Implementieren rollenbasierter Dateizugriffskontrollen in Microsoft Active Directory

Die Macht verschachtelter Gruppen

Abstract

Diese Arbeit untersucht die Implementierung der rollenbasierten Dateizugriffskontrolle (Role-Based File Access, RBFA) im Active Directory-Umfeld.

Das Ziel dieser Arbeit ist es, die Bedeutung von RBFA zu betonen und die Vorteile einer Integration in das Active Directory zu erläutern. Durch die Verwendung von Rollen, die den Zugriff auf Dateien basierend auf den zugewiesenen Berechtigungen steuern, kann RBFA die Sicherheit erhöhen und die Verwaltung von Dateizugriffen vereinfachen.

Der Fokus liegt auf den technischen Aspekten der Implementierung, einschließlich der Konfiguration von Sicherheitsgruppen, Berechtigungen und Richtlinien innerhalb des Active Directory. Darüber hinaus werden Risiko- und Erfolgsfaktoren diskutiert, die bei der Umsetzung von RBFA auftreten können.

Diese Arbeit bietet einen Einblick in die Bedeutung von RBFA für die Sicherheit und Effizienz der Dateiverwaltung in Unternehmen und gibt praktische Empfehlungen für die erfolgreiche Implementierung im Active Directory-Umfeld.

Inhaltsverzeichnis

Kapitel 1 Einleitung

1.1 Hintergrund und Motivation

In der heutigen digitalen Ära sind Unternehmen zunehmend darauf angewiesen, ihre sensiblen Daten effektiv zu schützen und einen effizienten Zugriff für autorisierte Benutzer zu ermöglichen. Angesichts der steigenden Bedrohungen durch Cyberangriffe ist es von entscheidender Bedeutung, die Datensicherheit zu gewährleisten und gleichzeitig sicherzustellen, dass autorisierte Benutzer schnell und gezielt auf die benötigten Daten zugreifen können.

Die vorliegende Arbeit entspringt der Notwendigkeit, Unternehmen bei der Implementierung von Role Based File Access (RBFA) zu unterstützen, um diesen Anforderungen gerecht zu werden. Angesichts der ständig wachsenden Herausforderungen im Bereich der Datensicherheit ist RBFA eine bewährte Methode, um den Zugriff auf sensible Daten zu kontrollieren und zu schützen. Durch die Implementierung von RBFA können Unternehmen sicherstellen, dass nur autorisierte Benutzer Zugriff auf bestimmte Dateien haben, während gleichzeitig die Effizienz des Zugriffsprozesses verbessert wird. Die klassischen Zugriffsmethoden, die oft auf der Vergabe von Berechtigungen basieren, die direkt an Benutzer oder Gruppen gebunden sind, stoßen zunehmend an ihre Grenzen. Diese Methoden erfordern häufig eine manuelle Verwaltung und Aktualisierung von Zugriffsrechten, was zu Ineffizienzen, Fehlern und Sicherheitslücken führen kann. RBFA bietet eine alternative und fortschrittliche Methode zur Steuerung des Dateizugriffs, indem es Berechtigungen basierend auf den spezifischen Rollen und Verantwortlichkeiten der Benutzer festlegt.

Das Ziel dieser Arbeit ist es, Unternehmen eine praktische Implementierungshilfe für RBFA bereitzustellen. Dabei sollen die RBFA-Prinzipien vermittelt und anhand konkreter Beispiele illustriert werden. Diese Implementierungshilfe soll Unternehmen dazu befähigen, RBFA in ihren eigenen Arbeitsabläufen erfolgreich einzusetzen und die klassischen Zugriffsmethoden zu überwinden. Darüber hinaus zielt die Arbeit darauf ab, das Verständnis für RBFA zu vertiefen und die Bedeutung

dieses Zugriffskontrollmechanismus für die Sicherheit sensibler Daten zu verdeutlichen.

Zusätzlich beleuchtet diese Arbeit auch die Projektrisiken und Erfolgsfaktoren im Zusammenhang mit der RBFA-Implementierung. Es werden die potenziellen Risiken und Herausforderungen beschrieben sowie Strategien zur Risikominimierung und Erfolgsoptimierung vorgestellt. Dadurch soll ein ganzheitlicher Einblick in die RBFA-Implementierung gewährleistet werden, der es Unternehmen ermöglicht, sowohl die technischen als auch die organisatorischen Aspekte dieser Technologie zu berücksichtigen.

Insgesamt strebt diese Arbeit danach, einen Beitrag zur Verbesserung der Datensicherheit in Unternehmen zu leisten und ihnen die notwendigen Instrumente an die Hand zu geben, um ihre Dateiverwaltung sicherer und effizienter zu gestalten.

1.2 Aufbau der Arbeit

Dieser Praktikumsbericht gliedert sich in mehrere Abschnitte, die einen umfassenden Einblick in die Implementierung der rollenbasierten Dateizugriffskontrolle (RBFA) im Active Directory bieten. Zunächst werden in der Einleitung der Hintergrund und die Motivation für die Durchführung des Berichts erläutert.

Im zweiten Abschnitt werden in den Grundlagen die wesentlichen Konzepte der Zugriffskontrolle vorgestellt. Hierbei wird verdeutlicht, warum herkömmliche Zugriffskontrollmethoden oft an ihre Grenzen stoßen und welche Probleme damit einhergehen.

Im darauffolgenden Kapitel werden die potenziellen Risiken und Erfolgsfaktoren im Zusammenhang mit der RBFA-Implementierung analysiert. Es werden die identifizierten Risiken und Herausforderungen beschrieben sowie Strategien zur Risikominimierung und Erfolgsoptimierung vorgestellt. Dabei wird aufgezeigt, wie mit den Risiken und Erfolgsfaktoren in der Praxis umgegangen wurde und welche Maßnahmen ergriffen wurden, um diese zu bewältigen.

In Kapitel 4 und 5 wird ein praxisnahes Szenario vorgestellt, in dem RBFA-Prinzipien angewendet werden. Anhand einer kleinen fiktiven Firma wird das

RBFA-Konzept umgesetzt, wobei die AGDLP-Methode (Account, Global Group, Domain Local group, Permissions) zur Anwendung kommt. Es werden die technischen Schritte und organisatorischen Maßnahmen zur Implementierung von RBFA in der Firmenumgebung beschrieben und aufgezeigt, wie RBFA in der Praxis umgesetzt werden kann.

Im sechsten Abschnitt werden die Lessons learned für zukünftige RBFA-Projekte abgeleitet. Dabei wird aufgezeigt, welche Erkenntnisse aus der Praxis gewonnen wurden und wie diese für zukünftige Projekte genutzt werden können.

Der Anhang enthält die komplette Installationsanleitung für das verwendete Active Directory

Kapitel 2 Grundlagen

2.1 Informationssicherheit und die Rolle von RBFA (least privilege)

Informationssicherheit bezeichnet den Prozess, sensible Daten vor unbefugtem Zugriff, Manipulation oder Diebstahl zu schützen. Ein grundlegendes Prinzip der Informationssicherheit ist das Prinzip des "Least Privilege" oder "Minimalen Zugriffsrechts". Dieses Prinzip besagt, dass Benutzer nur die Zugriffsrechte erhalten sollten, die für die Erfüllung ihrer Aufgaben unbedingt erforderlich sind. Durch die Anwendung des Least Privilege-Prinzips wird das Risiko von Datenschutzverletzungen und unbefugtem Zugriff erheblich verringert.

Traditionelle Zugriffskontrollmethoden vergeben Zugriffsrechte häufig auf der Grundlage von Benutzeridentitäten oder Gruppenmitgliedschaften. Diese Methode kann jedoch zu Problemen führen, da es oft schwierig ist, die Zugriffsrechte fein abzustimmen, um das Least Privilege-Prinzip zu erfüllen. Dies kann zu einer Übervergabe von Berechtigungen führen, bei der Benutzer mehr Zugriffsrechte erhalten, als für ihre jeweiligen Aufgaben notwendig sind. Dadurch entsteht ein erhöhtes Risiko von Sicherheitsverletzungen und Datenlecks.

Die rollenbasierte Dateizugriffskontrolle (RBFA) bietet eine effektive Lösung für diese Probleme. RBFA bindet Zugriffsrechte an vordefinierte Rollen, die spezifische Aufgaben oder Verantwortlichkeiten innerhalb der Organisation repräsentieren. Jedem Benutzer wird dann eine oder mehrere Rollen zugewiesen, wodurch ihm automatisch die entsprechenden Zugriffsrechte für seine Rolle gewährt werden.

Der Einsatz von RBFA ermöglicht eine präzisere und effektivere Steuerung des Dateizugriffs. Indem die Zugriffsrechte an Rollen gebunden sind, wird sichergestellt, dass Benutzer nur auf diejenigen Ressourcen zugreifen können, die für ihre jeweiligen Aufgaben erforderlich sind. Dies minimiert das Risiko von Datenschutzverletzungen und unbefugtem Zugriff erheblich und trägt zur Erfüllung von Compliance-Anforderungen bei.

Zusätzlich bietet RBFA eine effizientere Verwaltung von Zugriffsrechten. Da Rollen zentral definiert und verwaltet werden, ist es einfacher, Zugriffsrechte für neue Benutzer hinzuzufügen oder bestehende Zugriffsrechte zu aktualisieren. Dies trägt dazu bei, die Verwaltungskosten zu senken und die Effizienz der IT-Abteilung zu steigern.

Insgesamt ermöglicht RBFA eine präzisere Kontrolle des Dateizugriffs, indem es das Least Privilege-Prinzip unterstützt und gleichzeitig die Verwaltung von Zugriffsrechten vereinfacht. Im folgenden Abschnitt werden die Konzepte und Vorteile von RBFA genauer erläutert.

2.2 Konzept von RBFA

Im Gegensatz zu herkömmlichen Zugriffskontrollmethoden, die auf der direkten Zuweisung von Berechtigungen an Benutzer oder Gruppen beruhen, bindet RBFA-Zugriffsrechte an vordefinierte Rollen, die bestimmte Aufgaben oder Verantwortlichkeiten in der Organisation repräsentieren. Diese Rollen definieren, welche Aktionen ein Benutzer ausführen darf und welche Ressourcen er verwenden kann.

2.2.1 Grundprinzipien von RBFA:

- ✓ **Zuweisung von Rollen:** Benutzer werden einzelnen Rollen zugeordnet, je nach ihren Aufgaben und Verantwortlichkeiten innerhalb der Organisation. Ein Benutzer kann einer oder mehreren Rollen zugewiesen werden, abhängig von seinem Tätigkeitsbereich. Durch die Zuweisung von Rollen erhalten Benutzer automatisch die entsprechenden Zugriffsrechte für die in ihrer Rolle definierten Ressourcen.
- ✓ **Definition von Zugriffsrechten:** Jede Rolle definiert die Zugriffsrechte auf Dateien und Ressourcen, die für die Ausführung der damit verbundenen Aufgaben erforderlich sind. Dies umfasst Berechtigungen wie Lesen, Schreiben, Ausführen oder Löschen von Dateien sowie den Zugriff auf bestimmte Verzeichnisse oder Netzwerkfreigaben.
- ✓ **Dynamische Verwaltung:** RBFA ermöglicht eine dynamische Verwaltung von Rollen und Zugriffsrechten. Rollen können je nach Bedarf aktualisiert, erweitert oder eingeschränkt werden, um Änderungen in der

Organisationsstruktur oder den Zugriffsanforderungen zu berücksichtigen. Dies erleichtert die Anpassung an sich ändernde Geschäftsanforderungen und verbessert die Agilität der Organisation.

2.2.2 Vorteile von RBFA:

- ✓ **Verbesserte Sicherheit:** RBFA trägt dazu bei, die Sicherheit sensibler Informationen zu verbessern, indem es den Zugriff auf Dateien und Ressourcen auf diejenigen Benutzer beschränkt, die spezifische Rollen und Aufgaben in der Organisation haben. Durch die Implementierung des Prinzips des Least Privilege werden potenzielle Angriffsvektoren minimiert und das Risiko von Datenschutzverletzungen reduziert.
- ✓ **Effiziente Verwaltung:** Die zentrale Verwaltung von Rollen und Zugriffsrechten erleichtert die Administration von Zugriffsrechten erheblich. Neue Benutzer können schnell und einfach den entsprechenden Rollen zugewiesen werden, während sich Organisationsstrukturen ändern oder neue Zugriffsanforderungen entstehen.
- ✓ **Bessere Compliance:** RBFA unterstützt die Einhaltung von Compliance-Anforderungen, indem es eine transparente und nachvollziehbare Verwaltung von Zugriffsrechten ermöglicht. Durch die Definition klarer Zugriffsrichtlinien und die Protokollierung von Zugriffsaktivitäten können Unternehmen die Anforderungen an Datenschutz und Datensicherheit besser erfüllen.
- ✓ **Flexibilität und Skalierbarkeit:** RBFA ist flexibel und skalierbar und kann an die individuellen Anforderungen und Wachstumsbedürfnisse einer Organisation angepasst werden. Neue Rollen können einfach erstellt und bestehende Rollen angepasst werden, um neuen Geschäftsanforderungen gerecht zu werden.

2.3 RBFA und AGDLP im Fokus

AGDLP (Accounts, Global Groups, Domain Local Groups, Permissions) und RBFA (Role Based File Access) sind zwei wesentliche Konzepte im Bereich der Zugriffskontrolle und Ressourcenverwaltung, insbesondere im Kontext von Active Directory (AD). Oftmals werden sie verwechselt oder sogar als austauschbar

angesehen, jedoch handelt es sich um zwei eigenständige Konzepte, die verschiedene Ansätze zur Steuerung des Dateizugriffs bieten.

AGDLP ist ein Modell, das darauf abzielt, die Organisation von Benutzerkonten und Gruppen in Active Directory (AD) zu strukturieren. Es legt eine hierarchische Struktur fest, in der Benutzerkonten in globalen Gruppen organisiert sind, diese globalen Gruppen wiederum in Domänenlokalgruppen eingebettet sind und schließlich Domänenlokalgruppen in Datei- oder Ordnerberechtigungen verwendet werden. AGDLP bietet eine klare Struktur für die Verwaltung von Berechtigungen und ermöglicht eine effiziente Zugriffskontrolle in AD-Umgebungen.

RBFA hingegen basiert auf der Zuweisung von Berechtigungen basierend auf den Rollen und Verantwortlichkeiten der Benutzer innerhalb einer Organisation. Es legt fest, dass Berechtigungen an bestimmte Rollen oder Gruppen von Benutzern zugewiesen werden, anstatt sie direkt an individuelle Benutzerkonten zu binden. RBFA ermöglicht eine flexible und granulare Steuerung des Dateizugriffs, da Berechtigungen auf der Grundlage vordefinierter Rollen oder Funktionen innerhalb der Organisation vergeben werden.

Obwohl AGDLP und RBFA unterschiedliche Ansätze zur Zugriffskontrolle bieten, ergänzen sie sich in der Praxis oft gegenseitig. Während AGDLP eine Struktur für die Organisation von Benutzern und Gruppen bereitstellt, bietet RBFA eine Methode zur Zuweisung von Berechtigungen basierend auf den Rollen und Verantwortlichkeiten innerhalb dieser Struktur. Durch die Kombination beider Konzepte können Organisationen eine effektive Zugriffskontrolle implementieren, die den Anforderungen ihrer IT-Infrastruktur gerecht wird. Es ist wichtig, die Unterschiede und Synergien zwischen AGDLP und RBFA zu verstehen, um eine effektive und sichere Ressourcenverwaltung in Active Directory-Umgebungen zu gewährleisten.

Kapitel 3 Projekterfolgs- und Projektrisikofaktoren

Die Einführung eines Zugriffsmodells für rollenbasierten Dateizugriff ist ein entscheidender Schritt für Unternehmen, um die Sicherheit ihrer digitalen Ressourcen zu gewährleisten und die Datenzugriffsverwaltung zu optimieren. Dabei spielen sowohl Erfolgsfaktoren als auch Risiken eine maßgebliche Rolle.

Dieses Kapitel beleuchtet die entscheidenden Faktoren, die den Erfolg oder Misserfolg bei der Implementierung eines Zugriffsmodells beeinflussen können. Es beleuchtet nicht nur die Schlüsselfaktoren, die eine reibungslose Einführung unterstützen, sondern identifiziert auch potenzielle Risiken, die es zu berücksichtigen gilt.

Durch eine Analyse der Erfolgs- und Risikofaktoren können Organisationen fundierte Entscheidungen treffen und geeignete Maßnahmen ergreifen, um die Wirksamkeit und Sicherheit ihres Zugriffssystems zu gewährleisten. In den folgenden Abschnitten werden diese Faktoren eingehend untersucht, um Einblicke in die Komplexität und Herausforderungen der Einführung eines klassischen Zugriffsmodells für rollenbasierten Dateizugriff zu bieten.

3.1 Projekterfolgsfaktoren

3.1.1 Unterstützung durch das Management:

Die Unterstützung des Managements ist entscheidend für den Erfolg der Einführung eines neuen Zugriffsmodells. Durch die Bereitstellung von Ressourcen und die Beseitigung von Hindernissen können das Projektteam unterstützt und die erforderlichen Maßnahmen ergriffen werden, um das Projekt erfolgreich abzuschließen.

Eine klare Führung und Unterstützung seitens des Managements fördern das Engagement der Mitarbeiter und tragen dazu bei, die Ziele des Projekts zu erreichen. Die Unterstützung des Managements ist ein entscheidender Erfolgsfaktor und kann dazu beitragen, potenzielle Probleme zu lösen und das Projekt auf Kurs zu halten.

3.1.2 Klare Anforderungsdefinition:

Die klare Definition der Anforderungen bildet das Fundament für die erfolgreiche Einführung eines klassischen Zugriffsmodells für rollenbasierten Dateizugriff. Ein gründliches Verständnis der organisatorischen Struktur, der Geschäftsprozesse und der Benutzerbedürfnisse ist unerlässlich. Begonnen wird mit der Identifizierung aller beteiligten Parteien, einschließlich der Benutzergruppen und ihrer jeweiligen Rollen. Dies kann durch Interviews, Umfragen und Workshops erreicht werden, um ein umfassendes Bild von den Arbeitsabläufen und den benötigten Zugriffsrechten zu erhalten.

Nachdem die Benutzerrollen identifiziert wurden, ist es wichtig, die spezifischen Zugriffsanforderungen jeder Rolle zu ermitteln. Dies umfasst sowohl die Berechtigungen zum Lesen als auch zum Schreiben von Dateien sowie etwaige Einschränkungen oder Ausnahmen. Sicherheitsrichtlinien sollten ebenfalls definiert werden, um sicherzustellen, dass der Zugriff auf sensible Daten gemäß den geltenden Vorschriften und Richtlinien erfolgt.

Es ist von entscheidender Bedeutung, dass das Zugriffsmodell flexibel genug ist, um zukünftige Entwicklungen und Anpassungen zu berücksichtigen, ohne dabei die Integrität der Sicherheitsrichtlinien zu beeinträchtigen. Eine klare Anforderungsdefinition schafft Klarheit und sorgt dafür, dass das Zugriffsmodell den Bedürfnissen der Organisation entspricht.

3.1.3 Gute Planung und Design:

Eine gründliche Planung und ein sorgfältiges Design sind von entscheidender Bedeutung für die erfolgreiche Einführung eines effektiven Zugriffsmodells. Dieser Prozess beginnt mit der Erstellung einer detaillierten Projektplanung, die die verschiedenen Phasen des Projekts sowie die zu erledigenden Aufgaben und Meilensteine umfasst.

Bei der Strukturierung von Benutzerrollen ist es wichtig, Hauptrollen und Unterrollen zu identifizieren und die Zugriffsrechte für jede Rolle klar zu definieren. Die Definition von Zugriffsrechten ist ebenfalls ein wesentlicher Bestandteil des Designs und umfasst die Festlegung, welche Benutzer auf welche

Dateien zugreifen können sowie die Art und Weise, wie Zugriffsrechte gewährt, widerrufen oder eingeschränkt werden können.

Sicherheitsrichtlinien sollten im Designprozess berücksichtigt werden, um sicherzustellen, dass das Zugriffsmodell den geltenden Gesetzen, Branchenstandards und internen Richtlinien entspricht. Eine gründliche Planung und ein sorgfältiges Design legen den Grundstein für den Erfolg des Projekts und gewährleisten, dass das Zugriffsmodell den Anforderungen der Organisation gerecht wird.

3.1.4 Gerichtete und effektive Kommunikation:

Effektive Kommunikation ist entscheidend für den Erfolg der Einführung eines neuen Zugriffsmodells. Klare und regelmäßige Kommunikation fördert das Verständnis und die Akzeptanz der Benutzer und ermöglicht es, Bedenken oder Fragen rechtzeitig anzusprechen.

Durch eine offene und transparente Kommunikation können potenzielle Hindernisse überwunden und das Engagement der Mitarbeiter für das Projekt gestärkt werden. Es ist wichtig, dass die Kommunikation Feedback von den Benutzern einholt und darauf reagiert, um sicherzustellen, dass ihre Bedürfnisse und Anliegen angemessen berücksichtigt werden.

3.1.5 Überwachung und kontinuierliche Verbesserung:

Die Überwachung und kontinuierliche Verbesserung des Zugriffsmodells sind entscheidend, um seine Leistung zu optimieren und sicherzustellen, dass es den sich ändernden Anforderungen der Organisation gerecht wird.

Durch regelmäßige Bewertungen und Anpassungen können potenzielle Schwachstellen identifiziert und behoben werden. Eine kontinuierliche Verbesserung gewährleistet, dass das Zugriffsmodell effektiv bleibt und den langfristigen Erfolg der Organisation unterstützt.

3.1.6 Sicherstellung der Compliance:

Die Sicherstellung der Compliance ist ein wesentlicher Bestandteil der Einführung eines neuen Zugriffsmodells. Durch die Einhaltung gesetzlicher Vorschriften und

interner Richtlinien können rechtliche Risiken minimiert und das Vertrauen der Stakeholder gestärkt werden.

Die Überwachung und kontinuierliche Anpassung des Zugriffsmodells gewährleisten, dass alle relevanten Compliance-Anforderungen erfüllt sind und potenzielle Risiken frühzeitig erkannt werden können. Eine gründliche Überprüfung und Dokumentation der Compliance-Maßnahmen sind unerlässlich, um sicherzustellen, dass das Zugriffsmodell den geltenden Standards entspricht.

3.1.7 Zwischenfazit

Die erfolgreiche Einführung eines rollenbasierten Dateizugriffs hängt von einer Vielzahl von Faktoren ab, die eng miteinander verflochten sind. Eine klare Anforderungsdefinition legt den Grundstein für das Design des Zugriffsmodells und stellt sicher, dass es den Bedürfnissen der Organisation entspricht. Eine gründliche Planung und Designphase ermöglicht eine reibungslose Implementierung und Ausrichtung auf die Sicherheitsziele.

Die aktive Einbindung und Schulung der Benutzer fördern deren Verständnis und Akzeptanz des neuen Zugriffsmodells. Eine effektive Kommunikation trägt dazu bei, potenzielle Hindernisse zu überwinden und das Engagement der Mitarbeiter zu stärken. Die Sicherstellung der Compliance mit gesetzlichen Vorschriften und internen Richtlinien gewährleistet die Sicherheit und Integrität sensibler Daten.

Die fortlaufende Überwachung und Anpassung des Zugriffsmodells sowie die Unterstützung seitens des Managements sind entscheidend für den langfristigen Erfolg des Projekts. Durch die Berücksichtigung und Implementierung dieser Erfolgsfaktoren können Organisationen sicherstellen, dass ihr Zugriffsmodell effektiv und sicher ist, und gleichzeitig die Produktivität und Effizienz ihrer Arbeitsabläufe verbessern.

3.2 Projektrisikofaktoren

Die erfolgreiche Einführung eines klassischen Zugriffsmodells für rollenbasierten Dateizugriff kann durch verschiedene Risikofaktoren gefährdet sein, die eine sorgfältige Planung und Umsetzung erfordern.

3.2.1 Widerstand gegen Veränderungen und mangelnde Schulung:

Benutzer könnten sich gegen das neue Zugriffsmodell sträuben, insbesondere wenn es ihre gewohnten Arbeitsabläufe beeinträchtigt oder sie sich in ihren Rollen eingeschränkt fühlen. Dieser Widerstand kann durch unzureichende Schulung und Unterstützung verstärkt werden, was zu Fehlern und Unsicherheiten führen kann. Eine unzureichende Einbindung der Stakeholder und Kommunikationsprobleme können diesen Widerstand weiter verstärken und die Akzeptanz des neuen Modells beeinträchtigen.

Um diesem Risiko zu begegnen, ist eine umfassende Schulungsstrategie erforderlich, die nicht nur die technischen Aspekte des neuen Zugriffsmodells abdeckt, sondern auch die Vorteile für die Benutzer und das Unternehmen betont. Durch frühzeitige und transparente Kommunikation können Bedenken und Ängste der Benutzer adressiert und ihre Akzeptanz und Beteiligung am Schulungsprozess gefördert werden. Eine kontinuierliche Unterstützung durch Helpdesk- oder Supportteams ist ebenfalls entscheidend, um Fragen zu klären und Probleme beim Übergang zum neuen Zugriffsmodell zu lösen.

3.2.2 Komplexität des Zugriffsmodells:

Ein zu komplexes Zugriffsmodell könnte zu Verwirrung und Fehlern bei der Verwaltung von Berechtigungen führen, was die Effizienz und Sicherheit des Systems beeinträchtigen könnten. Um dieses Risiko zu minimieren, ist es wichtig, das Zugriffsmodell so einfach und transparent wie möglich zu gestalten. Dies kann durch eine sorgfältige Definition von Benutzerrollen und Zugriffsrechten, die Vermeidung übermäßiger Komplexität und die Bereitstellung klarer Anleitungen und Richtlinien erreicht werden. Regelmäßige Überprüfungen und Audits des Zugriffsmodells sind ebenfalls erforderlich, um sicherzustellen, dass es den aktuellen Anforderungen entspricht und keine unnötige Komplexität aufweist.

3.2.3 Fehlende Einhaltung gesetzlicher Vorschriften und interner Richtlinien:

Wenn das neue Zugriffsmodell nicht den geltenden rechtlichen Anforderungen oder internen Richtlinien entspricht, kann dies zu rechtlichen Konsequenzen und finanziellen Verlusten führen. Eine gründliche Analyse der rechtlichen

Anforderungen und interner Richtlinien ist daher unerlässlich, um sicherzustellen, dass das Zugriffsmodell den geltenden Vorschriften entspricht und keine rechtlichen Risiken birgt. Die Zusammenarbeit mit Rechtsexperten und Datenschutzbeauftragten kann dazu beitragen, potenzielle Compliance-Probleme frühzeitig zu identifizieren und zu lösen.

3.2.4 Technische Herausforderungen bei der Implementierung:

Die Implementierung des neuen Zugriffsmodells könnte aufgrund technischer Schwierigkeiten, Kompatibilitätsproblemen oder Datenmigrationsschwierigkeiten verzögert oder erschwert werden. Eine gründliche Analyse der bestehenden IT-Infrastruktur und eine sorgfältige Planung der Implementierung sind erforderlich, um technische Herausforderungen frühzeitig zu identifizieren und zu adressieren. Die Zusammenarbeit mit erfahrenen IT-Spezialisten und die Nutzung bewährter Methoden und Tools können dazu beitragen, die Implementierung reibungslos und effizient zu gestalten.

3.2.5 Unzureichende Ressourcen oder Budgetbeschränkungen:

Begrenzte Ressourcen oder Budgetbeschränkungen könnten die Umsetzung des Projekts behindern und zu Kompromissen bei der Schulung, Unterstützung oder Implementierung führen. Eine sorgfältige Ressourcenplanung und Budgetierung sind daher erforderlich, um sicherzustellen, dass ausreichende Mittel für alle erforderlichen Aktivitäten und Maßnahmen zur Verfügung stehen. Die Identifizierung alternativer Finanzierungsquellen und die Priorisierung von Aufgaben können dazu beitragen, Ressourcenengpässe zu minimieren und die Umsetzung des Projekts zu erleichtern.

3.2.6 Kommunikationsprobleme und Konflikte zwischen verschiedenen Interessengruppen:

Eine unzureichende Kommunikation mit den Beteiligten und Interessengruppen sowie mangelnde Einbindung der Stakeholder könnten zu Missverständnissen, Widerstand und Konflikten führen. Eine klare und offene Kommunikation mit allen relevanten Parteien ist daher entscheidend, um sicherzustellen, dass alle Stakeholder über den Fortschritt und die Auswirkungen des Projekts informiert sind. Die Einbindung der Stakeholder in den Entscheidungsprozess und die

Berücksichtigung ihrer Anliegen und Bedenken können dazu beitragen, das Engagement und die Unterstützung für das Projekt zu fördern.

3.2.7 Sicherheitsbedenken und Datenschutzrisiken:

Ein unzureichendes Zugriffsmodell könnte Sicherheitslücken und Datenschutzrisiken aufdecken, was zu Datenlecks oder unautorisiertem Zugriff führen könnte. Eine umfassende Sicherheitsanalyse und -bewertung sind daher erforderlich, um potenzielle Sicherheitsbedrohungen frühzeitig zu identifizieren und zu beheben. Die Implementierung von Sicherheitsmaßnahmen wie Verschlüsselung, Zugriffskontrollen und Überwachungssystemen kann dazu beitragen, die Sicherheit des Systems zu gewährleisten und Datenschutzrisiken zu minimieren.

