

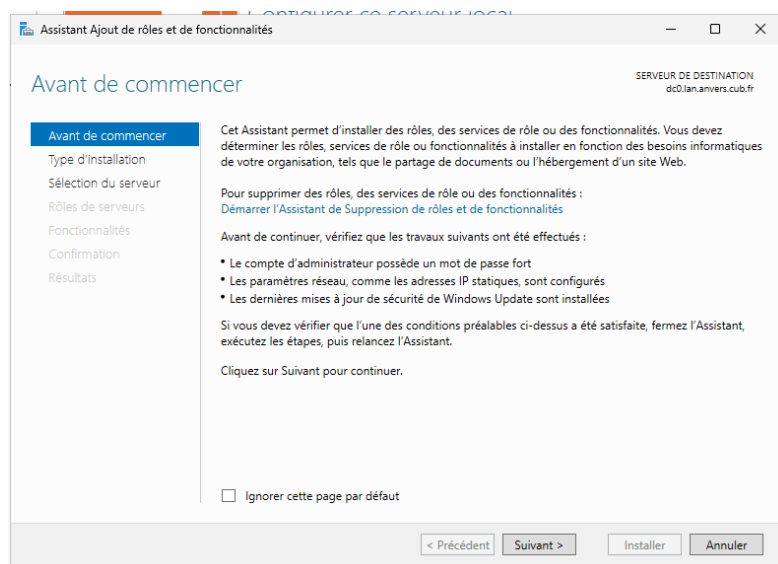
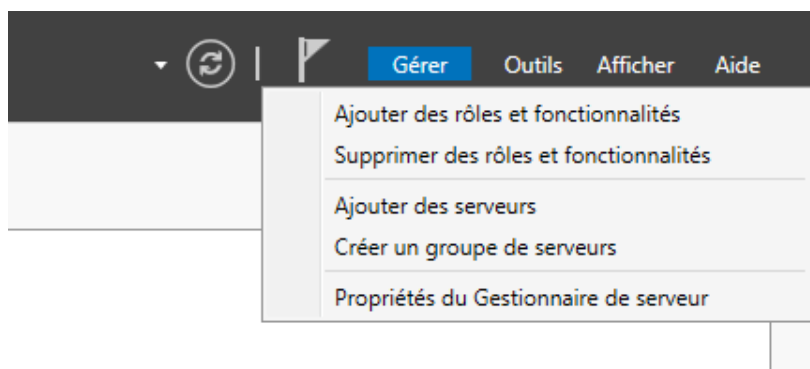
FICHE 2 – MISE EN PLACE D'UNE PKI POUR L'AUTHENTIFICATION SMARTCARD / PIV

INSTALLATION DU RÔLE "AUTORITÉ DE CERTIFICATION INTERNE (PKI)" SUR LE SERVEUR CONTRÔLEUR DE DOMAINE



Attention ! Les référentiels de bonnes pratiques recommandent de ne pas installer le rôle "Service de certificats Active Directory (AD CS)" sur un contrôleur de domaine en production. Cela a pour conséquence d'augmenter de façon importante la surface d'attaque et peut générer des problèmes supplémentaires.

Pour mettre en place cette nouvelle autorité de certification interne, il est nécessaire d'ajouter le rôle sur le contrôleur de domaine existant. Dans le Gestionnaire de serveur, cliquer sur Ajouter des rôles et fonctionnalités.



Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER le serveur de destination

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

SÉLECTIONNER le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs

☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
dc01.anivers.cub.fr	192.168.1.10	Microsoft Windows Server 2025 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER le type d'installation

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

SÉLECTIONNER 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.

☒ **Installation basée sur un rôle ou une fonctionnalité**

Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

☐ **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.

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER des rôles de serveurs

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD CS

Services de rôle

Confirmation

Résultats

SÉLECTIONNER un ou plusieurs rôles à installer sur le serveur sélectionné.

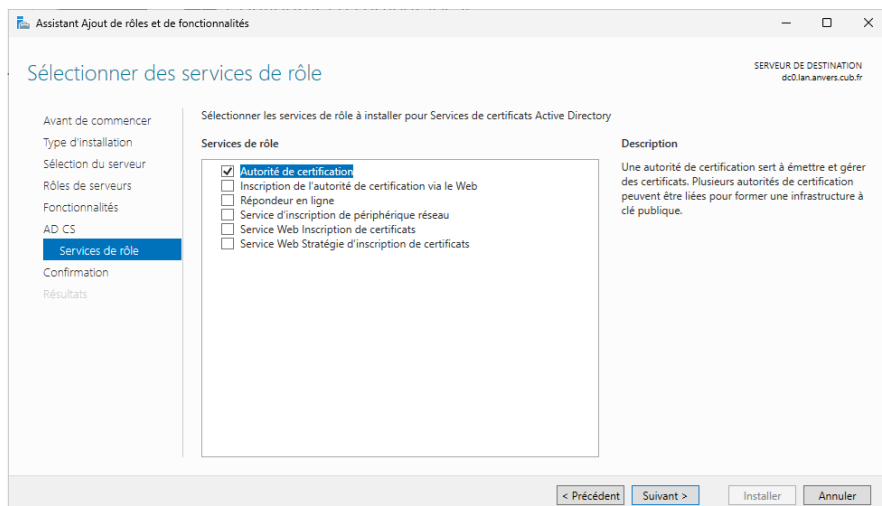
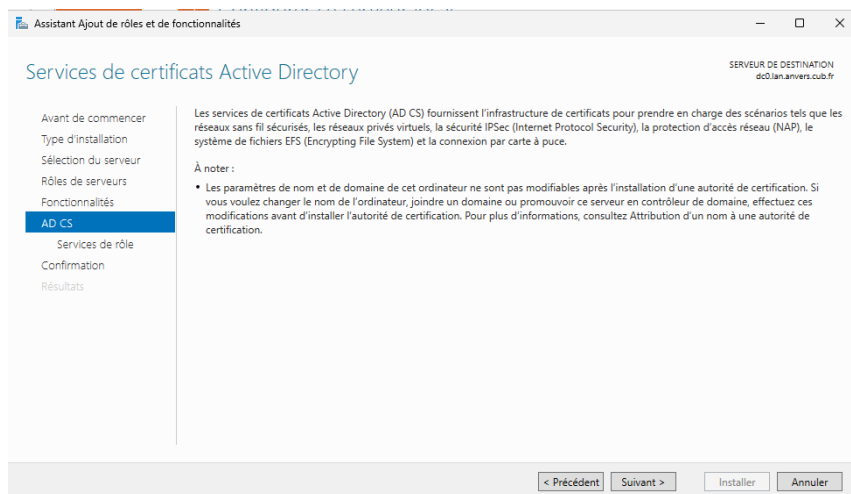
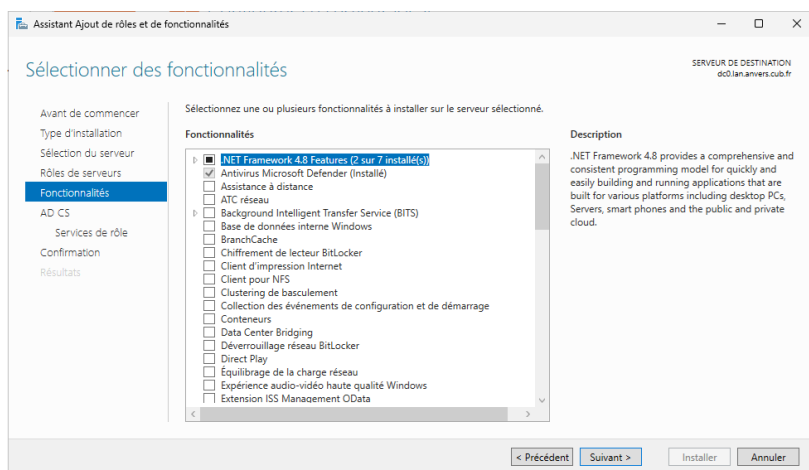
Rôles

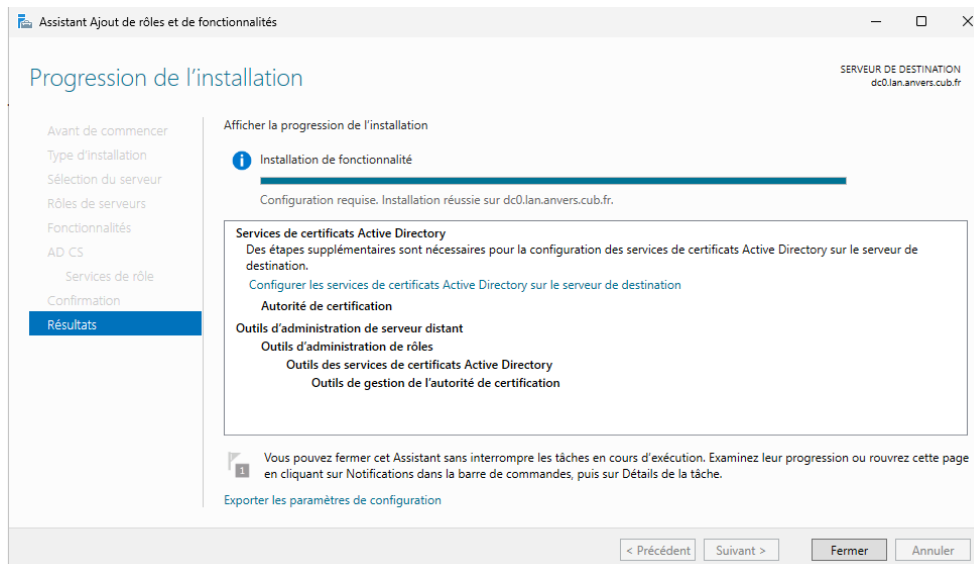
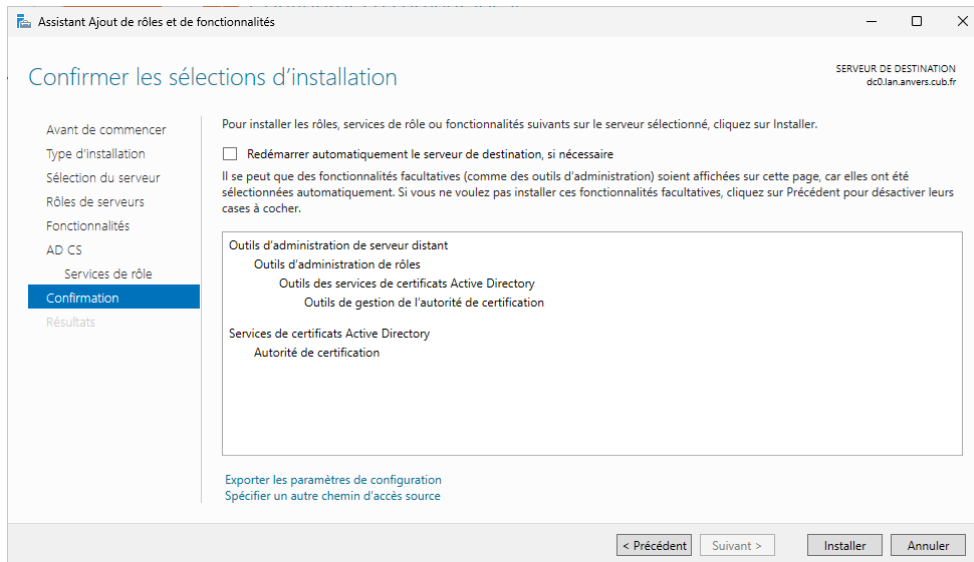
☐ Accès à distance
☐ Attestation d'intégrité de l'appareil
☐ Hyper-V
☐ Serveur de télécopie
☐ Serveur DHCP
☒ Serveur DNS (Installé)
☐ Serveur Web (IIS)
☐ Service Guardian hôte
☐ Services AD LDS (Active Directory Lightweight Directory Services)
☐ Services AD RMS (Active Directory Rights Management Services)
☐ Services Bureau à distance
☐ Services d'activation en volume
☐ Services d'impression et de numérisation de document
☒ **Services de certificats Active Directory**
☐ Services de déploiement Windows
☒ Services de domaine Active Directory (Installé)
☐ Services de fédération Active Directory (AD FS)
☒ Services de fichiers et de stockage (2 sur 12 installé(s))
☐ Services de stratégie et d'accès réseau
☐ Services WSUS (Windows Server Update Services)

Description

Les services de certificats Active Directory (AD CS) servent à créer des autorités de certification et les services de rôle associés pour émettre et gérer les certificats utilisés dans diverses applications.

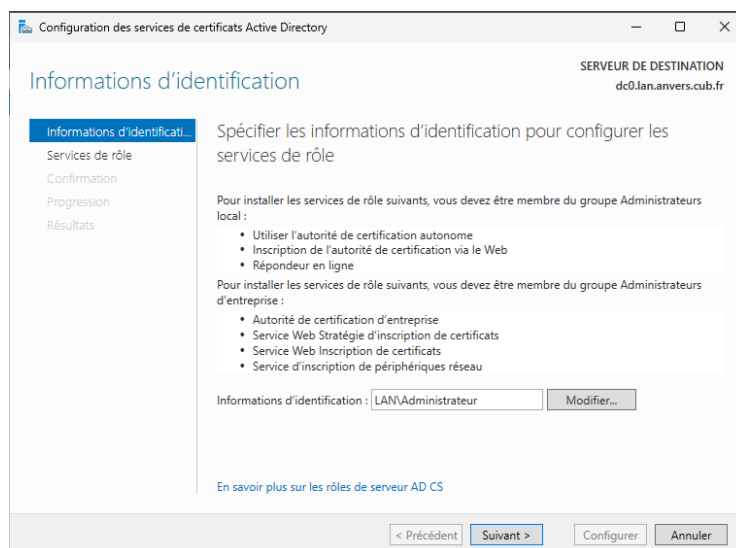
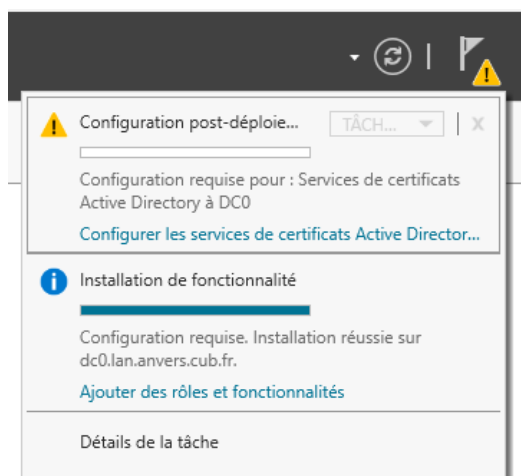
< Précédent Suivant > Installer Annuler





CONFIGURATION DE L'AUTORITÉ DE CERTIFICATION AD CS

Dans le Gestionnaire de serveur, cliquer sur le drapeau avec le point d'exclamation puis sur Configurer les services de certificats Active Directory.



Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
dc0.lan.anvers.cub.fr

Services de rôle

Informations d'identifiati...
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

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
dc0.lan.anvers.cub.fr

Type d'installation

Informations d'identifiati...
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

Spécifier le type d'installation de l'AC

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.

- ☒ 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.
- ☐ 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).

[En savoir plus sur le type d'installation](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

Clé privée

SERVEUR DE DESTINATION
dc01an.anvers.cub.fr

Informations d'identifi...
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

Spécifier le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

☒ Créer une clé privée
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.

☐ Utiliser la clé privée existante
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de 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 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



Attention ! Si vous décidez de modifier les paramètres de fournisseur de chiffrement, de longueur de clé ou d'algorithme de hachage, assurez-vous que les valeurs choisies sont supportées par la Yubikey et qu'il reste suffisamment d'espace sur cette dernière pour stocker des certificats X509 avec des longueurs de clé importantes.

	Taille maximum de certificat X509	Longueur de clé supporté	Algorithme de hachage supporté	Chiffrement
Yubikey 4/5	3052 octets	RSA – 1024, 2048 ECDSA – P256, P384	SHA-256, SHA-384	RSA, ECDH



Information : RSA 3072 et 4096 ne sont supportés que sur des Yubikey 5 disposant d'un firmware 5.7 et supérieur.

Configuration des services de certificats Active Directory

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION
dc0.lan.anvers.cub.fr

Informations d'identifi...
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

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement : RSA#Microsoft Software Key Storage Provider Longueur de la clé : 2048

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :
SHA256
SHA384
SHA512
SHA1

☐ Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

[En savoir plus sur le chiffrement](#)

< Précédent Suivant > Configurer Annuler

L'étape suivante est importante. Il faut fournir le nom commun de l'autorité de certification. Si l'on souhaite appliquer une convention de nommage cohérente, il est possible de choisir "pki", "ac", "ca", ou tout autre nom jugé pertinent.

Configuration des services de certificats Active Directory

Nom de l'autorité de certification

SERVEUR DE DESTINATION
dc0.lan.anvers.cub.fr

Informations d'identifi...
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

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC : pki

Suffixe du nom unique : DC=lan,DC=anvers,DC=cub,DC=fr

Aperçu du nom unique : CN=pki,DC=lan,DC=anvers,DC=cub,DC=fr

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler



Attention ! La période de validité fixée ici devra être nécessairement supérieure à celle choisie lors de la création du modèle de certificat spécifique pour les cartes à puce (SmartCard).

Configuration des services de certificats Active Directory

PERIODE DE VALIDITE

SERVEUR DE DESTINATION
dc0.lan.anvers.cub.fr

Informations d'identifi...
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

Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

5 Années

Date d'expiration de l'AC : 14/10/2030 14:05:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

En savoir plus sur la période de validité

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

BASE DE DONNEES DE L'AUTORITE DE CERTIFICATION

SERVEUR DE DESTINATION
dc0.lan.anvers.cub.fr

Informations d'identifi...
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

Spécifier les emplacements des bases de données

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

En savoir plus sur la base de données de l'autorité de certification

< Précédent Suivant > Configurer Annuler

Une fois, les différentes étapes validées, cliquer sur Configurer.

Configuration des services de certificats Active Directory

CONFIRMATION

SERVEUR DE DESTINATION
dc0.lan.anvers.cub.fr

Informations d'identifi...
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

Pour configurer les rôles, services de rôle ou fonctionnalités ci-après, cliquez sur Configurer.

Services de certificats Active Directory

Autorité de certification

Type d'AC : Racine d'entreprise

Fournisseur de services de chiffrement : RSA#Microsoft Software Key Storage Provider

Algorithme de hachage : SHA256

Longueur de la clé : 2048

Autoriser l'interaction de l'administrateur : Désactivé

Période de validité du certificat : 14/10/2030 14:05:00

Nom unique : CN=pci,DC=lan,DC=anvers,DC=cub,DC=fr

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

< Précédent Suivant > Configurer Annuler