DAC (engl. Dynamic Access Control) implementacija

Limiti trenutnih metoda rada sa dozvolama

- NTFS dozvole i ACL-ovi nude mogućnost podešavanja pristupa bazirano na SID-u
- AD RMS nudi još bolju zaštitu kroz kontrolu kako kako aplikacije koriste dokumente, isto po SID-u
- NTFS dozvole ne mogu koristiti logičke uvjete za dozvole (AND, OR)
- Ne možemo koristiti svoje uvjete za kontrolu pristupa dokumentima

Što je DAC?

- DAC (Dynamic Access Control) je nova mogućnost u WS2012/2012R2 za pristup datotečnim sustavima
- DAC koristi „claimove" i uvjetne izraze (AND, OR) za kontrolu pristupa i auditing
- Četiri scenarija:
  - Centralne politike pristupa za upravljanje pristupa datotekama
  - Auditing za provjeru i compliance
  - Zaštita osjetljivih dokumenata
  - Access-denied remediation

Što je claim?

- Claim je nešto što AD tvrdi o nekom specifičnom objektu
- U DAC-u, claimove definiramo korištenjem atributa korisnika ili uređaja
- U WS2012/2012R2, autorizacijski sustav je potrebno podesiti za korištenje claimova
- Može se napraviti:
  - User claim
  - Device claim

Što su Resource Properties?

- Definiraju atribute resursa koji želimo koristiti
- Grupiraju se u resource property liste
- Kada kreiramo resource proprety, možemo specificirati tip, dozvoljene i predložene vrijednosti

Pristup resursima sa DAC

File Server

NT access token	
Contoso\Alice	
User	Groups:….
	Claims: Title=SDE

AD DS Admin

Claim type
Display name
Source
Suggested values
Value type

Enable domain to issue claims

User attempts to log on

User

Receives a Kerberos ticket

Kerberos Ticket	
Contoso\Alice	
User	Groups:….
	Claims: Title=SDE

AD DS

Kerberos and a New Token

- DAC koristi Kerberos
  - Windows 8 Kerberos ekstenzije
  - DC izdaje grupe i claimove
  - DC radi enumeraciju user claimova

Pre-2012 Token
User Account
User Groups
(other data)

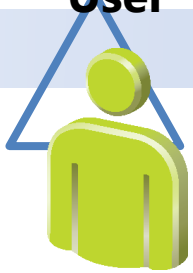
2012 Token	
User Account	
User	Groups
	Claims
Device	Groups
	Claims
(other data)	

Preduvjeti za DAC implementaciju

- Windows Server 2012 ili novije sa FSRM ulogom
- AD DS schema update, ili barem jedan WS2012 DC
- Windows 8 ili novije na klijentskoj strani za korištenje device claimova
- Uključenu podršku za DAC u ADDS (Default domain controllers GPO)

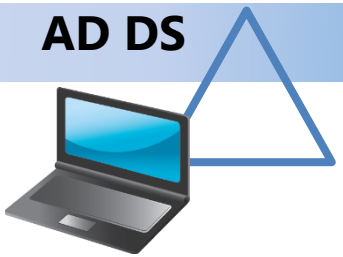
Conditional Expression Example

User



User claims
User.Department = Finance
User.Clearance = High

AD DS



Device claims
Device.Department = Finance
Device.Managed = True

File Server

Resource properties
Resource.Department = Finance
Resource.Impact = High

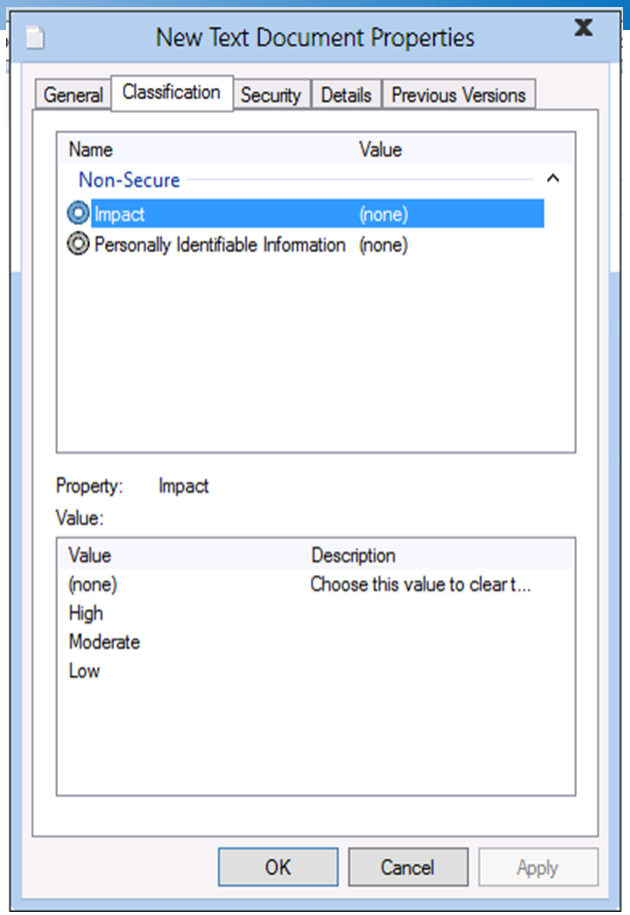
Access Rule

Applies to: @File.Impact = High
Allow | Read, Write | if (@User.Department = @File.Department) AND (@Device.Managed = True)

