Rechtliche Hinweise

© Copyright 2007–2020 Micro Focus oder eines seiner verbundenen Unternehmen.

Für Produkte und Services von Micro Focus oder seinen verbundenen Unternehmen und Lizenznehmern („Micro Focus“) gelten nur die Gewährleistungen, die in den Gewährleistungserklärungen, die solchen Produkten beiliegen, ausdrücklich beschrieben sind. Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine zusätzliche Gewährleistung. Micro Focus haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument. Die in diesem Dokument enthaltenen Informationen sind vorbehaltlich etwaiger Änderungen.

Inhalt

Info zu diesem Handbuch

Das *Benutzerhandbuch* enthält grundlegende Informationen zum Directory and Resource Administrator-Produkt (DRA). Dieses Handbuch enthält Definitionen der Terminologie und beschreibt verschiedene verwandte Konzepte.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die mit Verwaltungskonzepten und der Implementierung eines sicheren, verteilten Verwaltungsmodells vertraut sein müssen.

Weitere Dokumentation

Dieses Handbuch gehört zur Dokumentation von Directory and Resource Administrator. Die aktuelle Version dieses Handbuchs und andere Dokumentationsressourcen zu DRA finden Sie auf der DRA-Dokumentationswebsite (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

Kontaktangaben

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation dieses Produkts. Klicken Sie auf den Link zur **Kommentarfunktion** unten auf der Seite in der Online-Dokumentation oder senden Sie eine E-Mail an Documentation-Feedback@microfocus.com.

Bei konkreten Problemen mit einem Produkt wenden Sie sich an den Micro Focus-Kundenservice unter https://www.microfocus.com/support-and-services/.

1 Einführung

Bevor Sie mit der Verwaltung von Active Directory-Objekten mit Directory and Resource Administrator™ (DRA) beginnen, sollten Sie sich mit der grundlegenden Funktion von DRA in Ihrem Unternehmen und mit der Rolle der DRA-Komponenten in der Produktarchitektur vertraut machen.

1.1 Grundlegendes zu Directory and Resource Administrator

Directory and Resource Administrator bietet eine sichere und effiziente Administration der berechtigten Identitäten in Microsoft Active Directory (AD). DRA arbeitet mit einer granularen Delegierung nach dem Prinzip der „niedrigsten Berechtigung“, d. h. die Administratoren und Benutzer erhalten nur die Berechtigungen, die sie zum Ausführen ihrer jeweiligen Aufgaben wirklich benötigen. DRA erzwingt außerdem die Einhaltung von Richtlinien, stellt detaillierte Aktivitätsrevisionen und -berichterstellungen bereit und vereinfacht das Erledigen sich wiederholender Aufgaben dank IT-Prozessautomatisierung. All diese Funktionen tragen zum Schutz der AD- und Exchange-Umgebungen ihrer Kunden vor Berechtigungseskalation, Fehlern, schädlichen Aktivitäten und der Nichteinhaltung von Vorschriften bei, während durch Bereitstellen von Selbstbedienungsfunktionen für Benutzer, Geschäftsmanager und Helpdesk-Mitarbeiter gleichzeitig der Arbeitsaufwand für die Administratoren reduziert wird.

DRA erweitert die leistungsfähigen Funktionen von Microsoft Exchange zur nahtlosen Verwaltung von Exchange-Objekten. DRA stellt über eine einzige, gemeinsame Benutzeroberfläche Funktionen zur richtlinienbasierten Administration für die Verwaltung von Postfächern, öffentlichen Ordnern und Verteilerlisten in Ihrer Microsoft Exchange-Umgebung bereit.

DRA bietet die Lösungen, die Sie zum Steuern und Verwalten Ihrer Active Directory-, Microsoft Windows-, Microsoft Exchange- und Azure Active Directory-Umgebungen benötigen.

- **Unterstützung für Azure und Vor-Ort-Bereitstellungen von Active Directory, Exchange und Skype for Business:** Bietet administrative Verwaltungsfunktionen für Azure und Vor-Ort-Bereitstellungen von Active Directory, Vor-Ort-Bereitstellungen von Exchange Server, Vor-Ort-Bereitstellungen von Skype for Business, Exchange Online und Skype for Business Online.
- **Granulare Steuerung des Benutzerzugriffs und Zugriffs mit Administrationsberechtigungen:**

  Die patentierte ActiveView-Technologie sorgt dafür, dass nur die Berechtigungen delegiert werden, die für bestimmte Verantwortungsbereiche benötigt werden, und schützt vor Berechtigungseskalation.
- **Anpassbare Webkonsole:** Dank der intuitiven Bedienung können auch technisch weniger versierte Mitarbeiter schnell und sicher administrative Aufgaben mit beschränkten (und zugewiesenen) Rollen und Zugriffsrechten erledigen.
- **Detaillierte Aktivitätsrevision und -berichterstellung:** Stellt einen umfassenden Revisionsdatensatz aller mit dem Produkt ausgeführten Aktivitäten bereit. Speichert langfristige Daten auf sichere Weise und demonstriert Revisoren (wie PCI DSS, FISMA, HIPAA oder NERC CIP), dass Prozesse zur Steuerung des Zugriffs auf AD implementiert sind.

- **IT-Prozessautomatisierung:** Automatisiert Workflows für zahlreiche Aufgaben, wie Bereitstellung und Rücknahme der Bereitstellung, Benutzer- und Postfachaktionen, Richtlinienerzwingung und gesteuerte Selbstbedienungsaufgaben; steigert die Geschäftseffizienz und reduziert manuelle und wiederholte Verwaltungsaufgaben.
- **Operationelle Integrität:** Verhindert schädliche oder falsche Änderungen, die sich auf die Leistung und Verfügbarkeit von Systemen und Services auswirken, durch die Bereitstellung einer granularen Zugriffssteuerung für Administratoren und die Verwaltung des Zugriffs auf Systeme und Ressourcen.
- **Prozessdurchsetzung:** Bewahrt die Integrität von wichtigen Änderungsmanagementprozessen, mit denen Sie die Produktivität steigern, Fehler reduzieren, Zeit einsparen und die Verwaltungseffizienz verbessern können.
- **Integration mit Change Guardian:** Verbessert die Revision für Ereignisse, die in Active Directory außerhalb von DRA generiert wurden, und die Workflowautomatisierung.

1.2 Grundlegende Informationen zu den Directory and Administrator-Komponenten

Die Komponenten von DRA für die Verwaltung des berechtigten Zugriffs umfassen Primär- und Sekundärserver, Administratorkonsolen, Berichterstellungskomponenten und die Workflow-Engine zum Automatisieren von Workflowprozessen.

Die folgende Tabelle zeigt die typischen Benutzeroberflächen und Verwaltungsserver, die von den einzelnen Benutzertypen in DRA verwendet werden:

DRA-Benutzertyp	Benutzeroberflächen	Verwaltungsserver
DRA-Administrator (Person, die die Produktkonfiguration pflegt)	Delegierungs- und Konfigurationskonsole	Primärserver
Erweiterter Administrator	DRA Reporting PowerShell CLI DRA-ADSI-Anbieter	Beliebiger DRA-Server
Gelegentlicher Helpdesk-Administrator	Konto- und Ressourcenverwaltungsknoten in der Delegierungs- und Konfigurationskonsole Webkonsole	Beliebiger DRA-Server

1.2.1 DRA-Verwaltungsserver

Der DRA-Verwaltungsserver speichert Konfigurationsdaten (zu Umgebung, delegiertem Zugriff und Richtlinie), führt Bedieneraufgaben, automatisierte Aufgaben und die Revision der systemweiten Aktivität aus. Der Server unterstützt verschiedene Clients auf Konsolenebene und API-Ebene und wurde zur Bereitstellung von hoher Verfügbarkeit für sowohl Redundanz als auch geographische Isolierung durch ein Multi-Master-Set (MMS)-Skalierungsmodell konzipiert. In diesem Modell erfordert jede DRA-Umgebung einen primären DRA-Verwaltungsserver, der mit mehreren zusätzlichen, sekundären DRA-Verwaltungsservern synchronisiert wird.

Wir empfehlen dringend, Verwaltungsserver nicht auf Active Directory-Domänencontrollern zu installieren. Stellen Sie sicher, dass für jede von DRA verwaltete Domäne mindestens ein Domänencontroller am gleichen Standort wie der Verwaltungsserver vorhanden ist. Standardmäßig greift der Verwaltungsserver für alle Schreib- und Lesevorgänge auf den am nächsten liegenden Domänencontroller zu. Für Site-spezifische Aufgaben wie das Zurücksetzen von Passwörtern können Sie einen Site-spezifischen Domänencontroller zum Ausführen des Vorgangs angeben. Eine bewährte Vorgehensweise ist die Verwendung eines dedizierten sekundären Verwaltungsservers für Berichterstellung, Stapelverarbeitung und automatisierte Workloads.

1.2.2 Konto- und Ressourcenverwaltung

Die Konto- und Ressourcenverwaltung ist ein Knoten in der Delegierungs- und Konfigurationskonsole, mit der DRA-Hilfsadministratoren delegierte Objekte verbundener Domänen und Services anzeigen und verwalten können.

1.2.3 Webkonsole

Die Webkonsole ist eine webbasierte Benutzeroberfläche, die DRA-Hilfsadministratoren schnellen und einfachen Zugriff zum Anzeigen und Verwalten delegierter Objekte verbundener Domänen und Services bietet.

Der Administrator kann das Aussehen und die Verwendung der Webkonsole mit benutzerdefiniertem Unternehmens-Branding und benutzerdefinierten Objekteigenschaften anpassen. Außerdem kann er die Integration mit Change Guardian-Servern konfigurieren, um die Revision von Änderungen außerhalb von DRA zu aktivieren.

Der DRA-Administrator kann außerdem automatisierte Workflowformulare erstellen und bearbeiten, um automatisierte Routineaufgaben durch Auslöser auszuführen.

Der Unified-Änderungsverlauf ist eine weitere Funktion der Webkonsole. Sie ermöglicht die Integration mit Änderungsverlaufservern zum Prüfen von Änderungen, die außerhalb von DRA an AD-Objekten vorgenommen werden. Folgende Optionen sind für den Änderungsverlaufsbericht verfügbar:

- Änderungen an ...
- Änderungen durch ...
- Postfach erstellt von ...
- Benutzer-, Gruppen- und Kontakt-Email-Adresse erstellt von ...
- Benutzer-, Gruppen- und Kontakt-Email-Adresse gelöscht von ...

- Virtuelles Attribut erstellt von ...
- Objekte verschoben von ...

1.2.4 Berichterstellungskomponenten

Die DRA-Berichterstellung bietet integrierte, anpassbare Schablonen für das DRA-Management und Details der mit DRA verwalteten Domänen und Systeme:

- Ressourcenberichte für AD-Objekte
- AD-Objektdatenberichte
- AD-Zusammenfassungsberichte
- DRA-Konfigurationsberichte
- Exchange-Konfigurationsberichte
- Office 365 Exchange Online-Berichte
- Detaillierte Berichte zu Aktivitätstrends (nach Monat, Domäne und Spitze)
- Zusammenfassende DRA-Aktivitätsberichte

DRA-Berichte können zur bequemen Verteilung an die entsprechenden Personen und Gruppen über SQL Server Reporting Services geplant und veröffentlicht werden.

1.2.5 Workflow-Engine

DRA lässt sich mit der Workflow-Engine integrieren, um automatisierte Workflowaufgaben über die Webkonsole auszuführen. Die Hilfsadministratoren können den Workflowserver konfigurieren und angepasste Workflowautomatisierungsformulare ausführen und anschließend den Status dieser Workflows anzeigen. Weitere Informationen zur Workflow-Engine finden Sie in der Dokumentation zur Workflowautomatisierung auf der DRA-Dokumentations-Website.

1.2.6 Produktarchitektur

2 Arbeiten mit den Benutzeroberflächen

Die Benutzeroberflächen von DRA erfüllen die verschiedensten Administrationsanforderungen. Folgende Benutzeroberflächen sind verfügbar:

Webkonsole

In dieser webbasierten Benutzeroberfläche können Sie übliche Konto- und Ressourcenverwaltungsaufgaben ausführen. Auf die Webkonsole können Sie von einem beliebigen Computer aus zugreifen, auf dem Internet Explorer, Chrome oder Firefox ausgeführt wird.

PowerShell

Mit dem PowerShell-Modul können Nicht-DRA-Clients über PowerShell-Commandlets DRA-Vorgänge anfordern.

NetIQ Reporting Center-Konsole

Mit dieser Konsole können Sie Verwaltungsberichte anzeigen und bereitstellen, mit denen Sie die Sicherheit im Unternehmen prüfen und Administrationsaufgaben nachverfolgen können. Die Verwaltungsberichte umfassen Aktivitätsberichte, Konfigurationsberichte und Zusammenfassungsberichte. Viele dieser Berichte können grafisch dargestellt werden.

2.1 Webkonsole

Die Webkonsole ist eine webbasierte Benutzeroberfläche, die schnellen und einfachen Zugriff zu vielen Aufgaben in Bezug auf Benutzerkonten, Gruppen, Computer, Ressourcen und Microsoft Exchange-Postfächer bietet. Sie können die Objekteigenschaften anpassen, um Routineaufgaben effizienter zu erledigen. Außerdem können Sie hier allgemeine Eigenschaften Ihres eigenen Benutzerkontos verwalten, wie Ihre Anschrift oder Mobiltelefonnummer.

Die Webkonsole zeigt nur Aufgaben an, zu deren Ausführung Sie berechtigt sind.

2.1.1 Starten der Webkonsole

Sie können die Webkonsole von einem beliebigen Computer aus starten, auf dem Internet Explorer ausgeführt wird. Geben Sie zum Starten der Webkonsole die entsprechende URL im Adressfeld des Webbrowsers ein. Wenn Sie die Webkomponente beispielsweise auf dem Computer „HOUserver“ installiert haben, geben Sie `https://HOUserver.entDomain.com/draclient` im Adressfeld des Webbrowsers ein.

HINWEIS: Um die neuesten Konto- und Microsoft Exchange-Informationen in der Webkonsole anzuzeigen, legen Sie im Webbrowser fest, dass bei jedem Besuch nach neueren Versionen der gecachten Seiten gesucht wird.

2.1.2 Konfigurieren der Webkonsole

Sofern Sie über die entsprechenden Berechtigungen verfügen, können Sie alle erforderlichen Serververbindungen und Integrationen, das Verhalten für das automatische Anmelden und Advanced Authentication in der Webkonsole konfigurieren.

Automatische Abmeldung

Sie können ein Zeitinkrement definieren und festlegen, dass die Webkonsole bei Inaktivität nach einer bestimmten Zeit eine automatische Abmeldung ausführt. Alternativ können Sie festlegen, dass die Webkonsole nie eine automatische Abmeldung ausführt.

Um die automatische Abmeldung in der Webkonsole zu konfigurieren, wechseln Sie zu **Administration** > **Konfiguration** > **Automatische Abmeldung**.

DRA-Serververbindung

In der Webkonsole können Sie eine von drei Optionen konfigurieren, um die DRA-Serververbindungsoptionen festzulegen, die bei der Anmeldung angezeigt werden.

- Immer den standardmäßigen DRA-Serverstandort verwenden (**Immer**)
- Nie den standardmäßigen DRA-Serverstandort verwenden (**Nie**)
- Den standardmäßigen DRA-Serverstandort nur verwenden, wenn er ausgewählt ist (**Nur, wenn ausgewählt**)

Die Tabelle beschreibt das Verhalten beim Anmelden für die einzelnen Optionen.

Verbindungskonfiguration	Anmeldebildschirm – Optionen	Beschreibung der Verbindungsoption
Immer	Keine	Die Konfiguration der Optionen ist deaktiviert.
Nie	Automatische Erkennung verwenden	Sucht automatisch einen DRA-Server; keine Konfigurationsoptionen sind verfügbar.
	Mit einem bestimmten DRA-Server verbinden	Der Benutzer konfiguriert den Server und den Port.

Verbindungskonfiguration	Anmeldebildschirm – Optionen	Beschreibung der Verbindungsoption
	Mit einem DRA-Server verbinden, der eine bestimmte Domäne verwaltet	Der Benutzer gibt eine verwaltete Domäne an und wählt eine Verbindungsoption: ◆ Automatische Erkennung verwenden (in der angegebenen Domäne) ◆ Primärserver für diese Domäne ◆ DRA-Server suchen (in der angegebenen Domäne)
Nur, wenn ausgewählt	Automatische Erkennung verwenden	Sucht automatisch einen DRA-Server; keine Konfigurationsoptionen sind verfügbar.
	Mit dem standardmäßigen DRA-Server verbinden	Der standardmäßige Server wird ausgewählt und die DRA-Serverkonfiguration ist deaktiviert.
	Mit einem bestimmten DRA-Server verbinden	Der Benutzer konfiguriert den Server und den Port.
	Mit einem DRA-Server verbinden, der eine bestimmte Domäne verwaltet	Der Benutzer gibt eine verwaltete Domäne an und wählt eine Verbindungsoption: ◆ Automatische Erkennung verwenden (in der angegebenen Domäne) ◆ Primärserver für diese Domäne ◆ DRA-Server suchen (in der angegebenen Domäne)

Um die DRA-Serververbindung in der Webkonsole zu konfigurieren, wechseln Sie zu **Administration** > **Konfiguration** >**DRA-Serververbindung**.

REST-Serververbindung

Die Konfiguration der REST-Serviceverbindung umfasst das Festlegen eines standardmäßigen Serverstandorts und einer Verbindungszeitüberschreitung in Sekunden. In der Webkonsole können Sie eine von drei Optionen konfigurieren, um die REST-Serviceverbindungsoptionen festzulegen, die bei der Anmeldung angezeigt werden.

- Immer den standardmäßigen REST-Servicestandort verwenden (**Immer**)
- Nie den standardmäßigen REST-Servicestandort verwenden (**Nie**)
- Den standardmäßigen REST-Servicestandort nur verwenden, wenn er ausgewählt ist (**Nur, wenn ausgewählt**)

Die Tabelle beschreibt das Verhalten beim Anmelden für die einzelnen Optionen.

Verbindungskonfiguration	Anmeldebildschirm – Optionen	Beschreibung der Verbindungsoption
Immer	Keine	Die Konfiguration der Optionen ist deaktiviert.

Verbindungskonfiguration	Anmeldebildschirm – Optionen	Beschreibung der Verbindungsoption
Nie	Automatische Erkennung verwenden	Sucht automatisch einen REST-Server; keine Konfigurationsoptionen sind verfügbar.
	Mit einem bestimmten REST-Server verbinden	Der Benutzer konfiguriert den Server und den Port.
	Mit einem REST-Server in einer bestimmten Domäne verbinden	Der Benutzer gibt eine verwaltete Domäne an und wählt eine Verbindungsoption: ◆ Automatische Erkennung verwenden (in der angegebenen Domäne) ◆ REST-Server suchen (in der angegebenen Domäne)
Nur, wenn ausgewählt	Automatische Erkennung verwenden	Sucht automatisch einen REST-Server; keine Konfigurationsoptionen sind verfügbar.
	Mit dem standardmäßigen REST-Server verbinden	Der standardmäßige REST-Server wird ausgewählt und die REST-Serverkonfiguration ist deaktiviert.
	Mit einem bestimmten REST-Server verbinden	Der Benutzer konfiguriert den Server und den Port.
	Mit einem REST-Server in einer bestimmten Domäne verbinden	Der Benutzer gibt eine verwaltete Domäne an und wählt eine Verbindungsoption: ◆ Automatische Erkennung verwenden (in der angegebenen Domäne) ◆ REST-Server suchen (in der angegebenen Domäne)

Um die REST-Serviceverbindung in der Webkonsole zu konfigurieren, wechseln Sie zu **Administration** > **Konfiguration** > **REST-Serviceverbindung**.

Advanced Authentication

Advanced Authentication bietet Ihnen dank Multifaktor-Authentifizierung die Möglichkeit, Ihre sensiblen Informationen besser zu schützen als nur mit einem einfachen Benutzernamen und Passwort. Die Multifaktor-Authentifizierung ist ein Zugriffssteuerungsverfahren, bei dem zum Überprüfen der Benutzeridentität mehrere Authentifizierungsmethoden kombiniert werden müssen.

Nachdem der DRA-Administrator Ketten und Ereignisse konfiguriert hat, können Sie sich bei der Webkonsole anmelden und Advanced Authentication aktivieren, sofern Sie über die erforderlichen Befugnisse verfügen. Nachdem die Authentifizierung aktiviert ist, müssen sich die Benutzer zum Zugriff auf die Webkonsole über Advanced Authentification authentifizieren.

Um Advanced Authentication zu aktivieren, melden Sie sich an der Webkonsole an und navigieren Sie zu **Administration** > **Konfiguration** > **Advanced Authentication**. Aktivieren Sie das Kontrollkästchen **Aktiviert** und konfigurieren Sie das Formular gemäß den Anweisungen für jedes Feld.

Weitere Informationen zu Advanced Authentication finden Sie unter „Authentication“ (Authentifizierung) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

Integrationsserver

DRA bietet eine Integration mit einem Workflowautomatisierungs-Server und mit Change Guardian-Servern, um Zugriff auf Formulare für automatisierte Workflows bzw. auf Unified-Änderungsverlaufsberichte bereitzustellen. Mit den entsprechenden Befugnissen können Sie die Verbindung zum Workflowautomatisierungs-Server und zu einem oder mehreren Change Guardian-Servern konfigurieren.

Workflowautomatisierungs-Server konfigurieren

Um die Workflowautomatisierung in DRA zu verwenden, muss die Workflow-Engine auf einem Windows-Server installiert werden, auf dem die automatisierten Workflows erstellt werden. Die DRA-Integration mit dem Workflowautomatisierungs-Server wird in der Webkonsole konfiguriert.

Um den Workflowautomatisierungs-Server zu konfigurieren, melden Sie sich bei der Webkonsole an und navigieren Sie zu **Administration** > **Integrationen** > **Workflowautomatisierung**.

Server für den Unified-Änderungsverlauf (Unified Change History, UCH) konfigurieren

So konfigurieren Sie Server für den Unified-Änderungsverlauf:

1. Starten Sie die Webkonsole und melden Sie sich mit dem AA-Berechtigungsnachweis an.
2. Wechseln Sie zu **Administration > Integrationen > Unified-Änderungsverlauf** und klicken Sie auf das Symbol **Hinzufügen**.
3. Geben Sie den Namen oder die IP-Adresse des Servers für den Unified-Änderungsverlauf, die Portnummer, den Servertyp und die Details des Zugriffskontos in der Konfiguration des Unified-Änderungsverlaufs an.
4. Testen Sie die Serververbindung und klicken Sie auf **OK**, um die Konfiguration zu speichern.
5. Fügen Sie nach Bedarf weitere Server hinzu.

2.1.3 Anpassen der Webkonsole

In der Webkonsole können Sie Objekteigenschaften und das Branding der Benutzeroberfläche anpassen. Richtig implementiert vereinfacht diese Anpassung der Eigenschaften die Automatisierung von Aufgaben mit Objektverwaltung.

Anpassen von Eigenschaftsseiten

Sie können die Objekteigenschaftformulare, die Sie in der Active Directory-Verwaltungsrolle verwenden, nach Objekttyp anpassen. Dies umfasst auch das Erstellen und Anpassen neuer Objektseiten, die auf in DRA integrierten Objekttypen basieren. Sie können auch die Eigenschaften der integrierten Objekttypen ändern.

Eigenschaftenobjekte sind in der Liste der Eigenschaftsseiten in der Webkonsole klar definiert, sodass Sie einfach identifizieren können, welche Objektseiten integriert sind, welche integrierten Seiten angepasst wurden und welche Seiten nicht integriert sind und vom Administrator erstellt wurden.

Objekteigenschaftsseite anpassen

Sie können Objekteigenschaftenformulare anpassen, indem Sie Seiten hinzufügen oder entfernen, vorhandene Seiten und Felder ändern oder neue benutzerdefinierte Behandlungsroutinen für Eigenschaftenattribute erstellen. Wenn Sie benutzerdefinierte Behandlungsroutinen erstellen, werden diese je nach Konfiguration automatisch ausgeführt, wenn ein Eigenschaftenfeld geändert wird oder ein Administrator auf eine Aufforderung zum Ausführen einer Abfrage antwortet.

Die Objektliste in den Eigenschaftsseiten bietet zwei Operationstypen für jeden Objekttyp: „Objekt erstellen“ und „Eigenschaften bearbeiten“. Dies sind die beiden wesentlichen Operationen, die Sie im Web-Client ausführen. Die Anpassungen können die Verwaltung der Active Directory-Objekte in DRA in Bezug auf Effizienz und Benutzererlebnis verbessern.

So passen Sie eine Objekteigenschaftsseite in der Webkonsole an:

1. Navigieren Sie zu **Anpassung** > **Eigenschaftsseiten**.
2. Wählen Sie ein Objekt und einen Operationstyp (Erstellen oder Bearbeiten) in der Liste der Eigenschaftsseiten aus.
3. Klicken Sie auf die Schaltfläche **Bearbeiten** .
4. Passen Sie das Objekteigenschaftenformular an, indem Sie eine oder mehrere der folgenden Aktionen ausführen und dann die Änderungen anwenden:
   - Neue Eigenschaftsseite hinzufügen: **Seite hinzufügen**
   - Eigenschaftsseite auswählen und anpassen:
     - Konfigurationsfelder in der Seite neu sortieren:
     - Felder oder untergeordnete Felder bearbeiten:
     - Ein oder mehrere Felder hinzufügen oder **Feld hinzufügen**
     - Ein oder mehrere Felder entfernen:
   - Mit Skripten, Nachrichtenfeldern oder Abfragen (LDAP, DRA oder REST) benutzerdefinierte Behandlungsroutinen für Eigenschaften erstellen

     Weitere Informationen zur Verwendung von benutzerdefinierten Behandlungsroutinen finden Sie in Benutzerdefinierte Behandlungsroutinen hinzufügen.

Benutzerdefinierte Behandlungsroutinen hinzufügen

Benutzerdefinierte Behandlungsroutinen werden in DRA dazu verwendet, dass Eigenschaftenattribute zum Erfüllen einer Workflowaufgabe miteinander interagieren. Benutzerdefinierte Eigenschaften-Behandlungsroutinen können beispielsweise dazu verwendet werden, den Wert eines anderen Felds abzurufen, Werte zu aktualisieren, den Nur-Lesen-Zustand eines Felds umzuschalten oder Felder basierend auf konfigurierten Variablen anzuzeigen bzw. auszublenden.

DRA erleichtert die Erstellung von benutzerdefinierten Behandlungsroutinen mit verschiedenen JavaScript-Makros, die Sie beim Erstellen und Validieren der Behandlungsroutine auswählen können.

Grundlegende Schritte zum Erstellen einer benutzerdefinierten Behandlungsroutine:

Die nachfolgenden Schritte beginnen mit einer vorab ausgewählten Seite für benutzerdefinierte Behandlungsroutinen. Um zu diesem Punkt zu gelangen, greifen Sie über die Bearbeitungsschaltfläche eines Eigenschaftsfelds auf die benutzerdefinierten Behandlungsroutinen der Objekteigenschaft zu.

1. Klicken Sie auf die Registerkarte „Benutzerdefinierte Behandlungsroutinen“ und aktivieren Sie die Seite.
2. Wählen Sie im Dropdown-Menü eine benutzerdefinierte Behandlungsroutine und wählen Sie eine Ausführungszeit aus. Normalerweise wird die zweite oder dritte Option für die Ausführungszeit verwendet.

   HINWEIS: Typischerweise benötigen Sie meist nur eine benutzerdefinierte Behandlungsroutine. Sie können jedoch mehrere Behandlungsroutinen verwenden, indem Sie Flusssteuerungen im Skript konfigurieren, um die Behandlungsroutinen zu verknüpfen.

   ---

3. Sie müssen jede benutzerdefinierte Behandlungsroutine konfigurieren, die Sie zur Seite hinzufügen. Die Konfigurationsoptionen variieren je nach Typ der Behandlungsroutine. Alle Behandlungsroutinen werden jedoch über JavaScript ausgeführt.

   Sie können eigene Vanilla-JavaScript-Einträge erstellen oder die integrierten Makros verwenden.

   - **Behandlungsroutinen für LDAP- oder REST-Abfragen:**

     1. Wenn die Abfrage auf statischen Werten basieren soll, definieren Sie **Verbindungsinformationen** und **Abfrageparameter**.

