Directory and Resource Administrator

Guide d'installation

Juillet 2018

Avis juridique

À propos de ce guide

Le *Guide d'installation* fournit des renseignements sur la planification, l'installation, la licence et la configuration de 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 Directory and Resource Administrator. Pour obtenir la liste complète des publications à l'appui de cette version, visitez la page Web Documentation (https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

Communiquer avec le soutien aux ventes

Pour des questions sur les produits, les prix et les fonctionnalités, communiquez avec votre partenaire local. Si vous ne parvenez pas à joindre votre partenaire local, communiquez avec notre équipe de soutien aux ventes.

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

Communiquer avec le service d'assistance technique

Pour des problèmes concernant des produits en particulier, communiquez avec notre équipe d'assistance 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
Courriel :	support@netiq.com
Site Web :	www.netiq.com/support

Communiquer avec le service de soutien à la documentation

Notre objectif est de fournir une documentation qui répond à vos besoins. Si vous avez des suggestions d'amélioration à apporter à la documentation, cliquez sur **Envoyer un commentaire sur ce sujet** au bas de n'importe quelle page de la version HTML de la documentation. Vous pouvez également envoyer un courriel à Documentation-Feedback@netiq.com. Nous apprécions votre contribution et avons hâte de vous lire.

Communiquer avec la communauté d'utilisateurs en ligne

NetIQ Communities, la communauté en ligne de NetIQ est un réseau collaboratif qui vous met en relation avec vos pairs et des experts NetIQ. NetIQ Communities vous aide à maîtriser les connaissances dont vous avez besoin pour réaliser le plein potentiel des investissements informatiques sur lesquels vous comptez en vous fournissant immédiatement des renseignements, des liens vers des ressources utiles et l'accès à des experts NetIQ. Pour obtenir de plus amples renseignements, visitez le site http://community.netiq.com.

1 Mise en route

Avant d'installer et de configurer tous les composants de 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.

Qu'est-ce que Directory and Resource Administrator?

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.

Exchange Administrator (ExA) étend les puissantes fonctionnalités de DRA et offre une gestion transparente de Microsoft Exchange. Grâce à 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.

Ensemble, 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, d'Office 365, d'Exchange et de Skype Entreprises :**

  permet la gestion administrative d'Active Directory, 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 l'automatisation du processus de travail.

Comprendre les composants de Directory and Resource Administrator

Les composants de DRA que vous utiliserez pour gérer les accès privilégiés comprennent les serveurs principaux et secondaires, les consoles d'administrateur, les composants de création de rapports et le moteur de processus de travail d'Aegis 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 principal
	Module de création de rapports de DRA Configuration du centre (NRC) CLI *(facultatif)* Fournisseur DRA ADSI *(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 avec DRA REST installé

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 principal 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, Office 365, etc.).

Console de gestion des comptes et des ressources

La console de gestion des comptes et des ressources est une interface utilisateur installable permettant aux administrateurs assistants DRA de visualiser et de gérer les objets délégués des domaines et des services connectés.

Console Web

La console Web est une interface utilisateur basée sur le Web qui fournit un accès rapide et facile aux administrateurs assistants DRA 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 pour inclure une 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 en dehors de DRA.

Un administrateur DRA peut également créer et modifier des formulaires de processus de travail automatisés afin d'exécuter des tâches automatiques de routine lorsqu'elles sont déclenchées.

L'historique unifié des modifications est une autre caractéristique de la console Web qui permet l'intégration avec les serveurs de l'historique des modifications pour vérifier les modifications apportées aux objets AD en dehors de DRA. Les options du rapport sur l'historique des modifications comprennent les éléments suivants :

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

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 :

