

Alati sa lokalnu sigurnost - BitLocker, EFS, Alerting

12. PREDAVANJE



Algebra

visoka škola za
primijenjeno računarstvo

BitLocker je alat za enkripciju diska koji ima slijedeće karakteristike:

- Može se koristiti za enkripciju cijelog diska ili samo dijelova diska koje koristimo
- Može se koristiti sa EFS-om
- Štiti integritet Windows boot procesa
- Može koristiti TPM za naprednije opcije



Kako radi BitLocker

- Advanced Encryption Standard (AES)
 - 128-bit ili 256-bit encryption key
- Može se automatski konfigurirati kroz Windows PowerShell na računala u produkciji
- Kod novih instalacija računala možemo odmah napraviti enkripciju diska prije nego što su datoteke OS-a uopće zapisane na disk
- Postavke:
 - enkripcija samo korištenog prostora (brža implementacija)
 - enkripcija cijelog diska (najsigurnije, sporije)



Algebra

visoka škola za
primijenjeno računarstvo

Preduvjeti

- BitLocker je podržan na:
 - Windows Vista i novijim klijentskim OS-ovima
 - Windows Server 2008 i novijim serverskim OS-ovima
- korištenje TPM-a daje dodatne opcije:
 - verifikacija integriteta sustava
 - multifactor autentifikaciju



Algebra

visoka škola za
primijenjeno računarstvo

Konfiguracija BitLockera

- Uključiti TPM (opcija)
- Dodati BDE na server
- Konfigurirati GPO ili lokalni GP za BitLocker postavke
- Uključiti BitLocker na traženim diskovima



Algebra

visoka škola za
primijenjeno računarstvo

Management BitLocker-a kroz GPO

- GPO pruža oko 40 postavki za upravljanje BitLocker-om
- Uobičajene politike su:
 - metoda enkripcije i duljina ključa
 - zabrana write pristupa diskovima/izmjenjivim diskovima koji nisu zaštićeni kroz BitLocker
 - korištenjem lozinki za dodavanje diskova/izmjenjivih diskova
 - inzistiranje na dodatnoj autentifikaciji prilikom podizanja sustava
 - dozvoljavanje otključavanja sa mreže prilikom podizanja sustava



Algebra

visoka škola za
primijenjeno računarstvo

Recovery podataka na BitLocker diskovima

- kvalitetno planiranje
- Recovery opcije su:
 - korištenje recovery key datoteke za dobivanje ključa
 - uzimanje recovery ključa iz AD DS-a
 - korištenje Data Recovery Agent-a (korisnički računi koji imaju dozvolu dekripcije korištenjem pametnih kartica i PKI infrastrukture)
 - korištenje originalne BitLocker lozinke



Algebra

visoka škola za
primijenjeno računarstvo

EFS - Encrypted File System

- EFS može raditi enkripciju datoteka koje su pohranjene na NTFS particijama
- EFS je dodatni sigurnosni sloj
- EFS se može koristiti bez ikakve prethodne konfiguracije