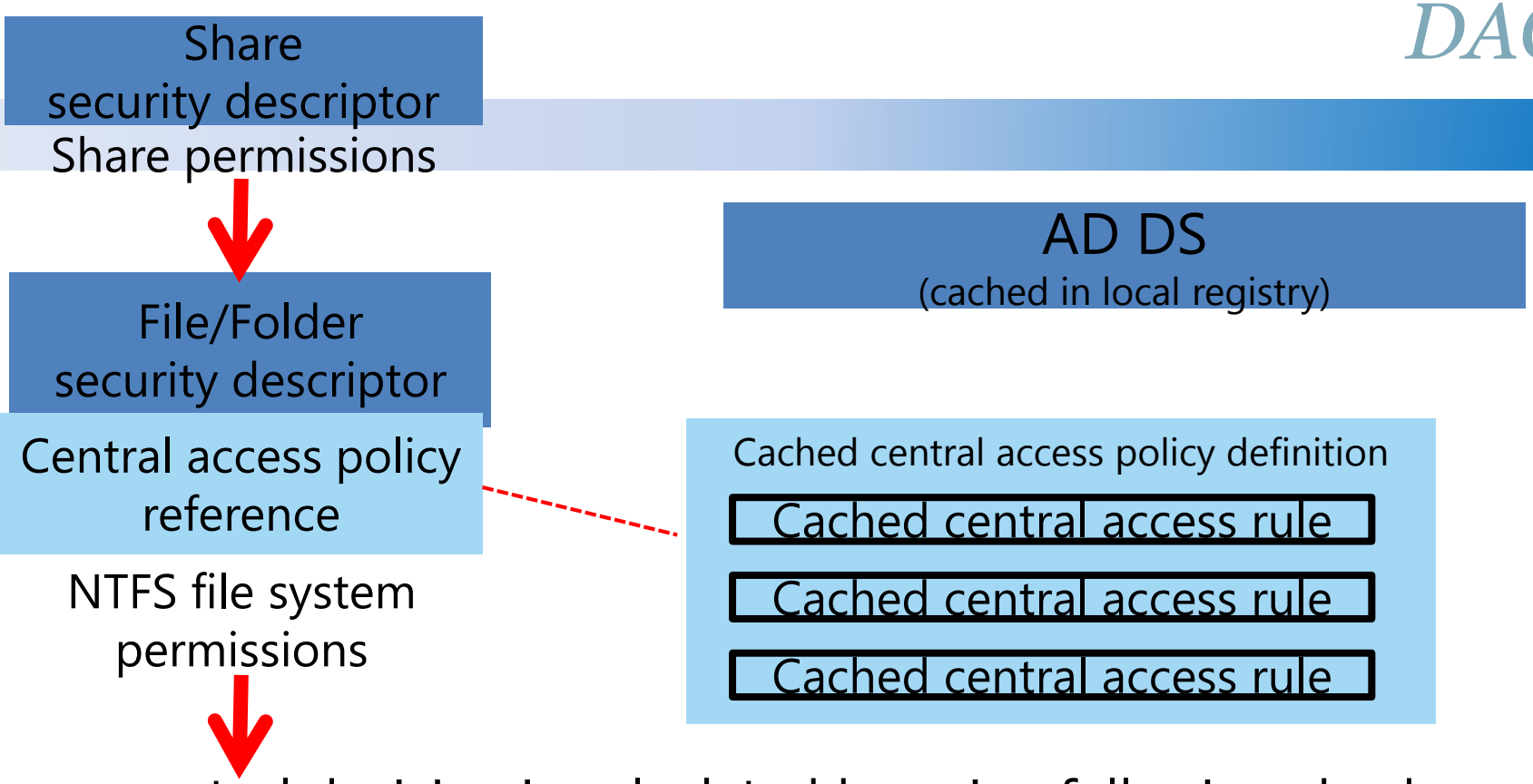
Algebra
visoka škola za primijenjeno računarstvo

Klasifikacija datoteka

- Resource property definicije se postavljaju u AD DS
- Resource property definicije se mogu koristiti za klasifikacije
- Klasifikacije se mogu koristiti automatski



Kako radi kontrola pristupa ako se koristi DAC?



