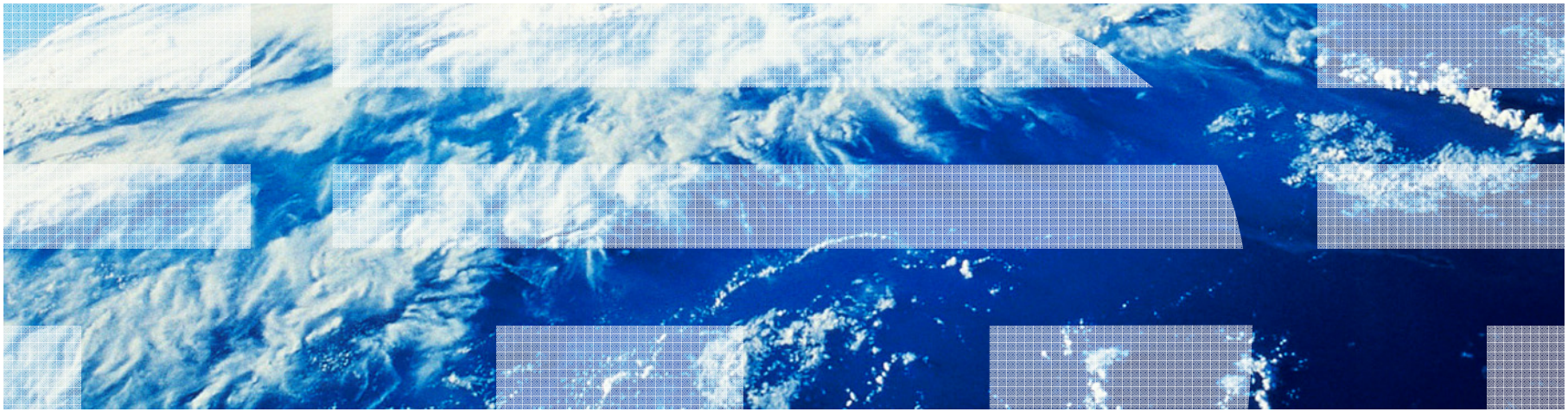
Brian W. Hugenbruch, CISSP
z/VM Security Design and Development
bwhugen@us.ibm.com

z/VM 6.2 Security Update



Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. 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.
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.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
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.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* 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.

Agenda

- Security-Relevant Updates to Current z/VM Releases
- RACF Updates for z/VM 6.2
- RACF Updates for Single System Image clustering (SSI) in z/VM 6.2

Security-Relevant Updates to z/VM

z/VM Security Certification Discussion

- IBM Statement of Direction: Common Criteria Evaluation of z/VM 6.1
  - Statement issued on 22 July 2010
  - **Pre-certification ID:** BSI-DSZ-CC-0752
  - Goal: OSPP-LS at EAL 4+

- Federal Information Protection Standards (FIPS)
  - z/VM 6.1 + PM43382 is evaluated for FIPS 197 (AES)
  - http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html#1873
  - Designed to conform to FIPS 140-2

- Help us understand your certification needs
  - Comments now, or contact offline

FIPS 140-2 Support for z/VM 6.1

- PM08418: Upgrade System SSL to z/OS R11
- VM64805: Add needed functions to LE
- VM64751: Upgrade Binder to z/OS R11
- PM10616: System SSL enablement of FIPS
- PM43382: System SSL Self-Defense

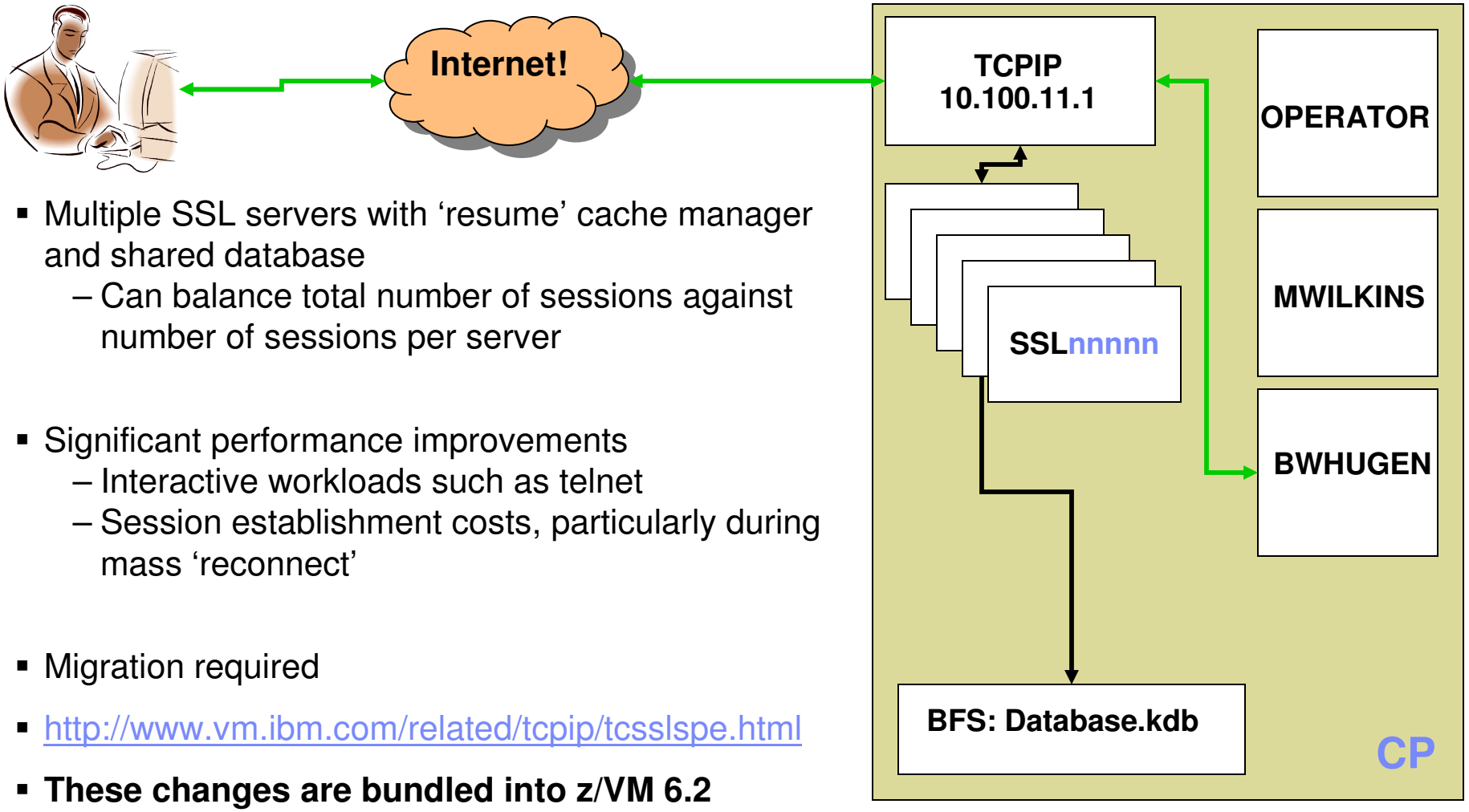
- Enablement of support: z/VM 6.1 can be configured to comply to Federal Information Protection Standard (FIPS) 140-2
  - Requisite cipher suites assure a level of cryptographic strength
  - Creation and validation of certificate database assures trust
  - Official evaluation in progress

- Changes to TCPIP, System SSL, the Binder, and the SSL Server are available for z/VM 6.1

- These changes are bundled in z/VM 6.2

SSL Server Reliability and Scalability

- PK97437: SSLADMIN, TCPRUN and Related Packaging Changes
- PK97438: SSLSERV Module Updates
- PK75662: TCPIP Module Updates



