

Saying Goodbye to the LDAP Server for z/VM

Brian Hugenbruch, CISSP
IBM z/VM Security and Cryptography Product Owner
[*bwhugen@us.ibm.com*](mailto:bwhugen@us.ibm.com)



Agenda

- **Statement of Direction**

- What LDAP is, and why it might have been load-bearing
- Some of its use-cases today

- **Why is it going away?**

- What breaks when it does?
- And what doesn't break?

- **Use-cases for Identity Management on z/VM with LDAP and RACF (and other things)**

- What can we do today without LDAP?
- What can we not do?

- **What does the future hold?**

- And how can that help us with these uses cases?
- Any gotchas?
- How can “I” help?

- **Summary**



z/VM and Identity Management

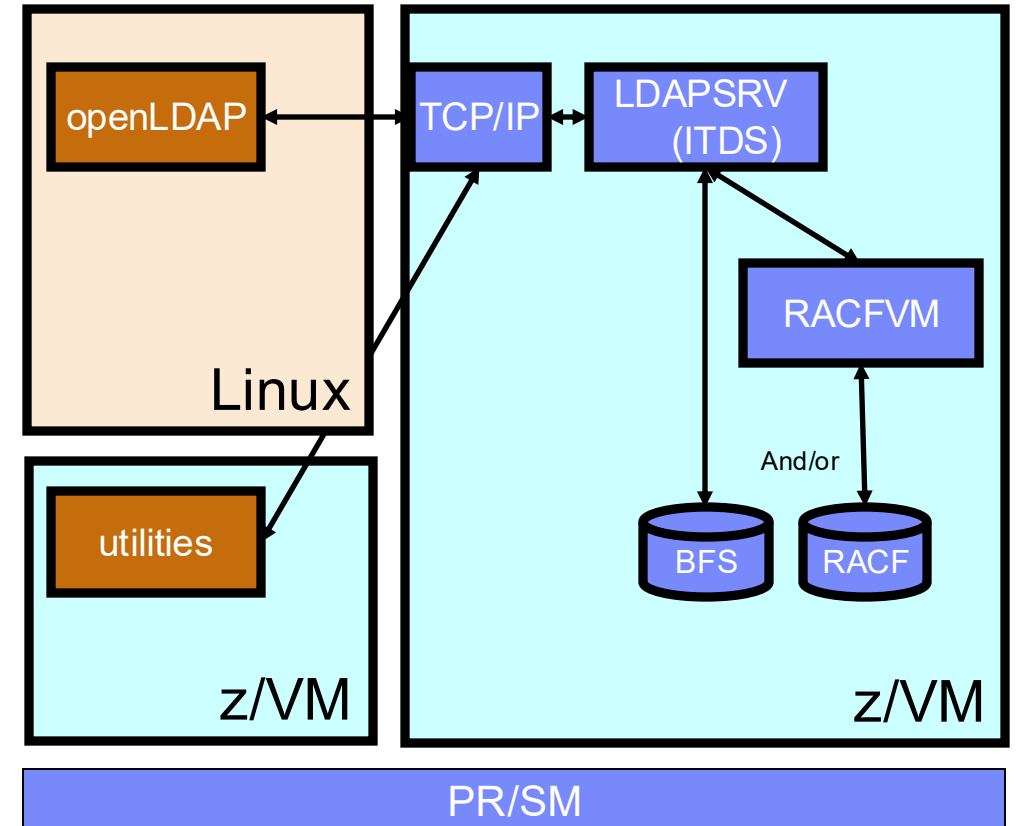
- A Statement of Direction was issued with z/VM V7.4 General Availability:

z/VM V7.4 is planned to be the last z/VM release to support the z/VM LDAP server. This server, a rehost of the z/OS Directory Server, will be removed from z/VM TCP/IP as part of a future release. This includes the LDAPSRV virtual machine and associated components. All future releases will continue to support ldap-bind as an authentication factor through the IBM Z Multi-factor Authentication product.

CMS-based LDAP client utilities, and the RACF r_admin interface, are not impacted by this statement.

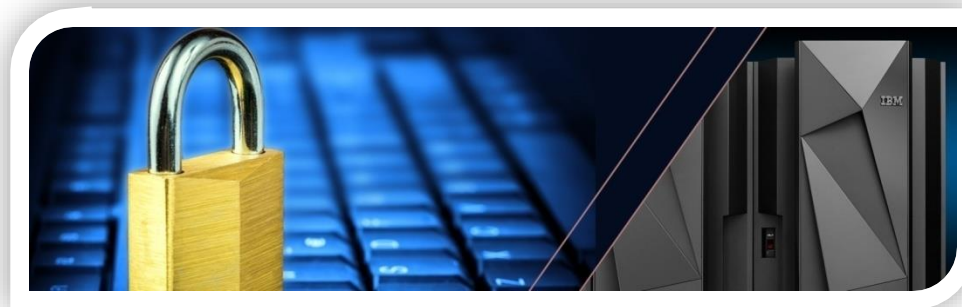
LDAP server and utilities

- **Port of z/OS ITDS V2.2**
- **Enables remote hosts or applications to securely authenticate** users against the RACF database on z/VM
 - E.g. Linux PAM
- **Enables central management** of z/VM passwords
- **Remote audit** via LDAP extended operation
- **CMS client utilities**
 - ldapadd, ldapsrch, ldapmdfy, ldapmrdn, ldapdlet

