HO
GENT

Faculteit Bedrijf en Organisatie

The migration process and advantages of Windows Server 2019

Jens Du Four

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Ludwig Stroobant
Co-promotor:
Glenn Verschuere

Instelling: delaware

Academiejaar: 2018-2019

Tweede examenperiode

Faculty of Business and Information Management

The migration process and advantages of Windows Server 2019

Jens Du Four

Thesis submitted in partial fulfilment of the requirements for the degree of professional bachelor of applied computer science

Promotor:
Ludwig Stroobant
Co-promotor:
Glenn Verschuere

Institution: delaware

Academic year: 2018-2019

Second examination period

Preface

Throughout the following pages, I will research the question: 'What are the advantages and disadvantages of a migration from Windows Server 2016 to Windows Server 2019 in a business environment?'. This bachelor's thesis was written in the context of my graduation at the University College Ghent where I studied Applied Computer Sciences and by order of delaware, where I researched and wrote my bachelor's thesis from February 2019 till June 2019.

In consultation with my promoter, Ludwig Stroobant, and my co-promoter, Glenn Verschuere, the research question was formulated as the basis. For the duration of this assignment, they were always there to answer the questions I had regarding the research. In addition, I would like to thank Kasper Heyndrickx. His technical knowledge of SAP was of immense importance for this bachelor's thesis.

I would like to thank them. Without them, this would not have been possible. Furthermore, I would like to give a special thanks to delaware and especially to Tomas Castro and Jonas Decoster. Without their effort, I would never have had the opportunity to do this research from their branch in Harbin, China. I would also like to thank Henry Hao and Cici Chen for their hospitality and guidance during my stay. It was an experience I will never forget and always be grateful for.

Finally, I would like to thank my parents. Their wisdom and motivating words have helped me to bring this bachelor's thesis to a successful conclusion.
I wish you a lot of reading pleasure.

Jens Du Four

Ghent, 31/05/2019

Samenvatting

Uit een studie is gebleken dat in 2016, 17.9% en 45.4% van de servers, in het Spiceworks-netwerk, respectievelijk Windows Server 2003 en Windows Server 2008 gebruikten. (Tsai, 2016) Deze worden niet langer ondersteund door Microsoft en de uitgebreide ondersteuning voor de laatste loopt ten einde in januari 2020. Dit betekent dat een grootschalige update naar een nieuwere versie een vereiste wordt voor een aanzienlijk aantal organisaties. In deze bachelorproef zijn de voor- en nadelen van een migratie naar Windows Server 2019 onderzocht. Er is rekening gehouden met de vier hoofdthema's waarin de nieuwe functies zijn onderverdeeld. De migratie tussen de twee versies wordt vervolgens uitgevoerd aan de hand van een in-place upgrade en een side-by-side migratie, beiden met Windows Server 2016 als startpunt. Hieruit bleek dat, hoewel een in-place upgrade in een eerste opzicht de eenvoudigste methode is, dit niet altijd de beste is. De voordelen van een side-by-side migratie, op vlak van veiligheid en performantie, verantwoorden op lange termijn de additionele inspanning die hiermee gemoeid is. Aangezien dit OS de basis vormt voor vele applicaties, is ook een migratie van een SAP-omgeving uitgevoerd. De SAP Kernel heeft reeds ondersteuning voor Windows Server 2019. Een migratie van de gangbare softwareproducten die SAP aanbiedt, is dus mogelijk. Dit vereist echter bijkomend onderzoek, zoals beschreven in deze bachelorproef. Opvallend is dat voor de migratie van andere softwarepakketten eveneens aanvullend onderzoek moet worden verricht. Dit om, net als bij Windows Server 2019 en SAP, ervoor te zorgen dat alles voldoet aan de kwaliteitseisen die een organisatie stelt. Hierna werden de verscheidene beschikbare base container images geanalyseerd. Door een verschil in grote en performantie ging de keuze naar de meest recente versie. Dit door de additionele functies, die doorheen deze bachelorproef besproken worden, en de toevoeging van de nieuwe Windows base container image. Tot slot wordt er gekeken naar de toekomst van Windows Server. Voornamelijk naar het gebruik van de cloud en de nieuwe functionaliteiten die hiermee gepaard gaan in Windows Admin Center.

Abstract

A study showed that in 2016, 17.9% and 45.4% of servers, in the Spiceworks network, respectively used Windows Server 2003 and Windows Server 2008. (Tsai, 2016) These are no longer supported by Microsoft and the extended support for the latter runs until the end of January 2020. This means that a large-scale update to a newer version is becoming a requirement for many organizations. In this bachelor's thesis, the advantages and disadvantages of migrating to Windows Server 2019, are investigated. The four main themes, in which the new features of Windows Server 2019 are divided, were taken into consideration. The migration between both versions is then carried out according to the in-place upgrade and side-by-side migration method, both starting from Windows Server 2016. This showed that although an in-place upgrade is in first respect the simplest method, it is not always the best. The advantages of a side-by-side migration in terms of safety and long-term performance justify the additional effort involved. Since for many organizations this OS is the basis for their applications, a migration of a SAP environment is also performed. The SAP Kernel supports Windows Server 2019. A migration of all the trivial software solutions offered by SAP is possible. However, this requires additional research, as described in this bachelor's thesis. It is striking that for the migration of other software solutions supplementary research needs to be carried out, as well as additional and rigorous testing. This, like done in this bachelor's thesis for Windows Server 2019 and SAP, to ensure that everything meets the quality demands of an organization. After this, the different available base container images were analysed. This showed that because of a difference in size and performance, the choice went to the most recent version. This due to the additional functions, which are discussed during this bachelor's thesis and the addition of the new Windows base container image. Finally, a look is taken at the future of Windows Server. Especially at the usage of the cloud and the new functionalities that are paired with this in Windows Admin Center is taken.

Contents

List of Figures

List of Tables

Acronyms

AI Artificial Intelligence. 52

d.VMMQ Dynamic Virtual Machine Multi-Queue. 31
DC Domain Controller. 12, 14, 35, 36, 39, 40, 41, 42, 43, 65, 67, 68, 69
DTLS Datagram Transport Layer Security. 28

EOL End of Life. 15, 19, 20, 55

GRE Generic Routing Encapsulation. 31

HCI Hyper-Converged Infrastructure. 10, 11, 13, 25, 31, 32, 33, 32, 33, 53, 55, 58, 59
HGS Host Guardian Service. 29
HR Human Resources. 25

IPSec Internet Protocol Security. 31
IT Information Technology. 19, 24, 27, 30, 31, 33, 52, 57

LEDBAT Low Extra Delay Background Transport. 31
LTSC Long-Term Servicing Channel. 19, 44, 46

MD5 Message Digest Algorithm 5. 47

OS Operating System. 5, 7, 10, 19, 20, 21, 23, 27, 30, 33, 35, 37, 39, 41, 43, 44, 46, 47, 52, 53, 55, 57, 58, 63

PAM Product Availability Matrix. 13, 44, 45, 46

RDP Remote Desktop Protocol. 39, 40, 42
ROI Return on Investment. 27

RSC Receive Segment Coalescing. 31

S2D Storage Spaces Direct. 10, 32, 33, 53
SAC Semi-Annual Channel. 19, 30, 47
SCCM System Center Configuration Manager. 33
SDDC Software-Defined Data Centre. 32
SDK Software Development Kit. 52
SDN Software Defined Networking. 9, 10, 27, 28, 31, 32, 33, 53, 58
SDS Software-Defined Storage. 32
SHA-3 Secure Hash Algorithm 3. 47
SHA-2 Secure Hash Algorithm 2. 47
SLES SUSE Linux Enterprise Server. 29

TLS Transport Layer Security. 28

UI User Interface. 33, 50, 55

VHD Virtual Hard Disk. 46
VM Virtual Machine. 11, 12, 13, 14, 26, 28, 29, 30, 31, 36, 39, 41, 42, 43, 45, 46, 47, 63, 64, 71, 77, 79
VPN Virtual Private Network. 25
vRSS Virtual Receive Side Scaling. 31

WAC Windows Admin Center. 5, 7, 10, 11, 25, 26, 30, 31, 32, 33, 35, 39, 51, 53, 52, 55, 61, 62, 61
WDATP Windows Defender Advanced Threat Protection. 9, 13, 27, 58

1. Introduction

Windows Server is an Operating System (OS) that is widely used by organizations all over the world, some with only a handful of employees to corporations that have a couple of thousand at their disposal. To keep up in the fast-paced world that is Information Technology (IT), updates are a necessary part of the daily operation, though they do not always present themselves at a convenient time. Semi-Annual Channel (SAC) updates which can be scheduled to Long-Term Servicing Channel (LTSC) updates, that could require entire systems to be taken offline for an extended duration. Since IT has become a core business, this can bring tremendous damage to the business value of many of these organizations. Therefore, asking how this can be done as efficient and cost-effective as possible is important before considering a migration to the latest version.

1.1 Problem statement

Since the latest version of the Windows Server was released, Windows Server 2019, many organizations are willing to investigate a migration from previous versions of the OS in the nearby future. delaware, one of these organizations, wants to research how these migrations would take place starting from Windows Server 2016 and how they can be achieved in an efficient and cost-effective way.

Products Released	Life Cycle Start Date	Mainstream Support End Date	Extended Support End Date
Windows Server 2016 Standard	15/10/2016	11/01/2022	12/01/2027
Windows Server 2016 Datacenter	15/10/2016	11/01/2022	12/01/2027

Table 1.1: End of Life of Windows Server 2016
Adapted from Microsoft Corporation, n.d.

With the ending of mainstream support for Windows Server 2016 scheduled at the start of 2022, as seen in Table 1.1, it is best to research the migration to the latest version well in advance. Especially when considering that organizations running an End of Life (EOL) OS, are very common.
In an article written by Tsai (2016), the Spiceworks network showed that the market share of Windows Server 2003 was at 17.9% and Windows Server 2008 was at 45.4%. The official support for both versions has already ended. The extended support for the latter will be ending at the start of 2020.

Products Released	Life Cycle Start Date	Mainstream Support End Date	Extended Support End Date
Windows Server 2019 Essentials	13/11/2018	09/01/2024	09/01/2029
Windows Server 2019 Standard	13/11/2018	09/01/2024	09/01/2029
Windows Server 2019 Datacenter	13/11/2018	09/01/2024	09/01/2029

Table 1.2: End of Life of Windows Server 2019
Adapted from Microsoft Corporation, n.d.

Those deadlines combined with the EOL of Windows Server 2016, make a strong case to investigate the migration to the latest version, which can offer enhanced security and additional features. The life cycle of the latest version, Windows Server 2019, started in November 2018 and it will continue to receive mainstream support until January 2024. The extended support is guaranteed until January 2029, as seen in Table 1.2.
This makes it a viable successor for the OS that makes up a large percent of the server infrastructure used in the world. This bachelor's thesis attempts to show that the benefits that are paired with migrating will outweigh the disadvantages. The new features of the latest version can be divided into four key themes (Microsoft Windows Server Team, 2018):

- Hybrid cloud
- Security
- Application platform
- Hyper-converged infrastructure

Those four themes will be examined thoroughly in Chapter 2.

1.2 Research question

What are the advantages and disadvantages of a migration from Windows Server 2016 to Windows Server 2019 in a business environment?

1.2.1 Sub-research question

- What are the differences between the Windows, Server Core and Nano Server base container images of Windows Server 2019?
- Can SAP be migrated from an existing Windows Server 2016 to Windows Server 2019 in a business environment?

- How can the new features of Windows Server 2019 be leveraged in the migrated infrastructure?

1.3 Research objective

The expected result of this bachelor's thesis is to demonstrate the advantages of utilizing Windows Server 2019 over Windows Server 2016, proving that migration is a long-term investment towards the future for any organization. It will also compare the base container images of the OS and show that a migration of a SAP environment to Windows Server 2019 can be done. This because the requirements between the latest version of both the OS and the SAP Kernel have been met.

1.4 Structure of this bachelor's thesis

The remainder of this bachelor's thesis is structured as follows:

In Chapter 2, an overview is given of the state of the art within the research domain, based on a literature study.

In Chapter 3, a methodology is explained, and the research techniques used to formulate an answer to the research questions are discussed.

In Chapter 4, the further development of Windows Server over the years to come will be analysed.

In Chapter 5, finally, the conclusion is given, and an answer is formulated to the research questions. This will also provide an impetus for future research within this domain.

2. State of the art

In this chapter, the state of the art will be examined. As mentioned in the introduction, this part of the bachelor's thesis will be used to establish an in-depth understanding of the four key themes that incorporate the changes that were made in Windows Server 2019. First, a basic understanding of what those four key themes are will be established. Afterwards, their implementation in the latest version of the OS will be investigated.

2.1 Hybrid cloud

Hybrid cloud is a topic that has gained more momentum over the past years. For organizations, this makes it a consistent topic of interest and makes it a natural choice as one of the four keystone themes in Windows Server 2019. (Microsoft Windows Server Team, 2018) The hybrid cloud will be discussed as an essential part of the bachelor's thesis, as it also returns as a topic of interest in Chapter 4. It is especially beneficial to know the advantages that it offers to Windows Server 2019. How these new and improved features enhance workflow and how they can be leveraged by organizations, like delaware.
First, the different types of clouds will be discussed in the Subsection 2.1.1.

2.1.1 Types of cloud solutions

The National Institute of Standards and Technology differentiates four types of clouds (Mell & Grance, 2011):

- Private cloud

- Community cloud
- Public cloud
- Hybrid cloud

It is important to keep in mind that virtualization and cloud computing are two different, although similar, technologies. While virtualization detaches computing environments from their physical infrastructure through software, cloud computing is a service that delivers computing resources through a network whenever they are requested. (Naeem, Mahar, Memon, Siddique, & Rauf, 2016)

Private cloud

A private cloud is an environment in the cloud that is designated for use by a single organization. It can, however, consist of multiple clients provided those are in the same organization. It is only accessible inside a private internal network or over the internet for a selected number of users. Private clouds cannot be accessed by the public. They can also be known by other names such as internal or corporate cloud. Their main advantage is the higher level of security and privacy, which is offered through the usage of an in-house hosted infrastructure and additional company firewalls. The biggest disadvantage that comes with this added layer of security, is the responsibility that is given to the IT team that manages the infrastructure that supports the private cloud. This means that on top of the additional infrastructure costs, they require the same amount of man-hours that comes with the management of a traditional data centre. Keep in mind that in-house does not necessarily mean on-premise.
Still, the private cloud holds a great benefit compared to long-standing infrastructure possibilities. As reported by IBM, an organization saved more than $1.5 billion by reducing its number of data centres from 115 to 5. This was a direct result of the implementation of a private cloud. (Hofmann & Woods, 2010)

Community cloud

When several organizations collaborate to meet the requirements that are demanded of the IT infrastructure, they are operating under a community cloud. The management of this environment can be outsourced to a third-party organization that is operating inside the same community. The alternative is that the organization manages the infrastructure itself. This form of operation tackles one of the main disadvantages of a private cloud. It shares the costs over multiple organizations, thus greatly reducing it. Since they are operating inside the same community, they share the same concerns and will be subjected to the same requirements that can be imposed by a governing instance. However, these advantages over private clouds come at a cost. This reduction in cost because of sharing the infrastructure results in a devaluation of security. Meaning that it is a viable alternative to organizations with mitigated security concerns around the usage of a public cloud environment but are willing to make some sacrifices in favour of a cost reduction.
An example of this is described in an article by Yao et al. (2014). The research shows how small hospitals in China, not all of which can provide their own infrastructure, could utilize a community cloud. These grass-roots healthcare institutions, that all operate within

the same community, can share the cost and management of the community cloud. This to provide an attractive hospital information solution to improve their services without the extensive cost nor the need for additional security concerns regarding confidential information in patient files.

Public cloud

Amazon Web Services, Alibaba Cloud and Microsoft Azure are some examples of public cloud solutions. Most of these solutions are offered by corporations who manage and operate their data centres and provide access to their cloud via the internet. Thus, eliminating the cost that is associated with the management and responsibility of a private cloud and significantly reducing the cost in comparable use cases. Public clouds also provide the possibility for effortless scalability and flexibility in comparison with private clouds, where the required hardware for scaling needs to be available in-house. This makes the public cloud ideal for temporary solutions and fast-growing organizations.
S. Singh and Jangwal (2012) concluded, in a comparison between the cost and security of private and public clouds over three years, that although security can be a real concern in the usage of public cloud it should not be ruled out immediately without analysing the requirements of an organization, keeping in mind the major investment that comes with the usage and implementation of a private cloud. The different obstacles that come with securing a public cloud have also been addressed by Ren, Wang, and Wang (2012), in which there is a call for additional research about the subject to fully take advantage of the breakthrough that cloud computing is.

Hybrid cloud

A hybrid cloud aims to be the solution for every kind of organization. It combines a higher level of security and privacy that is offered by a private cloud solution with easy scalability and flexibility that comes paired with the public cloud. A hybrid cloud is an amalgamation of two, or more, of the previously mentioned types. This translates to a combination of private and public cloud solutions in most use cases. As described in the book by Sarna (2010), hybrid clouds enable large organizations to move their less sensitive information, like Human Resources (HR), to the cloud. Thanks to the advantages of hybrid cloud, their sensitive data such as classified information about customers or the organization can remain in-house on the private cloud or even on-premise for an additional layer of security. The connection between the public and private cloud of the hybrid cloud is generally accomplished through a secure connection, for example, Virtual Private Network (VPN).

2.1.2 Hybrid cloud in Windows Server 2019

As mentioned in Subsection 2.1.1, Microsoft offers a public cloud solution: Microsoft Azure. This can be combined with a private cloud of an organization or an on-premise environment to create a hybrid environment. Microsoft Azure is offered from more than fifty different global Azure regions all over the world. They are confident that clients who are running the latest version of Windows Server and the associated software, can have

a hybrid environment set-up almost instantly. This through the usage of a new feature that significantly simplifies the management of this environment. Nowadays this feature is known as Windows Admin Center (WAC). Before the release, it was known as Project Honolulu. Windows Admin Center was built with a hybrid environment and HCI in mind. This tool, built to manage Windows Server and Windows 10, is optimized for use within Windows Server 2019. It uses the Azure Network Adapter to establish a point-to-site connection between your server and your Azure virtual network. This constitutes an additional argument for a migration to the latest version. The entire step-by-step plan for Windows Admin Center Azure Integration is given in Appendix B. Once this has been completed, the following features can be leveraged through Windows Admin Center (Washburn, Rowland, Woolslayer, & Poggemeyer, 2018):

Azure Active Directory authentication provides access to Azure Active Directory which adds a layer of security and ease of management and scalability.

Manage Azure IaaS virtual machines manage on-premise VMs as well as Azure VMs.

Azure Site Recovery provides back-up and recovery services for business continuity and disaster recovery.

Azure Update Management an Azure Automation solution to manage updates and patches for on-premise, external hosted or Azure VMs.

Azure Network Adapter securely connect the local computer to Azure Virtual Network.

As will be discussed in Chapter 4, new features will be introduced several times a year to improve the overall experience with the Windows Admin Center.

2.2 Security

With more than 53.000 reported incidents and 2.216 confirmed data breaches, security has become an essential part of IT. (Mansfield-Devine, 2018) The importance of security directly translates into Windows Server 2019 through various parts of the OS that have been reviewed to make them more resilient and accessible. Additional features have also been added to further improve security. In the following section all the major elements will be discussed, distributed among three subsections:

- Windows Defender Advanced Threat Protection (WDATP)
- Security with Software Defined Networking (SDN)
- Shielded Virtual Machines (VM)

2.2.1 Windows Defender Advanced Threat Protection (WDATP)

In a research study done by Musto (2017), WDATP was scrutinized. Keep in mind that when the endpoint security solution is implemented in Windows Server 2019, it will require additional licensing. Still, the efficiency with which it tackles security problems resulted in a 53% Return on Investment (ROI). The research reported that WDATP reduced the risk of a breach by 40%. It even enabled them to identify threats faster and resolve them in a more efficient fashion. In conclusion, the replacement of previous solutions with WDATP reduced costs and made security teams more efficient. With the advent of Windows Server 2019, additional features have been added to WDATP to ensure the safety of organizations in the years to come. The different components of WDATP are described in Figure 2.1. These will not be individually reviewed here as this subject of endpoint security alone offers enough substance for another bachelor's thesis.

