

Versionshinweise zu NetIQ Identity Manager 4.7

März 2018



NetIQ Identity Manager 4.7 bietet neue Funktionen und Verbesserungen und ist einfacher in der Bedienung. Einige in früheren Versionen auftretende Probleme wurden behoben.

Viele der eingeführten Verbesserungen sind 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. Feedback können Sie in unseren [Identity Manager Community-Foren](#) auf unserer Community-Website posten, auf der Sie auch Produktbenachrichtigungen, Blogs und Produktbenutzergruppen finden.

Informationen über die Neuheiten in früheren Versionen finden Sie im Abschnitt „Frühere Versionen“ auf der [Dokumentations-Website zu Identity Manager](#).

Weitere Informationen zu dieser Version und die aktuellen Versionshinweise finden Sie auf der [Dokumentationsseite](#). Dieses Produkt steht auf der Website der [Identity Manager-Produkte](#) zum Herunterladen bereit.

- ♦ [Abschnitt 1, „Neue und geänderte Funktionen“, auf Seite 1](#)
- ♦ [Abschnitt 2, „Identity Manager-Komponentenversionen“, auf Seite 19](#)
- ♦ [Abschnitt 3, „Systemanforderungen“, auf Seite 19](#)
- ♦ [Abschnitt 4, „Installation von NetIQ Identity Manager 4.7“, auf Seite 19](#)
- ♦ [Abschnitt 5, „Aufrüsten auf NetIQ Identity Manager 4.7“, auf Seite 23](#)
- ♦ [Abschnitt 6, „Bekannte Probleme“, auf Seite 27](#)
- ♦ [Abschnitt 7, „Kontaktangaben“, auf Seite 48](#)
- ♦ [Abschnitt 8, „Rechtliche Hinweise“, auf Seite 48](#)

1 Neue und geänderte Funktionen

In den folgenden Abschnitten werden die wichtigsten Funktionen beschrieben, die in dieser Version enthalten sind. Außerdem wird erläutert, welche Funktionen aus dem Produkt entfernt und welche Probleme in dieser Version behoben wurden:

- ♦ [Abschnitt 1.1, „Neue Funktionen“, auf Seite 2](#)
- ♦ [Abschnitt 1.2, „Unterstützte Betriebssysteme“, auf Seite 6](#)
- ♦ [Abschnitt 1.3, „Versionen der abhängigen Komponenten“, auf Seite 6](#)
- ♦ [Abschnitt 1.4, „Korrekturen“, auf Seite 6](#)
- ♦ [Abschnitt 1.5, „Geht auf eine Softwareschwachstelle ein“, auf Seite 16](#)
- ♦ [Abschnitt 1.6, „Was wurde geändert oder eingestellt und was ist ausgelaufen?“, auf Seite 17](#)
- ♦ [Abschnitt 1.7, „Separate Einrichtungshandbücher für Linux- und Windows-Plattformen“, auf Seite 18](#)

- [Abschnitt 1.8, „Die Endbenutzer-Lizenzvereinbarung ist nicht in allen unterstützten Sprachen verfügbar“, auf Seite 18](#)
- [Abschnitt 1.9, „NetIQ Corporation bietet keine Unterstützung für die Komponenten in der PostgreSQL- und Tomcat-Installation“, auf Seite 18](#)

1.1 Neue Funktionen

Mit dieser Version bietet Identity Manager 4.7 die folgenden wichtigen Funktionen, Verbesserungen und Korrekturen:

- [Abschnitt 1.1.1, „Vereinfachte Installation auf Linux-Plattformen“, auf Seite 2](#)
- [Abschnitt 1.1.2, „Einheitliche Revision“, auf Seite 2](#)
- [Abschnitt 1.1.3, „Erweiterte Unterstützung des Abonnenten-Dienstkanals für neue Treiber“, auf Seite 3](#)
- [Abschnitt 1.1.4, „Vereinfachte Dienste für den Berechtigungsabgleich“, auf Seite 3](#)
- [Abschnitt 1.1.5, „Geänderter Zugriff auf die Datenerfassungsdienste in Identity Manager“, auf Seite 4](#)
- [Abschnitt 1.1.6, „Neue Funktionen und Verbesserungen in den Identitätsanwendungen“, auf Seite 4](#)
- [Abschnitt 1.1.7, „Vereinfachtes Packen der Installationsdateien“, auf Seite 6](#)

Weitere Informationen zu den neuen Funktionen in NetIQ Identity Manager Designer 4.7 finden Sie in den [Versionshinweisen zu NetIQ Identity Manager Designer 4.7 \(vorläufige Fassung\)](#).

Für NetIQ Identity Manager Analyzer 4.7 sind keine neuen Funktionen vorhanden; es wurde nur die Java-Version aktualisiert. Weitere Informationen finden Sie in den [Versionshinweisen zu NetIQ Identity Manager Analyzer 4.7](#).

1.1.1 Vereinfachte Installation auf Linux-Plattformen

Identity Manager umfasst ein neues vereinfachtes, skriptgestütztes Installationsprogramm für Linux-Plattformen. Das neue Installationsprogramm unterstützt die interaktive und die unbeaufsichtigte Installation der Identity Manager-Komponenten. Der Installationsvorgang besteht aus einer Installationsphase und einer Konfigurationsphase. In der Installationsphase werden die erforderlichen Binärdateien abgelegt. In der Konfigurationsphase werden die Identity Manager-Komponenten konfiguriert. Das neue Installationsprogramm bietet typische und erweiterte Konfigurationsmodi.

Bei einer typischen Konfiguration werden gebräuchliche Standardeinstellungen für die meisten Werte herangezogen, sodass das Produkt rasch installiert werden kann. Die Benutzerkonfiguration eignet sich für Produktionsumgebungen. Das neue Installationsprogramm umfasst außerdem ein Dienstprogramm, mit dem die Eigenschaftsdatei für die unbeaufsichtigte Installation im interaktiven Modus erzeugt wird. Das neue Installationsprogramm unterstützt nicht die Installation über die grafische Benutzeroberfläche (GUI).

Weitere Informationen zum Herunterladen der Installationsdateien finden Sie unter [Abschnitt 4.4, „Installation von NetIQ Identity Manager 4.7“, auf Seite 23](#). Installationsanweisungen finden Sie im [Einrichtungshandbuch zu NetIQ Identity Manager für Linux](#).

1.1.2 Einheitliche Revision

Identity Manager bietet nunmehr den offenen Protokollmanagementstandard CEF (Common Event Format) für die Revision von Ereignissen über alle Identity Manager-Komponenten hinweg. Das erweiterbare textgestützte CEF-Format unterstützt mehrere Gerätetypen mit den jeweils relevanten

Informationen. CEF beschränkt die Anzahl der möglichen Nachrichtensyntaxen für die Embedded Syslog Manager-Normalisierung. CEF definiert eine Syntax für Protokolldatensätze, die einen Standard-Header und eine variable Erweiterung in Form von Schlüsselwertpaaren umfasst.

Die CEF-Protokollierung ist standardmäßig deaktiviert. Anweisungen zum Aktivieren finden Sie unter [Configuring Identity Manager Components to Log Audit Events in CEF Format](#) (Konfigurieren von Identity Manager-Komponenten zum Protokollieren von Auditereignissen im CEF-Format) im Handbuch *NetIQ Identity Manager – Configuring Auditing in Identity Manager* (NetIQ Identity Manager – Konfigurieren der Revision in Identity Manager).

HINWEIS: Wenn Sie ein Upgrade auf Identity Manager 4.7 durchführen, ist XDas für Identity Manager-Komponenten, mit Ausnahme von Identitätsanwendungen, immer noch verfügbar. NetIQ empfiehlt die CEF-Revision für alle Komponenten. XDas wird demnächst eingestellt.

1.1.3 Erweiterte Unterstützung des Abonnenten-Dienstkanals für neue Treiber

Die Unterstützung des Abonnenten-Dienstkanals, die für den JDBC-Fan-out-Treiber in Identity Manager 4.6 eingeführt wurde, wurde in dieser Version auf die folgenden Identity Manager-Treiber ausgeweitet: Active Directory, Multi-Domain Active Directory und JDBC.

Mit dem Abonnenten-Dienstkanal können Sie die Außerbandabfragen separat verarbeiten, ohne den normalen Ablauf für Ereignisse im Cache zu unterbrechen, z. B. Aktualisierung der Codezuordnung, Datenerfassung und durch dxcmd ausgelöste Abfragen. Dies trägt zur Verbesserung der Leistung des Treibers bei.

Weitere Informationen finden Sie unter [Improving Driver Performance Using Subscriber Service Channel](#) (Verbessern der Treiberleistung mit dem Abonnenten-Dienstkanal) im *NetIQ Identity Manager Driver Administration Guide* (NetIQ Identity Manager – Handbuch zur Treiberverwaltung).

1.1.4 Vereinfachte Dienste für den Berechtigungsabgleich

PCRS (Permission Collection Reconciliation Services) wurde für Active Directory-, MDAD(Multi-Domain Active Directory)- und LDAP-Treiber vereinfacht. Diese Implementierung wird als CPRS (Controlled Permission Reconciliation Services) bezeichnet.

In der neuen Implementierung ist CPRS in das Identity Manager-Dashboard integriert, was den Abgleich der Berechtigungen des verbundenen Systems mit den Identitätsanwendungen erleichtert. Weitere Informationen finden Sie unter [Verwenden der CPRS](#) im *NetIQ Identity Manager – Administratorhandbuch für die Identitätsanwendungen*.

Identity Manager unterstützt die Migration der Berechtigungen von PCRS zu CPRS für Active Directory-, MDAD- und LDAP-Treiber. Für andere Identity Manager-Treiber können Sie PCRS weiterhin nutzen. Weitere Informationen finden Sie unter [Migration zu CPRS](#) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

1.1.5 Geänderter Zugriff auf die Datenerfassungsdienste in Identity Manager

In Identity Manager wird eine neue Webseite für den Zugriff auf die DCS (Data Collection Services) eingeführt. Sie können die DCS-Seite direkt aus der Benutzeroberfläche der Identitätsanwendungen oder auch über einen Browser öffnen. Damit rückt das Ziel, eine einheitliche Benutzeroberfläche für alle Identity Manager-Komponenten zusammenzustellen, ein Stück näher.

Auf der DCS-Seite können Sie die Einstellungen für die verbundenen Systeme konfigurieren, die in Berichte aufgenommen werden sollen, und Informationen für Identity Reporting angeben. Weitere Informationen finden Sie unter [Exploring Identity Manager Data Collection Services](#) (Erste Schritte mit den Datenerfassungsdiensten in Identity Manager) im [Administrator Guide to NetIQ Identity Reporting](#) (Administratorhandbuch zu NetIQ Identity Reporting).

1.1.6 Neue Funktionen und Verbesserungen in den Identitätsanwendungen

Die Identitätsanwendungen umfassen die folgenden neuen Funktionen und Verbesserungen:

1.1.6.1 Unterstützung für Helpdesk

Identity Manager bietet eine neue Helpdesk-Funktion, die den Benutzern hilft, eventuelle Probleme beim Ausführen ihrer Aufgaben in Identity Manager zu beheben. Beispiele für Aufgaben des Helpdesks:

- ♦ Neuzuweisen einer Genehmigungsanforderung, die längere Zeit nicht beantwortet wurde
- ♦ Durchsuchen aller Aufgaben oder Filtern der Aufgaben für einen ausgewählten Benutzer
- ♦ Anfordern von Berechtigungen im Namen anderer Benutzer

Die Benutzer können sich über die Email-ID oder die Telefonnummer an den Helpdesk wenden oder auch ein Helpdesk-Ticket erstellen. Nach dem Einrichten eines Helpdesks kann der Administrator die Helpdesk-Informationen für die Clients über die Dashboard-Client-Einstellungen anpassen.

Weitere Informationen finden Sie unter folgenden Links:

- ♦ [Grundlagen des Client-Helpdesks](#) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*
- ♦ [Verwenden des Helpdesks](#) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*
- ♦ [Erstellen eines Helpdesk-Tickets](#) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*

1.1.6.2 Unterstützung für das Ablaufen von Ressourcen

In dieser Version können Sie den Ablaufzeitraum für die Ressourcen der Identitätsanwendungen festlegen. Dieser Zeitraum gibt an, wann der Zugriff auf eine bestimmte Ressource nach dem Zuweisungsdatum nicht mehr möglich sein soll. Darüber hinaus können die Benutzer eine Ressource für einen bestimmten Zeitraum anfordern. Weitere Informationen finden Sie in [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen).

1.1.6.3 Unterstützung für das Delegieren

Mit dieser Funktion können Sie Ihre Aufgaben gemäß der Delegierungskonfiguration an andere Benutzer delegieren. Die Delegierung wird über das Dashboard in den Identitätsanwendungen konfiguriert.

Weitere Informationen finden Sie unter [Erstellen und Verwalten von Delegierungen](#) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen* sowie unter [Verwalten von Delegierungen](#) im *NetIQ Identity Manager – Benutzerhandbuch zu den Identitätsanwendungen*.

1.1.6.4 Entziehen in anderem Namen

Diese Version bietet erweiterte Unterstützung für Administratoren und Teammanager, eine Berechtigung im Namen eines Dritten zu entziehen. Es ist außerdem möglich, mehrere Berechtigungen gleichzeitig zu entziehen.

Weitere Informationen finden Sie unter [Entziehen von Berechtigungen](#) im *NetIQ Identity Manager – Benutzerhandbuch zu den Identitätsanwendungen*.

1.1.6.5 Unterstützung für das Anpassen des Dashboards

In dieser Version können Sie die Widgets in Ihrem Dashboard individuell anpassen. Die Administratoren können Einstellungen festlegen, nach denen die Client-Benutzer die gewünschten Widgets im Dashboard einfügen oder wieder entfernen. Weitere Informationen finden Sie unter [Anpassen der Identitätsanwendungen für Ihr Unternehmen](#) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

1.1.6.6 Modernisierte Rollen- und Ressourcenverwaltung

In dieser Version werden Funktionen zur Rollen- und Ressourcenverwaltung in das Dashboard eingebunden. Diese Funktionen wurden bislang vom Katalogadministrator übernommen. Die Rollen- und Ressourcenverwaltung wurde in der neuen Benutzeroberfläche deutlich erweitert. Auch Funktionen zum Zuweisen oder Entziehen von Rollen und Ressourcen stehen bereit. Weitere Informationen finden Sie unter [Erstellen und Verwalten von Rollen](#) und [Erstellen und Verwalten von Ressourcen](#) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

1.1.6.7 Leistungsverbesserungen beim Rollen- und Ressourcendiensttreiber

Der Rollen- und Ressourcendiensttreiber umfasst nunmehr mehrere Threads für verschiedene Aufgaben (z. B. Rollen- und Ressourcenzuweisungen), die die Treiberleistung erheblich verbessern sollen. Weitere Informationen finden Sie unter [Multi-Threaded-Rollen- und Ressourcetreiber](#) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

1.1.6.8 Bereinigen des Ressourcenverlaufs im Rollen- und Ressourcendiensttreiber

Standardmäßig ist der Treiber so konfiguriert, dass der Ressourcenverlauf täglich bereinigt wird. Der Treiber bereinigt lediglich Daten aus dem Ressourcenverlauf, die älter als der Aufbewahrungswert (in Tagen) in der Einstellung „Ressourcenverlauf speichern für x Tage“ sind. Verlaufsdaten, die jünger als der angegebene Aufbewahrungswert sind, werden beibehalten.

1.1.6.9 Unterstützung für Rückgabe- und Neuzuweisungsaufgaben

Verschiedene Benutzer können nunmehr die zugewiesenen Aufgaben über das Identity Manager-Dashboard erneut zuweisen und zurückgeben. Identity Manager-Rollen wie Teammanager, Administratoren, Helpdesk und Endbenutzer besitzen verschiedene Funktionen zum erneuten Zuweisen und zum Zurückgeben von Aufgaben. Weitere Informationen finden Sie unter [Verwalten von Anforderungen zur Genehmigung oder Verweigerung](#) im *NetIQ Identity Manager – Benutzerhandbuch zu den Identitätsanwendungen*.

1.1.6.10 Vertretungsautorisierungssteuerung für Benutzeranwendung

Mit der Vertretungsautorisierungssteuerung für die Benutzeranwendung kann eine vorgangsspezifische Autorisierungsidentität festgelegt werden, sodass die Administratoren die jeweils nötigen Vorgänge im Namen anderer Benutzer effizient ausführen können. Damit sind keine SAML-Zertifikate für die Benutzeranwendung mehr erforderlich, wenn Vorgänge im Identitätsdepot ausgeführt werden sollen.

1.1.7 Vereinfachtes Packen der Installationsdateien

In diese Version sind die Identity Manager-Komponenten jeweils in eine einzige ISO-Datei für Linux- und Windows-Betriebssysteme gepackt. Auch Designer und Analyzer werden in separaten Dateien bereitgestellt. Sentinel für IGA steht in einer separaten Datei bereit und kann somit schnell und einfach für Identity Reporting konfiguriert werden.

1.2 Unterstützte Betriebssysteme

In dieser Version werden erstmals die folgenden Plattformen unterstützt:

- ♦ SUSE Linux Enterprise Server (SLES) 12 SP2, SLES 12 SP3
- ♦ Red Hat Enterprise Linux (RHEL) 7.3, RHEL 7.4
- ♦ Microsoft Windows Server 2016, 2012

WICHTIG: Sentinel Log Management für Identity Governance & Administration (IGA) wird nur auf den Plattformen SLES 12 SP2 und RHEL 7.3 unterstützt.

