Active Directory and Azure AD Connect

KCoder

Prepared by:
[insert your name]

Objective

One of the key aspects of deploying Microsoft 365 is the ability to provide users a single identity and ensuring it is properly configured. When this is accomplished, users can access seamlessly resources that are on-premises and in Microsoft 365 environment. Otherwise, users will have to use multiple accounts depending on where the resources are hosted. In this deliverable, you will use Microsoft Azure AD Connect tool to sync on-premises Active Directory to Azure AD. First, you will install Windows Server 2019 in a virtual environment and create an Active Directory Forest. Second, you will install and configure the Azure AD Sync tool. Finally, you will show the accounts that are synced to the Microsoft 365 Tenant.

Part 1: Install Windows Server 2019

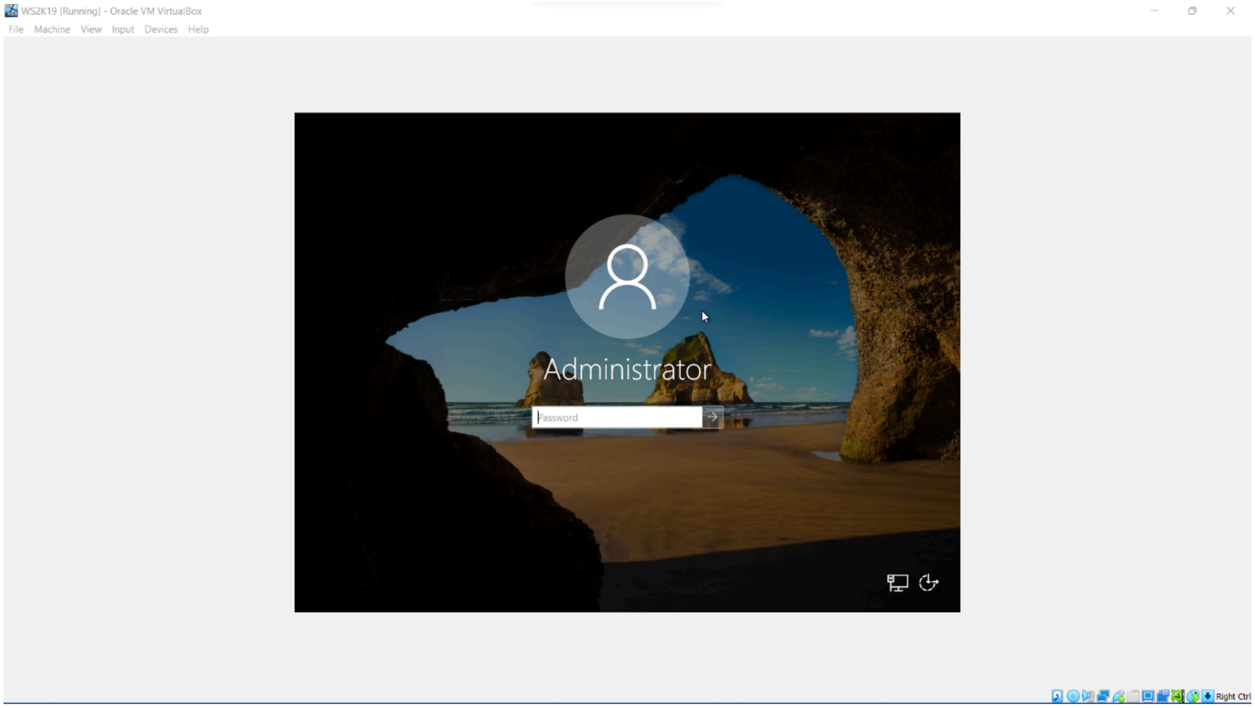
The recommended format is to provide screenshots incorporated within the written narrative. No external sources are required for this phase of the project; however, the screenshots must be your own. ***Screenshots from external sources are not permitted.***

Feel free to use Hyper-V, Oracle Virtualbox, or VMware workstation to install Windows Server 2019 as a virtual machine. To request VMware, please email your professor.

