



Cyber Security



Gruppenrichtlinien

AGENDA

01

02



AGENDA

01



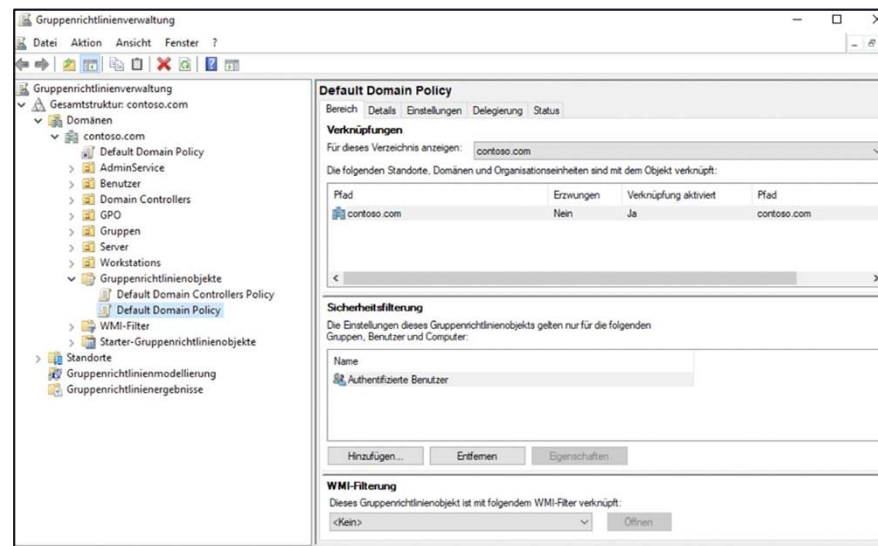
Einleitung

- **Gruppenrichtlinien** sind das Framework für die Konfigurationsverwaltung in einer AD DS-Domäne und umfasst neben den u.g. Elementen auch die Tools für Verwaltung, Konfiguration und Problembehandlung
- Eine **Konfigurationsverwaltung** bezeichnet einen zentralisierten Ansatz für die Anwendung einer oder mehrerer Änderungen auf einen oder mehrere Benutzer oder Computer
 - Einstellung: Definition einer Änderung oder Konfiguration
 - Gültigkeitsbereich: Definition der Benutzer oder Computer, für die die Änderung gilt
 - Anwendung: Ein Mechanismus, mit dem die Einstellung auf Benutzer und Computer innerhalb des Gültigkeitsbereichs angewendet wird



Gruppenrichtlinienobjekte

- Objekte in der Active Directory Datenbank, welche im Container „Gruppenrichtlinienobjekte“ gespeichert sind
- Werden mit der Gruppenrichtlinienverwaltung (gpedit) bearbeitet

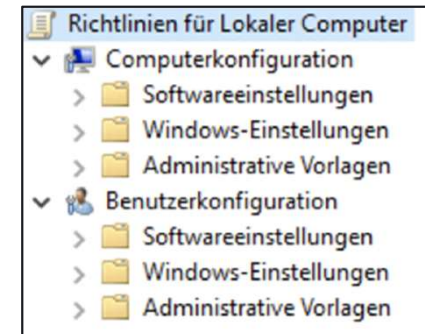
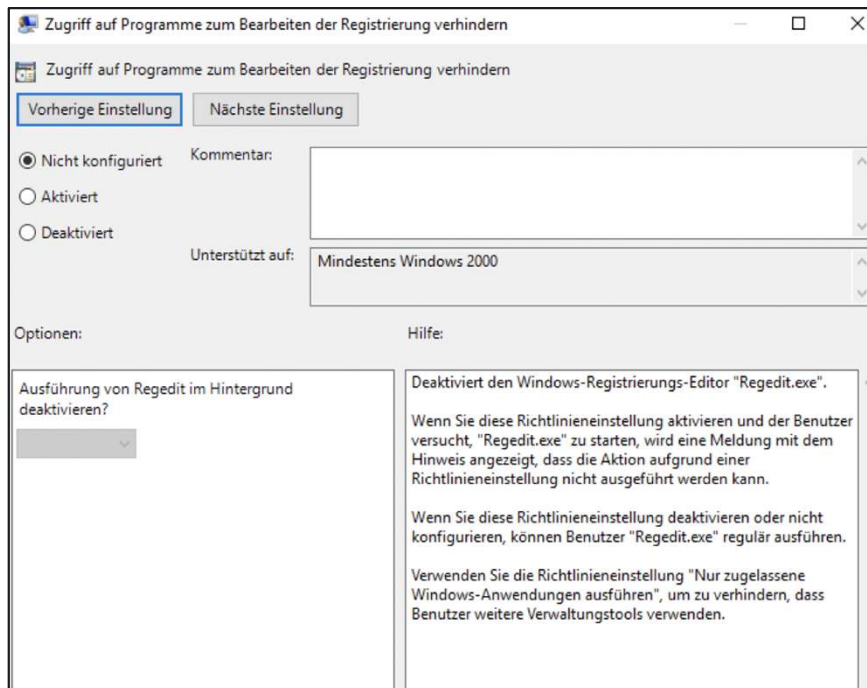


Gruppenrichtlinieneinstellungen

- Die präzise Definition einer Änderung oder Konfiguration: z.B.
 - Zugriff auf Programme zum Bearbeiten der Registrierung verhindern
 - Umbenennen des Administratorkontos
- Aufgeteilt zwischen
 - Benutzerkonfiguration ("Benutzerrichtlinien")
 - Computerkonfiguration ("Computerrichtlinien")
- Eine Einstellung definieren
 - Nicht konfiguriert (Standardeinstellung)
 - Aktiviert
 - Deaktiviert



Gruppenrichtlinieneinstellungen



Gültigkeitsbereich

- **Gültigkeitsbereich:** Definition von Objekten (Benutzer oder Computer), für die ein Gruppenrichtlinienobjekt gilt
- **Gruppenrichtlinienobjekt-Verknüpfung:** Ein Gruppenrichtlinienobjekt kann mit einem Standort, einer Domäne oder einer Organisationseinheit verknüpft sein (Site, Local, Global, Domain, Organizational Unit, SDOU).
 - Ein Gruppenrichtlinienobjekt kann mit mehreren Standorten oder Organisationseinheiten verknüpft sein.
 - Mit Gruppenrichtlinienobjekt-Verknüpfungen wird der maximale Gültigkeitsbereich des Gruppenrichtlinienobjekts definiert.



