Expertise
and insight
for the future

Ilmari Kallioniemi

Installing and Commissioning MCS Over an LTE -System

Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communication Technology

Bachelor's Thesis

24 April 2019

Author Title Number of Pages Date	Ilmari Kallioniemi Installing and Commissioning MCS Over an LTE system. 26 pages + 0 appendices 24 April 2019
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Professional Major	IoT and Cloud Computing
Instructors	Tapio Wikström, Senior Lecturer

The purpose of this thesis was to study the concept of system providing mission critical services over LTE or other cellular networks, compare the system to TETRA network and install the system. The thesis also goes through the different deployment options. Those options are local, public and private cloud deployments. Unlike traditional TETRA, or similar public safety radio systems, LTE has the benefits of much higher bandwidth, such as being able to transmit live video, or transfer files.

The system was installed on top of the VMWare ESXi 6.5 type 1 hypervisor as a local installation, meaning that all the aspects of the server, hypervisor and infrastructure had to be installed from scratch. The locally installed system was connected to a public network, where it could communicate with the end devices connected over LTE.

After a few hiccups, the system installation was proven to be working successfully with our own tests inside the same network, and over commercial LTE, which was the main goal of the installation. Live video, data and location information was transmitted well over the network

In conclusion, the benefits outweigh the negative aspects of using LTE in public safety. It is very useful to have higher bandwidth for public safety applications. With LTE, transferring of data is faster, and live video is possible. LTE also enables other applications which could be installed to next generation terminals, like almost instantaneous ID checking, or AI applications from video and audio feed.

Keywords	Mission critical services, virtualisation, LTE

Tekijä Otsikko Sivumäärä Aika	Ilmari Kallioniemi MCS yli LTE -järjestelmän käyttöönotto ja asennus 26 sivua + 0 liitettä 24.4.2019
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	Verkot ja pilvipalvelut
Ohjaajat	lehtori Tapio Wikström

Insinöörityön tavoite oli tutkia tehtävien kannalta oleellisen järjestelmän toimintaperiaatteita ja toimivuutta kaupallisten LTE-verkkojen yli sekä verrata tätä järjestelmää ja sen ominaisuuksia perinteisiin TETRA-verkkoihin. Työhön sisältyi myös järjestelmän asennus ja sen kuvaaminen. Kuvattuna ovat myös erilaiset mahdolliset vaihtoehdot mahdollisista arkkitehtuureista, joiden ympärille järjestelmä voidaan asentaa, kuten paikallisesti, paikalliseen pilveen tai julkiseen pilveen.

Insinöörityössä järjestelmä asennettiin paikallisesti yhden palvelimen asennuksena, joka tarkoittaa sitä, että myös infrastruktuuri oli pakko asentaa itse. Kyseessä oleva tehtävien kannalta oleellinen järjestelmä asennettiin VMWare ESXi 6.5 tyypin 1 virtualisointiympäristöön.

Muutaman alun vian jälkeen järjestelmä todettiin toimivaksi ja käyttökelpoiseksi niin samassa verkossa palvelimen kanssa, kuin kaupallisen mobiiliverkonkin yli, mikä oli myös työn päätavoite.

Insinöörityön lopputuloksena meillä on järjestelmä, joka pystyy puheen lisäksi välittämään myös elävää kuvaa ja dataa isomman kapasiteetin ansiosta, toisin kuin perinteiset yleisen turvallisuuden verkot. Tärkeintä järjestelmässä kuitenkin on, että valtiolliset operaattorit ynnä muut voivat käyttää jo olemassa olevia LTE-verkkoja, mikä taas johtaa isoihin säästöihin, jos ei tarvitse rakentaa omaa verkkoinfrastruktuuria. Tulevaisuudessa järjestelmään voidaan rakentaa myös lisäominaisuuksia, mm. nopea henkilöpapereiden tarkastus, ja uhkien tunnistus tekoälyn avulla kuva-, video- tai ääni-informaatiosta.

Avainsanat	Tehtävän kannalta oleellinen järjestelmä, virtualisointi, LTE

Contents

List of Abbreviations

MCS	Mission critical services. Services that are critical for the operation of system [1].
TETRA	Terrestrial Trunked Radio. European standard for a trunked radio system, is a professional mobile radio and two-way transceiver specification [2].
KMS	Key management system. Manages and distributes cryptographic encryption keys required for encryption.
DHCP	Dynamic Host Control Protocol. Management protocol enabling dynamic assignment of an IP address to a network attached device [3].
GW	Gateway. Server that enables two different systems to communicate with each other.
AMD	Automated Multimedia Dispatcher. Dispatcher solution with integrated maps and unit positioning tools.
LTE	Long Term Evolution. A Mobile broadband standard by 3GPP.
IP	Internet Protocol. Protocol that enables moving of datagrams trough interconnected networks [4].
NIC	Network Interface Card. NIC provides the physical layer for the computer to communicate with data link layer of network [5].
DNS	Domain Name System. DNS is a directory that translates human readable domain names to IP addresses and vice versa [6].
GUI	Graphical user interface. A type of interface that allows user to interact with the computer via graphical icons [7].
iLO	Integrated Lights-Out. Hewlett Packard Enterprise's remote management system for servers [8].

TEA	TETRA Encryption Algorithm. An algorithm that encrypts the air interface of radios and base stations.
AES	Advanced Encryption Standard. Standard specifying Rijndael algorithm established by US National Institute of Standards and Technology [9].
RTP	Real Time Protocol. Protocol providing end-to-end network transport functions for applications transmitting real time data [10].
DCUI	Direct Console User Interface. Interface that allows user to interact with a host machine locally using text-based menus [11].
SRTP	Secure Real Time Protocol. A version of Real Time protocol which can provide confidentiality, message authentication and replay protection [12].
WLAN	Wireless Local Area Network. IEEE 802.11 standard for connecting devices wirelessly to access point and network.

1 Introduction

The purpose of this thesis was to study the concept of a system providing mission critical services over cellular or other internetworks. This kind of system is most likely the future in public safety applications. Cellular network, like Long Term Evolution, or wireless networks provide much higher bandwidth than already existing narrowband professional mobile radio networks, which in turn enables the use of real-time video and data services [13]. It also gives flexibility to develop new applications on top of the network, like image recognition using artificial intelligence. One part of demand of such systems is most likely money. If the professional mobile radio network operators can move away from their own network infrastructure to commercial cellular networks, they would save potentially a considerable amount of money by not having the need to maintain the infrastructure anymore.

Another part of this thesis was to deploy this kind of system to working condition and test its benefits compared to those of a traditional professional mobile radio network. This thesis was done for a real-life customer as part of a pilot project, where a customer evaluates the benefits and downsides of moving away from their own professional mobile radio network to commercial cellular network.

1.1 Mission Critical Services over LTE

MCS stands for Mission Critical Services. Mission Critical means anything that is critical for everyday life, security, defence, health and so forth. Examples of mission critical systems are communication channels for authorities, and power distribution networks.

This MCS over LTE system is providing communication channels to be used with mission critical applications over commercial LTE/4G mobile networks. Current operators of traditional mission critical networks, like terrestrial trunked radio, or TETRA have usually their own infrastructure. The downside of this is that maintaining and buying new equipment is very expensive; thus, some operators opt for a solution where they buy bandwidth from commercial 4G/LTE operators, and in some cases laws are set to place that ensures that commercial operators get certain bandwidth allocation and QoS, or Quality of Service, where the MCS traffic is ensured to always have “right of way” in the network.

Some MCS over LTE systems also enable to communicate between traditional professional mobile radio networks, like TETRA or TETRAPOL. It would be possible to have traditional radio terminal users and smartphone users in the same call. [14]

1.2 Connection Technology

The MCS over LTE system is using IP, or Internet protocol, but it is medium agnostic. In other words, the connection method between the servers and the end-devices (smartphones and tablets) could be done with whatever technology that can carry IP packets.

4G or LTE is as the other marketing term implies, fourth generation of the digital GSM standard. 4G is chosen because it is suitable for the application needs. For the end-users, the solution must be as portable as possible, therefore mobile connection is necessary, and 4G provides higher bandwidth and lower latencies than its predecessors. Higher bandwidth, in addition to 4G being a packet switched network, makes sending of different types of data possible over the network. For example, real time video, or large files.

