Directory and Resource Administrator

Installationsanleitung

Juli 2018

NetIQ

Rechtliche Hinweise

Info zu diesem Handbuch

Die*Installationanleitung* 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. Eine vollständige Liste der Publikationen, die diese Version unterstützen, finden Sie auf der Dokumentations-Website (https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

Anfragen an die Verkaufsunterstützung

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Verkaufsunterstützungsteam.

Weltweit:	www.netiq.com/about_netiq/officelocations.asp
Vereinigte Staaten und Kanada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Kontakt zum technischen Support

Bei spezifischen Produktproblemen, wenden Sie sich an unseren technischen Support.

Weltweit:	www.netiq.com/support/contactinfo.asp
Nord- und Südamerika:	1-713-418-5555
Europa, Naher Osten und Afrika:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Kontakt zum Dokumentationssupport

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Wenn Sie uns einen Verbesserungsvorschlag in Bezug auf die Dokumentation mitteilen möchten, nutzen Sie die Schaltfläche **comment on this topic** (Kommentar zum Thema abgeben), die unten auf jeder Seite der HTML-Version der Dokumentation verfügbar ist. Sie können Verbesserungsvorschläge auch per Email an Documentation-Feedback@netiq.com senden. Wir freuen uns auf Ihre Rückmeldung.

Kontakt zur Online-Benutzer-Community

NetIQ Communities, die NetIQ-Online-Community, ist ein Netzwerk zur Zusammenarbeit mit anderen NetIQ-Benutzern und -Experten. NetIQ Communities bietet Ihnen aktuelle Informationen, nützliche Links zu hilfreichen Ressourcen und Kontakt zu NetIQ-Experten, damit Sie über die Voraussetzungen verfügen, um alles aus den IT-Investitionen herauszuholen, auf die Sie sich verlassen. Weitere Informationen hierzu finden Sie im Internet unter http://community.netiq.com.

1 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.

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.

Exchange Administrator (ExA) erweitert die leistungsfähigen Funktionen von DRA um die nahtlose Verwaltung von Microsoft Exchange. ExA ermöglicht über eine einzige, gemeinsame Benutzeroberfläche Funktionen zur richtlinienbasierten Administration für die Verwaltung von Postfächern, öffentlichen Ordnern und Verteilerlisten in Ihrer Microsoft Exchange-Umgebung.

Kombiniert bieten DRA und ExA die Lösungen, die Sie zum Steuern und Verwalten Ihrer Active Directory-, Microsoft Windows-, Microsoft Exchange- und Microsoft Office 365-Umgebungen benötigen.

- **Unterstützung für Active Directory, Office 365, Exchange und Skype for Business:** Bietet administrative Verwaltungsfunktionen für 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.

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
	DRA Reporting Center Setup (NRC) CLI *(optional)* DRA-ADSI-Anbieter *(optional)*	Sekundärserver
Gelegentlicher Helpdesk-Administrator	Konto- und Ressourcenverwaltungskonsole	Sekundärserver
Gelegentlicher Helpdesk-Administrator	Webkonsole	Jeder DRA-Server, auf dem DRA-REST installiert ist

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:** 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, Office 365 usw.).

Konto- und Ressourcenverwaltungskonsole

Die Konto- und Ressourcenverwaltungskonsole ist eine installierbare Benutzeroberfläche für DRA-Hilfsadministratoren zum Anzeigen und Verwalten delegierter Objekte verbundener Domänen und Services.

