The Seriousness of Securing your z/VM Environment Using Audit Data

MVMUA

Brian Jagos

Email: Brian.Jagos@Broadcom.com

Date: April 21st

Time: 09:00am

Abstract

Do I really want to go to jail? Do I want to be on the cover of the New York Times or CNN and not in a good way? Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in numbers. We are going to talk about in this session audit records and where to get them, and what to look for.

Why should you care

Software is properly functioning, meeting standard criteria, and adhering to your legal guidelines

Industry Guidelines

- PCI-DSS, HIPAA, GDPR

Internal Audit Compliance

- Proprietary data and it's protection
  - Contact information, Credit Card Numbers, Employees salaries, SSN…
- Avoid Fines and other penalties
- Eliminate the risk of compromised or pillaged Software
- Stay out of the news

"Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the numbers."
"cybercrime will cost the world $6 trillion annually by 2021"

2019: Cybersecurity Ventures

Times are changing

SHARE
EDUCATE • NETWORK • INFLUENCE

We've heard so many customers say:

- We always pass our audits so we're OK
- We don't have time or resources
- They've never asked for this before

Auditors are asking different questions:

- Do I have the information? If you are not sure just ask us

"People are always asking, where do I find information for ESM events or directory changes. I tell them, in the AUDIT data. It holds the history of all ESM and directory events on your system. If you archive it you will always know what happened on any particular day/time."

2019: Yvonne DeMeritt (Broadcom)

ESM Audit Data

When Auditing is turned on in your configuration (by default it's **NOT** turned on)

VERIFY THE EFFECTIVENESS OF YOUR SECURITY

Identifies that rules / authorities are setup correctly

- Validates authenticated users
- Protects against corruption

ENSURE SECURITY OBJECTIVES / GUIDELINES ARE MET

Pass internal system audits

- Documentation of events / changes that have occurred

DISCOVERY WHEN "STUFF" HAPPENS

Unexpected security related events

EEEEKKKK!!!!!

- Data gone BAD!
- Tapes that have gone missing!

For further help:

Check with your ESM documentation or support for audit options and selections

Historical data to help with your audits

SHARE
EDUCATE • NETWORK • INFLUENCE

Archiving audit data means archiving system event history

Capture event activity not found anywhere else

- When a user is created or deleted
- History of access to all resources
- Password change information
- Rules/permission change information
- When minidisks are created, moved or deleted
- …

Audit INSIGHTS

If it can happen, it probably will

SHARE
EDUCATE • NETWORK • INFLUENCE

Something unexpected happens on your system that requires looking at residual data evidence to determine what happened and why

-
- Users that haven't logged on to your system for months are suddenly being journaled out for invalid passwords. Where do you find out more about these attempted logons?
-
- A new user is being autologged and running applications that are wreaking havoc with system performance. You find out the system administrator didn't create that user. Who did and what is that user doing?
-
- A production database disk is damaged and data lost. How did that happen and who did it?

How to find out about what happened

Be Proactive versus Reactive

Know before CNN or the NY Times knows

- ESM audit data can tell you about logon attempts and users being logged on to the system
- ESM and/or directory management audit data can tell you about how users and resources are being created and who did it.
- ESM audit data can tell if and when a disk was linked write that may have caused destruction of the production database disk
- Directory management audit data can tell you if a minidisk overlay was created that may have caused the destruction of the production database disk

What audit data is provided by your ESM on z/VM

Everything the ESM protects results in **audit data**

Security Manager

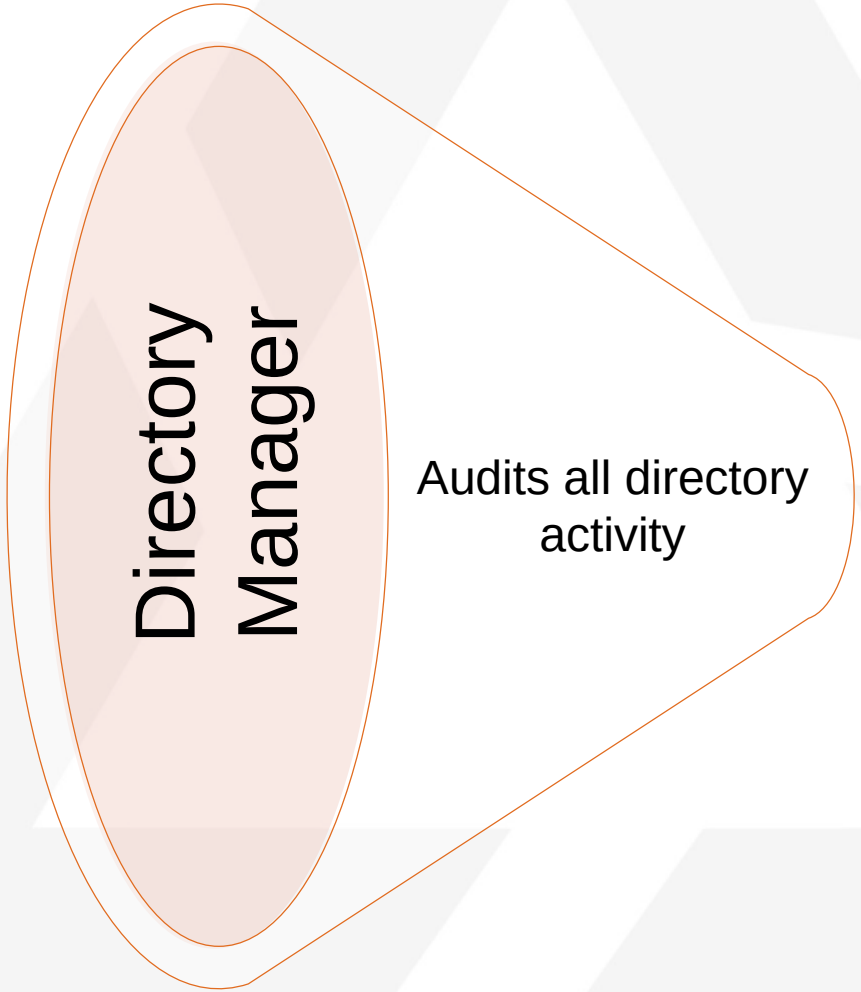
Pay a lot of attention to successions of failed attempts – this may help detect a possible intruder

Audit Data Examples:

- Logons
- Minidisk links
- COUPLE
- Rules or permission updates
- Command or application use
- Password changes

What audit data is provided by your Directory Manager on z/VM

Everything the Directory Manager executes results in **audit data**



Audit Data Examples:

- When users are created/deleted
- When users are modified or has resources added
- When a directory link is created
- When configuration changes occur

CA VM:SECURE

VM:Secure ESM audit data

SHARE
EDUCATE • NETWORK • INFLUENCE

Where is the audit data?

- Audit data is collected on VM:Secure 1D0 disk
  - Enabled through the ACCESS AUDT configuration file record
- For SSI each VM:Secure has it's own audit disk
  - Master VM:Secure audits all directory associated items
  - Master and agents audit CP resource access on their 1D0
- Warnings generated when the disk is getting full – if the disk becomes full – an audit record is punched to the reader versus being lost entirely

VM:Secure ESM audit data

SHARE
EDUCATE • NETWORK • INFLUENCE

What can I do with it?

- Extract and archive:
  - Use AUDITEXT to extract the data and clear the disk
  - We recommend you extract and archive daily to keep information in a daily packet
- Report on the contents:
  - Can proactively provide vital information

What do I use to report on it?