TETRA and 2G has these data implementations on top of the circuit switched networks as well, but they are, for example, slow and not suitable to send video.

Another benefit of 4G is that, like 3G, 4G is packet switched, whereas 2G and TETRA networks are circuit switched networks. Circuit switched networks need additional physical hardware to provide increased capacity to the network, unlike packet switched networks, which would not need so much physical hardware to ensure the capacity. In packet switched networks, the network is never unavailable because of the high load unlike in traditional circuit switched networks, but latencies can increase without additional hardware, due to the limited number of packets per second that the existing hardware can forward.

Downsides of 4G is higher frequencies, which make the faster data speeds possible. Higher frequencies do not, for example, bend around obstacles as much or go through

buildings; thus, density of base stations must be higher to ensure full coverage. Especially in cities, where buildings create a large number of obstacles. Sometimes even line of sight might be required.

2 Architecture

2.1 Server Architecture

The MCS system consists of multiple virtual machines running on top of the VMWare ESXi hypervisor like we can see in the Figure 1.

MCS server is responsible for handling the session initiation with the session initiation protocol and Kamailio SIP server; floor control with Freeswitch server; providing identity management and authentication of users; doing DNS, or domain name system name resolution, where human readable names, like example.com are translated to IP addresses.

KMS server is responsible for providing and distributing the cryptographic keys necessary for the end to end encryption in communication channel to work.

CCT + SRS server is distributing and updating the client configuration, and controlling what client versions can connect to the MCS server

MAP server, MAP DB server and MAP services + AMD GW server together are forming a map-centric dispatcher solution, enabling clients to see other units' position on the map and allowing dispatchers and the tablet clients, so called field commanders to create, modify and delete tasks and incidents on the map, and attach or detach any units to the task.

Server analytics VM is providing statistics and ways to analyse the server usage, network usage, peak hours, locations and so forth.

MCS-TetraPol GW is a gateway providing interoperability between this MCS system, and TETRAPOL, a digital trunked radio network standard similar to TETRA.

Network services VM is providing DHCP, which is needed to assign IP addresses to the other servers.

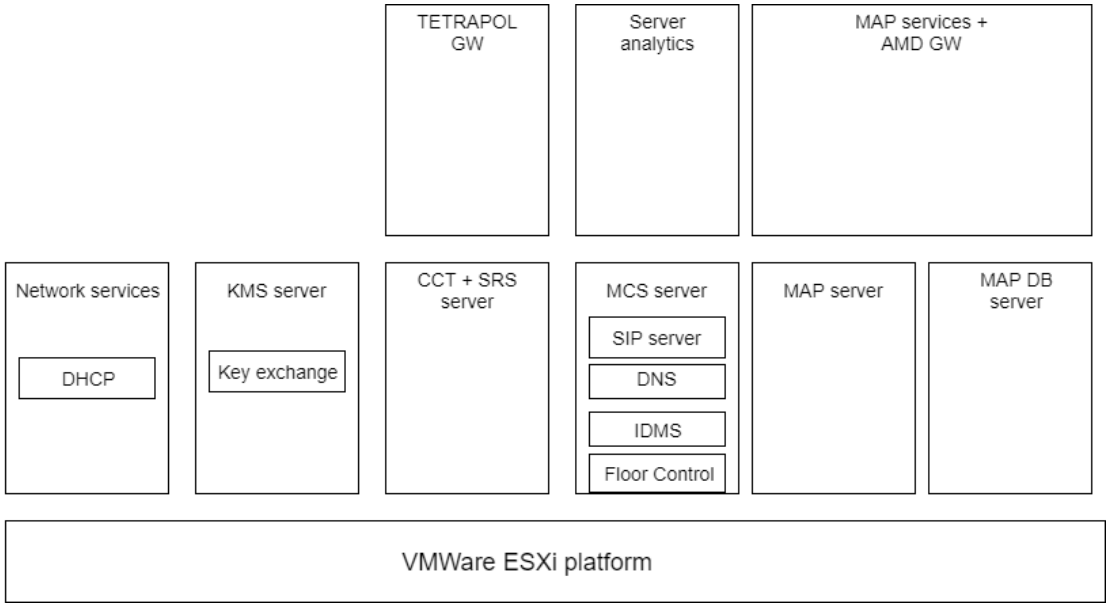

Figure 1. MCS system server architecture

The number of servers depend on customer needs and specifications, as each server in the architecture has a different role and provide different features onto the system.

The system is delivered with minimum of 2 servers, MCS and CCT + SRS servers. These servers are needed to provide the basic functionality of the system. Other servers are optional and can be tailored to the customer's needs

For example, if customer does not want map and location services in the system, virtual machines providing the map, named MAP VM and MAP DB VM in the infrastructure picture can be left undeployed. Or if customer does not need end to end encryption, KMS server could be left out.

2.2 Network Architecture

The MCS over LTE system network has two points of view where it can be observed. One is internal network inside the hypervisor platform, and one is external, how the physical server is connected to the end devices.

2.2.1 Internal Network

Internal network consists of three networks inside the virtualisation platform. One for internal communication between servers, one for operations and management of the system, and one for communications between clients and the system.

Internal network handles all the communications and signalling between the MCS servers, it has no outside connectivity because the exposing the network to networks outside the hosts could reveal crucial information on how the system works, what authentication messages etc. are being sent, and impose the system to additional cybersecurity risks.

Operation and management network is for configuration and operation of the system. It must be available to operators, so it must be reachable from external networks, but usually only locally and not over internet. Usually it is connected to one of the physical NICs, or network interface cards available on the host. However, in demo setup there might be limited ethernet connections available, or other reasons why you would not connect the operation and management network to a physical NIC. In that case, it is possible to use remote desktop tools over the management network of ESXi, we just need to install an additional (Windows or Linux) desktop VM to be able to do the management or operation related tasks on the system.

Communication network is a connection between the clients and the MCS system. Naturally, it must be connected to an external network, usually internet or internet service provider's 4G network to reach the clients. Communication network is the most secure network because it is subjected to all threats coming from the external networks. For example, it uses TLS, or transport layer security to ensure all the communication is encrypted and cannot be read by anyone sniffing the packets.

Figure 2 below describes the architecture and logical topology of internal networks of the MCS system. Note that the figure omits the host server running the hypervisor and its network. Only sign of the host server is on the right corner of the figure, which illustrates

what vSwitches are connected to the host's physical NICs or network interface card.

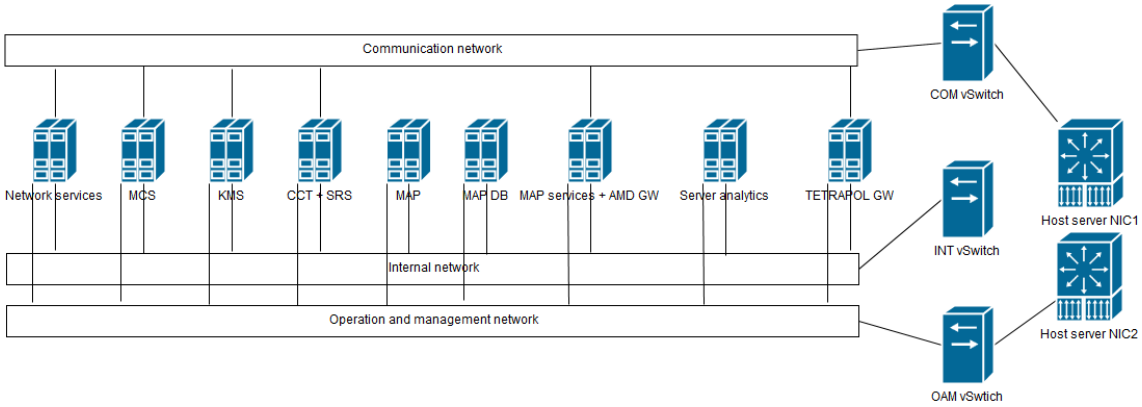

Figure 2. MCS system internal network architecture

vSwitch is a VMware virtualised switch that provides network connectivity to virtual machines. It can connect a portgroup, like INT, OAM and COM networks, to a physical NIC, or just enable network traffic between VMs within a portgroup.

