Nastavni predmet:	**POSLUŽITELJSKI OPERACIJSKI SUSTAVI**
Vježba: 03	Windows Server - Nadgledanje rada
Cilj vježbe:	Upoznati učenike s metodama nadgledanja rada poslužitelja

PRIPREMA ZA VJEŽBU

Ponoviti gradivo s predavanja vezano uz nadgledanje rada poslužitelja.

IZVOĐENJE VJEŽBE

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

Vbox mrežne postavke za Windows Server i Windows 7 virtualne mašine su: Bridged adapter

Zadatak 1: Dnevnički zapisi (Event Viewer)

a) Pokrenuti **Windows Server**.

Ulogirati se kao **Administrator**.

Unijeti password: **Server_2019**

b) U donjem lijevom kutu u **taskbaru** desni klik na **Start** te odabrati i pokrenuti **Event Viewer**.

Kliknuti na **Windows Logs**.

Kliknuti tj. odabrati **Security**.

Desno će se otvoriti prozor s događajima.

c) Uočite da se u **tab-u Keywords** može vidjeti **Audit Success** i **Audit Failure**.

U **Security** zapisima se nadgleda da li je nešto uspjelo ili nije!

Nema **Grešaka, upozorenja i informacija (Errors, Warnings, Informations)**.

Bitno je odrediti što se to nadgleda!

Često je bitno vidjeti da li se korisnik ulogirao ili odlogirao.

Pogledati **tab Task Category** i uočiti postoje li kategorije **logon i logoff.**

d) **Kako se zna zašto su generirani ovi zapisi?**

Odgovor na to može se vidjeti u **Group Policy Management-u**.

Pokrenuti **Server Manager**.

Kliknuti na **Tools**.

Odabrati **Group Policy Management**.

Otvoriti će se prozor **Default Domain Policy**.

Lijevo pod **Group Policy Objects** odabrati **Default Domain Policy** te desni klik na **Edit**.

Otvoriti će se novi prozor.

Lijevo pod **Computer Configuration** dvokllik na **Policies** -> dvoklik na **Windows Settings** -> dvoklik na **Security Settings** -> dvoklik na **Local Policies** -> Kliknuti na **Audit Policy**

e) Kliknuti dva puta na **Audit account logon events**.

Otvorit će se novi prozor.

Uočiti da ništa nije označeno! Što to znači?

Kako to da su zabilježeni događaji vezani uz **logon** i **logoff** ako ništa nije definirano!

Komentirati u bilježnicu, a kao pomoć pri odgovoru kliknuti na tab Explain!

Zatvoriti **Audit account logon events** postavke.

f) Kliknuti dva puta na Audit account management.

U bilježnicu napisati koji se događaji bilježe **korištenjem Audit account management** opcije.

Kao pomoć pri odgovoru opet kliknuti na tab Explain!

g) Pokrenuti **komandnu liniju**:

Desni klik na **Start** -> odabrati **cmd**

Upisati:

auditpol /get /category:*

Komentirati u bilježnicu što se prikazalo nakon izvođenja ove naredbe!

Zadatak 2: Nadgledanje rada

a) U donjem lijevom kutu u **taskbaru** desni klik na **Start** te odabrati i **pokrenuti Event Viewer**.

Kliknuti na **Windows Logs**.

Kliknuti tj. odabrati **Security**.

Desno će se otvoriti prozor sa logovima.

b) Desno kliknuti na **Filter Current Logs**.

U polje **<All Event IDs>** upisati **4663**

Da li postoje kakvi zapisi Evenata s ovim ID-jem?

Kliknuti na **Clear Filter**!

c) Na Desktopu napraviti direktorij **Nadzor**:

Desni klik miša -> odabrati New -> odabrati Folder

Direktorij nazvati **Nadzor**.

Pozicionirati se u direktorij **Nadzor**.

d) U direktoriju **Nadzor** napraviti novu **tekstualnu datoteku** naziva **NadzorDatoteka**:

Desni klik -> odabrati New -> odabrati Text Document

Datoteku nazvati **NadzorDatoteka**.

