Inhalt

Active-Directory

Verwaltete Dienstkonten

- Konten für Dienste
- Interaktive Anmelden mit diesen Konten nicht möglich
- Bsp.: SYSTEM
- Anwendungen
    - Datenbankserver
    - ERP-Server (SAP-Server)

Gruppenverwaltete Dienstkonten

- Dienstkonten, die sich an verschiedenen Servern mit den gleichen Daten anmelden
- Typen:
    - Sicherheit: Gruppen, die Zugriffsrechte regeln (z.B. im Dateisystem)
    - Verteilung: Mailverteiler

PowerShell

User anlegen

```
$password = ConvertTo-SecureString "LarsStinkt" -AsPlainText -Force


New-ADUser -Name "Max Mustermann" `
 -GivenName "Max" `
 -Surname "Mustermann" `
 -SamAccountName "mmustermann" `
 -UserPrincipalName "mmustermann@domain.local" `
 -Path "OU=IT,DC=domain,DC=local" `
 -AccountPassword $password `
 -ChangePasswordAtLogon $true `
 -Enabled $true
```

OU anlegen

Root-OU

```
New-ADOrganizationalUnit -Name "IT" -Path "DC=domain,DC=local"
```

Sub-OU

```
New-ADOrganizationalUnit -Name "Support" -Path "OU=IT,DC=domain,DC=local"
```

Gruppenrichtlinien

- Konfigurationsanweisungen -> Einstellungen werden erzwungen
- Vorteile:
    - Handlungsmöglichkeiten von Nutzern festlegen
    - Verwaltungsaufwand senken
    - Aufrechterhaltung von Computerkonfigurationen
- Einsatz:
    - Registry-Einträge überschreiben
    - Kennwortrichtlinie
    - RDP-Anmeldung
    - Softwareinstallation
    - Ordnerumleitung
    - Netzlaufwerk einbinden
    - Skript-Ausführung
- Lokale Richtlinien: Konfiguration des lokalen Systems
    - Keine Auswirkung auf die Domäne
- Standort-, Domänen-, OU-Richtlinien: Wirken auf alle Nutzer innerhalb des gewählten Scopes
- In Gruppenrichtlinienverwaltung können neue Vorlagen für Gruppenrichtlinien erstellt werden
    - Werden erst aktiv, wenn sie an einen Scope verknüpft werden

Anwendungsreihenfolge

1. Lokale Richtlinien
2. Multi-Lokale Richtlinien
3. Standortrichtlinie (Site)
4. Domänenrichtlinie (Domain)
5. OU-Richtlinie – übergeordnet zu untergeordnet

- Last-Write-Wins: Spätere Richtlinien überschreiben vorherige Richtlinien

Freigaben

- SMB
    - Windows-Freigabe
    - Netzwerkprotokoll für Dateizugriff
    - Aktuelle Version: SMBv3
- NFS: Linux-Freigabe
- Freigabe über Explorer/Server-Manager

Berechtigungen

- Vererbung: Rechte werden von übergeordneter Instanz übernommen
- Einträge werden von oben nach unten abgearbeitet
    - Oben: Verweigern
    - Unten: Zulassen

Access Control Lists (ACLs)

- Geordnete Liste von Zugriffseinträgen (ACEs)
- Access Control Entry (ACE)
    - SID des Nutzers oder der Gruppe
    - Spezifizierte Rechte
    - Bit zur Entscheidung der Vererbung
- Abarbeitung ist beendet, wenn
    - Explizit zugelassen
    - Explizit verweigert
    - Alle ACEs durchgelaufen
- Reihenfolge der Abarbeitung
    1. ACEs die explizit verweigern
    2. ACEs die explizit erlauben
    3. ACEs die vererbt verweigern
    4. ACEs die vererbt erlauben

Gruppenrechtevergabe

Gruppenart	**Lokale Gruppe**	**Globale Grupp**	**Universelle Gruppe**
Sichtbarkeit	Sichtbar nur in lokaler Domäne	Auch außerhalb der eigenen Domäne sichtbar	Überall
Mitgliederherkunft	Aus allen Domänen	Aus eigener Domäne	Aus allen Domänen
Mitgliedertypen	Mitglieder und Gruppen	Keine anderen Gruppen	Benutzer und Gruppen
Berechtigung	Innerhalb eigener Domäne	In beliebiger Domäne	In beliebiger Domäne
Bemerkung	Zusammenfassen globaler Gruppen möglich		Alle Informationen stehen im globalen Katalog, werden repliziert und produzieren damit Netzlast