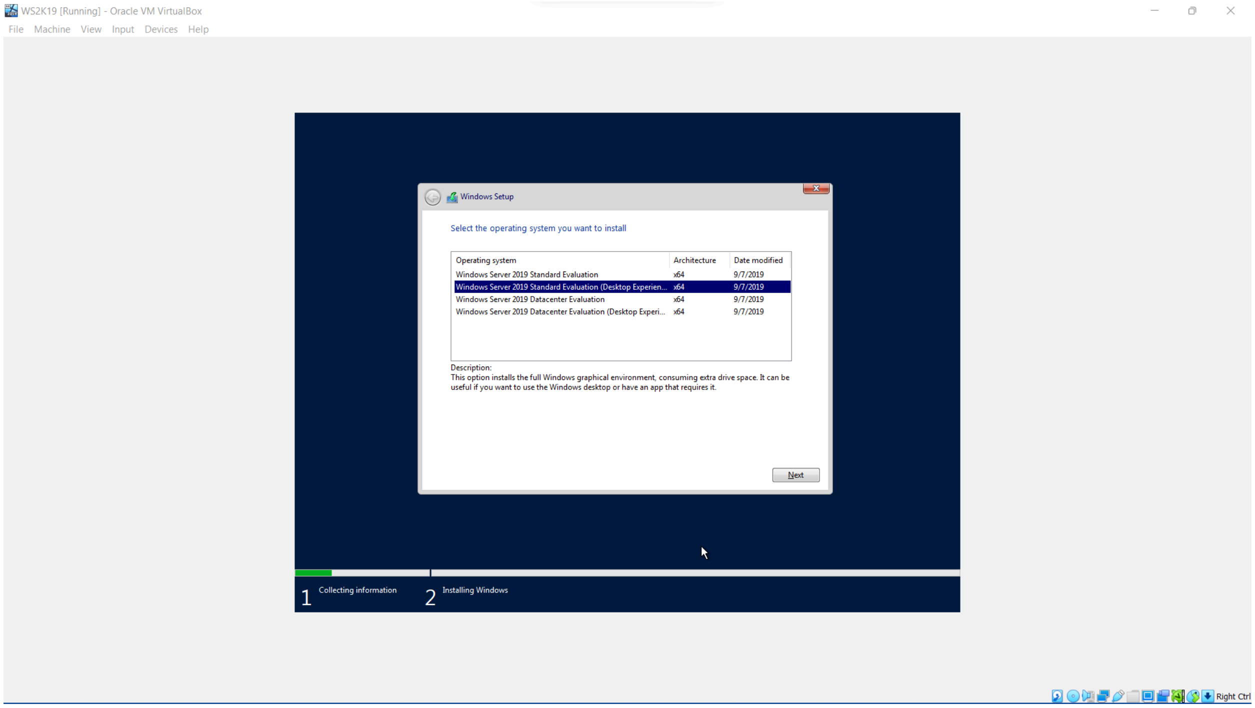
Note: It is not necessary to provide screenshots of the installation or configuration of virtualization software.

Plan: Windows Server 2019 Active Directory

1. Step 1 - Windows Server 2019 Screenshot


WS2K19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator
Password
Right Ctrl

2. Step 2 - Select the operating system to install (Choose the Standard Desktop Experience version)

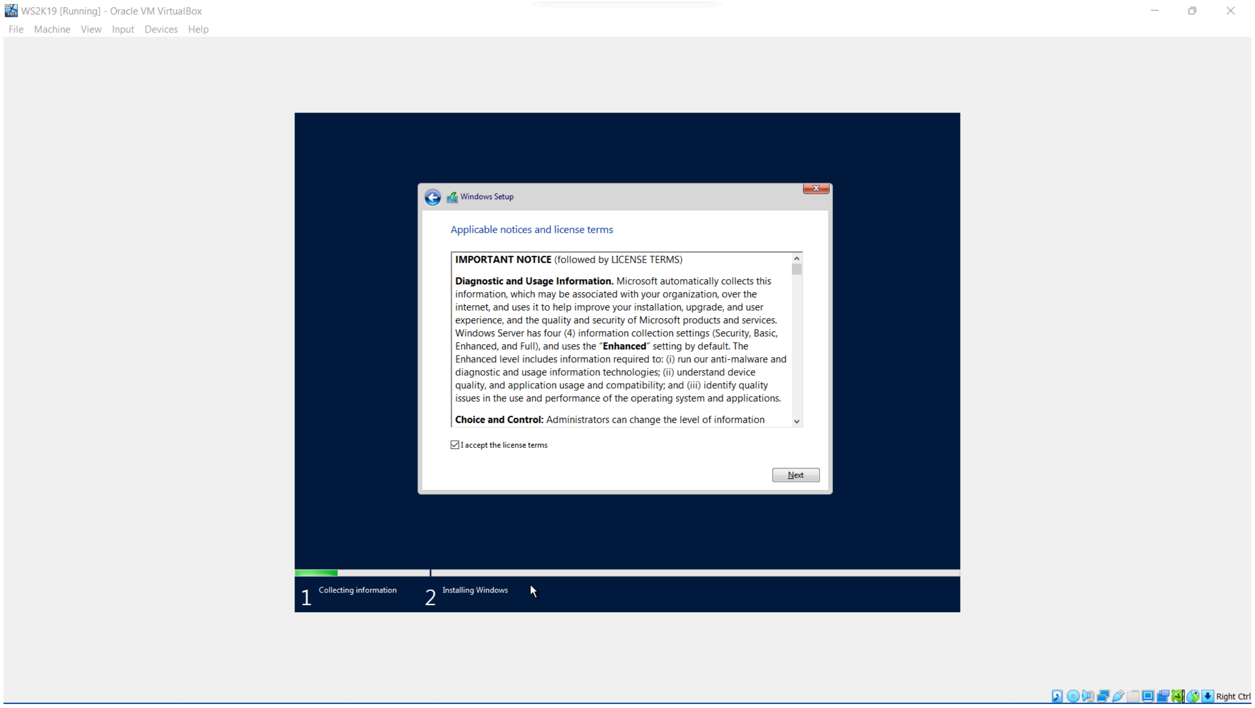

WS2K19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Setup
Next
1 Collecting information
2 Installing Windows
Right Ctrl

Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2019 Standard Evaluation	x64	9/7/2019
Windows Server 2019 Standard Evaluation (Desktop Experien...	x64	9/7/2019
Windows Server 2019 Datacenter Evaluation	x64	9/7/2019
Windows Server 2019 Datacenter Evaluation (Desktop Experi...	x64	9/7/2019

Description:
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.

