Pasi Lukkarinen

Data Center Automation- and Hybrid Cloud System Requirements

Metropolia University of Applied Sciences

Master of Engineering

Degree Programme

Thesis

29 May 2020

Author Title Number of Pages Date	Pasi Lukkarinen Data center automation- and hybrid cloud system requirements 58 pages + 6 appendices 29 May 2020
Degree	Master of Engineering
Degree Programme	Information Technology
Instructors	Juha Honkanen, Team Leader Ville Jääskeläinen, Title Principal Lecturer

This master’s thesis defines requirements for a new hybrid cloud- and automation solution in data centers of the case company. A hybrid cloud solution enables a resource usage from a local data center or utilizing the resources from public- or private clouds. It also gives possibility for a user to choose a location where to deploy workload.

A data center automation solution offers an automation platform for the case company specialist to automate their daily tasks by extending a target of the commands from one server to many and offering a programmable interface to the environment. It also enables a quick way to analyze the maintained environments.

Both hybrid cloud- and automation tools need to be integrated and cooperate with existing environment such as Configuration Management Data Base (CMDB), IT Service Management (ITSM), hyper visors, monitoring, backups, anti-virus systems and patching tools.

The objective of this thesis was to define requirements based on which the case company can prepare a Request for Proposal (RFP) documentation, can evaluate the candidate solutions and decide the best solution for the case company.

The study was conducted by using a case study research method. Data collections consist of interviews of the different stakeholders, investigation of published material about the topic, investigation of the case company documentation, processes and setting a benchmark for the ITSM of the case company. Business case calculations were conducted with one possible vendor to understand financial impacts on the economy of the case company. Request for Information (RFI) was conducted in order to achieve more information about the solutions on the markets.

The outcome of the thesis is a list of requirements for both hybrid cloud and data center automation solutions. On automation side a justification, why each requirement is on the list, are included beside the requirement. Requirements are divided into five different categories and a division between optional and mandatory requirements can be found from the list.

The outcome helps the case company to finish an RFI process by conducting a Proof of Concept (POC) with two chosen solutions and continue to RFP -phase smoothly after that. The thesis includes also discussions for the next steps related to possible system acquisition. What company should consider when totally a new way of doing things will be launched as it has impacts on different sides of the company, starting from the business process related to a server order and ending to a simple maintenance task to be done by the case company specialist.

Keywords	Hybrid Cloud, Data Center Automation, Requirement Definition, Server Automation, JHS, Juhta, Public Procurement, RFI, RFP

Contents

Appendices

List of Abbreviations

AS-IS environment	Environment which are adapted under the case company's service without any migration to common and standard services.
AWS	Public cloud service owned by Amazon
Azure	Public cloud service owned by Microsoft
Case company	Government ICT-center, governmental company which produces ICT services for the central government
Co-loco, colocation	Data center which is not owned by the case company but part of premises and rights to use of data center technology are rented. There can be multiple customers in the premises.
DevOps	Framework where Development and Operations personnel and tasks are done by same group of people. Activities and processes are supported by heavy automation.
CMDB	Configuration Management Data Base
FTE	One FTE (Full Time Equivalent) means that one employee is working full-time
Hybrid cloud	Cloud services scaled across private and public clouds. Gardner "Hybrid cloud computing refers to policy-based and coordinated service provisioning, use and management across a mixture of internal and external cloud services."
IaaS	Infrastructure as a Service
ITSM	IT Service Management
JHS	Julkisen Hallinnon Suositukset, Recommendations of Public Administration
Juhta	The Advisory Committee on Information Management in Public Administration (Julkisen hallinnon tietohallinnon neuvottelukunta)
PaaS	Platform as a Service
POC	Proof of Concept
RFI	Request for Information
RFP	Request for Proposal
VM	Valtiovarainministeriö, the Ministry of Finance

1 Introduction

This thesis focuses on requirements definitions for the system which provides data centers automation and hybrid cloud capabilities for the case company and its customers. The current model to manage and configure data centers services is mostly manual. It needs more automation as well as a portal for customers' needs and APIs to manage their IT services in a more effective and modern way.

The case company produces sector-independent ICT services for the central government. Sector-independent ICT services of the government refers to services or arrangements which don't require significant sector-specific know-how, they are so called common IT services and they are based on commonly used hardware and software solutions and technologies. The special security and preparedness need of the central government are taken into consideration in the production of the services.

The case company wants to harmonize and standardize the IT services and the related service management processes and procedures it offers for government agencies, institutions, public authorities and parliament.

Information System Services (ISS) division of the case company is producing hosting services which includes VAKA-case company (case company KApasiteettipalvelut) services which are delivered from local data centers of the case company. Data centers are in Finland and they are so called co-locations. Major data center rearrangements are being done at a moment when this thesis is being written.

VAKA-case company services consist of services shown in Table 1 below.

Table 1. Vaka case company services

Service
Virtual and physical server capacity services
Database support and capacity services
Backup services
Storage system services
Infrastructure monitoring services
Load balancer services

Virtual and physical server capacity services includes server provisioning and maintenance according the separate agreement of the service levels. Officially supported operating systems are

Windows and Redhat linux but under maintenance there are still large variations of the different linux variants. Used virtualisation platforms are HyperV, ESX and OVM.

Database support and capacity services provides new database instances and maintenance for them. Supported database are Mssql, Oracle and Postgre sql. Service includes deployment maintenance, backing up and monitoring of the db instance.

Backup services secures data of the systems in VAKA environments. There are available traditional backups based on tape and robot technologies and modern technologies based on system snapshots and disk storages.

Storage system services provides disks for the systems to be used in VAKA service. Available are Storage Area Network (SAN)- and Network Attached Storage (NAS) disks. SAN storage system offers different type of disk for different purpose like Solid-state drive (SSD) for the systems requires very fast performance from storage and Serial-Attached SCSI (SAS) disk for the system not so critical requirements. Available are also SAS disk with an SSD acceleration and a Near Line (NL)-SAS disk with a lowest performance.

Infrastructure monitoring services monitors services, traffics and equipment in VAKA environments. Used tools are System Center Operations Manager (SCOM) and Paessler Router Traffic Grapher (PRTG).

Load balancer services offer load balancing for the incoming traffic in VAKA environments. There are variable methods available how load balancing can be implemented.

1.1 Business Challenges

Even though the usage of public clouds is growing among governmental actors still the case company’s customers are not able to run all their IT services in public clouds because of legislation and governmental guidelines and instructions. Restricting laws and guidelines are e.g. GDPR (Union, 2016), KATAKRI (Defence, 2015), and Emergency Powers Act (Government, 2011). This is the reason why the case company needs to maintain local data centers and deliver services from there.

Managing and delivering capacity services on a traditional way is work force intensive, slow, exposed to human mistakes and expensive. To achieve any deliverables, such as a fully functional server with all needed components installed and tested, requires many kinds of cooperation with professional groups, coordination and still the quality of the deliverables varies, and a lead time is some days, even weeks.

One example of a time-consuming management task without automation is a server environment analyses and patching according to the requirements. In Spring 2017 40 people stopped their daily work and started to explore and remediate systems because of the WannaCry worm. It took five days and hundreds of hours to identify and fix vulnerable systems.

The case company is lacking technical people and there are difficulties to recruit suitable ones. The cost efficiency requirements prevent to add employees endlessly. Technical people are stressed because of over whelming amount of work and results they should be able to deliver. Customers pressure is strong to get “cloud like” services also from local data centers.

1.2 Objective and Outcome

This work defines requirements for the system which offers tools for specialist of the case company to automate technical management tasks and offers “cloud like” interface or portal and APIs for specialist of the case company and customers to build and manage their own environments and services.

Based on these requirements new system candidates can be evaluated and final decision can be made to purchase most suitable system for the purpose. Logical level architecture descriptions are also produced to help to describe the wanted system.

1.3 Scope of Study

This thesis emphasis on:

1. Requirements definition for data center automation and cloud services
2. Requirements gathering and definitions methods
3. Business case calculation and justification of the system
4. Defined requirements
5. Governmental procurement process, it’s requirements and impact on used process

Originally it was meant that cloud requirements should be gathered based on VAKA- case company environments. Soon it was obvious that there should be included requirements from VAKA

Cloud services (based on public clouds Azure and AWS) also in the solution and continue talking about hybrid cloud solutions instead of a private cloud.

The requirements definition phase includes also mapping the surrounding infrastructure where the new system should operate, and systems where it should be connected to. Based on this information and defined requirements a high-level architecture was described.

This thesis has been divided into 7 sections and references. The first section introduces the research problem and its scope. In the section two, research approach is described including Juhta, JHS framework, government procurement and research design. The section three presents and defines cloud computing and server automation terminology. Information about server automation and different approaches to the topic are also presented there.

Section four concentrates as-is situation in the case company and section five presents the RFI and its' results. Section six presents the solution and how it was built. Conclusions and discussion are shown in section seven.

2 Research Approach

This section describes the research approach and design in this thesis. First it describes a set of recommendations from JHS 173, (Juhta, 2009) for development of ICT services in public sector. After that there are explained shortly governmental procurement process which can affect even content of the tender. Third part of the sections describes the design of the study.

2.1 Juhta Recommendations

JHS (Juhta, 2006) recommendations have been developed since 1992. JHS are applying to IT administration of the government and municipalities. It offers definitions, procedures and instructions to improve the compatibility and co-operations of IT systems across the administration borders. Recommendations are meant to minimize parallel development work and guiding the development activities to adapt common and tested procedures. Recommendations are accepted by the Juhta. Juhta has ended its activities in the end of 2019 and JHS recommendations will be maintained by “Digital and Population Data Services Agency” from beginning of 2020.

JHS173 (Juhta, 2009) “Development of ICT- services, Requirement definitions” (ICT-palvelujen kehittäminen: Vaatimusmäärittely) gives suggestions and tools how the requirement definitions should be done. It collects best practices and instructions of the public sector together about the topic.

JHS173 is tool for the different stakeholders when requirements definition is conducted. Stakeholder are:

1. Information system owners
2. Decision makers for new information systems
3. People who are planning purchases
4. Project managers
5. People who conducting requirements definitions

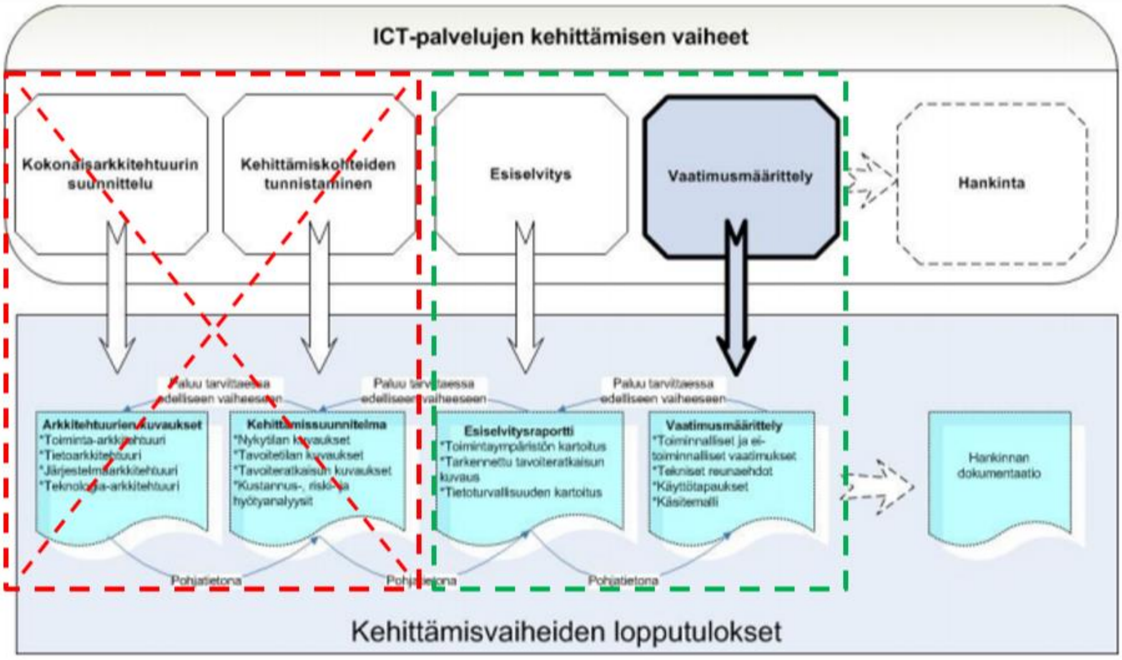

ICT-palvelujen kehittämisen vaiheet
Kokonaisarkkitehtuurin suunnittelu
Kehittämiskohteiden tunnistaminen
Esiselvitys
Vaatimusmäärittely
Hankinta
Paluu tarvittaessa edelliseen vaiheeseen
Paluu tarvittaessa edelliseen vaiheeseen
Paluu tarvittaessa edelliseen vaiheeseen
Arkkitehtuurien kuvaukset
*Toiminta-arkkitehtuuri
*Tietoarkkitehtuuri
*Järjestelmäarkkitehtuuri
*Teknologia-arkkitehtuuri
Kehittämissuunnitelma
*Nykytilan kuvaukset
*Tavoitetilan kuvaukset
*Tavoiteratkaisun kuvaukset
*Kustannus-, riski- ja hyötyanalyysit
Esiselvitysraportti
*Toimintaympäristön kartoitus
*Tarkennettu tavoiteratkaisun kuvaus
*Tietoturvallisuuden kartoitus
Vaatimusmäärittely
*Toiminnalliset ja ei-toiminnalliset vaatimukset
*Tekniset reunaehdot
*Käyttötapaukset
*Käsitemalli
Hankinnan dokumentaatio
Pohjatietona
Pohjatietona
Pohjatietona
Kehittämisvaiheiden lopputulokset

Figure 1 ICT development phases

As seen in Figure 1, “Vaatimusmäärittely” phase is located after “Esiselvitys” pre-investigations -phase (jhs 172, 2009) which means pre-investigations should be conducted before the requirements definitions. These JHS documents are guides not rules. This means document includes suggestions and instructions not requirements.

“Kokonaisarkkitehtuurin suunnittelu” and “Kehittämiskohteiden tunnistaminen” were not part of this work.

Phases of requirements definitions are described below in Figure 2.

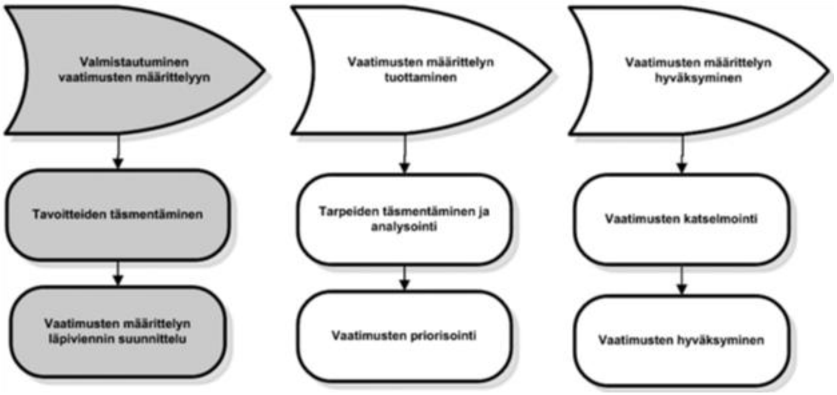

Valmistautuminen vaatimusten määrittelyyn
Tavoitteiden täsmentäminen
Vaatimusten määrittelyn läpiviennin suunnittelu
Vaatimusten määrittelyn tuottaminen
Tarpeiden täsmentäminen ja analysointi
Vaatimusten priorisointi
Vaatimusten määrittelyn hyväksyminen
Vaatimusten katselmointi
Vaatimusten hyväksyminen

Figure 2 Phases of requirement definition

1. Preparing requirements definiton, “Valmistautuminen vaatimusten määrittelyyn” includes objective definitions and planning of the requirement definition.
2. Implementing or producing requirements definition, “Vaatimusten määrittelyjen tuottaminen” includes objective definitions and analyses and prioritization of the requirements.
3. Accepting the requirements,” Vaatimusten määrittelyjen hyväksyminen” includes verifying and accepting the requirements.

Requirements have been divided in three categories in document as shown in Figure 3.

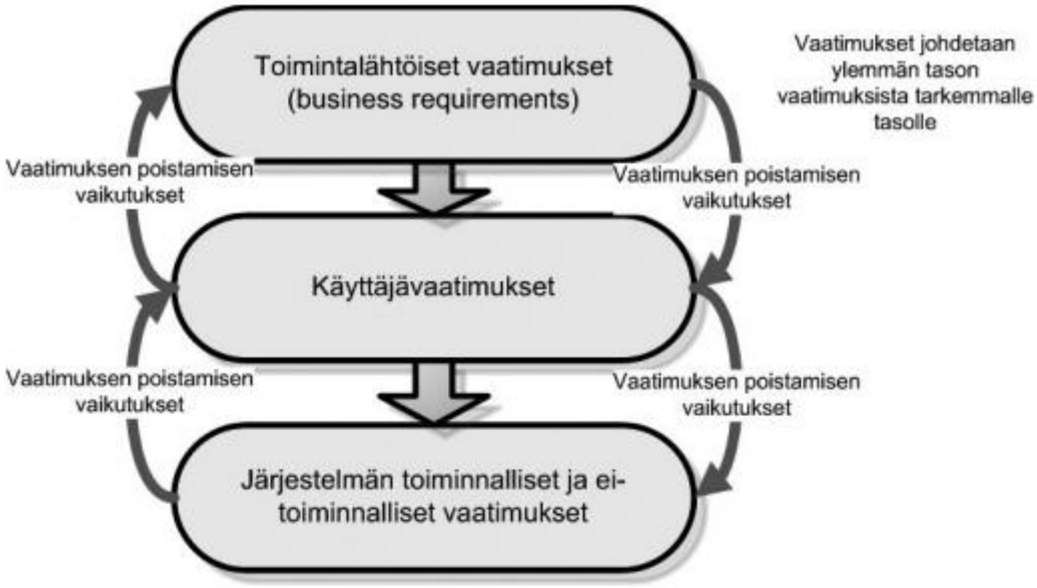

Toimintalähtöiset vaatimukset (business requirements)
Vaatimukset johdetaan ylemmän tason vaatimuksista tarkemmalle tasolle
Vaatimuksen poistamisen vaikutukset
Vaatimuksen poistamisen vaikutukset
Käyttäjävaatimukset
Vaatimuksen poistamisen vaikutukset
Vaatimuksen poistamisen vaikutukset
Järjestelmän toiminnalliset ja ei-toiminnalliset vaatimukset

Figure 3 Requirement groups and hierarchy

Business Requirements will be derived from the business processes and high-level visions and strategies.

“Käyttäjävaatimukset”, User Requirements describes actions what users supposed to be able to do by using the system. These requirements are described by use cases, real life examples or using different scenarios.

“Järjestelmän toiminnalliset ja ei-toiminnalliset vaatimukset”, functional and non-functional requirements of the system. Functional requirements determine functionality of the system. Non-functional requirements determine ‘other’ requirements for the system like usability and security related requirements.

Requirements can be defined from many different areas and stakeholders as we see in Figure 4, Requirements can be derived from the laws and regulations, management, end users, information security, customers and cooperation partners, vendors and actors of the business area.

