## **ACTIVE DIRECTORY : WINDOWS SERVER 2012 R2**

Source : http://www.it-connect.fr/creer-un-domaine-sous-windows-server-2012/

#### Installation du rôle ADDS

Avant de promouvoir le serveur en tant que contrôleur de domaine dans un nouveau domaine, il faut installer le rôle « Service de domaine Active Directory ».

Pour cela, dans la page d'accueil, cliquez sur « Gestionnaire de serveur ». Une fois que vous y êtes, cliquez sur « Ajouter des rôles et des fonctionnalités » présent dans la section « Démarrage rapide ».

E.	Gestionnaire de se	rveur	_ <b>D</b> X
<ul> <li>► Tableau de bord</li> <li>Erveur local</li> <li>Tous les serveurs</li> <li>AD DS</li> <li>DNS</li> <li>Services de fichiers et d ▷</li> </ul>	Gestionnaire de se de bord Performances Résultats BPA Tous les serveurs 1 • Facilité de gestion Événements Services Performances Résultats BPA	rveur       • ②       I       Performances       Résultats BPA	Gérer Outils Afficher Aide Ajouter des rôles et fonctionnalités Supprimer des rôles et fonctionnalités Ajouter des serveurs Créer un groupe de serveurs Propriétés du Gestionnaire de serveur
	Résultats BPA		=

L'assistant s'exécute et vous demande de vous assurer que le compte Administrateur possède un mot de passe fort, que la configuration réseau est en adresse statique et que votre serveur est à jour au niveau des mises à jour de sécurité. Cliquez sur « Suivant ».

à	Assistant Ajout de rôles et de fonctionnalités
Avant de comme	SERVEUR DE DESTINATION SRV12R2-DC1-XC/prevert-XClocal
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web. Pour supprimer des rôles, des services de rôle ou des fonctionnalités : Démarrer l'Assistant Suppression de rôles et de fonctionnalités Avant de continuer, vérifiez que les travaux suivants ont été effectués : • Le compte d'administrateur possède un mot de passe fort • Les paramètres réseau, comme les adresses IP statiques, sont configurés • Les dernières mises à jour de sécurité de Windows Update sont installées Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant. Cliquez sur Suivant pour continuer.
	< Précédent Suivant > Installer Annuler

Laissez le choix par défaut puisque nous souhaitons ajouter un nouveau rôle à notre serveur et non installer des services de Bureau à distance comme le propose le second choix.



Sélectionner le serveur de destination dans la liste indiquée et cliquer sur « Suivant ». Ceci est une nouveauté de Windows Server 2012 qui permet à partir d'un serveur de gérer plusieurs autres serveurs qui sont configurés pour être gérés par un autre serveur. Dans notre cas, il n'y a qu'un seul serveur, le choix est donc restreint.

à		Assistant Ajout de rôles et de fonctionnalités		
0	Sélectionner le se	rveur de destination SRV12R2-DC1-XX, prevent-XXLIOCAI		
	Avant de commencer	Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.		
	Type d'installation	<ul> <li>Sélectionner un serveur du pool de serveurs</li> </ul>		
	Sélection du serveur	○ Sélectionner un disque dur virtuel		
	Rôles de serveurs	Pool de serveurs		
	Fonctionnalités			
	Confirmation	Filtre :		
		Nom Adresse IP Système d'exploitation		
		SRV12R2-DC1-XX.prever 192.168.1.54 Microsoft Windows Server 2012 R2 Standard		
		1 ordinateur(s) trouvé(s)		
		Cette page presente les serveurs qui executent Windows Server 2012 et qui ont ete ajoutes a l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors ligne et les serveurs		
		nouvellement ajoutés dont la collection de données est toujours incomplète ne sont pas répertoriés.		
_				
		< Précédent Suivant > Installer Annuler		

Au niveau des rôles, sélectionnez «Service AD DS» qui correspond au service de domaine Active Directory en cochant la case. Une fenêtre va apparaître pour vous indiquer que d'autres éléments requis par AD DS doivent être installés, cliquez sur « Ajouter des fonctionnalités ». Ensuite, cliquez sur « Suivant ».

🚡 Assistant Ajout de rôles et de fonctionnalités 📃 🗖 🗙				
Sélectionner des rôles de serveurs serveur de serveur de serveur de destination serveur des rôles de serveurs				
Avant de commencer Type d'installation	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélec	ctionné.		
Sélection du serveur Rôles de serveurs Fonctionnalités AD DS Confirmation Résultats		Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.		
	< Précédent Suivan	t > Installer Annuler		

Au niveau des fonctionnalités, nous avons besoin de rien, cliquez sur « Ajouter des fonctionnalités » puis sur « Suivant » directement.

