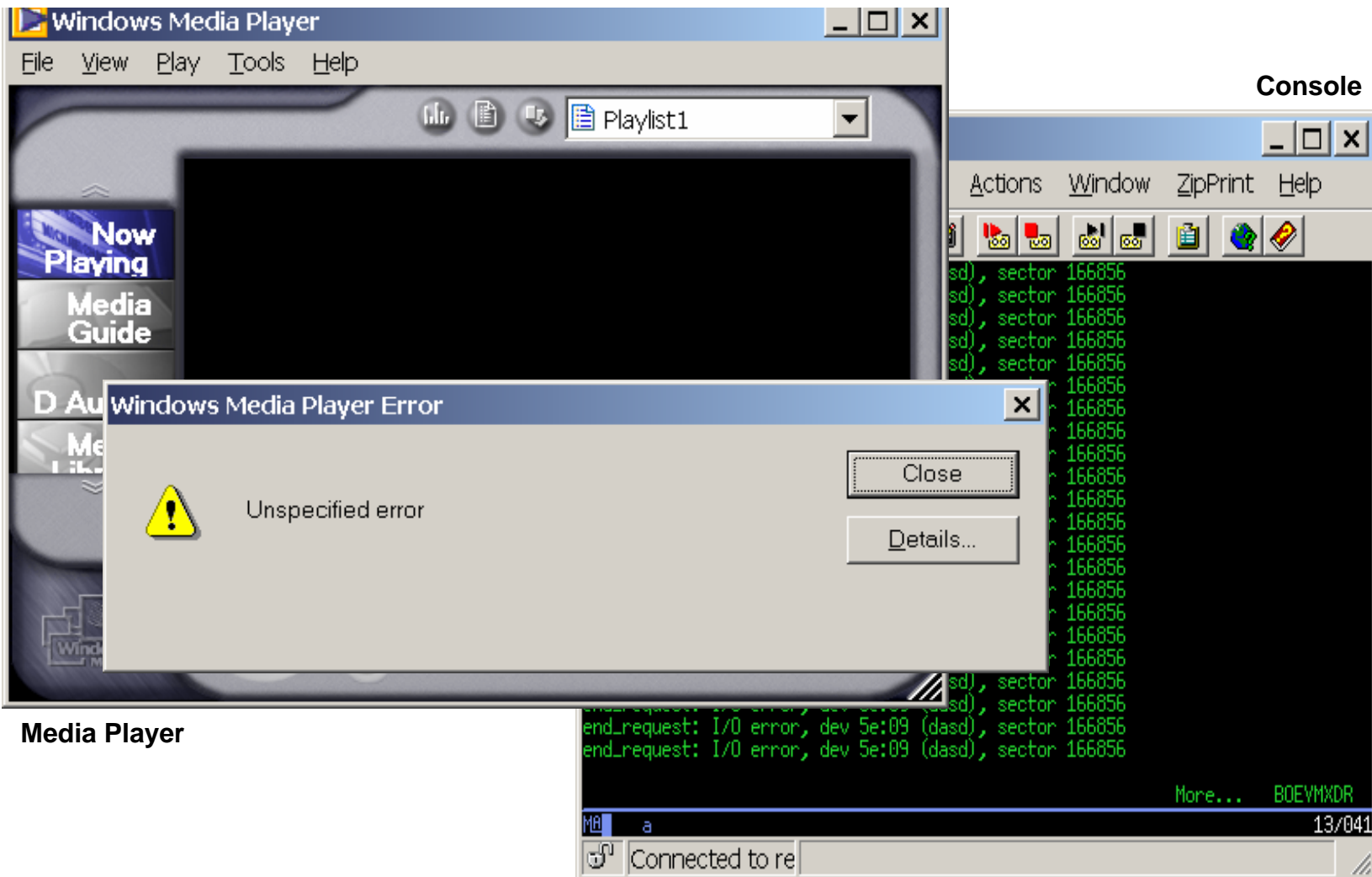
```
Session A - [24 x 80]
File Edit View Communication Actions Window ZipPrint Help
DASD 3B04 ON DASD 3B04 R/W 0X3B04 SUBCHANNEL = 0006
CP Q V DA
DASD 0190 3390 XDR44R R/O          107 CYL ON DASD 14B0 SUBCHANNEL = 000B
DASD 0191 3390 VM14B8 R/W           50 CYL ON DASD 14B8 SUBCHANNEL = 0003
DASD 0192 3390 VM14B8 R/W           700 CYL ON DASD 14B8 SUBCHANNEL = 0004
DASD 0193 3390 XDR019 R/W          10017 CYL ON DASD 5245 SUBCHANNEL = 0005
DASD 019D 3390 XDR44R R/O           120 CYL ON DASD 14B0 SUBCHANNEL = 000C
DASD 019E 3390 XDR44R R/O           250 CYL ON DASD 14B0 SUBCHANNEL = 000D
DASD 0592 3390 XDR44W R/O            67 CYL ON DASD 14B1 SUBCHANNEL = 000E
DASD 3B04 ON DASD 3B04 R/W 0X3B04 SUBCHANNEL = 0006
Running BOEVMXDR
MA a 13/041
Connected to re
```