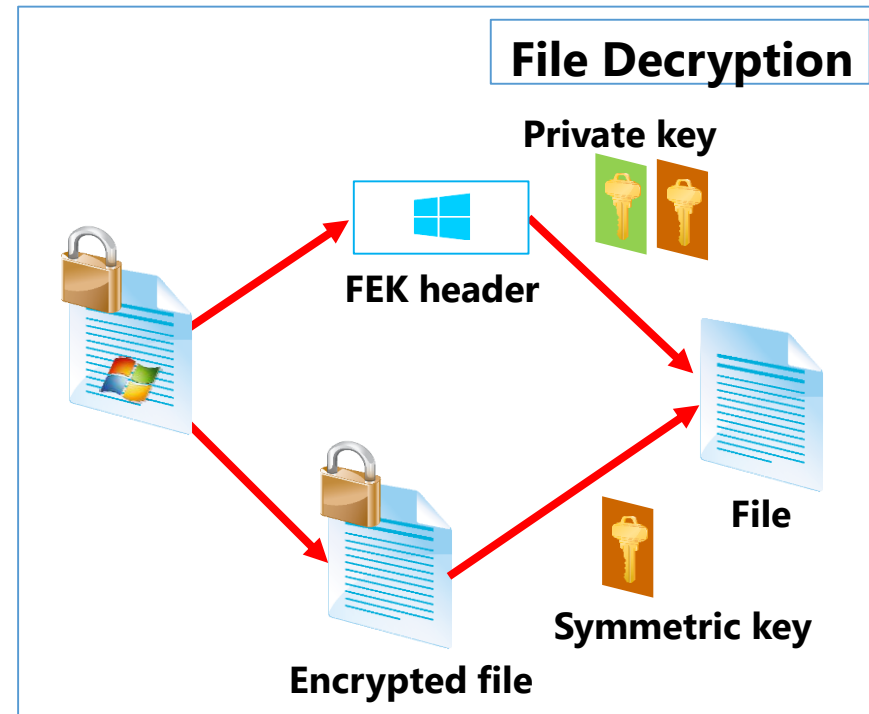
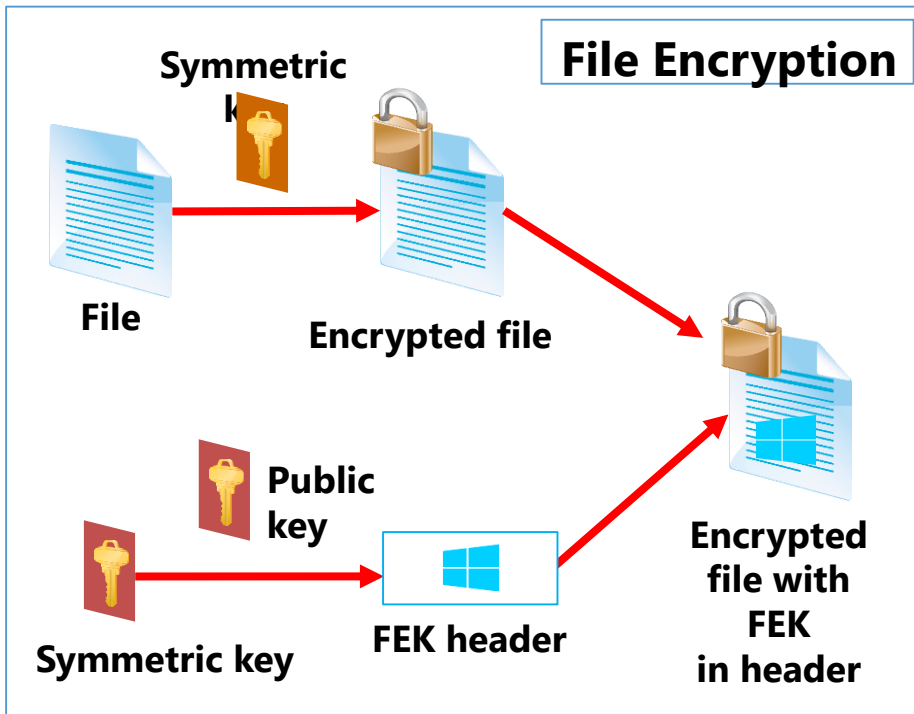


Algebra

visoka škola za
primijenjeno računarstvo

Kako EFS radi?

- Simetrična enkripcija se koristi za zaštitu podataka
- Infrastruktura javnog ključa se koristi za zaštitu simetričnog ključa



Recovery EFS-encrypted datoteka

- Da bismo bili sigurni da možemo napraviti recovery, trebamo napraviti:
 - backup korisničkih certifikata
 - konfigurirati recovery agent



Algebra

visoka škola za
primijenjeno računarstvo

EFS vs. BitLocker

- Shared računala
 - *bolji je EFS*: enkripcija foldera, zbog čega korisnici na shared računalima ne mogu pregledavati tuđe podatke
- Prijenosna računala
 - *bolji je BitLocker*: štiti cijeli disk, što znači da su podaci zaštićeni gdje god na disku bili
- High Security Environment
 - *najbolja je kombinacija EFS-a i BitLocker-a*: ovakva kombinacija daje više nivoa zaštite od pojedinačnog korištenja EFS-a ili BitLocker-a



Algebra

visoka škola za
primijenjeno računarstvo

Napredni Auditing



Algebra
visoka škola za
primijenjeno računarstvo

Auditing Politike

- Audit evenata po kategoriji, kao:
 - Pristup NTFS/ReFS datotekama i direktorijima
 - Promjene na AD objektima
 - Logon
 - prava korisnika
- Po defaultu, DC-ovi rade auditing uspješnih evenata za skoro sve kategorije

