

NetIQ Directory and Resource Administrator 10.2 - Notes de version

Mai 2022

Ces améliorations sont souvent apportées en réponse directe aux suggestions de nos clients. Nous vous remercions de votre temps et de votre précieuse contribution. Nous espérons que vous continuerez à nous aider à faire en sorte que nos produits répondent à tous vos besoins. Vous pouvez publier vos commentaires dans les forums de [NetIQ Directory and Resource Administrator](#) et de [Aegis](#) qui se trouvent dans Micro Focus Forums; il s'agit de nos communautés en ligne qui offrent également des informations sur les produits, des blogues et des liens vers des ressources utiles. Vous pouvez également partager vos idées pour améliorer le produit sur le [Portail des idées](#).

- ◆ « Quoi de neuf? » page 1
- ◆ « Configuration système requise » page 4
- ◆ « Installer et mettre à jour cette version » page 4
- ◆ « Résolution des problèmes des clients » page 5
- ◆ « Problèmes connus » page 6
- ◆ « Coordonnées » page 7
- ◆ « Avis juridique » page 8

Quoi de neuf?

- ◆ « Améliorations de Directory and Resource Administrator » page 1
- ◆ « Améliorations de Workflow Automation » page 4

Améliorations de Directory and Resource Administrator

Les sections suivantes décrivent les nouvelles fonctionnalités et les améliorations de DRA 10.2 :

- ◆ « Prise en charge des utilisateurs anonymes d'Azure » page 2
- ◆ « Prise en charge de l'authentification par certificat » page 2
- ◆ « Améliorations de PowerShell » page 2
- ◆ « Afficher les attributs virtuels des objets à l'aide de PowerShell » page 3

- ♦ « Installation à l'aide de certificats dans un autre magasin de certificats » page 3
- ♦ « Améliorations de la console Web » page 3

Prise en charge des utilisateurs anonymes d'Azure

Vous pouvez inviter des utilisateurs externes ou des utilisateurs anonymes à un rôle de locataire Azure pour une collaboration. Les utilisateurs anonymes peuvent accepter l'invitation pour le rôle de locataire Azure de votre organisation et accéder aux applications configurées à l'aide de leurs informations d'identification. Vous pouvez gérer ces utilisateurs à partir de la console Web DRA.

DRA inclut le rôle Administration des utilisateurs anonymes Azure pour gérer les utilisateurs anonymes Azure. L'applet de commande PowerShell `New-AzureDRAMSInvitation` est introduite pour inviter des utilisateurs anonymes.

Le paramètre `UserTypes` est ajouté aux applets de commande PowerShell suivantes pour distinguer les utilisateurs Azure de type Membre et Anonyme :

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

Prise en charge de l'authentification par certificat

DRA prend en charge l'authentification multi-facteurs en utilisant des certificats pour l'authentification avec Azure Active Directory. Vous pouvez maintenant gérer un locataire Azure en utilisant l'authentification basée sur un certificat ou l'authentification de base. Par défaut, DRA utilise une authentification basée sur un certificat. DRA génère un certificat auto-signé et l'attribue à l'application Azure. L'application Azure est créée hors ligne à l'aide du script PowerShell fourni par DRA.

L'authentification par certificat requiert la version 2.0.3 ou ultérieure du module Exchange Online V2 pour gérer les tâches d'Exchange Online. L'utilitaire DRA Health Check comprend les nouvelles vérifications suivantes pour la validation des locataires Azur :

- ♦ Autorisation d'application Azure
- ♦ Valider le certificat de locataire Azure

Pour utiliser l'authentification par certificat après la mise à niveau d'une version antérieure de DRA vers la version 10.2, vous devez exécuter le script `UpdateDraAzureApplicationPermission.ps1` pour appliquer les autorisations supplémentaires requises pour l'authentification par certificat. Pour plus d'informations, voir [Configuration des locataires Azure](#).

Améliorations de PowerShell

DRA PowerShell comprend les améliorations suivantes :

les applets de commande d'énumération des délégations

DRA PowerShell comprend désormais les nouvelles applets de commande suivantes pour l'énumération des délégations :

- ♦ `Get-DRAActiveViewRules` : récupère toutes les règles d'une ActiveView.

- ◆ Get-DRAAssistantAdminGroupMembers : récupère tous les membres d'un groupe d'assistants administrateurs.
- ◆ Get-DRAActiveViewAssignments : récupère toutes les affectations d'une ActiveView.

