AD CS : déployer une PKI d'entreprise avec Root CA offline et CA émettrice

Déployer une PKI d'entreprise avec AD CS (Active Directory Certificate Services) repose sur une architecture à deux niveaux : une Root CA hors ligne pour protéger la clé racine, et une CA émettrice connectée au domaine pour délivrer les certificats du quotidien. Ce guide couvre l'installation complète, la configuration CRL/AIA, et les bonnes pratiques ANSSI pour une infrastructure PKI souveraine et auditée.

L'infrastructure AD CS PKI d'entreprise constitue la colonne vertébrale de la confiance numérique dans un domaine Windows : elle signe les certificats de contrôleurs de domaine, sécurise les connexions LDAPS, authentifie les postes via 802.1X et protège les flux TLS internes. Selon l'ANSSI (rapport 2022), plus de 80 % des grandes entreprises françaises opèrent une PKI Active Directory, mais moins de 30 % respectent le modèle Root CA offline préconisé par le guide d'hygiène informatique. Un déploiement mal configuré expose l'ensemble du domaine aux attaques ESC1 à ESC16 documentées par SpecterOps. Ce guide vous conduit pas à pas à travers l'installation de Windows Server 2022, la configuration de la Root CA hors réseau, le déploiement de la CA émettrice subordonnée, la publication des CRL sur un serveur web dédié, et la validation via certutil. Durées de validité recommandées : Root CA 20 ans, CA émettrice 10 ans, certificats endpoint 1 à 2 ans. Chaque commande PowerShell est commentée et testée sur Windows Server 2022 Datacenter.

À RETENIR

À retenir

Root CA toujours hors ligne : la clé privée racine ne doit jamais être exposée sur le réseau — une VM éteinte ou un serveur physique isolé suffit à réduire le rayon de compromission à zéro.

CA émettrice rejoignant le domaine : la Subordinate CA est la seule connectée à l'AD ; c'est elle qui délivre les certificats aux utilisateurs, machines et services.

CRL et AIA sur HTTP, pas LDAP : les clients non-Windows (Linux, appliances réseau) ne résoudront pas les URL LDAP — publier les CRL sur un serveur web interne (port 80) est impératif.

Durée Root CA 20 ans, Sub CA 10 ans : tout certificat endpoint doit expirer avant sa CA émettrice ; respecter cette hiérarchie évite les ruptures de chaîne de confiance.

Audit ESC1-ESC8 après déploiement : utiliser Certify.exe ou l'outil intégré `certutil -v -template` pour vérifier qu'aucun template n'autorise l'enrollment arbitraire.

Prérequis et architecture — Qu'est-ce qu'on va déployer ?

Une PKI d'entreprise Active Directory repose sur une hiérarchie à deux niveaux. La **Root CA (autorité racine)** est une machine Windows Server installée hors domaine, sans carte réseau active, qui génère la clé privée racine et signe le certificat de la CA émettrice. Une fois cette opération effectuée, le serveur Root CA est éteint et stocké hors ligne. La **CA émettrice (Subordinate CA)** est un membre du domaine Active Directory ; c'est elle qui émet tous les certificats du quotidien : contrôleurs de domaine, serveurs web internes, postes utilisateurs, équipements réseau.

Les prérequis matériels et logiciels sont les suivants :

Deux serveurs (physiques ou VM) sous Windows Server 2019 ou 2022, avec au minimum 4 Go de RAM et 60 Go de stockage chacun.

Un domaine Active Directory fonctionnel avec au moins un contrôleur de domaine Windows Server 2016+.

Un serveur web (IIS ou Apache) joignable à l'URL `http://pki.mondomaine.lan/` pour publier les CRL et les certificats CA.

Les droits Administrateur du domaine pour rejoindre la Sub CA et publier les objets dans l'AD.

Le module PowerShell PSPKI optionnel : `Install-Module -Name PSPKI` pour automatiser certaines tâches.

Composant	Rôle	Connecté au réseau	Membre du domaine	Durée de vie du certificat
Root CA	Signe le certificat de la Sub CA	Non (hors ligne)	Non	20 ans
CA émettrice (Sub CA)	Émet tous les certificats endpoint	Oui	Oui	10 ans
Serveur CRL/AIA	Publie listes de révocation et chaîne	Oui (HTTP 80)	Optionnel	N/A
Certificats endpoint	Machines, users, services TLS	Oui	Oui	1–2 ans

Étape 1 — Installation et configuration de la Root CA hors ligne

La Root CA doit être configurée sur un serveur **isolé du réseau**. Si vous utilisez une VM Hyper-V ou VMware, désactivez l'interface réseau avant de démarrer l'installation d'AD CS. Cette isolation est la mesure de sécurité la plus importante de toute la PKI.

