Hewlett Packard Enterprise

Reference guide

Check if the document is available in the language of your choice.

HPE SMALL BUSINESS SOLUTIONS DEPLOYMENT GUIDE

Microsoft Windows-based solutions

CONTENTS

Notices

Revision history

Publication date	Edition	Summary of changes
Apr 2019	1	Initial publication of the HPE Small Business Solutions Deployment Guide
Jun 2019	2	Added HPE RDX Removable Disk Backup System installation instructions
Jul 2019	3	Included Microsoft Windows Server 2019
Aug 2019	4	New chapter on HPE Small Business Solutions for Hyperconverged Infrastructure (HCI) with Microsoft Storage Spaces Direct
Sept 2019	5	Revision on Rapid Setup to include new features and functions
Oct 2019	6	Revision to include steps for migrating to Microsoft Windows 2019 in Appendix A
Feb 2020	7	Added section on protection option for Microsoft Hyper-V server and virtual machines
Apr 2020	8	New chapter on HPE Small Business Solutions for Small Office Deployment

OVERVIEW

Purpose

HPE Small Business Solutions are part of the HPE SMB Offers portfolio.[1] They are based on HPE ProLiant Gen10 servers that are equipped to meet the needs of small businesses for a variety of company sizes and use cases. They are also the foundational on-premises component of HPE Small Business Solutions used in hybrid cloud deployments.

The **HPE Small Business Solutions Deployment Guide for Microsoft Windows-based solutions** is intended to provide SMBs with general, high-level instructions for deploying HPE Small Business Solutions.

Disclaimer

This guide provides basic setup instructions for deploying HPE Small Business Solutions. There are many additional business considerations that are outside of the scope of this document, such as security policies, organizational user and group structure, regulatory compliance, etc. This guide is good for both Microsoft Windows Server 2016 and 2019 but there may be instances where there are subtle differences in the wording or order of the prompts.

HPE claims no liability as a result of implementing procedures in this guide.

Audience

Important: The intended audience is IT professionals who are familiar with deploying small to midsized business (SMB) technology solutions on variety of operating systems (OSs) in both on-premises and cloud environments.

Organization

This HPE Small Business Solution Deployment Guide is a “living document” that is periodically updated as new HPE Small Business Solutions are brought to market and new configurations and use cases are developed.

The guide will help customers and partners quickly deploy HPE Small Business Solutions by providing high-level, step-by-step guidance that is grouped into several modules that follow the typical workflow stages of deploying a server in an SMB environment.

[1] HPE Small Business Solution offers are regionally released as “Smart Buy Express Offers” in the U.S. and Canada, “Top Value Offers” in Europe, and “Intelligent Buy Offers” in Asia Pacific and Japan.

INITIAL SETUP

Hardware configuration and operating system installation

This chapter addresses the initial hardware configuration and setup of HPE Small Business Solutions running Windows Server 2016 and 2019 operating system.

NOTE

If you are installing or deploying an HPE Small Business Solution for HCI (Hyperconverged Infrastructure) with Microsoft Storage Spaces Direct, skip this section and go directly to the HPE Small Business Solutions for HCI with Microsoft Storage Spaces Direct section of this guide.

Pre-deployment planning

Deploying an HPE Small Business Solution is relatively simple. Following these four pre-deployment preparation steps will help lead to a smooth deployment.

1. **Plan to choose one of four RAID controller setup methods:**

   a. **Rapid Setup (Integrated with Intelligent Provisioning version 3.31 or later)** is the latest automated setup feature that is embedded in HPE ProLiant Gen10 and later, 300 series and below servers. It greatly decreases the time required to deploy the server, simplifies initial controller and disk drive configuration, and automates OS installation. HPE recommends this method for most HPE Small Business Solution server deployments and is discussed in detail in the following section.

   NOTE

   HPE Integrated Lights Out (iLO) version 5 is a pre-requisite for HPE Intelligent Provisioning version 3.31 and Rapid Setup. Verify your HPE ProLiant Gen10 or later server has HPE Intelligent Provisioning version 3.31 or later firmware, and perform a firmware upgrade if necessary, before proceeding with the Rapid Setup installation steps described below

   NOTE

   The new HPE ProLiant MicroServer Gen10 Plus features iLO 5 and as such can be configured using Rapid Setup as described in this document. Note however the previous model—HPE ProLiant MicroServer Gen10—does not have iLO and thus cannot have the integrated version of Rapid Setup described in this document. The MicroServer Gen10 can however be configured using the USB-based Rapid Setup, refer to the HPE Rapid Setup Software Installation and Configuration Guide and the MicroServer Gen10 User Guide at support.hpe.com, to configure storage and install the operating system on the MicroServer Gen10.

   NOTE

   Rapid Setup requires that the Microsoft Windows installation software not be an evaluation or MSDN version. These versions are constantly updated by Microsoft and may not include necessary components to boot properly if installed using RSS. If using an evaluation or MSDN version, choose Intelligent Provisioning, not Rapid Setup, at the initial screen after pressing F10 at boot-up. You may need to provide additional hardware drivers using this alternate manual method.

   b. **SMB Setup Software** is the previous version of the automated setup feature embedded in HPE ProLiant Gen10 300 series servers and below. It is part of HPE Intelligent Provisioning version 3.30, which has been superseded by HPE Intelligent Provisioning 3.31 and is not covered in this Deployment Guide. HPE highly recommends updating firmware for older HPE ProLiant Gen10 300 and below series servers to HPE Intelligent Provisioning 3.31 for a much more robust automated setup experience.

c. **Rapid Setup (USB Based)** is the USB-based precursor to the integrated SMB and Rapid Setup functions. It provided limited automated setup of controller and disk configurations and prepared them for OS installation. The Rapid Setup (USB) method is superseded by the integrated Rapid Setup (Intelligent Provisioning version 3.31). Therefore, it will not be covered in this guide. If Rapid Setup (USB Based) is the desired method, please refer to the HPE Rapid Setup Software Installation and Configuration Guide.

d. **Manual configuration:** In some cases (such as when deploying a Microsoft Storage Spaces Direct server) you may not want to choose an automated setup. You have two options to manually configure and install the operating system:

I. For all HPE ProLiant Gen10 300 series servers and below, including MicroServer Gen 10 Plus, press F10 when prompted during system power-on self-test (POST) to start Intelligent Provisioning, then select Rapid Setup. Walk through the Rapid Setup process and when it presents the recommended RAID configuration you may select "CONFIGURE MANUALLY". Upon completion of manual configuration the utility will return to Rapid Setup to prompt for an operating system and you can complete the automated configuration.

II. Use the HPE Intelligent Storage Configuration feature of HPE Intelligent Provisioning. Intelligent Provisioning is accessible by pressing F10 during system power-on self-test (POST), or through the HPE Integrated Lights Out (iLO) tool

III. For the HPE ProLiant MicroServer Gen10: Use the UEFI storage utility.

For manual configuration refer to your server's user guide, which can be downloaded at support.hpe.com.

2. **Plan for the source of the Microsoft Windows Server 2016 or 2019 install files, which can be located:**

a. On physical media such as a USB flash drive or DVD

b. In a shared folder on the network (Note: Requires the server to receive IP address settings for iLO via DHCP, and login credentials of the shared folder)

3. **Plan for the initial OS host settings:**
Depending on the target environment you may need to know the following:

a. Host name

b. Host IP address (if not dynamically assigned via DHCP; a static IP address is recommended for servers in most cases)

NOTE
Rapid Setup Software features that need network connectivity requires the server be connected to a network that has existing DHCP services. Once the server initial hardware configuration is complete, you can re-configure the host NIC to a static IP address via the host operating system or iLO (recommended in most cases).

c. Domain name (if joining a Windows domain) and domain credentials with join domain privileges

4. **Make sure the local area network (LAN) infrastructure is ready to add a server:**
Which may include:

a. Active Directory

b. Domain name service (DNS—know the IP address of the DNS server if not using DHCP)

c. Public and private IP addresses and network ranges (DHCP)

d. Connectivity to the internet (know the default gateway address if not using DHCP)

Server hardware configuration overview

Hardware installation

HPE Small Business Solutions may come with add-on components that are not preinstalled, such as memory DIMMs, Smart Array Controllers, disk drives, etc. For installation guidance, refer to the user guide for your specific system. These can be found at support.hpe.com.

Server storage configuration planning

HPE ProLiant servers are capable of a large variety of storage configurations. This deployment guide focuses on the few standard configurations that are common to HPE Small Business Solutions, which are typically:

1. A pair of low-capacity solid-state drives (SSDs) or hard-disk drives (HDDs) for boot volume
2. A separate set of high-capacity HDDs for data and application storage
3. An HPE Smart Array Controller for managing and securing RAID volumes

The typical Smart Array Controller configuration is to create one RAID 1 volume from the two low capacity SSDs/HDDs, and one RAID 1, RAID 5, or RAID 6 volume from the high capacity HDDs/SSDs (RAID 1 for two HDDs/SSDs; RAID 5 for three or more HDDs/SSDs; or RAID 6 for four or more HDDs/SSDs). There are exceptions to this typical configuration as identified in the following table. You can also get more information from the HPE Smart Array SR Gen10 Configuration Guide.

NOTE
One exception worth noting is the HPE ProLiant MicroServer Gen10. It is unique in that it features a Marvell embedded software RAID controller, an optional 2.5" SSD slot (installed in the optional internal drive bay taking the place of the DVD/CD ROM drive bay), and four standard 3.5" LFF drive bays. If installed, the SSD in the optional internal drive bay is directly attached to the motherboard via a standard SATA port, and cannot be connected to the embedded Marvell RAID controller or to a HPE Smart Array Controller—and thus not configurable as a member of a RAID array. It is intended for the OS to be installed on the optional internal SSD and the remaining HDDs configured in a RAID. If redundant disks are required for the OS on this server, you must use two or more drives installed in the standard drive bays and configure the RAID array accordingly.

Refer to the HPE Rapid Setup Software Installation and Configuration Guide and the MicroServer Gen10 User Guide at support.hpe.com for complete configuration guidance as this model is no longer covered in this Deployment Guide

The recommended disk configuration for the most common HPE Small Business Solutions is shown in the following table.

HPE ProLiant server	Controller	OS volume	Data volume
MicroServer Gen10 Plus	E208 Smart Array Controller	2 x HDD (RAID 1)	2 x HDD (RAID 1); or all 4 x HDD (RAID5)
ML30 Gen10 4 LFF	E208 or P408 Smart Array Controller	2 x HDD (RAID 1)	2 x HDD (RAID 1); or all 4 x HDD (RAID5/6*)
ML30 Gen10 8 SFF	E208 or P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
ML110 Gen10 4 LFF	E208 or P408 Smart Array Controller	2 x HDD (RAID 1)	2 x HDD (RAID 1); or all 4 x HDD (RAID5)
ML110 Gen10 8 SFF	E208 or P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
ML350 Gen10 4 LFF	E208 or P408 Smart Array Controller	2 x HDD (RAID 1)	2 x HDD (RAID 1); or all 4 x HDD (RAID5)
ML350 Gen10 8 SFF	E208 or P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL20 Gen10 4 SFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	2 x HDD (RAID 1)
DL160 Gen10 8 SFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL180 Gen10 8 LFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL180 Gen10 8 SFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL325 Gen10 8 SFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL360 Gen10 8 SFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL380 Gen10 8 LFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL380 Gen10 8 SFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL385 Gen10 8 LFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL385 Gen10 8 SFF	P408 Smart Array Controller	2 x SSD/HDD (RAID 1)	3 x to 6 x HDD (RAID 5/6*)
DL380 Gen10 HCI**	P408 Smart Array Controller	2 x M.2 SSD (RAID 1)	4 x HDD (No RAID—storage) 2 x SSD (No RAID—cache)
DL385 Gen10 HCI**	P408 Smart Array Controller	2 x M.2 SSD (RAID 1)	4 x HDD (No RAID—storage) 2 x SSD (No RAID—cache)
ML350 Gen10 HCI**	P408 Smart Array Controller	2 x M.2 SSD (RAID 1)	4 x HDD (No RAID—storage) 2 x SSD (No RAID—cache)

* RAID 6 requires P408 controller.

** HPE Small Business Solutions for HCI (Hyperconverged Infrastructure) require the manual configuration method due to a unique requirement that disks used for the storage volume not be in a RAID configuration, and that the boot volume be on disks that are not part of the storage volume.

Storage configuration and Microsoft Windows installation using Rapid Setup Software 2.0

This section details the step-by-step instructions for configuring the server storage and installing the Microsoft Windows Server OS.

NOTE
The HPE MicroServer Gen10 does not have iLO, and therefore cannot take advantage of the Rapid Setup Software 2.0. Refer to the server MicroServer Gen10 User Guide at support.hpe.com, and the HPE Rapid Setup Software Installation and Configuration Guide to configure storage and install the Microsoft OS on the MicroServer Gen10. Note that the MicroServer Gen10 Plus does have iLO, and therefore you may use the following instructions.

NOTE
The following section refers to installing the Microsoft Windows OS on new physical servers. If you need to migrate existing Active Directory-Directory Services (ADDS), file storage data, or applications and databases to Microsoft Windows 2019, please refer to the appendix for more information and guidance.

The following example deployment walk-through assumes the Microsoft Windows Server install file is in one of two locations:

- In an .iso file located in the root directory of a USB stick and the USB is installed on an external USB port
- In an .iso file located in a folder on a network file share (Requires the iLO network port to receive IP address settings via DHCP, and login credentials for the shared folder)

This example also assumes the following hardware is installed, as is common for HPE Small Business Solutions:

- HPE Smart Array Controller
- One or more SSDs or HDDs installed in the standard drive bay(s)

Instructions

1. Install hardware and connect to the network (Requires the iLO network port to receive IP address settings via DHCP if installing the OS from a network share).
2. Boot the server and press F10 during POST.
3. The server will boot into the Intelligent Provisioning boot menu and automatically execute Intelligent Provisioning.
4. At the startup screen, select Rapid Setup.
5. Click the EULA “Accept” button to begin. Rapid Setup will perform an initial scan to detect the RAID controller and drives installed.
6. Review the Azure Services “Learn More” page and click CONTINUE when ready to proceed.
7. Review the Rapid Setup Software task list page and click CONTINUE when ready to proceed.
8. Select whether or not you have a web proxy server in your environment. You can also see your current network settings.
   a. If you have a proxy server, click YES to open a pop-up and configure the proxy server settings
   b. If you do not have a proxy server, click “No, it doesn’t”
9. You will be presented one of two options depending on the detected hardware.
   a. **Auto configuration:** Rapid Setup will automatically recommend an array controller configuration based on the installed controller and drives it detects in the initial scan. You can choose to accept the recommendation, in some cases choose an alternate configuration, or manually configure the controller.

   NOTE
   Rapid Setup will only automatically recommend a RAID configuration if it detects an S100i (embedded), E208i (PCIe or AROC), or P408i (PCIe or AROC) controller, and at least 1 HDD or SSD in the standard drive cage (M.2 and NVMe drives are not configured by Rapid Setup). In all other cases, only the “Continue” option for Manual Configuration will be enabled.

If a valid configuration is detected, Rapid Setup will inform you which controller is installed and present a graphical representation of the recommended configuration of array volumes and related drives.

The table below lists the possible recommendations depending on installed controller, drives, and number of volumes desired:

Single Volume

Selected by default if all drives are of the same type, speed, and capacity. User can opt to split 4 or more identical drives into Multiple Volumes

Installed disks	S100i (Embedded) and E208 Controller	P408 Controller
1 disk	RAID 0	RAID 0
2 disks	RAID 1	RAID 1
3 disks	RAID 5	RAID 5
4 or more disks	RAID 5	RAID 6

Multiple Volumes

Selected by default if any drives are of different type, speed, or capacity; or if user has opted to split a Single Volume into Multiple Volumes

Installed disks	S100i (Embedded) and E208 Controller	P408 Controller
All different disks	Each disk in a separate RAID 0 Volume	Each disk in a separate RAID 0 Volume
3 disks (2 identical)	RAID 1 plus RAID 0	RAID 1 plus RAID 0
4 disks (3 identical + 1)	RAID 5 plus RAID 0	RAID 5 plus RAID 0
4 disks (2 identical + 2 identical)	RAID 1 plus RAID 1	RAID 1 plus RAID 1
5 disks	RAID 1 from the 2 smallest capacity identical drives. Remaining matching drives in one or more volumes in priority order RAID 5, 1, or 0 as drive count allows.	RAID 1 from the 2 smallest capacity identical drives. Remaining matching drives in one or more volumes in priority order RAID 5, 1, or 0 as drive count allows.
6 or more disks	RAID 1 from the 2 smallest capacity identical drives. Remaining matching drives in one or more volumes in priority order RAID 5, 1, or 0 as drive count allows.	RAID 1 from the 2 smallest capacity identical drives. Remaining matching drives in one or more volumes in priority order RAID 6, 5, 1, or 0 as drive count allows.

NOTE

The drives in each volume (physical array) must be of the same:

- Type (SAS, SATA, HDD, SSD [including SSD durability: write intensive, mixed use, read intensive])
- Speed (HDD RPM, Interface Transfer Rate)
- Raw data capacity

Example: A system with 2 x 300 GB 10K 12G SAS HDDs and 3 x 1.2 TB 10K 12G SAS HDDs would be configured with a RAID 1 (2 x 300 GB) volume and a RAID 5 (3 x 1.2 TB) volume.

NOTE

Splitting a single volume when all the installed disks are identical:
If 4 or more identical disks are present a prompt will appear asking “Do you want to separate OS volume?” A checkbox will be displayed and you can select this to create OS and data volumes separately. Otherwise all disks will be combined into one volume.

b. **Manual configuration:** Click “Manual Configuration” if any of the following is true:

I. You do not want to use the recommended automatic configuration.

II. If no supported controller is detected (only the “Continue” button will be enabled).

Upon clicking “Continue,” Rapid Setup will collect additional information you will begin setting up the desired storage configuration in Intelligent Storage Configuration.

I. Click OK on the pop-up to acknowledge the instruction to click the “<” previous button to resume setup after finishing the configurations.

II. From the main page of Intelligent Storage Configuration screen, click “+ Create Array.”

III. Select the drives you want to include in the RAID array and select the drive usage. The drive bay representation will indicate the drives selected and remaining.

IV. Click “Next.”

V. Enter a logical name.

VI. Select a RAID Mode (for example, RAID 1 or RAID 5).

VII. (Optional) Select a stripe size or just accept the default setting.

VIII. Select an Accelerator if applicable or just accept the default setting.

IX. (Optional) Select a RAID size.

X. Click “Next” to review your settings and click “Submit.”

XI. (Optional) Repeat steps 7–15 to create another array.

XII. Click the “<” button to continue Rapid Setup.

XIII. Select the array that will be used for installing the OS and click “Next.”

10. After accepting the recommended configuration, or performing manual configuration, select the OS to install—in this case Microsoft Windows Server—and click “Continue.”
11. In the “Select” pop-up, choose the location of your Windows install media.
    a. Choose automatic scan if the media is on the DVD/CD ROM drive or on USB inserted in the external USB Port.
    b. Choose SMB/CIFS if the media is located on a network share and then enter the path and provide the credentials required to access the share.
12. Rapid Setup will present a notice that the system will reboot. When the system reboots it will resume the Rapid Setup and copy the installation files to the selected array volume and reboot again.
13. Once the server reboots the Windows setup wizard will begin so you can complete the Windows setup in the next section.

Completing OS installation

Once the Windows setup starts (after the OS files are copied to the OS volume for installation), Windows setup will prompt you for the following information.

- **Regional settings:** Language, time and currency format, and keyboard layout (for most U.S. deployments, you can accept the default settings and click “Next”).
- **Windows version to install:** The Windows setup will present a list of Windows versions to choose from and prompt you to make a selection. Typically, the list looks like this:
  - Windows Server 2016/2019 Datacenter
  - Windows Server 2016/2019 Datacenter (Desktop Experience)
  - Windows Server 2016/2019 Standard
  - Windows Server 2016/2019 Standard (Desktop Experience)

  Select the desired version and click “Next.” For most SMB deployments you can select Windows Server 2016/2019 Standard (Desktop Experience).
- **Type of installation (upgrade or custom):** Choose custom installation.

