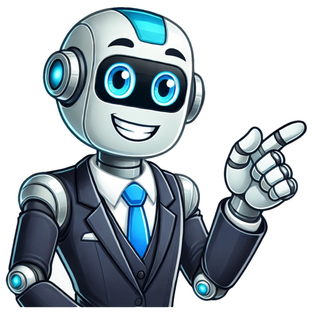
Click Here



Maintenant que votre autorité de certification racine autonome est configurée correctement, vous pouvez publier ses informations dans l'Active Directory. Pour récupérer son certificat et sa liste de révocation, allez dans le dossier "C:\Windows\System32\CertSvc\CertEnroll" de cette autorité de certification racine autonome. Créez un dossier "Root CA data" à la racine de la partition "C" de votre contrôleur de domaine. Note : j'utilise les partages administratifs par facilité pour ce tutoriel. Néanmoins, en entreprise, vous utiliserez plutôt une clé USB pour transférer ces données étant donné que l'autorité de certification autonome est censée rester hors connexion pour des raisons de sécurité. Copiez les fichiers du dossier "C:\Windows\System32\CertSvc\CertEnroll" de votre autorité de certification racine autonome et collez ceux-ci dans le dossier "Root CA data" que vous venez de créer sur votre contrôleur de domaine. Sur votre contrôleur de domaine, vous trouverez donc ce même dossier à la racine de sa partition "C". Ouvrez un invite de commandes et publiez le certificat de votre autorité de certification autonome dans votre infrastructure Active Directory en exécutant cette commande : Batch certutil -dspublish -f "C:\Root CA data\root-ca_InformatiWeb Root CA.crt" rootca Note : le mot-clé "rootca" indique qu'il s'agit d'un certificat d'une autorité de certification racine. Si vous réouvrez la console "Sites et services Active Directory" sur votre contrôleur de domaine, vous verrez que votre autorité de certification racine autonome apparait dans le dossier : Services -> Public Key Services -> Certification Authorities. Votre autorité de certification racine autonome apparait également dans le dossier : Services -> Public Key Services -> Certification Authorities. Maintenant, publiez la liste de révocation de certificats complète de votre autorité de certification racine autonome dans votre infrastructure Active Directory en utilisant la commande : Batch certutil -dspublish "C:\Root CA data\InformatiWeb Root CA.crl" Dans la console "Sites et services Active Directory", vous verrez la liste de révocation de certificats apparaitre dans le dossier : Services -> Public Key Services -> CDP -> [nom NETBIOS du serveur où la CA racine est installée]. Comme vous pouvez le voir, il s'agit d'un objet de type : cRLDistributionPoint. Comme précédemment, vous pouvez également voir ces informations via la console "Modification ADSI" en choisissant le contexte d'attribution "Configuration". En effet, pour rappel, ces données sont stockées dans la partition "Configuration" de votre infrastructure Active Directory. Vous retrouverez donc votre autorité de certification racine autonome dans le dossier : CN=Configuration,DC=informatiweb,DC=lan\CN=Services\CD=Public Key Services\CN=Certification Authorities. Vous retrouverez également votre autorité de certification racine autonome dans le dossier "CN=AIA". Pour finir, dans le dossier "...\CN=Public Key Services\CN=CDP\CN=[nom NETBIOS du serveur où la CA racine est installée]", vous retrouverez sa liste de révocation de certificats que vous venez de publier. 8. Configuration initiale de l'autorité de certification secondaire Maintenant que l'autorité de certification racine autonome est entièrement configurée et qu'elle peut être connue (détectée) par tous les serveurs et ordinateurs membres de votre domaine Active Directory, vous pouvez configurer votre autorité de certification secondaire. Pour cela, dans l'assistant "Ajout de rôles et de fonctionnalités" que vous aviez laissé ouvert sur votre serveur "sub-ca", cliquez sur le lien : Configurer les services de certificats Active Directory sur le serveur de destination. L'assistant "Configuration des services de certificats Active Directory" apparait. Comme prévu, la configuration sera effectuée par défaut avec le compte administrateur du domaine Active Directory auquel ce serveur est lié. Contrairement à votre autorité de certification autonome que vous aviez configurée avec le compte administrateur local. Cochez la case "Autorité de certification" et cliquez sur Suivant. Sélectionnez : Autorité de certification d'entreprise. Note : l'installation d'une autorité de certification d'entreprise est possible, car votre serveur "sub-ca" est lié à un domaine Active Directory. Ce qui est requis étant donné qu'une autorité de certification d'entreprise stocke automatiquement différents types d'informations dans l'Active Directory (y compris son certificat, ses listes de révocations et ses modèles de certificats). Ensuite, sélectionnez : Autorité de certification secondaire. Chaque autorité de certification (racine ou secondaire) possède sa propre paire de clés (clé publique / clé