



CARO-Suite
CUSATUM Access Rights Optimizer

CARO-AD-Observer
Voraussetzungen für den Betrieb

Version 2026.9

September 2026



Voraussetzungen für den Betrieb

Diese Anleitung beschreibt alle technischen Grundvoraussetzungen, die auf Ihren Domänencontrollern erfüllt sein müssen, damit der CARO-AD-Observer korrekt arbeiten kann. Die Schritte bauen aufeinander auf und sollten in der angegebenen Reihenfolge durchgeführt werden.

Zielgruppe: IT-Administratoren mit grundlegenden Active Directory-Kenntnissen

Berechtigungen: Domänen-Administrator oder gleichwertiges Konto erforderlich

Voraussetzungen für den Betrieb.....	1
Übersicht	3
Rechtlicher Hinweis zu Screenshots.....	3
Unterstützte Windows Server Versionen	3
Notwendige Berechtigungen überprüfen.....	4
Gruppe Event Log Readers	4
Unterstützung von mehreren DCs	4
Audit-Richtlinien konfigurieren	5
Was ist eine Audit-Richtlinie?	5
Schritt-für-Schritt-Anleitung per Gruppenrichtlinie	5
Empfohlene Größe des Windows-Sicherheitsprotokolls	10
SACL-Berechtigungen im Active Directory setzen	12
Was ist eine SACL?.....	12
Schritt-für-Schritt-Anleitung	12
Windows-Firewall konfigurieren.....	17
Warum ist das notwendig?.....	17
Schritt-für-Schritt-Anleitung	17
Einstellungen überprüfen.....	18
Audit-Richtlinien prüfen	18
SACL prüfen.....	20
Firewall prüfen.....	20
Schnell-Checkliste.....	20



Übersicht

Der CARO AD-Observer liest Sicherheitsereignisse aus den Domänencontrollern (DC) aus, um Änderungen im Active Directory zu protokollieren und auszuwerten. Damit das funktioniert, müssen drei Dinge sichergestellt sein:

1. **Audit-Richtlinien** – Windows muss angewiesen werden, die richtigen Ereignisse überhaupt aufzuzeichnen.
2. **SACL-Berechtigungen** – Active Directory-Objekte müssen so konfiguriert sein, dass Änderungen an ihnen im Sicherheitsprotokoll erscheinen.
3. **Windows-Firewall** – Der CARO-Server muss die Ereignislogs der Domänencontroller remote auslesen dürfen.

Rechtlicher Hinweis zu Screenshots

Alle in diesem Dokument verwendeten Screenshots zeigen Benutzeroberflächen von **Microsoft Windows Server 2022**.

© Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, Windows, Windows Server und das **Windows-Logo** sind Marken der Microsoft-Unternehmensgruppe. Die Screenshots werden ausschließlich zu Dokumentations- und Schulungszwecken verwendet.

Unterstützte Windows Server Versionen

⚠ Wichtiger Hinweis zum Support-Status Ihrer Domänencontroller

Die folgende Tabelle zeigt den aktuellen Support-Status der relevanten Windows Server Versionen. Wir empfehlen dringend, den Betrieb Ihrer Domänencontroller auf Windows Server 2019 oder neuer zu planen bzw. zu migrieren.

Version	Mainstream-Support Ende	Erweiterter Support Ende	Status
Windows Server 2012 R2	09.10.2018	10.10.2023	🚫 abgekündigt – kein Support mehr, ESU nur bis Okt. 2026
Windows Server 2016	11.01.2022	12.01.2027	⚠ Bald abgekündigt – erweiterter Support endet Jan. 2027
Windows Server 2019	09.01.2024	09.01.2029	✅ empfohlen – aktiv unterstützt
Windows Server 2022	13.10.2026	14.10.2031	✅ empfohlen – aktuell

Empfehlung:

Die Mindest-Zielpattform für neue oder modernisierte Domänencontroller ist **Windows Server 2019**. Windows Server 2016 läuft zwar noch bis Januar 2027, sollte aber nicht mehr für neue Deployments genutzt werden. Windows Server 2012 R2 ist seit Oktober 2023 vollständig abgekündigt – auch Extended Security Updates (ESU) laufen im Oktober 2026 endgültig aus.



Notwendige Berechtigungen überprüfen

Der AD-Observer liest AD-Security-Events in regelmäßigen Abständen aus dem Microsoft Security Event Log aus. Dazu muss das benutzte Service-Konto die notwendigen Zugriffe haben. Es wird das Anmeldekonto, welches im AD-Einstiegspunkt im CARO-Konfigurationsmanager hinterlegt ist, verwendet.

Active Directory - Einstiegspunkt bearbeiten

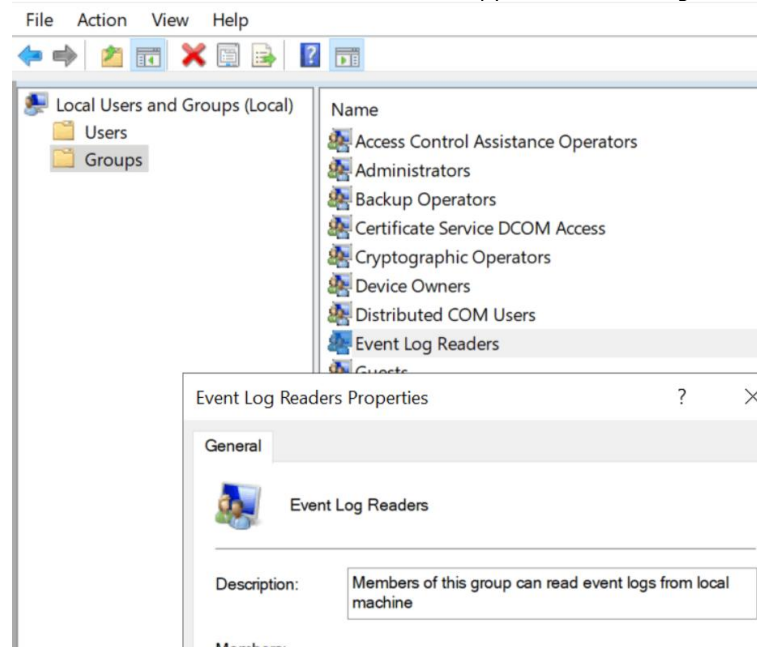
Anmeldedaten: Domäne:

Name:

Wenn das Servicekonto für die Nutzung des AD-Observers nicht über administrative oder Nur-Lese-Berechtigungen verfügt (Non-Admin oder Read-Only Access), müssen folgende Einstellungen vorgenommen werden.

Gruppe Event Log Readers

Das Service-Konto muss auf dem Domänencontroller in der Gruppe der **Event Log Readers** eingetragen sein.

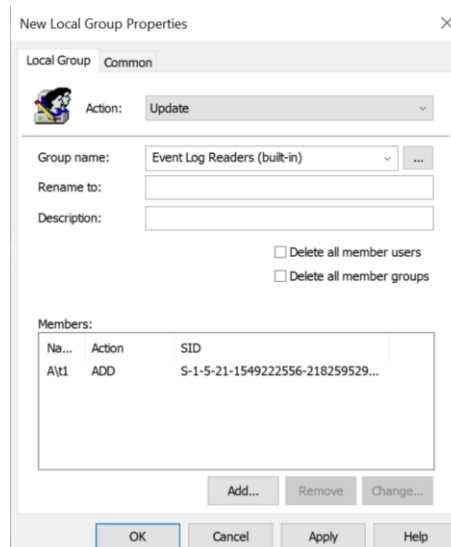


Fenster: Lokale Benutzer und Gruppen (lusrmgr.msc)

Unterstützung von mehreren DCs

Falls Sie mehrere DCs haben, können Sie die Einstellung auch über die **Gruppenrichtlinie (GPO)** umsetzen. Führen Sie dazu die folgenden Schritte aus:

1. Erstellen Sie eine Organisationseinheit (OU) und ordnen Sie diese Computer dieser OU zu.
2. Erstellen Sie eine Gruppenrichtlinie (GPO).
3. Verknüpfen Sie diese GPO mit der oben genannten OU.
4. Bearbeiten Sie die GPO. Navigieren Sie zu „Configuration\Preferences\Control Panel Settings\Local users and groups\New Local Group“.
5. Gruppenname: Event Log Readers (built-in)
6. Mitglieder: Fügen Sie den gewünschten Benutzer oder die gewünschte Gruppe hinzu.



