Directory and Resource Administrator

Guide d’installation

Juillet 2018

Mentions légales

À propos de ce guide

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

Ce manuel vous guide tout au long de la procédure d'installation et vous aide à prendre les décisions appropriées dans le cadre de l'installation et de la configuration de DRA.

Public

Ce manuel fournit des informations à quiconque effectue l'installation de DRA.

Documentation supplémentaire

Ce guide fait partie de la documentation consacrée à Directory and Resource Administrator. Pour obtenir une liste complète des publications relatives à cette version, visitez le site Web de la documentation (https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

Contacter le support

Pour toute question concernant les produits, tarifs et fonctionnalités, contactez votre partenaire local. Si vous ne pouvez pas contacter votre partenaire, contactez notre équipe de support ventes.

Monde :	www.netiq.com/about_netiq/officelocations.asp
États-Unis et Canada :	1-888-323-6768
Courrier électronique :	info@netiq.com
Site Web :	www.netiq.com

Contacter le support technique

Pour tout problème spécifique au produit, contactez notre équipe du support technique.

Monde :	www.netiq.com/support/contactinfo.asp
Amérique du Nord et du Sud :	1-713-418-5555
Europe, Moyen-Orient et Afrique :	+353 (0) 91-782 677
Courrier électronique :	support@netiq.com
Site Web :	www.netiq.com/support

Contacter le support en charge de la documentation

Notre objectif est de vous proposer une documentation qui réponde à vos besoins. Si vous avez des suggestions pour améliorer la documentation, cliquez sur **comment on this topic** (Ajouter un commentaire sur cette rubrique) situé en bas de chaque page dans la version HTML de la documentation. Vous pouvez également envoyer un message électronique à l'adresse Documentation-Feedback@netiq.com. Nous accordons une grande importance à vos commentaires et sommes impatients de connaître vos impressions.

Contacter la communauté d'utilisateurs en ligne

Les communautés NetIQ et la communauté en ligne de NetIQ sont un réseau collaboratif vous mettant en relation avec vos homologues et des spécialistes de NetIQ. En proposant des informations immédiates, des liens utiles vers des ressources et un accès aux experts NetIQ, les communautés NetIQ vous aident à maîtriser les connaissances nécessaires pour tirer pleinement parti du potentiel de vos investissements informatiques. Pour plus d'informations, consultez le site http://community.netiq.com.

1 Mise en route

Avant d'installer et de configurer l'ensemble des composants de Directory and Resource Administrator™ (DRA), vous devez comprendre les principes de base du fonctionnement de DRA au sein de votre entreprise et le rôle des composants DRA dans l'architecture du produit.

Qu'est-ce que Directory and Resource Administrator ?

Directory and Resource Administrator fournit une administration sécurisée et efficace des identités à privilèges au sein de Microsoft Active Directory (AD). DRA effectue une délégation granulaire du « privilège minimal » afin que les administrateurs et les utilisateurs reçoivent uniquement les autorisations nécessaires dans le cadre de leurs responsabilités spécifiques. DRA veille également au respect des stratégies, fournit des audits et des rapports détaillés sur les activités, mais simplifie aussi la réalisation des tâches répétitives grâce à l'automatisation des processus informatiques. Chacune de ces fonctionnalités contribue à protéger les environnements Active Directory et Exchange de vos clients contre le risque de réaffectation de privilèges, les erreurs, les activités malveillantes et la non-conformité réglementaire, tout en réduisant la charge de travail de l'administrateur en accordant des fonctionnalités en self-service aux utilisateurs, aux responsables de l'entreprise et au personnel du service d'assistance.

Exchange Administrator (ExA) étend les fonctions puissantes de DRA afin de fournir une gestion transparente de Microsoft Exchange. Par le biais d'une interface utilisateur unique et commune, ExA 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.

Conjointement, DRA et ExA fournissent les solutions dont vous avez besoin pour contrôler et gérer vos environnements Active Directory, Microsoft Windows, Microsoft Exchange et Microsoft Office 365.

- **Prise en charge d'Active Directory, Office 365, Exchange et Skype Entreprise :** assure la gestion administrative d'Active Directory, d'Exchange Server sur site, de Skype Entreprise sur site, d'Exchange Online et de Skype Entreprise Online.
- **Contrôles granulaires de l'accès aux privilèges utilisateur et administrateur :** la technologie brevetée ActiveView délègue uniquement les privilèges nécessaires à l'exécution de responsabilités spécifiques et empêche la réaffectation des privilèges.
- **Console Web personnalisable :** une approche intuitive permet à du personnel sans formation technique de réaliser facilement et en toute sécurité des tâches administratives au moyen d'un accès limité et d'un minimum de fonctionnalités (assignées).
- **Audit approfondi des activités et création de rapports :** fournit un enregistrement d'audit complet de toutes les activités réalisées avec le produit. Stocke en toute sécurité les données à long terme et démontre aux auditeurs (par exemple, PCI DSS, FISMA, HIPAA et NERC CIP) que des processus sont en place pour contrôler l'accès à Active Directory.
- **Automatisation des processus informatiques :** automatise les workflows pour des tâches aussi diverses que le provisioning et le déprovisioning, les actions des utilisateurs et des boîtes aux lettres, l'application de stratégies et les tâches en self-service contrôlées. Renforce l'efficacité de l'entreprise et réduit les tâches administratives manuelles et répétitives.

- **Intégrité opérationnelle :** empêche les modifications malintentionnées ou incorrectes qui affectent les performances et la disponibilité des systèmes et services en fournissant un contrôle d'accès granulaire aux administrateurs et en gérant l'accès aux systèmes et aux ressources.
- **Application des processus :** préserve l'intégrité des processus de gestion des modifications clés qui vous aident à améliorer la productivité, réduire les erreurs, gagner du temps et augmenter l'efficacité de l'administration.
- **Intégration avec Change Guardian :** permet d'améliorer l'audit des événements générés dans Active Directory en dehors de DRA et de l'automatisation du workflow.

Présentation des composants de Directory and Resource Administrator (DRA)

Les composants de DRA que vous utiliserez systématiquement pour gérer les accès privilégiés incluent les serveurs primaire et secondaires, les consoles de l'administrateur, les composants de création de rapports et le moteur de workflow Aegis permettant d'automatiser les processus de workflow.

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

Type d'utilisateur de DRA	Interfaces utilisateur	Serveur d'administration
Administrateur DRA (Personne en charge de la configuration du produit)	Console de délégation et de configuration	Serveur primaire
	DRA Reporting Center Setup (NRC) CLI *(facultatif)* Fournisseur ADSI DRA*(facultatif)*	Serveur secondaire
Administrateur occasionnel du service d'assistance	Console de gestion des comptes et des ressources	Serveur secondaire
Administrateur occasionnel du service d'assistance	Console Web	Tout serveur DRA sur lequel le service REST DRA est installé

Serveur d'administration DRA

Le serveur d'administration DRA stocke les données de configuration (environnementales, accès délégué et stratégie), exécute les tâches de l'opérateur et d'automatisation et audite l'activité de l'ensemble du système. Tout en prenant en charge plusieurs clients au niveau de la console et de l'API, le serveur est conçu pour offrir une haute disponibilité pour la redondance et l'isolement géographique via un modèle d'évolutivité d'ensemble multi-maître (MMS, Multi-Master Set). Dans ce modèle, chaque environnement DRA nécessite un serveur d'administration DRA primaire qui se synchronise avec un certain nombre de serveurs d'administration DRA secondaires supplémentaires.

Nous recommandons vivement 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 spécifiques à un site, telles que les

réinitialisations de mots de passe, vous pouvez spécifier un contrôleur de domaine spécifique du site pour traiter l'opération. Il est conseillé d'envisager de consacrer un serveur d'administration secondaire à la création de rapports, au traitement par lots et aux workloads automatisés.

Console de délégation et de configuration

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

- **Delegation Management (Gestion de la délégation) :** permet de spécifier et d'assigner de façon granulaire l'accès aux ressources et tâches gérées aux assistants administrateur.
- **Policy and Automation Management (Gestion des stratégies et de l'automatisation) :** permet de définir et d'appliquer une stratégie pour garantir la conformité aux normes et conventions applicables à l'environnement.
- **Configuration Management (Gestion de la configuration) :** permet de mettre à jour les paramètres et les options système DRA, d'ajouter des personnalisations et de configurer les services gérés (Active Directory, Exchange, Office 365, etc.).

Console de gestion des comptes et des ressources

La console de gestion des comptes et des ressources est une interface utilisateur à installer permettant aux assistants administrateur de DRA d'afficher et de gérer les objets délégués des domaines et services connectés.

Console Web

La console Web est une interface utilisateur Web qui fournit un accès rapide et simple aux assistants administrateur de DRA pour afficher et gérer les objets délégués des domaines et des services connectés.

Les administrateurs peuvent personnaliser l'apparence et l'utilisation de la console Web afin d'inclure une image de marque d'entreprise personnalisée et des propriétés d'objet personnalisées. Ils peuvent également configurer l'intégration avec les serveurs Change Guardian pour permettre l'audit des modifications effectué en dehors de DRA.

