

Notes de version de NetIQ Identity Manager 4.7

Mars 2018



NetIQ Identity Manager 4.7 offre de nouvelles fonctions et améliorations ainsi qu'une plus grande convivialité et résout divers problèmes des versions précédentes.

La plupart de ces améliorations ont été apportées en réponse directe aux suggestions de nos clients. Nous vous remercions pour votre temps et pour vos commentaires très utiles. Nous espérons que cette collaboration se poursuivra et que nos produits continueront de répondre à tous vos besoins. Vous pouvez publier vos commentaires sur notre site Web des [forums de la communauté Identity Manager](#). Vous y trouverez également des notifications de produit, des blogues et des groupes d'utilisateurs de produits.

Pour plus d'informations sur les nouveautés des versions précédentes, consultez la section « Previous Releases » (Versions précédentes) sur le [site Web de documentation d'Identity Manager](#).

Pour plus d'informations sur cette version et pour consulter les dernières notes de version, rendez-vous sur la [page de documentation](#). Pour télécharger ce produit, rendez-vous sur le [site Web du produit Identity Manager](#).

- ♦ [Section 1, « Nouveautés et changements », page 1](#)
- ♦ [Section 2, « Versions des composants Identity Manager », page 19](#)
- ♦ [Section 3, « Configuration système requise », page 19](#)
- ♦ [Section 4, « Installation de NetIQ Identity Manager 4.7 », page 19](#)
- ♦ [Section 5, « Mise à niveau vers NetIQ Identity Manager 4.7 », page 23](#)
- ♦ [Section 6, « Problèmes connus », page 27](#)
- ♦ [Section 7, « Coordonnées », page 48](#)
- ♦ [Section 8, « Mentions légales », page 48](#)

1 Nouveautés et changements

Les sections suivantes décrivent les principales caractéristiques et fonctions de cette version, ainsi que celles qui ont été supprimées du produit. Elles abordent également les problèmes résolus dans cette version :

- ♦ [Section 1.1, « Nouvelles fonctionnalités », page 2](#)
- ♦ [Section 1.2, « Prise en charge des systèmes d'exploitation », page 6](#)
- ♦ [Section 1.3, « Versions des composants dépendants », page 6](#)
- ♦ [Section 1.4, « Problèmes résolus », page 7](#)
- ♦ [Section 1.5, « Correction de vulnérabilités logicielles », page 16](#)
- ♦ [Section 1.6, « Fonctions modifiées, abandonnées ou discontinuées », page 17](#)
- ♦ [Section 1.7, « Guides d'installation distincts pour les plates-formes Windows et Linux », page 18](#)

- ♦ [Section 1.8, « L'accord de licence de l'utilisateur final n'est pas disponible dans toutes les langues prises en charge », page 18](#)
- ♦ [Section 1.9, « NetIQ Corporation ne fournit aucun support pour les composants de l'installation PostgreSQL et Tomcat », page 18](#)

1.1 Nouvelles fonctionnalités

La version 4.7 d'Identity Manager propose des fonctionnalités clés, des améliorations ainsi que les correctifs suivants :

- ♦ [Section 1.1.1, « Installation simplifiée sur les plates-formes Linux », page 2](#)
- ♦ [Section 1.1.2, « Fonction d'audit uniforme », page 2](#)
- ♦ [Section 1.1.3, « Support étendu du canal du service Abonné pour les nouveaux pilotes », page 3](#)
- ♦ [Section 1.1.4, « Simplification des services d'actualisation des autorisations », page 3](#)
- ♦ [Section 1.1.5, « Modification de l'accès aux services de collecte de données d'Identity Manager », page 4](#)
- ♦ [Section 1.1.6, « Nouvelles fonctionnalités et améliorations des applications d'identité », page 4](#)
- ♦ [Section 1.1.7, « Création de paquetages simplifiée pour les fichiers d'installation », page 6](#)

Pour plus d'informations sur les nouvelles fonctions de NetIQ Identity Manager Designer 4.7, reportez-vous aux [Notes de version de NetIQ Identity Manager Designer 4.7 \(en cours de rédaction\)](#).

À part la version mise à jour de Java, aucune nouvelle fonction n'a été ajoutée à NetIQ Identity Manager Analyzer 4.7. Pour plus d'informations, reportez-vous aux [Notes de version de NetIQ Identity Manager Analyzer 4.7](#).

1.1.1 Installation simplifiée sur les plates-formes Linux

Identity Manager propose un nouveau programme d'installation par script simplifié pour les plates-formes Linux. Le nouveau programme d'installation prend en charge les méthodes interactives et silencieuses pour l'installation des composants Identity Manager. Le processus d'installation comprend une phase d'installation et une phase de configuration. La phase d'installation installe les fichiers binaires requis. La phase de configuration configure les composants Identity Manager. Le nouveau programme d'installation propose des modes de configuration standard et avancés.

Une configuration standard utilise les valeurs par défaut courantes pour la plupart des valeurs et est idéale pour une installation rapide du produit. La configuration personnalisée est adaptée aux environnements de production. Le nouveau programme d'installation contient également un utilitaire pour créer le fichier de propriétés silencieux dans un mode interactif. Le nouveau programme d'installation ne prend pas en charge la méthode d'installation par interface graphique (GUI).

Pour plus d'informations sur le téléchargement des fichiers d'installation, reportez-vous à la [Section 4.4, « Installation de NetIQ Identity Manager 4.7 », page 23](#). Pour obtenir des instructions d'installation, reportez-vous au [Guide d'installation de NetIQ Identity Manager pour Linux](#).

1.1.2 Fonction d'audit uniforme

Identity Manager introduit le format CEF (Common Event Format), une norme ouverte de gestion des fichiers journaux pour l'audit des événements sur l'ensemble des composants Identity Manager. CEF est un format texte extensible, conçu pour prendre en charge plusieurs types de périphériques en fournissant les informations les plus pertinentes. L'utilisation du format CEF réduit les syntaxes des

messages pour fonctionner avec une normalisation de type ESM (Embedded Syslog Manager). Le format CEF définit une syntaxe pour les enregistrements de journaux qui comprend un en-tête standard et une extension variable, et se présente sous la forme de paires clé-valeur.

La consignation au format CEF est désactivée par défaut. Pour l'activer, reportez-vous à la section [Configuring Identity Manager Components to Log Audit Events in CEF Format](#) (Configuration des composants Identity Manager pour la consignation des événements d'audit au format CEF) dans le manuel *NetIQ Identity Manager - Configuring Auditing in Identity Manager* (NetIQ Identity Manager - Configuration de la fonction d'audit dans Identity Manager).

REMARQUE : si vous effectuez une mise à niveau vers Identity Manager 4.7, XDAS reste disponible pour les composants Identity Manager à l'exception des applications d'identité. NetIQ vous recommande d'utiliser le format CEF pour l'audit de tous les composants. étant donné que XDAS sera bientôt obsolète.

1.1.3 Support étendu du canal du service Abonné pour les nouveaux pilotes

La prise en charge du canal du service Abonné introduite pour le pilote de dissémination (fan-out) JDBC dans Identity Manager 4.6 a été étendue aux pilotes Identity Manager suivants dans cette version : Active Directory, Active Directory multi-domaine et JDBC.

Le canal du service Abonné permet de traiter séparément les requêtes hors bande sans interrompre le flux normal des événements mis en cache tels que les processus de rafraîchissement d'assignation de code, la collecte de données et les requêtes déclenchées depuis dxcmd. Cela permet d'améliorer les performances du pilote.

Pour plus d'informations, reportez-vous à la section [Improving Driver Performance Using Subscriber Service Channel](#) (Amélioration des performances du pilote à l'aide du canal du service Abonné) dans le manuel *NetIQ Identity Manager Driver Administration Guide* (Guide d'administration des pilotes NetIQ Identity Manager).

1.1.4 Simplification des services d'actualisation des autorisations

Les services PCRS (Permission Collection Reconciliation Services) sont simplifiés pour les pilotes Active Directory, Active Directory multi-domaine (MDAD) et LDAP. Cette implémentation est désignée sous l'abréviation CPRS (Controlled Permission Reconciliation Services).

Dans la nouvelle implémentation, les services CPRS sont intégrés au tableau de bord Identity Manager pour vous aider à actualiser les autorisations du système connecté avec les applications d'identité. Pour plus d'informations, reportez-vous à la section [Using Controlled Permission Reconciliation Services](#) (Utilisation des services des CPRS) dans le manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur des applications d'identité de NetIQ Identity Manager).

Identity Manager prend en charge la migration d'autorisations de PCRS vers CPRS pour les pilotes Active Directory, MDAD et LDAP. Pour d'autres pilotes Identity Manager, vous pouvez continuer à utiliser PCRS. Pour plus d'informations, reportez-vous à la section [Migrating to CPRS](#) (*Migration vers CPRS*) dans le manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur pour les applications d'identité de NetIQ Identity Manager).

1.1.5 Modification de l'accès aux services de collecte de données d'Identity Manager

Identity Manager présente une nouvelle page Web pour accéder aux services DCS (Data Collection Services). Vous pouvez directement lancer cette page à partir de l'interface utilisateur des applications d'identité ou y accéder depuis un navigateur. Il s'agit d'une étape vers l'harmonisation de l'interface utilisateur entre les différents composants Identity Manager.

La page DCS permet de configurer les paramètres des systèmes connectés pour lesquels vous souhaitez créer des rapports, et de fournir des informations pour Identity Reporting. Pour plus d'informations, reportez-vous à la section [Exploring Identity Manager Data Collection Services](#) (Exploration des services DCS d'Identity Manager) dans le manuel *Administrator Guide to NetIQ Identity Reporting* (Guide de l'administrateur de NetIQ Identity Reporting).

1.1.6 Nouvelles fonctionnalités et améliorations des applications d'identité

Le composant Applications d'identité comprend les nouvelles fonctionnalités et améliorations suivantes :

1.1.6.1 Support du service d'assistance

Identity Manager présente une nouvelle fonctionnalité de service d'assistance pour aider les utilisateurs à résoudre n'importe quel problème lors de l'exécution de leurs tâches dans Identity Manager. Quelques tâches que le service d'assistance peut effectuer :

- ◆ Réassigner une requête d'approbation restée sans réponse depuis un certain temps
- ◆ Rechercher toutes les tâches ou filtrer les tâches d'un utilisateur sélectionné
- ◆ Demander des autorisations pour le compte d'autres utilisateurs

Les utilisateurs peuvent contacter le service d'assistance via l'ID d'adresse électronique du service d'assistance ou le numéro de contact, ou ils peuvent déclencher un ticket de service d'assistance. Après avoir configuré un service d'assistance, l'administrateur peut personnaliser les informations de ce dernier pour vos clients à partir des paramètres clients du tableau de bord.

Pour plus d'informations, consultez les liens suivants :

- ◆ [Understanding a Client Helpdesk](#) (Présentation d'un service d'assistance client) dans le manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur pour les applications d'identité de NetIQ Identity Manager)
- ◆ [Using Helpdesk](#) (Utilisation du service d'assistance) dans le manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur pour les applications d'identité de NetIQ Identity Manager)
- ◆ [Ouverture d'un ticket de service d'assistance](#) dans le manuel *NetIQ Identity Manager - Guide de l'utilisateur des applications d'identité*

1.1.6.2 Prise en charge de l'expiration des ressources

Cette version permet de définir la période d'expiration des ressources des applications d'identité. Cette période détermine quand l'accès à une ressource particulière doit expirer en fonction de la date d'assignation de la ressource. En outre, les utilisateurs peuvent demander une ressource pour une période spécifique. Pour plus d'informations, reportez-vous au manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).

1.1.6.3 Prise en charge de la délégation

Cette fonction permet de déléguer vos tâches à d'autres utilisateurs sur base de la configuration de la délégation. Vous pouvez configurer la délégation par l'intermédiaire du tableau de bord dans les applications d'identité.

Pour plus d'informations, reportez-vous à la section [Creating and Managing Delegations](#) (Création et gestion des délégations) dans le manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur pour les applications d'identité de NetIQ Identity Manager) et à la section [Gestion des délégations](#) dans le manuel *NetIQ Identity Manager - Guide de l'utilisateur des applications d'identité*.

1.1.6.4 Révocation au nom d'un autre utilisateur

Cette version améliore la prise en charge pour les administrateurs et les gestionnaires d'équipe en permettant de révoquer une autorisation au nom d'une autre personne. Il est également possible de révoquer plusieurs autorisations simultanément.

Pour plus d'informations, reportez-vous à la section [Révocation des autorisations](#) dans le manuel *NetIQ Identity Manager - Guide de l'utilisateur des applications d'identité*.

1.1.6.5 Prise en charge de la personnalisation du tableau de bord

Cette version permet de personnaliser les widgets sur votre tableau de bord. Les administrateurs peuvent définir des préférences pour que les utilisateurs du client puissent ajouter ou supprimer des widgets sur leur tableau de bord. Pour plus d'informations, reportez-vous à la section [Customizing the Identity Applications for Your Enterprise](#) (Personnalisation des applications d'identité pour votre entreprise) dans le manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur pour les applications d'identité de NetIQ Identity Manager).

1.1.6.6 Modernisation de la gestion des ressources et des rôles

Cette version intègre des fonctionnalités d'administration des rôles et des ressources au tableau de bord. Celles-ci étaient précédemment assurées par l'administrateur de catalogue. La nouvelle interface fournit une expérience d'interface utilisateur plus riche pour la gestion des rôles et des ressources. Elle permet également d'attribuer ou de révoquer des rôles et des ressources. Pour plus d'informations, reportez-vous aux sections [Creating and Managing Roles](#) (Création et gestion des rôles) et [Creating and Managing Resources](#) (Création et gestion des ressources) dans le manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur pour les applications d'identité de NetIQ Identity Manager).

1.1.6.7 Améliorations des performances du pilote du service Rôles et ressource

Le pilote du service Rôles et ressource a été amélioré pour inclure plusieurs threads afin de gérer différentes tâches telles que les assignations de rôles et de ressources, de manière à améliorer considérablement les performances du pilote. Pour plus d'informations, reportez-vous à la section [Multi-Threaded Role and Resource Service Driver](#) (Pilote du service Rôles et ressources multithread) dans le manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur pour les applications d'identité de NetIQ Identity Manager).

1.1.6.8 Purge de l'historique des ressources du pilote du service Rôles et ressources

Par défaut, le pilote est configuré pour purger l'historique des ressources quotidiennement. Le pilote purge uniquement les données de l'historique des ressources qui sont plus anciennes que la valeur de conservation (en jours) spécifiée pour le paramètre Nombre de jours de stockage de l'historique des ressources. Toutes les données historiques plus récentes que la valeur de conservation spécifiée sont conservées.

1.1.6.9 Prise en charge des tâches de renvoi et de réassignation

Désormais, plusieurs utilisateurs peuvent réassigner et renvoyer les tâches réaffectées par l'intermédiaire du tableau de bord Identity Manager. Les profils Identity Manager tels que Gestionnaire d'équipe, Administrateur, Service d'assistance et Utilisateurs finaux, disposent de différentes fonctionnalités pour réassigner et renvoyer des tâches. Pour plus d'informations, reportez-vous à la section [Gestion des requêtes pour une approbation ou un refus](#) dans le manuel *NetIQ Identity Manager - Guide de l'utilisateur des applications d'identité*.