1.3 Versionen der abhängigen Komponenten

In dieser Version werden erstmals die folgenden abhängigen Komponenten unterstützt:

- ♦ Java 8 Update 162
- ♦ OpenSSL 1.0.2n-fips
- ♦ Apache Tomcat 8.5.27
- ♦ PostgreSQL 9.6.6
- ♦ Apache ActiveMQ 5.15.2
- ♦ MapDB 3.0.5

Wenn Sie die Identity Manager-Engine auf Version 4.7 aufrüsten, bereinigt das Engine-Installationsprogramm teilweise die vorhandenen MapDB-Cache-Dateien. Nach dem Aufrüsten des Treibers müssen Sie die vorhandenen MapDB-Cache-Dateien für den Treiber manuell entfernen. Weitere Informationen finden Sie in der Dokumentation des jeweiligen Treibers auf der [Dokumentations-Website zu den Identity Manager-Treibern](#).

1.4 Korrekturen

Diese Version umfasst die folgenden Software-Korrekturen:

- ♦ [Abschnitt 1.4.1, „SSPR fordert bei der ersten Anmeldung nicht mehr zum Festlegen von Sicherheitsfragen auf“, auf Seite 9](#)
- ♦ [Abschnitt 1.4.2, „Installationsprogramm der Identitätsanwendungen erstellt bei der Installation ordnungsgemäß die Datei „master-key.txt“ im Dateisystem“, auf Seite 9](#)

- ♦ Abschnitt 1.4.3, „Auf der Seite „Anwendungen“ werden externe Anwendungen nunmehr auf einer anderen Registerkarte geöffnet“, auf Seite 9
- ♦ Abschnitt 1.4.4, „Installation der Identity Manager-Engine umfasst Paket „novell-DXMLsch“ unter Linux“, auf Seite 9
- ♦ Abschnitt 1.4.5, „Beim Hinzufügen von Zusatzklassen in einem Treiberfilter wendet die Identity Manager-Engine eine Einschränkung an“, auf Seite 9
- ♦ Abschnitt 1.4.6, „Die Verbindungszeichenkette in der Tomcat-Datei „server.xml“ enthält einen nicht standardmäßigen Port für die Oracle-Datenbank, wenn Identity Reporting unter Linux konfiguriert ist“, auf Seite 10
- ♦ Abschnitt 1.4.7, „„Create_rpt_roles_and_schemas.sql“ vor der Installation von Identity Reporting für eine Oracle-Datenbank unter Linux erforderlich“, auf Seite 10
- ♦ Abschnitt 1.4.8, „Möglichkeit zum Steuern der Dateirechte mit Writelog in AJC-JavaScript“, auf Seite 10
- ♦ Abschnitt 1.4.9, „Klammern im Remote Loader-Passwort werden ignoriert“, auf Seite 10
- ♦ Abschnitt 1.4.10, „Token-Zuordnung gibt bei fehlender Übereinstimmung ein leeres Ergebnis zurück“, auf Seite 10
- ♦ Abschnitt 1.4.11, „Doppelte Ansicht „idmrpt_identity_v1“ wurde entfernt“, auf Seite 10
- ♦ Abschnitt 1.4.12, „Token „do-remove-role“ unterstützt Korrelations-ID“, auf Seite 10
- ♦ Abschnitt 1.4.13, „Identity Reporting legt ordnungsgemäße Platzhaltereinträge in der Oracle-Datenbank an“, auf Seite 10
- ♦ Abschnitt 1.4.14, „Die Ausgabetransformations-Richtlinie gibt ordnungsgemäß eine Statusmeldung über einen schwerwiegenden Fehler aus, die darauf hinweist, dass der Treiber angehalten werden muss“, auf Seite 11
- ♦ Abschnitt 1.4.15, „Identity Manager-Engine erkennt die Filtereinstellung „optimize-modify=false“ beim Zusammenführen von Herausgebern an“, auf Seite 11
- ♦ Abschnitt 1.4.16, „Passwortrichtlinien-Plugin zeigt richtige Informationen zur zulässigen Passwortlänge“, auf Seite 11
- ♦ Abschnitt 1.4.17, „Im Feld für die private Email-Adresse auf den Benutzerprofil-Eigenschaftsseiten kann ein Wert mit mehr als 32 Zeichen eingegeben werden“, auf Seite 11
- ♦ Abschnitt 1.4.18, „dxcmd-Massenmodus enthält Cache-Statistiken zur Prioritätssynchronisierung“, auf Seite 11
- ♦ Abschnitt 1.4.19, „Office365-Abgleichrichtlinie für Treiber/Abonnenten enthält „token-src-name“ statt „token-src-attr“, auf Seite 11
- ♦ Abschnitt 1.4.20, „Berichterstellungsdatenbank wird nach dem Entfernen von Ressourcen, bei dem eine Genehmigung erforderlich ist, ordnungsgemäß aktualisiert“, auf Seite 11
- ♦ Abschnitt 1.4.21, „Installationsprogramm für Identity Manager unter Linux gibt eine Fehlermeldung aus, wenn der Name des eingehängten Verzeichnisses ein Leerzeichen enthält“, auf Seite 12
- ♦ Abschnitt 1.4.22, „Aufruf einer Java-Funktion mit 36 Parametern aus einer Treiberrichtlinie schlägt nach dem Aufrüsten von Identity Manager 4.0.2 fehl“, auf Seite 12
- ♦ Abschnitt 1.4.23, „Löschen des Cache-Inhalts mit dxcmd im nicht interaktiven Modus“, auf Seite 12
- ♦ Abschnitt 1.4.24, „Treibersatz-Dashboard-Plugin löscht das temporäre Bildverzeichnis“, auf Seite 12
- ♦ Abschnitt 1.4.25, „Mitglieder in der Gruppendistribution oder der mailfähigen Sicherheit werden in Azure-Active Directory nicht synchronisiert“, auf Seite 12

- ♦ Abschnitt 1.4.26, „OSP führt die Prüfung nach der Authentifizierung durch, wenn OSP mit Kerberos konfiguriert ist“, auf Seite 12
- ♦ Abschnitt 1.4.27, „Identity Manager-Engine lässt zusätzliche Treiberzustandsaufträge zu“, auf Seite 12
- ♦ Abschnitt 1.4.28, „Identity Manager-Installationsprogramm mit Standort „Niederlande“ wird unter Windows standardmäßig auf Deutsch eingestellt“, auf Seite 12
- ♦ Abschnitt 1.4.29, „Beim Importieren der SQL-Datei für die Oracle-Datenbank werden keine Fehler zurückgegeben“, auf Seite 13
- ♦ Abschnitt 1.4.30, „Aufrüstungsprogramm der Identitätsanwendungen stellt Informationen zu den Versionen der aufzurüstenden Komponenten unter Windows bereit“, auf Seite 13
- ♦ Abschnitt 1.4.31, „Aufrüstungsprogramm der Identitätsanwendungen verarbeitet den benutzerdefinierten Kontext“, auf Seite 13
- ♦ Abschnitt 1.4.32, „Möglichkeit zum Verwenden eines nicht standardmäßigen Email-Ports in der Identity Manager-Konfiguration“, auf Seite 13
- ♦ Abschnitt 1.4.33, „Remote Loader-Trace-Bildschirm wird nach dem Neustart des Systems unter Windows 2012 geschlossen“, auf Seite 13
- ♦ Abschnitt 1.4.34, „Möglichkeit zum Suchen eines Benutzers nach dem vollständigen Namen im Dashboard“, auf Seite 13
- ♦ Abschnitt 1.4.35, „Anforderungsverlauf für einen bestimmten Zeitraum wird angezeigt“, auf Seite 13
- ♦ Abschnitt 1.4.36, „Verbesserte Darstellung der Berechtigungsliste“, auf Seite 13
- ♦ Abschnitt 1.4.37, „Popup-Fenster für Ressourcenbenachrichtigung zeigt CN statt FQDN im Dashboard an“, auf Seite 13
- ♦ Abschnitt 1.4.38, „Hinzufügen von Workflows, Ressourcen oder PRD auf der Seite „Anwendungen“, auf Seite 14
- ♦ Abschnitt 1.4.39, „Funktion für Anforderungen zum Entziehen der Rollen- und Ressourcenzuweisungen über einen SOAP-/REST-Endpunkt“, auf Seite 14
- ♦ Abschnitt 1.4.40, „Dynamische Ressourcenzuweisungssuche gibt die gewünschten Berechtigungen ordnungsgemäß zurück“, auf Seite 14
- ♦ Abschnitt 1.4.41, „Gelöschte Genehmiger werden nicht in der Genehmigerliste aufgeführt“, auf Seite 14
- ♦ Abschnitt 1.4.42, „Zeichenkette für Rollenaktualisierung und Rollenbeziehung wird fehlerfrei ins Spanische übersetzt“, auf Seite 14
- ♦ Abschnitt 1.4.43, „Öffnen von PRDs über die Seite „Anwendungen“ im Dashboard“, auf Seite 14
- ♦ Abschnitt 1.4.44, „Integrationsaktivität unterstützt die Kommunikation mit Servern, für die die beiderseitige Authentifizierung aktiviert ist“, auf Seite 14
- ♦ Abschnitt 1.4.45, „Organigramm im Dashboard zeigt die zugelassenen Objekte und Attribute für einen Benutzer“, auf Seite 14
- ♦ Abschnitt 1.4.46, „Im Skript „idmapps_tomcat_init“ sind keine Ausführungsberechtigungen mehr für „etc/rc.d/init.d/functions“ erforderlich, damit der Dienst als Daemon unter Linux ausgeführt wird“, auf Seite 15
- ♦ Abschnitt 1.4.47, „Standardmäßige Benachrichtigungserfassungsschablonen zeigen die richtigen Sprachen“, auf Seite 15
- ♦ Abschnitt 1.4.48, „Dashboard zeigt Aufgaben ordnungsgemäß an, wenn die Spalte „METAXML“ den Datentyp „ntext“ besitzt“, auf Seite 15

- Abschnitt 1.4.49, „In den Anmerkungen im Anforderungsverlauf wird der vollständige Name eines Benutzers statt des CN angezeigt“, auf Seite 15
- Abschnitt 1.4.50, „Breite des Listenfilds bleibt bei einer Datumsänderung unverändert“, auf Seite 15
- Abschnitt 1.4.51, „PRD wird ordnungsgemäß in einer neuen Registerkarte geöffnet“, auf Seite 15
- Abschnitt 1.4.52, „Anforderer-„fdn <req>“ in einem Benutzerobjekt für Rollen und Ressourcen wird beim Umbenennen des Benutzers geändert“, auf Seite 15
- Abschnitt 1.4.53, „„getRoleLevels“ gibt richtige Informationen zurück“, auf Seite 15
- Abschnitt 1.4.54, „Variable NETIQ_TOMCAT_USER wurde aus dem Tomcat-PostgreSQL-Installationsprogramm für Windows entfernt“, auf Seite 16
- Abschnitt 1.4.55, „Möglichkeit zum Sortieren des Anforderungsverlaufs im Dashboard“, auf Seite 16
- Abschnitt 1.4.56, „Rollen- und Ressourcenservice-Treiber“, auf Seite 16

1.4.1 SSPR fordert bei der ersten Anmeldung nicht mehr zum Festlegen von Sicherheitsfragen auf

Wenn Sie sich mit einem Benutzernamen, der ein Leerzeichen enthält, bei den Identitätsanwendungen anmelden, fordert SSPR Sie bei der ersten Anmeldung nicht mehr auf, Sicherheitsfragen festzulegen. (Bug 1025713)

1.4.2 Installationsprogramm der Identitätsanwendungen erstellt bei der Installation ordnungsgemäß die Datei „master-key.txt“ im Dateisystem

Das Installationsprogramm der Identitätsanwendungen erstellt nunmehr die Datei `master-key.txt` ordnungsgemäß im Verzeichnis `<UserApp-install>` unter Tomcat. Wenn Sie die Komponenten der Identitätsanwendungen auf einem Tomcat-Cluster einrichten, müssen Sie den Master-Schlüsselwert aus dieser Datei lesen, also nicht aus der Datei `ism-configuration.properties`. (Bug 900240)

1.4.3 Auf der Seite „Anwendungen“ werden externe Anwendungen nunmehr auf einer anderen Registerkarte geöffnet

Wenn Sie im Identity Manager-Dashboard auf der Seite **Anwendungen** auf eine externe Anwendung klicken, wird die Anwendung nicht mehr auf derselben Registerkarte geöffnet, sondern auf einer anderen. (Bug 1079325)

1.4.4 Installation der Identity Manger-Engine umfasst Paket „novell-DXMLsch“ unter Linux

In dieser Version wird ein benutzerdefinierter Installations- und Konfigurationsvorgang für Linux-Plattformen eingeführt. Mit dem Installationsvorgang für die Identity Manager-Engine wird das Paket „novell-DXMLsch“ für alle Installationsszenarien installiert. (Bug 1054169)

1.4.5 Beim Hinzufügen von Zusatzklassen in einem Treiberfilter wendet die Identity Manager-Engine eine Einschränkung an

Die Zusatzklassen werden nicht durch die Identity Manager-Engine verarbeitet. Dieser Vorgang wird ignoriert und in der Treiber-Trace-Datei wird eine Warnmeldung eingetragen. (Bug 1041056)

1.4.6 Die Verbindungszeichenkette in der Tomcat-Datei „server.xml“ enthält einen nicht standardmäßigen Port für die Oracle-Datenbank, wenn Identity Reporting unter Linux konfiguriert ist

Das neue Identity Manager-Installationsprogramm für Linux aktualisiert die Verbindungs-URL in der Tomcat-Datei „server.xml“ mit dem Wert, der in der Konfigurationsphase für einen nicht standardmäßigen Datenbank-Port angegeben wurde. (Bug 1063010)

1.4.7 „Create_rpt_roles_and_schemas.sql“ vor der Installation von Identity Reporting für eine Oracle-Datenbank unter Linux erforderlich

Wenn Sie das Installationsprogramm für Identity Reporting unter Linux ausführen, werden die erforderlichen .sql-Dateien für die Konfiguration des Datenbankschemas abgelegt. (Bug 1063009)

1.4.8 Möglichkeit zum Steuern der Dateirechte mit Writelog in AJC-JavaScript

ECMAScript wurde mit der neuen Funktion „setFilePermissions“ ergänzt, mit der Sie die POSIX-Dateirechte unter Linux ändern können. (Bug 1023201)

1.4.9 Klammern im Remote Loader-Passwort werden ignoriert

Identity Manager kann ein Remote Loader-Passwort mit oder ohne schließende Klammer verarbeiten, mit dem eine Verbindung zur Identity Manager-Engine hergestellt werden soll. (Bug 919823)

1.4.10 Token-Zuordnung gibt bei fehlender Übereinstimmung ein leeres Ergebnis zurück

Die Token-Zuordnungsrichtlinie wird nicht ausgeführt, wenn kein übereinstimmendes Token gefunden wird. (Bug 1063065)

1.4.11 Doppelte Ansicht „idmrpt_identity_v1“ wurde entfernt

Die Ansicht „idmrpt_identity_v1“ war ähnlich aufgebaut wie die Ansicht „idmrpt_identity_cs_v“. „idmrpt_identity_v1“ wurde aus dem Datenbankschema entfernt. (Bug 824615)

1.4.12 Token „do-remove-role“ unterstützt Korrelations-ID

Das Token „do-remove-role“ nimmt nunmehr einen Korrelations-ID-Wert an. Standardmäßig wird der Korrelations-ID-Wert aus der Vorgangsereignis-ID herangezogen, sofern der Korrelations-ID-Wert nicht explizit angegeben wurde. (Bug 933953)

1.4.13 Identity Reporting legt ordnungsgemäße Platzhaltereinträge in der Oracle-Datenbank an

Identity Reporting verarbeitet nunmehr keine Benutzer mehr, die zu einer Gruppe gehören, die nicht in der Oracle-Datenbank vorliegt. (Bug 1075816)

- 1.4.14 Die Ausgabetransformations-Richtlinie gibt ordnungsgemäß eine Statusmeldung über einen schwerwiegenden Fehler aus, die darauf hinweist, dass der Treiber angehalten werden muss**
- Die Ausgabetransformations-Richtlinie wurde überarbeitet und gibt nunmehr eine Statusmeldung über einen schwerwiegenden Fehler im Herausgeber-Trace aus, die darauf hinweist, dass der Treiber heruntergefahren werden sollte. (Bug 1050608)
- 1.4.15 Identity Manager-Engine erkennt die Filtereinstellung „optimize-modify=false“ beim Zusammenführen von Herausgebern an**
- Wenn nach einer erfolgreichen Übereinstimmung im Herausgeberkanal alle Attributwerte im Identitätsdepot fehlerfrei festgelegt sind, verarbeitet die Engine ordnungsgemäß einen Vorgang, der alle Attribute mit den Einstellungen „publisher=“sync“ und „optimize-modify=false“ enthält. (Bug 794273)
- 1.4.16 Passwortrichtlinien-Plugin zeigt richtige Informationen zur zulässigen Passwortlänge**
- Die Benutzeroberfläche des Passwortrichtlinien-Plugins weist nunmehr darauf hin, dass die Passwortrichtlinie keine Passwörter mit weniger als drei Zeichen mehr anerkennt. (Bug 936162)
- 1.4.17 Im Feld für die private Email-Adresse auf den Benutzerprofil-Eigenschaftsseiten kann ein Wert mit mehr als 32 Zeichen eingegeben werden**
- Im Feld für die private Email-Adresse auf den Benutzerprofil-Eigenschaftsseiten können Sie nunmehr einen Wert mit mehr als 32 Zeichen eingeben. (Bug 997453)
- 1.4.18 dxcmd-Massenmodus enthält Cache-Statistiken zur Prioritätssynchronisierung**
- dxcmd bietet nunmehr sowohl im Massenmodus als auch im interaktiven Modus die Cache-Statistiken zur Prioritätssynchronisierung. (Bug 1014476)
- 1.4.19 Office365-Abgleichrichtlinie für Treiber/Abonnenten enthält „token-src-name“ statt „token-src-attr“**
- Mit „token-src-name“ wird verhindert, dass der Treiber vor jedem einzelnen Abgleich eine unnötige Abfrage an das Identitätsdepot sendet. Damit wird die Leistung des Treibers bei starker Auslastung gesteigert, beispielsweise bei der ersten Migration der Benutzer. (Bug 881132)
- 1.4.20 Berichterstellungsdatenbank wird nach dem Entfernen von Ressourcen, bei dem eine Genehmigung erforderlich ist, ordnungsgemäß aktualisiert**
- Sobald der Genehmiger die Ressourcenzurücknahme genehmigt, wird die Tabelle „identity_trust“ ordnungsgemäß aktualisiert und der Verbürgungsstatus wechselt von 1 zu 0. (Bug 1067991)

