

NetIQ Directory and Resource Administrator 10.2- Versionshinweise

Mai 2022

Diese Verbesserungen sind oft Umsetzungen von Vorschlägen unserer Kunden. Wir möchten uns auf diesem Wege bei Ihnen für Ihr wertvolles Feedback bedanken. Wir hoffen, Sie unterstützen uns weiterhin dabei, unsere Produkte optimal an Ihre Bedürfnisse anzupassen. Senden Sie uns Ihr Feedback als Beitrag im [NetIQ Directory and Resource Administrator-Forum](#) oder im [Aegis-Forum](#) in den Micro Focus-Foren, unserer Online-Community. Hier finden Sie auch Produktinformationen, Blogs und Links zu weiteren nützlichen Ressourcen. Ideen zur Verbesserung des Produkts können Sie auch in unserem [Ideenportal](#) teilen.

- ◆ „Neue Funktionen“, auf Seite 1
- ◆ „Systemanforderungen“, auf Seite 4
- ◆ „Installieren und Aufrüsten dieser Version“, auf Seite 4
- ◆ „Behobene Kundenprobleme“, auf Seite 5
- ◆ „Bekannte Probleme“, auf Seite 6
- ◆ „Kontaktangaben“, auf Seite 7
- ◆ „Rechtliche Hinweise“, auf Seite 8

Neue Funktionen

- ◆ „Verbesserungen in Directory and Resource Administrator“, auf Seite 1
- ◆ „Verbesserungen von Workflow Automation“, auf Seite 4

Verbesserungen in Directory and Resource Administrator

In den folgenden Abschnitten werden die neuen Funktionen und Verbesserungen in DRA 10.2 beschrieben:

- ◆ „Unterstützung für Azure-Gastbenutzer“, auf Seite 2
- ◆ „Unterstützung für die zertifikatbasierte Authentifizierung“, auf Seite 2
- ◆ „PowerShell-Verbesserungen“, auf Seite 2
- ◆ „Virtuelle Attribute von Objekten mithilfe von PowerShell anzeigen“, auf Seite 3

- ♦ „Installation mithilfe von Zertifikaten im alternativen Zertifikatspeicher“, auf Seite 3
- ♦ „Verbesserungen der Webkonsole“, auf Seite 3

Unterstützung für Azure-Gastbenutzer

Sie können externe Benutzer oder Gastbenutzer zur Zusammenarbeit zu einem Azure-Mandanten einladen. Gastbenutzer können die Einladung annehmen, um dem Azure-Mandanten Ihrer Organisation beizutreten und mit ihrem Berechtigungsnachweis auf die konfigurierten Anwendungen zuzugreifen. Sie können diese Benutzer über die DRA-Webkonsole verwalten.

DRA enthält die Rolle `Azure Guest User Administration` (Azure-Gastbenutzerverwaltung) zum Verwalten von Azure-Gastbenutzern. Das PowerShell-Cmdlet `New-AzureDRAMSInvitation` wurde zum Einladen von Gastbenutzern eingeführt.

In den folgenden PowerShell-Cmdlets wurde der Parameter `UserTypes` (Benutzertypen) hinzugefügt, um zwischen Azure-Benutzern vom Typ „Mitglied“ und solchen vom Typ „Gast“ zu unterscheiden:

- ♦ `New-DRAAzureUserRule`
- ♦ `New-DRAAzureGroupRule`
- ♦ `New-DRAAzureTenantRule`

Unterstützung für die zertifikatbasierte Authentifizierung

DRA unterstützt die Multifaktor-Authentifizierung mithilfe von Zertifikaten zur Authentifizierung bei Azure Active Directory. Sie können Azure-Mandanten jetzt entweder mit der zertifikatbasierten Authentifizierung oder mit der Standardauthentifizierung verwalten. Standardmäßig verwendet DRA die zertifikatbasierte Authentifizierung. DRA generiert ein eigensigniertes Zertifikat und weist es der Azure-Anwendung zu. Die Azure-Anwendung wird offline mithilfe des von DRA bereitgestellten PowerShell-Skripts erstellt.

