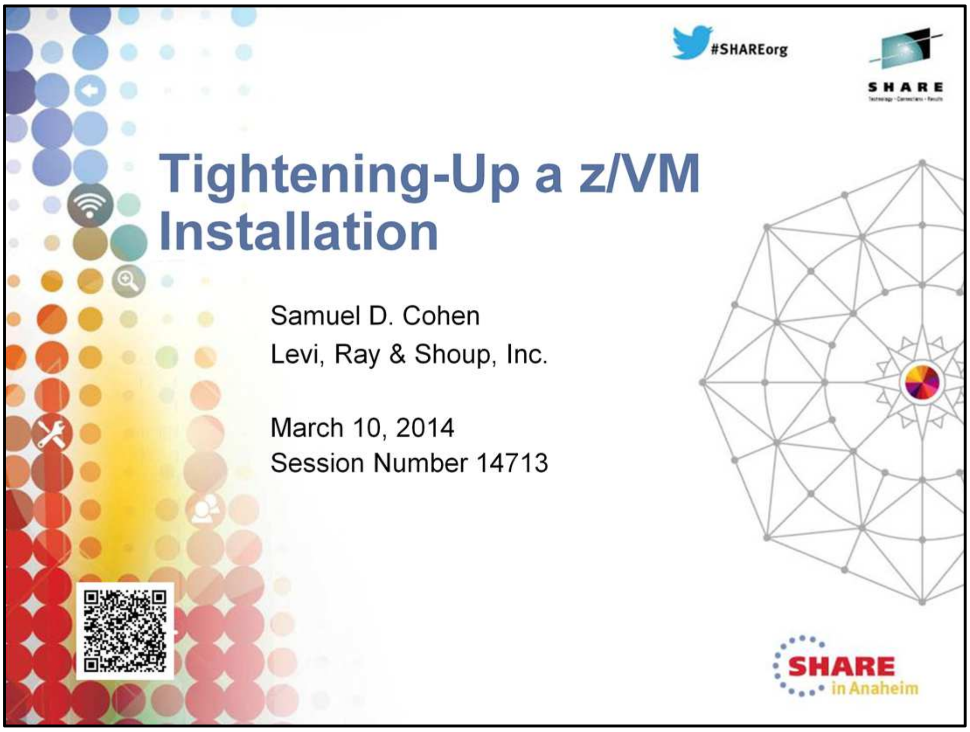


#SHAREorg

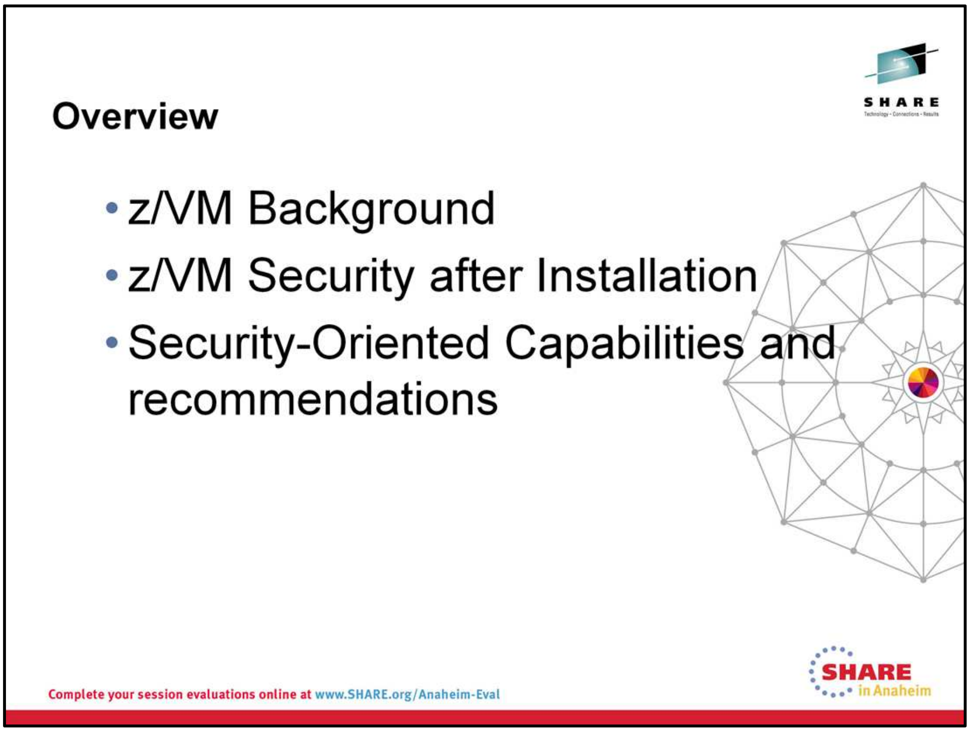
SHARE

Tightening-Up a z/VM Installation

Samuel D. Cohen
Levi, Ray & Shoup, Inc.

March 10, 2014
Session Number 14713

SHARE in Anaheim

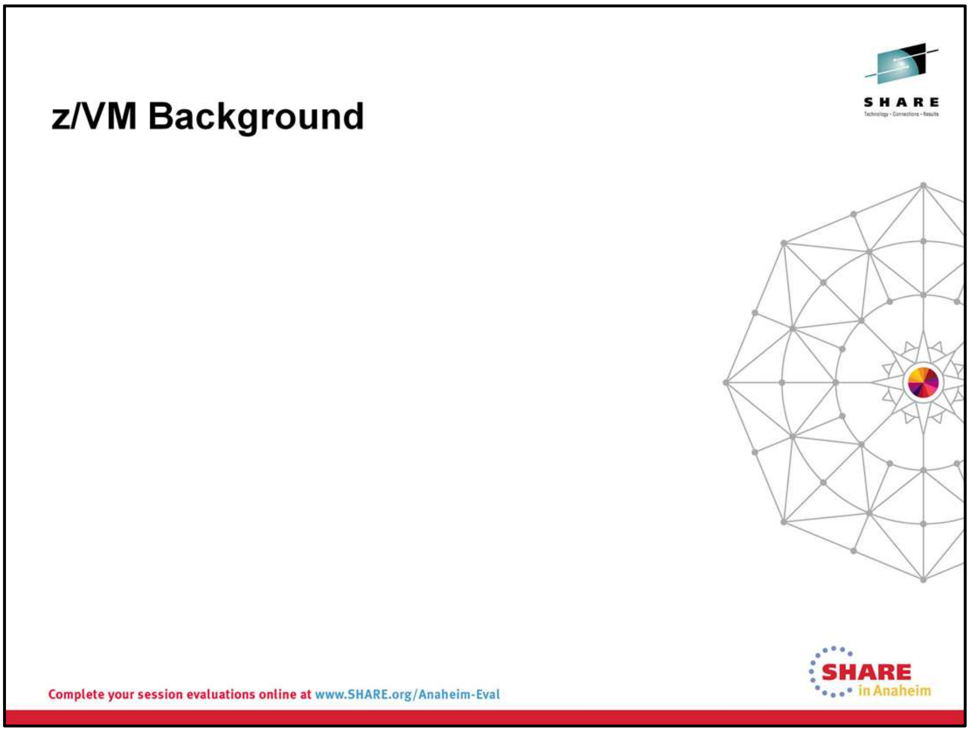


Overview

- z/VM Background
- z/VM Security after Installation
- Security-Oriented Capabilities and recommendations

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

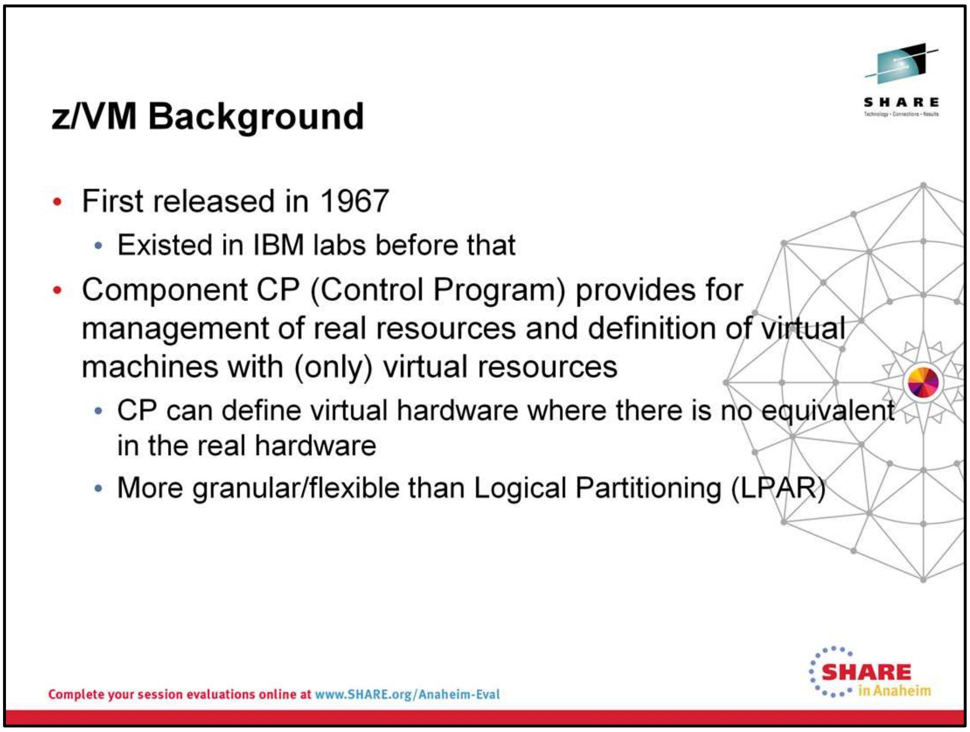
This session is not going to cover any particular Security Server from IBM or other vendors, it deals with the “native” capability of z/VM.