privée). Donc, sélectionnez : Créer une clé privée. Laissez les options de chiffrement par défaut. Note : le SHA1 est dépassé. Ne l'utilisez surtout pas. Indiquez un nom pour votre autorité de certification secondaire. Dans notre cas, nous la nommerons : InformatiWeb Sub CA. Note : les 2 autres cases seront automatiquement modifiées par l'assistant. Lorsque vous créez une autorité de certification secondaire, son certificat doit être émis et signé par une autorité de certification parente (votre autorité de certification racine autonome dans ce cas-ci) pour qu'il soit valide. Pour cela, l'assistant va créer automatiquement une demande de certificat et la stocker à la racine de votre serveur "sub-ca". Cliquez sur Suivant. Laissez les emplacements de stockage par défaut pour la base de données de votre autorité de certification secondaire. Un résumé de la configuration de votre autorité de certification secondaire d'entreprise apparait. Cliquez sur Configurer. Une fois la configuration des services de certificats Active Directory terminée, un avertissement apparait : Configuration réussie avec des avertissements. En résumé, cela signifie que votre autorité de certification secondaire n'est pas encore complètement installée. En effet, vous devez encore envoyer la demande de certificat créée par cet assistant à votre autorité de certification racine autonome, puis importer le certificat que celle-ci vous aura délivré pour que votre autorité de certification secondaire soit fonctionnelle. Cliquez sur Fermer. Cliquez sur : Fermer. Donnez-nous votre avis Ce chapitre évoque l'installation de l'autorité racine, en tant que CA autonome, afin de monter le premier niveau de l'architecture décrite en introduction, à savoir une PKI à deux niveaux. Concrètement, ce serveur nommé S-ROOTCA restera en Workgroup (donc il n'est pas intégré au domaine Active Directory). De plus, il sera, par ailleurs, éteint à la fin de l'implémentation des autres autorités de certification. Les chapitres suivants décrivent l'installation et la configuration de l'autorité. Remarque : la procédure décrite dans cet article est valide avec Windows Server 2022 et Windows Server 2025. La première étape consiste à ajouter le rôle d'autorité de certification sur la machine depuis le Gestionnaire de serveur. Cliquez sur "Ajouter des rôles et des fonctionnalités". Appuyez sur "Suivant" plusieurs fois, pour atteindre l'écran de sélection du rôle. Choisissez "Service de certificats Active Directory" et validez l'écran associé, d'ajout des fonctionnalités requises en cliquant sur le bouton "Ajouter des fonctionnalités". Passez l'écran des fonctionnalités sans rien changer et cliquez sur "Suivant" pour parvenir à l'écran de sélection des services de rôle. Cochez la case devant "Autorité de certification" uniquement. Cliquez alors sur le bouton "Suivant", puis sur "Installer". Une fois l'installation terminée, ne cliquez pas tout de suite sur le lien "Configurer les services de certificats...", une étape doit être réalisée au préalable. Juste après l'installation du rôle, et avant sa configuration, un fichier nommé CAPolicy.inf peut être créé, via bloc-notes, sous C:\Windows afin de fixer certains paramètres avant même le premier démarrage du service comme : Empêcher la publication des modèles de certificats par défaut, Définir la longueur de clé privée de l'autorité lors de son renouvellement, Fixer la durée de validité de la CRL. Pour une autorité racine, j'utilise habituellement, le fichier suivant : [Version] Signature="$Windows NT$" [Certsrv_Server] RenewalKeyLength=4096 RenewalValidityPeriod=Years RenewalValidityPeriodUnits=10 AlternateSignatureAlgorithm=0 CRLPeriod=years CRLPeriodUnits=1 Tous les paramètres sont expliqués dans cette documentation, toutefois voici des indications sur les plus importants : RenewalKeyLength : indique que la longueur de clé privée passera à 4096bits, lors du renouvellement du certificat d'autorité et de sa clé privée. RenewalValidityPeriod/Units : précise que la durée de validité du certificat lors de son renouvellement sera de 10 ans. AlternateSignatureAlgorithm : permet d'utiliser un algorithme de signature plus ancien issu du premier standard PKCS#1 V2.1 A présent, il est possible de terminer l'assistant de configuration, depuis le Gestionnaire de serveur. Cliquez sur le lien "Configurer les services de certificats..." Etant connecté avec un compte administrateur local, cliquez simplement sur "Suivant". Cochez la case devant l'intitulé Autorité de certification. Il peut se passer plus d'une minute avant que le bouton "Suivant" apparaisse. S'agissant d'un serveur en workgroup, seul le choix "Autorité de certification autonome" (Standalone CA) est disponible. Une autorité de type "Enterprise" nécessite que la machine soit