Unijeti **proizvoljni tekst** u datototeku **NadzorDatoteka.txt**.

e) Sve unutar tog direktorija (znači i sve datoteke u njemu) želimo nadzirati.

Desni klik na direktorij **Nadzor** -> odabrati **Properties** -> odabrati **Security Tab**

U **Security Tabu** kliknuti na **Advanced**.

U prozoru **Advanced** koji se otvorio odabrati **tab Auditing**.

Uočite da pod dijelom **Auditing Entries** nema ničega!

Što to znači!

Komentirati u bilježnicu!

Kliknuti na opciju **Add**!

Kliknuti na **Select a principal**!

Otvoriti će se novi prozor.

U polje **Enter the object name to select** upisati:

Administrator

Kliknuti na **Check Names**.

Opet odabrati **Administrator** i kliknuti **Ok**.

Pod **Basic permissions** označiti kvačicom **Full Control**.

Kliknuti **OK**.

f) Što se sada nalazi pod dijelom **Auditing Entries**?

Komentirati u bilježnicu!

Kliknuti **Ok**.

Opet kliknuti **Ok**.

Zadatak 3: Nadgledanje - GP

a) Pokrenuti **Server Manager**.

Kliknuti na **Tools**.

Odabrati **Group Policy Management**.

Otvoriti će se prozor **Default Domain Policy**.

b) U dijelu **Location** desni klik na **SKOLA.LOCAL**

Označiti opciju **Enforced**!

c) Lijevo pod **Group Policy Objects** odabrati **Default Domain Policy** te **desni klik** na **Edit**.

Otvoriti će se novi prozor.

Lijevo pod **Computer Configuration dvokllik na Policies** -> **dvoklik na Windows Settings** -> **dvoklik na Security Settings** -> **dvoklik na Local Policies** -> **Kliknuti na Audit Policy**

Ovdje kliknuti na **Audit object access**.

Odabrati **tab Explain** i pročitati što piše.

U bilježnicu zapisati što označava kratica SACL!

Vratiti se na **tab Security Policy Setting**.

Označiti kvačicom **Define these policy Settings**.

Nakon toga **označiti kvačicom** i **Success** i **Failure** opciju.

Kliknuti **Ok**.

d) Resetirati Windows Server.

U bilježnicu odgovoriti s kojim razlogom je napravljen restart Windows Server-a!

Zadatak 4: Nadgledanje – GP update

a) Da li se umjesto restarta moglo napraviti sljedeće?

Pokrenite command prompt.

Desni klik na **Start -> odabrati cmd**

Upišite:

gpupdate /force

Malo pričekati!

b) **Koje poruke su se pojavile tijekom ili nakon izvođenja naredbe?**

Komentirati u bilježnicu!

Zadatak 5: Nadgledanje – događaji (Eventi)

a) Pozicionirati se u direktorij **Nadzor**.

Upisati neki novi sadržaj u datoteku NadzorDatoteka.txt koja se nalazi **u direktoriju Nadzor**.

Pohraniti promjene koje su napravljene!

b) U donjem **lijevom kutu u taskbaru desni klik na Start** te odabrati i **pokrenuti Event Viewer**.

Kliknuti na **Windows Logs**.

Kliknuti tj. odabrati **Security**.

Desno će se otvoriti prozor sa logovima.

Desno kliknuti na **Filter Current Logs**.

U polje **<All Event IDs>** upisati **4663**.

Da li sada postoje kakvi zapisi Evenata s ID-jem 4663?

c) **Komentirati u bilježnicu zašto sada postoje zapisi?**

Na što se odnose ti zapisi?

d) Kliknuti na neki od zapisa.

U bilježnicu zapisati što piše u tabu General pod dijelom Subject:

Security ID:

Account Name:

Account Domain:

Što je navedeno pod:

Object Type:

Object Name:

Kliknuti na **tab Details** i prepisati u bilježnicu sljedeće:

SubjectUserName:

SubjectUserSID:

Zadatak 6: Nadgledanje – događaji (Windows PowerShell)

a) U donjem lijevom kutu u **taskbaru** kliknuti na ikonu i pokrenuti **Windows PowerShell**.