- Multiple SSL servers with 'resume' cache manager and shared database
  - Can balance total number of sessions against number of sessions per server
- Significant performance improvements
  - Interactive workloads such as telnet
  - Session establishment costs, particularly during mass 'reconnect'
- Migration required
- http://www.vm.ibm.com/related/tcpip/tcsslspe.html
- **These changes are bundled into z/VM 6.2**

z/VM SSL Client Certificate Support

- PM52716: Enable Client Certificate Authentication in z/VM SSL

- Expansion of SSL/TLS handshaking processes to include checking for a client-presented certificate
  - Dynamic TN3270 Support only
  - Certificate presented by client must match against data in the z/VM certificate database
  - New INTERNALCLIENTPARMS parameter: CLIENTCERTCHECK

- APAR available for z/VM 6.1 and z/VM 6.2

LDAP Support Updates

- **Upgrade to z/OS 1.11 ITDS in z/VM 6.1**
  - Support for password change logging
    - z/OS uses RACF certificate services
    - z/VM uses System SSL services
  - Password phrases can now be used in an ldap bind

- **Upgrade to z/OS 1.12 ITDS in z/VM 6.2**
  - RACF resource change-logging through LDAP
    - user, group, and general resource profiles
    - an open, remote method of change notification using only LDAP interfaces
    - an LDAP client can read the LDAP change log, detect updates to RACF users, groups, group membership, and general resources, and then retrieve RACF entries.
    - LDAP server must be configured to enable the SDBM backend.
  - Expanded password management
    - Expiry warnings
    - Interactively set new passwords

Crypto Support Updates

- APAR VM64656: **z/VM support for Crypto Express3 cards**
  - On the z10: z/VM 5.3, z/VM 5.4 and z/VM 6.1
  - On the z196: z/VM 5.4 and z/VM 6.1
  - Accelerator mode (CEX3A) and Coprocessor mode (CEX3C)

- APAR VM64793: **Protected Key CPACF for z/VM 5.4 and z/VM 6.1**
  - On both z10 and z196
  - Protection of key material when using CPACF, instead of Clear Key operations
    - Key does not exist outside of physical hardware
  - Not to be confused with Secure Key (for the Crypto Express cards)
  - Designed to increase throughput

- z/VM 6.2:
  - QUERY CRYPTO output changes

Security-Relevant Updates in RACF for z/VM 6.2

RACF Updates for z/VM 6.2

General Updates:

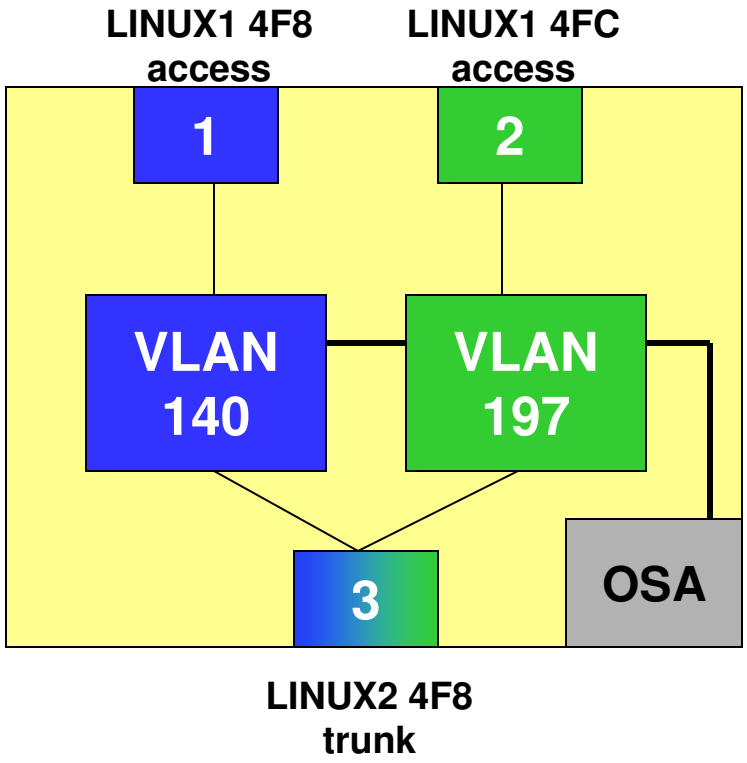
- High Level Assembler no longer required for most common customizations
- ALTER (MW) access for VMMDISK no longer conveys the ability to change the access list for the minidisk
- DBUnload requirement for T-Disk removed
  - Can use existing minidisk instead

RACF Updates for z/VM 6.2

- **User Attribute: PROTECTED**
  - Shields user access from being revoked due to
    - Logon failures
    - Inactivity or unsuccessful access attempts
    - Any method that uses a supplied password (logon, FTP …)
  - AUTOONLY service machines are a good candidate for this attribute
  - Specify “NOPASSWORD” and “NOPHRASE” on ADDUSER or ALTUSER:
    - `ALTUSER TCPIP10 NOPASSWORD NOPHRASE`
  - Any machine without a password or passphrase is Protected by default:
    - `ADDUSER BWHUGEN`
  - To remove the Protected attribute from a user, add a password or passphrase:
    - `ALTUSER BWHUGEN PHRASE('a_really!good_passw0rdp#r9$e,yo')`
  - Protected users can still be revoked through REVOKE

RACF Updates for z/VM 6.2

- **Multiple Access Ports per Guest**
  - Can now enable a guest with multiple unique access ports to the same VSWITCH
  - Associates NICs and VSWITCH ports (Switch not available on NICDEF)
  - Ports are associated with VLANs
  - Requires explicit CP enablement
    - `CP SET VSWITCH PORTNUMBER`
    - `CP SET VSWITCH VLANID`



- RACF Enablement is business-as-usual, authorizing by VLAN IDs instead of port numbers:

```
– RDEFINE VMLAN SYSTEM.SWITCH05 UACC(NONE)
– PERMIT SYSTEM.SWITCH05 CLASS(VMLAN) ID(LINUX1 LINUX2) ACCESS(UPDATE)
– RDEFINE VMLAN SYSTEM.SWITCH05.0140 UACC(NONE)
– PERMIT SYSTEM.SWITCH05.0140 CLASS(VMLAN) ID(LINUX1 LINUX2) ACCESS(UPDATE)
– RDEFINE VMLAN SYSTEM.SWITCH05.0197 UACC(NONE)
– PERMIT SYSTEM.SWITCH05.0197 CLASS(VMLAN) ID(LINUX1 LINUX2) ACCESS(UPDATE)
– ...
```

RACF Updates for z/VM 6.2

- **Protecting Real Devices**
  - Authorization checking based on the **VMDEV** class
    - Usual access levels (`NONE READ UPDATE CONTROL`) apply
  - Triggers when Connecting a real device to a virtual machine for exclusive use, or connecting a tape device to a virtual machine for shared use
    - `DEDICATE` statements in the User Directory
    - `ATTACH` command
    - `GIVE` command
- Define `RDEV.(rdevno).sysname` to VMDEV
  - `PERMIT RDEV.0456.* CLASS(VMDEV) ID(BWHUGEN) ACCESS(UPDATE)`
  - `SETROPTS CLASSACT(VMDEV)`
- Enable an appropriate event:
  - `RALTER VMXEVENT EVENTS1 ADDMEM(RDEVCTRL/NOCTL)`
  - `SETEVENT REFRESH EVENTS1`

RACF Updates for z/VM 6.2

RPIDIRCT updates:

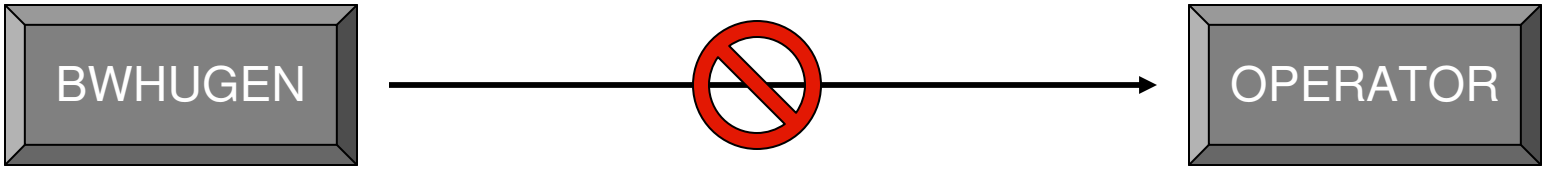
- Create VMLAN profiles from NICDEF statements
  - *Doesn't cover Multiple Access Ports (no NICDEF support)*
- Create VMDEV profiles from DEDICATE statements
- Recognize IDENTITY and SUBCONFIG definitions
- Passwords AUTOONLY, LBYONLY, and NOPASS cause user to be Protected
- Password NOLOG causes user to be revoked unless required for POSIX
  - POSIX users will be Protected

RACF Updates for z/VM 6.2

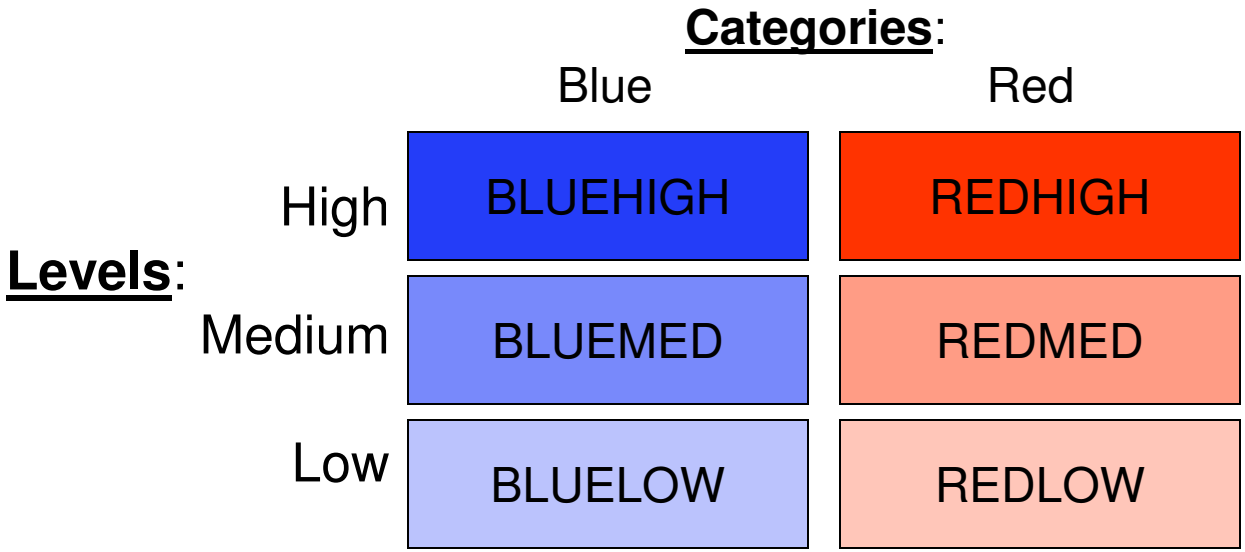
- **Enablement and Control of SECUSER and OBSERVER when Mandatory Access Controls (SECLABELs) are active**
  - CONSOLE OBSERVER (read-only)
  - SET OBSERVER (read-only)
  - CONSOLE SECUSER (read-write)
  - SET SECUSER (read-write)
  - CP SEND.G (read-write)
  - CP SEND.C (write-only)

- SECLABEL rules for read- and write-access apply:
  - "No read up, no write down."