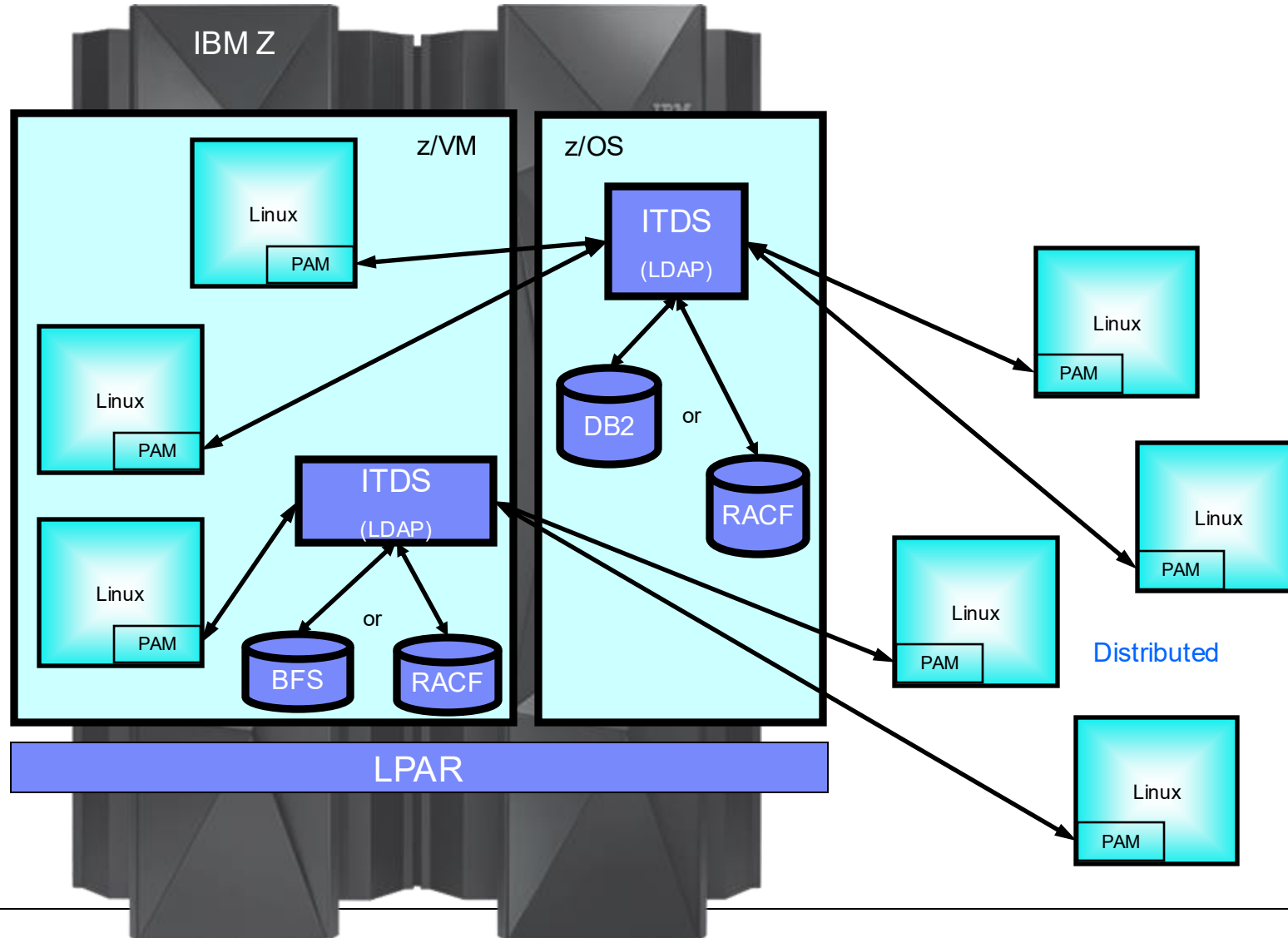


Leveraging the platform to Centralize Security Function

- Take advantage of the proximity of LinuxONE systems to other LinuxONE or IBM Z machines to streamline certain functionality, such as ...
 - **Centralized Identity, Authentication, and Audit**
 - ITDS (LDAP Server) for z/VM or z/OS, using DB2, BFS, or RACF as a back-end
 - PAM plug-ins for Linux machines (regardless of architecture)
 - Additional plug-ins to auditd for centralized audit – pushes events out to SMF records
 - **Password Synchronization**
 - Using ITDI (IBM Tivoli Directory Integrator), LDAP, and RACFVM
 - **PKI Services** (z/OS PKI Services, connected to Linux guests)



LDAP (ITDS) and Centralized Security



Authentication

- Common Client – Linux PAM
- Integrated LDAP Server on z/OS and z/VM
- LDAP backed by RACF or DB2® or BFS

Audit

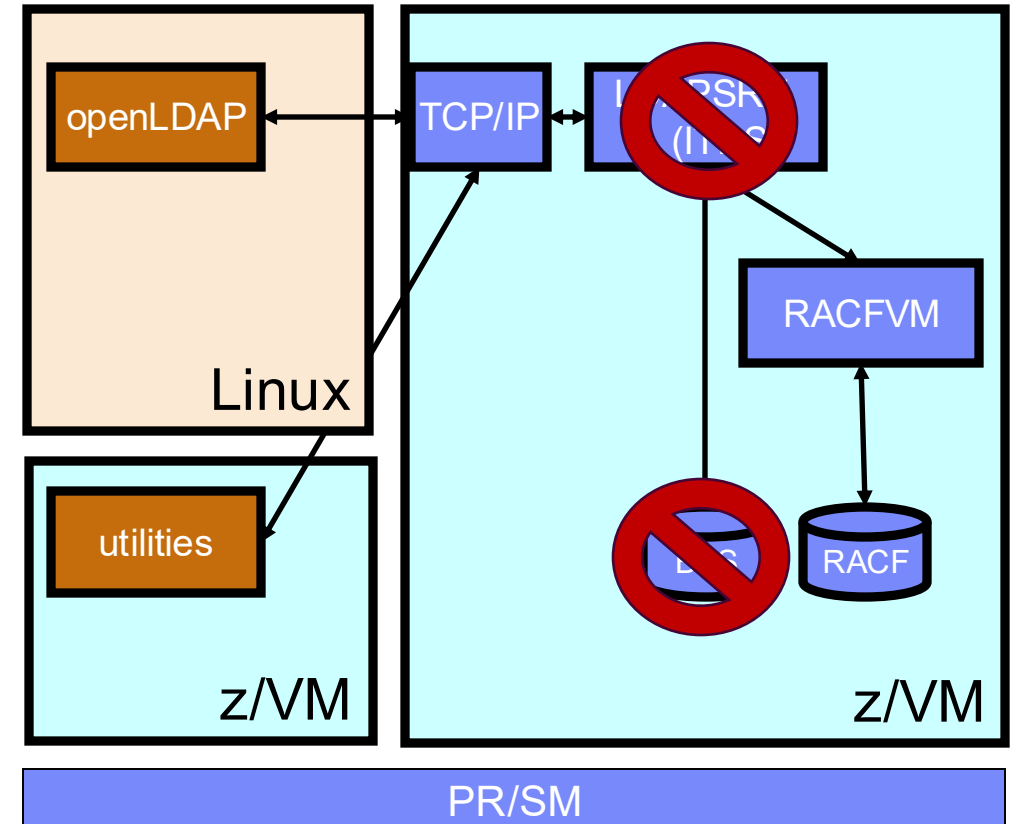
- Common Client – auditD with plug-in
- Integrated LDAP Server on z/OS and z/VM
- LDAP backed by RACF

...and it's going away? Why?

- Systems management has changed in the past 50 years
- “Port of z/OS ITDS 2.2”
- “What does the B stand for?”

Ok. So what's going to break?

