CNEXT SECURITY SERVICES · FINDINGS REPORT · ONE-OFF

Active Directory findings report

CUSTOMER
Muster AG, Bern (fictional)

SCOPE
Forest muster.local, 2 domains, 4 domain controllers, 184 users

ANALYSED ON
13 October 2026

TOOLS
PingCastle 3.3, Purple Knight 5, BloodHound CE, Microsoft security baselines

3	7	11	4
critical findings	high findings	medium findings	paths to Domain Admin

When you receive this document: After the analysis, before the first implementation wave.

Summary

The directory is in good working order but carries decisions from 2014 to 2019 forward: service accounts with Domain Admin rights, NTLMv1 on two servers and one domain controller on Windows Server 2016. Four paths lead from an ordinary user account to Domain Admin; two of them can be closed with one change each.

Findings by severity

NO.	FINDING	SEVERITY	LOCATION	RECOMMENDATION
AD-01	Service account svc_backup is a member of Domain Admins, password without expiry since 2014	**Critical**	OU Service Accounts, group Domain Admins	Group managed service account, rights only on backup servers
AD-02	Unconstrained Kerberos delegation on SRV-FILE01	**Critical**	Computer account SRV-FILE01	Switch to resource-based constrained delegation
AD-03	Domain controller DC02 on Windows Server 2016, support ends 12 January 2027	**Critical**	DC02, Bern site	Replace with Windows Server 2025 in wave 2
AD-04	NTLMv1 allowed on SRV-BACKUP01 and SRV-PRINT01	**High**	Policy LAN Manager authentication level	Enforce NTLMv2, audit for two weeks first
AD-05	23 accounts with password never expires outside the service account OU	**Medium**	Various OUs	Review, let expire or run as gMSA

Attack paths

- Path 1: users in the Helpdesk group may reset passwords of the Server Admins group; one Server Admin is local admin on DC02. Closed by AD-06.
- Path 2: svc_backup signs in to SRV-BACKUP01, where NTLMv1 is allowed and another account holds local admin rights. Closed by AD-01 and AD-04.
- Paths 3 and 4: through the delegation on SRV-FILE01. Closed by AD-02.

Deliberate exceptions

- None. Exceptions you keep after the review meeting are recorded here with reason, owner and review date.

Next steps

Review of the report with IT lead and management on 20 October 2026; the plan of measures follows with the decisions taken there.

Every name, system and number in this document is invented. Your report contains your environment on the day of the check.