CA VM:Secure Single System Image Support

Bob Bolch
Presented by Yvonne DeMeritt

04/24/2012

Terminology

Single System Image – IBM's multiple system environment that allows central management of the systems in the cluster as well as the ability for 'some' running virtual servers to be moved from one system to another

SSI – Single System Image

CA VM:Secure – for directory functions, also refers to CA VM:Director

Agenda

- CA VM:Secure/CA VM:Director SSI support
  - General information/Concepts
  - Directory Changes
  - Command Changes
  - SSI Configuration
- Other CA VM product SSI support
  - CA VM:Spool and V/SEG Plus
  - CA VM:Backup and HiDRO
  - CA VM:Operator
  - CA VM:Tape

SSI - Single System Image

CA VM:Secure maintains a consistent view of system administration definitions across members of a complex

- CP Object Directory virtual machine definitions
  - You get the same virtual machine wherever you log on
- Security Manager Rules definitions
  - You have the same authorizations and access to resources
- Directory Management or ESM Administration Interfaces
  - You enter VMSECURE commands the same way wherever you log on

SSI invalid password handling

Journaling accumulates excessive bad password attempts from any member.

- You can't try 3 bad passwords, error out, and try 3 other passwords on another member. You get 3 attempts (or whatever number of attempts was defined) from anywhere.
- Journal entries for terminals add the node name the terminal is attached to. (We don't want to lockout every 3270 at address 0020 on every member node.)

SSI synchronization must occur in real time

VM:Secure operates as a set of servers distributed across the members of the complex

- A “master” VM:Secure runs on one member node to perform all the function of a non-SSI VM:Secure server
  - Processes commands
  - Updates Configuration, Source Directory entries, and Rule files
  - Compiles the Object Directory and Rules tables
  - Responds to External Security Manager requests from CP

SSI synchronization must occur in real time

VM:Secure operates as a set of servers distributed across the members of the complex

- An “agent” VM:Secure runs on each other member node to perform a subset of the “master” server function
  - Compiles the Object Directory and Rules tables
  - Responds to External Security Manager requests from CP
- An “agent” implements additional new function
  - Responds to synchronization requests from the “master” server
  - Converts to replace a “master” if an outage situation occurs

New Directory Entry Types – IDENTITY

IDENTITY entries are similar to USER entries

- Each defines a virtual machine.
- Every directory statement in a USER entry is available in an IDENTITY entry.
- Every Security Manager permission or rule applies to either type of entry in exactly the same way.

New Directory Entry Types – IDENTITY

IDENTITY entries have additional capabilities and restrictions compared to USER entries

- LOGON
  - USER virtual machines can only LOGON to one member of the SSI complex at a time.
  - IDENTITY virtual machines may logon to more than one member simultaneously
- Spool
  - USER machines access spool files created on all members.
  - Each IDENTITY logon instance sees only files created on their specific member node.

New Directory Entry Types – SUBCONFIG

SUBCONFIG entries tailor the IDENTITY virtual machine definition for execution on a specific member node

- SUBCONFIG entries are restricted to a subset of statement types
- OPTION statement settings are restricted to a few values
- A SUBCONFIG entry is processed by a limited number of commands
- A SUBCONFIG entry is connected to one IDENTITY by a BUILD statement

New Directory Entry Types – SUBCONFIG

SUBCONFIG entries prohibit certain statements

- Authorization statements: ACCOUNT, ACIGROUP, ADJUNCT, APPCPASS, AUTOLOG, CLASS, D8ONECMD, IOPRIORITY, IUCV, LOGONBY, NAMESAVE, NOPDATA, POSIXGLIST, POSIXINFO, POSIXOPT, STDEVOPT, XAUTOLOG, VMRELOCATE
- Miscellaneous statements: INCLUDE, POOL, BUILD, CPU, MACHINE

New Directory Entry Types – SUBCONFIG

SUBCONFIG entries prohibit certain options

- Authorization options: ACCT, APPLMON, CFVM, CFUSER, CHPIDVIRTUALIZATION, COMSRV, CRYMEASURE, DEVINFO, DEVMAINT, DIAG88, DIAG98, D84NOPASS, IGNMAXU, LKFAC, LNKEXCL, LNKNOPAS, LNKSTABL, MAINTCCW, NETACCOUNTING, NETROUTER, RMCHINFO, SETORIG, STGEXEMPT, SVMSTAT
- Options no longer tolerated: DEDICATE, NODEDICATE, NOVF, VIRT=FIXED (V=F), VIRT=REAL (V=R)