L'administrateur DRA peut également créer et modifier des formulaires de workflow automatisés pour déclencher le cas échéant des tâches de routine automatisées.

L'historique des modifications unifiées est une autre fonction de la console Web qui permet l'intégration avec les serveurs d'historique des modifications afin d'auditer les modifications apportées aux objets Active Directory en dehors de DRA. Les options des rapports de l'historique des modifications incluent :

- Modifications apportées à...
- Modifications apportées par...
- Boîte aux lettres créée par...
- Utilisateur, groupe et adresse électronique du contact créés par...
- Utilisateur, groupe et adresse électronique du contact supprimés par...
- Attribut virtuel créé par...
- Objets déplacés par...

Composants de création de rapports

DRA Reporting fournit des modèles intégrés et personnalisables pour la gestion de DRA et des détails sur les domaines et les systèmes gérés par DRA :

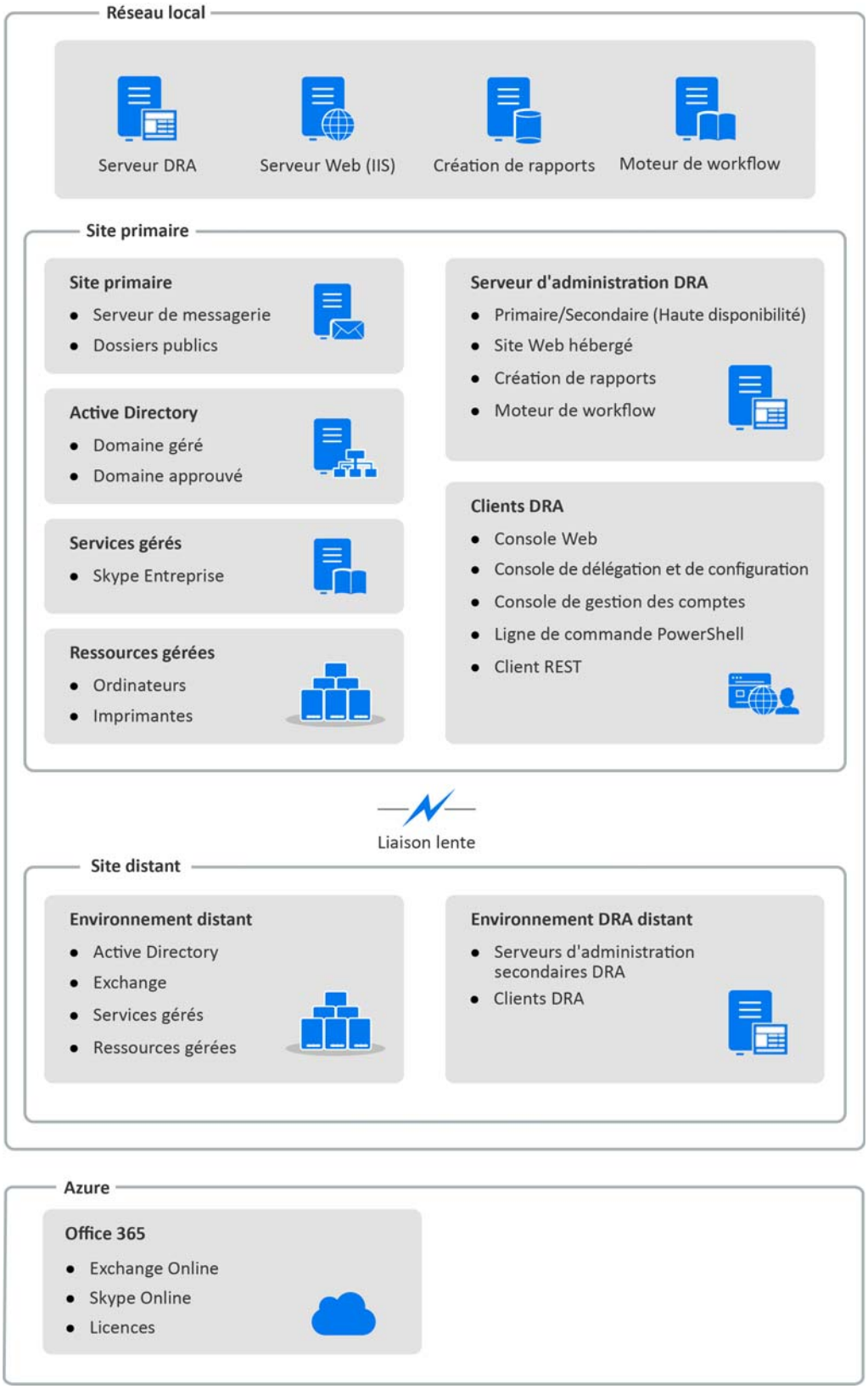
- Rapports sur les ressources pour les objets Active Directory
- Rapports sur les données d'objet Active Directory
- Rapports récapitulatifs Active Directory
- Rapports sur la configuration de DRA
- Rapports sur la configuration d'Exchange
- Rapports sur Office 365 Exchange Online
- Rapports détaillés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

Les rapports DRA peuvent être planifiés et publiés via SQL Server Reporting Services pour être facilement distribués aux participants.

Moteur de workflow

DRA s'intègre au moteur de workflow Aegis pour automatiser les tâches de workflow via la console Web dans laquelle les assistants administrateur peuvent configurer le serveur de workflow et exécuter des formulaires d'automatisation de workflow personnalisés, puis afficher l'état de ces workflows. Pour plus d'informations sur le moteur de workflow, reportez-vous au site de documentation DRA (https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

Architecture du produit



2 Installation et mise à niveau du produit

Ce chapitre décrit la configuration matérielle et logicielle requise de même que les exigences de compte pour Directory and Resource Administrator. Il vous guide ensuite tout au long de la procédure d'installation en fournissant une liste de contrôle pour chaque composant de l'installation.

Planification du 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 noter les ports et protocoles requis que vous devrez configurer pour le déploiement.

Recommandations relatives à la ressource testée

Cette section fournit des informations au sujet du dimensionnement recommandé pour notre ressource de base. Vos résultats peuvent varier en fonction du matériel disponible, de l'environnement spécifique, du type spécifique de données traitées, mais aussi d'autres facteurs. Des configurations matérielles plus puissantes et étendues pourront probablement gérer des charges plus importantes. Pour toute question, veuillez consulter les services NetIQ Consulting.

Exécution dans un environnement avec environ un million d'objets Active Directory :

Composant	UC	Mémoire	Stockage
Serveur d'administration DRA	4 UC (x64)/cœurs 2 GHz	16 Go	100 Go
Console Web DRA	2 UC (x64)/cœurs 2 GHz	8 Go	100 Go
DRA Reporting	4 UC (x64)/cœurs 2 GHz	16 Go	100 Go
Serveur de workflow DRA	4 UC (x64)/cœurs 2 GHz	16 Go	100 Go

Provisioning de ressources d'environnement virtuel

DRA conserve les segments de mémoire importants actifs pendant de longues périodes. Prenez en compte les recommandations suivantes lors du provisioning de ressources pour un environnement virtuel :

- Allouez l'espace de stockage en tant que « Thick Provisioned » (Provisioning lourd).
- Définissez la réservation de mémoire sur Reserve All Guest Memory(All Locked) [Réserver toute la mémoire invité(entièrement verrouillée)]
- Assurez-vous que le fichier de pagination est suffisamment volumineux pour permettre une éventuelle réallocation de la mémoire en ballon sur la couche virtuelle.

Ports et protocoles requis

Les ports et protocoles pour la communication DRA sont mentionnés dans cette section.

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

Serveurs d'administration DRA

Protocole et port	Sens	Destination	Utilisation
TCP 135	Bidirectionnel	Serveurs d'administration DRA	Mappeur de nœud d'extrémité, exigence de base pour la communication DRA ; permet aux serveurs d'administration de se localiser l'un l'autre dans MMS
TCP 445	Bidirectionnel	Serveurs d'administration DRA	Réplication du modèle de délégation ; réplication de fichiers lors de la synchronisation MMS (SMB)
Plage de ports TCP dynamique *	Bidirectionnel	Contrôleurs de domaine Microsoft Active Directory, clients DRA	Par défaut, DRA assigne des ports dynamiquement à partir de la plage de ports TCP comprise entre 1 024 et 65 535. Vous pouvez, toutefois, configurer cette plage à l'aide des services de composants. Pour plus d'informations, reportez-vous à l'article Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM) (Utilisation du modèle COM distribué avec des pare-feu (DCOM))
TCP 50000 *	Bidirectionnel	Serveurs d'administration DRA	Réplication d'attributs et communication ADAM avec le serveur DRA. (LDAP)
TCP 50001 *	Bidirectionnel	Serveurs d'administration DRA	Réplication d'attributs SSL (ADAM)
TCP/UDP 389	Sortant	Contrôleurs de domaine Microsoft Active Directory	Gestion des objets Active Directory (LDAP)
	Sortant	Serveur Microsoft Exchange	Gestion des boîtes aux lettres (LDAP)
TCP/UDP 53	Sortant	Contrôleurs de domaine Microsoft Active Directory	Résolution de noms
TCP/UDP 88	Sortant	Contrôleurs de domaine Microsoft Active Directory	Permet l'authentification du serveur DRA auprès des contrôleurs de domaine (Kerberos)
TCP 80	Sortant	Serveur Microsoft Exchange	Requis pour tous les serveurs Exchange locaux 2010 à 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 à Change Guardian (HTTPS)