- **Install location:** This window will show two drives that were previously configured in the array controller prior to starting Windows setup, one representing the boot volume and one representing the data volume. Select the boot volume, if in doubt the drive with the smaller total size should represent the boot volume.
- Click on “New,” then either accept the default format size for the new OS volume (recommended), or optionally change the size to a smaller value if you want to partition the volume, and click “Apply.”
- **Administrator password:** After Windows setup completes installing the OS files and reboots the server, you will need to provide a password for the local administrator account.

After providing the administrator password, the server will complete the installation and be ready for initial login and subsequent OS configuration.

Base OS configuration

Once the OS is installed, the server must be configured. A new installation of Windows Server 2016/2019 will start up with the Server Manager Dashboard. Click on “Local Server” in the navigation pane to begin the next steps of the server configuration.

1. **Set the time zone:** Click on the link next to “Time Zone” to go to the time zone settings.
2. **Configure a static IP address:** Click the link next to “Ethernet” to get to the network connections settings and open the interface properties to configure a static IP address per your network requirements.
3. **Rename the server:** Click the link next to “Computer Name” to get the system properties settings, go to the “Computer Name” tab and click “Change” to enter a new name, then provide a new name and click “OK.” The server will need to reboot to apply the change.
4. **Join the server to an Active Directory domain (this is optional and not applicable if no Active Directory domain exists on the network):** After the server reboots from step 3, click the link next to “Workgroup” to open the system properties, then click the computer name tab and click the “Domain” radio button under the “Member of” section. Enter the name of the domain you want to join and, when prompted, enter the logon credentials of a domain user with privileges to add computers to the domain, typically the domain administrator user. Click “OK” until prompted to reboot the server to apply changes, then reboot the server.
5. **Enable remote desktop (optional):** To enable remote administration of the server you can turn on remote desktop by clicking on the link next to “Remote Desktop.” Click the remote tab and select “Allow remote connections to this computer.” If you plan to connect to the server from a computer that is not on the domain, you will need to uncheck the checkbox under this section to allow non-domain computers to connect via remote desktop. It is recommended to only connect using domain computers for additional security.
6. **Automatic updates and security features:** Windows setup turns on Windows Firewall and Windows Defender, and sets updates to automatically download by default, but other settings may be required for your environment. Click on the link next to “Windows Update,” “Windows Defender,” or “Windows Firewall” to go to the configuration window.
7. **Update the server:** Once the initial Windows configurations are set, click Start > Settings > Update & Security > Windows Update, then click “Check for Updates” to download and install all available updates.

ON-PREMISES USE CASES

HPE Small Business Solutions for File and Backup with Microsoft Windows

The HPE Small Business Solution for File and Backup server is equipped with sufficient CPU, memory, and storage resources to enable the server to be used for use cases such as file and print, backup and recovery, and hybrid file and backup.

Once you’ve completed the step in the initial setup section, the server is ready to be deployed into the production environment, and you can begin to configure the necessary Windows roles and features.

File server role

The file server role is added to provide shared network files for users, and a storage location for backups of other systems such as personal computers and other servers.

Deployment planning

Prior to beginning, complete the following steps:

1. Set a static IP address on the server's network interface that clients will use to access shared folders.
2. If your environment has Microsoft Active Directory Services deployed, join the server to the Microsoft Windows Domain before configuring the file server.
   a. If Active Directory is planned for the environment but not yet deployed, it is recommended that you deploy Active Directory before all other network services because many services will have integrated features or dependencies on Active Directory. Adding Active Directory after deploying services may have unanticipated consequences and will likely require additional administration.
   b. If Active Directory is not part of the environment, ensure that the server host name can be resolved by clients using a local DNS server.
3. Prepare a folder-naming and folder-security structure before creating shared folders on the server.
4. Consider if logging security events—such as unauthorized access attempts—is appropriate.

Install the file server role

1. Open the server manager tool if not already open.
2. Launch the "Add Roles and Features" wizard. This can be done from the "Manage" menu of the server administrator.
3. Click "Next" through the "Before you begin" page to the "Select installation type" page, verify "Role-based or feature-based installation" is selected, and click "Next."
4. On the "Select destination server" page verify this server is selected and click "Next."
5. On the "Select Server roles" page scroll down to "File and Storage Services" and expand it to select "File Server" then click "Next."
6. Click "Next" through the "Select Features" page and on the "Confirm installation selections" page. Verify your wizard selections and click "Next" then "Install" to complete the wizard.

Create a shared folder

1. In the server manager dashboard navigation pane, click File and Storage Services > Volumes.
2. On the "Details" pane, click on the volume that will host the new file share.
3. In the "Shares" pane select the "Tasks" drop-down and select "New Share" to open the "New Share" wizard.
4. Select the "SMB Share—Quick" profile and click "Next."

NOTE

Other settings are available, but this configuration only assumes a simple setup. For details, refer to the Microsoft Windows Server documentation.

5. On the "Select the server and path for this share" page, verify that this server is selected.
6. Verify that "Share Location" is set to "Select by volume."
7. Select the volume that will host this new share and click "Next."
8. On the "Specify share name" page enter a name for the new file share (such as "Backups") and note the share file path and UNC path and click "Next."
9. On the "Other settings" page accept the default settings and click "Next."
10. On the "Specify permissions to control access" page note the settings and either click "Next," or configure additional security settings as needed. These settings can also be configured later, if necessary.

NOTE

- By default, the new share permissions are set to “Everyone group: Allow—Read Only.” This will prevent everyone, including administrators, from saving, making changes to, or deleting any files in the share when remotely accessing the folder over the network. Note that this does not prevent local users from saving to the folder using Windows Explorer or other normal methods.
- To enable users to save files in the share remotely over the network, you will need to configure “Allow—Change” share permissions for those users.
- If you do not want to allow read access to everyone, you must first configure the share permissions for specific users or groups and then remove the “Everyone” group.
- It is **not recommended** to give the “Everyone” group “Allow—Full Control” permissions.

11. Review the settings on the “Confirm selections” page and click “Create,” then click “OK” to close the wizard.

Backup server feature

The Microsoft Windows Server Backup feature can be installed for the HPE Small Business Solution for File and Backup server to perform in a backup server role. In this section, we will cover two likely scenarios:

1. The **HPE Small Business Solution for File and Backup** performs a full server backup of itself to an external USB hard drive, such as the HPE RDX Removable Disk Backup System (See the RDX section for installation procedure).
2. Client machines perform a custom backup of selected files to the **HPE Small Business Solution for File and Backup** via network share.

NOTE

Windows Server Backup can provide basic on-premises backups, or even simple backups to colocation data centers, but has very limited capabilities. If more robust, automated, or centralized backup services are desired, there are many third-party applications that perform these functions. Alternatively, adding Microsoft Azure Backup Service can be an excellent method for server backup to the cloud, which will be discussed in the coming “hybrid cloud use cases” section of this document.

Deployment planning

There are three options to choose from when considering where you will store the backup files from your on-premises server using Windows Server Backup.

1. **Back up to a dedicated disk on the local machine:** This method reserves one entire physical disk on the server strictly for backup data. The disk cannot be part of a RAID array. Alternatively, an external USB drive (such as the HPE RDX Removable Disk Backup System) may be used as the backup target, though there are some external USB drives that are not supported for this operation, so check the Windows Hardware Compatibility List. USB Flash Memory Sticks are not supported for Windows Server Backup.
2. **Back up to a volume:** This method allows backups to be stored on a local volume. The data to be backed up and the volume to store the backup must be on different volumes. You cannot store the backup on the same volume as the data being backed up. This method also puts your data at risk because if the server is down you will not have access to your backups.
3. **Back up to a shared network folder:** This method allows backups to be stored on a shared network folder located on a different machine. This type of backup has a severe limitation of having only the most recent backup available because each backup job overwrites the previous backup job.

NOTE

You can also configure local backup jobs to be stored on the local machine using the shared network folder method if you don’t have a dedicated backup disk or the data being backed up to the same volume. However, this plan also puts your backup data at risk by storing it on the same server. You will be able to recover files that have been backed up, but, if the server is down you will not have access to your backups.

If you are using Windows Backup Server, HPE recommends backing up to a dedicated removable USB hard disk such as the HPE RDX Removable Disk Backup System, or to a remote server, or backing up to a cloud storage provider such as Microsoft Azure.

Installing the External RDX Removable Disk Backup System

The RDX Removable Disk Backup System makes performing and complete system backups a snap. Simply schedule a recurring backup job and load a removable disk. Then simply eject the disk after the job is complete and insert a new disk for the next job, allowing you to take your backup copy off-site for greater protection against loss of data. Your Disaster Recovery plan should allow for multiple backup disks to be rotated. Creating your Disaster Recovery plan is beyond the scope of this document since each environment may have several different requirements. But this section of the guide will walk you through setting up the RDX to run with Windows Server Backup.

1. Unpack and connect the RDX to any available USB port with the provided cable. Note that the cable allows for the use of two USB ports on the server if one port does not supply enough power to the RDX unit. (Note: If you do not see the RDX as an available USB drive after installing and inserting a disk, this may mean you do not have enough power available on the single server USB port. Connect the second USB plug on the cable to a second port on the server, or alternatively you can purchase an external power supply for the RDX unit.)
2. Install the RDX Utility, update the firmware, Configure.
   a. The RDX Utility and Firmware update can be downloaded freely from support.hpe.com
   b. Run the RDX Utility setup file and step through the wizard, then reboot the server
   c. Open the RDX Utility and click the "Diagnostic" button
   d. Click the "Utility" tab, then click the "Change Firmware" button and navigate to and select the downloaded firmware file
3. Configure the RDX System for use with Windows Server Backup.
   a. Remove disk media if one is installed in the RDX System
   b. Open the RDX Utility and click the "Diagnostic" button
   c. Click the "Utility" tab, then click "Change Device Mode"
   d. Select the "Fixed Disk" option, click OK, then Exit
   e. Close the RDX Utility
4. Insert an RDX Removable Disk Cartridge and verify that the RDX ready light is solid **green**. Then open Windows Explorer to see that the drive appears in the list of volumes. (Note: Once configured for use with Windows Server Backup the drive will no longer appear in Windows Explorer.)
5. Schedule a Windows Backup job as described in the next section.

Adding the Windows Server Backup feature

To add Windows Server Backup to a remote Windows Server 2016/2019 machine, log on to that machine and perform the following.

1. Launch the "Add Roles and Features" wizard and click "Next" through the "Before you begin" page.
2. On the "Select installation type" page verify that the "Role-based or feature-based installation" option is selected and click "Next."
3. On the "Select destination server" page verify this server is selected and click "Next."
4. Click "Next" through the "Select server roles" page.
5. On the "Select Features" page scroll down to select "Windows Server Backup" and click "Next."
6. On the "Confirm installation selections" page select "Restart the destination server automatically if required," confirm that "Windows Server Backup" is being installed and click "Install."
7. Once the install wizard is complete, close the wizard.

Schedule a full-server backup job using an external USB disk drive

Backing up to an external disk provides the opportunity to rotate a set of external disks for safekeeping off-premises. To enable multi-disk capability, you must schedule the first backup job, then open the backup schedule and modify the backup job to add storage disks to the backup disk library.

NOTE

The external USB device must be an HDD or SSD, not a flash memory stick. The disk will be formatted and all data on the disk will be lost. Windows Server Backup will not recognize the disk if there is an operating system installed on it; manually remove all partitions on the disk using the Disk Management MMC or other tool if necessary.

Scheduling the first backup job:

1. On the “Server Manager” click Tools > Windows Server Backup to open the backup console.
2. Click “Local Backup” in the navigation pane.
3. Click “Backup Schedule” in the “Actions” pane.
4. On the “Getting Started” pane click “Next.”
5. Select “Full server” and click “Next.”
6. Schedule a time for the backup to occur and click “Next.”
7. Select “Backup to a hard disk that is dedicated for backups” and click “Next.”
8. Ensure the external USB connected disk (such as the RDX Removable Disk Backup System) is selected and click Next, then acknowledge the warning regarding the external disk, and monitor the wizard as it formats the new disk.
9. Review the “Confirmation page” settings and click “Finish.”
10. Monitor the wizard completion of the process and click “Close.”

Adding backup disks

To add backup disks, you must modify the backup schedule.

NOTE
It is recommended to physically mark the external disk with the volume identification in the Windows Server Backup tool when using multiple external disks in a rotation. When you want to restore data, you will need to know which external disk to restore from.

1. Change to a new external USB drive (or load a new RDX Disk Cartridge) for storing backups.
2. On the “Server Manager” click Tools > Windows Server Backup to open the backup console.
3. Click “Local Backup” in the navigation pane.
4. Click “Backup Schedule” in the “Actions” pane.
5. On the “Modify Scheduled Backup Settings” page select “Modify backup” and click “Next.”
6. On the “Select Backup Configuration” page select “Full server” and click “Next.”
7. On the “Specify Destination Type” select “Backup to a hard disk that is dedicated for backups” and click “Next.”
8. On the “Keep or Change Backup Destinations” page, select “Add more backup destinations,” and click “Next.”
9. On the “Select Destination Disk” page, ensure the new external USB disk (or new RDX Backup System Disk Cartridge) is selected and click “Next,” then acknowledge the warning regarding the external disk (if presented), and monitor the wizard as it formats the new disk.

Schedule a backup job using a shared network folder

Backing up remote hosts (client servers or user PCs) to a shared network folder requires that the target folder already exists. Then you can select it as the target for a remote host’s backup jobs.

NOTE
When performing backup of remote hosts to the HPE Small Business Solution for File and Backup server, it is recommended to configure and use a “Service Account” and assign that account only enough privileges to perform the backup task. Create a backup “Service Account”—either on the remote machine or in Active Directory—that will be given backup privilege on the remote host and have permission to write to the shared folder on the target HPE Small Business Solution for File and Backup server. Service accounts and share and folder permissions are controlled by your organization’s security policy, and are outside of the scope of this document. Refer to your company’s security policies and Microsoft documentation for guidance.

To create the target folder for remote backups, refer to the previous section "Create a shared folder" for instructions on creating a shared network folder, but with the following exceptions:

1. Give the folder a name like "Backups" or "Desktop Backups" that identifies what the folder is used for.
2. Create the network share and give it the same as the folder name. This folder should only be used for backups. As remote machines backup to this folder using Windows Server Backup, they will create sub-folders that start with the remote machine's NetBIOS name.
3. Make sure to set the share and folder permissions for the service account that will be used to perform the backup. The credentials of this service account will be required when you set up the backup job on the remote host.

To schedule a backup job on the remote Windows Server 2016/2019 machine:

1. On the "Server Manager" click Tools > Windows Server Backup to open the backup console.
2. In the navigation pane, click "Local Backup," then on the actions pane click "Backup Schedule" to open the Backup Schedule wizard.
3. On the "Getting started" page observe the choices available and click "Next."
4. On the "Select Backup Configuration" page select either "Full server" or "Custom" and click "Next." Note that for this example we will use the custom selection and backup select folder(s).
5. On the "Select Items for Backup" page click "Add Items."
6. Select the desired folders to be backed up and click "OK" and "Next."
7. On the "Specify Backup Time" page choose the desired backup time and click "Next."
8. On the "Specify Destination Type" page select "Backup to a shared network folder" and click "Next" and acknowledge the warning that backup jobs will be overwritten.
9. On the "Specify Remote Shared Folder" page:
    a. Enter the UNC path (example \\myserver\backups) of the network share that will store the backup.
    b. Select the desired access control method and click "Next."
    c. Provide credentials for the remote shared folder if prompted.
10. Review the "Confirmation" page and click "Finish" and close the wizard.

Reviewing backup jobs

You can review the scheduled backup task in "Task Scheduler" by opening the server manager and clicking Tools > Task Scheduler, then navigate through the task list by clicking Task Scheduler Library > Microsoft > Windows > Backup. Here you can see the status and history of backup jobs, as well as change some settings or even run the scheduled job manually.

Testing the backup with a recovery job

Recovering from a disaster depends on being able to access and recover files from the backups, whether there is a catastrophic loss of the server or there is a much smaller micro-disaster, such as recovering a corrupted file. Performing periodic test recoveries of your backups is essential for knowing that you can recover data in a real crisis. Testing recovery of backups also builds your skill confidence and will greatly improve your recovery performance when under the pressure of a real disaster. You should perform full server and simple file/folder test recoveries periodically.

NOTE
A full server test recovery is very complex and could negatively impact your production environment. It should always be done in an environment isolated from your production environment. Full server recovery is outside of the scope of this document.

To recover files previously backed up to a remote server using Windows Server Backup:

1. On the "Server Manager" click Tools > Windows Server Backup to open the Windows Server Backup console.
2. In the navigation pane, click "Local Backup," then on the actions pane click "Recover" to open the Recovery wizard.
3. On the "Getting Started" page select "A backup stored on another location" and click "Next."
4. On the "Specify Location Type" page select "Remote shared folder" and click "Next."
5. On the "Specify Remote Folder" page enter the UNC path of the remote folder that contains the backup file that has the files to be recovered and click "Next."

6. On the “Select Backup Date” page select the date and time (if necessary) of the backup job that has the files to be recovered and click “Next.”
7. On the “Select Recovery Type” page select “Files and folders” and click “Next.”
8. On the “Select Items to Recover” page browse the folder tree in the “Available items” pane and click on the file or folder to be recovered. Ensure that it appears in the “Items to recover” pane and click “Next.”
9. On the “Specify Recovery Options” page specify the recovery location, file overwrite options, and security settings options as desired (for example, for a test recovery you could specify a “Test Recovery” folder) and click “Next.”
10. On the “Confirmation” page review the job properties and click “Recover.”
11. Check the target location of the recovery job and verify the file was recovered. If possible, verify the file is not corrupted.

HPE Small Business Solution for Virtualization with Microsoft Windows

The HPE Small Business Solution for Virtualization server is equipped with sufficient CPU, memory, and storage resources to enable the server to host multiple virtual machines (VMs). Because they are based on Microsoft Windows, they also integrate seamlessly with many Microsoft Azure services, thus providing an agile and efficient hybrid cloud virtualization solution.

Once the server is ready to be deployed into the production environment (refer to the chapter “Initial Setup” in this document) you can begin to configure the necessary Windows roles and features to support Microsoft Hyper-V virtualization.

Installing and configuring virtualization using the Microsoft Windows Server Hyper-V role

The Windows Server Hyper-V role provides virtualization services to host multiple Windows- and Linux®-based VMs from a single physical server. This enables you to fully utilize the server investment and consolidate older servers, while segregating critical applications and infrastructure services to prevent one failing app or service from taking down the entire IT infrastructure.

Deployment planning

Prior to beginning, complete the following steps:

1. Set a static IP address on the network interface of the Hyper-V host.
2. Ensure that the server host name can be resolved by clients using a local DNS server.
3. Joining the Hyper-V host server to a local Active Directory Domain is not required, and in some cases it is undesirable. However, managing the server may be easier if the server is a domain member due to ease of administration and server management automation that is available in an Active Directory environment.

   It is recommended to:

   a. Join the domain if the server is only accessible on the private network. Join the server to the domain before configuring the Hyper-V role if your environment has Microsoft Active Directory Services deployed.
   b. Not join the domain if the server is or will be accessible from outside of the private network, such as when it is placed in the DMZ to host VMs that will be exposed to the internet (like web servers, for example).
4. Plan for where to store the files used by Hyper-V VMs. A typical scheme would be to set up a folder on a high-performance storage volume that is separate from the OS volume. HPE Small Business Solutions for Virtualization provide for this scenario.
5. Have your OS media ready. The recommended method is to store OS files in a designated folder on the host server.
6. Install the VM’s OS from a physical device such as a CD/DVD-ROM, from a floppy disk image (VFD file, or a virtual boot floppy disk), an .iso file that is accessible through a network share or stored on the local host server, or from a network-based installation server. The last option will install a legacy network adapter to your VM so you can boot from the network adapter.