3.2.8 Fehlende Akzeptanz oder Unterstützung seitens des Managements:

Wenn das Management das neue Zugriffsmodell nicht vollständig unterstützt oder akzeptiert, könnte dies die Umsetzung des Projekts behindern und die Motivation der beteiligten Teams beeinträchtigen. Eine enge Zusammenarbeit mit dem Management und die Überzeugung von den Vorteilen des neuen Zugriffsmodells können dazu beitragen, die Akzeptanz und Unterstützung seitens des Managements zu gewinnen. Die Bereitstellung von klaren und überzeugenden Geschäftsvorteilen sowie die Einbindung des Managements in den Entscheidungsprozess können dazu beitragen, die Zustimmung und Unterstützung für das Projekt zu sichern.

3.2.9 Zwischenfazit

Die Einführung eines rollenbasierten Dateizugriffs birgt eine Reihe von Risikofaktoren, die den Erfolg des Projekts gefährden können. Widerstand gegen Veränderungen und mangelnde Schulung können zu Unsicherheit und Fehlern bei der Umsetzung führen. Die Komplexität des Zugriffsmodells kann zu Verwirrung und Fehlern bei der Verwaltung von Berechtigungen führen, während die Nichteinhaltung gesetzlicher Vorschriften und interner Richtlinien rechtliche Konsequenzen nach sich ziehen kann.

Technische Herausforderungen bei der Implementierung, begrenzte Ressourcen oder Budgetbeschränkungen können die Umsetzung des Projekts verzögern oder erschweren. Kommunikationsprobleme und Konflikte zwischen verschiedenen

Interessengruppen können zu Missverständnissen und Widerstand führen. Sicherheitsbedenken und Datenschutzrisiken können die Integrität sensibler Daten gefährden.

Die Identifizierung und Bewertung dieser Risikofaktoren ist entscheidend, um angemessene Maßnahmen zur Risikominimierung zu ergreifen und den Erfolg der Einführung eines rollenbasierten Dateizugriffs zu gewährleisten. Durch eine sorgfältige Analyse und Planung können Organisationen potenzielle Hindernisse erkennen und proaktiv darauf reagieren, um sicherzustellen, dass das Projekt erfolgreich verläuft.

Nachdem die Risiko- und Erfolgsfaktoren des rollenbasierten Dateizugriffs ausführlich betrachtet wurden, ist es von essenzieller Bedeutung, nun den Fokus auf die praktische Umsetzung dieses Konzepts in einem fiktiven Unternehmen zu lenken. Hierbei ist anzumerken, dass aufgrund der Einfachheit des simulierten Unternehmens bestimmte Projekt- und Risikofaktoren, die in der realen Unternehmenswelt relevant sind, nicht berücksichtigt werden. Dennoch bietet die Analyse der praktischen Anwendung des rollenbasierten Dateizugriffs wertvolle Erkenntnisse und Erfahrungen, die im Rahmen dieses Praxisprojekts näher untersucht werden sollen.

Im kommenden Kapitel werden die Schritte von der Planung bis zur Implementierung des rollenbasierten Dateizugriffs im Detail erläutert.

Kapitel 4 RBFA in der Praxis. Teil 1: Die Planung

Bevor die praktische Implementierung der rollenbasierten Dateizugriffskontrolle (RBFA) im Active Directory betrachtet wird, ist es wichtig, einen Überblick über die Organisation zu geben, in der dieses Projekt stattfindet. Die folgenden Abschnitte stellen die " Entenhausener Finanz KG " vor, eine fiktive Firma, die sich für die RBFA-Implementierung entschieden hat, um ihren Dateizugriff effizienter und sicherer zu gestalten. Dabei wird bewusst eine kleinere Organisation gewählt, da eine zu große Firma die Implementierung unnötig verkomplizieren könnte. Dennoch ist anzumerken, dass das grundlegende Prinzip der RBFA sich nicht ändert, selbst wenn es um größere Unternehmen geht. Damit bleibt die praktische Umsetzung dieses Konzepts relevant und übertragbar, unabhängig von der Größe der Organisation.

4.1 Intermezzo: Die Entenhausener Finanz KG

Die "Entenhausener Finanz KG" ist ein etabliertes Unternehmen in Entenhausen, das sich auf den Handel mit Gold spezialisiert hat. Unter der Leitung von Dagobert Duck als CEO und Geschäftsführer hat sich das Unternehmen einen Ruf als führender Akteur im Goldmarkt erworben. Mit einem Team von rund 30 engagierten Mitarbeitern strebt die "Entenhausener Finanz KG" danach, ihren Kunden hochwertige Dienstleistungen im Bereich Goldeinankauf, -verkauf und Finanzberatung anzubieten.

Um einen besseren Überblick über die Organisation und die IT-Infrastruktur zu erhalten, wird im weiteren Verlauf dieses Berichts ein Organigramm sowie ein Netzwerkplan vorgestellt. Das Organigramm gibt Aufschluss über die Unternehmensstruktur und die verschiedenen Abteilungen, während der Netzwerkplan einen Überblick über die IT-Infrastruktur bietet, einschließlich der Verbindung zwischen den verschiedenen Komponenten wie Workstations, Servern und Netzwerkeinrichtungen. Durch die Visualisierung dieser Informationen wird es möglich sein, die rollenbasierte Dateizugriffskontrolle (RBFA) im Active Directory effektiv zu implementieren und zu verwalten.

Rahmenbedingung

Die vorliegende Darstellung präsentiert exemplarisch ein Netzwerkdiagramm und ein Organigramm, wobei der Fokus auf der Erläuterung des RBFA liegt. Ebenfalls wurden exemplarisch nur zwei Benutzer pro Abteilung angelegt. Es sei darauf hingewiesen, dass die präsentierten Strukturen rein hypothetischer Natur sind und keinerlei direkten Bezug zur realen Welt haben. Diese Darstellung dient ausschließlich didaktischen Zwecken, um die Konzepte des RBFA zu verdeutlichen.

4.1.1 Unternehmensstruktur:

Die "Entenhausener Finanz KG" ist in verschiedene Abteilungen unterteilt, die jeweils spezifische Funktionen erfüllen, um den Geschäftsbetrieb reibungslos zu gestalten. An der Spitze des Unternehmens steht Dagobert Duck als CEO und Geschäftsführer, der die strategische Ausrichtung des Unternehmens bestimmt. Unterstützt wird er von erfahrenen Führungskräften in den Bereichen Finanzen, Vertrieb und Administration.

- ✓ **Direktor und Geschäftsführung:** Dagobert Duck leitet als Direktor die "Entenhausener Finanz KG" und ist maßgeblich für die Festlegung der strategischen Ziele und die Überwachung des Geschäftsbetriebs verantwortlich. Seine Geschäftsführer Klaas Klever und Gundel Gaukeley teilen sich respektive die Bereich Vertrieb und Administration sowie Finanzen und Einkauf.
- ✓ **Finanzen:** Unter der Leitung des Finanzleiters kümmert sich die Finanzabteilung um alle finanziellen Angelegenheiten des Unternehmens, darunter Buchhaltung, Controlling und Budgetierung.
- ✓ **Vertrieb:** Die Vertriebsabteilung unter der Leitung des Vertriebsleiters ist für den Goldeinverkauf an Kunden und Geschäftspartner zuständig und arbeitet aktiv daran, neue Kunden zu gewinnen und den Umsatz zu steigern.

- ✓ **Einkauf:** Die Einkaufsabteilung, geleitet vom Einkaufsleiter, ist für den Ankauf von Goldein auf dem Markt verantwortlich und bemüht sich stets um die Beschaffung der besten Angebote.
- ✓ **Administration und Sekretariat:** Die Administrationsabteilung unterstützt den reibungslosen Geschäftsbetrieb durch die Verwaltung von Personalangelegenheiten, Büroorganisation und allgemeine Verwaltungsaufgaben. Das Sekretariat übernimmt die organisatorische Unterstützung der Geschäftsführung und stellt sicher, dass alle administrativen Prozesse effizient ablaufen.

4.1.2 IT-Infrastruktur:

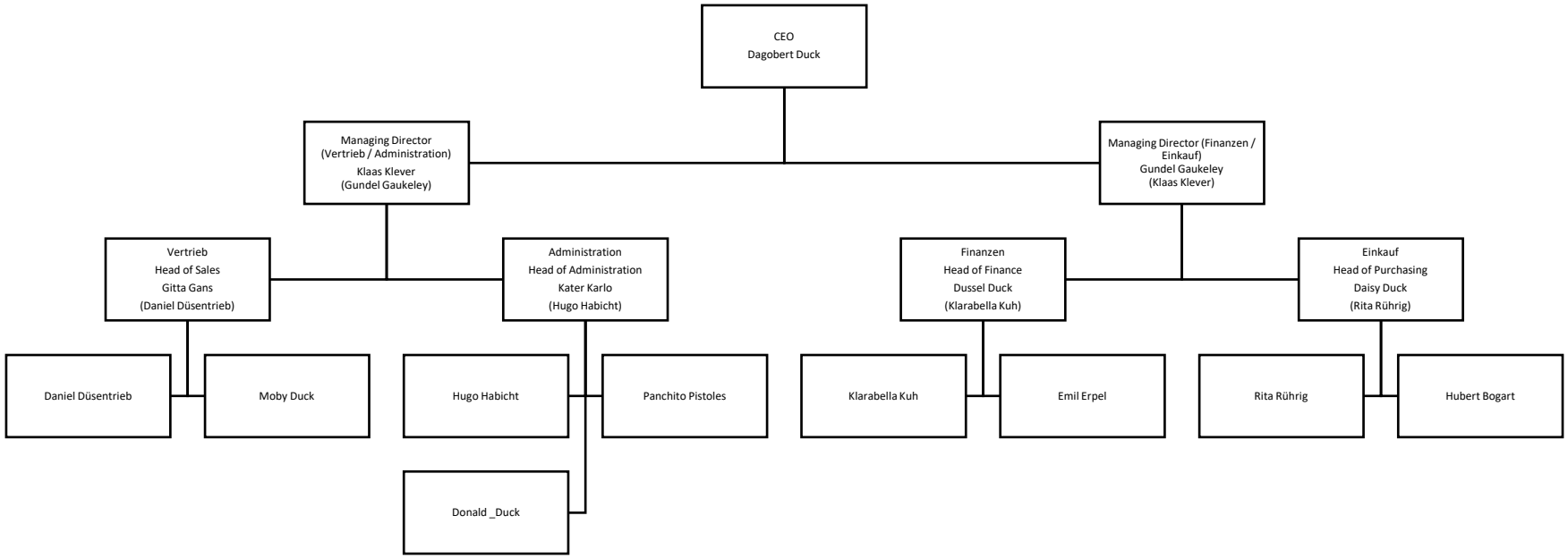
Die "Entenhausener Finanz KG" verfügt über eine moderne IT-Infrastruktur, die den Mitarbeitern eine effiziente Arbeitsumgebung bietet. Dazu gehören Workstations mit dem neuesten Betriebssystem Windows 11, die den Mitarbeitern die Durchführung ihrer Aufgaben erleichtern. Ein Domain Controller (DC) verwaltet die Benutzerkonten und Sicherheitsrichtlinien, während ein dedizierter Fileserver als zentraler Speicherort für Dateien und Dokumente dient.

Donald Duck, der „DUCK IT SERVICES“ leitet, fungiert als externer IT-Experte für die EFKG. Verwaltungstechnisch wird Donald in der Administration untergebracht und im Active Directory auch ebendort geführt.

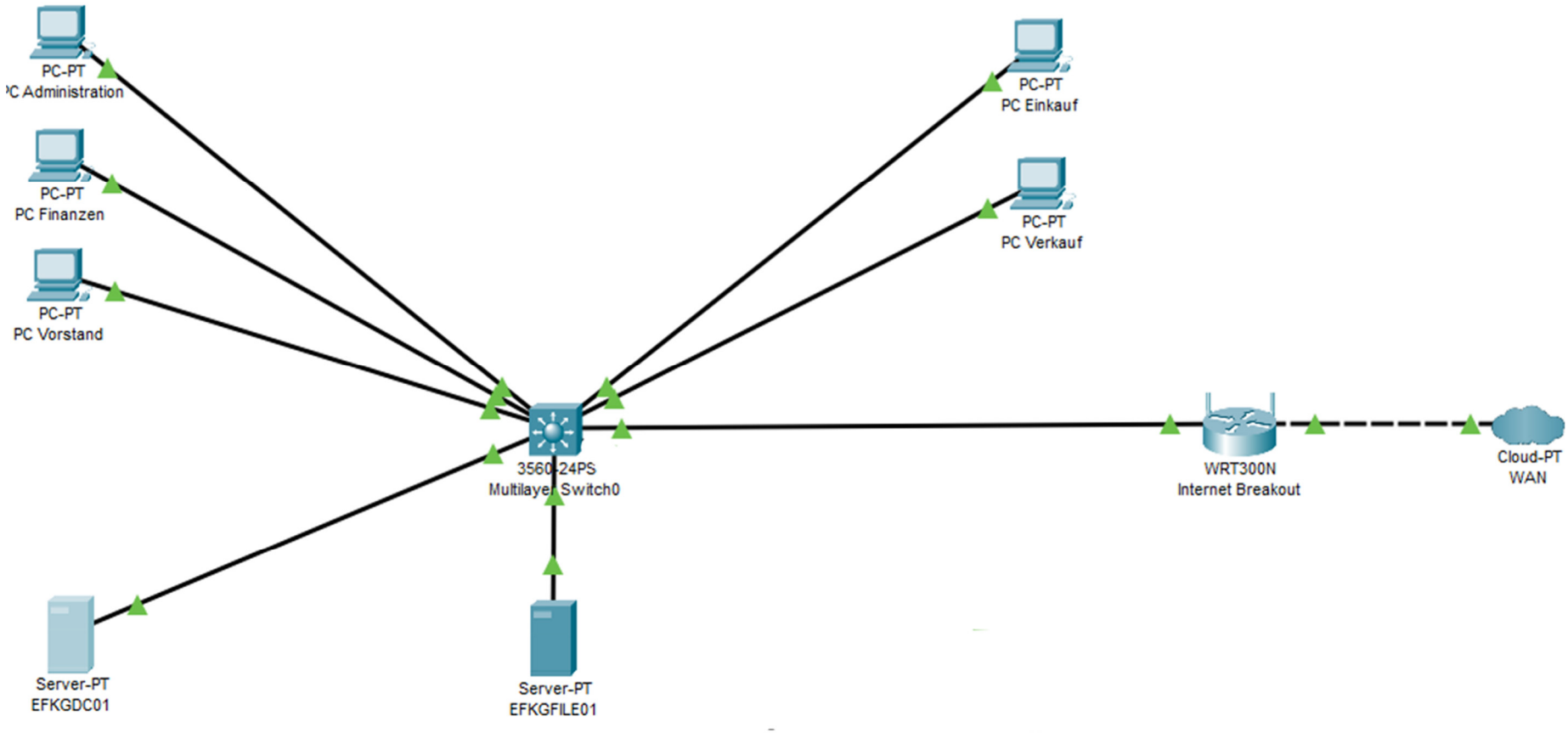
Donald ist zwar externer Dienstleister und müsste – aus Sicht der Informationssicherheit - gesondert und besonders betrachtet werden. Dies wird aber in dieser Arbeit NICHT getan, da der Rahmen dieses Papiers gesprengt werden würde und vom eigentlichen Thema abgelenkt wird. Es wird angenommen, dass Donald integer und vertrauenswürdig ist und somit die administrative Berechtigung, die ihm aus der Mitgliedschaft der Domänenadministratoren erteilt wird, nicht missbraucht.

In den folgenden Abschnitten werden die konkreten Schritte zur Implementierung von RBFA detailliert beschrieben, wobei die RBFA-Prinzipien aus dem Grundlagenkapitel auf die spezifischen Anforderungen der "Entenhausener Finanz KG" angewendet werden, um die Sicherheit und Effizienz der Dateiverwaltung zu verbessern.

4.1.3 Das Organigramm der Entenhausener Finanz KG



4.1.4 Netzwerkplan der Entenhausener Finanz KG



4.2 Planungsphase 1: Die Rollen in der EFKG (Entenhausener Finanz KG)

Die Rollen in der EFKG ergeben sich aus der Stellenbezeichnung des jeweiligen Mitarbeiters. Aus dem Organigramm lassen sich somit folgende Rollen extrahieren:

- ✓ CEO (im AD als Globale Gruppe „GG_CEO“ angelegt)
- ✓ Managing director (im AD als Globale Gruppe „GG_GF_$Geschäftsbereich“ (Geschäftsführung) angelegt)
- ✓ Head of (department) (im AD als Globale Gruppe „GG_AL_$Abteilung“ (Abteilungsleiter) angelegt)
- ✓ Mitarbeiter (im AD als Globale Gruppe „GG_MA_$Abteilung“ angelegt)

Außerdem muss die Aufgabe als Stellvertreter einer Geschäftsführung / Abteilung ebenfalls als Rolle in Betracht gezogen werden. Daraus ergeben sich die Rollen:

- ✓ Stellvertreter der Geschäftsführung (im AD als Globale Gruppe „GG_ST_GF_$Geschäftsbereich“ angelegt)
- ✓ Stellvertreter der Abteilungsleitung (im AD als Globale Gruppe „GG_ST_AL_$Abteilung“ angelegt)

Angemerkt werden muss auch, dass obwohl die GF mehrere Geschäftsbereiche führt, die Rollen pro Geschäftsbereich angelegt werden müssen. Letzteres mit Hinblick darauf, dass hier die Verantwortungsbereiche der Geschäftsführung erweitert bzw. eingeschränkt werden könnten.

Aus dieser einfachen Konstellation ergibt sich eine recht komplexe Benutzer / Gruppen Matrix.

Mitglied der Gruppe Kein Mitglied der Gruppe

Gruppen \ Benutzer	Dagobert Duck	Klaas Klever	Gundel Gaukeley	Gitta Gans	Kater Karlo	Dussel Duck	Daisy Duck	Daniel Düsentrieb	Moby Duck	Hugo Habicht	Panchito Pistoles	Klarabella Kuh	Emil Erpel	Rita Rührig	Hubert Bogart
GG_CEO	■														
GG_GF_Admin		■													
GG_GF_Vertrieb		■													
GG_GF_Finanz			■												
GG_GF_Einkauf			■												
GG_ST_GF_Admin			■												
GG_ST_GF_Vertrieb			■												
GG_ST_GF_Finanz		■													
GG_ST_GF_Einkauf		■													
GG_AL_Admin					■										
GG_AL_Vertrieb				■											
GG_AL_Finanz						■									
GG_AL_Einkauf							■								
GG_ST_AL_Admin										■					
GG_ST_AL_Vertrieb								■							
GG_ST_AL_Finanz												■			
GG_ST_AL_Einkauf														■	
GG_MA_Admin										■	■				
GG_MA_Vertrieb								■	■						
GG_MA_Finanz												■	■		
GG_MA_Einkauf														■	■

4.3 Planungsphase 2: Ressourcen und Ressourcengruppen

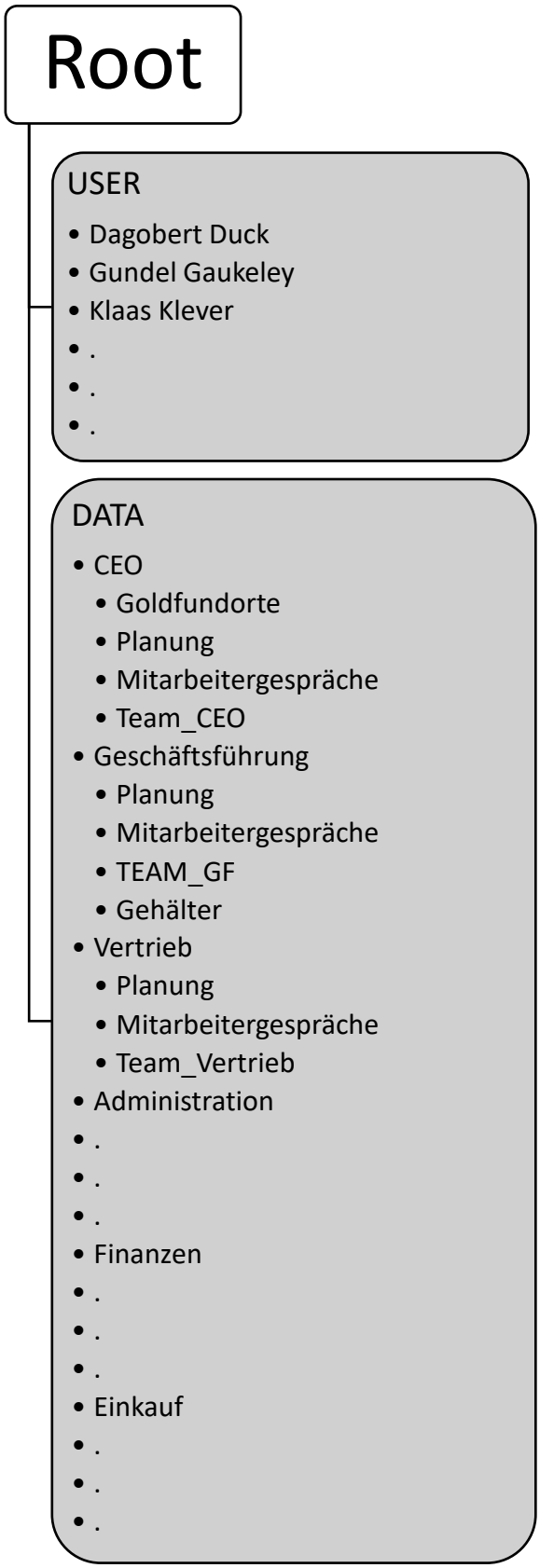
Nachdem die Rollenplanung erfolgreich abgeschlossen wurde, folgt ein entscheidender Schritt: die Identifizierung der Ressourcen, die einer Zugriffskontrolle bedürfen, sowie die Strukturierung dieser Ressourcen in sinnvolle Ressourcengruppen. Diese Phase ist von entscheidender Bedeutung für die effektive Implementierung eines Rollen-basierten Dateizugriffssystems.

Zunächst müssen alle relevanten Ressourcen innerhalb des Unternehmens identifiziert werden, die einer Zugriffskontrolle unterliegen sollen. Dies umfasst typischerweise Dateien, Ordner, Datenbanken, Anwendungen und andere digitale Assets, die sensible Informationen enthalten oder kritische Geschäftsprozesse unterstützen. Im Falle der EFKG wird der Umfang sich auf Ordner und Dateien beschränken.

4.3.1 Ressourcen oder die Ordnerstruktur

Zunächst soll die Ordnerstruktur beschreibend dargestellt werden, um dann in ein übersichtliches Diagramm überführt zu werden.

- ✓ Es sollen 2 Ordner in der Root des Laufwerks angelegt werden: User und Data
- ✓ Jede Abteilung wird im Data-Volume durch einen Ordnernamen, der den Abteilungsnamen trägt, repräsentiert.
- ✓ In jedem Abteilungsordner befinden sich drei Unterordner: Planung, Mitarbeitergespräche und ein allgemeiner Ordner Team_$Abteilung unter welchem alle benötigten Dokumente der Abteilung untergebracht sind.
- ✓ In den Ordnern der Geschäftsführung findet sich ein zusätzlicher Ordner „Gehälter“
- ✓ Im Ordner CEO befindet sich ein zusätzlicher Ordner „Goldfundorte“
- ✓ Jeder Benutzer soll einen persönlichen Ordner auf dem User-Volume erhalten.


Root
USER
• Dagobert Duck
• Gundel Gaukeley
• Klaas Klever
• .
• .
• .
DATA
• CEO
• Goldfundorte
• Planung
• Mitarbeitergespräche
• Team_CEO
• Geschäftsführung
• Planung
• Mitarbeitergespräche
• TEAM_GF
• Gehälter
• Vertrieb
• Planung
• Mitarbeitergespräche
• Team_Vertrieb
• Administration
• .
• .
• .
• Finanzen
• .
• .
• .
• Einkauf
• .
• .
• .

4.3.2 Die Ressourcengruppen oder die Domänenlokale Gruppen für die Berechtigungszuweisung.

Im Gegensatz zu den globalen Gruppen werden die domänenlokalen Gruppen keine Benutzer, sondern ausschließlich Gruppen beherbergen. Die globalen Gruppen enthalten Elemente, die eine gleiche oder ähnliche Rolle repräsentieren, die domänenlokale Gruppen dahingegen enthalten die Elemente, die gleiche oder ähnliche Berechtigungen brauchen.

Die Gruppe, die letztendlich die Berechtigung auf eine Ressource bekommt, wird folgendermaßen im Active Directory angelegt:

DL_$Abteilung_$Ordnername_READ

DL_$Abteilung_$Ordnername_MOD(ify).

Diese Konvention ergäbe für den Ordner Mitarbeitergespräche in Vertrieb:

DL_Vertrieb_Mitarbeitergespräche_READ (MOD)

4.4 Planungsphase 3: Die Berechtigungsstruktur

Nachdem nun festgelegt wurde, was zu schützen ist, sollte nun geplant werden, wie die Ressourcen geschützt werden sollen. Genauer gesagt, soll festgelegt werden, welche Rolle (Globale Gruppe) mit welcher Berechtigung auf die Ressourcen zugreifen darf.

In der Realität wird eine Berechtigungsmatrix angelegt, die eine grafische Übersicht über den Zugriff auf die Ressourcen bietet. Einfacher, oder in AGDLP-Nomenklatur ausgedrückt wird festgelegt, welche globalen Gruppen in die Domänenlokale Gruppen aufgenommen werden sollen. Aus Platzgründen wird an dieser Stelle darauf verzichtet, und die Anforderungen in beschreibender Form festgehalten.

4.5 Anfoderungen an die Berechtigungen

- Dagobert Duck als CEO soll ändernden Zugriff auf alle Ordner in „CEO“ erhalten. Zusätzlich bekommt er lesenden Zugriff auf ALLE Ordner innerhalb des Unternehmens.

- Die GF bekommt ändernden Zugriff auf alle Ordner in „Geschäftsführung“. Darüber hinaus mindestens lesenden Zugriff auf alle Abteilungsordner im jeweiligen Zuständigkeitsbereich. Ebenso darf die GF ändernd auf die Planungsdaten der Fachbereiche zugreifen, für die sie verantwortlich ist. Da die GF sich gegenseitig vertritt, darf jeder Geschäftsführer ebenfalls lesend auf die Mitarbeiterbesprechungen AUSSERHALB seines Fachbereichs zugreifen.
- Jede Abteilungsleitung darf ändernd auf alle Ordner des Fachbereichs zugreifen. Zusätzlich darf jede Abteilungsleitung lesend auf die Planungsordner der GF zugreifen.
- Jeder Mitarbeiter darf ändernd auf den Teams-Ordner zugreifen sowie lesend auf den Planungsordner. Ist der Mitarbeiter gleichzeitig Stellvertreter der AL, bekommt er / sie ändernden Zugriff auf den Planungsordner.
- Sonderreglung: Dagobert vertraut in höchstem Maße der Leitung der Administration und gewährt deshalb ändernden Zugriff auf seine Planungsdaten.

Dies sind die Anforderungen, wie vom CEO gewünscht. Ist eine Berechtigung nicht explizit erwähnt, so soll der Zugriff verboten sein.

Mit der Festlegung der Anforderungen endet dieses Kapitel. Im nächsten Kapitel sollen diese Anforderungen umgesetzt und getestet werden.

Kapitel 5 RBFA in der Praxis. Teil 2: Die Umsetzung

In diesem Kapitel liegt der Fokus auf der praktischen Umsetzung des AGDLP-Konzepts (Account, Global, Domain Local, Permission) in einem Active Directory-Umfeld.

Die folgenden Abschnitte beschreiben die Schritte und Verfahren, die erforderlich sind, um AGDLP in der realen Welt anzuwenden.

Es sei darauf hingewiesen, dass detaillierte Anleitungen zum Einrichten des Active Directory und zur Erstellung von Benutzern und Gruppen im Anhang zu finden sind, um Lesern eine umfassende Anleitung für die Einrichtung der Grundlagen zu bieten. Dieses Kapitel konzentriert sich speziell auf die praktische Umsetzung des AGDLP-Konzepts zur Zugriffsverwaltung.

Zur Verdeutlichung der Vorgehensweise werden noch einmal die erforderlichen Schritte, die für die Implementierung notwendig sind, aufgezählt. Die rot markierten Schritte sind bereits erledigt und dokumentiert im Anhang.

Account (Benutzerkonto):

Zu Beginn werden Benutzerkonten erstellt. Diese Konten repräsentieren die Benutzer innerhalb des Active Directory und werden normalerweise auf der globalen Ebene erstellt.

Global (Globale Gruppen):

Auf der globalen Ebene werden Sicherheitsgruppen erstellt.

Diese globalen Gruppen dienen dazu, Benutzer mit ähnlichen Aufgaben oder Zugriffsanforderungen zusammenzufassen.

Benutzerkonten werden dann in die entsprechenden globalen Gruppen platziert, um ihnen Zugriff auf Ressourcen zu gewähren, die für ihre Rolle relevant sind.

Domain Local (Domänenlokale Gruppen):

Auf der domänenlokalen Ebene werden Sicherheitsgruppen erstellt, die Berechtigungen für bestimmte Ressourcen definieren.

Die globalen Gruppen, die zuvor erstellt wurden und Benutzerkonten enthalten, werden dann in diese domänenlokalen Gruppen platziert.

