Read-Only Domain Controller

Greg Georges

Table des Matières

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 ?

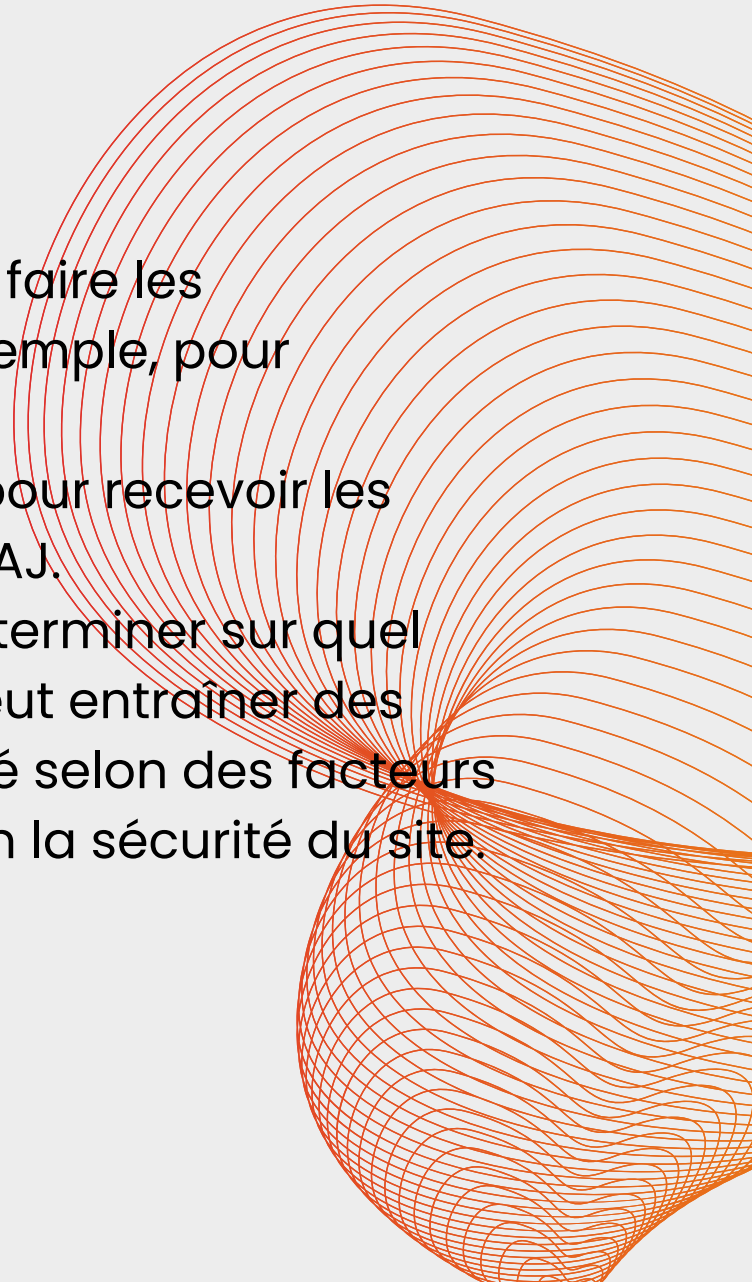
- Contient les mêmes informations qu'un DC classique sauf les données trop sensibles comme, par exemple, les mots de passe.
- Aucune modification de l'annuaire possible
- Mises à jour uniquement envoyées par le DC "maîtres".
- Généralement utilisé là où la sécurité est une préoccupation majeure comme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