z/VM Background

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

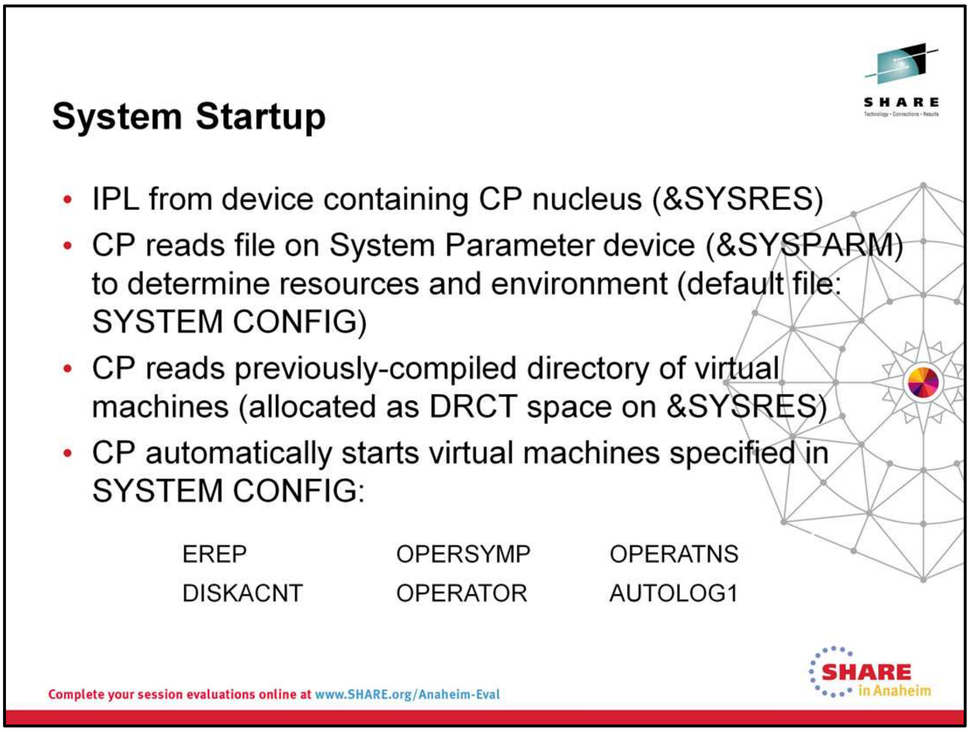
This section is a very brief summary of the Introduction to z/VM presentation available to SHARE participants



z/VM Background

- First released in 1967
  - Existed in IBM labs before that
- Component CP (Control Program) provides for management of real resources and definition of virtual machines with (only) virtual resources
  - CP can define virtual hardware where there is no equivalent in the real hardware
  - More granular/flexible than Logical Partitioning (LPAR)

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

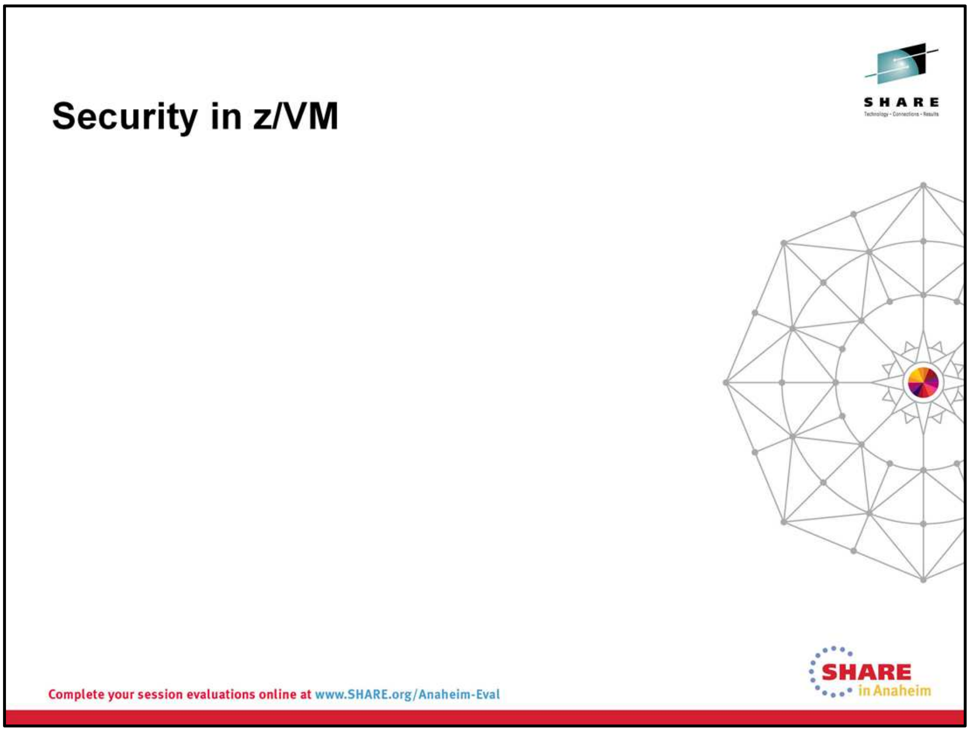


System Startup

- IPL from device containing CP nucleus (&SYSRES)
- CP reads file on System Parameter device (&SYSPARM) to determine resources and environment (default file: SYSTEM CONFIG)
- CP reads previously-compiled directory of virtual machines (allocated as DRCT space on &SYSRES)
- CP automatically starts virtual machines specified in SYSTEM CONFIG:

EREP
DISKACNT
OPERSYMP
OPERATOR
OPERATNS
AUTOLOG1

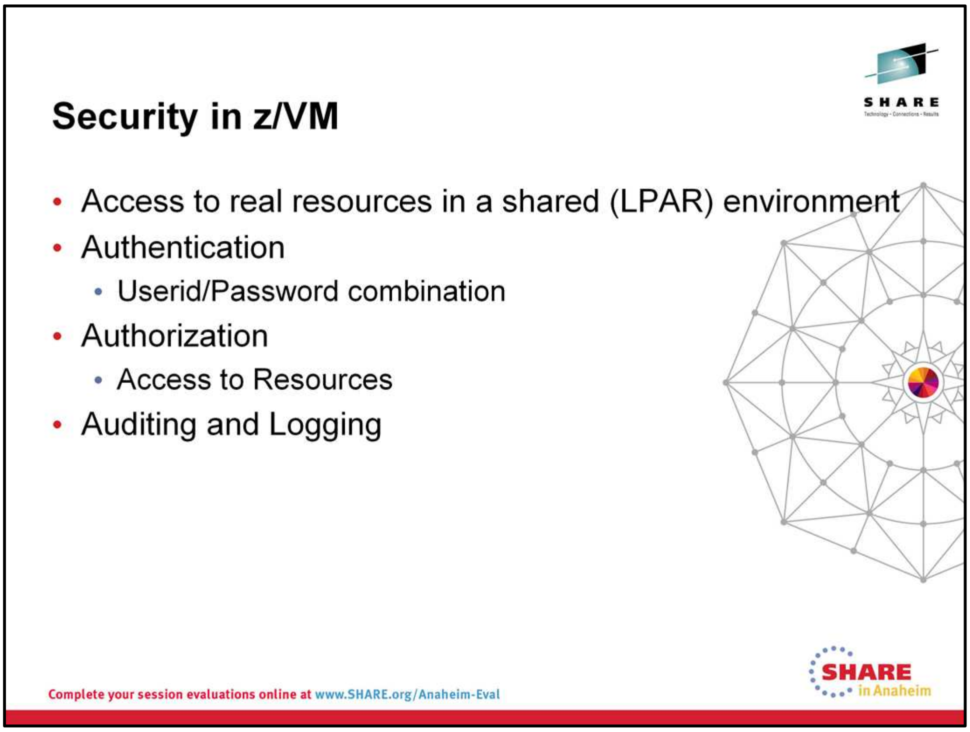
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



Security in z/VM

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

SHARE
Technology • Connections • Results
SHARE in Anaheim



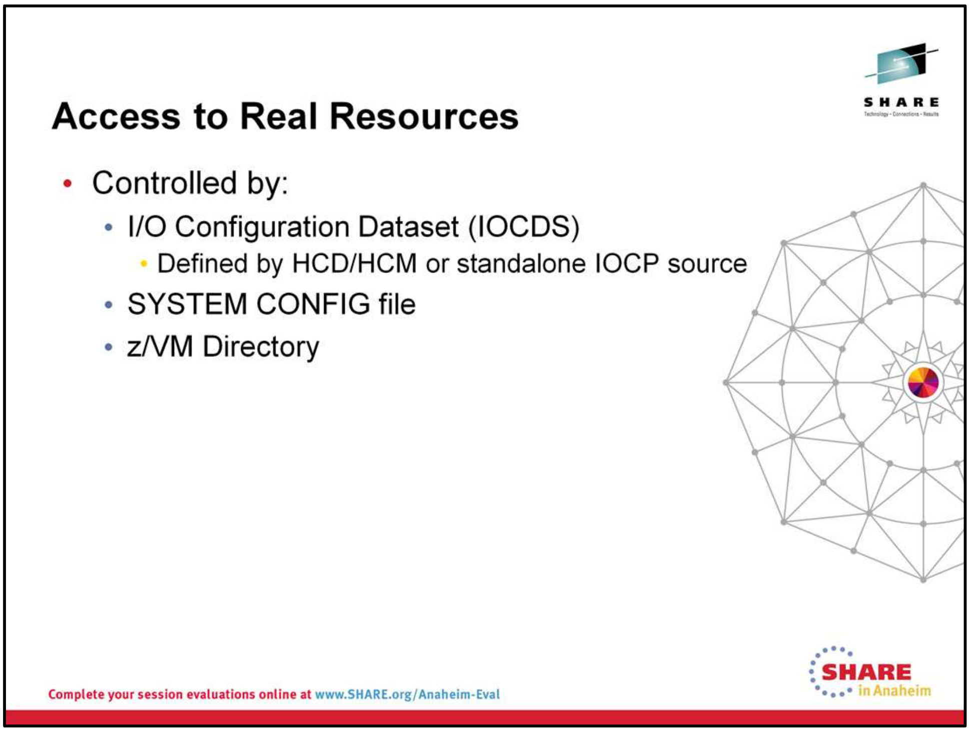
Security in z/VM

- Access to real resources in a shared (LPAR) environment
- Authentication
  - Userid/Password combination
- Authorization
  - Access to Resources
- Auditing and Logging

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

SHARE
Technology • Connections • Results
SHARE in Anaheim

Let’s start by defining “security” topics that will be covered.