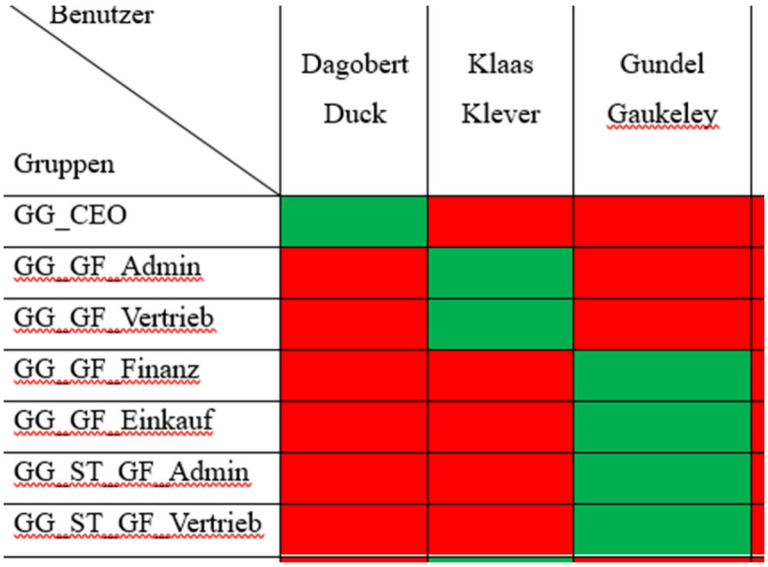
Permission (Berechtigung):

Berechtigungen werden den domänenlokalen Gruppen zugewiesen, um den Zugriff auf bestimmte Ressourcen zu steuern. Diese Berechtigungen können Lese-, Schreib- oder Ausführungsrechte umfassen, je nach den Anforderungen für die jeweilige Ressource.

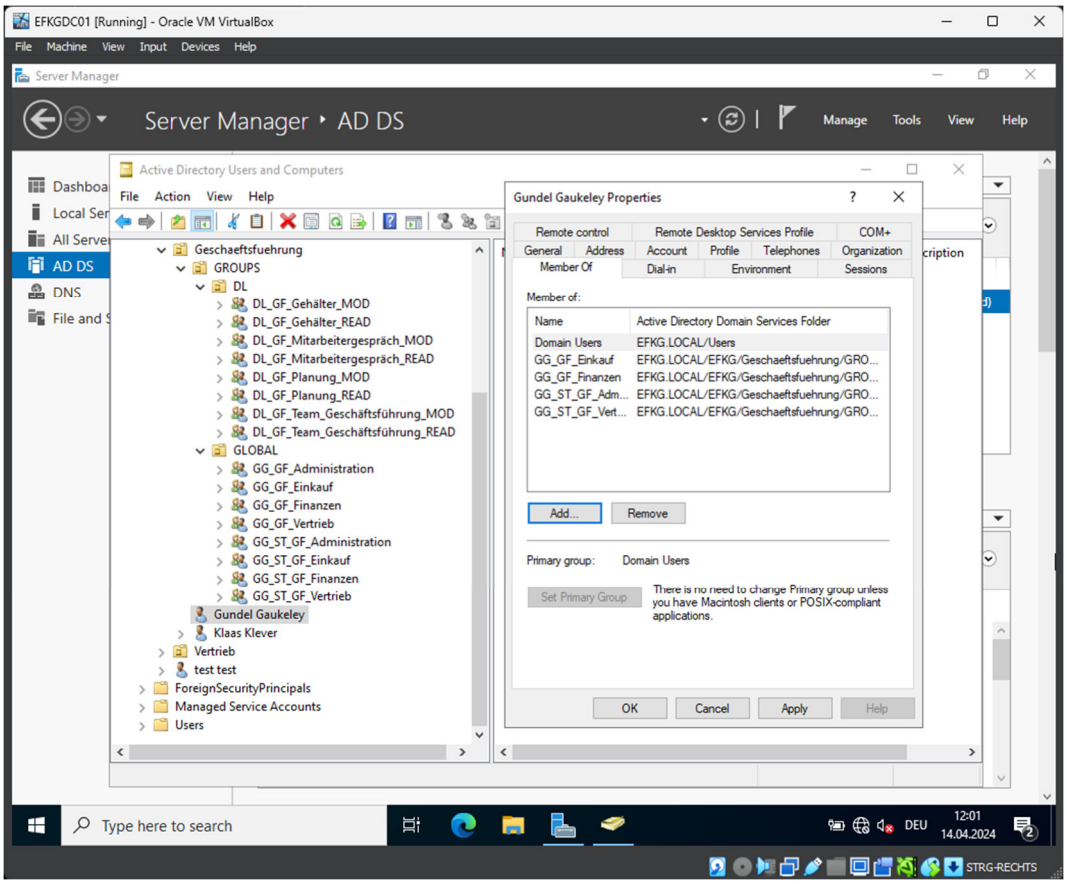
Indem Benutzerkonten in die globalen Gruppen und diese wiederum in die domänenlokalen Gruppen platziert werden, erben sie die entsprechenden Berechtigungen für die Ressourcen, die diesen Gruppen zugewiesen sind.

5.1 Benutzer den globalen Gruppen hinzufügen

Die Zuordnung geschieht mittels der Benutzer / Gruppen Matrix aus Kapitel 4. Es wird an einem Benutzer veranschaulicht, mit allen anderen Benutzern wird analog verfahren.



Gundel Gaukeley wird den grün markierten Gruppen hinzugefügt.



Damit ist die Rolle als Geschäftsführerin für Gundel Gaukeley festgelegt. Darüber hinaus hat sie die Stellvertreterrolle inne für die anderen Geschäftsbereiche.

Diese Vorgehensweise wird nun für alle Benutzer wiederholt.

5.2 Globale Gruppen den domänenlokalen Gruppen hinzufügen.

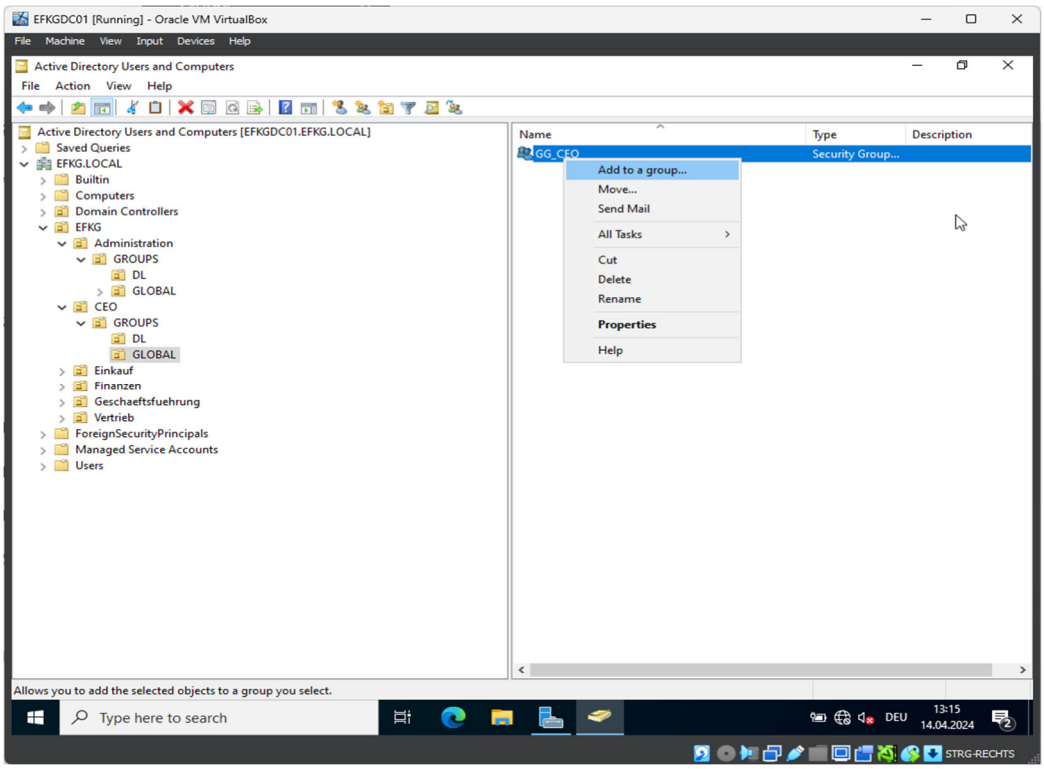
An dieser Stelle käme normalerweise die Berechtigungsmatrix zum Einsatz. Da aus Platzgründen darauf verzichtet wurde, folgt nun die praktische Umsetzung, orientiert an den Anforderungen aus Kapitel 4.

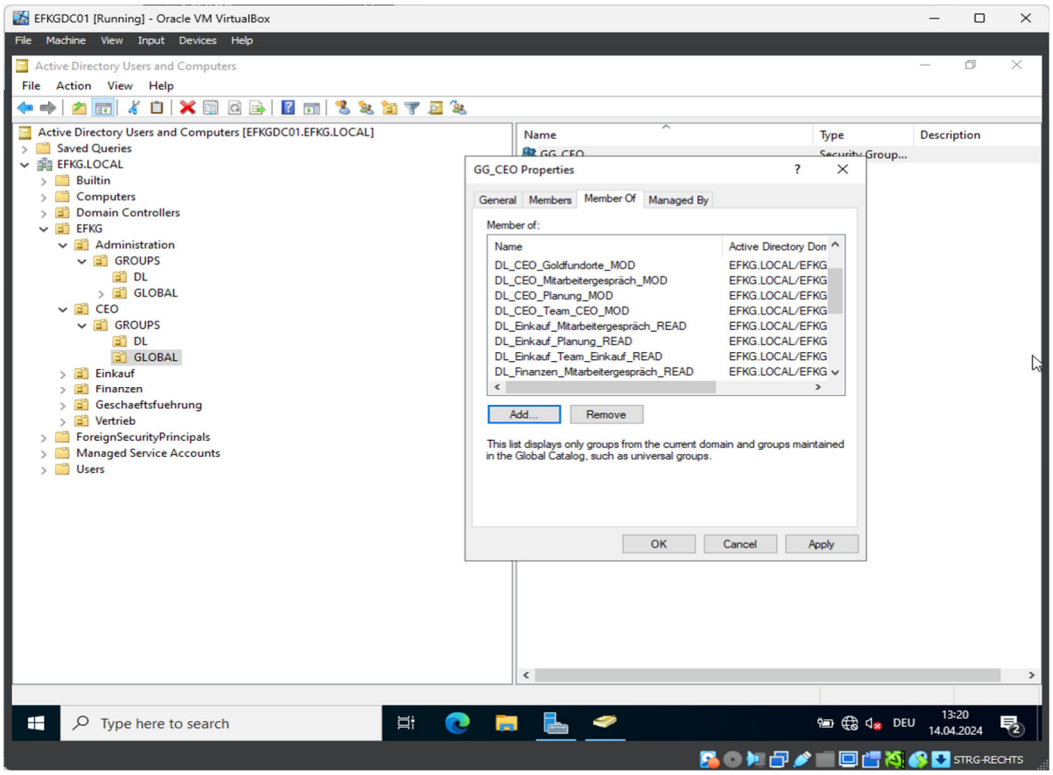
5.2.1 Erste Anforderung

Dagobert Duck als CEO soll ändernden Zugriff auf alle Ordner in „CEO“ erhalten. Zusätzlich bekommt er lesenden Zugriff auf ALLE Ordner innerhalb des Unternehmens.

Das bedeutet, dass die globale Gruppe GG_CEO in alle domänenlokalen Gruppen aufgenommen werden muss, die später ändernden Zugriff auf die Unterordner von „CEO“ bekommen. Zusätzlich muss diese Gruppe in alle domänenlokalen Gruppen

(aller Abteilungen) aufgenommen werden, die Lesenden Zugriff auf die Abteilungsdaten erhalten.





Diese Einstellung setzt die erste Anforderung um.

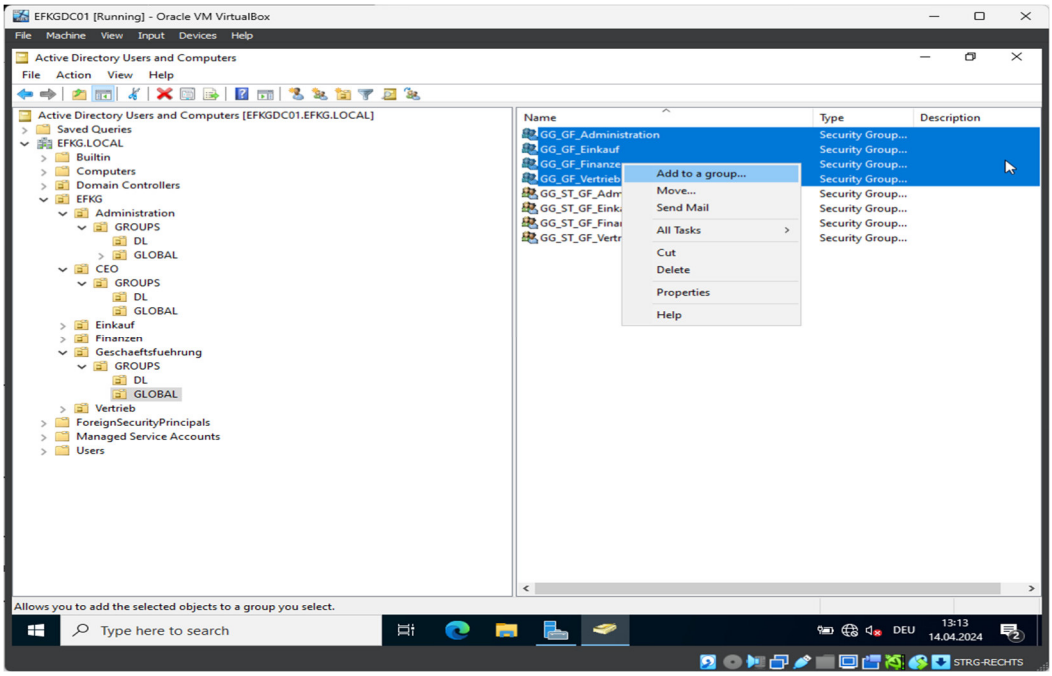
5.2.2 Zweite Anforderung

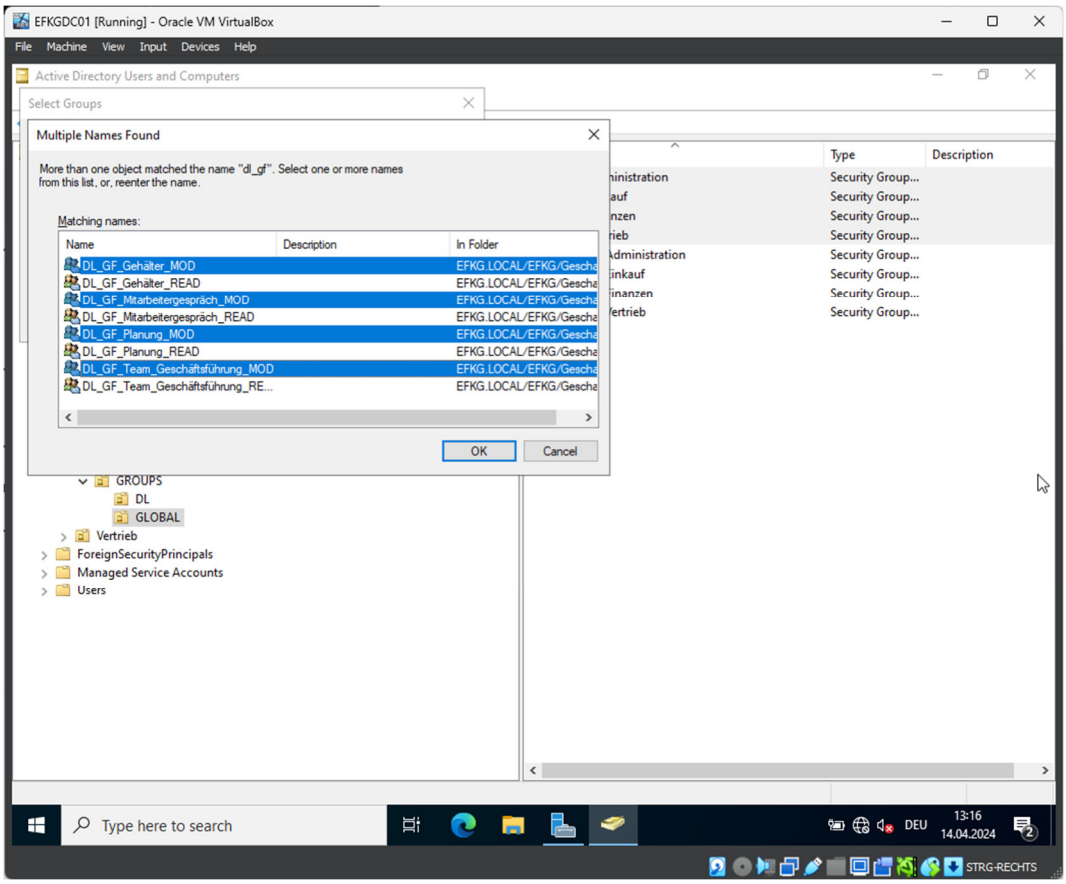
Die GF bekommt ändernden Zugriff auf alle Ordner in „Geschäftsführung“. Darüber hinaus mindestens lesenden Zugriff auf alle Abteilungsordner im jeweiligen Zuständigkeitsbereich. Ebenso darf die GF ändernd auf die Planungsdaten der Fachbereiche zugreifen, für die sie verantwortlich ist. Da die GF sich gegenseitig vertritt, darf jeder Geschäftsführer ebenfalls lesend auf die Mitarbeiterbesprechungen AUSSERHALB seines Fachbereichs zugreifen.

Das bedeutet, dass die globale Gruppe GG_GF_$Abteilung in alle domänenlokalen Gruppen aufgenommen werden muss, die später ändernden Zugriff auf die Unterordner von „Geschäftsführung“ bekommen. Zusätzlich muss diese Gruppe in alle domänenlokalen Gruppen aufgenommen werden, die lesenden Zugriff auf die Abteilungsordner bekommen. Die Planungsdaten der Fachbereiche bilden hier die Ausnahme: dort darf die GF in den eigenen Fachbereichen ändernd zugreifen. Zum Schluss muss die Vertreterreglung realisiert werden.

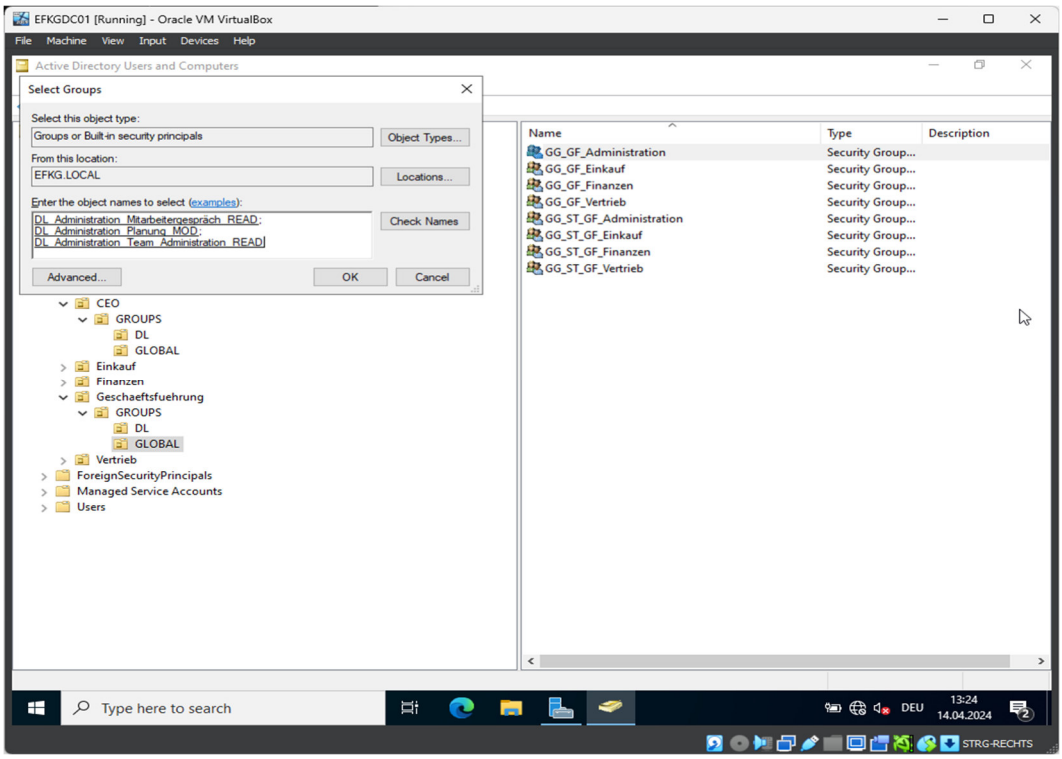
Da es sich dabei um eine recht komplexe Anforderung handelt, wird diese Schritt für Schritt bebildert.

Im ersten Schritt werden die ändernden Zugriffe auf die Abteilungsordner der GF sichergestellt.

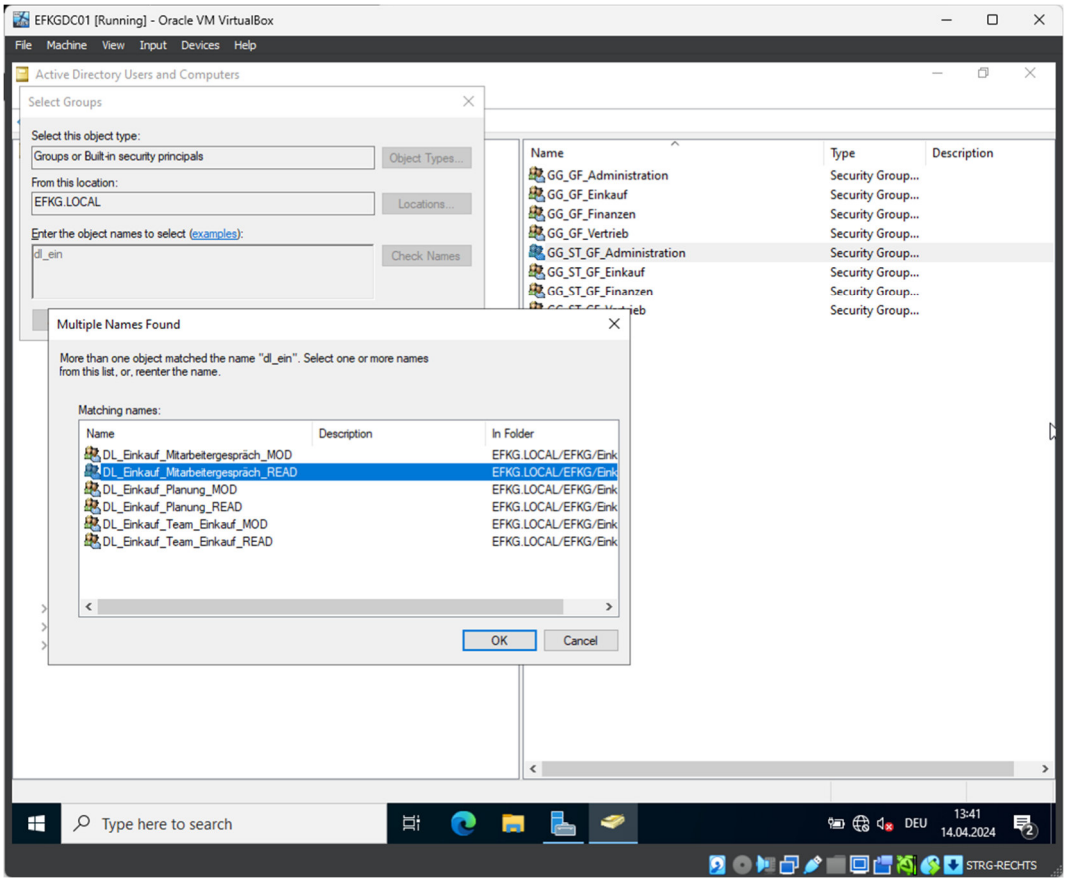




Im zweiten Schritt wird der Lesezugriff auf die Ordner Mitarbeitergespräch und Team_$Abteilung, sowie der ändernde Zugriff auf den Planungsordner der eigenen Fachbereiche Sichergestellt.



Um im letzten Schritt die Vertreterreglung zu sichern, wird die globale Gruppe der Geschäftsführung einer Abteilung in die Globale Gruppe der anderen drei Abteilungen aufgenommen, die das Leserecht auf den Ordner „Mitarbeitergespräche“ sicherstellt.

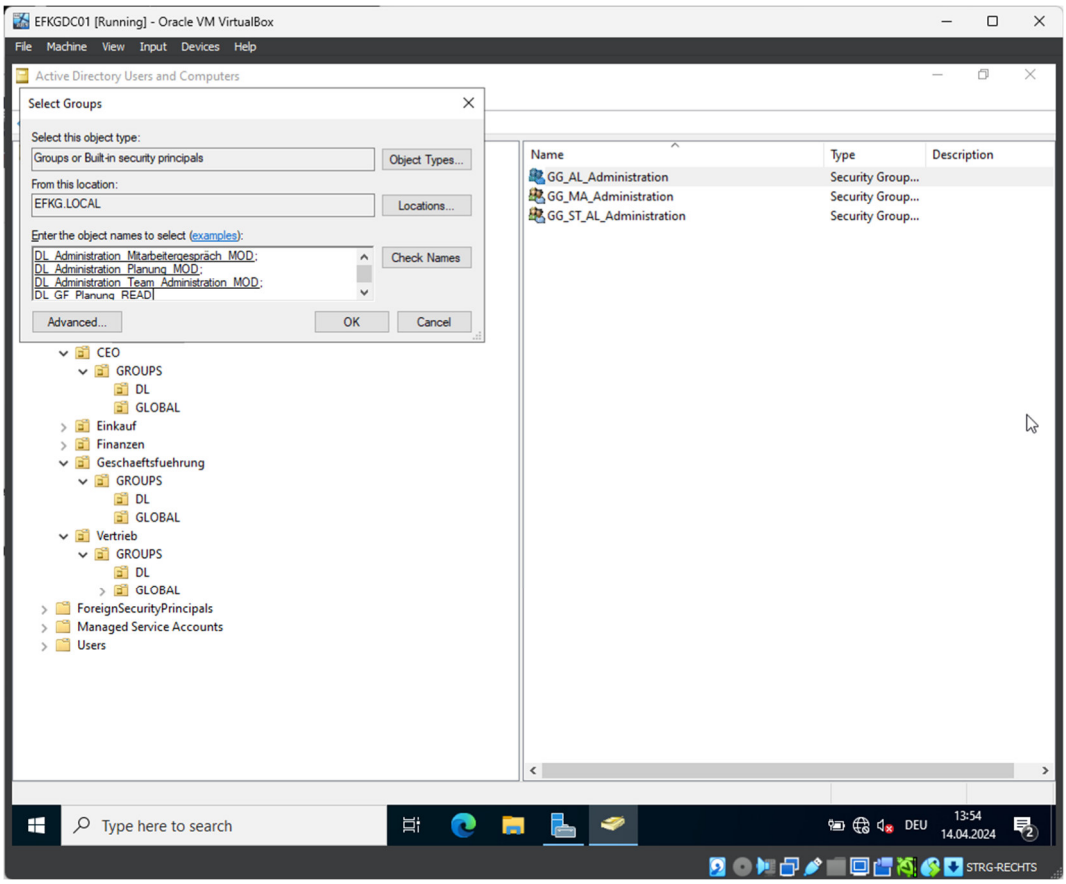


Diese Einstellung vereinfacht auch die Verwaltung, sollten sich die Zuständigkeiten der Geschäftsführer ändern.

Diese Einstellungen setzen die zweite Anforderung um.

5.2.3 Dritte Anforderung

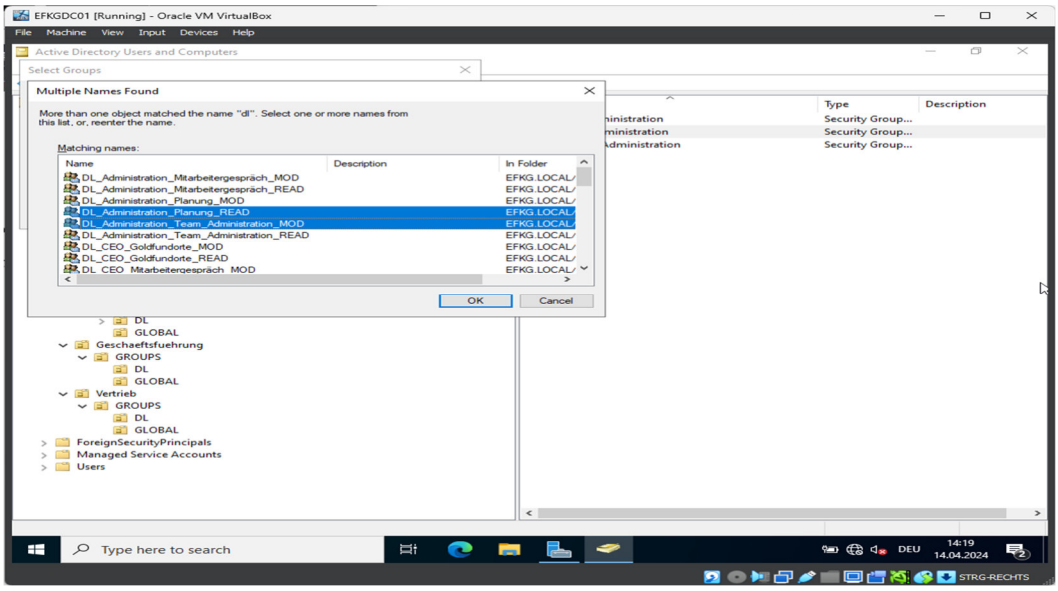
Jede Abteilungsleitung darf ändernd auf alle Ordner des Fachbereichs zugreifen. Zusätzlich darf jede Abteilungsleitung lesend auf den Planungsordner der GF zugreifen.