        Wenn die Abfrage dynamisch sein soll, geben Sie Platzhaltertext in die Pflichtfelder ein. Dies ist erforderlich, damit das Skript ausgeführt wird. Das Skript überschreibt die Platzhalterwerte.

        HINWEIS: Sie können auch Header und Cookies für die REST-Abfrage konfigurieren.

        ---

     2. Wählen Sie in der Aktion vor der Abfrage den Makrotyp **Global**, **Abfrage** oder **Formularfeld** aus.
     3. Wählen Sie in der Dropdown-Liste ein Makro und fügen Sie es ein (**</> Makro einfügen**).
     4. Fügen Sie je nach Bedarf weitere Makros ein und geben Sie dann die gewünschten Werte an, um das Skript fertigzustellen.

        Als Beispiel verwenden wir in der Aktion vor der Abfrage ein Skript, das bestätigt, dass ein vom Benutzer eingegebener Gruppenname beim Senden des Formulars nicht bereits in Active Directory vorhanden ist.

        Wir erstellen eine LDAP-Abfrage mit dem vom Benutzer eingegebenen Namen. Mit dem Makro `Field()` greifen wir auf den Wert des Felds „Name“ zu und erstellen die Abfragezeichenfolge, die dann mit dem Makro `Filter()` als Abfragefilter festgelegt wird.

        ```
        Filter() = '(&(objectCategory=group)(objectClass=group)(name=' +
        Field(name) + '))';
        ```

5. Anschließend überprüfen wir in der Aktion nach der Abfrage die Ergebnisse der Abfrage. Die Ergebnisse werden als Array an Objekten wiedergegeben, die die Abfragekriterien erfüllen. Wir müssen also nur überprüfen, ob die Länge des Arrays größer 0 ist.

   Wenn eine Gruppe gefunden wird, die die Abfragekriterien erfüllt, brechen wir das Senden des Formulars mit dem Makro `Cancel()` ab. Dem Makro kann optional eine Nachricht übergeben werden, die dem Benutzer angezeigt werden soll.

   ```
   if (QueryResults().length > 0) { Cancel('Eine Gruppe mit diesem Namen ist bereits vorhanden, bitte geben Sie einen eindeutigen Namen ein.');}
   ```

- **Skript:** Fügen Sie benutzerdefinierten JavaScript-Code ein oder verwenden Sie die Makros zum Erstellen des Skripts.
- **DRA-Abfrage:** Definieren Sie für die Abfrageparameter eine Nutzlast im JSON-Format. Verwenden Sie dann Makros ähnlich wie oben für LDAP- und REST-Abfragen beschrieben.
- **Behandlungsroutinen für Mitteilungsfeld:** Nachdem Sie die Eigenschaften für das Mitteilungsfeld selbst definiert haben, verwenden Sie Makros ähnlich wie oben für LDAP- und REST-Abfragen beschrieben. Anstelle der Aktionen vor und nach der Abfrage erstellen Sie jedoch stattdessen Makroskripte für die Aktionen vor dem Anzeigen und nach dem Schließen.

4 Klicken Sie auf **Behandlungsroutinen testen**, um das Skript vor dem Speichern des Formulars zu bestätigen.

   Dies generiert eine Zusammenfassung der Testergebnisse, in der Sie die Ausführungsergebnisse anzeigen können.

HINWEIS: Wenn die Behandlungsroutine vom aktuellen Zustand des Formulars abhängt (zum Beispiel davon, ob das Feld einen Wert enthält), kann sie nicht erfolgreich ausgeführt werden, weil beim Bearbeiten eines Formulars keine Daten geladen werden. Für solche Szenarien muss die Behandlungsroutine außerhalb des Formulareditors getestet werden. Speichern Sie dazu die Anpassung, navigieren Sie zum entsprechenden Formular und geben Sie die erforderlichen Daten ein.

Neue Objekteigenschaftsseite erstellen

So erstellen Sie eine neue Objekteigenschaftsseite:

1 Melden Sie sich bei der Webkonsole an und navigieren Sie zu **Anpassung** > **Eigenschaftsseiten**.

2 Klicken Sie unter „Aufgaben“ auf **Neue Aktion erstellen**.

3 Erstellen Sie das anfängliche Objekteigenschaftenformular, indem Sie den Namen, das Symbol, den Objekttyp und die Operationskonfiguration definieren.

4 Passen Sie das neue Formular je nach Bedarf an (siehe Objekteigenschaftsseite anpassen).

Anpassen des Branding der Benutzeroberfläche

Sie können die Titelleiste der DRA-Webkonsole mit einem eigenen Titel und Logobild anpassen. Diese Elemente werden direkt rechts neben dem DRA-Produktnamen angezeigt. Da diese Position auch für die Navigation der obersten Ebene verwendet wird, werden die Elemente nach der Anmeldung durch die DRA-Navigationslinks der obersten Ebene verdeckt. Auf der Browserregisterkarte wird die angepasste Kachel jedoch weiterhin angezeigt.

So passen Sie das Branding der Titelleiste in DRA an:

1. Melden Sie sich an der Webkonsole an und navigieren Sie zu **Anpassung** > **Branding**.
2. Wenn Sie ein Firmenlogo hinzufügen möchten, speichern Sie das Logobild in `components\lib\img` auf dem Webserver.
3. Fügen Sie die erforderlichen Informationen je nach Bedarf für die drei Felder auf der Branding-Anpassungsseite hinzu und speichern Sie die Änderungen.

2.1.4 Verwalten von Objekten in der Webkonsole

Um Objekte in der Webkonsole zu verwalten, navigieren Sie zum Mastertitel „Verwaltung“. Hier können Sie Objekte in Domänen, in Containern und im Papierkorb nach Objekttyp suchen. Wenn eine Domäne, ein Container oder eine organisatorische Einheit ausgewählt ist, können Sie außerdem neue Objekte erstellen, Mitglieder zu Gruppen hinzufügen oder daraus entfernen und Objekte verschieben.

Wenn Sie ein Objekt in der Suchergebnisliste auswählen, sind alle anwendbaren Aktionen, die Sie für das Objekt ausführen können, in der Symbolleiste über dem Raster verfügbar. Die verfügbaren Optionen hängen vom ausgewählten Objekttyp, von den zurzeit für DRA konfigurierten Komponenten und von den Ihnen zugewiesenen Administratorberechtigungen ab.

Um die Eigenschaften eines Objekts zu bearbeiten, bewegen Sie den Mauszeiger über das Objekt und klicken Sie auf das Symbol **Eigenschaften** ✎, das in der Objektzeile angezeigt wird. Von hier können Sie auf alle Eigenschaftenseiten des Objekts im linken Navigationsbereich zugreifen.

WICHTIG: Wenn Sie ein **Objekt vor dem unbeabsichtigten Löschen schützen** möchten, blättern Sie zum unteren Ende der Eigenschaftenseite **Allgemein**, aktivieren Sie das Kontrollkästchen für diese Funktion und klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen.

Weitere Informationen zu den Aktionen, die Sie für Objekte ausführen können, finden Sie in den folgenden Themen:

- Verwalten von Benutzerkonten, Gruppen und Kontakten
- Verwalten von Exchange-Postfächern und öffentlichen Ordnern
- Verwalten von Ressourcen

2.1.5 Verwenden des Unified-Änderungsverlaufs (UCH)

Informationen zur Konfiguration der Server für den Unified-Änderungsverlauf finden Sie in Server für den Unified-Änderungsverlauf (Unified Change History, UCH) konfigurieren.

Unified-Änderungsverlaufsberichte suchen und generieren

Sie können alle Unified-Änderungsberichte suchen oder die Suche über die Suchoptionen verfeinern. Sie können Unified-Änderungsverlaufsberichte nur über die Webkonsole anzeigen. Wenn Sie die Suche ohne Angabe von Parametern ausführen, werden alle Unified-Änderungsverlaufsberichte aufgelistet. Das Hinzufügen von Suchparametern filtert die Berichte, die in der Suche zurückgegeben werden.

WICHTIG: Zum Generieren von Unified-Änderungsverlaufsberichten benötigen Sie die Befugnis **Generate UI Reports** (Benutzeroberflächenberichte generieren).

So suchen und generieren Sie Unified-Änderungsverlaufsberichte:

1. Starten Sie die Webkonsole.
2. Wechseln Sie zu **Verwaltung > Suche**.
3. Führen Sie die Suche mit oder ohne Angabe von Kriterien für den Namen, den Speicherort oder den untergeordneten Container aus.

   Wenn Sie keine Kriterien angeben, geben die Suchergebnisse alle Objekte zurück. Fügen Sie Suchkriterien ein, um die Suchergebnisse einzugrenzen.
4. Klicken Sie auf das Symbol **Suchen**, um die Suchergebnisse anzuzeigen.
5. Wählen Sie die Objekte aus, für die Sie Berichte generieren möchten.
6. Klicken Sie auf das Symbol **Änderungsverlaufsberichte anzeigen**.

   Unter **Kriterien für Änderungsverlaufsbericht** können Sie den Bericht mit Kriterien wie Berichttypen, Zielobjekte, Anfangsdatum, Enddatum, maximale Anzahl an Zeilen und Server (DRA- oder Change Guardian-Server) bearbeiten und generieren.
7. Klicken Sie auf **Generieren**, um Revisionsdaten abzurufen und einen Unified-Änderungsverlaufsbericht zu generieren.
8. Sie können den Bericht sortieren und in ein gewünschtes Format wie CSV oder HTML exportieren.

Anzeigen der Eigenschaften des Unified-Änderungsverlaufs

Um die Eigenschaften eines Servers anzuzeigen, für den der Unified-Änderungsverlauf konfiguriert ist, navigieren Sie zu **Administration** > **Integrationen** > **Unified-Änderungsverlauf**, wählen Sie den konfigurierten Server aus und klicken Sie auf das Menü **Optionen**, das folgende Aktionen enthält:

- **Eigenschaften:** Eigenschaften des Unified-Änderungsverlaufs anzeigen und aktualisieren.
- **Verbindung testen:** Serververbindung überprüfen.
- **Löschen:** Den konfigurierten Server für den Unified-Änderungsverlauf löschen.

2.1.6 Zugreifen auf den Änderungsverlauf eines Benutzers

Über die Webkonsole können Sie den Verlauf der Änderungen anzeigen, die für oder von einem bestimmten Benutzer vorgenommen wurden. Die folgenden Änderungstypen können angezeigt werden:

- Vom Benutzer vorgenommene Änderungen
- Für den Benutzer vorgenommene Änderungen
- Vom Benutzer erstellte Benutzerpostfächer
- Vom Benutzer gelöschte Benutzerpostfächer
- Vom Benutzer erstellte Gruppen- und Kontakt-Email-Adressen
- Vom Benutzer gelöschte Gruppen- und Kontakt-Email-Adressen
- Vom Benutzer erstellte oder deaktivierte virtuelle Attribute
- Vom Benutzer verschobene Objekte

So zeigen Sie den Änderungsverlaufsbericht an oder generieren ihn:

1. Starten Sie die Webkonsole.
2. Suchen Sie das Objekt, dessen Verlauf Sie anzeigen möchten.
3. Klicken Sie auf das Symbol **Änderungsverlaufsberichte anzeigen**.
4. Um die Kriterien für die Berichtgenerierung zu ändern, klicken Sie auf **Bearbeiten**.

   Sie können das Anfangs- oder Enddatum, das nachverfolgte Objekt, den Berichttyp und andere Kriterien ändern.
5. Um eine CSV-Datei des Berichts zu erstellen, klicken Sie auf **Generieren**.

2.1.7 Verwenden der Workflowautomatisierung

Mit der Workflowautomatisierung können Sie IT-Prozesse automatisieren, indem Sie Workflowformulare starten, die beim Ausführen eines Workflows oder bei Auslösung durch ein benanntes, auf dem Workflowautomatisierungs-Server erstelltes Workflowereignis ausgeführt werden.

Die Workflowformulare werden beim Erstellen bzw. Bearbeiten auf dem Webserver gespeichert. Wenn Sie sich für diesen Server an der Webkonsole anmelden, erhalten Sie je nach delegierten Befugnissen und Konfiguration der Formulare Zugriff auf die Formulare. Formulare sind allgemein für alle Benutzer verfügbar, die über einen Webserver-Berechtigungsnachweis verfügen. Zum Senden des Formulars sind entsprechende Befugnisse erforderlich.

Workflowformular starten: Workflows werden auf dem Workflowautomatisierungs-Server erstellt, der über die Webkonsole mit DRA integriert sein muss. Um ein neues Formular speichern zu können, muss entweder die Option **Spezifischen Workflow starten** oder die Option **Workflow nach Ereignis auslösen** in den Formulareigenschaften konfiguriert sein. Weitere Informationen zu diesen Optionen finden Sie unten:

- **Spezifischen Workflow starten:** Diese Option listet alle verfügbaren Workflows auf, die auf dem Workflowserver für DRA in Produktion sind. Damit die Workflows in dieser Liste angezeigt werden, müssen Sie im Ordner `DRA_Workflows` auf dem Workflowautomatisierungs-Server erstellt worden sein.

- **Workflow nach Ereignis auslösen:** Mit dieser Option können Sie Workflows mit vordefinierten Auslösern ausführen. Die Workflows mit Auslösern werden auch auf dem Workflowautomatisierungs-Server erstellt.

HINWEIS: Nur Workflowformulare, die mit der Option „Spezifischen Workflow starten“ konfiguriert wurden, verfügen über einen Ausführungsverlauf, der im Hauptsuchbereich unter **Aufgaben** > **Anforderungen** abgefragt werden kann.

Weitere Informationen zur Workflowautomatisierung finden Sie im *DRA Administrator Guide* (DRA-Administratorhandbuch).

2.2 Konto- und Ressourcenverwaltung

Der Konto- und Ressourcenverwaltungsknoten in der Delegierungs- und Konfigurationskonsole bietet Zugriff auf die meisten Aufgaben für DRA-Hilfsadministratoren und eignet sich für unternehmensweite Verwaltungsaufgaben von der einfachen Administration bis hin zu fortgeschrittenen Helpdesk-Aufgaben. Über die Konto- und Ressourcenverwaltung können Sie Konto- und Ressourcenverwaltungsaufgaben ausführen und Microsoft Exchange-Postfächer verwalten.

Die Konto- und Ressourcenverwaltung enthält die folgenden Knoten:

All My Managed Objects (Alle meine verwalteten Objekte)

Hier können Sie Objekte verwalten, wie Benutzerkonten, Gruppen, Kontakte, Ressourcen, dynamische Gruppen, dynamische Verteilergruppen, Ressourcenpostfächer und öffentliche Ordner für jede Domäne, in der Sie über bestimmte Befugnisse verfügen.

Temporary Group Assignments (Temporäre Gruppenzuweisungen)

Hier können Sie Gruppenmitgliedschaften für Benutzer verwalten, die nur für einen bestimmten Zeitraum eine Gruppenmitgliedschaft benötigen.

Advanced Search Queries (Erweiterte Suchabfragen)

Hier können Sie erweiterte Abfragen verwalten, die auf dem Verwaltungsserver verfügbar sind.

Recycle Bin (Papierkorb)

Hier können Sie gelöschte Benutzerkonten, Gruppen, Kontakte und Ressourcen für eine beliebige Microsoft Windows-Domäne verwalten, in der die Papierkorbfunktion aktiviert ist.

Um auf den Konto- und Ressourcenverwaltungsknoten zuzugreifen, klicken Sie im Programmordner „NetIQ Administrator“ auf **Delegation and Configuration** (Delegierung und Konfiguration) und erweitern Sie den Delegierungs- und Konfigurationsknoten in der Konsole.

Beim Starten der Delegierungs- und Konfigurationskonsole stellen Sie anfänglich eine Verbindung zum Verwaltungsserver mit der besten Verfügbarkeit in der lokalen Domäne her. Der Verwaltungsserver mit der besten Verfügbarkeit ist der nächstgelegene Server, üblicherweise ein Server am Netzwerkstandort. Durch Ermitteln des Verwaltungsservers mit der besten Verfügbarkeit bietet DRA eine schnellere Verbindung und eine verbesserte Leistung.

Weitere Informationen zur Konto- und Ressourcenverwaltung finden Sie in den folgenden Themen:

2.2.1 Herstellen einer Verbindung zu einem Verwaltungsserver oder einer verwalteten Domäne

Standardmäßig stellt DRA eine Verbindung zum Verwaltungsserver mit der besten Verfügbarkeit für eine verwaltete Domäne bzw. einen verwalteten Computer her. Der Verwaltungsserver mit der besten Verfügbarkeit ist der nächstgelegene Server, üblicherweise ein Server am Netzwerkstandort. Wenn der Netzwerkstandort keinen Verwaltungsserver enthält, stellt DRA eine Verbindung zum Server mit der nächstbesten Verfügbarkeit in der verwalteten Domäne bzw. im verwalteten Teilbaum her. Sie können auch angeben, zu welchem Verwaltungsserver oder zu welcher Domäne Sie eine Verbindung herstellen möchten.

Wenn Sie die Benutzeroberfläche zum ersten Mal starten, stellt DRA anfänglich eine Verbindung zur Domäne Ihres Anmeldekontos her. Wenn Sie an einer Domäne angemeldet sind, die zurzeit von keinem Verwaltungsserver verwaltet wird, oder wenn DRA keine Verbindung zum Verwaltungsserver der Domäne herstellen kann, wird in DRA möglicherweise eine Fehlermeldung angezeigt. Stellen Sie sicher, dass der Verwaltungsserver verfügbar ist, und versuchen Sie es erneut.

So stellen Sie eine Verbindung zu einem Verwaltungsserver her:

1. Klicken Sie im Menü „Datei“ auf **Mit Server verbinden**.
2. Klicken Sie auf **Mit diesem DRA-Server verbinden**.
3. Geben Sie den Namen des Verwaltungsservers im folgenden Format ein: *Computername*.
4. Klicken Sie auf **OK**.

So stellen Sie eine Verbindung zu einer verwalteten Domäne oder einem verwalteten Computer her:

1. Klicken Sie im Menü „Datei“ auf **Mit Server verbinden**.

2 Wählen Sie die gewünschte Option aus und geben Sie den Namen der verwalteten Domäne oder des verwalteten Computers ein.

3 Um beispielsweise eine Verbindung zur Domäne „HOULAB“ herzustellen, klicken Sie auf **Mit einem DRA-Server verbinden, der eine bestimmte Domäne verwaltet** und geben Sie dann H0ULAB ein.

4 Um einen Verwaltungsserver für die verwaltete Domäne oder den verwalteten Computer anzugeben, klicken Sie auf **Erweitert** und wählen Sie dann die geeignete Option aus.

5 Klicken Sie auf **OK**.

2.2.2 Ändern des Konsolentitels

Sie können die in der Titelleiste der Delegierungs- und Konfigurationskonsole angezeigten Informationen ändern. Zur besseren Übersichtlichkeit können Sie den Benutzernamen, mit dem die Konsole gestartet wurde, und den Verwaltungsserver, mit dem die Konsole verbunden ist, hinzufügen. In komplexen Umgebungen, in denen Sie eine Verbindung zu mehreren Verwaltungsservern mit unterschiedlichen Berechtigungsnachweisen herstellen müssen, können Sie mithilfe dieser Funktion schnell ermitteln, welche Konsole Sie verwenden müssen.

So ändern Sie die Titelleiste der Konsole:

1 Starten Sie die Delegierungs- und Konfigurationskonsole.

2 Klicken Sie auf **View** (Ansicht) > **Options** (Optionen).

3 Wählen Sie die Registerkarte „Window Title“ (Fenstertitel) aus.

4 Legen Sie die gewünschten Optionen fest und klicken Sie auf **OK**.

2.2.3 Anpassen der Listenspalten

Sie können auswählen, welche Objekteigenschaften DRA in den Listenspalten anzeigt. Mit dieser flexiblen Funktion können Sie die Benutzeroberfläche anpassen, beispielsweise die Suchergebnislisten, um die besonderen Verwaltungsanforderungen in Ihrem Unternehmen zu erfüllen. Sie können zum Beispiel Spalten zum Anzeigen des Benutzeranmeldenamens oder des Gruppentyps festlegen, sodass Sie schnell und effizient die erforderlichen Daten finden und sortieren können.

So passen Sie Listenspalten an:

1 Wählen Sie den geeigneten Knoten aus. Wenn Sie beispielsweise wählen möchten, welche Spalten beim Anzeigen von Suchergebnissen zu verwalteten Objekten angezeigt werden, wählen Sie **All My Managed Objects** (Alle meine verwalteten Objekte) aus.

2 Klicken Sie im Anzeigemenü auf **Choose Columns** (Spalten wählen).

3 Wählen Sie aus der Liste der für diesen Knoten verfügbaren Eigenschaften die Objekteigenschaften aus, die angezeigt werden sollen.

4 Um die Spaltenreihenfolge zu ändern, wählen Sie eine Spalte aus und klicken Sie auf **Move Up** (Nach oben verschieben) oder auf **Move Down** (Nach unten verschieben).

5 Um die Spaltenbreite festzulegen, wählen Sie eine Spalte aus und geben Sie die gewünschte Anzahl an Pixeln im bereitgestellten Feld ein.

6 Klicken Sie auf **OK**.

2.2.4 Verwalten von Objekten in der Konto- und Ressourcenverwaltung

Um Objekte in der Konto- und Ressourcenverwaltung zu verwalten, wählen Sie **All My Managed Objects** (Alle meine verwalteten Objekte) oder einen Unterknoten im Verzeichnisbaum aus. Hier können Sie Objekte in Domänen, in Containern und organisatorischen Einheiten nach Objekttyp suchen.

Wenn Sie ein Objekt in der Suchergebnisliste auswählen, sind alle anwendbaren Aktionen, die Sie für das Objekt ausführen können, in der Symbolleiste im Menü **Aufgaben** oder im Kontextmenü verfügbar. Die verfügbaren Optionen hängen vom ausgewählten Objekttyp, von den zurzeit für DRA konfigurierten Komponenten und von den Ihnen zugewiesenen Administratorberechtigungen ab.

Um die Eigenschaften eines Objekts zu bearbeiten, wählen Sie das Objekt aus und klicken Sie auf **Eigenschaften** im Menü **Aufgaben**. Von hier können Sie auf alle Eigenschaftenseiten des Objekts zugreifen, in dem Sie im linken Navigationsbereich auf die Seitenlinks klicken.

WICHTIG: Wenn Sie ein **Objekt vor dem unbeabsichtigten Löschen schützen** möchten, wählen Sie das Objekt aus und öffnen Sie **Eigenschaften**, wählen Sie im Navigationsbereich **Allgemein** aus, aktivieren Sie das Kontrollkästchen für diese Funktion und klicken Sie dann auf **Anwenden**, um die Änderungen zu übernehmen.

Weitere Informationen zu den Aktionen, die Sie für Objekte ausführen können, finden Sie in den folgenden Themen:

- Verwalten von Benutzerkonten, Gruppen und Kontakten
- Verwalten von Exchange-Postfächern und öffentlichen Ordnern
- Verwalten von Ressourcen

2.2.5 Ausführen gespeicherter erweiterter Abfragen

Mit erweiterten Abfragen können Sie Benutzer, Kontakte, Gruppen, Computer, Drucker, Organisationseinheiten und beliebige andere von DRA unterstützte Objekte suchen. Wenn Sie über die Befugnis zum Ausführen gespeicherter erweiterter Abfragen verfügen, können Sie die in der Liste **Saved Queries** (Gespeicherte Abfragen) verfügbaren erweiterten Abfragen für einen beliebigen Container im Knoten der Konto- und Ressourcenverwaltung ausführen. Weitere Informationen zu den Ihnen zugewiesenen Befugnissen finden Sie unter Anzeigen der eigenen zugewiesenen Befugnisse und Rollen.

So führen Sie gespeicherte erweiterte Abfragen aus:

1. Erweitern Sie **Account and Resource Management** (Konto- und Ressourcenverwaltung) > **All My Managed Objects** (Alle meine verwalteten Objekte).
2. Wählen Sie den geeigneten Container aus. Wenn DRA zum Beispiel nach Benutzerkontoinformationen suchen soll, wählen Sie **Users** (Benutzer) aus.
3. Um den Bereich für erweiterte Suchen anzuzeigen, klicken Sie auf **Advanced Search** (Erweiterte Suche).

4 Wählen Sie im Bereich der erweiterten Suchen eine erweiterte Suchabfrage aus der Liste **Saved Queries** (Gespeicherte Abfragen) aus.

5 Klicken Sie auf **Load Query** (Abfrage laden) und dann auf **Find Now** (Jetzt suchen).

2.2.6 Wiederherstellen der Konsoleneinstellungen

Sie können die Fenstergröße in DRA ändern. Die geänderten Fenstergrößen werden dann beibehalten. Auch viele andere Einstellungen werden beibehalten, wie der letzte Verwaltungsserver, zu dem Sie eine Verbindung hergestellt haben, hinzugefügte oder entfernte Spalten in Listenergebnissen und Spaltenbreiten. Mit der Option „Restore Default Settings“ (Standardeinstellungen wiederherstellen) können Sie die ursprünglichen Einstellungen wiederherstellen, mit denen Sie DRA installiert haben.

So stellen Sie die standardmäßigen Konsoleneinstellungen wieder her:

1 Klicken Sie auf **View** (Ansicht) > **Options** (Optionen).

2 Wählen Sie die Registerkarte **Saved Settings** (Gespeicherte Einstellungen) aus.

3 Überprüfen Sie die im Fenster angezeigten Informationen und klicken Sie dann auf **Restore Default Settings** (Standardeinstellungen wiederherstellen).

2.2.7 Verwenden von Sonderzeichen

Die unten aufgeführten Sonderzeichen sind für das Benennen von Benutzerkonten, Gruppen, Kontakten, Organisationseinheiten, Computern, ActiveViews, Hilfsadministratorgruppen, Rollen, Richtlinien und Automatisierungsauslösern nicht zulässig. Diese Einschränkungen gelten sowohl für den Namen des Objekts als auch für den Namen der Regel, die das Objekt definiert.

Benutzerkonten, Gruppen und Computer benennen

Zum Festlegen eines Namens in Umgebungen vor Windows 2000 sind folgende Sonderzeichen nicht zulässig:

Umgekehrter Schrägstrich	\
Doppelpunkt	:
Komma	,
Doppeltes Anführungszeichen	"
Gleichheitszeichen	=
Schrägstrich	/
Größer als	>
Eckige Klammer links	[
Kleiner als	<
Pluszeichen	+
Eckige Klammer rechts	]
Semikolon	;

Senkrechter Strich	|

WICHTIG: Für die Verwaltung öffentlicher Ordner wird der umgekehrte Schrägstrich (\) nicht unterstützt.

Zum Benennen von Benutzerkonten, Gruppen und Computern in Microsoft Windows-Domänen können Sie beliebige Sonderzeichen verwenden.

Kontakte und Organisationseinheiten benennen

Zum Benennen von Kontakten und Organisationseinheiten können Sie beliebige Sonderzeichen verwenden.

ActiveViews, Hilfsadministratorgruppen und Rollen benennen

Zum Benennen von ActiveViews, Hilfsadministratorgruppen und Rollen darf kein umgekehrter Schrägstrich (\) verwendet werden.

Richtlinien und Automatisierungsauslöser benennen

Zum Benennen von Richtlinien und Automatisierungsauslösern darf kein umgekehrter Schrägstrich (\) verwendet werden.

Ungültige Zeichen in Azure

Ungültige Zeichen führen zu Fehlern bei der Synchronisierung zwischen Azure Active Directory und dem Verzeichnis vor Ort. Weitere Informationen zu diesen ungültigen Zeichen finden Sie im Abschnitt „Directory object and attribute preparation“ (Verzeichnisobjekt- und Attributsvorbereitung) auf der Microsoft Office Support-Website.

Gehen Sie folgendermaßen vor, um sicherzustellen, dass diese Zeichen nicht in den Eigenschaften von Online-Postfächern verwendet werden:

1. Klicken Sie in der Delegierungs- und Verwaltungskonsole auf den Knoten „Configuration Management“ (Konfigurationsmanagement) und wählen Sie **Update Administration Server Options** (Optionen für Verwaltungsserver aktualisieren) aus.
2. Klicken Sie im Registerkartenmenü auf **Azure Sync** (Azure-Synchronisierung).
3. Klicken Sie auf **Enforce online mailbox policies for invalid characters and character length** (Online-Postfachrichtlinien für ungültige Zeichen und Zeichenlänge erzwingen) und dann auf **OK**.