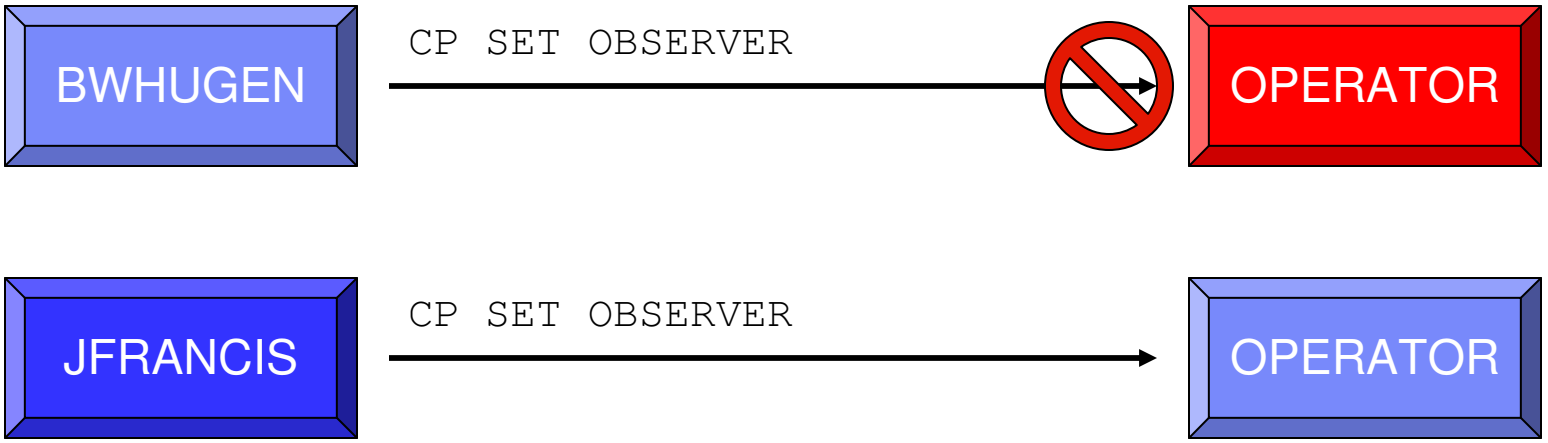
RACF Updates for z/VM 6.2

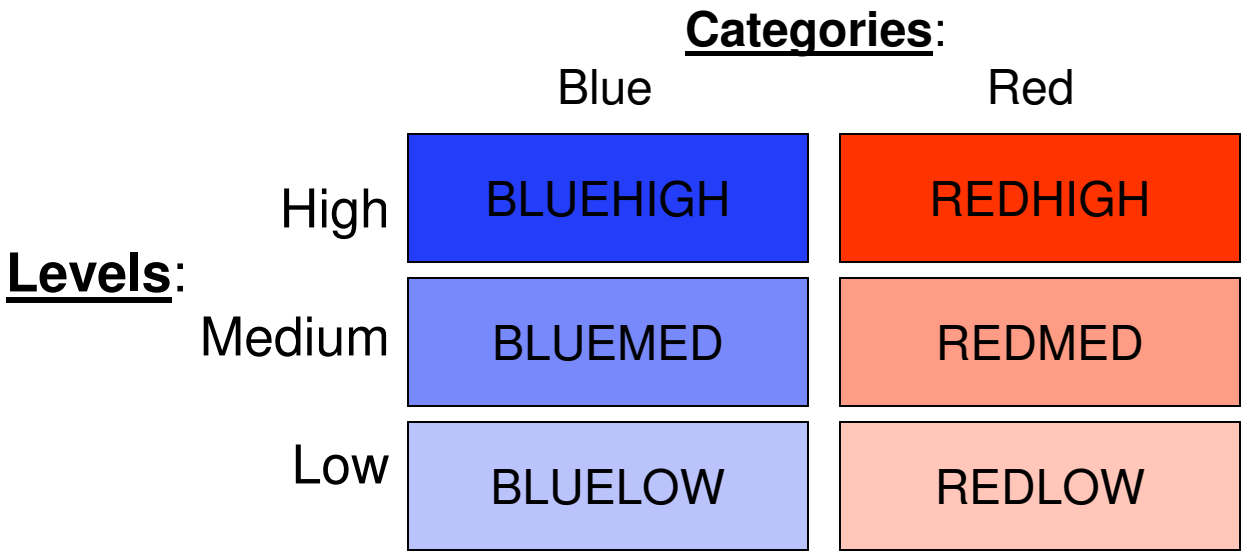


<SET SERVER Command>



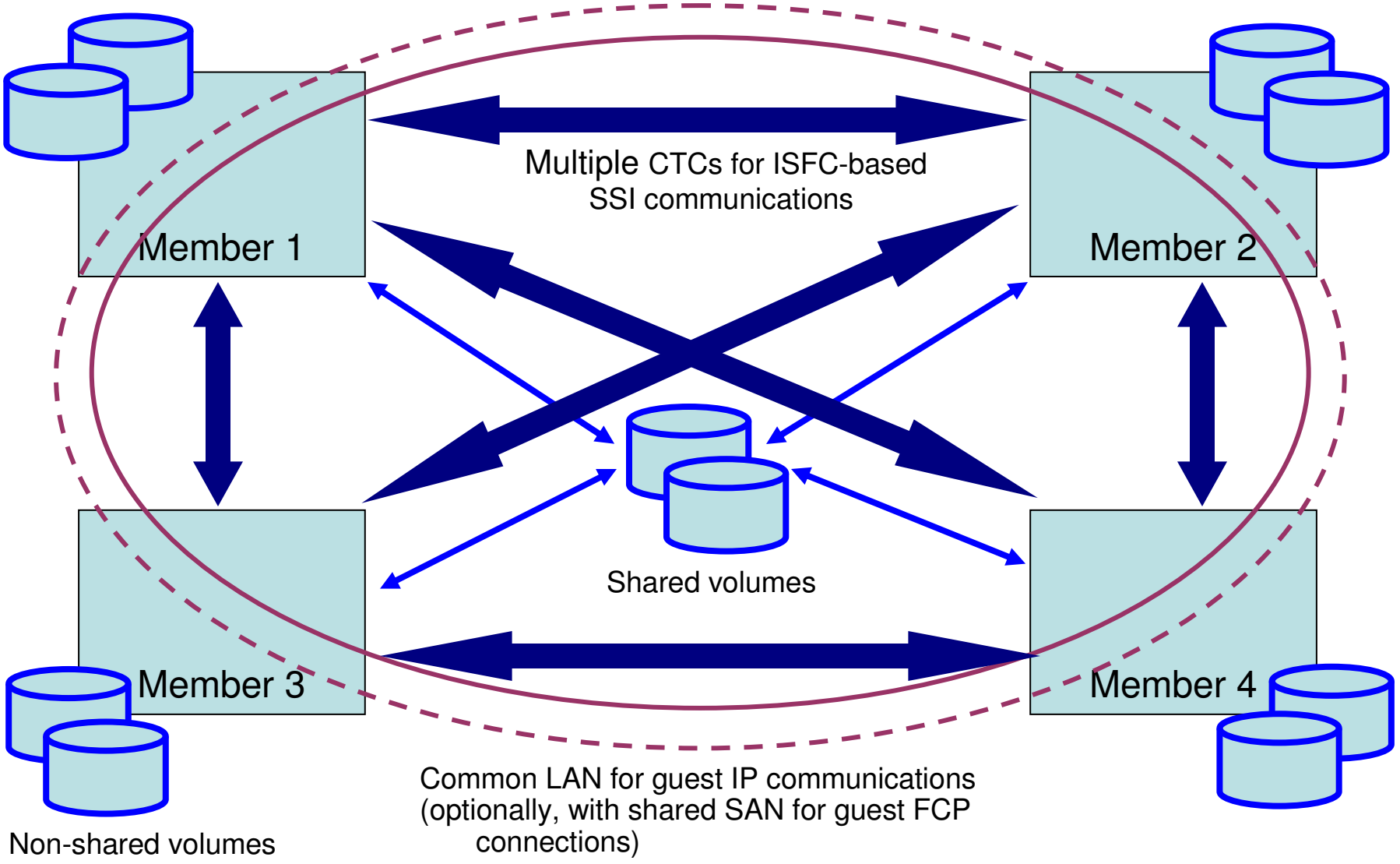
RACF Updates for z/VM 6.2





RACF In A
Single System Image Cluster

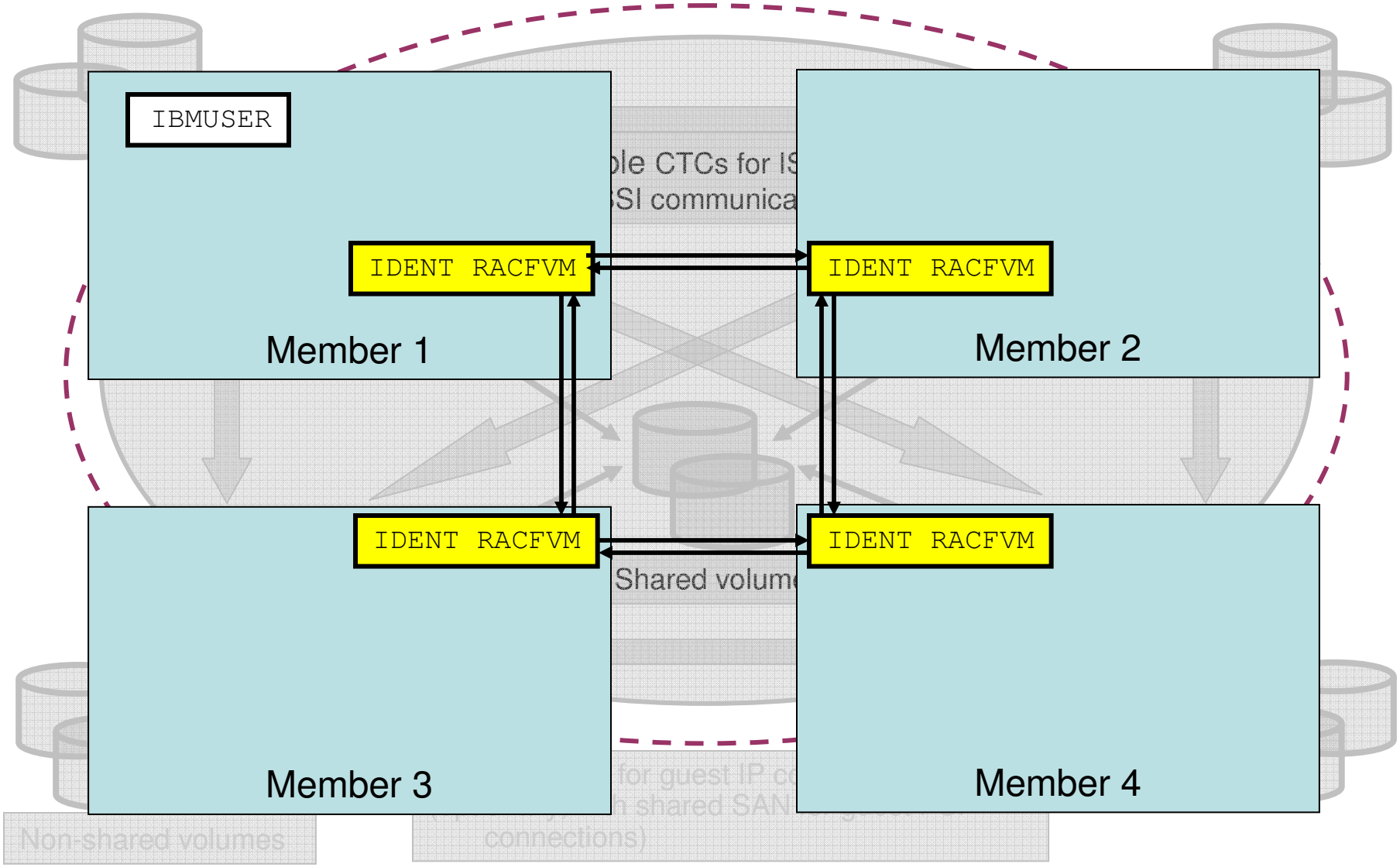
z/VM SSI Cluster



RACF in a Single System Image Cluster

- When installed in an SSI, RACF creates *a single security context* for the cluster
  - Shared database and definitions
  - Handshaking of RACFVM instances
  - Cluster-aware auditing
- RACF for SSI is for the entire cluster, it's not something you can enable one step at a time.
- RPIDIRCT has been updated to handle both single-configuration and multi-configuration virtual machines
- The virtual machines have been modified to operate both in and out of an SSI …

RACF Virtual Machines in an SSI cluster



RACF Virtual Machines in an SSI cluster

Handshaking and Command Propagation

- Each RACF server in the SSI must provide the same consistent security context.
- Commands that create broader changes need to be propagated across the cluster
  - SETROPTS
  - RVARY
  - SETEVENT
