NetIQ Directory and Resource Administrator 10.2

Installationshandbuch

Mai 2022

Rechtliche Hinweise

Informationen zu rechtlichen Hinweisen, Marken, Haftungsausschlüssen, Gewährleistungen, Ausfuhrbeschränkungen und sonstigen Nutzungseinschränkungen, Rechten der US-Regierung, Patentrichtlinien und zur Erfüllung von FIPS finden Sie unter https://www.microfocus.com/en-us/legal.

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

Inhalt

Info zu diesem Handbuch

Das *Installationshandbuch* enthält Informationen zur Planung, Installation, Lizenzierung und Konfiguration von Directory and Resource Administrator (DRA) und den darin enthaltenen Komponenten.

Dieses Handbuch führt Sie durch den Installationsvorgang und unterstützt Sie beim Treffen von Entscheidungen in Bezug auf die Installation und Konfiguration von DRA.

Zielgruppe

Die in diesem Handbuch enthaltenen Informationen richten sich an alle, die DRA installieren.

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.

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 und Exchange Online.
- **Granulare Steuerung des Benutzerzugriffs und Zugriffs mit Administrationsberechtigungen:**

  Die patentierte Aktivansicht-Technologie (ActiveView) 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 und Workflow Automation generiert wurden

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 Workflow Automation-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.).
- **Account and Resource Management (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:

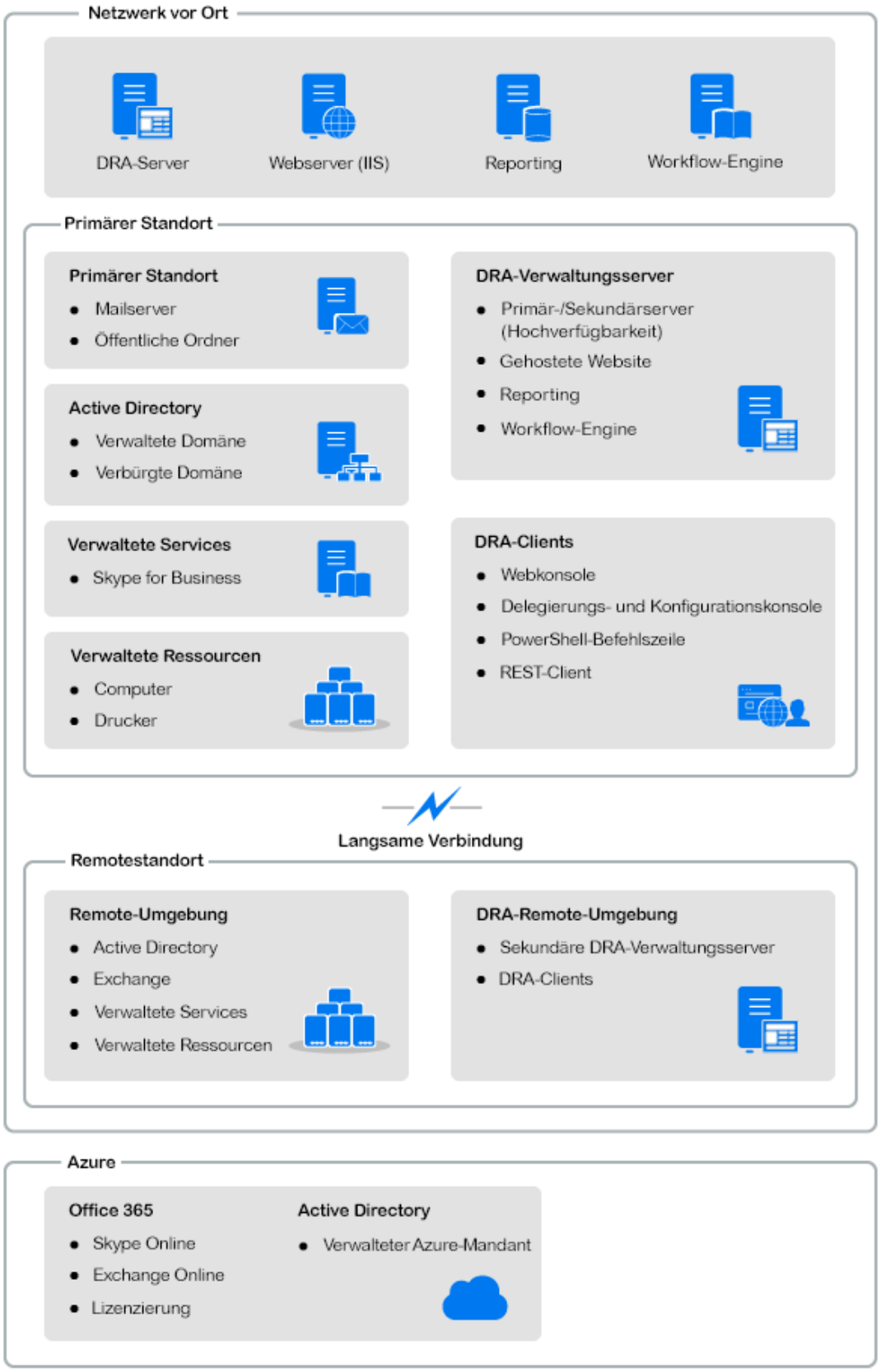
- Ressourcenberichte für Active Directory-Objekte
- Berichte zu Active Directory-Objektdaten
- Active Directory-Zusammenfassungsberichte
- DRA-Konfigurationsberichte
- Exchange-Konfigurationsberichte
- Office 365 Exchange Online-Berichte
- Detaillierte Berichte zu Aktivitätstrends (nach Monat, Domäne 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 Automation-Engine