intégrée au domaine Active Directory. Ici, il suffit logiquement de choisir "Autorité de certification racine". S'agissant d'une toute nouvelle autorité, il nous faut créer une nouvelle clé privée qui sera stockée localement sous Windows. Dans le cas de l'utilisation d'un HSM (voir le module dédié à la sécurité de ce cours pour plus d'explications), il est possible à ce stade de choisir l'emplacement correspondant au module de sécurité. Plusieurs sélections à faire sur cet écran : La longueur de la clé privée de l'autorité : 2048 bits est le minimum, 4096 bits est un plus en matière de sécurité L'algorithme de hachage pour l'émission des certificats : SHA256 est le minimum, SHA512 est un choix raisonnable pour une autorité racine L'option Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée est utile avec un module HSM (voir rubrique sur la Sécurité dans ce cours pour plus d'explications), l'administrateur devant parfois entrer un mot de passe pour autoriser l'accès à la clé privée. Sans module HSM, ici la case reste décochée. L'écran suivant présente les noms liés à l'autorité. Il s'agit d'informations que l'on retrouvera typiquement dans les certificats issus de cette autorité. Si j'ai barré les infos, c'est pour marquer le fait qu'il ne faut pas laisser les valeurs par défaut et ce pour plusieurs raisons : Le nom du serveur apparait dans le nom convivial mais lors d'une migration vers une nouvelle machine souvent avec un nom différent, il ne sera pas possible de le changer, d'où une incohérence, Divulguer le nom du serveur donne trop d'indications inutilement, et ce n'est pas idéal en termes de sécurité, Les informations minimales (organisation...) ne sont pas fournies dans le certificat, aussi il pourrait être considéré invalide par certains navigateurs. Pour toutes les raisons évoquées précédemment, une syntaxe telle qu'illustrée ci-dessous sera beaucoup plus pertinente : Indiquer ensuite la durée de validité de la clé privée : Concernant l'emplacement de la base de données et des journaux de transaction de l'autorité, il faut savoir que les bonnes pratiques Microsoft indiquent de les positionner sur un disque à part. La raison évoquée parle d'accès fréquents et simultanés. Objectivement, sauf à émettre des certificats par centaine toutes les minutes, ça ne sera pas nécessaire, aussi vous pouvez conserver un hébergement sur le disque système avec les chemins par défaut. Tout est prêt, il ne reste plus qu'à cliquer sur le bouton "Configurer". Quelques secondes plus tard, vous obtiendrez un message de réussite. Lancez la console MMC "Autorité de certification", à présent disponible dans les outils d'administration. Depuis les propriétés de la rubrique "Certificats révoqués", observez que la durée de validité de la CRL est bien de 1 an comme défini dans le fichier CAPolicy.inf. Bien que cette autorité autonome ne fasse pas partie du domaine, les CRL Distribution Points (CDP) et les emplacements Authority Information Access (AIA), vont être stockés dans l'Active Directory. Elle doit disposer des informations du domaine pour permettre une publication correcte. Exécutez la commande suivante (en adaptant le DistinguishedName pour qu'il corresponde à votre domaine) : certutil.exe -setreg ca\DSConfigDN CN=Configuration,DC=contoso,DC=ad Le certificat de l'autorité (sans sa clé privée) peut être désormais intégré à l'Active Directory. Cela aura pour effet de le pousser automatiquement sur toutes les machines du domaine. Une fois cette configuration établie, il ne sera pas nécessaire de le pousser en plus par GPO, comme je le vois souvent. Rien de grave si c'est le cas, néanmoins il sera présent en doublon sur les postes et serveurs du domaine. La première étape consiste à exporter le certificat d'autorité. Depuis la console MMC "Autorité de certification", appelez les propriétés sur le nom de l'autorité. Vous pourrez alors "Afficher le certificat" et le "Copier dans un fichier..." Sur le format d'export, choisissez Base64. Le format DER est lu, lui aussi,mpris par Windows, mais l'encodage en Base64 présente deux avantages principaux : Il est human-readable, cela signifie qu'en ouvrant le fichier avec un éditeur de texte, vous pourrez lire la structure qui commence généralement par ---BEGIN CERTIFICATE--- C'est un format PEM compris par des machines Linux Cliquez alors sur "Suivant". Un emplacement et un nom de fichier vous seront demandés. Terminez l'assistant jusqu'au bout. Copiez ce fichier sur un serveur membre du domaine ou sur un contrôleur de domaine. Puis lancez la commande suivante depuis une invite : certutil -dspublish -f C:\certificats\ContosoRootCA-cert.cer RootCA Note : le nom RootCA n'est pas le nom de l'autorité, mais l'indication du container où intégrer le certificat. Le résultat doit être similaire à celui-ci : Il est même possible de retrouver le certificat publié, en ouvrant la console "Sites et Services Active Directory". Dans le menu « Affichage », veillez à cocher "Afficher les nœuds des services". Vous pourrez observer la présence du certificat dans le conteneur "Certification Authorities". Par défaut, les certificats émis par l'autorité sont valables 2 ans. Puisque nous allons demander, peu plus tard, un certificat pour la première autorité intermédiaire qui devra être valable 5 ans, nous devons étendre cette durée. Depuis une invite de commandes PowerShell, exécutez ces commandes : Certutil -setreg CA\ValidityPeriodUnits 5 Certutil -setreg CA\ValidityPeriod "Years" Restart-Service certsvc Note : la commande modifie des entrées de registre qui sont présentes sous "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\". La liste de révocation de certificats (CRL) est valable 1 an comme nous l'avons paramétré précédemment. Elle sera utilisée pour vérifier la révocation des certificats émis par cette autorité. Toutefois, cette CRL n'est mise à disposition qu'en local, sur l'autorité racine. Pour le vérifier, il suffit de prendre les propriétés de l'autorité depuis la console de gestion de l'autorité de certification, à la rubrique « Extensions », puis « CDP ». On constate un chemin local sous « C:\Windows\System32 ». Allons voir de plus près : Le fichier de CRL est bien présent, de même que le certificat de l'autorité. De retour sur la console de gestion de l'autorité, on voit plusieurs emplacements pré-renseignés et des cases « Publier » ou « Inclure », certaines grisées, d'autres non. L'explication est la suivante : Publier : indique de générer le fichier à cet emplacement, Inclure : référence ce chemin dans tous les certificats émis par l'autorité, de sorte qu'un client qui se voit présenter un certificat et veut en vérifier sa révocation sache à quel endroit se référer. Pour que l'option soit accessible, il doit s'agir d'un chemin réseau de type UNC, LDAP, ou Web, commençant donc par \\, ldap, ou http. Dans notre architecture, un serveur est utilisé pour la publication des CRL, nous allons par conséquent ajouter l'information dans les extensions. Voici comment : Cliquez sur le bouton "Ajouter", Tapez le début de l'adresse (alias) du serveur CRL Dans la liste déroulante des "variables", sélectionnez puis, Cliquez sur "Insérer". Insérez une autre variable, SuffixeNom... pour refléter la liste de révocation, et terminez en tapant ".crl" pour l'extension du fichier. Il ne reste plus qu'à cocher la case "Inclure dans l'extension CDP...". Pour l'emplacement « file:// », vous pouvez aller décocher les deux cases "Inclure", elles ne nous seront pas utiles. Enfin, en validant par OK la fenêtre, un redémarrage du service de l'autorité vous sera demandé. Cliquez sur le bouton « Oui ». Dernière étape : copier le fichier de CRL vers le serveur « SERVICESCA » de notre architecture. Vous pouvez le récupérer sous « C:\Windows\System32\CertSrv\CertEnroll ». Copier également le fichier de certificat portant l'extension .crt, il nous sera utile un peu après. Si le dossier « wwwroot » n'existe pas à la cible, vérifiez que vous avez bien suivi l'installation du prérequis IIS mentionné au paragraphe d'introduction. Toujours depuis l'onglet Extensions, choisissez AIA dans la liste déroulante. Il nous faut à présent retirer le chemin "file" qui ne sera pas joignable, car il fait référence à l'autorité racine qui sera éteinte ensuite. Nous allons le remplacer par un emplacement http vers notre serveur SERVICES-CA qui lui restera joignable. Nom du serveur DNS>_.crt Pour terminer, cocher la case "Inclure dans l'extension AIA des certificats émis". À présent que notre autorité de certification racine est installée et configurée, nous allons pouvoir déployer une première autorité intermédiaire. Vous découvrirez comment dans le prochain chapitre. Offline Root Certificate Authority - Windows Server Every organization that has an Active Directory structure, or any other service that uses SSL/TLS services (ie. HTTPS, RDP, etc.), should have a certificate authority. This certificate authority is used to verify that you are indeed talking directly with the server you think you are and that the connection is secure. Having a certificate authority is also required to enable secure LDAP (LDAPS), though this can also be done with an external certificate authority.Choosing to host your offline root CA on a Windows-based system, rather than Linux, will feel more comfortable to those who are not familiar to Linux. However, since this server will be shutdown 99% of the time and should never be on the network once configured, it may seem like a waste of a server license.Why have an offline Root CA?If a root CA is in some way compromised (broken into, hacked, stolen, or accessed by an unauthorized or malicious person), then all of the certificates that were issued by that CA are also compromised. Since certificates are used for data protection, identification, and authorization, the compromise of a CA could compromise the security of an entire organizational network. For that reason, many organizations that run internal PKIs install their root CA offline. That is, the CA is never connected to the company network, which makes the root CA an offline root CA. Make sure that you keep all CAs in secure areas with limited access.1 – Microsoft TechNetRequirementsLatest Windows Server available installed on a single-purpose physical serverYou will need to be able to transfer files to and from this device via USB drive.We'll be using Windows Server 2022 for this example.This system will be used as an offline root CA, therefore it will be powered off after we're done.USB drive formatted with ExFAT or FAT32 file systemUpdate the server with Windows UpdateAt this point, there is no need for the server to be connected to the network. You should remove the network cable from the ethernet port. If this is a device with a wireless card, ensure it is not connected to the wireless or even remove the WLAN card.Create CAPolicy.inf FileOpen Powershell as AdministratorCreate a new file with notepad.exe called CAPolicy.inf in C:\Windows1 2 cd C:\Windows notepad.exe CAPolicy.inf Answer Yes to create the new fileCopy this text into the file1 2 3 4 5 6 7 [Version] Signature="$Windows NT$" [Certsrv_Server] RenewalKeyLength=4096 RenewalValidityPeriod=Years RenewalValidityPeriodUnits=20 AlternateSignatureAlgorithm=1 Save and close the CAPolicy.inf fileInstall the Active Directory Certificate Services RoleOpen Server Manager, if not already openClick Manage in the top right cornerClick Add Roles and FeaturesOn Before You Begin, click NextOn Installation Type, ensure Role-based or feature-based installation is selected and click NextOn Server Selection, ensure this server is selected and click NextOn Server Roles, check Active Directory Certificate Services, on the pop-up click Add Features, then click NextOn Features, click NextOn AD CS, click NextOn Role Services, ensure Cerificate Authority is checked and click NextOn Confirmation, click InstallIf the Installation Wizard is still open, click Configure Active Directory Certificate Services on the destination server. Otherwise, in Server Manager click the flag icon in the upper right which should have a warning symbol (⚠), then Post-deployment ConfigurationOn Credentials, click NextOn Role Services, check Certification Authority, then click NextOn Setup Type, click Next (Standalone CA is the only available option)On CA Type, select Root CA and click NextOn Private Key, ensure Create a new private key is selected, then click NextOn Cryptography, set the Key length to 4096On CA Name, set the Common name to a descriptive value, such as "Contoso Root CA", then click NextOn Validity Period, set the validity period to 20 Years.On Certificate Database, click NextOn Confirmation, click ConfigurePerform Post Installation ConfigurationOpen Powershell ad AdministratorDefine the Active Directory Configuration Partition Distinguished Name (Substitute your DC values)1 certutil -setreg CA\DSConfigDN "CN=Configuration,DC=ad,DC=example,DC=edu" Define CRL Period Units and CRL Period1 2 3 certutil -setreg CA\CRLPeriodUnits 52 certutil -setreg CA\CRLPeriod "Weeks" certutil -setreg CA\CRLDeltaPeriodUnits 0 Define CRL Overlap Period Units and CRL Overlap Period1 2 certutil -setreg CA\CRLOverlapPeriodUnits 12 certutil -setreg CA\CRLOverlapPeriod "Hours" Define Validity Period Units for all issued certificates by this CA1 2 certutil -setreg CA\ValidityPeriod "Years" certutil -setreg CA\ValidityPeriodUnits 10 certutil -setreg CA\ValidityPeriod "Years" Restart the CA service1 Restart-Service certsvc Publish the Certificate Revocation List (CRL)You should now copy *.crl and *.crt to a USB drive. The two files can be found at C:\Windows\system32\CertSrv\CertEnroll.You will need the root CA certificate and CRL file when you configure the Windows Enterprise Subordinate CAShutdown and Store the MachineYou may now shutdown the server and store it. The only times the server will be needed are when you stand up a new subordinate (intermediate) certificate authority, or when a sub-CA needs its certificate renewed. Sub-CA's should renew their certificates every ten years or so. windows certificate security This post is licensed under CC BY 4.0 by the author. Jul 4, 2022 Every organization that has an Active Directory structure, or any other service that uses SSL/TLS services (ie. HTTPS, RDP, etc.), should have a certificate authority. This certificate authority is... Jul 4, 2022 While extremely convenient, the Remote Desktop Protocol can be extremely dangerous if not secured correctly. Typical things you should consider are ACLs, firewall rules, smart cards, RDP Gateways, ... Jul 3, 2022 Every organization that has an Active Directory structure, or any other service that uses SSL/TLS services (ie. HTTPS, RDP, etc.), should have a certificate authority. This certificate authority is... Offline Root Certificate Authority - Linux Creating an Enterprise Subordinate CA from an Offline Root CA© 2025 Chris Lovett. Some rights reserved.Using the Chirpy theme for Jekyll. In this blog post, we will learn the steps on how to install and configure an Enterprise Root Certificate Authority on Windows Server 2019. An Enterprise Certificate Authority requires Active Directory and is typically used to issue certificates to users, computers, devices, and servers for an organization. Users can request certificates using manual enrollment, web enrollment, auto-enrollment, or an enrollment agent. Step-1. Install Active Directory Certificate Services As this is a virtual test lab, I have chosen to install the CA on to my Domain Controller rather than a dedicated server. Domain Controller: WS2K19-DC01.mylab.local 1. Open Server Manager Console. 2. In the Server Manager console, click on Manage and select Add roles and features. 3. On before you begin screen, click Next. 4. On the Select installation type page, make sure you choose Role-based or feature-based installation. Click Next. 5. On the Select destination server page, choose the local server. Click Next. 6. On the Select server roles page, select Active Directory Certificate Services. 7. When the Add Roles and Features Wizard window appears, click Add Features. 8. Click Next to continue. 9. On the Select features page, click Next. 10. On the Active Directory Certificate Services page, click Next. 11. On the Select role services, make sure you tick Certificate Authority and Certification Authority Web Enrollment checkbox. 12. When you select Certification Authority Web Enrollment, which will open a window explaining about additional features that are required to install Certification Authority Web Enrollment. Click on Add Features. 13. Click on the Next button until you reach to Confirm installation selection page. 14. On the Confirm installation selections page, click on Install button. Wait for few minutes to complete the installation. Step-2 Configure Active Directory Certificate Services 15. On the Installation progress page, after installation is successful, click on Configure Active Directory Certificate Services on the destination server link. 16. On the Credentials page, click Next as already we have login to the server with the credential of Domain Admin. 17. On the Select role services to configure page, select Certification Authority and Certification Authority Web Enrollment service. Click Next. 18. On the Setup Type page, select Enterprise CA, and then click Next. 19. On the CA Type page, ensure that Root CA is selected, and then click Next. 20. On the Private Key page, ensure that Create a new private key is selected, and then click Next. 21. On the Cryptography for CA page, keep the default selections for Cryptographic Service Provider (CSP) and Hash Algorithm. For better security, change the Key length to 4096, and then click Next. 22. On the CA Name page, you can specify any name of your choice. Click Next when you are done. 23. On the Validity Period page, the default is 5 years. Click Next. 24. The CA Database page displays where the certificate database will be stored. Click Next. 25. On the Confirmation page, click Configure. 26. On the Results page, click Close. Step-3 Verify AD CS installation and configuration 27. To confirm that the web enrollment page is working open a web browser and access the URL . 28. To launch the CA Management Console, On Server Manager console, click on Tools and select Certification Authority. At this point, we have successfully deployed the Enterprise Root Certificate Authority with Web Enrollment Service on Windows Server 2019. Cet article explique comment mettre en place une PKI en 2 parties dont l'autorité racine est déconnectée ((two-tier PKI hierarchy). Pour cela l'article reprendre les étapes de ce lien Microsoft Le rôle du rootCA est ici installé sur un serveur nommé MyRootCA. C'est un serveur autonome, non joint à un domaine pour des raisons de sécurité. Il pourra ainsi être éteint pour éviter les problèmes de compromission. En étant en dehors du domaine il n'a pas de problème d'expiration de compte de l'ordinateur (lifetime tombstone). Le rôle du subCA, l'autorité de certification secondaire, sera installé sur le serveur MySubCA qui appartient lui au domaine mydomain.local. Il servira également de CDP / CRL / Certificate Revocation List distribution point et d'AIA (Authorithy Information Access) au travers d'un site web. Les contrôleurs de domaine auront également le rôle de CDP et AIA via l'annuraire LDAP qu'ils hébergent. The CDP is where the certificate revocation list is maintained, which allows client computers to determine if a certificate has been revoked. The AIA is used to point to the public key for the certification authority. Il permet aux ordinateurs de localiser les chemins d'accès aux informations de l'autorité. Le serveur va avoir besoin d'un disque D qui contient un répertoire CertEnroll Dans server manager, ajouter un rôle Cocher Active Directory Services Cliquer sur Post Deployment Configuration Cocher Certification Authority et Next Créer une nouvelle clé privée puis Next Sélectionner une taille de clé ainsi que l'algorithme Choisir une durée de validité Indiquer l'emplacement des logs On peut ensuite re régler la durée de validité des certificats délivrés par le RootCa avec certutil .exe certutil -setreg ca\ValidityPeriod "Years" certutil -setreg ca\ValidityPeriodUnits "5" Lien vers le fichier : cliquez ici Et surtout on peut régler également la durée de validité de la CRL certutil -setreg CA\CRLPeriodUnits 1 certutil -setreg CA\CRLPeriod "Years" certutil -setreg CA\CRLOverlapPeriod "Months" certutil -setreg CA\CRLOverlapUnits 6 Lien vers le fichier : cliquez ici Tous ces paramètres se retrouvent dans la base de registre sous Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration Lien vers le fichier : cliquez ici Comme notre RootCA n'est pas jointe au domaine, il faut utiliser adapter cette commande pour indiquer où stocker les informations dans l'AD, dont l'emplacement de la CRL Certutil –setreg ca\DSConfigDN "CN=Configuration,DC=mydomain,DC=local" Lien vers le fichier : cliquez ici Le site tech-coffee.net partie Extensions configuration (AIA and CDP) indique qu'il faut configurer de suite les extensions AIA et CDP, sinon ces informations ne seront pas dans les certificats, et pour corriger le tir il faudra les regénérer. Pour le CDP, ce lien Microsoft indique qu'on peut paramétrer les options en ligne de commande. Accédez la console de gestion de la pki avec certsrv.msc Lien vers le fichier : cliquez ici Accédez aux propriétés de la Root Ca La configuration de la CRL Distribution Point et de l'AIA se voient sous Extensions Pour paramétrer la CRL Distribution Point vis à vis de notre infrastructure, la ligne de commande adaptée donne certutil -setreg CA\CRLPublicationURLs "1:D:\CertEnroll\%7%8%9.crl10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%102: Lien vers le fichier : cliquez ici certutil -setreg CA\CACertPublicationURLs "1:D:\CertEnroll\%1_%3%4.crt2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%112: Lien vers le fichier : cliquez ici Restart-Service CertSvc -force Lien vers le fichier : cliquez ici Visuellement la configuration du CDP est passé sur 3 lignes Et voici visuellement à quoi ressemble la configuration del'AIA Pour l'instant le répertoire CertEnroll est vide Mettez à jour la CRL du root en cliquant sur Revoked Certificates>All tasks>Publish Cela crée le fichier Certificate Revocation List On va exporter le certificat publique du root ca pour pouvoir ensuite le copier sur le futur subca. Pour cela, aller dans les propriétés du rootca, aller sur l'onglet General puis visualiser son certificat Aller sur l'onglet details du certificat du rootca puis cliquer sur Copy to File Cliquer sur Next puis exporter le rootca en Base-64 Le format DER convient aussi Ici on va le nommer rootca.cer Le codage en baes-64 a l'avantage d'être lisible quand on ouvre le fichier Copier le certificat du root CA ainsi que la crl sur le subCA dans D:\CertEnroll On les utilisera par la suite Passer sur le serveur du SubCA En point de détail, j'ai renommé le rootca.cer en rootca.crt Donc depuis le serveur du SubCA (lui seul est joint à l'AD), publier dans l'active directory le certificat du rootCA en adaptant cette commande. Le dernier paramètre est bien RootCA et pas autre chose, comme le nom du serveur. certutil -f -dspublish RootCA Lien vers le fichier : cliquez ici RootCA est un paramètre de certutil -f -dspublish Visuellement dans l'AD avec adsiedit, cela fait apparaitre ceci Publier dans l'active directory la CRL du rootCA en adaptant cette commande Mettez bien le nom du serveur de votre rootCA, pas le nom de l'autorité de la rootCA certutil -dsPublish -f Lien vers le fichier : cliquez ici Visuellement dans l'AD avec adsiedit, cela fait apparaitre ceci If you've been following best practices, you likely have a multi-tiered Microsoft PKI with an offline root CA. In this case you'll have to publish a new Certificate Revocation List using your offline CA server and install this on your online CA server. The steps involved in completing this process. Generating the new CRL Using the Offline CA First, you'll need to power up your offline CA. Once it's finished booting, navigate to C:\windows\system32\certsrv\certenroll and rename your current CRL (filename may vary, but should be the only file in this folder with a *.crl extension) to *.crl.old. Now under Administrative Tools open the Certificate Authority management console. Once this has loaded, right-click on the Revoked Certificates folder and choose All Tasks > Publish. Select New CRL from the next prompt that appears. This will generate a new CRL file in the same location as the one we just renamed (C:\windows\system32\certsrv\certenroll\yourfilename.crl), we need to copy this somewhere that will be accessible from the online CA server. Once you've copied the CRL file somewhere accessible, you can shut down the offline CA server again. Publishing the new CRL in Active Directory We now need to log onto our online CA server and copy the new CRL file to C:\windows\system32\certsrv\certenroll. Once you've copied the file here we need to open command prompt as an administrator and run the following command: Certutil -v -f -dsPublish "c:\windows\system32\certsrv\certenroll\yourfilename.crl" We should see a message as above stating that the dsPublish command completed successfully. We can verify this by opening MMC on the online CA, loading the Enterprise PKI snap-in and selecting our Root CA name (offline root). Verify that CDP locations 1 and 2 are showing with a status of OK and that the expiration date is X weeks ahead of the current date (this date will depend on the periods you configured when installing your PKI servers). Parmi les éléments importants dans la configuration d'une autorité de certification, il y a les extensions. Ces extensions sont généralement présentes sur les certificats que l'autorité émet et permettent de définir un lien vers le certificat de l'autorité racine ainsi qu'un lien vers la liste des certificats révoqués. Le principe de configuration est le même pour une autorité racine autonome ou pour une autorité d'entreprise. Néanmoins certains éléments, comme la publication de la liste de révocation dans Active Directory n'est exploitable que dans une autorité d'entreprise. Dans cette étape, nous allons configurer les URL pour la publication de la liste de révocation et les informations de l'autorité de certification (AIA). Pour configurer les extensions, ouvrez la console « Autorité de certification » depuis les outils du gestionnaire de serveurs, ou en exécutant la commande « certsrv.msc ». Dans la console de l'autorité, faites un clic droit sur le nom à droite, puis sélectionnez « propriétés ». Sélectionnez la page « extensions », puis vérifier que vous êtes bien sur l'extension « Point de distribution de liste de révocation des certificats (CPD) ». Vous retrouvez 4 lignes par défaut. Selon les cas, les différentes options peuvent servir soit à définir un chemin dans lequel l'autorité va écrire la liste de révocation (.crl), soit définir le chemin qui sera inclus dans les certificats émis. Par exemple, le chemin « c:\windows\system32\certsrv\certenroll » n'est pas écrit sur les certificats, mais est utilisé comme emplacement de dépôt de la liste de révocation. Sur une autorité racine autonome, il vous faudra prévoir de publier ses éléments sur un emplacement « http » accessible par les postes et serveurs. Nous verrons la configuration du site http avec IIS par la suite. Sélectionner la première ligne, en rouge ci-dessous, et vérifier que les options de publications sont bien sélectionnées. Sélectionner les 3 autres lignes (ldap, http, file) et décocher toutes les options. Cliquez sur le bouton « ajouter » et insérez l'url définit lors de la planification, puis « OK ». Dans notre exemple : Sélectionnez l'option « inclure dans l'extension CPD des certificats émis ». Les certificats qui seront créer par cette autorité incluront l'URL de la liste de révocation. Sélectionnez les informations de l'autorité « Accès aux informations de l'autorité (AIA) » dans la liste déroulante. Sélectionnez les 4 lignes une par une et vérifier que l'option « inclure dans l'extension AIA des certificats émis » n'est pas activé. Cliquez ensuite sur ajouter. Copier l'url qui sera utilisé pour afficher le certificat de l'autorité racine, puis cliquez sur ajouter et coller la valeur, et validez en cliquant sur « OK ». Dans notre exemple : Cocher l'option « inclure dans l'extension AIA des certificats émis ». Cliquez sur « OK » pour valider les modifications. Un redémarrage des services de l'autorité de certification sera nécessaire. Cliquez sur « oui » pour redémarrer maintenant.