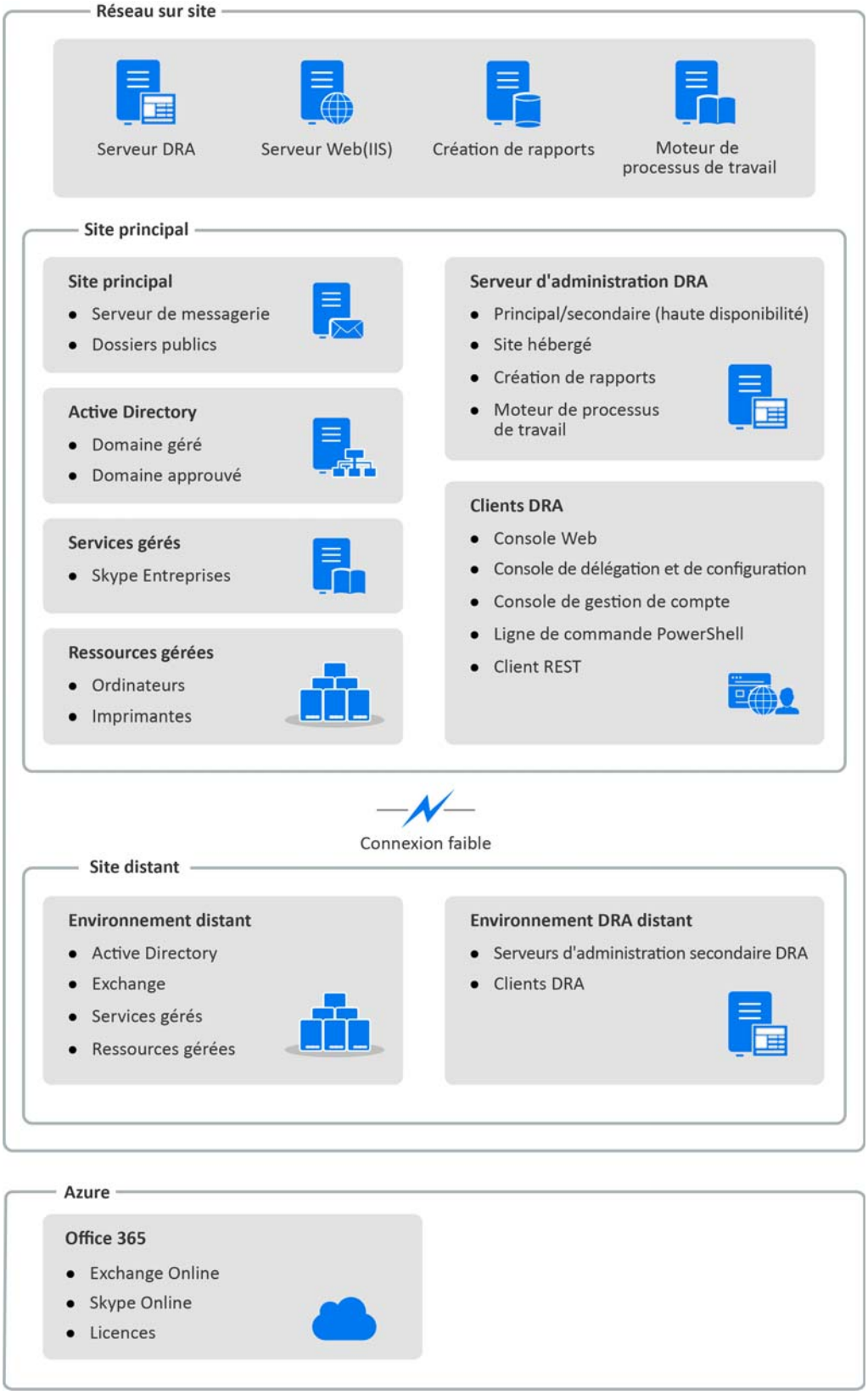
- Rapports de ressources pour les objets d'AD
- Rapports de données d'objet d'AD
- Rapports de synthèse d'AD
- Rapports de configuration de DRA
- Rapports de configuration d'Exchange
- Rapports d'Office 365 Exchange Online
- Rapports détaillés sur les tendances d'activité (par mois, domaine et pic)
-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

Moteur de processus de travail

DRA s'intègre au moteur de processus de travail d'Aegis 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 le moteur de processus de travail, consultez le site de la documentation de 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 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.

