Letort Léo

# Compte rendu d'Installation d'un « Windows 2012R2 PKI »

# Table des matières

Objectif(s) :	
Légende :	2
Configuration principale :	
Installation :	9
Configuration de l'installation :	
Certificat racine :	
Exporter le certificat racine :	
Interface Web Certsrv :	
Création d'un modèle de certificat :	
Création d'un certificat SSL :	
Configuration serveur IIS :	
Navigation sur l'interface web :	
Connexion certifié en TSE :	

# **Objectif(s) :**

Dans ce tutoriel, nous allons créer une autorité de certification racine d'entreprise (liée à l'Active Directory) et nous modifierons les stratégies de groupe pour que les clients de l'Active Directory reçoivent automatiquement le certificat de notre autorité de certification racine.

Ainsi, notre autorité sera reconnue par les ordinateurs clients et aucun avertissement ne s'affichera concernant nos certificats SSL.

# Légende :

Les commandes ou les chemins (absolue/relatif) sont en gras, souligné et en italique ex :

#### Apt-get update

> Des captures d'écrans ont été prises afin de faciliter la compréhension du lecteur.

Machine	Os	Distribution	Version	C/S	IP
POSTE21	Windows	Windows	2012	S	192.168.1.143
	R2				W2012R2PKI

# **Configuration principale :**

Installation du Système d'exploitation :

🕞 💰 Installation de Windows	l	x
Sélectionner le système d'exploitation à installer		
Système d'exploitation	Archi	
Version d'évaluation de Windows Server 2012 R2 Standard (installation minimale)	х64	
Version d'évaluation de Windows Server 2012 R2 Standard (serveur avec une interface gra	хб4	
Version d'évaluation de Windows Server 2012 R2 Datacenter (installation minimale)	х64	
Version d'évaluation de Windows Server 2012 R2 Datacenter (serveur avec une interface gr	хб4	
<	>	
Description : Cette option est utile lorsqu'une interface graphique utilisateur est nécessaire, par exemple, assurer la compatibilité descendante d'une application qui ne peut pas être exécutée sur ur installation minimale. Tous les rôles et fonctionnalités serveur sont pris en charge. Vous po changer d'option d'installation plus tard. Consultez « Options d'installation Windows Serve	pour ie uvez r ».	
	Suivant	t

# Paramètres

Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.

Nom d'utilisateur	Administrateur
Mot de passe	•••••
Entrez de nouveau le mot de passe	······

Password1234

Letort Léo



Nous allons ajouter le DNS de notre serveur LEBANNU 1 afin que notre serveur W2012R2PKI soit sur le domaine : GSB.local

Propriétés de : Protocole Intern	net version 4 (TCP/IPv4)
Généra	
んく Les paramètres IP peuvent être détern réseau le permet. Sinon, vous devez di appropriés à votre administrateur rése	ninés automatiquement si votre emander les paramètres IP au.
Obtenir une adresse IP automatiq	uement
$- \odot$ Utiliser l'adresse IP suivante :	
Adresse IP :	192.168.1.143
Masque de sous-réseau :	255 . 255 . 255 . 0
Passerelle par défaut :	192.168.1.254
Obtenir les adresses des serveurs	DNS automatiquement
<ul> <li>Otiliser l'adresse de serveur DNS s</li> </ul>	suivante :
Serveur DNS préféré :	192.168.1.130
Serveur DNS auxiliaire :	192.168.1.110
🗌 Valider les paramètres en quittan	t Avancé
	OK Annuler

Voici le gestionnaire de serveur :

<b>E</b>	Gestionnaire de serveur	_ 0 ×
Gestionna	aire de serveur 🔸 Tableau de bord 🛛 🔹 🕫 🖡 🖉 Gérer Outils	Afficher Aide
Image: Tableau de bord         Image: Serveur local         Image: Tous les serveurs         Image: Services de fichiers et d ▷	DÉMARRAGE       1       Configurer ce serveur local         DÉMARRAGE       2       Ajouter des rôles et des fonctionnalités         3       Ajouter d'autres serveurs à gérer         4       Créer un groupe de serveurs	
	<b>EX SAVOIR PLUS Rôles et groupes de serveurs</b> Rôles:1       Groupes de serveurs:1         Services de fichiers et de serveurs:1       1	Masquer

On va se diriger vers le serveur local afin de le configurer :

<b>B</b>		Gestionnaire de serv	eur				a x
Gestionnai	ire de serveur • Ser	veur local	• (2	)   🏲	Gérer Outils	Afficher	Aide
📰 Tableau de bord	PROPRIÉTÉS Pour WIN-9NOM4H5DANF					TÂCHES	•
Serveur local Tous les serveurs Services de fichiers et d >	Nom de l'ordinateur Groupe de travail	WIN-9NOM4H5DANF WORKGROUP			Dernières mi Windows Up Dernière recl	ses à jour ins date nerche de mi	tallé ses i ≡
	Pare-feu Windows Gestion à distance Bureau à distance Association de cartes réseau Ethernet	Privé : Actif Activé Désactivé Désactivé Adresse IPv4 attribuée ;	ar DHCP, Compatible IPv6		Rapport d'er Programme Configuratio Fuseau horai ID de produi	reurs Windo d'amélioratic n de sécurité re t (Product ID	vs n d€ ren
	Version du système d'exploitation Informations sur le matériel	Microsoft Version d'éva innotek GmbH VirtualBo	uation de Windows Server x	2012 R2 Star	ndard Processeurs Mémoire ins Espace disqu	tallée (RAM) e total	>
	ÉVÉNEMENTS Tous les événements   12 au total					TÂCHES	<b>•</b>
	Filtrer	<b>♀</b> (ii) <b>▼</b>	) •			6	•
	Nom du serveur ID Gra	vité Source		Journal	Date et heure		
Explorateur de fir	WIN-9NOM4H5DANF 8200 Erre WIN-9NOM4H5DANF 8198 Erre 	ur Microsoft-Wir ur Microsoft-Wir ur Microsoft-Wir	dows-Security-SPP dows-Security-SPP dows-Security-SPP	Application Application Application	29/05/2017 11:28:45 29/05/2017 11:28:45 29/05/2017 11:28:45		< = >
					P	🖥 🕼 29	11:34 /05/2017

On va modifier le nom de la machine et inscrire la machine dans le domaine GSB.local :

	Propriétés sys	tème	x	local • 🕲 I I
Paramètres systèm	e avancés nateur	Utilisation à distance Matériel		
Windows utilis ordinateur sur	se les informations su le réseau.	uivantes pour identifier votre		Modification du nom ou du domaine de l'
Description de l'ordinateur :	Par exemple : "Se "Serveur de gestie	rveur de production IIS'' ou on''.		Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom complet de 'ordinateur :	WIN-9NOM4H5D	ANF		Nom de l'ordinateur :
Groupe de travail :	WORKGROUP			W2012R2-PKI
Pour renommer cet ordin ou de groupe de travail,	ateur ou changer de cliquez sur Modifier.	e domaine Modifier		Nom complet de l'ordinateur : W2012R2-PKI
				Autres
				Membre d'un
				Domaine :
				GSB.local
				O Groupe de travail :
				WORKGROUP
	ОК	Annuler Appliq	uer	OK Annuler

Propriétés système	e 	x	
Modification du nom ou du domaine	ار الله الم		
Vous pouvez modifier le nom et l'appartenance de c ordinateur. Ces modifications peuvent influer sur l'ac ressources réseau.	cet ccès aux votre		KGU7NK0Q1NJ KGROUP
Nom de l'ordinateur :			
W2012R2PKI	" ou		
Nom complet de l'ordinateur : W2012R2PKI			Actif
	Autres		tivé
Membre d'un	Modification	du nor	n ou du domaine de l'ordinateur
Omaine :			
GSB.local			
◯ Groupe de travail :	Bienv	enue dar	ns le domaine GSB.local.
WORKGROUP			
ОК			ОК

On va ensuite devoir redémarrer le PC afin de pouvoir mettre en place nos modifications.



Password1234

On va ensuite activer le bureau a distance afin d'avoir plus d'aisance :

PROPRIÉTÉS Pour W2012R2PKI	
Nom de l'ordinateur	W2012R2PKI
Domaine	GSB.local
Pare-feu Windows	Domaine : Actif
Gestion à distance	Activé
<mark>Bureau à distance</mark>	Désactivé
Association de cartes réseau	Désactivé
Ethernet	192.168.1.143

Letort Compte rendu d'installation d'un Windows 2012R2 PKI Léo

Il suffit simplement de cliquer sur Désactivé en face de Bureau à distance, puis cliquer sur Autoriser comme ci-dessous.

Bureau à distance		
Choisissez une option, puis spécifiez qui peut se connecter.		
O Ne pas autoriser les connexions à distance à cet ordinateur		
Autoriser les connexions à distance à cet ordinateur		
<ul> <li>N'autoriser que la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA (recommandé)</li> </ul>		
Comment choisir ? Sélectionnez des utilisateurs		

Propriétés du windows server 2012 :

PROPRIÉTÉS Pour W2012R2PKI	
Nom de l'ordinateur	W2012R2PKI
Domaine	GSB.local
Pare-feu Windows	Domaine : Actif
Gestion à distance	Activá
Bureau à distance	Activé
Association de cartes réseau	Désactivé

# **Installation :**

On va maintenant ajouter le Rôle « Service de certificats Active Directory » Pour cela on va se connecter au serveur en Administrateur du domaine : GSB\Administrateur // Password123

Dans le gestionnaire de serveur, Ajouter des rôles et des fonctionnalités

#### **BIENVENUE DANS GESTIONNAIRE DE SERVEUR**

DÉMARRAGE RAPIDE	1 Configurer ce serveur local
	2 Ajouter des rôles et des fonctionnalités
	3 Ajouter d'autres serveurs à gérer
NOUVEAUTÉS	4 Créer un groupe de serveurs
EN SAVOIR PLUS	

#### Cliquez sur suivant :

à	Assistant Ajout de rôles et de fonctionnalités		
Avant de comm	encer	SERVEUR DE DESTINATION W2012R2PKI.GSB.local	
Avant de commencer Type d'installation	Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctio déterminer les rôles, services de rôle ou fonctionnalités à installer en fonctio de votre organisation, tels que le partage de documents ou l'hébergement o	onnalités. Vous devez n des besoins informatiques d'un site Web.	
Selection du serveur Rôles de serveurs	Pour supprimer des rôles, des services de rôle ou des fonctionnalités : Démarrer l'Assistant Suppression de rôles et de fonctionnalités		
Fonctionnalités Confirmation	Avant de continuer, vérifiez que les travaux suivants ont été effectués :		
Résultats	<ul> <li>Le compte d'administrateur possède un mot de passe fort</li> <li>Les paramètres réseau, comme les adresses IP statiques, sont configurés</li> <li>Les dernières mises à jour de sécurité de Windows Update sont installées</li> <li>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.</li> <li>Cliquez sur Suivant pour continuer.</li> </ul>		
	Ignorer cette page par défaut		
	< Précédent Suivant >	Installer Annuler	

