Wadaya Mean I Can't Share My RACF Database Between z/VM and z/OS

Aaron Graves, IBM

aaron.graves@ibm.com

Agenda

- Intro
- IBM Z ISV Development Programs
- The Official Statement
- Initial Plans
- Twists and Turns
- Where We Are Now
- Lessons Learned

About Me

- 5 Years with IBM
- Previously a customer for a long time
- Started as a COBOL and then a PL/I applications programmer
- Switched to Systems Programming – CICS, VTAM, NCP on MVS
- Introduced to VM via VM/VTAM installation
- After Linux on Z introduced became primary focus

IBM Z ISV Development Programs

- Administer on-premise hardware/software programs for ISV’s
- Provide z/OS (ADCD) and z/VM packaged systems for zPDT download
- Provide z/OS, z/VM and Linux on Z development systems for ISV’s
- Host website for ISV disclosure material
- Multiple z/VM systems hosting the ISV guest systems

The “Statement”

Removal of RACF for z/VM support for RACF database sharing between z/VM and z/OS

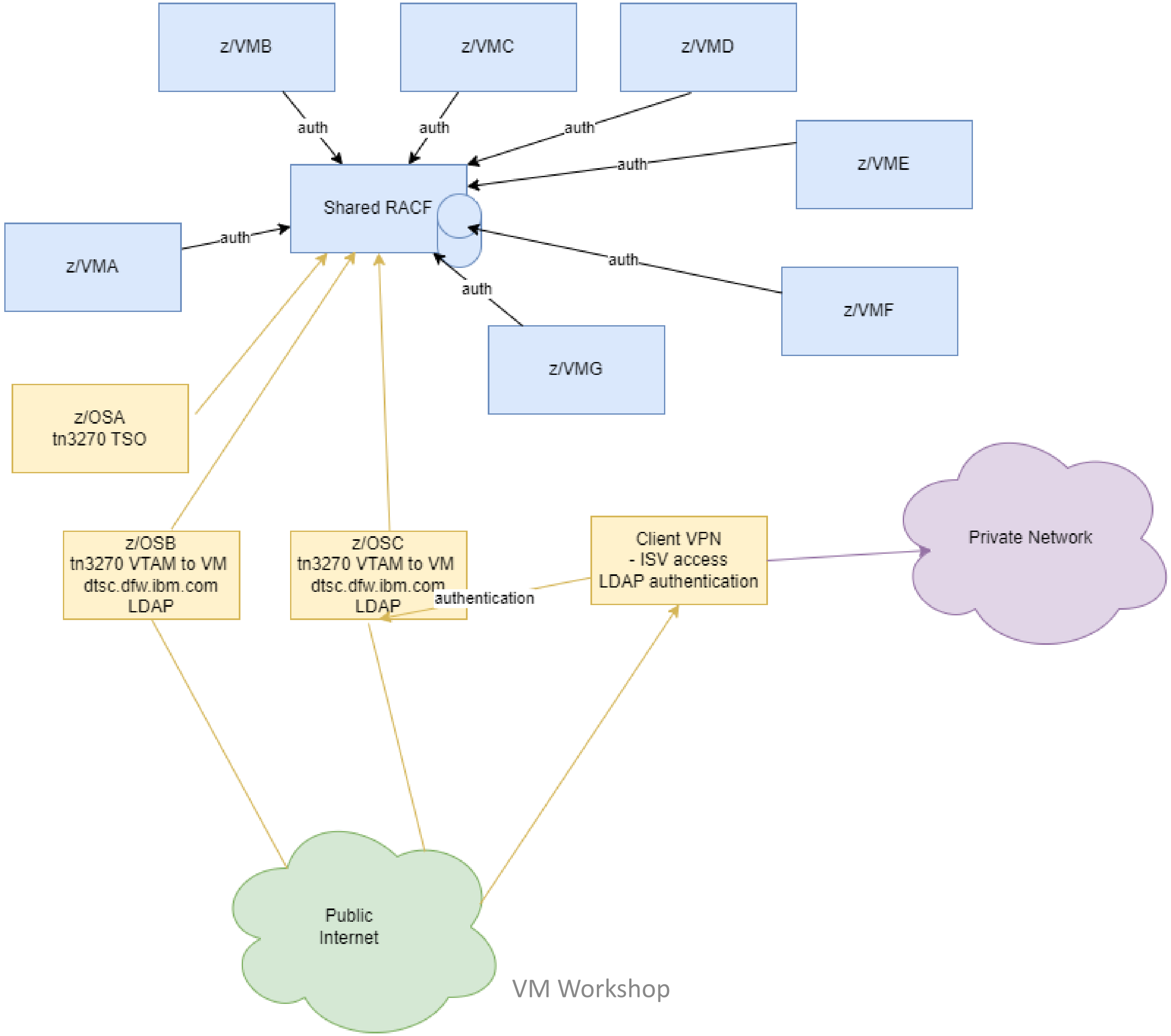
z/VM 7.2 is intended to be the last z/VM release to support sharing RACF databases between z/VM and z/OS systems.

While databases may remain compatible, sharing between operating systems is discouraged due to the distinct security and administration requirements of different platforms.

A future z/VM release will be updated to detect whether a database is flagged as a z/OS database and reject its use if so marked.

Sharing of databases between z/VM systems, whether in a Single System Image cluster or in stand-alone z/VM systems, is not affected by this statement.