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	4 UC (x64)/cœur 2,0 GHz	16 Go	100 Go
Console Web DRA	2 UC (x64)/cœur 2,0 GHz	8 Go	100 Go
Module de création de rapports de DRA	4 UC (x64)/cœur 2,0 GHz	16 Go	100 Go
Serveur de processus de travail DRA	4 UC (x64)/cœur 2,0 GHz	16 Go	100 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 **.

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, clients DRA	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 (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM)
TCP 50000 *	Bidirectionnel	Serveurs d'administration DRA	Réplication d'attribut et communication serveur DRA-ADAM. (LDAP)
TCP 50001 *	Bidirectionnel	Serveurs d'administration DRA	Réplication d'attribut SSL (ADAM)
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 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 de Change Guardian (HTTPS)

Protocole et port	Direction	Destination	Utilisation
TCP 443, 5986, 5985	Sortant	Microsoft PowerShell	Applets de commande PowerShell natifs (HTTPS) et PowerShell à distance.
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 unifiées

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 11192 * **	Sortant	Service hôte DRA	Pour la communication entre le service DRA REST et le service d'administration DRA
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 DRA, DRA PowerShell et le service hôte DRA.
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 (http://go.microsoft.com/fwlink/?LinkID=46088) (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).

Protocole et port	Direction	Destination	Utilisation
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 (http://go.microsoft.com/fwlink/?LinkID=46088) (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)
TCP 2219	Hôte local	Fournisseur d'espace de nommage	Utilisé par le fournisseur d'espace de nommage pour exécuter les adaptateurs.
TCP 9900	Hôte local	Moteur de corrélation	Utilisé par le moteur de corrélation pour communiquer avec le moteur de processus de travail 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 Directory and Resource Administrator sur le site Web de NetIQ : https://www.netiq.com/support

Système géré	Produits préalables
Active Directory	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	◆ Microsoft Exchange 2010 SP3 (sauf pour les dossiers publics) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online

Système géré	Produits préalables
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ Module Active Directory Windows Azure 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 du serveur d'administration DRA

La configuration requise pour les logiciels et les comptes du serveur DRA est la suivante :

Configuration logicielle requise :

Composant	Produits préalables
Cible d'installation	**Système d'exploitation du serveur d'administration NetIQ :**
Système d'exploitation	◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 2008 R2 est pris en charge pour la mise à niveau uniquement. **REMARQUE :** Le serveur doit également faire partie 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 les versions supérieures.

Composant	Produits préalables

Serveur d'administration	**Directory and Resource Administrator:**
	◆ Microsoft Net Framework 4.5.2 et les versions supérieures.
	◆ L'une des options suivantes :
	  ◆ Microsoft Visual C++ 2015 (mise à jour 3) Paquets redistribuables (x64 et x86)
	  ◆ Microsoft Visual C++ 2017 (mise à jour 3) Paquets redistribuables (x64 et x86)
	◆ Microsoft Message Queuing
	◆ Rôles Microsoft Active Directory Lightweight Directory Services
	◆ Service de registre distant démarré
	Microsoft Office 365/Exchange Online Administration :
	◆ Module Active Directory Windows Azure pour Windows PowerShell
	◆ Assistant de connexion Microsoft Online Services pour les professionnels de l'informatique
	◆ Skype Entreprise Online, Module Windows PowerShell
	Pour obtenir de plus amples renseignements, consultez Plateformes 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 (mise à jour 3) Paquet redistribuable (x86)

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	Description	Autorisations
Compte de service DRA	Les autorisations requises pour exécuter le service d'administration NetIQ	◆ 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) **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.
Administrateur DRA	Compte 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. **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 : Affectez les autorisations Active Directory suivantes au compte d'accès au domaine :

- Contrôle TOTAL sur les objets Utilisateurs
- Contrôle TOTAL sur les objets Ordinateurs
- Contrôle TOTAL sur les objets Groupes
- Contrôle TOTAL sur les objets Contacts
- Contrôle TOTAL sur les objets Unités organisationnelles
- Contrôle TOTAL sur les objets Inetorgperson
- Contrôle TOTAL sur les objets Imprimantes