- Canned reports are included (User Exit allows for customer records selection)
  - VMXSRA/VMXSRB (Security reports)
- Create custom reports via VMRGRW (VM Product Manager Generalized Report Writer)
- Flat files can be interpreted and data reported based on your requirements
  - Layouts provided in product documentation
  - Possibility of creating SMF style records and shipping to z/OS for inclusion in reports

Sample: VMXSRA Security Report Output

```
REPORTA   EDLINKS   A1   F 133   Trunc=133 Size=154 Line=14 Col=1 Alt=11

          VM:Secure (R)  Copyright (c) 2016 CA. All rights reserved
                      CP Command Audit - All Link Commands
                   FROM            ISSUING  TARGET   MDSK LINK REASON
DATE      TIME     TERMINAL        USERID   USERID   ADDR MODE REJECTED
_________ ________ _______________ ________ ________ ____ ____ ________
06/26/19 08:08:28 0020            VMUID12  MAINT    190  RR
06/26/19 08:08:28 0020            VMUID12  MAINT    19D  RR
06/26/19 08:08:28 0020            VMUID12  MAINT    19E  RR
06/26/19 08:08:28 0020            VMUID12  VMUID20  997  RR
06/26/19 08:08:28 0020            VMUID12  VMANAGER 193  RR
06/26/19 11:35:35 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 11:47:33 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 11:55:20 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 11:57:59 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 11:58:10 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 11:59:48 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 12:01:09 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 12:30:23 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 12:40:32 DSC             VMX$0002 VMSECURE 194  RR
06/26/19 15:30:48 DSC             VMX$0002 VMSECURE 194  RR
06/27/19 09:53:51 0020            VMUID12  MAINT    190  RR
06/27/19 09:53:51 0020            VMUID12  MAINT    19D  RR
06/27/19 09:53:51 0020            VMUID12  MAINT    19E  RR
06/27/19 09:53:51 0020            VMUID12  VMUID20  997  RR
06/27/19 09:53:51 0020            VMUID12  VMANAGER 193  RR
06/27/19 10:47:22 DSC             VMX$0002 VMSECURE 194  RR
06/27/19 10:52:59 DSC             VMX$0002 VMSECURE 194  RR
06/27/19 12:46:30 DSC             VMX$0002 VMSECURE 194  RR
====>
                                                    X E D I T   1 File
```

Provides audit information for all CP command activity covered by VM:Secure rules:

- AUTOLOG/XAUTOLOG
- DIAL
- LINK
- LOGON
- SPOOL
- STCP
- STORE
- TAG
- COUPLE
- ATTACH
- FOR
- TRSOURCE
- RDEVCTRL.

Sample: VMXSRA Security Report LOGONS

```
REPORTA   LOGONS   A1   F 133   Trunc=133 Size=39 Line=14 Col=1 Alt=16

          VM:Secure (R)  Copyright (c) 2016 CA. All rights reserved
                      CP Command Audit - All Logon Commands

                     FROM            ISSUING   TARGET    REASON
DATE      TIME       TERMINAL        USERID    USERID    REJECTED
_________ _________  ______________  ________  ________  ________
07/12/19  11:04:01   0020            VMUID12   VMUID12
07/12/19  11:22:18   0021            VMSCHED   VMSCHED   PASSWORD
07/12/19  11:22:25   0021            VMSCHED   VMSCHED
07/12/19  15:45:03   0020            VMANAGER  VMANAGER
07/15/19  13:30:25   0020            VMUID12   VMUID12   PASSWORD
07/15/19  13:30:29   0020            VMUID12   VMUID12
07/15/19  13:41:33   0023            MAINT     MAINT     PASSWORD
07/15/19  13:41:38   0023            MAINT     MAINT     PASSWORD
07/15/19  13:41:47   0023            MAINT     MAINT     PASSWORD
07/15/19  13:41:54   0023            MAINT     MAINT     PASSWORD
07/15/19  13:42:08   0023            MAINT     MAINT     RULE
07/15/19  13:42:33   0022            MAINT640  MAINT640  PASSWORD
07/15/19  13:42:45   0022            MAINT     MAINT     PASSWORD
07/15/19  13:42:56   0022            MAINT     MAINT     PASSWORD
07/15/19  13:43:03   0022            MAINT     MAINT     PASSWORD
07/15/19  14:00:26   0022            MAINT640  MAINT640  RULE
07/15/19  14:05:19   0022            VMANAGER  VMANAGER  RULE
07/15/19  14:05:35   0021            VMANAGER  VMANAGER  PASSWORD
07/15/19  14:05:38   0021            VMANAGER  VMANAGER  PASSWORD
07/15/19  14:05:44   0021            MAINT640  MAINT640  PASSWORD
07/15/19  14:05:51   0021            MAINT640  MAINT640  PASSWORD
07/15/19  14:06:05   0021            VMANAGER  VMANAGER  RULE
====>
                                                         X E D I T   1 File
```

Issue

Note all of the attempts to logon to privileged user IDs that ended up rejected due to an invalid password, or a rule put in place after the configured number of invalid passwords were attempted.

Action

Follow up to determine cause of activity.
Is this an attempt to hack into your system on a privileged user ID?
Be suspicious. Better be safe than sorry.

Sample: VMXSRA Security Report COUPLE

```
REPORTA   COUPLE   A1   F 133   Trunc=65 Size=24 Line=14 Col=1 Alt=26

     VM:Secure (R)  Copyright (c) 2016 CA. All rights reserved
                 CP Command Audit - All Couple Commands
                   FROM       ISSUING    LAN        LAN        REASON
DATE      TIME     TERMINAL   USERID     OWNER      NAME       REJECT

07/17/19 16:31:17 0020       VMUID12    SYSTEM     INTRAV6
07/17/19 16:31:17 0020       VMUID12    SYSTEM     INTRA059
07/19/19 13:09:49 0020       VMUID12    SYSTEM     INTRAV6
07/19/19 13:09:49 0020       VMUID12    SYSTEM     INTRA059
07/22/19 13:41:32 0020       VMUID12    SYSTEM     INTRAV6
07/22/19 13:41:32 0020       VMUID12    SYSTEM     INTRA059
07/23/19 09:21:09 0020       VMUID12    SYSTEM     INTRAV6
07/23/19 09:21:09 0020       VMUID12    SYSTEM     INTRA059
07/24/19 11:14:16 0020       VMUID12    SYSTEM     INTRAV6
07/24/19 11:14:16 0020       VMUID12    SYSTEM     INTRA059
07/24/19 16:12:01 0021       VMUID20    SYSTEM     INTRAV6    RULE
07/24/19 16:12:01 0021       VMUID20    SYSTEM     INTRAV6    RULE
07/24/19 16:12:01 0021       VMUID20    SYSTEM     INTRAV6    RULE
07/24/19 16:12:01 0021       VMUID20    SYSTEM     INTRAV6    RULE
07/24/19 16:12:01 0021       VMUID20    SYSTEM     INTRAV6    RULE
07/24/19 16:12:01 0021       VMUID20    SYSTEM     INTRAV6    RULE
07/24/19 16:12:01 0021       VMUID20    SYSTEM     INTRAV6    RULE
07/24/19 16:12:02 0021       VMUID20    SYSTEM     INTRAV6    RULE
07/24/19 16:12:02 0021       VMUID20    SYSTEM     INTRAV6    RULE
* * * End of File * * *

===>
                                                   X E D I T   1 File
```

CA TOP SECRET FOR Z/VM

CA Top Secret for z/VM

SHARE
EDUCATE • NETWORK • INFLUENCE

Where is the audit data?