3. Step 3 - Applicable Notices and License Terms Screenshot


WS2K19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Setup
Next
1 Collecting information
2 Installing Windows
Right Ctrl

Applicable notices and license terms

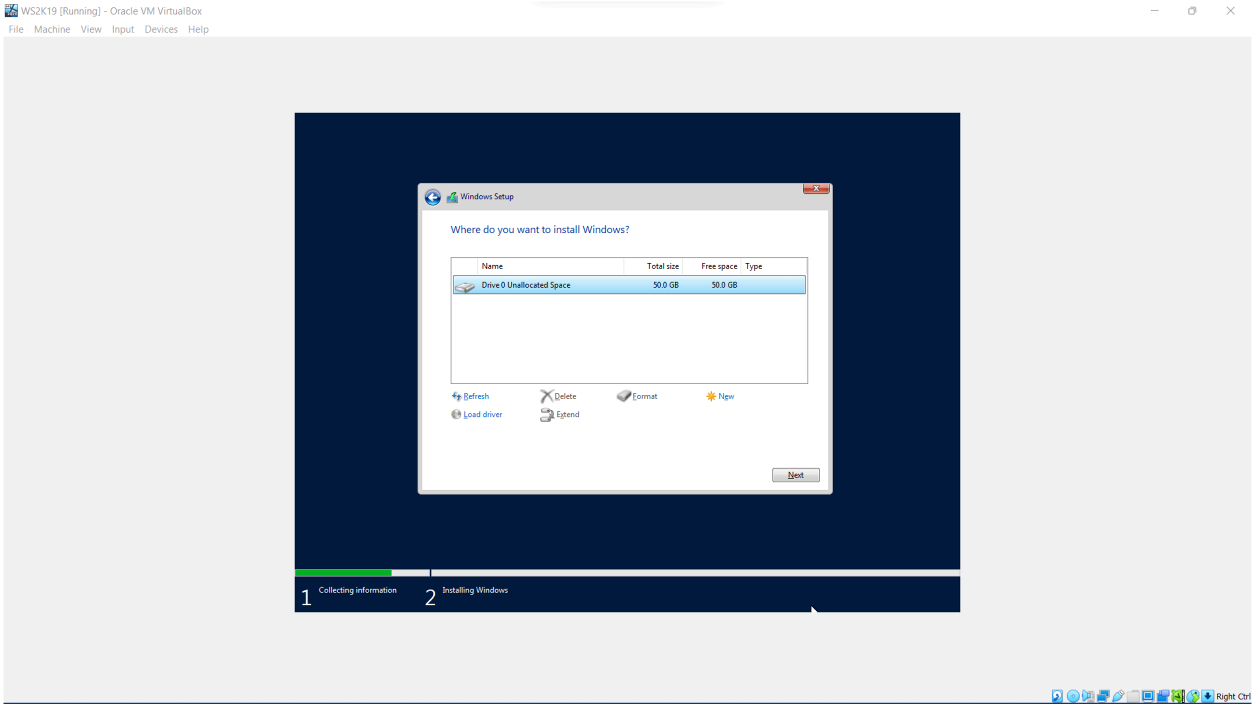
IMPORTANT NOTICE (followed by LICENSE TERMS)

Diagnostic and Usage Information. Microsoft automatically collects this information, which may be associated with your organization, over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Windows Server has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "**Enhanced**" setting by default. The Enhanced level includes information required to: (i) run our anti-malware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.