- Contrôle TOTAL sur les objets Domaines intégrés
- Contrôle TOTAL sur les objets Containeurs
- Contrôle TOTAL sur les objets MsExchSystemObjectContainer
- Contrôle TOTAL sur les Groupes de distribution dynamique
- Contrôle TOTAL sur les Dossiers publics

Spécifiez les privilèges suivants avec la portée « Cet objet et tous les objets enfants » dans le compte de service de 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 de Points de connexion de service
- Autoriser la suppression de Points de connexion de service
- Autoriser la création de Conteneurs
- Autoriser la suppression de Conteneurs
- Autoriser la création de Dossiers publics
- Autoriser la suppression de Dossiers publics

Office 365 - Compte d'accès des locataires : Affectez les autorisations Active Directory suivantes au compte d'accès des locataires d'Office 365 :

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

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

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

Après l'installation de DRA :

- Exécutez la commande suivante pour déléguer l'autorisation au « conteneur Objets supprimés » du dossier d'installation de DRA (Remarque : La commande doit être exécutée par un administrateur de domaine) :

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

- Exécutez la commande suivante pour déléguer l'autorisation à « l'unité d'organisation NetIQReceyleBin » dans le dossier d'installation de DRA (Remarque : Cette opération ne peut être effectuée qu'après l'ajout des domaines respectifs à gérer par DRA) :

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

- Ajoutez le compte de remplacement avec un droit d'accès minimal au groupe « Administrateurs locaux » sur chaque ordinateur sur lequel DRA gérera des ressources telles que les imprimantes, les services, le journal des événements, les périphériques, etc.
- 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.
- Ajoutez le compte de remplacement avec un droit d'accès minimal au rôle « Gestion de l'organisation » pour gérer les objets Exchange.

Configuration requise pour la console Web et les extensions de DRA

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

Configuration logicielle requise :

Composant	Produits 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
Point d'extrémité et service DRA REST	◆ Microsoft .Net Framework 4.5.2
Extensions PowerShell	◆ Microsoft .Net Framework 4.5.2 ◆ PowerShell 4.0

Composant	Produits 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 répertoire ◆ Erreurs HTTP ◆ Développement d'application ◆ ASP ◆ Intégrité et diagnostics ◆ Journalisation HTTP ◆ Moniteur de requête ◆ Sécurité ◆ Authentification de base ◆ Performance ◆ Compression du contenu statique ◆ Outils de gestion de serveur Web

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, 2012 R2, 2016

Composant	Produits 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:** Chaque serveur d'administration DRA qui se connecte au Module de création de rapports de DRA, nécessite également .NET Framework 3.5. **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.
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 une clé de licence d'évaluation (License1.lic) 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 d'informations sur la définition et les restrictions de licence.

Installation du produit

Ce chapitre vous guide dans l'installation de Directory and Resource Administrator. Pour plus d'informations 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 principal ou secondaire dans votre environnement. Les exigences pour un serveur d'administration principal et secondaire sont les mêmes; cependant, chaque déploiement DRA doit inclure un serveur d'administration principal.

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 NetIQ 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.
Exécution de l'installation de DRA	Lancez l'installation de DRA. **REMARQUE :** Pour exécuter l'installation plus tard, accédez à l'emplacement où le fichier d'installation a été extrait et exécutez `Setup.exe`.
Sélection des composants NetIQ Administration Server 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 pour l'installation. Options des composants : **NetIQ Administration Server** ◆ Log Archive Resource Kit ◆ NetIQ DRA SDK **Composant Web hérité** **Interfaces utilisateur** ◆ Gestion des comptes et des ressources ◆ Fournisseur DRA ADSI ◆ Interface de ligne de commande ◆ Délégation et configuration
Vérification 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.
Acceptation du CLUF	Acceptez les termes du contrat de licence d'utilisateur final.
Sélection du mode de fonctionnement du serveur	Sélectionnez **Principal** pour installer le premier serveur d'administration DRA dans un ensemble multimaître (il n'y aura qu'un seul serveur principal dans un déploiement) ou **Secondaire** pour joindre un nouveau serveur d'administration DRA à un ensemble multimaître existant. Pour obtenir de plus amples renseignements sur les ensembles multimaîtres, consultez la rubrique « Configuration d'un ensemble multimaître » dans le *Guide de l'administrateur de Directory and Resource Administrator*.
Spécification des comptes d'installation et des informations d'identification	◆ Compte de service DRA ◆ Groupe AD LDS ◆ Administrateur DRA Pour obtenir de plus amples renseignements, consultez :Configuration requise du serveur d'administration DRA.

