2 Verwalten der Active Directory Domänendienste

Prüfungsanforderungen von Microsoft:

- Manage and Maintain Active Directory Domain Services (AD DS)
    - Configure Service Authentication and account policies
    - Maintain Active Directory
    - Configure Active Directory in a complex enterprise environment

Quelle: Microsoft

Lernziele:

- Verwaltete Dienstkonten
- Das Klonen von Domänencontrollern
- Active Directory verwalten
- Kennwortrichtlinien
- Vertrauensstellungen
- Replikation und Standortverwaltung

2.1 Einführung

Das Active Directory ist zwar eine sehr robuste Datenbank, aber auch sie muss gewartet werden, um ordnungsgemäß zu funktionieren.

Einige Funktionen sind sehr praktisch für größere Unternehmen, diese

Technologien betrachten wir ebenfalls in diesem Kapitel.

2.2 Verwaltete Dienstkonten

Viele Anwendungen benötigen Dienstkonten, in deren Umfeld sie laufen.

Häufig wird hierfür ein vorhandenes Konto benutzt, wie beispielsweise der Netzwerkdienst.

Das funktioniert in den meisten Fällen auch einwandfrei.

Allerdings ist es nicht gerade besonders sicher, viele Anwendungen im gleichen Kontext laufen zu lassen. Auch ist es nicht möglich, den Dienst dann nach Wunsch zu konfigurieren.

Viele Administratoren sind aus diesem Grund bisher auf die Möglichkeit ausgewichen, ein normales Domänenkonto zu erstellen, und bei diesem den Haken „Kennwort läuft nie ab“ zu setzen. Dies gibt die Möglichkeit, die Kennwörter einmal zu vergeben, und nicht regelmäßig ändern zu müssen.

Auch das funktioniert gut. Allerdings entspricht es oft nicht den Sicherheitsanforderungen im Unternehmen, bei dem die Kennwörter aller Konten regelmäßig geändert werden müssen.

Um dieses Problem zu lösen, hat Microsoft bereits in der Version Server 2008 R2 die „verwalteten Dienstkonten“ eingeführt.

Diese Konten werden im Active Directory gespeichert, in der Klasse msDS-ManagedServiceAccounts.

Sie werden also getrennt von den Benutzerkonten verwaltet, und haben andere Eigenschaften. Sie haben beispielsweise die Möglichkeit, die gleiche Kennwortabgleichung zu machen, wie ein Computerkonto, das ja regelmäßig sein Kennwort mit dem Domänencontroller austauscht.

Dadurch ergeben sich folgende Vorteile:

- Automatisches Kennwortmanagement. Ein verwaltetes Dienstkonto benötigt keinerlei Kennworteinstellungen, es kann diese selber verwalten.
- Einfache Verwaltung des „Service Principal Names“ (SPN). Der „Service Principal Name“ ist der Name des Dienstes. Wenn er sich ändert, muss auch der Dienst angepasst werden. Dies wird mit verwalteten Dienstkonten automatisch gemacht.

2.2.1 Anforderungen für verwaltete Dienstkonten

Um verwaltete Dienstkonten verwenden zu können, benötigen Sie mindestens die Domänenfunktionsebene Windows Server 2008 R2.

Es ist zwar auch möglich, im Domänenfunktionsmodus Server 2008 zu arbeiten, dann natürlich mit einer Schemaerweiterung auf Server 2008 R2, aber das automatische Verwalten der SPN entfällt in diesem Fall.

Auch muss der Server, auf dem die Anwendung läuft, mindestens Windows Server 2008 R2 sein.

Auf ihm müssen das .NET Framework 3.5.x und das PowerShell - Modul für Active Directory installiert sein.

2.2.2 Anlegen von verwalteten Dienstkonten

Das Anlegen von verwalteten Dienstkonten erfolgt in mehreren Schritten.

- Anlegen des Root – Schlüssels
- Erstellen des Dienstkontos als Active Directory Objekt
- Verbinden des verwalteten Kontos mit einem Computerkonto
- Installieren des verwalteten Kontos auf dem Anwendungsserver
- Konfigurieren des Dienstes für die Verwendung dieses Kontos

Anlegen des Root – Schlüssels

Im ersten Schritt muss ein Root – Schlüssel angelegt werden.