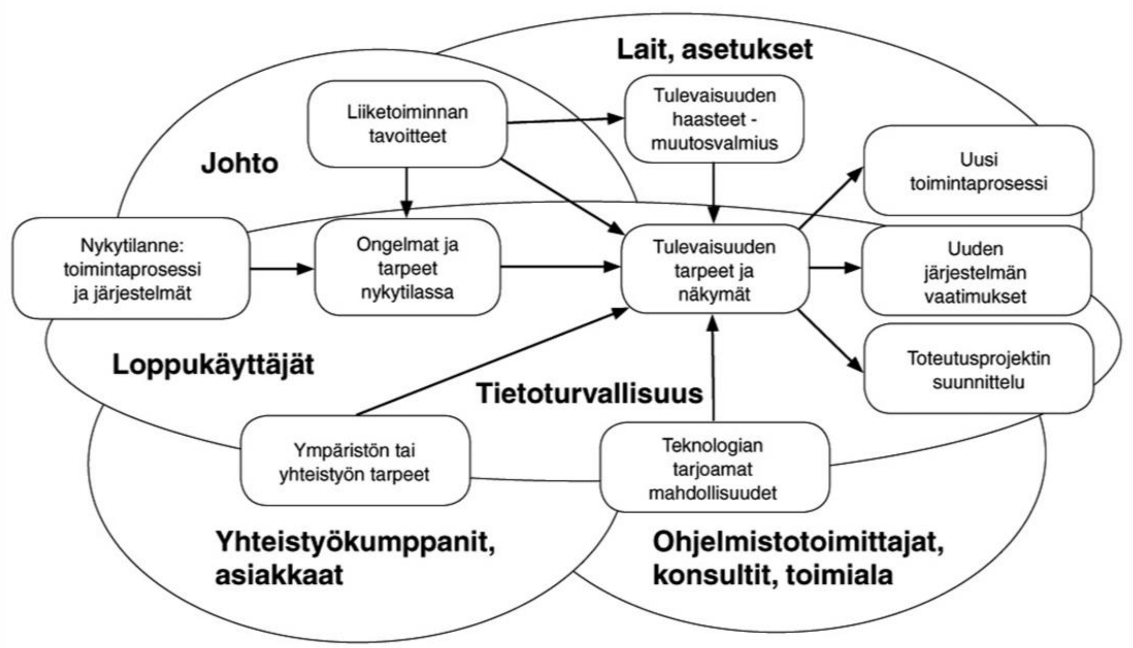

Lait, asetukset
Johto
Liiketoiminnan tavoitteet
Tulevaisuuden haasteet - muutosvalmius
Uusi toimintaprosessi
Nykytilanne: toimintaprosessi ja järjestelmät
Ongelmat ja tarpeet nykytilassa
Tulevaisuuden tarpeet ja näkymät
Uuden järjestelmän vaatimukset
Loppukäyttäjät
Tietoturvallisuus
Toteutusprojektin suunnittelu
Ympäristön tai yhteistyön tarpeet
Teknologian tarjoamat mahdollisuudet
Yhteistyökumppanit, asiakkaat
Ohjelmistotoimittajat, konsultit, toimiala

Figure 4 Stakeholders of Requirements

(Juhta, 2009, p. 13) suggests that views from different stakeholders should be available and specially system users have the best knowledge of the processes, old system's pros and cons.
Management must engage to the project and act actively to support project during the project lifecycle.

Functionalities are described as processes and use-cases. Users are described by different groups and roles depending on roles, access rights or amount of usage.
Requirements will be prioritized to be able to manage time and costs related to project. It is important to understand, is a requirement improvement type or must, for the sake of a usability of it. Prioritization will be done by projects' steering group after the evaluation.

(Juhta, 2009, p. 17) Data for requirements can be gathered various ways. Possibilities mentioned are existing documentation, questionnaire forms, oral interviews, oral structured interviews, oral unstructured interviews. In chapter 9.6 group-based meetings are listed which are, “aivoriihi”, focus groups and workshops. Some examples are FAST (facilitated application specification technique), JAD (Joint Application Design) sekä RAD (Rapid Application Development)-framework.

From requirement definition process must deliver list of requirements which include at least following information like uniq ID, requirement, originator of requirement, date, prioritization and justification.
If the list is used a part of RFI or RFP, a field for vendors’ comment is needed.

Security part of the JHS173 will be overwritten by the requirements of applicable part, chapter 5, Katakri (Defence, 2015, p. 9).

2.2 Government Procurements

The Government Procurements process rules and instructions are explained in Handbook on Government Procurements 2017, (Valtiovarainministeriö, 2017). As mentioned in abstract of the document. *The handbook describes in detail the most important implementation stages of the tendering process required by procurement legislation, as well as practical instructions on the implementation of procurements and agreements on procurements.*
There are mentioned in chapter 3.3. principles and objectives, e.g. that the law ensures that all vendors and other stake holders are treated equally, and tender process is transparent.

Available tender processes are listed and explained in chapter three. There are eight different processes where to choose. A used process needs to be decided case by case, according the total value of the case, nature of procurement, complexity etc. On practical level guide tells how the tender process need to be run and what are the options to do it.

A value of this this tender was over 500 000 € in a year which is the limit after the Tender should be treated as EU -level procurement. The Instructions concerned about this procurement are mainly mentioned in section 5 of the document.

2.3 Research Design

This section describes design of the research study. This research study is grouped into five different phases; business problem definition, data gathering, requirement definition and RFI as shown in Figure 5 below. The study does not cover the RFP- or POC phases and decision of the tool itself.

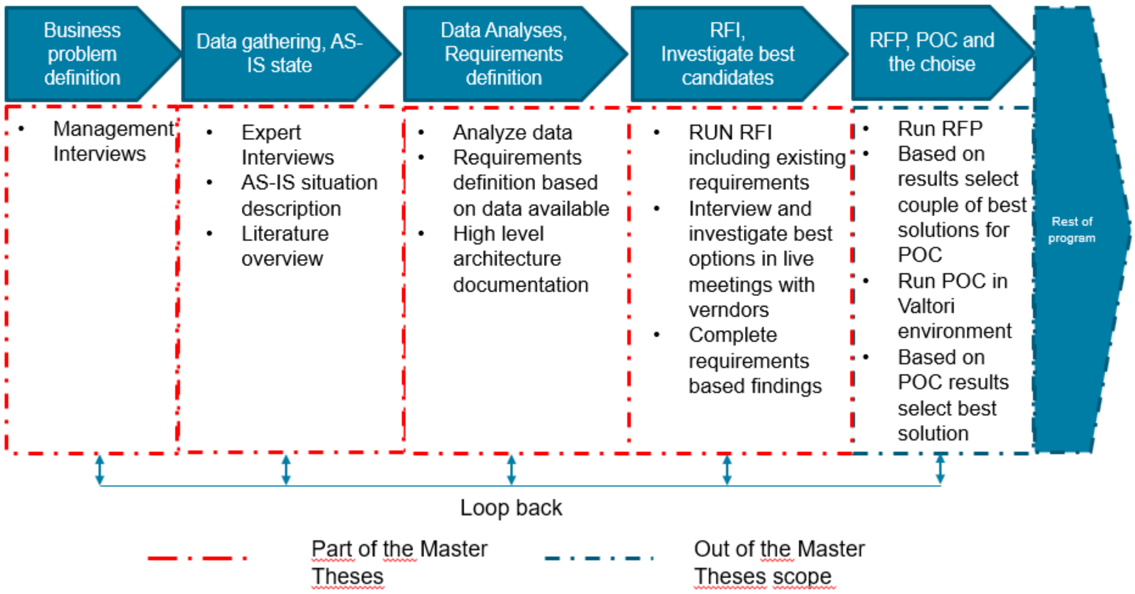

Business problem definition
Data gathering, AS-IS state
Data Analyses, Requirements definition
RFI, Investigate best candidates
RFP, POC and the choise
Rest of program
• Management Interviews
• Expert Interviews
• AS-IS situation description
• Literature overview
• Analyze data
• Requirements definition based on data available
• High level architecture documentation
• RUN RFI including existing requirements
• Interview and investigate best options in live meetings with verndors
• Complete requirements based findings
• Run RFP
• Based on results select couple of best solutions for POC
• Run POC in Valtori environment
• Based on POC results select best solution
Loop back
Part of the Master Theses
Out of the Master Theses scope

Figure 5 Research design

Business problem definition phase determines the actual problem what the company were facing. Data gathering phase concentrates to investigation of the existing data about the topic and investigating situation in the case company. There is need to understand how company operates at a moment and what kind of the challenges technical people are facing and what would be their solution for the existing challenges.

In data analyze and requirements definition phase all collected data were gathered together and list of requirements was defined.

In the RFI phase, based on the defined requirements RFI document was published. Answers were analyzed. After that few most promising and most suitable solutions were selected and their vendors were asked to give a presentation according the predefined use cases. Based on a material gathered in and based on these presentations final requirements were defined.

In order to define requirements for a new tool or solve the existing problem somehow else, researcher collected information from various of sources.

Interviews or discussions started from the management level by collecting information about problems and challenges related to VAKA services. Management level interviews were conducted with Unit leader, Capacity service team leader and VAKA service product manager. Management interviews gave a high-level picture of the challenges and based on these interviews business requirements were defined.

Researcher interviewed the case company's technical specialists and management as well architect of the customer of the case company. Interviews and discussion were held according the schedule in Table 2.

Table 2 Interviews and discussions

Role	Topics	Date	Time
Unit Manager Capacity services	- Challenges - Setting up program,	19.10.2017	15:00-16:00
Team lead VAKA-Case company	- Challenges - People, organizations - Project planning	9.11.2017	14:30-15:30
Virtualization specialist/Architect	- Technology description - Challenges - Pain points - Automation possibilities	8.12.2017	10:00-11:00
CMDB ITSM (TOP) specialist	- Technology description - CMDB/ITSSM usage and policies	22.12.2017	12:00-13:00
Backup responsible	- Technology description - Challenges - Pain points - Automation possibilities	22.12.2017	09.00-10:00
Product manager VAKA-Case company	- Challenges - Customers view - Business	27.12.2017	13:00-14:00
Monitoring responsible	- Technology description - Challenges - Pain points - Automation possibilities	27.12.2017	12:00-13:00
Storage systems responsible	- Technology description - Challenges - Pain points - Automation possibilities	29.12.2017	10:00-11:00
Physical servers, virtualization responsible	- Technology description - Challenges - Pain points - Automation possibilities	12.1.2018	12:00-13:00
Automation responsible	- Technology description - Challenges - Pain points - Automation possibilities	12.1.2018	13:00-14:00
Servers, linux responsible	- Technology description - Challenges - Pain points - Automation possibilities	12.1.2018	14:00-15:00
Network architect/VY-networks	- Technology description - Challenges - Pain points - Automation possibilities	17.1.2018	09:00-10:00
Network/DC- networks	- Technology description - Challenges - Pain points - Automation possibilities	17.1.2018	10:00-11:00

Security officer responsible	- KATAKRI, Requirements for the automation- and private cloud system itself	2.2.2018	15:00-16:00
Customer architect	- Customer technical environment - Customer needs and requirements	8.1.2019	

Technology specialist interviews concentrated to get information of each specialist own area. What kind of technology is being used and how things are being done at a moment. What are the challenges and automation possibilities?

Target of these interviews was to find out pain points of the processes and to gather improvement possibilities already know by the specialist.

Published material, investigations and studies related to topic cloud computing and data center automation were investigated to enrichen knowledge about the topic. To fulfill the picture of existing processes of the case company, relevant documentation and data from ITSM ticketing system was investigated.

Company strategy gave a high-level steering for the project. Requirements defined related to the topics mentioned in the strategy helped the project decide what is the right direction to proceed with the DC challenges. They also gave a base line against what to decide when requirements are being estimated.

Investigation of virtual server provisioning process highlights the steps needed in these environments and it determines compulsory requirements what automation should be able to do in new server provisioning use case. Change management process in ITSM needs to be able to understand what the steps are, where automation should be able to run process forward and what kind of authorization is required in existing process.

Investigation of the virtual server change requests from the history gives a benchmark what is the performance of the organization at a moment. The target was reveal pain points of the process in terms of consumed time and SLAs.

Financial view to the case was created like how much savings in terms of money and working effort can be achieved. A sort of business case is was developed together with a vendor who interviewed core people about existing way of working, time spent in tasks and compares values to the case they would be done by using their own tool.

In requirements definition phase requirements were defined and they were accepted by the team. High level information system diagrams were published which helped to understand the integrations to existing information systems.

In this case part (RFI) of the pre-investigations (jhs 172, 2009) was done during the requirements definition phase. RFI phase was used to collect information from the markets. In this phase, a representative from procurement unit joined into the project, to find out suitable way to run process through. RFI document and appendices were written and published. Document were based on the requirements defined in previous phases. Answers were analyzed, and most suitable vendors were asked to give a presentation in a private session where tools were demonstrated in live environment by following the given agenda of the case company. Vendors were also asked relevant questions to complete picture of the product and its possibilities. Based on these sessions and answers got, final requirements were completed. Final validity, reliability and priority of the requirements were decided in 'priority' meeting together with participants from the different stakeholder groups (product management, line management, technical specialists, security and customer).

The Customer view (business) was represented by product management. Security requirements were clear and undeniable, so a security representative didn't participate in meeting. All security related requirements were accepted. In this meeting requirements were divided in two groups, mandatory and optional requirements.

In order to be transparent in RFP process, optional requirements were supposed to be weighted with certain amount of points by each requirement. These points calculated together will decide the solution to be purchased.

The 'priority' meeting with key stakeholders representatives and wide range of interviews presented in Table 2 with stakeholders gave reliable and encompassing picture of the existing situation of the company and priority of all requirements. Besides these actions any other reliability or validity related confirmations were not done.

3 Cloud Computing and Server Automation

This section introduces different cloud computing options, benefits and challenges related them in the case company context. Data center automation possibilities and suggestions will be investigated as well.

3.1 Cloud Computing

Cloud computing terminology and its various subcategories are widely used, but actual meaning of terminology varies depending on the user. In this chapter we look over the terminology of public-, private- and hybrid cloud.

Cloud is defined by Gartner, (Waite, 2020) *as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies.*

3.1.1 Public Cloud

Public clouds are typically understood as three main cloud services of vendors Google Cloud Platform (GCP), Amazon AWS and Microsoft Azure. It can be used anybody by just logging in and giving the credit card number to be charged.

As (Goyal, 2014) describes *public cloud resources are offered as a service, usually over an internet connection, for a pay-per-usage fee. Users can scale their use on demand and do not need to purchase hardware to use the service. A public cloud is hosted on the internet and designed to be used by any user with an internet connection to provide a similar range of capabilities and services.*

Microsoft (Microsoft, 2020) defines the public cloud: *The public cloud is defined as computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them. They may be free or sold on-demand, allowing customers to pay only per usage for the CPU cycles, storage, or bandwidth they consume.*

3.1.2 Private Cloud

Private clouds are typically understood as companies dedicated on-site data center environments which are taken care by companies themselves. As (Goyal, 2014) determines *private cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. The cloud infrastructure is accessed only by*

the members of the organization and/or by granted third parties. The purpose is not to offer cloud services to the general public, but to use it within the organization.
(Microsoft, 2020) states about the topic. *Private cloud is defined as computing services offered either over the Internet or a private internal network and only to select users instead of the general public. Also called an internal or corporate cloud, private cloud computing gives businesses many of the benefits of a public cloud - including self-service, scalability, and elasticity - with the additional control and customization available from dedicated resources over a computing infrastructure hosted on-premises*.

Private cloud described by (Waite, 2020).
In private cloud context:

- Private means features like infrastructure isolation and single tenant
- Cloud is described like elastic, used self-service, metered by use and services delivered by control plane

Private is determined by Gartner that compute and storage part of the service are dedicated to one customer. Different cloud vendors are using private term when the compute part is single- tenant and rest of the infrastructure are shared. Waite also high lights that "on-premise" does not mean necessarily private.
As-a-service offerings with user self-service, elasticity and metering by use falls in cloud category and on the other hand quite many virtualization farms, automation and traditional data center infrastructures do fail the cloud part of the term "private cloud".
(Waite, 2020) also declares that "*Most organizations move through maturity stages of virtualization, automation, as-a-service offerings and finally, hybrid IT.*"
In a, "as-a-service" phase will be delivered characteristic features of the cloud through the control plane.
Anyway, what matter is not terminology but the service which is delivered by the business requirements.
(Waite, 2020) gives three aspects to consider when deciding to modernize workloads.

- Tenancy, what parts of infrastructure are shared according the tenants? What thoroughly need to be private?
- Control plane, what is location. who manage and operates it?
- Infrastructure location, where it is located and who operates it?

Alternatives based on infrastructure- and control plane location are shown in Figure 7.
There are some examples of technologies mentioned how to implement solutions. In the picture are described traditional data center services and public cloud providers also as-a-service.

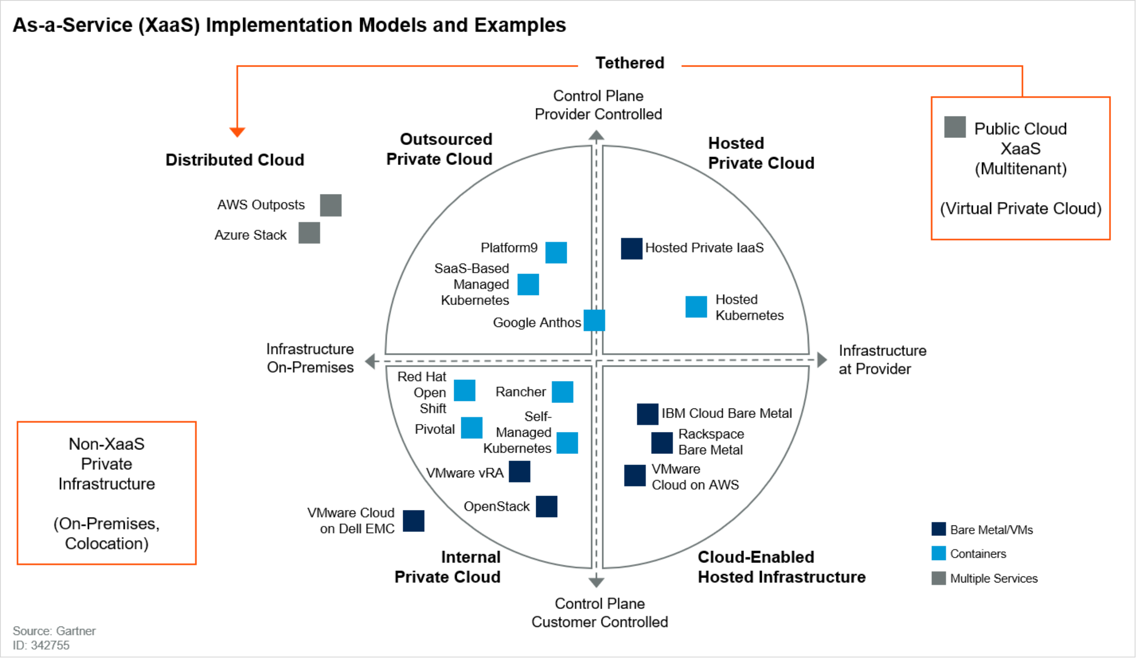


Figure 6 As-a-Service Implementation Models and Examples

Non-XaaS private infrastructure, refers to virtualized and nonvirtualized environments without an as-a-service control plane. Infrastructure can be on-premises in traditional data centers or located in a colocation or third-party hosting facility.

Internal private cloud is traditional on-premises or colocation-based IaaS, CaaS or PaaS environments where the customer is also managing the control plane. They offer the most visibility location for compliance or regulatory reasons but outsources the complexity of running the control plane to the provider.

Distributed cloud solutions are offered by public cloud vendors. Solutions offering public cloud services from various physical locations. Operation, governance, updates and the evolution of the services are the responsibility of the originating public cloud provider.