Choice and Control: Administrators can change the level of information

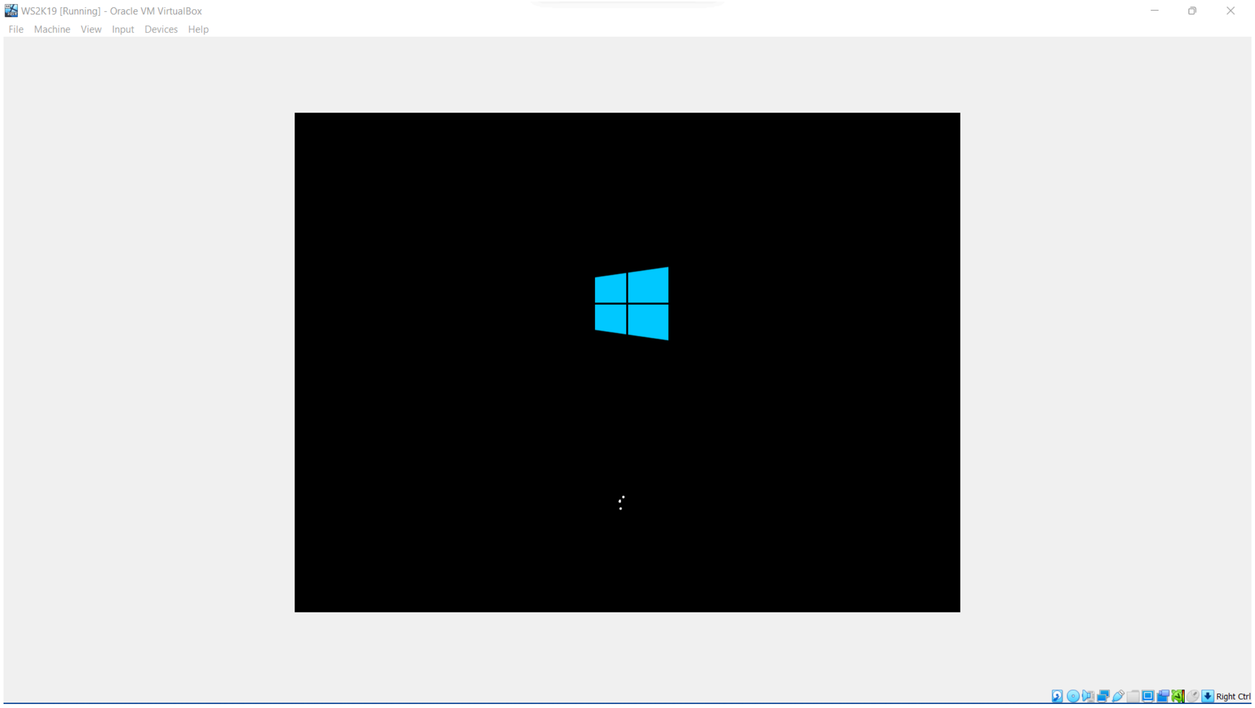
☑ I accept the license terms

4. Step 4 - Installing Windows Screenshot



Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	50.0 GB	50.0 GB	

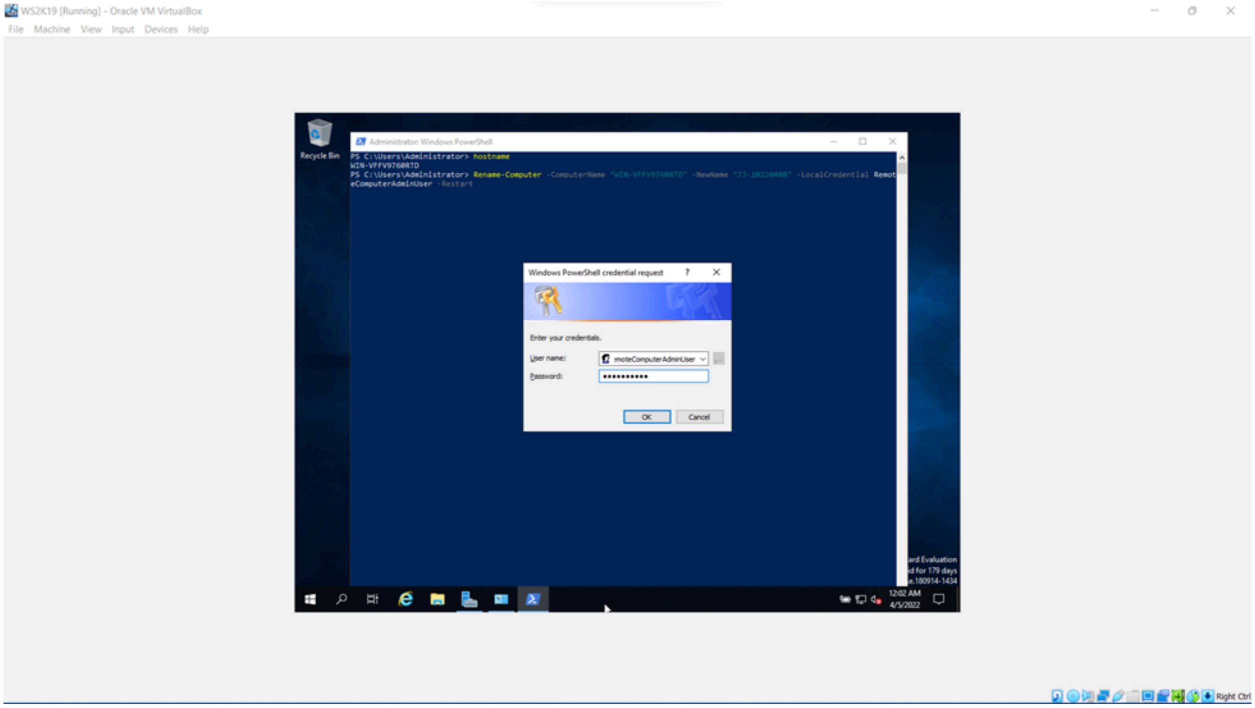

WS2K19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

Part 2: Install and Configure Active Directory

The recommended format is to provide screenshots incorporated within the written narrative. No external sources are required for this phase of the project; however, the screenshots must be your own. ***Screenshots from external sources are not permitted.***

Plan: Install Active Directory and Create Accounts

1. Step 1 – Change the computername to FirstNameInitialLastNameInitial-CurrentDate (i.e John Smith with the current date of 10/09/2020 would be JS-20201009, JJ-20220408) using PowerShell (Rename-Computer). Provide a screenshot of the PowerShell.