Dialog: Eigenschaften der neuen lokalen Gruppe

Audit-Richtlinien konfigurieren

Was ist eine Audit-Richtlinie?

Windows protokolliert standardmäßig nur wenige Ereignisse. Mit einer Audit-Richtlinie teilen Sie Windows mit: „Schreibe in das Sicherheitsprotokoll, wenn z. B. ein Benutzerkonto geändert oder eine Gruppe bearbeitet wird.“

Die Konfiguration erfolgt über eine **Gruppenrichtlinie (GPO)**. Das hat den Vorteil, dass Sie die Einstellung nur einmal festlegen müssen und sie automatisch auf alle Domänencontroller verteilt wird.

⚠ Hinweis für Windows Server 2012 R2: Diese Version ist abgekündigt. Die nachfolgende Anleitung funktioniert technisch, jedoch wird ein Upgrade auf Windows Server 2019 oder 2022 dringend empfohlen.

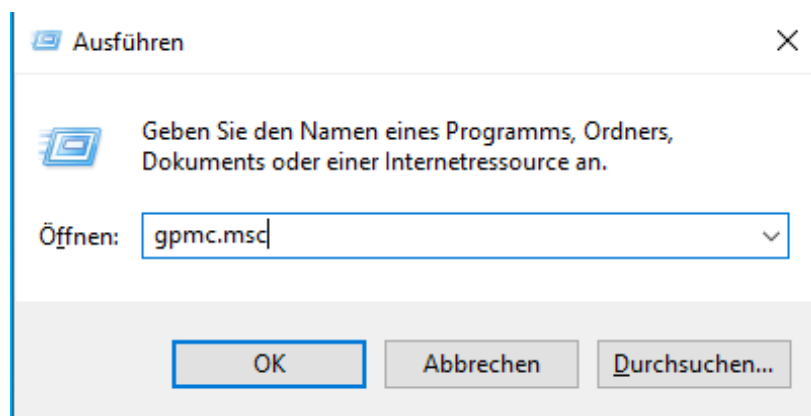
⚠ Hinweis für Windows Server 2016: Der Mainstream-Support ist bereits beendet, der erweiterte Support endet im Januar 2027. Planen Sie jetzt die Migration auf Windows Server 2019 oder 2022.

Schritt-für-Schritt-Anleitung per Gruppenrichtlinie

Wichtig: Die Reihenfolge der folgenden Schritte ist entscheidend. Bitte nicht vertauschen.

Schritt 1 – Gruppenrichtlinienverwaltung öffnen

Drücken Sie Windows + R, geben Sie folgenden Befehl ein und bestätigen Sie mit Enter: gpmc.msc



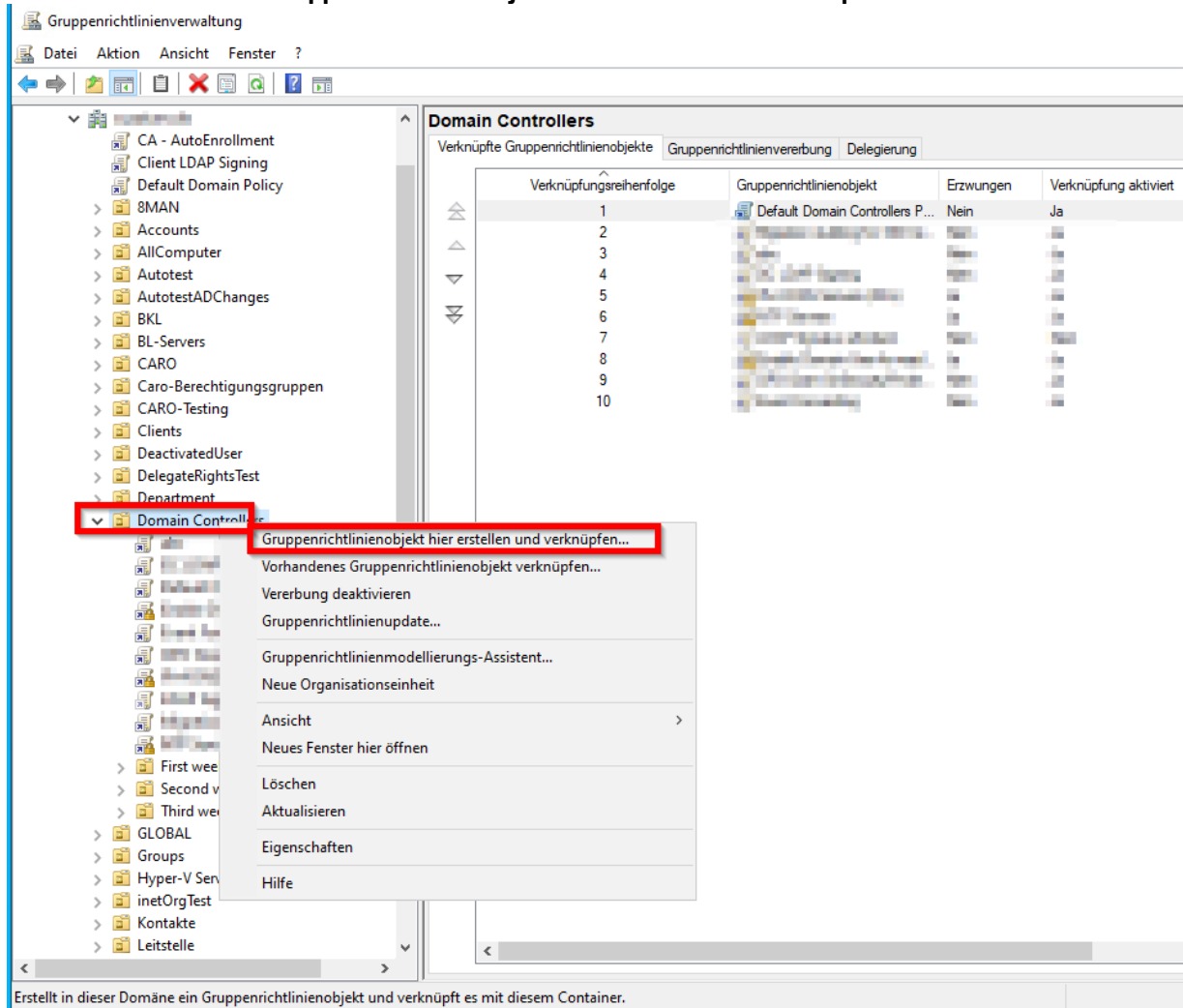
Ausführen-Dialog mit gpmc.msc



Schritt 2 – Neue Gruppenrichtlinie erstellen

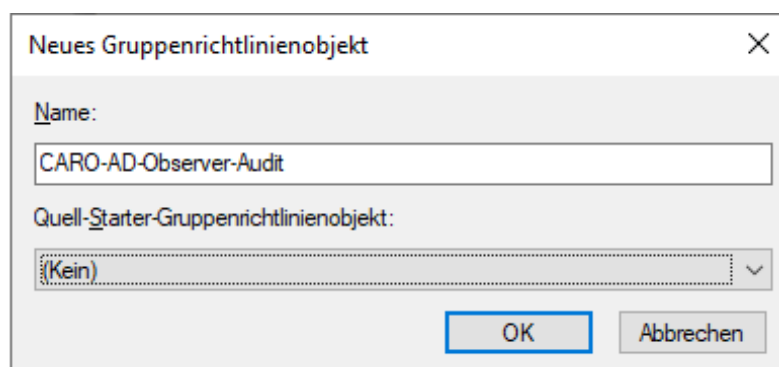
Navigieren Sie zur Organisationseinheit (OU) **Domain Controllers** in der Baumansicht links.

Rechtsklick auf die OU → **Gruppenrichtlinienobjekt hier erstellen und verknüpfen**.



Domain Controllers OU – Rechtsklick-Menü zum Erstellen der GPO

Geben Sie dem neuen Objekt einen aussagekräftigen Namen, z. B.: CARO-AD-Observer-Audit



Dialog „Neues Gruppenrichtlinienobjekt“ mit ausgefülltem Namen

Schritt 3 – Richtlinie bearbeiten

Rechtsklick auf die neue Richtlinie → **Bearbeiten**. Der Gruppenrichtlinien-Editor öffnet sich.



Schritt 4 – Unterkategorien erzwingen (wichtig!)