1.1.6.10 Contrôle de l'autorisation par proxy pour l'application utilisateur

Le contrôle de l'autorisation par proxy pour l'application utilisateur fournit un mécanisme permettant de spécifier une identité d'autorisation par opération, ce qui est intéressant pour les administrateurs qui doivent effectuer des opérations efficacement pour le compte d'autres utilisateurs. De cette façon, l'application utilisateur n'a pas besoin de certificats SAML pour l'exécution d'opérations sur le coffre-fort d'identité.

1.1.7 Création de paquetages simplifiée pour les fichiers d'installation

Cette version simplifie la mise en paquetage des composants Identity Manager dans un fichier ISO unique, tant pour les systèmes d'exploitation Linux que Windows. Designer et Analyzer sont également disponibles dans des fichiers séparés. Le service Sentinel for IGA est fourni dans un fichier séparé afin de faciliter la configuration avec Identity Reporting.

1.2 Prise en charge des systèmes d'exploitation

Cette version ajoute la prise en charge des plates-formes suivantes :

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

IMPORTANT : Sentinel Log Management for Identity Governance and Administration (IGA) est pris en charge uniquement sur les plates-formes SLES 12 SP2 et RHEL 7.3.

1.3 Versions des composants dépendants

Cette version ajoute la prise en charge des composants dépendants suivants :

- ♦ 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

Lorsque vous effectuez la mise à niveau du moteur Identity Manager vers la version 4.7, le programme d'installation du moteur nettoie partiellement les fichiers de cache MapDB existants. Vous devez supprimer manuellement les fichiers de cache MapDB existants de votre pilote après la mise à niveau du pilote. Pour plus d'informations, reportez-vous au guide d'implémentation du pilote en question sur le site Web de la [documentation des pilotes Identity Manager](#).

1.4 Problèmes résolus

Cette version inclut les correctifs logiciels suivants :

- ♦ Section 1.4.1, « SSPR ne demande plus de définir des questions de sécurité lors de la première connexion », page 9
- ♦ Section 1.4.2, « Le programme d'installation des applications d'identité crée correctement le fichier master-key.txt sur le système de fichiers pendant l'installation », page 9
- ♦ Section 1.4.3, « La page Applications ouvre à présent une application externe dans un autre onglet », page 9
- ♦ Section 1.4.4, « L'installation du moteur Identity Manager inclut un paquetage novell-DXMLsch sous Linux », page 9
- ♦ Section 1.4.5, « Le moteur Identity Manager applique une restriction pour l'ajout de classes auxiliaires dans un filtre de pilote », page 10
- ♦ Section 1.4.6, « La chaîne de connexion server.xml de Tomcat inclut correctement un port non standard spécifié pour la base de données Oracle lorsque Identity Reporting est configuré sous Linux », page 10
- ♦ Section 1.4.7, « Fichier Create_rpt_roles_and_schemas.sql requis avant d'installer Identity Reporting avec la base de données Oracle sous Linux », page 10
- ♦ Section 1.4.8, « Contrôle des droits des fichiers avec Writelog pour AJC-JavaScript », page 10
- ♦ Section 1.4.9, « Le mot de passe du chargeur distant ignore les parenthèses », page 10
- ♦ Section 1.4.10, « L'assignation de jeton renvoie un résultat vide en cas de non-correspondance », page 10
- ♦ Section 1.4.11, « Suppression de la vue en double pour idmrpt_identity_v1 », page 10
- ♦ Section 1.4.12, « Le jeton do-remove-role prend en charge l'ID de corrélation », page 10
- ♦ Section 1.4.13, « Identity Reporting crée correctement des entrées de marque de réservation dans la base de données Oracle », page 10
- ♦ Section 1.4.14, « La stratégie de transformation de sortie émet correctement un message d'état fatal indiquant d'arrêter le pilote », page 11
- ♦ Section 1.4.15, « Le moteur Identity Manager respecte le paramètre de filtre optimize-modify="false" lors d'une opération de fusion de l'éditeur », page 11
- ♦ Section 1.4.16, « Le plug-in de stratégie de mot de passe affiche les bonnes informations à propos de la longueur autorisée du mot de passe », page 11
- ♦ Section 1.4.17, « Le champ d'adresse électronique privée dans le plug-in des pages de propriétés du profil utilisateur accepte une valeur supérieure à trente-deux caractères », page 11
- ♦ Section 1.4.18, « Le mode Lot dxcmd inclut les statistiques du cache de synchronisation des priorités », page 11
- ♦ Section 1.4.19, « La stratégie de correspondance d'abonné de pilote Office 365 utilise token-src-name au lieu de token-src-attr », page 11
- ♦ Section 1.4.20, « La base de données de création de rapports est correctement mise à jour après l'exécution d'une opération de suppression de ressource nécessitant une approbation », page 11
- ♦ Section 1.4.21, « Le programme d'installation d'Identity Manager Linux émet un message d'erreur si le répertoire monté contient un espace », page 11
- ♦ Section 1.4.22, « L'appel d'une fonction Java avec trente-six paramètres à partir d'une stratégie de pilote échoue après la mise à niveau depuis Identity Manager 4.0.2 », page 12

- ♦ Section 1.4.23, « Utilisation de dxcmd en mode non interactif pour effacer le contenu du cache », page 12
- ♦ Section 1.4.24, « Le plug-in Tableau de bord de l'ensemble de pilotes nettoie le répertoire temporaire d'images », page 12
- ♦ Section 1.4.25, « Les membres de la distribution de groupe ou de la sécurité avec messagerie ne sont pas synchronisés dans Azure Active Directory », page 12
- ♦ Section 1.4.26, « OSP procède à la vérification post-authentification s'il est configuré avec Kerberos », page 12
- ♦ Section 1.4.27, « Le moteur Identity Manager prend en charge un nombre accru d'états de santé de pilote », page 12
- ♦ Section 1.4.28, « Le programme d'installation d'Identity Manager dont l'emplacement est configuré sur les Pays-Bas prend par défaut l'allemand sous Windows », page 12
- ♦ Section 1.4.29, « L'importation de fichier SQL pour la base de données Oracle ne renvoie pas les erreurs », page 12
- ♦ Section 1.4.30, « L'utilitaire de mise à niveau des applications d'identité fournit des informations sur les versions des composants qu'il met à niveau sous Windows », page 13
- ♦ Section 1.4.31, « L'utilitaire de mise à niveau des applications d'identité gère le contexte personnalisé », page 13
- ♦ Section 1.4.32, « Possibilité d'utiliser un port de messagerie non standard dans la configuration d'Identity Manager », page 13
- ♦ Section 1.4.33, « L'écran de trace du chargeur distant se ferme après le redémarrage du système sous Windows 2012 », page 13
- ♦ Section 1.4.34, « Possibilité de rechercher un utilisateur avec un nom complet dans le tableau de bord », page 13
- ♦ Section 1.4.35, « Affichage de l'historique des requêtes pour une période spécifique », page 13
- ♦ Section 1.4.36, « Affichage amélioré de la liste des autorisations », page 13
- ♦ Section 1.4.37, « La fenêtre contextuelle de notification de ressource affiche le CN au lieu du FQDN dans le tableau de bord », page 13
- ♦ Section 1.4.38, « Ajout de workflows, ressources ou PRD sur la page Applications », page 14
- ♦ Section 1.4.39, « Provisioning d'une demande d'assignation ou de retrait de rôles et de ressource à l'aide d'un noeud d'extrémité SOAP/REST », page 14
- ♦ Section 1.4.40, « La recherche d'assignation de ressource dynamique renvoie correctement les droits souhaités », page 14
- ♦ Section 1.4.41, « Les approbateurs supprimés ne sont pas affichés dans la liste des approbateurs », page 14
- ♦ Section 1.4.42, « La chaîne de mise à jour du rôle et de la relation de rôle est correctement traduite en espagnol », page 14
- ♦ Section 1.4.43, « Ouverture de PRD à partir de la page Applications dans le tableau de bord », page 14
- ♦ Section 1.4.44, « L'activité d'intégration prend en charge la communication avec les serveurs pour lesquels l'authentification mutuelle est activée », page 14
- ♦ Section 1.4.45, « L'organigramme du tableau de bord affiche les objets et attributs autorisés pour un utilisateur », page 14
- ♦ Section 1.4.46, « Le script idmapps_tomcat_init ne requiert plus que etc/rc.d/init.d/functions dispose d'autorisations d'exécution pour lancer le service en tant que daemon sous Linux », page 15

- ♦ Section 1.4.47, « Les modèles de collection de notifications par défaut affichent les langues adéquates », page 15
- ♦ Section 1.4.48, « Le tableau de bord affiche correctement les tâches si le type de données de la colonne METAXML est ntext », page 15
- ♦ Section 1.4.49, « Les commentaires de l'historique des requêtes affichent le nom complet d'un utilisateur au lieu du CN », page 15
- ♦ Section 1.4.50, « La largeur du champ de liste ne change pas lorsque la date est modifiée », page 15
- ♦ Section 1.4.51, « La PRD s'ouvre correctement dans un nouvel onglet », page 15
- ♦ Section 1.4.52, « La valeur fdn <req> du demandeur sur un objet Utilisateur pour les rôles et ressources est modifiée lorsque l'utilisateur est renommé », page 15
- ♦ Section 1.4.53, « getRoleLevels renvoie des informations correctes », page 15
- ♦ Section 1.4.54, « La variable NETIQ_TOMCAT_USER est supprimée du programme d'installation Tomcat PostgreSQL sous Windows », page 16
- ♦ Section 1.4.55, « Possibilité de trier l'historique des requêtes dans le tableau de bord », page 16
- ♦ Section 1.4.56, « Pilote du service Rôles et ressource », page 16

1.4.1 SSPR ne demande plus de définir des questions de sécurité lors de la première connexion

Lorsque vous vous connectez aux applications d'identité avec un nom d'utilisateur contenant un espace, SSPR ne vous invite plus à définir des questions de sécurité au cours de la première connexion. (Bogue 1025713)

1.4.2 Le programme d'installation des applications d'identité crée correctement le fichier master-key.txt sur le système de fichiers pendant l'installation

Désormais, le programme d'installation des applications d'identité crée le fichier `master-key.txt` dans le répertoire `<installation_application_utilisateur>` de Tomcat. Vous devez lire la valeur de clé principale à partir de ce fichier au lieu du fichier `ism-configuration.properties` lors de la configuration des composants Applications d'identité sur une grappe Tomcat. (Bogue 900240)

1.4.3 La page Applications ouvre à présent une application externe dans un autre onglet

Dans le tableau de bord Identity Manager, lorsque vous cliquez sur une application externe à partir de la page **Applications**, l'application s'ouvre dans un autre onglet au lieu de s'afficher dans le même onglet. (Bogue 1079325)

1.4.4 L'installation du moteur Identity Manager inclut un paquetage novell-DXMLsch sous Linux

Cette version introduit un processus de d'installation et de configuration personnalisées sur les plates-formes Linux. Le processus d'installation pour le moteur Identity Manager installe un paquetage novell-DXMLsch pour tous les scénarios d'installation. (Bogue 1054169)

1.4.5 Le moteur Identity Manager applique une restriction pour l'ajout de classes auxiliaires dans un filtre de pilote

Les classes auxiliaires ne sont pas traitées par le moteur Identity Manager. Il ne tient pas compte de cette opération et signale un avertissement dans le fichier de trace du pilote. (Bogue 1041056)

1.4.6 La chaîne de connexion server.xml de Tomcat inclut correctement un port non standard spécifié pour la base de données Oracle lorsque Identity Reporting est configuré sous Linux

Le nouveau programme d'installation d'Identity Manager pour Linux utilise la valeur spécifiée pour un port de base de données non standard lors de la phase de configuration afin de mettre à jour l'URL de connexion dans le fichier server.xml de Tomcat. (Bogue 1063010)

1.4.7 Fichier Create_rpt_roles_and_schemas.sql requis avant d'installer Identity Reporting avec la base de données Oracle sous Linux

Lorsque vous exécutez le programme d'installation d'Identity Reporting sous Linux, le processus installe les fichiers.sql requis pour configurer le schéma de base de données. (Bogue 1063009)

1.4.8 Contrôle des droits des fichiers avec Writelog pour AJC-JavaScript

ECMAScript a été amélioré pour inclure une nouvelle fonction, setFilePermissions, qui vous permet de modifier les droits de fichier POSIX sous Linux. (Bogue 1023201)

1.4.9 Le mot de passe du chargeur distant ignore les parenthèses

Identity Manager traite correctement un mot de passe de chargeur distant avec ou sans parenthèse de fermeture spécifié pour établir une connexion avec le moteur Identity Manager. (Bogue 919823)

1.4.10 L'assignation de jeton renvoie un résultat vide en cas de non-correspondance

La stratégie d'assignation de jeton ne s'exécute pas si elle ne trouve pas de jeton correspondant. (Bogue 1063065)

1.4.11 Suppression de la vue en double pour idmrpt_identity_v1

La vue idmrpt_identity_v1 était similaire à la vue idmrpt_identity_cs_v. La première a dès lors été supprimée du schéma de base de données pour éviter les doublons. (Bogue 824615)

1.4.12 Le jeton do-remove-role prend en charge l'ID de corrélation

Le jeton do-remote-role a été amélioré pour accepter une valeur d'ID de corrélation. Par défaut, il utilise la valeur provenant de l'ID d'événement d'opération, sauf s'il est défini. (Bogue 933953)

1.4.13 Identity Reporting crée correctement des entrées de marque de réservation dans la base de données Oracle

Identity Reporting ne traite plus un utilisateur appartenant à un groupe qui n'existe pas dans la base de données Oracle. (Bogue 1075816)

1.4.14 La stratégie de transformation de sortie émet correctement un message d'état fatal indiquant d'arrêter le pilote

La stratégie de transformation de sortie a été améliorée pour émettre un message d'état fatal dans la trace de l'éditeur indiquant que le pilote doit être arrêté. (Bogue 1050608)

1.4.15 Le moteur Identity Manager respecte le paramètre de filtre optimize-modify="false" lors d'une opération de fusion de l'éditeur

Lorsqu'une correspondance a été établie sur le canal Éditeur, quand toutes les valeurs d'attribut sont définies correctement dans le coffre-fort d'identité, le moteur traite correctement une opération qui contient tous les attributs avec les paramètres publisher="sync" et optimize-modify="false". (Bogue 794273)

1.4.16 Le plug-in de stratégie de mot de passe affiche les bonnes informations à propos de la longueur autorisée du mot de passe

L'interface utilisateur du plug-in de stratégie de mot de passe a été mise à jour afin que la stratégie de mot de passe refuse les mots de passe comportant moins de trois caractères. (Bogue 936162)

1.4.17 Le champ d'adresse électronique privée dans le plug-in des pages de propriétés du profil utilisateur accepte une valeur supérieure à trente-deux caractères