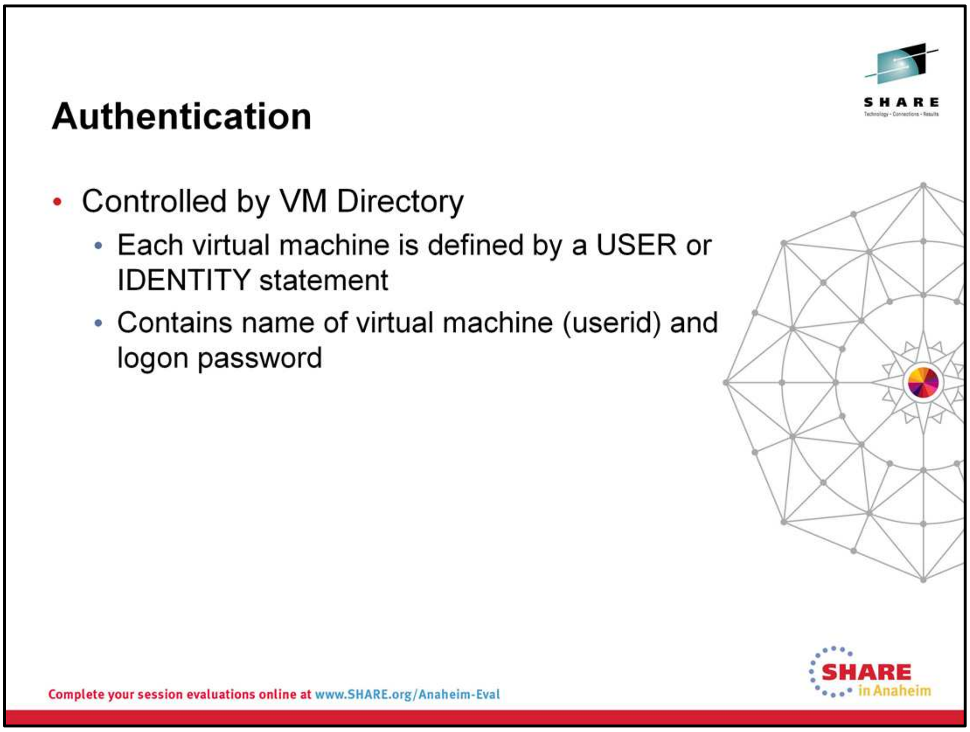


Access to Real Resources

- Controlled by:
  - I/O Configuration Dataset (IOCDS)
    - Defined by HCD/HCM or standalone IOCP source
  - SYSTEM CONFIG file
  - z/VM Directory

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

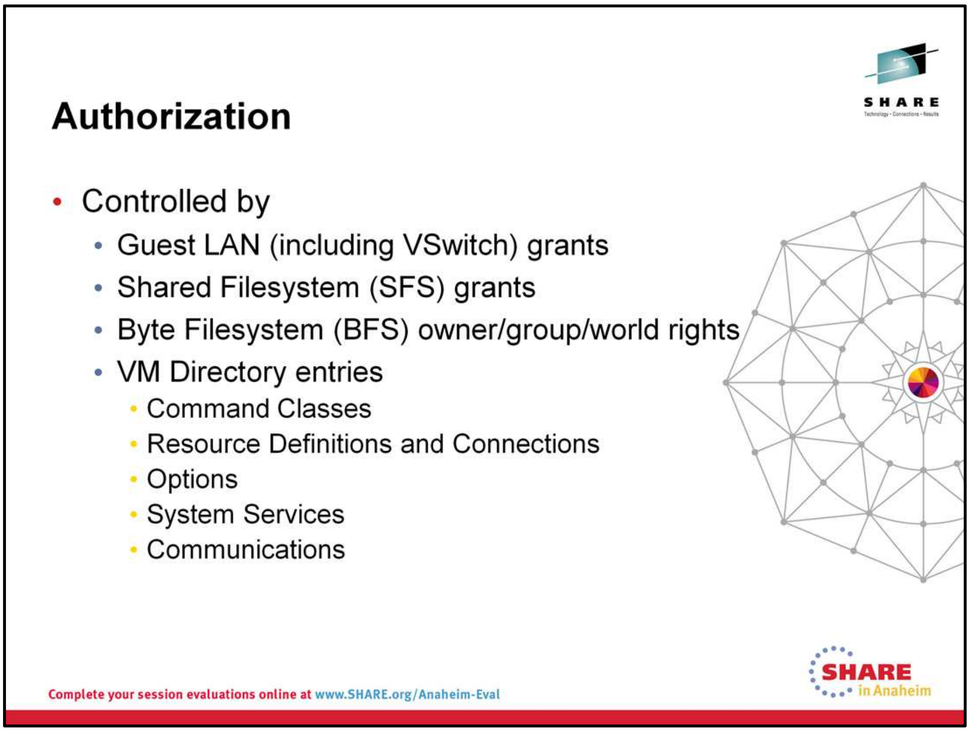
There is no requirement for an I/O Definition File (IODF) in z/VM, it is flexible enough to automatically add/delete devices upon a change to the IOCDS.



Authentication

- Controlled by VM Directory
  - Each virtual machine is defined by a USER or IDENTITY statement
  - Contains name of virtual machine (userid) and logon password

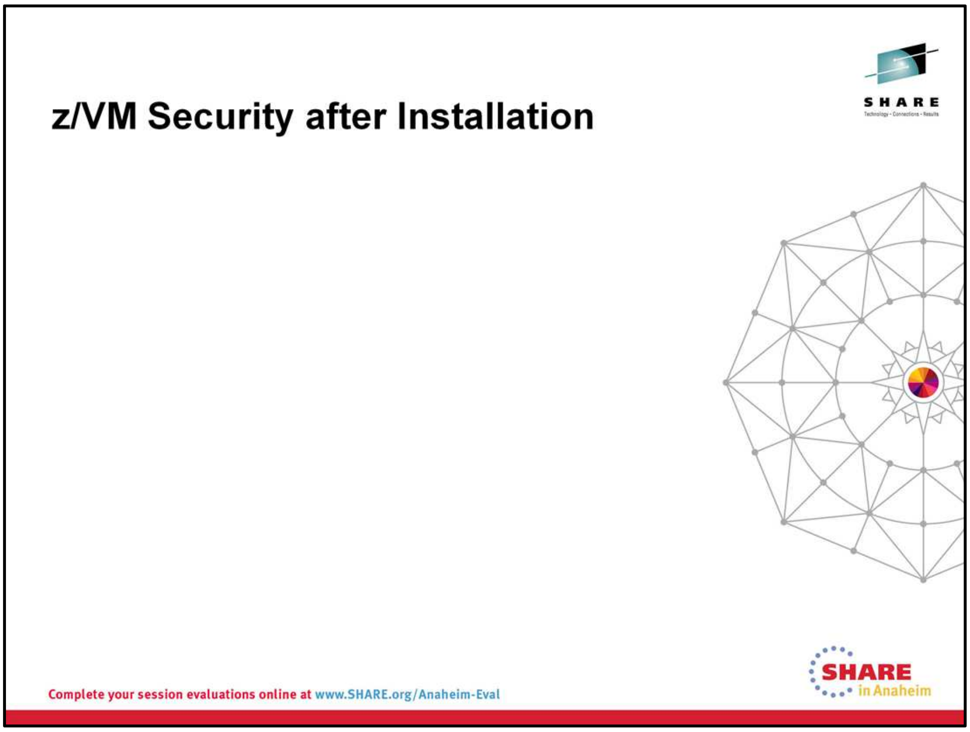
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



Authorization

- Controlled by
  - Guest LAN (including VSwitch) grants
  - Shared Filesystem (SFS) grants
  - Byte Filesystem (BFS) owner/group/world rights
  - VM Directory entries
    - Command Classes
    - Resource Definitions and Connections
    - Options
    - System Services
    - Communications