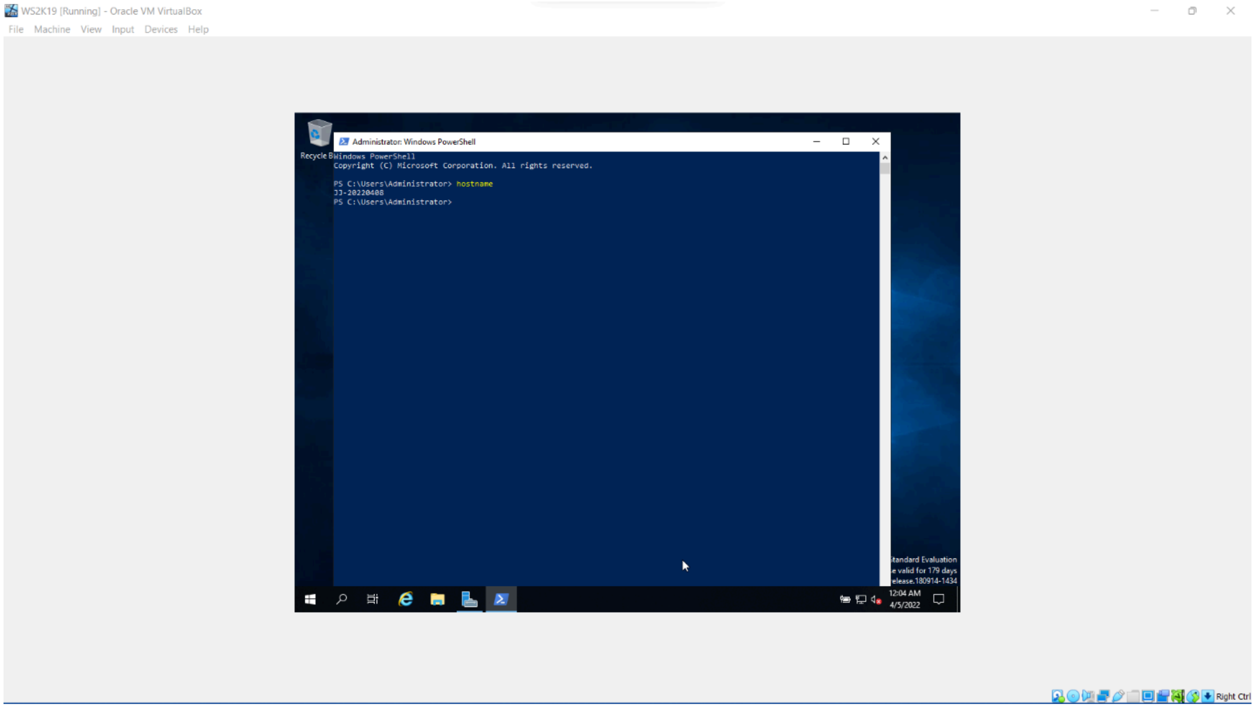
WS2K19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Administrator: Windows PowerShell
Windows PowerShell credential request
Enter your credentials.
User name:
Password:
OK
Cancel
Right Ctrl

```
PS C:\Users\Administrator> hostname
WIN-VFFV9760RTD
PS C:\Users\Administrator> Rename-Computer -ComputerName "WIN-VFFV9760RTD" -NewName "JJ-20220408" -LocalCredential Remot
eComputerAdminUser -Restart
```

