

Attaché d'État 2018 : les redirecteurs DNS

Proposition de corrigé — non officielle. Concours réservé Culture d'attaché d'administration de l'État, programmeur système d'exploitation, session 2018 : sujet technique n° 1 de l'oral, trois questions. La présentation personnelle du parcours est distincte.

[Sujet officiel](#) · [Annales de ce concours ou examen](#)

1. À quoi sert un redirecteur conditionnel ?

Un redirecteur conditionnel demande à des serveurs DNS déterminés de résoudre les noms appartenant à un domaine donné. La condition porte sur le suffixe du nom recherché. Par exemple, le serveur DNS d'une organisation peut envoyer les requêtes pour partenaire.example aux deux serveurs DNS du partenaire, tout en conservant son circuit habituel pour les autres domaines.

Le serveur reçoit la question du client, constate qu'il ne dispose pas lui-même de la réponse, sélectionne la règle correspondant au domaine et interroge le serveur maître configuré. Il transmet ensuite la réponse au client et peut la conserver dans son cache selon sa durée de validité. Il faut donc que les serveurs désignés soient joignables et capables de répondre pour le domaine concerné.

Cette configuration est utile entre deux infrastructures utilisant des espaces de noms privés : le DNS public ne connaît pas nécessairement leurs noms internes. Elle évite d'héberger une copie de toute la zone du partenaire. Elle ne crée ni relation d'approbation Active Directory, ni compte utilisateur, ni droit d'accès aux ressources dont le nom a été résolu.

Trois mécanismes doivent être distingués :

Mécanisme	Ce qui est conservé localement	Usage
Redirecteur général	Adresses de serveurs pour les requêtes non résolues localement	Circuit de résolution par défaut
Redirecteur conditionnel	Domaine cible et adresses des serveurs auxquels transmettre ses requêtes	Résolution particulière d'un espace de noms
Zone secondaire	Copie en lecture seule des enregistrements de la zone	Réponse locale à partir d'un transfert de zone autorisé

Un redirecteur conditionnel n'est pas non plus une zone de stub : celle-ci conserve certains enregistrements permettant de retrouver les serveurs faisant autorité, et non simplement une liste de destinations définie par l'administrateur. La [documentation Microsoft historique](#) explique le fonctionnement des redirecteurs conditionnels.

2. Comment le configurer dans Windows Server ?

Dans le **Gestionnaire DNS**, sélectionner le serveur concerné, ouvrir le nœud **Redirecteurs conditionnels**, puis choisir **Nouveau redirecteur conditionnel**. Renseigner le nom du domaine à traiter, par exemple partenaire.example, et les adresses IP de ses serveurs DNS. Le nom à saisir est un domaine, pas l'URL d'une application.

Ajouter de préférence plusieurs serveurs réellement disponibles. Vérifier leur accessibilité réseau et les règles autorisant les échanges DNS. Une réponse DNS peut utiliser UDP ou TCP sur le port 53 ; autoriser uniquement UDP peut donc laisser certaines résolutions échouer. La zone cible et les adresses doivent correspondre à l'architecture du partenaire, et non être déduites au hasard de son site web public.

Après validation, tester un nom connu de ce domaine en interrogeant explicitement le serveur que l'on vient de configurer. Comparer le résultat avec une interrogation directe d'un serveur maître permet de distinguer une erreur de destination d'un enregistrement absent. Tester aussi un autre domaine pour vérifier que la nouvelle règle ne perturbe pas le fonctionnement habituel.

La commande PowerShell `Add-DnsServerConditionalForwarderZone` permet également de créer la règle. Les paramètres `Name` et `MasterServers` indiquent respectivement le domaine et les serveurs cibles. Pour une configuration intégrée à AD, le paramètre `ReplicationScope` précise la portée de réplication. Ces paramètres figurent dans la [documentation Microsoft du module DnsServer](#).

Exemple pédagogique : nom partenaire.example, serveurs 192.0.2.10 et 192.0.2.11. Ces valeurs sont réservées à l'illustration ; elles doivent être remplacées par celles de l'environnement administré. La réussite du test exige un véritable enregistrement sur les serveurs cibles.

3. Peut-on le conserver dans Active Directory ?

Oui, lorsque le serveur DNS utilise l'intégration à Active Directory. Dans la boîte de création, l'administrateur peut demander le stockage du redirecteur dans AD et choisir la portée de réplication proposée : serveurs DNS du domaine, de la forêt ou d'une partition d'application définie, selon l'environnement.

Les portées de réplication du domaine ou de la forêt concernent les serveurs DNS installés sur des contrôleurs de domaine. La configuration est alors répliquée aux serveurs concernés au lieu d'être saisie séparément sur chacun. Cela facilite la cohérence du paramétrage et sa disponibilité. La réplication porte sur la **configuration du redirecteur** ; elle ne transforme pas le DNS local en serveur faisant autorité pour la zone distante et ne copie pas tous ses enregistrements.

Sans stockage AD, la règle reste attachée au serveur sur lequel elle a été créée. Le choix de la portée doit correspondre au besoin : un domaine partenaire accessible seulement depuis une partie de l'infrastructure ne justifie pas nécessairement une réplication à toute la forêt.

Réponse proposée à l'oral

« Un redirecteur conditionnel permet de transmettre les requêtes d'un domaine précis à des serveurs DNS désignés. Je le configure dans le Gestionnaire DNS en renseignant le domaine et les adresses IP des serveurs maîtres, puis je vérifie leur accessibilité et la résolution d'un nom connu. Je peux conserver sa configuration dans Active Directory et choisir une portée de réplication adaptée. Ce stockage partage la règle entre les serveurs concernés ; il ne copie pas la zone distante et ne crée pas de relation d'approbation. »

Cette réponse traite les trois questions du sujet technique n° 1. La présentation personnelle du parcours professionnel, distincte dans l'épreuve, doit être construite à partir de l'expérience réelle du candidat.