Protocole et port	Sens	Destination	Utilisation
TCP 443, 5986, 5985	Sortant	Microsoft PowerShell	Applets de commande natives PowerShell (HTTPS) et communication à distance PowerShell
TCP 8092 * **	Sortant	Serveur de workflow	État du workflow et déclenchement (HTTPS)
TCP 50101 *	Entrant	Client DRA	Cliquez avec le bouton droit sur le rapport Historique des modifications dans le rapport d'audit de l'interface utilisateur. Peut être configuré lors de l'installation.
TCP 8989	Localhost	Service d'archivage des journaux	Communication avec l'archivage des journaux (ouverture via le pare-feu non requise)
TCP 50102	Bidirectionnel	Service core DRA	Service d'archivage des journaux
TCP 50103	Localhost	Service de cache DRA	Communication avec le service de cache sur le serveur DRA (ouverture via le pare-feu non requise)
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 unifiées

Serveur REST DRA

Protocole et port	Sens	Destination	Utilisation
TCP 8755 * **	Entrant	Serveur IIS, applets de commande PowerShell DRA	Exécution des activités de workflow basées sur REST DRA (ActivityBroker)
TCP 11192 * **	Sortant	Service hôte DRA	Pour la communication entre le service REST DRA et le service d'administration DRA
TCP 135	Sortant	Contrôleurs de domaine Microsoft Active Directory	Découverte automatique à l'aide de SCP (Service Connection Point)
TCP 443	Sortant	Contrôleurs de domaine Microsoft AD	Découverte automatique à l'aide de SCP (Service Connection Point)

Console Web (IIS)

Protocole et port	Sens	Destination	Utilisation
TCP 8755 * **	Sortant	Service REST DRA	Pour la communication entre la console Web DRA, le PowerShell DRA et le service hôte DRA
TCP 443	Entrant	Navigateur client	Ouverture d'un site Web DRA
TCP 443 **	Sortant	Serveur d'authentification avancée	Authentification avancée

Console de délégation et d'administration DRA

Protocole et port	Sens	Destination	Utilisation
TCP 135	Sortant	Contrôleurs de domaine Microsoft Active Directory	Détection automatique à l'aide de SCP
Plage de ports TCP dynamique *	Sortant	Serveurs d'administration DRA	Activités de workflow de l'adaptateur DRA. Par défaut, DCOM assigne dynamiquement des ports à partir de la plage de ports TCP 1 024 à 65 535. Vous pouvez, toutefois, configurer cette plage à l'aide des services de composants. Pour plus d'informations, reportez-vous à l'article Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM) (Utilisation du modèle COM distribué avec des pare-feu (DCOM))
TCP 50102	Sortant	Service core DRA	Génération du rapport de l'historique des modifications

Serveur de workflow

Protocole et port	Sens	Destination	Utilisation
TCP 8755	Sortant	Serveurs d'administration DRA	Exécution des activités de workflow basées sur REST DRA (ActivityBroker)

Protocole et port	Sens	Destination	Utilisation
Plage de ports TCP dynamique *	Sortant	Serveurs d'administration DRA	Activités de workflow de l'adaptateur DRA. Par défaut, DCOM assigne dynamiquement des ports à partir de la plage de ports TCP 1 024 à 65 535. Vous pouvez, toutefois, configurer cette plage à l'aide des services de composants. Pour plus d'informations, reportez-vous à l'article Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM) (Utilisation du modèle COM distribué avec des pare-feu (DCOM))
TCP 1433	Sortant	Microsoft SQL Server	Stockage des données de workflow
TCP 8091	Entrant	Console des opérations et console de configuration	API de workflow BSL (TCP)
TCP 8092 **	Entrant	Serveurs d'administration DRA	API de workflow BSL (HTTP)
TCP 2219	Localhost	Fournisseur d'espace de noms	Utilisé par le fournisseur d'espaces de noms pour exécuter des adaptateurs
TCP 9900	Localhost	Correlation Engine	Utilisé par l'instance Correlation Engine pour communiquer avec le moteur de workflow et le fournisseur d'espaces de noms
TCP 10117	Localhost	Fournisseur d'espace de noms de gestion des ressources	Utilisé par le fournisseur d'espace de noms de gestion des ressources

Plates-formes prises en charge

Pour obtenir les informations les plus récentes sur les plates-formes logicielles prises en charge, reportez-vous à la page Directory and Resource Administrator sur le site Web de NetIQ : https://www.netiq.com/support

Système géré	Conditions préalables
Active Directory	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	◆ Microsoft Exchange 2010 SP3 (à l'exception des dossiers publics) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online

Système géré	Conditions préalables
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ Module Windows Azure Active Directory pour Windows PowerShell https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell ◆ Skype Entreprise Online, module Windows PowerShell https://www.microsoft.com/en-us/download/details.aspx?id=39366
Skype Entreprise	◆ Microsoft Skype Entreprise 2015
Historique des modifications	◆ Change Guardian 5.0, 5.1
Navigateurs Web	◆ Microsoft Internet Explorer 11, Edge ◆ Google Chrome ◆ Mozilla Firefox

Configuration requise pour le serveur d'administration DRA

DRA requiert la configuration de serveur suivante pour les logiciels et les comptes :

Configuration logicielle requise :

Composant	Conditions préalables
Cible d'installation	**Système d'exploitation du serveur d'administration de NetIQ :**
Système d'exploitation	◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 2008 R2 est uniquement pris en charge à des fins de mise à niveau. **REMARQUE :** Le serveur doit également être membre d'un domaine natif Microsoft Windows Server pris en charge. **Interfaces Windows DRA :** ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 8.1 (x86 et x64), 10 (x86 et x64)
Programme d'installation	◆ Microsoft .Net Framework 4.5.2 et versions ultérieures

Composant	Conditions préalables

Serveur d'administration	**Directory and Resource Administrator :**
	◆ Microsoft .Net Framework 4.5.2 et versions ultérieures
	◆ L'un des suivants :
	  ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Packages (x64 et x86)
	  ◆ Microsoft Visual C++ 2017 (Update 3) Redistributable Packages (x64 et x86)
	◆ Microsoft Message Queuing
	◆ Rôles Microsoft Active Directory Lightweight Directory Services
	◆ Service d'accès à distance au registre démarré
	Microsoft Office 365/Exchange Online Administration :
	◆ Module Windows Azure Active Directory pour Windows PowerShell
	◆ Assistant de connexion Microsoft Online Services pour professionnels de l'informatique
	◆ Skype Entreprise Online, module Windows PowerShell
	Pour plus d'informations, reportez-vous à la section Plates-formes prises en charge.

Composants Web hérités	**Serveur Web :** ◆ Microsoft Internet Information Services (IIS) Versions 8.0, 8.5, 10 **Composants Microsoft IIS :** ◆ Microsoft Active Service Pages (ASP) ◆ Microsoft Active Service Pages .NET (ASP .Net) ◆ Service de rôle de sécurité Microsoft IIS **Interfaces Windows DRA :** ◆ Microsoft .Net Framework 4.5.2 ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Package (x86)

Configuration requise pour le compte :

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	Description	Autorisations
Compte de service DRA	Autorisations requises pour exécuter le service d'administration NetIQ	◆ Autorisations de type « Utilisateurs du modèle COM distribué » ◆ Membre du groupe d'administrateurs AD LDS ◆ Groupe d'opérateurs de compte ◆ Groupes d'archivage de journaux (OnePointOp ConfgAdms et OnePointOp) **REMARQUE :** pour plus d'informations sur la configuration de comptes d'accès aux domaines à privilège minimal, reportez-vous à la section : Comptes d'accès DRA à privilège minimal.
Administrateur DRA	Compte utilisateur ou groupe provisionné pour le rôle intégré d'administrateur DRA	◆ Groupe de sécurité locale du domaine ou compte utilisateur du domaine ◆ Membre du domaine géré ou d'un domaine approuvé ◆ Si vous indiquez un compte à partir d'un domaine approuvé, vérifiez que l'ordinateur du serveur d'administration peut s'authentifier auprès de ce compte.
Comptes d'assistant administrateur DRA	Comptes qui recevront des pouvoirs par le biais de DRA.	◆ Ajoutez tous les comptes d'assistant administrateur de DRA au groupe « Utilisateurs du modèle COM distribué » afin qu'ils puissent se connecter au serveur DRA à partir de clients distants. **REMARQUE :** DRA peut être configuré pour effectuer cette gestion à votre place pendant l'installation.