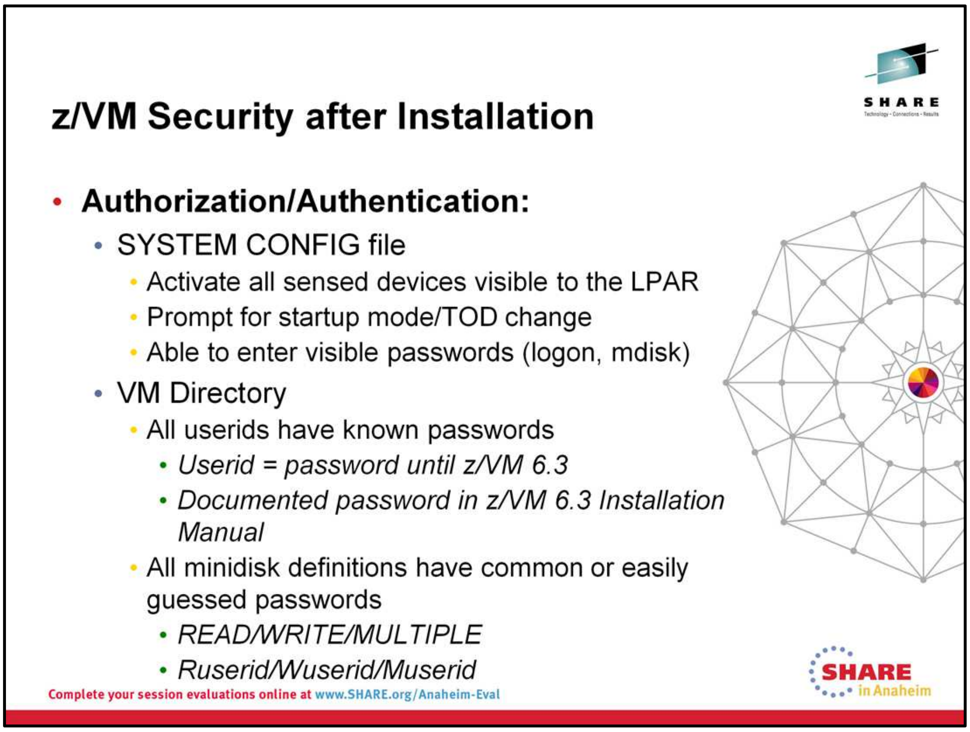
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



z/VM Security after Installation

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

SHARE
Technology • Connections • Results
SHARE in Anaheim

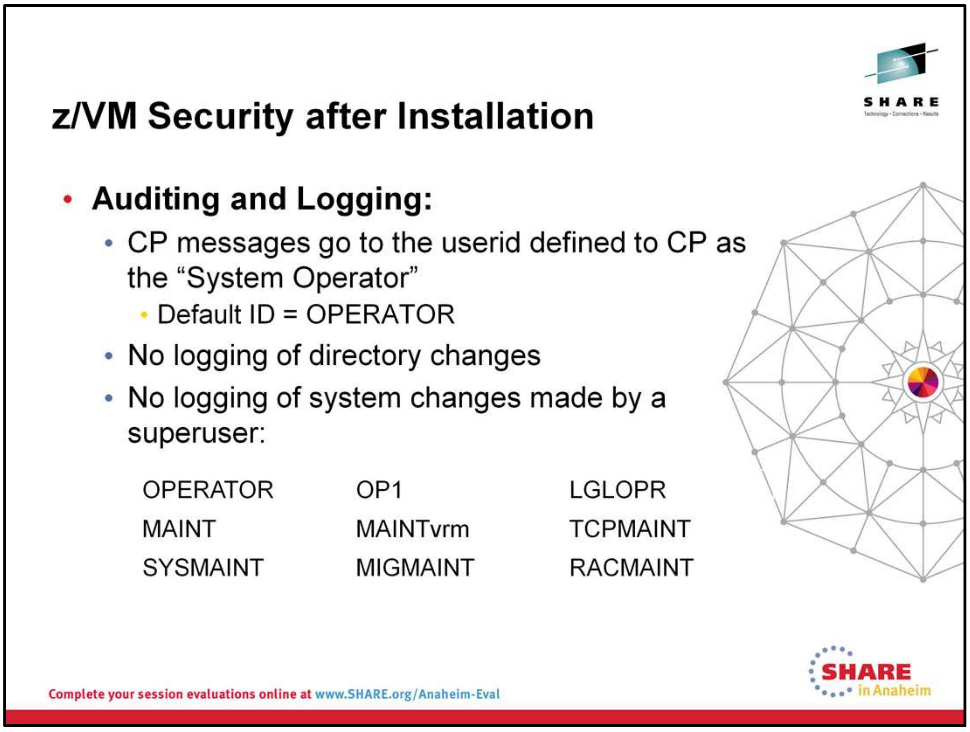


z/VM Security after Installation

- **Authorization/Authentication:**
  - SYSTEM CONFIG file
    - Activate all sensed devices visible to the LPAR
    - Prompt for startup mode/TOD change
    - Able to enter visible passwords (logon, mdisk)
  - VM Directory
    - All userids have known passwords
      - *Userid = password until z/VM 6.3*
      - *Documented password in z/VM 6.3 Installation Manual*
    - All minidisk definitions have common or easily guessed passwords
      - *READ/WRITE/MULTIPLE*
      - *Ruserid/Wuserid/Muserid*

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

There is no “TOD Enable” button on current hardware



z/VM Security after Installation

- **Auditing and Logging:**
  - CP messages go to the userid defined to CP as the “System Operator”
    - Default ID = OPERATOR
  - No logging of directory changes
  - No logging of system changes made by a superuser:

OPERATOR	OP1	LGLOPR
MAINT	MAINTvrm	TCPMAINT
SYSMAINT	MIGMAINT	RACMAINT

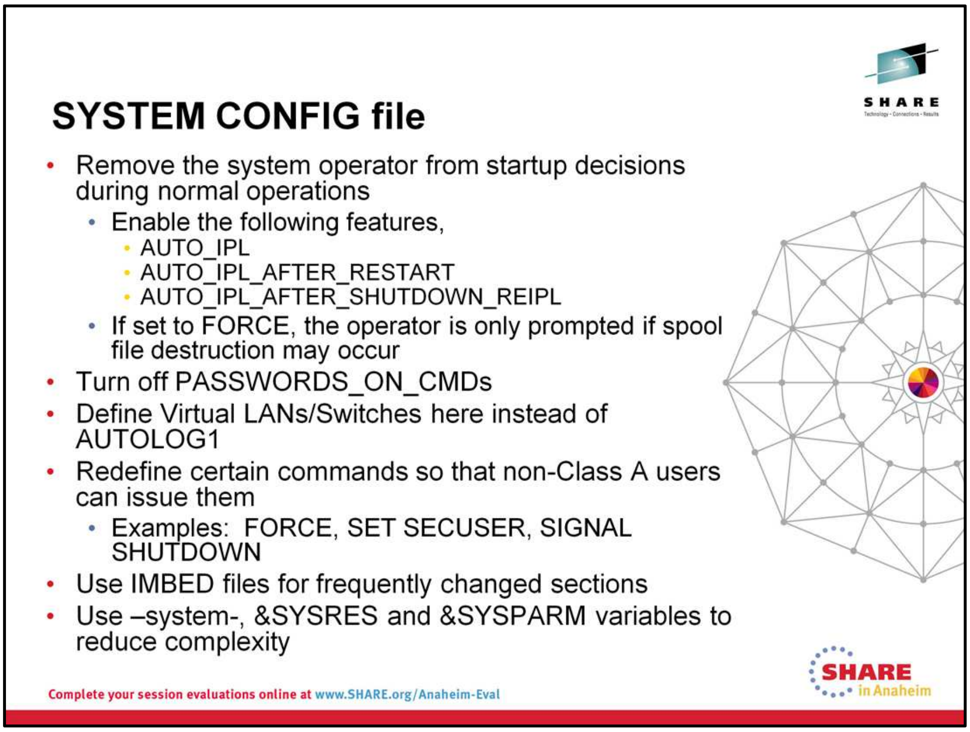
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

For purposes of this presentation, a “superuser” is a userid that has CP Class A authority and is not a service virtual machine.

Security-Oriented Recommendations

- SYSTEM CONFIG file
- VM Directory

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

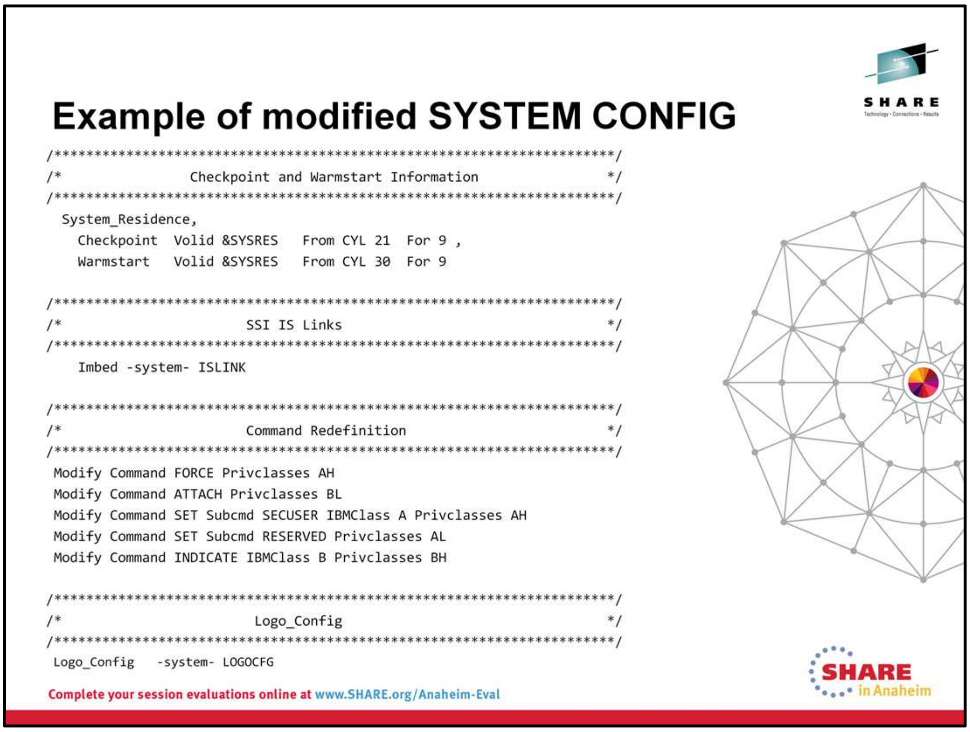


SYSTEM CONFIG file

- Remove the system operator from startup decisions during normal operations
  - Enable the following features,
    - AUTO_IPL
    - AUTO_IPL_AFTER_RESTART
    - AUTO_IPL_AFTER_SHUTDOWN_REIPL
  - If set to FORCE, the operator is only prompted if spool file destruction may occur
- Turn off PASSWORDS_ON_CMDs
- Define Virtual LANs/Switches here instead of AUTOLOG1
- Redefine certain commands so that non-Class A users can issue them
  - Examples: FORCE, SET SECUSER, SIGNAL SHUTDOWN
- Use IMBED files for frequently changed sections
- Use –system-, &SYSRES and &SYSPARM variables to reduce complexity

