TAMPEREEN
AMMATTIKORKEAKOULU

iDRACin KÄYTTÖÖNOTTO ST III -TASON VERKKOYMPÄRISTÖSSÄ

Jarkko Yli-Lankoski

Opinnäytetyö
Marraskuu 2016
Tietojenkäsittely
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

YLI-LANKOSKI, JARKKO:
iDRACin käyttöönotto ST III -tason verkkoympäristössä

Opinnäytetyö 54 sivua, joista liitteitä 3 sivua
Marraskuu 2016

Tämän opinnäytetyön tavoitteena oli kehittää Combitech Oy:n kykyä etähallinnoida ja valvoa omia palvelimiaan. Työn tarkoituksena oli ottaa iDRAC käyttöön yhdessä Combitech Oy:n palvelimessa ja samalla kartoittaa laajemman käyttöönoton kannattavuutta. iDRAC on palvelimen emolevyyn integroitu etähallintamoduuli. Työn yhteydessä toteutettiin myös dokumentaatio, joka toimii jatkossa ohjeistuksena yritykselle iDRACin käyttöönotosta. Yritys oli ostanut palvelimiinsa aina tilauksen yhteydessä lisenssin myös iDRACia varten, mutta ajasta ja muista resursseista johtuen käyttöönottoa ei ikinä ehditty tekemään.

Käyttöönotto toteutettiin yhteen Combitechin PowerEdge 730 -mallin palvelimeen. Työssä selvitettiin ensin iDRACin ominaisuuksia ja toimintatapoja, sekä mietittiin mitä pitää ottaa huomioon ottaessa iDRACia käyttöön korkean tietoturvan verkkoympäristöön. Työssä käytiin läpi myös iDRACin teknistä toimintaa. Kaikki työssä näkyvä verkkoympäristöä kuvaava materiaali on tietoturvasyistä muokattua eikä vastaa todellista ympäristöä.

Etähallinnan rooli on merkittävä jokaisessa verkkoympäristössä, ja siihen on tärkeää olla hyvät työkalut. Kun työkaluihin yhdistetään automatisoidut ilmoitukset ja laajat mahdollisuudet laitteiden monitorointiin, saadaan voimakas kokonaisuus, jolla säästetään paljon ylläpitäjien aikaa. Työn edetessä tuli nopeasti selväksi, että iDRACista saadaan merkittävää hyötyä palvelimien ylläpitoon. Työn loppuvaiheessa tiedettiin jo varmaksi, että iDRAC halutaan ottaa käyttöön kaikissa yrityksen palvelimissa. Tulevaisuudessa laajemman käyttöönoton lisäksi selvitetään mahdollisuuksia hallita kaikkia iDRAC-moduuleja keskitetysti Dellin OpenManage Essentials -ohjelmistolla.

Asiasanat: käyttöönotto, iDRAC, verkkoympäristö, ST III, tietoturva

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

YLI-LANKOSKI, JARKKO:
Deployment of iDRAC in an ST III Network Environment

Bachelor's thesis 54 pages, appendices 3 pages
November 2016

The objective of this thesis was to enhance Combitech Oy's ability to remotely configure and monitor their own servers. The purpose of this study was to deploy iDRAC on one of the company's servers and to determine if a wider scale deployment would be beneficial. iDRAC is an out-of-band remote management module that is integrated into the server's motherboard. Advisory documentation was also created to help the company deploy the rest of their iDRACs in the future.

Combitech had been buying licenses for iDRAC with new server purchases for a while, but time and resource limitations kept them from doing a test deployment. The deployment of iDRAC was implemented on one of the Combitech's Dell PowerEdge 730 -series servers. The thesis goes over the features of iDRAC and takes a closer look at the iDRAC's technical operation before diving into the implementation phase.

As the work progressed, it became clear that iDRAC could offer great improvements to the company's current remote management model. By the end of the deployment, it was clear that the rest of the iDRACs would also be deployed on all available servers in the near future. Combitech will also look into centralized management of all their future iDRACs with the Dell OpenManage Essentials software.

Key words: deployment, iDRAC, network environment, ST III, information security

SISÄLLYS

LYHENTEET JA TERMIT

CA	Certificate Authority
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
iDRAC	Integrated Dell Remote Access Controller
IPMI	Intelligent Platform Management Interface
KATAKRI	Kansallinen turvallisuusauditointikriteeristö
Management Station	Hallintakone
NTP	Network Time Protocol
RACADM	Remote Access Controller Admin
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Suojaustaso
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing

1 JOHDANTO

Etähallinta on kriittinen osa mitä tahansa hyvin toteutettua verkkoympäristöä. Tarve etähallinalle on välttämätön vähänkin suuremman verkon ylläpidossa, ja sen hyödyt kasvavat verkkoympäristön mukana. Hyvin toteutetulla etähallinnalla säästetään huomattavasti ylläpitäjien aikaa ja resursseja.

Tässä opinnäytetyössä käydään läpi Dellin valmistaman iDRACin (integrated Dell Remote Access Controller) ominaisuuksia ja toimintaa. Lisäksi suoritetaan sen käyttöönotto yhteen Dell PowerEdge 730 -mallin palvelimeen. iDRAC on palvelimen emolevyyn integroitu etähallintamoduuli. Monet muutkin palvelimien valmistajat myyvät laitteisiinsa etähallintamoduuleja. Etähallintamoduulit tarjoavat kattavan määrän työkaluja etähallinnointiin, sekä laitteen komponenttien tilan monitorointiin. Näiden etähallintamoduulien avulla pystytään toteuttamaan toimintoja, jotka muuten vaatisivat fyysisen läsnäolon palvelimen konsolilla. Etähallintamoduulien avulla voidaan myös ennakoida komponenttien vaihdon tarvetta, tai mahdollisesti paikantaa viallinen osa.

Opinnäytetyön toimeksiantaja on Combitech Oy. Combitech on turvallisuus- ja tietoturva-alan yritys, ja se on osa turvallisuuskonserni Saab AB:ta. Opinnäytetyön tarkoitus on ottaa iDRAC käyttöön yhdessä Combitech Oy:n palvelimessa, ja samalla kartoittaa laajemman käyttöönoton kannattavuutta. Lisäksi tuotetaan yksityiskohtainen ohjeistus, jonka avulla toinen työntekijä pystyy helposti ottamaan iDRACin käyttöön jatkossa. Työn tavoite on kehittää Combitech Oy:n mahdollisuuksia etähallinnoida ja valvoa omia palvelimiaan.

Opinnäytetyössä käydään aluksi läpi asioita Combitechistä ja sen korkean tietoturvan ympäristöstä, sen jälkeen kerrotaan hieman ST-luokituksista sekä KATAKRI:sta. Seuraavaksi siirrytään itse iDRACiin. Luvussa neljä käydään läpi iDRACin taustoja, toimintaa ja ominaisuuksia. Luvussa viisi iDRACin toimintaa käydään läpi teknisestä näkökulmasta, ja tarkastellaan lähemmin erityisesti HTTP- ja HTTPS-protokollia, sillä ne ovat tärkeimmät protokollat iDRACin toiminnassa. Lopuksi luvussa kuusi käydään läpi itse käyttöönottoprosessi. Luvussa tarkastellaan iDRACin konfigurointia erityisesti web-käyttöliittymän läpi, luvussa on runsaasti kuvia käyttöönotosta.

2 COMBITECH

2.1 Yrityksestä

Combitech Oy on Suomessa toimiva turvallisuus- ja tietoturva-alan yritys. Combitechillä työskentelee Suomessa noin 70 ihmistä. Yrityksen toimipisteet sijaitsevat Tampereella, Jyväskylässä, Espoossa ja Säkylässä. Yrityksen toiminta on keskittynyt puolustussektorille ja kyberturvallisuuteen. Yrityksen huomattavin asiakas on puolustusvoimat. Asiakkaita löytyy myös yksityiseltä- ja julkiselta sektorilta. (Combitechin verkkosivut – Tietoja Combitechistä.)

Combitech Oy muodostui vuonna 2014 Saab System Oy:n nimen vaihduttua samalla, kun se liitettiin osaksi Combitech AB:ta. Combitech AB on pohjoismaissa toimiva yritys, joka toimii pääosin Ruotsissa, mutta on haarautunut myös Suomeen ja Norjaan. Yhteensä Combitech AB työllistää noin 1400 ihmistä. Yritys on itsenäinen osa turvallisuuskonserni Saab AB:ta. (Combitechin verkkosivut – Tietoja Combitechistä.)

2.2 Opinnäytetyön taustaa

Opinnäytetyön taustalla on Combitechin halu ottaa käyttöön heidän Dellin valmistamissa palvelimissaan oleva iDRAC-etähallintamoduuli, ja tämän avulla laajentaa heidän mahdollisuuksiaan etähallinnoida ja valvoa omia palvelimiaan. Yritys on jo pitemmän aikaa ostanut aina palvelimen tilauksen yhteydessä lisenssin myös iDRACille, mutta ajasta ja muista resursseista johtuen käyttöönottoa ei ikinä ehditty tekemään.

Tässä työssä iDRAC otetaan käyttöön yhteen heidän palvelimeensa, jotta voidaan kartoittaa, onko laajempi käyttöönotto kannattavaa. Lisäksi tuotetaan ohjeistus tulevaa varten, jotta toinen työntekijä pystyy helposti ottamaan iDRACin käyttöön jatkossa, mikäli näin halutaan. Yritys pystyy heti alkuun hyödyntämään iDRACin ominaisuuksia omassa verkkoympäristössään, ja mahdollisesti jatkossa myös asiakasympäristöissä.

2.3 Verkkoympäristö

Yrityksen verkkoympäristö, johon tämä opinnäytetyö toteutettiin, on korkean tietoturvan ympäristö, ja on luokiteltu suojaustasolle ST III. Korkeat turvallisuusvaatimukset johtuvat yrityksen toimialasta, sekä asiakkaista. Luvussa kolme käydään läpi ST-luokituksien (suojaustaso) merkitystä, sekä tarkastellaan KATAKRI:n (kansallinen turvallisuusauditointikriteeristö) vaikutusta tähän opinnäytetyöhön. Asiat käydään läpi, sillä niillä on erittäin keskeinen rooli yrityksen oikeassa verkkoympäristössä, jonka vuoksi ne vaikuttavat myös opinnäytetyön toteutukseen.

Edellä mainituista syistä tässä opinnäytetyössä näytettävät verkkokuvat, käytetyt IP-osoitteet ja kaikki muu verkkoympäristöä kuvaava materiaali on muokattua, eikä vastaa todellista ympäristöä. Vaikka todellista ympäristöä ei kuvata, muokkaaminen on tehty siten, että se ei hankaloita työn ymmärtämistä, tai tee työstä vähemmän pätevää.

3 ST-LUOKITUKSET

3.1 Luokitukset

Suomen viranomaistahot käyttävät salassa pidettävien dokumenttien luokitteluun neliasteista suojaustasoluokitusta. Jokaisella suojaustasolla on omat vaatimuksensa käsittelyn ja säilytyksen suhteen. Nämä vaatimukset kiristyvät suojaustason mukana. Suojaustasot ovat seuraavat:

Suojaustaso I (ST I) – Erittäin salainen
Suojaustaso II (ST II) – Salainen
Suojaustaso III (ST III) – Luottamuksellinen
Suojaustaso IV (ST IV) – Käyttö rajoitettu

Asiakirjan suojaustaso määritellään sen mukaan, kuinka suurta haittaa sen paljastumisesta tai väärinkäytöstä voisi aiheutua. Esimerkiksi ST I asiakirjan paljastuminen tai väärinkäyttö saattaisi aiheuttaa erityisen suurta vahinkoa, kun taas ST IV asiakirjan tapauksessa aiheuttaisi vain haittaa. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681.)

3.2 KATAKRI

KATAKRI on viranomaisten käyttämä työkalu yrityksien verkkoympäristöjen, ja muun turvallisuuden auditointiin. Ideana on varmistaa kohdeyrityksen valmius salassa pidettävien tietojen säilyttämiseen ja suojaamiseen.

KATAKRI sisältää aihealueittain suojaustasojen ST IV, ST III ja ST II vähimmäisvaatimukset. Salaisimman materiaalin (ST I) vaatimuksia ei ole määritelty KATAKRI:ssa. KATAKRI koostuu kolmesta osiosta. Ensimmäisessä osiossa käydään läpi turvallisuusjohtamista, toisessa fyysistä turvallisuutta ja kolmannessa teknistä tietoturvallisuutta. (KATAKRI 2015.)

3.3 Vaikutukset tähän opinnäytetyöhön

Verkon suojaustason vuoksi iDRACin etähallintayhteys pitää toteuttaa omaan verkkosegmenttiinsä, erilleen muusta verkkoliikenteestä. Tällä tavalla saadaan rajattua iDRACin liikenteen kulkemista paljon pienemmälle alueelle, sillä vain hallintakone, jolta iDRACia käytetään, tarvitsee yhteyden iDRACiin, mutta itse palvelimelle pitää päästä monesta eri sijainnista.

Erillisen verkkosegmentin lisäksi iDRACin käyttäjät rajataan minimiin. Vain ylläpitäjillä on tarve päästä käsiksi iDRACin työkaluihin ja tietoihin. KATAKRI vaatii käyttäjien oikeuksien pitämisen vain sillä tasolla, kuin on tehtävien suorittamisen kannalta välttämätöntä (KATAKRI 2015. s. 38). Mielestäni missään verkkoympäristössä ei ole kannattavaa tai tarpeellista antaa normaalien käyttäjien käyttää iDRACia.

Edellä mainittujen seikkojen lisäksi Combitech noudattaa kaikkia muitakin KATAKRI:iin on merkittyjä vaatimuksia, mutta niillä ei ole olennaista vaikutusta juuri iDRACiin.

4 iDRAC YLEISESTI

4.1 iDRACin valmistaja – Dell

Dell (nykyään Dell Technologies), perustettiin vuonna 1984 Yhdysvalloissa, Texasissa. Dell on monimuotoinen kansainvälinen teknologiayritys, joka valmistaa valtavasti erilaisia tietoteknisiä tuotteita, sekä niiden oheislaitteita. Dell työllistää nykyään arviolta 140 000 ihmistä maailmanlaajuisesti 180:ssa eri maassa. Dell on tunnettu palvelimien valmistaja, ja heidän tuotteensa ovat laajasti yrityksien käytössä ympäri maailman. (Dell Technologies Key Facts.) Myös Combitech Oy:n palvelimet ovat pääasiassa Dellin valmistamia.

Kuten monet muutkin palvelimien valmistajat, myös Dell tekee laitteisiinsa etähallintamoduuleja. Moduulit ovat nykyään valmiiksi laitteisiin integroituja. Tällaisia moduuleja ovat esimerkiksi Dellin iDRAC, IBM:n IMM (Integrated Management Module) ja HP:n iLO (Integrated Lights-Out). Eri valmistajien etähallintamoduulien ominaisuudet vaihtelevat, mutta kaikista löytyy samat keskeisimmät ominaisuudet. Näitä keskeisiä ominaisuuksia ovat esimerkiksi firmware- ja BIOS-päivityksien asentaminen etänä ja laitteiston komponenttien kunnon tarkkailu.

Dell on valmistanut DRAC-etähallintamoduuleja jo pitkän aikaa. Tällä hetkellä uusin malli on sukupolvea kahdeksan. DRAC muuttui vuonna 2008 mallisarjan kuusi mukana erillisestä komponentista suoraan emolevyyn mukaan integroiduksi. (iDRAC6 Home.) Tässä työssä käytössä oleva versio on iDRAC8 with Lifecycle Controller, johon viitataan jatkossa vain sanalla iDRAC.

4.2 Ominaisuudet ja toiminnot

iDRACin ominaisuuksia ja toimintoja on jaettu osiin ja rajattu lisensseillä. Tasoja on kolme: Basic, Express ja Enterprise. Basic-tason lisenssi on äärimmäisen rajattu, ja antaa mahdollisuuden vain valvontaan ja diagnostiikkaan. Express-tason lisenssi on edellistä laajempi, ja sisältää kriittisimmät ominaisuudet. Enterprise-tason lisenssissä kaikki omi-

naisuudet ovat auki. Jotta iDRACista saataisiin kaikki hyöty irti, käytössä kannattaisi ehdottomasti olla Enterprise-tason lisenssi. Tässä työssä käytetty iDRAC käyttää Enterprise-lisenssiä, joten kaikkia ominaisuuksia päästiin halutessa tarkastelemaan. Lisänä Express-tasoon verrattuna tulee esimerkiksi Active Directory -kirjautuminen, enemmän todennus mahdollisuuksia, virtuaalinen konsolinäkymä ja ajastetut päivitykset. (iDRAC8 Manual, s. 20.)

4.2.1 Käyttöliittymät

iDRACilla on monia eri käyttöliittymiä. Käytettävissä olevat toiminnot vaihtelevat käyttöliittymien välillä. Kaksi keskeisintä käyttöliittymää ovat web-käyttöliittymä ja RACADM (Remote Access Controller Admin). Nämä kaksi käyttöliittymää ovat eniten käytettyjä, sillä niillä pystyy tekemään kaiken konfiguraation.

RACADM on komentoriviliittymä, jolla pystyy suorittamaan samat asiat kuin web-käyttöliittymällä. Tässä työssä demonstroidaan käyttöönottovaiheessa iDRACin käyttöä sekä web-käyttöliittymällä että RACADM:lla. RACADM:n komennot ovat monimutkaisia, ja melko vaikeita käyttää ilman ohjekirjaa. RACADM:n käyttämisen etuna on mahdollisuus ajaa skriptejä. Tässä työssä skriptejä ei kuitenkaan tehdä tai oteta käyttöön, niitä katsotaan mahdollisesti tulevaisuudessa.

Web-käyttöliittymä on graafinen käyttöliittymä, jota käytetään hallintakoneen verkkoselaimen kautta. Web-käyttöliittymä on huomattavasti käyttäjäystävällisempi kuin RACADM, se on helppokäyttöinen, ja siitä näkee nopeasti yhdellä vilkaisulla palvelimen tilanteen pääkohtaisesti. Tässä työssä suurin osa konfiguroinnista tehtiin web-käyttöliittymällä.

iDRACia voi käyttää myös paikallisesti Settings Utilityä tai Lifecycle Controlleria hyödyntäen. Paikallinen käyttö on kuitenkin tarkoitettu vain alustavan käyttöönoton yhteyteen, jotta etähallinnan aloittamiseen tarvittavat verkkoasetukset saadaan konfiguroitua.

Edellä mainittujen tapojen lisäksi iDRACilla on myös erikoistuneita ja vähemmän käytettyjä käyttöliittymiä, kuten VMCLI (Virtual Media Comman Line Interface). Tätä komentorivikäyttöliittymää käytetään vain käyttöjärjestelmien asentamiseen palvelimelle.

(iDRAC8 Manual, s. 229-230.) Samat toiminnot kuitenkin löytyvät esimerkiksi sekä web-käyttöliittymästä että RACADM:sta. Näitä vähemmän käytettyjä käyttöliittymiä ei käytetty työssä, eikä niitä käydä tarkemmin läpi, sillä niiden toiminnallisuus on täysin korvattu muiden käyttöliittymien toimesta. Niitä käytettäisiin vain, mikäli muut käyttöliittymät eivät olisi käytettävissä esimerkiksi kiellettyjen protokollien vuoksi.