Le champ d'adresse électronique privée dans le plug-in des pages de propriétés du profil utilisateur permet maintenant de spécifier une valeur supérieure à trente-deux caractères. (Bogue 997453)

1.4.18 Le mode Lot dxcmd inclut les statistiques du cache de synchronisation des priorités

dxcmd fournit désormais les statistiques du cache de synchronisation des priorités aussi bien dans le mode Lot que dans le mode interactif. (Bogue 1014476)

1.4.19 La stratégie de correspondance d'abonné de pilote Office 365 utilise token-src-name au lieu de token-src-attr

L'utilisation de token-src-name empêche le pilote de procéder à une requête inutile dans le coffre-fort d'identité avant chaque correspondance. Cela améliore les performances du pilote lors d'une charge importante telle qu'une migration initiale d'utilisateurs. (Bogue 881132)

1.4.20 La base de données de création de rapports est correctement mise à jour après l'exécution d'une opération de suppression de ressource nécessitant une approbation

Une fois la révocation de ressource approuvée par l'approbateur, la table identity_trust est correctement mise à jour et l'état d'approbation change de 1 à 0. (Bogue 1067991)

1.4.21 Le programme d'installation d'Identity Manager Linux émet un message d'erreur si le répertoire monté contient un espace

Le programme d'installation Identity Manager Linux a été amélioré pour signaler une erreur lorsqu'il trouve un espace dans le répertoire dans lequel vous montez le fichier ISO. (Bogue 910386)

1.4.22 L'appel d'une fonction Java avec trente-six paramètres à partir d'une stratégie de pilote échoue après la mise à niveau depuis Identity Manager 4.0.2

Le moteur Identity Manager a été amélioré afin de traiter correctement trente-six arguments. (Bogue 1055873)

1.4.23 Utilisation de dxcmd en mode non interactif pour effacer le contenu du cache

Vous pouvez désormais supprimer le cache d'un pilote à l'aide de dxcmd dans un mode non interactif et à tout moment. (Bogue 1006754)

1.4.24 Le plug-in Tableau de bord de l'ensemble de pilotes nettoie le répertoire temporaire d'images

Identity Manager crée temporairement les fichiers graphiques utilisés par les plug-ins Présentation d'Identity Manager et Tableau de bord de l'ensemble de pilotes dans le répertoire <dossier_installation_iManager>/nps/images/temp. Le répertoire temporaire est désormais nettoyé lors du redémarrage du serveur Tomcat qui héberge iManager. (Bogue 1001237)

1.4.25 Les membres de la distribution de groupe ou de la sécurité avec messagerie ne sont pas synchronisés dans Azure Active Directory

Un membre de groupe du coffre-fort d'identité est désormais correctement synchronisé avec les groupes Azure Active Directory. (Bogue 1077198)

1.4.26 OSP procède à la vérification post-authentification s'il est configuré avec Kerberos

Si vous avez configuré OSP avec Kerberos, OSP effectue désormais la vérification post-authentification de l'utilisateur pour déterminer s'il dispose d'un mot de passe expiré ou s'il doit répondre à des questions de stimulation-réponse. (Bogue 924221)

1.4.27 Le moteur Identity Manager prend en charge un nombre accru d'états de santé de pilote

Le moteur Identity Manager a été amélioré pour stocker et traiter plusieurs configurations d'état de santé sur un attribut de pilote. (Bogue 870219)

1.4.28 Le programme d'installation d'Identity Manager dont l'emplacement est configuré sur les Pays-Bas prend par défaut l'allemand sous Windows

Ce problème est désormais résolu. Le programme d'installation prend à présent l'anglais comme valeur par défaut. (Bogue 768958)

1.4.29 L'importation de fichier SQL pour la base de données Oracle ne renvoie pas les erreurs

Le fichier SQL est généré lorsque l'option **Écrire SQL** est sélectionnée pendant l'installation des applications d'identité. Ces dernières importent désormais correctement le fichier SQL dans la base de données Oracle. (Bogue 1057368)

1.4.30 L'utilitaire de mise à niveau des applications d'identité fournit des informations sur les versions des composants qu'il met à niveau sous Windows

L'utilitaire de mise à niveau affiche désormais les nouvelles versions vers lesquelles il va mettre à jour les composants déjà installés. (Bogue 1031435)

1.4.31 L'utilitaire de mise à niveau des applications d'identité gère le contexte personnalisé

Vous pouvez désormais utiliser un contexte différent de celui par défaut (IDMProv) au cours de la mise à niveau. (Bogue 1028475)

1.4.32 Possibilité d'utiliser un port de messagerie non standard dans la configuration d'Identity Manager

Vous pouvez à présent configurer votre serveur de messagerie pour qu'il écoute sur un port SMTP non standard. (Bogue 1041493)

1.4.33 L'écran de trace du chargeur distant se ferme après le redémarrage du système sous Windows 2012

Ce problème n'existe plus. L'écran de trace du chargeur distant se ferme correctement. (Bogue 892034)

1.4.34 Possibilité de rechercher un utilisateur avec un nom complet dans le tableau de bord

Tous les attributs utilisateur marqués comme recherche dans DAL peuvent désormais être marqués comme attribut de recherche dans le catalogue des utilisateurs à partir de la page de paramètres du tableau de bord. (Bogue 1073463)

1.4.35 Affichage de l'historique des requêtes pour une période spécifique

Le tableau de bord a été mis à jour de manière à afficher vos requêtes pour la période spécifiée par votre administrateur. (Bogue 1061696)

1.4.36 Affichage amélioré de la liste des autorisations

Le tableau de bord affiche uniquement les assignations directes. Il inclut également une icône vous permettant d'afficher la liste de toutes les autorisations. (Bogue 1061516)

1.4.37 La fenêtre contextuelle de notification de ressource affiche le CN au lieu du FQDN dans le tableau de bord

Le tableau de bord affiche désormais uniquement le nom CN de la ressource dans le panneau de notification. (Bogue 1055622)

1.4.38 Ajout de workflows, ressources ou PRD sur la page Applications

Dans la nouvelle interface utilisateur, vous pouvez créer des liens profonds dans la page Applications pour les workflows, les ressources et les PRD. Lorsque vous cliquez sur une mosaïque de cette page, le formulaire s'ouvre dans un nouvel onglet. Une fois la requête soumise, vous revenez sur la page Applications. (Bogue 988818)

1.4.39 Provisioning d'une demande d'assignation ou de retrait de rôles et de ressource à l'aide d'un noeud d'extrémité SOAP/REST

Vous pouvez désormais émettre une demande d'octroi ou de révocation de rôle via un noeud d'extrémité de rôle SOAP ou REST, en plus d'avoir la possibilité d'effectuer cette opération via l'interface utilisateur. (Bogue 846736)

1.4.40 La recherche d'assignation de ressource dynamique renvoie correctement les droits souhaités

Si vous utilisez le tableau de bord pour demander une ressource associée à un droit avec valeur, le tableau de bord filtre correctement les droits en fonction de vos critères de recherche. (Bogue 995889)

1.4.41 Les approbateurs supprimés ne sont pas affichés dans la liste des approbateurs

Les approbateurs supprimés ne figurent plus dans le catalogue de rôles de la nouvelle page Administration. (Bogue 632362)

1.4.42 La chaîne de mise à jour du rôle et de la relation de rôle est correctement traduite en espagnol

Ce problème est à présent résolu. (Bogue 1076780)

1.4.43 Ouverture de PRD à partir de la page Applications dans le tableau de bord

En fonction des paramètres de la page de requête et d'applications, vous pouvez ouvrir les PRD soit dans un nouvel onglet, soit dans la même fenêtre. (Bogue 1076155)

1.4.44 L'activité d'intégration prend en charge la communication avec les serveurs pour lesquels l'authentification mutuelle est activée

Lorsque vous disposez du certificat client et du certificat privé, vous pouvez communiquer avec un serveur pour lequel l'authentification mutuelle est activée grâce à l'activité d'intégration. (Bogue 1075309)

1.4.45 L'organigramme du tableau de bord affiche les objets et attributs autorisés pour un utilisateur

L'organigramme affiche correctement les informations que l'utilisateur est autorisé à consulter. (Bogue 1076155)

1.4.46 Le script idmapps_tomcat_init ne requiert plus que etc/rc.d/init.d/functions dispose d'autorisations d'exécution pour lancer le service en tant que daemon sous Linux

Le logiciel d'installation a été mis à jour pour supprimer cette dépendance. (Bogue 1064603)

1.4.47 Les modèles de collection de notifications par défaut affichent les langues adéquates

Les modèles de notifications par défaut sont correctement traduits dans la langue spécifiée. (Bogue 1063967)

1.4.48 Le tableau de bord affiche correctement les tâches si le type de données de la colonne METAXML est ntext

Si vous remplacez le type de colonne de METAXML dans AFDOCUMENT par le type de données d'argument ntext, le tableau de bord traite correctement le type de données d'argument modifié. (Bogue 1062342)

1.4.49 Les commentaires de l'historique des requêtes affichent le nom complet d'un utilisateur au lieu du CN

La section des commentaires de l'historique des requêtes affiche désormais le nom complet d'un utilisateur au lieu du CN. Lorsque vous cliquez sur le nom complet de l'utilisateur, le tableau de bord affiche une fenêtre contextuelle présentant des informations rapides sur l'utilisateur et un lien profond pour accéder à la page de l'utilisateur pour obtenir plus d'informations à son sujet. (Bogue 1060709)

1.4.50 La largeur du champ de liste ne change pas lorsque la date est modifiée

Lorsque vous définissez ou modifiez une date dans un formulaire d'application utilisateur, la largeur des champs de liste n'est plus définie sur la largeur de la première liste. (Bogue 1049919)

1.4.51 La PRD s'ouvre correctement dans un nouvel onglet

Lorsque vous exécutez une PRD personnalisée à partir de l'onglet Applications, les paramètres Formulaire de requête sont désormais chargés au moment opportun afin que la PRD s'ouvre dans un nouvel onglet, au lieu d'une nouvelle fenêtre. (Bogue 1044350)

1.4.52 La valeur fdn <req> du demandeur sur un objet Utilisateur pour les rôles et ressources est modifiée lorsque l'utilisateur est renommé

La valeur <req> contenant le fdn <req> sur un objet Utilisateur pour les attributs nrfassignedroles et nrfassignedresources est bien mise à jour lorsqu'un utilisateur est renommé. (Bogue 1028476)

1.4.53 getRoleLevels renvoie des informations correctes

Le noeud d'extrémité SOAP getRoleLevels a été mis à jour pour renvoyer les niveaux de rôles dans le bon ordre. (Bogue 935105)

1.4.54 La variable NETIQ_TOMCAT_USER est supprimée du programme d'installation Tomcat PostgreSQL sous Windows

La variable NETIQ_TOMCAT_USER est supprimée du fichier d'installation silencieuse du programme d'installation Tomcat PostgreSQL pour Windows. Le nouveau programme d'installation Linux autorise la création d'un fichier de propriétés silencieux sur la base de la saisie de l'utilisateur, au lieu de compiler un fichier de propriétés codées de manière irréversible. Cette modification n'est plus applicable à Linux. (Bogue 925699)

1.4.55 Possibilité de trier l'historique des requêtes dans le tableau de bord

La page de l'historique des requêtes liste maintenant l'historique des requêtes dans l'ordre inverse (par date). (Bogue 1061515)

1.4.56 Pilote du service Rôles et ressource

1.4.56.1 Possibilité de privilégier les requêtes des clients par rapport aux requêtes planifiées

Le pilote du service Rôles et ressources a été amélioré afin de privilégier les requêtes générées par les utilisateurs par rapport aux requêtes créées par le pilote lui-même. (Bogue 1008920)

1.4.56.2 La suppression de rôles ne supprime pas les valeurs de droits qui se chevauchent

Le pilote du service Rôles et ressources génère un cache temporaire des événements de création d'associations de ressources avant de resynchroniser l'association de ressource supprimée et de recalculer les ressources basées sur un rôle manquant. Cela garantit que seules ces associations qui ne sont pas assignées à d'autres rôles attribués sont retirées de l'utilisateur. (Bogue 1040935)

1.4.56.3 Capacité de gérer les déplacements d'objets

Le mécanisme de récupération du pilote gère maintenant correctement une opération de déplacement d'utilisateur lorsque le pilote assigne des rôles et ressources à cet utilisateur. (Bogue 1061399)

1.4.56.4 Le pilote du service Rôles et ressources gère correctement l'échec d'un changement d'adhésion à un groupe dynamique

Le pilote a été amélioré pour gérer l'échec d'un changement d'adhésion à un groupe dynamique. (Bogue 736047)

1.5 Correction de vulnérabilités logicielles

Cette version résout les expositions et vulnérabilités courantes (Common Vulnerabilities and Exposures, CVE) suivantes pour Identity Manager :

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

1.6 Fonctions modifiées, abandonnées ou discontinuées

Afin de rationaliser les fonctionnalités, plusieurs éléments ont été modifiés ou ne sont plus pris en charge par Identity Manager 4.7. Dans de nombreux cas, d'autres fonctionnalités remplacent les éléments abandonnés.

1.6.1 Caractéristiques et fonctions obsolètes

La liste suivante présente les caractéristiques et fonctions qui sont devenues obsolètes.

Self-service d'identité, Tableau de bord de travail, Conformité, Administration des rôles et des ressources dans l'application utilisateur

Cette version d'Identity Manager introduit l'interface d'administration des applications d'identité. Au lieu d'utiliser ces fonctions dans l'application utilisateur, vous devez employer la nouvelle interface. Ces fonctions de l'application utilisateur ne sont plus prises en charge à partir de cette version. Pour plus d'informations, reportez-vous au manuel [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).

Gestion des mots de passe hérités

La fonction de self-service de mot de passe hérité de l'application utilisateur n'est plus prise en charge à partir de cette version. Vous devez utiliser SSPR pour la consignation des événements. Pour plus d'informations, reportez-vous au [Guide d'installation de NetIQ Identity Manager pour Linux](#) ou au [Guide d'installation de NetIQ Identity Manager pour Windows](#).

1.6.2 Caractéristiques et fonctions abandonnées

La liste suivante présente un aperçu des caractéristiques et fonctions abandonnées à partir de cette version :

Programme d'installation intégré

Identity Manager 4.7 ne prend plus en charge le programme d'installation intégré. Celui-ci est abandonné à partir de cette version.

Audit XDAS pour les applications d'identité

L'audit avec XDAS pour les composants d'applications d'identité est abandonné à partir de cette version. Vous devez utiliser CEF pour consigner les événements d'applications d'identité.

Cette modification ne s'applique pas aux autres composants Identity Manager qui prennent XDAS en charge. NetIQ vous recommande d'utiliser l'audit CEF pour tous les composants Identity Manager.

Accès différent page d'accueil et tableau de bord de provisioning d'Identity Manager/ Administrateur de catalogue

Cette version offre une version améliorée du tableau de bord Identity Manager qui remplace la page d'accueil et le tableau de bord de provisioning. Ces derniers sont abandonnés à partir de cette version.

