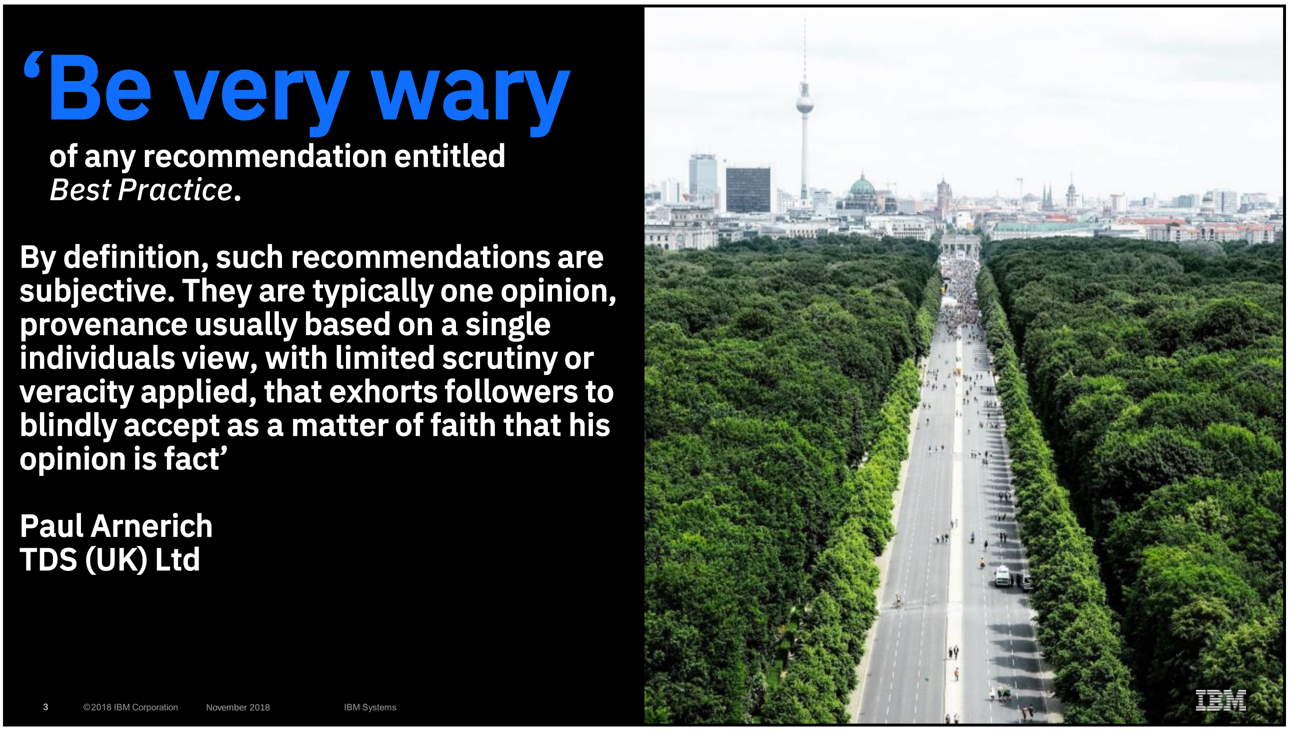
RACF & z/VM Best Practices

Geoff Rousell
IBM

November 2018
Session CM

Agenda

- Introduction – do you need an ESM?
- Certification
- Practical Steps
- How do *YOU* do it? – open discussion
- Conclusions