2.2.8 Verwenden von Platzhalterzeichen

DRA unterstützt die Verwendung von Platzhalterzeichen in zahlreichen Feldern der DRA-Konsolen und für Befehle in der Befehlszeilenschnittstelle. Mit Platzhaltern können Sie Regeln definieren, die mehrere Objekte in Bezug auf eine bestimmte Bedingung oder einen Standard abgleichen, zum Beispiel in Bezug auf eine Namenskonvention. Mithilfe von Platzhaltern anstelle von regulären Ausdrücken können Sie den Umfang einer Regel verfeinern oder erweitern. Die Groß- und Kleinschreibung wird für Platzhalter nicht beachtet. Wenn Sie die Platzhalterzeichen Fragezeichen

(?), Sternchen (*) oder Raute (#) als normale Zeichen verwenden möchten, stellen Sie diesem besonderen Platzhalterzeichen einen umgekehrten Schrägstrich (\) voran. Wenn Sie beispielsweise nach abc* suchen möchten, geben Sie den Suchtext abc* ein.

DRA unterstützt die folgenden Platzhalterzeichen. Platzhalterzeichen dürfen nicht in Namen verwendet werden.

Platzhalter für	Zeichen	Definition
Beliebiges Zeichen	Fragezeichen ?	Entspricht genau einem Zeichen
Beliebige Ziffer	Nummernzeichen #	Entspricht einer Ziffer
Beliebiges Zeichen, 0 oder mehr Übereinstimmungen	Sternchen *	Entspricht null oder mehreren Zeichen

Die folgende Tabelle zeigt Beispiele für die Verwendung von Platzhalterzeichen und passenden Entsprechungen.

Beispiel	Entspricht	Keine Übereinstimmung
Den???	„Denton“ und „Dennis“	Denison
El ????o	„El Campo“ und „El Indio“	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA unterstützt keine Platzhalterangaben, die logische Operationen enthalten.

2.2.9 Anzeigen der eigenen zugewiesenen Befugnisse und Rollen

Rollen und Befugnisse bestimmen, wie Sie Objekte verwalten. Eine Rolle ist ein Satz an Befugnissen, die die erforderlichen Berechtigungen zum Ausführen bestimmter Verwaltungsaufgaben bereitstellen, zum Beispiel zum Erstellen von Benutzerkonten oder Verschieben von freigegebenen Verzeichnissen.

Der DRA-Administrator weist Rollen zu, fügt Sie zu bestimmten Hilfsadministratorgruppen hinzu und verknüpft Sie mit ActiveVies (Sätzen an Domänenobjekten, die Sie verwalten können). Sie können diese Zuweisungen über die Delegierungs- und Konfigurationskonsole anzeigen. Sie benötigen keine Zusatzrechte, um die Ihnen zugewiesenen Rollen und Befugnisse anzuzeigen.

So zeigen Sie die Ihnen zugewiesenen Befugnisse und Rollen an:

1. Klicken Sie im Dateimenü auf **DRA Properties** (DRA-Eigenschaften).
2. Klicken Sie auf **Powers** (Befugnisse).
3. Wählen Sie die geeignete Ansicht aus. Klicken Sie beispielsweise auf **Flat view** (Flache Ansicht), um eine Tabelle Ihrer Mitgliedschaften in Hilfsadministratorgruppen, Ihrer zugewiesenen Befugnisse und Rollen und die verknüpften ActiveViews anzuzeigen.

4 Erweitern Sie das entsprechende Element. Erweitern Sie beispielsweise in der Spalte **Has Power** (Hat Befugnis) den Eintrag **Roles and Powers** (Rollen und Befugnisse), um die einzelnen Ihnen zugewiesenen Rollen oder Befugnisse anzuzeigen.

5 Klicken Sie auf **OK**.

2.2.10 Anzeigen der Produktversionsnummer und installierter HotFixes

Über das DRA-Eigenschaftenfenster können Sie die Produktversionsnummer und die installierten HotFixes anzeigen. In diesem Fenster werden die Versionsnummern und die Liste der installierten HotFixes für den Verwaltungsserver und den DRA-Clientcomputer angezeigt.

So zeigen Sie die Produktversionsnummer und die installierten HotFixes an:

1 Klicken Sie im Dateimenü auf **DRA Properties** (DRA-Eigenschaften).

2 Klicken Sie auf **General** (Allgemein).

3 Zeigen Sie die gewünschten Informationen an.

4 Klicken Sie auf **OK**.

2.2.11 Anzeigen der aktuellen Lizenz

Für DRA ist eine Lizenzschlüsseldatei erforderlich. Sie können die Produktlizenz auf jedem Verwaltungsserver-Computer anzeigen. Sie benötigen keine zusätzlichen Befugnisse, um die Produktlizenz anzuzeigen.

So zeigen Sie die Lizenz an:

1 Klicken Sie im Dateimenü auf **DRA Properties** (DRA-Eigenschaften).

2 Klicken Sie auf **License** (Lizenz).

3 Überprüfen Sie die Lizenzeigenschaften und klicken Sie dann auf **OK**.

2.2.12 Wiederherstellen eines BitLocker-Passworts

Microsoft BitLocker speichert Wiederherstellungskennwörter in Active Directory. Mit den entsprechenden Befugnissen können Sie mit der DRA-BitLocker-Wiederherstellungsfunktion verlorene BitLocker-Kennwörter für Endbenutzer wiederherstellen.

WICHTIG: Stellen Sie sicher, dass Ihr Computer einer Domäne zugewiesen ist und dass BitLocker eingeschaltet ist, bevor Sie die BitLocker-Wiederherstellungskennwortfunktion verwenden.

Anzeigen und Kopieren eines BitLocker-Wiederherstellungskennworts

Wenn das BitLocker-Kennwort für einen Computer verloren wurde, kann es mit dem Wiederherstellungsschlüssel aus den Computereigenschaften in Active Directory zurückgesetzt werden. Kopieren Sie den Kennwortschlüssel und teilen Sie ihn dem Endbenutzer mit.

So zeigen Sie ein Wiederherstellungskennwort an und kopieren es:

1. Starten Sie die Delegierungs- und Konfigurationskonsole und wechseln Sie zu **Account and Resource Management** (Konto- und Ressourcenverwaltung) > **All My Managed Objects** (Alle meine verwalteten Objekte).
2. Wählen Sie die Domäne aus und führen Sie eine Suche aus, um alle Computer in der Domäne aufzulisten.
3. Klicken Sie in der Computerliste mit der rechten Maustaste auf den gewünschten Computer und wählen Sie **Properties** (Eigenschaften) > **BitLocker Recovery Password** (BitLocker-Wiederherstellungspasswort) aus.
4. Klicken Sie mit der rechten Maustaste und kopieren Sie das BitLocker-Wiederherstellungspasswort. Fügen Sie den Passworttext in eine Textdatei ein.

Suchen eines Wiederherstellungskennworts

Wenn der Name des Computers geändert wurde, muss das Wiederherstellungspasswort in der Domäne mit den ersten acht Zeichen der Kennwort-ID gesucht werden.

So suchen Sie ein Wiederherstellungskennwort unter Verwendung der Kennwort-ID:

1. Starten Sie die Delegierungs- und Konfigurationskonsole und wechseln Sie zu **Account and Resource Management** (Konto- und Ressourcenverwaltung) > **All My Managed Objects** (Alle meine verwalteten Objekte).
2. Klicken Sie mit der rechten Maustaste auf **Managed Domain** (Verwaltete Domäne) und klicken Sie dann auf **Find BitLocker Recovery Password** (BitLocker-Wiederherstellungskennwort suchen).

   Um die ersten acht Zeichen des Wiederherstellungskennworts zu ermitteln, befolgen Sie die Anweisungen unter Anzeigen und Kopieren eines BitLocker-Wiederherstellungskennworts.
3. Fügen Sie auf der Seite **Find BitLocker Recovery Password** (BitLocker-Wiederherstellungskennwort suchen) die kopierten Zeichen in das Suchfeld ein und klicken Sie dann auf **Search** (Suche).

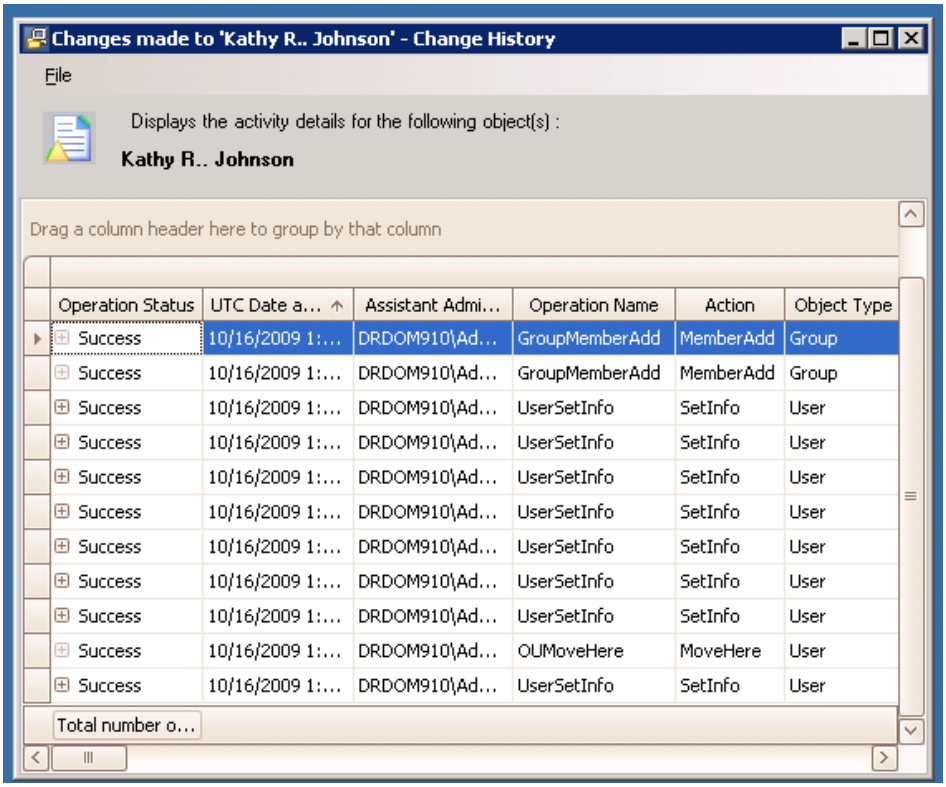
2.3 DRA-Berichterstellung

Die DRA-Berichterstellung bietet integrierte, einsatzbereite Berichte, mit denen Sie schnell doppelte Konten, die letzten Kontoanmeldungen, Details zu Microsoft Exchange-Postfächern und viele weitere Informationen nachverfolgen können. Reporting bietet außerdem Echtzeitdetails zu den Änderungen, die in der Umgebung vorgenommen wurden, einschließlich der Vorher- und Nachher-Werte für geänderte Eigenschaften. Sie können Berichte exportieren, drucken, anzeigen oder zu SQL Server Reporting Services veröffentlichen.

DRA bietet zwei Methoden zum Generieren von Berichten, mit denen Sie Benutzerkonto-, Gruppen- und Ressourcendefinitionen in der Domäne sammeln und überprüfen können: **Aktivitätsdetailberichte** und **DRA-Verwaltungsberichte**. Aktivitätsdetailberichte werden über die

Delegierungs- und Konfigurationskonsole angezeigt und bieten Echtzeitänderungsinformationen zu Objekten in der Domäne. Mit Aktivitätsdetailberichten können Sie beispielsweise eine Liste der Änderungen anzeigen, die innerhalb eines bestimmten Zeitraums an oder von einem Objekt vorgenommen wurden.

Die folgende Abbildung zeigt ein Beispiel eines Aktivitätsdetailberichts:



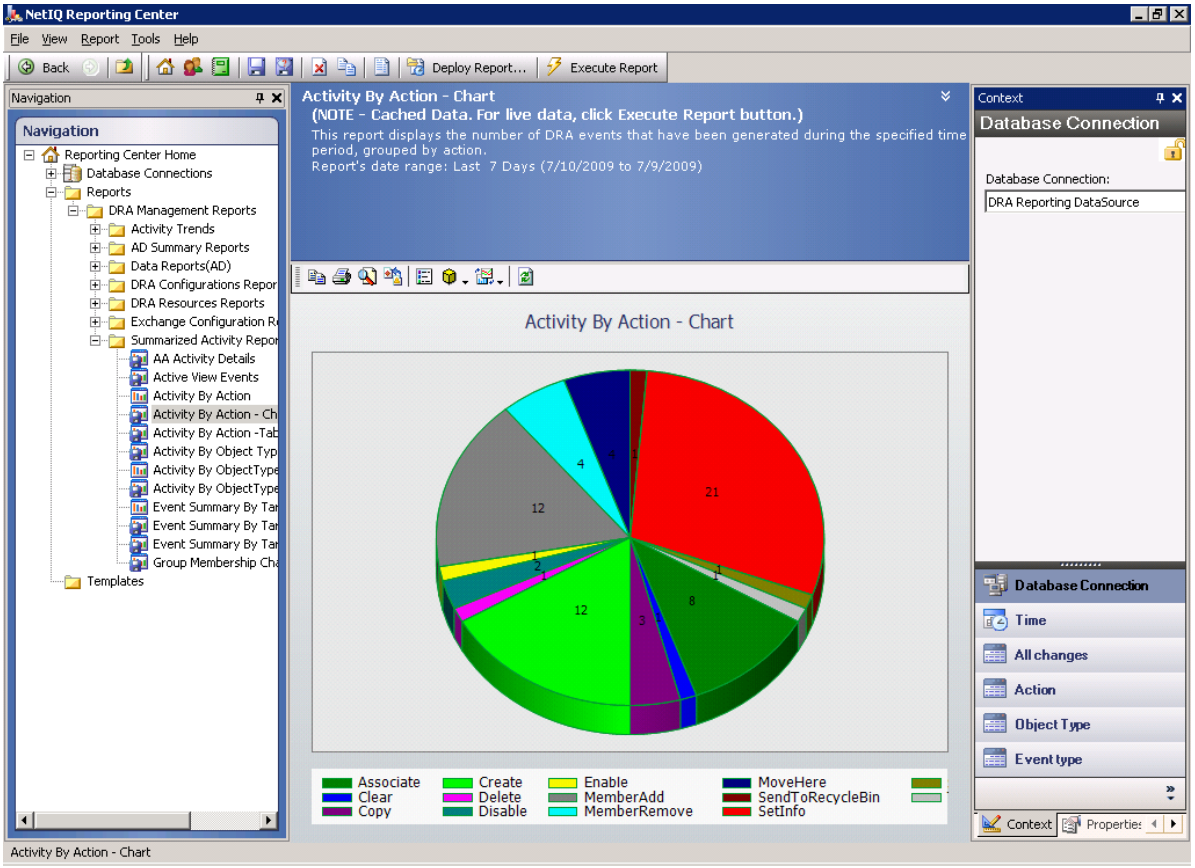
Optionale **DRA-Verwaltungsberichte**, die über NetIQ Reporting Center (Reporting Center) angezeigt werden können, bieten Aktivitäts-, Konfigurations- und Übersichtsinformationen zu Ereignissen in den verwalteten Domänen. Bestimmte Verwaltungsberichte sind als grafische Darstellung der Daten verfügbar. Diese integrierten Berichte können auch angepasst werden, damit sie genau die für Ihre Anforderungen geeigneten Informationen enthalten.

Mithilfe von Verwaltungsberichten können Sie beispielsweise eine Grafik anzeigen, die die Anzahl der Ereignisse in jeder verwalteten Domäne für einen bestimmten Zeitraum darstellt. Mit Reporting können Sie Details zum DRA-Sicherheitsmodell, wie ActiveView- und Hilfsadministratorgruppen-Definitionen, anzeigen.

Sie müssen die optionalen Verwaltungsberichte installieren, um diese Berichte anzeigen zu können. Weitere Informationen zum Installieren von Berichterstellungskomponenten finden Sie im *Installationshandbuch*. Weitere Informationen zur DRA-Berichterstellung finden Sie in „DRA-Berichterstellung“, auf Seite 36.

Starten Sie die Reporting Center-Konsole in der Programmgruppe „NetIQ > Reporting Center“.

Die folgende Abbildung zeigt die Reporting Center-Benutzeroberfläche mit ausgewählten DRA-Verwaltungsberichten.



Weitere Informationen zu DRA Reporting finden Sie in den folgenden Themen:

- Abschnitt 2.3.1, „Grundlegendes zur DRA-Berichterstellung“, auf Seite 38
- Abschnitt 2.3.2, „Verwendung von Protokollarchiven in DRA“, auf Seite 39
- Abschnitt 2.3.3, „Datums- und Uhrzeitangaben“, auf Seite 40
- Abschnitt 2.3.4, „DRA-Berichterstellungsaufgaben“, auf Seite 40

2.3.1 Grundlegendes zur DRA-Berichterstellung

Die DRA-Berichterstellung bietet zwei Methoden zum Generieren von Berichten, in denen Sie die neuesten Änderungen in Ihrer Umgebung anzeigen und Definitionen für Benutzerkonten-, Gruppen- und Ressourcendefinitionen in der Domäne erfassen und überprüfen können.

Aktivitätsdetailberichte

Diese Berichte, auf die Sie über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole zugreifen können, bieten Echtzeitinformationen zu Änderungen an den Objekten in der Domäne.

DRA-Verwaltungsberichte

Diese Berichte sind über NetIQ Reporting Center (Reporting Center) verfügbar und bieten Aktivitäts-, Konfigurations- und Übersichtsinformationen zu Ereignissen in den verwalteten Domänen. Bestimmte Berichte sind als grafische Darstellung der Daten verfügbar.

Mit Aktivitätsdetailberichten können Sie beispielsweise eine Liste der Änderungen anzeigen, die innerhalb eines bestimmten Zeitraums an oder von einem Objekt vorgenommen wurden. Sie können mit Verwaltungsberichten auch eine Grafik anzeigen, die die Anzahl der Ereignisse in jeder verwalteten Domäne für einen bestimmten Zeitraum darstellt. Mit Reporting können Sie außerdem Details zum DRA-Sicherheitsmodell, wie ActiveView- und Hilfsadministratorgruppen-Definitionen, anzeigen.

Funktionen und Berichte, die von Ihrer Lizenz nicht unterstützt werden, sind in DRA deaktiviert. Außerdem müssen Sie über die geeigneten Befugnisse verfügen, um Berichte ausführen und anzeigen zu können. Deshalb haben Sie unter Umständen keinen Zugriff auf bestimmte Berichte.

DRA-Verwaltungsberichte können als optionale Funktion installiert und konfiguriert werden und werden in Reporting Center angezeigt. Wenn Sie die Datensammlung aktivieren und konfigurieren, erfasst DRA Informationen über Revisionsereignisse und exportiert die Informationen gemäß einem von Ihnen definierten Zeitplan in eine SQL Server-Datenbank. Wenn Sie diese Datenbank in Reporting Center verbinden, erhalten Sie Zugriff auf über 60 integrierte Berichte:

- Aktivitätsberichte zeigen, wer wann welche Aktionen ausgeführt hat
- Konfigurationsberichte zeigen den Status von AD oder DRA zu einem bestimmten Zeitpunkt
- Zusammenfassungsberichte zeigen die Menge der Aktivitäten

Weitere Informationen zur Konfiguration der Datenerfassung für Verwaltungsberichte finden Sie im *Administratorhandbuch*.

2.3.2 Verwendung von Protokollarchiven in DRA

Zur Überprüfung und Berichterstellung von Hilfsadministratoraktionen protokolliert DRA alle Benutzervorgänge im Protokollarchive auf dem Verwaltungsservercomputer. Benutzervorgänge umfassen alle Versuche, Definitionen zu ändern, zum Beispiel das Aktualisieren von Benutzerkonten, das Löschen von Gruppen oder das Neudefinieren von ActiveViews. DRA protokolliert außerdem spezifische interne Operationen, zum Beispiel die Initialisierung des Verwaltungsservers und verknüpfte Serverinformationen. Neben diesen Revisionsereignissen protokolliert DRA die Vorher- und Nachher-Werte zum Ereignis, damit genau nachverfolgt werden kann, was geändert wurde.

DRA verwendet den Ordner **NetIQLogArchiveData**, das sogenannte **Protokollarchiv**, um die archivierten Protokolldaten sicher zu speichern. DRA archiviert die Protokolle im Laufe der Zeit und löscht dann ältere Daten, um Platz für neuere Daten zu schaffen. Dieser Vorgang wird als Bereinigung bezeichnet.

DRA verwendet die Revisionsereignisse, die in den Protokollarchivdateien gespeichert sind, zum Anzeigen der Aktivitätsdetailberichte, beispielsweise um anzuzeigen, welche Änderungen innerhalb eines bestimmten Zeitraums an einem Objekt vorgenommen wurden. Sie können DRA auch so konfigurieren, dass die Informationen aus diesen Protokollarchivdateien zu einer SQL Server-Datenbank exportiert werden, die NetIQ Reporting Center zum Anzeigen von Verwaltungsberichten verwendet.

DRA schreibt Revisionsereignisse immer in das Protokollarchiv. Sie können festlegen, ob DRA die Ereignisse zusätzlich in die Windows-Ereignisprotokolle schreiben soll.

Weitere Informationen zur Revision in DRA finden Sie im *Administratorhandbuch*.

2.3.3 Datums- und Uhrzeitangaben

Für die Berichtanzeige verwendet DRA den **Stil „kurzes Datum“** und den **Uhrzeitstil**, die in der Anwendung für die Ländereinstellungen in der Systemsteuerung festgelegt sind. DRA-Berichte enthalten für die Ereignisse neben dem örtlichen Datum und der örtlichen Uhrzeit auch die Datum- und Uhrzeitangabe im UTC-Format. DRA-Bericht unterstützen die folgenden Datumsformate:

- `m/t/jj`
- `m-t-jj`
- `m/t/jjjj`
- `m-t-jjjj`
- `mm/tt/jj`
- `mm-tt-jj`
- `mm/tt/jjjj`
- `mm-tt-jjjj`
- `tt/mm/jj`
- `tt-mm-jj`
- `tt/mm/jjjj`
- `tt-mm-jjjj`

2.3.4 DRA-Berichterstellungsaufgaben

Um DRA-Verwaltungsberichte zu generieren, installieren Sie Reporting Center und aktivieren Sie die Datenerfassung in DRA. Weitere Informationen zum Aktivieren der Datenerfassung finden Sie im *Administratorhandbuch*. Um Aktivitätsdetailberichte zu generieren, klicken Sie mit der rechten Maustaste auf ein beliebiges Objekt und klicken Sie dann auf **Berichterstellung**, um die Auswahl an Berichten für dieses Objekt anzuzeigen. Die folgenden Abschnitte führen Sie durch die verschiedenen Aufgaben der Berichterstellung.

Anzeigen von Aktivitätsdetailberichten

Aktivitätsdetailberichte zeigen Informationen über Änderungen in der Umgebung an. Sie können die Berichte anzeigen, drucken und im Excel-, CSV- oder TXT-Format speichern. Um Berichte anzeigen oder drucken zu können, muss Ihnen die Rolle für die Berichterstellungsadministration zugewiesen sein.

Geben Sie beim Anzeigen von Berichten Kriterien zum Festlegen des Zeitraums an, für den die Informationen angezeigt werden sollen. Sie können auch Berichte anzeigen, die auf die Änderungen auf bestimmten DRA-Servern beschränkt sind, und Sie können die Anzahl der im Bericht enthaltenen Zeilen begrenzen. Wenn die Berichtgröße einen der folgenden Grenzwerte überschreitet, wird in DRA eine Meldung angezeigt, die darauf hinweist, dass der Bericht nicht vollständig ist:

- Größe überschreitet 500 MB
- Zeit zum Abfragen aller DRA-Server überschreitet 5 Minuten
- Anzahl der anzuzeigenden Zeilen überschreitet 1000

Sie können dann wahlweise den Bericht mit den bisher abgerufenen Informationen anzeigen oder die Berichtkriterien ändern, um einen Bericht zu generieren, der diese Grenzwerte einhält.

So zeigen Sie einen Bericht an:

1. Erweitern Sie im linken Bereich **All My Managed Objects** (Alle meine verwalteten Objekte).
2. Um ein Objekt festzulegen, für das ein Bericht angezeigt werden soll, führen Sie die folgenden Schritte aus:
   - **2a** ***Wenn Sie den Objektstandort kennen***, wählen Sie die Domäne und die Organisationseinheit aus, die das Objekt enthalten.
   - **2b** Geben Sie im Suchbereich die Objektattribute ein und klicken Sie auf **Jetzt suchen**.
3. Klicken Sie im linken Bereich mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Berichterstellung**.
4. Wählen Sie die Art des Berichts aus, zum Beispiel **Änderungen an [Objektname]** oder **Änderungen durch [Objektname]**. Welche Berichte verfügbar sind, hängt vom ausgewählten Objekttyp ab.
5. Wählen Sie das Anfangs- und Enddatum aus, um den gewünschten Zeitraum der Änderungen festzulegen.
6. ***Wenn Sie die Anzahl der angezeigten Zeilen ändern möchten***, überschreiben Sie den Standardwert von 250 mit einem anderen Wert.

   HINWEIS: Die angezeigte Anzahl an Zeilen gilt für jeden Verwaltungsserver in Ihrer Umgebung. Wenn Sie 3 Verwaltungsserver in den Bericht einschließen und den Standardwert von 250 Zeilen verwenden, können bis zu 750 Zeilen im Bericht angezeigt werden.

   ---

7. ***Wenn Sie nur bestimmte Verwaltungsserver in den Bericht einschließen möchten***, wählen Sie **Abfrage auf diese DRA-Server beschränken** aus und geben Sie die Namen der Server ein, die eingeschlossen werden sollen. Trennen Sie mehrere Servernamen durch Kommas.
8. Klicken Sie auf **OK**.

HINWEIS: Es kann bis zu 5 Sekunden dauern, bis DRA die neuesten Änderungen in den Berichten anzeigt. Warten Sie nach dem Vornehmen einer Änderung deshalb mindestens 5 Sekunden, bevor Sie versuchen, den Bericht mit der Änderung anzuzeigen.

Exportieren von Aktivitätsdetailberichten

Sie können Aktivitätsdetailberichte in den folgenden Formaten exportieren: XLS, CSV und TXT. Standardmäßig ist das Microsoft Excel-Format festgelegt.

So exportieren Sie Aktivitätsdetailberichte:

1. Klicken Sie im Berichtfenster im Dateimenü auf **Vorschau anzeigen und exportieren**.
2. Klicken Sie im Vorschaufenster im Dateimenü auf **Dokument exportieren** > **Excel-Datei**.
3. Wählen Sie die Exportoptionen aus und klicken Sie auf **OK**.
4. Geben Sie im Fenster „Speichern unter“ einen Namen für die Datei ein und klicken Sie auf **Speichern**.

Drucken von Aktivitätsdetailberichten

Um Berichte drucken zu können, muss Ihnen die Rolle für die Berichterstellungsadministration zugewiesen sein. Sie können die Aktivitätsdetailberichte anzeigen, drucken oder in verschiedenen Formaten speichern.

So drucken Sie Aktivitätsdetailberichte:

1. Klicken Sie im Berichtfenster im Dateimenü auf **Vorschau anzeigen und exportieren**.
2. Klicken Sie im Vorschaufenster im Dateimenü auf **Drucken**.

Anzeigen von Verwaltungsberichten

Um Verwaltungsberichte in Reporting Center anzeigen zu können, müssen Sie die DRA-Berichterstellung installieren und die DRA-Datenkollektoren konfigurieren. Weitere Informationen zur Installation der DRA-Berichterstellung und Konfiguration der DRA-Kollektoren finden Sie im *Administratorhandbuch*.

Wenn Sie sich bei Reporting Center anmelden, bestätigt der Webservice über IIS die Kontoberechtigung gemäß der bei der Installation vorgenommenen Konfiguration des Webservices.