- It can alternate between two Audit/Tracking files at the same time
- Allows you to backup one AUDIT file while working on another

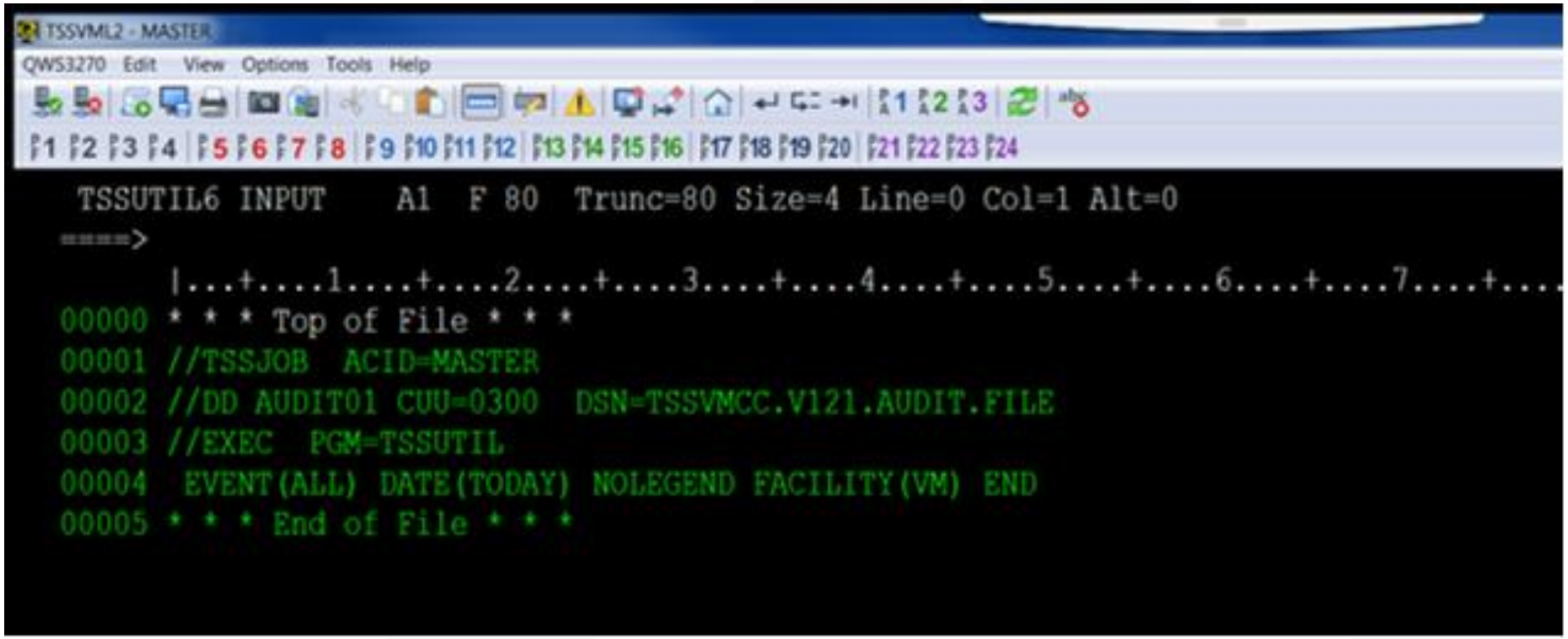
What can I do with it?

- Extract and archive
- Report on the contents

What do I use to report on it?

- TSSUTIL: used to monitor violations and other activity, including, audited activity
- TSSAUDIT: used to monitor changes made to the Security File
- TSSCFILE: used to extract TSS LIST, WHOHAS, and WHOOWNS information into a flat file for further processing by a report generator, such as CA Easytrieve