4.2.2 Tilanteen seuranta

iDRACin avulla voidaan seurata laitteen tilaa monipuolisesti. Tämä on yksi iDRACin keskeisimmistä ominaisuuksista. Voidaan esimerkiksi seurata palvelimen prosessorin ja muiden komponenttien kuntoa sekä lämpötiloja, ja mahdollisesti ennustaa kuluneiden osien hajoamista. Tarkkailtaviin komponentteihin kuuluvat muun muassa: prosessorit, kiintolevyt, keskusmuisti, virtalähteet, verkkokortit, USB-portit ja tuulettimet. Myös asennetun käyttöjärjestelmän tilan tarkastelu on mahdollista. (iDRAC8 Manual, s. 96, 158, 163.)

Reaaliaikaisen monitoroinnin lisäksi iDRAC pystyy seuraamaan palvelimelle tehtyjä muutoksia ja tekemään niistä lokia. iDRAC lokittaa myös oman toimintansa. Lokeilla voidaan selvittää tapahtumien kulkua tarkemmin, jotta saadaan parempi kuva tapahtuneesta. Enterprise-lisenssillä saatavilla olevalla Remote Syslog -ominaisuudella lokit voidaan lähettää erilliselle lokipalvelimelle. (iDRAC8 Manual, s. 154.)

iDRACin avulla voidaan myös selvittää syytä palvelimen kaatumiselle. iDRACin ongelmanratkontatyökaluihin kuuluvat Last Crash Screen - ja Boot Capture -ominaisuudet. Last Crash Screen säilyttää viimeisimmän kuvan palvelimen konsolinäkymästä. Joissakin tapauksissa kuva saattaa auttaa ongelman syyn jäljittämisessä. Ominaisuus vaatii, että palvelimen käyttöjärjestelmään on asennettu iDRAC Service Module -ohjelmisto. (iDRAC8 Manual, s. 85-86.) Boot Capture -ominaisuus kaappaa automaattisesti videon palvelimen konsolinäkymästä jokaisen käynnistyksen yhteydessä. Tämän ominaisuuden ansiosta palvelimen konsolinäkymän tapahtumia päästään tarkastelemaan jälkikäteen. iDRAC säilyttää videota kolmesta viimeisimmästä käynnistyskerrasta. (iDRAC8 Manual, s. 268-269.)

4.2.3 Päivittäminen

Toinen iDRACin keskimmäisistä ominaisuuksista on laitteiston firmware- ja BIOS-päivityksien asentaminen, normaalisti fyysistä läsnäoloa vaativa operaatio voidaan suorittaa täysin etänä. Päivityksiä voidaan tehdä sekä laitteistolle että iDRACille itselleen. Firmwaren päivittäminen tehdään joko web-käyttöliitymän tai RACADM:n kautta. (iDRAC8 Manual, s. 60.)

Enterprise-lisenssi mahdollistaa päivityksien ajastuksen. Tällä tavalla firmwaren päivittäminen voidaan toteuttaa helposti samanaikaisesti myös isommissa ympäristöissä. Tässä työssä päivityksiä ei ajasteta automaattisiksi, vaan niiden asennus aloitetaan manuaalisesti.

Jos firmware-päivitys epäonnistuu, tai ei jostain muusta syystä toimi odotetusti, päivitys voidaan peruuttaa ja firmware palauttaa entiselleen. Vanhan firmwaren palauttaminen on mahdollista, jos kyseessä on: BIOS, verkkokortti, virtalähde, RAID-ohjain, tai itse iDRAC. Muissa tapauksissa aikaisemman firmwaren palauttaminen ei ole mahdollista, joten päivityksien toimivuudesta ja tarpeellisuudesta täytyy olla varma. (iDRAC8 Manual, s. 68.)

4.2.4 Hälytykset

Hälytykset ovat olennainen osa iDRACin hyödyntämistä. Ilman hyvin konfiguroituja hälytyksiä laitteiden tilaa pitäisi manuaalisesti tarkastella aika ajoin. Ympäristön kasvaessa, tämä ei ole tehokas käytäntö, ja vie paljon ylläpitäjien aikaa. Hälytyksen laukaisemisesta vastuussa olevat suodattimet tulisi konfiguroida älykkäästi ilmoittamaan olennaisista asioista ylläpitäjille, jotta he voivat reagoida tilanteeseen asianmukaisesti.

Hälytyksien lähettämiseen voidaan käyttää esimerkiksi sähköpostia tai SNMP (Simple Network Management Protocol) Trap -ilmoituksia. Hälytyksien lähettäminen voidaan rajata kategorian tai vakavuuden mukaan. Tapahtumien yhteyteen voidaan asettaa automaattisesti tehtäviä toimintoja, kuten palvelimen uudelleen käynnistäminen. Yksittäisen tapahtuman yhteyteen voidaan konfiguroida vain yksi toiminto. (iDRAC8 Manual, s. 144.)

4.2.5 Virtuaalinen media ja -konsoli

iDRACin virtuaalinen konsolinäkymä mahdollistaa palvelimen käyttämisen etänä samalla tavalla kuin paikallisesti. Virtuaalista konsolia käytetään web-käyttöliittymän kautta hallintakoneelta. Ominaisuus vaati joko Javan tai ActiveX-lisäosan toimiakseen. Virtuaalinen konsoli emuloi hallintakoneen hiirtä ja näppäimistöä kuin ne olisivat paikallisesti kytkettyinä. Tämä ominaisuus on Enterprise tason lisenssin takana. Saman palvelimen virtuaalinen konsoli voi olla auki yhtä aikaa useammalla ylläpitäjällä. Myös virtuaalisen median liittäminen ja tiedostojen tuominen palvelimelle on mahdollista virtuaalisen konsolin kautta. (iDRAC8 Manual, s. 213.)

Virtuaalinen media -ominaisuus mahdollistaa hallitun palvelimen pääsyn mediaan, joka sijaitsee hallintakoneella, tai esimerkiksi jaetulla verkkolevyllä. Palvelimeen voidaan yhdistää etänä esimerkiksi CD/DVD-levyjä, USB-muisteja, tai ISO-levynkuvia. Tämä mahdollistaa ohjelmistojen ja käyttöjärjestelmien, sekä ajureiden asennuksen palvelimelle hallintakoneen kautta. Kuten virtuaalisen konsolin tapauksessa, myös virtuaalisen median käyttö vaatii Enterprise lisenssin. (iDRAC8 Manual, s. 222.)

5 iDRAC – TEKNINEN TOIMINTA

5.1 Out-of-band

iDRACin toiminta perustuu out-of-band, eli kaistan ulkopuoliseen hallinnointiin. Tällä tarkoitetaan, että iDRACilla on oma verkkoyhteys, virranhallinta, prosessori ja muisti. Omien komponenttiensa ansiosta se ei ole riippuvainen vastaavista palvelimen komponenteista, ja pystyy toimimaan vikatilanteidenkin sattuessa. Jos esimerkiksi palvelimen käyttöjärjestelmä kaatuisi, tai prosessoriin tulisi vikaa, iDRAC pystyisi edelleen normaalisti hälyttämään asiasta.

Ennen käyttöjärjestelmän käynnistymistä saatavilla olevat ominaisuudet, kuten BIOS-asetuksien muuttaminen, eivät olisi mahdollisia ilman kaistan ulkopuolista hallinnointia. iDRACin omien resurssien ansiosta palvelimen tarkkailu on mahdollista myös käynnistyksen aikana. Koska iDRAC käyttää omaa verkkoyhteyttään, pääsyä suoraan itse palvelimelle ei ole pakko antaa. Tällä tavalla voidaan rajata eri käyttäjien oikeuksia ja parantaa verkon turvallisuutta.

5.2 Management Station

Management Stationilla tarkoitetaan konetta, jolta muodostetaan iDRACiin yhteys, ja hallinnoidaan palvelinta. Tässä työssä Management Stationia kutsutaan hallintakoneeksi. Sekä Windows- että Linux-käyttöjärjestelmät ovat tuettuja hallintakoneeksi. Hallintakoneelle asennetaan ohjelmistoja käytettävien ominaisuuksien tarpeiden mukaisesti.

Web-käyttöliittymää varten koneella pitää olla yksi tuetuista selaimista asennettuna. Tuettuja selaimia ovat Internet Explorer, Firefox, Chrome ja Safari. (iDRAC8 Manual, s. 19.) Javan lisäksi web-käyttöliittymä ei vaadi toimiakseen muuta erityistä ohjelmistoa. Toisin kuin web-käyttöliittymä, RACADM ja VMCLI (Virtual Media Command Line Interface) vaativat erityisen ohjelmiston toimiakseen. Ohjelmistot tulevat iDRACin mukana ja ovat myös ladattavissa Dellin sivuilta.

5.3 iDRACin käyttämät keskeiset protokollat

iDRAC käyttää toiminnassaan useita eri protokollia esimerkiksi tiedonsiirtoon, konfigurointiin ja hälytyksiin. Tässä käydään läpi keskeisimmät protokollat iDRACin toiminnan ja tämän opinnäytetyön kannalta. HTTP- ja HTTPS-protokollat ovat tärkeimmät protokollat iDRACin toiminnassa, sillä web-käyttöliittymän toiminta perustuu niihin. Web-käyttöliittymä on iDRACin ydinosa, se on keskeisin ja eniten käytetty käyttöliittymä. Tästä syystä juuri HTTP- ja HTTPS-protokollat käydään paljon muita protokollia laajemmin läpi. Tässä luvussa avattujen protokollien lisäksi iDRAC käyttää muitakin protokollia. Protokollat joita ei mainita tässä osuudessa, käydään läpi lyhyesti käyttöönottoluvussa.

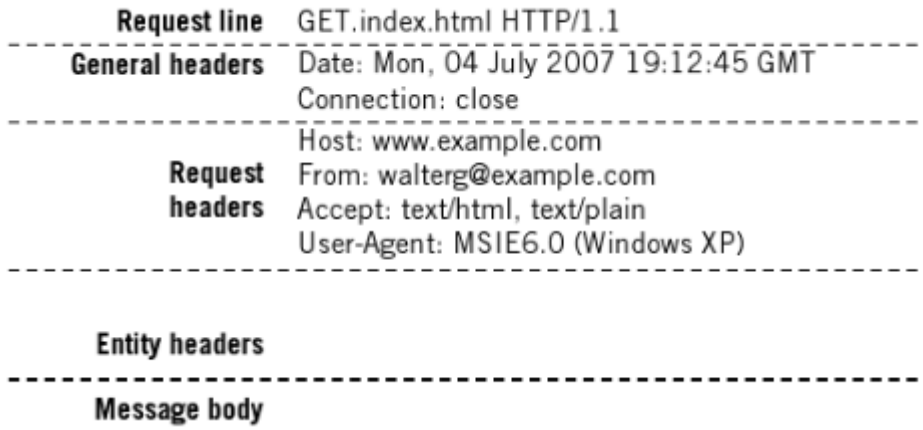
5.3.1 Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) on tiedon siirtämiseen käytetty sovellustason protokolla, jota esimerkiksi internetselaimet ja WWW-palvelimet käyttävät. Tämä protokolla on ydinroolissa internetin toiminnassa. Protokollan versio 1.0 määriteltiin alun perin RFC 1945:ssä vuonna 1996. Protokollan laajimmin käytössä oleva versio 1.1 on nykyään määritelty IETF:n (Internet Engineering Task Force) laatimissa RFC 7230-7237 standardeissa, jotka on julkaistu vuonna 2014. (RFC 1945; RFC 2616)

HTTP-protokolla perustuu pyyntöihin ja vastauksiin. Jokainen protokollan viesti on joko pyyntö tai vastaus asiakkaan ja palvelimen välillä. Käytännön esimerkki HTTP:n käytöstä: Internetselaimen (asiakkaan) muodostettua yhteyden palvelimeen, selain lähettää pyynnön, johon palvelin vastaa tilanteesta riippuen sopivalla tavalla. Palvelin saattaa esimerkiksi lähettää HTML-sivun, ääntä, kuvia, videota, tai kieltäytyä pyynnöstä. (RFC 7230)

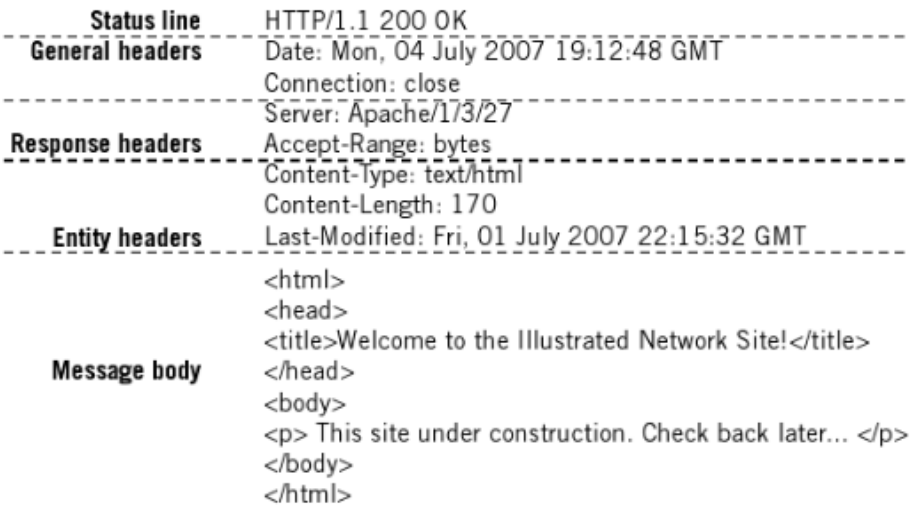
HTTP-pyyntöviestit sisältävät metodeja, jotka kertovat palvelimelle, mitä halutaan tehdä. Yleisin metodi on GET, tätä metodia käytetään resurssien lähetyksen pyytämiseen, haluttu resurssi voi olla esimerkiksi kuva tai verkkosivu (RFC 7231. Luku 4.3.1). Muita metodeja ovat HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE. Pyyntö-

viesteissä määritellään myös esimerkiksi resurssin sijainti, käytetty HTTP-versio, palvelin jolle pyyntö tehdään, ja mahdollisesti muita arvopareja. (RFC 7231) HTTP-pyyntöviestin rakenne nähdään kuvasta 1.



KUVA 1. Kuvassa esimerkki asiakkaan lähettämästä HTTP-pyyntöviestistä. (Goralski 2009, s. 574.)

HTTP-vastausviestit sisältävät vastauskoodin. Koodit ovat kolminumeroisia, ja kertovat asiakkaalle pyynnön tuloksesta. Esimerkiksi koodi 200 kertoo pyynnön onnistuneen, kun taas vastauskoodi 404 ilmoittaa, että resurssia ei löydetty. Esimerkki HTTP-vastausviestistä on nähtävissä kuvassa 2. Vastausviestit voivat pyyntöjen tapaan sisältää otsakkeita, joissa haluttuja arvopareja voidaan määritellä. (RFC 7231 Luku 6.) Vastausviestit sisältävät pyynnön onnistuessa pyydetyn resurssin.



KUVA 2. Kuvassa esimerkki palvelimen lähettämästä HTTP-vastausviestistä. (Goralski 2009, s. 574.)

HTTP-protokolla käyttää yhteyksiin oletuksena TCP (Transmission Control Protocol) -porttia 80. Joissakin harvinaisemmissa tapauksissa sovelluspalvelimet saattavat käyttää porttia 8080. (IANA)

HTTP on yhteydetön protokolla. Yhteydettömyys tarkoittaa sitä, että asiakkaan lähetettyä pyynnön palvelimelle, asiakas katkaisee yhteyden, ja jää odottamaan palvelimen vastausta. Palvelimen käsiteltyä pyynnön, palvelin muodostaa yhteyden uudelleen, ja välittää vastauksen. HTTP on myös niin sanottu tilaton protokolla. Tilattomuudella tarkoitetaan, että asiakas ja palvelin ovat tietoisia toisistaan vain pyynnön ja vastauksen ajan. Koska HTTP on tilattomuuden lisäksi myös yhteydetön protokolla, tietojen säilyttäminen ei onnistu istuntojen välillä. Tämän ympäri voidaan kuitenkin päästä esimerkiksi tallentamalla evästeitä. (RFC 7234.)

iDRAC käyttää HTTP-protokollaa viestintään hallintakoneen web-käyttöliittymän ja itsensä välillä. Tässä työssä ei kuitenkaan käytetä pelkkää HTTP-protokollaa, vaan sen salattua versiota HTTPS:ää, joka on HTTP- ja TLS (Transport Layer Security) -protokollien yhdistelmä.

5.3.2 Transport Layer Security (TLS) ja Secure Sockets Layer (SSL)

Transport Layer Security -protokolla (TLS) on uudempi versio Secure Sockets Layer -protokollasta (SSL). TLS- ja SSL-protokollia käytetään yhdessä muiden protokollien kanssa salaamaan verkkoliikennettä. Tunnetuin esimerkki tästä on HTTPS-protokolla, jota käytetään internetissä erittäin laajasti turvaamaan selaamista asiakkaan ja web-palvelimen välillä. TLS-protokolla on jatkumoa SSL-protokollalle. SSL-protokollasta on kolme eri versiota: SSL 1.0, SSL 2.0 ja SSL 3.0. TLS-protokollasta on myös kolme eri versiota: TLS 1.0, TLS 1.1 ja TLS 1.2. (Oppliger 2009, s. 75, 133.) Näiden lisäksi TLS-versio 1.3 on parhaillaan kehitteillä.

TLS- ja SSL-protokollat perustuvat asiakkaan ja palvelimen väliseen kättelyyn. Kättelyn aikana vaihdetaan tietoja, todennetaan toisen osapuolen oikeellisuus sertifikaattien, eli varmenteiden avulla, ja sovitaan käytetystä salaustavasta. Kättelyn onnistuessa asiakkaan

ja palvelimen välille muodostetaan salattu yhteys. (Oppliger 2009, s. 94-97.) Toisin sanoen tämän prosessin avulla voidaan varmistua toisen osapuolen identiteetistä, ja varmistaa yhteyden olevan salattu. Tätä prosessia käydään läpi tarkemmin kappaleessa 5.3.3.

5.3.3 Hypertext Transfer Protocol Secure (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) on HTTP- ja TLS-protokollien yhdistelmä, jota käytetään salattuun tiedonsiirtämiseen verkossa. Protokolla toimii kuten HTTP-protokolla, mutta hyödyntää TLS-protokollan toimintaa salatun yhteyden muodostuksessa. Protokollasta käytetään usein myös nimitystä HTTP Over TLS. HTTP-protokollan liikenne ei ole sellaisenaan salattua, ja tämän vuoksi se on haavoittuvainen muun muassa man-in-the-middle (MitM) -hyökkäyksille, ja muulle liikenteen kaappaamiselle. HTTPS-protokollan kehittämisen taustalla oli tarve salata verkkoliikennettä arkaluontoisen tiedonsiirron yleistyessä. (RFC 2818.)

