


Read-Only Domain Controller

Greg Georges





Table des Matières

- Domain Controller ?
 - Read-Only DC ?
 - Avantages
 - Inconvénients
 - Installation
 - Questions / Réponses
- 

Domain Controller

- Serveur qui gère et contrôle l'accès aux ressources d'un domaine : Active Directory.
- Gère les objets tels que users, computers, groups.
- En parallèle avec un autre DC, ils assurent la réplication des données pour garantir la disponibilité et la redondance des informations stockées dans l'annuaire.



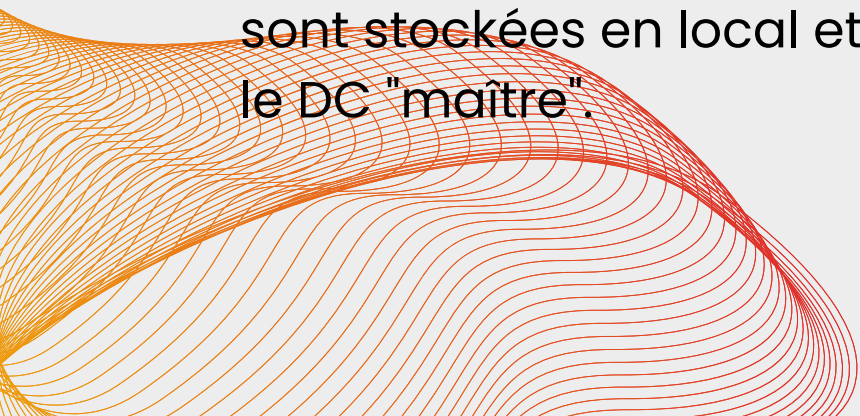
Read-Only ?

- Contient les mêmes informations qu'un DC classique sauf les données trop sensibles comme, par exemple, les mots de passe.
- Aucune modification de l'annuaire possible
- Mises à jour uniquement envoyées par le DC "maîtres".
- Généralement utilisé là où la sécurité est une préoccupation majeure comme dans des succursales ou dans des sites distants.





Avantages

- Sécurisation sur les sites distants :
 - Limitation des données sensibles sur site (users standards).
 - Protection en cas de vol du matériel, associé à Bitlocker.
 - Authentification locale :
 - Permet aux users locaux d'accéder aux ressources en cas de déconnexion avec le DC principal.
 - Peut servir de cache pour le DNS :
 - Les infos DNS peuvent également être répliquées.
 - Economie de bande-passante puisque beaucoup de données sont stockées en local et évite donc des requêtes inutiles vers le DC "maître".
- 

Inconvénients

- Limitation des modifications : nécessité de faire les modifications sur un DC en écriture. Par exemple, pour l'ajout/modification des users.
- Dépendance par rapport au DC principal pour recevoir les mises à jour. S'il est indisponible, plus de MAJ.
- Nécessite une bonne planification pour déterminer sur quel site l'utiliser. Une mauvaise planification peut entraîner des problèmes de performances ou de sécurité selon des facteurs comme la connexion au DC central ou bien la sécurité du site.

Installation

Installation semblable à celle d'un DC classique sauf qu'il faut cocher la case "**RODC**".

Assistant Configuration des services de domaine Active Directory

SERVEUR CIBLE
dc2-rodC

Options du contrôleur de domaine

Configuration de déploie...
Options du contrôleur de...
Options RODC
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats

Spécifier les capacités du contrôleur de domaine et les informations sur le site

- Serveur DNS (Domain Name System)
- Catalogue global (GC)
- Contrôleur de domaine en lecture seule (RODC)