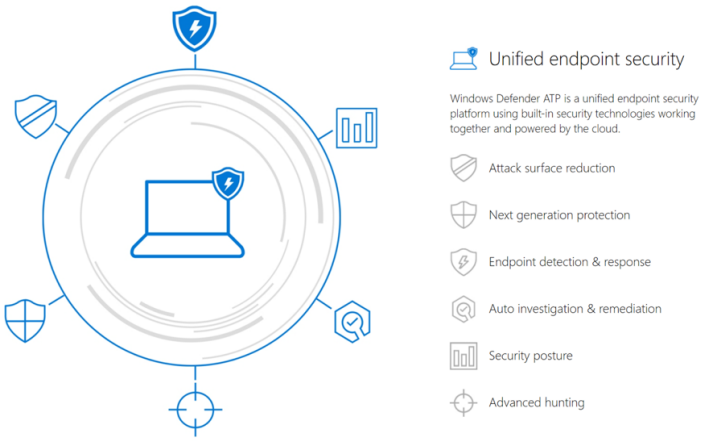


Figure 2.1: The different components of Windows Defender Advanced Threat Protection. (Aslaner, 2018)

2.2.2 Security with SDN

As described by Shin, Xu, Hong, and Gu (2016), SDN is a state-of-the-art technology that enables developers to design advanced networks effortlessly. According to Kreutz et al. (2015), SDN has paved the way for the next generation of networking. In Windows Server 2019 there have been new developments in this field. These can be boiled down to four features:

- Encrypted networks
- Firewall auditing
- Virtual network peering
- Egress metering

The discussion of these will be kept constrained.

Encrypted networks

Encrypted networks, or more specifically virtual encrypted networks, enable the encryption of network traffic between different VMs. This is achieved through the usage of Datagram Transport Layer Security (DTLS). DTLS was built as close to Transport Layer Security (TLS) as possible, which makes it ideal at securing connections. However, since the connections between VMs are delay sensitive, DTLS is preferred. (Modadugu & Rescorla, 2004)

Firewall auditing

One of the new features in Windows Server 2019 is SDN Firewall auditing. This means that the administrator can examine if every part of the Firewall is as secure as initially thought. When this feature is enabled, every data stream that gets processed by the SDN firewall gets recorded. The logs can be used in troubleshooting or archived for analysis. These can also be processed by tools such as Power BI.

Virtual network peering

Virtual network peering allows administrators to combine two individual virtual networks. A coherent connection is made that represents itself as an individual one. This means the connection between both networks can be routed through the infrastructure backbone. This in term means that there is no need for a public gateway, providing a more secure connection. All of this is done without accumulating downtime when peering the networks.

Egress metering

Egress metering for SDN enables an administrator to monitor the consumption of outgoing connections. Windows Server 2019 also makes a distinction between traffic that

leaves the virtual network and the data centre, in comparison to traffic that stays within the data centre.

2.2.3 Shielded Virtual Machines

Shielded VMs is a feature that was introduced with Windows Server 2016, aimed at securing Hyper-V VMs from tampering. The securing of the VM gets done through, for example: BitLocker encryption and Virtual Trusted Platform Modules. One of these features, Host Guardian Service (HGS), is also a requirement to run a Shielded VM. Since Windows Server 2019, it is possible to run Shielded VMs on machines with an irregular connection to the HGS. This can be done by leveraging the following two new features:

Fall-back HGS provide a redundant connection in case the primary HGS cannot be reached.

Offline Mode once a shielded VM has been set up, it can be started up seeing that the security configuration remains unchanged.

Another new feature is the addition of support for different flavours of Linux, like Ubuntu and SUSE Linux Enterprise Server (SLES) inside Shielded VMs.

2.3 Application platform

An application platform is an essential part of IT operations. It provides services to applications, so these can run fluently. A modern application platform is extensive, it provides an array of services to a variety of applications. According to a paper by Chappell (2011), there are five categories of services offered by an application platform:

- OS
- Execution services
- Data services
- Cloud services
- Development tool

These five categories are not necessary for every application but should be offered in a modern application platform nonetheless. There have been major improvements in this area with the arrival of Windows Server 2019. (Gerend, Poggemeyer, et al., 2018)
In the following subsections, these will be discussed and analysed.

Linux containers on Windows

Windows Server 2019 allows a system administrator or IT professional to run Linux and Windows container while utilizing the same Docker daemon. This is an important addition knowing that only 3.23% of all Apache servers run on Windows. (Security Space, 2019)

Building Support for Kubernetes

Kubernetes is a software solution designed to oversee containers. It is a management environment for network, computing and data infrastructure. With Windows Server 2019 this has been further developed inside the OS. For now, there has been a great improvement in container networking, but as new versions of Kubernetes are rolled out, additional features will be added with updates through Semi-Annual Channel (SAC) releases.

Container improvements

There is better support for Windows Authentication inside containers as well as improved application compatibility for the existing Server Core image. Containers have become more manageable thanks to their implementation in the Windows Admin Center. Other base container images have also been reduced in size and overall performance has been improved, which will be discussed in Chapter 3.

Encrypted Networks

This has been discussed in Subsection 2.2.2.

Network performance improvements for virtual workloads

Since Windows Server 2019, the throughput between VMs has been increased. This as a direct result of the three new features that have been introduced:

- Receive Segment Coalescing (RSC)
- Dynamic Virtual Machine Multi-Queue (d.VMMQ)
- Virtual Receive Side Scaling (vRSS)

Low Extra Delay Background Transport (LEDBAT)

LEDBAT is a delay-based congestion control algorithm that designates bandwidth to users and applications, while still using the totality of the network when it is available. (Shalunov, Hazel, Iyengar, & Kuehlewind, 2012) This makes it interesting for deploying updates in large-scale IT environments without impacting users.

High-performance SDN gateways

The throughput of existing SDN gateways has been improved, this by improving the throughput for Internet Protocol Security (IPSec) and Generic Routing Encapsulation (GRE) connections. Additionally, the required CPU utilization has been lowered.

Persistent Memory support for Hyper-V VMs

Storage-class memory, or also known as persistent memory, improves latency and delivers a high throughput. To leverage this in VMs, the two can now be directly connected.

New Deployment UI and Windows Admin Center extension for SDN

As already mentioned before, in Subsection 2.1.2, Windows Admin Center also implements certain features to make managing SDN easier. The extension that provides this is only available in a HCI.

2.4 Hyper-Converged Infrastructure (HCI)

Estimates made in a report by Gantz and Reinsel (2012), show that the digital universe will consist of 50.000 exabytes by the year 2020. This means that the infrastructure needs to be able to store these vast amounts of data. The static and inflexible way of storing data needs to become dynamic and agile to conform to modern standards. This can be achieved through a Software-Defined Data Centre (SDDC). An SDDC can be achieved in multiple ways but the most efficient and popular method is through HCI. It converges the compute, storage, networking and management components, as can be seen in Figure 2.2, through software that is running on the hypervisor. In addition to the advantages that come with HCI, they deliver strong support for the deployment of a hybrid cloud, one of the other key themes in Windows Server 2019. HCI reinvents how to store data through S2D, which was one of the most anticipated features to be included in Windows Server 2019. This will be discussed below together with Hyper-V, SDN and how these components can be managed through the Windows Admin Center. (Haag, 2016)

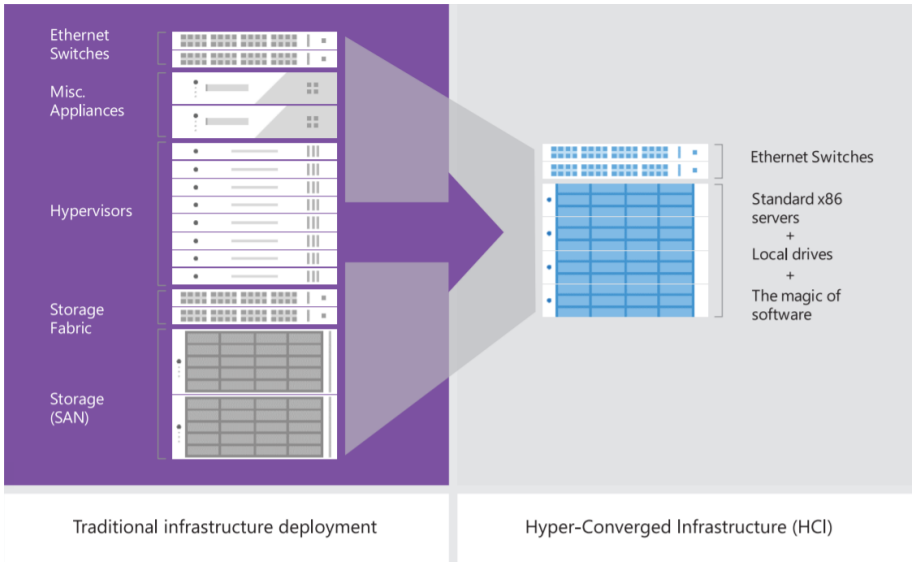


Figure 2.2: Hyper-Converged Infrastructure
Adapted from Woolslayer, 2018

2.4.1 Hyper-V

As mentioned in the introduction, a HCI requires a Hypervisor. In Windows Server, this is provided by Hyper-V. It can be used to virtualize compute, storage and networking components. They all run in their own isolated space, which translates in the ability to run multiple of these on a single hypervisor. The previously mentioned advantages also apply to Hyper-V. The provided services make room for a scalable and flexible infrastructure. To summarize, Hyper-V provides the Hypervisor that is an essential part of an HCI. (Short, 2016)

2.4.2 Storage Spaces Direct (S2D)

Another vital component of HCI is Software-Defined Storage (SDS). In Windows Server, this is done through S2D. This technology was developed to provide flexible and agile SDS. Some key benefits offered are simplicity, performant storage, fault tolerant and scalability. With Windows Server 2019 comes the largest update for S2D since its introduction. The licensing for this feature is also included in Windows Server 2019 Datacenter Edition which means, that for most clients, it will not involve an additional cost. (Gerend, Gries, et al., 2018)

2.4.3 Software Defined Networking (SDN)

As previously mentioned in Subsection 2.2.2, SDN gives form to the networking component of HCI. It provides IT administrators with the ability to design advanced networks effortlessly.

2.4.4 Windows Admin Center (WAC)

Windows Admin Center is an all-in-one platform for local and remote server management. It is not a replacement for Microsoft System Center Configuration Manager (SCCM), it is a complementary tool that does not require SCCM. WAC can be deployed as a local client on a Windows 10 machine, from where it is possible to manage all the connected servers. Alternatively, it can be deployed on Windows Server. It has been designed for Windows Server 2019 but can also be deployed to Windows Server 2016. The first option is to deploy it as a gateway server, this is the ideal solution for large-scale environments. When deploying the gateway server in a failover cluster, high availability can be enabled. The final option is to deploy it on a server which is going to be managed or is part of the cluster that is going to be managed. This option is recommended for distributed scenarios. The key components of which it consists, listed below, make it no surprise that the Windows Admin Center has been mentioned before.

- Core tools
- HCI Management
- Security
- Built for Hybrid
- Partner Ecosystem

It is Windows Server Management reimagined, with the input of costumers kept in high regard. It is the glue that joins all other components under one User Interface (UI). This tool is also the final part of our HCI environment, as it combines storage (S2D), network (SDN) and computing (Hyper-V) components under its management interface.

2.5 Conclusion

Windows Server 2019 is a highly advanced OS. With the new features, it provides a smooth and manageable experience to administrators and IT professionals. The four key themes, that have been further developed to offer improvements, have been thoroughly discussed in the previous sections and make it interesting to negotiate the migration regardless of its size and impact. Furthermore, extended support for Windows Server 2019 will be provided until 2029, this makes it an investment in the future for any organization. In Chapter 3, the different methods for migrating the system will be discussed.

3. Methodology

In this chapter, the migration from Windows Server 2016 to Windows Server 2019 will be executed. This migration will first be performed on an environment which has been based on the Modern Desktop Deployment and Management Lab Kit provided by Microsoft. (Gallagher, 2018) Here a Domain Controller (DC) will be migrated. After this, the migration of a typical SAP environment, as described by delaware, from Windows Server 2016 to Windows Server 2019, will be performed. Finally, the different versions of the Windows Server 2019 base container images will be analysed. How these can lower virtual machine overhead and improve virtualization efficiency compared to their predecessor, will be reviewed. But first, the infrastructure that was used for the initial migration will be discussed.

3.1 Migrating the OS

In this section, a DC will be migrated using both the in-place upgrade and side-by-side migration method. This to show the basics of the migration process in an environment where no third-party services, such as an SAP solution, are running. That will be discussed in Section 3.2.

3.1.1 Technical specifications of the proof of concept environment

The proof of concept was made using a bare-metal server, running Windows Server 2016. The proof of concept environment was than virtualized using Hyper-V. Additionally, Windows Admin Center was also installed locally, this to make the management of the re-

sources easier and more efficient. The specifications of the server are the following:

- CPU: Intel Xeon E5620
- RAM: 96 GB
- HDD: 500 GB
- OS Version: Windows Server 2016
- Hyper-V role installed
- Administrative rights on the device

The proof of concept environment was based on the Modern Desktop Deployment and Management Lab Kit provided by Microsoft. (Gallagher, 2018) This to make replication of the environment simple and efficient.
The Modern Desktop Deployment and Management Lab Kit consists of the components in Table 3.1.

Server Name	Roles & Products
HYD-DC1	Active Directory Domain Controller, DNS, DHCP, Certificate Services
HYD-MDT1	Microsoft Deployment Toolkit
	Windows 10 1809 ADK
	Windows Deployment Services
HYD-CM1	System Center Configuration Manager 1806
	Windows Deployment Services
	Microsoft Deployment Toolkit
	Windows 10 1809 ADK
	Windows Software Update Services
	Microsoft SQL Server 2014
HYD-APP1	Microsoft BitLocker Administration and Monitoring
	Microsoft SQL Server 2014
HYD-GW1	Remote Access for Internet Connectivity
HYD-INET1	Simulated Internet
HYD-VPN1	Remote Access for VPN
HYD-CLIENT1	Windows 10 1809 Domain Joined
	Office 365 ProPlus Build 16.0.11121.20000
HYD-CLIENT2	Windows 10 1809 Domain Joined
	Office 365 ProPlus Build 16.0.11121.20000
HYD-CLIENT3	Windows 10 1809 Workgroup
HYD-CLIENT4	Windows 10 1809 Workgroup
HYD-CLIENT5	Bare metal (no installations)
HYD-CLIENT6	Bare metal (no installations)
HYD-CLIENT7	Windows 7 Domain Joined

Table 3.1: Modern Desktop Deployment and Management Lab Kit Components
Adapted from Microsoft Corporation, 2019

Only HYD-CLIENT1 will be kept in the environment since there is no need for any additional clients. Connection to the VMs can be made using the credentials in Table 3.2.

User	Access Type	User Name	Password
Local Administrator	Administrative	Administrator	P@ssw0rd
Domain Administrator	Enterprise Administrator	CORP\LabAdmin	P@ssw0rd

Table 3.2: Modern Desktop Deployment and Management Lab Kit Credentials
Adapted from Microsoft Corporation, 2019

3.1.2 In-place upgrade to Windows Server 2019

In this subsection, an in-place upgrade will be performed on the Domain Controller (DC), HYD-DC1, from Windows Server 2016 to Windows Server 2019. At first, the operation and services running on the DC, as well as the connection to the other servers and clients in the domain, will be verified.

Prerequisites

Before starting the upgrade, it is important to verify that the server is backed-up. Be sure to check when the last back-up was performed and if it can be successfully restored. After this, it is important to verify that all the third-party applications on the server are supported by the newest version of the OS, this will be examined for SAP in Section 3.2, but is not of interest in this subsection. Finally, the forest and domain need to be prepared for the upgrade. The Windows Server 2019 installation media provides the necessary tools for this. The following commands complete this process, as is shown in Figure 3.1. Be sure to verify the mounting point of the installation media, in this scenario it has been mounted to D:\, change this accordingly on the first line of the commands.

```
:d
cd support\adprep
adprep /forestprep
adprep /domainprep
```

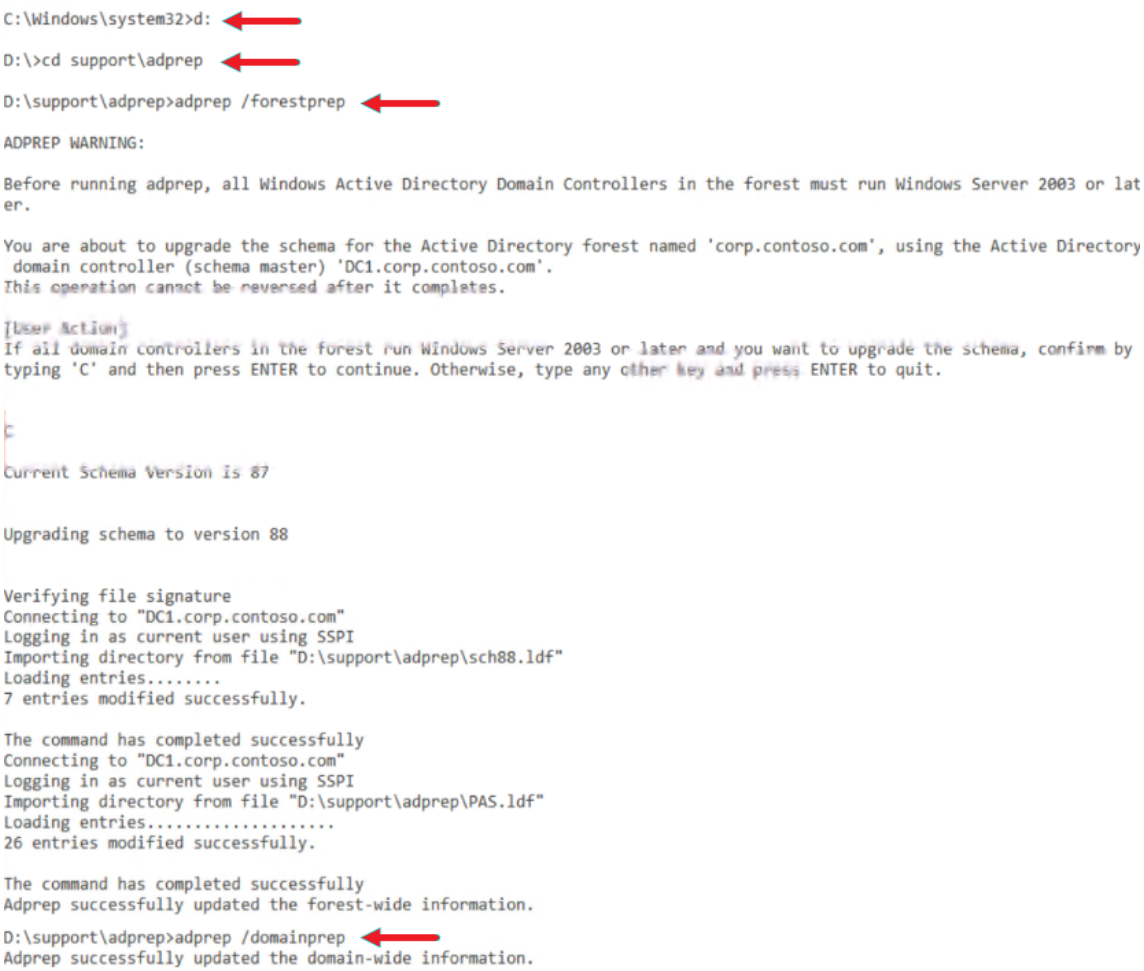
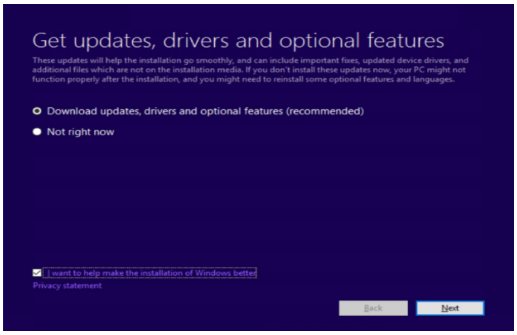


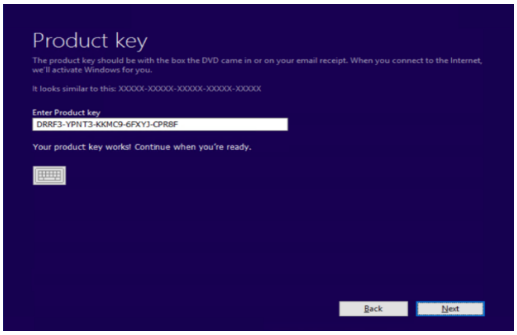
Figure 3.1: Preparing the forest and domain for in-place upgrade

In-place upgrade

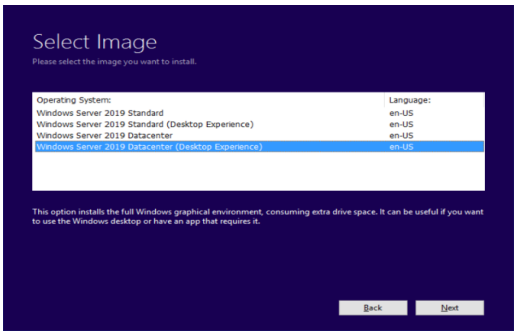
After preparing the forest and domain for the in-place upgrade, the setup from the installation media is to be launched. From this point on, the upgrade process has been visualized in Figure 3.2. Be sure not to use the evaluation version of Windows Server 2019, since this does not support in-place upgrades.