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

Recommendations are more “art” than “science”, but are based on a long history of implementations and multiple customer situations



Example of modified SYSTEM CONFIG

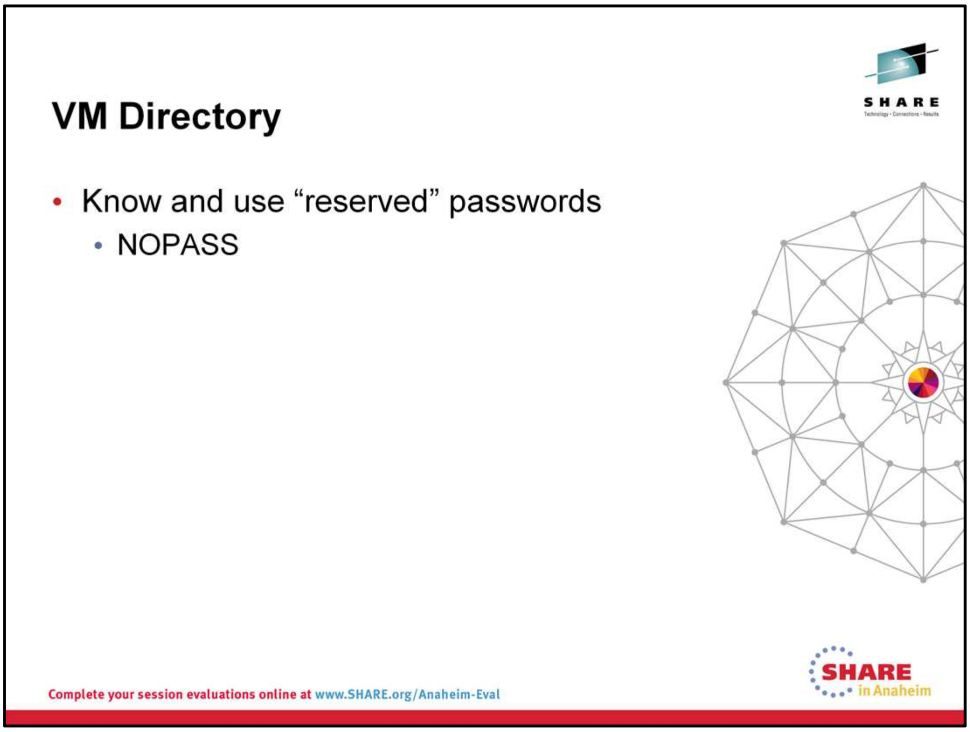
```
/**********************************************************************/
/*                Checkpoint and Warmstart Information                */
/**********************************************************************/
  System_Residence,
    Checkpoint  Volid &SYSRES   From CYL 21  For 9 ,
    Warmstart   Volid &SYSRES   From CYL 30  For 9

/**********************************************************************/
/*                       SSI IS Links                                 */
/**********************************************************************/
    Imbed -system- ISLINK

/**********************************************************************/
/*                       Command Redefinition                         */
/**********************************************************************/
 Modify Command FORCE Privclasses AH
 Modify Command ATTACH Privclasses BL
 Modify Command SET Subcmd SECUSER IBMClass A Privclasses AH
 Modify Command SET Subcmd RESERVED Privclasses AL
 Modify Command INDICATE IBMClass B Privclasses BH

/**********************************************************************/
/*                        Logo_Config                                 */
/**********************************************************************/
 Logo_Config   -system- LOGOCFG
```

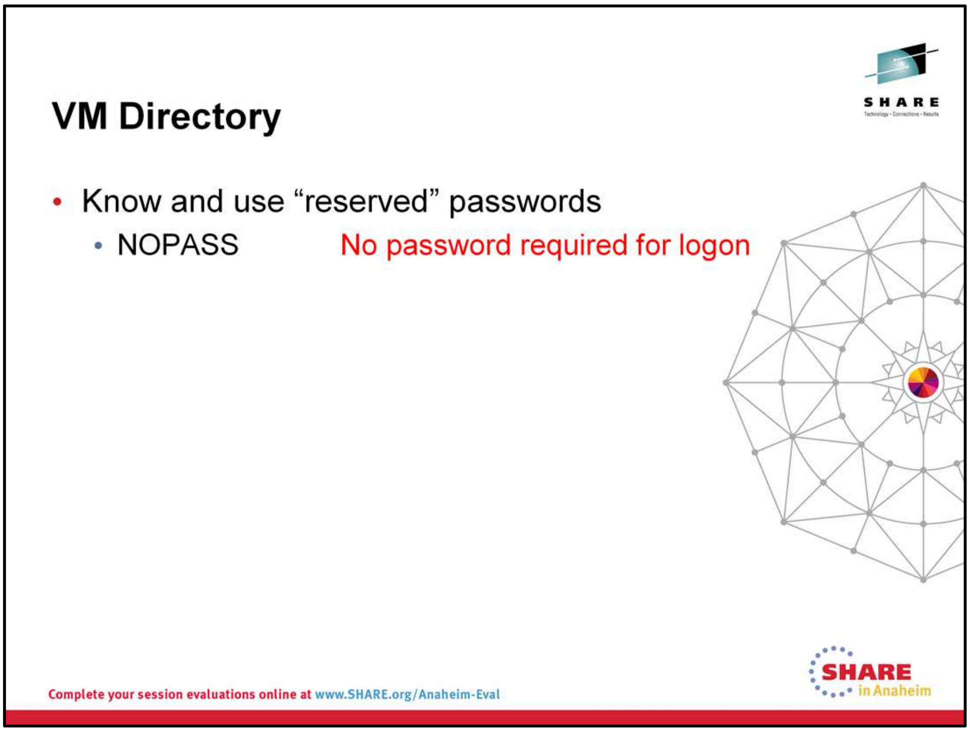
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



VM Directory

- Know and use “reserved” passwords
  - NOPASS

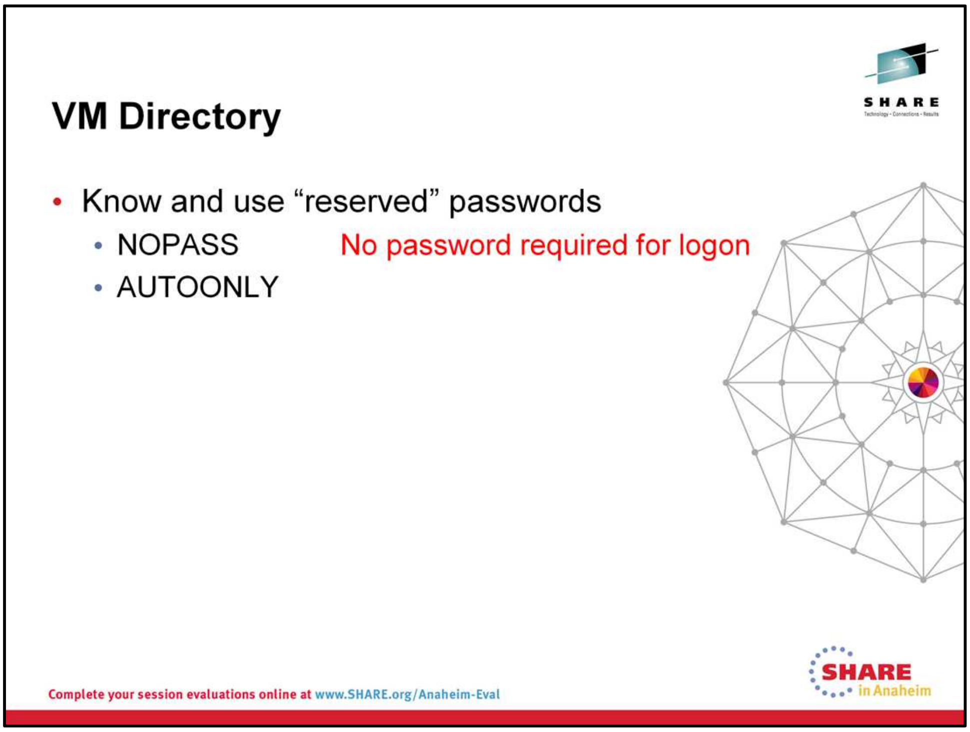
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