Comptes d'accès DRA à privilège minimal

Vous trouverez ci-dessous les autorisations et privilèges requis pour les comptes spécifiés et les commandes de configuration à exécuter.

Compte d'accès au domaine : Assignez les autorisations Active Directory suivantes au compte d'accès au domaine :

- Contrôle TOTAL sur les objets Utilisateur
- Contrôle TOTAL sur les objets Ordinateur
- Contrôle TOTAL sur les objets Groupe
- Contrôle TOTAL sur les objets Contact
- Contrôle TOTAL sur les objets Unité organisationnelle
- Contrôle TOTAL sur les objets Inetorgperson

- Contrôle TOTAL sur les objets Imprimante
- Contrôle TOTAL sur les objets Domaine intégré
- Contrôle TOTAL sur les objets Conteneur
- Contrôle TOTAL sur les objets MsExchSystemObjectContainer
- Contrôle TOTAL sur les groupes de distribution dynamique
- Contrôle TOTAL sur les dossiers publics

Indiquez les privilèges suivants avec une étendue de type « Cet objet et tous les objets enfants » dans le compte de service du domaine :

- Autoriser la création d'objets Ordinateur
- Autoriser la suppression d'objets Ordinateur
- Autoriser la création d'objets Contact
- Autoriser la suppression d'objets Contact
- Autoriser la création d'objets Groupe
- Autoriser la suppression d'objets Groupe
- Autoriser la suppression d'objets InetOrgPerson
- Autoriser la création d'objets Unité organisationnelle
- Autoriser la suppression d'objets Unité organisationnelle
- Autoriser la création d'objets Utilisateur
- Autoriser la suppression d'objets Utilisateur
- Autoriser la création de groupes de distribution dynamique
- Autoriser la suppression de groupes de distribution dynamique
- Autoriser la création d'un point de service de connexion
- Autoriser la suppression d'un point de service de connexion
- Autoriser la création d'un conteneur
- Autoriser la suppression d'un conteneur
- Autoriser la création de dossiers publics
- Autoriser la suppression de dossiers publics

Compte d'accès au locataire Office 365 : assignez les autorisations Active Directory suivantes au compte d'accès au locataire Office 365 :

- Administrateur de la gestion des utilisateurs dans Office 365
- Gestion des destinataires dans Exchange Online

Compte d'accès à Exchange : assignez le rôle **Gestion de l'organisation** au compte d'accès à Exchange pour gérer Exchange 2010.

Compte d'accès à Skype : assurez-vous que ce compte est employé par un utilisateur Skype et qu'il est membre d'au moins un des éléments suivants :

- Rôle CSAdministrator
- Rôles CSUserAdministrator et CSArchiving

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

- Gestion des dossiers publics
- Dossiers publics de messagerie

Opérations postérieures à l'installation de DRA :

- Exécutez la commande suivante pour déléguer l'autorisation sur le « Conteneur d'objets supprimés » à partir du dossier d'installation DRA (Remarque : la commande doit être exécutée par un administrateur de domaine) :

  `DraDelObjsUtil.exe /domain:<NomDomaineNetBIOS> /delegate:<Nom Compte>`
- Exécutez la commande suivante pour déléguer l'autorisation sur le « NetIQReceyleBin OU » à partir du dossier d'installation DRA (Remarque : cette opération ne peut être effectuée qu'après avoir ajouté les domaines respectifs à gérer par DRA) :

  `DraRecycleBinUtil.exe /domain:<NomDomaineNetBIOS> /delegate:<Nom Compte>`
- Ajoutez le compte de remplacement de privilège minimal au groupe « Administrateurs locaux » sur chaque ordinateur sur lequel DRA gère des ressources telles que des imprimantes, des services, un journal des événements, des périphériques, etc.
- Accordez au compte de remplacement de privilège minimal une « Autorisation complète » sur les dossiers de partage ou les dossiers DFS pour lesquels les répertoires privés sont provisionnés.
- Ajoutez le compte de remplacement de privilège minimal au rôle « Gestion de l'organisation » pour gérer des objets Exchange.

Configuration requise de la console Web et des extensions DRA

La configuration requise pour la console Web et les extensions REST est la suivante :

Configuration logicielle requise :

Composant	Conditions préalables
Cible d'installation	**Système d'exploitation :** ◆ Microsoft Windows Server 2016, Microsoft Windows 10, avec Microsoft IIS 10 ◆ Microsoft Windows Server 2012, 2012 R2 avec Microsoft IIS 8.0, 8.5
Service hôte DRA	◆ Microsoft .Net Framework 4.5.2 ◆ Serveur d'administration DRA
Service et nœud d'extrémité REST DRA	◆ Microsoft .Net Framework 4.5.2
Extensions PowerShell	◆ Microsoft .Net Framework 4.5.2 ◆ PowerShell 4.0

Composant	Conditions préalables
Console Web DRA	**Serveur Web :** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft Internet Information Services WCF (Activation) **Composants Microsoft IIS :** ◆ Serveur Web ◆ Fonctionnalités HTTP communes ◆ Contenu statique ◆ Document par défaut ◆ Navigateur de répertoires ◆ Erreurs HTTP ◆ Développement d'applications ◆ ASP ◆ Santé et diagnostics ◆ Consignation HTTP ◆ Moniteur de requête ◆ Sécurité ◆ Authentification de base ◆ Performances ◆ Compression de contenu statique ◆ Outils de gestion du serveur Web

Configuration requise pour la création de rapports

La configuration requise pour DRA Reporting est la suivante :

Configuration logicielle requise :

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

Composant	Conditions préalables
NetIQ Reporting Center (v3.2)	**Base de données :** ◆ Microsoft SQL Server 2012, 2014, 2016 ◆ Microsoft SQL Server Reporting Services **Serveur Web :** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Composants Microsoft IIS : ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** Tout serveur d'administration DRA qui se connecte à DRA Reporting nécessite également .NET Framework 3.5. **REMARQUE :** Lorsque vous installez NetIQ Reporting Center (NRC) sur un ordinateur SQL Server, vous devrez peut-être installer .NET Framework 3.5 manuellement avant d'installer NRC.
DRA Reporting	**Base de données :** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

Exigences de licence

Votre licence détermine les produits et les fonctions que vous pouvez utiliser. DRA exige qu'une clé de licence soit installée avec le serveur d'administration.

Après avoir installé le serveur d'administration, vous pouvez faire appel à l'utilitaire de contrôle de l'état de santé pour installer une clé de licence d'évaluation (License1.lic) qui permet de gérer un nombre illimité de comptes utilisateur et de boîtes aux lettres pendant 30 jours.

Reportez-vous au contrat de licence utilisateur final (CLUF) pour plus d'informations concernant la définition de la licence et les restrictions qui y sont associées.

Installation du produit

Ce chapitre vous guide tout au long de l'installation de Directory and Resource Administrator. Pour plus d'informations sur la planification de votre installation ou de la mise à niveau, reportez-vous à la section Planification du déploiement.

Installation du serveur d'administration DRA

Vous pouvez installer le serveur d'administration DRA en tant que nœud primaire ou secondaire dans votre environnement. La configuration requise pour les serveurs d'administration primaire et secondaires est identique, sachant toutefois que chaque déploiement DRA doit inclure un serveur d'administration primaire.

Liste de contrôle pour une installation interactive :

Étape	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour effectuer l'installation à l'aide d'un compte disposant de privilèges d'administration locaux.
Copie et exécution du kit d'installation d'administration NetIQ	Exécutez le kit d'installation DRA (NetIQAdminInstallationKit.msi) pour extraire le support d'installation DRA dans le système de fichiers local. **REMARQUE :** le kit d'installation installe .NET Framework sur le serveur cible, le cas échéant.
Exécution de l'installation de DRA	Lancez l'installation de DRA. **REMARQUE :** pour exécuter l'installation ultérieurement, accédez à l'emplacement auquel le support d'installation a été extrait et exécutez `Setup.exe`.
Sélection du composant du serveur d'administration NetIQ et de la cible d'installation	Choisissez les composants à installer et acceptez l'emplacement d'installation par défaut `C:\Program Files (x86)\NetIQ\DRA` ou spécifiez un autre emplacement d'installation. Options des composants : **Serveur d'administration NetIQ** ◆ Kit de ressources d'archivage des journaux ◆ SDK DRA NetIQ **Composant Web hérité** **Interfaces utilisateur** ◆ Gestion des comptes et des ressources ◆ Fournisseur ADSI DRA ◆ Interface de ligne de commande ◆ Délégation et configuration
Vérification des conditions préalables	La boîte de dialogue **Prerequisites** (Conditions préalables) affiche la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guide pour remplir les conditions préalables éventuelllement manquantes requises pour que l'installation se déroule correctement.
Acceptation du contrat de licence CLUF	Acceptez les termes du contrat de licence utilisateur final.
Sélection du mode de fonctionnement du serveur	Sélectionnez **Primary** (Primaire) pour installer le premier serveur d'administration DRA dans un MMS (il n'y aura qu'un seul serveur primaire par déploiement) ou **Secondary** (Secondaire) pour joindre un nouveau serveur d'administration DRA à un MMS existant. Pour plus d'informations sur un MMS, reportez-vous à la section « Configuring a Multi-Master Set » (Configuration d'un MMS) du *Directory and Resource Administrator Administrator Guide* (Guide de l'administrateur de Directory and Resource Administrator).