Navigieren Sie zu:

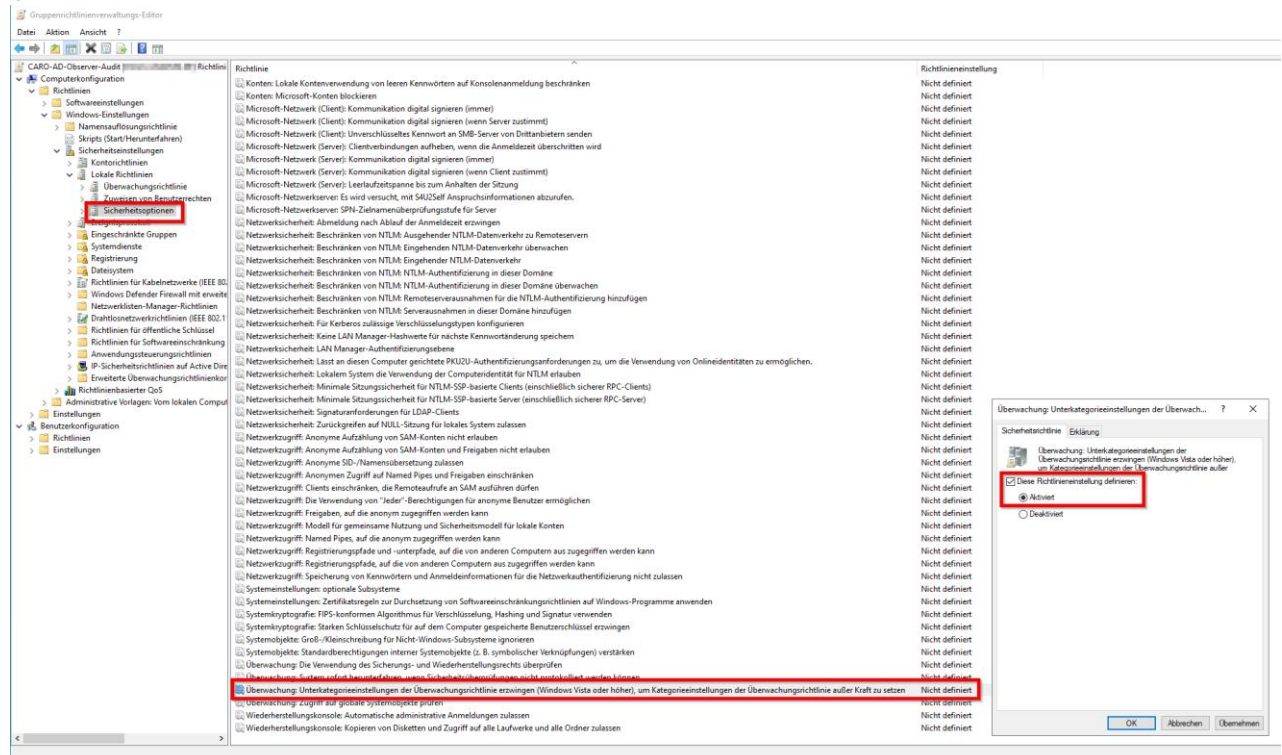
Computerkonfiguration

- Windows-Einstellungen
- Sicherheitseinstellungen
- Lokale Richtlinien
- Sicherheitsoptionen

Scrollen Sie in der rechten Spalte ganz nach unten und öffnen Sie den Eintrag:

„Überwachung: Unterkategorieeinstellungen der Überwachungsrichtlinie erzwingen (Windows Vista oder höher), um Kategorieeinstellungen der Überwachungsrichtlinie außer Kraft zu setzen“

Aktivieren Sie die Checkbox **„Diese Richtlinieneinstellung definieren“**, wählen Sie **Aktiviert** und klicken Sie auf **OK**.



Sicherheitsoptionen – Eintrag „Untercategoryeinstellungen erzwingen“ auf „Aktiviert“ gesetzt

Warum ist das wichtig?

Ohne diese Einstellung können die speziellen Unterkategorien weiter unten unter Umständen ignoriert werden. Dieser Schritt muss immer als Erstes erfolgen.

Schritt 5 – Kontoverwaltung überwachen

Navigieren Sie zu:

Computerkonfiguration

- Windows-Einstellungen
- Sicherheitseinstellungen
- Erweiterte Überwachungsrichtlinienkonfiguration ← (NICHT "Lokale Richtlinien!")
- Überwachungsrichtlinien
- Kontoverwaltung

Wählen Sie alle Einträge mit Strg + A aus, rechtsklicken Sie → **Eigenschaften**.

Aktivieren Sie **„Die ausgewählten Ereignisse, die überwacht werden sollen, konfigurieren“** und setzen Sie ein Häkchen bei **„Alle Erfolge überwachen“**. Klicken Sie auf **OK**.



Gruppenrichtlinienverwaltungs-Editor

Datei Aktion Ansicht ?

CARO-AD-Observer-Audit | Richtlini

Computerkonfiguration

Richtlinien

Softwareeinstellungen

Windows-Einstellungen

Namensauflösungsrichtlinie

Skripts (Start/Herunterfahren)

Sicherheitseinstellungen

Kontorichtlinien

Lokale Richtlinien

Überwachungsrichtlinie

Zuweisen von Benutzerrechten

Sicherheitsoptionen

Ereignisprotokoll

Eingeschränkte Gruppen

Systemdienste

Registrierung

Datensystem

Richtlinien für Kabelnetzwerke (IEEE 802.3)

Windows Defender Firewall mit erweiterter Netzwerklisten-Manager-Richtlinien

Drahtlosnetzwerkrichtlinien (IEEE 802.11)

Richtlinien für öffentliche Schlüssel

Richtlinien für Softwareeinschränkung

Anwendungssteuerungsrichtlinien

Erweiterte Überwachungsrichtlinienkonfiguration

Kontoanmeldung

Kontenverwaltung

Detaillierte Überwachung

DS-Zugriff

Anmelden/Abmelden

Objektzugriff

Richtlinienänderung

Berechtigungen

System

Globale Objektzugriffsüberwachung

Richtlinienbasierter QoS

Administrative Vorlagen: Vom lokalen Computer

Einstellungen

Benutzerkonfiguration

Richtlinien

Einstellungen

Unterkategorie	Überwachungsereignisse
Anwendungsgruppenverwaltung überwachen	Nicht konfiguriert
Computerkontoverwaltung überwachen	Nicht konfiguriert
Verteilerguppenverwaltung überwachen	Nicht konfiguriert
Andere Kontoverwaltungsereignisse überwachen	Nicht konfiguriert
Sicherheitsgruppenverwaltung überwachen	Nicht konfiguriert
Benutzerkontenverwaltung überwachen	Nicht konfiguriert

Eigenschaften für Mehrfachobjekte

Richtlinie

☒ Die ausgewählten Ereignisse, die überwacht werden sollen, konfigurieren:

☒ Alle Erfolge überwachen

☐ Alle Fehler überwachen

OK Abbrechen Übernehmen

Kontoverwaltung – alle Unterkategorien markiert, „Alle Erfolge überwachen“ aktiviert

Schritt 6 – Verzeichnisdienst-Änderungen überwachen

Navigieren Sie zu:

Computerkonfiguration

→ Windows-Einstellungen

→ Sicherheitseinstellungen

→ Erweiterte Überwachungsrichtlinienkonfiguration

→ Überwachungsrichtlinien

→ DS-Zugriff

6a) Öffnen Sie „Verzeichnisdienständerungen überwachen“.

Aktivieren Sie „Folgende Überwachungsereignisse konfigurieren“ → Häkchen bei „Erfolg“ → OK.



Gruppenrichtlinienverwaltungs-Editor

Datei Aktion Ansicht ?