Étape 1 — Installer le rôle AD CS : ouvrir une session PowerShell en administrateur et exécuter la commande suivante. Ne pas configurer l'intégration AD puisque ce serveur n'est pas membre du domaine.

```
 # Installer le rôle sans configurer l'entreprise
Install-WindowsFeature -Name ADCS-Cert-Authority -IncludeManagementTools

# Configurer la Root CA standalone (non liée à un domaine)
Install-AdcsCertificationAuthority `
  -CAType StandaloneRootCA `
  -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
  -KeyLength 4096 `
  -HashAlgorithmName SHA256 `
  -ValidityPeriod Years `
  -ValidityPeriodUnits 20 `
  -CACommonName "MonEntreprise Root CA" `
  -CADistinguishedNameSuffix "O=MonEntreprise,C=FR" `
  -Force
```

Étape 2 — Configurer les CDP et AIA : définir les URLs de publication CRL et AIA avant d'émettre le moindre certificat. Ces URLs doivent pointer vers votre serveur web interne accessible en HTTP.

```
 # Supprimer les URLs LDAP par défaut (inutilisables hors domaine)
$crlList = Get-CACrlDistributionPoint
foreach ($crl in $crlList) { Remove-CACrlDistributionPoint $crl.Uri -Force }

$aiaList = Get-CAAuthorityInformationAccess
foreach ($aia in $aiaList) { Remove-CAAuthorityInformationAccess $aia.Uri -Force }

# Ajouter l'URL HTTP pour le CDP (liste de révocation)
Add-CACrlDistributionPoint -Uri "http://pki.mondomaine.lan/crl/.crl" -AddToCertificateCdp -Force

# Ajouter l'URL HTTP pour l'AIA (chaîne de confiance)
Add-CAAuthorityInformationAccess -Uri "http://pki.mondomaine.lan/certs/_.crt" -AddToCertificateAi

# Redémarrer le service pour appliquer
Restart-Service certsvc
```

Étape 3 — Publier la CRL initiale : générer et exporter la liste de révocation ainsi que le certificat Root CA vers une clé USB pour transfert vers la Sub CA.

```
 # Publier la CRL dans C:\Windows\System32\CertSrv\CertEnroll
certutil -crl

# Exporter le certificat Root CA
certutil -ca.cert "E:\PKI-Export\RootCA.crt"

# Copier la CRL sur la clé USB
Copy-Item "C:\Windows\System32\CertSrv\CertEnroll\*" "E:\PKI-Export" -Force

# Vérifier le contenu de l'export
Get-ChildItem "E:\PKI-Export"
# Résultat attendu : RootCA.crt, MonEntreprise Root CA.crl
```

Après cette étape, **éteignez le serveur Root CA** et rangez-le dans un endroit sécurisé. Il ne sera rallumé que pour renouveler le certificat de la Sub CA ou révoquer une CA compromise.

Étape 2 — Déploiement de la CA émettrice (Subordinate CA)

La CA émettrice doit être un serveur **membre du domaine Active Directory**. Elle fera l'objet d'une demande de certificat signée par la Root CA. Ce processus nécessite un transfert de fichiers par clé USB entre les deux machines.

Étape 1 — Installer le rôle sur la Sub CA : sur le serveur membre du domaine, installer le rôle en mode entreprise.

```
 # Installer le rôle AD CS avec les outils de gestion
Install-WindowsFeature -Name ADCS-Cert-Authority, ADCS-Web-Enrollment -IncludeManagementTools

# Générer une demande de certificat subordonné (fichier .req)
# Cette commande crée la clé privée et le fichier de demande
Install-AdcsCertificationAuthority `
  -CAType EnterpriseSubordinateCA `
  -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
  -KeyLength 2048 `
  -HashAlgorithmName SHA256 `
  -CACommonName "MonEntreprise Issuing CA" `
  -CADistinguishedNameSuffix "O=MonEntreprise,C=FR" `
  -OutputCertRequestFile "C:\SubCA.req" `
  -Force
```