Shared RACF Database



Initial Plan

- Just split/copy the RACF database and use the Directory Integrator product to synchronize the z/VM and z/OS copies
- No other changes – same user experience
- Issue uncovered:
  - Current versions of DI (IBM Security Verify Directory Integrator) do not have an “all on Z” option – no desire to support “off-platform” components
- Began looking at alternatives
- Data center move - GH-breakfast240129Avsl_bluetoast240212B-v01-m01-f00-c00 (youtube.com)
- Project put on hold

Refresh and Resume

- Fresh approach – everything on the table
- New compliance requirements – Multifactor Authentication
- What about using “IBMid” for authentication?
  - Uses Open ID Connect (OIDC) protocol
  - Supports MFA
  - Most ISV’s already have one
- Cisco VPN supports SAML with OIDC – ☺
- Apache server – uses mod_auth_openidc module for OIDC
  - Not available on z/OS - ☹

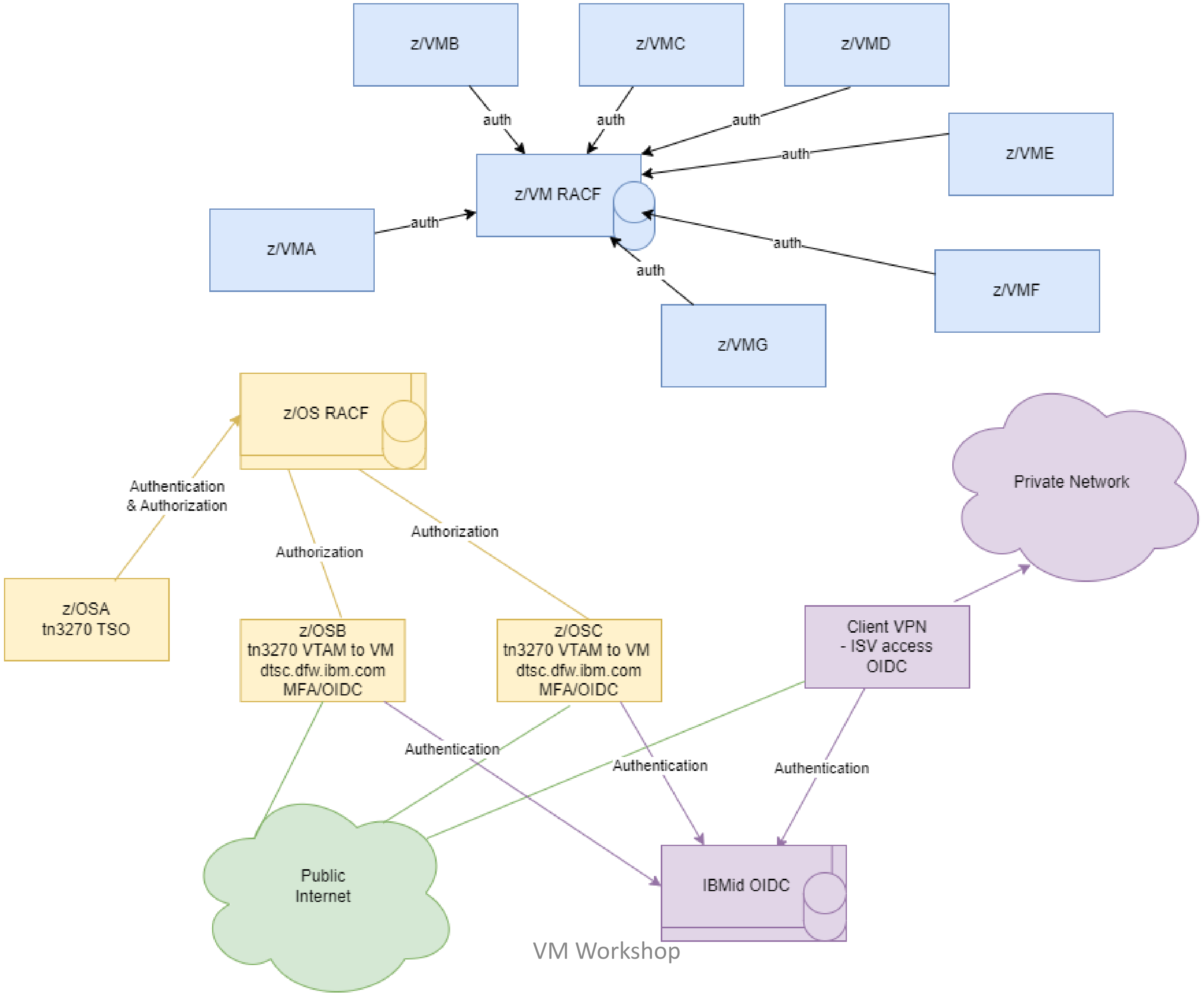
New Approach for z/OS Apache

- Look at IBM Z Multifactor Authentication product
- MFA V2.2 current
- RACF password + MFA token for authentication
- Satisfies compliance requirement
- Subset of users to manage separate passwords in z/OS and z/VM
- Paused for higher priority project

Serendipity!

- MFA V2.3 available
- From “Summary of Changes”
  - You can configure IBM MFA to perform single sign-on (SSO) by using the OpenID Connect (OIDC) protocol.
- YAY!
- Requires nodejs which provides the OIDC support
- IBMid gets mapped to RACF id for authorization

Split RACF Databases



End State

- RACF on z/VM for authentication and authorization
  - Adding passphrase and TN3270 encryption for compliance
- IBMid (OIDC) for VPN authentication
  - Cisco ISE server for authorization
- IBMid (OIDC) for z/OS website authentication via Z MFA
  - Mapping of z/OS RACF id to IBMid for authorization
- Native z/OS authentication and authorization for internal staff
  - Manage separate passwords for z/VM and z/OS

Lessons Learned

- Solutions are always “Point in Time”
- It’s OK to “Erase the Board”
  - If you have the time
- Sometimes you get lucky ☺

Questions?

Thank You!