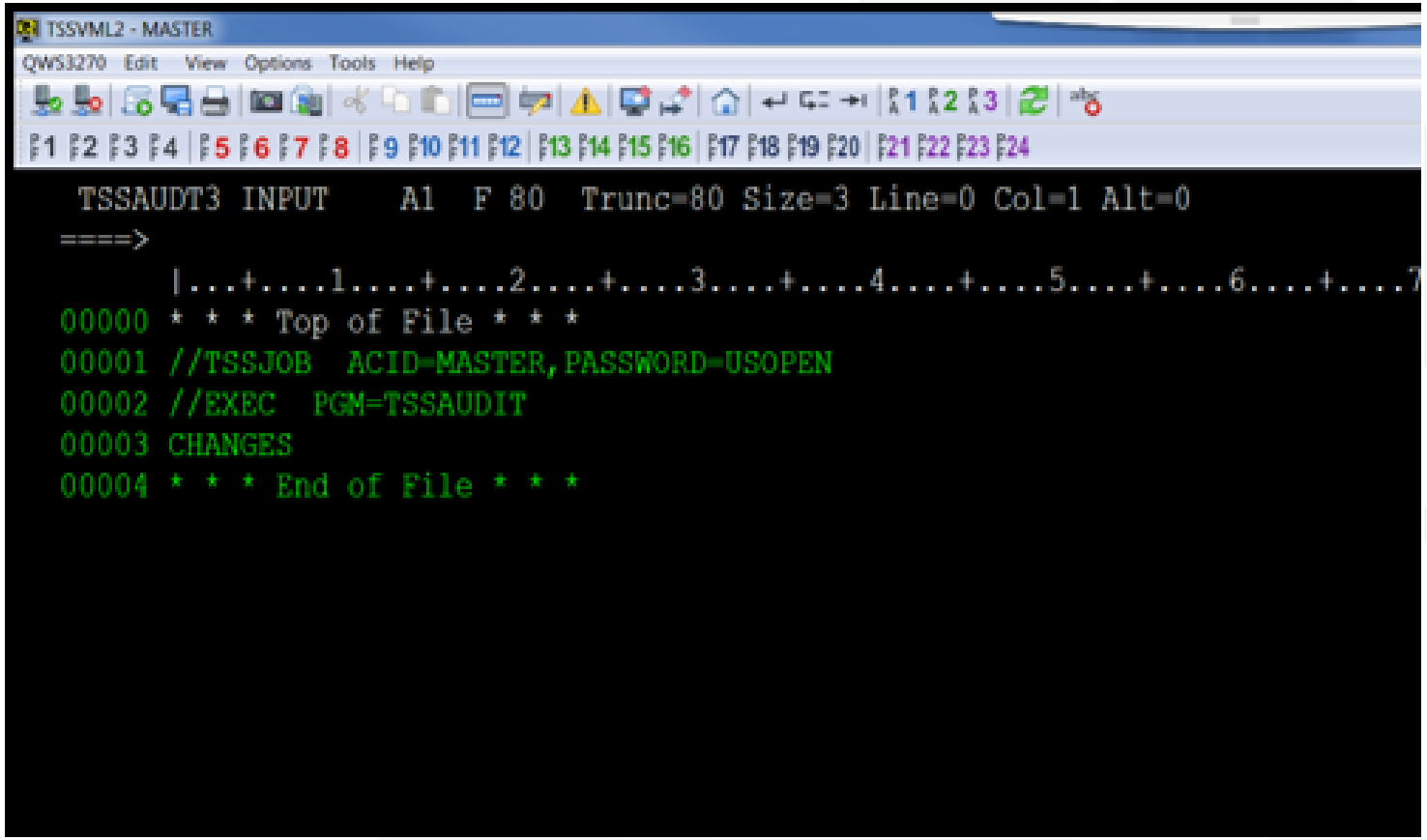
Sample: TSSUTIL Job



Sample: TSSUTIL Output

```
TSSVML2 - MASTER
QWS3270 Edit View Options Tools Help

 0010     PEEK     A0  V 132  Trunc=132 Size=40 Line=11 Col=1 Alt=0
File TSSJ0010 VM from TSSVMCC at TSSVML2 Format is PRINT.
CA Top Secret          VERSION 12.1        SECURITY ACTIVITY/INCIDENTS REPORT # 01          07/18/19  12:40:05        PAGE 001

  DATE     TIME    SYSI ACCESSOR JOBNAME  FFM VC PROGRAM  R-ACCESS A-ACCESS SRC/DRC SEC RESOURCE (TYPE & NAME)       JOBID   TERMINAL

-------- -------- ---- -------- -------- --- -- -------- -------- -------- ------- --- ---------------------------- ------- --------

07/18/19 12:26:55 VML2 AUTOLOG1 AUTOLOG1 V W                              OK    INI   NAME=AUTOLOG1                     DISC
07/18/19 12:26:55 VML2 AUTOLOG1 AUTOLOG1 V W                              OK    TRM                                     DISC
07/18/19 12:26:55 VML2 VRSCS    VRSCS    V W                              OK    INI   NAME=VRSCS                       DISC
07/18/19 12:27:17 VML2 MASTER   MASTER   V W                              OK+B  INI   NAME=MASTER SECURITY              GRAF0901

07/18/19 12:27:40 VML2 GCS      GCS      V W                              OK    INI   NAME=GCS                          DISC
07/18/19 12:27:40 VML2 GCS      GCS      V W 01         AUTOLOG  NONE    *04*-88     ? VRSCS                           DISC
07/18/19 12:27:40 VML2 VRSCS    VRSCS    V W                              OK    INI   NAME=VRSCS                       AUTOLOG
07/18/19 12:27:40 VML2 VRSCS    VRSCS    V W                              OK    TRM                                     AUTOLOG
07/18/19 12:27:40 VML2 GCS      GCS      V W 02         AUTOLOG  NONE    *04*-88     ? AVSVM                           DISC
07/18/19 12:27:40 VML2 AVSVM    AVSVM    V W                              OK    INI   NAME=AVSVM                       AUTOLOG
07/18/19 12:27:40 VML2 AVSVM    AVSVM    V W 01                  NONE    *04*-88     8 TERMINAL.CONMODE                DISC
```

Sample: TSSAUDIT Job



Sample: TSSAUDIT Output

```
TSSVML2 - MASTER
QWS3270  Edit  View  Options  Tools  Help

 0012      PEEK      A0   V 132   Trunc=132 Size=644 Line=15 Col=1 Alt=0
File TSSJ0012 VM from TSSVMCC at TSSVML2 Format is PRINT.

                                        ----- LISTING OF CHANGES TO SECURITY FILE -----
CHANGER    DATE      TIME     SYSID TYPE                        COMMAND/IMAGE
========= ======== ======== ===== ==== ==========================================================================

MASTER   12/23/14 08:50:46 VML2  PW   TSS REP(MASTER  ) PASSWORD(????????)
MASTER   12/23/14 08:51:11 VML2  CMND TSS REPL(MASTER) PASSWORD(?,0)
MASTER   12/23/14 12:43:12 VML2  CMND TSS CREATE(DEPTVMCC) NAME('DEPTVMCC') TYPE(DEPARTMENT)
MASTER   12/23/14 12:43:12 VML2  CMND TSS CREATE(VMUSER) NAME('VMUSER') DEPT(DEPTVMCC) TYPE(PROFILE)
MASTER   12/23/14 12:43:12 VML2  CMND TSS CREATE(GCSSYS) NAME('GCSSYS') DEPT(DEPTVMCC) TYPE(PROFILE)
MASTER   12/23/14 12:43:12 VML2  CMND TSS CREATE(XCOMPROF) NAME('XCOMPROF') DEPT(DEPTVMCC) TYPE(PROFILE)
MASTER   12/23/14 12:43:12 VML2  CMND TSS CREATE(USERPROF) NAME('USERPROF') DEPT(DEPTVMCC) TYPE(PROFILE)
MASTER   12/23/14 12:43:12 VML2  CMND TSS CREATE($ALLOC$) NAME('$ALLOC$') DEPT(DEPTVMCC) PASS(?) TYPE(USER)
MASTER   12/23/14 12:43:12 VML2  CMND TSS ADDTO(DEPTVMCC) VMMDISK($ALLOC$.)
MASTER   12/23/14 12:43:12 VML2  CMND TSS PERMIT($ALLOC$) VMMDISK($ALLOC$.) ACCESS(ALL)
MASTER   12/23/14 12:43:12 VML2  CMND TSS CREATE($END$) NAME('$END$') DEPT(DEPTVMCC) PASS(?) TYPE(USER)
MASTER   12/23/14 12:43:12 VML2  CMND TSS ADDTO(DEPTVMCC) VMMDISK($END$.)
MASTER   12/23/14 12:43:12 VML2  CMND TSS PERMIT($END$) VMMDISK($END$.) ACCESS(ALL)
MASTER   12/23/14 12:43:12 VML2  CMND TSS CREATE($DIRECT$) NAME('$DIRECT$') DEPT(DEPTVMCC) PASS(?) TYPE(USER)
```

What happened and Why?

Sample: TSSCFILE Job

```
TSSCFIL6 INPUT    A1   F 80   Trunc=80 Size=3 Line=0 Col=1 Alt=0
====>
      |...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....
00000 * * * Top of File * * *
00001 //TSSJOB  ACID=MASTER
00002 //EXEC  PGM=TSSCFILE
00003 TSS LIST(ACIDS) DATA(ALL)
00004 * * * End of File * * *
```

Sample: TSSCFILE Output

```
TSSVML2 - MASTER
QWS3270 Edit View Options Tools Help
F1 F2 F3 F4 | F5 F6 F7 F8 | F9 F10 F11 F12 | F13 F14 F15 F16 | F17 F18 F19 F20 | F21 F22 F23 F24
 0015     PEEK     A0  V 80  Trunc=80 Size=1717 Line=0 Col=1 Alt=0
File TSSJ0014 VM from TSSVMCC at TSSVML2 Format is PUNCH.
* * * Top of File * * *
"""  0001                    LIST(ACIDS) DATA(ALL)"
"" ""0100      MASTER        MASTER SECURITY
"""""0200      MASTER        MASTER       512
"""""3700      MASTER        *ALL*
"""""0500      MASTER        12/22/1409/12/1609:4800:00
Ø"Q""0700      MASTER
Ø                 CONSOLE
"
Ø"ø""0800      MASTER                                    NORESCHK
"
"""""0900      MASTER        07/18/1913:19VML2BATCH   00189
Ø"Ä""2004      MASTER        VMMDISK DEPTVMCC       MASTER.
"
Ø"("2021       MASTER        ALL
Ø
"
"""""2022      MASTER        MASTER  VML212/23/201412:43:13
Ø"Ä""2004      MASTER        VMMDISK DEPTVMCC       RON.0191
"
```

CA ACF2 FOR Z/VM

CA ACF2 for z/VM

SHARE
EDUCATE • NETWORK • INFLUENCE

Where is the audit data?