AGDLP-Regel

Problem

Admin sieht nicht direkt welche Rechte für einen User aktiv sind

Lösung

AGDLP: Accounts Global, Domain Local, Permission

- Freigaben werden nur an lokale Gruppen vergeben, die nur dafür zuständig sind
- Lokale Gruppen werden entsprechend ihres Zwecks und der damit verbundenen Rechte benannt
- Beispiel:
    - Lokale Gruppe „Share-Verwaltung“ wird auf die Freigabe \\server\Verwaltung berechtigt
    - Die globale Gruppe „Verwaltung wird Mitglied der lokalen Gruppe und bekommt somit die Rechte auf die Freigabe
    - In der globalen Gruppe sind die tatsächlichen User der Verwaltung

SYSVOL

- Freigabe in der Dateien mit Domäneneinstellungen geteilt werden
    - Logon-Scripts
    - Gruppenrichtlinien
    - File-Replication-Service
    - Junction-Points: Ähnlich wie eine Verlinkung

Domain Name System (DNS)

- DNS-Server: Zuordnung von FQDNs zu IP-Adressen und umgekehrt
- Alternative unter Windows: NetBIOS
- Hierarchische Gliederung – Getrennt durch Punkte
- Abfrage läuft Hierarchisch ab -> Anfragen werden weitergeleitet
- AD-Domain = DNS-Domain (Domänencontroller oft auch DNS-Server)
    - Bei Vertrauensstellungen zwischen Domänen muss DNS-Auflösung domänenübergreifend funktionieren
        - In Zonendatei werden Delegierungen für Subdomänen und andere Domänen angelegt

Zonendatei

- Enthält gesamten Inhalt einer Domäne
    - Autoritätsursprung (SOA): Eintrag für primären DNS-Server und Einstellungen z.B. zum Zonentransfer
    - Verschiedenste Records: NS, A, AAAA, PTR, CNAME, SRV, MX
- Ein Primary-Server (Master) und beliebig viele Secondary-Server (Slave)
- Replikationsmethoden
    - Vollständige Zonenübertragung: Gesamte Zonendatei auf Slaves übertragen
    - Inkrementelle Zonenübertragung: Nur Änderungen werden auf Slaves übertragen
    - Benachrichtigung vom Master: Nach Veränderung benachrichtigt Master alle Slaves
    - Slave veranlasst Zonenübertragung: Slave fragt bei Master nach Änderungen

Abfragenablauf

1. Client prüft, ob Hostname bereits in der lokalen Hostdatei enthalten ist
2. Wenn nicht wird rekursives Forward-Lookup-Request an den primären DNS-Server gesendet
3. DNS-Server prüft, ob er eine Zone für die angefragte Domain hat, wenn ja: Autoritativ Antwort zurück
4. Wenn der DNS-Server keine passende Zone hat prüft er den Cache -> Cache-Hit: Nicht-Autoritative Antwort zurück
5. Wenn auch im Cache nichts vorhanden ist wird die Anfragen an den Root-Server weitergeleitet

Antwortarten

- Autoritativ: Server hat Antwort in lokaler Zonendatei
- Nicht Autoritativ: Antwort obwohl Server nicht zuständig ist
    - Rekursiv: Server holt die Daten von einem anderen DNS-Server
    - Iterativ: Server antwortet mit einem Verweis auf einen anderen DNS-Server

DHCP: Dynamic Host Configuration Protocol

- Automatisierte Zuweisung von Netzwerkeinstellungen wie IP-Adresse, Subnetzmaske, Gateway und DNS-Server
- Gegenstück ist die statische Adressierung
- DHCP-Netzwerkgeräte fordern beim Verbinden zum Netzwerk DHCP-Daten an
- Die DHCP-Daten haben eine definierte Gültigkeitsdauer (Lease-Dauer)
    - Nach Ablauf werden die Daten neu angefordert

Ablauf (DORA)

