NetIQ Directory and Resource Administrator

Guide d'installation

Juin 2021

Avis juridique

Pour plus d'informations sur les mentions légales, les marques de commerce les avis de non-responsabilité, les garanties, les limitations en matière d'exportation et d'utilisation, les droits restreints du gouvernement américain, la politique relative aux brevets et la compatibilité avec la norme FIPS, consultez le site https://www.microfocus.com/about/legal/.

© Micro Focus ou l'une de ses filiales, 2007 à 2021.

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.

À propos de ce guide

Le *Guide d'installation* fournit des renseignements sur la planification, l'installation, la licence et la configuration de NetIQ Directory and Resource Administrator (DRA) et de ses composants intégrés.

Ce document vous guide tout au long du processus d'installation et vous aide à prendre les bonnes décisions pour installer et configurer DRA.

Public cible

Ce document fournit des renseignements à tous ceux qui installent DRA.

Documentation supplémentaire

Ce guide fait partie de la documentation de NetIQ Directory and Resource Administrator. Pour obtenir la plus récente version de ce guide ainsi que d'autres documents sur DRA, visitez le site web de la documentation de DRA (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

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 clientèle de Micro Focus à partir de l'adresse suivante : https://www.microfocus.com/support-and-services/.

Mise en route

Avant d'installer et de configurer tous les composants de NetIQ Directory and Resource Administrator (DRA), vous devez comprendre les fondements de ce que DRA fera pour votre entreprise et le rôle des composants de DRA dans l'architecture du produit.

1 Qu'est-ce que Directory and Resource Administrator?

NetIQ Directory and Resource Administrator est un outil qui offre une administration sécurisée et efficace de l'identité privilégiée de Microsoft Active Directory (AD). DRA effectue une délégation granulaire de « droit d'accès minimal » de sorte que les administrateurs et les utilisateurs ne reçoivent que les autorisations qui leur sont nécessaires pour s'acquitter de leurs responsabilités respectives. DRA assure également le respect des stratégies, fournit des audits et des rapports détaillés sur les activités et simplifie la réalisation de tâches répétitives grâce à l'automatisation des processus informatiques. Chacune de ces fonctionnalités contribue à protéger les environnements AD et Exchange de vos clients contre les risques d'élévation de privilèges, d'erreurs, d'activités malveillantes et de non-conformité réglementaire, tout en réduisant la charge de travail de l'administrateur par l'octroi des capacités de libre-service aux utilisateurs, aux gestionnaires d'entreprise et au personnel du service d'assistance.

DRA étend également les puissantes fonctionnalités de Microsoft Exchange, ce qui permet d'assurer une gestion transparente des objets Exchange. Grâce à une interface utilisateur unique et commune, DRA fournit une administration basée sur des stratégies pour la gestion des boîtes aux lettres, des dossiers publics et des listes de distribution dans votre environnement Microsoft Exchange.

DRA fournit les solutions dont vous avez besoin pour contrôler et gérer vos environnements Microsoft Active Directory, Windows, Exchange et Azure Active Directory.

- **Prise en charge d'Azure et d'Active Directory sur site, d'Exchange et de Skype Entreprise :**

  permet la gestion administrative d'Azure et d'Active Directory sur site, du serveur Exchange sur site, de Skype Entreprise sur site, d'Exchange Online et de Skype Entreprises Online.
- **Contrôles granulaires des accès/privilèges d'utilisateur et d'administration :** la technologie brevetée ActiveView ne délègue que les privilèges nécessaires pour s'acquitter de responsabilités précises et éviter l'élévation des privilèges.
- **Console Web personnalisable :** l'approche intuitive permet au personnel non technique d'effectuer facilement et en toute sécurité des tâches administratives grâce à des capacités et à des accès limités (et attribués).
- **Audit approfondi de l'activité et création de rapports :** fournit un enregistrement d'audit complet de toutes les activités effectuées par le produit. Stocke en toute sécurité les données à long terme et démontre aux auditeurs (p. ex. PCI DSS, FISMA, HIPAA et NERC CIP) que des processus sont en place pour contrôler l'accès à AD.
- **Automatisation des processus informatiques :** automatise les flux de travail pour une variété de tâches, comme le provisionnement et le déprovisionnement, les actions des utilisateurs et des boîtes aux lettres, l'application des stratégies et le contrôle des tâches en libre-service; augmente l'efficacité de l'entreprise et réduit les efforts administratifs manuels et répétitifs.
- **Intégrité opérationnelle :** empêche les changements malveillants ou incorrects qui affectent le fonctionnement et la disponibilité des systèmes et des services grâce à un contrôle d'accès granulaire accordé aux administrateurs et à la gestion de l'accès aux systèmes et aux ressources.

- **Application du processus :** garantit l'intégrité des processus clés de gestion du changement qui vous aident à améliorer la productivité, à réduire les erreurs, à gagner du temps et à accroître l'efficacité de l'administration.
- **Intégration avec Change Guardian :** améliore l'audit pour les événements générés dans Active Directory en dehors de DRA et de Workflow Automation.

2 Comprendre les composants de Directory and Resource Administrator

Les composants de DRA que vous utiliserez systématiquement pour gérer les accès privilégiés comprennent les serveurs principaux et secondaires, les consoles d'administrateur, les composants de création de rapports et Workflow Automation Engine pour automatiser les processus de travail.

Le tableau suivant indique les interfaces utilisateur et les serveurs d'administration habituellement utilisés par chaque type d'utilisateur DRA :

Type d'utilisateur DRA	Interfaces utilisateur	Serveur d'administration
Administrateur DRA (La personne qui gérera la configuration du produit)	Console de délégation et de configuration	Serveur primaire
Administrateur avancé	Configuration du centre de création de rapports de DRA (NRC) PowerShell *(facultatif)* CLI *(facultatif)* Fournisseur DRA ADSI *(facultatif)*	N'importe quel serveur DRA
Administrateur occasionnel du service d'assistance	Console Web	Tout serveur DRA

Serveur d'administration DRA

Le serveur d'administration DRA stocke les données de configuration (environnement, accès délégué et stratégie), exécute les tâches d'automatisation et d'opérateur et audite l'activité du système. Tout en prenant en charge plusieurs clients de niveau console et API, le serveur est conçu pour offrir une haute disponibilité pour la redondance et l'isolation géographique par un modèle d'extension MMS (ensemble multimaître). Dans ce modèle, chaque environnement DRA requiert un serveur d'administration DRA primaire qui se synchronise avec un certain nombre de serveurs d'administration DRA secondaires supplémentaires.

Nous vous recommandons fortement de ne pas installer les serveurs d'administration sur les contrôleurs de domaine Active Directory. Pour chaque domaine géré par DRA, assurez-vous qu'il existe au moins un contrôleur de domaine sur le même site que le serveur d'administration. Par défaut, le serveur d'administration accède au contrôleur de domaine le plus proche pour toutes les opérations de lecture et d'écriture. Lors de l'exécution de tâches propres au site, telles que les

réinitialisations de mot de passe, vous pouvez spécifier un contrôleur de domaine propre au site pour traiter l'opération. Il est recommandé d'utiliser un serveur d'administration secondaire dédié pour la création de rapports, le traitement par lots et les charges de travail automatisées.

Console de délégation et de configuration

La console de délégation et de configuration est une interface utilisateur installable qui permet aux administrateurs système d'accéder aux fonctions de configuration et d'administration de DRA.

- **Gestion de la délégation :** vous permet de spécifier et d'affecter de façon granulaire des ressources et des tâches gérées aux administrateurs assistants.
- **Gestion des stratégies et de l'automatisation :** vous permet de définir et d'appliquer des stratégies pour assurer la conformité aux normes et aux conventions de l'environnement.
- **Gestion de la configuration :** vous permet de mettre à jour les paramètres et les options du système DRA, d'ajouter des personnalisations et de configurer les services gérés (Active Directory, Exchange, Azure Active Directory etc.).
- **Gestion des comptes et des ressources:** permet aux administrateurs assistants de DRA de visualiser et de gérer les objets délégués des domaines et des services connectés à partir de la console de délégation et de configuration.

Console Web

La console Web est une interface utilisateur basée sur le Web qui fournit un accès rapide et facile aux administrateurs assistants pour visualiser et gérer les objets délégués des domaines et services connectés. Les administrateurs peuvent personnaliser l'apparence et l'utilisation de la console Web afin d'inclure une marque d'entreprise et des propriétés de l'objet personnalisées.

Composants de création de rapports

Le module de création de rapports de DRA fournit des modèles intégrés et personnalisables pour la gestion de DRA et des détails sur les domaines et les systèmes gérés par DRA :

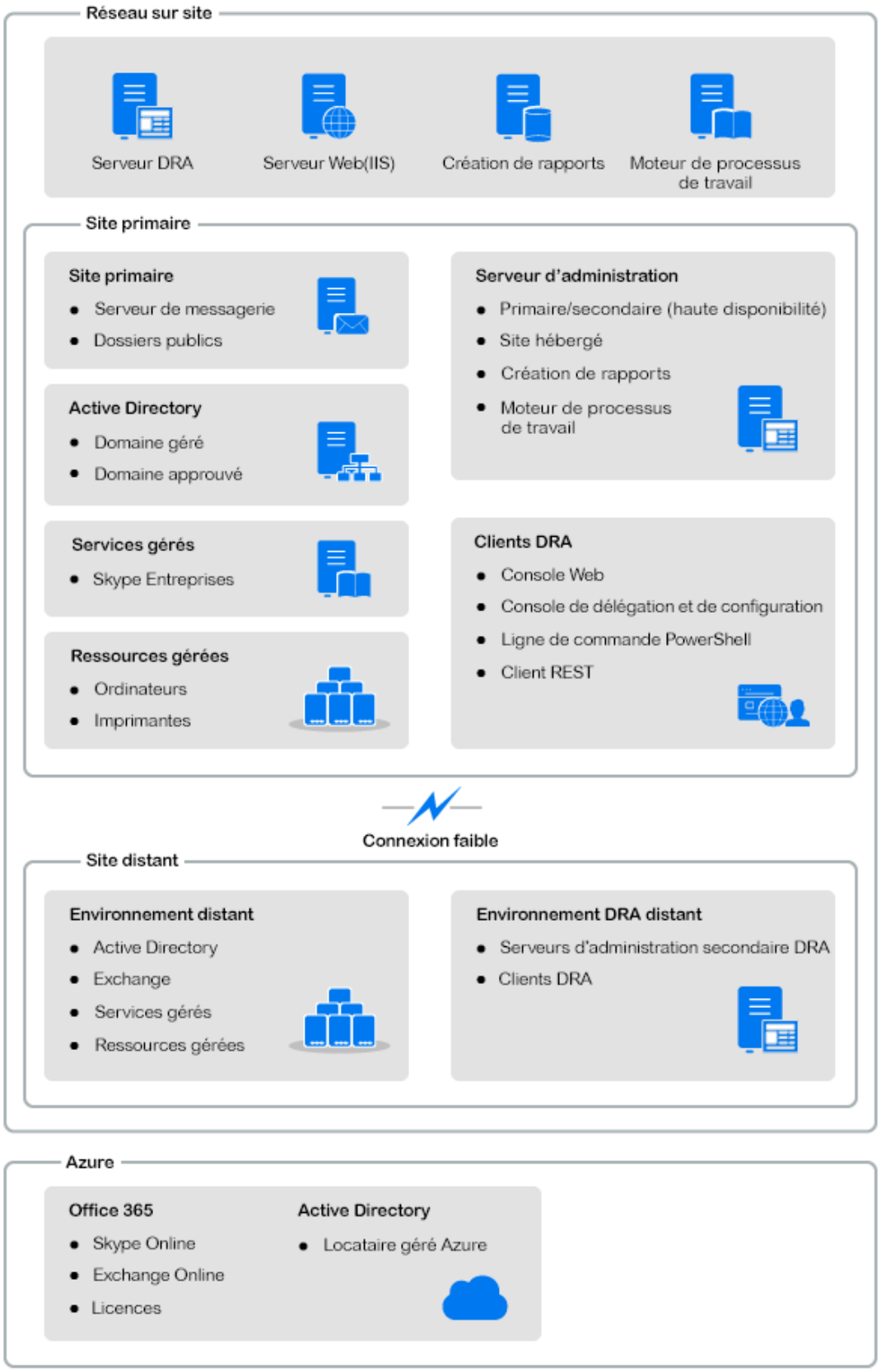
- Rapports de ressources pour les objets Active Directory
- Rapports sur les données d'objets Active Directory
- Rapports de synthèse d'Active Directory
- Rapports de configuration de DRA
- Rapports de configuration d'Exchange
- Rapports d'Office 365 Exchange Online
- Rapports détaillés sur les tendances d'activité (par mois, domaine et pic)
- Rapports récapitulatifs d'activité de DRA