Für die zertifikatbasierte Authentifizierung ist das Exchange Online V2-Modul, Version 2.0.3 oder höher, zur Verwaltung der Exchange Online-Aufgaben erforderlich. Das DRA-Systemdiagnoseprogramm (Dienstprogramm „Health Check“) umfasst die folgenden neuen Überprüfungen zur Azure-Mandantenvvalidierung:

- ♦ Azure-Anwendungsberechtigung
- ♦ Überprüfen des Azure-Mandantenzertifikats

Um die zertifikatbasierte Authentifizierung nach der Aufrüstung von einer früheren Version von DRA auf 10.2 zu verwenden, müssen Sie das Skript `UpdateDraAzureApplicationPermission.ps1` ausführen. Das Skript wendet die zusätzlichen Berechtigungen an, die für die zertifikatbasierte Authentifizierung erforderlich sind. Weitere Informationen finden Sie unter [Configuring Azure Tenants](#) (Konfigurieren von Azure-Mandanten).

PowerShell-Verbesserungen

DRA PowerShell enthält die folgenden Verbesserungen:

Cmdlets für die Delegierungsenumeration

DRA PowerShell enthält jetzt die folgenden neuen Cmdlets für die Delegierungsenumeration:

- ♦ `Get-DRAActiveViewRules`: ruft alle Regeln für eine Aktivansicht ab.

- Get-DRAAssistantAdminGroupMembers: ruft alle Mitglieder aus einer Hilfsadministratorgruppe ab.
- Get-DRAActiveViewAssignments: ruft alle Zuweisungen für eine Aktivansicht ab.

Das Cmdlet Remove-DRAAssignments wurde aktualisiert und akzeptiert nun ein Sternchen (*) als Platzhalterzeichen, um alle Befugnisse und Rollen zu entfernen.

Kontaktobjekte verschieben

Das Cmdlet Move-DRAContact verschiebt ein Kontaktobjekt von einem Speicherort in Active Directory an einen anderen.

Virtuelle Attribute von Objekten mithilfe von PowerShell anzeigen

Der Parameter `IncludeAllVAProperties` wird zu den folgenden Cmdlets hinzugefügt, um alle mit dem Objekt verknüpften virtuellen Attribute zurückzugeben:

- Get-DRAUser
- Get-DRAGroup
- Get-DRAContact
- Get-DRAComputer
- Get-DRAOU
- Get-DRADynamicDistributionGroup
- Get-DRAResourceMailbox
- Get-DRASharedMailbox

Installation mithilfe von Zertifikaten im alternativen Zertifikatspeicher

Sie können jetzt Zertifikate für den REST-Dienst und den DRA-Reproduktionsservice sowohl aus dem persönlichen Informationsspeicher (Personal-Speicher) als auch aus dem Webhosting-Speicher angeben.

Verbesserungen der Webkonsole

Die DRA-Webkonsole enthält mehrere Verbesserungen der Benutzerfreundlichkeit:

- **Ergebnisfilter in den Registerkarten zur Gruppenmitgliedschaft:** Auf den Eigenschaftenseiten „Mitglieder“ und „Mitglied von“ können Sie den Umfang der in der Tabellenansicht angezeigten Daten eingrenzen, indem Sie mithilfe des Objektnamens nach Objekten suchen. In der Tabellenansicht werden die Anzahl der Objekte, die den Suchkriterien entsprechen, sowie die Gesamtzahl der Objekte angezeigt. Sie können Objekte auch aus verschiedenen Seiten der Tabellenansicht entfernen. Die hinzuzufügenden und zu entfernenden Objekte werden in der Liste „Nicht gespeicherte Objekte“ aufgelistet.
- **Anpassen der Spalten in der Objektauswahl:** Sie können jetzt die Spalten anpassen, die in der Suchergebnisansicht der Objektauswahl angezeigt werden sollen.
- **Erweiterung des modalen Fensters:** Die Größe der Fenster wird so angepasst, dass Sie nicht vertikal scrollen müssen, um die Schaltflächen im Fenster anzuzeigen.
- **Anzeigen von Eigenschaften von referenzierten Objekten:** Sie können Eigenschaften von Objekten anzeigen, die als Teil der Eigenschaftenseiten eines anderen Objekts, des Änderungsverlaufsberichts und der temporären Gruppenzuweisungen zurückgegeben werden. Sie können auch die Eigenschaften von Objekten anzeigen, die für Massenvorgänge ausgewählt wurden.