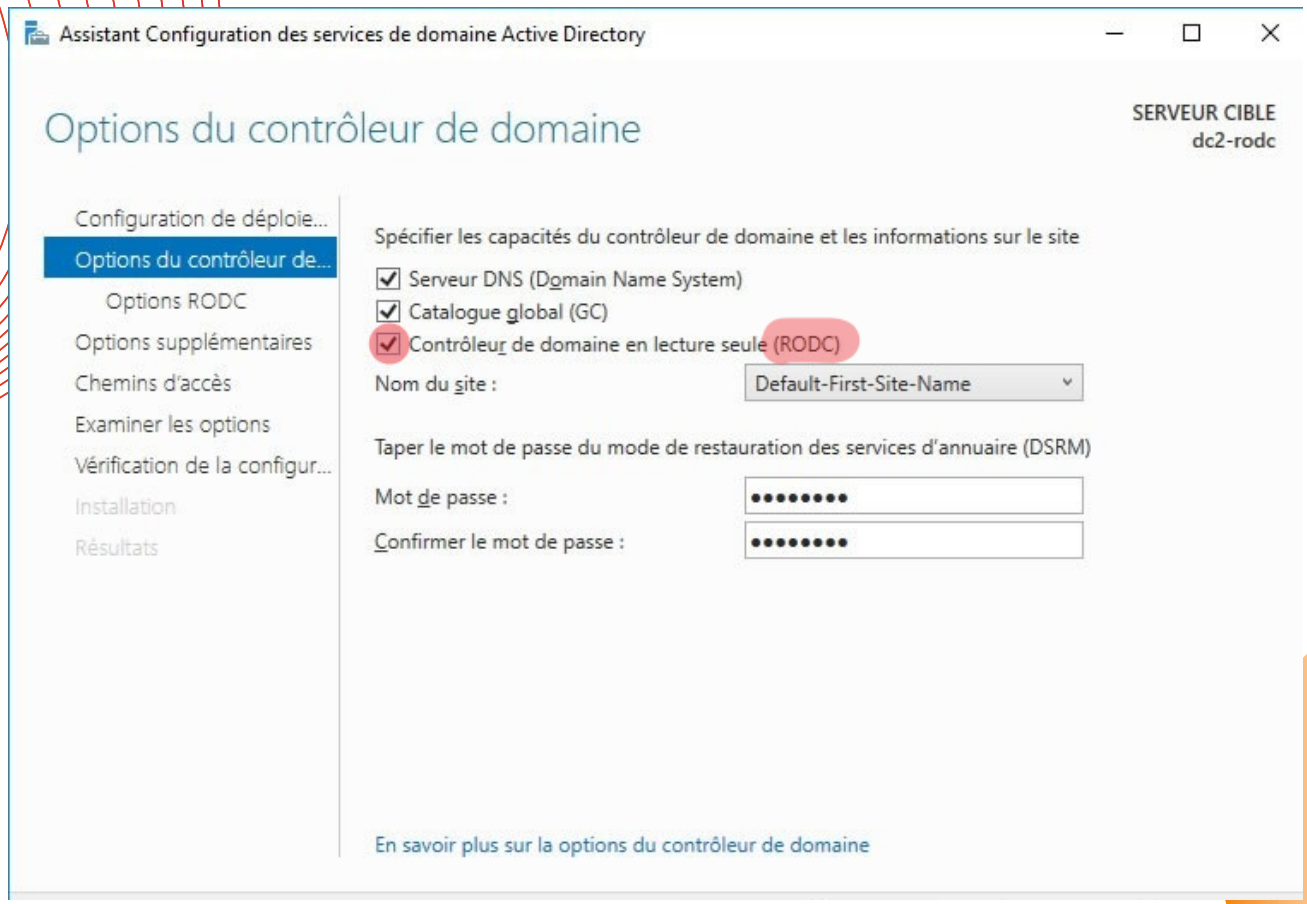
Inconvénients

- 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**".

