

Lokien keruu ja analysointi

Juha Immonen

Niina Villman

Projektisuunnitelma

Järjestelmäprojekti

07.02.2019

Sisällys

[1 Projektimääritys 1](#_Toc721870)

[1.1 Projektin tausta 1](#_Toc721871)

[1.2 Projektin tehtävä 1](#_Toc721872)

[1.3 Projektin tavoite ja lopputulokset 1](#_Toc721873)

[1.4 Projektin rajaus 2](#_Toc721874)

[1.5 Projektin organisaatio ja kumppanit 2](#_Toc721875)

[1.6 Projektin budjetti ja aikataulu 3](#_Toc721876)

[1.7 Projektin riskit ja projektin onnistumisen edellytykset 3](#_Toc721877)

[2 Työsuunnitelma 4](#_Toc721878)

[2.1 Kokonaistyön vaiheistus ja ajoitus 4](#_Toc721879)

[2.2 Projektinhallinnolliset menettelytavat 5](#_Toc721880)

[2.3 Muut järjestelmäprojektissa käytettävät menetelmät 6](#_Toc721881)

# Projektimääritys

## Projektin tausta

Projekti käynnistetään Järjestelmäprojekti -kurssia varten. Valitsemme aiheen, koska olemme kiinnostuneet lokienkeruusta ja sen analysoimisesta. Olemme aloittaneet projektin ja tehneet alustavaa aikataulutusta ja teknistä selvitystä. Aikaisempaa kokemusta meillä ei ole juuri tämän projektin pääkomponenteista, joita ovat Elasticsearch, Logstash ja Kibana.

Projekti antaa meille kokemusta ja osaamista keskitetystä lokien keruusta ja analysoinnista sekä siihen käytettävästä järjestelmästä. Keskitetty lokien hallinta on erittäin tärkeä osa yrityksen tietojärjestelmiä ja ongelman selvittämistä.

Projektin hallinnoimisessa käytetään Githubia. <https://github.com/niinavi/Jarjestelmaprojekti>

## Projektin tehtävä

Projektissa asennetaan lokien hallintaan, keruuseen, tallentamiseen ja analysoimiseen tarkoitettu järjestelmä (ELK Stack), jonka käyttöön tutustutaan ja analysoidaan lokidataa. Projektissa käytämme myös SaltStackia luomaan master ja minion. Master antaa komentoja minionille.

## Projektin tavoite ja lopputulokset

Projektin tavoitteena on asentaa avoimen lähdekoodin ohjelmistoja keskitettyä lokienhallintaa varten. Tavoite on tutustua järjestelmään ja analysoida lokidataa. Projektissa tulemme oppimaan tarvittavien komponenttien asentamista Linux käyttöjärjestelmälle, itse lokienhallintajärjestelmän käytön oppimista sekä lokien sisällön analysoimista. Lähtöajatuksena on järjestelmä yrityksen sisäverkossa. Tavoitteena on pystyttää järjestelmä ja kerätä lokidataa, jota voimme analysoida. Tätä palettia pystymme myös myöhemmin lähteä laajentamaan, lisäämään kohteita joista lokeja kerätään tai ottamaan edistyneemmin tietoturvaa huomioon. Tavoitteena on hallinnoida minionia masterilla StalkStackia hyödyntäen ja asentaa ohjelmistot käyttäen salt stateja.

Käytämme Githubia projektin dokumenttien hallintaan sekä käytämme Markdown kieltä dokumentoimiseen. Github löytyy täältä: <https://github.com/niinavi/Jarjestelmaprojekti> Käytämme työn seurantaan Trellon Kanban taulua, sillä haluamme tutustua ketterään työskentelyyn.

Ohjelmistokomponentteja ovat: Elasticsearch, Logstashs, Kibana, FileBeat ja StalkStack.

Projektissa syntyviä dokumentteja ovat, projektisuunnitelma, edistymisraportti, loppuraportti sekä dokumentteja teknisestä toteutuksesta ja kaaviokuva arkkitehtuurista.

## Projektin rajaus

Kerro, mitä projekti ei tee. Jos projektin tehtävä on yksiselitteisesti ymmärretty kaikkien osapuolten taholta, tämä kohta voi jäädä tyhjäksi.

## Projektin organisaatio ja kumppanit

Projektin omistaa ryhmä.