Étape	Détails
Indication des comptes d'installation et des informations d'identification	◆ Compte de service DRA ◆ Groupe LDS AD ◆ Administrateur DRA Pour plus d'informations, reportez-vous à la section Configuration requise pour le serveur d'administration DRA.
Configuration des autorisations DCOM	Activez DRA afin de configurer l'accès « DCOM » pour les utilisateurs authentifiés.
Configuration des ports	Pour plus d'informations sur les ports par défaut, reportez-vous à la section Ports et protocoles requis.
Indication de l'emplacement de stockage	Indiquez l'emplacement du fichier local à utiliser par DRA pour stocker les données d'audit et de cache.
Vérification de la configuration de l'installation	Vous pouvez vérifier la configuration sur la page de résumé de l'installation avant de cliquer sur **Installer** pour procéder à l'installation.
Vérification de post-installation	Une fois l'installation effectuée, le vérificateur de l'état de santé s'exécute pour vérifier l'installation et mettre à jour la licence du produit.

Installation des clients DRA

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

NetIQDRAUserConsole.mst	Installe la console de gestion des comptes et des ressources
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 spécifiques sur plusieurs ordinateurs de votre entreprise, configurez un objet Stratégie de groupe pour installer le paquetage .MST spécifique.

1. Lancez Utilisateurs et ordinateurs Active Directory et créez un objet Stratégie de groupe.
2. Ajoutez le paquetage DRAInstaller.msi à cet objet Stratégie de groupe.
3. Vérifiez que cet objet Stratégie de groupe comporte une des propriétés suivantes :
   - Chaque compte utilisateur du groupe dispose d'autorisations Utilisateur avec pouvoir pour l'ordinateur approprié.
   - Activez le paramètre de stratégie Toujours installer avec des droits élevés.
4. Ajoutez le fichier .mst de l'interface utilisateur, tel que NetIQDRAUserConsole.mst, à cet objet Stratégie de groupe.
5. Distribuez votre stratégie de groupe.

REMARQUE : pour plus d'informations sur la stratégie de groupe, reportez-vous à l'aide de Microsoft Windows. Pour tester et déployer facilement et en toute sécurité les stratégies de groupe dans votre entreprise, utilisez l'*administrateur de stratégie de groupe*.

Installation des extensions REST DRA

Le paquetage d'extensions REST DRA comporte quatre fonctions :

- **Service hôte DRA NetIQ :** passerelle utilisée pour communiquer avec le service d'administration DRA. Ce service doit s'exécuter sur un ordinateur sur lequel le service d'administration DRA est installé.
- **Service et nœuds d'extrémité REST DRA :** fournit les interfaces RESTful qui permettent à la console Web DRA et aux clients non-DRA de demander des opérations DRA. Ce service doit s'exécuter sur un ordinateur sur lequel une console DRA ou le service d'administration DRA est installé.
- **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 DRA :** interface du client Web principalement utilisée par les assistants administrateur, mais qui inclut également des options de personnalisation.

Étape	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour effectuer l'installation à l'aide d'un compte disposant de privilèges d'administration locaux.
Installation du certificat SSL	S'il n'est pas déjà installé sur le serveur Windows, un certificat SSL doit être installé avant d'exécuter l'installation.
Copie et exécution du kit d'installation d'administration NetIQ	Copiez le kit d'installation DRA `NetIQAdminINstallationKit.msi` sur le serveur cible et exécutez-le en double-cliquant sur le fichier ou en l'appelant à partir de la ligne de commande. Le kit d'installation extrait le support d'installation DRA dans le système de fichiers local vers un emplacement personnalisable.
Exécution du programme d'installation des extensions REST DRA	Une fois que le kit d'installation DRA a terminé l'extraction du support d'installation, il vous invite à lancer l'installation de DRA. Accédez à l'emplacement auquel le support d'installation a été extrait, cliquez avec le bouton droit sur le fichier `DRARESTExtensionsInstaller.exe`, puis sélectionnez **Exécuter en tant qu'administrateur**.
Acceptation du contrat de licence CLUF	Acceptez les termes du contrat de licence utilisateur final.
Sélection de composants et Indication de l'emplacement cible de l'installation	Dans la boîte de dialogue **Select Components** (Sélectionner les composants), installez toutes les options : DRA Host Service (service hôte DRA), DRA REST Endpoints and service (nœuds d'extrémité et service REST DRA), PowerShell Extensions (extensions PowerShell) et DRA Web Console (console Web DRA). Acceptez l'emplacement d'installation par défaut `C:\Program Files (x86)\NetIQ\DRA Extensions` ou indiquez un autre emplacement pour l'installation.
Vérification des conditions préalables	La boîte de dialogue **Prerequisites** (Conditions préalables) affiche la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guide pour remplir les conditions préalables éventuellement manquantes requises pour que l'installation se déroule correctement.

Étape	Détails
Spécification du compte de service à exécuter en tant que	Par défaut, le compte de service existant du serveur DRA est affiché. Indiquez le mot de passe du compte de service. Pour plus d'informations sur la configuration d'un compte de service pour le serveur d'administration DRA, reportez-vous à la section Configuration requise pour le serveur d'administration DRA.
Spécification du certificat SSL du service REST	Sélectionnez le certificat SSL que vous utiliserez pour le service REST et indiquez les ports de service REST et Hôte.
Spécification du certificat SSL de la console Web	Indiquez le certificat SSL que vous utiliserez pour la connexion HTTPS.
Vérification de la configuration de l'installation	Vous pouvez vérifier la configuration sur la page de résumé de l'installation avant de cliquer sur **Installer** pour procéder à l'installation.

Installation du serveur de workflow

Pour plus d'informations sur l'installation du serveur de workflow, reportez-vous au Guide de l'administrateur d'Aegis.

Installation de DRA Reporting

DRA Reporting vous demande d'installer deux fichiers exécutables à partir du kit d'installation NetIQ DRA : `NRCSetup.exe` et `DRAReportingSetup.exe`.

Étapes	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour effectuer l'installation à l'aide d'un compte disposant de privilèges d'administration locaux. Veillez à que ce compte possède des privilèges d'administrateur local et de domaine, mais aussi des privilèges d'administrateur système sur le serveur SQL.
Copie et exécution du kit d'installation d'administration NetIQ	Copiez le kit d'installation DRA `NetIQAdminINstallationKit.msi` sur le serveur cible et exécutez-le en double-cliquant sur le fichier ou en l'appelant à partir de la ligne de commande. Le kit d'installation extrait le support d'installation DRA dans le système de fichiers local vers un emplacement personnalisable. De plus, le kit d'installation installe .NET Framework sur le serveur cible si nécessaire pour remplir la condition préalable du programme d'installation du produit DRA.
Exécution du fichier d'installation de NetIQ Reporting Center (NRC)	Une fois que le kit d'installation DRA a terminé l'extraction du support d'installation, accédez à l'emplacement auquel le support d'installation a été extrait et exécutez le fichier `NRCSetup.exe`.
Sélection du composant NetIQ Reporting Center	Dans la boîte de dialogue **Select Components** (Sélectionner les composants), utilisez le composant par défaut « NetIQ Reporting Center » pour installer les quatre composants NRC.
Indication de l'emplacement cible de l'installation	Acceptez l'emplacement d'installation par défaut `C:\Program Files (x86)\NetIQ\Reporting Center` ou indiquez un autre emplacement d'installation.

Étapes	Détails
Vérification des conditions préalables et installation	La boîte de dialogue **Prerequisites** (Conditions préalables) affiche la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guide pour remplir les conditions préalables éventuellement manquantes requises pour que l'installation se déroule correctement. **IMPORTANT :** .NET Framework 3.5 doit être installé manuellement sur le serveur de création de rapports avant l'installation de NRC.
Acceptation du contrat de licence CLUF	Acceptez les termes du contrat de licence utilisateur final.
Installation de la base de données de configuration	Utilisez les valeurs par défaut de la boîte de dialogue **Configuration Database Installation - SQL Server Logon** (Installation de la base de données de configuration - Connexion à SQL Server) ou fournissez l'authentification SQL pour terminer l'installation de NRC. Si vous avez utilisé l'instance par défaut pour l'installation de SQL Server, le champ Instance doit rester vide.
Exécution de l'installation de DRA Reporting	Accédez à l'emplacement auquel le support d'installation a été extrait et exécutez le fichier `DRAReportingSetup.exe` pour installer le composant de gestion permettant l'intégration de DRA Reporting.
Acceptation du contrat de licence CLUF	Acceptez les termes du contrat de licence utilisateur final pour terminer l'exécution de l'installation.

Mise à jour de produit

Ce chapitre présente une procédure qui vous aide à mettre à niveau ou à migrer un environnement distribué par phases contrôlées.