Gültigkeitsbereich

Sicherheitsgruppen Filterung

- Anwenden oder Verweigern der Anwendung des Gruppenrichtlinienobjekts auf Mitglieder einer globalen Sicherheitsgruppe
- Filtern der Anwendung des Gültigkeitsbereichs des Gruppenrichtlinienobjekts innerhalb des Verknüpfungsbereichs

WMI-Filterung

- Optimieren des Gültigkeitsbereichs des Gruppenrichtlinienobjekts innerhalb der Verknüpfung anhand einer WMI-Abfrage



Gruppenrichtlinienclient

Anwendung von Gruppenrichtlinienobjekten und deren Einstellungen

- Der Gruppenrichtlinienclient ruft eine geordnete Liste von Gruppenrichtlinienobjekten beim Domain-Controller ab.
- Die Gruppenrichtlinienobjekte werden heruntergeladen (und dann zwischengespeichert).
- Die Einstellungen werden von Komponenten, die als clientseitige Erweiterungen (Client-Side Extensions, CSEs) bezeichnet werden, verarbeitet, um die Änderungen anzuwenden.
 - Von den meisten clientseitigen Erweiterungen werden Einstellungen nur angewendet, wenn das Gruppenrichtlinienobjekt (insgesamt) geändert wurde, dies verbessert die Leistung der Verarbeitung
 - Die Anwendung von Gruppenrichtlinienobjekten wird vom Client ausgelöst ("Pull").



Aktualisierung von Gruppenrichtlinien auf einem Client

Zeitpunkt der Anwendung von Gruppenrichtlinienobjekten und deren
Einstellungen

Computerkonfiguration

- Start
- Ausgelöst durch: Befehl GPUpdate → Neustart

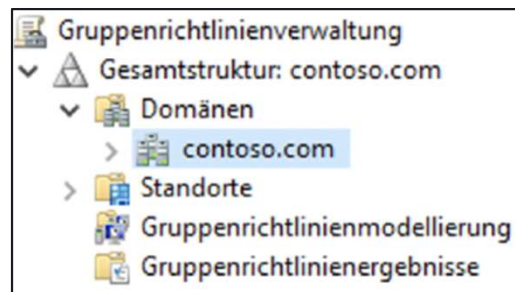
Benutzerkonfiguration

- Anmelden
- Ausgelöst durch: Befehl GPUpdate → Neuansmeldung



Richtlinien modellieren und testen

- Die "kumulative" Auswirkung von Gruppenrichtlinien
 - Ein Benutzer oder Computer befindet sich normalerweise im Gültigkeitsbereich vieler Gruppenrichtlinienobjekte.
 - Potenziell in Konflikt stehende Einstellungen: Rangfolge



Richtlinien modellieren und testen

- Tools zum Erstellen von Berichten, aus denen hervorgeht, welche Einstellungen angewendet wurden und welches Gruppenrichtlinienobjekt bei in Konflikt stehenden Einstellungen den Vorrang erhalten hat
- Tools zum Modellieren der Auswirkungen von Änderungen an der Gruppenrichtlinieninfrastruktur oder am Speicherort von Objekten in Active Directory



Lokale Gruppenrichtlinien

Lokale GPOs werden durch domänenbasierte Gruppenrichtlinienobjekte überschrieben

- Eine durch ein domänenbasiertes Gruppenrichtlinienobjekt angegebene Einstellung setzt die gleiche durch lokale Gruppenrichtlinienobjekte angegebene Einstellung außer Kraft.



Lokale Gruppenrichtlinien

Lokales Gruppenrichtlinienobjekt

- Lokales Gruppenrichtlinienobjekt: Computereinstellungen und Einstellungen für alle Benutzer
- Administratoren-Gruppenrichtlinienobjekt: Einstellungen für Benutzer in der Gruppe Administratoren
- Nicht-Administratoren-Gruppenrichtlinienobjekt: Einstellungen für Benutzer, die nicht zur Gruppe Administratoren gehören
- Pro-Benutzer-Gruppenrichtlinienobjekt: Einstellungen für einen bestimmten Benutzer



Lokale Gruppenrichtlinien

Domänenmitglieder können mithilfe von Gruppenrichtlinienobjekten, die mit der Domäne verknüpft sind, zentral verwaltet werden. In welchen Szenarien können lokale Gruppenrichtlinienobjekte folglich verwendet werden?



Domänenbasierte Gruppenrichtlinien

... werden in Active Directory erstellt und auf Domänencontrollern gespeichert

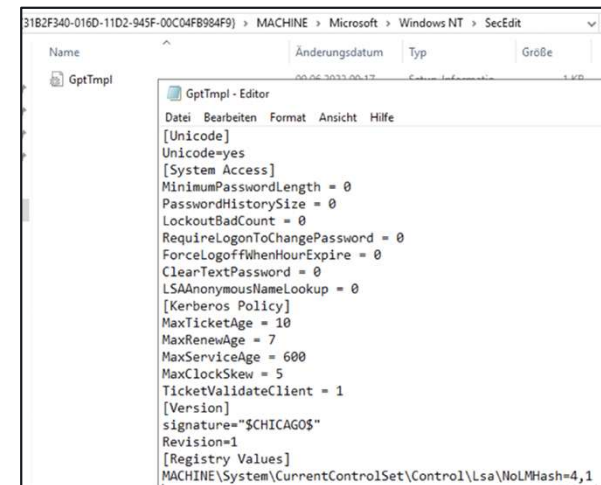
Zwei Standard-Gruppenrichtlinienobjekte

- Default Domain Policy
 - Definiert Kontorichtlinien für die Domäne: Kennwort, Kontosperrung und Kerberos-Richtlinien
 - Ist standardmäßig mit der Domain verknüpft
- Default Domain Controllers Policy
 - Definiert Überwachungsrichtlinien für Domänencontroller und für Active Directory
 - Ist standardmäßig mit der OU Domain Controllers verknüpft



Speichern von Gruppenrichtlinienobjekten

- GPOs sind Objekte in der Domäne, daher werden Sie auch als solche in der Domänendatenbank gespeichert
- Für die Verteilung der GPOs an die Clients werden diese zusätzlich mit ihrer GUID im SYSVOL Verzeichnis der Domain Controller gespeichert



Administrative Vorlagen

Mit den Richtlinieneinstellungen im Knoten “Administrative Vorlagen” werden Änderungen an der Registrierung vorgenommen.

