Algebra
visoka škola za
primijenjeno računarstvo

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo | Ilica 242 | 10000 Zagreb | Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 | matični broj: 2412926 | IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 | fax. +385 (0)1 2305 004 | info@racunarstvo.hr | www.racunarstvo.hr

KATEDRA ZA OPERACIJSKE SUSTAVE

Planiranje mrežne infrastrukture

Lab 07 – AD RMS

REV 2.0

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Sadržaj

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Uvod

U današnjoj vježbi ćete upoznati *Active Directory Rights Management Services* – **AD RMS**. AD RMS je uloga koju se instalira na Windows Server kada želimo napraviti kvalitetno rješenje za nadzor ovlasti nad operacijama koje korisnici rade nad datotekama. AD RMS nema funkcionalnosti kao BitLocker (enkripcija diska), niti kao EFS (enkripcija pojedinačnih datoteka), niti mu je to namjena. Ideja AD RMS-a je da se podaci zaštite "u prijenosu", i da budu dostupni samo autoriziranim korisnicima. AD RMS je tehnologija za zaštitu privatnosti podataka koja je namijenjena sprječavanju *curenja podataka* iz tvrtke prema drugim tvrtkama ili osobama, korištenjem metoda simetrične enkripcije (PKI infrastruktura). Također, može se integrirati sa Windows Serverom, Microsoft Exchange Serverom, Sharepoint Serverom, i aplikacijama iz skupa Microsoft Office.

Infrastruktura koju ovdje realizirate dobro bi vas služila i u produkcijskom okruženju (s par izmjena koje su naglašene u nastavku). Opišimo ju:

- **SERVERDC (10.10.10.1)**: domenski kontroler domene racunarstvo.edu. Potrebno je napraviti pripremu na DC-u prije nego što krenemo dalje sa instalacijom AD RMS uloge.
- **CLI1 (10.10.10.41)**: računalo učlanjeno u domenu racunarstvo.edu, na koje se logiramo kroz Horizon Client.
- **SERVER1 (10.10.10.2)**: računal• s Windows 2012 R2 operacijskim sustavom. Upotrijebiti ćemo ga kao centralni AD RMS server.

Pošto bi potpuna implementacija AD RMS-a zahtijevala nekoliko dana rada i temeljitu pripremu, na vježbi ćemo se fokusirati na ono što je unutar vježbi ostvarivo - pripremu domenskog kontrolera, AD RMS servera i izradu politike. To će nam kao vježba biti sasvim dovoljno da "zagrebemo" u kompleksnost AD RMS-a kojeg možda nećemo često pronaći u praksi u Hrvatskoj, ali ćemo ga svakako pronaći (ili neko slično rješenje) u velikim tvrtkama, poglavito izvan granica RH.

Današnja vježba se sastoji od 3 faze:

1. Priprema domenskog kontrolera
2. Priprema AD RMS servera (SERVER1)
3. Konfiguracija AD RMS template-a

Ovime završava današnji uvod i možemo krenuti na samu vježbu.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Prije vježbe

1. Prijavite se na Horizon sustav sa svojim korisničkim imenom i lozinkom**.**
2. Na CLI1 virtualnoj mašini, dodijelite na prvu mrežnu karticu (onu koja je u 10.10.10 subnetu) DNS adresu 10.10.10.1 i napravite reboot klijenta. Nakon toga, pričekajte 4-5 minuta da se računalo restarta i u PowerShell prozoru napišite komandu *Test-ComputerSecureChannel*. Trebali biste dobiti vrijednost True.
3. Korištenjem Remote Desktop Connection-a, ulogirajte se na SERVERDC (10.10.10.1).
4. Kasnije se, po potrebi, Remote Desktop Connection-om ulogirajte na SERVER1 (10.10.10.2). Prvu konekciju napravite kao localhost\Administrator sa passwordom Pa$$w0rd, podesite DNS IP na 10.10.10.1 i napravite restart. Za 3-4 minute se možete ulogirati kao racunarstvo\EntAdmin sa passwordom Pa$$w0rd.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Priprema okoline za instalaciju i konfiguraciju AD RMS

Konfiguracija DNS-a i AD RMS service accounta

1. Ulogirajte se u DC sa racunarstvo\EntAdmin accountom i passwordom Pa$$w0rd.

2. Korištenjem Active Directory Administrative Centera (ili Active Directory Users and Computers), kreirajte OU imena Service accounts u racunarstvo.edu domeni.