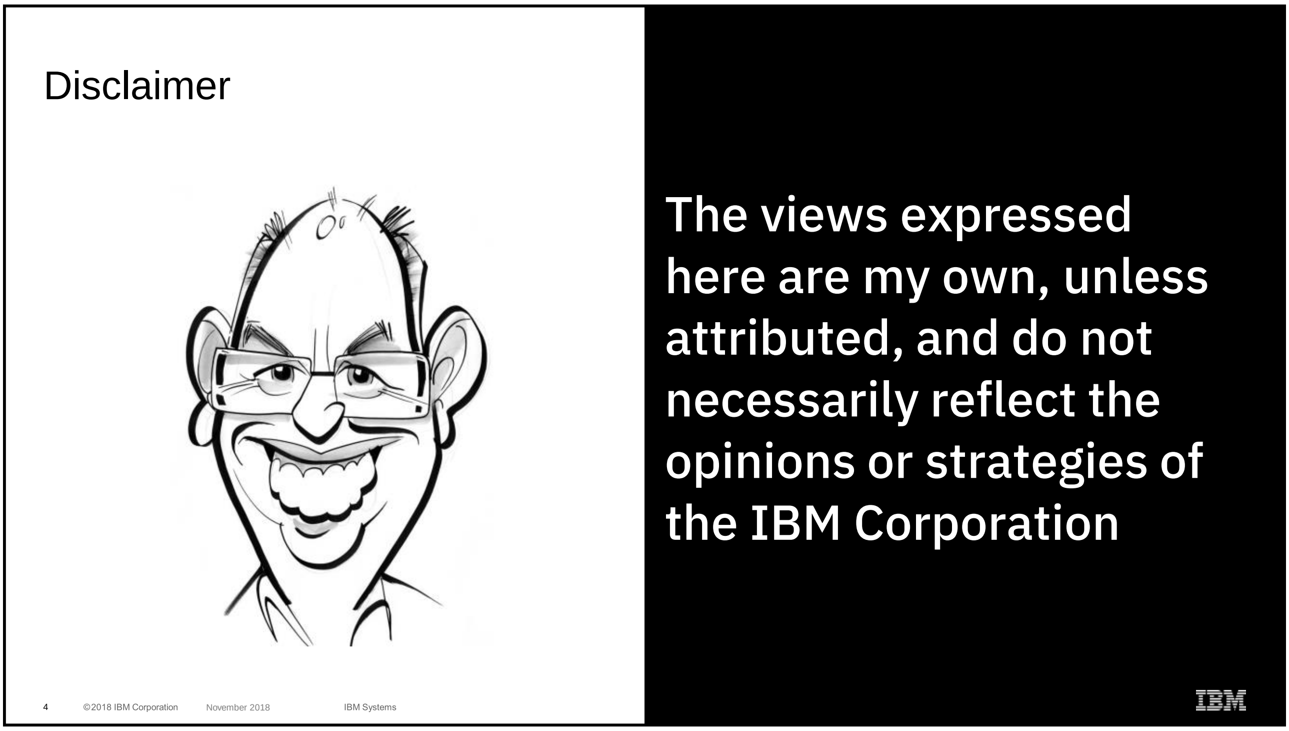


‘Be very wary

of any recommendation entitled
Best Practice.

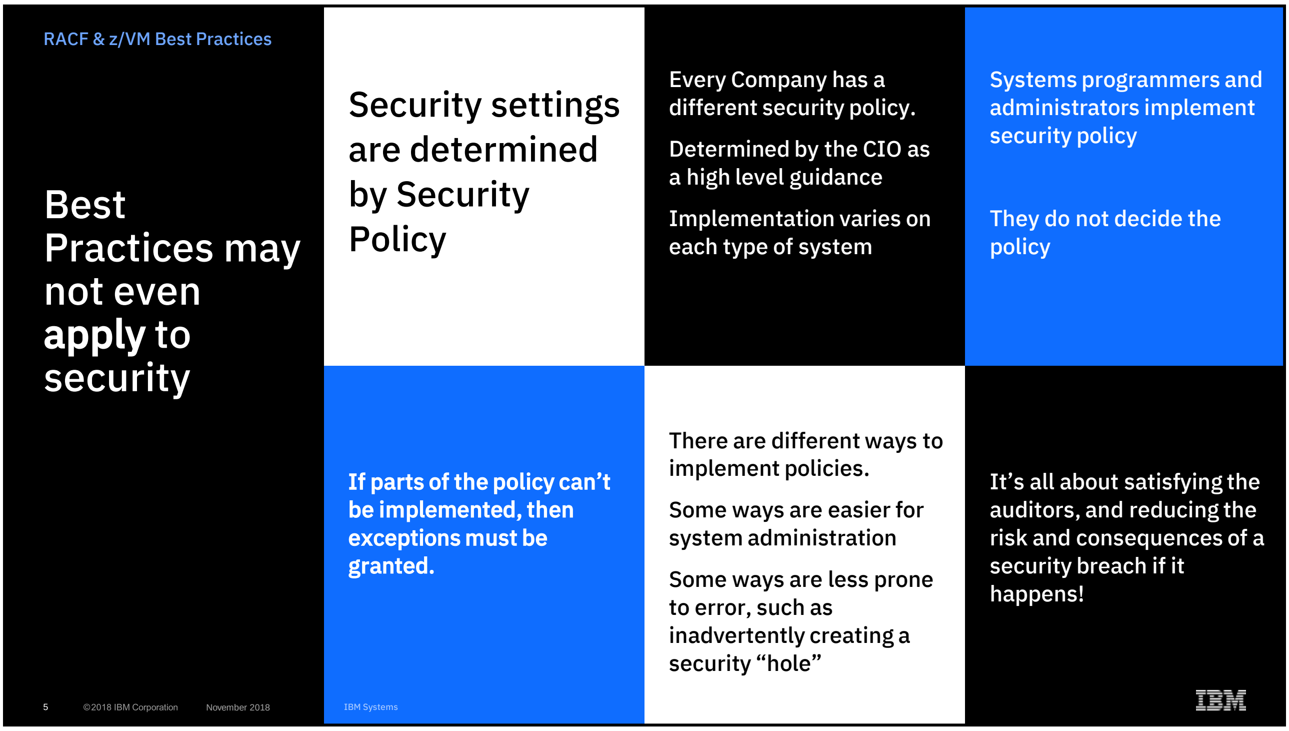
By definition, such recommendations are subjective. They are typically one opinion, provenance usually based on a single individuals view, with limited scrutiny or veracity applied, that exhorts followers to blindly accept as a matter of faith that his opinion is fact’

Paul Arnerich
TDS (UK) Ltd



Disclaimer

The views expressed here are my own, unless attributed, and do not necessarily reflect the opinions or strategies of the IBM Corporation



RACF & z/VM Best Practices

Best Practices may not even apply to security

Security settings are determined by Security Policy

Every Company has a different security policy.