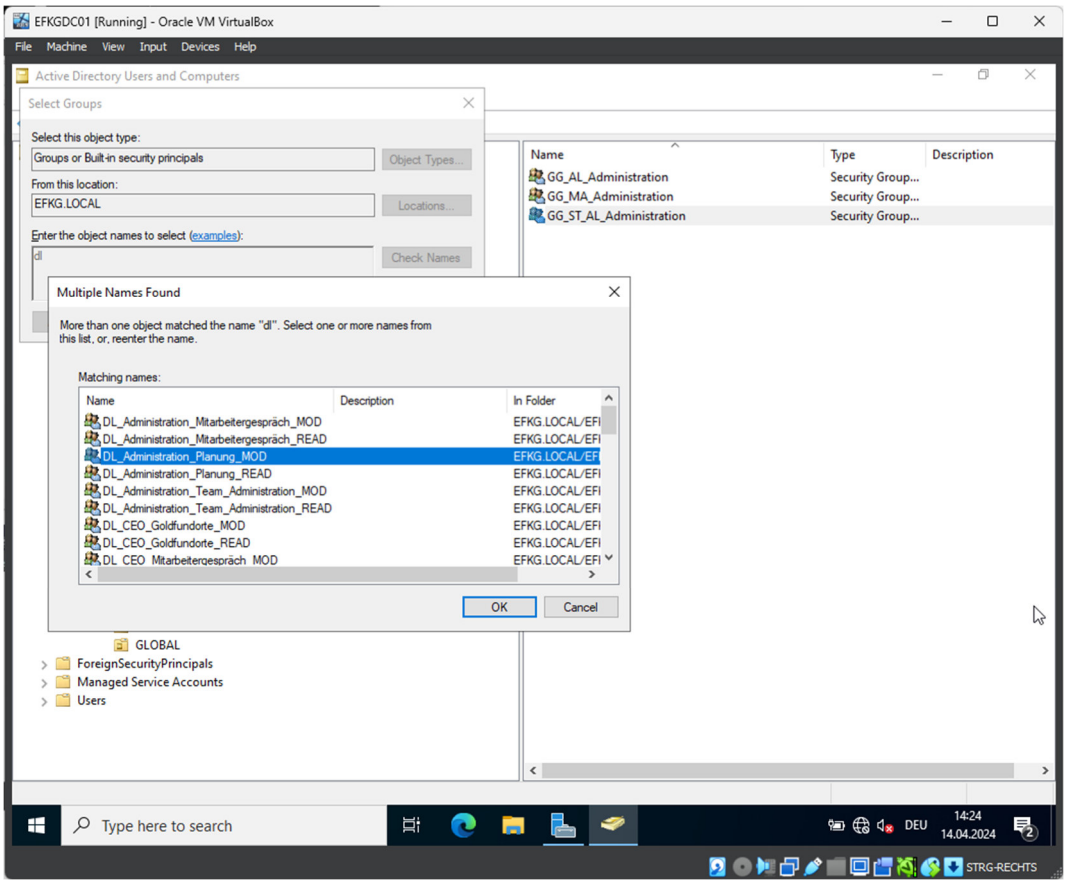


Diese Einstellung (gesetzt für alle Abteilungen) setzt die dritte Anforderung um

5.2.4 Vierte Anforderung

Jeder Mitarbeiter darf ändernd auf den Teams-Ordner zugreifen sowie lesend auf den Planungsordner. Ist der Mitarbeiter gleichzeitig Stellvertreter der AL, bekommt er / sie ändernden Zugriff auf den Planungsordner der Abteilung.

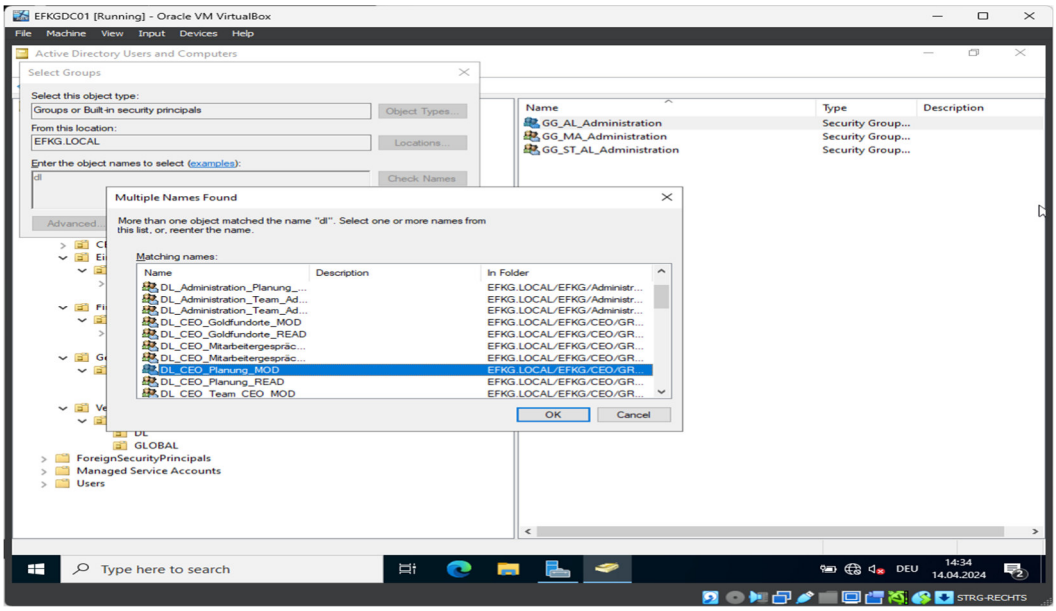




Diese Einstellung, vorgenommen in allen Abteilungen, setzt die vierte Anforderung um.

5.2.5 Fünfte Anforderung

Sonderreglung: Dagobert vertraut in höchstem Maße der Leitung der Administration und gewährt deshalb ändernden Zugriff auf seine Planungsdaten.

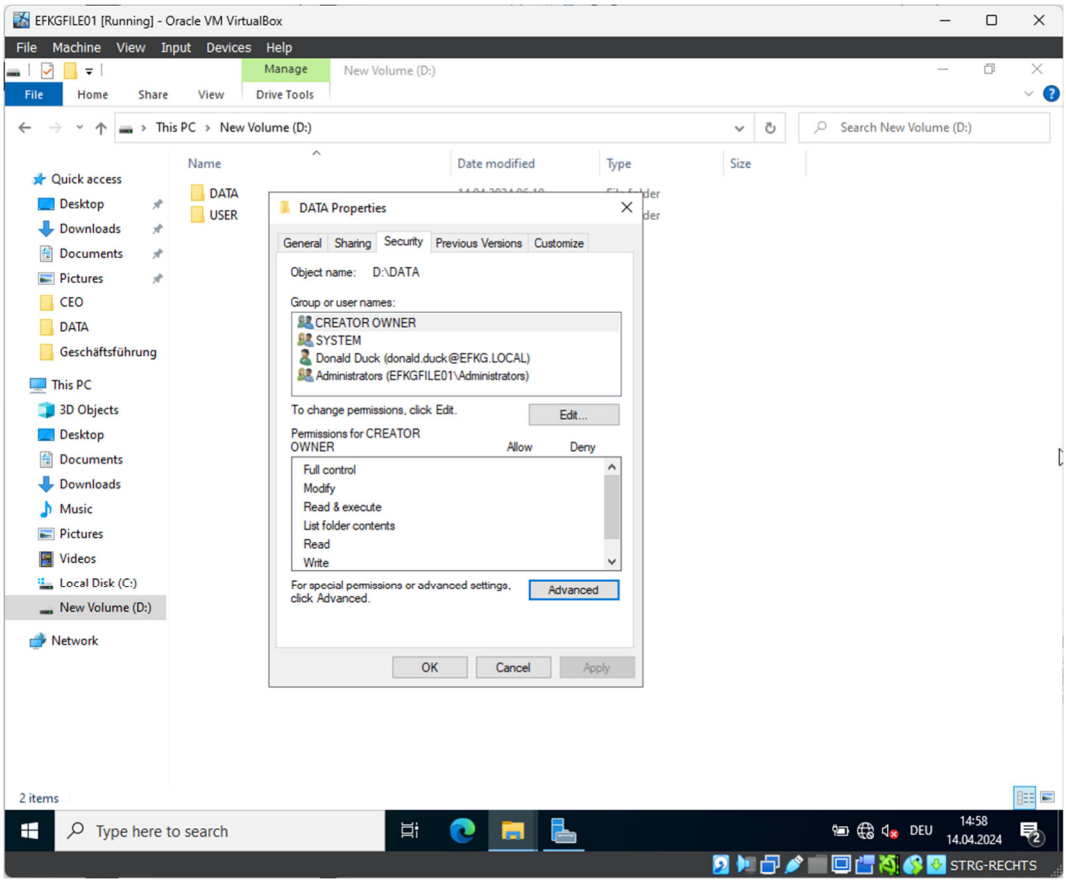


Diese Einstellung setzt die letzte Anforderung um.

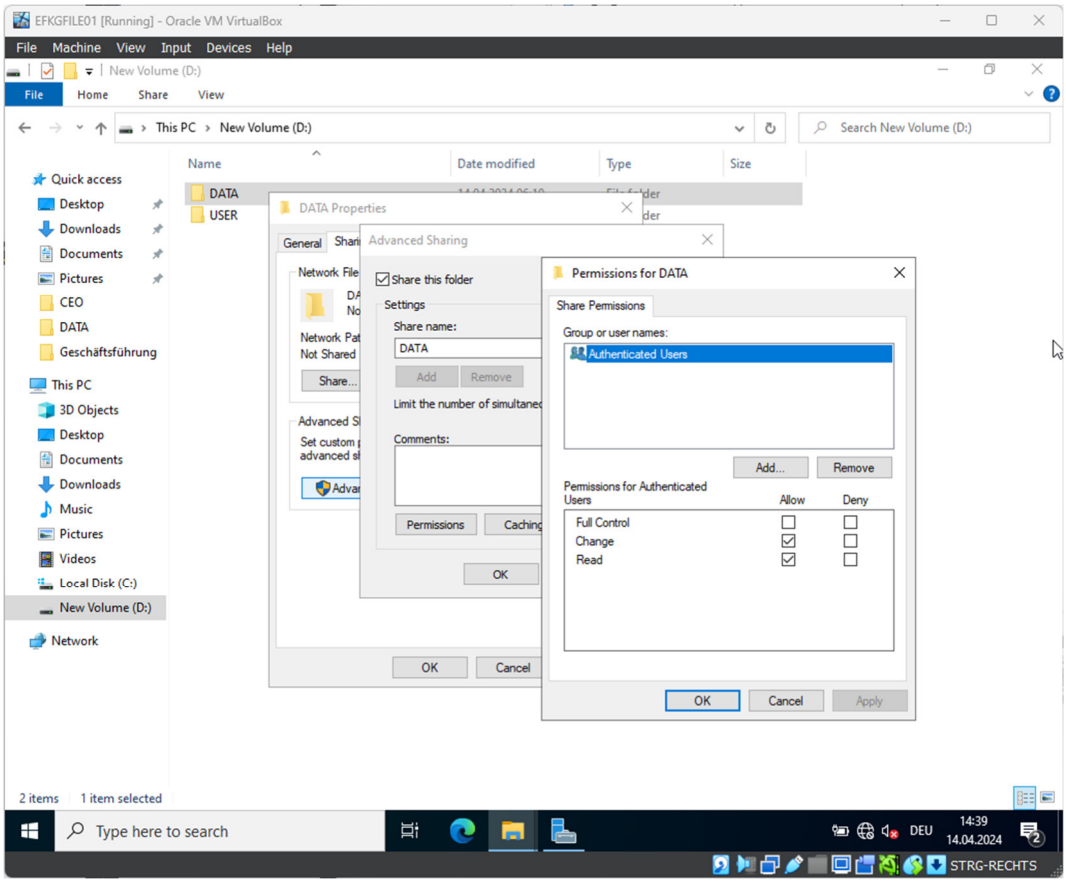
5.3 Die Berechtigungen für die domänenlokale Gruppen setzen

Der letzte Schritt der Umsetzung beinhaltet die Vergabe von Berechtigungen. Dazu sind weitere Arbeiten am Fileserver nötig.

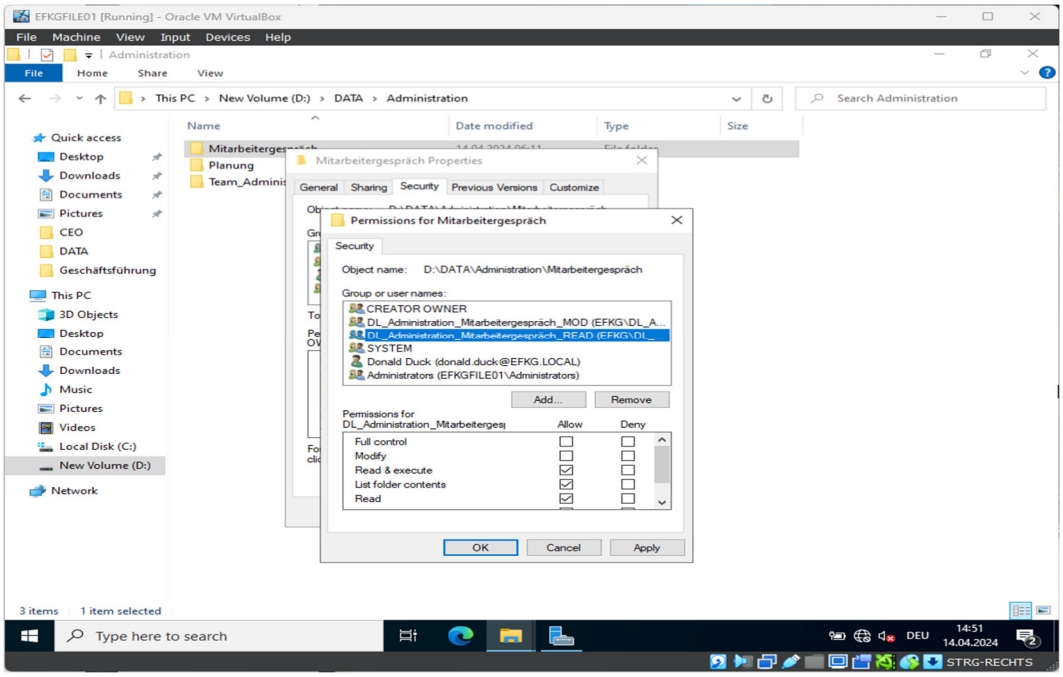
Zuerst werden die Vererbungen vom DATA-Volume entfernt und die EFKGFILE01\Users-Gruppe aus der Berechtigungsliste entfernt.



Im nächsten Schritt werden die Freigabeberechtigungen vergeben. Dafür wird das DATA-Volume freigegeben und authentifizierte Benutzer können über das Netzwerk zugreifen mit ändern als maximaler Berechtigung.



Danach werden die Berechtigungen für die einzelnen Unterordner vergeben. Dazu werden die entsprechenden domänenlokale Gruppen hinzugefügt und die jeweiligen Berechtigungen gesetzt. Die „Read-Gruppe“ bekommt Leseberechtigung, die „Mod-Gruppe“ dementsprechend Änderungsberechtigung.



Diese Verfahrensweise wird fortgesetzt, bis alle Unterordner aller Abteilungen mit Berechtigungen versehen sind.

Im nächsten Schritt werden die erzielten Ergebnisse stichprobenartig analysiert, um die Wirksamkeit dieser Maßnahmen zu dokumentieren und die Vorteile der AGDLP-Implementierung nachzuweisen.

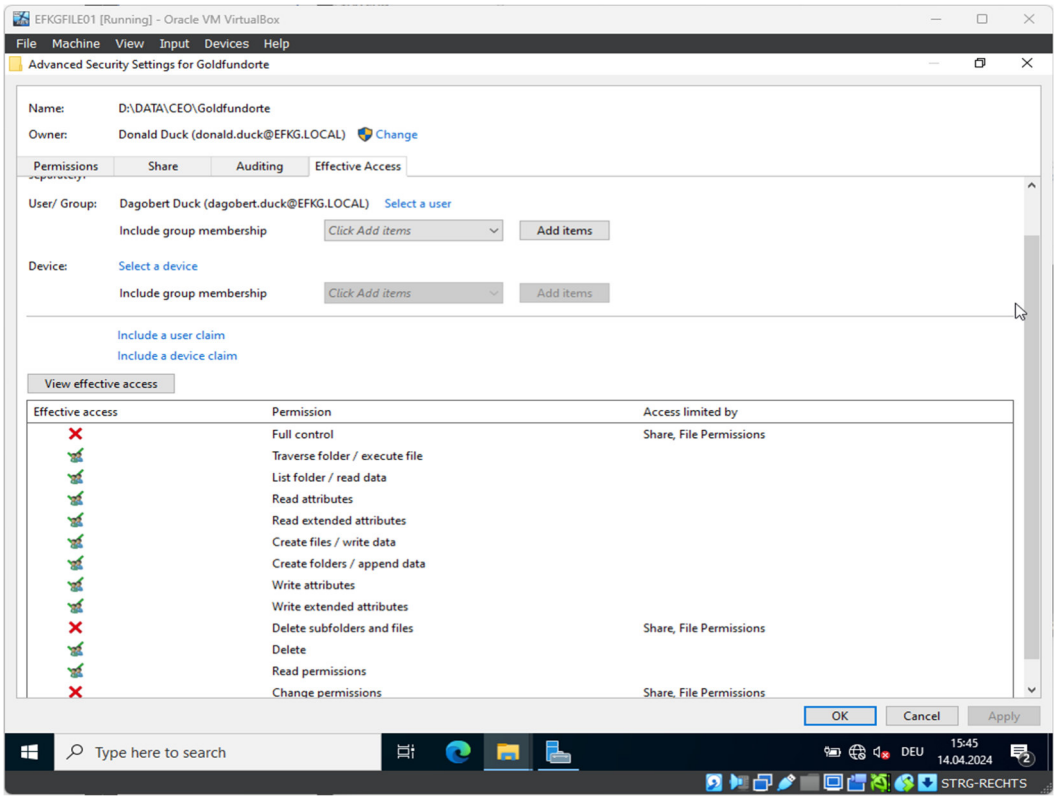
5.4 Nachweis der Umsetzung

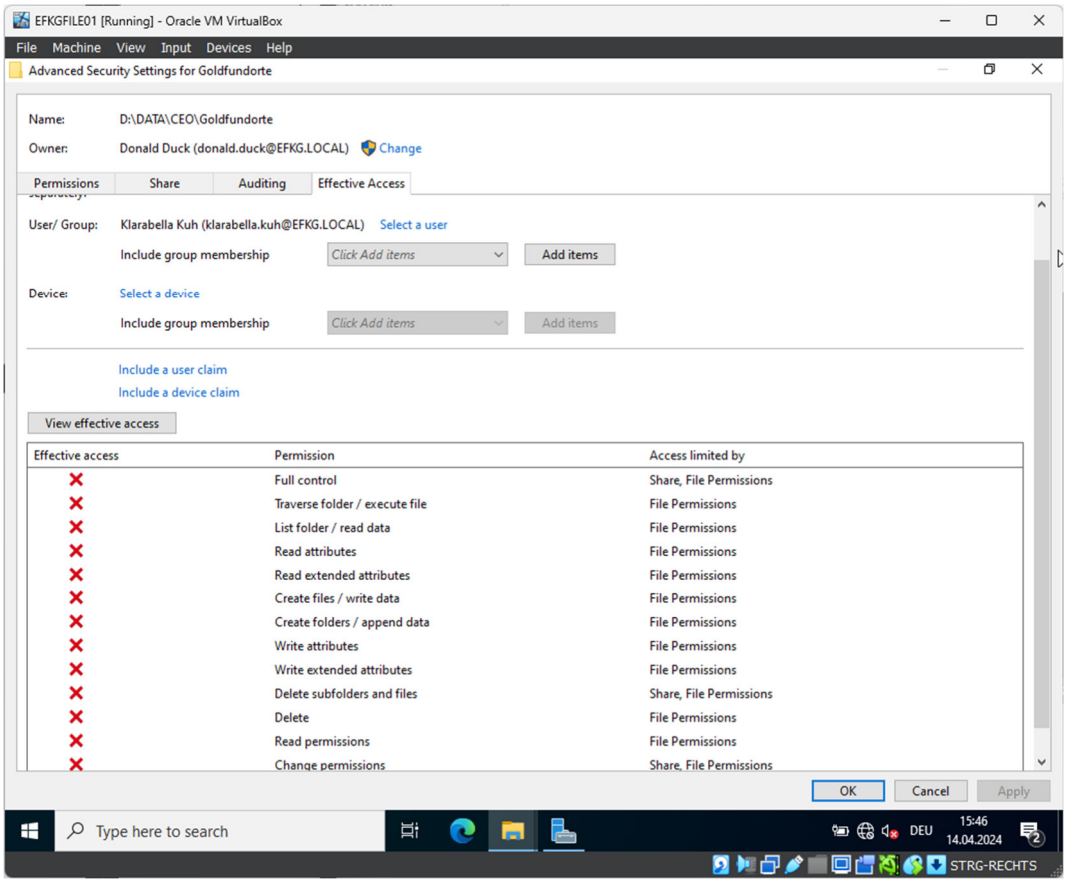
Um die Umsetzung nachzuweisen ist es nicht nötig einen Client zu verwenden. Windows Server bringt ein Tool namens „Effektive Berechtigungen“ mit, welches die Berechtigung einer AD-Identität auf eine Ressource ermittelt, wenn diese Identität über das Netzwerk zugreift. Dieses Tool kann direkt auf dem Fileserver ausgeführt werden.

Alle Nachweise werden stichprobenartig erbracht.

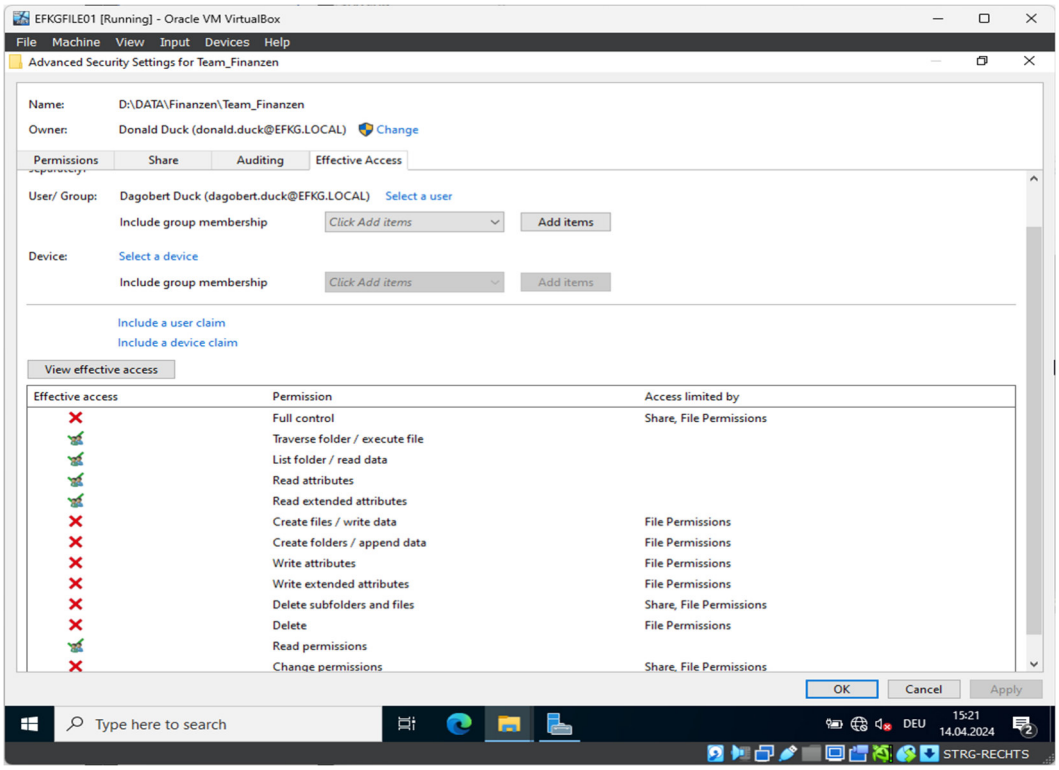
5.4.1 Nachweis der Umsetzung der ersten Anforderung

Dagobert Duck als CEO soll ändernden Zugriff auf alle Ordner in „CEO“ erhalten. Zusätzlich bekommt er lesenden Zugriff auf ALLE Ordner innerhalb des Unternehmens.





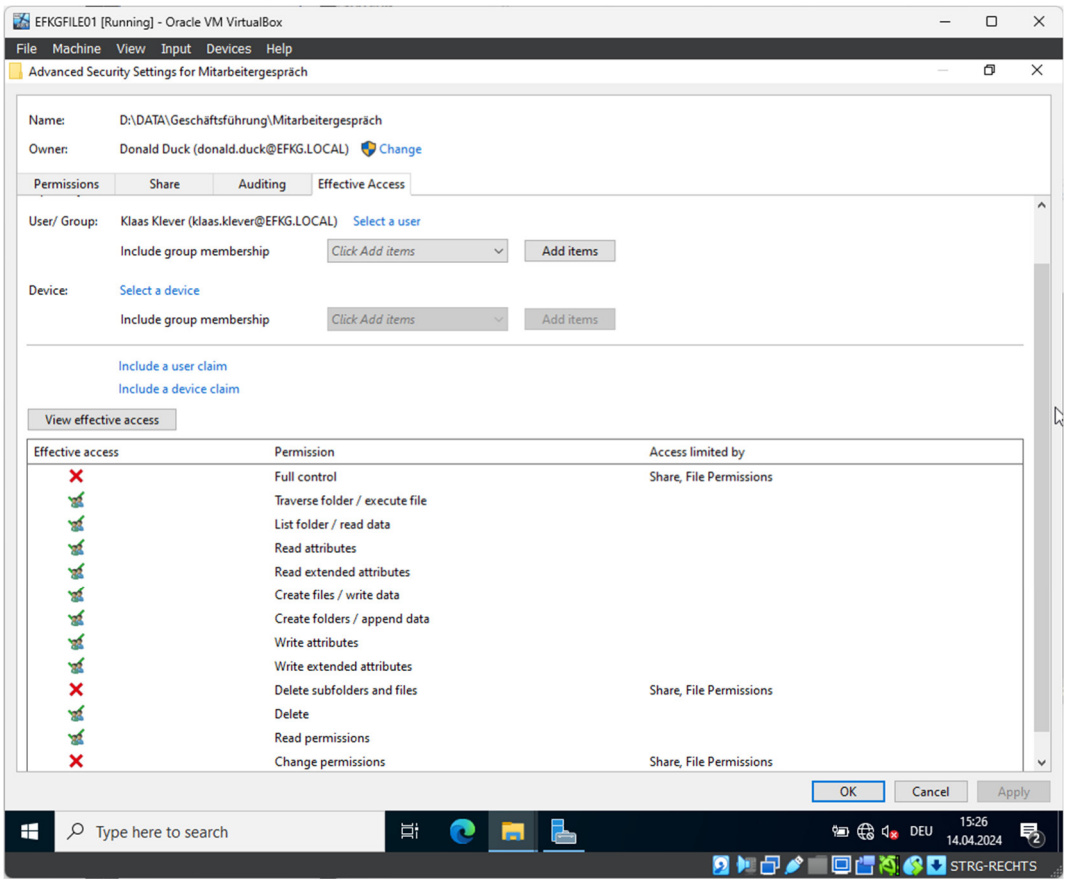
Dagobert hat ändernden Zugriff auf den eigenen Ordner. Die Gegenprobe mit einem anderen Benutzer zeigt, dass ausschließlich Dagobert diesen Zugriff besitzt.