Different networks use different VLAN, or virtual local area network tags. These tags are just arbitrary numbers ranging from 1 to 4095. VLAN numbers 0 and 4096 are reserved. In VMware ESXi, adding the VLAN tagging to packets can be done on the portgroup, VMware calls this external switch tagging (EST), or on the vSwitch itself, as a virtual switch tagging (VST). When the tagging is done on portgroup, the vSwitch port connected to the portgroup is running essentially on a trunk mode. When the tagging is done on the vSwitch, the same port now runs on an access mode.

Observing Figure 2 above, note that all the servers or network elements do not have to be connected to all networks, and even the topology described in Figure 2 can vary. Connection to communications network from network services VM is optional. Network services is providing IP addresses to servers with DHCP, and name resolution with DNS. Depending on the configuration of the external network where the communication network is connected to, it might be useful to have DHCP and DNS available from the MCS system. It is mandatory if the external network does not have a DNS service of its own. Due to how the MCS servers are configured, the servers can only be accessed by using DNS names.

2.2.2 External Network

External network topology is describing the connection from the host server, or server to the clients over a network whether it is internet or air gapped network. It consists of a management network for VMware ESXi, and connections to outside networks for communication and operations and management networks.

The topology in the Figure 3 is an example of system deployment which is deployed on-premises, and the connection to client devices is going over public internet. There are other deployment options as well, those are discussed more in chapter 3.

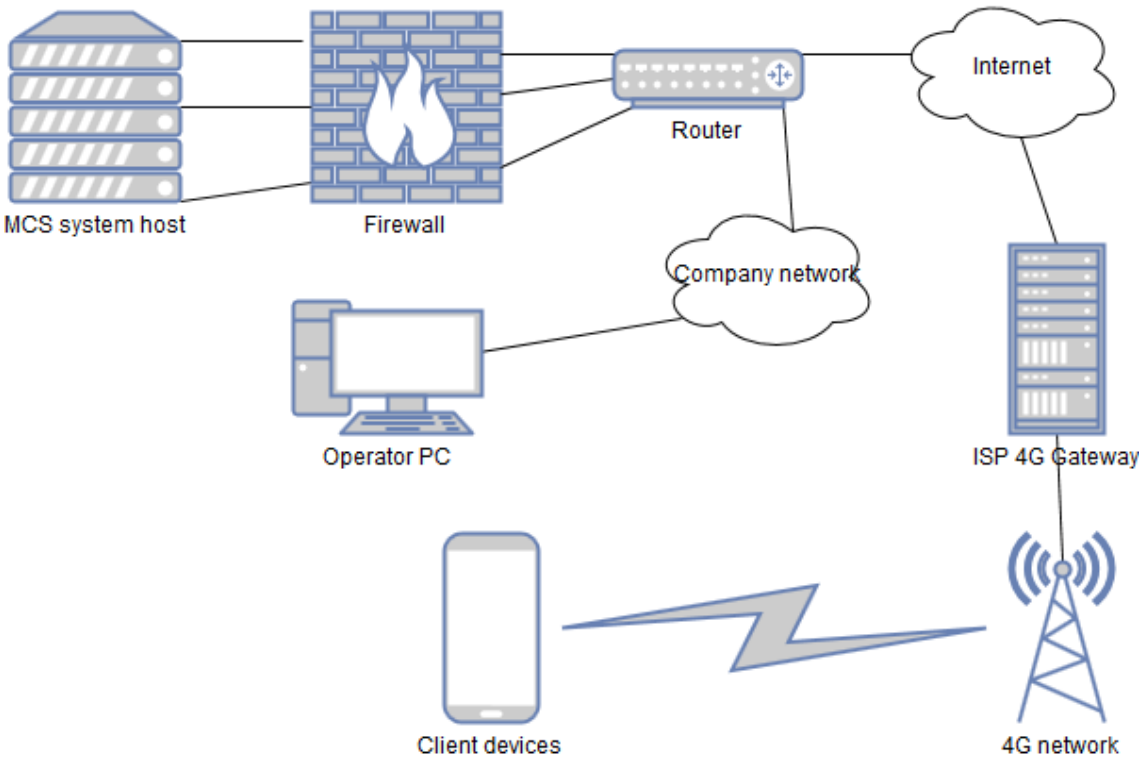

Figure 3. MCS system external network architecture

The MCS system host would need 3 or 4 physical connections in our scenario, depending on the hardware configuration, where communication and operation and management networks are connected to an external network. In addition to the two networks needed for the system operation, we also need a third network connected to an external network, which is for the management of the ESXi system. Without this network we cannot install any virtual machines to the host, as VMware ESXi does not offer local GUI, or

graphical user interface to allow installation and configuration of virtual machines. The fourth network is optional and hardware dependent. As we are using HP ProLiant Gen9 server as a physical host, it is possible to connect the host's iLO, or Integrated Lights-Out to the external network as well.

Hewlett Packard's integrated iLO management system makes it possible to connect and manage the system like you would have local access to the system over the network. It even works when the host server is shut down because the iLO system stays energized.

2.3 Transport Security

In traditional TETRA-networks the communication and signalling channels are using their own specific encoding on the air interface, so it cannot be deciphered without specific tools. However, the tools are available, so optionally it is possible to enable ciphering in the air interface, which encrypts the traffic in transit from the device to a base station. Additionally, there is a possibility to use end to end encryption with TETRA equipment. End-to-end encryption requires additional key distribution servers, but air interface encryption is available without any additional components to the network, the TEA, or Tetra Encryption Algorithms are built into the end devices and base stations.

The MCS system has end to encryption enabled by default. As described in chapter 2.1, key management system server is an integral part of the system, which takes care of distributing the cryptographic keys to end devices.

These keys enable the use of asymmetric TLS encryption of the authentication and signalling/ session control channels like described in Figure 4. Also, the map data is encrypted using TLS.

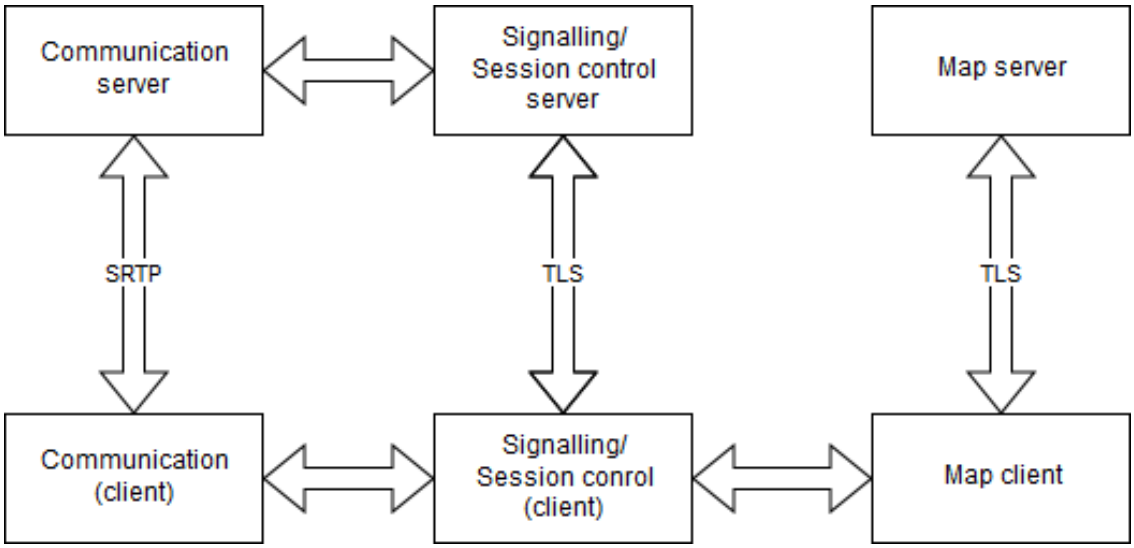

Figure 4. MCS system transport security

Communication channel is using SRTP, or secure real time protocol, a version of RTP, or real time protocol, which also uses asymmetric AES, advanced encryption standard cipher.