- ♦ **Sonstige Verbesserungen der Benutzeroberfläche:**

- ♦ Die Menüs für **Erstellungsvorgänge** und **Massenvorgänge** werden über den linken Navigationsbereich verschoben.
- ♦ Auf der Seite **Verwaltung > Suche** können Sie das Filtermenü **OBJEKTE** verwenden, um Objekttypen zu filtern. Das Filtermenü **OBJEKTE** ersetzt die Schaltfläche **FILTER**, die in der früheren Version verfügbar war.
- ♦ Die Webkonsole zeigt jetzt Validierungsmeldungen konsistent für jedes Dateneingabeproblem auf einer Seite an.
- ♦ Mit der Webkonsole können Sie Objekte ändern und anzeigen, ohne das Präfix `additionalAttributes` im Attributnamen zu verwenden.
- ♦ Die Webkonsole zeigt in den verschiedenen Objektansichten konsistente Symbole für den Objektstatus an.

Verbesserungen von Workflow Automation

Workflow Automation 10.2 bietet die folgende Verbesserung:

OAuth-Authentifizierung für Exchange-Webdienste

Der Workflow Automation-Email-Adapter unterstützt die OAuth-Authentifizierung für Exchange-Webdienste (EWS). Sie können Azure-Email-Konten mit einem geheimen Azure-Clientschlüssel oder einem Zertifikat überwachen.

Systemanforderungen

Ausführliche Informationen zu den Hardwareanforderungen und den unterstützten Betriebssystemen und Browsern finden Sie im [DRA Installation Guide](#) (DRA-Installationshandbuch) oder in der Referenz [DRA System Requirement](#) (DRA-Systemanforderungen).

Installieren und Aufrüsten dieser Version

Bei der Aufrüstung von 10.0. auf 10.2 erfordern Systeme, auf denen der REST-Service ohne die DRA-Serverkomponente installiert ist, eine modifizierte Installation, um vor der Aufrüstung den REST-Service zu entfernen.

Ausführliche Informationen zum Installieren oder Aufrüstung von Directory and Resource Administrator-Komponenten und -Modulen finden Sie im [DRA Installation Guide](#) (DRA-Installationshandbuch).

Unterstützte Aufrüstungspfade

Die folgende Tabelle zeigt die je nach Version unterstützten Aufrüstungspfade. Beachten Sie, dass Patch-Versionen (x.x.x.x) nicht aufgeführt sind. Alle Patches für die gezeigten Versionen werden jedoch unterstützt. Sie können beispielsweise eine Aufrüstung von DRA 10.1 oder einer beliebigen Patch-Version davon auf DRA 10.2 ausführen, also von 10.1.0.1, 10.1.0.2 usw.

DRA-Server-Basisversion	Aktualisierte DRA-Server-Version
10.0, 10.0.1, 10.0.2, 10.1 oder 10.1.1	10.2
10.0, 10.0.1, 10.0.2 oder 10.1	10.1.1

DRA-Server-Basisversion	Aktualisierte DRA-Server-Version
9.2.1, 10.0, 10.0.1 oder 10.0.2	10.1
9.1, 9.1.1, 9.2, 9.2.1, 10.0 oder 10.0.1	10.0.2
9.1, 9.1.1, 9.2, 9.2.1 oder 10.0	10.0.1
9.1, 9.1.1, 9.2 oder 9.2.1	10.0
9.1, 9.1.1 oder 9.2	9.2.1
9.0, 9.0.1, 9.0.2, 9.0.3, 9.1 oder 9.1.1	9.2
9.0, 9.0.1, 9.0.2, 9.0.3 oder 9.1	9.1.1
9.0, 9.0.1, 9.0.2 oder 9.0.3	9.1
9.0, 9.0.1 oder 9.0.2	9.0.3
9.0 oder 9.0.1	9.0.2
9.0	9.0.1

Behobene Kundenprobleme

Diese Version umfasst die folgenden Korrekturen zur Verbesserung der Stabilität:

- ◆ Es wurde ein Problem behoben, bei dem durch das Beenden eines WFA-Prozesses die PowerShell-Skripts nicht beendet wurden. (321356)
- ◆ Es wurde ein Problem behoben, bei dem das Erstellen eines Workflows mit der Aktivität Active Directory-Objekte suchen zu einem Speicherlust im PG Activity Broker-Prozess führte. (322342).
- ◆ Es wurde ein Problem in der Webkonsole behoben, bei dem die Objektauswahl beim Hinzufügen von Objekten zu einer Gruppe das Feld „Beschreibung“ nicht anzeigen. (329305)
- ◆ Es wurde ein Problem behoben, bei dem das DRA-Installationsprogramm Webfunktionen falsch installiert hat, wenn das IIS-Installationsverzeichnis vom Standardinstallationsverzeichnis abweicht. (376025)
- ◆ Es wurde ein Problem behoben, das dazu führte, dass die Systemdiagnose für die Azure-Mandantenkonten fehlschlug. (377066)
- ◆ Es wurde ein Problem in der Webkonsole behoben, das beim Anzeigen des BitLocker-Passworts zu einem Fehler führte. (401002)
- ◆ Es wurde ein Problem in der Webkonsole behoben, das dazu führte, dass eine LDAP-Abfrage einen Fehler zurückgab, wenn keine Ergebnisse gefunden wurden. (413076)
- ◆ Es wurde ein Problem in der Webkonsole behoben, bei dem das Festlegen statischer Werte für das Feld „Auswählen“ auf der Seite mit den benutzerdefinierten Benutzereigenschaften nicht wie erwartet funktionierte. (413325)
- ◆ Es wurde ein Problem in der Webkonsole behoben, bei dem die benutzerdefinierte Seite die definierten Filter nicht anwendete. (413440)
- ◆ Es wurde ein Problem in der Webkonsole behoben, bei dem der mithilfe eines benutzerdefinierten Behandlungsroutenskripts festgelegte Containerwert nicht angezeigt wird. (414322)
- ◆ Es wurde ein Problem in der Webkonsole behoben, das beim Versuch, ein Benutzerobjekt zu transformieren, einen Fehler verursachte. (434049)

- ♦ Es wurde ein Problem behoben, das die DRA-Installation verhinderte, wenn der Stammordner als Installationsspeicherort und als Speicherort für die Protokolldatei angegeben wurde. (448013)
- ♦ Es wurde ein Problem behoben, das dazu führte, dass die Systemdiagnose für die AD LDS-Konfiguration fehlschlug, wenn das Servicekonto Mitglied einer geschachtelten Gruppe ist. (449015)
- ♦ Ein Problem im Zusammenhang mit dem Speicherort der PostgreSQL-Protokolldatei wurde behoben. (450016)
- ♦ Es wurde ein Problem behoben, bei dem angepasste Seiten die Anzahl der Mitglieder nicht korrekt anzeigen. (476001)
- ♦ Es wurde ein Problem in der Webkonsole behoben, bei dem das Attribut „sAMAccountName“ eine zufällige Zeichenfolge anzeigte, wenn der Wert für das Postfachaliasattribut 20 Zeichen überschreitet. (479073)
- ♦ Es wurde ein Problem in der Webkonsole behoben, das die Anzeige von Erweiterungsattributen für Objekte verhinderte. (483035)
- ♦ Es wurde ein Problem behoben, bei dem der Benutzername in der Mitgliederliste der temporären Gruppenzuweisung falsch angezeigt wurde, wenn der Benutzername einen Schrägstrich (/) enthält. (496065)

Bekannte Probleme

Wir sind bestrebt, Produkte zu bieten, die hochwertige Lösungen für die Softwarebedürfnisse Ihres Unternehmens darstellen. Die nachfolgend genannten Probleme werden derzeit untersucht. Wenden Sie sich an den [Technischen Support](#), wenn Sie weitere Hilfe zu einem Problem benötigen.

Skype-Zugriffskonto wird auf dem Sekundärserver nicht angezeigt

Nach der Aufrüstung von DRA 10.1 auf 10.2 kann DRA das Skype-Zugriffskonto auf dem Sekundärserver nicht anzeigen.

