# X- Evidentiranje događaja

S A D R Ž A J

# 10.1 Oporavak od katastrofa

- Oporavak servera koji je otkazao jedan je od **najvažnijih ali i najtežih poslova** koje možete da naučite o administriranju sistema.
- Administriranje servera ne znači ništa ako ne možete da ga oživite kada mu se nešto dogodi, na primer katastrofalni kvar diska ili oštećenje baze podataka aktivnog imenika.
- Veština oporavka od katastrofa se ne sastoji samo od učitavanja rezervnih kopija datoteka, već podrazumeva i **lociranje potencijalnih problema** koji mogu dovesti do pada servera, **obnavljanje uslužnih programa** posle ponovne instalacije OS i mnoga druga zaduženja.
- Suočavamo se s pritiscima zbog ponovnog instaliranja OS, obnavljanja podataka sa rezervnih kopija, a zatim i zbog ponovnog instaliranja svih uslužnih programa neophodnih za ispravan rad servera.
- Vrlo je važno da primenite pravilan postupak za oporavak sistema
- Microsoft je svoje OS opremio sa alatom ***Automated System Recovery*** (ASR) koji nam omogućuje automatski oporavak sistema
- Kao početna osnova za oporavak potrebno je napraviti plan za oporavak od katastrofa (***Disaster Recovery Plan***, ***DRP***).

# 10.1 Oporavak od katastrofa

- Prvi korak u oporavku je definisanje **strategije** i **protokola**.
- Zadatak strategije je da se ustanovi šta treba uraditi i kojim redom.
- Protokol definiše uslove koji moraju biti ispunjeni da bi se preduzele određene aktivnosti.
- Izlaganje gotove strategije za oporavak od katastrofa nema mnogo smisla, zato što je ona za svaku firmu drugačija.
- Treba uzeti u obzir, na primer radno vreme firme, da definišemo vreme odgovora na hitne slučajeve,vreme za izradu rezervnih kopija i td.
- **Dokumentacija je temelj svakog plana oporavka od katastrofa**.
- Bez dokumentacije, svi koji su uključeni u plan oporavka od katastrofa moraju se osloniti na svoje pamćenje što nam neće mnogo koristiti
- Mnogi ljudi često propuštaju da pročitaju dokumentaciju o tome kako da poprave sistem posle pada servera jer ona jednostavno i ne postoji
- Važno je da se pri normalnim uslovima,bez pritisaka, unapred pripremi plan oporavka sistema u slučaju njegovog pada i ostavi dokumenat.
- Preporučujuje se pisanje dokumenta koji je podeljen na nivoe.

# 10.1 Oporavak od katastrofa

- Upotrebljiv plan podrazumeva da znamo kako se koristi taj dokument
- Važno je definisati **cilj dokumentacije** i znati kome je ona namenjena.
- Svaka firma ima sopstvenu terminologiju koja je njoj svojstvena
- Sledeći važan aspekt izrade dokumentacije je da se odredi **ko može pristupati** toj dokumentaciji, **kada** i **na koji način**.
- Takvi dokumenti često sadrže veoma osetljive informacije, kao što su lozinke administratora, podatke o *firewall*-u i korisničkim nalozima.
- Dokumenti se napišu, a zatim se obično smeste na mrežni disk, tako da ih mnogi čitaju, proveravaju i predlažu ispravke i dopune.
- Ta lokacija na mrežnom disku treba da bude dostupna samo korisnicima koji imaju dodeljeno pravo pristupa pa treba da definišete i ko može pristupati dokumentaciji koja se ne nalazi u tom imeniku.
- Uzmite u obzir mogućnost da će ovaj dokument nekada biti dostupan osobama koje ne treba da pristupaju poverljivim informacijama.
- Sve osetljive informacije smestite u jedan odeljak koji možete lako ukloniti ako se ukaže potreba (primer, u dodatak DR plana).
- Najvažnije je da dokumentacija bude jednostavna i lako čitljiva.