Les rapports de DRA peuvent être planifiés et publiés par l'intermédiaire de SQL Server Reporting Services pour être facilement distribués aux parties prenantes.

Workflow Automation Engine

DRA s'intègre à Workflow Automation Engine afin d'automatiser les tâches de processus de travail au moyen d'une console Web. Grâce à celle-ci, les administrateurs assistants peuvent configurer le serveur de processus de travail et exécuter des formulaires personnalisés d'automatisation des processus de travail, puis visualiser l'état de ces processus de travail. Pour obtenir de plus amples renseignements sur Workflow Automation Engine, consultez le site de la documentation de DRA.

Architecture du produit



II Installation et mise à niveau du produit

Ce chapitre décrit les configurations matérielles, logicielles et de compte nécessaires pour Directory and Resource Administrator. Il vous guide ensuite tout au long du processus d'installation avec une liste de contrôle pour chaque composant de l'installation.

3 Planification de votre déploiement

Lorsque vous planifiez le déploiement de Directory and Resource Administrator, utilisez cette section pour évaluer la compatibilité de votre environnement matériel et logiciel et pour prendre note des ports et des protocoles requis que vous devrez configurer pour le déploiement.

Recommandations de ressources testées

Cette section fournit des informations de dimensionnement que nous recommandons pour les ressources de base. Vos résultats peuvent varier en fonction du matériel disponible, d'un environnement précis, du type de données traitées et d'autres facteurs. Il est probable qu'il existe des configurations matérielles plus grandes et plus puissantes qui peuvent supporter une charge plus importante. Si vous avez des questions, veuillez consulter NetIQ Consulting Services.

Exécuté dans un environnement d'environ un million d'objets Active Directory :

Composant	UC	Mémoire	Stockage
Serveur d'administration DRA	8 UC/cœur 2,0 GHz	16 Go	120 Go
Console Web DRA	2 UC/cœur 2,0 GHz	8 Go	100 Go
Module de création de rapports de DRA	4 UC/cœur 2,0 GHz	16 Go	100 Go
Serveur de processus de travail DRA	4 UC/cœur 2,0 GHz	16 Go	120 Go

Provisionnement des ressources de l'environnement virtuel

DRA garde de grands segments de mémoire actifs pendant de longues périodes de temps. Lors du provisionnement des ressources pour un environnement virtuel, les recommandations suivantes devraient être prises en compte :

- Effectuer un « provisionnement statique » lors de l'allocation du stockage

- Mettre le paramètre de réservation de la mémoire à Réserver toute la mémoire de l'invité (toutes verrouillées)
- Assurez-vous que le fichier de pagination est suffisamment grand pour couvrir la réallocation potentielle de la mémoire gonflée au niveau de la couche virtuelle.

Ports et protocoles requis

Les ports et protocoles de communication DRA sont fournis dans cette section.

- Les ports configurables sont indiqués par un astérisque *.
- Les ports nécessitant un certificat sont indiqués par deux astérisques **.

Tableaux des composants :

- « Serveurs d'administration DRA » page 18
- « Serveur DRA REST » page 20
- « Console Web (IIS) » page 20
- « Console de délégation et d'administration DRA » page 21
- « Serveur de processus de travail » page 21

Serveurs d'administration DRA

Protocole et port	Direction	Destination	Utilisation
TCP 135	Bidirectionnel	Serveurs d'administration DRA	Mappeur de point d'extrémité, une exigence de base pour la communication DRA; permet aux serveurs d'administration de se localiser dans MMS
TCP 445	Bidirectionnel	Serveurs d'administration DRA	Réplication du modèle de délégation; réplication de fichiers pendant la synchronisation MMS (SMB)
Plage de ports TCP dynamique *	Bidirectionnel	Contrôleurs de domaine Microsoft Active Directory	Par défaut, DRA attribue des ports dynamiquement à partir de la plage de ports TCP comprise entre 1024 et 65535. Vous pouvez toutefois configurer cette plage en utilisant Component Services. Pour plus d'informations, consultez *Utilisation du modèle COM distribué avec des pare-feu*.
TCP 50000 *	Bidirectionnel	Serveurs d'administration DRA	Réplication des attributs et communication entre le serveur DRA et AD LDS. (LDAP)
TCP 50001 *	Bidirectionnel	Serveurs d'administration DRA	Réplication des attributs SSL (AD LDS)

Protocole et port	Direction	Destination	Utilisation
TCP/UDP 389	Sortant	Contrôleurs de domaine Microsoft Active Directory	Gestion d'objets Active Directory (LDAP)
	Sortant	Microsoft Exchange Server	Gestion de la boîte aux lettres (LDAP)
TCP/UDP 53	Sortant	Contrôleurs de domaine Microsoft Active Directory	Résolution de nom
TCP/UDP 88	Sortant	Contrôleurs de domaine Microsoft Active Directory	Permet l'authentification du serveur DRA aux contrôleurs de domaine (Kerberos).
TCP 80 *	Sortant	Microsoft Exchange Server	Nécessaire pour tous les serveurs Exchange sur site à partir de 2013 (HTTP)
	Sortant	Microsoft Office 365	Accès PowerShell à distance (HTTP)
TCP 443	Sortant	Microsoft Office 365, Change Guardian	Accès à l'API graphique et intégration de Change Guardian (HTTPS)
TCP 443, 5986, 5985	Sortant	Microsoft PowerShell	Applets de commande PowerShell natifs (HTTPS) et PowerShell à distance.
TCP 5984	Hôte local	Serveurs d'administration DRA	Accès IIS au service de réplication pour prendre en charge les affectations de groupe temporaires
TCP 8092 * **	Sortant	Serveur de processus de travail	État et déclenchement du processus de travail (HTTPS)
TCP 50101 *	Entrant	Client DRA	Cliquez avec le bouton droit de la souris sur l'historique des modifications dans le rapport d'audit de l'interface utilisateur. Peut être configuré pendant l'installation.
TCP 8989	Hôte local	Service d'archivage des journaux	Communication d'archive de journaux (il n'est pas nécessaire de l'ouvrir au moyen du pare-feu)
TCP 50102	Bidirectionnel	Service de base DRA	Service d'archivage des journaux
TCP 50103	Hôte local	Service de mise en cache DRA	Communication du service de mise en cache sur le serveur DRA (il n'est pas nécessaire de l'ouvrir à travers le pare-feu)
TCP 1433	Sortant	Microsoft SQL Server	Collecte des données de création de rapports
UDP 1434	Sortant	Microsoft SQL Server	Le service de navigateur SQL Server utilise ce port pour identifier le port de l'instance nommée.
TCP 8443	Bidirectionnel	Serveur Change Guardian	Historique des modifications unifié

Protocole et port	Direction	Destination	Utilisation
TCP 8898	Bidirectionnel	Serveurs d'administration DRA	Service de réplication de DRA : communication entre les serveurs de DRA pour les affectations de groupe temporaires
TCP 636	Sortant	Contrôleurs de domaine Microsoft Active Directory	Gestion d'objets Active Directory (LDAP SSL).

Serveur DRA REST

Protocole et port	Direction	Destination	Utilisation
TCP 8755 * **	Entrant	Serveur IIS, applets de commande DRA PowerShell	Exécuter les activités de processus de travail basées sur DRA REST (ActivityBroker).
TCP 135	Sortant	Contrôleurs de domaine Microsoft Active Directory	Autodécouverte à l'aide du Service Connection Point (SCP)
TCP 443	Sortant	Contrôleurs de domaine Microsoft AD	Autodécouverte à l'aide du Service Connection Point (SCP)

Console Web (IIS)

Protocole et port	Direction	Destination	Utilisation
TCP 8755 * **	Sortant	Service DRA REST	Pour la communication entre la console Web de DRA et DRA PowerShell
TCP 443	Entrant	Navigateur client	Ouvrir un site Web DRA
TCP 443 **	Sortant	Serveur d'authentification avancée	Authentification avancée

Console de délégation et d'administration DRA

Protocole et port	Direction	Destination	Utilisation
TCP 135	Sortant	Contrôleurs de domaine Microsoft Active Directory	Autodécouverte à l'aide de SCP
Plage de ports TCP dynamique *	Sortant	Serveurs d'administration DRA	Activités de processus de travail de l'adaptateur DRA. Par défaut, DCOM attribue des ports dynamiquement à partir de la plage de ports TCP comprise entre 1024 et 65535. Vous pouvez toutefois configurer cette plage en utilisant Component Services. Pour plus d'informations, consultez *Utilisation du modèle COM distribué avec des pare-feu* (DCOM)
TCP 50102	Sortant	Service de base DRA	Génération d'un rapport sur l'historique des modifications

Serveur de processus de travail

Protocole et port	Direction	Destination	Utilisation
TCP 8755	Sortant	Serveurs d'administration DRA	Exécuter les activités de processus de travail basées sur DRA REST (ActivityBroker).
Plage de ports TCP dynamique *	Sortant	Serveurs d'administration DRA	Activités de processus de travail de l'adaptateur DRA. Par défaut, DCOM attribue des ports dynamiquement à partir de la plage de ports TCP comprise entre 1024 et 65535. Vous pouvez toutefois configurer cette plage en utilisant Component Services. Pour de plus amples renseignements, consultez *Utilisation du modèle COM distribué avec des pare-feu* (DCOM)
TCP 1433	Sortant	Microsoft SQL Server	Stockage des données de processus de travail
TCP 8091	Entrant	Console des opérations et console de configuration	Processus de travail BSL API (TCP)
TCP 8092 **	Entrant	Serveurs d'administration DRA	Processus de travail BSL API (HTTP) et (HTTPS)
TCP 2219	Hôte local	Fournisseur d'espace de nommage	Utilisé par le fournisseur d'espace de nommage pour exécuter les adaptateurs.