Étape 2 — Signer la demande sur la Root CA : transférer `SubCA.req` sur la clé USB, démarrer la Root CA, et soumettre la demande.

```
 # Sur la Root CA (après transfert USB)
# Soumettre la demande et récupérer l'ID de la demande
certreq -submit -config "RootCA\MonEntreprise Root CA" "E:\SubCA.req"
# Résultat : Request ID: 2

# Émettre le certificat (remplacer 2 par l'ID obtenu)
certutil -resubmit 2

# Récupérer le certificat émis
certreq -retrieve -config "RootCA\MonEntreprise Root CA" 2 "E:\PKI-Export\SubCA.crt"

# Éteindre à nouveau la Root CA après export
```

Étape 3 — Installer le certificat sur la Sub CA : importer le certificat signé et la chaîne de confiance.

```
 # Sur la Sub CA — Importer le certificat Root CA dans les magasins système
certutil -addstore Root "E:\PKI-Export\RootCA.crt"
certutil -addstore CA "E:\PKI-Export\RootCA.crt"

# Importer la CRL de la Root CA
certutil -addstore Root "E:\PKI-Export\MonEntreprise Root CA.crl"

# Installer le certificat de la Sub CA et démarrer le service
certutil -installcert "E:\PKI-Export\SubCA.crt"
Start-Service certsvc

# Vérifier le statut de la CA
certutil -ping
```

Comment publier les CRL et l'AIA sur un serveur web ?

La publication des CRL (Certificate Revocation Lists) et de l'AIA (Authority Information Access) sur un serveur web HTTP est critique pour que tous les clients — y compris les serveurs Linux et les appliances réseau — puissent vérifier la validité des certificats. Un client qui ne peut pas joindre le CDP refusera systématiquement le certificat, générant des erreurs TLS silencieuses difficiles à diagnostiquer.

Étape 1 — Configurer IIS sur le serveur CRL : sur le serveur web dédié (ou sur la Sub CA elle-même), créer un dossier partagé et configurer un site IIS en HTTP sur le port 80.

```
 # Créer le répertoire de publication CRL
New-Item -Path "C:\CRLShare" -ItemType Directory
New-Item -Path "C:\CRLShare\crl" -ItemType Directory
New-Item -Path "C:\CRLShare\certs" -ItemType Directory

# Installer IIS avec la console de gestion
Install-WindowsFeature Web-Server, Web-Mgmt-Console

# Créer le site web PKI (port 80, pas HTTPS — les clients vérifient la CRL via HTTP)
Import-Module WebAdministration
New-WebSite -Name "PKI" -Port 80 -HostHeader "pki.mondomaine.lan" `
  -PhysicalPath "C:\CRLShare" -Force

# Autoriser la double extension .crl.der (nécessaire pour certutil)
Set-WebConfigurationProperty -Filter system.webServer/security/requestFiltering `
  -PSPath "IIS:\Sites\PKI" -Name allowDoubleEscaping -Value true
```

Étape 2 — Configurer la publication automatique depuis la Sub CA : créer une tâche planifiée pour copier les CRL vers le serveur web toutes les 24 heures, ou utiliser un partage réseau.

```
 # Sur la Sub CA — Configurer les CDPs avec le chemin réseau ET l'URL HTTP
# CDP avec chemin UNC pour la publication automatique
Add-CACrlDistributionPoint `
  -Uri "\pki\CRLShare\crl\.crl" `
  -PublishToServer -Force

# CDP avec URL HTTP pour les clients
Add-CACrlDistributionPoint `
  -Uri "http://pki.mondomaine.lan/crl/.crl" `
  -AddToCertificateCdp -Force

# AIA — URL HTTP uniquement
Add-CAAuthorityInformationAccess `
  -Uri "http://pki.mondomaine.lan/certs/_.crt" `
  -AddToCertificateAia -Force

# Publier les CRL immédiatement
certutil -crl

# Copier les CRL vers le serveur web (si partage réseau non configuré)
Copy-Item "C:\Windows\System32\CertSrv\CertEnroll\*.crl" "\pki\CRLShare\crl"
Copy-Item "C:\Windows\System32\CertSrv\CertEnroll\*.crt" "\pki\CRLShare\certs"
```