Trebalo bi upisati naredbu:

$Event = Get-WinEvent -filterHashTable @{logname='security'; id=4663;data='**SID**' ; starttime='27/1/2019'}

U **bilježnicu komentirati** što znače (čemu služe) sljedeći dijelovi:

Get-WinEvent?

logname='security'?

id=4663?

data='SID'?

starttime='28/1/2019'?

b) Pri upisu naredbe **SID** treba zamijeniti **SID** brojem koji odgovara **administratorskom računu**.

Gdje ćete naći **SID** od **Administratora**?

c) Kada pronađete **SID upišite naredbu u PowerShell**.

(Ako ne možete pronaći odgovarajući SID pozvati nastavnika!!!!!)

Još jednom naredba koju treba upisati je:

$Event = Get-WinEvent -filterHashTable @{logname='security'; id=4663; data='**SID**' ; starttime='27/1/2019'}

d) Što se dogodilo **nakon upisa naredbe (pod pretpostavkom da nistu javljene nikakve greške)**?

(Ako je došlo do pogrešaka koje ne možete otkloniti pozvati nastavnika!!!!!)

Da li je došlo do vidljivih promjena ili je naredba pokrenula nešto što radi u pozadini?

Komentirati u bilježnicu!

e) Nakon toga u **PowerShell upisati sljedeće**:

$Event | Format-List * >> 4663.txt

Ova naredba **bi trebala stvoriti datoteku 4663.txt**.

Čemu služi **Format-List** opcija?

Gdje će se pohraniti ova datoteka i zašto?

Ima li to kakve veze s **promptom** u **PowerShell-u**?

f) **Pronaći** datoteku **4663.txt** i **pogledati što se nalazi u datoteci**!

Komentirati u bilježnicu!

POZVATI NASTAVNIKA!

Zadatak 7: Nadgledanje – uklanjanje postavki

a) Pokrenuti **Server Manager -> Tools -> Group Policy Management**

Otvoriti će se prozor **Default Domain Policy**.

U tom prozoru u dijelu **Location desni klik na SKOLA.LOCAL**

Maknuti opciju **Enforced!**

b) Lijevo pod **Group Policy Objects** odabrati **Default Domain Policy** te **desni klik na Edit**.

Otvoriti će se novi prozor.

Lijevo pod **Computer Configuration** dvokllik na **Policies** -> dvoklik na **Windows Settings** -> dvoklik na **Security Settings** -> dvoklik na **Local Policies** -> Kliknuti na **Audit Policy**

Ovdje kliknuti na **Audit object access**.

Maknuti opciju **Define these policy Settings**.

Kliknuti Ok.

c) Pokrenite **command prompt**.

Desni klik na **Start** -> odabrati *cmd*

Upišite:

gpupdate /force

Malo pričekati!

e) Maknuti postavke nadziranja direktorija **Nadzor** koji se nalazi na **Desktopu**!

Desni klik na direktorij **Nadzor** -> odabrati **Properties** -> odabrati **Security Tab**

U **Security Tabu** kliknuti na **Advanced**.

U prozoru **Advanced** koji se otvorio odabrati **tab Auditing**.

Kliknuti na **Administrator**.

Kliknuti na opciju **Remove**!

Kliknuti **Ok**.

Opet kliknuti **Ok**.

f) **Obrisati** direktorij **Nadzor i sav njegov sadržaj**!

Obrisati datoteku **4663.txt**.

Provjera znanja:

1) Čemu služi audit opcija? (1 bod)
2) Što je sve moguće nadgledati? (1 bod)
3) Kako se nadgledaju datoteke? (1 bod)
4) Kako se nadgleda logiranje korisnika? (1 bod)
5) Što Group Policy Management? (1bod)
6) Čemu služi naredba **gpupdate /force** u cmd-u? (1bod)

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