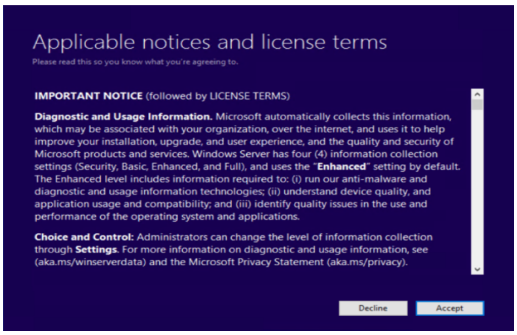
(a) Click next to migrate



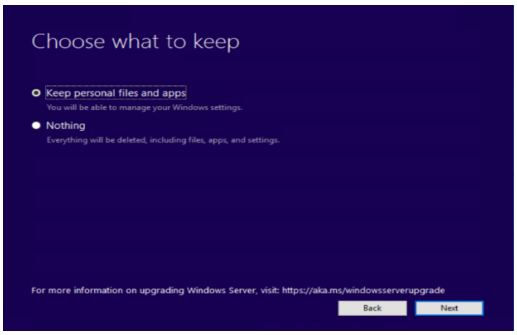
(b) Enter the product key



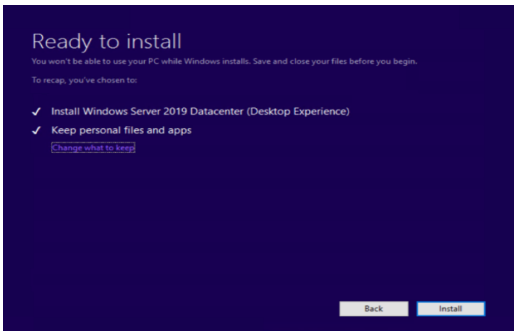
(c) Select a version of choice



(d) Accept the licence terms



(e) Select 'Keep personal files and apps' to perform an in-place upgrade



(f) Review the settings and start the installation

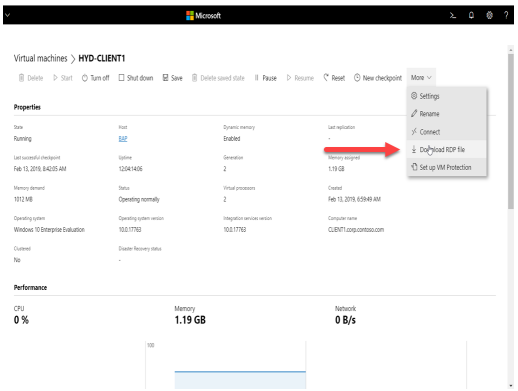
Figure 3.2: The in-place upgrade process

Verification

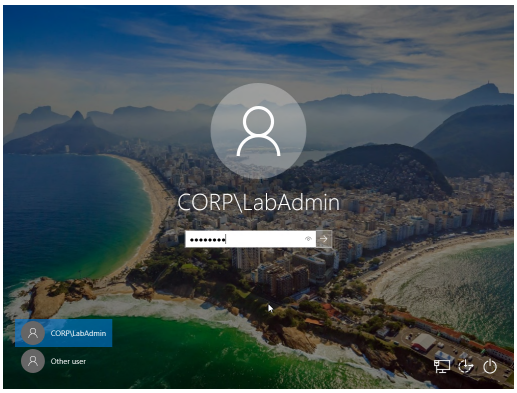
In this paragraph, the services of the DC, as well as the connection between the client and server, will be verified. First, the Remote Desktop Protocol (RDP) file will be downloaded

through the Windows Admin Center. Using this file, a connection to the Hyper-V VM can easily be made. After this, the ability to log in as a domain user is verified, as the DC provides the login server. Afterwards, the domain will be checked through the Control Panel and finally, using PowerShell. In this final verification, the logon server will be checked as well as how the client is connected to the domain. It is expected that the client is connected through the recently upgraded DC. The commands, that have been used to verify this, and their expected output can be found below. This is also visualized in Figure 3.3

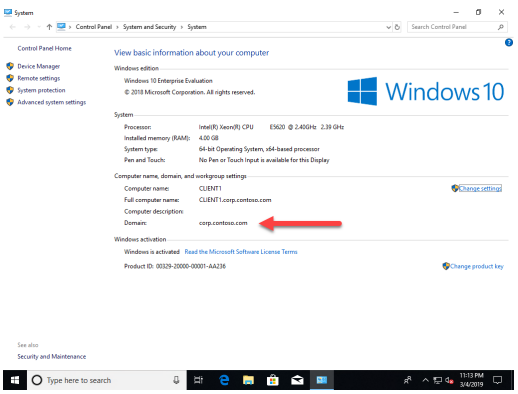
```
PS C:\Windows\system32> $env:LOGONSERVER
\\DC1
PS C:\Windows\system32> nltest /sc_query:corp.contoso.com
Flags: 30 HAS_IP HAS_TIMESERV
Trusted DC Name \DC1.corp.contoso.com
Trusted DC Connection Status Status = 0 0x0 NERR_Success
The command completed successfully
```



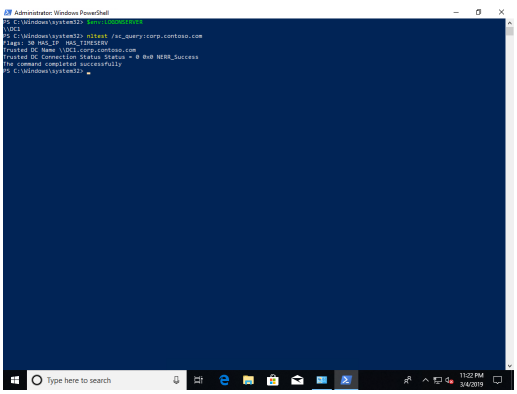
(a) Download and open the RDP file



(b) Log in as a domain user



(c) Verify the DC through the GUI



(d) Verify the DC through PowerShell

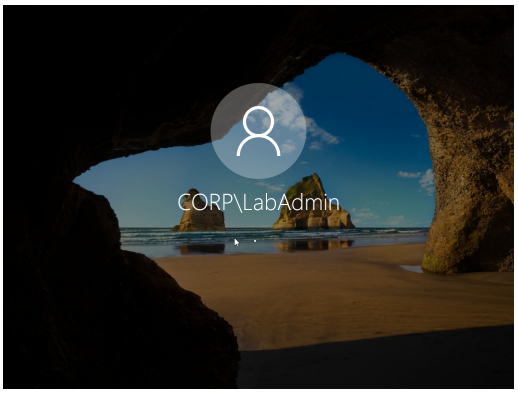
Figure 3.3: Verifying the connection to the upgraded DC

3.1.3 Side-by-side migration to Windows Server 2019

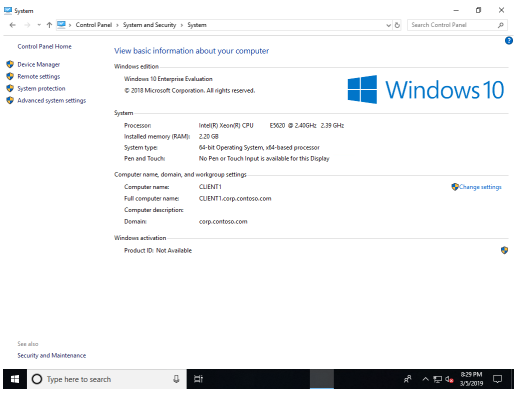
In this subsection, a side-by-side migration to Windows Server 2019 will be performed on the DC running Windows Server 2016. At first, the connection between the client and the DC will be verified. After this, the side-by-side migration will be performed by creating a new VM on which Windows Server 2019 will be installed and configured. This VM will, eventually, replace the DC running Windows Server 2016. Finally, the connection between the new DC running Windows Server 2019 and the client will be checked.

Prerequisites

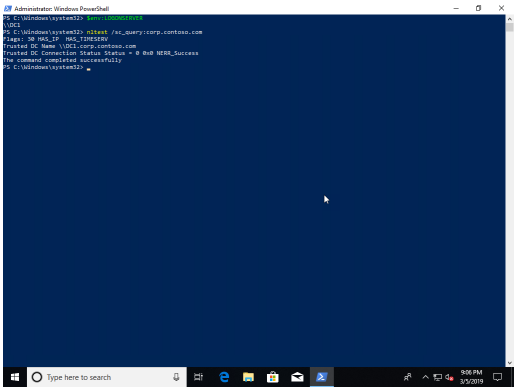
The connection between the DC and the client will be verified as was done in Subsection 3.1.2. Additionally, the Windows edition will be checked to verify the success of the side-by-side migration. The prerequisites are shown in Figure 3.4.



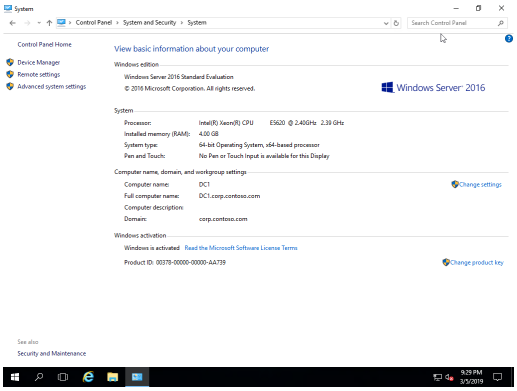
(a) Log in as a domain user



(b) Verify the DC through the GUI



(c) Verify the DC through PowerShell



(d) Verifying the Windows edition

Figure 3.4: Verifying the connection between the client and DC

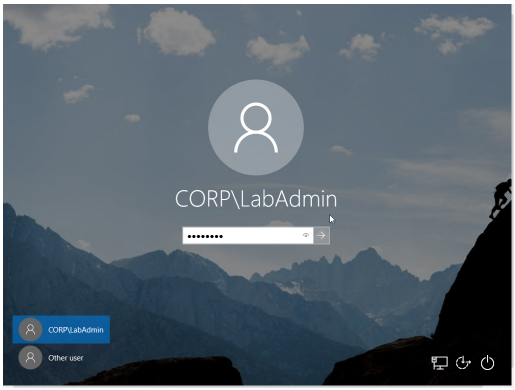
Side-by-side migration

The side-by-side migration to the new Windows Server 2019 DC, that will be performed in this paragraph, can be divided into seven parts:

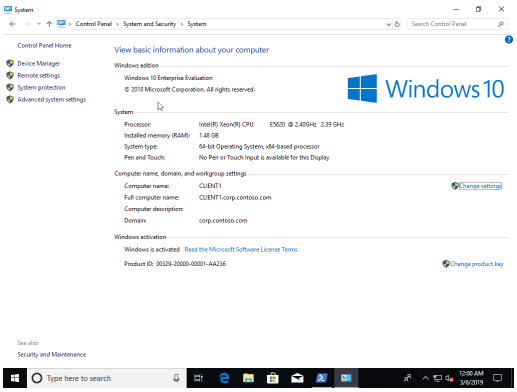
1. Creating the VM
2. Installing Windows Server 2019
3. Joining the existing domain
4. Promoting the new VM to DC
5. Migrating the FSMO roles
6. Configuring DNS and DHCP
7. Decommissioning the old DC

Considering the magnitude of this side-by-side migration it is not included in the main part of this bachelor's thesis. However, it can be found in Appendix C.

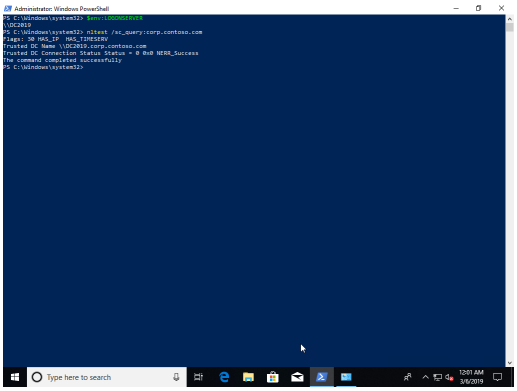
Verification



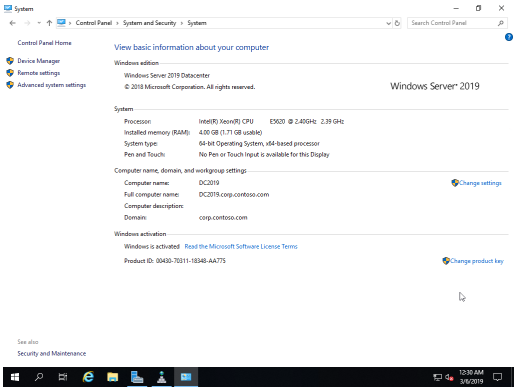
(a) Download and open the RDP file



(b) Log in as a domain user



(c) Verify the DC through the GUI



(d) Verify the DC through PowerShell

Figure 3.5: Verifying the connection to the migrated DC

3.1.4 Conclusion

After performing the migration from Windows Server 2016 to Windows Server 2019 using both methods, either of them has its own advantages and disadvantages. While an in-place upgrade may seem easier to perform at first glance, it is important to remember that every OS has a certain amount of baggage. Using this technique, these unnecessary files, such as old uninstallers and temporary files, will be transferred from the previous installation to the new one. This eventually can have an impact on the performance of the OS. It is also important to keep in mind that even though an in-place upgrade might be easier, it cannot be performed from every version to Windows Server 2019.
Using the in-place upgrade from older versions of the OS might require the process to be repeated multiple consecutive times. These all increase the additional baggage that gets transferred. When choosing for a side-by-side migration this is not the case. Only the necessary files and services get transferred to the new OS. When choosing for this approach, the old infrastructure or VM can be kept online so that in case of failure everything remains operational. Only after extensive testing, the old infrastructure can be taken offline, so that it gets replaced by the newer one. This provides an additional fall-back in case of any problems. It is important to note that the side-by-side migration currently is the only migration method that is supported for Microsoft Azure VMs. The approach is, however, much broader and requires more research in advance. In this part of the proof of concept, only the DC was migrated. This was done effortlessly thanks to the secondary DC. The research that is required to migrate Windows Server to the latest version in a business environment will be done in the following section, for a SAP environment.

3.1.5 Summary

In-place upgrade

+ Requires a minimal amount of research
- Replaces the old environment without providing redundancy
- Unnecessary files get transferred with the upgrade
- Consecutive upgrades could be required
- Limited support for older versions of Windows Server
- No support for Microsoft Azure

Side-by-side migration

+ Clean installation of Windows Server
+ Old environment remains in production during migration
+ Supported in Microsoft Azure
- Requires additional research for each individual migration

3.2 SAP migration

Before migrating a server, it is of great importance to ensure that all dependencies have been met. Afterwards, all of these dependencies should be verified. This to confirm the operation of the environment. In this section, the migration from Windows Server 2016 to Windows Server 2019 will be done in a SAP environment. This to provide an example of the additional research that comes with the migration of a server that is performing a critical task in a business environment. The migration is of interest in any kind of organization for the same reasons that were mentioned before. Additionally, SAP recommends the usage of the latest supported version of any OS for its software solutions. Currently, the latest supported version of Windows Server is Windows Server 2019 LTSC.

3.2.1 Technical specifications of the SAP environment

The proof of concept environment has been made using Microsoft Azure. For the environment, a system running Windows Server 2016 Datacenter Edition was used. The installation consisted of a SAP NetWeaver 7.5 ABAP stack combined with a SyBase ASE database. The architecture of the SAP environment can be seen in Figure 3.6. The installation and configuration of the SAP environment can be found in Appendix D.

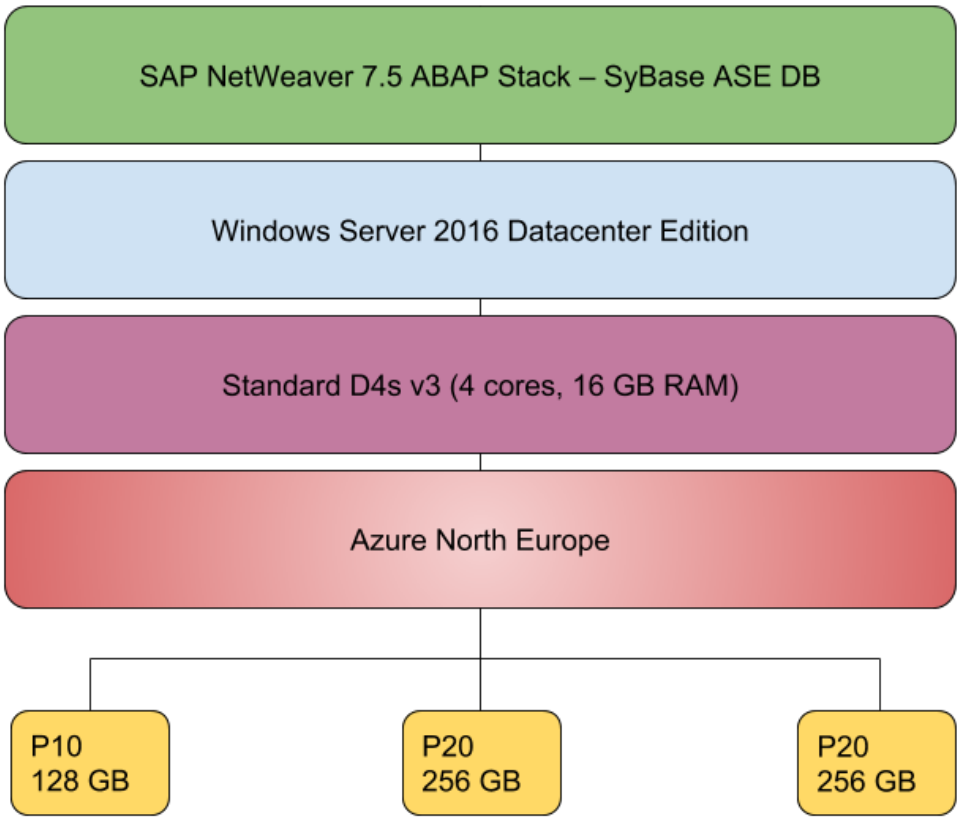


Figure 3.6: Infrastructure of the SAP environment

3.2.2 Migration of the SAP environment

Since Windows Server 2019, SAP offers support for full upgrades. This means that for non-clustered systems the in-place upgrade method is supported. However, the traditional method of migration, using a side-by-side migration, is still supported. Many parts of the migration process that was described in Section 3.1 are applicable to the current environment. Because of this reason, the migration of the SAP environment will be kept constraint and the focus will be on the additional chores that come with this migration. First, it was verified that Windows Server 2019 was supported using the SAP Product Availability Matrix (PAM), as can be seen in Figure 3.7.

