Information zur Sicherung und Wiederherstellung von Windows 10/11-Systemen

Information zur Sicherung und Wiederherstellung von Windows 10/11-Systemen

Bitte nehmt zur Kenntnis, dass die Sicherung und der Ersatz (z. B. Austausch der Hardware) eines Windows 10- oder Windows 11-PCs inzwischen sehr problematisch sein kann.

Hintergrund

Neue Windows 11-Systeme verschlüsseln die Festplatte standardmäßig.
Der Verschlüsselungsschlüssel ist dabei an die Hardware (Trusted Platform Module, TPM) gebunden.

Das bedeutet:

- Beim Umbau der Festplatte oder bei einer Wiederherstellung auf einem neuen PC (z. B. über URBackup) **kann das System nicht entschlüsselt werden**.
- Diese Basisverschlüsselung ist **ohne die ursprüngliche Hardware nicht aufhebbar** (Stand heute).

Mögliche Vorgehensweisen

1. Kein Bedarf an Verschlüsselung (z. B. PC steht in verschlossenen Räumen)

- **Prüfen**, ob eine Verschlüsselung aktiv ist:

  `manage-bde -status`

- **Deaktivieren** der Verschlüsselung:

  `manage-bde -off C:`
- **Alternative:** Falls Verschlüsselung gewünscht ist → BitLocker über *Einstellungen → System → Speicher → BitLocker* aktivieren und den Wiederherstellungsschlüssel **sicher aufbewahren**.

2. Bedarf an Verschlüsselung (z. B. bei mobilen Geräten)

- **Prüfung** wie oben:

  `manage-bde -status`
- Diese Verschlüsselung ist **an die jeweilige Hardware gebunden**.
- **Empfehlung:** BitLocker aktivieren und den Wiederherstellungsschlüssel **unbedingt sichern**.
  → Nur mit diesem Schlüssel ist eine vollständige Wiederherstellung möglich.

3. Zentrale Sicherung der BitLocker-Schlüssel über Gruppenrichtlinie (GPO)

In einer Active-Directory-Umgebung können BitLocker-Wiederherstellungsschlüssel **automatisch im AD gespeichert** werden.
Dies ermöglicht eine zentrale Verwaltung und Wiederherstellung der Schlüssel, auch wenn ein Benutzer den lokalen Key verliert.

Einrichtung (Kurzfassung):

1. GPO öffnen → `Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → BitLocker-Laufwerkverschlüsselung`
2. Unter *Betriebssystemlaufwerke* Richtlinie aktivieren:
   „Wiederherstellungsinformationen in Active Directory Domain Services speichern“
3. Optional: Speicherung erzwingen, bevor Verschlüsselung beginnt.
4. Anwendung prüfen mit `gpupdate /force`.

Hinweis: In Azure AD-Umgebungen werden die Schlüssel standardmäßig im Benutzerkonto im Azure-Portal hinterlegt.