Location may be important for other reasons, including data sovereignty. In these scenarios, distributed cloud provides organizations the capabilities of a public cloud delivered in a physical location that meets their requirements.

Outsourced private cloud is based on an outsourced control plane run as a SaaS-style offering by a provider. This type of environment allows the customer to maintain hardware in a private and control of the full stack from racks to applications, but also involve the most effort on the customer’s part.

Hosted private cloud solutions where provider owns and manages hardware, virtualization and control plane, and the customer is only responsible for management of their own applications and data.

Cloud-enabled hosted infrastructure is also known as bare metal as a service (BMaaS), these types of offerings provide dedicated hosts and storage on demand through an as-a-service interface.

These solutions still require the customer to implement and manage their own IaaS, CaaS or PaaS software on the bare-metal infrastructure.

Public cloud XaaS offer IaaS-, CaaS- and PaaS services from large public cloud providers. These solutions are off-premises and multitenant but should be the first option considered for workloads that require as-a-service functionality.

3.1.3 Hybrid Cloud

Hybrid cloud is typically understood as a cloud service which includes components from both private and public clouds.

(Goyal, 2014) describes, *hybrid clouds are more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity but is bound to others through standardized or proprietary technology that enables application and data portability among them. A hybrid cloud is a composition of at least one private cloud and at least one public cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms. Hybrid cloud infrastructure is a composition of two or more clouds that are unique entities, but at the same time are bound together by standardized or proprietary technology that enables data and application portability. In hybrid cloud, an organization provides and manages some resources inhouse and some out-house.*

(Microsoft, 2020) states, *a hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them. When computing and processing demand fluctuates, hybrid cloud computing gives businesses the ability to seamlessly scale their on-premises infrastructure up to the public cloud to handle any overflow—without giving third-party datacenters access to the entirety of their data.*

3.2 Server Automation

Before starting a servers automation program there are few things listed by (Delory, 2017) which need to clear out in an organization. These things need to think in advance because the answer brings in building a solution subject to the constraints of both technology and process. Questions are:

1. Will you automate physical hardware configuration? If so, how?
2. How will you configure network settings?
3. How will you configure privileged accounts?
4. Is the server managed by IT operations systems? How are those configured?

1.) Physical hardware configuration

Physical hardware or server deployment automation is really matter of question “Is it worth of doing by yourself or automate it at all”. If your organization install only few physical servers in a year, there is no point to start automation process. If you use more money or time to get automation done and maintain it, than you use to deploy servers manually, you should consider your options to manage physical server installations.

Options might be:

- Hosted infrastructure, usage of outsourced vendor or even public cloud provider to get IaaS type of service for physical servers.
- Preconfigured infrastructure delivered by the server provider might be one possibility
- Stay in manual process and install servers by yourself, especially when there are only few servers to be installed in a year.

If you decide to implement automation you probably need to find out do you need any frameworks between your automation framework and hardware. This could be case e.g. if you have hardware from many different vendors and APIs varies. This is always matter of decision what you can do through the framework and how much it cost money and how much it requires work to implement and maintain.

Lessons learned by (Delory, 2017):

- “Automate a process only when doing so delivers a quantifiable net benefit to the organization.”
- “The Pros and Cons of Frameworks”

Some of the possible quantifiable net benefits are mentioned:

- Cost savings, in terms of monetary Return Of Investment, (ROI) is the ultimate proof of automation project value.
- Labor savings means that automation saves more time and effort than it takes to build it. This could lead even savings of labor costs If people are not needed anywhere else.

- Compliance and/or error prevention can be only justification for automation in some cases.

2.) How will you configure network settings?
Thinking about network automation helps you to understand few things which are typical for the implementing successful automation.

Typically network configuration process for the physical server requires four stages:

- Acquire IP address
- Create Domain Name System (DNS) entry for the server
- Add the server in load balancer
- Create needed firewall rules for the server.

This is quite complex task to automate when automation need to configure all entries and make end-to-end test after implementation.
You need consider again is this something you want, and you can implement.
Typical case is that if you keep it manual work you need to make a separate request, hand off responsibility to someone else and wait at least couple of times during the process, depending on the organization where you are working.
Each hand off is sure source of delay and potential source of miscommunications and errors.

Some phases, e.g obtaining IP address might need face-to-face discussion with the network administrator and then challenges are not technical, but they are in process. You need to fix process first.
(Delory, 2017) states: *Automation is the implementation of a workflow. For a task to be automatable, therefore, it must be describable as a coherent and logical sequence of tasks, without resort to human intervention or decision making.*

All lessons learned by (Delory, 2017) under this topic are:

- “Handoffs are inimical to an efficient, automated workflow.”
- “Any process that relies on human action or judgment is not automatable and must be eliminated.”
- “Before you begin, you must be able to describe the workflow clearly and unambiguously. You can't automate what you don't understand.”

3.) How will you configure privileged accounts?
(Delory, 2017) comes to conclusion that this is more process related challenge than technical one. There is no need for third party framework because most common tools on market like Microsoft’s Active Directory and most Identity and Access Management (IAM) products are capable to be part of automation process.

Lessons learned by (Delory, 2017): “Design for compliance and Auditing”.
This means in practice that you need to have a policy according which you grant privileges and against what you will regularly audit the state of privileges access. This can be done easily by modern automation tools which can prevent configuration drifting even automatically if needed.

4.) Is the server managed by IT operations systems? How are those configured?
When you deploy new server there is need to join it under data center services like backup, monitoring, antivirus and patching. Typically, these services require agents to be installed and some configuration tasks in service side and this configuration might need a lot of information delivered like when backups can be done, what is needed to backup, when patching and possible reboot can be done etc. These questions are related to processes and policies once again. What kind of patching windows are available, how well we have defined server spec and file system structure what we will backup and so on?
Technically agent installations is easy part, collecting information from customer about the service related questions and delivering the answers to services by configuring them automatically can be even impossible. Even the processes can be rebuilt but existing tooling can prevent configurations by automation framework because lack of technical features like APIs.
If you can’t automate process totally do it as long as you can and consider removing obstacle in future development activities whatever they are

Lessons learned by (Delory, 2017):

- “Automation Capabilities Depend on the Underlying Systems”
- “Have Fallback Methods”

If you can’t remove obstacles preventing the full automation, remember partially implemented automation with some manual steps are better than no automation at all.

(Delory, 2017) collect lessons learned together as recommendations shown in Table 3 and he also extract three advices for each automation project shown in Table 4.

Table 3 Recommendations derived from lessons learned

Recommendation	Notifications
Determine whether the task is worth automating.	Instead of automating a manual task, it may be possible to outsource it to another provider or simply to leave the process as is. Automating a process that is rare or noncritical may be more trouble than it's worth.
Choose between addressing system components directly or using a third-party framework.	Frameworks can be a highly valuable intermediary between independent systems. But they always add complexity, and they may subtract functionality.
Fix the process first.	If you can't draw a flowchart of the underlying process, you can't automate it. If the underlying logic is incomplete or you don't understand it, then keep investigating until you have a clear map to a destination. If your flowchart includes decision points that require human judgment or manual action, then the process cannot be automated. Revise the process to eliminate human intervention or revise the scope of the automation effort to exclude those tasks that require it.
Design for compliance and auditing.	Use modern configuration management tools that bring a server to a desired state and keep it there. Your compliance with business policies will be assured, and your auditors will thank you.
Map the capabilities of the underlying systems.	These will determine the extent to which automation is possible. In many cases, the underlying systems will not support end-to-end automation. They must be replaced, or the automation project must be rescoped to exclude them. Mapping system capabilities is an important step when scoping an automation project because it will often determine the boundary of the project work.
Design a fallback method.	In practice, technical or process challenges often prove too difficult to overcome. When a preferred method is not viable, always have a Plan B.

Table 4 Advices for Automation Project

Advice	Notifications
Implement a minimum viable product.	Find the threshold at which an automation initiative provides real value and make that the goal of the initial project. Grow from that point, adding more value over time. Trying to implement a comprehensive end-to-end automation initiative will delay the project too long — if end-to-end automation is even possible at all.
Appoint an automation architect.	As shown above, automation projects will encounter both technical and business process challenges. Automation will require an architect who is both capable of addressing the technical challenges and empowered to address the business ones. Forthcoming Gartner research will explore the role of the automation architect in depth.
Measure the value of automation in time and money saved.	Showing an actual monetary return on investment is the ultimate trophy for an automation project. But even if the value cannot be measured in cash, measure gains in efficiency and productivity

As we can see by answering to four questions given, we will find out pretty much what we have ahead when we will start automation project.

Stated by (Delory, 2016) automating entirely server lifecycle is complicated task and requires many kinds of tools and skills in organization. What make it hard is the cross sections of complicated technology tasks and business processes and requirements demanding to make everything happen by “one klick”.

(Delory, 2016) dived automation tools in three categories. They are Server Automation (SA)- and Continuous Configuration Automation (CCA) -tools. Third category is tailored scripting which cannot be avoided when implementing edge cases.

Organizations will normally start automation activities to manage server configuration and automate server deployment by scripting. Quite soon it will be impossible to maintain framework together and help is needed by the tools. If organization want to make automation systematically and offer cloud like experience for the customers all three level of automation capabilities are needed.

- CCA-tools are mentioned like Puppet, Chef, Ansible, SaltStack and PowerShell Desired State Configuration (DSC). These kinds of tools offer developed methods to build and maintain server configurations and they are suggested to be used by the IT-organizations.

- SA-tools are usually commercial tools and they are commonly used in enterprise level data centers. There are verified tools like BMC Bladelogic, Microsoft SCCM and HPE server automation. These tools overlap by their capabilities with the CCA-tools but they can't be replaced and both are needed. How they will be used is depended on the combination of chosen tools and skills and passion of the people in organization.

- Scripting is needed you wanted or not. None of the tools mentioned before can't deliver full capabilities and features through the full server life cycle, but last mile needs scripting to deliver last wanted feature or function. Even the suggestion by the article is that scripting should favor other tools over the scripting, it is still needed.

In Table 5 are collected strength and weaknesses of each group of tools by the (Delory, 2016). It shows quite clearly that if we want to make automation seriously, we do need tooling on each level, especially in enterprise level automation programs.

Table 5 Comparison of Automation tools

Tools	**Strength**	**Weakness**
CCA	CCA tools offer a vastly improved and highly disruptive way to deliver and maintain configurations. They are the preferred tools for these tasks.	CCA tools operate in a relatively small part of the configuration management life cycle, and only where logic has been specifically written to enable them.
SA	SA tools operate across the entire configuration management life cycle, from initial provisioning through ongoing maintenance.	SA tools rely on scripts delivered to the target, making a CCA tool a far better option for deploying and maintaining configurations on targets.
Scriptis	Scripts can perform literally any task the computer itself can perform, making them the most flexible and customizable method.	Scripts are far more labor-intensive and fragile than any other means of automation. Thus, compared with other available options, scripts are inelegant and less favorable.

In Figure 8 are shown each tool capability indicated by thin line and thick line indicates the core functionality area. Most challenging task for the professionals is to make decision by which tool each task will be managed.

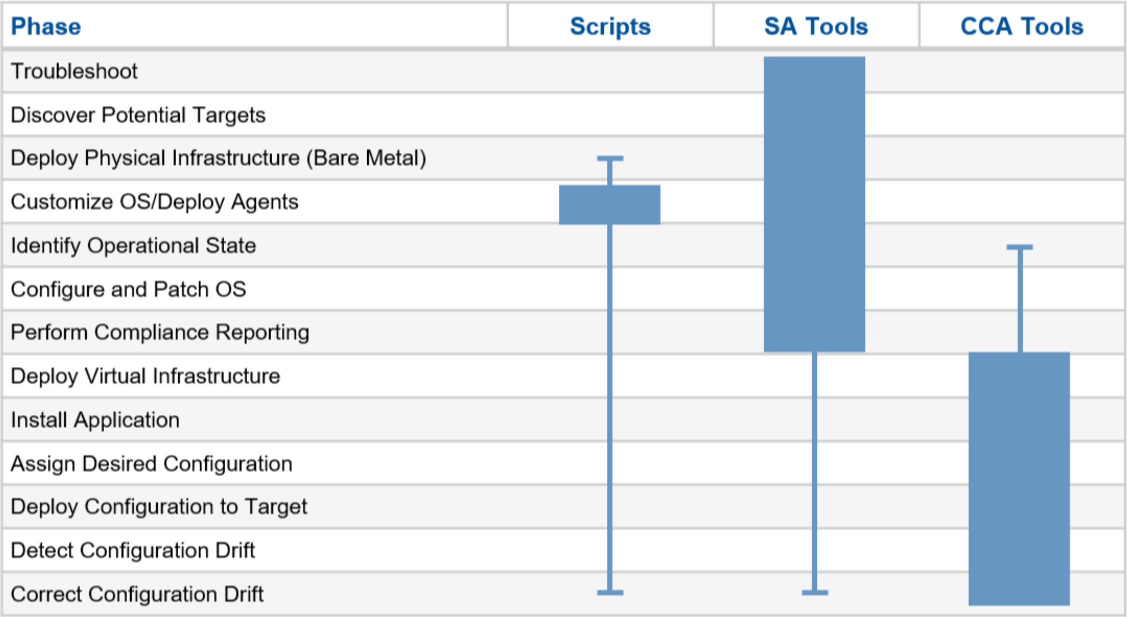


Figure 7 Tools capabilities by life cycle phase

Configuration management relationship to server automation has been also discussed by the (Delory, 2016) Server automation tools plays important role in process as deploying new servers and changing configurations and parameters in environment which are under configuration management systems. Automation tooling must be able to record specified changes in Configuration Management Data Base (CMDB) and information must be correct and up to date immediately when change has been done.

CMDB interact with data center automation- and other tools typically by:

- Orchestrators, which coordinate task between multiple tools and parties in data centers
- Application release automation frameworks, which automate software installations and deployments. These tools extend infrastructure management as part of the software development process.
- IT service managers provide user interfaces e.g. business usage. Typical solution is cloud like portal where customer can manage their own environments in data centers.

API's are playing vital role when information systems need to interact and collaborate with each other. One of the biggest barriers in data center automation is the lack of APIs.

4 Current State Analysis

This section first describes the interviews with different stakeholders and the results gathered. Second section presents investigation of the existing documentation and relevant findings related to this study. In third section are presented a workshop with one of a potential vendor and calculations to understand the economic influences on the case company if this kind of system would we launched. Server deployment process and its' implementation in ITSM are investigated as well as the benchmark of virtual server installations.

4.1 Interviews

This section presents interviews and findings from there. IT also presents categorization of findings and how it has been done.

Management discussion findings are collected in Table 6. In the table are collected topics only once even the same topic came out from more than one conversation.

According the discussion with management there were extracted high-level business requirements security, agility, quality and cost efficiency. These requirements helped to analyze existing processes and justify or estimate defined requirements.

Table 6 Management discussion results

Nmbr	Role	Notification/challenge	Responsible
1	Unit Manager	Server management and deployment challenge in VAKA-Case company product	1
2	Team manager	Lead time for new server too long	1
3	Product manager	Quality of deliverables varies	3
4		Too much man work is required, can't hire so many people as needed	2
5		Security cannot be confirmed	2
6		Expenses are too high for server installations and management requires a lot of manpower	3
7		Acting according the strategy	1
8		Customers are asking 'cloud like' services	3
9		Standardize deliverables	2
10		Customers need all kind of reports	3
11		More accurate data for invoicing is needed	3
12		Offering for specialist more demanding opportunities	2

13		Network configuration is difficult and take a lot of effort	2
14		Reliable is of items in production is missing	2

Notes were categorized to be able to get high level business requirements for the new system.

Security is important and it includes many different aspects such as security of the system itself and results it delivers. Security of the system itself includes terms as traceability, who did what and a multifactor authentication. Deliverables like new servers should be hardened same way every time. Servers should keep their security when they are in production.

Table 7 Security Category of Management Interviews

Notification/challenge	**Category**
Security can't be confirmed	Security
Reliable list of items in production is missing	Security, Quality

An agility category keeps inside quite wide range of topics in Table 8. Based on discussions the system should provide quick way to deploy services (servers), hide and simplify complexity of tasks and provide flexible reporting capabilities for the case company and its customer. All these comments are referring to 'cloud like' services offered through the portal which is one note or direct requirement discussed in these discussions.

Table 8 Agility Category of Management Interviews

Notification/challenge	**Category**
Lead time for new server too long	Agility
Customers are asking 'cloud like' self-services	Agility
Customers need all kind of reports	Agility
More accurate data for invoicing is needed	Agility
Network configurations is difficult	Agility

Quality or should one say quality improvements are divided to quality of deliverables and quality of work life generally.

Quality in deliverables refer in this context standardized delivery, no human mistakes included in deliverable.

Quality in HR (Human Resources) means that specialist will get new development paths e.g. automation specialist/architect to follow. On the other hand, simple and repeatable tasks should be automated, and specialist can concentrate higher level productivity tasks.

Table 9 Quality Category of Management Interviews

Notification/challenge	Category
Quality of deliverables varies	Quality
Standardize deliverables	Quality
Offering for specialist more demanding opportunities, new career paths	Quality/HR

Better cost efficiency is result of solving many topics discussed in quality or Agility category but couple of lines were referring directly in that direction.

Table 10 Cost Efficiency Category of Management Interviews

Notification/challenge	Category
Too much man work is required, can't hire so many people as needed	Cost efficiency, quality
Expenses are too high for server installations and management requires a lot of manpower	Cost efficiency

Last line written down from the discussions was line the topic “Acting according the strategy”. Strategy is being discussed in section 4.2 Company Documentation.

Notification/challenge	Category
Acting according the strategy	Strategy

Researcher started discussions and interviews with technical specialist (server related technologies) by asking them to fill in basic information of their technical area they are responsible. Specialist were also asked to think about their own area of tasks and work generally. What are 5 most irritating tasks you must do? What is working what is not? What would they automate on the area of their own expertise? What are they expecting from the system? Do they have requirements for the system?
Basic information was collected and based on that high-level integration picture, Figure 10, was produced.

It turned out that people were not prepared to sessions on and interviews were more like asking questions and the output was little thin. Mainly things what is not working and what kind of challenges people have, were recorded.
Server related technology people interview results can be found on Table 11.

Table 11 Server related technology interviews

Nmbr	Role	Notification/challenge	Responsible
1	Virtualization & Win specialist/Architect	Manual server provisioning specialist don't follow instructions and rules	1
2	Servers, component responsible	Company's high-level strategy is missing	1
3	OS, linux specialist	Dynamic memory enabled in virtual servers	1
4	Backup, component responsible	HyperV integrations tools and vmware tools not installed in servers	1
5	Monitoring, component responsible	People don't understand why things need to be done like they are instructed	1
6	Storage, component responsible	Server information is not correct in CMDB or missing totally	1
7		Too many virtual servers per LUN allocated	1
8		Win servers are not patched automatically	1
9		Wrong or general server templates are being used	1
10		HW server installation need to be automated as far as possible	2
11		Wrong virtual machine version used	2
12		Application level libraries are not updated	3
13		Linux servers are not patched properly	3
14		Too many linux servers are still created without templates	3
15		Too many linux variants under maintenance and new exceptions are still coming	3
16		Backup agent automated installation and system configuration	4
17		Servers are not configured in backup system	4
18		Automated operating procedure related incident	5
19		Automated SCOM monitoring agent installation and system configuration	5
20		Allocate disk for physical server according specs	6

Results of the interviews with CMDB/ITSM responsible and automation responsible are presented in Table 12. Problematic information from project point of view was that the CMDB is not used as it should be used.