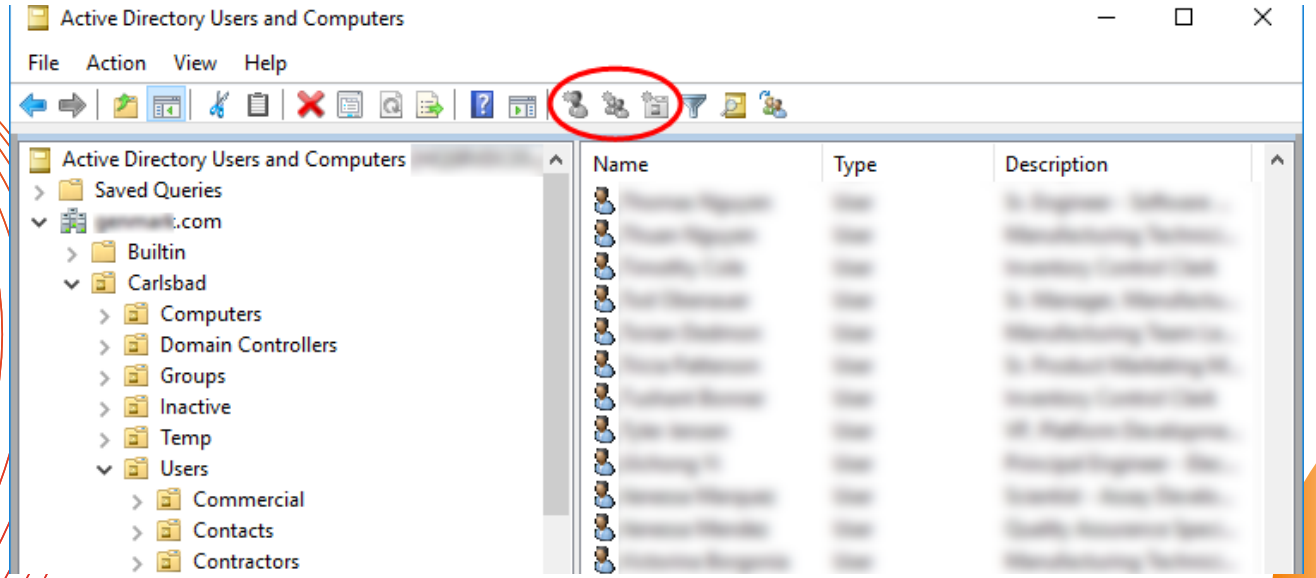


Source : www.abdel.com

Installation

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

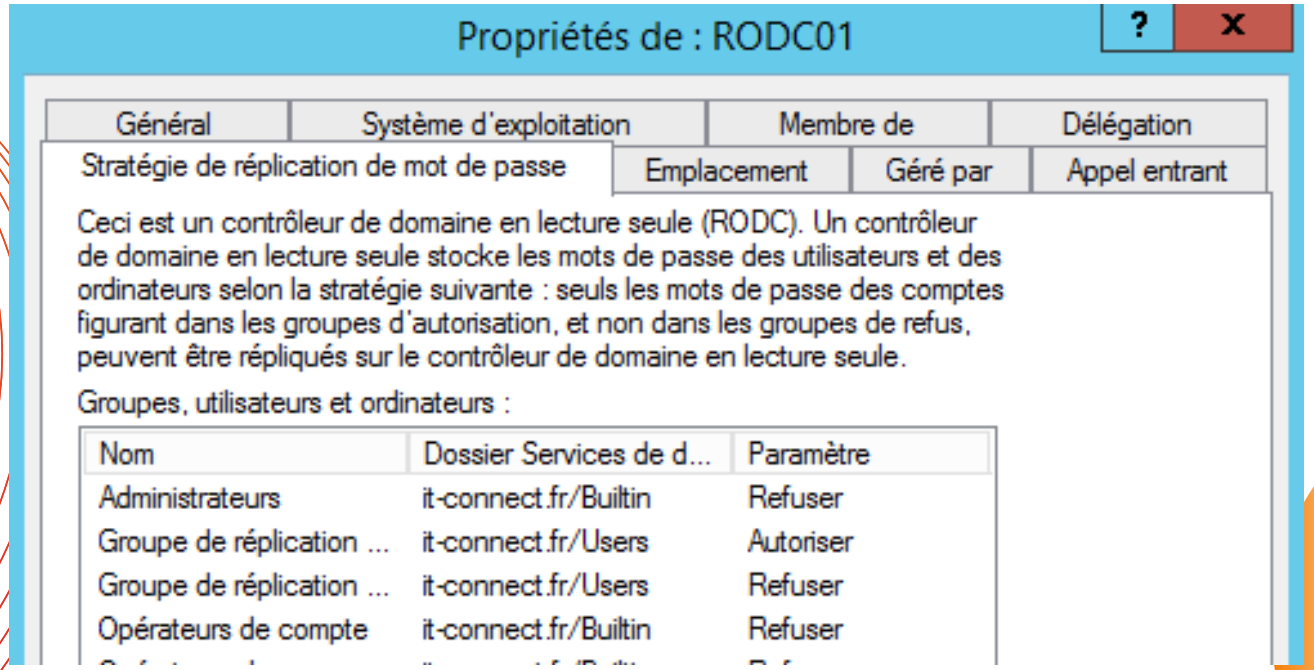
Après stabilisation de l'Active Directory, on peut constater que certaines options de paramétrages sont désactivées.