Projektityön tekijät ja ryhmän jäsenet ovat: Juha Immonen ja Niina Villman.

Projektin valvoja: Petri Hirvonen.  
Projektin sidosryhmiä ovat kurssin muut projektiryhmät.

## Projektin budjetti ja aikataulu

Projekti alkoi 4.2.2019 ja päättyy 15.4.2019. Katso tarkempi aikataulu kohdasta 2 Työsuunnitelma. Projektin resursseina ovat kolmen ryhmän jäsenen käyttämä aika ja osaaminen. Budjettina on 135 työtuntia ryhmäjäsentä kohden.

## Projektin riskit ja projektin onnistumisen edellytykset

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RISKI | Todennäköisyys | Seuraukset | Riskikerroin TxS | Hallintamenetelmät |
| Liian suuri työmäärä aikaan nähden | 2 | 2 | 4 | Aikataulutus ja organisointi |
| Osaamisen puute | 1 | 2 | 2 | Aikataulutetaan asiaan tutustumiselle tarpeeksi aikaa ja etsitään tietoa ja osaamista. |
| Ryhmän jäsenen sairastuminen | 1 | 1 | 1 | Jaetaan tietoa toisillemme ja pidetään yllä hyvää ja kattavaa dokumentaatiota. |
| Ryhmän jäsenen poisputoaminen | 1 | 1 | 1 | Jaetaan toisillemme tietoa ja pidetään yllä hyvää ja kattavaa dokumentaatiota |
| Tietoturva | 2 | 2 | 4 | Pidetään huolta perustietoturvasta kun toteutamme projektia. |

Tarvittavaa alkuosaamista ovat perusteet Linuxin käytöstä. Projektin aikana tulemme hankkimaan osaamista tarvittavien komponenttien asentamisesta, konfiguroimisesta ja itse käytöstä, lokien analysoimisesta ja tarvittavasta tietoturvasta.

# Työsuunnitelma

Projektin työvaiheita ovat:

* Kick off
* Projektisuunnitelman tekeminen
* Jokainen ryhmän jäsen tutustuu tekniikkaan, tekee testiasennuksia ja kirjoittaa lyhyen raportin tekemästään
* Manuaalinen asennus, jossa selvitämme mitä nousi esille teknisessä tutkimuksessa ja toteutetaan niiden perusteella manuaalinen asennus
* Automatisoitu asennus
* Testaamme järjestelmän toimintaa
* Toteutamme loppuraportin ja esityksen

*.*

## Kokonaistyön vaiheistus ja ajoitus

|  |  |  |  |
| --- | --- | --- | --- |
| Tehtävä # | Kuvaus | Tavoite | Ajankohta |
| 1 | Kick off | Projektin aihe ja tavoite tarkemmin | vko 6 |
| 1.1. | Projekti suunnitelma | Projektin tarkempi suunnitelma | vko 7 |
| 2 | Tekninen tutustuminen | Tarkempi tutustuminen valittuun tekniikkaan | vko 8 |
| 3 | Manuaalinen asennus | Komponenttien asennus | vko 9 |
| 4 | Automatisoitu asennus | Automatisoitu asennus | vko 10 |
| 5 | Testaus | Testattu ohjelmisto | vko 13-14 |
| 6 | PowerPont esitys | Esityksen valmistelu | vko 15 |
| 7 | Valmis projekti | Valmis projekti sekä viimeistelty projektiraportti | 15.4.2019 |

## Projektinhallinnolliset menettelytavat

Projektinhallinnan menettelytapanamme on viikoittainen palaveri koskien edistymistämme ja seuraavan viikon tarkempia työtehtäviä. Yhdistämme siten hiukan ketterää työskentelyä, sillä tulemme purkamaan tapaamisessa mitä olemme tehneet edellisellä viikolla.

Projektinhallinnassa käytämme Githubia keskitettynä dokumentaation hallinnassa. Trellon kanban taulusta jaamme tarkemmat työtehtävät jokaiselle viikolle.

Projektin edistymistä voi seurata Githubista ja Trellosta sekä teemme kirjallisen dokumentaation edistymisestä.

## Muut järjestelmäprojektissa käytettävät menetelmät

Pääpainomme on ELK Stackin asennuksessa ja lokien analysoimisessa, mutta mahdollisuuksien mukaan lähdemme myös tuomaan uusia laajennuksia.

# 