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 05 – Dinamičke dozvole pristupa

REV 2.0

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

Sadržaj

Uvod 2
Prije vježbe ..... **Error! Bookmark not defined.**
Priprema infrastrukture 5
Konfiguracija dinamičkih dozvola pristupa 7
Postavljanje tvrdnje 7
Povjerljivost datoteka 8
Kontrola pristupa 12
Uključenje dinamičkih dozvola pristupa 16
Provjera funkcionalnosti 17
Pomoć pri odbijenom pristupu 20
Samostalna vježba 22
Rezultat vježbe 23
Što treba znati nakon ove vježbe? 24
Dodatna literatura 24

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

Uvod

U današnjoj vježbi ćemo upoznati dinamičke dozvole pristupa – **DAC** (engl. *Dynamic access control*). Dinamičke dozvole su novi način određivanja razine pristupa koji, naspram klasičnih NTFS dozvola, donosi veću fleksibilnost i poboljšanu funkcionalnost. Podsjetimo se, NTFS dozvole su bazirane na SID-ovima (engl. *Security identifier*) i grupama od 6 glavnih dozvola. SID-ovi su numerički identifikatori jedinstveni za korisnika i/ili grupu. NTFS dozvole pristupa imaju nekoliko ograničenja koje u modernom korporativnom informacijskom sustavu dolaze sve više do izražaja. Nabrojimo neke:

- **Podrška iz aplikacija**: NTFS dozvole pristupa nije moguće koristiti unutar aplikacija (engl. *Application aware*). Primjerice, nije moguće dopustiti korisniku da pročita sadržaj Word datoteke ali mu zabraniti da ga kopira u drugu datoteku ili ju ispiše.
- **Višestruki kriteriji**: NTFS dozvole su krajnje rudimentarne pri određivanju pristupnih prava a možda najveće ograničenje je što nije moguće definirati višestruke uvjete. Zamislite situaciju u kojoj želite dozvoliti pristup nekom resursu samo korisnicima koji su članovi dvije točno određene grupe. NTFS ne podržava logičku AND operaciju s kojom bi prilično jednostavno definirali takav kriterij.
- **Baziranje na SID-ovima**: kao identifikator korisnika se koristi isključivo SID. Ipak, Active Directory za objekt *User* ima brojne atribute koje ne možemo koristiti sa NTFS dozvolama. Primjerice, ne možemo definirati dozvolu pristupa nekom resursu koja bi dopustila pristup korisnicima čiji je voditelj (engl. *Manager*) Marko Tomić.

Gore navedena ograničenja su već duže vremena poznata i može ih se djelomično anulirati na nekoliko načina. Vjerojatno najčešća praksa je izrada novih grupa za svaku gore opisanu situaciju a zatim dodjeljujemo dozvole novo stvorenim grupama nad željenim resursom. Ipak, velika količina grupa otežava administraciju. Primjerice, novo izrađenog korisnika morate ručno učlaniti u svaku grupu kako bi mu osigurali pristup nužnim resursima.

Ovdje na scenu stupa mehanizam dinamičkih dozvola pristupa koji je predstavljen sa Windows Server 2012 operacijskim sustavom. Osnovni preduvjet za dinamičke dozvole pristupa je minimalno jedan domenski kontroler u organizaciji s Windows Server 2012 operacijskim sustavom. Također, sam poslužitelj na kojem se nalaze datoteke na kojima se postavljaju dinamičke dozvole pristupa mora biti Windows Server 2012 te mu, naravno, mora biti omogućena komunikacija sa domenskim kontrolerom iste verzije operacijskog sustava. Od ostalih preduvjeta navedimo kako je potrebno instalirati **File Server Resource Management** konzolu (ulogu) te da je potrebno u *Default Domain Controller Policyju* uključiti podršku za dinamičke dozvole. Podrška omogućuje prevođenje autorizacijskih podataka iz *ticketa* verzije Kerberos 5, prevođenje *ticketa* u token te usporedbu podataka iz tokena s višestrukim kriterijima dinamičke dozvole.

Dinamičke dozvole pristupa djeluju u sprezi s postojećim NTFS i/ili Share dozvolama a moguće ih je integrirati i sa drugim servisima. Primjerice, često se integriraju sa sustavom za upravljanje pravima – **RMS** (engl. *Rights Management Service*) kako bi datoteka ostala zaštićena čak i kada napusti Windows Server okruženje. Nabrojimo scenarije u kojima se koriste dinamičke dozvole:

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

- **Nadzor pristupa podacima**: kao i klasične NTFS dozvole, dinamičke dozvole omogućuju nadgledanje pristupa podacima kako bi se, po potrebi, izvršila forenzička analiza u slučaju zloupotrebe.
- **Zaštita povjerljivih podataka**: najveća vrijednost dinamičkih dozvola je što kao kriterij pristupa mogu uzeti u obzir povjerljivost datoteke (engl. *File Confidentiality*). Naravno, mi sami moramo definirati što točno čini datoteku povjerljivom (izraz/fraza u datoteci, kriterij na osnovu regularnog izraza i sl.). Povjerljivost se definira putem File Server Resource Manager konzole.
- **Pomoć pri odbijenom pristupu**: česta greška koju korisnici vide je *Access Denied*. Kod NTFS dozvola korisnik može samo kliknuti gumb OK i zatim nekom metodom (e-pošta, sustav helpdeska i sl.) tražiti pomoć od administratora. Dinamičke dozvole integriraju sustav pomoći koji korisniku omogućuje da odmah zatraži pomoć te navede razlog zašto mu je potreban pristup povjerljivim podacima. Administrator može, naravno, odbiti zahtjev ako procijeni da je neopravdan.

Dinamičke dozvole pristupa su složen sustav čija inicijalna konfiguracija nije trivijalna. Najvažnija komponenta koju morate konfigurirati je **tvrdnja** (engl. *Claim*). Pojam tvrdnje smo neposredno već upoznali. Tvrdnja je informacija koja opisuje svojstvo nekog objekta a koja dolazi iz pouzdanog izvora. Primjerice, kod NAP mehanizma u kolegiju OSMIS smo tvrdili da je računalo zdravo jer je uključen Windows Firewall a na osnovu te tvrdnje je računalu odobren udaljeni pristup putem VPN-a. Kod dinamičkih dozvola pristupa tvrdnja je informacija o objektu Active Directoryja. Definiranjem tvrdnje govorite dinamičkoj dozvoli pristupa koji atribut objekta treba provjeriti kako bi odobrili pristup. Tvrdnje se mogu definirati za korisnika i računalo. Primjer tvrdnje za korisnika je da pripada odjelu Uprave a za računalo da mu je operacijski sustav Windows 8.1 Enterprise. Za korištenje dinamičkih dozvola pristupa nužno je definirati barem jednu tvrdnju. Opišimo infrastrukturu koju želimo postići:

- **SERVERDC**: domenski kontroler domene racunarstvo.edu. Na njemu danas odrađujemo cijelu vježbu. Dopunit ćemo atributa objektu korisnik, uključiti podršku za dinamičke dozvole pristupa te konfigurirati mapu sa dijeljenim podacima na kojima ćemo demonstrirati dinamičke dozvole. Velik dio vježbe provest ćemo u konzoli Active Directory Administrative Center s kojom se do sada nismo koristili. Sama konzola je prilično jednostavna za korištenje a omogućuje prečace do brzih radnji nad korisnicima (primjerice, resetiranje lozinke, pretragu i sl.), konfiguriranje dinamičkih dozvola pristupa, podizanje funkcionalnih razina šume i domene, uključenje Active Directory Recycle Bina i drugo.
- **SERVER1**: poslužitelj član domene racunarstvo.edu na kojem ćemo provjeriti funkcionalnost infrastrukture. Ovome je serveru (namjerno) broken secure channel sa domenom. Da biste mogli uspješno napraviti vježbu, pronađite razlog *zašto* je secure channel broken (HINT: nedostaje jedan ključan parametar u konfiguraciji SERVER1 virtualne mašine da bi sve radilo). Pri istraživanju pogreške, ulogirajte se Remote Desktopom na SERVER1 sa korisničkim imenom localhost\Administrator i standardnom lozinkom.
- **CLI1**: klijentsko računalo u domeni racunarstvo.edu na kojem ćemo provjeriti funkcionalnost infrastrukture.