1.4.21 Installationsprogramm für Identity Manager unter Linux gibt eine Fehlermeldung aus, wenn der Name des eingehängten Verzeichnisses ein Leerzeichen enthält

Das Installationsprogramm für Identity Manager unter Linux meldet nunmehr einen Fehler, wenn ein Leerzeichen im Namen des Verzeichnisses, in das die ISO-Datei eingehängt werden soll, aufgefunden wird. (Bug 910386)

1.4.22 Aufruf einer Java-Funktion mit 36 Parametern aus einer Treiberrichtlinie schlägt nach dem Aufrüsten von Identity Manager 4.0.2 fehl

Die Identity Manager-Engine kann nunmehr 36 Argumente verarbeiten. (Bug 1055873)

1.4.23 Löschen des Cache-Inhalts mit dxcmd im nicht interaktiven Modus

Sie können nunmehr den Cache eines Treibers jederzeit und im nicht interaktiven Modus mit dxcmd löschen. (Bug 1006754)

1.4.24 Treibersatz-Dashboard-Plugin löscht das temporäre Bildverzeichnis

Identity Manager erstellt die Grafikdateien für das Identity Manager-Überblick-Plugin und das Treibersatz-Dashboard-Plugin temporär im Verzeichnis <iManager-Installationsverzeichnis>/nps/images/temp. Das temporäre Verzeichnis wird nunmehr gelöscht, sobald der Tomcat-Server neu gestartet wird, auf dem iManager gehostet wird. (Bug 1001237)

1.4.25 Mitglieder in der Gruppendistribution oder der mailfähigen Sicherheit werden in Azure-Active Directory nicht synchronisiert

Ein Gruppenmitglied im Identitätsdepot wird ordnungsgemäß mit den Azure-Active Directory-Gruppen synchronisiert. (Bug 1077198)

1.4.26 OSP führt die Prüfung nach der Authentifizierung durch, wenn OSP mit Kerberos konfiguriert ist

Wenn Sie OSP mit Kerberos konfiguriert haben, stellt OSP nunmehr mit der Prüfung nach der Authentifizierung fest, ob der Benutzer ein abgelaufenes Passwort besitzt oder Fragen im Challenge-Response-Verfahren beantworten muss. (Bug 924221)

1.4.27 Identity Manager-Engine lässt zusätzliche Treiberzustandsaufträge zu

Die Identity Manager-Engine kann nunmehr mehrere Zustandsauftragskonfigurationen in einem Treiberattribut speichern und verarbeiten. (Bug 870219)

1.4.28 Identity Manager-Installationsprogramm mit Standort „Niederlande“ wird unter Windows standardmäßig auf Deutsch eingestellt

Dieser Fehler wurde behoben. Das Installationsprogramm wird nunmehr standardmäßig in englischer Sprache ausgeführt. (Bug 768958)

- 1.4.29 Beim Importieren der SQL-Datei für die Oracle-Datenbank werden keine Fehler zurückgegeben**
- Die SQL-Datei wird erzeugt, wenn Sie bei der Installation der Identitätsanwendung die Option **SQL schreiben** wählen. Die Identitätsanwendungen importieren die SQL-Datei nunmehr ordnungsgemäß in die Oracle-Datenbank. (Bug 1057368)
- 1.4.30 Aufrüstungsprogramm der Identitätsanwendungen stellt Informationen zu den Versionen der aufzurüstenden Komponenten unter Windows bereit**
- Das Aufrüstungsprogramm zeigt nunmehr die neuen Versionen der Komponenten an, auf die die derzeit installierten Komponenten aufgerüstet werden. (Bug 1031435)
- 1.4.31 Aufrüstungsprogramm der Identitätsanwendungen verarbeitet den benutzerdefinierten Kontext**
- Sie können nunmehr beim Aufrüsten einen anderen Kontext statt des standardmäßigen Kontexts (IDMProv) heranziehen. (Bug 1028475)
- 1.4.32 Möglichkeit zum Verwenden eines nicht standardmäßigen Email-Ports in der Identity Manager-Konfiguration**
- Der Email-Server kann nunmehr einen nicht standardmäßigen SMTP-Port überwachen. (Bug 1041493)
- 1.4.33 Remote Loader-Trace-Bildschirm wird nach dem Neustart des Systems unter Windows 2012 geschlossen**
- Dieser Fehler wurde behoben. Der Remote Loader-Trace-Bildschirm wird ordnungsgemäß geschlossen. (Bug 892034)
- 1.4.34 Möglichkeit zum Suchen eines Benutzers nach dem vollständigen Namen im Dashboard**
- Alle Benutzerattribute, die in DAL für die Suche markiert sind, können nunmehr über die Dashboard-Seite „Einstellungen“ als Suchattribut im Benutzerkatalog markiert werden. (Bug 1073463)
- 1.4.35 Anforderungsverlauf für einen bestimmten Zeitraum wird angezeigt**
- Im Dashboard werden nunmehr Ihre Anforderungen für den Zeitraum angezeigt, der vom Administrator festgelegt wurde. (Bug 1061696)
- 1.4.36 Verbesserte Darstellung der Berechtigungsliste**
- Im Dashboard werden nur direkte Zuweisungen angezeigt. Hier finden Sie außerdem ein Symbol, mit dem Sie die Liste aller Berechtigungen abrufen. (Bug 1061516)
- 1.4.37 Popup-Fenster für Ressourcenbenachrichtigung zeigt CN statt FQDN im Dashboard an**
- Das Dashboard zeigt nunmehr nur die Ressource „cn“ in der Benachrichtigungskontrolleiste an. (Bug 1055622)

1.4.38 Hinzufügen von Workflows, Ressourcen oder PRD auf der Seite „Anwendungen“

In der neuen Benutzeroberfläche können Sie Deep-Links auf der Seite „Anwendungen“ für Workflows, Ressourcen und PRDs erstellen. Wenn Sie auf dieser Seite auf eine Kachel klicken, wird das Formular in einer neuen Registerkarte geöffnet. Sobald die Anforderung gesendet wurde, gelangen Sie wieder zur Seite „Anwendungen“ zurück. (Bug 988818)

1.4.39 Funktion für Anforderungen zum Entziehen der Rollen- und Ressourcenzuweisungen über einen SOAP-/REST-Endpunkt

Sie können nunmehr eine Anforderung zum Erteilen oder Entziehen einer Rolle nicht mehr nur über die Benutzeroberfläche abgeben, sondern auch über einen Rollen-SOAP- oder REST-Endpunkt. (Bug 846736)

1.4.40 Dynamische Ressourcenzuweisungssuche gibt die gewünschten Berechtigungen ordnungsgemäß zurück

Wenn Sie eine Ressource, die einer Berechtigung mit einem Wert zugewiesen ist, über das Dashboard anfordern, filtert das Dashboard die Berechtigungen ordnungsgemäß gemäß Ihren Suchkriterien. (Bug 995889)

1.4.41 Gelöschte Genehmiger werden nicht in der Genehmigerliste aufgeführt

Die gelöschten Genehmiger werden im Rollenkatalog auf der neuen Seite „Administration“ nicht mehr angezeigt. (Bug 632362)

1.4.42 Zeichenkette für Rollenaktualisierung und Rollenbeziehung wird fehlerfrei ins Spanische übersetzt

Dieses Problem wurde in dieser Version behoben. (Bug 1076780)

1.4.43 Öffnen von PRDs über die Seite „Anwendungen“ im Dashboard

Je nach den Einstellungen auf der Seite „Anforderung“ und „Anwendungen“ können Sie PRDs entweder in einer neuen Registerkarte oder in demselben Fenster öffnen. (Bug 1076155)

1.4.44 Integrationsaktivität unterstützt die Kommunikation mit Servern, für die die beiderseitige Authentifizierung aktiviert ist

Wenn ein Client und ein privates Zertifikat angegeben sind, können Sie problemlos mit einem Server kommunizieren, für den die beiderseitige Authentifizierung über die Integrationsaktivität aktiviert ist. (Bug 1075309)

1.4.45 Organigramm im Dashboard zeigt die zugelassenen Objekte und Attribute für einen Benutzer

Das Organigramm zeigt nunmehr ordnungsgemäß die Informationen, die der Benutzer tatsächlich zu sehen berechtigt ist. (Bug 1076155)

1.4.46 Im Skript „idmapps_tomcat_init“ sind keine Ausführungsberechtigungen mehr für „etc/rc.d/init.d/functions“ erforderlich, damit der Dienst als Daemon unter Linux ausgeführt wird

Diese Abhängigkeit wurde aus der Installations-Software entfernt. (Bug 1064603)

1.4.47 Standardmäßige Benachrichtigungserfassungsschablonen zeigen die richtigen Sprachen

Die standardmäßigen Benachrichtigungsschablonen werden ordnungsgemäß in die angegebene Sprache übersetzt. (Bug 1063967)

1.4.48 Dashboard zeigt Aufgaben ordnungsgemäß an, wenn die Spalte „METAXML“ den Datentyp „ntext“ besitzt

Wenn Sie die Spaltentypen für „METAXML“ unter „AFDOCUMENT“ auf den Argumentdatentyp `ntext` umstellen, verarbeitet das Dashboard den geänderten Argumentdatentyp ordnungsgemäß. (Bug 1062342)

1.4.49 In den Anmerkungen im Anforderungsverlauf wird der vollständige Name eines Benutzers statt des CN angezeigt

Im Anmerkungsbereich im Anforderungsverlauf wird nunmehr der vollständige Name eines Benutzers statt des CN angezeigt. Wenn Sie auf den vollständigen Namen des Benutzers klicken, wird im Dashboard ein Popup-Fenster mit Kurzinformationen zu diesem Benutzer geöffnet. Dieses Fenster enthält außerdem einen Deep-Link zur Seite des Benutzers, auf der Sie weitere Informationen zum betreffenden Benutzer finden. (Bug 1060709)

1.4.50 Breite des Listenfelds bleibt bei einer Datumsänderung unverändert

Wenn Sie ein Datum in einem Benutzeranwendungsformular festlegen oder ändern, wird die Breite der Listenfelder nicht mehr auf die Breite der ersten Liste eingestellt. (Bug 1049919)

1.4.51 PRD wird ordnungsgemäß in einer neuen Registerkarte geöffnet

Wenn Sie eine benutzerdefinierte PRD über die Registerkarte „Anwendungen“ ausführen, werden die Einstellungen für die Anforderungsformulare nunmehr zum richtigen Zeitpunkt geladen, sodass die PRD nicht in einem neuen Fenster geöffnet wird, sondern in einer neuen Registerkarte. (Bug 1044350)

1.4.52 Anforderer-„fdn <req>“ in einem Benutzerobjekt für Rollen und Ressourcen wird beim Umbenennen des Benutzers geändert

Der `<req>` mit dem Anforderer-`fdn <req>` in einem Benutzerobjekt für die Attribute „`nrfassignedroles`“ und „`nrfassignedresources`“ wird ordnungsgemäß aktualisiert, wenn ein Benutzer umbenannt wird. (Bug 1028476)

1.4.53 „getRoleLevels“ gibt richtige Informationen zurück

Der SOAP-Endpunkt „`getRoleLevels`“ gibt nunmehr die Rollenebenen in der richtigen Reihenfolge zurück. (Bug 935105)

1.4.54 Variable NETIQ_TOMCAT_USER wurde aus dem Tomcat-PostgreSQL-Installationsprogramm für Windows entfernt

Die Variable NETIQ_TOMCAT_USER wurde aus der Installationsdatei für die unbeaufsichtigte Installation im Tomcat-PostgreSQL-Installationsprogramm für Windows gelöscht. Mit dem neuen Linux-Installationsprogramm kann die Eigenschaftendatei für die unbeaufsichtigte Installation auf der Grundlage der Benutzereingaben erstellt werden; ein Bundle mit einer fest programmierten Eigenschaftendatei ist nicht mehr erforderlich. Diese Änderung gilt für Linux nicht mehr. (Bug 925699)

1.4.55 Möglichkeit zum Sortieren des Anforderungsverlaufs im Dashboard

Auf der Seite „Anforderungsverlauf“ wird der Verlauf nunmehr in umgekehrter Reihenfolge (nach dem Datum) aufgelistet. (Bug 1061515)

1.4.56 Rollen- und Ressourcenservice-Treiber

1.4.56.1 Möglichkeit, den von Benutzern ausgelösten Anforderungen den Vorrang vor geplanten Anforderungen zu geben

Der Rollen- und Ressourcendiensttreiber gibt Anforderungen, die vom Benutzer ausgelöst wurden, nunmehr den Vorrang vor Anforderungen, die vom Treiber selbst erzeugt wurden. (Bug 1008920)

1.4.56.2 Beim Löschen von Rollen werden überlappende Berechtigungswerte nicht entfernt

Der Rollen- und Ressourcendiensttreiber baut einen temporären Cache mit Ressourcenverknüpfungs-Erstellungsereignissen auf; anschließend wird die gelöschte Ressourcenverknüpfung erneut synchronisiert und die Ressourcen werden mit Blick auf eine fehlende Rolle neu berechnet. Damit ist gewährleistet, dass ausschließlich Verknüpfungen entfernt werden, die keinen anderen zugewiesenen Rollen zugeordnet sind. (Bug 1040935)

1.4.56.3 Möglichkeit zum Verarbeiten von Objektverschiebungen

Der Wiederherstellungsmechanismus des Treibers verarbeitet Benutzerverschiebungen nunmehr ordnungsgemäß, wenn der Treiber diesem Benutzer bestimmte Rollen und Ressourcen zuweist. (Bug 1061399)

1.4.56.4 Rollen- und Ressourcendiensttreiber verarbeitet eine fehlgeschlagene Änderung der dynamischen Gruppenmitgliedschaft ordnungsgemäß

Der Treiber kann nunmehr fehlgeschlagene Änderungen der dynamischen Gruppenmitgliedschaft verarbeiten. (Bug 736047)

1.5 Geht auf eine Softwareschwachstelle ein

Mit dieser Version wird auf folgende häufige Schwachstellen und Sicherheitslücken (Common Vulnerabilities and Exposures, CVE) von Identity Manager eingegangen:

- ♦ CVE-2018-7676
- ♦ CVE-2018-7674
- ♦ CVE-2018-7673
- ♦ CVE-2018-1350
- ♦ CVE-2018-1349
- ♦ CVE-2018-1348

1.6 Was wurde geändert oder eingestellt und was ist ausgelaufen?

Zur Optimierung der Funktionalität wurden einige Komponenten geändert oder werden in Identity Manager 4.7 nicht mehr unterstützt. In vielen Fällen wurden die entsprechenden Komponenten durch alternative Funktionen ersetzt.

1.6.1 Veraltete Funktionen oder Funktionalitäten

In der nachfolgenden Liste finden Sie eine Übersicht der Features und Funktionen, die mittlerweile veraltet sind.

Identitätsselbstbedienung, Arbeits-Dashboard, Konformität, Rollen- und Ressourcenverwaltung in der Benutzeranwendung

In dieser Identity Manager-Version wird die Verwaltungsoberfläche der Identitätsanwendungen eingeführt. Diese Funktionen stehen nicht mehr in der Benutzeranwendung zur Verfügung, sondern nur noch in der neuen Benutzeroberfläche. Von dieser Version an werden diese Funktionen der Benutzeranwendung nicht mehr unterstützt. Weitere Informationen finden Sie in [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen).

Bisherige Passwortverwaltung

Die bisherige Selbstbedienungsfunktion für Passwörter wird ab dieser Version nicht mehr unterstützt. Für Protokollereignisse muss SSPR verwendet werden. Weitere Informationen finden Sie im [Einrichtungshandbuch zu NetIQ Identity Manager für Linux](#) bzw. im [Einrichtungshandbuch zu NetIQ Identity Manager für Windows](#).

1.6.2 Eingestellte Funktionen oder Funktionalitäten

In der folgenden Liste finden Sie eine Übersicht der Features und Funktionen, die mit dieser Version eingestellt wurden:

Programm für die integrierte Installation

Identity Manager 4.7 unterstützt das Programm für die integrierte Installation nicht mehr. Dieses Installationsprogramm wird mit dieser Version eingestellt.

XDAS-Revision für Identitätsanwendungen

Die Revision mit XDAS für die Komponenten der Identitätsanwendungen ist ab dieser Version nicht mehr möglich. Die Identitätsanwendungsereignisse müssen mit CEF protokolliert werden.

Diese Änderung gilt nicht für andere Identity Manager-Komponenten, die XDAS unterstützen. NetIQ empfiehlt die CEF-Revision für alle Identity Manager-Komponenten.