So zeigen Sie Verwaltungsberichte an:

1. Melden Sie sich am Computer an, auf dem die Reporting Center-Konsole ausgeführt wird.
2. Starten Sie die **Reporting Center-Konsole** in der Programmgruppe „NetIQ > Reporting Center“.
3. Geben Sie die erforderlichen Informationen im Anmeldedialogfeld an und klicken Sie auf **Anmelden**.
4. Erweitern Sie im Navigationsbereich den Eintrag **Berichte** > **DRA-Verwaltungsberichte**.
5. Erweitern Sie die Berichtkategorien, bis Sie den gewünschten Bericht gefunden haben.

6. Klicken Sie im Navigationsbereich auf den Berichtnamen. Der Bericht wird im Ergebnisbereich in der Mitte geladen und die im Cache gespeicherten Daten werden angezeigt.
7. ***Um den Bericht mit den neuesten Daten anzuzeigen***, klicken Sie im Ergebnisbereich auf **Bericht ausführen**.

Sie können die standardmäßigen Kontexteinstellungen ändern, um verschiedene Berichtergebnisse anzuzeigen. Weitere Informationen zu den Kontexteinstellungen in Reporting Center finden Sie im *Administratorhandbuch*.

Anpassen von Verwaltungsberichten

DRA wird mit über 60 Verwaltungsberichten bereitgestellt. In Reporting Center können Sie diese Berichte flexibel auf verschiedene Weisen anpassen und bereitstellen. Weitere Informationen zum Anpassen und Bereitstellen von Verwaltungsberichten in Reporting Center finden Sie im *Administratorhandbuch*.

So passen Sie einen Verwaltungsbericht an:

1. Zeigen Sie einen Bericht an, der dem gewünschten Bericht ähnelt. Weitere Informationen finden Sie unter Anzeigen von Verwaltungsberichten.
2. Passen Sie den Bericht an, indem Sie die Berichteigenschaften und Kontexteinstellungen so ändern, dass die gewünschten Informationen angezeigt werden.
3. Klicken Sie auf **Bericht ausführen**.
4. Klicken Sie im Berichtmenü auf **Bericht speichern unter** und geben Sie einen Titel und Speicherort für den neuen Bericht an.
5. Klicken Sie auf **Speichern**.

Weitere Informationen über das Arbeiten mit Verwaltungsberichten in Reporting Center finden Sie im *Administratorhandbuch*.

3 Suchen nach Objekten

Dieses Kapitel enthält grundlegende Informationen zur Suche und LDAP-Suche und beschreibt die Vorgehensweisen zum Verwenden dieser Suchfunktionen.

3.1 Suche

Mit DRA können Sie Objekte in der vor Ort bereitgestellten Active Directory-Domäne, in Microsoft Exchange und in Azure-Mandanten suchen. Sie können Benutzer und Gruppen in Ihren Azure-Mandanten, Objekte wie Benutzer, Gruppen, Kontakte, Computer, Drucker und organisatorische Einheiten in Ihren Active Directory-Domänen und Objekte wie Raumpostfächer, Gerätepostfächer, freigegebene Postfächer und dynamische Verteilergruppen in Exchange suchen. Verwenden Sie die Suchfilter, um die Suchen effizienter und wirksamer zu gestalten.

HINWEIS: Um beim Verwenden von Filtern eine genaue Rückgabe der gesuchten Objekte zu erhalten, sollten Änderungen an der Paginierung vor dem Anwenden der Filter und Ausführen der Suche vorgenommen werden. Das Ändern der Einstellung **Elemente pro Seite** unten in der Webkonsole wird nicht unterstützt, wenn Objekttypfilter angewendet sind.

Um auf die Suchfunktion in der Webkonsole zuzugreifen, wechseln Sie zu **Verwaltung** > **Suche**.

3.1.1 Verwenden von Platzhalterzeichen

DRA unterstützt Platzhalterzeichen wie Fragezeichen (?), Sternchen (*) und Doppelkreuz (#), mit denen Sie die Suchergebnisse verbessern können. Die Groß- und Kleinschreibung wird für Platzhalter nicht beachtet.

Die folgende Tabelle zeigt Beispiele für die Verwendung von Platzhalterzeichen und passenden Entsprechungen.

Zeichen	Platzhalter für
Fragezeichen ?	Beliebiges Zeichen oder einzelne Ziffer
Doppelkreuz #	Beliebige einzelne Ziffer
Sternchen *	Beliebige Folge an Zeichen oder Ziffern

3.1.2 Suchen in mehreren Feldern

Mit der Option „Übereinstimmung mehrerer Felder“ können Sie in einer einzigen Suche nach Übereinstimmungen in mehreren Attributen suchen. Wenn Sie mit der Option „Übereinstimmung mehrerer Felder“ suchen, wird die Suchzeichenkette mit mehreren Attributen verglichen, zum

Beispiel mit den Attributen Name, Anzeigename, Vorname und Nachname. Wenn der Wert eines dieser Attribute mit der Suchzeichenkette übereinstimmt, wird das Objekt in den Suchergebnissen zurückgegeben.

Die Option „Übereinstimmung mehrerer Felder“ unterstützt nur das Suchkriterium „**beginnt mit**“.

Wenn Sie beispielsweise zwei Benutzer haben, von denen einer für das Attribut *Anzeigename*den Wert „`Martin Smith`“ hat und der andere den Prinzipalnamen `martha.jones@acme.com`, und Sie eine Suche mit der Suchzeichenkette „`Mart`“ ausführen, werden beide Benutzer in den Suchergebnissen zurückgegeben.

In der Tabelle unten sind die Attribute aufgelistet, die für jeden Objekttyp durchsucht werden:

Objekttyp	Durchsuchte Attribute
Azure-Gruppe	displayName, mail
Azure-Benutzer	displayName, employeeId, givenName, mail, surname, userPrincipalName
Computer	displayName, name, sAMAccountName
Kontakt	displayName, employeeId, givenName, mail, mailNickname, name, surname
Dynamische Verteilergruppe	displayName, mail, mailNickname, name
Gruppe	displayName, mail, mailNickname, name, sAMAccountName
Organisatorische Einheit	name
Papierkorb	name, sAMAccountName
Benutzer	displayName, employeeId, givenName, mail, mailNickname, name, sAMAccountName, surname

HINWEIS: Die Funktion „Übereinstimmung mehrerer Felder“ wird nicht in Objektauswahlsuchen in der Delegierungs- und Konfigurationskonsole unterstützt, wenn Delegierungen oder Berechtigungen für die unten aufgelisteten Exchange-Objekte hinzugefügt werden:

- Benutzerpostfach
- E-Mail-aktivierter Benutzer
- E-Mail-aktivierte Gruppe
- E-Mail-aktivierter Kontakt
- dynamische Verteilergruppe
- freigegebenes Postfach
- Ressourcenpostfach

3.1.3 Hinzufügen und Sortieren von Spalten

Sie können die Suchergebnisobjekte nach einem beliebigen der folgenden Attribute sortieren, indem Sie auf den Spaltenkopf des gewünschten Attributs klicken:

- Alias
- Anzeigename
- Email
- Mitarbeiter-ID
- Vorname
- Nachname
- Standort
- Name
- Name vor Windows 2000
- Benutzerprinzipalname

Um Attributspalten hinzuzufügen oder zu entfernen, klicken Sie auf das Spaltensymbol.

3.2 Erweiterte Suche

Mit DRA können Sie über die Seite „Erweiterte Suche“ LDAP-Abfragen und Abfragen für virtuelle Attribute in den vor Ort bereitgestellten Active Directory-Domänen ausführen. Sie können eine Suche mit einer vorhandenen Abfrage ausführen, eine vorhandene Abfrage bearbeiten, eine neue Abfrage erstellen und neue oder bearbeitete Abfragen zur späteren Verwendung als öffentliche oder private Abfragen speichern. Verwenden Sie die Suchfilter, um die Suchen effizienter und wirksamer zu gestalten.

Um in der Webkonsole auf die Abfragefunktion der erweiterten Suche zuzugreifen, wechseln Sie zu **Verwaltung** > **Erweiterte Suche**.

3.2.1 Erweiterte Suchabfragen

DRA unterstützt Abfragen für virtuelle Attribute und LDAP-Abfragen zum Suchen von DRA- und Active Directory-Objekten. Virtuelle Attribute können mit Active Directory-Objekttypen wie Benutzern, Gruppen, dynamischen Verteilergruppen, Kontakten, Computern und organisatorischen Einheiten verknüpft werden. Mit einer Abfrage für virtuelle Attribute können Sie die von der LDAP-Abfrage zurückgegebenen Ergebnisse so filtern, dasss nur die Ergebnisse zurückgegeben werden, die mit der Abfrage für virtuelle Attribute übereinstimmen. Die Abfragezeichenketten für virtuelle Attribute müssen mit `(objectCategory=<Objekttyp>)` beginnen. Um eine Abfrage für virtuelle Attribute auszuführen, müssen Sie Zeichenketten für die LDAP-Abfrage und für die Abfrage für virtuelle Attribute angeben.

Beispiele für LDAP-Abfragen:

- Suche nach „allen Computerobjekten“ in DRA:

  LDAP-Abfrage: `(objectCategory=computer)`

- Suche nach Benutzerobjekten mit der Beschreibung „Umsatz Region Ost/West“ in DRA:

  LDAP-Abfrage: `(&(objectCategory=user)(description=Absatz Region Ost\5CWest))`

- Suche nach „allen Computerobjekten“ in DRA:

  LDAP-Abfrage: `(objectCategory=computer)`

WICHTIG: Der umgekehrte Schrägstrich muss in den LDAP-Filtern mit einer Escapesequenz verbunden werden. Ersetzen Sie den umgekehrten Schrägstrich durch \5C.

- „Liste aller deaktivierten Benutzerobjekte“ in DRA:

  LDAP-Abfrage:

  `(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2))`

  Die Zeichenkette `1.2.840.113556.1.4.803`steht für `LDAP_MATCHING_RULE_BIT_AND`. Dies steht für einen bitweisen AND-Operator eines Flag-Attributs (Ganzzahl), wie userAccountControl, groupType oder systemFlags, und eine Bitmaske (wie 2, 32 oder 65536). Die Klausel ist „true“ (wahr), wenn der bitweise AND-Operator des Attributwerts und die Bitmaske nicht null sind, d. h. wenn das Bit gesetzt ist.

Beispiele für Abfragen mit virtuellen Attributen:

- Suche nach Benutzern, deren Firmenname „ABC“ ist:

  Abfrage: `(&(objectCategory=User)(CompanyName=ABC))`

  Das DRA-Objekt ist „User“ (Benutzer) und das virtuelle Attribut ist „CompanyName“ (Firmenname; mit dem Benutzer verknüpft).

- Suchen nach allen Benutzern mit dem Firmennamen „ABC“ in der Domäne „Speicher“:

  Abfrage: `(&(objectCategory=User)(CompanyName=ABC)(Domain=Speicher))`

  Das DRA-Objekt ist „User“ (Benutzer) und die virtuellen Attribute sind „CompanyName“ (Firmenname; mit dem Benutzer verknüpft) und „Domain“ (Domäne; mit dem Benutzer verknüpft).

- Suche nach allen Gruppen mit dem Produktnamen „DRA“ und nach allen Benutzern mit dem Firmennamen „ABC“:

  Abfrage:

  `(|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=User)(CompanyName=ABC)))`

  Die DRA-Objekte sind „Group“ (Gruppe) und „User“ (Benutzer) und die virtuellen Attribute sind „CompanyName“ (Firmenname; mit dem Benutzer verknüpft) und „ProductGroupName“ (Produktgruppenname; mit der Gruppe verknüpft).

- Suche nach allen Gruppen, deren Produktname „DRA“ ist, und nach allen Benutzern mit dem Firmennamen „ABC“ in der Domäne „Speicher“:

Abfrage:

```
(|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=User)(CompanyName=ABC)(Domain=Speicher)))
```

Die DRA-Objekte sind „Group“ (Gruppe) und „User“ (Benutzer) und die virtuellen Attribute sind „CompanyName“ (Firmenname; mit dem Benutzer verknüpft), „ProductGroupName“ (Produktgruppenname; mit der Gruppe verknüpft) und „Domain“ (Domäne; mit dem Benutzer verknüpft).

3.2.2 Verwalten erweiterter Abfragen

Zur Unterstützung der Abfragefunktion mit erweiterter Suche wird LDAP in DRA verwendet. Mit erweiterten Abfragen können Sie Benutzer, Kontakte, Gruppen, Computer, organisatorische Einheiten und beliebige andere von DRA unterstützte Objekte suchen. Wenn Sie über die Befugnis „Execute Saved Advanced Queries“ (Gespeicherte erweiterte Abfragen ausführen) verfügen, können Sie erweiterte Abfragen ausführen, die in den Listen **Meine Suchen** und **Öffentliche Suchen** für einen beliebigen Container verfügbar sind.

Neben dem Ausführen einer Suche mit einer gespeicherten erweiterten Abfrage und dem Anzeigen der Abfragedetails können Sie mit den entsprechenden Berechtigungen über die Seite „Erweiterte Suche“ außerdem die folgenden Aktionen für erweiterte Abfragen ausführen:

Neue Abfrage erstellen

Erstellen Sie eine erweiterte Abfrage auf dem primären Verwaltungsserver oder dem sekundären Verwaltungsserver, indem Sie die Abfragezeichenkette (LDAP und ggf. virtuelles Attribut) für die neue erweiterte Abfrage angeben. Erweitern Sie nach dem Ausführen der Suche das Dropdown-Menü **Suche**, um die Abfrage in der Liste „Meine Suchen“ oder in der Liste „Öffentliche Suchen“ zu speichern.

Abfrage ändern

Wählen Sie unter „Meine Suchen“ oder „Öffentliche Suchen“ eine vorhandene erweiterte Abfrage aus und verwenden Sie die Option **Bearbeiten**, um beliebige Suchkriterien zu ändern. Nachdem Sie die Suche mit den aktualisierten Suchkriterien ausgeführt haben, können Sie je nach Bedarf das Dropdown-Menü **Suche** erweitern und **Speichern** auswählen, um die Änderungen an der Abfrage zu speichern.

Abfrage kopieren

Wählen Sie eine vorhandene erweiterte Abfrage unter „Meine Suchen“ oder „Öffentliche Suchen“ aus und führen Sie die Suche aus. Nachdem Sie die Suche ausgeführt haben, können Sie das Dropdown-Menü **Suche** erweitern und **Speichern unter** auswählen, um die Abfrage mit einem anderen Namen zu speichern.

Abfrageergebnisse anpassen

DRA stellt in der Suchergebnisliste einen standardmäßigen Satz an Spalten bereit. Um die Suchergebnisse einer gespeicherten oder nicht gespeicherten Abfrage anzupassen, klicken Sie rechts auf der Seite auf das Symbol **Spalten hinzufügen/entfernen**  , um die Art der Suchergebnisanzeige zu ändern.

Abfrage löschen

Sie können jede erweiterte Abfrage löschen, die in der Liste **Meine Suchen** enthalten ist. Mit den entsprechenden Berechtigungen können Sie auch erweiterte Abfragen löschen, die in der Liste **Öffentliche Suchen** enthalten sind. Um eine gespeicherte erweiterte Abfrage zu löschen, wählen Sie die Abfrage in der entsprechenden Liste aus und klicken Sie im Dropdown-Menü „Suche“ auf **Löschen**.

Inhalt der Abfrageformularfelder löschen

In der Webkonsole können Sie die Formularfelder einer gespeicherten oder nicht gespeicherten Abfrage löschen, um Änderungen von einem bereinigten Formular aus vorzunehmen. Um die Felder in einer Abfrage zu löschen, wählen Sie **Löschen** im Dropdown-Menü „Suche“ aus.

4 Verwalten von Benutzerkonten, Gruppen und Kontakten

Dieses Kapitel enthält grundlegende Informationen und eine Beschreibung der Vorgehensweisen zum Verwalten von Benutzerkonten, Gruppen, dynamischen Gruppen, dynamischen Verteilergruppen und Kontakten im Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole oder in der Webkonsole. Zu Benutzerkonten werden umfangreichere Informationen bereitgestellt, um die Verwaltung von Objekten in beiden Clientanwendungen allgemein an einem Beispiel zu beschreiben.

4.1 Verwalten von Benutzerkonten

Microsoft Windows bestimmt anhand des Benutzerkontotyps die Zugriffsberechtigungen des betreffenden Benutzerkontos. Ein Benutzer kann global oder lokal sein. DRA unterstützt auch InetOrgPerson-Objekte, betrachtet InetOrgPerson-Objekte jedoch als normale Benutzer.

Globales Benutzerkonto

Ein globales Benutzerkonto ist ein Benutzerkonto, das in jeder Domäne verwendet werden kann, die die Domäne, in der das Benutzerkonto erstellt wurde, verbürgt. Sie können einem Benutzerkonto spezifische Berechtigungen zuweisen. Sie können ein Benutzerkonto auch als Mitglied einer Gruppe festlegen und dann der Gruppe die gewünschten Berechtigungen zuweisen. Das Organisieren von Benutzerkonten in Gruppen vereinfacht die Verwaltung der Netzwerkberechtigungen für große Benutzeranzahlen.

Lokales Benutzerkonto

Ein lokales Benutzerkonto entspricht einem Konto, mit dem Sie sich beim Windows-Betriebssystem anmelden. Mit diesem Konto können Sie auf die Systemressourcen in Ihrem eigenen Benutzerbereich zugreifen.

Weitere Informationen zum Verwalten von Benutzerkonten finden Sie in den folgenden Themen:

- Abschnitt 4.1.1, „Benutzerkonten in verbürgten Domänen“, auf Seite 52
- Abschnitt 4.1.2, „Verwaltungsaufgaben für Benutzerkonten“, auf Seite 52
- Abschnitt 4.1.3, „Umwandeln von Benutzerkonten“, auf Seite 55

4.1.1 Benutzerkonten in verbürgten Domänen

Microsoft Windows speichert Benutzerkonto- und Gruppendefinitionen im Verzeichnis der verwalteten Domäne. Ein Verwaltungsserver kann daher nicht die Verzeichnisinformationen einer verbürgten Domäne ändern, sofern diese Domäne nicht ebenfalls von DRA verwaltet wird.

In der Konto- und Ressourcenverwaltung können beispielsweise Benutzerkonten und Gruppen angezeigt werden, die Sie nicht bearbeiten können. Diese Benutzerkonten und Gruppen sind in Domänen definiert, die von einer der verwalteten Domänen verbürgt sind. Sie können jedoch Konten und Gruppen einer verbürgten Domäne zu anderen Gruppen in der verwalteten Domäne hinzufügen.

4.1.2 Verwaltungsaufgaben für Benutzerkonten

Dieser Abschnitt beschreibt die Verwaltung von Benutzerkonten über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole und über die Webkonsole. Sofern Sie über die entsprechenden Befugnisse verfügen, können Sie verschiedene Verwaltungsaufgaben für Benutzerkonten ausführen, beispielsweise Konten erstellen oder löschen. Wenn Sie mehrere Benutzerkonten gleichzeitig auswählen, können Sie ausgewählte Aufgaben in einem Vorgang für mehrere Benutzer ausführen, beispielsweise Benutzer löschen, verschieben oder zu einer Gruppe hinzufügen. Weitere Informationen zu den Ihnen zugewiesenen Befugnissen finden Sie unter Anzeigen der eigenen zugewiesenen Befugnisse und Rollen.

Benutzerkontoaufgaben in der Konto- und Ressourcenverwaltung

Sie können alle anwendbaren, unten aufgeführten Aufgaben über das Menü **Aufgaben** oder über das Kontextmenü ausführen. Im Allgemeinen wählen Sie den Knoten **All My Managed Objects** (Alle meine verwalteten Objekte) aus und führen dann den Vorgang **Find Now** (Jetzt suchen) aus, um das gewünschte Benutzerobjekt zu suchen und auszuwählen. Wenn Sie einen neuen Benutzer erstellen möchten, wählen Sie die Domäne bzw. Organisationseinheit aus, in der Sie den Benutzer erstellen möchten. Das Aufgabenmenü zeigt, welche Aufgaben verfügbar sind, wenn Sie ein oder mehrere Benutzerkonten auswählen.

Eigenes Konto verwalten

Sie können Ihr eigenes Konto verwalten, indem Sie allgemeine Eigenschaften wie Ihre Telefonnummer ändern. Stellen Sie sicher, dass Sie über die erforderlichen Befugnisse verfügen, bevor Sie Ihr Konto verwalten.

Benutzerkonto in eine andere ActiveView kopieren

Sie können ein Benutzerkonto in eine andere ActiveView kopieren. Diese Aktion wird als Übertragen des Benutzerkontos bezeichnet. Um ein Benutzerkonto zu einer anderen ActiveView zu kopieren, benötigen Sie sowohl in der ursprünglichen ActiveView als auch in der als Ziel festgelegten ActiveView die Befugnis „Benutzer zu anderer ActiveView kopieren“. Beim Übertragen eines Benutzerkontos zu einer anderen ActiveView wird das Benutzerkonto nicht aus der ursprünglichen ActiveView entfernt.

HINWEIS: Das Kopieren eines Benutzerkontos in eine andere Aktivansicht ist nur über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole möglich.

Benutzerkonto umbenennen

Sie können Benutzerkonten in der verwalteten Domäne oder im verwalteten Teilbaum umbenennen. Wenn Sie den Anmeldenamen des Benutzers ändern, wird auch der Name des mit dem Benutzerkonto verknüpften Postfachs geändert.

Benutzerkontoaufgaben in der Webkonsole

Sie können die meisten der unten aufgeführten Aufgaben über die Registerkarte **Verwaltung** > **Suche** in der Webkonsole ausführen. Führen Sie eine Suchoperation aus, um das erforderliche Benutzerobjekt zu suchen und auszuwählen. Nachdem Sie ein oder mehrere Objekte in der Liste ausgewählt haben, wird die Symbolleiste mit Optionen wie „Erstellen“, „Konto“ und „Exchange“ aktiv. Klicken Sie auf die Optionen, um ihre Funktion anzuzeigen.

Benutzerkonto erstellen

Sie können Benutzerkonten in der verwalteten Domäne oder im verwalteten Teilbaum erstellen. Außerdem können Sie für das neue Konto die Eigenschaften bearbeiten, ein Postfach erstellen, die Email-Funktion aktivieren und Gruppenmitgliedschaften festlegen.

HINWEIS

- Möglicherweise wird in Ihrem Unternehmen eine Namenskonvention durch eine Richtlinie erzwungen, die festlegt, welchen Namen Sie dem neuen Benutzerkonto zuweisen dürfen.
- Standardmäßig platziert DRA das neue Benutzerkonto in die Organisationseinheit „Benutzer“ der verwalteten Domäne.
- InetOrgPerson-Objekte können in DRA nicht erstellt werden.

Benutzerkonto klonen

Beim Klonen eines Benutzerkontos werden die Gruppen, deren Mitglied der ursprüngliche Benutzer ist, automatisch zum neuen Benutzerkonto hinzugefügt, sodass Sie beim Konfigurieren des neuen Kontos Zeit sparen können. Wie mit jedem anderen neuen Konto können Sie auch hier Gruppen zum neuen Konto hinzufügen oder davon entfernen, die Email-Funktion aktivieren und andere Eigenschaftenkonfigurationen vornehmen.

HINWEIS: Durch Klonen eines InetOrgPerson-Objekts erstellen Sie ein neues Benutzerkonto.

Benutzerkontoeigenschaften ändern

Sie können die Eigenschaften der Benutzerkonten in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. Ihre Befugnisse legen fest, welche Eigenschaften eines Benutzerkontos Sie ändern dürfen. Wenn Sie Exchange installiert und die Microsoft Exchange-Unterstützung aktiviert haben, können Sie die Eigenschaften des verknüpften Postfachs bei der Verwaltung der Benutzerkonten ändern.

HINWEIS: Wenn Richtlinien für das Basisverzeichnis aktiviert sind, ändert DRA automatisch das Basisverzeichnis eines Benutzerkontos, wenn Sie das betreffende Konto verwalten. Wenn Sie beispielsweise den Speicherort des Basisverzeichnisses ändern, versucht DRA, das festgelegte Basisverzeichnis zu erstellen und Inhalte vom vorigen Basisverzeichnis zum neuen Speicherort zu verschieben. DRA wendet außerdem die zugewiesenen Zugriffssteuerungslisten vom vorigen Verzeichnis auf das neue Verzeichnis an.

Benutzerkonto aktivieren

Sie können Benutzerkonten in der verwalteten Domäne oder im verwalteten Teilbaum aktivieren. Wenn Sie ein Microsoft Windows-Konto verwalten, können Sie den Domänencontroller festlegen, auf dem DRA die Änderung anwendet.

Wenn Sie diese Änderung auf einen bestimmten Domänencontroller anwenden, wendet DRA die Änderung außerdem auf den standardmäßigen Domänencontroller der verwalteten Domäne an. In den Domäneneigenschaften können Sie überprüfen, welchen standardmäßigen Domänencontroller DRA verwendet.

Benutzerkonto deaktivieren

Sie können Benutzerkonten in der verwalteten Domäne deaktivieren. Wenn Sie ein Microsoft Windows-Konto verwalten, können Sie den Domänencontroller festlegen, auf dem DRA die Änderung anwendet.

Wenn Sie diese Änderung auf einen bestimmten Domänencontroller anwenden, wendet DRA die Änderung außerdem auf den standardmäßigen Domänencontroller der verwalteten Domäne an. In den Domäneneigenschaften können Sie überprüfen, welchen standardmäßigen Domänencontroller DRA verwendet.

Benutzerkonto entsperren

Sie können Benutzerkonten in der verwalteten Domäne oder im verwalteten Teilbaum entsperren.

DRA ruft den Benutzerkontostatus aus dem Konto-Cache ab. Deshalb kann in der Benutzeroberfläche angezeigt werden, dass ein ausgewähltes Konto entsperrt ist, obwohl es eigentlich gesperrt ist. DRA lässt das Entsperren eines Benutzerkontos auch dann zu, wenn der Kontostatus anzeigt, dass das Konto derzeit entsperrt ist. Sie können auch einen Domänencontroller festlegen, wenn Sie ein Benutzerkonto mit der DRA-Konsole entsperren, ohne das Benutzerkontopasswort zurücksetzen zu müssen.

Benutzerkontopasswort zurücksetzen

Sie können das Passwort für ein Konto in der verwalteten Domäne oder im verwalteten Teilbaum zurücksetzen. Ihre Befugnisse legen fest, welche Felder des Benutzerkontos Sie ändern können.

Wenn Sie das Passwort eines Benutzerkontos zurücksetzen, entsperrt DRA automatisch das Konto. Sie können auswählen, ob DRA ein neues Passwort für das Benutzerkonto generieren soll. Außerdem können Sie bestimmte passwortbezogene Optionen für das Konto ändern. Wenn Sie ein Microsoft Windows-Konto verwalten, können Sie den Domänencontroller festlegen, auf dem DRA die Änderungen anwendet.

HINWEIS: Wenn Sie diese Änderung auf einen bestimmten Domänencontroller anwenden, wendet DRA die Änderung außerdem auf den standardmäßigen Domänencontroller der verwalteten Domäne an. In den Domäneneigenschaften können Sie überprüfen, welchen standardmäßigen Domänencontroller DRA verwendet.

Benutzerkonto in einen anderen Container verschieben

Sie können ein Benutzerkonto in einen anderen Container, beispielsweise in eine Organisationseinheit, der verwalteten Domäne oder des verwalteten Teilbaums verschieben.

Benutzerkonto löschen

Sie können Benutzerkonten in der verwalteten Domäne oder im verwalteten Teilbaum löschen. Wenn der Papierkorb für die betreffende Domäne deaktiviert ist, wird das Benutzerkonto beim Löschen dauerhaft aus Active Directory gelöscht. Wenn der Papierkorb für die betreffende Domäne aktiviert ist, wird das Benutzerkonto beim Löschen in den Papierkorb verschoben.

WARNUNG: Wenn Sie ein neues Benutzerkonto erstellen, weist Microsoft Windows dem Konto eine Sicherheits-ID (SID) zu. Die SID wird nicht aus dem Kontonamen erstellt. Microsoft Windows verwendet SIDs, um die Berechtigungen in Zugriffssteuerungslisten für jede Ressource aufzuzeichnen. Wenn Sie ein Benutzerkonto löschen, können Sie dessen Zugriffsrechte nicht durch Erstellen eines Benutzerkontos mit dem gleichen Namen wiederherstellen.