Ovime završava današnji uvod i možemo početi s vježbom.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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. Kliknite mišem na PMI pool i ulogirajte se sa standardnim korisničkim imenom i lozinkom.
3. Do DC mašine (10.10.10.1) i SERVER1 mašine (10.10.10.2) možete doći korištenjem Remote Desktop Connectiona.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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 infrastrukture

U prvom dijelu vježbe ćemo pripremiti infrastrukturu. Prvo ćemo instalirat ćemo potrebnu ulogu kako bi kasnije definirali povjerljivost datoteke:

1. Prijavite se na računalo **SERVERDC** kao korisnik **RACUNARSTVO\DomAdmin** s lozinkom **Pa$$w0rd**
1. Prikažite ekran **Start** i kliknite na stavku **Server Manager**.
1. Prikazuje se **Server Manager** konzola. Kliknite na izbornik **Manage-> Add Roles and Features**.
2. Prikazuje se ekran **Before you begin**. Kliknite gumb **Next**.
3. Prikazuje se ekran **Select installation type**. Ostavite predefinirane postavke i kliknite gumb **Next.**
4. Prikazuje se ekran **Select destination server**. Ostavite predefinirane postavke i kliknite gumb **Next.**
5. Prikazuje se ekran **Select server roles**. Proširite stavku **File and Storage Services-> File and iSCSI Services**. Označite stavku **File Server Resource Manager**.
6. Prikazuje se prozor **Add Roles and Features Wizard** s informacijom o potrebnim dodatnim komponentama. Kliknite gumb **Add Features**.
7. Vraćate se na ekran **Select server roles**. Kliknite gumb **Next**.
8. Prikazuje se ekran **Select features**. Kliknite gumb **Next**.
9. Prikazuje se ekran sa sažetkom konfiguracije. Kliknite gumb **Install**.
10. Pričekajte završetak instalacije i kliknite gumb **Close**.
11. Zatvorite konzolu **Server Manager**.

Nakon instalacije uloga pripremit ćemo objekte u AD-u. Moramo postaviti oznake odjela i izraditi grupu računala:

1. Prikažite ekran **Start** i kliknite na **Active Directory Users and Computers**.
2. Prikazuje se konzola **Active Directory Users and Computers**. Unutar lijevog okna proširite domenu **racunarstvo.edu**.
3. Unutar lijevog okna kliknite na organizacijsku jedinicu **Korisnici**. Unutar desnog okna desnim gumbom miša kliknite na korisnika **Marko Tomić** te iz kontekstualnog izbornika odaberite opciju **Properties**.
4. Prikazuje se ekran **Marko Tomić Properties**. Kliknite na karticu **Organization**. U polje **Department** upišite **Prodaja** i kliknite gumb **OK**.
5. Vraćate se u konzolu **Active Directory Users and Computers**. Unutar desnog okna desnim gumbom miša kliknite na korisnicu **Ana Ivić** te iz kontekstualnog izbornika odaberite opciju **Properties**.
6. Prikazuje se ekran **Ana Ivić Properties**. Kliknite na karticu **Organization**. U polje **Department** upišite **Uprava** i kliknite gumb **OK**.
7. Vraćate se u konzolu **Active Directory Users and Computers**. Unutar lijevog okna desnim gumbom miša kliknite na organizacijsku jedinicu **Racunala** te iz kontekstualnog izbornika odaberite opciju **New-> Group**.
8. Prikazuje se ekran **New Object – Group**. U polje **Group name** upišite **RacunalaUprava** i kliknite gumb **OK**.
9. Vraćate se u konzolu **Active Directory Users and Computers**. Unutar lijevog okna kliknite na organizacijsku jedinicu **Racunala**.
10. Unutar desnog okna desnim gumbom miša kliknite na računalo **CLI1** te iz kontekstualnog izbornika odaberite opciju **Properties**.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

11. Prikazuje se ekran **CLI1 Properties**. Kliknite na karticu **Member Of** i zatim kliknite gumb **Add**.
12. Prikazuje se ekran **Select Groups**. U polje **Enter the object names to select** upišite **RacunalaUprava** i kliknite gumb **OK**.
13. Vraćate se na ekran **CLI1 Properties**. Kliknite gumb **OK**.
14. Vraćate se u konzolu **Active Directory Users and Computers**. Zatvorite ju.

Izradit ćemo datoteke na kojima ćemo demonstrirati klasifikaciju:

1. U **Windows Exploreru** prikažite lokaciju **C:\ShareDC**
2. Izradite datoteku **Godišnji.txt** sadržaja: **Marko 1.8.2015.**
3. Izradite datoteku **Plaće.txt** sadržaja: **Tajno – Marko ima najmanju plaću u firmi**.
4. Zatvorite **Windows Explorer**.

I za kraj ove cjeline uključujemo podršku za dinamičke dozvole pristupa na domenskom kontroleru:

1. Prikažite ekran **Start** i kliknite na **Group Policy Management**.
2. Prikazuje se konzola **Group Policy Management**. Unutar lijevog okna proširite stavke **Racunarstvo.edu-> Domain Controllers**.
3. Unutar lijevog okna desnim gumbom miša kliknite na stavku **Default Domain Controllers Policy** te iz kontekstualnog izbornika odaberite opciju **Edit**.
4. Prikazuje se **Group Policy Management Editor** konzola. Maksimizirajte ju radi preglednijeg rada.
5. Unutar lijevog okna proširite stavke
   Computer Configuration-> Policies-> Administrative Templates-> System-> KDC.
6. Unutar desnog okna desnim gumbom miša kliknite na stavku **KDC support for claims, compound authentication and Kerberos armoring** te iz kontekstualnog izbornika odaberite opciju **Edit**.
7. Prikazuje se ekran **KDC support for claims, compound authentication and Kerberos armoring**. Označite opciju **Enabled** a vrijednost padajućeg izbornika postavite na **Always provide claims**.
8. Kliknite gumb **OK**. Zatvorite **Group Policy Management Editor** konzolu.
9. Vraćate se u **Group Policy Management** konzolu. Minimizirajte ju.

Ažurirajmo GP postavke:

1. Prikažite ekran **Start** i upišite **cmd**
2. Desnim gumbom miša kliknite na stavku **Command Prompt** te iz kontekstualnog izbornika odaberite opciju **Run as Administrator**.
3. Prikazuje se **User Account Prozor**. Kliknite gumb **Yes**.
4. Prikazuje se **Command Prompt** konzola.
5. Upišite naredbu **`gpupdate /force`**
6. Minimizirajte **Command Prompt** konzolu.

Ovime smo ispunili preduvjete za dinamičke dozvole pristupa. Nastavimo s vježbom.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

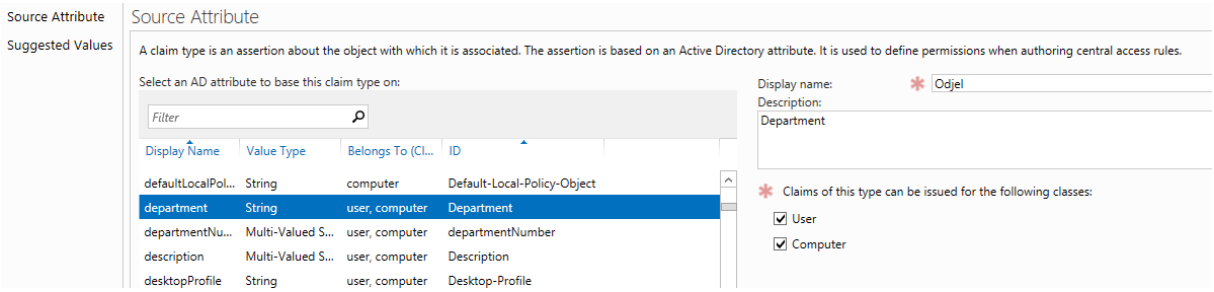
Konfiguracija dinamičkih dozvola pristupa

Nakon pripremljene infrastrukture možemo krenuti sa implementacijom dinamičkih dozvola pristupa. Moramo konfigurirati tvrdnje i svojstva resursa.

Postavljanje tvrdnje

Prvi korak u implementaciji dinamičkih dozvola pristupa je konfiguracija tvrdnje.