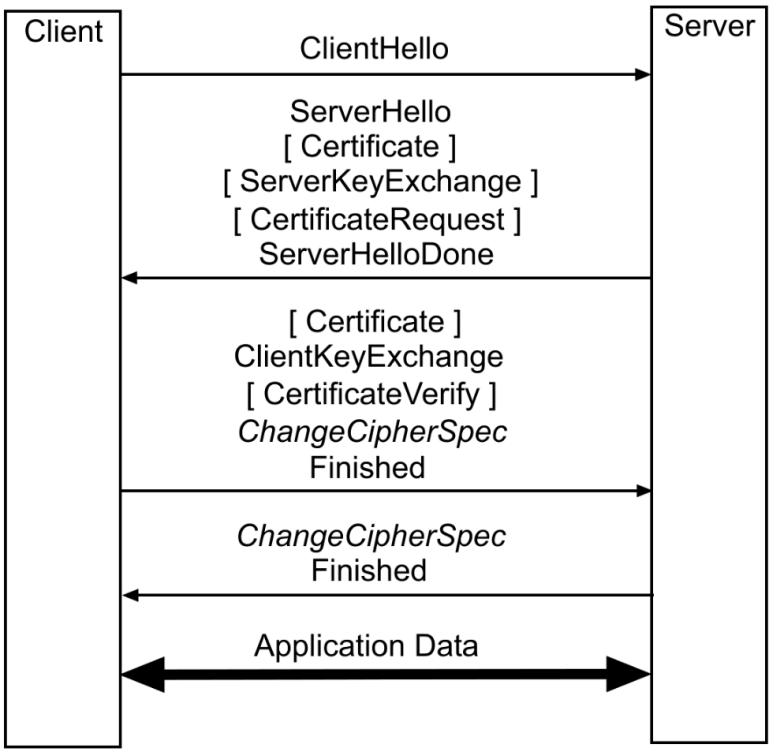
HTTPS-protokollaa käytetään laajasti internetissä. Selaimen ja palvelimen välisen liikenteen ollessa salattua, voidaan olla varmoja, ettei tietoja päädy vääriin käsiin. Verkkopankit ja muu maksuliikenne ovat hyviä esimerkkejä, joissa asiakkaan pitää olla varma palvelimen identiteetistä, oikeellisuudesta ja yhteyden salauksesta. Myös iDRAC hyödyntää HTTPS-protokollaa itsensä ja hallintakoneen välillä. Web- ja Remote RACADM -käyttöliittymien liikenne käyttää HTTPS-protokollaa liikenteen kuljettamiseen. (iDRAC8 Manual, 104.) HTTPS-protokollan oletusportti on 443. (IANA)

Asiakkaan muodostaessa HTTPS-yhteyden palvelimelle, asiakas aloittaa TLS-kättelyn. Oppliger (2009, s. 95) on kuvannut kättelyn vaiheet kuvassa 3. Ensimmäisenä asiakas lähettää palvelimelle ClientHello-viestin. Palvelin vastaa asiakkaalle tilanteesta riippuen useammalla viestillä. Palvelin lähettää asiakkaalle takaisin ServerHello-viestin, oman sertifikaattinsa ja ServerHelloDone-viestin. Palvelin saattaa myös pyytää asiakasta lähettämään oman sertifikaattinsa. Lisäksi palvelin saattaa erikoistapauksissa lähettää asiakkaalle myös avainten vaihtoon liittyvän viestin, mutta tässä esimerkissä oletetaan käytettävän RSA:ta avaintenvaihtoon, joten tälle viestille ei ole tarvetta, sillä asiakas saa palvelimen julkisen avaimen palvelimen sertifikaatista. ClientHello- ja ServerHello-viestien jälkeen asiakas ja palvelin tietävät käytetyn protokollaversion, liikenteen salaustavan,

sekä istunnon tunnuksen, jonka avulla tiedetään, mikä istunto tarvittaessa palautetaan. (Oppliger 2009, s. 95-96.)

Jos asiakas luottaa palvelimen sertifikaattiin, se generoi premaster-salaisuuden, salaa sen palvelimen julkisella avaimella, ja lähettää palvelimelle. Asiakas lähettää myös oman sertifikaattinsa, mikäli palvelin pyysi sitä edellisessä vaiheessa. Asiakas generoi lopullisen, salaamiseen käytetyn master-salaisuuden generoimansa premaster-salaisuuden avulla. Lopuksi asiakas ilmoittaa palvelimelle olevansa valmis aloittamaan salaamisen. (Oppliger 2009, s. 112, 114.)

Kun palvelin vastaanottaa premaster-salaisuuden asiakkaalta, se purkaa salauksen omalla yksityisellä avaimellaan ja generoi asiakkaan tapaan master-salaisuuden. Nyt kummallakin osapuolella on tiedossaan master-salaisuus, jonka avulla liikenteen salaaminen suoritetaan istunnon ajan. Lopuksi palvelin ilmoittaa asiakkaalle olevansa valmis aloittamaan salatun liikenteen lähettämisen. Tämän jälkeen TLS-kättely on valmis, ja salattu tiedonsiirto osapuolien välillä voi alkaa. Jos missään kättelyn vaiheessa toisen osapuolen vastaus ei tyydytä toista, istunto lopetetaan. (Oppliger 2009, s. 114-115.)



KUVA 3. Kuvasta nähdään SSL-kättelyn vaiheet ja lähetetyt paketit. (Oppliger 2009, s. 95.)

5.3.4 Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) on sähköpostin lähettämiseen käytetty protokolla. Protokolla on alun perin vuodelta 1982, ja määritellään nykyään RFC 5321:ssä. SMTP:n tarkoitus on kuljettaa sähköpostit perille luotettavasti ja tehokkaasti. Protokollan tärkeimpiin ominaisuuksiin kuuluu kyky kuljettaa sähköposteja usean eri verkon yli. (RFC 5321. Luku 1.1) SMTP-protokolla käyttää oletuksena porttia 25. (IANA)

Tässä opinnäytetyössä iDRAC konfiguroidaan käyttämään SMTP-protokollaa sähköpostin lähettämiseen. Tämä on tärkeää, sillä iDRAC voidaan asettaa lähettämään sähköposteja hälytyksistä, varoituksista ja muista tapahtumista. Jos esimerkiksi palvelin, jossa iDRAC on konfiguroitu, kuumenisi tietyn rajan yli, iDRAC lähettäisi siitä sähköpostia ylläpitäjille, ja he voisivat tulla korjaamaan tilanteen.

5.3.5 Secure Shell (SSH)

Secure Shell (SSH) on salattuun tiedonsiirtoon käytetty protokolla. Yleisimpiin käyttötarkoituksiin kuuluvat tiedostojen siirto ja laitteiden etähallinnointi turvallisesti verkon yli. Protokollan on alun perin kehittänyt suomalainen Tatu Ylönen vuonna 1995, jonka jälkeen sen käyttö levisi nopeasti. (SSH – Company Overview) Protokollasta on myöhemmin tullut uudempia versiota. Versio 2 oli ensimmäinen versio, jonka IETF määritteli RFC standardeissa 4250-4256, 4335, 4344 ja 4345 vuonna 2006. SSH-protokolla käyttää oletuksena porttia 22. (IANA)

iDRACin etähallinta on mahdollista SSH-protokollan avulla. Tässä työssä SSH-protokollaa käytetään turvallisen yhteyden muodostamiseen iDRACin ja hallintakoneen välille, ja sen jälkeen RACADM-komentojen käytön demonstroimiseen. (iDRAC8 Manual. Sivu 24.)

5.4 iDRACin sertifikaatit

iDRAC käyttää sertifikaatteja todistaakseen oman luotettavuutensa ja oikeellisuutensa yhteyttä muodostettaessa. Oletuksena iDRACilla on käytössään iDRACin itsensä allekirjoittama 128-bittinen SSL-sertifikaatti. iDRACilla on mahdollista tehdä sertifikaatin allekirjoitus pyyntö (CSR), joka voidaan lähettää luotetulle sertifikaattien allekirjoittajalle allekirjoitusta varten. Tässä työssä sertifikaattien allekirjoittamiseen käytetään Combitechin omaa CA:ta (Certificate Authority).

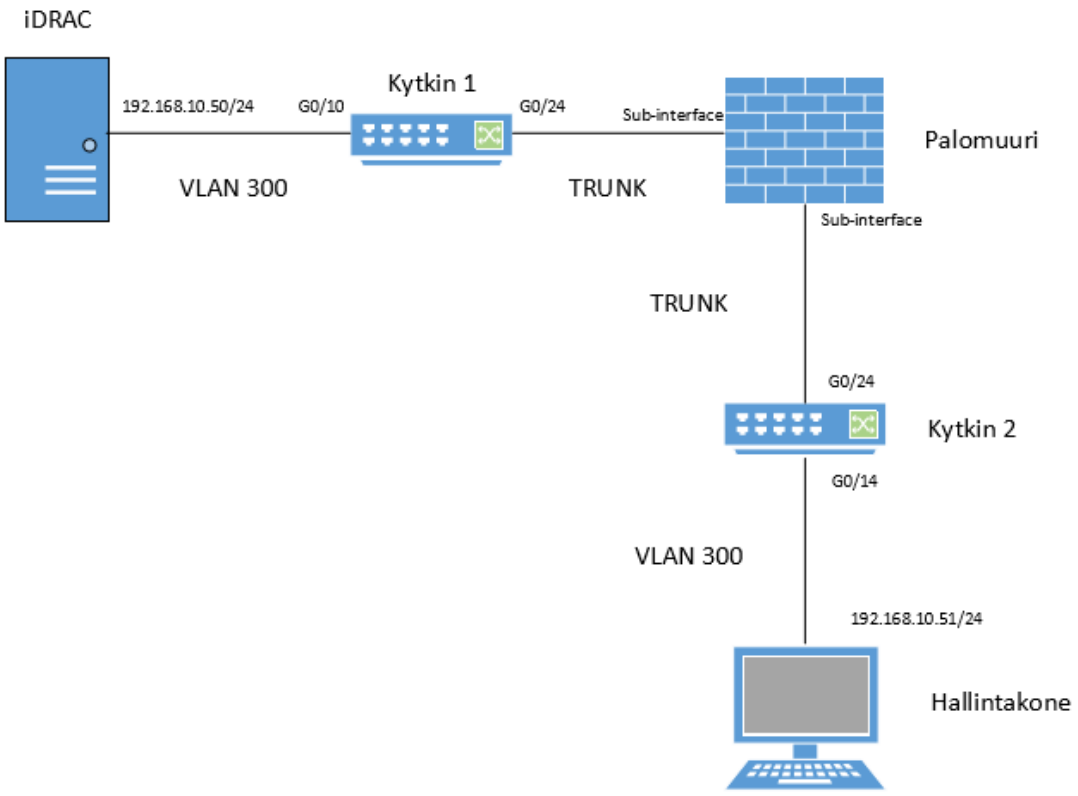
Tarve itse allekirjoittamisen tai CA:n käyttämisen välillä määräytyy iDRACin käyttötavan mukaan, sillä eri kirjautumistavoilla on eri vaatimukset käytetyn sertifikaatin suhteen. Esimerkiksi Active Directory -kirjautuminen vaatii luotetun CA:n käyttämistä, kun taas paikallisten käyttäjätunnuksien käyttö onnistuu myös itse allekirjoitetulla sertifikaatilla. Jos vain mahdollista, on suositeltua käyttää CA:n allekirjoittamaa sertifikaattia mieluummin kuin itse allekirjoitettua, tällä tavalla sertifikaatit pysyvät keskitetysti hallinnassa. Itse allekirjoitetuissa sertifikaateissa on myös tietoturvaheikkous yhteyttä ensimmäistä kertaa muodostettaessa. Ensimmäisellä kerralla sertifikaattia ei ole vielä lisätty luotetuksi, ja joku voisi mahdollisesti esiintyä laitteena johon yhteyttä muodostetaan.

6 TOTEUTUS

6.1 Verkkosegmentin suunnittelu ja toteuttaminen

Ensimmäinen vaihe käyttöönotossa on iDRACin verkkosegmentin suunnittelu ja toteuttaminen. iDRAC tarvitsee oman virtuaalisen lähiverkkonsa (VLAN), jotta liikenteen kulku saadaan rajattua turvallisuusvaatimusten mukaisesti vain tarvittuihin paikkoihin. Kytkimet joita työssä käytetään, ovat Ciscon 2960G -sarjaa. Työssä käytettävää palomuurin mallia ei voida tietoturvasyistä julkaista. Palomuurille tehtävät konfiguraatiot käydään kuitenkin yleisesti läpi.

Alla olevasta verkkokaaviosta (kuva 4) nähdään vasemmalla palvelin, johon iDRAC on asennettu. iDRAC on yhdistetty kytkimeen, jonka iDRACille menevä portti on konfiguroitu virtuaaliseen lähiverkkoon 300. Kytkimeltä yhteys jatkuu trunk-portista palomuurille, jossa määritellään sallitut protokollat, sekä lähde - ja kohde IP-osoitteet. Palomuurilta edetään toiselle kytkimelle trunk-porttiin. Myös hallintakoneelle menevä kytkimen portti on konfiguroitu virtuaaliseen lähiverkkoon 300.



KUVA 4. Muokattu kuva verkon topologiasta.

6.1.1 Kytkimien konfigurointi ja palomuurisääntöjen luonti

iDRACin ja hallintakoneen kytkinportit konfiguroitiin antamalla seuraavat komennot:

-**Enable** -komento vie kytkimen enable-tilaan.
-**Conf t** -komento vie kytkimen konfigurointitilaan.
-**Interface <portti>** -komento valitsee konfiguroitavan kytkinportin.
-**Switchport mode access** -komento vie portin access-tilaan.
-**Switchport access vlan <VLAN ID>** -komento määrittää virtuaalisen lähiverkon, johon portti kuuluu.

Kytkimiltä palomuurille menevät portit konfiguroitiin antamalla seuraavat komennot:

-**Enable** -komento vie kytkimen enable-tilaan.
-**Conf t** -komento vie kytkimen konfigurointitilaan.
-**Interface <portti>** -komento valitsee konfiguroitavan kytkinportin
-**Switchport mode trunk** -komento vie portin trunk-tilaan.
-**Switchport trunk allowed vlan <VLAN ID>** -komento määrittää trunk-portissa kulkemaan sallitut virtuaaliset lähiverkot

Palomuurille luotiin sääntö, joka sallii HTTPS- ja SSH-protokollien kulkemisen hallintakoneelta iDRACille, lisäksi avattiin portti 5900 virtuaalista konsolia varten. iDRACia varten luotiin myös säännöt sallimaan SMTP-protokolla iDRACilta sähköpostipalvelimelle, sekä NTP (Network Time Protocol) -protokolla iDRACilta NTP-palvelimelle.

6.2 Alustava käyttöönotto

iDRACin alustavalla käyttöönotolla tarkoitetaan paikallisesti tehtävää konfiguraatiota ennen etäyhteyden muodostamista. Tämä tarkoittaa pääasiassa verkkoasetuksien määrittämistä, mutta myös muita asetuksia pääsee haluttaessa muuttamaan jo tässä vaiheessa. Alustavaa käyttöönottoa pääsee tekemään painamalla F2-nappia palvelinta käynnistäessä. Tässä työssä palvelin, johon iDRAC otettiin käyttöön, on PowerEdge 730 -mallia.

Kyseessä oleva palvelin on täysin uusi, ja se otettiin käyttöön ensimmäistä kertaa tämän työn yhteydessä, joten iDRACin verkkoasetukset määriteltiin paikallisesti ennen etäkäytön aloittamista. Tässä työssä iDRACin IP-osoite määriteltiin staattisesti, mutta myös dynaaminen osoitteen antaminen on mahdollista DHCP (Dynamic Host Configration Protocol) -protokollan avulla. Verkkoasetuksien lisäksi alustavassa käyttöönotossa vaihdettiin root-käyttäjän oletussalasana, ja annettiin iDRACille sen oikea laitenimi.

Verkkoasetuksia ei ole välttämätöntä määritellä paikallisesti etukäteen, sillä iDRAC käyttää toimintaansa oletuksena IP-osoitetta 192.168.0.120/24. Tämä tarkoittaisi kuitenkin sitä, että verkkolaitteet pitäisi väliaikaisesti konfiguroida sallimaan iDRACin oletus IP-osoite, joka ei olisi tietoturvan kannalta järkevää. Varsinkaan niissä tapauksissa, joissa iDRACia käytetään turvattoman verkon yli, tämä ratkaisu ei tule kyseeseen, sillä iDRACille ei ole vielä tehty oikeita käyttäjätunnuksia, joten se käyttää oletuskäyttäjää ja -salasanaa. Kun verkkoasetukset on määritelty iDRACille ja muille verkkolaitteille, etäkäyttö voi iDRACin puolesta alkaa.

6.3 Hallintakoneen konfiguraatio

iDRACille asennettiin etukäteen virtuaalinen hallintakone, jonka käyttöjärjestelmä on Windows 7 Enterprise. Työssä päätettiin asentaa yksi keskitetty hallintakone iDRACia varten. Tältä koneelta voidaan hallinnoida myös kaikkia tulevaisuudessa asennettavia iDRAC-moduuleja. Ylläpitäjien kesken päätettiin, että tiimin koon johdosta useammalle ylläpitäjälle tuskin tulee tarvetta hallita iDRAC-moduuleja yhtä aikaa, joten yksittäinen hallintakone on riittävä ratkaisu.

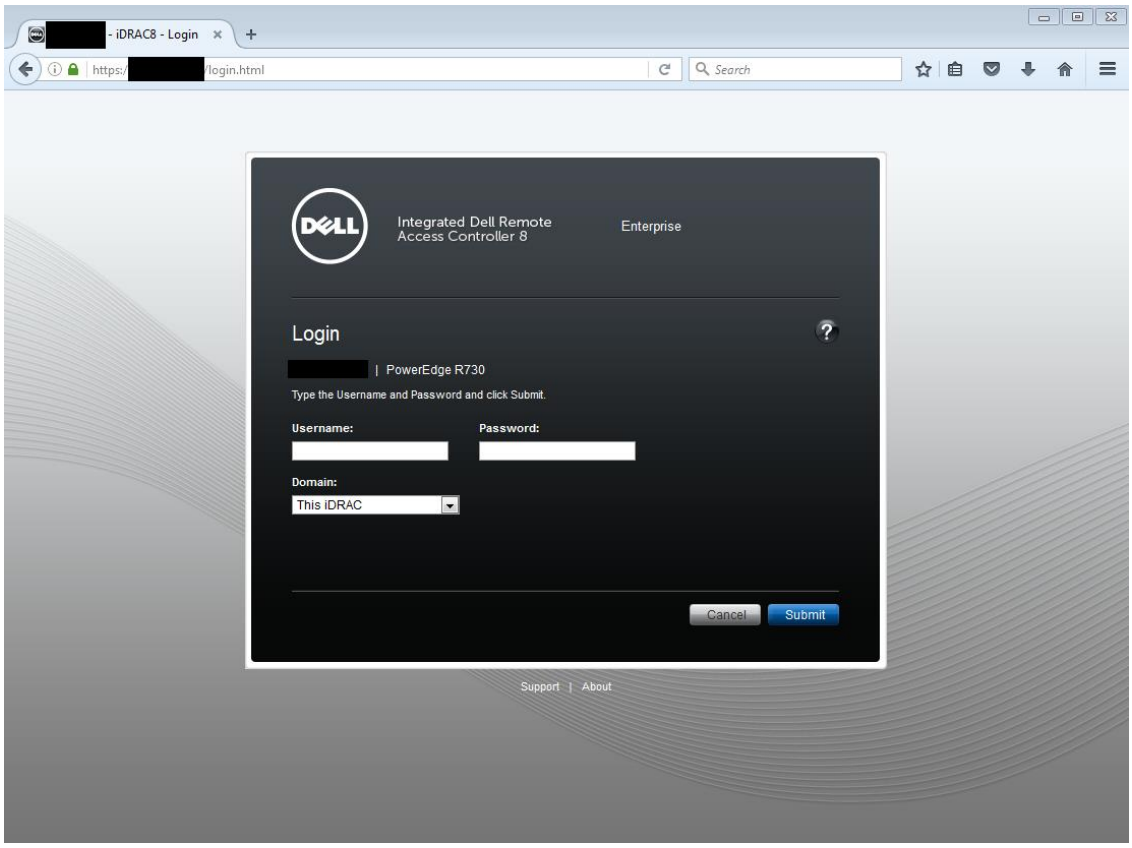
Toinen vaihtoehto olisi ollut luoda jo olemassa oleville, muiden verkkolaitteiden konfiguroimiseen käytetyille hallintakoneille ylimääräinen verkkokortti, joka olisi yhdistettynä iDRACille luotuun verkkosegmenttiin. Uusi verkkokortti voitaisiin ottaa käyttöön aina tarvittaessa. Verkkokorttien luominen, ja niiden käyttöönotto tarpeen mukaan katsottiin kuitenkin isommaksi vaivaksi, kuin yhden uuden keskitetyn hallintakoneen luominen.