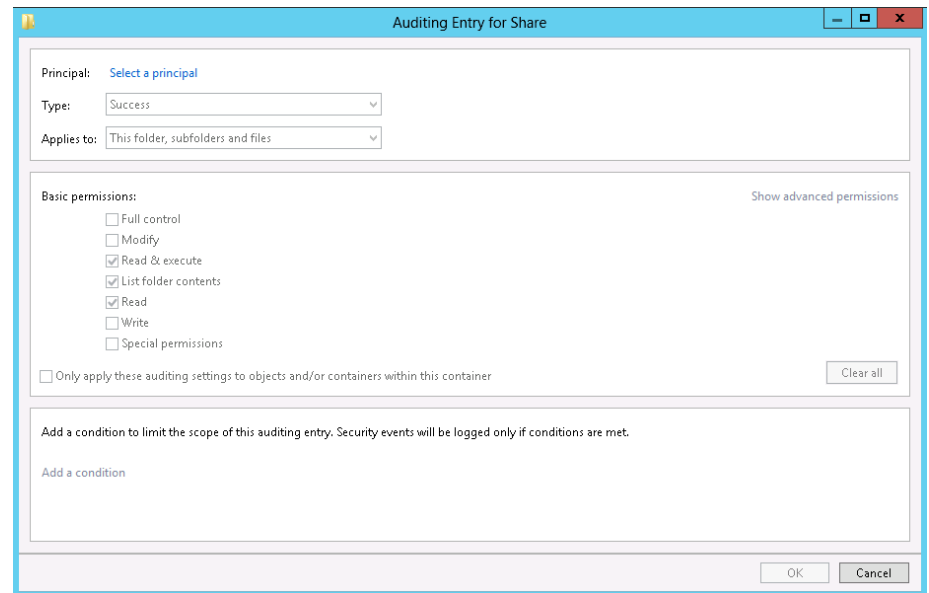


Algebra

visoka škola za
primijenjeno računarstvo

Auditing postavke na datoteci ili folderu

- Modifikacijom ACL-a na datoteci ili folderu:
- Full control snima sve pridružene evente
- snimanje audit evenata se ne događa dok ne uključimo audit politiku



Uključivanje Audit Politike

Konfiguracija Audit Policy postavki u GPO:



















- Uključiti postavke koje nam trebaju
- Primjeniti GPO na AD DS containeru gdje se nalaze serveri na kojima želimo uključiti auditing



Algebra

visoka škola za
primijenjeno računarstvo

Eventi u Security Log-u

Security Number of events: 57,667 (!) New events available					
Keywords	Date and Time	Source	Event ID	Task Category	
 Audit Success	9/20/2013 3:37:44 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:37:43 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:36:43 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:36:04 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:35:47 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:34:44 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:34:23 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:34:10 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:33:43 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:32:53 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:32:43 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:32:42 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:31:43 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:31:02 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:30:43 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:29:43 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:29:21 PM	Microsoft Windows ...	5140	File Share	
 Audit Success	9/20/2013 3:28:43 PM	Microsoft Windows ...	5140	File Share	

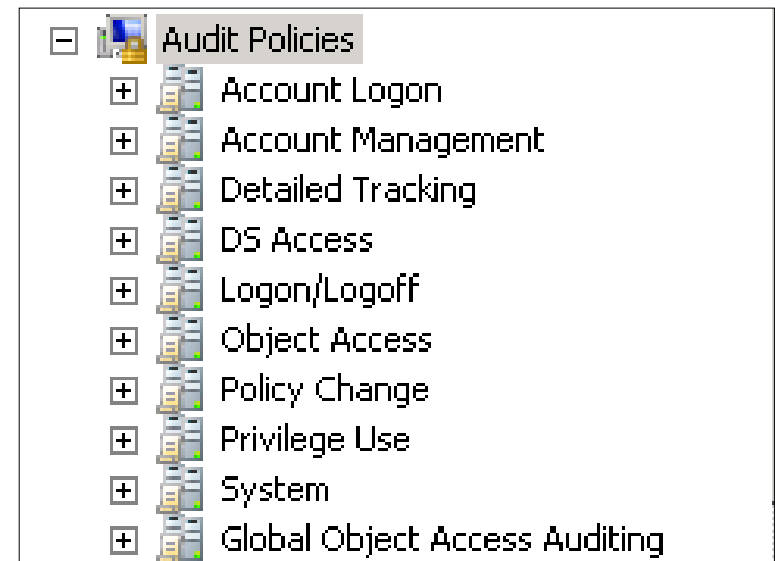


Algebra

visoka škola za
primijenjeno računarstvo

Napredne Audit Politike

Windows Server 2012(R2) i Windows Server 2008 R2 imaju dodatni set Advanced Audit politika koje možemo konfigurirati



Algebra

visoka škola za
primijenjeno računarstvo

Reliability Monitor

- Monitorira hw/sw probleme
- Daje Stability Index broj (od 1 do 10)
 - 1 za najniži nivo stabilnosti
 - 10 za najviši nivo stabilnosti
- Komponente u Reliability monitor-u
 - Povijesno izvješće stability index-a
 - Reliability details
 - Action to be performed - snimanje podataka, pokretanje "Problem Reports" konzole, provjera problema online



Algebra

visoka škola za
primijenjeno računarstvo

Monitoring kroz Server Manager

Server Manager console:

- se instalira automatski kod instalacije Windows Server 2012 (R2), možemo ga instalirati i na Windows 8(8.1)
- podržava monitoring Windows Server OS-ova
- Ima centralizirani *dashboard* za monitoring
- Analizira ili radi troubleshooting različitih problema
- Identificira kritične evente
- Monitorira status BPA tool-ova (Best Practices Analyzer)



Algebra

visoka škola za
primijenjeno računarstvo

?



Algebra

visoka škola za
primijenjeno računarstvo