1. Prikažite ekran **Start**, upišite **Active** te iz rezultata pretrage kliknite na stavku **Active Directory Administrative Center**.
2. Prikazuje se **Active Directory Administrative Center** konzola. Maksimizirajte ju radi preglednijeg rada.
3. Unutar lijevog okna označite stavku **Dynamic Access Control** a zatim unutar središnjeg okna dvostrukim klikom otvorite stavku **Claim Types**.
4. Unutar desnog okna kliknite na stavku **New-> Claim Type**.
5. Prikazuje se ekran **Create Claim Type**. Maksimizirajte ga radi preglednijeg rada.
6. Postavite opcije:
    a. Sa popisa **Source Attribute** označite stavku **department**.
    b. U polje **Display Name** upišite **Odjel**.
    c. Označite stavke **User** i **Computer**.
7. Usporedite izgled svog ekran s onime na sljedećoj slici.



Slika 1 Konfiguracija vrste zahtjeva

8. Iz kategorije **Suggested Values** označite opciju **The following values are suggested** i kliknite gumb **Add**.
9. Prikazuje se ekran **Add a suggested value**.
10. U polja **Value** i **Display name** upišite **Uprava** i kliknite gumb **OK**.
11. Vraćate se u **Active Directory Administrative Center** konzolu.
12. Iz kategorije **Suggested Values** kliknite gumb **Add**.
13. Prikazuje se ekran **Add a suggested value**.
14. U polja **Value** i **Display name** upišite **Prodaja** i kliknite gumb **OK**.
15. Vraćate se u **Create Claim Type** ekran. Kliknite gumb **OK**.
16. Vraćate se **Active Directory Administrative Center** konzolu. Ne zatvarajte ju!

Definirali smo tvrdnje koje će dinamičke dozvole pristupa provjeravati. Tvrdimo da će neki objekt (korisnik ili računalo) izjaviti da je član odjela Uprava ili Prodaja. Sada ćemo konfigurirati svojstva resursima kojima želimo odrediti pristup putem dinamičkih dozvola:

1. Unutar lijevog okna **Active Directory Administrative Center** konzole kliknite na **Dynamic Access Control**.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

2. Unutar središnjeg okna dvostrukim klikom otvorite stavku **Resource Properties**.
3. Unutar središnjeg okna desnim gumbom miša kliknite na stavku **Department** te iz kontekstualnog izbornika odaberite opciju **Enable**.
4. Unutar središnjeg okna desnim gumbom miša kliknite na stavku **Confidentiality** te iz kontekstualnog izbornika odaberite opciju **Enable**.

Uključili smo podršku za dva svojstva. Jedno je pripadnost odjelu (engl. *Department*) a drugo povjerljivost resursa (engl. *Confidentiality*). Odjel moramo dodatno konfigurirati jer nas zanima samo odjel Uprava:

1. Unutar središnjeg okna desnim gumbom miša kliknite na stavku **Department** te iz kontekstualnog izbornika odaberite opciju **Properties.**
2. Prikazuje se ekran **Department**. Maksimizirajte ga radi preglednijeg rada.
3. U kategoriji **Suggested Values** kliknite gumb **Add**.
4. Prikazuje se ekran **Add a suggested value**. U polja **Value** i **Display name** upišite **Uprava** i kliknite gumb **OK**.
5. Vraćate se na ekran **Department**. Kliknite gumb **OK**.
6. Vraćate se u **Active Directory Administrative Center** konzolu. Ne zatvarajte ju!

Provjerimo jesu li nova svojstva dodana na popis svih svojstava:

1. Unutar lijevog okna kliknite na stavku **Dynamic Access Control**.
2. Unutar središnjeg okna dvostrukim klikom otvorite stavku **Resource Property Lists.**
3. Unutar središnjeg okna dvostrukim klikom otvorite stavku **Global Resource Property List**.
4. Prikazuje se prozor **Global Resource Property List**. Provjerite jesu li na popisu **Resource Properties** stavke **Confidentiality** i **Department**:
    a. Ako jesu, kliknite gumb **Cancel**.
    b. Ako nisu, dodajte stavke na popisu pomoću gumba **Add** iz kategorije **Resource Properties** .
5. Vraćate se u **Active Directory Administrative Center** konzolu. Minimizirajte ju.

Završili smo sa osnovnom definicijom tvrdnji i svojstava. Sigurno ste primijetili da nigdje nismo definirali svojstvo povjerljivosti, već samo odjela. Povjerljivost definiramo u drugoj konzoli.

Povjerljivost datoteka

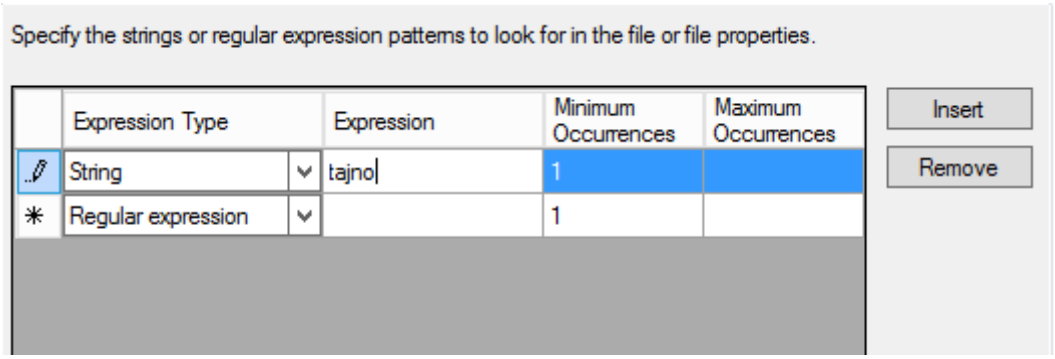
Povjerljivost datoteke definiramo pomoću File Server Resource Manager konzole:

1. Prikažite ekran **Start**, upišite **File** i kliknite na stavku **File Server Resource Manager**.
2. Prikazuje se **File Server Resource Manager** konzola. Maksimizirajte ju radi preglednijeg rada.
3. Unutar lijevog okna proširite stavku **Classification Management-> Classification Properties**.
4. Unutar lijevog okna desnim gumbom miša kliknite na stavku **Classification Properties** te iz kontekstualnog izbornika odaberite opciju **Refresh**.
5. Uočite kako su u središnjem oknu prikazane stavke **Confidentiality** i **Department**. Njih smo definirali kao svojstva u prethodnoj cjelini.
6. Unutar lijevog okna desnim gumbom miša kliknite na stavku **Classification Rules** te iz kontekstualnog izbornika odaberite opciju **Create Classification Rule**.
7. Prikazuje se prozor **Create Classification Rule.**

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

Sada ćemo definirati što točno datoteku čini povjerljivom:

1. Na kartici **General** u polje **Rule name** upišite **PovjerljivaDatoteka**.
2. Kliknite na karticu **Scope** i zatim kliknite gumb **Add**.
3. Prikazuje se ekran **Browse For Folder**. Označite mapu **C:\ShareDC** i kliknite gumb **OK**.
4. Vraćate se na ekran **Create Classification Rule**. Kliknite na karticu **Classification**.
5. Provjerite jesu li postavljene opcije (ako nisu postavite ih):
    a. **Classification method**: Content Classifier
    b. **Property**: Confidentiality
    c. **Value**: High
6. U kategoriji **Parameters** kliknite gumb **Configure**.
7. Prikazuje se ekran **Classification Parameters**.
8. Iz izbornika **Expression Type** odaberite vrijednost **String**.
9. U polje **Expression** za vrijednost **String** upišite **tajno**.
10. Usporedite izgled svog ekrana s onime na donjoj slici.



Slika 2 Kriterij povjerljive datoteke

11. Kliknite gumb **OK**.
12. Vraćate se na ekran **Create Classification Rule**. Kliknite na karticu **Evaluation Type**.
13. Označite stavku **Re-evaluate existing property values** i zatim uključite opciju **Overwrite the existing value**.
14. Kliknite gumb **OK**.
15. Vraćate se u **File Server Resource Manager** konzolu. Ne zatvarajte ju!

Izradili smo pravilo kojim definiramo povjerljive datoteke. Odlučili smo se za jednostavno ali efektno pravilo: datoteka koja sadrži minimalno jednu riječ „Tajno“ će biti označena kao povjerljiva. Primijetite kako sa NTFS dozvolama pristupa ovakav kriterij ne bi mogli nikako postaviti. Mapa na kojoj smo uključili klasifikaciju sadrži dvije datoteke – jedna mora udovoljiti kriteriju povjerljivosti (datoteka Plaće.txt). Provjerimo je li ta tvrdnja istinita:

1. Unutar desnog okna **File Server Resource Manager** konzole kliknite na opciju **Run Classification With All Rules Now**.
2. Prikazuje se prozor **Run Classification**. Označite opciju **Wait for classification to complete** i kliknite gumb **OK**.
3. Prikazuje se **Internet Explorer 11** prozor s konfiguracijom preglednika. Kliknite gumb **Ask me later**.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

4. Proučite izvještaj klasifikacije datoteka, tj. njegovo dno. Datoteka **Plaće.txt** mora bit označena kao povjerljiva, kako prikazuje donja slika.