# 10.1 Oporavak od katastrofa

- Kad pravite DR plan, treba odrediti resurse koji će vam olakšati posao
- Ako više osoba upravlja serverima, napravite raspored dolazaka po pozivu (*On-Call schedule)*, kojim se određuje ko će nastupiti i sprovesti neophodne korake ako bi došlo do pada servera.
- Što više servera imate, treba da uključite veći broj ljudi.
- Da bi se stvari efikasno dovele u red, osim administratora može vam biti potreban i član tima za administrira.mreže i članovi drugih timova
- Treba da sastavite spisak proizvodača hardvera, koje možete pozvati ako vam zatreba dodatni hardver ili tehnička podrška proizvodača
- U DR planu treba predvideti dodatne korake koji su neophodni ako otkaže udaljeni server.
- Pogodno sredstvo u ovom slučaju je **KVM** (*Keyboard*, *Video*, *Mouse*) sklopka koja prihvata TCP/IP vezu i omogucava da uspostavite vezu sa udaljenim serverom da bi ga ponovo inicijalizirali i konfigurisali.
- Pri određivanju resursa, može vam poslužiti dijagram servera.
- Ovaj dijagram bi imao hijerarhijsku strukturu i na njemu bi bili prikazani svi serveri, usluge i aplikacije na svakom serveru.

# 10.1 Oporavak od katastrofa

- Plan odgovora (*response plan)* ne možete napraviti preko noći.
- Morate potpuno poznavati server, i sve aplikacije koje koriste servere
- Da biste došli do tih informacija, verovatno ćete morati da razgovarate s više desetina ljudi u vašoj orgizaciji.
- Pošto sastavite spisak celokupne opreme i svih ljudi koje treba uključiti u plan odgovora, napravite grubi nacrt plana.
- Imajte na umu da možete čitavih mesec dana pisati plan, ali on nikada neće biti sasvim pouzdan jer će neki delovi svakako imati nedostatke
- Kada pravite plan odgovora pri definisanju vremena odziva, bolje je da pretpostavite najlošiju situaciju i date sebi više vremena za obnovu
- Pošto napravite plan, testiranje je najbolji način da se utvrdi da li on odgovara vašim potrebama.
- Bez obzira na to koju ćete tehniku primeniti za testiranje plana odgovora, imajte na umu sledeče tačke:

✓ **Ne postoji neuspeh:** *šta god da radite tokom testiranja, svi rezultati koje dobijete imaju vrednost. Svaki test daje rezultate koji pomažu administratorima da bolje upoznaju svoj sistem.*

# 10.1 Oporavak od katastrofa

- **Postavite ciljeve:** iscrpan plan s definisanim ciljevima može značajno skratiti testiranje sistema. Ovaj plan i njegovi ciljevi obično se mogu podeliti na više koraka koje nije neophodno izvršiti odjednom.
- **Stavke aktivnosti:** svaki test treba da bude vremenski određen i dobro dokumentovan; svaki korak testa i konačni ishod takođe treba dobro dokumentovati. Dokumentovanje i testiranje sistema nikome ne donosi nikakvu korist ako sve rezultate zadržite za sebe.
- **Učestalost:** ponavljajte testiranje! Jedno testiranje plana je dovoljno sve dok se neki aspekti sistema ne promene toliko da plan zastari. Osim redovnog testiranja plana na sistemu, treba da obavite i testiranje posle svake značajne izmene.
- **Savetnici:** neki savetnici su specijalizovani za testiranje sistema. Dobro je da iskoristite njihovo znanje i steknete uvid u svet testova. Postoje i mnogi softverski paketi koji vam mogu pomoći pri testiranju.

➢ Najbolji način da se uverite u adekvatnost svojih procedura za oporavak od katastrofe jeste da ih stavite na probu.