- If the LDAP server goes away, then that impacts...
 - Anyone using LDAPSrv in LDBM for local **authentication**
 - Anyone using LDAPSrv with native authentication / SDBM for **authentication** via RACF
 - Anyone using LDAPSrv to automate VM guest **provisioning** / remove humans from the identity management flow
 - Anyone using LDAPSrv and SDBM to **fuel logon decisions**



```
>> rac listuser brianh
```

```

USER=BRIANH NAME=UNKNOWN OWNER=IBMUER CREATED=10.209
DEFAULT-GROUP=SYS1 PASSDATE=11.031 PASS-INTERVAL=186 PHRASEDATE=N/A
ATTRIBUTES=SPECIAL OPERATIONS
ATTRIBUTES=AUDITOR
REVOKE DATE=NONE RESUME DATE=NONE
LAST-ACCESS=11.202/16:14:15
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED (DAYS) (TIME)
-----
ANYDAY ANYTIME
GROUP=SYS1 AUTH=USE CONNECT-OWNER=IBMUER CONNECT-DATE=10.209
CONNECTS= 70 UACC=NONE LAST-CONNECT=11.202/16:14:15
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
SECURITY-LABEL=SECL4
DEFINITION OF THIS SECURITY LABEL IS:
SECURITY-LEVEL=CONF
CATEGORY-AUTHORIZATION
PROJD
PROJE

```

User: Who am I?

Group: What is my security context?

Attributes: Any bonus authorities?

What's not changing?

- **RACF/VM.** RACF is not going anywhere.
 - Neither is VM:Secure, to be clear
 - But VM:Secure never integrated with the LDAP Server anyways

- **z/OS ITDS.** The MVS team has no plans to do anything like this.

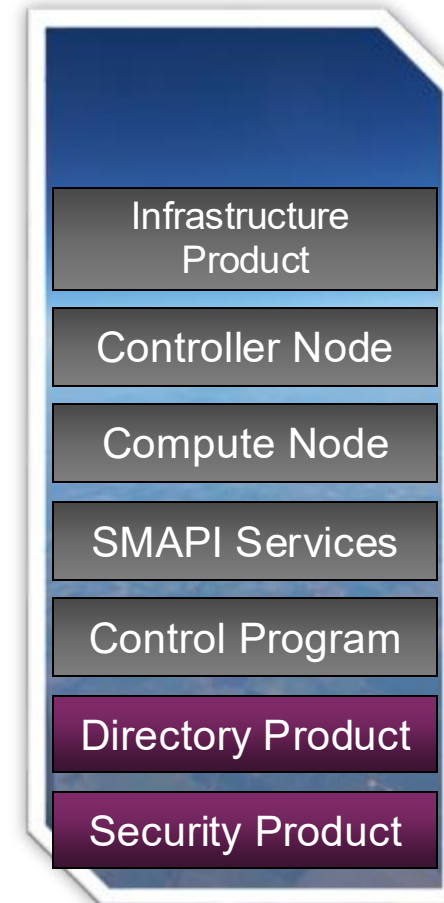
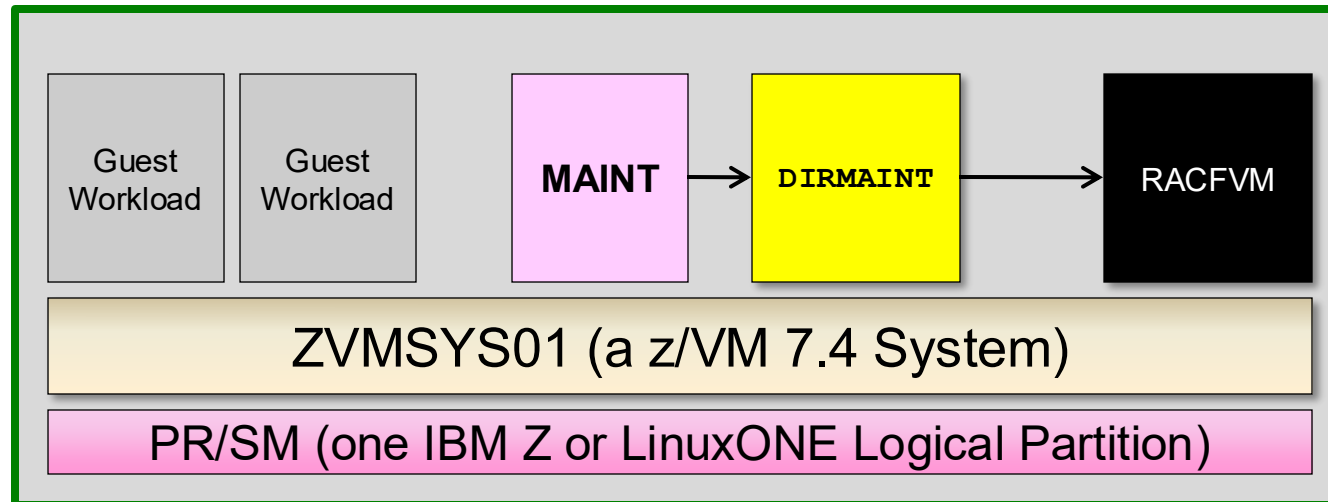
- **CMS client utilities.** You can't point them at a z/VM LDAP server...
 - But if you use them to talk to MVS LDAP, or Linux LDAP, that's fine

- **zSecure management of RACF/VM**
 - This continues to work based upon RACF exits and CMS-based management

- **The DirMaint-RACF Connector.** This translates directory changes into security policy
 - Used today by when running with IBM Cloud Infrastructure Center
 - LDAP functionality not involved here – used for other management applications

Security and Provisioning: *The DirMaint-RACF Connector*

- An exit between the Directory Maintenance Facility and RACF for VM
 - Enable in **CONFIGRC.DATADVH** (the initial EXEC is DVHRUN.EXEC)
 - Translates system admin tasks (e.g., the creation of a minidisk) to security policy
 - Lessens need for two administrators (one system, one security) to be work in tandem
 - Local plug-ins can be written, added, and enabled for extra functionality



LDAP? But I was using that! *What do I do now, IBM??*

- It is acknowledged that the IBM SoD did not also deliver (or even promise) an immediate and comprehensive replacement

- MFA may help in some use-cases
 - *It will not help in others*

- What we're going to do now is look at identity management and CP LOGON from a few different configurations

First: Ground rules.