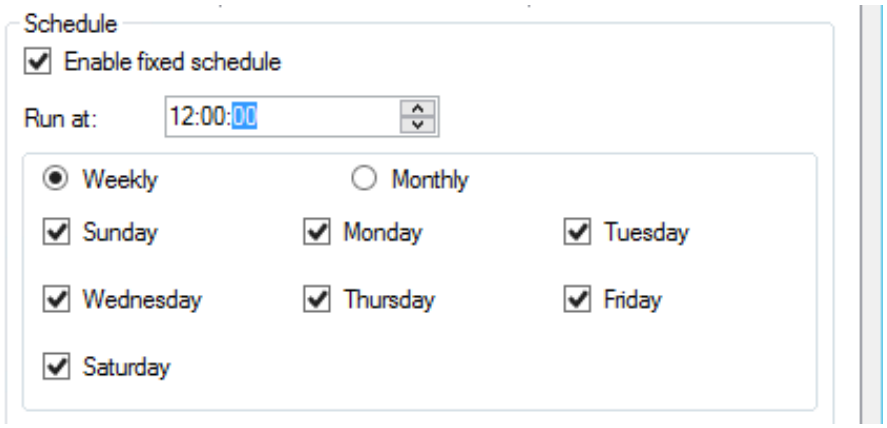
Statistics for files by 'Confidentiality'					
File name	Folder				
	Value	Rule	Last accessed	Last modified	Owner
Plaće.txt	C:\ShareDC				
	High	PovjerljivaDatoteka	10.11.2014. 14:41:55	10.11.2014. 14:42:11	RACUNARSTVO\DomAdmin

Slika 3 Povjerljiva datoteka

5. Zatvorite **Internet Explorer**.

Postupak klasifikacije je zahtjevan po pitanju resursa računala. Kao i postupak uklanjanja duplikata kojeg smo upoznali u prethodnoj vježbi, klasifikaciju je potrebno optimizirati kako bi se izvodila s minimalnim utjecajem na performanse. Predefinirano je automatska klasifikacija isključena (osim u slučaju zahtjeva za klasifikacijom od strane aplikacije) što implicira da ju moramo ručno pokretati. To je definitivno loša praksa. Postavimo automatsku klasifikaciju u periodu u kojem ne očekujemo veliko opterećenje poslužitelja:

1. Prikažite **File Server Resource Manager** konzolu.
2. Unutar desnog okna kliknite na opciju **Configure Classification Schedule**.
3. Prikazuje se prozor **File Server Resource Manager Options**. Kliknite na karticu (ako već nije aktivna) **Automatic Classification**.
4. Uključite opciju **Enable fixed schedule** i postavite opcije klasifikacije na izvođenje svaki dan u tjednu s početkom u 12h, kako prikazuje donja slika.



Slika 4 Interval klasifikacije

5. Kliknite gumb **OK**.
6. Zatvorite **File Server Resource Manager** konzolu.

Provjerimo kako se sustav klasifikacije manifestira sa stajališta Windows Explorera:

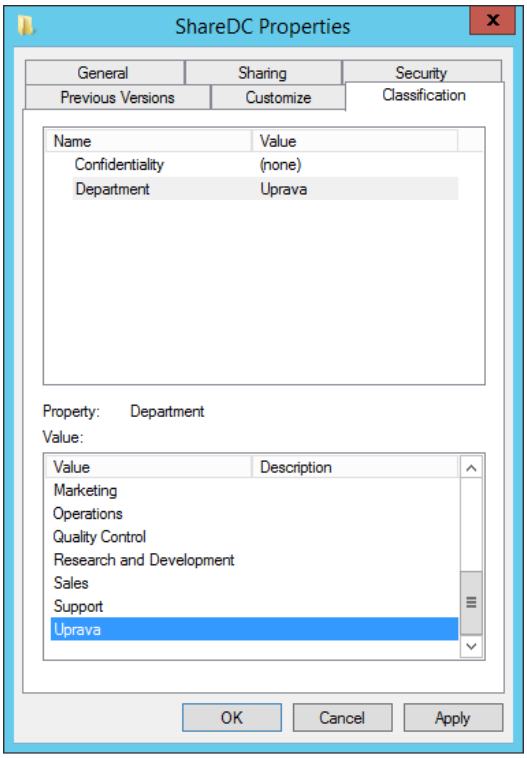
© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

1. Pokrenite **Windows Explorer** i prikažite lokaciju **C:\ShareDC**.
2. Desnim gumbom miša kliknite na datoteku **Plaće.txt** te iz kontekstualnog izbornika odaberite opciju **Properties**.
3. Prikazuje se ekran **Plaće Properties**. Kliknite na karticu **Classification**.
4. Uočite kako je vrijednost u kategoriji **Confidentiality** postavljena na **High**.
5. Kliknite gumb **Cancel**.
6. Vraćate se u **Windows Explorer**.
7. Desnim gumbom miša kliknite na datoteku **Godišnji.txt** te iz kontekstualnog izbornika odaberite opciju **Properties**.
8. Prikazuje se ekran **Godišnji Properties**. Kliknite na karticu **Classification**.
9. Uočite kako je vrijednost u kategoriji **Confidentiality** postavljena na **(none)**.
10. Kliknite gumb **Cancel**.
11. Vraćate se u **Windows Explorer**. Ne zatvarajte ga!

Uključimo klasifikaciju na razini cijele mape. Želimo da joj mogu pristupiti samo članovi odjela Uprava:

1. U **Windows Exploreru** prikažite lokaciju **C:**
2. Desnim gumbom miša kliknite na mapu **ShareDC** te iz kontekstualnog izbornika odaberite opciju **Properties**.
3. Prikazuje se prozor **ShareDC Properties**. Kliknite na karticu **Classification**.
4. U gornjem dijelu prozora kliknite na stavku **Department**.
5. U donjem dijelu prozora kliknite na stavku **Uprava**. Usporedite izgled svog prozora s onime na donjoj slici.



Slika 5 Postavke mape

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

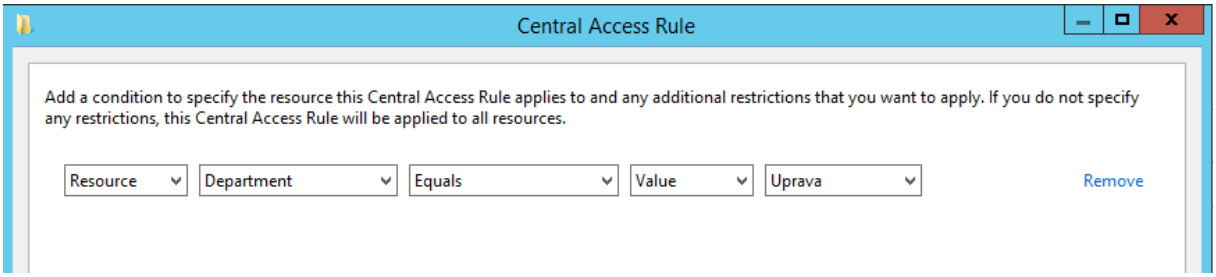
6. Kliknite gumb **OK**.
7. Minimizirajte **Windows Explorer** i prikažite **Active Directory Administrative Center** konzolu.

Definirali smo klasifikaciju datoteke na osnovu povjerljivosti njenog sadržaja. Nastavljamo vježbu.