Ce chapitre suppose que votre environnement contienne plusieurs serveurs d'administration, certains serveurs étant situés sur des sites distants. Cette configuration est appelée ensemble multi-maître (MMS, Multi-Master Set). Un MMS comprend un serveur d'administration primaire et un ou plusieurs serveurs d'administration secondaires associés. Pour plus d'informations sur le fonctionnement d'un MMS, reportez-vous à la section « Configuring a Multi-Master Set » (Configuration d'un MMS) du *Directory and Resource Administrator Administrator Guide* (Guide de l'administrateur de Directory and Resource Administrator).

Planification d'une mise à niveau DRA

Exécutez le kit `NetIQAdminInstallationKit.msi` pour extraire le support d'installation de DRA, puis installez et exécutez l'utilitaire de contrôle de l'état de santé.

Assurez-vous de planifier votre déploiement de DRA avant d'entamer la procédure de mise à niveau. Lorsque vous planifiez votre déploiement, tenez compte des instructions suivantes :

- Testez la procédure de mise à niveau dans votre environnement de test avant de déployer la mise à niveau dans votre environnement de production. Les tests vous permettent d'identifier et de résoudre les problèmes inattendus sans entraver les tâches quotidiennes des responsables administratifs.
- Reportez-vous à Ports et protocoles requis.
- Déterminez le nombre d'assistants administrateur qui s'appuient sur chaque MMS. Si la plupart de vos assistants administrateur s'appuient sur des serveurs ou des ensembles de serveurs spécifiques, commencez par mettre à niveau ces serveurs durant les heures creuses.

- Déterminez les assistants administrateur qui ont besoin de la console de délégation et de configuration. Vous pouvez obtenir cette information de l'une des façons suivantes :
  - Passez en revue les assistants administrateur associés aux groupes d'assistants administrateur intégrés.
  - Passez en revue les assistants administrateur associés à la technologie ActiveViews intégréee.
  - Utilisez DRA Reporting pour générer des rapports sur le modèle de sécurité, tels que les rapports ActiveView Assistant Admin Details (Détails des assistants administrateur ActiveView) et Groupes d'assistants administrateur.

  Informez ces assistants administrateur de vos plans de mise à niveau des interfaces utilisateur.
- Déterminez les assistants administrateur qui doivent se connecter au serveur d'administration primaire. Ces assistants administrateur doivent mettre à niveau leurs ordinateurs clients une fois que vous avez mis à niveau le serveur d'administration primaire.

  Informez ces assistants administrateur de vos plans 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 la procédure de mise à niveau. Selon votre environnement, cette décision peut être prise au cas par cas.
- Coordonnez la mise à niveau de vos ordinateurs clients et de vos serveurs d'administration pour assurer un temps hors service minimal. Sachez que DRA ne prend pas en charge l'exécution des versions antérieures de DRA avec la version actuelle de DRA sur le même serveur d'administration ou ordinateur client.

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 à la mise à niveau.

Étapes	Détails
Sauvegarde de l'instance AD LDS	Ouvrez l'utilitaire de contrôle de l'état de santé et procédez à la vérification de la **sauvegarde de l'instance AD LDS** pour créer une sauvegarde de votre instance AD LDS actuelle.
Création d'un plan de déploiement	Créez un plan de déploiement pour la mise à niveau des serveurs d'administration et des interfaces utilisateur (ordinateurs clients des assistants administrateur). Pour plus d'informations, reportez-vous à la section Planification d'une mise à niveau DRA.
Allocation d'un serveur secondaire pour l'exécution d'une version antérieure de DRA	*Facultatif :* allouez un serveur d'administration secondaire à l'exécution d'une version antérieure de DRA lors de la mise à niveau d'un site.
Introduction des modifications nécessaires 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.
Synchronisation des MMS	Synchronisez les ensembles de serveurs afin que chaque serveur d'administration contienne les derniers paramètres de configuration et de sécurité.
Sauvegarde du registre du serveur primaire	Sauvegardez le registre à partir du serveur d'administration primaire. La sauvegarde de vos anciens paramètres de registre permet de récupérer facilement votre configuration précédente et ses paramètres de sécurité.

REMARQUE : Si vous une bonne raison de 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. L'intitulé sera différent : `NetIQDRASecureStoragexxxxx`.
2. Remplacez le fichier **adamnts.dit** `actuel` par le fichier **adamnts.dit** `de sauvegarde` comme indiqué ci-dessous :
   - Emplacement du fichier actuel : `%ProgramData%/NetIQ/DRA/<NomInstanceDRA>/data/`
   - Emplacement du fichier de sauvegarde : `%ProgramData%/NetIQ/ADLDS/`
3. Redémarrez l'instance AD LDS.

Allocation d'un serveur d'administration local pour l'exécution d'une version antérieure de DRA

L'allocation d'un ou plusieurs serveurs d'administration secondaires pour exécuter localement une version antérieure de DRA sur un site pendant la mise à niveau peut aider à réduire le temps hors service et les connexions coûteuses vers des sites distants. Cette étape est facultative et permet aux assistants administrateur d'utiliser une version antérieure de DRA tout au long de la procédure de mise à niveau, jusqu'à ce que vous soyez certain que votre déploiement est terminé.

Envisagez cette option si vous êtes concerné par une ou plusieurs des exigences de mise à niveau suivantes :

- Vous souhaitez un minimum de temps hors service, voire aucun.
- Vous devez prendre en charge un grand nombre d'assistants administrateur sans pouvoir mettre immédiatement à niveau tous les ordinateurs clients.
- Vous voulez continuer à prendre en charge l'accès à une version antérieure de DRA après la mise à niveau du serveur d'administration primaire.
- Votre environnement inclut 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 antérieure de DRA. Si vous avez l'intention de mettre à niveau ce serveur, il doit être le dernier serveur que vous mettez à niveau. Dans le cas contraire, désinstallez complètement DRA de ce serveur lorsque vous avez terminé 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 les connexions coûteuses à des sites distants et garantit que vos assistants administrateur peuvent continuer à utiliser une version antérieure de DRA sans interruption. Si votre environnement comporte un MMS qui s'étend sur plusieurs sites, vous devriez envisager cette option. Par exemple, si votre MMS se compose d'un serveur d'administration primaire sur votre site de Paris et d'un serveur d'administration secondaire sur votre site de Tokyo, envisagez d'installer un serveur secondaire sur le site de Paris et de l'ajouter au MMS correspondant. Ce serveur supplémentaire permet aux assistants administrateur du site de Paris d'utiliser une version antérieure de DRA jusqu'à ce que la mise à niveau soit terminée.

Utilisation d'un serveur secondaire existant

Vous pouvez utiliser un serveur d'administration secondaire existant en tant que serveur dédié pour une version antérieure de DRA. 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 pour ce faire. L'allocation d'un ou plusieurs serveurs secondaires pour l'exécution d'une version antérieure de DRA permet à vos assistants administrateur de continuer à utiliser une version antérieure de DRA sans interruption jusqu'à la fin de la mise à niveau. Le recours à cette option est idéal dans les environnements étendus qui utilisent un modèle d'administration centralisée.

Synchronisation de votre ensemble de serveurs utilisant une version antérieure de DRA

Avant de sauvegarder le registre de la version antérieure de DRA ou d'entamer la procédure de mise à niveau, assurez-vous de synchroniser les ensembles de serveurs afin que chaque serveur d'administration contienne les derniers paramètres de configuration et de sécurité.

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

Pour synchroniser votre ensemble de serveurs existant :

1. Connectez-vous au serveur d'administration primaire en tant qu'administrateur intégré.
2. Démarrez l'interface MMC.
3. Dans le panneau de gauche, développez **Gestion de la configuration**.
4. Cliquez sur **Serveurs d'administration**.
5. Dans le volet de droite, sélectionnez le serveur d'administration primaire approprié pour cet ensemble de serveurs.
6. Cliquez sur **Propriétés**.
7. Sous l'onglet Planification de la synchronisation, cliquez sur **Rafraîchir maintenant**.
8. Vérifiez la réussite de la synchronisation et la disponibilité de tous les serveurs d'administration secondaires.

Sauvegarde du registre du serveur d'administration

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

Cependant, soyez prudent lorsque vous modifiez votre registre. En cas d'erreur dans votre registre, le serveur d'administration peut ne pas fonctionner comme prévu. Si une erreur se produit pendant la procédure de mise à niveau, vous pouvez utiliser la sauvegarde de vos paramètres de registre pour le restaurer. Pour plus d'informations, reportez-vous à l'*aide de l'Éditeur du Registre*.

IMPORTANT : la version du serveur DRA, le nom du système d'exploitation Windows de même que la configuration du domaine géré doivent être parfaitement identiques lors de la restauration du registre.

IMPORTANT : avant la mise à niveau, sauvegardez le système d'exploitation Windows de la machine qui héberge 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 sur le nœud `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint`, et sélectionnez **Exporter**.
3. Indiquez 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 de la procédure de mise à niveau. Réeffectuez cette procédure pour mettre à niveau chaque ensemble de serveurs de votre environnement. Si vous ne l'avez pas encore fait, employez l'utilitaire de contrôle de l'état de santé pour créer une sauvegarde de votre instance AD LDS actuelle.