Webkonsole

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

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

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

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

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

Berichterstellungskomponenten

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

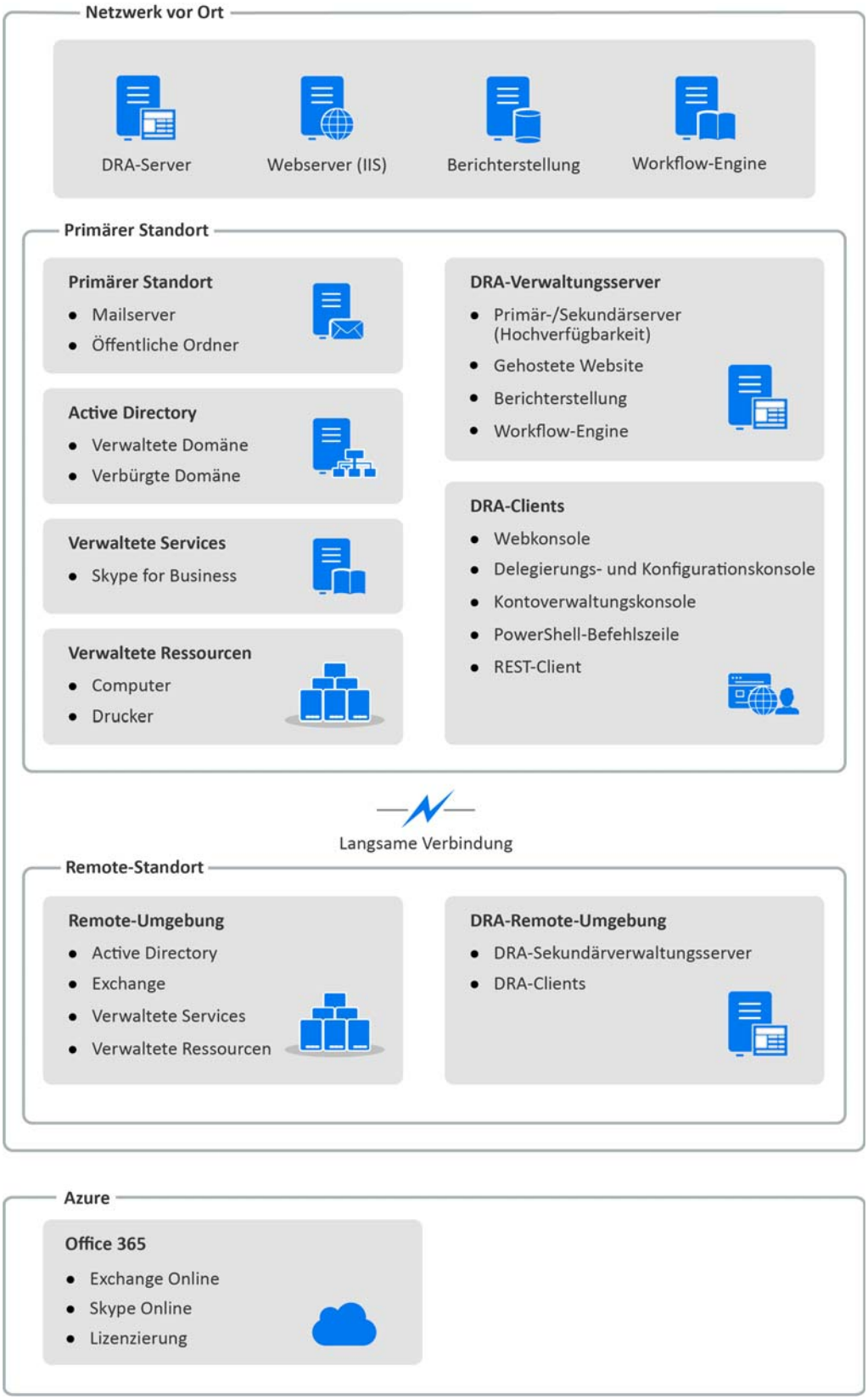
- Ressourcenberichte für AD-Objekte
- AD-Objektdatenberichte
- AD-Zusammenfassungsberichte
- DRA-Konfigurationsberichte
- Exchange-Konfigurationsberichte
- Office 365 Exchange Online-Berichte
- Detaillierte Berichte zu Aktivitätstrends (nach Monat, Domäne und Spitze)
- Zusammenfassende DRA-Aktivitätsberichte

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

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 (https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

Produktarchitektur



2 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.

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	4 Prozessorkerne (x64), 2,0 GHz	16 GB	100 GB
DRA-Webkonsole	2 Prozessorkerne (x64), 2,0 GHz	8 GB	100 GB
DRA-Berichterstellung	4 Prozessorkerne (x64), 2,0 GHz	16 GB	100 GB
DRA-Workflowserver	4 Prozessorkerne (x64), 2,0 GHz	16 GB	100 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.