Install the Hyper-V server role

1. Open Server Manager.
2. In the “Server Manager” menu click Manage > Add Roles and Features.
3. At the “Select Installation Type” page, choose the role-based and click “Next.”
4. On the “Select Destination Server” screen, verify your server is selected and click “Next.”
5. On the “Select Server Roles” screen, click the “Hyper-V” check box. When the “Add Features” dialog box appears, accept the defaults and click the “Add Features” button, then click “Next.”
6. At the “Select Features” screen, click “Next.”

7. At the “Hyper-V introduction” screen, click “Next.”
8. At the “Create Virtual Switches” screen, choose the appropriate network adapter and click “Next.”
   a. At least one network adapter must be installed, connected to the network, and active in order to configure a virtual switch. If no adapters are shown, check to ensure that there is at least one adapter connected to the network. You can choose to configure a virtual switch later.
   b. If multiple physical adapters are installed on the host server and they are connected to the network, you will be presented with a choice of network adapters.
      I. You may want to create multiple switches, for example, one for the connection to the LAN, and one to the DMZ. Select the one you want to configure now and go back later and add the second virtual switch and bind it to the other adapter.
      II. You may only want to use one of the adapters for VM connectivity. In this case, choose one and continue.
9. At the “Virtual Machine Migration” screen, click “Next.” Note that, while it is possible to configure this new Hyper-V server to migrate VMs to/from other Hyper-V servers, VM migration is outside of the scope of this guide. Please refer to Microsoft documentation.
10. At the “Default Stores” screen, browse to the folder location where you want to put the VM files by default. For HPE Small Business Solutions for Virtualization we recommend:
    a. Location for the virtual hard disk (.vhdx or .vhd) files—D:\Hyper-V\Virtual Hard Disks
    b. Location for the VM settings files—D:\Hyper-V
    c. Click “Next” to continue.
11. At the “Confirmation” screen, click the “Install” button.
12. After the installation is complete, click the “Close” button.
13. Restart your server.

Configure Hyper-V and add VMs

After you have installed the Hyper-V role, you can configure the settings of the Hyper-V server and begin adding VMs. The Hyper-V Manager is the tool used to perform these tasks. You can access the Hyper-V Manager by one of the following methods.

1. From the “Server Manager” menu click Tools > Hyper-V Manager.
2. From the Server Manager navigation pane, click “Hyper-V” then right click the server in the “Servers” pane, then click “Hyper-V Manager.”
3. From the Hyper-V manager you can configure default and global settings as well as virtual switches to enable VMs to communicate with the physical network.
4. By default, Hyper-V is ready to begin installing and hosting VMs. But there are some instances where you may want to adjust these settings to better fit your operating environment. You can find more information about Hyper-V configuration at docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-on-windows-server.

To create VMs:

1. In the “Hyper-V Manager” window right click the server in the navigation pane and either select New > Virtual Machine, or select the server and click New > Virtual Machine in the “Actions” pane.
2. In the “New Virtual Machine Wizard,” click “Next” on the “Before You Begin” page.
3. On the “Specify Name and Location” page, give your VM a name, and, if desired, change the default location of the VM configuration files. Click “Next” to continue.
4. The “Specify Generation” screen is next. Choose “Generation 2” (“Generation 1” should only be used if necessary for application compatibility, refer to your application guidance), and click “Next.”
5. On the “Assign Memory” page define how much of your host system’s memory you want to assign to this VM. You can also choose to allow the VM to start with only the memory that it needs and then “Dynamically Expand” up to the value you set here when it needs more.
6. Remember that once all of your VMs use up all of your host’s physical memory, it will start swapping to disk, thus reducing the performance of all VMs. Click “Next” to continue.
7. On the “Configure Networking” page, select the virtual switch that you previously configured during Hyper-V role installation, or another virtual switch if a different one was created and desired for this VM. Click “Next” to continue.
8. On the “Connect Virtual Hard Disk” page, select “Create a virtual hard disk”.
9. Browse to the previously created folder for storing virtual disks (i.e., D:\Hyper-V\Virtual Hard Disks), and enter a file name for the .vhdx file. It is a good idea to name .vhdx files by the VM name and function they perform. For example: “NewVM_Boot.vhdx,” or “NewVM_Data.vhdx.”

10. Enter the desired disk size and accept the default Dynamically Expanding disk type and click “Next”.
11. On the “Installation Options” page you can select how you want to install your OS. The fastest method is to store an .iso file on the host server file system and point the installation wizard to that file.
12. If you followed the recommendations, choose “Install an operating system from a bootable .iso file” and browse to the file and select it. Then click “Next.”
13. On the “Completing the New Virtual Machine Wizard” summary page, verify that all settings are correct. You also have the option to start the VM immediately after creation. Click “Next” to create the VM.
14. Start the VM. It will boot to the selected .iso file then begin the installation of the OS.
15. Repeat these steps for each VM you want to deploy on your Hyper-V server.

Protection option for Microsoft Hyper-V server and virtual machines

There are many solutions available for protecting Microsoft Hyper-V server and its VMs. This section covers an HPE recommended option that’s scaled for small businesses, low cost, and easy to implement: Veeam® Backup & Replication™ Community Edition with HPE RDX Removable Disk Backup System.

The HPE RDX Removable Disk Backup System is the storage target for this solution, and Veeam Backup & Replication Community Edition is the software that makes the solution easy to implement and manage for a small Microsoft Hyper-V virtualization environment. Veeam Backup & Replication Community Edition (referred to as “Veeam” for the remainder of this section) is free and can support up to ten VM guests. It offers most of the same features as the fully licensed version. Refer to the Veeam documentation for product details.

Pre-deployment planning

NOTE
HPE recommends that you review the Veeam Backup & Replication Users Guide to understand the various deployment strategies available and select the one that best meets your needs, before deploying Veeam.

While Veeam can be deployed in a variety of scenarios, this guide will focus on a single standalone configuration. Assumptions and prerequisites include:

- File and print sharing must be enabled on the server; refer to the “HPE Small Business Solutions for File and Backup with Microsoft Windows” section for details.
- The HPE RDX Removable Disk Backup System needs to be installed and running prior to installing and configuring the Veeam software. Refer to the “HPE Small Business Solutions for File and Backup with Microsoft Windows” section of this document for instructions.
- Microsoft Hyper-V must be installed and running on the system.
- The Hyper-V server must have a data volume to store guest VM files that is separate from the Windows OS boot volume.
  - Optional: For more efficient backups of the data volume, it should be formatted as a ReFS volume.
  - At least one VM to be protected must be running and its related files must be located on the data volume.
- Veeam will be installed on the same machine that is hosting the Microsoft Hyper-V VMs being protected (source host) and the VMs will be backed up to an external HPE RDX Removable Disk Backup System (target host).
- No more than the maximum VMs supported by Veeam will be backed up.
- You must know the administrator login credentials of the server.

Install Veeam

1. Download the free software from the Veeam website.
2. Mount the downloaded .iso file and run **setup.exe** from the root folder of the mounted .iso.
3. Click “Install” and accept the default options in the installation wizard:
   a. View and accept the EULA and click “Next.”
   b. Leave the “License file for Veeam Backup & Replication” field blank and click “Next.”
   c. At “Program features” leave the default settings and click “Next.”

d. At the “System Configuration Check” screen, review the results and click “Install” to automatically install the required software. (NOTE: This screen will be skipped if all required software is already installed.)

e. At the “Default Configuration” screen leave the “Let me specify different settings” checkbox unchecked and click “Install.”

f. Optional: Configure Veeam to automatically check for and notify you of available updates.

Configure the RDX as the target repository

1. Ensure that the RDX has a disk cartridge loaded.
2. Open Veeam and launch the “Add New Backup Repository” wizard.
   a. Open Backup Infrastructure.
   b. Click “Add Repository” in the command ribbon.
3. Select “Direct Attached Storage.”
4. Specify a name for the repository, such as SERVERNAME-RDX, and provide a description.
5. If the server was not already added to the Veeam Backup Infrastructure, add it now:
   a. At the Server page, click “Add New” to open the Add Server wizard.
   b. Click “Microsoft Hyper-V.”
   c. Enter the server name and description and click “Next.”
   d. At the Type screen select “Microsoft Hyper-V server (standalone)” and click “Next.”
   e. At the Credentials screen enter the administrative login credentials for the Hyper-V server.
   f. At the Apply screen click “Apply.”
   g. At the Results screen, click “Next” then “Finish.”
6. At the Server page click “Populate” to see the RDX drive and click “Next.” If the RDX drive is not visible, exit Veeam, go to the “Installing the External RDX Removable Disk Backup System”, and verify the RDX is installed and functioning. When RDX is functioning restart this Veeam configuration section.
7. At the Repository page enter or browse to the path of the RDX drive. Click “Populate” to verify disk capacity and free space.
8. Select “Advanced” and check the “This repository is backed by rotated hard drives” box, then click “OK.”

NOTE

The RDX only needs to be added to the Veeam Repository once. By default, Veeam will store a full backup on the RDX disk cartridge every time the cartridge is changed. If the cartridge is left in the drive during the next backup after a full backup is stored on the cartridge, Veeam will perform an incremental backup. Once the cartridge is changed, Veeam will perform a full backup again.

9. At the Mount Server page select this server and click “Next.”
10. At the Review screen, review the settings and click “Apply.”
11. At the Apply screen, wait for the Repository wizard to complete all tasks then click “Finish.” This may take a few minutes. **Do not** interrupt the wizard during this phase of the configuration.

Configure a scheduled backup job

1. Open the New Backup Job wizard: On the Home tab, click Backup Job > Virtual machine > Microsoft Hyper-V.
2. At the Name screen, specify a name and description for the job.
3. At the Virtual Machines page click "Add." Select all VMs in the Add Objects window and click "Add."
4. Use the up/down buttons to set the preferred order of the backups and click "Next."
5. At the Storage page, configure the following settings:
   a. Backup Proxy: Select "On-host backup."
   b. Backup Repository: Select the repository created in the previous steps. Note the Retention Policy and adjust if desired. The number represents the maximum number of backups retained on the media. The oldest job on the media will be deleted after exceeding the number of jobs specified by this policy.
   c. Click "Next."
6. At the Guest Processing page click "Next."
7. At the Schedule page:
   a. Select "Run the job automatically."
   b. Configure the desired schedule settings.
   c. Optional: Configure the desired retry settings.
   d. Optional: Configure the desired job termination settings.
   e. Click "Apply."
8. At the Summary page review the job settings and click "Finish." The first automated backup will start at the next scheduled interval.

Test the configuration

To test the configuration and ensure the job will run at the next interval, run an ad hoc job based on the scheduled job, before the next scheduled job is set to run.

1. Right click the job and click "Active Full" from the pop-up menu.

Test the solution by restoring a Veeam backup

WARNING!
Do not restore a production VM to its original location with default settings unless you intend to replace the existing VM with a copy from the backup. By default, Veeam will automatically shut down and delete the original VM so that when the restored VM is started it will not generate a conflicting duplicate VM configuration on the Hyper-V host. Be sure that you read the Veeam user guide and understand the way Veeam works when restoring VMs before restoring a production VM to its original location. HPE will not be responsible for any damages to customer environments as a result of performing this procedure.

There are several methods to restore VMs protected with Veeam. The following section documents the Entire VM Restore method. It's designed to test the ability to restore VMs protected by Veeam, by restoring the backup as a new VM disconnected from the existing network, effectively creating a disconnected copy of the original VM that was backed up. You will be able to start the VM and see that the recovery was successful, thus verifying that you can recover from a real disaster should the need arise. After you've completed the test you should delete the copied test VM to prevent accidental conflicts should the test VM be started in the production environment.

Perform the following steps

1. Open Veeam.
2. Launch the Restore wizard.
   a. On the Home tab, click Restore > Microsoft Hyper-V > Restore from backup > Entire VM restore > Entire VM restore.
3. At the Virtual Machines page, select the VMs you want to test restore.
   a. Click “Add VM.”
   b. Browse existing backups and select the backup from the list.
   c. Optional: Select the restore point if desired (Veeam automatically selects the latest restore point by default).
4. Click “Next.”
5. At the Restore Mode page, select “Restore to a new location, or with different settings.”
6. At the Host page, select the VM to restore and click “Host,” then choose the Hyper-V server as the (standalone) host.
7. At the Datastore page, select the VM, click “Path,” and point to the folder where the VM files will be stored, typically this would be the folder setup in Hyper-V as the location for VM files.
8. At the Network page, select the VM to be restored and click “Disconnected.”

NOTE
When the restored VM is started, you will need to use the server’s Hyper-V console to access the server—remote administration via RDP will not work since the restored server will not be connected to any virtual network.

9. At the Name page, select the VM and click “Name.” Enter a new name for the VM that is different from the original VM name. Optionally you can add a prefix/suffix to the name.

IMPORTANT!
You must change the VM UUID to avoid possible conflicts with the original VM.

10. From the Name page, select the VM and click “VM UUID” and select “Generate new virtual machine UUID.” Click “Next.”
11. At the Secure Restore page ensure the checkbox for “Scan the restored machine for malware prior to performing recovery” is unchecked and click “Next.” This malware scan is unnecessary for test recovery unless you also want to test the Secure Restore feature.
12. At the Reason page, enter the desired information and click “Next.”
13. At the Summary page, review the settings and click “Finish.” HPE recommends NOT selecting the “Power on VM after restoring” checkbox but instead starting the VM from within the Hyper-V management console.
14. Open the Hyper-V management console and locate the restored VM.
    a. Open the VM console screen and start the VM.
    b. Verify that the running VM is successfully restored.

HPE Small Business Solution for Small Office Deployment

The HPE Small Business Solution for Small Office Deployment is a complete small office IT package specifically designed to meet the unique IT needs of small businesses.

This chapter outlines a logical flow for a greenfield deployment of the server and network IT infrastructure. While any of the components can be deployed individually in an existing office network environment, the scope of this deployment scenario is a new deployment with no pre-existing IT environment beyond internet access.

This chapter includes the following:

1. Deployment planning
   a. Configuration options
   b. Physical installation overview
   c. Pre-deployment preparation
2. Networking deployment
   a. Network switch configuration
   b. Aruba Instant On WAP configuration
3. Server deployment
   a. Windows Server installation
   b. Active Directory configuration
   c. DNS
   d. DHCP
   e. File and backup services

Deployment planning

Configuration options

The HPE Small Business Solution for Small Office Deployment solution is offered in three configurations:

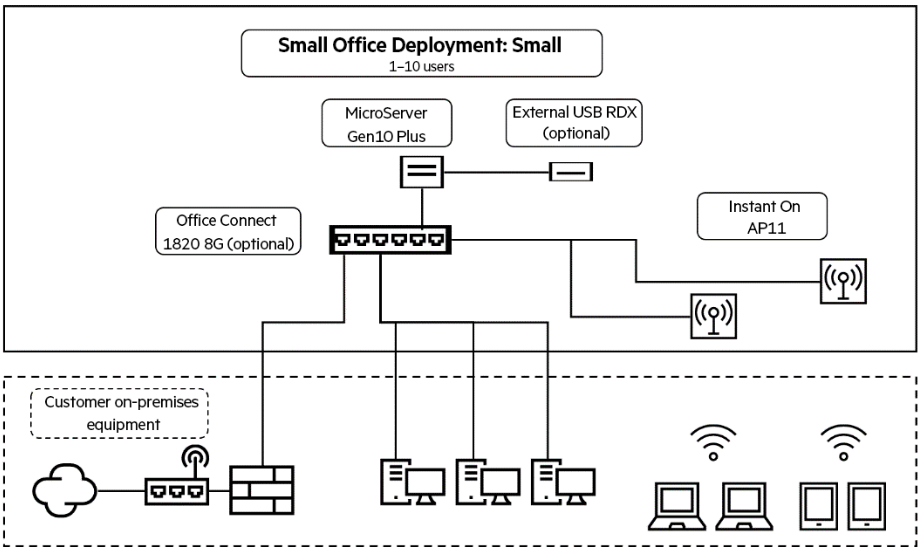
1. **Small**—Up to 10 users/20 devices featuring:
   a. 1 x HPE ProLiant MicroServer Gen10 Plus
   b. 1 x HPE OfficeConnect 1820 8G 4 port 1 GbE PoE + 4 port 1 GbE non-PoE managed switch
   c. 2 x Aruba Instant On AP11 wireless access points (WAPs)
2. **Medium**—Up to 25 users/50 devices featuring:
   a. 1 x HPE ProLiant ML30 Gen10 Server
   b. 1 x HPE OfficeConnect 1920s 24G 12 port 1GbE PoE + 12 port 1 GbE non-PoE managed switch
   c. 2 x Aruba Instant On AP12 WAPs
3. **Large**—Up to 100 users/200 devices
   a. 1 x HPE ProLiant DL20 Gen10 Server
   b. 2 x Aruba 2530 48G 48 port 1 GbE PoE
   c. 1 x Aruba Instant On AP15 WAPs
   d. 4 x Aruba Instant On AP12 WAPs

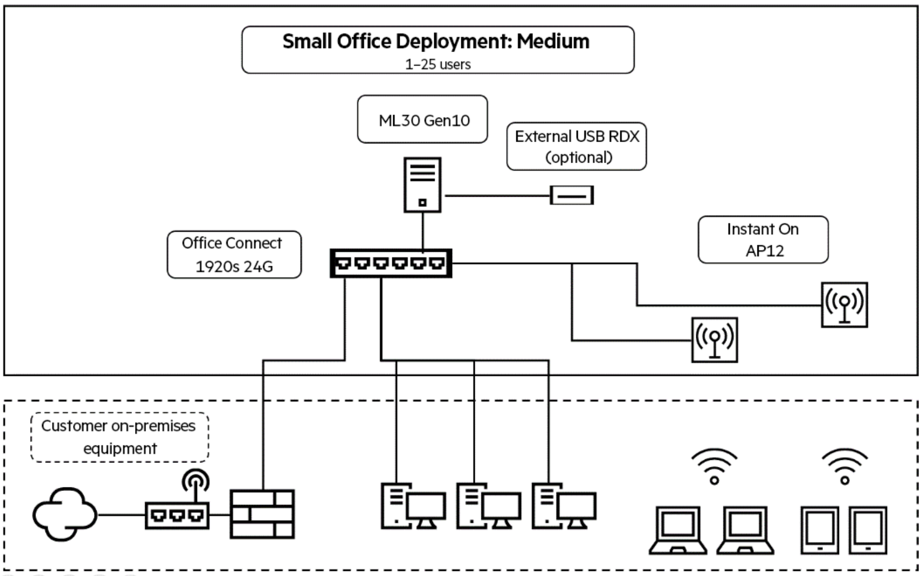
Each of the configurations can be expanded with:

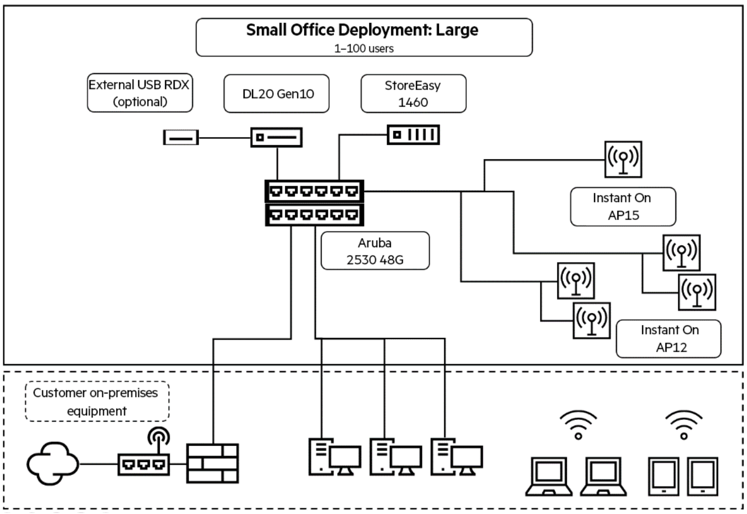
- Additional HPE OfficeConnect and Aruba networking
- Additional external storage via HPE StoreEasy 1460 Network Attached Storage (NAS)
- Additional external USB-based HPE RDX Removeable Disk Backup System

Physical installation overview

1. The physical location for your IT hardware should be:
    a. **Secure**—Restrict physical access to the server, switches, and router to authorized personnel only by placing it in a locked room.
    b. **Environmentally safe**—The location must be relatively free of dust, moisture, extreme temperatures, and the like. All hardware should be either rack mounted or placed in a location where it won't fall or have things fall on it. Usually the closet where telephone or internet services are connected is sufficient as long as there is enough ventilation or cooling to keep the ambient temperature within operating limits, and the room can be secured.
2. The diagrams below depict a simple topology of each of the HPE Small Business Solution for Small Office Deployment configurations.