La fonctionnalité fournie par l'administrateur de catalogue est incluse dans l'interface d'administration des applications d'identité. L'administrateur de catalogue est abandonné à partir de cette version.

Service d'interface REST (RIS)

Cette version d'Identity Manager permet d'accéder à la majorité des fonctionnalités des applications d'identité via l'interface de programmation d'application (API). Cette API est basée sur HTTP, avec une interface de programmation RESTful. Vous pouvez appeler l'API à l'aide d'un client REST ou grâce à la commande cURL dans des scripts afin d'automatiser les tâches administratives. RIS est abandonné à partir de cette version.

Plates-formes RHEL 6.x et SLES 11.x

La prise en charge des plates-formes RHEL 6.x et SLES 11.x cesse à partir de cette version.

1.7 Guides d'installation distincts pour les plates-formes Windows et Linux

Cette version met à disposition des guides distincts pour l'installation et la configuration, la mise à niveau et la désinstallation des composants Identity Manager pour les plates-formes Linux et Windows. Pour plus d'informations, reportez-vous à l'un des liens suivants :

- ♦ [Guide d'installation de NetIQ Identity Manager pour Linux](#)
- ♦ [Guide d'installation de NetIQ Identity Manager pour Windows](#)

1.8 L'accord de licence de l'utilisateur final n'est pas disponible dans toutes les langues prises en charge

Chaque programme d'installation comprend un accord de licence de l'utilisateur final. Bien que les programmes d'installation prennent en charge plusieurs langues, l'accord de licence n'est pas disponible dans les langues suivantes :

- ♦ Danois
- ♦ Néerlandais
- ♦ Russe
- ♦ Suédois

À la place, le programme d'installation affiche l'accord de licence en anglais. Pour plus d'informations, reportez-vous à la section « [Présentation de la prise en charge des langues](#) » dans le [Guide d'installation de NetIQ Identity Manager pour Linux](#) ou la section « [Présentation de la prise en charge des langues](#) » dans le [Guide d'installation de NetIQ Identity Manager pour Windows](#). (Bogue 896299)

1.9 NetIQ Corporation ne fournit aucun support pour les composants de l'installation PostgreSQL et Tomcat

Les composants PostgreSQL et Tomcat sont installés automatiquement sur un serveur Linux. Sous Windows, ces composants sont installés à l'aide d'un programme d'installation distinct. Sachez que NetIQ Corporation fournit l'installation de PostgreSQL et de Tomcat pour votre facilité. Si votre société ne fournit aucun serveur d'applications ni serveur de base de données, vous pouvez installer et utiliser ces composants. Pour obtenir un support, contactez le fournisseur du composant. NetIQ n'assure pas les mises à jour, l'administration, la configuration ou l'adaptation des informations de ces composants au-delà de ce qui est décrit dans le [Guide d'installation de NetIQ Identity Manager pour Linux](#) ou dans le [Guide d'installation de NetIQ Identity Manager pour Windows](#).

2 Versions des composants Identity Manager

Identity Manager 4.7 regroupe les composants suivants :

- ♦ NetIQ eDirectory 9.1
- ♦ NetIQ® iManager 3.1
- ♦ NetIQ Identity Manager Engine 4.7
- ♦ NetIQ Identity Manager Remote Loader 4.7
- ♦ Agent de dissémination NetIQ Identity Manager 1.2
- ♦ NetIQ Designer pour Identity Manager 4.7
- ♦ Applications NetIQ Identity 4.7
- ♦ NetIQ Single Sign-on (One SSO) 6.2.1
- ♦ NetIQ Identity Manager Self-Service Password Reset 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 for IGA 8.1.1 (pour l'audit des événements)
- ♦ NetIQ Analyzer for Identity Manager 4.7
- ♦ Pilotes NetIQ Identity Manager. Pour les versions de pilote, consultez le [Driver and Engine Version Compatibility Table](#) (tableau de compatibilité des versions de pilote et de moteur).

REMARQUE : les versions des pilotes Identity Manager sont indépendantes de la version du moteur et n'indiquent pas la version de moteur minimum requise pour exécuter un pilote.

3 Configuration système requise

Vous pouvez installer les composants Identity Manager sur diverses plates-formes de système d'exploitation. Pour obtenir des informations concernant les composants pouvant être installés en fonction des systèmes d'exploitation, reportez-vous à la section « [Sélection d'une plate-forme de système d'exploitation pour Identity Manager](#) » dans le *Guide d'installation de NetIQ Identity Manager pour Linux* ou « [Sélection d'une plate-forme de système d'exploitation pour Identity Manager](#) » dans le *Guide d'installation de NetIQ Identity Manager pour Windows*).

Pour plus d'informations sur les conditions préalables, la configuration de l'ordinateur, l'installation, la mise à niveau ou la migration pour votre plate-forme, consultez l'un des guides suivants :

- ♦ [Guide d'installation de NetIQ Identity Manager pour Linux](#)
- ♦ [Guide d'installation de NetIQ Identity Manager pour Windows](#)

4 Installation de NetIQ Identity Manager 4.7

Identity Manager 4.7 propose les versions Advanced Edition et Standard Edition dans un même fichier ISO. Avant de télécharger les fichiers d'installation, vous devez comprendre quelles sont les fonctionnalités contenues dans chaque édition ainsi que les options de téléchargement des composants Identity Manager.

- ♦ [Section 4.1, « Fonctionnalités prises en charge dans Identity Manager, versions Advanced Edition et Standard Edition », page 20](#)
- ♦ [Section 4.2, « Téléchargement d'Identity Manager », page 20](#)

- ♦ [Section 4.3, « Emplacement des fichiers exécutables et chemins d'installation par défaut », page 21](#)
- ♦ [Section 4.4, « Installation de NetIQ Identity Manager 4.7 », page 23](#)

4.1 Fonctionnalités prises en charge dans Identity Manager, versions Advanced Edition et Standard Edition

Afin de répondre aux différentes exigences des clients, les fonctionnalités d'Identity Manager sont proposées dans deux groupes de produits :

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

Identity Manager Advanced Edition intègre les mêmes fonctions qu'Identity Manager Standard Edition, mais aussi des outils supplémentaires. Le tableau suivant présente une comparaison des fonctions disponibles dans les versions Advanced Edition et Standard Edition d'Identity Manager :

Fonctionnalité	Advanced Edition	Standard Edition
Provisioning automatisé des utilisateurs basé sur des règles	Oui	Oui
Synchronisation des identités en temps réel	Oui	Oui
Gestion et self-service de mots de passe	Oui	Oui
Outil d'informations d'identité uniformes (Analyzer)	Oui	Oui
API REST et prise en charge de Single Sign-on	Oui	Oui (prise en charge limitée)
Rapport sur l'état actuel	Oui	Oui
Provisioning de niveau entreprise basé sur des rôles	Oui	Non
Workflows d'approbation automatisés pour l'application de la stratégie d'entreprise	Oui	Non
Self-service avancé pour les applications d'identité	Oui	Non
Catalogue et modèle de ressource pour provisioning aisé des ressources	Oui	Non
Rapports d'historique	Oui	Non
Création de rapports sur les systèmes connectés	Oui	Non
Administrateur de catalogue	Oui	Non

4.2 Téléchargement d'Identity Manager

Après avoir acheté Identity Manager 4.7, connectez-vous au [site Web du produit Identity Manager](#) et suivez le lien qui vous permet de procéder au téléchargement du logiciel. Les fichiers suivants contiennent les composants Identity Manager :

Nom du fichier	Description
Identity_Manager_4.7_Linux.iso	Contient le serveur Identity Manager (moteur Identity Manager, chargeur distant, agent de dissémination, administration Web d'iManager), les applications d'identité, Identity Reporting, Designer et Analyzer.
Identity_Manager_4.7_Windows.iso	Contient le serveur Identity Manager (moteur Identity Manager, chargeur distant, agent de dissémination, administration Web d'iManager), les applications d'identité, Identity Reporting, Designer et Analyzer.
Identity_Manager_4.7_Linux_Designer.tar.gz	Contient Designer.
Identity_Manager_4.7_Windows_Designer.zip	Contient Designer.
Identity_Manager_4.7_MacOSX_Designer.tar.gz	Contient les fichiers de Designer pour macOS 10.13 (High Sierra).
Identity_Manager_4.7_Linux_Analyzer.tar.gz	Contient Analyzer.
Identity_Manager_4.7_Windows_Analyzer.zip	Contient analyzer.
SentinelLogManagementForIGA8.1.1.0.tar.gz	Contient Sentinel Log Management for Identity Governance and Administration. Cette installation est prise en charge sous Linux uniquement.

- 1 Accédez au [site Web de téléchargement NetIQ](#).
- 2 Dans le menu **Produit ou Technologie**, sélectionnez Identity Manager, puis cliquez sur **Rechercher**.
- 3 Sur la page des **téléchargements de NetIQ Identity Manager**, cliquez sur le bouton **Télécharger** à côté du fichier à télécharger.
- 4 Suivez les invites à l'écran pour télécharger le fichier dans un répertoire sur votre ordinateur.

4.3 Emplacement des fichiers exécutables et chemins d'installation par défaut

- ♦ [Section 4.3.1, « Fichiers exécutables et chemins d'installation par défaut sous Linux », page 22](#)
- ♦ [Section 4.3.2, « Fichiers exécutables et chemins d'installation par défaut sous Windows », page 22](#)

4.3.1 Fichiers exécutables et chemins d'installation par défaut sous Linux

Composant Identity Manager	Emplacement de l'exécutable dans le fichier ISO	Chemin d'installation par défaut
Serveur Identity Manager (contient le moteur Identity Manager, le chargeur distant, l'agent de dissémination, l'administration Web iManager)	install.sh à l'emplacement monté	<ul style="list-style-type: none"> ♦ Moteur : /opt/novell/eDirectory/lib/dirxml ♦ Chargeur distant : /opt/novell/dirxml/bin/x86_64 ♦ Agent Fan-out : /opt/novell/dirxml/fanoutagent ♦ iManager : var/opt/novell/iManager
Applications d'identité (tableau de bord Identity Manager, interface d'administration Identity Manager, application utilisateur, pilote du service Rôles et ressource, pilote d'application utilisateur, utilitaire de mise à niveau de la configuration)	install.sh à l'emplacement monté	<ul style="list-style-type: none"> ♦ Applications d'identité : /opt/netiq/idm/apps ♦ Application utilisateur : /opt/netiq/idm/apps/UserApplication ♦ Utilitaire de mise à jour de la configuration : /opt/netiq/idm/apps/configupdate
Designer pour Identity Manager	/designer/packages	/root/designer
Identity Reporting	install.sh à l'emplacement monté	/opt/netiq/idm/apps/IDMReporting
Analyser pour Identity Manager	/analyzer/packages	/root/analyzer
Sentinel Log Management for IGA	./install.sh dans le répertoire / SentinelLogManagementforIGA du fichier SentinelLogManagementForIGA8.1.1.0.tar.gz	/opt/novell/sentinel

4.3.2 Fichiers exécutables et chemins d'installation par défaut sous Windows

Composant Identity Manager	Emplacement de l'exécutable dans le fichier ISO	Chemin d'installation par défaut
Coffre-fort d'identité	Setup.exe situé dans \products\eDirectory\x64\	C:\netiq\eDirectory
iManager	<ul style="list-style-type: none"> ♦ Installation des serveurs : iManagerInstall.exe situé dans \products\iManager\installs\win\ ♦ Installation du poste de travail : iManager.bat situé dans imanager\bin 	<ul style="list-style-type: none"> ♦ Installation des serveurs : C:\Program Files\Novell ♦ Installation du poste de travail : C:\Program Files\Novell

Composant Identity Manager	Emplacement de l'exécutable dans le fichier ISO	Chemin d'installation par défaut
Chargeur distant	idm_install.exe situé à l'emplacement \products\IDM\windows\setup	C:\Novell
PostgreSQL et Tomcat (base de données et serveur d'application pris en charge)	TomcatPostgreSQL.exe situé dans products\CommonApplication\postgre_tomcat_install\	C:\netiq\idm\apps\tomcat
Single Sign-on (OSP)	osp_install.exe situé dans \products\CommonApplication\osp_install	C:\netiq\idm\apps\osp
Réinitialisation des mots de passe en self-service (SSPR, Self Service Password Reset)	sspr_install.exe situé dans \products\CommonApplication\sspr_install	C:\netiq\idm\apps\sspr
Applications d'identité	IdmUserApp.exe situé dans products\UserApplication	C:\netiq\idm\apps\UserApplication
Designer pour Identity Manager	install.exe situé dans \products\Designer\	c:\netiq\idm\apps\Designer
Identity Reporting	rpt_install_win.exe situé dans \products\Reporting	C:\netiq\idm\apps\IdentityReporting
Analyser pour Identity Manager	install.exe situé dans \products\Analyzer\	C:\netiq\idm\apps\Analyzer

4.4 Installation de NetIQ Identity Manager 4.7

Selon l'édition que vous installez, passez en revue les informations de l'une des ressources suivantes :

- ♦ Advanced Edition : [Guide d'installation de NetIQ Identity Manager pour Linux](#)) ou [Guide d'installation de NetIQ Identity Manager pour Windows](#))
- ♦ Standard Edition : [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.7 Standard Edition](#) (Guide de démarrage rapide pour l'installation et la mise à niveau de NetIQ Identity Manager 4.7 Standard Edition)

5 Mise à niveau vers NetIQ Identity Manager 4.7

Vous pouvez effectuer la mise à niveau d'Identity Manager vers la version 4.7 à partir des versions 4.6.x et 4.5.6. Avant d'entamer la mise à niveau, NetIQ vous recommande de passer en revue les informations des notes de version relatives à votre version actuelle.

- ♦ [Section 5.1, « Mise à niveau à partir d'Identity Manager 4.6.x », page 24](#)
- ♦ [Section 5.2, « Mise à niveau à partir d'Identity Manager 4.5.6 », page 25](#)
- ♦ [Section 5.3, « Mise à niveau vers l'édition avancée », page 26](#)
- ♦ [Section 5.4, « Mise à niveau vers l'édition standard », page 27](#)

Pour plus d'informations sur la mise à niveau d'Identity Manager, reportez-vous à la section « [Mise à niveau d'Identity Manager](#) » dans le *Guide d'installation de NetIQ Identity Manager pour Linux* ou dans le *Guide d'installation de NetIQ Identity Manager pour Windows*.