Table 12 Interviews of CMDB/ITSM- and automation responsible

Nmbr	Role	Notification/challenge	Respon-sible
1	CMDB/ITSM specialist	CMDB Integration server installation for new network segments does not work	1
2	Automation responsible	There is no responsible for CMDB	1
3		CMDB project is not finished yet	1
4		APIs are not available in different tools	2
5		Automation done mainly for reporting purpose	2

Results of the interviews with network architect and data center network responsible are presented in Table 13. It appeared that the network environment is complex and there are quite many stakeholders managing the network environments.

Table 13 Network responsible interview

Nmbr	Role	Notification/challenge	Respon-sible
1	DC network responsible	e2e FW openings can be complicated, even three different organization and four FW instances	1
2	Network architect VY	Automation for FW opening is needed	1
		Configurations in switches and routers are in hands of three different organization. Difficult to find right ITSM queue so tickets are circulating around and are late always	2
		There is need to do QoS type of routing	2

Results of the interviews with security specialist are presented in Table 14. Requirements are from a security tool which content is based on chapter 5, Katakri (Defence, 2015, p. 9). These requirements were included in final requirements excluding the last requirement because it is pretty obvious that separate security contract will be signed and its requirements need to be followed.

Table 14 Security Requirements

Nmbr	Role	Notification/challenge
1	Security specialist	Roles and privileges of system user can be determined by using RBAC
2		Traffic to and from system components are crypted by algorithms accepted by Traficom. STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf
3		System support multifactor authentication
4		Management connections secured and crypted by algorithms accepted by Traficom. STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf
5		Data in system is secured and crypted by algorithms accepted by Traficom. STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf
6		System can be managed by using personal accounts without system accounts.
7		System will support audit trail -functionality which records all actions done in system
8		System can be scanned by antivirus software e.g. F-secure
9		System logs e.g. Audit trail -log can be written in a separate system log server at same time as in target server.
10		System supports strong server security keys and secure key distribution (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf)
11		System will be developed regularly, and security threads are reacted immediately.
12		In system can be configured log rotation interval.
13		System offered APIs are secured by unauthorized usage and usage of the APIs can be logged and reported easily.
14		System support Recover Point Objective (RPO) 24 h time
15		System support Recovery Time Objective (RTO) 48 h
16		Vendor engage responsibilities and obligations of security contract.

Researcher asked simple questions which helped each area representative to start thinking of their own area of expertise from automation point of view. What could be automated, what would be the quick wins to be able to achieve first, what are pain points in their daily routines, what they would like to do more quick and efficient way. Important aspects and things related to the area of technology.

Interviews also included short description of the used technology at a moment and fulfilling the Information system document.

A customer who were interviewed is running their own data center and server farm of couple of thousand servers. They were interested to utilize solution if possible. They did not have any extra requirements for the functional side. Because of case company strategy direct to consolidate services, and not to support customer in separate DC locations, decision was made that technological environment differences were not included in required support matrix.

4.2 Company Documentation

List of the relevant documents of the case company will be studied. Comments and notifications related to processes themselves will also be collected by the interviews explained in previous section.

Table 15 Document list of case company

	Document	**Description**
1	Server installations process	Describes phases of server installations process
2	VAKA Architecture descriptions	Technical description how VAKA service has been built.
3	Server deployment process	Describes phases and tasks of the server deployment.
4	Change Management	Change ticket phases and explanations
5	Company Strategy 2018	Describes the case company strategy for year 2018.

From the company strategy for year 2018, Figure 12 were extracted directives, Table 16, which steer the whole tool selection program.

Table 16 Strategy 2018 Impacts on Tool Selection

Nmbr	**Area**	**Notification/challenge**	**Category**
1	Goals	We produce **high-class, reliable** and **standardizes** IT services	Quality
2	Goals	We make **savings** by standardized processes and services	Cost effectiveness
3	Focus	**High-class** and **secure** activities	Quality
4	Focus	**Efficient** service production	Cost effectiveness in terms of money and time

5	Focus	Incident and **Change management** strengthening	Quality, Agile
6	Focus	**Security** of the services and preparing to cyber threats	Security
7	Efficient service production	**Cost effectiveness**	Cost effectiveness
8	Efficient service production	**Automating** actions and processes	Cost effectiveness, Quality
9	Efficient service production	**Self-service**	Customer wish, Cost effectiveness, agility

Findings were categorized on same way as management interviews findings were done. Category costs effectiveness and quality are mentioned quite often. These findings were used later for the decision whether Cloud- and automation is an answer for the problems or should there be something else to be done.

4.3 Vendor Workshop for Business Case

One possible vendor, later vendor in this section, was invited to investigate situation in the company and building a business case and Return of Investments (ROI) calculation for the program as there were a need to apply funding for the program from the Ministry of Finance. Vendor did few interviews how and what things are done now, how long it takes time and how much effort is needed at a moment. Scope of the discussions were servers, Mssql- and Oracle data base deploying and patching.
These interviews and discussions with vendor also gave information of the possibilities what could be available and doable by modern cloud- and automation tools.

From the Table 17 can be found interviews, topics and the participants who were interviewed by the vendor.

Table 17 Interviews by a Vendor

Topic	Role	Date	Time
Government	Team manager, Unit lead	16.2.2018	11:30-12:30
Operations	Production manager, Team manager	16.2.2018	15:00-16:00
Architecture, Windows OS	Virtualization architect	16.2.2018	12:45-14:00
Automation	Automation architect, server component resp.	20.2.2018	14:00-15:00
Linux OS	Specialist, Linux component resp.	19.2.2020	15:00-16:00
Databases	DB component resp.	15.2.2018	12:00-13:00
Networks	Specialist, architect	15.2.2018	10:00-11:00
Release Management	Virtualization architect	16.2.2018	12:45-14:00

Based on the information gathered from the interviews, costs and possible savings for next three years were calculated and project costs were included in calculations as well.

Calculations were done by using constraints shown in Table 18. Numbers are estimated figures, based on situation that there are about 1400 servers in own data centers, DBs to maintain 160 and yearly provisioned 30 DBs at a moment. All other parameters have been scaled up by multiplying existing figures by six. This means the figures we got out were theoretical.

There was an assumption used in patching use cases that whole process (pretesting, taking backup just before patching, running system down, patching, running system up, post testing) are automated as well as there is automated procedure to wake up on-call person who can make manual intervention in process if needed.

In new server and DB instances calculations, it was decided to allocate couple of hours to spend by instance by using the new tool, even technically speaking server deployment takes only couple of minutes in a cloud environment. Reason for that is that it is hard to see even in future that customer could do server deployment by their own or they could provide specifications good enough to the case company so that server administrators could make provisioning totally without questions or discussions with the customer. This is case now and automation does not help with the challenges in the planning phase.

Length of the implementation project was estimated about 6 months long and before that there would be 2 months project planning and preparing phase.

When calculating a cost reduction there was a realization factor taken into use to include 50% of all possible cost reduction in first year, 75% on second year and in 3rd year all possible savings. This is because of the learning curve of organization, which is industry standard with the complicated tool such like this one. It means in practice that organization can get all benefits out of the tool on the third year since it has been deployed and started to use in organization.

Table 18 Constants used in business case calculations

Total number	Unit
9000	Servers to maintain
600	New servers in year
1920	DB instances to maintain
180	New DB instances in year
6	months intallations project
2	months project planning
50	% realization factor 1st year
75	% realization factor 2nd year
100	% realization factor 3rd year

Calculation of **servers patching** costs reduction includes assumptions that all linux and windows servers will be under automated patching procedures. Automation enables patching and testing the whole services at once so there is no need for regular manual patching in future.

At a moment only Redhat linuxes and part of the windows servers are under automated patching. Rest of the servers are patched manually and only few times a year. That’s the reason why it was estimated that patching time, is a half an hour (average figure) per server in AS-IS situation and 0.1 hour per server by new a tool.

Total savings on first year have been calculated by subtracting forecast by new tool costs from current AS-IS costs and multiplying it by 50%. On second year, multiplier is 75% and on third year 100%.

Table 19 Total Servers Patching Savings

Yearly server patching savings €	Year 1	Year 2	Year 3	Total
Current AS-IS costs	2 160 000 €	2 160 000 €	2 160 000 €	6 480 000 €
Forecast by new tool costs	733 292 €	733 292 €	733 292 €	2 199 877 €
Realization factor	50 %	75 %	100 %	
Total savings	**713 354 €**	**1 070 031 €**	**1 426 708 €**	**3 210 092 €**

Table 20 Server Patching Savings, Hours

Yearly patching servers, savings, hours	Year 1	Year 2	Year 3	Total
Current AS-IS	54 000	54 000	54 000	162 000
Forecast by new tool	10 800	10 800	10 800	32 400
Realization factor	50 %	75 %	100 %	
Total savings hours	**21 600**	**32 400**	**43 200**	**97 200**

Total savings in three years are 3.2 million shown in Table 19. Savings are growing year by year as organization is learning to use system more efficiently. As we can see in Table 20 patching all those 9000 servers require a huge amount of work (32 fte) when it would be done properly. Now there are systems which are patched only few times in a year.

In **server provisioning** use case, there is an assumption that the case company will provision 390 windows and 290 linux servers in a year. In a AS-IS situation windows server deploying takes 10 hours and linux server 15 hours. Numbers are decreased to 2 and 4 hours per server with new tool.

Table 21 Servers Provisioning Savings in Euros

Yearly server provisioning savings, €	Year 1	Year 2	Year 3	Total
Current AS-IS	282 000 €	282 000 €	282 000 €	846 000 €
Forecast by new tool	64 800 €	64 800 €	64 800 €	194 400 €
Realization factor	50 %	75 %	100 %	
Total savings	**108 600 €**	**162 900 €**	**217 200 €**	**488 700 €**

Table 22 Server Provisioning Savings, Hours

Yearly server provisioning savings, hours	Year 1	Year 2	Year 3	Total
Current AS-IS	7 050	7 050	7 050	21 150
Forecast by new tool	1 620	1 620	1 620	4 860
Realization factor	50 %	75 %	100 %	
Total savings hours	**2 715**	**4 073**	**5 430**	**12 218**

Total expenses can be saved around half a million in three years shown in Table 21 and time could be save 12000 hours, around 5 FTEs shown in Table 22. Biggest benefits according the benchmarks and interviews can be achieved in delivery times. As one saw in our statistics from ITSM Table 43, one virtual server change request has been open 260 days in average between 2018 and 2019. Even the server ordering and implementation processes have been improved a lot, still in Q2/2019, a one change request has been open 68 calendar days in average.

If service request would be done in ITSM and it would be implemented by case company specialist, SLA would be days as today. Benefits by using automation, compared todays' situation, would be that, even corrections, in case of the wrong deployments, would be easier to do e.g. by new provisioning. A best option would be that provisioning is done through a portal by the customer itself and then SLA would be about an hour. This option still requires proper planning together with a customer and automation does not affect too much to that phase.

Data base (Oracle and Mssql) **patching costs** and savings have been presented below.

Total costs, Table 23 shows that by using old methods costs would be about 600 000 € and by utilizing new tool costs would be 39 000 k€. DB variants differ from each other only by number of instances. All other parameters are equal. AS-IS situation DB deployment takes 8 hours and 1 hour by utilizing new tool.

Table 23 Total DB Patching Costs

MSSQL and Oracle patching costs in year	**AS-IS**	**Estimated savings**	**Forecast by new tool**
Total costs of patching	614 400,00 €	576 000,00 €	38 400,00 €
Total number of hours of patching	15360	14400	960

Table 24 DB Patching Savings, €

Yearly DB patching savings	**Year 1**	**Year 2**	**Year 3**	**Total**
Current AS-IS	614 400 €	614 400 €	614 400 €	1 843 200 €
Forecast by new tool	38 400 €	38 400 €	38 400 €	115 200 €
Realization factor	50 %	75 %	100 %	
Total savings	**288 000 €**	**432 000 €**	**576 000 €**	**1 296 000 €**

Table 25 DB Patching Savings, hours

Yearly, DB patching savings, hours	Year 1	Year 2	Year 3	Total
Current AS-IS	15 360	15 360	15 360	46 080
Forecast by new tool	960	960	960	2 880
Realization factor	50 %	75 %	100 %	
Total savings hours	**7 200**	**10 800**	**14 400**	**32 400**

Total savings potential for three years are calculated in Table 24 and Table 25. They show that 1,3 million can be saved in money and in time savings could be 32 400 hours.

Data base (Oracle and Mssql) **instances provisioning** costs and savings are being presented below. In these calculations it was estimated strictly the time used in technical provisioning and was not calculated the time what is typically used for discussing details of the specs, asking questions and trying to find out all bits and pieces needed for provisioning.

Number of DB instances provisioned in a year is not that huge so total costs by using manual installations are roughly 20 k€ and by using automation roughly 2 k€. Parameters used in calculations are used time AS-IS which is 3 hours and by using new tool 0.3 hours.

Table 26 Combined DB Provisioning Costs

Mssql and Oracle provisioning costs in year	AS-IS	Estimated savings	Forecast by new tool
Total costs of patching	21 600,00 €	19 440,00 €	2 160,00 €
Total number of hours of patching	540	486	54

Table 27 DB Provisioning Savings, €

Yearly DB provisioning savings, €	Year 1	Year 2	Year 3	Total
Current AS-IS	21 600 €	21 600 €	21 600 €	64 800 €
Forecast by new tool	2 160 €	2 160 €	2 160 €	6 480 €
Realization factor	50 %	75 %	100 %	
Total savings	**9 720 €**	**14 580 €**	**19 440 €**	**43 740 €**

Table 28 DB Provisioning Savings, Hours

Yearly DB provisioning savings, hours	Year 1	Year 2	Year 3	Total
Current AS-IS	540	540	540	1 620
Forecast by new tool	54	54	54	162
Realization factor	50 %	75 %	100 %	
Total savings hours	**243**	**365**	**486**	**1 094**

Looking at savings for three years, Table 27 and Table 28 shows that one can find total savings about 43 k€ and 1000 hours by used time.

By decreasing all the costs related to deployment of the system in Table 29, training costs in Table 38, vendor related license- project- and support costs in Table 31 we can calculate that external costs are 88% of the total expenses excluding the training needs in next three years. This means that cash flow is strongly out of the company and part of the internal work should be increased if possible.

We will get the total business case related to new tool shown in Table 32.

We assumed that project length would be 6 months and there would be 2 months planning and preparing period before that. The figures below are calculated based on these assumptions.

Table 29 Project costs

Role	Nmb	€/h	€/fte	Number of days	Need %	Total
Project manager	1	48 €	346 €	114	75 %	29 590 €
Architect	1	45 €	324 €	122	100 %	39 453 €
Experienced specialist, automation	4	40 €	288 €	118	100 %	135 894 €
Specialist, automation	4	36 €	256 €	118	100 %	120 810 €
Member of the project steering group	3	50 €	361 €	152	5 %	8 219 €
Technology (server, backup, win, linux) specialist	4	40 €	288 €	152	10 %	17 535 €
Training project team	17	36 €	260 €	3	100 %	13 238 €
First introduction and training, maintenance teams	40	36 €	260 €	0,5	100 %	5 191 €
Total						**369 930 €**

Solutions consist of four different components which require different training for each one. Proposal included on-site training on first year and after that it was estimated that 3 person would be trained for each component and 2 person on third.

Table 30 Training costs

Training	**Year 1**	**Year 2**	**Year 3**	**Total**
Component 1	19 000 €	9 500 €	6 333 €	34 833 €
Component 2	19 000 €	9 500 €	6 333 €	34 833 €
Component 3	11 000 €	5 500 €	3 667 €	20 167 €
Component 4	11 000 €	5 500 €	3 667 €	20 167 €
Total	**60 000**	**30 000**	**20 000**	**110 000 €**

In Table 31 we can calculate that external costs are 88% of the total expenses excluding the training needs in next three years. This means that cash flow is strongly out of the company and part of the internal work should be increased if possible.

Table 31 Expenses

Expenses	Preliminary exp.	Year 1	Year 2	Year 3	Total
Licenses	1 090 000 €	0 €	0 €	0 €	1 090 000 €
Maintenance support		220 000 €	220 000 €	220 000 €	660 000 €
Project expenses, (vendor)	800 000 €				800 000 €
Project expenses, (case company)	369 930 €				369 930 €
Total	**1 890 000 €**	**220 000 €**	**220 000 €**	**220 000 €**	**2 919 930 €**

According the estimation, Table 32, saving potentials totally are 2,8 million euros in three years which makes approximately 0,93 million euros in a year starting from first year 0.26 million euros to the third year 1,6 million euros.

Table 32 Estimated savings

Total savings per year	**Year 1**	**Year 2**	**Year 3**	**Total**
Potential savings	1 293 540 €	1 940 310 €	2 587 080 €	5 820 930 €
Training	60 000 €	30 000 €	20 000 €	110 000 €
Project expenses	266 667 €	266 667 €	266 667 €	800 000 €
License costs	363 333 €	363 333 €	363 333 €	1 090 000 €
Maintenance support costs	220 000 €	220 000 €	220 000 €	660 000 €
Labour costs project	123 310 €	123 310 €	123 310 €	369 930 €
Total	**260 230 €**	**937 000 €**	**1 593 770 €**	**2 791 000 €**

During the process few findings were done related to requirements to be considered for the new tool.

1. Strong integrations between automation tool and vulnerability scanner would be beneficial. According the vulnerability scanner results automation tool could suggest right kind of correction and if needed, implement it in target environments without manual intervention.

2. Strong integrations into change process. Tool can initiate process based on vulnerability information and can continue process automatically according the given timetable based on the acceptance round by installing change, testing the system and finally closing the change ticket where all changes done are documented.

4.4 Server Order and Deployment Process

Servers are ordered and deployed by the process shown in Figure 9. Installation process starts planning phase (red dash line) by the customer and application vendor. They continue discussions with the case company service delivery manager and solution planning instance by creating a service request about the solution planning. In this phase customer responsible, architect or project manager collects final requirements and details together and customer creates a new service request for the server deployment. These discussions are quite often not so complete, which means details must be cleared out with the customer and application vendor in installation phase (red dash line) and it can cause then unnecessary delays. From delivery and automation point of view one is more interested about the installation phase in this study:

1. Service request has been done in ITSM system by the customer and it has been converted as a change request to be processed in production.

2. A change request is processed by production and on rough level next steps are done by the system services domain.

    a. Server will be created and joined in a domain

    b. Server will be added in the backup system

    c. Server will be added in the monitoring system

    d. Server will be added in the patching and virus protections systems

e. In a server will be installed all other required services such as data bases, application servers etc.

3. Customer will accept the delivery, all needed documents will be finalized and the solution will be transferred to production.

4.5 Change Process in ITSM

New server deployment will follow the change process which has been coded in ITSM. Process follows steps shown and explained in Table 33.

Table 33 Change Request Phases

Phase	Action	Responsible
Avoin	Change Request, (CR) created based on Service Request, (SR), from customer	Palvelintehdas
Uusi	Resource allocated for the CR.	Palvelintehdas
Suunnittelu	Technical planning	Palvelintehdas, customer, application vendor
CAB	Virtual server no use, Physical server Change Manager accept the change	Change manager
Valmistelu	Possible corrections and details before deployment	Palvelintehdas
GCAB/Hyväksyntä	Global Cab, not used with server installations CRs	Not used
Toteutus	Server deployment	Multiple responsible
Arviointi	Not used	Customer, normally not needed
PIR	Not used	Change manager with palvelintehdas
Suljettu	Closed	Change manager

Findings what were discovered during the process and suggested actions related to process are described below in Table 34.