New Directory Entry Types
Examples

SSI Ready

```
IDENTITY TEST1 SECRET

BUILD ON * USING SUBCONFIG TST1-1

OPTION LNKNOPAS

CONSOLE 009 3215

IPL CMS

MDISK 192 3390 4 1 SYSWRK MR ALL


SUBCONFIG TST1-1

MDISK 191 3390 5 1 SYSRS1 MR ALL
```

SSI Enabled

```
IDENTITY TEST1 SECRET

BUILD ON SYS1 USING SUBCONFIG TST1-1

BUILD ON SYS2 USIMG SUBCONFIG TST1-2

CONSOLE 009 3215


SUBCONFIG TST1-1

MDISK 191 3390 5 1 SYSRS1 MR ALL


SUBCONFIG TST1-2

MDISK 191 3390 5 1 SYSRS2 MR ALL
```

New Directory Object Formats – SSI-Ready and SSI-Enabled

VM:Secure compiles the Object Directory in one of two formats

- Controlled by the presence of SSINODE statements in the PRODUCT CONFIG file.
- SSI-Ready provides compatibility mode with prior VM releases
- SSI-Enabled allows for exploitation of full SSI capabilities
- Format controls when SUBCONFIG elements are merged into an IDENTITY entry

New Directory Object Formats – SSI-Ready

SSI-Ready merges SUBCONFIG elements into IDENTITY entry at compile time

- Creates a normal USER Object Directory entry.
- Used by non-SSI 6.2.0, by prior releases of VM, or by a single node SSI complex
- Allows a maximum of one SUBCONFIG per IDENTITY.
- Requires BUILD ON * USING SUBCONFIG *name*

New Directory Object Formats – SSI-Enabled

SSI-Enabled merges SUBCONFIG elements into IDENTITY entry at IDENTITY LOGON time

- Creates incompatible Object Directory entries.
- Used by z/VM 6.2.0 single node or multiple node SSI complexes
- Allows a maximum of four SUBCONFIGs per IDENTITY.
- Requires BUILD ON *node* USING SUBCONFIG *name* format

VM:Secure Command Processing
IDENTITY Entries

- Generally, commands operate on IDENTITY entries just as if they were USER entries.
- Skeleton entries may contain an IDENTITY statement
- A USER entry may be changed into an IDENTITY entry (or vice versa) using the CHGENTRY command:
  - CHGENTRY name [USER | IDENTITY]

VM:Secure Command Processing
IDENTITY Relationship to SUBCONFIGs

- No BUILD statement may name a SUBCONFIG entry which does not exist
- No SUBCONFIG entry may exist without a BUILD statement naming it
- BUILD statements may not be added or deleted by use of the EDIT, EDX, or REPENTRY commands

VM:Secure Command Processing
SUBCONFIG Entries

- Only a subset of commands operate on SUBCONFIG entries.
- Creation of a SUBCONFIG entry causes the creation of a BUILD statement in a specified IDENTITY
- Deletion of a SUBCONFIG entry causes the deletion of a BUILD statement in the appropriate IDENTITY