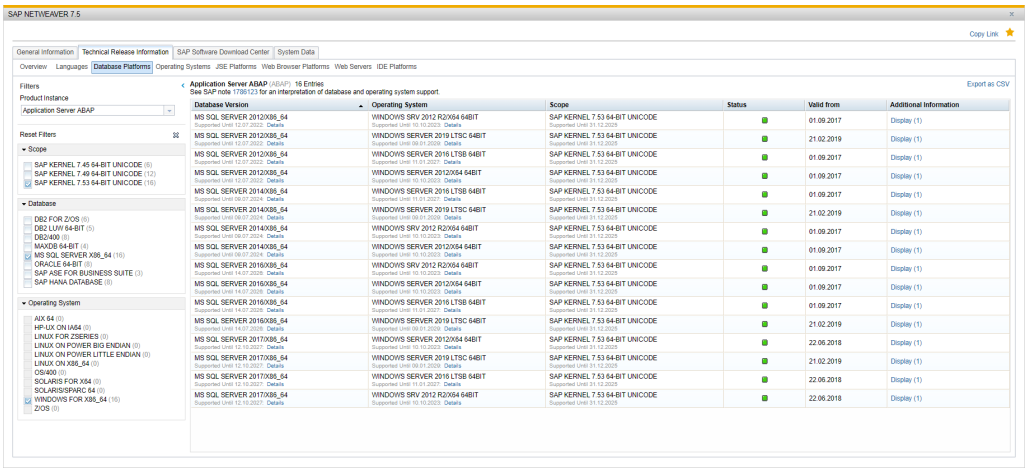
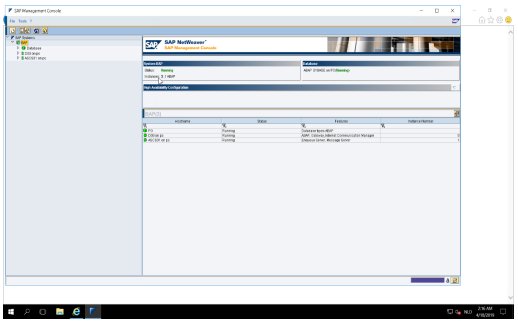


Figure 3.7: SAP Product Availability Matrix (PAM)

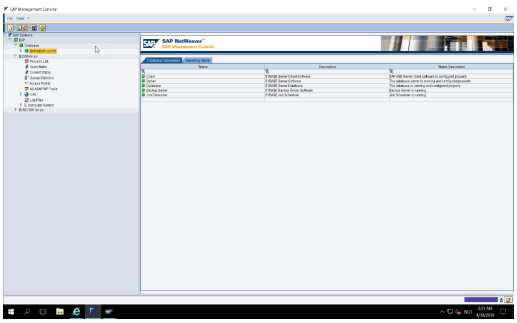
Prerequisites

Before any migration, the operation of the SAP solution will be verified. The following process will verify the operation of the software solution.

1. Browse to 'http://localhost:50013/' on the VM
2. Verify the SAP environment is running, as seen in Figure 3.8
3. Verify the database server as seen in Figure 3.8



(a) Verify the SAP environment



(b) Verify the Database Components

Figure 3.8: Verifying the operation through the SAP Management Console

SAP migration

After verifying the operation of the software solution, the in-place upgrade will be performed as described in Subsection 3.1.2. Therefore, the Virtual Hard Disk (VHD) was downloaded from Azure. The upgrade was performed through Hyper-V on the bare-metal server discussed in Section 3.1. Alternatively, a side-by-side migration can be performed. The side-by-side migration of the SAP environment can be divided into 4 parts:

1. Creating the VM
2. Installing Windows Server 2019
3. Installing and configuring the SAP environment
4. Backup and restore of the SyBase ASE DB
5. Decommissioning the old SAP environment

The first and second part of this procedure was already described in Subsection 3.1.3. The installation and configuration have been described in Appendix D. For the third part to reduce the cut over time, the backup and restore are used followed by log shipping. When the last log is applied, the new system is ready to cut over. This way, the downtime is limited by the last log ship instead of the backup and restore of the database. The final part is the deletion of the old VM after verifying the operation of the new VM, as shown in the following paragraph.

Verification

After a successful migration, the operation of the SAP solution will be verified once-more. This was done before the migration to verify the operation of the SAP environment on Windows Server 2016. This procedure is identical for both Windows Server 2016 and Windows Server 2019 and has been described in Subsection 3.2.2.

3.2.3 Conclusion

After the migration of the SAP environment, many of the aspects from the previous migration in Section 3.1 return. With the migration of a software solution, it is important to verify that it supports the version of the OS to which will be migrated beforehand. For SAP, this was verified using the SAP PAM. In the SAP PAM all supported solutions can be found. Here, all the different aspects that were installed, as described in Appendix D were verified to be supported for operation on Windows Server 2019 LTSC. Verifying the operation of all the third-party applications that need to be installed requires additional research. This section of the bachelor's thesis shows that no two migrations are the same. It emphasizes that for any migration, irrespective of the size and scope, its own research is required. Because no environment is identical to one another. There are always variables that should be taken into account.

3.3 Base container images of Windows Server 2019

In this final section, a comparison shall be made between the Windows, Server Core and Nano Server base container images. At first, the advantages of the new versions of the images will be discussed. This involves a comparison between version 1709 and version 1809 of the base container images. This will consist of comparing the size and performance of the base container images. Afterwards, the different use cases of the various versions will be discussed. These base container images have been tested in an environment as described in the following subsection.

3.3.1 Technical specifications of the container environment

The proof of concept environment for the Windows Server base container images was built using the Microsoft Azure platform. It uses the Standard D2s v3 (2 vcpus, 8 GB memory) Azure VM, running the Windows Server 2019 Datacenter Server Core and Containers image. The following packages will be installed inside the VM:

- Docker
- Hyper-V
- Windows Containers
- Chocolatey
- Git

The procedure to generate the container environment is described in Appendix E.

3.3.2 The advantages of version 1809

With the arrival of version 1809, the Semi-Annual Channel (SAC) equivalent of Windows Server 2019, there have been numerous improvements to the base container images. First, the overall size of the base container images has been significantly reduced. This can be seen in Figure 3.9. The only exception is the Nano Server image, which has slightly increased in size compared to its previous version. This is due to the addition of new features, such as major improvements for Linux containers and container networking through Kubernetes. The size of the different base images has been obtained by downloading and expanding them as described below. This was done through Windows PowerShell from inside the VM that was previously created on the Azure platform.

```
docker image pull mcr.microsoft.com/windows:1809
docker image pull mcr.microsoft.com/windows/servercore:1809
docker image pull mcr.microsoft.com/windows/nanoserver:1809
docker image pull mcr.microsoft.com/windows/servercore:1709
docker image pull mcr.microsoft.com/windows/nanoserver:1709
docker images | Out-File .container_images.csv
Import-Csv -Path .\container_images.csv
```

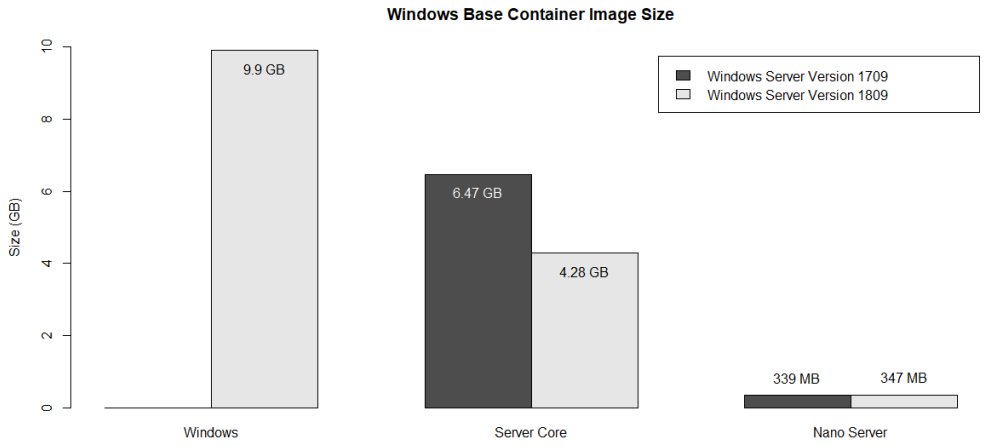


Figure 3.9: Comparison of the Windows base container image size

In this paragraph, the performance of the images shall be tested. This will be done using 'BenchmarkDotNet', a .NET library made for benchmarking. (Akinshin & Yakimets, 2019) Benchmarking using this library is done by calculating Message Digest Algorithm 5 (MD5) and Secure Hash Algorithm 2 (SHA-2) hash functions. The former is mostly used in the generation of identifiers, as it is not deemed secure enough for data security. The latter is better suited for this but has since been improved by Secure Hash Algorithm 3 (SHA-3). (Enkov & Karavasilev, 2017)
The container will be automatically built using a Dockerfile, each of these corresponds with its respective base container image. This is needed to add the required packages inside the container to successfully perform the benchmark. For the Windows and Server Core base container image, these were added manually, the Nano Server base container image was provided by Microsoft. Following commands need to be executed on the VM that was created on the Azure platform to benchmark every container individually. It is important to note that the kernel version of the OS must match the Windows image. While using Hyper-V isolation can circumvent this, it is not recommended since the additional virtualization of the kernel will lower the performance of the container. For the unambiguity of the benchmarks, Hyper-V isolation was used in every benchmark.

```
git clone https://github.com/jensdufour/Benchmark.git
cd Benchmark
docker build -t benchmark1 --isolation=hyperv -f .\
    WindowsNanoserver1709.dockerfile .
docker build -t benchmark2 --isolation=hyperv -f .\
    WindowsServercore1709.dockerfile .
docker build -t benchmark3 --isolation=hyperv -f .\
    WindowsNanoserver1809.dockerfile .
docker build -t benchmark4 --isolation=hyperv -f .\
    WindowsServercore1809.dockerfile .
docker build -t benchmark5 --isolation=hyperv -f .\
    Windows1809.dockerfile .
```

The results of running the individual benchmarks have been visualized in Figure 3.10 for MD5 and in Figure 3.11 for SHA-256. The figures show the average results after running the benchmarks twenty times. In Appendix F, all the data can be found, as well as the initial results after running the benchmarks ten times. Eventual outliers have been removed. As can be seen in Figure 3.10 there is no significant difference in performance between the two versions of Nano Server and Server Core. It is important to note that version 1709 was more performant in this benchmark.

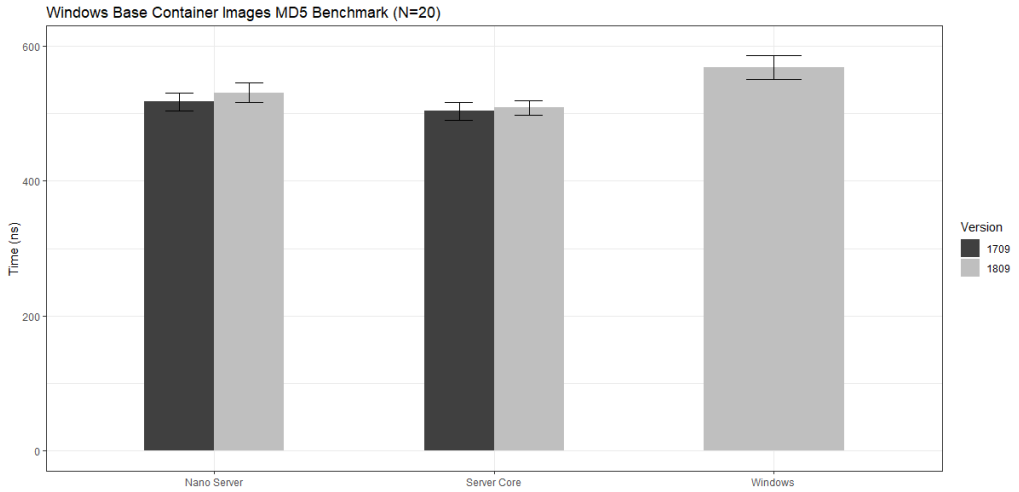


Figure 3.10: Windows Base Container Image MD5 benchmark (N=20)

In Figure 3.11 similar results can be found.

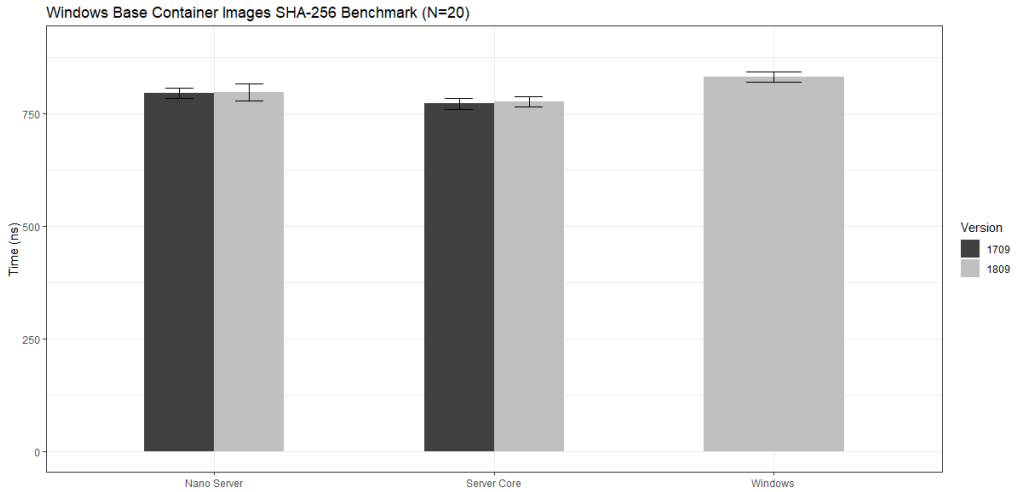


Figure 3.11: Windows Base Container Image SHA-256 benchmark (N=20)

When looking at the result of the benchmarks of Server Core and Nano Server, the performance of both versions is comparable, with the former version keeping the upper hand. However, the overall reduction in size and the additional features that have been added, as discussed in Chapter 2, make a strong case for the deployment of the latest images,

version 1809. The latest release of the base container images also included the Windows base container image. This base container image opens a whole array of new possibilities. The use case of this one and the others will be discussed in the following subsection.

3.3.3 Use cases of Windows, Server Core and Nano Server

The smallest one offered, is the Nano Server. This image is aimed at rapid and lightweight deployment using containers. It has been specifically designed for 'born in the cloud' applications. This is a term that has multiple usages, it refers to applications that are not legacy products. Applications that provide an agile deployment and offer on-demand availability. It is in no way meant to run typical Windows services. The bigger brother of Nano Server, Server Core, is more suited for this. This image offers application compatibility and has a wide array of built-in Windows roles and features. On top of this, it has full .NET Framework support instead of the basic .NET Core that is offered by the Nano Server. The final image that is offered is the new kid on the block. The Windows base container image offers almost all the Windows components in a lightweight package. This makes it exceptionally useful for automated UI tests as it also has DirectX graphics capabilities. It also includes a lot of dependencies which make it usable with out-of-date applications which won't be supported in the latest version of Server Core and Nano Server.
Thanks to the further development to these base container images, their footprint has been reduced significantly. Although older containers from Windows Server 2016 can still run through Hyper-V isolation on Windows Server 2019, it is recommended to rebuild them with the latest available images.

4. Future vision

This final chapter will focus on the public, private and on-premise solutions that Microsoft offers. Especially, how these are used as an extension of each other to build a modern infrastructure. It is not the first time that Microsoft Azure has been mentioned in this bachelor's thesis. It has been extensively used for the deployment of different proof of concept environments, as mentioned in Chapter 2. The future of this environment will be discussed first. Afterwards, the future of their private cloud solution, Microsoft Azure Stack, will be examined. Furthermore, what can be expected from their on-premise solution, Windows Server 2019, will be discussed. The Windows Admin Center will be reviewed. The discussion of the different aspects exclusively has the intention to give the reader an idea of what the future can hold. For this reason, it will be done cursory. Finally, how these can be used in unison to form the infrastructure of tomorrow, as described in Figure 4.1, will be concluded.

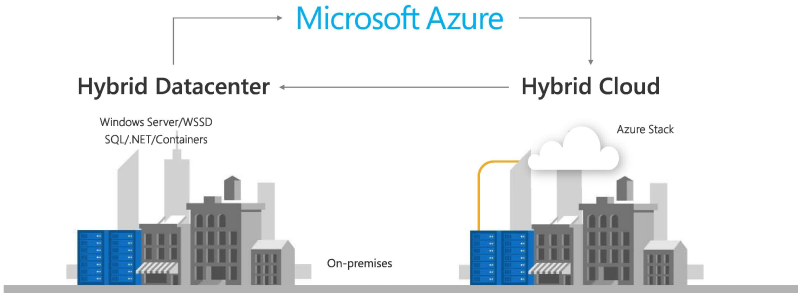


Figure 4.1: Bridging on-premise and cloud solutions for a modern infrastructure
Adapted from A. Singh and Shah, 2019

4.1 Microsoft Azure

As previously mentioned, Microsoft Azure is the public cloud solution Microsoft offers. There are currently more than fifty different global Azure regions and their network keeps expanding. It offers a wide array of solutions, some of which, like SAP on Azure, have been used in this bachelor's thesis. These are continuously updated to be on par with the latest developments in IT such as Artificial Intelligence (AI) and blockchain. Microsoft also offers a selection of these services in China. These services can be managed from the Windows, macOS and Linux OS through Azure PowerShell. Alternatively, they can be managed through the Azure Portal as can be seen in Figure 4.2.

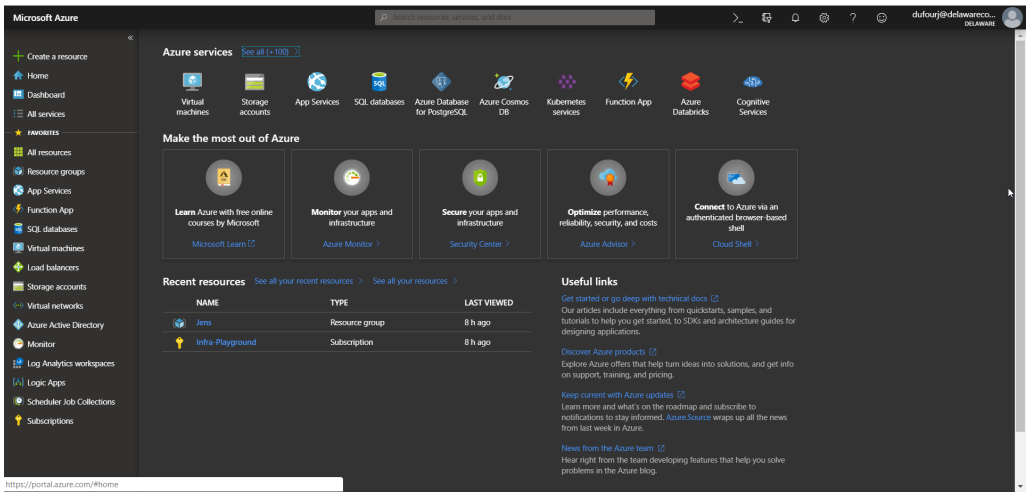


Figure 4.2: Microsoft Azure Portal landing page

Considering that the public cloud revenue is expected to grow with 17.3% in 2019, this is certainly one of the technologies that will play an important role in the future. (Ng et al., 2018)

4.2 Microsoft Azure Stack

As has been mentioned in Chapter 2, security concerns are one of the major bottlenecks when choosing a cloud solution. While most modern applications are being moved into the public cloud, some of these have additional requirements that can only be met by the usage of an on-premise solution. As an alternative, many organizations chose the additional security of the private cloud, a service that Microsoft offers through Microsoft Azure Stack. It allows organizations to bring the innovation of cloud computing to an on-premise environment. It can be seamlessly integrated into Microsoft Azure to provide a hybrid cloud environment, which is an essential part of this bachelor's thesis, and of which the advantages have already been thoroughly discussed.

4.3 Windows Admin Center (WAC)

The final part of the puzzle that is going to be discussed, is the Windows Admin Center. It is an essential part of Windows Server 2019 and provides the resources to manage your on-premise infrastructure with the ease and efficiency that comes with a cloud solution. It also provides everything needed to interlink your public cloud, hosted on Microsoft Azure, with the on-premise infrastructure. Some features available, like Azure Site Recovery and Azure Backup, have already been discussed in Chapter 2, but it is important to note that a lot of new features are going to be added to the Windows Admin Center over the following months. (A. Singh & Shah, 2019)
Features like Azure File Sync, file shares in the Azure public cloud and Azure Migration, which will make the migration from Windows Server to Microsoft Azure even more fluent, have already been announced. Windows Admin Center also provides support for manufacturers extensions through its own Software Development Kit (SDK), both now and in the future.

4.4 Conclusion

As has been described in Figure 4.1, Microsoft aims for a migration to the cloud. They want to provide an environment that distributes workloads dynamically, either between on-premise or cloud solutions. Windows Server 2019 was designed keeping this in mind This explains why hybrid cloud and HCI are key themes in the OS. It is an OS that forms a bridge between the on-premise and cloud environments. It does this through the implementation of features, like Storage Spaces Direct (S2D) and Software Defined Networking (SDN) which were previously only used in cloud environments. Microsoft aims to introduce new features several times a year which follow this ideology.
They want to offer support to all these components with a modern and future proof infrastructure in mind, either by using a hybrid data centre, Windows Server 2019 combined with Microsoft Azure or a hybrid cloud, Microsoft Azure combined with Microsoft Azure Stack.

5. Conclusion

The conclusion of this bachelor's thesis is that a migration to Windows Server 2019 is achievable. The latest version of the OS offers a smooth and manageable experience through the advancements made in the four key themes of Windows Server 2019. The extended support till 2029 makes it an ideal choice to future-proof any organization. While a migration to Windows Server 2019 in an environment with a third-party application requires additional research, it was attainable for a SAP environment. The migration from Windows Server 2016 to Windows Server 2019 is also feasible for any organization running an EOL OS, as expected with the latest version of the OS. This for either the general OS as for the base container images. Windows Server 2019 offers a wide array of improvements in terms of security, hybrid cloud, application platform and the Hyper-Converged Infrastructure. The addition of the new Windows base container image provides the tools for automated UI tests and its additional dependencies make it perfect for utilization with out-of-date packages. The Server Core base container image can be used to run typical Windows services. It offers application compatibility and has a wide array of built-in Windows roles and features. The Nano Server base container image was designed for 'born in the cloud' applications that provide an agile deployment and offer on-demand availability. The reduced footprint of the base container images without a drop of performance make the latest version the natural choice. The new features which are introduced can be leveraged through the usage of the Windows Admin Center (WAC). Organizations that are running EOL Operating Systems should consider the migration to Windows Server 2019. Organizations that are running EOL infrastructure could also consider a migration to the cloud, although this imposes additional research towards the advantages of a cloud solution in comparison to an in-house infrastructure.

A. Research proposal

The subject of this bachelor's thesis is based on a research proposal that has been assessed in advance by the promoter. This proposal is included in this Appendix.

A.1 Introduction

Windows Server is a well-known Operating System (OS) among Information Technology (IT) professionals. With major organizations all around the globe, like Infosys, that have implemented some form of the OS in their infrastructure. (Shailendra, 2015) One of the tasks that often need to be performed on the OS, is keeping applications up-to-date. However, it is not often described how to migrate to the latest version. This does not mean that frequent updates are not important, for both the addition of new features as well as the improvement of security, as this is becoming one of the big concerns of this century. This bachelor's thesis will go in-depth about the advantages and disadvantages of migrating to the latest version of Windows Server. In specific, this bachelor's thesis looks at the migration from Windows Server 2016 to Windows Server 2019, with as an optional requirement the migration of a SAP environment, as this is applicable to the business environment of the originator, delaware. The key purpose is to find a procedure that is efficient, minimizes possible downtime and is applicable not only to the originator, delaware but also to other organizations that find them self in the same situation and want to migrate their infrastructure to the latest version of the OS.

A.1.1 Research question

What are the advantages and disadvantages of a migration from Windows Server 2016 to Windows Server 2019 in a business environment?

A.1.2 Sub-research question

- What are the differences between the Windows, Server Core and Nano Server base container images of Windows Server 2019?
- Can SAP be migrated from an existing Windows Server 2016 to Windows Server 2019 in a business environment?
- How can the new features of Windows Server 2019 be leveraged in the migrated infrastructure?

A.2 State-of-the-art

Windows Server 2019 was built on the strong foundation of Windows Server 2016 although it introduces new features. (Gerend, Poggemeyer, et al., 2018) These can be boiled down to four key themes (Microsoft Windows Server Team, 2018):

1. Hybrid Cloud
2. Security
3. Application Platform
4. Hyper-Converged Infrastructure (HCI)

In the following subsections, the essence of the above themes is discussed.

A.2.1 Hybrid cloud

One of the new features in terms of hybrid cloud is the Server Core App Compatibility Feature on Demand. (Pacquer, Poggemeyer, & Plett, 2018) This is an optional feature pack that was designed for the Windows Server 2019 Server Core base container image and can always be applied to the system. It significantly improves application compatibility by adding binaries and packages. Even with these added packages, the footprint of the machine will remain as small as possible. It does not achieve this by implementing the Windows Desktop Experience GUI, but by using a lightweight GUI instead.

A.2.2 Security

Security has always been a fundamental part of any OS. With over 53.000 reported incidents and 2.216 confirmed data breaches, security is without a doubt hot topic. (Mansfield-Devine, 2018) This is heavily reflected in the newest edition of Windows Server, with the

seamless integration with Windows Defender Advanced Threat Protection (WDATP), Security with Software Defined Networking (SDN) and Shielded Virtual Machines. This bachelor's thesis will also explore the additional safety mechanisms that were added.

A.2.3 Application platform

At the heart of a server, applications can be found. The application platform provides the necessary services required by these applications. There have been key improvements in this aspect as well. These improvements are mostly virtualization and security related.

A.2.4 Hyper-Converged Infrastructure (HCI)

This technology could easily come out of buzzword bingo however, it is perhaps the most exciting feature that was improved in the release of Windows Server 2019. HCI makes it effortless to scale up from two nodes to a hundred node environment. This makes the technology intriguing for organizations with an in-house data centre.

A.3 Methodology

Extensive research will be done before attempting the migration. The proof of concept will consist of an environment with Windows Server 2016 that will be migrated to Windows Server 2019. This will be done both using the in-place upgrade and side-by-side migration method. By carrying out this migration, the advantages and disadvantages will become clear.
Carrying out the migration will show the limitations and features of the latest version. Afterwards, an attempt will be made to migrate an existing SAP environment to our new and optimized Windows Server 2019 environment.
Finally, the different base container images will be compared, both in terms of performance and size. The goal at the end of the proof of concept is to make a reasoned decision between Windows Server 2016 and Windows Server 2019.

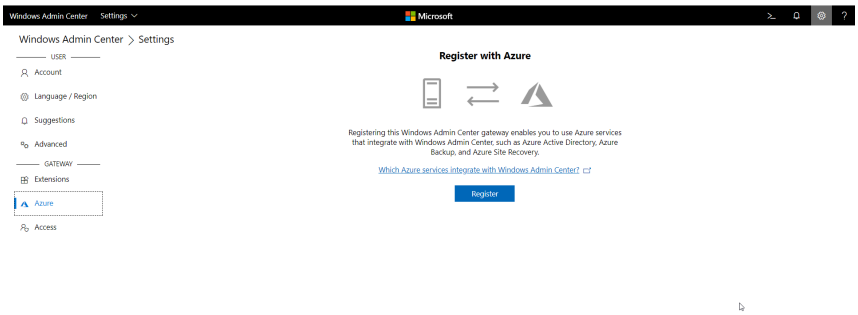
A.4 Expected results

It is expected that the proof of concept will demonstrate the advantages of the latest version of Windows Server and that the migration is an investment in the future. However, migrating a SAP will not yet be recommended due to the new nature of Windows Server 2019. Also, when looking at the base container images, the latest version will have the upper hand.

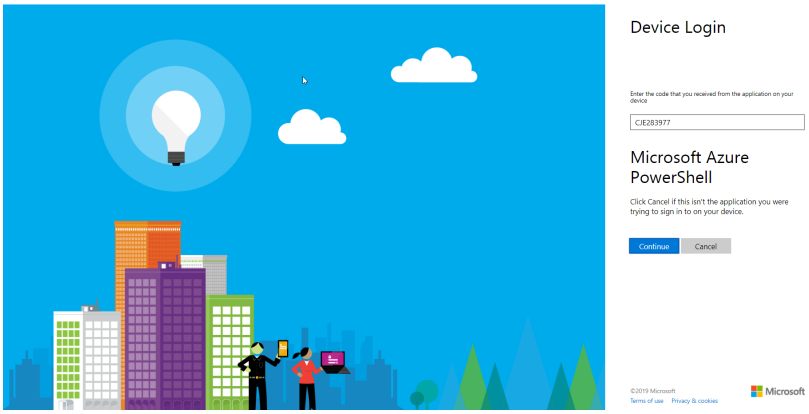
A.5 Expected conclusions

It is expected to conclude that migration from Windows Server 2016 to Windows Server 2019 is perfectly manageable, with a preference for a side-by-side migration, however additional research will be necessary for each individual software solution.

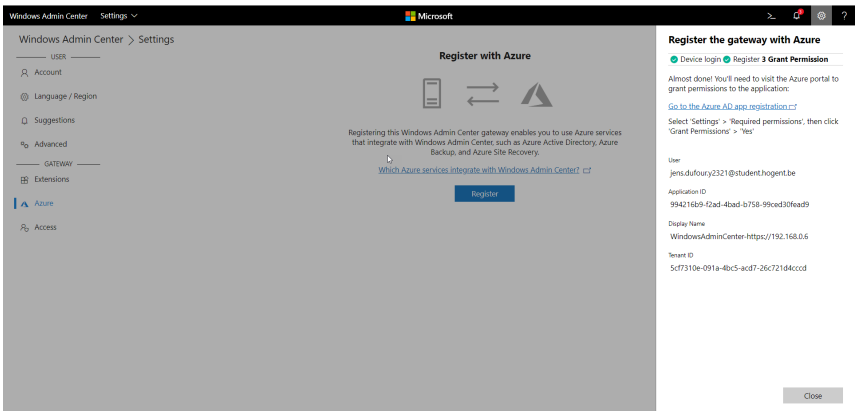
B. Windows Admin Center Azure integration



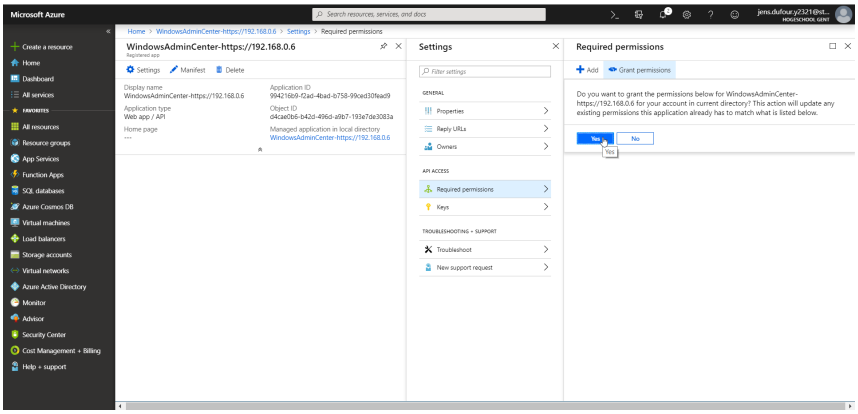
(a) Register with Microsoft Azure



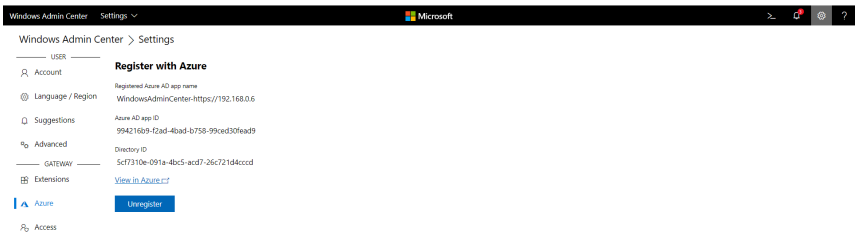
(b) Device login on Microsoft Azure



(c) Register the Gateway with Microsoft Azure



(d) Accept the permissions in the Microsoft Azure portal

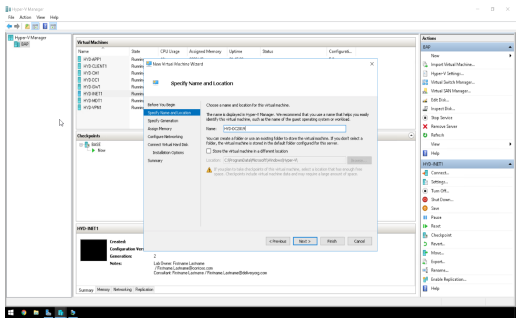


(e) The integration has succeeded

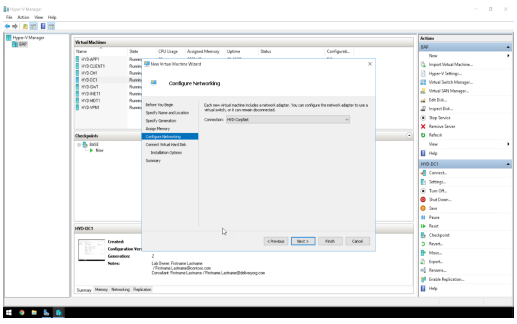
Figure B.1: Windows Admin Center (WAC) Microsoft Azure integration

C. Side-by-side migration

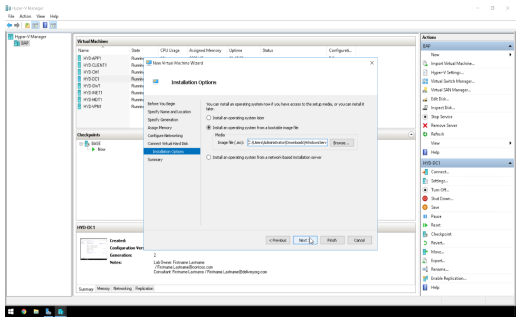
C.1 Virtual Machine (VM) creation



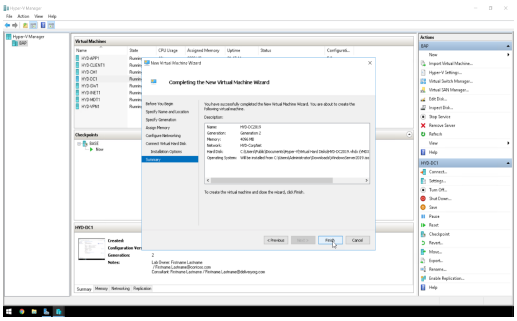
(a) Specify name and location



(b) Configure the network connection



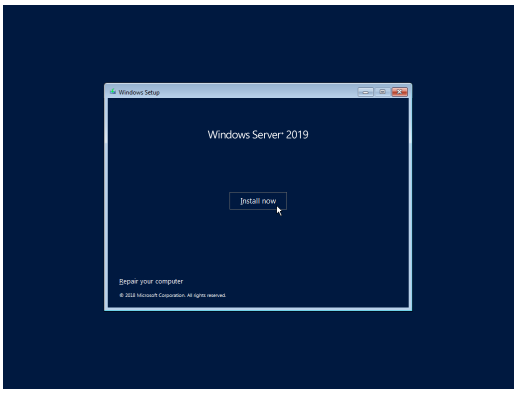
(c) Install an OS from a bootable image



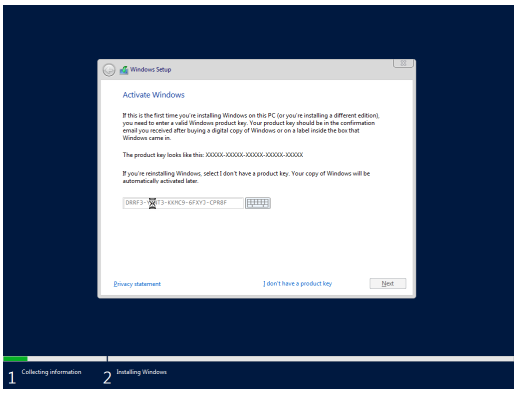
(d) Verify the VM

Figure C.1: Creation of the VM in Hyper-V

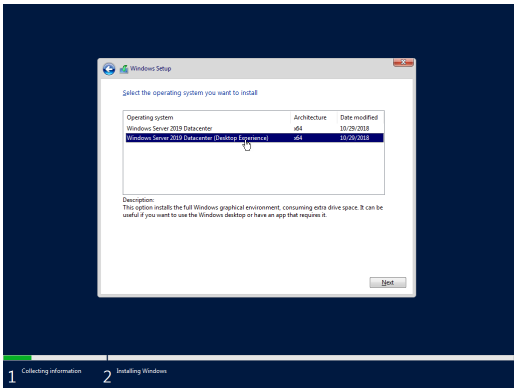
C.2 Windows Server installation



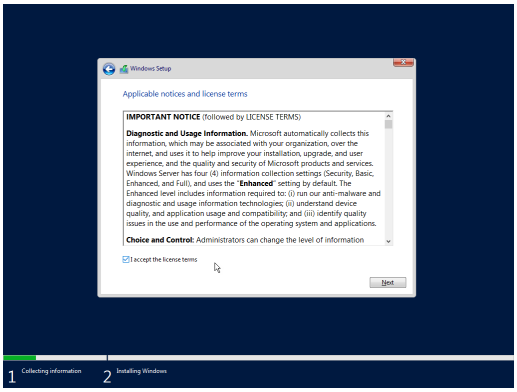
(a) Start Windows Server installation



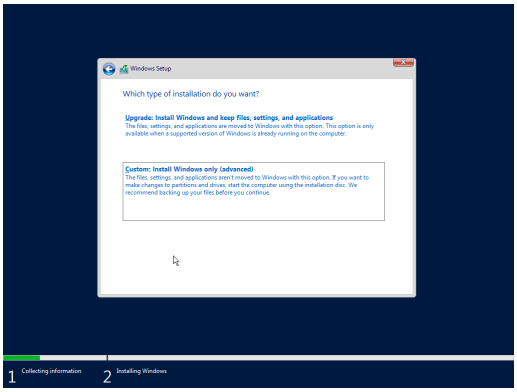
(b) Provide the product key



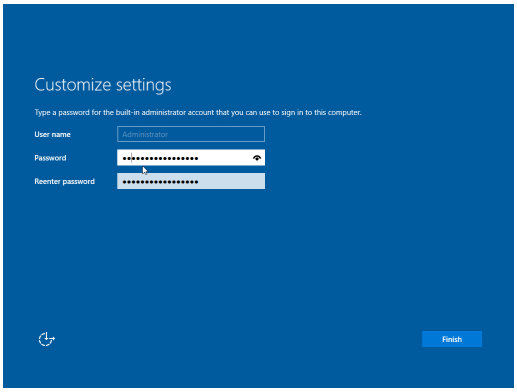
(c) Select Windows Server 2019 Datacenter (Desktop Experience)



(d) Agree with the notices and license terms



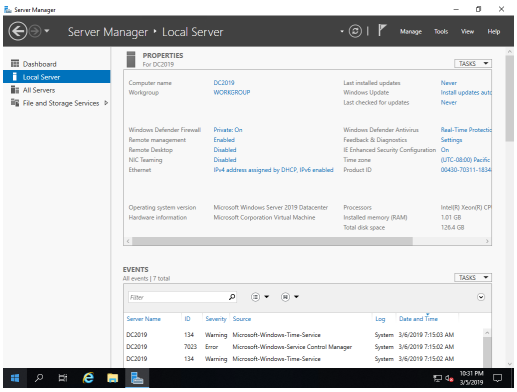
(e) Install Windows only



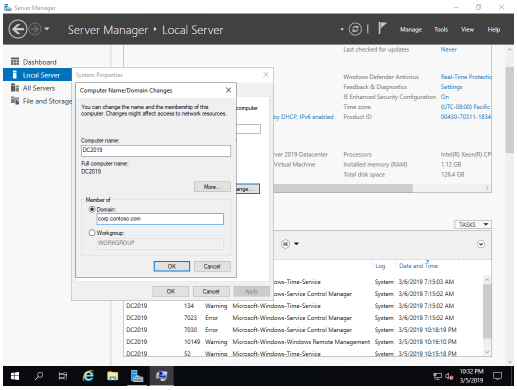
(f) Customize the final settings

Figure C.2: Installing Windows Server 2019 Datacenter Edition on the VM

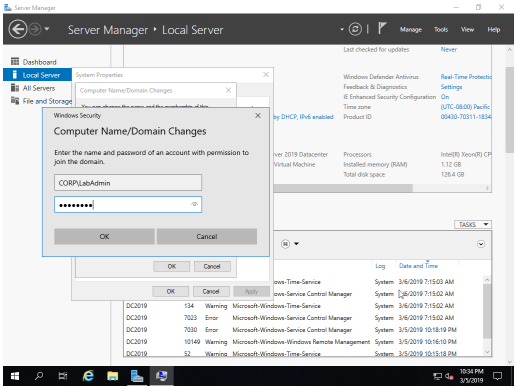
C.3 Joining the domain



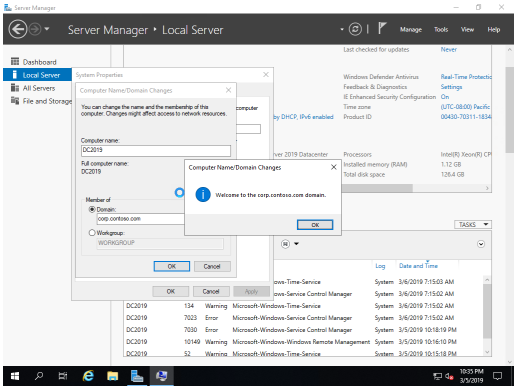
(a) Click the current Workgroup



(b) Select and enter the required domain



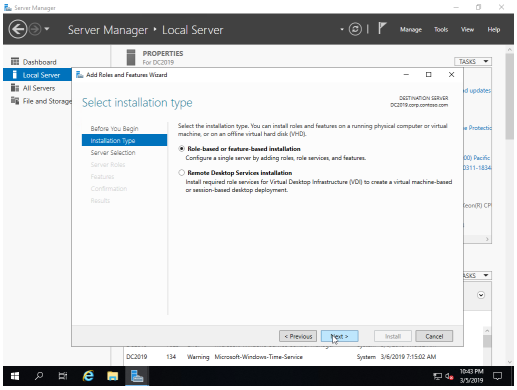
(c) Provide domain credentials



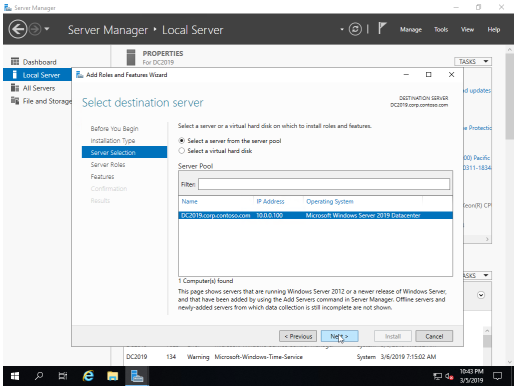
(d) Verify the domain changes

Figure C.3: Joining the corp.contoso.com domain

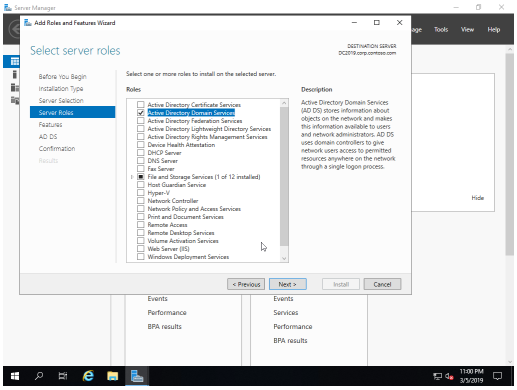
C.4 Promoting the server to DC



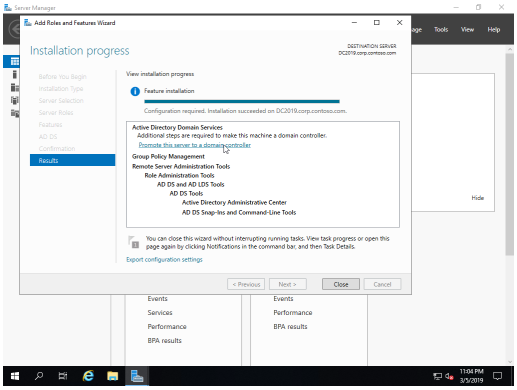
(a) Start the roles and features wizard



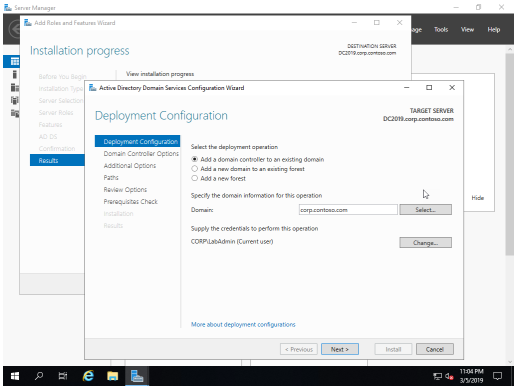
(b) Select the current server



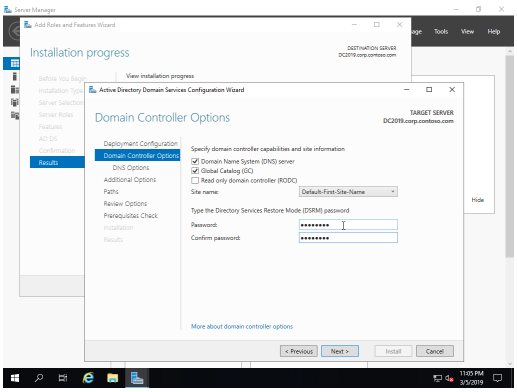
(c) Select the required server roles



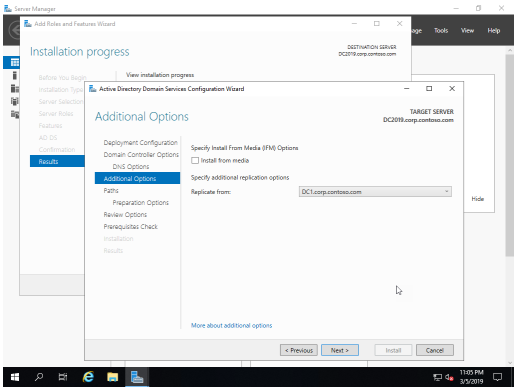
(d) Promote the server to DC



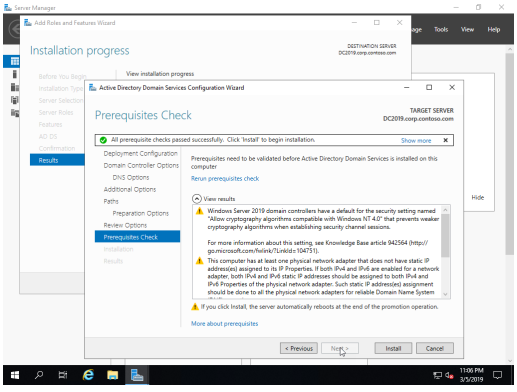
(e) Add a new DC to an existing domain



(f) Verify DSRM password



(g) Replicate from the previous DC



(h) Verifying and continue the promotion

Figure C.4: Promoting the server to DC

C.5 Migrating FSMO roles

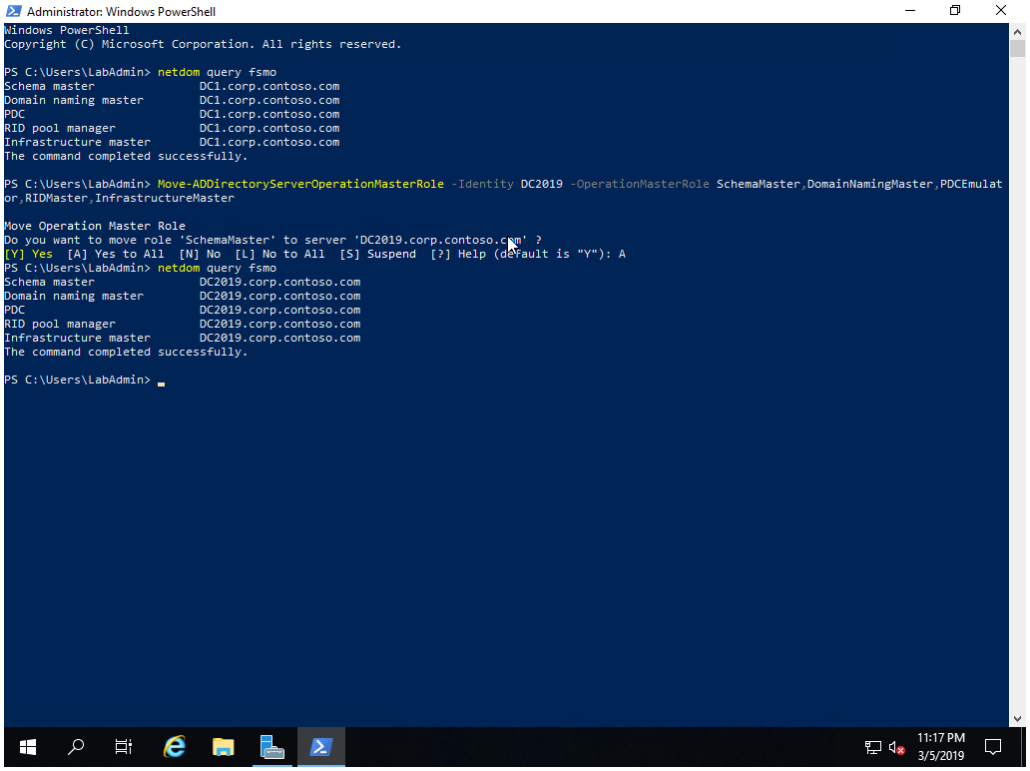
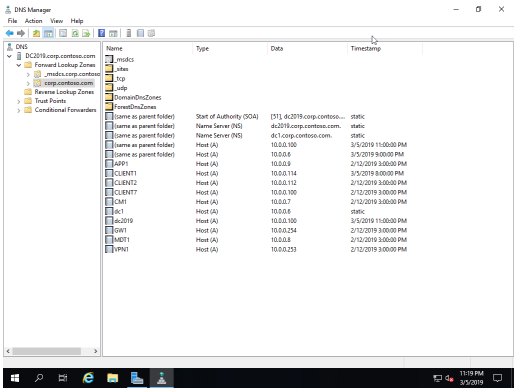
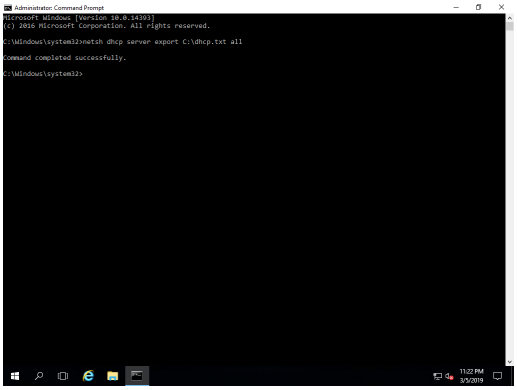


Figure C.5: Migrate the FSMO roles to the new DC

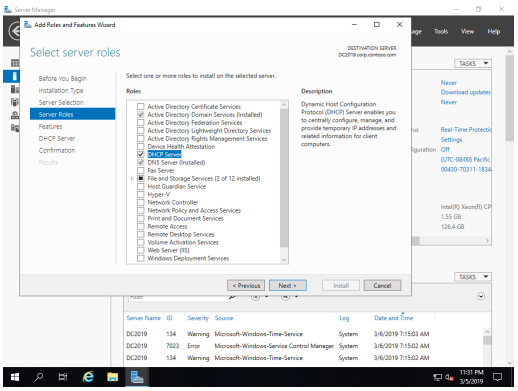
C.6 Configuring DNS and DHCP



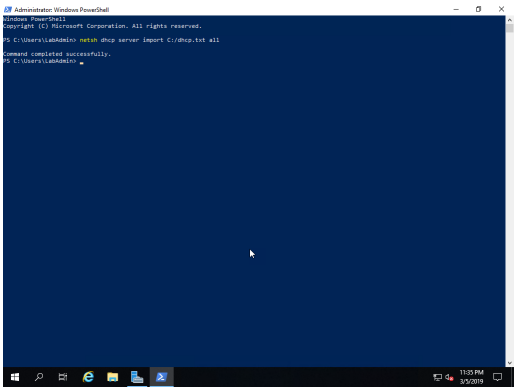
(a) DNS is automatically replicated



(b) Export the DHCP configuration



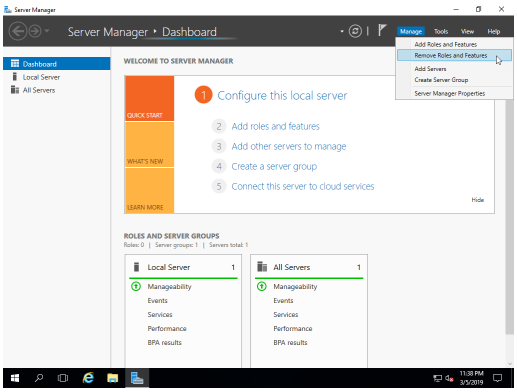
(c) Install the required roles on the new DC



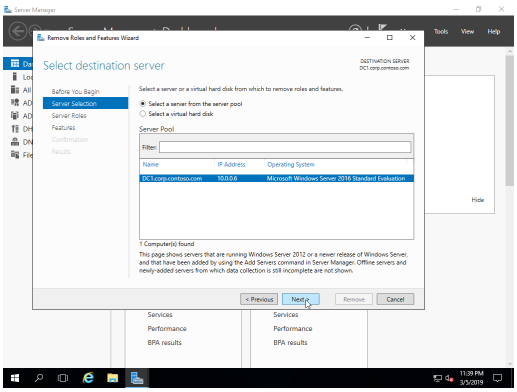
(d) Import the DHCP configuration

Figure C.6: Configuring DNS and DHCP on the new DC

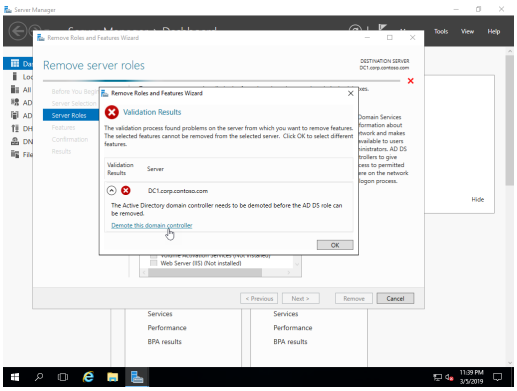
C.7 Decommissioning the old DC



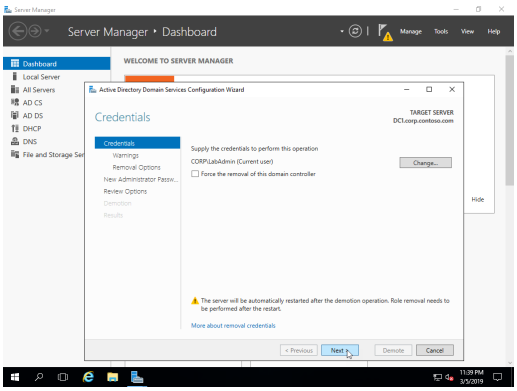
(a) Remove roles and features



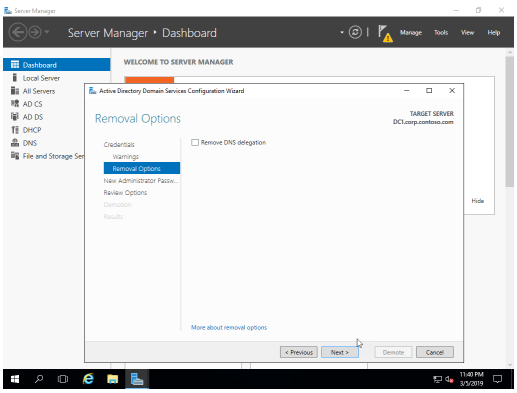
(b) Select the current DC



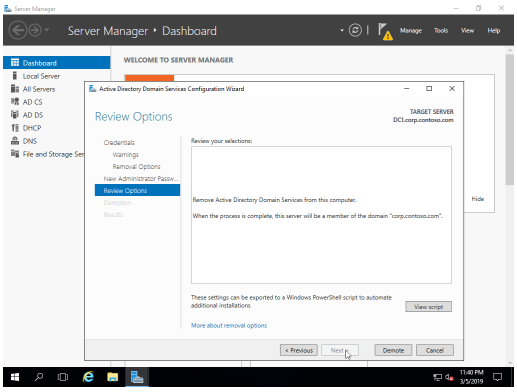
(c) Demote the old DC



(d) Verify the removal of the DC



(e) Uncheck removal of the DNS Delegation



(f) Demote the DC

Figure C.7: Decommissioning the old DC

D. SAP installation and configuration

D.1 Creation of the Microsoft Azure VM

The required Microsoft Azure VM will be created as described in Appendix E. The required Azure VM is shown in Figure 3.6.

D.2 Installation of the SAP environment

For the SAP environment a SAP NetWeaver 7.5 ABAP stack will be installed.

D.2.1 Preconditions

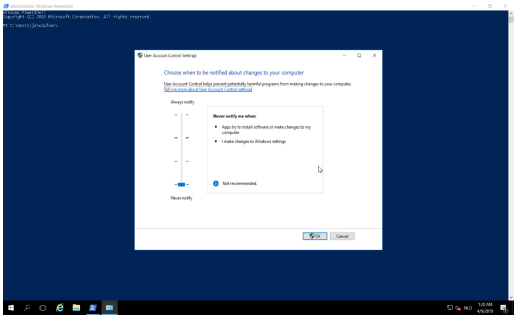
Server information

Azure VM Standard D4s v3
Ports RDP
Windows Release Windows Server 2016 Datacenter Edition

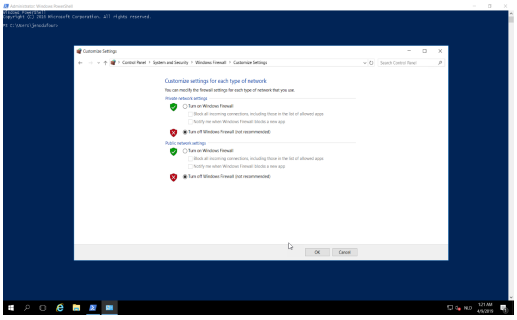
Disk layout

SAP EXE (E:) 128 GB
DB DISK (F:) 256 GB
TEMP SOFT (T:) 256 GB

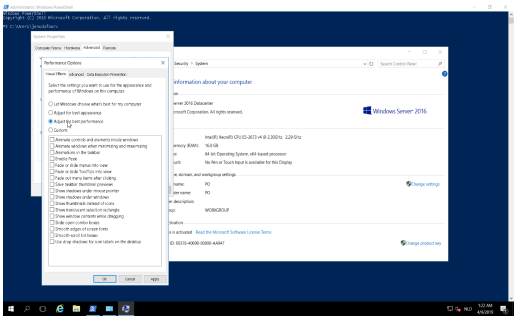
Windows preparations



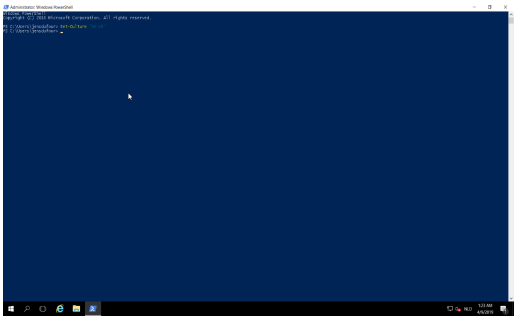
(a) Disable UAC



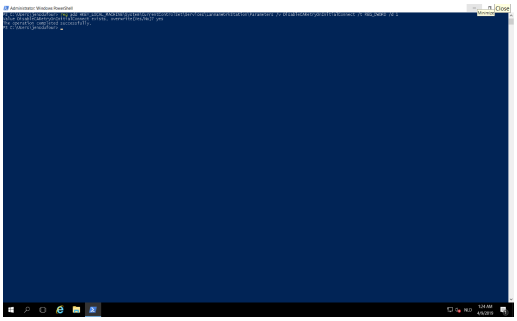
(b) Disable Firewall



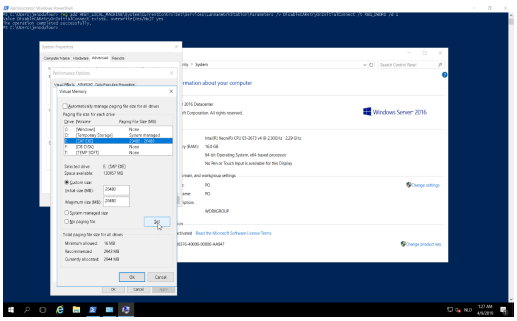
(c) Adjust visual effects



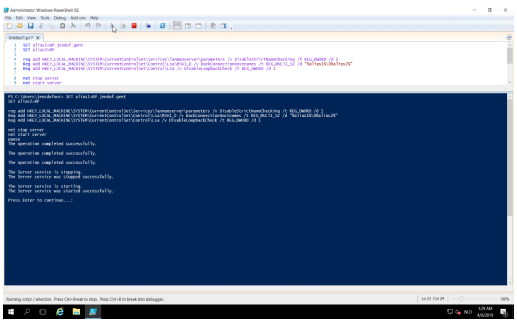
(d) Change system locale to EN



(e) Accessing time shares / file system



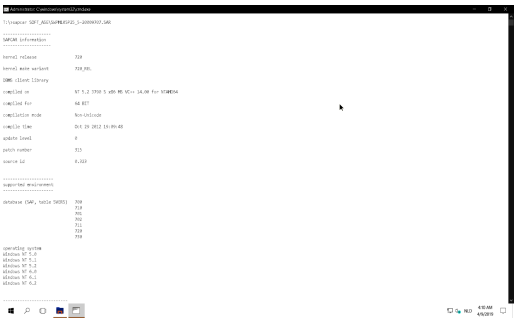
(f) Set paging file to 20480



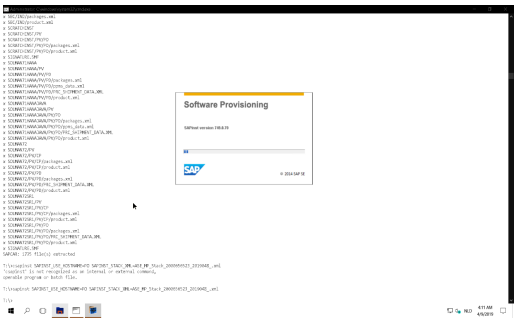
(g) Setting Virtual Host Names

Figure D.1: Preconditions for the installation of the SAP stack

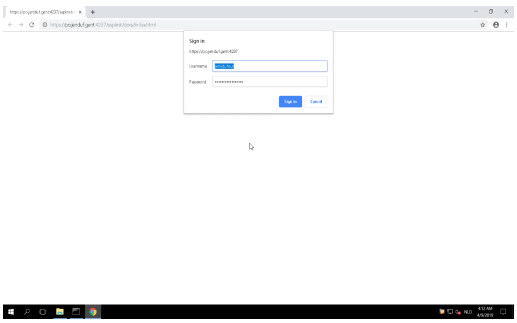
D.2.2 Installation



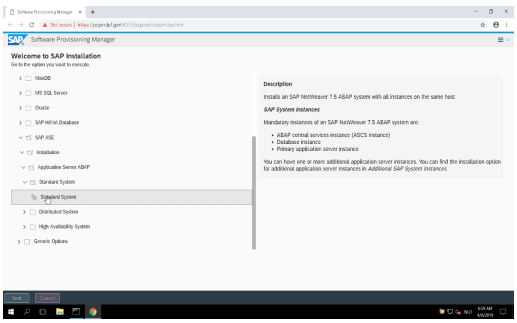
(a) Extract the software using 'SAPCAR'



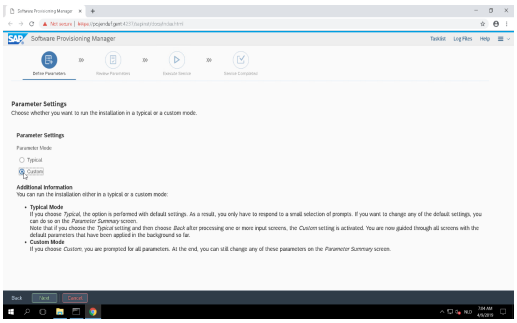
(b) Start the SPM



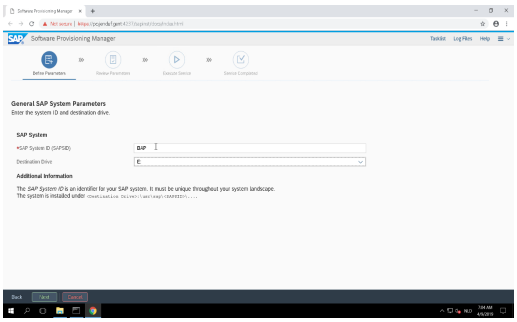
(c) Login as an administrator



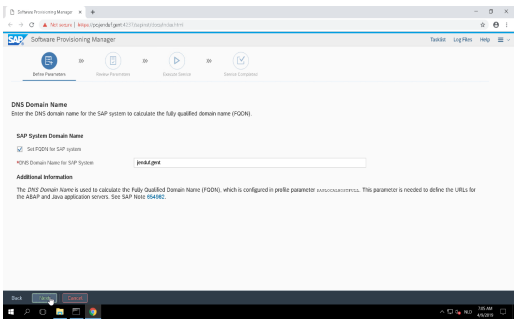
(d) Select the Standard System



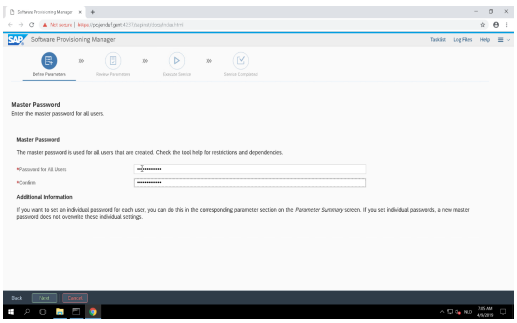
(e) Select the Custom Parameter



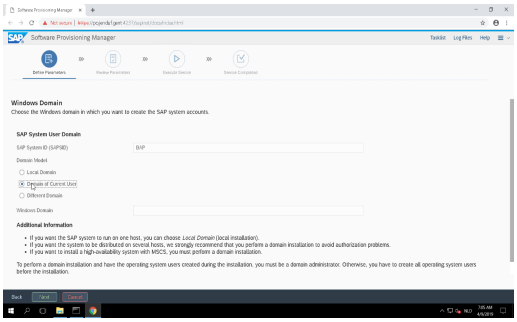
(f) Enter the general SAP System Parameters



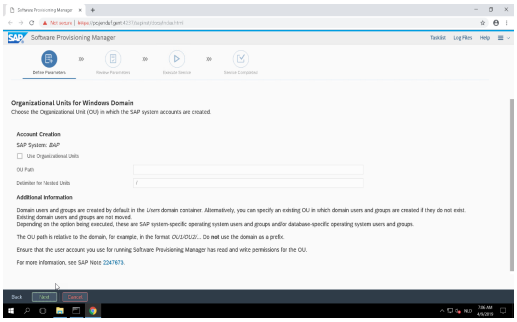
(g) Verify the DNS Domain Name



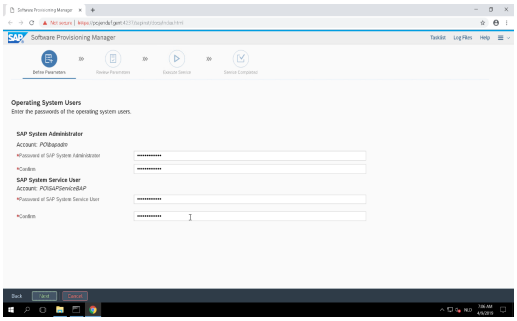
(h) Enter a Master Password



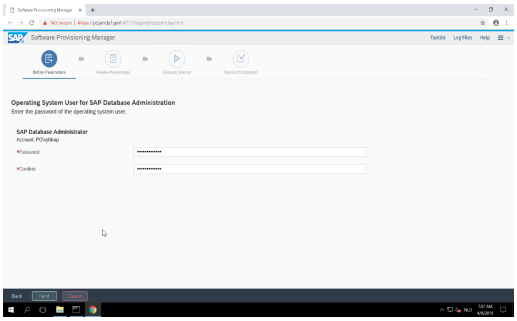
(i) Create the SAP system accounts to the domain of the current user



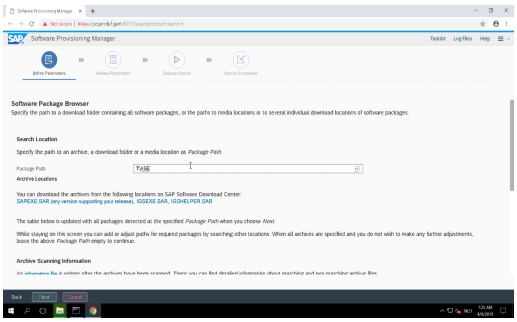
(j) Verify that no Organizational Units are used



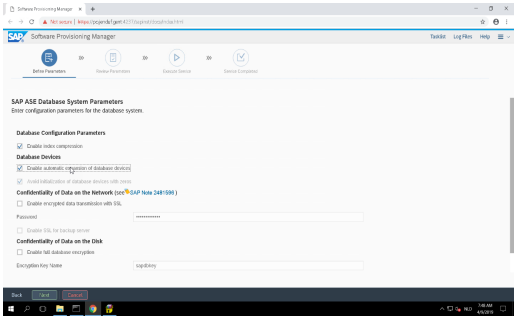
(k) Enter the System Administrator and Service User password



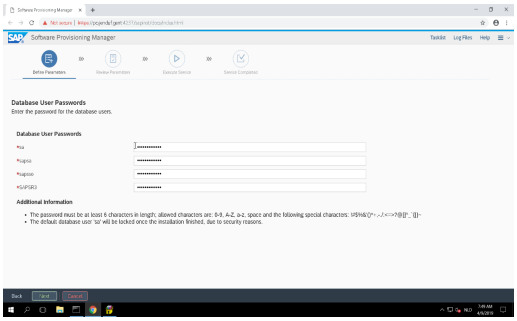
(l) Enter the SAP Database Administrator password



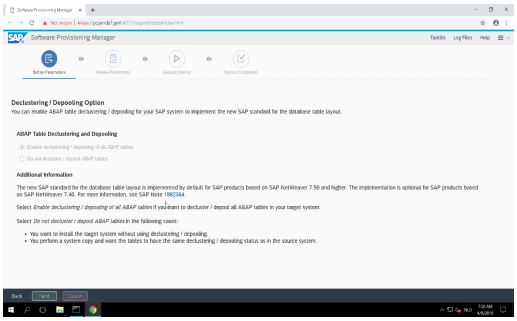
(m) Enter the Package Path



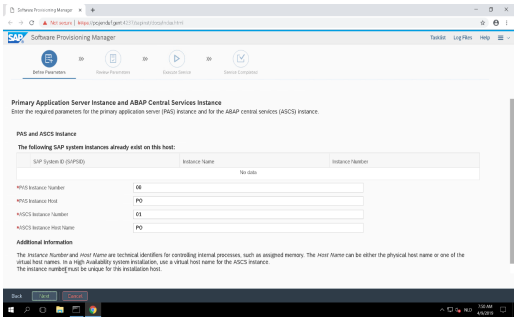
(n) Enable automatic expansion of database devices



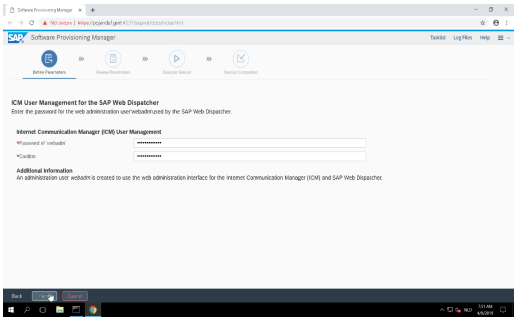
(o) Enter the Database User Passwords



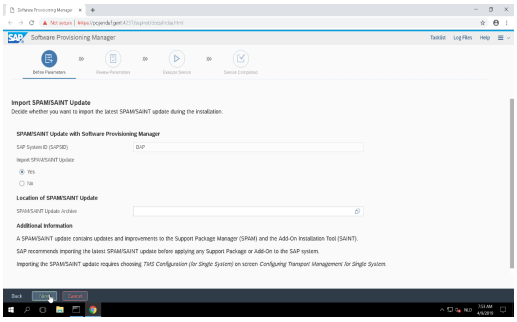
(p) Click next



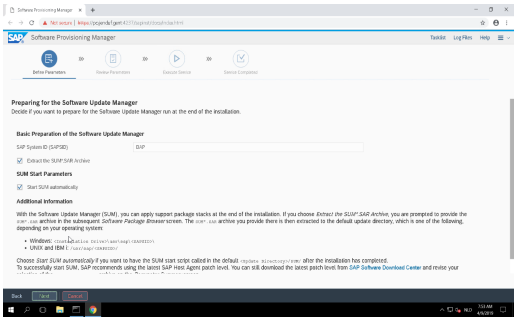
(q) Verify that no SAP system instances already exist



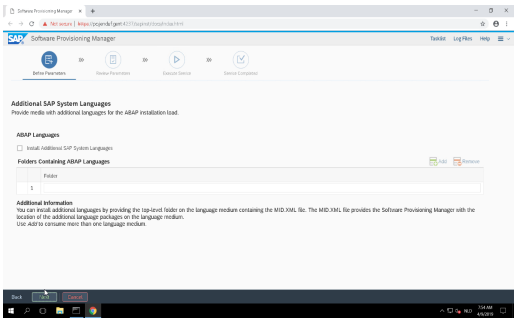
(r) Enter the webadmin password



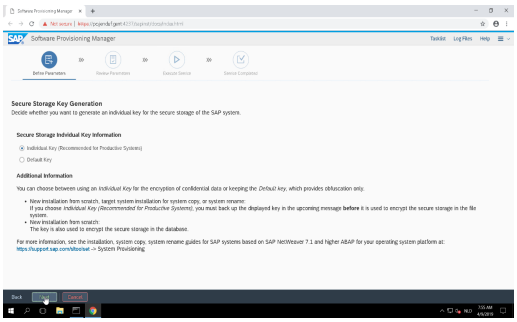
(s) Disable Import SPAM/SAINT Update



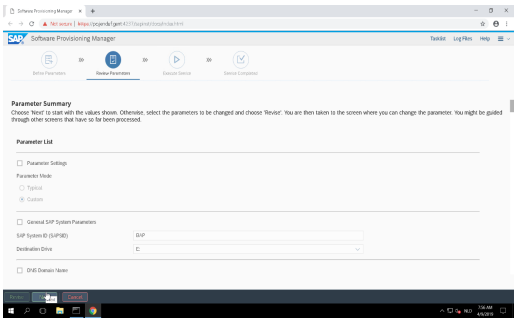
(t) Verify the Software Update Manager configuration



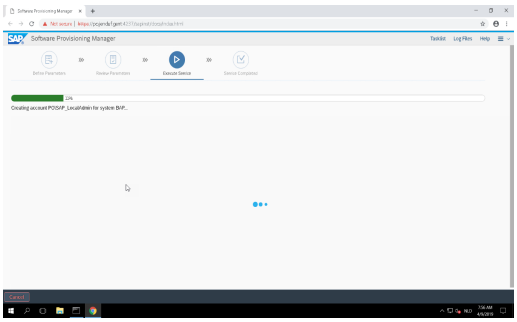
(u) Verify the installation of additional SAP System Languages



(v) Generate the Secure Storage Key



(w) Review all the Parameters in the summary

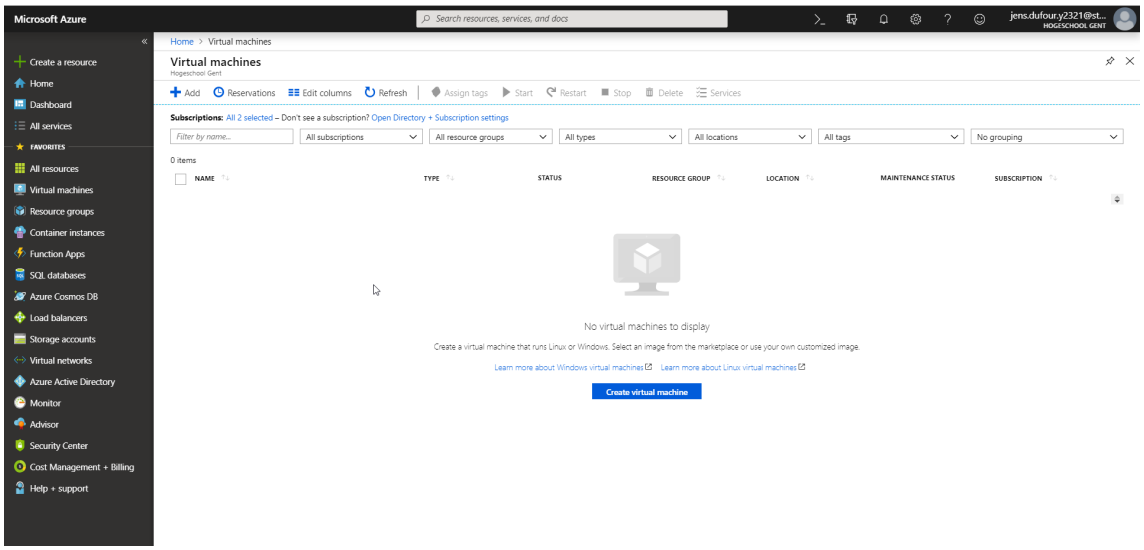


(x) The installation has successfully started

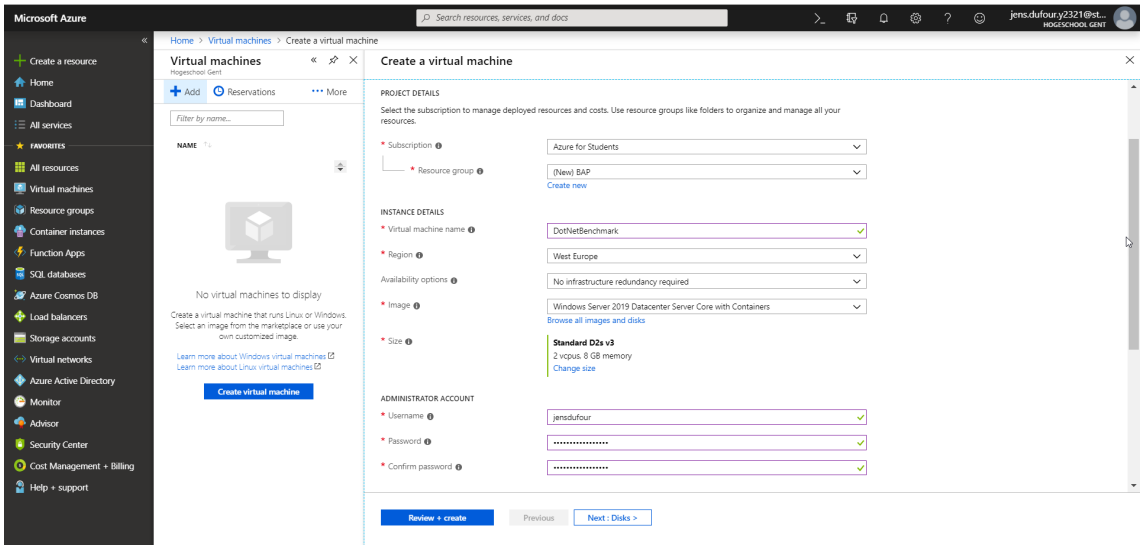
Figure D.2: Installation of the SAP application server with SyBase ASE DB

E. Creation of container environment

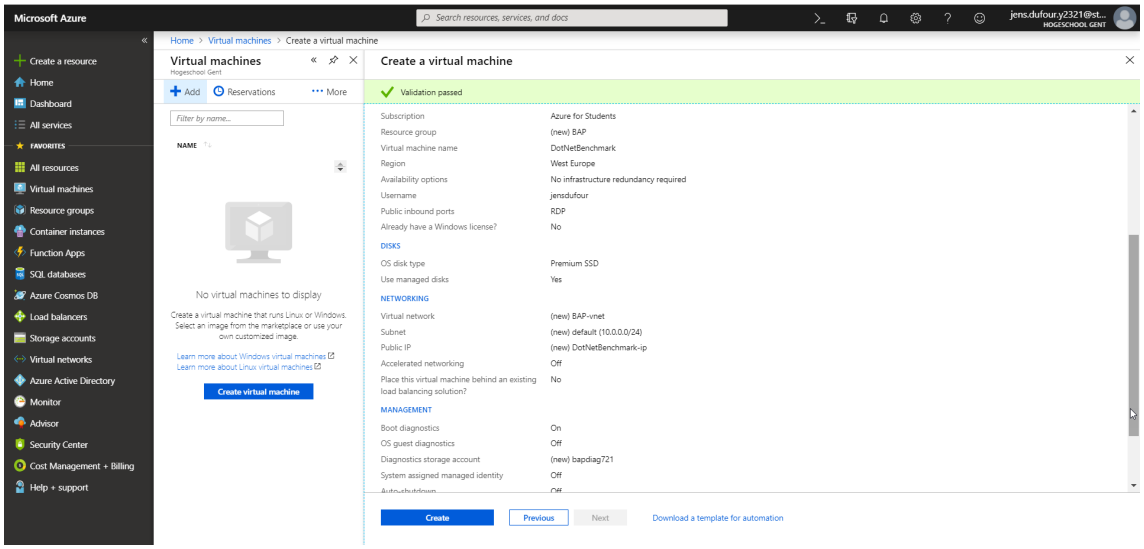
E.1 Creation of the Microsoft Azure VM



(a) Add a new VM through the Microsoft Azure Portal



(b) Fill in the required parameters and select the correct image



(c) Review the parameters and create the VM

Figure E.1: Creation of Microsoft Azure VM

E.2 Requirements for a nested VM

The following commands must be run through Powershell on the created VM to install the requirements needed to run a nested VM. This is necessary to run the containers isolated.

```
Install-WindowsFeature -Name Hyper-V
Install-WindowsFeature -Name Containers
Enable-WindowsOptionalFeature -Online -FeatureName
    Microsoft-Hyper-V -All
Enable-WindowsOptionalFeature -Online -FeatureName
    containers -All
```

E.3 Installation of Git

The following commands must be run through Powershell on the created VM to install Git. Git is necessary to clone the files needed to run the benchmarks.

```
Set-ExecutionPolicy Bypass -Scope Process -Force;iex ((New-
    Object System.Net.WebClient).DownloadString('https://
    chocolatey.org/install.ps1'))
choco install git -params '"/GitAndUnixToolsOnPath"' -y
refreshenv
```

E.4 Installation of Docker EE

The following commands must be run through Powershell on the created VM to install Docker EE.

```
Install-Module -Name DockerMsftProvider -Repository
    PSGallery -Force
Install-Package -Name docker -ProviderName
    DockerMsftProvider
Restart-Computer -Force
```

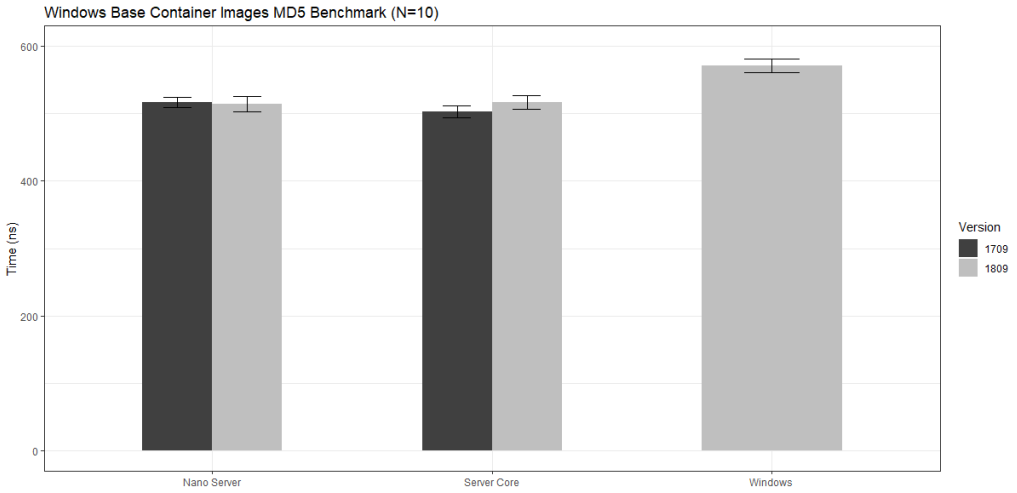
F. Benchmark data

F.1 Benchmark data

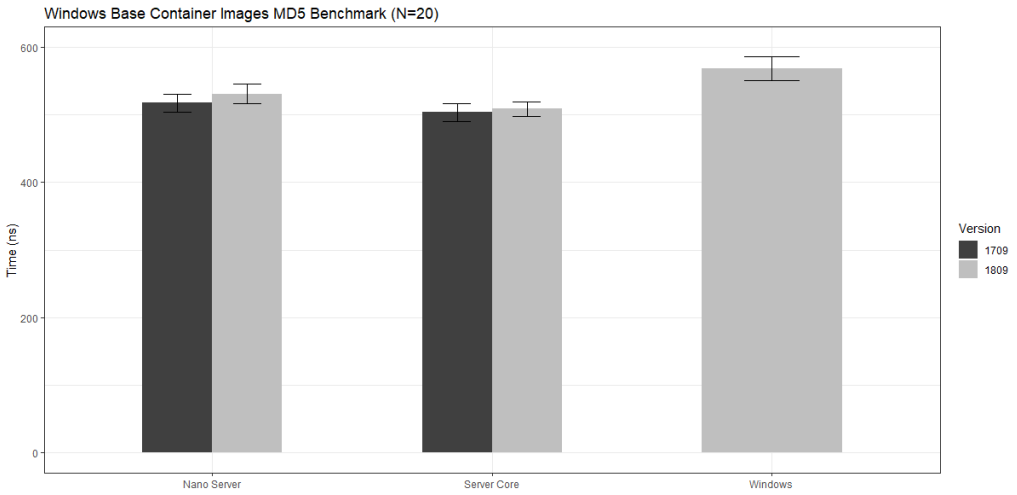
Server	Version	Method	N	Mean	Error	StdDev
Nano Server	1709	SHA256	10	769.900	11.909	9.945
Nano Server	1709	MD5	10	516.500	8.543	7.991
Nano Server	1809	SHA256	10	781.800	13.820	12.930
Nano Server	1809	MD5	10	513.700	10.950	11.240
Server Core	1709	SHA256	10	813.900	16.370	23.478
Server Core	1709	MD5	10	502.300	9.554	8.937
Server Core	1809	SHA256	10	777.900	13.352	18.275
Server Core	1809	MD5	10	516.500	9.911	9.734
Windows	1809	SHA256	10	854.200	16.730	20.543
Windows	1809	MD5	10	571.100	11.110	9.844
Nano Server	1709	SHA256	20	796.300	12.101	11.320
Nano Server	1709	MD5	20	517.400	10.550	13.465
Nano Server	1809	SHA256	20	797.800	16.060	18.490
Nano Server	1809	MD5	20	531.000	10.450	14.650
Server Core	1709	SHA256	20	772.400	14.251	11.901
Server Core	1709	MD5	20	503.400	9.842	12.798
Server Core	1809	SHA256	20	777.200	13.499	11.272
Server Core	1809	MD5	20	508.400	10.182	10.895
Windows	1809	SHA256	20	831.700	13.110	11.620
Windows	1809	MD5	20	568.700	15.020	17.882

Table F.1: Benchmarking results

F.2 Graphs

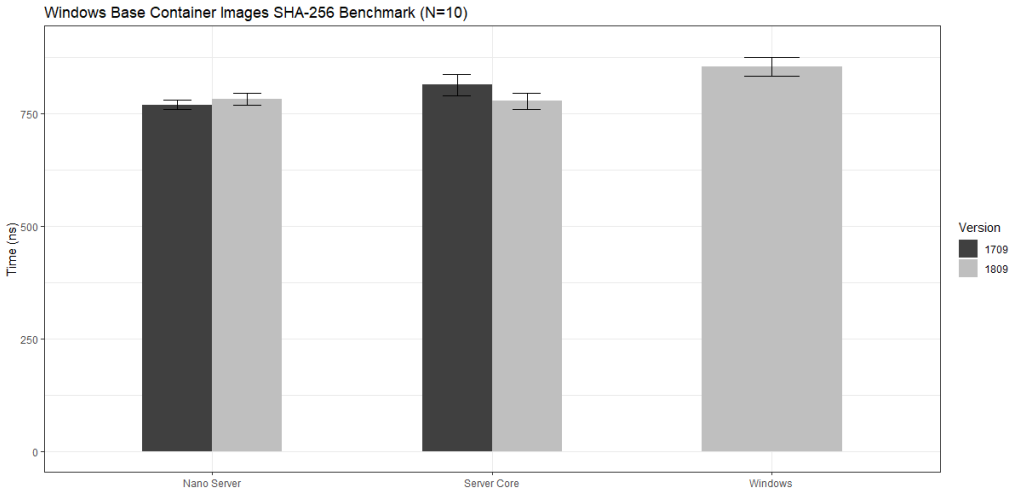


(a) Base Container Image MD5 benchmark (N=10)

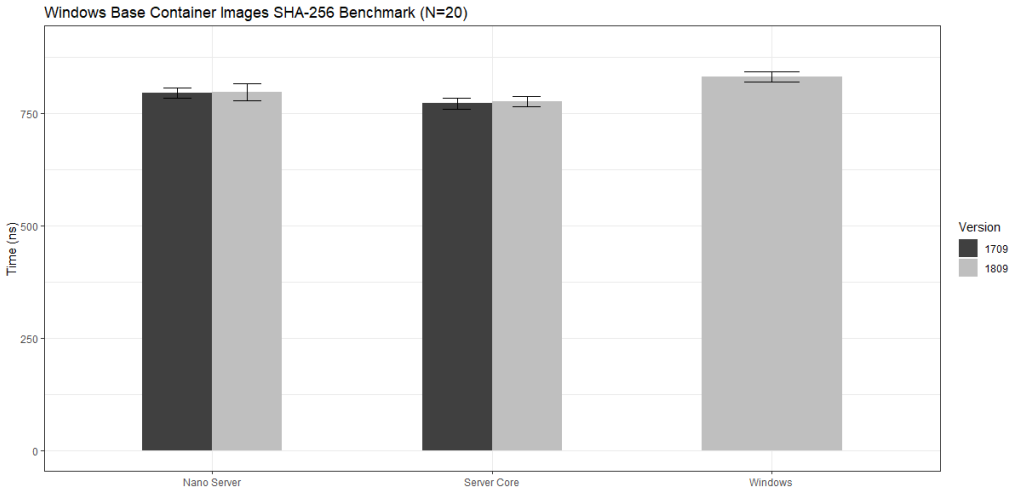


(b) Base Container Image MD5 benchmark (N=20)

Figure F.1: Base Container Image MD5 benchmark



(a) Base Container Image SHA-256 benchmark (N=10)



(b) Base Container Image SHA-256 benchmark (N=20)

Figure F.2: Base Container Image SHA-256 benchmark

Bibliography

Akinshin, A., & Yakimets, M. (2019). BenchmarkDotNet. Retrieved from https://benchmarkdotnet.org/articles/overview.html

Aslaner, M. (2018). Protecting Windows Server with Windows Defender ATP. Retrieved from https://gxcuf89792.i.lithium.com/t5/image/serverpage/image-id/55539i467D9A8C7674CE11/image-size/large?v=1.0&px=999

Chappell, D. (2011). What is an Application Platform? Retrieved from http://www.davidchappell.com/writing/white_papers/What_is_an_Application_Platform-Chappell.pdf

Enkov, S., & Karavasilev, T. (2017). Benchmarking Hash Functions. In *TechSys 2017*. Retrieved from https://www.researchgate.net/profile/Tony_Karavasilev/publication/315359560_Benchmarking_Hash_Functions/links/59370ed90f7e9b374c1df6f1/Benchmarking-Hash-Functions.pdf?origin=publication_detail

Gallagher, E. (2018). Modern Desktop Deployment and Management Lab Kit. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/enterprise/modern-desktop-deployment-and-management-lab

Gantz, J., & Reinsel, D. (2012). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. *IDC iView*. Retrieved from https://www.emc-technology.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf

Gerend, J., Gries, W., Poggemeyer, L., Watumull, G., Hansen, A., Schonning, N., ... Nikolaev, K. (2018). What's new in Storage in Windows Server. Retrieved from https://docs.microsoft.com/en-us/windows-server/storage/whats-new-in-storage#storage-spaces-direct

Gerend, J., Poggemeyer, L., Plett, C., Bazarewsky, M. C., Lee, T., Iwer, L., & Four, J. D. (2018, December 21). What's new in Windows Server 2019. Retrieved from https://docs.microsoft.com/en-us/windows-server/get-started-19/whats-new-19

Haag, M. (2016). *HyperConverged Infrastructure For Dummies® VMware and Intel Special Edition* (E. Kuball, K. Mohr, R. Mengle, K. Hattan, & S. Shaik, Eds.). John Wiley & Sons, Inc. Retrieved from http://gu.dimensionsystems.com/wp-content/uploads/2017/09/VSAN-0130_Hyperconverged_Infrastructure_For_Dummies_VMware_and_Intel_Special_Edition.pdf

Hofmann, P., & Woods, D. (2010). Cloud Computing: The Limits of Public Clouds for Business Applications. *IEEE Internet Computing*, *14*(6), 90–93. doi:10.1109/mic.2010.136

Kreutz, D., Ramos, F. M., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, *103*(1), 14–76.

Mansfield-Devine, S. (2018). 2018 Data Breach Investigations Report: the year of ransomware. *Computer Fraud & Security*, *2018*(5), 4. doi:10.1016/s1361-3723(18)30040-x

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology. doi:10.6028/nist.sp.800-145

Microsoft Corporation. (n.d.). Microsoft Lifecycle Policy. Retrieved from https://support.microsoft.com/en-hk/lifecycle/search?alpha=Windows%20Server

Microsoft Corporation. (2019). Modern Desktop Deployment and Management Lab Kit. Retrieved from http://download.microsoft.com/download/5/6/D/56DCD85A-DCA4-4F8D-AF2E-2CAAB4CFD0DE/MDlab_1809_guides_v2.13.zip

Microsoft Windows Server Team. (2018). Introducing Windows Server 2019 now available in preview. Retrieved from https://cloudblogs.microsoft.com/windowsserver/2018/03/20/introducing-windows-server-2019-now-available-in-preview/

Modadugu, N., & Rescorla, E. (2004). The Design and Implementation of Datagram TLS. In *In Proc. NDSS*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.6613&rep=rep1&type=pdf

Musto, S. (2017). *The Total Economic Impact Of Microsoft Windows Defender Advanced Threat Protection*. Forrester. [Online; accessed February 15, 2019]. Retrieved from http://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-Forrester-TEI-Report-WDATP.pdf

Naeem, M., Mahar, H., Memon, F., Siddique, M., & Rauf, A. (2016). An Overview of Virtualization & Cloud Computing. *Science International Journal Lahore*. Retrieved from https://www.researchgate.net/publication/307905618_AN_OVERVIEW_OF_VIRTUALIZATION_CLOUD_COMPUTING

Ng, F., Graham, C., Anderson, E., Ackerman, D., Dorosh, M., Nag, S., … Gupta, N. (2018). *Forecast: Public Cloud Services, Worldwide, 2016-2022, 2Q18 Update*. Gartner. Retrieved from https://www.gartner.com/doc/3884473/forecast-public-cloud-services-worldwide

Pacquer, K., Poggemeyer, L., & Plett, C. (2018, December 19). Server Core App Compatibility Feature on Demand (FOD). Retrieved from https://docs.microsoft.com/nl-be/windows-server/get-started-19/install-fod-19

Ren, K., Wang, C., & Wang, Q. (2012). Security Challenges for the Public Cloud. *IEEE Internet Computing*, *16*(1), 69–73. doi:10.1109/mic.2012.14

Sarna, D. E. Y. (2010, November 26). *Implementing and Developing Cloud Computing Applications*. [Online; accessed February 14, 2019]. Auerbach Publications. Re-

trieved from https://www.ebook.de/de/product/11419455/david_e_y_sarna_implementing_and_developing_cloud_computing_applications.html

Security Space. (2019). OS/Linux Distributions using Apache. Retrieved from https://secure1.securityspace.com/s_survey/data/man.201901/apacheos.html

Shailendra, C. (2015, September). *Infosys migrates from SQL server 2012 to SQL 2016*. Microsoft. Retrieved from https://ms-f1-sites-01-cdn.azureedge.net/docs/stories/infosyssql/resources/aa28c7fe-408e-421f-baa7-8e0bc9db1c00/infosys_sql_case_study.pdf

Shalunov, S., Hazel, G., Iyengar, J., & Kuehlewind, M. (2012). *Low Extra Delay Background Transport (LEDBAT)*. Internet Engineering Task Force. doi:10.17487/rfc6817

Shin, S., Xu, L., Hong, S., & Gu, G. (2016). Enhancing Network Security through Software Defined Networking (SDN). In *2016 25th International Conference on Computer Communication and Networks (ICCCN)*. doi:10.1109/icccn.2016.7568520

Short, P. (2016). Hyper-V Technology Overview. Retrieved from https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview

Singh, A., & Shah, M. (2019). *Introduction to Microsoft Windows Server 2019*. Retrieved from https://support.microsoft.com/nl-be/help/4487177/introduction-to-microsoft-windows-server-2019

Singh, S., & Jangwal, T. (2012). Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues. *International Journal of Computer Science and Information Technology*, *4*(2), 17–31. doi:10.5121/ijcsit.2012.4202

Tsai, P. (2016). Server Virtualization and OS Trends. Retrieved from https://community.spiceworks.com/networking/articles/2462-server-virtualization-and-os-trends

Washburn, N., Rowland, H., Woolslayer, J., & Poggemeyer, L. (2018). What Azure integration options are there with Windows Admin Center? Retrieved from https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/azure-integration-options

Woolslayer, J. (2018). *Windows Admin Center Server Management Reimagened*. Retrieved from https://github.com/MicrosoftDocs/windowsserverdocs/raw/master/WindowsServerDocs/manage/windows-admin-center/media/WindowsAdminCenter1809Poster.pdf

Yao, Q., Han, X., Ma, X.-K., Xue, Y.-F., Chen, Y.-J., & Li, J.-S. (2014). Cloud-Based Hospital Information System as a Service for Grassroots Healthcare Institutions. *Journal of Medical Systems*, *38*(9). doi:10.1007/s10916-014-0104-3