Nastavni predmet:	**OPERACIJSKI SUSTAVI**
Vježba: 06	Uvod u dnevničke zapise
Cilj vježbe:	Upoznati učenike s sinkronizacijom vremena i dnevničkim zapisima na Microsoft Windows sustavima

PRIPREMA ZA VJEŽBU

Proučiti osnovne pojmove vezane uz dnevničke zapise na Microsoft Windows sustavima.

IZVOĐENJE VJEŽBE

Postupke, korištene naredbe i dobivene rezultate zadataka zapisivati u bilježnicu te odgovoriti na postavljena pitanja vezana uz vježbu.

Zadatak 1: Korisnički račun

Pokrenuti Windows operacijski sustav.

Ulogirati se kao korisnik koji ima administratorske ovlasti.

U korijenskom direktoriju kreirati direktorij **OS_LV06**.

Za direktorij **OS_LV06** postaviti sva prava za sve korisnike – ako to već nije postavljeno.

a) Kreirati korisnika **LOGOVI**.

Pokrenite komandnu liniju s **administratorskim ovlastima**:

U tražilicu upisati cmd->odabrati Run as administrator

U komandnu liniju upisati naredbe:

net user LOGOVI /ADD

U komandnu liniju upisati naredbu:

net user

Da li je stvoren novi korisnik?

Pogledajte trenutne postavke stvorenog računa **LOGOVI**:

net user LOGOVI

Stvorenom korisniku **LOGOVI** dodijelite lozinku **logovi**:

net user LOGOVI *

(potvrdite dodijeljenu lozinku)!

Pogledajte trenutne postavke stvorenog računa **LOGOVI**:

net user LOGOVI

Izaći iz komandne linije naredbom **exit**..

Zadatak 2: Sinkronizacija s NTP serverom

Za sinkronizaciju vremena na operacijskim sustavima Windows koriste se ugrađeni **NTP (Network Time Protocol) klijenti** koji se nalaze u samom operacijskom sustavu.

a) Pozicionirati se u:

U tražilicu upisati Control Panel -> Clock and Region -> Date and Time

Odabrati tab **Internet Time**.

b) Promijeniti postavke sinkronizacije vremena i kao **NTP poslužitelj** koristiti **CARNet NTP poslužitelj** (**zg1.ntp.carnet.hr**).

U tabu **Internet Time** odabrati opciju **Change settings**.

U bilježnicu zapisati koji se **NTP poslužitelj** do tada koristio za sinkronizaciju vremena.

Označiti kvačicom opciju **Syncronize with an Internet time server**.

U polje **Server** upisati **zg1.ntp.carnet.hr**

Kliknuti **Update Now**.

Ako je sve u redu javit će se poruka **The clock was successfully syncronized with zg1.ntp.carnet.hr** (bit će navedeno i točno vrijeme sinkronizacije).

Pozvati nastavnika!

c) Vratiti postavke sinkronizacije vremena tako da se koristi **time.windows.com** NTP poslužitelj.

U polje **Server** upisati **time.windows.com**

Kliknuti **Update Now**.

Zadatak 3: Sinkronizacija s NTP serverom iz komandne linije

a) Pokrenite komandnu liniju s **administratorskim ovlastima**:

U tražilicu upisati cmd->odabrati Run as administrator

b) Pogledati trenutno vrijeme.

U komandnu liniju upisati:

time /T

c) Pogledati kada je izvršena zadnja sinkronizacija.

U komandnu liniju upisati:

w32tm /query /status

U bilježnicu zapisati što piše pod **Last Successful Sync Time** i **Source**.

d) Promijeniti postavke sinkronizacije vremena i kao **NTP poslužitelj** koristiti **CARNet NTP poslužitelj** (**zg1.ntp.carnet.hr**).

U komandnu liniju upisati:

w32tm /config /manualpeerlist:zg1.ntp.carnet.hr /update

e) Pogledati kada je izvršena zadnja sinkronizacija.

U komandnu liniju upisati:

w32tm /query /status

U bilježnicu zapisati što sada piše pod **Last Successful Sync Time** i **Source**.

Izaći iz komandne linije naredbom **exit**.

f) Koja je veza između sinkronizacije vremena i dnevničkih zapisa?

Zapisati odgovor u bilježnicu!

Zadatak 4: Dnevnički zapisi

a) Pogledati dnevničke zapise. Pokrenuti Event Viewer:

U tražilicu upisati Event Viewer -> kliknuti na Event Viewer

b) Pogledati koliko je događaja (**Event-a**) nastalo u posljednjih sat vremena, u posljednja 24 sata te u posljednjih 7 dana.

Summary of Administrative Events->tab Last hour->tab 24 Hours->tab 7 days

U bilježnicu zapisati koliko je **Event-a** nastalo u posljednja 24 sata i poredati ih po tipu **Event-a**.

Obratiti pozornost na to koji sve tipovi **Event-a** postoje!

c) Dva puta kliknuti na **Windows Logs**.

U bilježnicu zapisati koje sve **vrste** dnevničkih zapisa spadaju pod **Windows Logs** i kolika je njihova veličina (**Size**).

d) Kliknuti na:

Windows Logs->Application

U bilježnicu zapisati od čega se sastoje pojedini događaji (**Event-i**).

e) Poredati **Event-e** po datumu i vremenu (Date and Time) i odabrati najnoviji zapis.

Pogledati detaljnije informacije o tom **Event-u**:

Desni klik na zapis->Event Properties

Što je navedeno u tabu **General**?