Étape	Détails
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.
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.

Installation de clients DRA

Vous pouvez installer des consoles DRA et des clients de ligne de commande précis en exécutant DRAInstaller.msi avec le paquet .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 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 un fichier .mst de l'interface utilisateur, tel que NetIQDRAUserConsole.mst, 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 des extensions DRA REST

Le paquet d'extensions DRA REST comporte quatre fonctionnalités :

- **Service hôte NetIQ DRA :** passerelle utilisée pour communiquer avec le service d'administration DRA. Ce service doit être exécuté sur un ordinateur sur lequel le service d'administration DRA est installé.
- **Service DRA REST et points d'extrémité :** fournit les interfaces RESTful permettant à la console Web DRA et aux clients non DRA de demander des opérations DRA. Ce service doit être exécuté 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 administrateurs adjoints, mais également des options de personnalisation.

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.
Installation du certificat SSL	S'il n'est pas déjà installé sur le serveur Windows, vous devez installer un certificat SSL avant d'exécuter l'installation.
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 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.
Exécution du programme d'installation des extensions DRA REST	Une fois que la trousse d'installation DRA a terminé d'extraire le fichier d'installation, vous êtes invité à lancer l'installation de DRA. Accédez à l'emplacement où le fichier d'installation a été extrait, cliquez avec le bouton droit de la souris sur le fichier `DRARESTExtensionsInstaller.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
Acceptation du CLUF	Acceptez les termes du contrat de licence d'utilisateur final.
Sélectionnez les composants et spécifiez l'emplacement cible pour l'installation	Dans la boîte de dialogue d'installation **Sélectionner les composants**, installez toutes les options : service hôte DRA, points d'extrémité et service DRA REST, extensions PowerShell et 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 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.
Spécification du compte de service à exécuter en tant que	Par défaut, le compte de service existant du serveur DRA est affiché. Spécifiez le mot de passe du compte de service. Pour obtenir de plus amples renseignements sur la configuration d'un compte de service pour le serveur d'administration DRA, consultezConfiguration requise du serveur d'administration DRA.
Spécification du certificat SSL du service REST	Sélectionnez le certificat SSL que vous utiliserez pour le service REST et spécifiez les ports de service REST et hôte.

Étape	Détails
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.

Installez le serveur de processus de travail

Pour obtenir de plus amples renseignements sur l'installation du serveur de processus de travail, reportez-vous au Guide d'administrateur d'Aegis.

Installez le module de création de rapports de DRA

Le module de création de rapports de DRA requiert l'installation de deux fichiers exécutables à partir de la trousse d'installation NetIQ DRA : `NRCSetup.exe` et `DRAReportingSetup.exe`.

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 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. En outre, la trousse d'installation installera l'infrastructure .Net sur le serveur cible si nécessaire pour satisfaire les conditions préalables du programme d'installation du produit DRA.
Exécution de l'installation de NetIQ Reporting Center (NRC)	Une fois que la trousse d'installation DRA a fini d'extraire le fichier d'installation, accédez à l'emplacement où le fichier d'installation a été extrait et exécutez `NRCSetup.exe`.
Sélection du composant NetIQ Reporting Center.	Dans la boîte de dialogue d'installation **Sélectionner les composants**, utilisez le composant par défaut « NetIQ Reporting Center » pour installer les quatre composants NRC.
Spécification de l'emplacement cible pour l'installation	Acceptez l'emplacement d'installation par défaut `C:\Program Files (x86)\NetIQ\Reporting Center` ou indiquez un autre emplacement pour l'installation.
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. **IMPORTANT :** .NET Framework 3.5 doit être installé manuellement sur le serveur de création de rapports avant l'installation de NRC.
Acceptation du CLUF	Acceptez les termes du contrat de licence d'utilisateur final.