Note in figure 4, there is no encryption in communications between different servers on the MCS system, or between different processes of the client application. Client application is not a problem because it is a monolithic package, but the servers might pose a security risks depending on how the hardware is deployed.

3 Hardware Deployment Options

The MCS System can be deployed with few different configurations. When making the choice between the deployment options, there are multiple factors that must be considered. These factors include the investment to hardware and maintenance, room for the hardware, redundancy and resiliency needs, cost of using public cloud compared to own hardware, and cybersecurity considerations, which might include legal requirements if the system is used in public safety.

3.1 On-premises

Maybe the simplest deployment option to implement is on-premises. In on-premises deployment, the hardware is usually physically, like is visible in Figure 5, on the same location as the operators, or at least on the same network.

On-premises deployment can be single node, just one physical host server or cluster of servers. But on this example of on-premises deployment, the deployment is single node, and the cluster is left for the private cloud.

Benefits of on-premises single node deployment is that it is easy to implement, relatively secure, not so expensive hardware costs, and in most cases, it fills the requirements set by law about the processing of sensitive data.

The negatives are that the maintenance and the updating of the hardware must be done internally, and the hardware is a long-term investment, so it is unjustified if the system is going to be used for just a short amount of time or if the capacity needs fluctuates greatly. Also, with only single node, there is no resiliency or redundancy.

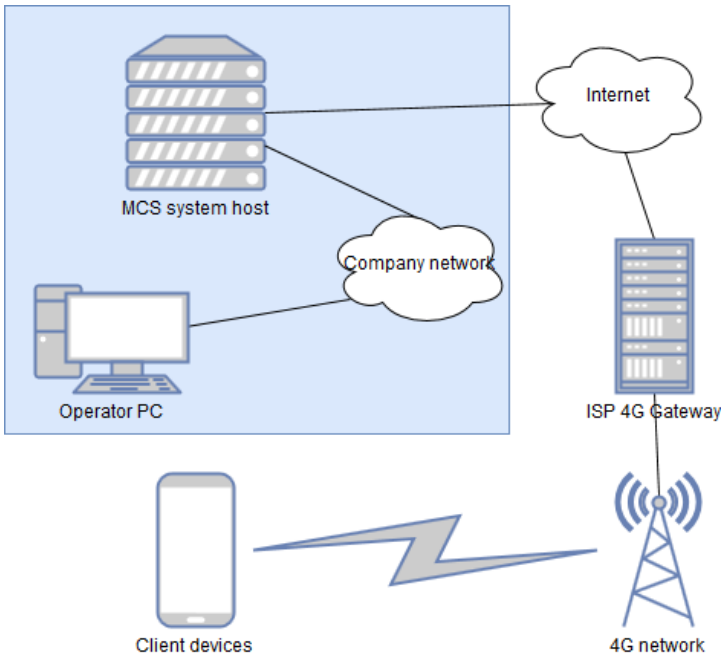

Figure 5. On-premises deployment of the MCS system.

3.2 Private Cloud

Cloud is a loosely defined term, but with private cloud in this case means a cluster of hosts in a company data centre or data centres like described in Figure 6. These data centres are usually on the same network as the operators, or even in the same physical location. Data centres could be connected over the internet as well, but that would lose some of the advantages of this kind of deployment. Mainly, the additional security of operators being in the same network than the MCS over LTE system. Private cloud, or server clusters add redundancy and resiliency to the system. The virtualisation platform allows other hosts to run same instances on hot standby, cold standby, or sharing the load between the hosts.

Disadvantages of such a deployment are mainly the same as in on-premises deployment. The high investment cost of the hardware, the space required, all the updates and upgrades of the hardware must be done internally, and the solution does not scale very well if the demands or requirements change suddenly.

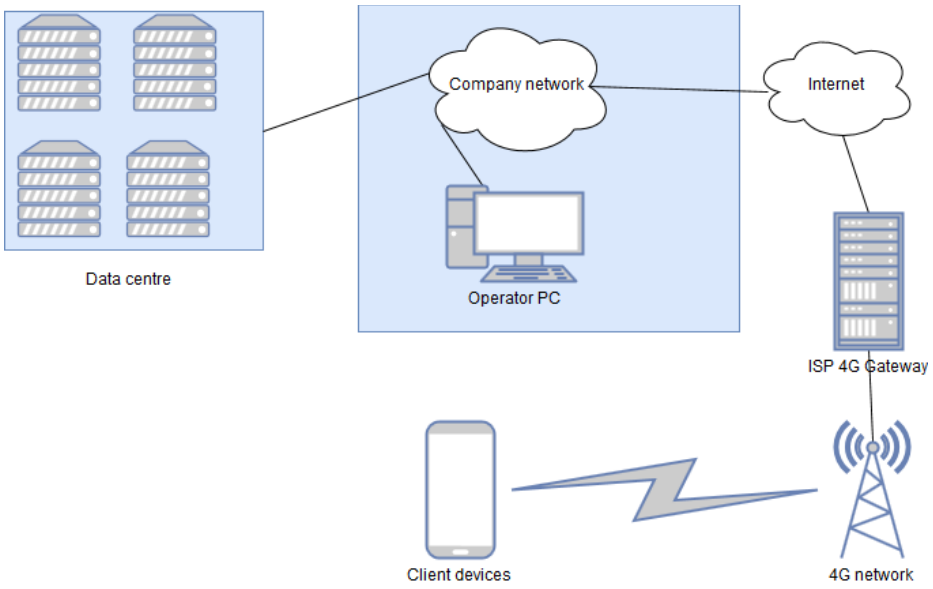

Figure 6. Private cloud deployment of the MCS system

3.3 Public Cloud

Public cloud is essentially the same as a private cloud, but over the internet, and most often it is offered as a IaaS- or Infrastructure as a Service-model, where the company providing the public cloud is providing the infrastructure, that is the hardware, underlying virtualisation platform and the network, the user's task is just to install the guest operating system. Examples of such systems are AWS, or Amazon Web Services, or Microsoft Azure.

In IaaS public cloud costs related to hardware are transferred to the cloud provider. Of course, there is periodical cost involved with subscription of such services, but it will give more flexibility with the demand when hardware reservations can be modified on the fly. Also, the cloud provider takes the responsibility of managing and updating the hardware, so workload is not as high as with the previous two options.

Disadvantage of the public cloud is, as the name implies, that it transverses the internet and usually you have no control over where your data is physically located. It can be in a host that also hosts other unrelated virtual machines and their data. Also, some jurisdictions do not allow the use of public clouds in public safety, for the reasons mentioned before.

[13] but these are more expensive solutions, making sure that there are no other tenants in the same hosts, or even steeper approach to security, AWS has their own data centre for US government to host their cloud. The last approach is more like a private cloud approach. Despite these different options, at least public safety sector in Europe is not very interested with the public cloud deployment of anything related to their data.