Small Office Deployment: Small
1–10 users
MicroServer Gen10 Plus
External USB RDX (optional)
Instant On AP11
Office Connect 1820 8G (optional)
Customer on-premises equipment


Small Office Deployment: Medium
1–25 users
ML30 Gen10
External USB RDX (optional)
Instant On AP12
Office Connect 1920s 24G
Customer on-premises equipment


Small Office Deployment: Large
1–100 users
External USB RDX (optional)
DL20 Gen10
StoreEasy 1460
Instant On AP15
Aruba 2530 48G
Instant On AP12
Customer on-premises equipment

NOTE
Be sure to follow local building codes and regulations as applicable when installing IT infrastructure

Pre-deployment preparation

Internet service provider (ISP) broadband router configuration

TIP
Set up may involve making configuration changes to on-premises equipment, mainly the ISP broadband router. Most ISP routers have a configuration backup utility. It is recommended to back up your ISP router's configuration before making any changes.

IMPORTANT
Consult your ISP's technical support before making changes to your ISP router.

1. **Wi-Fi:** Most ISP routers have Wi-Fi enabled by default. This Small Office Deployment scenario assumes you will disable Wi-Fi on the ISP router and deploy Aruba Instant On WAPs to provide Wi-Fi services.

   Alternatively, you can choose to leave the ISP router Wi-Fi enabled (such as to provide a separate Wi-Fi network for guest Wi-Fi access), but such an alternate scenario will require additional configurations on both the ISP router and the Small Office Deployment server and networking, and possibly require an additional firewall appliance. This alternate scenario is outside the scope of this document.

2. **DHCP:** Most ISP routers have DHCP enabled by default. This deployment scenario assumes you will first deploy Aruba Instant On WAPs then disable DHCP on the ISP router and deploy Windows Server DHCP services.

   Alternatively, you can leave DHCP enabled on the ISP router if you ensure Windows DHCP and the router DHCP are not providing IP addresses in the same IP address range. This alternate scenario will require additional configurations on both the ISP router and the Small Office Deployment server and networking and is not recommended if there is no firewall between the ISP router and the internal network. This alternate scenario is outside the scope of this document.

3. **Internet firewall:** Most ISP routers have at least a basic firewall capability enabled by default. Usually the default firewall settings can be left unchanged. Deploying Aruba Instant On products requires an active internet connection to register and manage them. If you experience difficulty deploying Aruba InstantOn WAPs please consult with the Aruba Technical Assistance Center (TAC).

   TIP
   Record network settings in the ISP router and have them handy for reference during the Small Office Deployment installation. Refer to the ISP router's user guide for details.

Network configuration

Have the following available for network hardware setup.

1. Networking hardware administration—check the hardware user guides for:
   a. Default administrator login credentials
   b. Network configuration instructions
   c. Factory reset instructions (just in case)
2. External public network:
   a. Public IP address(es)—If you intend to map external addresses to internal services such as a web server, obtain the these from the ISP or ISP router.
   b. Public DNS server IP addresses—Acquire these from the ISP router. They are needed to configure internal network DNS forwarding or to set additional DNS servers in DHCP IP configurations.
   c. Public internet domain name (if one exists)—this is needed to prepare for configuring Active Directory and can be acquired from the ISP/domain host provider.
3. Internal private network:
   a. Default route—This is the IP address of the ISP router's internal interface. It is needed to configure DHCP and static network configurations.
   b. Decide on a private network IP address scheme—This is needed to configure DHCP and static network interfaces. Note the following:
      i. Most ISP routers are configured with a default internal class C IP address and network. Typically 192.168.x.x/24 (i.e. subnet mask of 255.255.255.0).
      ii. Plan for expansion. The typical private class C IP address range of 192.168.x.x/24 is sufficient for an initial single segment network for most SMBs and is easily capable of expanding to additional segments.
      iii. Reserve a portion of the IP address range for devices with static IP addresses, including the default route. It is a good idea to use groups of addresses for specific purposes to aid in network administration and troubleshooting.

NOTE

This deployment guide scenario will feature the following IP network scheme, but you should choose the IP network that best meets your needs.

- IP network range: 192.168.1.0/24
- Reserved IP address range: 192.168.1.1 to 192.168.1.99 grouped by:
  - Networking devices: 192.168.1.1 to 192.168.1.24
  - Servers: 192.168.1.25 to 192.168.1.48
  - Printers, other: 192.168.1.49 to 192.168.1.99
- Default route: 192.168.1.254
- DHCP IP address scope: 192.168.1.101 to 192.168.1.253

Server configuration

Have the following available for server setup.

1. Windows Server installation media (USB/DVD), or network URL and log-on credentials to installation files if they are on the network.
2. Decide on a Windows Server name. Any valid name can be used, but it is helpful to give servers and other network equipment a logical name that describes its function, location, and sequential number when more than one of the same equipment type are deployed (for example, CORP-DC01 for the first domain controller deployed at the company headquarters).
3. Decide on a Windows Local Administrator login password.

IMPORTANT
These credentials become the credentials for the Active Directory “Domain Administrator” account upon promoting the server to domain controller. Use a strong password and restrict access to it.

TIP
It’s a best practice to create user-specific administrative accounts and restrict the default Local Administrator or Domain Administrator accounts strictly for last resort access such as when there is a change in personnel.

4. Decide on a Windows Active Directory DSRM password

IMPORTANT
Do not lose or forget this password. This password enables full access to Active Directory objects and can expose the domain to security risks. Use a strong password that is different from the Local Administrator password.

TIP
Record the DSRM password and keep it in a safe place. Best practice is to seal it in an envelope and lock it in a safe (the envelope provides evidence if it has been compromised).

5. Decide on a Windows Active Directory domain name. Note the following.
   a. This is needed to establish an internal private Active Directory domain.
   b. Do not use your public internet domain name as your private Active Directory name, as this has serious security implications.
   c. Best practice is to append a prefix to your internet domain name with a name that identifies your private network. For example, if your internet domain name is mycompany.com, you would append “corp.” to the internet domain name to get corp.mycompany.com.
   d. For more information, refer to this article on the Microsoft TechNet Wiki: “Active Directory: Best Practices for Internal Domain and Network Names.”
6. Windows DNS—Public DNS IP addresses from your ISP are needed to configure DNS forwarders in Windows.
7. To set up Windows DHCP, you will need to acquire:
   a. The IP network address and range.
   b. DHCP scope: The range of IP addresses which will be issued by DHCP.

TIP
Reserve the default route address as well as a contiguous portion of the IP network for assigning static IP addresses on servers and network equipment.

   c. DHCP options: Network settings to be sent with IP address leases for DHCP clients. At a minimum you will need:
      i. A default gateway IP address
      ii. A primary and alternate DNS IP address

Networking deployment

The basic order of network deployment steps is as follows:

1. Connect the Administrative PC (Admin PC) to the network switch.
2. Configure the network switch and connect the ISP to the router using one of two scenarios:
   a. If using Scenario 1, described below, configure the network switch then connect the switch to the ISP router.
   b. If using Scenario 2, described below, connect the switch to the ISP router, then configure the network switch.
3. Connect the Aruba Instant On WAP to the switch.
   a. Configure the WAP.
   b. Configure additional WAPs (optional).
4. Configure the ISP router:
   a. Disable Wi-Fi (recommended if deploying Aruba InstantOn WAPs).
   b. Disable DHCP server (required if deploying Windows DHCP).
5. Deploy Windows Server:
   a. Deploy Active Directory/DNS.
   b. Additional DNS configurations.
   c. Deploy DHCP.
6. Deploy HPE StoreEasy 1460 (optional).

Network switch configuration

The HPE Small Business Solution for Small Office Deployment features either HPE Office Connect 1820, HPE Office Connect 1920s, or Aruba 2530 network switches. These switches can be configured using the embedded Web Administration console. The Web Administration console is an intuitive GUI that enables easy configuration of most switch features.

This guide will cover configuring the HPE Office Connect 1920 switch, but the other switches will have a similar, if not identical, procedure. Refer to the appropriate user guide for details.

Start by connecting an Admin PC to the switch and opening the switch's Web Admin Console. There are two scenarios for performing this task.

1. Scenario 1: Use the default IP address (HPE Office Connect 1820 and 1920s only).

NOTE
The Aruba 2530 switch does not have a default IP address and must be configured using Scenario 2 below, or other methods as noted in the Aruba 2530 User Guide.

IMPORTANT
Do not connect the switch to anything yet.

   a. By default, the switch is configured with an IP address of 192.168.1.1/24.

NOTE
If the switch is connected to a network that also has an active DHCP server, the switch will likely be assigned a different IP address than the default IP address and you will have to use Scenario 2.

TIP
If you want to use the default address for initial, do not connect the switch to anything other than the Admin PC until configuration is complete.

b. Connect an Ethernet cable from the Admin PC to any port on the switch.

c. Configure the Ethernet NIC on the Admin PC with a static IP address of 192.168.1.10/24.

d. Open a supported internet browser and navigate to **http://192.168.1.1** and the switch's Web Admin Console home page will open.

e. Continue to step 3.

2. Scenario 2: Use an IP address configured by DHCP from an ISP router.

   a. Connect the switch to the network that also has an active DHCP server (usually this is your ISP router).

   b. The switch will receive an IP address from the DHCP server, but now you will have to determine what address was assigned.

   c. Connect the Admin PC to the switch (it should also be set to receive an IP address from DHCP).

   d. Most ISP routers have a Web Admin Console and you can browse to it by navigating your Admin PC web browser to its default gateway IP address (run ipconfig from a Windows command prompt to find your IP address and default gateway).

   e. You may be required to log on to the ISP router's console to perform the next steps.

   f. Locate the page that shows what devices are connected to your network (refer to the ISP router user manual). This page usually shows the IP addresses, but you may have to dig a little deeper in the ISP router's configuration pages to find the DHCP server page and locate the IP address that was assigned to the switch.

   g. One of the IP addresses from either page will be the one for the switch. If only the Admin PC and switch are connected to the network this is an easy deduction by knowing the Admin PC IP address from the ipconfig command.

   h. Navigate to **http://(yourSwitchIPAddress)** and the switch's Web Admin Console home page will open.

3. Log in to the switch Web Admin Console with the default username "admin" (there is no default password).

4. Navigate to Maintenance > Password Manager to change the default administrator password to a strong password. Log off and log back on to confirm the password change.

IMPORTANT
Leaving the switch default login unchanged is an extremely risky decision. The default "admin" account is a well-known account and a high-risk target for cyber-attack. Best practice is to:

a. Create a new administrator account for each person who will manage the switch.

b. Assign a strong password to the new account(s).

c. Assign **read/write** privileges only to the new account(s) that will need to make changes to the switch.

d. Log off the default administrator account and login with the new administrative user account and assign an extremely complex random password to the default "admin" account and the access level to **none** to disable the default administrator account.

e. For added security you can delete the admin account.

At a minimum, it is best to change the password then log out and log back in with the new password.

NOTE
You can perform a factory reset if you forget the password. This of course will also clear all configuration changes made to the switch.

5. Set the system name of the switch (recommended). Click “Dashboard” and enter a system name in the field provided, then click “Apply.”

TIP
Any valid name can be used, but it is helpful to give all network equipment and servers a logical name that describes its function, location, and a sequential number (for example, CORP-SW01 for the first switch deployed at the company headquarters).

6. Set a static IP address for remote administration (recommended). Many network devices are configured with a default static IP address of 192.168.1.1/24. Should such a device be introduced to your network it will cause an IP address conflict if this switch is also using 192.168.1.1/24 as its IP address. For this reason, it is highly recommended to change the default IP address. To change the switch IP address, click “Network Setup” to open the “Get Connected” page and configure a static IP address according to your network needs.

NOTE
If you change the IP address to a different network than the current network the Admin PC is using, you will lose connection to the switch once the change is applied and will need to reconfigure the Admin PC accordingly.

Aruba Instant On WAP configuration

Once your switch has been configured, you are ready to deploy Aruba Instant On WAPs to provide wireless access to users on your network.

NOTE
This guide will walk you through configuring Instant On WAPs via the Aruba Instant On mobile application. You can also use the cloud-based portal (web app) but is not discussed here. If required, contact Aruba Instant On support.

1. Mount the WAP(s) to the interior walls/ceilings, or use the AP11D desktop model, which can be placed on a desktop or cabinet shelf.
2. Connect an Ethernet cable to the first WAP and the network switch.
3. Confirm the power source to the WAP.
    a. If the network switch is providing PoE then the Instant On WAP receives power through the Ethernet cable and nothing else is needed.
    b. If the WAP is not connected to a PoE switch port, you must connect the AC power adaptor.
4. Power on the WAP. You should see the status light alternate between amber and green to indicate it’s ready to be configured.
5. Turn on Bluetooth® service on your mobile device.
6. Download and install the Aruba Instant On app to your mobile device.
7. Open the Aruba Instant On app and login; create an account if needed.
8. Tap “continue” on the “Setup a new site” screen.
9. Enter a name for your new network. This will become the Wi-Fi SSID.

IMPORTANT
Choose the network name carefully as it cannot be changed without deleting the site and thus losing all WAPs configured on this site.

10. Enter a password for the new wireless network and tap “Continue.”
11. The app will request access to the mobile devices’ location service. Allow the Aruba Instant On app to access the device’s location.

12. The Instant On app will now proceed to discover any Instant On WAPs that are active via Bluetooth.
    a. If a WAP is found, it will show the model number.
    b. If a WAP is not found, you can enter the WAP's serial number manually.
    c. Once a WAP is found or entered, the app will prompt you to click “Add Device.”
13. Set the site country and accept or modify the recommended site name (by default the app will append the word “site” to the SSID).
14. The app will notify you the new site is ready. Tap “Show it to me” and you will navigate to the site configuration dashboard page.
15. From the dashboard, you can configure many other settings and add WAPs. Please refer to the Aruba Instant On user guide for more details.

NOTE
You can easily add Instant On WAPs that are either connected to the switch or connected to the existing WAP(s) via wireless mesh. The process is the same except the first decision whether the new WAP is wired or mesh.

16. Install the WAP to the environment and, if a wired connection is desired, connect it to the switch.
17. Launch the Aruba Instant On mobile app and tap the devices tile to open the device inventory.
18. Tap the “+” button to open the “Add a new device” page.
19. Tap “How to extend my network.”
20. Tap the desired method:
    a. “Extend over the air” is for a wireless mesh. Just power on the WAP in the vicinity of the existing WAP.
    b. “Extend using a cable” is for a wired connection or to preconfigure a WAP then disconnect it from the switch. It will automatically change to a mesh configuration.
21. Tap “Search for my device.” The app will use Bluetooth to discover the next unconfigured WAP.
22. Tap “Add device” once the device is discovered.
23. Verify the WAP is the one you want to add by checking the serial number, then tap “Accept.”
24. Tap “Give it a name” to name the WAP (optional).
25. Tap “Finish.”
26. The new WAP will synchronize with the existing network. When the synchronization is complete it will be ready for use.

Completing the network configuration

Once the switch and WAPs have been configured, log on to the ISP router. Disable Wi-Fi and disable the DHCP server.

Server deployment

Windows Server installation

Configure the hardware and install the Windows Server OS using Rapid Setup, as described in the Hardware configuration and operating system installation section of this document.

Active directory configuration

This section covers the installation and configuration of Active Directory Domain Services (ADDS). This deployment scenario assumes this is the first domain controller in the ADDS forest and no other domain controllers are on the network.

IMPORTANT
Be sure that the server has been configured with a static IP address before beginning ADDS installation. Also ensure the IP address of the server is listed as the first IP address in the NIC's DNS server settings.

Before you begin deploying Active Directory, you will need to decide what to name your new Active Directory domain. Do not use your public internet domain name as your private Active Directory name, as this has serious security implications. Best practice is to append a prefix to your internet domain name with a name that identifies your private network. Example: If your internet domain name is mycompany.com, you might append "corp." to the internet domain name to get corp.mycompany.com. For more information, read the Microsoft TechNet article: "Active Directory: Best Practices for Internal Domain and Network Names."

NOTE
This scenario will use the name corp.mycompany.com. **Do not use this name in your real-world deployment**.

Install ADDS and DNS

1. From the Server Manager > Dashboard click "Add Roles and Features" to begin the Roles and Features Wizard.
2. From "Before you Begin," note the tasks and setup based on required permissions and network settings. Select "Next."
3. Select "Role-Based Installation." Select "Next."
4. Identify and select your server. Select "Next."
5. Select the ADDS role and the wizard will notify you of additional features that will be installed. Ensure the check box for "Include management tools" is selected. Click "Add Features" to continue.
6. Also select the DNS role and the wizard will again notify you of additional features that will be installed. Ensure the check box for "Include management tools" is selected. Click "Add Features" to continue.

   NOTE
   Leave "File and Storage services" selected on the Select Roles page as certain features are required for Active Directory functions.

7. Click "Next" to proceed to the Select Features page.
8. Click "Next" again on the Select Features page.
9. Click "Next" again to decline installing Azure Active Directory services if offered. You can add these services later if desired.
10. Review the DNS server information listed. Select "Next."
11. Review the "Confirmation installation selections" screen and click "Install" to begin installation.
12. When the installation is complete you will be notified of success (or failure) and presented with the option to configure Active Directory. Click "Close" as you will configure Active Directory in the next section.

Promote the server to domain controller

1. From Server Manager > Dashboard, select the flag in the upper-right corner of the screen to show a drop-down with notifications. Select "Promote this server to a domain controller" to open the ADDS Configuration Wizard. Alternatively, you can navigate directly to the ADDS Configuration Wizard by clicking Active Directory in the Navigation pane of the Server Manager, and selecting the wizard from the Tasks drop-down box in the Active Directory window.
2. From the Active Directory Domain Services Configuration Wizard > Deployment Configurations, select "Add a new forest" since this scenario will be the first server in the Active Directory forest.
3. Input a root domain name that is relevant to you, such as "corp.mycompany.com" and select "Next."

IMPORTANT
Take care when naming your domain because you cannot change it later. Read the Microsoft TechNet article "Active Directory: Best Practices for Internal Domain and Network Names" for more information.

4. Under domain controller options, select the highest functional level available in the drop-down lists for the new forest and root domain.

IMPORTANT
It is critical to the security of your IT environment that you save this password in a safe place with restricted access. This password grants the person using it the ability to do anything to your Active Directory environment and is the only way to recover your Active Directory domain should the need arise. It should be a complex, random password that is not used for anything else, and at least 12 characters so that is not easily guessed or hacked. A best practice is to write down the password, put it in a sealed envelope, and then secure the envelope restricting access to it by whatever physical means is appropriate for your organization. Generally, you should not change this password unless the password has been exposed to unauthorized persons. If it is changed, be sure to update this written password and re-secure it.

5. Review the DNS Options page and click "Next."
6. Under Additional Options, verify or enter the NetBIOS domain name. Normally this should be the prefix that was appended to the internet domain name—in this case "corp." Select "Next."
7. Accept the default file path for your Database, Log, and SYSVOL files to load, unless you have reason to change the path. Select "Next."
8. Review your selected options. Select "Next."
9. The system will perform a prerequisite check and highlight validations needed before promoting the server. Review any errors. If everything is approved, select "Install."