***Detaljno opišite nekoliko vrsta „katastrofa“ i simulirajte ih.***

# 10.1 Otpornost na greške

- Pojam otpornosti na greške, u računar.sistemu se odnosi da računar treba da ima mogućnost obrade hardverske ili softverske greške.
- Najjednostavniji problem je nestanak električnog napajanja.
- Taj problem možete jednostavno rešiti korišćenjem izvora neprekidnog napajanja (***Uninterrupted Power Supply - UPS***).
- Dvostruke komponente su neophodne ako server treba da bude izuzetno otporan na greške.
- Da biste dobili sistem koji je zaista neosetljiv na greške, potrebne su vam dve mrežne kartice, dva izvora napajanja, veći broj CPU i dva HD
- Važna je i upotreba redundantnog niza nezavisnih diskova (*Redundant Array Independent Disks*, ***RAID***) jedinica diskova izmenljivih u radu.
- Možemo koristiti nekoliko nivoa RAID sistema, ali se RAID 5 zbog svojih karakteristika najviše upotrebljava.
- RAID 5 zahteva najmanje tri jedinice diska, a pruža segmentiranje podataka i podatke za ispravljanje grešaka.
- Nedostatak RAID 5 sistema je to što zahteva izuzetno složen hardver koji je dosta skup.

# 10.1 Oporavak od katastrofa

- Poznato je da je sistem jak koliko i njegova najslabija karika.
- U slučaju da nastanu problemi, takode može koristiti poznavanje najslabije tačke sistema - to vam može pomoči da otkrijete odakle treba početi ispitivanje grešaka.
- Pri ispitivanju delova sistema koji su mogli prouzrokovati otkazivanje, treba da počnete od očiglednih:
  - ✓ jedinice čvrstog diska
  - ✓ napajanje električnom energijom
  - ✓ veze u mreži
  - ✓ kontroler jedinice čvrstog diska
  - ✓ procesor
- Windows Server OS podržava **bezglavu konfiguraciju** ( *headless configuration)* koja podrazumeva da možemo instalirati OS, podesiti sve aplikacije i zatim ukloniti grafičku karticu, tastaturu i miša.
- Sva dalja podešavanja možemo obaviti preko udaljenog računara.
- Kod planiranja konfiguracije servera,treba da razmislite i o LAN mreži
- Što je bolje upoznate i razmotrite, bolje ćete se snalaziti kod problema.

# 10.2 Registar baza podataka

- Registar je centralno skladište konfiguracionih podataka Windows Servera OS i u njemu se čuvaju informacije o OS, aplikacijama i korisničkom okruženju na samostalnim radnim stanicama i serverima
- U starijim verzijama OS iz Microsoft familije, većina konfiguracionih informacija čuvala se u *inicijalizacionim* datotekama - **.ini** datotekama.
- Ove datoteke bile su tekstualne i imale su odeljke u kojima su se čuvale vrednosti raznih konfiguracionih parametara, na primer podaci o upravljačkim programima, parametri korisničkog okruženja i td.
- **.ini** datoteke su i danas mehanizam koji se ponekad upotrebljava za čuvanje podataka o korisniku, parametara aplikacija i konfiguracije OS
- Iako omogučavaju jednostavno čuvanje i očitavanje podataka, **.ini** datoteke imaju i neke nedostatke – smanjena bezbednost
- Potreban je sistem za vođenje evidencije o konfiguracion.parametrima koji je otporan na greške kako bi se izbegla situacija kad sistem ne može da se inicijalizuje zbog toga što je **.ini** datoteka oštećena
- Rešenje je pronađeno u **Registar bazi** u kojoj se čuvaju informacije o hardveru i softveru sistema koje se odnose i na OS i na aplikacije.

# 10.2 Registar baza podataka

- U Registru se čuvaju i podaci o korisnicima, u koje spadaju korisnička prava pristupa, parametri bezbednosne strategije, parametri korisničkog okruženja (svojstva radne površine, direktorijum i td.)
- Za razliku od Windowsa NT, Win.Server OS u **Registru** više ne čuvaju naloge korisnika i računara niti podatke o mrežnim resursima.
- Ovaj posao sada pripada aktivnom imeniku.
- Kada server promovišete u upravljač domena, svi parametri koji pripadaju serveru upravljaču domena, na primer parametri radne površine, prenose se u aktivni imenik - obrnuto ne važi.

Načini na koji pojedine komponente menjaju sadržaj Registara:

- **Inicijalizacija sistema (*Setup*):** Kada instalirate Windows Server OS, *Setup* puni Registar na osnovu onoga što ste izabrali tokom instaliranja. Sadržaj Registra se menja kada se dodaje ili ukljanja hardver iz sistema.
- **Inicijalizacija aplikacija(*Application setup*):**Program za inicijalizaciju i pokretanje aplikacija obično menja sadržaj **Registra** prilikom instaliranja aplikacije da bi zabeležio konfigurac.parametre aplikacije. Registar se čita da bi odredili koje su komponente instalirane.