Jos tulevaisuudessa ilmenee, että useammalla ylläpitäjällä on tarvetta päästä käyttämään iDRAC-moduuleja yhtä aikaa, pystytään jo olemassa oleville virtuaalisille hallintakoneille nopeasti luomaan yksi verkkokortti lisää. Mahdollisen muutoksen tekee nopeaksi myös se, että kaikki tarvittavat verkkolaitteille tehtävät asetukset ovat jo tiedossa tämän opinnäytetyön pohjalta.

Hallintakoneelle asennettiin Mozilla Firefox verkkoselain, sekä Javan uusin versio iDRACin web-käyttöliittymää ja virtuaalista konsolia varten. Lisäksi koneelle asennettiin PuTTY, joka on SSH-asiakasohjelma. PuTTY-ohjelmaa käytetään SSH-yhteyden muodostamiseen iDRACille, ja sen jälkeen RACADM komentojen ajamiseen.

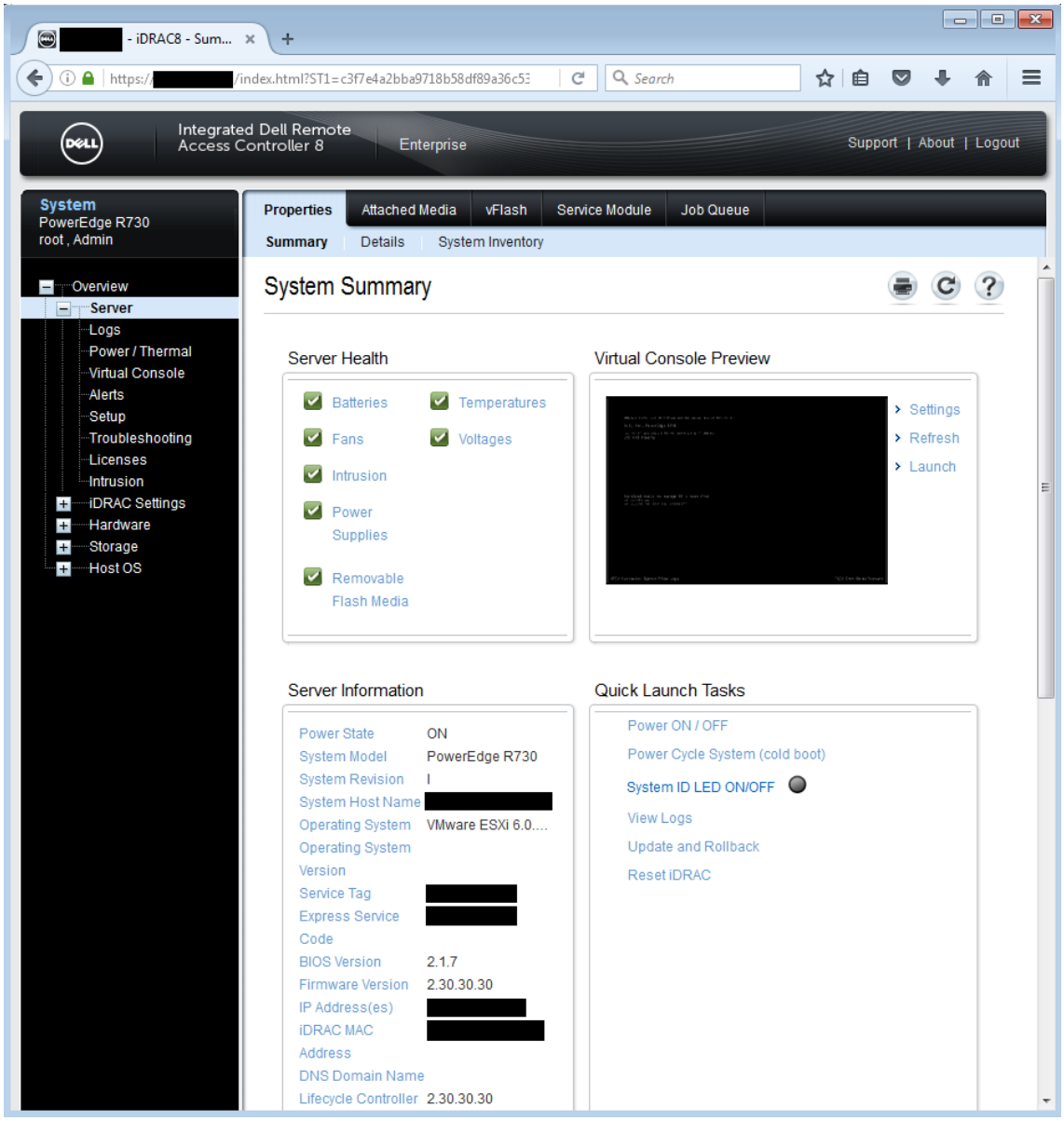
6.4 Asetuksien konfigurointi hallintakoneelta

Kun iDRACin alustavat asetukset ovat konfiguroitu, ja hallintakoneen valmistelu tehty, etähallinta voidaan aloittaa. iDRAC-moduuliin otetaan yhteyttä selaimella laittamalla iDRACin IP-osoite hakukenttään. Ensimmäisenä aukeaa kirjautumisnäkymä (kuva 5).



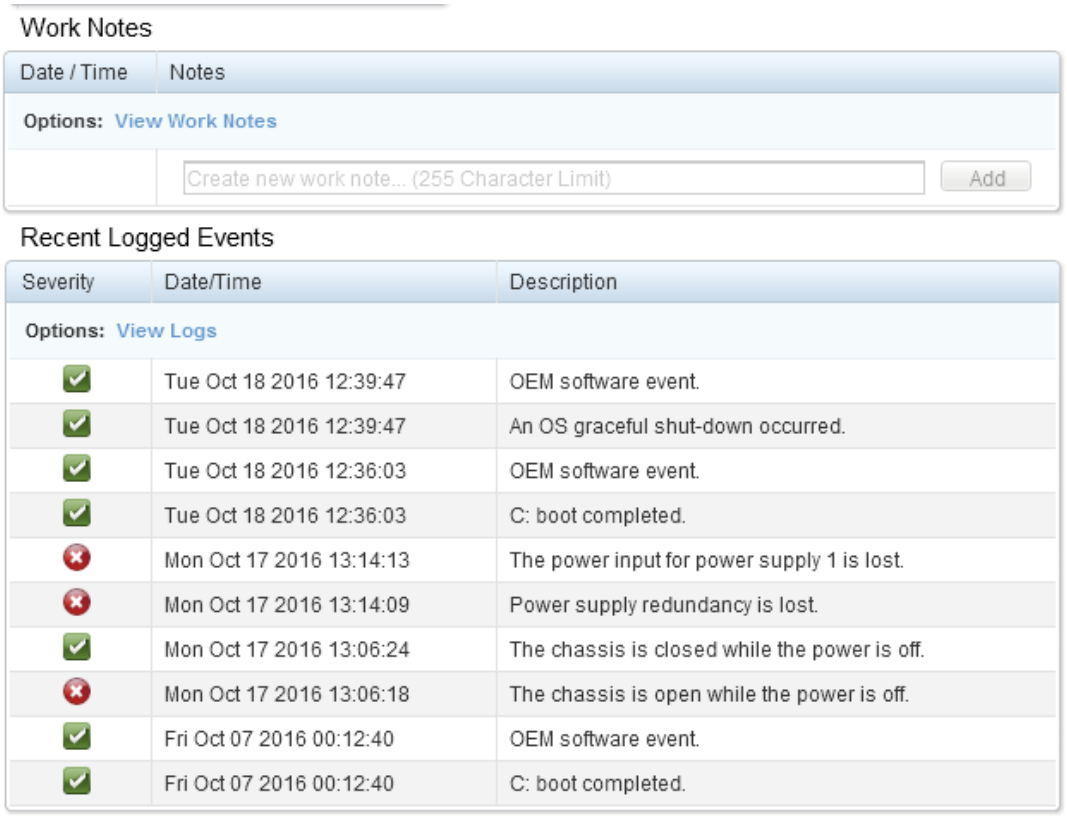
KUVA 5. Kuvakaappaus iDRACin web-käyttöliittymän kirjautumisruudusta. Kuvasta poistettu IP-osoite ja laitenimi.

Sisäänkirjautumisen jälkeen iDRACin Overview-näkymä aukeaa (kuva 6). Tästä näkymästä nähdään nopeasti yhdellä vilkaisulla palvelimen tilanne pääpiirteittäin. Näkymästä nähdään muun muassa palvelimen komponenttien yleistilanne, tämän hetken näkymä virtuaalisesta konsolista, tietoja palvelimesta, sekä linkkejä yleisimpiin toimintoihin.



KUVA 6. Kuvakaappaus Overview-näkymästä. Kuvasta poistettu palvelimen tietoja.

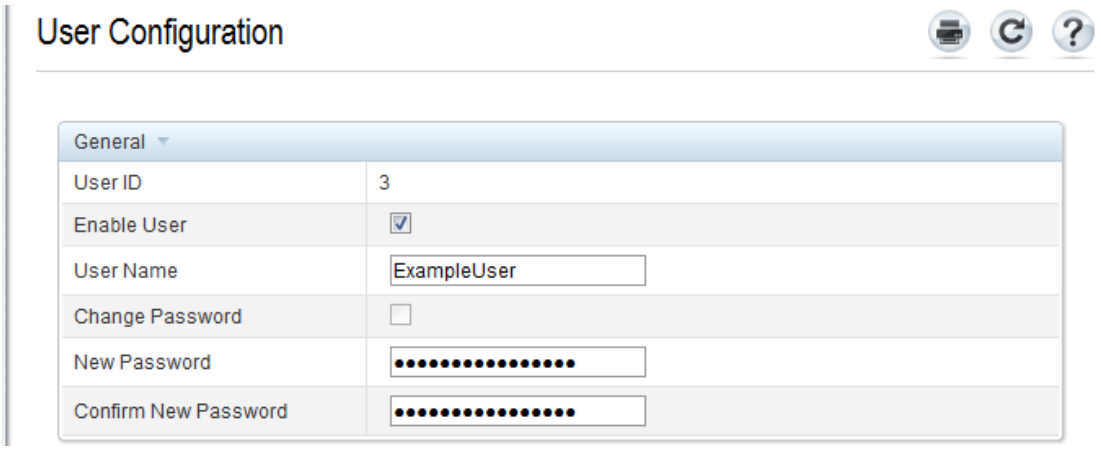
Lisäksi alempana nähdään myös viime aikaiset tapahtumat. Kuvassa 7 näkyvään Work Notes -osioon voidaan jättää merkintöjä ja viestejä muille ylläpitäjille. Tämä ominaisuus olisi hyödyllinen, jos ylläpitäjiä olisi paljon. Myös yksittäisten tapahtumien yhteyteen voidaan jättää kommentteja.



KUVA 7. Kuvakaappaus Overview-näkymästä. Kuvassa viimeisimmät tapahtumat.

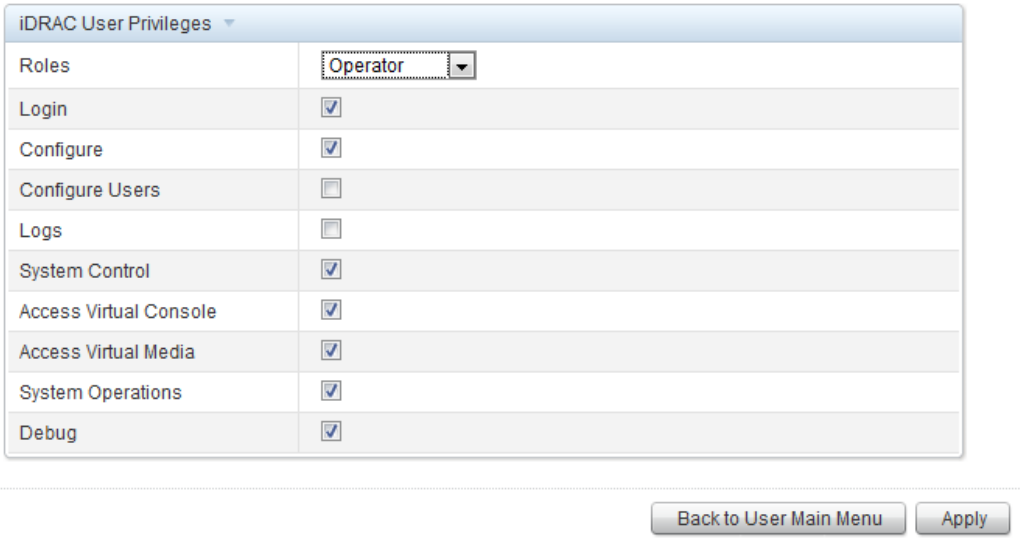
6.4.1 Käyttäjätunnuksien luominen web-käyttöliittymällä

Ensimmäinen konfiguroitava asia on lopullisten käyttäjätunnuksien luominen. iDRAC Settings-kohdan alta löytyvältä User Authentication -välilehdeltä (kuva 8) nähdään tämän hetken käyttäjät ja heidän oikeutensa. Uusien käyttäjien luominen tapahtuu samalta sivulta. Uudelle käyttäjälle määritellään nimi ja salasana.



KUVA 8. Kuvakaappaus User Configuration -välilehdeltä. Kuvassa uuden käyttäjän luonti.

Lisäksi käyttäjälle määritellään käyttöoikeudet. Kuvasta 9 nähdään käyttöoikeuksien antamiseen käytettävä näkymä. Valittavissa on kolme valmiiksi määriteltyä tasoa. Ensimmäinen taso on Read Only, joka antaa oikeudet vain katseluun, mitään muutoksia ei pysty tekemään. Toinen taso on Operator, tämä taso antaa oikeudet kaikkeen muuhun, paitsi lokien poistoon ja käyttäjien konfiguroimiseen. Kolmas ja viimeinen taso on Administrator, jolle on myönnetty kaikki oikeudet. Käyttöoikeuksia ei ole pakko valita näistä kolmesta tasosta, oikeuksia voi tarpeen mukaan kustomoida itse.



KUVA 9. Kuvakaappaus käyttäjän oikeuksien määrittelystä. Kuvassa Operator-tason oikeudet.

6.4.2 Käyttäjätunnuksien luominen komentorivillä

Web-käyttöliittymän lisäksi käyttäjiä voidaan konfiguroida komentoriviltä RACADM:n avulla, tämä on kuitenkin paljon monimutkaisempi tapa verrattuna web-käyttöliittymään. Käyttäjän luominen komentorivillä on demonstroitu kuvassa 10. RACADM-komentoihin saa kuitenkin apua help-parametrilla. Tässä työssä käytettiin PuTTY-ohjelmaa muodostamaan SSH-yhteys iDRACille. Yhteyden muodostamisen ja sisäänkirjautumisen jälkeen käyttäjän luomiseen käytetään seuraavia komentoja:

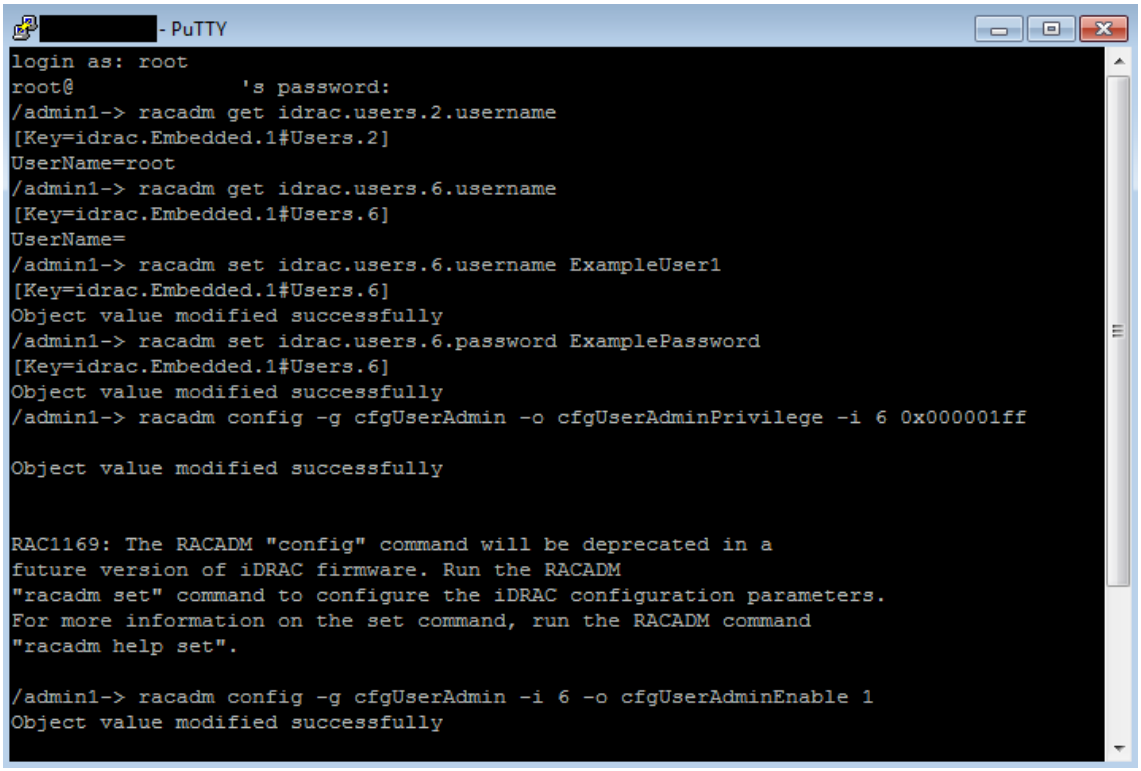
-**Racadm get idrac.users.<ID>.username**, komennolla tarkistetaan, onko käyttäjän indeksinumero jo käytössä, mikäli numero on käytössä, komento palauttaa käyttäjän nimen. Käyttäjiä luodaan ja muokataan indeksinumeron perusteella. Tällä komennolla varmistetaan, että muokataan haluttua käyttäjää, ja ettei uutta käyttäjää vahingossa luoda vanhan päälle.