Kontrola pristupa

Na neki način moramo „spojiti“ dva kriterija koji smo definirali u prethodnim cjelinama. To se postiže definiranjem središnjeg pristupnog pravila (engl. *Central access rule*). Prvo pravilo će omogućiti pristup mapama čija je klasifikacija postavljena kao vlasništvo odjela Uprava. Shodno tome, članovi drugih odjela neće moći pristupiti takvim podacima. Izradimo pravilo:

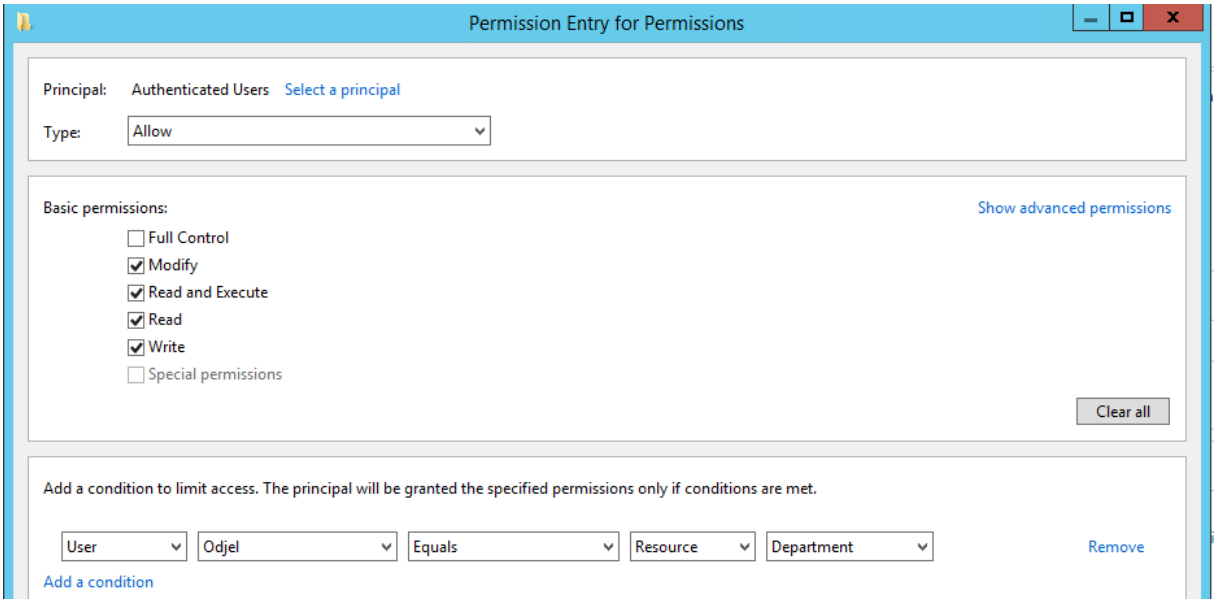
1. Unutar lijevog okna označite stavku **Dynamic Access Control** a zatim unutar središnjeg okna dvostrukim klikom otvorite stavku **Central Access Rules**.
2. Unutar desnog okna kliknite **New-> Central Access Rule**.
3. Prikazuje se prozor **Create Central Access Rule**. Maksimizirajte ga radi preglednijeg rada.
4. U polje **Name** upišite **OdgovarajućiOdjel**.
5. U kategoriji **Target Resources** kliknite gumb **Edit**.
6. Prikazuje se prozor **Central Access Rule**. Kliknite opciju **Add a condition**.
7. Dodaju se padajući izbornici za postavljanje kriterija. Postavite im vrijednosti **Resource-Department-Equals-Value-Uprava**, kako prikazuje donja slika.



Slika 6 Postavljanje kriterija

8. Kliknite gumb **OK**.
9. Vraćate se u prozor **Create Central Access Rule**. U kategoriji **Persmissions** označite opciju **Use following permissions as current permissions** i kliknite gumb **Edit**.
10. Prikazuje se prozor **Advanced Security Settings for Permissions**. Sa popisa označite grupu **Administrators** i kliknite gumb **Remove**.
11. Kliknite gumb **Add**.
12. Prikazuje se prozor **Permission Entry for Permissions**. Kliknite na opciju **Select a principal**.
13. Prikazuje se prozor **Select Users, Computer, Service Account, or Group**. U polje **Enter the object names to select** upišite **Authenticated Users** i zatim kliknite gumb **OK**.
14. Vraćate se u prozor **Permission Entry for Permissions.** U kategoriji **Basic permissions** označite dozvole **Modify, Read and Execute, Read** i **Write**.
15. Kliknite na opciju **Add a condition**.
16. Dodaju se padajući izbornici za postavljanje kriterija. Postavite im vrijednosti **User-Odjel-Equals-Resource-Department**. Usporedite izgled svog ekrana s onime na donjoj slici.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

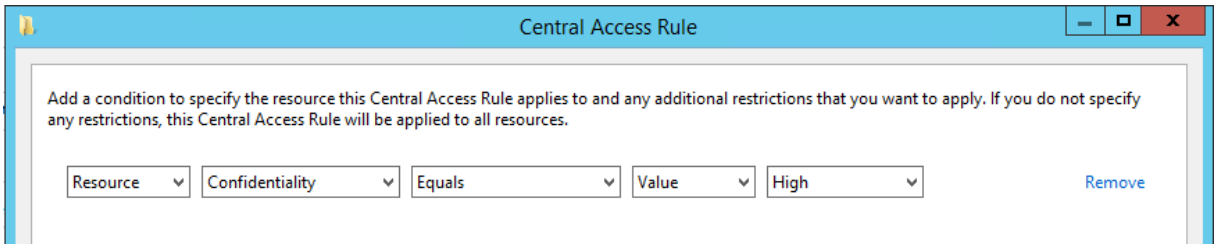


Slika 7 Kriteriji za dozvole pristupa

17. Kliknite gumb **OK**.
18. Vraćate se u prozor **Advanced Security Settings for Permissions**. Kliknite gumb **OK**.
19. Vraćate se u prozor **Create Central Access Rule**. Kliknite gumb **OK**.
20. Vraćate se u **Active Directory Administrative Center** konzolu. Ne zatvarajte ju!

Izradit ćemo još jedno pristupno pravilo koje će se odnositi na pristup povjerljivim datotekama, kao što je naša datoteka Plaće.txt. Ovo pravilo će sadržavati dva uvjeta: povjerljivim podacima mogu pristupiti samo članovi Uprave i to sa računala iz grupe RacunalaUprava. Konfigurirajmo ga:

1. Unutar desnog okna kliknite **New-> Central Access Rule**.
2. Prikazuje se prozor **Create Central Access Rule**. Maksimizirajte ga radi preglednijeg rada.
3. U polje **Name** upišite **PristupPovjerljivimPodacima**.
4. U kategoriji **Target Resources** kliknite gumb **Edit**.
5. Prikazuje se prozor **Central Access Rule**. Kliknite opciju **Add a condition**.
6. Dodaju se padajući izbornici za postavljanje kriterija. Postavite im vrijednosti **Resource-Confidentiality-Equals-Value-High**. Usporedite izgled svog ekrana s onime na donjoj slici.