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, DRA-Clients	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 (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM) (Verwendung von Distributed COM mit Firewalls (DCOM))
TCP 50000 *	Bidirektional	DRA-Verwaltungsserver	Attributreproduktion und Kommunikation zwischen dem DRA-Server und ADAM. (LDAP)
TCP 50001 *	Bidirektional	DRA-Verwaltungsserver	SSL-Attributreproduktion (ADAM)
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 von 2010 bis 2013 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)

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 443, 5986, 5985	Ausgehend	Microsoft PowerShell	Native PowerShell-Commandlets (HTTPS) und PowerShell-Remotebefehle
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

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 (http://go.microsoft.com/fwlink/?LinkID=46088) (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 (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM) (Verwendung von Distributed COM mit Firewalls (DCOM))
TCP 1433	Ausgehend	Microsoft SQL Server	Workflow-Datenspeicher

Protokoll und Port	Richtung	Ziel	Verwendung
TCP 8091	Eingehend	Betriebs- und Konfigurationskonsole	Workflow-BSL-API (TCP)
TCP 8092 **	Eingehend	DRA-Verwaltungsserver	Workflow-BSL-API (HTTP)
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-Seite auf der NetIQ-Website: https://www.netiq.com/support

Verwaltetes System	Voraussetzungen
Active Directory	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	◆ Microsoft Exchange 2010 SP3 (außer für öffentliche Ordner) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ Windows Azure Active Directory-Modul für Windows PowerShell https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell ◆ Skype for Business Online, Windows PowerShell-Modul https://www.microsoft.com/en-us/download/details.aspx?id=39366
Skype for Business	◆ Microsoft Skype for Business 2015
Änderungsverlauf	◆ Change Guardian 5.0, 5.1
Webbrowser	◆ Microsoft Internet Explorer 11, Edge ◆ Google Chrome ◆ Mozilla Firefox

Anforderungen an den DRA-Verwaltungsserver

Für DRA gelten die folgenden Serveranforderungen für Software und Konten:

Softwareanforderungen:

Komponente	Voraussetzungen
Installationsziel	**Betriebssystem des NetIQ-Verwaltungsservers:**
Betriebssystem	◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 2008 R2 wird nur für die Aufrüstung unterstützt. **HINWEIS:** Der Server muss außerdem Mitglied einer unterstützten, nativen Microsoft Windows Server-Domäne sein. **Windows-DRA-Benutzeroberflächen:** ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 8.1 (x86 & x64), 10 (x86 & x64)
Installationsprogramm	◆ Microsoft .Net Framework 4.5.2 oder höher

Verwaltungsserver	**Directory and Resource Administrator:**
	◆ Microsoft .Net Framework 4.5.2 oder höher
	◆ Eine der folgenden Komponenten:
	  ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Packages (x64 und x86)
	  ◆ Microsoft Visual C++ 2017 (Update 3) Redistributable Packages (x64 und x86)
	◆ Microsoft Message Queuing
	◆ Microsoft Active Directory Lightweight Directory Services-Rollen
	◆ Remoteregistrierungsdienst gestartet
	Administration von Microsoft Office 365/Exchange Online:
	◆ Windows Azure Active Directory-Modul für Windows PowerShell
	◆ Microsoft Online Services-Anmeldeassistent für IT-Experten
	◆ Skype for Business Online, Windows PowerShell-Modul
	Weitere Informationen finden Sie unter Unterstützte Plattformen.

Veraltete Webkomponenten	**Webserver:** ◆ Microsoft Internet Information Services (IIS) Version 8.0, 8.5, 10 **Microsoft IIS-Komponenten:** ◆ Microsoft Active Service Pages (ASP) ◆ Microsoft Active Service Pages .NET (ASP .Net) ◆ Microsoft IIS-Sicherheitsrollendienst **Windows-DRA-Benutzeroberflächen:** ◆ Microsoft .Net Framework 4.5.2 ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Package (x86)

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-Verwaltungsservice erforderliche Berechtigungen	◆ Berechtigungen „Distributed COM-Benutzer“ ◆ Mitglied der AD-LDS-Administratorgruppe ◆ Kontenoperatorgruppe ◆ Protokollarchivgruppen (OnePointOp ConfgAdms und OnePointOp) **HINWEIS:** Weitere Informationen zum Einrichten von Domänenzugriffskonten mit den niedrigsten Berechtigungen finden Sie in: DRA-Zugriffskonten mit niedrigsten Berechtigungen.
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.
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. **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: Weisen Sie dem Domänenzugriffskonto die folgenden Active Directory-Berechtigungen zu:

- VOLLSTÄNDIGE KONTROLLE über Benutzerobjekte
- VOLLSTÄNDIGE KONTROLLE über Computerobjekte
- VOLLSTÄNDIGE KONTROLLE über Gruppenobjekte