Publication dans Active Directory et auto-enrollment

La CA émettrice doit publier son certificat et les CRL dans l'annuaire Active Directory pour que les machines du domaine puissent faire confiance aux certificats émis sans configuration manuelle. La politique de groupe (GPO) permet ensuite d'activer l'auto-enrollment, ce qui automatise complètement la délivrance des certificats aux machines du domaine.

```
 # Publier le certificat Sub CA dans l'AD (NTAuthCertificates et AIA)
certutil -dspublish -f "C:\Windows\System32\CertSrv\CertEnroll\SubCA.crt" SubCA

# Publier la CRL Root CA dans l'AD
certutil -dspublish -f "E:\PKI-Export\MonEntreprise Root CA.crl" RootCA

# Forcer la synchronisation LDAP
gpupdate /force

# Vérifier que le certificat Root CA est dans NTAuth (contrôle domaine)
certutil -viewstore -enterprise NTAuth
```

Pour activer l'**auto-enrollment via GPO**, créer ou modifier une GPO appliquée à l'OU Computers :

Ouvrir *Group Policy Management Editor* → Computer Configuration → Windows Settings → Security Settings → Public Key Policies.

Double-cliquer sur *Certificate Services Client — Auto-Enrollment*.

Sélectionner *Enabled*, cocher *Renew expired certificates* et *Update certificates that use certificate templates*.

Appliquer et attendre la prochaine mise à jour GPO ou forcer avec `gpupdate /force`.

Sécurisation de la PKI — quelles mesures appliquer dès le départ ?

Une PKI mal sécurisée est une PKI compromise. Les vulnérabilités ESC1 à ESC16 documentées par SpecterOps permettent à un attaquant disposant de droits d'enrollment de s'émettre des certificats d'administrateur de domaine. Notre article AD CS Exploitation 2026 : ESC1 à ESC16 détaille chaque technique d'attaque. Les mesures préventives à appliquer dès l'installation sont les suivantes.

Restreindre les permissions sur les templates de certificats est la priorité absolue. Par défaut, le template *Machine* autorise tout membre du groupe *Domain Computers* à s'inscrire. Vérifier systématiquement que l'attribut *CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT*

(ENROLLEE_SUPPLIES_SUBJECT) n'est pas activé sur les templates sensibles, car il permet à l'enrollee de spécifier n'importe quel SAN, y compris celui d'un administrateur.

```
 # Lister tous les templates avec ENROLLEE_SUPPLIES_SUBJECT activé (risque ESC1)
certutil -v -template | Select-String -Pattern "CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT" -Context 5,0

# Auditer les ACLs des templates via ADSI
$templates = [ADSI]"LDAP://CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configu
$templates.Children | ForEach-Object {
    $acl = $_.ObjectSecurity.Access
    $acl | Where-Object { $_.ActiveDirectoryRights -match "ExtendedRight" } |
    Select-Object IdentityReference, ActiveDirectoryRights, AccessControlType |
    Format-Table -AutoSize
}
```

> En mission d'audit Active Directory (client grand compte, 2 000 postes, secteur industrie), la Root CA était une VM Hyper-V restée allumée depuis 8 ans, exposée sur le réseau interne sans restriction de flux. Trois templates configurés avec ENROLLEE_SUPPLIES_SUBJECT et enrollment ouvert à tous les utilisateurs du domaine permettaient une élévation de privilèges complète en moins de 5 minutes via Certify.exe. La migration vers une Root CA offline avec un nouveau serveur physique dédié, combinée à l'audit et la restriction de tous les templates, a réduit la surface d'attaque PKI à zéro vulnérabilité critique.
>
> *— Retour de mission PKI, juin 2026*

Consulter également notre guide complet AD CS : attaque et défense pour un inventaire des vecteurs d'exploitation courants et les contre-mesures associées, ainsi que notre guide Tiering Model Active Directory pour intégrer la PKI dans une architecture à niveaux.

Validation et tests de la PKI déployée

Après déploiement, une série de vérifications permet de confirmer que la chaîne de confiance est correcte, que les CRL sont accessibles, et qu'aucun template n'est mal configuré.

```
 # Vérifier la chaîne de confiance complète
certutil -verify -urlfetch "C:\Windows\System32\CertSrv\CertEnroll\SubCA.crt"
# Résultat attendu : "Certificate is valid" avec toutes les URLs CDP et AIA résolues

# Tester l'accès HTTP à la CRL depuis un poste client
$url = "http://pki.mondomaine.lan/crl/MonEntreprise Issuing CA.crl"
Invoke-WebRequest -Uri $url -UseBasicParsing | Select-Object StatusCode
# Résultat attendu : StatusCode 200

# Vérifier que le Root CA est dans le magasin Trusted Root de l'AD
certutil -viewstore -enterprise Root

# Tester l'auto-enrollment sur un poste du domaine
certutil -user -ping
certreq -enroll -user User
```

La commande `certutil -verify -urlfetch` est particulièrement utile car elle effectue une vérification complète : elle résout les URLs CDP et AIA déclarées dans le certificat, télécharge les CRL, et valide la signature de chaque niveau de la chaîne. Toute URL non résolue apparaît explicitement dans la sortie.