Protocole et port	Direction	Destination	Utilisation
TCP 9900	Hôte local	Moteur de corrélation	Utilisé par le moteur de corrélation pour communiquer avec Workflow Automation Engine et le fournisseur d'espace de nommage.
TCP 10117	Hôte local	Fournisseur d'espace de nommage pour la gestion des ressources	Utilisé par le fournisseur d'espace de nommage pour la gestion des ressources

Plateformes prises en charge

Pour obtenir les informations les plus récentes sur les plateformes logicielles prises en charge, reportez-vous à la page du produit Directory and Resource Administrator.

Système géré	Produits préalables
Azure Active Directory	Pour activer l'administration d'Azure, vous devez installer les modules PowerShell suivants : ◆ Azure Active Directory V2 (AzureAD) 2.0.2.4 ou une version ultérieure ◆ AzureRM.Profile 5.8.2 ou une version ultérieure ◆ Exchange Online PowerShell V2 1.0.1 ou une version ultérieure PowerShell 5.1 ou le module le plus récent est nécessaire pour installer les nouveaux modules Azure PowerShell.
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online
Skype Entreprise	◆ Microsoft Skype Entreprise 2015
Historique des modifications	◆ Change Guardian 5.1 ou une version ultérieure
Bases de données	◆ Microsoft SQL Server 2016
Navigateurs Web	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge
Automatisation de processus de travail	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019

Configuration requise pour le serveur d'administration et la console Web de DRA

Les composants DRA nécessitent les logiciels et les comptes suivants :

Configuration logicielle requise

Composant	Produits préalables
Cible d'installation **Système d'exploitation**	**Système d'exploitation du serveur d'administration NetIQ :** ◆ Microsoft Windows Server 2012 R2, 2016, 2019 **REMARQUE :** Le serveur doit également faire partie d'un domaine Active Directory pris en charge par Microsoft sur site. **Interfaces DRA :** ◆ Microsoft Windows Server 2012 R2, 2016, 2019
Programme d'installation	◆ Microsoft Net Framework 4.8 et les versions supérieures.

Composant	Produits préalables
Serveur d'administration	**Directory and Resource Administrator:** ◆ Microsoft Net Framework 4.8 et les versions supérieures. ◆ Microsoft Visual C++ 2015 à 2019, Paquets redistribuables (x64 et x86) ◆ Microsoft Message Queuing ◆ Rôles Microsoft Active Directory Lightweight Directory Services ◆ Service de registre distant démarré ◆ Module de réécriture d'URL pour Microsoft Internet Information Services ◆ Routage des demandes d'application pour Microsoft Internet Information Services **REMARQUE :** Le service et le point d'extrémité REST de DRA sont installés avec le serveur d'administration. **Microsoft Office 365/Exchange Online Administration :** ◆ Module Active Directory Windows Azure pour Windows PowerShell ◆ Module Windows PowerShell ◆ Module PowerShell Exchange Online V2 ◆ Activez WinRM pour l'authentification de base du côté client pour les tâches d'Exchange Online. Pour obtenir de plus amples renseignements, consultez Plateformes prises en charge.
Interface utilisateur	**Interfaces DRA :** ◆ Microsoft .Net Framework 4.8 ◆ Microsoft Visual C++ 2015 à 2019, Paquets redistribuables (x64 et x86)
Extensions PowerShell	◆ Microsoft .Net Framework 4.8 ◆ PowerShell 5.1 ou une version ultérieure
Console Web DRA	**Serveur Web :** ◆ Microsoft .Net Framework 4.x > Services WCF > Activation HTTP ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Module de réécriture d'URL pour Microsoft Internet Information Services ◆ Routage des demandes d'application pour Microsoft Internet Information Services

Domaine du serveur

Composant	Systèmes d'exploitation
Serveur DRA	◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

Exigences relatives aux comptes

Compte	Description	Autorisations
Groupe AD LDS	Le compte de service DRA doit être ajouté à ce groupe pour l'accès à AD LDS	◆ Groupe de sécurité locale de domaine

Compte de service DRA	Les autorisations requises pour exécuter le service d'administration NetIQ	◆ Pour autorisations « Utilisateurs du modèle COM distribué »
		◆ Membre du groupe AD LDS Admin
		◆ Groupe d'opérateurs de compte
		◆ Groupes d'archivage de journaux (OnePointOp ConfgAdms et OnePointOp)
		◆ L'une des options de l'onglet Account > **Account options** (Compte > Options de compte) doit être sélectionnée pour l'utilisateur du compte de service DRA si DRA est installé sur un serveur en utilisant la méthodologie STIG :
		  ◆ Chiffrement Kerberos AES 128 bits
		  ◆ Chiffrement Kerberos AES 256 bits
		REMARQUE
		◆ Pour plus d'informations sur la configuration des comptes d'accès aux domaines de droit d'accès minimal, consultez : Comptes d'accès DRA de droit d'accès minimal.
		◆ Pour en savoir plus sur la configuration d'un compte de service géré de groupe pour DRA, reportez-vous à « Configuration des services de DRA pour un compte de service géré de groupe » dans le *Guide de l'administrateur de DRA*.

Compte	Description	Autorisations
Administrateur DRA	compte d’utilisateur ou groupe provisionné dans le rôle DRA Admin intégré.	◆ Groupe de sécurité locale de domaine ou compte d'utilisateur de domaine ◆ Membre du domaine géré ou d'un domaine approuvé ◆ Si vous spécifiez un compte à partir d'un domaine approuvé, vérifiez que l'ordinateur serveur d'administration peut authentifier ce compte.
Comptes d'administrateur assistant DRA	Comptes qui se verront déléguer des pouvoirs par l'intermédiaire de DRA	◆ Ajoutez·tous·les·comptes·d'administrateur·Assistant·DRA·au·groupe·« Utilisateurs du modèle COM distribué » afin qu'ils puissent se connecter au serveur DRA à partir de clients distants. Cela n'est nécessaire que lorsque vous utilisez un client lourd ou la console de délégation et de configuration. **REMARQUE :** DRA peut être configuré pour gérer cela pour vous pendant l'installation.

Comptes d'accès DRA de droit d'accès minimal

Vous trouverez ci-dessous les autorisations et les privilèges nécessaires pour les comptes spécifiés ainsi que les commandes de configuration que vous devez exécuter.

Compte d'accès au domaine : L'utilisation d'ADSI Edit permet d'accorder au compte d'accès au domaine les autorisations Active Directory suivantes au niveau du domaine supérieur pour les types d'objets descendants suivants :

- Contrôle TOTAL sur les objets builtInDomain
- Contrôle TOTAL sur les objets Ordinateurs
- Contrôle TOTAL sur les objets Point de connexion
- Contrôle TOTAL sur les objets Contacts
- Contrôle TOTAL sur les objets Conteneurs
- Contrôle TOTAL sur les objets Groupes
- Contrôle TOTAL sur les objets InetOrgPerson
- Contrôle TOTAL sur les objets MsExchDynamicDistributionList
- Contrôle TOTAL sur les objets MsExchSystemObjectsContainer
- Contrôle TOTAL sur les objets msDS-GroupManagedServiceAccount
- Contrôle TOTAL sur les objets Unités organisationnelles
- Contrôle TOTAL sur les objets Imprimantes

- Contrôle TOTAL sur les objets Dossiers publics
- Contrôle TOTAL sur les objets Dossiers partagés
- Contrôle TOTAL sur les objets Utilisateurs

Accorder au compte d'accès au domaine les autorisations d'Active Directory suivantes au niveau du domaine supérieur pour cet objet et tous les objets descendants :

- Autoriser la création d'objets Ordinateurs
- Autoriser la création d'objets Contacts
- Autoriser la création de Conteneurs
- Autoriser la création d'objets Groupes
- Autoriser la création d'objets MsExchDynamicDistributionList
- Autoriser la création d'objets msDS-GroupManagedServiceAccount
- Autoriser la création d'objets Unités organisationnelles
- Autoriser la création d'objets Dossiers publics
- Autoriser la création d'objets Dossiers partagés
- Autoriser la création d'objets Utilisateurs
- Autoriser la suppression d'objets Ordinateurs
- Autoriser la suppression d'objets Contacts
- Autoriser la suppression de Conteneurs
- Autoriser la suppression d'objets Groupes
- Autoriser la suppression d'objets InetOrgPerson
- Autoriser la suppression d'objets MsExchDynamicDistributionList
- Autoriser la suppression d'objets msDS-GroupManagedServiceAccount
- Autoriser la suppression d'objets Unités organisationnelles
- Autoriser la suppression d'objets Dossiers publics
- Autoriser la suppression d'objets Dossiers partagés
- Autoriser la suppression d'objets Utilisateurs

REMARQUE

- Par défaut, certains objets conteneurs intégrés dans Active Directory n'héritent pas des autorisations du niveau supérieur du domaine. C'est pourquoi il faudra activer l'héritage pour ces objets, ou définir des autorisations explicites.
- Si vous utilisez un compte avec un droit d'accès minimal comme compte d'accès, assurez-vous que le compte se voit attribuer l'autorisation « Reset Password » (Réinitialiser le mot de passe) dans Active Directory pour qu'il soit possible de réinitialiser le mot de passe dans DRA.

Compte d'accès Exchange : Pour gérer les objets Microsoft Exchange sur site, attribuez le rôle de gestion organisationnelle au compte d'accès à Exchange et le compte d'accès à Exchange au groupe des opérateurs de compte.

Compte d'accès Skype : Assurez-vous que ce compte est un utilisateur compatible Skype et qu'il est membre d'au moins l'un des groupes suivants :

- Rôle CSAdministrator
- Les rôles CSUserAdministrator et CSArchiving

Compte d'accès aux dossiers publics : Affectez les autorisations Active Directory suivantes au compte d'accès aux dossiers publics :

- Gestion des dossiers publics
- Dossiers publics à extension messagerie

Compte d'accès du locataire Azure : Affectez les autorisations Azure Active Directory suivantes au compte d'accès du locataire Azure :

- Groupes de distribution
- Destinataires du courriel
- Création des destinataires du courriel
- Création du groupe de sécurité et adhésion
- (Facultatif) Administrateur de Skype Entreprise

  Si vous souhaitez gérer Skype Entreprise Online, attribuez les droits d'administrateur de Skype Entreprise au compte d'accès du locataire Azure.
- Administrateur des utilisateurs

Autorisations de compte du service d'administration NetIQ :

- Administrateurs locaux
- Accordez au compte de remplacement avec un droit d'accès minimal une « Autorisation totale » sur les dossiers de partage ou les dossiers DFS où les répertoires privés sont provisionnés.
- **Gestion des ressources :** Pour gérer les ressources publiées dans un domaine Active Directory géré, le compte d'accès au domaine doit obtenir des autorisations d'administration locale sur ces ressources.