- VOLLSTÄNDIGE KONTROLLE über Kontaktobjekte
- VOLLSTÄNDIGE KONTROLLE über Objekte vom Typ „organisatorische Einheit“
- VOLLSTÄNDIGE KONTROLLE über Inetorgperson-Objekte
- VOLLSTÄNDIGE KONTROLLE über Druckerobjekte
- VOLLSTÄNDIGE KONTROLLE über Objekte vom Typ „Integrierte Domäne“
- VOLLSTÄNDIGE KONTROLLE über Containerobjekte
- VOLLSTÄNDIGE KONTROLLE über MsExchSystemObjectContainer-Objekte
- VOLLSTÄNDIGE KONTROLLE über dynamische Verteilergruppen
- VOLLSTÄNDIGE KONTROLLE über öffentliche Ordner

Legen Sie für das Domänendienstkonto die folgenden Berechtigungen mit einem Umfang von „Dieses Objekt und alle untergeordneten Objekte“ fest:

- Erstellen von Computerobjekten zulassen
- Löschen von Computerobjekten zulassen
- Erstellen von Kontaktobjekten zulassen
- Löschen von Kontaktobjekten zulassen
- Erstellen von Gruppenobjekten zulassen
- Löschen von Gruppenobjekten zulassen
- Löschen von InetOrgPerson-Objekten zulassen
- Erstellen von Objekten vom Typ „organisatorische Einheit“ zulassen
- Löschen von Objekten vom Typ „organisatorische Einheit“ zulassen
- Erstellen von Benutzerobjekten zulassen
- Löschen von Benutzerobjekten zulassen
- Erstellen von dynamischen Verteilergruppen zulassen
- Löschen von dynamischen Verteilergruppen zulassen
- Erstellen von Dienstverbindungspunkten (SCP) zulassen
- Löschen von Dienstverbindungspunkten (SCP) zulassen
- Erstellen von Containern zulassen
- Löschen von Containern zulassen
- Erstellen von öffentlichen Ordnern zulassen
- Löschen von öffentlichen Ordnern zulassen

Office 365-Mandantenzugriffskonto: Weisen Sie dem Office 365-Mandantenzugriffskonto die folgenden Active Directory-Berechtigungen zu:

- Benutzerverwaltungsadministrator in Office 365
- Empfängerverwaltung in Exchange Online

Exchange-Zugriffskonto: Weisen Sie dem Exchange-Zugriffskonto die Rolle **Organisationsverwaltung** für die Verwaltung von Exchange 2010 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

Nach der DRA-Installation:

- Führen Sie den folgenden Befehl aus, um die Berechtigung auf den Container „Gelöschte Objekte“ vom DRA-Installationsordner zu delegieren (und beachten Sie dabei, dass der Befehl von einem Domänenadministrator ausgeführt werden muss):

  ```
  DraDelObjsUtil.exe /domain:<Netbios-Domänenname> /delegate:<Kontoname>
  ```

- Führen Sie den folgenden Befehl aus, um die Berechtigung auf die OU NetIQRecycleBin vom DRA-Installationsordner zu delegieren; (beachten Sie, dass dies erst nach dem Hinzufügen der entsprechenden Domänen zur Verwaltung durch DRA erledigt werden kann):

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

- Fügen Sie das Überschreibungskonto mit der niedrigsten Berechtigung auf jedem Computer, auf dem DRA zur Verwaltung von Ressourcen wie Druckern, Services, Ereignisprotokoll oder Geräten verwendet wird, zur Gruppe „Lokale Administratoren“ hinzu.
- Erteilen Sie dem Überschreibungskonto mit der geringsten Berechtigung die „uneingeschränkte Berechtigung“ auf Freigabeordner oder DFS-Ordner, wo Basisverzeichnisse bereitgestellt werden.
- Fügen Sie das Überschreibungskonto mit der geringsten Berechtigung zur Rolle „Organisationsverwaltung“ für die Verwaltung von Exchange-Objekten hinzu.

Anforderungen an die DRA-Webkonsole und an Erweiterungen

Die Anforderungen für die Webkonsole und die REST-Erweiterungen sind folgende:

Softwareanforderungen:

Komponente	Voraussetzungen
Installationsziel	**Betriebssystem:** ◆ Microsoft Windows Server 2016, Microsoft Windows 10, mit Microsoft IIS 10 ◆ Microsoft Windows Server 2012, 2012 R2 mit Microsoft IIS 8.0, 8.5
DRA-Hostservice	◆ Microsoft .Net Framework 4.5.2 ◆ DRA-Verwaltungsserver
DRA-REST-Endgerät und -Service	◆ Microsoft .Net Framework 4.5.2
PowerShell-Erweiterungen	◆ Microsoft .Net Framework 4.5.2 ◆ PowerShell 4.0