1. **Discover** (Broadcast): Client sendet DHCP-Discover beim booten bzw. beim Herstellen einer Verbindung in einem Netzwerk
2. **Offer**: Ein DHCP-Server, der den Discover-Broadcast erhalten hat antwortet mit einem DHCP-Offer, in dem die Netzwerkdaten über eine bestimmte Lease-Dauer enthalten sind
3. **Request** (Broadcast): Da ggf. mehrere DHCP-Server auf den Discover ein Offer senden muss der Client ein Offer wählen und es mit einem entsprechenden Request bestätigen. Das Paket ist ein Broadcast um ggf. anderen DHCP-Servern mitzuteilen für welches Offer sich der Client entschieden hat.
4. **Ack**
    a. Wenn die angebotene Adresse aus dem Offer am Server noch verfügbar ist antwortet dieser mit einer entsprechenden Bestätigung
    b. Ist die angebotene Adresse nicht mehr verfügbar antwortet der Server mit einer negativen Bestätigung (**NAK**). Das DHCP-Verfahren beginnt am Client mit einem **Discover** von vorne.

Lease Verlängerung

Funktioniert nur innerhalb eines Lease Zeitraums

Ablauf

1. DHCP-Request (Unicast): Eine direkte Anforderung an den DHCP-Server von dem das aktuelle Lease ist. Erhält der Client in einem bestimmten Zeitabstand keine Antwort sendet er das Request als Broadcast um andere verfügbare DHCP-Server zu erreichen.
2. DHCP-Ack (Unicast): Der Server bestätigt die Verlängerung

Authentifizierung

Echtheit bezeugen bei der Kommunikation zwischen Server und Client

Password Authentication Protocol (PAP)

- Client sendet Username und Passwort im Klartext
- Server akzeptiert bei korrekten Credentials
- Nachteil: Credentials können sehr leicht abgehört werden

New Technology LAN Manager (NTLM)

- Vorteil: Weder Passwort noch Passworthash werden im Klartext übertragen
- Problem:
    - Viele Anfragen -> Große Verwaltungslast durch Authentifizierungsprozess
    - Keine MFA-Unterstützung

Ablauf

1. Negotiate: Client sendet Anfrage mit Benutzernamen und Payload an Server
2. Challenge: Server generiert Zufallszahl und sendet diese an den Client
3. Authenticate: Client verschlüsselt die Zufallszahl mit DES und dem NT-Hash des eigenen Passworts als Schlüssel und sendet zurück an den Server. Damit beweist er, dass er das Passwort kennt.
4. Server führt parallel den gleichen Vorgang durch und gleicht die Ergebnisse ab. Server hat Zugriff auf den NT-Hash durch eigene SAM-Datenbank oder er leitet das Challenge/Response-Paar zur Validierung an den DC weiter

Angriffsvektoren

Pass the Hash

- Sobald ein Angreifer an den NT-Hash und den passenden Username gekommen ist kann er die Authentifizierung durchführen -> Es wird kein Passwort benötigt
- NT-Hash entweder aus lokaler SAM-Datei oder aus dem Arbeitsspeicher
- Username wird oft im Klartext übertragen

Brute-Force

- Hash-Algorithmus wird ohne Salt (Zufällige Zeichenkette am Ende des Passworts, vor der Verschlüsselung) verwendet
- Mithilfe eines Rainbow-Tables können leicht Brute-Force-Angriffe durchgeführt werden

NTLM-Relay

- Client kann die Identität des Servers nicht prüfen -> Angreifer kann sich als Server ausgeben (Man in the Middle)

Kerberos

- Standard-Authentifizierungsprotokoll im AD
- Beteiligte Parteien:
    - Client: Fordert Ressource an
    - Service-Server: Den der Client nutzen möchte
    - Kerberos-Server/Key Distribution Center (KDC): Stellt Authentifizierung zur Verfügung
- Wichtige Komponenten:
    - Ticket Granting Ticket (TGT): Ticket/Berechtigung mit dem man weitere Tickets/Berechtigungen erhalten kann (Vgl. Ticket für den Einlass zum Park)
        - Hat bestimmte Lebensdauer
        - Wird mit Passwort des krbtgt-Accounts verschlüsselt
    - TGS/Serviceticket: Ticket/Berechtigung für die Nutzung einer bestimmten Ressource/eines Services (Vgl. Ticket für das Fahrgeschäft)
        - Hat bestimmte Lebensdauer
        - Wird mit Passwort des angefragten Service-Nutzers verschlüsselt
- Durch Ticketsystem kann der Client selbst die Authentifizierung durchführen ohne den DC
- Es werden auch keine Passwort-Hashes verschickt
- Zeitsynchronisation zwischen Client und KDC ist Voraussetzung

