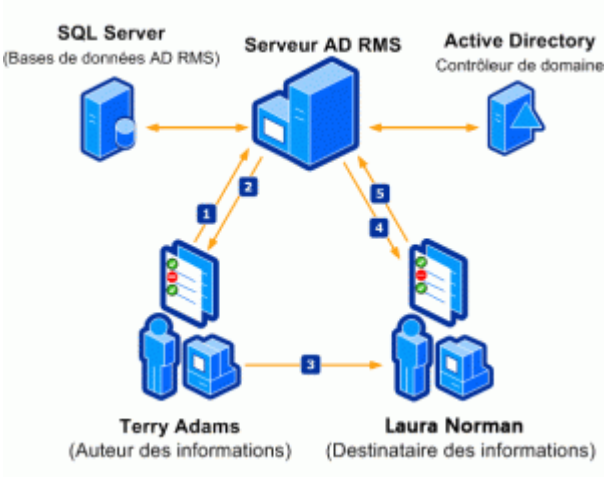
# Déployer AD RMS pour DAC

Nous avons vu dans un précédent article comment déployer DAC, je vous propose ici de renforcer la sécurisation de vos données en couplant DAC avec les services Rights Management Services.

Le rôle **Active Directory Right Management Services** est une fonctionnalité qui propose une sécurité supplémentaire pour les documents d'une entreprise. Elle permet de sécuriser les documents en proposant un chiffrage mais aussi d'attacher des **DRM** à ces derniers.

Dans ce billet, nous allons commencer par l'installation du rôle RMS (de façon basique), puis sa configuration et terminer par la création d'un Template. Cette fonctionnalité est disponible dans **Windows Server 20xx** pour les serveurs, côté client le minimum requis est **Windows Vista SP2**.

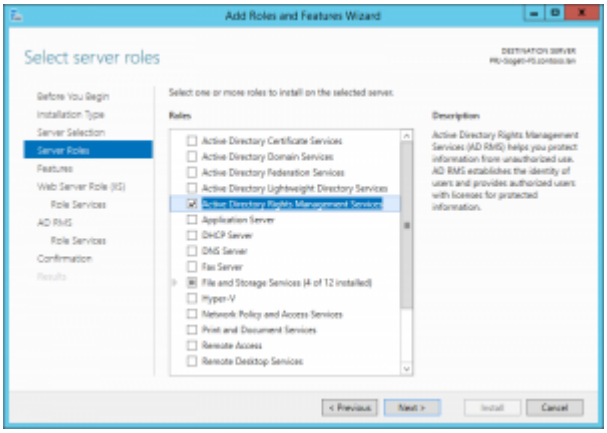
Voici un exemple du fonctionnement du service lorsqu'un utilisateur protège un élément :




1. Quand Terry applique ses restrictions d'accès, le client AD RMS émet une demande de service en son nom au serveur AD RMS de **Contoso**.
2. Le serveur AD RMS de **Contoso** renvoie un certificat de licence client au client AD RMS installé sur le bureau de Terry, ce qui lui permet d'enregistrer le document sous une forme chiffrée avec le niveau de protection des droits souhaité.
3. Terry envoie ensuite à Laura, sous la forme d'une pièce jointe à un message électronique, le document Word protégé par des droits.
4. Laura reçoit le message électronique de Terry, enregistre le document joint sur son bureau en local, puis ouvre le document. Le client AD RMS qui s'exécute sur son bureau contacte alors le serveur AD RMS de **Contoso** pour acquérir une licence utilisateur final.
5. Le client AD RMS sur le bureau de Laura reçoit en retour la licence utilisateur final, qui indique qu'elle est autorisée à afficher le document. Le client AD RMS déchiffre ensuite le document et applique les restrictions appropriées pour permettre à Laura d'accéder au contenu selon les autorisations d'accès accordées par Terry.