- RACF will suppress “extra” messages and marshal output when executing “remotely.”
- Locking done to ensure RVARY submissions are handled sequentially
- RACF command sessions don't support command propagation so in an SSI the commands SETROPTS, RVARY, and SETEVENT will be rejected with message:
  - `RPITMP0021E 'command-name' RACF COMMAND MUST BE ISSUED WITH RAC IN A SSI`
- RAC command, ISPF panels, and R_Admin API (used by LDAP) are interfaces which support command propagation

RACF Virtual Machines in an SSI cluster

Handshaking and Command propagation

- The propagated commands output from each RACF server on each system is bracketed by the lines:
  - `OUTPUT FROM <racfname> ON SYSTEM <ssinode>`
  - `END OF OUTPUT`

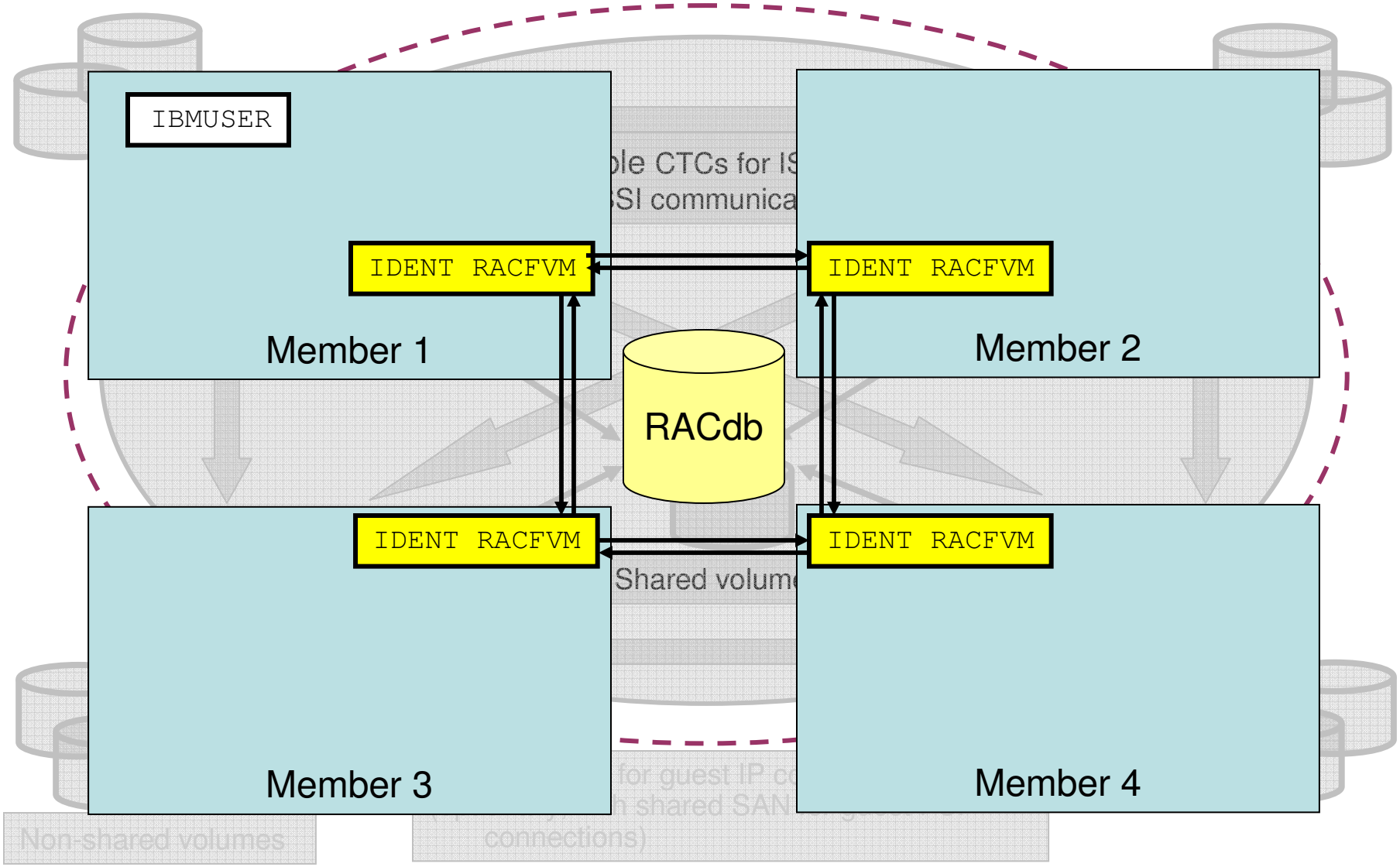
- SETROPTS and RVARY commands will be propagated in non-SSI multi-server environments.

RACF Virtual Machines in an SSI cluster

Propagation of MAC cache purge

- Purge initiated by specific operands instead of **any** SETROPTS command:
  - RACLIST REFRESH of SECLABEL class
  - Activating or inactivating VMMAC class
  - LOGOPTIONS auditing of VMMAC class
  - Any MLS change
  - MLQUIET
  - MLACTIVE(WARNING)
  - SECLABELAUDIT