L'applet de commande Remove-DRAAssignments a été mise à jour pour accepter le caractère générique astérisque (*) afin de supprimer tous les pouvoirs et les rôles.

Déplacer des objets de contact

L'applet de commande Move-DRAContact déplace un objet de contact d'un emplacement dans Active Directory à un autre.

Afficher les attributs virtuels des objets à l'aide de PowerShell

Le paramètre `IncludeAllVAProperties` est ajouté aux applets de commande suivantes pour renvoyer tous les attributs virtuels associés à l'objet :

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

Installation à l'aide de certificats dans un autre magasin de certificats

Vous pouvez maintenant spécifier des certificats pour le service REST et le service de réPLICATION DRA à partir du magasin personnel et du magasin d'hébergement Web.

Améliorations de la console Web

Plusieurs améliorations ont été apportées à la console Web DRA pour en faciliter l'utilisation :

- ◆ **Filtrer les résultats dans les onglets d'appartenance à un groupe** : Dans les pages de propriétés Membres et Membre de, vous pouvez réduire l'étendue des données qui sont affichées dans la représentation sous forme de tableau en recherchant des objets à l'aide du nom de l'objet. La représentation sous forme de tableau affiche le nombre d'objets qui correspondent aux critères de recherche ainsi que le nombre total d'objets. Vous pouvez également supprimer des objets de différentes pages dans la représentation sous forme de tableau. Les objets à ajouter et à supprimer sont répertoriés dans la liste des objets non enregistrés.
- ◆ **Personnaliser les colonnes dans le sélecteur d'objet** : vous pouvez désormais personnaliser les colonnes que vous souhaitez afficher dans la présentation des résultats de recherche du sélecteur d'objet.
- ◆ **Amélioration de la fenêtre modale** : les fenêtres ont été redimensionnées, ce qui élimine la nécessité de faire défiler verticalement les boutons de la fenêtre.

- ♦ **Afficher les propriétés des objets référencés** : vous pouvez afficher les propriétés des objets qui sont renvoyés comme faisant partie des pages de propriétés d'un autre objet, du rapport sur l'historique des modifications et des affectations de groupes temporaires. Vous pouvez également visualiser les propriétés des objets qui ont été sélectionnés pour des opérations en masse.
- ♦ **Autres améliorations de l'interface utilisateur** :
 - ♦ Les menus des opérations **Créer** et **En bloc** est déplacé au-dessus du volet de navigation gauche.
 - ♦ Dans la page **Management > Search**, vous pouvez utiliser le menu filtre **OBJETS** pour filtrer les types d'objets. Le menu de filtre **OBJETS** remplace le bouton **FILTRE** qui était disponible dans la version précédente.
 - ♦ La console Web affiche désormais les messages de validation de manière cohérente pour chaque problème de saisie de données sur une page.
 - ♦ La console Web vous permet de modifier et de visualiser les objets sans utiliser le préfixe `additionalAttributes` dans le nom de l'attribut.
 - ♦ La console Web affiche des icônes cohérentes pour indiquer l'état d'un objet dans les différentes vues de l'objet.

Améliorations de Workflow Automation

Les améliorations suivantes ont été apportées à Workflow Automation 10.2 :

Authentification OAuth pour Exchange Web Services

L'adaptateur de messagerie de Workflow Automation prend en charge l'authentification OAuth pour Exchange Web Services (EWS). Vous pouvez surveiller les comptes de messagerie Azure avec un code secret ou un certificat client Azure.

Configuration système requise

Pour des informations détaillées sur la configuration matérielle requise ainsi les systèmes d'exploitation et navigateurs pris en charge, consultez le [Guide d'installation de DRA](#) ou le document de référence [Exigences système de DRA](#).

Installer et mettre à jour cette version

Lors de la mise à niveau de la version 10.0 vers la version 10.2, les systèmes sur lesquels le service REST est installé, sans le composant serveur de DRA, nécessitent une installation modifiée pour supprimer le service REST avant de procéder à la mise à niveau.

Pour des informations détaillées sur l'installation ou la mise à niveau des composants et des modules de Directory and Resource Administrator, consultez le [Guide d'installation de DRA](#).

Chemins de mise à niveau pris en charge

Utilisez le tableau ci-dessous pour déterminer votre chemin de mise à niveau applicable en fonction de la version. Notez que les versions de correctifs (x.x.x.x) ne sont pas répertoriées. Cependant, tous les correctifs pour les versions indiquées sont pris en charge. Par exemple, vous pouvez passer à DRA 10.2 à partir de DRA 10.1 ou de l'un de ses correctifs suivants : 10.1.0.1, 10.1.0.2, et ainsi de suite.