Vous pouvez répartir cette procédure de mise à niveau en plusieurs phases, en mettant à jour un MMS à la fois. Cette procédure de mise à niveau vous permet également d'inclure temporairement des serveurs secondaires exécutant une version antérieure 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 antérieure de DRA et les serveurs exécutant la version actuelle de DRA. Cependant, sachez que DRA ne prend pas en charge l'exécution d'une version antérieure de DRA avec la version actuelle sur le même serveur d'administration ou ordinateur client.

Dans DRA 9.2 ou version ultérieure, la configuration du serveur d'automatisation du workflow est stockée dans AD LDS au lieu du registre. Lors de la mise à jour de DRA 9.1 ou version antérieure vers DRA 9.2 ou version ultérieure, la configuration du registre est automatiquement déplacée vers AD LDS et répliquée sur l'ensemble des serveurs secondaires.

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 de ce MMS.

Étapes	Détails
Exécution de l'utilitaire de contrôle de l'état de santé	Installez l'utilitaire de contrôle de l'état de santé DRA en mode autonome et exécutez-le à l'aide d'un compte de service. Résolvez tous les problèmes.
Exécution d'une mise à niveau test	Effectuez une mise à niveau test dans votre environnement de test afin d'identifier les problèmes potentiels et de minimiser les temps hors service en production.
Ordre de la 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 plus d'informations, reportez-vous aux 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.
Installation d'un nouveau serveur secondaire	*(Facultatif)* Pour réduire les temps hors service sur les sites distants, installez un serveur d'administration secondaire local exécutant la version de DRA la plus récente.
Déploiement des interfaces utilisateur	Déployez les interfaces utilisateur auprès de vos assistants administrateur.
Mise à niveau des serveurs secondaires	Mettez à niveau les serveurs d'administration secondaires du MMS.
Mise à niveau de DRA Reporting	Mettez à niveau DRA Reporting.
Mise à niveau des extensions REST	Exécutez le programme d'installation des extensions REST DRA.

Étapes	Détails
Exécution de l'utilitaire de contrôle de l'état de santé	Exécutez l'utilitaire de contrôle de l'état de santé qui a été installé dans le cadre de la mise à niveau. Résolvez tous les problèmes.

Mise à niveau du serveur d'administration primaire

Après avoir préparé votre MMS, mettez à niveau le serveur d'administration primaire. Ne mettez pas à niveau les interfaces utilisateur sur les ordinateurs clients des assistants administrateur tant que vous n'avez pas terminé la mise à niveau du serveur d'administration primaire. Pour plus d'informations, reportez-vous à la section Déploiement des interfaces utilisateur DRA.

REMARQUE : pour des considérations plus détaillées sur les mises à niveau, reportez-vous aux *Directory and Resource Administrator Release Notes* (Notes de version de Directory and Resource Administrator).

Avant de procéder à la mise à niveau, informez vos assistants administrateur de la date et heure auxquelles vous prévoyez de démarrer cette procédure. Si vous avez alloué un serveur d'administration secondaire pour l'exécution d'une version antérieure de DRA, spécifiez également ce serveur afin que les assistants administrateur puissent continuer à utiliser la version précédente de DRA pendant la mise à niveau.

REMARQUE : une fois que vous avez mis à niveau le serveur d'administration primaire, vous ne pouvez pas synchroniser les paramètres de délégation, de configuration ou de stratégie de ce serveur avec les serveurs d'administration secondaires exécutant une version antérieure 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 hors service globaux et en permettant un déploiement plus rapide des interfaces utilisateur. Cette étape est facultative et permet aux assistants administrateur d'utiliser à la fois la version actuelle de DRA et une version antérieure de DRA tout au long de la procédure de mise à niveau, jusqu'à ce que vous soyez certain que votre déploiement est terminé.

Envisagez cette option si vous êtes concerné par une ou plusieurs des exigences de mise à niveau suivantes :

- Vous souhaitez un minimum de temps hors service, voire aucun.
- Vous devez prendre en charge un grand nombre d'assistants administrateur sans pouvoir mettre immédiatement à niveau tous les ordinateurs clients.
- Vous voulez continuer à prendre en charge l'accès à une version antérieure de DRA après la mise à niveau du serveur d'administration primaire.
- Votre environnement inclut 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 Paris 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 assistants administrateur de l'un ou l'autre site d'utiliser une version antérieure de DRA ainsi que la version actuelle de DRA jusqu'à la fin de la mise à niveau. En outre, vos assistants administrateur ne

subissent aucun temps hors service puisque vous pouvez déployer immédiatement les interfaces utilisateur DRA actuelles. Pour plus d'informations sur la mise à niveau des interfaces utilisateur, reportez-vous à la section Déploiement des interfaces utilisateur DRA.

Déploiement des interfaces utilisateur DRA

En général, vous devez déployer les interfaces utilisateur DRA actuelles après la mise à niveau du serveur d'administration primaire et d'un serveur d'administration secondaire. Toutefois, pour les assistants administrateur qui doivent utiliser le serveur d'administration primaire, assurez-vous d'abord de mettre à niveau leurs ordinateurs clients en installant la console de délégation et de configuration. Pour plus d'informations, reportez-vous à la section Planification d'une mise à niveau DRA.

Si vous effectuez souvent un traitement par lots via l'interface de ligne de commande ou le fournisseur ADSI ou si vous générez fréquemment des rapports, envisagez d'installer ces interfaces utilisateur sur un serveur d'administration secondaire dédié pour conserver un équilibre de charge approprié sur le MMS.

Vous pouvez autoriser vos assistants administrateur à installer les interfaces utilisateur DRA ou déployer ces interfaces au moyen d'une stratégie de groupe. Vous pouvez également déployer facilement et rapidement la console Web pour plusieurs assistants administrateur.

REMARQUE : vous ne pouvez toutefois pas exécuter plusieurs versions des composants DRA côte à côte sur le même serveur DRA. Si vous prévoyez de mettre à niveau progressivement les ordinateurs clients des assistants administrateur, 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 secondaires

Lors de la mise à niveau des serveurs d'administration secondaires, vous pouvez mettre à niveau chaque serveur en fonction de vos besoins d'administration. Étudiez également la planification de la mise à niveau et le déploiement de l'interface utilisateur DRA. Pour plus d'informations, reportez-vous à la section Déploiement des interfaces utilisateur DRA.

Par exemple, un plan de mise à niveau standard peut comprendre les étapes suivantes :

1. Mettez à niveau un serveur d'administration secondaire.
2. Demandez aux assistants administrateur qui utilisent ce serveur d'installer les interfaces utilisateur appropriées, telles que la console de gestion des comptes et des ressources.
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 assistants administrateur de la date et heure auxquelles vous prévoyez de démarrer cette procédure. Si vous avez alloué un serveur d'administration secondaire pour l'exécution d'une version antérieure de DRA, spécifiez également ce serveur afin que les assistants administrateur puissent continuer à utiliser la version précédente de DRA pendant la mise à niveau. Lorsque vous avez terminé la procédure de mise à niveau pour ce MMS et que tous les ordinateurs clients des assistants administrateur exécutent des interfaces utilisateur mises à niveau, placez hors ligne tous les serveurs restants qui utilisent une version antérieure de DRA.

Mise à niveau des composants DRA Reporting

Avant de mettre à niveau DRA Reporting, assurez-vous que votre environnement répond à la configuration minimale requise pour NRC 3.2. Pour plus d'informations sur la configuration requise pour l'installation et les considérations de mises à niveau, reportez-vous au *Reporting Center Guide* (Guide de Reporting Center) sur le site de documentation DRA.

Étapes	Détails
Désactivation de la prise en charge de DRA Reporting	Pour vous assurer que les collecteurs de création de rapports ne s'exécutent pas pendant la procédure de mise à niveau, désactivez la prise en charge de DRA Reporting dans la fenêtre Reporting Service Configuration (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 SQL Server.
Lancement du programme d'installation de DRA Reporting	Exécutez le fichier exécutable `DRAReportingSetup.exe`. à partir du kit d'installation et suivez les instructions de l'Assistant d'installation.
Exécution du programme d'installation de NRC	*Conditionnel :* si votre service Web NRC est installé sur un autre ordinateur, connectez-vous à l'ordinateur sur lequel le service Web est installé et exécutez `NRCSetup.exe` pour mettre à niveau le service Web NRC. **REMARQUE :** si la base de données de configuration a été installée sur un serveur distinct, elle devra d'abord être mise à niveau.
Exécution du programme d'installation de NRC sur les ordinateurs clients	Exécutez `NRCSetup.exe` sur tous les ordinateurs clients NRC.
Activation de la prise en charge de DRA Reporting	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 devez redéployer vos rapports. Pour plus d'informations sur le redéploiement des rapports, reportez-vous au *NetIQ Reporting Center Reporting Guide* (Guide de création de rapports NetIQ Reporting Center) sur le site de documentation DRA.