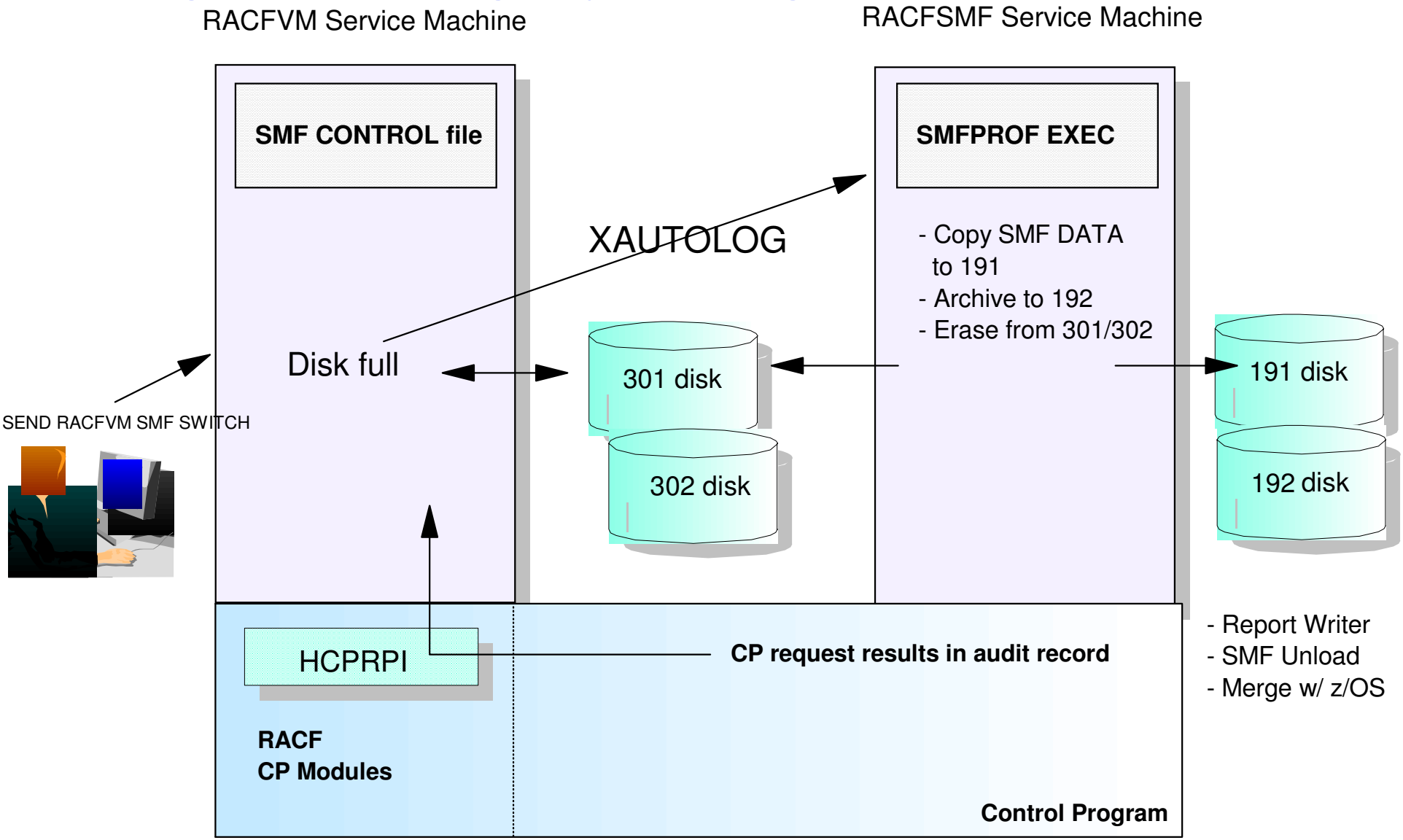
The RACF Database in an SSI



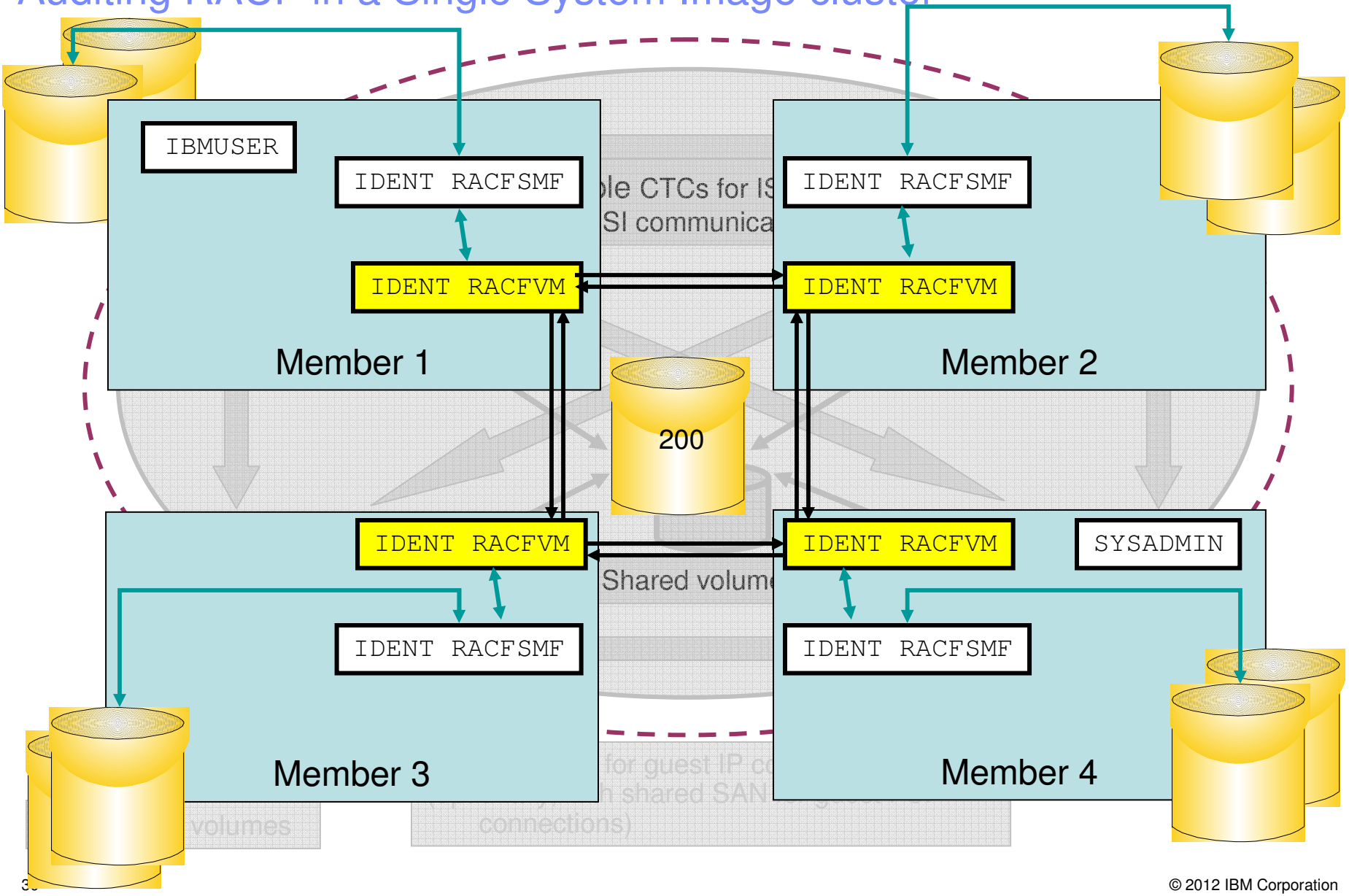
The RACF Database in an SSI

- All RACF servers in SSI must **share** the same RACF database
  - Databases are shareable today
  - Maintain a single security context; no confusion in security policy
- RACF database in SSI must be fullpack minidisk, must support reserve/release and can't be an FBA device
  - Full-pack 3390s for both the primary (200) and backup (300)
  - RDEVICE statements for each in the System Configuration file
  - Minidisk caching is automatically turned off
- Database synchronization
  - When a member joins, CP+RACF will ensure that the joining server has identical database datasets to those being used and active in the SSI
  - Automatic propagation of RVARY commands

Auditing RACF in a Single System Image cluster



Auditing RACF in a Single System Image cluster



Auditing RACF in a Single System Image cluster

- RACFVM is a multiconfiguration virtual machine
  - Shared RACF database
  - All other disks are local – including 301 and 302 for auditing
  - Separate SMF CONTROL files operating against a single security context
- RACFSMF is also multiconfiguration virtual machine
  - Separate 191 and 192 disks
  - Separate SMFPROF EXEC files
- Auditing automation should account for this disparity to gather all pertinent audit records