Après l'installation de DRA : Vous devez exécuter les commandes suivantes avant de gérer les domaines requis :

- Pour déléguer l'autorisation sur le « conteneur Objets supprimés » à partir du dossier d'installation de DRA (remarque : la commande doit être exécutée par un administrateur de domaine) :

  `DraDelObjsUtil.exe /domain:<NomDomaineNetBIOS> /delegate:<NomCompte>`
- Pour déléguer l'autorisation à « NetIQReceyleBin OU » à partir du dossier d'installation de DRA :

  `DraRecycleBinUtil.exe /domain:<NomDomaineNetBIOS> /delegate:<NomCompte>`

Accès à distance à SAM : Attribuer des contrôleurs de domaine ou des serveurs membres gérés par DRA pour activer les comptes énumérés dans le paramètre GPO ci-dessous, afin qu'ils puissent effectuer des interrogations à distance dans la base de données du gestionnaire de comptes de sécurité (SAM). La configuration doit inclure le compte de service DRA.

Accès au réseau : Restreindre les clients autorisés à passer des appels à distance vers SAM

Pour accéder à ce paramètre, procédez comme suit :

1. Ouvrez la console de gestion des stratégies de groupe sur le contrôleur de domaine.
2. Développez **Domains** > **[domain controller]** > **Group Policy Objects** (Domaines > [contrôleur de domaine] > Objets de stratégie de groupe) dans l'arborescence des nœuds.
3. Cliquez avec le bouton droit de la souris sur **Default Domain Controllers Policy** (Stratégie des contrôleurs de domaine par défaut) et sélectionnez **Edit** (Modifier) pour ouvrir l'éditeur GPO de cette stratégie.
4. Développez **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** (Configuration de l'ordinateur > Stratégies > Paramètres de Windows > Paramètres de sécurité > Stratégies locales) dans l'arborescence de nœuds de l'éditeur GPO.
5. Double-cliquez sur **Network access: Restrict clients allowed to make remote calls to SAM** (Accès au réseau : Restreindre les clients autorisés à effectuer des appels à distance vers SAM) dans le volet des stratégies, et sélectionnez **Define this policy setting** (Définir ce paramètre de stratégie).
6. Cliquez sur **Edit Security** (Modifier la sécurité) et activez **Allow** (Autoriser) pour l'accès à distance. Ajoutez le compte de service DRA s'il n'est pas déjà inclus en tant qu'utilisateur ou partie du groupe des administrateurs.
7. Appliquez les modifications. Cela ajoutera le descripteur de sécurité, `O:BAG:BAD:(A;;RC;;;BA)` aux paramètres de la stratégie.

Pour obtenir de plus amples renseignements, consultez l'article 7023292 de la base de connaissances.

Configuration requise pour la création de rapports

La configuration requise pour le composant de création de rapports de DRA comprend :

Configuration logicielle requise

Composant	Produits préalables
Cible d'installation	**Système d'exploitation** ◆ Microsoft Windows Server 2012 R2, 2016, 2019

Composant	Produits préalables
NetIQ Reporting Center (v3.3)	**Base de données :** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ L'administrateur de domaine qui gère les tâches de l'agent SQL doit disposer d'autorisations de sécurité pour Microsoft SQL Server Integration Services, sinon certains rapports du NRC ne seront pas traités. **Serveur Web :** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Composants Microsoft IIS : ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** ◆ Nécessaire pour faire fonctionner le programme d'installation du NRC ◆ Également requis sur le serveur primaire de DRA pour la configuration des services de création de rapports de DRA **REMARQUE :** Lors de l'installation du NetIQ Reporting Center (NRC) sur un ordinateur SQL Server, il peut être nécessaire d'installer .NET Framework 3.5 manuellement avant l'installation du NRC. **Protocole de sécurité des communications :** ◆ SQL Server doit prendre en charge TLS 1.2. Pour plus d'informations, reportez-vous à la rubrique Prise en charge de TLS 1.2 pour Microsoft SQL Server. ◆ Le serveur SQL doit avoir un pilote pris en charge par TLS mis à jour installé sur le serveur DRA. Le pilote suggéré est le dernier Microsoft® SQL Server® 2012 Native Client - QFE. ◆ La même version du protocole TLS doit être prise en charge dans le système d'exploitation du serveur SQL et du serveur d'administration de DRA. Par exemple, seul TLS 1.2 a été activé.
Module de création de rapports de DRA	**Base de données :** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

Exigences relatives aux licences

Votre licence détermine les produits et fonctionnalités que vous pouvez utiliser. DRA requiert une clé de licence installée avec le serveur d'administration.

Après avoir installé le serveur d'administration, vous pouvez utiliser l'utilitaire de contrôle de l'intégrité pour installer la licence que vous avez achetée. Une clé de licence d'essai (TrialLicense.lic) est également incluse dans le paquetage d'installation qui vous permet de gérer un nombre illimité de comptes d’utilisateurs et de boîtes aux lettres pendant 30 jours.

Reportez-vous au contrat de licence d'utilisateur final du produit (CLUF) pour plus de renseignements sur la définition et les restrictions de licence.

4 Installation du produit

Ce chapitre vous guide dans l'installation de Directory and Resource Administrator. Pour de plus amples renseignements sur la planification de votre installation ou de votre mise à niveau, consultez Planification de votre déploiement.

Installer le serveur d'administration DRA

Vous pouvez installer le serveur d'administration DRA en tant que nœud primaire ou secondaire dans votre environnement. Les exigences pour un serveur d'administration primaire et secondaire sont les mêmes; cependant, chaque déploiement DRA doit inclure un serveur d'administration primaire.

Le paquetage du serveur DRA présente les caractéristiques suivantes :

- **Serveur d'administration :** Stocke les données de configuration (environnement, accès délégué et stratégie), exécute les tâches des opérateurs et de l'automatisation, et vérifie l'activité de l'ensemble du système. Il possède les caractéristiques suivantes :
  - **Log Archive Resource Kit :** vous permet de consulter les informations relatives à l'audit.
  - **DRA SDK :** fournit les exemples de scripts ADSI et vous aide à créer vos propres scripts.
  - **Affectations de groupe temporaire:** Fournit les composants permettant d'activer la synchronisation des affectations de groupe temporaires.
- **Interfaces utilisateur :** interface du client Web principalement utilisée par les administrateurs assistants, mais également des options de personnalisation.
  - **Fournisseur ADSI :** vous permet de créer vos propres scripts de stratégie.
  - **Interface de ligne de commande :** vous permet d'effectuer des opérations liées à DRA.
  - **Délégation et configuration :** permet aux administrateurs système d'accéder aux fonctions de configuration et d'administration de DRA. Vous permet également de spécifier et d'affecter de façon granulaire l'accès aux ressources gérées et aux tâches aux administrateurs assistants.
  - **Extensions PowerShell :** fournit un module PowerShell qui permet aux clients non DRA de demander des opérations DRA à l'aide des applets de commande PowerShell.
  - **Console Web :** interface du client Web principalement utilisée par les administrateurs assistants, mais également des options de personnalisation.

Pour obtenir des informations sur l'installation de consoles DRA spécifiques et de clients de ligne de commande sur plusieurs ordinateurs, consultez la rubrique Installer les clients DRA.

Liste de contrôle d'installation interactive :

Étape	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour l'installation avec un compte disposant de droits d'accès d'administration locaux.
Copie et exécution de la trousse d'installation de Admin	Exécutez la trousse d'installation DRA (NetIQAdminInInstallationKit.msi) pour extraire le fichier d'installation de DRA vers le système de fichiers local. **REMARQUE :** La trousse d'installation installera .Net framework sur le serveur cible si nécessaire.
Installation de DRA	Cliquez sur **Install DRA** (Installer DRA), puis sur **Next** (Suivant) pour voir les options d'installation. **REMARQUE :** Pour exécuter l'installation plus tard, accédez à l'emplacement où le fichier d'installation a été extrait (consultez la trousse d'installation) et exécutez `Setup.exe`.
Installation par défaut	Choisissez les composants à installer et acceptez l'emplacement d'installation par défaut `C:\Program Files (x86)\NetIQ\DRA` ou spécifiez un autre emplacement pour l'installation. Options des composants : **Serveur d'administration** ◆ Log Archive Resource Kit (facultatif) ◆ DRA SDK ◆ Affectations de groupe temporaire **Interfaces utilisateur** ◆ Fournisseur ADSI (facultatif) ◆ Interface de ligne de commande (facultatif) ◆ Délégation et configuration ◆ Extensions PowerShell ◆ La console Web
Vérification des produits préalables	La boîte de dialogue **Prerequisites List** (Liste des produits préalables) affichera la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guidera lors de l'installation de tous les produits préalables qui sont nécessaires pour que l'installation réussisse.
Acceptation du CLUF	Acceptez les termes du contrat de licence d'utilisateur final.
Spécification de l'emplacement du journal	Indiquez l'emplacement où DRA stockera tous les fichiers journaux. **REMARQUE :** Les journaux de la console de délégation et de configuration et les journaux d'ADSI sont stockés dans le dossier du profil de l'utilisateur.

Étape	Détails
Sélection du mode de fonctionnement du serveur	Sélectionnez **Primary Administration Server** (Serveur d'administration primaire) pour installer le premier serveur d'administration DRA dans un ensemble multimaître (il n'y aura qu'un seul serveur primaire dans un déploiement) ou **Secondary Administration Server** (Serveur d'administration secondaire) pour joindre un nouveau serveur d'administration DRA à un ensemble multimaître existant. Pour obtenir des informations sur l'ensemble multimaître, consultez la rubrique « Configuration de l'ensemble multimaître » dans le *Guide de l'administrateur de DRA*.
Spécification des comptes d'installation et des informations d'identification	◆ Compte de service DRA ◆ Groupe AD LDS ◆ Administrateur DRA Compte Pour obtenir de plus amples renseignements, consultez :Configuration requise pour le serveur d'administration et la console Web de DRA.
Configuration des autorisations DCOM	Autorisez DRA à configurer l'accès « COM distribué » pour les utilisateurs authentifiés.
Configuration des ports	Pour obtenir de plus amples renseignements sur les ports par défaut, consultez Ports et protocoles requis.
Spécification de l'emplacement de stockage	Spécifiez l'emplacement du fichier local que DRA doit utiliser pour stocker les données d'audit et de mise en cache.
Spécification de l'emplacement de la base de données de réplication de DRA	◆ Spécifiez l'emplacement du fichier pour la base de données de réplication de DRA et le port du service de réplication. ◆ Spécifiez le certificat SSL que vous souhaitez utiliser pour les communications sécurisées avec la base de données via IIS, et indiquez le port de réplication IIS.
Spécification du certificat SSL du service REST	Sélectionnez le certificat SSL que vous utiliserez pour le service REST et spécifiez le port du service REST.
Spécification du certificat SSL de la console Web	Spécifiez le certificat SSL que vous utiliserez pour la liaison HTTPS.
Vérification de la configuration d'installation	Vous pouvez vérifier la configuration sur la page de synthèse de l'installation avant de cliquer sur **Installer** pour procéder à l'installation.
Vérification post-installation	Une fois l'installation terminée, l'outil de contrôle de l'intégrité s'exécute pour vérifier l'installation et mettre à jour la licence du produit. Pour de plus amples renseignements, consultez la section Utilitaire de contrôle de l'intégrité du *Guide de l'administrateur de DRA*.