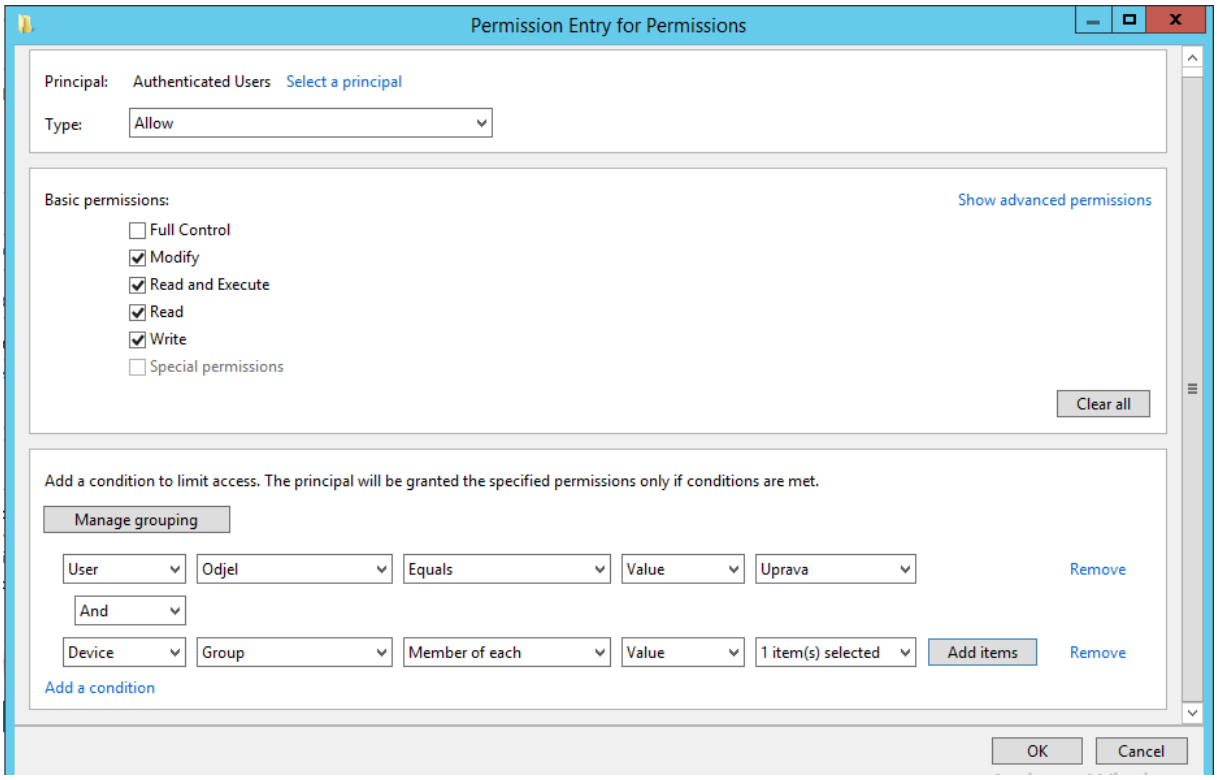
Slika 8 Pravilo za visoku povjerljivost

7. Kliknite gumb **OK**.
8. Vraćate se u prozor **Create Central Access Rule**. U kategoriji **Persmissions** označite opciju **Use following permissions as current permissions** i kliknite gumb **Edit**.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

9. Prikazuje se prozor **Advanced Security Settings for Permissions**. Sa popisa označite grupu **Administrators** i kliknite gumb **Remove**.
10. Kliknite gumb **Add**.
11. Prikazuje se prozor **Permission Entry for Permissions**. Kliknite na opciju **Select a principal**.
12. Prikazuje se prozor **Select Users, Computer, Service Account, or Group**. U polje **Enter the object names to select** upišite **Authenticated Users** i zatim kliknite gumb **OK**.
13. Vraćate se u prozor **Permission Entry for Permissions.** U kategoriji **Basic permissions** označite dozvole **Modify, Read and Execute, Read** i **Write**.
14. Kliknite na opciju **Add a condition**. Dodaju se padajući izbornici za postavljanje kriterija. Postavite im vrijednosti **User-Odjel-Equals-Value-Uprava**.
15. Kliknite na opciju **Add a condition**. Dodaju se još jedni padajući izbornici za postavljanje kriterija. Postavite im vrijednosti **Device-Group-Member of each-Value**.
16. Kliknite gumb **Add items**.
17. Prikazuje se prozor **Select Users, Computer, Service Account, or Group**. U polje **Enter the object names to select** upišite **RacunalaUprava** i kliknite gumb **OK**.
18. Vraćate se u prozor **Permission Entry for Permissions**. Usporedite izgled svog ekrana s onime na donjoj slici.



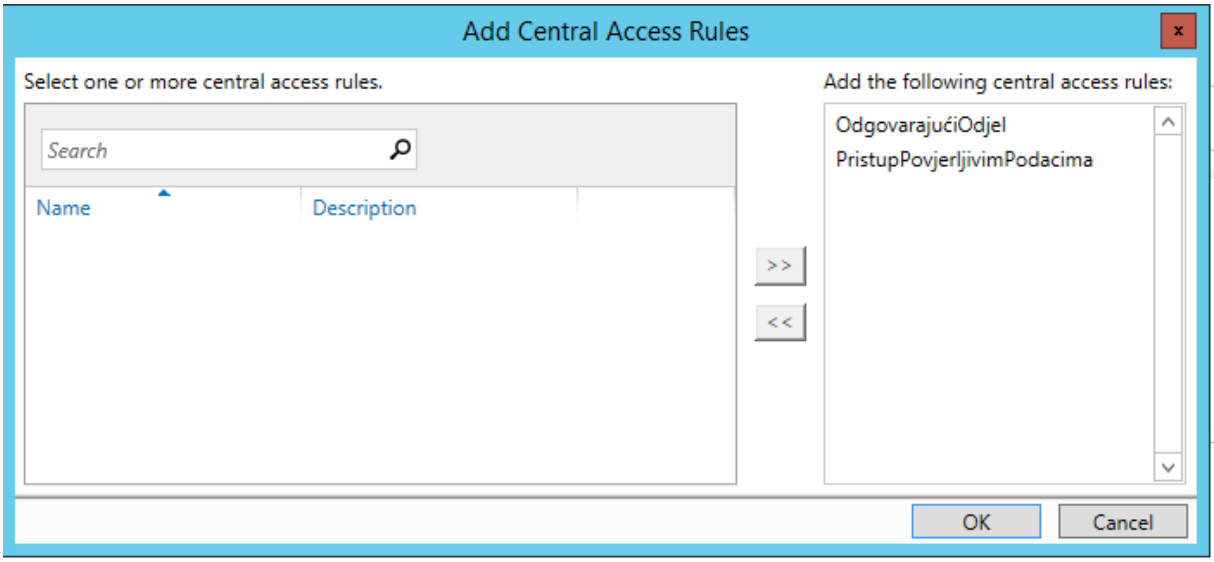
Slika 9 Pravilo za korisnika i računalo

19. Kliknite gumb **OK**.
20. Vraćate se u prozor **Advanced Security Settings for Permissions**. Kliknite gumb **OK**.
21. Vraćate se u prozor **Create Central Access Rule**. Kliknite gumb **OK**.
22. Vraćate se u **Active Directory Administrative Center** konzolu. Ne zatvarajte ju!

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

Pristupna pravila su sam po sebi trenutno beskorisna. Moramo konfigurirati mehanizam koji će djelovati prema postavljenim pravilima. Dodat ćemo oba pravila u mehanizam:

1. Unutar lijevog okna označite stavku **Dynamic Access Control** a zatim unutar središnjeg okna dvostrukim klikom otvorite stavku **Central Access Policies.**
2. Unutar desnog okna kliknite **New-> Central Access Policy**.
3. Prikazuje se prozor **Create Central Access Policy**. Maksimizirajte ga radi preglednijeg rada.
4. U polje **Name** upišite **ZastitaPovjerljivihDokumenata.**
5. U kategoriji **Member Central Access Rules** kliknite gumb **Add**.
6. Prikazuje se prozor **Add Central Access Rules**. U lijevom oknu označite pravilo **OdgovarajućiOdjel** i kliknite gumb **>>**.
7. Na isti način dodajte pravilo **PristupPovjerljivimPodacima**. Usporedite izgled svog ekrana s onime na donjoj slici.



Slika 10 Dodavanje pravila

8. Kliknite gumb **OK**.
9. Vraćate se u prozor **Create Central Access Policy**. Kliknite gumb **OK**.
10. Vraćate se u **Active Directory Administrative Center** konzolu. Minimizirajte ju.

Najveći dio konfiguracije je završen. Sada moramo pomoću Group Policyja uključiti mehanizam na razini cijele domene:

1. Prikažite **Group Policy Management** konzolu.
2. Unutar lijevog okna desnim gumbom miša kliknite na domenu **racunarstvo.edu** te iz kontekstualnog izbornika odaberite opciju **Create a GPO in this domain, and Link it here**.
3. Prikazuje se prozor **New GPO**. U polje **Name** upišite **DAC** i kliknite gumb **OK**.
4. Vraćate se u **Group Policy Management** konzolu. Unutar lijevog okna desnim gumbom miša kliknite na GP objekt **DAC** te iz kontekstualnog izbornika odaberite opciju **Edit**.
10. Prikazuje se **Group Policy Management Editor** konzola. Maksimizirajte ju radi preglednijeg rada.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

5. Unutar lijevog okna proširite stavke
   Computer Configuration-> Policies-> Windows Settings-> Security Settings-> File System.
6. Unutar lijevog okna desnim gumbom miša kliknite na stavku **Central Access Policy** te iz kontekstualnog izbornika odaberite opciju **Manage Central Access Policies**.
7. Prikazuje se prozor **Central Access Policies Configuration**. Unutar lijevog okna označite stavku **ZastitaPovjerljivihDatoteka.** Proučite polje **Description** – uočite kako pravilo sadrži dva kriterija (povjerljive podatke i odjel). Kliknite gumb **Add**.
8. Kliknite gumb **OK**.
9. Vraćate se u **Group Policy Management Editor** konzolu. Zatvorite ju.
10. Vraćate se u **Group Policy Management** konzolu. Minimizirajte ju.