Nom du site : Default-First-Site-Name

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

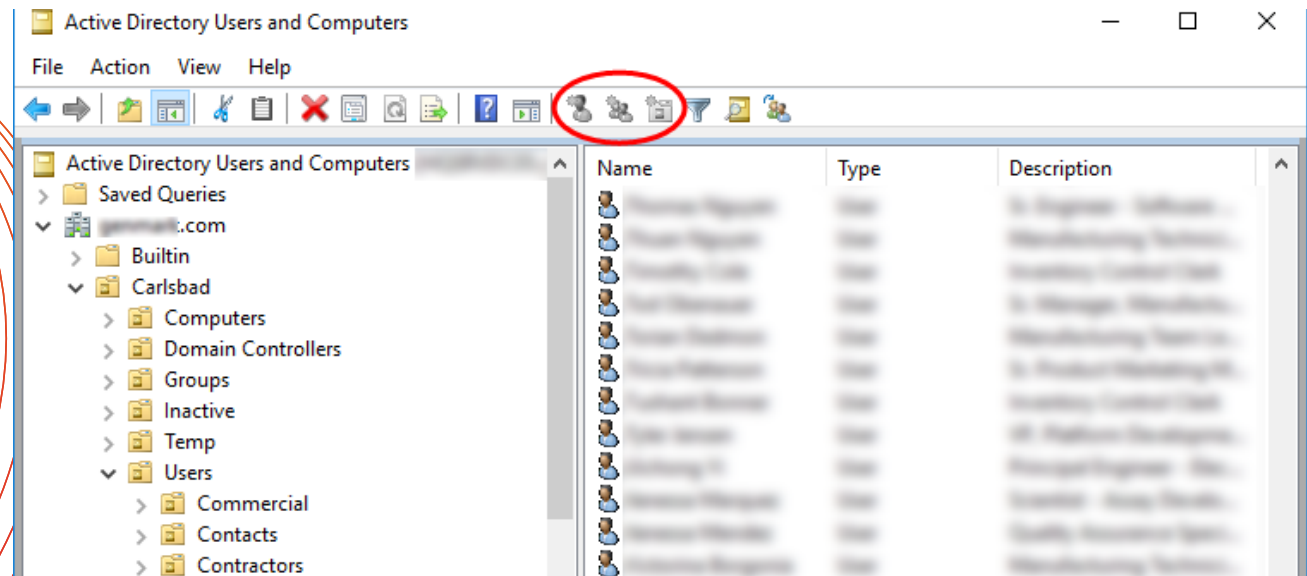
Confirmer le mot de passe :

[En savoir plus sur la options du contrôleur de domaine](#)

Installation

Après avoir fini l'installation, on peut exécuter la commande
CMD => repadmin/syncall sur le serveur maître pour forcer
la synchronisation.

Après stabilisation de l'Active Directory, on peut constater
que certaines options de paramétrages sont désactivées.



Installation

Ensuite, il est possible de créer des groupes d'users dont les mots de passe pourront être répliqués sur la RODC, leur permettant ainsi de pouvoir continuer à travailler même si la connexion avec le DC maître est interrompue.

Domain Controllers => Propriétés => Stratégie de Réplication de mot de passe.

Propriétés de : RODC01

Général	Système d'exploitation	Membre de	Délégation
Stratégie de réplication de mot de passe	Emplacement	Géré par	Appel entrant

Ceci est un contrôleur de domaine en lecture seule (RODC). Un contrôleur de domaine en lecture seule stocke les mots de passe des utilisateurs et des ordinateurs selon la stratégie suivante : seuls les mots de passe des comptes figurant dans les groupes d'autorisation, et non dans les groupes de refus, peuvent être répliqués sur le contrôleur de domaine en lecture seule.

Groupes, utilisateurs et ordinateurs :

Nom	Dossier Services de d...	Paramètre
Administrateurs	it-connect.fr/Builtin	Refuser
Groupe de réplication ...	it-connect.fr/Users	Autoriser
Groupe de réplication ...	it-connect.fr/Users	Refuser
Opérateurs de compte	it-connect.fr/Builtin	Refuser

Conclusion



+++

- Sécurité renforcée dans des environnements distribués (succursales).
- Réduction de la surface d'attaque car limitation des données sensibles.
- Maintien de l'activité si déconnexion avec le DC central.

- Obligation de passer par DC central pour modifier l'AD.
- Dépendance au DC central pour les mises à jour.



Questions/Réponses

Merci

Greg Georges