5.1 Mise à niveau à partir d'Identity Manager 4.6.x

Le tableau suivant répertorie les chemins de mise à niveau pour les composants Identity Manager :

Composant	Version de base	Remarques
Moteur Identity Manager	4.6.x	<ol style="list-style-type: none"> 1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Effectuez la mise à niveau du moteur Identity Manager vers la version 4.7. <p>REMARQUE : avant d'effectuer la mise à niveau du moteur, assurez-vous que le coffre-fort d'identité est mis à niveau vers la version 9.1.</p>
Chargeur distant	4.6.x	Installez le chargeur distant 4.7.
Agent Fan-out	4.6.x	Installez l'agent de dissémination (fan-out) 4.7.
Designer	4.6.x	<ol style="list-style-type: none"> 1. Installez Designer 4.7. 2. Convertissez votre espace de travail pour travailler avec Designer basé sur LDAP. <p>Avant d'utiliser cette version, reportez-vous aux Notes de version de NetIQ Identity Manager Designer 4.6.</p>
Applications d'identité	4.6.x	<p>Avant d'effectuer la mise à niveau des applications d'identité, assurez-vous que le coffre-fort d'identité et le moteur Identity Manager sont mis à niveau vers les versions 9.1 et 4.7 respectivement.</p> <ol style="list-style-type: none"> 1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à jour les paquetages du pilote d'application utilisateur et du pilote du service Rôles et ressources. 3. Mettez à niveau la base de données vers une version prise en charge (PostgreSQL, Oracle ou MS SQL). 4. (Conditionnel) Si SSPR est installé sur un autre ordinateur, mettez à niveau le composant vers la version 4.7. 5. Arrêtez Tomcat. 6. Mettez à niveau les applications d'identité vers la version 4.7.

Composant	Version de base	Remarques
Identity Reporting	4.6.x	<ol style="list-style-type: none"> 1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à niveau votre base de données vers une version prise en charge (PostgreSQL ou Oracle). 3. Mettez à jour SLM for IGA. 4. Installez Identity Reporting 4.7. 5. Mettez à jour les paquetages du pilote du service de collecte de données et du pilote de passerelle système gérée.

5.2 Mise à niveau à partir d'Identity Manager 4.5.6

Le tableau suivant répertorie les chemins de mise à niveau pour les composants Identity Manager :

Composant	Version de base	Étape intermédiaire	Remarques
Moteur Identity Manager	Identity Manager 4.5.x (où x va de 0 à 5) avec eDirectory 8.8.8.x (où x va de 3 à 9)	Appliquez le service pack Identity Manager 4.5.6.	<ol style="list-style-type: none"> 1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Effectuez la mise à niveau du moteur Identity Manager vers la version 4.7. <p>REMARQUE : avant d'effectuer la mise à niveau du moteur, assurez-vous que le coffre-fort d'identité a été mis à niveau vers la version 9.1.</p>
Chargeur distant	4.5.x		Installez le chargeur distant 4.7.
Agent Fan-out	4.5.x		Installez l'agent de dissémination (fan-out) 4.7.
Designer	4.5.x		<ol style="list-style-type: none"> 1. Installez Designer 4.7. 2. Convertissez votre espace de travail pour qu'il fonctionne avec Designer basé sur LDAP. <p>Avant d'utiliser cette version, reportez-vous aux Notes de version de NetIQ Identity Manager LDAP Designer.</p>

Composant	Version de base	Étape intermédiaire	Remarques
Applications d'identité	4.5.x	Si vous utilisez JBoss ou WebSphere en tant que serveur d'applications, migrez vers le serveur d'applications Tomcat.	<p>Avant d'effectuer la mise à niveau des applications d'identité, assurez-vous que le coffre-fort d'identité et le moteur Identity Manager sont mis à niveau vers les versions 9.1 et 4.7. respectivement.</p> <ol style="list-style-type: none"> 1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à jour les paquetages du pilote d'application utilisateur et du pilote du service Rôles et ressources. 3. Mettez à niveau la base de données vers une version prise en charge (PostgreSQL, Oracle ou MS SQL). 4. (Conditionnel) Si SSPR est installé sur un autre ordinateur, mettez à niveau le composant vers la version 4.7. 5. Arrêtez Tomcat. 6. Mettez à niveau les applications d'identité vers la version 4.7.
Identity Reporting	4.5.x	Si vous utilisez JBoss ou WebSphere en tant que serveur d'applications, migrez vers le serveur d'applications Tomcat.	<ol style="list-style-type: none"> 1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à niveau la base de données vers une version prise en charge. 3. Migrez les données EAS (Event Auditing Service) vers une version prise en charge de la base de données PostgreSQL ou Oracle. 4. Installez SLM for IGA. 5. Installez Identity Reporting 4.7. 6. Exécutez l'utilitaire de synchronisation des données. 7. Mettez à jour les paquetages du pilote du service de collecte de données et du pilote de passerelle système gérée.

5.3 Mise à niveau vers l'édition avancée

NetIQ fournit les chemins de mise à niveau suivants pour la mise à niveau d'une version précédente d'Identity Manager Advanced Edition ou Standard Edition vers Identity Manager 4.6 Advanced Edition :

- ♦ Identity Manager 4.5 Advanced Edition vers Identity Manager 4.6 Advanced Edition

- ♦ Pour mettre à niveau Identity Manager 4.5 Standard Edition vers Identity Manager 4.6 Advanced Edition, procédez de l'une des manières suivantes :
 - ♦ Identity Manager 4.5 Standard Edition vers Identity Manager 4.6 Standard Edition, puis vers Identity Manager 4.7 Advanced Edition
 - ♦ Identity Manager 4.5 Standard Edition vers Identity Manager 4.6 Advanced Edition, puis vers Identity Manager 4.7 Advanced Edition

5.4 Mise à niveau vers l'édition standard

Vous pouvez effectuer la mise à niveau vers Identity Manager 4.7 Standard Edition à partir d'Identity Manager 4.6 Standard Edition. Si vous procédez à une mise à niveau à partir d'une version antérieure à Identity Manager 4.6, vous devez migrer Identity Reporting depuis votre serveur d'applications existant vers Tomcat sur les plates-formes Linux et Windows. Pour des instructions de mise à niveau, consultez le [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.6 Standard Edition](#) (Guide de démarrage rapide pour l'installation et la mise à niveau de NetIQ Identity Manager 4.6 Standard Edition).

Identity Manager 4.7 Standard Edition prend toujours en charge les rapports suivants :

- ♦ Authentification par l'utilisateur
- ♦ Authentification par le serveur
- ♦ Statistiques de la base de données
- ♦ Modifications de mots de passe par l'utilisateur
- ♦ Réinitialisation de mot de passe
- ♦ État actuel du rapport d'associations du pilote du coffre-fort d'identité
- ♦ État actuel du rapport sur les utilisateurs du coffre-fort d'identité
- ♦ Résumé des événements de changement de mot de passe utilisateur

Pour plus d'informations, reportez-vous au [Administrator Guide to NetIQ Identity Reporting](#) (Guide de l'administrateur de NetIQ Identity Reporting).

IMPORTANT : pour utiliser les rapports, importez les définitions de rapport dans Identity Reporting. Connectez-vous à l'application de création de rapports et utilisez la page de **téléchargement** dans l'application afin de télécharger les rapports.

6 Problèmes connus

NetIQ s'efforce de garantir que ses produits offrent des solutions de qualité qui répondent aux besoins logiciels de votre entreprise. Les problèmes suivants font actuellement l'objet de recherches visant à établir des solutions. Si vous avez besoin d'aide pour résoudre un problème, contactez le [support technique](#).

- ♦ [Section 6.1, « Problèmes d'installation », page 28](#)
- ♦ [Section 6.2, « Problèmes liés au moteur Identity Manager », page 30](#)
- ♦ [Section 6.3, « Problèmes liés au chargeur distant », page 31](#)
- ♦ [Section 6.4, « Problèmes relatifs aux pilotes », page 33](#)
- ♦ [Section 6.5, « Problèmes liés aux applications d'identité », page 34](#)
- ♦ [Section 6.6, « Problèmes liés à Identity Reporting », page 41](#)
- ♦ [Section 6.7, « Problèmes liés au plug-in iManager », page 43](#)

- ♦ Section 6.8, « Problèmes de mise à niveau d'Identity Manager », page 43
- ♦ Section 6.9, « Problèmes liés à la localisation », page 45
- ♦ Section 6.10, « Problèmes de désinstallation », page 47

6.1 Problèmes d'installation

- ♦ Section 6.1.1, « L'option Démarrage pour la création de la base de données de création de rapports manquante signale une exception après la configuration sous Linux », page 28
- ♦ Section 6.1.2, « La source de données n'est pas ajoutée à la page de l'application de création de rapports lorsque le schéma de base de données est créé pendant l'installation d'Identity Reporting avec la base de données Oracle sous Windows », page 28
- ♦ Section 6.1.3, « Impossibilité de spécifier des chemins d'installation sous Windows comportant des espaces », page 29
- ♦ Section 6.1.4, « Impossible de redémarrer Tomcat à l'aide du gestionnaire de tâches sous Windows », page 29
- ♦ Section 6.1.5, « Le serveur LDAP affiche une erreur lors de l'utilisation des contrôles VLV et SSS », page 29
- ♦ Section 6.1.6, « Les tables ne sont pas créées si l'utilitaire ConfigUpdate est lancé juste après l'installation des applications d'identité », page 29
- ♦ Section 6.1.7, « Certains assistants d'installation affichent une icône incorrecte pour les composants », page 30
- ♦ Section 6.1.8, « Le panneau de navigation est tronqué dans le programme d'installation d'Identity Reporting sous Windows », page 30

6.1.1 L'option Démarrage pour la création de la base de données de création de rapports manquante signale une exception après la configuration sous Linux

Problème : Si vous installez Identity Reporting sur le même serveur que celui sur lequel les applications d'identité sont installées et que vous choisissez l'option de création de base de données **Démarrage** au cours de l'installation d'Identity Reporting, le script de configuration signale certaines exceptions dans le journal. (Bogue 1082959)

Solution : Effacez les exceptions en redémarrant manuellement Tomcat. Cela n'a aucun impact sur l'installation. Vous pouvez ignorer l'exception en toute sécurité.

6.1.2 La source de données n'est pas ajoutée à la page de l'application de création de rapports lorsque le schéma de base de données est créé pendant l'installation d'Identity Reporting avec la base de données Oracle sous Windows

Problème : Après l'installation et la configuration d'Identity Reporting, lorsque vous vous connectez à l'application de création de rapports, la source de données n'est pas disponible dans l'application. (Bogue 1082990)

L'erreur suivante est consignée dans le fichier `catalina.out` :

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

Solution : Après avoir terminé la configuration d'Identity Reporting, ajoutez manuellement la source de données à l'application de création de rapports.

- 1 Connectez-vous à Identity Reporting.
- 2 Cliquez sur **Sources de données > Ajouter**.
- 3 Dans **Ajouter une source de données**, cliquez sur **Effectuez la sélection à partir d'une liste prédéfinie**.
- 4 Sélectionnez la source **IDMDCSDataSource** et renommez-la `IDMDCSDataSource`.
Le bouton Enregistrer est activé uniquement lorsqu'un nom est spécifié.
- 5 Cliquez sur **Enregistrer**.

6.1.3 Impossibilité de spécifier des chemins d'installation sous Windows comportant des espaces

Les programmes d'installation des composants Identity Manager risquent de ne pas placer les fichiers d'installation à l'emplacement spécifié si le chemin contient des espaces. Veillez à ce que le chemin spécifié ne comporte aucun espace. (Bogue 620797)

6.1.4 Impossible de redémarrer Tomcat à l'aide du gestionnaire de tâches sous Windows

Problème : Vous ne pouvez pas utiliser le gestionnaire des tâches pour redémarrer Tomcat sur un serveur Windows. (Bogue 893155)

Solution : Utilisez l'une des méthodes suivantes pour redémarrer Tomcat :

- ♦ Dans le panneau de configuration Services, cliquez avec le bouton droit sur **IDM Apps Tomcat Service**, puis cliquez sur **Redémarrer**.
- ♦ Utilisez l'invite de commandes pour arrêter, puis redémarrer Tomcat :

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

ou

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

6.1.5 Le serveur LDAP affiche une erreur lors de l'utilisation des contrôles VLV et SSS

Problème : Lorsque vous configurez une recherche LDAP pour qu'elle utilise les commandes d'affichage de la liste virtuelle (VLV) et de tri côté serveur (SSS) et que le serveur LDAP ne contient aucune copie locale des objets Utilisateur, la recherche échoue et affiche une erreur.

Solution : Stockez les objets Utilisateur dans votre réplique locale pour pouvoir utiliser les commandes VLV et SSS. Pour plus d'informations, reportez-vous au document TID [7001493](#).

6.1.6 Les tables ne sont pas créées si l'utilitaire ConfigUpdate est lancé juste après l'installation des applications d'identité

Problème : Lors de l'installation des applications d'identité, si vous sélectionnez l'option de création des tables au démarrage sans démarrer l'application, mais que vous lancez à la place l'utilitaire configupdate et que vous cliquez sur OK, le paramètre `com.netiq.idm.create-db-on-startup` est

défini sur `false`. Étant donné qu'en réalité, vous n'avez pas lancé l'application, les tables ne sont pas créées. Ce problème entraîne l'échec du démarrage étant donné que les tables n'existent pas.
(Bogue 900284)

Solution : Ouvrez le fichier `ism-configuration.properties`, changez la valeur `false` en `true`, enregistrez le fichier, puis redémarrez l'application.

6.1.7 Certains assistants d'installation affichent une icône incorrecte pour les composants

Problème : Fourni par commodité, le programme d'installation de Tomcat et de PostgreSQL affiche une icône Java au lieu d'afficher une icône pour les composants Tomcat et PostgreSQL. Ce problème a également été observé dans OSP (One SSO Provider).

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.1.8 Le panneau de navigation est tronqué dans le programme d'installation d'Identity Reporting sous Windows

Problème : Dans certaines langues, le panneau de navigation qui s'affiche à gauche du programme d'installation d'Identity Reporting apparaît tronqué. Il se peut que tous les noms ne s'affichent pas sur le panneau de navigation. (Bogue 899888)

Solution : Vous pouvez sans problème ignorer le panneau de navigation tronqué et poursuivre l'installation.

6.2 Problèmes liés au moteur Identity Manager

- ♦ [Section 6.2.1, « Impossibilité d'exécuter des scripts ECMA volumineux », page 30](#)
- ♦ [Section 6.2.2, « L'augmentation de longueur de la valeur de l'attribut OSP provoque des problèmes de connexion », page 30](#)
- ♦ [Section 6.2.3, « Échec de l'ajout de plusieurs valeurs de droit à une ressource statique », page 31](#)

6.2.1 Impossibilité d'exécuter des scripts ECMA volumineux

Problème : Ce problème est dû au fait que le moteur Rhino n'est pas en mesure d'analyser des scripts très volumineux. (Bogues 1016963, 942241)

Solution : Identity Manager 4.6 prend en charge le moteur du script ECMAScript Nashorn. Utilisez ce moteur de script pour exécuter des scripts ECMA volumineux. Pour plus d'informations, reportez-vous à la section « [Engine Control Values](#) » (Valeurs de contrôle du moteur) du *NetIQ Identity Manager Driver Administration Guide* (Guide d'administration des pilotes de NetIQ Identity Manager).

Pour plus d'informations à propos du déplacement du moteur de script Nashorn, reportez-vous au *Rhino Migration Guide* (Guide de migration de Rhino).

6.2.2 L'augmentation de longueur de la valeur de l'attribut OSP provoque des problèmes de connexion

Problème : Si vous ne vous déconnectez pas après chaque connexion réussie aux applications d'identité, la valeur de l'attribut OSP augmente progressivement après plusieurs connexions. Une valeur devenant trop longue entraîne des problèmes de connexion.

