

CA ARCserve® Replication and High Availability pour Windows

Manuel des opérations pour le serveur Microsoft® IIS

r15



La présente documentation ainsi que tout programme d'aide informatique y afférant (ci-après nommés "Documentation") vous sont exclusivement fournis à titre d'information et peuvent être à tout moment modifiés ou retirés par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

SOUS RESERVE DES DISPOSITIONS PREVUES PAR LA LOI APPLICABLE, CA FOURNIT LA PRESENTE DOCUMENTATION "TELLE QUELLE" SANS AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, NOTAMMENT AUCUNE GARANTIE DE LA QUALITE MARCHANDE, D'UNE QUELCONQUE ADEQUATION A UN USAGE PARTICULIER OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ETRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RESULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITE, PERTE DE DONNEES OU DE CLIENTS, ET CE MEME DANS L'HYPOTHESE OU CA AURAIT ETE EXPRESSEMENT INFORME DE LA POSSIBILITE DE LA SURVENANCE DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

La présente Documentation étant éditée par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2010 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits CA référencés

Ce document fait référence aux produits CA suivants :

- CA ARCserve® Replication
- CA ARCserve® High Availability (HA)
- CA ARCserve® Assured Recovery
- CA ARCserve® Content Distribution

Tout au long de ce manuel, le terme CA ARCserve RHA représente la famille de produits, préalablement appelée CA XOsoft Replication (WANsync) et CA XOsoft High Availability (WANsyncHA).

Informations de contact de CA

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse <http://www.ca.com/worldwide>.

Modifications de la documentation

Les actualisations suivantes ont été réalisées depuis la dernière version de la présente documentation :

- Dans ce manuel, le nom du produit a été remplacé par CA ARCserve RHA.
- [Création d'un scénario Microsoft IIS](#) (page 15): cette section a été mise à jour pour inclure les nouvelles informations de la fenêtre de base de données pour la réplication.
- [Retour arrière des données](#) (page 47): cette section a été mise à jour pour inclure les nouvelles informations contenues dans la boîte de dialogue Sélection d'un point de retour arrière.
- [Boîte de dialogue Sélection d'un point de retour arrière](#) (page 52): nouvelle section décrivant les champs de la boîte de dialogue.

Table des matières

Chapitre 1 : Introduction	7
A propos de ce manuel	7
Documentation connexe	7
Configuration requise pour le serveur	8
Configuration de base	8
Configuration requise pour un serveur IIS	9
Conditions du compte de connexion	10
Serveurs fonctionnant dans un groupe de travail	10
A propos des clusters	11
Réplication d'une métabase IIS	11
Enregistrement des licences CA ARCserve RHA	12
Chapitre 2 : Création et utilisation de scénarios	15
Création d'un scénario Microsoft IIS	15
Propriétés du scénario	17
Exécution d'un scénario hors de l'assistant	20
Arrêt d'un scénario	22
Affichage d'un rapport	23
Chapitre 3 : Méthodes de redirection	25
Fonctionnement de la redirection	25
Redirection du système DNS	25
Redirection Transfert IP	26
Ajout d'une adresse IP sur le serveur maître	26
Transfert IP de cluster	30
Redirection Permutation du nom de l'ordinateur	34
Redirection automatique par permutation du nom de l'ordinateur	34
Redirection par scripts	35
Chapitre 4 : Permutation et permutation inversée	37
Fonctionnement de la permutation et de la permutation inversée	37
Démarrage d'une permutation	39
Démarrage d'une permutation inversée	41
Considérations sur la permutation	44

Chapitre 5 : Récupération de données	45
Processus de récupération des données	45
Définition de repères.....	45
Retour arrière des données.....	47
Retour arrière des données	48
Boîte de dialogue Sélection d'un point de retour arrière	52
Récupération de données perdues à partir du serveur de réPLICATION	54
Récupération du serveur actif	55
Annexe A : Informations et astuces supplémentaires	57
Paramètres de répertoire du spool	58
Configuration de comptes de service	59
Ressources supplémentaires	59
Récupération de serveurs	60
Récupération manuelle d'un serveur en échec - Transfert de l'adresse IP	61
Récupération manuelle d'un serveur en échec - Permutation du nom de l'ordinateur.....	62
Récupération manuelle d'un serveur en échec-Transfert IP et Permutation du nom	63
Annexe B : Installation d'IIS 6.0 Management Compatibility pour IIS 7.0	65
Index	69

Chapitre 1 : Introduction

CA ARCserve Replication and High Availability (CA ARCserve RHA) est une solution économique de haute disponibilité avec réplication asynchrone en temps réel, permutation et permutation inversée automatisée des applications, qui permet d'assurer la continuité de l'activité commerciale pour Microsoft IIS Server et d'autres serveurs d'applications sous Windows 32 et 64 bits.

Vous pouvez répliquer des données vers un serveur local ou distant à l'aide de CA ARCserve RHA, ce qui permet de récupérer ces données perdues en raison d'un arrêt brutal du serveur ou d'un sinistre des sites. Vous pouvez basculer manuellement ou automatiquement vos utilisateurs vers le serveur de réplication, si vous disposez d'une licence de High Availability. Ce manuel présente les concepts et procédures de réplication et de haute disponibilité.

Les procédures indiquées dans ce manuel doivent être rigoureusement suivies. Personnalisez les étapes uniquement dans les cas suivants :

- Vous connaissez CA ARCserve RHA et êtes pleinement conscient de l'impact potentiel des changements que vous y apportés.
- Vous avez intégralement testé les étapes dans un environnement de laboratoire avant de les implémenter dans un environnement de production.

Ce chapitre traite des sujets suivants :

[A propos de ce manuel](#) (page 7)

[Documentation connexe](#) (page 7)

[Configuration requise pour le serveur](#) (page 8)

[Enregistrement des licences CA ARCserve RHA](#) (page 12)

A propos de ce manuel

Ce document présente l'implémentation d'une solution CA ARCserve RHA pour Microsoft IIS Server. Il est essentiel que vous disposiez des ressources et des autorisations appropriées pour effectuer chaque tâche.

Documentation connexe

Utilisez ce manuel associé au *Manuel d'installation de CA ARCserve RHA* et au *Manuel d'administration de CA ARCserve RHA*.

Configuration requise pour le serveur

Pour implémenter CA ARCserve HA, reportez-vous ci-après à la liste de configuration requise appropriée au type de serveur que vous avez sélectionné. Ces composants sont vendus sous licences distinctes. Si vous ne disposez pas de la licence requise pour accéder au support pour un type de service donné, contactez le support technique.

Configuration de base

Configuration de base

- Deux serveurs exécutant Windows Server 2003 ou 2008, avec le même niveau de Service Packs et de correctifs
- Toutes les adresses IP sont attribuées statiquement. Les adresses IP attribuées par le serveur DHCP sur le serveur maître ou de réplication ne sont pas prises en charge.
- Le serveur protégé n'est pas un contrôleur de domaine ou un serveur DNS.
- Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou des mêmes domaines sécurisés.
- Microsoft IIS doit être installé sur le serveur maître et sur le serveur de réplication.

Configuration requise pour un serveur IIS

- Une instance du serveur Microsoft IIS Server 6 ou 7 doit être installée sur chaque serveur.
 - Les mêmes services IIS doivent être installés sur les deux serveurs : WWW, SMTP, etc.
 - Les mêmes extensions de services Web doivent être installées sur les deux serveurs.
 - Les chemins complets contenant les fichiers de site doivent être identiques sur les deux serveurs.
- Le serveur en attente doit disposer d'une installation propre à IIS avec les sites par défaut uniquement.
- Les sites du serveur maître ne doivent pas utiliser la redirection des URL ou la redirection de chemin de contrôlé réseau unifié.
- Les serveurs maître et de réplication doivent se trouver dans la même forêt Active Directory et être membres du même domaine ou des mêmes domaines sécurisés.
- Si un accès anonyme est activé et utilisé, configurez les éléments suivants.
 - Pour que les autorisations des deux serveurs soient toujours synchronisées, les deux processus IIS doivent utiliser le même compte d'utilisateur pour un accès en tant qu'utilisateur anonyme. Créez un nouveau compte d'utilisateur de domaine et configurez les deux serveurs IIS pour qu'ils utilisent ce compte. Pour en savoir plus, consultez la documentation de Microsoft.
 - Bien que la documentation de Microsoft ne le mentionne pas, vous devez modifier la stratégie de groupe locale (ou de domaine) afin d'accorder les droits suivants au compte d'utilisateur : Permettre l'ouverture d'une session locale, Ouvrir une session en tant que tâche et Accéder à cet ordinateur à partir du réseau. Veillez par ailleurs à dupliquer toutes les modifications d'autorisations apportées au système de fichiers pour le compte d'utilisateur anonyme d'origine dans le compte de domaine nouvellement affecté.
- Si vous utilisez le chiffrement SSL, consultez la documentation de Microsoft suivante. Elle contient des informations sur la copie du certificat requis.
- Si vous utilisez IIS 7.0, le composant IIS 6.0 Management Compatibility doit être installé. Etant donné qu'IIS 6.0 Management Compatibility est désactivé par défaut lors de l'installation d'IIS 7.0, vous devez activer cette option lors du processus d'installation d'IIS 7.0. Pour plus d'informations, consultez la section relative à l'[installation du composant IIS 6.0 Management Compatibility pour IIS 7.0](#) (page 65).

Installation d'IIS

Pour implémenter une solution CA ARCserve RHA pour Microsoft IIS Server, installez d'abord IIS sur les serveurs maître et de réPLICATION. Pour en savoir plus sur les conditions et les procédures d'installation d'IIS, consultez la documentation de Microsoft.

Conditions du compte de connexion

Le service du moteur CA ARCserve RHA doit respecter certaines conditions du compte pour assurer une communication correcte avec d'autres composants. Si ces conditions ne sont pas remplies, les scénarios risquent de ne pas s'exécuter. Si vous ne bénéficiez pas des autorisations requises, contactez votre équipe IS locale.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas membre des administrateurs du groupe local de domaine intégré, vous devez utiliser un compte qui le soit.
- Il s'agit d'un membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.
- Pour les serveurs faisant partie d'un groupe de travail, utilisez le compte du système local.
- Les serveurs maître et de réPLICATION doivent se trouver dans la même forêt Active Directory.

Serveurs fonctionnant dans un groupe de travail

Pour les serveurs d'un groupe de travail, définissez le compte de service du moteur CA ARCserve RHA sur Système local (sauf si vous avez ajouté des scripts personnalisés qui requièrent des niveaux d'autorisation plus élevés). Les serveurs d'un groupe de travail peuvent utiliser la redirection du système DNS uniquement avec les serveurs DNS qui autorisent les mises à jour non sécurisées. Vous pouvez utiliser normalement le transfert IP, la permutation du nom de l'ordinateur et les scripts de redirection personnalisés.

A propos des clusters

L'installation sur des clusters est très similaire à une installation standard. Pour configurer CA ARCserve HA sur un cluster, entrez la ressource de nom de réseau (ou d'adresse IP) du serveur virtuel (dans le groupe que vous souhaitez protéger) comme nom de l'ordinateur maître ou de réplication. N'utilisez pas de noms ou d'adresses IP de noeuds lorsque vous configurez le scénario. Vous devez également installer le moteur CA ARCserve RHA sur tous les noeuds du cluster. Reportez-vous à la section *Configuration du serveur*.

L'utilisation du transfert IP avec un cluster est la seule configuration nécessitant une préparation. Pour plus d'informations sur l'utilisation du transfert d'IP avec des clusters, consultez la section de [transfert d'IP avec clusters](#) (page 30).

RéPLICATION D'UNE MÉTABASE IIS

CA ARCserve Replication a été amélioré pour assurer une protection complète des métabases IIS. Il n'est plus nécessaire de créer des sites Web sur l'ordinateur de réplication avant d'exécuter un scénario de haute disponibilité IIS. La métabase est régulièrement répliquée lors de l'exécution des scénarios de haute disponibilité.

Remarque : La protection des métabases est uniquement prise en charge avec les versions 6.0 et 7.0 d'IIS dans les scénarios de haute disponibilité CA ARCserve Replication.

Les scénarios de haute disponibilité permettent désormais de surveiller et de restaurer les services IIS ainsi que les sites utilisant l'option de vérification d'activation. CA ARCserve Replication peut ainsi déterminer si le dysfonctionnement d'un service IIS a entraîné l'arrêt du site correspondant. La vérification d'activation permet de surveiller les services IIS répertoriés participant à un scénario de haute disponibilité, de vérifier le statut de chaque service et de restaurer ceux qui ne fonctionnent pas. Cela évite tout redémarrage inutile par CA ARCserve Replication de sites en cours d'exécution.

Dans les environnements Microsoft Cluster Server, l'option de détection automatique IIS a été améliorée afin que les sites locaux ou les sites contenant un emplacement ne figurant pas sur le disque MSCS partagé soient identifiés et automatiquement exclus du scénario, vous laissant ainsi la possibilité d'exécuter des scénarios avec les paramètres par défaut.

Enregistrement des licences CA ARCserve RHA

La stratégie d'octroi de licence CA ARCserve RHA est basée sur une combinaison de plusieurs paramètres qui porte sur les éléments suivants :

- systèmes d'exploitation impliqués
- solution requise
- serveurs d'applications et de base de données pris en charge
- nombre d'hôtes utilisés
- modules supplémentaires (module Récupération garantie par exemple)

La clé de licence générée pour vous est donc adaptée à vos besoins précis.

Si vous vous connectez pour la première fois ou si votre ancienne licence arrive à expiration, vous devez enregistrer le produit CA ARCserve RHA à l'aide de votre clé de licence. Pour enregistrer le produit, vous devez ouvrir le gestionnaire, qui ne dépend pas de l'existence d'une clé d'enregistrement valide. Une fois le gestionnaire ouvert, un message d'avertissement concernant la licence s'affiche et vous invite à enregistrer le produit. Un message d'avertissement concernant la licence apparaît également lorsque votre licence est sur le point d'arriver à expiration au cours des 14 prochains jours.

Lorsque vous créez un scénario, certaines options peuvent être désactivées selon les termes de votre licence. Toutefois, étant donné que la validité de votre clé de licence a été confirmée, vous pouvez créer le nombre de scénarios de votre choix, avant d'exécuter un scénario spécifique. Le système vérifie si vous êtes autorisé à exécuter le scénario sélectionné, conformément à votre clé de licence, uniquement lorsque vous cliquez sur le bouton Exécuter. Si le système détermine que vous ne disposez pas de la licence requise pour exécuter ce scénario, celui-ci ne s'exécute pas et un message apparaît dans le volet Evénement pour vous indiquer le type de licence dont vous avez besoin.