Determined by the CIO as a high level guidance

Implementation varies on each type of system

Systems programmers and administrators implement security policy

They do not decide the policy

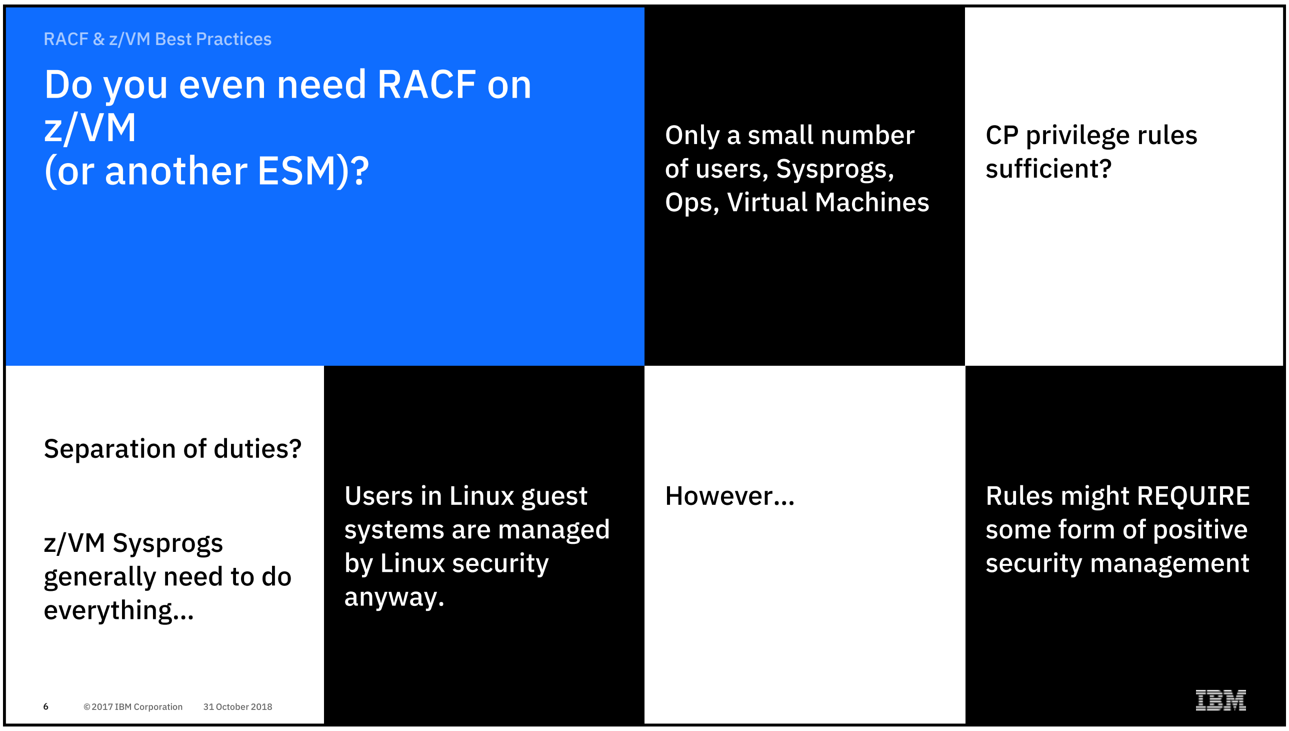
If parts of the policy can't be implemented, then exceptions must be granted.

There are different ways to implement policies.

Some ways are easier for system administration

Some ways are less prone to error, such as inadvertently creating a security "hole"

It's all about satisfying the auditors, and reducing the risk and consequences of a security breach if it happens!



RACF & z/VM Best Practices

Do you even need RACF on z/VM (or another ESM)?

Only a small number of users, Sysprogs, Ops, Virtual Machines

CP privilege rules sufficient?

Separation of duties?

z/VM Sysprogs generally need to do everything…

Users in Linux guest systems are managed by Linux security anyway.

However…

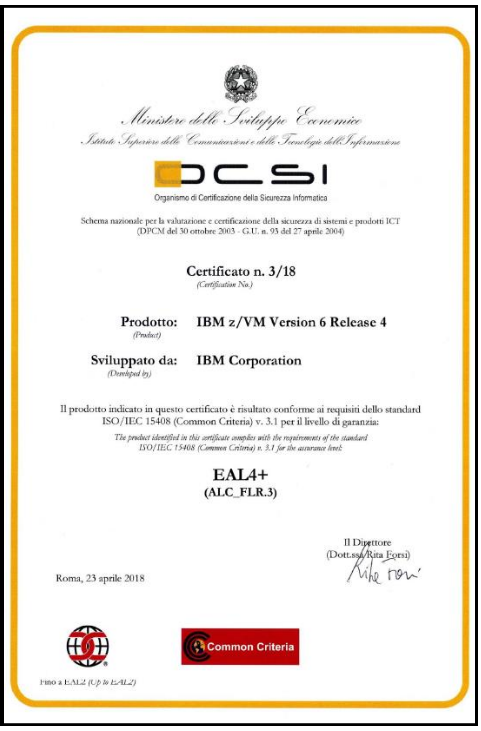
Rules might REQUIRE some form of positive security management

What does “IBM” recommend?

It probably depends on which IBMer you ask

How about a certification?

Operating System Protection Profile v2.0 [OSPP] with the following Extended Packages (EP):
- OSPP EP – Labeled Security v2.0 [OSPP-LS]
- OSPP EP – Virtualization v2.0 [OSPP-VIRT]



Ministero dello Sviluppo Economico
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI
Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 3/18
(Certification No.)

Prodotto: *(Product)* **IBM z/VM Version 6 Release 4**

Sviluppato da: *(Developed by)* **IBM Corporation**

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_FLR.3)

Roma, 23 aprile 2018

Il Direttore
(Dott.ssa Rita Forsi)
Rita Forsi

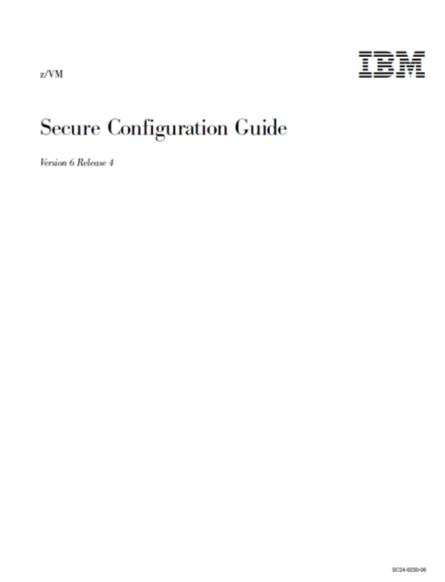
Common Criteria

Fino a EAL2 *(Up to EAL2)*

It comes with a manual!

