What is a gMSA?

A gMSA (Group Managed Service Account) is a service account whose password is generated and rotated automatically by Active Directory, typically a 240-character value that changes on a schedule and that no human ever sees. Because the password is long and random, gMSAs defeat Kerberoasting and Silver Tickets, which rely on cracking a weak service-account password. They are the recommended fix for service accounts, with one caveat: control over who can read the gMSA password must still be tight.

HOW IT WORKS

01 Why it defeats attacks (and the one caveat)

gMSAs neutralise the cracking-based attacks:

- Kerberoasting fails because the 240-character password cannot be cracked offline in any realistic time.
- Silver Tickets fail for the same reason, since they need the service-account hash.

The caveat is the ReadGMSAPassword right: whichever principals are allowed to read the gMSA password (the `msDS-GroupMSAMembership` setting) effectively hold the account. If an attacker compromises one of those principals, they can retrieve the password:

- `gMSADumper.py -u user -p pass -d corp.local` or BloodHound's ReadGMSAPassword edge

So gMSAs move the risk from "crackable password" to "who can read it," which is a far smaller, auditable surface.

> AUDIT WHO CAN READ IT
>
> *A gMSA is only as safe as the list of principals allowed to read its password. Keep that list minimal and watch BloodHound for ReadGMSAPassword edges to it.*

02 How to use gMSAs well

- Migrate service accounts to gMSAs so passwords are long, random, and auto-rotated.
- Restrict msDS-GroupMSAMembership to only the hosts that genuinely run the service.
- Audit ReadGMSAPassword rights with BloodHound and remove needless ones.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Best Practices for Securing Active Directory

[3] Microsoft: Kerberos Authentication Overview

- Keep gMSAs out of privileged groups so a compromised one is not also an admin.
- Ensure the KDS root key is deployed and protected, as it underpins gMSA password generation.