-**Racadm set idrac.users.<ID>.username <USERNAME>**, komento luo annetun käyttäjänimen määritetyllä indeksinumerolla.

-**Racadm set idrac.users.<ID>.password <PASSWORD>**, komento asettaa annetun salasanan indeksinumerolla määritellylle käyttäjälle.

-**Racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <ID> <VALUE>**, komennolla määritellään käyttäjän oikeudet. Komento antaa indeksinumerolla määritellylle käyttäjälle komennon lopussa määritellyt arvot. Alempana näkyvässä kuvassa määritellään administrator-tason oikeudet.

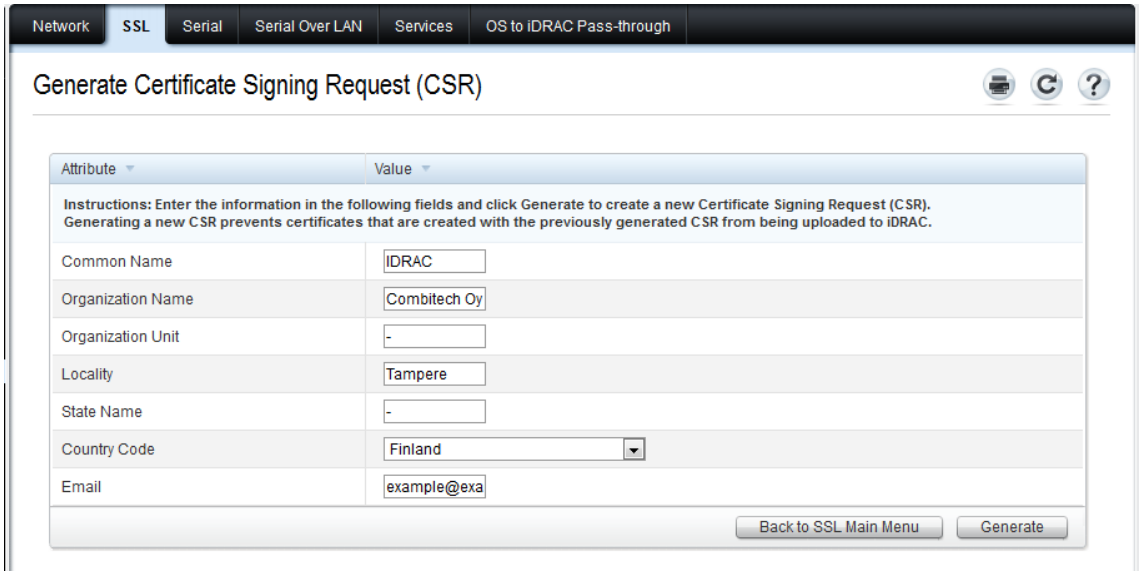
-**Racadm config -g cfgUserAdmin -i <ID> -o cfgUserAdminEnable 1**, komento aktivoi indeksinumerolla määritellyn tunnuksen.



KUVA 10. Kuvakaappaus käyttäjän luomisesta komentorivin avulla. Kuvassa RACADM-komentojen syöttämistä SSH-yhteydellä PuTTY-ohjelman läpi. Kuvasta poistettu iDRACin oikea IP-osoite.

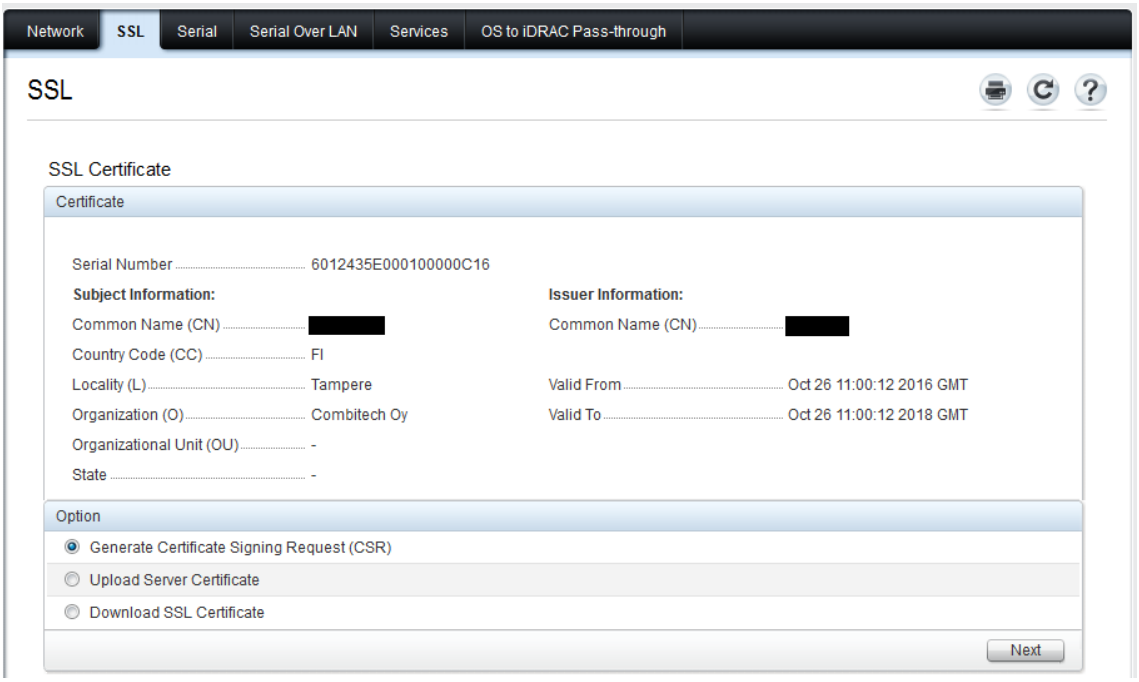
6.4.3 Sertifikaatin konfigurointi

Heti käyttäjien luomisen jälkeen iDRACille luotiin uusi sertifikaatti. Nykyistä sertifikaattia pääsee tarkastelemaan Network-osion alta SSL-välilehdeltä, myös uuden sertifikaattipyynnön generointi tapahtuu samalta sivulta. Sertifikaattipyyntöön määritellään iDRACin laitenimi, organisaation nimi, maa, kaupunki, sekä sähköpostiosoite. Kuvasta 11 nähdään sertifikaattipyynnön generoiminen.



KUVA 11. Kuvakaappaus sertifikaattipyynnön tekemisestä.

Pyynnön tekemisen jälkeen se voidaan ladata hallintakoneelle SSL-välilehdeltä (kuva 12). Seuraavaksi pyyntö toimitetaan sertifikaatin allekirjoittavalle taholle. Tässä työssä käytettiin Combitechin omaa CA:ta, allekirjoitusprosessia ei käydä tässä tapauksessa läpi. Kun sertifikaatti on allekirjoitettu, se tuodaan takaisin iDRACille hallintakoneelta web-käyttöliittymän kautta, myös takaisin tuonti suoritetaan SSL-välilehdeltä. Kun uusi allekirjoitettu sertifikaatti on tuotu iDRACille takaisin, iDRAC pitää käynnistää uudelleen muutosten voimaan tuomiseksi. Sertifikaattia tehdessä pitää huomioida, että iDRAC hyväksyy vain base64-formaattisia sertifikaatteja.

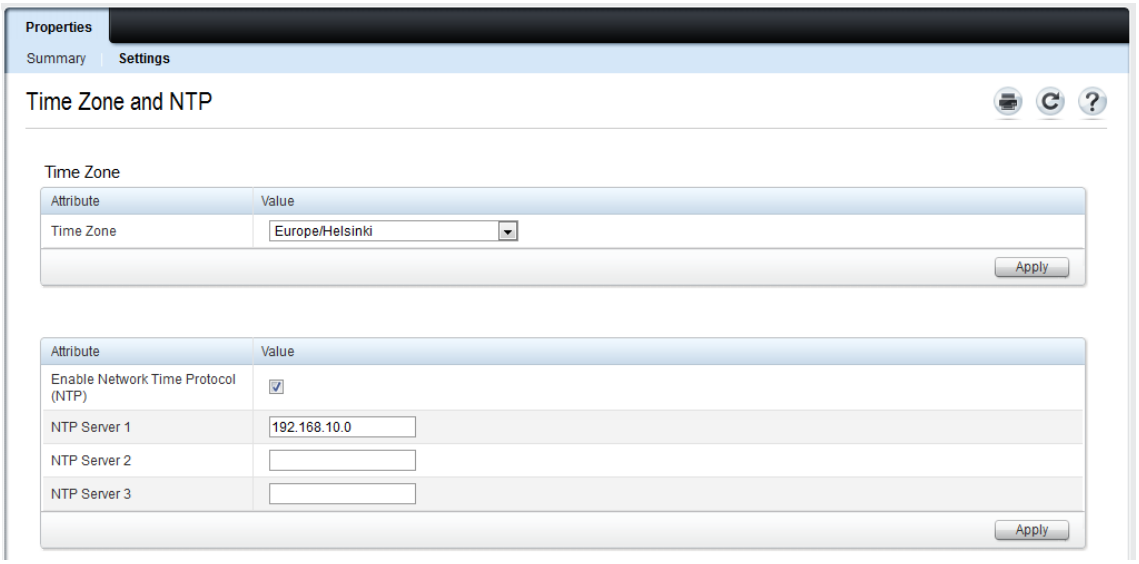


KUVA 12. Kuvakaappaus SSL-välilehdestä. Kuvassa käytössä olevan sertifikaatin tiedot. Kuvasta poistettu iDRACin ja sertifikaatin allekirjoittajan laitenimet.

6.4.4 NTP-asetuksien konfigurointi

Network Time Protocol (NTP) on kellojen synkronoimiseen verkossa käytetty protokolla. iDRAC hyödyntää NTP-protokollaa aikansa täsmällisenä pitämiseen. iDRACin ajan on tärkeää olla oikeassa, muuten lokien aikaleimat eivät täsmää muiden laitteiden kanssa. Myös ajastetut päivitykset vaativat täsmällisen ajan, päivittämisen aloittamisella väärään aikaan saattaisi olla vakavat seuraukset. NTP-protokolla käyttää porttia 123.

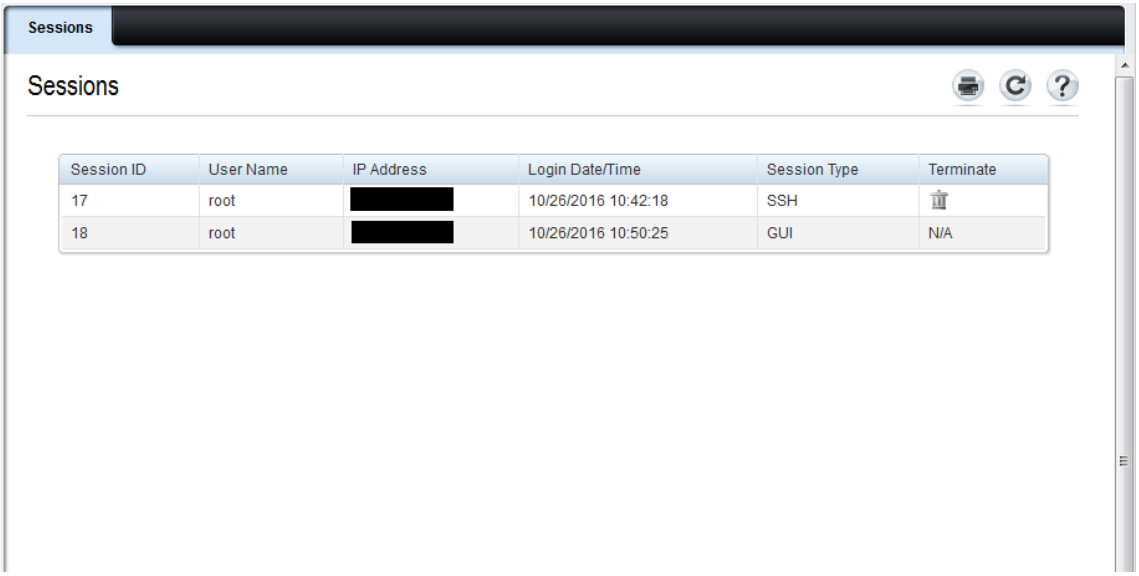
NTP-asetukset löytyvät iDRAC Settings-osiosta, settings-välilehdeltä (kuva 13). Sivulta määritellään laitteen aikavyöhyke sekä NTP-palvelin. Työssä käytetään Combitechin omaa NTP-palvelinta.



KUVA 13. Kuvakaappaus Time Zone and NTP-sivulta. Kuvassa NTP-asetukset.

6.5 Palvelimen tilanteen ja komponenttien tarkastelu

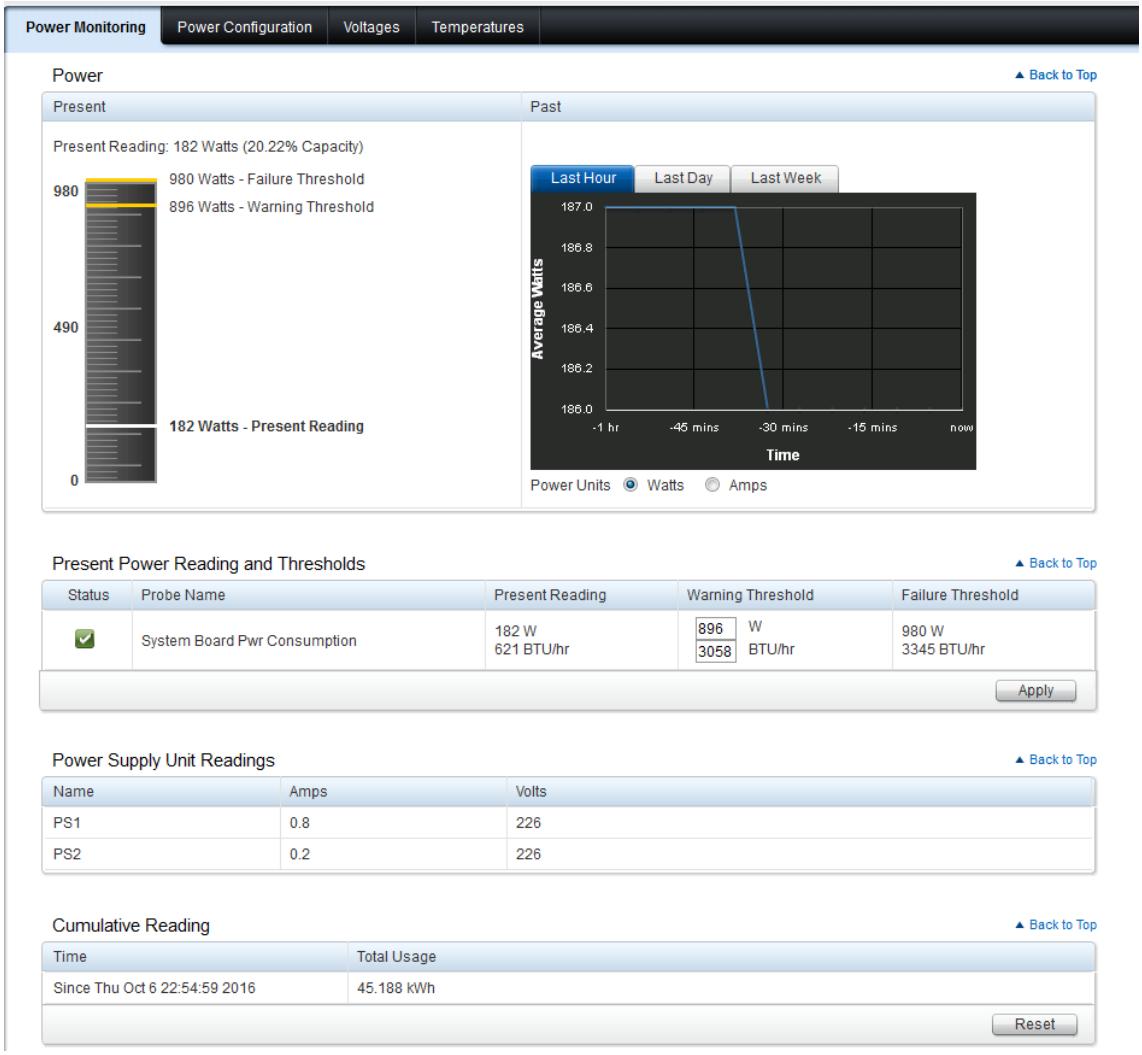
Palvelimen tilanteen ja komponenttien tarkastelua voidaan tehdä useammasta näkymästä. Tällä hetkellä käynnissä olevat iDRACin sessiot, ja niiden tyypit näkyvät Sessions-osiosta (kuva 14), sessioiden terminoiminen on mahdollista tältä sivulta.



KUVA 14. Kuvakaappaus Sessions-näkymästä. Kuvassa tällä hetkellä käynnissä olevat sessiot. Kuvasta poistettu IP-osoitteita.

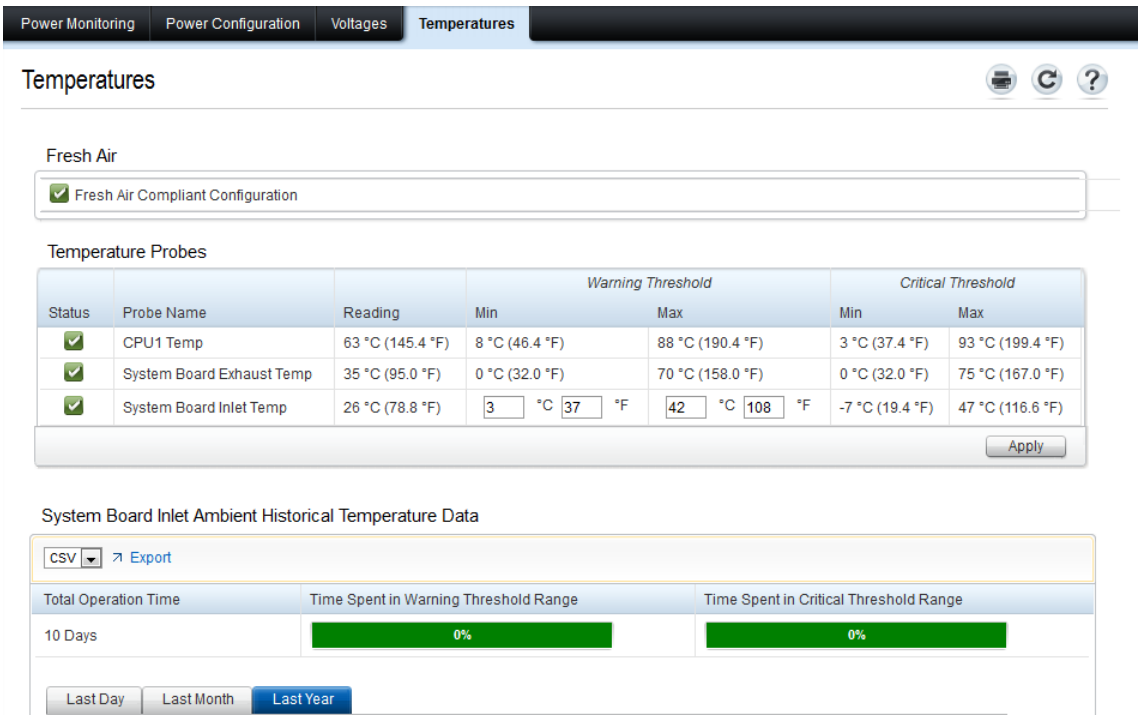
6.5.1 Virran ja lämpötilan seuranta

Palvelimen virtaa ja lämpötilaa voidaan seurata tarkasti Power / Thermal -osiosta. Power Monitoring -välilehdeltä (kuva 15) nähdään tämän hetken virrankulutus, sekä graafinen kuvaaja viimeaikaisesta kulutuksesta. Lisäksi saatavilla on paljon virrankäyttöön liittyvää statistiikkaa.