Mise à niveau des extensions REST DRA

Pour mettre à niveau la console Web et les extensions REST vers Directory and Resource Administrator 9.2, vous devez utiliser DRA 9.0.1 ou une version ultérieure. Pour plus d'informations sur la configuration requise, reportez-vous à la section Configuration requise de la console Web et des extensions DRA.

Pour mettre à niveau la console Web et les extensions DRA :

1. Après avoir téléchargé le kit d'installation DRA, accédez à l'emplacement auquel le support d'installation a été extrait, cliquez avec le bouton droit sur le fichier `DRARESTExtensionsInstaller.exe`, puis sélectionnez **Exécuter en tant qu'administrateur**.
2. Suivez les instructions de l'Assistant d'installation jusqu'à ce que l'installation soit terminée, puis cliquez sur **Terminer**.

Pour plus d'informations sur les étapes de l'assistant d'installation, reportez-vous aux étapes d'une nouvelle installation : Installation des extensions REST DRA.

Mise à jour du contenu personnalisé

Lorsque vous effectuez une mise à niveau vers une version plus récente de DRA, vous souhaitez conserver toutes les personnalisations que vous avez effectuées pour la console Web sur le serveur Web. Pour vous faciliter la tâche, DRA dispose d'un utilitaire de mise à niveau des personnalisations intégré au programme d'installation des extensions REST DRA. Cet utilitaire s'exécute automatiquement lorsque vous exécutez le fichier exécutable `DRARESTExtensionsInstaller.exe` pour mettre à niveau des extensions REST sur le serveur Web. Vous pouvez également réexécuter manuellement l'utilitaire à partir du répertoire d'installation de DRA après l'installation.

Une partie de la procédure de l'utilitaire de mise à niveau des personnalisations consiste à sauvegarder vos personnalisations avant le démarrage de la mise à niveau. Au cours de la procédure de mise à niveau, l'utilitaire crée un fichier journal de toutes les modifications apportées en raison de la mise à niveau et inclut également un avertissement relatif aux éléments de personnalisation qui ne peuvent pas être mis à jour automatiquement.

Nous recommandons de consulter le journal après la mise à niveau. Si nécessaire, vous pouvez restaurer l'état initial des personnalisations antérieures de la mise à niveau en les copiant à partir du dossier de sauvegarde. Vous pouvez définir le chemin du dossier pour les personnalisations mises à niveau lorsque l'utilitaire de mise à niveau des personnalisations s'ouvre ou vous pouvez utiliser le chemin par défaut, qui est renseigné automatiquement.

Les chemins par défaut pour les personnalisations mises à niveau et la sauvegarde des personnalisations sont fournis ci-dessous :

- Chemin par défaut du dossier personnalisé : `C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom`
- Dossier de sauvegarde par défaut : `$CustomFolderPath\custom_upgrade_$VERSIONFROM_to_$VERSIONTO_backup`

3 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.

Liste de contrôle de la configuration

Utilisez la liste de contrôle suivante pour vous aider à configurer DRA dans le cadre d'une première utilisation.

Étapes	Détails
Application d'une licence DRA	Employez l'utilitaire de contrôle de l'état de santé pour appliquer une licence DRA. Pour plus d'informations sur les licences DRA, reportez-vous à la section Exigences de licence.
Ouverture de la délégation et de la 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 l'issue du rafraîchissement complet du compte.
Ajout de domaines et des sous-arborescences gérés	*Facultatif :* ajoutez des domaines et des sous-arborescences gérés supplémentaires à DRA. Pour plus d'informations sur les domaines gérés, reportez-vous à la section Ajout de domaines gérés.
Configuration des paramètres DCOM	*Facultatif :* configurez les paramètres DCOM. Pour plus d'informations sur les paramètres DCOM, consultez la section Configuration des paramètres DCOM.

Installation ou mise à niveau de licences

DRA nécessite 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, employez l'utilitaire de contrôle de l'état de santé pour installer le fichier de clé de licence d'évaluation (`TrialLicense.lic`) fourni par NetIQ Corporation.

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

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 un ordinateur sur lequel la console de délégation et de configuration est installée, à l'aide du compte de service DRA. Vous devez également disposer des droits d'administrateur au sein du

domaine, tels que les droits accordés au groupe d'administrateurs de domaine. Pour ajouter des domaines gérés et des ordinateurs après l'installation du premier domaine géré, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré de configuration des serveurs et des domaines.

REMARQUE : après avoir ajouté les domaines gérés, vérifiez que les planifications de rafraîchissement du cache des comptes pour ces domaines sont correctes. Pour plus d'informations sur la modification de la planification de rafraîchissement du cache des comptes, reportez-vous à la section « Configuring Caching » (Configuration du caching) du *Directory and Resource Administrator Administrator Guide* (Guide de l'administrateur de Directory and Resource Administrator).

Ajout de sous-arborescences gérées

Vous pouvez ajouter des sous-arborescences gérées à partir de domaines Microsoft Windows spécifiques après l'installation du serveur d'administration. Vous pouvez ajouter les sous-arborescences manquantes que vous souhaitez gérer via le nœud de configuration avancée de la console de délégation et de configuration. Pour ajouter des sous-arborescences gérées après l'installation du serveur d'administration, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré de configuration des serveurs et domaines. Pour vous assurer que le compte d'accès spécifié dispose des autorisations nécessaires pour gérer cette sous-arborescence et effectuer des rafraîchissements incrémentiels du cache des comptes, employez l'utilitaire Deleted Objects (Objets supprimés) pour vérifier et déléguer les autorisations appropriées.

Pour plus d'informations sur l'emploi de cet utilitaire, reportez-vous à la section « Deleted Objects Utility » (Utilitaire Objets supprimés) du *Directory and Resource Administrator Administrator Guide* (Guide de l'administrateur de Directory and Resource Administrator).

Pour plus d'informations sur la configuration du compte d'accès, reportez-vous à la section « Specifying Domain Access Accounts » (Spécification des comptes d'accès au domaine) du *Directory and Resource Administrator Administrator Guide* (Guide de l'administrateur de Directory and Resource Administrator).

REMARQUE : après avoir ajouté les sous-arborescences gérées, assurez-vous que les planifications de rafraîchissement du cache des comptes pour les domaines correspondants sont correctes. Pour plus d'informations sur la modification de la planification de rafraîchissement du cache des comptes, reportez-vous à la section « Configure Caching » (Configuration du caching) du *Directory and Resource Administrator Administrator Guide* (Guide de l'administrateur de Directory and Resource Administrator).

Configuration des paramètres DCOM

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

Configuration du groupe Utilisateurs du modèle COM distribué

Si vous avez choisi de ne pas configurer DCOM pendant la procédure d'installation de DRA, vous devez mettre à jour l'adhésion au groupe Utilisateurs du modèle COM distribué afin d'inclure tous les comptes utilisateur qui utilisent DRA. Cette adhésion doit inclure le compte de service DRA et tous les assistants administrateur.

Pour configurer le groupe Utilisateurs du modèle COM distribué :

1. Connectez-vous à l'ordinateur client DRA en tant qu'administrateur DRA.
2. Démarrez la console de configuration et de délégation. 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 d'assistant administrateur. Dans ce cas, configurez le groupe Utilisateurs du modèle COM distribué à l'aide du snap-in Utilisateurs et ordinateurs Active Directory. Pour plus d'informations sur le snap-in Utilisateurs et ordinateurs Active Directory, consultez le site Web de Microsoft.

   ---
3. Dans le volet de gauche, développez **Account and Resource Management** (Gestion des comptes et des ressources).
4. Développez **Tous mes objets gérés**.
5. Développez le nœud de domaine pour chaque domaine dans lequel 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 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**.

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, accédez à **Paramètres > Système et sécurité > Panneau de configuration**.
2. Ouvrez Outils d'administration, puis Services de composants.
3. Développez **Services de composants > Ordinateurs > Poste de travail > Configuration DCOM**.
4. Sélectionnez **Service d'administration MCS OnePoint** sur le serveur d'administration.
5. Dans le menu Action, cliquez sur **Propriétés**.
6. Sous l'onglet Général de la zone Niveau d'authentification, sélectionnez **Paquet**.

7. Sous 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 ne l'est pas, ajoutez-le. Si le groupe Tout le monde est disponible, supprimez-le.
9. Vérifiez que le groupe Utilisateurs du modèle COM distribué dispose des autorisations Local et Accès à distance.
10. Sous l'onglet Sécurité de la zone Autorisations d'exécution et d'activation, sélectionnez **Personnaliser**, puis cliquez sur **Modifier**.
11. Assurez-vous que le groupe Utilisateurs du modèle COM distribué est disponible. S'il ne l'est pas, ajoutez-le. Si le groupe Tout le monde est disponible, supprimez-le.
12. Vérifiez que le groupe Utilisateurs du modèle COM distribué dispose des autorisations suivantes :
    - Exécution locale
    - Exécution à distance
    - Activation locale
    - Activation à distance
13. Appliquez les modifications.