Assistant Ajout de rôles et de fonctionnalités	Assistant Ajout de rôles et de fonctionnal	ités 📃 🗖 🗙
Assistant Ajout de rôles et de fonctionnalités Assistant Ajout de rôles et de fonctionnalités Ajouter les fonctionnalités requises pour Services AD DS ? Vous ne pouvez pas installer Services AD DS sauf si les services de rôle ou les fonctionnalités suivants sont également installés. [Outils] Gestion de stratégie de groupe Outils d'administration de rôles Outils AD DS et AD LDS Module Active Directory pour Windows PowerShell Outils] Coutils] Centre d'administration Active Directory [Outils] Composants logiciels enfichables et outils e Im Ajouter les outils de gestion (si applicable) Ajouter des fonctionnalités Annuler	Assistant Ajout de rôles et de fonctionnal      Sélectionner des fonctionnalités      Avant de commencer      Type d'installation     Sélection du serveur     Rôles de serveurs      Fonctionnalités      AD DS      Confirmation     Résultats      Sélection d'impression Internet     Client d'impression Internet     Client TFTP     Clustering avec basculement     Compression differentielle à distance     Data Center Bridging     Deverrouillage réseau BitLocker     Diata Center Bridging     Deverrouillage réseau BitLocker     DirectPlay	ités       Image: Construction of the serveur sélectionné.         SRV12R2-DC1-XXCprevert-XClocal         ur le serveur sélectionné.         Description         Grâce à l'assistance à distance, vous (ou une personne du support technique) pouvez aidre les utilisateurs à résoudre leurs problèmes ou à répondre à leurs questions en rapport avec leur PC. Vous pouvez afficher et prendre le contrôle du Bureau des utilisateurs pour dépanner et résoudre les problèmes. Les utilisateurs ont également la possibilité de solliciter l'aide de leurs amis ou de leurs collègues de travail.
	C III	
	< Précédent S	uivant > Installer Annuler

Lisez les explications concernant AD DS et cliquez sur « Suivant » à nouveau.



Un récapitulatif des éléments qui vont être installés et affichés, cliquez sur « Installer » pour exécuter l'installation des divers éléments.

<b>a</b>	Assistant Ajout de rôles et de fonctionnalités				
Confirmer les sé	ections d'installation SRV12R2-DC1-XX, prevent-XX, local				
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités	Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer. Redémarrer automatiquement le serveur de destination, si nécessaire Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.				
AD DS Confirmation Résultats	Gestion de stratégie de groupe Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS et AD LDS Module Active Directory pour Windows PowerShell Outils AD DS Centre d'administration Active Directory Composants logiciels enfichables et outils en ligne de commande AD DS Services AD DS Exporter les paramètres de configuration				
	Spécifier un autre chemin d'accès source           < Précédent				

Une fois terminé c'est-à-dire que le message «Installation réussie sur SRV12R2-DC1-XX» apparaît, cliquez sur «Fermer».

2	Assistant Ajout de rôles et de fonctionnalités			
Progression de l'i	nstallation serveur de destination srv12r2-dc1-xxcprevent-xxclocal			
Avant de commencer	Afficher la progression de l'installation			
Type d'installation	i Installation de fonctionnalité			
Sélection du serveur				
Rôles de serveurs	Installation démarrée sur SRV12R2-DC1-XX.prevert-XX.local			
Fonctionnalités	Gestion de stratégie de groupe			
AD DS	Outils d'administration de serveur distant			
Confirmation	Outils d'administration de rôles			
Résultats	Outlis AD DS et AD LDS Module Active Directory pour Windows PowerShell			
	Outils AD DS			
	Centre d'administration Active Directory			
	Composants logiciels enfichables et outils en ligne de commande AD DS			
	Services AD DS			
Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche. Exporter les paramètres de configuration				
	< Précédent Suivant > Fermer Annuler			

## Promouvoir en tant que contrôleur de domaine

Afin de promouvoir notre serveur en tant que contrôleur de domaine, vous avez l'habitude d'effectuer la commande « dcpromo » qui permet d'exécuter l'assistant de promotion de serveur.

Avec Windows Server 2012, dans le Gestionnaire de serveur un symbole d'avertissement apparaît auprès du Centre de maintenance, cliquez dessus et vous verrez apparaître ceci :



Il vous suffit de cliquer sur «Promouvoir ce serveur en contrôleur de domaine» pour exécuter l'équivalent d'un DCPROMO sous Windows Server 2012.

Vu que nous souhaitons créer un nouveau domaine appelé «**prevert-xx.local**», nous devons déployer une nouvelle forêt (une forêt étant un ensemble de domaines, ce qui permet d'ajouter d'autres domaines dans cette forêt par la suite). Cochez « Ajouter une nouvelle forêt » et indiquez «**prevert-xx.local**».

📥 Assistant Configuration des services de domaine Active Directory 📃 🗕 🗖 🗙			
Assi       Configuration de déploie       Options du contrôleur de       Options supplémentaires       Chemins d'accès       Examiner les options       Vérification de la configur       Installation       Résultats	stant Configuration des services de domaine Active D déploiement Sélectionner l'opération de déploiement Ajouter un contrôleur de domaine à un domaine existant Ajouter un nouveau domaine à une forêt existante Ajouter une nouvelle forêt Spécifiez les informations de domaine pour cette opération Nom de domaine racine : prevert-XX.loca	SERVEUR CIBLE SRV12R2-DC1-XX.prevert-XX.local	
	En savoir plus sur la configurations de déploiement Précédent	Installer Annuler	

Note: Un domaine créé à partir d'un serveur Windows Server 2012R2 peut fonctionner uniquement sur un niveau fonctionnel «Windows Server 2012R2». Cependant, le niveau fonctionnel de la forêt quant à lui peut aller de « Windows Server 2003 » à «Windows Server 2012R2».

Choisissez le niveau fonctionnel qui vous convient le mieux pour la forêt. Cela dépend de ce que vous prévoyez à l'avenir, dans le cas où vous créez d'autres domaines dans cette forêt vous allez devoir adaptez le système d'exploitation embarqué par vos serveurs par rapport au niveau fonctionnel sélectionné. Pour information, on peut augmenter le niveau fonctionnel, mais en aucun cas le diminuer.