DRA lässt sich mit der Workflow Automation-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 Automation-Engine finden Sie auf der DRA-Dokumentationswebsite.

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“, auf Seite 18
- „DRA-REST-Server“, auf Seite 20
- „Webkonsole (IIS)“, auf Seite 20
- „DRA-Delegierungs- und -Verwaltungskonsole“, auf Seite 21
- „Workflowserver“, auf Seite 21

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)

Protokoll und Port	Richtung	Ziel	Verwendung
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)
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 Cache DB Service (DRA-Cache-Datenbank-Service)	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

Protokoll und Port	Richtung	Ziel	Verwendung
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 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 und DRA-PowerShell
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 mit Firewalls (DCOM))
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	Operations Console (Betriebskonsole) 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 Automation-Engine und dem Namespace-Anbieter verwendet

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 10117	Localhost	Ressourcenverwaltungs-Namespace-Anbieter	Wird vom Ressourcenverwaltungs-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: ◆ Azure Active Directory V2 (AzureAD) Version 2.0.2.4 oder höher ◆ AzureRM.Profile Version 5.8.2 oder höher ◆ Exchange Online PowerShell V2.0.3 oder höher PowerShell 5.1 oder das neueste Modul ist zum Installieren der neuen Azure PowerShell-Module erforderlich.
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019 ◆ Microsoft Server 2022 ◆ Azure Active Directory
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online O365
Skype for Business	◆ Microsoft Skype for Business 2015
Änderungsverlauf	◆ Change Guardian 6.0 oder höher
Datenbanken	◆ Microsoft SQL Server 2016
Webbrowser	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge
Workflow Automation	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019 ◆ Microsoft Server 2022

Anforderungen an den DRA-Verwaltungsserver und die Webkonsole

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

- „Softwareanforderungen“, auf Seite 23
- „Serverdomäne“, auf Seite 25
- „Kontoanforderungen“, auf Seite 25
- „DRA-Zugriffskonten mit niedrigsten Berechtigungen“, auf Seite 27

Softwareanforderungen

Komponente	Voraussetzungen
Installationsziel	**Betriebssystem des NetIQ Administration-Servers:**
Betriebssystem	◆ Microsoft Windows Server 2012 R2, 2016, 2019, 2022 **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, 2022 ◆ Microsoft Windows 10, 11
Installationsprogramm	◆ Microsoft .Net Framework 4.8 oder höher