VM Directory

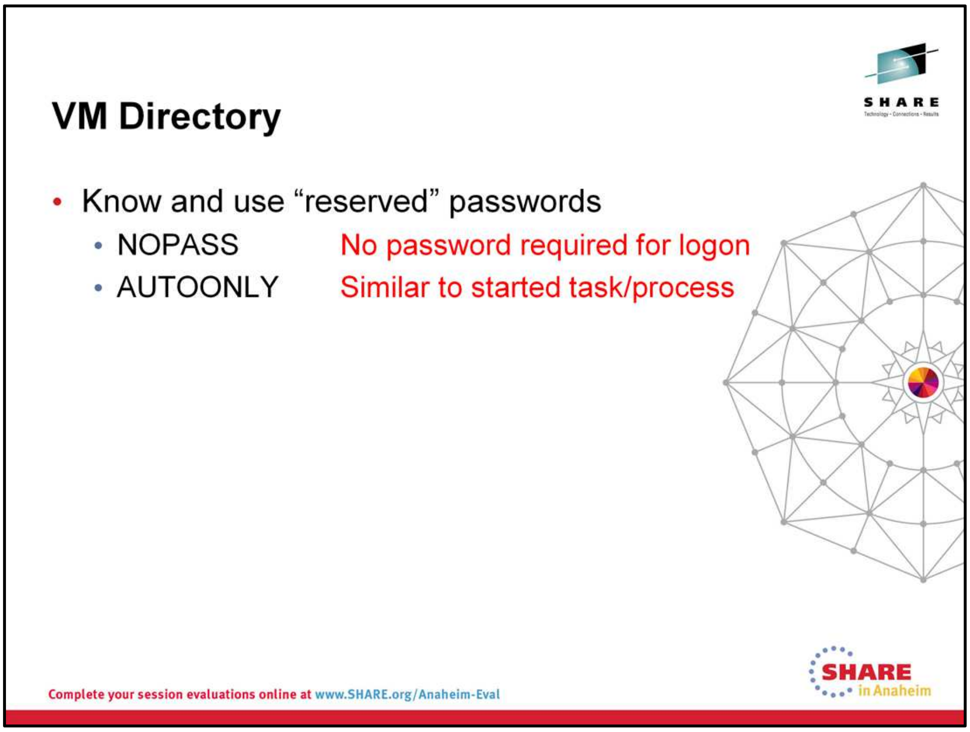
- Know and use “reserved” passwords
  - NOPASS No password required for logon

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



VM Directory

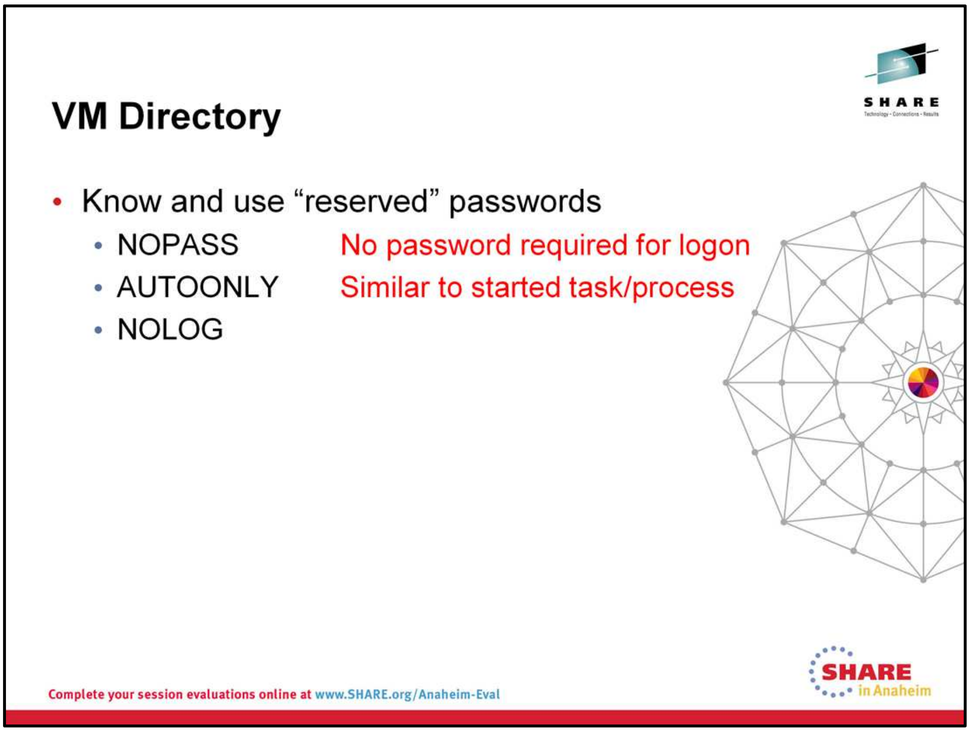
- Know and use “reserved” passwords
  - NOPASS No password required for logon
  - AUTOONLY



VM Directory

- Know and use “reserved” passwords
  - NOPASS No password required for logon
  - AUTOONLY Similar to started task/process

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

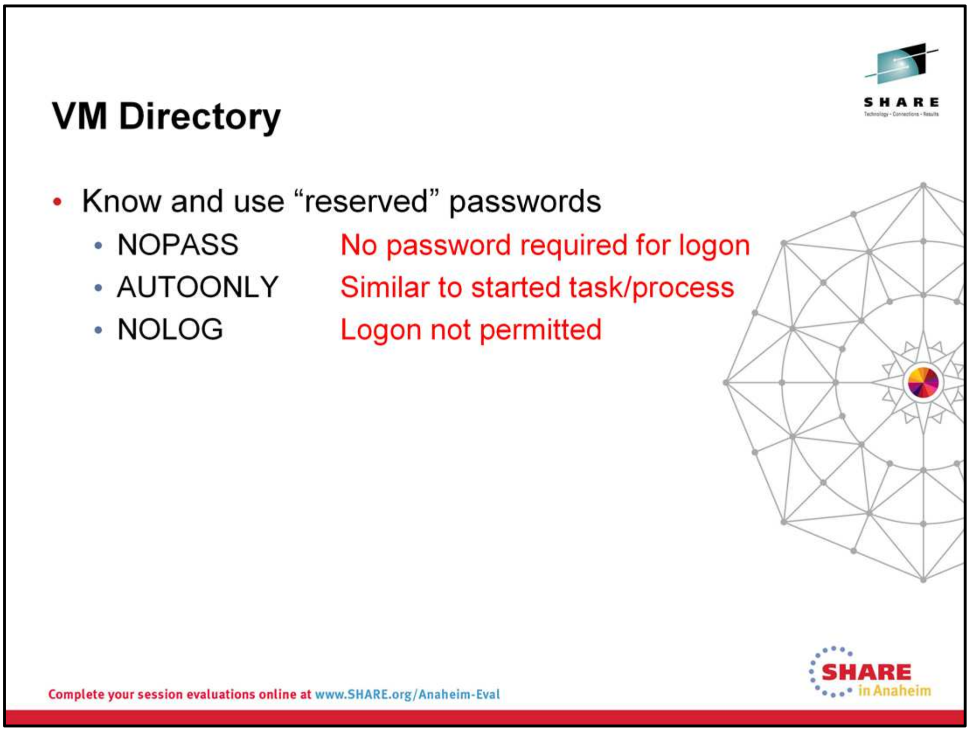


VM Directory

- Know and use “reserved” passwords

NOPASS	No password required for logon
AUTOONLY	Similar to started task/process
NOLOG	

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

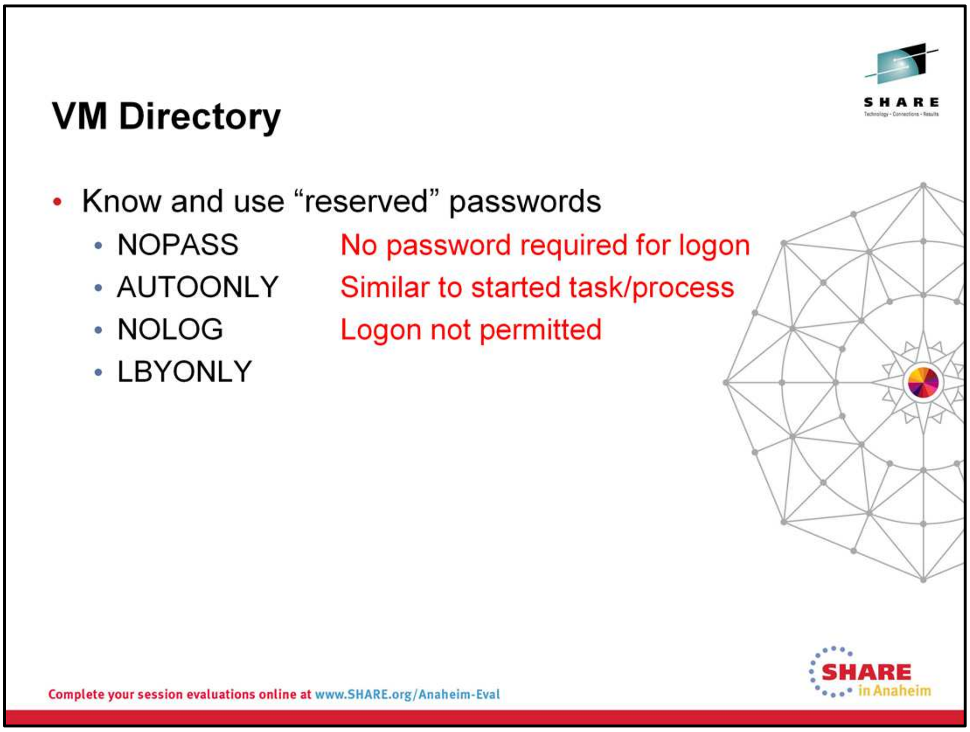


VM Directory

- Know and use “reserved” passwords

NOPASS	No password required for logon
AUTOONLY	Similar to started task/process
NOLOG	Logon not permitted