Table 34 Findings and Suggestions

Findings	Action
1.) In which phase ticket will be closed?	Clear out process steps. Make sure process will be monitored and corrective action will be done when necessary.
2.) Who is responsible and what?	Make sure people understand own responsibilities. Monitor process accordingly.
3.) There are too many hands off during the ticket lifetime.	Streamline process by decreasing people/teams who participate in process and responsibility moving between. E.g. person who create virtual machine will also install backup, monitoring agents and add server in patching process.
4.) Inaccurate specs lead unnecessary discussion rounds during the installation phase	Develop further order template to be used and make sure customer understand template and all details in there. Require all details available before start work with service request.

4.6 Benchmark of Virtual Server Installations CRs from ITSM

Table 53 shows that the whole server installations process has been in serious problems. Between February 2018 and December 2019 virtual server installation change tickets were opened 183 pieces. These were closed approximately 260 days after they were opened. In February 2018 started one dedicated coordinator to manage and develop this process. As a result of the development work a closing time of per ticket were reduced approximately to 66 days during second half of 2019.

Results of virtual server installations were not acceptable even it is a known fact that deliverables were delivered to customer faster than the figures based on the closing times of tickets indicates. This can’t be proven by the data because the ITSM system can’t report the data out how long each ticket was in each phase. This is related to existing licenses of the reporting tool integrated in ITSM. Researcher started working as service delivery manager for the VAKA services in beginning of 2019 and autumn 2019 were closed about 50 virtual server installations tickets, in one event, which were waiting the closing at “Arviointi” phase. This indicates strongly that problem was in process itself and how it was implemented and followed.

5 RFI

In this section RFI building and answers are explained. RFI was built against the requirements defined so far. One can roughly estimate that 90% of the final functional requirements were already known and understood but there was not any prioritization in place at that time, autumn 2019. Because the case company wanted to get as many serious and different answers as possible for the request, the RFI document and requirements were written on quite high level almost nothing limiting out in advance.

5.1 RFI Content

RFI included following sections:

- Backgrounds of the purchase
- The goals and objectives of RFI
- AS-IS description
- Requirements of the technology stack which must be supported by the solution
- Questions for the vendors
- Timetable

Goal of the RFI was described and there were high level expectations written out for the solution. *The goal of case company is to purchase solution which enable possibility to offer Data center- and hybrid cloud services flexible way for administrations of the government. Features such as cost efficiency, agility, capability to analyze environment, improvement of security and quality are being searched e.g. by:*

Cloud service: Case company customers can manage their own IT environment through the self-service portal. Services provisioned through the portal will be built up automatically in data centers of case company without manual intervention. IaaS and PaaS services can be enabled via portal.

DC automation supports used technologies in the case company DCs. Tool offers capability for specialist (e.g server- DB management,) to automate daily activities and reuse the results. Tool offers capability to analyze environment quickly e.g. (find servers where certain driver version is used in among of thousands of servers)

Non-Functional requirements were mentioned such as system enables secured connections in and out of the system. Data in transit and data in rest are also secured. The Traficom has approved list of accepted ways to secure connections and data. System offers APIs to be used

DevOps- or Infra as Code use cases. There is support for “Audit Trail” -type of logging as part of the system and system follow the “loose couple” principle related to system it manages.

AS-IS section described relevant technology stack in place which should be supported by the tool. The technology description included a brand and a model list covering relevant technologies starting from network switches and ending to Security Information and Event Management (SIEM) solution and containers. A logical level picture of the integrations of the new tool were included in RFI too. High level network topology was presented which emphasized the fact that support for configuration of network devices is a must.

In question section were asked several types of questions from the vendor. There are 55 questions categorized according a vendor and product, a vendor(s) role(s) and responsibilities in service chain, how services are produced and from where, how would you build described solutions, support for public clouds, description of control and management interfaces, description of management tools and reporting, a system performance requirements and scaling possibilities, security, description of cost component, functionality and references about the same kind of solutions delivered.

By asking these kinds of questions the case company tried to confirm that company and its product(s) are widely used, vendor(s) is experienced and trust worth and capable of delivering tool and related services.

5.2 RFI Answers

The case company got 18 answer for the RFI. In the first place there were limited out the consulting type of answers to continue discussions without a specified deliverable product. Solutions based on public clouds were also scoped out because the requirement was solution on premises. There were 6 vendors limited out in first round.

On second round, solutions based on the own dedicated hardware stack were limited out. These solutions required to purchase whole specified infrastructure or part of it as part of the solution. The case company was not willing to invest anything more than software-based solutions which can be run on default Intel hardware. On this round 5 candidates were dropped off.

On third round couple of vendors were dropped out based on a limited functionality or not complete answers which did not give information required.

After these three rounds there were five candidates left to be asked more detailed presentations of their solutions.

5.3 Detailed questionnaire and presentations

Presentations were held according the schedule shown in Table 35. For the vendors were sent questionnaire as a list of requirements to answer whether their solutions meet the requirement or not. Vendors had a chance to comment to each requirement, e.g. does it make sense or not.

For each vendor were scheduled three hours to give presentation, give comments and get answers for the possible questions from the case company.

Table 35 Vendor Presentations Schedule

Nmbr	Vendor	Date	Time
1	Vendor	5.12.2018	09:00-12:00
2	Vendor	17.12.2018	13:00-16:00
3	Vendor	9.1.2019	12:00-15:00
4	Vendor	14.1.2019	12:00-15:00
5	Vendor	16.1.2019	08:30-11:30

Topics of the presentation were prepared by the case company. On server automation following side were asked to present.

1. Find old driver from the group of 10 windows servers and update the driver.
2. Compare server image against the reference image, report differences and fix them back.
3. Startup a closed service in windows server.
4. Compare the fire wall rules against reference rule. Report the differences and correct them.
5. In linux server recognize old apache version and correct it.
6. Does user belong in wheel -group in linux server? Remove user from there.
7. Does linux server solve names against DNS service or against host file?

The automation requirements list, asked to be commented, is shown in Table 44. Related to cloud requirements there was asked to present use cases listed below.

1. Deploy a sql -server in AWS or Azure and open firewall between own data center and server cloud service. Test the connection that it is working.
2. Create new VLAN, deploy a server in there and join it to domain. Move server from one domain to another and enable remote connection on server from certain address.

3. Report costs and consumed technical details of the tenant before new server provisioning and after the provisioning has been done.

The list of the cloud requirements, asked to be commented, is shown in Table 45.

6 Final Requirements Building

This section presents requirements and explains analogy how requirements were derived from findings and interviews on the study. First there are answered questions “Is hybrid cloud- and automation system, the solution for the existing problems?”. An analyze below was done against findings from the management interviews and the strategy study. Then architecture decisions about the tooling type is presented. Justifications of the requirements are in last part of the section.

6.1 Solution

Business requirements derived from the management interviews Table 6 are security, agility, cost efficiency, quality and strategy. The solution building based on the requirements is shown in Table 36. Column “Response from study/Comments” is reference or answer how automation- and cloud solution responses the requirement or there is explanation how this requirement has been considered by the solution.

Table 36 Solution building by Business Requirements

Nmbr	Category	Notification/Challenge	Response from study/Comments
1	Agility	Lead time for new server too long	Table 22 Server Provisioning Savings, Hours Automation saves time and money according the estimation.
7	Agility	Customers are asking 'cloud like' self-services	Directing towards clouds and self service
9	Agility	Customers need all kind of reports	Directing towards clouds and self-service. Customers can extract such reports as they want.
10	Agility	More accurate data for invoicing is needed	Directing towards cloud and self-service where IT-services are consumed according the as pay per use -principle.
12	Agility	Network configurations is difficult	Automation helps to cover complexity. Solve technical challenge once and repeat solution by automating it.
5	Cost efficiency	Expenses are too high for server installations and management requires a lot of manpower	Table 21 Servers Provisioning Savings in Euros and Table 20 Server Patching Savings, Hours
3	Cost efficiency, quality	Too much man work is required, can't hire so many people as needed	Table 22 Server Provisioning Savings, Hours Table 28 DB Provisioning Savings, Hours

2	Quality	Quality of deliverables varies	Quality will be improved when deliverables are standardized and wanted configuration can be confirmed by preventing e.g. configuration drifting.
8	Quality	Standardize deliverables	Quality will be improved when deliverables are standardized and wanted configuration can be confirmed by preventing e.g. configuration drifting.
11	Quality/HR	Offering for specialist more demanding opportunities	By automating tasks which are repeated continuously new job opportunities are created.
4	Security	Security can't be confirmed	Status of the service can be confirmed e.g. by preventing configuration drifting. Status can be verified against snapshot or specification.
13	Security, Quality	Reliable list of items in production is missing	The requirement can be responded by existing CMDB tool which can make inventory-
6	Strategy	Acting according the strategy	4.2 Company Documentation

Agility type of requirements can be answered easily by cloud- and automation tools. As shown in Table 36 they make existing processes quicker, offer portal for customers and via portal there are reporting possibilities available as much as everything is based on strong network automation.

As one has seen cost efficiency requirements can be answered by the cloud- and automation tool based on what was calculated in the business case. Estimated savings, Table 32, based on four different use-cases were 0,9 million euros per year.

Quality and security categories will be responded as automation requires strong definitions what are delivered, and tooling gives possibilities to follow configuration and correct changes.

Based on the strategy for year 2018 we derived Table 37, which can be used to justify our decision to find out more automation and self-service for the environment.

Table 37 Solution Building Based on Strategy 2018

Nmbr	Category	Notification/challenge	Response from study/Comments
1	Quality	We produce **high-class, reliable** and **standardizes** IT services	Quality will be improved when deliverables are standardized, reliability will be improved when configuration can be confirmed by preventing configuration drifting.
2	Cost effectiveness	We make **savings** by **standardized** processes and services	According the business-case Table 32 Estimated savings

3	Quality	**High-class** and **secure** activities	Quality will be improved when deliverables are standardized. Security of the service can be confirmed e.g. by preventing configuration drifting. Status can be verified against snapshot or specification.
4	Cost effectiveness in terms of money and time	**Efficient** service production	Table 32 Estimated savings Table 22 Server Provisioning Savings, Hours Table 28 DB Provisioning Savings, Hours
5	Quality, Agile	Incident and **Change management** strengthening	Cloud and automation integration to ITSM and change process will improve quality of it. Figure 10 Hybrid Cloud and Automation System Integrations
6	Security	**Security** of the services and preparing to Cyber threats	Security aspects will improve from many points of view such as standardization, preventing configuration drifting, integration with vulnerability scanners, better picture of the environments and dynamic analyzing capabilities as an example.
7	Cost effectiveness	**Cost effectiveness**	Table 32 Estimated savings Table 22 Server Provisioning Savings, Hours Table 28 DB Provisioning Savings, Hours
8	Cost effectiveness, Quality	**Automation** of actions and processes	3.2 Server Automation, various lessons learned
9	Customer wish, Cost effectiveness, agility	**Self-service**	Cloud like user interface

Based on the cloud- and automation capabilities there was no doubt that the case company should consider new tooling set and continue to start defining the requirements for cloud- and automation solution.

6.2 High level architecture decisions

Should there be a solution for a cloud or an automation system or both combined? What else should be considered? Based on the investigations in chapter 3.2 Server Automation and described situation in case company, Figure 10, it was clear there is a need for SA -tool and the solution can be full filled with existing CCA-tool(s) like Ansible and tailored scripts.

From technical point of view, it appeared in many discussions that both systems combined together should come from one vendor because the cloud system needs strong automation tooling and integration together two systems from different vendors might be expensive. Maintenance and future development would require a lot of costs and effort.

When starting discussion with the procurement, a surprise was that these two sections should be managed separately or there should be included possibility to offer only one solution because of the principal mentioned in Government Procurements, each contender should be treated equally. In order to avoid unwanted delays in the end of the process in form of complains, this principle was interpreted by layers the way that because the value in year (more than 500 000€, EU level procurement) and nature (technically possible) of the solution these two sections are treated as a separate solutions.

Based on the fact of the customers of the case company, which are governmental bureaus, they can't rely on only public cloud-based solutions, so hybrid cloud was stated as a target solution to purchase. This decision was also supported by the strategy where customer dedicated data center solutions are being transformed in centralized data center and in public clouds whenever it is possible. Hybrid cloud would give a possibility to shift services between private cloud in company data center to public cloud if applicable.

6.3 Hybrid Cloud Requirements

Requirements for the Hybrid Cloud solution can be seen in Table 45. Requirements were not finalized and prioritized because the company made decision to purchase hybrid cloud even though the requirement definition project was not finished yet. In this work, listed requirements are not dealt with more detailed level.

6.4 Datacenter Automation Requirements

Requirements have been divided in five categories which are functional requirements, nonfunctional requirements which includes maintainability, usability and instructions & descriptions and finally security requirements.

Requirements are divided in two different classes inside each category mentioned above. These categories are V1 and V2. 'V' is referring to Finnish word 'Vaatimus' e.g. requirement. V1 is compulsory requirement and tool must meet the requirement. V2 is optional requirement. It was meant that meeting each requirement in V2 category gives a certain amount of points and based on these points final selection between tools would have been done. This final stage to give value for each V2 requirements were not implemented because the suspension of the automation requirements definition project also after half a year suspension decision of the cloud part of the project.

Functional requirements and justification are presented in Table 38.

Requirement 1.3 comes directly from the discussion with specialist and collected information of the existing systems. General rule of the required support matrix would be the same as vendors are supporting. Case company can't promise support if there is no vendor support on background.

Requirement 1.5 is related to quite many topics discusses in this study. Keep originally planned hardening in place, nothing else is allowed if not first created new reference. This requirement is part of the answers for security category requirements derived from Table 6.

Requirement 1.10 on general architecture perspective is needed in this context because there is no need or purpose to set up 24/7 support requirements for the system. Target systems must be fully operational even the 'management' or 'deployment' infrastructure is down.

Table 38 Automation, Functional requirements

ID	Class	Requirement	Source or Justification
1.1	V1	There is programmable interface (API) in the system to be used as part of "infrastructure as code"- or "devops" framework.	3.2 Server Automation, last line One of the biggest barriers in data center automation is the lack of APIs. Agility, Agile development
1.2	V1	System can integrate to other systems (e.g. ITSM, CMDB) via APIs	Figure 9 ITSM phases of the normal change, ITIL (Axelos, 2019)
1.3	V1	System can manage, deploy and patch next OS: Win 2008R2, Win 2016, Win 2012R2 RHEL 6, RHEL 7; SuSe 11, SuSe 12; Ubuntu 16, Ubuntu 18; CentOS 6, CentOS 7	Table 11 Server related technology interviews Table 34 Findings and Suggestions 2.) and 3.) Server order- and deployment process investigations findings
1.4	V1	System can automate and manage most common tasks related F-secure antivirus system	Tool used by Case company Table 14 Security Requirements ID 8
1.5	V1	System can report and update target system back to wanted state (e.g. prevent configuration drift) based on system image or separate configuration file.	Table 6 Management discussion results
1.6	V1	System provided API usage can be authenticated, logged actions and reported.	Table 14 Security Requirements ID 7
1.7	V1	Infrastructure changes will be recorded in ITSM and CMDB accordingly	Figure 9 ITSM phases of the normal change, ITIL (Axelos, 2019)

1.8	V1	System can be integrated to HyperV 2016 and Vmware 6.5	Tool used by Case company
1.9	V1	System support public cloud server management in Azure and AWS	Services used by Case company
1.10	V1	System creates "loosely coupled" -type relationship to target systems. Which means in this context target systems are fully functional if automation is dead.	See separate explanations
1.11	V1	System can automate and manage most common tasks related to backup and storage systems: NetApp FAS 8020 NatApp FAS 8200 tapelibrary Quantum scalar i500	Technology used by case company
1.12	V1	System can automate and manage most common tasks related to storage systems: NetApp FAS 8080 ja NetApp AFF 700	Technology used by case company
1.13	V1	System can automate and manage most common tasks related to monitoring systems: SCOM 2016 and 2019	Technology used by case company
1.14	V1	System performance will scale up without extra investments between 1 -15 000 servers	Estimated maximum number of servers
1.15	V1	System has multi domain support for the managed servers and servers outside of domain can be managed also	Customer servers are using their own domains, so multi domain support is needed.
1.16	V1	Authorization for the different roles comes from AD.	Authorization data maintained in one place only.
1.17	V1	System will be installed on top of Windows or Linux operating system and it does not need any vendor specific HW acquisition	HW investment were not in scope by the case company at that moment
1.18	V1	System can automate updates and patching Win and Linux (Redhat) Oss without any extra tools like SCCM or WSUS	Windows patching capabilities are limited so this system must be able to manage patching
1.19	V1	System can have own orchestrator, or it must be able to use Microsoft orchestrator.	MS orchestrator is used at a moment
1.20	V2	System understand clustering, allocation ratio and other needed parameters when loading servers to HyperV and vSphere.	Load balancing capabilities is needed
1.21	V2	System can update drivers, firmware and BIOS	HW maintenance support is needed. Takes a lot of manual work to be succeeded
1.22	V2	Automation capabilities to MSSQL, MariaDB 5-, MySQL 5-, Oracle 11-12, Postgre 9.2 - 10	Technology used by case company or customers of case company
1.23	V2	Automation capabilities to middleware tools: Jboss, apache, IIS, Tomcat, Nginx, WebSphere, Weblogic	Technology used by case company or customers of case company
1.24	V2	Physical server installation and configuration HPE, DELL, IBM, Fujitsu	Technology used by case company or customers of case company
1.25	V2	Support for Docker and Kubernetes containers	Technology used by case company or customers of case company
1.26	V2	Support for Oracle VMs	Technology used by case company or customers of case company

1.27	V2	System can invent objects from network	Security feature for quick response if something unauthorized appears in network.
1.28	V2	Data can be imported and exported to/from system in some common format like JSON, XML or CSV	Part of the reporting facilities
1.29	V2	Support for Patrol, PRTG and Tivoli monitorin system	Technology used by case company or customers of case company
1.30	V2	Monitoring capability, system can analyze incidents and act accordingly.	Part of the incident management discussions, automated actions after the incident created by the monitoring tool
1.31	V2	System can interact with Nessus Scanning system by acting according the Nessus report	Technology used by case company or customers of case company.
1.32	V2	Visibility to Nessus findings can be limited according a client or technology.	Technology used by case company or customers of case company. Security requirement.
1.34	V2	System can correct flaws according the Nessus report	Technology used by case company or customers of case company.
1.36	V2	System can be run on top of another database than Oracle	Oracle licensing costs are high

Table 39 Automation, Security Requirements

ID	Class	Requirement	Source or Justification
4.1	V1	Roles and privileges of system user can be determined by using RBAC	Table 14 Security Requirements
4.2	V1	Traffic to and from system components are crypted by algorithms accepted by Traficom. STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf	Table 14 Security Requirements
4.3	V1	System support multifactor authentication	Table 14 Security Requirements
4.4	V1	Management connections secured and crypted by algorithms accepted by Traficom. STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf	Table 14 Security Requirements
4.5	V1	Data in system is secured and crypted by algorithms accepted by Traficom. STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf	Table 14 Security Requirements
4.6	V1	System can be managed by using personal accounts without system accounts.	Table 14 Security Requirements
4.7	V1	System will support audit trail -functionality which records all actions done in system	Table 14 Security Requirements
4.8	V1	System can be scanned by antivirus software e.g. F-secure	Table 14 Security Requirements

4.9	V1	System logs e.g. Audit trail -log can be written in a separate system log server at same time as in target server.	Table 14 Security Requirements
4.10	V1	System supports strong server security keys and secure key distribution (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf)	Table 14 Security Requirements
4.11	V1	System will be developed regularly, and security threads are reacted immediately.	Table 14 Security Requirements
4.12	V1	In system can be configured log rotation interval.	Table 14 Security Requirements
4.13	V1	System offered API'a are secured by unauthorized usage and usage of the APIs can be logged and reported easily.	Table 14 Security Requirements
4.14	V1	System support Recover Point Objective (RPO) 24 h time	Table 14 Security Requirements
4.15	V1	System support Recovery Time Objective (RTO) 48 h	Table 14 Security Requirements
4.16	V1	Vendor engage responsibilities and obligations of security contract.	Table 14 Security Requirements

Table 40 Automation, Maintainability Requirements

ID	Class	Requirement	Source or Justification
2.1	V1	System capacity requirements can be scaled according the needs.	Number of managed servers can vary up and down in future
2.2	V1	System can be restored from backup.	
2.3	V1	System can be updated without configuration losses.	Major version updates tend to lead reconfiguring system
2.4	V1	Support SLA is "Next Business Day"	No need to 24/7 in beginning
2.5	V1	Instructions must be updated and available	
2.6	V1	Number of licenses is scalable up and down.	Depending on the licensing model
2.7	V1	A vendor needs to develop and support system during contract period.	Make sure you don’t buy system which will be terminated in near future
2.8	V2	For system can be arrange 24/7 support if needed.	In case of system will be used as extension of monitoring system
2.9	V2	One older version of system must be available and supported.	In case latest version does not work

Table 41 Automation, Usability Requirements

ID	Class	Requirement	Source or Justification
3.1	V1	System has a 'multisite support feature'	The case company has multiple data centers to manage
3.2	V1	Reports can be tailored according customer needs	There are various of different needs for the reporting. Dynamic reporting engine is needed.