# 10.2 Registar baza podataka

- ✓**Aplikacije:**Aplikacije koje čuvaju svoje parametre u **Registru** menjaju te parametre prilikom pokretanja, isključivanja ili pri normalnom radu, da bi sačuvali njihove izmene koje su načinili korisnici ili aplikacije.
- ✓**Ntdetect:** Program ***Ntdetect.com*** izvršava se tokom pokretanja sistema u cilju detekcije hardvera i priključenih periferijskih uređaja,on upisuje u **Registar** podatke o hardveru i uređajima radi inicijalizacije uređaja.
- ✓**Jezgro (Kemel):** Jezgro Windows Server OS očitava **Registar** pri pokretanju sistema da bi odredilo koje upravljačke programe treba da učita i kojim redom, i učitava druge inicijalne parametre.
- ✓**Upravljački programi:** Većina upravljačkih programa čuva svoje konfiguracione i radne parametre u **Registru**.
- ✓**Sistem:** Windows Server OS kao celina u **Registru** čuva podatke o uslugama, instaliranim aplikacijama, vezama izmedu dokumenata i OLE vezama, mreži, parametrima korisnika i drugim svojstvima.
- ✓**Alatke za administriranje:** programi kakvi su Editor Registra, Control Panel, razne MMC konzole i samostalni uslužni programi za administriranje, nude korisnički interfejs za izmenu sadržaja **Registra**.

# 10.2 Struktura Registar baze podataka

- **Registar** formira hijerarhijsku bazu podataka (stablo) s pet osnovnih grana koji s zovu ***ogranci*** koji mogu da sadrže ***odrednice*** (*keys)*
- ***Odrednice*** imaju ulogu kontejnera ***pododrednica*** i ***stavki***.
- Pododrednice su ogranci odrednica dok su stavke njihovi parametri
- Postoje dva fizička ogranka u **Registru** Windows Servera OS:
  1. HKEY_LOCAL_MACHINE (sadrži parametre sistema i hardvera)
  2. HKEY_USERS (sadrži podatke o korisničkim parametrima).
- Ova dva fizička ogranka podeljena su na pet logičkih ogranaka

**1.<u>HKEY_LOCAL_MACHINE</u>:** skraćeno **HKLM**, čuva parametre specifične za lokalnu mašinu, kojima se definišu hardver i svojstva OS i ne zavise od toga koji je korisnik prijavljen. HKLM se sastoji od:

- **HARDWARE:** čuva se fizička hardverska konfiguracija računara.
- **SAM:** čuva bezbednosne podatke o korisnicima i grupama loka.mašine
- **SECURITY:** podaci koji definišu lokalnu bezbedonosnu strategiju.
- **SOFTWARE:** čuvaju se podaci o instaliranim programima.
- **SYSTEM:** podaci o parametrima za pokretanje sistema, upravljačkim programima, uslugama i drugi parametri na nivou sistema.

# 10.2 Struktura Registar baze podataka

2. **HKEY_CLASSES_ROOT:** **HKCR**, sadrži podatke o vezama datoteka sa odgovarajućim programima i omogućava registraciju klasa specifičnih za svaki računar i korisnika. Sastoji se od podogranaka:
   - HKLM\SOFTWARE\Classes
   - HKEY_CURRENT_USER\SOFTWARE\Classes,
3. **HKEY_CURRENT_USER:** skraćeno **HKCU**, čuvaju se parametri specifični za korisnika koji trenutno lokalno koristi sistem i odnose se na parametre kojima se definišu korisnikovo radno okruženje i korisnički interfejs. Ova odrednica sadrži sledeče pododrednice:

- **AppEvents:** sadrži podatke o vezi između aplikacija i događaja,
- **Console:** sadrži podatke koji definišu pojavljivanje i ponašanje komandne konzole OS i aplikacija koje rade u komandnom režimu.
- **Control Panel:** podaci koji se obično podešavaju preko Control Panela.
- **Environment:** sadrži promenljive okruženja trenutnog korisnika.
- **Identities:** sadrži podatke o identitetu pojedinačnih korisnika:ID broj poslednjeg korisnika, korisničko ime poslednjeg korisnika, podatke o identifikaciji koji se odnose na određene aplikacije i tako dalje.