KUVA 15. Kuvakaappaus Power Monitoring -välilehdeltä. Kuvassa tilastoja virrankulutuksesta.

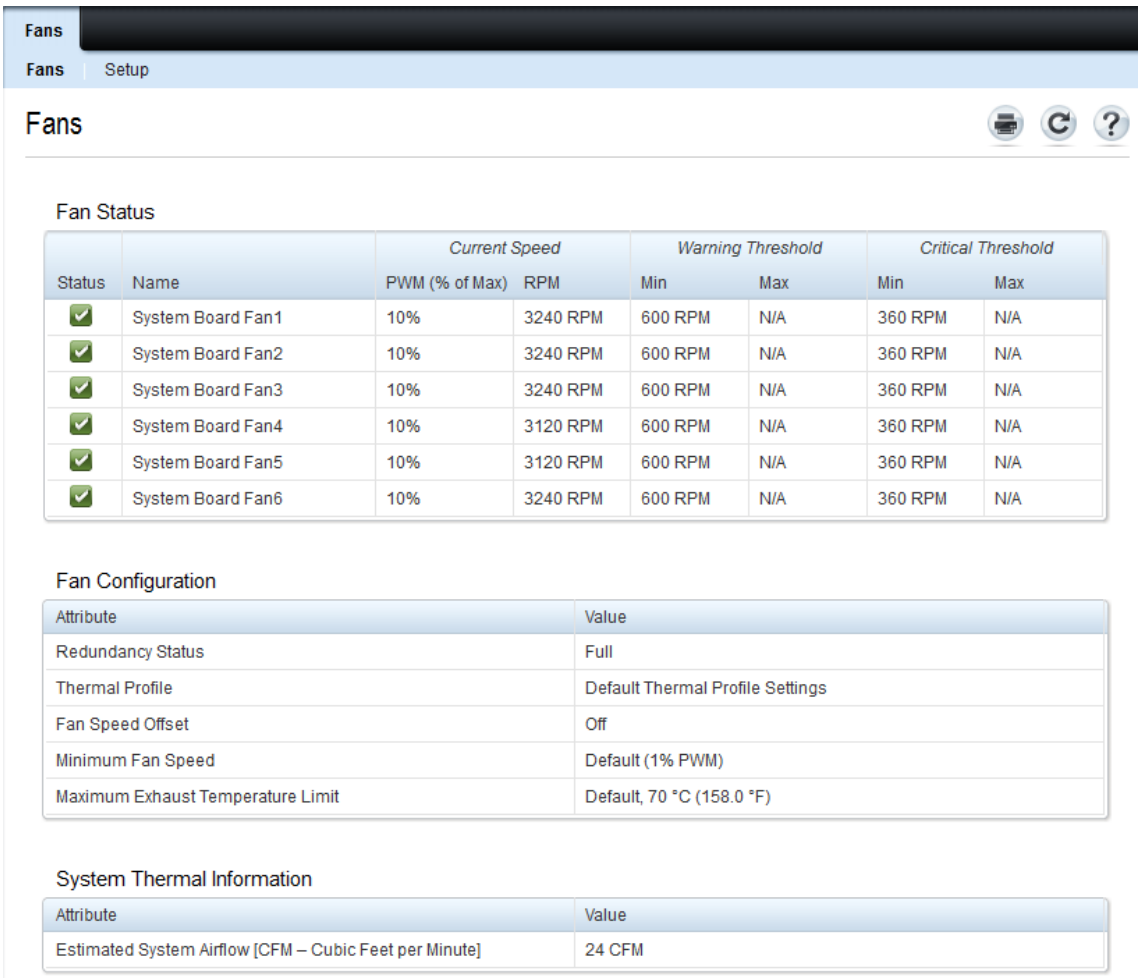
Temperatures-välilehdeltä (kuva 16) nähdään vastaavasti komponenttien tämän hetken lämpötiloja, sekä kuvaaja viimeaikaisista lämpötiloista. Lisäksi nähdään varoituksen ja hälytyksen laukaisevat lämpötila-arvot.



KUVA 16. Kuvakaappaus Temperatures-välilehdeltä. Kuvassa komponenttien tämän hetken lämpötiloja.

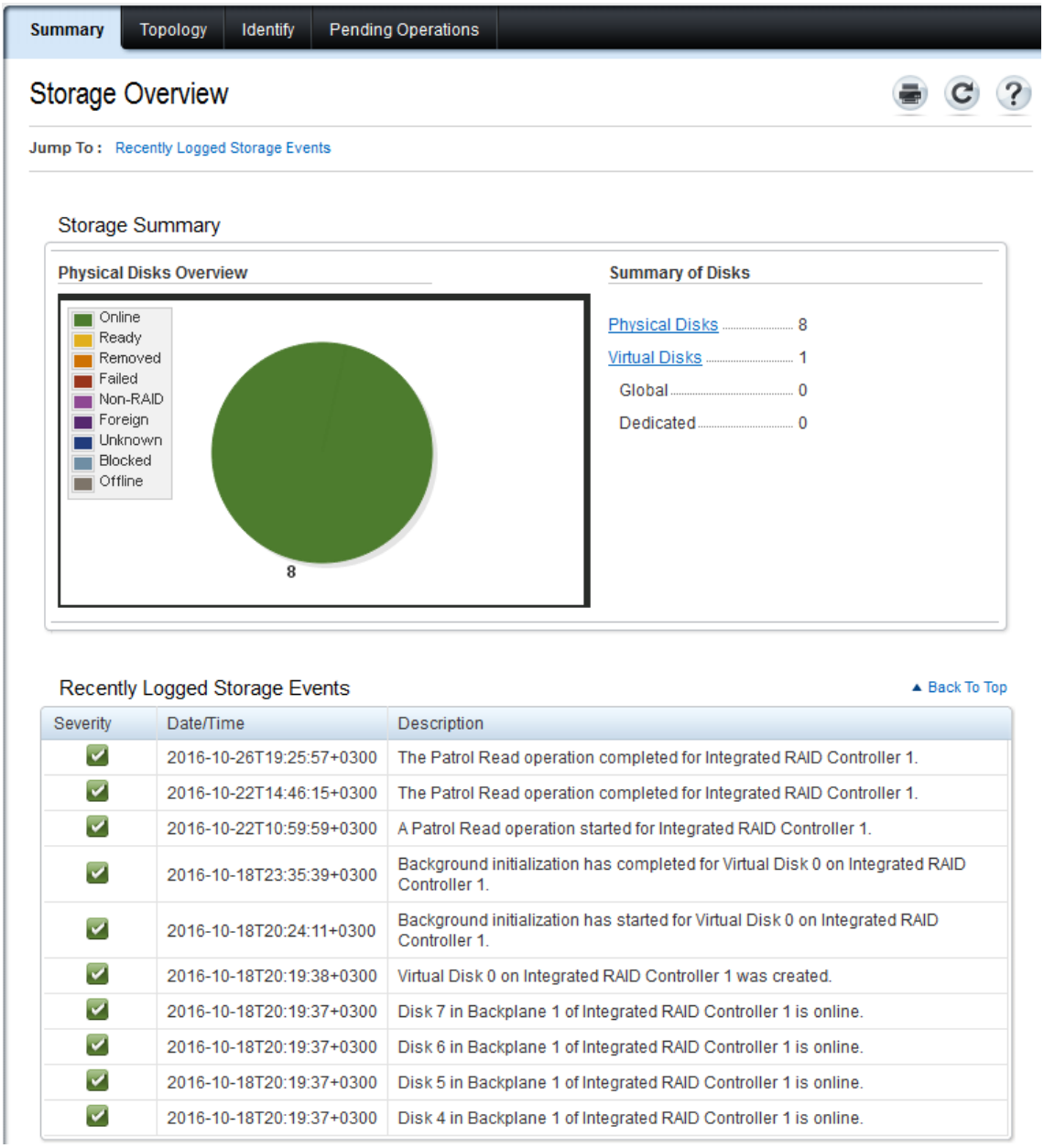
6.5.2 Komponenttien näkymät

Komponenttien yleistila nähdään Overview-näkymästä, mutta jokaista komponenttia voidaan myös tarkastella erikseen tarkemmin sen omasta osiosta. Esimerkiksi tuulettimien tilannetta voidaan seurata kuvassa 17 näkyvältä Fans-välilehdeltä. Hardware-valikon alle on listattu erillisiin osioihin patterit, tuulettimet, prosessorit, keskusmuisti, etupaneeli, verkkokortit ja virtalähteet. Näiltä sivuilta nähdään hyvin yksityiskohtaista tietoa komponenteista, tämän tiedon avulla voidaan määrittää tarkalleen esimerkiksi vaihdon tarpeessa oleva osa. Huonosta kunnosta ja epänormaalista toiminnasta saadaan myös tietoa, jonka avulla voidaan varautua ja toimia ennen komponentin pettämistä.



KUVA 17. Kuvakaappaus Fans-välilehdeltä. Kuvassa tietoja tuulettimien tilanteesta.

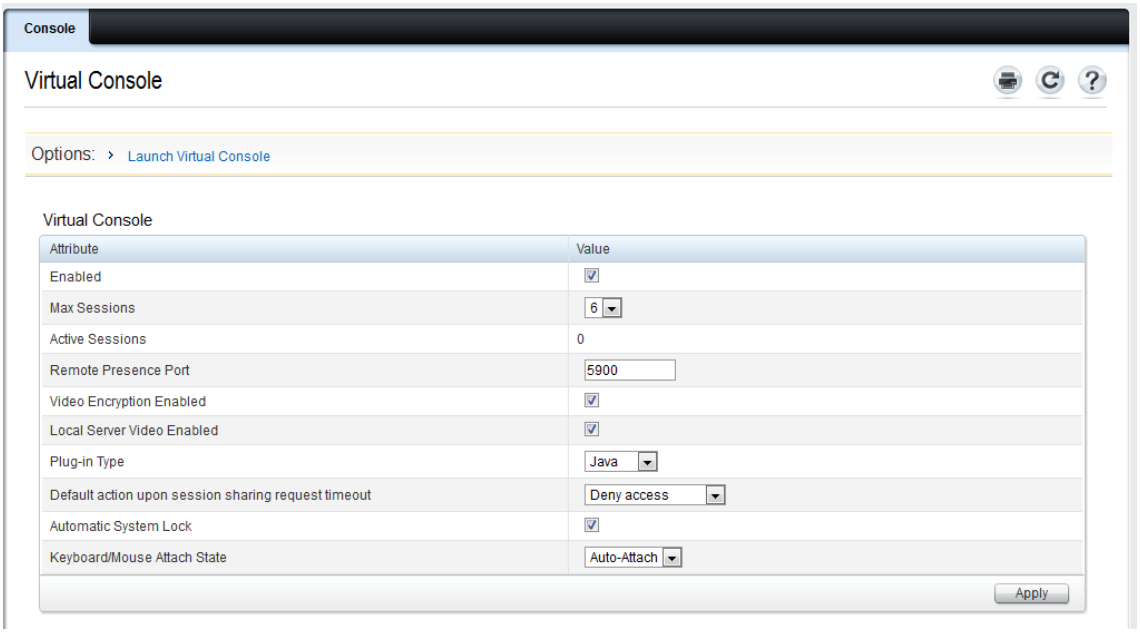
Kiintolevyillä on oma Storage-osio erillään muista komponenteista. Osiosta pääsee tarkastelemaan palvelimen fyysisiä- ja virtuaalisia kiintolevyjä. Summary-välilehdeltä (kuva 18) nähdään yleiskuva levyjen tilanteesta, myös yksittäisten levyjen tarkastelu on mahdollista. Sivulta nähdään myös viimeaikaiset kiintolevyihin liittyvät tapahtumat. Kyseessä olevan palvelimen kaikki fyysiset kiintolevyt muodostavat yhdessä yhden RAID10-kokonaisuuden.



KUVA 18. Kuvakaappaus Storage Overview -osiosta. Kuvassa graafinen kuvaaja kiintolevyjen yleistilanteesta, sekä lokia viimeaikaisista kiintolevyihin liittyvistä tapahtumista.

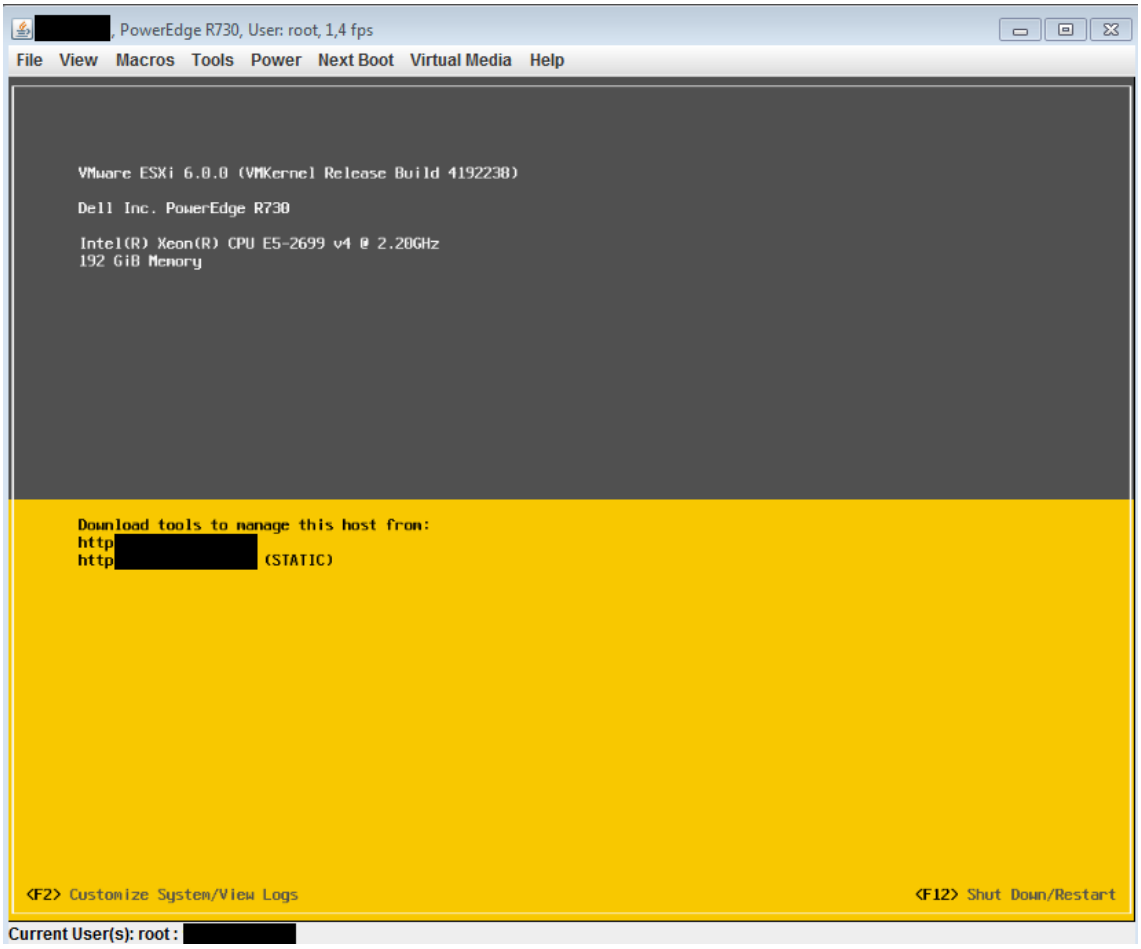
6.5.3 Virtuaalinen konsolinäkymä

Virtuaalisen konsolinäkymän voi aloittaa joko suoraan Overview-näkymästä, tai vaihtoehtoisesti erikseen Virtual Console -osiosta (kuva 19), josta pystyy myös määrittelemään konsolin asetuksia. Virtuaalista konsolia voi käyttää joko Javalla, tai HTML5:llä. Java aukaisee oman applikaationsa, ja HTML5 uuden ikkunan selaimeen. Työssä käytetään Javaa, sillä se antaa käyttöön enemmän ominaisuuksia. Virtuaalinen konsoli käyttää toimintaansa porttia 5900.



KUVA 19. Kuvakaappaus Virtual Console -välilehdeltä. Kuvassa virtuaalisen konsolin asetukset.