Komponente	Voraussetzungen
DRA-Webkonsole	**Webserver:** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft Internet Information Services-WCF (Aktivierung) **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

Anforderungen für die Berichterstellung

Die Anforderungen für die DRA-Berichterstellung sind folgende:

Softwareanforderungen:

Komponente	Voraussetzungen
Installationsziel	**Betriebssystem:** ◆ Microsoft Windows Server 2012, 2012 R2, 2016

Komponente	Voraussetzungen
NetIQ Reporting Center (v3.2)	**Datenbank:** ◆ Microsoft SQL Server 2012, 2014, 2016 ◆ 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:** Jeder DRA-Verwaltungsserver, der eine Verbindung zur DRA-Berichterstellung herstellt, benötigt außerdem .NET Framework 3.5. **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.

Nach der Installation des Verwaltungsservers können Sie mit dem Systemdiagnose-Dienstprogramm einen Probelizenzschlüssel (License1.lic) installieren, 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).

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.

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.
NetIQ-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-Installation ausführen	Starten Sie die DRA-Installation. **HINWEIS:** Um die Installation später auszuführen, navigieren Sie zum Speicherort, an dem die Installationsmedien extrahiert wurden, und führen Sie `Setup.exe` aus.
NetIQ-Verwaltungsserverkomponente und das Installationsziel auswählen	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: **NetIQ-Verwaltungsserver** ◆ Protokollarchiv-Ressourcenkit ◆ NetIQ DRA-SDK **Veraltete Webkomponente** **Benutzeroberflächen** ◆ Konto- und Ressourcenverwaltung ◆ DRA-ADSI-Anbieter ◆ Befehlszeilenbenutzeroberfläche ◆ Delegierung und Konfiguration
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 unter „What Is a Multi-Master Set?“ (Was ist ein Multi-Master-Set?) im *Directory and Resource Administrator Administrator Guide* (Directory and Resource Administrator-Administratorhandbuch).

Schritt	Details
Installationskonto und Berechtigungsnachweis angeben	◆ DRA-Servicekonto ◆ AD-LDS-Gruppe ◆ DRA-Administrator Weitere Informationen hierzu finden Sie unter: Anforderungen an den DRA-Verwaltungsserver.
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.
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.

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:

NetIQDRAUserConsole.mst	Installiert die Konto- und Ressourcenverwaltungskonsole
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, wie NetIQDRAUserConsole.mst, 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*.

DRA-REST-Erweiterungen installieren

Das DRA-REST-Erweiterungspaket bietet vier Funktionen:

- **NetIQ DRA-Hostservice:** Gateway zur Kommunikation mit dem DRA-Verwaltungsservice. Dieser Service muss auf einem Computer mit installiertem DRA-Verwaltungsservice ausgeführt werden.
- **DRA-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.
- **PowerShell-Erweiterungen:** Stellt ein PowerShell-Modul bereit, dank dem Nicht-DRA-Clients über PowerShell-Commandlets DRA-Vorgänge anfordern können.
- **DRA-Webkonsole:** Die Webclientoberfläche, die hauptsächlich von Hilfsadministratoren verwendet wird, aber auch Optionen zur benutzerdefinierten Anpassung bietet.

Schritt	Details
Am Zielserver anmelden	Melden Sie sich zur Installation mit einem Konto mit lokalen Administratorrechten am Microsoft Windows-Zielserver an.
SSL-Zertifikat installieren	Sofern nicht bereits auf dem Windows-Server installiert, müssen Sie vor dem Ausführen der Installation ein SSL-Zertifikat installieren.
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 klicken oder das Programm über die Befehlszeile aufrufen. Das Installationskit extrahiert die DRA-Installationsmedien an einen anpassbaren Speicherort im lokalen Dateisystem.
Installationsprogramm für DRA-REST-Erweiterungen ausführen	Nachdem das DRA-Installationskit die Installationsmedien extrahiert hat, fordert es sie zum Starten der DRA-Installation auf. Navigieren Sie zum Speicherort, an dem die Installationsmedien extrahiert wurden, klicken Sie mit der rechten Maustaste auf die Datei `DRARESTExtensionsInstaller.exe` und wählen Sie **Als Administrator ausführen** aus.
EULA-Lizenzvereinbarung akzeptieren	Akzeptieren Sie die Bedingungen der Endbenutzer-Lizenzvereinbarung.
Komponenten auswählen und Zielort für die Installation angeben	Installieren Sie über den Installationsdialog **Komponenten auswählen** alle Optionen: DRA-Hostservice, DRA-REST-Endgeräte und -Service, PowerShell-Erweiterungen und DRA-Webkonsole. Akzeptieren Sie den standardmäßigen Installationsort `C:\Program Files (x86)\NetIQ\DRA Extensions` oder geben Sie für die Installation einen alternativen Speicherort an.
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.