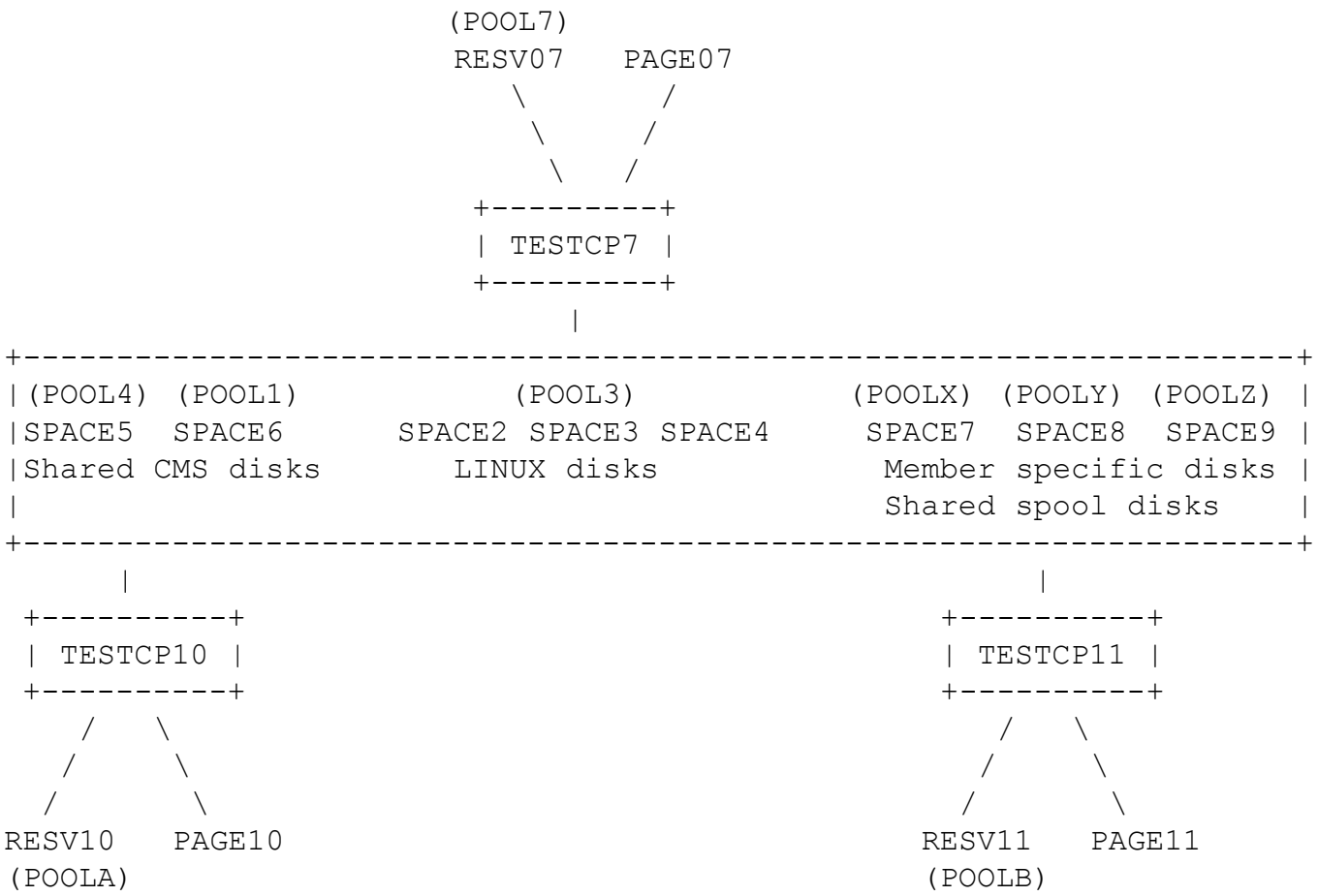
VM:Secure Command Processing
SUBCONFIG Entry Creation

- ADDENTRY *name-2* (IN *identity* ON *membername*
- IN and ON options cause a SUBCONFIG entry to be created and a BUILD statement to be added to the named IDENTITY entry
- ADDENTRY requires either a SKELETON file or a file containing the desired SUBCONFIG entry statements
- For SSI-Ready directories, membername must be '*'
- For SSI-Enabled directories, membername must be defined on an SSINODE configuration statement

VM:Secure Command Processing
SUBCONFIG Entry Deletion

- DELENTRY name-n
- The named entry is deleted and the BUILD statement naming it is removed from the owning IDENTITY entry

SUBCONFIG Minidisk Management - Reaching the Unreachable



SUBCONFIG Minidisk Management

- Standard minidisk commands and screens manipulate SUBCONFIG entries – ADDMDISK, CHGMDISK, DELMDISK, DUPMDISK, TRANSFER, MANAGE
- Unreachable disks cannot be formatted. Use the Servant Facility or issue the VMSECURE command from a member node that can reach the disk.
- DUPMDISK cannot copy from a SUBCONFIG disk on one node to a SUBCONFIG disk on another node.
- Avoid having the same virtual address in an IDENTITY and its SUBCONFIG. It will just confuse you.

SUBCONFIG Minidisk Management – Keep it Simple

- All USER and IDENTITY minidisks on shared volumes
  - Linux guest disks must be on shared volumes for Live Guest Relocation
- Put SUBCONFIG minidisks on private volumes

SUBCONFIGs Cannot Be Used with Some Commands

Commands relating to USER attributes or Resource Access are not appropriate or permitted for SUBCONFIG entries.

— CLASS, EXPIRE, GENACI, GENHS, GENINCL, IPLDISKX, MULTIPLE, RULEMAP, RULES, PASSWORD, GETPWEXP, NOLOG, DELETE, ENROLL, MODIFY

VM:Secure Configuration for SSI

VMSECURE Server Directory Entry Changes

- IDENTITY VMSECURE *password* 64M 256M BEG
- BUILD ON *member1* USING SUBCONFIG VMSEC-1
- BUILD ON *member2* USING SUBCONFIG VMSEC-2
- IUCV *IDENT *resource* GLOBAL
- Add new 1B6 LOG Minidisk
  - (3 3390 cylinders, 4K blocksize, label LOG)