Sélectionner «Windows Server 2012R2» pour les deux niveaux fonctionnels. Laissez coché «Serveur DNS» puisque ce serveur servira également de serveur DNS sur le domaine et indiquez un mot de passe de restauration des services d'annuaires. Une fois que tout est renseigné, cliquez sur «Suivant»

🚡 Assis	tant Configuration des services de domaine Active Directory
Options du contro	SERVEUR CIBLE SRV12R2-DC1-XX.prevert-XX.local
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine         Niveau fonctionnel de la forêt :       Windows Server 2012 R2         Niveau fonctionnel du domaine :       Windows Server 2012 R2         Spécifier les fonctionnalités de contrôleur de domaine         Serveur DNS (Domain Name System)         Catalogue global (GC)         Contrôleur de domaine en lecture seule (RODC)         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
	< Précédent Suivant > Installer Annuler

En ce qui concerne les options DNS, faites suivant puisqu'il n'y a aucune modification à effectuer. Ensuite, patientez pendant l'affichage du nom NETBIOS de votre domaine et modifiez le si nécessaire, le nom NETBIOS permet notamment d'ouvrir une session et de s'authentifier sur le domaine. Exemple, ouvrir une session «user1» sur le domaine «prevert-XX.local» ayant pour nom NETBIOS «PREVERT» : «PREVERT\user1».

🚡 Ass	istant Configuration des services de domaine Active Dire	ctory 🗕 🗖 🗙	
Options DNS	S	SERVEUR CIBLE RV12R2-DC1-XX.prevert-XX.local	
Il est impossible de créer	une délégation pour ce serveur DNS car la zone parente faisant autorité	é est intro Afficher plus 🛛 🗙	
Configuration de déploie Options du contrôleur de Options DNS	Spécifier les options de délégation DNS		
Options supplémentaires			Options DNS X
Chemins d'accès			
Examiner les options Vérification de la configur Installation Résultats		Il est impossible de cr zone parente faisant a serveur DNS Windows infrastructure DNS exi délégation avec ce se résolution de noms fi Sinon, aucune action	téer une délégation pour ce serveur DNS car la sutorité est introuvable ou elle n'exécute pas le s. Si vous procédez à l'intégration avec une istante, vous devez manuellement créer une rveur DNS dans la zone parente pour activer une able en dehors du domaine « btssio1a-xx.local ». n'est requise.
			ОК
	En savoir plus sur la Délégation DNS		
	< Précédent Suivant >	Installer Annuler	

🚡 Assi:	stant Configuration des services	de domaine Active Directory	_ 🗆 X
Options supplém	entaires	SRV12R2-D0	SERVEUR CIBLE C1-XX.prevert-XX.local
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Vérifiez le nom NetBIOS attribué au	domaine et modifiez-le si nécessaire. PREVERT-XX	
	En savoir plus sur la options supplén	nentaires Précédent Suivant > Insta	iller Annuler

Lorsqu'on vous demande de choisir les différents chemins d'accès pour le dossier SYSVOL, la base de données et les fichiers journaux, laisser les paramètres par défaut afin de rester standard et d'être sûr de pouvoir les retrouver facilement.

🚡 Assis	tant Configuration des services	de domaine Active Directory
Chemins d'accès		SERVEUR CIBLE SRV12R2-DC1-XX.prevert-XX.local
Configuration de déploie Options du contrôleur de	Spécifier l'emplacement de la base d	e données AD DS, des fichiers journaux et de SYSVOL
Options DNS	Dossier de la base de données :	C:\Windows\NTDS
Options supplémentaires	Dossier des fichiers journaux :	C:\Windows\NTDS
Chemins d'accès	Dossier SYSVOL :	C:\Windows\SYSVOL
Examiner les options		
Vérification de la configur		
Installation		
Résultats		
	En savoir plus sur la Chemins d'accès	Active Directory
	<	Précédent Suivant > Installer Annuler

🚡 Assi	stant Configuration des services de domaine Active Directory	_ 🗆 X	
Examiner les opti	ons srv12r2-dc1-3	SERVEUR CIBLE XX.prevert-XX.local	
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Vérifiez vos sélections : Configurez ce serveur en tant que premier contrôleur de domaine Active Directe nouvelle forêt. Le nouveau nom de domaine est « prevert-XX.local ». C'est aussi le nom de la n Nom NetBIOS du domaine : PREVERT-XX Niveau fonctionnel de la forêt : Windows Server 2012 R2 Niveau fonctionnel du domaine : Windows Server 2012 R2 Options supplémentaires : Catalogue global : Oui Serveur DNS : Oui Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires	ory d'une ∧ ouvelle forêt.	
	En savoir plus sur la options d'installation	Fichier Edition F	t Format A
	< Précédent Suivant > Installe	r # Script Windo # Import-Module Install-ADDSFd -CreateDnsDelt -DatabasePath -DomainMode "I -DomainName "; -DomainName "; -ForestMode "I -InstallDns:\$ -LogPath "C:\I	ADDSE orest egatic "C:\V Win201 prever sName Win201 true Win201 true

- 🗆 X

-NoRebootOnCompletion:\$false ` -SysvolPath "C:\Windows\SYSVOL" ` -Force:\$true

Cliquez sur « Suivant », puis examinez une dernière fois les options que vous avez définies dans la page récapitulative. Une fois que le tour est fait, cliquez une seconde fois sur « Suivant ». Enfin, vérifiez qu'il n'y a pas d'erreur(s) critique(s) et cliquez sur « Installer ». Le serveur redémarrera automatiquement une fois le déploiement terminé.