- SMF data written on minidisks are reserved for this purpose
- SMF-type files are used to record all CA ACF2 for z/VM loggings. These files are maintained and managed by the ACF2 service machine.
- ACFSERVE QUERY SMF will show the virtual address of the minidisk holding SMF data

What can I do with it?

- Extract and archive – close and dump currently active minidisks and archives
- Report on the contents – no need to close and dump since reports can work using active SMF files

What do I use to report on it?

- SMF data is used as input for all CA ACF2 for z/VM reporting and several utilities.
- The ACFSERVE commands allow you to monitor the status and manage SMF files
- Most report generators and the ACFRPTPP utility process CA ACF2 for z/VM SMF files.

Note: You must first link and access the minidisks that contain the SMF files

Sample: ACF2 ACFRPTDS (Dataset Logging) Report

```
CA-ACF2 SECURITY - ACFRPTDS DATASET ACCESS JOURNAL        - PAGE 1
DATE 06/13/19 (19.164) TIME 00.01 DATASET LOGGINGS FOR -.-

VMID12   19.163 06/12 09.27 DATASET  LOGGING   SEC-OFF
SECMGR   VOL=      DDN=        DSN=6VMTCP3.V0592.VOLUME
       VOL=      PGM=        LIB=
       DA-OPN INPUT   NORULE   NAM=JOHN SMITH
VMXA     SRC=LDEV0005          UID=SOMEUID12345
       FPOOL=               DIR=
```

Sample: ACF2 ACFRPTDS (Dataset Logging) Report

```
VMID12   19.163 06/12 09.27 DATASET  LOGGING   SEC-OFF
SECMGR   VOL=      DDN=        DSN=6VMTCP3.V0592.FTP.MODULE
       VOL=      PGM=        LIB=
       DA-OPN EXECUTE NORULE   NAM=JOHN SMITH
VMXA     SRC=LDEV0005          UID=SOMEUID12345
       FPOOL=               DIR=

VMID12   19.163 06/12 09.27 DATASET  LOGGING   SEC-OFF
SECMGR   VOL=      DDN=        DSN=6VMTCP30.V0592.STANDARD.TCPXLBIN
       VOL=      PGM=        LIB=
       DA-OPN INPUT   NORULE   NAM=JOHN SMITH
VMXA     SRC=LDEV0005          UID=SOMEUID12345
       FPOOL=               DIR=
```

The first page of a recent ACFRPTDS (Dataset Logging) report on an ACF2 system.

They are all loggins for id (VMID12) who is logged on to group machine SECMGR.

It looks like there was an attempt to get into FTP and there are no rules written. SECMGR has security so the access is allowed but logged.

RACF FOR Z/VM

RACF for z/VM

SHARE
EDUCATE • NETWORK • INFLUENCE

Where is the audit data?

- SMF data recorded on two disks for security-relevant events
- When one disk fills, or RACFSMF is XAUTOLOGged, it flips to another disk
  - Must specify SEVER=YES in the SMF CONTROL to prevent overwriting the next flip
- One audit trail per member of a Single System Image cluster

What can I do with it?

- Extract and archive
- Use the RACF SMF data unload utility to create a sequential file from the security relevant audit data
  - Can be viewed directly, used as input to your own applications and reports, output for viewing on a web browser (XML stylesheet) or placed in a database
- Can merge with z/OS SMF data for combined system reporting

What do I use to report on it?

- Use with RACF report writer or IBM zSecure for RACF/VM
- Write your own applications to produce custom reports or views
- Combined system reporting once merged with z/OS SMF data

z/VM RACF tools for audit records and security status

SHARE
EDUCATE • NETWORK • INFLUENCE

RACF provides System Administrators tools to implement their organizational security policies.

-**RACF report writer** RACRPORT. RACRPORT lists the contents of the SMF (System Management Facilities) records in a format that is easy to read.

-**RACF SMF Data Unloa**d RACFADU with XML. RACFADU creates a sequential file from the SMF audit data. You can create XML format and view using a Web browser.

-**Data Security Monitor** DSMON which reports on the status of the security environment. It shows RACF configuration and Profiles, etc.

For more information on the RACF utilities, see the z/VM 7.1.0 RACF Security Server Auditor's Guide. SC24-6305-00.

IBM Security zSecure Suite

Many customers use the IBM Security zSecure Suite to manage their audit data

Data collected on z/VM by IBM Security Manager for RACF z/VM can be processed on z/VM and also on z/OS by IBM Security zSecure

Admin and Audit. For more information on zSecure Audit, see https://www.ibm.com/us-en/marketplace/zsecure-audit

RACF report writer RACRPORT OUTPUT

RACF REPORT

ALL ACTIVITIES REPORT

Shows logon statistics/resource statistics, activities for a userid, etc.

DATE TIME NAME GROUP ID LVL Event Qualifier

19.276 10:40:18 MAINT SYS1 LOGN0020 0 1 12 JOBID=(00.000 00:00:00),USERDATA=() AUTH=(NONE),REASON=(NONE) LOGSTR='LOGON ‘ SESSION=TSO LOGON,TERMINAL=LOGN0020

19.276 10:40:53 MAINT 0 2 0 JOBID=(MAINT 00.000 00:00:00),USERDATA=() AUTH=(NORMAL),REASON=(VMAUDIT) VMXEVENT=MDISK MAINT 0123 AS 0123 RR

RACF SMF Data Unload RACFADU OUTPUT

RACFADU unloads raw SMF data. Here is some truncated RACFADU output (it is very long output):

JOBINIT RACINITI 10:40:18 2019-10-03 … MAINT… 7010 LOGON LOGN0020 TERMINAL ACCESS SUCCESS 10:40:53 2019-10-03 … MAINT … 7010 MDISK MAINT 0123 AS 0123

You can create RACFADU XML output which can then be viewed in a readable format with a Web browser:

ACCESS

Event	Date	Time	Qualifier	User ID	Profile Name
ACCESS	2019-10-03	10:36:41.78	SUCCESS	RACFSMF	LOGONBY.RACFSMF

JOBINIT

Event	Date	Time	Event Qualifier	Event User ID	LOGSTR
JOBINIT	2019-10-03	10:36:41.78	RACINITI	RACFSMF	LOGON
JOBINIT	**2019-10-03**	**10:40:18.37**	**RACINITI**	**MAINT**	**LOGON**

Data Security Monitor DSMON OUTPUT

Depending on the Reports you select you will see this output (many lines have been deleted and are not shown):

```
 RACF DATA SECURITY MONITOR
  R A C F     E X I T S
EXIT MODULE
NAME                    LENGTH
-----------------------------------------------------------------------
ICHPWX11            1,528
S E L E C T E D     U S E R     A T T R I B U T E S
USERID          -----------------  ATTRIBUTE TYPE  ----------------
                SPECIAL    OPERATIONS  AUDITOR    ROAUDIT    REVOKE
-----------------------------------------------------------------------
RACFADM  SYSTEM      SYSTEM

  R A C F     C L A S S     D E S C R I P T O R     T A B L E     R E P O R T
CLASS                                                  DEFAULT
NAME          STATUS       AUDITING       STATISTICS       UACC       OPERATIONS ALLOWED
-----------------------------------------------------------------------------------------
FACILITY      ACTIVE         NO              NO                        NONE         NO
```

zSecure Manager for z/VM RACF-Main Menu

zSecure Manager for RACF - Main menu
Option ===>

SE	Setup	Options and input data sets
RA	RACF	RACF Administration
AU	Audit	Audit security and system resources
RE	Resource	Resource reports
EV	Events	Event reporting from SMF and other logs
U	User	User events from SMF
G	Group	Group events from SMF
R	Resource	General resource events from SMF
1	SMF reports	Predefined analysis reports
2	RACF events	RACF logging for specific events
C	Custom	Custom report
CO	Commands	Run commands from library
IN	Information	Information and documentation

ZSecure Manager for RACF z/VM OUTPUT-Class

On main panel enter RA.R(RACF Administration, General Resource profiles), Then put in Facility Class

Look at Profile ICHCONN, there are two USERs with UPDATE access. No Audit Concerns shown.