Solution : Effectuez l'une des opérations suivantes :

Effacez manuellement la valeur de l'attribut OSP dans iManager.

- 1 Connectez-vous à iManager.
- 2 Dans **Afficher les objets**, sélectionnez l'objet Utilisateur.
- 3 Sous l'onglet **Autre**, double-cliquez sur l'attribut **oidInstanceData** et effacez la valeur.

Ou

Réduisez la valeur de durée de vie du jeton de rafraîchissement à l'aide de l'utilitaire ConfigUpdate :

- 1 Lancez l'utilitaire ConfigUpdate.
- 2 Sélectionnez l'onglet **Authentification**.
- 3 Dans **Configuration de l'authentification**, diminuez la valeur **Durée de vie du jeton de rafraîchissement (en heures)**.

Par défaut, la valeur **Durée de vie du jeton de rafraîchissement (en heures)** est définie sur 48 heures.

6.2.3 Échec de l'ajout de plusieurs valeurs de droit à une ressource statique

Problème : Lorsque vous créez une ressource statique avec plusieurs valeurs de droit à l'aide du jeton `do-create-resource`, le moteur Identity Manager ne crée qu'un seul objet `nrfEntitlementRef` pour la ressource. Par conséquent, vous ne pouvez pas créer de ressources statiques avec plusieurs valeurs d'assignation à l'aide de ce jeton. (Bogue 995486)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.3 Problèmes liés au chargeur distant

- ♦ [Section 6.3.1, « Impossible de générer des événements Novell Audit pour des chargeurs distants 32 et 64 bits hébergés sur le même serveur », page 31](#)
- ♦ [Section 6.3.2, « La clé de mot de passe spécifiée côté chargeur distant n'est pas validée à l'aide de l'authentification mutuelle », page 31](#)
- ♦ [Section 6.3.3, « L'instance de pilote du chargeur distant configuré pour l'authentification mutuelle ne démarre pas », page 32](#)

6.3.1 Impossible de générer des événements Novell Audit pour des chargeurs distants 32 et 64 bits hébergés sur le même serveur

Problème : Bien qu'il soit possible d'installer un chargeur distant de 32 bits et un autre de 64 bits sur le même ordinateur, les fichiers `lcache` de ces versions ne peuvent pas fonctionner simultanément. Les événements Novell Audit sont consignés dans le fichier `lcache` pour la version installée en premier. Le fichier journal de l'autre version affiche un message indiquant une erreur relative à un agent déjà en cours d'exécution. (Bogue 676310)

Solution : N'installez pas les deux versions sur le même ordinateur.

6.3.2 La clé de mot de passe spécifiée côté chargeur distant n'est pas validée à l'aide de l'authentification mutuelle

Problème : L'outil `dxcmd` génère le fichier `PEM` pour une clé privée sans mot de passe de chiffrement. Par conséquent, Identity Manager établit la connexion entre le chargeur distant et le moteur sans valider le mot de passe de chiffrement (mot de passe de clé). (Bogue 1077147)

Solution : Vous devez créer un KMO client à l'aide d'iManager avec un mot de passe codé. Générez `keyfile.pem` à partir de ce KMO et remplacez le fichier `keyfile.pem` existant comme suit :

- 1 Connectez-vous à iManager.
- 2 Créez un KMO pour une authentification client au format `.pfx` :
 - 2a Accédez à **Rôles et tâches > Accès aux certificats NetIQ > Certificats de serveur**.
 - 2b Cliquez sur **Nouveau**, spécifiez le **Surnom** de votre certificat.
 - 2c Sélectionnez **Personnalisé** comme méthode de création, puis cliquez sur **Suivant**. Cette option permet de définir les paramètres du certificat.
 - 2d Sélectionnez **Autorité de certification organisationnelle**, puis cliquez sur **Suivant**.
 - 2e Dans **Activer l'utilisation de la clé étendue**, sélectionnez **Utilisateur**, puis cliquez sur **Suivant**.
 - 2f Sélectionnez **Période de validité** dans la liste et cliquez sur **Suivant**.
 - 2g Sélectionnez **Certificat de votre organisation**, puis cliquez sur **Suivant**.
 - 2h Cliquez sur **Terminer**.
- 3 Sélectionnez le certificat qui vient d'être créé, puis cliquez sur **Valider**.
- 4 Sélectionnez le KMO client et cliquez sur **Exporter**.

REMARQUE : dans iManager, le KMO est exporté au format `.pfx`.

- 5 Convertissez le KMO client exporté du format `.pfx` vers le format `.pem` à l'aide de la commande suivante :

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

Exemples :

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

- 6 Remplacez `keyfile.pem` par `client_cert.pem`.

6.3.3 L'instance de pilote du chargeur distant configuré pour l'authentification mutuelle ne démarre pas

Problème : Après la mise à niveau du chargeur distant 32 ou 64 bits, un pilote pour lequel l'authentification mutuelle est activée ne parvient pas à démarrer l'instance du chargeur distant. (Bogue 1082989)

Solution : Après la mise à niveau du chargeur distant, procédez comme suit :

- 1 Éditez l'instance du chargeur distant, indiquez le même mot de passe de clé que celui défini avant la mise à niveau du chargeur distant.
Le mot de passe de clé par défaut est `dirxml`.
- 2 Enregistrez la configuration.
- 3 Démarrez l'instance du pilote de chargeur distant.

6.4 Problèmes relatifs aux pilotes

Lors de l'utilisation des pilotes Identity Manager, vous risquez de rencontrer les problèmes suivants :

- ♦ [Section 6.4.1, « Le rapport statistique affiche zéro pour les valeurs Rôle et Licence d'un pilote Office 365 », page 33](#)
- ♦ [Section 6.4.2, « L'instance de chargeur distant d'un pilote peut ne pas démarrer si la largeur par défaut de la fenêtre d'invite de commandes Windows a été modifiée », page 33](#)
- ♦ [Section 6.4.3, « La requête dxcmd avec sortie volumineuse est exécutée deux fois », page 33](#)
- ♦ [Section 6.4.4, « Problème d'ajout d'une entrée aux comptes DirXML lors de la migration d'un utilisateur », page 33](#)
- ♦ [Section 6.4.5, « L'inspecteur de cache de pilote ne peut pas afficher la dernière entrée dans la liste de cache », page 34](#)
- ♦ [Section 6.4.6, « Le pilote Remedy ne démarre pas lorsqu'il est exécuté en local avec le moteur Identity Manager », page 34](#)

6.4.1 Le rapport statistique affiche zéro pour les valeurs Rôle et Licence d'un pilote Office 365

Problème : Le rapport statistique concernant un pilote Office 365 affiche zéro pour les valeurs **Rôle** et **Licence** dans la section **Droits assignés par type** en raison d'une limite du pilote Office 365. (Bogue 893248)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.4.2 L'instance de chargeur distant d'un pilote peut ne pas démarrer si la largeur par défaut de la fenêtre d'invite de commandes Windows a été modifiée

Problème : Si vous définissez la largeur de la fenêtre d'invite de commandes Windows sur une valeur autre que celle par défaut, il se peut que l'instance du pilote ne démarre pas et n'enregistre pas les informations de trace. (Bogue 854488)

Solution : Réinitialisez la largeur de la fenêtre d'invite de commandes Windows sur la valeur par défaut 80.

6.4.3 La requête dxcmd avec sortie volumineuse est exécutée deux fois

Problème : Lorsque vous envoyez une commande `dxcmd` à un pilote pour qu'il traite une requête, le moteur Identity Manager patiente par défaut pendant 120 secondes pour obtenir une réponse du pilote. En l'absence de réponse, le moteur réexécute la requête après le timeout. S'il ne reçoit toujours aucune réponse au bout des 120 secondes supplémentaires, il affiche l'erreur `ERR_TRANSPORT_FAILURE`. Autrement dit, le pilote traite ainsi la requête deux fois. (Bogue 1014581)

Solution : Définissez la **variable d'environnement** `NCPCLIENT_REQ_TIMEOUT` sur une valeur supérieure au délai attendu pour exécuter la requête.

6.4.4 Problème d'ajout d'une entrée aux comptes DirXML lors de la migration d'un utilisateur

Problème : Lorsqu'un utilisateur est migré à partir du coffre-fort d'identité à l'aide d'un pilote sans paquetages de droits, Identity Manager n'indique aucune valeur pour l'attribut `DirXML-comptes` de l'utilisateur. Ce problème se produit lorsque les informations de l'utilisateur sont identiques dans une application connectée et dans le coffre-fort d'identité. (Bogue 1016682)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.4.5 L'inspecteur de cache de pilote ne peut pas afficher la dernière entrée dans la liste de cache

Problème : Dans les navigateurs Web tels que Google Chrome, Mozilla Firefox et Microsoft Edge, l'inspecteur de cache du pilote n'affiche pas de la dernière entrée dans la liste de cache du pilote.

Solution : Procédez comme suit :

- 1 Développez toutes les entrées de cache de la liste en sélectionnant **Opérations > Tout développer** à partir du menu principal.
- 2 Utilisez les flèches du clavier pour naviguer à travers les entrées développées de la liste.

6.4.6 Le pilote Remedy ne démarre pas lorsqu'il est exécuté en local avec le moteur Identity Manager

Problème : Lorsque le pilote est configuré pour s'exécuter en local avec le moteur Identity Manager, le pilote ne parvient pas à démarrer en raison d'un conflit avec une API JAXB incluse dans le fichier `activemq-tout-5.15.2.jar` et indique le message d'erreur suivant dans la trace :

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

Solution : Procédez comme suit :

- 1 Installez le pilote avec le chargeur distant.
- 2 Supprimez le fichier `activemq-tout-5.15.2.jar` du dossier `lib` dans le répertoire d'installation du chargeur distant.
- 3 Démarrez le pilote.

6.5 Problèmes liés aux applications d'identité

Vous pouvez rencontrer les problèmes suivants lorsque vous utilisez les applications d'identité, notamment le tableau de bord, l'administrateur des applications d'identité et l'Application utilisateur :

- ♦ [Section 6.5.1, « Erreur signalée si différentes bases de données sont configurées pour des instances des applications d'identité et d'Identity Reporting installées sur le même serveur », page 35](#)
- ♦ [Section 6.5.2, « Indication d'une taille nulle pour les journaux archivés à partir du fichier `catalina.out` malgré le remplacement des journaux », page 35](#)
- ♦ [Section 6.5.3, « La page Révoquer l'autorisation répertorie à tort des autorisations de personnes tierces pour l'administrateur de rôles et l'administrateur de rôles délégués », page 36](#)
- ♦ [Section 6.5.4, « Le tableau de bord affiche une valeur erronée pour le nombre total d'utilisateurs », page 37](#)
- ♦ [Section 6.5.5, « Les fenêtres contextuelles peuvent afficher du contenu dans plusieurs langues : celle par défaut du client et celle du navigateur », page 37](#)
- ♦ [Section 6.5.6, « Les libellés de champ des formulaires des workflows de requête et d'approbation sont alignés à droite », page 37](#)
- ♦ [Section 6.5.7, « Le navigateur à restriction CLE bloque l'accès à la page des mots de passe oubliés », page 37](#)

- ♦ Section 6.5.8, « Impossible d'approuver ou de refuser une requête de rôle après la suppression de ce dernier », page 38
- ♦ Section 6.5.9, « Échec du module de provisioning basé sur les rôles lors de la création et de la copie du paquetage de base des pilotes de l'application utilisateur », page 38
- ♦ Section 6.5.10, « Impossibilité d'utiliser < comme premier caractère du mot de passe du compte de l'application utilisateur », page 38
- ♦ Section 6.5.11, « Les workflows renvoient une erreur en cas d'utilisation de dateToString pour le contrôle du tampon horaire », page 38
- ♦ Section 6.5.12, « Les éléments de navigation de l'application utilisateur ne s'affichent pas en cas d'utilisation de Safari sur un iPad », page 39
- ♦ Section 6.5.13, « La feuille CSS personnalisée ne se synchronise pas avec les noeuds de grappe », page 39
- ♦ Section 6.5.14, « Exception ClientAbortException lors de la déconnexion des applications utilisateur sous Windows », page 39
- ♦ Section 6.5.15, « Impossible de modifier le mot de passe à l'aide du tableau de bord Identity Manager », page 40
- ♦ Section 6.5.16, « Les widgets du tableau de bord par défaut ne parviennent pas à charger l'information de widget sur le tableau de bord après mise à niveau », page 40
- ♦ Section 6.5.17, « Le bouton de déconnexion du tableau de bord peut ne pas fonctionner », page 41
- ♦ Section 6.5.18, « La suppression d'un rôle enfant nécessite de cliquer sur la description ou la description d'assignation de ce dernier », page 41

6.5.1 Erreur signalée si différentes bases de données sont configurées pour des instances des applications d'identité et d'Identity Reporting installées sur le même serveur

Problème : Identity Manager ne prend pas en charge l'utilisation de bases de données différentes pour les composants Applications d'identité et Identity Reporting installés sur le même serveur. Par exemple, vous ne pouvez pas utiliser une base de données PostgreSQL installée sur le même serveur pour les applications d'identité et faire pointer Identity Reporting vers une base de données Oracle à distance. Cela provoque des exceptions dans le fichier `catalina_<date>.log`. (Bogue 1079738)

Solution : Pour utiliser des bases de données différentes pour les applications d'identité et Identity Reporting, installez les composants sur des serveurs distincts.

6.5.2 Indication d'une taille nulle pour les journaux archivés à partir du fichier `catalina.out` malgré le remplacement des journaux

Problème : La taille de fichier archivée indique une valeur zéro. (Bogue 1044488)

Solution : Procédez comme suit :

- 1 Arrêtez le service Tomcat. Par exemple, exécutez la commande suivante à partir d'une invite de commandes :

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

- 2 Accédez au répertoire `Tomcat/conf`. Par exemple : `/opt/netiq/idm/apps/tomcat/conf`.