← → ↻ 📄 ? 📄

CARO-AD-Observer-Audit Richtlini

- Computerkonfiguration
 - Richtlinien
 - Softwareeinstellungen
 - Windows-Einstellungen
 - Namensauflösungsrichtlinie
 - Skripts (Start/Herunterfahren)
 - Sicherheitseinstellungen
 - Kontorichtlinien
 - Lokale Richtlinien
 - Überwachungsrichtlinie
 - Zuweisen von Benutzerrechten
 - Sicherheitsoptionen
 - Ereignisprotokoll
 - Eingeschränkte Gruppen
 - Systemdienste
 - Registrierung
 - Datensystem
 - Richtlinien für Kabelnetzwerke (IEEE 802.3)
 - Windows Defender Firewall mit erweiterter
 - Netzwerklisten-Manager-Richtlinien
 - Drahtlosnetzwerkrichtlinien (IEEE 802.11)
 - Richtlinien für öffentliche Schlüssel
 - Richtlinien für Softwareeinschränkung
 - Anwendungssteuerungsrichtlinien
 - IP-Sicherheitsrichtlinien auf Active Directory
 - Erweiterte Überwachungsrichtlinienkonfiguration**
 - Überwachungsrichtlinien
 - Kontoanmeldung
 - Kontenverwaltung
 - Detaillierte Überwachung
 - DS-Zugriff**
 - Anmelden/Abmelden
 - Objektzugriff
 - Richtlinienänderung
 - Berechtigungen
 - System
 - Globale Objektzugriffsüberwachung

Unterkategorie	Überwachungsereignisse
Detaillierte Verzeichnisdienstreplikation überwachen	Nicht konfiguriert
Verzeichnisdienstzugriff überwachen	Nicht konfiguriert
Verzeichnisdienständerungen überwachen	Nicht konfiguriert
Verzeichnisdienstreplikation überwachen	Nicht konfiguriert

Eigenschaften von Verzeichnisdienständerungen überwachen

Richtlinie Erklärung

Verzeichnisdienständerungen überwachen

☒ Folgende Überwachungsereignisse konfigurieren:

☒ Erfolg

☐ Fehler

OK Abbrechen Übernehmen

DS-Zugriff – „Verzeichnisdienständerungen überwachen“ auf „Erfolg“ gesetzt

Schritt 7 – Richtlinienänderungen überwachen

Navigieren Sie zu:

Computerkonfiguration

→ Windows-Einstellungen

→ Sicherheitseinstellungen

→ Erweiterte Überwachungsrichtlinienkonfiguration

→ Überwachungsrichtlinien

→ Richtlinienänderung

Öffnen Sie „Überwachungsrichtlinienänderung überwachen“.

Aktivieren Sie „Folgende Überwachungsereignisse konfigurieren“ → Häkchen bei „Erfolg“ → OK.



Gruppenrichtlinienverwaltungs-Editor

Datei Aktion Ansicht ?

CARO-AD-Observer-Audit [DC02.CUSATUM.DE] Richtlinien

- Computerkonfiguration
 - Richtlinien
 - Softwareeinstellungen
 - Windows-Einstellungen
 - Namensauflösungsrichtlinie
 - Skripts (Start/Herunterfahren)
 - Sicherheitseinstellungen
 - Kontorichtlinien
 - Lokale Richtlinien
 - Überwachungsrichtlinie
 - Zuweisen von Benutzerrechten
 - Sicherheitsoptionen
 - Ereignisprotokoll
 - Eingeschränkte Gruppen
 - Systemdienste
 - Registrierung
 - Dateisystem
 - Richtlinien für Kabelnetzwerke (IEEE 802.3)
 - Windows Defender Firewall mit erweiterter Netzwerklisten-Manager-Richtlinien
 - Drahtlosnetzwerkrichtlinien (IEEE 802.11)
 - Richtlinien für öffentliche Schlüssel
 - Richtlinien für Softwareeinschränkung
 - Anwendungssteuerungsrichtlinien
 - IP-Sicherheitsrichtlinien auf Active Directory
 - Erweiterte Überwachungsrichtlinienkonfiguration**
 - Überwachungsrichtlinien
 - Kontoanmeldung
 - Kontenverwaltung
 - Detaillierte Überwachung
 - DS-Zugriff
 - Anmelden/Abmelden
 - Objektzugriff
 - Richtlinienänderung**
 - Berechtigungen
 - System
 - Globale Objektzugriffsüberwachung

Unterkategorie	Überwachungsergebnisse
Überwachungsrichtlinienänderung überwachen	Erfolgreich
Authentifizierungsrichtlinienänderung überwachen	Nicht konfiguriert
Autorisierungsrichtlinienänderung überwachen	Nicht konfiguriert
Filterplattform-Richtlinienänderung überwachen	Nicht konfiguriert
MPSSVC-Richtlinienänderung auf Regelebene überwachen	Nicht konfiguriert
Andere Richtlinienänderungsergebnisse überwachen	Nicht konfiguriert

Eigenschaften von Überwachungsrichtlinienänderung überwachen

Richtlinie Erklärung

Überwachungsrichtlinienänderung überwachen

☒ Folgende Überwachungsergebnisse konfigurieren:

☒ Erfolg

☐ Fehler

OK Abbrechen Übernehmen

Richtlinienänderung – „Überwachungsrichtlinienänderung überwachen“ auf „Erfolg“ gesetzt

Schritt 8 – Richtlinie sofort anwenden

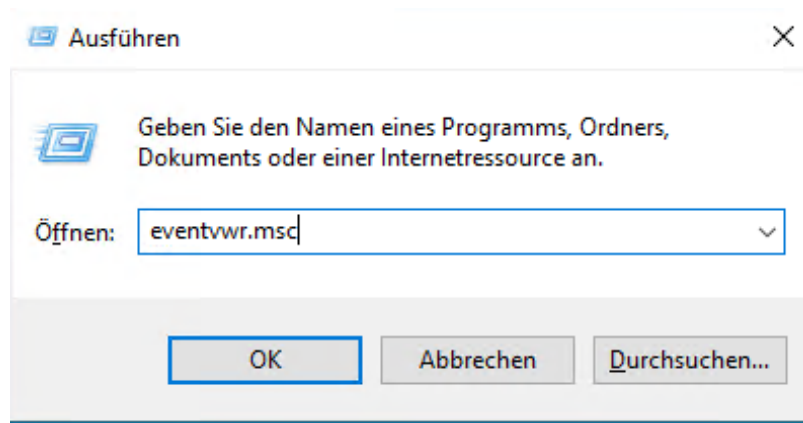
Öffnen Sie auf **jedem** Domänencontroller die Eingabeaufforderung als Administrator und führen Sie aus:
gpupdate /force

Hinweis: Abhängig von Ihrer Active Directory-Replikation kann es einige Minuten dauern, bis die Richtlinie auf allen Domänencontrollern aktiv ist.

Empfohlene Größe des Windows-Sicherheitsprotokolls

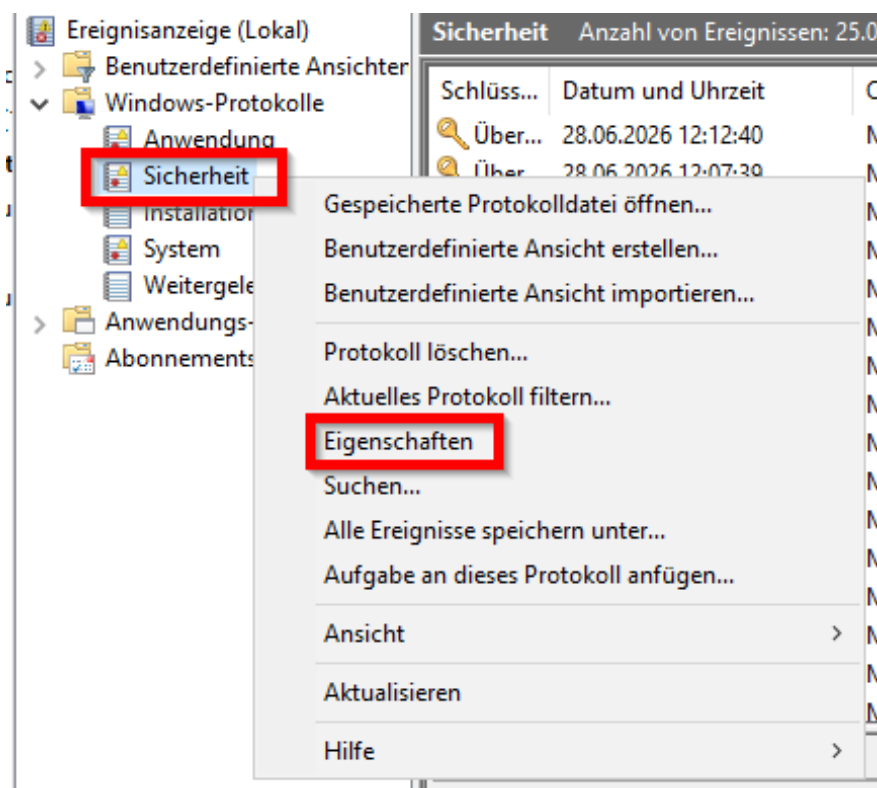
Damit keine Ereignisse verloren gehen, bevor der CARO AD-Observer sie ausliest, sollten Sie die maximale Größe des **Sicherheitsereignisprotokolls** anpassen.