Secure Manager for RACF - RACF - Resource Selection
Command ===>
Add new general resource profile or segment

Show general profiles that fit all of the following criteria
Class name . . . . **FACILITY** (class or filter)
Resource profile .
1 1 EGN
mask

Output/run options
/ Show segments / All Enable full ACL Specify scope
/ Summarize by class

zSecure Manager for RACF General resource Command ===>
Class FACILITY 3 Oct 2019 10:50

Class	Profile key	#	UACC	Owner
s_FACILITY	ICHCONN	1	NONE	MAINT710

==========

zSecure Manager for RACF General resource
Command ===>
Class **FACILITY** 3 Oct 2019 10:50

User	Access	ACL id	When	RI Name	Dfltgrp
DIRMAINT	**UPDATE**	**DIRMAINT**			**SYS1**
TCPIP	**UPDATE**	**TCPIP**			**SYS1**

Categories list
Audit concern

zSecure Manager for RACF z/VM OUTPUT-Compliance(1)

Issue the RACF command to make ICHCONN to UACC(UPDATE) - Universal access update authority.

Then view **option==> RA.AU.R** (in yellow below)

SE	Setup	Options and input data sets
RA	**RACF**	**RACF Administration**
AU	**Audit**	**Audit security and system resources**
R	**Compliance**	**Rule-based compliance evaluation**
S	Status	Status auditing of security and system tables/options
V	Verify	Verify and cleanup security database

On the third slide, when you view Audit concern, it will now be flagged.

zSecure Manager for RACF z/VM OUTPUT-Compliance(2)

zSecure Manager for RACF - Audit - Status

Command ===>

Enter / to select report categories

VM extended	VM oriented tables (reads whole CKFREEZE)
RACF control	RACF oriented tables
RACF user	User oriented RACF tables and reports
RACF resource	Resource oriented RACF tables and reports

Select options for reports: Audit policy

/	Select specific reports from selected categories	/ zSecure
/	Include audit concern overview in overall prio order	C1
	Only show reports that may contain audit concerns	C2
	Minimum audit priority for audit concerns (1-99)	B1
	Show differences	
	Print format	Concise (short) report

zSecure Manager for RACF z/VM OUTPUT-Compliance(3)

Audit concern overview by priority (higher priorities only)

Command

Pri	Complex	Syst	Area	Key	**Audit concern**
10	***VMLPAR***	**RACF**	**ICHCONN**		**Verify why UACC>=UPDATE**

zSecure shows priority 10 we set UACC to UPDATE authority from NONE.

Audit priorities reported by zSecure Audit are broadly categorized as follows:

0 through 9: Housekeeping. Usually of informational interest only.

10 through 19: May also represent housekeeping or normal system settings; however, these should be reviewed.

20 through 39: Usually indicates concerns, vulnerabilities, or dangerous security setting, which must be reviewed.

40 and above: Indicates a serious exposure and must be reviewed and either corrected or otherwise mitigated.

zSecure Manager for RACF z/VM OUTPUT-EVENTs from SMF(1)

zSecure Manager for RACF - Main menu

Option ===> EV

SE	Setup	Options and input data sets
RA	RACF	RACF Administration
AU	Audit	Audit security and system resources
RE	Resource	Resource reports
EV	Events	Event reporting from SMF and other logs
U	User	User events from SMF
G	Group	Group events from SMF
R	Resource	General resource events from SMF
1	SMF reports	Predefined analysis reports
2	RACF events	RACF logging for specific events
C	Custom	Custom report
CO	Commands	Run commands from library
IN	Information	Information and documentation

zSecure Manager for RACF z/VM OUTPUT-EVENTs from SMF(2)

zSecure Manager for RACF - Events - Resource Selection
Command ===> start panel

Show records that fit all of the following criteria:
Resource . . . . . ichconn
Class . . . . . facility (class or EGN mask)
Profile . . . . . .
System . . . . . (system name or EGN mask)

Advanced selection criteria
Date and time Further resource selection

Output/run options
/ Include detail Summarize Specify scope

zSecure Manager for RACF z/VM OUTPUT EVENTs from SMF(3)

zSecure looks at the SMF records and shows that I had updated FACILITY ICHCONN from ZSECURE userid successfully.

Event log record detail information

Command ===>

Date/time Description

- Oct 19 10:56:41.19 RACF RALTER success for ZSECURE: RALTER FACILITY ICHCONN

zSecure Manager for RACF z/VM OUTPUT-EVENTs from SMF(4)

ISPF Panel for EV, Option 2 **RACF events- RACF logging for specific events**

zSecure Manager for RACF - Events - RACF events

Command ===>

Enter "/" to select report(s)

- All events Overview of all following RACF events (except IPL)
- Logging RACF logging of all events except RACINIT
- Not normal RACF access not due to normal profile access
- Warnings RACF access due to profiles in warning modes
- Violations RACF access violations
- Commands RACF command auditing
- IPL RACF RACF initialization

You can select/view what reports you are interested in.

VM:SECURE DIRECTORY MANAGER

VM:Secure Directory Manager audit data

SHARE
EDUCATE • NETWORK • INFLUENCE

Where is the audit data?

- Audit data is collected on VM:Secure 1D0 disk
  - Enabled through the ACCESS AUDT configuration file record
- For SSI each VM:Secure has it's own audit disk
  - Master VM:Secure audits all directory associated items
  - Master and agents audit CP resource access on their 1D0
- Warnings generated when the disk is getting full – if the disk becomes full – an audit record is punched to the reader versus being lost entirely

VM:Secure Directory Manager audit data

SHARE
EDUCATE • NETWORK • INFLUENCE

What can I do with it?

- Extract and archive:
  - Use AUDITEXT to extract the data and clear the disk
  - We recommend you extract and archive daily to keep information in a daily packet
- Report on the contents:
  - Can proactively provide vital information

What do I use to report on it?