<b>b</b> /	Assistant Configuration des services de domaine Active Directory	
Vérification de	la configuration requise SRV12R2-DC1-XX,prevert-XX.local	
Voutes les vérifications	s de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commeAfficher plus 🛛 🗙	
Configuration de déploi Options du contrôleur c	e La configuration requise doit être validée avant que les services de domaine Active Directory soient le installés sur cet ordinateur	
Options DNS	Réexécuter la vérification de la configuration requise	
Options supplémentaire	15	
Chemins d'accès	<ul> <li>Voir les résultats</li> </ul>	
Examiner les options	▲ Les contrôleurs de domaines Windows Server 2012 R2 offrent un paramètre sécurisé	
Vérification de la config	Jr Windows NT 4.0 ». Ce paramètre empêche l'utilisation des algorithmes de chiffrement	
	faibles dans des sessions sur canal sécurisé.	
	Pour plus de détails à ce sujet, voir l'article 942564 de la Base de connaissances (http:// go.microsoft.com/fwlink/?Linkld=104751).	
	Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez	
	Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.	
	En savoir plus sur la conditions préalables	
	< Précédent Suivant > Installer Annuler	

nstallation	SERVEUR C SRV12R2-DC1-XX.prevert-XX.k
Configuration de déploie Options du contrôleur de Options DNS	État d'avancement Création en cours de la partition d'annuaire : CN=Configuration,DC= <b>prevert-XX</b> ,DC=local; 0 ob restants Afficher les résultats détaillés de l'opération
Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	<ul> <li>▲ Les contrôleurs de domaines Windows Server 2012 R2 offrent un paramètre sécurisé par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empéche l'utilisation des algorithmes de chiffrement faibles dans des sessions sur canal sécurisé.</li> <li>Pour plus de détails à ce sujet, voir l'article 942564 de la Base de connaissances (http:// go.microsoft.com/fivlink/?Linkld=104751).</li> <li>▲ Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a été attribuée à ses propriétés IP. Si IPv4 et IPv6 sont tous deux activés pour une carte réseau, vous devez attribuer des adresses IP statiques l'Av4 et IPv6 de la carte réseau physique. Ces affectations d'adresses IP statiques d'uter être effectuées sur toutes les cartes réseau physiques pour que l'opération DNS soit fiable.</li> <li>▲ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente</li> </ul>
	faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez En savoir plus sur la options d'installation <pre></pre>

# Vous allez être déconnecté L'ordinateur est redémarré car les services de domaine Active Directory ont été installés ou supprimés.

Une fois le serveur redémarré, connectez-vous avec le compte Administrateur présent désormais dans l'Active Directory et commencez à administrer votre domaine.

Autre utilisateur
Nom d'utilisateur
Mot de passe -
Connexion à : PREVERT-XX
Comment me connecter à un autre domaine ?

Vous devez vérifier une nouvelle fois le paramétrage du serveur DNS dans la connexion réseau. Le DNS préféré doit pointer sur le serveur A.D. :

Propriétés de : Protocole Internet version 4 (TCP/IPv4)					
Général					
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.					
Obtenir une adresse IP automatio	quement				
• Utiliser l'adresse IP suivante :					
Adresse IP :	192 . 168 . 1 . 200				
Masque de sous-réseau :	255 . 255 . 255 . 0				
Passerelle par défaut : 192 . 168 . 1 . 1					
Obtenir les adresses des serveurs DNS automatiquement					
• Utiliser l'adresse de serveur DNS suivante :					
Serveur DNS préféré :	127.0.0.1				
Serveur DNS auxiliaire :					
Valider les paramètres en quittant Avancé					
OK Annuler					

Sur l'image écran, le serveur DNS préféré est : 127.0.0.1. C'est l'IP de bouclage correspondant bien au serveur. On peut aussi utiliser l'IP : 192.168.1.200

Vous pouvez constater que l'outils système N'existe plus dans la gestion de l'ordinateur

#### > M Utilisateurs et groupes locaux

۲

\_ 🗆 🗙 æ Gestion de l'ordinateur Fichier Action Affichage ? 🗢 🄿 🔲 🖬 🔂 🔙 Gestion de l'ordinateur (local) Nom Actions 🔺 👔 Outils système 👔 Outils système Gestion de l'ordinateu... 🔺 Planificateur de tâches Stockage Autres actions Observateur d'événements Services et applications Dossiers partagés
 Performance 📇 Gestionnaire de périphériques ⊿ 🔮 Stockage A Marcel Sauvegarde Windows Server 📄 Gestion des disques Services et applications

C'est maintenant Utilisateur et ordinateur Active Directory qui prend en charge les utilisateurs

Ш

<

	h	Gestionnaire de serveur	
Corbeille	🗲 🗧 🛯 • • Tableau	de bord 🔹 🕄 l 🚩 Gére	er <mark>Outils</mark> Afficher Aide
	<ul> <li>Tableau de bord</li> <li>Serveur local</li> <li>Tous les serveurs</li> <li>AD DS</li> <li>DNS</li> <li>Services de fichiers et d ▷</li> </ul>	Rôles et groupes de serveurs :       I         Rôles : 3       Groupes de serveurs : 1       Nombre total de :         Image: Construction of the serveurs in th	Configuration du système Défragmenter et optimiser les lecteurs Diagnostic de mémoire Windows DNS Domaines et approbations Active Directory Gestion de l'ordinateur Gestion des stratégies de groupe Informations système Initiateur iSCSI Module Active Directory pour Windows PowerShell Monification ADSI Module Active Directory pour Windows PowerShell Moniteur de ressources Nettoyage de disque Observateur d'événements
		DNS 1 Facilité de gestion	Pare-feu Windows avec fonctions avancées de sécurité Planificateur de tâches Sauvegarde Windows Server Services Services de composants
			Sites et services Active Directory Sources de données ODBC (32 bits) Sources de données ODBC (64 bits) Stratégie de sécurité locale Utilisateurs et ordinateurs Active Directory Windows PowerShell Windows PowerShell (x86) Windows PowerShell ISE
			▲ 🕞 😢 🕼 23:14 12/10/2016

	Utilisateurs	et ordinateurs	Active Directory		- 🗆 X
Fichier Action Affichage ? Fichier Action Affichage ? Utilisateurs et ordinateurs Active Recuétes enregistrées Fichier Active Fichier Act	Utilisateurs	et ordinateurs	Active Directory          Description         Default container for up         Default container for do         Default container for sec         Default container for up         Default container for up		
< III >				1	

Les unités d'organisation peuvent contenir des utilisateurs, des groupes, des ordinateurs, des imprimantes, des dossiers partagés et une quantité illimitée d'autres unités d'organisation, mais elles ne peuvent pas contenir d'objets d'autres domaines.

Le compte administrateur se trouve dans l'OU Users

Utilisateurs et ordinateurs Active Directory					
Fichier Action Affichage ?					
← ⇒ 2 🖬 ¼ 📋 🗙 🖻 Q 🕞 🛛 🖬 🗏 📚 🖆 🍸 🗵 🍇					
<ul> <li>Utilisateurs et ordinateurs Active Directory [SRV12R</li> <li>Requêtes enregistrées</li> <li>Prevert-XX.local</li> <li>Computers</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipals</li> <li>Managed Service Accounts</li> <li>Users</li> </ul>	Administrateur Administrateur Administrateurs de l'entreprise Administrateurs du schéma Administrateurs du schéma Administrateurs du schéma Contrôleurs de domaine Contrôleurs de domaine d'ent Contrôleurs de domaine d'ent Contrôleurs de domaine en le Contrôleurs de domaine en le Contrôleurs de domaine en le Contrôleurs de certificats Contrôleurs de certificats Groupe de réplication dont le Groupe de réplication dont le Contrôleurs du domaine Cordinateurs du domaine Protected Users Serveurs RAS et IAS Utilisateurs du domaine	Type Utilisateur Groupe de sécurité Groupe de sécurité	Description Compte d'utilisateur d'administration Administrateurs désignés de l'entreprise Administrateurs désignés du schéma Administrateurs désignés du schéma Administrateurs désignés du domaine Tous les contrôleurs de domaine du d Les membres de ce groupe qui sont d Les membres de ce groupe sont des c Groupe des administrateurs DNS Les clients DNS qui sont autorisés à ef Les membres de ce groupe ont l'autor Les membres de ce groupe ont l'autor Les methes de ce groupe ont l'autor Les mots de passe des membres de ce Compte d'utilisateur invité Tous les invités du domaine Toutes les stations de travail et les ser Les membres de ce groupe peuvent Les membres de ce groupe peuvent Les membres de ce groupe peuvent Les membres de ce groupe bénéficien Les membres de ce groupe peuvent ac Tous les utilisateurs du domaine		
		Groupe de securite	wembers of this group can access W		

Le groupe Utilisateur se trouve dans l'OU Builtin ce sont des groupes intégrés

Utilisateurs et ordinateurs Active Directory					
Fichier Action Affichage ?					
⇔ ⇒ 2 💼 🗉 🗟 💀 🛛 🖬 % 🗞 🖆 🍸 💆 🎘					
Utilisateurs et ordinateurs Active Directory [SRV12R	Nom	Туре	Description		
Requêtes enregistrées	& Accès compatible pré-Windows	Groupe de sécurité	Un groupe de compatibilité des		
⊿ 🚔 prevert-XX.local	& Accès DCOM service de certificats	Groupe de sécurité	Les membres de ce groupe son		
🛗 Builtin	& Administrateurs	Groupe de sécurité	Les membres du groupe Admi		
Computers	& Administrateurs Hyper-V	Groupe de sécurité	Les membres de ce groupe dis		
Domain Controllers	& Duplicateurs	Groupe de sécurité	Prend en charge la réplication		
ForeignSecurityPrincipals	& Générateurs d'approbations de f	Groupe de sécurité	Les membres de ce groupe peu		
Managed Service Accounts	& Groupe d'accès d'autorisation W	Groupe de sécurité	Les membres de ce groupe ont		
Users	& IIS_IUSRS	Groupe de sécurité	Groupe intégré utilisé par les se		
	🍇 Invités	Groupe de sécurité	Les membres du groupe Invités		
	& Lecteurs des journaux d'événem	Groupe de sécurité	Des membres de ce groupe pe		
	💐 Opérateurs d'impression	Groupe de sécurité	Les membres peuvent administ		
	& Opérateurs d'assistance de contr	Groupe de sécurité	Les membres de ce groupe peu		
	용 Opérateurs de chiffrement	Groupe de sécurité	Les membres sont autorisés à e		
	💐 Opérateurs de compte	Groupe de sécurité	Les membres peuvent administ		
	& Opérateurs de configuration rés	Groupe de sécurité	Les membres de ce groupe peu		
	🍇 Opérateurs de sauvegarde	Groupe de sécurité	Les membres du groupe Opéra		
	🍇 Opérateurs de serveur	Groupe de sécurité	Les membres peuvent administ		
	💐 Serveurs Accès Distant RDS	Groupe de sécurité	Les serveurs de ce groupe perm		
	& Serveurs de licences des services	Groupe de sécurité	Les membres de ce groupe peu		
	💐 Serveurs Gestion RDS	Groupe de sécurité	Les serveurs de ce groupe peuv		
	Serveurs RDS Endpoint	Groupe de sécurité	Les serveurs de ce groupe exéc		
	& Utilisateurs	Groupe de sécurité	Les utilisateurs ne peuvent pas		
	Utilisateurs de gestion à distance	Groupe de sécurité	Les membres de ce groupe ont		
	🎎 Utilisateurs de l'Analyseur de per	Groupe de sécurité	Les membres de ce groupe peu		
	🍇 Utilisateurs du Bureau à distance	Groupe de sécurité	Les membres de ce groupe dis		
	🎎 Utilisateurs du journal de perfor	Groupe de sécurité	Les membres de ce groupe peu		
< III >	🎎 Utilisateurs du modèle COM dist	Groupe de sécurité	Les membres sont autorisés à l		
,					

## Sécurisation des comptes d'utilisateurs

Si un administrateur réseau ne modifie pas les droits et autorisations des comptes intégrés, un utilisateur (ou service) malveillant peut les utiliser pour ouvrir illégalement une session sur un domaine à l'aide des comptes Administrateur ou Invité. Pour assurer la protection de ces comptes, il est recommandé de les renommer ou de les désactiver. Dans la mesure où un compte renommé conserve son identificateur de sécurité (SID, Security Identifier), il conserve également toutes ses autres propriétés, comme la description, le mot de passe, l'appartenance à des groupes, le profil utilisateur, les informations sur le compte ainsi que les autorisations et les droits qui lui ont été accordés.

Pour bénéficier de la sécurité de l'autorisation et de l'authentification de l'utilisateur, utilisez le Centre d'administration Active Directory pour créer un compte pour chaque utilisateur qui participe à votre réseau. Vous pouvez ensuite ajouter chaque compte d'utilisateur (y compris le compte Administrateur et le compte Invité) à un groupe pour contrôler les droits et les autorisations qui sont affectés au compte. Lorsque vous disposez des comptes et des groupes appropriés pour votre réseau, vous pouvez identifier les utilisateurs qui se connectent à votre réseau et leur donner accès uniquement aux ressources autorisées.

Vous pouvez contribuer à protéger votre domaine contre les pirates en exigeant des mots de passe forts et en mettant en œuvre une stratégie de verrouillage de compte. Les mots de passe forts réduisent le risque de leur décodage intelligent et des attaques par dictionnaire sur les mots de passe. Une stratégie de verrouillage de compte contribue à diminuer les risques d'attaques sous la forme de tentatives répétées d'ouverture de session, pouvant porter atteinte à votre domaine. Une telle stratégie détermine le nombre possible d'échecs de tentatives d'ouverture de session pour un compte d'utilisateur avant sa désactivation.

Malgré toutes ces recommandations nous allons désactiver les exigences de complexités de mot de passe afin de rendre la création des comptes utilisateurs plus simple.

#### Désactiver les exigences de complexité du mot de passe

À l'installation du service AD DS, les paramètres de sécurité sont réinitialisés (Exigences de complexité du mot de passe, durée de vie minimale, ...). Si vous souhaitez modifier ces paramètres, procédez de la manière suivante :



=> Lancer le gestionnaire de serveur / Outils /Gestion des stratégies de groupe

- => Développez la "Forêt".
- => Sélectionnez votre domaine.
- =>Clique droit, sur "Default Domain Policy".
- => Sélectionnez l'option "Modifer".

k Fichier Action Affichage Fenêtre ?
b i Objets Appliqué Lien activé Chemin d'accès
Construction of the second secon
Ajouter       Supprimer       Propriétés         Filtrage WMI

=> Développez la stratégie "Configuration ordinateur" => "Stratégies" => "Paramètres Windows" => "Paramètres de sécurité" => "Stratégies de comptes".

=> Sélectionnez "Stratégie de mot de passe".

Fichier Action Affichage ?	
Configuration ordinateur Configuration ordinateur Stratégies Paramètres du logiciel Paramètres du logiciel Paramètres du logiciel Paramètres Windows Stratégie de résolution de noms Scripts (démarage/arrêt) Stratégies de scurité Paramètres de scurité Stratégies de comptes Stratégies de mot de passe Durée de vie maximale du mot de passe Unrée de vie minimale du mot de passe Jours Lot vie de vie minimale du mot de passe Jours Lot vie de vie minimale du mot de passe Jours Lot vie de vie minimale du mot de passe Jours Stratégie de comptes Stratégies de mot de passe Stratégies de sécurite Stratégies de sécurites Stratégies de mot de passe Stratégies de réseu filaire (IEEE 802.3) Pare-feu Windows avec fonctions avan Stratégies de réseu sans fil (IEEE 802.11) Stratégies de réseu sans fil (IEEE 802.11) Stratégies de réseu sans fil (IEEE 802.11) Stratégies de contrôle de l'application Stratégies de contrôle de l'application Stratégies de sécurité IP sur Active Direc Stratégies de sécurité IP sur Active Direc<	

Stratégie 🔺	Paramètres de stratégie
🕅 Conserver l'historique des mots de passe	0 mots de passe mémorisés
📖 Durée de vie maximale du mot de passe	0
📖 Durée de vie minimale du mot de passe	0 jours
📓 Enregistrer les mots de passe en utilisant un chiffrement rév	Désactivé
📖 Le mot de passe doit respecter des exigences de complexité	Désactivé
📖 Longueur minimale du mot de passe	4 caractère(s)

- => Modifiez les paramètres en tenant compte de l'image écran (Ci-dessus).
- => Validez vos choix.
- => Ouvrez l'invite de commandes puis tapez : gpupdate /force.
- => Lancez l'observateur d'événements pour corriger d'éventuelles erreurs.

Pour gérer votre Domaine vous devez créer un compte appartenant au groupe 용 Administrateurs

Dans l'unité d'organisation Users créer un nouvel utilisateur

	unsaleurs et ordinaleurs Activ	e Directory		
Fichier Action Affichage ?	Nom Administrateur Administrateur Administrateurs de l'entreprise Administrateurs du schéma Administrateurs du schéma Administrateurs du domaine Contrôleurs de domaine Contrôleurs de domaine d'ent	P Directory Type Utilisateur Groupe de sécurité Groupe de sécurité Groupe de sécurité Groupe de sécurité	Descript Compte Admini: Admini: Tous les Les mer Les mer	tion e d'utilisateur d'administration strateurs désignés de l'entreprise strateurs désignés du schéma strateurs désignés du domaine s contrôleurs de domaine du d mbres de ce groupe qui sont d mbres de ce groupe sont des c
Users	Contrôleurs de domaine de chie     Contrôleurs de domaine en le     DisAdmins     DisUpdateProxy     Éditeurs de certificats     Groupe de réplication de     Invité     Invité     Invité     Invité     Propriétaires créateurs d     Protected Users     Serveurs RAS et IAS     Utilisateurs du domaine	Groupe de sécurité Groupe de sécurité Délégation de contrôle Rechercher Vouveau Foutes les tâches Actualiser Exporter la liste Affichage Réorganiser les icônes Aligner les icônes Propriétés	Les mer	hind State Ce groupe sont des c des administrateurs DNS ts DNS qui sont autorisés à ef Ordinateur Contact Groupe InetOrgPerson msDS-ResourcePropertyList msImaging-PSPs Alias de file d'attente MSMQ Imprimante
< III >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		Aide		Dossier partagé
Créer un nouvel objet	JI			

🧏 Créer da	ns : prevert-XX.lo	cal/Users	Nouvel objet - Utilisateur
Prénom :	votre prénom	Initiales :	
Nom :	votre nom		Mot de passe :
Nom complet :	admidom		Confirmer le mot de passe :
Nom d'ouverture d admindom Nom d'ouverture d	le session de l'utilisa le session de l'utilisa	ateur : @prevert-XX.local v ateur (antérieur à Windows 2000) :	<ul> <li>L'utilisateur doit changer le mot de passe à la prochaine ouverture de session</li> <li>✓ L'utilisateur ne peut pas changer de mot de passe</li> <li>✓ Le mot de passe n'expire iamais</li> </ul>
PREVERT-XX\		admindom	Le compte est désactivé
	[	< Précédent Suivant > Annuler	< Précédent Suivant > Annuler

Nom d'ouverture de session: **admindom** Mot de passe: **Prevert77** 

Nouvel objet - Utilisateur	x
Créer dans : prevert-XX.local/Users	
Quand vous cliquerez sur Terminer, l'objet suivant sera créé :	
Nom complet : admidom	^
Nom de connexion de l'utilisateur : admindom@prevert-XX.local	
L'utilisateur ne peut pas changer de mot de passe.	
Le mor de passe il expire jamais.	
	$\sim$
< Précédent Terminer Annu	las

#### Ajouter admindom au groupe Administrateurs et Admin du domaine

Р	ropriétés de : admidom 🛛 🔹 🗙			
Environnement Sessions Cor Général Adresse Compte P	trôle à distance Profil des services Bureau à distance COM+ rofil Téléphones Organisation Membre de Appel entrant			
Membre de :         Dossier Services de domaine Active Directory           Administrateurs         prevert-XX.local/Builtin           Adminis du domaine         prevert-XX.local/Users           Utilisateurs du domaine         prevert-XX.local/Users				
Ajouter     Supprimer	III >			
Groupe principal : Utilisateurs	i du domaine Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.			
[	OK Annuler Appliquer Aide			

Connectez vous sur votre serveur avec ce nouveau compte

## Construction des unités d'organisation

Nous allons maintenant intégrer tous les utilisateurs et tous les ordinateurs de notre domaine. Pour cela nous allons construire une achitecture d'Unités d'Organisations qui refléte la structure de notre entreprise.

Utilisateurs et ordinateurs Active Directory [SRV12R2-DC1-XX.



## Création des comptes utilisateurs

Créer dans l'unité d'organisation nommée **classe 1** les comptes utilisateurs suivants :

Ordinateur
Contact
Groupe
InetOrgPerson
msImaging-PSPs
Alias de file d'attente MSMQ
Unité d'organisation
Imprimante
Utilisateur
Dossier partagé

Nom	prénom	Nom complet	Nom d'ouverture de	Mot de passe
			session	
Eleve1	Eleve1	Eleve1 de classe 1	eleve1	111111
Eleve2	Eleve2	Eleve2 de classe 1	eleve2	222222

- ☑ L'utilisateur ne peut pas changer de mot de passe
- ☑ Le mot de passe n'expire jamais

Créer dans l'unité d'organisation nommée classe 2 les comptes utilisateurs suivants :

Nom	prénom	Nom complet	Nom d'ouverture de	Mot de passe
			session	
Eleve3	Eleve3	Eleve3 de classe 2	eleve3	333333
Eleve4	Eleve4	Eleve4 de classe 2	eleve4	44444

- ☑ L'utilisateur ne peut pas changer de mot de passe
- $\square$  Le mot de passe n'expire jamais

## **Centre d'administration Active Directory**

Windows server 2012R2 introduit un nouvel outil pour gérer active directory.



A l'aide du centre d'administration Active Directory, créer dans l'unité d'organisation nommée **professeurs** les comptes utilisateurs suivants :

Nom	prénom	Description	Nom d'ouverture de	Mot de passe
			session	
Prof1	Prof1	Professeur1	prof1	ppp111
Prof2	Prof2	Professeur2	prof2	ppp222

☑ L'utilisateur ne peut pas changer de mot de passe

 $\square$  Le mot de passe n'expire jamais

	Centre	d'administration	Active Directory		_ 0 ×
evert-XX ••• prevert-XX	(local) • LMJP •	utilisateurs	• professeurs		• 闭   Gérer Aide
Centre d'adminis < profess	eurs (0)				Tâches
E Filtrer	م	· ·	•	$\odot$	Drofesseurs
Vue d'ensemble      ✓    Vue d'ensemble      ✓    ✓    ✓    ✓    ✓    ✓    ✓	n Type	Description			Nouveau Supprimer Déplacer
European Controllers      European Con	Créer Utilisateur : p compte	orof1 prof1 Compte			TÂCHES V SECTIONS V 2 8 0
<ul> <li>✓ ■ utilisateurs</li> <li>▷ ■ eleves</li> <li>○ professeurs</li> <li>▷ ■ LostAndFound</li> </ul>	Organisation Membre de Paramètres de mot de passe Profil Stratégie	Prénom : Initiales des autres pr Nom : Nom complet : Ouverture de session	prof1 pr	Date d'expiration Options de mot d O Changer le mo O Autres options	du cr ● Jamais
	Silo	Mot de passe : Confirmation : Créer dans : OU=profes -XX,DC=loc Protéger contre la su	seurs,OU=utilisateurs,OU=LMJP,DC=prevert al. Modifier uppression accidentelle e de session	Une carte à V Le mot de p L'utilisate Options de chiffre Autres options :	puce est nécessaire pour ouvrir une session passe n'expire jamais. eur peut changer de mot de passe. ement : •
		Organisation			?⊗⊙
		Nom complet : Bureau : Adresse de messagerie : Page Web :	prof1 prof1	Fonction : Service : Société : Responsable :	Modifier Effacer
	<ul> <li>Informations supplémenta</li> </ul>				OK Annuler

Bonne Pratiques : activer la corbeille afin de pouvoir récupérer facilement les utilisateurs supprimés ainsi que toutes les informations associées (adresse, groupe,...)

Centre	d'administrat <	prevert-XX (local) (13)					Tâches	
°⊑ Vue d'er	nsemble	Filtrer	٩	• • •		۲	🖄 Builtin	<b>^</b> ^
	Modifier le contrôleur de c Augmenter le niveau fonct Augmenter le niveau fonct Activer la Corbeille Nouveau Rechercher sous ce nœud Propriétés haged Service Accounts	Nom domaine tionnel de la forêt tionnel du domaine Description :	Type builtinDom Conteneur Unité d'org Conteneur	Default containe Default containe Default co Modifié	r for upgr Étes activ	Activer la -vous sûr de vou rée, elle ne peut	Nouveau Supprimer Rechercher sous Propriétés confirmation de loir effectuer cette plus être désactivée	ce nœud e la Corbeille action ? Une fois la (

## Joindre les machines au domaine



Faites en sorte que les stations ST1-XX et ST2-XX soient membre du domaine prevert-xx.local

#### Sur les STATIONS

Paramétrer le serveur DNS des stations pour qu'elles interrogent notre serveur 2012

Mettre à jour le nom de l'ordinateur, ST1-XX et ST2-XX,

Intégrer les stations au Domaine prevert-xx.local.

Modification du nom ou du domaine de l'ordinateur 💽	Madification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ceci peut influer sur l'accès aux ressources en réseau. <u>Informations complémentaires</u>	Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom de l'ordinateur : ST1-XX	Nom de l'ordinateur :
Nom complet de l'ordinateur : ST1-XX Autres	Nom complet de l'ordinateur : ST2-XX
Membre d'un Omaine : prevert-XX.local	Membre d'un Domaine : prevert-XX.local
© Groupe de travail : WORKGROUP	Groupe de travail : GW
OK Annuler	OK Annuler

#### Identifiez vous avec un compte du domaine administrateur / Prevert77



Dans active directory vérifier la présence des stations ST1-XX et ST2-XX dans le conteneur computers



Déplacer les machines **ST1-XX** dans l'Unité d'Organisation **salle A** et **ST2-XX** dans l'OU **salle B** Vérifier tous les comptes utilisateurs sur les deux machines.