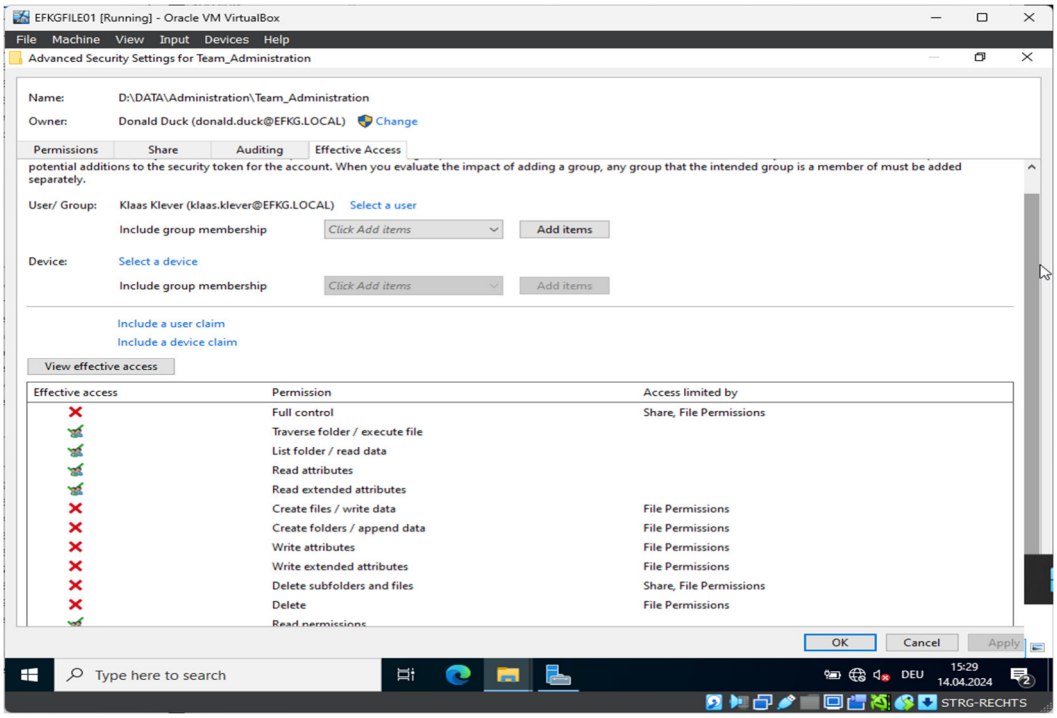
Dagobert hat lesenden Zugriff auf einen zufällig ausgewählten Ordner. Der Nachweis der Funktionalität ist für die erste Anforderung erbracht.

5.4.2 Nachweis der Umsetzung der zweiten Anforderung

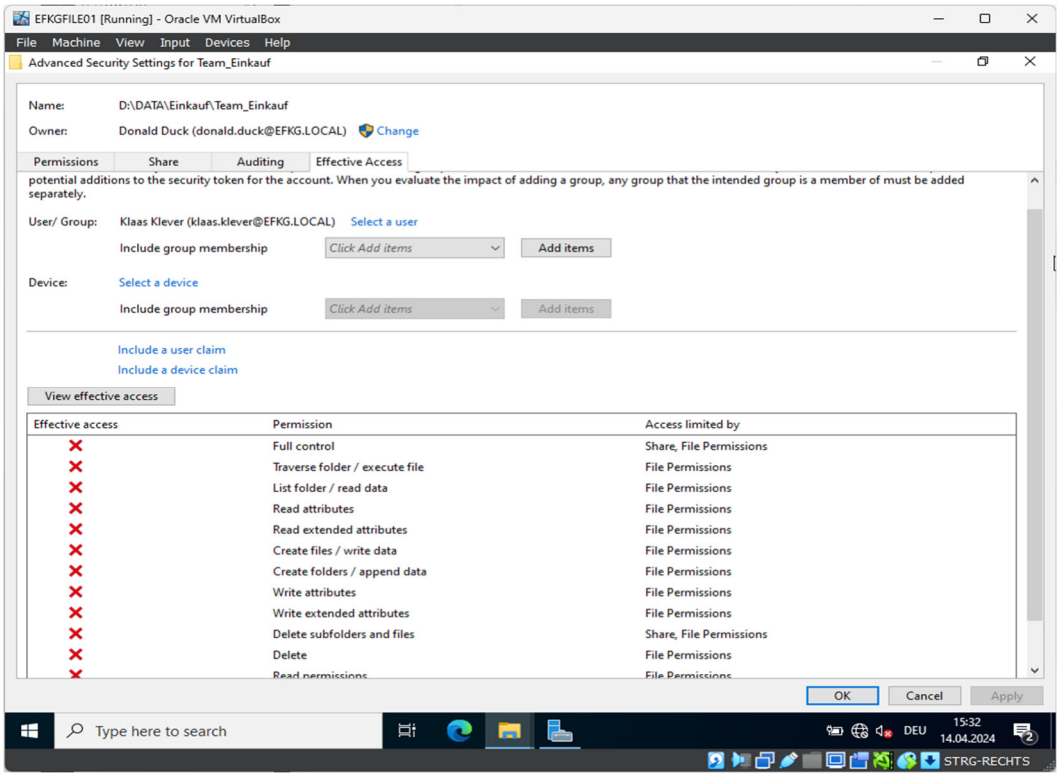
Die GF bekommt ändernden Zugriff auf alle Ordner in „Geschäftsführung". Darüber hinaus mindestens lesenden Zugriff auf alle Abteilungsordner im jeweiligen Zuständigkeitsbereich. Ebenso darf die GF ändernd auf die Planungsdaten der Fachbereiche zugreifen, für die sie verantwortlich ist. Da die GF sich gegenseitig vertritt, darf jeder Geschäftsführer ebenfalls lesend auf die Mitarbeiterbesprechungen AUSSERHALB seines Fachbereichs zugreifen.



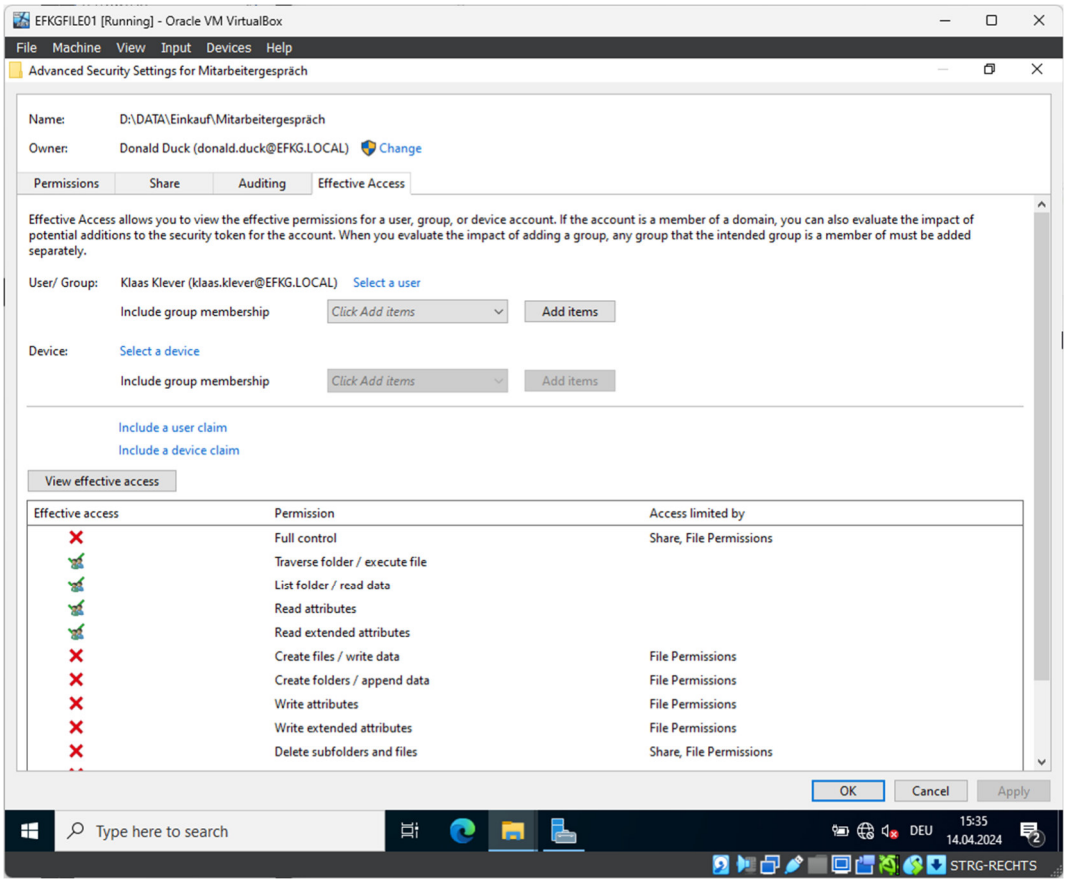
Klaas Klever hat ändernden Zugriff auf einen beliebigen Ordner unterhalb des Geschäftsführungsordners.



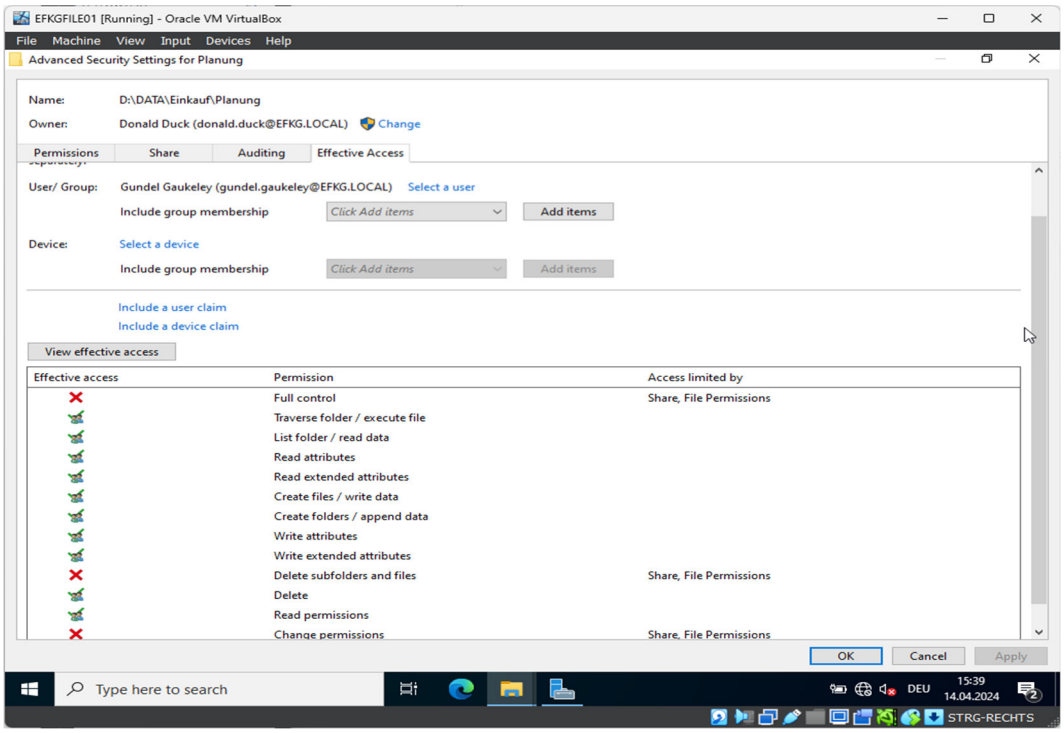
Klaas Klever hat einen lesenden Zugriff auf einen Abteilungsordner in seinem Zuständigkeitsbereich.



Klaas Klever hat keinerlei Zugriffsmöglichkeiten auf einen Ordner in einer Abteilung, die außerhalb seiner Zuständigkeit liegt.



Die Vertreterregel der GF sieht vor, dass die GF lesenden Zugriff auf den Ordner Mitarbeitergespräch erhält, wenn der Ordner außerhalb der Zuständigkeit der GF liegt.

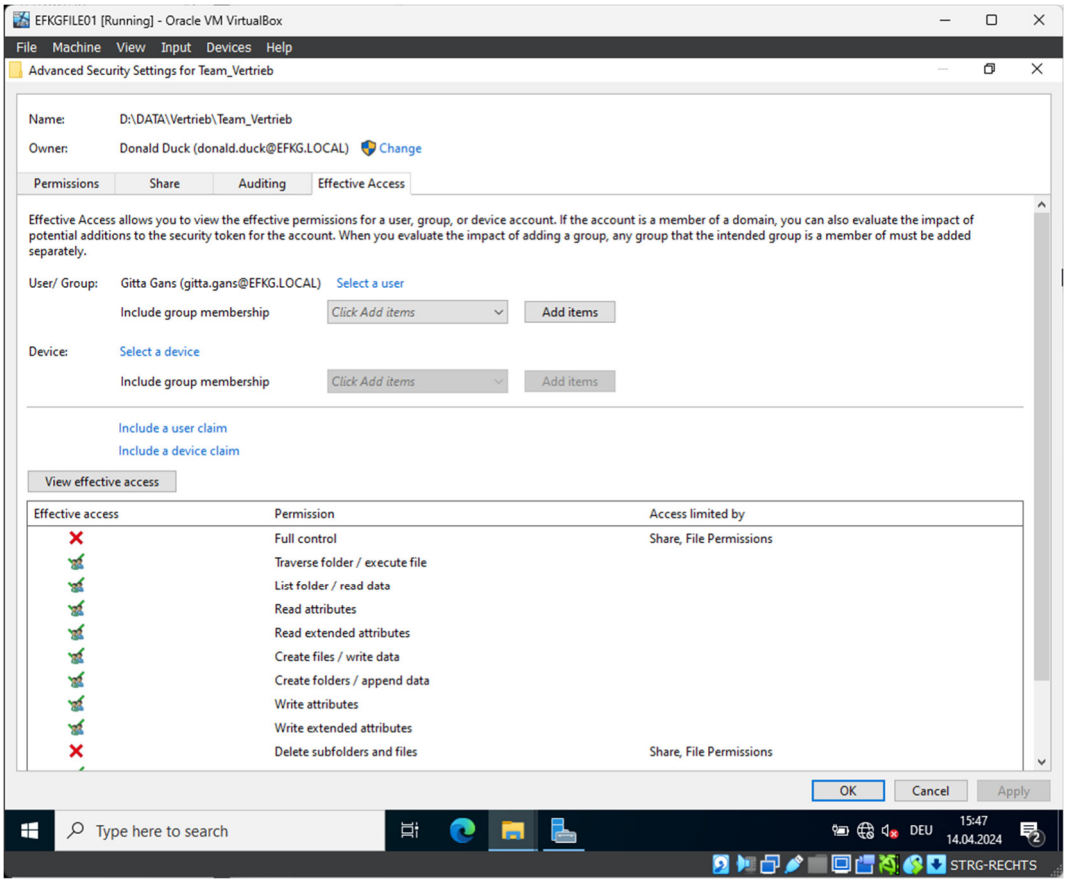


Gundel Gaukeley darf ändernd auf einen Planungsordner einer Abteilung zugreifen, die in ihren Zuständigkeitsbereich fällt.

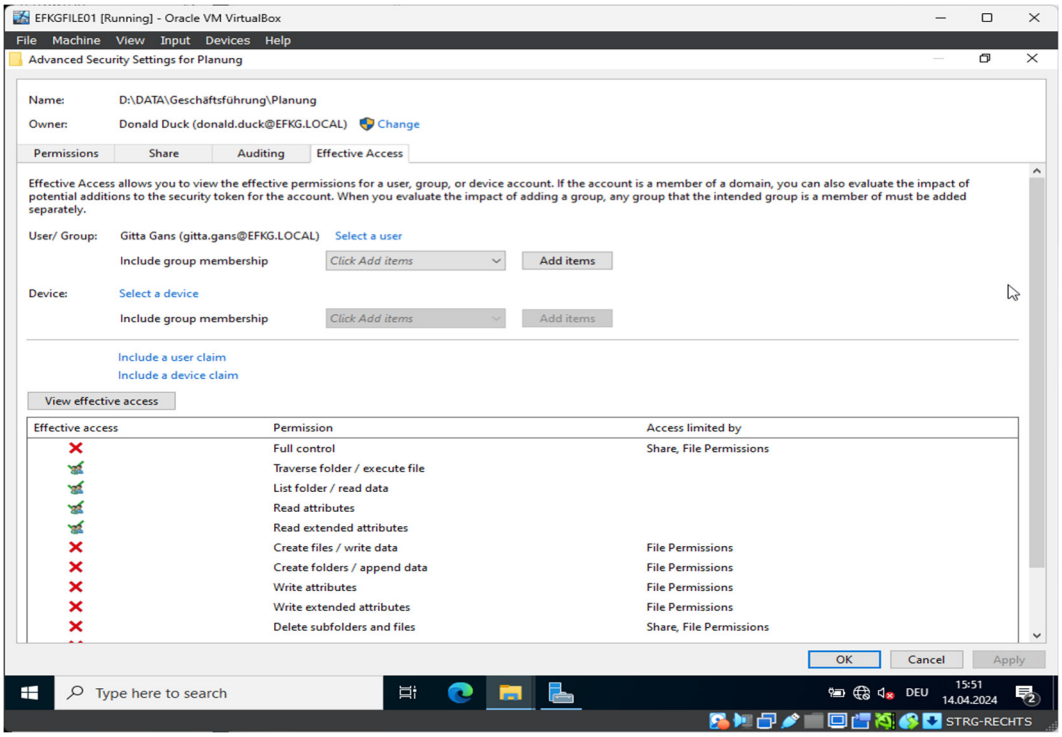
Die Funktionalität der Zugriffe weist die Wirksamkeit der Umsetzung nach. Der Nachweis gilt somit als erbracht.

5.4.3 Nachweis der Umsetzung der dritten Anforderung

Jede Abteilungsleitung darf ändernd auf alle Ordner des Fachbereichs zugreifen. Zusätzlich darf jede Abteilungsleitung lesend auf die Planungsordner der GF zugreifen.



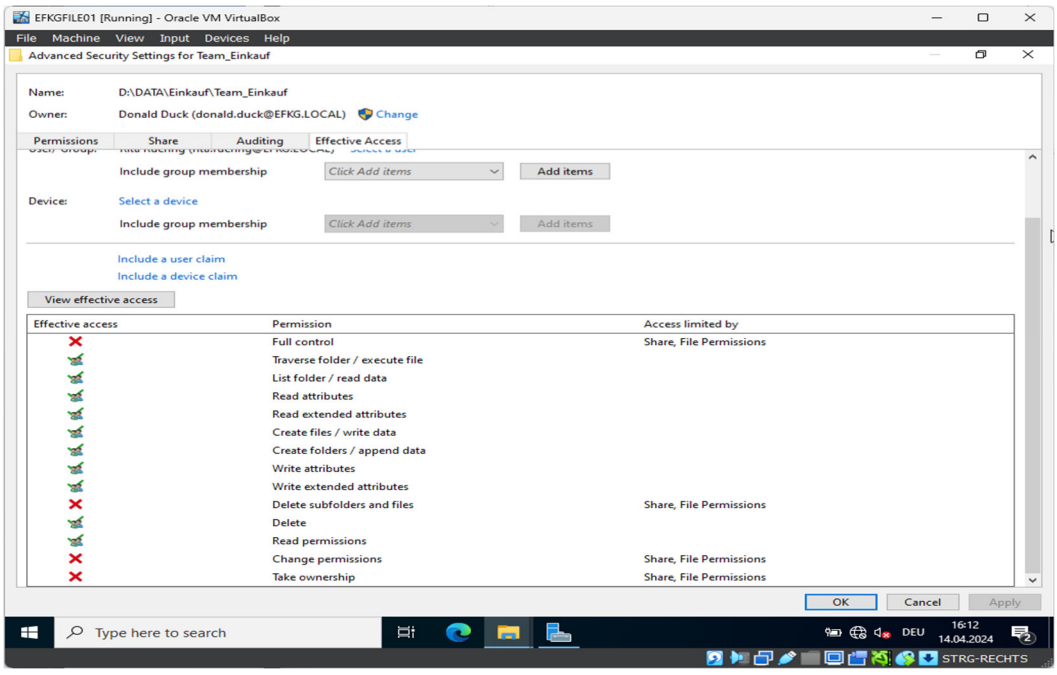
Gitta Gans hat als AL einen ändernden Zugriff auf einen beliebigen Ordner in ihrer Abteilung.



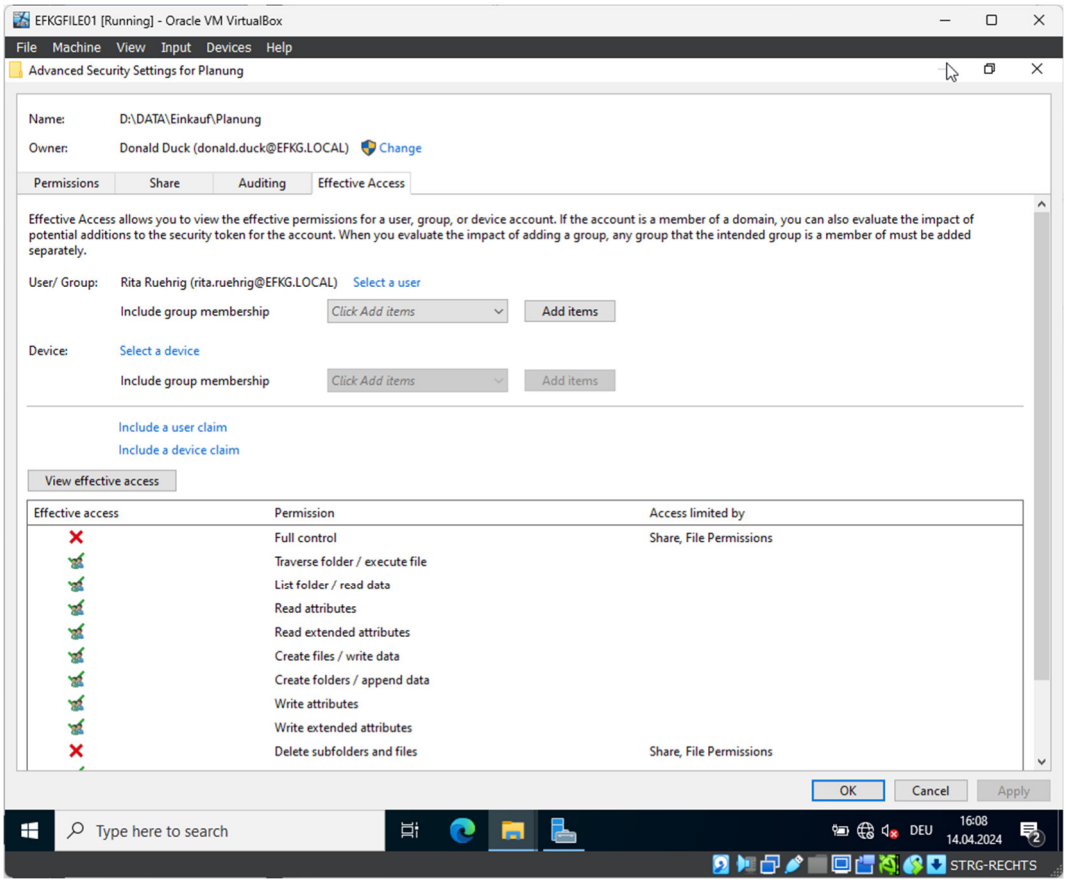
Gitta erhält lesenden Zugriff auf den Planungsordner der GF. Über die Umsetzung wurde der Nachweis erbracht.

5.4.4 Nachweis der Umsetzung der vierten Anforderung

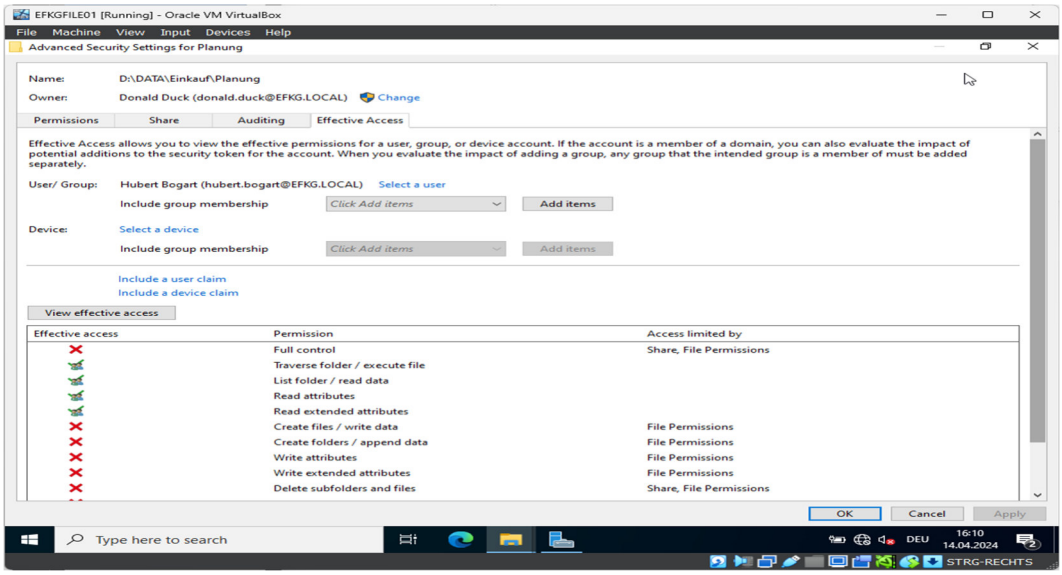
Jeder Mitarbeiter darf ändernd auf den Teams-Ordner zugreifen sowie lesend auf den Planungsordner. Ist der Mitarbeiter gleichzeitig Stellvertreter der AL, bekommt er / sie ändernden Zugriff auf den Planungsordner.



Rita Rührig erhält ändernden Zugriff auf den Teams-Ordner ihrer Abteilung.



Die Stellvertreterreglung sieht vor, das Rita Rührig ändernden Zugriff auf den Planungsordner der Abteilung bekommt.

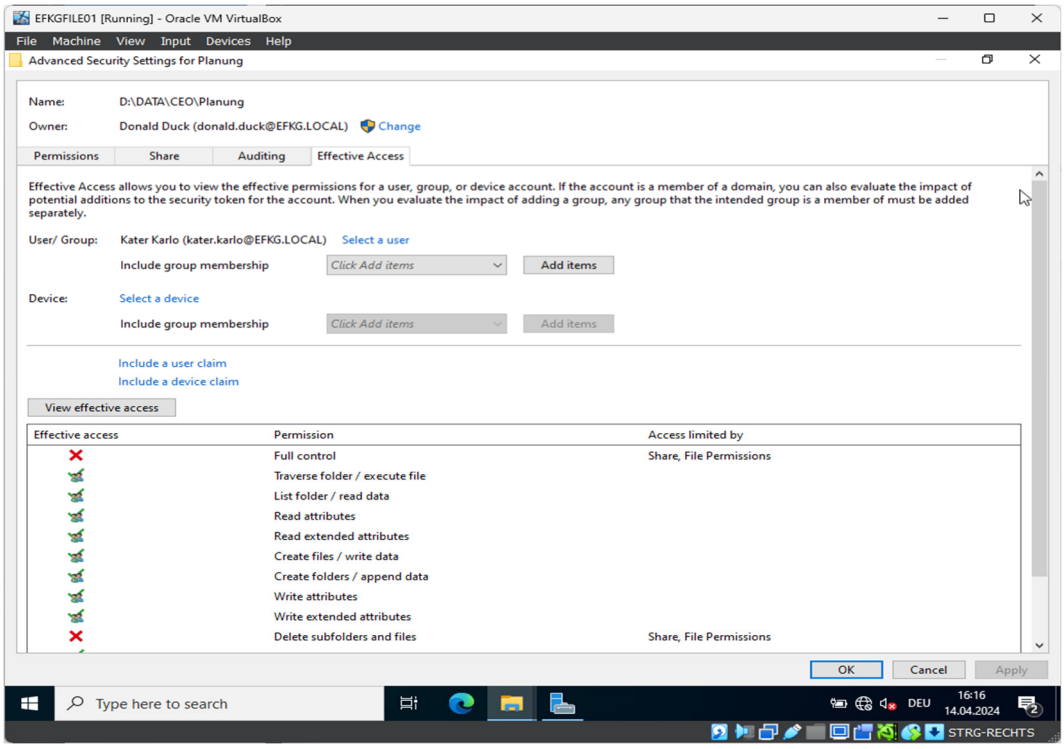


Hubert Bogart bekommt lediglich lesenden Zugriff auf das Planungsverzeichnis.

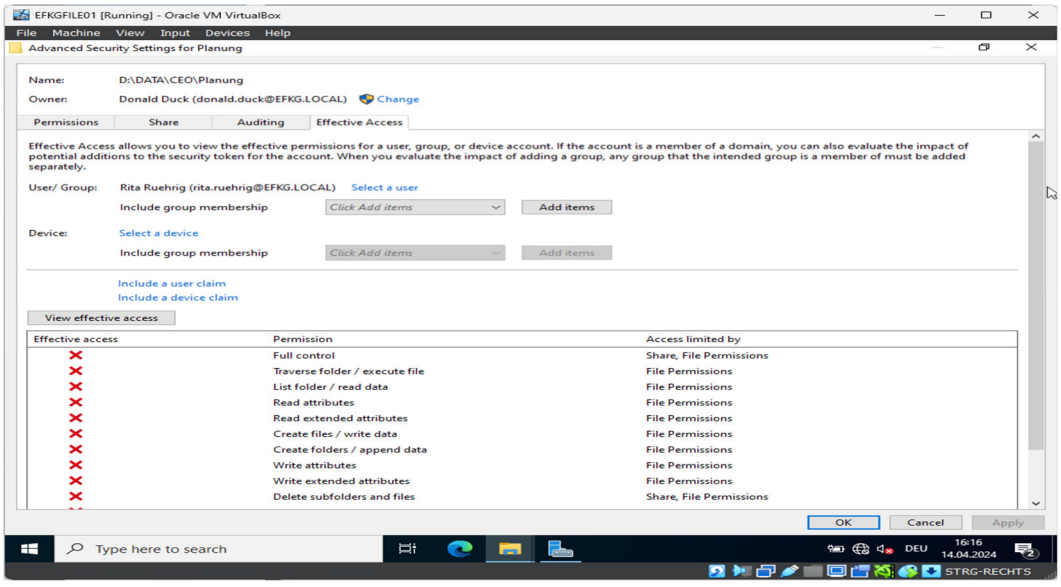
Die Funktionalität der Zugriffe und der Vertreterreglung sind nachgewiesen, somit gilt die Anforderung als umgesetzt.

