

# SADRŽAJ

|   |    |
|---|----|
| <b>1. UVOD</b> .....  | 1  |
| <b>2. UPOTREBA LOGOVA</b> .....   | 3  |
| 2.1. Upravljanje resursima .....  | 3  |
| 2.2. Detekcija upada ( <i>engl. Intrusion detection</i> ) .....                           | 4  |
| <b>3. BILJEŽENJE DOGAĐAJA</b> .....   | 7  |
| 3.1. Šta je pregledač događaja? ( <i>engl. Event Viewer</i> ) .....                       | 7  |
| 3.2. O logovanju događaja (Event Logging) .....   | 11 |
| 3.3. Tipovi događaja (Event Types) .....  | 12 |
| 3.3.1. Izbor događaja za evidentiranje .....  | 13 |
| 3.3.2. Smanjenje prekomjernog trošenja resursa ( <i>engl. Reducing overhead</i> ) .....   | 13 |
| 3.4. Elementi evidencije logovanja - ( <i>engl. Event Logging Elements</i> ) .....        | 14 |
| 3.5. Ključ evidencije događaja - ( <i>engl. Eventlog key</i> ) .....                      | 14 |
| 3.6. Izvori događaja – ( <i>engl. Event Sources</i> ) .....                               | 15 |
| 3.7. Kategorije događaja – ( <i>engl. Event Categories</i> ) .....                        | 17 |
| 3.8. Identifikatori događaja – ( <i>engl. Event Identifiers (Event Logging)</i> ) .....   | 18 |
| 3.8.1. Definicije poruka – ( <i>engl. Message Definitions</i> ) .....                     | 18 |
| 3.8.2. Stringovi za umetanje – ( <i>engl. Insertion Strings</i> ) .....                   | 19 |
| 3.9. Logovi aplikacija i servisa – ( <i>engl. Applications and Services Logs</i> ) .....  | 20 |
| 3.10. Microsoft Windows Admin Centar – ( <i>engl. Windows Admin Center</i> ) .....        | 21 |
| 3.10.1. Pregled logova događaja .....   | 22 |
| 3.11. Upotreba <i>Server Manager</i> konzole za pregled logova .....                      | 23 |
| 3.12. Korišćenje prilagođenog pregleda .....  | 26 |
| 3.13. Prijave na udaljene logove ( <i>engl. Event Log Subscription</i> ) .....            | 27 |
| 3.13.1. Omogućavanje prijave ( <i>engl. enabling subscriptions</i> ) .....                | 28 |
| 3.14. Unix/linux – bilježenje događaja ( <i>engl. Event logging</i> ) .....               | 30 |
| 3.14.1. Syslog protokol .....   | 30 |
| 3.14.2. Izvori logovanja – ( <i>engl. Logging sources</i> ) .....                         | 31 |
| 3.14.3. Syslog (Syslog-ng, rsyslog) .....   | 31 |
| 3.14.4. Osnovno logovanje sa " <i>rsyslogd</i> " .....                                    | 33 |
| 3.14.5. Klasifikacija syslog poruka – ( <i>engl. Syslog Message Clarification</i> ) ..... | 34 |
| 3.14.6. Syslog prioritet – ( <i>engl. Syslog priority</i> ) .....                         | 36 |
| 3.14.7. Interval "mark – ( <i>engl. The Mark Interval</i> ) .....                         | 38 |
| 3.14.8. Syslogd izlaz – ( <i>engl. Syslogd output</i> ) .....                             | 38 |
| 3.15. Studija slučaja – <i>syslog-ng</i> .....  | 38 |

|           |   |           |
|-----------|---|-----------|
| 3.15.1.   | Šta je syslog-ng?.....  | 39        |
| 3.15.2.   | Primjer postavljanja okruženja.....   | 40        |
| 3.15.3.   | Konfiguracije.....  | 41        |
| 3.15.4.   | Izvori logovanja.....   | 41        |
| 3.15.5.   | Lokalni syslog-ng server .....  | 42        |
| 3.15.6.   | Globalni syslog-ng server.....  | 43        |
| 3.15.7.   | Logovanje u baze podataka .....   | 43        |
| 3.15.8.   | Rješavanje problema syslog-ng servera .....                                 | 44        |
| 4.        | SNMP .....  | 47        |
| 4.1.      | Menadžeri i agenti – ( <i>engl. managers and agents</i> ) .....             | 47        |
| 4.2.      | SNMP Traps i Notifications .....  | 48        |
| 4.3.      | SNMP Get .....  | 48        |
| 4.4.      | SNMP Set.....   | 49        |
| 4.5.      | Problemi sa SNMP-om kao alternativom za evidenciju podataka .....           | 49        |
| <b>5.</b> | <b>PROMETHEUS, PROMQL, GRAFANA</b> .....                                    | <b>51</b> |
| 5.1.      | Prometheus .....  | 52        |
| 5.2.      | Grafana .....   | 56        |
| 5.3.      | PromQL – Prometheus Query Language .....                                    | 58        |
| 5.3.1.    | String literali .....   | 58        |
| 5.3.2.    | Float literali .....  | 58        |
| 5.3.3.    | Trenutni selektori vektora - ( <i>engl. Instant Vector Selector</i> ) ..... | 59        |
| 5.3.4.    | Selektori raspona vektora - ( <i>engl. Range Vector selector</i> ) .....    | 61        |
| 5.3.5.    | Vremenska trajanja .....  | 61        |
| 5.3.6.    | Modifikatori odstupanja - ( <i>engl. Offset modifier</i> ).....             | 61        |
| 5.3.7.    | @ modifikator .....   | 62        |
| 5.3.8.    | Operatori .....   | 63        |
| 5.3.9.    | Logički binarni operatori .....   | 65        |
| 5.3.10.   | Vektorsko podudaranje ( <i>engl. Vector matching</i> ) .....                | 66        |
| 5.3.11.   | Prioritet binarnog operatora .....  | 69        |
| 5.4.      | Postavljanje i korišćenje <i>Prometheus/Grafana</i> okruženja .....         | 69        |
| 5.4.1.    | Instalacija okruženja .....   | 69        |
| 5.4.2.    | Instalacija i podešavanje exportera .....                                   | 78        |
| 5.4.3.    | Node Exporter .....   | 78        |
| 5.4.4.    | Podešavanje – Prometheus i Grafana.....                                     | 81        |
| 5.4.5.    | Ručno podešavanje kontrolne table i metrike .....                           | 84        |
| <b>6.</b> | <b>ZAKLJUČAK</b> .....  | <b>88</b> |
| <b>7.</b> | <b>LITERATURA</b> .....   | <b>90</b> |