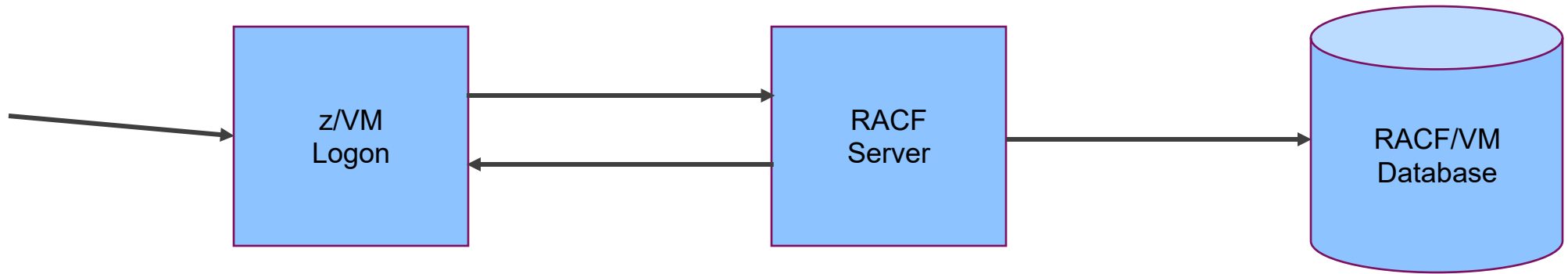
- **Passwords (or phrases) are for humans**

- You should be using **LOGONBY** for all service virtual machines
 - IBM has, over the course of z/VM V7.x, moved many of these to LBY IBMVM1
 - IBMVM1 should be replaced by your local humans (e.g. BWHUGEN)
 - We're still working on the rest for default configuration

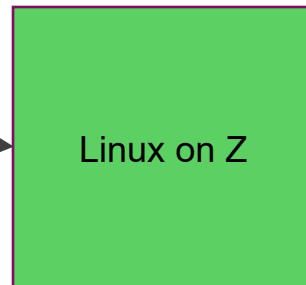
- **Check with your security people about the need for MFA**
 - It's a different authentication flow (out-of-band), but it may make your life easier long-term
 - Just because they haven't said anything doesn't mean the requirement isn't there

Logging onto a userid – the direct approach

z/VM Admin



Linux End User

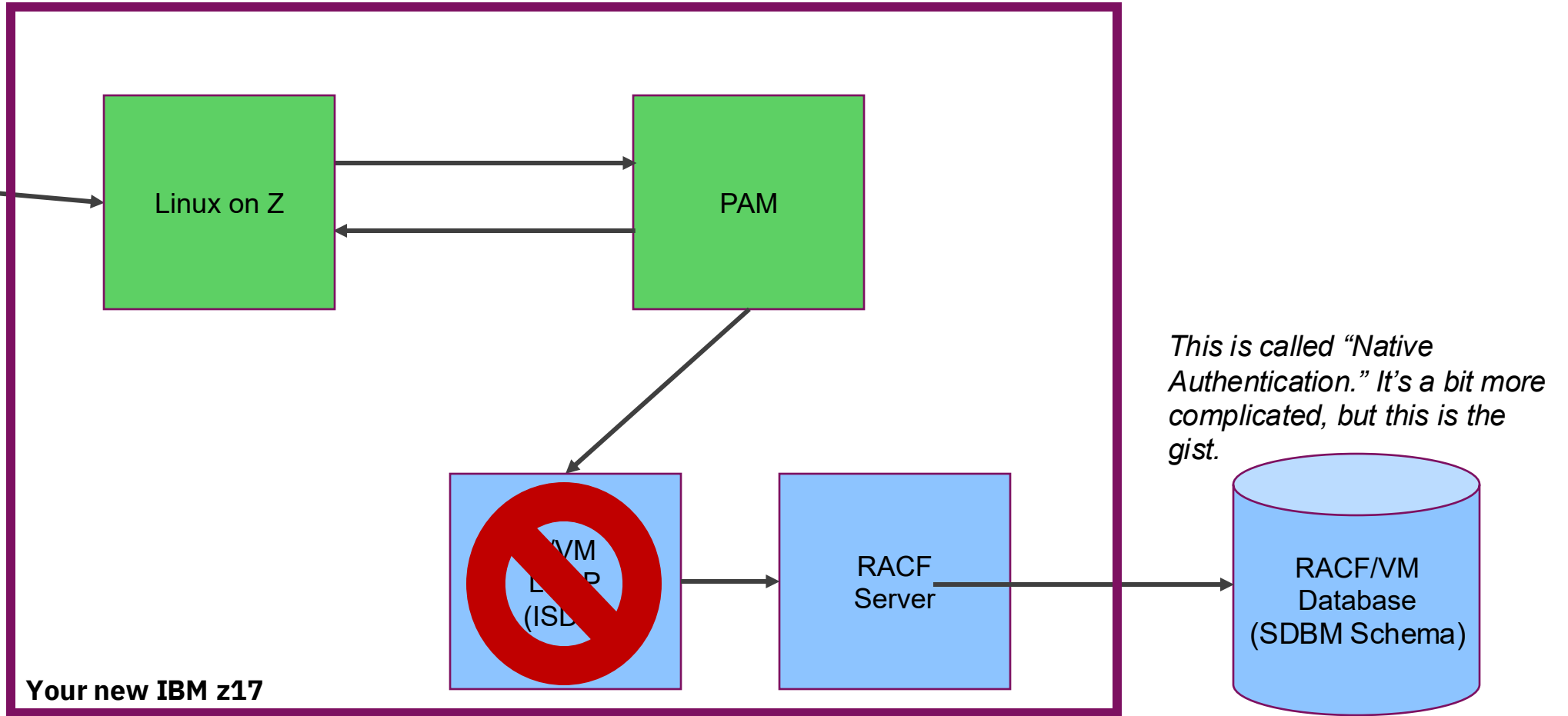


Absent adjustments made to the pluggable authentication module (PAM), Linux will check against local identity repositories. Please don't use root, you heathens.