Gruppenmitgliedschaft für Benutzerkonten festlegen

Sie können Benutzerkonten zu einer bestimmten Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum hinzufügen oder aus einer solchen Gruppe entfernen. Sie können außerdem die Eigenschaften vorhandener Gruppen, in denen das betreffende Konto Mitglied ist, anzeigen oder bearbeiten.

4.1.3 Umwandeln von Benutzerkonten

DRA bietet Ihnen die Möglichkeit, Benutzerkonten schnell und effizient umzuwandeln. Wenn die mit einem Benutzerkonto verbundene Person neue Verantwortungsbereiche übernimmt, können Sie die Umwandlungsfunktionen in DRA nutzen. Die Auftragsrollenschablonen ermöglichen ein einfaches Hinzufügen, Entfernen und Aktualisieren der Gruppenmitgliedschaften eines Kontos. Die Möglichkeit, ein Benutzerkonto umwandeln zu können, spart Zeit und Geld und erleichtert Ihnen die Arbeit, wenn ein Mitarbeiter befördert wird, die Abteilung wechselt oder das Unternehmen verlässt.

Grundlegendes zum Umwandlungsvorgang

Die Funktionen zum Umwandeln eines Benutzerkontos unterstützen Sie beim Ausführen der folgenden Aufgaben:

- Entfernen der Gruppenmitgliedschaften eines Benutzerkontos
- Hinzufügen von Gruppenmitgliedschaften zu einem Benutzerkonto
- Ändern der Benutzereigenschaften
- Entfernen bestimmter Gruppenmitgliedschaften und Hinzufügen anderer Gruppenmitgliedschaften zu einem Benutzerkonto

Gehen Sie zum Umwandeln eines Benutzerkontos folgendermaßen vor:

1. Überlegen Sie, ob Gruppenmitgliedschaften hinzugefügt, entfernt oder sowohl hinzugefügt als auch entfernt werden müssen.
2. Überprüfen Sie die vorhandenen Schablonen zum Entfernen bzw. Hinzufügen von Gruppenmitgliedschaften, um sicherzustellen, dass Sie über die erforderlichen Benutzerkontenschablonen verfügen.
3. Erstellen Sie je nach Bedarf erforderliche Kontoschablonen.
4. Schließen Sie den Assistenten zum Umwandeln von Benutzern ab.

Beim Umwandeln des Benutzers durch DRA werden die von der Entfernungsschablone bezeichneten Gruppenmitgliedschaften vom Benutzerkonto entfernt, während die von der Hinzufügungsschablone bezeichneten Gruppenmitgliedschaften zum Benutzerkonto hinzugefügt werden. Alle Mitgliedschaften, die in keiner der Schablonen enthalten sind, werden von DRA unverändert beibehalten. Beispiel: Ein Mitarbeiter der Vertriebsabteilung wird vom Vertriebsteam für die USA zum Vertriebsteam für Europa versetzt. Innerhalb der Organisation gibt es Verteiler- und Sicherheitsgruppen, die jeweils für ein bestimmtes Vertriebsteam gelten, aber auch bestimmte Gruppen, die von allen Vertriebsteams geteilt werden. Das US-Vertriebsteam nutzt die Verteilergruppen „US Hotspots“ und „US Vertriebsmanagement“, während das Vertriebsteam für Europa die Verteilergruppen „Euro Hotspots“ und „Euro Vertriebsmanagement“ nutzt. Beide Teams sind Mitglied der Sicherheitsgruppe „Sicherheit globaler Vertrieb“, haben aber auch standortspezifische Sicherheitsgruppen.

Ihrer Entfernungsschablone „Schablone Vertrieb US“ würden Sie folgende Gruppenmitgliedschaften zuweisen:

- US Hotspots
- US Vertriebsmanagement
- Sicherheit globaler Vertrieb
- Sicherheit US

Ihrer Hinzufügungsschablone „Schablone Vertrieb Euro“ würden Sie folgende Gruppenmitgliedschaften zuweisen:

- Euro Hotspots
- Euro Vertriebsmanagement
- Sicherheit globaler Vertrieb
- Sicherheit Euro

Während des Umwandlungsprozesses wird das Benutzerkonto des versetzten Mitarbeiters zuerst von allen Gruppenmitgliedschaften entfernt, die in der Schablone „Vertrieb US“ enthalten sind, und dann zu allen Gruppenmitgliedschaften hinzugefügt, die in der Schablone „Vertrieb Euro“ bezeichnet sind. Wenn der Benutzer außerdem Mitglied der Verteilergruppe „Pokerspieler“ ist, bleibt diese Gruppenmitgliedschaft unverändert beibehalten.

Die folgenden Befugnisse geben einem Hilfsadministrator die Möglichkeit, ein Benutzerkonto während der Umwandlung umfassender zu ändern:

- Adresseigenschaften während der Umwandlung eines Benutzerkontos ändern
- Beschreibung während der Umwandlung eines Benutzerkontos ändern
- Büro während der Umwandlung eines Benutzerkontos ändern
- Telefoneigenschaften während der Umwandlung eines Benutzerkontos ändern

Sie können die Fähigkeit zum Hinzufügen oder Entfernen von Gruppenmitgliedschaften auch einschränken, indem Sie einem Hilfsadministrator nur eines der folgenden Befugnisse gewähren:

- Benutzer zu Gruppen einer Schablone hinzufügen
- Benutzer aus Gruppen einer Schablone hinzufügen

Mit diesen Optionen zum Einschränken der Befugnisse können Sie eine zusätzliche Sicherheitsebene in Ihrem Unternehmen erstellen. Wenn Sie einzelnen Benutzern die Befugnis geben, die Gruppen einer Schablone nur zu entfernen, können Sie vorläufige Benutzerkonten erstellen. Diese vorläufigen Konten können dann überprüft werden, bevor ein anderer Hilfsadministrator mithilfe einer Hinzufügungsschablone neue Gruppenmitgliedschaften erteilt.

Erstellen von Benutzerumwandlungsschablonen

Die Umwandlung von Benutzerkonten ist direkt mit den Rollen und Aufgabenhierarchien in Ihrer Organisation verbunden. Erwägen Sie das Erstellen einer Schablone für jede Rolle bzw. jede Funktion im Unternehmen. DRA unterscheidet nicht zwischen Benutzerkontoschablonen zum Entfernen und Benutzerkontoschablonen zum Hinzufügen. Erstellen Sie eine einzelne Benutzerkontoschablone für jede Rolle in der Organisation. Während der Umwandlung wählen Sie die Schablone wahlweise als Entfernungsschablone oder als Hinzufügungsschablone aus. Wenn Sie eine Schablone als Entfernungsschablone verwenden, hindert Sie dies nicht daran, dieselbe Schablone in einer späteren Umwandlung als Hinzufügungsschablone zu verwenden.

Um eine Benutzerumwandlungsschablone zu erstellen, benötigen Sie die Befugnisse zum Erstellen eines Benutzerkontos und Zuweisen des Benutzerkontos zu den entsprechenden Gruppen. Diese Befugnisse können Sie erhalten, indem Ihr Konto den Rollen „Benutzerkonten erstellen und löschen“ und „Gruppenverwaltung“ in den entsprechenden ActiveViews zugewiesen wird oder indem Ihnen einzelne Befugnisse zugewiesen werden.

Umwandeln von Benutzerkonten

Beim Umwandeln eines Benutzerkontos können Sie Gruppenmitgliedschaften für ein Benutzerkonto hinzufügen, entfernen oder hinzufügen und entfernen. Verwenden Sie diesen Workflow, wenn Personen in Ihrer Organisation von einem Aufgabenbereich zu einem neuen Aufgabenbereich versetzt werden. Sie benötigen die Rolle „Benutzer umwandeln“ oder eine Rolle mit entsprechenden Befugnissen zum Umwandeln von Benutzerkonten. Diese Funktion kann nur über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole ausgeführt werden.

So wandeln Sie ein Benutzerkonto um:

1. Erweitern Sie im linken Bereich **All My Managed Objects** (Alle meine verwalteten Objekte).
2. Zum Festlegen des Benutzerkontos, das Sie verwalten möchten, führen Sie den Vorgang **Jetzt suchen** aus, um das gewünschte Benutzerobjekt zu suchen und auszuwählen.
3. Klicken Sie auf **Aufgaben** > **Umwandeln**.
4. Überprüfen Sie das Begrüßungsfenster und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster zum Auswählen der Benutzerschablone die Aktion **Durchsuchen** aus, um die gewünschte Entfernungsschablone auszuwählen.
6. Wenn Sie die Eigenschaften der Benutzerkontoschablone zum Entfernen überprüfen möchten, klicken Sie auf **Anzeigen**.
7. Wählen Sie mit der Aktion **Durchsuchen** die entsprechende Hinzufügungsschablone aus.
8. Wenn Sie die Eigenschaften der Benutzerkontoschablone zum Hinzufügen überprüfen möchten, klicken Sie auf **Anzeigen**.

9 Sofern Sie über die entsprechenden Befugnisse verfügen, können Sie die Option **Andere Eigenschaften des Benutzers ändern** aktivieren und die zu ändernden Eigenschaften auswählen. Klicken Sie auf **Weiter**, um durch die verfügbaren Eigenschaften zu navigieren.

10 Klicken Sie auf **Weiter**.

11 Überprüfen Sie das Zusammenfassungsfenster und klicken Sie auf **Fertig stellen**.

4.2 Verwalten von Gruppen

Als Hilfsadministrator können Sie mit DRA Gruppen verwalten und Gruppeneigenschaften ändern. Mithilfe von Gruppen können Sie einem definierten Satz Benutzerkonten spezifische Berechtigungen gewähren. Mit Gruppen können Sie steuern, auf welche Daten und Ressourcen ein Benutzerkonto in einer beliebigen Domäne zugreifen kann.

Sie können Gruppen beliebiger Art und beliebigen Umfangs verwalten. Beispielsweise ist es möglich, die Gruppen zu schachteln, sodass eine Gruppe Berechtigungen von einer anderen Gruppe erbt. Sie können die Gruppenmitgliedschaften auch effizient steuern, indem Sie Gruppen von verbürgten Domänen zu anderen Gruppen einer verwalteten Domäne hinzufügen und temporäre Gruppenzuweisungen verwalten.

Weitere Informationen zum Verwalten von Gruppen finden Sie in den folgenden Themen:

- Abschnitt 4.2.1, „Verwaltungsaufgaben für Gruppen“, auf Seite 58
- Abschnitt 4.2.2, „Verwalten temporärer Gruppenzuweisungen in der Delegierungs- und Konfigurationskonsole“, auf Seite 61
- Abschnitt 4.2.3, „Temporäre Gruppenzuweisungen in der Webkonsole verwalten“, auf Seite 62

4.2.1 Verwaltungsaufgaben für Gruppen

Dieser Abschnitt beschreibt das Verwalten von Gruppen über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole. Mit den entsprechenden Befugnissen können Sie verschiedene Gruppenverwaltungsaufgaben ausführen, zum Beispiel die Gruppenmitgliedschaften ändern. Wenn Sie mehrere Gruppen gleichzeitig auswählen, können Sie ausgewählte Aufgaben in einem Vorgang für mehrere Gruppen ausführen, beispielsweise Mitglieder löschen, verschieben oder zu einer Gruppe hinzufügen. Das Aufgabenmenü zeigt, welche Aufgaben verfügbar sind, wenn Sie eine oder mehrere Gruppen auswählen.

Konten zu Gruppen hinzufügen

Sie können Benutzerkonten, Kontakte und Computer zu einer verwalteten Domäne hinzufügen.

HINWEIS: Diese Aufgabe fügt mehrere Konten zu einer ausgewählten Gruppe hinzu. Sie können ein einzelnes Konto zu einer Gruppe hinzufügen, indem Sie das entsprechende Konto auswählen und dann im Aufgabenmenü auf „Zu Gruppen hinzufügen“ klicken.

Wenn durch das Hinzufügen eines Kontos zu einer anderen Gruppe Ihre Befugnisse auf das Konto erweitert werden, lässt DRA das Hinzufügen des Kontos nicht zu.

Gruppen zu anderen Gruppen hinzufügen

Sie können Gruppen schachteln, indem Sie eine Gruppe zu einer anderen verwalteten Gruppe hinzufügen. Wenn eine Gruppe in einer anderen Gruppe geschachtelt ist, kann die untergeordnete Gruppe Berechtigungen von der übergeordneten Gruppe erben.

HINWEIS: Wenn durch das Hinzufügen einer Gruppe zu einer anderen Gruppe Ihre Befugnisse auf die ursprüngliche Gruppe erweitert werden, lässt DRA das Hinzufügen der Gruppe nicht zu.

Gruppeneigenschaften ändern

Sie können die Eigenschaften lokaler und globaler Gruppen ändern. Ihre Befugnisse legen fest, welche Eigenschaften Sie für eine Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum bearbeiten können. Wenn Sie Exchange installiert und die Microsoft Exchange-Unterstützung aktiviert haben, können Sie die Eigenschaften der Verteilerliste bei der Verwaltung der Gruppen ändern.

Gruppe erstellen

Sie können eine Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum erstellen. Sie können auch die Eigenschaften einer neuen Gruppe bearbeiten, zum Beispiel die Mitglieder.

HINWEIS

- Möglicherweise wird in Ihrem Unternehmen eine Namenskonvention durch eine Richtlinie erzwungen, die festlegt, welchen Namen Sie der neuen Gruppe zuweisen dürfen.
- Standardmäßig platziert DRA die neue Gruppe in die Organisationseinheit „Benutzer“ der verwalteten Domäne.

Gruppenmitglieder festlegen

Sie können Benutzerkonten, Kontakte, Computer und andere Gruppen zur verwalteten Gruppe hinzufügen oder aus ihr entfernen. Fremdsicherheitsprinzipale können Sie in DRA nur entfernen. Sie können auch die Eigenschaften vorhandener Gruppenmitglieder (außer Fremdsicherheitsprinzipalen) anzeigen oder bearbeiten.

Wenn Sie Mitglieder aus einer Gruppe entfernen, löscht DRA die Objekte nicht. Wenn Sie Mitglieder zu einer Gruppe hinzufügen, benötigen Sie die Befugnis zum Ändern der Objekte, die Sie hinzufügen möchten.

HINWEIS: Sie können keine Benutzerkonten oder Gruppen zu einer der speziellen Windows-Gruppen hinzufügen (Administratoren, Kontenoperatoren, Sicherungsoperatoren, Serveroperatoren), es sei denn, Sie sind Windows-Administrator oder Mitglied der betreffenden spezifischen Gruppe.

Gruppenmitgliedschaft für Gruppen festlegen

Sie können Gruppen zu anderen Gruppen in der verwalteten Domäne oder im verwalteten Teilbaum hinzufügen oder aus ihnen entfernen. Sie können außerdem die Eigenschaften vorhandener Gruppen, zu denen die betreffende Gruppe gehört, anzeigen oder bearbeiten.

Sicherheitsberechtigungen für die Gruppenmitgliedschaft konfigurieren

Sie können Active Directory-Sicherheitsberechtigungen für Gruppenmitgliedschaften festlegen. Diese Berechtigungen legen fest, wer die Gruppenmitgliedschaften mit Microsoft Outlook anzeigen (lesen) und wer sie bearbeiten (schreiben) kann. Mit diesen Einstellungen können Sie Verteilerlisten und Sicherheitsgruppen in Ihrer Umgebung effizienter absichern. Geerbte Sicherheitsberechtigungen können nicht geändert werden.

HINWEIS: Beim Verwalten der Gruppenmitgliedschaftssicherheit können deaktivierte Berechtigungen auf geerbte Berechtigungen hinweisen.

Gruppeneigentümerschaft konfigurieren

Sie können die Eigentümerschaft beliebiger Microsoft Windows-Verteilergruppen oder -Sicherheitsgruppen festlegen. Die Berechtigung der Gruppeneigentümerschaft kann einem Benutzerkonto, einer Gruppe oder einem Kontakt gewährt werden. Durch das Gewähren der Gruppeneigentümerschaft wird das festgelegte Benutzerkonto, die festgelegte Gruppe bzw. der festgelegte Kontakt berechtigt, die Mitgliedschaft der Gruppe zu ändern.

HINWEIS: DRA deaktiviert das Kontrollkästchen **Manager kann die Mitgliedschaftsliste bearbeiten**, wenn die Gruppenmitgliedschaft vom Microsoft Exchange-Server ausgeblendet ist. Um das Kontrollkästchen zu aktivieren, klicken Sie auf der Exchange-Registerkarte im Fenster der Gruppeneigenschaften auf **Gruppenmitgliedschaft anzeigen**.

Gruppe klonen

Sie können lokale Gruppen und globale Gruppen in verwalteten Domänen klonen. Beim Klonen wird eine neue Gruppe des gleichen Typs und mit den gleichen Attributen wie die ursprüngliche Gruppe erstellt. DRA versucht außerdem, alle Mitglieder der ursprünglichen Gruppe zur neuen Gruppe hinzuzufügen.

Das Klonen von Gruppen ermöglicht ein schnelles Erstellen von Gruppen auf Grundlage anderer Gruppen mit ähnlichen Eigenschaften. Wenn Sie eine Gruppe klonen, füllt DRA den Assistenten „Gruppe klonen“ mit Werten aus der ausgewählten Gruppe aus. Sie können auch die Eigenschaften der neuen Gruppe bearbeiten.

HINWEIS

- Möglicherweise wird in Ihrem Unternehmen eine Namenskonvention durch eine Richtlinie erzwungen, die festlegt, welchen Namen Sie der neuen Gruppe zuweisen dürfen.
- Standardmäßig platziert DRA die neue Gruppe in die Organisationseinheit „Benutzer“ der verwalteten Domäne.

Gruppe löschen

Sie können sowohl lokale als auch globale Gruppen in der verwalteten Domäne oder im verwalteten Teilbaum löschen. Wenn der Papierkorb für die betreffende Domäne deaktiviert ist, wird die Gruppe beim Löschen dauerhaft aus Active Directory gelöscht. Wenn der Papierkorb für die betreffende Domäne aktiviert ist, wird die Gruppe beim Löschen in den Papierkorb verschoben und die Gruppeneigenschaften werden deaktiviert.

Weitere Informationen zum Papierkorb erhalten Sie unter Verwalten des Papierkorbs.

WARNUNG: Wenn Sie eine neue Gruppe erstellen, weist Microsoft Windows der Gruppe eine Sicherheits-ID (SID) zu. Die SID wird nicht aus dem Gruppennamen erstellt. Microsoft Windows verwendet SIDs, um die Berechtigungen in Zugriffssteuerungslisten für jede Ressource aufzuzeichnen. Wenn Sie eine Gruppe löschen, können Sie ihre Zugriffsrechte nicht durch Erstellen einer Gruppe mit dem gleichen Namen wiederherstellen.

Gruppe in einen anderen Container verschieben

Sie können eine Gruppe in einen anderen Container, beispielsweise in eine Organisationseinheit, der verwalteten Domäne oder des verwalteten Teilbaums verschieben.

Gruppenmitgliedschaft in Verteilerlisten anzeigen

Sie können die Gruppenmitgliedschaft in Verteilerlisten für Gruppen der verwalteten Domäne oder des verwalteten Teilbaums anzeigen.

Gruppenmitgliedschaft in Verteilerlisten ausblenden

Sie können die Gruppenmitgliedschaft in Verteilerlisten für Gruppen der verwalteten Domäne oder des verwalteten Teilbaums ausblenden.

4.2.2 Verwalten temporärer Gruppenzuweisungen in der Delegierungs- und Konfigurationskonsole

Mit temporären Gruppenzuweisungen können Sie Gruppenmitgliedschaften für Benutzer verwalten, die nur für einen bestimmten Zeitraum eine Gruppenmitgliedschaft benötigen. Dieser Abschnitt beschreibt das Verwalten temporärer Gruppenzuweisungen über die **Konto- und Ressourcenverwaltung** in der Delegierungs- und Konfigurationskonsole. Mit den entsprechenden Befugnissen können Sie Aufgaben wie das Erstellen temporärer Gruppenzuweisungen oder das Entfernen abgelaufener temporärer Gruppenzuweisungen ausführen.

Hilfsadministratoren können temporäre Gruppenzuweisungen nur für Gruppen anzeigen, für die der Hilfsadministrator über Befugnisse zum Hinzufügen oder Entfernen von Mitgliedern hat.

Während die temporäre Gruppenzuweisung den Status „Aktiv“ hat, können Sie nicht die zugeordnete Gruppe oder die Liste der Benutzer ändern. Wenn Sie diese Elemente ändern möchten, müssen Sie zuerst die temporäre Gruppenzuweisung abbrechen.

Eigenschaften temporärer Gruppenzuweisungen verwalten

Sie können die Eigenschaften temporärer Gruppenzuweisungen oder gespeicherter, abgelaufener temporärer Gruppenzuweisungen verwalten.

Wenn Sie eine temporäre Gruppenzuweisung neu planen möchten, ändern Sie den Zeitplan in den Eigenschaften der Zuweisung (**Properties**) und speichern Sie Ihre Änderungen.

Temporäre Gruppenzuweisung erstellen

Sie können eine temporäre Gruppenzuweisung auf dem primären oder auf einem sekundären Verwaltungsserver erstellen.

Eine temporäre Gruppenzuweisung wird standardmäßig sieben Tage nach ihrem Ablauf gelöscht, es sei denn, Sie haben die Option **Diese temporäre Gruppenzuweisung für die spätere Verwendung beibehalten** aktiviert. Um diesen Beibehaltungszeitraum zu ändern, klicken Sie mit der rechten Maustaste auf den Knoten **Temporary Group Assignment** (Temporäre

Gruppenzuweisung) unter „All My Managed Objects“ (Alle meine verwalteten Objekte), wählen Sie **Properties** (Eigenschaften) aus und ändern Sie die Anzahl der Tage, für die temporäre Gruppenzuweisungen beibehalten werden sollen.

Benutzerkonten in einer temporären Gruppenzuweisung verwalten

Sie können Benutzerkonten auf dem primären oder auf einem sekundären Verwaltungsserver zu einer temporären Gruppenzuweisung hinzufügen oder aus ihr entfernen.

HINWEIS: Sie können Benutzerkonten nur für temporäre Gruppenzuweisungen verwalten, die noch nicht aktiv sind.

Temporäre Gruppenzuweisung löschen

Sie können eine temporäre Gruppenzuweisung auf dem primären oder auf einem sekundären Verwaltungsserver löschen.

4.2.3 Temporäre Gruppenzuweisungen in der Webkonsole verwalten

Mit temporären Gruppenzuweisungen können Sie Gruppenmitgliedschaften für Benutzer verwalten, die für einen bestimmten Zeitraum eine Gruppenmitgliedschaft benötigen. In der Webkonsole können Sie Zuweisungen vom primären oder von einem sekundären DRA-Verwaltungsserver erstellen und verwalten. Die Aktionen, die für eine vorhandene Zuweisung verfügbar sind, hängen jedoch vom Status der Zuweisung ab.

Hilfsadministratoren können temporäre Gruppenzuweisungen nur für Gruppen anzeigen, für die sie über Befugnisse zum Ändern der Aktivansichtzuweisungen verfügen, beispielsweise über Befugnisse zum Hinzufügen oder Entfernen von Gruppenmitgliedern.

Um temporäre Gruppenzuweisungen in der Webkonsole zu verwalten, wechseln Sie zu **Aufgaben** > **Temporäre Gruppenzuweisungen**.

Sie können die folgenden Aktionen ausführen:

Vorhandene Zuweisungen suchen

Wenn Sie nach vorhandenen temporären Gruppenzuweisungen suchen, werden diese nach ihrem Status in den Ergebnissen aufgelistet. Folgende Status sind möglich:

- **Ausstehend:** Die temporäre Gruppenzuweisung ist zur Ausführung zu einem späteren Zeitpunkt geplant. Sie können die Zuweisung abbrechen, löschen oder neu planen.
- **Aktiv:** Die temporäre Gruppenzuweisung wurde gestartet und die betreffenden Mitglieder wurden zur Gruppe hinzugefügt. Sie können die Zuweisung abbrechen oder löschen.
- **Aktiv mit Fehler:** Die temporäre Gruppenzuweisung wurde gestartet, es konnten aber nicht alle betreffenden Mitglieder zur Gruppe hinzugefügt werden. Sie können die Zuweisung abbrechen oder löschen.
- **Abgeschlossen:** Die temporäre Gruppenzuweisung ist abgelaufen und alle betreffenden Mitglieder wurden aus der Gruppe entfernt. Sie können die Zuweisung löschen oder neu planen.
- **Mit Fehler abgeschlossen:** Die temporäre Gruppenzuweisung ist abgelaufen, es konnten aber nicht alle betreffenden Mitglieder aus der Gruppe entfernt werden. Sie können die Zuweisung löschen oder neu planen.

- **Abgebrochen:** Die temporäre Gruppenzuweisung wurde von einem Benutzer abgebrochen und alle betreffenden Mitglieder wurden aus der Gruppe entfernt. Sie können die Zuweisung löschen oder neu planen.
- **Mit Fehler abgebrochen:** Die temporäre Gruppenzuweisung wurde von einem Benutzer abgebrochen, es konnten aber nicht alle betreffenden Mitglieder aus der Gruppe entfernt werden. Sie können die Zuweisung löschen oder neu planen.
- **Fehler:** Die temporäre Gruppenzuweisung konnte nicht alle betreffenden Mitglieder zur Gruppe hinzufügen oder aus der Gruppe entfernen. Sie können die Zuweisung löschen oder neu planen.

Sie können die Ergebnisse nach diesen Status und nach anderen Kriterien filtern, zum Beispiel nach dem Namen der Zuweisung, der Zielgruppe, der Dauer oder dem Administrator, der die Zuweisung erstellt hat.

Temporäre Gruppenzuweisung erstellen

Sie können temporäre Gruppenzuweisungen für Gruppen erstellen, für die Sie über Änderungsbefugnisse und Befugnisse zum Angeben des Domänencontrollers haben. Eine abgelaufene temporäre Gruppenzuweisung wird in DRA nach sieben Tagen automatisch gelöscht, sofern Sie nicht die Option zum Beibehalten der temporären Gruppenzuweisung für die spätere Verwendung aktivieren.

Eigenschaften der temporären Gruppenzuweisung anzeigen oder ändern

Sie können beliebige Eigenschaften einer temporären Gruppenzuweisung, die beim Erstellen der temporären Gruppenzuweisung definiert wurden, anzeigen oder ändern. Wählen Sie nach dem Ausführen einer Suche nach temporären Gruppenzuweisungen eine Zuweisung aus, um ihre Eigenschaften anzuzeigen oder zu ändern.

Wenn Sie eine temporäre Gruppenzuweisung neu planen möchten, ändern Sie den Zeitplan in den Eigenschaften der Zuweisung (**Properties**) und speichern Sie Ihre Änderungen. Wenn die Zuweisung den Status „Aktiv“ hat, können Sie nur das Enddatum ändern.

WICHTIG: Während die temporäre Gruppenzuweisung den Status „Aktiv“ hat, können Sie nicht die zugeordnete Gruppe oder die Liste der Benutzer ändern. Wenn Sie diese Elemente ändern möchten, müssen Sie zuerst die Zuweisung abbrechen.

Temporäre Gruppenzuweisung abbrechen

Sie können eine temporäre Gruppenzuweisung nur abbrechen, wenn sie sich in einem der folgenden Status befindet:

- Aktiv
- Aktiv mit Fehler
- Ausstehend

Temporäre Gruppenzuweisung löschen

Sie können mehrere temporäre Gruppenzuweisungen auswählen und dann löschen. Wenn die ausgewählten temporären Gruppenzuweisungen den Status „Aktiv“, „Aktiv mit Fehler“ oder „Ausstehend“ hat, ist die Option **Abbrechen** verfügbar.

4.3 Dynamische Verteilergruppen verwalten

Eine dynamische Verteilergruppe ist ein Email-fähiges Active Directory-Gruppenobjekt, das Sie zum gruppierten Senden von Email-Nachrichten und anderen Informationen erstellen können.

Die Mitgliedschaftsliste einer dynamischen Verteilergruppe wird bei jedem Versand einer Nachricht an die Gruppe basierend auf den definierten Filtern und Bedingungen ermittelt. Dies unterscheidet sie von einer herkömmlichen Verteilergruppe, die einen festen Satz Mitglieder enthält. Wenn eine Email-Nachricht an eine dynamische Verteilergruppe gesendet wird, wird sie an alle Empfänger in der Organisation verteilt, die die für diese Gruppe definierten Kriterien erfüllen.