Behelfslösung: Geben Sie das Skype-Zugriffskonto erneut ein oder wählen Sie die Option [Use the primary Administrator server Skype access account](#) (Skype-Zugriffskonto für primären Verwaltungsserver verwenden) aus.

Bei der Datenerfassung mithilfe eines Außerkraftsetzungskontos für die Domäne tritt ein Fehler auf, wenn NTLM verweigert wird

Bei der Datenerfassung tritt ein Fehler auf, wenn NTLM verweigert wird und die Datenkollektoren mit dem Außerkraftsetzungskonto für die Domäne konfiguriert werden.

Behelfslösung: Verwenden Sie beim Konfigurieren des Datenkollektors die Option [Directory Resource Administrator Core service account](#) (Directory Resource Administrator-Kernservicekonto). Stellen Sie sicher, dass es sich bei dem mit dieser Option verwendeten Konto entweder um ein Konto mit den geringsten Rechten oder um ein Konto mit der Domänenadministratorberechtigung handelt.

Die Formularbehandlungsroutine behält den LDAP-Authentifizierungstyp nicht bei

Die Formularbehandlungsroutine aktualisiert den konfigurierten LDAP-Authentifizierungstyp automatisch auf [Anonym](#), nachdem DRA von 10.1 auf 10.1.1 oder höher aufgerüstet wurde.

Behelfslösung: Nach der Aufrüstung müssen Sie den erforderlichen LDAP-Authentifizierungstyp in der Formularbehandlungsroutine manuell konfigurieren.

Die Webkonsole gibt in einer STIG-Umgebung einen 404-Fehler zurück

Ein 404-Fehler wird zurückgegeben, wenn Sie die Webkonsole in einer STIG-kompatiblen Umgebung aktualisieren.

Behelfslösung: Reparieren Sie das Programm **IIS URL Rewrite Module 2** mithilfe der Windows-Funktion **Programme hinzufügen oder entfernen**.

Suche nach Aktivansichten nicht möglich

Wenn Sie nach der Installation von DRA die Delegierungs- und Konfigurationskonsole zum ersten Mal starten, wird die Option zum Suchen nach Aktivansichten für das Feld **Search for** (Suchen nach) im Bereich **Delegation Management > ActiveViews** (Delegierungsverwaltung > Aktivansichten) nicht angezeigt.

Behelfslösung: Um im Bereich **Delegation Management > ActiveViews** (Delegierungsverwaltung > Aktivansichten) nach Aktivansichten zu suchen, klicken Sie auf den Bindestrich, der für das Feld **Search for** (Suchen nach) angezeigt wird, und wählen Sie dann **activeviews** (Aktivansichten) aus der Liste aus.

Die vollständige Aktualisierung des Kontocache für einen Azure-Mandanten schlägt mit dem Fehler AADSTS700027 fehl

Nach dem Konfigurieren eines Azure-Mandanten schlägt die vollständige Aktualisierung des Kontocache für den Azure-Mandanten mit der folgenden Meldung fehl: AADSTS700027: Client assertion contains an invalid signature - Thumbprint of key used by client (Clientassertion enthält eine ungültige Signatur - Fingerabdruck des vom Client verwendeten Schlüssels).

Behelfslösung: Um diesen Fehler zu beheben, können Sie die vollständige Aktualisierung des Kontocache entweder manuell ausführen oder auf die nächste geplante vollständige Aktualisierung des Kontocache warten. Eine vollständige Aktualisierung des Kontocache kann einige Minuten dauern.

NetIQ Administration Service stürzt ab, wenn das Passwort für das manuelle Zertifikat schwach ist

NetIQ Administration Service stürzt ab, wenn das manuelle Zertifikat, das Sie für die zertifikatbasierte Authentifizierung angeben, mit einem schwachen Passwort geschützt ist.

Behelfslösung: Stellen Sie sicher, dass das manuelle Zertifikat, das Sie für die zertifikatbasierte Authentifizierung angeben, mit einem sicheren Passwort geschützt ist.

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/>.

Rechtliche Hinweise

© Copyright 2007–2022 Micro Focus oder eines seiner verbundenen Unternehmen.

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