3. Kreirajte novi korisnički account u Service Accounts OU sa ovim postavkama:

- First name: ADRMSSVC
- User UPN logon: ADRMSSVC
- Password: Pa$$w0rd
- Confirm Password: Pa$$w0rd
- Password never expires: Enabled
- User cannot change password: Enabled

4. Kreirajte novu Global security grupu u Users containeru imena ADRMS_SuperUsers. Podesite e-mail adresu grupe na ADRMS_SuperUsers@racunarstvo.edu. Otvorite postavke ADRMSSVC korisnika (obavezno uključite Advanced Features u ADU&C) i postavite mail adresu korisniku ADRMSSVC na adrmssvc@racunarstvo.edu. Također, koristnika ADRMSSVC dodajte u grupu ADRMS_SuperUsers.

5. Kreirajte novu Global security grupu u Users containeru imena Executives. Podesite e-mail adresu grupe na executives@racunarstvo.edu.

6. Napravite nove korisničke accounte vua1.profesor i vua2.profesor sa passwordom Pa$$w0rd i dodajte ih u Executives grupu.

7. Korištenjem DNS Manager console napravite host (A) resource record u zoni racunarstvo.edu zone sa slijedećim postavkama:

- Name: adrms
- IP Address: 10.10.10.2

Instalacija i konfiguracija AD RMS server uloge

Korištenjem Remote Desktop Connection-a, nakon procedure opisane u uvodu vježbe povežite se na SERVER1 (10.10.10.2) sa Racunarstvo\EntAdmin accountom i passwordom Pa$$w0rd.

2. Korištenjem Add Roles and Features Wizard dodajte Active Directory Rights Management Services ulogu to SERVER1 sa slijedećim postavkama:

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

- Role services: Active Directory Rights Management Services i sve default opcije

3. Instalacija će potrajati nekoliko minuta. Nakon toga, kroz AD RMS node u Server Manageru, kliknite na "More" za post-deployment konfiguraciju AD RMS-a.

4. U AD RMS Configuration Wizardu, upišite slijedeće informacije:

- Create a new AD RMS root cluster
- Use Windows Internal Database on this server
- Service account: Racunarstvo\ADRMSSVC
- Cryptographic Mode: Cryptographic Mode 2
- Cluster Key Storage: Use AD RMS centrally managed key storage
- Cluster Key Password: Pa$$w0rd
- Cluster Web Site: Default Web Site
- Connection Type: Use an unencrypted connection
- Fully Qualified Domain Name: http://adrms.racunarstvo.edu
- Port: 80
- Licensor Certificate: SERVER1
- Register AD RMS Service Connection Point: Register the SCP Now

Nakon popunjenog wizarda, kreće konfiguracija AD RMS-a, koja će potrajati oko 5 minuta.

5. Korištenjem Internet Information Services (IIS) Manager konzole uključite Anonymous Authentication na Default Web Site_wmcs i Default Web Site_wmcs\licensing virtualnim direktorijima.

6. Odlogirajte se iz SERVER1.

Napomena: Obavezno se morate odlogirati prije nego što počnete raditi management AD RMS-a. Naravno, u produkcijskim okolinama sigurno ne bismo koristili port 80 već 443 sa pripadajućim certifikatom.

Konfiguracija AD RMS Super Users grupe

1. Korištenjem Remote Desktop Connection-a, povežite se ponovo na SERVER1 (10.10.10.2) sa Racunarstvo\EntAdmin accountom i passwordom Pa$$w0rd.

2. Otvorite Active Directory Rights Management Services konzolu (Windows tipka Active Directory ...)

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

3. IZ AD RMS konzole, uključite Super Users (Security Policies, Super Users).

4. Postavite ADRMS_SuperUsers@racunarstvo.edu kao Super Users grupu (Klik na Super Users, klik na "Change super user group").