#### Cliquez de nouveau sur suivant :

Sélectionner le ty	pe d'installation SERVEUR DE DESTINATION W2012R2PKI.GSB.local
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	<ul> <li>Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.</li> <li>Installation basée sur un rôle ou une fonctionnalité Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.</li> <li>Installation des services Bureau à distance Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.</li> </ul>
	< Précédent Suivant > Installer Annuler

#### Cliquez encore sur suivant :

a	Assistant Ajout o	de rôles et de fo	nctionnalités	_ <b>D</b> X
Sélectionner le s	erveur de destina	ation		SERVEUR DE DESTINATION W2012R2PKI.GSB.local
Avant de commencer Type d'installation	Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.			
Rôles de serveurs Fonctionnalités Confirmation	Pool de serveurs			
Résultats	Nom W2012R2PKI.GSB.local	Adresse IP 192.168.1.143	Système d'exploitation Microsoft Version d'évaluatio	on de Windows Server 2012
	1 ordinateur(s) trouvé(s) Cette page présente les se commande Ajouter des se nouvellement ajoutés don	rveurs qui exécuten rveurs dans le Gesti t la collection de do	II t Windows Server 2012 et qui c onnaire de serveur. Les serveur nnées est toujours incomplète	ont été ajoutés à l'aide de la s hors ligne et les serveurs ne sont pas répertoriés.
		< Préc	édent Suivant >	Installer Annuler

#### Cochez Service de certificats Active Directory, puis suivant :

Berne and the second se	Assistant Ajout de rôles et de fonctionnalités				
Sélectionner des	rôles de serveurs	SERVEUR DE DESTINATION SRV1.idum.eu			
Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélect	ionné.			
Type d'installation	Rôles	Description			
Sélection du serveur	· · · · · · · · · · · · · · · · · · ·	Les services de certificats Active			
Rôles de serveurs	Serveur DNS (Installé)	Directory (AD CS) servent à créer des autorités de certification et les			
Fonctionnalités	✓ Services AD DS (Installé)	services de rôle associés pour			
AD CS	Services AD FS (Active Directory Federation Servic	utilisés dans diverses applications.			
Services de role	Services AD LDS (Active Directory Lightweight Dire				
Récultats	Services AD RMS (Active Directory Rights Manage				
Nesulata	Services d'activation en volume				
	Services d'impression et de numérisation de docu ≡				
	Services de certificats Active Directory				
	Services de déploiement Windows				
	Services de fichiers et de stockage (2 sur 12 install     Services de stratégie et d'accès réseau				
	Services WSUS (Windows Server Update Services)				
	< III >				
	< Précédent Suivant	> Installer Annuler			

puis suivant :

Avant de commencer Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

# Sélectionner des fonctionnalités

Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

#### Fonctionnalités

# Assistance à distance Base de données interne Windows BranchCache Chiffrement de lecteur BitLocker Client d'impression Internet Client pour NFS Client Telnet Client TFTP Clustering avec basculement Compression différentielle à distance Data Center Bridging Déverrouillage réseau BitLocker DirectPlay Équilibrage de la charge réseau

ш

SERVEUR DE DESTINATION W2012R2PKI.GSB.local

Description Grâce à l'assistance à distance, vous  $\sim$ (ou une personne du support technique) pouvez aider 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.

< Précédent Suivant >

>

Annuler

Installer

#### Puis suivant :

Services de certificats Active Directory Serveur de Destination SRV1.idum.eu	è	Assistant Ajout de rôles et de fonctionnalités 📃 🗖 🗙
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	Services de certif Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	Assistant Ajout de rôles et de fonctionnalités
< Précédent Suivant > Installer Annuler		< Précédent Suivant > Installer Annuler

Cochez les options « Autorité de certification » et « Inscription de l'autorité de certification via le Web »

B	Assistant Ajout de rôles et de fonctionnalités	_ <b>D</b> X	
Sélectionner des s Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	Assistant Ajout de rôles et de fonctionnalités Services de rôle Sélectionner les services de rôle à installer pour Services de ce Services de rôle Autorité de certification Marciption de l'autorité de certification via le Web Répondeur en ligne Service d'inscription de périphérique réseau Service Web Inscription de certificats Service Web Stratégie d'inscription de certificats	L'inscription de l'autorité de certificats Active Directory Description L'inscription de l'autorité de certification via le Web fournit une interface Web simple permettant aux utilisateurs d'effectuer des tâches telles que la demande et le renouvellement de certificats, la récupération des listes de révocation de certificats de carte à puce.	
< Précédent Suivant > Installer Annuler			

#### Puis suivant :

<b>B</b>	Assistant Ajout de rôles et de fonctionnalités	-		x
Rôle Web Server	(IIS) SERVEUR DE	E DESTI SRV1	NATIC .idum.	DN eu
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle <b>Rôle Web Server (IIS)</b> Services de rôle Confirmation Résultats	Les serveurs Web sont des ordinateurs qui vous permettent de partager des informations des intranets ou des extranets. Le rôle Web Server comprend Internet Information Service un sécurité, du diagnostic et de l'administration améliorés, un plate-forme Web unifiée qu 8.5, ASP.NET, ainsi que Windows Cummunication Foundation. À noter : • L'utilisation du Gestionnaire de ressources système Windows (WSRM) permet d'assurer équitable si le Web sert du trafic, particulièrement lorsque plusieurs rôles sont présents ordinateur. • L'installation par défaut du rôle de Web Server (IIS) comprend l'installation des services vous permettent de servir du contenu statique, d'effectuée de légères personnalisations les documents par défaut et les erreurs HTTP), de surveiller et de journaliser l'activité du de configurer la compression du contenu statique.	sur l'il s (IIS) un se sur ce de rô s (telle s serve	ntern 8.5 a gre II rvice et les qu s qu s qu s qu s qu r, e	ui et, vec IS
	Plus d'informations sur Web Server IIS			
	< Précédent Suivant > Installer	Ar	nule	r

# Cliquez sur suivant :

A	Assistant Ajout de rôles et de fonctionnalités	_ <b>D</b> X
Sélectionner des s	services de rôle Sélectionner les services de rôle à installer pour Serveur Web (IIS)	SERVEUR DE DESTINATION SRV1.idum.eu
Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Rôle Web Server (IIS) Services de rôle Confirmation Résultats	Services de rôle	Description Le serveur Web fournit une prise en charge pour les site Web HTML et une prise en charge facultative pour les extensions ASP.NET, ASP et Serveur Web. Vous pouvez utiliser le serveur Web pour héberger un site Web interne ou externe ou pour fournir aux développeur un environnement pour créer des applications basées sur le Web.
	< Précédent Suivant	> Installer Annuler

Cochez l'option « Redémarrer automatiquement le serveur de destination, si nécessaire », puis installer :

<b>b</b>	Assistant Ajout de rôles et de fonctionnalités 📃 🗖	x		
Confirmer les séle	ections d'installation Serveur de destination Serveur de destination Serveur de destination	4 4		
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Ecoctionnalitée	Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez su 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 d'activer leurs cases à cocher	лг		
AD CS Services de rôle Rôle Web Server (IIS) Services de rôle Confirmation	Outils d'administration de serveur distant     //       Outils d'administration de rôles     //       Outils de services de certificats Active Directory     //       Outils de gestion de l'autorité de certification       Serveur Web (IIS)			
Résultats	Outils de gestion Compatibilité avec la gestion IIS 6 Compatibilité de métadonnées IIS 6 Console de gestion IIS Console de gestion IIS Exporter les paramètres de configuration Spécifier un autre chemin d'accès source	5		
< Précédent Suivant > Installer Annuler				

# **Configuration de l'installation :**

Cliquez sur le lien « Configurer les services de certificats Active Directory sur le serveur de destination »

<b>a</b>	Assistant Ajout de rôles et de fonctionnalités 📃 🗖	x
Progression de l'ir	serveur de destinati srv1.idum	ON Leu
Avant de commencer	Afficher la progression de l'installation	
Type d'installation	1 Installation de fonctionnalité	
Sélection du serveur	·	
Rôles de serveurs	Configuration requise. Installation réussie sur SRV1.idum.eu.	
Fonctionnalités	Services de certificats Active Directory	^
AD CS	Des étapes supplémentaires sont nécessaires pour la configuration des services de certificats	=
Services de rôle	Active Directory sur le serveur de destination. Configurer les services de certificats Active Directory sur le serveur de destination	
Rôle Web Server (IIS)	Autorité de certification	
Services de rôle	Inscription de l'autorité de certification via le Web	
Confirmation	Outils d'administration de serveur distant	
Résultats	Outils d'administration de rôles Outils des services de certificats Active Directory	
	Outils de gestion de l'autorité de certification	<u> </u>
	Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examine 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	z
	<pre>&lt; Précédent   Suivant &gt; Fermer Annul </pre>	er

L'assistant de configuration vous demande ensuite de définir un compte avec les droits demandés pour continuer la configuration. Cliquez sur suivant :

Informations d'ider	tification	/EUR DE DESTINATION W2012R2PKI.GSB.local
Informations d'identificati Services de rôle Confirmation	Spécifier les informations d'identification pour config services de rôle	gurer les
Progression Résultats	Pour installer les services de rôle suivants, vous devez être membre du grou local : • Utiliser l'autorité de certification autonome • Inscription de l'autorité de certification via le Web • Répondeur en ligne	pe Administrateurs
	Pour installer les services de rôle suivants, vous devez être membre du grou d'entreprise : • Autorité de certification d'entreprise • Service Web Stratégie d'inscription de certificats • Service Web Inscription de certificats • Service d'inscription de périphériques réseau	pe Administrateurs
	Informations d'identification : W2012R2PKI\Administrateur Modifie	r
	< Précédent Suivant > Cont	figurer Annuler

Cochez les deux options « Autorité de certification « et Inscription de l'autorité de certification via le web » Ensuite cliquez sur Suivant :

<b>a</b>	Configuration des services de certificats Active Directory	_ <b>D</b> X
Services de rôle		SERVEUR DE DESTINATION W2012R2PKI.GSB.local
Informations d'identificati 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 Progression Résultats	Sélectionner les services de rôle à configurer Autorité de certification Inscription de l'autorité de certification via le Web Répondeur en ligne Service d'inscription de périphériques réseau Service Web Inscription de certificats Service Web Stratégie d'inscription de certificats	
	En savoir plus sur les rôles de serveur AD CS	
	< Précédent Suivant >	Configurer Annuler

Sélectionnez « Autorité de certification d'entreprise ». Pour info cette option est grisée si votre serveur n'est pas dans un domaine. Ensuite cliquez sur « Suivant ».

<b>a</b>	Configuration des services de certificats Active Directory
Type d'installation	SERVEUR DE DESTINATION W2012R2PKI.GSB.local
Informations d'identificati	specifier le type d'installation de l'AC
Services de roie Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC Demande de certificat Base de données de certi Confirmation Progression Résultats	<ul> <li>Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.</li> <li> Autorité de certification d'entreprise Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat. </li> <li> Autorité de certification autonome Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion). </li> </ul>
	En savoir plus sur le type d'installation           < Précédent

Sélectionnez « Autorité de certification racine », car nous n'avons pas de certificat signé par une autre autorité de certification supérieur et d'un organisme de certification. Ensuite cliquez sur « Suivant ».