NOTE
Some errors will likely be presented that are corrected automatically upon clicking "Install." The Install button will be disabled if there are errors that prevent successful installation.

10. Your system will reboot.

Verify Active Directory installation

1. Log on to the server using the domain/administrator account. (In our scenario, this is "CORP\Administrator," replacing "CORP" with the NetBIOS name you provide during setup.) This is a default account created during the ADDS promotion and has the same password as the local administrator account.
2. In the Server Manager, navigate to Tools > Active Directory Users and Computers.
3. In the Active Directory Users and Computers management console confirm that the newly created domain is listed in the navigation pane.
4. ADDS initial installation and configuration is complete, but additional settings must be configured in DNS for efficient Active Directory function.
5. There are many additional configuration settings that can be made to ADDS to simplify network administration, manage desktop clients, and manage network security. These settings will be mentioned as needed to complete configuration of the Small Office Deployment solution. All other configuration of Active Directory is beyond the scope of this document.

DNS

IMPORTANT
Be sure that the server has been configured with a static IP address before beginning ADDS installation. Also ensure the IP address of the server is listed as the first IP address in the NIC's DNS server settings. After installing Active Directory, additional settings should be made in DNS to aid in Active Directory functionality. Also, DNS should be configured to forward DNS queries for external network resources to other DNS servers for query resolution.

Verify Active Directory DNS integration

By installing DNS along with ADDS, DNS will be integrated with Active Directory to provide a secure mechanism for maintaining DNS records required by Active Directory. Perform the following steps to verify DNS is Active Directory integrated.

1. On the Server Manager page click Tools > DNS to open the DNS console.
2. Expand the server in the navigation tree and click "Forward Lookup Zones."
3. If DNS is Active Directory integrated you will see the zone "_msdcs.corp.mycompany.com" and the zone "corp.mycompany.com" (replace corp.mycompany.com with your new domain name).

Create a new reverse lookup zone for the new Active Directory Domain

1. Right-click "Reverse Lookup Zone" and select "New zone."
2. At the Welcome screen click "Next."
3. At the Zone Type screen select "Primary zone" (should be default) and ensure the checkbox for "Store the zone in Active Directory" is selected then click "Next."
4. From the AD Zone Replication Scope page, accept the default selection of all DNS servers running on domain controllers in the domain "corp.mycompany.com" (replace with your domain) and click "Next."
5. At the Reverse Lookup Zone Name screen accept the default IPv4 selection and click "Next."
6. At the second page of Reverse Lookup Zone Name enter the IP network address (192.168.1 in this scenario; use your network address in place of this example) and click "Next."
7. At the Dynamic Update screen accept the default "Allow only secure dynamic updates" and click "Next."
8. Click "Next" again to complete the zone configuration.
9. Expand the reverse lookup zone in the navigation pane and click on the newly created zone (shown as the network IP address in reverse order) and confirm "Start of Authority" and "Name Server" records are present.
10. Click on corp.mycompany.com under Forward Lookup Zones in the navigation pane. Then, in the results pane, right-click the DNS record for this server and click "Properties," then enable the checkbox "Update the associated pointer (PTR) record" and click "Apply," then "OK."
11. Navigate to the reverse lookup zone and find the new PTR record for this server. (You may have to refresh the zone view. Right-click in the results pane and click "Refresh.")
12. Verify the DNS server PTR record is listed in the reverse lookup zone.

Reconfigure the server NIC preferred DNS settings

1. In the Server Manager navigation pane, click "Local Server." In the results pane, click on the IP address link for "Ethernet" to open Network Connections to see the NIC.
2. Right-click the icon for the NIC and click "Properties."
3. Select internet Protocol IP version 4 and click "Properties."
4. If not already present, enter the server's IP address in "Preferred DNS Server."

NOTE
This will likely have the local loop address of 127.0.0.1. If so, replace this with the server's IP address.

Verify DNS is functioning

1. Open a PowerShell command window.
2. Type “nslookup” and press “Enter” to start the NSLOOKUP utility.
3. PowerShell should respond with the servers’ IP address and fully qualified domain name (servername.corp.mycompany.com in this scenario).
4. Type “corp.mycompany.com” and press “Enter.”
5. NSLOOKUP should respond with the server’s IP address.
6. Type the server’s IP address (e.g. 192.168.1.25 for this example) and press “Enter.”
7. NSLOOKUP should respond with the server’s fully qualified domain name.

Configure DNS forwarding

By default, Windows Server DNS installs a list of public “DNS Root Servers” which is used by Windows DNS to resolve DNS queries from clients when the Windows DNS server does not know how to resolve the client’s query.

This can be a slow process and a request can time out before getting a response. Adding a DNS Forwarder can speed up query response by checking with DNS connected “closer” to your network, such as the ISP’s own DNS servers. To do so:

1. Right-click on the DNS server in the navigation pane and click “Properties.”
2. Click on the Forwarders tab.
3. Click “Edit” to add a forwarder.
4. Enter the IP address for a DNS server that will resolve DNS queries if this server cannot resolve the query itself. In this deployment scenario, enter the Default Gateway IP address of 192.168.1.254.

NOTE
Typically, the ISP router is also configured as a forwarder to the ISP’s DNS server.

TIP
Leave the “Use Root Hints” checkbox enabled; this will be used as a last resort if no DNS server is able to answer the client query.

IMPORTANT
Be careful to ensure you have the correct IP address for an external DNS server. A common cyber-attack is to replace the legitimate DNS server IP address with the IP address for a malicious DNS server. When network clients try to resolve a DNS query, they will be given an IP address for a malicious server instead, potentially resulting in compromising the client computer’s security.

5. If desired, set a value for query time out (the default three seconds is generally sufficient for most cases), and click “OK.”
6. Click “OK” to close the DNS server properties.
7. Ensure DNS is functioning by attempting a ping of a common website like google.com.

DHCP

IMPORTANT
Be sure that the server has been configured with a static IP address before beginning DHCP installation. DHCP provides IP addresses for clients requesting IP address leases. If you are implementing Windows DHCP server, you must either:

1. Disable all other DHCP servers (recommended), including your ISP router if it is providing DHCP service.
2. Ensure other DHCP servers are not providing IP addresses in the same scope as the Windows DHCP server.

Before configuring DHCP you will need to know your planned IP address scheme. This deployment scenario uses the following scheme which you can use as a model:

- IP network range: 192.168.1.0/24
- Reserved IP address range: 192.168.1.1 to 192.168.1.99 grouped by:
  - Networking devices: 192.168.1.1 to 192.168.1.24
  - Servers: 192.168.1.25 to 192.168.1.48
  - Printers, other: 192.168.1.49 to 192.168.1.99
- Default Route: 192.168.1.254
- DHCP IP address scope: 192.168.1.101 to 192.168.1.25

Select DHCP from wizard

1. From the Server Manager > Dashboard click "Add Roles and Features" to begin the Roles and Features Wizard.
2. From "Before you Begin," note the tasks and setup based on required permissions and network settings. Select "Next."
3. Select "Role-Based Installation." Select "Next."
4. Choose this server as the host where the DHCP server should be installed. Select "Next."
5. Select "DHCP Server" from Server Roles screen by clicking the check box on the left-hand side. Select "Next."
6. Following the DHCP server selection, an additional window will appear adding extra tools that are needed to ensure successful installation. Select "Add Features" to accept the default features, then select "Next" to proceed.
7. From the DHCP server screen review the information. Select "Next."
8. Confirm final selections. Select "Install."
9. Monitor the progress bar. Once complete, select "Close."

DHCP configuration post-installation wizard

1. In the Server Manager, click on the yellow "Notifications" flag in the upper-right hand corner and select "Complete DHCP Configuration."
2. Review the DHCP Admin and users that will be created via the new wizard. Select "Next."
3. Authorize the DHCP server to be used in Active Directory using the default Domain Admin account then select "Commit."

NOTE
If your server is not part of any Active Directory, choose "Skip AD Authorization."

4. Verify the security groups and Active Directory authorization were successful, then select "Close."

Create a DHCP scope

NOTE
Creating a scope allows you to preconfigure a range of IP addresses that are available for your DHCP clients on a specific network. This deployment scenario will create a scope that provides a portion of the available addresses to DHCP clients, as was described at the start of the DHCP section.

1. On the Server Manager, click "Tools," then "DHCP." The DHCP manager will open.
2. From the menu select Action > New Scope.
3. Once the Scope Wizard launches review the introduction. Select "Next."
4. Give your scope a name and description so it is identifiable to you, click "Next."
5. Enter the start and end IP address (192.168.1.101 and 192.168.1.253 respectively for this deployment scenario).

6. Enter either the CIDR length (24) or the subnet mask (255.255.255.0). The other field will auto-populate. Click “Next.”
7. Add any exclusions and delays needed to reserve IP addresses for future devices. In this scenario we have excluded the appropriate IP addresses by not including them in the DHCP scope. Select “Next.”
8. Accept the default lease duration, or change it to meet your needs, and click “Next.”
9. Choose whether to configure DHCP options for this scope or not. Since this is the only scope in this deployment scenario, we will configure additional options. Select “Yes, I want to configure these options now” and click “Next.”

NOTE
DHCP clients will need default route and DNS server IP addresses to function on your network.

10. On the “Router (Default Gateway)” page enter the IP address of your ISP router or network gateway to the internet (e.g. 192.168.1.254 in this scenario). This can be quickly determined by running ipconfig in a Windows command prompt and looking up the default gateway IP address.
11. On the Domain Name and DNS server page include your internal domain (corp.mycompany.com in this scenario). Also enter the IP address of all DNS servers that the DHCP clients on your network should use (in this scenario we will use this server’s IP address and the ISP router’s IP address of 192.168.1.254 as a second DNS server). Again, you can use ipconfig to see a list of DNS servers used by the server.

NOTE
The list of DNS server IP addresses is a prioritized list. DHCP clients will use the address at the top of the list first and proceed downward through the list if there is no response from the DNS server. It is a good practice to put the address of the Active Directory DNS server first in the list if Active Directory is running. Adding the ISP router address as a second DNS server IP address enables DHCP clients to get a response from a DNS server on the ISP’s network in case this server is unable to respond.

12. Click “Next.”
13. Include WINS server information if necessary. WINS is a legacy technology and is typically no longer needed. Click “Next.”
14. Activate your scope or decide to postpone for later. If this is the case, no DHCP addresses will be provided by this scope until it is activated. Select “Next.”
15. Your DHCP server has been configured. Select “Finish.”

Test the DHCP service

1. Log on to a computer that is configured to get its IP address from DHCP.
2. Ensure the ISP router DHCP service is disabled.
3. Open a Windows command prompt.
4. Type “ipconfig /all” and press “Enter” to view current IP configurations.
5. If more than one NIC is installed, locate the interface connected to the same network as the DHCP server.
6. Ensure the IP address for “DHCP Server” is the address of the DHCP server just deployed.
7. Type “ipconfig /release” and press “Enter” to prepare for testing the DHCP server, all DHCP provided leases will be removed.
8. Type “ipconfig /renew” and press “Enter” to request a new IP address from the DHCP server. Wait a few seconds for the IP address to be renewed.

9. Type “ipconfig /all” and verify once again that the IP address was received from the DHCP server just deployed.

NOTE
If you get a lease from a different IP address than expected, it means you have multiple DHCP servers on your network and you must troubleshoot to find and disable the rogue DHCP server. This usually occurs when the ISP router DHCP service has not been disabled.

File and backup services

The installation and configuration of Microsoft Windows file and backup services is covered in the HPE Small Business Solutions for File and Backup with Microsoft Windows section of this document.

HPE Small Business Solutions for HCI (Hyperconverged Infrastructure) with Microsoft Storage Spaces Direct

The HPE Small Business Solution for HCI with Microsoft Storage Spaces Direct is the easiest and most cost-effective way to setup an on-premises hyperconverged infrastructure (HCI) with integrated software-defined storage (SDS). It enables you to create a Storage Spaces Direct cluster with as few as two servers and expand the cluster as your capacity needs grow by simply adding more servers to the cluster, with no downtime. The SDS redundancy provided by Microsoft Storage Spaces Direct combined with the reliability of HPE fault tolerance, high availability, and resiliency features work together to create a resilient Hyper-V virtualized environment with cluster-shared storage. In addition, the deduplication feature available on Windows Server 2019 Storage Spaces Direct provides improved write performance and optimized capacity utilization.

NOTE
Microsoft Storage Spaces Direct is the SDS technology built into Microsoft Windows Server 2016 and 2019 Datacenter versions. The Microsoft Windows Server Software-Defined (WSSD) program for Windows Server 2016 and Azure Stack HCI for Windows Server 2019 are Microsoft marketing and validation programs built around Storage Spaces Direct to offer specific Storage Spaces Direct based configurations to customers. The configurations approved by Azure Stack HCI program for Windows Server 2019 and the WSSD program for Windows Server 2016 have gone through Microsoft approved testing cycles in the vendor’s lab. See HPE Solutions for Microsoft Azure Stack HCI for the current list of validated configurations.

NOTE
The setup used in this deployment guide is a Microsoft Storage Spaces Direct configuration. In the future, the configuration used in the document may be approved by the Azure Stack HCI program. However, the deployment steps captured in this document remain the same in general for an Azure Stack HCI configuration. See HPE Solutions for Microsoft Azure Stack HCI for the current list of validated configurations.

The following setup instructions are based on HPE ProLiant DL360 Gen10 Servers but can also be applied to the other HCI configurations with HPE ProLiant ML350 Gen10, DL180 Gen10, DL380 Gen10, and DL385 Gen10 Servers.

This document was created using 2 ProLiant DL360 nodes to create a 2 node Storage Spaces Direct cluster using Windows Server 2019 Datacenter. Each of the DL360 in the cluster had the following components:

- 1 x Intel® Xeon® Silver 4110 CPU (8 cores) @ 2.10 GHz
- 64 GB RAM
- 4 x 1.2 TB SFF 10K SAS drives
- 2 x 480 GB SFF SATA SSD drives
- 2 x 240 GB SATA MU M.2 SSD (Mirrored OS drives)
- HPE Universal SATA HH M.2 Kit
- HPE Smart Array E208i-p storage controller
- Ethernet 10/25 GB 2-Port 640FLR-SFP28 Adapter

Set up the HPE ProLiant DL360 Gen10 servers

1. Install the 4 x 16 GB RAM in the memory slots as per the HPE DIMM installation guide.
2. Remove the disk drive covers from the front of the server and install the 4 x 1.2 TB SFF 10K SAS drives and the 2 x 480 GB SFF SATA SSD drives.
3. Remove the server top cover panel and raise the PCIe cage; set it aside.
4. Install the Ethernet 10/25 GB 2-port adapter in the slot that can be seen below after removing the PCIe cage. You will need to remove the metal cover from the 2-port slot opening in the back of the server, which is secured with a screw, before installing the Ethernet adapter.

NOTE
The HPE Small Business Solution for HCI comes with the P408i-p Smart Array controller. If no P408i-p controller is available, the E208i-p is a lower cost option.

5. Install the Smart Array controller in Slot 1 of the PCIe cage. You can install it in Slot 2 of the cage as well, but it may require a longer SAS cable to connect the drives from the front of the server to the 2-ports of the controller.
6. Connect the SAS cables from the disk drives at the front of the server to the controller, Port 1 to Port 1 and Port 2 to Port 2.
7. Install the 2 x 240 GB M.2 SATA SSD drives in the universal SATA M.2 kit. You will need to remove the screw to install the drive and replace the screw after installing the drive to secure it.
8. Install the universal M.2 kit in Slot 2 (or Slot 1 if Slot 2 was used for Smart Array controller in Step 5 above) of the PCIe cage. If installing on Slot 2, you will need to switch the metal rail on the M.2 kit to the supplied smaller rail so that it can install on the PCIe cage.
9. Connect the two SATA cables from the M.2 kit to the SATA ports on the motherboard.
10. Replace the PCIe cage and secure it until it latches.
11. Replace the server top cover panel and secure it.
12. Mount the server to the rack using the easy install rails supplied.

Prepare the servers for Windows 2019 installation

After both servers are mounted on the rack, perform these steps:

NOTE
This “direct-connect” configuration is for a 2-node solution. If more than two servers are used in the Storage Spaces Direct, please refer to Microsoft documentation listed on page 51.

1. Cross-connect the two servers using the SFP cable. Connect Port 1 on the Ethernet 10/25 GB adapter on Server 1 to the Port 2 on the Ethernet 10/25 GB adapter on Server 2. Similarly, connect Port 2 on Server 1 to Port 1 on Server 1.
2. Connect the iLO 1 GB Ethernet ports on Server 1 and Server 2 to the top of rack (ToR) switch.
3. Connect any one of the 4 x 1 GB Ethernet ports to the ToR switch for both servers.
4. Connect the dual power supply unit for each server to the power outlet, two power cables per server.
5. Power on the servers.
6. By default, the iLO DNS name, User name (Administrator) and Password printed on a label located on top of the server.
7. From your remote access device, point the browser to the https://<iLO_DNS_Name> and supply the iLO administrator/password to login to each server.
8. Install the iLO license key in the iLO license key section.

NOTE
Without the iLO license key, the remote session to the server will get disconnected after a minimal timeout.

9. Register the server with HPE per the iLO instructions, using your HPE passport credentials.

10. Ensure that the health of both the servers is **green** on the iLO pages.

NOTE
At times, the server health may report as “Degraded” with a warning symbol on the iLO page. Please refer to the Update firmware and drivers section of this document for more details on a possible fix.

Install Windows Server 2019

Windows Server 2019 can be installed on the M.2 SSDs of both the servers in the following way:

1. Acquire the Windows Server 2019 ISO image and the license code.
2. Create a bootable USB stick with the ISO image on your laptop.

NOTE
HPE recommends using Rufus software to create the image. Bootable USB sticks created from other software products caused the installation to fail or hang in the middle of the process.

NOTE
While installing Windows, disable secure boot in the server BIOS. You can turn secure boot back on after the OS is installed on the primary M.2 boot disk.

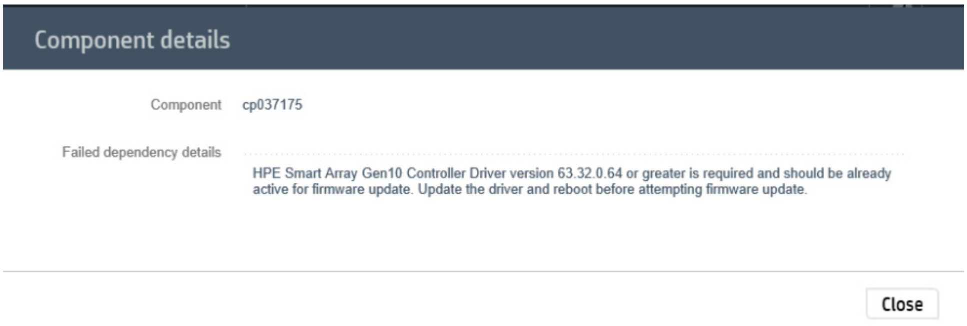
3. Insert the bootable USB sticks into the servers and reboot them from USB. This will start the OS installation on the server. This can be performed and monitored from a remote session to the iLO webpage of the servers.
4. Go through the Windows Server 2019 installation wizard, supply the license code, and start the installation.
5. You have the option to select either the Datacenter Edition or the Datacenter Desktop Experience Edition. Install the Datacenter edition if you are comfortable working with PowerShell and scripting. Install Datacenter with Desktop Experience Edition if you would like to use a graphical user interface (GUI). Note that the Datacenter Desktop Edition will take more storage space on the servers than the Datacenter Edition. Datacenter Desktop was used in this installation.
6. Choose the first M.2 SSD SATA drive that appears in the list of drives on the installation wizard.

NOTE
There are two M.2 SSD SATA drives in this configuration, which should be configured in RAID 1 so that one M.2 SSD drive is a mirror of the other drive. This RAID 1 configuration can be performed later, after the OS is installed, using the Windows RAID mechanism in the Windows Disk Configuration Utility. Refer to the Set up a RAID 1 mirror for the M.2 Boot drive section of this document for directions.