Installer les clients DRA

Vous pouvez installer des consoles DRA et des clients de ligne de commande précis en exécutant DRAInstaller.msi avec le paquetage .mst correspondant sur la cible d'installation :

NetIQDRACLI.mst	Installe l'interface de ligne de commande
NetIQDRAADSI.mst	Installe le fournisseur DRA ADSI
NetIQDRAClients.mst	Installe toutes les interfaces utilisateur DRA

Pour déployer des clients DRA donnés sur plusieurs ordinateurs de votre entreprise, configurez un objet de stratégie de groupe pour installer le paquet .MST correspondant.

1. Démarrez Utilisateurs et ordinateurs Active Directory et créez un objet de stratégie de groupe.
2. Ajoutez le paquet DRAInstaller.msi à cet objet de stratégie de groupe.
3. Assurez-vous que cet objet de stratégie de groupe possède l'une des propriétés suivantes :
   - Chaque compte d'utilisateur du groupe dispose des autorisations d'utilisateur expérimenté pour l'ordinateur approprié.
   - Activez le paramètre de stratégie Toujours installer avec des privilèges élevés.
4. Ajoutez le fichier .mst de l'interface utilisateur à cet objet de stratégie de groupe.
5. Distribuez votre stratégie de groupe.

REMARQUE : Pour obtenir de plus amples renseignements sur la stratégie de groupe, consultez l'aide de Microsoft Windows. Pour tester et déployer facilement et en toute sécurité la stratégie de groupe dans votre entreprise, utilisez *Administrateur de stratégie de groupe*.

Installation de Workflow Automation et configuration des paramètres

Pour gérer les requêtes de Workflow Automation dans DRA, vous devez procéder comme suit :

- Installez et configurez Workflow Automation et DRA Adapter.

  Pour plus d'informations, reportez-vous au *Guide de l'administrateur de Workflow Automation* et au *Guide de référence de Workflow Automation Adapter pour DRA*.
- Configurez l'intégration de Workflow Automation avec DRA.

  Pour en savoir plus, reportez-vous à la rubrique « Configuration du serveur de Workflow Automation » dans le *Guide de l'administrateur de DRA*.
- Déléguez les pouvoirs de Workflow Automation dans DRA.

  Pour en savoir plus, reportez-vous à à la rubrique « Délégation des pouvoirs de configuration du serveur de Workflow Automation » dans le *Guide de l'administrateur de DRA*.

Les documents mentionnés ci-dessus sont disponibles sur le site de la documentation de DRA.

Installez le module de création de rapports de DRA

Le module de création de rapports de DRA nécessite l'installation du fichier DRAReportingSetup.exe à partir de la trousse d'installation NetIQ DRA.

Étapes	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour l'installation avec un compte disposant de droits d'accès d'administration locaux. Assurez-vous que ce compte dispose des privilèges d'administrateur local et de domaine, ainsi que des privilèges d'administrateur système sur le serveur SQL.
Copie et exécution de la trousse d'installation de NetIQ Admin	Copiez la trousse d'installation de DRA NetIQAdminINstallationKit.msi sur le serveur cible et exécutez le programme en double-cliquant sur le fichier ou en l'appelant à partir de la ligne de commande. La trousse d'installation extrait le fichier d'installation de DRA sur le système de fichiers local vers un emplacement personnalisable. De plus, la trousse d'installation installera .Net framework sur le serveur cible si nécessaire pour satisfaire les conditions préalables du programme d'installation du produit DRA.
Exécution de l'installation du module de création de rapports de DRA	Accédez à l'emplacement où le fichier d'installation a été extrait et exécutez DRA`ReportingSetup.exe` pour installer le composant de gestion pour l'intégration du module de création de rapports de DRA.
Vérification et installation des produits préalables	La boîte de dialogue **Produits préalables** affichera la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guidera dans l'installation de tous les produits préalables manquants qui sont requis pour que l'installation se termine avec succès. Pour obtenir de plus amples renseignements sur le centre de création de rapport de NetIQ, consultez le *Guide du centre de création de rapports* sur le site de la documentation.
Acceptation du CLUF	Acceptez les termes du contrat de licence d'utilisateur final pour terminer l'installation.

5 Mise à niveau du produit

Ce chapitre fournit un processus qui vous aide à mettre à niveau ou à migrer un environnement distribué en phases contrôlées.

Dans ce chapitre, nous supposons que votre environnement contient plusieurs serveurs d'administration, certains serveurs étant situés sur des sites distants. Cette configuration s'appelle un ensemble multimaître (MMS). Un MMS comprend un serveur d'administration primaire et un ou plusieurs serveurs d'administration secondaires associés. Pour obtenir de plus amples renseignements sur le fonctionnement d'un MMS, consultez la rubrique « Configuration d'un ensemble multimaître » du *Guide de l'administrateur de DRA*.

Planification de la mise à niveau de DRA

Exécutez le `NetIQAdminInstallationKit.msi` pour extraire le fichier d'installation de DRA, puis installez et exécutez l'utilitaire de contrôle de l'intégrité.

Veillez à planifier votre déploiement de DRA avant de commencer le processus de mise à niveau. Lors de la planification de votre déploiement, tenez compte des règles suivantes :

- Testez le processus de mise à niveau dans votre environnement de laboratoire avant de procéder à la mise à niveau vers votre environnement de production. Les tests vous permettent d'identifier et de résoudre tout problème inattendu sans affecter les responsabilités d'administration quotidiennes.
- Examinez Ports et protocoles requis.
- Déterminez combien d'administrateurs assistants dépendent de chaque MMS. Si la majorité de vos administrateurs assistants utilisent des serveurs ou des ensembles de serveurs précis, mettez d'abord à niveau ces serveurs pendant les heures creuses.
- Déterminez quels administrateurs assistants ont besoin de la console de délégation et de configuration. Vous pouvez obtenir ces informations de l'une des façons suivantes :
  - Vérifiez quels sont les administrateurs assistants associés aux groupes d'administrateurs assistants intégrés.
  - Examinez les administrateurs assistants associés aux ActiveViews intégrées.
  - Utilisez Directory and Resource Administrator Reporting pour générer des rapports sur les modèles de sécurité, tels que les rapports sur les détails d'administrateurs assistants ActiveView et les groupes d'administrateurs assistants.

Informez ces administrateurs assistants de vos projets de mise à niveau des interfaces utilisateur.

- Déterminez les administrateurs assistants qui doivent se connecter au serveur d'administration primaire. Ces administrateurs assistants doivent mettre à niveau leurs ordinateurs clients après la mise à niveau du serveur d'administration primaire.

  Informez ces administrateurs assistants de vos projets de mise à niveau des serveurs d'administration et des interfaces utilisateur.
- Déterminez si vous devez implémenter des modifications de délégation, de configuration ou de stratégie avant de commencer le processus de mise à niveau. Selon votre environnement, cette décision peut être prise site par site.
- Coordonnez la mise à niveau de vos ordinateurs clients et de vos serveurs d'administration pour garantir des temps d'arrêt minimaux. Sachez que DRA ne prend pas en charge l'exécution simultanée des versions précédentes et actuelle de DRA sur le même serveur d'administration ou ordinateur client.

IMPORTANT

- Si la console de gestion des comptes et des ressources (ARM) est installée sur votre version précédente de DRA, elle sera supprimée lors de la mise à niveau.
- Lorsque vous mettez à niveau le serveur DRA à partir d'une version 9.x de DRA, tous les locataires gérés sont supprimés de DRA. Pour continuer à utiliser ces locataires en utilisant Azure, vous devez les ajouter après la mise à niveau. Pour en savoir plus sur l'ajout de locataires, consultez les rubriques Création d'une application Azure et Ajout d'un locataire Azure dans le *Guide de l'administrateur de DRA*.
- Étant donné qu'Exchange 2010 n'est pas pris en charge dans DRA 10.1, Exchange est désactivé lors de la mise à niveau à partir de DRA 9.x. Pour continuer à effectuer des opérations Exchange après la mise à niveau, désactivez et réactivez l'option **Enable Exchange Policy** (Activer la stratégie Exchange) dans la console de délégation et de configuration. Les deux modifications doivent être « appliquées » pour que la stratégie soit réinitialisée.

  Pour obtenir de plus amples renseignements sur cette configuration de stratégie, consultez la rubrique « Activation de Microsoft Exchange » du *Guide de l'administrateur de DRA*.

Tâches préalables à la mise à niveau

Avant d'installer les mises à niveau, effectuez au préalable les étapes suivantes pour préparer chaque ensemble de serveurs.

Étapes	Détails
Sauvegardez l'instance AD LDS	Ouvrez l'utilitaire de contrôle de l'intégrité et exécutez la vérification **Sauvegarde d'instance AD LDS** pour créer une sauvegarde de votre instance AD LDS actuelle.
Établissez un plan de déploiement	Établissez un plan de déploiement pour la mise à niveau des serveurs d'administration et des interfaces utilisateur (ordinateurs clients d'administrateurs assistants). Pour obtenir de plus amples renseignements, consultez Planification de la mise à niveau de DRA.

Étapes	Détails
Dédiez un serveur secondaire pour exécuter une version précédente de DRA	*Facultatif :* Dédiez un serveur d'administration secondaire pour exécuter une version précédente de DRA lorsque vous mettez à niveau un site.
Apportez les modifications requises pour ce MMS	Apportez les modifications nécessaires aux paramètres de délégation, de configuration ou de stratégie pour ce MMS. Utilisez le serveur d'administration primaire pour modifier ces paramètres.
Synchronisez le MMS	Synchronisez les ensembles de serveurs afin que chaque serveur d'administration contienne les derniers paramètres de configuration et de sécurité.
Sauvegardez le registre du serveur primaire	Sauvegardez le registre à partir du serveur d'administration primaire. La sauvegarde de vos paramètres de registre précédents vous permet de récupérer facilement vos paramètres de configuration et de sécurité précédents..
Convertissez les comptes d'utilisateurs gMSA en comptes d'utilisateurs DRA	*Facultatif :* si vous utilisez un compte de service géré de groupe (gMSA) pour le compte de service DRA, remplacez le compte gMSA par un compte d'utilisateur DRA avant la mise à niveau. Après la mise à niveau, vous devrez changer le compte pour revenir à un compte gMSA.

REMARQUE : Si vous devez restaurer la sauvegarde de l'instance AD LDS, procédez comme suit :

1. Arrêtez l'instance AD LDS en cours dans Gestion de l'ordinateur > Services. Le titre sera différent : `NetIQDRASecureStoragexxxxx`.
2. Remplacez le **fichier actuel** `adamnts.dit` par le **fichier de sauvegarde** `adamnts.dit`, comme indiqué ci-dessous :
   - Emplacement du fichier actuel : `%ProgramData%/NetIQ/DRA/<DRAInstanceName>/data/`
   - Emplacement du fichier de sauvegarde : `%ProgramData%/NetIQ/ADLDS/`
3. Redémarrez l'instance AD LDS.