Komponente	Voraussetzungen
Verwaltungsserver	**Directory and Resource Administrator:** ◆ Microsoft .Net Framework 4.8 oder höher ◆ Microsoft Visual C++ 2015–2019 Redistributable Packages (x64 und x86) ◆ Microsoft Message Queuing ◆ Microsoft Active Directory Lightweight Directory Services-Rollen ◆ Remoteregistrierungsdienst gestartet ◆ Microsoft Internet Information Services ◆ URL-Rewrite-Modul für Microsoft-Internetinformationsdienste ◆ Routing von Anwendungsanforderungen für Microsoft-Internetinformationsdienste **HINWEIS:** Der NetIQ DRA REST-Service wird mit dem Verwaltungsserver installiert. **Administration von Microsoft Office 365/Exchange Online:** ◆ Windows Azure Active Directory-Modul für Windows PowerShell ◆ Windows PowerShell-Modul ◆ Exchange Online PowerShell V2.0.3 oder höher ◆ Aktivieren Sie WinRM für die Standardauthentifizierung auf der Clientseite für Exchange Online-Aufgaben. Weitere Informationen finden Sie unter Unterstützte Plattformen.
Benutzeroberfläche	**DRA-Benutzeroberflächen:** ◆ Microsoft .Net Framework 4.8 ◆ Microsoft Visual C++ 2015–2019 Redistributable Packages (x64 und x86)
PowerShell-Erweiterungen	◆ Microsoft .Net Framework 4.8 ◆ PowerShell 5.1 oder höher
DRA-Webkonsole	**Webserver:** ◆ Microsoft .Net Framework 4.x > WCF-Dienste > HTTP-Aktivierung ◆ Microsoft Internet Information Server 8.5, 10 ◆ URL-Rewrite-Modul für Microsoft-Internetinformationsdienste ◆ Routing von Anwendungsanforderungen für Microsoft-Internetinformationsdienste **Webserver (IIS)-Komponenten:** ◆ Webserver > Sicherheit > URL-Autorisierung

Serverdomäne

Komponente	Betriebssysteme
DRA-Server	◆ Microsoft Windows Server 2022 ◆ 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

Konto	Beschreibung	Berechtigungen

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 „Configuring DRA Services for a Group Managed Service Account“ (DRA-Services für ein gruppenverwaltetes Servicekonto konfigurieren) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

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 msDS-GroupManagedServiceAccount-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

HINWEIS: Wenn das Active Directory-Schema der verwalteten Domäne nicht für Exchange Online erweitert wird, werden die folgenden Objekte nicht aufgelistet:

- MsExchDynamicDistributionList-Objekte

- MsExchSystemObjectsContainer-Objekte
- publicFolder-Objekte

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 msDS-GroupManagedServiceAccount-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
- Erstellen von Druckerobjekten 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 msDS-GroupManagedServiceAccount-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
- Löschen von Druckerobjekten 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 Sie das Konto mit der geringsten Berechtigung als Zugriffskonto verwenden, stellen Sie sicher, dass dem Konto in Active Directory die Berechtigung „Kennwort zurücksetzen“ zugewiesen wurde, damit das Zurücksetzen des Kennworts in DRA erfolgreich ist.

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-Mandant: Für die Standardauthentifizierung sind Azure Active Directory-Berechtigungen sowohl für das Azure-Mandantenzugriffskonto als auch für die Azure-Anwendung erforderlich. Für die zertifikatbasierte Authentifizierung sind Azure Active Directory-Berechtigungen für die Azure-Anwendung erforderlich. Standardmäßig erstellt DRA automatisch ein eigensigniertes Zertifikat, das für die Authentifizierung erforderlich ist.

Azure-Anwendung: Für die Azure-Anwendung sind die folgenden Rollen und Berechtigungen erforderlich:

Rollen:

- Benutzeradministrator
- Exchange-Administrator

Berechtigungen:

- Lese- und Schreibzugriff auf die vollständigen Profile aller Benutzer
- Lese- und Schreibzugriff auf alle Gruppen
- Lesezugriff auf Verzeichnisdaten
- Verwaltung von Exchange Online als Anwendung für den Zugriff auf Exchange Online-Ressourcen
- Lese- und Schreibzugriff auf alle Anwendungen
- Exchange-Empfängeradministrator