Separater Zugriff auf die Identity Manager-Startseite und das Bereitstellungs-Dashboard sowie auf Catalog Administrator

Diese Version umfasst eine optimierte Version des Identity Manager-Dashboards, die die Startseite und das Bereitstellungs-Dashboard ersetzt. Die Identity Manager-Startseite und das Bereitstellungs-Dashboard werden mit dieser Version eingestellt.

Die Funktionalität von Catalog Administrator wird in die Verwaltungsoberfläche der Identitätsanwendungen eingebunden. Catalog Administrator wird mit dieser Version eingestellt.

REST-Oberflächendienst (RIS)

In dieser Identity Manager-Version wird die Funktionalität der Identitätsanwendungen über eine API (Application Programming Interface) bereitgestellt. Die API beruht auf HTTP und umfasst eine RESTful-Programmierschnittstelle. Sie können die API über einen REST-Client oder mit dem Befehl „curl“ in Skripten aufrufen und so die Verwaltungsaufgaben automatisieren. RIS wird mit dieser Version eingestellt.

RHEL 6.x- und SLES 11.x-Plattformen

Die Plattformen RHEL 6.x und SLES 11.x werden ab dieser Version nicht mehr unterstützt.

1.7 Separate Einrichtungshandbücher für Linux- und Windows-Plattformen

Diese Version umfasst separate Handbücher für die Installation, Konfiguration, Aufrüstung und Deinstallation von Identity Manager-Komponenten auf Linux- und Windows-Plattformen. Weitere Informationen finden Sie unter den folgenden Links:

- ♦ [Einrichtungshandbuch zu NetIQ Identity Manager für Linux](#)
- ♦ [Einrichtungshandbuch zu NetIQ Identity Manager für Windows](#)

1.8 Die Endbenutzer-Lizenzvereinbarung ist nicht in allen unterstützten Sprachen verfügbar

Jedes Installationsprogramm umfasst eine Endbenutzer-Lizenzvereinbarung. Obwohl die Installationsprogramme mehrere Sprachen unterstützen, ist die Lizenzvereinbarung in den folgenden Sprachen nicht verfügbar:

- ♦ Dänisch
- ♦ Niederländisch
- ♦ Russisch
- ♦ Schwedisch

Stattdessen zeigt das Installationsprogramm die Lizenzvereinbarung in englischer Sprache an. Weitere Informationen finden Sie unter „[Erläuterungen zu unterstützten Sprachen](#)“ im [Einrichtungshandbuch zu NetIQ Identity Manager für Linux](#) bzw. im [Einrichtungshandbuch zu NetIQ Identity Manager für Windows](#). (Bug 896299)

1.9 NetIQ Corporation bietet keine Unterstützung für die Komponenten in der PostgreSQL- und Tomcat-Installation

Auf einem Linux-Server werden die PostgreSQL- und Tomcat-Komponenten automatisch installiert. Unter Windows werden diese Komponenten mit einem separaten Installationsprogramm installiert. Bitte beachten Sie, dass NetIQ Corporation die PostgreSQL- und Tomcat-Installation als unverbindliche Zusatzleistung zur Verfügung stellt. Wenn Ihr Unternehmen noch keinen Anwendungsserver und Datenbankserver bereitgestellt hat, können Sie diese Komponenten installieren und nutzen. Wenn Sie Unterstützung benötigen, wenden Sie sich an den Anbieter der Komponente. Neben den Angaben im [Einrichtungshandbuch zu NetIQ Identity Manager für Linux](#) bzw. im [Einrichtungshandbuch zu NetIQ Identity Manager für Windows](#) bietet NetIQ keine Aktualisierungen und keine Informationen zur Verwaltung, Konfiguration oder Optimierung dieser Komponenten.

2 Identity Manager-Komponentenversionen

Identity Manager 4.7 bündelt die folgenden Komponenten:

- ♦ NetIQ eDirectory 9.1
- ♦ NetIQ iManager 3.1
- ♦ NetIQ Identity Manager Engine 4.7
- ♦ NetIQ Identity Manager Remote Loader 4.7
- ♦ NetIQ Identity Manager Fanout Agent 1.2
- ♦ NetIQ Designer für Identity Manager 4.7
- ♦ NetIQ-Identitätsanwendungen 4.7
- ♦ NetIQ Single Sign-on (One SSO) 6.2.1
- ♦ NetIQ Identity Manager – Zurücksetzen von Passwörtern per Selbstbedienung 4.2.0.4
- ♦ Platform Agent 2011.1r6
- ♦ NetIQ Identity Manager Client Login Extension 4.2
- ♦ NetIQ Identity Manager Identity Reporting 6.0
- ♦ NetIQ Sentinel Log Management für IGA 8.1.1 (für die Ereignisrevision)
- ♦ NetIQ Analyzer für Identity Manager 4.7
- ♦ NetIQ Identity Manager-Treiber. Die Versionen der Treiber finden Sie in der [Tabelle zur Kompatibilität der Treiber- und Engine-Versionen](#).

HINWEIS: Die Versionen der Identity Manager-Treiber sind von der Engine-Version unabhängig und lassen nicht darauf schließen, welche Engine-Version zum Ausführen dieser Treiber mindestens erforderlich ist.

3 Systemanforderungen

Die Identity Manager-Komponenten können auf verschiedenen Betriebssystemplattformen installiert werden. Weitere Informationen zu den Komponenten, die unter den verschiedenen Betriebssystemen installiert werden können, finden Sie unter „[Auswählen einer Betriebssystemplattform für Identity Manager](#)“ im *Einrichtungshandbuch zu NetIQ Identity Manager für Linux* bzw. im *Einrichtungshandbuch zu NetIQ Identity Manager für Windows*.

Weitere Informationen zu den Voraussetzungen und Computeranforderungen sowie zur Installation, Aufrüstung oder Migration für Ihre Plattform finden Sie hier:

- ♦ [Einrichtungshandbuch zu NetIQ Identity Manager für Linux](#)
- ♦ [Einrichtungshandbuch zu NetIQ Identity Manager für Windows](#)

4 Installation von NetIQ Identity Manager 4.7

Identity Manager 4.7 enthält die Advanced Edition und Standard Edition in einer einzelnen ISO-Datei. Bevor Sie die Installationsdateien herunterladen, machen Sie sich mit den Funktionen in den verschiedenen Editionen und mit den Optionen zum Herunterladen der Identity Manager-Komponenten vertraut.

- ♦ [Abschnitt 4.1, „In Identity Manager Advanced und Standard Edition unterstützte Funktionen“, auf Seite 20](#)
- ♦ [Abschnitt 4.2, „Herunterladen von Identity Manager“, auf Seite 20](#)

- ♦ [Abschnitt 4.3, „Suchen der ausführbaren Dateien und Standardinstallationspfade“, auf Seite 21](#)
- ♦ [Abschnitt 4.4, „Installation von NetIQ Identity Manager 4.7“, auf Seite 23](#)

4.1 In Identity Manager Advanced und Standard Edition unterstützte Funktionen

Die Identity Manager-Funktionen werden in zwei Produktgruppen ausgeliefert, um verschiedene Kundenanforderungen zu erfüllen:

- ♦ Identity Manager Advanced Edition
- ♦ Identity Manager Standard Edition

Die Identity Manager Advanced Edition enthält die Identity Manager-Funktionen der Identity Manager Standard Edition sowie zusätzliche Funktionen. In der folgenden Tabelle sehen Sie einen Vergleich der Funktionen, die in der Identity Manager Advanced Edition und in der Standard Edition vorhanden sind:

| Funktion | Advanced Edition | Standard Edition |
|---|------------------|-----------------------------------|
| Automatische regelbasierte Benutzerbereitstellung | Ja | Ja |
| Identitätssynchronisierung in Echtzeit | Ja | Ja |
| Passwortverwaltung und Passwortselbstbedienung | Ja | Ja |
| Einheitliches Identitätsinformations-Tool (Analyzer) | Ja | Ja |
| REST APIs und Single Sign-on-Support | Ja | Ja (eingeschränkte Unterstützung) |
| Berichterstellung über den aktuellen Zustand | Ja | Ja |
| Rollenbasierte unternehmensgerechte Bereitstellung | Ja | Nein |
| Automatische Genehmigungs-Workflows für die Durchsetzung von Geschäftsrichtlinien | Ja | Nein |
| Erweiterte Selbstbedienung in den Identitätsanwendungen | Ja | Nein |
| Ressourcenmodell und Katalog für die einfache Ressourcenbereitstellung | Ja | Nein |
| Berichterstellung über den Zustandsverlauf | Ja | Nein |
| Berichterstellung über verbundene Systeme | Ja | Nein |
| Katalogadministrator | Ja | Nein |

4.2 Herunterladen von Identity Manager

Nachdem Sie Identity Manager 4.7 käuflich erworben haben, melden Sie sich bei der [Identity Manager-Produkt-Website](#) an und folgen Sie dem Link zum Herunterladen der Software. Die folgenden Dateien enthalten die Identity Manager-Komponenten:

| Dateiname | Beschreibung |
|--|--|
| Identity_Manager_4.7_Linux.iso | Enthält Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration), Identitätsanwendungen, Identity Reporting, Designer und Analyzer |
| Identity_Manager_4.7_Windows.iso | Enthält Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration), Identitätsanwendungen, Identity Reporting, Designer und Analyzer |
| Identity_Manager_4.7_Linux_Designer.tar.gz | Enthält Designer |
| Identity_Manager_4.7_Windows_Designer.zip | Enthält Designer |
| Identity_Manager_4.7_MacOSX_Designer.tar.gz | Enthält Designer-Dateien für macOS 10.13 (High Sierra) |
| Identity_Manager_4.7_Linux_Analyzer.tar.gz | Enthält Analyzer |
| Identity_Manager_4.7_Windows_Analyzer.zip | Enthält Analyzer |
| SentinelLogManagementForIGA8.1.1.0.tar.gz | Enthält Sentinel Log Management für Identity Governance & Administration |
| Diese Installation wird nur unter Linux unterstützt. | |

- 1 Gehen Sie zur [NetIQ Downloads-Website](#).
- 2 Wählen Sie im Menü **Produkt oder Technologie** den Eintrag Identity Manager aus, und klicken Sie auf **Suchen**.
- 3 Klicken Sie auf der **Download-Website von NetIQ Identity Manager** auf die Schaltfläche **Download** neben der herunterzuladenden Datei.
- 4 Befolgen Sie die Bildschirmanweisungen, um die Datei in einen Ordner auf Ihrem Computer herunterzuladen.

4.3 Suchen der ausführbaren Dateien und Standardinstallationspfade

- ♦ [Abschnitt 4.3.1, „Ausführbare Dateien und Standard-Installationspfade unter Linux“, auf Seite 22](#)
- ♦ [Abschnitt 4.3.2, „Ausführbare Dateien und Standard-Installationspfade unter Windows“, auf Seite 22](#)

4.3.1 Ausführbare Dateien und Standard-Installationspfade unter Linux

| Identity Manager-Komponente | Speicherort der ausführbaren Datei innerhalb der ISO | Standardinstallationspfad |
|---|--|---|
| Identity Manager Server (enthält Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration) | install.sh im eingehängten Speicherort | <ul style="list-style-type: none"> ♦ Engine: /opt/novell/eDirectory/lib/dirxml ♦ Remote Loader: /opt/novell/dirxml/bin/x86_64 ♦ Fan-out-Agent: /opt/novell/dirxml/fanoutagent ♦ iManager: var/opt/novell/iManager |
| Identitätsanwendungen (Identity Manager-Dashboard, Identity Manager-Verwaltungsoberfläche, Benutzeranwendung, Rollen- und Ressourcendienstreiber, Benutzeranwendungstreiber, Konfigurationsaktualisierungsprogramm) | install.sh im eingehängten Speicherort | <ul style="list-style-type: none"> ♦ Identitätsanwendungen: /opt/netiq/idm/apps ♦ Benutzeranwendung: /opt/netiq/idm/apps/UserApplication ♦ Konfigurationsaktualisierungsprogramm: /opt/netiq/idm/apps/configupdate |
| Designer für Identity Manager | /designer/packages | /root/designer |
| Identitätsberichterstellung | install.sh im eingehängten Speicherort | /opt/netiq/idm/apps/IDMReporting |
| Analyzer für Identity Manager | /analyzer/packages | /root/analyzer |
| Sentinel Log Management für IGA | ./install.sh unter /SentinelLogManagementforIGA in der Datei SentinelLogManagementForIGA8.1.1.0.tar.gz | /opt/novell/sentinel |

4.3.2 Ausführbare Dateien und Standard-Installationspfade unter Windows

| Identity Manager-Komponente | Speicherort der ausführbaren Datei innerhalb der ISO | Standardinstallationspfad |
|-----------------------------|--|---------------------------|
| Identitätsdepot | Setup.exe unter \products\eDirectory\x64\ | C:\netiq\eDirectory |

| Identity Manager-Komponente | Speicherort der ausführbaren Datei innerhalb der ISO | Standardinstallationspfad |
|---|---|---|
| iManager | <ul style="list-style-type: none"> ♦ Serverinstallation: iManagerInstall.exe unter \products\iManager\inst alls\win\ ♦ Installation der Arbeitsstation: iManager.bat unter imanager\bin | <ul style="list-style-type: none"> ♦ Serverinstallation: C:\Programme\Novell ♦ Installation der Arbeitsstation: C:\Programme\Novell |
| Remote Loader | idm_install.exe unter \products\IDM\windows\setup | C:\Novell |
| PostgreSQL und Tomcat (unterstützte Datenbank und Anwendungsserver) | TomcatPostgreSQL.exe unter products\CommonApplication\ postgre_tomcat_install\ | C:\netiq\idm\apps\tomcat |
| Single Sign-on (OSP) | osp-install.exe unter \products\CommonApplication \osp_install | C:\netiq\idm\apps\osp |
| Zurücksetzen von Passwörtern per Selbstbedienung (SSPR) | sspr-install.exe unter \products\CommonApplication \sspr_install | C:\netiq\idm\apps\sspr |
| Identitätsanwendungen | IdmUserApp.exe unter products\UserApplication | C:\netiq\idm\apps\UserApplication |
| Designer für Identity Manager | install.exe unter \products\Designer\ | C:\netiq\idm\apps\Designer |
| Identitätsberichterstellung | rpt-install-win.exe unter \products\Reporting | C:\netiq\idm\apps\IdentityReporting |
| Analyzer für Identity Manager | install.exe unter \products\Analyzer\ | C:\netiq\idm\apps\Analyzer |

4.4 Installation von NetIQ Identity Manager 4.7

Prüfen Sie die Informationen aus einer der folgenden Ressourcen (je nach der zu installierenden Edition):

- ♦ Advanced Edition: [Einrichtungshandbuch zu NetIQ Identity Manager für Linux](#) bzw. [Einrichtungshandbuch zu NetIQ Identity Manager für Windows](#)
- ♦ Standard Edition: [Kurzanleitung für die Installation und Aktualisierung von NetIQ Identity Manager 4.7 Standard Edition](#)

5 Aufrüsten auf NetIQ Identity Manager 4.7

Sie können von Identity Manager 4.6.x und 4.5.6 auf Identity Manager 4.7 aufrüsten. NetIQ empfiehlt, vor dem Starten der Aufrüstung die Informationen in den Versionshinweisen zu Ihrer aktuellen Version zu lesen.

- ♦ [Abschnitt 5.1, „Aufrüsten von Identity Manager 4.6.x“, auf Seite 24](#)
- ♦ [Abschnitt 5.2, „Upgrade von Identity Manager 4.5.6“, auf Seite 25](#)

- ♦ [Abschnitt 5.3, „Aufrüsten auf Advanced Edition“, auf Seite 26](#)
- ♦ [Abschnitt 5.4, „Aufrüsten auf Standard Edition“, auf Seite 27](#)

Weitere Informationen zum Aufrüsten von Identity Manager finden Sie unter „[Aufrüsten von Identity Manager](#)“ im *Einrichtungshandbuch zu NetIQ Identity Manager für Linux* bzw. im *Einrichtungshandbuch zu NetIQ Identity Manager für Windows*.