Schritt	Details
Servicekonto für die Ausführung angeben	Standardmäßig wird das vorhandene Servicekonto des DRA-Servers angezeigt. Geben Sie das Passwort für das Servicekonto an. Weitere Informationen zum Einrichten eines Servicekontos für den DRA-Verwaltungsserver finden Sie in Anforderungen an den DRA-Verwaltungsserver.
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.

Workflowserver installieren

Informationen zur Installation des Workflowservers finden Sie im Aegis Administrator Guide (Aegis-Administratorhandbuch).

DRA-Berichterstellung installieren

Für die DRA-Berichterstellung müssen Sie zwei ausführbare Dateien aus dem NetIQ DRA-Installationskit installieren: `NRCSetup.exe` und `DRAReportingSetup.exe`.

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 klicken 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.
NetIQ Reporting Center (NRC)-Installation ausführen	Nachdem das DRA-Installationskit die Installationsmedien extrahiert hat, navigieren Sie zum Speicherort, an dem die Installationsmedien extrahiert wurden, und führen Sie `NRCSetup.exe` aus.
NetIQ Reporting Center-Komponente auswählen	Wählen Sie im Installationsdialog **Komponenten auswählen** die standardmäßige „NetIQ Reporting Center“-Komponente, um die vier NRC-Komponenten zu installieren.
Zielort für Installation angeben	Akzeptieren Sie den standardmäßigen Installationsort `C:\Program Files (x86)\NetIQ\Reporting Center` oder geben Sie für die Installation einen alternativen Speicherort an.

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. **WICHTIG:** Vor der Installation von NRC muss .NET Framework 3.5 manuell auf dem Berichterstellungsserver installiert werden.
EULA-Lizenzvereinbarung akzeptieren	Akzeptieren Sie die Bedingungen der Endbenutzer-Lizenzvereinbarung.
Konfigurationsdatenbank installieren	Verwenden Sie im Dialogfeld **Installation der Konfigurationsdatenbank - SQL Server-Anmeldung** die Standardwerte oder geben Sie eine SQL-Authentifizierung an, um die NRC-Installation abzuschließen. Wenn Sie die Standardinstanz für die SQL Server-Installation verwendet haben, muss das Instanzfeld leer bleiben.
Installation der DRA-Berichterstellung ausführen	Navigieren Sie zum Speicherort, in dem die Installationsmedien extrahiert wurden, und führen Sie `DRAReportingSetup.exe` aus, um die Verwaltungskomponente für die DRA-Berichterstellungsintegration zu installieren.
EULA-Lizenzvereinbarung akzeptieren	Akzeptieren Sie die Bedingungen der Endbenutzer-Lizenzvereinbarung, um die Installation abzuschließen.

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 (MMS) im *Directory and Resource Administrator Administrator Guide* (Directory and Resource Administrator-Administratorhandbuch).

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 einen 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 ActiveViews verknüpft sind.
  - Erstellen Sie mithilfe der Directory and Resource Administrator-Berichterstellung Sicherheitsmodellberichte, wie die ActiveView-Berichte zu Hilfsadministratordetails oder Hilfsadministratorgruppen.

  Informieren Sie diese Hilfsadministratoren über Ihre Aufrüstungspläne für die Benutzeroberflächen.
- Ermitteln Sie, wie viele 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.

Voraufrüstungsaufgaben

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.
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.

HINWEIS: Wenn Sie die Sicherung der 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.

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. Starten Sie die MMC-Benutzeroberfläche.
3. Erweitern Sie im linken Bereich den Eintrag **Configuration Management** (Konfigurationsmanagement).
4. Klicken Sie auf **Administration Servers** (Verwaltungsserver).
5. Wählen Sie im rechten Bereich den entsprechenden primären Verwaltungsserver für diesen Serversatz aus.
6. Klicken Sie auf **Properties** (Eigenschaften).
7. Klicken Sie auf der Registerkarte für den Synchronisierungszeitplan auf **Refresh Now** (Jetzt aktualisieren).
8. 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.

Sie können diesen Aufrüstungsprozess über mehrere Phasen verteilen und jeweils ein MMS auf einmal 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.