„Cut“ links by varying CHPIDs offline



```
Inxxdr02.boeblingen.de.ibm.com - PuTTY
Inxxdr02:~ # hcp q path to 3b04
Device 3B04, Status ONLINE
  CHPIDs to Device 3B04 (PIM)   : 63 72
  Physically Available (PAM)   : + -
  Online (LPM)                  : + -
                                Legend   + Yes - No
Inxxdr02:~ # hcp vary offline chpid 63 force
Channel path 0063 was successfully varied offline
Inxxdr02:~ # █
```

Without xDR: A lot of I/O errors, the movie fails



Media Player

With xDR enabled: HyperSwap

1. DASD error detected,
EIF event sent

2. EIF Event received,
HyperSwap issued

Proxy

```
Inxxdr02.boeblingen.de.ibm.com - PuTTY
0
lnxxdr02:~ # hcp vary offline chpid 63 force
Sending EIF event class XDR_EVENT_ERP_DASD:
=====
0:TRIGGER=IOS107I
1:DEVNUM=3B04
2:REASON=
3:IP=9.152.82.22
4:VERSION=1
=====
Channel path 0063 was successfully varied offline
lnxxdr02:~ #
```

Netview/GDPS

```
Session B - [24 x 80]
File Edit View Communication Actions Window Help
NetView Y5R1 IPWFL - XD Tivoli NetView IPWFL BUMU 01/23/04 13:58:59 A
C IPWFL Heartbeat von: lnxxdr01
C IPWFL Heartbeat von: lnxxdr01
C IPWFL DASD Failure !!! Will do hyperswap
' IPWFL
```


HyperSwap done, movie continues playing without error

Console

```
dasd: /proc/dasd/devices: 'add 3B04'
dasd: device range 3b04-3b04: device 3b04 is already in a range.

CP Q V DA
DASD 0190 3390 XDR44R R/O      107 CYL ON DASD 14B0 SUBCHANNEL = 000B
DASD 0191 3390 VM14B8 R/W       50 CYL ON DASD 14B8 SUBCHANNEL = 0003
DASD 0192 3390 VM14B8 R/W       700 CYL ON DASD 14B8 SUBCHANNEL = 0004
DASD 0193 3390 XDR019 R/W     10017 CYL ON DASD 5245 SUBCHANNEL = 0005
DASD 019D 3390 XDR44R R/O      120 CYL ON DASD 14B0 SUBCHANNEL = 000C
DASD 019E 3390 XDR44R R/O       250 CYL ON DASD 14B0 SUBCHANNEL = 000D
DASD 0592 3390 XDR44W R/O        67 CYL ON DASD 14B1 SUBCHANNEL = 000E
DASD 3B04 ON DASD 6544 R/W 0X3B04 SUBCHANNEL = 0006

Running BOEVMXDR
23/001
```