Rubriques sur les préalables à la mise à niveau :

- « Utilisation d'un serveur d'administration local dédié pour exécuter une version précédente de DRA » page 42
- « Synchronisation de votre ensemble de serveurs DRA des versions précédentes » page 43
- « Sauvegarde du registre du serveur d'administration » page 43

Utilisation d'un serveur d'administration local dédié pour exécuter une version précédente de DRA

L'utilisation d'un ou de plusieurs serveurs d'administration secondaires pour exécuter une version précédente de DRA localement sur un site pendant la mise à niveau peut aider à réduire les temps d'arrêt et les connexions coûteuses aux sites distants. Cette étape est facultative et permet aux administrateurs assistants d'utiliser une version précédente de DRA tout au long du processus de mise à niveau, jusqu'à ce que vous soyez satisfait de votre déploiement.

Considérez cette option si vous avez une ou plusieurs des exigences de mise à niveau suivantes :

- Vous exigez peu ou pas de temps d'arrêt.
- Vous devez prendre en charge un grand nombre d'administrateurs assistants et vous ne pouvez pas mettre à niveau tous les ordinateurs clients immédiatement.
- Vous souhaitez continuer à prendre en charge l'accès à une version précédente de DRA après la mise à niveau du serveur d'administration primaire.
- Votre environnement comprend un MMS qui s'étend sur plusieurs sites.

Vous pouvez installer un nouveau serveur d'administration secondaire ou désigner un serveur secondaire existant exécutant une version précédente de DRA. Si vous avez l'intention de mettre à niveau ce serveur, il devrait être le dernier serveur mis à niveau. Sinon, désinstallez complètement DRA de ce serveur lorsque vous terminez votre mise à niveau.

Configuration d'un nouveau serveur secondaire

L'installation d'un nouveau serveur d'administration secondaire sur un site local peut vous aider à éviter des connexions coûteuses à des sites distants, et garantit que vos administrateurs assistants peuvent continuer à utiliser une version précédente de DRA sans interruption. Si votre environnement comprend un MMS qui s'étend sur plusieurs sites, vous devez envisager cette option. Par exemple, si votre MMS se compose d'un serveur d'administration primaire sur votre site de Londres et d'un serveur d'administration secondaire sur votre site de Tokyo, envisagez d'installer un serveur secondaire sur le site de Londres et de l'ajouter au MMS correspondant. Ce serveur supplémentaire permet aux administrateurs assistants du site de Londres d’utiliser une version précédente de DRA jusqu’à la fin de la mise à niveau.

Utilisation d'un serveur secondaire existant

Vous pouvez utiliser un serveur d'administration secondaire existant comme serveur dédié pour une version de DRA précédente. Si vous ne prévoyez pas de mettre à niveau un serveur d'administration secondaire sur un site donné, vous devez envisager cette option. Si vous ne pouvez pas dédier un serveur secondaire existant, envisagez d'installer un nouveau serveur d'administration à cette fin. L'utilisation d'un ou de plusieurs serveurs secondaires dédiés pour exécuter une version de DRA précédente permet à vos administrateurs assistants de continuer à utiliser une version de DRA précédente sans interruption jusqu'à la fin de la mise à niveau. Cette option fonctionne mieux dans les environnements plus grands qui utilisent un modèle d'administration centralisé.

Synchronisation de votre ensemble de serveurs DRA des versions précédentes

Avant de sauvegarder le registre des versions précédentes de DRA ou de commencer le processus de mise à niveau, assurez-vous d'avoir synchronisé les ensembles de serveurs afin que chaque serveur d'administration contienne les derniers paramètres de configuration et de sécurité.

REMARQUE : Assurez-vous d'avoir apporté les modifications nécessaires aux paramètres de délégation, de configuration ou de stratégie pour ce MMS. Utilisez le serveur d'administration primaire pour modifier ces paramètres. Une fois que vous avez mis à niveau le serveur d'administration primaire, vous ne pouvez plus synchroniser les paramètres de délégation, de configuration ou de stratégie avec les serveurs d'administration exécutant les versions précédentes de DRA.

Pour synchroniser votre ensemble de serveurs existant :

1. Connectez-vous au serveur d'administration primaire en tant qu'administrateur intégré.
2. Ouvrez la console de délégation et de configuration et développez l'option **Configuration Management** (Gestion de la configuration).
3. Cliquez sur **Serveurs d'administration**.
4. Dans le volet droit, sélectionnez le serveur d'administration primaire approprié pour cet ensemble de serveurs.
5. Cliquez sur **Propriétés**.
6. Dans l'onglet Planification de la synchronisation, cliquez sur **Actualiser maintenant**.
7. Vérifiez que la synchronisation est terminée et que tous les serveurs d'administration secondaires sont disponibles.

Sauvegarde du registre du serveur d'administration

La sauvegarde du registre du serveur d'administration vous permet de revenir à vos configurations précédentes. Par exemple, si vous devez désinstaller complètement la version actuelle de DRA et utiliser la version précédente, une sauvegarde de vos paramètres de registre précédents vous permet de récupérer facilement vos paramètres de configuration et de sécurité précédents.

Toutefois, soyez prudent lorsque vous modifiez votre registre. S'il y a une erreur dans votre registre, le serveur d'administration peut ne pas fonctionner comme prévu. Si une erreur se produit pendant le processus de mise à niveau, vous pouvez utiliser la sauvegarde de vos paramètres de registre pour restaurer ce dernier. Pour obtenir de plus amples renseignements, consultez l'aide de l'*Éditeur de registre*.

IMPORTANT : La version du serveur DRA, le nom du système d'exploitation Windows et la configuration du domaine géré doivent être exactement les mêmes lors de la restauration du registre.

IMPORTANT : Avant de procéder à la mise à niveau, sauvegardez le système d'exploitation Windows de la machine hébergeant DRA ou créez une image instantanée de la machine virtuelle.

Pour sauvegarder le registre du serveur d'administration :

1. Exécutez `regedit.exe`.
2. Cliquez avec le bouton droit de la souris sur le nœud `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint`, puis sélectionnez **Exporter**.
3. Spécifiez le nom et l'emplacement du fichier dans lequel enregistrer la clé de registre, puis cliquez sur **Enregistrer**.

Mise à niveau du serveur d'administration DRA

La liste de contrôle suivante vous guide tout au long du processus de mise à niveau. Utilisez ce processus pour mettre à niveau chaque ensemble de serveurs de votre environnement. Si vous ne l'avez pas encore fait, utilisez l'utilitaire de vérification de l'intégrité pour créer une sauvegarde de votre instance AD LDS actuelle.

AVERTISSEMENT : Ne mettez pas à niveau vos serveurs d'administration secondaires tant que vous n'avez pas mis à niveau le serveur d'administration primaire pour ce MMS.

Vous pouvez répartir le processus de mise à niveau en plusieurs phases, en mettant à niveau un MMS à la fois. Ce processus de mise à niveau vous permet également d'inclure temporairement des serveurs secondaires exécutant une version précédente de DRA et des serveurs secondaires exécutant la version actuelle de DRA dans le même MMS. DRA prend en charge la synchronisation entre les serveurs d'administration exécutant une version précédente de DRA et les serveurs exécutant la version actuelle de DRA. Sachez cependant que DRA ne prend pas en charge l'exécution simultanée des versions précédentes et actuelle de DRA sur le même serveur d'administration ou ordinateur client.

IMPORTANT : L'installation de la mise à niveau de DRA apporte les modifications suivantes lorsque vous mettez à niveau le serveur DRA d'une version DRA 9.x vers une version DRA 10.x :

- Déplace les configurations utilisateur du serveur UCH et de Workflow Automation de la console Web vers la console de délégation et de configuration
- Supprime l'ancien composant Web du serveur.
- Supprime tout locataire géré.

  Pour en savoir plus sur l'ajout de locataires, consultez la rubrique « Configuration des locataires Azure » dans le *Guide de l'administrateur de DRA*.
- Si vous avez installé la console de gestion des comptes et des ressources dans une version antérieure, celle-ci est supprimée lorsque vous passez à une version 10.x de DRA.
- Lors d'une mise à niveau de MMS, le serveur primaire est mis à niveau en premier, suivi par les serveurs secondaires. Pour une réplication réussie des affectations de groupe temporaires dans le serveur secondaire, exécutez **Multi-master synchronization schedule** (programme de synchronisation multimaître) manuellement ou attendez son exécution planifiée.

- Étant donné qu'Exchange 2010 n'est pas pris en charge dans DRA 10, Exchange est désactivé lors de la mise à niveau à partir de DRA 9.x. Pour continuer à effectuer des opérations Exchange après la mise à niveau, désactivez et réactivez l'option **Enable Exchange Policy** (Activer la stratégie Exchange) dans la console de délégation et de configuration. Les deux modifications doivent être « appliquées » pour que la stratégie soit réinitialisée.

  Pour obtenir de plus amples renseignements sur cette configuration de stratégie, consultez la rubrique « Activation de Microsoft Exchange » du *Guide de l'administrateur de DRA*.

Étapes	Détails
Exécution de l'utilitaire de contrôle de l'intégrité	Installez l'utilitaire autonome de contrôle de l'intégrité de DRA et exécutez-le à l'aide d'un compte de service. Corrigez les problèmes.
Réalisation d'une mise à niveau d'essai	Effectuez une mise à niveau d'essai dans votre environnement de laboratoire pour identifier les problèmes potentiels et limiter les temps d'arrêt de production.
Définition de l'ordre de mise à niveau	Déterminez l'ordre dans lequel vous souhaitez mettre à niveau vos ensembles de serveurs.
Préparation de chaque MMS pour la mise à niveau	Préparez chaque MMS pour la mise à niveau. Pour obtenir de plus amples renseignements, consultez Tâches préalables à la mise à niveau.
Mise à niveau du serveur primaire	Mettez à niveau le serveur d'administration primaire dans le MMS approprié. Pour plus de renseignements, consultez Mise à niveau du serveur d'administration primaire.
Installation du nouveau serveur secondaire	*(Facultatif)* Pour réduire les temps d'arrêt sur les sites distants, installez un serveur d'administration secondaire local exécutant la dernière version de DRA. Pour plus de renseignements, consultez Installation d'un serveur d'administration secondaire local pour la version actuelle de DRA.
Déploiement des interfaces utilisateur	Déployez les interfaces utilisateur vers vos administrateurs assistants. Pour plus de renseignements, consultez Déploiement des interfaces utilisateur DRA
Mise à niveau les serveurs secondaires	Mettez à niveau les serveurs d'administration secondaires dans le MMS. Pour plus de renseignements, consultez Mise à niveau des serveurs d'administration secondaire.
Mise à niveau du module de création de rapports de DRA	Mettez à niveau le module de création de rapports de DRA. Pour plus de renseignements, consultez Mise à niveau du module de création de rapports.
Exécution de l'utilitaire de contrôle de l'intégrité	Exécutez l'utilitaire de contrôle de l'intégrité qui a été installé dans le cadre de la mise à niveau. Corrigez les problèmes.
Ajouter des locataires Azure *(après la mise à niveau)*	(*Facultatif, après la mise à niveau)* Si vous gériez des locataires Azure avant la mise à niveau, alors ils seront supprimés lors de la mise à niveau. Vous devrez ajouter ces locataires à nouveau et exécuter une actualisation complète du cache des comptes à partir de la console de délégation et de configuration. Pour en savoir plus, reportez-vous à la rubrique « Configuration des locataires Azure » dans le *Guide de l'administrateur de DRA*.