Source : www.abdel.com

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.



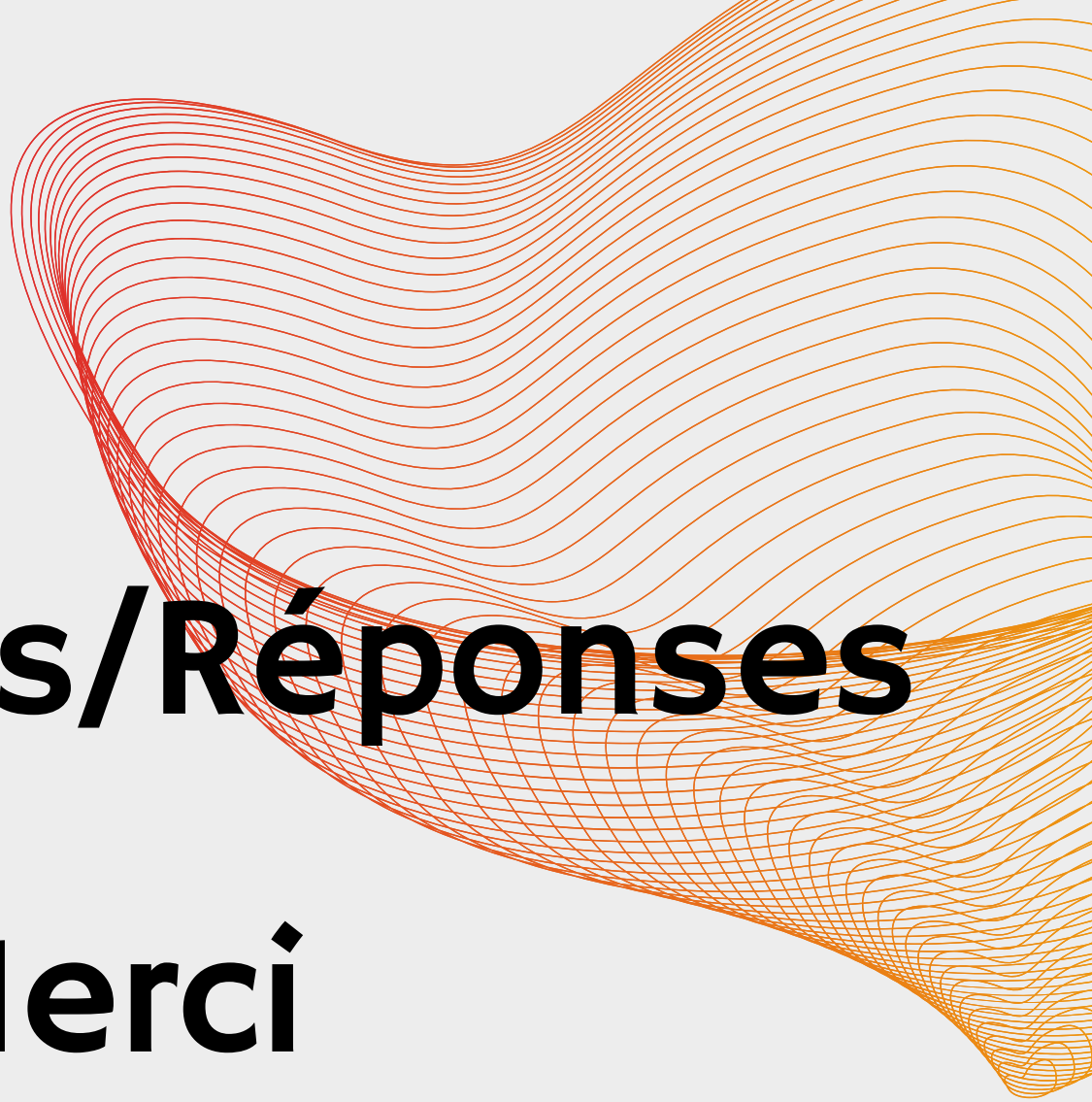
Source : www.abdel.com

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