7. Once the installation is complete, the server will reboot and prompt you to set the Administrator password. Set the password and login to Windows Server 2019.

Upgrade the HPE Smart Array Controller drivers

The Smart Array Controller’s driver must be updated on Windows Server 2019. If the Smart Array Controller driver is not updated, you will receive an error message:



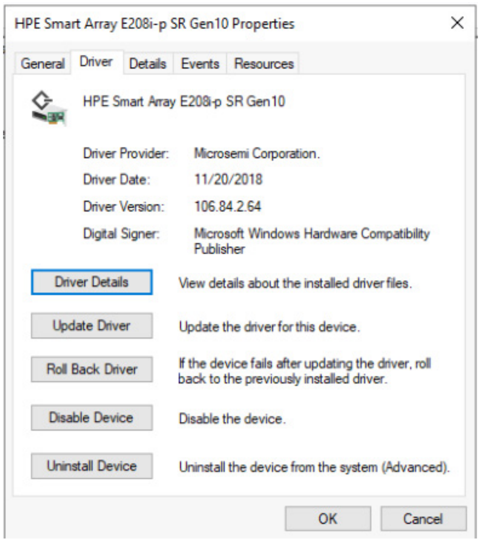
Component details

Component cp037175

Failed dependency details

HPE Smart Array Gen10 Controller Driver version 63.32.0.64 or greater is required and should be already active for firmware update. Update the driver and reboot before attempting firmware update.

1. Install the latest Windows Server 2019 driver controllers from the HPE Support Center.
2. After performing the driver update, the driver version can be double-checked as below:



HPE Smart Array E208i-p SR Gen10 Properties

HPE Smart Array E208i-p SR Gen10

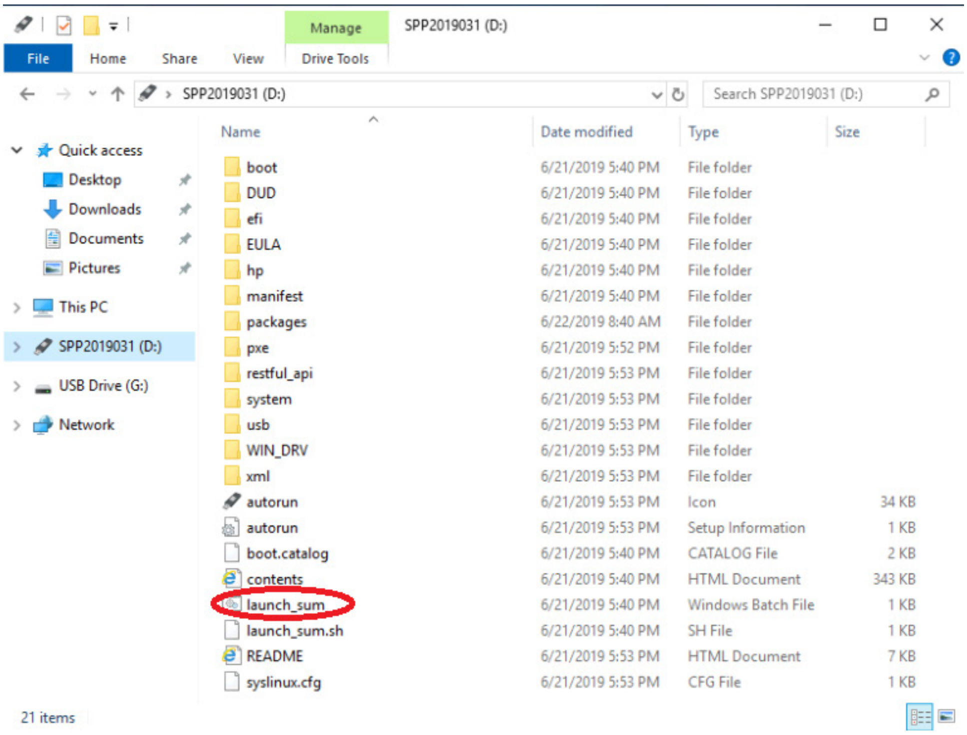
Driver Provider: Microsemi Corporation.
Driver Date: 11/20/2018
Driver Version: 106.84.2.64
Digital Signer: Microsoft Windows Hardware Compatibility Publisher

Driver Details — View details about the installed driver files.
Update Driver — Update the driver for this device.
Roll Back Driver — If the device fails after updating the driver, roll back to the previously installed driver.
Disable Device — Disable the device.
Uninstall Device — Uninstall the device from the system (Advanced).

Update server firmware and drivers

After logging in to Windows Server 2019 on both servers, it is important to update the servers' firmware and Windows Server drivers. This is required for the successful installation of the Windows Server components necessary to deploy Storage Spaces Direct and to fix any degraded levels in the iLO health monitor on the servers.

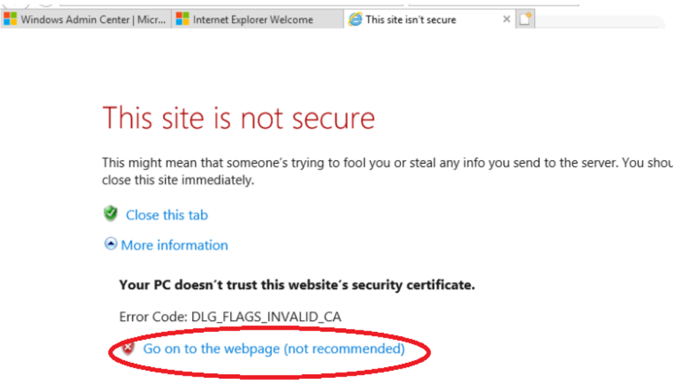
1. Download the HPE Service Pack for ProLiant (SPP) ISO image.
2. Create a bootable USB stick as described earlier in this document.
3. Insert the USB stick into the servers and navigate to the USB drive in the File Explorer.
4. Run the launch_sum.bat file from the USB drive on the Windows Server 2019 desktop.



Name	Date modified	Type	Size
boot	6/21/2019 5:40 PM	File folder	
DUD	6/21/2019 5:40 PM	File folder	
efi	6/21/2019 5:40 PM	File folder	
EULA	6/21/2019 5:40 PM	File folder	
hp	6/21/2019 5:40 PM	File folder	
manifest	6/21/2019 5:40 PM	File folder	
packages	6/22/2019 8:40 AM	File folder	
pxe	6/21/2019 5:52 PM	File folder	
restful_api	6/21/2019 5:53 PM	File folder	
system	6/21/2019 5:53 PM	File folder	
usb	6/21/2019 5:53 PM	File folder	
WIN_DRV	6/21/2019 5:53 PM	File folder	
xml	6/21/2019 5:53 PM	File folder	
autorun	6/21/2019 5:53 PM	Icon	34 KB
autorun	6/21/2019 5:53 PM	Setup Information	1 KB
boot.catalog	6/21/2019 5:40 PM	CATALOG File	2 KB
contents	6/21/2019 5:40 PM	HTML Document	343 KB
launch_sum	6/21/2019 5:40 PM	Windows Batch File	1 KB
launch_sum.sh	6/21/2019 5:40 PM	SH File	1 KB
README	6/21/2019 5:53 PM	HTML Document	7 KB
syslinux.cfg	6/21/2019 5:53 PM	CFG File	1 KB

21 items

5. This will launch the HPE SUM web-based UI in the default browser on the Windows Server 2019 desktop. Accept the insecure server side certificate (as the root certificates aren't installed and configured yet) and proceed to the SUM page.



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You shou close this site immediately.

Close this tab

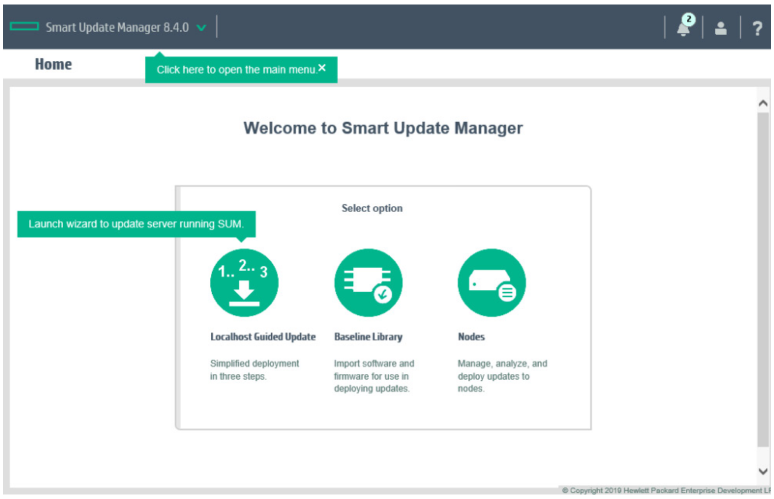
More information

Your PC doesn't trust this website's security certificate.

Error Code: DLG_FLAGS_INVALID_CA

Go on to the webpage (not recommended)

6. From the SUM UI, choose "Localhost Guided Update."


Smart Update Manager 8.4.0
Home
Click here to open the main menu ×
1.. 2.. 3
© Copyright 2019 Hewlett Packard Enterprise Development LP

Welcome to Smart Update Manager

Launch wizard to update server running SUM.

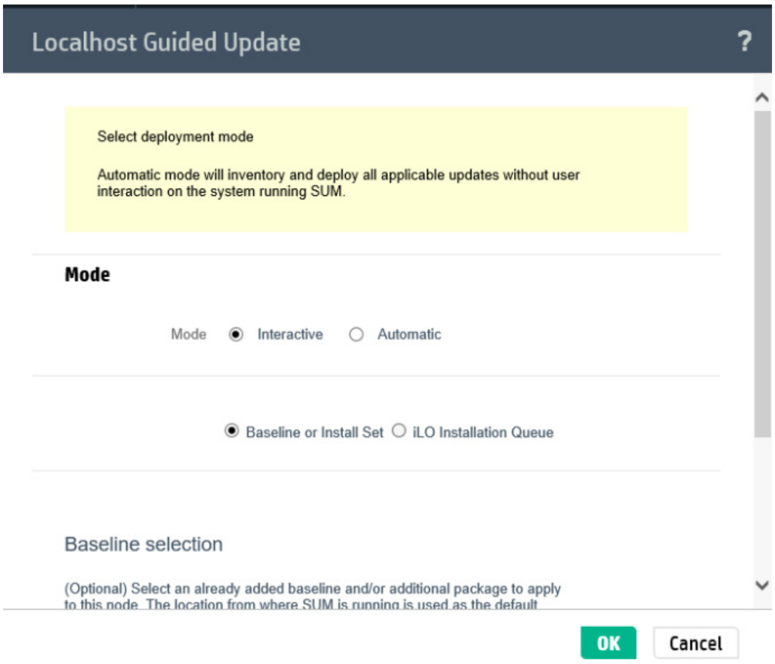
Select option

Localhost Guided Update: Simplified deployment in three steps.

Baseline Library: Import software and firmware for use in deploying updates.

Nodes: Manage, analyze, and deploy updates to nodes.

7. Choose "Interactive" mode, "Baseline or Install Set" for the SUM firmware update as shown below. Note that Automatic mode can also be selected, however, interactive mode was used for this documentation. Click "OK" to continue.



Localhost Guided Update

Select deployment mode

Automatic mode will inventory and deploy all applicable updates without user interaction on the system running SUM.

Mode

Mode ● Interactive ○ Automatic

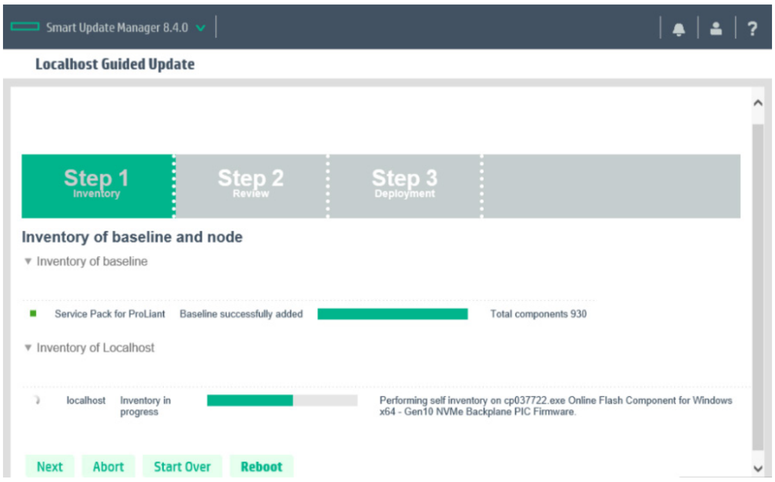
● Baseline or Install Set ○ iLO Installation Queue

Baseline selection

(Optional) Select an already added baseline and/or additional package to apply to this node. The location from where SUM is running is used as the default

8. This will start the baselining and inventory building processes. Once completed, SUM will list the components to be updated. Review and accept them to start the firmware update.

NOTE
During the firmware update, the remote session to the server via the iLO will disconnect briefly, which is normal.



Inventory of baseline and node

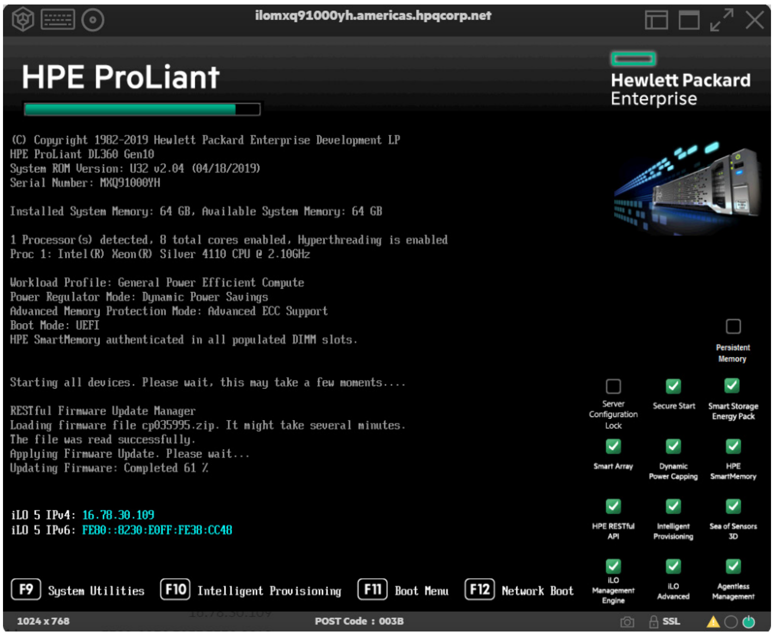
▼ Inventory of baseline

■ Service Pack for ProLiant Baseline successfully added Total components 930

▼ Inventory of Localhost

localhost Inventory in progress Performing self inventory on cp037722.exe Online Flash Component for Windows x64 - Gen10 NVMe Backplane PIC Firmware.

9. Once the firmware is updated successfully, reboot the server by clicking on the "Reboot" button on the SUM page. The firmware will update during the reboot, as shown below.

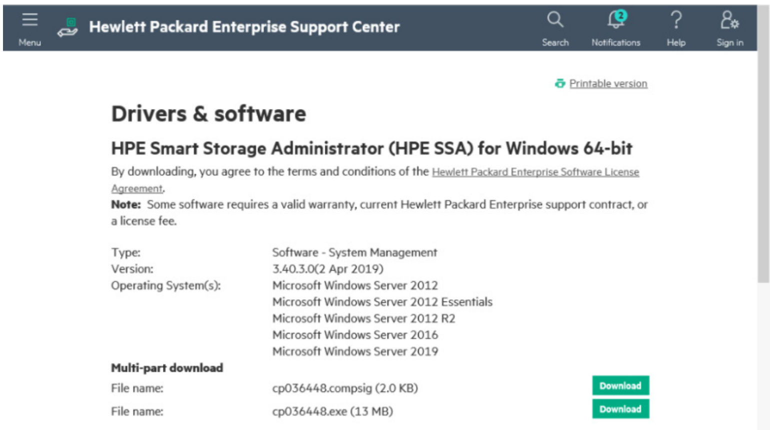


```
(C) Copyright 1982-2019 Hewlett Packard Enterprise Development LP
HPE ProLiant DL360 Gen10
System ROM Version: U32 v2.04 (04/18/2019)
Serial Number: MXQ91000YH

Installed System Memory: 64 GB, Available System Memory: 64 GB

1 Processor(s) detected, 8 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz

Workload Profile: General Power Efficient Compute
Power Regulator Mode: Dynamic Power Savings
Advanced Memory Protection Mode: Advanced ECC Support
Boot Mode: UEFI
HPE SmartMemory authenticated in all populated DIMM slots.

Starting all devices. Please wait, this may take a few moments....

RESTful Firmware Update Manager
Loading firmware file cp035995.zip. It might take several minutes.
The file was read successfully.
Applying Firmware Update. Please wait...
Updating Firmware: Completed 61 %

iLO 5 IPv4: 16.78.30.109
iLO 5 IPv6: FE80::8230:E0FF:FE38:CC48
```

Configure the HPE Smart Array Controller to operate in HBA mode

The HPE Smart Array Controller is set by default to operate in Mixed Mode, where the raw drives attached to the servers can be presented directly to the OS as raw drives in HBA mode or can be presented as hardware-controlled RAID drives in RAID mode. For Storage Spaces Direct, the drives must be presented to the servers in HBA mode.

1. Download the HPE Smart Storage Administrator (SSA).



Drivers & software

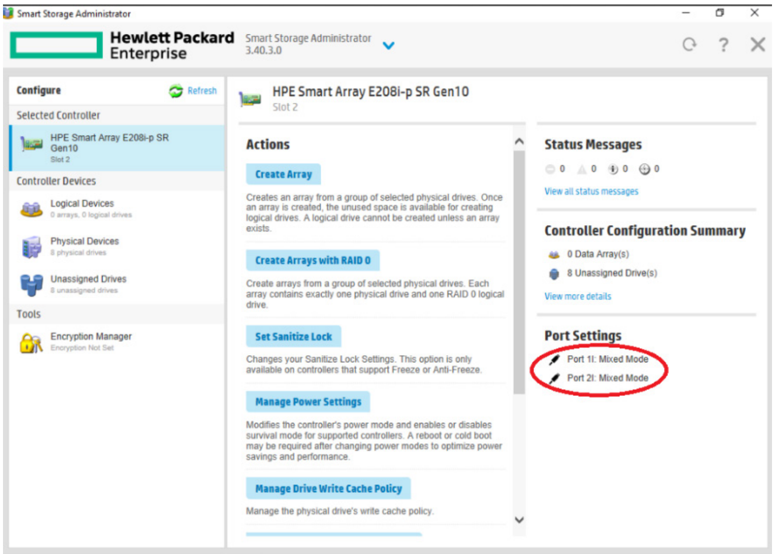
HPE Smart Storage Administrator (HPE SSA) for Windows 64-bit

By downloading, you agree to the terms and conditions of the Hewlett Packard Enterprise Software License Agreement.

Note: Some software requires a valid warranty, current Hewlett Packard Enterprise support contract, or a license fee.

Type:	Software - System Management
Version:	3.40.3.0(2 Apr 2019)
Operating System(s):	Microsoft Windows Server 2012 Microsoft Windows Server 2012 Essentials Microsoft Windows Server 2012 R2 Microsoft Windows Server 2016 Microsoft Windows Server 2019
Multi-part download	
File name:	cp036448.compsig (2.0 KB) Download
File name:	cp036448.exe (13 MB) Download

2. Open the HPE SSA. Confirm that the Smart Array Controller to which the Storage Spaces Direct drives are connected via SAS cable are set to operate in Mixed Mode, as shown in the screenshot below:



HPE Smart Array E208i-p SR Gen10
Slot 2

Actions

Create Array

Creates an array from a group of selected physical drives. Once an array is created, the unused space is available for creating logical drives. A logical drive cannot be created unless an array exists.

Create Arrays with RAID 0

Create arrays from a group of selected physical drives. Each array contains exactly one physical drive and one RAID 0 logical drive.