5.1 Aufrüsten von Identity Manager 4.6.x

Die nachfolgende Tabelle zeigt die Aufrüstungspfade für die Identity Manager-Komponenten:

| Komponente | Basisversion | Anmerkungen |
|-------------------------|--------------|---|
| Identity Manager-Engine | 4.6.x | <ol style="list-style-type: none"> 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie Identity Manager auf Version 4.7 auf. HINWEIS: Vor dem Aufrüsten der Engine muss das Identitätsdepot auf Version 9.1 aufgerüstet werden. |
| Remote Loader | 4.6.x | Installieren Sie Remote Loader 4.7. |
| Fan-out-Agent | 4.6.x | Installieren Sie Fanout Agent 4.7. |
| Designer | 4.6.x | <ol style="list-style-type: none"> 1. Installieren Sie Designer 4.7. 2. Stellen Sie Ihren Arbeitsbereich auf den LDAP-gestützten Designer um. Bevor Sie die Arbeit mit dieser Version aufnehmen, beachten Sie die Versionshinweise zu NetIQ Identity Manager Designer 4.6. |
| Identitätsanwendungen | 4.6.x | <p>Bevor Sie die Identitätsanwendungen aufrüsten, müssen das Identitätsdepot auf Version 9.1 und die Identity Manager-Engine auf Version 4.7 aufgerüstet werden.</p> <ol style="list-style-type: none"> 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Aktualisieren Sie das Benutzeranwendungstreiber- und das Rollen- und Ressourcenservicetreiber-Paket. 3. Rüsten Sie die Datenbank auf eine unterstützte Version auf (PostgreSQL, Oracle oder MS SQL). 4. (Bedingt) Wenn SSPR auf einem separaten Computer installiert ist, rüsten Sie die Komponente auf Version 4.7 auf. 5. Halten Sie Tomcat an. 6. Rüsten Sie die Identitätsanwendungen auf Version 4.7 auf. |

| Komponente | Basisversion | Anmerkungen |
|-----------------------------|--------------|--|
| Identitätsberichterstellung | 4.6.x | <ol style="list-style-type: none"> 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie die Datenbank auf eine unterstützte Version auf (PostgreSQL oder Oracle). 3. Rüsten Sie SLM für IGA auf. 4. Installieren Sie Identity Reporting 4.7. 5. Rüsten Sie das Data Collection Services-Treiberpaket und das Treiberpaket „Veraltetes System – Gateway“ auf. |

5.2 Upgrade von Identity Manager 4.5.6

Die nachfolgende Tabelle zeigt die Aufrüstungspfade für die Identity Manager-Komponenten:

| Komponente | Basisversion | Zwischenschritt | Anmerkungen |
|-------------------------|--|--|--|
| Identity Manager-Engine | Identity Manager 4.5.x (x = 0 bis 5) mit eDirectory 8.8.8.x (x = 3 bis 9) | Wenden Sie das Service Pack für Identity Manager 4.5.6 an. | <ol style="list-style-type: none"> 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie Identity Manager auf Version 4.7 auf. <p>HINWEIS: Vor dem Aufrüsten der Engine muss das Identitätsdepot auf Version 9.1 aufrüstet werden.</p> |
| Remote Loader | 4.5.x | | Installieren Sie Remote Loader 4.7. |
| Fan-out-Agent | 4.5.x | | Installieren Sie Fanout Agent 4.7. |
| Designer | 4.5.x | | <ol style="list-style-type: none"> 1. Installieren Sie Designer 4.7. 2. Stellen Sie Ihren Arbeitsbereich auf den LDAP-gestützten Designer um. <p>Bevor Sie die Arbeit mit dieser Version aufnehmen, beachten Sie die Versionshinweise zu NetIQ Identity Manager LDAP Designer.</p> |

| Komponente | Basisversion | Zwischenschritt | Anmerkungen |
|------------------------------|--------------|--|---|
| Identitätsanwendungen | 4.5.x | Wenn Sie mit einem JBoss- oder WebSphere-Anwendungsserver arbeiten, migrieren Sie zum Tomcat-Anwendungsserver. | <p>Bevor Sie die Identitätsanwendungen aufrüsten, müssen das Identitätsdepot auf Version 9.1 und die Identity Manager-Engine auf Version 4.7 aufrüstet werden.</p> <ol style="list-style-type: none"> 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Aktualisieren Sie das Benutzeranwendungstreiber- und das Rollen- und Ressourcenservicetreiber-Paket. 3. Rüsten Sie die Datenbank auf eine unterstützte Version auf (PostgreSQL, Oracle oder MS SQL). 4. (Bedingt) Wenn SSPR auf einem separaten Computer installiert ist, rüsten Sie die Komponente auf Version 4.7 auf. 5. Halten Sie Tomcat an. 6. Rüsten Sie die Identitätsanwendungen auf Version 4.7 auf. |
| Identitätsberichtserstellung | 4.5.x | Wenn Sie mit einem JBoss- oder WebSphere-Anwendungsserver arbeiten, migrieren Sie zum Tomcat-Anwendungsserver. | <ol style="list-style-type: none"> 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 3. Migrieren Sie die Ereignisrevisionsdienst-Daten zu einer unterstützten Version einer PostgreSQL- oder Oracle-Datenbank. 4. Installieren Sie SLM für IGA. 5. Installieren Sie Identity Reporting 4.7. 6. Führen Sie das Datensynchronisierungsprogramm aus. 7. Rüsten Sie das Data Collection Services-Treiberpaket und das Treiberpaket „Veraltetes System – Gateway“ auf. |

5.3 Aufrüsten auf Advanced Edition

NetIQ bietet die folgenden Aufrüstungspfade für die Aufrüstung auf Identity Manager 4.6 Advanced Edition von einer früheren Advanced Edition oder Standard Edition:

- ♦ Identity Manager 4.5 Advanced Edition auf 4.6 Advanced Edition

- ♦ Identity Manager 4.5 Standard Edition auf 4.6 Advanced Edition anhand einer der folgenden Methoden:
 - ♦ Von Identity Manager 4.5 Standard Edition auf 4.7 Standard Edition und dann auf 4.6 Advanced Edition
 - ♦ Von Identity Manager 4.6 Standard Edition auf 4.5 Advanced Edition und dann auf 4.7 Advanced Edition

5.4 Aufrüsten auf Standard Edition

Sie können von Identity Manager 4.6 Standard Edition auf Identity Manager 4.7 Standard Edition aufrüsten. Wenn Sie von einer früheren Version vor Identity Manager 4.6 aufrüsten, müssen Sie Identity Reporting vom bisherigen Anwendungsserver auf Tomcat migrieren. Dies gilt sowohl für Linux- als auch für Windows-Plattformen. Anweisungen zum Aufrüsten finden Sie in der [Kurzanleitung für die Installation und Aktualisierung von NetIQ Identity Manager 4.6 Standard Edition](#).

Identity Manager 4.7 Standard Edition unterstützt weiterhin die folgenden Berichte:

- ♦ Authentifizierung nach Benutzer
- ♦ Authentifizierung nach Server
- ♦ Datenbankstatistik
- ♦ Eigene Passwortänderungen
- ♦ Passwortrücksetzungen
- ♦ Identitätsdepottreiber: Verknüpfungsbericht: Aktueller Status
- ♦ Identitätsdepotbenutzer-Bericht: Aktueller Status
- ♦ Ereigniszusammenfassung: Benutzerpasswortänderungen

Weitere Informationen finden Sie im [Verwaltungshandbuch für die NetIQ-Identitätsberichterstellung](#).

WICHTIG: Zur Verwendung der Berichte müssen Sie die Berichtsdefinitionen in die Identitätsberichterstellung importieren. Melden Sie sich bei der Berichterstellungsanwendung an und laden Sie die Berichte über die **Download**-Seite in der Anwendung herunter.

6 Bekannte Probleme

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

- ♦ [Abschnitt 6.1, „Probleme bei der Installation“, auf Seite 28](#)
- ♦ [Abschnitt 6.2, „Probleme bei der Identity Manager-Engine“, auf Seite 30](#)
- ♦ [Abschnitt 6.3, „Probleme mit Remote Loader“, auf Seite 31](#)
- ♦ [Abschnitt 6.4, „Probleme in Verbindung mit Treibern“, auf Seite 33](#)
- ♦ [Abschnitt 6.5, „Probleme mit Identitätsanwendungen“, auf Seite 34](#)
- ♦ [Abschnitt 6.6, „Probleme mit der Identitätsberichterstellung“, auf Seite 41](#)
- ♦ [Abschnitt 6.7, „Probleme mit iManager-Plugins“, auf Seite 43](#)
- ♦ [Abschnitt 6.8, „Probleme beim Aufrüsten von Identity Manager“, auf Seite 43](#)

- ♦ [Abschnitt 6.9, „Lokalisierungsprobleme“, auf Seite 45](#)
- ♦ [Abschnitt 6.10, „Probleme bei der Deinstallation“, auf Seite 47](#)

6.1 Probleme bei der Installation

- ♦ [Abschnitt 6.1.1, „Fehlender Startschlüssel für Berichterstellungsdatenbank meldet nach der Konfiguration unter Linux eine Ausnahme“, auf Seite 28](#)
- ♦ [Abschnitt 6.1.2, „Datenquelle wird nicht in die Seite der Berichterstellungsanwendung eingetragen, wenn das Datenbankschema bei der Installation von Identity Reporting mit einer Oracle-Datenbank unter Windows erstellt wird“, auf Seite 28](#)
- ♦ [Abschnitt 6.1.3, „Unter Windows können keine Installationspfade angegeben werden, die Leerzeichen enthalten“, auf Seite 29](#)
- ♦ [Abschnitt 6.1.4, „Tomcat kann mit dem Task-Manager unter Windows nicht neu gestartet werden“, auf Seite 29](#)
- ♦ [Abschnitt 6.1.5, „LDAP-Server zeigt bei Verwendung der VLV- und SSS-Steuerelemente einen Fehler an“, auf Seite 29](#)
- ♦ [Abschnitt 6.1.6, „Es werden keine Tabellen erstellt, wenn das ConfigUpdate-Dienstprogramm unmittelbar nach dem Installieren der Identitätsanwendungen gestartet wird“, auf Seite 29](#)
- ♦ [Abschnitt 6.1.7, „Einige Installationsassistenten zeigen ein falsches Symbol für die Komponenten an“, auf Seite 30](#)
- ♦ [Abschnitt 6.1.8, „Das Navigationspanel wird im Installationsprogramm für die Identitätsberichterstellung abgeschnitten unter Windows“, auf Seite 30](#)

6.1.1 Fehlender Startschlüssel für Berichterstellungsdatenbank meldet nach der Konfiguration unter Linux eine Ausnahme

Problem: Wenn Sie Identity Reporting auf demselben Server installieren, auf dem die Identitätsanwendungen installiert sind, und Sie beim Installieren von Identity Reporting die Option **Start** für das Erstellen der Datenbank festlegen, trägt das Konfigurationsskript einige Ausnahmen in das Protokoll ein. (Bug 1082959)

Behelfslösung: Starten Sie Tomcat manuell neu; hiermit werden die Ausnahmen gelöscht. Dies wirkt sich nicht auf die Installation aus. Sie können diese Ausnahme ignorieren.

6.1.2 Datenquelle wird nicht in die Seite der Berichterstellungsanwendung eingetragen, wenn das Datenbankschema bei der Installation von Identity Reporting mit einer Oracle-Datenbank unter Windows erstellt wird

Problem: Wenn Sie Identity Reporting installiert und konfiguriert haben und sich dann bei der Berichterstellungsanwendung anmelden, ist die Datenquelle nicht in der Anwendung verfügbar. (Bug 1082990)

In der Datei `catalina.out` wird der folgende Fehler protokolliert:

```
com.netiq.persist.PersistenceException: javax.naming.NameNotFoundException: Name [IDMDCSDataSource] is not bound in this Context. Unable to find [IDMDCSDataSource].
```

Behelfslösung: Konfigurieren Sie Identity Reporting und tragen Sie die Datenquelle dann manuell in die Berichterstellungsanwendung ein.

- 1 Melden Sie sich bei Identity Reporting an.
- 2 Klicken Sie auf **Datenquellen > Hinzufügen**.

- 3 Klicken Sie unter **Datenquelle hinzufügen** auf **Wählen Sie aus der vordefinierten Liste**.
- 4 Wählen Sie den Eintrag **IDMDCSDataSource** aus und geben Sie den Namen `IDMDCSDataSource` an.
Die Schaltfläche „Speichern“ wird nur dann aktiviert, wenn Sie einen Namen angeben.
- 5 Klicken Sie auf **Speichern**.

6.1.3 Unter Windows können keine Installationspfade angegeben werden, die Leerzeichen enthalten

Die Installationsprogramme für Identity Manager legen die Installationsdateien eventuell nicht im angegebenen Speicherort ab, wenn der Pfad Leerzeichen enthält. Stellen Sie sicher, dass der angegebene Pfad keine Leerzeichen enthält. (Bug 620797)

6.1.4 Tomcat kann mit dem Task-Manager unter Windows nicht neu gestartet werden

Problem: Mit dem Task-Manager kann Tomcat nicht auf einem Windows-Server neu gestartet werden. (Bug 893155)

Behelfslösung: Starten Sie Tomcat mit einem der folgenden Verfahren neu:

- ♦ Klicken Sie in der Services-Systemsteuerung mit der rechten Maustaste auf **IDM Apps Tomcat Service** und klicken Sie dann auf **Neu starten**.
- ♦ Halten Sie Tomcat an der Eingabeaufforderung an und starten Sie Tomcat dann neu:

```
net stop "IDM Apps Tomcat Service"  
net start "IDM Apps Tomcat Service"
```

Alternativ:

```
sc stop "IDM Apps Tomcat Service"  
sc start "IDM Apps Tomcat Service"
```

6.1.5 LDAP-Server zeigt bei Verwendung der VLV- und SSS-Steuerelemente einen Fehler an

Problem: Wenn Sie eine LDAP-Suche zur Verwendung von VLV (Virtual List View) und SSS (Server Side Sort) konfigurieren und der LDAP-Server keine lokale Kopie der Benutzerobjekte enthält, wird die Suche nicht durchgeführt und ein Fehler wird angezeigt.

Behelfslösung: Speichern Sie die Benutzerobjekte in Ihrer lokalen Reproduktion, um die VLV- und SSS-Steuerelemente zu verwenden. Weitere Informationen finden Sie in TID [7001493](#)

6.1.6 Es werden keine Tabellen erstellt, wenn das ConfigUpdate-Dienstprogramm unmittelbar nach dem Installieren der Identitätsanwendungen gestartet wird

Problem: Wenn Sie beim Installieren der Identitätsanwendungen die Option zum Erstellen von Tabellen beim Start wählen und die Anwendung nicht starten, sondern `configupdate` aufrufen und auf OK klicken, wird die Einstellung `com.netiq.idm.create-db-on-startup` auf `false` festgelegt. Da Sie die Anwendung nicht tatsächlich gestartet haben, werden keine Tabellen erstellt. Dieses Problem verursacht einen Fehler beim Start, da die Tabellen nicht vorhanden sind. (Bug 900284)

Behelfslösung: Öffnen Sie die Datei `ism-configuration.properties`, ändern Sie den Wert von `false` in `true`, speichern Sie die Datei und starten Sie die Anwendung anschließend neu.

6.1.7 Einige Installationsassistenten zeigen ein falsches Symbol für die Komponenten an

Problem: Das zusätzliche Installationsprogramm für Tomcat und PostgreSQL zeigt ein Java-Symbol statt eines Symbols für die Tomcat- und PostgreSQL-Komponenten an. Dieses Problem tritt auch in One SSO Provider (OSP) auf.

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.1.8 Das Navigationspanel wird im Installationsprogramm für die Identitätsberichterstellung abgeschnitten unter Windows

Problem: In einigen Sprachen wird das Navigationspanel auf der linken Seite des Installationsprogramms für das Identitätsberichterstellungsmodul abgeschnitten dargestellt. Sie können möglicherweise nicht alle Bezeichnungen auf dem Navigationspanel sehen. (Bug 899888)

Behelfslösung: Sie können das Navigationspanel bedenkenlos ignorieren und die Installation fortsetzen.

6.2 Probleme bei der Identity Manager-Engine

- [Abschnitt 6.2.1, „Große ECMAScripts können nicht ausgeführt werden“, auf Seite 30](#)
- [Abschnitt 6.2.2, „Größere Länge des OSP-Attributwerts verursacht Anmeldeprobleme“, auf Seite 30](#)
- [Abschnitt 6.2.3, „Fehler beim Hinzufügen mehrerer Berechtigungswerte zu einer statischen Ressource“, auf Seite 31](#)

6.2.1 Große ECMAScripts können nicht ausgeführt werden

Problem: Dieses Problem tritt auf, weil äußerst große Skripte nicht durch die Rhino-Engine analysiert werden können. (Bug 1016963, 942241)

Behelfslösung: Identity Manager 4.6 unterstützt die Nashorn-ECMAScript-Engine. Führen Sie große ECMAScripts mithilfe dieser Skript-Engine aus. Weitere Informationen finden Sie unter „[Werte zur Engine-Steuerung](#)“ im *Verwaltungshandbuch für den NetIQ Identity Manager-Treiber*.

Weitere Informationen zur Umstellung auf die Nashorn-Skript-Engine finden Sie im *[Rhino Migration Guide](#)* (Handbuch zur Rhino-Migration).

6.2.2 Größere Länge des OSP-Attributwerts verursacht Anmeldeprobleme

Problem: Wenn Sie sich nicht nach jeder erfolgreichen Anmeldung bei den Identitätsanwendungen wieder abmelden, erhöht sich der Wert des OSP-Attributs allmählich mit jeder Anmeldung. Die größere Länge des Werts führt zu Anmeldeproblemen.

Behelfslösung: Führen Sie einen der folgenden Schritte durch:

Löschen Sie den Wert des OSP-Attributs manuell in iManager.

- 1 Melden Sie sich bei iManager an.
- 2 Wählen Sie unter **Objekte anzeigen** das Benutzerobjekt aus.
- 3 Doppelklicken Sie auf der Registerkarte **Sonstige** auf das Attribut **oidInstanceData** und löschen Sie den Wert.

Oder,

Vermindern Sie den Wert für die Lebensdauer des Zugriffstokens mit dem ConfigUpdate-Dienstprogramm:

- 1 Starten Sie das ConfigUpdate-Dienstprogramm.
- 2 Wechseln Sie zur Registerkarte **Authentication**.
- 3 Vermindern Sie unter **Authentifizierungskonfiguration** den Wert für **Lebensdauer des Aktualisierungstokens (Stunden)**.

Standardmäßig ist für **Lebensdauer des Aktualisierungstokens (Stunden)** der Wert 48 Stunden eingestellt.