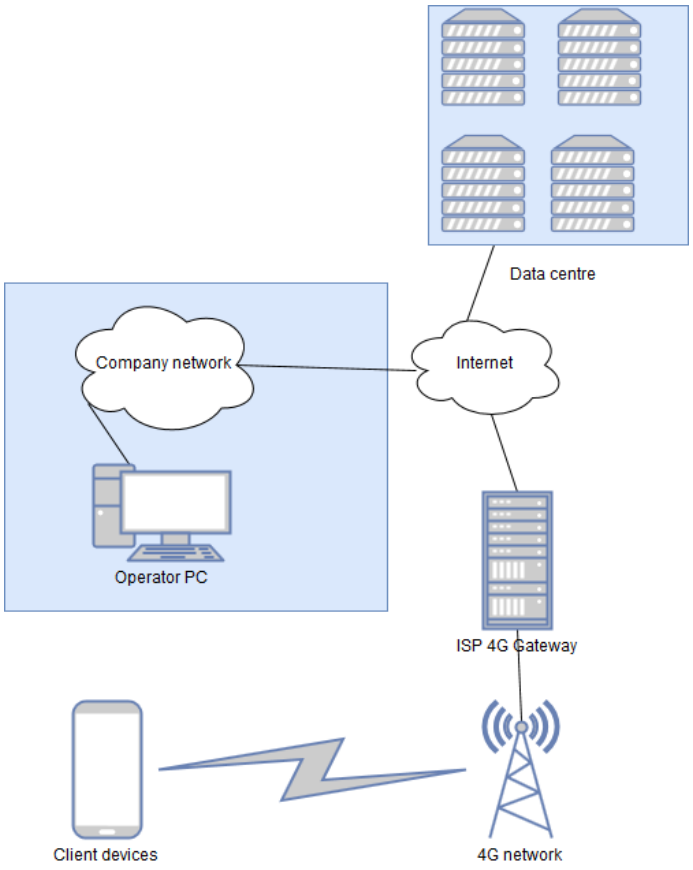

Figure 7. Public cloud deployment of the MCS system

4 Installation

The MCS over LTE system is installed on top of the hypervisor, as the servers are installed as virtual machines. Servers as a physical hardware is not really an option, as we need to be able to define the media access control, or MAC addresses manually, and with physical hardware it is very hard or impossible to do that. Benefits of virtual machines are also the space savings and the fore mentioned deployment options, which virtual machines enable.

4.1 Installation VMWare ESXi Hypervisor

Installation of VMWare ESXi 6.5 hypervisor and configuring it to a physical server is relatively easy, but a little time-consuming task that must be done for every physical host

To start the installation, insert the boot media onto the server, and boot from it. In the case of this thesis, the media is a bootable USB stick

After booting from the selected media, you are greeted with the ESXi 6.5 installation program as shown in Figure 8.

Figure 8. ESXi 6.5 installation program

The installation program guides the installation through step by step, where the target disk, keyboard layout and other options are selected.

After installation prompt appears that tells that the system must be rebooted reboot as shown in Figure 9. Installation media must be removed before rebooting.

Figure 9. ESXi 6.5 installation completed

After rebooting the server, the server still needs to be accessed the server locally or through iLO, as the management network address has not been set up. From the initial DCUI menu shown in Figure 10, F2 is pressed to access the system customization menu and configure the system. DCUI Stands for Direct Console User Interface [3], and it is used for configuring the ESXi system locally and accessing the local shell of ESXi system.

Figure 10. Initial DCUI menu after startup

From system customization menu the IP and interface settings of the management network are changed as required, as seen in Figure 11.

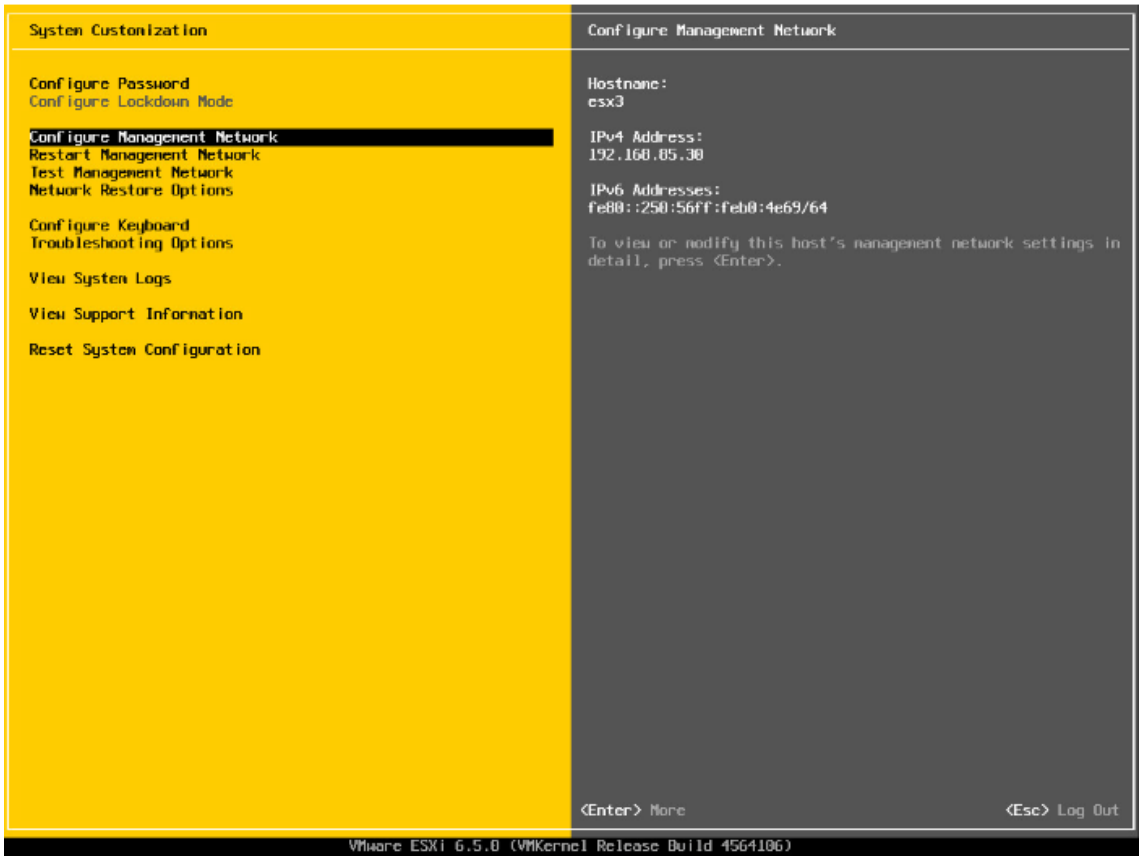

Figure 11. System Customization menu

After these steps, the system is initially configured in such a way, that it is possible to begin the installation of virtual machines and network elements. The system is now accessible through the ESXi web GUI, or graphical user interface on the IP address that was defined earlier.

4.2 Installation of Servers

After installing the ESXi hypervisor in the state that it is possible to access the web GUI, the installation of virtual machines can begin.

A web browser is required to navigate to the ESXi hosts IP-address. You are greeted with login dialog, like shown in Figure 12. By default, just the root account is created, so *root* is entered as a username, and password that was defined during the ESXi installation process.

Figure 12. ESXi web GUI login page

Once logged in, on the “Host” page, visible on Figure 13, “Actions” is selected on the top right-hand corner and options “Enable secure shell (SSH)” and “Enable console shell” clicked, like shown in Figure 14. Console shell is not strictly required, but it helps if something goes wrong, and physical connection is needed to take into the host.