Der Befehl dazu lautet

Add-KDSRootKey –EffectiveImmediately

Der Schalter –EffectiveImmediately bedeutet, dass dieses Objekt in 10 Stunden aktiv wird.

Diese Zeitverzögerung ist wichtig, damit die Replikation an alle Domänencontroller durchgereicht werden kann.

Für uns hier wäre es aber besser, wenn die Änderungen sofort aktiv sind, deswegen benutzen wir einen modifizierten Befehl:

Add-KDSRootKey –EffectiveTime ((Get-Date).AddHours(-10))

Abbildung 2.1: Root – Schlüssel erstellen

Erstellen des Dienstkontos als Active Directory Objekt

Nun können wir ein Dienstkonto erstellen.

Der Befehl lautet:

New-ADServiceAccount -name <NameDesKontos> -DNSHostName <DNSName> -PrincipalsAllowedToRetrieveManagedPassword Domänencomputer

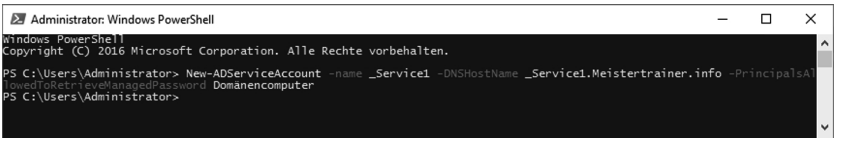

Abbildung 2.2: Erstellen des verwalteten Kontos

Verbinden des verwalteten Kontos mit einem Computerkonto

Der nächste Schritt ist das Verbinden des verwalteten Kontos mit einem Computerkonto

Add-ADComputerServiceAccount –Identity <ComputerName> -ServiceAccout <NameDesVerwaltetenKontos>

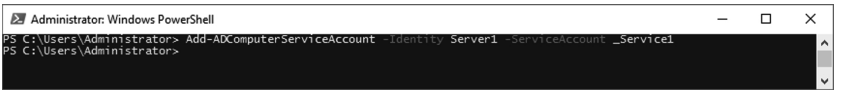

Abbildung 2.3: Verbinden mit einem Computerkonto

Nun können Sie überprüfen, ob das Konto erstellt worden ist.
Dies können Sie mit folgendem Befehl tun:

*Get-ADServiceAccount –Filter **

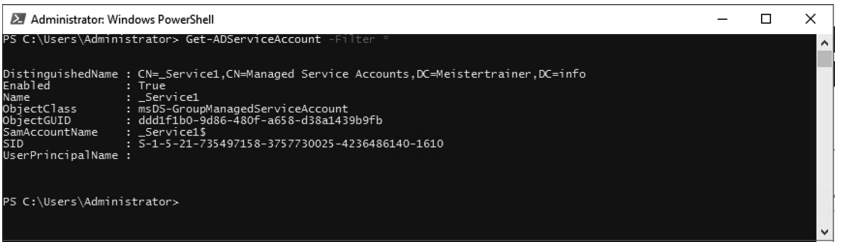

Abbildung 2.4: Konten betrachten

Hier sehen Sie auch deutlich, dass der SamAccountName ein „$“ Zeichen dahinter hat.

ACHTUNG!
In vielen Fällen müssen Sie das verwaltete Dienstkonto mit dem SamAccountName angeben! Beachten Sie das „$“ Zeichen!

Auch in der grafischen Oberfläche ist das verwaltete Konto jetzt sichtbar.