Öffnen Sie die Ereignisanzeige:
eventvwr.msc



Ausführen-Dialog mit eventvwr.msc

Navigieren Sie zu **Windows-Protokolle** → Rechtsklick auf **Sicherheit** → **Eigenschaften**.



Ereignisanzeige – Rechtsklick auf „Sicherheit“ → „Eigenschaften“

Passen Sie die **maximale Protokollgröße (KB)** an – empfohlen sind mindestens **131.072 KB (= 128 MB)**.

Stellen Sie sicher, dass **„Ereignisse bei Bedarf überschreiben (älteste Ereignisse zuerst)“** ausgewählt ist.



Protokolleigenschaften - Sicherheit (Typ Verwaltung) X

Allgemein

Vollständiger Name: Security

Protokollpfad: %SystemRoot%\System32\Winevt\Logs\Security.evtx

Protokollgröße: 128,00 MB(134.221.824 Bytes)

Erstellt: Freitag, 24. Oktober 2025 16:51:16

Geändert: Sonntag, 28. Juni 2026 12:18:11

Letzter Zugriff: Sonntag, 28. Juni 2026 12:18:11

☒ Protokollierung

Max. Protokollgröße (KB): 131072

Bei Erreichen der maximalen Ereignisprotokollgröße:

☒ Ereignisse bei Bedarf überschreiben (älteste Ereignisse zuerst)

☐ Volles Protokoll archivieren, Ereignisse nicht überschreiben

☐ Ereignisse nicht überschreiben (Protokoll manuell löschen)

Protokoll löschen

OK Abbrechen Übernehmen

Sicherheitsprotokoll-Eigenschaften - maximale Größe 131.072 KB und Überschreiben-Option aktiv

SACL-Berechtigungen im Active Directory setzen

Was ist eine SACL?

Eine SACL (System Access Control List) ist eine unsichtbare „Wachliste“ für Active Directory-Objekte. Sie legt fest, welche Aktionen auf einem Objekt (z. B. dem Domain-Objekt) protokolliert werden sollen. Ohne SACL-Einträge erzeugt Windows keine Einträge im Sicherheitsprotokoll, selbst wenn die Audit-Richtlinien aktiv sind.

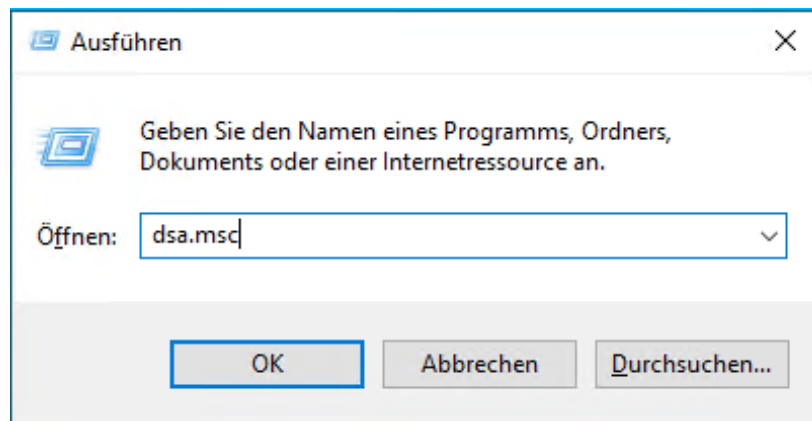
Gut zu wissen: Die SACL muss nur auf **einem** Domänencontroller konfiguriert werden. Die Einstellung wird automatisch durch die AD-Replikation auf alle anderen DCs übertragen.

Voraussetzung: Sie benötigen das Benutzerrecht **Überwachungs- und Sicherheitsprotokoll verwalten** (SeSecurityPrivilege). Domänen-Administratoren haben dieses Recht standardmäßig.

Schritt-für-Schritt-Anleitung

Schritt 1 - Active Directory-Benutzer und -Computer öffnen

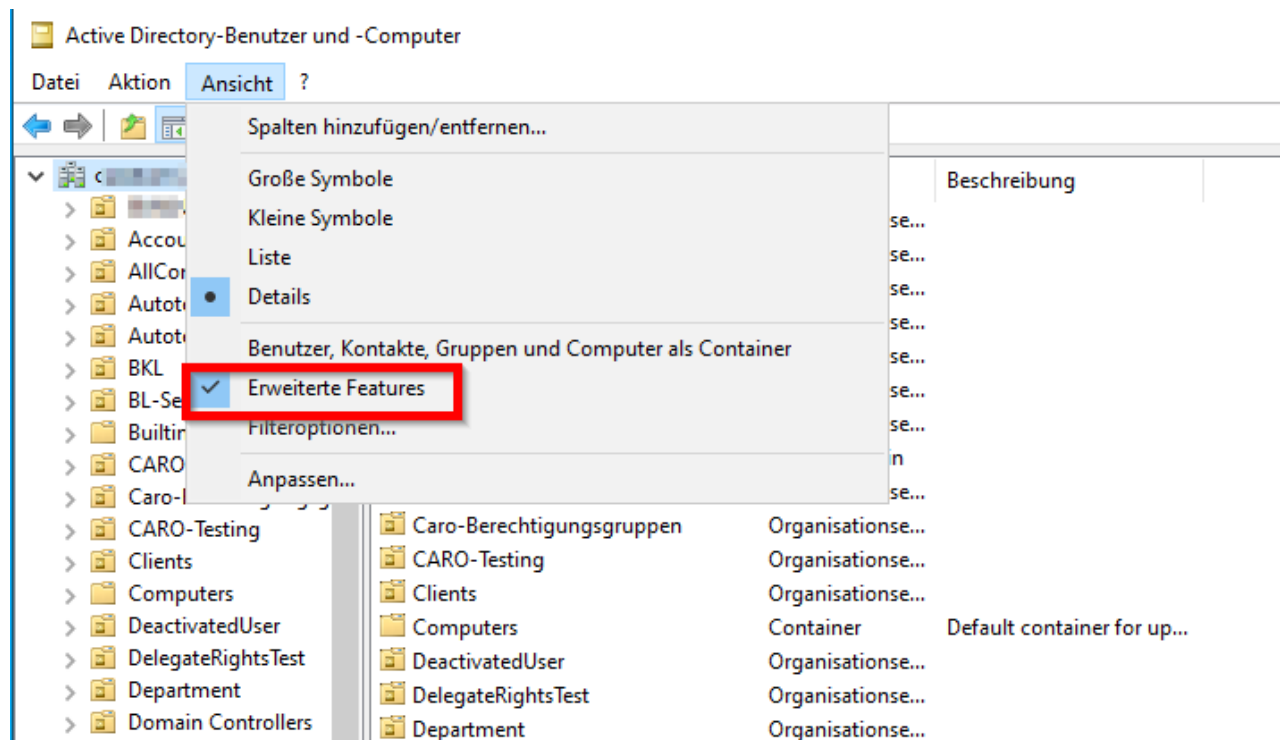
Drücken Sie Windows + R, geben Sie ein und bestätigen Sie mit Enter:
dsa.msc



Ausführen-Dialog mit dsa.msc

Schritt 2 – Erweiterte Features einblenden

Klicken Sie im Menü auf **Ansicht** → **Erweiterte Features**.