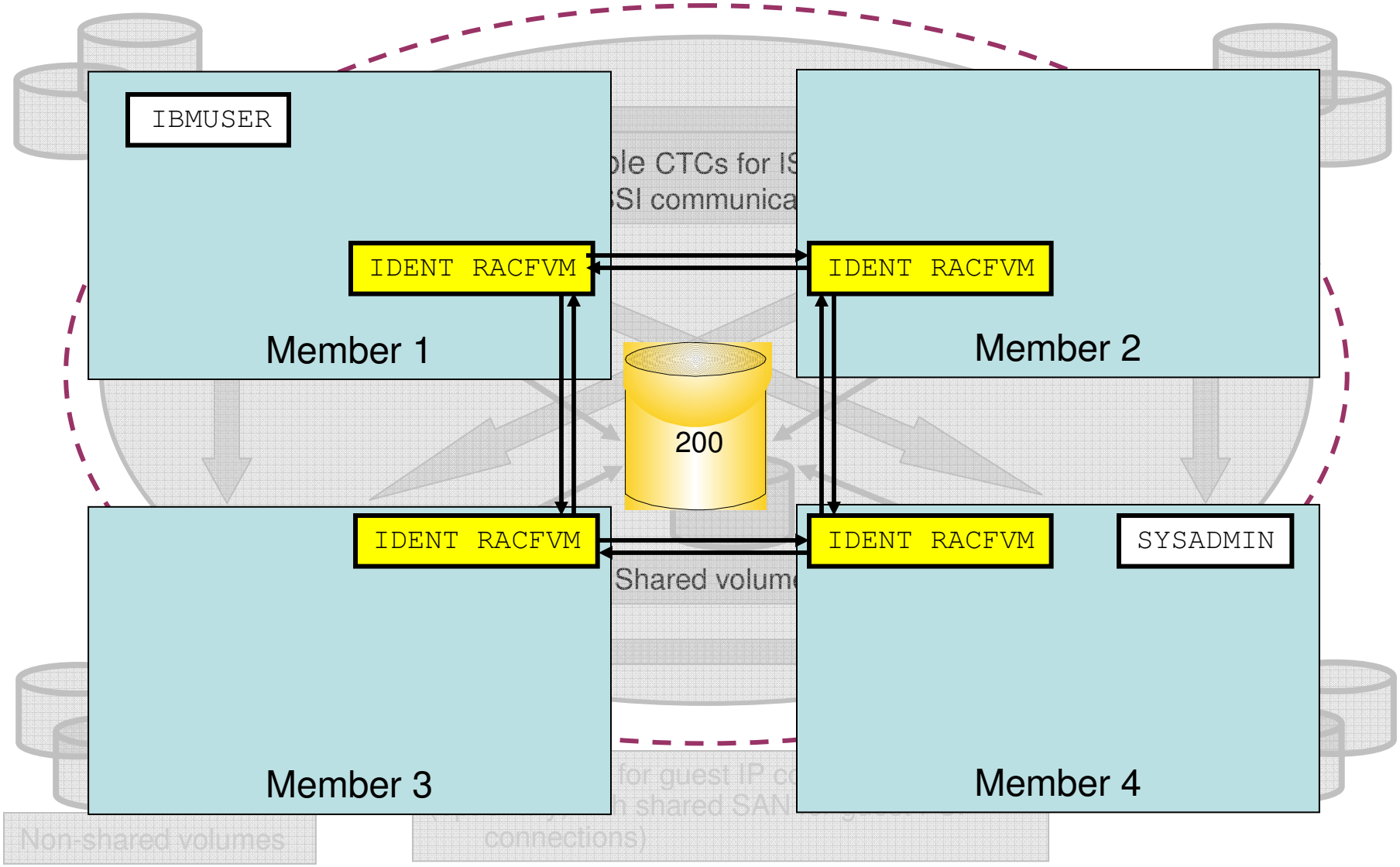
Auditing RACF in a Single System Image cluster

- In the case of some commands – the AT command in particular – auditing records will appear on the destination system
  - AT_LOGON
  - AT_FROM
  - AT_LOGOFF

- Auditing distinguishes between local and remote nodes in a cluster, even when sharing the same security context
  - Controlled commands are the same
  - Auditing requisites are the same
  - Events are the same

  …. But the systems are distinct, from the point of view of a virtual machine “in the know”

RACF and Live Guest Relocation



RACF and Live Guest Relocation

Live Guest Relocation

- `VMRELOCATE MOVE USER` *`userid`* `TO` *`sysid`*
  - Class B command

- RACF cleans up a user's presence on the source system, and prepares for the target system for the relocate-logon of the user

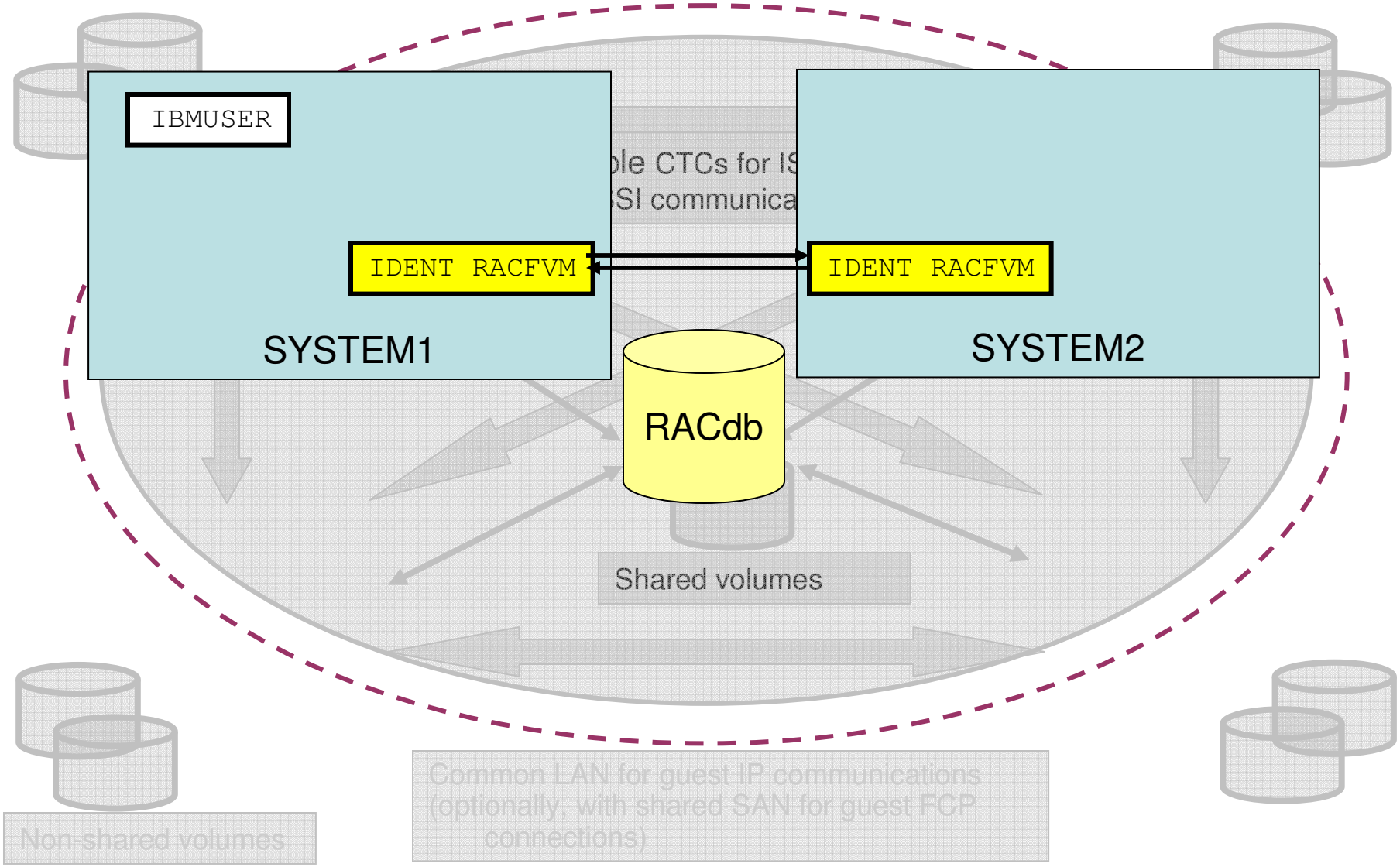
- Generate LOGOFF/LOGON auditing events on source/target system, to note the transition