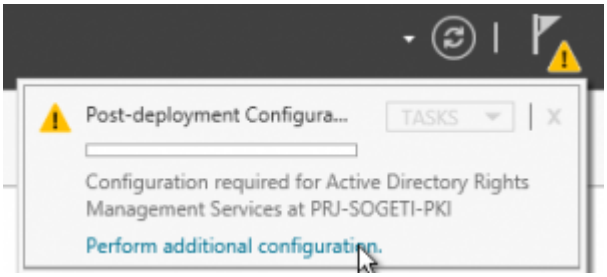
## Installation du rôle AD RMS

L'installation se fait à partir du menu d'installation des rôles et fonctionnalités de **Windows Serveur 2012**. L'installation ne demande pas d'autres actions particulières.

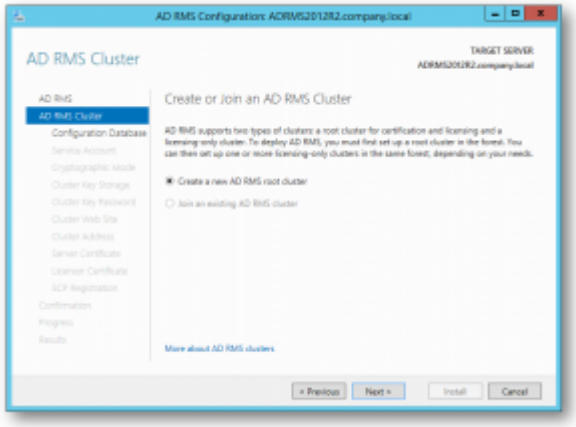



## Configuration du rôle AD RMS

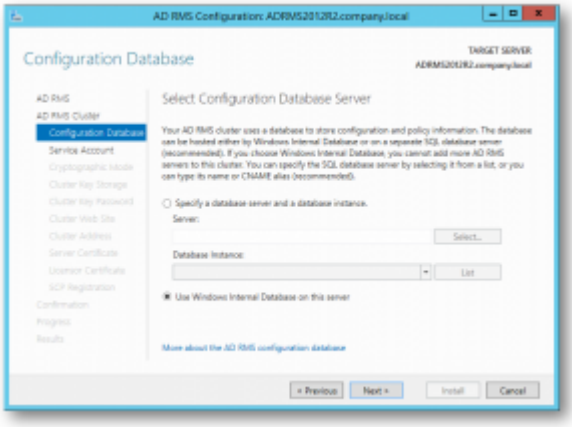
Une fois l'installation terminée une notification apparait dans le menu du **Tableau de bord Active Directory**. **Perform additional configuration** permet la configuration du serveur **RMS**.



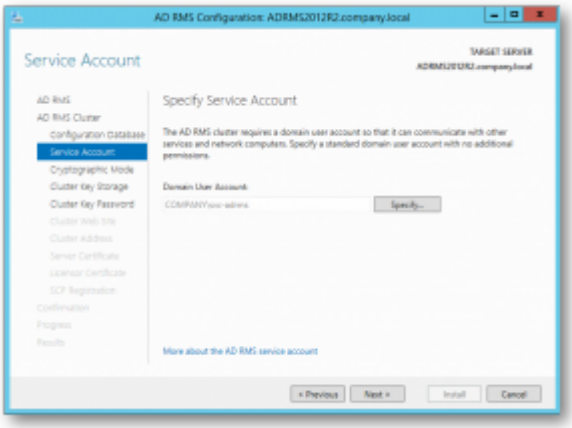

Puis nous suivons l'assistant d'installation. Nous créons une nouveau **Cluster**. Il est possible d'ajouter des serveurs **Right Management Services** pour assurer la haute disponibilité du service. Dans notre scénario nous nous concentrons sur un seul serveur.



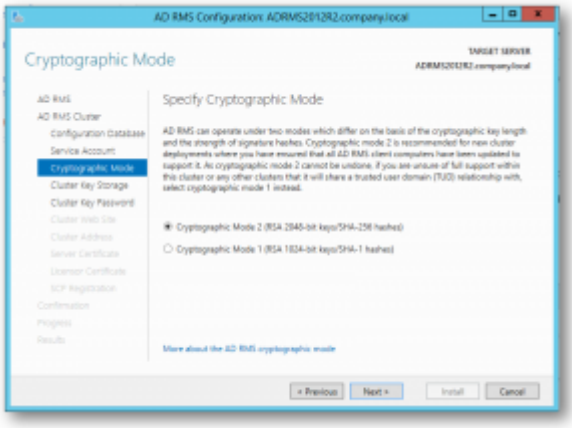

Nous choisissons de stocker toutes les configurations sur la **Database local**. Il est possible de le stocker sur un **serveur SQL** dédié. Cette fonctionnalité est sélectionnée uniquement si nous installons un cluster de server **RMS**.