3.3	V1	User interfaces are in Finnish or English.	These two languages accepted only
3.5	V2	Fluent user experienced and generally accepted response times are expected.	General requirements from the case company
3.6	V2	System is intuitive and easy to use.	General requirements from the case company
3.7	V2	System supports needed characters (Finnish, English)	These two languages accepted only
3.8	V2	User Interfaces can be tailored according the case company's needs.	Flexibility is a valued feature

Table 42 Automation, Requirements for Instructions and Descriptions

ID	Class	Requirement	Source or Justification
5.1	V1	User Instructions in Finnish or English	These two languages accepted only
5.2	V1	Support is available in Finnish or English	These two languages accepted only
5.3	V1	Vendor specialists must be senior level specialist who deliver services.	General requirements from the case company
5.4	V2	Vendor can arrange training for the solution.	Possible benefits in training costs

As one can see there are many requirements which comes by the case company polices and are mandatory requirements.

7 Conclusion and Discussion

This section summarizes what was the target of the theses and a justification for it. It explains what the core results and benefits for the company were. Validity and reliability view is discussed as well as possible future steps for the project.

The major goal of this study was to define requirements for the solution which can solve the challenges in DC delivery and modernize the delivery- and management model. It was quite clear from the beginning that described challenges by the management would be solved by automating core processes, start developing an automation for maintenance purposes and set up a cloud environment where customer could manage their own environments through a web portal. Challenges described by the management were used to define high-level business requirements for the solution. Four separate categories of the business requirements were defined as security, agility, quality and cost efficiency. The strategy did not give any extra viewpoints to the topic but strengthened the management view.

The study found multiple concrete steps how security could be improved by adding the automation and cloud services on top of the DC-services. Improvements determined in other categories improve also security category e.g. prevention of configuration drifting, standardization, integrations to other systems such as CMDB, ITSM and vulnerability scanners. A principal, as less manual intervention as possible when servers are managed or deployed, decreases the possibility of a human mistake which improves security.

From agility point of view one found out that existing processes don’t not work properly. The server installation process is slow and work effort consuming. IT should be managed and develop continuously. Even improvements related to server provisioning process were done during the requirements definition project, a benchmark of the server installation process was bad. Changing the operational mode from manual implementation to fully automated provisioning process, giving possibility to customers to manage their own environments through a portal and adding an automation possibility to maintenance side would create a huge difference and improvement from agility point of view.

From quality point of view one accepted the fact and it was proven by the literature investigations that the more people and manual tasks are included in the process, more mistakes and flaws will be found and quality decreases. From this point of view strong automation focus and increasing a self-service would be a solution which improves a quality of deliverables.

Investigations of cost efficiency with one of the possible vendor gave an eye open view of the inefficiency of the manual work around the server deployment and maintenance. When the number of servers is increasing something must be done to the way how the case company is delivering the services. Traditional way is not an answer anymore.

7.1 Validity and Reliability

Validity of a case study research can be measured by investigating the answer to the question "Did the investigation give an answer to the original research question?". In this case the question was to define requirements for cloud and automation system. From this point of view answer is yes but in this case one should rather qualify the content of requirements and answer to the question "Are defined requirements valid for the case company and were all stakeholders able to contribute the process and requirements?"

As shown in Figure 5, there are listed 6 different stakeholder groups who had an opportunity to influence on the requirements. Those groups are 'laws and regulations', 'management', 'end users', 'it security', 'cooperation's partners and customers' and 'vendors, consultants and industry'.

Laws and decrees part was covered when procurement was involved in process and regulations were considered even from EU-level point of view concerning the tender process itself. Management interviews were a starting point of the process and business requirements were derived from these discussions. End users -group was represented by all technical interviewees. Security point of view was strongly included in the process and requirements by the representative form security unit. Partners, vendors and industry were included in the process in a business case calculation phase and in the end when the RFI was published. A customer view was represented by the product manager and one customer interview of the case company was done, though the results were thin. From this point of view the coverage of the study was extensive and the validity can be considered good.

Reliability can be investigated by setting a question "Would somebody else got the same results by redoing the research?" and "Would the results be the same, if same research would be done in different point of time?"

Results would be pretty much the same if somebody else would do the research by using the same data sources and interviewing the same people. The formulation of the requirements would differ, but e.g. same business level requirements would be defined. More detailed requirements might slightly differ because the interviews of technical specialist were difficult and researcher's previous experience about topic helped him to lead discussions and interviews in relevant direction.

In time wise results would differ because when experiences about cloud and automation topic are gained the viewpoints and opinions are also changing. From technical point of view technology is evolving all the time. Features which seems to be important now would not be that important after couple of years because the same task might be possible to take care some other way or by using some other system.

Reliability of the study could be improved by planning interviews in more detailed level. Now management interviews were more discussions than interviews. Somehow one should improve the results of the specialist interviews. As mentioned earlier specialists didn’t have time or interest to prepare questionnaire or even think about the topic before the interview.

7.2 Next steps

For the case company next steps would be to arrange a POC validation in real environment with the two most promising solutions. The POC would confirm that the solution is working in the case company environment as it has been described. Based on the POC experiences and points collected from V2 (optional) requirements valuation, the best solution for the case company can be announced.

One should initiate a process development project in the case company which would have impacts on the all processes related to topic. It covers processes starting from a server order process and ending up to the all internal DC processes, which need to adjust to follow the procedures of the new system. It is good to understand also that connection to public cloud would create a new channel to consume and procure the IT services which need to be considered widely over the organization. Employees of the case company need to be trained to use the new system and to act according the new processes. From the case company point of view this means a massive training program where on is talking about hundreds of people who should get different levels of training for the new system.

8 References

Axelos, 2019. *what is ITIL.* [Online] Available at: https://www.axelos.com/best-practice-solutions/itil/what-is-itil [Accessed 2020].

Defence, M. o., 2015. *Katakri - Tietoturvallisuuden auditointityökalu viranomaisille.* [Online] Available at: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf [Accessed 21 April 2020].

Delory, P., 2016. *Comparing Three Approaches to Modern Server Automation, From Scripting to DevOps Tools.* [Online] Available at: https://www.gartner.com/document/3494618?ref=lib [Accessed 22 April 2018].

Delory, P., 2017. *Four Questions to Ask When Getting Started With Server Automation.* [Online] Available at: https://www.gartner.com/document/3688617?ref=lib [Accessed 22 April 2018].

Government, F., 2011. *Valmiuslaki.* [Online] Available at: https://www.finlex.fi/fi/laki/alkup/2011/20111552 [Accessed 24 April 2020].

Goyal, S., 2014. Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. *International Journal of Computer Network and Information Security,* Volume 6, pp. 20-29.

jhs 172, J., 2009. *JHS-Suositukset - JHS 172.* [Online] Available at: http://jhs-suositukset.netum.fi/web/guest/jhs/recommendations/172 [Accessed 2018].

Juhta, 2006. *JHS.* [Online] Available at: http://www.jhs-suositukset.fi/web/guest/jhs/organization/section/jhs_strategy#1 [Accessed 30 December 2019].

Juhta, 2009. *JHS173, ICT-palvelujen kehittäminen: Vaatimusmäärittely.* [Online] Available at: http://docs.jhs-suositukset.fi/jhs-suositukset/JHS173/JHS173.pdf [Accessed 29 Decembe 2019].

Juhta, 2017. *JHS198 Kokonaisarkkitehtuurin peruskuvaukset.* [Online] Available at: http://docs.jhs-suositukset.fi/jhs-suositukset/JHS198/JHS198.pdf [Accessed 29 December 2019].

Microsoft, 2020. *hat is a hybrid cloud?.* [Online] Available at: https://azure.microsoft.com/en-us/overview/what-is-hybrid-cloud-computing/ [Accessed 14 April 2020].

Microsoft, 2020. *What is a private cloud?.* [Online] Available at: https://azure.microsoft.com/en-us/overview/what-is-a-private-cloud/ [Accessed 14 March 2020].

Microsoft, 2020. *What is a public cloud?.* [Online] Available at: https://azure.microsoft.com/en-us/overview/what-is-a-public-cloud/ [Accessed 13 April 2020].

Union, E., 2016. *Document 32016R0679.* [Online] Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 24 April 2020].

Waite, A., 2020. *The Many Faces of Private Cloud.* [Online] Available at: https://www.gartner.com/document/3979549?ref=lib [Accessed 22 January 2020].

Valtiovarainministeriö, 2017. *Valtion Hankintakäsikirja 2017.* [Online] Available at: https://vm.fi/documents/10623/4040240/Valtion+hankintak%C3%A4sikirja+2017/868b80fa-c2de-4328-ae93-36b17968f780/Valtion+hankintak%C3%A4sikirja+2017.pdf?version=1.0
[Accessed 2018].

Yin, R. K., 2018. *Case study research and applications.* 6 ed. Los Angeles: SAGE Publications, Inc.

Appendix 1. High Level Process of Server Installation

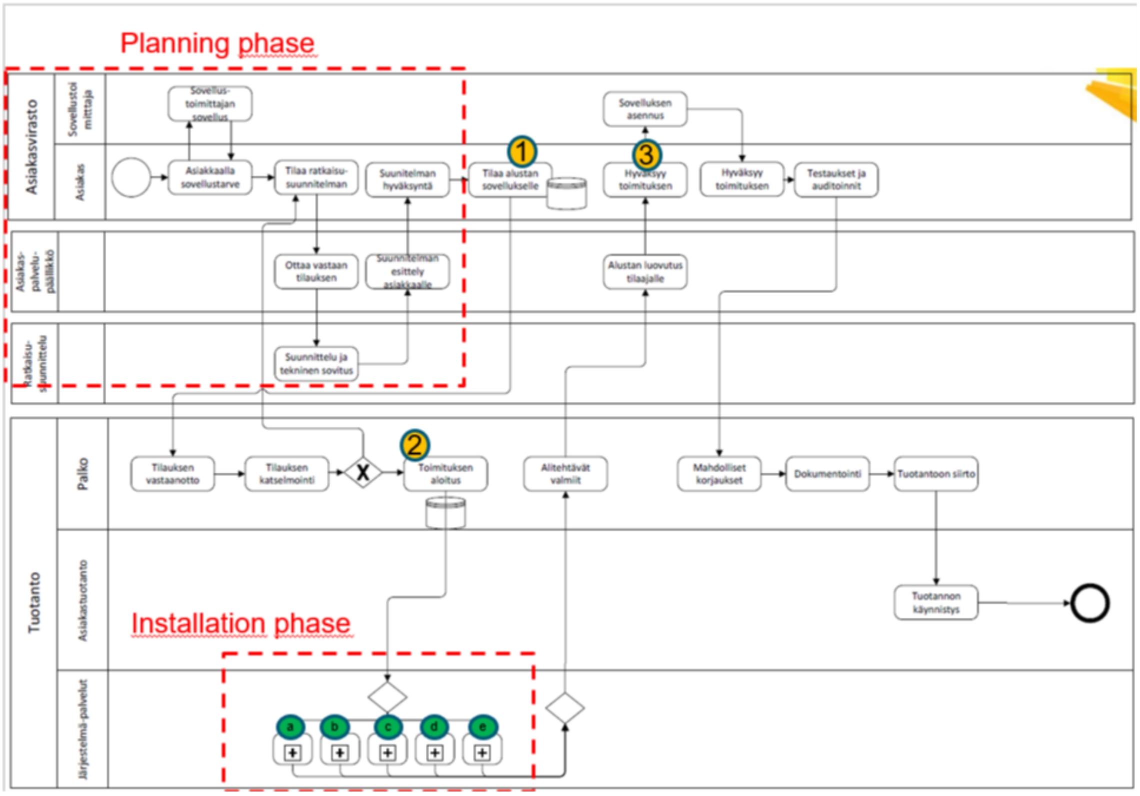


Figure 8 High Level Server Installation Process

Appendix 2. Virtual Server Installations

Table 43 Virtual Server Installations Benchmark

Item	Open	Closed	Days	
Average in Q2/2019			**68**	**days**
Average			**260**	**days**
Number of tickets			**183**	**tickets**
CHG0031451	1.2.2018	3.9.2018	214	
CHG0031458	6.2.2018	20.6.2018	134	
CHG0031465	9.2.2018	3.12.2019	662	
CHG0031467	12.2.2018	10.10.2019	605	
CHG0031483	16.2.2018	9.10.2019	600	
CHG0031514	28.2.2018	23.9.2019	572	
CHG0031517	2.3.2018	2.12.2019	640	
CHG0031518	2.3.2018	23.9.2019	570	
CHG0031557	16.3.2018	3.12.2019	627	
CHG0031563	20.3.2018	23.9.2019	552	
CHG0031591	3.4.2018	2.12.2019	608	
CHG0031597	6.4.2018	3.7.2019	453	
CHG0031609	11.4.2018	10.10.2019	547	
CHG0031642	16.4.2018	14.1.2020	638	
CHG0031648	17.4.2018	23.9.2019	524	
CHG0031661	18.4.2018	2.12.2019	593	
CHG0031673	23.4.2018	23.9.2019	518	
CHG0031692	2.5.2018	9.10.2019	525	
CHG0031704	3.5.2018	2.12.2019	578	
CHG0031705	4.5.2018	2.12.2019	577	
CHG0031739	16.5.2018	20.12.2019	583	
CHG0031743	17.5.2018	23.9.2019	494	
CHG0031772	25.5.2018	9.10.2019	502	
CHG0031791	30.5.2018	11.2.2019	257	
CHG0031792	30.5.2018	23.9.2019	481	
CHG0031816	5.6.2018	2.12.2019	545	
CHG0031830	7.6.2018	23.9.2019	473	
CHG0031893	20.6.2018	23.9.2019	460	
CHG0031926	5.7.2018	23.9.2019	445	
CHG0031930	9.7.2018	23.9.2019	441	
CHG0031943	12.7.2018	16.9.2019	431	
CHG0031944	12.7.2018	9.12.2019	515	
CHG0031947	13.7.2018	13.11.2019	488	
CHG0031961	24.7.2018	11.10.2019	444	
CHG0031979	31.7.2018	11.10.2019	437	
CHG0031981	1.8.2018	2.12.2019	488	

CHG0032003	14.8.2018	4.10.2019	416
CHG0032007	16.8.2018	2.12.2019	473
CHG0032013	16.8.2018	9.10.2019	419
CHG0032054	29.8.2018	23.9.2019	390
CHG0032055	29.8.2018	23.9.2019	390
CHG0032067	3.9.2018	28.10.2019	420
CHG0032081	4.9.2018	11.10.2019	402
CHG0032122	10.9.2018	9.12.2019	455
CHG0032136	12.9.2018	20.1.2020	495
CHG0032143	13.9.2018	23.9.2019	375
CHG0032157	17.9.2018	4.10.2019	382
CHG0032202	25.9.2018	20.1.2020	482
CHG0032210	28.9.2018	23.10.2018	25
CHG0032220	1.10.2018	23.9.2019	357
CHG0032221	2.10.2018	9.10.2019	372
CHG0032237	3.10.2018	3.2.2020	488
CHG0032239	4.10.2018	23.9.2019	354
CHG0032292	9.10.2018	4.10.2019	360
CHG0032297	10.10.2018	4.10.2019	359
CHG0032298	10.10.2018	9.10.2019	364
CHG0032299	10.10.2018	23.9.2019	348
CHG0032328	15.10.2018	23.9.2019	343
CHG0032351	18.10.2018	23.9.2019	340
CHG0032363	19.10.2018	11.2.2019	115
CHG0032386	29.10.2018	23.9.2019	329
CHG0032417	2.11.2018	20.1.2020	444
CHG0032427	5.11.2018	23.9.2019	322
CHG0032429	6.11.2018	9.10.2019	337
CHG0032463	13.11.2018	4.10.2019	325
CHG0032464	13.11.2018	23.9.2019	314
CHG0032471	14.11.2018	23.9.2019	313
CHG0032477	15.11.2018	23.9.2019	312
CHG0032493	19.11.2018	23.9.2019	308
CHG0032501	21.11.2018	23.9.2019	306
CHG0032504	22.11.2018	20.1.2020	424
CHG0032537	3.12.2018	27.1.2020	420
CHG0032570	7.12.2018	4.10.2019	301
CHG0032621	14.12.2018	14.8.2019	243
CHG0032665	31.12.2018	23.9.2019	266
CHG0032673	4.1.2019	9.10.2019	278
CHG0032711	14.1.2019	9.10.2019	268
CHG0032713	15.1.2019	9.10.2019	267
CHG0032740	18.1.2019	23.9.2019	248
CHG0032750	21.1.2019	5.12.2019	318
CHG0032751	22.1.2019	3.10.2019	254
CHG0032791	30.1.2019	3.10.2019	246

