

Installation d'Active Directory Certificate Services



<u>Sommaire :</u>

- I. Présentation du projet
- II. Mise en place d'Active Directory Certificate Services
- III. Accès au site et aperçu
- IV. Compétences mises en œuvre



I. <u>Présentation du projet :</u>

Dans le cadre de ce projet, l'objectif principal est de mettre en place **Active Directory Certificate Services (ADCS)** sur un serveur Windows. ADCS permet de créer et de gérer des certificats numériques dans un environnement Active Directory, garantissant ainsi la sécurité des communications et l'authentification des utilisateurs et des services.

L'utilisation des certificats numériques est essentielle pour assurer la confidentialité et l'intégrité des données échangées sur un réseau. Grâce à l'ADCS, il est possible de gérer les demandes de certificats, de les émettre, de les révoquer, et d'assurer une gestion centralisée des certificats pour les utilisateurs et les ordinateurs de l'organisation.

Ce projet vise à :

- Installer et configurer le rôle ADCS sur un serveur Windows.
- Créer une autorité de certification (CA) interne pour gérer la délivrance des certificats.
- Mettre en place des certificats pour des services spécifiques comme l'authentification des utilisateurs, le chiffrement des communications, et la signature des données.

Le projet s'inscrit dans un contexte de renforcement de la sécurité du réseau, avec une gestion centralisée des certificats permettant de garantir une meilleure gestion de la sécurité des communications entre les différents composants de l'infrastructure réseau.

II. <u>Mise en place d'Active Directory Certificate</u> <u>Services :</u>

Sur un Windows Serveur 2022 du domaine, ici basé sur mon serveur AD, il suffit de cliquer dans le gestionnaire de serveurs sur Ajouter des rôles et des fonctionnalités :



4

📥 Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION SRV-AD1.archambault.ca

×



Sur la partie service de rôle cocher l'option Autorité de certification :

Progression de l'insta	allation	SERVEUR DE	DESTINATIO	274	N
Avant de commencer	fficher la progression de l'installation				
Type d'installation	 Installation de fonctionnalité 				
	Configuration requise. Installation réussie				
Fonctionrialités AD CS Services de rôle Confirmation Résultats	Services de certificats Active Directory Des étapes supplémentaires sont nécessaires pour la config Active Directory sur le serveur de destination. Configurer les services de certificats Active Directory sur le Autorité de certification Outils d'administration de serveur distant Outils d'administration de rôles Outils des services de certificats Active Directory Outils de gestion de l'autorité de certification	uration des services de cert serveur de destination	ificats		
1	Vous pouvez fermer cet Assistant sans interrompre les ta leur progression ou rouvrez cette page en cliquant sur N commandes, puis sur Détails de la tâche.	iches en cours d'exécution. Jotifications dans la barre d	Examinez e		
Đ	xporter les paramètres de configuration.				
	< Précédent Suivant	> Fermer	Annule		

Une fois l'installation terminée, continuer et créer l'autorité de certification et saisir le compte d'identification :

Informations d'identifica	5. Spécifier les informations d'identification pour configurer les
Services de rôle	services de rôle
	Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local :
	 Utiliser l'autorité de certification autonome Inscription de l'autorité de certification via le Web Répondeur en ligne
	Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs 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
	Informations d'identification : Modifier

Continuer les différentes étapes en venant déclarer les paramètres spécifiques à cette autorité de certification.

6

- Autorité racine
- Génération de clé privé
- Options de chiffrement

Une fois l'autorité de certification créée, il est possible de retrouver le certificat dans la console Autorité de certification.

Tableau de bord	BIENVENUE DANS GESTION	NAIRE DE SERVEUR		- (窓) 🏴 Gérer Outils Afficher Aide
Lorever local Tous les serveurs AD CS AD DS Centry- IA DNS Chiefe Actic DNS Control Contro Control Control Control Control Control C	utorité de certification (Local)] n Affichage ? ?	Configurer ce serveur local Propriétés de : archambault-SRV-AD1-CA ? ×		
Services de fichiers	eetification (Local) Sault-SRV-ADT-CA	Extensions Stockage Gestionnaires de conflicats Agents d'incorption Avuit Agents de ricopération Securité Général Module de atratégie Module de aotre Autoré de centification Nom : archambaut-SRV-AD1-CA Centificats d'autoré de centification : Centificats d'autoré de centification : Centificats d'autoré de centification : Centificats n° 0 Paramètres de chiffement Examples de chiffement Examples de chiffement	Certificat Genéral Détais Chemn d'accès de certificato Informations sur le certificat Ce certificat est conçu pour les rôles suivants : Outes les stratégies d'application Délivré à : archambault-SRV-4D1-CA Délivré par archambault-SRV-4D1-CA	Masquer Services de fichiers et de stockage 1 Facilité de gestion Événements Senvices
	Serveur local Facilité de gestion Cuestion Cuestion	SHA256 SHA256 Algorithme de hachage : OK Annuler Acceleuer Adde 1 OK Annuler Acceleuer Adde 2 Événements	Valide du 25/11/2024 au 25/11/2029 Dédaration de l'émétreur CK	Performances Résultats BPA

Ce certificat sera à distribuer sur toutes les machines qui auront accès sur des sites certifiés par cette autorité de certification.



III. Accès au site et aperçu:

Il est possible d'accéder au site de l'autorité de certification en saisissant : IPDUSERVEUR/certsrv

Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats



IV. <u>Compétences mises en œuvre :</u>

Compétence du référentiel	Mise en œuvre dans le projet
Gérer le patrimoine informatique	Installation d'un service de gestion et de sécurisation basé sur une autorité de certification.
Mettre à disposition des utilisateurs un service informatique	Mise en place d'un service permettant d'avoir une authentification forte sur les services interne. Chiffrement des communications des services.