Pour un guide complémentaire sur la sécurisation de l'ensemble de l'infrastructure Active Directory, consultez notre Guide de Sécurisation Active Directory Windows Server 2025. La PKI doit être intégrée dans la stratégie globale de défense en profondeur du domaine.

Renouvellement et maintenance opérationnelle

La maintenance d'une PKI d'entreprise se résume à trois opérations récurrentes : le renouvellement des CRL (automatique si bien configuré), le renouvellement du certificat de la CA émettrice (tous les 5 à 8 ans en pratique, avant expiration), et le renouvellement de la Root CA (tous les 15 à 18 ans). Programmer une alerte calendrier pour 6 mois avant l'expiration de chaque certificat CA.

```
 # Vérifier la date d'expiration du certificat Sub CA
certutil -CA.cert "C:\SubCA.crt" | Select-String "NotAfter"

# Configurer la durée de validité des certificats endpoint émis
# (à faire sur la Sub CA avant d'émettre les premiers certs)
certutil -setreg CA\ValidityPeriod "Years"
certutil -setreg CA\ValidityPeriodUnits 2
Restart-Service certsvc

# Configurer la durée de publication CRL (ici 7 jours)
certutil -setreg CA\CRLPeriodUnits 7
certutil -setreg CA\CRLPeriod "Days"

# CRL delta (pour les révocations rapides) : 1 jour
certutil -setreg CA\CRLDeltaPeriodUnits 1
certutil -setreg CA\CRLDeltaPeriod "Days"
Restart-Service certsvc
```

La documentation Microsoft sur AD CS fournit les paramètres de référence pour chaque registre de configuration. Il est recommandé d'exporter régulièrement la configuration de la CA via `certutil -backup` et de stocker cette sauvegarde hors ligne, séparément du serveur Root CA.

Questions fréquentes

Peut-on déployer AD CS sur le même serveur que le contrôleur de domaine ?

Microsoft déconseille fortement de colocater la CA émettrice sur un contrôleur de domaine. La compromission du serveur CA donnerait accès à l'annuaire, et inversement. En pratique, dédier un serveur membre du domaine (pas DC) à la Sub CA est la règle minimale. La Root CA, elle, ne doit jamais rejoindre le domaine ni être connectée au réseau.

Quelle différence entre CDP et AIA ?

Le CDP (CRL Distribution Point) indique où télécharger la liste des certificats révoqués : si un client ne peut atteindre le CDP, il refusera le certificat (comportement fail-closed selon la politique). L'AIA (Authority Information Access) indique où trouver le certificat de la CA émettrice pour construire la chaîne de confiance. Les deux doivent être publiés en HTTP accessible par tous les clients, y compris les équipements réseau et serveurs Linux.

Comment révoquer un certificat compromis en urgence ?

Sur la Sub CA, ouvrir la console certsrv.msc, naviguer vers Issued Certificates, clic droit sur le certificat → Revoke Certificate, choisir le motif (Key Compromise), puis publier une CRL delta immédiatement via `certutil -crl`. La CRL delta propage la révocation en quelques minutes sans attendre le renouvellement de la CRL complète. Les clients qui ont mis en cache l'ancienne CRL complète liront la delta à la prochaine vérification.

AD CS est-il compatible avec les clients Linux et macOS ?

Oui, à condition que les CRL soient publiées en HTTP (et non uniquement en LDAP). Les clients Linux font confiance au certificat Root CA si celui-ci est importé dans le magasin système (`update-ca-certificates` sur Debian/Ubuntu). Pour la délivrance automatique de certificats vers des serveurs Linux, utiliser le protocole SCEP ou des scripts `certreq` / `openssl`. Notre article AD CS : générer un certificat TLS pour un serveur Linux détaille ce processus complet.