Azure-Mandantenzugriffskonto: Für das Azure-Mandantenzugriffskonto sind die folgenden Berechtigungen erforderlich:

- 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
- Privilegierter Authentifizierungsadministrator

Berechtigungen für NetIQ Administration-Servicekonto:

- Lokale Administratoren
- Erteilen Sie dem Überschreibungskonto mit der geringsten Berechtigung Vollzugriff 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: Sie müssen die folgenden Befehle ausführen, bevor Sie die erforderlichen Domänen verwalten:

- 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 **NetIQ Reporting Center (v3.3)**	**Betriebssystem:** ◆ Microsoft Windows Server 2012 R2, 2016, 2019, 2022 **Datenbank:** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ Der Domänenadministrator, der SQL-Agent-Aufträge verwaltet, benötigt Sicherheitsberechtigungen für Microsoft SQL Server Integration Services. Andernfalls werden bestimmte NRC-Berichte möglicherweise nicht richtig verarbeitet. **Webserver:** ◆ Microsoft Internet Information Server 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. **Kommunikationssicherheitsprotokoll:** ◆ SQL Server muss TLS 1.2 unterstützen. Weitere Informationen finden Sie unter TLS 1.2 support for Microsoft SQL Server (TLS 1.2-Unterstützung für Microsoft SQL Server). ◆ Für SQL Server muss ein aktualisierter Treiber mit TLS-Unterstützung auf dem DRA-Server installiert sein. Der vorgeschlagene Treiber ist der neueste Microsoft® SQL Server® 2012 Native Client – QFE. ◆ Im Betriebssystem von SQL Server und im Betriebssystem des DRA-Verwaltungsservers muss die gleiche TLS-Protokollversion unterstützt werden. Beispielsweise wurde nur TLS 1.2 aktiviert.

Komponente	Voraussetzungen
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 DRA-Lizenzen finden Sie unter Installieren oder Aufrüsten von Lizenzen.

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.
  - **Temporäre Gruppenzuweisungen:** Stellt die Komponenten zur Synchronisierung temporärer Gruppenzuweisungen bereit.
- **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 Install the DRA Clients.

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 (Optional) ◆ DRA-SDK ◆ Temporäre Gruppenzuweisungen **Benutzeroberflächen** ◆ ADSI-Anbieter (Optional) ◆ Befehlszeilenschnittstelle (optional) ◆ Delegierung und Konfiguration ◆ PowerShell-Erweiterungen ◆ Webkonsole
Voraussetzungen überprüfen	Im Dialogfeld **Prerequisites List** (Liste der 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.
Protokollspeicherort festlegen	Geben Sie einen Speicherort an, an dem DRA alle Protokolldateien speichern soll. **HINWEIS:** Die Protokolle der Delegierungs- und Konfigurationskonsole sowie die ADSI-Protokolle werden im Benutzerprofilordner gespeichert.

Schritt	Details
Serverbetriebsmodus auswählen	Wählen Sie **Primärer Verwaltungsserver** aus, um den ersten DRA-Verwaltungsserver in einem Multi-Master-Set zu installieren (eine Bereitstellung enthält jeweils nur einen Primärserver), oder wählen Sie **Sekundärer Verwaltungsserver** aus, um einen DRA-Verwaltungsserver zu einem vorhandenen Multi-Master-Set hinzuzufügen. Informationen zu Multi-Master-Sets finden Sie in „Configuring the Multi-Master Set“ (Konfigurieren des Multi-Master-Sets) im *DRA Administrator Guide* (DRA-Administratorhandbuch).
Installationskonto und Berechtigungsnachweis angeben	◆ DRA-Servicekonto ◆ AD-LDS-Gruppe ◆ DRA-Administrator konto Weitere Informationen hierzu finden Sie unter: Anforderungen an den DRA-Verwaltungsserver und die Webkonsole.
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. **HINWEIS:** Im Feld **SSL-Zertifikat der IIS-Replikationswebsite** werden sowohl die Zertifikate aus dem Webhosting-Speicher als auch die aus dem persönlichen Informationsspeicher aufgelistet.
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 an. **HINWEIS:** Im Feld **SSL-Zertifikat des REST-Diensts** werden sowohl die Zertifikate aus dem Webhosting-Speicher als auch die aus dem persönlichen Informationsspeicher aufgelistet.
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 „Health Check Utility“ (Dienstprogramm „Health Check“ (Systemdiagnose)) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

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*.