“Secure Configuration Guide”,
SC24-6230

HOW to configure your system to meet the EAL test results



z/VM

IBM

Secure Configuration Guide

Version 6 Release 4

SC24-6230-06

At the start

Have the right software levels:

- z/VM 6.4 (now 7.1)
- Service level 6401RSU*
- Make sure the z/VM came from somewhere reputable!

System Initialization

- “Early” VMs don’t have RACF control:
  - e.g. AUTOLOG1, DISKACNT, OPERATOR, EREP, OPERSYMP
- To avoid issues:
  - Specify DRAIN and DISABLE for the type of startup
  - Be certain the AUTOLOG1 enables only the RACF VM no others. AUTOLOG2 starts after RACF to start everything else.

Installing & Customising RACF – the database

RACF on z/VM is heavily based on RACF from z/OS

Same underlying database, "same" commands.

Different security resources

EVEN THOUGH YOU CAN, DO NOT SHARE THE DATABASE WITH z/OS SYSTEMS

SSI Considerations:

- The RACF Database must be shared by all members of the SSI
- Virtual reserve/ release must be enabled

"It is highly recommended to keep a current copy of your primary RACF database distinct from your primary and backup volumes in case it is needed for recovery"

Installing & Customising RACF – part 1a

Follow the steps in the program directory ;-)

BUT, some other considerations:

- SMF Archiving policy
  - Force archive whenever primary or secondary SMF fills (SMFFREQ = "AUTO" and SMFSWITCH = "NO")
  - Set the SEVER option in case both SMF minidisks become unexpectedly full

- Remove the shipped ICHRCX02 exit (allows alternate user to access resources the service machine can access)
- Define the HCPRWA
  - The most common customisations
  - HCPRWAC is shipped as the "OSPP compliant" version

Installing & Customising RACF – part 1b - HCPRWAC

```
RACSERV  USERID=RACFVM
RACSERV  USERID=RACMAINT
SYSSEC   DISKP=ALLOW,DISKU=FAIL,DISKF=FAIL,DISKW=FAIL,DISKM=ON,
         RDRP=ALLOW,RDRU=FAIL,RDRF=FAIL,RDRW=FAIL,RDRM=ON,
         NODEP=ALLOW,NODEU=FAIL,NODEF=FAIL,NODEW=FAIL,NODEM=ON,
         CMDP=ALLOW,CMDU=FAIL,CMDF=FAIL,CMDW=FAIL,CMDM=ON,
         LANP=ALLOW,LANU=FAIL,LANF=FAIL,LANW=FAIL,LANM=ON
         DEFLTP=ALLOW,DEFLTU=FAIL,DEFLTF=FAIL,DEFLTW=FAIL
```

- All minidisks will be subject to RACF control & auditing
- Requires VMMDISK, VMRDR, VMNODE, VMCMD & VMLAN Classes to be active
- The designated RACF service machines are RACFVM and RACMAINT

Installing & Customising RACF – part 3

Prevent CP DIAL & MSG commands from being used prior to logon:

- `RAC SETEVENT NODIAL NOPRELOGMSG`

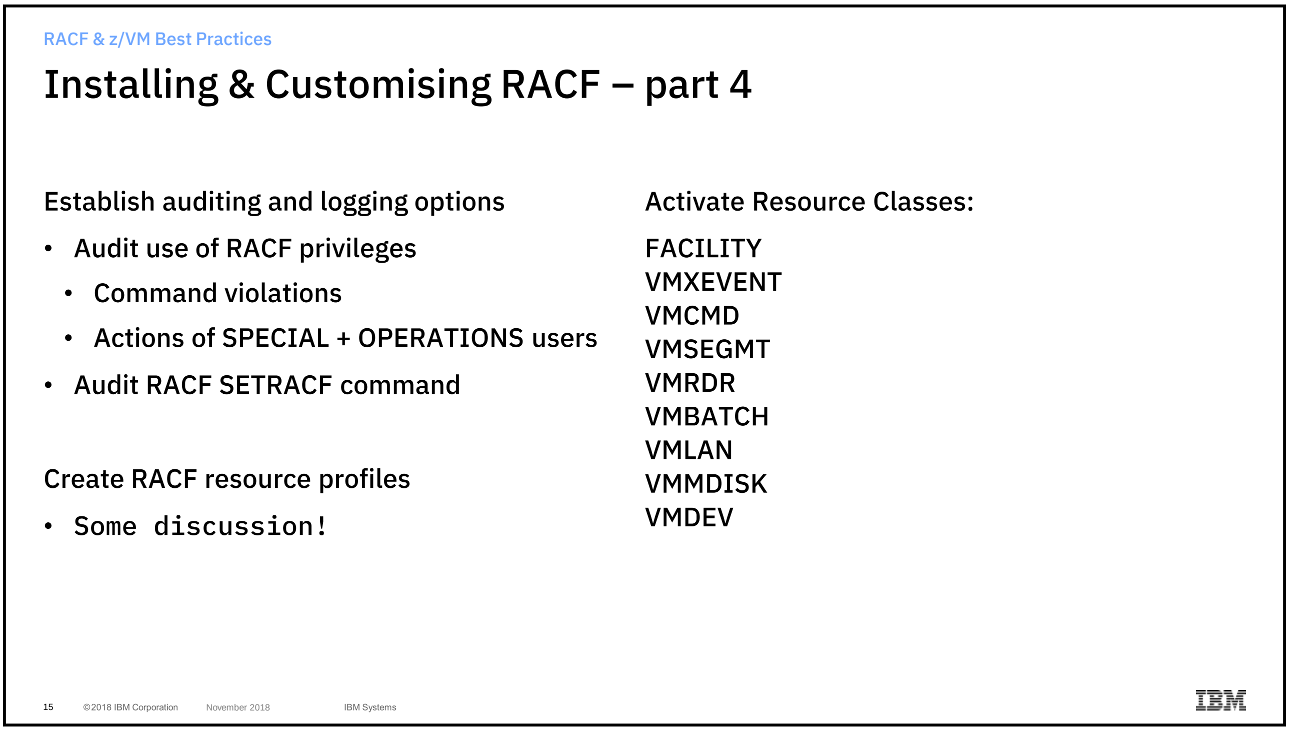
Define Password Encryption Policy

- `RAC SETROPTS PASSWORD(ALGORITHM(KDFAES))`

Define Password Policy

- OSPP specifies >7 characters, 1 numeric not in the first or last position, revoke after 5 incorrect attempts

```
SETROPTS PASSWORD(REVOKE(5)
      RULE1(LENGTH(7:8) ALPHA(1,7)
      ALPHANUM(2:6))
      RULE2(LENGTH(8) ALPHA(1,8)
      ALPHANUM(2:7)))
```



Installing & Customising RACF – part 4

Establish auditing and logging options

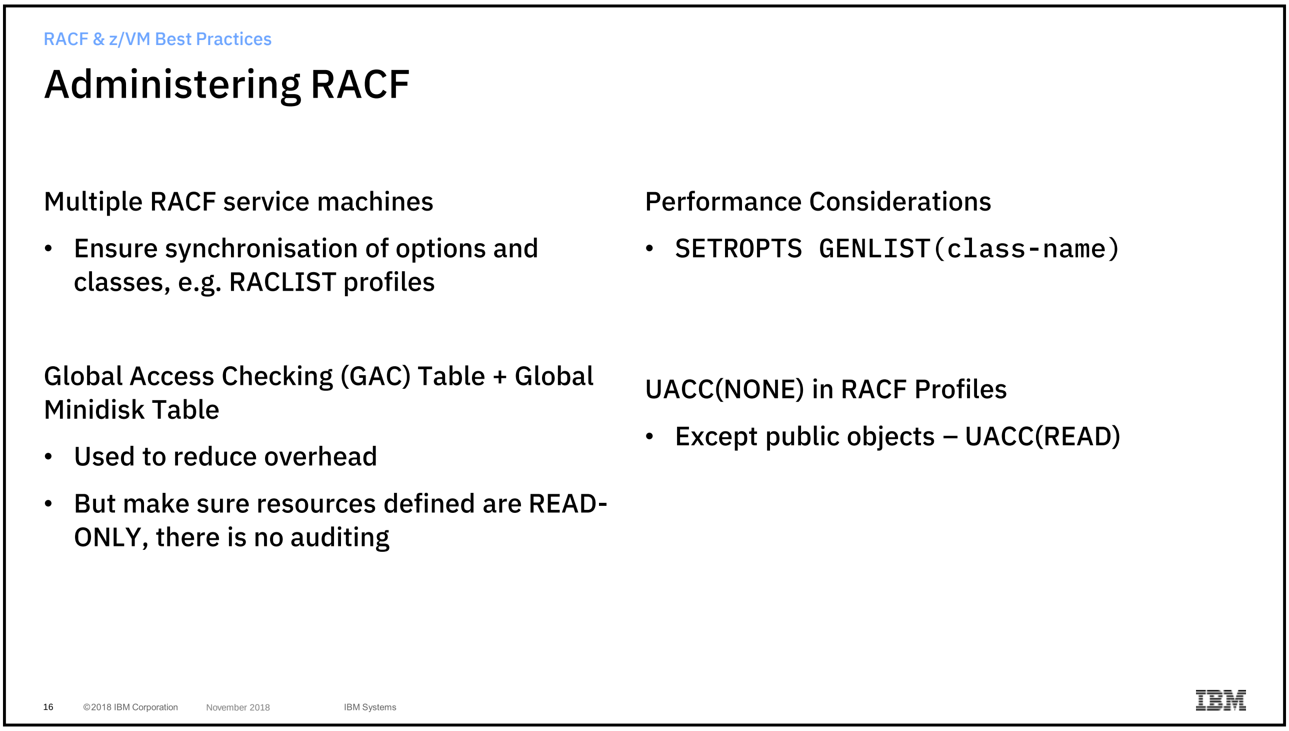
- Audit use of RACF privileges
  - Command violations
  - Actions of SPECIAL + OPERATIONS users
- Audit RACF SETRACF command

Create RACF resource profiles

- `Some discussion!`

Activate Resource Classes:

FACILITY
VMXEVENT
VMCMD
VMSEGMT
VMRDR
VMBATCH
VMLAN
VMMDISK
VMDEV



Administering RACF

Multiple RACF service machines

- Ensure synchronisation of options and classes, e.g. RACLIST profiles

Global Access Checking (GAC) Table + Global Minidisk Table

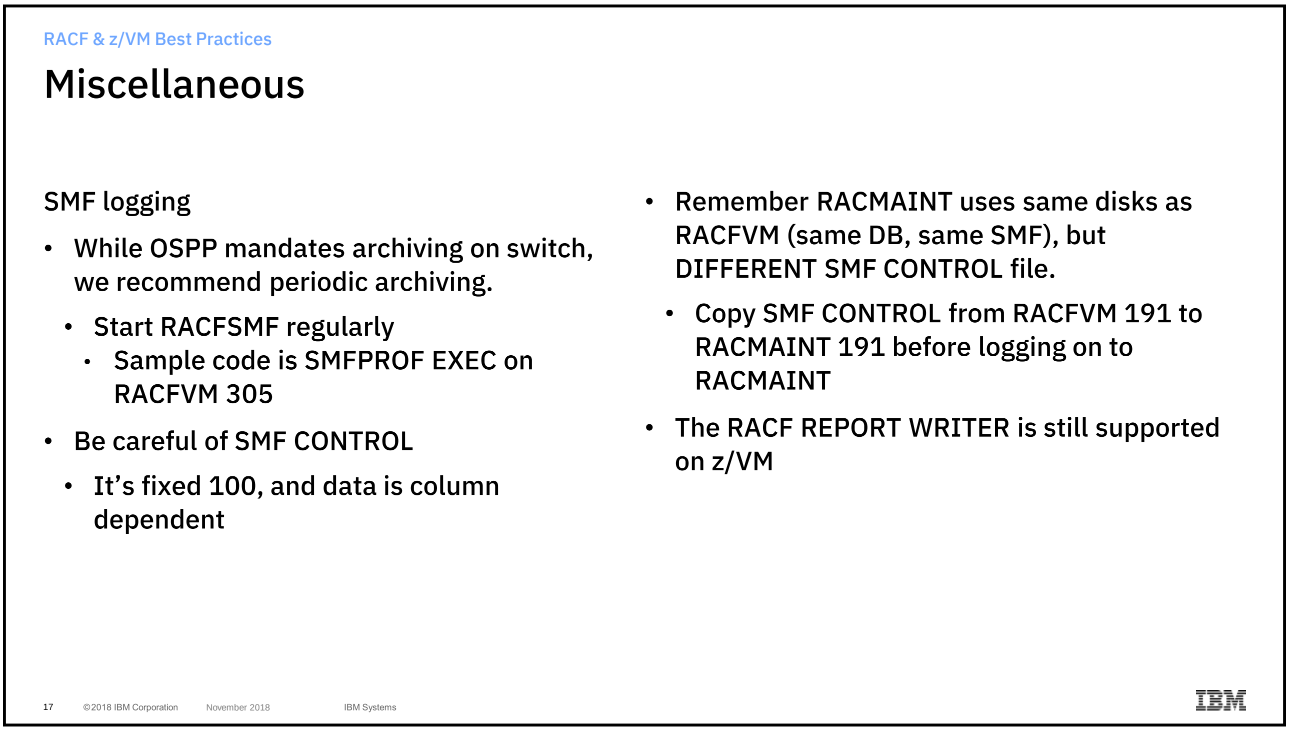
- Used to reduce overhead
- But make sure resources defined are READ-ONLY, there is no auditing

Performance Considerations

- `SETROPTS GENLIST(class-name)`

UACC(NONE) in RACF Profiles

- Except public objects – UACC(READ)

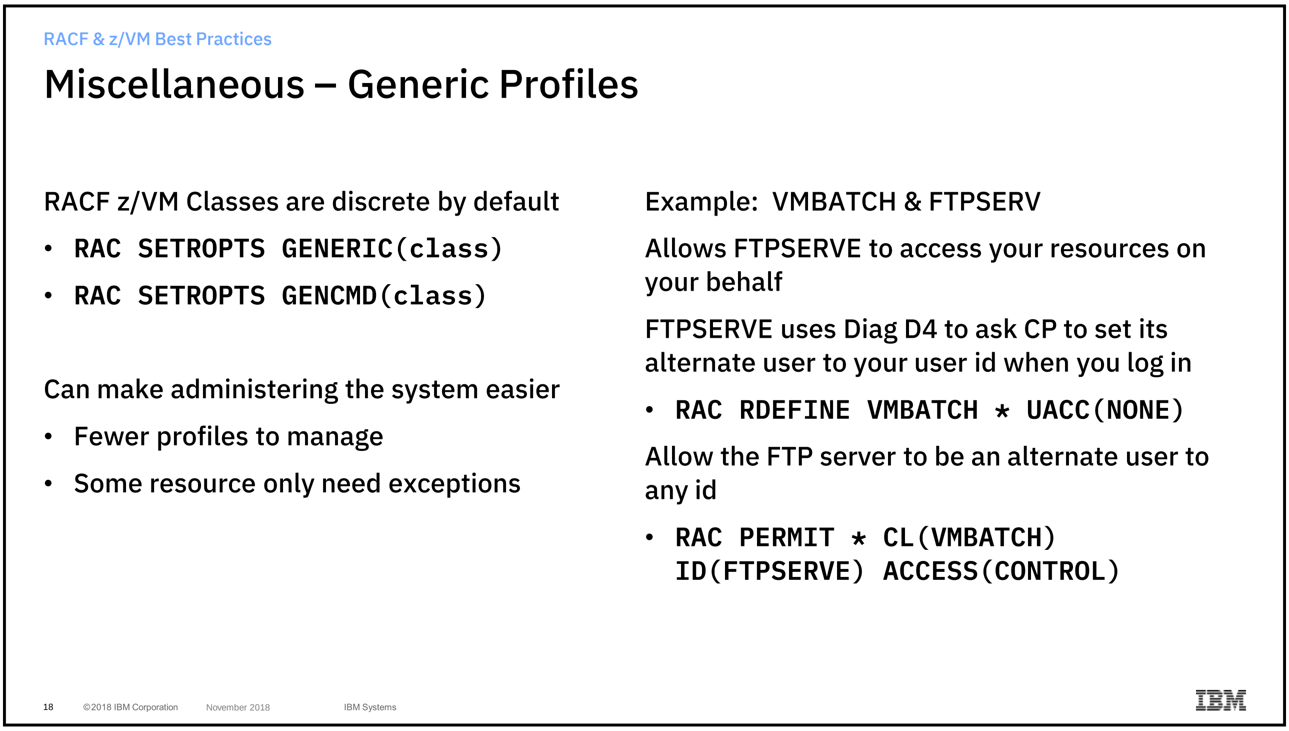


Miscellaneous

SMF logging

- While OSPP mandates archiving on switch, we recommend periodic archiving.
  - Start RACFSMF regularly
    - Sample code is SMFPROF EXEC on RACFVM 305
- Be careful of SMF CONTROL
  - It’s fixed 100, and data is column dependent