Set Sanitize Lock

Changes your Sanitize Lock Settings. This option is only available on controllers that support Freeze or Anti-Freeze.

Manage Power Settings

Modifies the controller's power mode and enables or disables survival mode for supported controllers. A reboot or cold boot may be required after changing power modes to optimize power savings and performance.

Manage Drive Write Cache Policy

Manage the physical drive's write cache policy.

Status Messages

0 0 0 0

View all status messages

Controller Configuration Summary

0 Data Array(s)

8 Unassigned Drive(s)

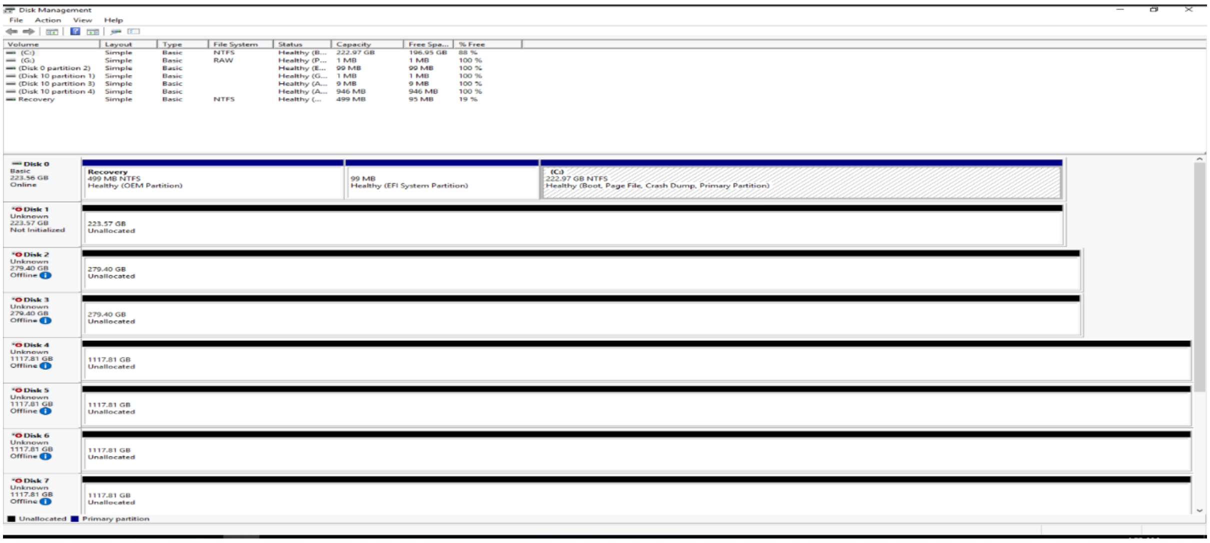
View more details

Port Settings

Port 1I: Mixed Mode

Port 2I: Mixed Mode

3. With the proper configuration of the controller, the OS will show the raw drives as below:



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	222.97 GB	196.95 GB	88 %
(G:)	Simple	Basic	RAW	Healthy (P...	1 MB	1 MB	100 %
(Disk 0 partition 2)	Simple	Basic		Healthy (E...	99 MB	99 MB	100 %
(Disk 10 partition 1)	Simple	Basic		Healthy (G...	1 MB	1 MB	100 %
(Disk 10 partition 3)	Simple	Basic		Healthy (A...	9 MB	9 MB	100 %
(Disk 10 partition 4)	Simple	Basic		Healthy (A...	946 MB	946 MB	100 %
Recovery	Simple	Basic	NTFS	Healthy (...	499 MB	95 MB	19 %

Disk 0
Basic
223.56 GB
Online

Recovery
499 MB NTFS
Healthy (OEM Partition)

99 MB
Healthy (EFI System Partition)

(C:)
222.97 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Unknown
223.57 GB
Not Initialized

223.57 GB
Unallocated

Disk 2
Unknown
279.40 GB
Offline

279.40 GB
Unallocated

Disk 3
Unknown
279.40 GB
Offline

279.40 GB
Unallocated

Disk 4
Unknown
1117.81 GB
Offline

1117.81 GB
Unallocated

Disk 5
Unknown
1117.81 GB
Offline

1117.81 GB
Unallocated

Disk 6
Unknown
1117.81 GB
Offline

1117.81 GB
Unallocated

Disk 7
Unknown
1117.81 GB
Offline

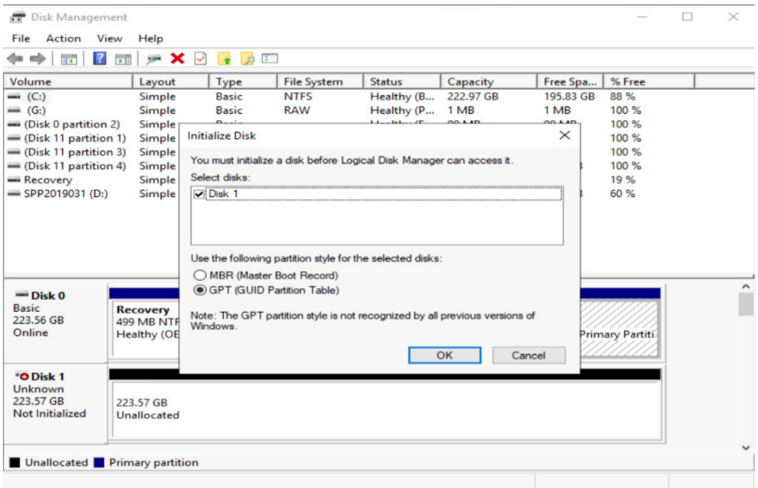
1117.81 GB
Unallocated

■ Unallocated ■ Primary partition

Set up a RAID 1 mirror for the M.2 Boot drive

The M.2 SATA SSD drives must be configured as RAID 1 mirror drives so that the Windows Server 2019 boot drive can be protected against a single M.2 drive failure. Perform the following steps on both servers.

1. Open the Disk Management utility in Windows Server 2019.
2. Locate the second M.2 SATA SSD drive (on which there is nothing installed) and initialize the disk as a GPT disk.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	222.97 GB	195.83 GB	88 %
(G:)	Simple	Basic	RAW	Healthy (P...	1 MB	1 MB	100 %
(Disk 0 partition 2)	Simple						100 %
(Disk 11 partition 1)	Simple						100 %
(Disk 11 partition 3)	Simple						100 %
(Disk 11 partition 4)	Simple						100 %
Recovery	Simple						19 %
SPP2019031 (D:)	Simple						60 %

Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1

Use the following partition style for the selected disks:

○ MBR (Master Boot Record)

● GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

OK Cancel

Disk 0
Basic
223.56 GB
Online

Recovery
499 MB NTF
Healthy (OE

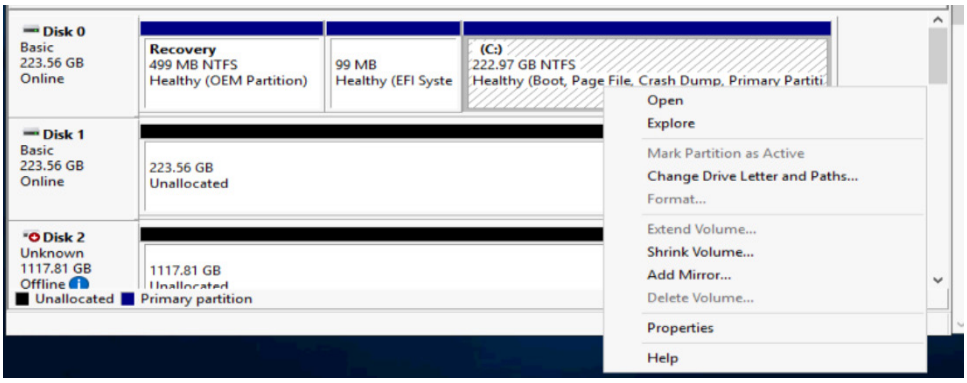
Primary Partiti

Disk 1
Unknown
223.57 GB
Not Initialized

223.57 GB
Unallocated

■ Unallocated ■ Primary partition

3. Locate the M.2 SATA SSD drive on which the Windows Server 2019 is installed and right click on it to locate the “Add Mirror” option as shown below:



Disk 0
Basic
223.56 GB
Online

Recovery
499 MB NTFS
Healthy (OEM Partition)

99 MB
Healthy (EFI Syste

(C:)
222.97 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partiti

Disk 1
Basic
223.56 GB
Online

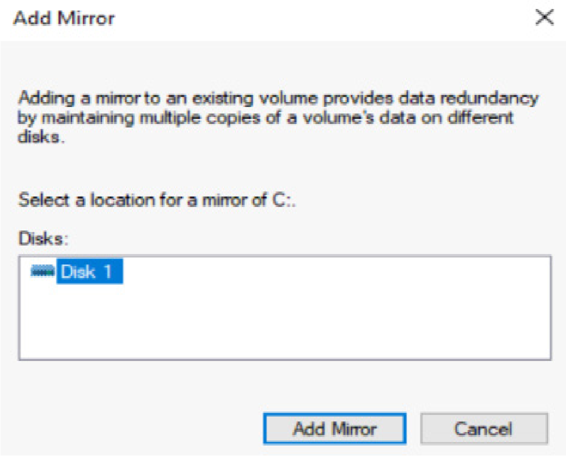
223.56 GB
Unallocated

Disk 2
Unknown
1117.81 GB
Offline

1117.81 GB
Unallocated

■ Unallocated ■ Primary partition

4. Select “Add Mirror” and choose the second M.2 SSD drive as the mirror destination.



Add Mirror

Adding a mirror to an existing volume provides data redundancy by maintaining multiple copies of a volume's data on different disks.

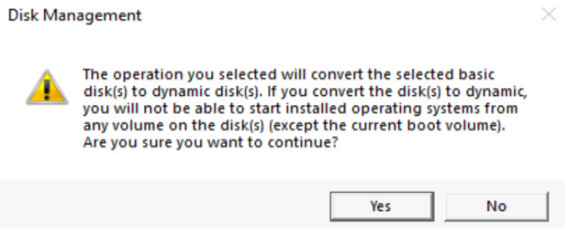
Select a location for a mirror of C:.

Disks:

Disk 1

Add Mirror Cancel

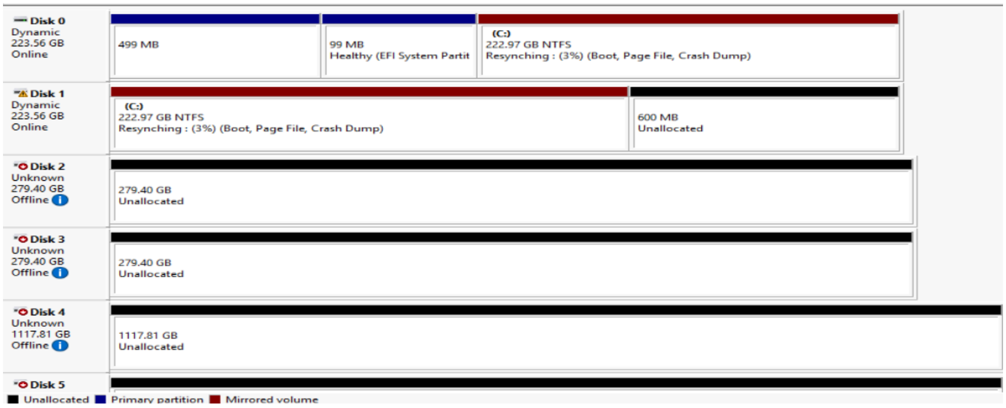
5. Click "OK." You will see a warning message as below. Accept the message and proceed.



Disk Management

The operation you selected will convert the selected basic disk(s) to dynamic disk(s). If you convert the disk(s) to dynamic, you will not be able to start installed operating systems from any volume on the disk(s) (except the current boot volume). Are you sure you want to continue?

6. This will begin the process of synching the drives so that the current M.2 boot drive and the second M.2 drive become a mirror of each other.



Disk 0
Dynamic
223.56 GB
Online

499 MB

99 MB
Healthy (EFI System Partit

(C:)
222.97 GB NTFS
Resynching : (3%) (Boot, Page File, Crash Dump)

Disk 1
Dynamic
223.56 GB
Online

(C:)
222.97 GB NTFS
Resynching : (3%) (Boot, Page File, Crash Dump)

600 MB
Unallocated

Disk 2
Unknown
279.40 GB
Offline

279.40 GB
Unallocated

Disk 3
Unknown
279.40 GB
Offline

279.40 GB
Unallocated

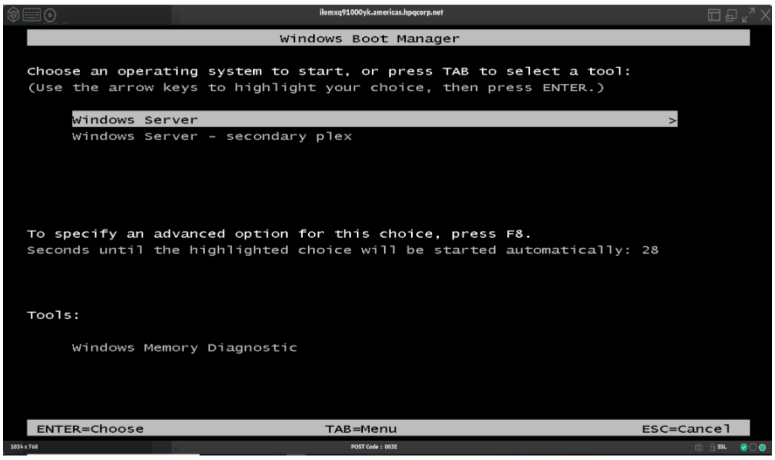
Disk 4
Unknown
1117.81 GB
Offline

1117.81 GB
Unallocated

Disk 5

■ Unallocated ■ Primary partition ■ Mirrored volume

7. Once the sync is complete, subsequent reboots of the server will start showing two options for boot as shown below, which indicates that the configuration is correct.



```
                         Windows Boot Manager

Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)

     Windows Server                                                >
     Windows Server - secondary plex




To specify an advanced option for this choice, press F8.
Seconds until the highlighted choice will be started automatically: 28



Tools:

     Windows Memory Diagnostic



 ENTER=Choose                    TAB=Menu                    ESC=Cancel
```

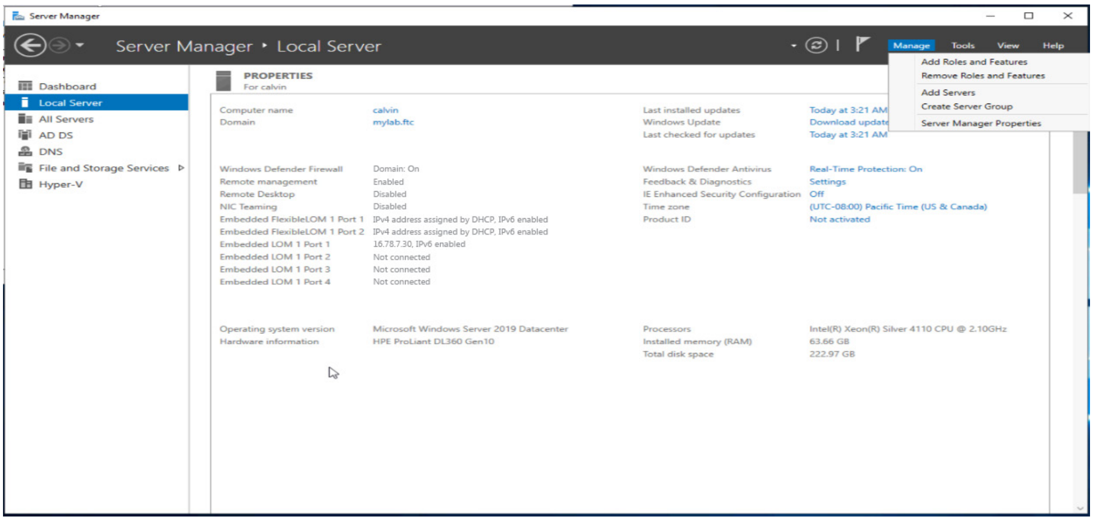
Install and configure Active Directory and DNS

The servers in the Storage Spaces Direct cluster need to be joined to the same Active Directory domain. Also, the Active Directory domain user name that is used to login to the Storage Spaces Direct cluster servers should be added to the server's Windows Server 2019 local Administrator group. For example, if the servers are joined to the Active Directory domain "mylab.ftc" and if the domain user called administrator@mylab.ftc is used to administer the servers then administrator@mylab.ftc needs to be added to the localhost\Administrator account group on those servers.

NOTE

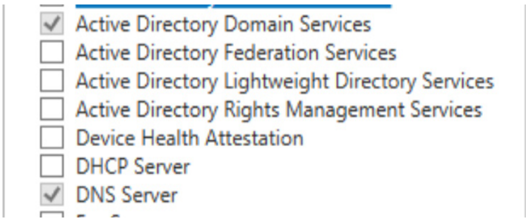
Do not promote one of the Storage Spaces Direct servers as a Domain Controller. Storage Spaces Direct is not supported on Domain Controller nodes. This means a separate Domain Controller Windows system is required to provide the Active Directory domain services. If there is no existing Active Directory Domain Controller, then refer to the "Install and Configure Active Directory and DNS" section of this Deployment Guide.

1. Identify a separate server that can act as the Active Directory Domain Controller. **Do not** use one of the HPE Small Business Solutions for HCI with Microsoft Storage Spaces Direct cluster nodes.
2. Install Windows Server 2019 as described earlier in this document.
3. Configure a static IP address for the server:
   a. Go to Server Manager → 1 GB Ethernet Adapter → Properties → TCP/IP IPv4 → Properties → Use Static IP address.
   b. Set the static IP, Subnet Mask, Default Gateway, and DNS servers.
4. Install the Active Directory and DNS services on the designated Active Directory Domain Controller server.
   a. Go to Server Manager → Manage → Add Roles and Features → Role Based or feature based installation.
   b. Select the local server and check the box for "Active Directory Domain Services" and "DNS Server."
   c. Click on "Add Features."



PROPERTIES
For calvin

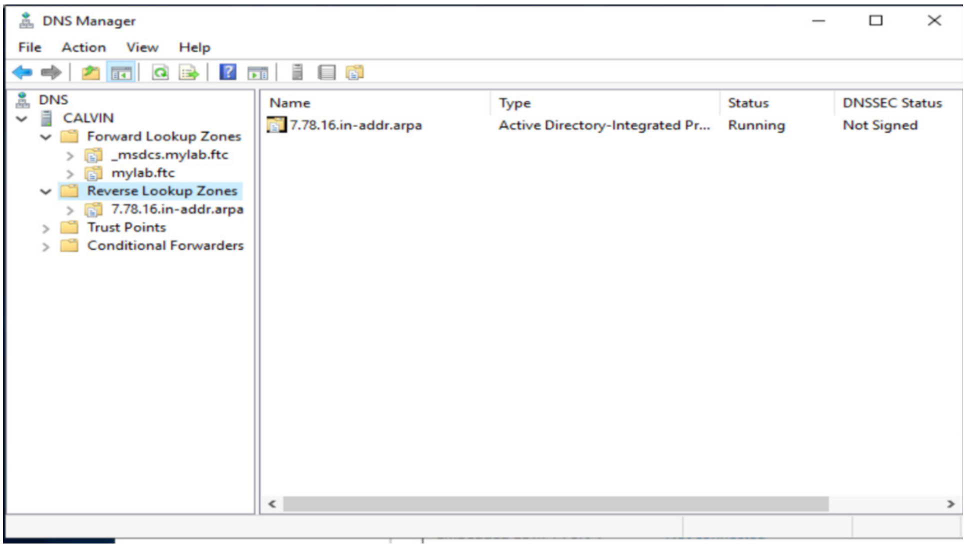
Computer name	calvin	Last installed updates	Today at 3:21 AM
Domain	mylab.ftc	Windows Update	Download update
		Last checked for updates	Today at 3:21 AM
Windows Defender Firewall	Domain: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Embedded FlexibleLOM 1 Port 1	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	Not activated
Embedded FlexibleLOM 1 Port 2	IPv4 address assigned by DHCP, IPv6 enabled		
Embedded LOM 1 Port 1	16.78.7.30, IPv6 enabled		
Embedded LOM 1 Port 2	Not connected		
Embedded LOM 1 Port 3	Not connected		
Embedded LOM 1 Port 4	Not connected		
Operating system version	Microsoft Windows Server 2019 Datacenter	Processors	Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
Hardware information	HPE ProLiant DL360 Gen10	Installed memory (RAM)	63.66 GB
		Total disk space	222.97 GB



☑ Active Directory Domain Services
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Device Health Attestation
☐ DHCP Server
☑ DNS Server

5. Click "Next" repeatedly, accepting the default selections, and start the install.
6. Once the installation is complete, click on the "Promote this server to a domain controller" link that appears at the end of the installation. This will promote the computer as domain controller for the chosen domain.
7. Accept the defaults and click "Next" until the promotion starts.
8. The server will automatically restart after the promotion is complete.
9. After the reboot you will see the login as <domain_name>\Administrator where <domain_name> is the domain name you chose.
10. After reboot go to Server Manager → Tools → DNS → Expand Server.

