

# Windows 2016 - Works-Folder

Windows 2016 – Works folder – dossiers de travail windows 10 Michel Cabaré – Ver 1.1 – décembre 2016-

# Windows 2016 - Works Folder

Michel Cabaré – Ver 1.1 – Décembre 2016

www.cabare.net©



# TABLE DES MATIERES

WORKS FOLDER	3
Works Folder – Dossier de travail	3
VERSION CONFIGURATION MINIMALE	3
GROUPE DE SECURITE UTILISATEUR WORK FOLDER	4
Dossier NTFS sur volume dedie	4
ALIAS CNAME DNS (OPTION)	5
WORKS FOLDER – SERVEUR	6
Ajout du Role Dossier de travail	6
PARAMETRAGE DU ROLE DOSSIER DE TRAVAIL	7
INTERFACE DE GESTION DOSSIER DE TRAVAIL	12
SERVICE SYNCSHARESVC - SUPERVISION JOURNAUX	13
WORKS FOLDER – CLIENT	14
UTILISATEUR ITIN MEMBRE DU GROUPE WORKFOLDER	14
PARAMETRAGE CLIENT EN HTTP (SANS HTTPS)	14
CLIENT VIA LE PANNEAU DE CONFIGURATION	15
CLIENT VIA GPO	
TEST - UTILISATION	19
SOUPLESSE D'UTILISATION "A LA VOLEE"	20
SSL ET CERTIFICATS	21
SSL ET CERTIFICATS	21
Quel certificat pour quel serveur	21
Installation de la console gestion IIS	22
Création du certificat de domaine du serveur	22
Ajout du protocole https avec le certificat	25
GPO avec nouvelle adresse en https	26
MACHINE HORS DOMAINE	27
PB VALIDITE DE CERTIFICAT "HORS DOMAINE"	27
Situation dans un domaine	27
Situation en Workgroup	
EXPORT DE CERTIFICAT:	29
IMPORT DE CERTIFICAT SUR UNE MACHINE EN WORKGROUP:	31
CERTIFICAT ET PKI	
Types de Certificats et PKI	
CREATION PKI DE DOMAINE:	34
Ajout rôle Service de certificats AD	34
Paramétrage du rôle Service de certificats AD	
Visualisation PKI	40
RENOUVELLEMENT PKI DE DOMAINE:	41



# **WORKS FOLDER**

# Works Folder – Dossier de travail

Les **Works Folder** ou « Dossier de travail » font partie des nouveautés de Windows serveur 2012 R2 et Windows 8.1. Il s'agit d'un dossier de synchronisation entre différents périphérique appartenant au même utilisateur.

Il s'agit d'utiliser un nouveau protocole de synchronisation pour les données sur un serveur **on-premise** (et non **SaaS**)

Les Works Folders sont une nouvelle fonctionnalité apparues pour le rôle de Services de fichiers et de stockage

L'objectif c'est de faire en sorte que l'on partage sur plusieurs appareils différents une même base qui est en fait centralisée sur un serveur interne de l'entreprise. Lorsque l'on modifie un fichier sur un appareil donné, (stocké dans un dossier nommé **Work Folders**), il y a mise à jour des tous les autres endroits de stockages appartenant à cet utilisateur, qu'il s'agisse du serveur central, (mais à la limite c'est le seul qu'il n'utilise pas directement...), mais aussi de tous les autres périphériques utilisés.

En d'autres termes, lorsqu'un utilisateur crée ou modifie un fichier dans son **Work Folders**, depuis n'importe lequel de ses PC ou tablettes, il y a :

- d'abord une réplication automatique via Secure Sockets Layer (SSL) sur le serveur d'entreprise
- puis une réplication sur tous les autres périphériques configurés, dans leurs dossiers respectifs **Work Folders**

# Version configuration minimale

Coté Serveur:	Windows 2016 ou 2012R2, dédié car va héberger un IIS
	Un espace dossier de stockage NTFS
Coté Client:	Windows 10 - Windows 8.1

**N.B**: Si l'ouverture avec SSH est requise, alors la gestion des certificats sera obligatoire



# Groupe de sécurité utilisateur Work Folder

Pour que l'on s'y retrouve, il serait bien de se créer un groupe de sécurité spécifique à l'utilisation de cette fonctionnalité.

En effet les partages vont être gérés avec de la sécurité NTFS, et donc il peut être plus simple de créer un groupe, auquel on donnera les droits au dossier work folder stocké sur Nouvel objet - Groupe Х le serveur interne. Dans l'AD on va se créer Créer dans : cabare-intra.net/z-utilisateurs donc un nouveau Groupe de Sécurité Globale dans Nom du groupe : l'exemple nommé workwork-folder-byod folder-byod Nom de groupe (antérieur à Windows 2000) : work-folder-byod avec au moins un futur Étendue du groupe Type de groupe utilisateur itinérant... O Domaine local Sécurité dans l'exemple itin Globale Oistribution ○ Universelle Propriétés de : work-folder-byod Général Membres Membre de Géré par Objet Sécurité Éditeur d'a Membres : Nom Dossier Services de domaine Active Directory گ itin cabare-intra.net/z-utilisateurs

# Dossier NTFS sur volume dédié

Il faut préparer l'emplacement de nos dossiers de stockage dans un espace **NTFS**, dédié

par exemple ici un Volume d:

De base Ré 500,00 Go 500	0 Mo NT	99,51 Go NTFS	48,83 Go NTFS	
En ligne Sai	in (Systè	Sain (Démarrer, Fichier	Sain (Partition princir	avec

avec le dossier dossiers-byod

> 🏪 os-virtuel (C:)
💙 👝 stock-dossiers (D:)
> \$RECYCLE.BIN
dossiers-byod



# Alias Cname DNS (option)

Ce n'est pas obligatoire, mais si on veut ensuite utiliser des **GPO** et s'affranchir des contraintes de re-nomage – modifications, on peut créer dans le **DNS** un **alias** pour le nom du serveur hébergeant les services **Work Folder** 

louvel enregistrement de ressource	×
Nom canonique (CNAME)	
Nom de l'alias (utilise le domaine parent si ce champ est vide) :	
workfolders	]
Nom de domaine pleinement qualifié (FQDN) :	
workfolders.cabare-intra.net.	
Nom de domaine complet (FQDN) pour l'hôte de destination :	
srv-dc2.cabare-intra.net Parcourir	

Si le serveur hébergeant les fonctionnalités **Work Folder** est nommé par exemple **srv-dc2.cabare-intra.net**,

on peut faire un alias du genre workfolder!

Nom	Туре	Données	Horodateur
workfolders	Alias (CNAME)	srv-dc2.cabare-intra.net.	statique



# **WORKS FOLDER – SERVEUR**

# Ajout du Rôle Dossier de travail

On a dans l'exemple un serveur *srv-dc2* sur lequel on souhaite installer cette fonctionnalité. Dans le **gestionnaire de** *serveur* on demande Gérer, *Ajouter des Rôles et des Fonctionnalités* 



On indique que l'on veut un rôle ...

## Sélectionner le type d'installation

SERVEUR DE DESTINATION srv-dc2.cabare-intra.net

Avant de commencer	Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un preliasteur physique ou virtuel de fonctionnement, ou sur un disque dur virtuel berg connexion.
Type d'installation	-
Sélection du serveur	Installation basée sur un rôle ou une fonctionnalité Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités

#### On indique notre serveur

Pool de serveurs		
Filtre :		
Nom	Adresse IP	Système d'exploitation
srv-dc2.cabare-intra.net	192.168.1.92	Microsoft Windows Server 2016 Standard

#### Et on coche dans Services de fichiers et de stockage que Dossier de travail





#### On confirme en demandant Installer

📥 Assistant Ajout de rôles et de fonctionnalités

#### – 🗆 🗙

 $\times$ 



# Paramétrage du Rôle Dossier de travail

Maintenant que le rôle est installé il faut le configurer.

# SERVEUR DE DESTINATION Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats



http://www.cabare.net Page 7 / 41 - Michel Cabaré - Dans le gestionnaire de serveur, on demande Services de fichiers et de stockage,



Dans lequel on va demander Dossier de travail

Gesti	onnaire de serveur		
	Services de fichiers	s et de stockage 🔹 Serveu	irs
	Serveurs	SERVEURS Tous les serveurs   1 au total	
i.	Volumes	Filtrer	م
Ī	Disques		
	Pools de stockage	Nom du serveur Adresse IPv4 Facil	ité c
	Partages	SRV-DC2 192.168.1.92 En lie	ane
	iSCSI		
	Dossier de travail		

Où l'on voit qu'il n'y a aucun dossier de travail installé

📥 Gesti	onnaire de serveur		×
$\mathbf{E}$	. ✓ Tossier	de travail 🔹 🕫 🖡 Gérer Outils Afficher Aide	
	Serveurs Volumes Disques Pools de stockage Partages iSCSI Dossier de travail	DOSSIERS DE TRAVAIL       TÂCHES         Tous les partages de synchronisation   0 au total       TÂCHES         Il n'existe aucun partage de synchronisation.         Pour créer un partage de synchronisation pour les dossiers de travail, démarrez l'Assistant Nouveau partage de synchronisation.	^
On de <b>Nouv</b> e	emande alors vic eau partage de sy	Tâches d'ajouter un Inchronisation	

cela déclanche un assistant

N.B : On a déjà préparé l'emplacement de nos dossiers de stockage dans un espace NTFS dédié, par exemple ici un Volume d: avec le dossier dossiers-byod







# On choisit le serveur, et le <u>chemin local</u> de stockage de nos futurs **dossiers de travail**

	Serveur :			1
Serveur et chemin d'accè	S Nom du serveur	Statut	Rôle du cluster	Nœud propriétaire
Structure des dossiers uti	li srv-dc2	En ligne	Non-cluster	
Nom du partage de sync				
Accès à la synchronisation	n			
Stratégies de sécurité PC				
	Seuls les serveurs et in	nstances de serveurs o	de fichiers en cluster o	ù sont installés les do
Résultats	de travail sont affiche	s.		
	Emplacement :	1.615		
	Selectionner par parta	ge de fichiers :		
	Nom Chemin d'accès	5		
			2	

On choisit plutôt une appellation complète de type utilisateur@domaine





🚡 Assistant Nouveau partage de synchronisation

– 🗆 🗙

## Entrer le nom du partage de synchronisation

Avant de commencer	Nom :	dossiers-byod
Serveur et chemin d'accès		
Structure des dossiers utili	Description :	dossiers pour la fonction dossier de travail
Nom du partage de sync		$\searrow$

On affecte le groupe de sécurité crée auparavant, et on coche ou non **Désactiver les autorisations héritées** (si l'on souhaite que l'administrateur puisse accéder à ces dossiers on décoche)

📥 Assistant Nouveau partage de syn	chronisation			-		×
Assistant Nouveau partage de syn Accorder aux grou Avant de commencer Serveur et chemin d'accès Structure des dossiers utili Nom du partage de sync Accès à la synchronisation	Des l'accès à Domaine CABARE-INTRA	la synchronisa Principal work-folder-byod	ntion Description	-		×
Stratégies de sécurité PC Confirmation Résultats		k₃.				
	Ajouter       Supprimer         ✓       Désactiver les autorisations héritées et accorder aux utilisateurs un accès exclusif à fichiers					

#### Politique de sécurité sur le partage (du client):



Dans l'état actuel de la technologie, on n'impose rien !

le **chiffrement EFS** des fichiers synchronisés sur le poste client le verrouillage de l'écran et un mot de passe obligatoire



_						
æ	Assistant	Nouveau	partage	de s	vnchronisa	ation
<b>Market</b>	/ cashaconne	recau	purcuge		y nem or mar	

_	$\times$

## Confirmer les sélections

erveur et chemin d'accès	EMPLACEMENT DU PARTAGE DE SYNCHRONISATION		
tructure des dossiers utili	Nom du serveur :	srv-dc2.cabare- intra.net	l
om du partage de sync	Rôle du cluster :	Non-cluster	
ccès à la synchronisation	Chemin d'accès :	D:\dossiers-byod	
tratégies de sécurité PC	PROPRIÉTÉS DU PARTAGE DE SYNCHRONISATION		
oniirmation	Nom :	dossiers-byod	
	Description :	dossiers pour la fonction dossier de travail	
	Accès à la synchronisation :	CABARE-INTRA \work-folder-byod	
	Accorder aux utilisateurs un accès exclusif :	Oui	
	Structure des dossiers utilisateur :	Alias_utilisateur@d omaine	
	Synchroniser uniquement ce sous-dossier :		
	STRATÉGIES DE SÉCURITÉ PC		
	Chiffrer les dossiers de travail :	Non	

#### Et on obtient

Le partage de synchronisation a été correctement créé.						
Tâche	État d'avancement	Statut				
Créer un partage de synchronisa		Terminé				
Actualiser le Gestionnaire de sen		Terminé				

Actuellement donc on se retrouve donc avec un accès ouvert à la syncrhonisation des work folder via l'URL Domaine\nom de partage que l'on retrouve dans **Dossiers de travail – Utilisateurs** :

	ssier	de trava	ail		- (2		Gérer	Outils	Afficher A
Serveurs Volumes Disques Pools de stocka	🖓	Dernière ac UTILISATE dossiers-byo	tualisation : 12 <b>URS</b> d sur srvdc1-fc	2/06/2017 14:39:57 prm16   Utilisateurs : 1					
Partages iSCSI	Ĵ	Filtrer		٩					۲
Dossier de travail		Domaine	Utilisateur	Groupe	Nom du partage de synchronisation	Nom	complet du serveur	Sus	pendu
		FORM1	itin itin	work-folder-byod	dossiers-byod	srvdc	1-form16.form1.edu	Non	l.
	Nom	du parta	ge de syno	chronisation	Nom complet du serveur	r			
	dossi	ers-byod			srvdc1-form16.form1.edu	J I			



# Interface de gestion Dossier de travail

Depuis le gestionnaire de serveur,

🚡 Gesti	onnaire de serveur						- 0
$\mathbf{E}$	→   •• Dossier	de travail			• 3	🏲 Gérer	Outils Afficher Aid
	Serveurs Volumes Disques Pools de stockage Partages	DOSSIERS DE TRAV         Tous les partages de sy         Filtrer         Nom du partage         Description         srv-dc2 (1)	AIL nchronisation   1 au total	<ul> <li>Chemin d'accès</li> </ul>	Statut	Groupe d'accès	TÂCHES V
	iSCSI Dossier de travail	dossiers-byod dossiers	pour la fonction dossier de trava	il D:\dossiers-byod	Activé	CABARE-INTRA\work-f	older-byod

Sur lequel on peut demander **Propriétés** par exemple pour remodifier notamment les autorisations d'accès (accès synchronisation)

Chemin d'accès	Statut	Groupe d'ac	ccès.			
D:\dossiers-byod	Activé	CABARE-IN	TRA\work-fo			
	Désactive Supprime Propriétés	r le partage de r le partage de s	synchronisation synchronisation			
Propriétés de dossiers-byo	d			_		×
dossiers-byod Afficher tou Général 4 Accès à la synchro Stratégies de ségu	ut A	ccès à la s	ynchronisation			
Strategies de seculi		Domaine	Principal	Descript	ion	
G		FORM1 w Ajouter Désactiver le accès exclusi	vork-folder-byod Supprimer s autorisations héritées et f à leurs fichiers	accorder aux util	isateurs u	ın

#### Plus bas on peut voir aussi

VOLUME	QUOTA
dossiers-byod sur srv-dc2 TÂCHES	Aucun partage n'est sélectionné. TÂCHES ▼
stock-dossiers (D:) Capacité : 97,7 Go	Pour utiliser les quotas, le Gestionnaire de ressources du serveur de fichiers doit être installé.
0,1 % utilisés I 23 Mo Espace utilisé	Pour installer le Gestionnaire de ressources du serveur de fichiers,
97,5 Go Espace disponible	démarrez l'Assistant Ajout de rôles et de fonctionnalités.



# Service SyncShareSvc - Supervision journaux

#### Le service se nomme SyncShareSvc

SRVDC1-FORM16	Partage de synchronisation Windows	SyncShareSvc	En co
SRVDC1-FORM16	Fournisseur de cliché instantané de logiciel Microsoft	swprv	En cc ^
Nom du serveur	Nom complet	Nom du service	Statı
Filtrer			$\odot$
SERVICES Tous les services   2	01 au total		TÂCHES 🔻

Dans l'observateur d'évènement on pourra lire le journal SyncShare





# **WORKS FOLDER – CLIENT**

# Utilisateur Itin membre du groupe Workfolder

L'idée c'est qu'un utilisateur itinérant, nommé **itin** mdp **Domaine2016** puisse utiliser les workfolder..ll faut donc vérifier que l'on ait bien un compte **itin** 

Managed Service Accourt	💐 Serveurs RA	Groupe de sécurité - Domai
📋 Users	🔱 util	Utilisateur
_	💐 Utilisateurs	Groupe de sécurité - Global
>	🂐 work-folder	Groupe de sécurité - Global

Membre du groupe de sécurité global Work-folder-byod ... :

Pro	Propriétés de : work-folder-byod							
G	énéral	Membres	Membre de	Géré par				
Membres :								
Nom & itin itin		Dossier Se form1.edu	Dossier Services de domaine Active Directory form1.edu/Users					

# Paramétrage client en http (sans https)

La configuration du client peut se faire soit :

- manuellement, via le panneau de configuration,
- soit par GPO.

Par défaut la connexion va chercher à se connecter en https (SSL). Avant de configurer des certificats on va autoriser la connexion en http. Pour cela il faut ajouter dans la base de registre du client : la clé WorkFolders valeur REG\_DWORD 1 dans HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion

Soit avec donc une commande (en administrateur) du genre

Reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WorkFolders /v AllowUnsecureConnection /t REG\_DWORD /d 1

🔤 Administrateur : Invite de commandes	_		$\times$
(c) 2015 Microsoft Corporation. Tous droits réservés.			^
C:\Windows\system32>Reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersio /v AllowUnsecureConnection /t REG_DWORD /d 1 L'opération a réussi.	n\Wor	kFolde	ns -

#### Que l'on peut vérifier via regedit

*	Nom (par défaut) AllowUnsecureConnection	Type REG_SZ REG_DWORD	Données (valeur non définie) 0x0000001 (1)
	*	Nom b) (par défaut) AllowUnsecureConnection	Nom Type (par défaut) REG_SZ AllowUnsecureConnection REG_DWORD



# Client Via le panneau de configuration

Dans le panneau de configuration, on deamnde Dossiers de Travail





**N.B**: Si on a créé le CNAME pour workfolders dans le DNS, on peut utiliser ce nom et donc entrer comme URL: **http://workfolders.cabare-intra.net**.

Si on avait cela : srvdc1-form16.form1.edu



#### alors on peut rentrer http:srvdc1-form16.form1.edu

#### Entrer l'URL de Dossiers de travail

Si vous n'avez pas d'URL pour Dossiers de travail, contactez votre organisation la fonctionnalité Dossiers de travail.

URL de Dossiers de travail :

http://srvdc1-form16.form1.edu

Forcement il y a une demande d'authentification (il faut rentrer l'identifiant de notre utilisateur itinérant..)

	Sécurité Windows	×
Entrer l'URL de Dossiers de travail	Dossiers de travail	
Si vous n'avez pas d'URL pour Dossiers de travail, ce la fonctionnalité Dossiers de travail. URL de Dossiers de travail :	Entrez votre domaine, votre no passe.	om d'utilisateur et votre mot de
http://srvdc1-form16.form1.edu		
	itin@form1.edu	
	•••••	୍
	Mémoriser mes information	ons
	ОК	Annuler

On choisit ensuite où l'on veut poser sur notre machine le dossier de travail... par défaut le dossier de travail est posé dans le profil utilisateur qui s'est authentifié, mais on peut le mettre ou l'on veut via **Modifier...** 



Cabaré 🕖

#### Il faut accepter obligatoire les GPO de sécurité



Et voilà !

#### La fonctionnalité Dossiers de travail a démarré la synchronisation avec ce PC.

La fonctionnalité Dossiers de travail synchronise actuellement vos fichiers en arrière-plan.

Tout fichier que vous stockez dans Dossiers de travail est chargé vers votre organisation. Vous pourrez ensuite les utiliser sur d'autres PC et appareils sur lesquels la fonctionnalité Dossiers de travail a été configurée.



# **Client Via GPO**

Il parait plus "sain de créer une **GPO** que l'on appliquera aux postes sur lesquels on veut mettre en place les **works folders**...

On se crée une nouvelle GPO utilisateur, par exemple strat-util-work-folders



Dans laquelle assez simplement on indique l'Url du serveur stockant les Dossiers de travail, dans l'exemple http://srv-dc2.cabare-intra.net

💭 Spécifier les paramètres de Dossiers de t	ivail — 🗆 🗡
📆 Spécifier les paramètres de Dossiers de	avail Paramètre précédent Paramètre suivant
O Non configuré Commentaire :	
<ul> <li>Activé</li> </ul>	
○ Désactivé	
Pris en charge sur :	u minimum Windows Server 2008 R2 ou Windows 7
Options :	Aide :
URL de Dossiers de travail :	L'antian « Forcer la configuration automatique » enécifie que la
http://srv-dc2.cabare-intra.net	fonctionnalité Dossiers de travail doit être configurée
Forcer la configuration automatique	automatiquement sans demander aux utilisateurs. Cela empeche les utilisateurs non seulement de choisir de ne pas utiliser la fonctionnalité Dossiers de travail sur l'ordinateur, mais aussi de spécifier manuellement le dossier local dans lequel la fonctionnalité Dossiers de travail stocke les fichiers. Par défaut, la fonctionnalité Dossiers de travail est stockée dans le dossier « %USERPROFILE%\Dossiers de travail ». Si cette option n'est pas spécifiée. les utilisateurs doivent utiliser l'élément Dossiers de

<sup>1</sup>Il est de bon ton de ne pas laisser le choix à l'utilisateur

Du coup, le dossier de travail apparaît directement dans le Profil utilisateur



# Test - utilisation

Depuis un client paramétré, l'utilisateur **itin@cabare-intra.net** travaille simplement avec ce nouveau dossier **Dossiers de travail** qui apparaît dans l'interface du gestionnaire de fichier, Ou applicative

Soit là où l'on l'a paramétré (dans le cas d'une installation du client manuelle), soit directement sous le Bureau (si utilisation d'une **GPO** : mieux !)

🖈 Accès rapide	^	Nom		
Bureau		Controle-saisie-personnalisé.xlsx	👿 Enregistrer sous	
Dossiers de travail			← → → ↑ 📑 > Dossiers de travail	
			Organiser 🔻 Nouveau dossier	
			> 👿 Microsoft Word	
			🛩 🔜 Bureau	
			> 🙀 Dossiers de travail	
lout ce qui s'y trouve est	t tra	nsmis sur le serveur		
늘 os-virtuel (C:)		^ Nom		
stock-dossiers (D:)		itin@CABARE-INTRA		
\$RECYCLE.BIN				
dossiers-byod				

Vérification Possible depuis le **panneau de configuration / dossier de travail** du client ou en cliquant sur le bas de la barre des tâches, lorsque l'on est dans le dossier de travail

<ul> <li>Accès rapide</li> <li>Dossiers de travail</li> <li>Ce PC</li> <li>Bureau</li> <li>E Documents</li> </ul>	<ul> <li>Nom</li> <li>Nouveau dossier</li> <li>Nouveau Document Microsoft Word.docx</li> <li>Nouveau document texte.txt</li> <li>Nouveau Texte OpenDocument (2).odt</li> <li>Nouveau Texte OpenDocument.odt</li> </ul>
> 📰 Images	v <
5 élément(s) Statut de la synchronisation : D	Dernière synchronisation : 07/04/2017 10:52
	Dernière synchronisation : 07/04/2017 10:52

L'utilisateur peut aussi demander rapidement (clic droit) **Synchroniser** maintenant

> 📑 Dossiers de tr	avail
🗸 🛄 Ce PC	Développer
> <mark></mark> Bureau > 🚔 Document	Ouvrir dans une nouvelle fen Épingler dans Accès rapide
> 💽 Images	Partager avec
5 élément(s) Sta	🔋 Synchroniser maintenant





Notamment avec une possibilité d'arrêt (si pas de GPO) Page d'accueil du panneau de

Demander de l'aide à votre organisation :

Aucune erreur de fichier

configuration
<u>Arrêter d'utiliser Dossiers de</u> <u>travail</u>
Gérer les informations d'identification
Synchroniser maintenant

#### Gérer Dossiers de travail Utilisez Dossiers de travail pour rendre vos fichiers de travail dis même hors connexion. Dossiers de travail 2 Voulez-vous arrêter d'utiliser Dossiers de travail ?

lorsque l'on coupe la stratégie créant un work folder pour un utilsateur, celuici va se retrouver avec un dossier de travail "normal"

# Souplesse d'utilisation "à la volée"

A tout moment, sur une machine en domaine, (ou en workgroup si on a importé le certificat de racine de confiance du domaine) on peut dans le panneau de configuration demander de mettre en place les dossiers de travail, et éventuellement les démonter après usage...

#### Entrer l'URL de Dossiers de travail

Si vous n'avez pas d'URL pour Dossiers de travail, contactez votre organisation pour savoir si vous avez accès à la fonctionnalité Dossiers de travail.

URL de Dossiers de travail : https://srv-dc2.cabare-intra.net	Sécurité de Windows           Dossiers de travail           Entrez votre domaine, votre nom d'utilisateur et votre mot de passe.	×	
	Nom d'utilisateur Mot de passe		



Envoyer un message électronique au support

technique

# SSL ET CERTIFICATS

# SSL et certificats

Pour utiliser SSL, il faut un certificat SSL pour notre serveur gérant les dossiers de travail srv-dc2.cabare-intra.net ou workfolders.cabare-intra.net.

En effet le protocole **https** a besoin d'un certificat authentifiant le serveur d'où proviennent les communications en **https-443**. Si on tente une connexion **https** <u>sans certificat</u> on a une erreur bloquante :



- Certificat de Domaine + machine de Domaine, tout est Ok.
- Certificat de Domaine + machine hors Domaine alors il faudra importer le certificat de l'autorité de certification dans le magasin des autorités racines de confiance des machines hors domaine. en effet, celles-ci ne font pas confiance par défaut à la CA du domaine. (évidemment les membres du domaine eux font confiance automatiquement).
- **N.B**: Ce point peut justifier l'achat d'un **certificat SSL** auprès d'une **autorité de certification publique** déjà reconnue par tous les types de clients.

# Quel certificat pour quel serveur

Actuellement, aucun certificat spécifique n'a été demandé, par conséquent dans la liste des certificats attribués, le seul certificat qui peut apparaitre sera celui octroyé par défaut au **Contrôleur de Domaine** 

a certsrv - [Autorité de certification	(Local)\f	orm1-pki-CA\Certificats délivre	és]	— 🗆	×
Fichier Action Affichage ?					
🗧 📥 🔯 🖌 🚔			/		
Autorité de certification (Local)	ID d	Nom du demandeur	Certificat binaire	Modèle de certificat	Numé
✓ of form1-pki-CA Contificate révolution	<b>a</b> 2	FORM1\SRVDC1-FORM16\$	BEGIN CERTI	Contrôleur de domaine (DomainController)	11000
Certificats délivrés					
Demandes en attente					
📔 Demandes ayant échoué					
Modèles de certificats					



# Installation console de gestion IIS

Il va falloir que l'on soit capable de faire une demande de **certificat** pour notre serveur hébergeant les **Works Folders** 

Cela pourra se faire de manière interactive via la **console de gestion IIS**, qu'il va falloir installer

N.B : ne jamais installer en production un IIS sur un contrôleur de domaine

(IIS) ?

Cela suppose d'ajouter le rôle se serveur Web IIS



N.B: On pourra constater que le site web par défaut est arrêté. C'est normal, car le service de synchronisation de fichiers n'utilise pas un site IIS mais le service IIS Hostable Web Core (HWC).

Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être install sur le même serveur.	és
<ul> <li>Serveur Web (IIS)</li> <li>Outils de gestion         [Outils] Console de gestion IIS     </li> </ul>	
✓ Inclure les outils de gestion (si applicable)	
Ajouter des frenctionnalités	ler

Ajouter les fonctionnalités requises pour Serveur Web

Х

📥 Assistant Ajout de rôles et de fonctionnalités

# Création du certificat de domaine du serveur

Via la console Gestionnaire de service Internet (IIS)



Dans la console, on se place sur notre serveur ...



(ici SRV-DC2), puis dans la section IIS on clic sur Certificats de serveur



un **certificat auto-signé** du serveur peut apparaître, mais souvent aucun certificat n'existe sur une machine fraichement installée

N.B : il peut y avoir d'autres certificats de type autre que serveur Web

🕞 Gestionnaire des services Internet (IIS)		– 🗆 X
← → ♥ SRV-DC2 →		🖸 🐼 🔯 🕡 🕶
Fichier Affichage Aide		
Connexions Connexions Page de démarrage SRV-DC2 (CABARE-INTRA\Administrateur) Cabarter Pools d'applications Sites	Certificats de serveur         Utilisez cette fonction pour demander et gérer les certificats servant au serveur Web pour accéder aux sites Web configurés pour le protocole SSL.         Filtrer :       • • • • • • • • • • • • • • • • • • •	Actions Importer Créer une demande de certificat Terminer la demande de certificat Créer un certificat de domaine Créer un certificat auto-signé

Pour avoir un certificat de domaine (la racine PKI étant déjà créé), il faut demander Créer un certificat de domaine... (et surtout pas auto-signé)

N.B: on peut voir coté autorité de certification (là où notre pki est installée)que pour l'instant notre serveur **srv-dc2** n'a pas de certificat

a certsrv - [Autorité de certification (Local)\cabare-intra-SRV-DC1-pki-CA\Certificats délivrés]

Fichier Action Affichage ?			
🗢 🔿 🖄 🔯			
<ul> <li>Autorité de certification (Local)</li> <li>cabare-intra-SRV-DC1-pki-CA</li> <li>Certificats révoqués</li> <li>Certificats délivrés</li> <li>Demandes en attente</li> <li>Demandes ayant échoué</li> <li>Modèles de certificats</li> </ul>	ID de la demande 2 3 5 6 8 9	Nom du demandeur CABARE-INTRA\Administrateur CABARE-INTRA\Administrateur CABARE-INTRA\SRV-DC\$ CABARE-INTRA\SRV-DC\$ CABARE-INTRA\SRV-DC1\$ CABARE-INTRA\Administrateur	Nom commun d'émission srv-rds1.cabare-intra.net srv-gtw.cabare-intra.net SRV-DC.cabare-intra.net srv-dc.cabare-intra.net srv-dc1.cabare-intra.net Users Administrateur



Cela déclenche un assistant, dont seule la première ligne **Nom commun** avec le **FQDN du serveur à certifier** est importante

Créer un certificat		?	×
Propriétés du no	om unique		
Indiquez les informations requi ville/localité, utilisez des noms	ses pour le certificat. Lorsque vous entrez le département ou région et la complets et officiels, et n'employez aucune abréviation.		
Nom commun :	srv-dc2.cabare-intra.net		
 Organisation :	formation dossiers de travail		
Unité d'organisation :	formation		
Ville :	grenoble		
Département/région :	isère		
Pays/région :	FR v		

On va chercher notre **autorité racine PKI** de domaine et on peut donner un nom logique à ce certificat...

Créer un certificat	? ×
Autorité de certification en ligne	
Indiquez l'autorité de certification de votre domaine qui signera le certificat. Un nom convivial il doit être facile à retenir. Indiquer une autorité de certification en ligne :	est nécessaire ;
cabare-intra-SRV-DC1-pki-CA\srv-dc.cabare-intra.net	Sélectionner
Exemple : NomAutoritéCertification\NomServeur Nom convivial :	
certif-work-folders	

#### Et on obtient

Connexions	Certifica	ts de serveur			
SRV-DC2 (CABARE-INTRA\Administrateur)	Utilisez cette fonction Web pour accéder aux	pour demander et gérer les sites Web configurés pour l	demander et gerer les certificats servant au serveur Web configurés pour le protocole SSL.		
✓ i Sites	Filtrer :	🔹 🖤 Atteindre 🕞 🤇	Afficher tout 🗸 🗸		
	Nom	Délivré à	Émis par		
	certif-work-folders	srv-dc2.cabare-intra.net	cabare-intra-SRV-DC1-pki-CA		

N.B: on peut voir coté autorité de certification (là où notre pki est installée) que maintenant notre serveur *srv-dc2* possède bien un certificat

🙀 certsrv - [Autorité de certification (Local)\cabare-intra-SRV-DC1-pki-CA\Certificats délivrés]

Fichier Action Affichage ?			
🗢 🔿 🖄 🙆 🖄			
Autorité de certification (Local)	ID de la demande	Nom du demandeur	Nom commun d'émission
✓ dia cabare-intra-SRV-DC1-pki-CA	<b>2</b>	CABARE-INTRA\Administrateur	srv-rds1.cabare-intra.net
Certificats révoqués	3	CABARE-INTRA\Administrateur	srv-gtw.cabare-intra.net
Certificats délivrés	5	CABARE-INTRA\SRV-DC\$	SRV-DC.cabare-intra.net
Demandes en attente	<b>5</b> 6	CABARE-INTRA\SRV-DC\$	srv-dc.cabare-intra.net
Demandes ayant echoue	<b>3</b> 8	CABARE-INTRA\SRV-DC1\$	srv-dc1.cabare-intra.net
Modeles de certificats	<b>1</b> 9	CABARE-INTRA\Administrateur	Users Administrateur
	<b>5</b> 10	CABARE-INTRA\Administrateur	srv-dc2.cabare-intra.net



# Ajout du protocole https avec le certificat

Toujours via la console **Gestionnaire de service Internet (IIS)** on demande dans les **Sites**, sur le Site Web par défaut **Default Web Site** et clic droit **Modifier les liaisons...** 

← → € → SRV-DC2 → S	Sites 🕨 Defaul	t Web Site	•			
Fichier Affichage Aide						
Connexions			D			
🔍 - 📊 🖄 🕼			Page d'ac	cuell o	le Default W	eb Site
Page de démarrage	lministrateur)	Filtrer		- 3	Atteindre 🕞 🖓	Afficher tout
- 👘 Pools d'applications	-	Gestio	on			
V 🖸 Sites						
Default Web Site	Explorer		1	]		
	Modifier les au	torisations				
2	Ajouter une ap	plication				
Ajouter un répe		ertoire virtuel		2		
	Modifier les liai	isons		pression	Document par	En-têtes d

#### On demande Ajouter...

iaisons d	e sites				?	×
Туре	Nom de l'hôte	Port	Adresse IP	Informations sur	Ajouter	
http		80	*		14 PC	

#### https, port 443 avec notre certificat nouvellement crée !

Ajouter la liaison de site	:		$\mathbf{X}$	?	$\times$
Type : https	Adresse IP : Toutes non attribuées		Port:	]	
Nom de l'hôte :					
Certificat SSL :	de nom du serveur				
certif-work-folders		~	Sélectionner	Afficher	
		[	ОК	Annuler	



## GPO avec nouvelle adresse en https

Modification de la GPO avec une adresse en https comme par exemple https://srv-sdc2.cabare-intra.net

💭 Spécifier les paramètres de Dossiers de	travail			—		×
Spécifier les paramètres de Dossiers de	travail	Paramètr	re précédent	Paramètre su	ivant	
<ul> <li>Non configuré</li> <li>Commentaire :</li> <li>Activé</li> <li>Désactivé</li> </ul>						<u>`</u>
Pris en charge sur :	Au minimu	m Windows Server 2008	R2 ou Windows	7		~
Options :		Aide :				
URL de Dossiers de travail : http <mark>s</mark> //srv-dc2.cabare-intra.net		Ce paramètre de straté pour les utilisateurs co autorisés, ou non, à m configuration de la for ordinateur appartenan	égie spécifie le s oncernés, et indi odifier les parar nctionnalité Dos nt à un domaine	erveur Dossiers ique si les utilisat mètres lors de la ssiers de travail s e.	de travail teurs sont sur un	t
Forcer la configuration automatique		Si vous activez ce para concernés reçoivent le de travail lorsqu'ils se o un domaine.	mètre de straté es paramètres de connectent à ur	gie, les utilisateu e la fonctionnali n ordinateur app	irs té Dossier partenant	à

#### Et donc désormais, là ou on avait



#### Entrer l'URL de Dossiers de travail

Si vous n'avez pas d'URL pour Dossiers de travail, contactez votre organisation pour savoir si vous avez accès à la fonctionnalité Dossiers de travail.

URL de Dossiers de travail : https://srvdc1-form16.form1.edu	Sécurité Windows × Dossiers de travail	
	Entrez votre domaine, votre nom d'utilisateur et votre mot de passe.	
	Nom d'utilisateur	
	Mot de passe	
	Mémoriser mes informations	



# **MACHINE HORS DOMAINE**

# PB validité de certificat "hors domaine"

Il parait évidemment impossible de pouvoir utiliser une **GPO utilisateur** de **domaine.** De plus comment faire pour que, que lorsque l'on voudra saisir l'URL de destination, de la forme *https://srv-dc2.cabare-intra.net* on puisse valider le **SSL**... avec un « certificat de domaine »...

## Situation dans un domaine

Une machine de domaine possède comme **Autorité de certification de racine de confiance**, La **PKI** de son domaine

On peut le voir dans le gestionnaire de certificats, (utilisateur) ou mieux via une console mmc dans laquelle on ajouterais le composant logiciel enfichable certificat – ordinateur



» 🗎 Coก์ที่เลnce de l'entreprise



Du coup les certificats "de domaine" sont valables, car ils font référence à une **PKI** connue et accessible



## Situation en Workgroup

Par défaut, une machine en **workgroup**, ne connait évidemment pas la **PKI** de domaine...

Consultation da la consultation		fe de contificación en sie en de constitues	VC
Fichier Action Affichage	Favoris Fenêtre ?	es de certification racines de confianci	e(Certificats)
<ul> <li>Racine de la console</li> <li>Certificats (ordinateur local)</li> <li>Personnel</li> <li>Autorités de certification</li> <li>Certificats</li> <li>Confiance de l'entrepris</li> <li>Autorités de certification</li> <li>Éditeurs approuvés</li> </ul>	Délivré à AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certificat COMODO RSA Certification Au COMODO RSA Code Signing CA Copyright (c) 1997 Microsoft C	Délivré par AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certificatio COMODO RSA Certification Auth COMODO RSA Certification Auth Copyright (c) 1997 Microsoft Corp.	Date d'expir 30/05/2020 13/05/2025 02/08/2028 19/01/2038 09/05/2028 31/12/1999
> Certificats non autorisés	🔄 DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031

sur une machine en workgroup	o par Par	ramètres de	nom d'ord	inateur, de doma	aine et de groupe de trav	ail -
exemple ici <b>PERSO</b>		Nom de l'o	ordinateur :	PORT-P16	5	
		Nom comp	olet :	PORT-P16	5	
	Descri		n de l'ordina	ateur :		
		Groupe de	travail :	PERSO		
si on veut configurer les	Page d'accueil du panne configuration	au de	Gérer D	ossiers de tra	avail	
dossier de travail, on	Configurer Dossiers de tr	Utilisez Dos travail utilisez mê		ez Dossiers de travail pour rendre vos fichiers de travail d ez. même hors connexion.		le travail di
passe manuellement par	comparer bossiers de m					
le panneau de configuration / Configurer dossier de travail				<u>Configurer Dos</u>	ssiers de travail	



#### sauf que au moment ou on tape l'URL du serveur



# Export de certificat:

Depuis une machine du domaine, on va d'exporter le certificat de l'autorité de certification qui se trouve dans le magasin des autorités racines de confiance

pour exporter le certificat obtenu du domaine, on se place dessus, puis on demande **Toutes les taches/ Exporter...** 



Un assistant se declanche



#### Bienvenue dans l'Assistant Exportation du certificat

Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un magasin de certificats vers votre disque.

#### On garde le format par défaut

← 🧽 Assistant Exportation du certificat

Format du fichier d'exportation Les certificats peuvent être exportés dans divers formats de fichiers.

Sélectionnez le format à utiliser :

X.509 binaire encodé DER (\*.cer)

○ X.509 encodé en base 64 (\*.cer)

○ Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)

Indure tous les certificats dans le chemin d'accès de certification, si possible

Échange d'informations personnelles - PKCS #12 (.PFX)

#### Et on le stocke ou l'on veut

← 🧽 Assistant Exportation du certificat

	Fichier à exporter
	Spécifica la part du fichiar à avaarter
	specifiez le nom du fichier a exporter
	Nom du fichier :
	H:\export-certif-client-pki-domaine\export-certif-client-pki-domaine Parcourir
Il n'y a plus	s qu'à confirmer

← 🥜 Assistant Exportation du certificat

#### Fin de l'Assistant Exportation du certificat

Vous avez terminé l'Assistant Exportation du certificat.

Vous avez spécifié les paramètres suivants :	
Nom du fichier	H:\export-certif-clie
Exporter les clés	Non
Inclure tous les certificats dans le chemin d'accès de certification	Non
Format de fichier	X.509 binaire encod

Pour obtenir le fichier contenant la cle publique du certificat

Nom

apport-certif-client-pki-domaine.cer

 $\sim$ 



# Import de certificat sur une machine en workgroup:

Sur notre machine en workgroup, on va donc décider d'importer le certificat de l'autorité de certification dans le magasin des autorités racines de confiance

On se place sur Certificats, Autorités de Certification/ Certificats et on demande Toutes les tâches / importer

🜇 Console1 - [Racine de la console\Certificats (ordinateur local)\Autorités de certification racines de ce

🚟 Fichier Action Affichage	Favoris Fenêtre ?		
🗢 🔿 🔁 📰 📋 🛛 🗟 😹 🛛 🛅			
Racine de la console	Délivré à	Délivré par	
<ul> <li>Certificats (ordinateur local)</li> <li>Personnel</li> </ul>	🔄 AddTrust External CA Root	AddTrust External CA Root	
<ul> <li>Autorités de certification</li> </ul>	Baltimore CyberTrust Root	Baltimore CyberTrust Root	
Certificats	Class 3 Public Primary Certificat	Class 3 Public Primary Certifi	
> 🦳 Confiance de 🛛 Tout	es les tâches >	Importer	

Un assistant se déclenche...



On va chercher le certificat préalablement exporté

🗧 嵾 Assistant Importation du certificat

#### Fichier à importer

Spécifiez le fichier à importer.

Nom du fichier :

Parcourir...

Remarque : plusieurs certificats peuvent être stockés dans un même fichier aux formats suivants :

Échange d'informations personnelles-PKCS #12 (.PFX,.P12)

Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)

Magasin de certificats sérialisés Microsoft (.SST)



On demande de la restaurer



#### On confirme

Assistant Importation du certificat

#### Fin de l'Assistant Importation du certificat

Le certificat sera importé après avoir cliqué sur Terminer.

Vous avez spécifié les paramètres suivants :

Magasin de certificats sélectionné par l'utilisateur	Autorités de certification racines de co
Contenu	Certificat
Nom du fichier	F:\export-certif-client-pki-domaine\exp

#### Et on obtient

\overline \overline Console1 - [Racine de la console\Certificats (ordinateur loca])\Autorités de certification racines de confiance





# Types de Certificats et PKI

Le Certificat sert à être sûr que la machine que l'on utilise soit la bonne. Il existe 3 types de certificats SSL selon leur origine d'émission :

- Autosigné (interne): la machine génère son propre certificat, qui n'est valable que sur... cette machine ! (à éviter !)
- PKI-de-domaine (interne): le certificat est valable sur tout le domaine (il suffit d'être sur une machine membre du domaine pour en bénéficier) (pour les tests, formations, c'est ok)
- PKI-internet (publique): le certificat est valable dans le monde entier. On peut en trouver des gratuits mais en général le service est payant(\*) (obligatoire en production)

(\*) **STARTSSL** propose des certificats gratuits fonctionnant sur 90 % des browser, **RAPIDSSL** propose des certificats connus par quasiment 100% des navigateurs pour environ 40€/an... ensuite il y a **Verisign.**. etc...

Les **PKI = PUBLIC KEY INFRASTRUCTURE** contiennent les clés publiques et privées permettant la reconnaissance et le cryptage= ETAT

Les **PKI** sont elles-mêmes émises, renouvelées et éventuellement révoquées, elles sont construites selon une structure pyramidale. Une **PKI** est une identité qui effectue 3 opérations, elle émet, révoque et renouvelle des **certificats**.

Le **Certificat** = Pièce d'identité. On peut comparer les certificats à des pièces d'identités, permettant de reconnaître des machines dans un domaine. La signature de la carte d'identité prouve que le document de l'état est officiel, la signature du certificat par la PKI fait de même





# Création PKI de domaine:

Si cela n'est pas fait, on crée une **PKI de Domaine**, qui a vocation à être connue dans toute l'**AD**.

La **PKI** se pose sur un serveur unique (pas de redondance possible) que l'on doit par conséquent sauvegarder. Il faut absolument ne pas la perdre !

On peut la stocker sur le **DC** qui intègre les **5 rôles**, et un **CG**. Lorsque l'on sauvera le **System State**, ou l'**AD**, elle fera partie de la sauvegarde...

# Ajout rôle Service de certificats AD

Le rôle peut se poser sur un **DC** ou un serveur spécifique (...). C'est le rôle nommé **Services de certificats Active Directory** 

<b>b</b>	Assistant Ajout de rôles et de fonctionna	alités 📃 🗖 🗙
Sélectionner des	rôles de serveurs	SERVEUR DE DESTINATION dc-form.form.edu
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	Sélectionnez un ou plusieurs rôles à installer sur le serve <b>Rôles</b>	eur sélectionné.
Et toutes les associées n ne modifie rien d'autre	fonctions Assistant Ajout de r Ajouter les fonctionnalité certificats Active Director Les outils suivants sont requis p fonctionnalité, mais ils ne doive sur le même serveur. Outils d'administration de a Outils d'administration doutils des services o [Outils] Outils de	rôles et de fonctionnalités és requises pour Services de ry ? pour la gestion de cette ent pas obligatoirement être installés serveur distant de rôles de certificats Active Directory e gestion de l'autorité de certification
	Assistant Ajout de rôles et de fonctionn	alités 📃 🗖 🗙
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités	fonctionnalités Sélectionnez une ou plusieurs fonctionnalités à installer Fonctionnalités Assistance à distance Base de données interne Windows BranchCache	SERVEUR DE DESTINATION dc-form.form.edu



On est informé que les noms poste et de domaine devront être immuables...



#### Dans les Services de Rôle on demande uniquement Autorité de certification



Outile d'administration de rôles



http://www.cabare.net Page 35 / 41 - Michel Cabaré -

## Paramétrage du rôle Service de certificats AD

Le Gestionnaire de Serveur nous indique qu'il reste à effectuer la configuration des services de certificat Active directory



Cela déclenche un assistant (évidemment il faut être loggué en Administrateur de domaine)



#### Qui va configurer notre rôle Autorité de certification (il faut cocher)

Services de rôle		SERVEUR DE DESTINATIO dc-form.form.ed
Informations d'identificati	Sélectionner les services de rôle à configurer	
Services de rôle Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi Confirmation	<ul> <li>Autorité de certification</li> <li>Inscription de l'autorité de certification via le Web</li> <li>Répondeur en ligne</li> <li>Service d'inscription de périphériques réseau</li> <li>Service Web Inscription de certificats</li> <li>Service Web Stratégie d'inscription de certificats</li> </ul>	

- Michel Cabaré -



- works folder. - ver 1.1

#### De type entreprise (avec publication dans l'AD) la portée sera la forêt



On créé une PKI RACINE, (=équivalent ETAT) Dans certains cas on peut être une autorité de certification secondaire (=équivalent déclarer PREFECTURE)



On demande de créer une nouvelle clé privée... sauf dans le cas d'une réinstallation, car alors on utiliserait une clé déjà existante...

N.B: Si lors d'une réinstallation on génère par erreur une nouvelle clé, il faudra refaire tous les certificats...





– works folder. - ver 1.1

http://www.cabare.net Page 37 / 41 - Michel Cabaré -

On garde le chiffrement proposé **RSA - 2048 - SHA1 et** on autorise l'administrateur à gérer la clé privée

<b>a</b> (	Configuration des services de certificats Active Directory	_ <b>D</b> X
Chiffrement pour	l'autorité de certification	SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati	Spécifier les options de chiffrement	
Services de rôle		
Type d'installation	Sélectionnez un fournisseur de chiffrement :	Longueur de la clé :
Type d'AC	RSA#Microsoft Software Key Storage Provider	<b>2</b> 048 <b>•</b>
Clé privée	Sélectionnez l'algorithme de hachage pour signer les certificats émi	s par cette AC :
Chiffrement	SHA256	
Nom de l'AC	SHA384	
Période de validité	SHA512	
Base de données de certi	SHA1	
Confirmation	· Autorian Pintanatian de Padarinistation la comp Pautorité de s	
Progression	<ul> <li>Autorisez i interaction de l'administrateur lorsque l'autorité de c privée.</li> </ul>	ertification accede à la cle

Le nom proposé par défaut peut être et devrait être modifié, par exemple de form-DC-FORM-CA en form-pki-CA (pour Certification Autorité pki du domaine FORM)

۵ (	Configuration des services de certificats Active Directory	_ <b>D</b> X
Nom de l'autorité	de certification	SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati	Spécifier le nom de l'AC	
Services de rôle		
Type d'installation	Tapez un nom commun pour identifier cette autorité de certification.	Ce nom est ajouté à tous les
Type d'AC	certificats emis par l'autorite de certification. Les valeurs des suffixes automatiquement, mais elles sont modifiables.	du nom unique sont generees
Clé privée		
Chiffrement	Nom commun de cette AC :	
Nom de l'AC	тогт-ркі-СА	
Période de validité	Suffixe du nom unique :	
Base de données de certi	DC=form,DC=edu	
Confirmation	Apercu du nom unique :	
Progression	CN=form-pki-CA.DC=form.DC=edu	
Résultats		

Cela deviendra le nom de l'Autorité de Certification qui apparaîtra dans la console Services de Certificats Active Directory

On indique une durée de validité (on met la durée que l'on veut)

Période de validite	SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati Services de rôle	Spécifier la période de validité
Type d'installation Type d'AC Clé privée	Sélectionnez la période de validité du certificat généré pour cette autorité de certification :           5         Années           Date d'expiration de l'AC : 24/05/2021 22:32:00
Chiffrement Nom de l'AC Période de validité	La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.
Base de données de certi Confirmation	



#### On garde les emplacements de stockage par défaut

P	Configuration des services de certificats Active Directory	_ <b>D</b> X
Base de données	de l'autorité de certification	SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati Services de rôle	Spécifier les emplacements des bases de donn	ées
Type d'installation	Emplacement de la base de données de certificats :	
Type d'AC	C:\Windows\system32\CertLog	
Clé privée	Emplacement du journal de la base de données de certificats :	
Chiffrement	C:\Windows\system32\CertLog	
Nom de l'AC		
Période de validité		
Base de données de certi		
Confirmation		

## Un résumé est affiché, on demande **Configurer**

<b>a</b>	Configuration des services de	e certificats Active Directory
Confirmation		SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati	Pour configurer les rôles, service	s de rôle ou fonctionnalités ci-après, cliquez sur Configurer.
Services de rôle	<ul> <li>Services de certificats Act</li> </ul>	ive Directory
Type d'installation Type d'AC	Autorité de certification	
Clé privée	Type d'AC : Fournisseur de services de	Racine d'entreprise RSA#Microsoft Software Key Storage Provider
Chiffrement Nom de l'AC	chiffrement : Algorithme de hachage :	SHA1
Période de validité Base de données de certi	Longueur de la clé : Autoriser l'interaction de l'administratour :	2048 Désactivé
Confirmation	Période de validité du certificat	: 24/05/2021 22:32:00
Progression Résultats	Nom unique : Emplacement de la base de données de certificats :	CN=torm-pki-CA,DC=torm,DC=edu C:\Windows\system32\CertLog
	Emplacement du journal de la base de données de certificats :	C:\Windows\system32\CertLog
		< Précédent Suivant > Configurer Annuler

#### Et on a une confirmation

A	Configuration des services de certificats Active Directory
Résultats	SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati	Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :
Services de rôle	<ul> <li>Services de certificats Active Directory</li> </ul>
Type d'installation	Autorité de cartification
Type d'AC	En savoir plus sur la configuration de l'autorité de certification
Clé privée	



# **Visualisation PKI**

Désormais une MMC nouvelle est disponible dans les Outils du **gestionnaire de serveur**...nommée **Autorité de certification !** 

Sur le Serveur ou on a installé l'autorité nom de l'Autorité Ì۵ certsrv - [Autorité de certification (Local)] Fichier Action Affichage ? Þ 🔿 🗟 🚺 🕨 🔳 🙀 Autorité de certification (Local) Nom Description 🔺 🝶 form-pki-CA 🚽 form-pki-CA Autorité de certification Certificats révoqués Certificats délivrés On se place sur la Pki et on demande Propriétés autorité de certification (Local) Nom Description 🗸 🚽 form1-pki-CA form1-pki-CA Autorité de certification Certificats révoqués Toutes les tâches > Certificats délivrés Demandes en attente Actualiser 📔 Demandes ayant échoué Propriétés Modèles de certificats ? × Propriétés de : form1-pki-CA ll ne reste plus au'à Extensions Stockage Gestionnaires de certificats afficher le certificat Agents d'inscription Audit Agents de récupération Sécurité Général Module de stratégie Module de sortie Autorité de certification Nom : form1-pki-CA Certificats d'autorité de certification : Afficher le certificat Onglet Général





http://www.cabare.net Page 40 / 41 - Michel Cabaré -

# **Renouvellement PKI de domaine:**

forcément cette PKi va arriver à échéance un jour

il suffira alors de demander Toutes les tâches / Renouveler le Certificat d'autorité de certification



un message apparaît pour stopper le service

Installer un certificat d'autorité de certification	×
Les services de certificats Active Directory ne peuvent pas s'exécuter pendant cette opération. Voulez-vous arrêter les services de certificats Active Directory maintenant ?	
Oui	Non

il ne faut pas renouveler les clés...



et on obtient le renouvellement pour 5 ans...



NON