5.4.5 Nachweis der Umsetzung der fünfte Anforderung

Sonderreglung: Dagobert vertraut in höchstem Maße der Leitung der Administration und gewährt deshalb ändernden Zugriff auf seine Planungsdaten.



Kater Karlo erhält die Änderungsberechtigung für Dagoberts Planungsverzeichnis.



Rita Rührig erhält keinerlei Zugriffe auf Dagoberts Planungsverzeichnis. Somit gilt auch die letzte Maßnahme als erwiesen umgesetzt.

Zusammenfassend wurden im Rahmen dieser Arbeit die Grundsätze des AGDLP-Modells (Accounts, Global Groups, Domain Local Groups, Permissions) erfolgreich umgesetzt. Die Anforderungen wurden definiert, die entsprechenden Gruppenstrukturen wurden entworfen und implementiert, und die Zuweisung von Berechtigungen wurde gemäß dem AGDLP-Prinzip durchgeführt. Der Nachweis dieser Umsetzung erfolgte anhand konkreter Beispiele und mithilfe des Tools "Effektive Berechtigungen" auf einem Windows Server. Die erfolgreiche Implementierung des AGDLP-Modells stellt eine solide Grundlage für eine effektive Zugriffsverwaltung dar.

Kapitel 6 Lessons learned

Die Implementierung des AGDLP-Modells zur Zugriffsverwaltung erwies sich als eine komplexe und herausfordernde Aufgabe, die sowohl technische als auch organisatorische Aspekte umfasste. Während des Prozesses wurden eine Reihe von Lehren gezogen, die eine tiefere Einsicht in die Bedeutung der klaren Rollenverteilung, effektiven Kommunikation und kontinuierlichen Verbesserung bieten.

6.1 Herausforderungen und Widerstände während der Implementierung

Die Implementierung des AGDLP-Modells war von verschiedenen Herausforderungen geprägt, die den Prozess beeinträchtigten und zusätzliche Anstrengungen erforderten. Insbesondere traten Verständigungsprobleme aufgrund unterschiedlicher Interpretationen der Rollenverteilung auf. Einige Teammitglieder hatten Schwierigkeiten, die konzeptionelle Tiefe des Modells zu erfassen, und waren daher nicht in der Lage, die Vorteile einer klaren Rollenstruktur zu erkennen. Dies führte zu Unklarheiten und Diskussionen über die optimale Verteilung von Berechtigungen, was den Implementierungsprozess verzögerte.

Darüber hinaus stieß das Projekt auf Widerstand seitens einiger Teammitglieder sowie auf eine gewisse Uneinigkeit über die Rollenverteilung. Einige Mitarbeiter waren besorgt darüber, dass das AGDLP-Modell ihre bisherigen Zugriffsrechte beeinträchtigen könnte, während andere die Notwendigkeit der Veränderung nicht eindeutig erkannten. Diese Differenzen führten zu Verzögerungen und zusätzlichen Diskussionen, die den Fortschritt behinderten und die Ressourcen belasteten.

Ein weiteres Hindernis war die unzureichende Unterstützung seitens der Geschäftsführung. Obwohl die Vorteile des AGDLP-Modells klar kommuniziert wurden, gab es immer wieder Bedenken seitens der Geschäftsführung bezüglich der Auswirkungen auf bestehende Prozesse und den damit verbundenen Aufwand für die Umstellung. Dies führte zu einem Mangel an finanziellen und personellen Ressourcen, was die Implementierung zusätzlich erschwerte.

Beispiel: In einem Team gab es Diskussionen darüber, wie die Berechtigungen für bestimmte Ressourcen aufgeteilt werden sollten. Einige Teammitglieder waren der Meinung, dass ihre bestehenden Zugriffsrechte ausreichend waren und keine Änderungen erforderlich seien, während andere darauf bestanden, dass eine klare Rollenverteilung die Sicherheit und Effizienz des Systems verbessern würde.

6.2 Vorteile und Erleichterungen nach der Implementierung

Trotz der anfänglichen Herausforderungen brachte die erfolgreiche Implementierung des AGDLP-Modells zahlreiche Vorteile mit sich. Sobald das Modell umgesetzt war, erleichterte es die Zuweisung von Benutzerrollen und Berechtigungen erheblich. Die klare Gruppenstruktur und das AGDLP-Prinzip ermöglichten eine effiziente Verwaltung von Berechtigungen und eine einfache Anpassung an sich ändernde Anforderungen. Selbst komplexe Umstrukturierungen des Zugriffsmanagements konnten durchgeführt werden, wenn auch mit einem gewissen Aufwand. Die klare Rollenverteilung erleichterte es den Administratoren, den Überblick über die Zugriffsrechte zu behalten und sicherzustellen, dass nur autorisierte Benutzer auf sensible Daten zugreifen konnten.

Die Verschachtelung von Gruppen und die Anwendung des AGDLP-Modells ermöglichten auch eine effektive Implementierung von rollenbasiertem Dateizugriff. Durch die klare Definition von Benutzerrollen und Berechtigungen konnten Administratoren mühelos neue Benutzer erstellen und ihnen die entsprechenden Rollen zuweisen. Dies führte automatisch zur Festlegung der Berechtigungen entsprechend den definierten Rollen, was den Verwaltungsaufwand erheblich reduzierte und die Einhaltung von Sicherheitsrichtlinien erleichterte.

Skeptische Teammitglieder und Benutzer, die anfänglich Bedenken gegenüber dem AGDLP-Modell hatten, wurden bei der Implementierung in vielerlei Hinsicht positiv überrascht. Durch den direkten Einsatz des Modells konnten sie erkennen, wie effizient und sicher die Zugriffsverwaltung sein kann. Die klare Rollenstruktur und die automatisierte Zuweisung von Berechtigungen überzeugten selbst die größten Skeptiker von den Vorteilen des AGDLP-Ansatzes. Dies führte zu einer breiteren Akzeptanz und Unterstützung innerhalb des Teams und trug dazu bei, den Implementierungsprozess erfolgreich abzuschließen.

Beispiel: Einige Teammitglieder hatten Bedenken hinsichtlich der Komplexität und des Aufwands, der mit der Umstellung auf das AGDLP-Modell verbunden sein könnte. Als jedoch deutlich wurde, wie einfach es war, Benutzer zu erstellen und ihnen Rollen zuzuweisen, ohne dass komplexe Berechtigungskonfigurationen erforderlich waren, wurden ihre Bedenken zerstreut. Die Möglichkeit, schnell auf Änderungen zu reagieren und neue Benutzer nahtlos in das System zu integrieren, überzeugte selbst die skeptischsten Mitglieder von den Vorteilen des AGDLP-Modells.

6.3 Empfehlungen

Die Implementierung des AGDLP-Modells bot wichtige Erkenntnisse und Lehren, die für zukünftige Projekte von Nutzen sein können:

- ✓ Klare Kommunikation und Einbindung aller Stakeholder sind entscheidend für den Erfolg eines Implementierungsprojekts. Dies umfasst die Erklärung der Ziele, Vorteile und Auswirkungen der Veränderungen.
- ✓ Die Unterstützung der Geschäftsführung ist von entscheidender Bedeutung, um Widerstände zu überwinden und die Ressourcen für die Implementierung bereitzustellen.
- ✓ Ein sorgfältiges Training ist erforderlich, um die Mitarbeiter auf Veränderungen vorzubereiten und sicherzustellen, dass sie die neuen Prozesse und Richtlinien akzeptieren und umsetzen.
- ✓ Die kontinuierliche Überprüfung und Anpassung des Zugriffsmanagements ist unerlässlich, um sicherzustellen, dass die Sicherheitsanforderungen erfüllt und die Effizienz der Zugriffsverwaltung maximiert werden.

Schlussfolgerungen:

Die Implementierung des AGDLP-Modells war nicht nur ein technisches Projekt, sondern auch eine organisatorische Veränderung, die eine klare Rollenverteilung und effektive Kommunikation erforderte. Die Herausforderungen, die während des Prozesses auftraten, boten wichtige Lektionen für die Zukunft. Durch die Überwindung von Widerständen und die erfolgreiche Umsetzung konnten wertvolle Erkenntnisse gewonnen werden, die als Grundlage für zukünftige

Projekte dienen können. Die Flexibilität und Effizienz des AGDLP-Modells haben gezeigt, dass eine klare Rollenstruktur und eine effektive Zugriffsverwaltung entscheidend für die Sicherheit und Effizienz von IT-Systemen sind.

Anhang

Inhaltsverzeichnis

1. Installation der virtuellen Umgebung (Teil 1)

Die Implementierung der virtuellen Umgebung für das Rollen-basierte Dateizugriffssystem erfolgt unter Verwendung der VirtualBox-Virtualisierungsplattform, wobei alle virtuellen Maschinen auf dem Windows Server 2022-Betriebssystem basieren. Da der Installationsprozess des Betriebssystems für die Erläuterung des Rollen-basierten Dateizugriffssystems nicht relevant ist, wird darauf verzichtet, diesen zu beschreiben.

Nach der erfolgreichen Installation des Windows Server 2022-Betriebssystems auf den virtuellen Maschinen beginnt der Prozess mit der Einrichtung des Active Directory-Dienstes. Dieser Schritt markiert den Beginn der Domänenkonfiguration, die für das Rollen-basierte Dateizugriffssystem von entscheidender Bedeutung ist.

1.1. Einrichtung des DC (Domain Controller)

Konfiguration (verkürzt):

Name des DC: EFKGDC01

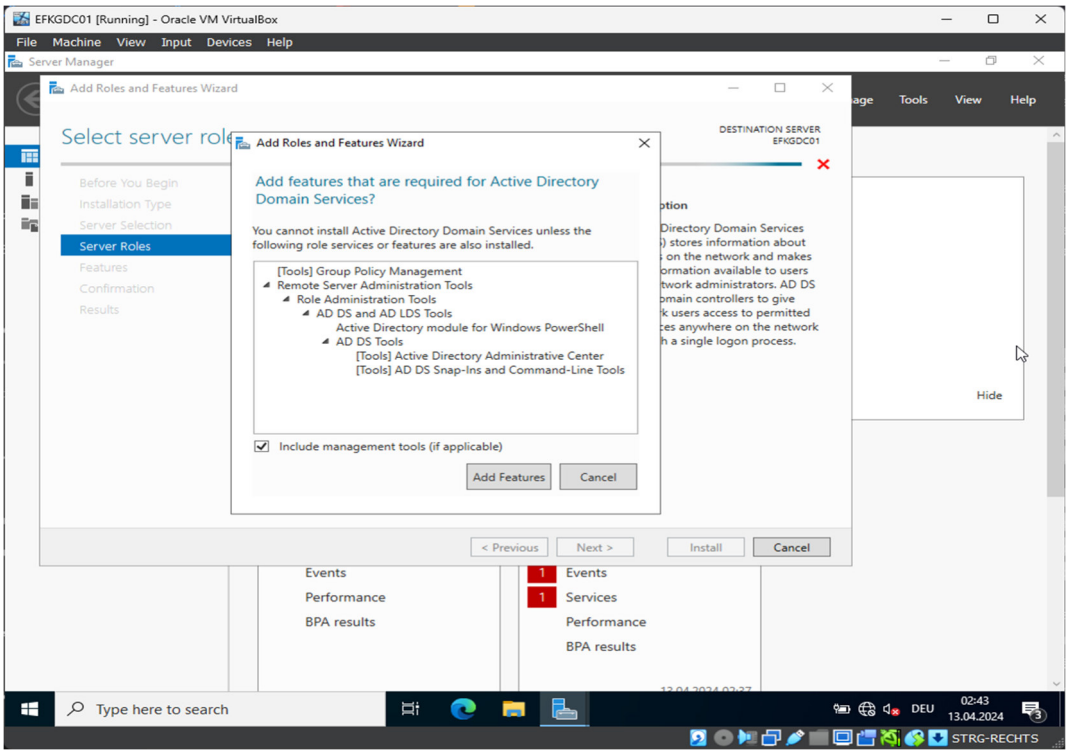
Installierte Rollen nach Fertigstellung:

Active Directory Domain Services, Domain Name Services

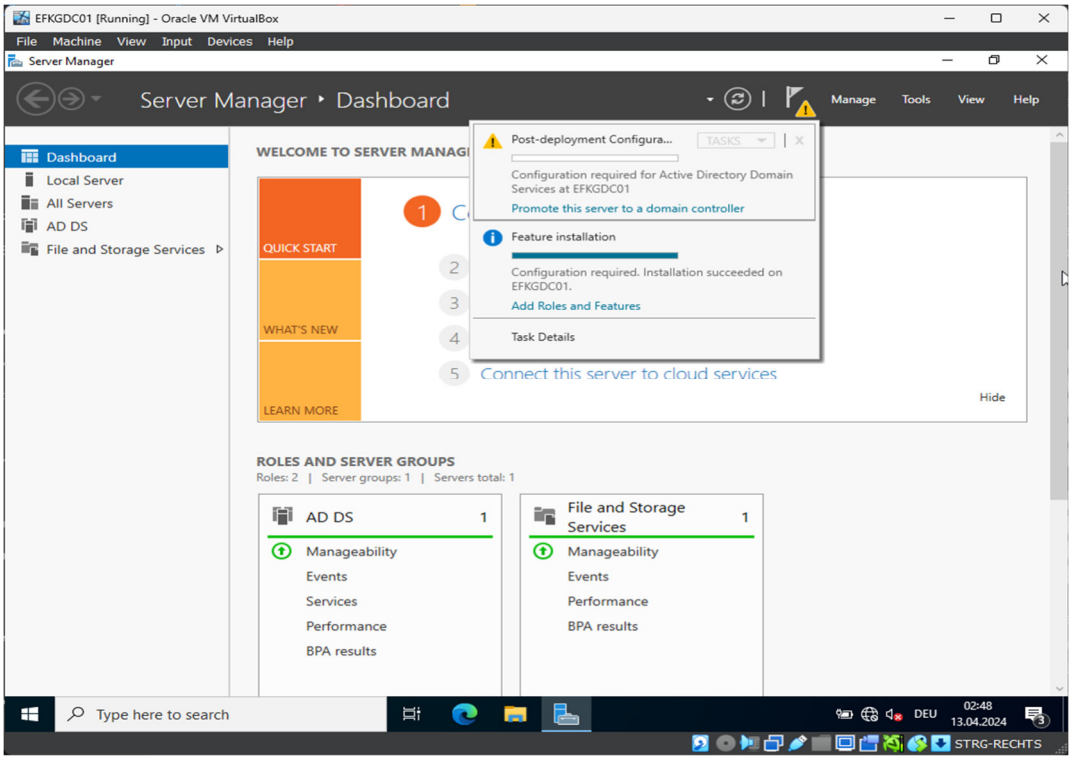
IP-Konfiguration:

IP: 192.168.0.1 / 24 Gateway: 192.168.0.254 (nicht nötig aber eingetragen) DNS: 192.168.0.1

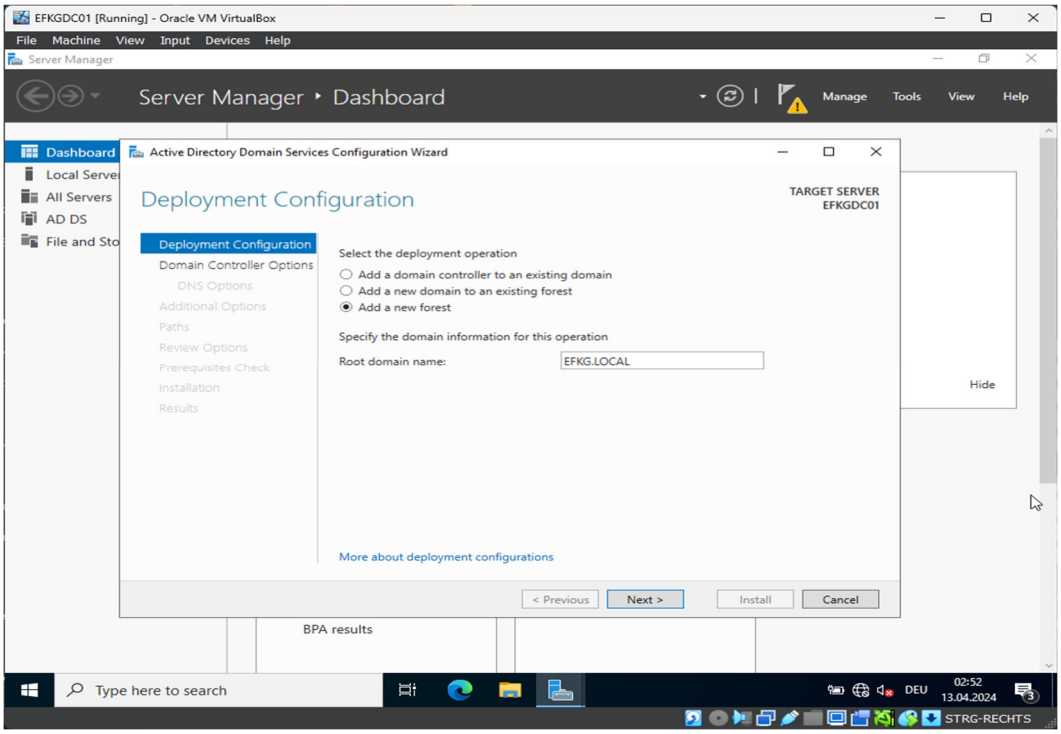
1.1.1. Installation und Konfiguration der Rolle Active Directory Domain Services



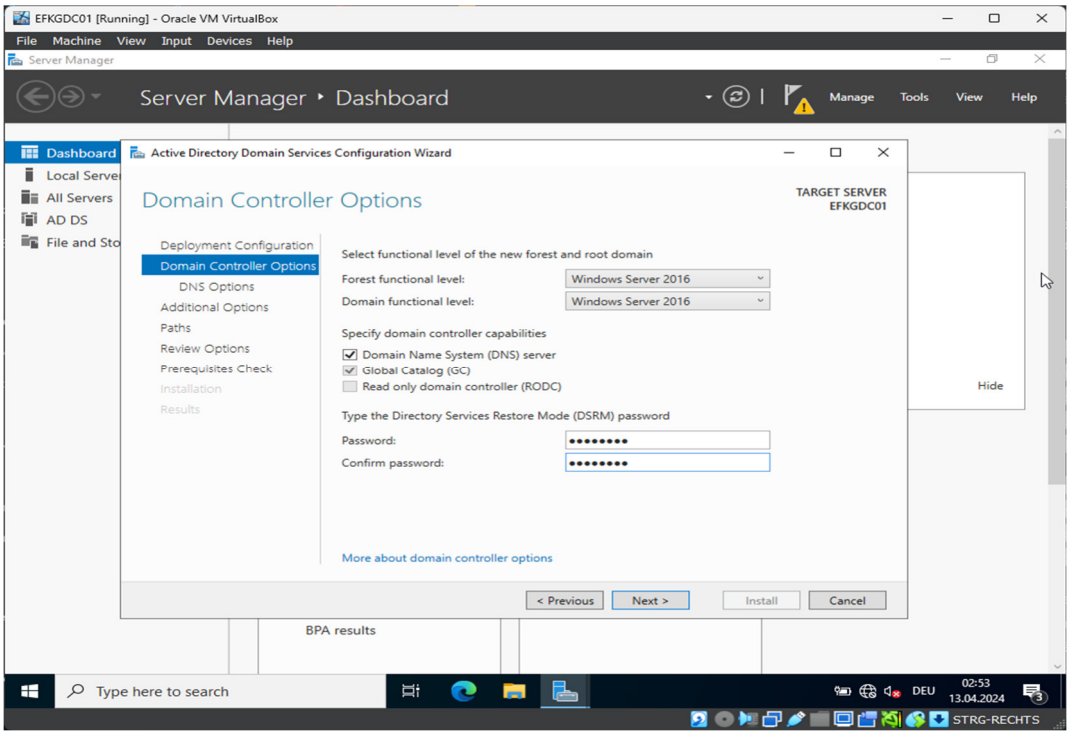
Nach der Installation der Rolle kann die Konfiguration des Active Directory vorgenommen werden.



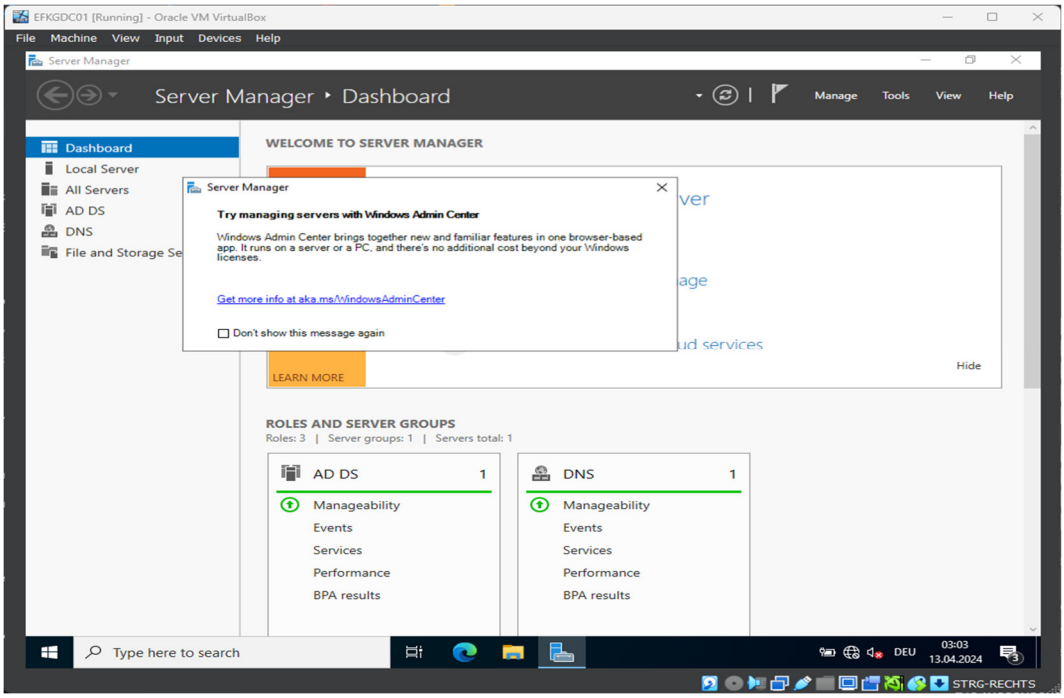
Der Name der Gesamtstruktur und auch Domainname wird auf EFKG.LOCAL festgelegt.



Der DC wird als globaler Katalog sowie DNS-Server konfiguriert. Das Passwort für den Restore Mode wird festgelegt.

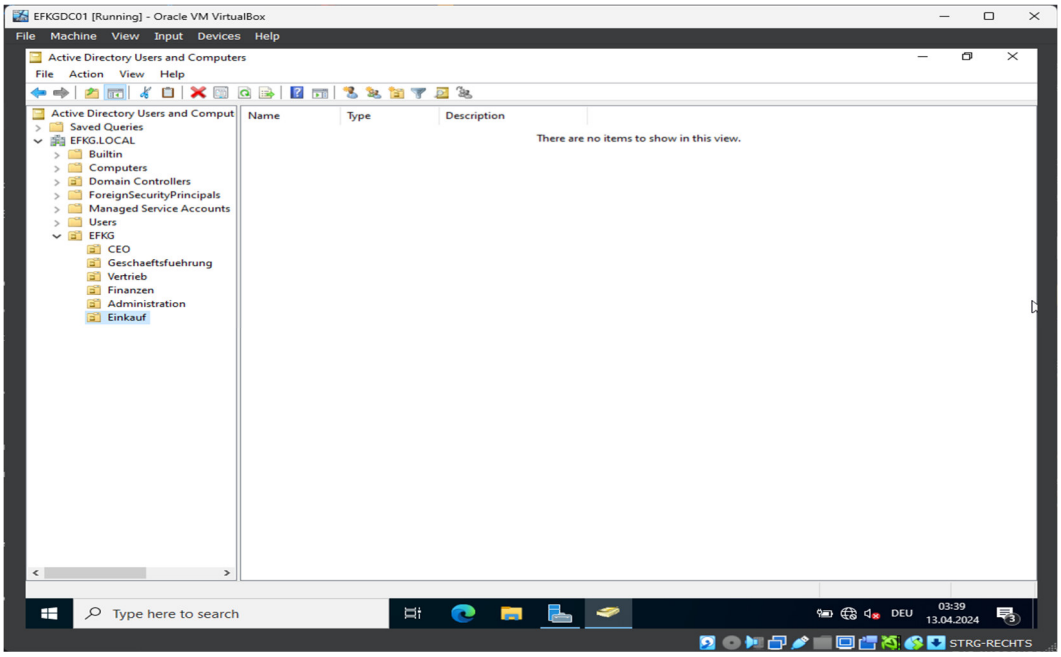


Alle weiteren Optionen werden in der Standardkonfiguration übernommen. Nach Abschluss der Konfiguration und Neustart sind die Dienste in Bereitschaft und zur Verwendung vorbereitet.

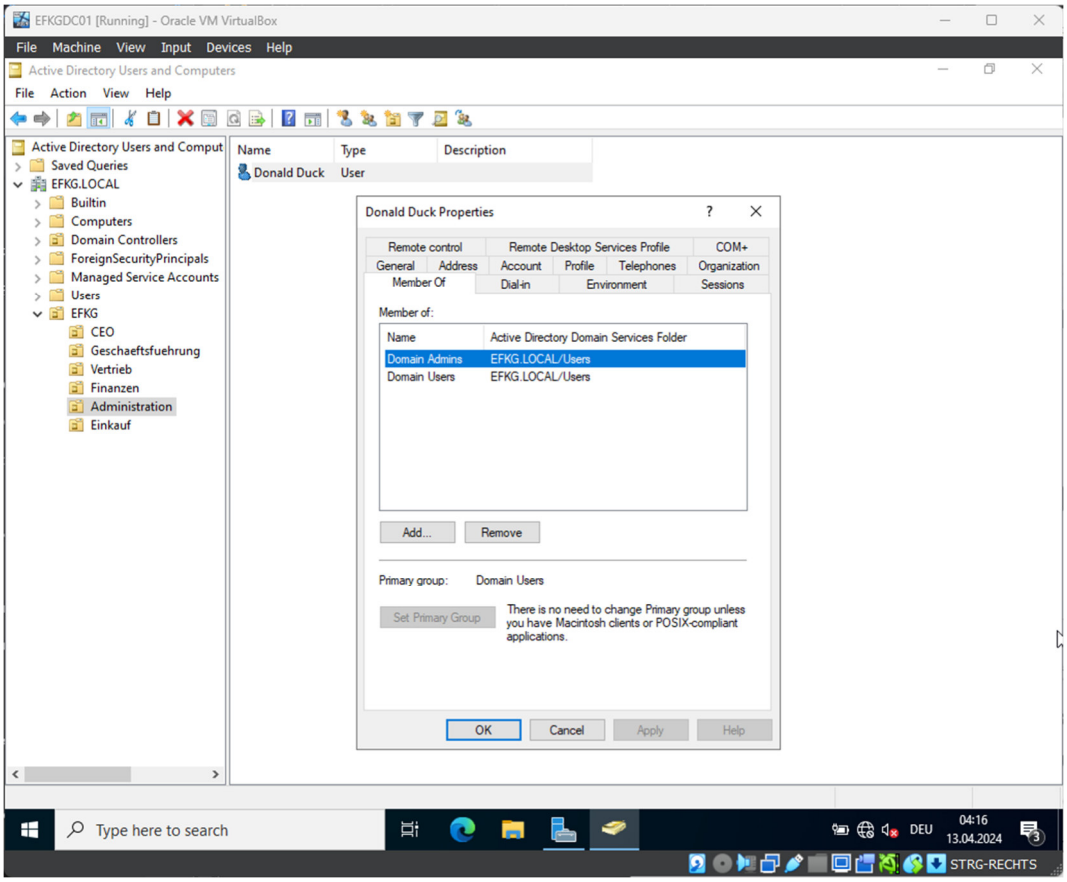


1.1.2. Anlegen der Container (Abteilungen) und im Active Directory

Im SnapIn ADUC (Active Directory Users and Computers) wird zuerst das Unternehmen abgebildet.



Da es unüblich ist, das Administratorkonto (welches der Gruppe Organisationsadministratoren angehört und somit überprivilegiert ist) zur Verwaltung zu verwenden, wird der Benutzer Donald Duck angelegt und der Gruppe der Domänenadministratoren hinzugefügt. Ein persönliches Laufwerk ist für Donald nicht notwendig.



Vor der Erstellung der anderen Benutzerkonten und der Festlegung zu schützender Ordner ist die Installation und Vorbereitung eines Fileservers erforderlich. Dies beinhaltet die Zuweisung eines zusätzlichen Datenträgers, der als Speicherort für die Daten fungiert. Darüber hinaus ist die Bereitstellung des USER-Volumes notwendig, da während der Benutzererstellung dynamisch deren persönliche Laufwerke "on-the-fly" generiert werden.