Ažurirajmo GP postavke:

1. Prikažite **Command Prompt** konzolu.
2. Upišite naredbu **`gpupdate /force`**
3. Naredba se mora uspješno izvršiti.
4. Minimizirajte **Command Prompt**.

Konfiguracija je završena. Ipak, dinamičke dozvole još nisu aktivne. Kao i NTFS dozvole, valja ih postaviti direktno na resurs (u našem slučaju mapa ShareDC).

Uključenje dinamičkih dozvola pristupa

Sada napokon možemo na razini mape sa povjerljivim podacima uključiti dinamičke dozvole pristupa:

1. U **Windows Exploreru** prikažite lokaciju **C:\.**
2. Desnim gumbom miša kliknite na mapu **ShareDC** te iz kontekstualnog izbornika odaberite opciju **Properties**.
3. Prikazuje se prozor **ShareDC Properties**. Kliknite na karticu **Security**.
4. Kliknite gumb **Advanced**.
5. Prikazuje se prozor **Advanced Security Settings for ShareDC**. Kliknite na karticu **Central Policy** i zatim kliknite opciju **Change**.
6. Postavite opcije:
   a. **Central Policy**: ZastitaPovjerljivihDatoteka
   b. **Applies to**: This folder, subfolders and files
7. Proučite sadržaj pravila u donjem dijelu prozora.
8. Kliknite gumb **OK**.
9. Vraćate se u **ShareDC Properties** prozor. Kliknite gumb **OK**.
10. Zatvorite **Windows Explorer**.

Ovime je konfiguracija dinamičkih dozvola pristupa završena. U sljedećoj cjelini ćemo isprobati njihovu funkcionalnost.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

Provjera funkcionalnosti

Nakon dugotrajne konfiguracije dinamičkih dozvola pristupa došlo je vrijeme da napokon isprobamo funkcionalnost tog sustava. Podsjetimo se, imamo dva uvjeta za povjerljive podatke. Smiju im pristupiti članovi odjela Uprava i to isključivo s određenih računala (jedno u našem slučaju). Ostali korisnici ne smiju imati pristup povjerljivim podacima. Marko Tomić nije član Uprave pa s njim počinjemo provjeru dinamičkih dozvola:

1. Prijavite se na računalo **CLI1** kao korisnik **RACUNARSTVO\marko.tomic** s lozinkom **Pa$$w0rd**
2. Pokrenite **Windows Explorer** i prikažite sadržaj mrežnog diska **ShareDC**.
3. Nećete moći pristupiti mrežnom disku. Ispisuje se poruka **You do not have permissions to access**.
4. Odjavite se s računala **CLI1**.

Provjerimo može li Ana, kao članica Uprave, pristupiti podacima:

1. Prijavite se na računalo **CLI1** kao korisnik **RACUNARSTVO\ana.ivic** s lozinkom **Pa$$w0rd**
2. Pokrenite **Windows Explorer** i prikažite sadržaj mrežnog diska **ShareDC.**
3. Pokušajte otvoriti obje datoteke – morate uspjeti.
4. Odjavite se s računala **CLI1**.

-----NAPOMENA-----

Ukoliko Ana ne može pristupiti datoteci Plaće.txt (uz poruku *Access is denied*) ažurirajte GP postavke i prvo pokušajte napraviti *logoff* sa računala. Ako to ne radi, ponovno pokrenite računalo CLI1. Ako ponovo pokrenete računalo CLI1, pričekajte 4-5 minuta da vam računalo CLI1 ponovo postane dostupno kroz Horizon sustav.

Ana ima pristup povjerljivim podacima sa svog računala CLI1. Može li im pristupiti sa drugog računala? Provjerimo:

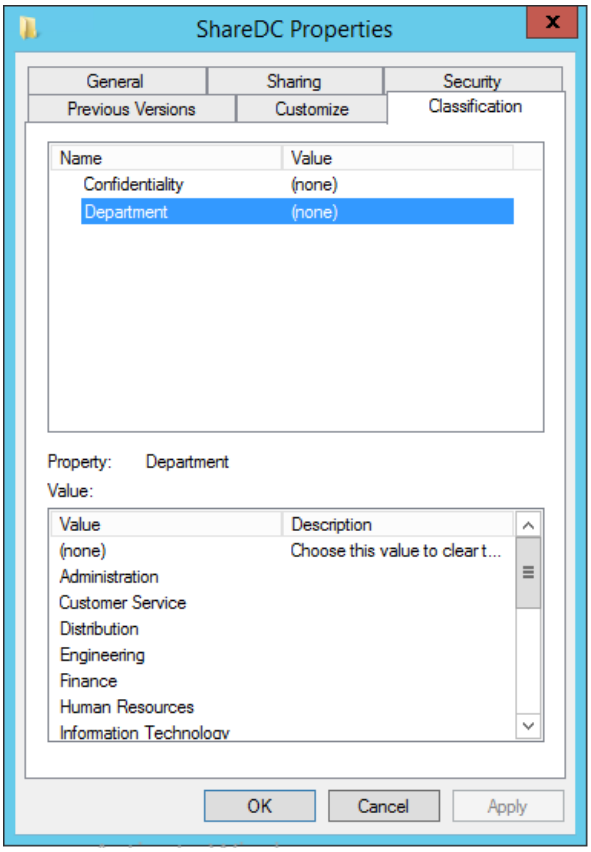
1. Prijavite se na računalo **SERVER1** kao korisnik **RACUNARSTVO\ana.ivic** s lozinkom **Pa$$w0rd**
2. Pokrenite **Windows Explorer** i prikažite sadržaj mrežnog diska **ShareDC**.
3. Sadržaj mrežnog diska se prikazuje. Pokušajte otvoriti obje datoteke.
4. Datoteku **Plaće.txt** nećete moći otvoriti. Ispisuje se poruka **Access is Denied**.
5. Odjavite se s računala **SERVER1**.

Dinamičke dozvole funkcioniraju i jedino Ana ima pristup datotekama. Ipak, što je s Markom? On ne smije imati uvid u plaće ali smije koristiti drugu datoteku. Naša pravila mu u potpunosti onemogućavaju pristup mrežnom disku, bez obzira što druga datoteka nije povjerljiva. Razlog tome leži u činjenici da smo postavili klasifikaciju vlasništva na vršnu mapu ShareDC, i tako ju cijelu označili kao mapu kojoj mogu pristupiti članovi odjela Uprava. Ispravimo tu pogrešku:

1. Prebacite se na računalo **SERVERDC**.
2. Pokrenite **Windows Explorer** i prikažite lokaciju **C:**.
3. Desnim gumbom miša kliknite na mapu **ShareDC** te iz kontekstualnog izbornika odaberite opciju **Properties**.
4. Prikazuje se prozor **ShareDC Properties**. Kliknite na karticu **Classification**.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

5. U gornjem dijelu prozora označite stavku **Department** a u donjem prvu stavku **(none)**. Usporedite izgled svog ekrana s onime na donjoj slici.



Slika 11 Isključenje povjerljivosti mape

6. Kliknite gumb **OK**.
7. Zatvorite **Windows Explorer**.

Provjerimo funkcioniraju li sada dinamičke dozvole pristupa u skladu s očekivanjima:

1. Prebacite se na računalo **CLI1**.
2. Prijavite se na računalo **CLI1** kao korisnik **RACUNARSTVO\marko.tomic** s lozinkom **Pa$$w0rd**
3. Pokrenite **Windows Explorer** i prikažite sadržaj mrežnog diska **ShareDC**.
4. Prikazuje se sadržaj mrežnog diska. Otvorite datoteku **Godišnji.txt**.
5. Datoteka se uspješno otvorila. Zatvorite ju.
6. Otvorite datoteku **Plaće.txt**. Prikazuje se poruka **Access is denied**. Kliknite gumb **OK**.
7. Odjavite se s računala **CLI1**.