In DRA 9.2 und höher wird die Konfiguration des Workflowautomatisierungsservers in AD LDS und nicht in der Registrierung gespeichert. Bei der Aktualisierung von DRA 9.1 oder früher auf DRA 9.2 oder höher wird die Registrierungskonfiguration automatisch zu AD LDS verschoben und auf allen Sekundärservern reproduziert.

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

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 Voraufrüstungsaufgaben.
Primärserver aufrüsten	Rüsten Sie den primären Verwaltungsserver im entsprechenden MMS auf.
Neuen Sekundärserver installieren	*(Optional)* Installieren Sie einen lokalen sekundären Verwaltungsserver, der die neueste DRA-Version ausführt, um Ausfallzeiten an Remotestandorten zu vermeiden.
Benutzeroberflächen bereitstellen	Stellen Sie die Benutzeroberflächen für ihre Hilfsadministratoren bereit.
Sekundärserver aufrüsten	Rüsten Sie die sekundären Verwaltungsserver im MMS auf.
DRA-Berichterstellung aufrüsten	Rüsten Sie die DRA-Berichterstellung auf.
REST-Erweiterungen aufrüsten	Führen Sie das Installationsprogramm für DRA-REST-Erweiterungen aus.
Systemdiagnose-Dienstprogramm ausführen	Führen Sie das Systemdiagnose-Dienstprogramm aus, das im Rahmen der Aufrüstung installiert wurde. Beheben Sie etwaige Probleme.

Primären Verwaltungsserver aufrüsten

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

HINWEIS: Ausführliche 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 weiterarabeiten 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 den CLI- oder ADSI-Anbieter 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 entsprechende Benutzeroberfläche zu installieren, zum Beispiel die Konto- und Ressourcenverwaltungskonsole.
3. Wiederholen Sie die oben genannten Schritte 1 und 2, bis der 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 weiterarabeiten können. Nachdem Sie den Aufrüstungsprozess für diesen MMS fertiggestellt haben und alle Clientcomputer der Hilfsadministratoren aufgerüstete Benutzeroberflächen ausführen, versetzen Sie alle verbleibenden Server mit früheren DRA-Versionen in den Offlinezustand.

DRA-Berichterstellungskomponenten 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 *Reporting Center Guide* (Reporting Center-Handbuch) auf der DRA-Dokumentations-Website.

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 `DRAReportingSetup.exe` aus dem Installationskit aus und befolgen Sie die Anweisungen im Installationsassistenten.
NRC-Setup ausführen	*Bedingt:* Wenn der NRC-Webservice auf einem anderen Computer installiert ist, melden Sie sich am Computer an, auf dem der Webservice installiert ist, und führen Sie `NRCSetup.exe` aus, um den NRC-Webservice aufzurüsten. **HINWEIS:** Wenn die Konfigurationsdatenbank auf einem separaten Server installiert wurde, muss sie zuerst aufgerüstet werden.
NRC-Setup auf Clientcomputern ausführen	Führen Sie `NRCSetup.exe` auf allen NRC-Clientcomputern aus.
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 *NetIQ Reporting Center Reporting Guide* (NetIQ Reporting Center-Berichterstellungshandbuch) auf der DRA-Dokumentations-Website.

DRA-REST-Erweiterungen aufrüsten

Zum Aufrüsten der Webkonsole und REST-Erweiterungen auf Directory and Resource Administator 9.2 müssen Sie Version DRA 9.0.1 oder höher verwenden. Informationen zu den Anforderungen finden Sie unter Anforderungen an die DRA-Webkonsole und an Erweiterungen.

So rüsten Sie die DRA-Webkonsole und die Erweiterungen auf:

1. Nachdem Sie das DRA-Installationskit heruntergeladen haben, navigieren Sie zum Speicherort, an dem die Installationsmedien extrahiert wurden, klicken Sie mit der rechten Maustaste auf die Datei `DRARESTExtensionsInstaller.exe` und wählen Sie **Als Administrator ausführen** aus.
2. Befolgen Sie die Anweisungen des Installationsassistenten bis zum Abschluss der Installation. Klicken Sie dann auf **Finish** (Fertigstellen).

Ausführliche Informationen zu den Schritten des Installationsassistenten finden Sie in der Beschreibung der Schritte für eine neue Installation: DRA-REST-Erweiterungen installieren.