# 10.2 Struktura Registar baze podataka

- **Keyboard Layout:** podaci o rasporedu tastera na korisničkoj tastaturi i preslikavanju tastera za međunarodne parametre.
- **Network:** čuvaju se podaci o mrežnim vezama korisnika
- **Printers:** podaci o korisničkim vezama sa štampačima.
- **RemoteAccess:** podaci o korisnikovom interfejs profilu i parametrima veza koje se ostvaruju preko telefonskih linija.
- **Software:** podaci o aplikacijama koje je korisnik instalirao.
- **Volatile Environment:**sadrži privremene podatke o radnom okruženju, na pr. korisnički direktorijum za aplikacije i server za prijavljivanje.

4. **HKEY_USERS: HKU** čuva podatke o profilu korisnika koji koriste računar lokalno kao i podatke o podrazumevanom korisniku za lokalni računar. Ova odrednica sadrži pododrednice za svakog korisnika čiji se profil čuva na računaru i odrednicu za podrazumevanog korisnika
5. **HKEY_CURRENT_CONFIG: HKCC** čuva podatke o hardverskoj konfiguraciji lokalnog računara koji su utvrđeni prilikom inicijalizacije i pokretanja sistema: podaci o dodeljivanju uređaja, upravljačkim programima i tako dalje.

# 10.2 Struktura Registar baze podataka

- Svaki navedeni ogranak naziva se *grana* Registra (*hive).*
- Microsoft definiše granu Registra kao telo sastavljeno od odrednica, pododrednica i vrednosti, ukorenjeno na vrhu hijerarhije Registra.
- Jedna grana Registra sadrži dve datoteke:

1. Datoteku Registra-sadrži strukturu Registra i parametre za datu granu.
2. Dnevnik- predstavlja dnevnik transakcija za sve modifikacije u datoteci

- OS koristi proces poznat pod imenom ***ispiranje*** (*flushing)* da bi obezbedio pouzdanu, radnu kopiju Registra u bilo kom trenutku.
- Ispiranje predstavlja zaštitu od nedovršenih pokušaja izmene Registra.
- Pokušaji izmene Registra, po isteku zadatog broja sekundi ili kada aplikacija eksplicitno zahteva,ne upisuju se u Registar već se "ispiraju"
- To znači da se izmenjeni podaci prvo upisuju u datoteku događaja grane Registra da bi se mogli rekonstruisati ako se sistem zaustavi ili otkaže pre nego što se podaci upišu u datoteku Registra.
- Datoteka događaja se ispira posle uspešnog ažuriranja dnevnika
- U toku ažuriranja OS označava prvi sektor u datoteci Registra da bi ukazao da je u toku izmena (da je Registar ,,prljav").

# 10.3 Praćenje događaja

- Evidencija događaja omogućava beleženje svih događaja u OS u cilju kontrolisanja pristupa sistemu i osiguravanja bezbednosti sistema.
- To je značajna alatka za osiguravanje bezbednosti, ali može znatno da preoptereti server ako se nepravilno konfiguriše i koristi.
- Microsoft definiše događaj kao značajnu pojavu u OS ili aplikaciji, o kojoj korisnici, posebno administratori, treba da budu obavešteni.
- Događaji se beleže u dnevnike događaja (*event logs)* kojima možete baratati pomoću modula konzole ***Event Viewer***.
- Evidencija događaja omogućava da pratite određene događaje, tj. da beležite ***uspešne/neuspešne*** pokušaje odigravanja određenih događaja
- U sledećoj listi navedene su kategorije događaja i šta one prate:

- **Account logon events:** Beleži se prijavljivanje i odjavljivanje korisnika preko korisničkih naloga.
- **Account management:** Beleži se kada je otvoren korisnički ili grupni nalog, kada je nalog promenjen ili izbrisan, kada je promenjen naziv, kada je dozvoljen ili zabranjen, kada je zadata ili promenjena lozinka.
- **Directory service access:** Beleže se pristupi aktivnom imeniku.

