

Errata partie 2

Kit de formation 70-640

Configuration d'une infrastructure Active Directory avec Windows Server 2008

Microsoft Press remercie Sylvie GREGOIRE,
professeur pour la préparation à la certification Microsoft 70-640 & 70-642,
pour sa relecture attentive.

Chapitre 15 Leçon 1 Page 778 :

Service d'inscription de périphériques réseau Les équipements qui exécutent des systèmes d'exploitation de bas niveau, comme les routeurs et les commutateurs, peuvent également participer à une PKI *via* le service d'inscription de périphériques réseau (NDES, *Network Device Enrollment Service*) en utilisant le protocole SCEP (*Simple Certificate Enrollment Protocol*) développé par Cisco Systems. Comme ces ~~services-équipements~~ ne font généralement pas partie de l'annuaire, ils ne possèdent pas de compte AD DS.

Chapitre 15 Leçon 1 page 779 :

Inscription web pour les requêtes et la validation des certificats	Prise en charge	Pries-Prise en charge
--	-----------------	----------------------------------

Chapitre 15 Leçon 1 page 780 :

Publication et gestion des certificats par AD DS	N/A	Prise en charge
--	-----	-----------------

Chapitre 15 Leçon 1 page 793 :

Exercice 2 : Installer AD CS ~~avec comme~~ une autorité de certification d'entreprise émettrice

Chapitre 15 Leçon 1 page 794 :

Normalement, vous devriez effectuer cette procédure hors ligne en utilisant un périphérique de stockage amovible comme une disquette ~~ou un support USB~~.

Chapitre 15 Leçon 2 page 801 :

■ Pour protéger vos réseaux sans fil, vous devez configurer des certificats spécifiques. Cela applique un mécanisme d'authentification forte et chiffre toutes les communications entre équipements sans fil.

Chapitre 15 Leçon 2 page 804 :

Utilisez un nom valide, par exemple **EFS Basique WS08**, et utilisez les onglets de propriétés pour personnaliser son contenu. Prêtez une attention particulière à l'archivage des clés dans l'onglet Traitement de la demande et vérifiez que vous avez coché la case Archive la clé privée de chiffrement du sujet. ~~Utilisez-Cochez~~ également ~~Utiliser le-un algorithme symétrique avancé chiffrement~~ pour envoyer la clé à l'~~autorité de certification~~-CA. L'archivage de la clé privée vous permet de la protéger pour le cas où l'utilisateur la perdrait.

Chapitre 15 Leçon 2 page 805 :

- Pour utiliser des réseaux sans-fil, créez un modèle de serveur de stratégies réseau (NPS, *Network Policy Server*).

Chapitre 15 Leçon 2 page 807 :

15. Pour que les certificats soient délivrés automatiquement, sélectionnez Suivre les paramètres dans le modèle de certificats, si cela est applicable. ~~Si non~~ Dans le cas contraire, sélectionnez délivrez—~~Emettre~~ automatiquement le certificat. Cliquez sur OK.

Finaliser la configuration ~~d'une CA émettrice~~ d'un répondeur en ligne

Chapitre 15 Leçon 2 page 808 :

5. Cliquez sur l'onglet Extensions, ~~ouvrez~~ cliquez sur la liste déroulante Sélectionnez l'extension et cliquez sur Accès aux informations de l'autorité (AIA).

Chapitre 15 Leçon 2 page 809 :

23. Sélectionnez le nouveau certificat OCSP et cliquez sur ~~Inscrire~~ Inscription.
28. Dans la boîte de dialogue Sélectionnez les utilisateurs, les ordinateurs ou les groupes, cliquez sur ~~eEmplacements~~ emplacement et sélectionnez le nom du serveur local. Cliquez sur OK.

Chapitre 15 Leçon 2 page 810 :

4. Cliquez droit sur Configuration de révocation et choisissez ~~Ajout~~—~~Ajouter~~ d'une configuration de révocation.

Chapitre 15 Leçon 2 page 811 :

12. Cliquez sur Suivant.
Dans la page Sélectionner ~~un~~ le certificat utilisé pour la signature, vous devez choisir une méthode de signature parce que chaque répondeur en ligne signe chaque réponse avant de l'envoyer aux clients.

Chapitre 15 Leçon 2 page 814 :

Paramètres du Registre	5, 19, 20, 28, 95	Lié à la corruption ou à l'effacement des éléments de paramètres du <u>registre</u> <u>configuration dans la base de</u>
------------------------	-------------------	---

...

Il s'agit avant tout un outil d'exploration et de diagnostic car il affiche des informations sur le fonctionnement des membres de la hiérarchie PKI.

Chapitre 15 Leçon 2 page 819 :

2. Cliquez sur l'onglet Extensions et vérifiez que Points de distribution de liste de révocation de certificats est sélectionné dans la liste déroulante.
5. ... Pour prendre en charge les listes de révocation *via* le Web, même s'il s'agit d'un déploiement interne, vous devrez créer le répertoire virtuel dans IIS. En l'occurrence, ce n'est pas nécessaire.

Chapitre 15 Leçon 2 page 819 :

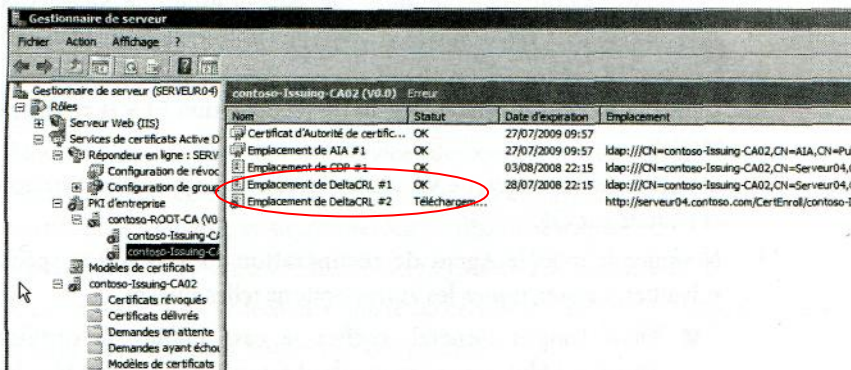
8. Dans la barre d'outils, cliquez sur Actualiser pour mettre à jour PKI d'Entreprise. Notez qu'il ne reste qu'une erreur pour la CA émettrice.

9. Pour finaliser votre configuration, allez à Contoso-Issuing-CA sous AD CS et sélectionnez Certificats délivrés. Tous les certificats émis par cette CA s'affichent dans le volet de détails.

14. Dans la boîte de dialogue Publication-Publier de la liste de révocation de certificats, sélectionnez Nouvelle liste de révocation de certificats et cliquez sur OK.

Chapitre15 Leçon 2 page 821 :

15. Attention la dernière ligne ne devrait pas apparaître



Chapitre15 Leçon 2 page 823 :

7. Cochez la case Notification d'expiration pour les utilisateurs et laissez la valeur à 10 %. Cela informera les utilisateurs que leurs certificats sont sur le point d'expirer.

1. Retournez sur SERVER04 et ouvrez une session en tant qu'administrateur de domaine.

...

3. Cliquez droit sur ~~son le nom du serveur CA émettrice, Contoso-Issuing-CA01,~~ sous Services de certificats Active Directory, Contoso-Issuing-CA01, et choisissez Propriétés.

5. Pour que les certificats soient délivrés automatiquement, sélectionnez Suivre les paramètres dans le modèle de certificats si cela est applicable. ~~Si non Dans le cas contraire, délivrez-émettrez~~ automatiquement le certificat. Cliquez sur OK. Cliquez encore sur OK pour fermer la boîte de dialogue Propriétés.

Chapitre15 Leçon 2 page 824 :

- Chaque autorité de certification qui est un répondeur en ligne doit posséder sa propre configuration de révocation, parce que chacune a son propre certificat. Pour opérer dans chaque groupe, chacune de ces certificats doit être approuvée.

Chapitre 16 Page 831 :

Les services de gestion des droits Active Directory (AD RMS, *Active Directory Rights Management Services*), connus auparavant sous le nom de Service de gestion des droits, sont conçus pour étendre la portée de votre réseau interne.

Chapitre 16 Page 832 :

AD FS étend vos stratégies AD RMS au-delà du pare-feu et prend en charge la protection de votre-la propriété intellectuelle parmi avec vos-entre partenaires commerciaux (voir figure 16-1).

Chapitre 16 Leçon 1 Page 837 :

Dans des environnements de test, vous pouvez utiliser la base de données interne ~~s~~ WID (*Windows Internal Database*) livrée avec Windows Server 2008.

Chapitre 16 Leçon 1 Page 847 :

Compte d'installation	Compte basé sur le domaine. Ne Doit <u>doit pas</u> se trouver sur une carte à puce. Doit avoir des privilèges d'administrateur local <u>local</u> . Pour générer des points de connexion au service, doit être membre du groupe Administrateurs de l'entreprise. Pour utiliser une base de données externe, vous devez être membre du rôle Administrateurs du système sur un serveur de base de données.
-----------------------	---

Chapitre 16 Leçon 1 Page 851 :

15. Dans la page Spécifier ~~un mot de passe de~~une clé de cluster AD RMS, sélectionnez le CSP à utiliser. Il peut s'agir de fournisseurs logiciels ou matériels.

Chapitre 16 Leçon 1 Page 852 :

18. ... Vous devez posséder un nom de domaine pleinement qualifié valide que vous ne pourrez plus modifier ultérieurement. Vous pouvez modifier le port par défaut sur lequel AD RMS communique depuis cette page de l'assistant. Faites-le à cette étape car vous ne pourrez plus le modifier ~~passé ce cap~~une fois l'installation terminée.

...
20. ~~Sur a~~Dans la page Choisir un certificat d'authentification serveur pour le chiffrement SSL, Sélectionnez sélectionnez Choisir un certificat existant pour le chiffrement SSL (recommandé) et choisissez le certificat que vous avez installé puis cliquez sur Suivant.

21. ~~Sur~~Dans la page Nommer le certificat de licence Sserveur, ~~Tapez~~tapez un nom valide qui vous permettra d'identifier le cluster AD RMS dans la zone Nom convivial puis cliquez sur Suivant.

22. ~~Sur~~Dans la page, Inscire un point de connexion de service AD RMS, Vérifiez~~vérifiez~~ que l'option Enregistrer le point de connexion de service AD RMS ~~est~~ maintenant ~~est~~est cochée et cliquez sur Suivant.

Chapitre 16 Leçon 1 Page 853 :

25. ~~Dans la page Confirmer les sélections pour l'installation~~Dans la page suivante, passez en revue vos choix et cliquez sur Installer.

Chapitre 16 Leçon 1 Page 854 :

5. Dans la boîte de dialogue Nouvel enregistrement de ressource, tapez le nom d'alias ~~Gestion~~des droits et assignez-le à SERVER04.contoso.com dans la section Nom de domaine pleinement qualifié (FQDN) pour l'hôte de destination. Cliquez sur OK.

Chapitre 16 Leçon 1 Page 855 :

Comme AD RMS a besoin de connexions Web SSL chiffrées, vous devez créer et installer un certificat de serveur Web avant de poursuivre l'installation.

Chapitre 16 Leçon 1 Page 856 :

4. Sélectionnez le modèle Serveur Web dans la partie volet de détails puis cliquez droit dessus pour sélectionner Modèle dupliqué.

6. Attribuez à SERVER04 les autorisations Autoriser: :Lecture et ~~Inscription~~Inscire puis cliquez sur OK.

9. Pour ~~affecter~~délivrer un modèle, cliquez du bouton droit sur Modèles de certificats, choisissez Nouveau puis sélectionnez Modèle de certificat à délivrer.

Chapitre 16 Leçon 1 Page 857 :

8. Sélectionnez le certificat Serveur Web WS2008 et cliquez sur [Plus d'informations](#)[Détails](#) pour l'inscrire.

9.

b. Dans la section Autre nom, sélectionnez l'URL dans la liste déroulante Type, tapez **Gestiondroits.contoso.com** dans le champ *Valeur* et cliquez sur [OK](#)[Ajouter](#).

Chapitre 16 Leçon 1 Page 858 :

19. Dans la page ~~suivante~~[Choisir un certificat d'authentification serveur pour le cryptage SSL](#), sélectionnez Choisir un certificat ~~existant~~ pour le chiffrement SSL (recommandé), sélectionnez le certificat SERVER04 et cliquez sur Suivant.

Chapitre 16 Leçon 1 Page 859 :

21. ~~Sur~~[Dans la page Inscrire un point de connexion de service AD RMS](#), ~~Vérifiez~~[vérifiez](#) que l'option Enregistrer le point de connexion de service AD RMS ~~est~~ maintenant ~~est~~ cochée et cliquez sur Suivant.

23. Dans la page ~~suivante~~[Sélection des services de rôle](#), conservez les sélections par défaut pour le serveur Web et cliquez sur Suivant.

24. Dans la page ~~suivante~~[Confirmer l'installation des sélections](#), passez en revue vos choix et cliquez sur Installer.

IMPORTANT Groupes d'administration AD RMS

Pour rendre opérationnels les groupes d'administration que vous avez créés dans AD DS, vous devez les ajouter à leurs groupes locaux respectifs sur ce serveur. Dans un environnement de production, vous devez accomplir ~~des~~[cette](#) ~~étapes~~ supplémentaires pour achever l'installation.

- Les utilisateurs dépendent également d'applications activées pour AD RMS pour protéger leur contenu. Il peut s'agir d'outils tels que Word, [Outlook](#), PowerPoint, Internet Explorer ou d'une application personnalisée activée pour AD RMS.

Chapitre 16 Leçon 2 Page 862 :

Créer une URL ~~de cluster~~ extranet

Chapitre 16 Leçon 2 page 866

2. Le cluster racine offre tous les services de gestion de droits Active Directory tandis que le cluster gérant uniquement ~~les~~ licences ne fait rien d'autre.

Chapitre 16 Leçon 2 page 868

4. Sous le nœud AD RMS de la console, sélectionnez Modèles de stratégie de droits (Gestionnaire de serveur\Rôle\AD RMS\NomServeur).

8. Dans la page Ajouter des droits d'utilisateur, procédez comme suit :

Aa. Cliquez sur Ajouter pour sélectionner l'utilisateur ou le groupe qui aura accès au modèle.

B. Sélectionnez Tout le monde pour que n'importe quel utilisateur puisse demander une licence d'utilisation pour ce contenu. Pour sélectionner un groupe spécifique, utilisez le bouton Parcourir.

CBb. Sous Utilisateurs et droits, sélectionnez d'abord l'utilisateur puis assignez les droits à cet utilisateur ou à un groupe particulier dans le volet Droits de l'utilisateur. Vous pouvez également créer un droit personnalisé pour l'utilisateur.

Ec. [Notez que l'autorisation Octroyer le contrôle total au propriétaire \(l'auteur\) sans date d'expiration est sélectionnée par défaut.](#)

Ed. Dans la zone URL de demande de droits, tapez l'URL appropriée. Cela permet aux utilisateurs de demander des droits supplémentaires en se rendant à l'URL

Chapitre 16 Leçon 2 page 869

11. **Bb.** Sélectionnez Demander une nouvelle licence d'utilisation à chaque accès fois que le au contenu (désactiver la mise en cache côté client)est consommé si vous voulez que les utilisateurs demandent une nouvelle licence d'utilisation à chaque fois que le contenu protégé avec ce modèle de stratégie est ouvert. Notez que cela ne fonctionne pas pour les utilisateurs hors connexion.

12. Cliquez sur Suivant. Dans la page Spécifier une stratégie de révocation, activez la révocation en sélectionnant l'option Néessite une Activer la révocation, puis :

Aa. Dans Emplacement de publication de la liste de révocation (URL ou UNC), tapez l'URL permettant d'accéder au fichier de la liste de révocation.

...

Bb. Dans Intervalle d'actualisation de la liste de révocation (jours), tapez la durée de validité (en jours) de la liste de révocation.

Chapitre 17 page 880

Le pare-feu externe idéal utilise un ensemble et un seul de ports clés et seulement cet ensemble, dont :

Chapitre 17 Leçon 1 page 893

Le serveur de fédération de comptes peut interroger le magasin de l'annuaire interne et les fournir à un partenaire de ressource.

Chapitre 17 Leçon 1 page 896

La clé publique est également stockée sur le ou les serveur(s) de fédération et dans les stratégies d'approbation. Quand vous travaillez avec ce type de certificat dans la console AD FS, ils sont appelés certificats proxys du service de fédération.

AD FS peut aisément utiliser AD CS pour obtenir et gérer ces certificats. Toutefois, comme de nombreux rôles AD FS sont tournés vers l'extérieur, vos certificats doivent provenir d'une autorité de certification approuvée. Sinon, yvous devrez done modifier le magasin des autorités de certification approuvées sur chaque client web.

Chapitre 17 Leçon 1 page 900

WS-Fédération	Spécification de serveur web qui décrit les <u>normés-normes</u> à utiliser pendant la mise en œuvre de la fédération.
---------------	--

Etant-Étant donné la nature d'AD FS, les horloges des ordinateurs doivent être synchronisés ou ne doivent jamais avoir moins-plus de cinq minutes de différence entre elles ; dans le cas contraire, le processus ne fonctionnera pas car les tampons d'heurel'horodatage des jetons ne seront-sera pas valides.

Chapitre 17 Leçon 1 page 906

10. Dans la page Choisir-Sélectionner une stratégie d'approbation, sélectionnez Créer une nouvelle stratégie d'approbation et cliquez sur Suivant.

Chapitre 17 Leçon 1 page 907

Exercice 3 : Installer les proxys du service de fédération.

Dans cet exercice, vous allez installer les ~~serveurs proxys du service~~ de fédération.

7. Dans la page Choisir des services de rôle, sélectionnez Proxy du ~~serveur service~~ de fédération et cliquez sur Ajouter les services de rôle requis. Sélectionnez également Agents Web AD FS et cliquez sur Suivant.

11. Dans la page Choisir un certificat de d'authentification client, choisissez Créer un certificat d'authentification client auto-signé et cliquez sur Suivant.

Chapitre 17 Leçon 2 page 915

7. Lancez les Services ~~de fédération~~AD FS (Active Directory Federation Services) ~~depuis~~ le ~~groupe~~ ~~de programmes~~ -Outils d'administration.

8. Cliquez droit sur Service de fédération et choisissez Propriétés dans l'onglet Général. Cliquez sur ~~Affichage~~Afficher.

Chapitre 17 Leçon 2 page 916

4. Dans ~~l'affichage Liste~~Affichage des fonctionnalités, double-cliquez sur Certificats de serveur dans la section IIS.

Chapitre 17 Leçon 2 page 917

5. Double-cliquez sur le certificat ~~de l'autorité de certification racine~~ContosoContoso-ROOT-CA et cliquez sur l'onglet Détails.

6. Dans l'onglet Détails, cliquez sur Copier dans un fichier. Cliquez sur Suivant.

...

4. Dans ~~l'affichage Liste~~Affichage des fonctionnalités, double-cliquez sur Certificats de serveur dans la section IIS.

5. Double-cliquez sur le certificat ~~de l'autorité de certification émettrice~~ContosoContoso-Issuing-CA et cliquez sur l'onglet Détails.

Chapitre 17 Leçon 2 page 918

4. Dans ~~l'affichage Liste~~Affichage des fonctionnalités, double-cliquez sur Certificats de serveur dans la section IIS.

...

4. Dans ~~l'affichage Liste~~Affichage des fonctionnalités, double-cliquez sur Certificats de serveur dans la section IIS.

Chapitre 17 Leçon 2 page 919

2. Cliquez du bouton droit sur le ~~site~~certificat et sélectionnez Copier.

3. Dans la barre d'adresses située en haut de ~~la fédération de~~l'Explorateur Windows, tapez \\SERVER03.Contoso.com\temp.

...

4. Choisissez Le compte de l'ordinateur et cliquez sur Suivant. Assurez-vous que Ordinateur local est sélectionné, cliquez sur Terminer puis sur OK. Enregistrez la console.

5. Dans le menu Fichier, choisissez Enregistrer sous, localisez le dossier Documents et nommez-~~la le~~ Certificats ordinateur.

Chapitre 17 Leçon 2 page 921

2. Lancez les Services ~~de fédération~~ADFS depuis le groupe de programmes Outils d'administration.

Chapitre 17 Leçon 2 page 922

2. Cliquez droit sur Magasins de comptes, choisissez Nouveau puis choisissez Magasin de comptes.
4. Dans la page Type de magasin de comptes, choisissez Services de domaine Active Directory (AD DS) et cliquez sur Suivant.

Notez que l'on ne peut associer qu'un seul magasin de compte à une implémentation AD FS. Toutefois, il est possible d'ajouter des magasins AD LDS ainsi en même temps que le magasin AD DS.

2. Lancez les Services ~~de fédération~~ADES depuis le groupe de programmes Outils d'administration.

Chapitre 17 Leçon 2 page 923

4. Dans la page Type de magasin de comptes, sélectionnez Services de domaine Active Directory (AD DS) et cliquez sur Suivant.

Chapitre 17 Leçon 2 page 925

8. Dans la page Détails sur le partenaire de comptes, lisez les informations, puis cliquez sur Suivant...
9. Dans la page Certificat de vérification du partenaire de comptes, assurez-vous que l'option indiquant d'utiliser le certificat de vérification contenu dans le fichier ~~d'importation~~ de la stratégie d'importation est cochée et cliquez sur Suivant.
11. Dans la page ~~Affirmations~~Revendications d'identité de partenaires de comptes, sélectionnez Revendication UPN et Revendication d'identité (courrier électronique) sont sélectionnées et cliquez sur Suivant.
14. Dans la page Activer ce partenaire de comptes, assurez-vous que la case Activer ce partenaire de comptes est cochée et cliquez sur Suivant.

Chapitre 17 Leçon 2 page 926

1. Cliquez droit sur Contoso sous le nœud Partenaires de compte, choisissez Nouveau puis Mappage de revendications de groupe entrantes.
2. Dans la boîte de dialogue Créer un nouveau mappage de revendications de groupe entrantes, tapez **Revendication Application Woodgrove Bank**. Assurez-vous que Revendication Application Woodgrove Bank est sélectionné dans la liste déroulante et cliquez sur OK.

Chapitre 17 Leçon 2 page 927

15. Dans la page ~~Affirmations~~Revendications d'identité de partenaires de ressources, assurez-vous que Revendication de nom UPN et Revendication d'identité (courrier électronique) sont sélectionnées et cliquez sur Suivant.
16. Dans la page Sélectionner ~~le un~~ suffixe UPN, assurez-vous que l'option Remplacer tous les suffixes UPN par est sélectionnée et que contoso.com est le suffixe UPN qui apparaît dans la liste. Cliquez sur Suivant.
- ...
17. Dans la page Sélectionner ~~le un~~ suffixe d'adresse de messagerie, assurez-vous que l'option Remplacer tous les suffixes d'adresses de messagerie par est sélectionnée et que contoso.com est le suffixe de messagerie qui s'affiche. Cliquez sur Suivant.
18. Dans la page Activer ce partenaire de ressources, assurez-vous que la case Activer ce partenaire de ressources est cochée et cliquez sur Suivant.