Pour enregistrer CA ARCserve RHA au moyen de la clé de licence :

1. Ouvrez le gestionnaire.

Le message de bienvenue s'affiche, suivi d'un message d'avertissement relatif à la licence vous informant que votre produit n'a pas été enregistré. Vous êtes invité à l'enregistrer.

2. Cliquez sur OK pour fermer le message.
3. Ouvrez le menu Aide et sélectionnez l'option Enregistrer.

La boîte de dialogue Enregistrer CA ARCserve RHA s'ouvre.

4. Renseignez les champs suivants :
 - Dans le champ Clé d'enregistrement, entrez votre clé d'enregistrement.
 - (Facultatif) Dans le champ Nom de la société, entrez le nom de votre société.
5. Cliquez sur le bouton Enregistrer pour enregistrer votre produit et fermer la boîte de dialogue.

Vous pouvez désormais utiliser le gestionnaire CA ARCserve RHA dans la limite des autorisations accordées par votre licence.

Chapitre 2 : Création et utilisation de scénarios

Ce chapitre traite des sujets suivants :

[Création d'un scénario Microsoft IIS](#) (page 15)

[Propriétés du scénario](#) (page 17)

[Exécution d'un scénario hors de l'assistant](#) (page 20)

[Arrêt d'un scénario](#) (page 22)

[Affichage d'un rapport](#) (page 23)

Création d'un scénario Microsoft IIS

La création de scénarios est détaillée dans le Manuel d'administration de CA ARCserve RHA. Cette section contient des informations supplémentaires propres aux scénarios de haute disponibilité Microsoft IIS Server. L'assistant de création de scénarios vous guide à chaque étape requise pour créer un scénario de haute disponibilité. Lorsqu'il a terminé, vous devez exécuter votre scénario pour démarrer la synchronisation des données. La synchronisation peut prendre un certain temps, selon la taille de la base de données et la bande passante du réseau. Une fois la synchronisation terminée, votre scénario de haute disponibilité maintient le serveur de réplication prêt à remplacer le serveur maître dès qu'une défaillance est détectée.

Lisez la procédure complète, y compris les informations référencées, le cas échéant, avant de continuer.

Pour créer un scénario de haute disponibilité Microsoft IIS

1. Ouvrez le gestionnaire CA ARCserve RHA, sélectionnez Scénario, Nouveau ou cliquez sur le bouton Nouveau scénario.
La boîte de dialogue Bienvenue s'ouvre.
2. Sélectionnez Créer un scénario, puis cliquez sur Suivant.
La boîte de dialogue de sélection du type de scénario s'affiche.
3. Sélectionnez Microsoft IIS Server, Scénario de haute disponibilité et Test d'intégrité de l'ordinateur de réplication pour la récupération garantie (facultatif).
La boîte de dialogue Hôtes maître et de réplication s'ouvre. Pour plus d'informations sur la récupération garantie, reportez-vous au Manuel d'administration de CA ARCserve RHA.

4. Entrez le nom du scénario, le nom d'hôte ou l'adresse IP et le numéro de port pour les serveurs maître et de réplication. Si l'un ou l'autre des serveurs est un cluster MSCS, entrez le nom ou l'adresse IP du serveur virtuel de la ressource de cluster. Vérifiez que l'option Vérifier le moteur CA ARCserve RHA sur les hôtes est activée (par défaut).
5. Cliquez sur Suivant.
6. Patientez jusqu'à la fin de la Vérification du moteur, puis cliquez sur Suivant. Si nécessaire, cliquez sur Installer pour mettre à niveau le moteur sur un ou sur les deux serveurs, puis cliquez sur Suivant.

La boîte de dialogue Base de données à répliquer s'ouvre et répertorie tous les résultats de la détection automatique pour l'ordinateur maître spécifié. Par défaut, toutes les bases de données sont incluses.
7. [Facultatif] Sélectionnez l'option Répliquer les nouveaux sites dans les répertoires racines sélectionnés.

Si vous ajoutez de nouveaux sites à un répertoire racine après avoir créé le scénario, CA ARCserve RHA le réplique automatiquement. Les nouveaux sites apparaîtront dans le gestionnaire IIS pendant la réplication.
8. Cliquez sur Suivant.

La boîte de dialogue Configuration de la réplication s'ouvre. CA ARCserve RHA compare les configurations de Microsoft IIS de l'hôte maître et de l'hôte de réplication, puis configure le serveur de réplication automatiquement.
9. [Facultatif] Sélectionnez l'option Ignorer la configuration sur l'ordinateur de réplication.
10. Cliquez sur Suivant.

La boîte de dialogue Propriétés du scénario s'ouvre.
11. Si nécessaire, vous pouvez configurer des propriétés supplémentaires. Si vous utilisez les listes de contrôle d'accès NTFS (New Technology File System, système de fichiers conçu pour Windows NT) avec des comptes de domaine pour contrôler l'accès des utilisateurs, nous vous recommandons de sélectionner l'option Réplication de la liste de contrôle d'accès NTFS ; cliquez ensuite sur Suivant.

La boîte de dialogue Propriétés des hôtes maître et de réplication s'ouvre. Pour plus d'informations, reportez-vous à la section Propriétés du scénario ou au Manuel d'administration de CA ARCserve RHA.

12. Acceptez ou modifiez les paramètres par défaut. Planifiez le test d'intégrité pour la récupération garantie, puis cliquez sur Suivant.
13. Patientez jusqu'à ce que les informations soient récupérées dans la boîte de dialogue Propriétés de la permutation. Configurez les propriétés de redirection souhaitées, puis cliquez sur Suivant.

La boîte de dialogue Démarrage de la permutation et de la réplication inversée s'ouvre. Pour plus d'informations, reportez-vous à la section [Permutation et permutation inversée](#) (page 37).
14. Choisissez la permutation et la réplication inversée automatiques ou manuelles, si nécessaire.

Pour plus d'informations, reportez-vous à la section Propriétés du scénario ou au Manuel d'administration de CA ARCserve RHA.

Remarque : Ne définissez pas ces deux options sur Automatique.
15. Cliquez sur Suivant.

CA ARCserve RHA commence la vérification du scénario. Résolvez les erreurs et les avertissements avant de poursuivre.
16. Une fois le scénario vérifié, cliquez sur Suivant.

Le scénario est créé.
17. Choisissez Exécuter ou Terminer, comme souhaité.

Exécuter démarre la synchronisation. Terminer vous permet d'exécuter le scénario ultérieurement. Reportez-vous à la section Exécution d'un scénario hors de l'assistant.

Propriétés du scénario

Pour modifier un scénario configuré via l'assistant ou configurer des paramètres supplémentaires, utilisez le volet Propriétés.

Le volet Propriétés et ses onglets sont fonction du contexte et changent à chaque fois que vous sélectionnez un noeud différent dans un dossier de scénarios. Vous devez arrêter un scénario avant de configurer ses propriétés. Certaines valeurs ne peuvent pas être modifiées une fois définies ; elles sont notées. Vous trouverez des informations détaillées sur la configuration des propriétés de scénarios ainsi que leurs descriptions dans le manuel d'administration de CA ARCserve RHA.

Les propriétés sont réparties dans les onglets du volet Cadre d'applications du gestionnaire CA ARCserve RHA. Les onglets affichés dépendent du type de serveur, de la solution CA ARCserve RHA et du statut du scénario. Sélectionnez le scénario dont vous souhaitez modifier les propriétés, puis cliquez sur l'onglet adéquat. La fenêtre suivante présente un exemple de scénario IIS.

Paramètres de l'onglet Répertoires racines

Dans le volet Scénario, sélectionnez un serveur maître. Double-cliquez sur son dossier Répertoires pour ajouter ou supprimer des répertoires racines de l'ordinateur maître. Sélectionnez ou désélectionnez les cases à cocher situées en regard des dossiers pour inclure ou exclure ceux-ci comme souhaité. Vous pouvez également modifier les noms des répertoires.

Dans le volet Scénario, sélectionnez un serveur de réplication. Pour chaque répertoire racine de l'ordinateur maître, vous devez spécifier un répertoire racine de l'ordinateur de réplication. Double-cliquez sur le dossier Répertoires pour le serveur de réplication. Comme souhaité, sélectionnez ou désélectionnez les cases à cocher situées en regard des dossiers qui doivent contenir le répertoire de l'ordinateur maître correspondant.

Paramètres de l'onglet Propriétés

Propriétés du scénario

Ces propriétés établissent le comportement par défaut de l'intégralité du scénario.

- Propriétés générales : ces propriétés ne peuvent plus être modifiées une fois créées.
- Propriétés de réplication : choisissez le mode de réplication (En ligne, Planifié ou Périodique), les valeurs de synchronisation (de niveau fichiers ou blocs, Ignorer les fichiers dont la taille et l'heure sont identiques) et les paramètres facultatifs (Réplication de l'attribut de compression NTFS, Réplication de la liste de contrôle d'accès NTFS, Synchronisation des partages Windows, Empêcher la resynchronisation automatique en cas d'erreur).
- Propriétés de notification d'événements : spécifiez un script à exécuter ou choisissez la notification par courriel.
- Gestion des rapports : spécifiez les paramètres des rapports, la distribution de courriel ou l'exécution d'un script.

Propriétés des hôtes maître et de réPLICATION

Ces paramètres établissent les propriétés des serveurs maître et de réPLICATION. Certains paramètres varient selon le type de serveur.

- Propriétés de connexion d'hôte : entrez l'adresse IP, ainsi que le numéro de port de l'ordinateur maître et celui de l'ordinateur de réPLICATION.
- Propriétés de réPLICATION : ces propriétés sont différentes pour l'ordinateur maître et l'ordinateur de réPLICATION. Pour plus d'informations, consultez le manuel d'administration de CA ARCserve RHA.
- Propriétés du spool : définissez la taille, l'espace disque minimum et le chemin d'accès au répertoire. Pour plus d'informations, reportez-vous à la section [Paramètres de répertoire du spool](#) (page 58).
- Propriétés de notification d'événements : spécifiez un script à exécuter ou choisissez la notification par courriel.
- Propriétés des rapports : choisissez des rapports de synchronisation ou de réPLICATION, spécifiez la distribution des rapports ou l'exécution d'un script.
- Tâches planifiées (ordinateur de réPLICATION) : définissez ou suspendez des tâches, notamment le Test d'intégrité de l'ordinateur de réPLICATION pour la récupération garantie. Pour plus de détails, reportez-vous au manuel d'administration de CA ARCserve RHA.
- Propriétés de récupération (ordinateur de réPLICATION) : définissez le délai ou les propriétés de retour arrière des données.

Paramètres de l'onglet Propriétés de haute disponibilité

Ces paramètres contrôlent l'exécution de la permutation et de la permutation inversée.

- Propriétés de la permutation : choisissez la permutation automatique ou manuelle, indiquez le nom d'hôte de permutation et les paramètres de réplication inversée.
- Propriétés des hôtes : spécifiez le nom complet des ordinateurs maître et de réplication.
- Propriétés de redirection du trafic réseau : choisissez Transfert IP, Redirection du système DNS, Permutation du nom de l'ordinateur ou Scripts définis par l'utilisateur.
- Propriétés d'activation : définissez la fréquence du signal d'activité et la méthode de vérification.
- Propriétés de gestion de base de données : ces propriétés indiquent à CA ARCserve RHA de gérer les partages ou les services sur un serveur de base de données.
- Propriétés d'action en cas de réussite : elles définissent les scripts personnalisés et les arguments à utiliser.

Exécution d'un scénario hors de l'assistant

Après avoir créé un scénario, exécutez-le pour démarrer le processus de réplication. Normalement, l'ordinateur maître et celui de réplication doivent être synchronisés avant que les changements de données survenant sur l'ordinateur maître puissent être répliqués. La première étape du démarrage d'une réplication consiste donc à synchroniser les serveurs maître et de réplication. Une fois ces serveurs synchronisés, une réplication en ligne démarre automatiquement et l'ordinateur de réplication est continuellement mis à jour avec tous les changements qui surviennent sur l'ordinateur maître.

Remarque : La réplication de points de montage est possible uniquement si ceux-ci ont été ajoutés à l'ordinateur maître avant le lancement du moteur. Si vous avez inclus les points de montage dans les répertoires racines de l'ordinateur maître alors que le moteur était déjà lancé, aucune erreur n'est signalée mais la réplication ne démarre pas. Dans ce cas, vous devez redémarrer le moteur sur l'ordinateur maître et sur l'ordinateur de réplication avant de lancer la réplication.

Remarque : Pour une réplication sans erreur, vérifiez que l'utilisateur qui exécute le moteur CA ARCserve RHA dispose des autorisations de lecture sur l'ordinateur maître et de lecture/écriture pour tous les répertoires racines de réplication et pour tous les fichiers qu'ils contiennent, sur tous les hôtes de réplication participants.

Pour exécuter un scénario hors de l'assistant :

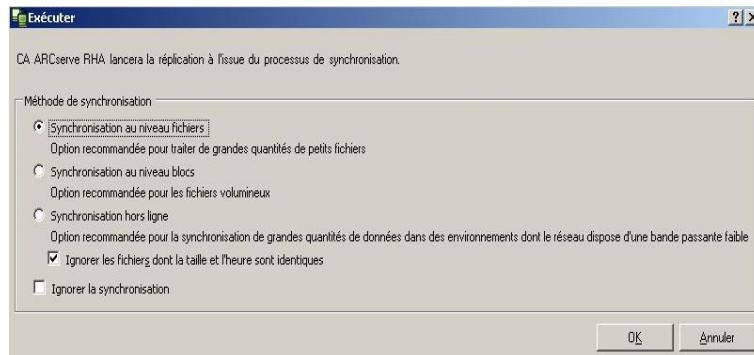
1. Dans le volet Scénario, sélectionnez le scénario à exécuter.
2. Cliquez sur Exécuter  dans la barre d'outils standard.

Avant de lancer la synchronisation et la réplication, CA ARCserve RHA vérifie la configuration de votre scénario. Lorsque la vérification s'achève, le gestionnaire CA ARCserve RHA affiche ce message : *Voulez-vous vraiment exécuter le scénario "nom_du_scénario" ?* En cas de détection de problèmes, le volet supérieur affiche les messages d'avertissement et d'erreur résultant de la vérification.

Remarque : La vérification de scénario contrôle plusieurs types de paramètres entre les serveurs maître et de réplication, pour garantir la permutation. Si des erreurs ou des avertissements sont signalés, vous ne devez pas continuer tant que les problèmes correspondants ne sont pas résolus.

3. Corrigez les erreurs avant de poursuivre. Les erreurs sont signalées dans le volet Événement.

Si aucune erreur n'est signalée, la boîte de dialogue Exécution apparaît et affiche les options de synchronisation.