VM:Secure Configuration for SSI

VMSECURE Server Directory Entry MDISKs

- RR MDISKs on shared volumes
  - 192, 292, 492, 176, 276, 476, 293, 493
- MR MDISKs on shared volumes
  - 191, 194, 1B0, 1B1, 1B2, 1B3, 1B4, 1B6
- Member specific MDISKs (in SUBCONFIGs)
  - 1D0 AUDT minidisk

VM:Secure Configuration for SSI

VMSEC-n SUBCONFIG Entries

SUBCONFIG VMSEC-n

*** Audit Minidisk

MDISK 1D0 3390 28 2 SPACE6 MR

*** LINK or MDISK for Object Directory

LINK MAINT 123 1A0 MW

VM:Secure Configuration for SSI

VMSECURE PRODUCT CONFIG File Changes

- Define the SSI members to VMSECURE
  - SSINODE VMSYS01
  - SSINODE VMSYS02
- Use the DIRECT statement to define member specific Object Directory Volume Serials. Up to 4 *volser* are defined on the DIRECT statement.
  - DIRECT 1A0 M01RES M02RES
- Define APPC communications Resource Name
  - RESID *resource* GLOBAL

VM:Secure Configuration for SSI (continued)

VMSECURE PRODUCT CONFIG File Changes

- Define the LOG minidisk
  - ACCESS LOG 1B6 L

VM:Secure Configuration for SSI

IBM Requirements for External Security Managers

— The *ACI Exit Routines (HCPRPI and friends) MUST be identical in every SSI member node CPLOAD MODULE, or the members cannot join the complex.

Using VM:Secure for Conversion to SSI

- Procedures for converting from Non SSI to SSI enabled documented in the CA VM:Secure and VM:Director System Administrator guide.

- SSIENAB utility provided
  - retrieves the SSI member name from the running system, and converts all BUILD statements on the source directory minidisk from the form “BUILD ON *” to the form “BUILD ON membername” convert the source to SSI Enabled format.

Other CA VM Products and SSI

CA VM:Spool and SSI

- New release of CA VM:Spool - 1.8
  - Install as IDENTITY user for each system that requires its function
  - Spool files from other systems can be accessed as long as the owning user is logged on to the requesting system
  - For backup and accounting CA VM:Spool only works with spool files originating on the system where the service machine runs

CA VM:Spool V/SEG Plus and SSI

- New release of CA VM:Spool V/SEG Plus Feature – 1.7
  - Install as Identity user for each system that requires its function
  - Spool files from other systems can be accessed as long as the owning user is logged on to the requesting system
  - If Linux guest uses DCSSs and is to be relocated to another member of the SSI complex the same DCSS must exist on the other member
    - Use SPDISK utility to back up DCSS and restore it on another system

CA VM:Backup and SSI

- Informational solution for release 3.5 - RI37867
  - Describes how to set up and use VM:Backup in an SSI environment
    - Set up separate VM:Backup service virtual machines
      - USER entries vs. IDENTITY
        - Minidisks need to be on shared volumes
      - Set up one for backing up all minidisks on shared volumes
        - Can run on any member since captures shared volume minidisks
      - Set up additional server on each system to back up the minidisks that exist on volumes that are available to only one system
        - Must always run on the system the volumes being backed up exist on
      - All done with inclusion/exclusion features

CA VM:Backup HiDRO and SSI

- Informational solution for release 2.8 – RI38224
  - Describes how to set up and use CA VM:Backup HiDRO in an SSI environment
  - Same set up as CA VM:Backup
    - Multiple server sets (HIDRO, SYBMON and SYBCOM) vs. 1 server
    - Also normal USER entries with minidisk on shared dasd
    - One set to back up minidisks on shared volumes
    - Other sets to back up minidisks on volumes available to only one system
    - Also done with HiDRO flavor of inclusion/exclusion features

CA VM:Operator and SSI

- Informational solution for release 3.1 – RI37868
  - Describes how to set up and use CA VM:Operator in an SSI environment
    - IBM supplies OPERATOR virtual machine definition as an IDENTITY entry
    - Install VM:Operator into that environment
    - Steps given to get product installed and operational in this environment

CA VM:Tape and SSI

- Informational solution for release 2.0 – RI37869
  - Describes how to set up and use CA VM:Tape in an SSI environment
  - Allocate the server virtual machine as normal USER with all minidisks on shared dasd
  - Then convert directory entry to an IDENTITY adding BUILD and SUBCONFIG information for each member of the complex
    - Steps given to do this
  - Information also given for sharing TMCs and tape drives among systems
  - Set up information also supplied to enable Linux guests that use the VM:Tape Linux agent to run without interruption if relocated

Questions?

Thank you!