Étapes	Détails
Installation de la base de données de configuration	Utilisez les valeurs par défaut de la boîte de dialogue **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 du module de création de rapports de DRA	Accédez à l'emplacement où le fichier d'installation a été extrait et exécutez `DRAReportingSetup.exe` pour installer le composant de gestion pour l'intégration du module de création de rapports de DRA.
Acceptation du CLUF	Acceptez les termes du contrat de licence d'utilisateur final pour terminer l'installation.

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 principal 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 » dans le *Guide de l'administrateur de Directory and Resource Administrator*.

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'AA dépendent de chaque MMS. Si la majorité de vos AA utilisent des serveurs ou des ensembles de serveurs précis, mettez d'abord à niveau ces serveurs pendant les heures creuses.
- Déterminez quels AA ont besoin de la console de délégation et de configuration. Vous pouvez obtenir ces informations de l'une des façons suivantes :
  - Examinez les AA associés aux groupes AA intégrés.
  - Examinez les AA associés aux ActiveView 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 AA de vos projets de mise à niveau pour des interfaces utilisateur.

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

  Informez ces AA 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.

Tâches préalables à la mise à niveau

Avant de commencer les installations de mise à niveau, suivez les étapes de pré-mise à niveau ci-dessous pour préparer chaque ensemble de serveurs pour la mise à niveau.

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 AA). Pour obtenir de plus amples renseignements, consultez Planification de la mise à niveau de DRA.
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 principal 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 principal	Sauvegardez le registre à partir du serveur d'administration principal. La sauvegarde de vos paramètres de registre précédents vous permet de récupérer facilement vos paramètres de configuration et de sécurité précédents.

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. Redémarez l'instance AD LDS.

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 AA 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'AA 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 principal.
- 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 à garantir que vos AA puissent 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 principal 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 AA 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 AA 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 principal pour modifier ces paramètres. Une fois que vous avez mis à niveau le serveur d'administration principal, 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 principal en tant qu'administrateur intégré.
2. Démarrez l'interface MMC.
3. Dans le volet gauche, développez **Gestion de la configuration**.
4. Cliquez sur **Serveurs d'administration**.
5. Dans le volet droit, sélectionnez le serveur d'administration principal approprié pour cet ensemble de serveurs.
6. Cliquez sur **Propriétés**.
7. Dans l'onglet Planification de la synchronisation, cliquez sur **Actualiser maintenant**.
8. 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.

Vous pouvez répartir ce 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.

Dans DRA 9.2 ou dans les versions ultérieures, la configuration du serveur Automatisation du processus de travail est stockée dans AD LDS au lieu du registre. Lors de la mise à jour de DRA 9.1 ou d'une version antérieure vers DRA 9.2 ou vers une version ultérieure, la configuration du registre est automatiquement déplacée vers AD LDS et répliquée sur tous les 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 principal pour ce MMS.

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 principal	Mettez à niveau le serveur d'administration principal dans le MMS approprié.
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.
Déploiement des interfaces utilisateur	Déployez les interfaces utilisateur sur vos administrateurs assistants.

Étapes	Détails
Mise à niveau les serveurs secondaires	Mettez à niveau les serveurs d'administration secondaires dans le MMS.
Mise à niveau du module de création de rapports de DRA	Mettez à niveau le module de création de rapports de DRA.
Mise à niveau des extensions REST	Exécutez le programme d'installation des extensions DRA REST.
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.

Mise à niveau du serveur d'administration principal

Une fois que vous avez terminé avec la préparation de votre MMS, mettez à niveau le serveur d'administration principal. Ne mettez pas à niveau les interfaces utilisateur sur les ordinateurs clients AA tant que vous n'avez pas mis à niveau le serveur d'administration principal. 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 de mise à jour de Directory and Resource Administrator*.