Izvrsno, Marko sada ima pristup samo podacima koji nisu klasificirani kao povjerljivi. Provjerimo ima li Ana pristup svim podacima sa svog računala:

1. Prijavite se na računalo **CLI1** kao korisnik **RACUNARSTVO\ana.ivic** s lozinkom **Pa$$w0rd**
2. Pokrenite **Windows Explorer** i prikažite sadržaj mrežnog diska **ShareDC.**
3. Pokušajte otvoriti obje datoteke – morate uspjeti.
4. Odjavite se s računala **CLI1**.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

I za kraj ove cjeline provjerimo ima li Ana pristup povjerljivim podacima sa drugog računala:

1. Prijavite se na računalo **SERVER1** kao korisnik **RACUNARSTVO\ana.ivic** s lozinkom **Pa$$w0rd**
2. Pokrenite **Windows Explorer** i prikažite sadržaj mrežnog diska **ShareDC**.
3. Sadržaj mrežnog diska se prikazuje. Pokušajte otvoriti obje datoteke.
4. Datoteku **Plaće.txt** nećete moći otvoriti. Ispisuje se poruka **Access is Denied**. Kliknite gumb **OK**.
5. Odjavite se s računala **SERVER1**.

Infrastruktura sada funkcionira u skladu s očekivanjima. U sljedećoj cjelini ćemo upoznati još jednu korisnu značajku dinamičkih dozvola pristupa.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

Pomoć pri odbijenom pristupu

Prosječnom se korisniku greška *Access is denied* čini prilično nerazumljivom. To je za razumjeti jer poruka ne ispisuje nikakve dodatne informacije o odbijenom pristupu. Dinamičke dozvole pristupa imaju praktičnu mogućnost asistiranja korisnicima koji ne mogu pristupiti željenim podacima. Pomoć pri odbijenom pristupu se uključuje putem Group Policyja:

1. Prebacite se na računalo **SERVERDC**.
2. Prikažite **Group Policy Management** konzolu.
3. Unutar lijevog okna desnim gumbom miša kliknite na GP objekt **DAC** te iz kontekstualnog izbornika odaberite opciju **Edit**.
4. Prikazuje se **Group Policy Management Editor** konzola. Maksimizirajte ju radi preglednijeg rada.
5. Unutar lijevog okna proširite stavke
   Computer Configuration-> Policies-> Administrative Templates-> System-> Access Denied Assistance
6. Unutar desnog okna desnim gumbom miša kliknite na stavku **Customize Message for Access Denied** te iz kontekstualnog izbornika odaberite opciju **Edit**.
7. Prikazuje se prozor **Customize Message for Access Denied**. Uključite opciju **Enabled**.
8. U polje **Display the following message to users who are denied access** upišite **Podaci kojima pokušavate pristupiti su povjerljivi. Molimo zatražite pristup**.
9. Uključite opciju **Enable users to request assistance**.
10. Kliknite gumb **OK**.
11. Unutar desnog okna desnim gumbom miša kliknite na stavku **Enable access-denied assistance on client for all file types** te iz kontekstualnog izbornika odaberite opciju **Edit**.
12. Prikazuje se prozor **Enable access-denied assistance on client for all file types**. Uključite opciju **Enabled** i kliknite gumb **OK**.
13. Vraćate se u konzolu **Group Policy Management Editor**. Zatvorite ju.

Ažurirajmo GP postavke:

1. Prikažite **Command Prompt** konzolu.
2. Upišite naredbu **`gpupdate /force`**
3. Naredba se mora uspješno izvršiti.
4. Zatvorite sve prikazane prozore na računalu **SERVERDC**.

Proučimo kako pomoć pri odbijenom pristupu izgleda s klijentske strane. Prvo moramo ažurirati GP postavke i na klijentskom računalu:

1. Prebacite se na računalo **CLI1**.
2. Prijavite se na računalo **CLI1** kao korisnik **RACUNARSTVO\marko.tomic** s lozinkom **Pa$$w0rd**
3. Prikažite ekran **Start** i upišite **cmd**
4. Upišite naredbu **`gpupdate /force`**
5. Naredba se mora uspješno izvršiti.
6. Minimizirajte **Command Prompt**.

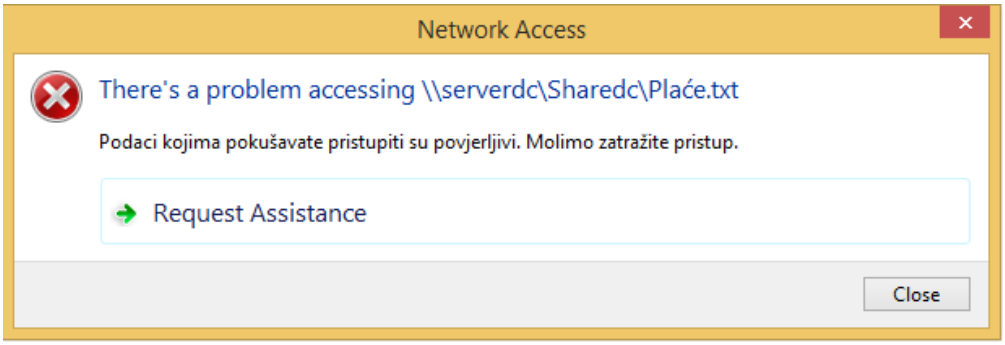
Provjerimo sada novosti pri odbijenom pristupu:

1. Pokrenite **Windows Explorer** i prikažite sadržaj mrežnog diska **ShareDC**.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

2. Otvorite datoteku **Plaće.txt**. Prikazuje se **Network Access** prozor kao na donjoj slici.



Slika 12 Informacije o odbijenom pristupu

3. Kliknite gumb **Request Assistance**.
4. Prikazuje se prozor **Request Assistance**. Proučite dostupne opcije i kliknite gumb **Close**.
5. Odjavite se s računala **CLI1**.

-----NAPOMENA-----

Iako se prikazuje prozor pomoći pri odbijenom pristupu, sam mehanizam slanja zahtjeva ne funkcionira. Drugim riječima, gumb Send na prethodnom prozoru bi samo prikazao pogrešku. Razlog leži u činjenici da se slanje poruka za zahtjevima za pristup odvija putem e-pošte. Kako naša infrastruktura nema poslužitelj e-pošte ni sustav poruka ne radi. U produkcijskom okruženju e-pošta funkcionira te bi s njom mehanizam pomoći pri odbijenom pristupu doveli do pune funkcionalnosti konfiguracijom u *File Server Resource Manager* konzoli. U njoj se, naime, konfiguriraju adrese poslužitelja e-pošte koji su zaduženi za slanje i primanje poruka sa zahtjevima za pristup. Upute za taj dio konfiguracije se nalaze u dodatnoj literaturi.

S ovom smo cjelinom završili. Dinamičke dozvole pristupa funkcioniraju i s njima smo spriječili potencijalno „curenje“ podataka, ali i Markov revolt kada bi saznao bolnu istinu.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

Samostalna vježba

Nakon što ste s korak-po-korak uputama upoznali dinamičke dozvole pristupa vrijeme je da sami ispunite sljedeće zahtjeve u našem testnom okruženju:

1. Unutar mape C:\ShareDC na računalu SERVERDC izradite novu mapu Prodaja.
2. Postavite dinamičke dozvole pristupa koje omogućuju da mapi Prodaja mogu pristupiti članovi odjela Prodaja i Uprava s bilo kojeg računala u domeni.
3. Unutar mape C:\ShareDC na računalu SERVERDC izradite novu mapu Win8.1
4. Postavite dinamičke dozvole pristupa koje omogućuju pristup mapi Win8.1 samo s Windows 8.1 Enterprise računala.

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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 na virtualnim računalima kako slijedi:

SERVERDC:

- Group Policyjem uključena podrška za dinamičke dozvole pristupa
- Instalirana File Server Resource Manager konzola.
- Konfigurirane tvrdnje za odjel i povjerljivost dokumenata.
- Datoteke koje sadrže riječ „tajno“ su klasificirane kao povjerljive.
- Definirano središnje pravo pristupa bazirano na odjelu i klasifikaciji datoteke.

SERVER1:

- Bez izmjena

CLI1:

- Učlanjen u grupu RacunalaUprava

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.

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

Što treba znati nakon ove vježbe?

1. Pripremiti Windows Server 2012 R2 okruženje za dinamičke dozvole pristupa.
2. Konfigurirati tvrdnju, svojstva i središnja prava pristupa.
3. Konfigurirati klasifikaciju datoteka na osnovu ključnih riječi.
4. Implementirati dinamičke dozvole pristupa sa višestrukim kriterijima.

Dodatna literatura

- Upute za konfiguraciju pomoći pri odbijenom pristupu:

http://technet.microsoft.com/en-us/library/hh831402.aspx

© Vedran Dakić, Visoko učilište Algebra
Zagreb, 2016.