DRA unterstützt die folgenden Funktionen:

- Revision und Benutzeroberflächen-Berichterstellung
- Auflistungsunterstützung für dynamische Verteilergruppen
- NetIQ Reporting Center(NRC)-Bericht für dynamische Verteilergruppen
- Unterstützung für Auslöseroperation für dynamische Verteilergruppen
- Unterstützung für Benutzeroberflächenerweiterung für dynamische Verteilergruppen aus Exchange

Aufgaben in Bezug auf dynamische Verteilergruppen:

Dynamische Verteilergruppe erstellen

Sie können eine dynamische Verteilergruppe in der verwalteten Domäne oder im verwalteten Teilbaum erstellen. Sie können auch die Eigenschaften einer neuen dynamischen Verteilergruppe bearbeiten, zum Beispiel die Mitglieder.

HINWEIS

- Möglicherweise wird in Ihrem Unternehmen eine Namenskonvention durch eine Richtlinie erzwungen, die festlegt, welchen Namen Sie der neuen dynamischen Verteilergruppe zuweisen dürfen.
- Standardmäßig platziert DRA die neue dynamische Verteilergruppe in die Organisationseinheit „Benutzer“ der verwalteten Domäne.

Dynamische Verteilergruppe klonen

Sie können sowohl lokale als auch globale dynamische Verteilergruppen in verwalteten Domänen klonen. Beim Klonen dynamischer Verteilergruppen werden neue dynamische Verteilergruppen vom gleichen Typ und mit den gleichen Attributen wie das zugrunde liegende Original erstellt.

Durch Klonen einer dynamischen Verteilergruppe können Sie schnell dynamische Verteilergruppen erstellen, indem Sie als Grundlage eine andere dynamische Verteilergruppe mit ähnlichen Eigenschaften verwenden. Wenn Sie eine dynamische Verteilergruppe klonen, füllt DRA den Assistenten zum Klonen dynamischer Verteilergruppen mit Werten aus der ausgewählten dynamischen Gruppe aus. Sie können auch die Eigenschaften der neuen dynamischen Verteilergruppe bearbeiten.

Dynamische Verteilergruppe in einen anderen Container verschieben

Sie können eine dynamische Verteilergruppe in einen anderen Container, beispielsweise in eine Organisationseinheit, der verwalteten Domäne oder des verwalteten Teilbaums verschieben.

Dynamische Verteilergruppe löschen

Sie können sowohl lokale als auch globale dynamische Verteilergruppen in der verwalteten Domäne oder im verwalteten Teilbaum löschen. Wenn der Papierkorb für die betreffende Domäne deaktiviert ist, wird die dynamische Verteilergruppe beim Löschen dauerhaft aus Active Directory gelöscht. Wenn der Papierkorb für die betreffende Domäne aktiviert ist, wird die dynamische Verteilergruppe beim Löschen in den Papierkorb verschoben und die Eigenschaften der dynamischen Verteilergruppe werden deaktiviert.

Weitere Informationen zum Papierkorb erhalten Sie unter Verwalten des Papierkorbs.

WARNUNG: Wenn Sie eine neue dynamische Verteilergruppe erstellen, weist Microsoft Windows der dynamischen Verteilergruppe eine Sicherheits-ID (SID) zu. Die SID wird nicht aus dem Namen der dynamische Verteilergruppe erstellt. Microsoft Windows verwendet SIDs, um die Berechtigungen in Zugriffssteuerungslisten für jede Ressource aufzuzeichnen. Wenn Sie eine dynamische Verteilergruppe löschen, können Sie ihre Zugriffsrechte nicht durch Erstellen einer dynamischen Verteilergruppe mit dem gleichen Namen wiederherstellen.

Eigenschaften dynamischer Verteilergruppen ändern

Sie können die Eigenschaften lokaler und globaler dynamischer Verteilergruppen ändern. Ihre Befugnisse legen fest, welche Eigenschaften Sie für eine Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum bearbeiten können.

Filter festlegen

Die Mitgliedschaft einer dynamischen Verteilergruppe wird durch einen Filter festgelegt, den Sie definieren können.

Bedingungen festlegen

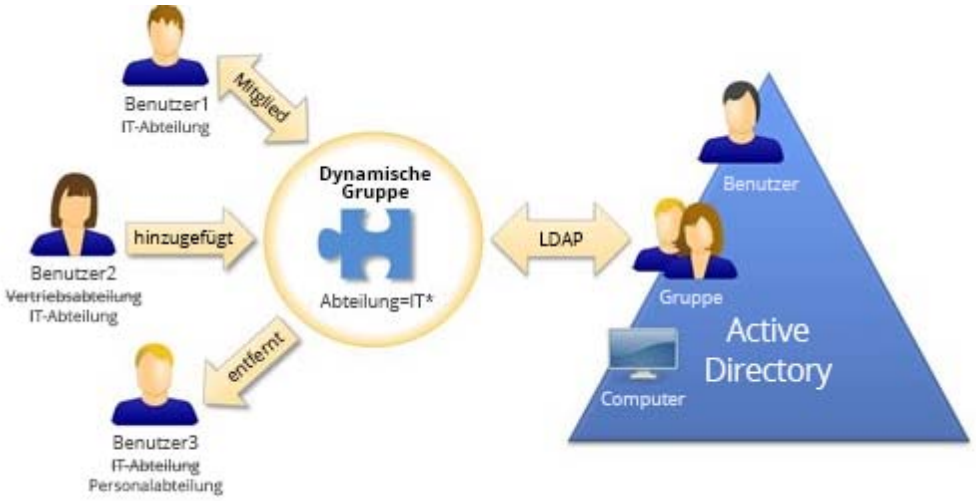
Bedingungen legen die Kriterien fest, die ein Objekt erfüllen muss, um Mitglied der dynamischen Verteilergruppe zu sein.

4.4 Dynamische Gruppen verwalten

Eine dynamische Gruppe ist eine Gruppe, deren Mitgliedschaft basierend auf einem Satz Kriterien variiert. In DRA können Sie dynamische Gruppen erstellen, ohne über eine Exchange-Umgebung zu verfügen. Die Mitgliedschaftsfilter zum Verwalten von dynamischen Gruppen in Active Directory sind eine Besonderheit von DRA.

Die Grafik unten beschreibt die typische Verwendung einer dynamischen Active Directory-Gruppe. Die Grafik zeigt drei dynamische Gruppen. Jede Gruppe verfügt über einen Satz an Kriterien, die festlegen, wer zur Gruppe hinzugefügt werden kann. Jede Gruppe steuert den Zugriff auf einen bestimmten Satz Dateien, Ordner und Anwendungen.

TIPP: Sie können eine *statische Mitgliederliste* erstellen, die dauerhafte Mitglieder einer dynamischen Gruppe enthält, oder eine *Liste ausgeschlossener Mitglieder*, deren Mitgliedschaft in der dynamischen Gruppe dann verweigert wird.



Benutzer2 arbeitet seit Kurzem in der IT-Abteilung. Wenn die dynamische Gruppe der IT-Abteilung aktualisiert wird, wird Benutzer2 zur Gruppe hinzugefügt. Wenn die dynamische Gruppe der Vertriebsabteilung aktualisiert wird, wird Benutzer2 aus der Mitgliederliste entfernt.

TIPP: Um die Mitgliederliste einer dynamischen Gruppe zu aktualisieren, klicken Sie mit der rechten Maustaste auf die Liste und wählen Sie **Mitglieder aktualisieren** aus.

Benutzer3 ist von der IT-Abteilung zur Personalabteilung gewechselt. Er wird aus der dynamischen Gruppe der IT-Abteilung entfernt und zur dynamischen Gruppe der Personalabteilung hinzugefügt.

Dynamische Gruppe erstellen

Sie können eine dynamische Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum erstellen. Sie können auch die Eigenschaften einer neuen dynamischen Gruppe bearbeiten, zum Beispiel die Mitglieder.

HINWEIS

- Möglicherweise wird in Ihrem Unternehmen eine Namenskonvention durch eine Richtlinie erzwungen, die festlegt, welchen Namen Sie der neuen dynamischen Gruppe zuweisen dürfen.
- Standardmäßig platziert DRA die neue dynamische Gruppe in die Organisationseinheit „Benutzer“ der verwalteten Domäne.

Filter erstellen

Die dynamische Gruppe verwendet Filter, um bei jedem Aktualisieren der Gruppe Benutzer zu ihrer Mitgliedschaftsliste hinzuzufügen bzw. aus der Liste zu entfernen.

Statische Mitgliederliste verwalten

Benutzer, die in der statischen Mitgliederliste einer dynamischen Gruppe enthalten sind, sind dauerhafte Mitglieder der Gruppen, bis sie manuell entfernt werden.

Wenn Sie Mitglieder aus einer dynamischen Gruppe entfernen, löscht DRA die Objekte nicht. Wenn Sie Mitglieder zu einer dynamischen Gruppe hinzufügen, benötigen Sie die Befugnis zum Ändern der Objekte, die Sie hinzufügen möchten.

Liste ausgeschlossener Mitglieder verwalten

Mitglieder, die in der Liste der ausgeschlossenen Mitglieder der dynamischen Gruppe enthalten sind, können der Gruppe erst beitreten, nachdem sie manuell aus der Liste entfernt wurden.

Mitgliederliste aktualisieren

Über die Aktion **Mitglieder aktualisieren** können Sie die Mitglieder einer dynamischen Gruppe aktualisieren.

Dynamische Gruppe klonen

Sie können sowohl lokale als auch globale dynamische Gruppen in verwalteten Domänen klonen. Beim Klonen dynamischer Gruppen werden neue dynamische Gruppen vom gleichen Typ und mit den gleichen Attributen wie das zugrunde liegende Original erstellt.

Durch Klonen einer dynamischen Gruppe können Sie schnell dynamische Gruppen erstellen, indem Sie als Grundlage eine andere dynamische Gruppe mit ähnlichen Eigenschaften verwenden. Wenn Sie eine dynamische Gruppe klonen, füllt DRA den Assistenten zum Klonen dynamischer Gruppen mit Werten aus der ausgewählten dynamischen Gruppe aus. Sie können auch die Eigenschaften der neuen dynamischen Gruppe bearbeiten.

Dynamische Gruppe in einen anderen Container verschieben

Sie können eine dynamische Gruppe in einen anderen Container, beispielsweise in eine Organisationseinheit, der verwalteten Domäne oder des verwalteten Teilbaums verschieben.

Dynamische Gruppe löschen

Sie können sowohl lokale als auch globale dynamische Gruppen in der verwalteten Domäne oder im verwalteten Teilbaum löschen. Wenn der Papierkorb für die betreffende Domäne deaktiviert ist, wird die dynamische Gruppe beim Löschen dauerhaft aus Active Directory gelöscht. Wenn der Papierkorb für die betreffende Domäne aktiviert ist, wird die dynamische Gruppe beim Löschen in den Papierkorb verschoben und die Eigenschaften der dynamischen Gruppe werden deaktiviert.

Weitere Informationen zum Papierkorb erhalten Sie unter Verwalten des Papierkorbs.

WARNUNG: Wenn Sie eine neue dynamische Gruppe erstellen, weist Microsoft Windows der dynamischen Gruppe eine Sicherheits-ID (SID) zu. Die SID wird nicht aus dem Namen der dynamischen Gruppe erstellt. Microsoft Windows verwendet SIDs, um die Berechtigungen in Zugriffssteuerungslisten für jede Ressource aufzuzeichnen. Wenn Sie eine dynamische Gruppe löschen, können Sie ihre Zugriffsrechte nicht durch Erstellen einer dynamischen Gruppe mit dem gleichen Namen wiederherstellen.

Eigenschaften dynamischer Gruppen ändern

Sie können die Eigenschaften lokaler und globaler dynamischer Gruppen ändern. Ihre Befugnisse legen fest, welche Eigenschaften Sie für eine Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum bearbeiten können.

Dynamische Gruppen zu anderen dynamischen Gruppen hinzufügen

Sie können dynamische Gruppen schachteln, indem Sie eine dynamische Gruppe zu einer anderen verwalteten dynamischen Gruppe hinzufügen. Wenn eine dynamische Gruppe in einer anderen dynamischen Gruppe geschachtelt ist, kann die untergeordnete dynamische Gruppe Berechtigungen von der übergeordneten dynamischen Gruppe erben.

HINWEIS: Wenn durch das Hinzufügen einer dynamischen Gruppe zu einer anderen dynamischen Gruppe Ihre Befugnisse auf die ursprüngliche dynamische Gruppe erweitert werden, lässt DRA das Hinzufügen der dynamischen Gruppe nicht zu.

Sicherheitsberechtigungen für die Gruppenmitgliedschaft konfigurieren

Sie können Active Directory-Sicherheitsberechtigungen für Mitgliedschaften in dynamischen Gruppen festlegen. Diese Berechtigungen legen fest, wer die Mitgliedschaften in der dynamischen Gruppe mit Microsoft Outlook anzeigen (lesen) und wer sie bearbeiten (schreiben) kann. Mit diesen Einstellungen können Sie Verteilerlisten und dynamische Sicherheitsgruppen in Ihrer Umgebung effizienter absichern. Geerbte Sicherheitsberechtigungen können nicht geändert werden.

HINWEIS: Beim Verwalten der Sicherheit der Mitgliedschaft in dynamischen Gruppen können deaktivierte Berechtigungen auf geerbte Berechtigungen hinweisen.

Eigentümerschaft einer dynamischen Gruppe konfigurieren

Die Berechtigung der Eigentümerschaft einer dynamischen Gruppe kann einem Benutzerkonto, einer Gruppe oder einem Kontakt gewährt werden. Durch das Gewähren der Eigentümerschaft an einer dynamischen Gruppe wird das festgelegte Benutzerkonto, die festgelegte Gruppe bzw. der festgelegte Kontakt berechtigt, die Mitgliedschaft der dynamischen Gruppe zu ändern.

Mitgliedschaften in dynamischer Gruppe in Verteilerlisten anzeigen

Sie können die Mitgliedschaft in einer dynamischen Gruppe in Verteilerlisten für Gruppen der verwalteten Domäne oder des verwalteten Teilbaums anzeigen.

Mitgliedschaften der dynamischen Gruppe in Verteilerlisten ausblenden

Sie können die Mitgliedschaft in einer dynamischen Gruppe in Verteilerlisten für Gruppen der verwalteten Domäne oder des verwalteten Teilbaums ausblenden.

HINWEIS: Die Option **Gruppenmitgliedschaft ausblenden** ist für Microsoft Exchange 2007-Verteilerlisten deaktiviert.

4.5 Verwalten von Kontakten

Mit DRA können Sie zahlreiche Netzwerkobjekte verwalten, einschließlich Kontakte und die zugehörigen Email-Adressen. Kontakte sind nur in Domänen im gemischten Modus und in nativen Microsoft Windows-Domänen verfügbar. Kontakten wird keine Sicherheits-ID (SID) zugewiesen, wie dies für Benutzerkonten und Gruppen der Fall ist. Mithilfe von Kontakten können Sie Mitglieder zu Verteilerlisten oder zu Gruppen hinzufügen, ohne ihnen Zugriff auf die Netzwerkservices zu gewähren.

Sie können Kontakte in Domänen im gemischten oder im nativen Modus zu Sicherheits- und Verteilergruppen hinzufügen. Weil Sicherheitsgruppen in Microsoft Windows als Verteilerlisten verwendet werden können, ist es unter Umständen sinnvoll, Kontakte zu diesen Gruppen hinzuzufügen. Das Vorhandensein eines Kontakts in einer globalen Sicherheitsgruppe verhindert nicht, dass die Gruppe beim Migrieren in eine Microsoft Windows-Domäne im nativen Modus in eine universelle Sicherheitsgruppe konvertiert wird.

Kontakteigenschaften ändern

Sie können die Kontakteigenschaften bearbeiten. Ihre Befugnisse legen fest, welche Eigenschaften Sie für einen Kontakt in der verwalteten Domäne bearbeiten können. Wenn Sie Exchange installiert und die Unterstützung für Exchange aktiviert haben, können Sie beim Verwalten der Kontakte auch die Email-Adresseigenschaften bearbeiten.

Kontakt erstellen

Sie können Kontakte in der verwalteten Domäne oder im verwalteten Teilbaum erstellen. Für die neuen Kontakte können Sie auch die Eigenschaften bearbeiten, die Email-Funktion aktivieren und Email-Adressen festlegen und die Gruppenmitgliedschaften angeben.

Kontakt klonen

Das Klonen von Kontakten ermöglicht ein schnelles Erstellen von Kontakten auf Grundlage anderer Kontakte mit ähnlichen Eigenschaften. Wenn Sie einen Kontakt klonen, füllt DRA den Assistenten „Kontakt klonen“ mit Werten aus dem ausgewählten Kontakt aus. Für die neuen Kontakte können Sie auch die Eigenschaften bearbeiten, die Email-Funktion aktivieren und Email-Adressen festlegen und die Gruppenmitgliedschaften angeben.

Gruppenmitgliedschaften für Kontakte verwalten

Sie können Kontakte zu einer bestimmten Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum hinzufügen oder aus einer solchen Gruppe entfernen. Sie können außerdem die Eigenschaften vorhandener Gruppen, zu denen der betreffende Kontakt gehört, anzeigen oder bearbeiten.

Kontakt zu einer anderen Organisationseinheit verschieben

Sie können einen Kontakt in einen anderen Container, beispielsweise in eine Organisationseinheit, der verwalteten Domäne oder des verwalteten Teilbaums verschieben.

Kontakt löschen

Sie können Kontakte aus der verwalteten Domäne oder dem verwalteten Teilbaum löschen. Wenn der Papierkorb für die betreffende Domäne deaktiviert ist, wird der Kontakt beim Löschen dauerhaft aus Active Directory gelöscht. Wenn der Papierkorb für die betreffende Domäne aktiviert ist, wird der Kontakt beim Löschen in den Papierkorb verschoben.

Weitere Informationen zum Papierkorb erhalten Sie unter Verwalten des Papierkorbs.

5 Verwalten von Azure-Benutzern und -Gruppen

Dieses Kapitel enthält grundlegende Informationen und eine Beschreibung der Vorgehensweisen zum Verwalten von Azure-Benutzerkonten und Azure-Gruppen in der Webkonsole. Mit den entsprechenden Befugnissen können Sie verschiedene Verwaltungsaufgaben für Azure-Benutzer und -Gruppen ausführen, zum Beispiel Azure-Benutzerkontoobjekte erstellen oder löschen.

Die meisten der Aufgaben für Azure-Benutzerobjekte und -Gruppenobjekte können Sie über die Registerkarte **Verwaltung**> **Suche** in der Webkonsole ausführen, indem Sie in einem der folgenden Knoten nach den gewünschten Objekten suchen:

- Alle meine verwalteten Objekte
- Alle meine verwalteten Mandanten
- Unterknoten von „Alle meine verwalteten Mandanten“

5.1 Verwalten von Azure-Benutzerkonten

Als Hilfsadministrator können Sie DRA zum Verwalten von Azure-Benutzerkonten und Ändern der Eigenschaften von Azure-Benutzerkonten verwenden, wenn Azure Active Directory vom DRA-Administrator konfiguriert wurde.

Führen Sie eine Suchoperation aus, um das erforderliche Azure-Benutzerobjekt zu suchen und auszuwählen. Nachdem Sie ein oder mehrere Objekte in der Liste ausgewählt haben, wird die Symbolleiste mit Optionen wie „Löschen“, „Zulassen“, „Sperren“, „Passwort zurücksetzen“, „Office 365-Postfach-Eigenschaften“ und „Eigenschaften ändern“ aktiv. Klicken Sie auf die Optionen, um ihre Funktion anzuzeigen.

Azure-Benutzerkonto erstellen

Sie können Azure-Benutzerkonten in Azure Active Directory erstellen.

Azure-Benutzerkontoeigenschaften ändern

Sie können die Eigenschaften von Azure-Benutzerkonten in Azure Active Directory ändern. Ihre Befugnisse bestimmen, welche Eigenschaften eines Azure-Benutzerkontos Sie ändern können.

Anmeldung mit Azure-Benutzerkonto zulassen

Sie können die Anmeldung mit einem Azure-Benutzerkonto bei Azure Active Directory zulassen.

Anmeldung mit Azure-Benutzerkonto sperren

Sie können die Anmeldung mit einem Azure-Benutzerkonto bei Azure Active Directory sperren.

Passwort für Azure-Benutzerkonto zurücksetzen

Sie können das Passwort für ein Azure-Benutzerkonto in Azure Active Directory zurücksetzen und wählen, ob DRA ein neues Passwort für das Konto generieren soll.

Azure-Benutzerkonto löschen

Sie können ein Azure-Benutzerkonto aus Azure Active Directory löschen. Das Konto kann dann jedoch nicht über DRA wiederhergestellt werden.

Azure-Gruppenmitgliedschaft für Azure-Benutzerkonten festlegen

Sie können Azure-Benutzerkonten zu einer bestimmten Azure-Gruppe in Azure Active Directory hinzufügen oder daraus entfernen.

5.2 Verwalten von Azure-Gruppen

Als Hilfsadministrator können Sie mit DRA Azure-Gruppen verwalten, wenn Azure Active Directory vom DRA-Administrator konfiguriert wurde. Mithilfe von Azure-Gruppen können Sie einem definierten Satz Benutzerkonten spezifische Berechtigungen gewähren. Mit Azure-Gruppen können Sie steuern, auf welche Daten und Ressourcen ein Benutzerkonto in einem beliebigen Mandanten zugreifen kann.

Dieser Abschnitt beschreibt das Verwalten von Azure-Gruppen in der Webkonsole. Wenn Sie über die entsprechenden Befugnisse verfügen, können Sie verschiedene Aufgaben zur Verwaltung von Azure-Gruppen ausführen.

HINWEIS: Unterstützte Mitglieder: Azure-Gruppenmitglieder können Azure-Benutzer, Azure-Gruppen, synchronisierte Benutzer und synchronisierte Gruppen sein.

Benutzerkonten zu Azure-Gruppen hinzufügen

Sie können Benutzerkonten (vor Ort bereitgestellte Konten und Azure-Konten) zu einer verwalteten Azure-Gruppe hinzufügen.

Mit dieser Aufgabe können Sie mehrere Konten zu einer ausgewählten Gruppe hinzufügen. Um ein einzelnes Konto zu einer Gruppe hinzuzufügen, wählen Sie das gewünschte Konto aus. Wenn Sie durch das Hinzufügen eines Kontos zu einer anderen Gruppe umfangreichere Befugnisse für das Konto erhalten würden, lässt DRA das Hinzufügen des Kontos zur Gruppe nicht zu.

Gruppen in Azure schachteln

Sie können Gruppen schachteln, indem Sie andere Gruppen (vor Ort bereitgestellte Gruppen oder Azure-Gruppen) zu einer verwalteten Azure-Gruppe hinzufügen. Wenn eine Gruppe in einer Azure-Gruppe geschachtelt ist, kann die untergeordnete Gruppe Berechtigungen von der übergeordneten Gruppe erben.

Wenn durch das Hinzufügen einer Domäne oder einer Azure-Gruppe zu einer anderen Azure-Gruppe Ihre Befugnisse auf die ursprüngliche Gruppe erweitert werden, lässt DRA das Hinzufügen der Gruppe nicht zu.

Azure-Gruppe erstellen

Sie können eine Azure-Gruppe in Azure Active Directory erstellen. Sie können auch die Eigenschaften bearbeiten, zum Beispiel Azure-Gruppenmitglieder zur neuen Gruppe hinzufügen.

Wenn kein Eigentümer angegeben ist, legt DRA standardmäßig das Azure-Mandantenzugriffskonto als Eigentümer fest.

Eigenschaften einer Azure-Gruppe ändern

Ihre Befugnisse legen fest, welche Eigenschaften Sie für eine Gruppe in Azure Active Directory ändern können.

Eigentümerschaft einer Azure-Gruppe konfigurieren

Sie können die Eigentümerschaft beliebiger Gruppen festlegen. Die Berechtigung der Gruppeneigentümerschaft kann einem Benutzerkonto oder einer Gruppe gewährt werden. Durch Erteilen der Gruppeneigentümerschaft erhält das betreffende Benutzerkonto bzw. die Gruppe die Berechtigung, die Gruppe einschließlich der Gruppenmitgliedschaft zu verwalten.

Azure-Gruppe löschen

Sie können Azure-Gruppen aus Azure Active Directory löschen. Die Gruppen können dann jedoch nicht über DRA wiederhergestellt werden.

6 Verwalten von Exchange-Postfächern und öffentlichen Ordnern

In DRA können Sie Microsoft Exchange-Postfächer als Erweiterung der Benutzerkontoeigenschaften verwalten. Mit dieser Integration können Sie Ihre Verwaltungsabläufe vereinfachen und so Ihre Exchange-Eigenschaften effizient verwalten. Außerdem können Sie Postfächer aus Benutzerkonto- und Exchange-Konto-Gesamtstrukturen verknüpfen und Ressourcenpostfächer, freigegebene Postfächer und öffentliche Ordner verwalten.

Verwalten von Postfachaufgaben in der Delegierungs- und Konfigurationskonsole

Über den Konto- und Ressourcenverwaltungsknoten führen Sie die zutreffenden Postfachaufgaben über die Registerkarte **Exchange Tasks** (Exchange-Aufgaben) in den Objekteigenschaften aus. Die Registerkarte ist auch über das Menü **Tasks** (Aufgaben) und über das Kontextmenü eines ausgewählten Objekts verfügbar. Im Allgemeinen wählen Sie den Knoten **All My Managed Objects** (Alle meine verwalteten Objekte) aus und führen dann den Vorgang **Find Now** (Jetzt suchen) aus, um das gewünschte Objekt zu suchen und auszuwählen.

Postfachaufgaben in der Webkonsole verwalten

Wenn Sie die Webkonsole verwenden, führen Sie die unten abgebildeten, zutreffenden Postfachaufgaben über die Registerkarte **Verwaltung** > **Suche** aus. Üblicherweise führen Sie eine Suchoperation aus, um das gewünschte Postfachobjekt zu suchen und auszuwählen. Nachdem Sie ein oder mehrere Objekte in der Liste ausgewählt haben, wird die Symbolleiste aktiv. Klicken Sie auf die Optionen, um ihre Funktion anzuzeigen.

6.1 Verwaltungsaufgaben für Benutzerpostfächer

Sie können Microsoft Exchange-Postfächer für Benutzerkonten in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. Für die verschiedenen Aspekte der Verwaltung von Microsoft Exchange-Postfächern sind jeweils unterschiedliche Befugnisse erforderlich. Ihre Befugnisse legen fest, welche Postfacheigenschaften Sie bearbeiten können, und ob Sie Microsoft Exchange-Postfächer erstellen, klonen, anzeigen oder löschen können. Sie können außerdem die Postfachrechte und -berechtigungen verwalten, die mit einem Benutzerkonto verknüpft sind, und so die Sicherheit der Microsoft Exchange-Umgebungen steuern. Wenn Sie nicht über die erforderlichen Befugnisse zum Bearbeiten einer Registerkarte oder eines Felds für das ausgewählte Postfach verfügen, deaktiviert DRA die entsprechenden Registerkarten und Felder, die Sie nicht bearbeiten können.

Neben den unten beschriebenen Aufgaben kann der DRA-Administrator Optionen in den Objekteigenschaften der Benutzerkonten zum Konfigurieren von Skype- und Skype Online-Einstellungen aktivieren. Skype kann sowohl über die Delegierungs- und Konfigurationskonsole als auch über die Webkonsole in den Benutzerkonten konfiguriert werden. Skype Online lässt sich nur über die Webkonsole konfigurieren.

Postfach erstellen

Sie können ein Microsoft Exchange-Postfach für ein vorhandenes Benutzerkonto erstellen. Sie können auch die Eigenschaften des neuen Postfachs bearbeiten.

HINWEIS: Wenn Sie ein Postfach erstellen, generiert Exchange die erforderlichen Proxy-Zeichenfolgen basierend auf den Exchange-Richtlinieneinstellungen. Microsoft Exchange generiert außerdem die standardmäßigen Proxy-Zeichenfolgen. Wenn Sie die Eigenschaften des neu erstellten Postfachs anzeigen, sehen Sie daher beide Arten Proxy-Zeichenfolge.