Remarque : N'utilisez pas la fonction Ignorer la synchronisation pour tous les scénarios répliquant une base de données.

4. Pour réduire la durée de synchronisation, sélectionnez l'option Ignorer les fichiers dont la taille et l'heure sont identiques afin d'ignorer la comparaison des fichiers dont le chemin, le nom, la taille et l'heure de modification sont identiques, car ces fichiers sont généralement identiques.
5. Sélectionnez Ignorer la synchronisation uniquement si vous êtes certain que les fichiers sur l'ordinateur maître et sur l'ordinateurs de réPLICATION sont identiques.

Options sélectionnées par défaut : Synchronisation au niveau fichiers et Ignorer les fichiers dont la taille et l'heure sont identiques

6. Cliquez sur OK.

La synchronisation peut prendre quelques instants, selon la taille de la base de données et la bande passante du réseau entre l'ordinateur maître et celui de réPLICATION. Une fois la synchronisation terminée, le message suivant s'affiche dans la fenêtre des événements : *Toutes les modifications effectuées pendant la synchronisation ont été répliquées.*

A ce stade, le scénario est opérationnel et actif. Par défaut, un rapport de synchronisation est généré à la fin d'une synchronisation. Pour afficher ce rapport, reportez-vous à la rubrique Affichage d'un rapport. Vous pouvez également générer des rapports de réPLICATION réguliers afin de surveiller le processus de réPLICATION sur chaque serveur participant. Pour plus d'informations, reportez-vous au *Manuel d'administration de CA ARCserve RHA*.

Arrêt d'un scénario

Pour arrêter un scénario :

1. Dans le volet Scénario, sélectionnez le scénario que vous souhaitez arrêter.
2. Pour arrêter le scénario, cliquez sur le bouton  Arrêter de la barre d'outils standard.
Un message de confirmation apparaît, vous invitant à approuver l'arrêt du scénario.
3. Cliquez sur Oui dans le message de confirmation. Le scénario s'arrête.
Une fois le scénario arrêté, le gestionnaire n'affiche plus le symbole de lecture vert à gauche du scénario, l'état du ce scénario devient Arrêté par l'utilisateur et l'onglet Statistiques n'est plus disponible dans le volet Cadre d'applications.

Affichage d'un rapport

CA ARCserve RHA peut générer des rapports sur les processus de réplication et de synchronisation. Ces rapports peuvent être stockés à l'emplacement que vous souhaitez, ouverts pour affichage à partir du centre de rapports ou envoyés par courriel à une adresse indiquée ; ils peuvent également déclencher l'exécution d'un script.

Le répertoire de stockage par défaut des rapports générés est *[DossierFichiersProgrammes]\CA\ARCserve RHA\Manager\reports*

Pour afficher des rapports :

Remarque : Bien qu'un rapport Exchange soit présenté à des fins d'illustration, les étapes et les fenêtres sont similaires quel que soit le type de scénario.

1. Pour afficher des rapports, accédez au menu Outils, cliquez sur Rapports, puis sélectionnez Afficher les rapports de scénario.

Le centre de rapports s'affiche dans une nouvelle fenêtre.

Rapports disponibles par scénario							
Scénarios	Nom du scénario	Synchronisation	Comparaison	Réplication	Mode d'évaluation	Récupération garantie	Rapports
FullSystem		1	0	0	0	0	1
Exchange 2010		2	0	0	0	0	2
FileServer 2		1	0	0	0	0	1

Rapports						
Pour effectuer un regroupement par colonne, déplacez son en-tête ici.						
Hôte	Modifications	Date	Heure	Type	Récepteur(s)	Détailé
FileServer 3						

Le centre de rapports est constitué de deux tableaux.

- Le tableau supérieur intitulé Rapports disponibles par scénario, contient la liste de tous les scénarios comportant des rapports, ainsi que le type et le nombre de rapports disponibles pour chaque scénario.
- Le tableau inférieur, Rapports, contient la liste de tous les rapports disponibles pour le scénario sélectionné dans le tableau supérieur.

2. Pour afficher un rapport donné, sélectionnez dans le tableau Rapports disponibles par scénario le scénario représenté par ce rapport. Puis, dans le tableau Rapports situé en dessous, cliquez sur le rapport que vous souhaitez ouvrir.

Rapports							
Pour effectuer un regroupement par colonne, déplacez son en-tête ici.							
Hôte	Modifications	Date	Heure	Type	Récapitulatif	Détailé	Taille (octets)
10.50.48.227	Aucune modification n'a été effectuée.	Aujourd'hui	11:05:33	Synchronisation			1497

Remarque : Selon la configuration des paramètres des rapports de synchronisation et de réplication, un rapport détaillé peut être généré en plus du rapport récapitulatif. Ces deux rapports représentent le même processus, mais un rapport détaillé contient également la liste des fichiers ayant participé au processus.

Le rapport que vous avez sélectionné apparaît dans une nouvelle fenêtre.



The screenshot shows a report titled 'RAPPORT DE SYNCHRONISATION' for a scenario named 'Exchange 2010'. The report details the synchronization process between a master host ('localhost(1)') and a replication host ('155.35.75.128(2)'). The report was generated on 04/13/2010 at 00:44:50, and the synchronization mode is 'Synchronisation au niveau fichiers (ignorer les fichiers dont la taille et l'heure de modification sont identiques)'. The report table includes columns for Mode de synchronisation, Scénario, Hôte maître, Hôte de réplication, Heure de début du scénario, Heure de début du rapport, and Heure de fin du rapport.

Mode de synchronisation	Synchronisation au niveau fichiers (ignorer les fichiers dont la taille et l'heure de modification sont identiques)
Scénario	Exchange 2010
Hôte maître	localhost(1)
Hôte de réplication	155.35.75.128(2)
Heure de début du scénario	04/13/2010 00:44:50
Heure de début du rapport	04/13/2010 00:44:56
Heure de fin du rapport	04/13/2010 00:44:59

Chapitre 3 : Méthodes de redirection

Ce chapitre traite des sujets suivants :

- [Fonctionnement de la redirection](#) (page 25)
- [Redirection du système DNS](#) (page 25)
- [Redirection Transfert IP](#) (page 26)
- [Redirection Permutation du nom de l'ordinateur](#) (page 34)
- [Redirection par scripts](#) (page 35)

Fonctionnement de la redirection

Vous pouvez configurer chaque type de serveur pris en charge par CA ARCserve RHA pour utiliser une ou plusieurs méthodes de redirection. Vous devez activer les méthodes de redirection correspondant à votre environnement et répondant à vos besoins commerciaux. Les sections suivantes présentent en détail les méthodes de redirection prises en charge pour Microsoft IIS Server.

Redirection du système DNS

La redirection du système DNS modifie l'enregistrement "A" DNS du serveur maître pour résoudre l'adresse IP du serveur de réplication. En cas de défaillance du serveur maître, le serveur de réplication modifie l'enregistrement DNS approprié afin que les références au serveur maître soient résolues en l'adresse IP du serveur de réplication plutôt qu'en celle du maître. Cette méthode de redirection ne nécessite aucune reconfiguration du réseau et s'applique aux réseaux locaux (LAN) et étendus (WAN).

La redirection du système DNS fonctionne uniquement avec des enregistrements de type A (hôte) et ne peut pas mettre à jour les enregistrements CNAME (alias) directement. Toutefois, si un enregistrement CNAME pointe vers l'enregistrement A modifié, il est redirigé indirectement.

Par défaut, l'enregistrement comportant le nom du serveur maître est utilisé, mais vous pouvez configurer CA ARCserve RHA pour rediriger tout enregistrement A (hôte) DNS à l'aide du paramètre du *nom du maître dans DNS* dans l'onglet Propriétés de la permutation.

Redirection Transfert IP

La redirection Transfert IP implique le déplacement de l'adresse IP du serveur maître sur le serveur de réPLICATION.

Cette méthode de redirection est la méthode préférée pour les scénarios d'ordinateurs virtuels et elle est utilisable uniquement dans une configuration LAN où les serveurs maître et de réPLICATION se trouvent dans le même segment de réseau. Dans cette configuration, lorsque le serveur maître est permuted, le serveur de réPLICATION récupère une ou plusieurs des adresses IP attribuées au serveur maître.

Important : Utilisez cette méthode uniquement lorsque les deux serveurs se trouvent sur le même sous-réseau IP.

Si vous utilisez la méthode de redirection Transfert IP, vous devez d'abord ajouter les adresses IP à l'hôte maître. Pour plus d'informations, reportez-vous à la rubrique traitant de l'ajout d'une adresse IP sur le serveur maître.

Ajout d'une adresse IP sur le serveur maître

Pour utiliser la redirection Transfert IP dans les scénarios de haute disponibilité, vous devez ajouter une adresse IP supplémentaire à l'hôte maître (appelée *RHA-IP* dans les étapes suivantes). Cette nouvelle adresse IP est utilisée pour la communication interne de CA ARCserve RHA et pour la réPLICATION. Elle est nécessaire, car l'adresse IP de production actuelle n'est plus disponible sur l'ordinateur maître après permutation, elle passe au serveur de réPLICATION.

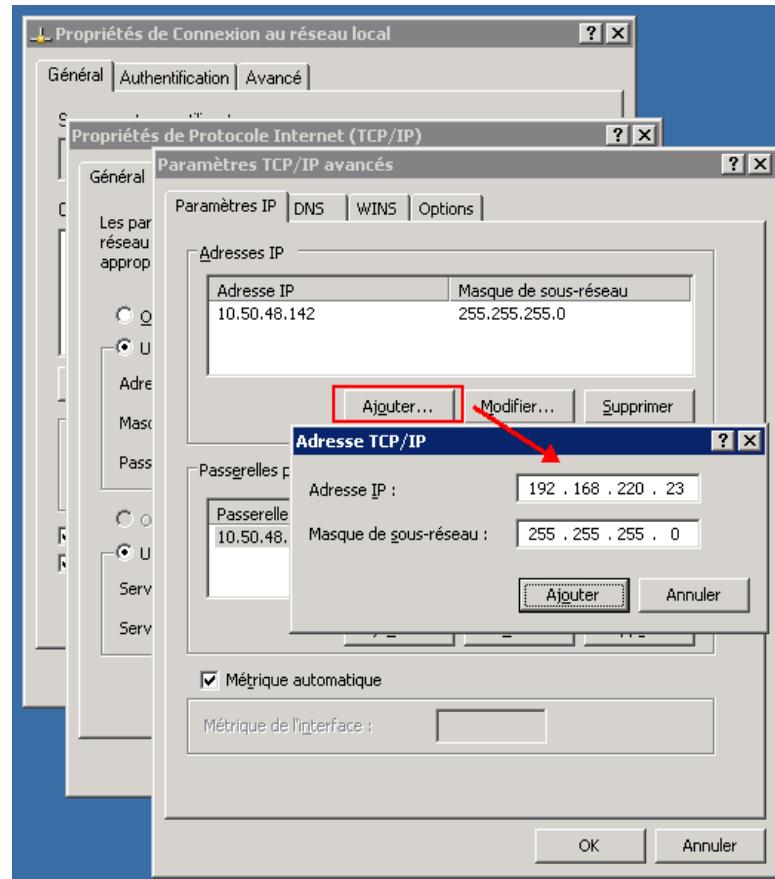
Important : Effectuez les opérations suivantes uniquement si vous utilisez la méthode de redirection Transfert IP.

Pour ajouter une adresse IP au serveur maître :

1. Ouvrez le Panneau de configuration et choisissez Connexions réseau.
2. Cliquez avec le bouton droit de la souris sur Réseau local, puis sélectionnez Propriétés.
3. Cliquez sur Protocole Internet (TCP/IP), puis cliquez sur le bouton Propriétés.
4. Cliquez sur Avancé.

5. Cliquez sur Ajouter et saisissez une adresse IP supplémentaire (RHA-IP).

Dans la capture de la fenêtre suivante, l'adresse RHA-IP est 192.168.220.23 et l'adresse IP du serveur de production actuel est 192.168.220.111.



6. Cliquez sur Ajouter.

7. Cliquez sur OK.

8. Cliquez sur OK pour quitter les paramètres LAN.

Après avoir ajouté l'adresse IP au serveur maître, vous devez ajouter l'adresse RHA-IP à vos scénarios de haute disponibilité. Deux méthodes sont possibles pour ajouter l'adresse XO-IP à un scénario de haute disponibilité :

- Pour les nouveaux scénarios, directement via l'assistant
- Pour les scénarios existants, en modifiant le nom d'hôte du serveur maître

Les deux procédures sont décrites ci-après.

Ajout de l'adresse RHA-IP à des scénarios existants

Effectuez cette procédure uniquement si vous utilisez la méthode de redirection Transfert IP.

Pour ajouter l'adresse RHA-IP à des scénarios existants

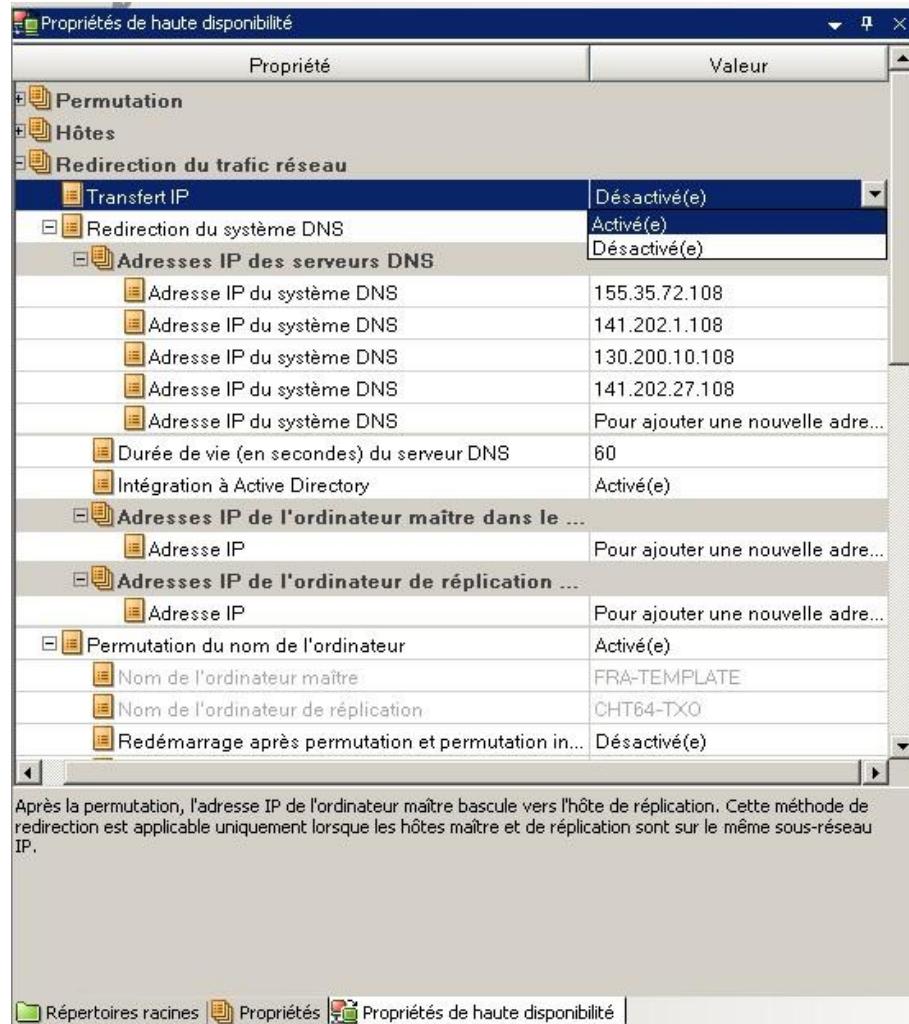
1. Dans le volet Scénario, sélectionnez l'hôte maître requis.



Scénario	Etat	Produit	Serveur	Mode
Exchange 2007	En cours d'exéc...	DR/Récupératio...	Exchange	Périodique
Hôtes	Modification	Données en...	Fichiers env...	Données reç...
localhost	0,00 octets	0,00 octets	0	-
155.35.75.128	0,00 octets	-	-	0,00 octets

2. Cliquez avec le bouton droit de la souris sur l'ordinateur maître et sélectionnez Renommer dans le menu contextuel. Entrez ensuite l'adresse RHA-IP.
3. Dans le volet Cadre d'applications, sélectionnez l'onglet Permutation, puis sélectionnez le serveur de réPLICATION comme hôte de permutation.

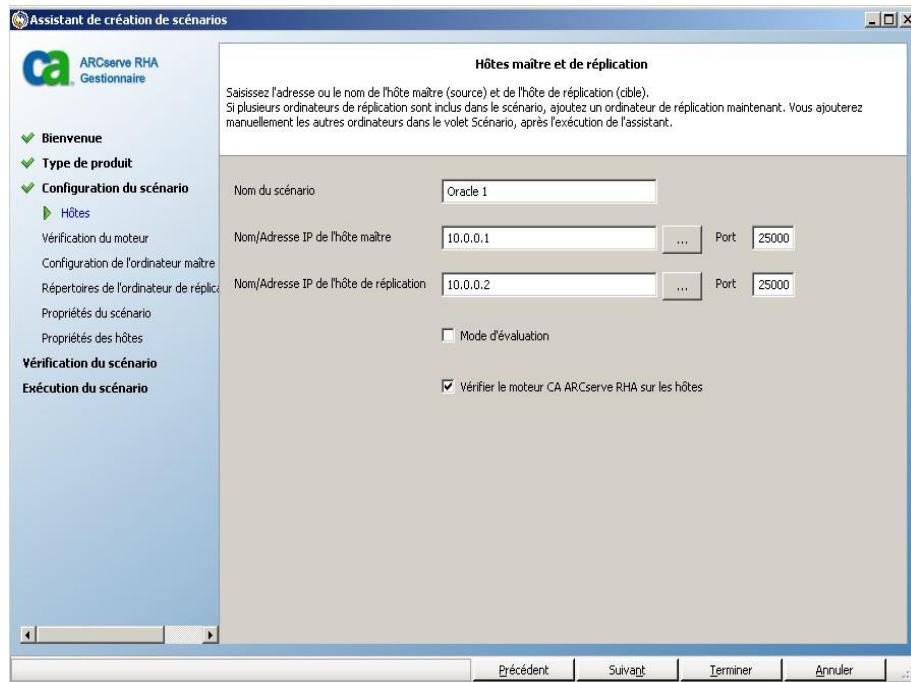
4. Définissez l'option Transfert IP sur Activé. Vérifiez que l'adresse IP sous *Transfert IP*, IP/Masque corresponde à l'adresse IP du serveur de production : il s'agit de l'adresse IP qui effectuera la permutation. Si vous transférez plusieurs adresses IP, vous pouvez ajouter plusieurs adresses IP de production en sélectionnant Pour ajouter une adresse IP ou un masque, cliquez ici.



Ajout de l'adresse RHA-IP à de nouveaux scénarios

Remarque : Effectuez cette procédure uniquement si vous utilisez la méthode de redirection Transfert IP.

Lors de la première exécution de l'assistant de création de scénario, au lieu des noms des serveurs, entrez les adresses IP RHA et du serveur de réplication dans les champs Nom/Adresse IP de l'hôte maître et Nom/Adresse IP de l'hôte de réplication.



Transfert IP de cluster

Cette section décrit la procédure de configuration de la méthode de redirection Transfert IP lors de l'utilisation de clusters.

Remarque : Si les ordinateurs maître et de réplication sont tous les deux des clusters, le processus de redirection Transfert IP présente certains problèmes de configuration qui ne sont pas détaillés dans ce manuel. Pour un scénario cluster-cluster, utilisez Redirection du système DNS ou contactez le support technique pour obtenir une assistance et des instructions détaillées.

Utilisation du cluster maître

Si vous souhaitez utiliser la redirection Transfert IP avec un maître en cluster (MSCS avec stockage partagé), ajoutez une ressource IP supplémentaire au groupe de ressources Exchange du cluster maître.

Pour utiliser le transfert IP de cluster via un cluster maître :

1. Ouvrez l'administrateur de cluster.
2. Dans le groupe de ressources Exchange du cluster maître, créez une nouvelle ressource IP et appelez-la **XO-IP**.
3. Placez cette ressource en ligne et vérifiez qu'elle est visible par l'ordinateur de réplication au moyen d'une commande ping.

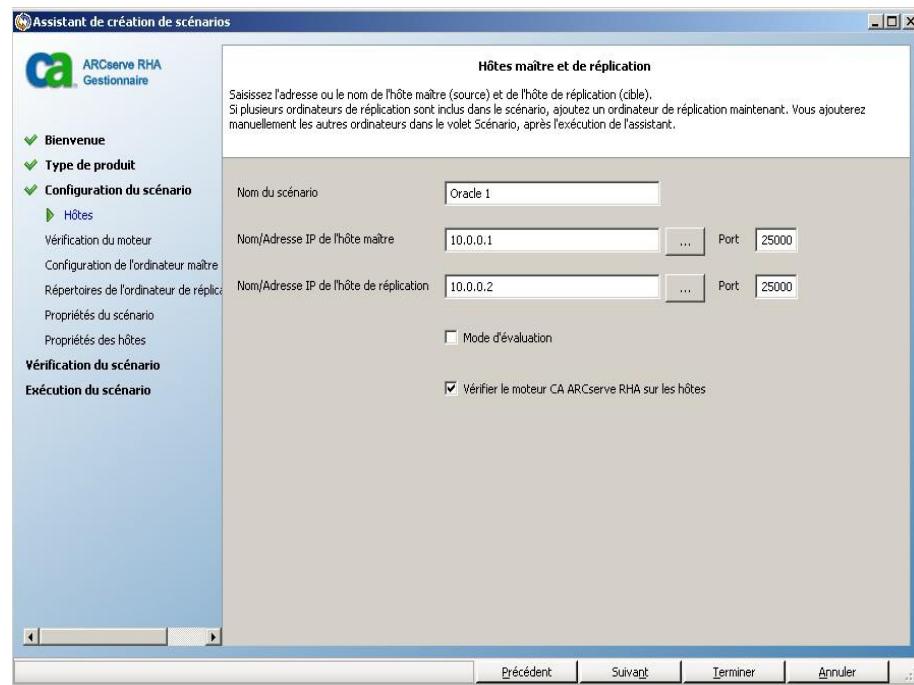
Cette nouvelle adresse IP est utilisée pour la communication interne de CA ARCserve RHA et pour la réplication. Elle est nécessaire, car l'adresse IP de production actuelle n'est pas disponible sur le cluster maître après permutation : elle passe au serveur de réplication.

Utilisation du gestionnaire

Cette section détaille la redirection Transfert IP de cluster au moyen du gestionnaire.

Nouveaux scénarios

Lors de l'exécution initiale de l'assistant, entrez l'adresse RHA-IP et l'adresse IP du serveur de réplication au lieu des noms des serveurs virtuels de cluster. L'illustration suivante présente l'adresse IP RHA saisie dans le champ Nom/Adresse IP de l'hôte maître et l'adresse IP du serveur de réplication saisie dans le champ Nom/Adresse IP de l'hôte de réplication.



Scénarios existants

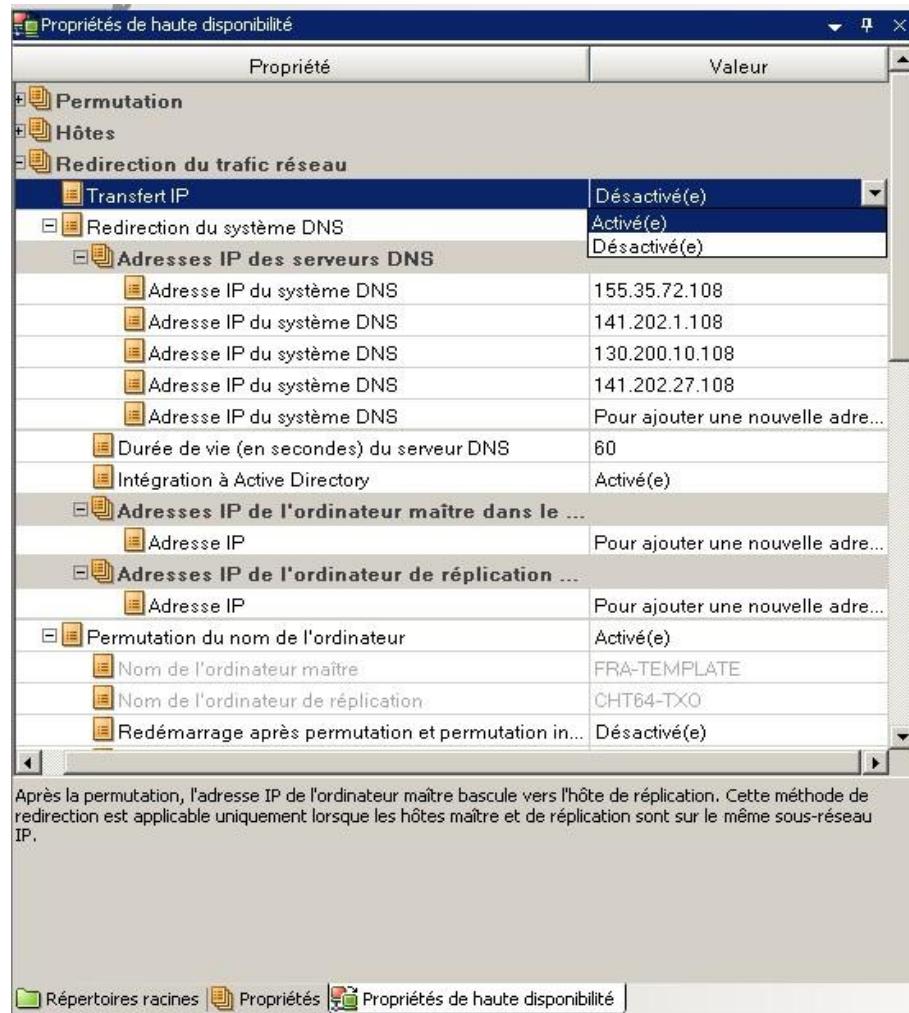
Pour utiliser le transfert IP de cluster avec des scénarios existants :

1. Dans le volet Scénario, sélectionnez l'hôte maître requis.

Vue du scénario						
Scénario	Etat	Produit	Serveur	Mode		
				En cours d'exéc...	DR/Récupératio...	Exchange
Exchange 2007	En cours d'exéc...	DR/Récupératio...	Exchange	Périodique		
	Hôtes	Modification	Données en...	Fichiers env...	Données reç...	Fichiers reçus
	localhost	0,00 octets	0,00 octets	0	-	-
	155.35.75.128	0,00 octets	-	-	0,00 octets	0,00 octet

2. Cliquez avec le bouton droit de la souris sur l'ordinateur maître et sélectionnez Renommer dans le menu contextuel. Entrez ensuite l'adresse RHA-IP.
3. Dans le volet Cadre d'applications, sélectionnez l'onglet Permutation, puis sélectionnez le serveur de réplication comme hôte de permutation.

4. Définissez l'option Transfert IP sur Activé. Vérifiez que l'adresse IP sous Move IP, IP/Masque corresponde à l'adresse IP de serveur de production.



Il s'agit de l'adresse IP vers laquelle l'ordinateur maître effectuera la permutation. Si vous transférez plusieurs adresses IP, vous pouvez ajouter plusieurs adresses IP de production en sélectionnant Pour ajouter une adresse IP ou un masque, cliquez ici.

Redirection Permutation du nom de l'ordinateur

Si vous redirigez des partages de fichiers auxquels les clients se connectent via le nom du serveur maître, activez l'option de permutation du nom de l'ordinateur. Par exemple, si le serveur maître s'appelle fs01 et que les clients se connectent à \\fs01\nom_partage ou à \\fs01.domain.com\nom_partage, la méthode Permutation du nom de l'ordinateur redirige les clients vers le serveur de basculement. Pour utiliser la Redirection par permutation du nom de l'ordinateur, les ordinateurs maître et de réplication doivent appartenir au même domaine.

Ceci est également recommandé pour l'activation d'une autre méthode. La méthode la plus courante est l'utilisation associée de Redirection du système DNS et de Permutation du nom de l'ordinateur. CA ARCserve RHA permute le nom de l'ordinateur requis en attribuant un nom temporaire au serveur maître et en récupérant son nom d'ordinateur initial pour l'utiliser avec le serveur de réplication.

CA ARCserve RHA met directement à jour les enregistrements et en général, aucun redémarrage n'est nécessaire. Toutefois, si des problèmes surviennent après une permutation, vous devez envisager de définir l'option Redémarrage sur Activé et tester à nouveau.

Remarque : Pour les systèmes Windows Server 2008, redémarrez l'ordinateur après une permutation lorsque la méthode de permutation du nom de l'ordinateur est utilisée. Nous vous recommandons d'activer la propriété Redémarrage après permutation et permutation inversée lorsque vous utilisez cette méthode.