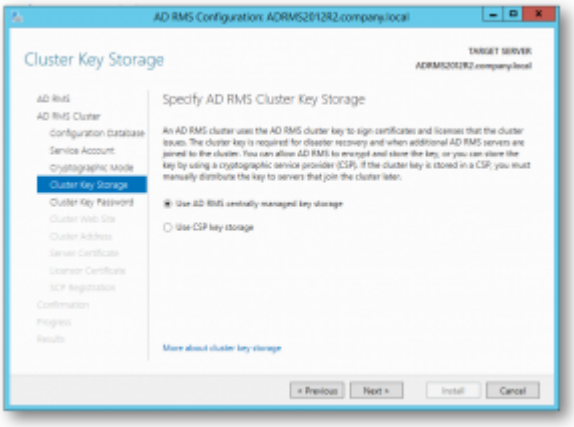

Nous allons ensuite spécifier le compte administrateur spécifique au service **RMS** que nous créons dans l'annuaire **Active Directory**.



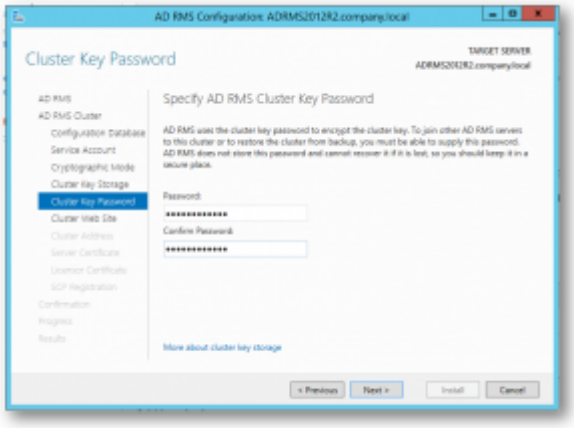

L'étape suivante permet de sélectionner le mode de cryptage. Dans notre scénario nous sélectionnons le **Mode 2**.



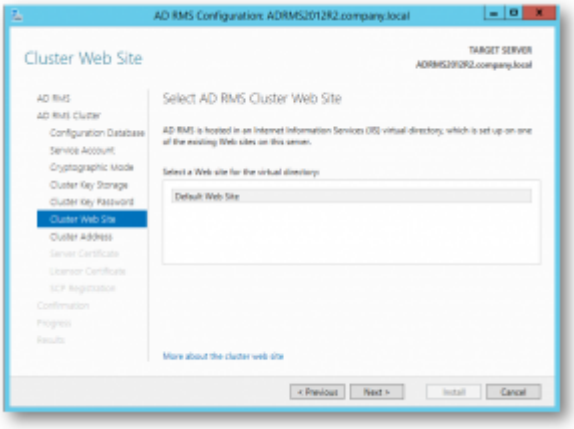

**AD RMS centrally managed key storage** va permettre aux documents d'être cryptés via le serveur **RMS**.



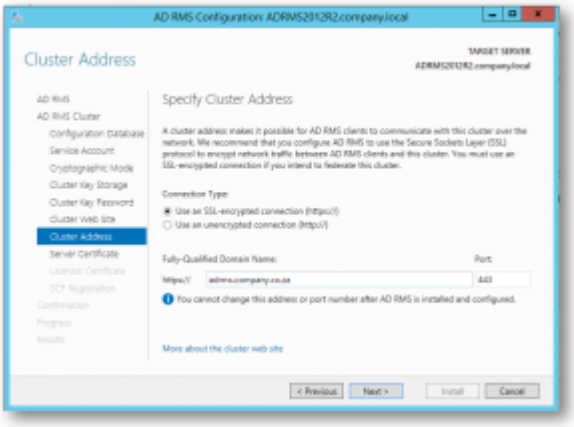

Dans ce menu on renseigne le mot de passe s'il l'on rajoute un serveur en cluster ou bien réaliser un backup des configurations.



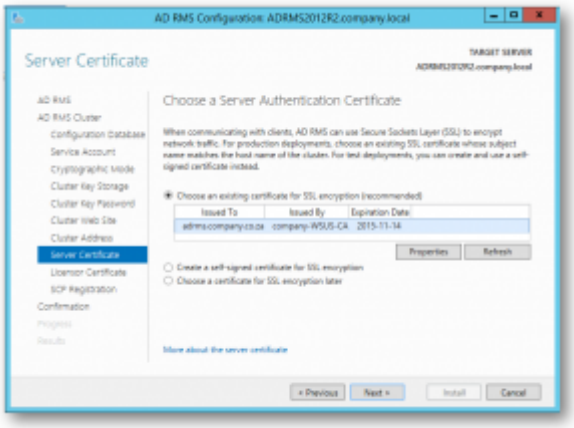

Par défaut nous utilisons le **Default Web Site** du **IIS**.



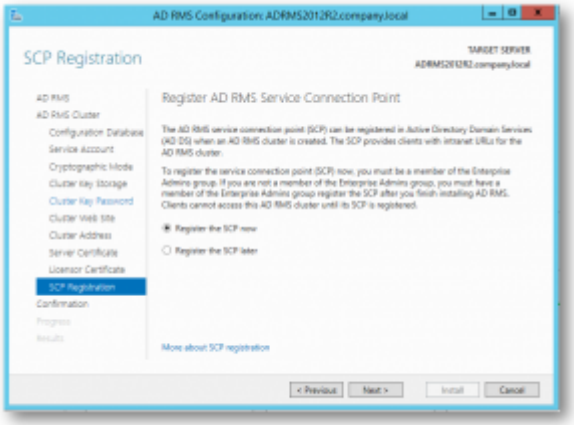

Puis nous allons renseigner le nom DNS que les clients vont contacter. Nous utilisons le port **443** pour plus de sécurité.



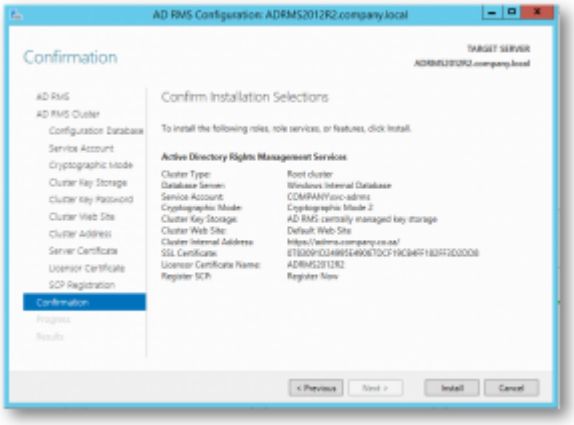

Entre temps nous créons un nouveau certificat pour le cluster **RMS**, ce certificat peut être auto-signé.




Pour terminer, nous finalisons la configuration en renseignant le **SCP** (service connection point) directement dans l' **Active Directory**.

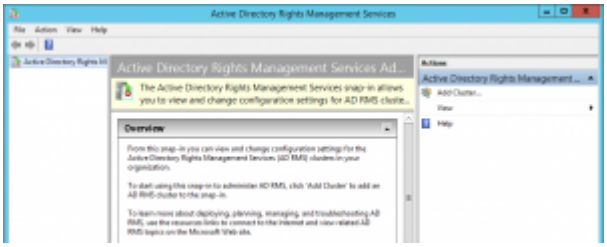


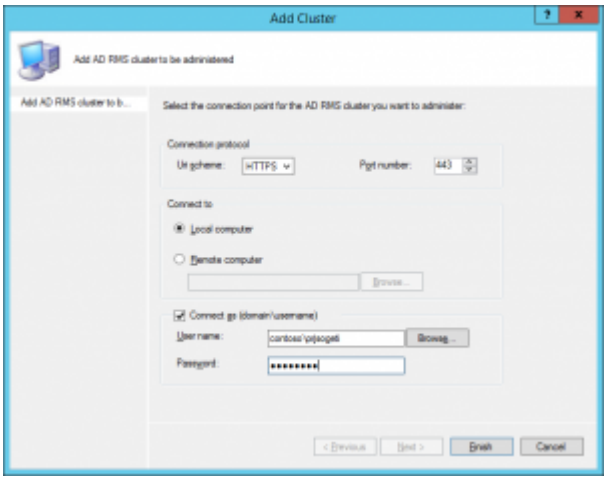

Finalisons la configuration de RMS !



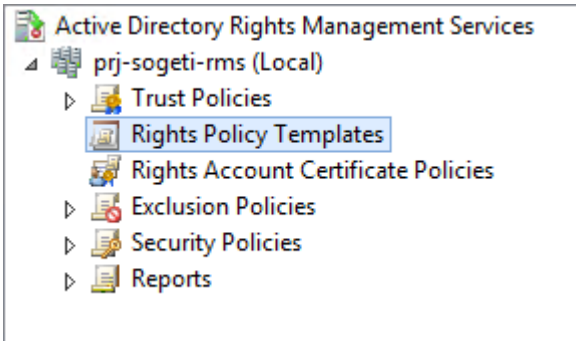

## Création d'un template

Passons maintenant à la création d'un Template. Dans le menu **Active Directory Right Management Services** nous nous connectons sur le serveur local avec le bouton **Add Cluster...**.

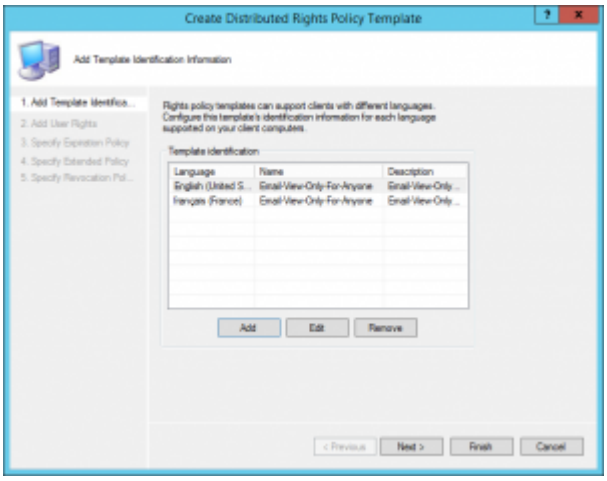


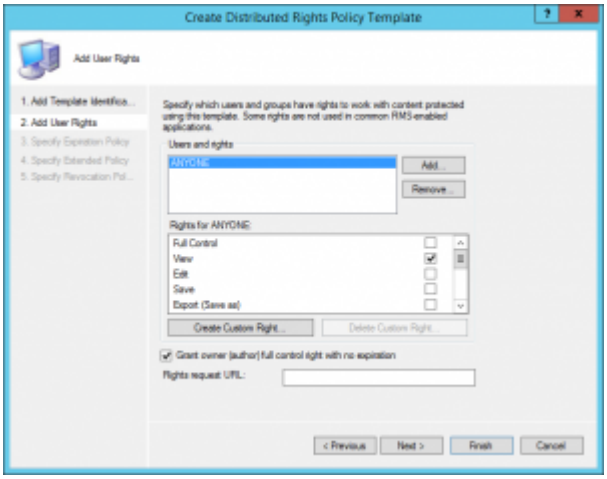

Ensuite dans le menu **prj-sogeti-rms -> Right Policy Templates** nous allons créer notre Template avec le bouton **Create distributed rights policy template**..



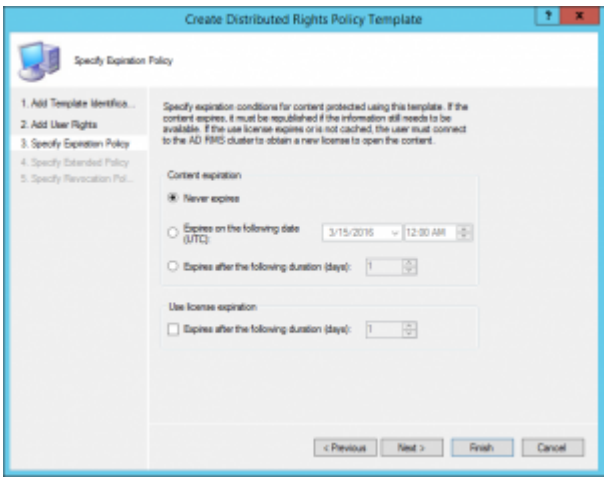
La création d'un Template se fait en plusieurs étapes, dans notre exemple nous allons seulement autoriser la lecture et nous allons l'appliquer aux Email envoyés. Premièrement nous choisissons la langue qui va identifier les utilisateurs concernés. Dans notre cas les utilisateurs français et anglais.




Deuxièmement nous sélectionnons quels utilisateurs sont concernés dans l'annuaire **Active Directory**. Les utilisateurs sont renseignés par leur adresse Email.

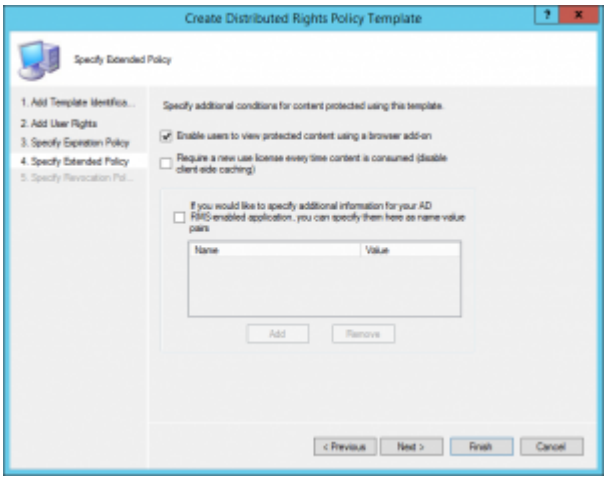



Il est ensuite possible de mettre une date d'expiration pour que la règle ne s'applique plus à une date donnée.

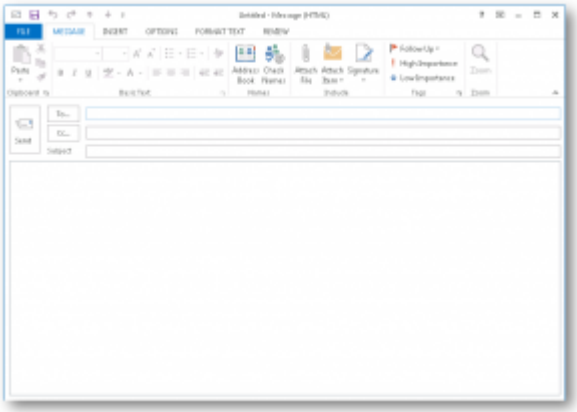


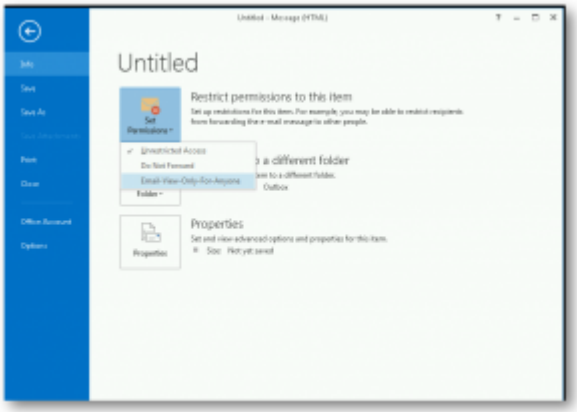

Quatrièmement nous pouvons choisir d'afficher à l'utilisateur les éléments protégés. Il est aussi

possible de demander une nouvelle License à chaque utilisation.




Maintenant que notre Template est prêt nous allons l'appliquer sur un nouvel Email. C'est lors de la création de l'Email que nous allons dans **File -> Info -> Set Permissions** pour ensuite sélectionner la règle créée précédemment.






Une fois l'Email envoyé à l'utilisateur nous pouvons remarquer que l'élément n'est qu'en lecteur, il est donc impossible de faire suivre l'Email.