Étapes	Détails
Mise à jour de la configuration de la console Web *après la mise à jour)*	*(Conditionnel, après la mise à niveau)* Si vous avez l'une ou l'autre des configurations de la console Web ci-dessous avant la mise à niveau, elles devront être mises à jour une fois l'installation de la mise à niveau terminée : ◆ Connexions au serveur par défaut activées ◆ Fichiers de configuration modifiés Pour obtenir de plus amples renseignements, consultez Mise à jour de la configuration de la console Web - après l'installation.

Rubriques relatives à la mise à niveau du serveur :

- « Mise à niveau du serveur d'administration primaire » page 46
- « Installation d'un serveur d'administration secondaire local pour la version actuelle de DRA » page 46
- « Déploiement des interfaces utilisateur DRA » page 47
- « Mise à niveau des serveurs d'administration secondaire » page 48
- « Mise à jour de la configuration de la console Web - après l'installation » page 48

Mise à niveau du serveur d'administration primaire

Une fois que vous avez terminé avec la préparation de votre MMS, mettez à niveau le serveur d'administration primaire. Ne mettez pas à niveau les interfaces utilisateur sur les ordinateurs clients tant que vous n'avez pas mis à niveau le serveur d'administration primaire. Pour obtenir de plus amples renseignements, consultez Déploiement des interfaces utilisateur DRA.

REMARQUE : Pour obtenir des considérations et des instructions de mise à niveau plus détaillées, consultez les *notes de mise à jour de Directory and Resource Administrator*.

Avant de procéder à la mise à niveau, informez vos administrateurs assistants lorsque vous prévoyez de démarrer ce processus. Si vous avez dédié un serveur d'administration secondaire pour exécuter une version précédente de DRA, identifiez également ce serveur afin que les administrateurs assistants puissent continuer à utiliser la version précédente de DRA lors de la mise à niveau.

REMARQUE : Une fois que vous avez mis à niveau le serveur d'administration primaire, vous ne pouvez plus synchroniser les paramètres de délégation, de configuration ou de stratégie de ce serveur vers les serveurs d'administration secondaires exécutant une version précédente de DRA.

Installation d'un serveur d'administration secondaire local pour la version actuelle de DRA

L'installation d'un nouveau serveur d'administration secondaire pour exécuter la version actuelle de DRA sur un site local peut vous aider à réduire les connexions coûteuses aux sites distants tout en réduisant les temps d'arrêt généraux et en permettant un déploiement plus rapide des interfaces

utilisateur. Cette étape est facultative et permet aux administrateurs assistants d'utiliser la version actuelle et une version précédente de DRA tout au long du processus de mise à niveau, jusqu'à ce que vous soyez satisfait de votre déploiement.

Considérez cette option si vous avez une ou plusieurs des exigences de mise à niveau suivantes :

- Vous exigez peu ou pas de temps d'arrêt.
- Vous devez prendre en charge un grand nombre d'administrateurs assistants et vous ne pouvez pas mettre à niveau tous les ordinateurs clients immédiatement.
- Vous souhaitez continuer à prendre en charge l'accès à une version précédente de DRA après la mise à niveau du serveur d'administration primaire.
- Votre environnement comprend un MMS qui s'étend sur plusieurs sites.

Par exemple, si votre MMS se compose d'un serveur d'administration primaire sur votre site de Londres et d'un serveur d'administration secondaire sur votre site de Tokyo, envisagez d'installer un serveur secondaire sur le site de Tokyo et de l'ajouter au MMS correspondant. Ce serveur supplémentaire équilibre mieux la charge d'administration quotidienne sur le site de Tokyo et permet aux administrateurs assistants de chaque site d'utiliser une version précédente de DRA ainsi que la version actuelle de DRA jusqu'à la fin de la mise à niveau. De plus, vos administrateurs assistants ne subissent aucun temps d'arrêt, car vous pouvez immédiatement déployer les interfaces utilisateur actuelles de DRA. Pour obtenir de plus amples renseignements sur la mise à niveau des interfaces utilisateur, consultezDéploiement des interfaces utilisateur DRA.

Déploiement des interfaces utilisateur DRA

En règle générale, vous devez déployer les interfaces utilisateur actuelles de DRA après avoir mis à niveau le serveur d'administration primaire et un serveur d'administration secondaire. Toutefois, pour les administrateurs assistants qui doivent utiliser le serveur d'administration primaire, assurez-vous de mettre à niveau leurs ordinateurs clients en premier en installant la console de délégation et de configuration. Pour obtenir de plus amples renseignements, consultez Planification de la mise à niveau de DRA.

Si vous effectuez souvent un traitement par lots par l'interface CLI, le fournisseur ADSI ou PowerShell, ou si vous générez fréquemment des rapports, envisagez d'installer ces interfaces utilisateur sur un serveur d'administration secondaire dédié afin de maintenir un équilibre de charge approprié dans le MMS.

Vous pouvez laisser vos administrateurs assistants installer les interfaces utilisateur de DRA ou déployer ces interfaces à l'aide d'une stratégie de groupe. Vous pouvez également déployer facilement et rapidement la console Web sur plusieurs administrateurs assistants.

REMARQUE : Vous ne pouvez pas exécuter plusieurs versions de composants DRA côte à côte sur le même serveur DRA. Si vous prévoyez de mettre à niveau progressivement vos ordinateurs clients administrateurs assistants, envisagez de déployer la console Web pour garantir un accès immédiat à un serveur d'administration exécutant la version actuelle de DRA.

Mise à niveau des serveurs d'administration secondaire

Lors de la mise à niveau de serveurs d'administration secondaires, vous pouvez mettre à niveau chaque serveur en fonction de vos exigences en matière d'administration. Tenez également compte de la manière dont vous envisagez de mettre à niveau et de déployer les interfaces utilisateur DRA. Pour obtenir de plus amples renseignements, consultez Déploiement des interfaces utilisateur DRA.

Par exemple, un schéma de mise à niveau classique peut comprendre les étapes suivantes :

1. Mise à niveau d'un serveur d'administration secondaire.
2. Demandez aux administrateurs assistants qui utilisent ce serveur d'installer les interfaces utilisateur appropriées, telles que la console Web.
3. Répétez les étapes 1 et 2 ci-dessus jusqu'à la mise à niveau complète du MMS.

Avant de procéder à la mise à niveau, informez vos administrateurs assistants lorsque vous prévoyez de démarrer ce processus. Si vous avez dédié un serveur d'administration secondaire pour exécuter une version précédente de DRA, identifiez également ce serveur afin que les administrateurs assistants puissent continuer à utiliser la version précédente de DRA lors de la mise à niveau. Lorsque vous terminez le processus de mise à niveau pour ce MMS et que tous les ordinateurs clients d'administrateurs assistants exécutent des interfaces utilisateur mises à niveau, déconnectez tous les serveurs ayant des versions précédentes de DRA.

Mise à jour de la configuration de la console Web - après l'installation

Effectuez l'une ou l'autre ou les deux actions suivantes, après l'installation de la mise à niveau, si elles sont applicables à votre environnement DRA :

Connexion par défaut au serveur DRA

Le composant Service REST de DRA est consolidé avec le serveur DRA à partir de DRA 10.1. Si la connexion par défaut au serveur DRA est configurée avant la mise à niveau à partir d'une version DRA 10.0.x ou antérieure, vous devez revoir ces paramètres après la mise à niveau, car il n'existe désormais qu'une seule configuration de connexion, la connexion au serveur DRA. Vous pouvez accéder à cette configuration dans la console Web en cliquant sur **Administration** > **Configuration** > **DRA Server Connection** (Administration > Configuration > Connexion au serveur DRA).

Vous pouvez également mettre à jour ces paramètres après la mise à niveau dans le fichier `web.config` situé à `C:\inetpub\wwwroot\DRAClient\rest` sur le serveur de la console Web de DRA, en procédant comme suit :

```
<restService useDefault="Never">
<serviceLocation address="<REST server name>" port="8755"/>
</restService>
```

Configuration de la connexion à la console Web

Lors de la mise à niveau à partir de DRA 10.0.x ou de versions antérieures, si le service DRA REST est installé sans le serveur DRA, la désinstallation du service DRA REST est une condition préalable à la mise à niveau. Une copie des fichiers qui ont été modifiés avant la mise à niveau est effectuée sur `C:\ProgramData\NetIQ\DRA\Backup\` sur le serveur. Vous pouvez utiliser ces fichiers comme référence pour mettre à jour ceux qui sont pertinents après la mise à niveau.

Mise à niveau de Workflow Automation

Pour effectuer une mise à niveau sur place dans des environnements 64 bits non regroupés, il suffit d'exécuter le programme d'installation de Workflow Automation sur vos ordinateurs sur lesquels Workflow Automation est déjà installé. Il n'est pas nécessaire d'arrêter les services de Workflow Automation en cours d'exécution.

Tous les adaptateurs de Workflow Automation qui ne sont pas intégrés au programme d'installation de Workflow Automation doivent être désinstallés et réinstallés après la mise à niveau.

Pour des informations plus détaillées sur la mise à niveau de Workflow Automation, consultez la rubrique « Mise à niveau à partir d'une version précédente » dans le *Guide de l'administrateur de Workflow Automation*.

Mise à niveau du module de création de rapports

Avant de mettre à niveau le module de création de rapports de DRA, assurez-vous que votre environnement répond à la configuration minimale requise pour NRC 3.3. Pour obtenir de plus amples renseignements sur les exigences d'installation et les considérations relatives à la mise à niveau, consultez le *Guide de NetIQ Reporting Center Reporting*.

Étapes	Détails
Désactivation de la prise en charge du module de création de rapports de DRA	Pour vous assurer que les collecteurs de rapports ne s'exécutent pas pendant le processus de mise à niveau, désactivez la prise en charge du module de création de rapports de DRA dans la fenêtre Configuration du service de création de rapports de la console de délégation et de configuration.
Connexion au serveur d'instance SQL avec les informations d'identification applicables	Connectez-vous au serveur Microsoft Windows sur lequel vous avez installé l'instance SQL pour les bases de données de création de rapports avec un compte d'administrateur. Assurez-vous que ce compte dispose des privilèges d'administrateur local, ainsi que des privilèges d'administrateur système sur le serveur SQL.
Exécution du programme d'installation du module de création de rapports de DRA	Exécutez DRA`ReportingSetup.exe`. à partir de la trousse d'installation et suivez les instructions de l'assistant d'installation.
Activation de la prise en charge du module de création de rapports de DRA	Sur votre serveur d'administration primaire, activez la création de rapports dans la console de délégation et de configuration.

Si votre environnement utilise l'intégration SSRS, vous devrez redéployer vos rapports. Pour obtenir de plus amples renseignements sur le redéploiement des rapports, consultez le *Guide de Reporting Center* sur le site de la documentation.

III Configuration du produit

Ce chapitre décrit les étapes et les procédures de configuration requises si vous installez Directory and Resource Administrator pour la première fois.