<b>b</b>	Configuration des services de certificats Active Directory		
Type d'autorité de	e certification SERVEUR DE DESTINATION W2012R2PKI.GSB.local		
Informations d'identificati	Spécifier le type de l'AC		
Services de rôle			
Type d'installation	Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez		
Type d'AC	une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de		
Clé privée	certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la		
Chiffrement	hiérarchie PKI.		
Nom de l'AC	<ul> <li>Autorité de certification racine</li> </ul>		
Période de validité	Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.		
Base de données de certi			
Confirmation	Autorité de certification secondaire		
Progression	autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la		
Résultats	hiérarchie.		
	En savoir plus sur le type d'autorité de certification		
	< Précédent Suivant > Configurer Annuler		

Sélectionnez « Créer une clé privée », car nous ne disposons pas de clé existante. Ensuite cliquez sur « Suivant ».

<b>b</b>	Configuration des services de certificats Active Directory
Clé privée	SERVEUR DE DESTINATION W2012R2PKI.GSB.local
Informations d'identificati. Services de rôle Turos d'installation	Spécifier le type de la clé privée Pour générer et émettre des certificats aux clients une autorité de certification doit posséder une
Type d'AC	clé privée.
Clé privée Chiffrement	<ul> <li>Créer une clé privée</li> <li>Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.</li> </ul>
Nom de l'AC Période de validité	<ul> <li>Utiliser la clé privée existante</li> <li>Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de</li> </ul>
Base de données de certi. Confirmation	la réinstallation d'une AC. Sélectionner un certificat et utiliser sa clé privée associée Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un
Progression Résultats	certificat et utiliser sa clé privée associée. Sélectionner une clé privée existante sur cet ordinateur Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure
	ou pour utiliser une clé privée d'une autre source. En savoir plus sur la clé privée
	< Précédent Suivant > Configurer Annuler

#### Sélectionnez « SHA256 » et cliquez sur « Suivant » :

2	Configuration des services de certificats Active Directory	_ <b>_</b> X
Chiffrement pour	l'autorité de certification	SERVEUR DE DESTINATION W2012R2PKI.GSB.local
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 🔹	2048 🔻
Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi	Sélectionnez l'algorithme de hachage pour signer les certificats émis SHA256 SHA384 SHA512 SHA1 v	par cette AC :
Progression Résultats	Autorisez l'interaction de l'administrateur lorsque l'autorité de ce privée.	rtification accède à la clé
	En savoir plus sur le chiffrement	
	< Précédent Suivant >	Configurer Annuler

#### Suivant :

Letort

Léo

<b>b</b> (	Configuration des services de certificats Active Directory	
Nom de l'autorité	de certification	SERVEUR DE DESTINATION W2012R2PKI.GSB.local
Informations d'identificati Services de rôle	Spécifier le nom de l'AC	
Type d'installation Type d'AC	Tapez un nom commun pour identifier cette autorité de certification. certificats émis par l'autorité de certification. Les valeurs des suffixes o automatiquement, mais elles sont modifiables.	Ce nom est ajouté à tous les du nom unique sont générées
Clé privée Chiffrement	Nom commun de cette AC : GSR-W2012R2PKI-CA	
Nom de l'AC Période de validité	Suffixe du nom unique :	
Confirmation Progression	Aperçu du nom unique :	
Résultats	CN-030-W201212PN-CA,DC-030,DC-100a1	
	En savoir plus sur le nom de l'autorité de certification	
	< Précédent Suivant >	Configurer Annuler

On va ensuite définir une durée de validité du certificat de l'autorité :

<b>a</b>	Configuration des services de certificats Active Directory
Période de validi	té SERVEUR DE DESTINATION W2012R2PKI.GSB.local
Informations d'identificati	Spécifier la période de validité
Services de rôle	
Type d'installation	Sélectionnez la période de validité du certificat généré pour cette autorité de certification :
Type d'AC	15 Années 💌
Clé privée	Date d'expiration de l'AC : 29/05/2032 17:20:00
Chiffrement	La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la
Nom de l'AC	période de validité pour les certificats qu'elle émettra.
Période de validité	
Base de données de certi	
Confirmation	
Progression	
Résultats	
	En savoir plus sur la période de validité
	< Précédent Suivant > Configurer Annuler

#### Cliquez ensuite sur « Suivant » :

<u>Ъ</u> (	Configuration des services de certificats Active Directory	_ <b>D</b> X
Base de données	de l'autorité de certification	SERVEUR DE DESTINATION W2012R2PKI.GSB.local
Informations d'identificati Services de rôle Type d'installation	Spécifier les emplacements des bases de donn Emplacement de la base de données de certificats :	ées
Type d'AC	C:\Windows\system32\CertLog	
Clé privée	Emplacement du journal de la base de données de certificats :	
Nom de l'AC	C:\Windows\system32\CertLog	
Période de validité		
Base de données de certi		
Confirmation		
Progression		
Résultats		
	En savoir plus sur la base de données de l'autorité de certification	
	< Précédent Suivant >	Configurer Annuler

Cliquez sur « Configurer » si les paramètres affichés sont corrects :

<b>A</b>	Configuration des services de	e certificats Active Directory	_ <b>_</b> ×
Confirmation		SEF	RVEUR DE DESTINATION W2012R2PKI.GSB.local
Informations d'identificati	Pour configurer les rôles, service	s de rôle ou fonctionnalités ci-après, cliqu	ez sur Configurer.
Services de rôle	<ul> <li>Services de certificats Acti</li> </ul>	ive Directory	
Type d'installation	Autorité de certification		
Type d'AC	Type d'AC :	Racine d'entreprise	
Clé privée	Fournisseur de services de	RSA#Microsoft Software Key Storage Pro	vider
Chiffrement	chiffrement :		
Nom de l'AC	Algorithme de hachage :	SHA256	
Période de validité	Longueur de la clé :	2048	
Base de données de certi	Autoriser l'interaction de l'administrateur :	Désactivé	
Confirmation	Période de validité du certificat	: 29/05/2032 17:20:00	
Progression	Nom unique :	CN=GSB-W2012R2PKI-CA,DC=GSB,DC=I	local
Résultats	Emplacement de la base de données de certificats :	C:\Windows\system32\CertLog	
	Emplacement du journal de la base de données de certificats :	C:\Windows\system32\CertLog	
	Inscription de l'autorité de cer	tification via le Web	
		< Précédent Suivant > Co	nfigurer Annuler

#### Une fois la configuration terminée, cliquez sur « Fermer » :

<b>a</b> (	Configuration des services de certificats Active Directory
Résultats	SERVEUR DE DESTINATION W2012R2PKI.GSB.local
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 certification
Type d'AC	En savoir plus sur la configuration de l'autorité de certification
Clé privée	
Chiffrement	Inscription de l'autorité de certification via le 💟 Configuration réussie Web
Nom de l'AC	En savoir plus sur la configuration de l'inscription par le Web
Période de validité	
Base de données de certi	
Confirmation	
Progression	
Résultats	
	< Précédent Suivant > Fermer Annuler

Lors de l'installation de l'autorité de certification dans un domaine, le certificat de l'autorité de certification crée est automatiquement déployé sur les machines du domaine dans le « magasin autorité racine de confiance ».

certm	ngr - [Certificats - Utilisateur ac	tuel\Autorités de certification	racines de cont	iance\Certificats]		×
Fichier Action Affichage ?						
🗢 🔿 🙍 📆 📋 🗟 😽	?					
<ul> <li>Certificats - Utilisateur actuel</li> <li>Personnel</li> <li>Autorités de certification raci</li> <li>Certificats</li> <li>Confiance de l'entreprise</li> <li>Autorités de certification inte</li> <li>Objet utilisateur Active Direct</li> <li>Éditeurs approuvés</li> <li>Certificats non autorisés</li> <li>Autorités de certification raci</li> <li>Personnes autorisées</li> <li>Émetteurs d'authentification</li> <li>Racines de confiance de carte</li> </ul>	Délivré à Baltimore CyberTrust Root Class 3 Public Primary Certificat Copyright (c) 1997 Microsoft C didum-SRV1-CA Microsoft Root Authority Microsoft Root Certificate Auth Microsoft Root Certificate Auth Microsoft Root Certificate Auth NO LIABILITY ACCEPTED, (c)97 thavte Primary Root CA Thavte Timestamping CA	Délivré par Baltimore CyberTrust Root Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. idum-SRV1-CA Microsoft Authenticode(tm) Root Microsoft Root Certificate Authori Microsoft Root Certificate Authori Microsoft Root Certificate Authori Microsoft Root Certificate Authori MO LIABILITY ACCEPTED, (c)97 V thawte Primary Root CA	Date d'expirati 13/05/2025 02/08/2028 31/12/1999 24/09/2020 01/01/2000 31/12/2020 10/05/2021 24/06/2035 23/03/2036 08/01/2004 17/07/2036 01/01/2021	Rôles prévus Authentification du Messagerie électro Enregistrement des <tout> Messagerie électro <tout> <tout> <tout> <tout> <tout> erout&gt; Enregistrement des Authentification du Enregistrement des</tout></tout></tout></tout></tout></tout>	Nom convivial Baltimore CyberTru VeriSign Class 3 Pu Microsoft Timesta <aucun> Microsoft Authenti Microsoft Root Aut Microsoft Root Cert Microsoft Root Cert VeriSign Time Stam thawte</aucun>	Stat
	UTN-USERFirst-Object	UTN-USERFirst-Object VeriSign Class 3 Public Primary Ce	09/07/2019 17/07/2036	Système de fichiers Authentification du	USERTrust VeriSign	>
Le magasin Autorités de certification r	racines de confiance contient 14 certific	cats.				

# **Certificat racine :**

Pour voir le certificat racine suivez les instructions suivantes :

Appuyez sur les touches WIN + R, afin d'ouvrir la fenêtre « Exécuter » puis tapez « MMC ».

	Exécuter	x	
	Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.		
<u>O</u> uvrir :	mmc	<b>~</b>	
	🛞 Cette tâche sera créée avec les autorisations d'administrateur.		
	OK Annuler Parco <u>u</u> rir.		

On van ensuite allez dans « Fichier », puis « Ajouter/supprimer un composant logiciel enfichable »

-									
-	Fich	ier	?						
		No		Ctrl+N					
		Ou	vrir					Ctrl+O	
		Eni	registrer					Ctrl+S	
		Enregistrer sous							
		Ajouter/Supprimer un composant logiciel enfichable Ctrl+M							
		Options							
		1 C:\Windows\system32\certsrv							
		2 C:\Windows\system32\CompMgmt							
		3 C:\Windows\system32\gpmc							
		4 C:\Windows\system32\dnsmgmt							
		Quitter							

On va ensuite cliquez sur « Certificats » puis l' « ajouter ».

Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et les configurer. Pour les composants logiciels enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées.         Composants logiciels enfichables disponibles :       Composants logiciels enfichables disponibles :         Composant logiciel enfi       Fournisseur         Autorité de certifica       Microsoft Cor         Configuration du clie       Microsoft Cor         Contrôle ActiveX       Microsoft Cor         Contrôle ActiveX       Microsoft Cor         DHCP       Microsoft Cor         DNS       Microsoft Cor         É cliteur d'objets de s       Microsoft Cor         Microsoft Cor       V         É cliteur d'objets de s       Microsoft Cor         É cliteur d'objets de s       Microsoft Cor         É cliteur d'objets de s       Microsoft Cor         Microsoft Cor       V         É cliteur d'objets de s       M	Ajo	outer ou sup	oprimer des co	mposants logiciels enficha	bles 🛛 🗙
Composants logiciels enfichables disponibles : Composant logiciel enfi Fournisseur Analyseur de perfor Microsoft Cor Autorité de certificas: Microsoft Cor Configuration du clie Microsoft Cor Contrôle ActiveX Microsoft Cor Contrôle WMI Microsoft Cor DHCP Microsoft Cor DDNS Microsoft Cor Dossier Microsoft Cor É diteur d'objets de s Microsoft Cor É diteur d'objets de s Microsoft Cor Description : Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.	Vous pouvez sélectionner des co composants logiciels enfichables	omposants logic ; extensibles, vo	iels enfichables par ous pouvez spécifie	mi ceux disponibles sur votre ordinate r quelles extensions doivent être acti	eur, et les configurer. Pour les vées.
Composant logiciel enfi Fournisseur   Analyseur de perfor Microsoft Cor   Alutorité de certificat Microsoft Cor   Configuration du clie Microsoft Cor   Configuration et an Microsoft Cor   Contrôle ActiveX Microsoft Cor   Contrôle ActiveX Microsoft Cor   Contrôle ActiveX Microsoft Cor   DhCP Microsoft Cor   DhCP Microsoft Cor   Dossier Microsoft Cor   E diteur d'objets de s Microsoft Cor   É diteur d'objets de s Microsoft Cor   É diteur d'objets de s Microsoft Cor   Microsoft Cor V	Composants logiciels enfichables	; disponibles :		Composants logiciels enfi, sélectionné	és :
Analyseur de perfor Microsoft Cor   Autorité de certificats Microsoft Cor   Configuration du clie Microsoft Cor   Configuration et an Microsoft Cor   Contrôle ActiveX Microsoft Cor   Contrôle ActiveX Microsoft Cor   DHCP Microsoft Cor   DNS Microsoft Cor   Domaines et approb Microsoft Cor   Dossier Microsoft Cor   Dossier Microsoft Cor   E diteur d'objets de s Microsoft Cor   É diteur d'objets de s Microsoft Cor   Microsoft Cor Avancé   Description :  Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.     OK Annuler	Composant logiciel enfi For	urnisseur	~	🚞 Racine de la console	Modifier les extensions
Autorité de certifica Microsoft Cor   Certificats Microsoft Cor   Configuration du clie Microsoft Cor   Contrôle ActiveX Microsoft Cor   Contrôle ActiveX Microsoft Cor   Contrôle WMI Microsoft Cor   DHCP Microsoft Cor   DNS Microsoft Cor   Dossier Microsoft Cor   E diteur d'objets de s Microsoft Cor   É diteur d'objets de s Microsoft Cor   Description : Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.	🔊 Analyseur de perfor Mic	crosoft Cor			
Certificats       Microsoft Cor       Monter         Configuration du clie       Microsoft Cor       Monter         Contrôle ActiveX       Microsoft Cor       Descendre         Contrôle WMI       Microsoft Cor       Descendre         OHCP       Microsoft Cor       Descendre         Domaines et approb       Microsoft Cor       Ajouter >         Dossier       Microsoft Cor       Avancé         Éditeur d'objets de s       Microsoft Cor       Avancé         Description :       Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.         OK       Annuler	🔄 🚋 Autorité de certifica Mic	crosoft Cor	=		Supprimer
Configuration du clie Microsoft Cor   Configuration et an Microsoft Cor   Contrôle ActiveX Microsoft Cor   Contrôle WMI Microsoft Cor   Contrôle WMI Microsoft Cor   PDHCP Microsoft Cor   DNS Microsoft Cor   Dossier Microsoft Cor   Dossier Microsoft Cor   Contrôle diteur d'objets de s Microsoft Cor   É diteur d'objets de s Microsoft Cor   É diteur d'objets de s Microsoft Cor   Microsoft Cor V	Certificats Mic	crosoft Cor	-		
Image: Configuration et an       Microsoft Cor         Image: Contrôle ActiveX       Microsoft Cor         Image: Contrôle ActiveX       Microsoft Cor         Image: Contrôle WMI       Microsoft Cor         Image: Control WMI       Microsoft Cor         Image: Control With Without Control With Without Cortain Cortain Without Cortain Without Cortain Without Cortain Without	Configuration du clie Mic	crosoft Cor			Monter
Image: Contrôle ActiveX       Microsoft Cor         Image: Contrôle WMI       Microsoft Cor         Image: DhCP       Microsoft Cor         Image: Dossiers partagés       Microsoft Cor         Image: Dossiers partagés       Microsoft Cor         Image: Editeur d'objets de s       Microsoft Cor         Image: Description :       Image: Editeur d'objets de s         Image: Descender Image: Editeur d'objets de s       Image: Editeur d'objets de s     <	📑 🔤 Configuration et an Mic	crosoft Cor			
Image: Contrôle WMI       Microsoft Cor         Image: DHCP       Microsoft Cor         Image: DNS       Microsoft Cor         Image: Dossier       Microsoft Cor         Image: Dossier Dossier       Microsoft Cor         Image: Dossier Dossier       Microsoft Cor         Image: Editeur d'objets de s       Microsoft Cor         Image: Dossier       Microsoft Cor         Image: Editeur d'objets de s       Microsoft Cor         Image: Dossier       Microsoft Cor         Image: Dossier       Microsoft Cor         I	Contrôle ActiveX Mic	crosoft Cor			Descendre
PHCP       Microsoft Cor         DNS       Microsoft Cor         Domaines et approb       Microsoft Cor         Dossier       Microsoft Cor         Dossiers partagés       Microsoft Cor         É diteur d'objets de s       Microsoft Cor         É Éditeur d'objets de s       Microsoft Cor         Microsoft Cor       Y         Description :       Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.         OK       Annuler	🛋 Contrôle WMI Mic	crosoft Cor	Ajouter >		
DNS       Microsoft Cor         Domaines et approb       Microsoft Cor         Dossier       Microsoft Cor         Dossiers partagés       Microsoft Cor         Éditeur d'objets de s       Microsoft Cor         Pescription :       Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.         OK       Annuler	🖞 DHCP Mic	crosoft Cor			
Image: Domaines et approb       Microsoft Cor         Image: Dossier       Microsoft Cor         Image: Dossier partagés       Microsoft Cor         Image: Editeur d'objets de s       Microsoft Cor         Image: Description :       Image: Editeur d'objets de service ou un ordinateur.         Image: Domage: Description :       Image: Editeur d'objets de service ou un ordinateur.         Image: Docs in the description in	📲 DNS Mic	crosoft Cor			
Image: Dossier Microsoft Cor       Microsoft Cor         Image: Dossiers partagés Microsoft Cor       Microsoft Cor         Image: Éditeur d'objets de s Microsoft Cor       Microsoft Cor         Image: Éditeur d'objets de s Microsoft Cor       Microsoft Cor         Image: Editeur d'objets de s Microsoft Cor       Microsoft Cor         Image: Editeur d'objets de s Microsoft Cor       Microsoft Cor         Image: Description :       Image: Cortex and the parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.         OK       Annuler	🛛 🚮 Domaines et approb Mic	crosoft Cor			
	📄 Dossier 🛛 Mic	crosoft Cor			
Image: Éditeur d'objets de s Microsoft Cor       Image: Microsoft Cor       Image: Microsoft Cor         Image: Éditeur d'objets de s Microsoft Cor       Image: Microsoft Cor       Image: Microsoft Cor         Description :       Image: Microsoft Cor       Image: Microsoft Cor       Image: Microsoft Cor         Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.       Image: Microsoft Cor       Image: Microsoft Cor         OK       Annuler	👔 Dossiers partagés 🛛 Mic	crosoft Cor			
Image: Editeur d'obiets de s Microsoft Cor       Mance         Description :       Image: Editeur d'obiets de service ou parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.         OK       Annuler	🗐 🗐 Éditeur d'objets de s Mic	crosoft Cor			· · ·
Description : Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur. OK Annuler	🗐 Éditeur d'obiets de s Mic	crosoft Cor	×		Avance
Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur. OK Annuler	Description :				
un ordinateur.	Le composant logiciel enfichable	o Cortificato vo	is permet de perso	vir le contenu des magasins de sortifi	
OK Annuler	un ordinateur.	e certificats vot	is permec de parco	uni le concenu des magasins de cercin	icats pour vous, un service ou
OK Annuler					
OK Annuler	L				
					OK Appuler

Sélectionnez « Un compte d'ordinateur »

Composant logiciel enfichable Certificats	x
Ce composant logiciel enfichable gérera toujours les certificats pour : Mon compte d'utilisateur Un compte de service Un compte d'ordinateur	
< Précédent Suivant > Annule	·

#### Sélectionnez « L'ordinateur local », puis cliquez sur « Terminer »

Sélectionner un ordinateur
Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable.         Ce composant logiciel enfichable gérera toujours : <ul> <li>L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)</li> <li>Un autre ordinateur :</li> <li>Parcourir</li> </ul> Autoriser la modification de l'ordinateur sélectionné lors de l'exécution à partir de la ligne de commande. Ceci ne s'applique que si vous enregistrez la console.
< Précédent Terminer Annuler

On va maintenant Développez l'arborescence de « Certificats »

Ajouter ou su	pp	rimer des co	mposants logiciels enfichable	s
Vous pouvez sélectionner des composants logi composants logiciels enfichables extensibles, v	ciels ous	enfichables parm pouvez spécifier	ni ceux disponibles sur votre ordinateur, e quelles extensions doivent être activées	et
Composants logiciels enfichables disponibles :			Composants logiciels enfit selectionnes :	_
Composant logiciel enfi Fournisseur	^		Racine de la console	L
Nicrosoft Cor			🙀 Certificats (ordinateur local)	Ē
🙀 Autorité de certifica Microsoft Cor				L
Certificats Microsoft Cor	≣			
E Configuration du clie Microsoft Cor				Г
Configuration et an Microsoft Cor				L
Contrôle ActiveX Microsoft Cor				Γ
Contrôle WMI Microsoft Cor		Ajouter >		
Dossier Microsoft Cor				
👸 Dossiers partagés 🛛 Microsoft Cor				
🗐 Éditeur d'objets de s Microsoft Cor				
Gestion de l'ordinateur Microsoft Cor				
🛃 Gestion de la straté Microsoft Cor				
Gestion des disques Microsoft et V				
Gestion du module d Microsoft Cor	$\sim$			

On va ensuite Développez l'arborescence de « certificats » :

🚟 Fichier Action Affichage Favoris	Fenêtre ?
📔 Racine de la console	Nom
⊿ 🙀 Certificats (ordinateur local)	🙀 Certificats (ordinateur local)
Personnel	
Autorités de certification racines (	
Confiance de l'entreprise	
Autorités de certification interméi	
Éditeurs approuvés	
Certificats non autorisés	
Autorités de certification racine ti	
Personnes autorisées	
Émetteurs d'authentification de c	
▷ 🚞 Bureau à distance	
👂 🧮 Demandes d'inscription de certifi	
🔈 📔 Racines de confiance de carte à p	
Périphériques approuvés	
🔈 🧰 Hébergement Web	

Développez l'arborescence de « Autorités de certification racines de confiance », puis « Certificats ».

🚡 Fichier Action Affichage Favoris Fenêtre	?						
🗢 🏟 🙍 📰 🤞 💺 🖾 🛤 🚺 🗊							
Racine de la console	Délivré à 🔺	Délivré par	Date d'expirati	Rôles prévus	Nom convivial	Statut	Modèle de certificat
⊿ 🙀 Certificats (ordinateur local)	🔄 Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	02/08/2028	Messagerie électro	VeriSign Class 3 Pu		
Personnel	🔄 Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Enregistrement des	Microsoft Timesta		
Autorités de certification racines de confiar	GSB-LABANNU1-CA	GSB-LABANNU1-CA	24/05/2022	<tout></tout>	<aucun></aucun>		
Certificats	GSB-W2012R2PKI-CA	GSB-W2012R2PKI-CA	29/05/2032	<tout></tout>	<aucun></aucun>		Autorité de certification racin
Confiance de l'entreprise	GSB-W2012R2PKI-CA	GSB-W2012R2PKI-CA	29/05/2032	<tout></tout>	<aucun></aucun>		Autorité de certification racin
Autorités de certification intermédiaires	Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	01/01/2000	Messagerie électro	Microsoft Authenti		
Editeurs approuvés	🔄 Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<tout></tout>	Microsoft Root Aut		
Certificats non autorisés	Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	10/05/2021	<tout></tout>	Microsoft Root Cert		
Autorites de certification racine tierce partir	Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	24/06/2035	<tout></tout>	Microsoft Root Cert		
Personnes autorisees	Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	23/03/2036	<tout></tout>	Microsoft Root Cert		
Emetteurs à autrentification de client	NO LIABILITY ACCEPTED, (c)97	NO LIABILITY ACCEPTED, (c)97 V	08/01/2004	Enregistrement des	VeriSign Time Stam		
Dureau a distance	Thawte Timestamping CA	Thawte Timestamping CA	01/01/2021	Enregistrement des	Thawte Timestamp		
Dérinhériques approuvés				-			
V Prenphenques approuves							
/ incongenient web							

On voit ici nos deux certificats racine de GSB-W2012R2-PKI-CA

Pour pouvoir revenir rapidement à cette console, vous pouvez créer un raccourcis sur le bureau en cliquant sur « Fichier », puis « Enregistrer sous ».

							Console1	- [Racine c
-	Fich	ier	Action	Affichage	Favoris	Fenêtre	?	
¢		No	uveau		Ctrl+N			
	Ouvrir Ctrl+O							
⊿		Enr	registrer					Ctrl+S
		Enregistrer sous						
		Ajo	uter/Supp	orimer un co	mposant l	ogiciel enf	ichable	Ctrl+M
		Options						
		1 C:\Windows\system32\certsrv						
		2 C:\Windows\system32\CompMgmt						
		3 C:\Windows\system32\gpmc						
	4 C:\Windows\system32\dnsmgmt							
	Quitter							

		Enregis	trer sous			x
Enregistrer dans :	📃 Bureau			v 🌀 🖄	• 🖽 💜	
Emplacements récents	admin	istrateur hèques		Ce PC	; u	
Bureau	Certifi	cats				
<b>Bibliothèques</b>						
Ce PC						
<b>Réseau</b>	Nom du fichier : Type :	Certificats Fichiers Microso	ft Management	: Console (*.m:	♥ sc] ♥	Enregistrer Annuler

Compte rendu d'installation d'un Windows 2012R2 PKI

29/05/2017 2 A BTS SIO

v 🕜

P

#### - 🗆 X Certificats 🌆 l 💽 👪 = l Accueil Partage Affichage 🍥 🛞 🔻 🕇 🐌 Certificats ✓ ♂ Rechercher dans : Certificats . Modifié le Taille Nom Туре 쑦 Favoris 📰 Bureau 🚟 Certificats 30/05/2017 12:21 Document de la c... 64 Ko 📃 Emplacements récer \rm Téléchargements 💻 Ce PC 📬 Réseau

### **Exporter le certificat racine :**

Comme expliqué dans l'introduction, un ordinateur souhaitant vérifier une clé publique ou certificat doit comparer la signature de l'autorité de certification présente dans la clé publique ou certificat, avec le certificat de l'autorité racine.

Notre certificat étant généré par une autorité de certification autonome, nous devons partager le certificat racine avec toutes les machies du domaine. Ainsi chaque ordinateur devra avoir le certificat racine dans le conteneur « Autorité de certification racines de confiance »

Pour pouvoir partager le certificat racine, il faut commencer par l'exporter

Pour cela on va ouvrir la console MMC pour accéder aux certificats comme indique dans le chapitre précédent :

藩 Fichier Action Affichage Favoris Fenêtre	?	4					
🗢 🄿 🙍 🐺 🐇 🐂 🙀 🖬 🚺							
<ul> <li>Racine de la console</li> <li>Qertificats (ordinateur local)</li> <li>Personnel</li> <li>Autorités de certification racines de confiar</li> <li>Certificats</li> <li>Confiance de l'entreprise</li> <li>Autorités de certification intermédiaires</li> <li>Éditeurs approuvés</li> <li>Certificats non autorisés</li> <li>Autorités de certification racine tierce partir</li> <li>Personnes autorisées</li> </ul>	Délivré à Class 3 Public Primary Certificat Copyright (c) 1997 Microsoft C GSB-LABANNU1-CA GSB-W2012R2PKI-CA GSB-W2012R2PKI-CA Microsoft Authenticode(tm) Ro Microsoft Root Certificate Auth Microsoft Root Certificate Auth Microsoft Root Certificate Auth	Délivré par Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. GSB-LABANNU1-CA GSB-V2012R2PKI-CA Microsoft Authenticode(tm) Root Microsoft Root Authority Microsoft Root Certificate Authori Microsoft Root Certificate Authori	Date d'expirati 02/08/2028 31/12/1999 24/05/2022 29/05/2032 29/05/2032 01/01/2000 31/12/2020 10/05/2021 24/06/2035 23/03/036	Rôles prévus Messagerie électro Enregistrement des <tout> <tout> <tout> Messagerie électro <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <tout> <t< td=""><td>Nom convivial VeriSign Class 3 Pu Microsoft Timesta <aucun> <aucun> <aucun> Microsoft Authenti Microsoft Root Cert Microsoft Root Cert Microsoft Root Cert</aucun></aucun></aucun></td><td>Statut</td><td>Modèle de certificat Autorité de certification racine Autorité de certification racine</td></t<></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout></tout>	Nom convivial VeriSign Class 3 Pu Microsoft Timesta <aucun> <aucun> <aucun> Microsoft Authenti Microsoft Root Cert Microsoft Root Cert Microsoft Root Cert</aucun></aucun></aucun>	Statut	Modèle de certificat Autorité de certification racine Autorité de certification racine
<ul> <li>Emetteurs d'authentification de client</li> <li>Eureau à distance</li> <li>Racines de confiance de carte à puce</li> <li>Périphériques approuvés</li> <li>Hébergement Web</li> </ul>	NO LIABILITY ACCEPTED, (c)97	NO LIABILITY ACCEPTED, (c)97 V Thawte Timestamping CA	08/01/2004 01/01/2021	Enregistrement des Enregistrement des	VeriSign Time Stam Thawte Timestamp		

#### Letort Léo

On va sélectionner le premier certificat racine. Puis faire un clic droit, « Toute les taches » et enfin cliquez sur « Exporter ».

~

L'assistant d'exportation se lance. Cliquez sur « suivant » :

Seistant Exportation du certificat
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.
Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.
Pour continuer, cliquez sur Suivant.
Suivant Annuler

Choisissez « X.509 binaire encodé DER ». Cliquez sur « suivant »

📀 🍠 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)
O Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)
Inclure tous les certificats dans le chemin d'accès de certification, si possible
Échange d'informations personnelles - PKCS #12 (.PFX)
Inclure tous les certificats dans le chemin d'accès de certification, si possible
Supprimer la clé privée si l'exportation réussit
Exporter toutes les propriétés étendues
Magasin de certificats sérialisés Microsoft (.SST)
Suivant Annuler

Letort Compte rendu d'installation d'un Windows 2012R2 PKI Léo

Il suffit ensuite de définir le chemin pour enregistrer le certificat. On va enregistrer temporairement le certificat sur le bureau du serveur dans le dossier certificats. Puis appuyez sur « Terminer ».

	X
📀 🍠 Assistant Exportation du certificat	
Fichier à exporter	
Spécifiez le nom du fichier à exporter	
	_
Nom du fichier :	
C:\Users\Administrateur.GSB\Desktop\Certificats\W2012R2PKI-CA Parcourir	
Suivant Annul	er

Assista	nt Exportation du cer	tificat 💌			
L'export	tation a réussi.				
		ОК			
l De te e				Certificats	
Partag	e Affichage				
🌗 🕨 Cer	tificats				
	Nom		Modifié le	Туре	Taille
	\overline Certificats		30/05/2017 12:21	Document de la c	64 Ko
ients récer ements	W2012R2PKI-CA		30/05/2017 13:16	Certificat de sécur	1 Ko

## **Interface Web Certsry :**

Nous allons maintenant configurer l'interface web de l'autorité de certification pour que celle-ci utilise un certificat délivré par l'autorité de certification. Les ordinateurs du domaine verront alors un site sécurisé.

On va tout d'abord commencer par la création d'un modèle de certificat.

#### Création d'un modèle de certificat :

Tout d'abord un modèle de certificat que l'on peut appeler aussi « Template » de certificat permet de définir des paramètres comme la durée de validité, le domaine, les droits, etc. Ces paramètres seront appliqués à chaque certificat généré à partir du modèle.

On va ouvrir le « Gestionnaire de serveur », puis dans le menu en haut à droite, cliquez sur « Outils » puis « Autorité de certification ».

		· 3		Gérer	Outils	Afficher	Aid
ļ		Analyse	eur de perf	formances			
	Assistant Configuration de la sécurité						
	Autorité de certification						
		Centre d'administration Active Directory					
		Configu	uration du	système			

#### On va ensuite allez dans « Modèles de certificats »



On va ensuite faire un clic droit sur le répertoire « Modèle de certificats », puis cliquer sur « Gérer », dans la nouvelle fenêtre qui s'ouvre à vous, trouvez le modèle « Serveur Web ». Faites un clic droit, puis cliquez sur « Dupliquer le modèle ».

Iodèles de certificats (LABANNU1.GS	Nom complet du modèle	Version de schéma	~
	Agent de récupération de clé	2	
	Agent de récupération EFS	1	
	Authentification de station de travail	2	
	🚇 Authentification du contrôleur de domai	2	
	Authentification Kerberos	2	
	Autorité de certification croisée	2	
	Autorité de certification racine	1	
	Autorité de certification secondaire	1	
	Chiffrement CEP	1	
	Connexion par carte à puce	1	
	Contrôleur de domaine	1	
	Échange d'autorité de certification	2	
	🚇 EFS basique	1	
	🚇 IPSec	1	
	IPSec (demande hors connexion)	1	
	🚇 Ordinateur	1	
	🚇 pfsense	2	≡
	🚇 Réplication de la messagerie de l'annuaire	2	
	Routeur (demande hors connexion)	1	
	Serveur RAS et IAS	2	
	🚇 Serveur Web	1	
	Session authentifiée	1	

Notre autorité de certification sera pour notre Windows serveur 2012 R2 PKI. Nous allons permettre de résoudre le fait qu'un client qui se connecte en bureau à distance n'est pas de message d'avertissement. Nous allons donc mettre le destinataire du certificat :

Les options de modèle disponibles reposent sur les versions de système d'exploitation les plus anciennes définies dans Paramètres de compatibilité.

Afficher les modifications résultantes

aramètres de compatibilité	
Autorité de certification	
Windows Server 2012 R2	~
Destinataire du certificat	
Windows 7 / Server 2008 R2	~

Il se peut que ces paramètres n'empêchent pas les systèmes d'exploitation plus anciens d'utiliser ce modèle. Puis dans l'onglet « Général », saisissez le nom du modèle. Puis définissez la « période de validité » ainsi que la « Période de renouvellement ». N'oubliez pas, la « Période de validité » doit être inférieure à la Période de validité du certificat de l'autorité de certification qu'on a défini juste avant (15 ans).

	Propriétés du nouveau modèle				
Attestation	de clé	Nom du s	ujet	9	Serveur
Conditions d'ém	nission N	Aodèles obsolètes	Exter	nsions	Sécurité
Compatibilité	Général	Traitement de	la deman	de	Chiffrement
Nom complet d	u modèle :				
Serveur Web	W2012R2PK	(I			
Nom du modèle ServeurWebW	9 : /2012R2PKI				
Période de valio	dité :	Période de	e renouvel	lement :	
8 année	s V	6	emaines	V	
✓ Publier le ce Ne pas u existe da	Publier le certificat dans Active Directory Ne pas utiliser la réinscription automatique si un certificat dupliqué				
		-			
	ОК	Annuler	Appliqu	ier	Aide

Letort Léo Dans l'onglet « Sécurité », pour le groupe d'utilisateur « utilisateurs authentifiés » cochez les deux options suivantes : « Inscrire » et « Inscription automatique ». Pour terminer, cliquez sur « Appliquer » puis « OK ».

	Propriété	s du nouveau	modèle	
Attestation	de clé	Nom du suje	et	Serveur
Compatibilité	Général	Traitement de la	a demande	Chiffrement
Conditions d'ém	ission M	odèles obsolètes	Extensions	s Sécurité
Noms de groupes ou d'utilisateurs :				
& Utilisateurs	authentifiés			
🔏 Administrate	eur			
🎎 Admins du	domaine (GSE	Admins du domair	ne)	
용 Administrate	eurs de l'entre	prise (GSB\Adminis	strateurs de l'e	entreprise)
			A:	Constants
			Ayouter	Supprimer
Autorisations pou	ur Utilisateurs			
authentifiés			Autoriser	Refuser
Contrôle total				
Lecture			~	
Lecture Écriture				
Lecture Écriture			▼ □ ▼	
Lecture Écriture Inscrire	omatique			
Lecture Écriture Inscrire Inscription aut	omatique		> 	
Lecture Écriture Inscrire Inscription aut	omatique		> > >	
Lecture Écriture Inscrire Inscription aut	omatique -			
Lecture Écriture Inscrire Inscription aut	omatique -			
Lecture Écriture Inscription aut	omatique	s et les paramètres		
Lecture Écriture Inscription aut Pour les autorisa avancés, cliquez	omatique tions spéciale sur Avancé.	s et les paramètres		Avancé
Lecture Écriture Inscription aut Pour les autorisa avancés, cliquez	omatique tions spéciale sur Avancé.	s et les paramètres		Avancé
Lecture Écriture Inscription aut Pour les autorisa avancés, cliquez	omatique tions spéciale 2 sur Avancé. le contrôle d'a	s et les paramètres iccès et les autorisa		Avancé
Lecture Écriture Inscription aut Pour les autorisa avancés, cliquez	omatique tions spéciale sur Avancé.	s et les paramètres Iccès et les autorisa	ations	Avancé

Pour que le nouveau modèle soit correctement pris en compte, il est conseillé de faire une mise à jour des GPO. Il faut donc ouvrir l'invite de commande (CMD), puis tapez la commande « gpupdate /force ».

Administrateur : C:\Windows\system32\	cmd.exe
Microsoft Windows [version 6.3.9600] (c) 2013 Microsoft Corporation. Tous droits réservés.	
C:\Users\Administrateur.GSB>gpupdate /force Mise à jour de la stratégie	
La mise à jour de la stratégie d'ordinateur s'est term La mise à jour de la stratégie utilisateur s'est termi	inée sans erreur. née sans erreur.
C:\Users\Administrateur.GSB>_	

Letort Léo On va ensuite retournez sur la fenêtre « CERTSRV », puis faites de nouveau un clic droit sur le répertoire « Modèles de certificats ». Cliquez sur « Nouveau » et enfin sur « Modèle de certificat à délivrer »

違 🔹 certsrv - [,	Autorité de cer	rtification (	Local)\GSB-W2012R2PK	I-CA\Modèl	es de certificats]	- <b>-</b> ×
Fichier Action	Affichage ?					
🗢 🄿 🖄 🙆	B ?					
Autorité de certif GSB-W2012R Certificats Certificats	fication (Local) A2PKI-CA is révoqués is délivrés es en attente	Nom Réplicatio Authentit Authentit Agent de	on de la messagerie de l'ann fication du contrôleur de do fication Kerberos récupération EFS	Rôle prévu Réplication de Authentificati Authentificati Récupération	e messages du service d'a. on du client, Authentifica. on du client, Authentifica. de fichiers	
Commande Com	es ayant échoué de certificats Gérer Nouveau	EFS basiq	ue r de domaine eb Modèle de certificat à de	Système de fi Authentificati <u>Authentificati</u> Élivrer	chiers EFS (Encrypting File. on du client, Authentifica. on du serveur n du client, Authentifica.	
	Affichage Actualiser Exporter la list Aide	•	e certification secondaire ateur	Système de fi <tous> Signature de l</tous>	chiers EFS (Encrypting File. iste d'approbation Micros.	

Modèles de Certificat additionnel activés dans cette autorité de certification

On va ensuite recherchez le modèle qu'on vient de créer (serveur web W2012R2PKI)

	Activer les modèle	s de certificat	x
Sél Rer éve Cer Po	ectionnez un modèle de certificat à activer sur cette autorit marque : si un modèle de certificat qui a été récemment cré entuellement attendre que les informations sur ce modèle air tains modèles de certificats dans l'organisation risquent de ur plus d'informations, voir <u>Concepts de modèles de</u>	é de certification. é n'apparaît pas dans cette liste, vous devrez ent été répliquées dans tous les contrôleurs de doma ne pas être accessibles à votre autorité de certificat <u>certificats.</u>	aine. ion.
N	om	Rôle prévu	~
J.	Serveur Web W2012R2PKI	Authentification du serveur	
5	Session authentifiée	Authentification du client	
5	Signature de liste d'approbation	Signature de liste d'approbation Microsoft	
1 1	Signature de l'utilisateur uniquement	Messagerie électronique sécurisée, Authentification	
1 1	Signature de réponse OCSP	Signature OCSP	
1	Signature du code	Signature du code	
1	Signature Exchange uniquement	Messagerie électronique sécurisée	=
1	Utilisateur de carte à puce	Messagerie électronique sécurisée, Authentification	
1	Utilisateur Exchange	Messagerie électronique sécurisée	_
1	Échange d'autorité de certification	Archivage de clé privée	~
<		>	
		OK Annuler	

#### On voit que le nouveau modèle de certificat à délivrer s'affiche maintenant dans la liste :

🗔 certsrv - [Autorité de ce	rtification (Local)\GSB-W2012R2PK	I-CA\Modèles de certificats]
Fichier Action Affichage ?		
🗢 🔿 🞽 🗶 🗐 🛃		
Autorité de certification (Local) GSB-W2012R2PKI-CA Certificats révoqués Certificats délivrés Demandes en attente Demandes ayant échoué Modèles de certificats	Nom Serveur Web W2012R2PKI Réplication de la messagerie de l'ann Authentification du contrôleur de do Authentification Kerberos Agent de récupération EFS EFS basique Contrôleur de domaine Serveur Web Ordinateur Utilisateur Autorité de certification secondaire Administrateur	Rôle prévu         Authentification du serveur         Réplication de messages du service d'a         Authentification du client, Authentifica         Authentification du client, Authentifica         Authentification du client, Authentifica         Récupération de fichiers         Système de fichiers EFS (Encrypting File         Authentification du client, Authentifica         Authentification du serveur         Authentification du client, Authentifica         Système de fichiers EFS (Encrypting File <tous>         Signature de liste d'approbation Micros</tous>

Letort Léo

# Création d'un certificat SSL :

Nous voulons maintenant générer un nouveau certificat SSL :

Ouvrez la console MMC avec le composant logiciel enfichable « Certificats ». Développez l'arborescence, faites un clic droit sur le répertoire « Personnel », puis cliquez sur « Toutes les tâches » et enfin « Demander un nouveau certificat ».

🚟 Fichier 🛛 Actio	n Affichage Favoris Fenêtre	?		
🗢 🄿 🔁 🗖	📋 🖸 🚔 🔽 📰			
Racine de la cons	Type d'o	bjet		
🗐 Certificats (or	📔 Certif	cats		
⊿ 🣔 Personnel			1	
🖆 C	Rechercher des certificats			
⊿ 📔 Autor	Toutes les tâches	•		Rechercher des certificats
► Confi	Affichage	•		Demander un nouveau certificat
Autor	Nouvelle fenêtre à partir d'ici			Importer
Édite	Neuvelle une de la liste des têches			
Certif	Nouvelle vue de la liste des taches		_	Operations avancees
Autor	Actualiser			
Perso	Exporter la liste			
⊳ 🧮 Émet	Aide			
👂 🧮 Burea	Alde	11		
Racines de	confiance de carte à puce			
Périphériq	ues approuvés			
b I Hébergem	ent Web			

Une fenêtre s'ouvre, il suffit simplement de faire suivant :

📮 Inscription de certificats
Avant de commencer Les étapes suivantes vous aideront à installer des certificats, qui sont des informations d'identification numériques utilisées pour se connecter à des réseaux sans fil, protéger du contenu, établir une identité et effectuer d'autres tâches relatives à la sécurité. Avant de demander un certificat, vérifiez que : votre ordinateur est connecté au réseau ; vous disposez d'informations d'identification qui peuvent servir à vérifier que vous avez le droit d'obtenir le certificat.
Suivant Annuler

Cliquez de nouveau sur suivant :

		_ <b>□</b> ×					
🔄 Inscription de certificats							
	Sélectionner la stratégie d'inscription de certificat La stratégie d'inscription de certificat permet l'inscription de certificats e certificats prédéfinis. Il est possible qu'elle soit déjà configurée.	n fonction de modèles de					
	Configurés par votre administrateur						
	Stratégie d'inscription à Active Directory	*					
	Configurés par vous	Ajouter une nouvelle URL					
		Suivant Annuler					

Sélectionnez le modèle précédemment créé, puis cliquez sur le lien en dessous « L'inscription pour obtenir ce certificat nécessite des informations supplémentaires ».

cription de certificats		
Demander des certificats		
ous pouvez demander les types de cer emander, puis cliquez sur Inscription.	tificats suivants. Sélectionnez les certificats q	jue vous voulez
Stratégie d'inscription à Active Dire	ectory	
Ordinateur	i Statut : Disponible	Détails
Serveur Web W2012R2PKI	③ Statut : Disponible	Détails
L'inscription pour obtenir ce ici pour configurer les paran	e certificat nécessite des informations supplé nètres.	mentaires. Cliquez
] Afficher tous les modèles		
	Inceri	ation Annul

Dans le premier onglet, définissez le nom du domaine pour le champ « Nom commun ».

Nom du sujet :		
Type :		
Nom commun 🗸 🗸	Ajouter >	
Valeur :	< Supprimer	
W2012R2PKI.GSB.local	( Supplified	
Autre nom :		Г

Cliquez ensuite sur « Ajouter »

A Objet Général Extensions	Clé privée	Autorité de cer	tification	Signature			
Le sujet d'un certificat est l'utilisateur ou l'ordinateur vers lequel le certificat est émis. Vous pouvez entrer des informations sur les types de noms de sujet et d'autres noms qui peuvent être utilisés dans un certificat.							
Sujet du certificat L'utilisateur ou l'ordinateur qui reçoit le certificat							
Type:			CN=W2	012R2PKI.G	SB.local		
Nom commun 🗸	Ajou	ıter >					
Valeur :	< Sup	primer					

Letort

Léo

Vous pouvez définir ensuite un « Nom convivial » Dans l'onglet Général. Cliquez pour terminer sur « Ok ».

Propriétés du certificat									
🛕 Objet	A Objet Général Extensions Clé privée Autorité de certification Signature								
Un nom o certificat.	Un nom convivial et une description facilitent l'identification et l'utilisation d'un certificat.								
Nom con	Nom convivial :								
CERT_W2	CERT_W2012R2PKI.GSB.local								
Description :									

Cliquez ensuite sur « Inscription ».

Letort

Léo

			_ <b>D</b> X
📮 Inscr	iption de certificats		
De Va de	emander des certificats ous pouvez demander les types de certificats s mander, puis cliquez sur Inscription.	suivants. Sélectionnez les certificats que vou	s voulez
	Stratégie d'inscription à Active Directory		
	Ordinateur	<b>i</b> Statut : Disponible	Détails 🗸
	Serveur Web W2012R2PKI	③ Statut : Disponible	Détails 🗸
	] Afficher tous les modèles		
		Inscription	Annuler

#### Cliquez sur « Terminer »

Inscription de certificats		
Résultats de l'installation des	s certificats	
Les certificats suivants ont été inscrit	s et installés sur cet ordinateur.	
Stratégie d'inscription à Active D	irectory	
Serveur Web W2012R2PKI	🖌 Statut : Opération réussie	Détails 🗸
		<u>T</u> erminer

# **Configuration serveur IIS :**

• ھي	Gestionnaire d	le serveur 🔸 Tableau de	bord
🔛 Tableau de	<b>V</b>		
Serveur loo	Fichier Affichage Aide	R2PKI   Sites   Default Web Site	
AD CS	Connexions	Page d'accueil ministra ns Gestion Explorer Modifier les autorisations Ajouter une application	de Default V Atteindre - 🕁
		Ajouter un répertoire virtuel Modifier les liaisons Gérer le site Web Actualiser Supprimer Renommer Basculer vers l'affichage du contenu	Compression

Letort Léo

	Modifier la liaiso	n de	site	? X
Type : https	Adresse IP : V Toutes non attribuées		Port :	]
Nom de l'hôte	:			
Exiger l'indic	cation de nom du serveur			
Certificat SSL :				
CERT_W2012R2	2PKI.GSB.local	¥	Sélectionner	Afficher
		Γ	ОК	Annuler

			Liaisons	de sites	? X
-					
Туре	Nom de l'hôte	Port	Adresse IP	Informations sur	 Ajouter
https		443	*		Modifier
					Supprimer
					Parcourir
					Fermer

## Navigation sur l'interface web :

#### L'interface web permet de :

- Demander un certificat : En copiant une requête de certificat à faire signer par l'autorité de certification
- Afficher le statut d'une requête de certificat : Ne concerne que l'autorité autonome (donc cela ne nous concerne pas)
- Télécharger un certificat d'autorité de certification ... : Vous permet de télécharger le certificat de votre autorité, la chaîne de certificat d'autorités (si vous avez créé une autorité secondaire au lieu d'une autorité racine) et les listes de révocation (celle de base + les listes delta).

Accès à l'interface et vérification HTTPS :

On va ouvrir notre navigateur web et tapez dans la barre d'adresse :

https://W2012R2PKI.GSB.local/certsrv/

Attps://w2012r2pki.gsb.local/certsrv/		₽-₽	ර් 🥖 Services de certificats Activ 🗙
de certificats <i>Microsoft</i> Active Directory	Identification du site Web	×	
ue !	GSR-W2012R2DKL-CA		
e site Web pour demander un certi	a identifié ce site comme suit :		rogramme client de messagerie
eb, signer et chiffrer des messages	w2012r2pki.gsb.local		lemandez, effectuer d'autres tâ
uvez également utiliser ce site Web	Cette connexion au serveur est chiffrée.		de certification une chaîne de i
· · · · · · · · · · · ·	Dois-je faire confiance à ce site ?		
enir plus d'informations sur les Sen	Affiches les estificate		Documentation sur les Services
nnez une tâche :	Amoner les certificats		

	Certificat
Général D	Vétails Chemin d'accès de certification
	Informations sur le certificat
Ce cer	rtificat est conçu pour les rôles suivants :
•	Garantit l'identité d'un ordinateur distant
D	vélivré à : W2012R2PKI.GSB.local
D	<b>élivré par</b> GSB-W2012R2PKI-CA
v	<b>/alide du</b> 01/06/2017 <b>au</b> 01/06/2019
P	Installer un certificat Déclaration de l'émetteur
L	ОК

A partir de ce point mon autorité de certificat permet à chaque machine sur le domaine, pour n'importe quel utilisateur d'aller sur mon interface web avec une connexion certifié.

Voici donc la premier expression de besoin qui est réalisé :

✓ Connexion certifié à l'interface web du serveur IIS

Nous allons donc nous attaquer maintenant à la connexion certifiée sur un client en connexion à distance (connexion TSE)

# Connexion certifié en TSE :

Letort

Léo

Faisons d'abord le test sans la configuration pour voir ce qu'on ne devrait pas obtenir !

Nous allons créer une VM W7 se nommant « W7TEST\_OUT\_TSE », puis nous allons nous connecter à un contrôleur du domaine (LABANNU1 // LABANNU2 ou sur mon serveur 2IS) avec un identifiant Admin du domaine car pour se connecter à un contrôleur de domaine il faut être admin du domaine.

🌄 Connexion Bureau à distance 📃 💷	Sécurité de Windows
Remote Desktop Connection	Entrer vos informations d'identification Ces informations d'identification seront utilisées pour vous connecter à LABANNU1.
Ordinateur : LABANNU1	GSB\AD_LETORT GSB\AD_LETORT
Nom Aucun paramètre n'a été spécifié. d'utilisateur : Vos informations d'identification seront demandées lors de la connevien	Utiliser un autre compte
	Mémoriser ces informations
Options     Connexion     Aide	OK Annuler

AD\_LETORT est un utilisateur promu au rang d'admin du domaine par mes soins afin de pouvoir tester mes différents tests à effectuer pour valider mes situations professionnels.

ID : AD\_LETORT // MDP : Password123



Une fois cette partie finit nous allons pouvoir nous connecter directement avec une connexion certifiée.

Nous allons aller sur l'AD puis dans « Autorité de certification ». Nous allons ensuite faire un clic droit sur modèles de certificats puis gérer :

On arrive dans la console des modèles de certificat, on va faire un clic droit sur le modele Ordinateur et faire « Dupliquer le modèle » :

Voici les modifications à faire :

Propriétés du nouveau modèle	Propriétés du nouveau modèle
Attestation de clé Nom du sujet Serveur	Attestation de clé Nom du sujet Serveur
Conditions d'émission Modèles obsolètes Extensions Sécurité	Conditions d'émission Modèles obsolètes Extensions Sécurité
Compatibilité Général Traitement de la demande Chiffrement	Compatibilité Général Traitement de la demande Chiffrement
Les options de modèle disponibles reposent sur les versions de système d'exploitation les plus anciennes définies dans Paramètres de compatibilité.	Nom complet du modèle : Cert_TSE_Auth
☑ Afficher les modifications résultantes	
Paramètres de compatibilité	Nom du modèle :
Autorité de certification	Cert_TSE_Auth
Windows Server 2012 R2 V	
	Période de validité : Période de renouvellement :
Destinataire du certificat	1 années V 6 semaines V
Windows 7 / Server 2008 R2 V	
	Publier le certificat dans Active Directory
Il se peut que ces paramètres n'empêchent pas les systèmes d'exploitation	Ne pas utiliser la réinscription automatique si un certificat dupliqué
plus anciens d'utiliser ce modèle.	existe dans Active Directory
OK Annuler <u>A</u> ppliquer Aide	OK Annuler Appliquer Aide
· · · · ·	
	Modifier l'extension des stratégies d'a
	Modifier restension des strategies d'a
	Une stratégie d'application détermine comment un
Descuiétés du nouveau modèle	certificat peut être utilisé.
Proprietes du nouveau modele	
Attestation de clé Nom du sujet Serveur	Stratégies d'application :
Compatibilité Général Traitement de la demande Chiffrement	Authoratifaction du diant
Conditions d'émission Modèles obsolètes Extensions Sécurité	Authentification du serveur
	Addientification du serveur
Four modifier une extension, selectionnez-la et cliquez sur Modifier.	
Extensions inclues dans ce modèle :	
Contraintes de base	
Informations du modèle de certificat	
Stratégies d'application	
	Ajouter Modifier Supprimer
	Ajouter
	Rendre cette extension critique
Modifier	
Description de Christophientien :	
Description de Strategies o application :	
Authentification du client	
	OK Appuler
	Ander
*	

Modifier l'extension des stratégies d'a	
the shatf is the balles of the start of the	Ajouter une stratégie d'application
Une stratégie d'application détermine comment un certificat peut être utilisé. Stratégies d'application :          Authentification du serveur         Authentification du serveur         Ajouter       Modifier         Supprimer         Rendre cette extension critique	Une stratégie d'application (nommée utilisation de la clé améliorée dans Windows 2000) définit la manière dont un certificat peut être utilisé. Sélectionnez la stratégie d'application nécessaire pour des signatures valides de certificats émis par ce modèle. Stratégies d'application : Extension de la couche HAL Fin du tunnel de sécurité IP Générateur de code dynamique Licences de jeux de clés Liste non autorisée Messagerie électronique sécurisée Microsoft Publisher Ouverture de session par catte à puce Pilote de logiciel anti-programme malveillant à lancement anticipé Récupération de fichiers Hemote Desktop Authentification Hepication de messages ou service d'annuaire Sécurité IP IKE intermédiaire
OK Annuler Modifier l'extension des stratégies d'a ×	OK Annuler
Une stratégie d'application détermine comment un certificat peut être utilisé.	
Stratégies d'application : Authentification du serveur Remote Desktop Authentification	
	Modifier la stratégie d'application
Ajouter Modifier Supprimer	Entrez un nouveau nom pour cette stratégie. Nom : Remote Desktop Authentification dentificateur d'objet : 1.3.6.1.4.1.311.54.1.2
OK Annuler	OK Annuler

Propriétés du nouveau modèle 🛛 🗙	Propriétés du nouveau modèle
Attestation de clé       Nom du sujet       Serveur         Compatibilité       Général       Traitement de la demande       Chiffrement         Conditions d'émission       Modèles obsolètes       Extensions       Sécurité         Noms de groupes ou d'utilisateurs :	Attestation de clé       Nom du sujet       Serveur         Compatibilité       Général       Traitement de la demande       Chiffrement         Conditions d'émission       Modèles obsolètes       Extensions       Sécurité         Noms de groupes ou d'utilisateurs :
Ajouter       Supprimer         Autorisations pour Ordinateurs du domaine       Autoriser       Refuser         Contrôle total	Ajouter       Supprimer         Autorisations pour AD_LETORT       Autoriser       Refuser         Contrôle total
Pour les autorisations spéciales et les paramètres Avancé avancés, cliquez sur Avancé.	Pour les autorisations spéciales et les paramètres Avancé Avancé

Une fois toutes ces modifications faites, nous allons pouvoir faire ok !

Nous allons ensuite aller dans les modèles de Certificats :

🖕 🛛 certsrv - [Autorité de certification (Local)\GSB-W2012R2PKI-CA\Modèles de certificats]						-	
Fichier Action	Affichage ?						
le 🔿 🖄 🙆	<b>B</b>						
🙀 Autorité de cert	🙀 Autorité de certification (Local)		Nom		Rôle prévu		
⊿ 🚽 GSB-W2012	R2PKI-CA	🚇 Cert_TSE_A	Auth		Authenti	ification du serveur, Remote De	
📔 Certifica	ts révoqués	🚇 Serveur We	eb W	/2012R2PKI	Authentification du serveur		
Certifica	ts délivrés	Réplication de la messagerie de l'ann		Réplication de messages du service d'a			
Demand	es en attente	<ul> <li>Authentification du contrôleur de do</li> <li>Authentification Kerberos</li> </ul>		Authentification du client, Authentifica Authentification du client, Authentifica			
Demand	es ayant échoué						
Modéles	de certificats	🖾 Agont do r	Accent do récupération EFS		Récupération de fichiers		
	Gérer		ie		Système	de fichiers EFS (Encrypting File	
	Nouveau	•		Modèle de certificat à de	élivrer	n du client, Authentifica	
	Affichage	•	eb		Authenti	itication du serveur	
	Actualiser Exporter la liste		r e certification secondaire		Authentification du client, Authentifica		
					Système de fichiers EFS (Encrypting File <tous></tous>		
	Aide	Aide		ateur		e de liste d'approbation Micros	

On va ensuite trouver notre modèle est cliquer dessus, et faire ok

Nous allons ensuite créer la GPO qui correspond à notre modèle :

,	• 🕄   🚩 Gére		Outils	Afficher	Aide	
	Analyseur de performances					
	Assistant Configuration de	la sécu	urité			
	Autorité de certification					
	Autorité HRA (Health Regis	tratior	h Author	ity)		
	Centre d'administration Act	tive Di	rectory			
	Configuration du système					
	Défragmenter et optimiser	les lec	teurs			
	DHCP					
	Diagnostic de mémoire Wir	ndows				
	DNS					
	Domaines et approbations Active Directory					
	Gestion de l'accès à distance					
	Gestion de l'ordinateur					
	Gestion des stratégies de g	roupe				
	Gestionnaire des services Ir	ternet	t (IIS)			

On va ensuite créer une UO correspondant à notre certification, on va l'appeler « TSE\_Secure » :



On va pouvoir ensuite créer une GPO pour cela on va directement faire un clic droit sur TSE\_Secure et faire



Letort
Léo

Nouvel o	bjet GPO	x
Nom : GPO_certificat_Tse_LLETORT		
Objet Starter GPO source : (aucun)		~
	OK	Annuler

Une fois créée elle apparait dans les Objets de stratégie de groupe liés, nous allons simplement faire un clic droit dessus et faire gérer :

Puis « Configuration d'ordinateur », puis « modèles d'administration … », puis « Composants Windows », puis « Service Bureau à distance », puis « Hôte de la session Bureau à distance », puis « Sécurité », et enfin « Modèle de certificat d'authentification serveur ».

On arrive donc sur cette page, il suffira ensuite d'activé le modèle et de choisir le modèle que nous avons créé précédemment !!

	Mod	Modèle de certificat d'authentification serveur				x		
Modèle de certif	on serveur		Paramètre précédent	Paramètre	suivant			
O Non configuré	Commentaire :	e:						^
<ul> <li>Désactivé</li> </ul>	Pris en charge sur	: Au minimur	m Windows V	sta				× × ×
Options :			Aide :					
Nom du modèle de certificat Cert_TSE_Auth			Ce paramèt modèle de c automatiqu Bureau à dis Un certifical session Bur sécuriser les de session E (Remote De Si ce param nom de mo modèle de c sélection au Hôte de ses automatiqu spécifié.	re de stratégie vous pe certificat qui détermine ement pour authentifi itance. cest nécessaire pour au eau à distance lorsque communications entr ureau à distance pend sktop Protocol). ètre de stratégie est ac dèle de certificat. Seul certificat spécifié sont tomatique d'un certifi sion Bureau à distance ement uniquement si aucun certificat créé à erveur Hôte de session	rmet de spécifier e quel certificat es er un serveur Hôt uthentifier un sen SSL (TLS 1.0) est o se un client et un lant des connexio tivé, vous devez s s les certificats cro pris en compte lo cat pour authenti . Un certificat est aucun certificat est aucun certificat modèle n Bureau à distance	le nom st sélecti e de ses veur Hôi utilisé pi serveur ons RDP spécifier éés à l'ai ors de la ifier le se sélectio l'a été de certi ce émet	du ionné ision te de our Hôte un ide du erveur nné	
				ОК	Annuler	A	oplique	er

Ensuite sur la même page, on va allez sur « Nécessite l'utilisation d'une couche de sécurité .... » :

📮 Sécurité			
Nécessite l'utilisation d'une couche	Paramètre	État	Commentaire
de sécurité spécifique pour les	Modèle de certificat d'authentification serveur	Activé	Non
connexions distantes (RDP)	Définir le niveau de chiffrement de la connexion client	Non configuré	Non
Mardiffica la compañía de start (sin	🗈 Toujours demander le mot de passe à la connexion	Non configuré	Non
Nodifier <u>le parametre de strategie</u>	Requérir des communications RPC sécurisées	Non configuré	Non
Configuration requise :	Nécessite l'utilisation d'une couche de sécurité spécifique p	Activé	Non
Au minimum Windows Vista	🗈 Ne pas autoriser les administrateurs locaux à personnaliser I	Non configuré	Non
Description :	🗄 Requérir l'authentification utilisateur pour les connexions à	Non configuré	Non

Nous allons donc l'activé et mettre en couche de sécurité SSL (TLS 1.0), puis faire ok.

Se Nécessite l'utilisation d'une couche de sécurité spécifique pour les connexions dista				
📷 Nécessite l'utilis	ation d'une couche de	sécurité spécifique pour les connexions distantes (RDP)		
Paramètre précéde	ent Paramètre suiv	vant		
O Non configuré	Commentaire :			
<ul> <li>Activé</li> </ul>				
<ul> <li>Désactivé</li> </ul>	Pris en charge sur :	A contraction of the second se		
	·	Au minimum Windows Vista		
Options :		Aide :		
Couche de sécurité Choisissez le niveau déroulante.	SSL (TLS 1.0) de sécurité dans la liste	Ce paramètre de stratégie spécifie s'il faut requérir l'ur d'une couche de sécurité spécifique pour sécuriser le: communications entre les clients et les serveurs Hôte Bureau à distance lors des connexions RDP (Remote E Protocol). Si vous activez ce paramètre de stratégie, toutes les communications entre les clients et les serveurs Hôte Bureau à distance doivent utiliser la méthode de sécu spécifiée dans ce paramètre lors des connexions à disi méthodes de sécurité suivantes sont disponibles :		
		* Négocier : la méthode Négocier applique la méthod sécurisée qui est prise en charge par le client. Si TLS (1 Layer Security) version 1.0 est pris en charge, elle est u authentifier le serveur Hôte de session Bureau à distar n'est pas pris en charge, le chiffrement RDP (Remote l Protocol) natif est utilisé pour sécuriser les communic mais le serveur Hôte de session Bureau à distance n'e		
		OK Annuler		

Tout est maintenant configuré pour la GPO.

Nous allons pouvoir maintenant faire les tests et regarder si les certificats sont délivrés, nous allons prendre notre VM de test quiise nomme « W7Test\_Situation » et qui se situe dans l'UO sur l'AD ou nous avons appliqué la GPO :

Nonnexior	n Bureau à distance			
- Color	Remote Desktop Connection			
Ordinateur : Nom d'utilisateur : Vos informatio	W2012R2pki GSB\AD_LETORT ns d'identification seront demande	✓		
connexion.		Connexion	Aide	AD_LETORT // Password12.

Et nous nous connectons bien sur notre serveur d'autorité dfe certificaiton :



Les deux expressions de besoins sont maintenant remplies !

- ✓ Connexion certifié à l'interface web du serveur IIS
- ✓ Connexion certifié a distance a partir d'un client client sur un controlaire de domaine ou un Serveur d'autorité de certification