Od čega se sastoji tab **Details**?

f) Filtrirati **Application Log-ove** tako da prikazuju samo **Critical** i **Error** događaje (**Event-e**):

Windows Logs->Application->desni klik->Filter Current Log

U bilježnicu zapisati po čemu sve možete filtrirati dnevničke zapise.

Pod dijelom **Event Level** kvačicom označiti opcije **Critical** i **Error**.

Kliknuti **Ok**.

Uočiti da se iznad opisa **Evenata** pojavila poruka koja pokazuje koja je vrsta filtera trenutno uključena za **Application** dnevničke zapise.

g) Ukloniti postavljene filtere:

Windows Logs->Application->desni klik->Clear Filter

h) Napraviti filtriranje korištenjem **Custom View** opcije.

Windows Logs->Application->desni klik->Create Custom View

Filtrirati tako da se prikazuju samo **Critical**, **Error** i **Warning** događaji.

Pod dijelom **Event Level** kvačicom označiti opcije **Critical**, **Error i Warning**.

Kliknuti **Ok**.

U polje **Name** napisati:

Application Critical, Error i Warning.

Kliknuti **Ok**.

Uočiti da je stvoren novi **Custom View Event** pod imenom **Application Critical, Error i Warning**.

i) Pogledati defaultne postavke dnevničkih zapisa.

Windows Logs->Security->desni klik->Properties

Koje se opcije mogu promijeniti?

j) Kod **Security** dnevničkih zapisa pogledati uz što su vezani **Event-i**. Pod **Event-ima** pogledati tab **Task Category**. Komentirati u bilježnicu.

Zadatak 5: Dnevnički zapisi – Logon i Logoff

a) **Odlogirati se iz administratorskog računa**.

Ulogirati se kao korisnik **LOGOVI**.

Odlogirati se kao korisnik **LOGOVI**.

Ulogirati se kao korisnik koji ima administratorske ovlasti.

Da li su gore navedene radnje zabilježene u dnevničkim zapisima?

Pozvati nastavnika i pokazati odgovor!

b) **Odlogirati se iz administratorskog računa**.

Pokušajte se ulogirati kao korisnik **LOGOVI**, ali **dva puta namjerno unesite krivu lozinku**.

Ulogirati se kao korisnik koji ima administratorske ovlasti.

Pogledati da li su ta dva neuspješna logiranja zabilježena u dnevničkim zapisima:

Windows Logs->Security

U bilježnicu napisati komentar o tome!

Zadatak 6: Dnevnički zapisi – omogućiti dnevnički zapis o neuspješnom logiranju

a) **U tražilicu** upisati **gpedit.msc**

Pokrenuti **gpedit**.

Odabrati:

Local Computer Policy -> Computer Configuration -> Windows Settings->Security Settings->Local Policies->Audit Policy->dvoklik na Audit logon events

Označiti kvačicama opcije **Success** i **Failure**.

Kliknuti **Ok**.

b) **Odlogirati se iz administratorskog računa**.

Pokušajte se ulogirati kao korisnik **LOGOVI**, ali **dva puta namjerno unesite krivu lozinku**.

Ulogirati se kao korisnik koji ima administratorske ovlasti.

Pogledati da li su sada ta dva neuspješna logiranja zabilježena u dnevničkim zapisima:

Windows Logs->Security

U bilježnicu napisati komentar o tome!

Zadatak 7: Dnevnički zapisi i Microsoft Management Console (MMC)

Napraviti zasebni dnevnički zapis s upozorenjem (Warning) o tome koliko traje boot proces.

a) Pokrenuti **Microsoft Management Console (MMC)**:

U tražilicu upisati **mmc** i pokrenuti.

Odabrati:

File->Add or Remove Snap-ins

Odabrati **Event Viewer**.

Kliknuti **Add**.

Odabrati **Local computer**.

Kliknuti **Ok** dva puta.

Odabrati:

Console Root->dvoklik na Event Viewer (Local)->desni klik na Custom Views->odabrati Create Custom View

U otvorenom prozoru u tabu **Filter** odabrati:

Event level->kvačica na Warning

Pod **Event Logs** odabrati:

Applications and Services Logs->Microsoft->Windows->Diagnostics-Performance->staviti kvačicu na Operational

U polje **<All Event IDs>** upisati identifikacijski broj za ovaj događaj – boot proces:

Upisati broj **100**.

Kliknuti **Ok**.

U otvorenom prozoru u polje **Name** upisati:

Trajanje boot procesa

Kliknuti **Ok**.

b) Odabrati neke **Event-e (tj. Warning-e)** i pogledati koliko je trajao boot proces.

Desni klik na Event->Event Properties->Boot Duration

c) Pohraniti ove postavke za buduće korištenje.

U **Microsoft Management Console** odabrati opciju:

File->Save As

Kao direktorij za pohranu odabrati **OS_LV06**.

Pohraniti pod imenom: **Boot proces**.

Provjera znanja:

1) Čemu služi NTP poslužitelj? (1 bod)
2) Što su dnevnički zapisi? (1 bod)
3) Od čega se sastoji pojedini dnevnički zapis? (1 bod)
4) Koje vrste dnevničkih zapisa postoje? (1 bod)
5) Kako se filtriraju dnevnički zapisi? (1 bod)
6) Kako napraviti dnevnički zapis o trajanju boot procesa? (1 bod)

Ocjene: 6 bodova = 5 ; 5 bodova = 4 ; 4 boda = 3 ; 3 boda = 2 ; <3 boda = 1