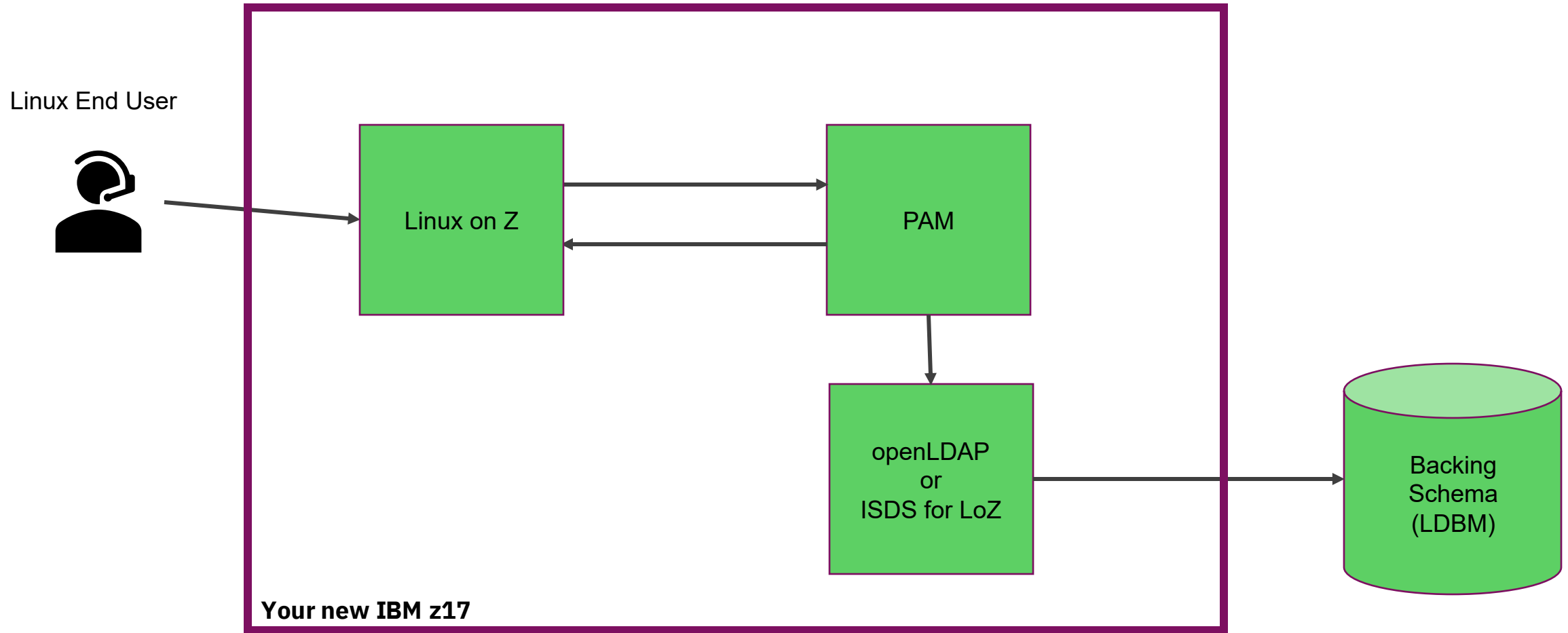
We're assuming you have an ESM, because we assume you want security. If you don't want security, this is a short discussion.

Logging onto a Linux guest using LDAP on z/VM (backed by RACF)