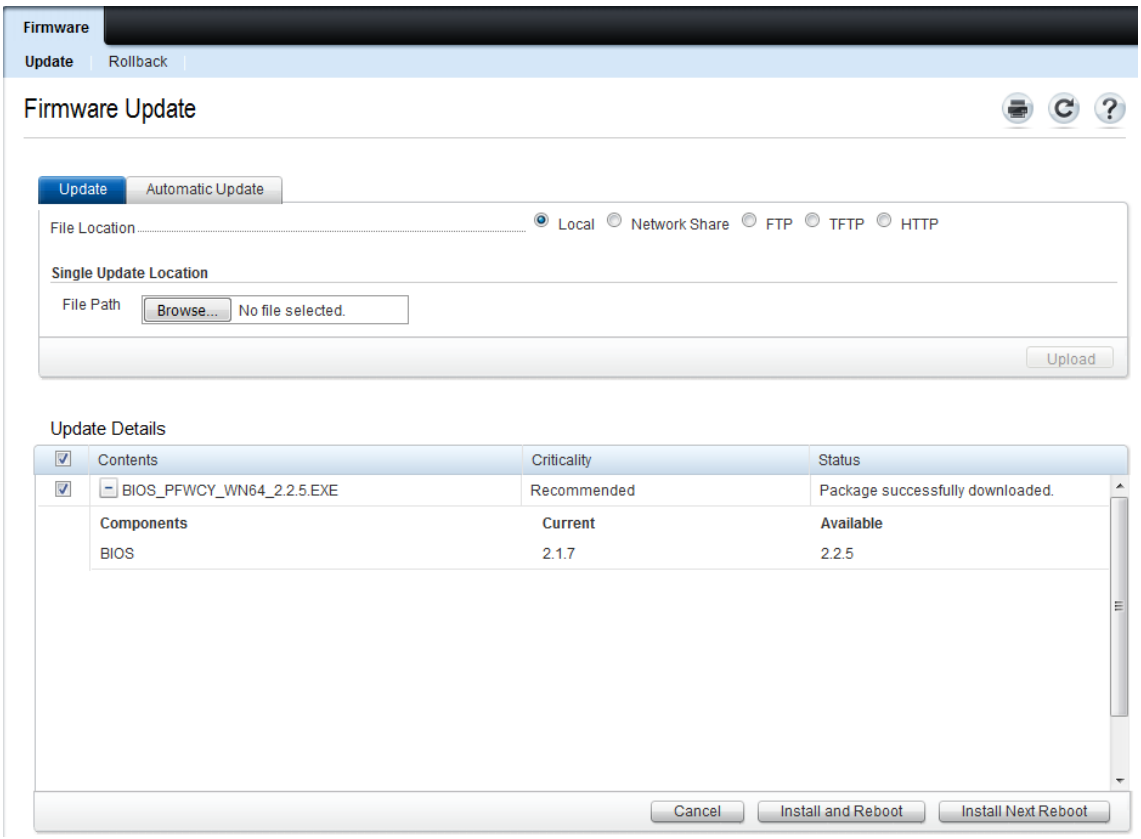
Virtuaalisesta konsolinäkymästä (kuva 20) pystytään hallinnoimaan palvelimen virtaa, käynnistystapaa, yhdistämään virtuaalista mediaa, ottamaan kuvakaappauksia, säätelemään näkymän tarkkuutta ja tarkastelemaan yhteyden tietoja. Lisäksi näkymästä pystyy viestittelemään muiden ylläpitäjien kanssa, mikäli heillä on sessio samanaikaisesti auki. Työssä käytetylle palvelimelle on asennettu VMware ESXi -käyttöjärjestelmä, joten itse palvelimen käyttöjärjestelmän konfigurointia virtuaalisen konsolin kautta ei tarvitse juurikaan tässä tapauksessa tehdä. Järjestelmää voitaisiin kuitenkin käyttää virtuaalisen konsolin avulla etänä aivan kuten paikallisesti.



KUVA 20. Kuvakaappaus virtuaalisesta konsolinäkymästä. Kuvassa palvelimen käyttöjärjestelmä VMware ESXi 6.0.0. Kuvasta poistettu palvelimen IP-osoite ja laitenimi.

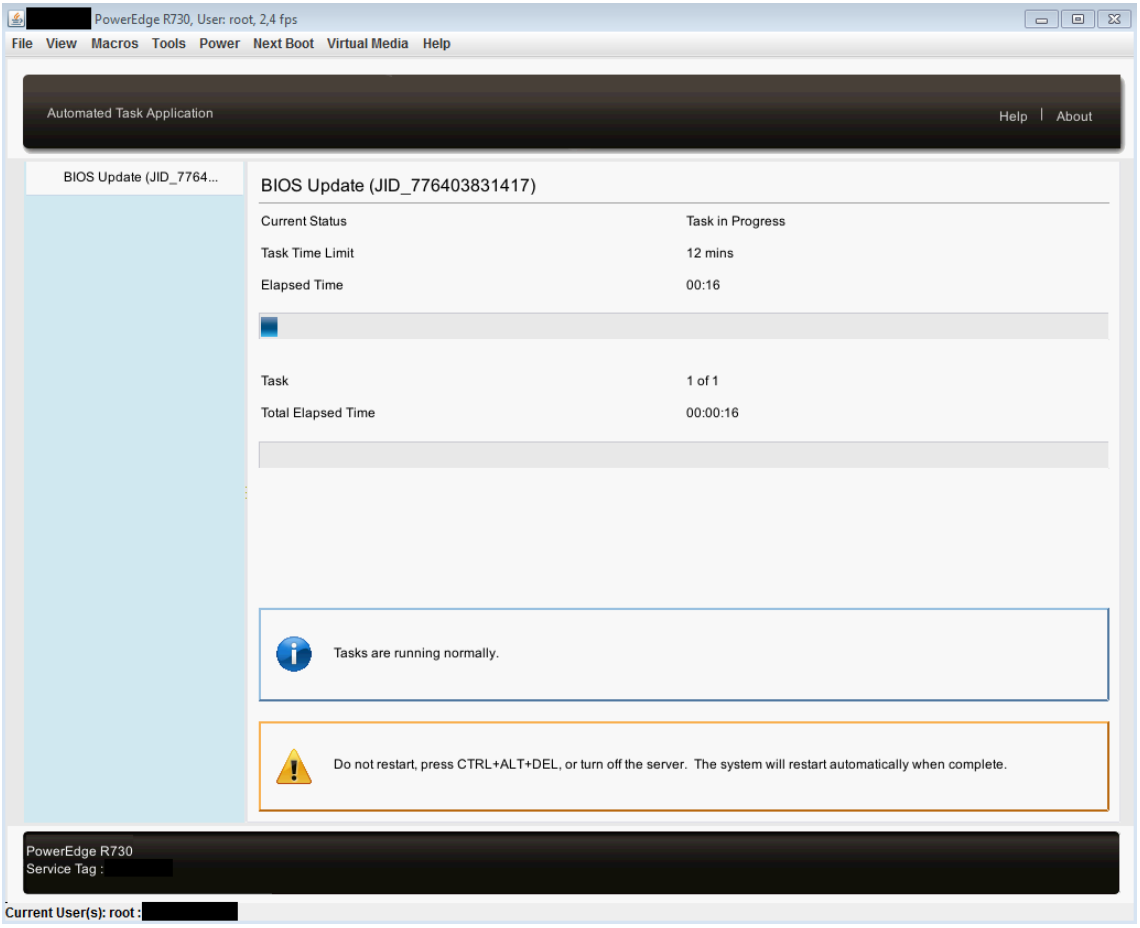
6.6 Firmwaren päivittäminen iDRACilla

Palvelimen komponenttien firmware-päivityksien tekeminen iDRACilla tapahtuu Update and Rollback -osiosta. Päivityksien tuominen iDRACille voidaan tehdä tuomalla päivitys ensin hallintakoneelle, ja sen jälkeen lataamalla se web-käyttöliittymän kautta iDRACille. Päivitykset voidaan tuoda myös jaetulle verkkolevylle, josta ne voidaan valita web-liittymän kautta. Asennettavissa olevat päivitykset ovat nähtävissä kuvassa 21 näkyvällä Firmware Update -välilehdellä. Firmware-päivitykset ovat ladattavissa Dellin sivuilta palvelimen service tag -numerosarjan avulla.



KUVA 21. Kuvakaappaus Firmware Update -välilehdeltä. Kuvassa asennusta odottava iDRACille tuotu BIOS-päivitys.

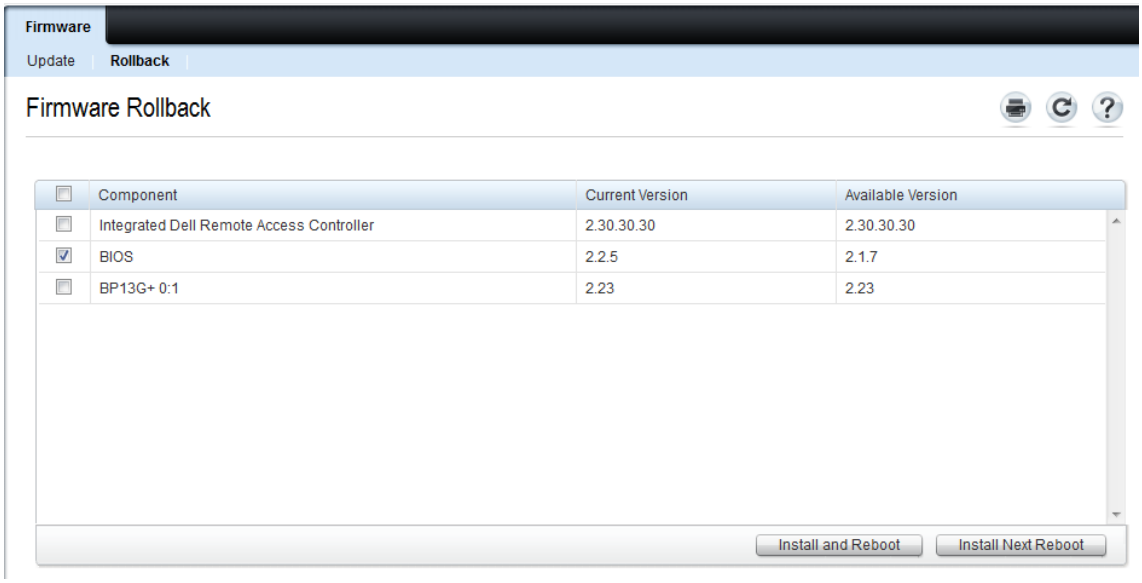
Kun tuotava päivitys on valittu, iDRAC tarkistaa päivityksen sopivuuden, jos päivitys on sopiva, asennus voidaan aloittaa. Asennuksen kulkua voidaan halutessa seurata virtuaalisen konsolin avulla (kuva 22), tai vaihtoehtoisesti Job Queue -välilehdeltä.



KUVA 22. Kuvakaappaus virtuaalisesta konsolista. Kuvassa palvelimen BIOS-päivityksen eteneminen.

6.6.1 Firmware-päivityksen peruuttaminen

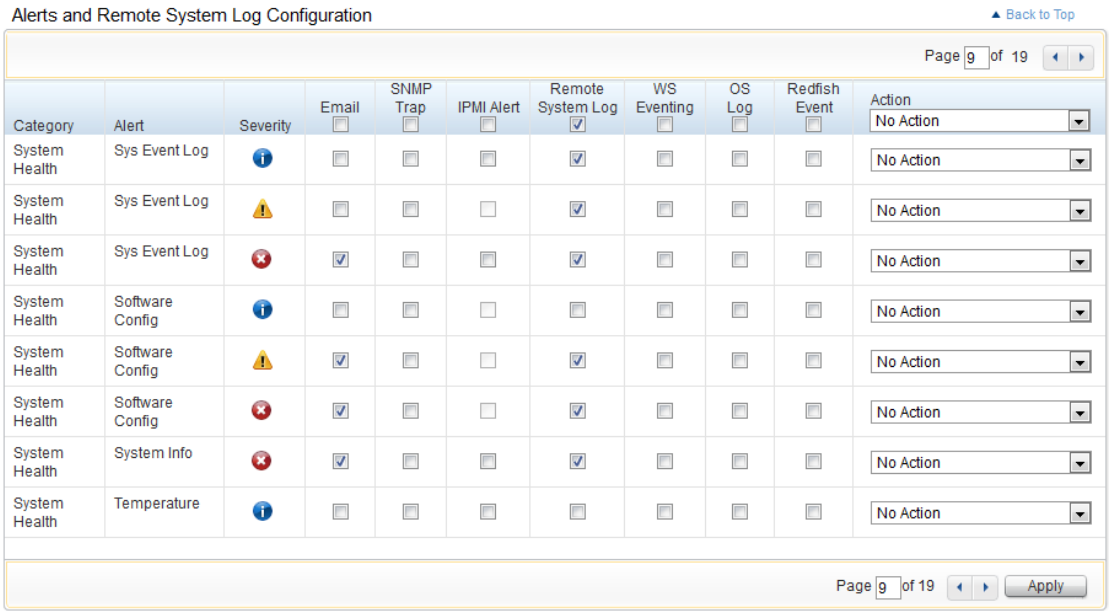
Jos syystä tai toisesta firmware-päivitys halutaan peruuttaa, se voidaan palauttaa taikaisin vanhaan. Vanhan version palauttaminen tapahtuu kuvassa 23 näkyvältä Rollback-välilehdeltä. Päivityksiä asentaessa täytyy huomioida, että kaikkien komponenttien firmwarea ei voida palauttaa takaisin vanhaan. Rollback-välilehdeltä nähdään tällä hetkellä asennetun firmwaren versio, ja saatavilla olevat vanhat versiot.



KUVA 23. Kuvakaappaus Firmware Rollback -välilehdeltä. Kuvasssa tämän hetken, ja saatavilla olevat vanhat firmwaren versiot.

6.7 Lokit ja hälytykset

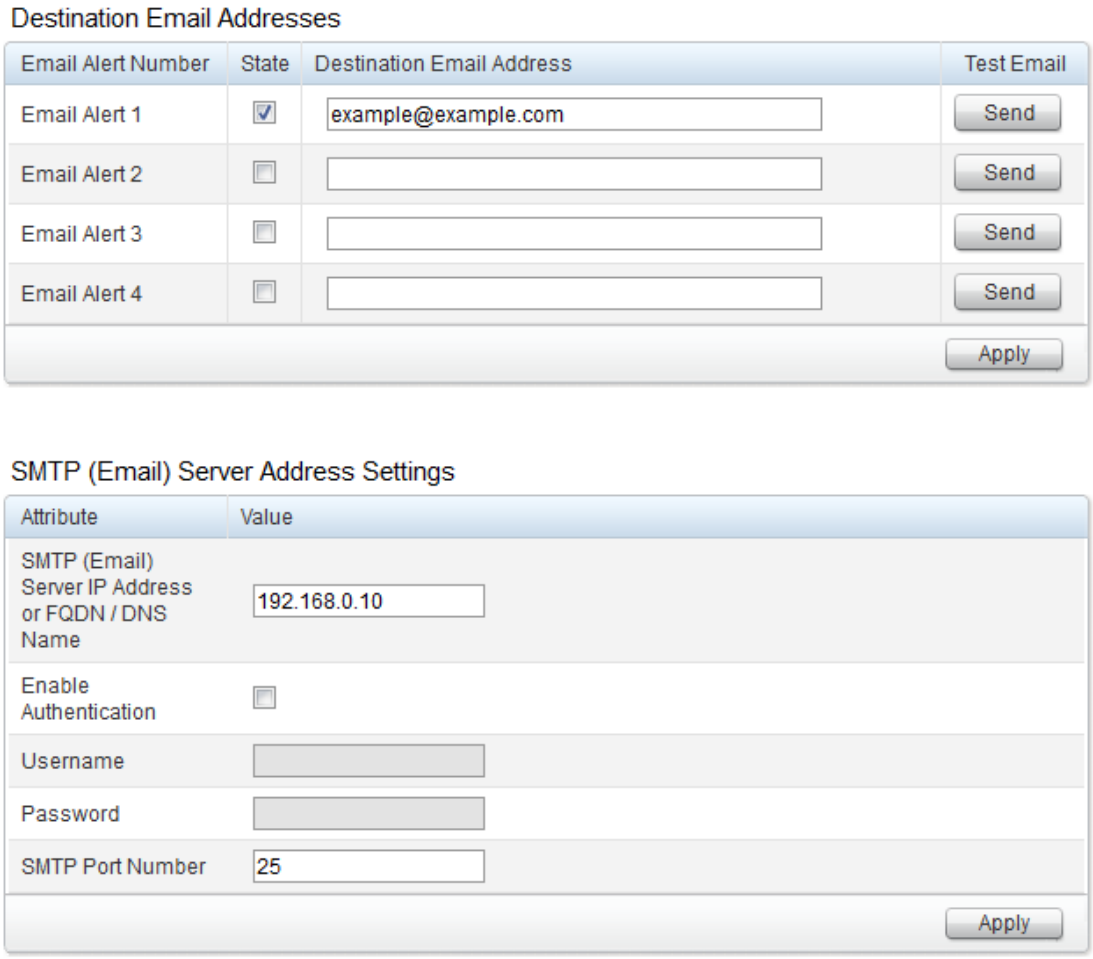
Tapahtumat joista tehdään lokia ja lähetetään hälytyksiä, määritellään Alerts-osiossa (kuva 24). Näkymästä pystytään määrittämään, mistä tapahtumista hälytyksiä ja lokia lähetetään, ja kuinka vakava tilan pitää olla aiheuttaakseen hälytyksen tai lokimerkinnän. Tilanteen vakavuutta kuvaavia tasoja on kolme: informatiivinen, varoittava ja kriittinen. Testitapahtumia voidaan generoida sivun alalaidasta ilmoitusten toiminnan testaamiseksi. Myös hälytyksien lähettämisen tiheyttä voidaan säädellä. Lisäksi jokaisen tapahtuman yhteyteen voidaan liittää yksi toiminto. Toiminto voi olla esimerkiksi palvelimen sammutus tai uudelleenkäynnistys. Tässä käyttöönotossa ei katsottu tarpeelliseksi liittää toimintoja tapahtumiin ainakaan toistaiseksi.



KUVA 24. Kuvakaappaus Alerts-osiosta. Kuvassa tapahtumien valinta, jotka aiheuttavat hälytyksiä ja lokimerkintöjä.

6.7.1 Sähköpostiasetuksien konfigurointi

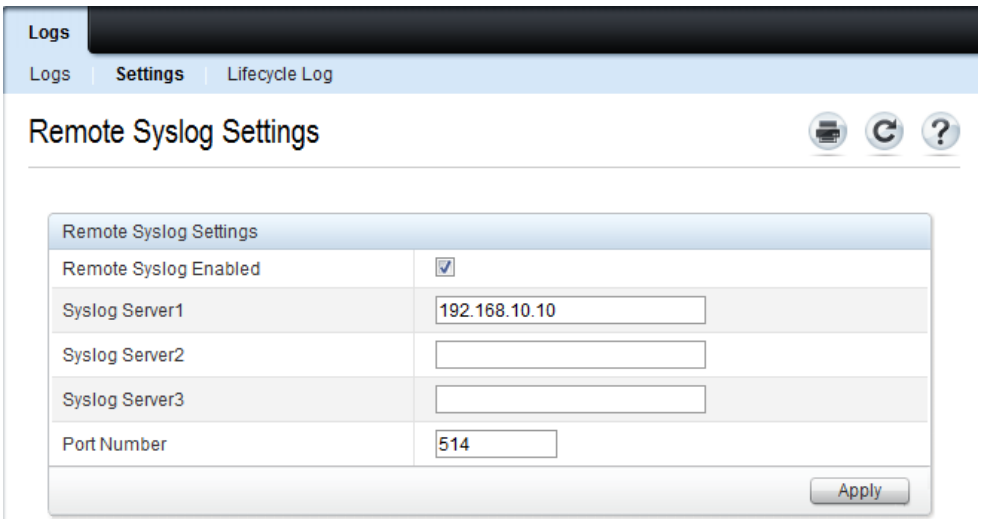
Hälytyksien lähettäminen sähköpostilla vaatii sähköpostiasetuksien konfiguroinnin. Asetukset sijaitsevat Alerts-osion alla, SNMP and Email Settings -välilehdellä (kuva 25). Sivulle määritellään hälytyksien kohde sähköpostiosoite, tässä työssä käytettiin sähköpostilistaa, jolle kaikki ylläpitäjät kuuluvat. Sivulle määritellään myös sähköpostipalvelimen IP-osoite. Sähköpostin lähetyksen toimintaa voidaan testata lähettämällä testisähköpostiviesti.



KUVA 25. Kuvakaappaus SNMP and Email Settings -välilehdeltä. Kuvassa sähköpostin lähettämiseen käytetyt asetukset.