Konfiguracija AD RMS Template-a

1. Na SERVER1 virtualnoj mašini, iskoristite Rights Policy Template node u AD RMS konzoli za izradu Distributed Rights Policy Template-a sa slijedećim postavkama:

- Language: English (United States) o Name: ReadOnly
- Description: Read only access. No copy or print
- Users and rights: executives@racunarstvo.edu
- Rights for Anyone: View
- Grant owner (author) full control right with no expiration
- Content Expiration: 7 days
- Use license expiration: 7 days
- Require a new use license: every time content is consumed (disable client-side caching)

Konfiguracija AD RMS Template distribucije

1. Na SERVER1 virtualnoj mašini, otvorite Windows PowerShell prompt, i onda natipkajte slijedeće komande:

New-Item c:\rmstemplates -ItemType Directory

New-SmbShare -Name RMSTEMPLATES -Path c:\rmstemplates -FullAccess RACUNARSTVO\ADRMSSVC - ako ova komanda "pukne", napravite share imena RMSTEMPLATES nad direktorijem c:\rmstemplates, sa full pravima za ADRMSSVC korisnika kroz GUI

New-Item c:\docshare -ItemType Directory

New-SmbShare -Name docshare -Path c:\docshare -FullAccess Everyone

2. U Active Directory Rights Management Services konzoli, podesite lokaciju za Rights Policy Templates na \\SERVER1\RMSTEMPLATES.

3. U File Explorer-u, izlistajte sadržaj c:\rmstemplates foldera. Provjerite da postoji template ReadOnly.xml.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Konfiguracija exclusion policy-ja

1. U Active Directory Rights Management Services konzoli, uključite Application exclusion (Exclusion Policies, applications, Enable).

2. U Exclude Application dialog box, upišite slijedeće informacije:

- Application File name: Powerpnt.exe
- Minimum version: 14.0.0.0
- Maximum version: 16.0.0.0

Korištenje AD RMS-a kroz kompatibilnu aplikaciju

U slijedećem koraku, vratite se na CLI1 virtualnu mašinu, pokrenite Internet Explorer i sa URL-a:

http://bit.ly/2giCZIK

skinite instalaciju Foxit-a (budite strpljivi, Foxit web je jako spor), te skinutu aplikaciju instalirajte na CLI1 virtualku. Foxit instalirajte sa svim opcijama "na disku", te ga podesite da bude default system printer.

Nakon toga, treba instalirati dodatni plug-in, sa slijedećeg URL-a:

http://bit.ly/2fGUejl

Prebacite PDF od vježbe na vašu CLI1 virtualnu mašinu (copy-paste u Horizon Client). Otvorite datoteku u Foxit Reader. Kliknite na "Protect" tab, pa na "restrict access", pa na "Connect to digital rights management servers and get templates" i odgovorite sa "yes" na slijedeće pitanje kako biste skinuli zadnju verziju IRM clienta (continue free trial opcija). Slijedite instalaciju AD RMS klijenta (next-next, bez MS updatea). Nakon instalacije klijenta, napravite logoff sa CLI1 i iz Horizona, pričekajte jednu minutu te se ulogirajte natrag.

Nakon ponovnog logiranja, otvorite PDF sa vježbom, kliknite na "Protect" tab i onda na "restrict access", te na istu opciju kao maločas. Pitati će vas za korisničko ime i password. Upišite adrmssvc@racunarstvo.edu i password Pa$$w0rd. Nakon toga, primjetiti ćete da se u "Restric access" meniju nalazi AD RMS politika koju smo napravili u jednom od prethodnih koraka, imena ReadOnly. Kliknite na ReadOnly, pustite AD RMS da odradi svoj posao, i nakon toga će vam se pojaviti poruka da je dokument AD RMS-protected i "žuta žaruljica" u gornjem desnom kutu.

Time završava današnja vježba.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Rezultat vježbe

Rezultat današnje vježbe su izmjene virtualnih računala kako slijedi:

SERVERDC:

- Napravljena priprema za AD RMS instalaciju

SERVER1:

- Napravljena instalacija AD RMS uloge

CLI1:

- Instalacija Foxit Readera, potrebnog dodatnog plug-ina i RMS klijenta
- Isprobana je integracija Foxit-a i AD RMS-a.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Što treba znati nakon ove vježbe?

1. Nabrojati faze *deploymenta* AD RMS-a
2. Objasniti kako se izrađuje AD RMS template
3. Objasniti kako se izrađuje exclusion policy
4. Objasniti kako se radi RMS template distribucija

Dodatna literatura

- Technet dokumentacija i *tutorial* za AD RMS ulogu:

https://technet.microsoft.com/en-us/library/hh831364(v=ws.11).aspx

- Technet dokumentacija za AD RMS sa AD FS-om:

https://technet.microsoft.com/en-us/library/dn758110(v=ws.11).aspx

- AD RMS Prerequisites

https://technet.microsoft.com/en-us/library/dd772659(v=ws.10).aspx

- AD RMS Best Practices Guide

https://technet.microsoft.com/en-us/library/jj735304(v=ws.11).aspx