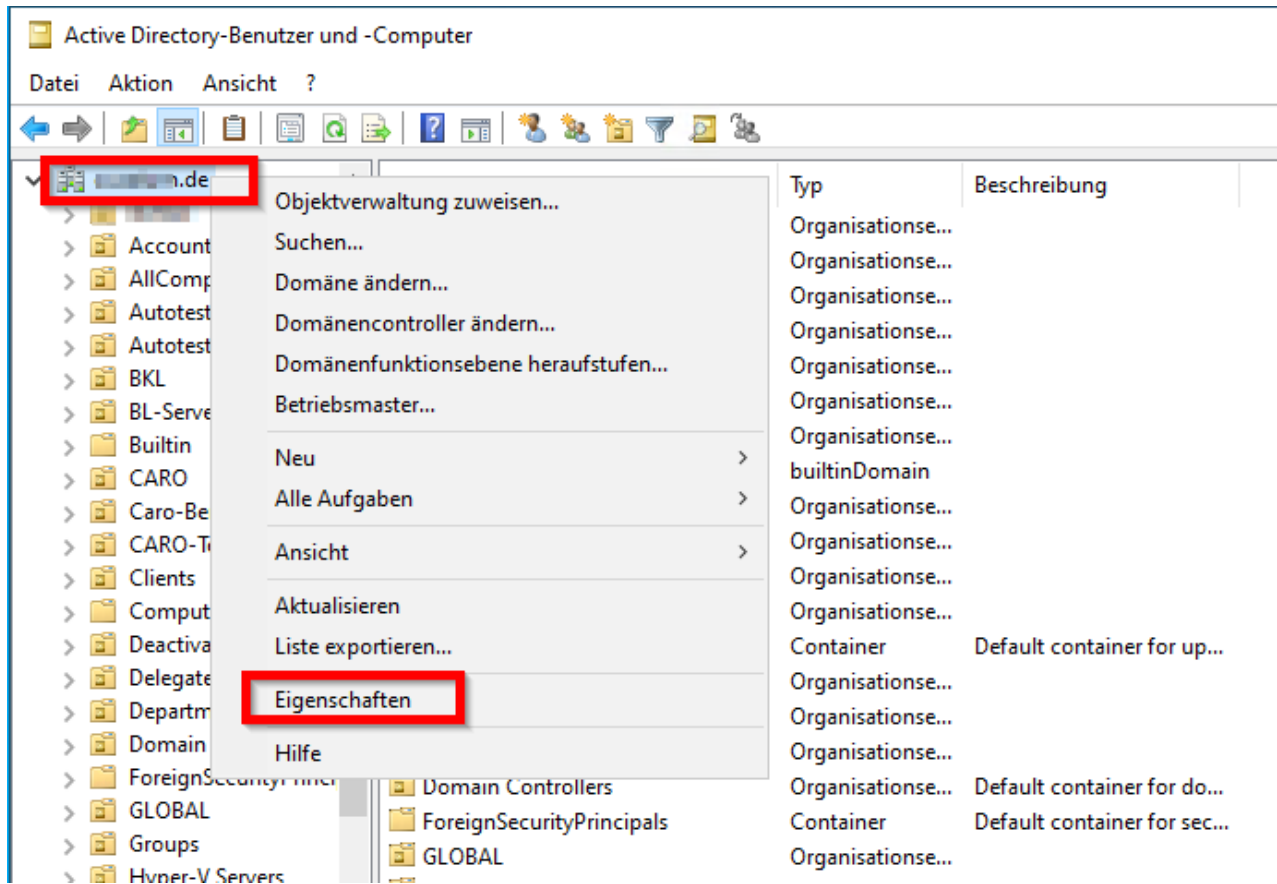
dsa.msc – Menü „Ansicht“ → „Erweiterte Features“ mit Häkchen aktiviert

Dieser Schritt ist wichtig – ohne ihn sind die Sicherheits- und Überwachungsdetails nicht sichtbar.

Schritt 3 – Domain-Objekt öffnen

Suchen Sie im linken Navigationsbaum Ihre **Domäne** (z. B. firma.local).

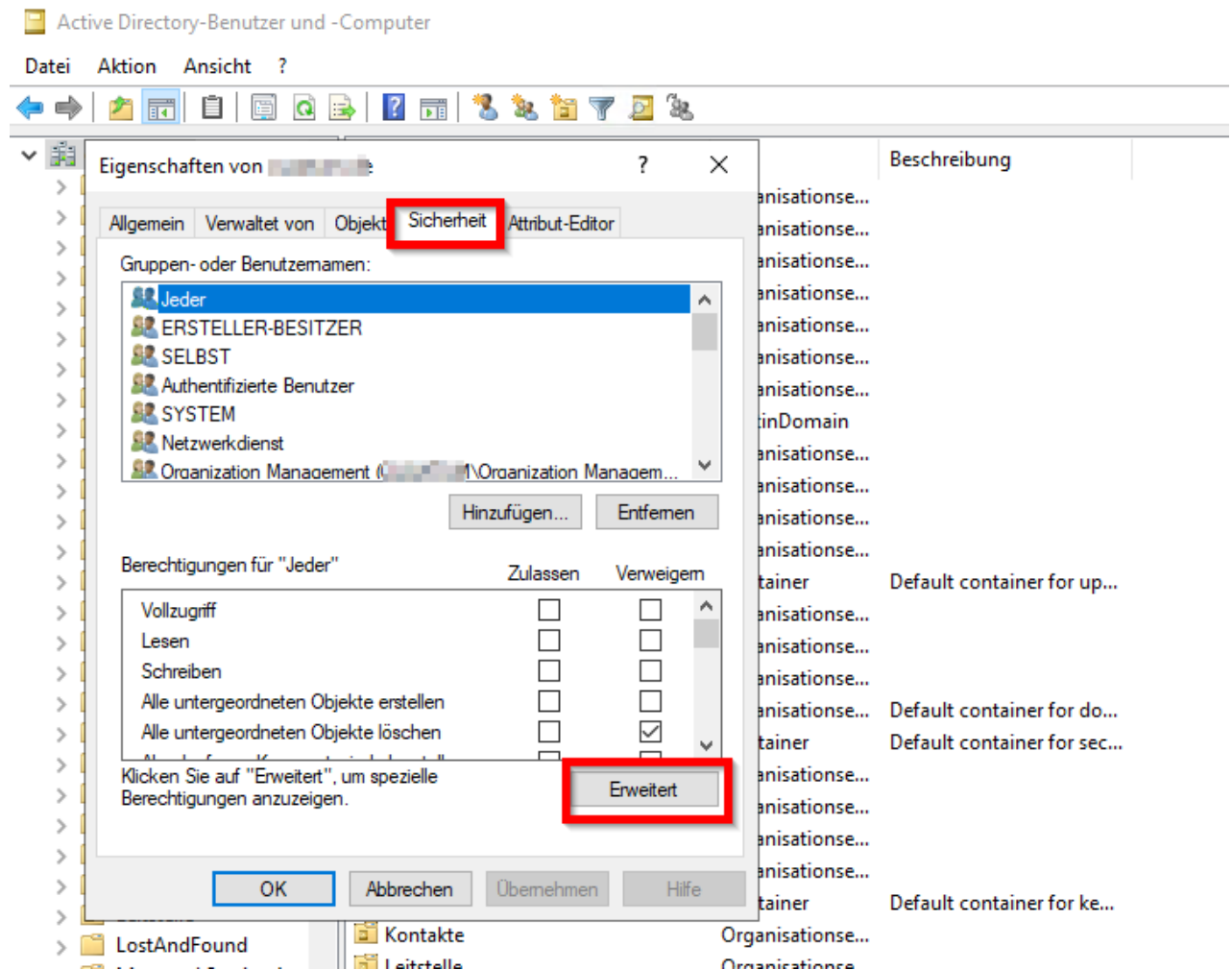
Rechtsklick auf die Domäne → **Eigenschaften**.



dsa.msc – Rechtsklick auf die Domäne → „Eigenschaften“

Schritt 4 – Sicherheitseinstellungen aufrufen

Im Eigenschaften-Fenster klicken Sie auf den Reiter **Sicherheit** → dann auf die Schaltfläche **Erweitert**.