6.2.3 Fehler beim Hinzufügen mehrerer Berechtigungswerte zu einer statischen Ressource

Problem: Wenn Sie eine statische Ressource mit mehreren Berechtigungswerten anhand des Tokens `do-create-resource` erstellen, legt die Identity Manager-Engine nur ein „`nrfEntitlementRef`“-Objekt für die Ressource an. Mit diesem Token ist es daher nicht möglich, statische Ressourcen mit mehreren Zuweisungswerten zu erstellen. (Bug 995486)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.3 Probleme mit Remote Loader

- ♦ Abschnitt 6.3.1, „Fehler beim Erzeugen von Novell-Audit-Ereignissen für 32-Bit- und 64-Bit-Remote Loader auf demselben Server“, auf Seite 31
- ♦ Abschnitt 6.3.2, „Das auf der Remote Loader-Seite angegebene Schlüsselpasswort wird nicht mithilfe der beiderseitigen Authentifizierung validiert“, auf Seite 31
- ♦ Abschnitt 6.3.3, „Die für die beiderseitige Authentifizierung konfigurierte Remote Loader-Treiberinstanz startet nicht“, auf Seite 32

6.3.1 Fehler beim Erzeugen von Novell-Audit-Ereignissen für 32-Bit- und 64-Bit-Remote Loader auf demselben Server

Problem: Sie können zwar sowohl einen 32-Bit als auch einen 64-Bit Remote Loader auf demselben Computer installieren, allerdings können die `lcache`-Dateien für diese Versionen nicht gleichzeitig funktionieren. Die Novell-Audit-Ereignisse werden in der `lcache`-Datei für die Version protokolliert, die Sie zuerst installiert haben. Die Protokolldatei für die andere Version zeigt die Fehlermeldung an: `Agent wird bereits ausgeführt.` (Bug 676310)

Behelfslösung: Installieren Sie nicht beide Versionen auf demselben Computer.

6.3.2 Das auf der Remote Loader-Seite angegebene Schlüsselpasswort wird nicht mithilfe der beiderseitigen Authentifizierung validiert

Problem: Das `dxcmd`-Tool erzeugt die Datei `PEM` für einen privaten Schlüssel ohne Verschlüsselungspasswort. Identity Manager stellt daher die Verbindung zwischen Remote Loader und Engine her, ohne das Verschlüsselungspasswort (das Schlüsselpasswort) zu validieren. (Bug 1077147)

Behelfslösung: Erstellen Sie in iManager ein Client-KMO mit einem verschlüsselten Passwort. Erzeugen Sie die Datei `keyfile.pem` aus diesem KMO heraus und ersetzen Sie die vorhandene Datei `keyfile.pem` wie folgt:

- 1 Melden Sie sich bei iManager an.
- 2 Erstellen Sie ein KMO für eine Client-Authentifizierung im `.pfx`-Format:
 - 2a Wählen Sie **Rollen und Aufgaben > Zugriff auf NetIQ-Zertifikate > Serverzertifikate**.
 - 2b Klicken Sie auf **Neu** und geben Sie den **Kurznamen** für das Zertifikat an.
 - 2c Wählen Sie **Benutzerdefiniert** als Erstellungsmethode und klicken Sie auf **Weiter**.
Mit dieser Option können Sie Zertifikatparameter definieren.
 - 2d Wählen Sie **Organisations-Zertifizierungsstelle** und klicken Sie auf **Weiter**.
 - 2e Wählen Sie unter **Erweiterte Schlüsselnutzung aktivieren** die Option **Benutzer** und klicken Sie auf **Weiter**.
 - 2f Wählen Sie den **Gültigkeitszeitraum** in der Liste aus und klicken Sie auf **Weiter**.
 - 2g Wählen Sie **Zertifikat Ihrer Organisation** und klicken Sie auf **Weiter**.
 - 2h Klicken Sie auf **Fertig stellen**.
- 3 Wählen Sie das soeben erstellte Zertifikat aus und klicken Sie auf **Validieren**.
- 4 Wählen Sie das Client-KMO aus und klicken Sie auf **Exportieren**.

HINWEIS: Das KMO wird in iManager im `.pfx`-Format exportiert.

- 5 Konvertieren Sie das exportierte Client-KMO mit dem folgenden Befehl aus dem `.pfx`-Format in das `.pem`-Format:

```
openssl pkcs12 -in <exported_certificate_name>.pfx -out  
<converted_certificate_name>.pem
```

Beispiel:

```
openssl pkcs12 -in cert.pfx -out client_cert.pem
```

- 6 Ersetzen Sie `keyfile.pem` durch `client_cert.pem`

6.3.3 Die für die beiderseitige Authentifizierung konfigurierte Remote Loader-Treiberinstanz startet nicht

Problem: Nach dem Aufrüsten des 32-Bit- oder 64-Bit-Remote Loader kann ein Treiber, in dessen Konfiguration die beiderseitige Authentifizierung aktiviert ist, die Remote Loader-Instanz nicht starten. (Bug 1082989)

Behelfslösung: Gehen Sie nach dem Aufrüsten des Remote Loader wie folgt vor:

- 1 Bearbeiten Sie die Remote Loader-Instanz und geben Sie dasselbe Schlüsselpasswort an, das vor dem Aufrüsten des Remote Loader festgelegt war.
Das Standard-Schlüsselpasswort lautet `dirxml`.
- 2 Speichern Sie die Konfiguration.
- 3 Starten Sie die Remote Loader-Treiberinstanz.

6.4 Probleme in Verbindung mit Treibern

Bei Verwendung der Identity Manager-Treiber treten möglicherweise die folgenden Probleme auf:

- ♦ Abschnitt 6.4.1, „Im Statistikbericht wird null für Rollen- und Lizenzwerte für einen Office 365-Treiber angezeigt“, auf Seite 33
- ♦ Abschnitt 6.4.2, „Beim Starten der Remote Loader-Instanz eines Treibers tritt möglicherweise ein Fehler auf, wenn die Standardbreite des Windows-Eingabeaufforderungsfensters geändert wurde“, auf Seite 33
- ♦ Abschnitt 6.4.3, „dxcmd-Abfrage mit riesigem Ausgabevolumen wird zweimal durchgeführt“, auf Seite 33
- ♦ Abschnitt 6.4.4, „Problem beim Hinzufügen des Eintrags für DirXML-Konten bei der Migration eines Benutzers“, auf Seite 34
- ♦ Abschnitt 6.4.5, „Der Treiber-Cache-Inspector kann den letzten Eintrag in der Cache-Liste nicht anzeigen“, auf Seite 34
- ♦ Abschnitt 6.4.6, „Remedy-Treiber wird beim lokalen Ausführen mit der Identity Manager-Engine nicht gestartet“, auf Seite 34

6.4.1 Im Statistikbericht wird null für Rollen- und Lizenzwerte für einen Office 365-Treiber angezeigt

Problem: Der Statistikbericht für den Office 365-Treiber zeigt aufgrund einer Einschränkung im Office 365-Treiber null für die Werte **Rolle** und **Lizenz** im Abschnitt **Zugewiesene Kontoberechtigungen pro Typ** an. (Bug 893248)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.4.2 Beim Starten der Remote Loader-Instanz eines Treibers tritt möglicherweise ein Fehler auf, wenn die Standardbreite des Windows-Eingabeaufforderungsfensters geändert wurde

Problem: Wenn Sie den Standardwert für die Breite des Eingabeaufforderungsfensters ändern, wird die Treiberinstanz möglicherweise nicht gestartet und es werden keine Trace-Informationen erfasst. (Bug 854488)

Behelfslösung: Setzen Sie die Breite des Windows-Eingabeaufforderungsfensters auf den Standardwert 80 zurück.

6.4.3 dxcmd-Abfrage mit riesigem Ausgabevolumen wird zweimal durchgeführt

Problem: Wenn Sie den Befehl `dxcmd` zur Verarbeitung einer Abfrage an einen Treiber ausgeben, wartet die Identity Manager-Engine standardmäßig 120 Sekunden auf eine Antwort des Treibers. Wenn sie keine Antwort erhalten hat, versucht die Engine die Abfrage nach der Zeitüberschreitung erneut. Wenn sie nach weiteren 120 Sekunden keine Antwort erhält, zeigt die Engine den Fehler `ERR_TRANSPORT_FAILURE` an. Hierdurch verarbeitet der Treiber die Abfrage zweimal. (Bug 1014581)

Behelfslösung: Legen Sie die **Umgebungsvariable** `NCPCLIENT_REQ_TIMEOUT` auf einen Wert fest, der über dem für die Ausführung der Abfrage erwarteten Zeitraum liegt.

6.4.4 Problem beim Hinzufügen des Eintrags für DirXML-Konten bei der Migration eines Benutzers

Problem: Wenn ein Benutzer aus dem Identitätsdepot mit einem Treiber ohne Berechtigungspaket migriert wird, trägt Identity Manager keinen Wert in das Attribut `DirXML-Accounts` für den Benutzer ein. Dieses Problem tritt auf, wenn die Informationen für den Benutzer in der verbundenen Anwendung und im Identitätsdepot identisch sind. (Bug 1016682)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.4.5 Der Treiber-Cache-Inspector kann den letzten Eintrag in der Cache-Liste nicht anzeigen

Problem: Auf Webbrowsern wie Google Chrome, Mozilla Firefox und Microsoft Edge zeigt der **Treiber-Cache-Inspector** den letzten Eintrag in der Treiber-Cache-Liste nicht an.

Behelfslösung: Führen Sie die folgenden Schritte aus:

- 1 Erweitern Sie alle Cache-Einträge in der Liste mit dem Befehl **Aktionen > Alle erweitern** im Hauptmenü.
- 2 Navigieren Sie mit den Pfeiltasten auf der Tastatur zu einem erweiterten Eintrag in der Liste.

6.4.6 Remedy-Treiber wird beim lokalen Ausführen mit der Identity Manager-Engine nicht gestartet

Problem: Wenn der Treiber für die lokale Ausführung mit der Identity Manager-Engine konfiguriert ist, kann der Treiber aufgrund von Konflikten der JAXB-API in der Datei `activemq-all-5.15.2.jar` nicht gestartet werden. Im Trace wird die folgende Fehlermeldung eingetragen:

```
com.sun.xml.internal.ws.spi.db.DatabindingException: Unknown JAXBContext
implementation: class com.sun.xml.bind.v2.runtime.JAXBContextImpl
```

Behelfslösung: Führen Sie die folgenden Schritte aus:

- 1 Installieren Sie den Treiber mit dem Remote Loader.
- 2 Entfernen Sie die Datei `activemq-all-5.15.2.jar` aus dem Ordner `lib` im Remote Loader-Installationsverzeichnis.
- 3 Starten Sie den Treiber.

6.5 Probleme mit Identitätsanwendungen

Sie haben bei Verwendung der Identitätsanwendungen mit dem Dashboard, dem Identitätsanwendungsadministrator und der Benutzeranwendung möglicherweise die folgenden Probleme:

- ♦ [Abschnitt 6.5.1, „Fehlermeldung, wenn verschiedene Datenbanken für Identitätsanwendungen und Identity Reporting \(auf demselben Server installiert\) konfiguriert sind“, auf Seite 35](#)
- ♦ [Abschnitt 6.5.2, „Für archivierte Protokolle aus der Datei „catalina.out“ wird trotz Protokoll-Rollover eine Dateigröße von Null angezeigt“, auf Seite 35](#)
- ♦ [Abschnitt 6.5.3, „Auf der Seite zum Entziehen von Berechtigungen werden fälschlicherweise die Berechtigungen anderer Benutzer für den Rollenadministrator und den Administrator für delegierte Rollen angezeigt“, auf Seite 36](#)
- ♦ [Abschnitt 6.5.4, „Das Dashboard zeigt eine falsche Gesamtanzahl der Benutzer an“, auf Seite 37](#)

- Abschnitt 6.5.5, „Das Popup-Fenster zeigt möglicherweise Inhalte in unterschiedlichen Browser- und Client-Standardsprachen an“, auf Seite 37
- Abschnitt 6.5.6, „Anforderungs- und Genehmigungs-Workflow-Formulare weisen rechtsbündige Feldbezeichnungen auf“, auf Seite 37
- Abschnitt 6.5.7, „CLE-beschränkter Browser blockiert den Zugriff auf die Seite "Passwort vergessen"“, auf Seite 37
- Abschnitt 6.5.8, „Eine Rollenanforderung kann genehmigt oder abgelehnt werden, nachdem die Rolle gelöscht wurde“, auf Seite 38
- Abschnitt 6.5.9, „Das Erstellen und Kopieren des Basispakets für die Benutzeranwendungstreiber verursacht einen Fehler im rollenbasierten Bereitstellungsmodul“, auf Seite 38
- Abschnitt 6.5.10, „Ein Passwort für ein Benutzeranwendungskonto darf nicht mit dem Zeichen „<“ beginnen“, auf Seite 38
- Abschnitt 6.5.11, „Workflows melden einen Fehler bei Verwendung von „dateToString“ zur Zeitstempelkontrolle“, auf Seite 38
- Abschnitt 6.5.12, „Die Navigationselemente der Benutzeranwendung werden mit Safari auf einem iPad nicht angezeigt“, auf Seite 39
- Abschnitt 6.5.13, „Benutzerdefiniertes CSS wird nicht mit den Clusterknoten synchronisiert“, auf Seite 39
- Abschnitt 6.5.14, „„ClientAbortException“ beim Abmelden bei den Benutzeranwendungen unter Windows“, auf Seite 40
- Abschnitt 6.5.15, „Ändern des Passworts im Identity Manager-Dashboard nicht möglich“, auf Seite 40
- Abschnitt 6.5.16, „Standardmäßige Dashboard-Widgets laden nach dem Aufrüsten keine Widget-Informationen in das Dashboard“, auf Seite 40
- Abschnitt 6.5.17, „Schaltfläche „Abmelden“ im Dashboard funktioniert eventuell nicht“, auf Seite 41
- Abschnitt 6.5.18, „Untergeordnete Rolle durch Klicken auf Beschreibung oder Zuordnungsbeschreibung zum Löschen auswählen“, auf Seite 41

6.5.1 Fehlermeldung, wenn verschiedene Datenbanken für Identitätsanwendungen und Identity Reporting (auf demselben Server installiert) konfiguriert sind

Problem: Identity Manager unterstützt nicht die Verwendung unterschiedlicher Datenbanken für die Identitätsanwendungen und die Identity Reporting-Komponenten, die auf demselben Server installiert sind. Sie können beispielsweise nicht eine PostgreSQL-Datenbank für die Identitätsanwendungen auf einem Server verwenden und in Identity Reporting auf eine Oracle-Ferndatenbank verweisen. Dies führt zu Ausnahmen in der Datei `catalina_<Datum>.log`. (Bug 1079738)

Behelfslösung: Sollen unterschiedliche Datenbanken für die Identitätsanwendungen und Identity Reporting verwendet werden, installieren Sie die Komponenten auf separaten Servern.

6.5.2 Für archivierte Protokolle aus der Datei „catalina.out“ wird trotz Protokoll-Rollover eine Dateigröße von Null angezeigt

Problem: Es wird eine Archivdateigröße von Null angezeigt. (Bug 1044488)

Behelfslösung: Führen Sie die folgenden Schritte aus:

- 1 Halten Sie den Tomcat-Dienst an. Führen Sie beispielsweise den folgenden Befehl an einer Eingabeaufforderung aus:

```
systemctl stop netiq-tomcat.service
```

2 Wechseln Sie zum Verzeichnis Tomcat/conf. Beispiel: /opt/netiq/idm/apps/tomcat/conf.

3 Bearbeiten Sie die Datei userapp-log4j.xml in einem Texteditor.

3a Fügen Sie die nachfolgenden Einträge für Protokoll-Appender nach dem Abschnitt Catalina Appender ein.

```
<!-- catalina.out logrollover -->
<appender name="CATALINALOG"
class="org.apache.log4j.DailyRollingFileAppender">
  <param name="Append" value="true"/>
  <param name="DatePattern" value="'.'yyyy-MM-dd'.log'"/>
  <param name="Encoding" value="UTF-8"/>
  <param name="File" value="${catalina.base}/logs/catalina.out"/>
  <param name="Threshold" value="ALL"/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="%d [%p] %c{1} %m%n"/>
  </layout>
</appender>
```

3b Fügen Sie den Eintrag <appender-ref ref="CATALINALOG"/> in den Abschnitt <root> vor dem Abschnitt </log4j:configuration> ein.

Ein Beispiel für diesen Abschnitt:

```
<!-- ===== -->
<!-- Setup the Root category -->
<!-- ===== -->
<root>
  <level value="INFO"/>
  <appender-ref ref="CONSOLE"/>
  <appender-ref ref="IDAPPS"/>
  <appender-ref ref="CATALINALOG"/>
</root>
```

4 Starten Sie den Tomcat-Dienst.

6.5.3 Auf der Seite zum Entziehen von Berechtigungen werden fälschlicherweise die Berechtigungen anderer Benutzer für den Rollenadministrator und den Administrator für delegierte Rollen angezeigt

Problem: Wenn Sie sich als Rollenadministrator oder als Administrator für delegierte Rollen beim Dashboard anmelden, werden auf der Seite „Sonstige“ (**Zugriff > Berechtigungen > Berechtigungen zurückziehen > Sonstige**) die Benutzerberechtigungen angezeigt, die außerhalb Ihrer Domäne oder Ihres Bereichs liegen.