Version de base du serveur de DRA	Version mise à jour du serveur de DRA
10.0, 10.0.1, 10.0.2, 10.1 ou 10.1.1	10.2
10.0, 10.0.1, 10.0.2, or 10.1	10.1.1
9.2.1, 10.0, 10.0.1 ou 10.0.2	10.1
9.1, 9.1.1, 9.2, 9.2.1, 10.0 ou 10.0.1	10.0.2
9.1, 9.1.1, 9.2, 9.2.1 ou 10.0	10.0.1
9.1, 9.1.1, 9.2 ou 9.2.1	10.0
9.1, 9.1.1 ou 9.2	9.2.1
9.0, 9.0.1, 9.0.2, 9.0.3, 9.1 ou 9.1.1	9.2
9.0, 9.0.1, 9.0.2, 9.0.3 ou 9.1	9.1.1
9.0, 9.0.1, 9.0.2 ou 9.0.3	9.1
9.0, 9.0.1 ou 9.0.2	9.0.3
9.0 ou 9.0.1	9.0.2
9.0	9.0.1

Résolution des problèmes des clients

Cette version comprend les corrections de stabilisation suivantes :

- ♦ Résolution d'un problème où la fin d'un processus WFA ne mettait pas fin aux scripts PowerShell. (321356)
- ♦ Résolution d'un problème où la création d'un processus de travail avec l'activité Trouver des objets Active Directory provoquait une fuite de mémoire dans le processus de courtier d'activité PG. (322342).
- ♦ Résolution d'un problème dans la console Web où le sélecteur d'objets n'affichait pas le champ Description lors de l'ajout d'objets à un groupe. (329305)
- ♦ Résolution d'un problème où le programme d'installation de DRA installait incorrectement les fonctionnalités Web lorsque l'emplacement d'installation d'Internet Information Server était différent de l'emplacement d'installation par défaut. (376025)
- ♦ Résolution d'un problème qui entraînait l'échec du contrôle de l'intégrité des comptes de locataires Azure. (377066)
- ♦ Résolution d'un problème dans la console Web qui produisait une erreur lors de la tentative d'affichage du mot de passe BitLocker. (401002)
- ♦ Résolution d'un problème dans la console Web qui faisait qu'une requête LDAP renvoyait une erreur lorsque les résultats n'étaient pas trouvés. (413076)
- ♦ Résolution d'un problème dans la console Web où la définition de valeurs statiques pour le champ Sélectionner dans la page des propriétés personnalisées de l'utilisateur ne fonctionnait pas comme prévu. (413325)
- ♦ Résolution d'un problème dans la console Web où la page personnalisée n'appliquait pas les filtres définis. (413440)

- ♦ Résolution d'un problème dans la console Web où la valeur du conteneur définie à l'aide d'un script de gestionnaire personnalisé ne s'affichait pas. (414322)
- ♦ Résolution d'un problème dans la console Web qui produisait une erreur lors de la tentative de transformation d'un objet utilisateur. (434049)
- ♦ Résolution d'un problème qui empêchait l'installation de DRA lorsque le dossier racine était spécifié comme emplacement d'installation et emplacement du fichier journal. (448013)
- ♦ Résolution d'un problème qui entraînait l'échec du contrôle d'intégrité de la configuration AD LDS lorsque le compte de service était membre d'un groupe imbriqué. (449015)
- ♦ Résolution d'un problème lié à l'emplacement du fichier journal PostgreSQL. (450016)
- ♦ Résolution d'un problème où les pages personnalisées n'affichaient pas correctement le nombre de membres. (476001)
- ♦ Résolution d'un problème dans la console Web où l'attribut sAMAccountName affichait une chaîne aléatoire lorsque la valeur de l'attribut alias de la boîte aux lettres dépassait 20 caractères. (479073)
- ♦ Résolution d'un problème dans la console Web qui empêchait l'affichage des attributs d'extension pour les objets. (483035)
- ♦ Résolution d'un problème d'affichage incorrect du nom de l'utilisateur dans la liste des membres de la TGA lorsque le nom de l'utilisateur contenait une barre oblique (/). (496065)

Problèmes connus

Nous nous efforçons de garantir que nos produits fournissent des solutions de qualité pour vos besoins en matière de logiciels d'entreprise. Le problème suivant fait actuellement l'objet de recherches. Si vous avez besoin d'aide pour un problème quelconque, veuillez contacter le [support technique](#).