1.2. Installation des Fileservers

Konfiguration (verkürzt):

Name des DC: EFKGFILE01

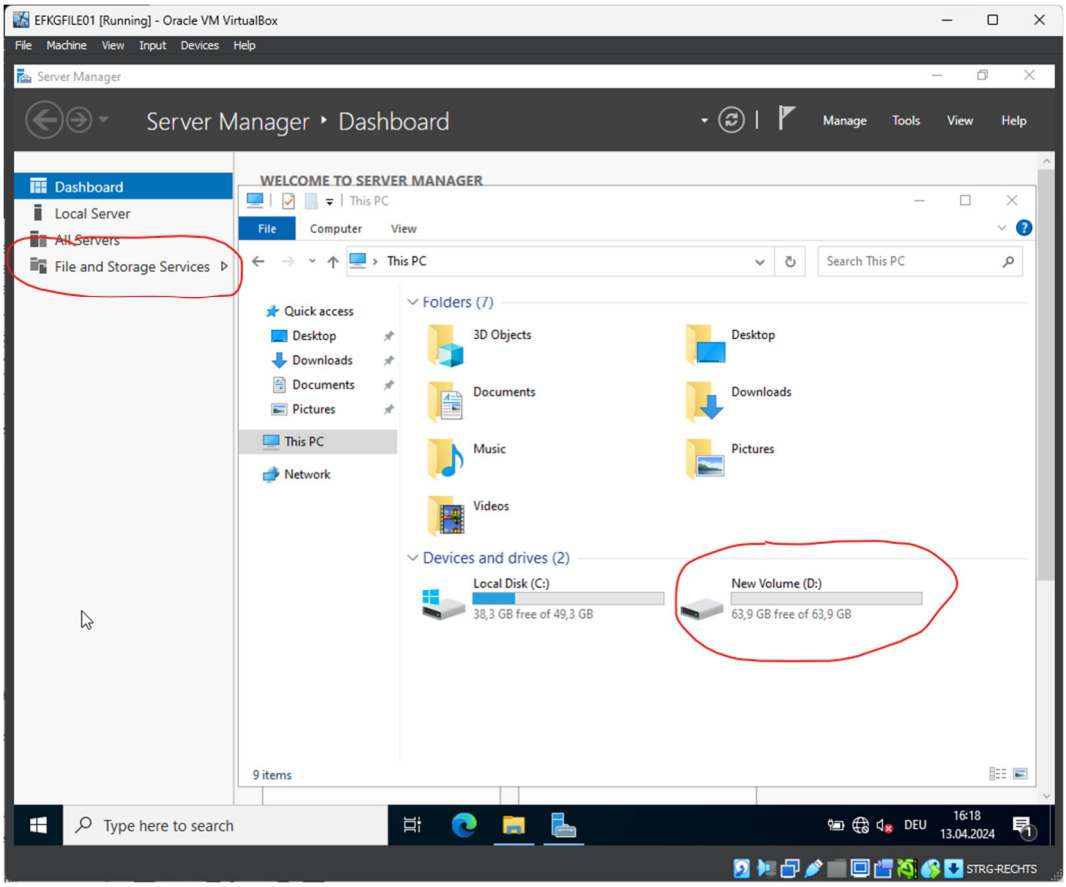
Installierte Rollen nach Fertigstellung:

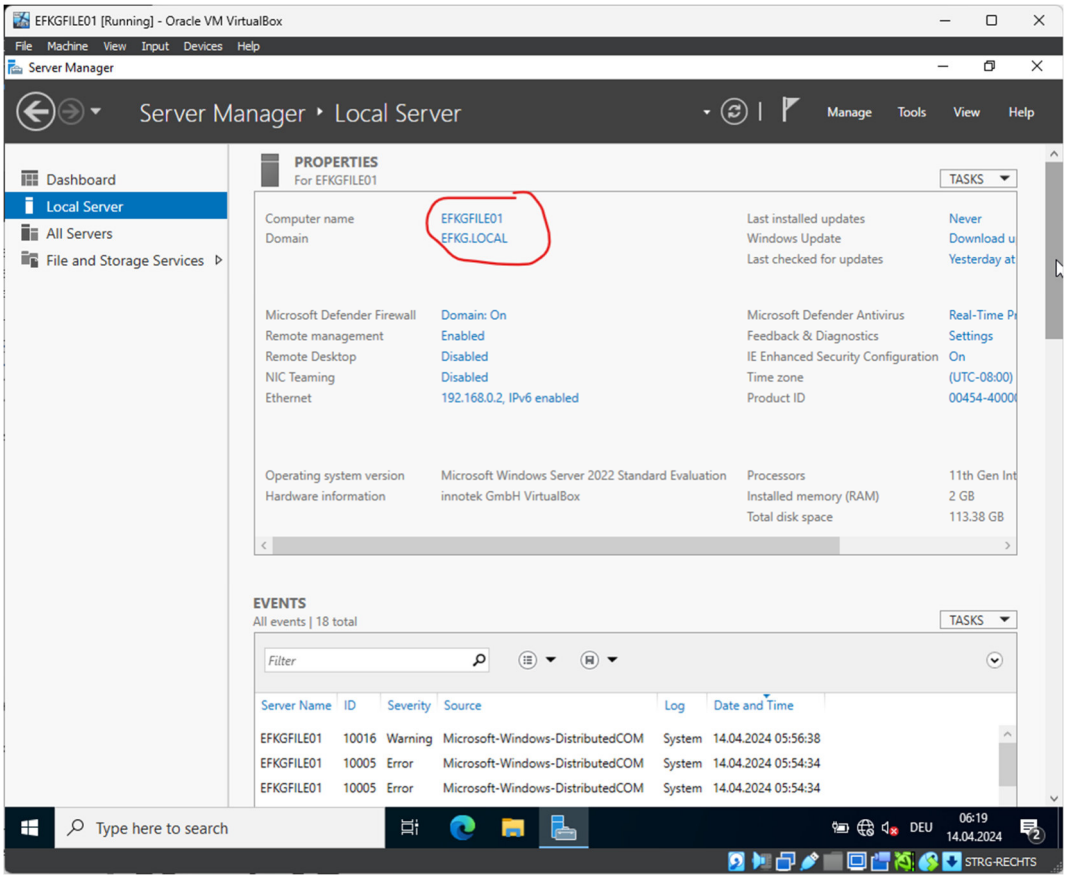
File and Print Services

IP-Konfiguration:

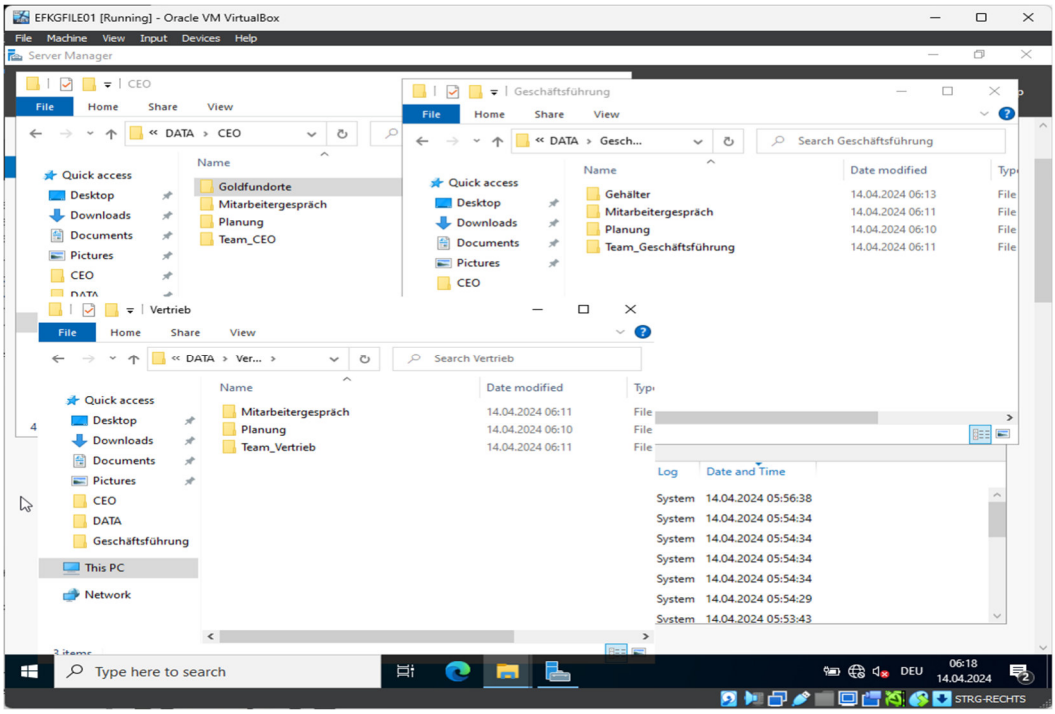
IP: 192.168.0.2 / 24 Gateway: 192.168.0.254 (nicht nötig aber eingetragen) DNS: 192.168.0.1

Die Serverkonfiguration kann auf das Wesentliche reduziert werden, da die erforderliche Serverrolle bereits vorinstalliert ist. Es ist lediglich erforderlich, wie bereits erwähnt, die zweite Festplatte einzurichten und den Mitgliedsstatus des Fileservers von einer Arbeitsgruppe auf ein Domänenmitglied zu ändern.

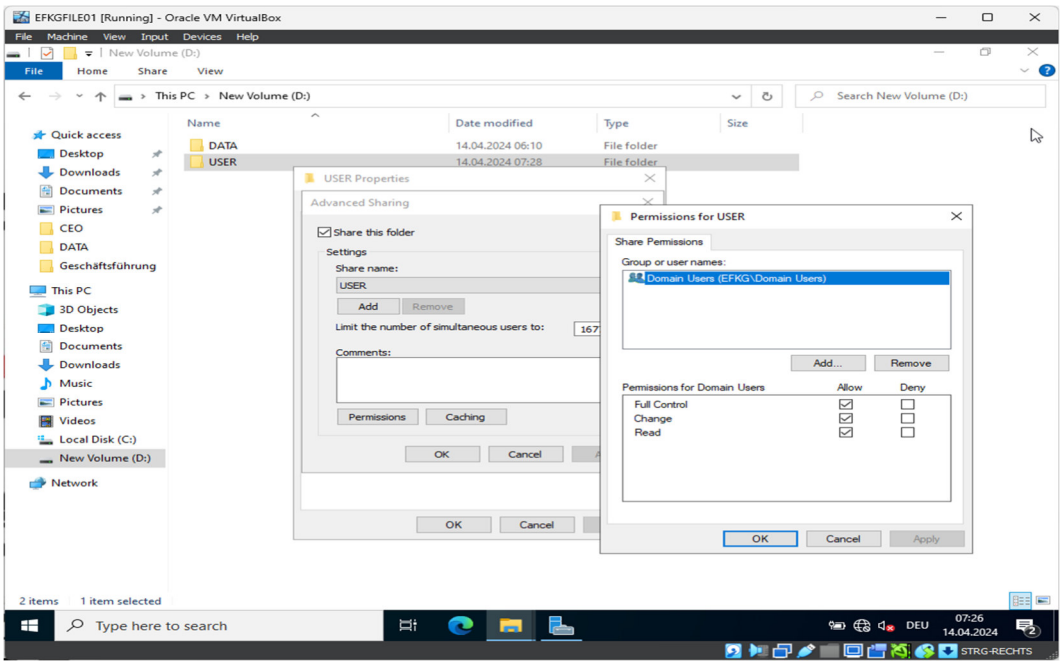




Die Ordnerstruktur wird nach Vorgabe eingerichtet.

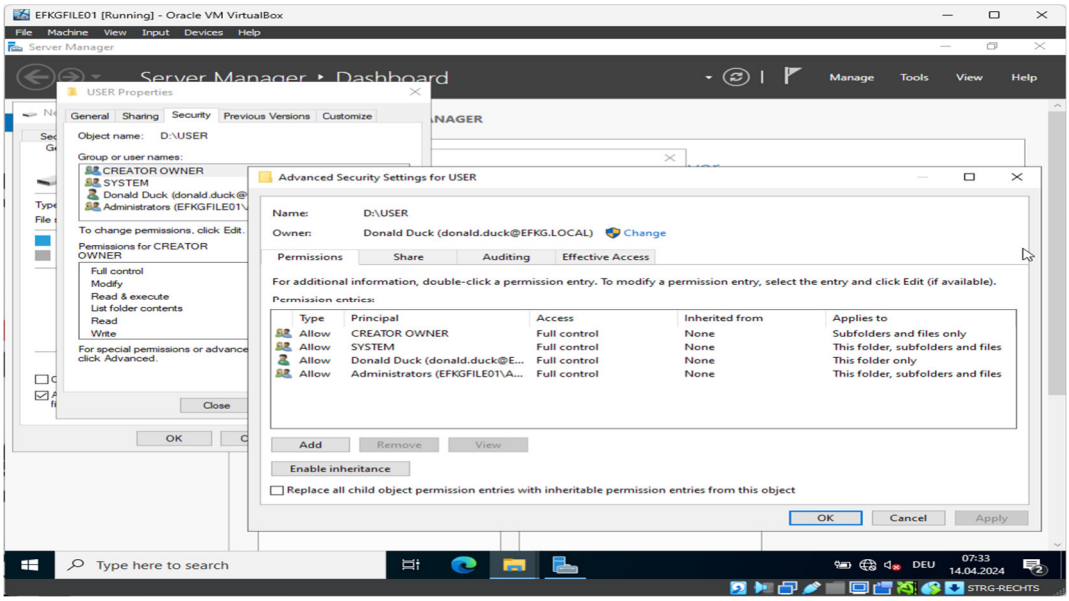


Zunächst sollen die Freigabe und die NTFS-Berechtigungen für das USER-Volume eingerichtet werden.



Die Freigabeberechtigung wird auf Domain Users mit Full Access festgelegt. Das versichert, dass kein Benutzer, der nur über ein lokales Konto auf diesem Fileserver verfügt, eine Remoteverbindung an diese Freigabe herstellen kann.

Die NTFS-Berechtigungen werden dahingehend angepasst, dass die vererbte Gruppe EFKGFILE01\USERS in den erweiterten Einstellungen entfernt wird.

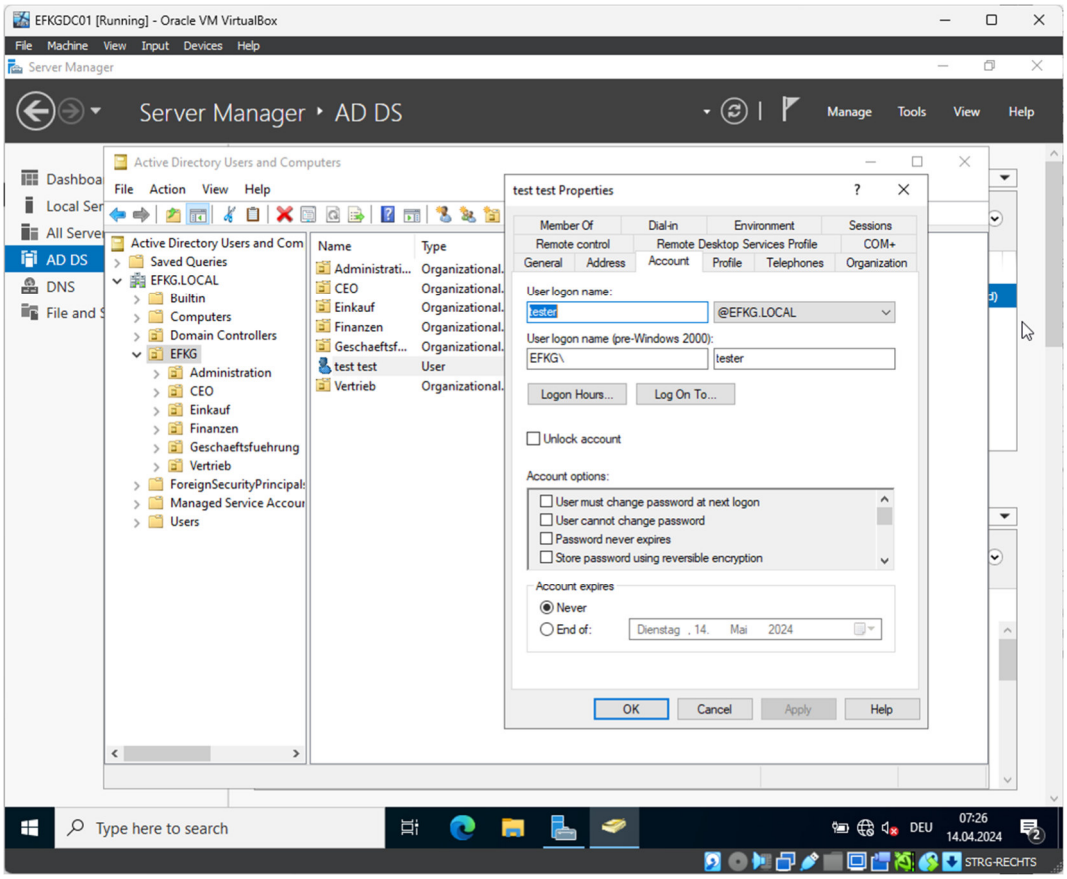


Der Erhalt der Creator / Owner – Gruppe garantiert, dass der bei der Benutzererstellung erstellte, persönliche Ordner die passenden Berechtigungen erhält.

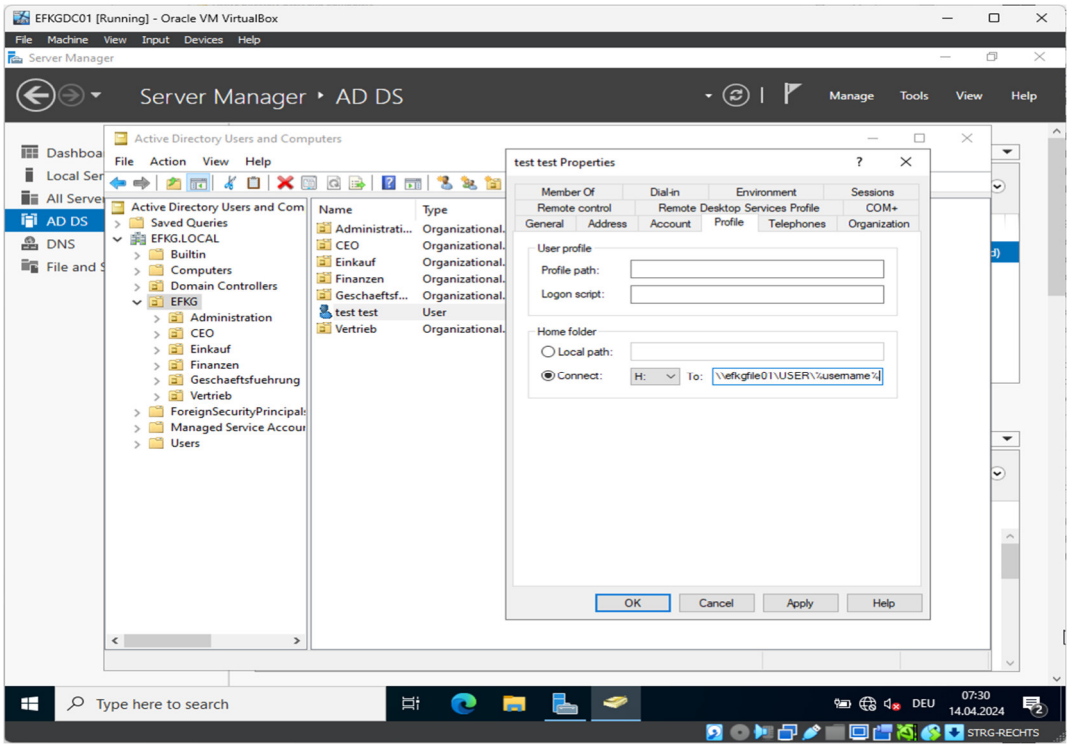
Damit endet dieser Abschnitt und es kann übergegangen werden zur Erstellung der Benutzerkonten.

1.3. Erstellen der Benutzerkonten (mit persönlichem Laufwerk)

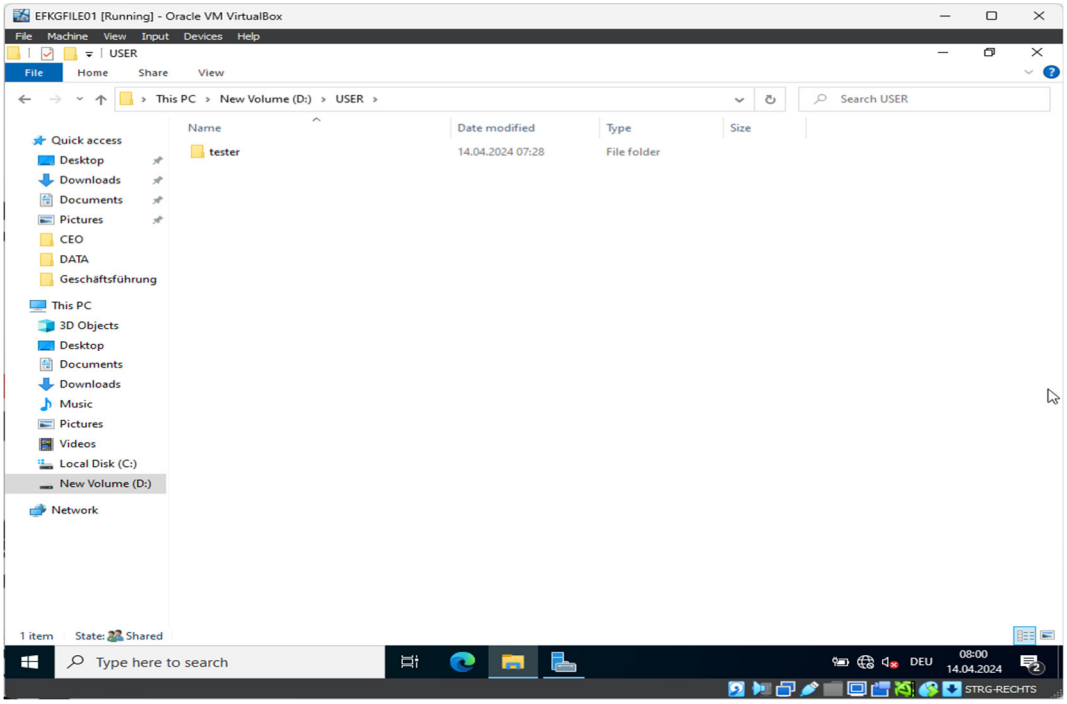
Zunächst soll ein Testbenutzer erstellt werden, mit dem die einwandfreie Funktion der Laufwerkserstellung überprüft werden kann.



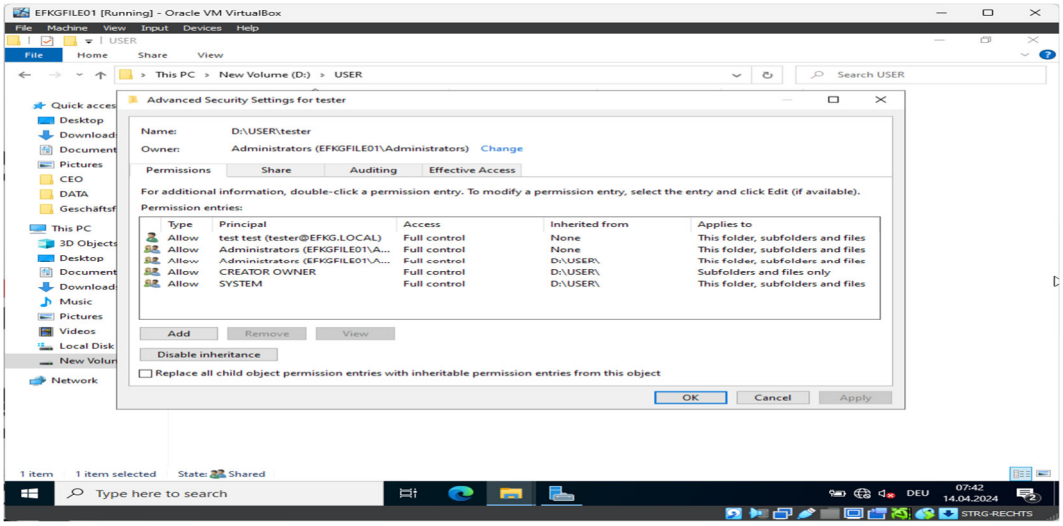
Das persönliche Laufwerk soll verbunden werden über den Laufwerkbuchstaben H:. Um sicher zu gehen, dass der Benutzerordner auch mit dem richtigen Benutzernamen angelegt wird, wird die Variable %USERNAME% bei der Laufwerksangabe verwendet.



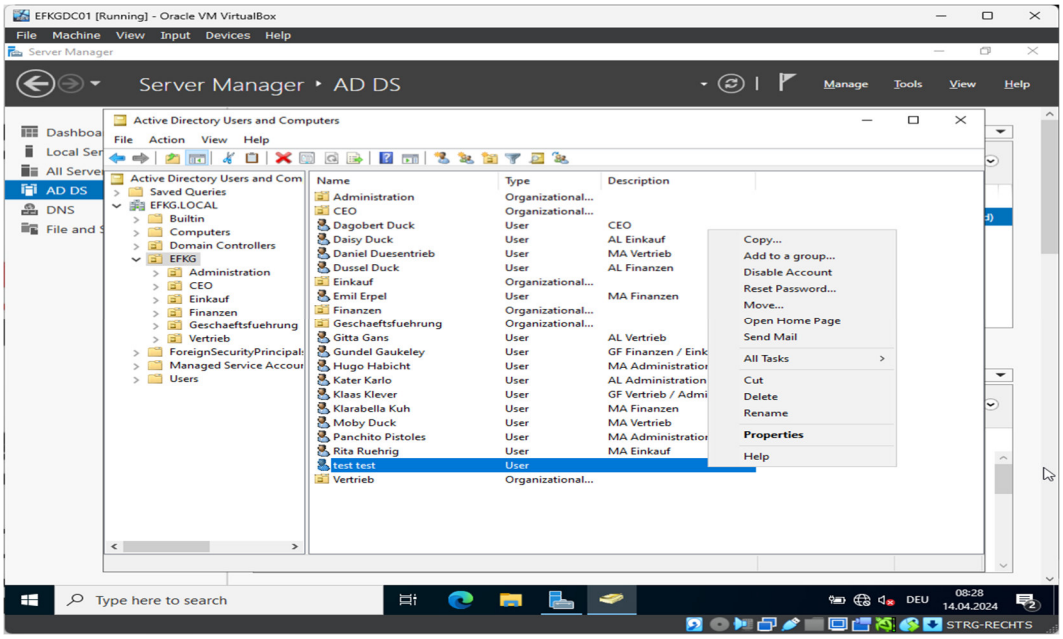
Nach Bestätigung der Einstellung erscheint der erstellte Benutzerordner im Verzeichnis USER auf dem Fileserver.