- RACF perspective of relocate events:
  - User data is created for *userid* on *sysid* with all the above
  - User resources are allocated on sysid
  - Associated authorization calls are approved without a RACF check
  - Relocate-logon is requested for *userid* on *sysid* when the inbound relocation is complete

Migrating to RACF in an SSI

- **Recommendations:**
  - If you don't have an ESM, get one.
  - Line up the shared DASD required for the database; remember that this needs to be a fullpack minidisk!
  - If you're converting one or more ESM-controlled systems into an SSI:

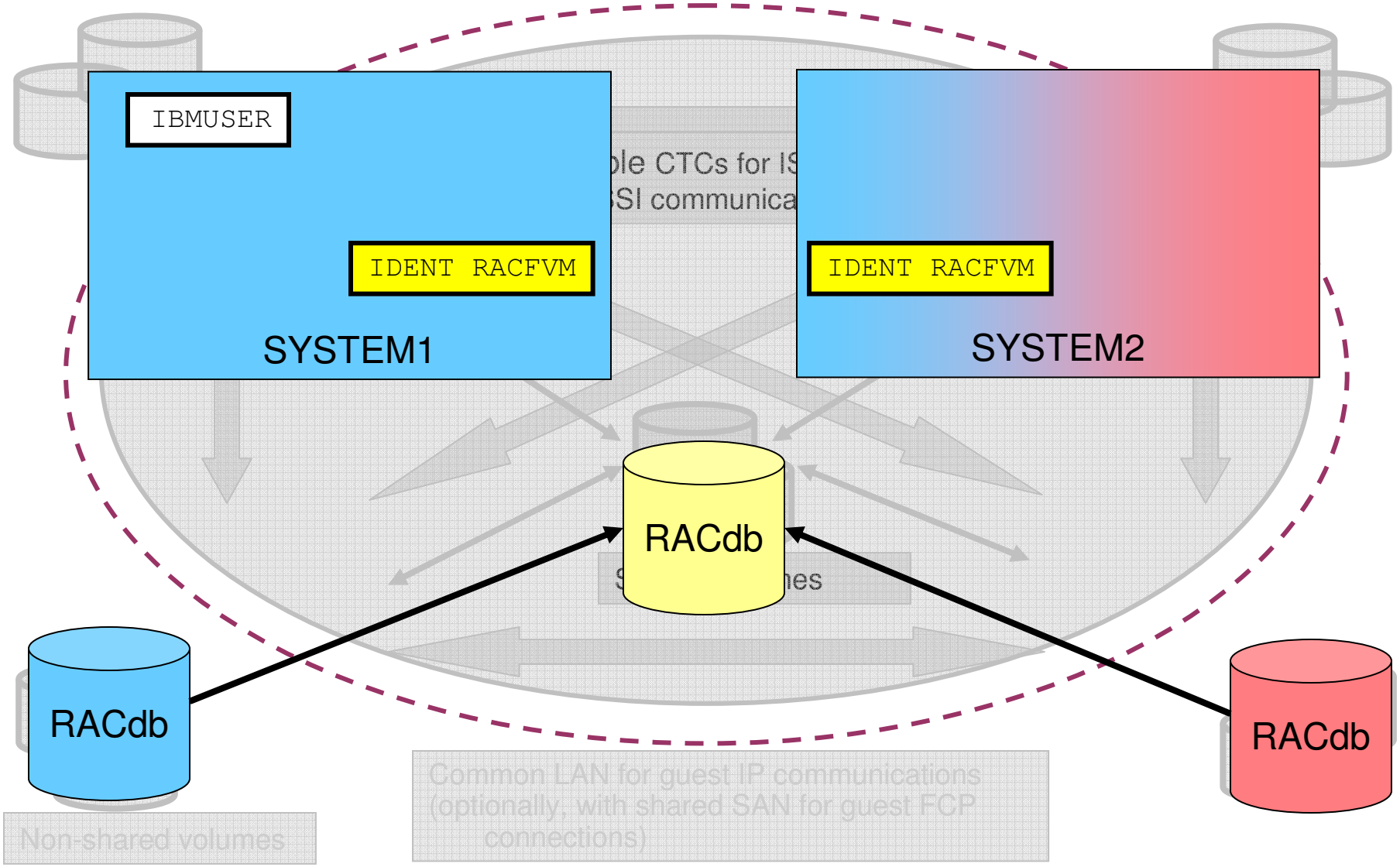
Migrating to SSI: RACF Considerations



Migrating to RACF in an SSI

- **Recommendations:**
  - If you don't have an ESM, get one.
  - Line up the shared DASD required for the database; remember that this needs to be a fullpack minidisk!
  - If you're converting one or more ESM-controlled systems into an SSI:
    - Migrate your "master" system to 6.2 in a non-SSI format
    - Convert associated resource profiles to 6.2 format, using RPIDIRCT as necessary
    - Take the steps to enable SSI; turn on RACFVM as part of the outlined process
  - If you're converting two (or more) distinct ESM-controlled systems to an SSI

Migrating to SSI: RACF Considerations



Migrating to RACF in an SSI

- **Recommendations:**
  - If you don't have an ESM, get one.
  - Line up the shared DASD required for the database; remember that this needs to be a fullpack minidisk!
  - If you're converting one or more ESM-controlled systems into an SSI:
    - Migrate your "master" system to 6.2 in a non-SSI format
    - Convert associated resource profiles to 6.2 format, using RPIDIRCT as necessary
    - Take the steps to enable SSI; turn on RACFVM as part of the outlined process
  - If you're converting two (or more) distinct ESM-controlled systems to an SSI
    - You will need to merge the databases
    - You may want to consider which of your 2+ systems has the most complex security context before choosing which one is the "master" system
    - After one system is enabled, make directory and RACF database updates for the secondary system

Summary

- Certification work continues
- Improvements continue to enhance base z/VM security
- RACF has been adapted to handle the Single System Image clustering technology
- z/VM continues to secure the road to Smarter Computing

For more information …

Speaker: Brian W. Hugenbruch, CISSP

- Web: http://www.vm.ibm.com/devpages/hugenbru
- Mail: bwhugen at us dot ibm dot com

On the web:

- z/VM Security resources: http://www.VM.ibm.com/security
- z/VM Secure Configuration Guide: http://publibz.boulder.ibm.com/epubs/pdf/hcss0b30.pdf
- System z Security: http://www.ibm.com/systems/z/advantages/security/
- Redbook: z/VM Security, SG24-7471
- http://www.vm.ibm.com/related/tcpip/vmsslinf.html -- SSL Information and Walk-through

Back-up Slides

IBM Statement of Direction:

Common Criteria for z/VM 6.1

- IBM issued a Statement of Direction on 22 July 2010:

  "IBM intends to evaluate z/VM V6.1 with the RACF Security Server optional feature, including labeled security, for conformance to the Operating System Protection Profile (OSPP) of the Common Criteria standard for IT security, ISO/IEC 15408, at Evaluation Assurance Level 4 (EAL4+)."

Note: All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice, and represent goals and objectives only.