Workflow Automation installieren und Einstellungen konfigurieren

Zum Verwalten von Workflow Automation-Anforderungen in DRA ist Folgendes erforderlich:

- Installieren und konfigurieren Sie Workflow Automation und den DRA-Adapter.

  Weitere Informationen finden Sie im *Workflow Automation Administrator Guide* (Workflow Automation-Administratorhandbuch) und in der *Workflow Automation Adapter Reference for DRA* (Workflow Automation-Adapterreferenz für DRA).

- Konfigurieren Sie die Workflow Automation-Integration mit DRA.

  Weitere Informationen finden Sie unter „Configuring the Workflow Automation Server“ (Konfigurieren des Workflow Automation-Servers) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

- Delegieren Sie Workflow Automation-Befugnisse in DRA.

  Weitere Informationen finden Sie unter „Delegating Workflow Automation Server Configuration Powers“ (Delegieren von Befugnissen für die Workflow Automation-Serverkonfiguration) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

Die oben genannten Dokumente sind auf der DRA-Dokumentationswebsite verfügbar.

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-Admin-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.
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 „Configuring the Multi-Master Set“ (Konfigurieren des Multi-Master-Sets) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

Planen einer DRA-Aufrüstung

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.

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 Planen einer DRA-Aufrüstung.
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.
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 41
- „Serversatz mit früherer DRA-Version synchronisieren“, auf Seite 42
- „Registrierung des Verwaltungsservers sichern“, auf Seite 43

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**.

Aufrüsten des DRA-Verwaltungsservers

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: Zur erfolgreichen Reproduktion der temporären Gruppenzuweisungen auf dem Sekundärserver führen Sie den **Multi-Master-Synchronisierungszeitplan** manuell aus oder warten Sie auf die geplante Ausführung.

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.
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 Aufrüsten von Reporting.
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 „Configuring Azure Tenants“ (Azure-Mandanten verwalten) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

Schritt	Details
Webkonsolenkonfiguration aktualisieren *(nach der Aufrüstung)*	*(Bedingt, nach der Aufrüstung)* Wenn Sie vor der Aufrüstung eine der folgenden Webkonsolenkonfigurationen verwenden, müssen diese nach Abschluss der Aufrüstungsinstallation aktualisiert werden: ◆ Standardmäßige Serververbindungen aktiviert ◆ Geänderte Konfigurationsdateien Weitere Informationen finden Sie unter Webkonsolenkonfiguration aktualisieren – nach der Installation.

Themen zur Serveraufrüstung:

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 in 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 in Planen einer DRA-Aufrüstung.

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.

Webkonsolenkonfiguration aktualisieren – nach der Installation

Führen Sie nach der Aufrüstungsinstallation eine oder beide der folgenden Aktionen aus, sofern sie auf Ihre DRA-Umgebung anwendbar sind:

Standardmäßige DRA-Serververbindung

Die DRA-REST-Service-Komponente wird ab DRA 10.1 mit dem DRA-Server konsolidiert. Wenn Sie die standardmäßige DRA-Serververbindung vor der Aufrüstung von einer DRA 10.0.x-Version oder einer früheren Version konfiguriert haben, müssen Sie diese Einstellungen nach der Aufrüstung überprüfen, da es jetzt nur noch eine Verbindungskonfiguration gibt, die DRA-Serververbindung. Sie können auf diese Konfiguration in der Webkonsole unter **Administration** > **Konfiguration** > **DRA-Serververbindung** zugreifen.

