Bonnes pratiques d'une PKI ADCS

Voici quelques bonnes pratiques pour déployer une infrastructure de clés publiques, autrement appelé Active Directory Certificates Services. Tour d'horizon…

Installation du rôle ADCS

- Installer le rôle ADCS en Enterprise Edition pour les versions inférieures à Windows Server 2012, l'édition Standard est suffisante à partir de la version 2012
- Les noms de serveurs, de l'autorité de certification, GPO, template et comptes de services doivent respecter une charte de nommage standardisée mais différente de celle dédiée à votre infrastructure interne
  - Eviter de changer les noms après l'installation des rôles
  - L'enrollment va s'arrêter de fonctionner
  - Remédiation possible mais compliquée et non recommandée par Microsoft
- Ne pas installer le rôle ADCS sur un contrôleur de domaine
- Déployer le rôle ADCS à l'aide du fichier CAPolicy.inf qui permet une installation plus avancée au niveau des options. Lien Microsoft
- Créer des comptes de services différentes pour les opérateurs, les templates, auditeurs, administrateurs PKI et certificats

Architecture multi-tiers

- Déployer à minima une architecture à 2 niveaux (ROOT CA et Issuing CA) mieux à 3 niveaux(ROOT CA, Intermediate/Policy CA, Issuing CA). Lien Microsoft – Déploiement d'un architecture PKI à 2 niveaux
- Issuing CA de doit être employée que pour les utilisateurs
- Utiliser un module HSM dès la construction de votre autorité. Lien Microsoft
- Utiliser de préférence des clés d'une longueur de 4096 pour la ROOT CA et un algorithme de hash SHA256 (Deprecation SHA1)
- Placer les VM ou disque virtuels dans un emplacement sécurisé et doivent être Offline hormis pour renouveler une CRL ou un certificat
- Changer les comptes systèmes par défaut et utiliser des mots de passe complexes
- Le groupe Domain Admins doit être retiré des groupes administrateurs locaux sur l'ensemble des serveurs PKI
- Utiliser OCSP qui offre une fonction de vérification en ligne de la validité d'une certificat en interne et en externe
- Le delta CRL doit être de 1 journée
  - `certutil -setreg CA\CRLDeltaPeriodUnits 1`
  - `certutil –setreg CA\CRLDeltaPeriod "Days"`
- Utiliser NTP sur les serveurs PKI

Global

- Utiliser des chemins HTTP (grandement recommandé) plutôt que LDAP pour le path CDP

- [1]CRL Distribution Point
- [1]Authority Info Access
- Distribution Point Name:
  Full Name:

  URL=ldap:///CN=Contoso%20CA,CN=DC1,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,

  DC=contoso,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
  URL=http://dc1.contoso.com/CertEnroll/Contoso%20CA.crl Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
  Alternative Name:

  URL=ldap:///CN=Contoso%20CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,
  DC=contoso,DC=com?cACertificate?base?objectClass=certificationAuthority

  [2]Authority Info Access

  Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
  Alternative Name:
  URL=http://dc1.contoso.com/CertEnroll/DC1.contoso.com_Contoso%20CA.crt
- Pour le déploiement EFS, déployer KRA (Key Recovery Agent qui permet de retrouver un key privée perdue) et DRA (Data Recovery Agent qui permet de décrypter des données). Lien Microsoft
- Utiliser des templates personnalisés. Vous pouvez vous baser sur un Private Enterprise Number (PEN) – Lien SANS – Demande de PEN

Root CA

- Ne jamais joindre un ROOT ou Subordinate CA à un domaine
  - Laisser les serveurs dans un WORKGROUP
- Ne jamais délivrer de certificats aux utilisateurs depuis la ROOT CA

Maintenance

- Sauvegarder et vérifier régulièrement l'infrastructure PKI
  - Exporter la clé de registre HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc
  - Exporter les templates, sauvegarder les logs, la base de données, CAPolicy.inf …
  - Sauvegarder l'emplacement C:\Windows\System32\certsrv\CertEnroll*
- L'outil PKIview permet de vérifier la santé de votre PKI
- L'observateur d'événements -Sécurité – permet d'auditer votre PKI

- Accroître les logs via la clé de registre suivante HKLM\CurrentControlSet\Services\certsrv\configuration\Subordinate CA\Loglevel en changeant la valeur de 3 à 4
- Auditer l'ensemble des événements via la ligne de commande certutil -setreg CA\AuditFilter 127

Quelques sources d'informations additionnelles:

https://www.sysadmins.lv/blog-en/designing-crl-distribution-points-and-authority-informatio--access-locations.aspx

http://www.tech-coffee.net/public-key-infrastructure-part-4-configure-certificate-revocation-list/