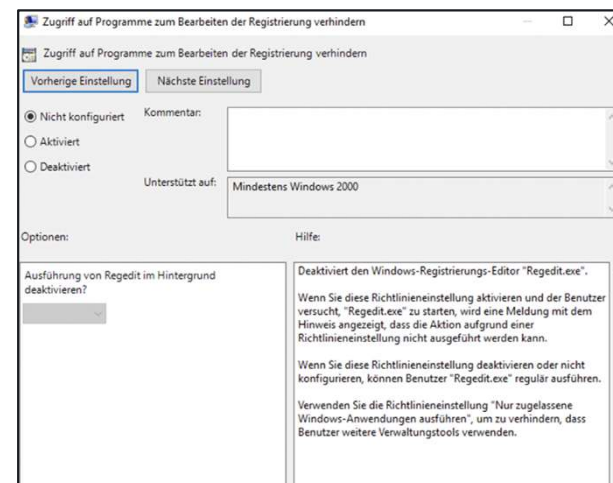
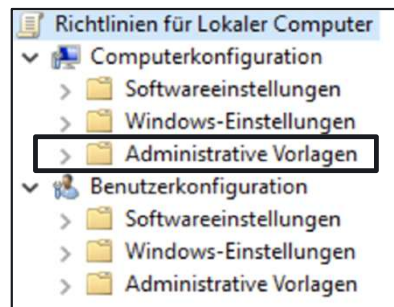
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
 - DisableRegeditMode
 1. Nur mit dem Benutzeroberflächentool Regedit
 2. Deaktivieren Sie auch regedit /s.



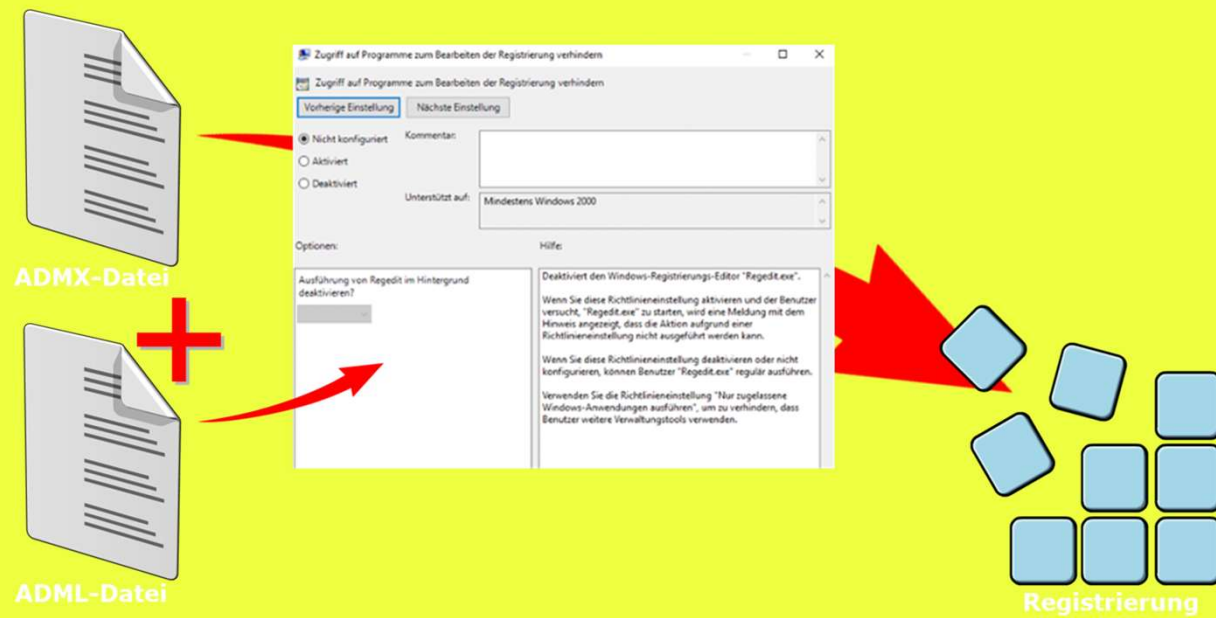
Administrative Vorlagen

Durch das Konfigurieren der Einstellungen wird die Benutzeroberfläche gesperrt; Benutzer können keine Änderungen an der Einstellung vornehmen.

- Die Sperrungen für Änderungen und die Benutzeroberfläche werden aufgehoben, wenn der Benutzer oder Computer nicht mehr zum Gültigkeitsbereich gehört.



ADMX & ADML



ADMX & ADML

ADMX- und ADML-Dateien

- Vom Client abgerufen
- Problematisch, wenn der Client nicht über die entsprechenden Dateien verfügt



ADMX & ADML

Zentraler Speicher

- Erstellen Sie auf einem Domänencontroller einen Ordner mit dem Namen PolicyDefinitions.
 - Remote:
\\contoso.com\SYSTEMVOLUME2\contoso.com\Policies\PolicyDefinitions
 - Lokal:
%SystemRoot%\SYSTEMVOLUME2\contoso.com\Policies\PolicyDefinitions
- Kopieren Sie ADMX-Dateien aus %SystemRoot%\PolicyDefinitions.
- Kopieren Sie die ADML-Datei aus den sprachspezifischen Unterordnern (z.B. de-de).