# 10.3 Praćenje događaja

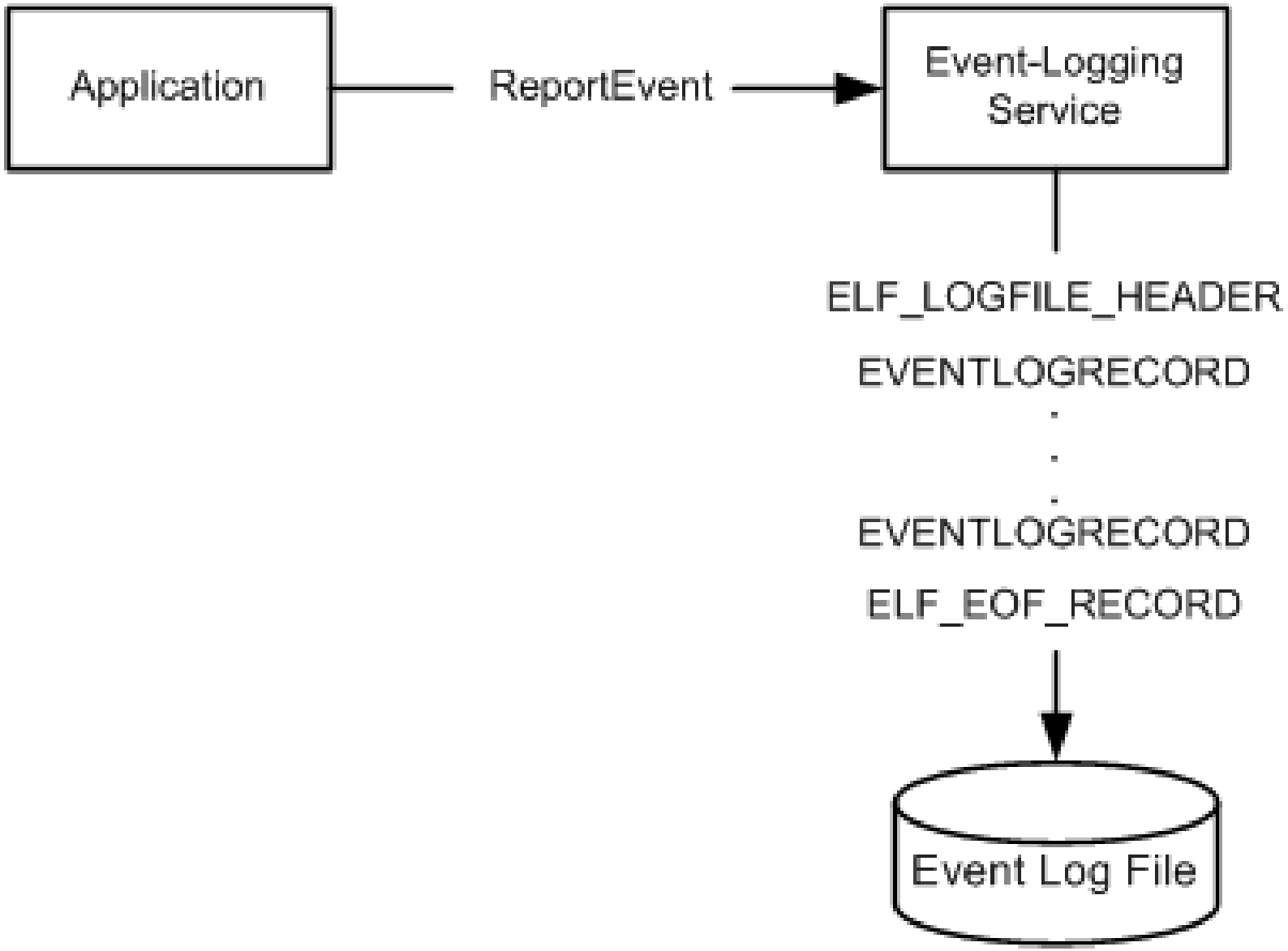
- **Logon events:** Beleže se prijave sa daljine na sistem, na primer korišćenje resursa preko mreže ili priključivanje udaljenih usluga.
- **Object access:** Beleži se kada se pristupilo određenom objektu i koji je tip pristupa primenjen.
- **Policy change:** promene prava korisnika i strategija evidentir.događaja
- **Privilege use:** Prati se kada je korisnik pokušavao da koristi prava koja mu nisu dodeljena prilikom prijavljivanja na sistem i odjavljivanja.
- **Process tracking:** događaji koji se odnose na izvršavanje procesa
- **System events:** Beleže se sistemski događaji: resetovanje, pokretanje i isključivanje sistema kao i događaji koji utiču na bezbednost sistema