User name: moteComputerAdminUser

Password: ••••••••••

ard Evaluation
id for 179 days
e.180914-1434
12:02 AM
4/5/2022

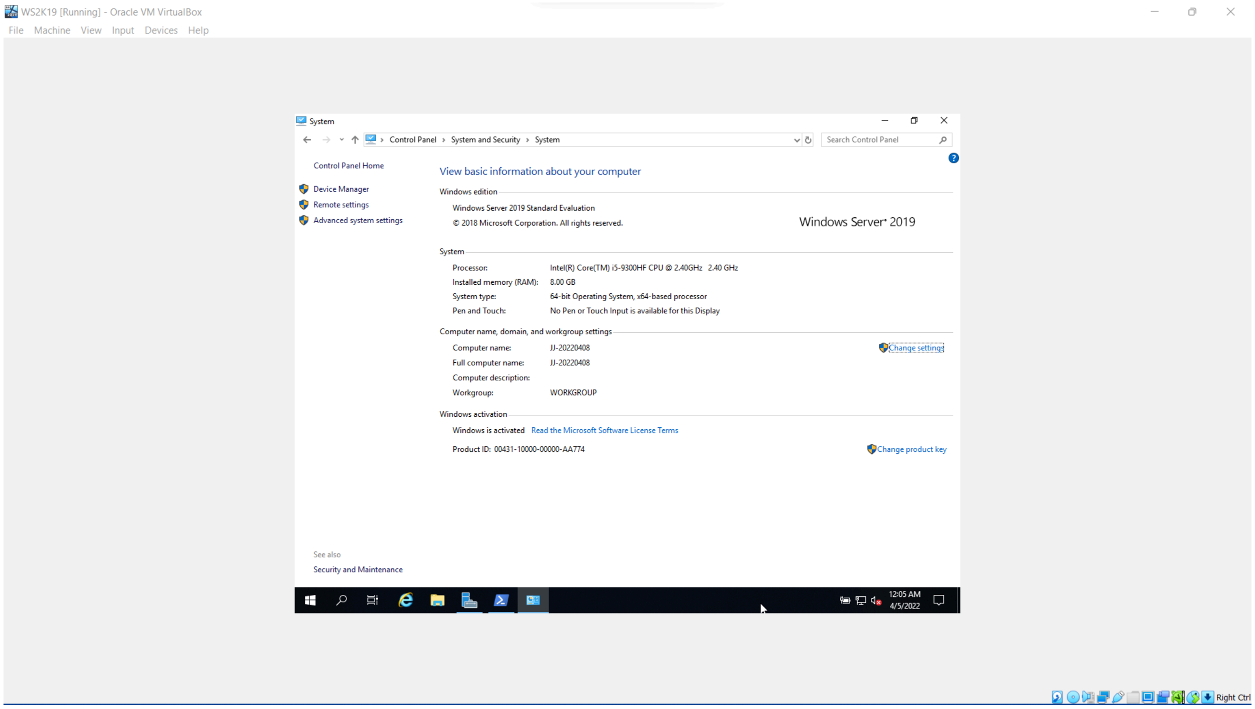


WS2K19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle B
Administrator: Windows PowerShell
Right Ctrl

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> hostname
JJ-20220408
PS C:\Users\Administrator>
```

tandard Evaluation
e valid for 179 days
elease.180914-1434
12:04 AM
4/5/2022

2. Step 2 – Computer Systems showing Domain Name Screenshot



View basic information about your computer

Windows edition

Windows Server 2019 Standard Evaluation

© 2018 Microsoft Corporation. All rights reserved.

Windows Server® 2019

System

Processor:	Intel(R) Core(TM) i5-9300HF CPU @ 2.40GHz 2.40 GHz
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	JJ-20220408
Full computer name:	JJ-20220408
Computer description:	
Workgroup:	WORKGROUP

Change settings

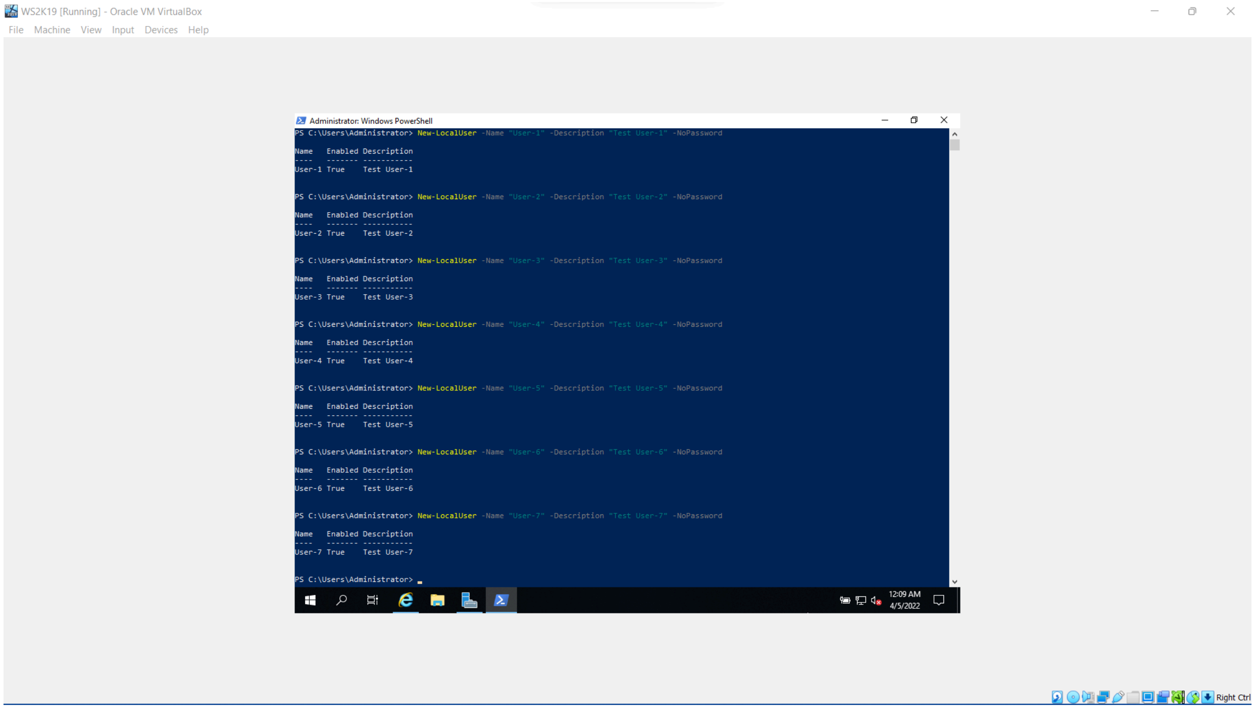
Windows activation

Windows is activated Read the Microsoft Software License Terms

Product ID: 00431-10000-00000-AA774

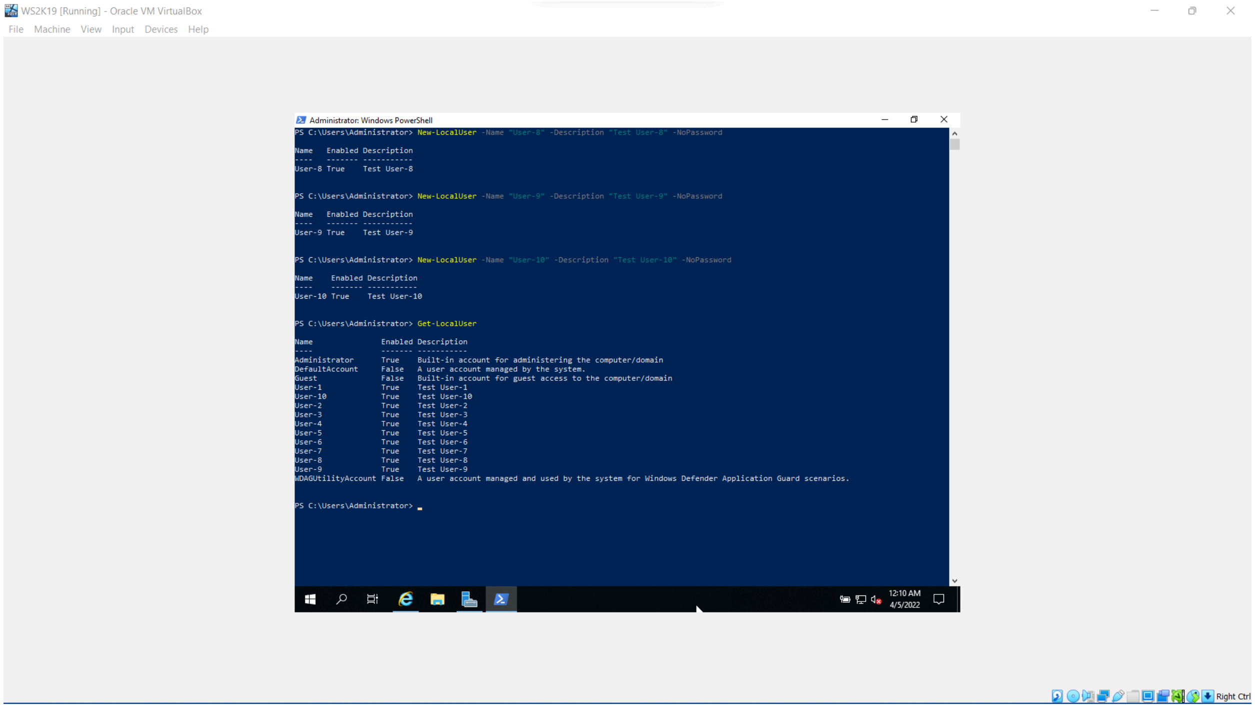
Change product key

3. Step 3 – Screenshot of PowerShell showing the creation of 10 user accounts.



WS2K19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
12:09 AM
4/5/2022
Right Ctrl