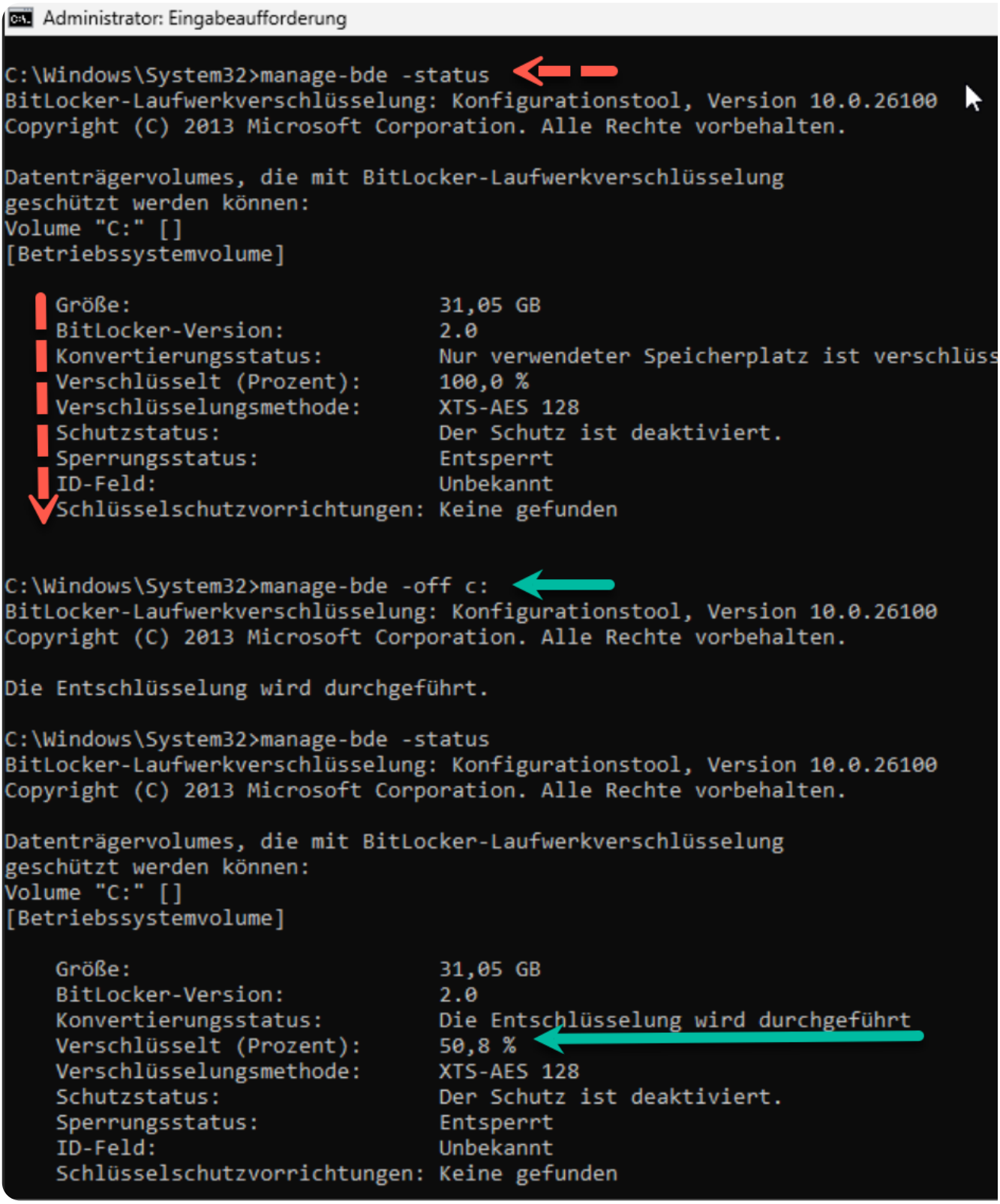
Hinweise zur Datensicherung

- **Plattensicherung (Image-Backup):** Wiederherstellung nur mit vorhandenem Schlüssel möglich.
- **Dateisicherung:** z. B. mit URBackup oder ähnlichen Tools.
- **Proxmox Backup Server:** Rücksicherung ist nur komplett möglich, da einzelne Dateien aus verschlüsselten Systemen nicht direkt extrahiert werden können.

Hier der technische Nachweis

Zugriff auf die frisch mit Windows 11 24H2 installierte Festplatte.

root@PVE250:~# mount /dev/zvol/rpool/data/vm-101-disk-1-part3 /mnt/restore/
mount: /mnt/restore: unknown filesystem type ‚BitLocker‘.



Version #1
Erstellt: 2025-10-31 11:32:14 UTC von Christian Zengel (sysops GmbH)
Zuletzt aktualisiert: 2025-10-31 11:38:27 UTC von Christian Zengel (sysops GmbH)