- Svaka od ovih kategorija ima nekoliko različitih tipova događaja
- Log datoteka je skup zapisa o svim događajima koji su se dogodili
- Jedan zapis predstavlja jedan događaj unutar sistema.
- Skladno tome analiza logova predstavlja kontrolu računarskog sistema
- Analiza logova pomaže u pronalasku događaja koji je prouzrokovao incident u informacijskom sistemu, ali može poslužiti i za prevenciju mogućih incidenata.

# 10.3 Vrste Log zapisa

- Za razumevanje zapisa unutar logova potrebno je razumeti format zapisa u logovima.
- Svaki OS, program ili servisi imaju vlastiti format zapisa.
- Postoji više različitih podela logova prema vrstama, ali kao dve glavne vrste logova mogu se uzeti sistemski (System) i aplikacijski logovi
- ***Error*** i ***access*** su vrlo važni logovi i njihove zapise mogu generisati OS ili razne aplikacije koje se izvršavaju na računaru.
- Dve glavne vrste logova dele se na druge podvrste.
- Takođe, logove je moguće podeliti i na vremenske i statičke.
- Vremenski zapisi sadrže tačno vreme događaja dok statički zapisi sadrže generalne podatke o konfiguraciji.
- Kod Windows OS podela logova se razlikuje jer jer pored sistemskih i aplikacijskih logova postoje još i sigurnosni (Security) logovi.
- U sigurnosnim logovima nalaze se zapisi o događajima vezanim uz prijavu i odjavu korisnika, kreiranje, uređivanje i brisanje datoteka, itd.
- Kako je većina sigurnosnih zapisa kreirana od strane OS moguće je sigurnosne logove svrstati u sistemske logove.

# 10.3 Postupak formiranja zapisa



# 10.3 Praćenje događaja

- Događaji u logovima mogu se klasificirati prema stepenu važnosti:
  1. Kritična (*Critical*),
  2. Pogreška (*Error*),
  3. Upozorenje (*Warning*),
  4. Informacija (*Information*),
  5. Opširan zapis (*Verbose*).
- Kod zapisa u Windows OS svaki zapis se sastoji od zaglavlja koje sadrži sistemske podatke i „tela“, odnosno podataka o specifičnom događaju koji se beleži.
- Ovakvi logovi se najčešće smeštaju u obliku XML datoteke, ali u nekim slučajevima postoje i zapisi u HTML obliku.
- Uz to aplikacijski logovi mogu imati sažeti oblik koji se najčešće smešta sa **.log** ekstenzijom što je slično zapisima u Linux okruženju.
- Logovima se pristupa putem ***Control panel***, zatim se odabere ***Administrative Tools*** i na kraju odabere se ***Event Viewer***.
- Isti postupak pristupanja i analize logova važi i za Windows servere s tim da postoje pojedine razlike među novijim i starijim verzijama OS.