Sichern, Wiederherstellen, Kopieren und Importieren

- Gruppenrichtlinienobjekte lassen sich manuell sichern
 - Dies ist immer dann sinnvoll, wenn Veränderungen gemacht werden
- Aus den Sicherungen lassen sich die GPOs (innerhalb derselben Domäne) wiederherstellen
- Ebenfalls können aus den Sicherungen die Einstellungen in neue GPOs importiert werden
 - Dies ist besonders beim Übertragen von Einstellungen in andere Domänen hilfreich
- Wie viele Objekte in der AD lassen sich auch GPOs kopieren/duplizieren
 - Dies ist immer dann sinnvoll, wenn man vorhandene Richtlinien mit neuen Einstellungen versehen möchte. Diese Kopie wendet man dann zunächst auf eine Testgruppe an



Verknüpfung von Gruppenrichtlinien

- Gruppenrichtlinienobjekt-Verknüpfungen bewirken, dass Richtlinieneinstellungen in Gruppenrichtlinienobjekten für Benutzer oder Computer innerhalb der jeweiligen Organisationseinheit gelten
- Verknüpft ein Gruppenrichtlinienobjekt mit einem Standort, einer Domäne oder einer Organisationseinheit (SDOU)
- Ein Gruppenrichtlinienobjekt kann mit mehreren Standorten oder Organisationseinheiten verknüpft werden.
- Eine Verknüpfung kann vorhanden, aber deaktiviert sein.
- Eine Verknüpfung kann gelöscht werden, während das Gruppenrichtlinienobjekt erhalten bleibt.



Verknüpfung von Gruppenrichtlinien



Anwendung/Vererbung von Gruppenrichtlinien

Die Anwendung der mit den einzelnen Containern verknüpften Gruppenrichtlinienobjekte führt zu einem kumulativen Effekt, der als Vererbung bezeichnet wird.

Standard Rangfolge:

Lokal > Standort > Domäne > Organisationseinheit > Organisationseinheit > OU ...

Verknüpfungsreihenfolge:

Niedrigere Nummer > Höhere Position in der Liste > Vorgänger



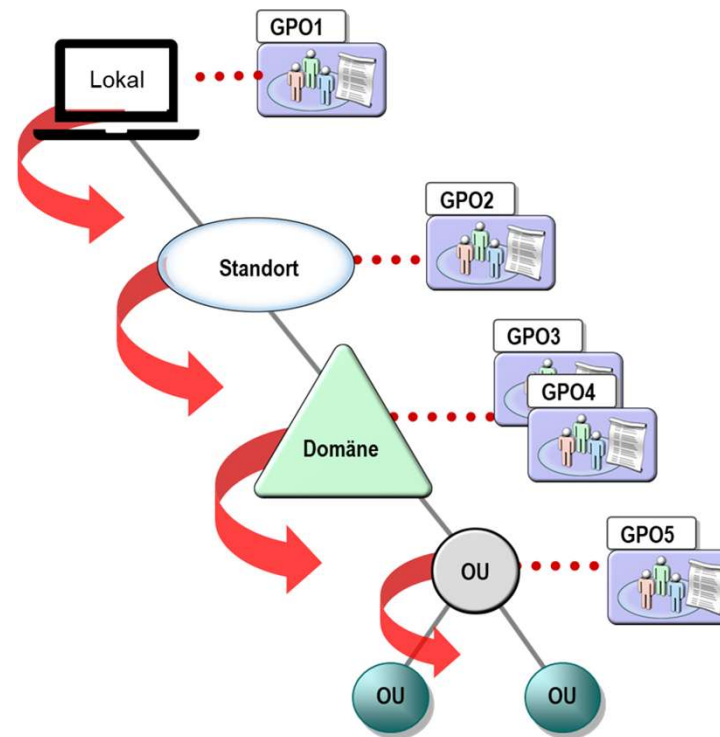
Anwendung/Vererbung von Gruppenrichtlinien

- **Deaktivieren** der Vererbung: Deaktiviert die Verarbeitung der Gruppenrichtlinienobjekte von oben
- **Erzwungene** Gruppenrichtlinienobjekte "durchbrechen" die Deaktivierung der Vererbung.
 - Erzwungene Einstellungen für Gruppenrichtlinienobjekte haben Vorrang vor in Konflikt stehenden Einstellungen in rangniedrigeren Gruppenrichtlinienobjekten.

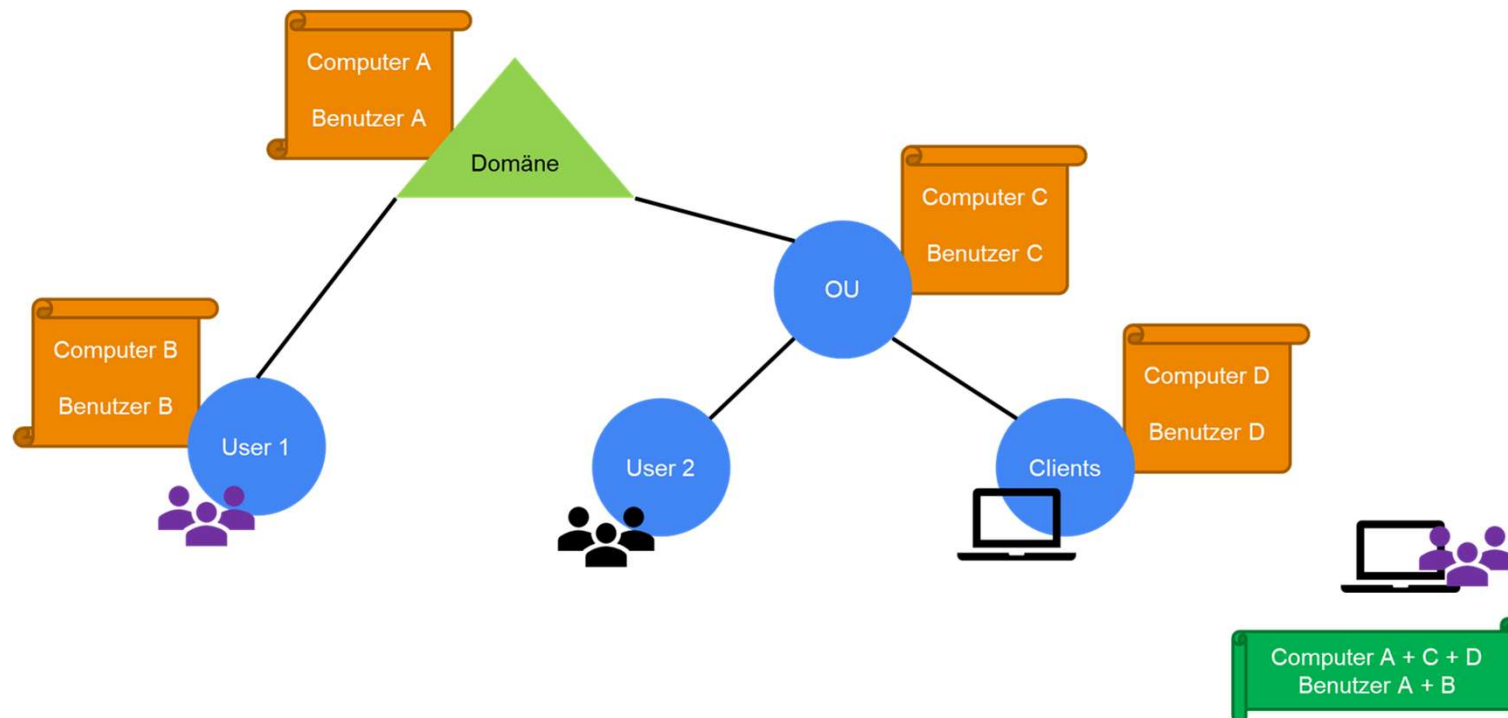
Notebooks				
Verknüpfte Gruppenrichtlinienobjekte Gruppenrichtlinienvererbung Delegierung				
Verknüpfungsreihenfolge		Gruppenrichtlinienobjekt	Erzwungen	Verknüpfung aktiviert
1		Contoso Client WLAN + LAN	Nein	Ja
2		Notebook Sicherheitsrichtlinie	Nein	Ja