- Bei einem Rollenadministrator zeigt das Dashboard die Ressourcen von Benutzern an, die nicht zur Domäne des Administrators gehören.
- Bei einem Administrator für delegierte Rollen zeigt das Dashboard alle Ressourcen und Rollen von Benutzern an, die nicht delegiert sind. (Bug 1079043)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.5.4 Das Dashboard zeigt eine falsche Gesamtanzahl der Benutzer an

Problem: Die folgenden Probleme sind gemeldet:

- Wenn Sie Benutzer hinzufügen und die Ansicht sofort aktualisieren, werden im Dashboard die neuen Benutzer aufgeführt, doch die Gesamtanzahl der Benutzer wird nicht aktualisiert. Die aktualisierte Gesamtanzahl der Benutzer wird jedoch korrekt angezeigt, wenn Sie die Ansicht erst nach einigen Sekunden aktualisieren.
- Wenn ein Benutzer über mehrere Werte entweder für den `Nachnamen` oder für `sn` verfügt, zeigt das Dashboard verschiedene Werte für die Suchanzahl und die Gesamtanzahl an. (Bug 1006448)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.5.5 Das Popup-Fenster zeigt möglicherweise Inhalte in unterschiedlichen Browser- und Client-Standardsprachen an

Problem: Wenn Sie eine Aktion durchführen, die ein Popup-Fenster öffnet, zeigt das Dashboard möglicherweise einen Bereich des Fensters in der Sprache des Clients statt in der Sprache des Browsers an. Beispielsweise wird durch die Anzeige der Details für eine Aufgabe ein Popup-Fenster geöffnet. Dieses Problem tritt in Microsoft Internet Explorer- oder Edge-Browsern auf, nachdem der Benutzer die Sprache des Browsers zu einer Sprache geändert hat, die nicht der Sprache des Clients entspricht. (Bug 1019020)

Behelfslösung: Ändern Sie die Sprache des Browsers und schließen Sie die aktuelle Registerkarte. Öffnen Sie dann die neue Registerkarte, um sich beim Dashboard anzumelden.

6.5.6 Anforderungs- und Genehmigungs-Workflow-Formulare weisen rechtsbündige Feldbezeichnungen auf

Problem: Wenn Sie auf Anforderungs- und Genehmigungsformulare im Dashboard zugreifen, werden die Formularfeldbezeichnungen rechtsbündig ausgerichtet. (Bug 921403)

Behelfslösung: Fügen Sie dem Onload-Ereignis der einzelnen Formulare die folgende Anweisung hinzu, damit die Formularfeldbezeichnungen des Anforderungs- und Genehmigungs-Workflows linksbündig ausgerichtet werden:

```
$(".div.nv-formFieldLabel").parent().css("text-align", "left");
```

6.5.7 CLE-beschränkter Browser blockiert den Zugriff auf die Seite "Passwort vergessen"

Problem: Wenn Sie den Zugriff auf Websites beschränken, doch die Landeseite für die Identitätsanwendungen auf die weiße Liste setzen, blockiert der CLE-beschränkte Browser möglicherweise den Zugriff auf die Seite "Passwort vergessen" für SSPR (Self Service Password Reset). Benutzer sehen möglicherweise folgenden Fehler:

```
"Access is restricted to your Target Server"
```

(Bug 1021647)

Behelfslösung: Fügen Sie in der weißen Liste der Seite "Passwort vergessen" die URL hinzu.

Wenn Sie von Identity Manager 4.5 aufrüsten, aktualisieren Sie unter „SSPR-Umleitungs-URL“ den Link zur Landingpage, damit Benutzer zum neuen Dashboard (`/idmdash/#/Landeseite`) statt zur Identity Manager-Startseite (`/Landingpage`) weitergeleitet werden.

6.5.8 Eine Rollenanforderung kann genehmigt oder abgelehnt werden, nachdem die Rolle gelöscht wurde

Problem: Wenn ein Administrator eine Rolle löscht, für die ein Workflow erforderlich ist, nachdem ein Benutzer eine Rolle angefordert hat, sieht der Adressat des Workflows für die Rollenanforderung den Workflow immer noch in der Jobliste und kann die Anforderung genehmigen oder ablehnen. (Bug 752860)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.5.9 Das Erstellen und Kopieren des Basispakets für die Benutzeranwendungstreiber verursacht einen Fehler im rollenbasierten Bereitstellungsmodul

Problem: Wenn Sie bestimmte Vorgänge im Basispaket der Benutzeranwendung ausführen, z. B. ein Rollenkonfigurationsobjekt entfernen, tritt ein Fehler im rollenbasierten Bereitstellungsmodul auf. (Bug 879595)

Behelfslösung: NetIQ empfiehlt, das Basispaket des Benutzeranwendungstreibers nicht zu erstellen oder zu kopieren.

6.5.10 Ein Passwort für ein Benutzeranwendungskonto darf nicht mit dem Zeichen „<“ beginnen

Problem: Das Sonderzeichen „<“ darf nicht als erstes Zeichen in einem Passwort für die Benutzeranwendung verwendet werden. Beispiel: <testing12. Der Browser interpretiert das Passwort als falsch formatierten HTML-Text, sodass sich der Benutzer nicht anmelden kann. (Bug 759297)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.5.11 Workflows melden einen Fehler bei Verwendung von „dateToString“ zur Zeitstempelkontrolle

Problem: Workflows, die Sie in der Benutzeranwendung erstellt haben und die die Formularskriptmethode `dateToString` für einen Zeitstempel verwenden, funktionieren auf der Identity Manager-Startseite nicht ordnungsgemäß. Das Formularskript `dateToString` in der API enthält Sekunden, das neue Datum/Zeit-Steuerelement auf der Identity Manager-Startseite hingegen nicht. Das neue Skript verwendet ein anderes Format. Um sicherzustellen, dass Ihre Formulare mit der Identity Manager-Startseite funktionieren, müssen Sie `dateToString` durch das neue Skript ersetzen: `new Date().toString('Date.CultureInfo.formatPatterns.shortDate+' + Date.CultureInfo.formatPatterns.shortTime')`.

Behelfslösung: Sie können den folgende Code verwenden, um das Steuerelement für ein einzelnes Datum in Ihrem Formular zu ersetzen:

```
document.getElementById('%Field-Name').value = new
Date().toString('Date.CultureInfo.formatPatterns.shortDate+'
'+Date.CultureInfo.formatPatterns.shortTime');
```

Sie müssen jedoch möglicherweise Steuerelemente ersetzen, die zwei Datumsangaben darstellen. Beispielsweise kann es für ein Formular erforderlich sein, dass der Benutzer ein Start- und ein Enddatum für eine Berechtigungsanforderung angibt.

Verwenden Sie den folgenden Code, um den Wert `startDate` festzulegen:

```
document.getElementById('_startDate').value = new
Date().toString('Date.CultureInfo.formatPatterns.shortDate+'
"+Date.CultureInfo.formatPatterns.shortTime');
```

Verwenden Sie den folgenden Code, um einen Wert `endDate` festzulegen, der drei Tage nach dem Startdatum liegt.

```
var s = new Date().getTime();
s = s + 3 * 1000 * 24 * 60 * 60;
document.getElementById('_furDate').value = new
Date(s).toString('Date.CultureInfo.formatPatterns.shortDate+'
"+Date.CultureInfo.formatPatterns.shortTime');
```

In diesem Beispiel gibt der Workflow folgende Informationen zurück:

```
startDate: 3/14/2014 12:03 PM
endDate: 3/17/2014 12:03 PM
```

HINWEIS: Wenn Sie in den oben genannten Codes in Ihrem Formular nur **DatePicker** verwenden möchten, schließen Sie `'Date.CultureInfo.formatPatterns.shortTime'` vom Code aus.

Beispiel: Wenn Sie für `startDate` nur das Datum angeben möchten, verwenden Sie folgenden Codetyp:

```
document.getElementById('_startDate').value = new
Date().toString('Date.CultureInfo.formatPatterns.shortDate');
```

6.5.12 Die Navigationselemente der Benutzeranwendung werden mit Safari auf einem iPad nicht angezeigt

Problem: Wenn Sie die Benutzeranwendung mit Safari auf einem iPad ausführen, das das Hochformat verwendet, werden die Navigationselemente in der Kopfzeile nicht immer ordnungsgemäß angezeigt.

Behelfslösung: Um das Navigationselement in der Kopfzeile anzuzeigen, wählen Sie das Element links aus.

6.5.13 Benutzerdefiniertes CSS wird nicht mit den Clusterknoten synchronisiert

Problem: Wenn Sie das benutzerdefinierte CSS über das Identity Manager-Dashboard in den Cluster hochladen, werden die CSS-Änderungen nicht auf allen Clusterknoten angewendet. (1025836)

Behelfslösung: Speichern Sie auf allen Knoten im Cluster jeweils dieselbe CSS-Kopie im folgenden Speicherort:

```
<user home directory>/netiq_custom_css
```

6.5.14 „ClientAbortException“ beim Abmelden bei den Benutzeranwendungen unter Windows

Problem: Wenn Sie versuchen, die Benutzer entweder mit **Identity Manager-Dashboard > Personen > Benutzer** oder mit **Benutzer verwalten** aufzulisten, und sich dann bei den Identitätsanwendungen abmelden, bevor das Dashboard die Gesamtanzahl der Benutzer im Browser anzeigt, entsteht die Ausnahme `ClientAbortException` in der Datei `catalina.out`. Diese Ausnahme kann auch in den folgenden Fällen bei der Arbeit mit den Identitätsanwendungen auftreten:

- ♦ Das Browserfenster wird geschlossen.
- ♦ Das Netzwerk wird getrennt.
- ♦ Bei der Sitzung ist eine Zeitüberschreitung eingetreten.

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen. Sie können diese Ausnahme ignorieren, da sie sich nicht auf die Funktionalität auswirkt.

6.5.15 Ändern des Passworts im Identity Manager-Dashboard nicht möglich

Problem: Wenn Sie SSPR und die Identitätsanwendungen auf separaten Servern installiert haben und dann versuchen, das Passwort auf der Seite **Anwendungen** zu ändern, zeigen die Identitätsanwendungen den Fehler `Seite nicht gefunden an`. (Bug 1077395)

Behelfslösung: Geben Sie die Netzwerk-IP-Adresse des SSPR-Servers unter **Passwort ändern** auf der Seite **Anwendungen** an.

- 1 Melden Sie sich als Administrator bei Ihrem Identity Manager-Dashboard an.

`https://<IP-Adresse_der_Identitätsanwendungen:Port>/idmdash`

- 2 Wählen Sie **Anwendungen** und klicken Sie auf .

- 3 Klicken Sie unter **Passwort ändern** auf .

- 4 Geben Sie unter **Link** die Adresse des SSPR-Servers an.

`https://<SSPR-IP-Adresse:Port>/sspr/private/ChangePassword`

- 5 Klicken Sie auf **Speichern**.

6.5.16 Standardmäßige Dashboard-Widgets laden nach dem Aufrüsten keine Widget-Informationen in das Dashboard

Problem: Wenn Sie einen anderen Kontextnamen definiert haben (also nicht `IDMProv`), können die standardmäßigen Dashboard-Widgets, die auf REST-APIs zugreifen, keine Widget-Informationen aus den Identitätsanwendungen abrufen. (Bug 1080591)

Behelfslösung: Ändern Sie den Kontextnamen für die Widgets, die auf REST-APIs zugreifen:

- 1 Klicken Sie im **Dashboard** auf  und wählen Sie **Widgets**.

- 2 Klicken Sie in einem Widget, dessen Kontextname geändert werden soll, auf .

- 3 Ersetzen Sie unter **URL** den Eintrag `/IDMProv` durch `<definierter Kontextname>`.

In der nachfolgenden URL

```
/IDMProv/rest/access/assignments/  
advanced?nextIndex=1&sortBy=name&sortOrder=ASC&forceRefresh=true&searchScope=r  
ole&size=20
```

ersetzen Sie beispielsweise `/IDMProv` durch `/IDMProv_new`.

6.5.17 Schaltfläche „Abmelden“ im Dashboard funktioniert eventuell nicht

Problem: Unter bestimmten Umständen gelangen Sie mit der Schaltfläche „Abmelden“ im Dashboard nicht zur Anmeldeseite zurück. (Bug 1082178)

Behelfslösung: Führen Sie einen der folgenden Schritte aus:

- 1 Aktualisieren Sie die Dashboard-Seite.
- 2 Navigieren Sie zu einer anderen Anwendung (z. B. Rollenadministration oder IDMPProv) und melden Sie sich über deren Anwendungsseite ab.

6.5.18 Untergeordnete Rolle durch Klicken auf Beschreibung oder Zuordnungsbeschreibung zum Löschen auswählen

Problem: In der neuen Benutzeroberfläche der Identitätsanwendungen wird die Liste der übergeordneten und untergeordneten Rollen auf der Seite „Rollendetails“ angezeigt. Auf der Seite können Sie eine untergeordnete Rolle nicht durch einfaches Markieren des Namens auswählen. Stattdessen werden Kurzinformationen zur betreffenden untergeordneten Rolle eingeblendet. (Bug 1082533)

Behelfslösung: Zum Löschen einer untergeordneten Rolle klicken Sie auf die zugehörige Beschreibung oder Zuordnungsbeschreibung. Sollen mehrere untergeordnete Rollen gelöscht werden, halten Sie die `Strg`-Taste auf der Tastatur gedrückt und klicken Sie nacheinander auf die Beschreibung oder Zuordnungsbeschreibung der gewünschten Rollen.

6.6 Probleme mit der Identitätsberichterstellung

Bei Verwendung der Identitätsberichterstellung treten möglicherweise die folgenden Probleme auf:

- [Abschnitt 6.6.1, „Die Häufigkeit von Zeitplänen kann nicht geändert werden“, auf Seite 41](#)
- [Abschnitt 6.6.2, „Identitätsanwendungen können nicht über die Seiten von Identity Reporting und Identity Data Collection Services gestartet werden“, auf Seite 41](#)
- [Abschnitt 6.6.3, „Hilfeseite zur Datenerfassung in nichtenglischen Sprachen wird zur englischen Hilfeseite weitergeleitet“, auf Seite 42](#)
- [Abschnitt 6.6.4, „Seite „Identity Manager Data Collection Services“ wird in der Standard Edition unter Linux nicht angezeigt“, auf Seite 42](#)

6.6.1 Die Häufigkeit von Zeitplänen kann nicht geändert werden

Problem: Sie können die Häufigkeit von Zeitplänen nicht ändern. Beispiel: Monat statt Woche. (Bug 677430)

Behelfslösung: Zum Ändern der Häufigkeit, löschen Sie den Zeitplan und erstellen Sie einen neuen.

6.6.2 Identitätsanwendungen können nicht über die Seiten von Identity Reporting und Identity Data Collection Services gestartet werden

Problem: Dieses Problem tritt nach dem Aufrüsten von Identity Manager auf die aktuelle Version auf. Wenn Sie in der Benutzeroberfläche von Identity Reporting oder Identity Data Collection Services auf [Startseite](#) klicken und diese nicht auf demselben Server wie die Identitätsanwendungen installiert sind, werden die Identitätsanwendungen nicht gestartet. Stattdessen wird der Fehler Seite nicht gefunden angezeigt. (Bug 1080514)

Behelfslösung: Ändern Sie die Portalseiten-URL für Identity Reporting. Aktualisieren Sie hierzu das configupdate-Dienstprogramm manuell mit der URL des Identity Manager-Dashboards:

- 1 Starten Sie das configupdate-Dienstprogramm.

Standardmäßig befindet sich dieses Dienstprogramm im Verzeichnis /opt/netiq/idm/apps/configupdate

- 2 Wählen Sie **SSO-Clients > Berichterstellung**.

- 3 Geben Sie unter **URL-Link zur Portalseite** die URL des Identity Manager-Dashboards an.

Beispiel: `https://<Netzwerk-IP-Adresse_der_Identitätsanwendungen:Port>/idmdash/#/landing`

| Berichterstellung | |
|---------------------------------|---|
| OAuth-Client-ID | <input type="text" value="rpt"/> |
| OAuth-Client-Geheimnis | <input type="password" value="....."/> |
| URL-Link zur Portalseite | <input type="text" value="https://192.168.0.2:8443/idmdash/#/landing"/> |
| URL-Link zu Identity Governance | <input type="text"/> |
| OSP-OAuth-Umleitungs-URL | <input type="text" value="https://192.168.0.1:8543/IDMRPT/oauth.html"/> |

So ändern Sie die Portalseiten-URL für Identity Manager Data Collection Services:

- 1 Öffnen Sie die Datei `ism-configuration.properties` im Texteditor aus /opt/netiq/idm/apps/tomcat/conf.

- 2 Hängen Sie die Portalseiten-URL an den folgenden Text an:

```
com.netiq.idmdcs.landing.url = https://<Identity Applications network IP address:Port>/idmdash/#/landing
```

Beispiel:

```
com.netiq.idmdcs.landing.url = https://192.168.0.2:8443/idmdash/#/landing
```

- 3 Starten Sie Tomcat neu.

Wenn Sie mit der Standard Edition arbeiten, die die Identitätsanwendungen nicht enthält, können Sie dieses Problem ignorieren. Dieses Problem wirkt sich nicht auf die Funktionalität in Standard Edition-Installationen aus.

6.6.3 Hilfeseite zur Datenerfassung in nichtenglischen Sprachen wird zur englischen Hilfeseite weitergeleitet

Problem: Wenn Sie Data Collection Services in einem nichtenglischen Gebietsschema installieren und dann auf der Seite „Data Collection Services“ auf das Symbol **Hilfe** klicken, gelangen Sie zur englischsprachigen Hilfe. (Bug 1082987)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.6.4 Seite „Identity Manager Data Collection Services“ wird in der Standard Edition unter Linux nicht angezeigt

Problem: Nach dem Installieren und Konfigurieren von Identity Reporting in der Standard Edition wird die Seite „Identity Manager Data Collection Services“ nicht angezeigt. (Bug 1082564)

Behelfslösung: Wählen Sie beim Konfigurieren von Identity Reporting die Option **Nein (N)** an der folgenden Eingabeaufforderung:

Möchten Sie eine Verbindung zu einem externen One SSO-Server herstellen (J/N)?