6 Liste de contrôle de configuration

Utilisez la liste de contrôle suivante pour vous guider dans la configuration de DRA lors de la première utilisation.

Étapes	Détails
Application d'une licence DRA	Utilisez l'utilitaire de contrôle de l'intégrité pour appliquer une licence DRA. Pour obtenir de plus amples renseignements sur les licences DRA, consultez Exigences relatives aux licences.
Ouverture de Délégation et configuration	À l'aide du compte de service DRA, connectez-vous à un ordinateur sur lequel la console de délégation et de configuration est installée. Ouvrez la console.
Ajout du premier domaine géré à DRA	Ajoutez le premier domaine géré à DRA. **REMARQUE :** Vous pouvez commencer à déléguer des pouvoirs à la fin de la première actualisation complète du compte.
Ajout des domaines gérés et des sous-arborescences	*Facultatif :* Ajoutez des domaines gérés et des sous-arborescences supplémentaires à DRA. Pour obtenir de plus amples renseignements sur les domaines gérés, consultezAjout de domaines gérés.
Configuration des paramètres DCOM	*Facultatif :* Configurer les paramètres DCOM. Pour obtenir de plus amples renseignements sur les paramètres DCOM, consultez Configuration des paramètres DCOM.
Configurer les contrôleurs de domaine et les serveurs d'administration	Configurez l'ordinateur client exécutant la console de délégation et de configuration pour chaque contrôleur de domaine et chaque serveur d'administration. Pour obtenir de plus amples renseignements, consultez Configuration du contrôleur de domaine et du serveur d'administration.
Configurer les services de DRA pour un gMSA	*Facultatif :* configurer les services DRA pour un compte de service géré de groupe (gMSA). Pour obtenir de plus amples renseignements, consultez Configurer des services DRA pour un compte de service géré de groupe.

7 Installation ou mise à niveau de licences

DRA requiert un fichier de clé de licence. Ce fichier contient vos informations de licence et est installé sur le serveur d'administration. Après avoir installé le serveur d'administration, utilisez l'utilitaire de contrôle de l'intégrité pour installer la licence que vous avez achetée. Si cela est nécessaire, une clé de licence d'essai (`TrialLicense.lic`) est également incluse dans le paquetage d'installation qui vous permet de gérer un nombre illimité de comptes d'utilisateurs et de boîtes aux lettres pendant 30 jours.

Pour mettre à niveau une licence existante ou d'évaluation, ouvrez la console de délégation et configuration et accédez à **Configuration Management**> **Mettre à jour la licence**. Lorsque vous mettez à niveau votre licence, mettez à niveau le fichier de licence sur chaque serveur d'administration.

8 Ajout de domaines gérés

Vous pouvez ajouter des domaines gérés, des serveurs ou des postes de travail après avoir installé le serveur d'administration. Lorsque vous ajoutez le premier domaine géré, vous devez vous connecter à l'aide du compte de service DRA sur un ordinateur sur lequel la console de délégation et de configuration est installée. Vous devez également disposer de droits d'administration dans le domaine, tels que les droits accordés au groupe Administrateurs de domaine. Pour ajouter des domaines gérés et des ordinateurs après avoir installé le premier domaine géré, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

REMARQUE : Une fois l'ajout des domaines gérés terminé, assurez-vous que les planifications d'actualisation du cache des comptes pour ces domaines sont correctes. Pour obtenir de plus amples renseignements sur la modification de la planification d'actualisation du cache de comptes, consultez la rubrique « Configuration de la mise en cache » dans le *Guide de l'administrateur de DRA*.

---

9 Ajout de sous-arborescences gérées

Vous pouvez ajouter des sous-arborescences gérées et manquantes à partir de domaines Microsoft Windows précis après avoir installé le serveur d'administration. Ces fonctions sont exécutées dans la console de délégation et de configuration à partir du nœud **Configuration Management** > **Managed Domains** (Gestion de la configuration > Domaines gérés). Pour ajouter des sous-arborescences gérées après avoir installé le serveur d'administration, vous devez disposer des pouvoirs appropriés, telles que celles incluses dans le rôle intégré Configurer les serveurs et les domaines. Pour vous assurer que le compte d'accès spécifié dispose des autorisations nécessaires pour gérer cette sous-arborescence et effectuer des actualisations incrémentielles du cache de comptes, utilisez l'utilitaire Objets supprimés pour vérifier et déléguer les autorisations appropriées.

Pour obtenir de plus amples renseignements sur l'utilisation de cet utilitaire, consultez la rubrique « Utilitaire Objets supprimés » dans le *Guide d'administration de DRA*.

Pour obtenir de plus amples renseignements sur la configuration du compte d'accès, consultez la rubrique « Spécification des comptes d'accès au domaine » dans le *Guide de l'administrateur de DRA*.

REMARQUE : Une fois l'ajout des sous-arborescences gérées terminé, assurez-vous que les planifications d'actualisation du cache des comptes pour les domaines correspondants sont correctes. Pour obtenir de plus amples renseignements sur la modification de la planification d'actualisation du cache de comptes, consultez la rubrique « Configuration de la mise en cache » dans le *Guide de l'administrateur de DRA*.

---

10 Configuration des paramètres DCOM

Configurez les paramètres DCOM sur le serveur d'administration principal si vous n'avez pas autorisé le programme d'installation à configurer DCOM pour vous.

Si vous avez choisi de ne pas configurer le modèle COM distribué pendant le processus d'installation de DRA, vous devez mettre à jour l'adhésion au groupe Utilisateurs du modèle COM distribué pour inclure tous les comptes d'utilisateurs qui utilisent DRA. Cette adhésion doit inclure le compte du service de DRA, tous les administrateurs assistants, et le compte utilisé pour gérer les services de DRA REST, DRA Host et DRA Admin.

Pour configurer le groupe Utilisateurs du modèle COM distribué :

1. Connectez-vous à un ordinateur d'administration de DRA en tant qu'administrateur DRA.
2. Démarrez la console de délégation et de configuration. Si la console ne se connecte pas automatiquement au serveur d'administration, établissez la connexion manuellement.

   REMARQUE : Vous ne pourrez peut-être pas vous connecter au serveur d'administration si le groupe Utilisateurs du modèle COM distribué ne contient aucun compte Administrateur assistant. Si tel est le cas, configurez le groupe Utilisateurs du modèle COM distribué à l'aide du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Pour obtenir de plus amples renseignements sur l'utilisation du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, consultez le site Web de Microsoft.

   ---
3. Dans le volet gauche, développez **Gestion des comptes et des ressources**.
4. Développez **Tous mes objets gérés**.
5. Développez le nœud de domaine pour chaque domaine où vous avez un contrôleur de domaine.
6. Cliquez sur le conteneur **Intégré**.
7. Recherchez le groupe Utilisateurs du modèle COM distribué.
8. Dans la liste des résultats de la recherche, cliquez sur le groupe **Utilisateurs du modèle COM distribué**.
9. Cliquez sur **Membres** dans le volet inférieur, puis cliquez sur **Ajouter des membres**.
10. Ajoutez des utilisateurs et des groupes qui utiliseront DRA. Assurez-vous d'ajouter le compte de service DRA à ce groupe.
11. Cliquez sur **OK**.

11 Configuration du contrôleur de domaine et du serveur d'administration

Après avoir configuré l'ordinateur client exécutant la console de délégation et de configuration, vous devez configurer chaque contrôleur de domaine et chaque serveur d'administration.

Pour configurer le contrôleur de domaine et le serveur d'administration :

1. Dans le menu Démarrer, allez à **Control Panel** > **System and Security** (Panneau de configuration > Système et sécurité).
2. Ouvrez les outils d'administration, puis les services de composants.
3. Développez **Component Services** > **Computers** > **My Computer** > **DCOM Config** (Services de composants > Ordinateurs > Poste de travail > Config DCOM).
4. Sélectionnez **Service d'administration MCS OnePoint** sur le serveur d'administration.
5. Sur le menu Action, cliquez sur **Propriétés**.
6. Dans l'onglet Général de la zone Niveau d'authentification, sélectionnez **Paquet**.
7. Dans l'onglet Sécurité de la zone Autorisations d'accès, sélectionnez **Personnaliser**, puis cliquez sur **Modifier**.
8. Assurez-vous que le groupe Utilisateurs du modèle COM distribué est disponible. S'il n'est pas disponible, ajoutez-le. Si le groupe Tout le monde est disponible, supprimez-le.
9. Assurez-vous que le groupe Utilisateurs du modèle COM distribué possède des autorisations Accès local et distant.
10. Dans l'onglet Sécurité de la zone Autorisations de lancement et d'activation, sélectionnez **Personnaliser**, puis cliquez sur **Modifier**.
11. Assurez-vous que le groupe Utilisateurs du modèle COM distribué est disponible. S'il n'est pas disponible, ajoutez-le. Si le groupe Tout le monde est disponible, supprimez-le.
12. Assurez-vous que le groupe Utilisateurs du modèle COM distribué dispose des autorisations suivantes :
    - Lancement local
    - Lancement à distance
    - Activation locale
    - Activation à distance
13. Appliquez les modifications.

12 Configurer des services DRA pour un compte de service géré de groupe

Si nécessaire, vous pouvez utiliser un compte de service géré de groupe (gMSA) pour les services DRA. Pour obtenir de plus amples renseignements sur l'utilisation d'un gMSA, consultez la référence Microsoft *Présentation des comptes de services gérés de groupe*. Cette section explique comment configurer DRA pour un compte de service de gestion de groupe après avoir préalablement ajouté le compte à Active Directory.

IMPORTANT : N'utilisez pas le gMSA comme un compte de service lors de l'installation de DRA.

Pour configurer le serveur d'administration primaire de DRA pour un gMSA :

1. Ajoutez le gMSA en tant que membre des groupes suivants :
   - Groupe d'administrateurs locaux sur le serveur de DRA
   - Groupe AD LDS dans le domaine géré par DRA
2. Remplacez le compte de connexion dans les propriétés du service pour chacun des services ci-dessous par gMSA :
   - Service d'administration NetIQ
   - Service d'audit NetIQ DRA
   - Service de cache de BD NetIQ DRA

     Service de cache NetIQ DRA
   - Service de base NetIQ DRA
   - Archivage des journaux NetIQ DRA
   - Service de réplication NetIQ DRA
   - Service Rest NetIQ DRA
   - Service Skype NetIQ DRA
3. Redémarrez tous les services.

Pour configurer le serveur d'administration secondaire de DRA pour un gMSA :

1. Installez le serveur secondaire.
2. Sur le serveur primaire, attribuez le rôle **Configure Servers and Domains** (Configurer les serveurs et les domaines) à l'ActiveView **Administration Servers and Managed Domains** (Serveurs d'administration et domaines gérés) pour le compte de service du serveur secondaire.
3. Sur le serveur primaire, ajoutez un nouveau serveur secondaire et spécifiez le compte de service du serveur secondaire.

4. Ajoutez le gMSA au groupe d'administrateurs local sur le serveur d'administration secondaire de DRA.
5. Sur le serveur secondaire, remplacez le compte d'ouverture de session de tous les services DRA par gMSA, puis redémarrez les services DRA