

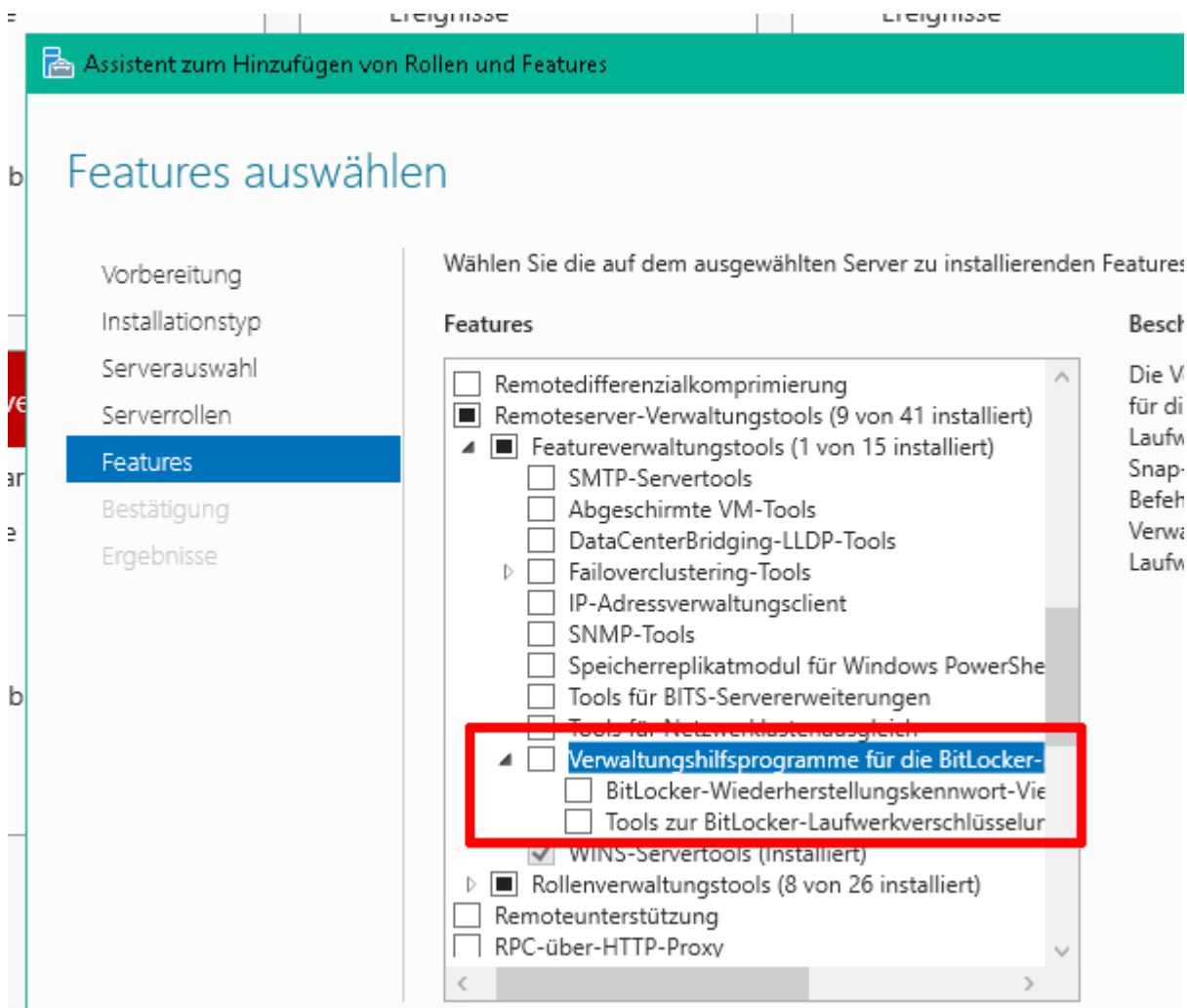
# Bitlocker in einer AD-Umgebung

Diese Anleitung umfasst:

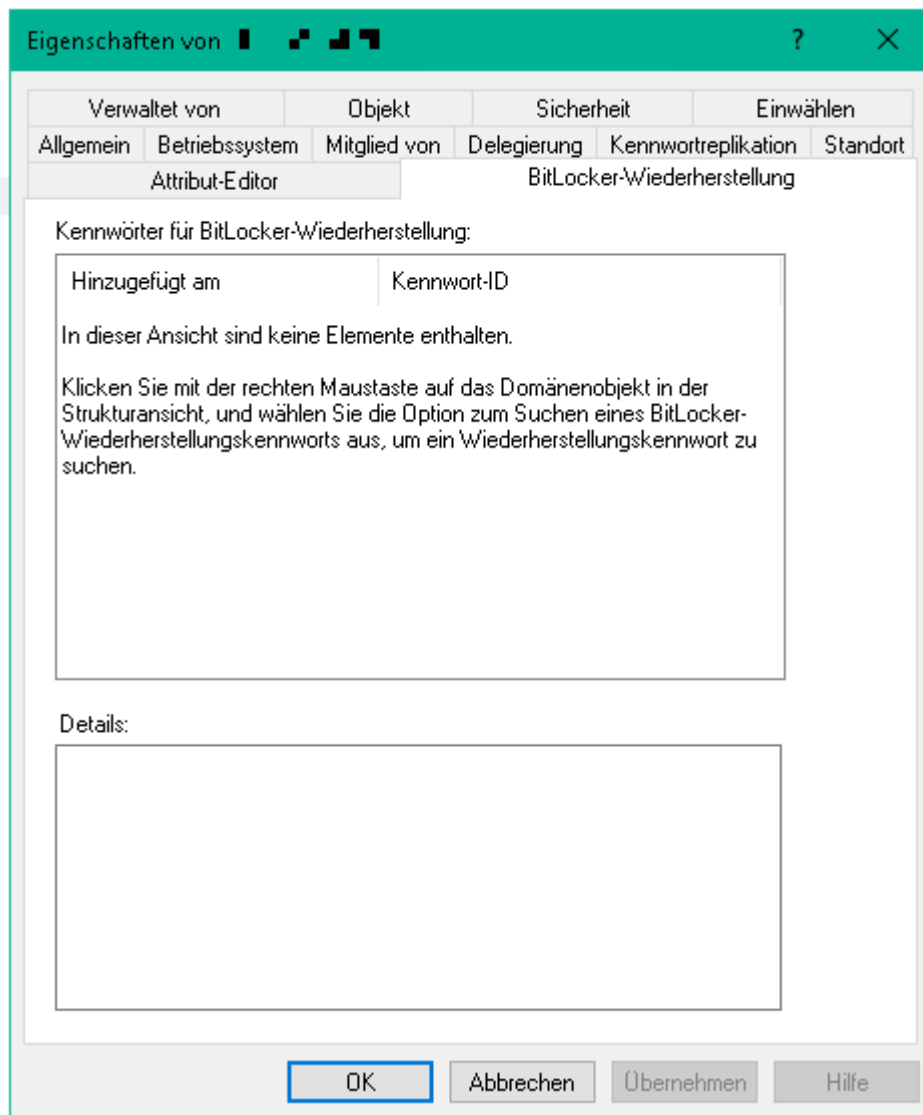
- Schlüssel in der AD gespeichert
- TPM wird vorausgesetzt
- Bitlocker wird am Rechner manuell aktiviert

## Feature auf dem DC

Damit der im AD abgelegte Schlüssel in der Konsole „Active Directory Users & Computers“ nachgeschlagen werden kann, muss über den Servermanager folgendes Feature installiert werden. Dies muss auf jedem Domain Controller geschehen, über den die Schlüssel verwaltet werden sollen.



In der Konsole sollte das hinterher so aussehen:



Das Feature installiert nicht nur die Tools, sondern auch die Schemaerweiterung im AD, in der die Informationen abgelegt werden. Mittels folgenden Powershell-Befehl.

```
Get-ADObject -SearchBase ((GET-ADRootDSE).SchemaNamingContext) -Filter {Name
-like 'ms-FVE-*'}
```

DistinguishedName ObjectGUID	Name	ObjectClass
CN=ms-FVE-KeyPackage,CN=Sc... 80dd0b7b-4c78-4305-9844-ce...	ms-FVE-KeyPackage	attributeSchema
CN=ms-FVE-RecoveryGuid,CN=... d9b3a270-cela-4514-9f73-c2...	ms-FVE-RecoveryGuid	attributeSchema
CN=ms-FVE-RecoveryInformat... 82dac378-fa82-46ae-a49f-16...	ms-FVE-RecoveryInformation	classSchema
CN=ms-FVE-RecoveryPassword... 1b97cf96-65b7-4939-834c-ff...	ms-FVE-RecoveryPassword	attributeSchema
CN=ms-FVE-VolumeGuid,CN=Sc... 47080651-54da-4a8b-bfc9-a0...	ms-FVE-VolumeGuid	attributeSchema

# Gruppenrichtlinie für die Clients

Computerkonfiguration → Richtlinien → Administrative Vorlagen → Windows-Komponenten → BitLocker-Laufwerksverschlüsselung

