Online Responder (CA)

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

Prečo OCSP

CRL list je stále väčší a väčší

Synchronizácia a sťanutie CRL a delta CRL je periodické

Ak klient nevie stiahnúť CRL, nevie overiť pravosť certifikátu

OCSP

Online Certificate Status Protocol

- Dostupny od server 2008
- CRL obsahuje SN cert ktoré boli revocate a delta CRL zasa len rozdielove SN cert od posledného publikovania CRL
- Publikovanie CRL robí CA
- Defaultne je publikácia vykonávaná 1 za týždeň a delta CRL 1 za deň
- Pre zistenie satusu musí client stiahnut CRL I delta CRL
- Toto stahovanie generuje nie malý traffic

Výhody

OCSP je check certifikát statusu cez HTTP na OCSP responder a klient tak nemusí sťahovať CRL ale dostane odpoved čí je alebo nie je cert platný (OCSP responder porovnáva CRL listy s daným certifikátom)

OCSP

Jedna z podrolí AD CA

Client sa obracia na responder ak chce zistiť status certifikátu

Jednoznačným identifikátorom je seriálové číslo certifikátu

Komponenty:

- OCSP klient
- Online OCSP responder
- Web proxy cache

Online responder vie fungovať so STANDALONE alebo ENTERIPRISE CA

Online responder

Ako to funguje ?

Klient request ohladom statusu certifikátu.

1. Online responder skontroluje svoju cache
   - Ak áno, odpovie klientovi
2. Zistí, či má kópiu CRL vydanú CA lokálne uloženú
   - Ak áno, odpovie klientovi
3. Stiahne CRL list z CDP lokácie

Odpovede online responder sú tiež digitálne podpísané

OCSP Requirements

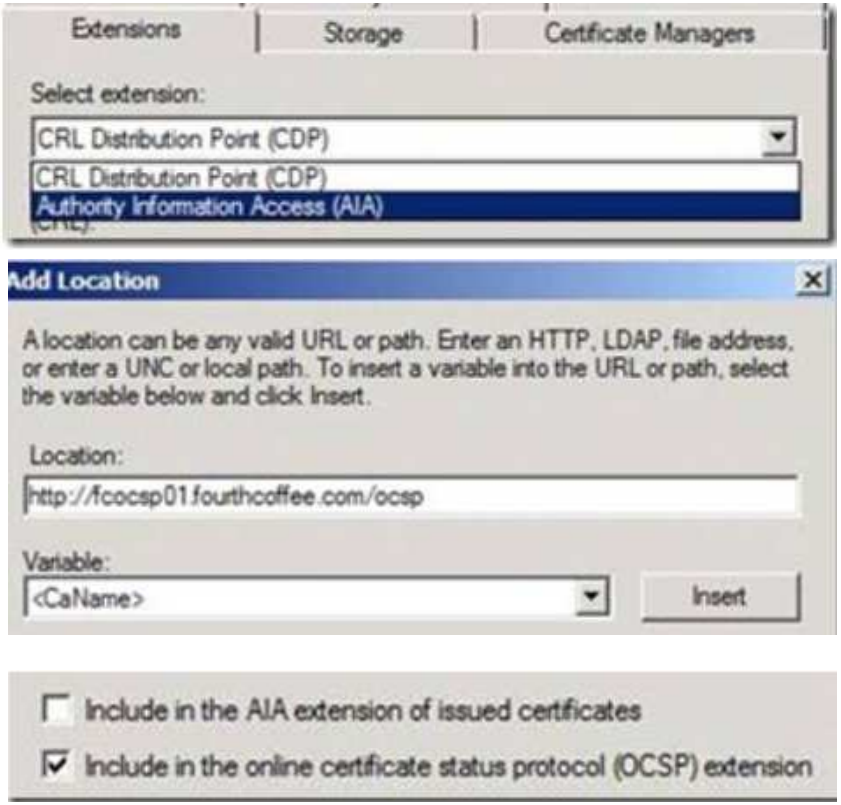
- ✓Server, ktorý bude hosťovať OCSP nemusí byť členom domény
- ✓idálne je aby nebol na tom istom systéme ako CA)
- ✓ AD DS nainštalovaná v prostredí
- ✓Konfigurácia podporujúca OCSP response