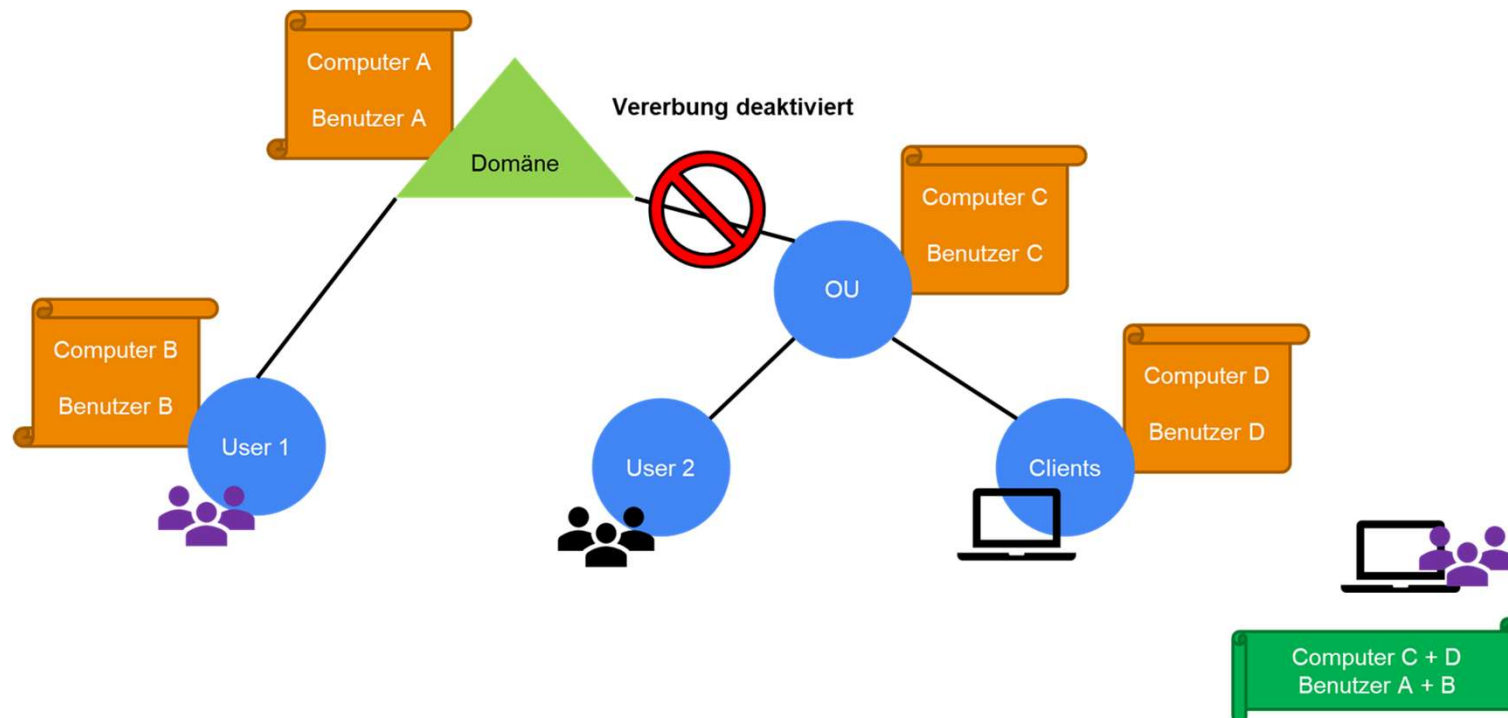
Anwendung/Vererbung von Gruppenrichtlinien