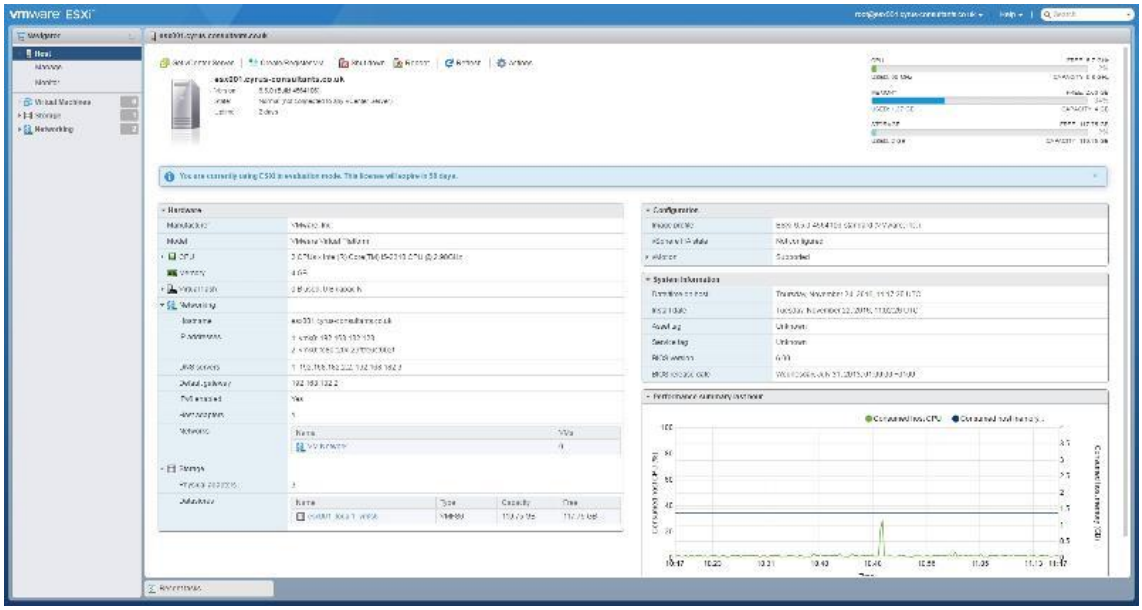

Figure 13. ESXi web GUI host page

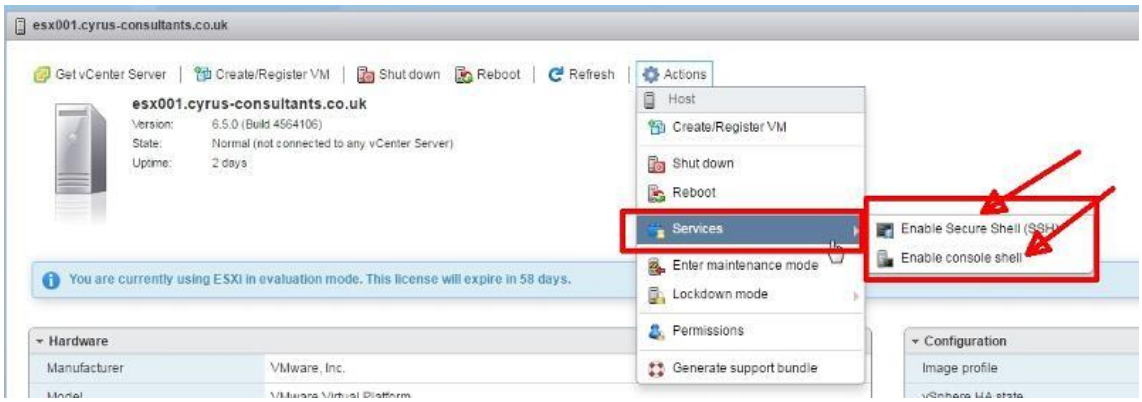

Figure 14. Enabling console access locally and remotely over SSH on a host.

After enabling the console access, connection with SSH to the same management IP-address where the ESXi web GUI is running is possible.

The MCS system virtual machines comes with a pre-installed hard drives as a .vmdk files, as well as with an installation media as an .iso file. These files must be transferred to the host machine using Secure File Transfer Protocol, or SFTP, which uses the same port and technology than SSH to secure the files in transit.

After transferring the files to the host, the .vmdk files must be set as thin provisioned with ESXi command line utility called *vmkfstools*. Open a SSH connection to the host, and navigate to the datastore folder, where the hard disk files and the disc image were uploaded. Hard disks are made thin provisioned with vmkfstools, by entering command

```
vmkfstools -i /vmfs/volumes/datastore1/hdd_file_name.vmdk  -d thin
hdd_file_name.vmdk
```

This operation is to be done for all the .vmdk files, and it might take a while to complete.

After changing the hard disk files thin provisioned, virtual machine is created normally, by opening a New Virtual Machine dialog, shown in Figure 15.

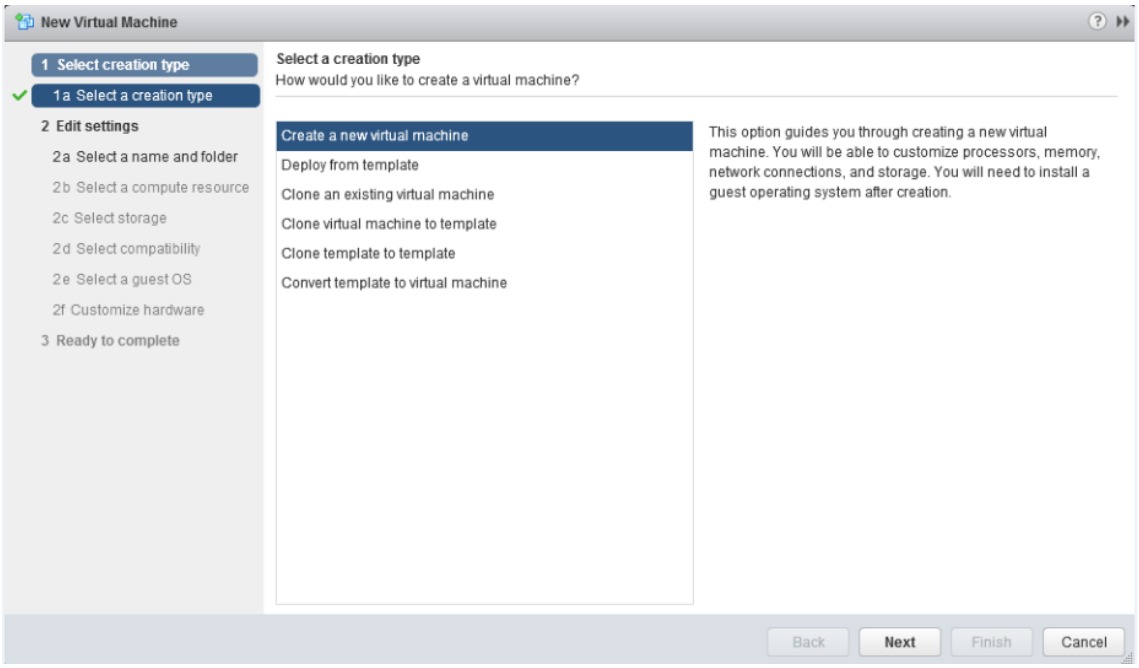

Figure 15. New Virtual Machine dialog

Virtual machine name is entered, and a folder or a Datacenter where the virtual machine is deployed, shown in Figure 16. On the next page, host server where the virtual machine is deployed is selected, shown in Figure 17. With single node installations there is only one option.