Sie können diese Einstellungen auch nach der Aufrüstung in der Datei `web.config` unter `C:\inetpub\wwwroot\DRAClient\rest` auf dem DRA-Webkonsolenserver wie folgt aktualisieren:

```
<restService useDefault="Never">
<serviceLocation address="<REST server name>" port="8755"/>
</restService>
```

Konfiguration der Webkonsolenanmeldung

Wenn bei der Aufrüstung von DRA 10.0.x oder früheren Versionen der DRA-REST-Service ohne den DRA-Server installiert ist, ist die Deinstallation des DRA-REST-Services eine Voraussetzung für die Aufrüstung. Eine Kopie der Dateien, die vor der Aufrüstung geändert wurden, wird auf dem Server in `C:\ProgramData\NetIQ\DRA\Backup\` erstellt. Sie können diese Dateien als Referenz verwenden, um alle relevanten Dateien nach der Aufrüstung zu aktualisieren.

Aufrüsten von Workflow Automation

Um eine Vor-Ort-Aufrüstung einer nicht geclusterten 64-Bit-Umgebung auszuführen, führen Sie einfach das Workflow Automation-Setup-Programm auf Ihren vorhandenen Workflow Automation-Computern aus. Es ist nicht erforderlich, möglicherweise ausgeführte Workflow Automation-Services zu stoppen.

Alle Workflow Automation-Adapter, die nicht im Workflow Automation-Installationsprogramm integriert sind, müssen deinstalliert und nach der Aufrüstung neu installiert werden.

Ausführlichere Informationen zum Aufrüsten von Workflow Automation finden Sie unter „Upgrading from a Previous Version“ (Aufrüsten von einer früheren Version) im *Workflow Automation Administrator Guide* (Workflow Automation-Administratorhandbuch).

Aufrüsten von Reporting

Bevor Sie DRA Reporting aufrüsten, stellen Sie sicher, dass Ihre Umgebung die Mindestanforderungen für NRC 3.3 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.
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 Produktkonfiguration

Dieses Kapitel beschreibt die erforderlichen Konfigurationsschritte und -prozeduren für die Erstinstallation von Directory and Resource Administrator.

6 Konfigurationscheckliste

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

Schritt	Details
DRA-Lizenz anwenden	Wenden Sie mithilfe des Systemdiagnose-Dienstprogramms eine DRA-Lizenz an. Weitere Informationen zu DRA-Lizenzen finden Sie in Lizenzierungsanforderungen.
Delegierung und Konfiguration öffnen	Melden Sie sich mit dem DRA-Servicekonto an einem Computer an, auf dem die Delegierungs- und Konfigurationskonsole installiert ist. Öffnen Sie die Konsole.
Erste verwaltete Domäne zu DRA hinzufügen	Fügen Sie die erste verwaltete Domäne zu DRA hinzu. **HINWEIS:** Nachdem die erste vollständige Kontoaktualisierung abgeschlossen ist, können Sie Befugnisse delegieren.
Verwaltete Domänen und Teilbäume hinzufügen	*Optional:* Fügen Sie zusätzliche verwaltete Domänen und Teilbäume zu DRA hinzu. Weitere Informationen zu verwalteten Domänen finden Sie in Hinzufügen verwalteter Domänen.
DCOM-Einstellungen konfigurieren	*Optional:* Konfigurieren Sie die DCOM-Einstellungen. Weitere Informationen über DCOM-Einstellungen finden Sie unter Konfigurieren der DCOM-Einstellungen.
Domänencontroller und Verwaltungsserver konfigurieren	Konfigurieren Sie den Clientcomputer, auf dem die Delegierungs- und Verwaltungskonsole ausgeführt wird, für jeden Domänencontroller auf jedem Verwaltungsserver. Weitere Informationen finden Sie in Konfigurieren von Domänencontroller und Verwaltungsserver.
DRA-Services für ein gruppenverwaltetes Servicekonto konfigurieren	*Optional:* Konfigurieren Sie DRA-Services für ein gruppenverwaltetes Servicekonto. Weitere Informationen finden Sie in Konfigurieren von DRA-Services für ein gruppenverwaltetes Servicekonto.

7 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, 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.

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.