3 Modifier le fichier userapp-log4j.xml dans un éditeur de texte.

3a Ajoutez les entrées suivantes pour les appenders de journal après la section Catalina Appender.

```
<!-- 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 Ajoutez l'entrée `<appender-ref ref="CATALINALOG"/>` sous la section `<root>` avant la section `</log4j:configuration>`.

La section doit ressembler à ceci :

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

4 Démarrez le service Tomcat.

6.5.3 La page Révoquer l'autorisation répertorie à tort des autorisations de personnes tierces pour l'administrateur de rôles et l'administrateur de rôles délégués

Problème : Si vous vous connectez au tableau de bord en tant qu'administrateur de rôles ou administrateur de rôles délégués, la page Autres (**Accès > Autorisations > Révoquer l'autorisation > Autres**) répertorie les autorisations d'utilisateur qui sont en dehors de votre domaine ou étendue.

- ♦ Pour un administrateur de rôles, le tableau de bord répertorie les ressources d'utilisateurs qui ne font pas partie du domaine de l'administrateur.
- ♦ Pour un administrateur de rôles délégués, le tableau de bord répertorie tous les rôles et ressources des utilisateurs qui ne sont pas délégués. (Bogue 1079043)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.5.4 Le tableau de bord affiche une valeur erronée pour le nombre total d'utilisateurs

Problème : Les problèmes suivants sont signalés :

- ◆ Lorsque vous ajoutez des utilisateurs et rafraîchissez immédiatement l'affichage, le tableau de bord répertorie les nouveaux utilisateurs, mais ne met pas à jour le nombre total d'utilisateurs. Le nombre total mis à jour d'utilisateurs s'affiche toutefois correctement si vous rafraîchissez l'affichage après quelques secondes.
- ◆ Si un utilisateur possède plusieurs valeurs pour le nom donné ou sn, le tableau de bord affiche des valeurs différentes pour le nombre de recherches et le nombre total. (Bogue 1006448)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.5.5 Les fenêtres contextuelles peuvent afficher du contenu dans plusieurs langues : celle par défaut du client et celle du navigateur

Problème : Lorsque vous effectuez une opération qui ouvre une fenêtre contextuelle, le tableau de bord peut afficher une partie du contenu de la fenêtre dans la langue du client au lieu de celle du navigateur. Par exemple, l'affichage des détails d'une tâche ouvre une fenêtre contextuelle. Ce problème se produit dans les navigateurs Microsoft Internet Explorer ou Edge après que l'utilisateur a remplacé la langue du navigateur par une langue qui n'est pas celle du client par défaut. (Bogue 1019020)

Solution : Après avoir modifié la langue du navigateur, fermez l'onglet actif. Ouvrez ensuite un nouvel onglet pour vous connecter au tableau de bord.

6.5.6 Les libellés de champ des formulaires des workflows de requête et d'approbation sont alignés à droite

Problème : Lors de l'accès aux formulaires de requête et d'approbation dans le tableau de bord, les libellés de champ des formulaires sont alignés à droite. (Bogue 921403)

Solution : Pour aligner les libellés de champ de formulaire des workflows de requête et d'approbation à gauche, ajoutez l'instruction suivante à l'événement onload de chaque formulaire :

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

6.5.7 Le navigateur à restriction CLE bloque l'accès à la page des mots de passe oubliés

Problème : Si vous limitez l'accès aux sites Web, mais que vous mettez sur liste blanche la page de renvoi des applications d'identité, le navigateur à restriction CLE peut bloquer l'accès à la page des mots de passe oubliés pour la réinitialisation de mot de passe en self-service. Les utilisateurs voient alors le message d'erreur suivant :

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

(Bogue 1021647)

Solution : Dans la liste blanche, ajoutez l'URL vers la page des mots de passe oubliés.

De même, si vous effectuez la mise à niveau à partir d'Identity Manager 4.5, mettez à jour le lien vers la page de renvoi afin de diriger les utilisateurs vers le nouveau tableau de bord (/idmdash/#/landing) au lieu de la page d'accueil (/landing) d'Identity Manager dans la section URL de redirection SSPR.

6.5.8 Impossible d'approuver ou de refuser une requête de rôle après la suppression de ce dernier

Problème : Si un administrateur supprime un rôle qui nécessite un workflow après qu'un utilisateur a effectué une requête de rôle, le destinataire du workflow pour la requête de rôle le voit toujours s'afficher dans la liste des tâches et peut approuver ou refuser la requête. (Bogue 752860)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.5.9 Échec du module de provisioning basé sur les rôles lors de la création et de la copie du paquetage de base des pilotes de l'application utilisateur

Problème : Lorsque vous effectuez certaines opérations sur le paquetage de base de l'application utilisateur que vous avez créé, par exemple, supprimer l'objet Configuration de rôle, RBPM échoue. (Bogue 879595)

Solution : NetIQ recommande de ne pas créer ni copier le paquetage de base du pilote d'application utilisateur.

6.5.10 Impossibilité d'utiliser < comme premier caractère du mot de passe du compte de l'application utilisateur

Problème : Vous ne pouvez pas utiliser le caractère spécial < comme premier caractère dans un mot de passe de l'application utilisateur. Par exemple, <testing12. Le navigateur interprète le mot de passe comme un texte HTML au format incorrect et l'utilisateur ne peut pas se connecter. (Bogue 759297)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.5.11 Les workflows renvoient une erreur en cas d'utilisation de `dateToString` pour le contrôle du tampon horaire

Problème : Les workflows que vous avez créé dans l'application utilisateur et qui utilisent la méthode de script de formulaire `dateToString` pour un tampon horaire ne fonctionnent pas correctement dans le composant Accueil d'Identity Manager. Le script de formulaire `dateToString` dans l'API comprend des secondes, alors que le contrôle de la date et de l'heure dans le composant Accueil d'Identity Manager n'en a pas. Le nouveau script utilise un format différent. Pour vous assurer que vos formulaires fonctionnent avec la page d'accueil d'Identity Manager, vous devez remplacer `dateToString` par le nouveau script : `new Date ().toString ('Date.CultureInfo.formatPatterns.shortDate+' '+Date.CultureInfo.formatPatterns.shortTime')`.

Solution : Pour remplacer le contrôle d'une date unique dans votre formulaire, vous pouvez utiliser le code suivant :

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

Cependant, il peut être nécessaire de remplacer des contrôles qui représentent deux dates. Par exemple, vous pouvez avoir un formulaire nécessitant que l'utilisateur indique une heure de début et de fin pour une requête de droit.

Pour spécifier une date de début `startDate`, utilisez le type de code suivant :

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

Pour spécifier une date de fin `endDate` qui intervient trois jours après la date de début, utilisez le type de code suivant :