Redirection automatique par permutation du nom de l'ordinateur

Si cela est possible lors de la permutation, CA ARCserve RHA remplace le nom de l'hôte maître par *nom_hôte_maître-RHA* et attribue son nom d'origine au serveur de réplication. Cette étape permet d'éviter les conflits de noms, car le nom du maître est alors attribué au serveur de réplication. Dans ce cas idéal, si la réplication inversée automatique est activée, CA ARCserve RHA démarre automatiquement le scénario arrière. Si elle est désactivée, exécutez à nouveau le scénario manuellement en cliquant sur le bouton Exécuter ou en sélectionnant Exécuter dans le menu Outils. Un fois le scénario arrière exécuté et la synchronisation terminée, vous pouvez cliquer sur le bouton Effectuer la permutation pour effectuer la permutation inversée.

Redirection par scripts

CA ARCserve RHA peut déclencher des scripts ou des fichiers de commandes personnalisés pour rediriger les utilisateurs ou pour toute étape supplémentaire non effectuée par les méthodes intégrées. Si les méthodes décrites ci-dessus ne sont pas appropriées ou ne répondent pas intégralement à tous vos besoins, reportez-vous au *Manuel d'administration de CA ARCserve RHA* pour obtenir plus de détails sur les méthodes de redirection par scripts.

Chapitre 4 : Permutation et permutation inversée

La *permutation* et la *permutation inversée* forment le processus au cours duquel les rôles passif et actif sont échangés entre les serveurs maître et de réplication. Ainsi, si le serveur maître est actuellement actif, il devient passif une fois que la permutation a rendu le serveur de réplication actif.

Inversement, si le serveur de réplication est actif, il devient passif une fois que la permutation a rendu le serveur maître actif. Si l'option Permutation automatique de la boîte de dialogue Démarrage de la permutation et de la réplication inversée est activée, la permutation peut être déclenchée en cliquant sur un bouton ou de manière automatique par CA ARCserve RHA, s'il détecte que l'hôte maître n'est pas disponible. Si cette option est désactivée, le système vous signale que le serveur maître est arrêté et vous pourrez alors démarrer manuellement la permutation à partir du gestionnaire CA ARCserve RHA.

Ce chapitre traite des sujets suivants :

[Fonctionnement de la permutation et de la permutation inversée](#) (page 37)

[Démarrage d'une permutation](#) (page 39)

[Démarrage d'une permutation inversée](#) (page 41)

[Considérations sur la permutation](#) (page 44)

Fonctionnement de la permutation et de la permutation inversée

Lorsque le scénario de haute disponibilité s'exécute et que le processus de synchronisation est terminé, l'ordinateur de réplication vérifie régulièrement l'ordinateur maître, par défaut toutes les 30 secondes, pour voir s'il est actif. Les différents types de vérifications de surveillance sont disponibles.

- Ping--demande envoyée à l'ordinateur maître pour vérifier qu'il fonctionne et qu'il répond.
- Vérification de la base de données--demande vérifiant que les services appropriés fonctionnent et que toutes les bases de données sont montées
- Vérification définie par l'utilisateur--demande que vous pouvez personnaliser pour surveiller des applications spécifiques

Si une erreur survient dans l'une des parties de cet ensemble, l'ordinateur de réPLICATION considère que toute la vérification est en échec. Si toutes les vérifications sont en échec durant une période de temporisation configurée (5 minutes par défaut), le serveur maître est considéré comme arrêté. Ainsi, selon la configuration du scénario haute disponibilité, CA ARCserve RHA vous envoie une alerte ou lance automatiquement une permutation.

Lorsque vous avez créé un scénario de haute disponibilité, vous avez défini le mode de démarrage de la permutation.

- Si vous avez sélectionné l'option de permutation manuelle dans la page Démarrage de la permutation et de la réPLICATION inversée, vous devez effectuer une permutation manuelle. Pour plus d'informations, reportez-vous à la rubrique [Démarrage d'une permutation](#) (page 39).
- Si vous avez sélectionné l'option de permutation automatique, vous pouvez tout de même effectuer une permutation manuelle, même si l'ordinateur maître est actif. Vous pouvez démarrer une permutation si vous souhaitez tester votre système ou si vous souhaitez utiliser le serveur de réPLICATION pour continuer le service d'application pendant une opération de maintenance sur le serveur maître. Une permutation déclenchée (automatique) est en tout point identique à une permutation manuelle effectuée par l'administrateur, à l'exception du fait qu'elle est déclenchée par la défaillance d'une ressource sur le serveur maître et non par un administrateur qui lance la permutation manuellement en cliquant sur le bouton Effectuer la permutation. Les paramètres de temporisation sont configurables et évoqués plus en détails dans le *Manuel d'administration de CA ARCserve RHA*.

Lorsque vous avez créé un scénario de haute disponibilité, vous avez défini le mode de démarrage du scénario inverse.

- Si vous avez sélectionné l'option Démarrer automatiquement la réPLICATION inversée dans la page Démarrage de la permutation et de la réPLICATION inversée, la réPLICATION inversée (de l'ordinateur de réPLICATION vers l'ordinateur maître) démarre automatiquement une fois la permutation achevée.
- Si vous avez sélectionné l'option Démarrer manuellement la réPLICATION inversée, vous devez resynchroniser les données de l'ordinateur de réPLICATION vers l'ordinateur maître, même en cas de test d'une permutation "propre", sans défaillance de l'ordinateur maître.

Lorsque la fonctionnalité RéPLICATION inversée est désactivée, vous devez cliquer sur le bouton Exécuter, après une permutation, pour démarrer la réPLICATION inversée. Cette fonctionnalité présente un avantage si les serveurs maître et de réPLICATION sont en ligne et connectés pendant une permutation, car la resynchronisation en sens inverse n'est alors pas requise. En effet, la resynchronisation nécessite la comparaison des données sur les serveurs maître et de réPLICATION, afin de déterminer les modifications à transférer avant le démarrage de la réPLICATION en temps réel ; cela peut prendre un certain temps. Si la réPLICATION inversée automatique est activée et si les deux serveurs sont en ligne pendant une permutation, la réPLICATION est inversée sans qu'une resynchronisation ne soit nécessaire. Il s'agit du seul cas où la resynchronisation n'est pas requise.

Démarrage d'une permutation

Une fois déclenché, manuellement ou automatiquement, le processus de permutation est entièrement automatisé.

Remarque : Les étapes suivantes donnent des fenêtres de scénarios Exchange pour exemple. Cependant, la procédure est similaire pour tous les types de serveurs.

Pour démarrer une permutation manuelle

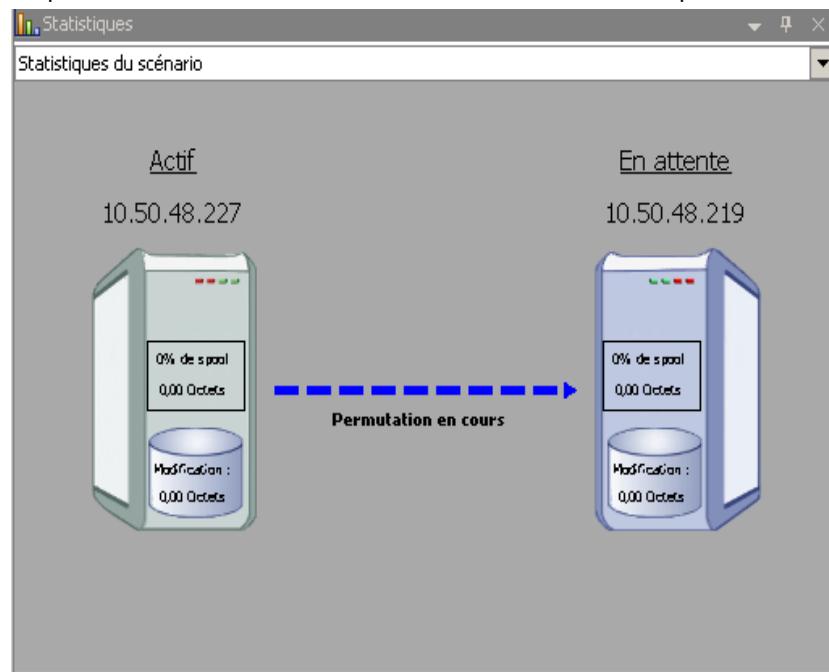
1. Lancez le gestionnaire et sélectionnez le scénario souhaité dans le volet Scénario. Vérifiez qu'il est en cours d'exécution.
2. Cliquez sur Effectuer la permutation.



Un message de confirmation s'affiche.

3. Cliquez sur OK.

La permutation du serveur maître vers le serveur de réPLICATION est lancée.



Au cours de la permutation, des informations détaillées sur les processus de permutation sont disponibles dans le volet Événements.

Une fois la permutation terminée, le scénario s'arrête.

Scénario	Etat	Produit	Serveur	Mode
MS Exchange HA	Arrêté par l... HA	Exchange	En ligne	

Remarque : L'exécution du scénario peut se poursuivre après la permutation uniquement si la réPLICATION inversée automatique est définie sur Démarrer automatiquement.

Un message apparaît dans le volet Événements, indiquant que la permutation est terminée et que le scénario est arrêté.

L'ordinateur maître devient alors le serveur en attente et l'ordinateur de réPLICATION devient le serveur actif.

Démarrage d'une permutation inversée

A la suite d'une permutation, manuelle ou automatique, vous pourrez inverser les rôles des serveurs afin que l'ordinateur maître d'origine redevienne le serveur actif et que l'ordinateur de réPLICATION redevienne le serveur en attente. Avant d'effectuer une permutation inversée des rôles entre les serveurs, indiquez si vous souhaitez remplacer les données sur le serveur maître d'origine avec les données du serveur de réPLICATION d'origine. Si vous souhaitez écraser les données du serveur maître d'origine, vous devez d'abord effectuer un scénario inverse, appelé scénario arrière.

Remarque : Les étapes ci-dessous sont identiques, quel que soit le type de serveur.

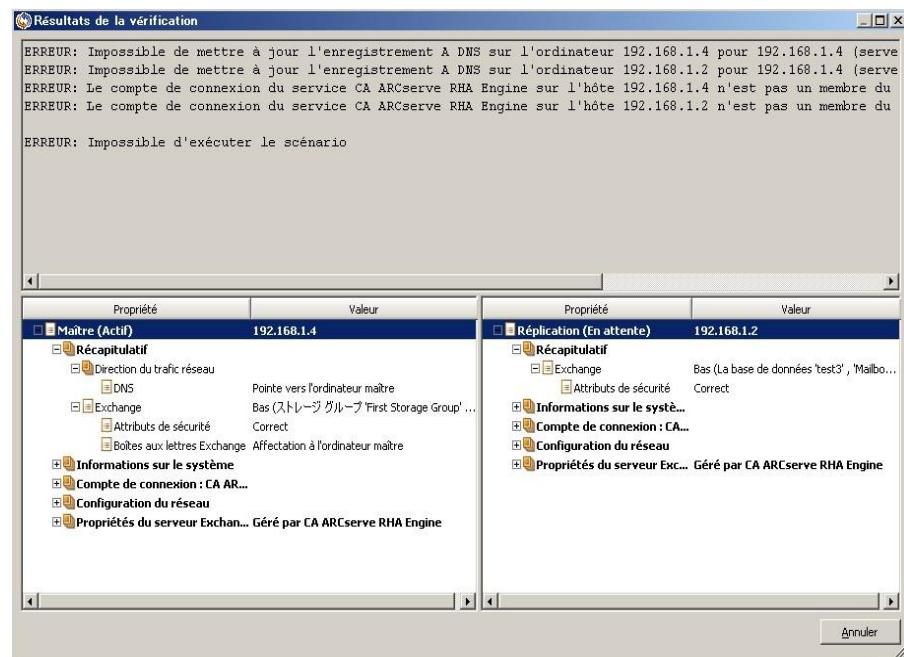
Pour démarrer une permutation inversée manuelle

1. Vérifiez que les serveurs maître et de réPLICATION sont disponibles sur le réseau et que le moteur est en cours d'exécution.
2. Lancez le gestionnaire et sélectionnez le scénario souhaité dans le volet Scénario.

3. Effectuez l'une des opérations suivantes.

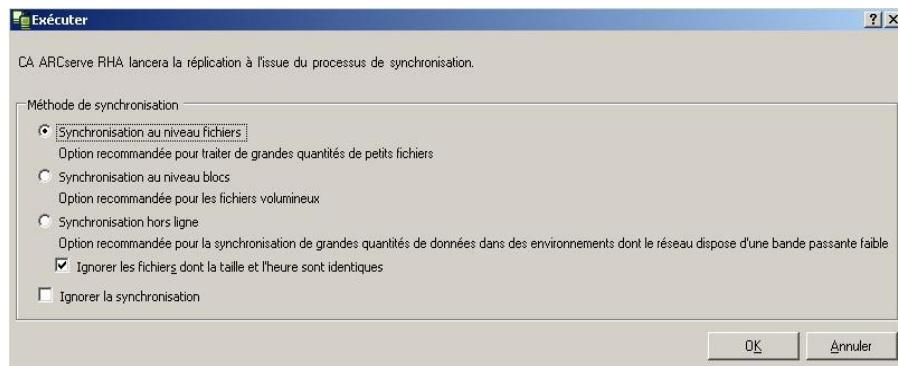
- Si le scénario est déjà en cours d'exécution, passez directement à l'étape 4.
- Si le scénario ne s'exécute pas, effectuez les étapes ci-dessous, puis passez à l'étape 4.
 - a. Dans la barre d'outils, cliquez sur Exécuter pour démarrer le scénario.

CA ARCserve RHA détecte qu'une permutation a eu lieu et vérifie son état et sa configuration. Une fois la vérification terminée, la boîte de dialogue Résultats de la vérification apparaît, répertoriant les erreurs et avertissements existants détectés et vous invitant à approuver l'exécution du scénario arrière. Si vous le souhaitez, cliquez sur le bouton Avancé pour ouvrir un volet supplémentaire contenant des informations détaillées sur les hôtes qui participent au scénario.

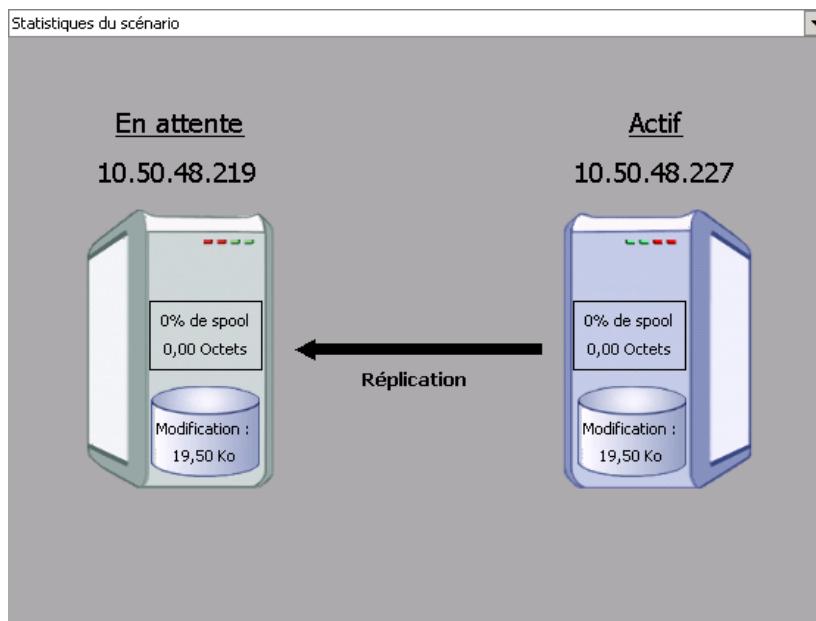


- b. Sélectionnez une méthode de synchronisation dans la boîte de dialogue Exécution, puis cliquez sur OK pour démarrer la resynchronisation.

Remarque : Pour plus d'informations sur les méthodes de synchronisation, consultez le *Manuel d'administration de CA ARCserve RHA*.



Une fois la resynchronisation terminée, le message suivant s'affiche dans le volet Événement : Toutes les modifications effectuées pendant la synchronisation ont été répliquées. La réplication du serveur actif sur le serveur en attente démarre.



Remarque : Vous êtes désormais prêt à effectuer une permutation inversée des rôles entre les serveurs maître et de réplication.

4. Pour effectuer une permutation inversée des rôles de serveurs, cliquez sur Effectuer la permutation, dans la barre d'outils, alors que le scénario s'exécute. Un message de confirmation s'affiche.

5. Cliquez sur Oui pour effacer le message et démarrer le processus de permutation inversée.

Une fois la permutation inversée terminée, les rôles des serveurs reviennent aux rôles d'origine et le scénario s'arrête automatiquement.

Remarque : l'exécution du scénario se poursuit après la permutation inversée si l'option Lancement de la réplication inversée est définie sur Démarrer automatiquement.

Vous pouvez à présent exécuter à nouveau le scénario dans son état d'origine (scénario avant).

Considérations sur la permutation

Pour empêcher l'écrasement de données, il est recommandé de définir *soit* la propriété de permutation, *soit* la propriété de démarrage de la réplication inversée sur Automatique. Si un serveur échoue alors que les deux propriétés sont définies sur Automatique, CA ARCserve RHA déclenche la permutation sans impliquer l'administrateur et peut lancer la réplication inversée avant de rechercher la cause de l'échec. Au cours de la réplication inversée, CA ARCserve RHA écrase des données sur votre serveur de production.

En cas d'arrêt brutal ou d'interruption lors de la permutation, vous devrez peut-être lancer la procédure de [réécriture du serveur actif](#) (page 58).

Chapitre 5 : Récupération de données

Ce chapitre traite des sujets suivants :

[Processus de récupération des données](#) (page 45)

[Définition de repères](#) (page 45)

[Retour arrière des données](#) (page 47)

[Boîte de dialogue Sélection d'un point de retour arrière](#) (page 52)

[Récupération de données perdues à partir du serveur de réPLICATION](#) (page 54)

[Récupération du serveur actif](#) (page 55)

Processus de récupération des données

Lorsqu'un événement cause une perte de données sur l'ordinateur maître, les données peuvent être restaurées à partir de tout serveur de réPLICATION. Le processus de récupération est en fait un processus de synchronisation de direction inverse, c'est-à-dire de l'ordinateur de réPLICATION à l'ordinateur maître.

CA ARCserve RHA permet de récupérer des données de deux manières.

- **Récupérer les données perdues de l'ordinateur de réPLICATION vers l'ordinateur maître** : cette option consiste en un processus de synchronisation dans le sens inverse, pour lequel vous devez arrêter le scénario (déconseillée pour les scénarios Oracle, SQL ou Exchange).
- **Récupération des données perdues à partir d'un événement ou d'un point dans le temps spécifique (retour arrière des données)** : cette option utilise des points de contrôle horodatés et des repères définis par l'utilisateur pour ramener les données endommagées sur l'ordinateur maître à un moment antérieur à l'endommagement.

Important : Vous devez arrêter la réPLICATION avant de lancer la récupération.

Définition de repères

Un *repère* est un point de contrôle qui est manuellement défini pour marquer un état antérieur que vous pouvez réutiliser. Nous vous recommandons de définir un repère avant toute activité pouvant entraîner l'instabilité des données. Les repères sont définis en temps réel, ils ne s'appliquent pas aux événements antérieurs.

Remarques :

- Utilisez cette option uniquement si vous définissez l'option *Récupération - Retour arrière des données* sur *Activé(e)* (le paramètre par défaut est *Désactivé(e)*).
- Vous ne pouvez pas définir de repères pendant le processus de synchronisation.

Pour définir un repère :

1. Sélectionnez l'hôte de réPLICATION dans le volet Scénario qui vous permettra d'effectuer le retour arrière des données lors de l'exécution du scénario requis.
2. Sélectionnez le repère de retour arrière dans le menu Outils.

La boîte de dialogue Repère de retour arrière s'affiche.



Le texte affiché dans la boîte de dialogue Repère de retour arrière est utilisé comme nom du repère dans la boîte de dialogue de sélection des points de retour arrière. Le nom par défaut comporte la date et l'heure.

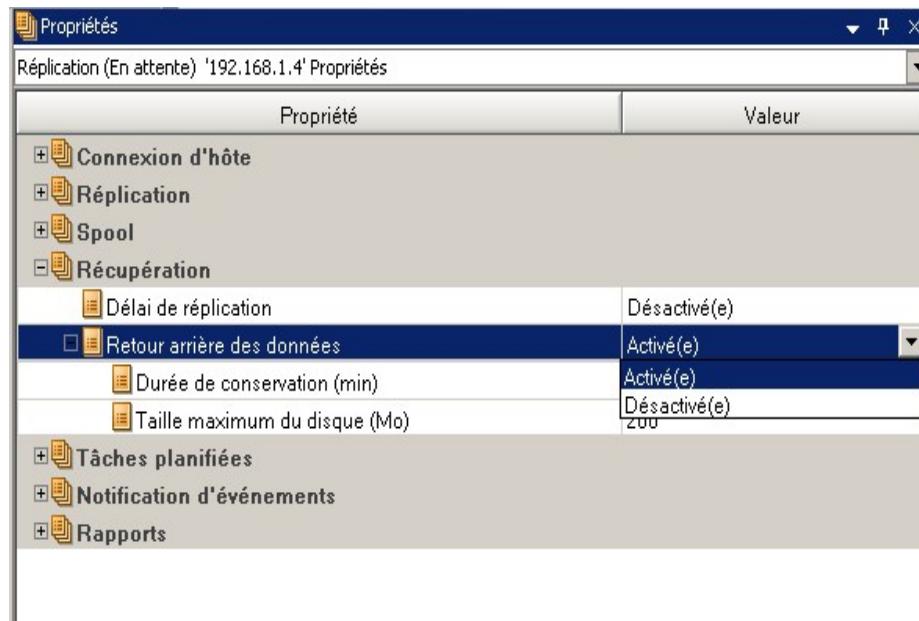
3. Acceptez le nom de repère par défaut ou entrez un nom explicite, et cliquez sur OK.

Le repère est défini.

Retour arrière des données

La méthode de récupération par retour arrière des données vous permet de récupérer les données telles qu'elles étaient à un point dans le temps antérieur à leur endommagement. Le processus de retour arrière a lieu sur le serveur de réplication, avant le démarrage du processus de synchronisation inverse. Cette méthode utilise des points de retour arrière ou des repères qui vous permettent de rétablir un état antérieur des données.

Vous pouvez utiliser cette possibilité uniquement si vous activez l'option Retour arrière des données dans les propriétés de récupération.



Si vous définissez cette option sur Désactivé(e), CA ARCserve RHA n'enregistrera pas de points de retour arrière des données. Pour plus d'informations sur les paramètres de retour arrière des données (durée de conservation, taille maximum du disque), reportez-vous au *Manuel d'administration*.

Remarque : L'enregistrement automatique des points de retour arrière démarre uniquement à l'issue du processus de synchronisation et le message suivant apparaît dans le volet Événement : Toutes les modifications effectuées pendant la synchronisation ont été répliquées. De même, vous ne pouvez pas définir de repères manuellement pendant la synchronisation. L'exemple ci-dessous repose sur un scénario de serveur de fichiers, mais les étapes sont identiques pour tous les types de scénarios.

Informations complémentaires :

[Boîte de dialogue Sélection d'un point de retour arrière \(page 52\)](#)

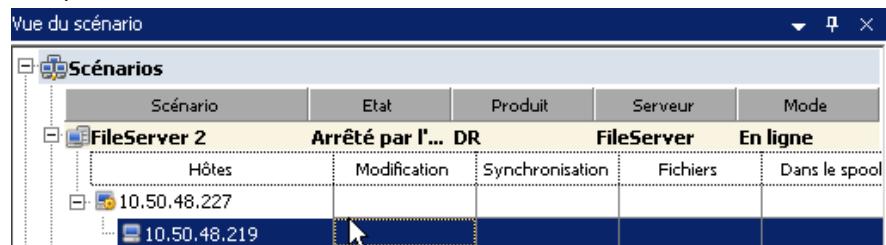
Retour arrière des données

Important : Le processus de retour arrière des données fonctionne dans un seul sens. Le retour avant est impossible. Une fois le retour arrière terminé, toutes les données postérieures au point de retour arrière sont perdues, car les données modifiées après ce point sont écrasées par de nouvelles données.

Pour récupérer des données perdues à l'aide de points de retour arrière

1. Dans le gestionnaire, utilisez le volet Scénario pour sélectionner le scénario souhaité et l'arrêter.
2. Arrêtez les services de base de données sur l'hôte maître (pour les applications de bases de données uniquement).
3. Dans le gestionnaire, sélectionnez l'hôte de réPLICATION dans le dossier des scénarios.

Remarque : Si plusieurs serveurs de réPLICATION participent au scénario requis, sélectionnez la réPLICATION à partir de laquelle vous souhaitez récupérer les données.



Scénario	Etat	Produit	Serveur	Mode
FileServer 2	Arrêté par l'... DR		FileServer	En ligne
	Hôtes	Modification	Synchronisation	Fichiers
	10.50.48.227			Dans le spool
	10.50.48.219			

4. Cliquez sur Outils, puis sur Restaurer les données. Si nécessaire, saisissez les informations d'identification de l'utilisateur, puis cliquez sur OK.
- La page Méthode de récupération de l'assistant de restauration des données s'ouvre.

5. Sélectionnez l'une des options de retour arrière des données : vous pouvez laisser les données récupérées sur l'ordinateur de réPLICATION uniquement (option 3) ou synchroniser les données de l'ordinateur maître avec ces données (option 2).

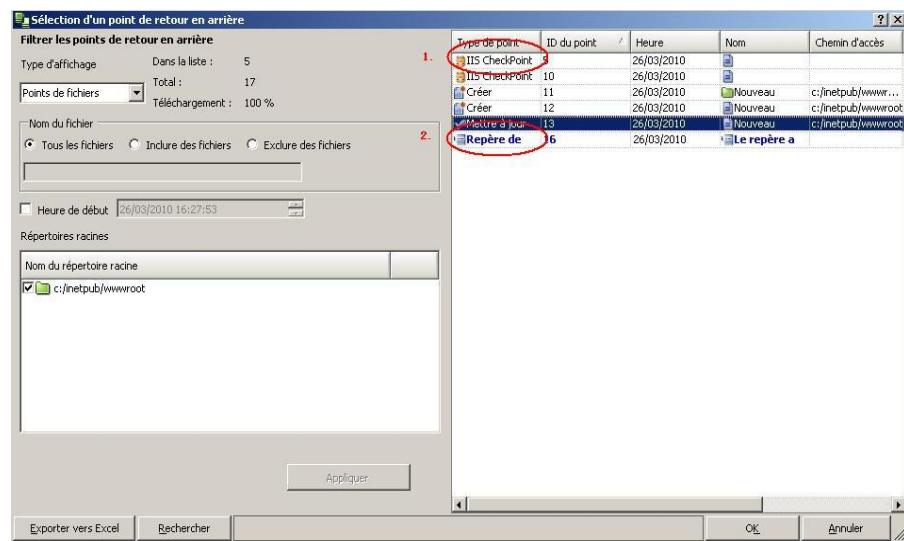
Remarques :

- Si les informations d'identification de l'utilisateur que vous avez utilisées pour vous connecter au gestionnaire sont différentes de celles requises pour utiliser le moteur sur l'ordinateur de réPLICATION, la boîte de dialogue Informations d'identification de l'utilisateur qui s'affiche vous invite à saisir les informations du compte de connexion pour l'ordinateur de réPLICATION sélectionné.
- La case à cocher Inclure la synchronisation des clés de registre est disponible uniquement si vous avez activé cette option avant de démarrer le scénario. Si la case à cocher est disponible, vous pouvez la sélectionner pour inclure les clés de registre synchronisées dans le processus de récupération.

Après avoir sélectionné une option de retour arrière des données, un scénario de récupération est créé automatiquement. Ce scénario de récupération s'exécutera jusqu'à la fin du processus de retour arrière.

6. Cliquez sur Suivant.
- La fenêtre Sélection d'un point de retour arrière s'ouvre.
7. Cliquez sur Sélectionner un point de retour arrière, si cette option est activée.

La boîte de dialogue Sélection d'un point de retour arrière s'affiche.



Cette boîte de dialogue affiche la liste de tous les points de retour arrière. Ceux-ci incluent des modifications de dossiers et des fichiers que CA ARCserve RHA enregistre automatiquement et les repères que vous avez définis.

Vous pouvez filtrer cette liste selon le type de point de retour arrière ou selon d'autres critères, au moyen du volet Filtrer les points de retour arrière situé sur la gauche.

8. Sélectionnez le point de retour arrière requis, puis cliquez sur OK.

Remarque : Si vous souhaitez utiliser un repère comme point de retour arrière, nous vous conseillons de sélectionner le point de retour arrière le plus proche qui indique un événement réel.

La fenêtre Sélection de point de retour arrière s'affiche. Elle contient les informations relatives au point de retour arrière sélectionné.

9. Cliquez sur Suivant.

La fenêtre Méthode de synchronisation s'ouvre.

10. Sélectionnez la méthode Synchronisation au niveau blocs, puis cliquez sur Terminer.

Remarque : Si les informations d'identification de l'utilisateur que vous avez utilisées pour vous connecter au gestionnaire sont différentes de celles requises pour utiliser le moteur sur l'ordinateur de réplication, la boîte de dialogue Informations d'identification de l'utilisateur qui s'affiche. Vous pouvez alors entrer les informations du compte de connexion pour l'ordinateur de réplication sélectionné.

CA ARCserve RHA effectue le retour arrière des données jusqu'au point sélectionné. A l'issus du retour arrière, le message suivant apparaît dans le volet Événement : Le processus de retour arrière est terminé.

Si vous choisissez de remplacer les données de l'ordinateur maître par les données de réplication, CA ARCserve RHA lance un processus de synchronisation des données de l'ordinateur maître avec les données de l'ordinateur de réplication. Une fois la synchronisation terminée, le scénario de récupération temporaire est arrêté, puis supprimé.

Le rapport de synchronisation est généré.

Le processus de réplication peut alors redémarrer conformément au scénario d'origine.

Boîte de dialogue Sélection d'un point de retour arrière

Cette boîte de dialogue contient la liste de tous les points de retour arrière pour IIS. Ceux-ci incluent des modifications de dossiers et des fichiers que CA ARCserve RHA enregistre automatiquement et les repères que vous avez définis.

La volet gauche contient les sections suivantes :

Filtrer les points de retour arrière

Permet de sélectionner un type spécifique de point de retour arrière et contient les statistiques d'affichage correspondantes. Les statistiques sont présentées de la façon suivante :

- Dans la liste : nombre de types de points disponibles dans la liste sélectionnée. Ces types de points sont affichés dans le volet droit.
- Total : nombre total de points dans le type sélectionné de points de retour arrière.
- Téléchargement : pourcentage de téléchargement des types de point sélectionnés.

Nom du fichier

Indique les types de fichiers dont l'état doit être récupéré. Pour inclure ou exclure des fichiers spécifiques, sélectionnez le bouton d'option correspondant et introduisez le nom dans la zone située dessous.

Heure de début

Indique l'heure de début du processus de retour arrière. Activez la case à cocher pour modifier l'heure de début.

Nom du répertoire racine

Indique les répertoires racines qui ont été inclus dans le processus de retour arrière. Tous les répertoires sont sélectionnés. Pour exclure un répertoire, désactivez la case à cocher et cliquez sur Appliquer.

Les champs suivants sont affichés dans le volet droit :

Type de point

Indique le type de point : IIS Checkpoint, événement de fichier ou repère défini par l'utilisateur. IIS Checkpoint est défini par le point de fermeture du métafichier après modification. La présence de l'icône dans cette colonne indique que les métadonnées IIS ont été modifiées. Le métafichier est mis à jour sur l'ordinateur de réplication toutes les 30 secondes. Si vous changez des paramètres sur l'ordinateur maître et lancez une récupération juste après, il se peut que les dernières mises à jour n'apparaissent pas sur l'ordinateur de réplication.

ID du point

Indique l'ID du point.

Heure

Indique l'heure d'exécution du retour arrière indiquée par le système.

Nom

Indique le nom du point de contrôle.

Récupération de données perdues à partir du serveur de réPLICATION

La procédure qui suit est identique pour tous les types de serveurs.

Pour récupérer toutes les données perdues à partir d'un ordinateur de réPLICATION :

1. Dans le volet Scénario du gestionnaire, sélectionnez le scénario souhaité et arrêtez-le.
2. (Pour les applications de bases de données uniquement) Arrêtez les services de base de données sur l'hôte maître.
3. Dans le gestionnaire, sélectionnez l'hôte de réPLICATION dans le dossier du scénario. Si plusieurs ordinateurs de réPLICATION participent à un scénario, sélectionnez celui à partir duquel vous souhaitez récupérer les données. L'option Restaurer les données est alors activée.
4. Dans le menu Outils, sélectionnez Restaurer les données ou cliquez sur Restaurer les données dans la barre d'outils standard.

Remarque : Si les informations d'identification de l'utilisateur que vous avez utilisées pour vous connecter au gestionnaire sont différentes de celles requises pour utiliser le moteur sur l'ordinateur de réPLICATION, la boîte de dialogue Informations d'identification de l'utilisateur qui s'affiche vous invite à saisir les informations du compte de connexion pour l'ordinateur de réPLICATION sélectionné.

La page Méthode de récupération de l'assistant de restauration des données apparaît.

Remarque : Si la propriété Retour arrière des données est activée, une autre boîte de dialogue Restauration des données apparaît. Dans ce cas, sélectionnez la première option : Remplacer toutes les données du maître par les données de réPLICATION. Cette option restaure simplement les données, sans retour arrière.

5. Cliquez sur Suivant.

La page Méthode de synchronisation s'affiche.

6. Assurez-vous que la bonne Méthode de synchronisation est sélectionnée. Pour plus d'informations, consultez le *manuel d'administration*. Cliquez sur Terminer.

A l'issue de la récupération, CA ARCserve RHA crée une arborescence inversée temporaire en utilisant la réplication sélectionnée en tant que racine et l'ordinateur maître en tant que noeud final. A la fin du processus de récupération des données du maître, le scénario temporaire est supprimé et le message suivant apparaît dans le volet Événement : La synchronisation est terminée.

Remarque : En cas d'erreur lors de l'exécution du scénario de récupération temporaire, ce scénario peut s'interrompre et rester dans le volet Scénario. Dans ce cas, vous devez le supprimer en cliquant dessus avec le bouton droit de la souris et en sélectionnant l'option Supprimer dans le menu contextuel. Une fois le scénario de récupération supprimé, le scénario d'origine réapparaît dans le volet Scénario. Vous pouvez alors relancer le scénario d'origine et réitérer le processus de récupération, le cas échéant.

Par défaut, à chaque récupération de données, un rapport de synchronisation est généré.

Le processus de réplication peut ensuite redémarrer conformément au scénario d'origine.

Récupération du serveur actif

Dans certaines circonstances, il peut s'avérer nécessaire de forcer le serveur maître ou de réplication à assumer le rôle de serveur actif sans effectuer le processus de synchronisation des données, comme lorsqu'une permutation a eu lieu et qu'aucune donnée n'a été modifiée sur le serveur de réplication. Dans ce cas, il se peut même que vous disposiez de données plus récentes sur le serveur maître ; il n'est pas souhaitable alors de synchroniser les données du serveur maître à partir du serveur de réplication. CA ARCserve RHA offre cette possibilité grâce à un processus de récupération du serveur actif.

Pour utiliser ce processus, arrêtez le scénario, puis sélectionnez *Récupérer le serveur actif* dans le menu Outils.

Important : Bien que cette option soit utile dans de nombreuses situations, utilisez-la avec prudence. Une utilisation incorrecte peut entraîner la perte de données. En règle générale, CA ARCserve RHA permet la permutation d'un hôte vers un autre uniquement si toutes les données sont synchronisées. De cette façon, les utilisateurs ne sont pas redirigés vers un ensemble de données obsolètes, qui écraseraient un ensemble de données potentiellement plus récentes. Lorsque vous utilisez l'option Récupérer le serveur actif, CA ARCserve RHA force la redirection des utilisateurs vers l'un des serveurs sans vérifier s'il contient l'ensemble de données correctes. Par conséquent, en tant qu'administrateur, vous devez vous assurer manuellement que le serveur que vous rendez actif est bien celui dont l'ensemble de données est le plus à jour.

Si Récupération du serveur actif ne résout pas le problème, vous pouvez récupérer manuellement un serveur. Pour plus d'informations, reportez-vous à la section [Récupération de serveurs](#) (page 60).

Sélectionnez soit *Activer le serveur maître*, soit *Activer le serveur de réplication* en fonction du serveur auquel vous souhaitez attribuer le rôle actif.

Important : Si une permutation légitime se produit lors d'un sinistre et que les utilisateurs sont redirigés vers le serveur de réplication pendant un certain temps, il est important de répliquer toutes les modifications présentes sur le serveur de réplication vers le serveur maître avant de rendre le serveur maître actif. L'utilisation de la fonction *Récupérer le serveur actif* dans une telle situation entraîne une perte de données.

Important : Nous déconseillons d'utiliser la réplication inversée automatique dans les scénarios IIS. Pour pouvoir valider les données de réplication, les données du serveur maître doivent être écrasées (après la permutation). Dans les scénarios de base de données (SQL, Exchange) cette option est fiable, car CA ARCserve RHA valide les bases de données de réplication avant d'écraser les données du serveur maître. Une telle protection n'existe pas pour les scénarios IIS. Vous devez l'utiliser uniquement si vous comprenez entièrement les implications possibles.

Annexe A : Informations et astuces supplémentaires

Ce chapitre traite des sujets suivants :

[Paramètres de répertoire du spool](#) (page 58)

[Configuration de comptes de service](#) (page 59)

[Récupération de serveurs](#) (page 60)

Paramètres de répertoire du spool

Le spool CA ARCserve RHA est un dossier situé sur le disque dans lequel les données à répliquer sont sauvegardées (mises en file d'attente) si la bande passante n'est pas suffisante pour transférer toutes les modifications en temps réel. Les données peuvent être mises en file d'attente en cas de déconnexion temporaire ou de congestion du réseau ou tout simplement parce que la bande passante du réseau n'est pas suffisante pour transférer toutes les données modifiées sur le serveur. En plus de stocker les modifications en attendant que la bande passante soit disponible, l'espace de spool est également utilisé dans le cadre du processus normal de synchronisation. Par conséquent, il est normal que la dimension du spool augmente pendant la synchronisation.

Placez le dossier de spool CA ARCserve RHA sur un lecteur relativement peu utilisé, un volume dédié ou un volume de démarrage/système par exemple. Ne le placez pas sur un volume contenant un système fréquemment utilisé (système d'exploitation), des données utilisateur ou des données d'application, par exemple un volume contenant des bases de données, des fichiers partagés ou le fichier d'échange du système. Par défaut, le dossier de spool se trouve dans le dossier tmp, dans le répertoire d'installation de CA ARCserve RHA. Les paramètres du spool, situés dans l'onglet Propriétés (à la fois sur l'ordinateur maître et sur celui de réplication) ou définis à l'aide de l'assistant de création de scénarios, déterminent la quantité d'espace disque disponible pour le spool. Dans la plupart des cas, les valeurs par défaut sont suffisantes. Toutefois, si vous modifiez cette valeur, elle doit représenter au moins 10 % de la taille totale de l'ensemble de données. Par exemple, si vous répliquez 50 Go de données sur un serveur, vous devez vous assurer qu'un espace de 5 Go au moins est disponible pour le spool.

Important : Si vous modifiez l'emplacement du spool, n'oubliez pas de supprimer le nouveau chemin d'accès dans les analyses antivirus de niveau fichier, à la fois dans les analyses planifiées et dans les analyses en temps réel.

Remarque: Le répertoire de spool n'est pas un dossier d'espace disque préalablement alloué et il est utilisé uniquement en cas de besoin.

Configuration de comptes de service

Pour les serveurs d'un groupe de travail, définissez le compte du service moteur CA ARCserve RHA en tant que compte de système local (sauf si vous avez ajouté des scripts personnalisés qui exigent des niveaux d'autorisation plus élevés).

Pour configurer des comptes de service :

1. Créez des comptes d'utilisateur identiques sur les deux serveurs.
2. Attribuez des mots de passe identiques aux deux comptes.
3. Dans les propriétés de chaque site Web pour lequel l'accès anonyme est activé, configurez ce compte comme le compte utilisé pour accès anonyme.
4. Pour utiliser le compte par défaut *IUSR_<nom_ordinateur>* sur les deux serveurs pour un accès anonyme, attribuez des mots de passe identiques aux deux comptes et désélectionnez l'option d'autorisation de la vérification de mot de passe par IIS dans Propriétés > Sécurité de répertoire > Méthodes d'authentification, pour chaque site Web pour lequel l'accès anonyme est activé.

Important : Si le scénario IIS est configuré pour répliquer les listes de contrôle d'accès, l'affichage des propriétés de sécurité des dossiers de contenu de site Web sur l'ordinateur de réplication indique un SID (identificateur de sécurité) non résolu : il s'agit là d'une caractéristique de conception que vous pouvez ignorer.

Ressources supplémentaires

Les articles suivants de la base de connaissances de Microsoft traitent de la configuration de l'authentification de sites Web.

- **Pour IIS 6.0 :** Configuration de l'authentification d'un site Web IIS sous Windows Server 2003 <http://support.microsoft.com/kb/324274>

Récupération de serveurs

CA ARCserve RHA peut détecter l'activation d'un serveur de réplication et exécute automatiquement le processus de récupération. Si la récupération ne se termine pas correctement pour un motif quelconque, effectuez l'une des actions ci-dessous.

- Lancez la procédure de récupération du serveur actif. Pour plus d'informations, reportez-vous à la section [Récupération du serveur actif](#) (page 55).
- Si la procédure de récupération du serveur actif ne résout pas le problème, essayez une ou plusieurs tâches manuelles appropriées à la méthode de redirection utilisée et répertoriées ci-dessous.
 - En cas de redirection IP, supprimez manuellement l'adresse IP. Vous ne pouvez pas utiliser cette méthode pour les scénarios ne prenant pas en charge la redirection Transfert IP (haute disponibilité Hyper-V, haute disponibilité du service de contrôle). Pour plus d'informations, reportez-vous à la section [Récupération manuelle d'un serveur en échec - Transfert de l'adresse IP](#) (page 61)
 - En cas de redirection Permutation du nom de l'ordinateur, permutez manuellement les noms. Vous ne pouvez pas utiliser cette méthode pour les scénarios ne prenant pas en charge la redirection Permutation du nom de l'ordinateur (haute disponibilité Hyper-V, haute disponibilité Exchange, haute disponibilité vCenter en cas d'utilisation locale d'Oracle). Pour plus d'informations, reportez-vous à la section [Récupération manuelle d'un serveur en échec - Permutation du nom de l'ordinateur](#) (page 61).
 - Si les deux méthodes de redirection, Transfert IP et Permutation du nom de l'ordinateur, sont utilisées, supprimez manuellement l'adresse IP et permutez manuellement les noms des ordinateurs. Vous ne pouvez pas utiliser cette méthode pour les scénarios ne prenant pas en charge la redirection Transfert IP et Permutation du nom de l'ordinateur (haute disponibilité Exchange, haute disponibilité du service de contrôle). Pour plus d'informations, reportez-vous à la rubrique traitant de la [récupération manuelle d'un serveur en échec en cas d'utilisation de la redirection Transfert IP et Permutation du nom de l'ordinateur](#) (page 63).

Récupération manuelle d'un serveur en échec - Transfert de l'adresse IP

Si vous utilisez la redirection d'adresse IP, supprimez l'adresse IP manuellement. Vous ne pouvez pas utiliser cette méthode pour les scénarios ne prenant pas en charge la redirection Transfert IP (haute disponibilité Hyper-V, haute disponibilité du service de contrôle).

Pour récupérer un serveur en échec lorsque la redirection Transfert IP est utilisée :

1. Pour éviter des conflits d'adresses IP, démarrez le serveur maître sans connexion au réseau.
2. Dans la boîte de dialogue des propriétés TCP/IP, supprimez l'adresse IP supplémentaire.
3. Redémarrez le serveur et reconnectez-le au réseau.
4. Si le scénario n'est pas déjà en cours d'exécution, démarrez-le à partir du gestionnaire. Si la réplication inversée automatique a été activée, le scénario s'exécute en mode arrière : le serveur de réplication est alors le serveur actif et le serveur maître est en attente.
5. Patientez jusqu'à la fin de la synchronisation.
6. Effectuez une permutation manuelle pour restaurer le rôle actif du serveur maître. Nous vous recommandons de le faire en dehors des heures de travail normales.

Récupération manuelle d'un serveur en échec - Permutation du nom de l'ordinateur

Si vous utilisez la redirection par permutation du nom de l'ordinateur, permutez les noms manuellement. Vous ne pouvez pas utiliser cette méthode pour les scénarios ne prenant pas en charge la redirection Permutation du nom de l'ordinateur (haute disponibilité Hyper-V, haute disponibilité Exchange, haute disponibilité vCenter en cas d'utilisation locale d'Oracle).

Pour récupérer manuellement un serveur en échec à l'aide de la méthode de redirection Permutation du nom de l'ordinateur

1. Démarrez le serveur maître sans connexion réseau, pour éviter les noms de réseau en double.
2. Remplacez le nom du serveur par <NouveauNomServeur>-RHA et déplacez-le dans un groupe de travail temporaire.

Par exemple, si le serveur s'appelle "Serveur1", renommez-le "Serveur1-RHA". Vous devrez alors redémarrer l'ordinateur. Après le redémarrage, le message d'erreur suivant s'affiche : "Au moins un service n'a pas pu démarrer." Ignorez-le, ceci est normal dans ce type de situations, car le moteur CA ARCserve RHA s'exécute généralement dans un compte de domaine.
3. Connectez-vous au réseau.
4. Rejoignez le domaine, en veillant à utiliser le nom -RHA affecté lors de l'étape 2.
5. Réinitialisez l'ordinateur.
6. Si le scénario n'est pas déjà en cours d'exécution, démarrez-le à partir du gestionnaire. Si la réplication inversée automatique a été activée, le scénario s'exécute en mode arrière : le serveur de réplication est alors le serveur actif et le serveur maître est en attente.
7. Patiencez jusqu'à la fin de la synchronisation. Effectuez une permutation manuelle pour rendre actif le serveur maître. Nous vous recommandons de le faire en dehors des heures de travail normales.

Récupération manuelle d'un serveur en échec-Transfert IP et Permutation du nom

Si vous utilisez les deux méthodes de redirection, transfert IP et permutation du nom de l'ordinateur, supprimez manuellement l'adresse IP et permutez manuellement les noms des ordinateurs. Vous ne pouvez pas utiliser cette méthode pour les scénarios ne prenant pas en charge la redirection Transfert IP et Permutation du nom de l'ordinateur (haute disponibilité Exchange, haute disponibilité du service de contrôle).

Pour récupérer manuellement un serveur en échec lorsque les deux méthodes de redirection Transfert IP et Permutation du nom de l'ordinateur sont utilisées

1. Réparez, le cas échéant, les problèmes matériels pouvant être à l'origine de la permutation.
2. Redémarrez le serveur sans connexion au réseau, afin d'éviter les conflits d'IP.
3. Dans la boîte de dialogue des propriétés TCP/IP, supprimez l'adresse IP supplémentaire.
4. Dans la boîte de dialogue Nom de l'ordinateur des propriétés du système, remplacez le nom de l'ordinateur par <NomServeur>-RHA. Par exemple, si votre serveur s'appelle Serveur 3, renommez-le Serveur 3-RHA.
5. Affectez le serveur à un groupe de travail temporaire.
6. Redémarrez l'ordinateur pour que vos modifications prennent effet. Une fois le redémarrage terminé, reconnectez-vous au réseau. Ignorez le message d'erreur "Au moins un service a échoué lors du démarrage du système." Ce message est normal car le moteur s'exécute dans un domaine actuellement indisponible.
7. Rejoignez le domaine, en veillant à utiliser le nom -RHA, et redémarrez une nouvelle fois.
8. Le scénario inverse commence et le serveur de réplication devient l'ordinateur actif. Attendez la fin de la synchronisation.
9. Effectuez une permutation manuelle, en cliquant sur le bouton Effectuer la permutation dans la barre d'outils, pour rétablir le rôle actif du serveur maître.

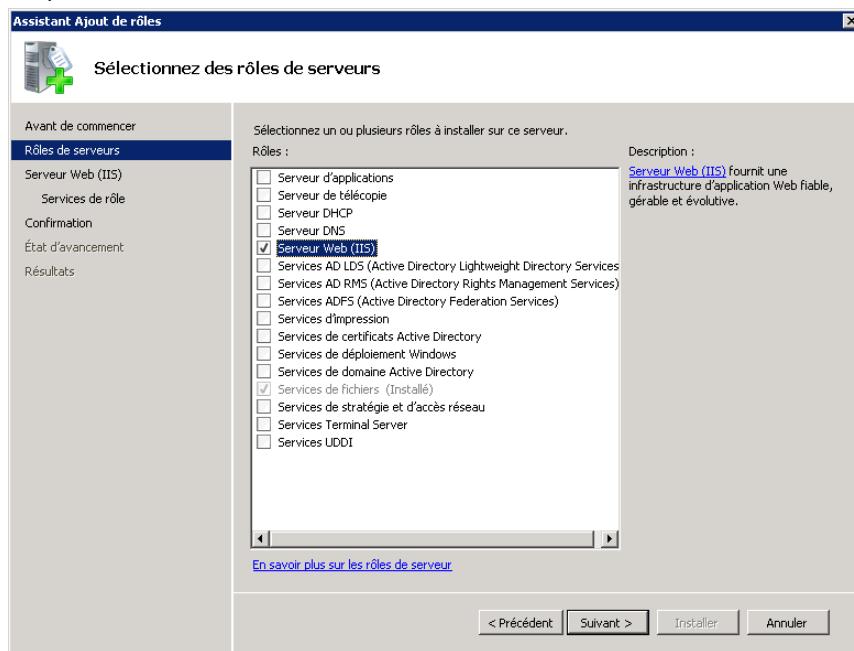
Annexe B : Installation d'IIS 6.0 Management Compatibility pour IIS 7.0

Cette section décrit les étapes nécessaires à l'installation d'IIS 6.0 Management Compatibility pour IIS 7.0. Cette procédure est requise lorsque vous voulez créer un scénario de haute disponibilité pour IIS 7.0.

Remarque : Si vous voulez créer un scénario de haute disponibilité pour IIS 7.0, vous devez répéter cette procédure sur l'hôte maître et sur celui de réPLICATION.

Pour installer IIS 6.0 Management Compatibility :

1. Sur l'hôte maître ou sur l'hôte de réPLICATION, ouvrez le gestionnaire de serveurs et sélectionnez l'option Rôles. Cliquez ensuite sur le bouton Ajouter des rôles.
La première page de l'assistant d'ajout de rôles apparaît.
2. Cliquez sur Suivant. La fenêtre de sélection des rôles de serveur s'affiche.

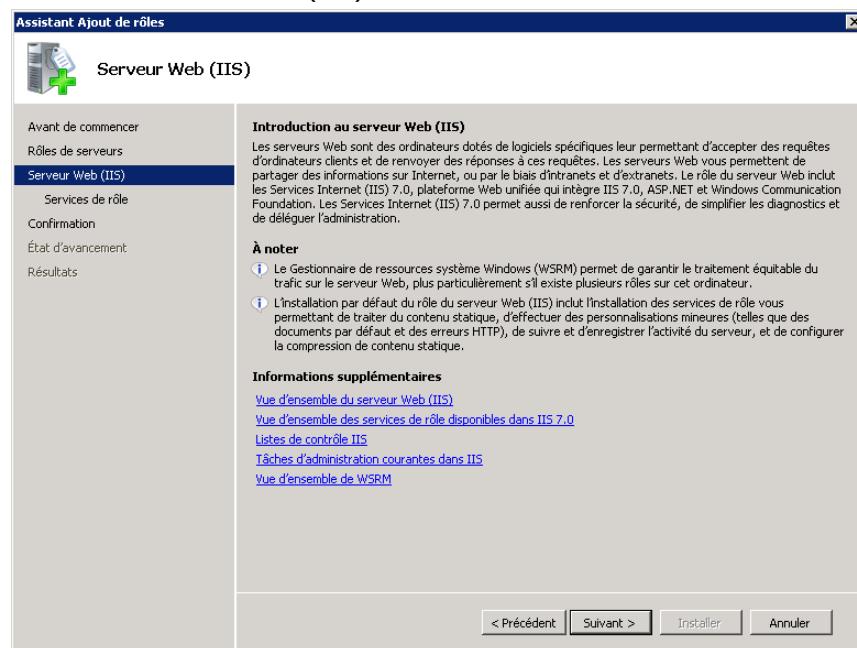


3. Activez la case à cocher Serveur Web (IIS), puis cliquez sur Suivant.
Un message contextuel s'affiche et vous demande si vous souhaitez ajouter les fonctionnalités requises pour le serveur Web (IIS).
4. Cliquez sur Ajouter les fonctionnalités requises.

La fenêtre de sélection des rôles de serveur s'affiche.

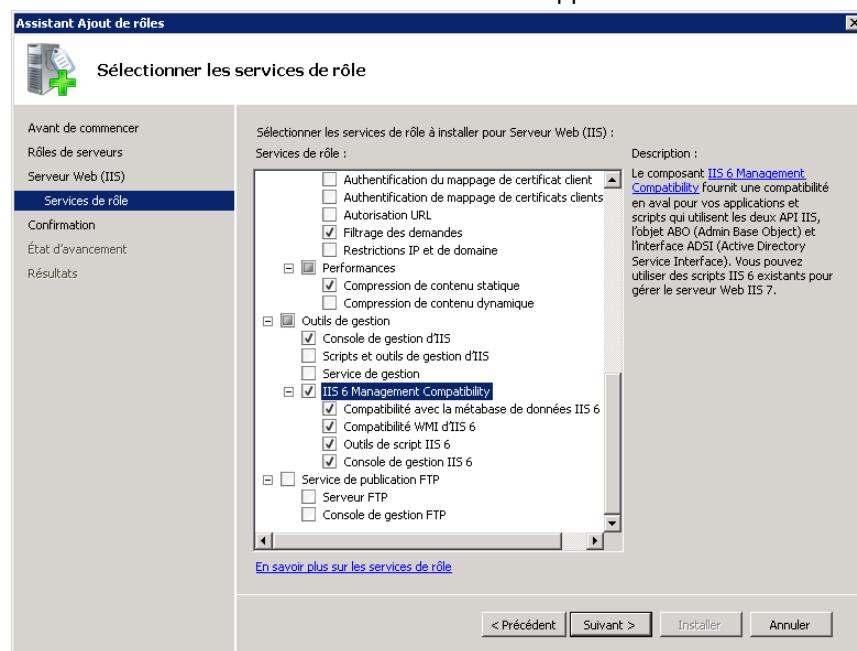
5. Cliquez sur Suivant.

La fenêtre Serveur Web (IIS) s'affiche.



6. Cliquez sur Suivant.

La fenêtre de sélection de services de rôles apparaît.



7. Dans la liste des services de rôles, activez la case à cocher IIS 6 Management Capability.
8. Cliquez sur Suivant et suivez les instructions de l'assistant jusqu'à la fin de l'installation.

Index

A

- A propos de ce manuel - 7
- A propos des clusters - 11
- Affichage d'un rapport - 23
- Ajout de l'adresse RHA-IP à de nouveaux scénarios - 30
- Ajout de l'adresse RHA-IP à des scénarios existants - 28
- Ajout d'une adresse IP sur le serveur maître - 26
- Arrêt d'un scénario - 22

B

- Boîte de dialogue Sélection d'un point de retour arrière - iv, 52

C

- Conditions du compte de connexion - 10
- Configuration de base - 8
- Configuration de comptes de service - 59
- Configuration requise pour le serveur - 8
- Configuration requise pour un serveur IIS - 9
- Considérations sur la permutation - 44
- Création d'un scénario Microsoft IIS - iv, 15
- Création et utilisation de scénarios - 15

D

- Définition de repères - 45
- Démarrage d'une permutation - 38, 39
- Démarrage d'une permutation inversée - 41
- Documentation connexe - 7

E

- Enregistrement des licences CA ARCserve RHA - 12
- Exécution d'un scénario hors de l'assistant - 20

F

- Fonctionnement de la permutation et de la permutation inversée - 37
- Fonctionnement de la redirection - 25

I

- Informations de contact de CA - iii
- Informations et astuces supplémentaires - 57
- Installation d'IIS - 10
- Installation d'IIS 6.0 Management
- Compatibility pour IIS 7.0 - 9, 65
- Introduction - 7

M

- Méthodes de redirection - 25
- Modifications de la documentation - iv

N

- Nouveaux scénarios - 32

P

- Paramètres de répertoire du spool - 19, 44, 58
- Permutation et permutation inversée - 17, 37
- Processus de récupération des données - 45
- Produits CA référencés - iii
- Propriétés du scénario - 17

R

- Récupération de données - 45
- Récupération de données perdues à partir du serveur de réplication - 54
- Récupération de serveurs - 56, 60
- Récupération du serveur actif - 55, 60
- Récupération manuelle d'un serveur en échec - Permutation du nom de l'ordinateur - 62
- Récupération manuelle d'un serveur en échec - Transfert de l'adresse IP - 60, 61
- Récupération manuelle d'un serveur en échec - Transfert IP et Permutation du nom - 60, 63
- Redirection automatique par permutation du nom de l'ordinateur - 34
- Redirection du système DNS - 25
- Redirection par scripts - 35
- Redirection Permutation du nom de l'ordinateur - 34
- Redirection Transfert IP - 26
- Réplication d'une métabase IIS - 11
- Ressources supplémentaires - 59
- Retour arrière des données - iv, 47, 48

S

Scénarios existants - 32
Serveurs fonctionnant dans un groupe de travail - 10

T

Transfert IP de cluster - 11, 30

U

Utilisation du cluster maître - 31
Utilisation du gestionnaire - 31