Linux End User

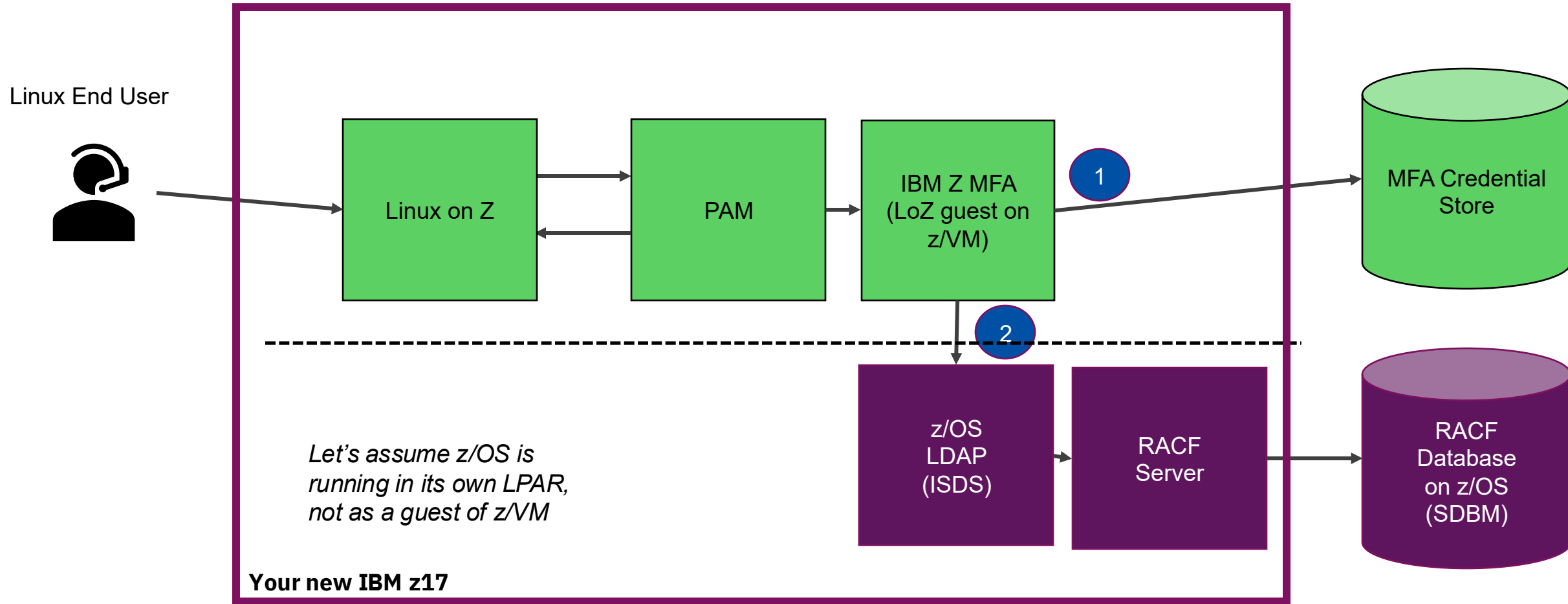


Try instead: Logging onto a Linux guest using Linux-hosted LDAP



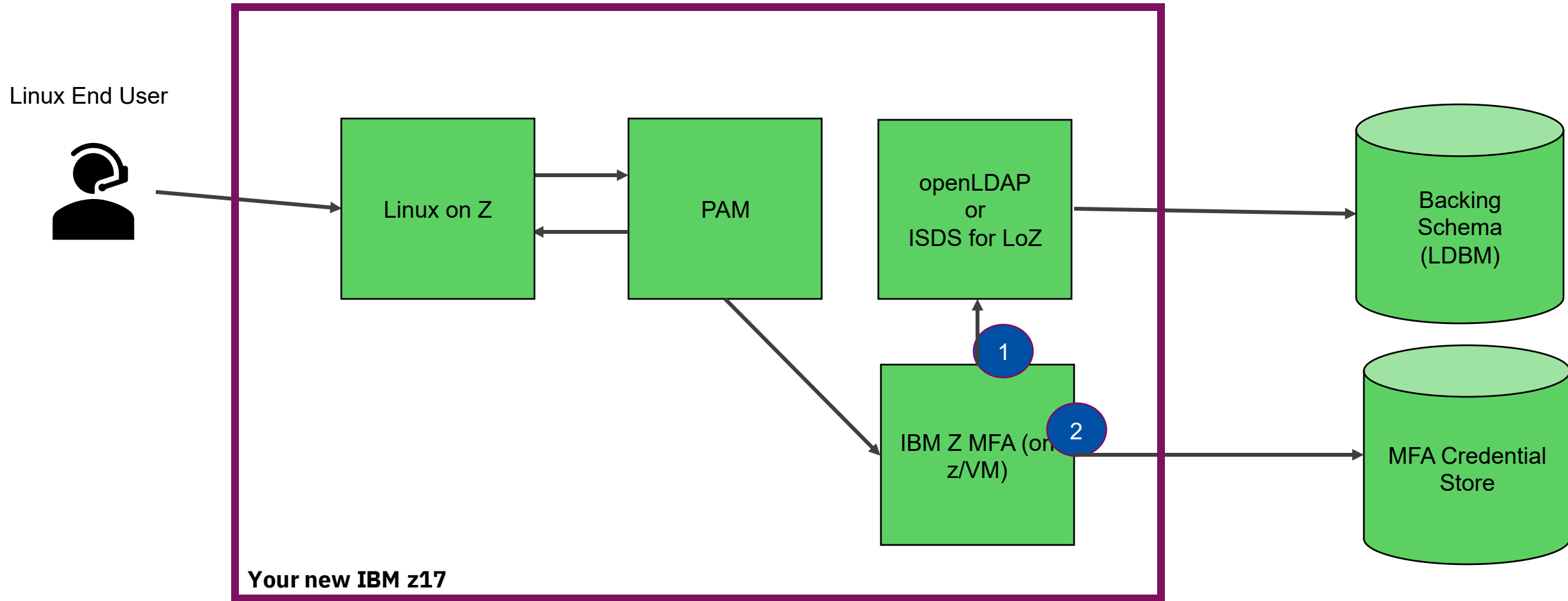
Try instead:

Logging onto a Linux guest using IBM Z MFA with both Idap-bind and Yubikey (with z/OS)

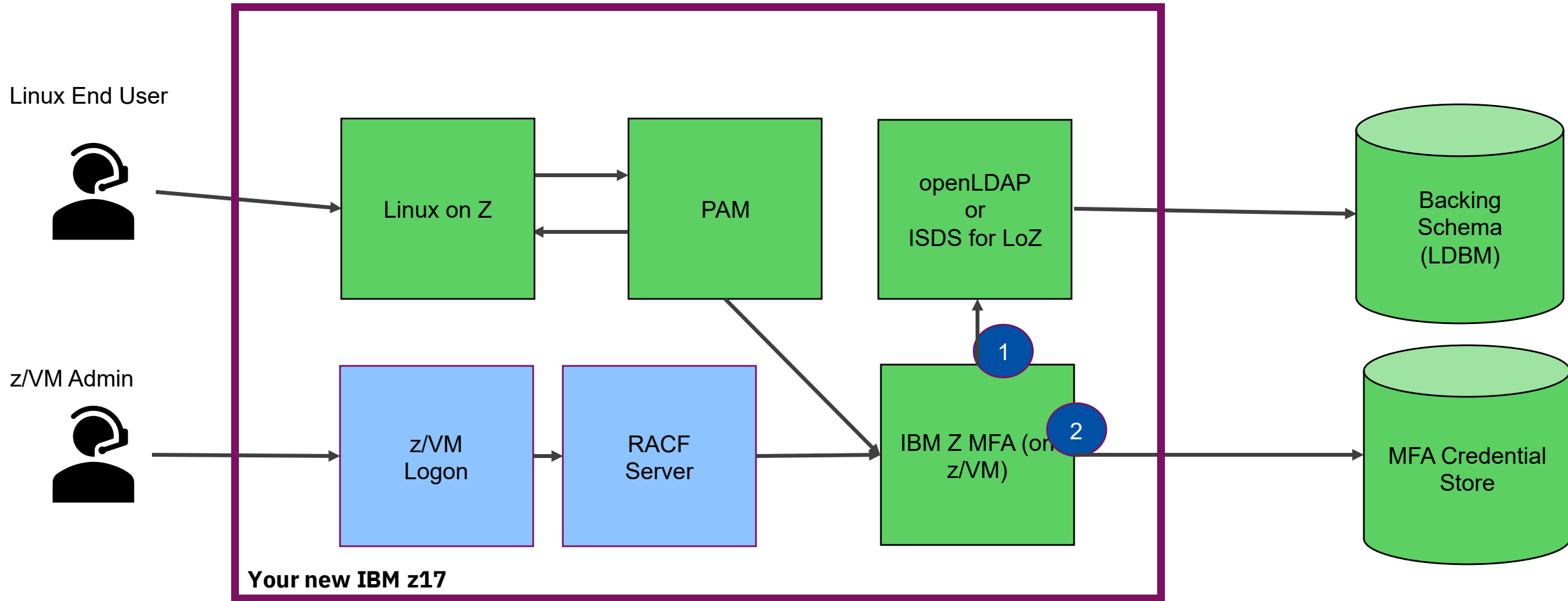


Try instead:

Logging onto a Linux guest using IBM Z MFA with both Idap-bind and Yubikey (all Linux)



...and then let's add z/VM back in.