Combien de temps garder les logs de la CA en production ?

La réglementation française (NIS 2, RGPD) et les recommandations ANSSI préconisent une conservation minimale de 12 mois pour les logs d'émission et de révocation de certificats. En pratique, conserver les logs de la base de données AD CS (fichier .edb) pendant 5 ans pour les audits de sécurité. Les logs Windows Event (journal Application, source CertificationAuthority) doivent être centralisés dans un SIEM avec une rétention de 90 jours minimum en ligne.

Templates de certificats — configuration et restrictions recommandées

Les templates de certificats AD CS définissent les propriétés des certificats émis : usage (authentification client, serveur TLS, signature de code), durée de validité, longueur de clé et, surtout, qui peut demander un certificat. La mauvaise configuration des templates est à l'origine de la quasi-totalité des vulnérabilités ESC dans les audits AD CS. Voici les paramètres critiques à vérifier et configurer sur chaque template.

Le paramètre le plus dangereux est **CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT**. Activé, il permet à l'enrollee de spécifier n'importe quel Subject Alternative Name dans sa demande, ce qui lui permet de demander un certificat au nom de n'importe quel utilisateur du domaine, y compris un administrateur. Ce flag ne doit être activé que sur les templates qui l'exigent fonctionnellement, et uniquement pour des groupes restreints.

```
 # Créer un template personnalisé pour les serveurs web internes
# Dupliquer le template WebServer existant
$template = Get-CATemplate -Name "WebServer"

# Via l'interface graphique certtmpl.msc :
# 1. Dupliquer WebServer -> "WebServer-Interne"
# 2. Onglet General : Validity Period = 1 year, Renewal Period = 2 weeks
# 3. Onglet Subject Name : "Supplied in the request" UNIQUEMENT si nécessaire
#    Sinon : "Built from Active Directory information"
# 4. Onglet Security : retirer "Domain Users" de l'enrollment,
#    ajouter un groupe dédié "PKI-WebServers-Enrollment"
# 5. Onglet Extensions : Application Policies = Server Authentication seulement
# 6. Onglet Issuance Requirements : "CA certificate manager approval" pour les certs sensibles

# Publier le template sur la CA
Add-CATemplate -Name "WebServer-Interne"

# Vérifier les templates publiés et leurs ACLs
certutil -catemplates
```

Pour les certificats de contrôleurs de domaine (template *Domain Controller Authentication* ou *Kerberos Authentication*), activer l'auto-enrollment uniquement pour le groupe *Domain Controllers*. Ces templates permettent l'authentification Kerberos et LDAPS ; leur

compromission permettrait l'émission de certificats de DC frauduleux exploitables pour des attaques Golden Certificate.

Monitoring de la PKI — quels indicateurs surveiller ?

Une PKI d'entreprise doit être supervisée en continu. Les événements critiques à monitorer dans le journal Windows Application (source *CertificationAuthority*) incluent : les émissions de certificats (Event ID 4886), les révocations (4890), les demandes refusées (4889) et les modifications de configuration de la CA (4892). Un SIEM doit alerter sur toute émission de certificat hors template habituel ou vers des comptes à privilèges.

```
 # Extraire les 50 derniers certificats émis avec leur template et sujet
$caName = "MonEntreprise Issuing CA"
$certDB = New-Object -ComObject CertificateAuthority.View
$certDB.OpenConnection($caName)
$certDB.SetResultColumnCount(4)
$certDB.SetResultColumn($certDB.GetColumnIndex($false, "Request.RequesterName"))
$certDB.SetResultColumn($certDB.GetColumnIndex($false, "CertificateTemplate"))
$certDB.SetResultColumn($certDB.GetColumnIndex($false, "NotAfter"))
$certDB.SetResultColumn($certDB.GetColumnIndex($false, "SerialNumber"))

# Surveiller via PowerShell les événements d'émission (Event ID 4886)
Get-WinEvent -LogName Security -FilterXPath "*[System[EventID=4886]]" -MaxEvents 20 |
  Select-Object TimeCreated, Message | Format-List
```

Intégrer ces alertes dans votre SIEM (Microsoft Sentinel, Wazuh, ou Splunk) avec une règle de corrélation détectant l'émission de certificats pour des comptes d'administration ou des templates non approuvés. La surveillance proactive de la PKI est l'un des contrôles les plus efficaces contre les attaques de type Golden Certificate ou Shadow Credentials.