6.7.2 Lokien konfigurointi

Kuten aikaisemmin mainittu, hälytyksien lisäksi myös lokeihin kirjattavat tapahtumat määritellään Alerts-osiossa, mutta lokien lähettämiseksi iDRACilta lokipalvelimelle, Remote Syslog -asetukset pitää konfiguroida. Asetukset löytyvät Logs-osiosta Settings-välilehdeltä (kuva 26). Sivulla määritellään lokipalvelimen IP-osoite ja käytettävän portin numero. Oletuksena syslog käyttää porttia 514.



KUVA 26. Kuvakaappaus Remote Syslog Settings -välilehdeltä. Kuvassa Remote Syslog -asetukset.

Kuvasta 27 nähdään palvelimen tapahtumista kirjattuja lokeja, joita voidaan tarkastella paikallisesti Logs- ja Lifecycle Log -välilehdiltä. Lokien lähettämisessä erilliselle loki-palvelimelle on pitemmällä aikavälillä kuitenkin etuja paikalliseen tarkasteluun verrattuna. Kun iDRAC-moduuleja on käytössä useampia, ei tarvitse käydä kaikilla erikseen, vaan kaikki saapuneet ilmoitukset ovat yhdessä paikassa. Kun lokia muodostuu paljon, iDRAC pakkaa ja arkistoi sitä automaattisesti säästääkseen tilaa. Lokit voidaan halutessa ottaa pihalle iDRACista myös manuaalisesti tiedostona.

+	✓	2016-10-28T10:41:16+0300	RED030	Reboot is complete.	
+	✓	2016-10-28T10:41:15+0300	SYS1003	System CPU Resetting.	
+	✓	2016-10-28T10:41:14+0300	SYS1000	System is turning on.	
+	✓	2016-10-28T10:41:06+0300	RAC0701	Requested system powerup.	
+	✓	2016-10-28T10:41:06+0300	SYS1003	System CPU Resetting.	
+	✓	2016-10-28T10:41:05+0300	SYS1001	System is turning off.	
+	✓	2016-10-28T10:40:36+0300	RAC0705	Requested system graceful shutdown.	
+	✓	2016-10-28T10:40:21+0300	USR107	The operation SetupJobQueue of the DCIM_JobService was performed by root	
+	✓	2016-10-28T10:40:21+0300	RED055	A reboot job RID_776404215689 was created.	
+	⚠	2016-10-28T10:40:21+0300	RED029	A reboot is pending.	
+	✓	2016-10-28T10:40:21+0300	JCP027	Job created successfully.	
+	✓	2016-10-28T10:40:21+0300	USR107	The operation CreateRebootJob of the DCIM_SoftwareInstallationService was performed by root	
+	✓	2016-10-28T10:40:12+0300	RED002	Package successfully downloaded.	
+	✓	2016-10-28T10:39:45+0300	RED003	Downloading package.	
+	✓	2016-10-28T10:39:43+0300	RED054	An update job JID_776403831417 was created.	
+	✓	2016-10-28T10:39:43+0300	JCP027	Job created successfully.	
+	✓	2016-10-28T10:39:42+0300	USR107	The operation InstallFromURI of the DCIM_SoftwareInstallationService was performed by root	
+	✓	2016-10-28T10:39:39+0300	RED052	Processing of update packages is starting.	
+	✓	2016-10-28T10:39:39+0300	LOG007	The previous log entry was repeated 1 times.	
+	✓	2016-10-28T10:35:47+0300	RED002	Package successfully downloaded.	

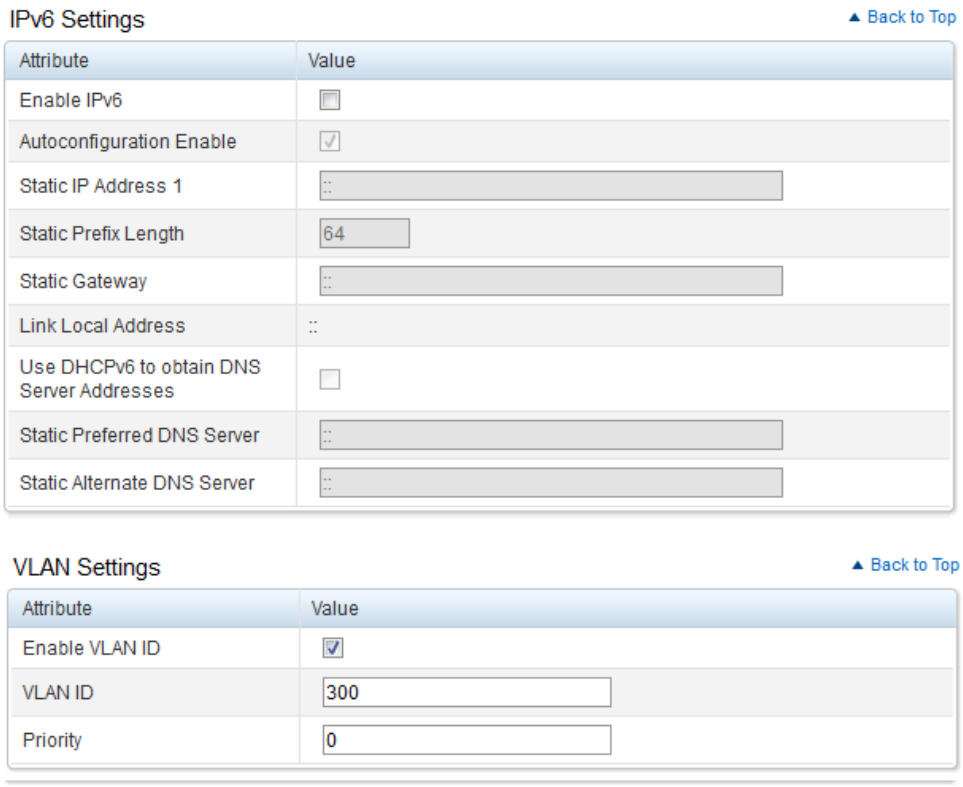
KUVA 27. Kuvakaappaus Lifecycle Log -välilehdeltä. Kuvassa lokia palvelimen tapahtumista.

6.8 iDRACin tietoturvan koventaminen

iDRACin tietoturvaa voidaan koventaa poistamalla käytöstä tarpeettomia asetuksia. Tässä työssä käytöstä poistettiin kokonaisuudessaan IPv6-, Telnet-, SNMP-, DNS- ja DHCP-protokollat. Asetukset löytyvät Network-osiosta (kuva 28). Protokollien lisäksi käytöstä poistettiin myös mahdollisuus ottaa yhteyttä iDRACiin käyttäen IMPI- (Intelligent Platform Management Interface) ja Serial-yhteyksiä. Toisien sanoen iDRACiin pystyy muodostamaa etäyhteyden vain web-käyttöliittymää, tai SSH-yhteyttä käyttäen. Myös iDRACin toiminta VNC (Virtual Network Computing) -palvelimena estetään.

Halutessa myös mahdollisuus paikalliseen konfigurointiin voidaan estää. Tätä ei kuitenkaan tehdä tässä työssä, sillä palvelintilat ovat hyvin turvattuja. Lisäksi paikalliselle konfiguroinnille voisi joskus tulla tarvetta, jos etähallinta pettäisi.

Selaimen käytön turvallisuutta lisää iDRACille tehty sertifikaatti, ja että HTTP-protokolla on oletuksena poistettu käytöstä, sillä iDRAC ohjaa HTTP-yhteyspyynnöt automaattisesti HTTPS-porttiin. iDRAC asetettiin myös hyväksymään yhteyksiä vain sen omasta VLAN:sta 300, kaikki muut yhteydet tiputetaan. Nämäkin asetukset löytyvät Network-osiosta.



KUVA 28. Kuvakaappaus Network-osiosta. Kuvassa tietoturvaa koventavia asetuksia.

7 POHDINTA

Opinnäytetyön loppuvaiheessa on jo selvää, että työ on onnistunut. Työn teko päästiin aloittamaan hieman suunniteltua myöhemmin, mutta aikataulussa pysyttiin. iDRACin käyttöönotto sujui todella nopealla tahdilla sen jälkeen, kun käyttöönottoon sopiva palvelin löydettiin. Yrityksen palvelimiin oli aina tilauksen yhteydessä sisällytetty lisenssi myös iDRACia varten, mutta hyötyjen selvitykseen ja itse käyttöönottoon ei oltu aikaisemmin, ajasta johtuen, käytetty resursseja.

Käyttöönottoa tehdessä paljastui heti paljon hyviä puolia. Palvelimien rautaa päästään tarkastelemaan ja päivittämään helposti web-käyttöliittymän kautta, kummatkin ovat asioita, jotka saattavat helposti jäädä vähemmälle muiden asioiden painaessa päälle. Työn lopussa tiedetään jo, että iDRAC halutaan ottaa käyttöön yrityksen jokaisessa Dellin palvelimessa. Opinnäytetyön tavoite on siis täyttynyt.

Ennen opinnäytetyötä en tiennyt mitään iDRACista, tai muista etähallintamoduuleista. Valmistajan dokumentaatio oli kuitenkin kattavaa, ja iDRACin käyttö ei tuottanut ongelmia. Tietoa protokollista löytyi helposti, ja osaaminen muista verkkolaitteista oli jo ennestään vahvaa. Sain yritykseltä tarvittaessa ohjausta käyttöönottoon liittyvissä asioissa, työn teko tapahtui kuitenkin hyvin pitkälti täysin itsenäisesti. Työn jälkeen koen hahmottavani oikean, isommankin verkkoympäristön etähallintatarpeita ja -ratkaisuja aivan uudella tasolla.

Työssä ei otettu käyttöön kaikkia iDRACin ominaisuuksia, sillä kaikki niistä eivät olleet tarpeellisia, tai soveliaita yrityksen ympäristöön. Tulevaisuudessa tarkoitus on kuitenkin vielä hioa iDRACin asetuksia ja käyttötapaa juuri Combitechin tarpeisiin. Samalla kun lähitulevaisuudessa yritys ottaa iDRACin käyttöön kaikkiin Dellin palvelimiinsa, aiotaan selvittää keskitetyn etähallinnan mahdollisuuksia Dellin OpenManage Essentials -ohjelmistolla. Tällä hetkellä näyttää siltä, että työssä tehty Windows 7 -hallintakone korvataan Windows Server -koneella, jota tullaan käyttämään uutena, keskitettynä hallintakoneena.

Pääsen seuraamaan työni kehittymistä ensi kädessä, sillä tein opinnäytetyön aikana sopimuksen Combitechin kanssa vakituisesta työsuhteesta. Olen opinnäytetyöhöni tyytyväinen, ja voin rehellisesti sanoa olevani ylpeä tuloksista.

LÄHTEET

Combitechin verkkosivut – Tietoja Combitechistä. Luettu 2.9.2016 http://www.combitech.fi/Tietoja-Combitechista-/

Dell. 2016. Dell Technologies Key Facts. Luettu 1.10.2016 https://www.delltechnologies.com/content/dam/delltechnologies/assets/press/resources/Dell_Technologies_Key_Facts.pdf

Dell. 2016. iDRAC 8/7 V2.40.40.40 User's Guide. Luettu 3.9.2016 http://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_remote_ent_sys_mgmt/idrac7-8-lifecycle-controller-v2.40.40.40_user%27s%20guide_en-us.pdf

Dell. 2012. iDRAC6 Home. Luettu 1.10.2016 http://en.community.dell.com/techcenter/systems-management/w/wiki/4357.idrac6-home

Goralski, W. 2009. The Illustrated Network: How TCP/IP Works in a Modern Network. Morgan Kaufmann.

Internet Assigned Numbers Authority. Service Name and Transport Protocol Port Number Registry. Luettu 8.10.2016. http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Oppliger, R. 2009. SSL and TLS. Artech House.

Puolustusministeriö. 2015. KATAKRI 2015 – Tietoturvallisuuden auditointityökalu viranomaisille. http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

SSH verkkosivut – Company Overview. Luettu 16.10.2016 https://www.ssh.com/about/ssh-communications-security

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681.

RFC 1945. 1996. https://tools.ietf.org/html/rfc1945

RFC 2616. 1999. https://tools.ietf.org/html/rfc2616

RFC 2818. 2000. https://tools.ietf.org/html/rfc2818

RFC 5321. 2008. https://tools.ietf.org/html/rfc5321

RFC 7230. 2014. https://tools.ietf.org/html/rfc7230

RFC 7231. 2014. https://tools.ietf.org/html/rfc7231

RFC 7234. 2014. https://tools.ietf.org/html/rfc7234

LIITTEET

Liite 1. Combitech Oy:lle laadittu ohjeistus iDRACin käyttöönottoon

1 (3)

iDRACin käyttöönotto

1. Kytke läppäri iDRACin porttiin.
2. Aseta läppärin IP-osoite verkkoon 192.168.0.0/24. iDRAC käyttää oletuksena osoitetta 192.168.0.120.
3. Avaa selain ja kirjoita hakukenttään iDRACin ip-osoite. Kirjautumis ruutu aukeaa, käytä kirjautumiseen käyttäjää: root ja oletussalasanaa: calvin HUOM! Ota F-Secure alustavan konfiguraation ajaksi pois käytöstä, muuten et pääse web-käyttöliittymään kiinni.
4. Vaihda root-käyttäjän salasana pois oletuksesta User Authentication -välilehdellä. Valitse konfiguroitava käyttäjä, valitse ”User Configuration” ja anna uusi salasana.
5. Aseta iDRACin pysyvät verkkoasetukset. Mene Network-välilehdelle ja aseta IPv4-osoite, maski ja oletusyhdyskäytävä. Kun hyväksyt uudet verkkoasetukset, nykyinen yhteytesi katkeaa.
6. iDRACin alustava konfiguraatio on nyt valmis. Laita lopuksi iDRACin portti kiinni kytkimen porttiin ja ota läppärin F-Secure takaisin käyttöön.
7. Mene verkkolaitteiden hallintakoneelle ja ota yhteys PuTTY:llä kytkimelle johon iDRAC on yhdistetty. Jos iDRACin VLAN:ia ei ole olemassa, luo ja nimeä se.
8. Aseta portti jossa iDRAC on kiinni käyttämään iDRACin VLAN:ia.
9. Tarkista, että trunk-portissa kulkee myös iDRACin VLAN.
10. Hallintakone ja sen virtuaaliset kytkimet ovat jo konfiguroituna, niiden asetuksia ei tarvitse muokata.
11. Mene palomuurille, ja luo iDRACista uusi network-elementti.
12. Mene Security Engine -kohtaan, ja valitse oikea palomuuri. Etsi palomuurilta olemassa olevat iDRAC-säännöt ja lisää uuden iDRACin elementti olemassa oleviin sääntöihin. Tallenna muutokset ja ota ne käyttöön.
13. Verkkolaitteiden konfiguraation on nyt valmis.

(jatkuu)

14. Kirjaudu sisään virtuaaliselle iDRACin hallintakoneelle. Avaa selain ja kirjoita asettamasi iDRACin IP-osoite selaimen hakukenttään.
15. Kirjaudu iDRACiin sisään käyttäjätunnuksella: root ja asettamallasi salasanalla. HUOM! Lisää iDRACin salasana tässä kohtaa verkkolaitteiden keepassiin.
16. Tee ensimmäiseksi itsellesi oma administrator-tunnus iDRACille. Uusi käyttäjä User Authentication -välilehdeltä. Anna käyttäjänimi, salasana ja valitse sivun alalaidasta privilege-tasoksi Administrator!
17. Kirjaudu root-käyttäjältä ulos ja käytä tästä eteenpäin omaa käyttäjätunnustasi iDRACin yhteydessä.
18. Seuraavaksi luodaan iDRACin sertifikaatti. Mene Network-välilehdelle ja muuta iDRACin hostname oikeaksi.
19. Mene SSL-välilehdelle joka löytyy Network-asetuksien alta. Laita valinta kohtaan ”Generate Certificate Signing Request (CSR)” ja paina Next.
20. Täytä sertifikaatin allekirjoituspyyntöön tarvittavat tiedot ja paina Generate. iDRAC tarjoaa pyynnön tallentamista, ota pyyntö talteen ja vie se allekirjoitusta varten sertifikaattipalvelimelle.
21. Kun sertifikaatti on allekirjoitettu, ota se pihalle **base64**-formaatissa. Tuo allekirjoitettu sertifikaatti takaisin hallintakoneelle.
22. Mene takaisin SSL-välilehdelle, valitse kohta ”Upload Server Certificate” ja paina Next.
23. Uuden sertifikaatin käyttöönotto vaatii iDRACin uudelleen käynnistymisen. Hyväksy iDRACin tarjoama uudelleen käynnistus.
24. Seuraavaksi kannattaa asettaa iDRAC käyttämään NTP-aikaa. Mene iDRAC Settings -kohdan alta Settings-välilehdelle. Aseta aikavyöhyke, NTP-palvelimen IP-osoite ja laita valinta ”Enable Network Time Protocol (NTP)” kohtaan.
25. Valitse Virtual Console-välilehdeltä virtuaalisen konsolin Plug-in Type -kohtaan Java.
26. Mene Alerts-osioon konfiguroimaan hälytyksien ja lokikirjauksien aiheuttajia. Kannattaa avata toinen iDRAC ja kopioida sen asetukset uudelle iDRACille. Muista asettaa sivun ylälaidasta pallo ”Alerts: Enabled” kohtaan.
27. Seuraavaksi pitää asettaa SMTP-asetukset ”SNMP and Email Settings” –välilehdeltä sähköpostin lähettämistä varten. Laita sivun alalaitaan SMTP-palvelimen IP-osoite, ja anna Destination Email Addresses -kohtaan ICT:n postituslista. Testaa sähköpostihälytyksien toiminta painamalla Test Email -nappia.

28. Sähköpostiasetuksien lisäksi pitää konfiguroida Remote Syslog Settings -asetukset, jotka löytyvät Logs-osion alta Settings-sivulta. Sivulle annetaan Syslog-palvelimen IP-osoite, sekä pistetään rasti kohtaan ”Remote Syslog Enabled”. Tarkista lokien perille pääsy lokipalvelimelle generoimalla testitapahtuma Alerts-osiosta.
29. Lopuksi tehdään tietoturvan kovennuksia Network-osiosta. Poista käytöstä Network-välilehdeltä DNS-, DHCP- ja IPv6-protokollat. Lisäksi poista käytöstä sivun alalaidasta IPMI.
30. Ota käyttöön VLAN ID -ominaisuus Network-välilehdeltä. Aseta VLAN ID-kohtaan arvoksi iDRACin käyttämä VLAN.
31. Services-välilehdeltä poistetaan käytöstä Telnet- ja SNMP-protokollat. Lisäksi sivulta otetaan VNC-palvelin pois käytöstä.
32. Poista käytöstä myös serial-yhteydet Serial- ja Serial Over LAN -välilehdiltä.
33. iDRACin käyttöönotto on nyt valmis.

HUOM! Dokumenttia jouduttu muokkaamaan julkaisun takia. Dokumentista on poistettu IP-osoitteita, laitenimiä, VLAN-numeroita, sekä palomuurin ja kytkimien konfiguraatioita. Dokumentti on tarkoitettu Combitech Oy:n ylläpitäjien käyttöön.