Le compte d'accès Skype ne s'affiche pas sur le serveur secondaire

Après la mise à niveau de DRA 10.1 à 10.2, DRA ne parvient pas à afficher le compte d'accès Skype sur le serveur secondaire.

Solution : Saisissez à nouveau le compte d'accès Skype ou sélectionnez l'option **Utiliser le compte d'accès Skype du serveur administrateur principal**.

La collecte de données à l'aide d'un compte de remplacement de domaine échoue lorsque NTLM est refusé

La collecte de données échoue lorsque NTLM est refusé et que les collecteurs de données sont configurés à l'aide du compte de remplacement du domaine.

Solution : Lors de la configuration du collecteur de données, utilisez l'option **Compte de service de Directory Resource Administrator Core**. Assurez-vous que le compte utilisé avec cette option est soit un compte de moindre privilège, soit un compte avec le privilège d'administrateur de domaine.

Le gestionnaire de formulaire ne conserve pas le type d'authentification LDAP

Le gestionnaire de formulaire met automatiquement à jour le type d'authentification LDAP configuré en **Anonyme** après la mise à niveau de DRA de la version 10.1 à 10.1.1 ou plus.

Solution : Après la mise à niveau, vous devez configurer manuellement le type d'authentification LDAP requis dans le gestionnaire de formulaires.

La console Web renvoie une erreur 404 dans un environnement STIG

Une erreur 404 est renvoyée lorsque vous actualisez la console Web dans un environnement conforme à la norme STIG.

Solution : Réparez le programme **Module de réécriture d'URL d'Internet Information Server 2** en utilisant la fonctionnalité **Ajout ou suppression de programmes de Windows**.

Impossible de rechercher des ActiveViews

Après l'installation de DRA, lorsque vous lancez la console de délégation et de configuration pour la première fois, l'option de recherche des ActiveViews n'apparaît pas dans le champ **Search for** (Rechercher) de la zone **Delegation Management > ActiveViews** (ActiveViews de gestion des délégations).

Solution : Pour rechercher des ActiveViews dans la zone **ActiveViews de > gestion des délégations**, cliquez sur le tiret qui s'affiche pour le champ **Rechercher**, puis sélectionnez **Activeviews** dans la liste.

Le rafraîchissement du cache des comptes complets pour un locataire Azure échoue et le message d'erreur AADSTS700027 s'affiche.

Après avoir configuré un locataire Azure, le rafraîchissement du cache du compte complet pour le locataire Azure échoue avec le message d'erreur suivant: AADSTS700027 : Client assertion contains an invalid signature - Thumbprint of key used by client. (AADSTS700027 : l'assertion du client contient une signature invalide. Empreinte de la clé utilisée par le client)

Solution : Pour résoudre cette erreur, vous pouvez soit exécuter manuellement le rafraîchissement du cache des comptes complets, soit attendre le prochain rafraîchissement du cache des comptes complets dont l'exécution est programmée. Effectuer une actualisation complète du cache des comptes peut nécessiter plusieurs minutes.

NetIQ Administration Service cesse de fonctionner lorsque le mot de passe du certificat manuel est faible.

NetIQ Administration Service cesse de fonctionner lorsque le certificat manuel que vous spécifiez pour l'authentification par certificat est protégé par un mot de passe faible.

Solution : Assurez-vous que le certificat manuel que vous spécifiez pour l'authentification par certificat est protégé par un mot de passe robuste.

Coordonnées

Nous souhaitons recevoir vos commentaires et vos suggestions concernant ce livre et les autres documents inclus dans ce produit. Vous pouvez utiliser le lien [comment on this topic](#) (Faire un commentaire sur ce sujet) au bas de chaque page de la documentation en ligne, ou envoyer un courriel à Documentation-Feedback@microfocus.com.

Pour les questions spécifiques aux produits, contactez le service clients de Micro Focus à partir de l'adresse suivante : <https://www.microfocus.com/support-and-services/>.

Avis juridique

© Micro Focus ou l'une de ses filiales, 2007 à 2022.

Les seules garanties offertes pour les produits et services par Micro Focus, ses filiales et ses concédants de licence (« Micro Focus ») sont énoncées dans les déclarations de garantie expresses accompagnant ces produits et services. Rien dans le présent document ne doit être interprété comme constituant une garantie supplémentaire. Micro Focus n'est pas responsable des erreurs techniques ou éditoriales, ni des omissions contenues dans ce document. Les renseignements contenus dans le présent document peuvent être modifiés sans préavis.