CHG0032798	30.1.2019	14.3.2019	43
CHG0032875	8.2.2019	23.9.2019	227
CHG0032876	9.2.2019	9.10.2019	242
CHG0032883	11.2.2019	23.9.2019	224
CHG0032891	13.2.2019	20.1.2020	341
CHG0032924	19.2.2019	23.9.2019	216
CHG0032955	21.2.2019	3.10.2019	224
CHG0032962	25.2.2019	3.10.2019	220
CHG0032971	25.2.2019	20.1.2020	329
CHG0033006	1.3.2019	9.10.2019	222
CHG0033048	7.3.2019	23.9.2019	200
CHG0033057	8.3.2019	3.2.2020	332
CHG0033066	11.3.2019	23.9.2019	196
CHG0033094	13.3.2019	2.12.2019	264
CHG0033109	15.3.2019	23.9.2019	192
CHG0033167	22.3.2019	9.10.2019	201
CHG0033176	22.3.2019	3.10.2019	195
CHG0033287	5.4.2019	3.2.2020	304
CHG0033299	8.4.2019	23.9.2019	168
CHG0033322	10.4.2019	4.11.2019	208
CHG0033351	12.4.2019	23.9.2019	164
CHG0033360	12.4.2019	13.1.2020	276
CHG0033364	15.4.2019	9.1.2020	269
CHG0033368	16.4.2019	23.9.2019	160
CHG0033369	16.4.2019	23.9.2019	160
CHG0033370	16.4.2019	23.9.2019	160
CHG0033371	16.4.2019	3.10.2019	170
CHG0033375	17.4.2019	21.10.2019	187
CHG0033397	24.4.2019	10.9.2019	139
CHG0033399	24.4.2019	3.10.2019	162
CHG0033405	25.4.2019	23.9.2019	151
CHG0033422	29.4.2019	20.1.2020	266
CHG0033434	2.5.2019	3.10.2019	154
CHG0033451	3.5.2019	3.2.2020	276
CHG0033467	7.5.2019	10.10.2019	156
CHG0033472	8.5.2019	30.10.2019	175
CHG0033485	9.5.2019	14.11.2019	189
CHG0033584	17.5.2019	3.10.2019	139
CHG0033594	21.5.2019	2.12.2019	195
CHG0033612	22.5.2019	23.9.2019	124
CHG0033636	23.5.2019	11.12.2019	202
CHG0033759	29.5.2019	16.9.2019	110
CHG0033786	3.6.2019	9.9.2019	98
CHG0033829	10.6.2019	15.1.2020	219
CHG0033881	13.6.2019	9.1.2020	210
CHG0033892	13.6.2019	9.1.2020	210

CHG0033893	13.6.2019	18.10.2019	127
CHG0033894	14.6.2019	29.11.2019	168
CHG0033921	18.6.2019	16.1.2020	212
CHG0033931	18.6.2019	28.1.2020	224
CHG0033994	27.6.2019	13.11.2019	139
CHG0034062	11.7.2019	7.1.2020	180
CHG0034064	12.7.2019	2.12.2019	143
CHG0034078	15.7.2019	13.11.2019	121
CHG0034083	16.7.2019	30.9.2019	76
CHG0034104	22.7.2019	2.12.2019	133
CHG0034112	24.7.2019	3.2.2020	194
CHG0034116	26.7.2019	14.11.2019	111
CHG0034120	29.7.2019	17.9.2019	50
CHG0034130	31.7.2019	13.8.2019	13
CHG0034132	1.8.2019	21.1.2020	173
CHG0034264	22.8.2019	17.9.2019	26
CHG0034299	27.8.2019	16.9.2019	20
CHG0034300	28.8.2019	2.12.2019	96
CHG0034406	5.9.2019	4.2.2020	152
CHG0034412	6.9.2019	20.9.2019	14
CHG0034418	6.9.2019	14.11.2019	69
CHG0034458	10.9.2019	9.12.2019	90
CHG0034474	11.9.2019	24.9.2019	13
CHG0034509	12.9.2019	3.10.2019	21
CHG0034532	12.9.2019	23.1.2020	133
CHG0034540	13.9.2019	23.1.2020	132
CHG0034547	16.9.2019	3.1.2020	109
CHG0034616	20.9.2019	20.1.2020	122
CHG0034643	23.9.2019	15.1.2020	114
CHG0034675	25.9.2019	16.12.2019	82
CHG0034681	25.9.2019	2.10.2019	7
CHG0034696	25.9.2019	23.1.2020	120
CHG0034720	26.9.2019	1.10.2019	5
CHG0034725	27.9.2019	18.11.2019	52
CHG0034735	30.9.2019	23.10.2019	23
CHG0034771	1.10.2019	2.10.2019	1
CHG0034842	7.10.2019	23.1.2020	108
CHG0034867	8.10.2019	11.12.2019	64
CHG0034884	8.10.2019	2.12.2019	55
CHG0034986	16.10.2019	6.11.2019	21
CHG0034988	16.10.2019	1.11.2019	16
CHG0035065	22.10.2019	4.2.2020	105
CHG0035081	22.10.2019	13.11.2019	22
CHG0035105	23.10.2019	31.1.2020	100
CHG0035186	29.10.2019	4.11.2019	6
CHG0035227	29.10.2019	29.10.2019	0

CHG0035389	1.11.2019	14.11.2019	13
CHG0035421	4.11.2019	14.11.2019	10
CHG0035428	5.11.2019	19.11.2019	14
CHG0035608	14.11.2019	31.1.2020	78
CHG0035639	18.11.2019	13.1.2020	56
CHG0035783	27.11.2019	28.1.2020	62
CHG0035792	27.11.2019	19.12.2019	22
CHG0035804	28.11.2019	22.1.2020	55
CHG0035805	28.11.2019	17.12.2019	19

Appendix 3. ITSM Process for Server Installations

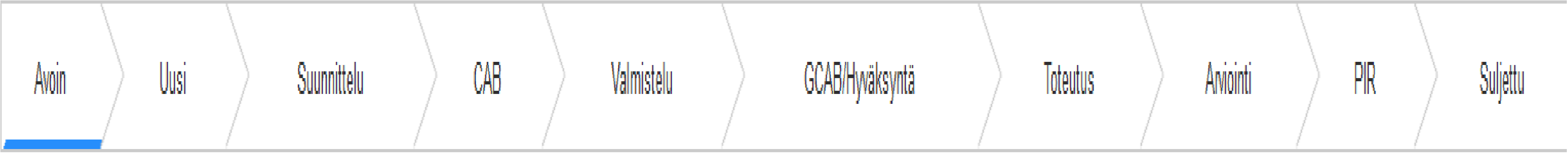


Figure 9 ITSM phases of the normal change

Appendix 4. System Integrations

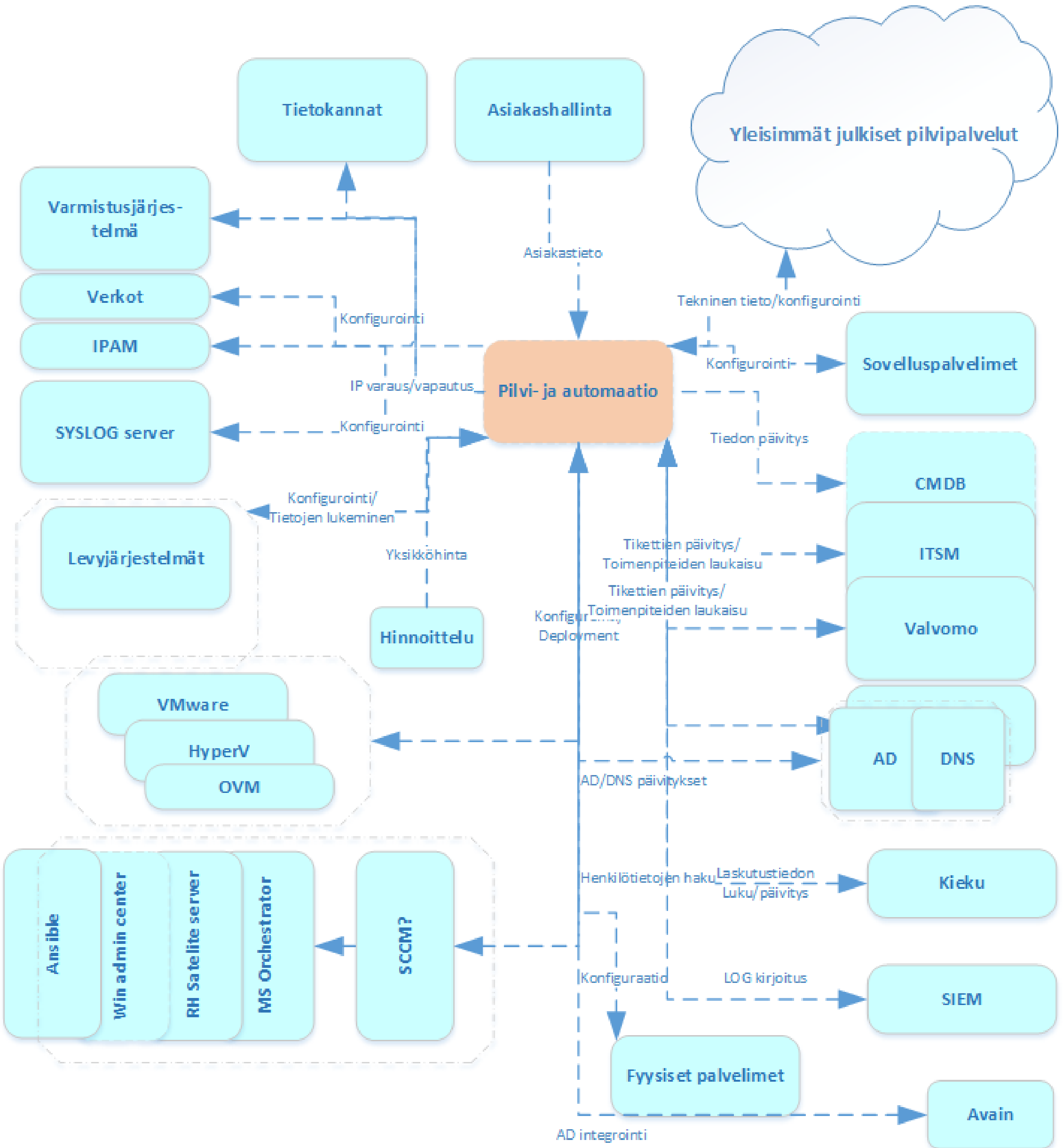
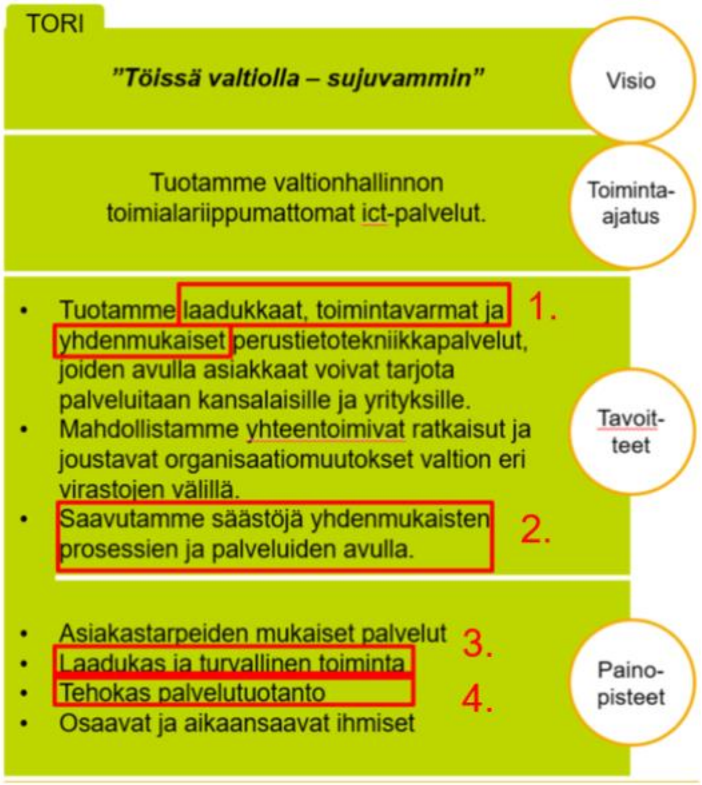


Figure 10 Hybrid Cloud and Automation System Integrations

Appendix 5. Strategy 2018 Impacts on project



TORI

"Töissä valtiolla – sujuvammin" — Visio

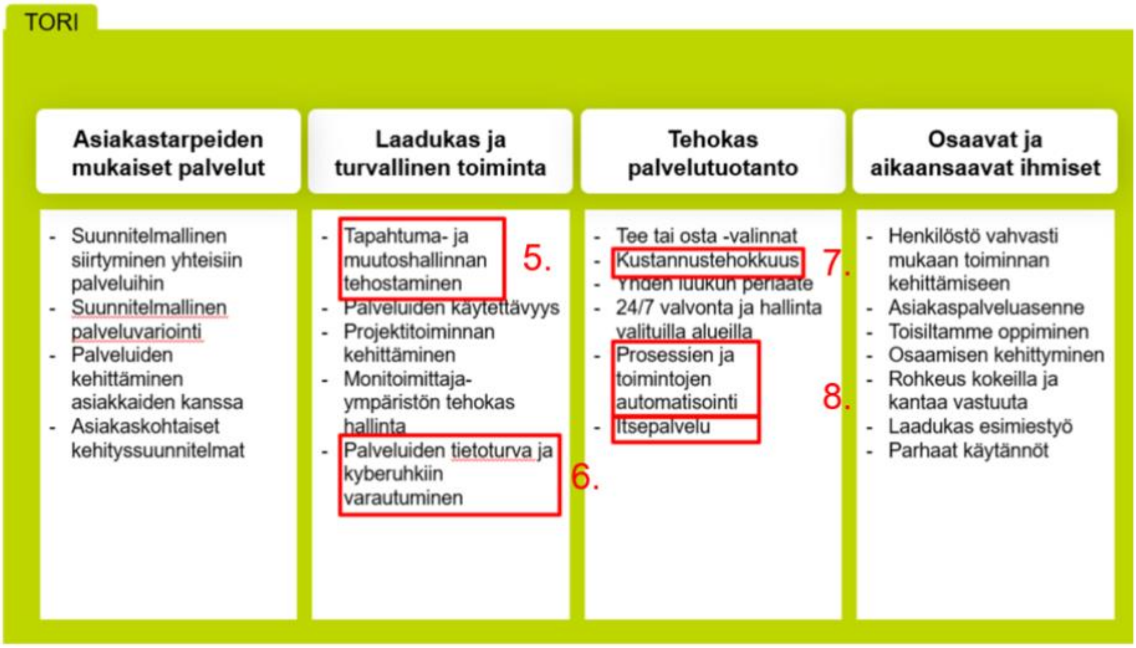
Tuotamme valtionhallinnon toimialariippumattomat ict-palvelut. — Toiminta-ajatus

Tavoit-teet

- Tuotamme laadukkaat, toimintavarmat ja yhdenmukaiset perustietotekniikkapalvelut, joiden avulla asiakkaat voivat tarjota palveluitaan kansalaisille ja yrityksille. 1.
- Mahdollistamme yhteentoimivat ratkaisut ja joustavat organisaatiomuutokset valtion eri virastojen välillä.
- Saavutamme säästöjä yhdenmukaisten prosessien ja palveluiden avulla. 2.

Paino-pisteet

- Asiakastarpeiden mukaiset palvelut
- Laadukas ja turvallinen toiminta 3.
- Tehokas palvelutuotanto 4.
- Osaavat ja aikaansaavat ihmiset



TORI

Asiakastarpeiden mukaiset palvelut	Laadukas ja turvallinen toiminta	Tehokas palvelutuotanto	Osaavat ja aikaansaavat ihmiset
- Suunnitelmallinen siirtyminen yhteisiin palveluihin - Suunnitelmallinen palveluvariointi - Palveluiden kehittäminen asiakkaiden kanssa - Asiakaskohtaiset kehityssuunnitelmat	- Tapahtuma- ja muutoshallinnan tehostaminen 5. - Palveluiden käytettävyys - Projektitoiminnan kehittäminen - Monitoimittaja-ympäristön tehokas hallinta - Palveluiden tietoturva ja kyberuhkiin varautuminen 6.	- Tee tai osta -valinnat - Kustannustehokkuus 7. - Yhden luukun periaate - 24/7 valvonta ja hallinta valituilla alueilla - Prosessien ja toimintojen automatisointi 8. - Itsepalvelu	- Henkilöstö vahvasti mukaan toiminnan kehittämiseen - Asiakaspalveluasenne - Toisiltamme oppiminen - Osaamisen kehittyminen - Rohkeus kokeilla ja kantaa vastuuta - Laadukas esimiestyö - Parhaat käytännöt

Figure 11 Case Company Strategy 2018 Impacts on Hybrid Cloud- and Automation projects

Appendix 6. Questionnaire in RFI presentation phase

Table 44 RFI, Presentation Phase Questionaire, Automation

Tunnus (ID)	Kategoria	Vaatimus	Ratkaisu täyttää vaatimuksen	Kommentit
AuVa_1	Yleinen	Järjestelmään voidaan konfiguroida työjonoja vapaasti "ohjelmoiden" liittyen tietojärjestelmiin tietopyyntö -dokumentissa, kuva 1	kyllä/ei/osittain	
AuVa_2	Yleinen	Järjestelmällä voidaan orkestroida töitä eri tietojärjestelmissä jos ne vain suinkin antavat siihen mahdollisuuden		
AuVa_3	Virtualisointi	Palvelujen "älykäs" sijoittelu hypervisorin (HyperV, vSphere) päälle. Ottaa huomioon mm.klusteroinnin, allokointiasteen sekä muut mahdolliset parametrit.		
AuVa_4	Palvelimet	Automaatiolla on pystyttävä asentamaan, hallitsemaan ja päivittämään ainakin seuraavia käyttöjärjestelmiä: Win 2008R2, Win 2016, Win 2012R2 RHEL 6, RHEL 7; SuSe 11, SuSe 12; Ubuntu 16, Ubuntu 18; CentOS 6, CentOS 7		
AuVa_5	Palvelimet	Järjestelmällä pystytään päivittämään laitteiden ajurit sekä BIOS:n versiot		
AuVa_6	Tietoturva	Pystyttävä asentamaan ja hallitsemaan yleisimmät (F-secure jne.) virustorjunta ohjelmistot palvelinympäristössä.		
AuVa_7	Tietokannat	Automaatiolla on pystyttävä automatiosoimaan tehtäviä seuraavien tietokantoihin liittyviä tehtäviä, MSSQL, MariaDB 5-, MySQL 5-, Oracle 11-12, Postgre 9.2 - 10		
AuVa_8	Sovelluspalvelimet	Automaatiolla on pystyttävä automatiosoimaan tehtäviä seuraaviin sovelluspalvelimiin liittyen, Jboss, apache, IIS, Tomcat, Nginx, WebSphere, Weblogic vers x		
AuVa_9	Tietoliikenne	Palvelun on pystyttävä hallitsemaan ja automatiosoimaan tehtäviä liittyen seuraaviin verkkokomponentteihin Reitittimet: Juniper MX480 Kytkimet: Extreme Summit x670 G2 ja X460 G2 Virtuaalikytkimet System Center ja vmware Palomuurit: Check point, Juniper IPAM: Fusion Layerin Infinity Data Center Infrastructure Management: OpenDCIM		

AuVa_10	Yleinen	Tuki seuraavien varmenteiden ja salausavainten generoimiseen sekä asentamiseen kohdepalvelimelle: Palvelimen SSL-varmenteet. Telia/Entrust		
AuVa_11	Tietoturva	Kohdepalvelun (palvelin-, tietoliikennelaite jne. konfiguraation tai tilan) tarkistus, raportointi ja korjaus erikseen tuotettua (PCI tms.) tai itse muodostettua (palvelinkuva tms.) referenssiä vasten.		
AuVa_12	Yleinen	Yleinen REST tms. rajapinta minkä kautta järjestelmää voidaan käyttää ohjelmallisesti (XML, Json tms. viestit.) . Käyttäjät voidaan autentikoida, logittaa ja tilastoida.		
AuVa_13	Yleinen	Fyysisen palvelimen ja/tai kehikon (HPE, DELL, IBM, Fujitsu, Huawei) asennus ja konfigurointi		
AuVa_14	Yleinen	Muutokset infrastruktuuriin päivittyvät CMDB- ja ITSM-järjestelmään (Servicenow) automaattisesti		
AuVa_15	Tietoliikenne	Järjestelmän pitää pystyä tuottamaan QoS tyyppisiä konfiguraatioita missä esim. puhe saa korkeamman prioriteetin ja nopeammat vasteet kuin normaali internetin selausliikenne		
AuVa_16	Tietoturva	Järjestelmän käyttäjien roolit ja niiden oikeudet on voitava määritellä jokainen erikseen (RBAC tai vastaava)		
AuVa_17	Virtualisointi	Virtualisointialustojen tuki HyperV 2016, Vmware 6.5, Oracle VM		
AuVa_18	Tietoturva	Liikenne hallittaviin komponentteihin on salattu viestintäviraston hyväksymillä salausmenetelmillä. STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf		
AuVa_19	Tietoturva	Järjestelmä tukee monivaiheista tunnistautumista.		
AuVa_20	Tietoturva	Järjestelmän hallintayhteydet ovat salattuja (HTTPS, SCP, SSH jne.) toteutetaan viestintäviraston hyväksymillä salausmenetelmillä kuten STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf		