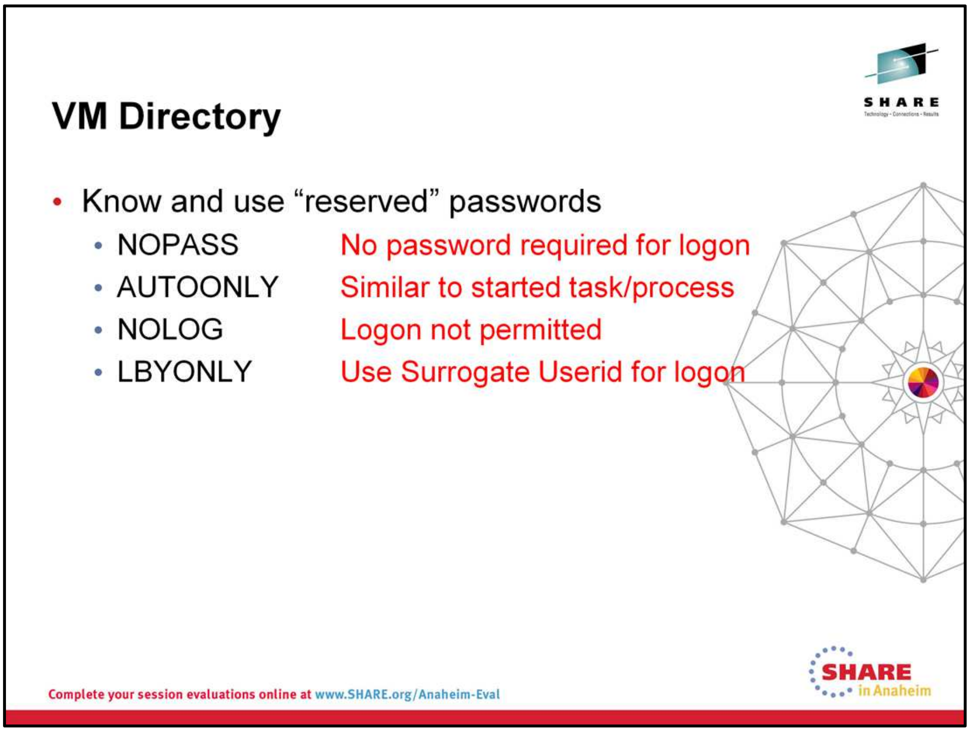
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



VM Directory

- Know and use “reserved” passwords
  - NOPASS   No password required for logon
  - AUTOONLY   Similar to started task/process
  - NOLOG   Logon not permitted
  - LBYONLY

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

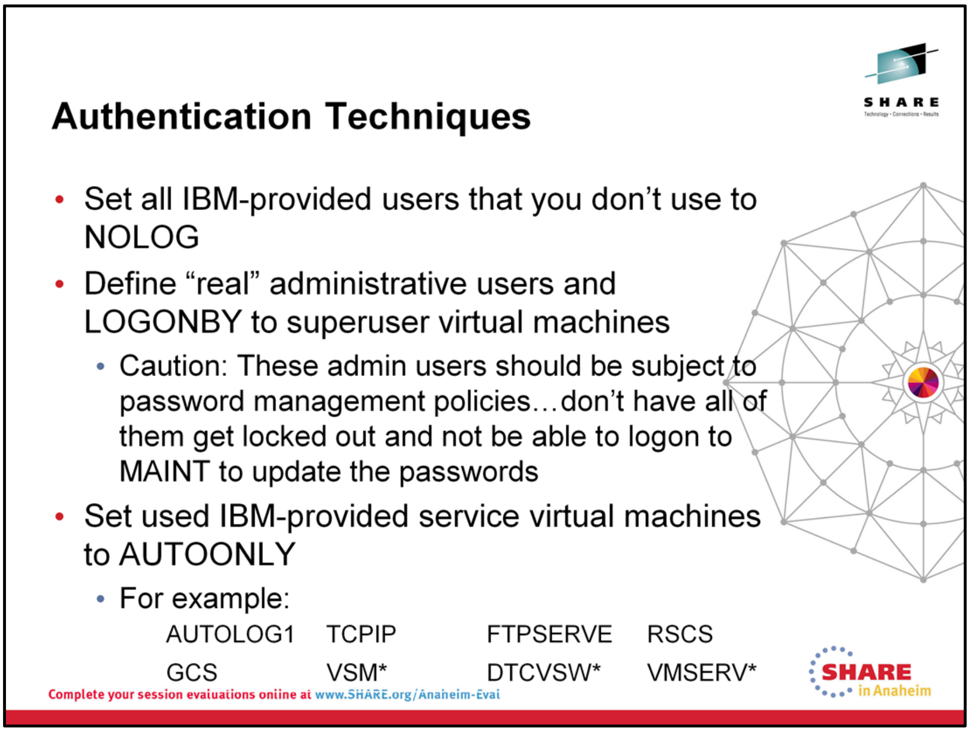


VM Directory

- Know and use “reserved” passwords

• NOPASS	No password required for logon
• AUTOONLY	Similar to started task/process
• NOLOG	Logon not permitted
• LBYONLY	Use Surrogate Userid for logon

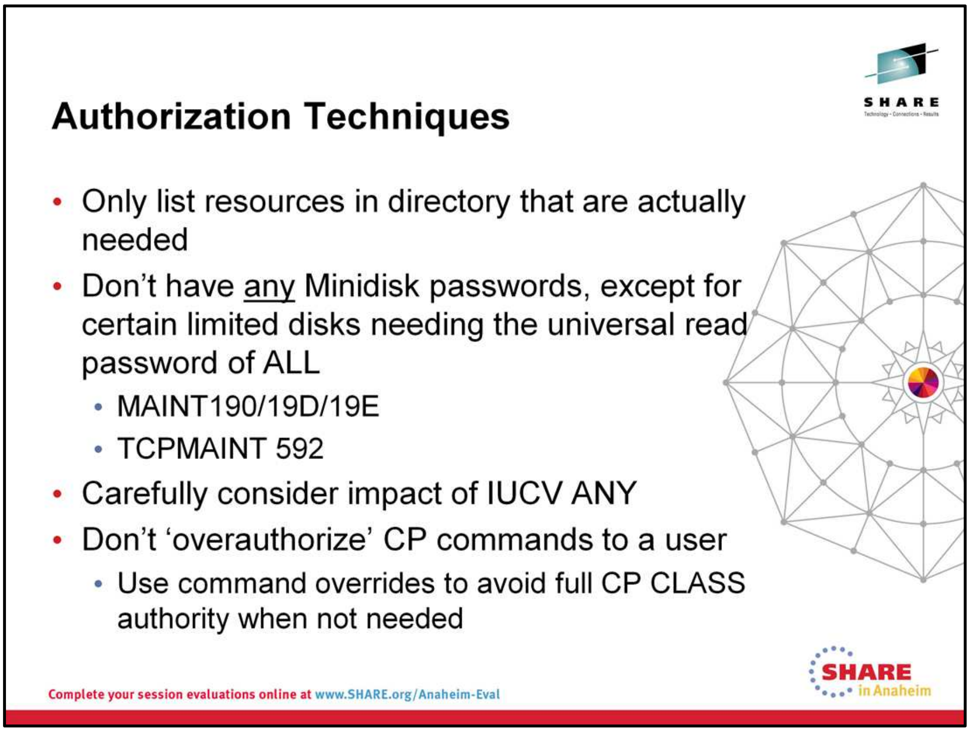
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



Authentication Techniques

- Set all IBM-provided users that you don't use to NOLOG
- Define "real" administrative users and LOGONBY to superuser virtual machines
  - Caution: These admin users should be subject to password management policies…don't have all of them get locked out and not be able to logon to MAINT to update the passwords
- Set used IBM-provided service virtual machines to AUTOONLY
  - For example:

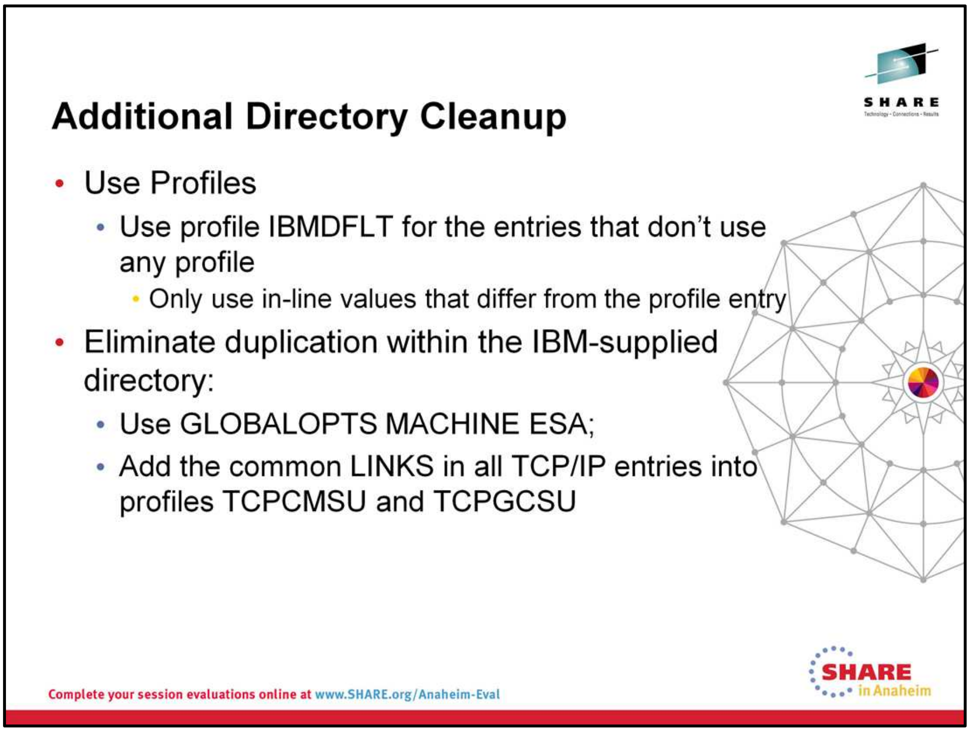
AUTOLOG1	TCPIP	FTPSERVE	RSCS
GCS	VSM*	DTCVSW*	VMSERV*



Authorization Techniques

- Only list resources in directory that are actually needed
- Don't have any Minidisk passwords, except for certain limited disks needing the universal read password of ALL
  - MAINT190/19D/19E
  - TCPMAINT 592
- Carefully consider impact of IUCV ANY
- Don't 'overauthorize' CP commands to a user
  - Use command overrides to avoid full CP CLASS authority when not needed