ENT CA konfigurácia

CA musí byť nakonfigurovaná na podporu OCSP

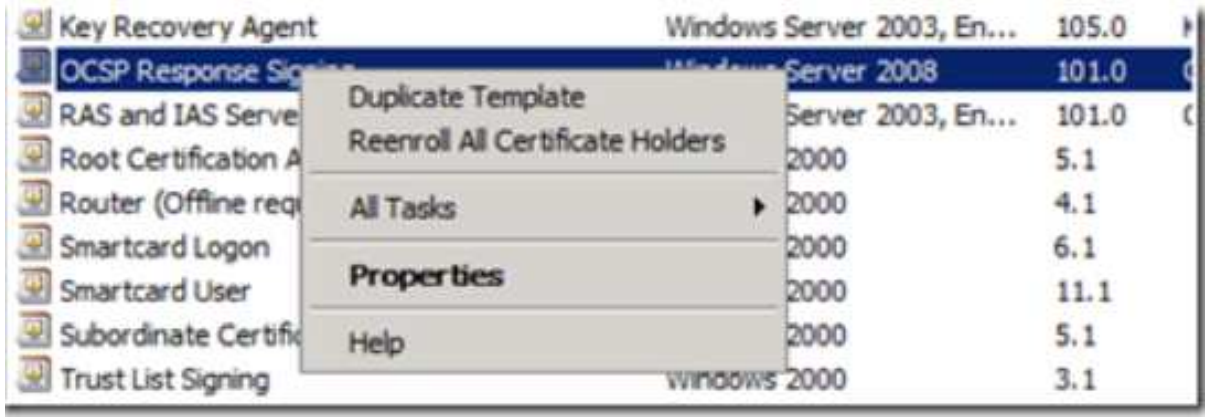
AIA záznam musí obsahovať lokáciu OCSP respondera

http://<fqdn of the ocsp responder>/ocsp



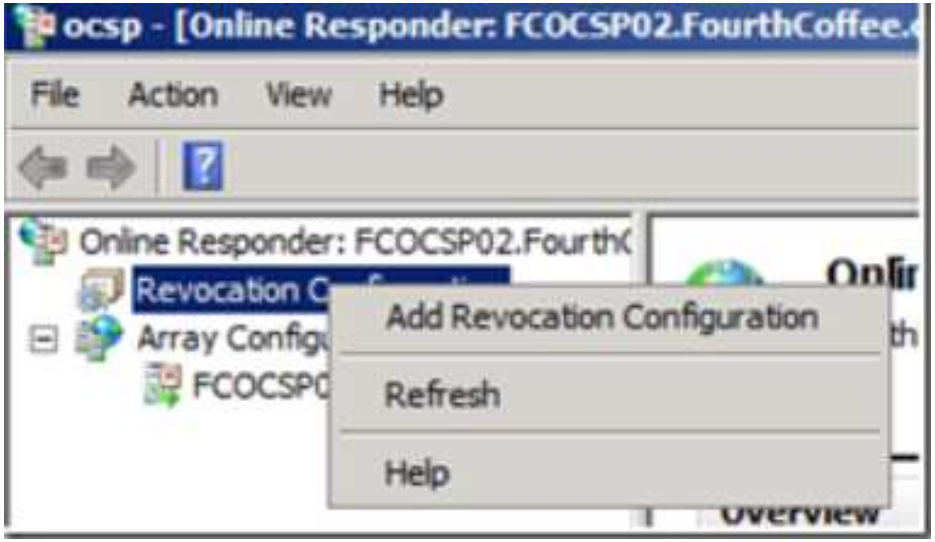
ENT CA konfigurácia

Pripravenie template pre OCSP



OCSP konfigurácia

Vytvorenie Revocation konfigurácie



OCSP klient konfigurácia

Presmerovanie klientov na OCSP responder

Toto nastavenie je možné urobiť pomocou GPO

OCSP HA

OCSP responder môže byť konfigurovaný ako vysoko dostupná služba v rámci NLB

Deje sa to usporiadaním OCSP responderov do poľa

Toto pole neposkytuje FT funktionalitu

Pole umožňuje spraovať viacero OCSP responderov

Jeden OCSP responder v poli bude nastavený ako Array controller

Next

Inštalácia Online respondera na ENT CA (SRV3)