Disk 3B04 is
mapped to 6544

Back-up: Tivoli Security Products

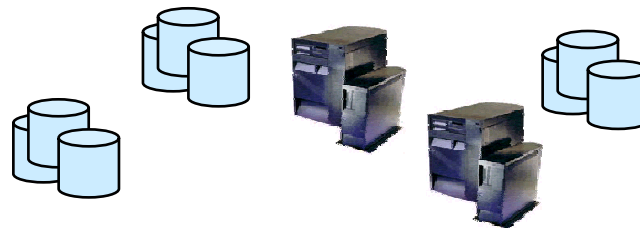
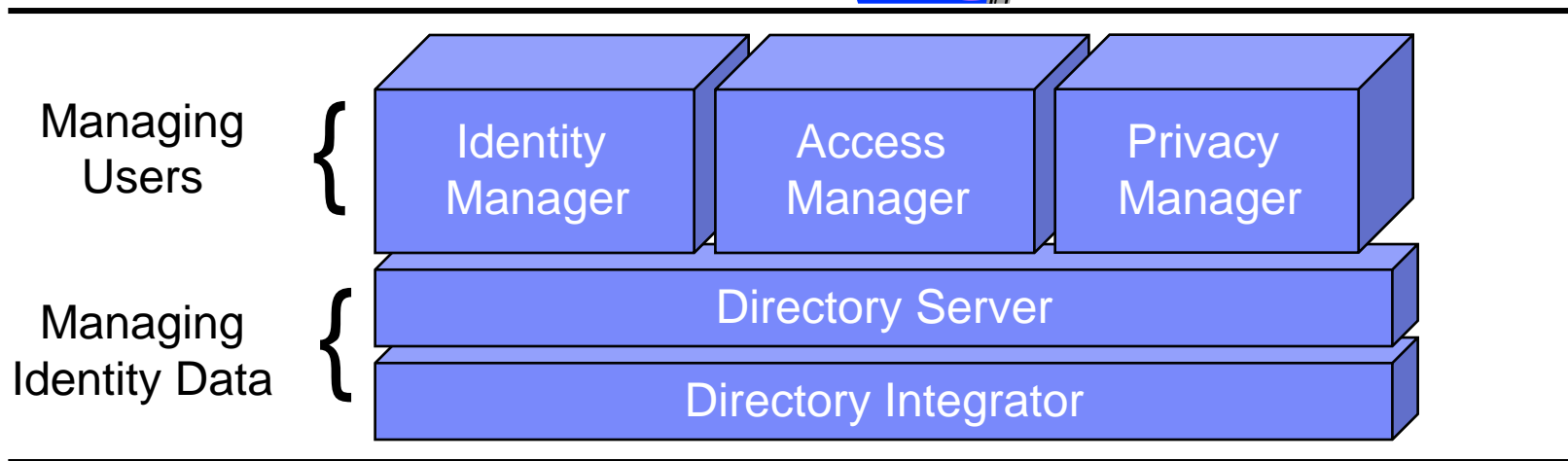
Agenda

TIM	➤ Enterprise Identity Management and User Provisioning
TAMeb	
TAMOS	
TAMBI	
TPM	
TDS	
TDI	
TRM	
TSCM	

IBM's Integrated Identity Management Solution



Users & Applications

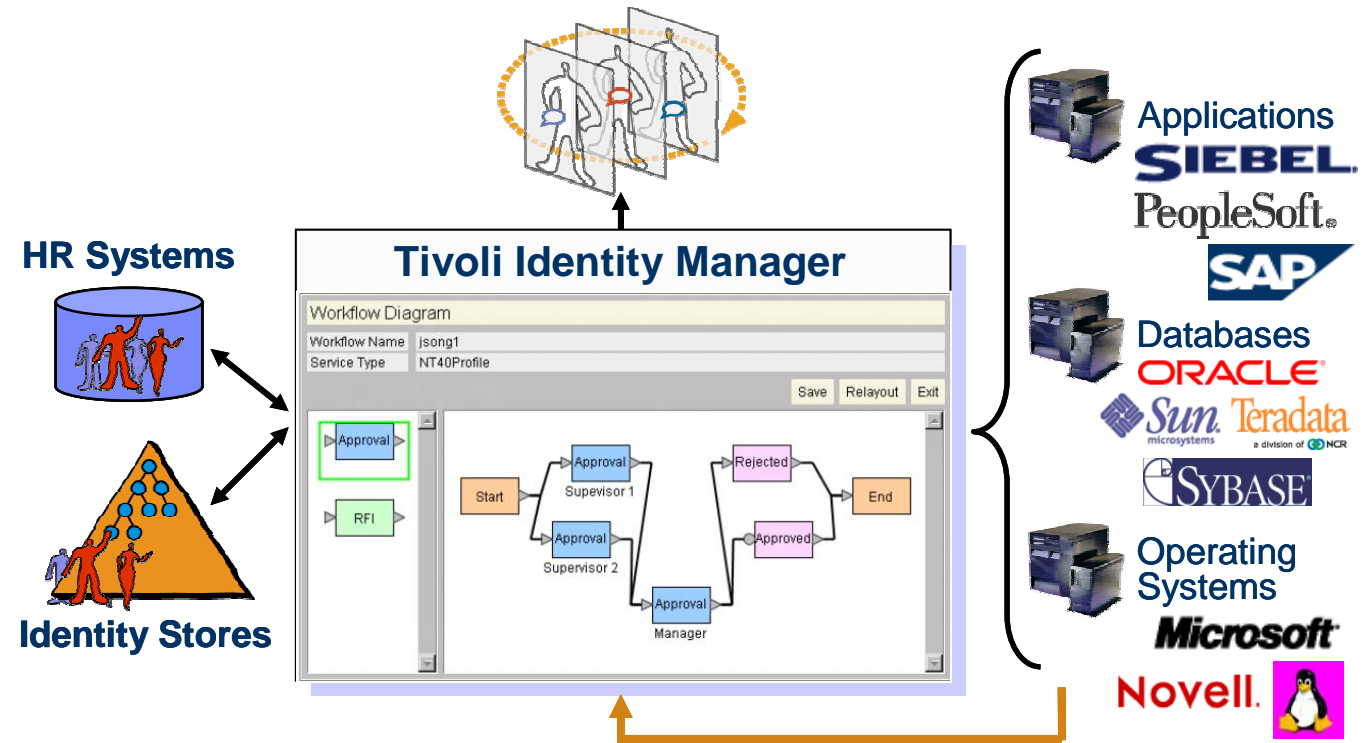
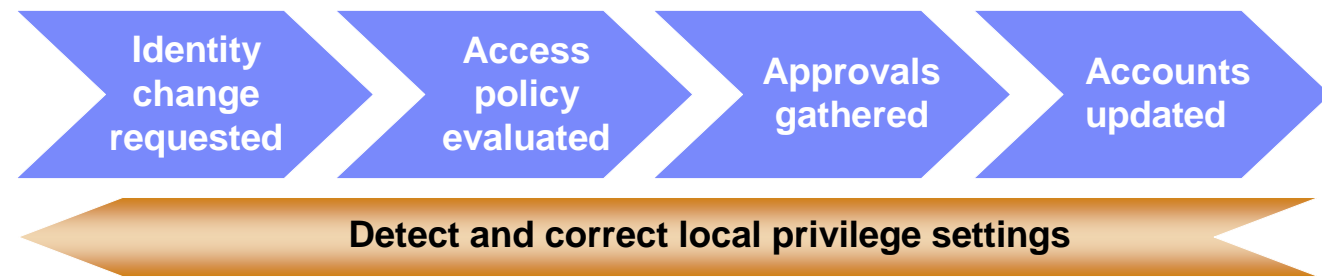


Systems & Resource Information

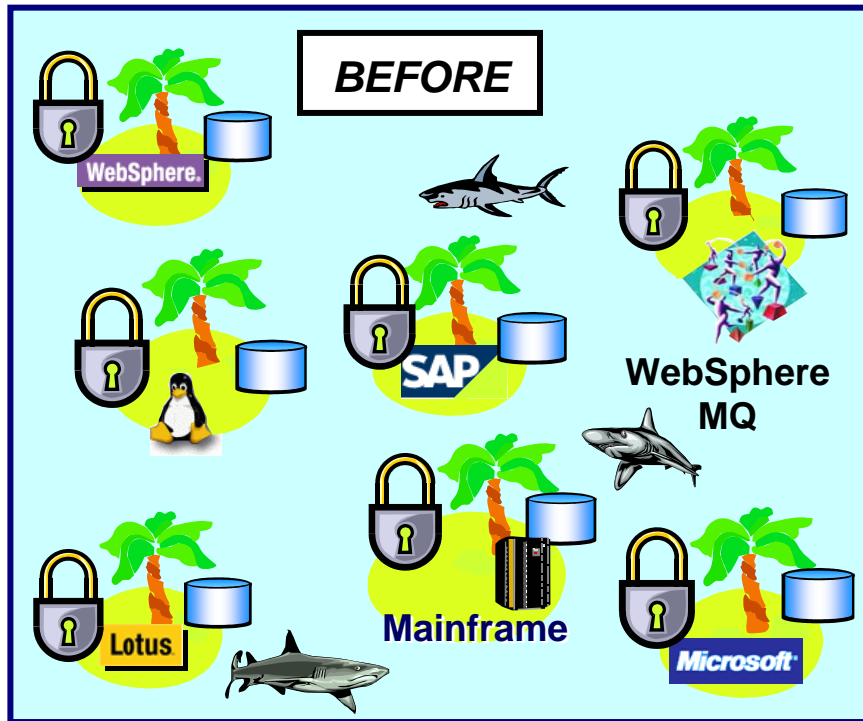
www.ibm.com/software/tivoli/solutions/security/

Tivoli Identity Manager

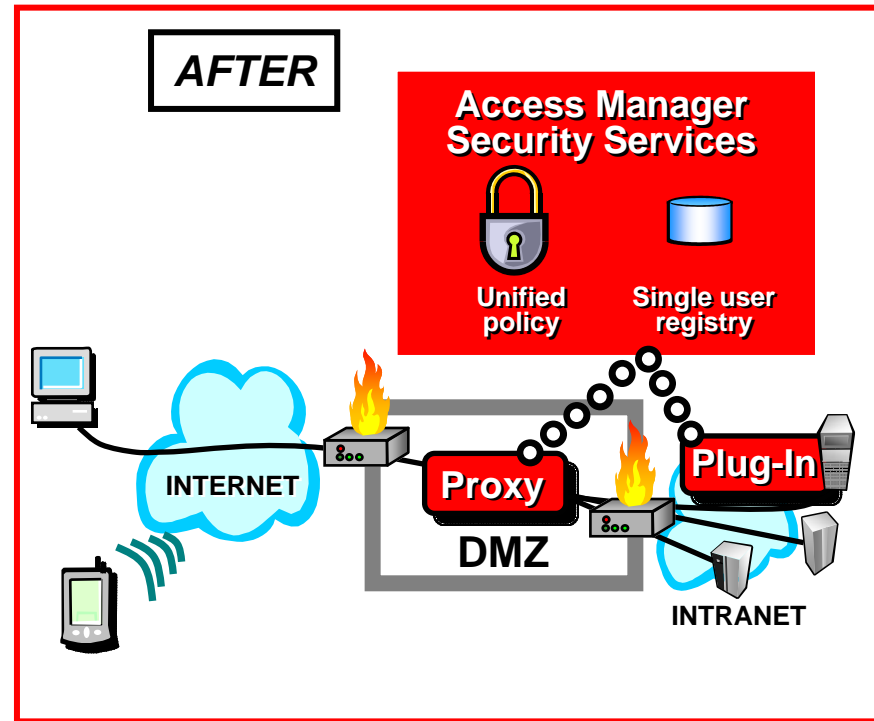
Identity	Access	Privacy
Directory		
Directory Integration		



Customers Want TAMEb's Integrated Approach



- Too many passwords to remember
- Multiple admins w/ too many admin tools
- Tools don't work together
- User & access control info everywhere
- Security as an appl. developer task



- Web single sign-on
- Unified admin
- Unified approach
- User & security info centralized/clear
- Secure HTML & SOAP transactions

What is Access Manager for Operating Systems?

AMOS is a “firewall” for applications and the operating system

- Addresses the #1 security threat

- Provides mainframe-class security

- Provides centralized auditing and recording

Powerful performance results in

- Ability to audit without degrading performance or impacting applications

- Ability to run AMOS even during system back up

- Centralized policy management for greater security

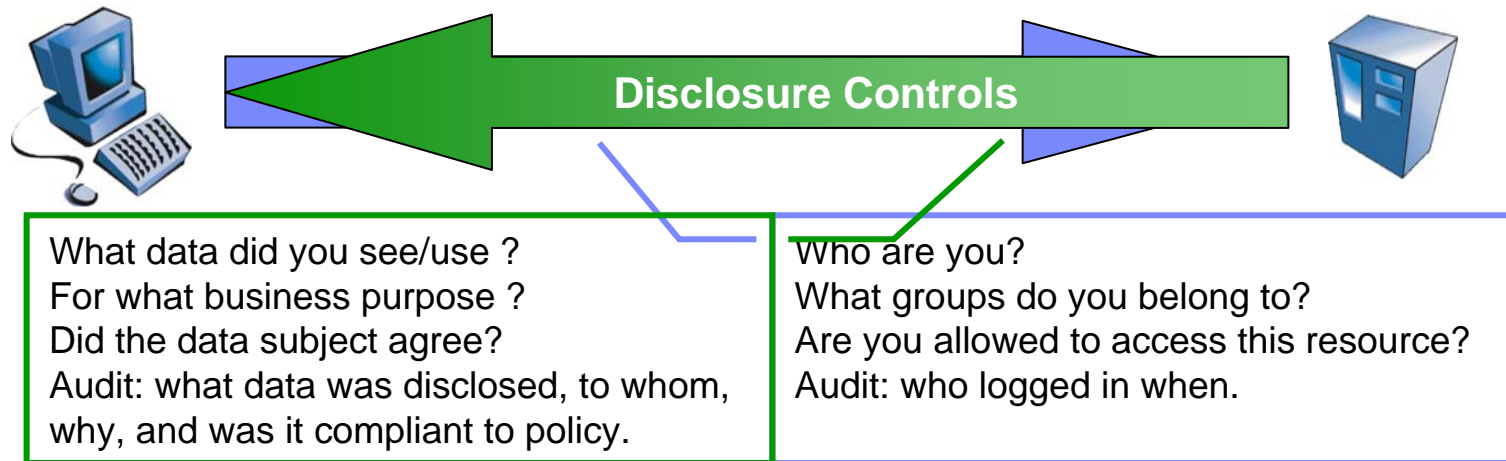
Recent enhancements have made AMOS

- Easier to configure

- Better for auditing

- More secure

How Is Privacy Management Different?



- Disclosure Control

While a user may be authorized to log in to an application, they may not be able to see certain data.

You can apply policy to a data set *BEFORE* it is returned to the application (and the user).

Audit the “return path for data”

IBM Tivoli Privacy Manager for e-business

IBM's tool for externalizing, managing and auditing privacy rules, based on OECD Guidelines 

- **Where it fits**

Wherever application tasks are calling out data requests for sensitive information

Applications can abstract their data protection and privacy logic to Privacy Manager.

- **What it does**

Centralise privacy rules.

Create a flexible system so rules can easily be modified and enforced.

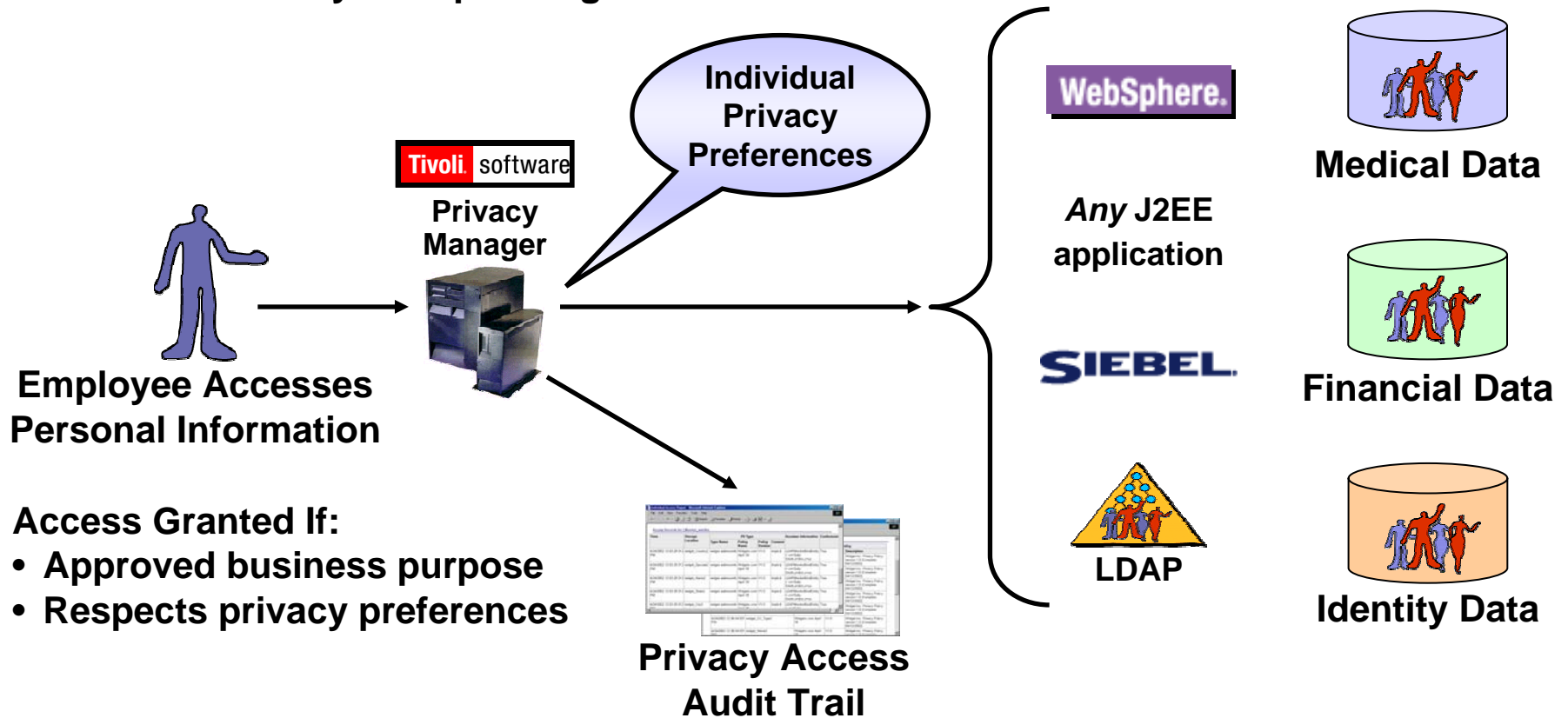
Friendly, natural language interface for policy authorship.

Audit trails demonstrating compliance to policy

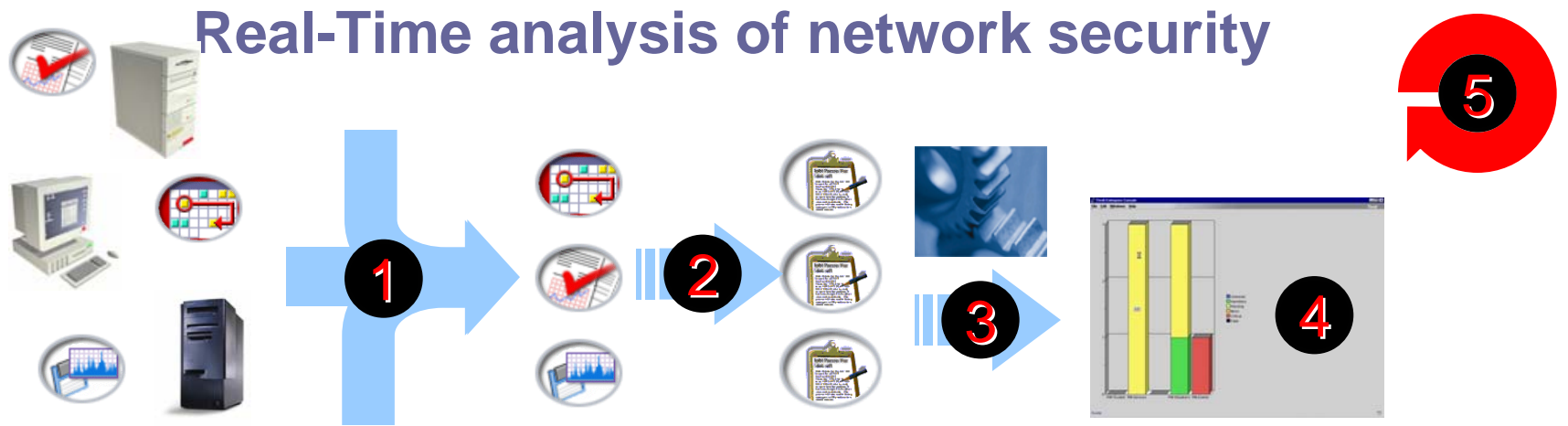
Version history of policies.

Tivoli Privacy Manager

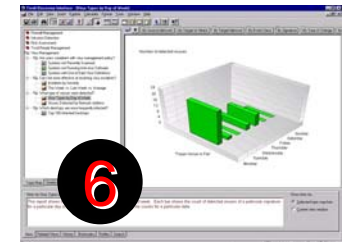
- Add privacy controls to new and existing applications
- Demonstrate compliance to privacy policy
- Increase trust by incorporating consent



Risk Manager: Major Functions



- 1 : Centralization of the security events
- 2 : Standardization of the events
- 3 : Correlation for incident detection and prioritization
- 4 : Real-time display of the network security status
- 5 : Automatic reactions and management for incidents
- 6 : Reporting and forensic capabilities



What we do



- **Look for anomalies**
 - **Viruses**
 - **Hacker break-ins**
 - **Denial of service attacks**
 - **Unusual audit log items**
 - **Unusual activities**
 - **Anything suspicious**

1) Centralize all the alerts coming from multiple sources

2) Analyze these alerts in order to:

Correlate related events issued by multiple sources.

Eliminate false alarms and redundancies.

Gather all the alerts produced by a single attack.

3) In the aim of:

Displaying a single alert per « real » intrusion detected.