- Canned reports are included (User Exit allows for customer records selection)
  - VMXSRA/VMXSRB (Security reports)
- Create custom reports via VMRGRW (VM Product Manager Generalized Report Writer)
- Flat files can be interpreted and data reported based on your requirements
  - Layouts provided in product documentation
  - Possibility of creating SMF style records and shipping to z/OS for inclusion in reports

VM:Secure Directory Manager: VMXSRB Report

```
REPORTB   OUTPUT   A1   F 133   Trunc=133 Size=650 Line=12 Col=1 Alt=8

 VM:Secure (R)  Copyright (c) 2016 CA. All rights reserved
                        System Actions

                     FROM          ISSUING
DATE      TIME       TERMINAL      USERID    ACTION
_________ _________  __________    _________ ____________________________________________

06/25/19 12:59:11 0020          VMUID12   extracted audit file into EXTRACT A0
06/25/19 14:31:50 0021          VMSECURE issued accepted LOGON to VMSECURE via RUL
E
06/25/19 14:33:37 0020          VMUID12   edited the managers file
06/25/19 14:56:16 0020          VMUID12   edited the SECURITY CONFIG file
06/25/19 17:03:31 DSC           VMUID12   logged off
06/26/19 08:08:28 0020          VMUID12   issued accepted LOGON to VMUID12 via RULE

06/26/19 08:08:28 0020          VMUID12   LINKed to MAINT's 190 (RR) via RULE
06/26/19 08:08:28 0020          VMUID12   LINKed to MAINT's 19D (RR) via RULE
06/26/19 08:08:28 0020          VMUID12   LINKed to MAINT's 19E (RR) via RULE
06/26/19 08:08:28 0020          VMUID12   accepted COUPLE to SYSTEM INTRAV6 via RUL
E
06/26/19 08:08:28 0020          VMUID12   LINKed to VMUID20's 997 (RR) via RULE
06/26/19 08:08:28 0020          VMUID12   accepted COUPLE to SYSTEM INTRA059 via NO
RULE
06/26/19 08:08:28 0020          VMUID12   LINKed to VMANAGER's 193 (RR) via RULE
06/26/19 11:35:32 0020          VMUID12   created userid YVO9 skeleton GENERAL acco
unt 99
06/26/19 11:35:35 DSC           VMX$0002 issued SPOOL/TRANSFER to VMUID12 via RULE

====>
                                                                  X E D I T  1 File
```

Use the VMXSRB report program to generate formatted output of all audit data captured by CA VM:Secure

You can create the report without CP data (NOCP), so you exclude the data you may see in the VMXSRA output. You also have the ability to select on requesting and target user IDs only. Additionally, there is a user exit to allow for more selection customization.

This report shows a variety of activity from the audit file being extracted, configuration files changed and that a user was created (YVO9) out of skeleton file GENERAL.

VM:Secure Directory Manager: VMXSRB Report

```
 REPORTB   OUTPUT    A1   F 133   Trunc=133 Size=114 Line=14 Col=1 Alt=11

                     FROM          ISSUING
DATE      TIME       TERMINAL      USERID    ACTION
_________ _________  ____________  ________  ____________________________________________

07/15/19 13:30:25 0020          VMUID12   failed LOGON to VMUID12 due to PASSWORD
07/15/19 13:30:29 0020          VMUID12   issued accepted LOGON to VMUID12 via RULE

07/15/19 13:30:29 0020          VMUID12   LINKed to MAINT's 190 (RR) via RULE
07/15/19 13:30:29 0020          VMUID12   LINKed to MAINT's 19D (RR) via RULE
07/15/19 13:30:29 0020          VMUID12   LINKed to MAINT's 19E (RR) via RULE
07/15/19 13:30:29 0020          VMUID12   accepted COUPLE to SYSTEM INTRAV6 via RUL
E
07/15/19 13:30:29 0020          VMUID12   LINKed to VMUID20's 997 (RR) via RULE
07/15/19 13:30:29 0020          VMUID12   accepted COUPLE to SYSTEM INTRA059 via NO
R
07/15/19 13:30:29 0020          VMUID12   LINKed to VMANAGER's 193 (RR) via RULE
07/15/19 13:41:33 0023          MAINT     failed LOGON to MAINT due to PASSWORD
07/15/19 13:41:38 0023          MAINT     failed LOGON to MAINT due to PASSWORD
07/15/19 13:41:47 0023          MAINT     failed LOGON to MAINT due to PASSWORD
07/15/19 13:41:54 0023          MAINT     exceeded password count 0023 LOGON *
07/15/19 13:41:54 0023          TERMPASS  added SYSTEM rule to file OVERRIDE SYSRUL
E
         REJECT 0023 LOGON ( EXPIRE 12/30/21 09:09:00
07/15/19 13:41:54 0023          MAINT     system rule created, denying access from
t
07/15/19 13:41:54 0023          MAINT     exceeded password count * LOGON MAINT
07/15/19 13:41:54 0023          MAINT     failed LOGON to MAINT due to PASSWORD

====>
                                                                X E D I T  1 File
```

In this VMXSRB output we see the same activity that we saw in the security report with someone attempting to logon to privileged user IDs.

We see the password denial and rule created to prevent further logons from this terminal address.

IBM DIRECTORY MANAGEMENT AUDIT DATA

Directory Management IBM DIRMAINT Audit Data

SHARE
EDUCATE • NETWORK • INFLUENCE

Where is the audit data?

- All transactions captured, by spooling the console messages as commands are processed
- Creates the transaction logs which are essentially copies of the console information
- Transaction logs are automatically pruned on an interval which can be changed using a DirMaint configuration option
  - Other configuration and user exits to record/filter data

What can I do with it?

- IBM provided exit that will filter and forward the logging information to RACF for inclusion within the RACF SMF data

What do I use to report on it?

- No DirMaint tools to parse or create reports for this data
- SMF reporting once RACF data is merged with z/OS SMF data
- Write your own application to report on logged data

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 1 –

You have a company requirement for all resource access to be rules/permissions based. No default access to any resource. If access is needed to a resource it will require a rule to allow it.

How can you use audit data to see where rules that need to be set up to allow or deny access?

- Situation 1 – ESM not implemented
- Situation 2 - Partial ESM implementation
  - Some rules in place

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 1 – Example with VM:Secure – Situation 1

1. Install ESM configure as ‘open’ (in VM:Secure, NORULE ACCEPT)
2. Configure auditing
3. Allow audit data to collect to get a good sample of what resources are accessed
    1. Set up daily collection of the audit data and after using, if possible, archive it for future reference
4. Continue with steps in situation 2

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 1 – Example with CA VM:Secure – Situation 2 (NORULE ACCEPT)

1. Run AUDITEXT to get audit file extract.
2. Run VMXSRA report utility with NORULE option.
    1. Report output tells you all resource access that is happening without rules in place.
3. Add rule to allow or deny access as appropriate
4. Keep doing 1-3 until you are set up with rules for all resources. Give access where it is needed otherwise protect the resource by denying access
    1. Give time to allow runs of timed events (monthly, quarterly) to make sure find all required access
    2. Use rules hierarchy and order to protect if no rule found to allow before reject found
5. When satisfied all required access has a rule, close system access
    1. NORULE REJECT configuration

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 1 – Example with CA VM:Secure. VMXSRA output.

Command Audit - All Link Commands Processed by NORULE

DATE	TIME	FROM TERMINAL	ISSUING USERID	TARGET USERID	MDSK ADDR	LINK MODE	REASON REJECTED
04/06/20	11:05:36	10.230.148.121	USERA	USERB	666	M	PASSWORD
04/06/20	11:07:01	10.230.148.121	USERA	USERB	666	M	
04/06/20	11:07:46	10.230.148.121	USERA	USERB	191	W	PASSWORD
04/06/20	11:08:14	10.230.148.121	USERA	USERB	191	W	

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 1 – Example with CA VM:Secure.

After investigation, it is decided USERA needs to be able to link to USERB's 666 disk read only but **not** to USERB's 191 disk.

Rules to add to the USERB user rules file:

ACCEPT USERA LINK 666 RR (NOPASS → *Allows link to 666 read only*

REJECT USERA LINK * → *Disallows all other links*

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 1 – Example with CA VM:Secure. USERA links after new rules were added:

link userb 191 555 rr → *Can't link to the 191*

VMXACJ0171I CP command 'LINK USERB 191 RR'

VMXACJ0172I Rejected via user rule: REJECT USERA LINK *

HCPLNM298E USERB 0191 not linked; request denied

Ready(00298);

link userb 666 555 m → *Can't link to the 666 with 'M' mode*

VMXACJ0171I CP command 'LINK USERB 666 M'

VMXACJ0172I Rejected via user rule: REJECT USERA LINK *

HCPLNM298E USERB 0666 not linked; request denied

Ready(00298);

Now I know how to collect audit data, what do I do with it?