```
PS C:\Users\Administrator> New-LocalUser -Name "User-1" -Description "Test User-1" -NoPassword

Name   Enabled Description
----   ------- -----------
User-1 True    Test User-1


PS C:\Users\Administrator> New-LocalUser -Name "User-2" -Description "Test User-2" -NoPassword

Name   Enabled Description
----   ------- -----------
User-2 True    Test User-2


PS C:\Users\Administrator> New-LocalUser -Name "User-3" -Description "Test User-3" -NoPassword

Name   Enabled Description
----   ------- -----------
User-3 True    Test User-3


PS C:\Users\Administrator> New-LocalUser -Name "User-4" -Description "Test User-4" -NoPassword

Name   Enabled Description
----   ------- -----------
User-4 True    Test User-4


PS C:\Users\Administrator> New-LocalUser -Name "User-5" -Description "Test User-5" -NoPassword

Name   Enabled Description
----   ------- -----------
User-5 True    Test User-5


PS C:\Users\Administrator> New-LocalUser -Name "User-6" -Description "Test User-6" -NoPassword

Name   Enabled Description
----   ------- -----------
User-6 True    Test User-6


PS C:\Users\Administrator> New-LocalUser -Name "User-7" -Description "Test User-7" -NoPassword

Name   Enabled Description
----   ------- -----------
User-7 True    Test User-7


PS C:\Users\Administrator> _
```


WS2K19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
12:10 AM
4/5/2022
Right Ctrl

```
PS C:\Users\Administrator> New-LocalUser -Name "User-8" -Description "Test User-8" -NoPassword

Name   Enabled Description
----   ------- -----------
User-8 True    Test User-8


PS C:\Users\Administrator> New-LocalUser -Name "User-9" -Description "Test User-9" -NoPassword

Name   Enabled Description
----   ------- -----------
User-9 True    Test User-9


PS C:\Users\Administrator> New-LocalUser -Name "User-10" -Description "Test User-10" -NoPassword

Name    Enabled Description
----    ------- -----------
User-10 True    Test User-10


PS C:\Users\Administrator> Get-LocalUser

Name               Enabled Description
----               ------- -----------
Administrator      True    Built-in account for administering the computer/domain
DefaultAccount     False   A user account managed by the system.
Guest              False   Built-in account for guest access to the computer/domain
User-1             True    Test User-1
User-10            True    Test User-10
User-2             True    Test User-2
User-3             True    Test User-3
User-4             True    Test User-4
User-5             True    Test User-5
User-6             True    Test User-6
User-7             True    Test User-7
User-8             True    Test User-8
User-9             True    Test User-9
WDAGUtilityAccount False   A user account managed and used by the system for Windows Defender Application Guard scenarios.