Benutzerkonto klonen

Beim Klonen eines Benutzerkontos werden die Gruppen, deren Mitglied der ursprüngliche Benutzer ist, automatisch zum neuen Benutzerkonto hinzugefügt, sodass Sie beim Konfigurieren des neuen Kontos Zeit sparen können. Wie mit jedem anderen neuen Konto können Sie auch hier Gruppen zum neuen Konto hinzufügen oder davon entfernen, die Email-Funktion aktivieren und andere Eigenschaftenkonfigurationen vornehmen.

HINWEIS: Durch Klonen eines InetOrgPerson-Objekts erstellen Sie ein neues Benutzerkonto.

Postfach verschieben

Sie können ein Microsoft Exchange-Postfach für ein Benutzerkonto zu einem anderen Postfachspeicher oder Microsoft Exchange-Server verschieben.

Postfacheigenschaften ändern

Sie können die Eigenschaften für Microsoft Exchange-Postfächer bearbeiten, während Sie die verknüpften Benutzerkonten verwalten. Ihre Befugnisse legen fest, welche Postfacheigenschaften Sie ändern können.

HINWEIS: Die Postfacheigenschaften von Benutzerkonten, die auf Mitgliederservern verwaltet werden, können nicht geändert werden.

Postfach-Sicherheitsberechtigungen konfigurieren

Sie können festlegen, welchen Benutzerkonten, Gruppen oder Computern Sie das Recht zum Senden und Empfangen von Emails mit einem bestimmten Microsoft Exchange-Postfach gewähren oder verweigern möchten. Mit diesen Einstellungen können Sie effizienter die Sicherheit der Exchange-Umgebung steuern. Geerbte Sicherheitsberechtigungen können nicht geändert werden.

HINWEIS: Beim Verwalten der Postfachsicherheit können deaktivierte Berechtigungen auf geerbte Berechtigungen hinweisen.

Postfach-Sicherheitsberechtigungen entfernen

Sie können die Postfach-Sicherheitsberechtigungen von einem Benutzerkonto, einer Gruppe oder einem Computer entfernen, die mit einem Microsoft Exchange-Postfach verknüpft sind. Nach dem Entfernen der Postfach-Sicherheitsberechtigungen können die Benutzerkonten, Gruppen oder Computerkonten keine Emails über das festgelegte Postfach mehr senden oder empfangen. Geerbte Sicherheitsberechtigungen können nicht entfernt werden.

Postfachrechte konfigurieren

Sie können anderen Benutzerkonten, Gruppen oder Computern Rechte auf ein bestimmtes Microsoft Exchange-Postfach gewähren oder verweigern. Mit diesen Einstellungen können Sie effizienter die Sicherheit der Exchange-Umgebung steuern. Geerbte Postfachrechte können nicht geändert werden.

HINWEIS: Beim Verwalten der Postfachrechte können deaktivierte Berechtigungen auf geerbte Berechtigungen hinweisen.

Postfachrechte entfernen

Sie können Postfachrechte von Benutzerkonten, Gruppen oder Computern entfernen, die mit einem bestimmten Microsoft Exchange-Postfach verknüpft sind. Nach dem Entfernen der Postfachrechte kann das entsprechende Benutzerkonto, die Gruppe oder das Computerkonto das festgelegte Postfach nicht mehr verwenden. Geerbte Postfachrechte können nicht entfernt werden.

Postfach löschen

Sie können ein Postfach löschen, das mit einem Benutzerkonto in der verwalteten Domäne oder im verwalteten Teilbaum verknüpft ist. Beim Löschen des Postfachs werden auch alle Nachrichten im Postfach gelöscht.

Email-Adresse hinzufügen oder bearbeiten

Sie können Email-Adressen für Postfächer festlegen, die mit Benutzerkonten in der verwalteten Domäne oder im verwalteten Teilbaum verknüpft sind. Sie können auch Benutzerkonten, die noch keine Postfächer haben, Email-Adressen zuweisen. Beim Verwalten von Microsoft Exchange-Postfächern können Sie nur die Email-Adresstypen hinzufügen, die von den Proxy-Generierungsrichtlinien definiert sind.

Antwortadresse festlegen

Sie können Antwortadressen für ein Postfach festlegen, das mit einem Benutzerkonto in der verwalteten Domäne oder im verwalteten Teilbaum verknüpft ist. Für ein Postfach können mehrere Antwortadressen festgelegt werden. Sie können jedoch nicht mehr als einen Email-Adresstyp als Antwortadresse festlegen. Beispielsweise ist es nicht möglich, mehr als eine Internetadresse als Antwortadresse festzulegen.

Email-Adresse löschen

Sie können Email-Adressen löschen, indem Sie die Adresse vom Postfach entfernen.

Zustellungsoptionen festlegen

Sie können festlegen, welche Postfächer der Benutzer zum Senden von Nachrichten verwenden darf, Weiterleitungsoptionen festlegen und Empfängergrenzwerte angeben.

Zustellungseinschränkungen festlegen

Durch das Festlegen von Zustellungseinschränkungen können Sie die Größe eingehender und ausgehender Nachrichten und das Akzeptieren von eingehenden Nachrichten für ein bestimmtes Postfach einschränken.

Speicherlimits angeben

Sie können Speicherlimits festlegen, beispielsweise Warnmeldungen, die je nach Größe des Postfachs zurückgegeben werden. Zusätzlich können Sie eine Beibehaltungsdauer für die gelöschten Elemente definieren.

Postfachverschiebungsstatus überprüfen

Sie können den Status von Postfachverschiebungen überprüfen und entsprechende Aktionen ausführen, beispielsweise den Status zurücksetzen, ein Verschieben abbrechen oder ein unterbrochenes Verschieben wieder aufnehmen.

6.2 Verwaltungsaufgaben für Office 365-Postfächer

Dieser Abschnitt enthält Informationen zur Verwaltung von Microsoft Office 365-Postfächern über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole oder über die Webkonsole. Sofern Sie über die entsprechenden Befugnisse verfügen, können Sie verschiedene Verwaltungsaufgaben für Benutzerkonten ausführen, beispielsweise das Einrichten von Beweissicherungsverfahren und der Email-Weiterleitung.

WICHTIG: DRA ermöglicht die Verwaltung von Office 365-Benutzerpostfächern sowie von migrierten freigegebenen Postfächern, Raumpostfächern und Gerätepostfächern. Damit diese Postfächer mit DRA verwaltet werden können, müssen die Postfächer mit einem vor Ort bereitgestellten, von DRA verwalteten Benutzer verknüpft sein. Die Postfacheigenschaften sind über die Eigenschaftenseiten der verknüpften Benutzer verfügbar.

Beweissicherungsverfahren einrichten

Bei begründeter Erwartung von Rechtsstreitigkeiten kann ein Beweissicherungsverfahren erforderlich sein. Organisationen müssen elektronisch gespeicherte Informationen beibehalten. Dies umfasst auch Emails, die für den jeweiligen Fall relevant sind.

Nach Einrichten eines Beweissicherungsverfahrens für ein Postfach wird sämtlicher Postfachinhalt, einschließlich gelöschter Elemente und der Originalversionen geänderter Elemente, beibehalten. Wenn ein Beweissicherungsverfahren für ein Benutzerpostfach eingerichtet wird, werden auch die Inhalte im Archivpostfach des Benutzers, sofern vorhanden, beibehalten. Das Verfahren kann für einen festgelegten Zeitraum dauern oder bis Sie das Beweissicherungsverfahren vom Postfach entfernen.

Sie müssen über eine Exchange Online E3-Lizenz verfügen, um ein Beweissicherungsverfahren einzurichten. Die Funktion wird über die Registerkarte **Beweissicherungsverfahren** in den Eigenschaften des Benutzerobjekts konfiguriert.

Postfachberechtigungen delegieren

Sie können Office 365-Berechtigungen über die Registerkarte für die Postfachdelegierung in den Benutzerobjekteigenschaften delegieren. Es gibt drei Arten von Berechtigungen, die Sie delegieren können: „Senden als“, „Senden im Auftrag von“ und „Vollzugriff“.

Email-Weiterleitung einrichten

Über die Nachrichtenübermittlungsoption in den Eigenschaften des Benutzerobjekts können Sie die Email-Weiterleitung für Benutzerkonten aktivieren.

6.3 Verwaltungsaufgaben für Ressourcenpostfächer

Mit der Ressourcenpostfachfunktion von Microsoft Exchange können Sie Postfächer für Ressourcen erstellen, beispielsweise ein Postfach für einen Konferenzraum, das zum Reservieren des Raums per Email verwendet wird. DRA bietet verschiedene Rollen, Befugnisse und Richtlinien, mit denen Sie das Ressourcenpostfach effizient verwalten können.

DRA unterstützt Benutzeroberflächenerweiterungen für Ressourcenpostfächer und bietet Unterstützung für das Generieren von Revisions- oder Benutzeroberflächenberichten. Die Unterstützung für ADSCI-Skripte ist ebenfalls in DRA integriert.

Ressourcenpostfach erstellen

Sie können Ressourcenpostfächer in der verwalteten Domäne oder im verwalteten Teilbaum erstellen.

Ressourcenpostfach zu einem anderen Container verschieben

Sie können ein Ressourcenpostfach in einen anderen Container, beispielsweise in eine Organisationseinheit, der verwalteten Domäne oder des verwalteten Teilbaums verschieben.

Ressourcenpostfach zu einem anderen Postfachspeicher oder Exchange-Server verschieben

Sie können ein Ressourcenpostfach zu einem anderen Postfachspeicher oder Microsoft Exchange-Server verschieben.

Ressourcenpostfach klonen

Durch Klonen eines Ressourcenpostfachs können Sie schnell weitere Ressourcenpostfächer mit ähnlichen Eigenschaften erzeugen. Wenn Sie ein Ressourcenpostfach klonen, füllt DRA den Assistenten zum Klonen von Ressourcenpostfächern mit Werten der ausgewählten Ressource aus.

Ressourcenpostfach umbenennen

Sie können Ressourcenpostfächer in der verwalteten Domäne oder im verwalteten Teilbaum umbenennen. Wenn Sie den Anmeldenamen des Benutzers ändern, wird auch der Name des mit dem Benutzerkonto verknüpften Postfachs geändert.

Ressourcenpostfach zu einer Gruppe hinzufügen

Sie können Ressourcenpostfächer von einer bestimmten Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum hinzufügen oder aus einer solchen Gruppe entfernen.

Ressourcenpostfach löschen

Sie können ein Ressourcenpostfach in der verwalteten Domäne oder im verwalteten Teilbaum löschen. Beim Löschen eines Ressourcenpostfachs werden auch alle Nachrichten im Postfach und alle deaktivierten Benutzerobjekte, die mit dem Ressourcenpostfach verknüpft sind, gelöscht. Bei Bedarf können Sie das Löschen deaktivierter Benutzerobjekte beim Löschen des Postfachs außer Kraft setzen. Wenn Sie ein Benutzerobjekt löschen, das mit einem Ressourcenpostfach verknüpft ist, wird auch das Ressourcenpostfach gelöscht.

Gelöschtes Ressourcenpostfach wiederherstellen

Wenn der Papierkorb für die betreffende Domäne aktiviert ist, kann ein gelöschtes Ressourcenpostfach wiederhergestellt werden.

Ressourcenpostfacheigenschaften ändern

Sie können die Eigenschaften der Ressourcenpostfächer in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. Ihre Befugnisse legen fest, welche Eigenschaften Sie ändern können.

6.4 Verwaltungsaufgaben für freigegebene Postfächer

Freigegebene Postfächer sind hilfreich für Helpdesk-Administratoren und Mitarbeiter des technischen Supports, weil sie so konfiguriert werden können, dass alle Antworten in ein einzelnes Postfach geleitet werden, auf das mehrere Benutzer zugreifen können. Das Postfach muss sich in einer von DRA verwalteten Domäne mit aktivierter Exchange-Richtlinie befinden. Sie benötigen die erforderlichen Befugnisse zum Verwalten freigegebener Postfächer.

Wenn Sie ein freigegebenes Postfach erstellen, gibt es zwei Arten an Berechtigungen, die Sie an Benutzer delegieren können: „Senden als“ und „Vollzugriff“. Mit „Senden als“ wird die Berechtigung zum Lesen und Senden von Emails gewährt. Sie können Berechtigungen sowohl an Benutzer als auch an Gruppenobjekte delegieren. In den Objekteigenschaften können Sie außerdem Zustellungseinschränkungen, Zustellungsoptionen, Speicherlimits, Ordnerberechtigungen und verschiedene andere Optionen festlegen.

HINWEIS: Verwaltungsaufgaben für freigegebene Postfächer können nur über die Webkonsole ausgeführt werden.

Freigegebenes Postfach erstellen

Sie können freigegebene Postfächer in der verwalteten Domäne oder im verwalteten Teilbaum erstellen.

Freigegebenes Postfach zu einem anderen Container verschieben

Sie können freigegebene Postfächer in einen anderen Container, beispielsweise in eine Organisationseinheit, der verwalteten Domäne oder des verwalteten Teilbaums verschieben.

Freigegebenes Postfach zu einem anderen Postfachspeicher verschieben

Sie können ein freigegebenes Postfach zu einem anderen Postfachspeicher verschieben.

Freigegebenes Postfach klonen

Durch Klonen eines freigegebenen Postfachs können Sie schnell weitere freigegebene Postfächer mit ähnlichen Eigenschaften erzeugen.

Freigegebenes Postfach umbenennen

Sie können freigegebene Postfächer in der verwalteten Domäne oder im verwalteten Teilbaum umbenennen. Wenn Sie den Anmeldenamen des Benutzers ändern, wird auch der Name des mit dem Benutzerkonto verknüpften Postfachs geändert.

Freigegebenes Postfach löschen

Sie können ein freigegebenes Postfach in der verwalteten Domäne oder im verwalteten Teilbaum löschen. Wenn der Papierkorb für die betreffende Domäne deaktiviert ist, wird das freigegebene Postfach beim Löschen dauerhaft aus Active Directory gelöscht. Wenn der Papierkorb für die betreffende Domäne aktiviert ist, wird das freigegebene Postfach beim Löschen in den Papierkorb verschoben.

Beim Löschen eines freigegebenen Postfachs werden auch alle Nachrichten im Postfach und alle deaktivierten Benutzerobjekte, die mit dem freigegebenen Postfach verknüpft sind, gelöscht. Wenn Sie ein Benutzerobjekt löschen, das mit einem freigegebenen Postfach verknüpft ist, wird auch das freigegebene Postfach gelöscht.

Gelöschtes freigegebenes Postfach wiederherstellen

Wenn der Papierkorb für die betreffende Domäne aktiviert ist, kann ein gelöschtes freigegebenes Postfach wiederhergestellt werden.

Freigegebenes Archivpostfach erstellen

Sie können ein freigegebenes Archivpostfach in der verwalteten Domäne oder im verwalteten Teilbaum erstellen.

Freigegebenes Archivpostfach löschen

Sie können ein freigegebenes Archivpostfach in der verwalteten Domäne oder im verwalteten Teilbaum löschen.

Eigenschaften des freigegebenen Postfachs ändern

Sie können die Eigenschaften des freigegebenen Postfachs in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. Ihre Befugnisse legen fest, welche Eigenschaften Sie ändern können.

6.5 Verwaltungsaufgaben für verknüpfte Postfächer

Verknüpfte Postfächer sind hilfreich für große Umorganisierungen bei Zusammenschlüssen, Übernahmen oder Aufspaltungen eines Unternehmens, die häufig mit einer Postfachmigration verbunden sind. Diese Funktion ermöglicht das Verknüpfen von Postfächern aus verschiedenen Exchange-Gesamtstrukturen, um die Unterbrechung der Benutzer-Email-Funktion zu verhindern. Die Postfächer müssen sich in von DRA verwalteten Domänen mit aktivierter Exchange-Richtlinie befinden. Sie benötigen die erforderlichen Befugnisse zum Verwalten verknüpfter Postfächer. Wenn Sie ein verknüpftes Postfach erstellen, wird die Registerkarte **Verknüpftes Postfach** zu den Eigenschaften des Benutzerobjekts hinzugefügt.

Die Verwaltung verknüpfter Postfächer wird nur in der Webkonsole unterstützt. Die Erstellung eines verknüpften Postfachs erfolgt über die Symbolleiste eines ausgewählten Benutzerkontos. Diese Option ist nur aktiviert, wenn die Domäne des ausgewählten Benutzers eine Verbürgung für eine externe Gesamtstruktur mit anderen verwalteten Domänen in DRA hat. Beim Suchen nach einem zu verknüpfenden Konto in einer anderen von DRA verwalteten Domäne werden nur deaktivierte Benutzerkonten angezeigt.

Verknüpftes Postfach erstellen

Wählen Sie zwei Benutzerkonten in unterschiedlichen verwalteten Exchange-Gesamtstrukturen aus, um ein verknüpftes Postfach zu erstellen.

Verknüpftes Postfach löschen

Sie können ein verknüpftes Postfach über die Symbolleiste eines ausgewählten Benutzers löschen, der über ein solches verknüpftes Postfach verfügt.

Eigenschaften des verknüpften Postfachs ändern

Sie können die Eigenschaften eines verknüpften Postfachs über die Registerkarte **Verknüpftes Postfach** in den Eigenschaften des ausgewählten Benutzers bearbeiten.

Verknüpftes Archivpostfach erstellen

Wählen Sie einen Benutzer aus, der über ein verknüpftes Postfach verfügt, um ein verknüpftes Archivpostfach zu erstellen.

Verknüpftes Archivpostfach löschen

Sie können ein verknüpftes Archivpostfach über die Symbolleiste eines ausgewählten Benutzers löschen, der über ein solches verknüpftes Archivpostfach verfügt.

Gelöschtes verknüpftes Postfach wiederherstellen

Wenn der Papierkorb für die betreffende Domäne aktiviert ist, kann ein gelöschtes verknüpftes Postfach wiederhergestellt werden.

6.6 Verwaltungsaufgaben für öffentliche Ordner

Wenn der DRA-Administrator eine Gesamtstruktur für öffentliche Ordner im mit DRA verwalteten Unternehmen erstellt und Ihnen entsprechende Befugnisse zur Verwaltung öffentlicher Ordner in DRA erteilt hat, können Sie öffentliche Ordner erstellen, deren Eigenschaften bearbeiten und Änderungsverlaufsberichte generieren. Öffentliche Ordner können nur über die Webkonsole erstellt und bearbeitet werden. Mit der Suchoption können Sie öffentliche Ordner suchen. Informationen hierzu erhalten Sie unter *Abschnitt 3.1, „Suche“, auf Seite 45*.

Aufgaben für öffentliche Ordner führen Sie über die Registerkarte **Verwaltung** > **Öffentliche Ordner** aus.

Öffentlichen Ordner erstellen

Über die Webkonsole können Sie neue öffentliche Ordner in spezifizierten Domänen, Teilbäumen und Postfächern für öffentliche Ordner erstellen. Sie können das standardmäßige Postfach für die ausgewählte Domäne verwenden oder ein anderes Postfach wählen.

Email-Funktion für einen öffentlichen Ordner aktivieren

Über die Option **Email aktivieren** in der Listensymbolleiste können Sie die Email-Funktion für einen öffentlichen Ordner aktivieren. Anschließend können Sie dem öffentlichen Ordner Email-Adressen zuweisen und die Eigenschaften des öffentlichen Ordners bearbeiten.

Email-Funktion für einen öffentlichen Ordner deaktivieren

Über die Option **Email deaktivieren** in der Listensymbolleiste können Sie die Email-Funktion für einen öffentlichen Ordner deaktivieren.

Eigenschaften eines öffentlichen Ordners ändern

Nachdem Sie die Email-Funktion für einen öffentlichen Ordner aktiviert haben, können Sie die Ordnerstatistik anzeigen und die Eigenschaften des öffentlichen Ordners bearbeiten. In diesen Eigenschaften können Sie Optionen für die Benutzerzustellung und für Einschränkungen sowie Größenlimits und Kontingentwarnungen, Email-Eigenschaften, Speicheralterlimits, Email-Genehmigungen durch Moderatoren und benutzerdefinierte Attribute festlegen.

HINWEIS: Sie können auch bestimmte Eigenschaften, wie Speicherkontingente, für mehrere öffentliche Ordner aktualisieren, wenn mehrere Ordner ausgewählt sind.

Öffentlichen Ordner löschen

Sie können öffentliche Ordner löschen, wenn sie keine Unterordner enthalten und wenn die Email-Option deaktiviert ist.

7 Verwalten von Ressourcen

Mit DRA können Sie Ressourcen wie Computer, Drucker und andere Geräte sowie Prozesse verwalten, die mit diesen Ressourcen verknüpft sind. Wenn Sie beispielsweise einen bestimmten Service auf einem verwalteten Computer starten möchten, können Sie das entsprechende Computerobjekt in DRA suchen, über die Objekteigenschaften auf seine Services zugreifen und eine bestimmten Service auf dem Computer von DRA aus starten, ohne jemals eine Remoteverbindung zum Computer herstellen zu müssen.

7.1 Verwalten von organisatorischen Einheiten

Dieser Abschnitt beschreibt das Verwalten von organisatorischen Einheiten über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole. Mit den entsprechenden Befugnissen können Sie verschiedene Aufgaben zur Verwaltung organisatorischer Einheiten ausführen, beispielsweise das Verschieben einer organisatorischen Einheit in einen anderen Container.

HINWEIS: Organisatorische Einheiten können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.

Eigenschaften von organisatorischen Einheiten ändern

Sie können die Eigenschaften organisatorischer Einheiten bearbeiten. Ihre Befugnisse legen fest, welche Eigenschaften Sie für eine organisatorische Einheit in der verwalteten Domäne oder im verwalteten Teilbaum bearbeiten können.

Organisatorische Einheiten erstellen

Sie können eine organisatorische Einheit in der verwalteten Domäne oder im verwalteten Teilbaum erstellen. Sie können außerdem die allgemeinen Eigenschaften bearbeiten, beispielsweise die Beschreibung der organisatorischen Einheit.

Organisatorische Einheiten klonen

Sie können eine neue organisatorische Einheit erstellen, indem Sie eine vorhandene organisatorische Einheit in der verwalteten Domäne oder dem verwalteten Teilbaum klonen. Sie können die allgemeinen Eigenschaften der neuen organisatorischen Einheit bearbeiten, beispielsweise die Beschreibung der organisatorischen Einheit. Beim Klonen einer organisatorischen Einheit werden die in der organisatorischen Einheit enthaltenen Objekte nicht geklont.

Active Directory-Baum am Speicherort einer organisatorischen Einheit öffnen

Sie können den Active Directory-Baum schnell und einfach am Speicherort einer bestimmten organisatorischen Einheit in der verwalteten Domäne bzw. im verwalteten Teilbaum öffnen.

Organisatorische Einheiten in einen anderen Container verschieben

Sie können eine organisatorische Einheit in einen anderen Container in der verwalteten Domäne verschieben. Beim Verwalten von Teilbäumen einer Domäne können Sie organisatorische Einheiten innerhalb der Hierarchie des Teilbaums verschieben.

HINWEIS

- Wenn Sie durch das Verschieben einer organisatorischen Einheit in einen anderen Container höhere Befugnisse über die verschobene organisatorische Einheit erhalten würden, lässt DRA das Verschieben der organisatorischen Einheit nicht zu.
- Sie können eine organisatorische Einheit auch durch Ziehen an den neuen Speicherort verschieben.

Organisatorische Einheiten löschen

Sie können organisatorische Einheiten aus der verwalteten Domäne oder dem verwalteten Teilbaum löschen. Sie können nur leere organisatorische Einheiten löschen. Organisatorische Einheiten, die Objekte enthalten, können Sie nicht löschen. Wenn Sie eine organisatorische Einheit löschen möchten, die Objekte enthält, löschen Sie zuerst alle enthaltenen Objekte und dann die organisatorische Einheit.

7.2 Verwalten von Computern

Mit DRA können Sie Computer in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. Beispielsweise können Sie Computerkonten zur verwalteten Domäne hinzufügen oder aus ihr entfernen und Ressourcen auf jedem Computer verwalten. Wenn Sie einen Computer zur Domäne hinzufügen, erstellt DRA für den Computer ein Computerkonto in dieser Domäne. Sie können dann den Computer in dieser Domäne verbinden und den Computer zur Verwendung des Computerkontos konfigurieren. Sie können auch die Eigenschaften der Computerkonten anzeigen und bearbeiten. Mit DRA können Sie Computer herunterfahren und Domänencontroller in einer verwalteten Domäne synchronisieren.

HINWEIS

- Computer können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.
- Ausgeblendete Domänencontroller können nicht verwaltet werden. Der Domänen-Cache enthält keine ausgeblendeten Domänencontroller. Deshalb zeigt DRA ausgeblendete Domänencomputer nicht in Listen oder Eigenschaftenfenstern an.

Gruppenmitgliedschaft für Computer festlegen

Sie können Computer zu einer bestimmten Gruppe in der verwalteten Domäne oder im verwalteten Teilbaum hinzufügen oder aus einer solchen Gruppe entfernen. Sie können außerdem die Eigenschaften vorhandener Gruppen, zu denen der betreffende Computer gehört, anzeigen oder bearbeiten.

Eigenschaften von Computerkonten verwalten

Sie können die Eigenschaften von Computerkonten verwalten. Ihre Befugnisse legen fest, welche Eigenschaften Sie für einen Computer in der verwalteten Domäne oder im verwalteten Teilbaum bearbeiten können.

Computer zur Domäne hinzufügen

Sie können einen Computer zu einer verwalteten Domäne oder zu einem verwalteten Teilbaum hinzufügen, indem Sie ein neues Computerkonto erstellen.

Computer aus der Domäne entfernen

Durch Löschen des Computerkontos können Sie einen Computer aus der verwalteten Domäne oder dem verwalteten Teilbaum entfernen.

Computer verschieben

Sie können einen Computer in einen anderen Container, beispielsweise in eine Organisationseinheit, der verwalteten Domäne oder des verwalteten Teilbaums verschieben.

Computer herunterfahren oder neu starten

Sie können einen Computer sofort oder zu einem festgelegten Zeitpunkt herunterfahren oder neu starten.

Administratorpasswort zurücksetzen

Zum Zurücksetzen des Administratorpassworts benötigen Sie die Befugnis „Passwort für lokalen Administrator zurücksetzen“ oder müssen mit einer Rolle verknüpft sein, die diese Befugnis umfasst. Sie können das Administratorpasswort für Mitgliedserver in der verwalteten Domäne oder im verwalteten Teilbaum zurücksetzen. Das Administratorpasswort für einen Domänencontroller können Sie nicht zurücksetzen.

Computerkonto zurücksetzen

Sie können ein Computerkonto für Mitgliedserver in der verwalteten Domäne oder im verwalteten Teilbaum zurücksetzen. Das Computerkonto für einen Domänencontroller können Sie nicht zurücksetzen.

Computerkonto löschen

Sie können Computerkonten aus der verwalteten Domäne oder dem verwalteten Teilbaum löschen. Wenn Sie eine Microsoft Windows-Domäne verwalten, können Sie Computerkonten löschen, die andere Objekte enthalten, beispielsweise eine freigegebene Ressource. Aktivieren Sie die Option **Löschen erzwingen**, um Computerobjekte aus Active Directory zu löschen. Damit werden auch alle untergeordneten Objekte gelöscht, wie Drucker und freigegebene Ordner. Gelöschte Computer und ihre verknüpften Objekte werden in den DRA-Papierkorb verschoben. Wenn der Papierkorb nach dem Löschen deaktiviert wird, werden die Objekte dauerhaft gelöscht.

HINWEIS: Computerkonten für Mitgliedsserver in der verwalteten Domäne oder im verwalteten Teilbaum können Sie nicht löschen.

Computerkonto deaktivieren

Sie können Computerkonten in der verwalteten Domäne oder dem verwalteten Teilbaum deaktivieren. Wenn Sie ein Computerkonto deaktivieren, können sich die Benutzer mit diesem Computer in keiner Domäne mehr anmelden.

Computerkonto aktivieren

Sie können Computerkonten in der verwalteten Domäne oder dem verwalteten Teilbaum aktivieren. Wenn Sie ein Computerkonto aktivieren, können sich die Benutzer am betreffenden Computer in einer beliebigen Domäne anmelden.

Computerressourcen verwalten

Für jedes Computerkonto in der verwalteten Domäne oder im verwalteten Teilbaum können Sie die verknüpften Ressourcen verwalten, wie Services, Freigaben, Geräte, Drucker und Druckaufträge.