```
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');
```

Dans cet exemple, le workflow répond avec les informations suivantes:

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

REMARQUE : dans les codes ci-dessus, si vous souhaitez utiliser uniquement **DatePicker** dans votre formulaire, vous pouvez exclure `'Date.CultureInfo.formatPatterns.shortTime'` du code.

Par exemple, si vous souhaitez spécifier uniquement une date pour `startDate`, vous pouvez utiliser le type de code suivant :

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

6.5.12 Les éléments de navigation de l'application utilisateur ne s'affichent pas en cas d'utilisation de Safari sur un iPad

Problème : Si vous exécutez l'application utilisateur à l'aide de Safari sur un iPad en orientation portrait, les éléments de navigation de l'en-tête ne s'affichent pas toujours correctement.

Solution : Pour afficher l'élément de navigation de l'en-tête, sélectionnez un élément de navigation sur la gauche.

6.5.13 La feuille CSS personnalisée ne se synchronise pas avec les noeuds de grappe

Problème : Dans le tableau de bord Identity Manager, lorsque vous téléchargez la feuille CSS personnalisée dans la grappe, les modifications CSS ne sont pas appliquées à tous les noeuds de la grappe. (1025836)

Solution : Veillez à ce que chaque noeud de la grappe dispose de la même copie de CSS à l'emplacement suivant :

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

6.5.14 Exception ClientAbortException lors de la déconnexion des applications utilisateur sous Windows

Problème : Si vous tentez d'obtenir une liste des utilisateurs soit en sélectionnant **Tableau de bord Identity Manager > Personnes > Utilisateurs** ou en sélectionnant **Gérer les utilisateurs**, puis que vous vous déconnectez des applications d'identité avant que le tableau de bord affiche le nombre

total d'utilisateurs dans le navigateur, ce processus génère une exception `ClientAbortException` dans le fichier `catalina.out`. Cette exception peut également se produire dans les cas suivants lorsque vous employez les applications d'identité :

- ♦ La fenêtre du navigateur se ferme.
- ♦ Le réseau est déconnecté.
- ♦ La session a expiré.

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème. Vous pouvez ignorer cette exception dans la mesure où elle ne provoque aucune perte de fonctionnalité.

6.5.15 Impossible de modifier le mot de passe à l'aide du tableau de bord Identity Manager

Problème : Si vous avez installé SSPR et les applications d'identité sur des serveurs distincts et avez essayé de modifier le mot de passe sur la page **Applications**, les applications d'identité affichent l'erreur `Page non trouvée`. (Bogue 1077395)

Solution : Indiquez l'adresse IP du réseau du serveur SSPR dans **Modifier mon mot de passe** sur la page **Applications**.

- 1 Connectez-vous à votre tableau de bord Identity Manager en tant qu'administrateur.

`https://<adresse_IP_applications_identité:Port>/idmdash`

- 2 Accédez à **Applications**, cliquez sur .

- 3 Dans **Modifier mon mot de passe**, cliquez sur .

- 4 Dans **Lien**, indiquez l'adresse du serveur SSPR.

`https://<adresse_IP_SSPR:port>//sspr/private/ChangePassword`

- 5 Cliquez sur **Enregistrer**.

6.5.16 Les widgets du tableau de bord par défaut ne parviennent pas à charger l'information de widget sur le tableau de bord après mise à niveau

Problème : Si vous avez défini un nom de contexte autre que `IDMProv`, les widgets de tableau de bord par défaut qui utilisent des API REST n'obtiennent pas les informations de widget des applications d'identité. (Bogue 1080591)

Solution : Modifiez le nom de contexte des widgets qui utilisent des API REST :

- 1 Dans **Tableau de bord**, cliquez sur  et sélectionnez **Widgets**.
- 2 Cliquez sur  sur un widget dont vous souhaitez modifier le nom de contexte.
- 3 Dans **URL**, remplacez `/IDMProv` par `<nom_contexte_défini>`.

Par exemple, dans l'URL suivante,

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

remplacez `/IDMProv` par `/IDMProv_new`.

6.5.17 Le bouton de déconnexion du tableau de bord peut ne pas fonctionner

Problème : Parfois, les applications d'identité ne vous dirigent pas vers la page de connexion lorsque vous cliquez sur le bouton Déconnexion du tableau de bord. (Bogue 1082178)

Solution : Effectuez l'une des opérations suivantes :

- 1 Rafraîchissez la page Tableau de bord.
- 2 Accédez à une autre application (par exemple, l'administration de rôles ou IDMProv) et déconnectez-vous de cette page d'application.

6.5.18 La suppression d'un rôle enfant nécessite de cliquer sur la description ou la description d'assignation de ce dernier

Problème : La nouvelle interface utilisateur Applications d'identité affiche la liste des rôles parents et enfants dans la page Détails du rôle. Cette page ne permet pas de sélectionner un rôle enfant en sélectionnant son nom, mais elle affiche des informations rapides sur le rôle enfant. (Bogue 1082533)

Solution : Pour supprimer un rôle enfant, cliquez sur la description ou la description d'assignation de ce dernier. Pour supprimer plusieurs rôles enfants, maintenez la touche `Ctrl` enfoncée et cliquez sur la description ou la description d'assignation des rôles sélectionnés.

6.6 Problèmes liés à Identity Reporting

Lors de l'utilisation d'Identity Reporting, vous risquez de rencontrer les problèmes suivants :

- ♦ [Section 6.6.1, « Impossible de modifier la fréquence d'une planification », page 41](#)
- ♦ [Section 6.6.2, « Les pages Identity Reporting et Services de collecte de données ne parviennent pas à lancer les applications d'identité », page 41](#)
- ♦ [Section 6.6.3, « L'aide de la page de collecte de données pour des paramètres régionaux autres que l'anglais renvoie vers l'Aide en anglais », page 42](#)
- ♦ [Section 6.6.4, « La page Services de collecte de données d'Identity Manager ne s'affiche pas dans l'édition Standard sous Linux », page 42](#)

6.6.1 Impossible de modifier la fréquence d'une planification

Problème : Vous ne pouvez pas modifier la fréquence d'une planification. Par exemple, de semaine à mois. (Bogue 677430)

Solution : Pour modifier la fréquence, supprimez la planification et créez-en une nouvelle.

6.6.2 Les pages Identity Reporting et Services de collecte de données ne parviennent pas à lancer les applications d'identité

Problème : Ce problème se produit après la mise à niveau d'Identity Manager vers la version la plus récente. Lorsque vous cliquez sur **Accueil** à partir de l'interface utilisateur d'Identity Reporting ou des services de collecte de données qui sont installés sur d'autres serveurs que ceux utilisés pour les applications d'identité, ces dernières ne se lancent pas. En revanche, l'erreur `Page non trouvée` s'affiche. (Bogue 1080514)

Solution : Pour modifier l'URL de renvoi pour Identity Reporting, mettez à jour manuellement l'utilitaire `configupdate` avec l'URL du tableau de bord Identity Manager :

- 1 Lancez l'utilitaire `configupdate`.

Par défaut, cet utilitaire se trouve dans /opt/netiq/idm/apps/configupdate.

2 Accédez à **Clients SSO > Création de rapports**.

3 Dans **Lien URL vers la page de renvoi**, indiquez l'URL du tableau de bord Identity Manager.

Par exemple : `https://<adresse_IP_réseau_applications_identité:port>/idmdash/#/landing`

Création de rapports	
ID du client OAuth	<input type="text" value="rpt"/>
Secret du client OAuth	<input type="password" value="....."/>
Lien URL vers la page de renvoi	<input type="text" value="https://192.168.0.2:8443/idmdash/#/landing"/>
Lien URL vers Identity Governance	<input type="text"/>
URL de redirection OAuth OSP	<input type="text" value="https://192.168.0.1:8543/IDMRPT/oauth.html"/>

Pour modifier l'URL de renvoi pour les services de collecte de données Identity Manager :

1 Ouvrez `ism-configuration.properties` dans l'éditeur de texte à partir de `/opt/netiq/idm/apps/tomcat/conf`.

2 Annexez l'URL de renvoi au texte suivant :

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

Exemple :

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

3 Relancez Tomcat.

Vous pouvez ignorer ce problème si vous utilisez l'édition Standard qui n'inclut pas les applications d'identité. Ce problème ne provoque aucune perte de fonctionnalités pour les installations Standard Edition.

6.6.3 L'aide de la page de collecte de données pour des paramètres régionaux autres que l'anglais renvoie vers l'Aide en anglais

Problème : Lorsque vous installez les services de collecte de données sous des paramètres régionaux autres que l'anglais et que vous cliquez sur l'icône **Aide** de la page Services de collecte de données, cela vous renvoie vers la version anglophone de l'Aide. (Bogue 1082987)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.6.4 La page Services de collecte de données d'Identity Manager ne s'affiche pas dans l'édition Standard sous Linux

Problème : Après l'installation et la configuration d'Identity Reporting Standard Edition, la page Services de collecte de données d'Identity Manager ne s'affiche pas. (Bogue 1082564)

Solution : Lors de la configuration d'Identity Reporting, sélectionnez **Non (N)** à l'invite suivante :

Vouslez-vous vous connecter à un serveur SSO One externe (Y/N) ?

6.7 Problèmes liés au plug-in iManager

Lors de l'utilisation d'iManager, vous risquez de rencontrer les problèmes suivants :

- ♦ [Section 6.7.1, « Exception sous Windows 2016 lors de l'utilisation de KMO », page 43](#)
- ♦ [Section 6.7.2, « Dépendance par rapport à l'assistant de certificats du pilote NDS-to-NDS », page 43](#)
- ♦ [Section 6.7.3, « Certaines opérations ne sont pas disponibles dans le plug-in du générateur de stratégies », page 43](#)

6.7.1 Exception sous Windows 2016 lors de l'utilisation de KMO

Problème : Lorsque vous exportez un certificat d'une autorité de certification au format .b64 à partir d'iManager, une ligne vide est ajoutée à la fin du certificat. Le certificat devient non valide. (Bogue 1018732)

Solution : Supprimez manuellement la ligne vide du certificat.

6.7.2 Dépendance par rapport à l'assistant de certificats du pilote NDS-to-NDS

Problème : Pour fonctionner correctement, iManager a besoin de l'assistant de certificats du pilote NDS-to-NDS.

Solution : Afin d'utiliser l'assistant de certificats du pilote NDS-to-NDS, téléchargez et installez le plug-in iManager pour le serveur de certificats NetIQ.

6.7.3 Certaines opérations ne sont pas disponibles dans le plug-in du générateur de stratégies

Problème : Cette version ne prend pas en charge la création des opérations suivantes à l'aide du Générateur de stratégies d'iManager. (Bogue 1018354)

- ♦ Création d'un rôle
- ♦ Création d'une ressource
- ♦ Ajout d'une ressource
- ♦ Suppression d'une ressource
- ♦ Génération d'un événement XDAS

Solution : Pour créer ces opérations, utilisez le Générateur de stratégies de Designer.

6.8 Problèmes de mise à niveau d'Identity Manager

- ♦ [Section 6.8.1, « La stratégie de synchronisation des données existante ne figure pas sur la page Services de collecte de données après la mise à niveau d'Identity Manager de la version 4.6.x vers 4.7 », page 44](#)
- ♦ [Section 6.8.2, « Mise à niveau des composants Identity Manager dans un environnement distribué », page 44](#)
- ♦ [Section 6.8.3, « L'indicateur de progression affiche des noms de répertoire tronqués pour certains composants pendant la mise à niveau sous Windows », page 45](#)
- ♦ [Section 6.8.4, « Le processus de mise à niveau échoue en raison de valeurs de port manquantes dans l'URL », page 45](#)

6.8.1 La stratégie de synchronisation des données existante ne figure pas sur la page Services de collecte de données après la mise à niveau d'Identity Manager de la version 4.6.x vers 4.7

Problème : Si vous effectuez une mise à niveau vers Sentinel 8.1.1 et Identity Reporting 4.7, la nouvelle page Services de collecte de données n'affiche pas la stratégie de synchronisation des données existante. (Bogue 1080081)

Solution : Effectuez les étapes suivantes après avoir mis Sentinel à jour :

- 1 Supprimez votre stratégie de synchronisation des données.
 - ♦ Si vous avez procédé à une mise à niveau à partir de Sentinel 8.0.1 ou d'une version antérieure, supprimez la stratégie de synchronisation des données de Sentinel et supprimez la table `sentinel_events` de la base de données de création de rapports. Connectez-vous à la base de données PostgreSQL et supprimez la table `sentinel_events` sous le schéma public. La mise à jour de Sentinel supprime les données de la table `sentinel_events`. Connectez-vous à **Sentinel > Stockage > Synchronisation des données**, sélectionnez votre stratégie, puis cliquez sur **Supprimer**. Connectez-vous à la base de données de création de rapports et supprimez la table `sentinel_events` sous le schéma public.
 - ♦ Si vous avez procédé à la mise à niveau à partir d'une version ultérieure à Sentinel 8.1, supprimez uniquement la stratégie de synchronisation des données. Connectez-vous à **Sentinel > Stockage > Synchronisation des données**, sélectionnez votre stratégie, puis cliquez sur **Supprimer**.
- 2 Lancez la page Services de collecte de données et accédez à **Paramètres > Synchronisation des données > Stratégies de synchronisation de données**.
- 3 Pour ajouter une stratégie, cliquez sur **Nouvelle stratégie**.
- 4 Dans la page Nouvelle stratégie de synchronisation des données, spécifiez les détails du serveur Sentinel et de la base de données.
- 5 Cliquez sur **Afficher les paramètres avancés** pour configurer la charge utile de la stratégie que vous créez.
- 6 Cliquez sur **Créer**.

6.8.2 Mise à niveau des composants Identity Manager dans un environnement distribué

Problème 1 : Si OSP et SSPR sont installés sur un serveur distinct dans votre environnement distribué.

Le processus de mise à niveau remplace le fichier non standard `oauth-keystore.file` (par exemple, `idmnew.jks`) avec le nom de fichier par défaut (`osp.jks`). (Bogue 1081968)

Solution : Procédez comme suit pour remplacer le fichier par défaut par le fichier non standard après avoir terminé la mise à niveau :

- 1 Lancez l'utilitaire de **mise à jour de configuration**.
- 2 Sous l'onglet **Authentification**, faites défiler jusqu'à atteindre la section **Configuration de l'authentification**.

- 3 Dans le fichier **Keystore OAuth**, remplacez le chemin d'accès au fichier Keystore JKS par le fichier non standard (par exemple, `idmnew.jks`). Ce fichier se trouve dans le dossier de sauvegarde d'OSP.
- 4 Dans **Mot de passe du fichier Keystore OAuth**, spécifiez le mot de passe pour charger le fichier Keystore OAuth non standard.

Problème 2 : Si Identity Manager est configuré pour procéder à l'authentification avec NetIQ Access Manager et que vous avez importé des certificats tiers dans le répertoire `cacerts` de Tomcat.

Solution : Réimportez les certificats tiers dans le fichier Keystore `idm.jks`. Cela est nécessaire, car l'instance Tomcat d'Identity Manager 4.7 utilise le fichier Keystore `idm.jks`. Par exemple, si Identity Manager est configuré pour utiliser le serveur Access Manager pour l'authentification, importez le certificat Access Manager dans `idm.jks`.

6.8.3 L'indicateur de progression affiche des noms de répertoire tronqués pour certains composants pendant la mise à niveau sous Windows

Problème : Lors de la mise à niveau d'OSP, de SSPR et des composants des applications d'identité, les noms de répertoire d'installation de ces composants apparaissent tronqués dans l'indicateur de progression.

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

6.8.4 Le processus de mise à niveau échoue en raison de valeurs de port manquantes dans l'URL

Problème : Si les numéros de port ne sont pas spécifiés dans le paramètre **URL de redirection OAuth OSP** pour chaque application d'identité, la mise à niveau échoue.

Solution : Avant de lancer le programme de mise à niveau, vous devez entrer manuellement les numéros de port dans l'utilitaire de mise à jour de la configuration. Effectuez les étapes suivantes pour spécifier les valeurs de port :

- 1 Lancez l'utilitaire de **mise à jour de configuration**.
- 2 Sous l'onglet **Clients SSO**, spécifiez les valeurs de port appropriées dans toutes les URL requises.

Utilisez le format suivant : `protocol//serveur:port/chemin`

Par exemple, `http://192.0.2.0:80/dash`

6.9 Problèmes liés à la localisation

- ♦ [Section 6.9.1, « Identity Manager ne parvient pas à installer certains pilotes avec des paramètres régionaux non anglais », page 46](#)
- ♦ [Section 6.9.2, « Les programmes d'installation d'Identity Manager contiennent des caractères altérés en mode Console sous Windows », page 46](#)
- ♦ [Section 6.9.3, « Certains programmes d'installation de composants ne sont pas localisés », page 47](#)
- ♦ [Section 6.9.4, « L'installation de PostgreSQL échoue si le mot de passe de l'utilisateur postgres est fourni en russe sous Windows », page 47](#)

6.9.1 Identity Manager ne parvient pas à installer certains pilotes avec des paramètres régionaux non anglais

Problème : Lorsque vous installez certains pilotes à l'aide de l'option **Personnaliser les composants sélectionnés** avec des paramètres régionaux non anglais, l'installation échoue. (Bogue 926490)

Solution : Effectuez l'une des opérations suivantes :

- ♦ Sélectionnez l'anglais comme langue d'installation d'Identity Manager (et non une autre langue que l'anglais).
- ♦ Sous Windows, copiez les fichiers JAR nécessaires se trouvant sur le support d'installation dans le dossier d'installation d'Identity Manager. Sous Linux, accédez à `products/IDM/linux/setup/packages` sur le support d'installation et exécutez la commande suivante :
 - ♦ **Nouvelle installation** : `rpm -ivf <nom du fichier>`
 - ♦ **Mise à niveau** : `rpm -Uvf <nom du fichier>`

6.9.2 Les programmes d'installation d'Identity Manager contiennent des caractères altérés en mode Console sous Windows

Problème : Si vous sélectionnez l'allemand, l'anglais, le brésilien, le danois, l'espagnol, le français, l'italien, le néerlandais, le portugais, le russe ou le suédois comme langue d'installation d'Identity Manager, le programme d'installation affiche des caractères corrompus lors de l'installation.

Si vous choisissez l'anglais, le programme d'installation contient un caractère corrompu dans la page de *sélection de la langue* du programme d'installation. Les caractères s'affichent toutefois correctement pour les langues asiatiques si le programme d'installation est exécuté sous une version asiatique de Windows. (Bogue 672070)

Solution : Pour que les caractères apparaissent correctement, veillez à remplacer la police par défaut de l'ordinateur Windows par la police Lucida Console en effectuant la procédure suivante avant d'installer Identity Manager :

- 1 Sélectionnez **Démarrer > Exécuter > Regedit > HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage** et remplacez la valeur d'**OEMCP 850** par **1252**.
Pour le russe, remplacez la valeur d'**OEMCP 866** par **1251** dans le répertoire `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage`.
- 2 Sélectionnez **Démarrer > Exécuter**, saisissez `cmd` dans la zone de texte **Ouvrir**, puis cliquez sur **Entrée** pour lancer l'invite de commande.
- 3 Cliquez avec le bouton droit sur la barre de titre de la fenêtre d'invite de commande afin d'ouvrir le menu contextuel.
- 4 Faites défiler le menu contextuel et sélectionnez l'option **Par défaut** afin d'ouvrir la boîte de dialogue Propriétés de Console Windows.
- 5 Cliquez sur l'onglet **Police** et remplacez la police par défaut **Raster** par **Lucida Console (TrueType)**.
- 6 Cliquez sur **OK**.
- 7 Redémarrez l'ordinateur.

6.9.3 Certains programmes d'installation de composants ne sont pas localisés

Problème : Les versions localisées du programme d'installation fourni par commodité d'Apache Tomcat, de PostgreSQL, d'OSP et d'Identity Reporting ne sont pas disponibles dans cette version. Vous devez exécuter les programmes d'installation des composants uniquement en langue anglaise. (Bogue 1008039)

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème. Sélectionnez l'**anglais** comme langue d'installation d'Identity Manager (et non une autre langue que l'anglais).

6.9.4 L'installation de PostgreSQL échoue si le mot de passe de l'utilisateur postgres est fourni en russe sous Windows

Problème : Le programme d'installation de PostgreSQL n'accepte pas le mot de passe pour l'administrateur de base de données (**Mot de passe de l'administrateur**) en russe. (Bogue 1075752)

Solution : Spécifiez le mot de passe en anglais.

6.10 Problèmes de désinstallation

- ♦ [Section 6.10.1, « La désinstallation de la structure d'Identity Manager ne supprime pas l'ensemble des dossiers du répertoire d'installation sous Windows », page 47](#)
- ♦ [Section 6.10.2, « Les fichiers journaux de désinstallation de la structure Identity Manager ne sont pas créés dans le dossier correspondant sous Windows », page 47](#)
- ♦ [Section 6.10.3, « Désinstallation de l'entrée Identity Manager à partir du panneau de configuration après avoir mis à niveau le moteur Identity Manager sous Windows », page 47](#)
- ♦ [Section 6.10.4, « Un message incorrect s'affiche au cours de la désinstallation », page 48](#)

6.10.1 La désinstallation de la structure d'Identity Manager ne supprime pas l'ensemble des dossiers du répertoire d'installation sous Windows

Problème : Le programme de désinstallation ne supprime pas les fichiers JAR à partir du répertoire lib. (Bogue 643077)

Solution : Supprimez manuellement les fichiers JAR du répertoire lib.

6.10.2 Les fichiers journaux de désinstallation de la structure Identity Manager ne sont pas créés dans le dossier correspondant sous Windows

Problème : Les fichiers journaux de désinstallation sont créés dans le répertoire temp. (Bogue 613225)

Solution : Dans la mesure où aucune perte de fonctionnalités n'est à signaler, vous pouvez ignorer ce problème.

6.10.3 Désinstallation de l'entrée Identity Manager à partir du panneau de configuration après avoir mis à niveau le moteur Identity Manager sous Windows

Problème : Après la mise à niveau du moteur Identity Manager vers la version 4.5, si vous exécutez le programme de désinstallation à partir du panneau de configuration, les fichiers Identity Manager nécessaires sont effectivement supprimés à l'exception d'une clé de registre spécifique. De ce fait, l'entrée Identity Manager reste affichée dans le panneau de configuration, même après avoir exécuté la désinstallation. (Bogue 901219)

Solution : Supprimez la clé de registre du chemin d'accès au registre suivant lorsque vous exécutez la désinstallation :

♦ **Pour les ordinateurs 32 bits :**

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

♦ **Pour les ordinateurs 64 bits :**

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

6.10.4 Un message incorrect s'affiche au cours de la désinstallation

Problème : Au cours de la désinstallation, le programme affiche un message indiquant qu'InstallAnywhere prépare l'installation, alors que le programme effectue en réalité une désinstallation.

Solution : Il n'y a pour l'instant aucun moyen de contourner ce problème.

7 Coordonnées

Notre objectif est de vous proposer une documentation qui répond à vos besoins. Si vous avez des conseils pour l'améliorer, n'hésitez pas à nous envoyer un e-mail à l'adresse suivante :

Documentation-Feedback@netiq.com (<mailto:Documentation-Feedback@netiq.com>). Nous accordons une grande importance à vos commentaires et sommes impatients de connaître vos impressions.

Pour obtenir toutes nos coordonnées, rendez-vous sur le [site Web reprenant les informations de contact du support](http://www.netiq.com/support/process.asp#phone) (<http://www.netiq.com/support/process.asp#phone>).

Pour obtenir des informations générales sur les produits et l'entreprise, rendez-vous sur le [site Web de NetIQ Corporation](http://www.netiq.com/) (<http://www.netiq.com/>).

Pour mener des conversations interactives avec vos pairs et experts NetIQ, devenez un membre actif de notre [communauté](https://www.netiq.com/communities/) (<https://www.netiq.com/communities/>). La communauté en ligne NetIQ fournit des informations sur les produits, des liens vers des ressources utiles, des blogs et des canaux de réseaux sociaux.

8 Mentions légales

Pour plus d'informations sur les mentions légales, les marques, les exclusions de garantie, les garanties, les limitations en matière d'exportation et d'utilisation, les droits du gouvernement américain, la politique relative aux brevets et la compatibilité avec la norme FIPS, consultez le site <https://www.netiq.com/company/legal/>.

Copyright © 2018 NetIQ Corporation. Tous droits réservés.