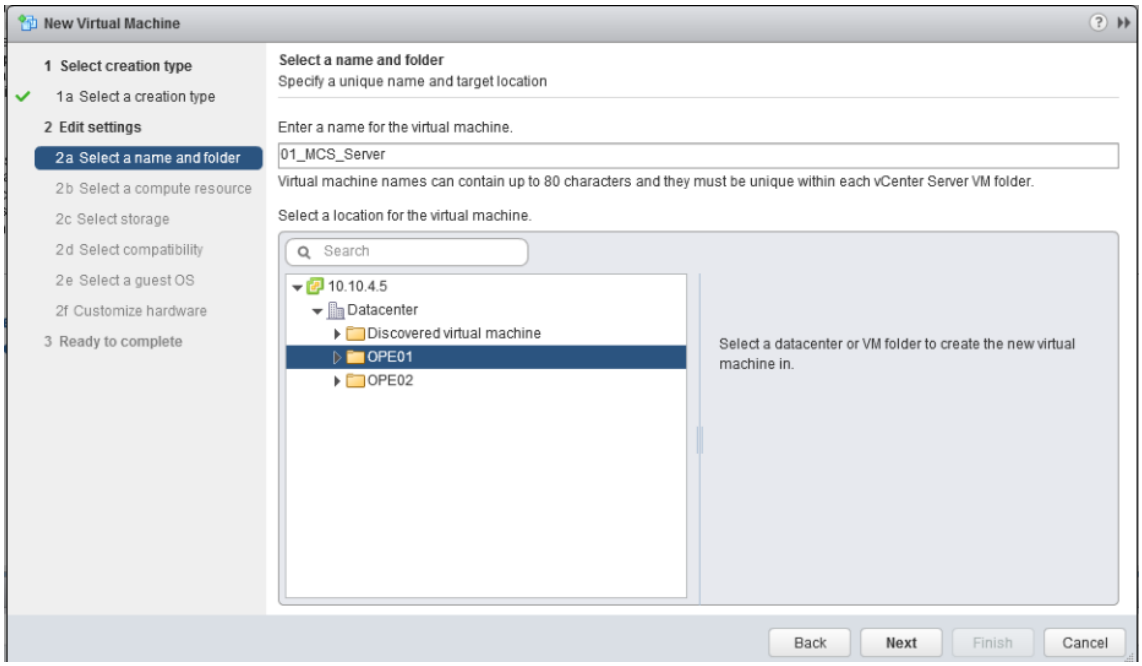

Figure 16. Virtual machine name and folder selection

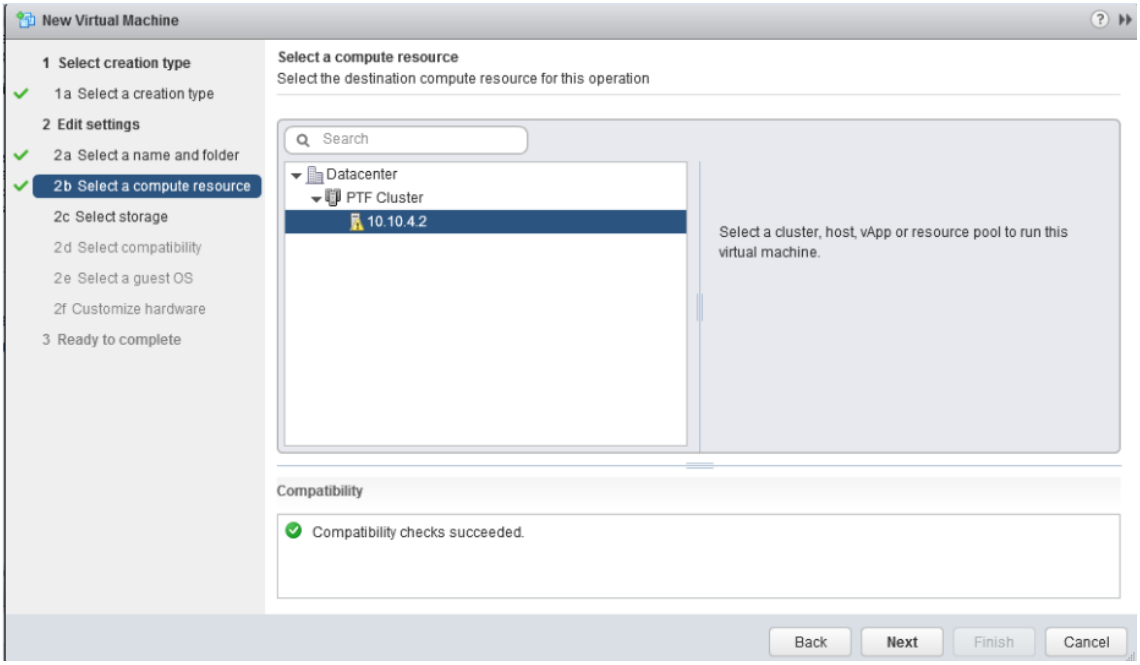

Figure 17. Virtual machine host selection

The datastore where to store the hard disks and configuration files is selected, shown in Figure 18. After this the compatibility settings are selected. On the Figure 19, the compatibility setting is set to ESXi 5.5, but must be set to the lowest ESXi version on the cluster. In an ideal situation the ESXi versions are the same across all the hosts, so this setting could be set to 6.5.

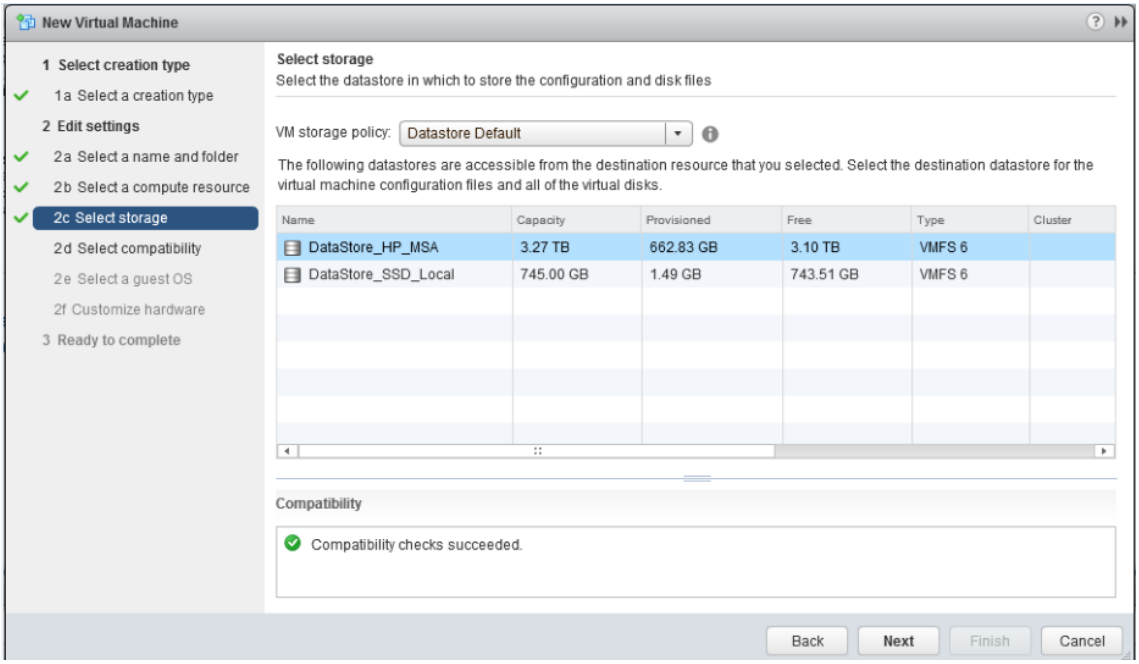

Figure 18. Datastore selection

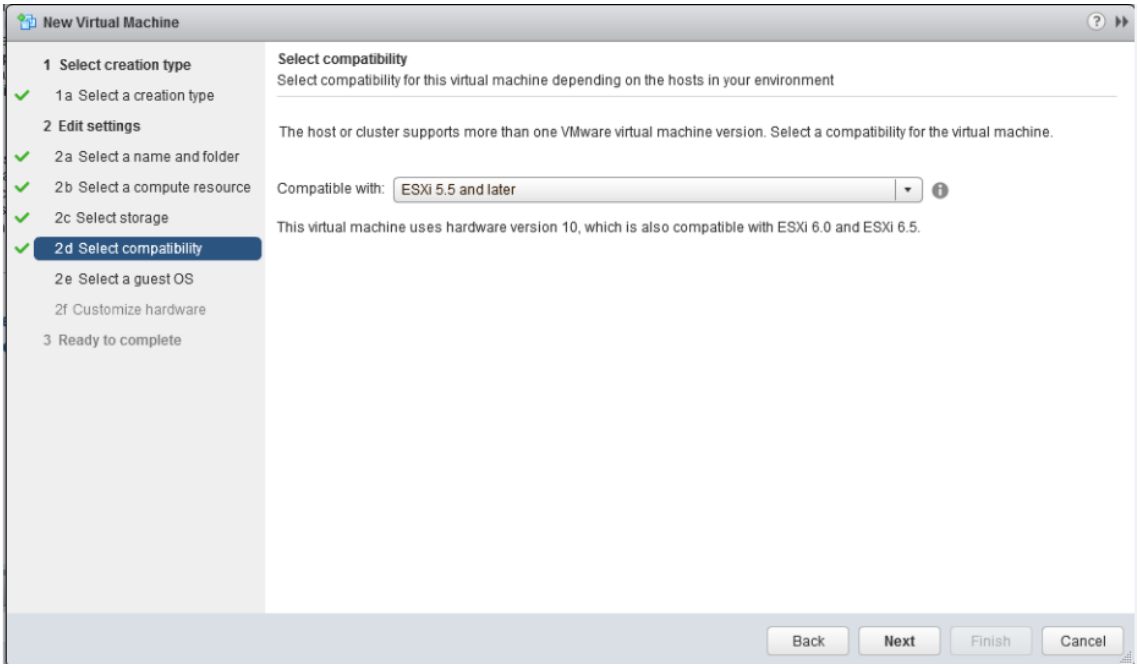

Figure 19. ESXi compatibility setting

Next the operating system type and version are selected, this is just information for the ESXi hypervisor, and will not install an operating system, or affect already installed operating system.