Benutzerdefinierten Inhalt aufrüsten

Wenn Sie auf eine neuere Version von DRA aufrüsten, möchten Sie üblicherweise alle Anpassungen beibehalten, die Sie auf dem Webserver für die Webkonsole vorgenommen haben. Um Ihnen diese Aufgabe zu erleichtern, bietet DRA ein Dienstprogramm zur Aufrüstung von Anpassungen an, das im Installationsprogramm für DRA-REST-Erweiterungen enthalten ist. Das Dienstprogramm wird automatisch ausgeführt, wenn Sie `DRARESTExtensionsInstaller.exe` zum Aufrüsten von REST-Erweiterungen auf dem Webserver ausführen. Sie können das Dienstprogramm auch unabhängig von der Installation manuell aus dem Installationsverzeichnis ausführen.

Als Teil des Prozesses erstellt das Dienstprogramm zur Aufrüstung der Anpassungen eine Sicherung der Anpassungen, bevor die Aufrüstung gestartet wird. Während des Aufrüstungsprozesses erstellt das Dienstprogramm eine Protokolldatei aller Änderungen, die aufgrund der Aufrüstung vorgenommen wurden. Die Protokolldatei enthält außerdem Warnmeldungen zu allen Anpassungsobjekten, die nicht automatisch aktualisiert werden konnten.

Es empfiehlt sich, das Protokoll nach der Aufrüstung zu überprüfen. Bei Bedarf können Sie ein Rollback auf die Anpassungen vor der Aufrüstung ausführen, indem Sie die Anpassungen aus dem Sicherungsordner kopieren. Wenn das Dienstprogramm für die Aufrüstung der Anpassungen gestartet wird, können Sie den Ordnerpfad für die aufgerüsteten Anpassungen definieren oder den automatisch ausgefüllten Standardpfad beibehalten.

Standardmäßig werden die folgenden Pfade für die aufgerüsteten Anpassungen und die Sicherung der Anpassungen verwendet:

- Standardmäßiger Ordnerpfad für Anpassungen:
  `C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom`
- Standardmäßiger Sicherungsordner:
  `$CustomFolderPath\custom_upgrade_$VERSIONFROM_to_$VERSIONTO_backup`

3 Produktkonfiguration

Dieses Kapitel beschreibt die erforderlichen Konfigurationsschritte und -prozeduren 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 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.

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 die Probelizenzschlüsseldatei (`TrialLicense.lic`), die Ihnen von NetIQ Corporation bereitgestellt wird.

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.

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 über das Bearbeiten des Zeitplans für die Cache-Aktualisieren der Konten finden Sie in „Configuring Caching“ (Konfigurieren des Caching) im *Directory and Resource Administrator Administrator Guide* (Directory and Resource Administrator-Administratorhandbuch).

Hinzufügen verwalteter Teilbäume

Sie können verwaltete Teilbäume von spezifischen Microsoft Windows-Domänen hinzufügen, nachdem Sie den Verwaltungsserver installiert haben. Sie können fehlende Teilbäume hinzufügen, die Sie über den Knoten für die erweiterte Konfiguration in der Delegierungs- und Konfigurationskonsole verwalten möchten. 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 „Gelöschte Objekte“) im *Directory and Resource Administrator Adminstrator Guide* (Directory and Resource Administrator-Administrationshandbuch).

Weitere Informationen über das Einrichten des Zugriffskontos finden Sie unter „Specifying Domain Access Accounts“ (Festlegen von Domänenzugriffskonten) im *Directory and Resource Administrator Adminstrator Guide* (Directory and Resource Administrator-Administrationshandbuch).

HINWEIS: Nachdem Sie das Hinzufügen von verwalteten Teilbäumen abgeschlossen haben, stellen Sie sicher, dass die Zeitpläne für die Cache-Aktualisierung der Konten für die entsprechenden Domänen richtig festgelegt sind. Weitere Informationen über das Bearbeiten des Zeitplans für die Cache-Aktualisieren der Konten finden Sie in „Configuring Caching“ (Konfigurieren des Caching) im *Directory and Resource Administrator Administrator Guide* (Directory and Resource Administrator-Administratorhandbuch).

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.

Distributed COM-Benutzergruppe konfigurieren

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 alel Benutzerkonten, die DRA verwenden, enthalten sind. Diese Mitgliedschaft sollte das DRA-Servicekonto und alle Hilfsadministratoren enthalten.

So konfigurieren Sie die Distributed COM-Benutzergruppe:

1. Melden Sie sich als DRA-Administrator an einem DRA-Clientcomputer 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 **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**.

Domänencontroller und Verwaltungsserver konfigurieren

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 **Einstellungen > System und Sicherheit > Systemsteuerung**.
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.