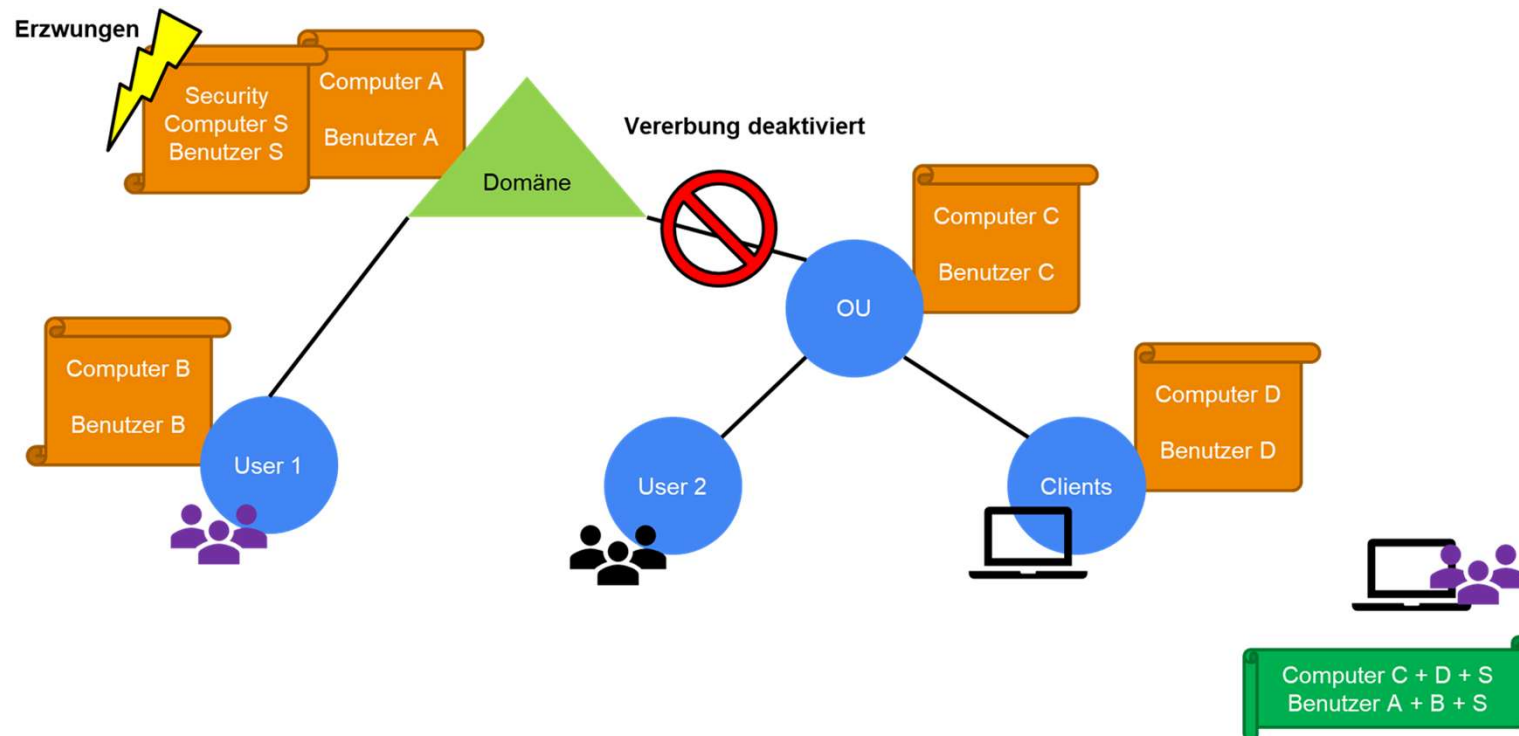
Anwendung/Vererbung von Gruppenrichtlinien