7.3 Verwalten von Services

Ein Service ist eine Art Anwendung, die vom Windows-Betriebssystem gesondert behandelt wird. Services können auch ausgeführt werden, wenn gerade kein Benutzer am Computer angemeldet ist. Mit DRA können Hilfsadministratoren, die über die entsprechenden Befugnisse verfügen, Services über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole verwalten.

HINWEIS: Services können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.

Serviceeigenschaften verwalten

Sie können die Eigenschaften von Services verwalten, die auf Computern in der verwalteten Domäne oder im verwalteten Teilbaum ausgeführt werden. Sie können Services während der Verwaltung anderer Ressourcen für den Computer verwalten.

Service starten

Sie können Services auf einem beliebigen Computer in der verwalteten Domäne oder im verwalteten Teilbaum starten.

Service mit Parametern starten

Wenn Sie Services starten, die Parameter akzeptieren, geben Sie diese Parameter beim Starten an. Sie können Services auf Computern in der verwalteten Domäne oder im verwalteten Teilbaum starten.

Servicestarttyp festlegen

Sie können den Starttyp eines Services ändern, beispielsweise einen manuellen Start erfordern.

Anmeldekonto für Service festlegen

Sie können das Anmeldekonto des Services vom aktuellen Systemkonto in ein anderes Konto ändern. Sie können Anmeldekonten für Services festlegen, die auf Computern in der verwalteten Domäne oder im verwalteten Teilbaum ausgeführt werden. Legen Sie das lokale Systemkonto oder ein spezifisches Benutzerkonto fest.

Service neu starten

Sie können Services, die auf einem Computer in der verwalteten Domäne oder im verwalteten Teilbaum ausgeführt werden, neu starten.

Um einen Service neu starten zu können, benötigen Sie die Befugnisse zum Stoppen und zum Starten eines Services oder müssen mit einer Rolle verknüpft sein, die diese Befugnisse enthält, zum Beispiel die Rolle „Service starten und stoppen“.

Service stoppen

Sie können Services, die auf einem Computer in der verwalteten Domäne oder im verwalteten Teilbaum ausgeführt werden, stoppen.

Service anhalten

Sie können Services, die auf einem Computer in der verwalteten Domäne oder im verwalteten Teilbaum ausgeführt werden, anhalten. Ob ein Service angehalten werden kann, hängt vom Typ des Services ab. Ein Service, der abhängige Services hat, kann zum Beispiel möglicherweise nicht angehalten werden.

Ausführung eines angehaltenen Services wieder aufnehmen

Sie können die Ausführung von Services, die auf einem Computer in der verwalteten Domäne oder im verwalteten Teilbaum angehalten wurden, wieder aufnehmen.

7.4 Verwalten von Druckern und Druckaufträgen

Die Verwaltung von Druckern umfasst das Verwalten der Druckwarteschlangen dieser Drucker. In DRA können Sie Ressourcendrucker und veröffentlichte Drucker anhalten und wieder aufnehmen, starten, ändern, stoppen und anzeigen. Außerdem können Sie in DRA die Eigenschaften und Prioritäten von Druckaufträgen bearbeiten. Verwenden Sie die nativen Windows-Tools, um einen Drucker hinzuzufügen oder zu löschen.

Ein Druckserver ist ein Computer, auf dem ein oder mehrere logische Drucker installiert sind. Ein logischer Drucker ist auf dem Computer definiert, der über den Druckergerätetreiber verfügt. Ein logischer Drucker umfasst den Druckertreiber, die Druckwarteschlange und Anschlüsse für den Drucker. Der Druckserver verknüpft logische Drucker mit Druckgeräten.

Ein verbundener Drucker wird auf den Computern definiert, von denen Dokumente zum Drucken ausgewählt werden. Ein verbundener Drucker stellt eine Verbindung zum einer Druckfreigabe im Netzwerk dar. Deshalb können Sie Drucker und Druckaufträge über die verknüpften Computer verwalten.

Ein veröffentlichter Drucker ist ein Drucker, der in Active Directory veröffentlicht ist. Ein veröffentlichter Drucker kann ein Netzwerkdrucker sein, der nicht direkt mit einem Server verbunden ist, oder ein Drucker, der von einem Cluster-Server gehostet wird.

HINWEIS: Drucker und Druckaufträge können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.

Weitere Informationen zum Verwalten von Druckern und Druckeraufgaben finden Sie in den folgenden Themen:

- Abschnitt 7.4.1, „Druckerverwaltungsaufgaben“, auf Seite 90
- Abschnitt 7.4.2, „Aufgaben der Druckauftragsverwaltung“, auf Seite 90
- Abschnitt 7.4.3, „Verwaltungsaufgaben für veröffentlichte Drucker“, auf Seite 91
- Abschnitt 7.4.4, „Aufgaben der Druckauftragsverwaltung für veröffentlichte Drucker“, auf Seite 92

7.4.1 Druckerverwaltungsaufgaben

Sie können Drucker verwalten, die mit Computern in der verwalteten Domäne oder im verwalteten Teilbaum verknüpft sind. Mit DRA können Sie Drucker während der Verwaltung anderer Ressourcen für den Computer verwalten.

Dieser Abschnitt beschreibt das Verwalten von Druckern über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole. Mit den entsprechenden Befugnissen können Sie verschiedene Druckerverwaltungsaufgaben ausführen, zum Beispiel einen Drucker stoppen.

Druckereigenschaften verwalten

Sie können die Eigenschaften von Druckern in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. Mit DRA können Sie Drucker während der Verwaltung anderer Ressourcen für den Computer verwalten.

Drucker anhalten

Sie können Drucker, die mit einem Computer in der verwalteten Domäne oder im verwalteten Teilbaum verknüpft sind, anhalten. Mit DRA können Sie Drucker während der Verwaltung anderer Ressourcen für den Computer verwalten.

Drucker wieder aufnehmen

Sie können angehaltene Drucker, die mit einem Computer in der verwalteten Domäne oder im verwalteten Teilbaum verknüpft sind, wieder aufnehmen. Mit DRA können Sie Drucker während der Verwaltung anderer Ressourcen für den Computer verwalten.

7.4.2 Aufgaben der Druckauftragsverwaltung

Sie können Druckaufträge verwalten, die mit Druckern in der verwalteten Domäne oder im verwalteten Teilbaum verknüpft sind. Da die Druckaufträge mit einem Drucker verknüpft sind, können Sie die Druckaufträge während der Verwaltung des Druckers verwalten.

Dieser Abschnitt beschreibt das Verwalten von Druckaufträgen über den Konto- und Ressourcenverwaltungsknoten der Delegierungs- und Konfigurationskonsole. Mit den entsprechenden Befugnissen können Sie verschiedene Aufgaben der Druckauftragsverwaltung ausführen, beispielsweise einen Druckauftrag abbrechen.

Eigenschaften eines Druckauftrags verwalten

Sie können die Druckauftragseigenschaften innerhalb des Workflows der Druckerverwaltung ändern. Da Druckaufträge mit Druckern verknüpft sind, können Sie die Druckaufträge während der Verwaltung des entsprechenden Druckers ändern. Welche Druckauftragseigenschaften Sie ändern können, hängt von Ihren Befugnissen ab. Um Druckauftragseigenschaften zu ändern, benötigen Sie Zugriff auf den entsprechenden Drucker und Computer.

Druckauftrag anhalten

Sie können Druckaufträge, die auf einem Drucker in der verwalteten Domäne oder im verwalteten Teilbaum ausgeführt werden, anhalten. Um einen Druckauftrag anzuhalten, benötigen Sie Zugriff auf den entsprechenden Drucker und Computer. Beim Anhalten eines Druckauftrags wird der Druckauftrag nicht aus der Druckwarteschlange gelöscht.

Druckauftrag wieder aufnehmen

Sie können angehaltene Druckaufträge wieder aufnehmen. Um einen Druckauftrag wieder aufzunehmen, benötigen Sie Zugriff auf den entsprechenden Drucker und Computer.

Druckauftrag neu starten

Sie können gestoppte Druckaufträge neu starten. Um einen Druckauftrag neu zu starten, benötigen Sie Zugriff auf den entsprechenden Drucker und Computer.

Druckauftrag abbrechen

Sie können einen Druckauftrag in der Druckerwarteschlange abbrechen. Wenn Sie einen Druckauftrag abbrechen, löscht DRA den Druckauftrag dauerhaft aus der Druckerwarteschlange. Um einen Druckauftrag abzubrechen, benötigen Sie Zugriff auf den entsprechenden Drucker und Computer.

7.4.3 Verwaltungsaufgaben für veröffentlichte Drucker

Sie können veröffentlichte Drucker in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. Sie können einen beliebigen Drucker, der in Active Directory veröffentlicht ist, und Drucker, die auf einem Clusterserver gehostet werden, hinzufügen oder suchen.

Dieser Abschnitt beschreibt die Verwaltung von veröffentlichten Druckern im Konto- und Ressourcenverwaltungsknoten. Mit den entsprechenden Befugnissen können Sie verschiedene Druckerverwaltungsaufgaben ausführen, zum Beispiel einen Drucker stoppen.

Eigenschaften veröffentlichter Drucker verwalten

Sie können die Eigenschaften von veröffentlichten Druckern in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. In DRA können Sie die veröffentlichten Drucker während der Verwaltung anderer Ressourcen verwalten.

Informationen zu veröffentlichten Druckern aktualisieren

Sie können die Seite mit den Informationen zum veröffentlichten Drucker in der verwalteten Domäne oder im verwalteten Teilbaum aktualisieren. In DRA können Sie die veröffentlichten Drucker während der Verwaltung anderer Ressourcen verwalten.

Veröffentlichten Drucker anhalten

Sie können einen veröffentlichten Drucker in der verwalteten Domäne oder im verwalteten Teilbaum anhalten. In DRA können Sie die veröffentlichten Drucker während der Verwaltung anderer Ressourcen verwalten.

Veröffentlichten Drucker wieder aufnehmen

Sie können einen angehaltenen, veröffentlichten Drucker in der verwalteten Domäne oder im verwalteten Teilbaum wieder aufnehmen. In DRA können Sie die veröffentlichten Drucker während der Verwaltung anderer Ressourcen verwalten.

Veröffentlichten Drucker verschieben

Sie können einen veröffentlichten Drucker, der in einem Container in der verwalteten Domäne verfügbar ist, in einen anderen Container in der gleichen Domäne verschieben. In DRA können Sie die veröffentlichten Drucker während der Verwaltung anderer Ressourcen verwalten.

Veröffentlichten Drucker umbenennen

Sie können freigegebene veröffentlichte Drucker in Active Directory umbenennen. In DRA können Sie die veröffentlichten Drucker während der Verwaltung anderer Ressourcen verwalten.

HINWEIS: Wenn Sie einen veröffentlichten Drucker in Active Directory umbenennen, wird der Freigabename des Ressourcendruckers nicht geändert und die Namensänderung auch nicht an den Ressourcendrucker, den Sie verwalten möchten, weitergereicht. Wenn der Ressourcendrucker beispielsweise den Namen „Emerald“ trägt und Sie den Drucker in Active Directory in „Ruby“ umbenennen, wird der Druckername anderen Benutzern als „Ruby“ angezeigt, der Ressourcendruckername bleibt aber weiterhin „Emerald“.

7.4.4 Aufgaben der Druckauftragsverwaltung für veröffentlichte Drucker

Sie können Druckaufträge verwalten, die mit veröffentlichten Druckern in der verwalteten Domäne oder im verwalteten Teilbaum verknüpft sind. Da die Druckaufträge mit einem Drucker verknüpft sind, können Sie die Druckaufträge während der Verwaltung des veröffentlichten Druckers verwalten.

Dieser Abschnitt beschreibt die Verwaltung von veröffentlichten Druckern im Konto- und Ressourcenverwaltungsknoten. Mit den entsprechenden Befugnissen können Sie verschiedene Aufgaben der Druckauftragsverwaltung ausführen, beispielsweise einen Druckauftrag abbrechen.

Eigenschaften eines Druckauftrags verwalten

Sie können die Druckauftragseigenschaften innerhalb des Workflows zur Verwaltung veröffentlichter Drucker ändern. Da Druckaufträge mit Druckern verknüpft sind, können Sie die Druckaufträge während der Verwaltung des entsprechenden veröffentlichten Druckers ändern. Welche Druckauftragseigenschaften Sie ändern können, hängt von Ihren Befugnissen ab. Um Druckauftragseigenschaften zu ändern, benötigen Sie Zugriff auf den entsprechenden veröffentlichten Drucker.

Druckauftrag anhalten

Sie können Druckaufträge, die auf einem veröffentlichten Drucker in der verwalteten Domäne oder im verwalteten Teilbaum ausgeführt werden, anhalten. Um einen Druckauftrag anzuhalten, benötigen Sie Zugriff auf den entsprechenden veröffentlichten Drucker. Beim Anhalten eines Druckauftrags wird der Druckauftrag nicht aus der Druckwarteschlange gelöscht.

Druckauftrag wieder aufnehmen

Sie können einen angehaltenen Druckauftrag in der verwalteten Domäne oder im verwalteten Teilbaum wieder aufnehmen. Um einen Druckauftrag wieder aufzunehmen, benötigen Sie Zugriff auf den entsprechenden veröffentlichten Drucker.

Druckauftrag neu starten

Sie können einen gestoppten Druckauftrag in der verwalteten Domäne oder im verwalteten Teilbaum neu starten. Um einen Druckauftrag neu zu starten, benötigen Sie Zugriff auf den entsprechenden veröffentlichten Drucker.

Druckauftrag abbrechen

Sie können einen Druckauftrag in der verwalteten Domäne oder im verwalteten Teilbaum, der in der Druckerwarteschlange steht, abbrechen. Wenn Sie einen Druckauftrag abbrechen, löscht DRA den Druckauftrag dauerhaft aus der Druckerwarteschlange. Um einen Druckauftrag abzubrechen, benötigen Sie Zugriff auf den entsprechenden veröffentlichten Drucker.

7.5 Verwalten von Freigaben

Freigaben sind eine Möglichkeit, Ressourcen wie Dateien oder Drucker für andere Benutzer im Netzwerk verfügbar zu machen. Jede Freigabe hat einen Freigabenamen, der sich auf einen freigegebenen Ordner auf dem Server bezieht. DRA verwaltet Freigaben nur auf den Computern in den verwalteten Domänen. Zur erfolgreichen Verwaltung von Freigaben muss das Zugriffskonto auf allen Computern, auf denen Sie Ressourcen verwalten möchten, über Administratorberechtigungen verfügen, beispielsweise als Mitglied der lokalen Administratorgruppe. Um diese Berechtigungen zuzuweisen, fügen Sie das Zugriffskonto zur nativen Gruppe der Domänenadministratoren in der Domäne des Computers hinzu.

HINWEIS: Freigaben können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.

Freigabeeigenschaften verwalten

Sie können die Eigenschaften von Freigaben in der verwalteten Domäne oder im verwalteten Teilbaum verwalten. Mit DRA können Sie Freigaben während der Verwaltung anderer Ressourcen für den Computer verwalten.

Freigabe erstellen

Sie können Freigaben für einen Computer in der verwalteten Domäne oder im verwalteten Teilbaum erstellen. Sie können außerdem die Eigenschaften für diese Freigabe bearbeiten.

Freigabe klonen

Sie können Freigaben für einen Computer in der verwalteten Domäne oder im verwalteten Teilbaum klonen. Das Klonen von Freigaben ermöglicht ein schnelles Erstellen von Freigaben auf Grundlage anderer Freigaben mit ähnlichen Eigenschaften. Diese Flexibilität ermöglicht Ihnen das Erzwingen konsistenter Einstellungen für alle Freigaben, die Sie in einer bestimmten Domäne erstellen.

Wenn Sie eine Freigabe klonen, füllt DRA den Assistenten „Freigabe klonen“ mit Werten aus der ausgewählten Freigabe aus. Sie können auch die Eigenschaften der neuen Freigabe bearbeiten.

Freigabe löschen

Sie können Freigaben auf Computern in der verwalteten Domäne oder im verwalteten Teilbaum löschen.

7.6 Verwalten von verbundenen Benutzern

Jedes Mal, wenn ein Benutzer eine Verbindung zu einer bestimmten Ressource auf einem Remotecomputer herstellt, wird eine Sitzung gegründet. Ein verbundener Benutzer ist ein Benutzer, der eine Verbindung zu einer freigegebenen Ressource im Netzwerk hat.

DRA verwaltet verbundene Benutzer nur auf den Computern in den verwalteten Domänen. Das Zugriffskonto muss auf allen Computern, auf denen Sie verbundene Benutzer verwalten möchten, über Administratorberechtigungen verfügen, beispielsweise als Mitglied der lokalen Administratorgruppe. Um diese Berechtigungen zuzuweisen, fügen Sie das Zugriffskonto zur nativen Gruppe der Domänenadministratoren in der Domäne des Computers hinzu.

HINWEIS: Verbundene Benutzer können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.

Benutzer trennen

Sie können verbundene Benutzer von einem Computer in der verwalteten Domäne oder im verwalteten Teilbaum trennen. Dazu benötigen Sie Zugriff auf den Computer und die offene Sitzung. Durch das Trennen eines verbundenen Benutzers wird die geöffnete Sitzung beendet.

Liste verbundener Benutzer anzeigen

Um sicherzustellen, dass Sie die neuesten Informationen zu den offenen Sitzungen auf dem Computer anzeigen, aktualisieren Sie manuell die Liste der verbundenen Benutzer. Dazu benötigen Sie Zugriff auf den Computer und die offene Sitzung.

7.7 Verwalten von Geräten

Ein Gerät ist ein Ausrüstungselement, das mit einem Netzwerk verbunden ist, zum Beispiel ein Computer, ein Drucker, ein Modem oder ein anderes Peripheriegerät.

Auch wenn ein Gerät auf dem Computer installiert ist, erkennt Windows das Gerät erst, wenn der geeignete Treiber installiert und konfiguriert ist. Ein Gerätetreiber sorgt dafür, dass eine bestimmte Hardware mit dem Betriebssystem kommunizieren kann.

Mit DRA können Sie Geräte nur auf den Computern in der verwalteten Domäne konfigurieren und verwalten. Das Zugriffskonto muss auf allen Computern, auf denen Sie Geräte verwalten möchten, über Administratorberechtigungen verfügen, beispielsweise als Mitglied der lokalen Administratorgruppe. Um diese Berechtigungen zuzuweisen, fügen Sie das Zugriffskonto zur nativen Gruppe der Domänenadministratoren in der Domäne des Computers hinzu.

HINWEIS: Geräte können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.

Geräteeigenschaften verwalten

Sie können die Eigenschaften eines Geräts auf einem bestimmten Computer bearbeiten. Beim Ändern der Geräteeigenschaften können Sie auch den Starttyp für das Gerät ändern.

Gerät starten

Sie können Geräte auf einem bestimmten Computer in der verwalteten Domäne oder im verwalteten Teilbaum starten.

Gerät stoppen

Sie können Geräte auf einem bestimmten Computer in der verwalteten Domäne oder im verwalteten Teilbaum stoppen.

7.8 Verwalten von Ereignisprotokollen

Ein Ereignis ist ein wichtiges Geschehnis im System oder in einer Anwendung. Das Windows-Betriebssystem zeichnet Informationen über Ereignisse in Ereignisprotokolldateien auf. Auf jedem Computer können mehrere Ereignisprotokolle gespeichert sein. In der nativen Windows-Ereignisanzeige können Sie die Ereignisprotokolle anzeigen. DRA verwaltet Ereignisprotokolle nur auf den Computern in den verwalteten Domänen.

DRA zeichnet vom Benutzer initiierte Operationen im Protokollarchiv auf, einem sicheren Repository. Wahlweise können Sie festlegen, dass DRA die vom Benutzer initiierten Operationen nicht nur im DRA-Protokollarchiv, sondern auch im Windows-Ereignisprotokoll aufzeichnet. Weitere Informationen finden Sie unter Datums- und Uhrzeitangaben.

HINWEIS: Ereignisprotokolle können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.

7.8.1 Ereignisprotokolltypen

Computers, die unter Microsoft Windows ausgeführt werden, zeichnen in verschiedenen Protokollen zusätzliche Informationen auf. Diese Protokolle werden nachfolgend kurz beschrieben:

Protokolltyp	Beschreibung
ADAM	Zeichnet Ereignisse auf, die vom ADAM-Repository protokolliert werden.
Anwendung	Zeichnet Ereignisse auf, die von einer Anwendung auf dem Computer protokolliert werden, zum Beispiel ein Servicestart oder Servicefehler. DRA speichert Ereignisse beispielsweise im Anwendungsprotokoll.
Verzeichnisdienst	Zeichnet Ereignisse in Bezug auf die Domänencontroller auf, die die Sicherheitsdatenbank warten.
Dateireplikationsdienst	Zeichnet Ereignisse in Bezug auf die Dateireplikationsdienste auf, die vom Betriebssystem bereitgestellt werden.
Sicherheit	Zeichnet Ereignisse auf, die Anmeldeversuche, Datei- und Verzeichniszugriffe und Änderungen der Sicherheitsrichtlinie, die auf den Revisionsrichtlinienoptionen basieren, enthalten.
System	Zeichnet Ereignisse auf, die von Windows-Systemkomponenten protokolliert werden, beispielsweise der Ausfall eines Treibers oder das Starten und Stoppen von Services.

7.8.2 Verwaltungsaufgaben zum Ereignisprotokoll

Sie können die maximale Größe für eine Ereignisprotokolldatei festlegen und bestimmen, wie vorgegangen werden soll, wenn ein Ereignisprotokoll „voll“ ist. Das Eigenschaftenfenster zeigt außerdem den Namen des Protokolls, den Pfad und Namen der Protokolldatei, den Erstellungszeitpunkt des Protokolls, den Zeitpunkt der letzten Änderung des Protokolls und den Zeitpunkt des letzten Zugriffs auf das Protokoll an. Wenn Sie die Protokolldatei sichern, speichert DRA das Ereignisprotokoll mit einem eindeutigen Dateinamen an einem Standardspeicherort auf dem ausgewählten Computer.

Mit DRA können Sie Ereignisprotokolle während der Verwaltung anderer Ressourcen für den Computer verwalten. Mit den entsprechenden Befugnissen können Sie verschiedene Verwaltungsaufgaben für Freigaben ausführen, zum Beispiel die Eigenschaften des Ereignisprotokolls ändern.

Revision für Windows-Ereignisprotokolle aktivieren oder deaktivieren

Wenn Sie DRA installieren, werden Revisionsereignisse standardmäßig nicht im Windows-Ereignisprotokoll protokolliert. Sie können diese Art der Protokollierung durch Änderung eines Registrierungsschlüssels aktivieren.

WARNUNG: Gehen Sie beim Bearbeiten der Windows-Registrierung mit Bedacht vor. Ein Fehler in der Registrierung kann dazu führen, dass der Computer nicht mehr funktionsfähig ist. Wenn ein Fehler auftritt, können Sie die Registrierung auf den Zustand beim letzten erfolgreichen Starten des Computers wiederherstellen. Weitere Informationen finden Sie in der Hilfe im Windows-Registrierungseditor.

Ereignisprotokolleigenschaften verwalten

Sie können die Ereignisprotokolleigenschaften für einen bestimmten Computer ändern.

Protokolleinträge anzeigen

Sie können die Einträge in einem bestimmten Ereignisprotokoll eines Computers in der verwalteten Domäne oder im verwalteten Teilbaum anzeigen. Zum Anzeigen eines Ereignisprotokolls startet DRA die native Windows-Ereignisanzeige.

Ereignisprotokoll löschen

Sie können die Einträge in einem bestimmten Ereignisprotokoll eines Computers in der verwalteten Domäne oder im verwalteten Teilbaum löschen. Sie können die Einträge im Ereignisprotokoll wahlweise speichern, bevor Sie das Protokoll löschen.

7.9 Verwalten offener Dateien

Eine offene Datei ist eine Verbindung zu freigegebenen Ressourcen wie Dateien oder Pipes. Eine Pipe ist ein Kommunikationsmechanismus zwischen Prozessen, der die Kommunikation zwischen einem Prozess und einem anderen lokalen Prozess oder Remoteprozess ermöglicht.

DRA verwaltet offene Dateien nur auf Computern in der verwalteten Domäne oder im verwalteten Teilbaum. Das offene Dateien mit einem Computer verknüpft sind, können Sie die offenen Dateien während der Verwaltung anderer Ressourcen für den betreffenden Computer verwalten. Möglicherweise möchten Sie zum Beispiel offene Dateien schließen, wenn das System

heruntergefahren wird, oder ein neues Gerät oder einen neuen Service installieren. Sie können auch überwachen, auf welche Dateien die Benutzer am häufigsten zugreifen, und so die Dateisicherheit besser beurteilen.

HINWEIS: Offene Dateien können Sie nur über die Delegierungs- und Konfigurationskonsole verwalten.

Datei schließen

Sie können offene Dateien von Ressourcen im Netzwerk schließen. Es empfiehlt sich, die Benutzer zu benachrichtigen, wenn Sie beabsichtigen, offene Dateien zu schließen, damit die Benutzer Zeit haben, ihre Daten zu speichern. Um eine offene Datei zu schließen, benötigen Sie Zugriff auf den entsprechenden Computer.

Liste der offenen Dateien aktualisieren

Um sicherzustellen, dass Sie die neuesten Informationen zu den offenen Sitzungen auf dem Computer anzeigen, aktualisieren Sie manuell die Liste der verbundenen Benutzer. Um die Liste der offenen Dateien zu aktualisieren, benötigen Sie Zugriff auf den entsprechenden Computer.

8 Verwalten des Papierkorbs

Der Papierkorb stellt ein Sicherheitsnetz dar, indem er das temporäre Löschen von Benutzerkonten, Gruppen, Kontakten und Computerkonten ermöglicht. Die gelöschten Objekte können aus dem Papierkorb in ihren ursprünglichen Zustand mit allen Daten, wie SIDs, Zugriffssteuerungslisten und Gruppenmitgliedschaften, wiederhergestellt werden. Diese Flexibilität bietet eine größere Sicherheit beim Verwalten von Benutzerkonten, Gruppen, Kontakten und Computerkonten. Mit der Suchoption können Sie nach erforderlichen Objekten suchen. Informationen hierzu erhalten Sie unter *Suchen nach Objekten*.

Objekt aus dem Papierkorb wiederherstellen

Sie können gelöschte Objekte in die Container, aus denen sie gelöscht wurden, wiederherstellen. DRA stellt die Objekte in ihrem ursprünglichen Zustand wieder her. Alle Daten des Objekts, wie SIDs, Zugriffssteuerungslisten und Gruppenmitgliedschaften bleiben intakt. Ein Objekt kann ein Benutzerkonto, ein Kontakt, eine dynamische Gruppe, ein Ressourcenpostfach, eine dynamische Verteilergruppe oder ein Computerkonto sein.

Alle Objekte wiederherstellen

Sie können alle Objekte einer verwalteten Domäne gleichzeitig aus dem Papierkorb wiederherstellen. Sie können Objekte für eine bestimmte Domäne oder für alle verwalteten Domänen aus dem Papierkorb wiederherstellen. Um Objekte für eine bestimmte Domäne aus dem Papierkorb wiederherzustellen, muss der Papierkorb für diese Domäne aktiviert sein.

Objekt aus dem Papierkorb löschen

Sie können die Objekte einer verwalteten Domäne dauerhaft aus dem Papierkorb löschen. Ein aus dem Papierkorb gelöschtes Objekt kann anschließend nicht mehr wiederhergestellt werden. Ein Objekt kann ein Benutzerkonto, ein Kontakt, eine dynamische Gruppe, ein Ressourcenpostfach, eine dynamische Verteilergruppe oder ein Computerkonto sein.

Papierkorb leeren

Sie können den Papierkorb einer verwalteten Domäne leeren. Beim Leeren des Papierkorbs werden alle im Papierkorb enthaltenen Objekte dauerhaft gelöscht. Sie können den Papierkorb für eine bestimmte Domäne oder für alle verwalteten Domänen leeren. Um den Papierkorb für eine bestimmte Domäne zu leeren, muss der Papierkorb für diese Domäne aktiviert sein. Nachdem Sie den Papierkorb geleert haben, können Sie die gelöschten Objekte nicht mehr wiederherstellen.