

DKM HARDENING IS SCHEDULED. THE PROOF IS NOT.

KB5121391 · CVE-2026-56155 · enforcement by October 13, 2026

Audit, opt-in, enforcement

THE SCHEDULE MICROSOFT PUBLISHED IN JULY

01 AUDIT

July 14 update

Detects one minute after AD FS starts, then every every 24 hours. Changes nothing. A mismatch logs mismatch logs event **1132**.

02 OPT-IN

Registry value

Set **RemediateDkmAcl = 1** on any one AD FS server in the farm. Runs at the next cycle or service restart.

03 ENFORCEMENT

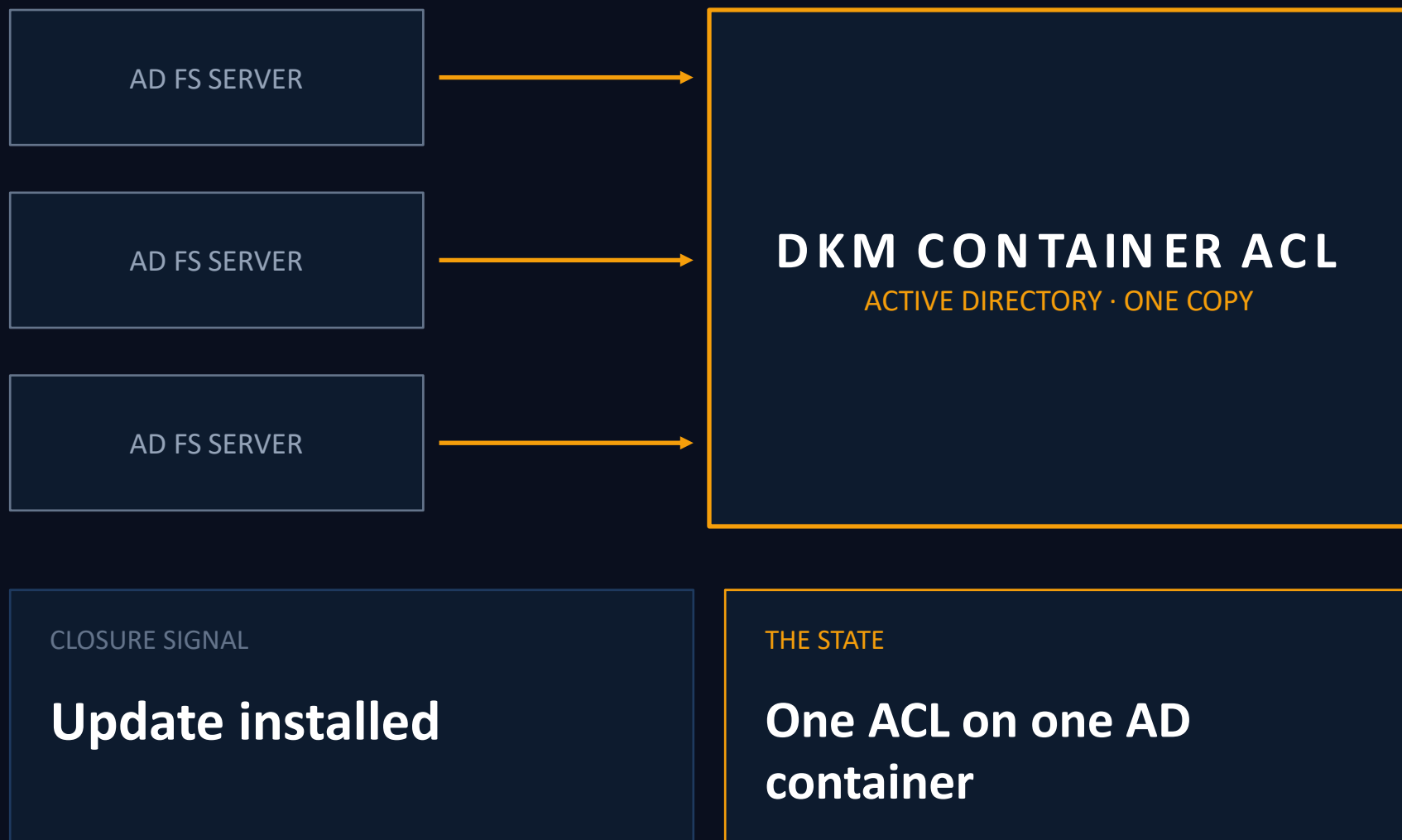
October update

Remediation runs by default. **RemediateDkmAcl = 0** opts out, and Microsoft says that leaves the container vulnerable.

An announced date is not a deployed update.

One ACL. One AD container

THE CLOSURE SIGNAL IS NOT THE STATE



Evidence lives in an event log on each AD FS server. In many organizations, the AD the AD team holds the container and the AD FS team holds the log.

Two paths to the same container

THE OCTOBER UPDATE DOES NOT TREAT THEM ALIKE

2016 · 2019 · 2022 · 23H2 · 2025

Remediates by default

The October update remediates remediates without the registry registry key.

RemediateDkmAcl = 0 opts out.

SERVER 2012 · 2012 R2

Does not auto-enable

Grant the AD FS service account explicit Allow ACEs for **WriteOwner** **WriteOwner** and **WriteDacl** on the container. Then set **RemediateDkmAd = 1**. Skip the grant and remediation attempts fail. fail.

The page does not describe a farm that mixes both generations. Neither does this deck.

What each event proves

AND WHAT IT CANNOT

EVENT	PROVES	CANNOT PROVE
1132 Warning	ACL mismatched at check time	Who changed it, or that anyone reviewed it
1133 Info	ACL matched at check time	That remediation ran, or the old ACL was kept
1134 Error	Detection failed	Anything about the ACL
1135 Info	Remediation succeeded; previous ACL logged as SDDL	That the SDDL still exists tomorrow