Anwendung/Vererbung von Gruppenrichtlinien

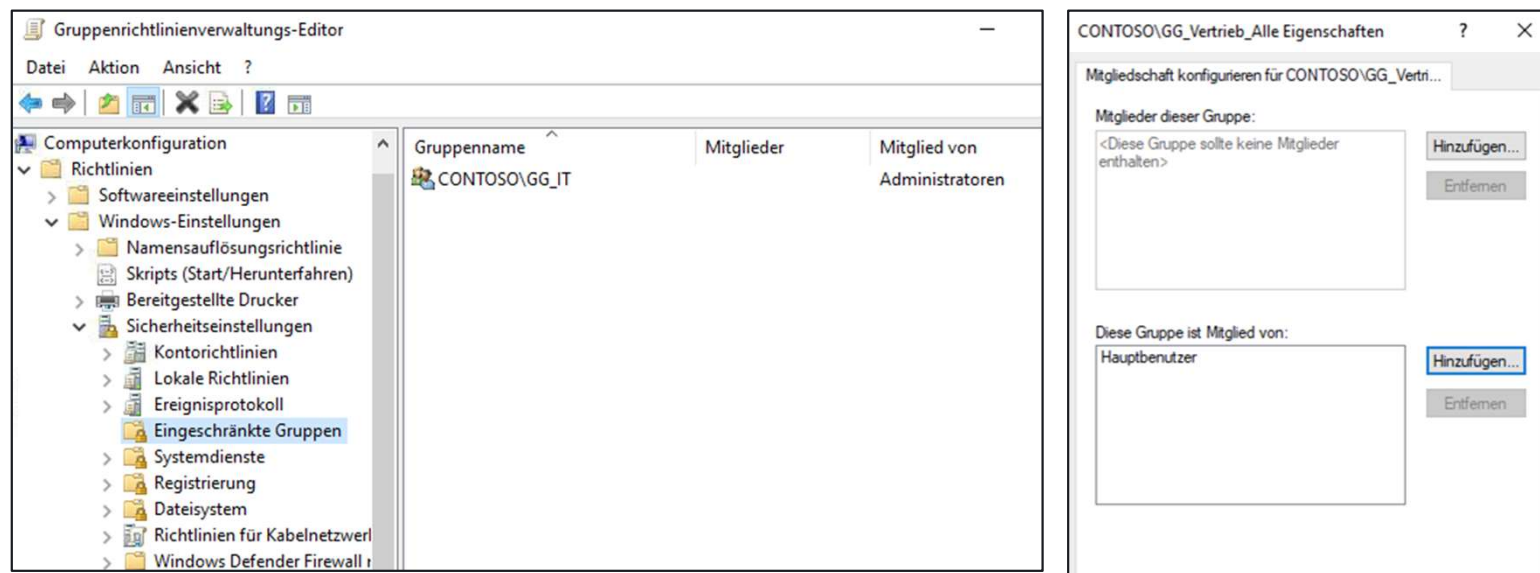


Anwendung/Vererbung von Gruppenrichtlinien



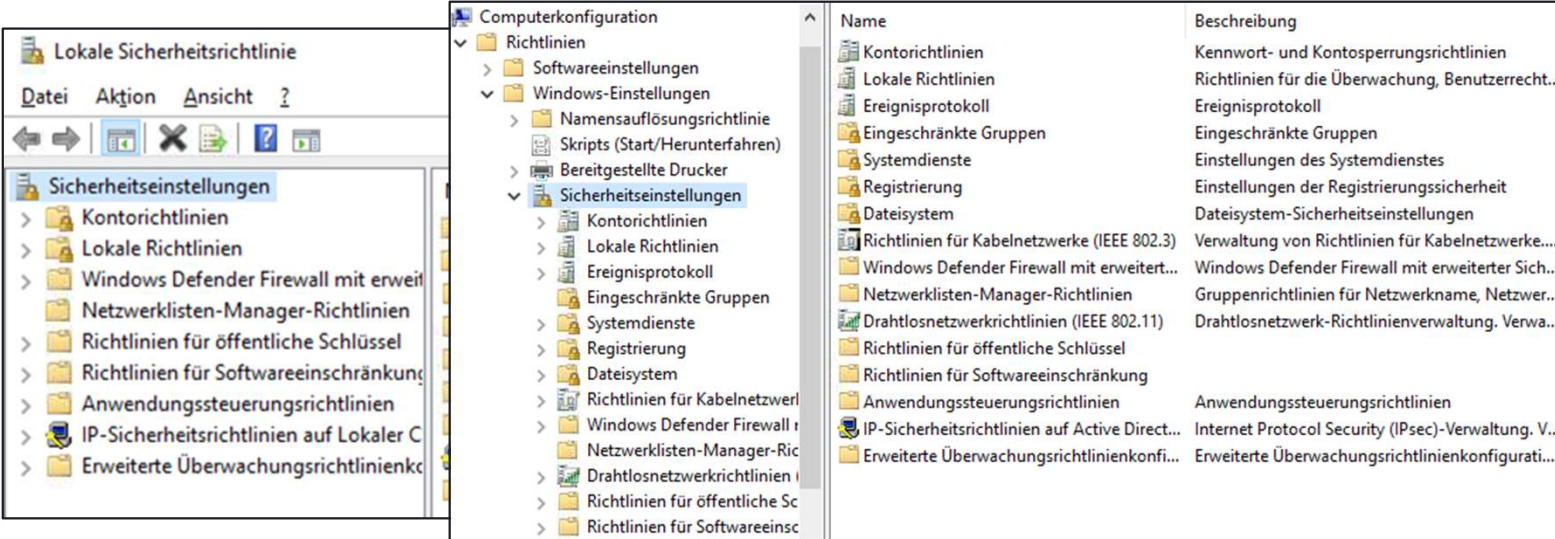
Steuern der Sicherheit mittels Richtlinien

- Anpassen von lokalen Gruppen – insbesondere „Administratoren“



Steuern der Sicherheit mittels Richtlinien

- Anpassen der Sicherheitsrichtlinie



The screenshot displays two overlapping Windows administrative tool windows. The background window is 'Computerkonfiguration' (Computer Configuration), showing a tree view under 'Richtlinien' (Policies) > 'Sicherheitseinstellungen' (Security Settings). The foreground window is 'Lokale Sicherheitsrichtlinie' (Local Security Policy), showing a list of security settings on the left and a detailed view on the right.

Name	Beschreibung
Kontorichtlinien	Kennwort- und Kontosperrungsrichtlinien
Lokale Richtlinien	Richtlinien für die Überwachung, Benutzerrecht...
Ereignisprotokoll	Ereignisprotokoll
Eingeschränkte Gruppen	Eingeschränkte Gruppen
Systemdienste	Einstellungen des Systemdienstes
Registrierung	Einstellungen der Registrierungssicherheit
Dateisystem	Dateisystem-Sicherheitseinstellungen
Richtlinien für Kabelnetzwerke (IEEE 802.3)	Verwaltung von Richtlinien für Kabelnetzwerke....
Windows Defender Firewall mit erweitert...	Windows Defender Firewall mit erweiterter Sich...
Netzwerklisten-Manager-Richtlinien	Gruppenrichtlinien für Netzwerkname, Netzwer...
Drahtlosnetzwerkrichtlinien (IEEE 802.11)	Drahtlosnetzwerk-Richtlinienverwaltung. Verwa...
Richtlinien für öffentliche Schlüssel	
Richtlinien für Softwareeinschränkung	
Anwendungssteuerungsrichtlinien	Anwendungssteuerungsrichtlinien
IP-Sicherheitsrichtlinien auf Active Direct...	Internet Protocol Security (IPsec)-Verwaltung. V..
Erweiterte Überwachungsrichtlinienkonfi...	Erweiterte Überwachungsrichtlinienkonfigurati...



Steuern der Sicherheit mittels Richtlinien

- Vorlagen für Sicherheitsrichtlinie

Richtlinie	Computereinstellung
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen	24 gespeicherte Kennwörter
Kennwörter mit umkehrbarer Verschlüsselung speichern	Nicht definiert
Maximales Kennwortalter	Nicht definiert
Minimale Kennwortlänge	12 Zeichen
Minimales Kennwortalter	Nicht definiert
Überwachung der Mindestpasswortlänge	Nicht definiert

- Verwenden von verschiedenen Richtlinien für Benutzer & Administratoren



Überwachungsrichtlinien

- Überwachen von Ereignissen in einer Kategorie von Aktivitäten
 - Zugriff auf NTFS-Dateien/-Ordner
 - Änderungen an Konten oder Objekten in Active Directory
 - Anmeldung
 - Zuweisung oder Verwendung von Benutzerrechten
- Standardmäßig werden auf Domänencontrollern Erfolgsereignisse für die meisten Kategorien überwacht.