z/VM and Identity Management

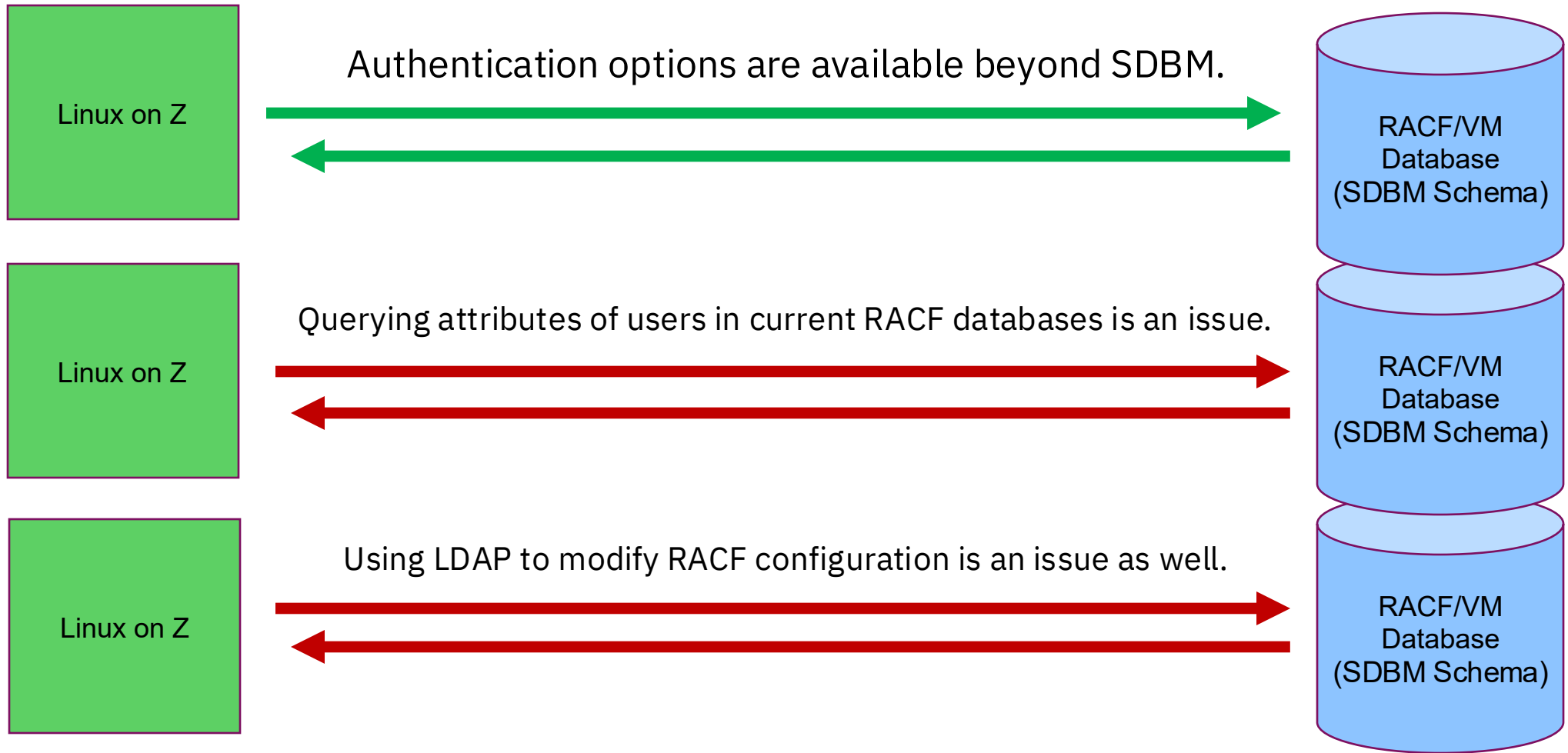
- **There are immediate alternatives to z/VM LDAP under CMS**

- Linux ISDS and openLDAP do exist (does not talk to RACF)
- If SDBM schema matters to you, hooking into **IBM z/OS LDAP** (through IBM Z MFA, or directly via PAM) is an option
 - You can still copy a RACF/VM database over to z/OS RACF and have it function...
 - But you're back to worrying about collisions in name-space between z/OS and z/VM

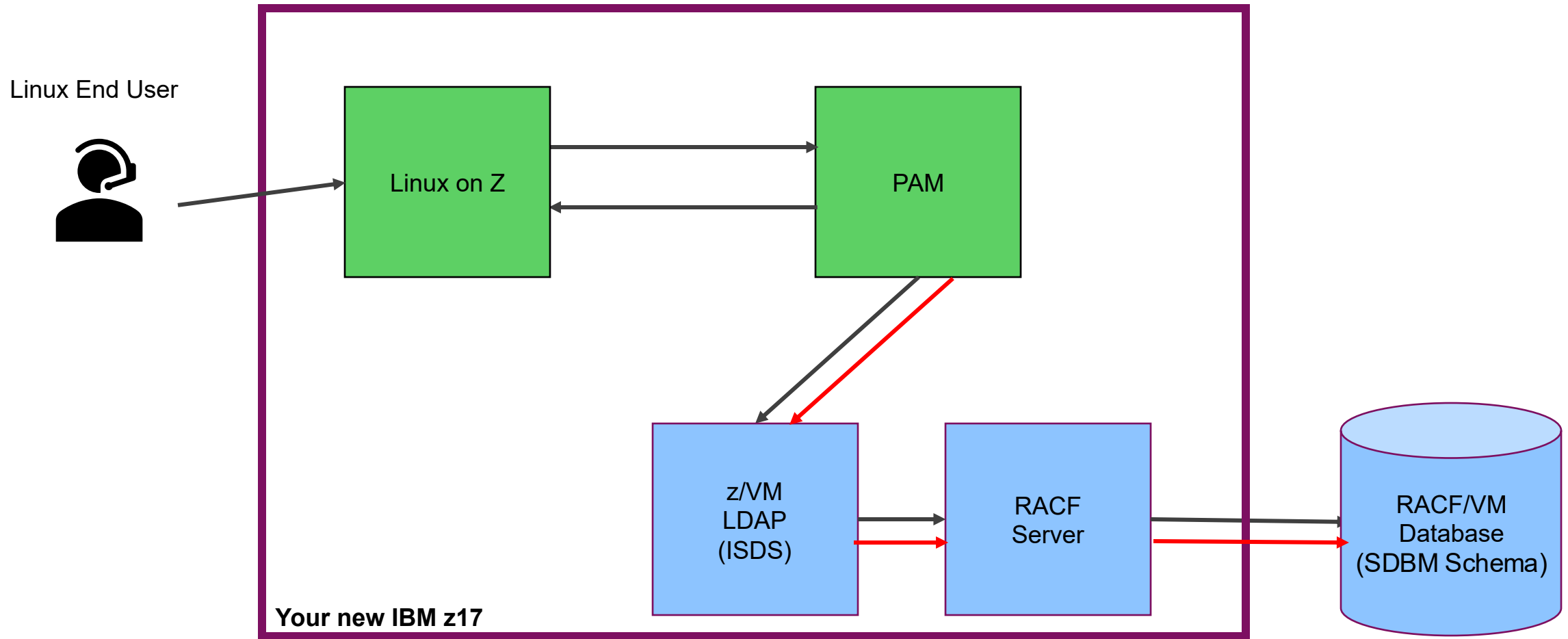
- **IBM Z Multi-Factor Authentication** allows for an all-Linux solution and supports z/VM host logon as well