1136 Error	Remediation was attempted and failed	That the failure is resolved

1133 is a status. 1135 is the change evidence.

1135 is the evidence

AND IT LIVES IN A LOG THAT ROLLS OVER

Event 1135 records the previous ACL as SDDL when remediation succeeds.

Microsoft's note: logs can roll over at their size limit. An overwritten event means the previous SDDL is permanently lost.

Save the message off the server the moment it fires.

AD FS/ADMIN LOG (SIZE-LIMITED)



OLDEST ENTRIES ROLL OFF AT THE SIZE LIMIT

ANALYSIS: a later 1135 would record a drifted ACL as "previous." Keep the first one.

What stays on the container

THE FINAL ACL, AS MICROSOFT STATES IT

Domain Admins

Generic All (Full Control)

Enterprise Admins

Generic All (Full Control)

System

Generic All (Full Control)

AD FS service account

Read, Write, Create Child, Write Owner, Delete Tree

Every other explicit Allow ACE is removed. Inheritance is disabled and inherited ACEs are discarded. The page names none of them.

Before it enforces

01 • NAME THE OWNERS

Name the owner of the container ACL and of the AD FS/Admin log. Different teams? Put both on the change.

02 • READ THE EVENTS

Check every AD FS server for 1132, 1133 and 1134. Export any 1132: it carries the current ACL.

03 • DECIDE

Remediate now or opt out. Microsoft frames opt-out as for a specific compatibility need, with a manual hardening plan.

04 • 2012 AND 2012 R2

Grant the ACEs, set the value, expect 1135. Watch for 1136.

05 • PRESERVE 1135

Save the full message off the server. Forward the log somewhere a size limit cannot erase it.

06 • RECORD IT

Record the 1135 text as the change evidence. 1133 is a status: it carries only the DN.

THE UPDATE CLOSES THE TICKET.
ONLY THE EVENT TEXT CLOSES
THE QUESTION.

rack2cloud.com | Follow The Architect for more