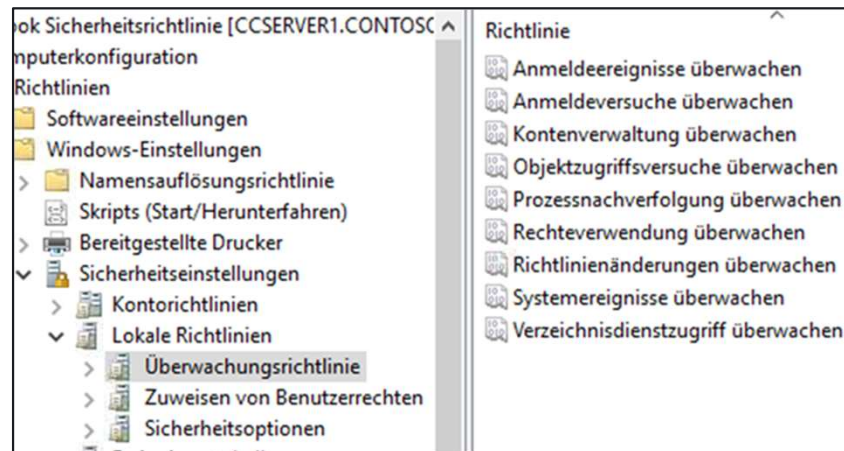


Überwachungsrichtlinien

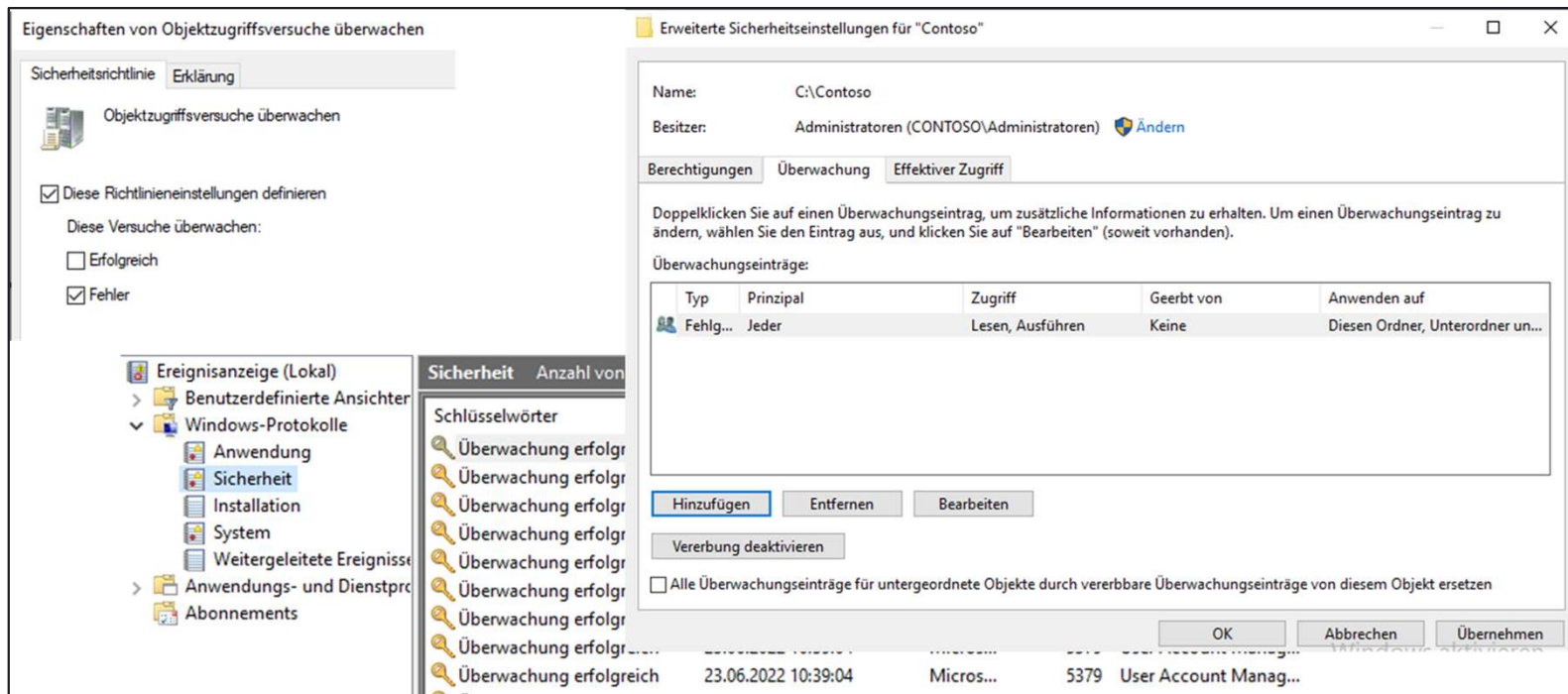
- Ziel: Abstimmen der Überwachungsrichtlinien auf die Sicherheitsrichtlinien des Unternehmens und auf die Realität
 - Übermäßige Überwachung: Die Protokolle werden zu groß, um die relevanten Ereignisse zu finden.
 - Unzureichende Überwachung: Wichtige Ereignisse werden nicht protokolliert.
 - Tools zum Konsolidieren und Verarbeiten von Protokollen können hilfreich sein.



Überwachungsrichtlinien



Überwachung des Ordnerzugriffs



Schreibgeschützter Domänencontroller

- Wird z.B. in einer Zweigstelle ein Domain Controller für die Authentifizierung benötigt, die Sicherheit vor Ort aber nicht wie in einem Rechenzentrum gegeben ist, so kann ein schreibgeschützter Domänencontroller (RODC) eine gute Wahl sein.
- Ein RODC kann KEINE Änderungen in der Domäne vornehmen
- Ein RODC kennt alle Objekte in der Domäne, aber nicht alle Attribute und keine „Geheimnisse“
 - Kennwörter von vorab definierten Gruppen können lokal zur Authentifizierung zwischengespeichert werden
- Ein RODC verfügt über eine lokale Administratorengruppe zur Verwaltung des RODC ohne Verbindung zur Domäne
- Die Installation des RODC erfolgt über den Assistenten zum Installieren der ADDS oder mittels dcpromo



DANKE!

Gibt es noch Fragen?





CloudCommand