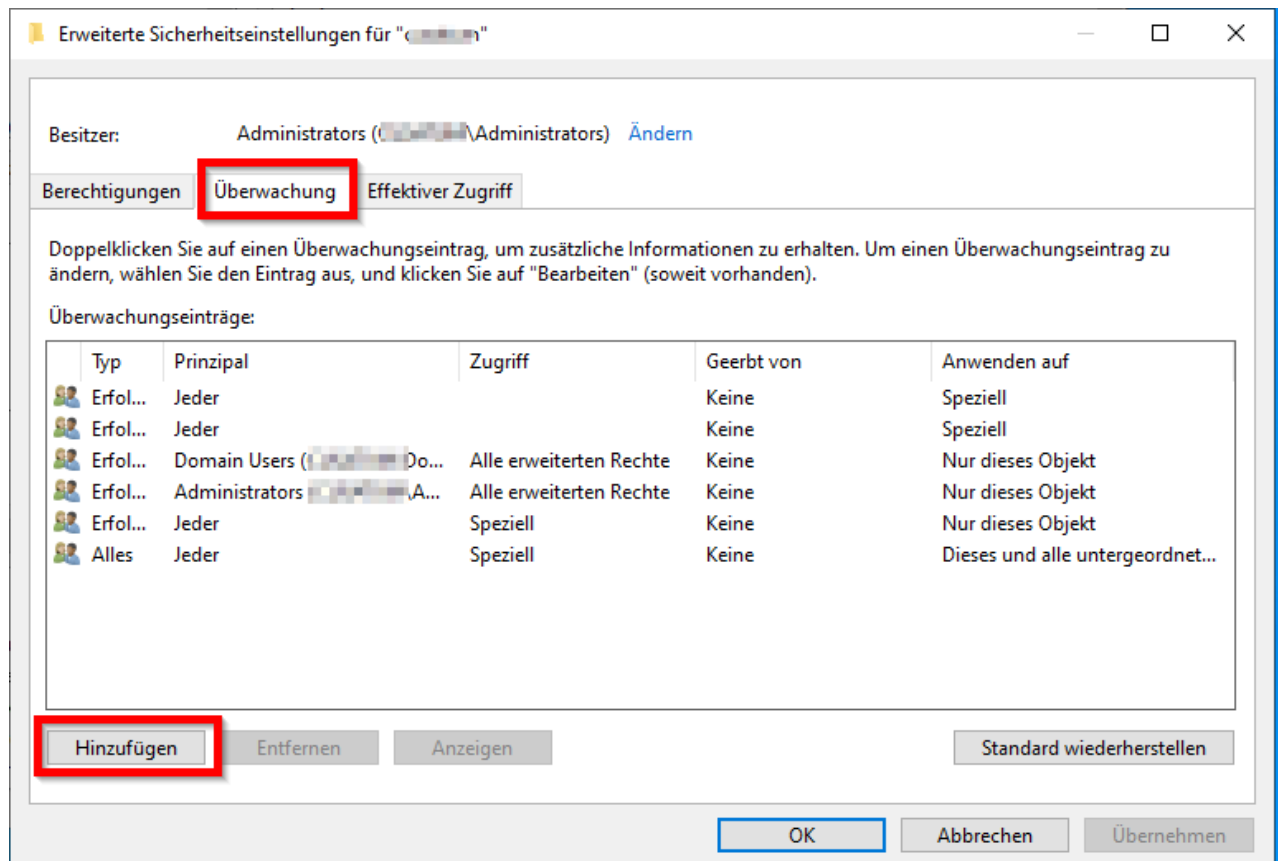
Domänen-Eigenschaften – Reiter „Sicherheit“, Schaltfläche „Erweitert“

Schritt 5 – Überwachungs-Tab öffnen und Eintrag hinzufügen

Im Fenster „Erweiterte Sicherheitseinstellungen“ wechseln Sie auf den Reiter **Überwachung** und klicken Sie auf **Hinzufügen**.

Prüfen Sie, ob ein Eintrag für den Sicherheitsprinzipal **Jeder** bereits vorhanden ist.

- Falls **ja**: Öffnen Sie den Eintrag und überprüfen Sie, ob die unten aufgeführten Berechtigungen alle gesetzt sind.
- Falls **nein**: Klicken Sie auf **Hinzufügen**, dann auf **Prinzipal auswählen** und geben Sie Jeder (auf englischsprachigen Systemen Everyone) ein.



Erweiterte Sicherheitseinstellungen –
Reiter „Überwachung“ mit vorhandenen Einträgen und Schaltfläche „Hinzufügen“

Schritt 6 – Mindestberechtigungen für die SACL setzen

Stellen Sie sicher, dass der Eintrag folgende Mindesteinstellungen hat:

Einstellung	Wert
Sicherheitsprinzipal	Jeder
Typ	Zulassen
Anwenden auf	Dieses und alle untergeordneten Objekte

Folgende Berechtigungen müssen aktiviert sein:

- ☒ Alle Eigenschaften schreiben
- ☒ Löschen
- ☒ Unterstruktur löschen
- ☒ Berechtigungen ändern
- ☒ Alle untergeordneten Objekte erstellen
- ☒ Alle untergeordneten Objekte löschen



Berechtigungseintrag für "cusatum"

Prinzipal: Jeder [Prinzipal auswählen](#)

Typ: Zulassen

Anwenden auf: Dieses und alle untergeordneten Objekte

Berechtigungen:

☐ Vollzugriff	☒ "msExchOmaCarrier"-Objekte löschen
☐ Inhalt auflisten	☒ "msExchOmaConfigurationContainer"-Objekte erstellen
☐ Alle Eigenschaften lesen	☒ "msExchOmaConfigurationContainer"-Objekte löschen
☒ Alle Eigenschaften schreiben	☒ "msExchOmaContainer"-Objekte erstellen
☒ Löschen	☒ "msExchOmaContainer"-Objekte löschen
☒ Unterstruktur löschen	☒ "msExchOmaDataSource"-Objekte erstellen
☐ Berechtigungen lesen	☒ "msExchOmaDataSource"-Objekte löschen
☒ Berechtigungen ändern	☒ "msExchOmaDeliveryProvider"-Objekte erstellen
☐ Besitzer ändern	☒ "msExchOmaDeliveryProvider"-Objekte löschen
☐ Alle bestätigten Schreibvorgänge	☒ "msExchOmaDeviceCapability"-Objekte erstellen
☐ Alle erweiterten Rechte	☒ "msExchOmaDeviceCapability"-Objekte löschen
☒ Alle untergeordneten Objekte erstellen	☒ "msExchOmaDeviceType"-Objekte erstellen
☒ Alle untergeordneten Objekte löschen	☒ "msExchOmaDeviceType"-Objekte löschen
☒ "Benutzer"-Objekte erstellen	☒ "msExchOrganizationContainer"-Objekte erstellen
☒ "Benutzer"-Objekte löschen	☒ "msExchOrganizationContainer"-Objekte löschen

OK Abbrechen

SACL-Berechtigungseintrag für „Jeder“ – alle erforderlichen Berechtigungen aktiviert

Hinweis: Aktivieren Sie nur die oben aufgelisteten sechs Berechtigungen. Berechtigungen wie „Vollzugriff“, „Berechtigungen lesen“ oder „Besitzer ändern“ sind **nicht** erforderlich. Klicken Sie auf **OK** und schließen Sie alle Fenster mit **Übernehmen** → **OK**.

Windows-Firewall konfigurieren

Warum ist das notwendig?

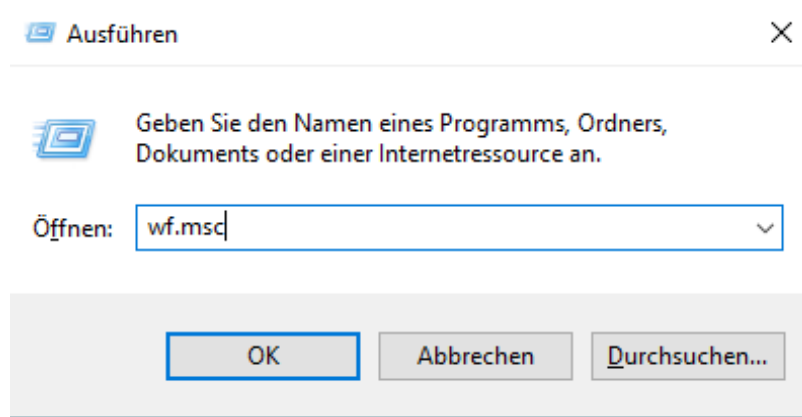
Der CARO AD-Observer liest die Sicherheitsereignisse der Domänencontroller über das Netzwerk (remote) aus. Die Windows-Firewall blockiert diesen Zugriff standardmäßig. Sie müssen daher gezielt drei Firewall-Regeln aktivieren.

Hinweis: Diese Konfiguration muss auf **jedem** Domänencontroller durchgeführt werden, den Sie überwachen möchten.

Schritt-für-Schritt-Anleitung

Schritt 1 – Windows-Firewall mit erweiterter Sicherheit öffnen

Drücken Sie Windows + R, geben Sie ein und bestätigen Sie mit Enter:
wf.msc



Ausführen-Dialog mit wf.msc

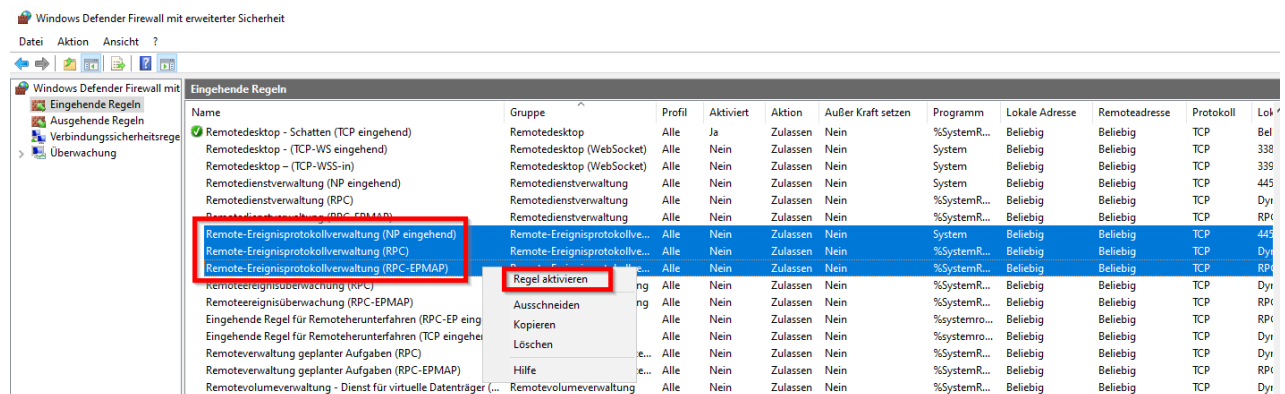
Schritt 2 – Eingehende Regeln anzeigen

Klicken Sie im linken Navigationsbereich auf **Eingehende Regeln**.