- Remember RACMAINT uses same disks as RACFVM (same DB, same SMF), but DIFFERENT SMF CONTROL file.
  - Copy SMF CONTROL from RACFVM 191 to RACMAINT 191 before logging on to RACMAINT
- The RACF REPORT WRITER is still supported on z/VM



Miscellaneous – Generic Profiles

RACF z/VM Classes are discrete by default

- `RAC SETROPTS GENERIC(class)`
- `RAC SETROPTS GENCMD(class)`

Can make administering the system easier

- Fewer profiles to manage
- Some resource only need exceptions

Example: VMBATCH & FTPSERV

Allows FTPSERVE to access your resources on your behalf

FTPSERVE uses Diag D4 to ask CP to set its alternate user to your user id when you log in

- `RAC RDEFINE VMBATCH * UACC(NONE)`

Allow the FTP server to be an alternate user to any id

- `RAC PERMIT * CL(VMBATCH) ID(FTPSERVE) ACCESS(CONTROL)`

Miscellaneous – VMXEVENT

No VM commands or events are audited by default

A system event profile in the VMXEVENT class defines what to audit.

Many things you can select to audit or not:

e.g. All CP commands (183), SET (176) & QUERY(396) subcommands, Diagnose instructions (87), other special events

Example:

```
RAC RALTER VMXEVENT EVENTS1
  ADDMEM(DIAG03C/AUDIT DIAG084/AUDIT)
RAC SETEVENT REFRESH EVENTS1
```

List the settings that are active on the system, along with the profile name (new service)

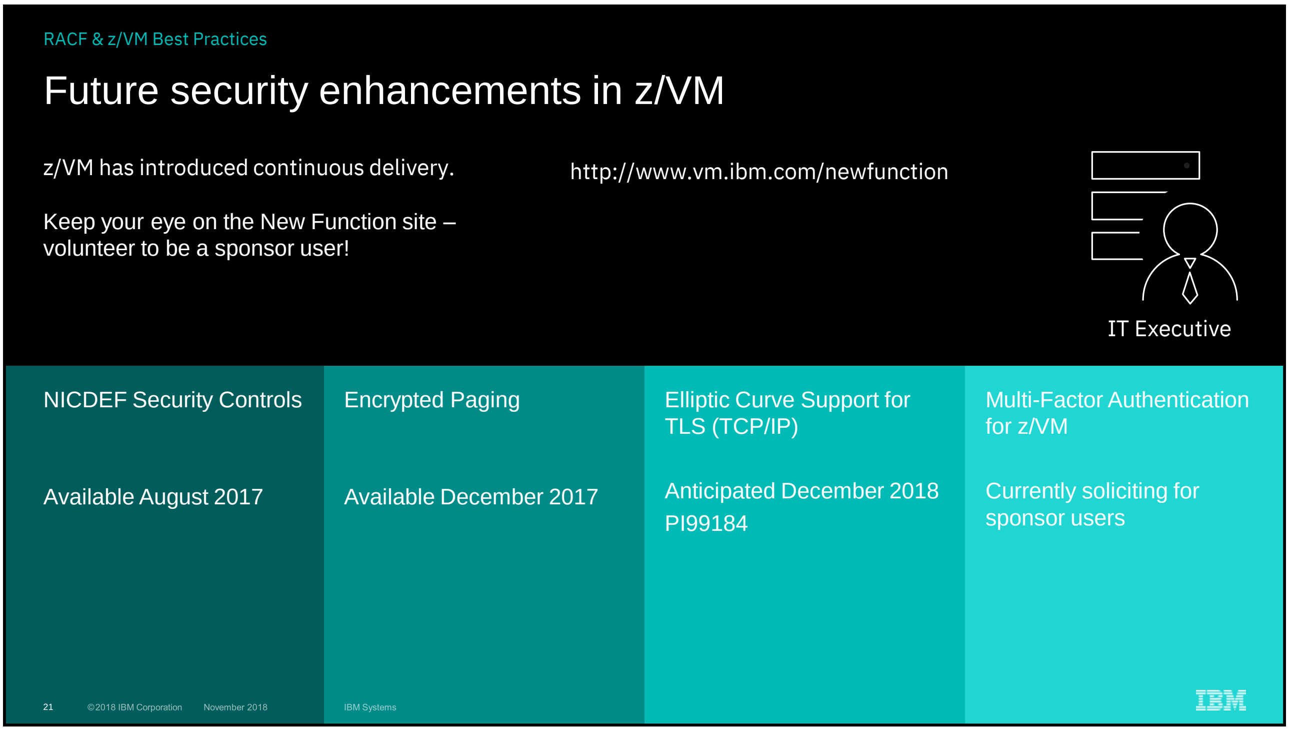
```
RAC SETEVENT LIST
```

List the settings in this profile

```
RAC RLIST VMXEVENT EVENTS1
```

What are YOUR opinions?