Ablauf

1. Nutzer meldet sich am PC an
2. Anmeldedaten werden an den DC übergeben
    a. Client erhält TGT vom DC.
    b. Client kann sich mit TGT am KDC authentifizieren und TGS lösen

Beispiel Webaufruf

1. Client verwendet Webbrowser um Verbindung zum Server aufzubauen. Vorerst Anonym.
2. Server antwortet mit HTTP-Status 401 (Unauthorized) und fordert Client zur Anmeldung auf.
    a. Durch die Aufforderung erhält der Client den Namen der Ressource für die er ein Ticket braucht
3. Der Client verlangt am KDC nach einem TGS für die entsprechende Ressource
4. KDC sucht im AD nach der angeforderten Ressource (über ServicePrincipalName)
5. KDC stellt TGS auf den Namen und mit den Daten des Benutzers aus. TGS wird signiert und an den Client übergeben
    a. Client speichert TGS im Cache
    b. TGS ist mit dem Passwort des Service-Benutzers verschlüsselt. Dieses Passwort kennt der Webserver ebenfalls.
6. Client stellt die Anfrage an den Webserver erneut und übergibt das TGS dabei an den Webserver.
7. Der Webserver vertraut dem KDC und kann somit unabhängig das Ticket validieren

Betriebsmasterrollen / Flexible Single Master Operations (FSMOs)

- AD kann über mehrere DCs verteilt sein
- Jeder DC darf Objekte im AD anlegen
    - Es gilt „last write wins“ -> Nur der letzte Schreibvorgang ist gültig
- FSMOs sind Aufgaben die eine zentrale Instanz benötigen, da ein Konflikt fatal wäre
- FSMOs: Spezielle Aufgaben innerhalb einer Domäne, die auf verschiedene Server verteilt werden können
- FSMOs sind immer einmalig (Gesamtstruktur/Domäne)

Auflistung

Domain Naming Master (Gesamtstruktur)

- Zuständig für (Sub-)Domainnamen
- Muss neue Domainnamen freigeben

Schema Master (Gesamtstruktur)

- Zwingend gleicher Server wie Domain Naming Master
- Definiert Klassen-Schablone für AD-Objekte

Relative ID Master (Domäne)

- Sorgt dafür, dass RID eindeutig ist
- SID besteht vereinfacht aus:
    - Local-ID
    - Relative-ID
- SIDs identifizieren Objekte im AD

Primary Domain Controller (PDC) Emulator (Domäne)

- Problem: Replikation des Ads dauert sehr lange
    - Passwortänderungen sind erst nach langer Zeit aktiv
- PDC-Emulator zieht Passwortänderungen vor
- Bei fehlerhaftem Anmeldeversuch: PDC-Emulator wird befragt ob Passwort gültig ist

Domain Infrastructure Master (Domäne)

- Stellt referentielle Integrität zwischen verlinkten Objekten sicher
- Bsp.: Bei Gruppen und Mitgliedern: Attribute „Members“ und „MemberOf“ müssen übereinstimmen
- DIM sorgt dafür, dass Änderung eines Attributs in das andere nachgezogen wird

Just Enough Administration (JEA)

- Administrative Mitarbeiter sollen nur die minimalen Rechte für bestimmte Arbeiten erhalten
- Unter PowerShell: User kann nur bestimmte CMDlets ausführen
- Rechte werden in Role Capability Files (.psrc) gespeichert
- Funktioniert nur in Bereichen für die es entsprechend auch PowerShell-Befehle gibt

Just-In-Time Administration (JIT)

- Nur temporäres freigeben von administrativen Berechtigungen
- Administrative Fähigkeiten werden nur auf Anfrage erlangt
- Zur Verwaltung der Time-To-Live wird ein TGT von Kerberos verwendet. Privilegierter Zugriff ist nur möglich solange das TGT gültig ist.

Offene Punkte

Nur Klick-Für-Klick Anleitungen

- Freigaben und Gruppenrichtlinien: Netzlaufwerk freigeben, Software installieren, Skript beim Start ausführen
- User Homes

Unbekanntes Thema

- NTLM für Service Server