Case 1 – Example with CA VM:Secure. USERA links after new rules were added:

link userb 666 555 rr → *Can link to the 666 disk read*

VMXACJ0171I CP command 'LINK USERB 666 RR'

VMXACJ0172I Accepted via user rule: ACCEPT USERA LINK 666 RR (NOPASS

DASD 0555 LINKED R/O; R/W BY USERB

Ready;

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 1 – Example with CA VM:Secure. Alternative rules

Set up USERB user rule to allow USERA to link read only its 191 and add a system default rule to deny USERA linking to any other mini disk. (Rules hierarchy processes USER rules before default SYSTEM rules)

USERB user rules
ACCEPT USERA LINK 191 RR (NOPASS

System Default rules
REJECT USERA LINK *

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 1 – Example with CA VM:Secure. Alternative rules to control links to USERB

link userb 191 555 rr → *Still can't link USERB 191*
VMXACJ0171I CP command 'LINK USERB 191 RR'
VMXACJ0172I Rejected via default system rule: REJECT USERA LINK *
HCPLNM298E USERB 0191 not linked; request denied
Ready(00298);

link userb 666 555 rr → *Can link to USERB 666 read*
VMXACJ0171I CP command 'LINK USERB 666 RR'
VMXACJ0172I Accepted via user rule: ACCEPT USERA LINK 666 RR (NOPASS
DASD 0555 LINKED R/O; R/W BY USERB
Ready;

Now I know how to collect audit data, what do I do with it?

Case 2 – Coworker that should be able to logon to VMANAGER cannot. Every attempt to logon is rejected. Coworker states this was working fine the previous day and the password has not been changed.

Now I know how to collect audit data, what do I do with it?

SHARE
EDUCATE • NETWORK • INFLUENCE

Case 2 – Example with VM:Secure

1. Extract audit information (AUDITEXT)
   - If you thought ahead, you've been extracting audit data daily so will only have data since your last extraction
2. Run VMXSRB – start by looking at what happened after 17:00 when you know your co-worker was logged off for the day

TESTCPA1

QWS3270 Edit View Options Tools Help

```
REPORTB  LISTING2 A0   F 133   Trunc=133 Size=55 Line=14 Col=1 Alt=1

                 VM:Secure (R)  Copyright (c) 2016 CA. All rights reserved
                                System Actions
                   FROM                ISSUING
DATE       TIME    TERMINAL            USERID          ACTION
_________ _________ _________________ _________ ____________________________________
04/06/20 17:07:08 DSC                JOHNH     logged off
04/06/20 17:07:51 10.230.148.121     MAINT     failed LOGON to MAINT due to PASS
04/06/20 17:07:55 10.230.148.121     MAINT     failed LOGON to MAINT due to PASS
04/06/20 17:08:03 10.230.148.121     MAINT     failed LOGON to MAINT due to PASS
04/06/20 17:08:09 10.230.148.121     MAINT     exceeded password count 0AE69479
04/06/20 17:08:09 10.230.148.121     TERMPASS  added SYSTEM rule to file OVERRID
                                               REJECT 10.230.148.121 LOGON ( IPA
04/06/20 17:08:09 10.230.148.121     MAINT     system rule created, denying acce
04/06/20 17:08:09 10.230.148.121     MAINT     exceed password count * LOGON MAI
04/06/20 17:08:09 10.230.148.121     MAINT     failed LOGON to MAINT due to PASS
04/06/20 17:09:05 0020               VMANAGER  failed LOGON to VMANAGER due to P
04/06/20 17:09:11 0020               VMANAGER  failed LOGON to VMANAGER due to P
04/06/20 17:09:22 0020               VMANAGER  failed LOGON to VMANAGER due to P
04/06/20 17:09:28 0020               VMANAGER  exceeded password count 0020 LOGO
04/06/20 17:09:28 0020               TERMPASS  added SYSTEM rule to file OVERRID
                                               REJECT 0020 LOGON ( EXPIRE 12/30/
04/06/20 17:09:28 0020               VMANAGER  system rule created, denying acce
04/06/20 17:09:28 0020               VMANAGER  exceeded password count * LOGON V
04/06/20 17:09:28 0020               USERPASS  added USER rule to file VMANAGER
                                               REJECT * LOGON (NOTIFY
04/06/20 17:09:28 0020               VMANAGER  user rule created, denying LOGON
04/06/20 17:09:28 0020               VMANAGER  failed LOGON to VMANAGER due to P
04/06/20 17:10:03 0020               MAINT     failed LOGON to MAINT due to RULE
====>
                                                                X E D I T  1 File
```

Connected to testcpa1.lvn.broadcom.net port 23 21/28 NUM 960 14:55:54 IBM-DYNAMIC

TESTCPA1

QWS3270 Edit View Options Tools Help

```
 REPORTB   LISTING2 A0   F 133   Trunc=133 Size=50 Line=42 Col=1 Alt=2

04/06/20 17:16:12 0021            MAINT      failed LOGON to MAINT due to PASS
04/06/20 17:16:30 0021            MAINT      failed LOGON to MAINT due to PASS
04/06/20 17:16:39 0021            MAINT      failed LOGON to MAINT due to PASS
04/06/20 17:16:54 0021            MAINT      exceeded password count 0021 LOGO
04/06/20 17:16:54 0021            TERMPASS   added SYSTEM rule to file OVERRID
                                             REJECT 0021 LOGON ( EXPIRE 12/30/
04/06/20 17:16:54 0021            MAINT      system rule created, denying acce
04/06/20 17:16:54 0021            MAINT      exceeded password count * LOGON M
04/06/20 17:16:54 0021            MAINT      failed LOGON to MAINT due to PASS
04/06/20 17:19:10 0021            VMSECURE   failed LOGON to VMSECURE due to R
04/06/20 17:20:47 0022            MAINT640   failed LOGON to MAINT640 due to P
04/06/20 17:20:58 0022            MAINT640   failed LOGON to MAINT640 due to P
04/06/20 17:21:09 0022            MAINT640   failed LOGON to MAINT640 due to P
04/06/20 17:21:23 0022            MAINT640   exceeded password count 0022 LOGO
04/06/20 17:21:23 0022            TERMPASS   added SYSTEM rule to file OVERRID
                                             REJECT 0022 LOGON ( EXPIRE 12/30/
04/06/20 17:21:23 0022            MAINT640   system rule created, denying acce
04/06/20 17:21:23 0022            MAINT640   exceeded password count * LOGON M
04/06/20 17:21:23 0022            USERPASS   added USER rule to file MAINT640
                                             REJECT * LOGON (NOTIFY
04/06/20 17:21:23 0022            MAINT640   user rule created, denying LOGON
04/06/20 17:21:23 0022            MAINT640   failed LOGON to MAINT640 due to P
* * * End of File * * *

====>

                                                          X E D I T   1 File
```

Connected to testcpa1.lvn.broadcom.net port 23 | 31/7 | NUM | 15:01:43 | IBM-DYNAMIC

Why do I care about audit data?

Use it to verify the effectiveness of your security

Determine whether your security objectives are being met

Finding more information when “scary stuff” happens

Let the audit information prove your worth!