Avant de procéder à la mise à niveau, informez vos AA 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 AA 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 principal, 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 AA 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'AA 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 principal.
- Votre environnement comprend un MMS qui s'étend sur plusieurs sites.

Par exemple, si votre MMS se compose d'un serveur d'administration principal 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 AA 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 AA 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 principal et un serveur d'administration secondaire. Toutefois, pour les AA qui doivent utiliser le serveur d'administration principal, 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 ou le fournisseur ADSI, 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 AA 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 AA.

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 AA, 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 utilisateurs de 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 AA 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 AA 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 AA exécutent des interfaces utilisateur mises à niveau, déconnectez tous les serveurs ayant des versions précédentes de DRA.

Mise à niveau des composants du module de création de rapports de DRA

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 3.2. Pour obtenir de plus amples renseignements sur les exigences d'installation et les considérations relatives à la mise à niveau, consultez le *Guide de Reporting Center* sur le site de la documentation de DRA.

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 `DRAReportingSetup.exe` à partir de la trousse 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 celui-ci 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 de la configuration de NRC sur les ordinateurs clients	Exécutez `NRCSetup.exe` sur tous les ordinateurs clients de NRC.
Activation de la prise en charge du module de création de rapports de DRA	Sur votre serveur d'administration principal, 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 NetIQ Reporting Center Reporting* sur le site de la documentation de DRA.

Mise à niveau des extensions de DRA REST

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 obtenir de plus amples renseignements sur les exigences, consultez Configuration requise pour la console Web et les extensions de DRA.

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

1. Après avoir téléchargé la trousse d'installation de DRA, accédez à l'emplacement où le fichier d'installation a été extrait, cliquez avec le bouton droit de la souris sur le fichier `DRARESTExtensionsInstaller.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
2. Suivez les instructions de l'assistant d'installation jusqu'à la fin, puis cliquez sur **Terminer**.

Pour obtenir des renseignements détaillés sur les étapes de l'assistant d'installation, reportez-vous à la procédure à suivre pour une nouvelle installation :Installation des extensions DRA REST.

Mise à niveau d'un contenu personnalisé

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

Une partie du processus de l'utilitaire de mise à niveau des personnalisations consiste à sauvegarder vos personnalisations avant le démarrage de la mise à niveau. Pendant le processus 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 pour tous les éléments de personnalisation qui ne peuvent pas être mis à jour automatiquement.

Il est recommandé de consulter le journal après la mise à niveau. Si nécessaire, vous pouvez revenir aux personnalisations d'avant 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 à l'ouverture de l'utilitaire de personnalisation ou utiliser le chemin par défaut, qui se remplit automatiquement.

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

- Chemin d'accès au dossier des personnalisations par défaut : `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 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.

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 le fichier de clé de licence d'évaluation (`TrialLicense.lic`) fourni par NetIQ Corporation.

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.

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, telles que celles incluses 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 Directory and Resource Administrator*.

Ajout de sous-arborescences gérées

Vous pouvez ajouter des sous-arborescences gérées à partir de domaines Microsoft Windows précis après avoir installé le serveur d'administration. Vous pouvez ajouter les sous-arborescences manquantes à gérer à l'aide du nœud Configuration avancée de la console de délégation et de configuration. 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 Directory and Resource Administrator*.

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 Directory and Resource Administrator*.

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 Directory and Resource Administrator*.

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.

Configuration du groupe Utilisateurs du modèle COM distribué

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'appartenance au groupe Utilisateurs du modèle COM distribué pour inclure tous les comptes d'utilisateurs qui utilisent DRA. Cette adhésion doit inclure le compte de service DRA et tous les administrateurs assistants.

Pour configurer le groupe Utilisateurs du modèle COM distribué :

1. Connectez-vous à un ordinateur client 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**.

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 les outils d'administration, puis les services de composants.
3. Développez **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.