8 Hinzufügen verwalteter Domänen

Sie können verwaltete Domänen, Server oder Arbeitsstationen hinzufügen, nachdem Sie den Verwaltungsserver installiert haben. Zum Hinzufügen der ersten verwalteten Domäne müssen Sie sich mit dem DRA-Servicekonto an einem Computer anmelden, auf dem die Delegierungs- und Konfigurationskonsole installiert ist. Sie benötigen außerdem Verwaltungsrechte innerhalb der Domäne, beispielsweise die Rechte, die der Domänenadministratorgruppe erteilt sind. Um nach dem Installieren der ersten verwalteten Domäne weitere verwaltete Domänen und Computer hinzuzufügen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der 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 Cache-Aktualisierung der Konten für diese Domänen richtig festgelegt sind. Weitere Informationen zum Ändern des Zeitplans für die Aktualisierung des Konto-Cache finden Sie in „Configuring Caching“ (Konfiguration des Caching) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

---

9 Hinzufügen verwalteter Teilbäume

Sie können verwaltete oder fehlende Teilbäume von spezifischen Microsoft Windows-Domänen hinzufügen, nachdem Sie den Verwaltungsserver installiert haben. Diese Funktionen werden in der Delegierungs- und Konfigurationskonsole über den Knoten **Configuration Management** (Konfigurationsmanagement) > **Managed Domains** (Verwaltete Domänen) ausgeführt. Um nach dem Installieren des Verwaltungsservers verwaltete Teilbäume hinzuzufügen, müssen Sie über die entsprechenden Befugnisse verfügen, beispielsweise über die in der Rolle zum Konfigurieren von Servern und Domänen enthaltenen Befugnisse. Um sicherzustellen, dass das angegebene Zugriffskonto über Berechtigungen zum Verwalten dieses Teilbaums und zum Ausführen inkrementeller Cache-Aktualisierungen für die Konten verfügt, überprüfen und delegieren Sie mit dem Dienstprogramm für gelöschte Objekte die entsprechenden Berechtigungen.

Weitere Informationen zum Verwenden dieses Dienstprogramms finden Sie unter „Deleted Objects Utility“ (Dienstprogramm „Deleted Objects“ (Gelöschte Objekte)) im *DRA Administrator Guide* (DRA-Administrationshandbuch).

Weitere Informationen über das Einrichten des Zugriffskontos finden Sie unter ? „Specifying Domain Access Accounts? “ (Domänenzugriffskonten festlegen) im ? *DRA Administrator Guide?* (DRA-Administrationshandbuch).

HINWEIS: 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. Weitere Informationen zum Ändern des Zeitplans für die Aktualisierung des Konto-Cache finden Sie in „Configuring Caching“ (Konfiguration des Caching) im *DRA Administrator Guide* (DRA-Administratorhandbuch).

---

10 Konfigurieren der DCOM-Einstellungen

Konfigurieren Sie die DCOM-Einstellungen auf dem primären Verwaltungsserver, wenn Sie nicht zugelassen haben, dass das Setup-Programm DCOM für Sie konfiguriert.

Wenn Sie während des DRA-Installationsprozesses ausgewählt haben, dass Distributed COM nicht konfiguriert werden soll, sollten Sie die Mitgliedschaft der Distributed COM-Benutzergruppe so aktualisieren, dass alle Benutzerkonten, die DRA verwenden, enthalten sind. Diese Mitgliedschaft sollte das DRA-Servicekonto, alle Hilfsadministratoren und das Konto enthalten, das zur Verwaltung der DRA-REST-, DRA-Host- und DRA-Verwaltungsservices verwendet wird.

So konfigurieren Sie die Distributed COM-Benutzergruppe:

1. Melden Sie sich als DRA-Administrator an einem DRA-Verwaltungscomputer an.
2. Starten Sie die Delegierungs- und Konfigurationskonsole. Wenn die Konsole nicht automatisch eine Verbindung zum Verwaltungsserver herstellt, stellen Sie die Verbindung manuell her.

   HINWEIS: Sie können unter Umständen keine Verbindung zum Verwaltungsserver herstellen, wenn die Distributed COM-Benutzergruppe keine Hilfsadministratorkonten enthält. Konfigurieren Sie in diesem Fall die Distributed COM-Benutzergruppe mit dem Snapin für Active Directory-Benutzer und -Computer. Weitere Informationen über die Verwendung des Snapins für Active Directory-Benutzer und -Computer finden Sie auf der Microsoft-Website.