The virtualised hardware is set according to the specifications on the next page. MAC address of the network cards is set manually, so that DHCP can provide right IP addresses accordingly to the servers.

the configuration is confirmed on the next page. Often there are bugs on the ESXi web GUI, and these settings are not the ones required, but these issues can be fixed on the next step, as the virtual machines must be edited again.

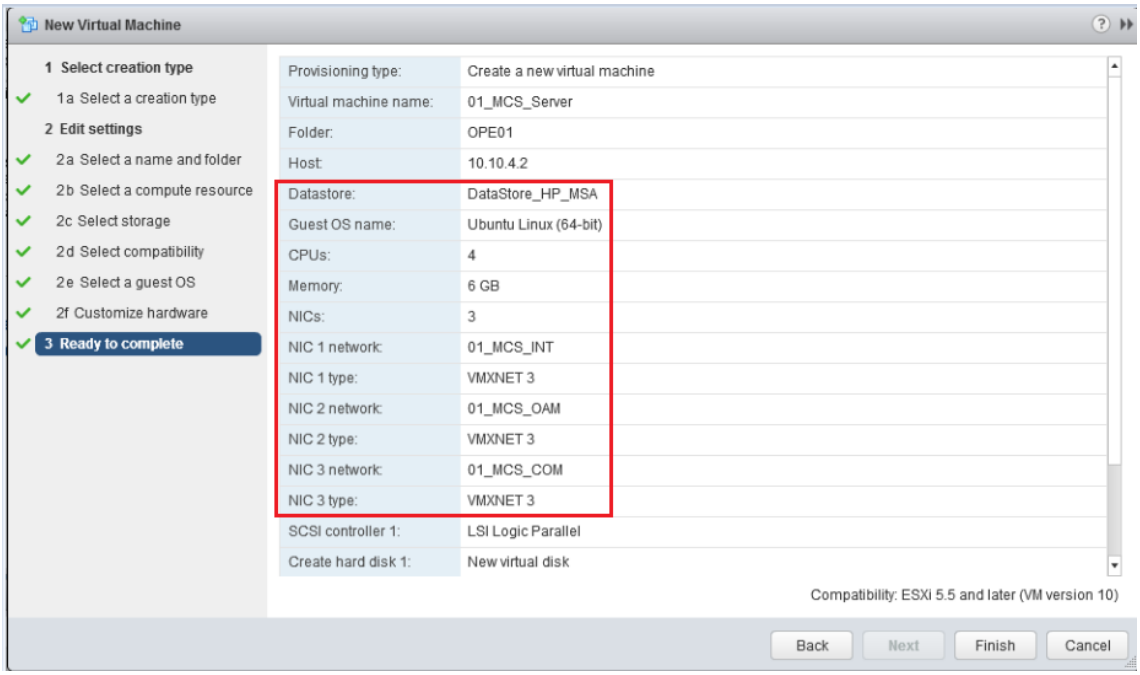

Figure 20. Confirm virtual machine settings

New Virtual Machine setup is completed by clicking “Finish”.

After finishing the setup, virtual machine settings are opened by clicking the virtual machine with the mouse’s secondary button and selecting “Edit Settings…” from the context menu.

Datastore ISO File option is selected for CD/DVD and .iso file is selected by navigating to the datastore folder where the .iso file was uploaded. Existing Hard Disk option is selected from New Device dropdown menu and this is repeated until all the uploaded hard disk files are added as hard disks to the virtual machine.

The virtual machine can be started now, and the installation process will begin. During the installation, it must be ensured, that the VM gets an IP address from DHCP. Otherwise installation cannot continue.

After installation the system can be configured using operation and management network.

4.3 Demo Setup

For demonstrations of the system around the world in various expositions, a portable MCS system is used. This system is running on a laptop, unlike ESXi, which is a type 1 hypervisor, the system is virtualised using VMWare Workstation, a type 2 hypervisor software. This gives the possibility to run a small MCS system on the laptop and run presentations among other things at the same time. Wireless local area network, or WLAN is used to establish the connection between servers and clients.

5 Testing And Conclusions

After commissioning the system was tested for about a month. First by the author and then by the customer. Testing done by the author was not especially extensive, and customer did their testing in secrecy. The customer was mainly interested to determine if the audio quality is better with this MCS over LTE system, than their existing similar MCS system. Also, the quality of cellular service from certain operators was evaluated. Testing included possible use cases for real-time video, data and location services, but these features were not the focus of the tests.

Reliability of LTE network was good, as was expected. Video and audio were delivered clearly over the network, and the system worked as expected. No issues were reported by the customer. In the light of this, it can be said that the tests were a success.

However, customer did not provide enough feedback from the pilot to make any conclusions about the pilot, whether it was a success or not. Being a commercial product, one

of the main goals was to make customer aware of the product and raise interest of buying it.

References

[1] W. Kenton, “Mission Critical,” Investopedia, [Online]. Available: http://www.investopedia.com/terms/m/mission-critical.asp. [Accessed 22 April 2019].

[2] “Terrestrial Trunked Radio,” [Online]. Available: http://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio. [Accessed 22 April 2019].

[3] M. Rouse, “DHCP (Dynamic Host Configuration Protocol),” TechTarget, [Online]. Available: https://searchnetworking.techtarget.com/definition/DHCP. [Accessed 23 April 2019].

[4] Information Sciences Institute, University of Southern California, “DOD standard internet protocol,” January 1980. [Online]. Available: https://tools.ietf.org/html/rfc760. [Accessed 24 April 2019].

[5] M. Rouse, “network interface card (NIC),” TechTarget, [Online]. Available: https://searchnetworking.techtarget.com/definition/network-interface-card. [Accessed 24 April 2019].

[6] C. Gonyea, “DNS: Why It’s Important and How It Works,” Oracle, 9 August 2018. [Online]. Available: https://dyn.com/blog/dns-why-its-important-how-it-works/. [Accessed 24 April 2019].

[7] Computer Hope, “GUI,” Computer Hope, [Online]. Available: https://www.computerhope.com/jargon/g/gui.htm. [Accessed 24 April 2019].

[8] “HPE Integrated Lights Out iLO,” Hewlett Packard Enterprise, [Online]. Available: https://www.hpe.com/emea_middle_east/en/servers/integrated-lights-out-ilo.html#overview. [Accessed 24 April 2019].

[9] National Institute of Standards and Technology, “Announcing the ADVANCED ENCRYPTION STANDARD (AES),” 26 November 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. [Accessed 24 April 2019].

[10] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” Internet Engineering Task Force, July 2003. [Online]. Available: https://tools.ietf.org/html/rfc3550. [Accessed 24 April 2019].

[11] VMWare, “Use the Direct Console User Interface (DCUI) to Enable Access to the ESXi Shell,” VMWare, [Online]. Available: https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.security.doc/GUID-94F0C54F-05E3-4E16-8027-0280B9ED1009.html. [Accessed 24 April 2019].

[12] M. Baugher, D. McGrew, N. Naslund, E. Carrara and K. Norrman, “The Secure Real-time Transport Protocol (SRTP),” Internet Engineering Task Force, March 2004. [Online]. Available: https://tools.ietf.org/html/rfc3711. [Accessed 24 April 2019].

[13] J. Ambrozy, “Great momentum for mission-critical LTE,” Nokia, 28 November 2016. [Online]. Available: https://www.nokia.com/blog/great-momentum-mission-critical-lte/. [Accessed 25 April 2019].

[14] P. Laakso-Kuivalainen, “What does "TETRA over LTE" mean?,” Airbus, 23 October 2018. [Online]. Available: https://www.securelandcommunications.com/blog/pmr-future-what-does-tetra-over-lte-mean. [Accessed 30 April 2019].

[15] Amazon Web Services, “AWS Global Infrastructure,” Amazon Web Services, [Online]. Available: https://aws.amazon.com/about-aws/global-infrastructure/. [Accessed 21 4 2019].