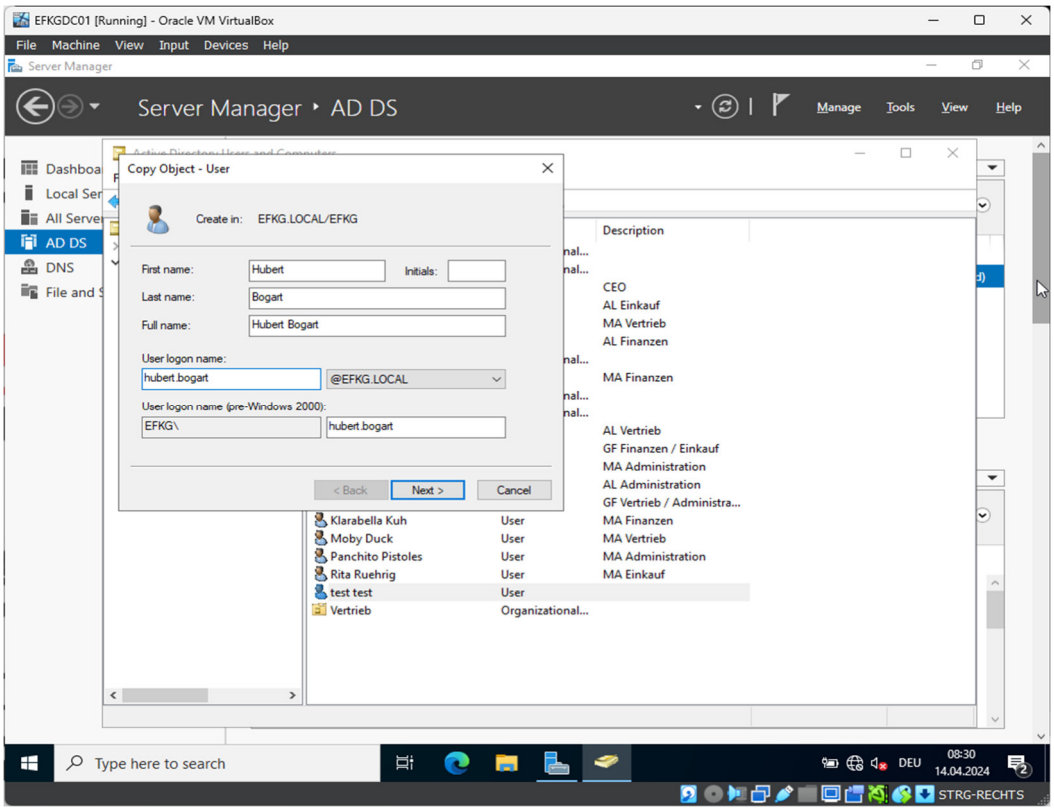


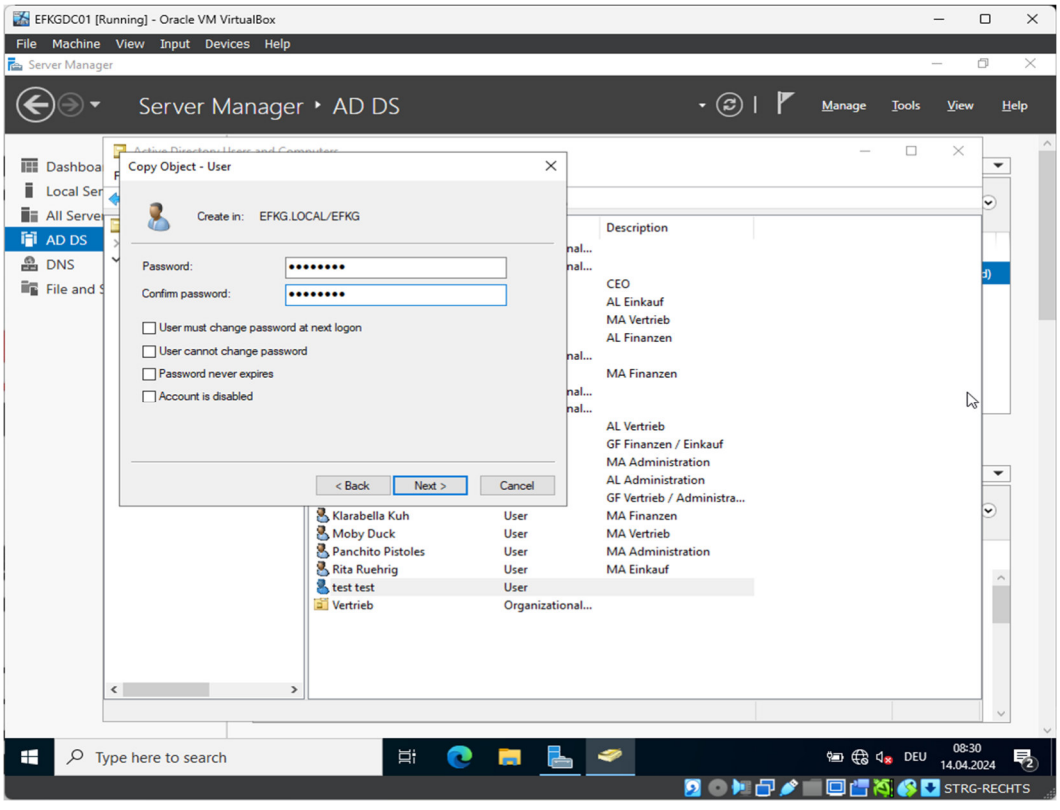
Die jeweiligen Zugriffsberechtigungen werden überprüft:

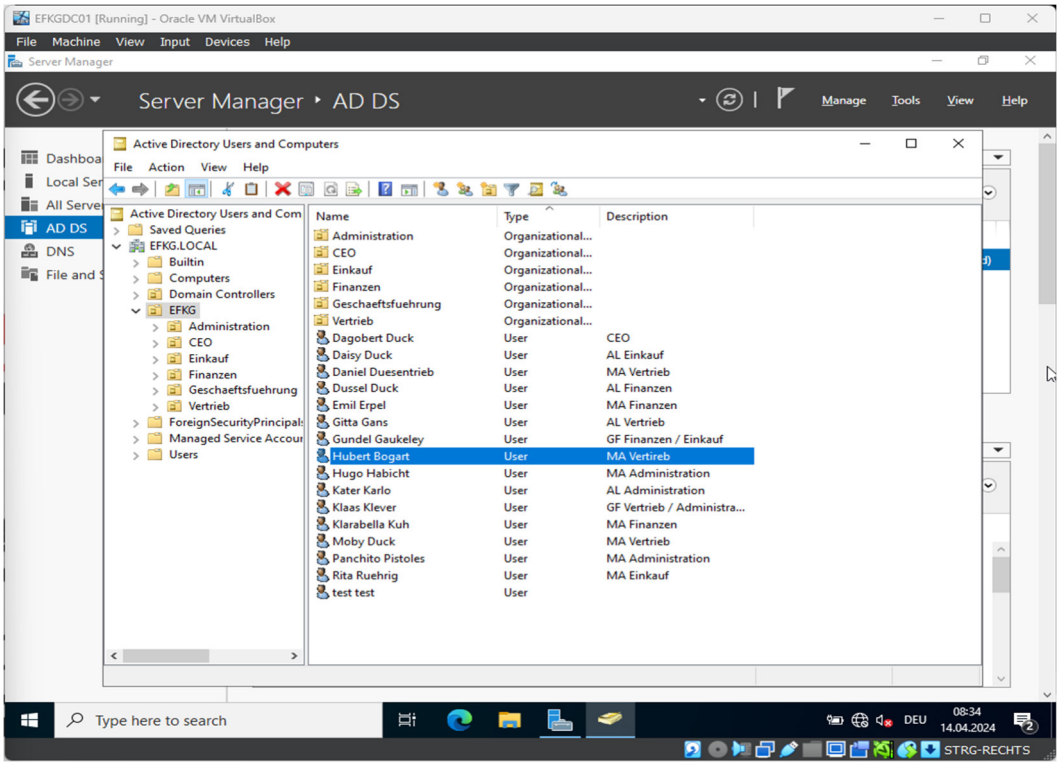


Letzteres bestätigt die Funktionalität und die Sicherheit der Einstellung. Somit kann nun mit der operativen Erstellung der Benutzer begonnen werden. Dazu wird eine Vorlage für einen Benutzer verwendet. In dieser Vorlage sind bestimmte Einstellungen festgelegt, wie z.B. der eben erstellte Pfad zum Benutzerlaufwerk. Aus dieser Vorlage werden dann die Benutzer erstellt. Der vorher erstellte Testbenutzer kann als Vorlage für neu anzulegende Benutzer dienen. Allerdings, um bei den späteren Tests nicht unnötig Passwörter ändern zum müssen vor der ersten Anmeldung, wird selbige Option in den Passwortoptionen deaktiviert.

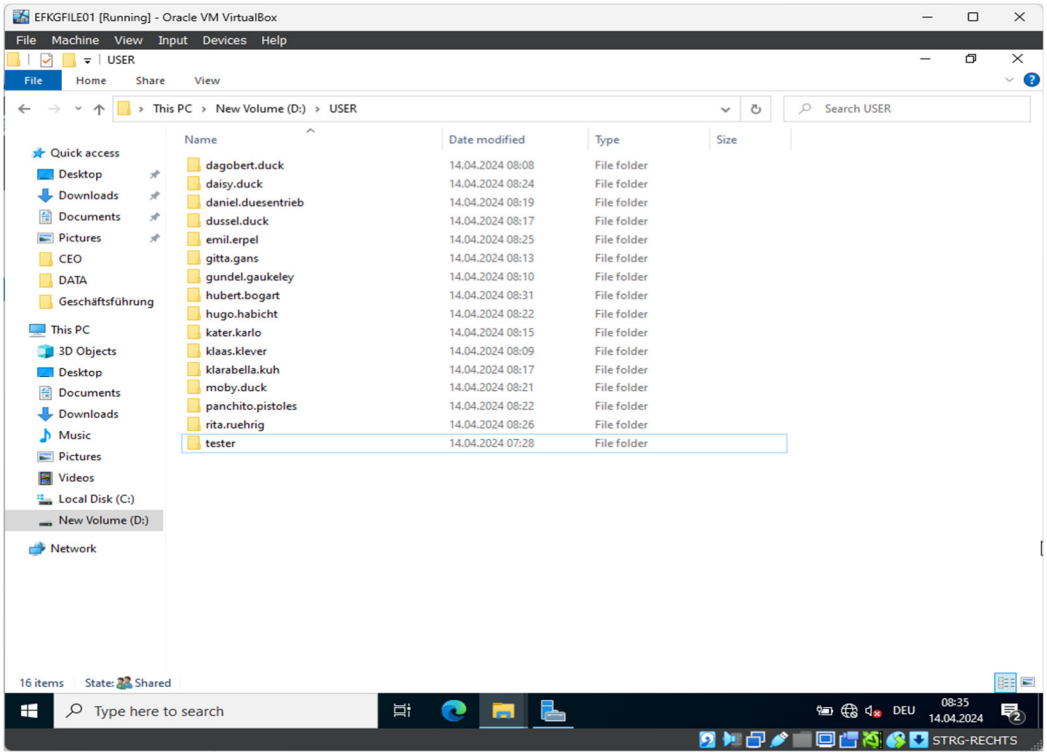



EFKGDC01 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • AD DS
Manage Tools View Help
Copy Object - User
Create in: EFKG.LOCAL/EFKG
First name: Hubert
Initials:
Last name: Bogart
Full name: Hubert Bogart
User logon name:
hubert.bogart
@EFKG.LOCAL
User logon name (pre-Windows 2000):
EFKG\
hubert.bogart
< Back
Next >
Cancel
Description
Klarabella Kuh User MA Finanzen
Moby Duck User MA Vertrieb
Panchito Pistoles User MA Administration
Rita Ruehrig User MA Einkauf
test test User
Vertrieb Organizational...
CEO
AL Einkauf
MA Vertrieb
AL Finanzen
MA Finanzen
AL Vertrieb
GF Finanzen / Einkauf
MA Administration
AL Administration
GF Vertrieb / Administra...
Type here to search
DEU
08:30
14.04.2024
STRG-RECHTS

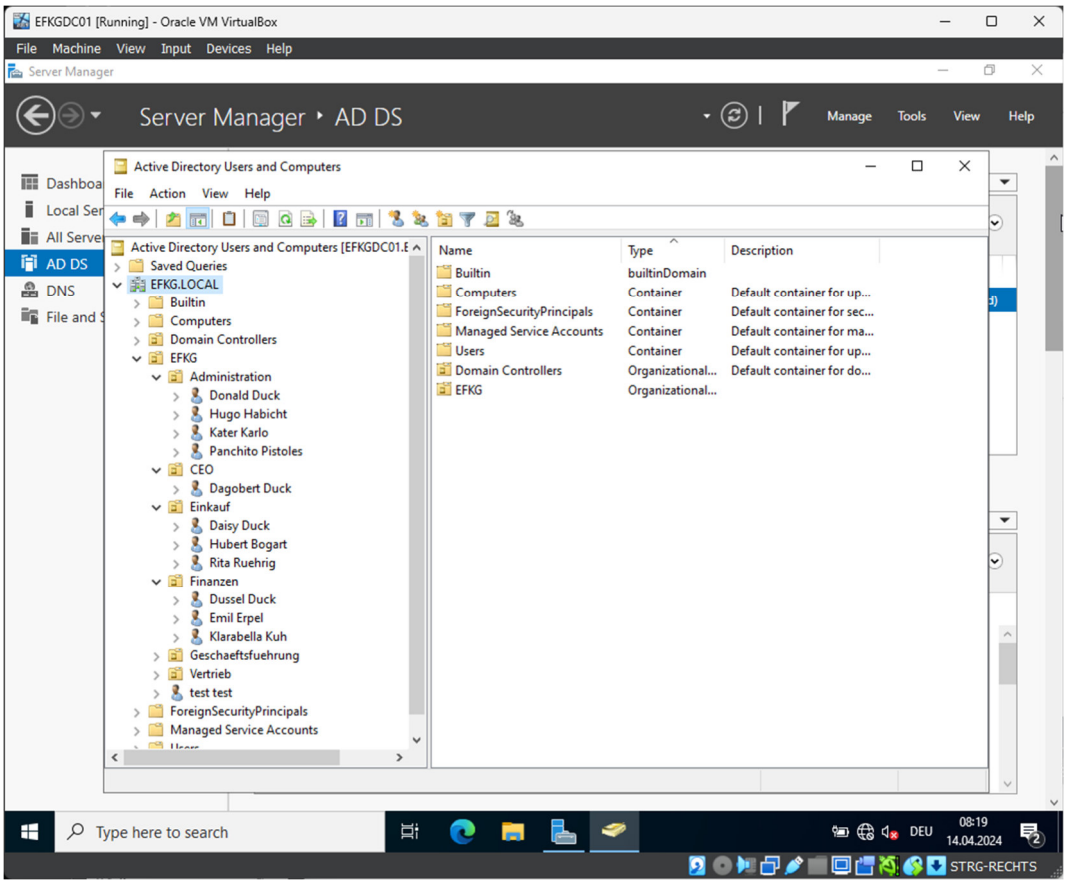

EFKGDC01 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • AD DS
Manage Tools View Help
Copy Object - User
Create in: EFKG.LOCAL/EFKG
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel
Description
Klarabella Kuh User MA Finanzen
Moby Duck User MA Vertrieb
Panchito Pistoles User MA Administration
Rita Ruehrig User MA Einkauf
test test User
Vertrieb Organizational...
CEO
AL Einkauf
MA Vertrieb
AL Finanzen
MA Finanzen
AL Vertrieb
GF Finanzen / Einkauf
MA Administration
AL Administration
GF Vertrieb / Administra...
Type here to search
DEU
08:30
14.04.2024
STRG-RECHTS



Der Benutzer wurde korrekt angelegt und der persönliche Ordner für jeden Benutzer erstellt.



Zum Schluss werden noch die Benutzerkonten in die jeweiligen organisatorischen Einheiten verschoben.



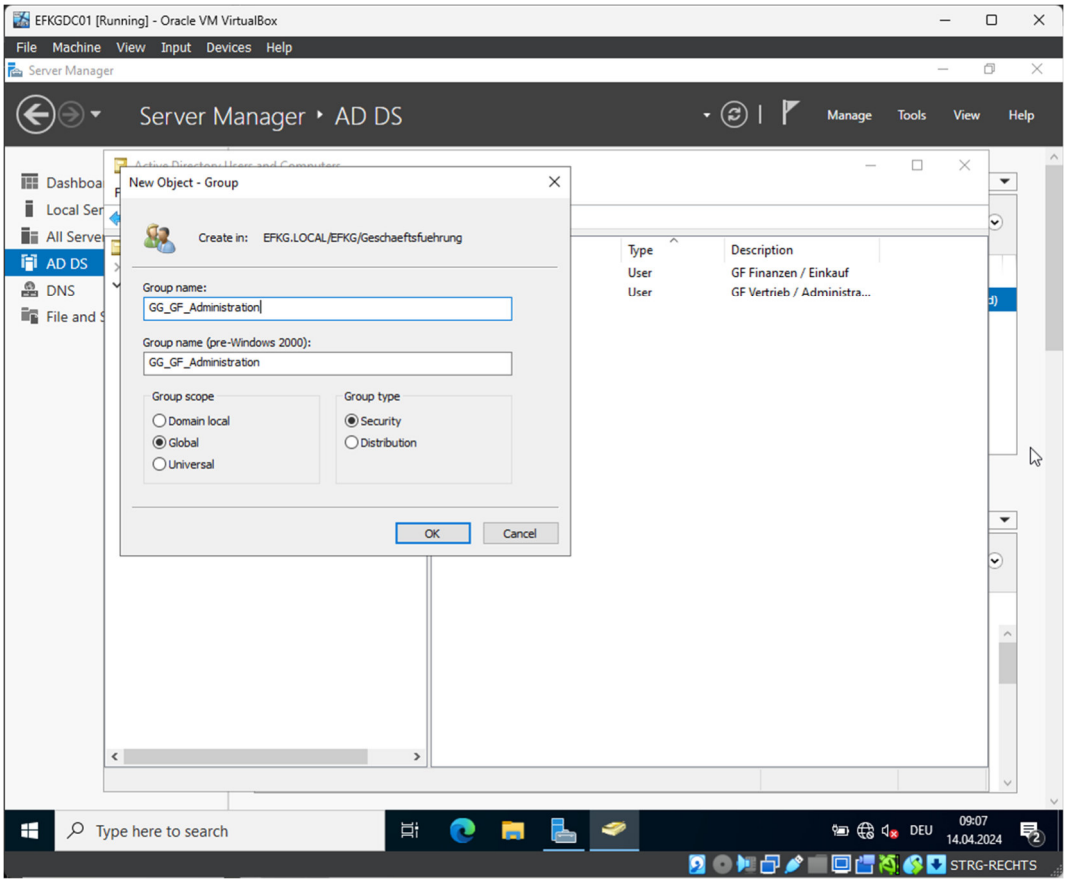
Mit diesem Schritt endet auch der erste Teil der Installation der virtuellen Umgebung. Gleichzeitig beschrieben diese Schritte den ersten Teil des AGDLP-Konzepts: das erstellen der Benutzerkonten oder Accounts.

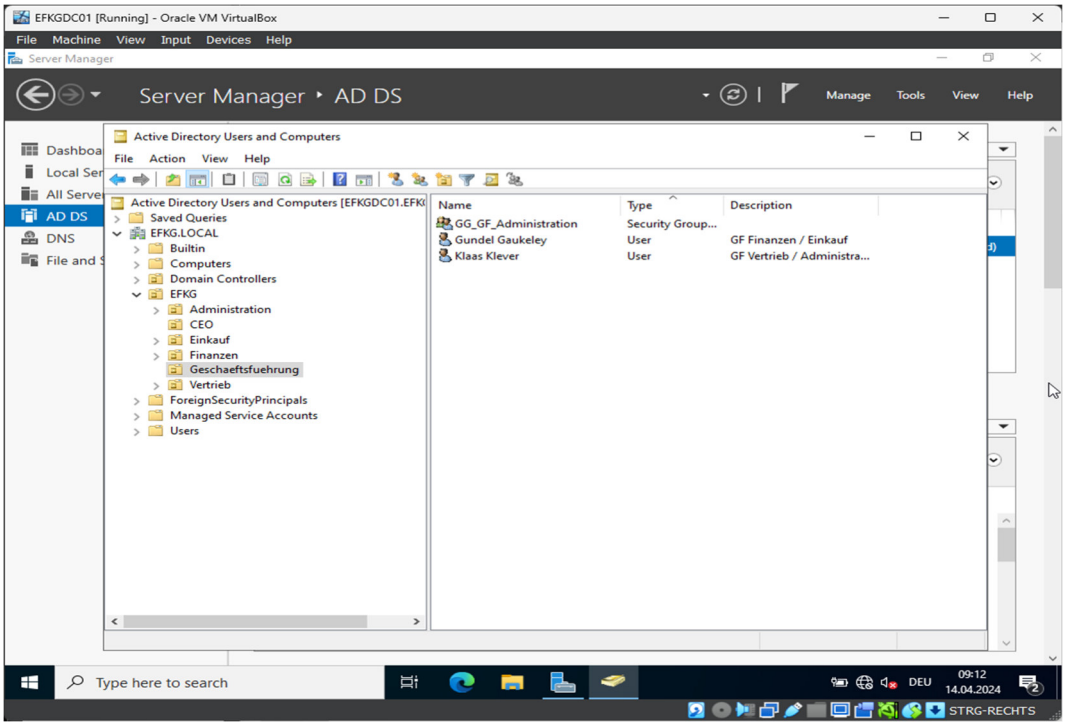
2. Installation der virtuellen Umgebung (Teil 2)

Der zweite, kurze Teil der Installation umfasst das Anlegen sowohl der globalen als auch der domänenlokale Gruppen. Begonnen wird mit den globalen Gruppen, die repräsentativ für die jeweiligen Rollen im Unternehmen stehen.

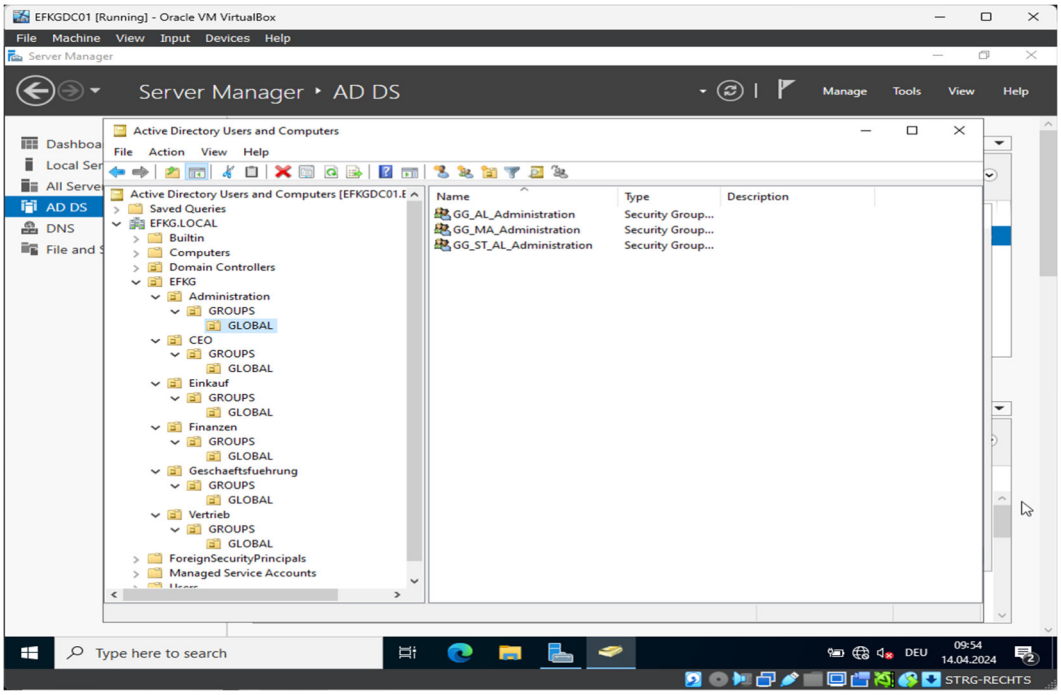
2.1. Anlegen der globalen Gruppen

Die globalen Gruppen werden in den jeweiligen Organisationseinheiten angelegt gemäß der Konvention, beschrieben in Punkt 4.2 der Hauptarbeit. Das Anlegen soll exemplarisch anhand einer Gruppe gezeigt werden. Die übrigen Gruppen werden auf die gleiche Weise angelegt.





Im letzten Schritt wird noch in den jeweiligen Organisationseinheiten der Abteilungen eine weitere Organisationseinheiten „GROUPS“ angelegt. Diese beinhaltet 2 weitere Organisationseinheiten „GLOBAL“ und “DL“. Dort werden die dementsprechenden Gruppen untergebracht.

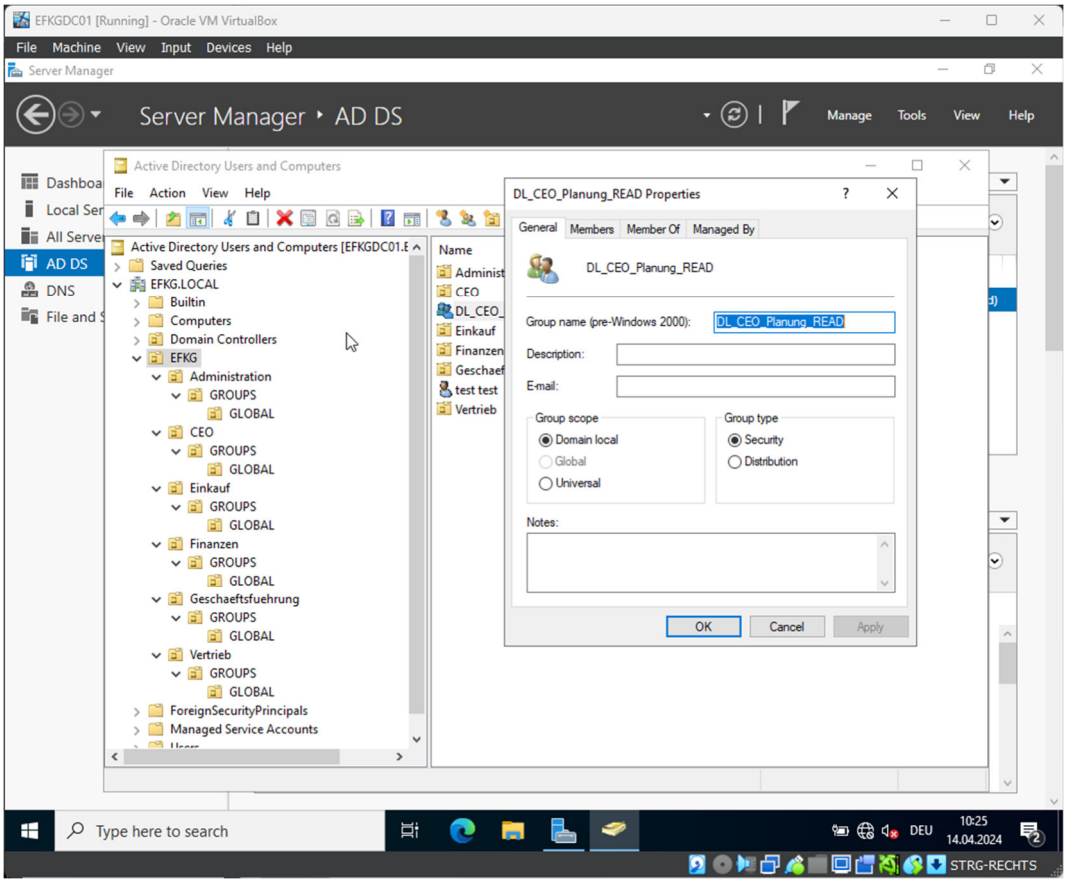


2.2. Anlegen der domänenlokalen Gruppen

Wie die globalen Gruppen auch, werden die domänenlokale Gruppen nach einem vorgegebenen Schema erstellt. Letztere ist zu finden unter Punkt 4.4 der Hauptarbeit.

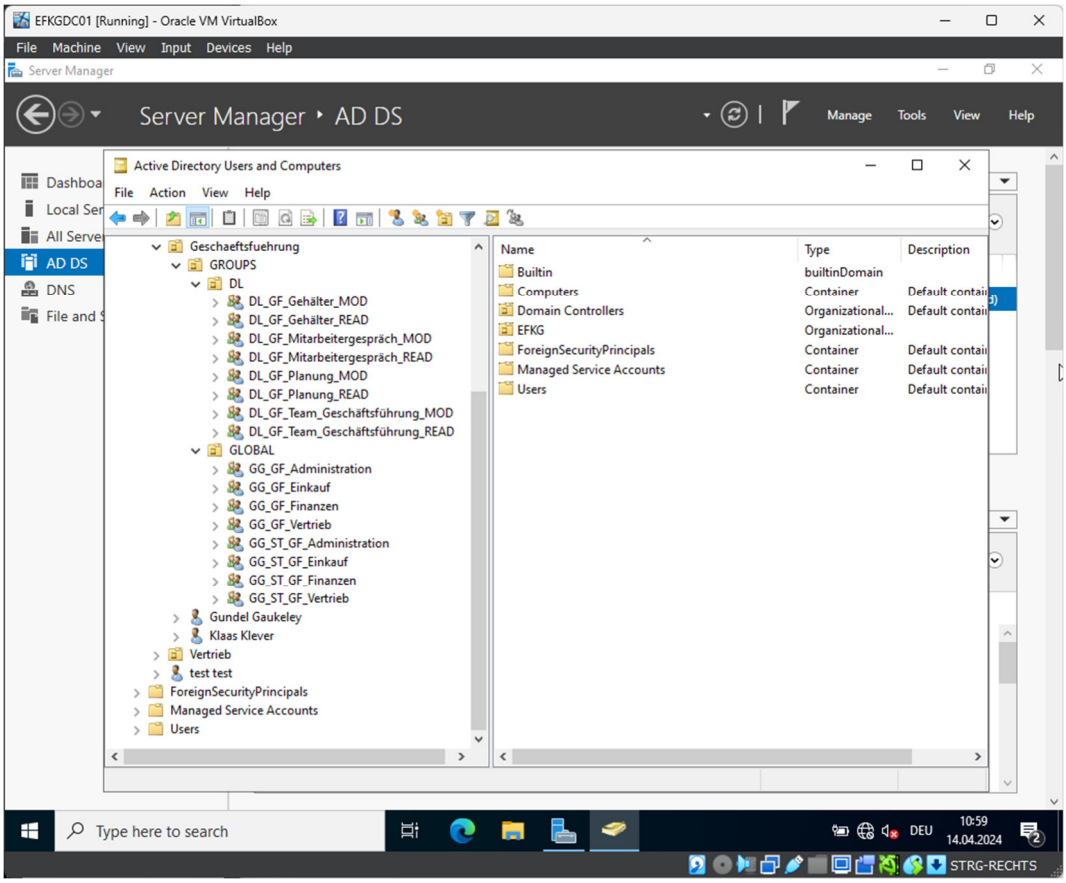
Rechnerisch müsste für jede Ressource eine Gruppe pro Berechtigung angelegt werden. Es soll sich hier auf die Berechtigungen „ändern“ und „lesen“ beschränkt werden, um die Erstellung der Gruppen nicht unnötig zu komplex zu gestalten.

Wieder soll eine Gruppe exemplarisch erstellt werden. Die restlichen Gruppen folgen dieser Vorgabe.



Die Gruppe in der Abbildung wird die Berechtigung „lesen“ auf den Unterordner „Planung“ im Ordner „CEO“ bekommen.

Das fertige Active Directory (für dieses Papier) ist auf der nachstehenden Abbildung zu sehen:



Formal endet an dieser Stelle die Installation des Active Directory. Alle weiteren Schritte finden sich nicht an dieser Stelle, da sie zur Umsetzung gehören und somit in der Hauptarbeit zu finden sind.

Legal

The Shelby Security Company has no affiliation or formal relationship with Microsoft. This document has not been commissioned or endorsed by Microsoft. Its sole purpose is to provide guidance to companies seeking to implement role-based file access. The information provided herein is intended to support the digitalization efforts within these organizations by facilitating the secure and efficient management of file permissions.

Shelby Security Company assumes no responsibility or liability for any actions taken based on the content of this document.

Author: Patrick Blockeel