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

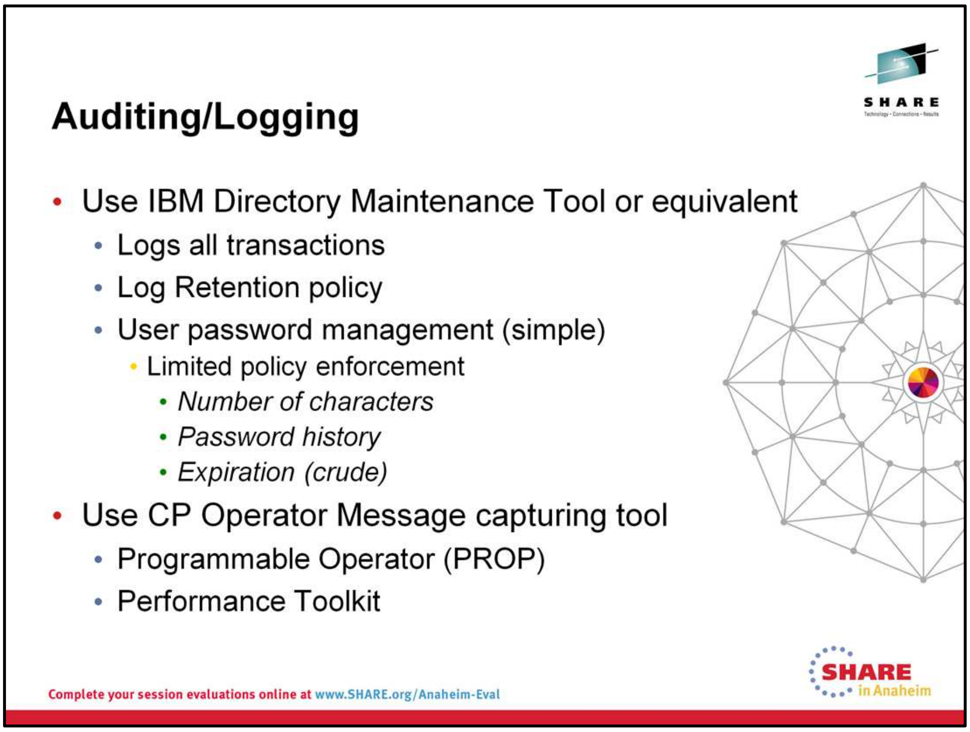


Additional Directory Cleanup

- Use Profiles
  - Use profile IBMDFLT for the entries that don’t use any profile
    - Only use in-line values that differ from the profile entry
- Eliminate duplication within the IBM-supplied directory:
  - Use GLOBALOPTS MACHINE ESA;
  - Add the common LINKS in all TCP/IP entries into profiles TCPCMSU and TCPGCSU

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval

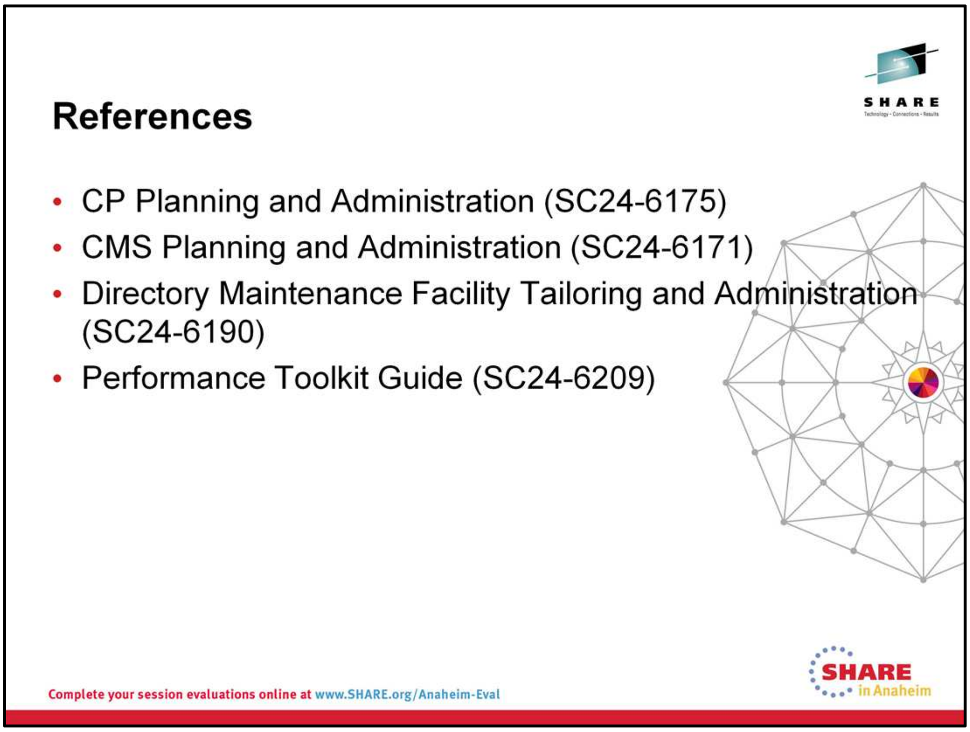
While these cleanup steps are not necessary, they reduce the size of the compiled directory and reduce complexity by eliminating information that already exists in a directory profile.



Auditing/Logging

- Use IBM Directory Maintenance Tool or equivalent
  - Logs all transactions
  - Log Retention policy
  - User password management (simple)
    - Limited policy enforcement
      - *Number of characters*
      - *Password history*
      - *Expiration (crude)*
- Use CP Operator Message capturing tool
  - Programmable Operator (PROP)
  - Performance Toolkit

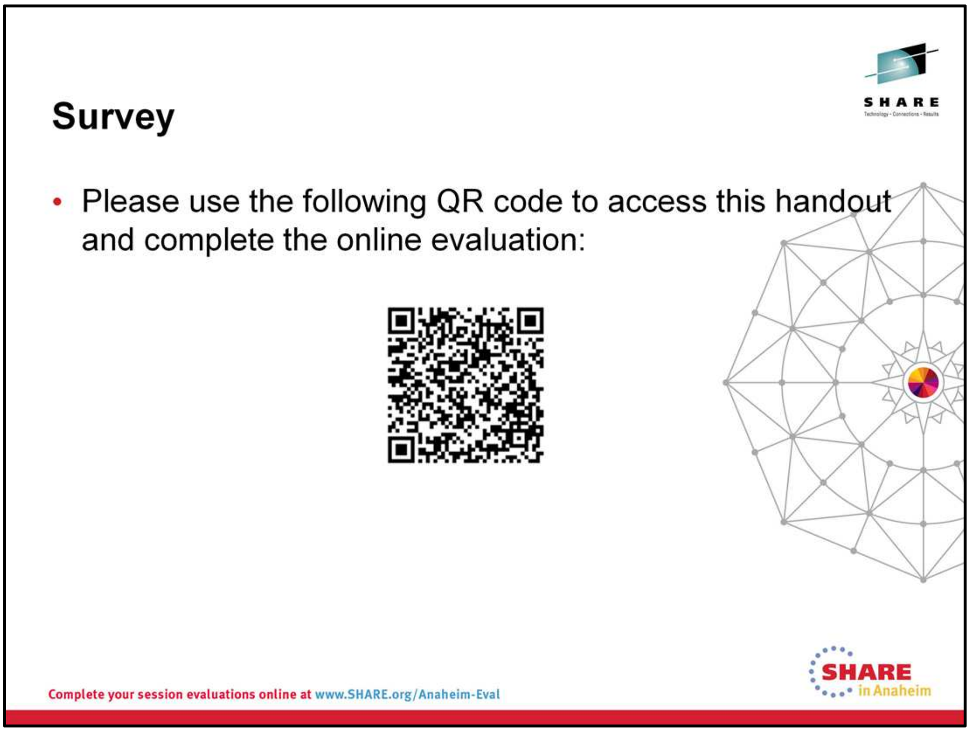
Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



References

- CP Planning and Administration (SC24-6175)
- CMS Planning and Administration (SC24-6171)
- Directory Maintenance Facility Tailoring and Administration (SC24-6190)
- Performance Toolkit Guide (SC24-6209)

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval



Survey

- Please use the following QR code to access this handout and complete the online evaluation:

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval