04 - Gérer la révocation de certificats

Dans le cadre de la gestion d'un cycle de vie des certificats, vous devez non seulement contrôler leur émission, mais également suivre leur utilisation et, si nécessaire, appliquer leur révocation. Cela est essentiel pour atténuer et corriger la compromission potentielle de la sécurité basée sur les certificats.

Qu'est-ce que la révocation de certificats ?

La révocation est le processus dans lequel vous désactivez la validité d'un ou plusieurs certificats. En lançant le processus de révocation, vous publiez une empreinte de certificat dans la liste de révocation de certificats correspondante. Cela indique qu'un certificat spécifique n'est plus valide.

> **Chaque certificat a sa propre période de validité, après quoi il n'est plus considéré comme valide. Avec la révocation, vous pouvez invalider le certificat avant que cette période ne s'écoule, par exemple, pour corriger la compromission du certificat.**

Le processus de révocation se compose généralement de la séquence d'étapes suivante :

1. Révoquer un certificat et indiquer la raison ainsi que la date et l'heure cibles. Vous pouvez effectuer cette tâche à partir de la console de l'autorité de certification.
2. Publier une liste de révocation de certificats. Vous avez la possibilité de déclencher la publication à partir de la console de l'autorité de certification ou de planifier une publication automatique à intervalles réguliers. Vous pouvez publier des listes de révocation de certificats dans AD DS, dans un dossier partagé ou sur un site web.
3. Si un système d'exploitation, une application ou un service lance une action sécurisée qui implique l'utilisation d'un certificat, une vérification automatique de l'état de révocation de ce certificat est déclenchée en interrogeant l'autorité de certification émettrice et l'emplacement CDP correspondant. Ce processus détermine si le certificat est révoqué.

> **La prise en charge de la vérification automatique de l'état de révocation d'un certificat dépend de la façon dont un système d'exploitation, une application ou un service a été implémenté. La plupart des logiciels commerciaux modernes prennent en charge cette fonctionnalité.**

Les systèmes d'exploitation Windows incluent CryptoAPI, qui est responsable des processus de révocation de certificat et de vérification de l'état. CryptoAPI utilise les phases suivantes dans le processus de vérification de certificat :

- Détection de certificats. La détection de certificats collecte les certificats d'autorité de certification, les informations AIA dans les certificats émis et les détails du processus d'inscription de certificats.
- Validation du chemin d'accès. La validation du chemin d'accès est le processus qui consiste à vérifier le certificat via la chaîne d'autorité de certification, ou chemin d'accès, jusqu'à ce que le certificat d'autorité de certification racine soit atteint.
- Vérification de la révocation. Chaque certificat dans la chaîne de certificats est vérifié pour s'assurer qu'aucun des certificats n'est révoqué.
- Récupération du réseau et mise en cache. La récupération du réseau s'effectue à l'aide du protocole OCSP. CryptoAPI est responsable de la vérification préalable dans le cache local des informations de révocation et, s'il n'existe aucune correspondance, d'effectuer un appel à l'aide du protocole OCSP qui est basé sur l'URL fournie par le certificat émis.

Qu'est-ce qu'un service Répondeur en ligne ?

Un service Répondeur en ligne offre un moyen plus efficace de vérifier l'état de révocation des certificats. Le service Répondeur en ligne s'appuie sur le protocole OCSP pour déterminer l'état de révocation d'un certificat. Le protocole OCSP soumet les requêtes d'état de certificat à l'aide du protocole HTTP.

Les clients accèdent aux listes de révocation de certificats pour déterminer l'état de révocation d'un certificat. Les listes de révocation de certificats peuvent être volumineuses et les clients peuvent consacrer beaucoup de temps à la recherche dans ces listes de révocation de certificats. Un service Répondeur en ligne peut rechercher dynamiquement dans ces listes de révocation de certificats pour les clients et renvoyer l'état du certificat demandé au client. Vous pouvez utiliser un répondeur en ligne unique pour déterminer les informations d'état de révocation pour les certificats émis par une autorité de certification unique ou par plusieurs autorités de certification. Vous pouvez également implémenter plusieurs répondeurs en ligne pour distribuer les requêtes de révocation de l'autorité de certification.

Vous devez configurer les autorités de certification de façon à inclure l'URL du répondeur en ligne dans l'extension AIA des certificats émis. Le client OCSP utilise cette URL pour valider l'état du certificat. Vous devez également émettre le modèle de certificat de signature de réponse OCSP afin que les répondeurs en ligne puissent inscrire ce certificat.

Atelier

Objectif

- Configurer la publication des listes de révocation de certificats.

Configurer la publication des listes de révocation de certificats :

- Dans la console `Autorité de certification`, faire bouton droit sur le nom de l'autorité
  puis `Propriétés` et ensuite l'onglet `Extensions`
- Sur le dossier `Certificats révoqués`, choisir `Toutes les tâches` puis `Publier`
- Aller dans le dossier `C:\Windows\System32\CertSrv\CertEnroll`, nous voyons le fichier `staff-SRVROOTCA.crl`

Configurer l'emplacement CDP :

- Créer sur un serveur Windows membre de l'AD, un dossier : `c:\Crl' partagé avec les autorisations` Tout le monde` (Modification)
- Mettre les permissions NTFS `Tout le monde` (Modification)
- Dans la console `Autorité de certification`, faire bouton droit sur le nom de l'autorité puis `Propriétés` et ensuite l'onglet `Extensions`
- Ajouter un pont de distribution de liste de révocaltion des certificats (CDP) :
  `file://\\srvdc1\Crl\<NomAutoritéCertification>`
  `<SuffixeNomListeRévocationCertificats>`
  `<ListeRévocationCertificatsDeltaAutorisée>.crl`
- Cocher :
  - `Publier les listes de révocation des certificats à cet emplacement`
  - `Publier Les listes de rstaff-SRVROOTCA.crlévocations des certificats delta à cet emplacement`
- Faire `Appliquer` et redémarrer le service
- Fermer la boite de dialogue
- Sur le dossier `Certificats révoqués`, choisir `Toutes les tâches` puis `Publier`
- Sur le serveur `\\srvdc1\Crl\`, vous avez 2 fichiers :
  - Fichier CRL : `staff-SRVROOTCA.crl`
  - Fichier delta CRL : `staff-SRVROOTCA+.crl`

Le symbole "+" dans le nom du fichier CRL indique qu'il s'agit d'une "Delta CRL", qui est une liste de révocation incrémentielle. Elle ne contient que les certificats révoqués ou expirés depuis la publication de la dernière CRL complète, afin de réduire la taille des fichiers transférés et accélérer la distribution des informations de révocation.