6.7 Probleme mit iManager-Plugins

Bei Verwendung von iManager treten möglicherweise die folgenden Probleme auf:

- ♦ [Abschnitt 6.7.1, „Ausnahmefehler unter Windows 2016 bei Verwendung von KMO“, auf Seite 43](#)
- ♦ [Abschnitt 6.7.2, „Abhängigkeit vom Assistenten für NDS-zu-NDS-Treiberzertifikate“, auf Seite 43](#)
- ♦ [Abschnitt 6.7.3, „Einige Aktionen sind im Richtlinien-Builder-Plugin nicht verfügbar“, auf Seite 43](#)

6.7.1 Ausnahmefehler unter Windows 2016 bei Verwendung von KMO

Problem: Wenn Sie ein CA-Zertifikat in einem .b64-Format aus iManager exportieren, wird am Ende des Zertifikats eine leere Zeile eingefügt. Damit wird das Zertifikat ungültig. (Bug 1018732)

Behelfslösung: Entfernen Sie die leere Zeile manuell aus dem Zertifikat.

6.7.2 Abhängigkeit vom Assistenten für NDS-zu-NDS-Treiberzertifikate

Problem: iManager benötigt den Assistenten für NDS-zu-NDS-Treiberzertifikate, um ordnungsgemäß zu funktionieren.

Behelfslösung: Um den Assistenten für NDS-zu-NDS-Treiberzertifikate zu verwenden, laden Sie das iManager Plugin für den NetIQ Certificate Server herunter und installieren Sie es.

6.7.3 Einige Aktionen sind im Richtlinien-Builder-Plugin nicht verfügbar

Problem: Diese Version unterstützt nicht die Erstellung der folgenden Aktionen anhand des Richtlinien-Builders in iManager. (Bug 1018354)

- ♦ Rolle erstellen
- ♦ Ressource erstellen
- ♦ Ressource hinzufügen
- ♦ Ressource entfernen
- ♦ XDAS-Ereignis generieren

Behelfslösung: Erstellen Sie diese Aktionen mit dem Richtlinien-Builder in Designer.

6.8 Probleme beim Aufrüsten von Identity Manager

- ♦ [Abschnitt 6.8.1, „Die vorhandene Datensynchronisierungsrichtlinie wird nach dem Aufrüsten von Identity Manager 4.6.x auf 4.7 nicht auf der Seite „Data Collection Services“ angezeigt“, auf Seite 44](#)
- ♦ [Abschnitt 6.8.2, „Aufrüsten von Identity Manager-Komponenten in einer dezentralen Umgebung“, auf Seite 44](#)
- ♦ [Abschnitt 6.8.3, „In der Fortschrittsanzeige werden Verzeichnisnamen bestimmter Komponenten bei der Aufrüstung unter Windows abgeschnitten“, auf Seite 45](#)
- ♦ [Abschnitt 6.8.4, „Aufrüstungsvorgang schlägt wegen fehlender Portwerte in der URL fehl“, auf Seite 45](#)

6.8.1 Die vorhandene Datensynchronisierungsrichtlinie wird nach dem Aufrüsten von Identity Manager 4.6.x auf 4.7 nicht auf der Seite „Data Collection Services“ angezeigt

Problem: Wenn Sie auf Sentinel 8.1.1 und Identity Reporting 4.7 aufrüsten, wird die vorhandene Datensynchronisierungsrichtlinie nicht auf der Seite „Data Collection Services“ angezeigt. (Bug 1080081)

Behelfslösung: Führen Sie nach dem Aufrüsten von Sentinel die folgenden Schritte aus:

- 1 Löschen Sie die Datensynchronisierungsrichtlinie.
 - ♦ Wenn Sie von Sentinel 8.0.1 (oder früher) aufgerüstet haben, löschen Sie die Datensynchronisierungsrichtlinie aus Sentinel und löschen Sie die Tabelle „sentinel_events“ aus der Berichterstellungsdatenbank. Melden Sie sich bei der PostgreSQL-Datenbank an und löschen Sie die Tabelle „sentinel_events“ aus dem öffentlichen Schema. Beim Aktualisieren von Sentinel werden Daten aus der Tabelle „sentinel_events“ entfernt. Melden Sie sich mit **Sentinel > Speicher > Datensynchronisierung** an, wählen Sie die Richtlinie aus und klicken Sie auf **Löschen**. Melden Sie sich bei der Berichterstellungsdatenbank an und löschen Sie die Tabelle „sentinel_events“ aus dem öffentlichen Schema.
 - ♦ Wenn Sie eine Version von Sentinel 8.1 aufgerüstet haben, löschen Sie lediglich die Datensynchronisierungsrichtlinie. Melden Sie sich mit **Sentinel > Speicher > Datensynchronisierung** an, wählen Sie die Richtlinie aus und klicken Sie auf **Löschen**.
- 2 Öffnen Sie die Seite „Data Collection Services“ und wählen Sie **Einstellungen > Datensynchronisierung > Datensynchronisierungsrichtlinien**.
- 3 Klicken Sie zum Hinzufügen einer neuen Richtlinie auf **Neue Richtlinie**.
- 4 Geben Sie auf der Seite „Neue Datensynchronisierungsrichtlinie“ die Details zu Sentinel und zum Datenbankserver an.
- 5 Soll die Nutzlast für die zu erstellende Richtlinie konfiguriert werden, klicken Sie auf **Erweiterte anzeigen**.
- 6 Klicken Sie auf **Erstellen**.

6.8.2 Aufrüsten von Identity Manager-Komponenten in einer dezentralen Umgebung

Problem 1: OSP und SSPR sind auf separaten Servern in der dezentralen Umgebung installiert.

Beim Aufrüsten wird die nicht standardmäßige Datei `oauth-keystore.file` (z. B. `idmnew.jks`) durch den Standard-Dateinamen (`osp.jks`) ersetzt. (Bug 1081968)

Behelfslösung: Ersetzen Sie die Standarddatei nach dem Aufrüsten wie folgt durch die nicht standardmäßige Datei:

- 1 Starten Sie das Dienstprogramm **Konfigurationsaktualisierung**.
- 2 Blättern Sie auf der Registerkarte **Authentifizierung** zum Abschnitt **Authentifizierungskonfiguration**.
- 3 Ersetzen Sie in der **OAuth-Keystore**-Datei den Pfad zur JKS-Keystore-Datei durch die nicht standardmäßige Datei (z. B. `idmnew.jks`). Diese Datei befindet sich im Sicherungsordner von OSP.
- 4 Geben Sie unter **Passwort für OAuth-Keystore-Datei** das Passwort an, mit dem die nicht standardmäßige OAuth-Keystore-Datei geladen wird.

Problem 2: Identity Manager ist für die Authentifizierung bei NetIQ Access Manager konfiguriert und Sie haben Drittanbieter-Zertifikate in das Tomcat-Verzeichnis `cacerts` importiert.

Behelfslösung: Importieren Sie die Drittanbieter-Zertifikate erneut in den Keystore `idm.jks`. Dieser Schritt ist erforderlich, da Tomcat in Identity Manager 4.7 auf den Keystore `idm.jks` zurückgreift. Wenn Identity Manager beispielsweise für die Authentifizierung über Access Manager konfiguriert ist, importieren Sie das Access Manager-Zertifikat in `idm.jks`.

6.8.3 In der Fortschrittsanzeige werden Verzeichnisnamen bestimmter Komponenten bei der Aufrüstung unter Windows abgeschnitten

Problem: Beim Aufrüsten von OSP, SSPR und der Identitätsanwendungen werden die Installationsverzeichnisnamen dieser Komponenten in der Fortschrittsanzeige abgeschnitten.

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6.8.4 Aufrüstungsvorgang schlägt wegen fehlender Portwerte in der URL fehl

Problem: Wenn im Parameter **OSP-OAuth-Umleitungs-URL** keine Portnummern für die einzelnen Identitätsanwendungen angegeben werden, schlägt der Aufrüstungsvorgang fehl.

Behelfslösung: Tragen Sie die Portnummern manuell in das Konfigurationsaktualisierungsprogramm ein, bevor Sie das Aufrüstungsprogramm starten. So geben Sie die Portwerte an:

- 1 Starten Sie das Dienstprogramm **Konfigurationsaktualisierung**.
- 2 Geben Sie auf der Registerkarte **SSO-Clients** die entsprechenden Portwerte für alle erforderlichen URLs an.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`

Beispiel: `http://192.0.2.0:80/dash`

6.9 Lokalisierungsprobleme

- ♦ [Abschnitt 6.9.1, „Identity Manager installiert bestimmte Treiber nicht in den nicht-englischen Gebietsschemata“, auf Seite 45](#)
- ♦ [Abschnitt 6.9.2, „Die Installationsprogramme von Identity Manager enthalten nicht korrekt angezeigte Zeichen im Konsolenmodus unter Windows“, auf Seite 46](#)
- ♦ [Abschnitt 6.9.3, „Einige Komponenten-Installationsprogramme sind nicht lokalisiert“, auf Seite 46](#)
- ♦ [Abschnitt 6.9.4, „Bei der PostgreSQL-Installation unter Windows tritt ein Fehler auf, wenn das Postgres-Benutzerpasswort in russischer Sprache angegeben wird“, auf Seite 47](#)

6.9.1 Identity Manager installiert bestimmte Treiber nicht in den nicht-englischen Gebietsschemata

Problem: Wenn Sie die ausgewählten Treiber anhand der Option **Ausgewählte Komponenten anpassen** in nicht-englischen Gebietsschemata installieren, wird die Installation nicht durchgeführt. (Bug 926490)

Behelfslösung: Führen Sie einen der folgenden Schritte durch:

- ♦ Wählen Sie für die Installation von Identity Manager Englisch als Sprache aus, keine nichtenglischen Sprachen.

- ♦ Kopieren Sie unter Windows die erforderlichen JAR-Dateien vom Installationsmedium in den Identity Manager-Installationsordner. Navigieren Sie unter Linux zu `products/IDM/linux/setup/packages` im Installationsmedium und führen Sie folgendes Kommando aus:
 - ♦ **Neueinstallation:** `rpm -ivf <Dateiname>`
 - ♦ **Upgrade:** `rpm -Uvf <Dateiname>`

6.9.2 Die Installationsprogramme von Identity Manager enthalten nicht korrekt angezeigte Zeichen im Konsolenmodus unter Windows

Problem: Wenn Sie brasilianisches Portugiesisch, Dänisch, Niederländisch, Englisch, Französisch, Deutsch, Italienisch, Schwedisch, Spanisch oder Russisch als Installationssprache für Identity Manager auswählen, werden während der Installation einige Zeichen auf dem Bildschirm nicht korrekt dargestellt.

Wenn Sie Englisch als Installationssprache wählen, wird auf der Seite *Sprache auswählen* des Installationsprogramms ein Zeichen nicht korrekt angezeigt. Unter der asiatischen Windows-Version werden die Zeichen der asiatischen Sprachen jedoch ordnungsgemäß wiedergegeben. (Bug 672070)

Behelfslösung: Damit die Zeichen ordnungsgemäß dargestellt werden, führen Sie auf Ihrem Windows-Computer vor der Installation von Identity Manager die folgenden Schritte zum Ändern der Standardschrift in „Lucida Console“ aus:

- 1 Wählen Sie **Start > Ausführen > Regedit > HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage** und ändern Sie den Wert für **OEMCP** von **850** in **1252**.
Für Russisch ändern Sie den Wert **OEMCP** von **866** in **1251** im Verzeichnis `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage`.
- 2 Wählen Sie **Start > Ausführen** und geben Sie `cmd` in das Textfeld **Öffnen** ein. Drücken Sie anschließend die Eingabetaste, um das Eingabeaufforderungsfenster zu öffnen.
- 3 Klicken Sie mit der rechten Maustaste auf die Titelleiste des Eingabeaufforderungsfensters, um das Popup-Menü zu öffnen.
- 4 Wählen Sie im Popup-Menü die Option **Standardwerte** aus. Das Dialogfeld „Eigenschaften“ des Eingabeaufforderungsfensters wird angezeigt.
- 5 Klicken Sie auf die Registerkarte **Schriftart** und ändern Sie die Standardschrift von **Rasterschriftart** in **Lucida Console (TrueType)**.
- 6 Klicken Sie auf **OK**.
- 7 Führen Sie einen Neustart des Computers durch.

6.9.3 Einige Komponenten-Installationsprogramme sind nicht lokalisiert

Problem: In dieser Version sind keine lokalisierten Versionen des zusätzlichen Installationsprogramms für Apache Tomcat und PostgreSQL sowie für OSP und die Identitätsberichterstellung verfügbar. Führen Sie diese Komponenten-Installationsprogramme ausschließlich in englischer Sprache aus. (Bug 1008039)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen. Wählen Sie für die Installation von Identity Manager **Englisch** als Sprache aus, keine nichtenglischen Sprachen.

6.9.4 Bei der PostgreSQL-Installation unter Windows tritt ein Fehler auf, wenn das Postgres-Benutzerpasswort in russischer Sprache angegeben wird

Problem: Das PostgreSQL-Installationsprogramm akzeptiert keine russischen Passwörter für den Datenbankadministrator (**Passwort für Admin-Benutzer**). (Bug 1075752)

Behelfslösung: Geben Sie das Passwort in englischer Sprache an.

6.10 Probleme bei der Deinstallation

- ♦ [Abschnitt 6.10.1, „Bei der Deinstallation von Identity Manager Framework unter Windows werden nicht alle Ordner aus dem Installationsverzeichnis entfernt“, auf Seite 47](#)
- ♦ [Abschnitt 6.10.2, „Die Protokolldateien der Deinstallation von Identity Manager Framework werden unter Windows nicht im Deinstallationsordner abgelegt“, auf Seite 47](#)
- ♦ [Abschnitt 6.10.3, „Deinstallieren des Identity Manager-Eintrags in der Systemsteuerung nach Aufrüstung der Identity Manager-Engine unter Windows“, auf Seite 47](#)
- ♦ [Abschnitt 6.10.4, „Während der Deinstallation wird eine falsche Meldung angezeigt“, auf Seite 48](#)

6.10.1 Bei der Deinstallation von Identity Manager Framework unter Windows werden nicht alle Ordner aus dem Installationsverzeichnis entfernt

Problem: Das Deinstallationsprogramm entfernt die JAR-Dateien nicht aus dem Verzeichnis lib. (Bug 643077)

Behelfslösung: Entfernen Sie die JAR-Dateien manuell aus dem Verzeichnis lib.

6.10.2 Die Protokolldateien der Deinstallation von Identity Manager Framework werden unter Windows nicht im Deinstallationsordner abgelegt

Problem: Die Protokolldateien der Deinstallation werden im temp-Verzeichnis erstellt. (Bug 613225)

Behelfslösung: Diese Meldungen wirken sich nicht auf die Funktionalität aus. Dieses Problem können Sie ignorieren.

6.10.3 Deinstallieren des Identity Manager-Eintrags in der Systemsteuerung nach Aufrüstung der Identity Manager-Engine unter Windows

Problem: Wenn Sie das Deinstallationsprogramm nach dem Aufrüsten der Identity Manager-Engine auf Version 4.5 in der Systemsteuerung ausführen, werden die notwendigen Identity Manager-Dateien bis auf einen bestimmten Registrierungsschlüssel erfolgreich entfernt. Dieser Registrierungsschlüssel führt dazu, dass der Identity Manager-Eintrag auch nach der Deinstallation in der Systemsteuerung angezeigt wird. (Bug 901219)

Behelfslösung: Löschen Sie den Registrierungsschlüssel bei der Deinstallation im folgenden Registrierungspfad:

- ♦ **Für 32-Bit-Computer:**

`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Identity Manager`

- ♦ **Für 64-Bit-Computer:**

`\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Identity Manager`

6.10.4 Während der Deinstallation wird eine falsche Meldung angezeigt

Problem: Während der Deinstallation zeigt das Programm die Meldung „InstallAnywhere is preparing to install..." (InstallAnywhere bereitet die Installation vor...) an, obwohl das Programm eigentlich deinstalliert wird.

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

7 Kontaktangaben

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Sie haben Verbesserungsvorschläge? Dann senden Sie sie uns per Email an Documentation-Feedback@netiq.com (<mailto:Documentation-Feedback@netiq.com>). Wir freuen uns auf Ihre Rückmeldung.

Ausführliche Kontaktinformationen finden Sie auf der [Website mit den Support-Kontaktangaben](http://www.netiq.com/support/process.asp#phone) (<http://www.netiq.com/support/process.asp#phone>).

Allgemeine Informationen zu unserem Unternehmen und unseren Produkten finden Sie auf der [NetIQ-Firmenwebsite](http://www.netiq.com/) (<http://www.netiq.com/>).

Werden Sie Mitglied in unserer [Community](https://www.netiq.com/communities/) (<https://www.netiq.com/communities/>), und führen Sie interaktive Gespräche mit Fachkollegen und NetIQ-Experten. In der NetIQ-Online-Community finden Sie Produktinformationen, Links zu nützlichen Ressourcen, Blogs und Social-Media-Kanäle.

8 Rechtliche Hinweise

Informationen zu rechtlichen Hinweisen, Marken, Haftungsausschlüssen, Gewährleistungen, Ausführbeschränkungen und sonstigen Nutzungseinschränkungen, Rechten der US-Regierung, Patentrichtlinien und Erfüllung von FIPS finden Sie unter <https://www.netiq.com/company/legal/>.

Copyright © 2018 NetIQ Corporation. Alle Rechte vorbehalten.