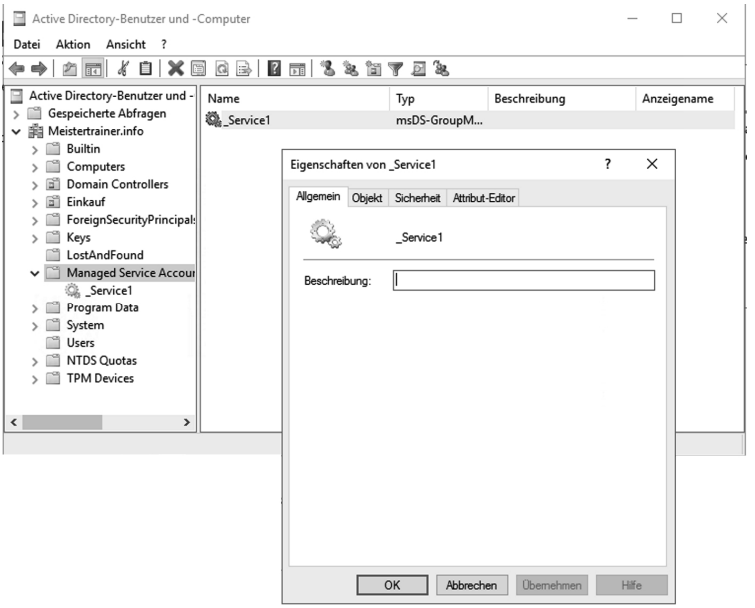

Abbildung 2.5: Managed Service Accounts

Im Snap-In „Active Directory-Benutzer und -Computer" finden Sie im Container „Managed Service Accounts" den Eintrag. Hier lässt sich leider nicht viel konfigurieren.

Installieren des verwalteten Kontos auf dem Anwendungsserver

Nun können Sie das Konto auf dem Zielserver installieren.

Dazu müssen Sie zunächst das Feature „Active Directory-Modul für Windows PowerShell" installieren.

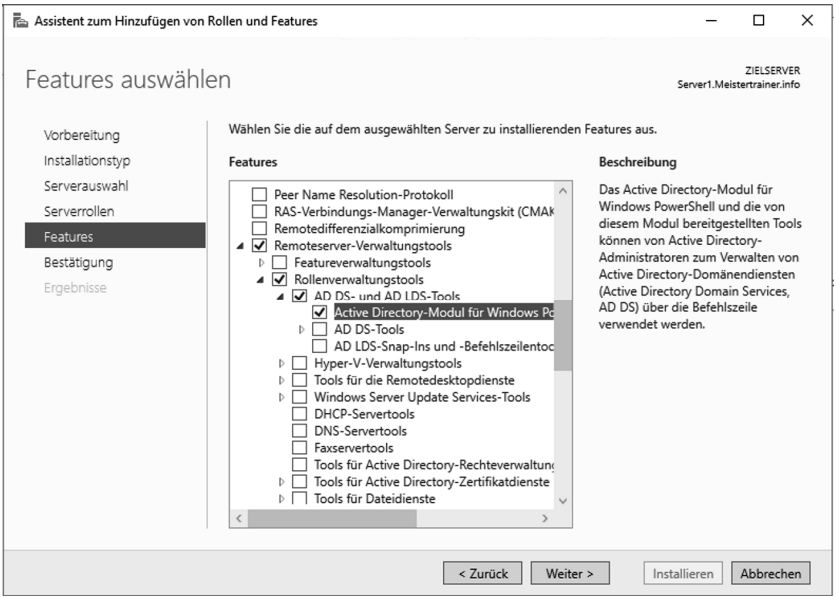

Abbildung 2.6: Active Directory-Modul für Windows PowerShell

Nun installieren Sie das Konto mit dem Befehl

Install-ADServiceAccount –Identity <NameDesKontos>

Abbildung 2.7: Installieren des Kontos

Konfigurieren des Dienstes für die Verwendung dieses Kontos

Nun müssen Sie nur noch dem gewünschten Dienst das eben erstellte Konto zuweisen.

Abbildung 2.8: Konto zuweisen

Sie sehen, dass hier wieder der SAMAccountName benutzt wird!

Lassen Sie das Kennwort leer, denn es wird ja vom System verwaltet.

Nach Klicken auf „OK“ erhalten Sie noch folgende Meldung:

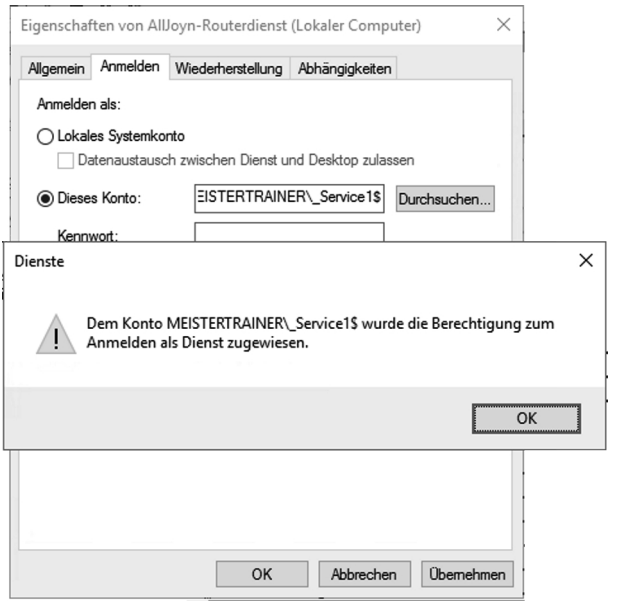

Abbildung 2.9: Konto wird zugewiesen

Nun ist der Dienst mit diesem Konto konfiguriert.

2.2.3 Benutzerkonten als Dienstkonten

Wie am Anfang bereits angesprochen, ist es auch immer noch möglich, normale Benutzerkonten als Dienstkonten zu benutzen, hierbei muss aber die Problematik der Kennwortänderung beachtet werden!

Aber auch der Service Principal Name ist ein Problem.

Mit dem SPN erkennt der Client unverwechselbar einen Dienst oder eine Instanz des Dienstes.

Wenn der SPN nicht definiert ist, gibt es bei vielen Diensten Probleme, so zum Beispiel beim SQL-Server.

Verwaltete und gruppenverwaltete Dienstkonten haben dieses Flag bereits gesetzt, aber wenn Sie ein normales Benutzerkonto als Dienstkonto verwenden möchten, müssen Sie dies erst noch durchführen.

Der Befehl dazu lautet

Setspn -s http/<computername> <domain-user-account>

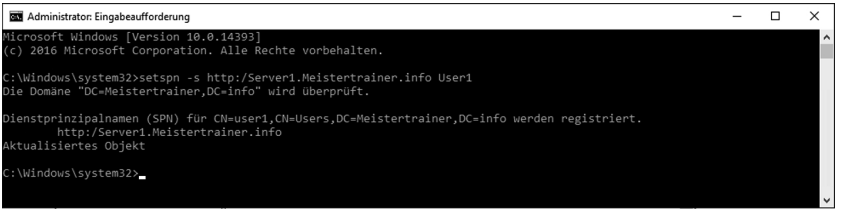

Abbildung 2.10: SPN anlegen

Nun ist eine neue Registerkarte im Konto aufgetaucht: Die Karte „Delegierung“.

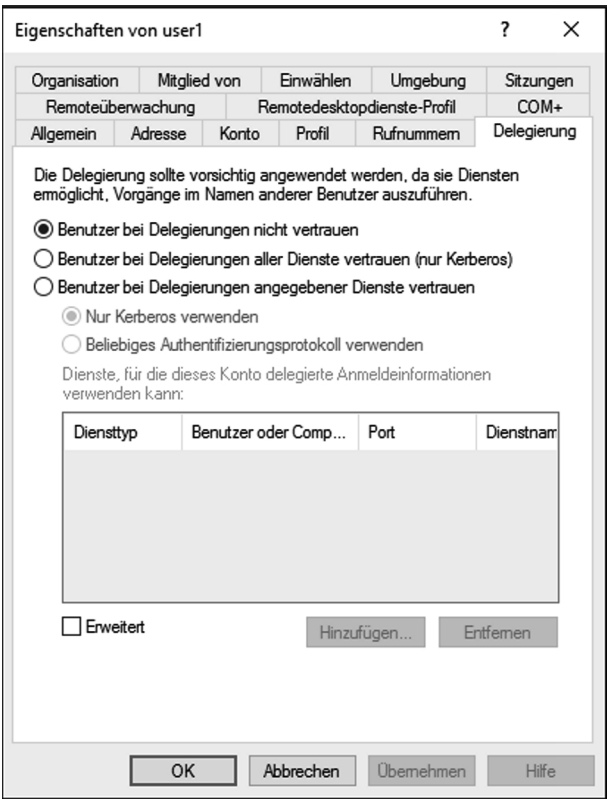

Abbildung 2.11: Delegierung

Hier müssen Sie noch eine Delegierung einrichten, die den gewünschten Diensten entspricht.