# 10.3 Sistemski zapis Windows OS

***Provider*** - Izvor tj. proces koji je zatražio zapis događaja.
***EventID*** - Broj koji identificira tip događaja (ID događaja)
***Version*** - Može sadržavati podatke o verziji događaja.
***Level*** - Numerička oznaka stepena važnosti događaja
***Task*** - Ovo polje ostavlja se na korištenje procesu koji poziva zapisivanje događaja, a može sadržavati podatke o pozivu.
***Opcode*** - Numerička vrednost koja označava aktivnost koja se izvršavala u vreme kada je kreiran zahtev za stvaranjem zapisa o događaju.
***Keywords*** - Ključne reči koje pomažu pri pretraživanju srodnih zapisa
***TimeCreated*** - Sistemsko vreme kreiranja zapisa.
***EventRecordID*** - Specifična oznaka tog zapisa, odnosno događaja.
***Execution*** - Sadrži oznaku procesa koji je generisao događaj.
***Channel*** - Log u koji se zapisuje događaj.
***Computer*** - Ime računara na kojem se dogodio događaj.
***Security*** - Sigurnosni podaci o aktivnom korisniku / računalu.
***EventData*** - predstavlja telo zapisa unutar kojeg se nalaze podaci
***Data*** - Podaci o samom događaju.

# 10.3 Vrste Log zapisa kod WIN.Servera 2012

**Event:** Windows OS uključuje dve kategorije event logs: *Windows Logs* and *Applications and Services Logs*.

**Windows:** Uključuje logove koji su bili dostupni kod kod ranijih verzija OS: Application, Security, i System logs. Oni uključuju i dva nova loga: Setup log i ForwardedEvents log.  Namnjeni su za čuvanje događaja iz starih aplikacija i događaje koji se odnose na čitav sistem.

**Application:** Sadrže događaje koje izazivaju različite aplikacije

**Security:** Sadrži događaje kao što su ispavni i neispravni pokušaji prijavljivanja na sistem, kao i događajima vezanim za upotrebu resursa, kao kreiranje, otvaranje ili brisanje datoteka ili drugih resursa.

**Setup:** Beleži događaje koji su vezani za setup aplikacije.

**System:** Sadrži sve događaje koje su izazvali sistemski resursi kao što su greške kod pristupa HD, memoriji i td.

**ForwardedEvents:** Beleži sve događaje izazvane od udaljenih (remote) korisnika koji su se prijavili na sistem

# 10.3 Vrste Log zapisa kod WIN.Servera 2012

**Applications and Services:** nova kategoriju logova koja beleže sve događaje koje izazivaju aplikacije ili komponente a odnose se na sistem.

**Admin:** Ovi događaji su prvenstveno usmereni ka krajnjim korisnicima, administratorima i tehničkom osoblju. Događaji koji se nalaze u admin logovima ukazuju na neki problem koji se javio u radu sistema

**Operational:** Operativni događaji se koriste za analizu i dijagnostiku problema ili pojave.

**Analytic:** Analitički događaji opisuju rad programa i ukazuju na probleme koji se ne mogu rešiti intervencijom korisnika.

**Debug:** Debug događaji se koriste od strane programera za rešavanje problema oko rada programima.

**XML-Based Infrastructure**

Informacije o svakom događaju pamte se u vidu jedne XML šeme što omogućava Event Viever da pristupi log fajlovima na jedan jednostavan način putem grafičkog formata.

# 10.4 Strategije evidentiranja događaja

- Možete da evidentirate svaki događaj, ali to je nepraktično zato što time mnogo opterećujujemo sistem – CPU i sekundarnu memoriju
- Enormno velika datoteka dnevnika – problem smeštanja i pronalaženja

1. **Isključivanje evidencije događaja** - uopšte ne uključujete evidenciju dogadaja i time smanjuje se opterečenost sistema ali i bezbednost.
2. **Uključivanje evidencije svih događaja** - evidencija svih događaja. Sistem će generisati ogroman broj događaja koji zahtevaju veoma aktivno baratanje dnevnikom bezbednosti. Kao alternativu treba razmotriti mogućnost beleženja samo neuspešnih pokušaja.
3. **Evidentiranje problematičnih korisnika** – prate se samo događaji problematičnih korisnika a tipovi događaja koje čete pratiti zavise od vrste problema i konkrtnog korisnika
4. **Praćenje administratora** - Evidencija događaja vezanih za akcije administratora omogućuje otkrivanje neovlašćenog korišćenja dozvola administratora. Bolje je da administratore kontolišete primenom delegiranja i pametnom primenom grupa i organizacionih jedinica.
5. **Evidentiranje događaja vezanih za važne datoteke i direktorijume**

# Hvala na pažnji !!!

Pitanja

? ? ?