Guide & Share



RACF & z/VM Best Practices

Future security enhancements in z/VM

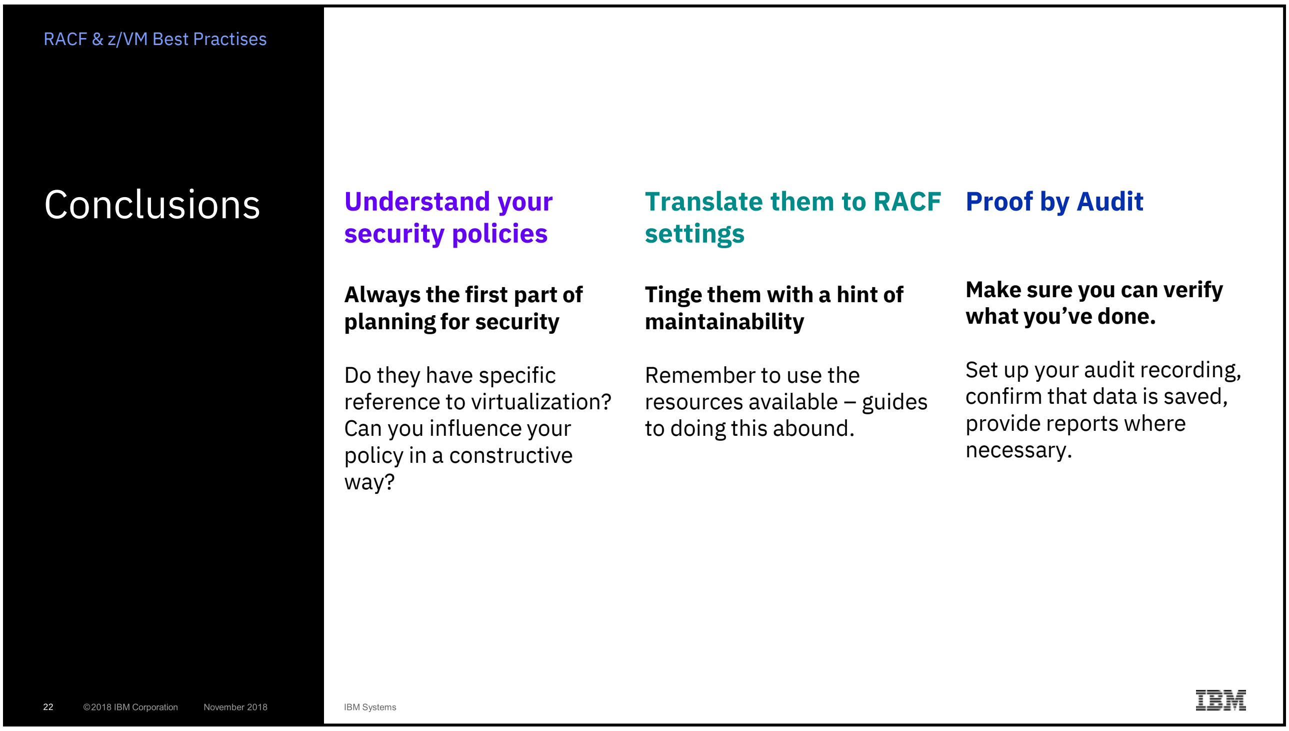
z/VM has introduced continuous delivery.

Keep your eye on the New Function site – volunteer to be a sponsor user!

http://www.vm.ibm.com/newfunction

IT Executive

NICDEF Security Controls	Encrypted Paging	Elliptic Curve Support for TLS (TCP/IP)	Multi-Factor Authentication for z/VM
Available August 2017	Available December 2017	Anticipated December 2018 PI99184	Currently soliciting for sponsor users



RACF & z/VM Best Practises

Conclusions

Understand your security policies

Always the first part of planning for security

Do they have specific reference to virtualization? Can you influence your policy in a constructive way?

Translate them to RACF settings

Tinge them with a hint of maintainability

Remember to use the resources available – guides to doing this abound.

Proof by Audit

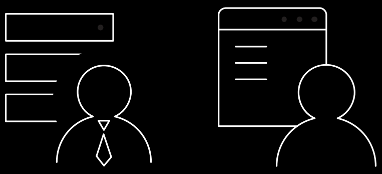
Make sure you can verify what you've done.

Set up your audit recording, confirm that data is saved, provide reports where necessary.

Acknowledgements

Without the following folks, I would have been struggling to make meaningful comments!

Any mistakes are my own.



Brian Hugenbruch,
IBM Z Security for Virtualization and Cloud

For source material and useful conversations while enjoying the Mediterranean hospitality

Bruce Hayden,
IBM Washington Systems Center

For source material from RACF on z/VM presentations at recent conferences

Paul Arnerich,
TSD Ltd

For allowing me to quote his view on "Best Practices", and other opinions

Malcolm Beattie,
IBM UK, z/VM Expert

For being the person I rely on to keep me straight on z/VM and Linux

References

Papers and Publications by Brian W. Hugenbruch:

https://www.vm.ibm.com/devpages/hugenbru/pubs.html

Includes:

- 'Validating and Repairing RACF Database Integrity on z/VM'
- 'Passtickets, Please: Introducing Security Changes for z/VM 6.4'
- 'The Care and Feeding of Your RACF for z/VM Passwords'
- 'Best Practices for NJE on z/VM: Security Configuration Steps for RSCS and VMBATCH'
- 'Enabling the FACILITY Class for Use by RACF for z/VM'

z/VM Security and Integrity Resources

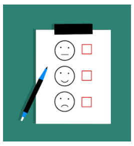
- http://www.vm.ibm.com/security

z/VM Statement of Integrity

- http://www.vm.ibm.com/security/zvminteg.html

We want your feedback!

- Please submit your feedback online at ….
  - ➢http://conferences.gse.org.uk/2018/feedback/CM
- Paper feedback forms are also available from the Chair person
- This session is CM



GSE UK Conference 2018

Better, stronger, faster; The Mainframe….. the Machine!

RACF & z/VM Best Practices

Geoff Rousell
IBM

November 2018
Session CM