Centralised Enterprise Security and Audit

Unique qualities of System z that make it an ideal choice as Enterprise Security Server

PulseANZ 2010

Meet the people who can help advance your infrastructure

Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

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

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance 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 or performance improvements equivalent to the ratios stated here.

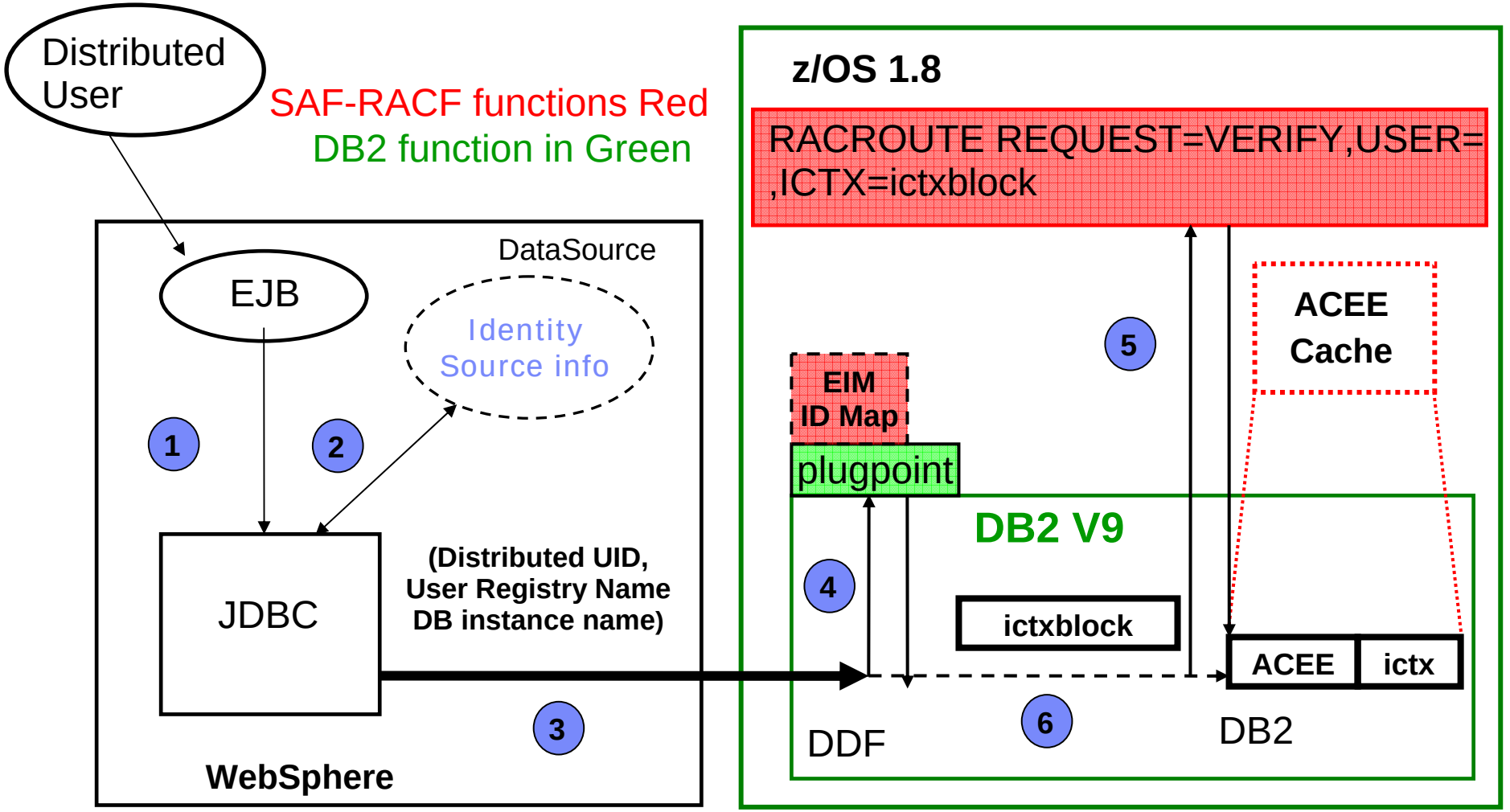
Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

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

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

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.

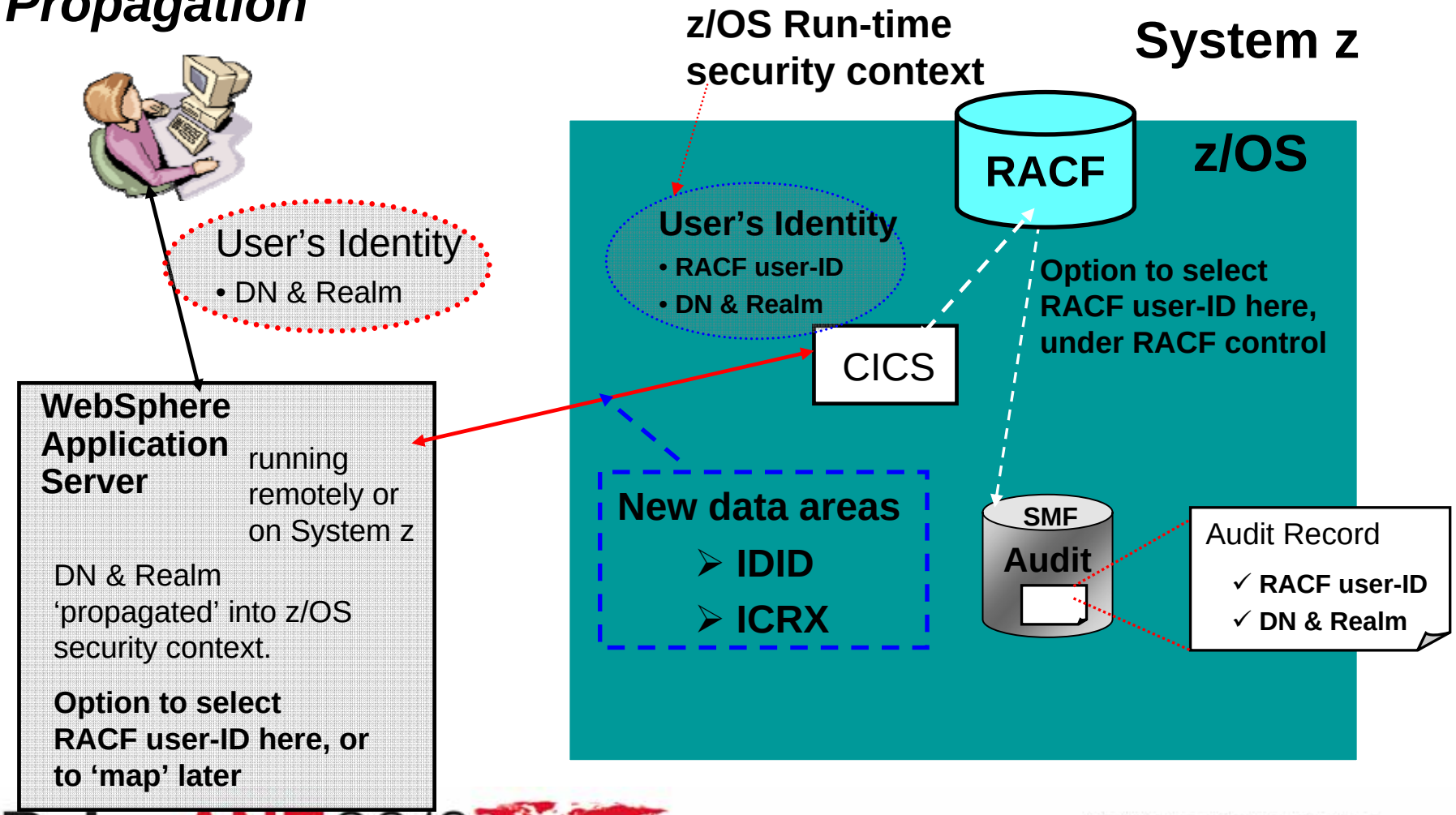
SAF Identity Propagation… DB2 V9 and z/OS 1.8



z/OS Local security context is tailored with the distributed identity

z/OS V1R11: z/OS Identity Propagation

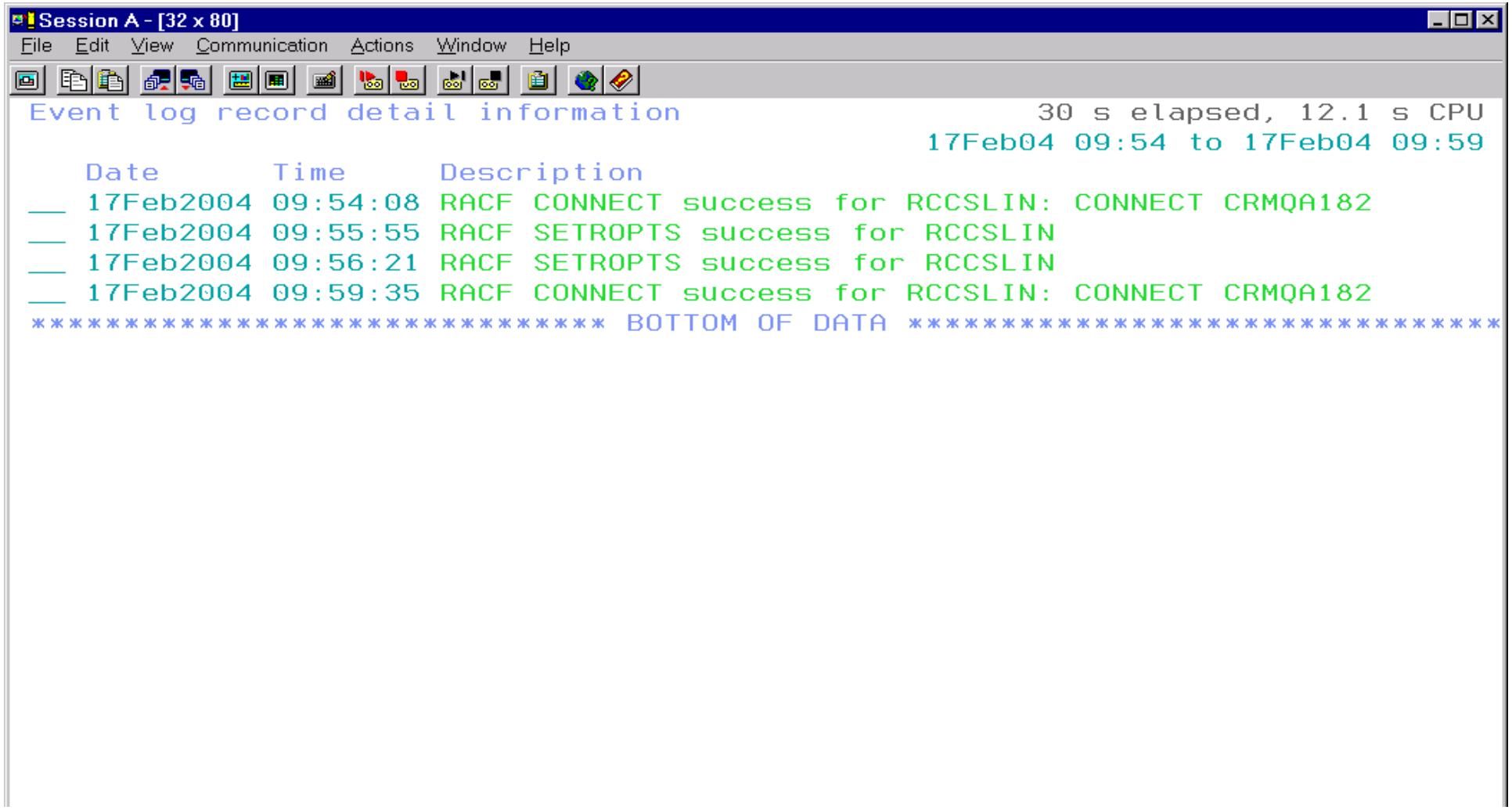
With z/OS Identity Propagation



zSecure Audit

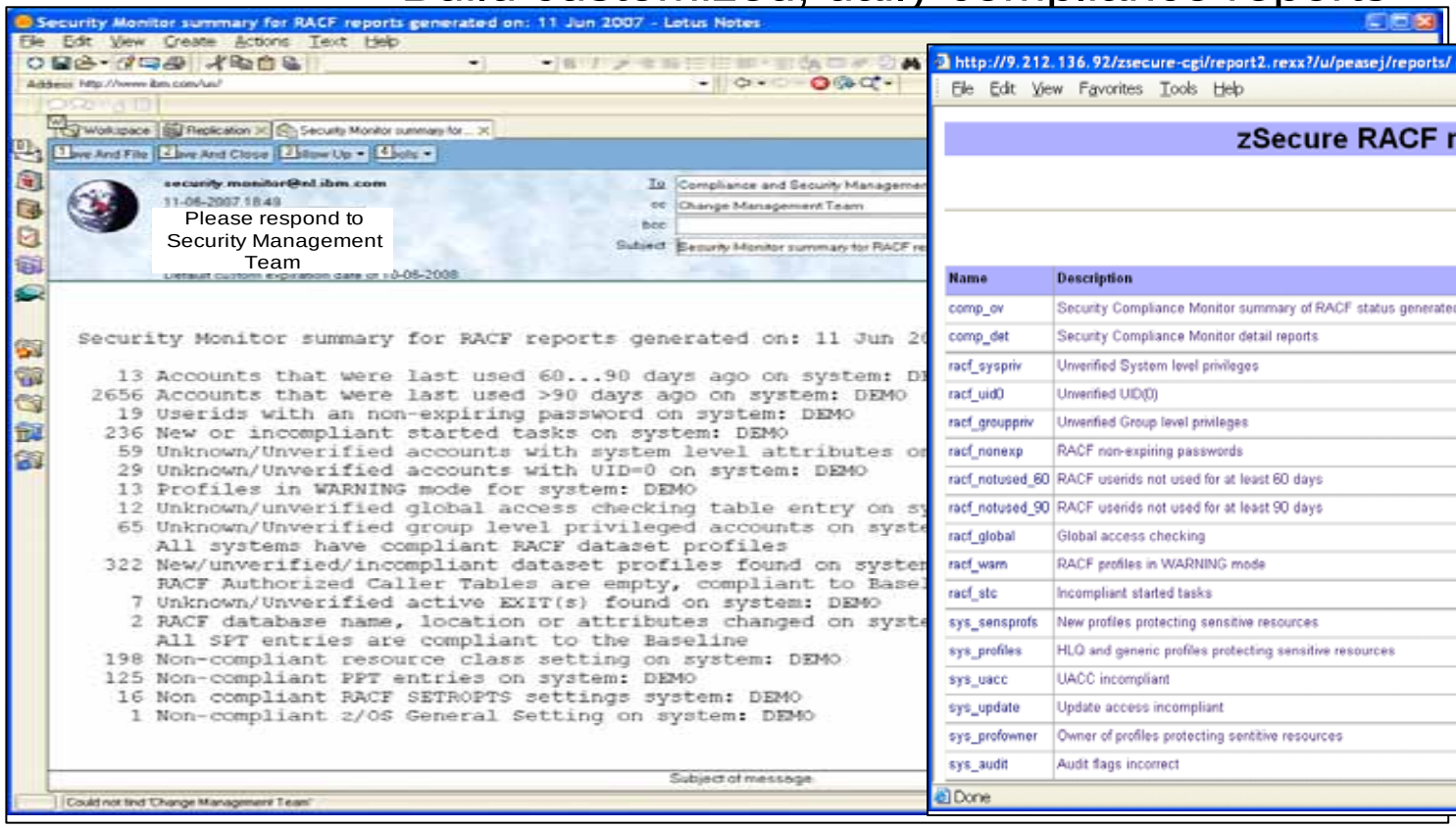
```
 BROWSE - CRMAROB.CNRACF1.SDEMO.REPORT -------------- LINE 00000000 COL 001 080
******************************** Top of Data *********************************
S M F   R E C O R D   L I S T I N G   20Jul05 07:30 to 28Jul05 07:00
System utilities

Program  User     Jobname  Count
ATBINITM                     387
         STRTASK  APPC         386
         SYSOPER  APPC           1
BPXINIT                      384
         OMVS     OMVS         384
CNLSSDT                      384
         STRTASK  MMS          384
CSVLLCRE                     384
         STRTASK  LLA          384
DFHSIP                       309
         DEMOROB  CICS23         1
         STRTASK  CICS23       308
ERBMFMFC                     387
         STRTASK  RMF          386
         SYSOPER  RMF            1
ERB3GMFC                     392
         STRTASK  RMFGAT       391
         SYSOPER  RMFGAT         1
EZBREINI                     387
         DEMOROB  RESOLVER       1
         OMVS     RESOLVER     386
EZBTCPIP                     392
         DEMOROB  TCPIP          1
         TCPIP    TCPIP        391
HASJES20                     393
 COMMAND ===>                                   SCROLL ===> CSR
```

zSecure Audit



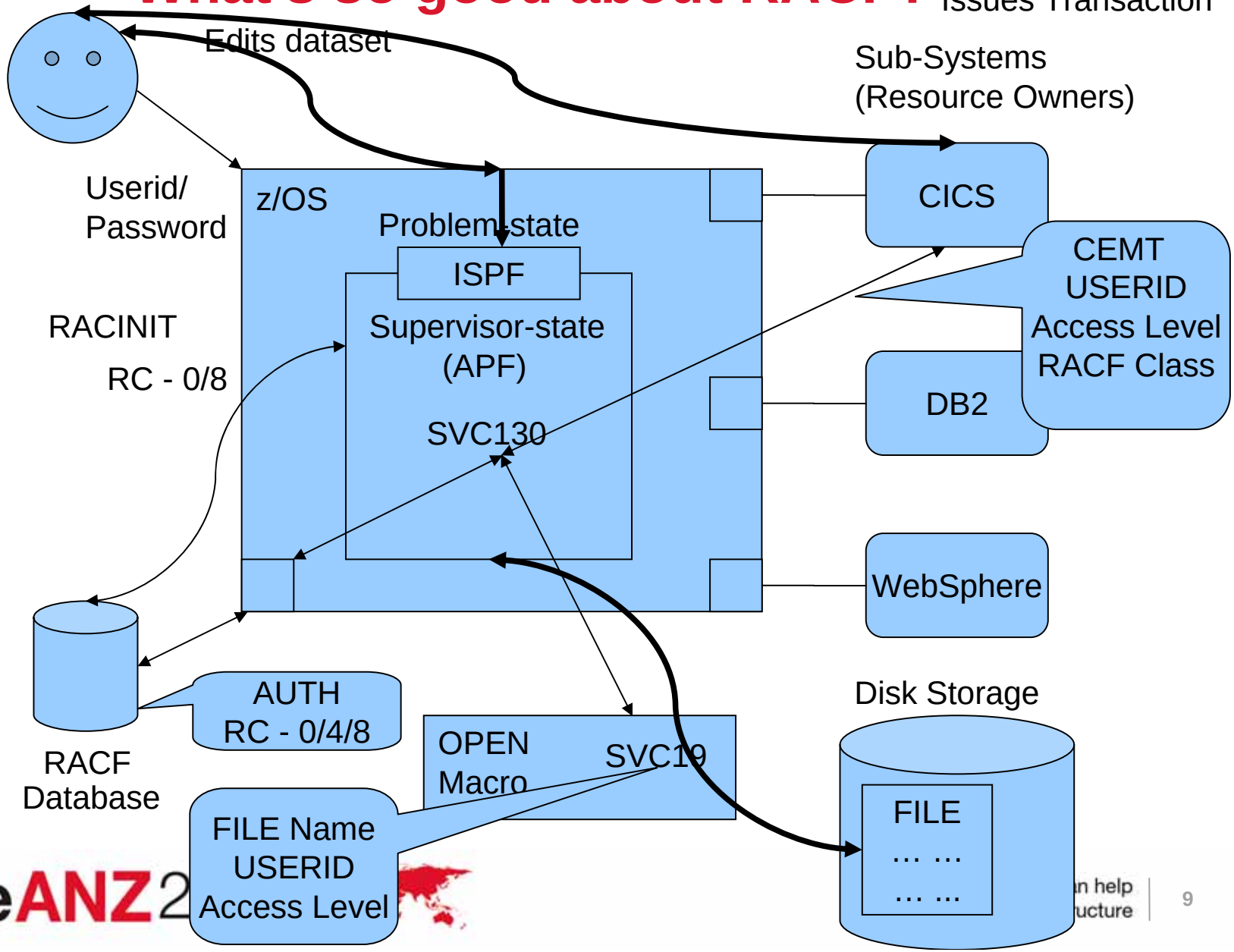
zSecure Audit Advanced

- Analyze, summarize, apply thresholds
  - ISPF, batch, email, flat file, XML
- Customize, automation
  - Input sources, selection, output
  - Build customized, daily compliance reports



What's so good about RACF?

What's so good about RACF?

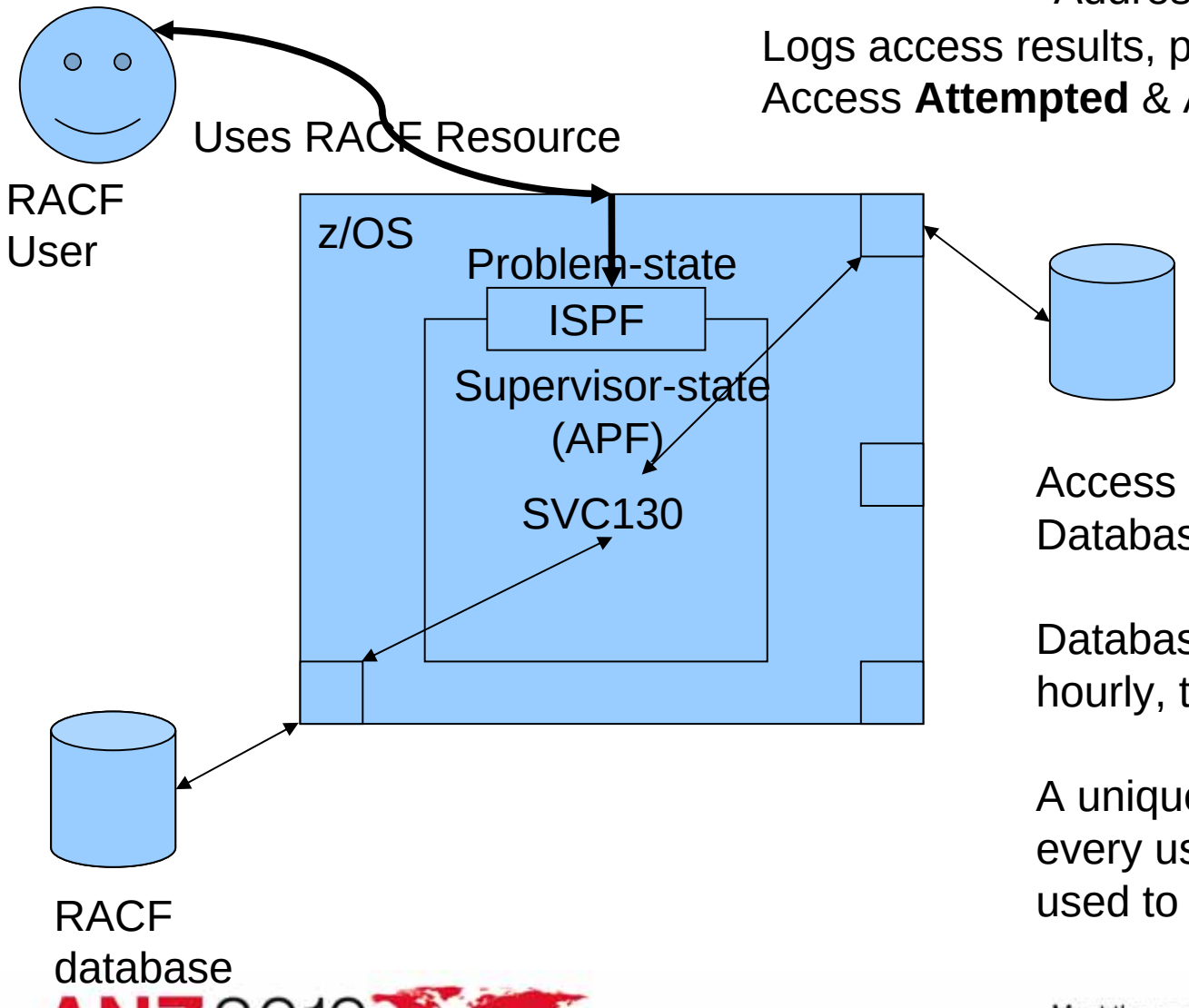


RACF Access Monitor

RACF Access Monitor Address space

Logs access results, path taken

Access **Attempted** & Access **Allowed**

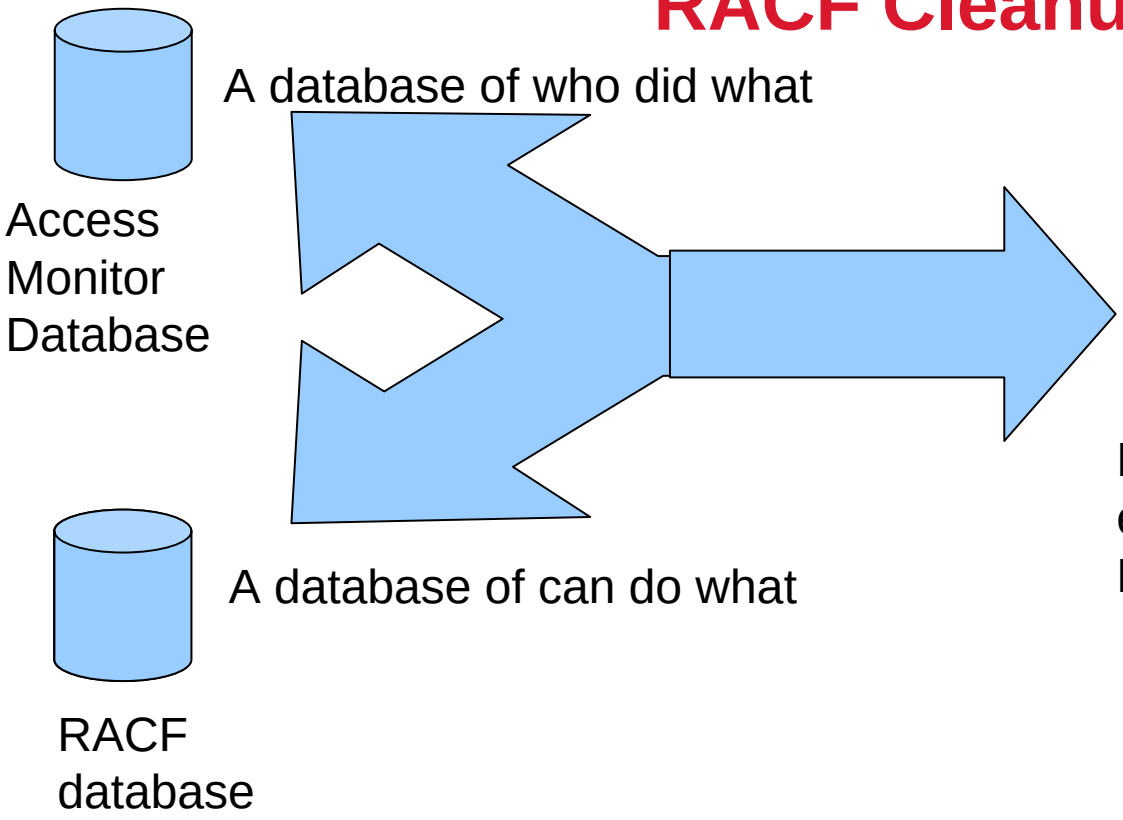


Access Monitor Database

Database consolidated hourly, then daily etc.

A unique record of every users access used to every resource.

RACF Cleanup



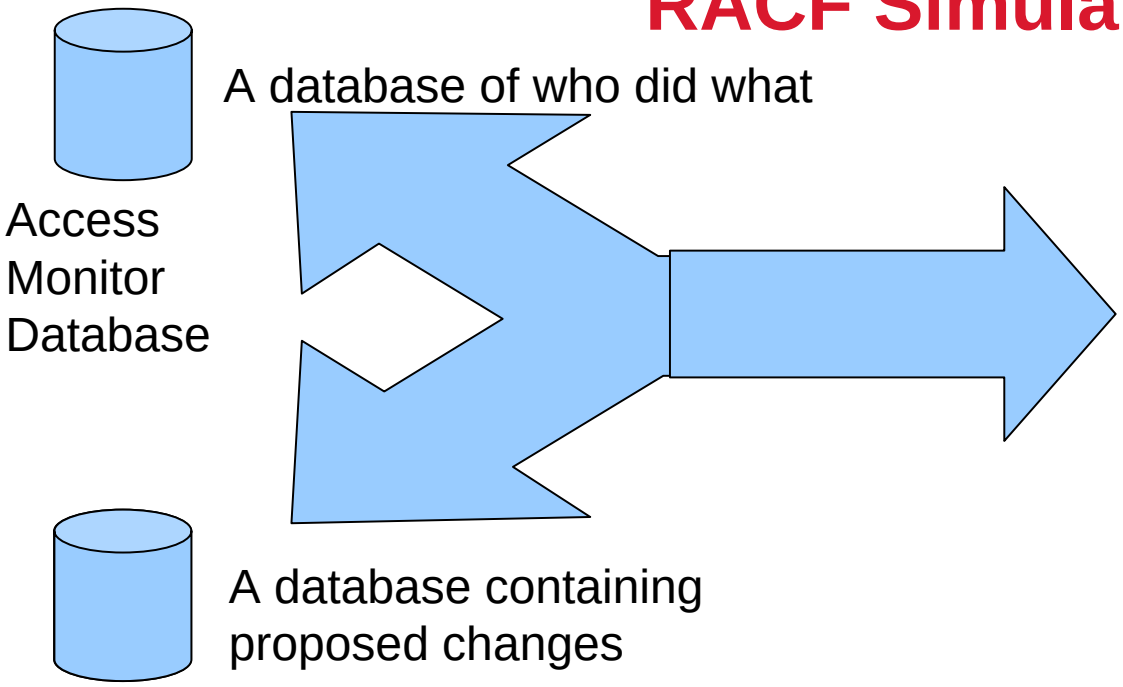
Reports of users who possess higher access than they used.

RACF commands to reduce access to the minimal level used

Reduce privileges to only those exercised – IT Security 101 – Principle of Least Privilege nirvana

But wait, there's more!

RACF Simulate

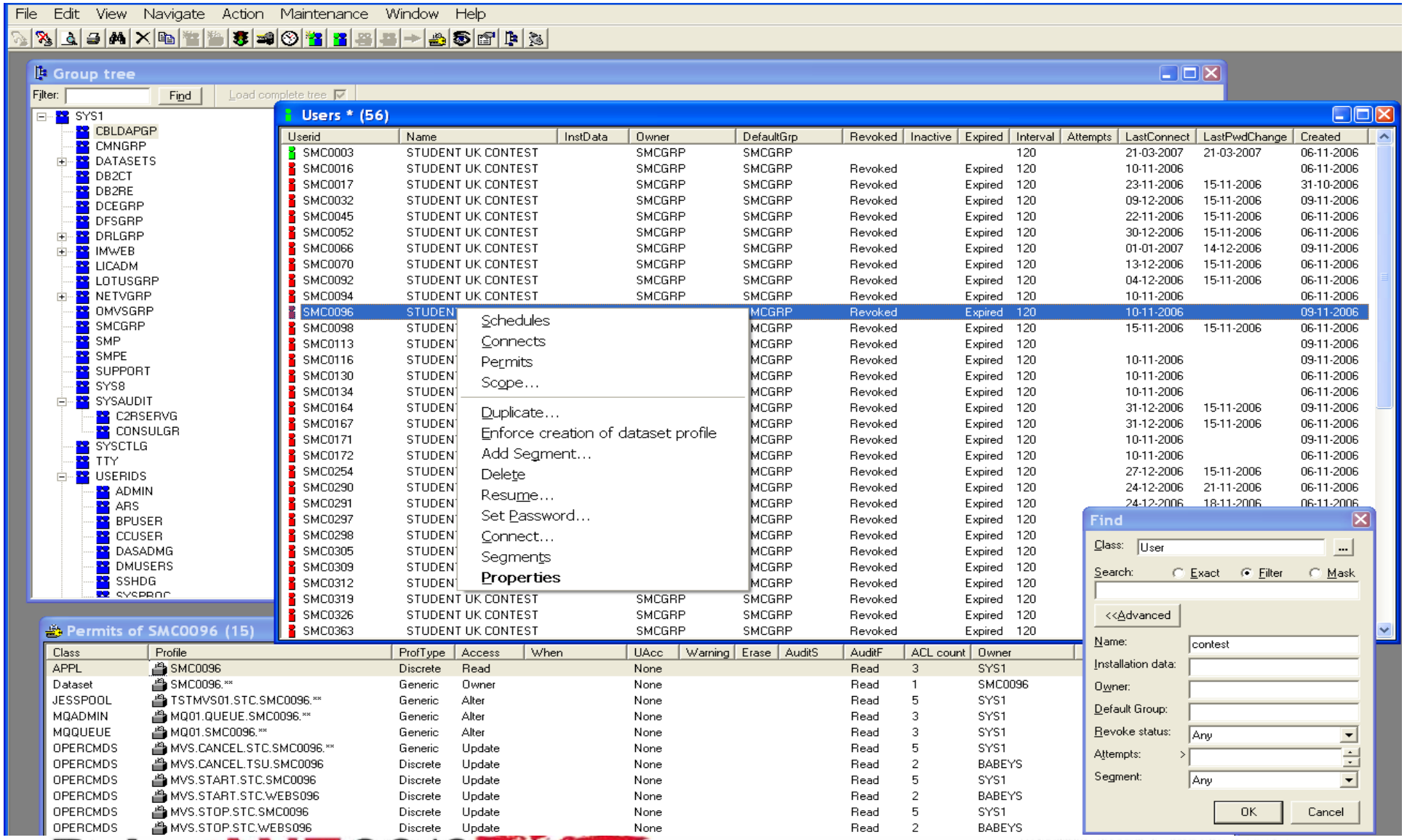


Reports of users whose access would change – i.e. fail where previously they succeeded.

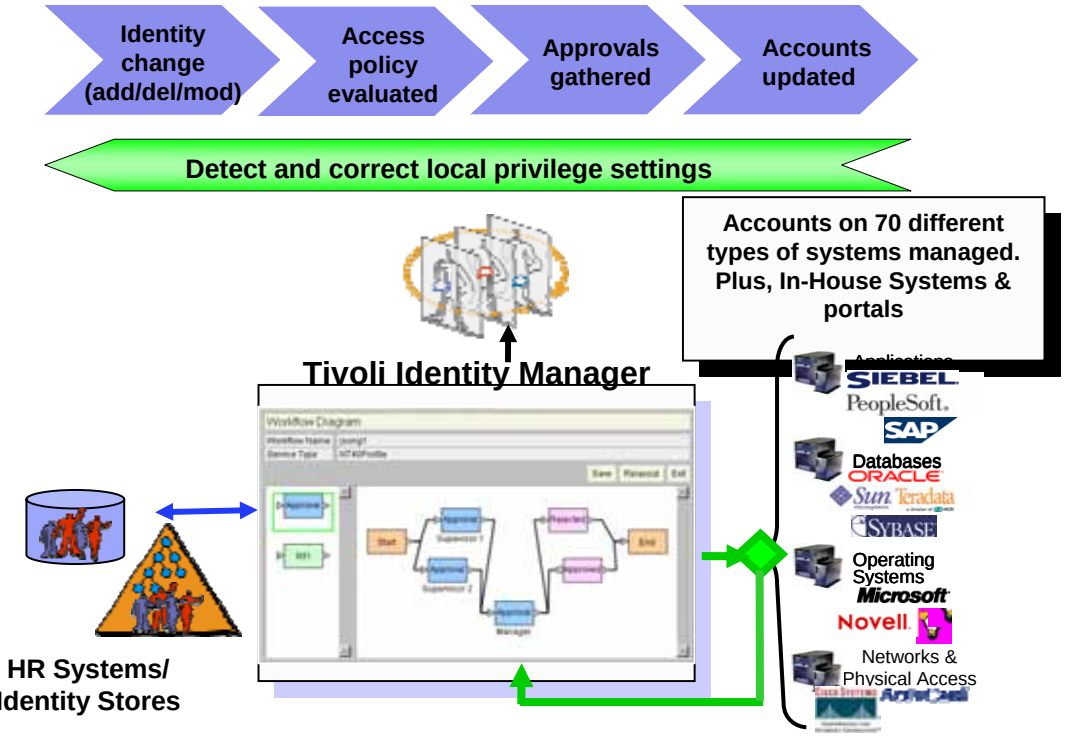
True access testing – unheard of in any IT security paradigm. Security nirvana? Not yet...

Later, we will look at the logs

Easy to Administer?



Tivoli Identity Manager (TIM)



- Know the ***people*** behind the accounts and ***why*** they have the access they do
- Fix non-compliant accounts
- Automate user privileges lifecycle across entire IT infrastructure
- Match your workflow processes

Visibility

See your business

…ify Complexity

- …ess-relevant view of …ity
- …s rights audit & reports

Control

Govern your assets

…ess Compliance

- …arding & …ification workflows
- Closed-loop provisioning

Automation

Build agility into Operations

…ce Costs

- …ervice password …
- …nated user …ioning & de-provisioning

Complete Single Sign-On—Tivoli Unified SSO

Internet

Extranet

Intranet/Kiosk

TFIM

TAMeb

TAM E-SSO
Web Workplace

Web Services

Federated

SOA

Web SSO Targets

Web Servers

Web Applications

Portals, e.g. WPS

Non-Web Targets

Windows

URL

Java

Citrix/ Term. Svcs.

Mainframe

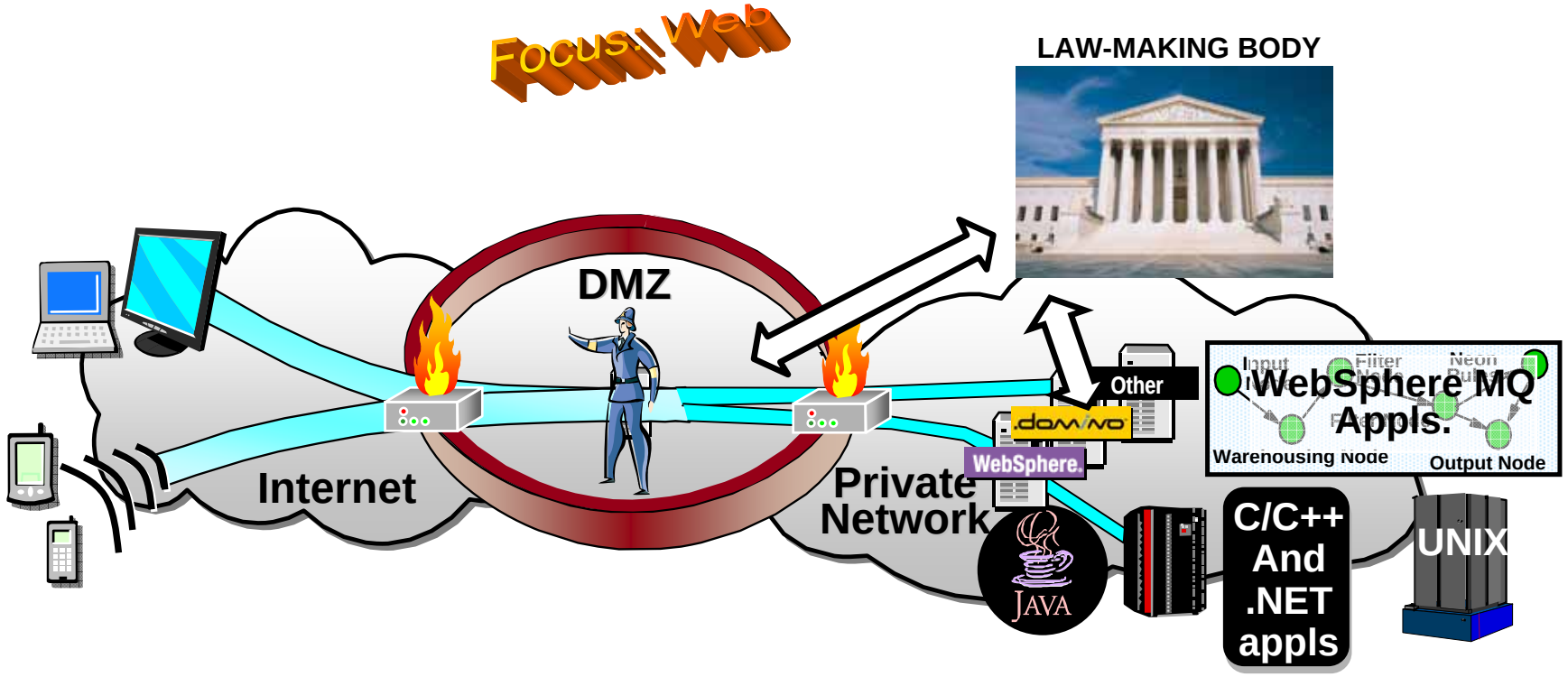
Tivoli Federated Identity Manager (TFIM) Analogy

Similar to presenting a driver's license to a bank teller, to look up your account number

In day-to-day life, it's proving who you are, as you move from one environment to another.

TFIM addresses this exact paradigm as an identity passes from one domain to another (or one Web service to another).

Tivoli Access Manager for e-business (TAMeb) Analogy

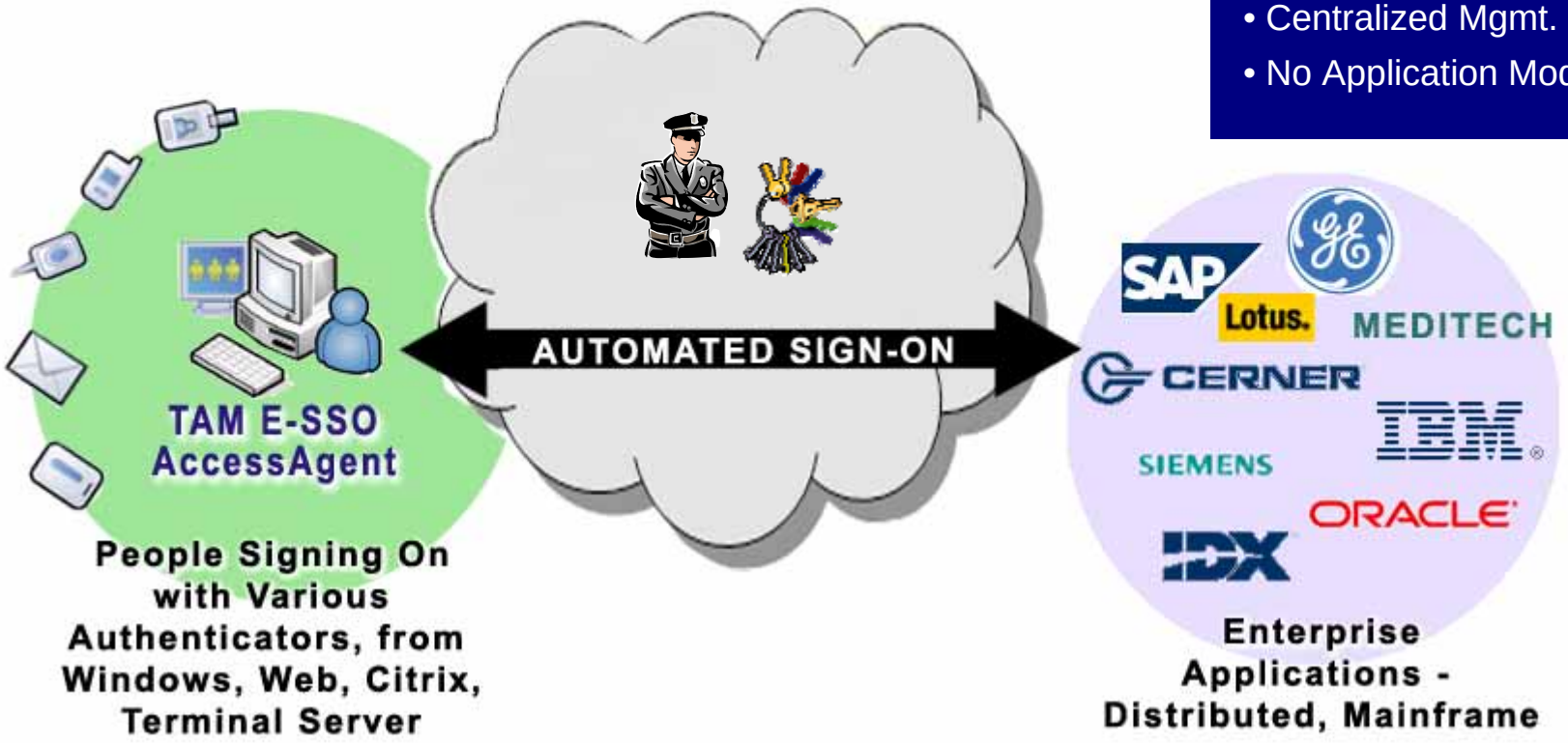


- *TAMeb policy setting is like a body (e.g. legislature) that sets laws in place (including rules for who can gain access to what)*
- *The TAMeb enforcement point is like an armed guard, checking that we know who you are and that you're conforming to the rules*

Tivoli Access Manager for Enterprise Single Sign-On (TAM E-SSO) in Action

Focus: Enterprise

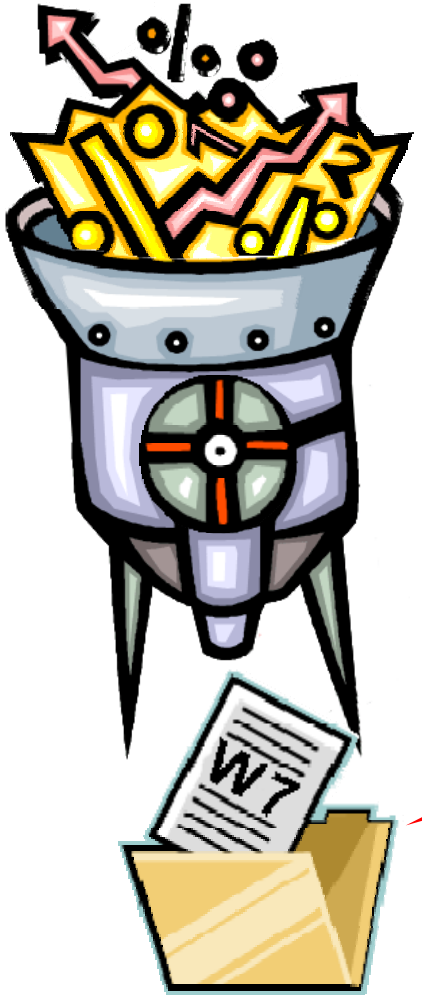
- Enterprise SSO
- Workflow Automation
- Context Management
- 2-Factor Authentication
- User Access Tracking
- Fast User Switching
- Centralized Mgmt.
- No Application Mods



Tivoli Access Manager for Operating Systems (TAMOS) Analogy

TAMOS acts as a "throttle", holding back users (notably root users) from taking undesirable or possibly errant/harmful actions

Tivoli Compliance Insight Manager Analogy

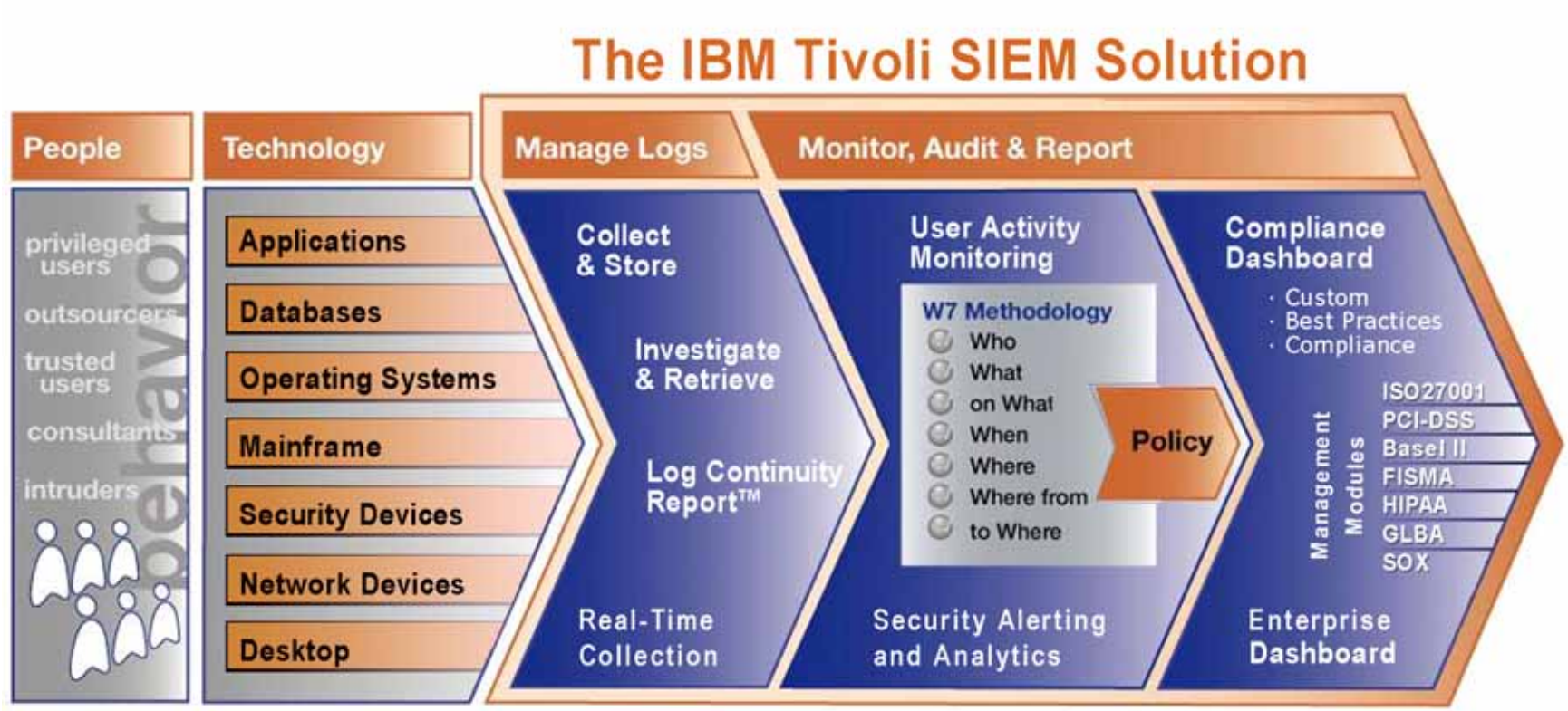


Voluminous audit information from many different sources

Clear, crisp, normalized audit info

Tivoli Compliance Insight Manager (TCIM)

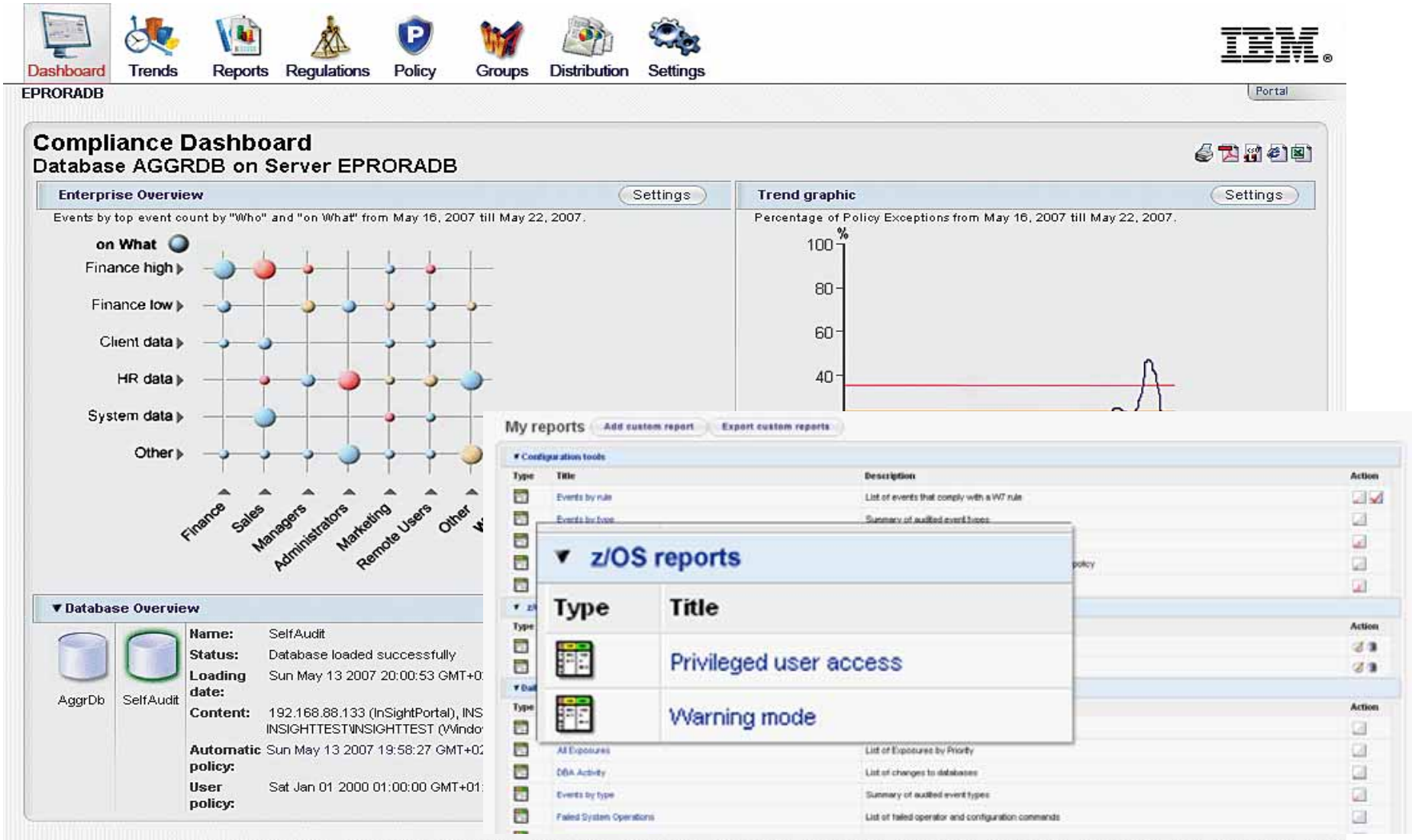
TCIM is a primary component of the Tivoli Security Information and Event Manager (TSIEM) Solution:



3 Key Points:

1. Across resource types
2. W7 Technology
3. Reports by Compliance Regulation

Standard and User defined reports



Tivoli Key Lifecycle Manager Analogy

If cryptography is the heart of your security infrastructure

TKLM is a monitor that looks out for this heart's health

TKLM and PCI-DSS

Have a requirement to meet PCI DSS? TKLM is the essential (I was going to say "key") in helping.

Consider:

- Section 3.5.1 Restrict access to keys to the fewest number of custodians necessary
- Section 3.5.2 Store keys securely in the fewest possible locations and forms
- Section 3.6.1 Generation of strong keys
- Section 3.6.2 Secure key distribution
- Section 3.6.3 Secure key storage
- Section 3.6.4 Periodic changing of keys
- Section 3.6.5 Destruction of old keys
- Section 3.6.6 Split knowledge and establishment of dual control of keys
- Section 3.6.7 Prevention of unauthorized substitution of keys
- Section 3.6.8 Replacement of known or suspected compromised keys
- Section 3.6.9 Revocation of old or invalid keys

More PCI...

1) Build and Maintain a Secure Network

2) Protect Cardholder Data

3) Maintain a Vulnerability Management Program

4) Implement Strong Access Control Measures

5) Regularly Monitor and Test Networks

6) Maintain an Information Security Policy

firewalls (1 - z/OS Comms Server)

removal of default passwords (1 - RACF)

access and storage management (2 & 4 - RACF)

anti-virus software (3 - z/OS Comms Server)

secure applications development (3 - IBM Rational tools)

identity management (4 - Tivoli Identity and Access management tools)

physical access controls (4)

incident management and pen-testing (5 - Tivoli zSecure tools)

policy management (6)

Multi-Zoning with RACF

A Security Label combines the concepts of

- Security clearance (secret, top secret, eyes only)
- Information zones

Information zones apply to any place data may exist

- disks, networks, and other users

Security clearance

- Ensures servers cannot see extra-sensitive data in their information zone
- Prevents copying of data to medium that is readable by servers with lower security clearance ("No write down")
- Not prevalent since there is no equivalent in distributed networking solutions

Label "dominance" is established based on intersection of zones and security clearance

- Not just a simple string comparison

Multi-Zoning with RACF

Create security levels and data partitions

RDEFINE SECDATA SECLEVEL ADDMEM(DEFAULT/100)
RDEFINE SECDATA CATEGORY ADDMEM(INTERNET DMZ APPS DATA COMMON)

RDEFINE SECLABEL PUBLIC SECLEVEL(DEFAULT)ADDCATEGORY(COMMON)
UACC(NONE)
RDEFINE SECLABEL RED SECLEVEL(DEFAULT)ADDCATEGORY(DMZ COMMON)
UACC(NONE)
RDEFINE SECLABEL GREEN SECLEVEL(DEFAULT) ADDCATEGORY(APPS COMMON) UACC(NONE)
RDEFINE SECLABEL BLUE SECLEVEL(DEFAULT) ADDCATEGORY(DATA COMMON) UACC(NONE)

Multi-Zoning with RACF

Assign virtual machines their SECLABELs

PERMIT RED CLASS(SECLABEL) ID(LXHTTP01) ACCESS(READ)
ALTUSER LXHTTP01 SECLABEL(RED)

PERMIT GREEN CLASS(SECLABEL) ID(LXWAS001) ACCESS(READ)
ALTUSER LXWAS001 SECLABEL(GREEN)

Multi-Zoning with RACF

But sometimes a server serves the Greater Good, providing services to all users

To exempt a server from label checking

Assign system servers label SYSNONE

PERMIT SYSNONE CLASS(SECLABEL) ID(TCPIP) ACCESS(READ)
ALTUSER TCPIP SECLABEL(SYSNONE)

Multi-Zoning with RACF

Assign labels to resources

- **VMMDISK – Minidisk**
- **VMLAN – Guest LANs and Virtual Switches**

– RALTER VMMDISK LXHTTP01.201 SECLABEL(RED)
– RALTER VMLAN SYSTEM.NET1 SECLABEL(RED)
– RALTER VMLAN SYSTEM.NET2.0307 SECLABEL(GREEN)
– RALTER VMLAN SYSTEM.NET2.0410 SECLABEL(BLUE)

If you intend to activate TERMINAL or VMSEGMT classes, those resources all need
SECLABELs

Multi-Zoning with RACF

Activate RACF protection

– SETROPTS CLASSACT(SECLABEL VMMDISK VMLAN)
– SETROPTS RACLIST(SECLABEL)
– SETROPTS MLACTIVE(WARNINGS)

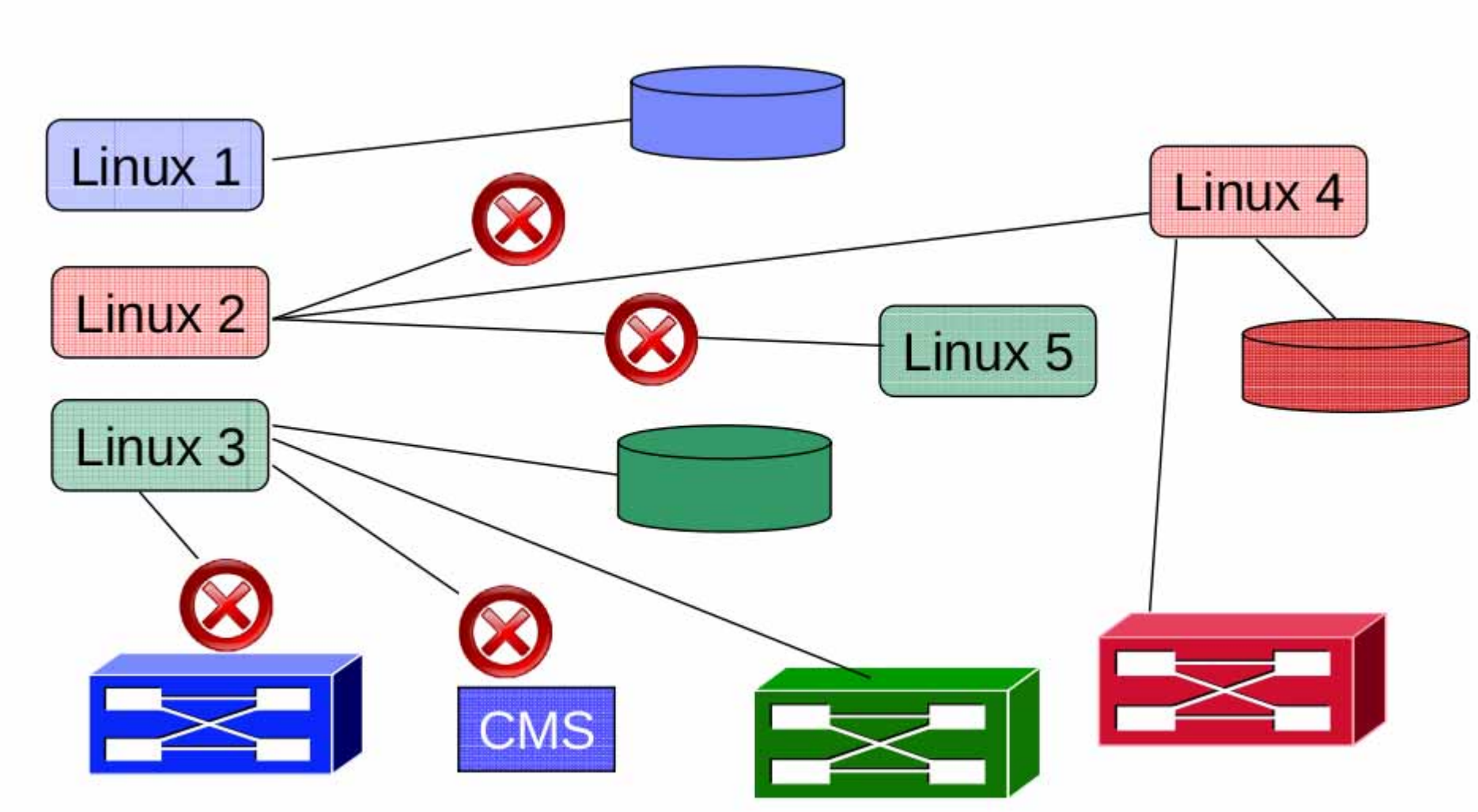
If resource doesn't have a seclabel, message is issued and seclabels are ignored.

Or

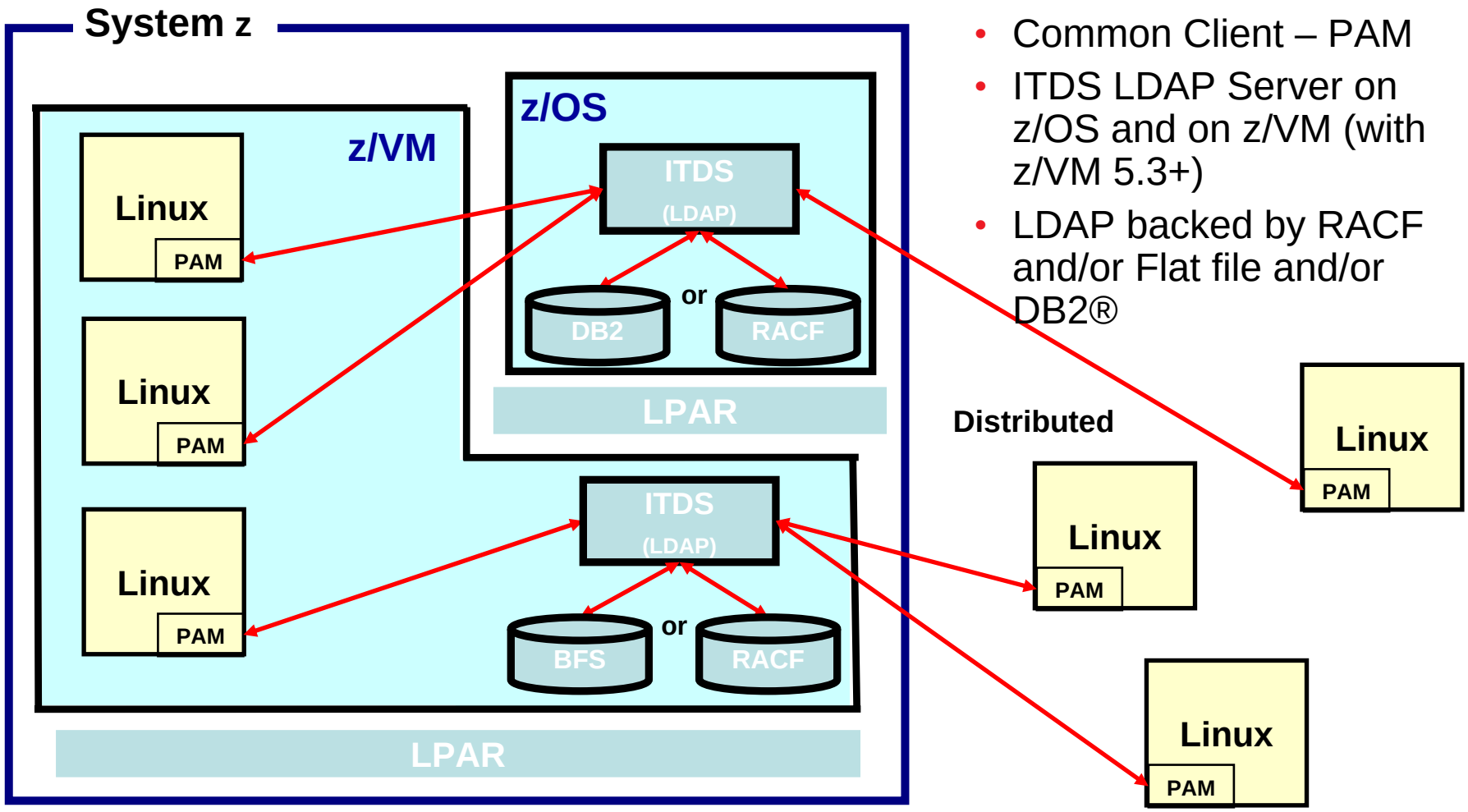
– SETROPTS MLACTIVE(FAILURES)

If resource doesn't have a seclabel, command fails.
This is more secure!

Segregated Security Zones – Firewalls need not apply



Linux on System z, LDAP and PAM



- Common Client – PAM
- ITDS LDAP Server on z/OS and on z/VM (with z/VM 5.3+)
- LDAP backed by RACF and/or Flat file and/or DB2®

Member level changes

- DFSMS now logs changes to PDS and PDSE
  - Starting with z/OS 1.11, back level via PTF
    - » RA10 PSY UA42647 UP08/09/16 P F809
    - » R180 PSY UA42648 UP08/09/16 P F809
    - » R190 PSY UA42649 UP08/09/16 P F809
  - SMF 42
    - » INITIALIZE, DELETE, ADD, CHANGE, REPLACE, RENAME
- zSecure Audit and Alert recognize these records
  - Also from SMF 14 and 15
    - » When *member* code in TSO ALLOC, DYNALLOC or JCL DD
  - Monitor updates to Trusted Computing Base
    - With date, time, userid, dsname and member name

Links

- **Tivoli zSecure 1.11 information center:**
- http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc/welcome.html
- **Release note information**: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc/releaseinfo/releaseinformation.html
- **Tivoli support Web** site: http://www.ibm.com/software/sysmgmt/products/support/doc.html
- **Tivoli zSecure Message Updates for zSecure 1.11** - Provides additional information on messages that were added after the publication of the Tivoli zSecure Message Guide.
- **Tivoli zSecure Admin and Audit documentation updates** - Provides documentation additions and corrections for Tivoli zSecure Admin and Audit.
- **Tivoli zSecure Alert notification 1409, Extended attribute change** - New Alert notification for monitoring extended attribute changes in UNIX files and programs
- **Tivoli zSecure Visual documentation updates for version 1.11.0**
- **Tivoli zSecure Visual Upgrade procedure -** Provides additional information on upgrading the Tivoli zSecure Visual Server and Visual Client application.
- **Fix Central FAQs:** http://www-947.ibm.com/systems/support/fixes/en/fixcentral/help/faq_sw.html
- **Internal zSecure forum**: http://ibmforums.ibm.com/forums/forum.jspa?forumID=3020
- **CARLa forum:** http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1255
- **zSecure Redbook:** http://www.redbooks.ibm.com/abstracts/sg247633.html?Open