Schritt 3 – Drei Regeln aktivieren

Suchen Sie die folgenden vordefinierten Regeln. Markieren Sie alle drei gleichzeitig (mit Strg + Klick) und wählen Sie Rechtsklick → **Regel aktivieren**:

Regelname	Beschreibung
Remote-Ereignisprotokollverwaltung (NP eingehend)	Zugriff über Named Pipes (SMB)
Remote-Ereignisprotokollverwaltung (RPC)	Zugriff über RPC-Verbindung
Remote-Ereignisprotokollverwaltung (RPC-EPMAP)	RPC-Endpunktzuordnung



wf.msc – drei Remote-Ereignisprotokollverwaltungs-Regeln markiert,
Rechtsklick → „Regel aktivieren“

Hinweis: Wenn Sie die Firewall per Gruppenrichtlinie verwalten, können Sie diese drei Regeln auch zentral für alle Domänencontroller aktivieren.

Einstellungen überprüfen

Audit-Richtlinien prüfen

Öffnen Sie auf einem Domänencontroller die Eingabeaufforderung als Administrator und führen Sie aus:
auditpol /get /category:*

In der Ausgabe sollten für die folgenden Kategorien mindestens **Erfolg** angezeigt werden:

- **Kontoverwaltung** – alle Unterkategorien
- **DS-Zugriff** → Verzeichnisdienständerungen



- **DS-Zugriff** → Verzeichnisdienstzugriff
- **Richtlinienänderungen** → Überwachungsrichtlinienänderung überwachen

Eingabeaufforderung

```
C:\Users\...>auditpol /get /category:*
```

Kategorie/Unterkategorie	Einstellung
System	
Sicherheitssystemerweiterung	Keine Überwachung
Systemintegrität	Keine Überwachung
IPSEC-Treiber	Keine Überwachung
Andere Systemereignisse	Keine Überwachung
Sicherheitsstatusänderung	Keine Überwachung
An-/Abmeldung	
Anmelden	Keine Überwachung
Abmelden	Keine Überwachung
Kontosperrung	Keine Überwachung
IPsec-Hauptmodus	Keine Überwachung
IPsec-Schnellmodus	Keine Überwachung
IPsec-Erweiterungsmodus	Keine Überwachung
Spezielle Anmeldung	Keine Überwachung
Andere Anmelde-/Abmeldeereignisse	Keine Überwachung
Netzwerkrichtlinienserver	Keine Überwachung
Benutzer-/Geräteansprüche	Keine Überwachung
Gruppenmitgliedschaft	Keine Überwachung
Zugriffsrechte	Keine Überwachung
Objektzugriff	
Dateisystem	Keine Überwachung
Registrierung	Keine Überwachung
Kernelobjekt	Keine Überwachung
SAM	Keine Überwachung
Zertifizierungsdienste	Keine Überwachung
Anwendung wurde generiert.	Keine Überwachung
Handleänderung	Keine Überwachung
Dateifreigabe	Keine Überwachung
Filterplattform: Verworfen Pakete	Keine Überwachung
Filterplattformverbindung	Keine Überwachung
Andere Objektzugriffseignisse	Keine Überwachung
Detaillierte Dateifreigabe	Keine Überwachung
Wechselmedien	Keine Überwachung
Staging zentraler Richtlinien	Keine Überwachung
Berechtigungen	
Nicht sensible Verwendung von Rechten	Keine Überwachung
Andere Rechteverwendungsereignisse	Keine Überwachung
Sensible Verwendung von Rechten	Keine Überwachung
Detaillierte Nachverfolgung	
Prozesserstellung	Keine Überwachung
Prozessbeendigung	Keine Überwachung
DPAPI-Aktivität	Keine Überwachung
RPC-Ereignisse	Keine Überwachung
Plug & Play-Ereignisse	Keine Überwachung
Ereignisse zu angepassten Tokenrechten	Keine Überwachung
Richtlinienänderung	
Richtlinienänderungen überwachen	Erfolg
Authentifizierungsrichtlinienänderung	Keine Überwachung
Autorisierungsrichtlinienänderung	Keine Überwachung
MPSSVC-Richtlinienänderung auf Regelebene	Keine Überwachung
Filterplattform-Richtlinienänderung	Keine Überwachung
Andere Richtlinienänderungsereignisse	Keine Überwachung
Kontenverwaltung	
Computerkontoverwaltung	Erfolg
Sicherheitsgruppenverwaltung	Erfolg
Verteilerguppenverwaltung	Erfolg
Anwendungsgruppenverwaltung	Erfolg
Andere Kontoverwaltungsereignisse	Erfolg
Benutzerkontenverwaltung	Erfolg
DS-Zugriff	
Verzeichnisdienstzugriff	Erfolg
Verzeichnisdienständerungen	Erfolg
Verzeichnisdienstreplikation	Keine Überwachung
Detaillierte Verzeichnisdienstreplikation	Keine Überwachung
Kontoanmeldung	
Ticketvorgänge des Kerberos-Diensts	Keine Überwachung
Andere Kontoanmeldungsereignisse	Keine Überwachung
Kerberos-Authentifizierungsdienst	Keine Überwachung
Überprüfung der Anmeldeinformationen	Keine Überwachung

Eingabeaufforderung – Ausgabe von auditpol /get /category:*

mit „Erfolg“ für die relevanten Kategorien



SACL prüfen

Öffnen Sie erneut dsa.msc, navigieren Sie zur Domäne → Eigenschaften → Sicherheit → Erweitert → Überwachung und überprüfen Sie, ob der Eintrag für **Jeder** mit den oben beschriebenen Berechtigungen vorhanden ist.

Firewall prüfen

Öffnen Sie wf.msc auf dem Domänencontroller und prüfen Sie, ob die drei Regeln **Remote-Ereignisprotokollverwaltung** im Abschnitt **Eingehende Regeln** den Status **Aktiviert** haben (erkennbar am grünen Symbol in der Spalte).

Schnell-Checkliste

Nutzen Sie diese Checkliste, um sicherzustellen, dass alle Voraussetzungen erfüllt sind:

- ☐ Domänencontroller laufen auf Windows Server 2019 oder neuer (empfohlen)
- ☐ Berechtigung für Auslesen des Security Event Logs vorhanden
- ☐ GPO CARO-AD-Observer-Audit erstellt und mit OU „Domain Controllers“ verknüpft
- ☐ Sicherheitsoption „Unterkategorien erzwingen“ aktiviert (Schritt 4 – vor allen anderen Audit-Einstellungen!)
- ☐ Kontoverwaltung: alle Unterkategorien auf „Alle Erfolge“ gesetzt
- ☐ DS-Zugriff: Verzeichnisdienständerungen auf „Erfolg“ gesetzt
- ☐ DS-Zugriff: Verzeichnisdienstzugriff auf „Erfolg“ gesetzt
- ☐ Richtlinienänderung: Überwachungsrichtlinienänderung auf „Erfolg“ gesetzt
- ☐ gpupdate /force auf allen Domänencontrollern ausgeführt
- ☐ Audit-Richtlinien mit auditpol /get /category:* verifiziert
- ☐ Maximale Protokollgröße in eventvwr.msc auf mindestens 128 MB gesetzt
- ☐ SACL auf dem Domain-Objekt gesetzt (Jeder / Zulassen / Dieses und alle untergeordneten Objekte)
- ☐ Windows-Firewall: alle drei Remote-Ereignisprotokoll-Regeln aktiviert
- ☐ Firewall-Konfiguration auf **jedem** zu überwachenden Domänencontroller geprüft