- Out-of-band authentication (yes, I know, I know)
- \$\$\$

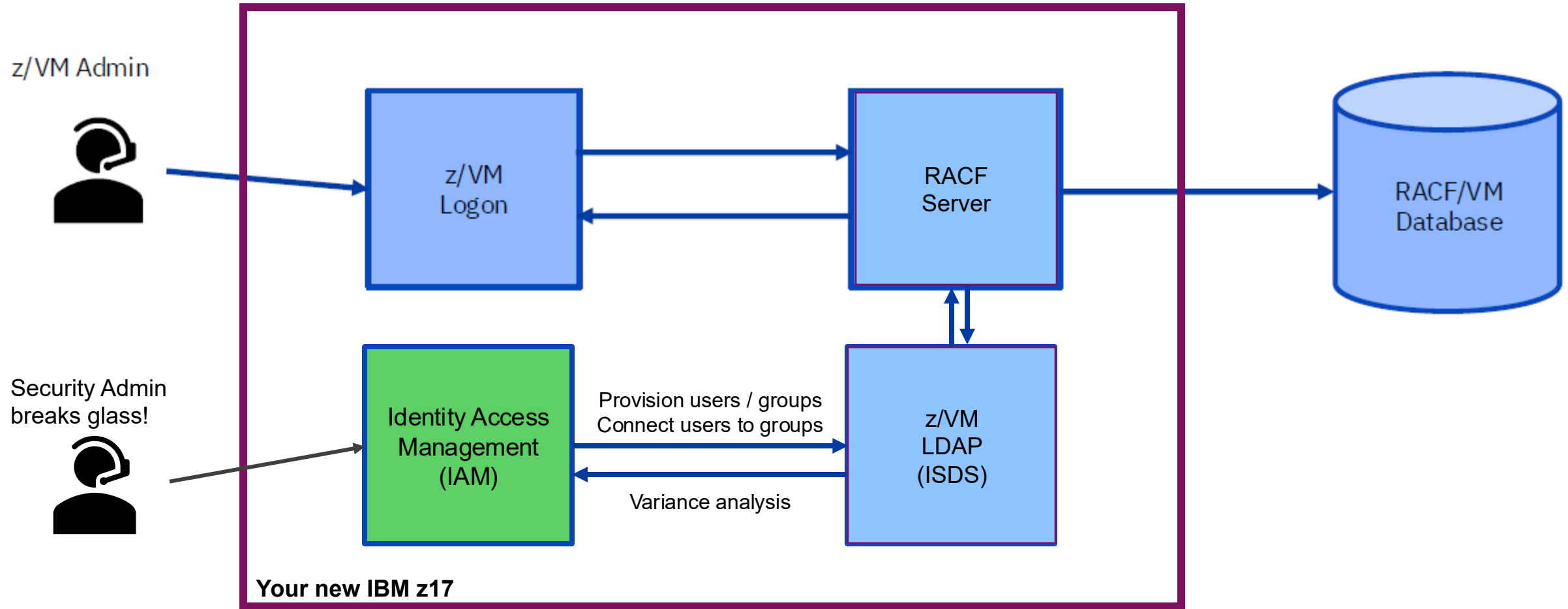
- *No option is perfect, and IBM is looking to upgrade certain interfaces to enable new forms of support*



LDAP on z/VM with SDBM backend, querying RACF attributes to make security decisions in PAM



LDAP on z/VM with SDBM backend to integrate RACF on z/VM with Identity and Access Management (IAM) Tooling



z/VM and Identity Management

- **There are immediate alternatives to z/VM LDAP under CMS**
 - Linux ISDS and openLDAP do exist (does not talk to RACF)
 - If SDBM schema matters to you, hooking into IBM z/OS LDAP (through IBM Z MFA, or directly via PAM) is an option
 - You can still copy a RACF/VM database over to z/OS RACF and have it function...
 - IBM Z MFA allows for an all-Linux solution and would support z/VM host logon as well

- ***No option is perfect, and IBM is looking to upgrade certain interfaces to enable new forms of support***

- **The goal is, ultimately, to simplify management**
 - We're having this discussion now because it will take time to adjust
 - Guidance on migration paths is coming soon
 - The z/VM New Function Webpage will be updated with new projects in this area as they grow

What do you mean by “new projects” ...?

The following is a mix of concepts and projects in design phase.

This is a mix of topics that are conceptual in nature and projects in design phase. There are **no** plans in place at this point to deliver some of this capability. **We simply want to discuss these, get your reaction and feedback in order to determine if/how to pursue.**

We do not recommend basing any plans on this capability.

For formally committed projects under development, refer to the z/VM New Function Webpage: <https://www.vm.ibm.com/newfunction/>

Be advised, the next few slides won't be in the handouts

[REDACTED]

Linux Native Interface for RACF	
Name	Linux Native Interface for RACF
Description	An interface for management of RACF from Linux on IBM Z is required as a successor interface to LDAP. This may be used for general authentication to RACF, to inquire about security policy, and to make authorized updates to z/VM security.
Status	Currently in design.
Target availability	TBD
Compatibility	No known incompatibilities.
Enablement	Apply Linux specific service and update RACF settings as appropriate.
Effect	There is no effect on systems that do not enable the new behavior.
ISV impact	No known impacts at this time.
Linux or hardware interaction	Linux interaction. Linux distribution and version TBD.
Environment variable name	N/A
Release(s)	z/VM Next
Service details	See below for the IBM service information.
<u>APAR</u>	TBD
<u>PTF</u>	TBD
<u>RSU</u>	TBD
Sign up	Contact Kerry Wilson - kerryw@us.ibm.com to become a Sponsor User .

Questions?
(Anyone throwing tomatoes should use this opportunity, thanks!)

Summary

- **LDAP/VM (the server) is going away**
 - Not the CMS client utilities
 - Not RACF/VM
 - Not z/OS ITDS

- **Some options exist to help with authentication and provisioning today**
 - MFA may be needed in your shops soon enough
 - ICIC or zSecure would provide a wildly different path toward secure provisioning

- **Sponsor user project for a **successor** interface starting soon**
 - **Won't solve every use case**
 - **Will position z/VM for a simplified management experience in the future**
 - Your feedback is vital to our success – please get involved!

Thank you!



Brian W. Hugenbruch

IBM Z and LinuxONE Security Certification Lead &&
IBM LinuxONE Resiliency Lead &&
IBM z/VM Security and Cryptography Product Owner


VM Security Page: <https://www.vm.ibm.com/security/>

VM New Function Webpage: <https://www.vm.ibm.com/newfunction/>

Brian's Technical blog: <https://bwhugen.github.io>

Social Media:

 <https://www.linkedin.com/in/bwhugen/>

 @the_lettersea

 @apictureofaman@infosec.exchange



Fun