   ---
3. Erweitern Sie im linken Bereich **Account and Resource Management** (Konto- und Ressourcenverwaltung).
4. Erweitern Sie **All My Managed Objects** (Alle meine verwalteten Objekte).
5. Erweitern Sie den Domänenknoten für jede Domäne, für die Sie über einen Domänencontroller verfügen.
6. Klicken Sie auf den Container **Vordefiniert**.
7. Suchen Sie die Distributed COM-Benutzergruppe.
8. Klicken Sie in der Suchergebnisliste auf die Gruppe **Distributed COM-Benutzer**.
9. Klicken Sie im unteren Bereich auf **Mitglieder** und dann auf **Mitglieder hinzufügen**.
10. Fügen Sie Benutzer und Gruppen hinzu, die DRA verwenden werden. Stellen Sie sicher, dass Sie das DRA-Servicekonto zu dieser Gruppe hinzufügen.
11. Klicken Sie auf **OK**.

11 Konfigurieren von Domänencontroller und Verwaltungsserver

Nachdem Sie den Clientcomputer konfiguriert haben, auf der die Delegierungs- und Verwaltungskonsole ausgeführt wird, konfigurieren Sie jeden Domänencontroller und jeden Verwaltungsserver.

So konfigurieren Sie den Domänencontroller und den Verwaltungsserver:

1. Wechseln Sie vom Startmenü zu **Systemsteuerung**> **System und Sicherheit**.
2. Öffnen Sie die Verwaltungstools und dann die Komponentendienste.
3. Erweitern Sie **Komponentendienste** > **Computer** > **Arbeitsplatz** > **DCOM-Konfiguration**.
4. Wählen Sie auf dem Verwaltungsserver **MCS OnePoint Administration Service** (MCS OnePoint-Verwaltungsdienst) aus.
5. Klicken Sie im Aktionsmenü auf **Eigenschaften**.
6. Wählen Sie auf der Registerkarte „Allgemein“ im Bereich „Authentifizierungsebene“ **Paket** aus.
7. Wählen Sie auf der Registerkarte „Sicherheit“ im Bereich „Zugriffsberechtigungen“ **Anpassen** aus und klicken Sie dann auf **Bearbeiten**.
8. Stellen Sie sicher, dass die Distributed COM-Benutzergruppe verfügbar ist. Wenn Sie nicht verfügbar ist, fügen Sie die Gruppe hinzu. Wenn die Gruppe „Jeder“ verfügbar ist, entfernen Sie sie.
9. Stellen Sie sicher, dass die Distributed COM-Benutzergruppe Berechtigungen für den lokalen Zugriff und den Fernzugriff hat.
10. Wählen Sie auf der Registerkarte „Sicherheit“ im Bereich „Start- und Aktivierungsberechtigungen“ **Anpassen** aus und klicken Sie dann auf **Bearbeiten**.
11. Stellen Sie sicher, dass die Distributed COM-Benutzergruppe verfügbar ist. Wenn Sie nicht verfügbar ist, fügen Sie die Gruppe hinzu. Wenn die Gruppe „Jeder“ verfügbar ist, entfernen Sie sie.
12. Stellen Sie sicher, dass die Distributed COM-Benutzergruppe über die folgenden Berechtigungen verfügt:
    - Lokaler Start
    - Remotestart
    - Lokale Aktivierung
    - Remoteaktivierung
13. Wenden Sie die Änderungen an.

12 Konfigurieren von 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 gruppenverwalteten Servicekonten). Dieser Abschnitt beschreibt, wie DRA für ein gruppenverwaltetes Servicekonto konfiguriert wird, nachdem das Konto 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 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.
4. Delegieren Sie die Rolle „Audit all objects“ (Alle Objekte überwachen) an das gruppenverwaltete Servicekonto, indem Sie den folgenden Befehl ausführen:

   ```
   Add-DRAAssignments -Identifier "All Objects" -Users
   "CN=<Name_des_gruppenverwalteten_Servicekontos>, CN=Managed Service
   Accounts, DC=MyDomain, DC=corp" -Roles "Audit All Objects"
   ```

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.