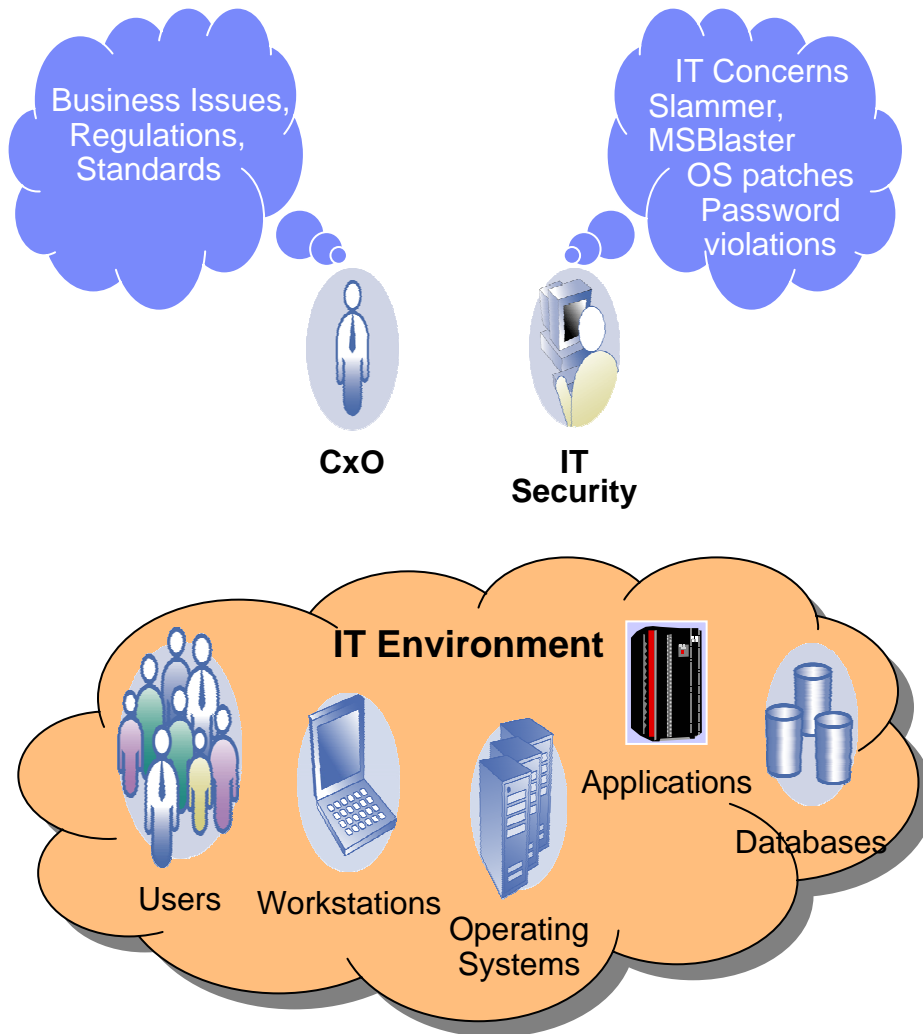
Detecting intrusions previously hardly detectable.

Allowing quicker detection and more effective response.

Simplifying the edition of audit and security reports.



Introducing Security Compliance Manager



- IBM Tivoli Security Compliance Manager is a security policy compliance product that checks systems and applications for vulnerabilities and identifies violations against security policies

Key benefits to our customers:

- Helps to secure corporate data and integrity
- Identifies software security vulnerabilities
- Helps decrease IT costs through automation, centralization, and separation of duties
- Assists in complying with legislative and governmental standards

Security Target Defined

Security Target (ST)

- A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation.
- The security target specifies
 - The Target of Evaluation (TOE)
 - the security objectives
 - the threats to those objectives
 - any specific security mechanisms that will be employed.
 - Assurance level sought, e.g EAL2, EAL3+, EAL4
 - Strength of security function claim – SOF Basic, Medium, High

Back-up: Security Certifications

Conclusion: “Letter of the Law vs. Spirit”

Letter

- Certificate that is issued is “valid” for the **instantiation of** or exact configuration evaluated. (Now is this practical? No!)

Spirit

- SLES 8 is CC certified for Intel, 390, PPC and Opteron
- If the same SLES 8 software runs on x335 and x440, and you tested on x335, “it’s good for x440”

All vendors face the same problem.

- It is not economically feasible to test on every hardware model