

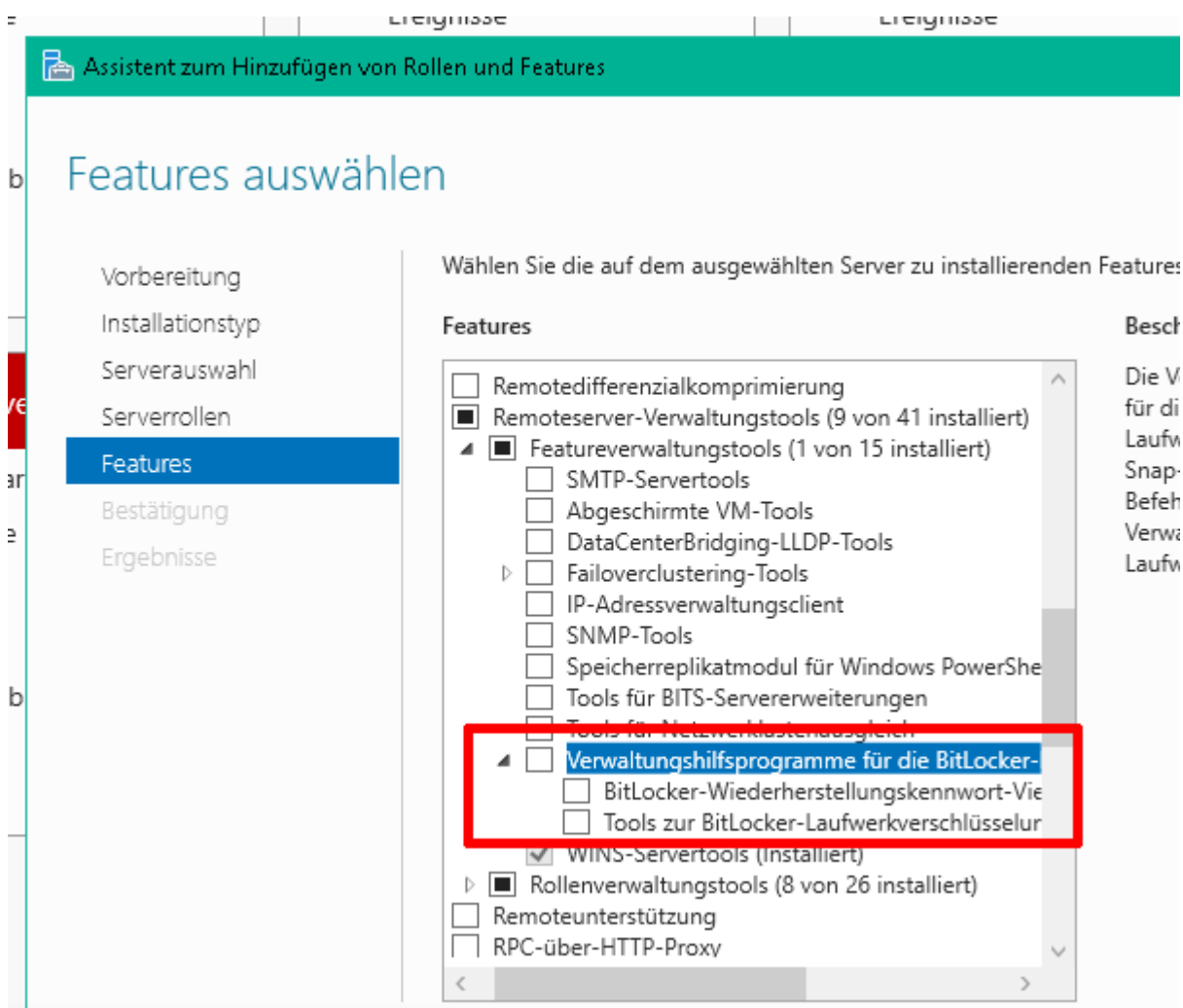
# Bitlocker in einer AD-Umgebung

Diese Anleitung umfasst:

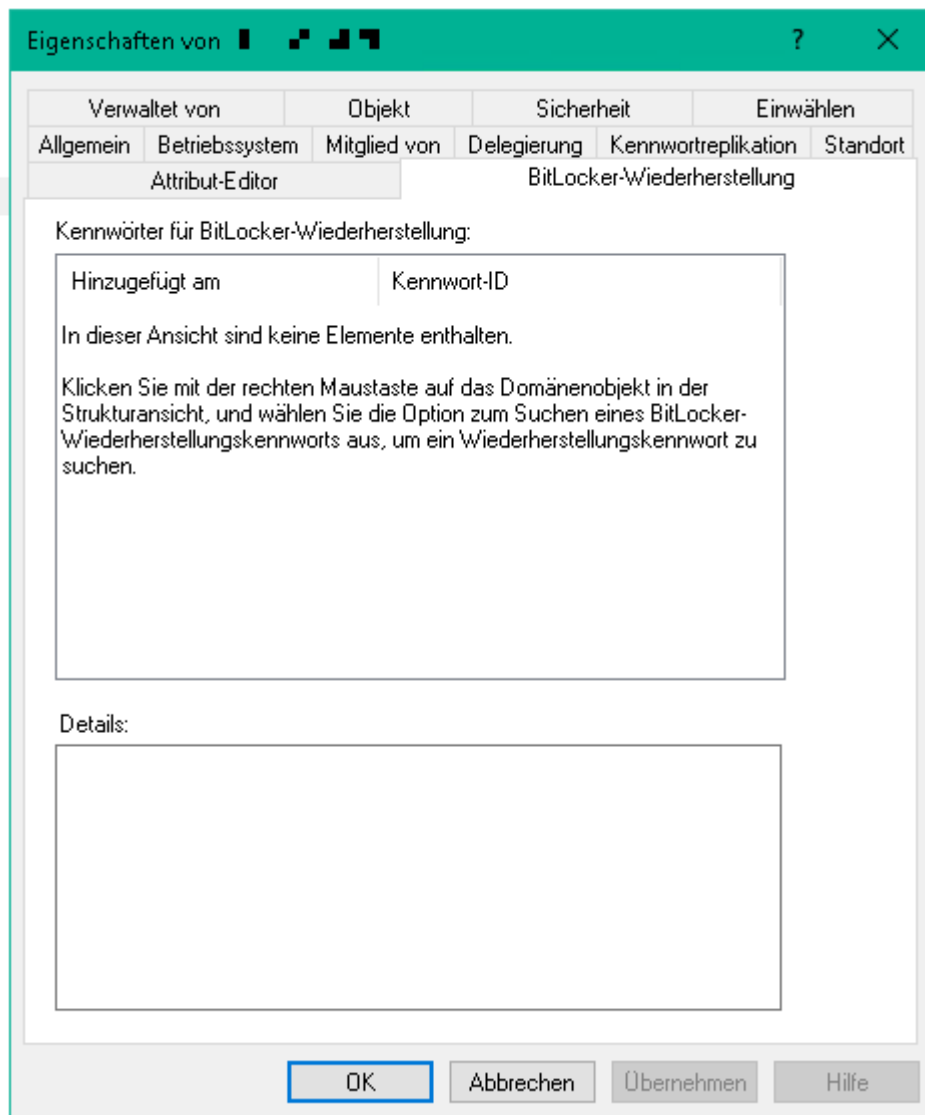
- Schlüssel in der AD gespeichert
- TPM wird vorausgesetzt
- Bitlocker wird am Rechner manuell aktiviert

## 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

BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten speichern (Windows Server 2008 und Windows Vista)

BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten speichern (Windows Server 2008 und Windows Vista) [Vorherige Einstellung] [Nächste Einstellung]

☐ Nicht konfiguriert    Kommentar:

☒ Aktiviert

☐ Deaktiviert

Unterstützt auf: Windows Server 2008 und Windows Vista

Optionen:

☒ BitLocker-Sicherung in AD DS erforderlich

Wenn diese Option aktiviert ist, kann BitLocker bei einem Sicherungsfehler nicht aktiviert werden (empfohlene Standardeinstellung).

Wenn diese Option deaktiviert ist, kann BitLocker selbst bei einem Sicherungsfehler aktiviert werden. Die Sicherung wird nicht automatisch wiederholt.

Wählen Sie die zu speichernden BitLocker-Wiederherstellungsinformationen aus:

Wiederherstellungskennwörter und Schlüsselpakete

Ein Wiederherstellungskennwort ist eine 48-stellige Nummer, die den Zugriff auf ein BitLocker-geschütztes Laufwerk entsperrt.

Ein Schlüsselpaket enthält den durch mindestens ein Wiederherstellungskennwort gesicherten BitLocker-Verschlüsselungsschlüssel eines Laufwerks.

Schlüsselpakete können Sie beim Ausführen einer spezialisierten Wiederherstellung unterstützen, wenn der Datenträger beschädigt ist.

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.

Wenn Sie diese Richtlinieneinstellung aktivieren, werden bei aktivierter BitLocker-Laufwerksverschlüsselung für einen Computer automatisch BitLocker-Wiederherstellungsinformationen im Hintergrund in AD DS gesichert. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.

Hinweis: Möglicherweise müssen Sie zuerst geeignete Schemaerweiterungen und Zugriffssteuerungseinstellungen in der Domäne einrichten, damit die AD DS-Sicherung erfolgreich ausgeführt werden kann. Weitere Informationen zum Einrichten der AD DS-Sicherung für BitLocker finden Sie in Microsoft TechNet.

Die BitLocker-Wiederherstellungsinformationen enthalten das Wiederherstellungskennwort und einige eindeutige ID-Daten. Sie können auch ein Paket einfügen, das einen Verschlüsselungsschlüssel für ein mit BitLocker geschütztes Laufwerk enthält. Dieses Schlüsselpaket wird durch mindestens ein Wiederherstellungskennwort gesichert und kann dazu dienen, bei einer Datenträgerbeschädigung eine spezialisierte Wiederherstellung durchzuführen.

Wenn Sie die Option "BitLocker-Sicherung in AD DS erforderlich" auswählen, kann BitLocker nur dann aktiviert werden, wenn der Computer mit der Domäne verbunden ist und die BitLocker-Wiederherstellungsinformationen erfolgreich in AD DS gesichert wurden. Diese Option ist standardmäßig aktiviert, um sicherzustellen, dass eine BitLocker-Wiederherstellung möglich ist. Wenn diese Option nicht aktiviert ist, wird zwar versucht, eine AD DS-Sicherung auszuführen, das BitLocker-Setup wird jedoch durch Netzwerk- oder andere Sicherungsfehler nicht verhindert. Die Sicherung wird nicht automatisch wiederholt, und das Wiederstellungskennwort wurde beim BitLocker-Setup möglicherweise nicht gespeichert.

Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden keine BitLocker-Wiederherstellungsinformationen in AD DS gesichert.

OK    Abbrechen    Übernehmen

From:

<https://wiki.sebastianhetzel.net/> - Sebastians IT-Wiki

Permanent link:

[https://wiki.sebastianhetzel.net/win\\_server:ad\\_bitlocker?rev=1633345550](https://wiki.sebastianhetzel.net/win_server:ad_bitlocker?rev=1633345550)

Last update: **2021/10/04 13:05**