Access control decision is calculated by using following checks:

1. Access check – Share permissions if applicable
2. Access check – File permissions
3. Access check – Every matching central access rule in central access policy

Sample Staging Event (4818)

Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy

Subject:
- Security ID: CONTOSODOM\alice
- Account Name: alice
- Account Domain: CONTOSODOM

Object:
- Object Server: Security
- Object Type: File
- Object Name: C:\FileShare\Finance\FinanceReports\FinanceReport.xls

Current Central Access Policy results:
- Access Reasons: READ_CONTROL: Granted by Ownership
  ReadAttributes: Granted by D:(A;ID;FA;;;BA)

Proposed Central Access Policy results that differ from the current Central Access Policy results:
- Access Reasons: READ_CONTROL: NOT Granted by CAR "HBI Rule"
  ReadAttributes: NOT Granted by CAR "HBI Rule"

Što je Access Denied Assistance?

Na file serveru:

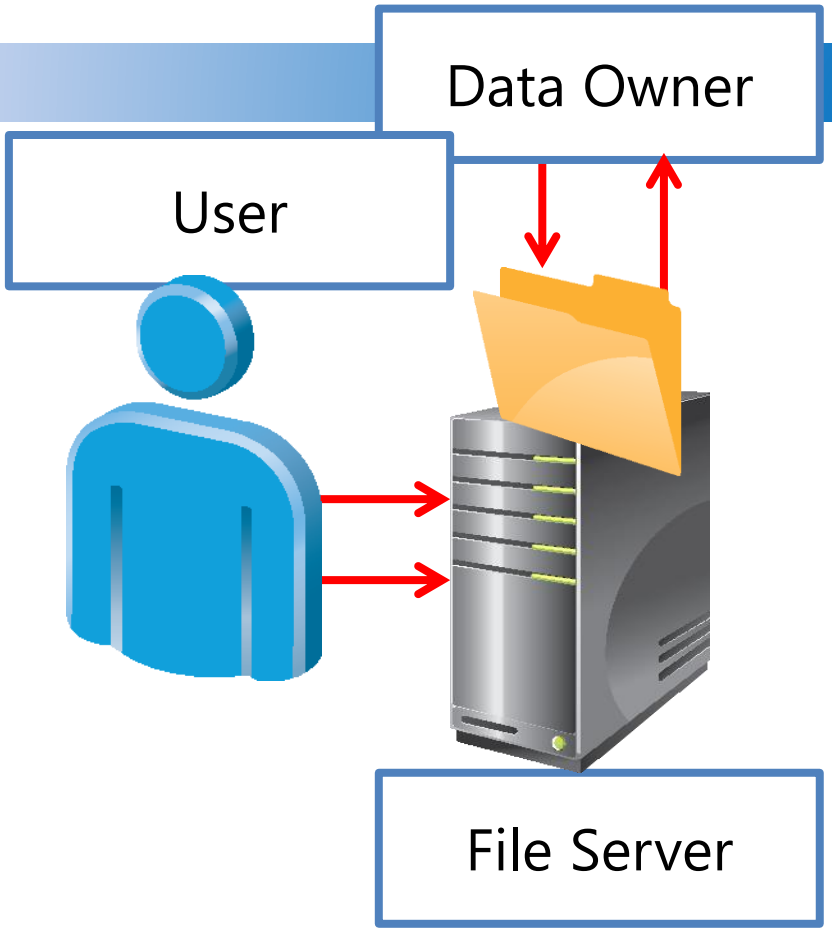
- Specificiramo tekst za ADA
- Specificiramo vlasnikovu e-mail adresu za share ili folder

Pokušaj pristupa:

- Korisniku se odbija pristup, dobiva troubleshooting tekst
- Korisnik može zatražiti pristup kroz e-mail

Vlasnik podataka ili helpdesk:

- Vlasnik dobiva korisnikov zahtjev
- Korištenjem effective permissions UI alata vlasnik odlučuje o adekvatnim akcijama
- Može preusmjeriti zahtjev IT adminu



Work Folders

- Work Folders opcija omogućava korisnicima siguran pristup poslovnim podacima sa bilo koje lokacije i uređaja
- Work Folders opcijom upravljaju administratori
- Trenutno podržani Windows 8.1 uređaji, uskoro iOS uređaji

Konfiguracija Work Folders

- Barem jedan WS2012 R2 file server
- Barem jedan WS2012 R2 domain controller
- Instalirati Work Folders na file server
- Napraviti share za korisničke podatke
- Pokrenuti New Sync Share Wizard da se napravi Work Folders struktura
- Konfigurirati klijente da koriste Work Folders kroz Group Policy (ili ručno)