PS C:\Users\Administrator> _
```

Part 3: Install and Configure Azure Active Directory

The recommended format is to provide screenshots incorporated within the written narrative. No external sources are required for this phase of the project; however, the screenshots must be your own. ***Screenshots from external sources are not permitted.***

Plan: Install and Configure Azure Active Directory Connect

1. Step 1 – Screenshot of user accounts in Azure AD.

Part 4: Azure AD Connect Health

The Opportunity: Azure AD Connect Health

- Write a few paragraphs on the what is Azure AD Connect Health and its importance. There are additional tasks that be completed when configuring Azure Active Directory Connect (see screenshot below). Choose two options available and explain their importance.

Azure AD Connect is an on-premises Microsoft application that's designed to meet and accomplish your hybrid identity goals. If you're evaluating how to best meet your goals, you should also consider the cloud-managed solution Azure AD Connect cloud sync.

Azure Active Directory (Azure AD) Connect Health provides robust monitoring of your on-premises identity infrastructure. It enables you to maintain a reliable connection to Microsoft 365 and Microsoft Online Services. This reliability is achieved by providing monitoring capabilities for your key identity components. Also, it makes the key data points about these components easily accessible.

The information is presented in the Azure AD Connect Health portal. Use the Azure AD Connect Health portal to view alerts, performance monitoring, usage analytics, and other information. Azure AD Connect Health enables the single lens of health for your key identity components in one place.

Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources. Users and organizations can take advantage of:

- Users can use a single identity to access on-premises applications and cloud services such as Microsoft 365.
- Single tool to provide an easy deployment experience for synchronization and sign-in.
- Provides the newest capabilities for your scenarios. Azure AD Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync. For more information, see Hybrid Identity directory integration tools comparison.

Features of Azure AD Connect

PRIVACY SETTINGS

Improve user privacy for Azure AD Connect installations in two ways

- Upon request, extract data for a person and remove data from that person from the installations
- Ensure no data is retained beyond 48 hours.

The Azure AD Connect team recommends the second option since it is much easier to implement and maintain.

An Azure AD Connect sync server stores the following user privacy data:

Data about a person in the Azure AD Connect database

Data in the Windows Event log files that may contain information about a person

Data in the Azure AD Connect installation log files that may contain about a person

Azure AD Connect customers should use the following guidelines when removing user data:

Delete the contents of the folder that contains the Azure AD Connect installation log files on a regular basis – at least every 48 hours

This product may also create Event Logs. To learn more about Event Logs logs, please see the documentation here.

Data about a person is automatically removed from the Azure AD Connect database when that person's data is removed from the source system where it originated from. No specific action from administrators is required to be GDPR compliant. However, it does require that the Azure AD Connect data is synced with your data source at least every two days.

CONFIGURING STAGING MODE

Staging mode can be used for several scenarios, including:

High availability.

Test and deploy new configuration changes.

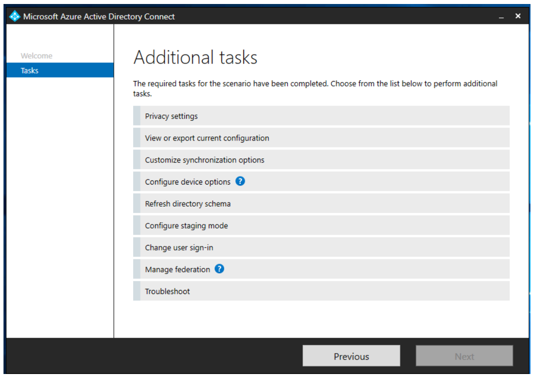
Introduce a new server and decommission the old.

During installation, you can select the server to be in staging mode. This action makes the server active for import and synchronization, but it does not run any exports. A server in staging mode is not running password sync or password writeback, even if you selected these features during installation. When you disable staging mode, the server starts exporting, enables password sync, and enables password writeback.

You can still force an export by using the synchronization service manager.

A server in staging mode continues to receive changes from Active Directory and Azure AD and can quickly take over the responsibilities of another server in the event of a failure. If you make configuration changes to your primary server, it is your responsibility to make the same changes to the server in staging mode.

For those of you with knowledge of older sync technologies, the staging mode is different since the server has its own SQL database. This architecture allows the staging mode server to be located in a different datacenter.



Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

- Privacy settings
- View or export current configuration
- Customize synchronization options
- Configure device options
- Refresh directory schema
- Configure staging mode
- Change user sign-in
- Manage federation
- Troubleshoot

Resources

Windows Server 2019 Download:
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019

Install Windows Server 2019 on Hyper-V:
https://www.itechguides.com/install-windows-server-2019-on-hyper-v/

Install Windows Server 2019 on VM:
https://www.sysnettechsolutions.com/en/install-windows-server-2019-vmware-workstation-14/

Install Windows Server 2019 on Oracle VirtualBox:
https://www.sysnettechsolutions.com/en/install-windows-server-2019-oracle-vm-virtualbox/

Download Azure AD Connect: https://www.microsoft.com/en-us/download/details.aspx?id=47594

Install Azure AD Connect:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom