Rechtliche Hinweise

Inhalt

Info zu diesem Handbuch

Das *Administratorhandbuch* enthält grundlegende Informationen zum Directory and Resource Administrator-Produkt. Dieses Handbuch enthält Definitionen der Terminologie und beschreibt verschiedene verwandte Konzepte. Außerdem enthält es schrittweise Anleitungen für viele Konfigurations- und Betriebsaufgaben.

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/.

Einführung

Bevor Sie mit der Installation und Konfiguration der Komponenten von 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 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 Microsoft Active Directory-, Windows-, 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.

2 Grundlegende Informationen zu den Directory and Administrator-Komponenten

Die Komponenten von DRA, mit denen Sie den berechtigten Zugriff verwalten, umfassen Primär- und Sekundärserver, Administratorkonsolen, Berichterstellungskomponenten und die Aegis-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
Administrator mit erweiterterten Befugnissen	DRA Reporting Center-Setup (NRC) PowerShell *(optional)* CLI *(optional)* DRA-ADSI-Anbieter *(optional)*	Beliebiger DRA-Server
Gelegentlicher Helpdesk-Administrator	Webkonsole	Beliebiger DRA-Server

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.

Delegierungs- und Konfigurationskonsole

Die Delegierungs- und Konfigurationskonsole ist eine installierbare Benutzeroberfläche, die Systemadministratoren Zugriff auf die Konfigurations- und Verwaltungsfunktionen von DRA bietet.

- **Delegierungsmanagement:** Das Delegierungsmanagement ermöglicht das granulare Festlegen und Zuweisen von Zugriff für Hilfsadministratoren auf verwaltete Ressourcen und Aufgaben.
- **Richtlinien- und Automatisierungsmangement:** Ermöglicht das Definieren und Erzwingen von Richtlinien zur Gewährleistung der Einhaltung von Standards und Konventionen in der Umgebung.
- **Konfigurationsmanagement:** Ermöglicht das Aktualisieren von DRA-Systemeinstellungen und Optionen, Hinzufügen von Anpassungen und Konfigurieren von verwalteten Services (Active Directory, Exchange, Azure Active Directory usw.).
- **Konto- und Ressourcenverwaltung:** Bietet DRA-Hilfsadministratoren die Möglichkeit, delegierte Objekte verbundener Domänen und Services über die Delegierungs- und Konfigurationskonsole anzuzeigen und zu verwalten.

Webkonsole

Die Webkonsole ist eine webbasierte Benutzeroberfläche, die Hilfsadministratoren schnellen und einfachen Zugriff zum Anzeigen und Verwalten delegierter Objekte verbundener Domänen und Services bietet. Die Administratoren können das Aussehen und die Verwendung der Webkonsole anpassen, indem sie ein angepasstes Branding und angepasste Objekteigenschaften einfügen.

Berichterstellungskomponenten

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

- Ressourcenberichte für Active Directory-Objekte
- Berichte zu Active Directory-Objektdaten
- Active Directory-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.

Workflow-Engine

DRA lässt sich mit der Aegis-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 auf der DRA-Dokumentations-Website.

Produktarchitektur

II Produktinstallation und -aufrüstung

Dieses Kapitel enthält eine kurze Beschreibung der empfohlenen Hardware und Software sowie der Kontoanforderungen für Directory Resource Administrator. Anschließend werden Sie durch den Installationsprozess geführt. Das Dokument enthält hierzu eine Checkliste für jede Installationskomponente.

3 Planen der Bereitstellung

Dieser Abschnitt enthält Angaben zur Beurteilung der Kompatibilität Ihrer Hardware- und Softwareumgebung und zu den erforderlichen Ports und Protokollen, die Sie für die Bereitstellung konfigurieren müssen. Beachten Sie diese Informationen bei der Planung Ihrer Directory and Resource Administrator-Bereitstellung.

Getestete Ressourcenempfehlungen

Dieser Abschnitt enthält Informationen zur Größe der empfohlenen Basisressourcen. Je nach verfügbarer Hardware, der spezifischen Umgebung, der Art der verarbeiteten Daten und anderen Faktoren können Ihre Ergebnisse abweichen. Unter Umständen stehen nun größere, leistungsstärkere Hardwarekonfigurationen zur Verfügung, die eine größere Last verarbeiten können. Wenden Sie sich bei Fragen an NetIQ Consulting Services.

Ausführung in einer Umgebung mit ungefähr einer Million Active Directory-Objekten:

Komponente	Prozessor	Arbeitsspeicher	Speicher
DRA-Verwaltungsserver	8 Prozessorkerne, 2,0 GHz	16 GB	120 GB
DRA-Webkonsole	2 Prozessorkerne, 2,0 GHz	8 GB	100 GB
DRA-Berichterstellung	4 Prozessorkerne, 2,0 GHz	16 GB	100 GB
DRA-Workflowserver	4 Prozessorkerne, 2,0 GHz	16 GB	120 GB

Bereitstellung von Ressourcen für die virtuelle Umgebung

DRA hält große Arbeitsspeichersegmente über längere Zeiträume aktiv. Berücksichtigen Sie beim Bereitstellen von Ressourcen für eine virtuelle Umgebung die folgenden Empfehlungen:

- Weisen Sie den Speicher als „Thick-Provisioning“ zu
- Legen Sie die Arbeitsspeicherreservierung auf „Reserve All Guest Memory (All Locked)“ (Gesamten Gastarbeitsspeicher reservieren (Alle gesperrt)) fest
- Stellen Sie sicher, dass die Auslagerungsdatei groß genug ist, um die potenzielle Neuzuweisung von Arbeitsspeicher zu decken, der durch Ballooning gesperrt wurde

Erforderliche Ports und Protokolle

Dieser Abschnitt beschreibt die Ports und Protokolle für die DRA-Kommunikation.

- Konfigurierbare Ports sind mit einem Sternchen (*) gekennzeichnet.
- Ports, für die ein Zertifikat erforderlich ist, sind mit zwei Sternchen (**) gekennzeichnet.

Komponententabellen:

DRA-Verwaltungsserver

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 135	Bidirektional	DRA-Verwaltungsserver	Der Endgerät-Mapper, eine grundlegende Anforderung für die DRA-Kommunikation, ermöglicht Verwaltungsservern das gegenseitige Auffinden in MMS
TCP 445	Bidirektional	DRA-Verwaltungsserver	Reproduktion des Delegierungsmodells; Dateireproduktion während der MMS-Synchronisierung (SMB)
Dynamischer TCP-Portbereich *	Bidirektional	Microsoft Active Directory-Domänencontroller	Standardmäßig weist DRA dynamisch Ports aus dem TCP-Portbereich von 1024 bis 65535 zu. Sie können diesen Bereich jedoch mit den Komponentendiensten konfigurieren. Weitere Informationen finden Sie in *Using Distributed COM with Firewalls* (Verwendung von Distributed COM mit Firewalls).
TCP 50000 *	Bidirektional	DRA-Verwaltungsserver	Attributreproduktion und Kommunikation zwischen DRA-Server und AD LDS (LDAP)
TCP 50001 *	Bidirektional	DRA-Verwaltungsserver	SSL-Attributreproduktion (AD LDS)
TCP/UDP 389	Ausgehend	Microsoft Active Directory-Domänencontroller	Active Directory-Objektverwaltung (LDAP)
	Ausgehend	Microsoft Exchange Server	Postfachmanagement (LDAP)
TCP/UDP 53	Ausgehend	Microsoft Active Directory-Domänencontroller	Namensauflösung
TCP/UDP 88	Ausgehend	Microsoft Active Directory-Domänencontroller	Ermöglicht die Authentifizierung vom DRA-Server an den Domänencontrollern (Kerberos)

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 80	Ausgehend	Microsoft Exchange Server	Für alle vor Ort installierten Exchange-Server der Version 2013 und höher erforderlich (HTTP)
	Ausgehend	Microsoft Office 365	PowerShell-Fernzugriff (HTTP)
TCP 443	Ausgehend	Microsoft Office 365, Change Guardian	Graph API-Zugriff und Change Guardian-Integration (HTTPS)
TCP 443, 5986, 5985	Ausgehend	Microsoft PowerShell	Native PowerShell-Commandlets (HTTPS) und PowerShell-Remotebefehle
TCP 5984	Localhost	DRA-Verwaltungsserver	IIS-Zugriff auf den Reproduktionsservice zur Unterstützung temporärer Gruppenzuweisungen
TCP 8092 * **	Ausgehend	Workflowserver	Workflowstatus und Auslösung (HTTPS)
TCP 50101 *	Eingehend	DRA-Client	Rechtsklick-Änderungsverlaufbericht bis Benutzeroberflächen-Revisionsbericht. Kann während der Installation konfiguriert werden.
TCP 8989	Localhost	Protokollarchivdienst	Protokollarchivkommunikation (muss nicht über die Firewall geöffnet werden)
TCP 50102	Bidirektional	DRA-Kernservice	Protokollarchivdienst
TCP 50103	Localhost	DRA-Cacheservice	Kommunikation des Cacheservice auf dem DRA-Server (muss nicht über die Firewall geöffnet werden)
TCP 1433	Ausgehend	Microsoft SQL Server	Datenerfassung für Berichterstellung
UDP 1434	Ausgehend	Microsoft SQL Server	Der SQL Server-Browserdienst verwendet diesen Port zum Identifizieren des Ports für die benannte Instanz.
TCP 8443	Bidirektional	Change Guardian-Server	Unified-Änderungsverlauf
TCP 8898	Bidirektional	DRA-Verwaltungsserver	Kommunikation des DRA-Reproduktionsservices zwischen den DRA-Servern für temporäre Gruppenzuweisungen
TCP 636	Ausgehend	Microsoft Active Directory-Domänencontroller	Active Directory-Objektverwaltung (LDAP SSL).

DRA-REST-Server

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 8755 * **	Eingehend	IIS-Server, DRA-PowerShell-Commandlets	Ausführen DRA-REST-basierter Workflowaktivitäten (ActivityBroker)
TCP 11192 * **	Ausgehend	DRA-Hostservice	Kommunikation zwischen dem DRA-REST-Service und dem DRA-Verwaltungsservice
TCP 135	Ausgehend	Microsoft Active Directory-Domänencontroller	Automatische Erkennung mit Dienstverbindungspunkt (SCP)
TCP 443	Ausgehend	Microsoft AD-Domänencontroller	Automatische Erkennung mit Dienstverbindungspunkt (SCP)

Webkonsole (IIS)

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 8755 * **	Ausgehend	DRA-REST-Service	Kommunikation zwischen DRA-Webkonsole, DRA PowerShell und DRA-Hostservice
TCP 443	Eingehend	Clientbrowser	Öffnen einer DRA-Website
TCP 443 **	Ausgehend	Advanced Authentication Server	Advanced Authentication

DRA-Delegierungs- und -Verwaltungskonsole

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 135	Ausgehend	Microsoft Active Directory-Domänencontroller	Automatische Erkennung mit Dienstverbindungspunkt (SCP)
Dynamischer TCP-Portbereich *	Ausgehend	DRA-Verwaltungsserver	DRA-Adapter-Workflowaktivitäten. Standardmäßig weist DCOM dynamisch Ports aus dem TCP-Portbereich von 1024 bis 65535 zu. Sie können diesen Bereich jedoch mit den Komponentendiensten konfigurieren. Weitere Informationen finden Sie in *Using Distributed COM with Firewalls* (DCOM) (Verwendung von Distributed COM (DCOM) mit Firewalls)
TCP 50102	Ausgehend	DRA-Kernservice	Erstellung des Änderungsverlaufberichts

Workflowserver

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 8755	Ausgehend	DRA-Verwaltungsserver	Ausführen DRA-REST-basierter Workflowaktivitäten (ActivityBroker)
Dynamischer TCP-Portbereich *	Ausgehend	DRA-Verwaltungsserver	DRA-Adapter-Workflowaktivitäten. Standardmäßig weist DCOM dynamisch Ports aus dem TCP-Portbereich von 1024 bis 65535 zu. Sie können diesen Bereich jedoch mit den Komponentendiensten konfigurieren. Weitere Informationen finden Sie in *Using Distributed COM with Firewalls* (DCOM) (Verwendung von Distributed COM mit Firewalls (DCOM))
TCP 1433	Ausgehend	Microsoft SQL Server	Workflow-Datenspeicher
TCP 8091	Eingehend	Betriebs- und Konfigurationskonsole	Workflow-BSL-API (TCP)
TCP 8092 **	Eingehend	DRA-Verwaltungsserver	Workflow-BSL-API (HTTP) und (HTTPS)
TCP 2219	Localhost	Namespace-Anbieter	Wird vom Namespace-Anbieter zum Ausführen von Adaptern verwendet
TCP 9900	Localhost	Correlation Engine	Wird von Correlation Engine für die Kommunikation mit der Workflow-Engine und dem Namespace-Anbieter verwendet
TCP 10117	Localhost	Ressourcenmanagement -Namespace-Anbieter	Wird vom Ressourcenmanagement-Namespace-Anbieter verwendet

Unterstützte Plattformen

Die neuesten Informationen zu den unterstützten Softwareplattformen finden Sie auf der Directory and Resource Administrator-Produktseite.

Verwaltetes System	Voraussetzungen
Azure Active Directory	Zur Aktivierung der Azure-Verwaltung müssen Sie die folgenden PowerShell-Module installieren: ◆ Skype for Business Online https://www.microsoft.com/en-us/download/details.aspx?id=39366 ◆ Azure Active Directory V2 (AzureAD) Version 2.0.2.4 oder höher ◆ AzureRM.Profile Version 5.8.2 oder höher PowerShell 5.1 oder das neueste Modul ist zum Installieren der neuen Azure PowerShell-Module erforderlich.

Verwaltetes System	Voraussetzungen
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online
Skype for Business	◆ Microsoft Skype for Business 2015
Änderungsverlauf	◆ Change Guardian 5.1 oder höher
Datenbanken	◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server 2017 ◆ Microsoft SQL Server 2019
Webbrowser	◆ Microsoft Internet Explorer 11 ◆ Google Chrome ◆ Mozilla Firefox
Workflowautomatisierung	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016

Anforderungen für DRA-Verwaltungsserver, Webkonsole und REST-Erweiterungen

Für die DRA-Komponenten sind die folgende Software und die folgenden Konten erforderlich:

- „Softwareanforderungen“, auf Seite 29
- „Serverdomäne“, auf Seite 30
- „Kontoanforderungen“, auf Seite 31
- „DRA-Zugriffskonten mit niedrigsten Berechtigungen“, auf Seite 32

Softwareanforderungen

Komponente	Voraussetzungen
Installationsziel	**Betriebssystem des NetIQ Administration-Servers:**
Betriebssystem	◆ Microsoft Windows Server 2012 R2, 2016, 2019 **HINWEIS:** Der Server muss außerdem Mitglied einer unterstützten, vor Ort bereitgestellten Microsoft Active Directory-Domäne sein.
	DRA-Benutzeroberflächen:
	◆ Microsoft Windows Server 2012 R2, 2016, 2019 ◆ Microsoft Windows 8.1 (x86 & x64), 10 (x86 & x64)
Installationsprogramm	◆ Microsoft .Net Framework 4.6.2 oder höher
Verwaltungsserver	**Directory and Resource Administrator:**
	◆ Microsoft .Net Framework 4.6.2 oder höher ◆ Microsoft Visual C++ 2013 Redistributable Packages (x64) und Microsoft Visual C++ 2017 (Update 3) Redistributable Packages (x64 und x86) ◆ Microsoft Message Queuing ◆ Microsoft Active Directory Lightweight Directory Services-Rollen ◆ Remoteregistrierungsdienst gestartet ◆ URL-Rewrite-Modul für Microsoft-Internetinformationsdienste ◆ Routing von Anwendungsanforderungen für Microsoft-Internetinformationsdienste
	Administration von Microsoft Office 365/Exchange Online:
	◆ Windows Azure Active Directory-Modul für Windows PowerShell ◆ Skype for Business Online, Windows PowerShell-Modul
	Weitere Informationen finden Sie unter Unterstützte Plattformen.
Benutzeroberfläche	**DRA-Benutzeroberflächen:**
	◆ Microsoft .Net Framework 4.6.2 ◆ Microsoft Visual C++ 2017 (Update 3) Redistributable Packages (x64 und x86)
DRA-Hostservice	◆ Microsoft .Net Framework 4.6.2 ◆ DRA-Verwaltungsserver
DRA-REST-Endgerät und -Service	◆ Microsoft .Net Framework 4.6.2
PowerShell-Erweiterungen	◆ Microsoft .Net Framework 4.6.2 ◆ PowerShell 5.1 oder höher

Komponente	Voraussetzungen
DRA-Webkonsole	**Webserver:** ◆ Microsoft .Net Framework 4.x > WCF-Dienste > HTTP-Aktivierung ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ URL-Rewrite-Modul für Microsoft-Internetinformationsdienste ◆ Routing von Anwendungsanforderungen für Microsoft-Internetinformationsdienste **Microsoft IIS-Komponenten:** ◆ Webserver ◆ Allgemeine HTTP-Funktionen ◆ Statischer Inhalt ◆ Standarddokument ◆ Verzeichnisbrowser ◆ HTTP-Fehler ◆ Anwendungsentwicklung ◆ ASP ◆ Integrität und Diagnose ◆ HTTP-Protokollierung ◆ Anforderungsmonitor ◆ Sicherheit ◆ Basic Authentication ◆ Leistung ◆ Komprimierung statischer Inhalte ◆ Webserver-Verwaltungstools

Serverdomäne

Komponente	Betriebssysteme
DRA-Server	◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

Kontoanforderungen

Konto	Beschreibung	Berechtigungen
AD-LDS-Gruppe	Das DRA-Servicekonto muss zu dieser Gruppe hinzugefügt werden, um Zugriff auf AD-LDS zu erhalten.	◆ Lokale Sicherheitsgruppe der Domäne

DRA-Servicekonto	Zum Ausführen des NetIQ Administration-Services erforderliche Berechtigungen	◆ Für Berechtigungen „Distributed COM-Benutzer“
		◆ Mitglied der AD-LDS-Administratorgruppe
		◆ Kontenoperatorgruppe
		◆ Protokollarchivgruppen (OnePointOp ConfgAdms und OnePointOp)
		◆ Wenn DRA auf einem Server mit STIG-Methode installiert wird, muss auf der Registerkarte „Konto“ eine der folgenden **Kontooptionen** für den DRA-Servicekontobenutzer ausgewählt werden:
		  ◆ Kerberos-AES-128-Bit-Verschlüsselung
		  ◆ Kerberos-AES-256-Bit-Verschlüsselung
		HINWEIS
		◆ Weitere Informationen zum Einrichten von Domänenzugriffskonten mit den niedrigsten Berechtigungen finden Sie in: DRA-Zugriffskonten mit niedrigsten Berechtigungen.
		◆ Weitere Informationen zum Einrichten eines gruppenverwalteten Servicekontos für DRA finden Sie in: „Konfigurieren der DRA-Services für ein gruppenverwaltetes Servicekonto“.

DRA-Administrator	Benutzerkonto oder Gruppe, das/die für die integrierte DRA-Administratorrolle bereitgestellt wird	◆ Lokale Sicherheitsgruppe der Domäne oder Domänenbenutzerkonto ◆ Mitglied der verwalteten Domäne oder einer verbürgten Domäne ◆ Wenn Sie ein Konto von einer verbürgten Domäne angeben, stellen Sie sicher, dass der Verwaltungsserver das Konto authentifizieren kann.

Konto	Beschreibung	Berechtigungen
DRA-Hilfsadministratorkonten	Konten, denen über DRA Befugnisse delegiert werden	◆ Fügen Sie alle DRA-Hilfsadministratorkonten zur Gruppe „Distributed COM-Benutzer“ hinzu, damit sie von Remoteclients aus eine Verbindung zum DRA-Server herstellen können. Dies ist nur bei Verwendung des Thick Clients oder der Delegierungs- und Konfigurationskonsole erforderlich. **HINWEIS:** DRA kann während der Installation so konfiguriert werden, dass es dies für Sie verwaltet.

DRA-Zugriffskonten mit niedrigsten Berechtigungen

Nachstehend finden Sie Informationen zu den Berechtigungen und Privilegien, die für die angegebenen Konten und für die auszuführenden Konfigurationsbefehle erforderlich sind.

Domänenzugriffskonto: Erteilen Sie dem Domänenzugriffskonto mit dem ADSI-Editor die folgenden Active Directory-Berechtigungen auf der obersten Domänenebene für die folgenden Nachfolgerobjekttypen:

- VOLLZUGRIFF auf builtInDomain-Objekte
- VOLLZUGRIFF auf Computerobjekte
- VOLLZUGRIFF auf Verbindungspunktobjekte
- VOLLSTÄNDIGE KONTROLLE über Kontaktobjekte
- VOLLSTÄNDIGE KONTROLLE über Containerobjekte
- VOLLZUGRIFF auf Gruppenobjekte
- VOLLZUGRIFF auf InetOrgPerson-Objekte
- VOLLZUGRIFF auf MsExchDynamicDistributionList-Objekte
- VOLLZUGRIFF auf MsExchSystemObjectsContainer-Objekte
- VOLLZUGRIFF auf Objekte vom Typ „organisatorische Einheit“
- VOLLZUGRIFF auf Druckerobjekte
- VOLLZUGRIFF auf publicFolder-Objekte
- VOLLZUGRIFF auf Objekte vom Typ „freigegebener Ordner“
- VOLLZUGRIFF auf Benutzerobjekte

Erteilen Sie dem Domänenzugriffskonto die folgenden Active Directory-Berechtigungen auf oberster Domänenebene für dieses Objekt und alle Nachfolgerobjekte:

- Erstellen von Computerobjekten zulassen
- Erstellen von Kontaktobjekten zulassen
- Erstellen von Containerobjekten zulassen
- Erstellen von Gruppenobjekten zulassen

- Erstellen von MsExchDynamicDistributionList-Objekten zulassen
- Erstellen von Objekten vom Typ „organisatorische Einheit“ zulassen
- Erstellen von publicFolder-Objekten zulassen
- Erstellen von Objekten vom Typ „freigegebener Ordner“ zulassen
- Erstellen von Benutzerobjekten zulassen
- Löschen von Computerobjekten zulassen
- Löschen von Kontaktobjekten zulassen
- Löschen von Containern zulassen
- Löschen von Gruppenobjekten zulassen
- Löschen von InetOrgPerson-Objekten zulassen
- Löschen von MsExchDynamicDistributionList-Objekten zulassen
- Löschen von Objekten vom Typ „organisatorische Einheit“ zulassen
- Löschen von publicFolder-Objekten zulassen
- Löschen von Objekten vom Typ „freigegebener Ordner“ zulassen
- Löschen von Benutzerobjekten zulassen

HINWEIS

- Bestimmte integrierte Containerobjekte in Active Directory übernehmen standardmäßig nicht die Berechtigungen von der obersten Domänenebene. Aus diesem Grund muss für diese Objekte die Vererbung aktiviert werden oder es müssen explizite Berechtigungen festgelegt werden.
- Wenn der REST-Server nicht auf dem gleichen Server wie der DRA-Verwaltungsserver installiert ist, benötigt das ausgeführte REST-Servicekonto in Active Directory Vollzugriff auf den REST-Server. Legen Sie zum Beispiel VOLLZUGRIFF auf `CN=DRARestServer,CN=System,DC=myDomain,DC=com` fest.

Exchange-Zugriffskonto: Weisen Sie zur Verwaltung von vor Ort bereitgestellten Microsoft Exchange-Objekten dem Exchange-Zugriffskonto die Rolle „Organisationsverwaltung“ zu und weisen Sie das Exchange-Zugriffskonto der Gruppe „Konten-Operatoren“ zu.

Skype-Zugriffskonto: Stellen Sie sicher, dass dieses Konto ein Skype-fähiger Benutzer ist und mindestens eine der folgenden Rollenmitgliedschaften erfüllt:

- Mitglied der CSAdministrator-Rolle
- Mitglied der CSUserAdministrator-Rolle und der CSArchiving-Rolle

Konto für den Zugriff auf öffentliche Ordner: Weisen Sie dem Konto für den Zugriff auf öffentliche Ordner die folgenden Active Directory-Berechtigungen zu:

- Verwaltung öffentlicher Ordner
- Für Mail aktivierte öffentliche Ordner

Azure-Mandantenzugriffskonto: Weisen Sie dem Azure-Mandantenzugriffskonto die folgenden Azure Active Directory-Berechtigungen zu:

- Verteilergruppen

- E-Mail-Empfänger
- Erstellung von E-Mail-Empfängern
- Erstellung von Sicherheitsgruppen und Sicherheitsgruppenmitgliedschaft
- (Optional) Skype for Business-Administrator

  Wenn Sie Skype for Business Online verwalten möchten, weisen Sie dem Azure-Mandantenzugriffskonto die Befugnis „Skype for Business-Administrator“ zu.
- Benutzeradministrator

Berechtigungen für NetIQ Administration-Servicekonto:

- Lokale Administratoren
- Erteilen Sie dem Überschreibungskonto mit der geringsten Berechtigung die „uneingeschränkte Berechtigung“ auf Freigabeordner oder DFS-Ordner, wo Basisverzeichnisse bereitgestellt werden.
- **Ressourcenverwaltung**: Zum Verwalten von veröffentlichten Ressourcen in einer verwalteten Active Directory-Domäne müssen dem Domänenzugriffskonto lokale Administrationsberechtigungen für diese Ressourcen erteilt werden.

Nach der DRA-Installation: Nachdem die erforderlichen Domänen hinzugefügt wurden oder mit DRA verwaltet werden, führen Sie die folgenden Befehle aus:

- Berechtigung auf den Container „Gelöschte Objekte“ vom DRA-Installationsordner delegieren (Befehl muss von einem Domänenadministrator ausgeführt werden):

  `DraDelObjsUtil.exe /domain:<NetBIOS-Domänenname> /delegate:<Kontoname>`
- Berechtigung auf organisatorische Einheit „NetIQRecycleBin“ vom DRA-Installationsordner delegieren:

  `DraRecycleBinUtil.exe /domain:<NetBIOS-Domänenname> /delegate:<Kontoname>`

Fernzugriff auf SAM: Weisen Sie Domänencontroller oder von DRA verwaltete Mitgliedsserver zu, damit die in den Einstellungen für Gruppenrichtlinienobjekte unten aufgeführten Konten Fernabfragen in der Datenbank von Security Account Manager (SAM) ausführen können. Die Konfiguration muss das DRA-Servicekonto enthalten.

Netzwerkzugriff: Clients einschränken, die Remoteaufrufe an SAM ausführen dürfen

Gehen Sie wie folgt vor, um auf diese Einstellung zuzugreifen:

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole auf dem Domänencontroller.
2. Erweitern Sie **Domänen** > **[Domänencontroller]** > **Gruppenrichtlinienobjekte** in der Baumstruktur.
3. Klicken Sie mit der rechten Maustaste auf **Standard-Domänencontrollerrichtlinie** und wählen Sie **Bearbeiten** aus, um den Gruppenrichtlinienobjekt-Editor für diese Richtlinie zu öffnen.
4. Erweitern Sie **Computerkonfiguration** > **Richtlinien** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Lokale Richtlinien** in der Baumstruktur des Gruppenrichtlinienobjekt-Editors.
5. Doppelklicken Sie im Richtlinienbereich auf **Netzwerkzugriff: Clients einschränken, die Remoteaufrufe an SAM ausführen dürfen** und wählen Sie **Diese Richtlinieneinstellung definieren** aus.

6 Klicken Sie auf **Sicherheit bearbeiten** und aktivieren Sie **Zulassen** für den Fernzugriff. Fügen Sie das DRA-Servicekonto hinzu, falls es noch nicht als Benutzer oder Teil der Administratorengruppe enthalten ist.

7 Wenden Sie die Änderungen an. Dies fügt die Sicherheitsbeschreibung `O:BAG:BAD:(A;;RC;;;BA)` zu den Richtlinieneinstellungen hinzu.

Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7023292.

Anforderungen für die Berichterstellung

Die Anforderungen für die DRA-Berichterstellung sind folgende:

Softwareanforderungen

Komponente	Voraussetzungen
Installationsziel	**Betriebssystem:** ◆ Microsoft Windows Server 2012 R2, 2016, 2019
NetIQ Reporting Center (v3.2)	**Datenbank:** ◆ Microsoft SQL Server 2016, 2017, 2019 ◆ Microsoft SQL Server Reporting Services **Webserver:** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft IIS-Komponenten: ◆◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** ◆ Erforderlich zum Ausführen des NRC-Installationsprogramms ◆ Ebenfalls erforderlich auf dem DRA-Primärserver zur Konfiguration der DRA Reporting-Services **HINWEIS:** Wenn NetIQ Reporting Center (NRC) auf einem SQL Server-Computer installiert wird, muss .NET Framework 3.5 unter Umständen vor der Installation von NRC manuell installiert werden.
DRA-Berichterstellung	**Datenbank:** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server-Agent

Lizenzierungsanforderungen

Ihre Lizenz bestimmt, welche Produkte und Funktionen Sie verwenden können. Für DRA muss ein Lizenzschlüssel mit dem Verwaltungsserver installiert werden.

Nachdem Sie den Verwaltungsserver installiert haben, können Sie mit dem Systemdiagnose-Dienstprogramm Ihre gekaufte Lizenz installieren. Im Installationspaket ist außerdem ein Probelizenzschlüssel (TrialLicense.lic) enthalten, mit dem Sie 30 Tage lang eine unbegrenzte Anzahl an Benutzerkonten und Postfächern verwalten können.

Weitere Informationen zu Lizenzdefinitionen und -einschränkungen finden Sie in der Endbenutzer-Lizenzvereinbarung (EULA).

4 Produktinstallation

Dieses Kapitel führt Sie durch die Installation von Directory and Resource Administrator. Weitere Informationen zur Planung der Installation oder Aufrüstung finden Sie in Planen der Bereitstellung.

DRA-Verwaltungsserver installieren

Sie können den DRA-Verwaltungsserver als primären oder sekundären Knoten in Ihrer Umgebung installieren. Die Anforderungen für Primär- und Sekundärverwaltungsserver sind die gleichen. Jede DRA-Bereitstellung muss jedoch einen Primärverwaltungsserver enthalten.

Das DRA-Serverpaket bietet die folgenden Funktionen:

- **Verwaltungsserver:** Speichert Konfigurationsdaten (Umgebungsdaten, delegierter Zugriff, Richtlinie), führt Operator- und Automatisierungsaufgaben aus und prüft die systemweite Aktivität. Der Verwaltungsserver umfasst die folgenden Funktionen:
  - **Protokollarchiv-Ressourcenkit:** Ermöglicht die Anzeige von Revisionsinformationen.
  - **DRA-SDK:** Stellt die ADSI-Beispielskripte bereit und unterstützt Sie beim Erstellen eigener Skripte.
- **REST-Service und -Endgeräte:** Stellt die RESTful-Schnittstellen bereit, mit der die DRA-Webkonsole und die Nicht-DRA-Clients DRA-Vorgänge anfordern können. Dieser Service muss auf einem Computer ausgeführt werden, auf dem entweder die DRA-Konsole oder der DRA-Verwaltungsservice installiert ist.
- **Benutzeroberflächen:** Die Webclientoberfläche, die hauptsächlich von Hilfsadministratoren verwendet wird, aber auch Optionen zur benutzerdefinierten Anpassung bietet.
  - **ADSI-Anbieter:** Ermöglicht das Erstellen eigener Richtlinienskripte.
  - **Befehlszeilenschnittstelle:** Ermöglicht das Ausführen von DRA-Vorgängen.
  - **Delegierung und Konfiguration:** Bietet Systemadministratoren Zugriff auf die Konfigurations- und Verwaltungsfunktionen von DRA. Ermöglicht außerdem das granulare Festlegen und Zuweisen von Zugriff für Hilfsadministratoren auf verwaltete Ressourcen und Aufgaben.
  - **PowerShell-Erweiterungen:** Stellt ein PowerShell-Modul bereit, dank dem Nicht-DRA-Clients über PowerShell-Commandlets DRA-Vorgänge anfordern können.
  - **Webkonsole:** Die Webclientoberfläche, die hauptsächlich von Hilfsadministratoren verwendet wird, aber auch Optionen zur benutzerdefinierten Anpassung bietet.

Informationen zur Installation spezifischer DRA-Konsolen und Befehlszeilen-Clients auf mehreren Computern finden Sie in DRA-Clients installieren.

Checkliste für die interaktive Installation:

Schritt	Details
Am Zielserver anmelden	Melden Sie sich zur Installation mit einem Konto mit lokalen Administratorrechten am Microsoft Windows-Zielserver an.
Admin-Installationskit kopieren und ausführen	Führen Sie das DRA-Installationskit (NetIQAdminInstallationKit.msi) aus, um die DRA-Installationsmedien im lokalen Dateisystem zu extrahieren. **HINWEIS:** Das Installationskit installiert bei Bedarf das .NET Framework auf dem Zielserver.
DRA installieren	Klicken Sie auf **DRA installieren** und **Weiter**, um die Installationsoptionen anzuzeigen. **HINWEIS:** Um die Installation später auszuführen, navigieren Sie zum Speicherort, an dem die Installationsmedien extrahiert wurden (Installationskit anzeigen), und führen Sie `Setup.exe` aus.
Standardinstallation	Wählen Sie die zu installierenden Komponenten und akzeptieren Sie entweder den Standardinstallationspfad `C:\Program Files (x86)\NetIQ\DRA` oder geben Sie für die Installation einen alternativen Speicherort an. Komponentenoptionen: **Verwaltungsserver** ◆ Protokollarchiv-Ressourcenkit ◆ DRA-SDK **REST-Services** **Benutzeroberflächen** ◆ ADSI-Anbieter ◆ Befehlszeilenschnittstelle ◆ Delegierung und Konfiguration ◆ PowerShell-Erweiterungen ◆ Webkonsole
Voraussetzungen überprüfen	Im Dialogfeld **Voraussetzungen** wird die Liste der Software angezeigt, die für die zur Installation ausgewählten Komponenten erforderlich ist. Das Installationsprogramm führt Sie durch die Installation aller fehlenden Voraussetzungen, die zum erfolgreichen Abschließen der Installation erforderlich sind.
EULA-Lizenzvereinbarung akzeptieren	Akzeptieren Sie die Bedingungen der Endbenutzer-Lizenzvereinbarung.
Serverbetriebsmodus auswählen	Wählen Sie **Primär** aus, um den ersten DRA-Verwaltungsserver in einem Multi-Master-Set zu installieren (eine Bereitstellung enthält jeweils nur einen Primärserver), oder wählen Sie **Sekundär** aus, um einen DRA-Verwaltungsserver zu einem vorhandenen Multi-Master-Set hinzuzufügen. Informationen zu Multi-Master-Sets finden Sie in „Konfigurieren des Multi-Master-Sets“.

Schritt	Details
Installationskonto und Berechtigungsnachweis angeben	◆ DRA-Servicekonto ◆ AD-LDS-Gruppe ◆ DRA-Administrator Weitere Informationen hierzu finden Sie unter: Anforderungen für DRA-Verwaltungsserver, Webkonsole und REST-Erweiterungen.
DCOM-Berechtigungen konfigurieren	Aktivieren Sie DRA zum Konfigurieren des „Distributed COM“-Zugriffs auf authentifizierte Benutzer.
Ports konfigurieren	Weitere Informationen zu den standardmäßigen Ports finden Sie in Erforderliche Ports und Protokolle.
Speicherort angeben	Geben Sie den lokalen Dateispeicherort an, den DRA zum Speichern von Revisionsdaten und Cache-Daten verwenden soll.
Speicherort für DRA-Reproduktionsdatenbank festlegen	◆ Geben Sie den Dateispeicherort für die DRA-Reproduktionsdatenbank und den Reproduktionsservice-Port an. ◆ Geben Sie das SSL-Zertifikat an, das für die sichere Kommunikation der Datenbank über IIS verwendet werden soll, und geben Sie den IIS-Reproduktions-Port an.
SSL-Zertifikat für REST-Service angeben	Wählen Sie das SSL-Zertifikat aus, das für den REST-Service verwendet werden soll, und geben Sie den REST-Serviceport und den Hostserviceport an.
SSL-Zertifikat für Webkonsole angeben	Geben Sie das SSL-Zertifikat an, das zum HTTPS-Binden verwendet werden soll.
Installationskonfiguration überprüfen	Sie können die Konfiguration auf der Installationsübersichtsseite überprüfen, bevor Sie durch Klicken auf **Installieren** mit der Installation fortfahren.
Überprüfung nach der Installation	Nach dem Abschluss der Installation wird die Systemdiagnose ausgeführt, um die Installation zu überprüfen und die Produktlizenz zu aktualisieren. Weitere Informationen finden Sie unter „Dienstprogramm „Health Check“ (Systemdiagnose)“.

DRA-Clients installieren

Führen Sie das Installationsprogramm „DRAInstaller.msi“ mit dem entsprechenden MST-Paket auf dem Installationsziel aus, um spezifische DRA-Konsolen und Befehlszeilen-Clients zu installieren:

NetIQDRACLI.mst	Installiert die Befehlszeilenbenutzeroberfläche
NetIQDRAADSI.mst	Installiert den DRA-ADSI-Anbieter
NetIQDRAClients.mst	Installiert alle DRA-Benutzeroberflächen

Um bestimmte DRA-Clients auf mehreren Computern im ganzen Unternehmen bereitzustellen, konfigurieren Sie ein Gruppenrichtlinienobjekt zur Installation des jeweiligen MST-Pakets.

1. Starten Sie Active Directory-Benutzer und -Computer und erstellen Sie ein Gruppenrichtlinienobjekt.
2. Fügen Sie das Paket „DRAInstaller.msi“ zu diesem Gruppenrichtlinienobjekt hinzu.
3. Stellen Sie sicher, dass dieses Gruppenrichtlinienobjekt über eine der folgenden Eigenschaften verfügt:
   - Jedes Benutzerkonto in der Gruppe verfügt über Hauptbenutzerberechtigungen für den entsprechenden Computer.
   - Aktivieren Sie die Richtlinieneinstellung „Immer mit erhöhten Rechten installieren“.
4. Fügen Sie die MST-Datei der Benutzeroberfläche zu diesem Gruppenrichtlinienobjekt hinzu.
5. Verteilen Sie die Gruppenrichtlinie.

HINWEIS: Weitere Informationen über Gruppenrichtlinien finden Sie in der Hilfe von Microsoft Windows. Verwenden Sie zum einfacheren und sicheren Testen und Bereitstellen der Gruppenrichtlinie in Ihrem Unternehmen den *Gruppenrichtlinienadministrator*.

Workflowserver installieren

Informationen zur Installation des Workflowservers finden Sie im *Workflow Automation Administrator Guide* (Administratorhandbuch zur Workflowautomatisierung).

DRA Reporting installieren

Für DRA Reporting müssen Sie die Datei „DRAReportingSetup.exe“ aus dem NetIQ DRA-Installationskit installieren.

Schritt	Details
Am Zielserver anmelden	Melden Sie sich zur Installation mit einem Konto mit lokalen Administratorrechten am Microsoft Windows-Zielserver an. Stellen Sie sicher, dass dieses Konto lokale Verwaltungsrechte und Domänenverwaltungsrechte und Systemadministratorrechte auf SQL Server hat.
NetIQ Administration-Installationskit kopieren und ausführen	Kopieren Sie das DRA-Installationskit „NetIQAdminINstallationKit.msi“ auf den Zielserver und führen Sie es aus, indem Sie auf die Datei doppelklicken oder das Programm über die Befehlszeile aufrufen. Das Installationskit extrahiert die DRA-Installationsmedien an einen anpassbaren Speicherort im lokalen Dateisystem. Zusätzlich installiert das Installationskit bei Bedarf .NET Framework auf dem Zielserver, um die Voraussetzungen für das DRA-Produktinstallationsprogramm zu erfüllen.
DRA Reporting-Installation ausführen	Navigieren Sie zum Speicherort, in dem die Installationsmedien extrahiert wurden, und führen Sie DRA`ReportingSetup.exe` aus, um die Verwaltungskomponente für die DRA-Berichterstellungsintegration zu installieren.

Schritt	Details
Voraussetzungen überprüfen und installieren	Im Dialogfeld **Voraussetzungen** wird die Liste der Software angezeigt, die für die zur Installation ausgewählten Komponenten erforderlich ist. Das Installationsprogramm führt Sie durch die Installation aller fehlenden Voraussetzungen, die zum erfolgreichen Abschließen der Installation erforderlich sind. Informationen über NetIQ Reporting Center finden Sie im *Reporting Center Guide* (Reporting Center-Handbuch) auf der Dokumentations-Website.
EULA-Lizenzvereinbarung akzeptieren	Akzeptieren Sie die Bedingungen der Endbenutzer-Lizenzvereinbarung, um die Installation abzuschließen.

5 Produktaufrüstung

Dieses Kapitel beschreibt eine Vorgehensweise, die Ihnen dabei hilft, eine verteilte Umgebung in kontrollierten Schritten aufzurüsten oder zu migrieren.

Die Angaben in diesem Kapitel basieren auf der Annahme, dass Ihre Umgebung mehrere Verwaltungsserver enthält und sich einige Server an Remotestandorten befinden. Dieses Art der Konfiguration wird als Multi-Master-Set (MMS) bezeichnet. Ein MMS besteht aus einem primären Verwaltungsserver und einem oder mehreren verknüpften, sekundären Verwaltungsservern. Weitere Informationen zur Funktionsweise von MMS finden Sie unter „Konfigurieren des Multi-Master-Sets“.

DRA-Aufrüstung planen

Führen Sie `NetIQAdminInstallationKit.msi` aus, um die DRA-Installationsmedien zu extrahieren, und installieren Sie das Systemdiagnose-Dienstprogramm und führen Sie es aus.

Planen Sie Ihre DRA-Bereitstellung, bevor Sie mit dem Aufrüstungsprozess beginnen. Beachten Sie beim Planen der Bereitstellung den folgenden Leitfaden:

- Testen Sie den Aufrüstungsprozess in einer Laborumgebung, bevor Sie die Aufrüstung in der Produktionsumgebung implementieren. Beim Testen können Sie unerwartete Probleme identifizieren und auflösen, ohne die Erledigung von Administrationsaufgaben zu beeinträchtigen, für die Sie verantwortlich sind.
- Lesen Sie Erforderliche Ports und Protokolle.
- Ermitteln Sie, wie viele Hilfsadministratoren jeweils auf ein MMS angewiesen sind. Wenn der Großteil Ihrer Hilfsadministratoren auf bestimmte Server oder Serversätze angewiesen ist, rüsten Sie diese Server zuerst außerhalb der Spitzenbetriebszeiten auf.
- Ermitteln Sie, welche Hilfsadministratoren die Delegierungs- und Konfigurationskonsole benötigen. Diese Informationen können Sie auf eine der folgenden Weisen ermitteln:
  - Überprüfen Sie, welche Hilfsadministratoren mit den integrierten Hilfsadministratorgruppen verknüpft sind.
  - Überprüfen Sie, welche Hilfsadministratoren mit den integrierten Aktivansichten verknüpft sind.
  - Erstellen Sie mithilfe von Directory and Resource Administrator Reporting Sicherheitsmodellberichte, wie die Aktivansichtberichte zu Hilfsadministratordetails oder Hilfsadministratorgruppen.

  Informieren Sie diese Hilfsadministratoren über Ihre Aufrüstungspläne für die Benutzeroberflächen.
- Ermitteln Sie, welche Hilfsadministratoren eine Verbindung zum primären Verwaltungsserver herstellen müssen. Diese Hilfsadministratoren sollten ihre Clientcomputer aufrüsten, nachdem Sie den primären Verwaltungsserver aufgerüstet haben.

  Informieren Sie diese Hilfsadministratoren über Ihre Aufrüstungspläne für die Verwaltungsserver und Benutzeroberflächen.

- Ermitteln Sie, ob Sie Delegierungs-, Konfigurations- oder Richtlinienänderungen implementieren müssen, bevor Sie mit dem Aufrüstungsprozess beginnen. Je nach Umgebung kann diese Entscheidung für jeden Standort einzeln getroffen werden.
- Koordinieren Sie die Aufrüstung der Clientcomputer und der Verwaltungsserver, um die Ausfallzeit möglichst gering zu halten. Beachten Sie, dass das gemeinsame Ausführen von früheren DRA-Versionen und der aktuellen DRA-Version auf dem gleichen Verwaltungsserver oder Clientcomputer nicht unterstützt wird.

WICHTIG

- Wenn in Ihrer früheren DRA-Version die Konto- und Ressourcenverwaltungskonsole installiert ist, wird diese Konsole während der Aufrüstung entfernt.
- Bei der Aufrüstung des DRA-Servers von DRA 9.x werden verwaltete Mandanten aus DRA entfernt. Wenn Sie diese Mandanten mit Azure weiterhin verwenden möchten, müssen Sie die Mandanten nach der Aufrüstung hinzufügen. Informationen·zum·Hinzufügen·von·Mandanten·finden·Sie·in·„Erstellen einer Azure-Anwendung und Hinzufügen eines Azure-Mandanten“.
- Weil Exchange 2010 in DRA 10 nicht unterstützt wird, wird Exchange bei der Aufrüstung von DRA 9.x deaktiviert. Um nach der Aufrüstung weiterhin Exchange-Vorgänge auszuführen, deaktivieren Sie die Option **Enable Exchange Policy** (Exchange-Richtlinie aktivieren) in der Delegierungs- und Konfigurationskonsole und aktivieren Sie die Option dann erneut. Beide Änderungen müssen „übernommen“ werden, um die Richtlinie zurückzusetzen.

  Informationen zu dieser Richtlinienkonfiguration finden Sie unter „Aktivieren von Microsoft Exchange“.

Aufgaben vor der Aufrüstung

Führen Sie vor dem Beginn einer Aufrüstungsinstallation die unten aufgeführten Voraufrüstungsschritte aus, um jeden Serversatz auf die Aufrüstung vorzubereiten.

Schritt	Details
AD LDS-Instanz sichern	Öffnen Sie das Systemdiagnose-Dienstprogramm und führen Sie die Prüfung **AD LDS-Instanzicherung** aus, um eine Sicherung der aktuellen AD LDS-Instanz zu erstellen.
Bereitstellungsplan erstellen	Erstellen Sie einen Bereitstellungsplan für die Aufrüstung der Verwaltungsserver und Benutzeroberflächen (Clientcomputer der Hilfsadministratoren). Weitere Informationen finden Sie unter DRA-Aufrüstung planen.
Dedizierten Sekundärserver zum Ausführen einer früheren DRA-Version festlegen	*Optional:* Legen Sie einen dedizierten, sekundären Verwaltungsserver fest, der eine frühere DRA-Version ausführt, während Sie einen Standort aufrüsten.
Erforderliche Änderungen für diesen MMS vornehmen	Nehmen Sie alle erforderlichen Änderungen an den Delegierungs-, Konfigurations- und Richtlinieneinstellungen für diesen MMS vor. Bearbeiten Sie diese Einstellungen mit dem primären Verwaltungsserver.

Schritt	Details
MMS synchronisieren	Synchronisieren Sie die Serversätze, sodass jeder Verwaltungsserver die neuesten Konfigurations- und Sicherheitseinstellungen hat.
Primärserver-Registrierung sichern	Sichern Sie die Registrierung des primären Verwaltungsservers. Wenn Sie über eine Sicherung der früheren Registrierungeinstellungen verfügen, können Sie die früheren Konfigurations- und Sicherheitseinstellungen mühelos wiederherstellen.
Gruppenverwaltetes Servicekonto in DRA-Benutzerkonto umwandeln	*Optional:* Wenn Sie ein gruppenverwaltetes Servicekonto als DRA-Servicekonto verwenden, ändern Sie das gruppenverwaltete Servicekonto vor der Aufrüstung in ein DRA-Benutzerkonto. Nach der Aufrüstung müssen Sie das Konto wieder in ein gruppenverwaltetes Servicekonto ändern.

HINWEIS: Wenn Sie die AD LDS-Instanz wiederherstellen müssen, gehen Sie folgendermaßen vor:

1. Stoppen Sie die aktuelle AD LDS-Instanz unter „Computerverwaltung“ > „Dienste“. Sie trägt einen anderen Titel: `NetIQDRASecureStoragexxxxx`.
2. Ersetzen Sie die **aktuelle Datei** `adamnts.dit` wie unten angegeben durch die **Sicherungsdatei** `adamnts.dit`:
   - Speicherort der aktuellen Datei: `%ProgramData%/NetIQ/DRA/<DRA-Instanzname>/data/`
   - Speicherort der Sicherungsdatei: `%ProgramData%/NetIQ/ADLDS/`
3. Starten Sie die AD LDS-Instanz neu.

Relevante Themen für vor der Aufrüstung:

- „Dedizierten lokalen Verwaltungsserver zum Ausführen einer früheren DRA-Version festlegen“, auf Seite 45
- „Serversatz mit früherer DRA-Version synchronisieren“, auf Seite 46
- „Registrierung des Verwaltungsservers sichern“, auf Seite 47

Dedizierten lokalen Verwaltungsserver zum Ausführen einer früheren DRA-Version festlegen

Wenn Sie einen oder mehrere dedizierte sekundäre Verwaltungsserver festlegen, die während der Aufrüstung eine frühere DRA-Version lokal am jeweiligen Standort ausführen, können Sie Ausfallzeiten und kostenaufwändige Verbindungen zu Remote-Standorten minimieren. Dieser Schritt ist optional und ermöglicht Hilfsadministratoren, während des gesamten Aufrüstungsprozesses mit einer früheren DRA-Version zu arbeiten, bis Sie die Bereitstellung fertiggestellt haben.

Erwägen Sie die Verwendung dieser Option, wenn eine oder mehrere der folgenden Aufrüstungsanforderungen auf Ihre Umgebung zutreffen:

- Ausfallzeit müssen verhindert oder minimiert werden.
- Sie müssen eine große Anzahl Hilfsadministratoren unterstützen und können nicht alle Clientcomputer gleichzeitig aufrüsten.

- Sie möchten nach dem Aufrüsten des primären Verwaltungsservers weiterhin den Zugriff auf eine frühere DRA-Version unterstützen.
- Ihre Umgebung enthält einen MMS, der mehrere Standorte umfasst.

Sie können einen neuen sekundären Verwaltungsserver installieren oder einen vorhandenen Sekundärserver verwenden, der eine frühere DRA-Version ausführt. Wenn Sie beabsichtigen, diesen Server aufzurüsten, sollten Sie diesen Server als letztes aufrüsten. Deinstallieren Sie andernfalls DRA komplett von diesem Server, nachdem Sie die Aufrüstung abgeschlossen haben.

Neuen Sekundärserver einrichten

Die Installation eines neuen Sekundärservers vor Ort kann dazu beitragen, kostenaufwändige Verbindungen zu Remotestandorten zu vermeiden, und gewährleistet, dass die Hilfsadministratoren mit der früheren DRA-Version ohne Unterbrechung weiterarbeiten können. Wenn die Umgebung einen MMS enthält, der mehrere Standorte umfasst, sollten Sie diese Option in Betracht ziehen. Wenn Ihr MMS beispielsweise einen primären Verwaltungsserver am Standort London und einen sekundären Verwaltungsserver am Standort Tokio umfasst, erwägen Sie die Installation eines Sekundärservers am Standort London, den Sie zum entsprechenden MMS hinzufügen. Die Hilfsadministratoren am Standort London können dann diesen zusätzlichen Server verwenden und so bis zum Fertigstellen der Aufrüstung mit einer früheren DRA-Version arbeiten.

Vorhandenen Sekundärserver verwenden

Sie können auch einen vorhandenen sekundären Verwaltungsserver als dedizierten Server für eine frühere DRA-Version verwenden. Wenn Sie beabsichtigen, einen sekundären Verwaltungsserver an einem bestimmten Standort nicht aufzurüsten, sollten Sie diese Option in Betracht ziehen. Wenn Sie keinen vorhandenen Sekundärserver als dedizierten Server festlegen können, erwägen Sie zu diesem Zweck die Installation eines neuen Verwaltungsservers. Wenn Sie einen oder mehrere Sekundärserver als dedizierten Server zum Ausführen einer früheren DRA-Version festlegen, können die Hilfsadministratoren bis zum Fertigstellen der Aufrüstung ohne Unterbrechung mit einer früheren DRA-Version weiterarbeiten. Diese Option eignet sich am besten in größeren Umgebungen, die ein zentralisiertes Verwaltungsmodell verwenden.

Serversatz mit früherer DRA-Version synchronisieren

Bevor Sie die Registrierung der früheren DRA-Version sichern oder den Aufrüstungsprozess starten, stellen Sie sicher, dass Sie die Serversätze synchronisiert haben, damit jeder Verwaltungsserver über die neuesten Konfigurations- und Sicherheitseinstellungen verfügt.

HINWEIS: Stellen Sie sicher, dass Sie alle erforderlichen Änderungen an den Delegierungs-, Konfigurations- und Richtlinieneinstellungen für diesen MMS vorgenommen haben. Bearbeiten Sie diese Einstellungen mit dem primären Verwaltungsserver. Nachdem Sie den primären Verwaltungsserver aufgerüstet haben, können Sie keine Delegierungs-, Konfigurations- oder Richtlinieneinstellungen mit Verwaltungsservern synchronisieren, die eine frühere DRA-Version ausführen.

So synchronisieren Sie einen vorhandenen Serversatz:

1. Melden Sie sich mit dem integrierten Admin-Konto beim primären Verwaltungsserver an.

2 Öffnen Sie die Delegierungs- und Konfigurationskonsole und erweitern Sie **Configuration Management** (Konfigurationsmanagement).

3 Klicken Sie auf **Administration Servers** (Verwaltungsserver).

4 Wählen Sie im rechten Bereich den entsprechenden primären Verwaltungsserver für diesen Serversatz aus.

5 Klicken Sie auf **Properties** (Eigenschaften).

6 Klicken Sie auf der Registerkarte für den Synchronisierungszeitplan auf **Refresh Now** (Jetzt aktualisieren).

7 Überprüfen Sie den erfolgreichen Abschluss der Synchronisierung und überprüfen Sie, ob alle sekundären Verwaltungsserver verfügbar sind.

Registrierung des Verwaltungsservers sichern

Wenn Sie eine Sicherung der Registrierung des Verwaltungsservers erstellen, können Sie frühere Konfigurationen wiederherstellen. Wenn Sie beispielsweise die aktuelle DRA-Version vollständig deinstallieren müssen und zur vorigen DRA-Version zurückkehren, können Sie mithilfe einer Sicherung der früheren Registrierungseinstellungen Ihre vorigen Konfigurations- und Sicherheitseinstellungen einfach wiederherstellen.

Gehen Sie jedoch mit Bedacht vor, wenn Sie die Registrierung bearbeiten. Fehler in der Registrierung können dazu führen, dass der Verwaltungsserver nicht wie erwartet funktioniert. Wenn während des Aufrüstungsprozesses ein Fehler auftritt, können Sie mithilfe der Sicherung der Registrierungseinstellungen die Registrierung wiederherstellen. Weitere Informationen finden Sie in der *Registrierungseditor-Hilfe*.

WICHTIG: Die DRA-Serverversion, der Name des Windows-Betriebssystems und die Konfiguration der verwalteten Domäne müssen beim Wiederherstellen der Registrierung identisch sein.

WICHTIG: Sichern Sie vor dem Aufrüsten das Windows-Betriebssystem des Computers, der als Host für DRA fungiert, oder erstellen Sie ein VM-Snapshot-Image der Maschine.

So sichern Sie die Registrierung des Verwaltungsservers:

1 Führen Sie `regedit.exe` aus.

2 Klicken Sie mit der rechten Maustaste auf den Knoten `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint` und wählen Sie **Exportieren** aus.

3 Geben Sie den Namen und den Speicherort der Datei zum Speichern des Registrierungsschlüssels an und klicken Sie auf **Speichern**.

DRA-Verwaltungsserver aufrüsten

Die folgende Checkliste leitet Sie durch den gesamten Aufrüstungsprozess. Rüsten Sie jeden Serversatz in Ihrer Umgebung gemäß diesem Prozess auf. Sofern noch nicht erfolgt, erstellen Sie mit dem Systemdiagnose-Dienstprogramm eine Sicherung der aktuellen AD-LDS-Instanz.

WARNUNG: Rüsten Sie die sekundären Verwaltungsserver erst auf, wenn Sie den primären Verwaltungsserver für dieses MMS aufgerüstet haben.

Sie können diesen Aufrüstungsprozess über mehrere Phasen verteilen und die einzelnen MMS nacheinander aufrüsten. Dieser Aufrüstungsprozess ermöglicht Ihnen außerdem das vorübergehende gleichzeitige Einschließen von Sekundärservern, die eine frühere DRA-Version ausführen, und von Sekundärservern, die die aktuelle DRA-Version ausführen, in den gleichen MMS. DRA unterstützt die Synchronisierung zwischen Verwaltungsservern, die eine frühere DRA-Version ausführen, und Servern, die die aktuelle DRA-Version ausführen. Beachten Sie jedoch, dass das gemeinsame Ausführen einer früheren DRA-Version und der aktuellen DRA-Version auf dem gleichen Verwaltungsserver oder Clientcomputer nicht unterstützt wird.

WICHTIG: Die DRA-Aufrüstungsinstallation nimmt die folgenden Änderungen vor, wenn der DRA-Server von DRA 9.x auf DRA 10.x aufgerüstet wird:

- Die Benutzerkonfigurationen für UCH und den Workflowautomatisierungsserver werden von der Webkonsole zur Delegierungs- und Konfigurationskonsole verschoben.
- Die alte Webkomponente wird vom Server entfernt.
- Verwaltete Mandanten werden entfernt.

  Informationen zum Hinzufügen von Mandanten finden Sie unter „Mandanten verwalten“.
- Wenn Sie die Konto- und Ressourcenverwaltungskonsole in einer früheren Version installiert haben und auf DRA 10.x aufrüsten, wird die Konto- und Ressourcenverwaltungskonsole entfernt.
- Während einer MMS-Aufrüstung wird zuerst der Primärserver aufgerüstet und anschließend die Sekundärserver. Zur erfolgreichen Reproduktion der temporären Gruppenzuweisungen auf dem Sekundärserver führen Sie den **Multi-Master-Synchronisierungszeitplan** manuell aus oder warten Sie auf die geplante Ausführung.
- Weil Exchange 2010 in DRA 10 nicht unterstützt wird, wird Exchange bei der Aufrüstung von DRA 9.x deaktiviert. Um nach der Aufrüstung weiterhin Exchange-Vorgänge auszuführen, deaktivieren Sie die Option **Enable Exchange Policy** (Exchange-Richtlinie aktivieren) in der Delegierungs- und Konfigurationskonsole und aktivieren Sie die Option dann erneut. Beide Änderungen müssen „übernommen“ werden, um die Richtlinie zurückzusetzen.

  Informationen zu dieser Richtlinienkonfiguration finden Sie unter *Enabling Microsoft Exchange* (Aktivieren von Microsoft Exchange).

Schritt	Details
Systemdiagnose-Dienstprogramm ausführen	Installieren Sie das eigenständige DRA-Systemdiagnose-Dienstprogramm und führen Sie es mit einem Servicekonto aus. Beheben Sie etwaige Probleme.
Testaufrüstung ausführen	Führen Sie eine Testaufrüstung in der Laborumgebung aus, um mögliche Probleme zu identifizieren und die Ausfallzeit zu minimieren.
Aufrüstsreihenfolge ermitteln	Legen Sie die Reihenfolge fest, in der Sie die Serversätze aufrüsten möchten.
MMS für die Aufrüstung vorbereiten	Bereiten Sie jeden MMS für die Aufrüstung vor. Weitere Informationen finden Sie unter Aufgaben vor der Aufrüstung.

Schritt	Details
Primärserver aufrüsten	Rüsten Sie den primären Verwaltungsserver im entsprechenden MMS auf. Informationen hierzu erhalten Sie unter Primären Verwaltungsserver aufrüsten.
Neuen Sekundärserver installieren	*(Optional)* Installieren Sie einen lokalen sekundären Verwaltungsserver, der die neueste DRA-Version ausführt, um Ausfallzeiten an Remotestandorten zu vermeiden. Informationen hierzu erhalten Sie unter Lokalen sekundären Verwaltungsserver für die aktuelle DRA-Version installieren.
Benutzeroberflächen bereitstellen	Stellen Sie die Benutzeroberflächen für die Hilfsadministratoren bereit. Informationen hierzu erhalten Sie unter DRA-Benutzeroberflächen aufrüsten.
Sekundärserver aufrüsten	Rüsten Sie die sekundären Verwaltungsserver im MMS auf. Informationen hierzu erhalten Sie unter Sekundäre Verwaltungsserver aufrüsten.
DRA Reporting aufrüsten	Rüsten Sie DRA Reporting auf. Informationen hierzu erhalten Sie unter Reporting aufrüsten.
Systemdiagnose-Dienstprogramm ausführen	Führen Sie das Systemdiagnose-Dienstprogramm aus, das im Rahmen der Aufrüstung installiert wurde. Beheben Sie etwaige Probleme.
Azure-Mandanten hinzufügen *(nach der Aufrüstung)*	(*Optional, nach der Aufrüstung)* Wenn Sie vor der Aufrüstung Azure-Mandanten verwaltet haben, werden die Mandanten während der Aufrüstung entfernt. Sie müssen diese Mandanten neu hinzufügen und in der Delegierungs- und Konfigurationskonsole eine vollständige Aktualisierung des Konto-Cache ausführen. Weitere Informationen finden Sie unter „Mandanten verwalten“.

Themen zur Serveraufrüstung:

- „Primären Verwaltungsserver aufrüsten“, auf Seite 49
- „Lokalen sekundären Verwaltungsserver für die aktuelle DRA-Version installieren“, auf Seite 50
- „DRA-Benutzeroberflächen aufrüsten“, auf Seite 50
- „Sekundäre Verwaltungsserver aufrüsten“, auf Seite 51

Primären Verwaltungsserver aufrüsten

Nachdem Sie den MMS erfolgreich vorbereitet haben, rüsten Sie den primären Verwaltungsserver auf. Rüsten Sie keine Benutzeroberflächen auf den Clientcomputern auf, solange die Aufrüstung des primären Verwaltungsservers noch nicht abgeschlossen ist. Weitere Informationen finden Sie unter DRA-Benutzeroberflächen aufrüsten.

HINWEIS: Weitere Informationen zu Erwägungen und Anweisungen für die Aufrüstung finden Sie in den *Directory Resource Administrator Release Notes* (Versionshinweise zu Directory Resource Administrator).

Informieren Sie vor dem Beginn der Aufrüstung die Hilfsadministratoren über den geplanten Start des Prozesses. Wenn Sie einen dedizierten sekundären Verwaltungsserver zum Ausführen einer früheren DRA-Version festgelegt haben, identifizieren Sie außerdem diesen Server, damit die Hilfsadministratoren während der Aufrüstung mit der früheren DRA-Version weiterarbeiten können.

HINWEIS: Nachdem Sie den primären Verwaltungsserver aufgerüstet haben, können Sie keine Delegierungs-, Konfigurations- oder Richtlinieneinstellungen von diesem Server mit sekundären Verwaltungsservern synchronisieren, die eine frühere DRA-Version ausführen.

Lokalen sekundären Verwaltungsserver für die aktuelle DRA-Version installieren

Durch das Installieren eines neuen sekundären Verwaltungsservers zum Ausführen der aktuellen DRA-Version am lokalen Standort können Sie kostenaufwändige Verbindungen zu Remotestandorten minimieren, Ausfallzeiten reduzieren und eine schnellere Bereitstellung der Benutzeroberflächen ermöglichen. Dieser Schritt ist optional und ermöglicht Hilfsadministratoren, während des gesamten Aufrüstungsprozesses sowohl mit der aktuellen DRA-Version als auch mit einer früheren DRA-Version zu arbeiten, bis Sie die Bereitstellung fertiggestellt haben.

Erwägen Sie die Verwendung dieser Option, wenn eine oder mehrere der folgenden Aufrüstungsanforderungen auf Ihre Umgebung zutreffen:

- Ausfallzeit müssen verhindert oder minimiert werden.
- Sie müssen eine große Anzahl Hilfsadministratoren unterstützen und können nicht alle Clientcomputer gleichzeitig aufrüsten.
- Sie möchten nach dem Aufrüsten des primären Verwaltungsservers weiterhin den Zugriff auf eine frühere DRA-Version unterstützen.
- Ihre Umgebung enthält einen MMS, der mehrere Standorte umfasst.

Wenn Ihr MMS beispielsweise einen primären Verwaltungsserver am Standort London und einen sekundären Verwaltungsserver am Standort Tokio umfasst, erwägen Sie die Installation eines Sekundärservers am Standort Tokio, den Sie zum entsprechenden MMS hinzufügen. Dieser zusätzliche Server ermöglicht einen besseren Ausgleich der täglichen Verwaltungsarbeitslast am Standort Tokio. Außerdem können Hilfsadministratoren beider Standorte bis zum Fertigstellen der Aufrüstung wahlweise mit einer früheren DRA-Version oder mit der aktuellen DRA-Version arbeiten. Des Weiteren sind die Hilfsadministratoren nicht mit Ausfallzeiten konfrontiert, weil Sie die Benutzeroberflächen mit der aktuellen DRA-Version sofort bereitstellen können. Weitere Informationen zum Aufrüstung der Benutzeroberflächen finden Sie in DRA-Benutzeroberflächen aufrüsten.

DRA-Benutzeroberflächen aufrüsten

Typischerweise sollten Sie die Benutzeroberflächen mit der aktuellen DRA-Version bereitstellen, nachdem Sie den primären Verwaltungsserver und einen sekundären Verwaltungsserver aufgerüstet haben. Rüsten Sie jedoch zuerst die Clientcomputer der Hilfsadministratoren auf, die den primären Verwaltungsserver verwenden müssen, indem Sie die Delegierungs- und Konfigurationskonsole installieren. Weitere Informationen finden Sie unter DRA-Aufrüstung planen.

Wenn Sie oft Stapelverarbeitungen über die Befehlszeilenschnittstelle, den ADSI-Anbieter oder PowerShell ausführen oder oft Berichte generieren, erwägen Sie die Installation dieser Benutzeroberflächen auf einem dedizierten sekundären Verwaltungsserver, um einen angemessenen Lastausgleich im MMS zu gewährleisten.

Sie können die DRA-Benutzeroberflächen von den Hilfsadministratoren installieren lassen oder diese Benutzeroberflächen über eine Gruppenrichtlinie bereitstellen. Sie können außerdem die Webkonsole schnell und einfach für mehrere Hilfsadministratoren bereitstellen.

HINWEIS: Es ist nicht möglich, mehrere Versionen von DRA-Komponenten nebeneinander auf dem gleichen DRA-Server auszuführen. Wenn Sie beabsichtigen, die Clientcomputer der Hilfsadministratoren in mehreren Phasen aufzurüsten, erwägen Sie die Bereitstellung der Webkonsole, um den sofortigen Zugriff auf einen Verwaltungsserver mit der aktuellen DRA-Version zu ermöglichen.

Sekundäre Verwaltungsserver aufrüsten

Beim Aufrüsten von sekundären Verwaltungsservern können Sie jeden Server je nach Bedarf und Verwaltungsanforderungen aufrüsten. Berücksichtigen Sie dabei auch, wie Sie die Aufrüstung und Bereitstellung der DRA-Benutzeroberflächen geplant haben. Weitere Informationen finden Sie unter DRA-Benutzeroberflächen aufrüsten.

Ein typischer Aufrüstungspfad kann beispielsweise die folgenden Schritte umfassen:

1. Rüsten Sie einen sekundären Verwaltungsserver auf.
2. Weisen Sie die Hilfsadministratoren, die diesen Server verwenden, an, die geeigneten Benutzeroberflächen zu installieren, zum Beispiel die Webkonsole.
3. Wiederholen Sie die oben genannten Schritte 1 und 2, bis das gesamte MMS aufgerüstet ist.

Informieren Sie vor dem Beginn der Aufrüstung die Hilfsadministratoren über den geplanten Start des Prozesses. Wenn Sie einen dedizierten sekundären Verwaltungsserver zum Ausführen einer früheren DRA-Version festgelegt haben, identifizieren Sie außerdem diesen Server, damit die Hilfsadministratoren während der Aufrüstung mit der früheren DRA-Version weiterarbeiten können. Nachdem Sie den Aufrüstungsprozess für dieses MMS fertiggestellt haben und alle Clientcomputer der Hilfsadministratoren aufgerüstete Benutzeroberflächen ausführen, versetzen Sie alle verbleibenden Server mit früheren DRA-Versionen in den Offlinezustand.

Reporting aufrüsten

Bevor Sie die DRA-Berichterstellung aufrüsten, stellen Sie sicher, dass Ihre Umgebung die Mindestanforderungen für NRC 3.2 erfüllt. Weitere Informationen zu den Installationsanforderungen und Überlegungen zur Aufrüstung finden Sie im *NetIQ Reporting Center Reporting Guide* (NetIQ Reporting Center-Berichterstellungshandbuch).

Schritt	Details
Unterstützung für die DRA-Berichterstellung deaktivieren	Um sicherzustellen, dass die Berichterstellungskollektoren nicht während des Aufrüstungsprozesses ausgeführt werden, deaktivieren Sie die Unterstützung für die DRA-Berichterstellung in der Delegierungs- und Konfigurationskonsole im Fenster zur Konfiguration des Berichterstellungsservices.
Mit dem entsprechenden Berechtigungsnachweis am SQL-Instanzserver anmelden	Melden Sie sich mit einem Administratorkonto am Microsoft Windows-Server an, auf dem Sie die SQL-Instanz für die Berichterstellungsdatenbanken installiert haben. Stellen Sie sicher, dass dieses Konto lokale Verwaltungsrechte und Systemadministratorrechte auf SQL Server hat.

Schritt	Details
Setup-Programm der DRA-Berichterstellung ausführen	Führen Sie DRA`ReportingSetup.exe` aus dem Installationskit aus und befolgen Sie die Anweisungen im Installationsassistenten.
Unterstützung für DRA-Berichterstellung aktivieren	Aktivieren Sie auf dem primären Verwaltungsserver die Berichterstellung in der Delegierungs- und Konfigurationskonsole.

Wenn Ihre Umgebung die SSRS-Integration verwendet, müssen Sie die Berichte erneut bereitstellen. Weitere Informationen über die erneute Bereitstellung von Berichten finden Sie im *Reporting Center Guide* (Reporting Center-Handbuch) auf der Dokumentations-Website.

III Komponenten- und Prozesskonfiguration

Dieses Kapitel enthält Informationen zur erstmaligen Konfiguration von DRA, einschließlich Server und Serveranpassungen, Konsolen und Konsolenanpassung, Azure-Verwaltung, die Verwaltung öffentlicher Ordner und das Herstellen einer Verbindung zu den Servern.

6 Anfängliche Konfiguration

Dieser Abschnitt beschreibt die erforderlichen Konfigurationsschritte für die Erstinstallation von Directory and Resource Administrator.

Konfigurationscheckliste

Verwenden Sie die folgende Checkliste zur Konfiguration von DRA für die erstmalige Verwendung.

Schritt	Details
DRA-Lizenz installieren	Wenden Sie mithilfe des Systemdiagnose-Dienstprogramms eine DRA-Lizenz an. Weitere Informationen zu DRA-Lizenzen finden Sie in Lizenzierungsanforderungen.
DRA-Server und -Funktionen konfigurieren	Konfigurieren Sie MMS, Ausnahmen für das Klonen, Dateireproduktion, Ereignisstempel, Caching, AD LDS, dynamische Gruppen, den Papierkorb, die Berichterstellung, den Unified-Änderungsverlauf (UCH, Unified Change History) und den Workflowserver.
Delegierungs- und Konfigurationsclient konfigurieren	Konfigurieren Sie, wie im Konfigurations- und Delegierungsclient auf Elemente zugegriffen wird und wie diese Elemente dort angezeigt werden.
Webclient konfigurieren	Konfigurieren Sie die automatische Abmeldung, Zertifikate, Serververbindungen und Authentifizierungskomponenten.

Installieren oder Aufrüsten von Lizenzen

Für DRA ist eine Lizenzschlüsseldatei erforderlich. Diese Datei enthält Ihre Lizenzinformationen und wird auf dem Verwaltungsserver installiert. Nachdem Sie den Verwaltungsserver installiert haben, installieren Sie mit dem Systemdiagnose-Dienstprogramm Ihre gekaufte Lizenz. Mit dem Installationspaket wird außerdem ein Probelizenzschlüssel (`TrialLicense.lic`) bereitgestellt, mit dem Sie bei Bedarf 30 Tage lang eine unbegrenzte Anzahl an Benutzerkonten und Postfächern verwalten können.

Um eine vorhandene Lizenz oder Probelizenz aufzurüsten, öffnen Sie die Delegierungs- und Konfigurationskonsole und wechseln Sie zu **Configuration Management** (Konfigurationsmanagement) > **Update License** (Lizenz aktualisieren). Wenn Sie Ihre Lizenz aufrüsten, rüsten Sie die Lizenzdatei auf jedem Verwaltungsserver auf.

Sie können Ihre Produktlizenz in der Delegierungs- und Konfigurationskonsole anzeigen. Navigieren Sie zum Anzeigen der Produktlizenz zum Menü **Datei** > **DRA Properties** (DRA-Eigenschaften) > **License** (Lizenz).

DRA-Server und -Funktionen konfigurieren

Zum Verwalten des Zugriffs auf Active Directory-Aufgaben mit den niedrigsten Berechtigungen in DRA müssen zahlreiche Komponenten und Prozesse konfiguriert werden. Dies umfasst die Konfiguration allgemeiner Komponenten und von Clientkomponenten. Dieser Abschnitt bietet Informationen zu den allgemeinen Komponenten und Prozessen, die für DRA konfiguriert werden müssen.

Konfigurieren des Multi-Master-Sets

In einer MMS-Umgebung werden mehrere Verwaltungsserver zur Verwaltung des gleichen Satzes an Domänen und Mitgliedsservern verwendet. Ein MMS besteht aus einem primären Verwaltungsserver und mehreren sekundären Verwaltungsservern.

Der Standardmodus für den Verwaltungsserver ist der Primärmodus. Beachten Sie beim Hinzufügen von Sekundärservern zur MMS-Umgebung, dass ein sekundärer Verwaltungsserver nur zu einem Serversatz gehören kann.

Um sicherzustellen, dass jeder Server im Satz die gleichen Daten verwaltet, synchronisieren Sie die Sekundärserver regelmäßig mit dem primären Verwaltungsserver. Um die Wartung zu reduzieren, verwenden Sie das gleiche Servicekonto für alle Verwaltungsserver in der Gesamtstruktur der Domäne.

WICHTIG

- Wählen Sie bei der Installation des Sekundärservers **Secondary Administration Server** (Sekundärer Verwaltungsserver) im Installationsprogramm aus.
- Die DRA-Version des neuen Sekundärservers muss der Version des DRA-Primärservers entsprechen, damit alle Funktionen des Primärservers auf dem Sekundärserver verfügbar sind.

Sekundären Verwaltungsserver hinzufügen

Im Delegierungs- und Konfigurationsclient können Sie einen sekundären Verwaltungsserver zu einem vorhandenen MMS hinzufügen. Um einen Sekundärserver hinzuzufügen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse.

HINWEIS: Um einen neuen Sekundärserver erfolgreich hinzuzufügen, installieren Sie zunächst das Directory and Resource Administrator-Produkt auf dem Verwaltungsservercomputer. Weitere Informationen finden Sie unter DRA-Verwaltungsserver installieren.

Um einen sekundären Verwaltungsserver hinzuzufügen, klicken Sie mit der rechten Maustaste im Konfigurationsmanagementknoten auf **Administration Server** (Verwaltungsserver) und wählen Sie **Add Secondary Server** (Sekundärserver hinzufügen).

Sekundären Verwaltungsserver hochstufen

Sie können einen sekundären Verwaltungsserver auf einen primären Verwaltungsserver hochstufen. Wenn Sie einen sekundären Verwaltungsserver auf einen primären Verwaltungsserver hochstufen, wird der ursprüngliche primäre Verwaltungsserver in einen sekundären Verwaltungsserver im Serversatz umgewandelt. Um einen sekundären Verwaltungsserver hochzustufen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse. Bevor Sie einen sekundären Verwaltungsserver hochstufen, synchronisieren Sie den MMS, um die neueste Konfiguration zu übernehmen.

Weitere Informationen über das Synchronisieren des MMS finden Sie in Synchronisierung planen.

HINWEIS: Ein neu hochgestufter Primärserver kann nur Verbindungen zu Sekundärservern herstellen, die während des Hochstufungsprozesses verfügbar waren. Wenn ein Sekundärserver während des Hochstufens unverfügbar geworden ist, wenden Sie sich an den technischen Support.

So stufen Sie einen sekundären Verwaltungsserver hoch:

1. Navigieren Sie zum Knoten **Configuration Management** (Konfigurationsmanagement) >**Administration Servers** (Verwaltungsserver).

2 Wählen Sie im rechten Bereich den sekundären Verwaltungsserver aus, den Sie hochstufen möchten.

3 Klicken Sie im Aufgabenmenü auf **Advanced** (Erweitert) > **Promote Server** (Server hochstufen).

WICHTIG: Wenn das Servicekonto des Sekundärservers vom Primärserver abweicht oder der Sekundärserver in einer anderen Domäne als der Primärserver installiert ist (verbürgte/nicht verbürgte Domänen) und Sie den Sekundärserver hochstufen, stellen Sie sicher, dass Sie vor dem Hochstufen des Sekundärservers die folgenden Rollen delegieren: **Audit All Objects** (Alle Objekte überwachen), **Configure Servers and Domains** (Server und Domänen konfigurieren) und **Generate UI Reports** (Benutzeroberflächenberichte generieren). Überprüfen Sie dann, ob die MMS-Synchronisierung erfolgreich war.

Primären Verwaltungsserver herabstufen

Sie können einen primären Verwaltungsserver auf einen sekundären Verwaltungsserver herabstufen. Um einen primären Verwaltungsserver herabzustufen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse.

So stufen Sie einen primären Verwaltungsserver herab:

1 Navigieren Sie zum Knoten **Configuration Management** (Konfigurationsmanagement) >**Administration Servers** (Verwaltungsserver).

2 Wählen Sie im rechten Bereich den primären Verwaltungsserver aus, den Sie herabstufen möchten.

3 Klicken Sie im Aufgabenmenü auf **Advanced** (Erweitert) > **Demote Server** (Server herabstufen).

4 Geben Sie den Computer an, der als neuer primärer Verwaltungsserver dienen soll, und klicken Sie auf **OK**.

Synchronisierung planen

Die Synchronisierung gewährleistet, dass alle Verwaltungsserver im MMS die gleichen Konfigurationsdaten verwenden. Sie können die Server jederzeit manuell synchronisieren, aber der standardmäßige Zeitplan ist auf eine Synchronisierung des MMS alle 4 Stunden festgelegt. Sie können diesen Zeitplan ändern, um ihn an die besonderen Anforderungen Ihres Unternehmens anzupassen.

Um den Synchronisierungszeitplan zu ändern oder MMS-Server manuell zu synchronisieren, müssen Sie über geeignete Befugnisse verfügen, beispielsweise über die Befugnisse, die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthalten sind.

Um auf den Synchronisierungszeitplan zuzugreifen oder eine manuelle Synchronisierung auszuführen, navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Administration Servers** (Verwaltungsserver) und verwenden Sie das Menü **Tasks** (Aufgaben) oder die Optionen im Kontextmenü des ausgewählten Servers. Der Synchronisierungszeitplan ist in den Eigenschaften eines ausgewählten Servers enthalten.

Grundlegende Informationen zu den Synchronisierungsoptionen

Es gibt im Wesentlichen vier unterschiedliche Optionen zum Synchronisieren von MMS-Servern:

- Den Primärserver auswählen und alle Sekundärserver mit „Synchronize All Servers“ (Alle Server synchronisieren) synchronisieren
- Einen Sekundärserver auswählen und nur diesen Server synchronisieren
- Den Synchronisierungszeitplan für Primär- und Sekundärserver unabhängig voneinander konfigurieren
- Den Synchronisierungszeitplan für alle Server konfigurieren. Diese Option ist aktiviert, wenn die folgende Einstellung im Synchronisierungszeitplan des Primärservers ausgewählt ist:

  Configure secondary Administration servers when refreshing the primary Administration server (Sekundäre Verwaltungsserver konfigurieren, wenn primärer Verwaltungsserver aktualisiert wird)

  HINWEIS: Wenn Sie diese Option deaktivieren, werden die Konfigurationsdateien gemäß Zeitplan des Primärservers zu den Sekundärservern kopiert, zu diesem Zeitpunkt aber nicht auf dem Sekundärserver geladen. Sie werden auf dem Sekundärserver gemäß dem für den Sekundärserver konfigurierten Zeitplan geladen. Dies ist hilfreich, wenn sich die Server in unterschiedlichen Zeitzonen befinden. Beispielsweise können Sie konfigurieren, dass alle Server ihre Konfiguration mitten in der Nacht aktualisieren, auch wenn dies je nach Zeitzone nicht gleichzeitig erfolgt.

Verwalten von Klonausnahmen

Über Klonausnahmen können Sie Eigenschaften für Benutzer, Gruppen, Kontakte und Computer definieren, die beim Klonen dieser Objekte nicht kopiert werden sollen.

Wenn Sie über die entsprechenden Befugnisse verfügen, können Sie Klonausnahmen verwalten. Die Rolle „Manage Clone Exceptions“ (Klonausnahmen verwalten) gewährt die Befugnisse zum Anzeigen, Erstellen und Löschen von Klonausnahmen.

Um eine vorhandene Klonausnahme anzuzeigen oder zu löschen oder um eine neue Klonausnahme zu erstellen, navigieren Sie zu **Configuration Management** (Konfigurationsmanagement> **Clone Exceptions** (Klonausnahmen) > **Tasks** (Aufgaben) oder öffnen Sie das Kontextmenü.

Dateireproduktion

Wenn Sie benutzerdefinierte Tools erstellen, müssen Sie möglicherweise unterstützende Dateien installieren, die das benutzerdefinierte Tool auf dem Computer mit der Delegierungs- und Konfigurationskonsole von DRA verwendet, damit es ausgeführt werden kann. Mit den Dateireproduktionsfunktionen von DRA können Sie Unterstützungsdateien für benutzerdefinierte Tools schnell und einfach vom primären Verwaltungsserver auf sekundäre Verwaltungsserver im MMS und auf DRA-Clientcomputer reproduzieren. Die Dateireproduktion kann auch zum Reproduzieren von Auslöserskripten vom Primär- auf Sekundärserver verwendet werden.

Sie können benutzerdefinierte Tools und die Dateireproduktion zusammen verwenden, um sicherzustellen, dass DRA-Clientcomputer auf Dateien benutzerdefinierter Tools zugreifen können. DRA reproduziert Dateien benutzerdefinierter Tools zu sekundären Verwaltungsservern, um sicherzustellen, dass DRA-Clientcomputer, die eine Verbindung zu sekundären Verwaltungsservern herstellen, auf die benutzerdefinierten Tools zugreifen können.

DRA reproduziert die Dateien benutzerdefinierter Tools während des MMS-Synchronisierungsprozesses vom primären Verwaltungsserver zu den sekundären Verwaltungsservern. Wenn die DRA-Clientcomputer eine Verbindung zu den Verwaltungsservern herstellen, lädt DRA die Dateien benutzerdefinierter Tools auf die DRA-Clientcomputer herunter.

HINWEIS: DRA lädt die Dateien des benutzerdefinierten Tools zum folgenden Speicherort auf den DRA-Clientcomputern herunter:

{DRA-Installationsverzeichnis}\{MMS-ID}\Download

„MMS-ID“ steht für die ID des Multi-Master-Sets, von dem DRA die Dateien für das benutzerdefinierte Tool herunterlädt.

Dateien für benutzerdefinierte Tools zur Reproduktion hochladen

Wenn Sie Dateien auf den primären Verwaltungsserver hochladen, legen Sie fest, welche Dateien Sie hochladen und zwischen dem primären Verwaltungsserver und allen sekundären Verwaltungsservern im MMS reproduzieren möchten. Mit DRA können Sie Bibliothekdateien, Skriptdateien und ausführbare Dateien hochladen.

Mit der Rolle „Replicate Files“ (Dateien reproduzieren) können Sie Dateien vom primären Verwaltungsserver zu den sekundären Verwaltungsservern im MMS und zu DRA-Clientcomputern reproduzieren. Die Rolle „Replicate Files“ (Dateien reproduzieren) umfasst die folgenden Befugnisse:

- **Dateien vom Server löschen:** Mit dieser Befugnis kann DRA Dateien löschen, die auf dem primären Verwaltungsserver, auf den sekundären Verwaltungsservern und auf den DRA-Clientcomputern nicht mehr vorhanden sind.
- **Dateiinformationen festlegen:** Mit dieser Befugnis kann DRA Dateiinformationen für Dateien auf den sekundären Verwaltungsservern aktualisieren.
- **Dateien auf Server hochladen:** Mit dieser Befugnis kann DRA Dateien vom DRA-Clientcomputer auf den primären Verwaltungsserver hochladen.

HINWEIS: Sie können immer nur eine Datei gleichzeitig über die Benutzeroberfläche zur Dateireproduktion in der Delegierungs- und Konfigurationskonsole hochladen.

So laden Sie eine Datei eines benutzerdefinierten Tools zum primären Verwaltungsserver hoch:

1. Navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **File Replication** (Dateireproduktion).
2. Klicken Sie im Aufgabenmenü auf **Upload File** (Datei hochladen).
3. Um eine Datei, die Sie hochladen möchten, zu suchen und auszuwählen, klicken Sie auf **Browse** (Durchsuchen).
4. *Wenn Sie die ausgewählte Datei auf alle DRA-Clientcomputer herunterladen möchten*, aktivieren Sie das Kontrollkästchen **Download to all client computers** (Auf alle Clientcomputer herunterladen).
5. *Wenn Sie eine COM-Bibliothek registrieren möchten*, aktivieren Sie das Kontrollkästchen **Register COM library** (COM-Bibliothek registrieren).
6. Klicken Sie auf **OK**.

HINWEIS

- DRA lädt die Skriptdatei bzw. die unterstützenden Dateien, die auf andere sekundäre Verwaltungsserver reproduziert werden müssen, in den Ordner *{DRA-Installationsverzeichnis}*\FileTransfer\Replicate auf dem primären Verwaltungsserver hoch. Auf den Ordner *{DRA-Installationsverzeichnis}*\FileTransfer\Replicate wird auch mit *{DRA_Pfad_für_reproduzierte_Dateien}* verwiesen.
- DRA lädt die Skriptdatei bzw. die unterstützenden Dateien, die auf DRA-Clientcomputer reproduziert werden müssen, in den Ordner *{DRA-Installationsverzeichnis}*\FileTransfer\Download auf dem primären Verwaltungsserver hoch.
- Die Datei für das benutzerdefinierte Tool, die auf den primären Verwaltungsserver hochgeladen wird, wird bei der nächsten geplanten Synchronisierung oder durch eine manuelle Synchronisierung an die sekundären Verwaltungsserver verteilt.

Mehrere Dateien zwischen Verwaltungsservern reproduzieren

Wenn Sie mehrere Dateien hochladen und zwischen dem primären Verwaltungsserver und den sekundären Verwaltungsservern im MMS reproduzieren möchten, können Sie die Dateien manuell zur Reproduktion hochladen, indem Sie sie in das Reproduktionsverzeichnis des primären Verwaltungsservers kopieren. Dies befindet sich an folgendem Speicherort:

{DRAInstallDir}\FileTransfer\Replicate

Das Reproduktionsverzeichnis wird bei der Installation von DRA erstellt.

Der Verwaltungsserver identifiziert automatisch die Dateien im Reproduktionsverzeichnis und reproduziert die Dateien zwischen den Verwaltungsservern während der nächsten planmäßigen Synchronisierung. Nach der Synchronisierung zeigt DRA die hochgeladenen Dateien im Fenster „File Replication“ (Dateireproduktion) in der Delegierungs- und Konfigurationskonsole an.

HINWEIS: Wenn Sie Dateien reproduzieren möchten, die COM-Bibliotheken enthalten, die registriert werden müssen, können Sie die Dateien nicht manuell in das Reproduktionsverzeichnis des Verwaltungsservers kopieren. Stattdessen müssen Sie die Dateien mit der Delegierungs- und Konfigurationskonsole hochladen und die COM-Bibliothek registrieren.

Mehrere Dateien auf DRA-Clientcomputer reproduzieren

Wenn Sie mehrere Dateien zwischen dem primären Verwaltungsserver und DRA-Clientcomputern reproduzieren möchten, können Sie die Dateien in das Client-Reproduktionsverzeichnis auf dem primären Verwaltungsserver kopieren. Es befindet sich an folgendem Speicherort:

{DRAInstallDir}\FileTransfer\Download

Das Client-Reproduktionsverzeichnis wird bei der Installation von DRA erstellt.

Der Verwaltungsserver identifiziert automatisch die Dateien im Download-Ordner und reproduziert die Dateien während der nächsten planmäßigen Synchronisierung auf die sekundären Verwaltungsserver. Nach der Synchronisierung zeigt DRA die hochgeladenen Dateien im Fenster

„File Replication“ (Dateireproduktion) in der Delegierungs- und Konfigurationskonsole an. DRA lädt die reproduzierten Dateien auf die DRA-Clientcomputer herunter, wenn die DRA-Clientcomputer nach der Reproduktion zum ersten Mal eine Verbindung zu den Verwaltungsservern herstellen.

HINWEIS: Wenn Sie Dateien reproduzieren möchten, die COM-Bibliotheken enthalten, die registriert werden müssen, können Sie die Dateien nicht in das Downloadverzeichnis des Verwaltungsservers kopieren. Stattdessen müssen Sie die Dateien mit der Delegierungs- und Konfigurationskonsole hochladen und die COM-Bibliothek registrieren.

Ereignisstempel

Wenn die AD Domain Services-Überwachung aktiviert ist, werden DRA-Ereignisse als vom DRA-Servicekonto oder vom Domänenzugriffskonto generiert protokolliert, sofern eines dieser Konten konfiguriert ist. Ereignisstempel erweitern diese Funktion und generieren ein zusätzliches AD DS-Ereignis, das den Hilfsadministrator identifiziert, der den Vorgang ausgeführt hat.

Damit diese Ereignisse generiert werden, müssen Sie die AD DS-Überwachung konfigurieren und Ereignisstempel auf dem DRA-Verwaltungsserver aktivieren. Wenn Ereignisstempel aktiviert sind, können Sie die von den Hilfsadministratoren vorgenommenen Änderungen in den Change Guardian-Ereignisberichten anzeigen.

- Informationen zur Konfiguration der AD DS-Überwachung finden Sie in der Microsoft-Referenz *AD DS Auditing Step-by-Step Guide* (Schritt-für-Schritt-Handbuch für die AD DS-Überwachung).
- Informationen zur Konfiguration der Change Guardian-Integration finden Sie in Server für Unified-Änderungsverlauf (UCH) konfigurieren.
- Um Ereignisstempel zu aktivieren, öffnen Sie die Delegierungs- und Konfigurationskonsole als DRA-Administrator und führen Sie die folgenden Schritte aus:
  1. Navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Update Administration Server Options** (Verwaltungsserveroptionen aktualisieren) > **Event Stamping** (Ereignisstempel).
  2. Wählen Sie einen Objekttyp aus und klicken Sie auf **Update** (Aktualisieren).
  3. Wählen Sie ein Attribut aus, das für die Ereignisstempel dieses Objekttyps verwendet werden soll.

     Aktuell unterstützt DRA Ereignisstempel für Benutzer, Gruppen, Kontakte, Computer und organisatorische Einheiten.

     DRA erfordert außerdem, dass die Attribute im AD-Schema für alle verwalteten Domänen vorhanden sind. Dies muss beachtet werden, wenn verwaltete Domänen nach dem Konfigurieren von Ereignisstempeln hinzugefügt werden. Wenn Sie eine verwaltete Domäne hinzufügen, die ein ausgewähltes Attribut nicht enthält, können die Vorgänge in dieser Domäne nicht anhand der Ereignisstempeldaten überwacht werden.

     DRA ändert diese Attribute. Wählen Sie daher Attribute aus, die nicht von DRA oder anderen Anwendungen in der Umgebung verwendet werden.

Weitere Informationen zu Ereignisstempeln finden Sie unter Funktionsweise von Ereignisstempeln.

Azure Sync (Azure-Synchronisierung)

Mit Azure Sync können Sie Richtlinien in Bezug auf ungültige Zeichen und auf die Zeichenlänge erzwingen, um Verzeichnissynchronisierungsfehler zu verhindern. Wenn diese Option aktiviert ist, wird sichergestellt, dass für Eigenschaften, die mit Azure Active Directory synchronisiert werden, ungültige Zeichen eingeschränkt und Zeichenlängenlimits erzwungen werden.

So aktivieren Sie Azure Sync:

1. Klicken Sie im linken Bereich auf **Configuration Management** (Konfigurationsmanagement).
2. Klicken Sie unter „Common Tasks“ (Allgemeine Aufgaben) im rechten Bereich auf **Update Administration Server Options** (Verwaltungsserveroptionen aktualisieren).
3. Wählen Sie auf der Registerkarte „Azure Sync“ die Option **Enforce online mailbox policies for invalid characters and character length** (Online-Postfach-Richtlinien für ungültige Zeichen und Zeichenlänge erzwingen) aus.

Aktivieren mehrerer Manager für Gruppen

Wenn Sie die Unterstützung mehrerer Manager für die Verwaltung einer Gruppe aktivieren, werden die Manager der Gruppe in einem von zwei standardmäßigen Attributen gespeichert. Wenn Microsoft Exchange ausgeführt wird, ist dies das Attribut `msExchCoManagedByLink`. Wenn Microsoft Exchange nicht ausgeführt wird, ist das standardmäßige Attribut `nonSecurityMember`. Die letzte der beiden Optionen kann geändert werden. Wir empfehlen jedoch, den technischen Support zu kontaktieren, falls Sie diese Einstellung ändern möchten.

So aktivieren Sie die Unterstützung für mehrere Manager für Gruppen:

1. Klicken Sie im linken Bereich auf **Configuration Management** (Konfigurationsmanagement).
2. Klicken Sie unter „Common Tasks“ (Allgemeine Aufgaben) im rechten Bereich auf **Update Administration Server Options** (Verwaltungsserveroptionen aktualisieren).
3. Aktivieren Sie auf der Registerkarte „Enable Support for Group Multiple Managers“ (Unterstützung für mehrere Gruppenmanager aktivieren) das Kontrollkästchen **Enable support for group's multiple managers** (Unterstützung für mehrere Gruppenmanager aktivieren).

Verschlüsselte Kommunikation

Mit dieser Funktion können Sie die Verschlüsselung der Kommunikation zwischen dem Delegierungs- und Konfigurationsclient und dem Verwaltungsserver aktivieren und deaktivieren. Standardmäßig verschlüsselt DRA Kontopasswörter. Die Funktion betrifft nicht die Webclient- oder PowerShell-Kommunikationen, die separat von Serverzertifikaten gehandhabt werden.

Die Verwendung einer verschlüsselten Kommunikation kann die Leistung beeinträchtigen. Standardmäßig ist die verschlüsselte Kommunikation deaktiviert. Wenn Sie die Option aktivieren, werden die Daten während der Kommunikation zwischen den Benutzeroberflächen und dem Verwaltungsserver verschlüsselt. DRA verwendet die Microsoft-Standardverschlüsselung für Remoteprozeduraufruf (RPC, Remote Procedure Call).

Um die verschlüsselte Kommunikation zu aktivieren, navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Update Administration Server Options** (Verwaltungsserveroptionen aktualisieren) > Registerkarte **General** (Allgemein) und aktivieren Sie das Kontrollkästchen **Encrypted Communications** (Verschlüsselte Kommunikation).

HINWEIS: Um die gesamte Kommunikation zwischen dem Verwaltungsserver und den Benutzeroberflächen zu verschlüsseln, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle zum Konfigurieren von Servern und Domänen.

Definieren virtueller Attribute

Mithilfe von virtuellen Attributen können Sie neue Eigenschaften erstellen und diese Eigenschaften mit Benutzern, Gruppen, dynamischen Verteilergruppen, Kontakten, Computern und organisatorischen Einheiten verknüpfen. Mit virtuellen Attributen können Sie neue Eigenschaften erstellen, ohne das Active Directory-Schema erweitern zu müssen.

Mithilfe von virtuellen Attributen können Sie neue Eigenschaften zu Objekten in Active Directory hinzufügen. Virtuelle Attribute können nur auf dem primären Verwaltungsserver erstellt, aktiviert, deaktiviert, verknüpft und aus einer Verknüpfung gelöst werden. DRA speichert die virtuellen Attribute, die Sie erstellen, in AD LDS. DRA reproduziert die virtuellen Attribute während des MMS-Synchronisierungsprozesses vom primären Verwaltungsserver zu den sekundären Verwaltungsservern.

Wenn Sie über die entsprechenden Befugnisse verfügen, können Sie virtuelle Attribute verwalten. Die Rolle „Manage Virtual Attributes“ (Virtuelle Attribute verwalten) umfasst Befugnisse zum Erstellen, Aktivieren, Verknüpfen, Lösen der Verknüpfung, Deaktivieren und Anzeigen von virtuellen Attributen.

Virtuelle Attribute erstellen

Sie benötigen die Befugnis *Create Virtual Attributes* (Virtuelle Attribute erstellen), um virtuelle Attribute zu erstellen, und die Befugnis *View Virtual Attributes* (Virtuelle Attribute anzeigen), um virtuelle Attribute anzuzeigen.

Um ein virtuelles Attribut zu erstellen, navigieren Sie zum Knoten **Configuration Management** (Konfigurationsmanagement) > **Virtual Attributes** (Virtuelle Attribute) > **Managed Attribures** (Verwaltete Attribute) und klicken Sie im Aufgabenmenü auf **New Virtual Attribute** (Neues virtuelles Attribut).

Virtuelle Attribute mit Objekten verknüpfen

Sie können nur aktivierte virtuelle Attribute mit Active Directory-Objekten verknüpfen. Nachdem Sie ein virtuelles Attribut mit einem Objekt verknüpft haben, ist das virtuelle Attribut als Teil der Objekteigenschaften verfügbar.

Um virtuelle Attribute über die DRA-Benutzeroberflächen verfügbar zu machen, müssen Sie eine benutzerdefinierte Eigenschaftenseite erstellen.

Um ein virtuelles Attribut mit einem Objekt zu verknüpfen, navigieren Sie zum Knoten **Configuration Management** (Konfigurationsmanagement) > **Virtual Attributes** (Virtuelle Attribute) > **Managed Attributes** (Verwaltete Attribute), klicken Sie mit der rechten Maustaste auf das virtuelle Attribut, das Sie verwenden möchten, und wählen Sie **Associate** (Verknüpfen) > (Objekttyp) aus.

HINWEIS

- Sie können virtuelle Attribute nur mit Benutzern, Gruppen, dynamischen Verteilergruppen, Computern, Kontakten und organisatorischen Einheiten verknüpfen.
- Wenn Sie ein virtuelles Attribut mit einem Objekt verknüpfen, erstellt DRA automatisch zwei standardmäßige benutzerdefinierte Befugnisse. Die Hilfsadministratoren müssen über diese benutzerdefinierten Befugnisse verfügen, um das virtuelle Attribut verwalten zu können.

Verknüpfung virtueller Attribute aufheben

Sie können die Verknüpfung virtueller Attribute mit Active Directory-Objekten aufheben. Für neu erstellte Objekte werden virtuelle Attribute, deren Verknüpfung zum betreffenden Objekttyp aufgehoben wurde, nicht in den Objekteigenschaften angezeigt.

Um die Verknüpfung zwischen einem virtuellen Attribut und einem Active Directory-Objekt aufzuheben, navigieren Sie zum Knoten **Configuration Management** (Konfigurationsmanagement) > **Virtual Attributes** (Virtuelle Attribute) > **Managed Classes** (Verwaltete Klassen) > (Objekttyp). Klicken Sie mit der rechten Maustaste auf das virtuelle Attribut und wählen Sie **Disassociate** (Zuordnung aufheben) aus.

Virtuelle Attribute deaktivieren

Sie können virtuelle Attribute deaktivieren, wenn sie mit keinem Active Directory-Objekt verknüpft sind. Wenn Sie ein virtuelles Attribut deaktivieren, können die Administratoren das virtuelle Attribut nicht anzeigen oder mit einem Objekt verknüpfen.

Um ein virtuelles Attribut zu deaktivieren, navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Managed Attributes** (Verwaltete Attribute). Klicken Sie mit der rechten Maustaste auf das Attribut im Listenbereich und wählen Sie **Disable** (Deaktivieren) aus.

Konfiguration des Caching

Der Verwaltungsserver erstellt und pflegt einen **Konto-Cache**, der Teile von Active Directory für die verwalteten Domänen enthält. Der Konto-Cache in DRA dient der Leistungsverbesserung beim Verwalten von Benutzerkonten, Gruppen, Kontakten und Computerkonten.

Um einen Zeitplan für das Aktualisieren des Cache zu erstellen oder den Cache-Status anzuzeigen, benötigen Sie die entsprechenden Befugnisse, beispielsweise die Befugnisse der integrierten Rolle zum Konfigurieren von Servern und Domänen.

HINWEIS: Um inkrementelle Aktualisierungen des Konto-Cache in Domänen mit verwalteten Teilbäumen auszuführen, stellen Sie sicher, dass das Servicekonto über Lesezugriff auf den Container „Gelöschte Objekte“ und auf alle Objekte in der Domäne des Teilbaums verfügt. Mit dem Dienstprogramm „Gelöschte Objekte“ können Sie die entsprechenden Berechtigungen überprüfen und delegieren.

Vollständige und inkrementelle Aktualisierungen

Eine inkrementelle Aktualisierung des Konto-Cache aktualisiert nur die Daten, die seit der letzten Aktualisierung geändert wurden. Inkrementelle Aktualisierungen sind eine optimierte Methode, die Änderungen in Active Directory laufend zu übernehmen. Verwenden Sie die inkrementelle Aktualisierung, um den Konto-Cache schnell zu aktualisieren und die Unternehmensvorgänge möglichst wenig zu beeinträchtigen.

WICHTIG: Microsoft Server begrenzt die Anzahl an gleichzeitigen Benutzern mit einer Verbindung zur WinRM/WinRS-Sitzung und die Anzahl der Shells pro Benutzer auf jeweils fünf. Stellen Sie daher sicher, dass das gleiche Benutzerkonto für DRA-Sekundärserver ebenfalls auf fünf Shells begrenzt ist.

Bei der inkrementellen Aktualisierung werden die folgenden Daten aktualisiert:

- Neue und geklonte Objekte
- Gelöschte und verschobene Objekte
- Gruppenmitgliedschaften
- Alle im Cache gespeicherten Objekteigenschaften für geänderte Objekte

Bei der vollständigen Cache-Aktualisierung wird der Konto-Cache von DRA für die angegebene Domäne neu erstellt.

HINWEIS: Während der Ausführung einer vollständigen Cache-Aktualisierung ist die Domäne für DRA-Benutzer nicht verfügbar.

Vollständige Aktualisierung des Konto-Cache

Um den Konto-Cache zu aktualisieren, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der integrierten Rolle „Configure Servers and Domains“ (Server und Domänen konfigurieren) enthaltenen Befugnisse.

So führen Sie eine sofortige, vollständige Aktualisierung des Konto-Cache aus:

1. Navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Managed Domains** (Verwaltete Domänen).
2. Klicken Sie mit der rechten Maustaste auf die gewünschte Domäne und wählen Sie **Properties** (Eigenschaften) aus.
3. Klicken Sie auf **Refresh Now** (Jetzt aktualisieren) auf der Registerkarte **Full refresh** (Vollständige Aktualisierung).

Standardmäßig geplante Zeiten

Die erforderliche Häufigkeit der Aktualisierung des Konto-Cache hängt von der Frequenz der Änderungen in Ihrem Unternehmen ab. Aktualisieren Sie den Konto-Cache regelmäßig mit der inkrementellen Aktualisierung, um sicherzustellen, dass DRA über die neuesten Informationen aus Active Directory verfügt.

Standardmäßig führt der Verwaltungsserver in den folgenden Intervallen eine inkrementelle Aktualisierung des Konto-Cache aus:

Domänentyp	Standardmäßige planmäßige Aktualisierung
Verwaltete Domänen	Alle 5 Minuten
Verbürgte Domänen	Jede Stunde

Eine vollständige Aktualisierung des Konto-Cache kann nicht geplant werden. DRA führt unter folgenden Umständen automatisch eine vollständige Aktualisierung des Konto-Cache aus:

- Nach der ersten Konfiguration einer verwalteten Domäne
- Nach der Aufrüstung von DRA von einer früheren Version auf eine neue Vollversion
- Nach der Installation eines DRA Service Pack

Eine vollständige Aktualisierung des Konto-Cache kann einige Minuten dauern.

Vorüberlegungen

Der Konto-Cache muss regelmäßig aktualisiert werden, damit DRA über die neuesten Informationen verfügt. Beachten Sie die folgenden Hinweise, bevor Sie eine Aktualisierung des Konto-Cache ausführen oder planen:

- Zum Ausführen einer inkrementellen Aktualisierung des Konto-Cache muss das Servicekonto oder Zugriffskonto des Verwaltungsservers berechtigt sein, auf gelöschte Objekte im Active Directory-Verzeichnis der verwalteten bzw. verbürgten Domäne zuzugreifen.
- Wenn DRA eine Aktualisierung des Konto-Cache ausführt, schließt der Verwaltungsserver die lokalen Sicherheitsgruppen von verbürgten Domänen nicht ein. Da der Cache diese Gruppen nicht enthält, lässt DRA nicht zu, dass Sie eine lokale Sicherheitsgruppe der Domäne von der verbürgten Domäne zu einer lokalen Gruppe auf dem verwalteten Mitgliedsserver hinzufügen.
- Wenn Sie eine verbürgte Domäne aus einer Aktualisierung des Konto-Cache auslassen, lässt der Verwaltungsserver diese Domäne auch bei der Aktualisierung der Domänenkonfiguration aus.
- Wenn Sie eine zuvor ausgelassene verbürgte Domäne in die Aktualisierung des Konto-Cache einschließen, führen Sie eine vollständige Aktualisierung des Konto-Cache für die verwaltete Domäne aus. So gewährleisten Sie, dass der Konto-Cache auf dem Verwaltungsserver der verwalteten Domäne die Gruppenmitgliedschaftsdaten in den verwalteten und verbürgten Domänen richtig widerspiegelt.
- Wenn Sie das Intervall für die inkrementelle Aktualisierung des Konto-Cache auf **Nie** festlegen, führt der Verwaltungsserver nur vollständige Aktualisierungen des Konto-Cache aus. Eine vollständige Aktualisierung des Konto-Cache kann eine gewisse Zeit in Anspruch nehmen. Währenddessen können Sie die Objekte in der betreffenden Domäne nicht verwalten.

- DRA kann nicht automatisch ermitteln, wann Änderungen durch andere Tools, wie Microsoft Directory Services, vorgenommen werden. Außerhalb von DRA ausgeführte Operationen können die Genauigkeit der Informationen im Cache beeinträchtigen. Wenn Sie beispielsweise ein anderes Tool verwenden, um ein Postfach zu einem Benutzerkonto hinzuzufügen, können Sie dieses Postfach erst nach einer Aktualisierung des Konto-Cache mit Exchange verwalten.
- Bei einer vollständigen Aktualisierung des Konto-Cache werden die neuesten Anmeldestatistiken, die im Cache gepflegt werden, gelöscht. Der Verwaltungsserver erfasst dann die neuesten Anmeldeinformationen von allen Domänencontrollern.

Aktivieren der Active Directory-Druckersammlung

Die AD-Druckersammlung ist standardmäßig deaktiviert. Um sie zu aktivieren, navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Update Administration Server Options** (Verwaltungsserveroptionen aktualisieren) > Registerkarte **General** (Allgemein) und aktivieren Sie das Kontrollkästchen „Collect Printers“ (Drucker erfassen).

AD LDS

Sie können die AD LDS-Bereinigungsaktualisierung zur Ausführung nach Zeitplan für bestimmte Domänen konfigurieren. Die standardmäßige Einstellung ist „Nie“, d. h. es wird nie nach Zeitplan aktualisiert. Sie können außerdem den Bereinigungsstatus und spezifische Informationen zur AD LDS (ADAM)-Konfiguration anzeigen.

Um den Zeitplan zu konfigurieren oder den Status der AD LDS-Bereinigung anzuzeigen, klicken Sie im Knoten **Account and Resource Management** (Konto- und Ressourcenverwaltung) > **All My Managed Objects** (Alle meine verwalteten Objekte) mit der rechten Maustaste auf die gewünschte Domäne und wählen Sie **Properties** (Eigenschaften) > **Adlds Cleanup Refresh Schedule** (AD LDS-Aktualisierungszeitplan) bzw. **Adlds Cleanup Status** (AD LDS-Bereinigungsstatus) aus.

Um die AD LDS (ADAM)-Konfigurationsinformationen anzuzeigen, navigieren Sie zu **Configuration Management Konfigurationsmanagement** > **Update Server Options** (Serveroptionen aktualisieren) > **ADAM Configuration** (ADAM-Konfiguration).

Dynamische Gruppe

Eine dynamische Gruppe ist eine Gruppe, deren Mitgliedschaft basierend auf einem festgelegten Satz Kriterien variiert, die Sie in den Eigenschaften der Gruppe konfigurieren. In den Domäneneigenschaften können Sie konfigurieren, dass die Aktualisierung der dynamischen Gruppen für bestimmte Domänen nach einem Zeitplan ausgeführt wird. Die standardmäßige Einstellung ist „Nie“, d. h. es wird nie nach Zeitplan aktualisiert. Sie können den Aktualisierungsstatus auch manuell aktualisieren.

Um den Zeitplan zu konfigurieren oder den Status der Aktualisierung der dynamischen Gruppen anzuzeigen, klicken Sie im Knoten **Account and Resource Management** (Konto- und Ressourcenverwaltung) > **All My Managed Objects** (Alle meine verwalteten Objekte) mit der rechten Maustaste auf die gewünschte Domäne und wählen Sie **Properties** (Eigenschaften) > **Dynamic group refresh** (Aktualisierung der dynamischen Gruppe) bzw. **Dynamic group status** (Status der dynamischen Gruppe) aus.

Weitere Informationen zu dynamischen Gruppen finden Sie unter Dynamische Gruppen in DRA.

Konfigurieren des Papierkorbs

Sie können den Papierkorb für jede Microsoft Windows-Domäne bzw. für Objekte in jeder Domäne aktivieren oder deaktivieren. Außerdem können Sie konfigurieren, wann und wie die Papierkorbbereinigung ausgeführt werden soll.

Weitere Informationen zur Verwendung des Papierkorbs finden Sie unter Papierkorb.

Papierkorb aktivieren

Sie können den Papierkorb für bestimmte Microsoft Windows-Domänen und für Objekte in diesen Domänen aktivieren. Standardmäßig aktiviert DRA den Papierkorb für jede Domäne, die mit DRA verwaltet wird, und für alle in der Domäne enthaltenen Objekte. Sie müssen Mitglied der Gruppe der DRA-Administratoren oder der DRA-Konfigurationsadministratoren sein, um den Papierkorb aktivieren zu können.

Wenn die Umgebung die folgende Konfiguration enthält, aktivieren Sie den Papierkorb mit dem Recycle Bin-Dienstprogramm:

- DRA verwaltet einen Teilbaum dieser Domäne.
- Das Service- oder Zugriffskonto des Verwaltungsservers verfügt nicht über die erforderlichen Berechtigungen zum Erstellen des Papierkorb-Containers, Verschieben von Konten in diesen Container und Bearbeiten der Konten in diesem Container.

Mit dem Recycle Bin-Dienstprogramm können Sie die Berechtigungen des Service- oder Zugriffskontos des Verwaltungsservers auf den Papierkorb-Container überprüfen.

Um den Papierkorb zu aktivieren, klicken Sie im Knoten **Recycle Bin** (Papierkorb) mit der rechten Maustaste auf die gewünschte Domäne und wählen Sie **Enable Recycle Bin** (Papierkorb aktivieren) aus.

Papierkorb deaktivieren

Sie können den Papierkorb für bestimmte Microsoft Windows-Domänen und für Objekte in diesen Domänen deaktivieren. Wenn ein deaktivierter Papierkorb Konten enthält, können Sie diese Konten nicht anzeigen, dauerhaft löschen oder wiederherstellen.

Sie müssen Mitglied der Gruppe der DRA-Administratoren oder der DRA-Konfigurationshilfsadministratoren sein, um den Papierkorb deaktivieren zu können.

Um den Papierkorb zu deaktivieren, klicken Sie im Knoten **Recycle Bin** (Papierkorb) mit der rechten Maustaste auf die gewünschte Domäne und wählen Sie **Disable Recycle Bin** (Papierkorb deaktivieren) aus.

Papierkorbobjekte und -bereinigung konfigurieren

Standardmäßig wird der Papierkorb täglich bereinigt. Sie können diese Konfiguration so ändern, dass der Papierkorb der Domäne alle x Tage bereinigt wird. Während der planmäßigen Bereinigung werden Objekte im Papierkorb, die älter als die für den betreffenden Objekttyp konfigurierte Anzahl Tage sind, aus dem Papierkorb gelöscht. Standardmäßig werden für jeden Objekttyp alle Objekte

gelöscht, die älter als 1 Tag sind. Sie können das Verhalten der Papierkorbbereinigung anpassen, indem Sie sie deaktivieren, erneut aktivieren oder das Alter der zu löschenden Objekte je nach Objekttyp festlegen.

Um die Bereinigung des Papierkorbs zu konfigurieren, wählen Sie in der Delegierungs- und Konfigurationskonsole die gewünschte Domäne aus und wechseln Sie zur Registerkarte **Tasks** (Aufgaben) > **Properties** (Eigenschaften) > **Recycle Bin** (Papierkorb).

Konfiguration der Berichterstellung

Die folgenden Abschnitte enthalten grundlegende Informationen über die Verwaltungsberichte in DRA und über die Berichtkollektoren, die Sie aktivieren können. Um auf den Assistenten zuzugreifen, in dem Sie die Kollektoren konfigurieren, navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Update Reporting Service Configuration** (Konfiguration des Berichterstellungsservices aktualisieren).

Active Directory-Kollektor konfigurieren

Der Active Directory-Kollektor erfasst für jeden verwalteten Benutzer, jede verwaltete Gruppe, jeden verwalteten Kontakt, jeden verwalteten Computer, jede verwaltete organisatorische Einheiten und jede verwaltete dynamische Verteilergruppe in DRA einen festgelegten Satz an Attributen aus Active Directory. Diese Attribute werden in der Berichterstellungsdatenbank gespeichert und dienen dem Generieren von Berichten in der Reporting-Konsole.

In der Konfiguration des Active Directory-Kollektors können Sie festlegen, welche Attribute erfasst und in der Reporting-Datenbank gespeichert werden sollen. Sie können auch konfigurieren, auf welchem DRA-Verwaltungsserver der Kollektor ausgeführt wird.

DRA-Kollektor konfigurieren

Der DRA-Kollektor erfasst Informationen zur Konfiguration von DRA und speichert diese Informationen in der Reporting-Datenbank, die zum Generieren von Berichten in der Reporting-Konsole verwendet wird.

Um den DRA-Kollektor zu aktivieren, müssen Sie festlegen, auf welchem DRA-Verwaltungsserver der Kollektor ausgeführt werden soll. Eine bewährte Vorgehensweise ist es, die Ausführung des DRA-Kollektors nach der erfolgreichen Ausführung des Active Directory-Kollektors und zu Uhrzeiten mit geringer Belastung des Servers bzw. außerhalb der normalen Betriebszeiten zu planen.

Azure-Mandantenkollektor konfigurieren

Der Azure-Mandantenkollektor erfasst Informationen über Azure-Benutzer und -Gruppen, die mit Azure Active Directory-Mandanten synchronisiert werden, und speichert diese Informationen in der Reporting-Datenbank, die zum Generieren von Berichten in der Reporting-Konsole verwendet wird.

Um den Azure-Mandantenkollektor zu aktivieren, müssen Sie festlegen, auf welchem DRA-Verwaltungsserver der Kollektor ausgeführt werden soll.

HINWEIS: Der Azure-Mandant kann eine erfolgreiche Sammlung nur ausführen, nachdem der Active Directory-Kollektor der entsprechenden Domäne eine erfolgreiche Sammlung ausgeführt hat.

Verwaltungsberichte-Kollektor konfigurieren

Der Verwaltungsberichte-Kollektor erfasst DRA-Revisionsinformationen und speichert diese Informationen in der Reporting-Datenbank, die zum Generieren von Berichten in der Reporting-Konsole verwendet wird. Beim Aktivieren des Kollektors können Sie konfigurieren, wie oft die Daten in der Datenbank für Abfragen im DRA-Berichterstellungstool aktualisiert werden sollen.

Für diese Konfiguration muss das DRA-Servicekonto über die Berechtigung **sysadmin** in SQL Server auf dem Reporting-Server verfügen. Die konfigurierbaren Optionen werden nachfolgend beschrieben:

- **Audit Export Data Interval** (Intervall für Export der Revisionsdaten): Dies legt das Zeitintervall zum Exportieren von Revisionsdaten aus dem DRA-Ablaufprotokoll (LAS) zur Datenbank „SMCubeDepot“ in SQL Server fest.
- **Management Report Summarization Interval** (Zusammenfassungsintervall für Verwaltungsbericht): Dies legt das Zeitintervall fest, gemäß dem Revisionsdaten aus der SMCubeDepot-Datenbank zur DRA-Berichterstellungsdatenbank übertragen werden, wo sie mit dem DRA-Berichterstellungstool abgefragt werden können.

Statistik zu letzten Anmeldungen erfassen

Sie können DRA so konfigurieren, dass die Statistiken zu den letzten Anmeldungen von allen Domänencontrollern in der verwalteten Domäne erfasst werden. Um das Erfassen von Statistiken zu den letzten Anmeldungen zu aktivieren und zu planen, müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse.

Standardmäßig ist die Funktion zum Erfassen von Statistiken zu den letzten Anmeldungen deaktiviert. Wenn Sie Statistiken zu den letzten Anmeldungen erfassen möchten, müssen Sie die Funktion aktivieren. Nachdem Sie das Erfassen von Statistiken zu den letzten Anmeldungen aktiviert haben, können Sie Statistiken zur letzten Anmeldung eines bestimmten Benutzers anzeigen oder den Status der Erfassung der Statistiken zur letzten Anmeldung anzeigen.

So erfassen Sie Statistiken zur letzten Anmeldung:

1. Navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Managed Domains** (Verwaltete Domänen).
2. Klicken Sie mit der rechten Maustaste auf die gewünschte Domäne und wählen Sie **Properties** (Eigenschaften) aus.
3. Klicken Sie auf die Registerkarte **Last logon schedule** (Zeitplan für letzte Anmeldung), um die Erfassung von Statistiken zu den letzten Anmeldungen zu aktivieren.

Unified-Änderungsverlauf

Mit der Unified-Änderungsverlauf-Serverfunktion können Sie Berichte zu außerhalb von DRA vorgenommenen Änderungen generieren.

Befugnisse für Serverkonfiguration für Unified-Änderungsverlauf delegieren

Um den Unified-Änderungsverlauf-Server zu verwalten, weisen Sie den Hilfsadministratoren die Rolle „Unified Change History Server Administration“ (Unified-Änderungsverlauf-Serveradministration) oder die unten aufgeführten zutreffenden Befugnisse zu:

- Delete Unified Change History Server Configuration (Serverkonfiguration des Unified-Änderungsverlaufs löschen)
- Set Unified Change History Configuration Information (Konfigurationsinformationen für Unified-Änderungsverlauf festlegen)
- View Unified Change History Configuration Information (Konfigurationsinformationen für Unified-Änderungsverlauf anzeigen)

So delegieren Sie Befugnisse für den Unified-Änderungsverlauf-Server (UCH-Server):

1. Klicken Sie im Knoten „Delegation Management“ (Delegierungsverwaltung) auf **Powers** (Befugnisse), suchen Sie mit der Objektsuchfunktion die gewünschten UCH-Befugnisse und wählen Sie sie aus.
2. Klicken Sie mit der rechten Maustaste auf eine der ausgewählten UCH-Befugnisse und wählen Sie **Delegate Roles and Powers** (Rollen und Befugnisse delegieren) aus.
3. Suchen Sie nach dem bestimmten Benutzer, der Gruppe oder der Hilfsadministratorgruppe, dem bzw. der Sie Befugnisse delegieren möchten.
4. Verwenden Sie die **Objektauswahl**, um die gewünschten Objekte zu suchen und hinzuzufügen, und klicken Sie im **Assistenten** auf **Roles and Powers** (Rollen und Befugnisse).
5. Klicken Sie auf **ActiveViews** (Aktivansichten) und verwenden Sie die **Objektauswahl**, um die gewünschten Aktivansichten zu suchen und hinzuzufügen.
6. Klicken Sie auf **Next** (Weiter) und dann auf **Finish** (Fertigstellen), um den Delegierungsprozess abzuschließen.

Server für Unified-Änderungsverlauf (UCH) konfigurieren

So konfigurieren Sie die Server für den Unified-Änderungsverlauf:

1. Melden Sie sich bei der Delegierungs- und Konfigurationskonsole an.
2. Erweitern Sie **Configuration Management**(Konfigurationsmanagement) > **Integration Servers** (Integrationsserver).
3. Klicken Sie mit der rechten Maustaste auf **Unified Change History** (Unified-Änderungsverlauf) und wählen Sie **New Unified Change History Server** (Neuer Unified-Änderungsverlauf-Server) aus.
4. 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.

5 Testen Sie die Serververbindung und klicken Sie auf **Finish** (Fertig stellen), um die Konfiguration zu speichern.

6 Fügen Sie nach Bedarf weitere Server hinzu.

Befugnisse für die Konfiguration des Workflowautomatisierungsservers delegieren

Weisen Sie den Hilfsadministratoren zum Verwalten von Workflows die Rolle „Workflow Automation Server Administration“ (Workflowautomatisierungsserver-Administration) oder die unten aufgeführten zutreffenden Befugnisse zu:

- Create Workflow Event and Modify All Properties (Workflowereignis erstellen und alle Eigenschaften ändern)
- Delete Workflow Automation Server Configuration (Konfiguration des Workflowautomatisierungsservers löschen)
- Set Workflow Automation Server Configuration Information (Informationen für Konfiguration des Workflowautomatisierungsservers festlegen)
- Start Workflow (Workflow starten)
- View All Workflow Event Properties (Alle Workflowereigniseigenschaften anzeigen)
- View All Workflow Properties (Alle Workfloweigenschaften anzeigen)
- View Workflow Automation Server Configuration Information (Informationen für Konfiguration des Workflowautomatisierungsservers anzeigen)

So delegieren Sie Befugnisse für die Konfiguration des Workflowautomatisierungsservers:

1 Klicken Sie im Knoten „Delegation Management“ (Delegierungsverwaltung) auf **Powers** (Befugnisse), suchen Sie mit der Objektsuchfunktion die gewünschten Workflowbefugnisse und wählen Sie sie aus.

2 Klicken Sie mit der rechten Maustaste auf eine der ausgewählten Workflowbefugnisse und wählen Sie **Delegate Roles and Powers** (Rollen und Befugnisse delegieren) aus.

3 Suchen Sie nach dem bestimmten Benutzer, der Gruppe oder der Hilfsadministratorgruppe, dem bzw. der Sie Befugnisse delegieren möchten.

4 Verwenden Sie die **Objektauswahl**, um die gewünschten Objekte zu suchen und hinzuzufügen, und klicken Sie im **Assistenten** auf **Roles and Powers** (Rollen und Befugnisse).

5 Klicken Sie auf **ActiveViews** (Aktivansichten) und verwenden Sie die **Objektauswahl**, um die gewünschten Aktivansichten zu suchen und hinzuzufügen.

6 Klicken Sie auf **Next** (Weiter) und dann auf **Finish** (Fertigstellen), um den Delegierungsprozess abzuschließen.

Workflowautomatisierungsserver konfigurieren

Um die Workflowautomatisierung in DRA verwenden zu können, müssen Sie die Workflow-Engine auf einem Windows-Server installieren und dann den Workflowautomatisierungsserver in der Delegierungs- und Konfigurationskonsole konfigurieren.

So konfigurieren Sie den Workflowautomatisierungsserver:

1. Melden Sie sich bei der Delegierungs- und Konfigurationskonsole an.

   Informationen zu Befugnissen für die Workflowautomatisierung finden Sie unter Befugnisse für die Konfiguration des Workflowautomatisierungsservers delegieren.
2. Erweitern Sie **Configuration Management**(Konfigurationsmanagement) > **Integration Servers** (Integrationsserver).
3. Klicken Sie mit der rechten Maustaste auf **Workflow Automation** (Workflowautomatisierung) und wählen Sie **New Workflow Automation Server** (Neuer Workflowautomatisierungsserver) aus.
4. Geben Sie im Assistenten **Add Workflow Automation Server** (Workflowautomatisierungsserver hinzufügen) die Details wie Servername, Port, Protokoll und Zugriffskonto an.
5. Testen Sie die Serververbindung und klicken Sie auf **Finish** (Fertig stellen), um die Konfiguration zu speichern.

Weitere Informationen zur Installation der Workflow-Engine finden Sie im *Workflow Automation Administrator Guide* (Workflowautomatisierung-Administratorhandbuch).

Befugnisse für die LDAP-Suche delegieren

Mit DRA können Sie vom LDAP-Server in Vor-Ort-Bereitstellungen von Active Directory-Domänen nach LDAP-Objekten wie Benutzern, Kontakten, Computern, Gruppen und organisatorischen Einheiten suchen. Der DRA-Server verarbeitet den Vorgang und die Suche wird auf dem Domänencontroller ausgeführt. Verwenden Sie die Suchfilter, um effizientere und wirksamere Suchen auszuführen. Sie können Suchabfragen auch zur späteren Verwendung speichern und entweder öffentlich freigeben oder als privat markieren. Die gespeicherten Abfragen können Sie bearbeiten. Die Rolle „LDAP Advanced Queries“ (Erweiterte LDAP-Abfragen) erteilt Hilfsadministratoren Befugnisse zum Erstellen und Verwalten von LDAP-Suchabfragen. Mit den folgenden Befugnissen können Sie die Erstellung und Verwaltung von LDAP-Suchabfragen delegieren:

- Create Private Advanced Query (Private erweiterte Abfrage erstellen)
- Create Public Advanced Query (Öffentliche erweiterte Abfrage erstellen)
- Delete Public Advanced Query (Öffentliche erweiterte Abfrage löschen)
- Execute Advanced Query (Erweiterte Abfrage ausführen)
- Execute Saved Advanced Query (Erweiterte gespeicherte Abfrage ausführen)
- Modify Public Query (Öffentliche Abfrage ändern)
- View Advanced Query (Erweiterte Abfrage anzeigen)

So delegieren Sie Befugnisse für LDAP-Abfragen:

1. Klicken Sie im Knoten „Delegation Management“ (Delegierungsverwaltung) auf **Powers** (Befugnisse), suchen Sie mit der Objektsuchfunktion die gewünschten Befugnisse für erweiterte LDAP-Abfragen und wählen Sie sie aus.
2. Klicken Sie mit der rechten Maustaste auf eine der ausgewählten LDAP-Befugnisse und wählen Sie **Delegate Roles and Powers** (Rollen und Befugnisse delegieren) aus.
3. Suchen Sie nach dem bestimmten Benutzer, der Gruppe oder der Hilfsadministratorgruppe, dem bzw. der Sie Befugnisse delegieren möchten.
4. Verwenden Sie die **Objektauswahl**, um die gewünschten Objekte zu suchen und hinzuzufügen, und klicken Sie im **Assistenten** auf **Roles and Powers** (Rollen und Befugnisse).
5. Klicken Sie auf **ActiveViews** (Aktivansichten) und verwenden Sie die **Objektauswahl**, um die gewünschten Aktivansichten zu suchen und hinzuzufügen.
6. Klicken Sie auf **Next** (Weiter) und dann auf **Finish** (Fertigstellen), um den Delegierungsprozess abzuschließen.

Um in der Webkonsole auf die Suchfunktion zuzugreifen, wechseln Sie zu **Management > LDAP Search** (Management > LDAP-Suche).

Konfigurieren der DRA-Services für ein gruppenverwaltetes Servicekonto

Bei Bedarf können Sie ein gruppenverwaltetes Servicekonto für die DRA-Services verwenden. Weitere Informationen zum Verwenden eines gruppenverwalteten Servicekontos finden Sie in der Microsoft-Referenz *Group Managed Service Accounts Overview* (Übersicht über gruppenverwaltete Servicekonten). Dieser Abschnitt beschreibt, wie DRA für ein gruppenverwaltetes Servicekonto konfiguriert wird, nachdem das Konto zuvor zu Active Directory hinzugefügt wurde.

WICHTIG: Verwenden Sie das gruppenverwaltete Servicekonto nicht als Servicekonto während der Installation von DRA.

So konfigurieren Sie den primären DRA-Verwaltungsserver für ein gruppenverwaltetes Servicekonto:

1. Fügen Sie das gruppenverwaltete Servicekonto als Mitglied zu den folgenden Gruppen hinzu:
   - Lokale Administratorengruppe auf dem DRA-Server
   - AD LDS-Gruppe in der DRA-verwalteten Domäne
2. Ändern Sie das Anmeldekonto in den Serviceeigenschaften aller unten aufgeführten Services in das gruppenverwaltete Servicekonto:
   - NetIQ Administration-Service
   - NetIQ DRA Audit Service (NetIQ DRA-Prüfungsservice)
   - NetIQ DRA Cache Service (NetIQ DRA-Cache-Service)
   - NetIQ DRA Core Service (NetIQ DRA-Kernservice)
   - NetIQ DRA Host Service (NetIQ DRA-Hostservice)
   - NetIQ DRA Log Archive (NetIQ DRA-Protokollarchiv)
   - NetIQ DRA Replication Service (NetIQ DRA-Reproduktionsservice)

- NetIQ DRA Rest Service (NetIQ DRA-REST-Service)
- NetIQ DRA Skype Service (NetIQ DRA-Skype-Service)

3 Starten Sie alle Services neu.

So konfigurieren Sie einen sekundären DRA-Verwaltungsserver für ein gruppenverwaltetes Servicekonto:

1 Installieren Sie den Sekundärserver.
2 Weisen Sie auf dem Primärserver die Rolle **Configure Servers and Domains** (Server und Domänen konfigurieren) der Aktivansicht **Administration Servers and Managed Domains** (Verwaltungsserver und verwaltete Domänen) für das Servicekonto des Sekundärservers zu.
3 Fügen Sie auf dem Primärserver einen neuen Sekundärserver hinzu und geben Sie das Servicekonto des Sekundärservers an.
4 Fügen Sie das gruppenverwaltete Servicekonto zur Gruppe der lokalen Administratoren auf dem sekundären DRA-Verwaltungsserver hinzu.
5 Ändern Sie auf dem Sekundärserver das Anmeldekonto für alle DRA-Services in das gruppenverwaltete Servicekonto und starten Sie dann die DRA-Services neu.

Konfigurieren des Delegierungs- und Konfigurationsclients

Der Delegierungs- und Konfigurationsclient bietet Zugriff auf Konfigurations- und Delegierungsaufgaben und eignet sich für unternehmensweite Verwaltungsaufgaben von der verteilten Administration bis zur Richtlinienerzwingung. Über die Delegierungs- und Konfigurationskonsole können Sie das Sicherheitsmodell und die Serverkonfigurationen einrichten, die Sie zur effizienten Verwaltung Ihres Unternehmens benötigen.

So konfigurieren Sie den Delegierungs- und Konfigurationsclient:

1 Starten Sie den Delegierungs- und Konfigurationsclient und navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Update Administration Server Options** (Verwaltungsserveroptionen aktualisieren).
2 Klicken Sie auf die Registerkarte **Client Options** (Clientoptionen) und definieren Sie die bevorzugten Einstellungen in Bezug auf die folgenden Konfigurationsoptionen:
   - Allow users to search by ActiveView (Zulassen, dass Benutzer nach ActiveView suchen)
   - Hide source-only objects from console lists (Nur-Ursprungs-Objekte aus Konsolenliste ausblenden)
   - Show advanced Active Directory objects (Erweiterte Active Directory-Objekte anzeigen)
   - Show Security command (Sicherheitsbefehl anzeigen)
   - Show resource and shared mailboxes when searching for users (Ressourcenpostfächer und freigegebene Postfächer beim Suchen nach Benutzern anzeigen)
   - Default user UPN suffix to current domain (Standardmäßiges Benutzer-UPN-Suffix für aktuelle Domäne)
   - Maximum items editable at a time (Multi-select) (Höchstanzahl an gleichzeitig bearbeitbarer Elemente (Mehrfachauswahl))
   - Search Options (Optionen für die Suche)

- Carriage Return Option (Zeilenschaltungsoption)
- Exchange Mailbox Storage Limits Units (Einheiten für Exchange-Postfach-Speicherlimits)

Konfigurieren des Webclients

Sie können die Webkonsole zur Authentifizierung mit Smartcards oder zur Multifaktor-Authentifizierung konfigurieren. Außerdem können Sie das Branding mit einem eigenen Logo und eigenem Anwendungstitel anpassen.

Starten der Webkonsole

Sie können die Webkonsole von einem beliebigen Computer, iOS-Gerät oder Android-Gerät aus mit einem Webbrowser starten. Geben Sie zum Starten der Konsole die entsprechende URL in das Adressfeld des Webbrowsers ein. Wenn Sie die Webkomponente beispielsweise auf dem Computer „HOUserver“ installiert haben, geben Sie in das Adressfeld des Webbrowsers die Zeichenfolge `https://HOUserver/draclient` ein.

HINWEIS: Um die aktuellsten Konto- und Microsoft Exchange-Informationen in der Webkonsole anzuzeigen, konfigurieren Sie den Webbrowser so, dass bei jedem Besuch nach neueren Versionen der im Cache gespeicherten Seiten gesucht wird.

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-Serviceverbindungsoptionen festzulegen, die bei der Anmeldung angezeigt werden. Nach der Konfiguration steht den Administratoren und Hilfsadministratoren bei der Anmeldung bei der Webkonsole im Dropdown-Bereich **Optionen** die gleiche Verbindungskonfiguration zur Verfügung.

- Immer den standardmäßigen 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.
	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. Nach der Konfiguration steht den Administratoren und Hilfsadministratoren bei der Anmeldung bei der Webkonsole im Dropdown-Bereich **Optionen** die gleiche Verbindungskonfiguration zur Verfügung.

- 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.
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**.

Authentifizierung

Dieser Abschnitt enthält Informationen über die Konfiguration der Smartcard-Authentifizierung, der Windows-Authentifizierung und der Multifaktor-Authentifizierung mit der Advanced Authentication-Integration.

Authentifizierung per Smartcard

Um die Webkonsole so zu konfigurieren, dass sie einen Benutzer basierend auf der Clientberechtigung seiner Smartcard akzeptiert, müssen Sie Internet Information Services (IIS) und die REST-Services-Konfigurationsdatei konfigurieren.

WICHTIG: Stellen Sie sicher, dass die Zertifikate auf der Smartcard auch im Stammzertifikatspeicher auf dem Webserver installiert sind, weil IIS Zertifikate finden muss, die mit denen auf der Smartcard übereinstimmen.

---

1. Installieren Sie die Authentifizierungskomponenten auf dem Webserver.
   - **1a** Starten Sie den Server-Manager.
   - **1b** Klicken Sie auf **Webserver (IIS)**.
   - **1c** Wechseln Sie zum Bereich der Rollendienste und klicken Sie auf **Rollendienste hinzufügen**.
   - **1d** Wechseln Sie zum Knoten der Sicherheitsrollendienste und wählen Sie **Windows-Authentifizierung** und **Authentifizierung durch Clientzertifikatszuordnung** aus.
2. Aktivieren Sie die Authentifizierung auf dem Webserver.
   - **2a** Starten Sie **IIS-Manager**.
   - **2b** Wählen Sie den Webserver aus.
   - **2c** Suchen Sie im Bereich zu IIS das Symbol **Authentifizierung** und doppelklicken Sie darauf.
   - **2d** Aktivieren Sie „Active Directory-Clientzertifikatauthentifizierung“ und „Windows-Authentifizierung“.
3. Konfigurieren Sie den DRA-Client.
   - **3a** Wählen Sie den DRA-Client aus.
   - **3b** Suchen Sie im Bereich zu IIS das Symbol **Authentifizierung** und doppelklicken Sie darauf.
   - **3c** Aktivieren Sie „Windows-Authentifizierung“ und deaktivieren Sie „Anonyme Authentifizierung“.
4. Aktivieren Sie SSL und Clientzertifikate auf dem DRA-Client.
   - **4a** Suchen Sie im Bereich zu IIS das Symbol **SSL-Dienste** und doppelklicken Sie darauf.
   - **4b** Wählen Sie **SSL erforderlich** aus und wählen Sie **Erfordern** für die Clientzertifikate aus.

     TIPP: Wenn die Option verfügbar ist, wählen Sie **128-Bit-SSL erforderlich** aus.

     ---

5 Konfigurieren Sie die REST-Services-Webanwendung.

5a Wählen Sie die REST-Services-Webanwendung aus.

5b Suchen Sie im Bereich zu IIS das Symbol **Authentifizierung** und doppelklicken Sie darauf.

5c Aktivieren Sie „Windows-Authentifizierung“ und deaktivieren Sie „Anonyme Authentifizierung“.

6 Aktivieren Sie SSL und Clientzertifikate in der REST-Services-Webanwendung.

6a Suchen Sie im Bereich zu IIS das Symbol **SSL-Dienste** und doppelklicken Sie darauf.

6b Wählen Sie **SSL erforderlich** aus und wählen Sie **Erfordern** für die Clientzertifikate aus.

TIPP: Wenn die Option verfügbar ist, wählen Sie **128-Bit-SSL erforderlich** aus.

---

7 Konfigurieren Sie die WCF-Webservice-Datei.

7a Wählen Sie die REST-Services-Webanwendung aus und wechseln Sie zur Inhaltsansicht.

7b Suchen Sie die SVC-Datei und klicken Sie mit der rechten Maustaste darauf.

7c Wählen Sie **Switch to Features View** (Zur Funktionsansicht wechseln) aus.

7d Suchen Sie im Bereich zu IIS das Symbol **Authentifizierung** und doppelklicken Sie darauf.

7e Aktivieren Sie „Anonyme Authentifizierung“ und deaktivieren Sie alle anderen Authentifizierungsmethoden.

8 Bearbeiten Sie die REST-Services-Konfigurationsdatei.

8a Öffnen Sie die Datei `C:\inetpub\wwwroot\DRAClient\rest\web.config` in einem Texteditor.

8b Suchen Sie die Zeile `<authentication mode="None" />` und löschen Sie sie.

8c Heben Sie die Auskommentierung der unten angegebenen Zeilen auf:

- Unter der Zeile `<system.serviceModel>`:

```
<services> <service name="NetIQ.DRA.DRARestProxy.RestProxy"> <endpoint
address="" binding="webHttpBinding"
bindingConfiguration="webHttpEndpointBinding" name="webHttpEndpoint"
contract="NetIQ.DRA.DRARestProxy.IRestProxy" /> </service> </services>
```

- Unter der Zeile `<serviceDebug includeExceptionDetailInFaults="false"/>`:

```
<serviceAuthorization impersonateCallerForAllOperations="true" />
<serviceCredentials> <clientCertificate> <authentication
mapClientCertificateToWindowsAccount="true" /> </clientCertificate> </
serviceCredentials>
```

- Über der Zeile `<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />`:

```
<bindings> <webHttpBinding> <binding name="webHttpEndpointBinding"> <security
mode="Transport"> <transport clientCredentialType="Certificate" /> </
security> </binding> </webHttpBinding> </bindings>
```

9 Speichern Sie die Datei und starten Sie den IIS-Server neu.

Windows-Authentifizierung

Um die Windows-Authentifizierung auf der Webkonsole zu aktivieren, müssen Sie Internet Information Services (IIS) und die REST-Services-Konfigurationsdatei konfigurieren.

1. Öffnen Sie IIS-Manager.
2. Suchen Sie im Verbindungsbereich die REST-Services-Webanwendung und wählen Sie sie aus.
3. Wechseln Sie im rechten Bereich zum Abschnitt zu IIS und doppelklicken Sie auf **Authentifizierung**.
4. Aktivieren Sie **Windows-Authentifizierung** und deaktivieren Sie alle anderen Authentifizierungsmethoden.
5. Öffnen Sie die Datei `C:\inetpub\wwwroot\DRAClient\rest\web.config` in einem Texteditor und suchen Sie die Zeile `<authentication mode="None" />`.
6. Ändern Sie `"None"` in `"Windows"` und speichern Sie die Datei.
7. Starten Sie den IIS-Server neu.

Multifaktor-Authentifizierung mit Advanced Authentication

Advanced Authentication Framework (AAF) ist unser führendes Softwarepaket, das Ihnen mit der Multifaktor-Authentifizierung die Möglichkeit bietet, Ihre sensiblen Informationen besser zu schützen als nur mit einem einfachen Benutzernamen und Passwort.

Advanced Authentication unterstützt die folgenden Kommunikationsprotokolle zur Gewährleistung der Sicherheit:

- TLS 1.2 (Standardeinstellung), TLS 1.1, TLS 1.0
- SSL 3.0

Die Multifaktor-Authentifizierung ist ein Zugriffssteuerungsverfahren, bei dem zum Überprüfen der Benutzeridentität mehrere Authentifizierungsmethoden kombiniert werden müssen.

Es drei Arten von Authentifizierungskategorien bzw. Faktoren:

- *Wissen*. Bei dieser Kategorie benötigen Sie eine bestimmte Informationen, wie ein Passwort oder einen Aktivierungscode.
- *Besitz*. Bei dieser Kategorie benötigen Sie ein Authentifizierungsgerät, zum Beispiel eine Smartcard oder ein Smartphone.
- *Körper*. Bei dieser Kategorie verwenden Sie zur Authentifizierung ein Körperteil, wie bei der Identitätsüberprüfung mittels Fingerabdrucks.

Jeder Authentifizierungsfaktor enthält mindestens eine Authentifizierungsmethode. Eine Authentifizierungsmethode ist ein bestimmtes Verfahren, das Sie zur Überprüfung der Identität eines Benutzers einsetzen, beispielsweise durch Scannen eines Fingerabdrucks oder Anfordern eines Passworts.

Ein Authentifizierungsprozess kann als stark bezeichnet werden, wenn mindestens zwei verschiedene Authentifizierungsmethoden verwendet werden, zum Beispiel eine Authentifizierung mittels Passworteingabe und Fingerabdruck.

Advanced Authentication unterstützt die folgenden Authentifizierungsmethoden:

- LDAP-Passwort
- Remote Authentication Dial-In User Service (RADIUS)
- Smartphone

TIPP: Für die Smartphone-Methode muss der Benutzer eine iOS- oder Android-App herunterladen. Weitere Informationen finden Sie im *Advanced Authentication - Smartphone Applications User Guide* (Advanced Authentication – Benutzerhandbuch für Smartphone-Anwendungen), das auf der NetIQ-Dokumentationswebsite verfügbar ist.

Verwenden Sie die Informationen der folgenden Abschnitte, um die Webkonsole für die Multifaktor-Authentifizierung zu konfigurieren.

WICHTIG: Während einige Schritte in den folgenden Abschnitten in der Webkonsole ausgeführt werden, ist für den Großteil des Konfigurationsprozesses der Multifaktor-Authentifizierung Zugriff auf AAF erforderlich. Für diese Prozedur wird davon ausgegangen, dass Sie AAF bereits installiert haben und Zugriff auf die AAF-Hilfedokumentation haben.

Repositories zu Advanced Authentication Framework hinzufügen

Im ersten Schritt der Konfiguration der Webkonsole für die Multifaktor-Authentifizierung werden alle Active Directory-Domänen, die die von DRA verwalteten DRA-Administratoren und Hilfsadministratoren enthalten, zu AAF hinzugefügt. Diese Domänen werden als Repositorys bezeichnet. Sie enthalten die Identitätsattribute der Benutzer und Gruppen, die Sie authentifizieren möchten.

1. Melden Sie sich mit einem Benutzernamen mit Administratorberechtigungen und dem entsprechenden Passwort beim AAF-Administrationsportal an.
2. Klicken Sie im linken Bereich auf **Repositorys**.
3. Klicken Sie auf **Hinzufügen**.
4. Füllen Sie das Formular aus.

   TIPP: Der **LDAP-Typ** ist **AD**.

   TIPP: Geben Sie einen Benutzernamen mit Administratorberechtigungen und das entsprechende Passwort in die jeweiligen Felder ein.

   ---
5. Klicken Sie auf **Server hinzufügen**.
6. Geben Sie die IP-Adresse des LDAP-Servers in das Feld **Adresse** ein.
7. Klicken Sie auf **Speichern**.
8. Wiederholen Sie die Schritte 3 bis 7 für alle AD-Repositorys, die von DRA verwaltet werden.
9. Klicken Sie für jedes Repository auf der Repository-Seite auf **Jetzt synchronisieren**, um es mit dem AAF-Server zu synchronisieren.

Authentifizierungsketten erstellen

Eine Authentifizierungskette enthält mindestens eine Authentifizierungsmethode. Die Methoden in der Kette werden in der Reihenfolge aufgerufen, in der Sie zur Kette hinzugefügt wurden. Um sich zu authentifizieren, muss ein Benutzer alle Methoden der Kette durchlaufen. Sie können beispielsweise eine Kette erstellen, die die LDAP-Passwort-Methode und die SMS-Methode umfasst. Wenn sich ein Benutzer mit dieser Kette authentifizieren möchte, muss er sich zunächst mit dem LDAP-Passwort authentifizieren. Anschließend wird eine Textnachricht mit einem Einmalpasswort an das Mobiltelefon des Benutzers gesendet. Nach Eingabe des Einmalpassworts sind alle Methoden in der Kette erfüllt und die Authentifizierung erfolgt. Eine Authentifizierungskette kann einem bestimmten Benutzer oder einer bestimmten Gruppe zugewiesen werden.

So erstellen Sie eine Authentifizierungskette:

1. Melden Sie sich mit einem Benutzernamen mit Administratorberechtigungen und dem entsprechenden Passwort beim AAF-Administrationsportal an.
2. Klicken Sie im linken Bereich auf **Ketten**. Im rechten Bereich wird eine Liste der zurzeit verfügbaren Ketten angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Füllen Sie das Formular aus. Alle Felder müssen ausgefüllt werden.

   WICHTIG: Fügen Sie die Methoden in der Reihenfolge hinzu, in der sie aufgerufen werden sollen. Wenn die Benutzer beispielsweise zuerst ein LDAP-Passwort eingeben sollen, fügen Sie die LDAP-Passwort-Methode als erste Methode zur Kette hinzu.

   WICHTIG: Stellen Sie sicher, dass der Schalter **Anwenden, wenn von Endgeräteigentümer verwendet** ausgeschaltet ist.
5. Setzen Sie den Schalter **Ist aktiviert** auf EIN.
6. Geben Sie die Namen der Rollen oder Gruppen, die dieser Authentifizierungsanforderung unterliegen sollen, in das Feld **Rollen und Gruppen** ein.

   TIPP: Wenn die Kette für alle Benutzer gelten soll, geben Sie `alle Benutzer` in das Feld **Rollen und Gruppen** ein und wählen Sie **Alle Benutzer** aus der angezeigten Dropdown-Liste aus.

   Alle Benutzer und Gruppen, die Sie auswählen, werden unter dem Feld **Rollen und Gruppen** hinzugefügt.
7. Klicken Sie auf **Speichern**.

Authentifizierungsereignisse erstellen

Ein Authentifizierungsereignis wird durch eine Anwendung ausgelöst (in diesem Fall von der Webkonsole), die einen Benutzer authentifizieren möchte. Einem Ereignis muss mindestens eine Authentifizierungskette zugewiesen sein, damit beim Auslösen des Ereignisses die Methoden der mit dem Ereignis verknüpften Kette aufgerufen werden und der Benutzer sich authentifizieren kann.

Ein Endgerät ist das eigentliche Gerät (zum Beispiel ein Computer oder ein Smartphone), auf dem die Software ausgeführt wird, die das Authentifizierungsereignis auslöst. DRA registriert das Endgerät bei AAF, nachdem Sie ein Ereignis erstellt haben.

Über das Feld der Endgeräte-Positivliste können Sie den Zugriff auf ein Ereignis auf bestimmte Endgeräte beschränken. Alternativ können Sie zulassen, dass alle Endgeräte auf das Ereignis zugreifen können.

So erstellen Sie ein Authentifizierungsereignis:

1. Melden Sie sich mit einem Benutzernamen mit Administratorberechtigungen und dem entsprechenden Passwort beim AAF-Administrationsportal an.
2. Klicken Sie im linken Bereich auf **Ereignisse**. Im rechten Bereich wird eine Liste der zurzeit verfügbaren Ereignisse angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Füllen Sie das Formular aus. Alle Felder müssen ausgefüllt werden.

   WICHTIG: Stellen Sie sicher, dass der Schalter **Ist aktiviert** auf EIN festgelegt ist.

5. Wenn Sie den Zugriff auf bestimmte Endgeräte beschränken möchten, wechseln Sie zum Bereich der Endgeräte-Positivliste und verschieben Sie die gewünschten Ziel-Endgeräte aus der Liste *Verfügbar* zur Liste *Verwendet*.

   TIPP: Wenn die Liste *Verwendet* keine Endgeräte enthält, ist das Ereignis für alle Endgeräte verfügbar.

Webkonsole aktivieren

Nachdem Sie Ketten und Ereignisse konfiguriert haben, können Sie sich als Administrator bei der Webkonsole anmelden und Advanced Authentication aktivieren.

Nachdem die Authentifizierung aktiviert ist, muss sich jeder Benutzer über AAF authentifizieren, bevor er Zugriff auf die Webkonsole erhält.

WICHTIG: Bevor Sie die Webkonsole aktivieren, müssen Sie bereits bei den Authentifizierungsmethoden registriert sein, die von der Webkonsole zur Authentifizierung der Benutzer verwendet wird. Weitere Informationen zum Registrieren der Authentifizierungsmethoden finden Sie im *Advanced Authentication Framework User Guide* (Advanced Authentication Framework-Benutzerhandbuch).

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

TIPP: Nachdem Sie die Konfiguration gespeichert haben, wird das Endgerät in AAF erstellt. Um ein Endgerät anzuzeigen oder zu bearbeiten, melden Sie sich mit einem Benutzernamen mit Administratorberechtigungen und dem entsprechenden Passwort am AAF-Administrationsportal an und klicken Sie im linken Bereich auf **Endgeräte**.

Abschließende Schritte

1. Melden Sie sich mit einem Benutzernamen mit Administratorberechtigungen und dem entsprechenden Passwort am AAF-Administrationsportal an und klicken Sie im linken Bereich auf **Ereignisse**.
2. Bearbeiten Sie jedes Webkonsolenereignis:
   - **2a** Öffnen Sie das Ereignis zur Bearbeitung.
   - **2b** Wechseln Sie zum Bereich mit der Endgeräte-Positivliste und verschieben Sie das Endgerät, das Sie beim Konfigurieren der Webkonsole erstellt haben, aus der Liste **Verfügbar** zur Liste **Verwendet**. So stellen Sie sicher, dass nur die Webkonsole diese Ereignisse verwenden kann.
3. Klicken Sie auf **Speichern**.

7 Verbinden verwalteter Systeme

Dieser Abschnitt enthält Informationen zum Verbinden und Konfigurieren von verwalteten Systemen in Bezug auf Domänen und zu Microsoft Exchange-Komponenten wie öffentliche Ordner, Exchange, Office 365 und Skype for Business Online.

Verwalten von Active Directory-Domänen

Sie können neue verwaltete Domänen und Computer über den Delegierungs- und Verwaltungsclient hinzufügen, nachdem Sie den Verwaltungsserver installiert haben. Sie können auch Teilbäume und verbürgte Domäne hinzufügen und Domänen- und Exchange-Zugriffskonten für die Teilbäume und verbürgten Domänen erstellen. Um verwaltete Domänen und Computer hinzufügen zu können, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse.

HINWEIS: Nachdem Sie das Hinzufügen von verwalteten Domänen abgeschlossen haben, stellen Sie sicher, dass die Zeitpläne für die Aktualisierung des Konto-Cache für diese Domänen richtig festgelegt sind.

Hinzufügen von verwalteten Domänen und Computern

So fügen Sie eine verwaltete Domäne oder einen verwalteten Computer hinzu:

1. Navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **New Managed Domain** (Neue verwaltete Domäne).
2. Geben Sie die hinzuzufügende Komponente an, indem Sie das entsprechende Optionsfeld auswählen und den Namen der Domäne bzw. des Computers angeben:
   - **Domäne verwalten**
     - Informationen zum Verwalten eines Teilbaums einer Domäne finden Sie in Hinzufügen eines verwalteten Teilbaums.
     - Wenn Sie eine neue Domäne mit aktiviertem sicherem LDAP auf den Domänencontrollern hinzufügen und DRA über SSL mit den Domänencontrollern kommunizieren soll, aktivieren Sie **This domain is configured for LDAP over SSL** (Diese

Domäne ist für LDAP über SSL konfiguriert). Weitere Informationen finden Sie unter Konfigurieren von DRA zum Ausführen von Secure Active Directory (sicherem Active Directory).

- **Computer verwalten**

Klicken Sie nach Abschluss der Konfiguration auf **Next** (Weiter).

3. Geben Sie auf der Registerkarte **Domain access** (Domänenzugriff) die Kontoberechtigung ein, die DRA für den Zugriff auf diese Domäne bzw. diesen Computer verwenden soll. Standardmäßig verwendet DRA das Servicekonto des Verwaltungsservers.
4. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertigstellen**.
5. Um mit der Verwaltung von Objekten von dieser Domäne bzw. diesem Computer zu beginnen, aktualisieren Sie die Domänenkonfiguration.

Festlegen von Domänenzugriffskonten

Für jede verwaltete Domäne bzw. jeden verwalteten Teilbaum können Sie ein Konto festlegen, das anstelle des Verwaltungsserver-Servicekontos für den Zugriff auf diese Domäne verwendet werden soll. Dieses alternative Konto wird als Zugriffskonto bezeichnet. Um ein Zugriffskonto zu konfigurieren, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse.

Um ein Zugriffskonto für einen Mitgliedsserver festzulegen, müssen Sie zur Verwaltung der Domäne berechtigt sein, in der das Domänenmitglied vorhanden ist. Sie können Domänenmitglieder nur verwalten, wenn sie in einer verwalteten Domäne enthalten sind, auf die Sie über den Verwaltungsserver zugreifen können.

So legen Sie ein Zugriffskonto fest:

1. Navigieren Sie zum Knoten **Configuration Management** (Konfigurationsmanagement) > **Managed Domains** (Verwaltete Domänen).
2. Klicken Sie mit der rechten Maustaste auf die Domäne oder den Teilbaum, für die bzw. den Sie ein Zugriffskonto festlegen möchten, und klicken Sie auf **Properties** (Eigenschaften).
3. Klicken Sie auf der Registerkarte für den Domänenzugriff auf **Use the following account to access this domain** (Folgendes Konto für den Zugriff auf diese Domäne verwenden).
4. Geben Sie den Berechtigungsnachweis für das Konto an und bestätigen Sie die Angaben. Klicken Sie dann auf **OK**.

Informationen zur Konfiguration dieses Konto mit den niedrigsten Berechtigungen finden Sie in DRA-Zugriffskonten mit niedrigsten Berechtigungen.

Festlegen von Exchange-Zugriffskonten

Für jede Domäne in DRA verwalten Sie Exchange-Objekte mit dem DRA-Domänenzugriffskonto oder mit einem separaten Exchange-Zugriffskonto. Um ein Exchange-Zugriffskonto zu konfigurieren, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse.

WICHTIG: Microsoft Server begrenzt die Anzahl an gleichzeitigen Benutzern mit einer Verbindung zur WinRM/WinRS-Sitzung und die Anzahl der Shells pro Benutzer auf jeweils fünf. Stellen Sie daher sicher, dass das gleiche Benutzerkonto für DRA-Sekundärserver ebenfalls auf fünf Shells begrenzt ist.

So legen Sie ein Exchange-Zugriffskonto fest:

1. Navigieren Sie zum Knoten **Configuration Management** (Konfigurationsmanagement) > **Managed Domains** (Verwaltete Domänen).
2. Klicken Sie mit der rechten Maustaste auf die Domäne oder den Teilbaum, für die bzw. den Sie ein Zugriffskonto festlegen möchten, und klicken Sie auf **Properties** (Eigenschaften).
3. Klicken Sie auf der Registerkarte für das Exchange-Zugriffskonto auf **Use the following account to access all Exchange servers** (Folgendes Konto für den Zugriff auf alle Exchange-Server verwenden).
4. Geben Sie den Berechtigungsnachweis für das Konto an und bestätigen Sie die Angaben. Klicken Sie dann auf **OK**.

Informationen zur Konfiguration dieses Konto mit den niedrigsten Berechtigungen finden Sie in .

Hinzufügen eines verwalteten Teilbaums

Sie können verwaltete und fehlende Teilbäume von spezifischen Microsoft Windows-Domänen hinzufügen, nachdem Sie den Verwaltungsserver installiert haben. Um einen verwalteten Teilbaum hinzuzufügen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der integrierten Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse.

Weitere Informationen zu den unterstützten Microsoft Windows-Versionen finden Sie in Anforderungen für DRA-Verwaltungsserver, Webkonsole und REST-Erweiterungen.

Durch Verwalten eines Teilbaums einer Windows-Domäne können Sie DRA zum sicheren Verwalten einer Abteilung oder eines Geschäftsbereichs innerhalb einer größeren Unternehmensdomäne verwenden.

Beispielsweise können Sie einen Teilbaum für Houston in der Domäne SUEDWEST festlegen, sodass DRA zur Verwaltung nur der Objekte in der organisatorischen Einheit „Houston“ und deren untergeordneten organisatorischen Einheiten verwendet wird. Auf diese Weise können Sie flexibel einen oder mehrere Teilbäume verwalten, ohne Verwaltungsberechtigungen für die gesamte Domäne zu benötigen.

HINWEIS

- Um sicherzustellen, dass das angegebene Konto über Berechtigungen zum Verwalten dieses Teilbaums und zum Ausführen inkrementeller Aktualisierungen des Konto-Cache verfügt, überprüfen und delegieren Sie mit dem Dienstprogramm für gelöschte Objekte die entsprechenden Berechtigungen.
- Nachdem Sie das Hinzufügen von verwalteten Teilbäumen abgeschlossen haben, stellen Sie sicher, dass die Zeitpläne für die Aktualisierung des Konto-Cache für die entsprechenden Domänen richtig festgelegt sind.

So fügen Sie einen verwalteten Teilbaum hinzu:

1. Navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **New Managed Domain** (Neue verwaltete Domäne).
2. Klicken Sie auf der Domänen- oder Serverregisterkarte auf **Manage a domain** (Domäne verwalten) und geben Sie die Domäne oder den Teilbaum an, die bzw. den Sie verwalten möchten.
3. Geben Sie die Domäne des Teilbaums an, den Sie verwalten möchten.
4. Wählen Sie **Manage a subtree of this domain** aus und klicken Sie dann auf **Next** (Weiter).
5. Klicken Sie auf der Registerkarte der Teilbäume auf **Add** (Hinzufügen), um den Teilbaum hinzuzufügen, den Sie verwalten möchten. Sie können mehrere Teilbäume angeben.
6. Geben Sie auf der Registerkarte „Zugriffskonto“ die Kontoberechtigung ein, die DRA für den Zugriff auf diesen Teilbaum verwenden soll. Standardmäßig verwendet DRA das Servicekonto des Verwaltungsservers.
7. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Finish** (Fertigstellen).
8. Um mit der Verwaltung von Objekten von diesem Teilbaum zu beginnen, aktualisieren Sie die Domänenkonfiguration.

Hinzufügen einer verbürgten Domäne

Verbürgte Domänen ermöglichen die Benutzerauthentifizierung in verwalteten Systemen in der gesamten verwalteten Umgebung. Nachdem Sie eine verbürgte Domäne hinzugefügt haben, können Sie Domänen- und Exchange-Zugriffskonten festlegen, Cache-Aktualisierungen planen und weitere Aktionen in den Eigenschaften der Domäne wie für eine verwaltete Domäne ausführen.

So fügen Sie eine verbürgte Domäne hinzu:

1. Wählen Sie im Knoten **Configuration Management** (Konfigurationsmanagement) > **Managed Domains** (Verwaltete Domänen) die verwaltete Domäne aus, die eine verknüpfte verbürgte Domäne hat.
2. Klicken Sie im Detailbereich auf **Trusted domains** (Verbürgte Domänen). Der Detailbereich muss im Anzeigemenü aktiviert sein.
3. Klicken Sie mit der rechten Maustaste auf die verbürgte Domäne und wählen Sie **Properties** (Eigenschaften) aus.
4. Deaktivieren Sie **Ignore this trusted domain** (Diese verbürgte Domäne ignorieren) und wenden Sie die Änderungen an.

HINWEIS: Durch das Hinzufügen einer verbürgten Domäne wird eine vollständige Aktualisierung des Konto-Cache initiiert. Sie erhalten hierzu eine Benachrichtigung mit einer Aufforderung zur Bestätigung, wenn Sie auf **Apply** (Anwenden) klicken.

Konfigurieren von DRA zum Ausführen von Secure Active Directory (sicherem Active Directory)

Secure Active Directory (sicheres Active Directory) bezieht sich auf eine DRA-Umgebung, in der die Kommunikation zwischen DRA und Active Directory zur Verbesserung der Sicherheit mit dem LDAPS-Protokoll (LDAP über SSL) verschlüsselt wird.

Beim Aufrüsten von DRA 9.x auf DRA 10.x muss LDAPS zur Verwendung von sicherem Active Directory nach der Aufrüstung aktiviert werden. Für diese Funktion muss außerdem die Funktion der automatischen Erkennung aktiviert werden, die der Erkennung und Verbindung zu DRA- und REST-Servern dient.

LDAP über SSL (LDAPS) aktivieren

Befolgen Sie die unten aufgeführten Schritte, wenn Sie von DRA 9.x auf DRA 10.x aufrüsten. Wenn Sie DRA für eine Neuinstallation konfigurieren, beachten Sie die Anweisungen in Hinzufügen von verwalteten Domänen und Computern.

1. Wechseln Sie in der Delegierungs- und Konfigurationskonsole von DRA zu **Configuration Management**(Konfigurationsmanagement) > **Managed Domains** (Verwaltete Domänen).
2. Klicken Sie mit der rechten Maustaste auf die Domäne und öffnen Sie die Eigenschaften.
3. Aktivieren Sie auf der Registerkarte „General“ (Allgemein) die Option **This domain is configured for LDAP over SSL** (Diese Domäne ist für LDAP über SSL konfiguriert) und klicken Sie auf **OK**.
4. Starten Sie den NetIQ Administration-Service neu.

HINWEIS: Wenn Sie außerdem die automatische Erkennung zur Verwendung von sicherem Active Directory konfigurieren, können Sie zuerst diese Konfiguration abschließen, bevor Sie die Services neu starten. Weitere Informationen finden Sie unter Automatische Erkennung für LDAPS konfigurieren.

Automatische Erkennung für LDAPS konfigurieren

Die automatische Erkennung bezeichnet den Mechanismus, mit dem der Client automatisch eine Verbindung zur verfügbaren DRA-Umgebung herstellt.

Um DRA für eine Umgebung zu konfigurieren, in der sicheres Active Directory ausgeführt wird, konfigurieren Sie den Registrierungsschlüssel `ClientSSLAllDomains`:

1. Starten Sie das Dienstprogramm des Registrierungseditors.
2. Klicken Sie mit der rechten Maustaste auf den Knoten `HKEY_LOCAL_MACHINE SOFTWARE\Wow6432Node\Mission Critical Software\RestExtentions`.
3. Wählen Sie **Neu** > **DWORD-Wert (32-Bit)** aus.
4. Benennen Sie den neuen Schlüssel `ClientSSLAllDomains`.
5. Legen Sie den Wert des Registrierungsschlüssels auf 1 fest.
6. Starten Sie nach dem Hinzufügen des Registrierungsschlüssels `ClientSSLAllDomains` die folgenden Services neu:
   - World Wide Web Publishing Service (WWW-Publishingdienst)

- NetIQ DRA Host Service (NetIQ DRA-Hostservice)
- NetIQ DRA Rest Service (NetIQ DRA-REST-Service)

Verbinden öffentlicher Ordner

Mit DRA können Sie öffentliche Ordner aus Microsoft Exchange verwalten. Sie können bestimmte Eigenschaften öffentlicher Ordner mit DRA verwalten, indem Sie Domänen für die Gesamtstruktur der öffentlichen Ordner erstellen und den Hilfsadministratoren entsprechende Befugnisse gewähren.

WICHTIG: Zum Verwalten der Administration öffentlicher Ordner müssen Sie zuerst die Microsoft Exchange-Unterstützung in DRA aktivieren und Sie müssen über die entsprechenden Befugnisse verfügen.

- Informationen zum Aktivieren von Microsoft Exchange finden Sie in Aktivieren von Microsoft Exchange.
- Informationen zu Kontoberechtigungen finden Sie in DRA-Zugriffskonten mit niedrigsten Berechtigungen.

So konfigurieren Sie die Unterstützung für öffentliche Ordner aus Microsoft Exchange:

1. Klicken Sie mit der rechten Maustaste auf **Managed Public Folder Forests** (Verwaltete Gesamtstrukturen öffentlicher Ordner) im Konfigurations- und Verwaltungsknoten und klicken Sie dann auf **New Public Folder Forest** (Neue Gesamtstruktur öffentlicher Ordner).
2. Klicken Sie auf **Forest Domain** (Gesamtstrukturdomäne), geben Sie die Active Directory-Gesamtstruktur an, in der sich die öffentlichen Ordnerobjekte befinden, und klicken Sie auf **Next** (Weiter).
3. Geben Sie unter **Domain access** (Domänenzugriff) das Zugriffskonto an.

   WICHTIG: Wenn Sie den Sekundärserver verwenden, ist die Option **Use the Primary Administration Server domain access account** (Domänenzugriffskonto für primären Verwaltungsserver verwenden) verfügbar.

   ---
4. Geben Sie unter **Exchange access** (Exchange-Zugriff) das Konto an, das DRA für den sicheren Zugriff auf die Exchange-Server verwenden soll.

   WICHTIG: Wenn Sie den Sekundärserver verwenden, ist die Option **Use the Primary Administration Server Exchange access account** (Exchange-Zugriffskonto für primären Verwaltungsserver verwenden) verfügbar.

   ---
5. Wählen Sie unter **Exchange server** (Exchange-Server) den Exchange-Server aus, den DRA für die Verwaltung der öffentlichen Ordner verwenden soll.
6. Überprüfen Sie in der **Summary** (Zusammenfassung) die Kontodetails und Exchange-Serverdetails und klicken Sie dann auf **Finish** (Fertigstellen), um den Prozess abzuschließen.

   Der DRA-Server führt eine vollständige Aktualisierung des Konto-Cache für den öffentlichen Ordner aus. Die neue Gesamtstruktur der öffentlichen Ordner wird in der Konsole angezeigt, nachdem die Cache-Aktualisierung abgeschlossen ist. Dies kann einige Minuten dauern.

HINWEIS: Sie können eine ausgewählte Gesamtstrukturdomäne für öffentliche Ordner aus den **Aufgaben** oder über das Kontextmenü entfernen.

Anzeigen und Ändern der Eigenschaften einer Domäne für öffentliche Ordner

So können Sie die Eigenschaften einer Domäne für öffentliche Ordner anzeigen und ändern:

1. Klicken Sie im Konfigurationsmanagement-Knoten auf **Managed Public Folder Forests** (Verwaltete Gesamtstrukturen öffentlicher Ordner), um die öffentlichen Ordner anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf das Konto für öffentliche Ordner, das Sie anzeigen möchten, und wählen Sie **Properties** (Eigenschaften) aus.
3. In den Eigenschaften für die **Public Folder Forest** (Gesamtstruktur öffentlicher Ordner) können Sie die folgenden Aktionen ausführen:
   - **Allgemein:** Hier können Sie die Details des Kontos für öffentliche Ordner anzeigen und das Feld **Exchange Server** aktualisieren, das vom DRA-Server zum Ausführen von Exchange-Aktivitäten auf dem Server der öffentlichen Ordner verwendet wird.
   - **Statistik:** Hier können Sie die Anzahl der öffentlichen Ordner und die Anzahl öffentlichen Ordner mit aktivierter Mail anzeigen.
   - **Incremental Status (Status der inkrementellen Aktualisierung):** Hier können Sie den Status der inkrementellen Aktualisierung des Konto-Cache anzeigen.
   - **Incremental schedule (Zeitplan für inkrementelle Aktualisierung):** Hier können Sie den Zeitplan für die inkrementelle Cache-Aktualisierung anzeigen und die Cache-Aktualisierung neu planen.
   - **Full status (Status der vollständigen Aktualisierung):** Hier können Sie den Status der vollständigen Aktualisierung des Konto-Cache anzeigen.
   - **Full refresh (Vollständige Aktualisierung):** Hier können Sie sofort eine vollständige Aktualisierung des Konto-Cache ausführen.

     NetIQ empfiehlt, **Full refresh** (Vollständige Aktualisierung) nur auszuführen, wenn die Daten im Cache der öffentlichen Ordner beschädigt sind.
   - **Domain access (Domänenzugriff):** Hier können Sie die Details zum DRA-Servicekonto anzeigen und Zugriffskonten überschreiben.
   - **Exchange access (Exchange-Zugriff):** Hier können Sie den sicheren Zugriff auf Exchange-Server anzeigen oder aktualisieren.

Delegieren von Befugnissen für öffentliche Ordner

Mit Aktivansichten können Sie Befugnisse definieren und Delegierungen für öffentliche Ordner verwalten. Sie können Regeln zum Hinzufügen verwalteter Objekte festlegen, Domänen wählen und Befugnisse zuweisen und dann Hilfsadministratoren diese Befugnisse für öffentliche Ordner delegieren.

So erstellen Sie eine Aktivansicht und delegieren Befugnisse für öffentliche Ordner:

1. Klicken Sie im Knoten **Delegation Management** (Delegierungsmanagement) auf **ActiveViews**.
2. Klicken Sie auf **Next** (Weiter) im Assistenten **Create ActiveView** (ActiveView erstellen), wählen Sie in der Dropdown-Liste **Add** (Hinzufügen) die erforderliche Regel aus und wählen Sie öffentliche Ordner als Objekttyp. So erstellen Sie beispielsweise eine Objektzuordnungsregel: Wählen Sie **Objects that match a rule** (Mit Regel übereinstimmende Objekte) und wählen Sie als Objekttyp **Public Folders** (Öffentliche Ordner).
3. Geben Sie die Aktivansicht-Regel an, die Sie zum öffentlichen Ordner hinzufügen möchten, und klicken Sie dann auf **Next** (Weiter).
4. Geben Sie den Namen für die Aktivansicht an und klicken Sie auf **Finish** (Fertig stellen).
5. Klicken Sie auf **ActiveViews** (Aktivansichten) und wechseln Sie zu **Delegate Administration** (Verwaltung delegieren) > **Assistant Admins** (Hilfsadministratoren). Geben Sie den Administratortyp in der Dropdown-Liste **Add** (Hinzufügen) im **Assistenten** an.
6. Suchen Sie nach dem bestimmten Benutzer, der Gruppe oder der Hilfsadministratorgruppe, dem bzw. der Sie Befugnisse delegieren möchten.
7. Verwenden Sie die **Objektauswahl**, um die gewünschten Objekte zu suchen und hinzuzufügen, und klicken Sie im **Assistenten** auf **Roles and Powers** (Rollen und Befugnisse).
8. Wählen Sie **Roles** (Rollen) aus der Dropdown-Liste **Hinzufügen** aus, suchen Sie die Administratorrolle für öffentliche Ordner und fügen Sie sie hinzu.
9. Wählen Sie Befugnisse in der Dropdown-Liste **Add** (Hinzufügen) aus, suchen Sie alle zusätzlichen Befugnisse, die Sie den Hilfsadministratoren zuweisen möchten, die nicht Mitglied der Rolle der Administratoren der öffentlichen Ordner sind, und weisen Sie diese zusätzlichen Befugnisse zu.
10. Klicken Sie auf **Next** (Weiter) und dann auf **Finish** (Fertigstellen), um den Delegierungsprozess abzuschließen.

Nachdem Sie das Delegieren von Befugnissen für öffentliche Ordner abgeschlossen haben, können die autorisierten Benutzer Eigenschaften von öffentlichen Ordnern in konfigurierten Domänen mit der Webkonsole erstellen, lesen, aktualisieren und löschen.

Aktivieren von Microsoft Exchange

Durch Aktivieren von Microsoft Exchange können Sie Exchange- und Exchange Online-Funktionen nutzen und Microsoft Exchange-Richtlinien, integrierte Postfächer und Mail-aktivierte Objektverwaltung einschließen. Sie können die Unterstützung für Microsoft Exchange auf jedem Verwaltungsserver für Microsoft Exchange Server 2013 und höhere Versionen aktivieren und deaktivieren.

Um Exchange zu aktivieren, müssen Sie über die erforderlichen Berechtigungen verfügen, beispielsweise über die Befugnisse, die in der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) enthalten sind. Außerdem muss Ihre Lizenz das Exchange-Produkt unterstützen. Weitere Informationen zu den Anforderungen für Microsoft Exchange finden Sie unter Unterstützte Plattformen.

So aktivieren Sie die Unterstützung für Microsoft Exchange und Exchange Online:

1. Wechseln Sie in der Delegierungs- und Konfigurationskonsole zu**Policy and Automation Management** (Richtlinien- und Automatisierungsverwaltung) > **Configure Exchange Policies** (Exchange-Richtlinien konfigurieren).
2. Wählen Sie **Enable Exchange Policy** (Exchange-Richtlinie aktivieren) aus und klicken Sie auf **Apply** (Anwenden).

Konfigurieren von Azure-Mandanten

Mit einem aktiven Azure-Konto und einem oder mehreren Azure-Mandanten können Sie DRA zur Verwaltung von Benutzer- und Gruppenobjekten mit Azure Active Directory konfigurieren. Diese Objekte umfassen Benutzer und Gruppen, die in Azure erstellt wurden oder von DRA-verwalteten Domänen mit dem Azure-Mandanten synchronisiert werden.

Zum Verwalten von Azure-Aufgaben sind die Azure PowerShell-Module, Azure Active Directory and Azure Resource Manager Profile, erforderlich. Außerdem benötigen Sie ein Konto in Azure Active Directory. Informationen zu den Kontoberechtigungen für den Azure-Mandantenzugriff finden Sie in DRA-Zugriffskonten mit niedrigsten Berechtigungen.

WICHTIG: Vorgänge wie das Erstellen, Ändern, Löschen, Deaktivieren und Aktivieren von Azure-Objekten werden in der Delegierungs- und Konfigurationskonsole nicht unterstützt.

- „Rollen und Befugnisse delegieren“, auf Seite 95
- „Erstellen einer Azure-Anwendung und Hinzufügen eines Azure-Mandanten“, auf Seite 97
- „Zurücksetzen eines Azure-Anwendungspassworts“, auf Seite 98

Rollen und Befugnisse delegieren

Zum Verwalten von Azure-Mandanten müssen Sie entweder den DRA-Administrator oder einen Hilfsadministrator mit der delegierten Rolle „Configure Servers and Domains“ (Server und Domänen konfigurieren) verwenden und zum Verwalten von Azure-Objekten sind die integrierten Azure-Rollen erforderlich.

Integrierte Azure-Rollen

Weisen Sie zum Delegieren von Azure-Objekten die folgenden Azure-Rollen zu:

- **Azure Group Administration (Azure-Gruppenverwaltung):** Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Azure-Gruppen und der Azure-Gruppenmitgliedschaft erforderlich sind.
- **Azure User Administration (Azure-Benutzerverwaltung):** Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Azure-Benutzern erforderlich sind.

Azure-Befugnisse

Mit den folgenden Befugnissen können Sie die Erstellung und Verwaltung von Azure-Benutzern und -Gruppen delegieren.

Befugnisse für Azure-Benutzerkonten:

- Create Azure User and Modify All Properties (Azure-Benutzer erstellen und alle Eigenschaften ändern)
- Delete Azure User Account Permanently (Azure-Benutzerkonto dauerhaft löschen)
- Manage Sign-In for Azure Users (Anmeldung für Azure-Benutzer verwalten)
- Manage Sign-In for Azure Users Synced to Azure Tenant (Anmeldung für mit Azure-Mandant synchronisierte Azure-Benutzer verwalten)
- Modify All Azure User Properties (Alle Azure-Benutzereigenschaften ändern)
- Reset Azure User Account Password (Azure-Benutzerkontopasswort zurücksetzen)
- View All Azure User Properties (Alle Azure-Benutzereigenschaften anzeigen)

Befugnisse für Azure-Gruppen:

- Add Object to Azure Group (Objekt zu Azure-Gruppe hinzufügen)
- Create Azure Group and Modify All Properties (Azure-Gruppe erstellen und alle Eigenschaften ändern)
- Delete Azure Group Account (Azure-Gruppenkonto löschen)
- Modify All Azure Group Properties (Alle Azure-Gruppeneigenschaften ändern)
- Remove Object from Azure Group (Objekt aus Azure-Gruppe entfernen)
- View All Azure Group Properties (Alle Azure-Gruppeneigenschaften anzeigen)

Um die Eigenschaften der Azure-Benutzer oder -Gruppen auf granularer Ebene zu verwalten, können Sie benutzerdefinierte Befugnisse erstellen, indem Sie bestimmte Objektattribute auswählen.

Unterstützte Azure-Objekte

Die folgenden Azure-Gruppentypen werden unterstützt:

- Verteilerliste
- Mail-aktivierte Sicherheit
- Office 365
- Sicherheit

HINWEIS: In Azure erstellte Gastbenutzer werden nicht unterstützt.

Erstellen einer Azure-Anwendung und Hinzufügen eines Azure-Mandanten

Um einen neuen Azure-Mandanten zu verwalten, fügen Sie den neuen Mandanten hinzu, indem Sie eine Azure-Anwendung in der Delegierungs- und Konfigurationskonsole fertigstellen. DRA unterstützt die Online- und Offline-Erstellung von Azure-Anwendungen und erfordert eine Azure-Anwendung mit den folgenden Berechtigungen, um Objekte im Mandanten zu verwalten:

- Lese- und Schreibzugriff auf die vollständigen Profile aller Benutzer
- Lese- und Schreibzugriff auf alle Gruppen
- Lesezugriff auf Verzeichnisdaten

Diese Berechtigungen werden der Azure-Anwendung sowohl beim Online- als auch beim Offline-Verfahren automatisch erteilt.

So erstellen Sie eine Azure-Anwendung online und fügen einen Mandanten hinzu:

1. Wechseln Sie in der Delegierungs- und Konfigurationskonsole zu **Configuration Management**(Konfigurationsmanagement) > **Azure Tenants** (Azure-Mandanten).
2. Klicken Sie mit der rechten Maustaste auf **Azure Tenants** (Azure-Mandanten) und wählen Sie „New Azure Tenant“ (Neuer Azure-Mandant) aus.
3. (Optional) Geben Sie das Quellankerattribut an, mit dem die Active Directory-Objekte während der Synchronisierung Azure zugeordnet werden.
4. Geben Sie das Konto für den Zugriff auf den Azure-Mandanten an und bestätigen Sie den Berechtigungsnachweis.

   Informationen zu den Kontoberechtigungen für den Azure-Mandantenzugriff finden Sie in DRA-Zugriffskonten mit niedrigsten Berechtigungen.
5. Aktivieren Sie die Option **Allow DRA to create the Azure application** (DRA das Erstellen der Azure-Anwendung erlauben) aus.
6. Geben Sie den Berechtigungsnachweis für ein Benutzerkonto mit der Rolle „Azure AD Company Administrator“ (Azure AD-Unternehmensadministrator) an und bestätigen Sie dann den Berechtigungsnachweis.
7. Klicken Sie auf **Finish** (Fertig stellen).

   Das Hinzufügen des Azure-Mandanten kann mehrere Minuten dauern. Nachdem der Mandant erfolgreich hinzugefügt wurde, führt DRA eine vollständige Aktualisierung des Konto-Cache für den Mandanten aus und der hinzugefügte Mandant wird im Anzeigebereich der Azure-Mandanten angezeigt.

So erstellen Sie eine Azure-Anwendung für DRA offline und fügen einen Mandanten hinzu:

1. Wechseln Sie in der Delegierungs- und Konfigurationskonsole zu **Configuration Management**(Konfigurationsmanagement) > **Azure Tenants** (Azure-Mandanten).
2. Klicken Sie mit der rechten Maustaste auf **Azure Tenants** (Azure-Mandanten) und wählen Sie **New Azure Tenant** (Neuer Azure-Mandant) aus.

3 (Optional) Geben Sie das Quellankerattribut an, mit dem die Active Directory-Objekte während der Synchronisierung Azure zugeordnet werden.

4 Geben Sie das Konto für den Zugriff auf den Azure-Mandanten an und bestätigen Sie den Berechtigungsnachweis.

5 Aktivieren Sie die Option **Create the Azure application offline** (Azure-Anwendung offline erstellen).

6 Starten Sie eine PowerShell-Sitzung auf dem DRA-Verwaltungsserver und wechseln Sie zu `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`.

7 Führen Sie `. .\NewDraAzureApplication.ps1` aus, um PowerShell zu laden.

8 Führen Sie das Cmdlet `New-DRAAzureApplication` aus, um die Eingabeaufforderung für die Parameter zu erhalten.

9 Geben Sie für `New-DraAzureApplication` die folgenden Parameter an:

- <name> – Name der Anwendung vom Mandanten-Assistenten.

  WICHTIG: Micro Focus empfiehlt, den in der DRA-Konsole angegebenen Namen zu verwenden.

- (Optional) <environment> – Geben Sie je nachdem, welchen Mandanten Sie verwenden, „AzureCloud“, „AzureChinaCloud“, „AzureGermanyCloud“ oder „AzureUSGovernment“ an.

10 Geben Sie im Dialogfeld „Credential“ (Anmeldedaten) den Berechtigungsnachweis des Unternehmensadministrators an.

Die ID und das Passwort für die Azure-Anwendung werden generiert.

11 Kopieren Sie die Anwendungs-ID und das Passwort in die DRA-Konsole (Mandanten-Assistent, **DRA Azure Application Credentials** (Berechtigungsnachweis für DRA Azure-Anwendung) und bestätigen Sie die Anmeldedaten.

12 Klicken Sie auf **Finish** (Fertig stellen).

Das Hinzufügen des Azure-Mandanten kann mehrere Minuten dauern. Nachdem der Mandant erfolgreich hinzugefügt wurde, führt DRA eine vollständige Aktualisierung des Konto-Cache für den Mandanten aus und der hinzugefügte Mandant wird dann im Anzeigebereich der Azure-Mandanten angezeigt.

Zurücksetzen eines Azure-Anwendungspassworts

Führen Sie die unten aufgeführten Schritte aus, um ein Azure-Passwort online oder offline zurückzusetzen.

So setzen Sie ein Azure-Anwendungspasswort für DRA mit den Azure-Anmeldedaten zurück:

1 Wechseln Sie in der Delegierungs- und Konfigurationskonsole zu **Configuration Management**(Konfigurationsmanagement) > **Azure Tenants** (Azure-Mandanten).

2 Klicken Sie mit der rechten Maustaste auf den verwalteten Azure-Mandanten und wählen Sie **Properties** (Eigenschaften) aus.

3 Klicken Sie im Eigenschaftenbereich auf **Azure Application** (Azure-Anwendung).

4 Wählen Sie die Option **Allow DRA to reset the password using your Azure Credentials**(DRA erlauben, das Passwort mit den Azure-Anmeldedaten zurückzusetzen) und geben Sie die Azure-Anmeldedaten ein.

5 Wenden Sie die Änderungen an.

So setzen Sie ein Azure-Anwendungspasswort für DRA offline zurück:

1 Starten Sie eine PowerShell-Sitzung auf dem DRA-Verwaltungsserver und wechseln Sie zu `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`.

2 Führen Sie `. .\ResetDraAzureApplicationPassword.ps1` aus, um PowerShell zu laden.

3 Führen Sie das Cmdlet `. .\ResetDraAzureApplicationPassword` aus, um die Eingabeaufforderung für die Parameter zu erhalten.

4 Geben Sie für `Reset-DRAAzureApplicationPassword` die folgenden Parameter an:

- <name> – Name der Anwendung vom Mandanten-Assistenten.

  WICHTIG: Micro Focus empfiehlt, den in der DRA-Konsole angegebenen Namen zu verwenden.

- (Optional) <environment> – Geben Sie je nachdem, welchen Mandanten Sie verwenden, „AzureCloud“, „AzureChinaCloud“, „AzureGermanyCloud“ oder „AzureUSGovernment“ an.

5 Geben Sie im Dialogfeld „Credential“ (Anmeldedaten) den Berechtigungsnachweis des Unternehmensadministrators an.

Die ID und das Passwort für die Azure-Anwendung werden generiert.

6 Kopieren Sie die Anwendungs-ID und das Passwort in die DRA-Konsole (Mandanten-Assistent, **DRA Azure Application Credentials** (Berechtigungsnachweis für DRA Azure-Anwendung) und bestätigen Sie die Anmeldedaten.

7 Öffnen Sie die Delegierungs- und Konfigurationskonsole und wechseln Sie zu **Configuration Management** (Konfigurationsmanagement) > **Azure Tenants** (Azure-Mandanten).

8 Klicken Sie mit der rechten Maustaste auf einen Azure-Mandanten und wechseln Sie zu **Properties** (Eigenschaften) > **Azure Application** (Azure-Anwendung).

9 Wählen Sie **Reset the password offline** (Passwort offline zurücksetzen) mit der bereitgestellten Skriptoption und fügen Sie das Azure-Anwendungspasswort ein, das vom Skript generiert wird.

10 Wenden Sie die Änderungen an.

IV Delegierungsmodell

Mit DRA können Administratoren ein Berechtigungsschema nach dem Prinzip der „niedrigsten Berechtigungen“ implementieren, indem sie spezifischen verwalteten Objekten im Unternehmen mit den flexiblen Steuerungskomponenten granulare Befugnisse gewähren. Mit diesen Delegierungen können die Administratoren sicherstellen, dass Hilfsadministratoren genau die zum Ausführen ihrer jeweiligen Aufgaben und Verantwortlichkeiten erforderlichen Berechtigungen erhalten.

8 Grundlegendes zum dynamischen Delegierungsmodell

Mit DRA können Sie den administrativen Zugriff auf Ihr Unternehmen innerhalb des Kontexts eines Delegierungsmodells verwalten. Das Delegierungsmodell bietet Ihnen die Möglichkeit, einen Zugriff mit den „geringsten Berechtigungen“ für Hilfsadministratoren einzurichten. Es stellt dazu einen dynamischen Satz an Steuerungskomponenten bereit, die an die Änderungen und Entwicklungen im Unternehmen angepasst werden können. Mit dem Delegierungsmodell können Sie eine Zugriffssteuerung für den administrativen Zugriff einrichten, die besser an die Art und Weise, wie in Ihrer Organisation gearbeitet wird, angepasst ist:

- Flexible Regeln bieten den Administratoren die Möglichkeit, Berechtigungen auf bestimmte verwaltete Objekte basierend auf Geschäftsanforderungen anstelle auf der Unternehmensstruktur zu begrenzen.
- Die rollenbasierte Delegierung gewährleistet, dass Berechtigungen auf konsistente Weise gewährt werden, und vereinfacht die Bereitstellung.
- Die Zuweisung der Berechtigungen kann von einem einzigen Standort aus für Domänen, Cloud-Mandanten und verwaltete Anwendungen verwaltet werden.
- Granulare Befugnisse bietet Ihnen die Möglichkeit, den spezifischen Zugriff für Hilfsadministratoren maßgeschneidert festzulegen.

Steuerungselemente im Delegierungsmodell

Die Administratoren stellen den Zugriff mithilfe der folgenden Steuerungselemente über das Delegierungsmodell bereit:

- **Delegierung:** Die Administratoren stellen den Benutzern und Gruppen Zugriff bereit, indem sie eine Rolle zuweisen, die spezifizierte Berechtigungen im Kontext einer ActiveView gewährt. Die ActiveView legt den Bereich fest.
- **ActiveViews:** Eine ActiveView stellt einen bestimmten Bereich verwalteter Objekte dar, die durch eine oder mehrere Regeln definiert sind. Verwaltete Objekte, die von einer Regel in einer ActiveView identifiziert sind, werden in einem vereinheitlichten Bereich zusammengefasst.
- **ActiveView-Regel:** Regeln werden mithilfe von Ausdrücken definiert, die basierend auf verschiedenen Bedingungen wie Objekttyp, Speicherort, Name usw. mit einem Satz verwalteter Objekte übereinstimmen.
- **Rollen:** Eine Rolle stellt einen bestimmten Satz an Befugnissen (Berechtigungen) dar, die zum Ausführen einer bestimmten Verwaltungsfunktion erforderlich sind. DRA enthält eine Reihe integrierter Rollen für übliche Geschäftsaufgaben und Sie können benutzerdefinierte Rollen für die besonderen Anforderungen in Ihrem Unternehmen definieren.
- **Befugnisse:** Eine Befugnis definiert eine bestimmte Berechtigung für Aufgaben, die vom verwalteten Objekt unterstützt werden, wie das Anzeigen, Bearbeiten oder Erstellen. Die Berechtigungen zum Ändern eines verwalteten Objekts können weiter verfeinert werden, indem sie für bestimmte Eigenschaften, die geändert werden dürfen, festgelegt werden. DRA

stellt eine umfassende Liste integrierter Befugnisse für die verwalteten Objekte bereit und bietet die Möglichkeit, benutzerdefinierte Befugnisse zu definieren, um die Bereitstellung über das Delegierungsmodell zu erweitern.

Verarbeitung der Anforderungen durch DRA

Wenn der Verwaltungsserver eine Anforderung zu einer Aktion erhält, beispielsweise zum Ändern eines Benutzerpassworts, wird folgender Prozess angewendet:

1. Die ActiveViews, die zur Verwaltung der Zielobjekte des Vorgangs konfiguriert sind, werden gesucht.
2. Die Befugnisse, die dem Konto zugewiesen sind, das die Aktion anfordert, werden bestätigt.
    a. Alle ActiveView-Zuweisungen, die den Hilfsadministrator enthalten, der den Vorgang anfordert, werden bewertet.
    b. Wenn diese Liste erstellt ist, wird eine Liste aller ActiveViews erstellt, die sowohl das Zielobjekt als auch den Hilfsadministrator enthalten.
    c. Die Befugnisse werden mit den zum Ausführen des angeforderten Vorgangs erforderlichen Befugnissen verglichen.
3. *Wenn das Konto über die geeigneten Befugnisse verfügt*, lässt der Verwaltungsserver das Ausführen der Aktion zu.

    Wenn das Konto nicht über die erforderlichen Befugnisse verfügt, gibt der Verwaltungsserver einen Fehler zurück.
4. ActiveDirectory wird aktualisiert.

Beispiele der Verarbeitung von Delegierungszuweisungen durch DRA

Die folgenden Beispiele beschreiben übliche Szenarien der Bewertung des Delegierungsmodells durch DRA während der Verarbeitung einer Anforderung:

Beispiel 1: Ändern eines Benutzerpassworts

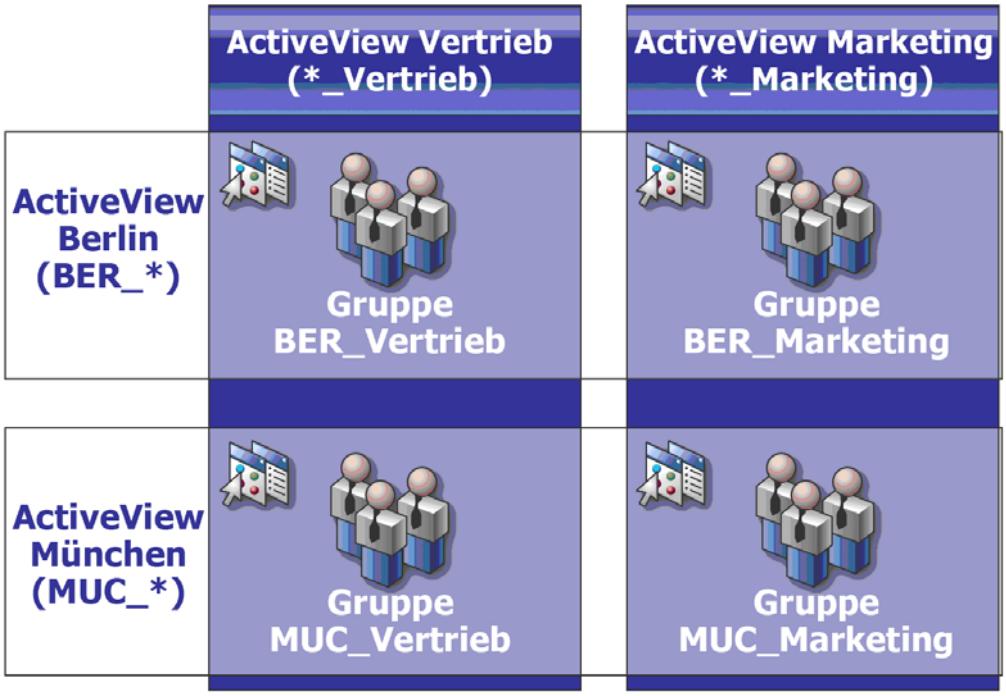
Wenn ein Hilfsadministrator versucht, ein neues Passwort für das Benutzerkonto „JSmith“ festzulegen, sucht der Verwaltungsserver alle ActiveViews, die „JSmith“ enthalten. Hierbei wird nach allen ActiveViews gesucht, die „JSmith“ direkt, über eine Platzhalterregel oder über eine Gruppenmitgliedschaft enthalten. Wenn eine ActiveView andere ActiveViews enthält, durchsucht der Verwaltungsserver auch diese zusätzlichen ActiveViews. Der Verwaltungsserver ermittelt, ob der Hilfsadministrator in einer dieser ActiveViews über die Befugnis *Reset User Account Password* (Benutzerkontopasswort zurücksetzen) verfügt. Wenn der Hilfsadministrator über die Befugnis *Reset User Account Password* (Benutzerkontopasswort zurücksetzen) verfügt, setzt der Verwaltungsserver das Passwort für „JSmith“ zurück. Wenn er nicht über die Befugnis verfügt, verweigert der Verwaltungsserver die Anforderung.

Beispiel 2: Überlappende ActiveViews

Eine Befugnis definiert die Eigenschaften eines Objekts, die ein Hilfsadministrator in der verwalteten Domäne bzw. im verwalteten Teilbaum anzeigen, ändern oder erstellen kann. Ein Objekt kann in mehreren ActiveViews enthalten sein. Diese Konfiguration wird als **überlappende ActiveViews** bezeichnet.

Im Falle von überlappenden ActiveViews können Sie verschiedene Befugnissätze über die gleichen Objekte kumulieren. Wenn Sie beispielsweise über eine ActiveView die Befugnis erhalten, Benutzerkonten zu einer Domäne hinzuzufügen, und über eine andere ActiveView die Befugnis haben, Benutzerkonten aus der gleichen Domäne zu löschen, können Sie in der Domäne sowohl Benutzerkonten hinzufügen als auch Benutzerkonten löschen. Hier sind die Befugnisse, die Sie für ein bestimmtes Objekt haben, kumulativ.

Das Prinzip der überlappenden ActiveViews und der sich daraus möglicherweise ergebenden höheren Befugnisse über Objekte in den ActiveViews ist von wesentlicher Bedeutung. Betrachten Sie die ActiveView-Konfiguration in der folgenden Abbildung.



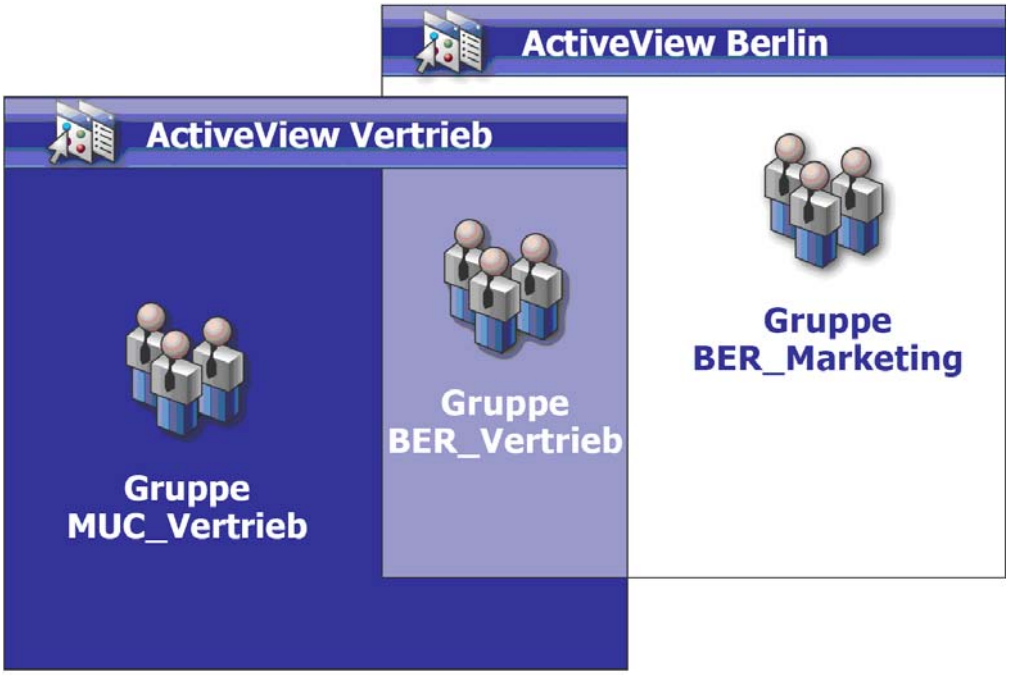
Die weißen Felder identifizieren die ActiveViews nach Standort: *Berlin* und *München*. Die dunklen Felder identifizieren die ActiveViews nach organisatorischer Funktion: *Vertrieb* und *Marketing*. In den Zellen sind die Gruppen dargestellt, die in jeder ActiveView enthalten sind.

Die Gruppen BER_Vertrieb und MUC_Vertrieb sind beide in der ActiveView „Vertrieb“ enthalten. Wenn Sie über eine Befugnis in der ActiveView „Vertrieb“ verfügen, können Sie Mitglieder der Gruppe BER_Vertrieb und Mitglieder der Gruppe MUC_Vertrieb verwalten. Wenn Sie außerdem über die Befugnis für die ActiveView für Berlin verfügen, gelten diese zusätzlichen Befugnisse für die Gruppe BER_Marketing. Auf diese Weise werden Befugnisse bei überlappenden ActiveViews kumuliert.

Die Überlappung von ActiveViews ermöglicht das Erstellen eines leistungsfähigen, flexiblen Delegierungsmodells. Diese Funktion kann jedoch auch unerwünschte Konsequenzen haben. Planen Sie die Aktivansichten mit Bedacht, um sicherzustellen, dass jeder Hilfsadministrator nur über die beabsichtigten Befugnisse über ein Benutzerkonto, eine Gruppe, eine organisatorische Einheit, einen Kontakt oder eine Ressource verfügt.

Gruppen in mehreren ActiveViews

In diesem Beispiel ist die Gruppe BER_Vertrieb in mehreren ActiveViews enthalten. Die Mitglieder der Gruppe BER_Vertrieb sind in der ActiveView „Berlin“ enthalten, weil der Gruppenname mit der Regel BER_* der ActiveView übereinstimmt. Gruppe ist auch in der ActiveView „Vertrieb“ enthalten, weil der Gruppennamen mit der Regel `*_Vertrieb` übereinstimmt. Indem sie eine Gruppe in mehrere ActiveViews einschließen, können Sie verschiedenen Hilfsadministratoren unterschiedliche Befugnisse zum Verwalten derselben Objekte gewähren.

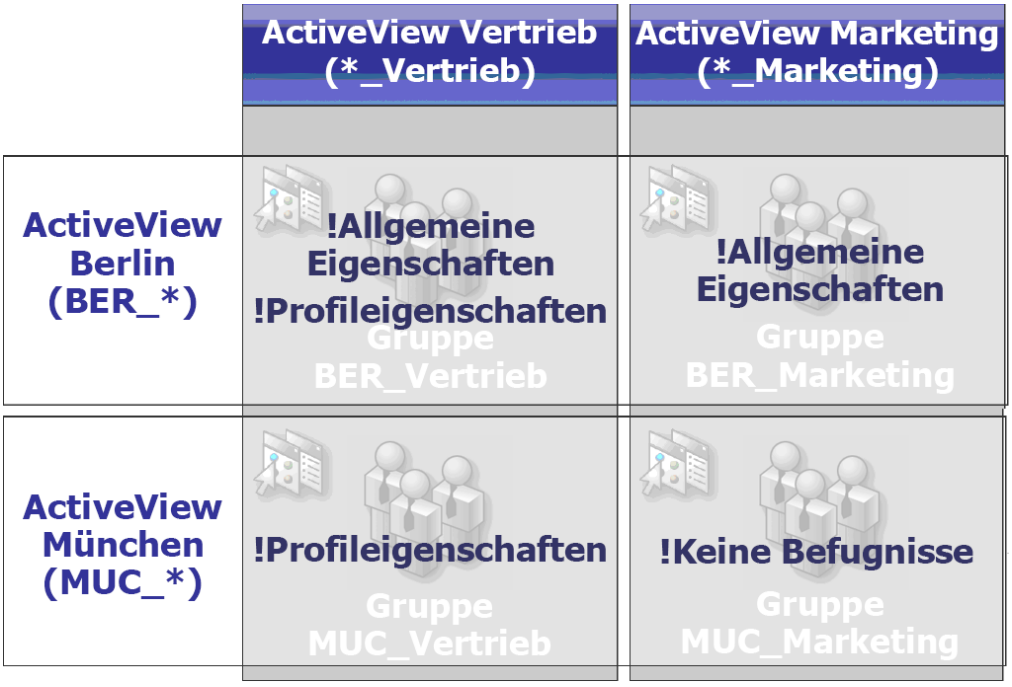


Befugnisse in ActiveViews

Angenommen, es gibt den Hilfsadministrator „JSmith“, der für die ActiveView „Berlin“ über die Befugnis *Modify General User Properties* (Allgemeine Benutzereigenschaften bearbeiten) verfügt. Diese erste Befugnis erlaubt „JSmith“, alle Eigenschaften auf der Registerkarte „Allgemein“ im Eigenschaftenfenster eines Benutzers bearbeiten. „JSmith“ verfügt in der ActiveView „Vertrieb“ über

die Befugnis *Modify User Profile Properties* (Benutzerprofileigenschaften ändern). Diese zweite Befugnis erlaubt „JSmith“, alle Eigenschaften auf der Registerkarte „Profil“ im Eigenschaftenfenster eines Benutzers bearbeiten.

Die folgende Abbildung präsentiert die Befugnisse von „JSmith“ über jede Gruppe.



„JSmith“ verfügt über die folgenden Befugnisse:

- Allgemeine Eigenschaften in der ActiveView „BER_*“
- Profileigenschaften in der ActiveView „*_Vertrieb“

Durch die Befugnisdelegierung in diesen überlappenden ActiveViews kann „JSmith“ die allgemeinen Eigenschaften und die Profileigenschaften der Gruppe „BER_Vertrieb“ ändern. „JSmith“ verfügt also über alle Befugnisse, die in allen ActiveViews für die Gruppe „BER_Vertrieb“ gewährt werden.

9 ActiveViews

Mit ActiveViews können Sie ein Delegierungsmodell mit den folgenden Merkmalen implementieren:

- Unabhängig von der Active Directory-Struktur
- Ermöglicht das Zuweisen von Befugnissen und das Definieren von Richtlinien, die zu den vorhandenen Workflows passen
- Bietet Automatisierungsfunktionen zur besseren Integration und Anpassung in Ihrem Unternehmen
- Dynamische Antwort auf Änderungen

Eine ActiveView stellt einen Satz Objekte in einer oder in mehreren Domänen dar. Sie können ein Objekt in mehrere ActiveViews einschließen. Sie können auch mehrere Objekte aus verschiedenen Domänen oder organisatorischen Einheiten einschließen.

Integrierte ActiveViews

Integrierte ActiveViews sind die standardmäßig in DRA enthaltenen ActiveViews. Diese ActiveViews stellen alle aktuellen Objekte und Sicherheitseinstellungen dar. Die integrierten ActiveViews bieten daher sofortigen Zugriff auf alle Objekte und Einstellungen und auf das standardmäßige Delegierungsmodell. Mit ActiveViews können Sie Objekte wie Benutzerkonten und Ressourcen verwalten oder das standardmäßige Delegierungsmodell auf die aktuelle Unternehmenskonfiguration anwenden.

DRA bietet mehrere integrierte ActiveViews, die das Delegierungsmodell darstellen können. Der integrierte ActiveView-Knoten enthält die folgenden ActiveViews:

All Objects (Alle Objekte)

Umfasst alle Objekte in allen verwalteten Domänen. Über diese ActiveView können Sie jeden Aspekt des Unternehmens verwalten. Weisen Sie diese Aktivansicht dem Administrator oder einem Hilfsadministrator zu, der Revisionsbefugnisse für das gesamte Unternehmen benötigt.

Objects Current User Manages as Windows Administrator (Objekte, die vom aktuellen Benutzer als Windows-Administrator verwaltet werden)

Dies umfasst Objekte aus der aktuell verwalteten Domäne. Über diese ActiveView können Sie Benutzerkonten, Gruppen, Kontakte, organisatorische Einheiten und Ressourcen verwalten. Weisen Sie diese ActiveView nativen Administratoren zu, die für die Konto- und Ressourcenobjekte in der verwalteten Domäne verantwortlich sind.

Administration Servers and Managed Domains (Verwaltungsserver und verwaltete Domänen)

Dies umfasst die Verwaltungsserver-Computer und die verwalteten Domänen. Über diese ActiveView können Sie die tägliche Wartung der Verwaltungsserver verwalten. Weisen Sie diese Aktivansicht denjenigen Hilfsadministratoren zu, deren Aufgabenbereich die Überwachung des Synchronisierungsstatus und das Ausführen von Cache-Aktualisierungen umfasst.

DRA Policies and Automation Triggers (DRA-Richtlinien und Automatisierungsauslöser)

Dies umfasst alle Richtlinien- und Automatisierungsauslöseobjekte in allen verwalteten Domänen. Über diese ActiveView können Sie die Eigenschaften und den Umfang von Richtlinien sowie die Eigenschaften von Automatisierungsauslösern verwalten. Weisen Sie diese Aktivansicht den Hilfsadministratoren zu, die für das Erstellen und Warten der Unternehmensrichtlinien verantwortlich sind.

DRA Security Objects (DRA-Sicherheitsobjekte)

Dies umfasst alle Sicherheitsobjekte. Über diese Aktivansicht können Sie Aktivansichten, Hilfsadministratorgruppen und Rollen verwalten. Weisen Sie diese Aktivansicht den Hilfsadministratoren zu, die für das Erstellen und Warten des Sicherheitsmodells verantwortlich sind.

SPA Users from All Managed and Trusted Domains (SPA-Benutzer aus allen verwalteten und verbürgten Domänen)

Dies umfasst alle Benutzerkonten aus verwalteten und verbürgten Domänen. Über diese ActiveView können Sie Benutzer Passwörter mit Secure Password Administrator (SPA) verwalten.

Zugriff auf integrierte ActiveViews

Greifen sie auf die integrierten ActiveViews zu, um das standardmäßige Delegierungsmodell zu überwachen oder eigene Sicherheitseinstellungen zu verwalten.

So greifen sie auch integrierte ActiveViews zu:

1. Navigieren Sie zu **Delegation Management** (Delegierungsverwaltung) > **Manage ActiveViews** (ActiveViews verwalten).
2. Stellen Sie sicher, dass das Suchfeld leer ist, und klicken Sie auf **Find Now** (Jetzt suchen) im Bereich **List items that match my criteria** (Mit meinen Kriterien übereinstimmende Elemente auflisten).
3. Wählen Sie die geeignete ActiveView aus.

Arbeiten mit integrierten ActiveViews

Sie können integrierte ActiveViews nicht löschen, klonen oder ändern. Sie können diese ActiveViews jedoch in Ihr vorhandenes Delegierungsmodell einschließen oder mit diesen ActiveViews ein eigenes Modell gestalten.

Sie können die integrierten ActiveViews auf folgende Weise verwenden:

- Weisen Sie einzelne der integrierten Aktivansichten den entsprechenden Hilfsadministratorgruppen zu. Dank dieser Zuweisung können die Mitglieder der Hilfsadministratorgruppe den entsprechenden Satz an Objekten mit den geeigneten Befugnissen verwalten.
- Nutzen Sie die Regeln und Verknüpfungen der integrierten ActiveViews als Leitfaden beim Gestalten und Implementieren Ihres Delegierungsmodells.

Weitere Informationen über das Gestalten eines dynamischen Delegierungsmodells finden Sie in Grundlegendes zum dynamischen Delegierungsmodell.

Implementieren einer benutzerdefinierten ActiveView

Eine ActiveView bietet Echtzeitzugriff auf bestimmte Objekte in einer oder mehreren Domänen oder organisatorischen Einheiten. Sie können Objekte zu einer ActiveView hinzufügen oder aus ihr entfernen, ohne die zugrunde liegende Domäne oder Struktur der organisatorischen Einheit zu ändern.

Betrachten Sie eine ActiveView als virtuelle Domäne oder organisatorische Einheit oder als Ergebnis einer Auswahlanweisung für eine Datenbankansicht einer relationalen Datenbank. ActiveViews können beliebige Objektsätze aus- oder einschließen, andere ActiveViews enthalten und überlappende Inhalte haben. ActiveViews können Objekte aus unterschiedlichen Domänen, Bäumen und Gesamtstrukturen enthalten. Sie können die ActiveViews beliebig konfigurieren, um die Verwaltungsanforderungen des Unternehmens zu erfüllen.

ActiveViews können die folgenden Objekttypen enthalten:

Konten:

- Benutzer
- Gruppen
- Computer
- Kontakte
- Dynamische Verteilergruppen
- Veröffentlichte Drucker
- Druckaufträge von veröffentlichten Druckern
- Ressourcenpostfächer
- Freigegebene Postfächer
- Öffentliche Ordner

Verzeichnisobjekte:

- Organisatorische Einheiten
- Domänen
- Mitgliederserver

Delegierungsobjekte:

- ActiveViews
- Selbstverwaltung
- Direkt unterstellt
- Verwaltete Gruppen

Ressourcen:

- Verbundene Benutzer
- Geräte
- Ereignisprotokolle
- Offene Dateien

- Drucker
- Druckaufträge
- Services
- Freigaben

Azure-Objekte:

- Azure-Benutzer
- Azure-Gruppe
- Azure-Mandant

ActiveViews können je nach Wachstum oder Entwicklung des Unternehmens geändert werden, um neue Objekte ein- oder auszuschließen. Mithilfe von ActiveViews können Sie so die Komplexität des Modells reduzieren, die erforderliche Sicherheit bieten und über eine deutlich größere Flexibilität als mit anderen Tools für die Unternehmensorganisation verfügen.

ActiveView-Regeln

Eine ActiveView kann aus Regeln bestehen, die Objekte wie Benutzerkonten, Gruppen, organisatorische Einheiten, Kontakte, Ressourcen, Computer, Ressourcenpostfächer, freigegebene Postfächer, dynamische Verteilergruppen und ActiveViews ein- oder ausschließen. Diese Flexibilität macht ActiveViews dynamisch.

Die Übereinstimmungsregeln verwenden **Platzhalter**. Sie können beispielsweise eine Regel definieren, die alle Computer enthält, deren Name mit der Zeichenfolge `DOM*` übereinstimmt. Diese Platzhalterspezifikation sucht alle Computerkonten, deren Name mit der Zeichenfolge „DOM“ beginnt. Diese Platzhalterregeln ermöglichen eine dynamische Verwaltung, weil alle Konten automatisch eingeschlossen werden, wenn sie die Regel erfüllen. Dank der Verwendung von Platzhaltern ist es nicht erforderlich, die ActiveViews bei einer Änderung der Organisation neu zu konfigurieren.

Sie können ActiveViews auch basierend auf der Gruppenmitgliedschaft definieren. Legen Sie eine Regel fest, die alle Mitglieder der Gruppen einschließt, deren Name mit „BER“ beginnt. Wenn dann Mitglieder zu einer beliebigen Gruppe hinzugefügt werden, die mit dieser Regel übereinstimmt, werden diese Mitglieder automatisch in die ActiveView eingeschlossen. Bei Änderungen oder Entwicklungen im Unternehmen wendet DRA die Regeln erneut an, um neue Objekte in die richtigen ActiveViews einzuschließen bzw. daraus auszuschließen.

10 Rollen

Dieser Abschnitt umfasst eine Liste und Beschreibungen der in DRA integrierten Rollen, Erläuterungen zu ihrer Verwendungsweise und Informationen zum Erstellen und Verwalten von benutzerdefinierten Rollen.

Eine Beschreibung der Rollen und ihrer allgemeinen Verwendung finden Sie in Steuerungselemente im Delegierungsmodell.

Integrierte Rollen

Die integrierten Hilfsadministratorrollen bieten sofortigen Zugriff auf einen Satz häufig verwendeter Befugnisse. Sie können die aktuelle Sicherheitskonfiguration erweitern, indem Sie diese standardmäßigen Rollen zum Delegieren von Befugnissen an bestimmte Benutzerkonten oder andere Gruppen verwenden.

Diese Rollen enthalten die Befugnisse, die zum Ausführen üblicher Verwaltungsaufgaben erforderlich sind. Die Rolle „DRA Administration“ enthält zum Beispiel alle Befugnisse, die zum Verwalten von Objekten erforderlich sind. Um diese Befugnisse verwenden zu können, muss die Rolle jedoch mit einem Benutzerkonto oder mit einer Hilfsadministratorgruppe und mit der verwalteten Aktivansicht verknüpft sein.

Da die integrierten Rollen Teil des standardmäßigen Delegierungsmodells sind, können Sie mit den integrierten Rollen schnell Befugnisse delegieren und Sicherheitsfunktionen implementieren. Diese integrierten Rollen eignen sich für übliche Aufgaben, die Sie über die DRA-Benutzeroberflächen ausführen können. Die folgende Liste beschreibt jede integrierte Rolle und fasst die Befugnisse zusammen, die mit der Rolle verknüpft sind.

Application Servers Administration (Anwendungsserververwaltung)

Diese Rolle enthält die Befugnisse, die zum Konfigurieren, Anzeigen und Löschen der Konfigurationen des Anwendungsservers erforderlich sind.

Audit All Objects (Alle Objekte überwachen)

Diese Rolle enthält alle Befugnisse, die zum Anzeigen der Eigenschaften von Objekten, Richtlinien und Konfigurationen im Unternehmen erforderlich sind. Diese Rolle ermöglicht den Hilfsadministratoren nicht, Eigenschaften zu ändern. Weisen Sie diese Rolle Hilfsadministratoren zu, die für die Überwachung von Aktionen im gesamten Unternehmen verantwortlich sind. Sie erlaubt den Hilfsadministratoren das Anzeigen aller Knoten außer „Custom Tools“ (Benutzerdefinierte Tools).

Audit Limited Account and Resource Properties (Beschränkte Konto- und Ressourceneigenschaften überwachen)

Diese Rolle enthält Befugnisse für alle Objekteigenschaften.

Audit Resources (Ressourcen überwachen)

Diese Rolle enthält alle Befugnisse, die zum Anzeigen der Eigenschaften von verwalteten Ressourcen erforderlich sind. Weisen Sie diese Rolle Hilfsadministratoren zu, die für das Überwachen von Ressourcenobjekten verantwortlich sind.

Audit Users and Groups (Benutzer und Gruppen überwachen)

Diese Rolle enthält alle Befugnisse, die zum Anzeigen der Eigenschaften von Benutzerkonten und Gruppen erforderlich sind, jedoch keine Befugnisse zum Ändern dieser Eigenschaften. Weisen Sie diese Rolle Hilfsadministratoren zu, die für das Überwachen von Kontoeigenschaften verantwortlich sind.

Azure Group Administration (Azure-Gruppenverwaltung)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Azure-Gruppen und der Azure-Gruppenmitgliedschaft erforderlich sind.

Azure User Administration (Azure-Benutzerverwaltung)

Diese Rolle umfasst alle Befugnisse, die zum Erstellen, Ändern, Löschen, Aktivieren, Deaktivieren und Anzeigen der Eigenschaften verwalteter Azure-Benutzer erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Azure-Benutzern verantwortlich sind.

Built-in Scheduler - Internal Use Only (Integrierter Planer – nur für internen Gebrauch)

Diese Rolle enthält die Befugnisse zum Planen des Zeitpunkts für die Cache-Aktualisierung in DRA.

Clone User with Mailbox (Benutzer mit Postfach klonen)

Diese Rolle enthält alle Befugnisse, die zum Klonen eines vorhandenen Benutzerkontos und des entsprechenden Kontopostfachs erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Benutzerkonten verantwortlich sind.

HINWEIS: Um zuzulassen, dass der Hilfsadministrator ein neues Benutzerkonto während der Klonaufgabe zu einer Gruppe hinzufügt, weisen sie zusätzlich die Rolle „Manage Group Membership“ (Gruppenmitgliedschaft verwalten) zu.

Computer Administration (Computerverwaltung)

Diese Rolle enthält alle Befugnisse, die zum Ändern der Computereigenschaften erforderlich sind. Hilfsadministratoren, denen diese Rolle zugewiesen ist, können Computer hinzufügen, löschen und herunterfahren und Domänencontroller synchronisieren. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten von Computern in der Aktivansicht verantwortlich sind.

Configure Servers and Domains (Server und Domänen konfigurieren)

Diese Rolle enthält alle Befugnisse, die zum Ändern der Verwaltungsserveroptionen und der verwalteten Domänen erforderlich sind. Außerdem enthält sie die Befugnisse zum Konfigurieren und Verwalten von Azure-Mandanten. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Überwachung und Wartung der Verwaltungsserver und die Verwaltung der Azure-Mandanten verantwortlich sind.

Contact Administration (Verwaltung von Kontakten)

Diese Rolle enthält alle Befugnisse, die zum Erstellen eines neuen Kontakts, Ändern der Kontakteigenschaften oder Löschen eines Kontakts erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Kontakten verantwortlich sind.

Create and Delete Computer Accounts (Computerkonten erstellen und löschen)

Diese Rolle enthält alle Befugnisse, die zum Erstellen und Löschen von Computerkonten erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Computern verantwortlich sind.

Create and Delete Groups (Gruppen erstellen und löschen)

Diese Rolle enthält alle Befugnisse, die zum Erstellen und Löschen von Gruppen erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Gruppen verantwortlich sind.

Create and Delete Resource Mailbox (Ressourcenpostfach erstellen und löschen)

Diese Rolle enthält alle Befugnisse, die zum Erstellen und Löschen von Postfächern erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Postfächern verantwortlich sind.

Create and Delete Resources (Ressourcen erstellen und löschen)

Diese Rolle enthält alle Befugnisse, die zum Erstellen und Löschen von Freigaben und Computerkonten und zum Löschen von Ereignisprotokollen erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten von Ressourcenobjekten und Ereignisprotokollen verantwortlich sind.

Create and Delete User Accounts (Benutzerkonten erstellen und löschen)

Diese Rolle enthält alle Befugnisse, die zum Erstellen und Löschen von Benutzerkonten erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Benutzerkonten verantwortlich sind.

DRA Administration (DRA-Verwaltung)

Diese Rolle umfasst alle Befugnisse, die der Hilfsadministrator benötigt. Die Rolle berechtigt einen Benutzer dazu, alle Verwaltungsaufgaben in DRA auszuführen. Die Rolle entspricht den Berechtigungen eines Administrators. Ein Hilfsadministrator, dem die Rolle „DRA Administration“ (DRA-Verwaltung) zugewiesen ist, kann auf alle Knoten in Directory and Resource Administration zugreifen.

Dynamic Group Administration (Verwaltung dynamischer Gruppen)

Diese Rolle enthält alle Befugnisse, die zum Verwalten von dynamischen Active Directory-Gruppen erforderlich sind.

Execute Advanced Queries (Erweiterte Abfragen ausführen)

Diese Rolle enthält alle Befugnisse, die zum Ausführen von gespeicherten erweiterten Abfragen erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Ausführen von erweiterten Abfragen verantwortlich sind.

Group Administration (Gruppenverwaltung)

Diese Rolle enthält alle Befugnisse, die zum Verwalten von Gruppen und Gruppenmitgliedschaften und zum Anzeigen der entsprechenden Benutzereigenschaften erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten von Gruppen oder Konto- und Ressourcenobjekten, die über diese Gruppen verwaltet werden, verantwortlich sind.

Help Desk Administration (Helpdesk-Verwaltung)

Diese Rolle umfasst die Befugnisse, die zum Anzeigen der Benutzerkontoeigenschaften und zum Ändern von Passwörtern und passwortbezogenen Eigenschaften erforderlich sind. Diese Rolle berechtigt den Hilfsadministrator außerdem, Benutzerkonten zu deaktivieren, zu aktivieren und zu entsperren. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für Helpdesk-Aufgaben zum Gewährleisten des Zugriffs der Benutzer auf ihre Konten verantwortlich sind.

Mailbox Administration (Postfachverwaltung)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten der Eigenschaften von Microsoft Exchange-Postfächern erforderlich sind. Wenn Sie Microsoft Exchange verwenden, weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten der Microsoft Exchange-Postfächer verantwortlich sind.

Manage Active Directory Collectors, DRA Collectors, and Management Reporting Collectors (Active Directory-Kollektoren, DRA-Kollektoren und Verwaltungsberichte-Kollektoren verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Active Directory-Kollektoren, DRA-Kollektoren und Verwaltungsberichte-Kollektoren für die Datenerfassung erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung der Reporting-Konfiguration verantwortlich sind.

Manage Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and Database Configuration (Active Directory-Kollektoren, DRA-Kollektoren, Verwaltungsberichte-Kollektoren und Datenbankkonfiguration verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Active Directory-Kollektoren, DRA-Kollektoren und Verwaltungsberichte-Kollektoren und für die Datenbankkonfiguration zur Datenerfassung erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung der Reporting- und Datenbank-Konfiguration verantwortlich sind.

Manage Advanced Queries (Erweiterte Abfragen verwalten)

Diese Rolle enthält alle Befugnisse, die zum Erstellen, Verwalten und Ausführen von erweiterten Abfragen erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten von erweiterten Abfragen verantwortlich sind.

Manage and Execute Custom Tools (Benutzerdefinierte Tools verwalten und ausführen)

Diese Rolle enthält alle Befugnisse, die zum Erstellen, Verwalten und Ausführen von benutzerdefinierten Tools erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten von benutzerdefinierten Tools verantwortlich sind.

Manage Clone Exceptions (Klonausnahmen verwalten)

Diese Rolle enthält alle Befugnisse, die zum Erstellen und Verwalten von Klonausnahmen erforderlich sind.

Manage Computer Properties (Computereigenschaften verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten aller Eigenschaften eines Computerkontos erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Computern verantwortlich sind.

Manage Database Configuration (Datenbankkonfiguration verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten der Datenbankkonfiguration für Verwaltungsberichte erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung der Reporting-Datenbank-Konfiguration verantwortlich sind.

Manage Dynamic Distribution Groups (Dynamische Verteilergruppen verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten der Eigenschaften von dynamischen Microsoft Exchange-Verteilergruppen erforderlich sind.

Manage Exchange Mailbox Rights (Rechte für Exchange-Postfächer verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten der Sicherheit und der Rechte für Microsoft Exchange-Postfächer erforderlich sind. Wenn Sie Microsoft Exchange verwenden, weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten der Microsoft Exchange-Postfachberechtigungen verantwortlich sind.

Manage Group Email (Gruppen-Email verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Anzeigen, Aktivieren oder Deaktivieren der Email-Adresse einer Gruppe erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten von Gruppen oder Email-Adressen für Kontoobjekte verantwortlich sind.

Manage Group Membership Security (Gruppenmitgliedschaftsicherheit verwalten)

Diese Rolle umfasst alle Befugnisse, die erforderlich sind, um festzulegen, wer die Microsoft Windows-Gruppenmitgliedschaften über Microsoft Outlook anzeigen und ändern kann.

Manage Group Memberships (Gruppenmitgliedschaften verwalten)

Diese Rolle umfasst alle Befugnisse, die erforderlich sind, um Benutzerkonten oder Gruppen zu einer vorhandenen Gruppe hinzuzufügen oder daraus zu entfernen und um die Primärgruppe eines Benutzers oder eines Computerkontos anzuzeigen. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Gruppen oder Benutzerkonten verantwortlich sind.

Manage Group Properties (Gruppeneigenschaften verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten aller Eigenschaften einer Gruppe erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Gruppen verantwortlich sind.

Manage Mailbox Move Requests (Anforderungen zum Verschieben von Postfächern verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Anforderungen zum Verschieben von Postfächern erforderlich sind.

Manage Policies and Automation Triggers (Richtlinien und Automatisierungsauslöser verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Definieren von Richtlinien und Automatisierungsauslösern erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Pflegen der Unternehmensrichtlinien und der Automatisierungsworkflows verantwortlich sind.

Manage Printers and Print Jobs (Drucker und Druckaufträge verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Druckern, Druckwarteschlangen und Druckaufträgen erforderlich sind. Um Druckaufträge zu verwalten, die mit einem Benutzerkonto verknüpft sind, müssen der Druckauftrag und das Benutzerkonto in der gleichen ActiveView enthalten sein. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Warten von Druckern und das Verwalten von Druckaufträgen verantwortlich sind.

Manage Resource Mailbox Properties (Eigenschaften von Ressourcenpostfächern verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten aller Eigenschaften eines Postfachs erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Postfächern verantwortlich sind.

Manage Resources for Managed Users (Ressourcen für verwaltete Benutzer verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Ressourcen erforderlich sind, die mit bestimmten Benutzerkonten verknüpft sind. Der Hilfsadministrator und die Benutzerkonten müssen in der gleichen Aktivansicht enthalten sein. Weisen Sie diese Rolle Hilfsadministratoren zu, die für das Verwalten von Ressourcenobjekten verantwortlich sind.

Manage Security Model (Sicherheitsmodell verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Definieren der Verwaltungsregeln erforderlich sind, einschließlich Aktivansichten, Hilfsadministratoren und Rollen. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Implementieren und Warten des Sicherheitsmodells verantwortlich sind.

Manage Services (Services verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Services erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Services verantwortlich sind.

Manage Shared Folders (Freigegebene Ordner verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten freigegebener Ordner erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von freigegebenen Ordnern verantwortlich sind.

Manage Temporary Group Assignments (Temporäre Gruppenzuweisungen verwalten)

Diese Rolle enthält alle Befugnisse, die zum Erstellen und Verwalten von temporären Gruppenzuweisungen erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Gruppen verantwortlich sind.

Manage UI Reporting (Benutzeroberflächen-Berichterstellung verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Generieren und Exportieren von Aktivitätsdetailberichten über Benutzer, Gruppen, Kontakte, Computer, organisatorische Einheiten, Befugnisse, Rollen, ActiveViews, Container, veröffentlichte Drucker und Hilfsadministratoren erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Berichterstellung verantwortlich sind.

Manage User Dial in Properties (Einwahleigenschaften der Benutzer verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Ändern der Einwahleigenschaften von Benutzerkonten erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten von Benutzerkonten verantwortlich sind, die einen Fernzugriff auf das Unternehmen haben.

Manage User Email (Benutzer-Email verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Anzeigen, Aktivieren oder Deaktivieren der Email-Adresse eines Benutzerkontos erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten von Benutzerkonten oder Email-Adressen für Kontoobjekte verantwortlich sind.

Manage User Password and Unlock Account (Benutzerpasswort verwalten und Konto entsperren)

Diese Rolle umfasst alle Befugnisse, die zum Zurücksetzen des Passworts, Festlegen der Passworteinstellungen und Entsperren von Benutzerkonten erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Pflege des Benutzerkontozugriffs verantwortlich sind.

Manage User Properties (Benutzereigenschaften verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten aller Eigenschaften eines Benutzerkontos erforderlich sind, einschließlich der Eigenschaften von Microsoft Exchange-Postfächern. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Benutzerkonten verantwortlich sind.

Manage Virtual Attributes (Virtuelle Attribute verwalten)

Diese Rolle enthält alle Befugnisse, die zum Erstellen und Verwalten von virtuellen Attributen erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von virtuellen Attributen verantwortlich sind.

Manage WTS Environment Properties (Eigenschaften der WTS-Umgebung verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Ändern der Eigenschaften der WTS-Umgebung für ein Benutzerkonto erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Pflegen der WTS-Umgebung bzw. das Verwalten von Benutzerkonten verantwortlich sind.

Manage WTS Remote Control Properties (Eigenschaften der WTS-Fernsteuerung verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Ändern der Eigenschaften der WTS-Fernsteuerung für ein Benutzerkonto erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Pflegen des WTS-Zugriffs bzw. das Verwalten von Benutzerkonten verantwortlich sind.

Manage WTS Session Properties (Eigenschaften der WTS-Sitzung verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Ändern der Eigenschaften der WTS-Sitzung für ein Benutzerkonto erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Pflegen von WTS-Sitzungen bzw. das Verwalten von Benutzerkonten verantwortlich sind.

Manage WTS Terminal Properties (Eigenschaften des WTS-Terminals verwalten)

Diese Rolle umfasst alle Befugnisse, die zum Ändern der Eigenschaften des WTS-Terminals für ein Benutzerkonto erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Pflegen von WTS-Terminaleigenschaften bzw. das Verwalten von Benutzerkonten verantwortlich sind.

OU Administration (Verwaltung organisatorischer Einheiten)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten organisatorische Einheiten erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Verwalten der Active Directory-Struktur verantwortlich sind.

Public Folder Administration (Verwaltung öffentlicher Ordnung)

Diese Rolle umfasst die Befugnisse, die zum Erstellen, Ändern, Löschen, Aktivieren und Deaktivieren der Email-Funktion und zum Anzeigen der Eigenschaften der öffentlichen Ordner erforderlich sind. Sie können diese Rolle allen Hilfsadministratoren zuweisen, die für das Verwalten von öffentlichen Ordnern verantwortlich sind.

Rename Group and Modify Description (Gruppe umbenennen und Beschreibung ändern)

Der Rolle umfasst alle Befugnisse, die zum Ändern des Namens und der Beschreibung einer Gruppe erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Gruppen verantwortlich sind.

Rename User and Modify Description (Benutzer umbenennen und Beschreibung ändern)

Der Rolle umfasst alle Befugnisse, die zum Ändern des Namens und der Beschreibung eines Benutzerkontos erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Benutzerkonten verantwortlich sind.

Replicate Files (Dateien reproduzieren)

Diese Rolle umfasst alle Befugnisse, die zum Hochladen, Löschen und Ändern von Dateiinformationen erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Reproduzieren von Dateien vom primären Verwaltungsserver zu anderen Verwaltungsservern im MMS und zu DRA-Clientcomputern verantwortlich sind.

Reset Local Administrator Password (Passwort des lokalen Administrators zurücksetzen)

Diese Rolle umfasst alle Befugnisse, die zum Zurücksetzen des Passworts des lokalen Administrators und zum Anzeigen des Namens des Computeradministrators erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Administratorkonten verantwortlich sind.

Reset Password (Passwort zurücksetzen)

Diese Rolle umfasst alle Befugnisse, die zum Zurücksetzen und Ändern von Passwörtern erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Passwortverwaltung verantwortlich sind.

Reset Password and Unlock Account Using SPA (Passwort zurücksetzen und Konto entsperren mit SPA)

Diese Rolle umfasst alle Befugnisse, die erforderlich sind, um mit Secure Password Administrator (SPA) Passwörter zurückzusetzen und Benutzerkonten zu entsperren.

Reset Unified Messaging PIN Properties (Eigenschaften der Unified Messaging-PIN zurücksetzen)

Diese Rolle umfasst alle Befugnisse, die zum Zurücksetzen der Eigenschaften der Unified Messaging-PIN für Benutzerkonten erforderlich sind.

Resource Administration (Ressourcenverwaltung)

Diese Rolle umfasst alle Befugnisse, die zum Ändern der Eigenschaften von verwalteten Ressourcen erforderlich sind, einschließlich Ressourcen, die mit einem beliebigen Benutzerkonto verknüpft sind. Weisen Sie diese Rolle Hilfsadministratoren zu, die für das Verwalten von Ressourcenobjekten verantwortlich sind.

Resource Mailbox Administration (Verwaltung von Ressourcenpostfächern)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Ressourcenpostfächern erforderlich sind.

Selbstverwaltung

Diese Rolle umfasst alle Befugnisse, die zum Ändern der grundlegenden Eigenschaften, wie Telefonnummern, Ihres eigenen Benutzerkontos erforderlich sind. Weisen Sie diese Rolle Hilfsadministratoren zu, damit diese ihre eigenen persönlichen Informationen verwalten können.

Shared Mailbox Administration (Verwaltung von freigegebenen Postfächern)

Diese Rolle umfasst alle Befugnisse, die zum Erstellen, Ändern, Löschen und Anzeigen der Eigenschaften der freigegebenen Postfächer erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von freigegebenen Postfächern verantwortlich sind.

Start and Stop Resources (Ressourcen starten und stoppen)

Diese Rolle umfasst alle Befugnisse, die zum Anhalten, Starten, Fortsetzen oder Stoppen eines Services, Starten oder Stoppen eines Geräts oder Druckers, Herunterfahren eines Computers oder Synchronisieren der Domänencontroller erforderlich sind. Außerdem enthält die Rolle die Befugnisse, die zum Anhalten, Fortsetzen und Starten von Services, Stoppen von Geräten oder Druckwarteschlangen und Herunterfahren von Computern erforderlich sind. Weisen Sie diese Rolle Hilfsadministratoren zu, die für das Verwalten von Ressourcenobjekten verantwortlich sind.

Transform a User (Benutzer umwandeln)

Diese Rolle umfasst alle Befugnisse, die zum Hinzufügen eines Benutzers zu Gruppen in einer Kontoschablone bzw. Entfernen des Benutzers aus Gruppen in einer Kontoschablone erforderlich sind, einschließlich den Befugnissen zum Ändern der Benutzereigenschaften beim Umwandeln des Benutzers.

Unified Change History Server Administration (Serververwaltung für Unified-Änderungsverlauf)

Diese Rolle enthält die Befugnisse, die zum Konfigurieren, Anzeigen und Löschen der Serverkonfiguration des Unified-Änderungsverlaufs (UCH, Unified Change History) erforderlich sind.

User Administration (Benutzerverwaltung)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten von Benutzerkonten, verknüpften Microsoft Exchange-Postfächern und Gruppenmitgliedschaften erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Verwaltung von Benutzerkonten verantwortlich sind.

View Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and Database Configuration Information (Informationen zu Active Directory-Kollektoren, DRA-Kollektoren, Verwaltungsberichte-Kollektoren und Datenbankkonfiguration anzeigen)

Diese Rolle umfasst alle Befugnisse, zum Anzeigen von Informationen zu AD-Kollektoren, DRA-Kollektoren, Verwaltungsberichte-Kollektoren und Datenbankkonfigurationen erforderlich sind.

View All Computer Properties (Alle Computereigenschaften anzeigen)

Diese Rolle umfasst alle Befugnisse, die zum Anzeigen der Eigenschaften eines Computerkontos erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Überwachung von Computern verantwortlich sind.

View All Group Properties (Alle Gruppeneigenschaften anzeigen)

Diese Rolle umfasst alle Befugnisse, die zum Anzeigen der Eigenschaften einer Gruppe erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Überwachung von Gruppen verantwortlich sind.

View All Resource Mailbox Properties (Alle Eigenschaften von Ressourcenpostfächern anzeigen)

Diese Rolle umfasst alle Befugnisse, die zum Anzeigen der Eigenschaften eines Ressourcenpostfachs erforderlich sind. Weisen Sie diese Rolle Hilfsadministratoren zu, die für das Überwachen von Ressourcenpostfächern verantwortlich sind.

View All User Properties (Alle Benutzereigenschaften anzeigen)

Diese Rolle umfasst alle Befugnisse, die zum Anzeigen der Eigenschaften eines Benutzerkontos erforderlich sind. Weisen Sie diese Rolle den Hilfsadministratoren zu, die für die Überwachung von Benutzerkonten verantwortlich sind.

Workflow Automation Server Administration (Verwaltung von Servern für die Workflowautomatisierung)

Diese Rolle enthält die Befugnisse, die zum Konfigurieren, Anzeigen und Löschen der Konfigurationen von Workflowautomatisierungsservern erforderlich sind.

WTS Administration (WTS-Verwaltung)

Diese Rolle umfasst alle Befugnisse, die zum Verwalten der Eigenschaften von Windows Terminal Server (WTS) für die Benutzerkonten in der ActiveView erforderlich sind. Wenn Sie WTS verwenden, weisen Sie diese Rolle den Hilfsadministratoren zu, die für das Warten der WTS-Eigenschaften der Benutzerkonten verantwortlich sind.

Zugriff auf integrierte Rollen

Greifen sie auf die integrierten Rollen zu, um das standardmäßige Delegierungsmodell zu überwachen oder eigene Sicherheitseinstellungen zu verwalten.

So greifen sie auch integrierte Rollen zu:

1. Navigieren Sie zu **Delegation Management** (Delegierungsverwaltung) > **Manage Roles** (Rollen verwalten).
2. Stellen Sie sicher, dass das Suchfeld leer ist, und klicken Sie auf **Find Now** (Jetzt suchen) im Bereich **List items that match my criteria** (Mit meinen Kriterien übereinstimmende Elemente auflisten).
3. Wählen Sie die geeignete Rolle aus.

Arbeiten mit integrierten Rollen

Sie können die integrierten Rollen nicht löschen oder ändern. Sie können die integrierten Rollen jedoch in das vorhandene Delegierungsmodell einfügen oder die Rollen zum Gestalten und Implementieren eines eigenen Modells verwenden.

Sie können die integrierten Rollen auf folgende Weise verwenden:

- Verknüpfen Sie eine integrierte Rolle mit einem Benutzerkonto oder mit einer Hilfsadministratorgruppe. Diese Verknüpfung gewährt dem Benutzer bzw. dem Mitglied der Hilfsadministratorgruppe die geeigneten Befugnisse zum Ausführen einer Aufgabe.
- Klonen Sie eine integrierte Rolle und verwenden Sie den Klon als Grundlage für eine benutzerdefinierte Rolle. Sie können weitere Rollen oder Befugnisse zur neuen Rolle hinzufügen und ursprünglich in der integrierten Rolle enthaltene Befugnisse entfernen.

Weitere Informationen über das Gestalten eines dynamischen Delegierungsmodells finden Sie in Grundlegendes zum dynamischen Delegierungsmodell.

Erstellen benutzerdefinierter Rollen

Durch Erstellen einer Rolle können Sie schnell und einfach ein Satz Befugnisse delegieren, die eine Verwaltungsaufgabe oder einen Workflow darstellen. Die Erstellung und Verwaltung von Rollen erfolgt über den Knoten **Delegation Management** (Delegierungsverwaltung) > **Roles** (Rollen) in der Delegierungs- und Konfigurationskonsole. Über diesen Knoten können Sie die folgenden Aktionen ausführen:

- Neue Rollen erstellen
- Vorhandene Rollen klonen
- Rolleneigenschaften ändern
- Rollen löschen
- Rollenzuweisungen verwalten
  - Neue Zuweisung delegieren
  - Vorhandene Zuweisung entfernen
  - Eigenschaften eines zugewiesenen Hilfsadministrators anzeigen
  - Eigenschaften einer zugewiesenen Active View anzeigen
- Rollen und Befugnisse eine Rolle verwalten (Rollen können geschachtelt sein)
- Rollenänderungsberichte generieren

Der allgemeine Workflow zum Ausführen beliebiger in diesem Abschnitt genannter Aktionen besteht im Auswählen des Knotens **Roles** (Rollen) und Ausführen einer der folgenden Schritte:

- Öffnen Sie über das Menü **Tasks** (Aufgaben) oder über das Kontextmenü den entsprechenden Assistenten bzw. das Dialogfeld, um die erforderlichen Aktionen abzuschließen.
- Suchen Sie das Rollenobjekt im Bereich **List items that match my criteria** (Objekte auflisten, die mit meinen Kriterien übereinstimmen) und verwenden Sie das Menü **Tasks** (Aufgaben) oder das Kontextmenü, um den entsprechenden Assistenten bzw. das Dialogfeld auszuwählen und zu öffnen und die erforderlichen Aktionen abzuschließen.

Um beliebige der oben genannten Aktionen ausführen zu können, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse der Rolle „Manage Security Model“ (Sicherheitsmodell verwalten).

11 Befugnisse

Befugnisse sind die Grundbausteine für die Verwaltung nach dem Prinzip der „geringsten Berechtigung“. Durch das Zuweisen von Befugnissen an Benutzer können Sie ein dynamisches Sicherheitsmodell implementieren und pflegen. Diese Prozeduren führen Sie in der Delegierungs- und Konfigurationskonsole aus.

Integrierte Befugnisse

Es stehen über 390 integrierte Befugnisse zum Verwalten von Objekten und Ausführen üblicher Verwaltungsaufgaben zur Verfügung, mit denen Sie beim Definieren von Rollen und Zuweisen von Delegierungen arbeiten können. Integrierte Befugnisse können nicht gelöscht werden, aber Sie können sie klonen, um benutzerdefinierte Befugnisse zu erstellen. Nachstehend finden Sie einige Beispiele für integrierte Befugnisse:

Create Group and Modify All Properties (Gruppe erstellen und alle Eigenschaften ändern)

Diese Befugnis gewährt das Recht zum Erstellen von Gruppen und Festlegen aller Eigenschaften während der Gruppenausstellung.

Delete User Account (Benutzerkonto löschen)

Wenn die Papierkorbfunktion aktiviert ist, ermöglicht diese Befugnis das Verschieben von Benutzerkonten in den Papierkorb. Wenn die Papierkorbfunktion deaktiviert ist, ermöglicht diese Befugnis das dauerhafte Löschen von Benutzerkonten.

Modify All Computer Properties (Alle Computereigenschaften ändern)

Diese Befugnis gewährt das Recht zum Ändern aller Eigenschaften der Computerkonten.

Implementieren von benutzerdefinierten Befugnissen

Um eine benutzerdefinierte Befugnis zu erstellen, erstellen Sie eine neue Befugnis oder klonen Sie eine vorhandene Befugnis. Sie können vorhandene Befugnisse als Schablone für neue Befugnisdelegierungen verwenden. Eine Befugnis definiert die Eigenschaften eines Objekts, die ein Hilfsadministrator in der verwalteten Domäne bzw. im verwalteten Teilbaum anzeigen, ändern oder erstellen kann. Benutzerdefinierte Befugnisse können den Zugriff auf mehrere Eigenschaften enthalten, wie die Befugnis *View All User Properties* (Alle Benutzereigenschaften anzeigen).

HINWEIS: Nicht alle integrierten Befugnisse können geklont werden.

Benutzerdefinierte Befugnisse werden über den Knoten **Delegation Management** (Delegierungsverwaltung) > **Powers** (Befugnisse) in der Delegierungs- und Konfigurationskonsole implementiert. Über diesen Knoten können Sie die folgenden Aktionen ausführen:

- Alle Befugniseigenschaften anzeigen
- Neue Befugnisse erstellen

- Vorhandene Befugnisse klonen
- Benutzerdefinierte Befugnisse ändern
- Befugnisänderungsberichte generieren

Um die oben genannten Aktionen ausführen zu können, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse der Rolle „Manage Security Model“ (Sicherheitsmodell verwalten).

Beachten Sie die folgenden Punkte, bevor Sie eine neue Befugnis erstellen.

1. Überprüfen Sie die mit DRA bereitgestellten Befugnisse.
2. Ermitteln Sie, ob Sie eine benutzerdefinierte Befugnis benötigen. Möglicherweise können Sie eine vorhandene Benutzerdefinierte Befugnis klonen.
3. Schließen Sie die Prozeduren im entsprechenden Assistenten ab. Schließen Sie beispielsweise den Assistenten „New Power“ (Neue Befugnis) ab.
4. Zeigen Sie die neue Befugnis an.
5. Ändern Sie die neue Befugnis je nach Bedarf.

Der allgemeine Workflow zum Ausführen beliebiger in diesem Abschnitt genannter Aktionen besteht im Auswählen des Knotens **Powers** (Befugnisse) und Ausführen einer der folgenden Schritte:

- Öffnen Sie über das Aufgabenmenü oder über das Kontextmenü den entsprechenden Assistenten bzw. das Dialogfeld, um die erforderlichen Aktionen abzuschließen.
- Suchen Sie das Befugnisobjekt im Bereich **List items that match my criteria** (Objekte auflisten, die mit meinen Kriterien übereinstimmen) und verwenden Sie das Menü **Tasks** (Aufgaben) oder das Kontextmenü, um den entsprechenden Assistenten bzw. das Dialogfeld auszuwählen und zu öffnen und die erforderlichen Aktionen abzuschließen.

Erweitern von Befugnissen

Sie können Berechtigungen oder Funktionalitäten zu einer Befugnis hinzufügen, indem Sie die Befugnis erweitern.

Um beispielsweise einem Hilfsadministrator das Recht zu gewähren, ein Benutzerkonto zu erstellen, können Sie entweder die Befugnis *Create User and Modify All Properties* (Benutzer erstellen und alle Eigenschaften ändern) oder die Befugnis *Create User and Modify Limited Properties* (Benutzer erstellen und begrenzte Eigenschaften ändern) zuweisen. Wenn Sie zusätzlich die Befugnis *Add New User to Group* (Neuen Benutzer zur Gruppe hinzufügen) zuweisen, kann der Hilfsadministrator während der Verwendung des Assistenten zur Benutzererstellung das neue Benutzerkonto zu einer Gruppe hinzufügen. In diesem Fall liefert die Befugnis *Add New User to Group* (Neuen Benutzer zur Gruppe hinzufügen) eine zusätzliche Assistentenfunktion. Die Befugnis *Add New User to Group* (Neuen Benutzer zur Gruppe hinzufügen) ist die sogenannte **Erweiterungsbefugnis**.

Erweiterungsbefugnisse können nicht eigenständig Berechtigungen oder Funktionalitäten hinzufügen. Um eine Aufgabe, die eine Erweiterungsbefugnis enthält, erfolgreich zu delegieren, müssen sie Die Erweiterungsbefugnis zusammen mit der zur erweiternden Befugnis zuweisen.

HINWEIS

- Um erfolgreich eine Gruppe zu erstellen und die neue Gruppe in eine ActiveView einzuschließen, müssen Sie in der betreffenden ActiveView über die Befugnis *Add New Group to ActiveView* (Neue Gruppe zu ActiveView) verfügen. Die betreffende ActiveView muss außerdem die organisatorische Einheit oder den integrierten Container einschließen, in der bzw. dem die neue Gruppe enthalten ist.
- Um erfolgreich eine Gruppe zu klonen und die neue Gruppe in eine ActiveView einzuschließen, müssen Sie in der betreffenden ActiveView über die Befugnis *Add Cloned Group to ActiveView* (Geklonte Gruppe zu ActiveView) verfügen. Die betreffende ActiveView muss außerdem die Ursprungsgruppe und die organisatorische Einheit bzw. den integrierten Container enthalten, in der bzw. dem die neue Gruppe enthalten sein soll.

Die folgende Tabelle listet einige Beispiele für die Aktionen auf, die beim Erstellen einer neuen Befugnis oder Ändern der Eigenschaften einer vorhandenen Befugnis konfiguriert werden können:

Zu delegierende Aufgabe	**Zuzuweisende Befugnis**	**Zuzuweisende Erweiterungsbefugnis**
Gruppe klonen und die neue Gruppe in eine angegebene ActiveView einschließen	Clone Group and Modify All Properties (Gruppe klonen und alle Eigenschaften ändern)	Add Cloned Group to ActiveView (Geklonte Gruppe zur ActiveView hinzufügen)
Gruppe erstellen und die neue Gruppe in eine angegebene ActiveView einschließen	Create Group and Modify All Properties (Gruppe erstellen und alle Eigenschaften ändern)	Add New Group to ActiveView (Neue Gruppe zur ActiveView hinzufügen)
Kontakt mit aktivierter Email-Funktion erstellen	Create Contact and Modify All Properties (Kontakt erstellen und alle Eigenschaften ändern) Create Contact and Modify Limited Properties (Kontakt erstellen und begrenzte Eigenschaften ändern)	Enable Email for New Contact (Email-Funktion für neuen Kontakt aktivieren)
Gruppe mit aktivierter Email-Funktion erstellen	Create Group and Modify All Properties (Gruppe erstellen und alle Eigenschaften ändern)	Enable Email for New Group (Email-Funktion für neue Gruppe aktivieren)
Benutzerkonto mit aktivierter Email-Funktion erstellen	Create User and Modify All Properties (Benutzer erstellen und alle Eigenschaften ändern) Create User and Modify Limited Properties (Benutzer erstellen und begrenzte Eigenschaften ändern)	Enable Email for New User (Email-Funktion für neuen Benutzer aktivieren)
Benutzerkonto erstellen und das neue Konto zu angegebenen Gruppen hinzufügen	Create User and Modify All Properties (Benutzer erstellen und alle Eigenschaften ändern) Create User and Modify Limited Properties (Benutzer erstellen und begrenzte Eigenschaften ändern)	Add New User to Group (Neuen Benutzer zur Gruppe hinzufügen)

12 Delegierungszuweisungen

Delegierungszuweisungen werden über den Knoten **Delegation Management** (Delegierungsverwaltung) > **Assistant Admin** (Hilfsadministrator) in der Delegierungs- und Konfigurationskonsole verwaltet. In diesem Knoten können Sie die Befugnisse und Rollen anzeigen, die den Hilfsadministratoren zugewiesen sind, und die Zuweisung von Rollen und ActiveViews verwalten. Außerdem können Sie die folgenden Aktionen in Bezug auf Hilfsadministratorgruppen ausführen:

- Gruppenmitglieder hinzufügen
- Gruppen erstellen
- Gruppen klonen
- Gruppen löschen
- Gruppeneigenschaften ändern

Um Zuweisungen anzuzeigen und zu verwalten und um Änderungen an den Hilfsadministratorgruppen vorzunehmen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse der Rolle „Manage Security Model“ (Sicherheitsmodell verwalten).

Der allgemeine Workflow zum Ausführen beliebiger in diesem Abschnitt genannter Aktionen besteht im Auswählen des Knotens **Assistant Admins** (Hilfsadministratoren) und Ausführen einer der folgenden Schritte:

- Öffnen Sie über das Aufgabenmenü oder über das Kontextmenü den entsprechenden Assistenten bzw. das Dialogfeld, um die erforderlichen Aktionen abzuschließen.
- Suchen Sie die Gruppe oder den Hilfsadministrator im Bereich **List items that match my criteria** (Objekte auflisten, die mit meinen Kriterien übereinstimmen) und verwenden Sie das Menü **Tasks** (Aufgaben) oder das Kontextmenü, um den entsprechenden Assistenten bzw. das Dialogfeld auszuwählen und zu öffnen und die erforderlichen Aktionen abzuschließen.

V Richtlinien- und Prozessautomatisierung

Dieses Kapitel enthält Informationen über die Funktionsweise von Richtlinien in der DRA-Umgebung und über die verfügbaren Richtlinienoptionen. Außerdem wird beschrieben, wie Auslöser und Workflowautomatisierungen eingesetzt werden, um beim Arbeiten mit Objekten in Active Directory Prozesse zu automatisieren.

13 Grundlegendes zu DRA-Richtlinien

Mit DRA können Sie verschiedene Richtlinien konfigurieren, um die Sicherheit im Unternehmen zu erhöhen und die Beschädigung von Daten zu verhindern. Diese Richtlinien funktionieren im Kontext des dynamischen Sicherheitsmodells, das sicherstellt, dass die Richtlinienerzwingung bei Änderungen im Unternehmen schnell angepasst werden kann. Durch das Erstellen von Richtlinien wie Benennungskonventionen, Grenzwerte für die Speicherplatzauslastung und Eigenschaftenvalidierungen können Sie die Einhaltung von Regeln erzwingen, die zur Erhaltung der Datenintegrität im Unternehmen beitragen.

In DRA können Sie Richtlinienregeln für die folgenden Unternehmensbereiche schnell erstellen:

- Microsoft Exchange
- Office 365- Lizenz
- Basisverzeichnis
- Passwortgenerierung

DRA stellt außerdem integrierte Richtlinien für Gruppen, Benutzerkonten und Computer zur Verfügung.

Um Richtlinien zu verwalten oder zu definieren, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse der Rolle „DRA Administration“ (Verwaltung von DRA) oder „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten). Der Bericht „Policy Details“ in DRA unterstützt Sie bei der Verwaltung der Richtlinien. Dieser Bericht enthält die folgenden Informationen:

- Gibt an, ob die Richtlinie aktiviert ist
- Führt die verknüpften Vorgänge auf
- Führt die von der Richtlinie geregelten Objekte auf
- Liefert Details zum Umfang der Richtlinie

Verwenden Sie diesen Bericht, um sicherzustellen, dass die Richtlinien richtig definiert sind. Sie können den Bericht auch dazu verwenden, Richtlinieneigenschaften zu vergleichen, Konflikte zu ermitteln oder die Erzwingung der Richtlinien im Unternehmen zur verbessern.

Erzwingung von Richtlinien durch den Verwaltungsserver

Sie können jede Aufgabe bzw. jeden administrativen Vorgang mit einer oder mehreren Richtlinien verknüpfen. Wenn Sie einen Vorgang ausführen, der mit einer Richtlinie verknüpft ist, führt der Verwaltungsserver die Richtlinie aus und erzwingt die angegebenen Regeln. Wenn der Server eine Richtlinienverletzung erkennt, gibt er eine Fehlermeldung zurück. Wenn der Server keine

Richtlinienverletzung erkennt, führt er den angeforderten Vorgang aus. Sie können den Umfang einer Richtlinie begrenzen, indem Sie sie mit bestimmten ActiveViews oder Hilfsadministratorgruppen verknüpfen.

Wenn ein Vorgang mit mehr als einer Richtlinie verknüpft ist, erzwingt der Verwaltungsserver die Richtlinien in alphabetischer Reihenfolge. Das heißt, dass die Richtlinie A unabhängig von den angegebenen Regeln vor der Richtlinie B erzwungen wird.

Halten Sie sich an den folgenden Leitfaden, sicherzustellen, dass die Richtlinien nicht miteinander in Konflikt geraten:

- Benennen Sie die Richtlinien so, dass sie in der richtigen Reihenfolge ausgeführt werden.
- Stellen Sie sicher, dass keine der Richtlinien mit Überprüfungen oder Aktionen anderer Richtlinien interferiert.
- Testen Sie benutzerdefinierte Richtlinien gründlich, bevor Sie sie in der Produktionsumgebung implementieren.

Der Verwaltungsserver trägt den Richtlinienstatus bei jeder Richtlinienausführung in das Revisionsprotokoll ein. Diese Protokolleinträge enthalten einen Rückgabecode und Informationen über die verknüpften Vorgänge, die behandelten Objekte und den Erfolg der Ausführung der benutzerdefinierten Richtlinie.

WARNUNG: Richtlinien werden mit dem DRA-Servicekonto ausgeführt. Da das Servicekonto über Administratorberechtigungen verfügt, haben Richtlinien vollen Zugriff auf alle Unternehmensdaten. Aus diesem Grund können Hilfsadministratoren, denen die integrierte Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) zugewiesen ist, unter Umständen über höhere Befugnisse als beabsichtigt verfügen.

Integrierte Richtlinien

Integrierte Richtlinien werden bei der Installation des Verwaltungsservers implementiert. Bei der Arbeit mit diesen Richtlinien sind Sie möglicherweise mit den folgenden Begriffen konfrontiert:

Richtlinienumfang

Legt die Objekte oder Eigenschaften fest, auf die DRA die Richtlinie anwendet. Bestimmte Richtlinien ermöglichen Ihnen beispielsweise das Anwenden einer Richtlinie auf bestimmte Hilfsadministratoren in bestimmten Aktivansichten. Bei anderen Richtlinien können Sie aus verschiedenen Objektklassen auswählen, wie Benutzerkonten oder Gruppen.

Globale Richtlinien

Erzwingen Richtlinienregeln auf allen Objekten der spezifizierten Klasse oder des spezifizierten Typs in den verwalteten Domänen. Bei globalen Richtlinien können Sie den Richtlinienumfang der Objekte, auf die die Richtlinie angewendet wird, nicht eingrenzen.

Richtlinienbeziehung

Legt fest, ob die Richtlinie in Verbindung mit anderen Richtlinien oder eigenständig angewendet wird. Um eine Richtlinienbeziehung zu erstellen, definieren Sie zwei oder mehr Regeln, die auf die gleiche Aktion angewendet werden, und wählen Sie die Option „Mitglied einer Richtliniengruppe“. Wenn die Vorgangsparameter oder Eigenschaften mit einer der Regeln übereinstimmen, ist der Vorgang erfolgreich.

Themen zu integrierten Richtlinien:

Grundlegendes zu integrierten Richtlinien

Integrierte Richtlinien stellen Geschäftsregeln zur Bewältigung allgemeiner Aspekte in Bezug auf die Gewährleistung der Sicherheit und der Datenintegrität bereit. Diese Richtlinien sind Bestandteil des standardmäßigen Sicherheitsmodells und ermöglichen die Integration der DRA-Sicherheitsfunktionen in die vorhandene Unternehmenskonfiguration.

DRA bietet zwei Möglichkeiten zum Erzwingen von Richtlinien. Sie können benutzerdefinierte Richtlinien erstellen oder aus verschiedenen integrierten Richtlinien wählen. Die integrierten Richtlinien ermöglichen ein einfaches Anwenden von Richtlinien, ohne dass benutzerdefinierte Skripte entwickelt werden müssen. Wenn Sie eine benutzerdefinierte Richtlinie müssen, können Sie eine vorhandene integrierte Richtlinie verwenden und an Ihre Anforderungen anpassen. Für die meisten Richtlinien können Sie den Fehlermeldungstext ändern, die Richtlinie umbenennen, eine Beschreibung hinzufügen und festlegen, wie die Richtlinie angewendet werden soll.

Bei der Installation von DRA werden mehrere integrierte Richtlinien aktiviert. Die folgenden Richtlinien werden standardmäßig implementiert. Wenn Sie diese Richtlinien nicht erzwingen möchten, können Sie sie deaktivieren oder löschen.

Richtlinienname	Standardwert	Beschreibung
$ComputerNameLengthPolicy	64 15 (vor Windows 2000)	Begrenzt die Anzahl der Zeichen im Computernamen bzw. im Computernamen vor Windows 2000
$GroupNameLengthPolicy	64 20 (vor Windows 2000)	Begrenzt die Anzahl der Zeichen im Gruppennamen bzw. im Gruppennamen vor Windows 2000
$GroupSizePolicy	5.000	Begrenzt die Anzahl der Mitglieder in einer Gruppe
$NameUniquenessPolicy	Keine	Stellt sicher, dass Namen vor Windows 2000 und Eigennamen (CN) in allen verwalteten Domänen eindeutig sind
$SpecialGroupsPolicy	Keine	Verhindert die nicht überprüfte Eskalation von Befugnissen in der Umgebung
$UCPowerConflictPolicy	Keine	Verhindert die Eskalation von Befugnissen, indem festgelegt wird, dass sich die Befugnis zum Klonen von Benutzern und die Befugnis zum Erstellen von Benutzern gegenseitig ausschließen

Richtlinienname	Standardwert	Beschreibung
$UPNUniquenessPolicy	Keine	Gewährleistet, dass die UPN-Namen in allen verwalteten Domänen eindeutig sind
$UserNameLengthPolicy	64 20 (Anmeldenamen älterer Systeme)	Beschränkt die Anzahl der Zeichen für den Benutzeranmeldenamen bzw. Benutzeranmeldenamen älterer Systeme

Verfügbare Richtlinien

DRA stellt mehrere Richtlinien bereit, die Sie für ihr Sicherheitsmodell anpassen können.

HINWEIS: Sie können eine Richtlinie erstellen, die einen Eintrag für eine Eigenschaft erfordert, die über die DRA-Benutzeroberflächen zurzeit nicht verfügbar ist. Wenn die Richtlinie einen Eintrag erfordert und die Benutzeroberfläche kein Feld zur Eingabe des Werts bereitstellt, beispielsweise ein Abteilungsfeld für ein neues Benutzerkonto, können Sie das Objekt nicht erstellen oder verwalten. Um dieses Problem zu verhindern, konfigurieren Sie Richtlinien, die nur Eigenschaften erfordern, auf die über die Benutzeroberfläche zugegriffen werden kann.

Create a Custom Policy (Benutzerdefinierte Richtlinie erstellen)

Sie können ein Skript oder ein ausführbares Programm mit einem DRA- oder Exchange-Vorgang verknüpfen. Mit benutzerdefinierten Richtlinien können Sie beliebige Vorgänge bestätigen.

Enforce a Maximum Name Length (Höchstlänge für Namen erzwingen)

Sie können global eine Höchstlänge für Namen von Benutzerkonten, Gruppen, organisatorischen Einheiten, Kontakten oder Computern erzwingen.

Die Richtlinie überprüft den Namencontainer (Eigenname oder cn für „Common Name“) und den Namen aus Systemen vor Windows 2000 (Benutzeranmeldenamen).

Enforce Maximum Number of Group Members (Höchstanzahl an Gruppenmitgliedern erzwingen)

Sie können global einen Grenzwert für die Anzahl der Mitglieder in einer Gruppe erzwingen.

Enforce Unique Pre-Windows 2000 Account Names (Eindeutige Kontonamen aus Systemen vor Windows 2000 erzwingen)

Diese Richtlinie gewährleistet, dass Namen vor Windows 2000 in allen verwalteten Domänen eindeutig sind. In Microsoft Windows-Domänen müssen Namen vor Windows 2000 innerhalb einer Domäne eindeutig sein. Diese globale Richtlinie erzwingt diese Regel in allen verwalteten Domänen.

Enforce unique User Principal Names (UPNs) (Eindeutige Benutzerprinzipalnamen (UPN) erzwingen)

Diese Richtlinie gewährleistet, dass Benutzerprinzipalnamen (UPN) in allen verwalteten Domänen eindeutig sind. In Microsoft Windows-Domänen müssen Benutzerprinzipalnamen innerhalb einer Domäne eindeutig sein. Diese Richtlinie erzwingt diese Regel in allen verwalteten Domänen. Weil dies eine globale Richtlinie ist, stellt DRA den Richtliniennamen, die Richtlinienbeschreibung und die Richtlinienbeziehung bereit.

Limit actions on members of special groups (Aktionen für Mitglieder spezieller Gruppen einschränken)

Diese Richtlinie verhindert, dass der Benutzer Mitglieder einer Administratorgruppe verwaltet, sofern er nicht selbst Mitglied dieser Administratorgruppe ist. Diese globale Richtlinie ist standardmäßig aktiviert.

Wenn Sie Aktionen für Mitglieder der Administratorgruppe einschränken, sind im Assistenten zum Erstellen von Richtlinien keine weiteren Informationen erforderlich. Sie können eine benutzerdefinierte Fehlermeldung angeben. Weil dies eine globale Richtlinie ist, stellt DRA den Richtliniennamen, die Richtlinienbeschreibung und die Richtlinienbeziehung bereit.

Prevent assistant administrators from Creating and Cloning Users in Same AV (Verhindern, dass Hilfsadministratoren Benutzer in der gleichen Aktivansicht erstellen und klonen)

Diese Richtlinie verhindert eine mögliche Eskalation von Befugnissen. Wenn diese Richtlinie aktiviert ist, können Sie entweder Benutzerkonten erstellen oder Benutzerkonten klonen. Sie können jedoch nicht gleichzeitig über beide Befugnisse verfügen. Diese globale Richtlinie gewährleistet, dass Sie keine Benutzerkonten in der gleichen ActiveView erstellen und klonen können.

Die Richtlinie erfordert keine zusätzlichen Informationen.

Set Naming Convention Policy (Richtlinie für Benennungskonvention festlegen)

Sie können Benennungskonventionen festlegen, die für bestimmte Hilfsadministratoren, Aktivansichten und Objektklassen wie Benutzerkonten oder Gruppen gelten.

Sie können auch die genauen Namen angeben, die von dieser Richtlinie überwacht werden.

Create a Policy to Validate a Specific Property (Richtlinie zum Überprüfen einer bestimmten Eigenschaft erstellen)

Sie können eine Richtlinie erstellen, die eine beliebige Eigenschaft einer organisatorischen Einheit oder eines Kontoobjekts überprüft. Sie können hierzu einen Standardwert, eine Eigenschaftsformatmaske und gültige Werte bzw. Bereiche angeben.

Verwenden Sie diese Richtlinie, um die Datenintegrität zu erzwingen, indem Sie bestimmte Eingabefelder beim Erstellen, Klonen oder Ändern der Eigenschaften bestimmter Objekte überprüfen. Diese Richtlinie bietet eine herausragende Flexibilität und Leistungsfähigkeit für das Bestätigen von Eingaben, Angeben von Standardeinträgen und Begrenzen der Eingabeauswahl für verschiedene Eigenschaftenfelder. Mit dieser Richtlinie können Sie die Richtigkeit einer Eingabe erzwingen, bevor eine Aufgabe abgeschlossen wird, und so die Datenintegrität in den verwalteten Domänen erhalten.

Nehmen Sie beispielsweise an, dass Sie drei Abteilungen haben: Fertigung, Vertrieb und Verwaltung. Sie können die Einträge, die DRA akzeptiert, auf diese drei Werte beschränken. Sie können diese Richtlinie auch dazu verwenden, das richtige Telefonnummernformat zu erzwingen, einen gültigen Wertebereich bereitzustellen oder eine Eingabe in einem Email-Adressfeld zu erzwingen. Um mehrere Formatmasken für eine Telefonnummer anzugeben, zum Beispiel `(123)456 7890` und `456 7890`, definieren Sie die Eigenschaftsformatmaske als `(###)### ####,### ####`.

Create Policy to Enforce Office 365 Licenses (Richtlinie zum Erzwingen von Office 365-Lizenzen)

Sie können eine Richtlinie erstellen, um Office 365-Lizenzen basierend auf der Mitgliedschaft in einer Active Directory-Gruppe zuzuweisen. Diese Richtlinie erzwingt außerdem das Entfernen der Office 365-Lizenz, wenn ein Mitglied aus der entsprechenden Active Directory-Gruppe entfernt wird.

Wenn ein Benutzer, der nicht mit der Cloud synchronisiert ist, zur Active Directory-Gruppe hinzugefügt wird, wird der Benutzer synchronisiert, bevor ihm eine Office 365-Lizenz zugewiesen wird.

Während der Erstellung der Richtlinie können Sie bestimmte Eigenschaften und Einstellungen festlegen, wie den Namen der Richtlinie und den Text der Fehlermeldung, der angezeigt wird, wenn ein Hilfsadministrator versucht, eine Aktion auszuführen, die diese Richtlinie verletzt.

Die Einstellung **Ensure only licenses assigned by DRA policies are enabled on accounts. All other licenses will be removed.** (Sicherstellen, dass nur Lizenzen, die durch DRA-Richtlinien zugewiesen werden, für die Konten aktiviert sind. Alle anderen Lizenzen werden entfernt.) ist auf der Seite „Tenant Properties“ (Mandanteneigenschaften) enthalten, die pro Mandant konfiguriert werden kann. Diese Einstellung wird für DRA Office 365-Lizenzrichtlinien zur Konfiguration der Erzwingung von Lizenzzuweisungen verwendet:

Wenn diese Einstellung aktiviert ist, stellt die DRA-Lizenzerzwingung sicher, dass nur Lizenzen, die über DRA-Richtlinien zugewiesen werden, für die Konten bereitgestellt werden (außerhalb von DRA zugewiesene Lizenzen werden von den Konten, die der Lizenzrichtlinien zugewiesen sind, entfernt). Wenn diese Einstellung deaktiviert ist (Standardeinstellung), stellt die DRA-Lizenzerzwingung nur sicher, dass die spezifischen Lizenzen, die Sie in die Office 365-Richtlinien eingeschlossen haben, für die Konten bereitgestellt werden (wenn die Zuweisung eines Kontos zu einer Lizenzrichtlinie aufgehoben wird, wird nur die Bereitstellung der durch diese Richtlinie zugewiesenen Lizenzen aufgehoben).

Arbeiten mit integrierten Richtlinien

Integrierte Richtlinien sind Bestandteil des standardmäßigen Sicherheitsmodells. Sie können diese Richtlinien zum Erzwingen des aktuellen Sicherheitsmodells verwenden oder sie an Ihre besonderen Anforderungen anpassen. Sie können den Namen, die Regeleinstellungen, den Umfang, die Richtlinienbeziehung und die Fehlermeldung verschiedener integrierter Richtlinien ändern. Sie können jede integrierte Richtlinie aktivieren oder deaktivieren.

Außerdem können Sie ganz einfach neue Richtlinien erstellen.

Implementieren einer benutzerdefinierten Richtlinie

Mit benutzerdefinierten Richtlinien können Sie die Leistungsfähigkeit und Flexibilität des standardmäßigen Sicherheitsmodells optimal nutzen. Mithilfe von benutzerdefinierten Richtlinien können Sie DRA mit vorhandenen Unternehmenskomponenten integrieren und sicherstellen, dass die proprietären Regeln erzwungen werden. Mit der Funktion der benutzerdefinierten Richtlinien können Sie Ihre Unternehmensrichtlinien erweitern.

Um benutzerdefinierte Richtlinien zu erstellen und zu erzwingen, verknüpfen Sie ein ausführbares Programm oder ein Skript mit einem Verwaltungsvorgang. Beispielsweise könnten Sie ein Richtlinienskript verwenden, das mit dem Vorgang `UserCreate` (Benutzer erstellen) verknüpft ist und in der Personaldatenbank überprüft, ob ein angegebener Mitarbeiter vorhanden ist. Wenn der Mitarbeiter in der Personaldatenbank vorhanden ist, aber kein vorhandenes Konto hat, ruft das Skript die Mitarbeiter-ID, seinen Vornamen und seinen Nachnamen aus der Datenbank ab. Der Vorgang wird erfolgreich ausgeführt und füllt die richtigen Informationen in das Eigenschaftenfenster des Benutzerkontos ein. Wenn der Mitarbeiter bereits über ein Konto verfügt, schlägt der Vorgang fehl.

Skripte bieten eine herausragende Flexibilität und Leistungsfähigkeit. Sie können eigene Richtlinienskripte mit Directory and Resource Administrator ADSI Provider (ADSI-Anbieter), Software Development Kit (SDK) und PowerShell-Cmdlets erstellen. Weitere Informationen über das Erstellen Ihrer eigenen Richtlinien Skripte finden Sie im Referenzabschnitt auf der Website der DRA-Dokumentation.

Einschränken nativer integrierter Sicherheitsgruppen

Um eine sicherere Umgebung bereitzustellen, bietet Ihnen DRA die Möglichkeit, die Befugnisse der in Microsoft Windows integrierten Sicherheitsgruppen einzuschränken. Die Möglichkeit, Gruppenmitgliedschaften, die Eigenschaften integrierter Sicherheitsgruppen oder die Eigenschaften der Gruppenmitglieder ändern zu können, kann wichtige Auswirkungen auf die Sicherheit haben. Wenn Sie beispielsweise das Passwort in der Gruppe der Serveroperatoren ändern, können Sie sich anschließend als dieser Benutzer anmelden und die Befugnisse nutzen, die dieser integrierten Sicherheitsgruppe zugewiesen sind.

DRA verhindert dieses Sicherheitsproblem mithilfe einer Richtlinie, die Ihre Befugnisse über die nativen integrierten Sicherheitsgruppen und deren Mitglieder überprüft. Diese Bestätigung gewährleistet, dass die angeforderten Aktionen keine Befugniseskalation bewirken. Wenn Sie diese Richtlinie aktivieren, kann ein Hilfsadministrator, der Mitglied einer integrierten Sicherheitsgruppe ist, beispielsweise Mitglied der Gruppe der Serveroperatoren, nur die anderen Mitglieder der gleichen Gruppe verwalten.

Einschränkbare native integrierte Sicherheitsgruppen

Mit DRA-Richtlinien können Sie die Befugnisse der folgenden integrierten Microsoft Windows-Sicherheitsgruppen einschränken:

- Konten-Operatoren
- Administratoren
- Sicherungs-Operatoren
- Zertifikatherausgeber
- DNS-Administratoren
- Domänenadministratoren
- Organisations-Admins
- Richtlinien-Ersteller-Besitzer
- Druck-Operatoren
- Schema-Admins

HINWEIS: DRA verwendet die internen IDs zur Bezugnahme auf integrierte Sicherheitsgruppen. DRA unterstützt diese Gruppen also auch dann, wenn sie umbenannt wurden. Diese Funktion gewährleistet, dass DRA integrierte Sicherheitsgruppen unterstützt, die in verschiedenen Ländern verschiedene Bezeichnungen tragen. DRA nimmt beispielsweise mit der gleichen internen ID Bezug auf die Gruppe „Administratoren“ und auf die Gruppe *Administrators*.

Einschränken der Aktionen auf nativen integrierten Sicherheitsgruppen

Mithilfe einer Richtlinie beschränkt DRA die Befugnisse, die von den nativen integrierten Sicherheitsgurten und deren Mitgliedern ausgeübt werden können. Diese Richtlinie, `$SpecialGroupsPolicy`, schränkt die Aktionen ein, die ein Mitglied einer nativen integrierten Sicherheitsgruppe auf andere Mitglieder oder andere native integrierte Sicherheitsgruppen ausführen kann. Diese Richtlinie ist in DRA standardmäßig aktiviert. Wenn Sie die Aktionen für native integrierte Sicherheitsgruppen und deren Mitglieder nicht einschränken möchten, können Sie diese Richtlinie deaktivieren.

Wenn diese Richtlinie aktiviert ist, verwendet DRA die folgenden Validierungstests, um zu bestimmen, ob eine Aktion auf eine native integrierte Sicherheitsgruppe oder deren Mitglieder zulässig ist:

- Wenn Sie ein Microsoft Windows-Administrator sind, können Sie Aktionen auf native integrierte Sicherheitsgruppen und deren Mitglieder ausführen, für die Sie über die entsprechenden Befugnisse verfügen.
- Wenn Sie Mitglied einer integrierten Sicherheitsgruppe sind, können Sie Aktionen auf die gleiche integrierte Sicherheitsgruppe und auf deren Mitglieder ausführen, sofern Sie über die entsprechenden Befugnisse verfügen.
- Wenn Sie kein Mitglied einer integrierten Sicherheitsgruppe sind, können Sie keine integrierte Sicherheitsgruppe und keine ihrer Mitglieder ändern.

Wenn Sie beispielsweise Mitglied der Gruppen der Serveroperatoren und der Kontenoperatoren sind und über die entsprechenden Befugnisse verfügen, können Sie Aktionen für Mitglieder der Gruppe der Serveroperatoren, Mitglieder der Gruppe der Kontenoperatoren und Mitglieder beider Gruppen ausführen. Sie können jedoch keine Aktionen für ein Benutzerkonto ausführen, das Mitglied der Gruppe der Druckoperatoren und der Gruppe der Kontenoperatoren ist.

DRA verhindert, dass Sie die folgenden Aktionen in nativen integrierten Sicherheitsgruppen ausführen:

- Gruppen klonen
- Gruppen erstellen
- Gruppen löschen
- Mitglieder zu einer Gruppe hinzufügen
- Mitglieder aus einer Gruppe entfernen
- Gruppen in eine organisatorische Einheit verschieben
- Eigenschaften einer Gruppe ändern
- Postfächer kopieren
- Postfächer entfernen
- Benutzerkonten klonen
- Benutzerkonten erstellen
- Benutzerkonten löschen
- Benutzerkonten in eine organisatorische Einheit verschieben
- Benutzerkontoeigenschaften ändern

DRA schränkt außerdem die Aktionen ein, um sicherzustellen, dass keine Befugnisse über ein Objekt erlangt werden. Wenn Sie beispielsweise ein Benutzerkonto zu einer Gruppe hinzufügen, überprüft DRA, ob Sie dadurch zusätzliche Befugnisse über das Benutzerkonto erhalten. Diese Überprüfung trägt zum Schutz vor einer Befugniseskalation bei.

Verwalten von Richtlinien

Über den Knoten „Richtlinien- und Automatisierungsmanagement“ können Sie auf Richtlinien für Microsoft Exchange und für das Basisverzeichnis sowie auf integrierte und benutzerdefinierte Richtlinien zugreifen. Mit den folgenden allgemeinen Aufgaben können Sie die Sicherheit und Datenintegrität im Unternehmen verbessern.

Configure Exchange Policies (Exchange-Richtlinien konfigurieren)

Sie können Regeln für die Microsoft Exchange-Konfiguration, Postfachrichtlinien, automatische Benennung und Vertretungserzeugung definieren. Mit diesen Regeln kann definiert werden, wie Postfächer verwaltet werden, wenn ein Hilfsadministrator ein Benutzerkonto erstellt, ändert oder löscht.

Configure Home Directory Policies (Richtlinien für Basisverzeichnis konfigurieren)

Mit dieser Aufgabe können Sie Basisverzeichnisse und Basisfreigaben automatisch erstellen, umbenennen oder löschen, wenn ein Hilfsadministrator ein Benutzerkonto erstellt, umbenennt oder löscht. Mit der Basisverzeichnisrichtlinie können Sie außerdem die Unterstützung für ein Speicherplatzkontingent für Basisverzeichnisse auf Microsoft Windows-Servern und auf Nicht-Windows-Servern aktivieren oder deaktivieren.

Configure Password Generation Policies (Richtlinien für die Passwortgenerierung konfigurieren)

Mit dieser Aufgabe können Sie die Anforderungen für Passwörter, die von DRA generiert werden, definieren.

Ausführlichere Informationen zum Verwalten von Richtlinien in DRA finden Sie in den folgenden Abschnitten:

- „Microsoft Exchange-Richtlinie“, auf Seite 141
- „Office 365-Lizenzrichtlinie“, auf Seite 143
- „Erstellen und Implementieren einer Basisverzeichnis-Richtlinie“, auf Seite 144
- „Passwortgenerierung zulassen“, auf Seite 151
- „Richtlinienaufgaben“, auf Seite 151

Microsoft Exchange-Richtlinie

Exchange stellt mehrere Richtlinien bereit, mit denen Sie Microsoft Exchange-Objekte effizienter verwalten können. Mit der Microsoft Exchange-Richtlinie können Sie die Postfachverwaltung automatisieren, Benennungskonventionen für Aliasse erzwingen und Postfachspeicher erzwingen und automatisch Email-Adressen erzeugen.

Mit diesen Richtlinien können Sie Ihre Workflows optimieren und die Datenintegrität erhalten. Beispielsweise können Sie festlegen, wie Exchange Postfächer verwaltet, wenn Sie Benutzerkonten erstellen, ändern oder löschen. Zum Definieren und Verwalten von Microsoft Exchange-Richtlinien

müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten).

Festlegen einer standardmäßigen Richtlinie für Email-Adressen

Um eine standardmäßige Email-Adress-Richtlinie festzulegen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse, die in der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) enthalten sind. Außerdem muss Ihre Lizenz das Exchange-Produkt unterstützen.

So legen Sie eine standardmäßige Email-Adress-Richtlinie fest:

1. Navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Configure Exchange Policies** (Exchange-Richtlinien konfigurieren) > **Proxy Generation** (Stellvertretungserzeugung).
2. Geben Sie die Domäne des Microsoft Exchange-Servers an.
   - **2a** Klicken Sie auf **Durchsuchen**.
   - **2b** Geben Sie je nach Bedarf zusätzliche Suchkriterien ein und klicken Sie dann auf **Find Now** (Jetzt suchen).
   - **2c** Wählen Sie die zu konfigurierende Domäne aus und klicken Sie auf **OK**.
3. Geben Sie die Regeln für die Vertretungsgenerierung für die ausgewählte Domäne an.
   - **3a** Klicken Sie auf **Hinzufügen**.
   - **3b** Wählen Sie einen Vertretungstyp aus. Klicken Sie beispielsweise auf **Internetadresse**.
   - **3c** Akzeptieren Sie den Standardwert oder geben Sie eine neue Regel für die Vertretungsgenerierung ein und klicken Sie dann auf **OK**.

     Weitere Informationen zu den unterstützten Ersetzungszeichenfolgen für Vertretunsgenerierungsregeln finden Sie in Richtlinie des Delegierungs- und Konfigurationsclients.
4. Klicken Sie auf **Benutzerdefinierte Attribute**, um den benutzerdefinierten Namen der benutzerdefinierten Postfacheigenschaften zu bearbeiten.
   - **4a** Wählen Sie das Attribute aus und klicken Sie auf die Schaltfläche **Bearbeiten**.
   - **4b** Geben Sie im Fenster der Attributeigenschaften den Attributnamen in das Feld **Custom name** (Benutzerdefinierter Name) ein und klicken Sie auf **OK**.
5. Klicken Sie auf **OK**.

HINWEIS: DRA-Richtlinienadministratoren sollten über die Befugnis *Manage Custom Tools* (Benutzerdefinierte Tools verwalten) verfügen, um benutzerdefinierte Attribute in der Microsoft Excel-Richtlinie zu ändern.

Postfachregeln

Mit Postfachregeln können Sie festlegen, wie Exchange Postfächer verwaltet, wenn Hilfsadministratoren Benutzerkonten erstellen, klonen, ändern oder löschen. Postfachregeln verwalten die Microsoft Exchange-Postfächer automatisch auf Grundlage der Verwaltung der verknüpften Benutzerkonten durch die Hilfsadministratoren.

HINWEIS: Wenn Sie die Option **Do not allow Assistant Admins to create a user account without a mailbox** (Nicht zulassen, dass Hilfsadministratoren Benutzerkonten ohne Postfach erstellen) in Microsoft Windows-Domänen aktivieren, stellen Sie sicher, dass der Hilfsadministrator über die Befugnis entweder zum Klonen oder zum Erstellen eines Benutzerkontos verfügt. Wenn diese Option aktiviert ist, können die Hilfsadministratoren Windows-Benutzerkonten nur mit einem Postfach erstellen.

Um Microsoft Exchange-Postfachregeln festzulegen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse, die in der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) enthalten sind. Außerdem muss Ihre Lizenz das Exchange-Produkt unterstützen.

So legen Sie Exchange-Postfachregeln fest:

1. Navigieren Sie zu **Richtlinien- und Automatisierungsmanagement** > **Configure Exchange Policies** (Exchange-Richtlinien konfigurieren) > **Mailbox Rules** (Postfachregeln).
2. Wählen Sie die Postfachrichtlinien aus, die Exchange erzwingen soll, wenn Benutzerkonten erstellt oder geändert werden.
3. Klicken Sie auf **OK**.

Office 365-Lizenzrichtlinie

Zum Festlegen von Office 365-Lizenzrichtlinien müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten). Außerdem muss Ihre Lizenz das Microsoft Exchange-Produkt unterstützen.

Verwaltung der Office 365-Lizenzen durch DRA zulassen (optional)

Wenn Sie zulassen möchten, dass DRA die Office 365-Lizenzen verwaltet, führen Sie die folgenden Schritte aus:

- Erstellen Sie eine Lizenzerzwingungsrichtlinie.
- Aktivieren Sie **License update schedule** (Lizenzaktualisierungszeitplan) auf der Mandanteneigenschaftenseite.

Richtlinie zum Erzwingen der Office 365-Lizenzen erstellen

Um eine Richtlinie für das Erzwingen von Office 365-Lizenzen zu erstellen, klicken Sie auf den Knoten **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) in der Delegierungs- und Konfigurationskonsole und wählen Sie **New Policy** > **Create New Policy to Enforce Office 365 Licenses** (Neue Richtlinie > Neue Richtlinie zum Erzwingen von Office 365-Lizenzen erstellen) aus.

Wenn die Richtlinie erzwungen ist und ein Benutzer zu Active Directory hinzugefügt wird, weist DRA dem Benutzer basierend auf der Gruppenmitgliedschaft automatisch die Office 365-Lizenz zu.

Office 365-Lizenzaktualisierungszeitplan

Richtlinien, die Sie zum Erzwingen von Office 365-Lizenzen erstellen, werden nicht angewendet, wenn Änderungen außerhalb von DRA vorgenommen werden, es sei denn, Sie aktivieren außerdem **License update schedule** (Lizenzaktualisierungszeitplan) auf der Mandanteneigenschaftenseite. Der Lizenzaktualisierungsauftrag gewährleistet, dass die Office 365-Lizenzen, die den Benutzern zugewiesen sind, mit den Office 365-Lizenzrichtlinien übereinstimmen.

Der Lizenzaktualisierungsauftrag und die Office 365-Lizenzrichtlinien stellen gemeinsam sicher, dass allen verwalteten Benutzern nur die beabsichtigten Office 365-Lizenzen zugewiesen sind.

HINWEIS

- DRA verwaltet keine Office 365-Lizenzen für reine Online-Benutzerkonten. Damit DRA die Benutzer mit Office 365-Lizenzen verwaltet, müssen diese Benutzer mit Active Directory synchronisiert sein.
- Wenn Sie die Office 365-Lizenzen mit DRA verwalten, überschreibt DRA bei jeder jeweils nächsten Ausführung des Lizenzaktualisierungszeitplans alle manuellen Änderungen an Office 365-Lizenzen, die außerhalb von DRA vorgenommen wurden.
- Wenn Sie den Office 365-Lizenzaktualisierungsauftrag aktivieren, bevor Sie sicherstellen, dass die Office 365-Lizenzrichtlinien richtig konfiguriert sind, können die zugewiesenen Lizenzen nach dem Ausführen des Lizenzaktualisierungszeitplans falsch sein.

Erstellen und Implementieren einer Basisverzeichnis-Richtlinie

Wenn Sie eine große Anzahl an Benutzerkonten verwalten, kann das Erstellen und Pflegen der Basisverzeichnisse und Freigaben sehr zeitaufwendig und eine Quelle von Sicherheitsfehlern sein. Jedes Mal, wenn ein Benutzer erstellt, umbenannt oder gelöscht wird, ist möglicherweise eine zusätzliche Wartung erforderlich. Die Basisverzeichnisrichtlinien unterstützen Sie beim Warten der Basisverzeichnisse und Basisfreigaben.

Mit DRA können Sie das Erstellen und Pflegen von Benutzerbasisverzeichnissen automatisieren. Sie können DRA beispielsweise ganz einfach so konfigurieren, dass der Verwaltungsserver ein Basisverzeichnis erstellt, wenn ein Benutzerkonto erstellt wird. Wenn Sie beim Erstellen eines Benutzerkontos einen Basisverzeichnispfad angeben, erstellt der Server in diesem Fall automatisch das Basisverzeichnis am festgelegten Pfad. Wenn Sie keinen Pfad angeben, erstellt der Server kein Basisverzeichnis.

DRA unterstützt DFS-Pfade (Distributed File System) für das Erstellen von Benutzerbasisverzeichnissen und das Konfigurieren der Basisverzeichnisrichtlinien für Benutzer in zulässigen übergeordneten Pfaden. Sie können Basisverzeichnisse in Netapp Filers und DFS-Pfade oder Partitionen erstellen, umbenennen und löschen.

Richtlinien für Basisverzeichnisse konfigurieren

Zum Konfigurieren von Richtlinien für Basisverzeichnisse, Freigaben und Volume-Speicherplatzkontingenten müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien

und Automatisierungsauslöser verwalten). Jede Richtlinie verwaltet basierend auf der Verwaltung der verknüpften Benutzerkonten automatisch die Basisverzeichnisse, Freigaben und Volume-Speicherplatzkontingente.

Um Richtlinien für Basisverzeichnisse zu konfigurieren, navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Configure Home Directory Policies** (Richtlinien für Basisverzeichnis konfigurieren) >

- Home directory (Basisverzeichnis)
- Home share (Basisfreigabe)
- Home Volume Disk Quota (Basis-Volume-Speicherplatzkontingent)

Anforderungen an den Verwaltungsserver

Das Servicekonto oder Zugriffskonto des Verwaltungsservers sollte auf jedem Computer, auf dem ein Basisverzeichnis erstellt werden soll, ein Administrator oder Mitglied der Administratorengruppe in der entsprechenden Domäne sein.

Für jedes Laufwerk, für das DRA Basisverzeichnisse verwaltet und speichert, muss eine Verwaltungsfreigabe wie C$ oder D$ vorhanden sein. DRA verwendet die Verwaltungsfreigaben zum Ausführen von Automatisierungsaufgaben für Basisverzeichnisse und Basisfreigaben. Wenn diese Freigaben nicht vorhanden sind, kann DRA keine Automatisierung für Basisverzeichnisse und Basisfreigaben bereitstellen.

Zulässige Basisverzeichnispfade für NetApp Filer konfigurieren

So konfigurieren Sie die zulässigen übergeordneten Pfade für NetApp Filer:

1. Navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Configure Home Directory Policies** (Basisverzeichnisrichtlinien konfigurieren).
2. Geben Sie im Textfeld **Allowable parent paths** (Zulässige übergeordnete Pfade) einen der zulässigen Pfade aus der folgenden Tabelle ein:

Freigabetyp	Zulässiger Pfad
Windows	(*FileName*\adminshare:\volumerootpath*directorypath*)
Andere Systeme	(*non-windows**share*)

3. Klicken Sie auf **Hinzufügen**.
4. Wiederholen Sie die Schritte 1–3 für jeden zulässigen übergeordneten Pfad, an dem die Basisverzeichnisrichtlinien angewendet werden sollen.

Grundlegendes zu Basisverzeichnisrichtlinien

Um die Konsistenz mit richtigen Microsoft Windows-Sicherheitsrichtlinien zu erhalten, erstellt DRA Zugriffssteuerungseinschränkungen nur auf der Verzeichnisebene. Das Einrichten von Zugriffssteuerungseinschränkungen auf Ebene des Freigabenamens und auf Ebene des Datei- oder Verzeichnisobjekts führt für Administratoren und Benutzer oft zu verwirrenden Zugriffsschemen.

Wenn Sie die Zugriffssteuerungseinschränkung für ein Basisverzeichnis ändern, ändert DRA nicht die vorhandene Sicherheit für das Verzeichnis. In diesem Fall müssen Sie sicherstellen, dass die Benutzerkonten über entsprechenden Zugriff auf ihr eigenes Basisverzeichnis verfügen.

Automatisierung und Regeln für Basisverzeichnisse

DRA automatisiert die Wartungsaufgaben von Basisverzeichnissen, indem es die Basisverzeichnisse verwaltet, wenn ein Benutzerkonto geändert wird. DRA kann verschiedene Aktionen ausführen, wenn ein Benutzerkonto erstellt, geklont, geändert, umbenannt oder gelöscht wird.

Beachten Sie zur erfolgreichen Implementierung einer Basisverzeichnisrichtlinie die folgenden Hinweise:

- Stellen Sie sicher, dass der angegebene Pfad das richtige Format hat.
  - Um einen Pfad für ein einzelnes Basisverzeichnis anzugeben, verwenden Sie eine der Schablonen aus der folgenden Tabelle:

Freigabetyp	Pfadschablone
Windows	`\\computer\share\`. Wenn DRA beispielsweise automatisch ein Basisverzeichnis im Ordner `Home Share` auf dem Computer „server01“ erstellen soll, geben Sie `\\server01\Home Share\` ein.
Andere Systeme	`\\non-windows\share`

  - Um die Basisverzeichnisverwaltung im Stammverzeichnis der entsprechenden Basisfreigabe zu standardisieren, verwenden Sie die UNC-Syntax (UNC: Universal Naming Convention; universelle Benennungskonvention), wie `\\`*server name*`\C:\`*path to root directory*.
  - Um einen Pfad für geschachtelte Basisverzeichnisse anzugeben, verwenden Sie eine der Schablonen aus der folgenden Tabelle:

Freigabetyp	Pfadschablone
Windows	`\\computer\share\first directory\second directory\` Wenn DRA zum Beispiel automatisch ein Basisverzeichnis im vorhandenen Verzeichnis `JSmith\Home Share` unter dem Basisfreigabeordner auf dem Computer `server01` erstellen soll, geben Sie `\\server01\Home Share\JSmith\Home` ein.
Andere Systeme	`\\non-windows\share\first directory\second directory\`

HINWEIS: DRA unterstützt außerdem die folgenden Formate: `\\computer\share\username` und `\\computer\share\%username%`. In beiden Fällen erstellt DRA automatisch ein Basisverzeichnis für das verknüpfte Benutzerkonto.

- Wenn Sie eine Richtlinie oder einen Automatisierungsauslöser zum Verwalten von Basisverzeichnissen in NetApp Filer definieren, müssen Sie für die Verzeichnisspezifikation ein anderes Format verwenden.
  - Wenn Sie NetApp Filer verwenden, geben Sie das übergeordnete Verzeichnis im folgenden Format an: `\\`*FilerName*`\`*adminshare:*`\`*volumerootpat*h`\`*directorypath*
  - Die Variable „adminshare“ ist das ausgeblendete Verzeichnis, das dem Stammvolume in NetApp Filer zugeordnet ist, zum Beispiel *c$*. Wenn der lokale Pfad der Freigabe in NetApp Filer, „usfiler“ genannt, beispielsweise `c$\vol\vol0\mydirectory` ist, können Sie für NetApp Filer den Stammpfad `\\usfiler\c:\vol\vol0\mydirectory` festlegen.
- Um einen DFS-Pfad anzugeben, wenn Sie Benutzerbasisverzeichnisse erstellen oder Basisverzeichnisrichtlinien für Benutzer konfigurieren, verwenden Sie das Format `\\`*server*`\`*root*`\<`*link*`>`, wobei „root“ entweder die verwaltete Domäne oder ein eigenständiges Stammverzeichnis im folgenden Format sein kann: `\\`*FilerName*`\`*adminshare:*`\`*volumerootpath*`\`*directorypath* .
- Erstellen Sie ein freigegebenes Verzeichnis zum Speichern des Basisverzeichnisses für dieses Benutzerkonto.
- Stellen Sie sicher, dass DRA Zugriff auf den im Pfad spezifizierten Computer bzw. die im Pfad spezifizierte Freigabe hat.

Create home directory when user account is created (Basisverzeichnis beim Erstellen des Benutzerkontos erstellen)

Mit dieser Regel erstellt DRA automatisch Basisverzeichnisse für neue Benutzerkonten. Wenn DRA ein Basisverzeichnis erstellt, verwendet der Verwaltungsserver den Pfad, der in den Feldern **Home directory** (Basisverzeichnis) im Assistenten zur Benutzererstellung angegeben ist. Sie können diesen Pfad später über die Profil-Registerkarte im Fenster der Benutzereigenschaften ändern und DRA verschiebt das Basisverzeichnis dann an den neuen Speicherort. Wenn Sie für diese Felder keine Werte angeben, erstellt DRA kein Basisverzeichnis für das Benutzerkonto.

DRA legt die Sicherheit für das neue Verzeichnis basierend auf den unter **Home directory permissions** (Basisverzeichnisberechtigungen) ausgewählten Optionen fest. Mit diesen Optionen können Sie den allgemeinen Zugriff für alle Basisverzeichnisse steuern.

Sie können beispielsweise festlegen, dass Mitglieder der Administratorengruppe Vollzugriff und Mitglieder der Helpdesk-Gruppe Lesezugriff auf die Freigabe haben, in der die Basisverzeichnisse der Benutzer erstellt werden. Wenn DRA dann ein Basisverzeichnis für einen Benutzer erstellt, kann das neue Basisverzeichnis die Rechte des übergeordneten Verzeichnisses erben. Die Mitglieder der Administratorengruppe haben deshalb Vollzugriff auf alle Benutzerbasisverzeichnisse und die Mitglieder der Helpdesk-Gruppe Lesezugriff auf alle Benutzerbasisverzeichnisse.

Wenn das angegebene Basisverzeichnis bereits vorhanden ist, erstellt DRA kein Basisverzeichnis und ändert auch nicht die vorhandenen Verzeichnisberechtigungen.

Rename home directory when user account is created (Basisverzeichnis beim Umbenennen des Benutzerkontos umbenennen)

Mit dieser Regel kann DRA die folgenden Optionen automatisch ausführen:

- Basisverzeichnis erstellen, wenn ein neuer Basisverzeichnispfad angegeben wird
- Basisverzeichnisinhalt verschieben, wenn der Basisverzeichnispfad geändert wird
- Basisverzeichnis umbenennen, wenn das verknüpfte Benutzerkonto umbenannt wird

Wenn Sie ein Benutzerkonto umbenennen, benennt DRA das vorhandene Basisverzeichnis basierend auf dem neuen Kontonamen um. Wenn das vorhandene Basisverzeichnis zurzeit verwendet wird, erstellt DRA ein neues Basisverzeichnis mit dem neuen Namen und ändert das vorhandene Basisverzeichnis nicht.

Wenn Sie den Basisverzeichnispfad ändern, versucht DRA, das angegebene Basisverzeichnis zu erstellen und den Inhalt des vorigen Basisverzeichnisses an den neuen Speicherort zu verschieben. Sie können die Basisverzeichnisrichtlinie auch so konfigurieren, dass beim Erstellen des neuen Basisverzeichnisses der Inhalt des vorigen Basisverzeichnisses nicht verschoben wird. DRA weist außerdem die zugewiesenen Zugriffssteuerungslisten vom vorigen Verzeichnis auf das neue Verzeichnis an. Wenn das angegebene Basisverzeichnis bereits vorhanden ist, erstellt DRA das neue Verzeichnis nicht und ändert auch nicht die vorhandenen Verzeichnisberechtigungen. Wenn das vorige Basisverzeichnis nicht gesperrt ist, wird es von DRA gelöscht.

Wenn DRA das Basisverzeichnis nicht umbenennen kann, versucht DRA, ein neues Basisverzeichnis mit einem neuen Namen zu erstellen und den Inhalt des vorigen Basisverzeichnisses in das neue Basisverzeichnis zu kopieren. Anschließend versucht DRA, das vorige Basisverzeichnis zu löschen. Sie können DRA so konfigurieren, dass der Inhalt des vorigen Basisverzeichnisses nicht in das neue Basisverzeichnis kopiert wird, und die Inhalte des vorigen Basisverzeichnisses manuell zum neuen Basisverzeichnis verschieben, um Probleme wie das Kopieren geöffneter Dateien zu verhindern.

Zum Löschen des vorigen Basisverzeichnisses benötigt DRA explizite Berechtigungen, um schreibgeschützte Dateien und Unterverzeichnisse aus dem vorigen Basisverzeichnis löschen zu können. Sie können DRA die explizite Berechtigung erteilen, schreibgeschützte Dateien und Unterverzeichnisse aus dem vorigen Basisverzeichnis zu löschen.

Allow parent directory or path for a home share (Übergeordnetes Verzeichnis oder übergeordneten Pfad für ein Basisverzeichnis zulassen)

Sie können in DRA zulässige übergeordnete Verzeichnisse oder Pfade für Basisverzeichnisse auf Dateiservern angeben. Wenn Sie viele Verzeichnis- oder Dateiserverpfade angeben müssen, können Sie diese Pfade in eine CSV-Datei exportieren und die Pfade aus der CSV-Datei über die DRA-Konsole zu DRA hinzufügen. Mithilfe der im Feld **Allowable parent paths** (Zulässige übergeordnete Pfade) eingegebenen Informationen gewährleistet DRA Folgendes:

- DRA löscht das übergeordnete Verzeichnis auf dem Dateiserver nicht, wenn Hilfsadministratoren ein Benutzerkonto und das Basisverzeichnis das Benutzerkontos löschen.
- DRA verschiebt das Basisverzeichnis zu einem gültigen übergeordneten Verzeichnis oder Pfad auf dem Dateiserver, wenn Sie das Benutzerkonto umbenennen oder den Basisverzeichnispfad des Benutzerkontos ändern.

Delete home directory when user account is deleted (Basisverzeichnis löschen, wenn Benutzerkonto gelöscht wird)

Mit dieser Regel kann DRA ein Basisverzeichnis automatisch löschen, wenn das verknüpfte Benutzerkonto gelöscht wird. Wenn Sie den Papierkorb aktivieren, löscht DRA das Basisverzeichnis erst, wenn Sie das Benutzerkonto im Papierkorb löschen. Zum Löschen des Basisverzeichnisses benötigt DRA explizite Berechtigungen, um schreibgeschützte Dateien und Unterverzeichnisse aus dem vorigen Basisverzeichnis löschen zu können. Sie können DRA die explizite Berechtigung erteilen, schreibgeschützte Dateien und Unterverzeichnisse aus dem vorigen Basisverzeichnis zu löschen.

Automatisierung und Regeln für Basisfreigaben

DRA automatisiert Wartungsaufgaben für Basisfreigaben, indem es Basisfreigaben verwaltet, wenn ein Benutzerkonto geändert wird oder Basisverzeichnisse verwaltet werden. DRA kann verschiedene Aktionen ausführen, wenn ein Benutzerkonto erstellt, geklont, geändert, umbenannt oder gelöscht wird.

Um die Konsistenz mit den richtigen Microsoft Windows-Sicherheitsrichtlinien zu erhalten, erstellt DRA keine Zugriffssteuerungseinschränkungen auf Ebene der Freigabenamen. Stattdessen erstellt DRA Zugriffssteuerungseinschränkungen nur auf Verzeichnisebene. Das Einrichten von Zugriffssteuerungseinschränkungen auf Ebene des Freigabenamens und auf Ebene des Datei- oder Verzeichnisobjekts führt für Administratoren und Benutzer oft zu verwirrenden Zugriffsschemen.

HINWEIS: Der angegebene Speicherort muss eine gemeinsame Basisfreigabe haben, zum Beispiel `HOMEDIRS`, die sich eine Ebene über den Basisverzeichnissen befindet.

Der folgende Pfad ist beispielsweise gültig: *HOUSERV1**HOMEDIRS**%username%*

Der folgende Pfad ist ungültig: *HOUSERV1**%username%*

Namen für Basisfreigaben festlegen

Beim Definieren der Automatisierungsregeln für Basisfreigaben können Sie ein Präfix und ein Suffix für jede automatisch erstellte Basisfreigabe festlegen. Durch Festlegen eines Präfixes oder Suffixes können Sie eine Benennungskonvention für die Basisfreigaben erzwingen.

Beispiel: Sie aktivieren die Automatisierungsregeln „Create home directory“ (Basisverzeichnis erstellen) und „Create home share“ (Basisfreigabe erstellen). Für die Basisfreigabe legen Sie einen Unterstrich als Präfix und ein Dollarzeichen als Suffix fest. Wenn Sie einen Benutzer mit dem Namen „TomS“ erstellen, ordnen Sie sein neues Verzeichnis dem Laufwerk U zu und legen `\\HOUSERV1\HOMEDIRS\%username%` als Verzeichnispfad fest In diesem Beispiel erstellt DRA eine Netzwerkfreigabe mit dem Namen `_TomS$`, die auf das Verzeichnis `\\HOUSERV1\HOMEDIRS\TomS` zeigt.

Basisfreigaben für neue Benutzerkonten erstellen

Wenn DRA eine Basisfreigabe erstellt, verwendet der Verwaltungsserver den Pfad, der in den Feldern **Home directory** (Basisverzeichnis) im Assistenten zur Benutzererstellung angegeben ist. Sie können diesen Pfad später über die Profil-Registerkarte im Fenster der Benutzereigenschaften ändern.

DRA erstellt den Freigabenamen durch Anfügen des ggf. festgelegten Präfix und Suffix an den Benutzernamen. Wenn sie lange Benutzerkontonamen verwenden, kann DRA das für die Basisfreigabe angegebene Präfix und Suffix möglicherweise nicht hinzufügen. Das Präfix und das Suffix und die Anzahl der zulässigen Verbindungen basieren auf den ausgewählten Optionen zum Erstellen der Basisfreigaben.

Basisfreigaben für geklonte Benutzerkonten erstellen

Wenn der Basisverzeichnisname, der auf Grundlage des neu erstellten Benutzerkontonamens generiert wird, bereits vorhanden ist, löscht DRA die vorhandene Freigabe und erstellt eine neue Freigabe im festgelegten Basisverzeichnis.

Beim Klonen eines Benutzerkontos ist der Freigabename des vorhandenen Benutzerkontos zwingenderweise bereits vorhanden. Wenn Sie ein Benutzerkonto klonen, klont DRA auch die Informationen für das Basisverzeichnis und passt die Informationen für den neuen Benutzer an.

Eigenschaften von Basisfreigaben ändern

Wenn Sie den Speicherort des Basisverzeichnisses ändern, löscht DRA die vorhandene Freigabe und erstellt eine neue Freigabe im neuen Basisverzeichnis. Wenn das originale Basisverzeichnis leer ist, löscht DRA es.

Basisfreigaben für umbenannte Benutzerkonten umbenennen

Wenn Sie ein Benutzerkonto umbenennen, löscht DRA die vorhandene Basisfreigabe und erstellt basierend auf dem neuen Kontonamen eine neue Freigabe. Die neue Freigabe zeigt zum vorhandenen Basisverzeichnis.

Basisfreigaben für gelöschte Benutzerkonten löschen

Wenn Sie ein Benutzerkonto dauerhaft löschen, löscht DRA die verknüpfte Basisfreigabe.

Regeln zur Verwaltung des Speicherplatzkontingents für das Basis-Volume

Mit DRA können Sie Speicherplatzkontingente für Basis-Volumes verwalten. Sie können diese Richtlinie in nativen Domänen implementieren, wo sich das Basisverzeichnis auf einem Microsoft Windows-Computer befindet. Wenn Sie diese Richtlinie implementieren, sollten Sie ein Speicherplatzkontingent von mindestens 25 MB festlegen, um ausreichend Platz zur Verfügung zu stellen.

Passwortgenerierung zulassen

Mit dieser Funktion können Sie Richtlinieneinstellungen für die von DRA generierten Passwörter festlegen. DRA erzwingt diese Einstellungen nicht für Passwörter, die von Benutzern erstellt werden. Beim Konfigurieren der Eigenschaften der Passwortrichtlinie darf die Passwortlänge nicht auf weniger als 6 Zeichen oder mehr als 127 Zeichen festgelegt werden. Alle Werte außer der Passwortlänge und der Höchstgrenze können auf null gesetzt werden.

Um Richtlinien für die Passwortgenerierung zu konfigurieren, navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Configure Password Generation Policies** (Richtlinien für die Passwortgenerierung konfigurieren) und aktivieren Sie das Kontrollkästchen **Enable Password Policy** (Passwortrichtlinie aktivieren). Klicken Sie auf **Password Settings** (Passworteinstellungen) und konfigurieren Sie die Eigenschaften der Passwortrichtlinie.

Richtlinienaufgaben

Zum Löschen, Aktivieren oder Deaktivieren von Richtlinien müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten).

Um eine dieser Aktionen auszuführen, navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Policy** (Richtlinie). Klicken Sie im rechten Bereich mit der rechten Maustaste auf die Richtlinie, die Sie löschen, aktivieren oder deaktivieren möchten, und wählen Sie die gewünschte Aktion aus.

Integrierte Richtlinien implementieren

Zum Implementieren von integrierten Richtlinien müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten). Weitere Informationen zu integrierten Richtlinien finden Sie unter Grundlegendes zu integrierten Richtlinien.

HINWEIS: Bevor Sie eine integrierte Richtlinie mit einem Hilfsadministrator und einer Aktivansicht verknüpfen, stellen Sie sicher, dass der Hilfsadministrator der gewünschten Aktivansicht zugewiesen ist.

So implementieren Sie integrierte Richtlinien:

1. Navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Policy** (Richtlinie).

2 Klicken Sie im Aufgabenmenü auf **New Policy** (Neue Richtlinie) und wählen Sie dann die Art der zu erstellenden integrierten Richtlinie aus.

3 Geben Sie in den einzelnen Fenstern des Assistenten die gewünschten Werte ein und klicken Sie auf **Next** (Weiter). Sie können die neue Richtlinie beispielsweise mit einer bestimmten ActiveView verknüpfen, sodass DRA die Richtlinie für Objekte erzwingt, die in der angegebenen ActiveView enthalten sind.

4 Überprüfen Sie die Zusammenfassung und klicken Sie auf **Finish** (Fertigstellen).

Benutzerdefinierte Richtlinien implementieren

Zum Implementieren einer benutzerdefinierten Richtlinie müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten).

Um eine benutzerdefinierte Richtlinie erfolgreich zu implementieren, müssen Sie ein Skript erstellen, das während eines bestimmten Vorgangs (Verwaltungsaufgabe) ausgeführt wird. Im Skript der benutzerdefinierten Richtlinie können Sie Fehlermeldungen definieren, die angezeigt werden sollen, wenn eine Aktion die Richtlinie verletzt. Sie können auch eine standardmäßige Fehlermeldung über den Assistenten zum Erstellen von Richtlinien festlegen.

Weitere Informationen zum Verfassen von benutzerdefinierten Richtlinien, Anzeigen einer Liste der Verwaltungsaufgaben und Verwenden von Argument-Arrays finden Sie im SDK. Weitere Informationen finden Sie unter Skripte oder ausführbare Programme für benutzerdefinierte Richtlinien erstellen.

HINWEIS

- Bevor Sie eine benutzerdefinierte Richtlinie mit einem Hilfsadministrator und einer Aktivansicht verknüpfen, stellen Sie sicher, dass der Hilfsadministrator der gewünschten Aktivansicht zugewiesen ist.
- Wenn der Pfad für das Skript oder das ausführbare Programm der benutzerdefinierten Richtlinie Leerzeichen enthält, schließen Sie den Pfad in Anführungszeichen (") ein.

So implementieren Sie eine benutzerdefinierte Richtlinie:

1 Verfassen Sie ein Skript oder ausführbares Programm für die Richtlinie.

2 Melden Sie sich an einem DRA-Clientcomputer mit einem Konto an, dem in der verwalteten Domäne die integrierte Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) zugewiesen ist.

3 Starten Sie die Delegierungs- und Konfigurationskonsole.

4 Stellen Sie eine Verbindung zum primären Verwaltungsserver her.

5 Erweitern Sie im linken Bereich **Richtlinien- und Automatisierungsmanagement**.

6 Klicken Sie auf **Policy** (Richtlinie).

7 Klicken Sie im Aufgabenmenü auf **New Policy > Create a Custom Policy** (Neue Richtlinie > Benutzerdefinierte Richtlinie erstellen).

8 Geben Sie in den einzelnen Fenstern des Assistenten die gewünschten Werte ein und klicken Sie auf **Next** (Weiter). Sie können die neue Richtlinie beispielsweise mit einer bestimmten ActiveView verknüpfen, sodass DRA die Richtlinie für Objekte erzwingt, die in der angegebenen ActiveView enthalten sind.

9 Überprüfen Sie die Zusammenfassung und klicken Sie auf **Finish** (Fertigstellen).

Richtlinieneigenschaften ändern

Zum Ändern der Eigenschaften einer benutzerdefinierten Richtlinie müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten).

So ändern Sie Richtlinieneigenschaften:

1 Navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Policy** (Richtlinie).

2 Klicken Sie mit der rechten Maustaste auf die Richtlinie, die Sie ändern möchten, und wählen Sie **Properties** (Eigenschaften) aus.

3 Ändern Sie die gewünschten Eigenschaften und Einstellungen der Richtlinie.

Skripte oder ausführbare Programme für benutzerdefinierte Richtlinien erstellen

Weitere Informationen zum Erstellen von Skripten oder ausführbaren Programmen für benutzerdefinierte Richtlinien finden Sie im SDK.

So greifen Sie auf das SDK zu:

1 Stellen Sie sicher, dass das SDK auf dem Computer installiert ist. Das Setup-Programm erstellt eine Verknüpfung zum SDK in der Directory and Resource Administrator-Programmgruppe. Weitere Informationen hierzu finden Sie in der Installations-Checkliste unter DRA-Verwaltungsserver installieren.

2 Klicken Sie auf die SDK-Verknüpfung in der im Directory and Resource Administrator-Programmgruppe.

Weitere Informationen zum SDK finden Sie im „DRA REST Services Guide“ (DRA-REST-Services-Handbuch) auf der Website der DRA-Dokumentation.

Richtlinie des Delegierungs- und Konfigurationsclients

Die Richtlinie für die automatische Benennung umfasst drei Richtlinienkonfigurationen in den Exchange-Richtlinien, die exklusiv im Delegierungs- und Konfigurationsclient verfügbar sind, das heißt, es handelt sich um eine clientseitige Richtlinie.

Die Richtlinie für die automatische Benennung ermöglicht das Festlegen von Regeln für die automatisierte Benennung bestimmter Eigenschaften eines Postfachs. Mit diesen Optionen können Sie Benennungskonventionen erstellen und schnell Standardwerte für den Anzeigenamen, den Verzeichnisnamen und die Aliaseigenschaften generieren. Exchange bietet Ihnen für verschiedene Optionen der automatisierten Benennung die Möglichkeit, Ersatzzeichenfolgen festzulegen, wie `%First` oder `%Last`.

Wenn Exchange einen Verzeichnisnamen oder ein Alias generiert, überprüft es, ob der generierte Wert eindeutig ist. Wenn der generierte Wert nicht eindeutig ist, hängt Exchange einen Bindestrich (-) und eine zweistellige Nummer (beginnend mit `-01`) an, um einen eindeutigen Wert zu erhalten. Beim Generieren von Anzeigenamen überprüft Exchange nicht, ob der Wert eindeutig ist.

Exchange unterstützt die folgenden Ersatzzeichenfolgen für die Richtlinien zur automatischen Benennung und Vertretungsgenerierung:

`%First`	**Gibt den Wert der Eigenschaft „First name“ (Vorname) des verknüpften Benutzerkontos an.**
`%Last`	Gibt den Wert der Eigenschaft „Last name“ (Nachname) des verknüpften Benutzerkontos an.
`%Initials`	Gibt den Wert der Eigenschaft „Initials“ (Initialen) des verknüpften Benutzerkontos an.
`%Alias`	Gibt den Wert der Eigenschaft „Alias“ des Postfachs an.
`%DirNam`	Gibt den Wert der Eigenschaft „Directory name“ (Verzeichnisname) des Postfachs an. Für das Generieren von Email-Adressen für Microsoft Exchange-Postfächer unterstützt Exchange keine Vertretungsgenerierungs-Zeichenfolgen mit der Variable `%DirName`.
`%UserName`	Gibt den Wert der Eigenschaft „User name“ (Benutzername) des verknüpften Benutzerkontos an.

Sie können auch eine Zahl zwischen dem Prozentzeichen (%) und der Ersatzzeichenfolge angeben, um die Anzahl der aus dem Wert zu übernehmenden Zeichen festzulegen. Beispiel: `%2First` entspricht den ersten zwei Zeichen der Eigenschaft **First name** (Vorname) des Benutzerkontos.

Jede automatische Benennungsregel oder Vertretungsgenerierungsrichtlinie kann eine oder mehrere Ersatzzeichenfolgen enthalten. Sie können in jeder Regel auch Zeichen als Präfix oder Suffix für eine bestimmte Ersatzzeichenfolge angeben, zum Beispiel ein Punkt oder ein Leerzeichen (`.`) nach der Ersatzzeichenfolge `%Initials` (Initialen). Wenn die Eigenschaft der Ersatzzeichenfolge leer ist, schließt Exchange das Suffix für diese Eigenschaft nicht ein.

Beispiel: Angenommen, Sie verwenden die folgende automatische Benennungsregel für die Eigenschaft **Display name** (Anzeigename):

```
%First %1Initials. %Last
```

Wenn der Wert der Eigenschaft **First name** (Vorname) `Susan` ist, der Wert der Eigenschaft **Initials** (Initialen) `May` ist und der Wert der Eigenschaft **Last name** (Nachname) `Smith`, legt Exchange die Eigenschaft **Display name** auf `Susan M. Smith` fest.

Wenn der Wert der Eigenschaft **First name** (Vorname) `Michael` ist, der Wert der Eigenschaft **Initials** (Initialen) leer ist und der Wert der Eigenschaft **Last name** (Nachname) `Jones`, legt Exchange die Eigenschaft **Display name** (Anzeigename) auf `Michael Jones` fest.

Festlegen einer Richtlinie für die automatische Postfachbenennung

Um Optionen für die automatisierte Benennung von Postfächern festzulegen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse, die in der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) enthalten sind. Außerdem muss Ihre Lizenz das Exchange-Produkt unterstützen.

So legen Sie eine Richtlinie für die automatisierte Benennung von Postfächern fest:

1. Navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Configure Exchange Policies** (Exchange-Richtlinien konfigurieren) > **Alias naming** (Aliasbenennung).
2. Geben Sie die geeigneten Informationen für die Namensgenerierung an.
3. Wählen Sie **Enforce alias naming rules during mailbox updates** (Alias-Benennungsregeln bei Postfachaktualisierungen erzwingen) aus.
4. Klicken Sie auf **OK**.

Festlegen einer Richtlinie für die Ressourcenbenennung

Um Optionen für die Benennung von Ressourcen festzulegen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse, die in der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) enthalten sind. Außerdem muss Ihre Lizenz das Exchange-Produkt unterstützen.

So legen Sie eine Richtlinie für die Ressourcenbenennung fest:

1. Navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Configure Exchange Policies** (Exchange-Richtlinien konfigurieren) > **Resource naming** (Ressourcenbenennung).
2. Geben Sie die geeigneten Informationen für die Generierung des Ressourcennamens an.
3. Wählen Sie **Enforce resource naming rules during mailbox updates** (Ressourcen-Benennungsregeln bei Postfachaktualisierungen erzwingen) aus.
4. Klicken Sie auf **OK**.

Festlegen einer Richtlinie für die Archivbenennung

Um Optionen für die Benennung von Archiven festzulegen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse, die in der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) enthalten sind. Außerdem muss Ihre Lizenz das Exchange-Produkt unterstützen.

So legen Sie eine Richtlinie für die Archivbenennung fest:

1. Navigieren Sie zu **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement) > **Configure Exchange Policies** (Exchange-Richtlinien konfigurieren) > **Archive naming** (Archivbenennung).
2. Geben Sie die geeigneten Informationen für die Generierung der Archivnamen für Benutzerkonten an.

3 Wählen Sie **Enforce archive naming rules during mailbox updates** (Archiv-Benennungsregeln bei Postfachaktualisierungen erzwingen) aus.

4 Klicken Sie auf **OK**.

14 Automatisierung von Auslösern vor und nach Aufgaben

Ein Automatisierungsauslöser ist eine Regel, die ein Skript oder eine ausführbare Datei mit einem oder mehreren Vorgängen verknüpft. Über das Skript oder die ausführbare Datei können Sie einen vorhandenen Workflow automatisieren und eine Informationsbrücke zwischen DRA und anderen Daten-Repositorys herstellen. Mit Automatisierungsauslösern können Sie die von DRA gebotene Funktionalität und Sicherheit erweitern.

Zum Definieren eines Automatisierungsauslösers legen Sie die Regelparameter, die mit dem Auslöser zu verknüpfenden Vorgänge, das auszuführende Skript bzw. ausführbare Programm und, sofern zutreffend, die Aktivansichten oder die Hilfsadministratoren, die mit dem Auslöser verknüpft sein sollen, fest. Diese Regeln bestimmen, wie der Verwaltungsserver den Auslöser anwendet.

Sie können für den Auslöser auch ein Skript oder ein ausführbares Programm festlegen, das den Vorgang rückgängig macht. Mit einem **Skript zum Rückgängigmachen** können Sie Ihre Änderungen rückgängig machen, falls der Vorgang nicht abgeschlossen werden kann.

DRA unterstützt VBScript- und PowerShell-Skripte.

Automatisierung von Prozessen durch den Verwaltungsserver

Neben der auf ActiveViews basierenden Verwaltung bietet DRA die Möglichkeit, vorhandene Workflows zu automatisieren und verknüpfte Aufgaben über Automatisierungsauslöser automatisch auszuführen. Durch die Automatisierung vorhandener Workflows können Sie die Vorgänge im Unternehmen optimieren und bessere und schnellere Services bereitstellen.

Wenn der Verwaltungsserver den Vorgang ausführt, der mit dem Automatisierungsauslöser verknüpft ist, führt der Server auch das Auslöserskript bzw. das ausführbare Programm des Auslösers aus. Wenn es sich um einen Auslöser „vor der Aufgabe“ handelt, führt der Server das Skript oder ausführbare Programm vor dem Ausführen der Aufgabe aus. Wenn es sich um einen Auslöser „nach der Aufgabe“ handelt, führt der Server das Skript oder ausführbare Programm nach dem Ausführen der Aufgabe aus. Dieser Prozess wird als Transaktion bezeichnet. Eine **Transaktion** stellt den vollständigen Implementierungszyklus für jede Aufgabe bzw. jeden Vorgang dar, die/der vom Verwaltungsserver ausgeführt wird. Eine Transaktion umfasst die Aktionen, die zum Abschließen eines Vorgangs erforderlich sind, sowie alle Aktionen, die der Verwaltungsserver im Falle eines Fehlers beim Vorgang zum Rückgängigmachen ausführen soll.

Der Verwaltungsserver trägt den Auslöserstatus bei jeder Ausführung eines Automatisierungsauslösers in das Revisionsprotokoll ein. Diese Protokolleinträge enthalten einen Rückgabecode und Informationen über die verknüpften Vorgänge, die behandelten Objekte und den Erfolg der Ausführung der des Auslöserskripts.

WARNUNG: Automatisierungsauslöser werden mit dem Servicekonto des Verwaltungsservers ausgeführt. Da das Servicekonto über Administratorberechtigungen verfügt, haben Richtlinien und Automatisierungsauslöser vollen Zugriff auf alle Unternehmensdaten. Zum Definieren von Automatisierungsauslösern müssen Sie über die erforderlichen Befugnisse verfügen, beispielsweise über die Befugnisse der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten). Diese Automatisierungsauslöser werden im Sicherheitskontext des Servicekontos ausgeführt. Aus diesem Grund können Hilfsadministratoren, denen die integrierte Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) zugewiesen ist, unter Umständen über höhere Befugnisse als beabsichtigt verfügen.

Implementieren eines Automatisierungsauslösers

Um Automatisierungsauslöser zu implementieren, müssen Sie zunächst Skripte oder ausführbare Programme für den Auslöser schreiben und über die entsprechenden Befugnisse verfügen, beispielsweise über die Befugnisse, die in der integrierten Rolle „Manage Policies and Automation Triggers“ (Richtlinien und Automatisierungsauslöser verwalten) enthalten sind.

Um einen benutzerdefinierten Auslöser erfolgreich zu implementieren, müssen Sie ein Skript erstellen, das während eines bestimmten Vorgangs (Verwaltungsaufgabe) ausgeführt wird. Sie können festlegen, ob DRA den Auslöser vor oder nach der Ausführung des betreffenden Vorgangs ausführen soll. Im Auslöserskript können Sie Fehlermeldungen definieren, die im Falle eines Fehlers beim Ausführen des Auslösers angezeigt werden. Sie können auch eine standardmäßige Fehlermeldung über den Assistenten zum Erstellen von Automatisierungsauslösern festlegen.

Weitere Informationen zum Verfassen von benutzerdefinierten Auslösern, Anzeigen einer Liste der Verwaltungsaufgaben und Verwenden von Argument-Arrays finden Sie im *SDK*.

HINWEIS

- Bevor Sie einen benutzerdefinierten Automatisierungsauslöser mit einem Hilfsadministrator und einer Aktivansicht verknüpfen, stellen Sie sicher, dass der Hilfsadministrator der gewünschten Aktivansicht zugewiesen ist.
- Wenn der Pfad für das Skript oder das ausführbare Programm des benutzerdefinierten Auslösers Leerzeichen enthält, schließen Sie den Pfad in Anführungszeichen (") ein.
- Wenn der Vorgang **UserSetInfo** für ein Skriptautomatisiserungsauslöser verwendet wird und ein Benutzerattribut geändert wird (und den Auslöser ausführt), wird das geänderte Attribut derzeit erst dann im Unternehmen verbreitet, nachdem der Vorgang **Find Now** (Jetzt suchen) für das Benutzerobjekt ausgeführt wird.
- Beim Implementieren von Auslösern für bestimmte Aktivansichten, d. h. von Auslösern mit einem begrenzten Bereich, müssen die GetInfo-Vorgänge auch den Eigenschaftenvorgang für den entsprechenden Objekttyp enthalten. Beim Auslösen über den Vorgang **UserGetInfo** muss zum Beispiel auch der Vorgang **UserProperties** zur Auslöservorgangsliste hinzugefügt werden.

So implementieren Sie einen Automatisierungsauslöser:

1 Erstellen Sie ein Skript oder eine ausführbare Datei für den Auslöser.

2 Melden Sie sich an einem DRA-Clientcomputer mit einem Konto an, dem in der verwalteten Domäne die integrierte Rolle **Manage Policies and Automation Triggers** (Richtlinien und Automatisierungsauslöser verwalten) zugewiesen ist.

3 Starten Sie die Delegierungs- und Konfigurationskonsole.

4 Stellen Sie eine Verbindung zu einem primären Verwaltungsserver her.

5 Verwenden Sie die Dateireproduktion, um die Auslöserdatei auf die primären und sekundären DRA-Server hochzuladen.

   Der Ordnerpfad muss auf allen DRA-Servern in der verwalteten Domäne bereits vorhanden sein. Dieser Pfad, einschließlich der Datei, wird im **Do file path** (Pfad der DO-Datei) des Assistenten für den Automatisierungsauslöser verwendet.

6 Erweitern Sie im linken Bereich **Policy and Automation Management** (Richtlinien- und Automatisierungsmanagement).

7 Klicken Sie auf **Automation Triggers** (Automatisierungsauslöser).

8 Klicken Sie im Aufgabenmenü auf **New Trigger** (Neuer Auslöser).

9 Geben Sie in den einzelnen Fenstern des Assistenten die gewünschten Werte ein und klicken Sie auf **Next** (Weiter). Sie können den neuen Auslöser beispielsweise mit einer bestimmten Aktivansicht verknüpfen, sodass DRA den Auslöser auf alle Objekte anwendet, die in der angegebenen Aktivansicht enthalten sind.

10 Überprüfen Sie die Zusammenfassung und klicken Sie auf **Finish** (Fertig stellen).

WICHTIG: Wenn Sie mehr als eine Aktivansicht für einen Auslöser konfiguriert haben, indem Sie Aktivansichten durch Kommas getrennt haben, werden diese Aktivansichten beim Aufrüsten auf eine neue Version von DRA im Auslöser zweigeteilt und der Auslöser wird dann nicht ausgeführt. Damit der Vorgang nach einer Aufrüstung ausgeführt wird, muss der Auslöser neu konfiguriert oder muss ein neuer Auslöser erstellt werden.

---

15 Automatisierte Workflows

Mit der Workflowautomatisierung können Sie IT-Prozesse automatisieren, indem Sie benutzerdefinierte Workflowformulare erstellen, die beim Ausführen eines Workflows ausgeführt oder durch ein benanntes Workflowereignis ausgelöst werden, das im Workflowautomatisierungsserver erstellt wird. Beim Erstellen eines Workflowformulars definieren Sie die Administratorgruppen, die das Formular anzeigen können. Das Übertragen des Formulars bzw. die Ausführung des Workflowprozesses hängt von den Befugnissen ab, die der Gruppe bzw. den Gruppen beim Erstellen des Workflowformulars delegiert wurden.

Workflowformulare werden, wenn sie erstellt oder geändert werden, auf dem Webserver gespeichert. Hilfsadministratoren, die sich bei der Webkonsole für diesen Server anmelden, erhalten je nach Konfiguration des Formulars Zugriff auf die Formulare. Die Formulare sind im Allgemeinen für alle Benutzer verfügbar, die über einen Berechtigungsnachweis für den Webserver verfügen. Wenn Sie den Zugriff auf ein bestimmtes Formular einschränken möchten, fügen Sie Hilfsadministratorgruppen hinzu und blenden Sie das Formular für andere Benutzer aus. Zum Übertragen des Formulars ist eines der folgenden Befugnisse erforderlich:

- Workflowereignis erstellen und alle Eigenschaften ändern
- Workflow starten

Workflowformular starten: Workflows werden auf dem Workflowautomatisierungsserver erstellt, der über die Delegierungs- und Konfigurationskonsole 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 Workflowanforderungen, die mit „Spezifischen Workflow starten“ konfiguriert wurden, verfügen über einen Ausführungsverlauf, der im Hauptsuchbereich unter **Aufgaben** > **Anforderungen** abgefragt werden kann.

Sie können eine vorhandene Anforderung ändern oder eine Anforderung erstellen. Um eine Workflowanforderung zu erstellen oder eine vorhandene Anforderung zu ändern, wechseln Sie zu **Aufgaben** > **Anpassung** > **Workflow (Anforderungen)**.

Führen Sie diese einfachen Schritte aus, um eine Anforderung zu erstellen:

1. Konfigurieren Sie die Anforderung so, dass sie einen *spezifizierten Workflow* ausführt, wenn das Formular übertragen wird, oder konfigurieren Sie die Anforderung so, dass sie ausgeführt wird, wenn sie von einem vordefinierten *benannten Ereignis* ausgelöst wird.

2. Wählen Sie die Hilfsadministratorgruppe oder -gruppen, die im Workflowprozess eingeschlossen sind, und aktivieren Sie die Option **Formular ist ausgeblendet** auf der Registerkarte **Allgemein**, um den Formularzugriff auf diese Benutzer zu beschränken.
3. Fügen Sie beliebige erforderliche Eigenschaftenfelder oder zusätzliche Eigenschaftenseiten zum Formular hinzu.
4. Erstellen Sie je nach Bedarf benutzerdefinierte Behandlungsroutinen, um den Workflowprozess und seine Ausführung weiter zu definieren.

   HINWEIS: Benutzerdefinierte Optionen für Behandlungsroutinen werden für eine neue Workflowanforderung erst angezeigt, nachdem die Anforderung zum ersten Mal gespeichert wurde. Über **Formulareigenschaften** können Sie auf die benutzerdefinierten Behandlungsroutinen zugreifen und benutzerdefinierte Behandlungsroutinen erstellen oder ändern.

   ---

5. Deaktivieren Sie die Option **Formular ist ausgeblendet**, damit die Benutzer die Formulare anzeigen können.

Informationen zum Konfigurieren des Workflowautomatisierungsservers finden Sie in „Workflowautomatisierungsserver konfigurieren“, auf Seite 74 und Informationen zur Anpassung von Workflowanforderungen in Anpassen von Anforderungsformularen.

VI Revision und Berichterstellung

Die Revision von Benutzeraktionen ist einer der wichtigsten Aspekte einer einwandfreien Sicherheitsimplementierung. DRA protokolliert alle Benutzervorgänge im Protokollarchiv auf dem Verwaltungsserver-Computer, damit Sie die Aktionen der Hilfsadministratoren überprüfen und Berichte dazu erstellen können. DRA bietet klare und umfassende Berichterstellungsfunktionen mit Vorher- und Nachher-Werten der überwachten Ereignisse, damit Sie genau sehen können, was geändert wurde.

16 Überwachungsaktivität

Die Revision der Aktivitäten in den Ereignisprotokollen unterstützt Sie beim Isolieren, Diagnostizieren und Lösen von Problemen in der Umgebung. Die Informationen in diesem Abschnitt unterstützen Sie beim Aktivieren und Verstehen der Ereignisprotokollierung und beschreibt die Arbeit mit Protokollarchiven.

Natives Windows-Ereignisprotokoll

DRA protokolliert alle Benutzervorgänge im Protokollarchiv auf dem Verwaltungsserver-Computer, damit Sie die Aktionen der Hilfsadministratoren überprüfen und Berichte dazu erstellen können. Benutzervorgänge umfassen alle Versuche, Definitionen zu ändern, beispielsweise das Aktualisieren von Benutzerkonten, Löschen von Gruppen oder 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.

Aktivieren und Deaktivieren der Windows-Ereignisprotokollrevision für DRA

Bei der Installation von DRA 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.

So aktivieren Sie die Ereignisrevision:

1. Klicken Sie auf **Start > Ausführen**.
2. Geben Sie `regedit` in das Feld **Öffnen** ein und klicken Sie auf **OK**.
3. Erweitern Sie den folgenden Registrierungsschlüssel: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
4. Klicken Sie auf **Bearbeiten > Neu > DWORD-Wert**.
5. Geben Sie `IsNTAuditEnabled` als Schlüsselnamen ein.
6. Klicken Sie auf **Bearbeiten > Ändern**.
7. Geben Sie `1` in das Feld **Wertdaten** ein und klicken Sie auf **OK**.
8. Schließen Sie den Registrierungseditor.

So deaktivieren Sie die Ereignisrevision:

1. Klicken Sie auf **Start > Ausführen**.
2. Geben Sie `regedit` in das Feld **Öffnen** ein und klicken Sie auf **OK**.
3. Erweitern Sie den folgenden Registrierungsschlüssel: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
4. Wählen Sie den Schlüssel `IsNTAuditEnabled` aus.
5. Klicken Sie auf **Bearbeiten > Ändern**.
6. Geben Sie `0` in das Feld **Wertdaten** ein und klicken Sie auf **OK**.
7. Schließen Sie den Registrierungseditor.

Gewährleisten der Revisionsintegrität

Um sicherzustellen, dass alle Benutzeraktionen überwacht werden, stellt DRA alternative Protokollierungsmethoden zur Verfügung, wenn das Produkt die Protokollierungsaktivität nicht überprüfen kann. Bei der Installation von DRA werden der AuditFailsFilePath-Schlüssel und -Pfad zur Registrierung hinzugefügt, um die folgenden Aktionen zu gewährleisten:

- Wenn DRA erkennt, dass die Revisionsereignisse nicht mehr in einem Protokollarchiv protokolliert werden, protokolliert DRA die Revisionsereignisse in einer lokalen Datei auf dem Verwaltungsserver.
- Wenn DRA die Revisionsereignisse nicht in eine lokale Datei schreiben kann, werden die Revisionsereignisse von DRA in das Windows-Ereignisprotokoll geschrieben.
- Wenn DRA die Revisionsereignisse nicht in das Windows-Ereignisprotokoll schreiben kann, schreibt das Produkt die Revisionsereignisse in das DRA-Protokoll.
- Wenn DRA erkennt, dass die Revisionsereignisse nicht mehr protokolliert werden, sperrt es weitere Benutzervorgänge.

Um Schreibvorgänge zu ermöglichen, während das Protokollarchiv nicht verfügbar ist, müssen Sie außerdem einen Wert für den Registrierungsschlüssel „AllowOperationsOnAuditFailure“ festlegen.

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.

So ermöglichen Sie Schreibvorgänge:

1. Klicken Sie auf **Start > Ausführen**.
2. Geben Sie `regedit` in das Feld **Öffnen** ein und klicken Sie auf **OK**.
3. Erweitern Sie den folgenden Registrierungsschlüssel: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\`.
4. Klicken Sie auf **Bearbeiten > Neu > DWORD-Wert**.
5. Geben Sie `AllowOperationsOnAuditFailure` als Schlüsselnamen ein.
6. Klicken Sie auf **Bearbeiten > Ändern**.
7. Geben Sie 736458265 in das Feld **Wertdaten** ein.
8. Wählen Sie **Dezimal** im Feld **Basis** aus und klicken Sie auf **OK**.
9. Schließen Sie den Registrierungseditor.

Grundlegendes zu Protokollarchiven

DRA protokolliert die Benutzeraktivitätsdaten in Protokollarchiven auf dem Verwaltungsserver. DRA erstellt tägliche Protokollarchivpartitionen, um die am jeweiligen Tag erfassten und normalisierten Daten zu speichern. DRA verwendet das lokale Datum des Verwaltungsservers (*YYYYMMDD*) als Benennungskonvention für die täglichen Protokollarchivpartitionen.

Wenn Sie den Verwaltungsberichte-Kollektor aktiviert haben, exportiert DRA die Protokollarchivdaten als Quelle für die DRA-Verwaltungsberichte in eine SQL Server-Datenbank.

Anfänglich behält DRA die Protokolldaten im Protokollarchiv standardmäßig ohne zeitliche Einschränkung bei. Die Protokollarchivgröße kann einen Höchstwert erreichen, der bei der Installation basierend auf dem verfügbaren Festplattenspeicher festgelegt wird. Wenn das Protokollarchiv diese maximale Größe überschreitet, werden keine neuen Revisionsereignisse mehr gespeichert. Sie können ein Zeitlimit für die Datenbeibehaltung festlegen, sodass DRA die älteren Daten entfernt, um Platz für neuere Daten zu schaffen. Dieser Vorgang wird als Bereinigung bezeichnet. Stellen Sie sicher, dass Sie eine Sicherungsstrategie eingerichtet haben, bevor Sie die Bereinigung aktivieren. Sie können den Beibehaltungszeitraum für das Protokollarchiv mit dem Dienstprogramm „Log Archive Configuration“ (Protokollarchivkonfiguration) konfigurieren. Weitere Informationen finden Sie unter Ändern der Einstellungen für die Protokollarchivbereinigung.

Arbeiten mit dem Dienstprogramm „Log Archive Viewer“ (Protokollarchivanzeige)

Mit dem Dienstprogramm für die Protokollarchivanzeige können Sie die in den Protokollarchivdateien gespeicherten Daten anzeigen. Das Dienstprogramm wird mit NetIQ DRA Log Archive Resource Kit (LARK) bereitgestellt, einem Ressourcenkit, den Sie wahlweise mit DRA installieren können. Weitere Informationen finden Sie in der *NetIQ DRA Log Archive Resource Kit Technical Reference* (Technische Referenz zu NetIQ DRA Log Archive Resource Kit).

Sichern von Protokollarchivdateien

Eine **Protokollarchivdatei** ist eine Sammlung an Datensatzblöcken. Da Protokollarchivdateien komprimierte Dateien im Binärformat sind, die sich außerhalb einer physischen Datenbank befinden, benötigen Sie Microsoft SQL Server Management Studio nicht zum Sichern der Protokollarchive. Wenn ein automatisiertes Dateisicherungssystem eingerichtet ist, werden die Protokollarchivdateien automatisch wie Ihre anderen Dateien gesichert.

Zur Planung der Sicherungsstrategie haben sich die folgenden Methoden bewährt:

- Jeden Tag wird eine einzelne Partition erstellt, die alle Ereignisdaten des Tags enthält. Wenn Sie die Bereinigung aktivieren, bereinigt der Protokollarchivservice die Daten dieser Partitionen standardmäßig automatisch alle 90 Tage. Zur Ermittlung der Häufigkeit der Sicherungen sollte die Sicherungsstrategie den Bereinigungszeitplan berücksichtigen. Wenn die Protokollarchivpartitionen bereinigt sind, löscht DRA die Binärdateien. Bereinigte Daten können nicht abgerufen werden. Bereinigte Daten können nur aus einer Sicherung wiederhergestellt werden. Weitere Informationen finden Sie unter Ändern der Einstellungen für die Protokollarchivbereinigung.
- Sichern Sie Partitionen erst, nachdem sie geschlossen wurden. Unter normalen Bedingungen wird eine Partition innerhalb von 2 Stunden nach Mitternacht am nächsten Tag geschlossen.
- Sichern und stellen Sie Partitionsordner und ihre Unterordner immer als Einheit wieder her. Sichern Sie die Datei `VolumeInfo.xml` als Teil der Partitionssicherung.
- Wenn Sie die Protokollarchivpartitionen für Berichte wiederherstellen möchten, stellen Sie sicher, dass die gesicherten Protokollarchive das Originalformat beibehalten oder wieder im Originalformat wiederhergestellt werden können.
- Für die Konfiguration des Prozesses zum Sichern der Protokollarchivdateien empfiehlt NetIQ, die beiden Unterordner `index_data` und `CubeExport` im Hauptordner für die Protokollarchivierung auszuschließen. Diese Unterordner enthalten temporäre Dateien und sollten nicht gesichert werden.

Ändern der Einstellungen für die Protokollarchivbereinigung

Bei der Installation von DRA ist die Protokollarchivbereinigung standardmäßig deaktiviert. Wenn Sie regelmäßige Sicherungsprozeduren für Protokollarchivdateien einrichten, sollten Sie die Protokollarchivbereinigung archivieren, um den Speicherplatz zu erhalten. Im Konfigurationsprogramm für das Protokollarchiv können Sie die Anzahl der Tage ändern, nach der Protokollarchivpartitionen bereinigt werden.

So ändern Sie die Anzahl der Tage, nach der die Protokollarchivpartitionen bereinigt werden:

1. Melden Sie sich mit einem Konto, das Mitglied der lokalen Administratorgruppe ist, am Verwaltungsserver an.
2. Starten Sie **Log Archive Configuration** (Protokollarchivkonfiguration) aus der NetIQ Administration-Programmgruppe.
3. Klicken Sie auf **Log Archive Server Settings** (Einstellungen des Protokollarchivservers).
4. *Wenn Sie die Partitionsbereinigung aktivieren möchten,* legen Sie den Wert für das Feld **Partition Grooming Enabled** (Partitionsbereinigung aktivieren) auf „wahr“ fest.
5. Geben Sie in das Feld **Number of Days before Grooming** (Anzahl der Tage bis zur Bereinigung) den Zeitraum in Tagen ein, über den die Protokollarchivpartitionen vor der Bereinigung beibehalten werden sollen.
6. Klicken Sie auf **Apply** (Anwenden).
7. Klicken Sie auf **Yes** (Ja).
8. Klicken Sie auf **Close** (Schließen).
9. Suchen Sie den Pfad zum Ordner *NetIQLogArchiveData*\<*Partitionsname*>. Üblicherweise ist dies `C:\ProgramData\NetIQ\DRA\NetIQLogArchiveData`.

   Wenn das Attribut „File is ready for archiving“ (Datei ist bereit für Archivierung) der Dateien und Ordner (in den Datei- bzw. Ordnereigenschaften) in den spezifizierten Partitionen nicht aktiviert ist, müssen Sie die CONFIG-Datei bearbeiten, um die Protokollarchivbereinigung zu aktivieren. Informationen dazu, warum das Attribut aktiviert oder deaktiviert ist, finden im Abschnitt **Additional Information** (Zusätzliche Informationen) im Knowledgebase-Artikel *How do you configure the data retention period for DRA Logarchival Data?* (Wie wird der Datenbeibehaltungszeitraum für DRA-Protokollarchivdaten konfiguriert?).

Wert	
Aktiviert	Klicken Sie in der Bestätigungsnachricht auf **Yes** (Ja), um den NetIQ Security Manager Log Archive-Service neu zu starten. **HINWEIS:** Wenn Sie Protokollarchiveinstellungen ändern, müssen Sie den Protokollarchiv-Service neu starten, damit die Änderungen übernommen werden.
Nicht aktiviert	Klicken Sie in der Bestätigungsnachricht auf **No** (Nein). Siehe So aktivieren Sie den DRA Log Archive-Service zum Bereinigen der nicht archivierten Daten:.

So aktivieren Sie den DRA Log Archive-Service zum Bereinigen der nicht archivierten Daten:

1. Melden Sie sich als Mitglied der lokalen Administratorgruppe lokal an jedem DRA-Server an der Windows-Konsole an.
2. Öffnen Sie die Datei `C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config` mit einem Texteditor und suchen Sie die Zeile `<Property name="GroomUnarchivedData" value="false" />`.
3. Ändern Sie `"false"` in `"true"` und speichern Sie die Datei.
4. Starten Sie den NetIQ DRA LogArchive-Service neu.

HINWEIS: Wenn Sie Protokollarchiveinstellungen ändern, müssen Sie den Protokollarchiv-Service neu starten, damit die Änderungen übernommen werden.

---

17 Berichterstellung

Dieser Abschnitt enthält Informationen zur Berichterstellung in DRA, zur Sammlung von Daten für die Berichterstellung, zur Datensammlung und Berichterstellung mit Active View Analyzer und zum Zugreifen auf die integrierten Berichte.

Funktionen und Berichte, die von Ihrer Lizenz nicht unterstützt werden, werden von 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.

Aktivitätsdetailberichte sind in der Delegierungs- und Konfigurationskonsole sofort nach der Installation von DRA verfügbar und zeigen die neuesten Details der Netzwerkänderungen.

- „Verwalten der Datensammlung für die Berichterstellung“, auf Seite 171
- „Integrierte Berichte“, auf Seite 173

Verwalten der Datensammlung für die Berichterstellung

Die DRA-Berichterstellung bietet zwei Methoden zum Generieren von Berichten, mit denen Sie die neuesten Änderungen in der Umgebung anzeigen und Definitionen von Benutzerkonten, Gruppen und Ressourcen in der Domäne sammeln und überwachen können.

Aktivitätsdetailberichte

Diese Berichte sind über die Delegierungs- und Konfigurationskonsole verfügbar und bieten Echtzeitinformationen zu 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 Details zum DRA-Sicherheitsmodell anzeigen, wie Definitionen zu Aktivansichten und Hilfsadministratorgruppen.

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 in Konfiguration der Berichterstellung.

Anzeigen des Kollektor-Status

Auf der Registerkarte „Collectors Status“ (Kollektorstatus) können Sie Details zu jedem Daten-Kollektor anzeigen.

So zeigen Sie den Status der Kollektoren an:

1. Erweitern Sie **Configuration Management** (Konfigurationsmanagement) und klicken Sie dann auf **Update Reporting Server Configuration** (Konfiguration des Berichterstellungsservers aktualisieren).
2. Klicken Sie auf der Registerkarte „Collectors Status“ (Kollektorstatus) auf jeden Eintrag, um zusätzliche Informationen zur Datensammlung anzuzeigen, beispielsweise wann zuletzt Daten erfasst wurden und ob die letzte Datensammlung erfolgreich war.
3. Wenn in der Serverliste keine Daten angezeigt werden, klicken Sie auf **Aktualisieren**.

Aktivieren der Berichterstellung und Datensammlung

Nachdem Sie die Komponenten der DRA-Berichterstellung installiert haben, aktivieren und konfigurieren Sie die Sammlung von Berichterstellungsdaten für den Zugriff auf Reporting Center-Berichte.

So aktivieren Sie die Berichterstellung und Datensammlung:

1. Navigieren Sie zu **Configuration Management** (Konfigurationsmanagement) > **Update Reporting Service Configuration** (Konfiguration des Berichterstellungs-Services).
2. Wählen Sie auf der Registerkarte „SQL Server“ **Enable DRA Reporting support** aus (Unterstützung für DRA-Berichterstellung aktivieren).
3. Klicken Sie im Feld für den Servernamen auf **Browse** (Durchsuchen) und wählen Sie den Computer aus, auf dem SQL Server installiert ist.
4. Geben Sie auf der Registerkarte für den Berechtigungsnachweis den geeigneten Berechtigungsnachweis für die Interaktionen mit SQL Server an.
5. Wenn dieses Konto auch zum Erstellen der Datenbank und Initialisieren des Schemas verwendet wird, aktivieren Sie das Kontrollkästchen „Use the above credentials for creating a database and initializing the database schema“ (Oben genannten Berechtigungsnachweis auch zum Erstellen einer Datenbank und Initialisieren des Datenbankschemas verwenden).
6. Wenn Sie zum Erstellen der Datenbank ein anderes Konto angeben möchten, geben Sie es mit dem entsprechenden Passwort auf der Registerkarte „Admin Credentials“ (Administratorberechtigung) an.
7. Klicken Sie auf **OK**.

Informationen über das Konfigurieren von spezifischen Kollektoren finden Sie in Konfiguration der Berichterstellung.

Integrierte Berichte

Mit integrierten Berichten können Sie Berichte zu Objektänderungen, Objektlisten und Objektdetails generieren. Diese Berichte sind nicht Bestandteil der DRA Reporting-Services und es ist keine Konfiguration erforderlich, um die integrierten Änderungsverlaufsberichte zu aktivieren. Die Themen in diesem Abschnitt beschreiben, wie Sie auf diese Berichte zugreifen können.

HINWEIS: Änderungsverlaufsberichte sind auch für Ereignisse außerhalb von DRA verfügbar, wenn DRA mit Change Guardian integriert ist. Informationen zu diesem Berichttyp und zum Konfigurieren von Change Guardian-Server finden Sie in Unified-Änderungsverlauf.

Berichterstellung zu Objektänderungen

Durch Generieren von Aktivitätsdetailberichten können Sie in Echtzeit Informationen zu Änderungen an Objekten in den Domänen anzeigen. Sie können beispielsweise eine Liste der Änderungen anzeigen, die innerhalb eines bestimmten Zeitraums an einem Objekt oder von einem Objekt vorgenommen wurden. Sie können die Aktivitätsdetailberichte auch exportieren und drucken.

So erstellen Sie einen Bericht zu Objektänderungen:

1. Suchen Sie die Objekte, die mit den gewünschten Kriterien übereinstimmen.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Reporting > Changes made to objectName** (Berichterstellung > Änderungen an objectName) oder **Reporting > Changes made by objectName** (Berichterstellung > Änderungen durch objectName) aus.
3. Wählen Sie das Start- und Enddatum aus, um festzulegen, für welchen Zeitraum Sie Änderungen anzeigen möchten.
4. *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.

   ---
5. *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.
6. Klicken Sie auf **OK**.

Berichterstellung zu Objektlisten

Sie können Daten aus Objektlisten exportieren oder drucken. Mit dieser Funktion können Sie schnell und einfach Berichte über allgemeine Informationen zu den verwalteten Objekte erstellen und verteilen.

Beim Exportieren einer Objektliste können Sie den Speicherort, den Namen und das Format der Datei angeben. DRA unterstützt die Formate HTML, CSV und XML, d. h. Sie können diese Informationen zu Datenbankanwendungen exportieren oder Listenergebnisse auf einer Website publizieren.

HINWEIS: Sie können auch mehrere Elemente in einer Liste auswählen und diese Elemente dann in eine Textanwendung kopieren beispielsweise in den Editor.

So erstellen Sie einen Bericht zu Objektlisten:

1. Suchen Sie die Objekte, die mit den gewünschten Kriterien übereinstimmen.
2. Um die Objektliste zu exportieren, klicken Sie im Dateimenü auf **Export List** (Liste exportieren).
3. Um die Objektliste zu drucken, klicken Sie im Dateimenü auf **Print List** (Liste drucken).
4. Geben Sie die geeigneten Informationen an, um die Liste zu speichern oder zu drucken.

Berichterstellung zu Objektdetails

Sie können Daten aus den Detail-Registerkarten, die Objektattribute wie Gruppenmitgliedschaften enthalten, exportieren oder drucken. Mit dieser Funktion können Sie schnell und einfach Berichte zu häufig benötigten Details über bestimmte Objekte erstellen und verteilen.

Beim Exportieren einer Objektdetails-Registerkarte können Sie den Speicherort, den Namen und das Format der Datei angeben. DRA unterstützt die Formate HTML, CSV und XML, d. h. Sie können diese Informationen zu Datenbankanwendungen exportieren oder Listenergebnisse auf einer Website publizieren.

So erstellen Sie einen Bericht zu Objektdetails:

1. Suchen Sie das Objekt, das den gewünschten Kriterien entspricht.
2. Klicken Sie im Menü „Ansicht“ auf **Details**.
3. Wählen Sie im Detailbereich die gewünschte Registerkarte aus.
4. Um diese Objektdetails zu exportieren, klicken Sie im Dateimenü auf **Export Details List** (Detailliste exportieren).
5. Um diese Objektdetails zu drucken, klicken Sie im Dateimenü auf **Print Details List** (Detailliste drucken).
6. Geben Sie die geeigneten Informationen an, um die Liste zu speichern oder zu drucken.

VII Weitere Funktionen

Temporäre Gruppenzuweisungen, dynamische Gruppen, Ereignisstempel und BitLocker-Wiederherstellungskennwörter sind weitere Funktionen in DRA, die Sie in der Unternehmensumgebung einsetzen können.

18 Temporäre Gruppenzuweisungen

Mit DRA können Sie temporäre Gruppenzuweisungen erstellen, um autorisierten Benutzern temporären Zugriff auf Ressourcen bereitzustellen. Hilfsadministratoren können Benutzer mithilfe von temporären Gruppenzuweisungen für einen begrenzten Zeitraum einer Zielgruppe zuweisen. Nach Ablauf des Zeitraums entfernt DRA die Benutzer automatisch aus der Gruppe.

Die Rolle „Manage Temporary Group Assignments“ (Temporäre Gruppenzuweisungen verwalten) gewährt Hilfsadministratoren die Befugnis zum Erstellen und Verwalten von temporären Gruppenzuweisungen.

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

Mit den folgenden Befugnissen können Sie die Erstellung und Verwaltung von temporären Gruppenzuweisungen delegieren:

- Create Temporary Group Assignments (Temporäre Gruppenzuweisungen erstellen)
- Delete Temporary Group Assignments (Temporäre Gruppenzuweisungen löschen)
- Modify Temporary Group Assignments (Temporäre Gruppenzuweisungen ändern)
- Reset Temporary Group Assignment State (Status der temporären Gruppenzuweisung zurücksetzen)
- View Temporary Group Assignments (Temporäre Gruppenzuweisungen anzeigen)
- Add Object to Group (Objekt zu Gruppe hinzufügen)
- Remove Object from Group (Objekt aus Gruppe entfernen)

Die Zielgruppe und die Zielbenutzer müssen zur gleichen Aktivansicht gehören.

HINWEIS

- Sie können keine temporäre Gruppenzuweisung für einen Benutzer erstellen, der bereits Mitglied einer Zielgruppe ist. Wenn Sie versuchen, eine temporäre Gruppenzuweisung für einen Benutzer zu erstellen, der bereits Mitglied einer Zielgruppe ist, zeigt DRA eine Warnmeldung an und lässt das Erstellen der temporären Gruppenzuweisung für den Benutzer nicht zu.
- Wenn Sie eine temporäre Gruppenzuweisung für einen Benutzer erstellen, der kein Mitglied einer Zielgruppe ist, entfernt DRA den Benutzer aus der Gruppe, sobald die temporäre Gruppenzuweisung abläuft.

Beispiel:

Bob, der Personalleiter, informiert John, einen Helpdesk-Administrator, über die auf einen bestimmten Zeitraum befristete Anstellung des neuen Mitarbeiters Joe. John führt folgende Aufgaben aus:

- Er erstellt eine temporäre Gruppenzuweisung

- Er fügt eine Personalgruppe für temporäre Mitarbeiter zur temporären Gruppenzuweisung hinzu.
- Er fügt Joe als Mitglied zur Gruppe der temporären Mitarbeiter hinzu.
- Er legt die Dauer der temporären Gruppenzuweisung auf einen Monat fest (03.07.2019 bis 02.08.2019).

Erwartetes Ergebnis:

Standardmäßig wird die Mitgliedschaft von Joe in der Mitarbeitergruppe nach Ablauf der temporären Gruppenzuweisung entfernt. Die temporäre Gruppenzuweisung bleibt sieben weitere Tage verfügbar, sofern John nicht die Option **Diese temporäre Gruppenzuweisung für die spätere Verwendung beibehalten** aktiviert hat.

Weitere Informationen zum Erstellen und Verwenden von temporären Gruppenzuweisungen finden Sie im *Benutzerhandbuch*.

19 Dynamische Gruppen in DRA

Eine dynamische Gruppe ist eine Gruppe, deren Mitgliedschaft basierend auf einem festgelegten Satz Kriterien variiert, die Sie in den Eigenschaften der Gruppe konfigurieren. Sie können eine beliebige Gruppe als dynamisch festlegen und den Dynamikfilter von jeder Gruppe entfernen, für die er konfiguriert ist. Diese Funktion bietet auch die Möglichkeit, Gruppenmitglieder zu einer statischen Liste oder einer Ausschlussliste hinzuzufügen. Gruppenmitglieder in diesen Listen sind von den dynamischen Kriterien nicht betroffen.

Wenn Sie eine dynamische Gruppe wieder in eine reguläre Gruppe zurückverwandeln, werden alle Mitglieder in der Liste der statischen Mitglieder zur Gruppenmitgliedschaft hinzugefügt und ausgeschlossene Mitglieder und Dynamikfilter werden ignoriert. Sie können sowohl in der Delegierungs- und Konfigurationskonto als auch in der Webkonsole vorhandene Gruppen als dynamisch festlegen oder eine neue dynamische Gruppe erstellen.

So legen Sie eine Gruppe als dynamisch fest:

1. Suchen Sie die Gruppe in der betreffenden Konsole.
   - Delegierungs- und Konfigurationskonsole: Wechseln Sie zu **All My Managed Objects** (Alle meine verwalteten Objekte) > **Find Now** (Jetzt suchen).

     HINWEIS: Um den Abfrage-Generator zu aktivieren, klicken Sie auf **Durchsuchen** und wählen Sie eine Domäne, einen Container oder eine organisatorische Einheit aus.
   - Webkonsole: Wechseln Sie zu **Verwaltung** > **Suchen**.
2. Öffnen Sie die Gruppeneigenschaften und wählen Sie auf der Registerkarte „Dynamischer Mitgliedsfilter“ **Gruppe dynamisch machen** aus.
3. Fügen Sie die gewünschten LDAP-Attribute und virtuellen Attribute zum Filtern der Gruppenmitgliedschaft hinzu.
4. Fügen Sie alle gewünschten statischen oder ausgeschlossenen Mitglieder zur dynamischen Gruppe hinzu und wenden Sie die Änderungen an.

So legen Sie eine neue Gruppe als dynamisch fest:

- **Delegierungs- und Konfigurationskonsole:** Klicken Sie mit der rechten Maustaste auf die Domäne oder auf den Unterknoten unter „All My Managed Objects“ (Alle meine verwalteten Objekte) und wählen Sie **New** (Neu) > **Dynamic Group** (Dynamische Gruppe) aus.
- **Webkonsole:** Navigieren Sie zu **Verwaltung** > **Erstellen** > **Dynamische Gruppe**.

20 Funktionsweise von Ereignisstempeln

Wenn Sie ein Attribut für einen Objekttyp konfigurieren und DRA einen der unterstützten Vorgänge ausführt, wird das Attribut mit DRA-spezifischen Informationen aktualisiert (gestempelt). Diese Informationen zeigen beispielsweise auch, wer den Vorgang ausgeführt hat. Der Ereignisstempel führt dazu, dass AD ein Revisionsereignis für diese Attributänderung generiert.

Angenommen, Sie haben das Attribut `extensionAttribute1` als Benutzerattribut ausgewählt und die AD DS-Revision ist konfiguriert. Jedes Mal, wenn ein Hilfsadministrator einen Benutzer aktualisiert, aktualisiert DRA das Attribut `extensionAttribute1` mit Ereignisstempeldaten. Das bedeutet, dass zusätzlich zu den AD DS-Ereignissen für jedes Attribut, das der Hilfsadministrator aktualisiert (wie Beschreibung, Name usw.), ein zusätzliches AD DS-Ereignis für das Attribut `extensionAttribute1` erzeugt wird.

Jedes dieser Ereignisse enthält eine Korrelations-ID, die für jedes Attribut, das beim Ändern des Benutzers geändert wurde, dieselbe ist. Auf diese Weise können die Anwendungen die Ereignisstempeldaten mit den anderen Attributen verknüpfen, die aktualisiert wurden.

AD DS-Ereignis

Jedes Mal, wenn DRA einen unterstützten Vorgang ausführt, wird ein solches Ereignis im Windows-Sicherheitsereignisprotokoll angezeigt.

LDAP-Anzeigename:	**`extensionAttribute1`**
Syntax (OID): 2.5.5.12	.2.5.5.12
Wert:	<dra-event **user**="DRDOM300\drauseradmin" **sid**="S-1-5-21-53918190-1560392134-2889063332-1914" **tid**="E0E257E6B4D24744A9B0FE3F86EC7038" **SubjectUserSid**="S-1-5-21-4224976940-2944197837-1672139851-500" **ObjectDN**="CN=admin_113,OU=Vino_113,DC=DRDOM113,DC=LAB"/ >+a+02ROO+bJbhyPbR4leJpKWCGTp/ KXdqI7S3EBhVyniE7iXvxIT6eB6IdcXQ5StkbIAHJgKzLN5FCOM5fZcITxyAPLWhbstaA7ZA0VbVC9MGlVIaAcjl3z7mpF9GKXsfDogbSeNlmHliXvH5KpOX3/29AKMPj/ zvf6Yuczoos=

Der Ereigniswert besteht aus zwei Elementen. Das erste Element ist eine XML-Zeichenkette mit den Ereignisstempeldaten. Das zweite Element ist eine Signatur der Daten, mit der bestätigt werden kann, dass die Daten tatsächlich von DRA erzeugt wurden. Zur Bestätigung der Signatur muss eine Anwendung über den öffentlichen Schlüssel der Signatur verfügen.

Die XML-Zeichenkette umfasst die folgenden Informationen:

Benutzer	Der Hilfsadministrator, der den Vorgang ausgeführt hat
Sid	Die SID des Hilfsadministrators, der den Vorgang ausgeführt hat
Tid	Die Revisionstransaktions-ID von DRA, die gewährleistet, dass jedes Ereignis eindeutig ist
SubjectUserSid	Die SID des DRA-Servicekontos oder -Zugriffskontos, mit dem AD aktualisiert wurde
ObjectDN	Der eindeutige Name des Objekts, das geändert wurde

Unterstützte Vorgänge

Benutzer	◆ Erstellen ◆ Umbenennen ◆ Bearbeiten ◆ Klonen
Gruppe	◆ Erstellen ◆ Umbenennen ◆ Bearbeiten ◆ Klonen
Kontakt	◆ Erstellen ◆ Umbenennen ◆ Bearbeiten ◆ Klonen
Computer	◆ Erstellen ◆ Aktivieren ◆ Deaktivieren ◆ Umbenennen ◆ Bearbeiten
Organisatorische Einheit	◆ Erstellen ◆ Umbenennen ◆ Klonen

21 BitLocker-Wiederherstellungskennwort

Microsoft BitLocker speichert Wiederherstellungskennwörter in Active Directory. Mit der DRA-BitLocker-Wiederherstellungsfunktion können Sie Hilfsadministratoren die Befugnis erteilen, 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 **Delegation and Configuration Console** (Delegierungs- und Konfigurationskonsole) und erweitern Sie die Baumstruktur.
2. Navigieren Sie im Knoten **Account and Resource Management** (Konto- und Ressourcenverwaltung) zu **All My Managed Objects** (Alle meine verwalteten Objekte) > **Domain** (Domäne) > **Computer**.
3. Klicken Sie in der Computerliste mit der rechten Maustaste auf den gewünschten Computer und wählen Sie **Properties** (Eigenschaften) aus.
4. Klicken Sie auf die Registerkarte **BitLocker Recovery Password** (BitLocker-Wiederherstellungskennwort), um das BitLocker-Wiederherstellungskennwort anzuzeigen.
5. Klicken Sie mit der rechten Maustaste auf das BitLocker-Wiederherstellungskennwort, klicken Sie auf **Copy** (Kopieren) und fügen Sie den Text in eine Textdatei oder ein Tabellenkalkulationsblatt Ihrer Wahl 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 **Delegation and Configuration Console** (Delegierungs- und Konfigurationskonsole) und erweitern Sie die Baumstruktur.
2. Navigieren Sie im Knoten **Account and Resource Management** (Konto- und Ressourcenverwaltung) zu **All My Managed Objects** (Alle meine verwalteten Objekte), 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).

22 Papierkorb

Sie können den Papierkorb für jede Microsoft Windows-Domäne oder für Objekte in diesen Domänen aktivieren oder deaktivieren und so die Verwaltung von Konten im Unternehmen steuern. Wenn Sie den Papierkorb aktivieren und dann ein Benutzerkonto, eine Gruppe, eine dynamische Verteilergruppe, eine dynamische Gruppe, ein Ressourcenpostfach, einen Kontakt oder ein Computerkonto löschen, deaktiviert der Verwaltungsserver das ausgewählte Konto und verschiebt es in den Papierkorb-Container. Nachdem DRA das Konto in den Papierkorb verschoben hat, wird das Konto nicht mehr in den ActiveViews angezeigt, zu denen es gehörte. Wenn Sie ein Benutzerkonto, eine Gruppe, einen Kontakt oder ein Computerkonto löschen, während der Papierkorb deaktiviert ist, löscht der Verwaltungsserver das ausgewählte Konto dauerhaft. Sie können einen Papierkorb, der zuvor gelöschte Konten enthält, deaktivieren. Nachdem der Papierkorb deaktiviert wurde, sind diese Konten jedoch nicht mehr im Papierkorb-Knoten verfügbar.

Zuweisen von Befugnissen für den Papierkorb

Um zuzulassen, dass ein Hilfsadministrator Konten dauerhaft aus dem Knoten „Alle meine verwalteten Objekte“ und aus dem Papierkorb löschen kann, weisen Sie die relevanten Befugnisse aus der folgenden Liste zu:

- Delete User Account Permanently (Benutzerkonto dauerhaft löschen)
- Delete Group Permanently (Gruppe dauerhaft löschen)
- Delete Computer Permanently (Computer dauerhaft löschen)
- Delete Contact Permanently (Kontakt dauerhaft löschen)
- Delete Dynamic Distribution Group Permanently (Dynamische Verteilergruppe dauerhaft löschen)
- Delete Dynamic Group Permanently (Dynamische Gruppe dauerhaft löschen)
- Delete Resource Mailbox Permanently (Ressourcenpostfach dauerhaft löschen)

Wenn mehrere Verwaltungsserver verschiedene Teilbäume in der gleichen Microsoft Windows-Domäne verwalten, können Sie im Papierkorb beliebige gelöschte Konten aus dieser Domäne anzeigen. Dies ist unabhängig davon, von welchem Verwaltungsservers das Konto verwaltet wird.

Arbeiten mit dem Papierkorb

Mit dem Papierkorb können Sie Konten dauerhaft löschen, Konten wiederherstellen und Eigenschaften von gelöschten Konten anzeigen. Sie können auch nach spezifischen Konten suchen und nachverfolgen, seit wie vielen Tagen ein gelöschtes Konto bereits im Papierkorb ist. Eine Papierkorb-Registerkarte ist außerdem im Eigenschaftenfenster der ausgewählten Domäne

vorhanden. Über diese Registerkarte können Sie den Papierkorb für die gesamte Domäne oder für spezifische Objekte deaktivieren und aktivieren. Außerdem können Sie hier einen Zeitplan für die Papierkorbbereinigung festlegen.

Mit den Optionen **Restore All** (Alles wiederherstellen) und **Empty Recycle Bin** (Papierkorb leeren) können Sie diese Konten schnell und einfach wiederherstellen oder löschen.

Wenn Sie ein Konto wiederherstellen, holt DRA das Konto mit allen Berechtigungen, Befugnisdelegierungen, Richtlinienzuweisungen, Gruppenmitgliedschaften und ActiveView-Mitgliedschaften zurück. Wenn Sie ein Konto dauerhaft löschen, entfernt DRA das Konto aus Active Directory.

Um die Sicherheit beim Löschen von Konten zu gewährleisten, können nur Hilfsadministratoren mit den folgenden Befugnissen Konten dauerhaft aus dem Papierkorb löschen:

- Delete User Account Permanently (Benutzerkonto dauerhaft löschen)
- Delete User from Recycle Bin (Benutzer aus dem Papierkorb löschen)
- Delete Group Account Permanently (Gruppenkonto dauerhaft löschen)
- Delete Group from Recycle Bin (Gruppe aus dem Papierkorb löschen)
- Delete Computer Account Permanently (Computerkonto dauerhaft löschen)
- Delete Computer from Recycle Bin (Computer aus dem Papierkorb löschen)
- Delete Contact Account Permanently (Kontaktkonto dauerhaft löschen)
- Delete Contact from Recycle Bin (Kontakt aus dem Papierkorb löschen)
- Delete Dynamic Distribution Group Permanently (Dynamische Verteilergruppe dauerhaft löschen)
- Delete Dynamic Distribution Group from Recycle Bin (Dynamische Verteilergruppe aus dem Papierkorb löschen)
- Delete Dynamic Group Permanently (Dynamische Gruppe dauerhaft löschen)
- Delete Dynamic Group from Recycle Bin (Dynamische Gruppe aus dem Papierkorb löschen)
- Delete Resource Mailbox Permanently (Ressourcenpostfach dauerhaft löschen)
- Delete Resource Mailbox from Recycle Bin (Ressourcenpostfach aus dem Papierkorb löschen)
- View all Recycle Bin Objects (Alle Objekte im Papierkorb anzeigen)

Um ein Konto aus dem Papierkorb wiederherstellen zu können, müssen die Hilfsadministratoren in der organisatorischen Einheit, die das Konto enthält, über die folgenden Befugnisse verfügen:

- Restore User from Recycle Bin (Benutzer aus Papierkorb wiederherstellen)
- Restore Group from Recycle Bin (Gruppe aus dem Papierkorb wiederherstellen)
- Restore Dynamic Distribution Group from Recycle Bin (Dynamische Verteilergruppe aus dem Papierkorb wiederherstellen)
- Restore Dynamic Group from Recycle Bin (Dynamische Gruppe aus dem Papierkorb wiederherstellen)
- Restore Resource Mailbox from Recycle Bin (Ressourcenpostfach aus dem Papierkorb wiederherstellen)
- Restore Computer from Recycle Bin (Computer aus dem Papierkorb wiederherstellen)

- Restore Contact from Recycle Bin (Kontakt aus dem Papierkorb wiederherstellen)
- View all Recycle Bin Objects (Alle Objekte im Papierkorb anzeigen)

HINWEIS

- Wenn Sie ein Hilfsadministratorkonto in den Papierkorb verschieben, zeigt DRA weiterhin die Aktivansicht- und Rollenzuweisungen des Kontos an. Anstelle des Namens des gelöschten Hilfsadministratorkontos zeigt DRA die Sicherheits-ID (SID) an. Sie können diese Zuweisungen entfernen, bevor Sie das Hilfsadministratorkonto dauerhaft löschen.
- DRA löscht das Basisverzeichnis, nachdem Sie das Benutzerkonto aus dem Papierkorb gelöscht haben.
- Wenn Sie einen Benutzer löschen, der über eine Office 365-Lizenz verfügt, wird das Benutzerkonto in den Papierkorb verschoben und die Lizenz entfernt. Wenn Sie später das Benutzerkonto wiederherstellen, wird auch die Office 365-Lizenz wiederhergestellt.

VIII Anpassung des Clients

Sie können den Delegierungs- und Konfigurationsclient und die Webkonsole anpassen. Zum Anpassen der Konsolenclients sind ein physischer Zugriff oder Fernzugriff und ein Berechtigungsnachweis erforderlich. Zum Anpassen der Webkonsole sind die Server-URL und die Kontoberechtigung zum Anmelden über einen Webbrowser erforderlich.

23 Delegierungs- und Konfigurationsclient

Dieser Abschnitt beschreibt das Anpassen des Delegierungs- und Konfigurationsclients. Dies umfasst das Erstellen benutzerdefinierter Eigenschaftenseiten, das Erstellen benutzerdefinierter Tools in DRA, die auf Server- und Clientcomputern im Netzwerk ausgeführt werden, und das Anpassen der Konfiguration der Benutzeroberfläche.

Benutzerdefinierte Eigenschaftenseiten

Sie können die Delegierungs- und Konfigurationskonsole anpassen und erweitern, indem Sie benutzerdefinierte Eigenschaften implementieren. Mithilfe von benutzerdefinierten Eigenschaften können Sie proprietäre Eigenschaften für Konten und organisatorische Einheiten zu bestimmten Assistenten und Eigenschaftenfenstern hinzufügen, wie Active Directory-Schemaerweiterungen und virtuelle Attribute. Mit diesen Erweiterungen können Sie DRA Benutzerdefiniert anpassen, um die Lösung an Ihre besonderen Anforderungen anzupassen. Mit dem Assistenten für neue benutzerdefinierte Seiten in der Delegierung- und Konfigurationskonsole können Sie schnell und einfach benutzerdefinierte Seiten erstellen, um die entsprechende Benutzeroberfläche zu erweitern.

Wenn die Hilfsadministratoren einzigartige Befugnisse zur sicheren Verwaltung der benutzerdefinierten Seite benötigen, können Sie auch benutzerdefinierte Befugnisse erstellen und delegieren. Sie können beispielsweise die Verwaltung von Benutzerkonten auf die Eigenschaften beschränken, die auf der benutzerdefinierten Seite enthalten sind. Weitere Informationen finden Sie unter Implementieren von benutzerdefinierten Befugnissen.

Funktionsweise von benutzerdefinierten Eigenschaftenseiten

Erweiterungen der Benutzeroberfläche sind benutzerdefinierte Seiten, die von DRA im entsprechenden Assistenten und in den Eigenschaftenfenstern angezeigt werden. Sie können benutzerdefinierte Seiten zum Anzeigen von Active Directory-Attributen, Schemaerweiterungen und virtuellen Attributen in der Delegierungs- und Konfigurationskonsole konfigurieren.

Wenn Sie ein beliebiges unterstütztes Active Directory-Attribut, eine unterstützte Schemaerweiterung oder ein unterstütztes virtuelles Attribut auswählen, können Sie benutzerdefinierte Seiten auf folgende Weise verwenden:

- Sie können die Verwaltungsbefugnisse der Hilfsadministratoren auf einen klar definierten und kontrollierten Eigenschaftensatz beschränken. Dieser Eigenschaftensatz kann *Standardeigenschaften* und Schemaerweiterungen enthalten. Standardeigenschaften sind Active Directory-Attribute, die standardmäßig über die Konto- und Ressourcenverwaltungskonsole angezeigt werden.
- Sie können Active Directory-Attribute anzeigen, die keine von DRA verwalteten Standardeigenschaften darstellen.
- Sie können die Delegierungs- und Konfigurationskonsole mit proprietären Eigenschaften erweitern.

Außerdem können Sie konfigurieren, wie DRA diese Eigenschaften anzeigt und anwendet. Sie können beispielsweise Steuerelemente mit standardmäßigen Eigenschaftenwerten für die Benutzeroberfläche definieren.

DRA wendet benutzerdefinierte Seiten auf alle anwendbaren verwalteten Objekte im Unternehmen an. Wenn Sie beispielsweise eine benutzerdefinierte Seite erstellen, um Active Directory-Schemaerweiterungen zum Fenster der Gruppeneigenschaften hinzuzufügen, wendet DRA die Eigenschaften auf dieser Seite auf jede verwaltete Gruppe in einer Domäne an, die die spezifizierten Schemaerweiterungen unterstützt. Für jede benutzerdefinierte Seite ist ein eindeutiger Eigenschaftensatz erforderlich. Sie können ein Active Directory-Attribut nicht zu mehr als einer benutzerdefinierten Seite hinzufügen.

Sie können keine einzelnen Fenster oder Registerkarten der vorhandenen Benutzeroberfläche deaktivieren. Ein Hilfsadministrator kann einen Eigenschaftswert entweder über die standardmäßige Benutzeroberfläche oder über eine benutzerdefinierte Seite auswählen. DRA wendet den zuletzt ausgewählten Wert für eine Eigenschaft an.

DRA liefert eine vollständige Revisionsliste für benutzerdefinierte Eigenschaften. DRA protokolliert die folgenden Daten im Ereignisprotokoll der Anwendung:

- Änderungen an benutzerdefinierten Seiten

  WICHTIG: Sie müssen die Revision des Windows-Anwendungsprotokolls manuell konfigurieren. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel *How do I re-enable DRA to write events to the Application Event log in DRA 8.5 and later?* (Wie lege ich in DRA 8.5 und höher fest, dass DRA Ereignisse wieder in das Anwendungsereignisprotokoll schreibt?).

- Erstellung und Löschung von benutzerdefinierten Seiten
- Dargestellte Schemaerweiterungen, Active Directory-Attribute und virtuelle Attribute, die auf benutzerdefinierten Seiten enthalten sind

Sie können auch Änderungsaktivitätsberichte ausführen, um die Konfigurationsänderungen der benutzerdefinierten Eigenschaften zu überwachen.

Implementieren und ändern Sie benutzerdefinierte Seiten über den primären Verwaltungsserver. Während der Synchronisierung reproduziert DRA die Konfigurationen der benutzerdefinierten Seiten im Multi-Master-Set. Weitere Informationen finden Sie unter Konfigurieren des Multi-Master-Sets.

Unterstützte benutzerdefinierte Seiten

Für jede benutzerdefinierte Seite, die Sie erstellen, können Sie einen Satz an Active Directory-Eigenschaften, Schemaerweiterungen und virtuellen Attributen auswählen und diese Eigenschaften auf einer benutzerdefinierten Registerkarte darstellen. Sie können die folgenden Arten von benutzerdefinierten Seiten erstellen:

Benutzerdefinierte Benutzerseite

Ermöglicht das Anzeigen von benutzerdefinierten Registerkarten in den folgenden Fenstern:

- Benutzereigenschaftenfenster
- Assistent zum Erstellen von Benutzern
- Assistent zum Klonen von Benutzern

Benutzerdefinierte Gruppenseite

Ermöglicht das Anzeigen von benutzerdefinierten Registerkarten in den folgenden Fenstern:

- Gruppeneigenschaftenfenster
- Assistent zum Erstellen von Gruppen
- Assistent zum Klonen von Gruppen

Benutzerdefinierte Computerseite

Ermöglicht das Anzeigen von benutzerdefinierten Registerkarten in den folgenden Fenstern:

- Computereigenschaftenfenster
- Assistent zum Erstellen von Computern

Benutzerdefinierte Kontaktseite

Ermöglicht das Anzeigen von benutzerdefinierten Registerkarten in den folgenden Fenstern:

- Kontakteigenschaftenfenster
- Assistent zum Erstellen von Kontakten
- Assistent zum Klonen von Kontakten

Benutzerdefinierte Seite für organisatorische Einheit

Ermöglicht das Anzeigen von benutzerdefinierten Registerkarten in den folgenden Fenstern:

- Eigenschaftenfenster für organisatorische Einheit
- Assistent zum Erstellen von organisatorischen Einheiten
- Assistent zum Klonen von organisatorischen Einheiten

Benutzerdefinierte Ressourcenpostfachseite

Ermöglicht das Anzeigen von benutzerdefinierten Registerkarten in den folgenden Fenstern:

- Fenster der Ressourcenpostfacheigenschaften
- Assistent zum Erstellen von Ressourcenpostfächern
- Assistent zum Klonen von Ressourcenpostfächern

Benutzerdefinierte Seite für dynamische Verteilergruppe

Ermöglicht das Anzeigen von benutzerdefinierten Registerkarten in den folgenden Fenstern:

- Eigenschaftenfenster für dynamische Verteilergruppen
- Assistent zum Erstellen von dynamischen Verteilergruppen
- Assistent zum Klonen von dynamischen Verteilergruppen

Unterstützte Steuerelemente für benutzerdefinierte Eigenschaften

Wenn Sie ein Active Directory-Attribut, eine Schemaerweiterung oder ein virtuelles Attribut zu einer benutzerdefinierten Seite hinzufügen, konfigurieren Sie auch das Steuerelement der Benutzeroberfläche, über das der Hilfsadministrator den Eigenschaftswert eingeben kann. Sie können Eigenschaftswerte beispielsweise auf die folgenden Weisen angeben:

- Definieren eines spezifischen Wertebereichs
- Festlegen standardmäßiger Eigenschaftswerte
- Festlegen, ob eine Eigenschaft erforderlich ist

Sie können das Steuerelement der Benutzeroberfläche auch zum Anzeigen von proprietären Informationen oder Anweisungen konfigurieren. Wenn Sie beispielsweise einen spezifischen Bereich für eine Mitarbeiter-ID definieren, können Sie die Beschriftung des Textfeldsteuerelements so konfigurieren, dass es die Zeichenfolge **Mitarbeiter-Idee angeben (001 bis 100)** anzeigt.

Jedes Benutzeroberflächensteuerelement unterstützt ein einzelnes Active Directory-Attribut, eine einzelne Schemaerweiterung oder ein einzelnes virtuelles Attribut. Konfigurieren Sie die folgenden Steuerelemente der Benutzeroberfläche abhängig vom Eigenschaftentyp:

Typ des Active Directory-Attributs	Unterstützte Benutzeroberflächensteuerelemente
Boolesch	Kontrollkästchen
Datum	Kalendersteuerelement
Integer	Textfeld (Standard) Auswahlliste
Zeichenkette	Textfeld (Standard) Auswahlliste Objektauswahl
Mehrwertige Zeichenkette	Auswahlliste

Arbeiten mit benutzerdefinierten Seiten

Sie können benutzerdefinierte Seiten über den Knoten „User Interface Extensions“ (Benutzeroberflächenerweiterungen) erstellen. Nachdem Sie eine Seite erstellt haben, können Sie AD-Attributeigenschaften hinzufügen oder entfernen und die Seite deaktivieren oder löschen. Erstellen Sie für jede Anpassung, die Sie konfigurieren möchten, eine benutzerdefinierte Seite und weisen Sie dem Hilfsadministrator die entsprechende Befugnis oder Rolle zu. Beachten Sie beim Arbeiten mit benutzerdefinierten Seiten die folgenden bewährten Methoden:

1. Um sicherzustellen, dass DRA die Active Directory-Attribute, Schemaerweiterungsattribute und virtuellen Attribute erkennt, starten Sie den NetIQ Administration-Service auf jedem Verwaltungsserver neu.
2. Identifizieren Sie die Art der benutzerdefinierten Seite, die Sie erstellen möchten, und die Eigenschaften, die von den Hilfsadministratoren mithilfe dieser Seite verwaltet werden sollen. Sie können beliebige Active Directory-Attribute auswählen, einschließlich Schemaerweiterungsattributen und Attributen in vorhandenen DRA-Assistenten und Eigenschaftenfenstern sowie beliebige virtuelle Attribute, die Sie erstellen. Für jede benutzerdefinierte Seite ist jedoch ein eindeutiger Eigenschaftensatz erforderlich. Sie können ein Active Directory-Attribut nicht zu mehr als einer benutzerdefinierten Seite hinzufügen.

   Benutzerdefinierte Seiten ersetzen nicht die vorhandene Benutzeroberfläche. Weitere Informationen hierzu finden Sie in Funktionsweise von benutzerdefinierten Eigenschaftenseiten und Unterstützte benutzerdefinierte Seiten.
3. Legen Sie fest, wie die Hilfsadministratoren diese Eigenschaften festlegen sollen. Sie können beispielsweise eine bestimmte Eigenschaft auf nur drei mögliche Werte beschränken. Für jede Eigenschaft können Sie ein geeignetes Steuerelement in der Benutzeroberfläche definieren. Weitere Informationen finden Sie unter Unterstützte Steuerelemente für benutzerdefinierte Eigenschaften.
4. Ermitteln Sie, ob die Hilfsadministratoren zum erfolgreichen Verwalten der Eigenschaften proprietäre Informationen oder Anweisungen benötigen. Legen Sie beispielsweise fest, ob Active Directory für den Eigenschaftswert eine besondere Syntax erfordert, wie einen eindeutigen Namen (DN) oder einen LDAP-Pfad.
5. Bestimmen Sie die Reihenfolge, in der die Eigenschaften auf der benutzerdefinierten Seite angezeigt werden sollen. Sie können die Anzeigereihenfolge jederzeit ändern.
6. Legen Sie fest, wie DRA die benutzerdefinierte Seite verwenden soll. Sie können beispielsweise eine benutzerdefinierte Benutzerseite zum Assistenten „New User“ (Neuer Benutzer) und zum Fenster „User Properties“ (Benutzereigenschaften) hinzufügen.
7. Überprüfen Sie über die Registerkarte „Zuweisungen“ im Bereich der Hilfsadministratordetails, ob die Hilfsadministratoren über geeignete Befugnisse für den richtigen Objektsatz verfügen. Wenn sie benutzerdefinierte Befugnisse für die benutzerdefinierte Seite erstellt haben, delegieren Sie diese Befugnisse den entsprechenden Hilfsadministratoren.
8. Ermitteln Sie, ob die Hilfsadministratoren zum Verwalten der Eigenschaften auf der Seite eine benutzerdefinierte Befugnis benötigen. Wenn Sie beispielsweise eine benutzerdefinierte Seite zum Fenster „User Properties“ (Benutzereigenschaften) hinzufügen, erhält der Hilfsadministrator durch Delegieren der Befugnis *Modify All User Properties* (Alle Benutzereigenschaften ändern) möglicherweise zu umfangreiche Befugnisse. Erstellen Sie die erforderlichen benutzerdefinierten Befugnisse zum Implementieren der benutzerdefinierten Seite. Weitere Informationen finden Sie unter Implementieren von benutzerdefinierten Befugnissen.

9. Erstellen Sie mithilfe der Antworten aus den obigen Schritten geeignete benutzerdefinierte Seiten.
10. Übermitteln Sie den entsprechenden Hilfsadministratoren, zum Beispiel den Helpdesk-Mitarbeitern, alle erforderlichen Informationen über die benutzerdefinierten Eigenschaftenseiten, die Sie implementiert haben.

Zum Implementieren von Eigenschaftenanpassungen benötigen Sie die Befugnisse, die in der Rolle „DRA Administration“ (DRA-Verwaltung) enthalten sind. Weitere Informationen zu benutzerdefinierten Seiten finden Sie in Funktionsweise von benutzerdefinierten Eigenschaftenseiten.

Erstellen benutzerdefinierter Eigenschaftenseiten

Durch Erstellen verschiedener benutzerdefinierter Seiten können Sie verschiedene benutzerdefinierte Eigenschaften erstellen. Neue benutzerdefinierte Seiten sind standardmäßig aktiviert.

Wenn Sie eine benutzerdefinierte Seite erstellen, können Sie diese deaktivieren. Eine deaktivierte benutzerdefinierte Seite wird in der Benutzeroberfläche ausgeblendet. Wenn Sie mehrere benutzerdefinierte Seiten erstellen, kann es hilfreich sein, die Seiten zu deaktivieren, bis die Anpassungen getestet und fertiggestellt sind.

HINWEIS: Computerkonten erben die Active Directory-Attribute von den Benutzerkonten. Wenn Sie das Active Directory-Schema um zusätzliche Attribute für Benutzerkonten erweitern, können Sie diese Attribute auswählen, wenn Sie eine benutzerdefinierte Seite zum Verwalten von Computerkonten erstellen.

So erstellen Sie eine benutzerdefinierte Eigenschaftsseite:

1 Navigieren Sie zum Knoten **Konfigurationsmanagement** > **User Interface Extensions** (Erweiterung der Benutzerschnittstellen).

2 Klicken Sie im Aufgabenmenü auf **New** (Neu) und klicken Sie dann auf das entsprechende Menüelement für die zu erstellende benutzerdefinierte Seite.

3 Geben Sie auf der Registerkarte „General“ (Allgemein) den Namen der benutzerdefinierten Seite ein und klicken Sie dann auf **OK**. Wenn Sie die Seite deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Enabled** (Aktiviert).

4 Führen Sie für jede Eigenschaft, die auf der benutzerdefinierten Seite eingeschlossen werden soll, die folgenden Schritte aus:

4a Klicken Sie auf der Registerkarte „Properties“ (Eigenschaften) auf **Add** (Hinzufügen).

4b Um eine Eigenschaft auszuwählen, klicken Sie auf **Browse** (Durchsuchen).

4c Geben Sie im Feld **Control label** (Beschriftung des Steuerelements) den Eigenschaftennamen ein, den DRA als Beschriftung für das Steuerelement in der Benutzeroberfläche verwenden soll. Achten Sie darauf, eine benutzerfreundliche und selbsterklärende Beschriftung zu verwenden. Sie können auch Anweisungen, gültige Wertebereiche oder Syntaxbeispiele angeben.

4d Wählen Sie im Menü **Control type** (Steuerelementtyp) das geeignete Steuerelement für die Benutzeroberfläche aus.

4e Wählen Sie aus, wo in der Delegierungs- und Konfigurationskonsole DRA diese benutzerdefinierte Seite anzeigen soll.

4f Um zusätzliche Attribute festzulegen, beispielsweise eine Mindestlänge oder Standardwerte, klicken Sie auf **Advanced** (Erweitert).

4g Klicken Sie auf **OK**.

5 Um die Reihenfolge zu ändern, in der DRA diese Eigenschaften auf der benutzerdefinierten Seite anzeigt, wählen Sie die entsprechende Eigenschaft aus und klicken Sie auf **Move Up** (Nach oben verschieben) oder **Move Down** (Nach unten verschieben).

6 Klicken Sie auf **OK**.

Ändern benutzerdefinierter Eigenschaften

Sie können eine benutzerdefinierte Seite ändern, indem Sie die benutzerdefinierten Eigenschaften ändern.

So ändern Sie benutzerdefinierte Eigenschaften:

1 Navigieren Sie zum Knoten **Konfigurationsmanagement** > **User Interface Extensions** (Erweiterung der Benutzerschnittstellen).

2 Wählen Sie im Listenbereich die gewünschte benutzerdefinierte Seite aus.

3 Klicken Sie im Aufgabenmenü auf **Properties** (Eigenschaften).

4 Ändern Sie die gewünschten Eigenschaften und Einstellungen der benutzerdefinierten Seite.

5 Klicken Sie auf **OK**.

Identifizieren von Active Directory-Attributen, die mit benutzerdefinierten Seiten verwaltet werden

Sie können schnell identifizieren, welche Active Directory-Eigenschaften, Schemaerweiterungen oder virtuellen Attribute mit einer bestimmten benutzerdefinierten Seite verwaltet werden.

So identifizieren Sie Active Directory-Eigenschaften, die mit benutzerdefinierten Seiten verwaltet werden:

1 Navigieren Sie zum Knoten **Konfigurationsmanagement** > **User Interface Extensions** (Erweiterung der Benutzerschnittstellen).

2 Wählen Sie im Listenbereich die gewünschte benutzerdefinierte Seite aus.

3 Klicken Sie im Detailbereich auf die Registerkarte **Properties** (Eigenschaften). Um den Detailbereich anzuzeigen, klicken Sie im Anzeigemenü auf **Details**.

4 Um zu überprüfen, wie DRA eine Eigenschaft anzeigt und anwendet, wählen Sie das entsprechende Active Directory-Attribut, die Schemaerweiterung oder das virtuelle Attribute aus der Liste aus und klicken Sie auf das Symbol **Properties** (Eigenschaften).

Aktivieren, Deaktivieren und Löschen von benutzerdefinierten Seiten

Wenn Sie eine benutzerdefinierte Seite aktivieren, fügt DRA diese benutzerdefinierte Seite zu den verknüpften Assistenten und Fenstern hinzu. Um festzulegen, welche Assistenten und Fenster eine benutzerdefinierte Seite anzeigen sollen, ändern Sie die Eigenschaften der benutzerdefinierten Seite.

HINWEIS: Um sicherzustellen, dass jede benutzerdefinierte Seite einen eindeutigen Eigenschaftensatz anzeigt, aktiviert DRA keine benutzerdefinierten Seiten, die Eigenschaften enthalten, welche bereits auf anderen benutzerdefinierten Seiten angezeigt werden.

Wenn Sie eine benutzerdefinierte Seite deaktivieren, entfernt DRA diese benutzerdefinierte Seite aus den verknüpften Assistenten und Fenstern. DRA löscht nicht die benutzerdefinierte Seite. Um sicherzustellen, dass eine bestimmte benutzerdefinierte Seite nie in der Benutzerfläche angezeigt wird, löschen Sie die benutzerdefinierte Seite.

Wenn Sie eine benutzerdefinierte Seite löschen, entfernt DRA diese benutzerdefinierte Seite aus den verknüpften Assistenten und Fenstern. Eine gelöschte benutzerdefinierte Seite kann nicht wiederhergestellt werden. Um eine benutzerdefinierte Seite vorübergehend aus der Benutzeroberfläche zu entfernen, deaktivieren Sie die benutzerdefinierte Seite.

Um eine benutzerdefinierte Seite zu aktivieren, deaktivieren oder löschen, navigieren Sie zum Knoten **Konfigurationsmanagement** > **User Interface Extensions** (Benutzeroberflächenerweiterungen) und wählen Sie im Aufgaben- oder Kontextmenü die gewünschte Aktion aus.

Befehlszeilenschnittstelle

Über die Befehlszeilenschnittstelle können Sie mithilfe von Befehlen oder Batchdateien auf leistungsfähige Verwaltungsproduktfunktionen zugreifen und diese anwenden. Mit der Befehlszeilenschnittstelle können Sie durch Eingabe nur eines Befehls Änderungen für mehrere Objekte implementieren.

Wenn Sie beispielsweise die Basisverzeichnisse von 200 Mitarbeitern auf einen neuen Server migrieren müssen, können Sie in der Befehlszeilenschnittstelle den folgenden einfachen Befehl eingeben und dadurch alle 200 Benutzerkonten ändern:

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE
HOMEDIR:\\HOU2\USERS\@Target()
```

Dieser Befehl weist DRA an, das Basisverzeichnisfeld von jedem der 200 Benutzerkonten in den Gruppen `HOU_SALES` und `HOU_MIS` in `\\HOU2\USERS\`*user_id* zu ändern. Um diese Aufgabe mit den nativen Verwaltungswerkzeugen von Microsoft Windows auszuführen, müssten Sie mindestens 200 separate Aktionen ausführen.

HINWEIS: Die Befehlszeilenschnittstelle wird in zukünftigen Versionen als veraltet betrachtet werden, während neue Funktionen zur PowerShell hinzugefügt werden.

Benutzerdefinierte Tools

Mit benutzerdefinierten Tools kann eine beliebige Anwendung zur Ausführung auf Client- und Servercomputern im Netzwerk aufgerufen werden, indem ein beliebiges von DRA verwaltetes Active Directory-Konto ausgewählt wird.

DRA unterstützt zwei Arten von benutzerdefinierten Tools:

- Benutzerdefinierte Tools, die übliche Desktop-Dienstprogramme starten, wie Microsoft Office
- Benutzerdefinierte Tools, die Sie erstellen und auf jeden DRA-Clientcomputer verteilen

Sie können ein benutzerdefiniertes Tool erstellen, das von allen Computern, auf denen der DRA-Client installiert ist, eine Virenprüfung startet. Sie können auch ein benutzerdefiniertes Tool erstellen, das eine externe Anwendung startet, oder ein Tool, das DRA regelmäßig zum Aktualisieren eines Skripts zwingt. Diese regelmäßigen Aktualisierungen können Änderungen in der Konfiguration oder Änderungen einer Geschäftsregel darstellen. Nach den periodischen Aktualisierungen reproduziert DRA die benutzerdefinierten Tools vom primären Verwaltungsserver auf die sekundären Verwaltungsserver und die DRA-Clientcomputer.

Erläuterungen zur Reproduktion der benutzerdefinierten Tools im Multi-Master-Set des Servers finden Sie in Dateireproduktion.

Erstellen benutzerdefinierter Tools

Sie können benutzerdefinierte Tools auf dem DRA-Primärserver erstellen, indem Sie eine Verknüpfung entweder zu einem ausgewählten Active Directory-Objekt oder zu allen Active Directory-Objekten herstellen, die im Assistenten zum Erstellen des benutzerdefinierten Tools angezeigt werden. Das benutzerdefinierte Tool wird mittels Dateireproduktion auf die Sekundärserver im MMS und auf die DRA-Clients reproduziert.

Ein neues benutzerdefiniertes Tool erstellt je nach Bedarf ein Menü und ein Untermenü, um den Vorgang für die verknüpften Active Directory-Objekte in DRA auszuführen.

Sie können Hilfsadministratoren die erforderlichen Befugnisse delegieren, damit sie benutzerdefinierte Tools erstellen und ausführen können und auf die Anwendungen zugreifen und diese ausführen können.

Beim Erstellen eines benutzerdefinierten Tools müssen Sie wie folgt die Parameter eingeben:

Registerkarte „General“ (Allgemein)

1. **Name:** Beliebiger erforderlicher Kundenname für das Tool.
2. **Menu and Submenu** (Menü und Untermenü): Um einen Menüeintrag für ein neues benutzerdefiniertes Tool zu erstellen, geben Sie den Menütitel im Feld **Menu and Submenu Structure** (Menü- und Untermenüstruktur) ein. Wenn Sie ein benutzerdefiniertes Tool erstellen und das Objekt auswählen, zeigt DRA den Menüeintrag des benutzerdefinierten Tools über die Menu- und Untermenüstruktur an, die Sie im Aufgabenmenü, im Verknüpfungsmenü und in der DRA-Symbolleiste festlegen.

   Beispielstruktur für Menü und Untermenü: Geben Sie den Namen für den Menüeintrag ein, gefolgt von einem umgekehrten Schrägstrich (\) und dem Namen des Untermenüeintrags.

Festlegen einer Zugriffstaste: Geben Sie ein kaufmännisches Und-Zeichen (&) vor dem Namen des Menüeintrags ein.

a. Beispiel: `SendEmail\ApproveAction` ---- `SendEmail`ist das Menü und `ApproveAction` ist das Untermenü; der erste Buchstabe „A“ in `ApproveAction` wird als Zugriffstaste aktiviert.

3. **Enabled** (Aktiviert): Aktivieren Sie dieses Kontrollkästchen, um das benutzerdefinierte Werkzeug zu aktivieren.
4. **Description** (Beschreibung): Sie können einen beliebigen Beschreibungswert hinzufügen.
5. **Comment** (Kommentar): Sie können beliebige erforderliche Kommentare zum benutzerdefinierten Tool hinzufügen.

Registerkarte „Supported Objects“ (Unterstützte Objekte)

Wählen Sie das erforderliche AD-Objekt oder alle AD-Objekte aus, mit denen das erstellte benutzerdefinierte Tool verknüpft werden soll.

Zurzeit werden die folgenden Optionen für benutzerdefinierte Tools unterstützt: verwaltete Domänen, Container, Benutzer, Kontakte, Gruppen, Computer, organisatorische Einheiten und veröffentlichte Drucker.

HINWEIS: Andere neu eingeführte Objekte wie Ressourcenpostfächer, dynamische Gruppen und dynamische Exchange-Gruppen werden mit benutzerdefinierten Tools nicht unterstützt.

Registerkarte „Application Settings“ (Anwendungseinstellungen)

Location of the application (Speicherort der Anwendung): Geben Sie den Pfad/Speicherort an, an dem die Anwendung installiert ist. Sie können entweder den genauen Anwendungspfad kopieren und einfügen oder die Option **Insert** (Einfügen) verwenden.

Dieser Pfad muss auf allen DRA-Servern im MMS bereits vorhanden sein. Bei Bedarf können Sie mit der Dateireproduktion eine Datei zu einem nutzbaren Pfad auf den MMS-Servern hochladen und reproduzieren, bevor Sie ein neues benutzerdefiniertes Tool erstellen.

Sie können den Speicherort der externen Anwendung in diesem Feld auch anhand von DRA-Variablen, Umgebungsvariablen und Registrierungswerten angeben. Um diese Variablen zu verwenden, klicken Sie auf **Insert** (Einfügen) und wählen Sie die Variablen aus, die Sie verwenden möchten.

Geben Sie nach dem Einfügen der Variable einen umgekehrten Schrägstrich (\) und dann den Rest des Anwendungspfads einschließlich Namen der ausführbaren Datei der Anwendung ein.

Beispiele:

- *Beispiel 1:*Um den Speicherort einer externen Anwendung anzugeben, die vom benutzerdefinierten Tool ausgeführt wird, wählen Sie die Umgebungsvariable {%PROGRAMFILES%} aus und geben Sie dann den Rest des Anwendungspfads im Feld „Location of the application“ (Speicherort der Anwendung) an: {%PROGRAMFILES%}\ABC `Associates\VirusScan\Scan32.exe`

HINWEIS: DRA stellt den Registrierungswert für das Office-Installationsverzeichnis als Beispiel bereit. Um einen Registrierungsschlüssel festzulegen, der einen Pfad als Wert enthält, verwenden Sie die folgende Syntax:
`{HKEY_LOCAL_MACHINE\SOFTWARE\MyProduct\SomeKey\(Default)}`

- *Beispiel 2:* Um den Speicherort einer benutzerdefinierten Skriptdatei anzugeben, die vom benutzerdefinierten Tool ausgeführt werden soll, wählen Sie die DRA-Variable `{DRA_Replicated_Files_Path}` aus und geben Sie dann den Rest des Pfads zur Skriptdatei im Feld „Location of the application“ (Speicherort der Anwendung) an: `{DRA_Replicated_Files_Path}\cscript.vbs`; wobei `{DRA_Replicated_Files_Path}` der Pfad der reproduzierten Datei ist oder der Ordner `{DRAInstallDir}\FileTransfer\Replicate` auf dem Verwaltungsserver.

HINWEIS: Bevor Sie das benutzerdefinierte Tool erstellen, laden Sie die Skriptdatei mithilfe der Dateireproduktionsfunktion auf den primären Verwaltungsserver hoch. Die Dateireproduktionsfunktion lädt die Skriptdatei in den Ordner `{DRAInstallDir}\FileTransfer\Replicate` auf dem primären Verwaltungsserver hoch.

- *Beispiel 3:* Um den Speicherort eines DRA-Dienstprogramms anzugeben, das vom benutzerdefinierten Tool ausgeführt wird, wählen Sie die DRA-Variable `{DRA_Application_Path}` aus und geben Sie dann den Rest des Pfades zum Dienstprogramm im Feld „Location of the application“ (Speicherort der Anwendung) an: `{DRA_Application_Path}\DRADiagnosticUtil.exe`; `{DRA_Application_Path}` ist dabei der Speicherort, an dem DRA installiert ist.
- *Beispiel 4:* Kopieren Sie einfach den Speicherort der Anwendung zusammen mit dem Anwendungsnamen und der Erweiterung.

Parameters to pass to the application (An die Anwendung zu überreichende Parameter): Um einen Parameter zu definieren, der an eine externe Anwendung überreicht werden soll, geben Sie im Feld „Parameters to pass to the application field“ (An die Anwendung zu überreichende Parameter) einen oder mehrere Parameter durch Kopieren und Einfügen oder durch Eingeben ein. DRA stellt Parameter bereit, die Sie im Feld „Parameters to pass to the application field“ (An die Anwendung zu überreichende Parameter) verwenden können. Um diese Parameter zu verwenden, klicken Sie auf „Insert“ (Einfügen) und wählen Sie den oder die Parameter aus, den/die Sie verwenden möchten. Stellen Sie beim Bereitstellen einer Objekteigenschaft als Parameter sicher, dass der Hilfsadministrator über die erforderliche Leseberechtigung für die Objekteigenschaft und über die Befugnis *Execute Custom Tools* (Benutzerdefinierte Tools ausführen) zum Ausführen des benutzerdefinierten Tools verfügt.

Beispiele:

- *Beispiel 1:*Um den Gruppennamen und den Domänennamen als Parameter an eine externe Anwendung oder einen Skript zu überreichen, wählen Sie die Parameter „Object Property Name“ (Objekteigenschaftsnamen) und „Domain Property Name“ (Domäneneigenschaftsname) aus und geben Sie die Parameternamen im Feld „Parameters to pass to the application“ (An die Anwendung zu überreichende Parameter) an: `"{Object.Name}" "{Domain.$McsName}"`
- *Beispiel 2:* Um den Eingabeparameter „ipconfig“ für die Anwendung „C:\Windows\SysWOW64\cmd.exe“ zu überreichen, geben Sie einfach `"{C:\Windows\SysWOW64\cmd.exe}" "{ipconfig}"` in das Feld ein.

Directory where the application will run (Verzeichnis, in dem die Anwendung ausgeführt wird): Dies ist der Speicherort, an dem die Anwendung auf dem Client- oder Servercomputer ausgeführt werden muss. Sie müssen den Pfad, an dem die Anwendung ausgeführt werden soll, überreichen. Sie können auch genau wie für das Feld „Location of the application“ (Speicherort der Anwendung) die Option „Insert“ (Einfügen) verwenden, um den Parameter weiterzureichen. Die anderen Parameter auf diese Registerkarte sind explizit genug, um die Verwendung zu erklären.

Anpassen der Benutzeroberfläche

Die Konfiguration der Delegierungs- und Konfigurationskonsole kann mit verschiedenen Optionen angepasst werden. Die meisten dieser Optionen bieten die Möglichkeit, Funktionen in den verschiedenen Funktionsbereichen in der Anwendung auszublenden, anzuzeigen oder neu zu konfigurieren. Sie können außerdem die Symbolleiste anzeigen oder ausblenden, den Anwendungstitel anpassen und Spalten hinzufügen, entfernen oder neu anordnen. Alle diese Anpassungsoptionen befinden sich im Menü **View** (Ansicht).

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 „Windows Title“ (Fenstertitel) aus.
4. Legen Sie die gewünschten Optionen fest und klicken Sie auf **OK**. Klicken Sie auf das Fragezeichensymbol **?**, um weitere Informationen anzuzeigen.

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**.

24 Webclient

Im Webclient können Sie Objekteigenschaften, Workflowautomatisierungs-Formulare und das Branding der Benutzeroberfläche anpassen. Richtig implementiert vereinfachen Eigenschaften- und Workflowanpassungen die Automatisierung von Hilfsadministratoraufgaben zur Objektverwaltung und automatisierten Workflowübertragung.

Benutzerdefinierte Eigenschaftenseiten

Sie können die Objekteigenschaftenformulare, die von den Hilfsadministratoren in den Active Directory-Verwaltungsrollen verwendet werden, 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 unter „Anpassung > Eigenschaftenseiten“ 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. Die benutzerdefinierten Behandlungsroutinen für ein Feld werden immer dann ausgeführt, wenn der Wert des Felds geändert wird. Die Zeitsteuerung kann auch konfiguriert werden, d. h der Administrator kann festlegen, ob die Behandlungsroutinen sofort (bei jedem Tastendruck), beim Verlust des Feldfokus oder nach einer bestimmten Verzögerung ausgeführt werden sollen.

Die Objektliste in den Eigenschaftenseiten bietet die folgenden Vorgangstypen für jeden Objekttyp: „Objekt erstellen“ und „Eigenschaften bearbeiten“. Dies sind die hauptsächlichen Vorgänge, die Hilfsadministratoren in der Webkonsole ausführen. Zum Ausführen dieser Vorgänge navigieren die Hilfsadministratoren zu **Verwaltung** > **Suche** oder **Erweiterte Suche**. Hier können sie über das Dropdown-Menü „Erstellen“ Objekte erstellen oder über das Symbol „Eigenschaften“ vorhandene Objekte bearbeiten, die in der Suchergebnistabelle ausgewählt sind.

So passen Sie eine Objekteigenschaftsseite in der Webkonsole an:

1. Melden Sie sich als „DRA Administrator“ an der Webkonsole an.
2. Navigieren Sie zu **Administration** > **Anpassung** > **Eigenschaftenseiten**.
3. Wählen Sie ein Objekt und einen Vorgangstyp (Objekt erstellen oder Objekt bearbeiten) in der Liste der Eigenschaftenseiten aus.
4. Klicken Sie auf das Symbol **Eigenschaften** .

5 Passen Sie das Objekteigenschaftenformular an, indem Sie eine oder mehrere der folgenden Aktionen ausführen und dann die Änderungen anwenden:

- Neue Eigenschaftenseite hinzufügen: **+ Seite hinzufügen**
- Eigenschaftenseiten neu ordnen oder löschen
- Eigenschaftsseite auswählen und anpassen:
  - Konfigurationsfelder in der Seite neu sortieren: ↑ ↓
  - Felder oder untergeordnete Felder bearbeiten:
  - Ein oder mehrere Felder hinzufügen: + oder **Neues Feld einfügen**
  - 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 Hinzufügen benutzerdefinierter Behandlungsroutinen.

Erstellen einer neuen Objekteigenschaftenseite

So erstellen Sie eine neue Objekteigenschaftenseite:

1 Melden Sie sich als „DRA Administrator“ an der Webkonsole an.

2 Navigieren Sie zu **Administration** > **Anpassung** > **Eigenschaftenseiten**.

3 Klicken Sie auf + **Erstellen**.

4 Erstellen Sie das anfängliche Objekteigenschaftenformular, indem Sie den Aktionsnamen, das Symbol, den Objekttyp und die Vorgangskonfiguration definieren.

  Erstellungsaktionen werden zum Dropdown-Menü „Erstellen“ hinzugefügt, während Eigenschaftenaktionen im Objektformular angezeigt werden, wenn der Benutzer ein Objekt in der Suchliste auswählt und bearbeitet.

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

Anpassen von Anforderungsformularen

Die Anforderungsformulare werden beim Erstellen bzw. Bearbeiten auf dem Webserver gespeichert. Der DRA-Administrator verwaltet diese über **Administration** > **Anpassung** > **Anforderungen**. Hilfsadministratoren verwalten sie über **Aufgaben** > **Anforderungen**. Mit diesen Formularen werden automatisierte Workflows gesendet, die auf dem Workflowautomatisierungsserver erstellt werden. Formularersteller nutzen diese Anforderungen, um die Objektverwaltungsaufgaben weiter zu automatisieren und zu verbessern.

Sie können vorhandene Formulareigenschaften und benutzerdefinierte Behandlungsroutinen hinzufügen und ändern. Das Verhalten der Benutzeroberfläche beim Hinzufügen und Anpassen von Eigenschaften ist in einem Workflowautomatisierungsformular und beim Anpassen von Objekteigenschaften im Wesentlichen das gleiche. Eine Ausnahme stellen die Workflowkonfigurationsoptionen und die Steuerelemente zum Festlegen, wer das Formular

verwenden kann, dar. Die Themen unten enthalten weitere Informationen über das Hinzufügen und Ändern von Eigenschaften, dass Hinzufügen von benutzerdefinierten Behandlungsroutinen und über die Workflowautomatisierung im Allgemeinen.

- Benutzerdefinierte Eigenschaftenseiten (Webclient)
- Hinzufügen benutzerdefinierter Behandlungsroutinen
- Automatisierte Workflows

Hinzufügen benutzerdefinierter Behandlungsroutinen

Benutzerdefinierte Behandlungsroutinen werden in DRA dazu verwendet, dass Eigenschaftenattribute zum Erfüllen einer Workflowaufgabe miteinander interagieren. Außerdem werden Sie für Anpassungen der Funktionen zum Laden und Senden in einem Workflow, einer Eigenschaft oder in einem Erstellungsformular.

Benutzerdefinierte Behandlungsroutinen für Eigenschaften

Einige Beispiele für benutzerdefinierte Behandlungsroutinen für Eigenschaften sind folgende:

- Abrufen des Wert anderer Felder
- Aktualisieren von Feldwerten
- Umschalten des Nur-Lesen-Status eines Felds
- Anzeigen oder Ausblenden von Feldern basierend auf konfigurierten Variablen

Behandlungsroutinen zum Laden von Formularen

Behandlungsroutinen zum Laden von Formularen führen typischerweise Initialisierungssteuerungen aus. Sie werden nur einmal beim ersten Laden des Formulars ausgeführt. Bei Eigenschaftenseiten werden sie ausgeführt, bevor der Server auf die Eigenschaften des ausgewählten Objekts abgerufen wird.

Behandlungsroutinen zum Senden von Formularen

Behandlungsroutinen zum Senden von Formularen ermöglichen eine Art der Überprüfung und gegebenenfalls das Abbrechen der Formularübermittlung, falls Fehler erkannt werden.

Ausführlichere Beispiele zum Verwenden von benutzerdefinierten Behandlungsroutinen und Anpassungen in der Webkonsole finden Sie in den Abschnitten „Web Console Customization“ (Anpassung der Webkonsole) und „Workflow Customization“ (Workflowanpassungen) in der Referenz *Product Customization* (Produktanpassung) auf der DRA-Dokumentationsseite.

Benutzerdefiniertes JavaScript aktivieren

Benutzerdefiniertes JavaScript ist aus Sicherheitsgründen standardmäßig deaktiviert. Nach dem Aktivieren von benutzerdefiniertem JavaScript können Administrators JavaScript-Codeausschnitte erstellen, die von der Webkonsole unverändert ausgeführt werden. Sie sollten diese Ausnahme nur aktivieren, wenn Sie die verbundenen Gefahren verstehen und akzeptieren.

So ermöglichen Sie Anpassungen mit benutzerdefiniertem JavaScript-Code:

1. Wechseln Sie zum Speicherort `C:\ProgramData\NetIQ\DRARESTProxy`.
2. Öffnen Sie die Datei `restProxy.config`.
3. Fügen Sie `allowCustomJavaScript="true"`zum Element `<consoleConfiguration>` hinzu.

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 das Eigenschaftensymbol eines Eigenschaftsfelds auf die benutzerdefinierten Behandlungsroutinen der Objekteigenschaft zu. Der Zugriff auf die Behandlungsroutinen zum **Laden des Formulars** und zum **Senden des Formulars** erfolgt über die Schaltfläche **Formulareigenschaften** eines ausgewählten Workflowformulars, einer Objekterstellungsseite oder einer Eigenschaftenbearbeitungsseite.

1. Wählen Sie je nach anzupassender Eigenschaft bzw. Seite die Registerkarte der geeigneten Behandlungsroutine aus:
   - Benutzerdefinierte Behandlungsroutinen
   - Behandlungsroutinen zum Laden von Formularen
   - Behandlungsroutinen zum Senden von Formularen
2. Aktivieren Sie die Behandlungsroutinenseite  und führen Sie einen der folgenden Schritte aus:
   - **Benutzerdefinierte Behandlungsroutine für Eigenschaftenfeld:**
     1. Wählen Sie eine Ausführungszeit aus. *Normalerweise ist die zweite oder dritte Option für die Ausführungszeit geeignet.*
     2. Klicken Sie auf **+ Hinzufügen** und wählen Sie eine benutzerdefinierte Behandlungsroutine im Menü **Benutzerdefinierte Behandlungsroutine hinzufügen**.
   - **Behandlungsroutine für Formular:**Klicken Sie auf **+ Hinzufügen** und wählen Sie eine benutzerdefinierte Behandlungsroutine im Menü **Benutzerdefinierte Behandlungsroutine hinzufügen**.

   HINWEIS: Üblicherweise benötigen Sie nur eine benutzerdefinierte Behandlungsroutine, Sie können jedoch auch mehrere Behandlungsroutinen verwenden. Mehrere Behandlungsroutinen werden der Reihe nach in der aufgeführten Reihenfolge ausgeführt. Wenn Sie die Reihenfolge der Behandlungsroutinen ändern oder eine nicht benötigte Behandlungsroutine überspringen möchten, können Sie Flusskontrollmakros zum Skript hinzufügen.

   ---
3. Sie müssen jede benutzerdefinierte Behandlungsroutine konfigurieren, die Sie zur Seite hinzufügen. Die Konfigurationsoptionen hängen vom Typ der Behandlungsroutinen ab.

   Sie können Ihre eigenen Behandlungsroutinentypen erstellen.
   - **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 Platzhalterwerte in die Pflichtfelder ein. Dies ist erforderlich, damit die Behandlungsroutine ausgeführt wird. Das Skript überschreibt die Platzhalterwerte.

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

---

2. Verwenden Sie in der Aktion vor der Abfrage den Skripteditor, um benutzerdefinierten JavaScript-Code zu erstellen, der vor dem Senden der Abfrage ausgeführt wird. Dieses Skript hat Zugriff auf alle Verbindungsinformationen und Abfrageparameter und kann beliebige dieser Elemente ändern, um die Abfrage benutzerdefiniert anzupassen. Zum Beispiel können Abfrageparameter basierend auf Werten, die der Benutzer im Formular eingegeben hat, festgelegt werden.
3. In der Aktion nach der Abfrage können Sie ein Skript zum Verarbeiten der Abfrageergebnisse einschließen. Übliche Aufgaben sind zum Beispiel das Überprüfen auf Fehler, das Aktualisieren von Werten auf Grundlage der zurückgegebenen Ergebnisse und das Bestätigen der Objekteindeutigkeit basierend auf der Anzahl der von der Abfrage zurückgegebenen Objekte.

- **Skript:** Fügen Sie benutzerdefinierten JavaScript-Code ein, um das Skript zu erstellen.
- **DRA-Abfrage:** Geben Sie die JSON-Nutzlast auf der Registerkarte „Abfrageparameter“ an. Das Nutzlastformat muss mit dem VarSet-Schlüssel oder den Wertepaaren übereinstimmen, die an den DRA-Server gesendet werden. Ähnlich wie bei REST- und LDAP-Abfragen können Sie eine Aktion vor der Abfrage angeben, mit der die Nutzlast vor dem Senden an den Server geändert werden kann, und eine Aktion nach der Abfrage zum Verarbeiten der Ergebnisse.
- **Behandlungsroutinen für Mitteilungsfeld:** Nachdem Sie die Eigenschaften des Mitteilungsfelds definiert haben, können Sie außerdem die JavaScript-Segmente für die **Aktion vor dem Anzeigen** und die **Aktion nach dem Schließen** erstellen.

  Diese Aktionen sind optional. Mit der Aktion vor dem Anzeigen können die Eigenschaften des Mitteilungsfelds angepasst werden, bevor das Mitteilungsfeld für den Benutzer angezeigt wird. Mit der Aktion nach dem Schließen wird die Schaltflächenauswahl des Benutzers verarbeitet und eine damit verbundene, zusätzliche Logik ausgeführt.

4 Klicken Sie auf **OK**, um die Behandlungsroutine zu speichern.

Ausführlichere Beispiele zum Verwenden von benutzerdefinierten Behandlungsroutinen und Anpassungen in der Webkonsole finden Sie in den Abschnitten „Web Console Customization“ (Anpassung der Webkonsole) und „Workflow Customization“ (Workflowanpassungen) in der Referenz *Product Customization* (Produktanpassung) auf der DRA-Dokumentationsseite.

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 DRA-Webkonsole an:

1. Melden Sie sich als „DRA Administrator“ an der Webkonsole an.
2. Wechseln Sie zu **Administration** > **Konfiguration** > **Branding**.
3. Wenn Sie ein Firmenlogobild hinzufügen möchten, speichern Sie das Logobild auf dem Webserver in `inetpub\wwwroot\DRAClient\assets`.
4. Aktualisieren Sie die Konfiguration der Kacheln für den Mastertitel und für die Anmeldung.
5. Klicken Sie nach Abschluss aller Änderungen auf **Speichern**.

IX Tools und Dienstprogramme

Diese Abschnitte beschreiben die mit DRA bereitgestellten Dienstprogramme „ActiveView Analyzer“ (Aktivansicht-Analyse), „Diagnostic“ (Diagnose), „Deleted Object“ (Gelöschtes Objekt), „Health Check“ (Systemdiagnose) und „Recycle Bin“ (Papierkorb).

25 Dienstprogramm „ActiveView Analyzer“ (Aktivansicht-Analyse)

Jede DRA-Aktivansicht enthält eine oder mehrere Regeln, die auf die von einem DRA-Multi-Master-Set verwalteten Active Directory (AD)-Objekte angewendet werden. Das Dienstprogramm „ActiveView Analyzer“ (Aktivansicht-Analyse) überwacht die Verarbeitungszeit jeder DRA-Aktivansicht-Regel, während diese auf die AD-Objekte in einem bestimmten DRA-Vorgang angewendet wird. Während eines DRA-Vorgangs stimmt der DRA-Server die Zielobjekte des Vorgangs mit jeder Regel in jeder Aktivansicht ab. Anschließend erstellt DRA eine Ergebnisliste mit allen zutreffenden Regeln. Das Aktivansicht-Analyseprogramm berechnet, wie lange die Verarbeitung beim Anwenden jeder Regel auf einen DRA-Vorgang gedauert hat.

Mithilfe dieser Informationen können Sie Probleme mit Aktivansichten diagnostizieren, indem Sie nach Anomalien bei der Verarbeitungsdauer der Aktivansichten suchen, unter anderem auch nach Verarbeitungszeiten für nicht verwendete Aktivansichten. Das Dienstprogramm erleichtert außerdem die Suche nach doppelten Aktivansichten.

Nach dem Ausführen einer Datenerfassung und der Anzeige eines Berichts stellen Sie möglicherweise fest, dass die Regeln einer oder mehrerer Aktivansichten geändert werden müssen.

Sie können von jedem DRA-Verwaltungsserver auf das Dienstprogramm „ActiveView Analyzer“ (Aktivansicht-Analyse) zugreifen. Sie sollten das Aktivansicht-Analyseprogramm jedoch auf dem Verwaltungsserver ausführen, auf dem das zu diagnostizierende Problem auftritt.

Um auf das Aktivansicht-Analyseprogramm zuzugreifen, melden Sie sich mit den Berechtigungen der Rolle „DRA Administration“ am Verwaltungsserver an und wechseln Sie vom Startmenü zu **NetIQ Administration** > **ActiveView Analyzer Utility** (Aktivansicht-Analyseprogramm). Alternativ können Sie `ActiveViewAnalyzer.exe` im DRA-Installationspfad `Program Files (x86)\NetIQ\DRA\X64` ausführen.

Mit diesem Dienstprogramm können Sie die folgenden Aufgaben ausführen:

- Daten zu Aktivansichten erfassen
- Analysebericht generieren

Beispiel

Der Hilfsadministrator Paul teilt dem DRA-Administrator Bob mit, dass das Erstellen von Benutzern länger als üblich dauert. Bob startet das Dienstprogramm „ActiveView Analyzer“ für das Benutzerobjekt von Paul und bittet Paul, einen Benutzer zu erstellen. Nach der Datenerfassung erzeugt Bob einen Analysebericht und erkennt, dass eine Regel mit der Bezeichnung „Share MBX“ 50 s lang aufzählt. Bob identifiziert die Aktivansicht, die diese Regel enthält, und stellt nach Änderung der Regel fest, dass das Problem behoben ist.

Starten einer Aktivansicht-Datensammlung

Mit dem Dienstprogramm „ActiveView Analyzer“ (Aktivansicht-Analyse) können Sie Daten zu Aktivansichten von Aktionen, die von Hilfsadministratoren ausgeführt wurden, sammeln. Diese Daten können dann im Analysebericht angezeigt werden. Um Daten zu erfassen, müssen Sie den Hilfsadministrator angeben, für den Daten erfasst werden sollen, und dann die Aktivansicht-Sammlung starten.

HINWEIS: Der Hilfsadministrator, zu dem Daten gesammelt werden sollen, muss mit dem DRA-Server verbunden sein, auf dem auch das Analyseprogramm ausgeführt wird.

So starten Sie eine Aktivansicht-Sammlung:

1. Klicken Sie auf **Start** > **NetIQ Administration** > **ActiveView Analyzer Utility** (Aktivansicht-Analyseprogramm).
2. Geben Sie auf der Seite des Aktivansicht-Analyseprogramms Folgendes an:
   - 2a **Target DRA Server (DRA-Zielserver):** Der DRA-Server, der Leistungsdaten zu den Vorgängen eines Hilfsadministrators sammelt.
   - 2b **Target Assistant Administrator (Ziel-Hilfsadministrator):** Klicken Sie auf „Browse“ (Durchsuchen) und wählen Sie einen Hilfsadministrator aus, für den Daten gesammelt werden sollen.
   - 2c **Monitoring Duration (Überwachungsdauer):** Geben Sie die Gesamtzahl an Stunden an, die zum Erfassen der Analysedaten erforderlich ist. Nach Ablauf der angegebenen Dauer wird die Datensammlung beendet.
3. Klicken Sie auf **Start Collection** (Sammlung starten), um Aktivansichtdaten zu erfassen..

   Nachdem die Sammlung von Aktivansichtdaten gestartet wurde, löscht das Dienstprogramm die vorhandenen Daten und zeigt den letzten Status an.
4. (Optional) Sie können die Datensammlung manuell stoppen, bevor die geplante Zeitdauer abgelaufen ist, und dennoch einen Bericht erzeugen. Klicken Sie auf **Stop Collection** (Sammlung stoppen), um die Aufzeichnung der Hilfsadministratorvorgänge auf Aktivansichten zu stoppen.
5. (Optional) Um den letzten Status abzurufen, klicken Sie auf **Collection Status** (Sammlungsstatus).

WICHTIG: Wenn Sie die Sammlung stoppen und den Hilfsadministrator ändern oder eine Datensammlung für den gleichen Hilfsadministrator wieder starten, löscht das Aktivansicht-Analyseprogramm die vorhandenen Daten. Zu einem gegebenen Zeitpunkt können immer nur Analysedaten von einem Hilfsadministrator auf einmal in der Datenbank enthalten sein.

Generieren eines Analyseberichts

Stoppen Sie das Sammeln von Daten, bevor Sie einen Analysebericht generieren.

Auf der Seite des Aktivansicht-Analyseprogramms wird eine Liste der vom Hilfsadministrator ausgeführten Vorgänge angezeigt. So generieren Sie einen Analysebericht:

1. Klicken Sie auf **Select Report** (Bericht auswählen) und wählen Sie den Bericht, den Sie anzeigen möchten.

2 Klicken Sie auf **Generate Report** (Bericht generieren), um einen Analysebericht mit Details zu Aktivansichtaktionen anzuzeigen. Dies umfasst zum Beispiel die vom Vorgang betroffenen AD-Objekte, die Aktivansicht, von der die aufgelisteten Objekte verwaltet werden, die angewendeten und die nicht zutreffenden Aktivansichtregeln sowie die Verarbeitungsdauer jeder einzelnen Aktivansichtregel.

   Mit dem Bericht können Sie analysieren, welche Regeln länger brauchen, um Vorgänge auszuführen, und dann entscheiden, ob beliebige dieser Regeln geändert oder aus den entsprechenden Aktivansichten gelöscht werden sollen.

3 (Optional) Bewegen Sie den Mauszeiger über das Raster, klicken Sie mit der rechten Maustaste und kopieren Sie den Bericht über das Kopiermenü in die Zwischenablage. Aus der Zwischenablage können Sie die Spaltentitel und Daten in eine andere Anwendung einfügen, beispielsweise in Notepad oder in Excel.

Ermitteln der Leistung von Objekten

So ermitteln Sie die Leistung aller von einer Aktivansicht oder Regel verwalteten Objekte:

1 Starten Sie die Delegierungs- und Konfigurationskonsole.

2 Wechseln Sie zu **Delegation Management** (Delegierungsverwaltung) und klicken Sie auf **Manage ActiveViews** (Aktivansichten verwalten).

3 Führen Sie eine Suche aus, um eine bestimmte Aktivansicht zu finden.

   Von hier können Sie die Regel bzw. das Objekt identifizieren, die/das ein Problem verursacht, und Änderungen vornehmen.

   - Doppelklicken Sie auf die Aktivansicht und wählen Sie **Rules** (Regeln) aus, um die Regeln aufzulisten. Sie können eine bestimmte Regel über das Kontextmenü bearbeiten.
   - Klicken Sie mit der rechten Maustaste auf die Aktivansicht und wählen Sie **Show Managed Objects** (Verwaltete Objekte anzeigen) aus, um die Objekte aufzulisten. Sie können ein Objekt durch Klicken mit der rechten Maustaste und Auswählen von **Properties** (Eigenschaften) ändern.

4 Nehmen Sie Änderungen an der Regel oder am verwalteten Objekt vor und überprüfen Sie, ob die Änderungen das Problem behoben haben.

26 Dienstprogramm „Diagnostic“ (Diagnose)

Das Diagnoseprogramm sammelt Informationen vom Verwaltungsserver, die bei der Diagnose von Problemen mit DRA hilfreich sein können. Verwenden Sie dieses Dienstprogramm, um einem Mitarbeiter des technischen Supports Protokolldateien bereitzustellen. Das Diagnoseprogramm bietet eine Assistentenoberfläche, die Sie durch das Festlegen des Protokollierumfangs und Sammeln von Diagnoseinformationen führt.

Sie können von einem beliebigen Verwaltungsservercomputer auf das Diagnoseprogramm zugreifen. Sie sollten das Diagnoseprogramm jedoch auf dem Verwaltungsserver ausführen, auf dem das zu diagnostizierende Problem auftritt.

Um auf das Diagnoseprogramm zuzugreifen, melden Sie sich mit einem Administratorkonto mit lokalen Administratorrechten am Verwaltungsserver-Computer an und öffnen Sie das Dienstprogramm über die Programmgruppe „NetIQ Administration“ im Windows-Startmenü.

Weitere Informationen zu diesem Dienstprogramm erhalten Sie vom Technischen Support.

27 Dienstprogramm „Deleted Objects“ (Gelöschte Objekte)

Mit diesem Dienstprogramm können Sie die Unterstützung für die inkrementelle Aktualisierung des Konto-Cache für eine bestimmte Domäne aktivieren, wenn das Domänenzugriffskonto kein Administratorkonto ist. Wenn das Domänenzugriffskonto keine Leseberechtigungen für den Container der gelöschten Objekte in dieser Domäne hat, kann DRA keine inkrementelle Aktualisierung des Konto-Cache ausführen.

Mit diesem Dienstprogramm können Sie die folgenden Aufgaben ausführen:

- Überprüfen, ob das angegebene Benutzerkonto bzw. die angegebene Gruppe über Leseberechtigungen für den Container der gelöschten Objekte in der angegebenen Domäne verfügt
- Leseberechtigungen an ein angegebenes Benutzerkonto oder an eine angegebene Gruppe delegieren bzw. Leseberechtigung vom Konto/von der Gruppe entfernen
- Benutzerrecht zum Synchronisieren der Verzeichnisservicedaten an ein Benutzerkonto delegieren bzw. vom Konto entfernen
- Sicherheitseinstellungen für den Container der gelöschten Objekte anzeigen

Sie können die Datei für das Dienstprogramm für gelöschte Objekte (`DraDelObjsUtil.exe`) im Ordner `Program Files (x86)\NetIQ\DRA` auf dem Verwaltungsserver ausführen.

Erforderliche Berechtigungen für das Dienstprogramm „Deleted Objects“ (Gelöschte Objekte)

Um das Dienstprogramm verwenden zu können, benötigen Sie die folgenden Berechtigungen:

Aktion	Erforderliche Berechtigung
Kontoberechtigungen überprüfen	Leseberechtigung für den Container der gelöschten Objekte
Leseberechtigungen für den Container der gelöschten Objekte delegieren	Administratorberechtigungen in der Domäne, in der sich der Container der gelöschten Objekte befindet
Benutzerrecht zum Synchronisieren der Verzeichnisservicedaten delegieren	Administratorberechtigungen in der Domäne, in der sich der Container der gelöschten Objekte befindet
Zuvor delegierte Berechtigungen entfernen	Administratorberechtigungen in der Domäne, in der sich der Container der gelöschten Objekte befindet
Sicherheitseinstellungen für den Container der gelöschten Objekte anzeigen	Leseberechtigung für den Container der gelöschten Objekte

Syntax für das Dienstprogramm „Deleted Objects“ (Gelöschte Objekte)

```
DRADELOBJSUTIL /DOMAIN:DOMAENENNAME[/DC:COMPUTERNAME] {/
DELEGATE:KONTONAME| /VERIFY:KONTONAME| /REMOVE:KONTONAME| /DISPLAY [/
RIGHT]}
```

Optionen für das Dienstprogramm „Deleted Objects“ (Gelöschte Objekte)

Sie können die folgenden Optionen festlegen:

/DOMAIN:*Domaene*	Legt den NETBIOS oder DNS-Namen der Domäne fest, in der sich der Container der gelöschten Objekte befindet.
/SERVER:*Computername*	Legt den Namen oder die IP-Adresse des Domänencontrollers für die angegebene Domäne fest.
/DELEGATE:*Kontoname*	Delegiert Berechtigungen an das angegebene Benutzerkonto bzw. der angegebenen Gruppe.
/REMOVE:*Kontoname*	Entfernt Berechtigungen, die zuvor einem bestimmten Benutzerkonto oder einer bestimmten Gruppe delegiert wurden.
/VERIFY:*Kontoname*	Überprüft die Berechtigungen des angegebenen Benutzerkontos bzw. der angegebenen Gruppe.
/DISPLAY	Zeigt die Sicherheitseinstellungen für den Container der gelöschten Objekte in der angegebenen Domäne an.
/RIGHT	Stellt sicher, dass das angegebene Benutzerkonto bzw. die angegebene Gruppe über das Benutzerrecht zum Synchronisieren der Verzeichnisservicedaten verfügt. Mit dieser Option können Sie das Recht delegieren und überprüfen. Das Benutzerrecht zum Synchronisieren der Verzeichnisservicedaten gewährt dem Konto das Recht, alle Objekte und Eigenschaften in Active Directory zu lesen.

HINWEIS

- Wenn der Name des Benutzerkontos oder der Gruppe, den/die Sie angeben möchten, ein Leerzeichen enthält, schließen Sie den Kontonamen in Anführungszeichen ein. Wenn Sie beispielsweise die Gruppe Berlin IT angeben möchten, geben Sie „Berlin IT“ in Anführungszeichen ein.
- Verwenden Sie zum Angeben einer Gruppe den Vor-Windows 2000-Namen der Gruppe.

Beispiele für das Dienstprogramm „Deleted Objects“ (Gelöschte Objekte)

Die folgenden Beispiele zeigen Beispielbefehle für übliche Szenarien.

Beispiel 1

Um zu überprüfen, ob das Benutzerkonto MYCOMPANY\JSmith über Leseberechtigungen für den Container der gelöschten Objekte in der Domäne hou.mycompany.com verfügt, geben Sie Folgendes ein:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Beispiel 2

Um Leseberechtigungen auf den Container der gelöschten Objekte in der Domäne MYCOMPANY an die Gruppe MYCOMPANY\DraAdmins zu delegieren, geben Sie Folgendes ein:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Beispiel 3

Um Leseberechtigungen auf den Container der gelöschten Objekte und das Benutzerrecht zum Synchronisieren der Verzeichnis Servicedaten in der Domäne MYCOMPANY an das Benutzerkonto MYCOMPANY\JSMITH zu delegieren, geben Sie Folgendes ein:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

Beispiel 4

Um die Sicherheitseinstellungen für den Container der gelöschten Objekte in der Domäne hou.mycompany.com mit dem Domänencontroller HQDC anzuzeigen, geben Sie Folgendes ein:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

Beispiel 5

Um Leseberechtigungen auf den Container der gelöschten Objekte in der Domäne MYCOMPANY von der Gruppe MYCOMPANY\DraAdmins zu entfernen, geben Sie Folgendes ein:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

28 Dienstprogramm „Health Check“ (Systemdiagnose)

Das Systemdiagnose-Programm ist eine eigenständige Anwendung, das im DRA-Installationskit enthalten ist. Mit dem Systemdiagnose-Programm können Sie nach der Installation und vor und nach einer Aufrüstung den Status der einzelnen Komponenten und Prozesse des DRA-Servers, der DRA-Website und der DRA-Clients überprüfen, bestätigen und melden. Sie können das Dienstprogramm auch zum Installieren oder Aktualisieren einer Produktlizenz, zum Sichern einer AD LDS-Instanz vor einer Produktaufrüstung, zum Anzeigen von Beschreibungen der Überprüfungen und zum Korrigieren von Problemen oder zum Ermitteln und Bestätigen von Maßnahmen verwenden, die zum Korrigieren der Probleme erforderlich sind.

Das Systemdiagnose-Programm ist im DRA-Programmordner enthalten, nachdem das Installationsprogramm `NetIQAdminInstallationKit.msi` ausgeführt wurde.

Sie können das Systemdiagnose-Programm jederzeit durch Ausführen der Datei `NetIQ.DRA.HealthCheckUI.exe` ausführen. Wenn die Anwendung geöffnet wird, können Sie wahlweise einen bestimmten Vorgang ausführen, Überprüfungen für bestimmte Komponenten ausführen oder Überprüfungen für alle Komponenten ausführen. Nachstehend finden Sie einige nützliche Funktionen, die Sie mit dem Systemdiagnose-Programm ausführen können:

Funktion	Benutzeraktionen
Select All (Alles auswählen), Unselect All (Gesamte Auswahl aufheben)	Über die Optionen der Symbolleiste oder des Dateimenüs können Sie mit den Funktionen **Select** (Auswählen) und **Unselect** (Auswahl aufheben) alle Überprüfungspunkte auswählen bzw. die Auswahl aufheben. Sie können auch einzelne Kontrollkästchen aktivieren, um bestimmte Überprüfungen auszuführen.
Run Selected Checks (Ausgewählte Überprüfungen ausführen)	Mit dieser Option in der Symbolleiste oder im Dateimenü können Sie die ausgewählten Überprüfungen (alle oder bestimmte) ausführen.
Save Results (Ergebnisse speichern), Write Results (Ergebnisse schreiben)	Mit dieser Option der Symbolleiste oder des Dateimenüs können Sie einen detaillierten Bericht für die ausgeführte Überprüfung erstellen und speichern.
Run This Check (Diese Überprüfung ausführen)	Wählen Sie einen Elementtitel aus, um eine Beschreibung der Überprüfung anzuzeigen, und klicken Sie dann auf dieses Symbolleistensymbol, um die Überprüfung auszuführen. Zum Beispiel können Sie einen der folgenden Vorgänge ausführen: ◆ License Validation (Lizenzvalidierung) (Produktlizenz installieren oder aktualisieren) ◆ AD LDS Instance Backup (AD LDS-Instanzsicherung) (AD LDS-Instanz sichern) ◆ Replication (Reproduktion) (Reproduktionsdatenbank validieren)

Funktion	Benutzeraktionen
Fix This Issue (Dieses Problem beheben)	Wählen Sie einen Elementtitel aus und verwenden Sie dann diese Symbolleistenoption, falls eine Überprüfung nicht bestanden wurde. Wenn das Problem beim erneuten Ausführen der Überprüfung nicht behoben ist, sollte die Beschreibung Informationen bzw. Angaben zu Maßnahmen enthalten, die zum Beheben des Problems beitragen können.

29 Dienstprogramm „Recycle Bin“ (Papierkorb)

Mit diesem Dienstprogramm können Sie die Unterstützung für den Papierkorb aktivieren, wenn Sie einen Teilbaum einer Domäne verwalten. Wenn das Domänenzugriffskonto keine Berechtigungen auf den ausgeblendeten NetIQRecycleBin-Container in der angegebenen Domäne hat, kann DRA gelöschte Konten nicht in den Papierkorb verschieben.

HINWEIS: Nachdem Sie den Papierkorb mit diesem Dienstprogramm aktiviert haben, führen Sie eine vollständige Aktualisierung des Konto-Cache aus, um sicherzustellen, dass der Verwaltungsserver diese Änderung anwendet.

Mit diesem Dienstprogramm können Sie die folgenden Aufgaben ausführen:

- Überprüfen, ob das angegebene Konto über Leseberechtigungen für den NetIQRecycleBin-Container in der angegebenen Domäne verfügt
- Leseberechtigungen an ein angegebenes Konto delegieren
- Sicherheitseinstellungen für den NetIQRecycleBin-Container anzeigen

Erforderliche Berechtigungen für das Dienstprogramm „Recycle Bin“ (Papierkorb)

Um das Dienstprogramm verwenden zu können, benötigen Sie die folgenden Berechtigungen:

Aktion	Erforderliche Berechtigung
Kontoberechtigungen überprüfen	Leseberechtigungen für den NetIQRecycleBin-Container
Leseberechtigungen für den NetIQRecycleBin-Container delegieren	Administratorberechtigungen in der angegebenen Domäne
Sicherheitseinstellungen für den NetIQRecycleBin-Container anzeigen	Leseberechtigungen für den NetIQRecycleBin-Container

Syntax für das Dienstprogramm „Recycle Bin“ (Papierkorb)

```
DRARECYCLEBINUTIL /DOMAIN:DOMAENENNAME[/DC:COMPUTERNAME] {/
DELEGATE:KONTONAME| /VERIFY:KONTONAME| /DISPLAY}
```

Optionen für das Dienstprogramm „Recycle Bin“ (Papierkorb)

Mit den folgenden Optionen können Sie das Dienstprogramm „Recycle Bin“ (Papierkorb) konfigurieren:

/DOMAIN:Domaene	Legt den NETBIOS oder DNS-Namen der Domäne fest, in der sich der Papierkorb befindet.
/SERVER:*Computername*	Legt den Namen oder die IP-Adresse des Domänencontrollers für die angegebene Domäne fest.
/DELEGATE:*Kontoname*	Delegiert Berechtigungen an das angegebene Konto.
/VERIFY:*Kontoname*	Überprüft die Berechtigungen des angegebenen Kontos.
/DISPLAY	Zeigt die Sicherheitseinstellungen für den NetIQRecycleBin-Container in der angegebenen Domäne an.

Beispiele für das Dienstprogramm „Recycle Bin“ (Papierkorb)

Die folgenden Beispiele zeigen Beispielbefehle für übliche Szenarien.

Beispiel 1

Um zu überprüfen, ob das Benutzerkonto `MYCOMPANY\JSmith` über Leseberechtigungen für den NetIQRecycleBin-Container in der Domäne `hou.mycompany.com` verfügt, geben Sie Folgendes ein:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Beispiel 2

Um Leseberechtigungen auf den NetIQRecycleBin-Container in der Domäne `MYCOMPANY` an die Gruppe `MYCOMPANY\DraAdmins` zu delegieren, geben Sie Folgendes ein:

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Beispiel 3

Um die Sicherheitseinstellungen für den NetIQRecycleBin-Container in der Domäne `hou.mycompany.com` mit dem Domänencontroller `HQDC` anzuzeigen, geben Sie Folgendes ein:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```