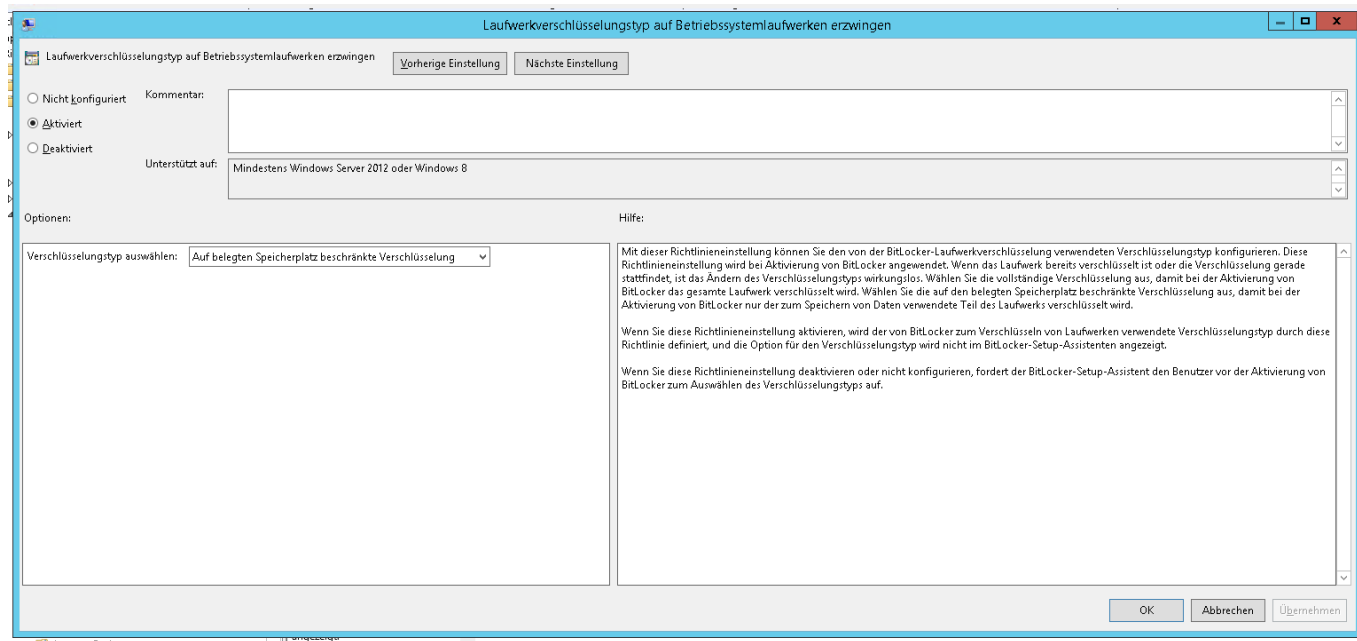
Die Konfiguration muss jeweils für das Betriebssystem-Laufwerk, (weitere) Festplattenlaufwerke sowie Wechseldatenträger erfolgen:

The screenshot displays the Group Policy Editor window titled "BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten speichern (Windows Server 2008 und Windows Vista)". The left pane shows the hierarchy: Computerkonfiguration → Richtlinien → Administrative Vorlagen → Windows-Komponenten → BitLocker-Laufwerksverschlüsselung. The right pane shows the policy settings:

- Policy Name:** BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten speichern (Windows Server 2008 und Windows Vista)
- Options:**
  - ☐ Nicht konfiguriert
  - ☒ Aktiviert
  - ☐ Deaktiviert
- Unterstützt auf:** Windows Server 2008 und Windows Vista
- Optionen:**
  - ☒ BitLocker-Sicherung in AD DS erforderlich
- Hilfe:** Diese Richtlinieneinstellung ermöglicht das Verwalten der Active Directory-Domänendienste-Sicherung (AD DS, Active Directory Domain Services) von Wiederherstellungsinformationen zur BitLocker-Laufwerksverschlüsselung. Hierbei handelt es sich um ein administratives Verfahren für die Wiederherstellung der von BitLocker verschlüsselten Daten, mit dem Datenverluste aufgrund fehlender Schlüsselinformationen vermieden werden. Diese Richtlinieneinstellung gilt nur für Computer, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird.

The second screenshot shows the Group Policy Editor window titled "Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können". The left pane shows the hierarchy: Computerkonfiguration → Richtlinien → Administrative Vorlagen → Windows-Komponenten → BitLocker-Laufwerksverschlüsselung. The right pane shows the policy settings:

- Policy Name:** Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können
- Options:**
  - ☐ Nicht konfiguriert
  - ☒ Aktiviert
  - ☐ Deaktiviert
- Unterstützt auf:** Mindestens Windows Server 2008 R2 oder Windows 7
- Optionen:**
  - ☒ Datenwiederherstellungs-Agenten zulassen
- Hilfe:** Mit dieser Richtlinieneinstellung können Sie steuern, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden, falls keine Informationen zum erforderlichen Systemstartschlüssel verfügbar sind. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.



From:

<https://wikinet.webby.hetzel-netz.de/> - **Sebastians IT-Wiki**

Permanent link:

[https://wikinet.webby.hetzel-netz.de/win\\_server:ad\\_bitlocker?rev=1633347184](https://wikinet.webby.hetzel-netz.de/win_server:ad_bitlocker?rev=1633347184)Last update: **2021/10/04 13:33**