AuVa_21	Tietoturva	Tiedot järjestelmän tietokannassa sekä hallintayhteydet salataan viestintäviraston hyväksymillä salausmenetelmillä kuten STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf		
AuVa_22	Tietoturva	Järjestelmää hallitaan ilman yhteiskäyttötunnuksia ja audit trail on käytössä		
AuVa_23	Tietoturva	Järjestelmän palvelinalusta voidaan koventaa Case companyn määrittelemällä tavalla?		
AuVa_24	Tietoturva	Haittatorjuntaohjelmistoa, kuten F-secure, on pystyttävä ajamaan järjestelmän alustoilla		
AuVa_25	Tietoturva	Järjestelmä tukee lokitiedon (myös Audit trail log) sijoittamista erilliselle logituspalvelimelle, oletuspalvelimen lisäksi.		
AuVa_26	Tietoturva	Järjestelmä tukee kryptografisesti vahvoja avaimia, turvallista avainten jakelua sekä säännöllistä avainten vaihtoa? Tiedot järjestelmän tietokannassa salataan viestintäviraston hyväksymillä salausmenetelmillä kuten STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf)		
AuVa_27	Tietoturva	Järjestelmään on toimitettava säännöllisesti korjauksia ja toimittajan on reagoitava uusiin tietoturvauhkiin välittömästi. Toimittajalla on oltava ajantasainen tieto järjestelmän eri komponenttien tietoturvatilanteesta.		
AuVa_28	Tietoturva	Järjestelmä tukee tietojen tuontia järjestelmään ja vientiä järjestelmästä yleisesti määritellyssä formaatissa kuten XML, JSON, CSV tms.		
AuVa_29	Tietoturva	Jos järjestelmä kirjoittaa varmuuskopiota itsestään niin kopio on salattava viestintäviraston hyväksymillä salausmenetelmillä kuten STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf)		

AuVa_30	Yleinen	Järjestelmä sisältää discovery toiminta, joka löytää uudet objektit (palvelimet, reitittimet jne.) verkosta		
AuVa_31	Yleinen	Voidaan noudattaa loose couple periaatetta. Provisioitavien ja hallittavien järjestelmien toiminta ei saa olla riippuvainen tämän järjestelmän uptimesta/käyttövarmuudesta		
AuVa_32	Kontit	Järjestelmä tukee 'kontti' tekniikoita kuten Docker, Kubernetes		
AuVa_33	Ei toiminnallinen	RPO 24h		
AuVa_34	Ei toiminnallinen	RTO 48h		
AuVa_35	Saatavuus	Järjestelmälle voidaan varmistaa 24/7 saatavuus		
AuVa_36	Skaalautuvuus	Järjestelmän on toimittava monikonesaliympäristössä missä hallittavat järjestelmät ovat useassa konesalissa		
AuVa_37	Skaalautuvuus	Järjestelmään voidaan lisätä/vähentää kapasiteettia (CPU, muistia, palvelimia jne.) tarpeen mukaan.		
AuVa_38	Siirrettävyys	Järjestelmä pystytään palauttamaan varmistuksista uuteen ympäristöön		
AuVa_39	Ylläpidettävyys	Järjestelmä on voitava päivittää ilman konfiguraatiotietojen katoamista tai radikaalia uudelleen kirjoittamista.		
AuVa_40	Ei toiminnallinen	Järjestelmä tukee yleisimipiä ohjelmointi/skriptaus kieliä.		
AuVa_41	Integroitavuus	Integraatiot muihin järjestelmiin yleisten rajapintojen kautta.		
AuVa_42	Suorituskyky	Yleisesti hyväksyttävät vasteajat on täytyttävä ja käyttökokemus on sujuva.		
AuVa_43	Ei toiminnallinen	Tietojärjestelmä on helppo käyttää ja nopea oppia.		
AuVa_44	Ei toiminnallinen	Tukipalvelujen vasteaika häiriötilanteissa Next Business Day		
AuVa_45	Ei toiminnallinen	Järjestelmä voidaan asentaa windowsin tai linuxin päälle.		
AuVa_46	Ei toiminnallinen	Ajantasainen ohjeistus oltava saatavilla ja todennettavissa		
AuVa_47	Ei toiminnallinen	Järjestelmä tukee tarvittavia merkistöjä Suomi, Ruotsi, Englanti		
AuVa_48	Ei toiminnallinen	Kaksi vanhempaa versiota järjestelmästä pitää olla saatavilla ja tuettuna		
AuVa_49	Ei toiminnallinen	Historiatietojen säilytys/saatavuus. Järjestelmään voidaan määrittää logien säilytysajat ja -tasot		

AuVa_50	Yleinen	Järjestelmä on pystyttävä asentamaan Case companyn konesaleihin		
AuVa_51	Varmistus	Järjestelmä tukee seuraavia varmistusjärjestelmiä TSM, Veritas netbackup 8.0, netapp FAS 8200, FAS 8020, FAS 8040		
AuVa_52	Levyjärjestelmä	Järjestelmä tukee seuraavia levyjärjestelmiä: Netapp FAS 8020, nauhakirjasto Quantum scalar i500, Veritas netbackup 8.0 Veritas netbackup 8.0 TSM, Netapp FAS 8200 levytallennus, veritas netback 8.0		
AuVa_53	Valvonta	Järjestelmä tukee seuraaavia valvontajärjestelmiä SCOM 2016, Patrol, Tivoli		
AuVa_54	Yleinen	Raportteja voidaan räätälöidä Case companyn tarpeiden mukaan		
AuVa_55	Käytettävyys	Käyttöliittymää voidaan muokaa Case companyn tarpeiden mukaan		
AuVa_56	Suorituskyky	Suorituskyky on skaalautuva käyttäjämäärän ja hallittavien laitemäärien (ainakin 7000 palvelinta) mukaan.		
AuVa_57	Yleinen	Monidomain tuki, palvelee useita erillisiä domaineja ja workgrouppeja tarvittaessa.		
AuVa_58	Yleinen	Järjestelmä tukee LDAP protokollaa		
AuVa_59	Tietoturva	Järjestelmän rajapinnat on suojattu luvattomalta käytöltä ja sen on kestettävä laajamittaista haavoittuvuusskannaus.		
AuVa_60	Tietoturva	Järjestelmä tukee monivaiheista tunnistautumista.		
AuVa_61	Yleinen	Järjestelmällä voidaan hallita olemassa olevat palvelimet ja verkkolaitteet sekä automatisoida niihin liittyvät päivittäiset toimenpiteet		
AuVa_62	Yleinen	Toimittajan kautta pystytään järjestämään tarvittavat koulutukset Case companyn henkilökunnalle		

Table 45 Presentation Phase Questionnaire, Cloud

Tunnus (ID)	Kategoria	Vaatimus	Ratkaisu täyttää vaatimuksen	Kommentit
PiVa_1	Yleinen	Asiakas (tai Case companyn edustaja asiakkaan puolesta) voi lisätä, poistaa, sammuttaa, käynnistää ja muokata palveluja itse	kyllä/ei/osittain	
PiVa_2	Tietoturva	Järjestelmä tukee monivaiheista tunnistautumista.		
PiVa_3	Yleinen	Käyttäjän voi vaihtaa roolia oman autorisoinnin mukaan.		
PiVa_4	Palvelimet	Palvelun on pystyttävä hallitsemaan ja provisioimaan ainakin seuraavia käyttöjärjestelmiä: Win 2016, Win 2012R2 RHEL 6, RHEL 7; SuSe 11, SuSe 12;		

		Ubuntu 16, Ubuntu 17; CentOS 6, CentOS 7		
PiVa_5	Tietokannat	Palvelun on pystyttävä hallitsemaan ja provisioimaan ainakin seuraavia tietokantoja: MSSQL, MariaDB 5-, MySQL 5-,Oracle 11-12, Postgre 9.2 - 10		
PiVa_6	Sovelluspalvelimet	Palvelun on pystyttäva hallitsemaan ja provisioimaan seuraavia sovelluspalvelimia: Jbos, apache, IIS, Tomcat, Nginx, WebSphere, Weblogic		
PiVa_7	Tietoliikenne	Palvelun on pystyttävä hallitsemaan ja provisioimaan ainakin seuraavia verkkokomponentteja: Reitittimet: Juniper MX480 Kytkimet: Extreme Summit x670 G2 ja X460 G2 Palomuurit: Check point, Juniper IPAM: Fusion Layerin Infinity Data Center Infrastructure Management: OpenDCIM		
PiVa_8	Tietoturva	Roolit ja niiden oikeudet on pystyttävä määritelemään jokainen erikseen ja myös lisämään käyttöönoton jälkeen (RBAC tai vastaava)		
PiVa_9	Container	Palvelu tukee 'kontti' tekniikoita kuten Docker, Kubernetes		
PiVa_10	Raportointi	Asiakas (tai Case companyn edustaja asiakkaan puolesta) näkee online raportin asiakkaan omista palveluista sekä pystyy tulostamaan raportin tiedot tiedostoon.		
PiVa_11	Raportointi	Järjestelmässä voidaan muokata haluttuja raportteja ja raportoida ne mm. ajastetusti		
PiVa_12	Yleinen	Järjestelmää voidaan käyttää ohjelmallisesti rajapintojen (API) kautta.		
PiVa_13	Yleinen	Järjestelmä tukee kolmannen osapuolen pilvipalveluita AWS, Azure, Google Cloud, RH Openshift		
PiVa_14	Tietoturva	Autentikointi tukee keskitettyä autentikointia (AD tms.) siten että käyttäjiä, oikeuksia ja rooleja pidetään yllä ainoastaan yhdessä paikassa		
PiVa_15	Palvelimet	Olemassa olevat virtuaalipalvelimet/palvelut voidaan näyttää ja hallita osana pilvipalvelua ilman uudelleen pystytystä		
PiVa_16	Palvelimet	Järjestelmä tukee palvelujen vertikaalista ja horisontaalista skaalautuvuutta muun tekniikan asettamien vaatimusten rajoissa (esim. palvelin voidaan kahdentaa ja muokata kuorman jakajaa ohjaamaan liikenne kummallekkin palvelimelle kun tietty ehto täyttyy)		
PiVa_17	Tietoturva	Hallittavien kohdepalvelujen käyttöjärjestelmät ja muut ohjelmistot pystytään päivittämään graafisen- tai ohjelmallisen rajapinnan kautta		

PiVa_18	Yleinen	Tuki seuraavien varmenteiden ja salausavainten generoimiseen sekä asentamiseen kohdepalvelimelle: Palvelimen SSL-varmenteet. Telia/Entrust		
PiVa_19	Integroitavuus	Muutokset infrastruktuuriin pitää päivittyä CMDB- ja ITSM-järjestelmiin automaattisesti		
PiVa_20	Tietoliikenne	Järjestelmän pitää pystyä tuottamaan QoS tyyppisiä konfiguraatioita missä esim. puhe saa korkeamman prioriteetin ja nopeammat vasteet kuin normaali internetin selausliikenne		
PiVa_21	Virtualisointi	Virtualisointialustojen tuki HyperV 2016, Vmware 6.5, OVM x.y		
PiVa_22	Tietoturva	Kohdepalvelun (palvelin-, tietoliikennelaite jne. konfiguraatio) tarkistus, raportointi ja korjaus erikseen tuotettua (PCI tms.) tai itse muodostettua (palvelinkuva tms.) referenssiä vasten.		
PiVa_23	Tietoturva	Liikenne hallittaviin komponentteihin on salattu viestintäviraston hyväksymillä salausmenetelmillä. STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf		
PiVa_24	Tietoturva	Järjestelmä voidaan toteuttaa verkon osalta segementoidusti (palvelu, sovellus ja tietokanta).		
PiVa_25	Tietoturva	Järjestelmän hallintayhteydet ovat salattuja (HTTPS, SCP, SSH jne.) toteutetaan viestintäviraston hyväksymillä salausmenetelmillä kuten STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf		
PiVa_26	Tietoturva	Tiedot järjestelmän tietokannassa sekä hallintayhteydet salataan viestintäviraston hyväksymillä salausmenetelmillä kuten STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf		
PiVa_27	Tietoturva	Järjestelmää hallitaan ilman yhteiskäyttö- ja yleisiä admin (esim. root) tunnuksia.		
PiVa_28	Tietoturva	Palvelinalusta voidaan koventaa Case companyn määrittelemällä tavalla		
PiVa_29	Tietoturva	Haittatorjuntaohjelmistoa, kuten F-secure, on pystyttävä ajamaan järjestelmän alustoilla		
PiVa_30	Tietoturva	Järjestelmä tukee kaiken oleellisen lokitiedon (myös Audit trail log) sijoittamista erilliselle logituspalvelimelle, oletuspalvelimen lisäksi.		

PiVa_31	Tietoturva	Järjestelmä tukee kryptografisesti vahvoja avaimia, turvallista avainten jakelua sekä säännöllistä avainten vaihtoa? Tiedot järjestelmän tietokannassa salataan viestintäviraston hyväksymillä salausmenetelmillä kuten STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf)		
PiVa_32	Tietoturva	Järjestelmään on toimitettava säännöllisesti korjauksia ja toimittajan on reagoitava uusiin tietoturvauhkiin välittömästi. Toimittajalla on oltava ajantasainen tieto järjestelmän eri komponenttien tietoturvatilanteesta. Järjestelmän rajapintojen on suojattu luvattomalta käytöltä ja sen on kestettävä laajamittaista haavoittuvuusskannaus.		
PiVa_33	Tietoturva	Järjestelmä tukee tietojen tuontia järjestelmään ja vientiä järjestelmästä yleisesti määritellyssä formaatissa kuten XML, JSON, CSV tms.		
PiVa_34	Tietoturva	Jos järjestelmä kirjoitaa varmuuskopiota itsestään niin kopio on salattava viestintäviraston hyväksymillä salausmenetelmillä kuten STIV AES 192, SHA 256, source: viestintävirasto (https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf)		
PiVa_35	Yleinen	Loose couple periaate, provisioitavien ja hallittavien järjestelmien toiminta ei saa olla riippuvainen tämän järjestelmän uptimesta/käyttövarmuudesta		
PiVa_36	Ei toiminnallinen	RPO 24h		
PiVa_37	Ei toiminnallinen	RTO 48h		
PiVa_38	Saatavuus	Järjestelmälle voidaan varmistaa 24/7 saatavuus		
PiVa_39	Skaalautuvuus:	Järjestelmän on toimittava monikonesaliympäristössä missä hallittavat järjestelmät ovat useassa konesalissa		
PiVa_40	Skaalautuvuus	Järjestelmään voidaan lisätä/vähentää kapasiteettia (CPU, muistia, palvelimia jne.) tarpeen mukaan.		
PiVa_41	Siirrettävyys	Järjestelmä pystytään palauttamaan varmistuksista uuteen ympäristöön		
PiVa_42	Ylläpidettävyys	Järjestelmä on voitava päivittää ilman konfiguraatiotietojen katoamista tai radikaalia uudelleen kirjoittamista.		
PiVa_43	Räätälöitävyys	Järjestelmä tukee yleisimipiä ohjelmointi/skriptaus kieliä.		
PiVa_44	Integroitavuus	Integraatiot muihin järjestelmiin yleisten rajapintojen kautta.		
PiVa_45	Suorituskyky	Yleisesti hyväksyttävät vasteajat on täytyttävä ja käyttökokemus on sujuva.		

PiVa_46	Ei toiminnallinen	Tietojärjestelmä on helppo käyttää ja nopea oppia.		
PiVa_47	Ei toiminnallinen	Tukipalvelujen vasteaika häiriötilanteissa Next Business Day		
PiVa_48	Ei toiminnallinen	Käytönaikaisen tuen saanti: Tukipalvelujen vasteaika häiriötilanteissa Next Business Day		
PiVa_49	Ei toiminnallinen	Järjestelmä voidaan asentaa windowsin tai linuxin päälle.		
PiVa_50	Ei toiminnallinen	Ajantasainen ohjeistus oltava saatavilla ja todennettavissa		
PiVa_51	Ei toiminnallinen	Järjestelmä tukee tarvittavia merkistöjä Suomi, Ruotsi, Englanti		
PiVa_52	Ei toiminnallinen	Kaksi vanhempaa versiota järjestelmästä pitää olla saatavilla ja tuettuna		
PiVa_53	Ei toiminnallinen	Historiatietojen säilytys/saatavuus. Järjestelmään voidaan määrittää logien säilytysajat ja -tasot		
PiVa_54	Ei toiminnallinen	Järjestelmä on pystyttävä asentamaan Case companyn konesaleihin		
PiVa_55	Varmistus	Järjestelmä tukee seuraavia varmistusjärjestelmiä TSM, Veritas netbackup 8.0, netapp FAS 8200, FAS 8020, FAS 8040		
PiVa_56	Levyjärjestelmä	Järjestelmä tukee seuraavia levyjärjestelmiä: Netapp FAS 8020, nauhakirjasto Quantum scalar i500, Veritas netbackup 8.0 Veritas netbackup 8.0 TSM, Netapp FAS 8200 lyvytallennus, veritas netback 8.0		
PiVa_57	Valvonta	Järjestelmä tukee seuraaavia valvontajärjestelmiä SCOM 2016, Patrol, Tivoli		
PiVa_58	Yleinen	Raportteja voidaan räätälöidä Case companyn tarpeiden mukaan		
PiVa_59	Tietoturva	Asiakasympäristöt on eristetty toisistaan ja tietojen sekoittuminen voidaan varmasti välttää		
PiVa_60	Käytettävyys	Käyttöliittymää voidaan muokaa Case companyn tarpeiden mukaan		
PiVa_61	Suorituskyky	Suorituskyky on skaalautuva käyttäjämäärän ja hallittavien laitemäärien (ainakin 7000 palvelinta) mukaan.		
PiVa_62	Yleinen	Monidomain tuki, palvelee useita erillisiä domaineja ja workgrouppeja tarvittaessa.		
PiVa_63	Yleinen	Järjestelmä tukee LDAP protokollaa		
PiVa_64	Tietoturva	Järjestelmän rajapinnat on suojattu luvattomalta käytöltä ja sen on kestettävä laajamittaista haavoittuvuusskannaus.		
PiVa_65	Yleinen	Järjestelmässä voidaan tuoda olemassa olevat palvelimet pilvikäyttöliittymään asiakkaan hallittaviksi.		
PiVa_66	Yleinen	Järjestelmällä voidaan siirtää palvelinkuormaa julkisen pilven (azure AWS) ja oman virtualisointialustan (hyperV, vSphere) välillä		
PiVa_67	Yleinen	Toimittajan kautta pystytään järjestämään tarvittavat koulutukset Case companyn henkilökunnalle		