11. Right click on “Reverse Lookup Zones” and click “New Zone.”

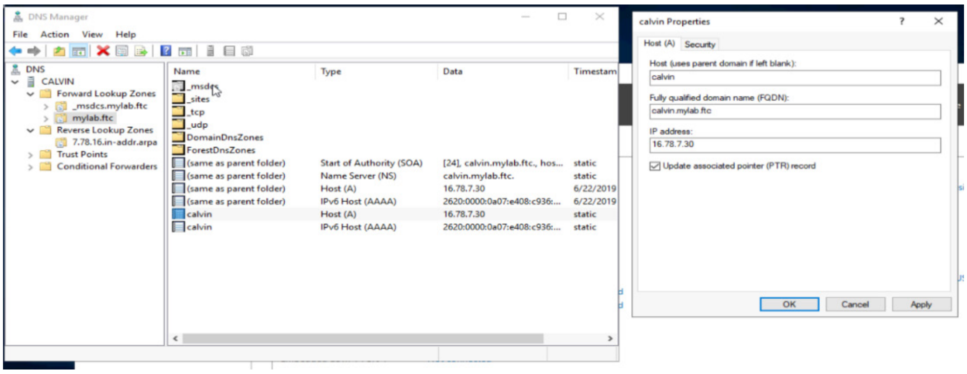


Name	Type	Status	DNSSEC Status
7.78.16.in-addr.arpa	Active Directory-Integrated Pr...	Running	Not Signed

12. Click “Next” repeatedly to accept defaults. When you reach the Network ID input section, enter the first three octets of the server’s IP address.

13. Click “Next” to accept the defaults and click “Finish.”

14. Ensure that the DNS PTR record is updated as shown below:



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[24], calvin.mylab.ftc., hos...	static
(same as parent folder)	Name Server (NS)	calvin.mylab.ftc.	static
(same as parent folder)	Host (A)	16.78.7.30	6/22/2019
(same as parent folder)	IPv6 Host (AAAA)	2620:0000:0a07:e408:c936:...	6/22/2019
calvin	Host (A)	16.78.7.30	static
calvin	IPv6 Host (AAAA)	2620:0000:0a07:e408:c936:...	static

Host (uses parent domain if left blank): calvin

Fully qualified domain name (FQDN): calvin.mylab.ftc

IP address: 16.78.7.30

☑ Update associated pointer (PTR) record

15. Set the preferred DNS of the current server to the current server’s own IP address, as the current server is the domain controller and the DNS for the forest. This needs to be performed at Server Manager → 1 GB Ethernet Adapter → Properties → TCP/IP IPv4 → Properties.

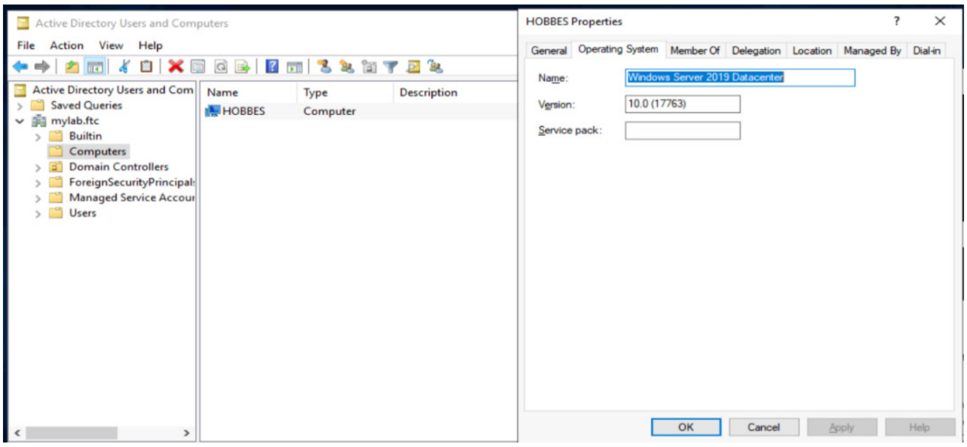
16. After this step, make sure you can nslookup and ping your domain name. It should resolve to the current server’s IP address.

Join the servers to the Active Directory Domain

The Storage Spaces Direct cluster servers must be joined to that domain. Perform the below steps on all the Storage Spaces Direct cluster servers.

1. Rename the cluster servers to have a meaningful name that will be easy to remember/identify. This can be done in Server Manager.
2. Go to Server Manager → 1 GB Ethernet → Properties → TCP/IP IPv4 → Properties and set the preferred DNS to the IP address of Active Directory domain controller.
3. Make sure you can nslookup and ping the domain name.
4. Make sure you can nslookup and ping <domain_controller>.<domain_name>
5. Once the nslookup and ping works, go to Server Manager → Local Server → Workgroup → Change → Add to Domain and enter the new domain name.
6. The last step will prompt for a user name and password. Specify the user name/password of an existing user from the domain with privileges to add computers to the domain.
7. A success message will appear.
8. Reboot the server.

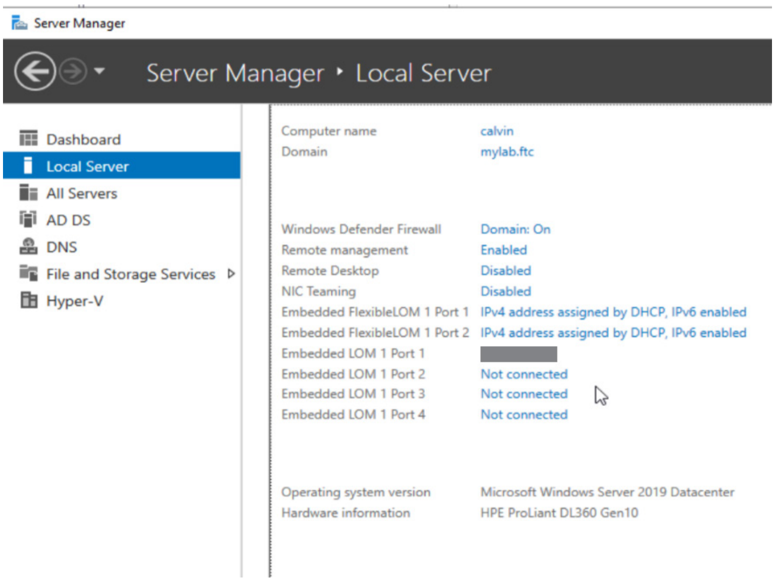
9. After the reboot, login to the domain controller server using the domain administrator account and ensure that the newly joined server is visible under Server Manager → Tools → Active Directory Domain Users and Computers.



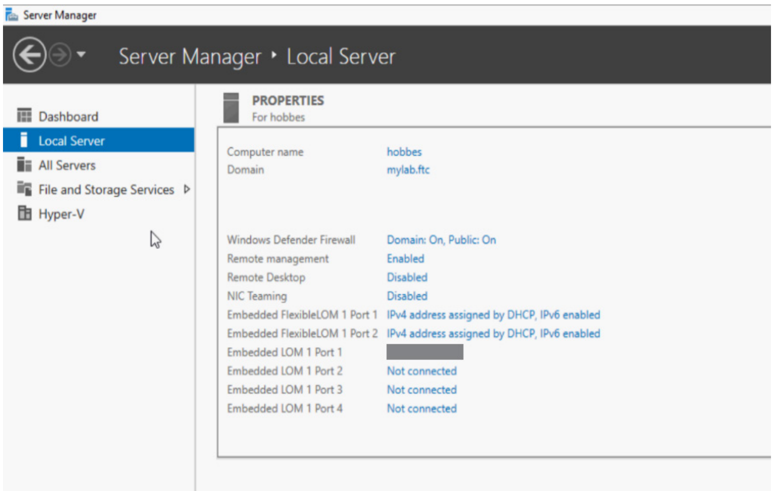
Name	Type	Description
HOBBES	Computer	

Name: Windows Server 2019 Datacenter
Version: 10.0 (17763)
Service pack:

10. After successfully joining, the Storage Spaces Direct cluster nodes Server Manager will show that they belong to the new domain as shown below:



Computer name	calvin
Domain	mylab.ftc
Windows Defender Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Embedded FlexibleLOM 1 Port 1	IPv4 address assigned by DHCP, IPv6 enabled
Embedded FlexibleLOM 1 Port 2	IPv4 address assigned by DHCP, IPv6 enabled
Embedded LOM 1 Port 1	[redacted]
Embedded LOM 1 Port 2	Not connected
Embedded LOM 1 Port 3	Not connected
Embedded LOM 1 Port 4	Not connected
Operating system version	Microsoft Windows Server 2019 Datacenter
Hardware information	HPE ProLiant DL360 Gen10



Computer name	hobbes
Domain	mylab.ftc
Windows Defender Firewall	Domain: On, Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Embedded FlexibleLOM 1 Port 1	IPv4 address assigned by DHCP, IPv6 enabled
Embedded FlexibleLOM 1 Port 2	IPv4 address assigned by DHCP, IPv6 enabled
Embedded LOM 1 Port 1	[redacted]
Embedded LOM 1 Port 2	Not connected
Embedded LOM 1 Port 3	Not connected
Embedded LOM 1 Port 4	Not connected

Configure the network

Refer to the following documentation to learn about how to set up the network on the Storage Spaces Direct cluster nodes.

- Storage Spaces Direct in Windows Server 2019: Section 3.2.3: RDMA networking options
- Deploying Storage Spaces Direct from Microsoft

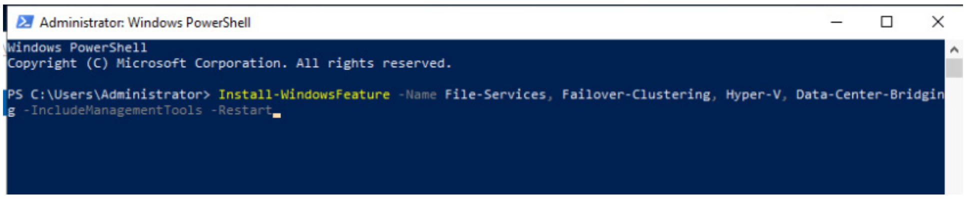
Set up Storage Spaces Direct

The servers should now be in a ready state for Storage Spaces Direct to be turned on and configured. Follow the steps below to set up and enable the Storage Spaces Direct on the two-node cluster.

Install the prerequisite Windows features

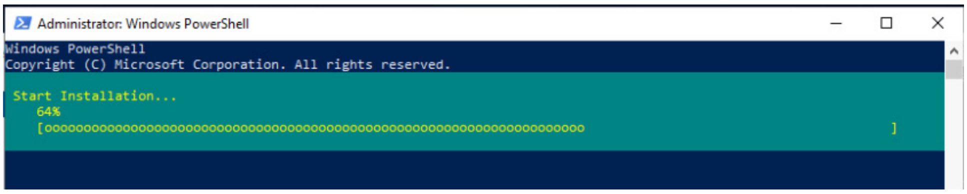
On each of the servers, open the PowerShell command line window and run:

```
Install-WindowsFeature -Name File-Services, Failover-Clustering, Hyper-V, Data-Center-Bridging
-IncludeManagementTools -Restart
```



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

PS C:\Users\Administrator> Install-WindowsFeature -Name File-Services, Failover-Clustering, Hyper-V, Data-Center-Bridgin
g -IncludeManagementTools -Restart
```

This will install the prerequisites and restart the server automatically.

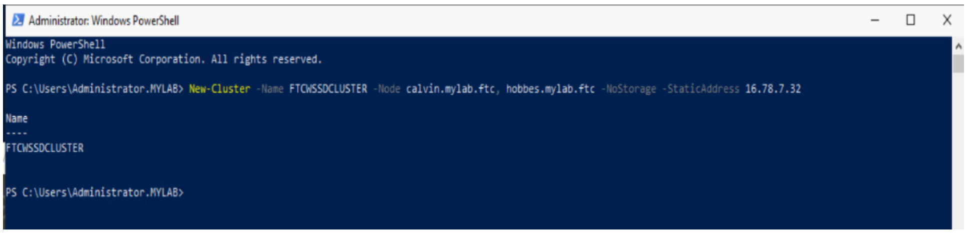


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

 Start Installation...
    64%
    [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo                                      ]
```

Create the Windows Server Cluster

On one of the cluster nodes, open the PowerShell command line window and run the following command:

```
New-Cluster -Name <cluster_name> -Node <server1_name>.<domain_name>,
<server2_name>.<domain_name> -NoStorage -StaticAddress <Static_IP_address_for_Cluster>.
```



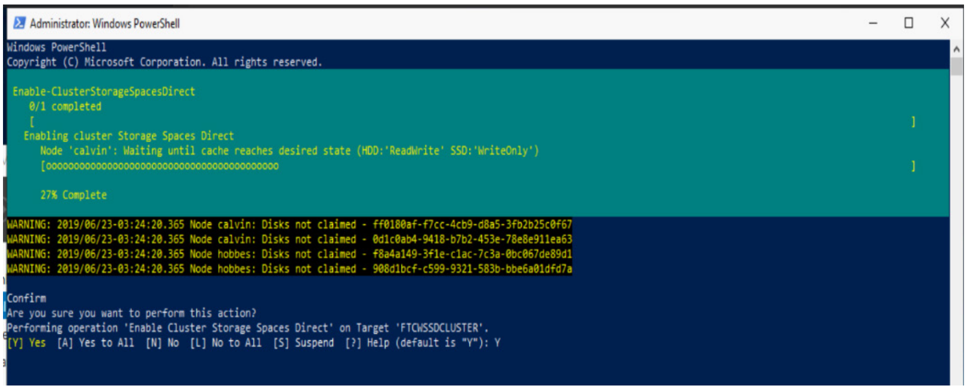
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.MYLAB> New-Cluster -Name FTCWSSDCLUSTER -Node calvin.mylab.ftc, hobbes.mylab.ftc -NoStorage -StaticAddress 16.78.7.32

Name
----
FTCWSSDCLUSTER


PS C:\Users\Administrator.MYLAB>
```

Enable Storage Spaces Direct

Before you can enable Storage Spaces Direct, all the disk drives which will be used by Storage Spaces Direct must be empty. One way to accomplish this is by using the PowerShell scripts available from Microsoft in the **Clean Drives** section of the Storage Spaces Direct documentation.

1. Once the drives are clean, you can enable Storage Spaces Direct using the PowerShell command:

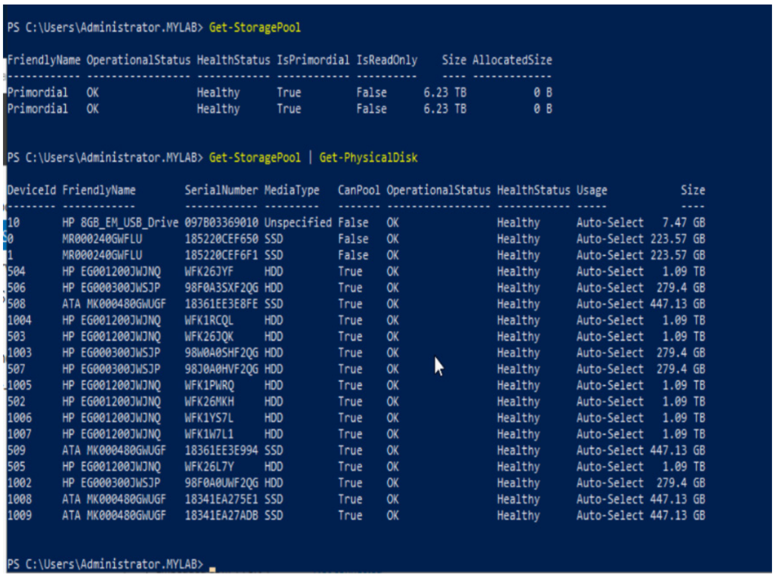
   `Enable-ClusterStorageSpacesDirect`.



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

 Enable-ClusterStorageSpacesDirect
    0/1 completed
    [                                                                                                                   ]
   Enabling cluster Storage Spaces Direct
      Node 'calvin': Waiting until cache reaches desired state (HDD:'ReadWrite' SSD:'WriteOnly')
      [oooooooooooooooooooooooooooooooooooooooooo                                                                      ]

      27% Complete

WARNING: 2019/06/23-03:24:20.365 Node calvin: Disks not claimed - ff0180af-f7cc-4cb9-d8a5-3fb2b25c0f67
WARNING: 2019/06/23-03:24:20.365 Node calvin: Disks not claimed - 0d1c0ab4-9418-b7b2-453e-78e8e911ea63
WARNING: 2019/06/23-03:24:20.365 Node hobbes: Disks not claimed - f8a4a149-3f1e-c1ac-7c3a-0bc067de89d1
WARNING: 2019/06/23-03:24:20.365 Node hobbes: Disks not claimed - 908d1bcf-c599-9321-583b-bbe6a01dfd7a

Confirm
Are you sure you want to perform this action?
Performing operation 'Enable Cluster Storage Spaces Direct' on Target 'FTCWSSDCLUSTER'.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
```

2. While Storage Spaces Direct is being configured, you can see that all the raw disk drives from all the nodes in the cluster are visible via the PowerShell command:

   `Get-StoragePool | Get-PhysicalDisk`.



```
PS C:\Users\Administrator.MYLAB> Get-StoragePool

FriendlyName OperationalStatus HealthStatus IsPrimordial IsReadOnly    Size AllocatedSize
------------ ----------------- ------------ ------------ ----------    ---- -------------
Primordial   OK                Healthy      True         False      6.23 TB           0 B
Primordial   OK                Healthy      True         False      6.23 TB           0 B


PS C:\Users\Administrator.MYLAB> Get-StoragePool | Get-PhysicalDisk

DeviceId FriendlyName       SerialNumber MediaType   CanPool OperationalStatus HealthStatus Usage          Size
-------- ------------       ------------ ---------   ------- ----------------- ------------ -----          ----
10       HP 8GB_EM_USB_Drive 097B03369010 Unspecified False   OK                Healthy      Auto-Select   7.47 GB
0        MR000240GWFLU      185220CEF650 SSD         False   OK                Healthy      Auto-Select 223.57 GB
1        MR000240GWFLU      185220CEF6F1 SSD         False   OK                Healthy      Auto-Select 223.57 GB
504      HP EG001200JWJNQ   WFK26JYF     HDD         True    OK                Healthy      Auto-Select   1.09 TB
506      HP EG000300JWSJP   98F0A3SXF2QG HDD         True    OK                Healthy      Auto-Select  279.4 GB
508      ATA MK000480GWUGF  18361EE3E8FE SSD         True    OK                Healthy      Auto-Select 447.13 GB
1004     HP EG001200JWJNQ   WFK1RCQL     HDD         True    OK                Healthy      Auto-Select   1.09 TB
503      HP EG001200JWJNQ   WFK26JQK     HDD         True    OK                Healthy      Auto-Select   1.09 TB
1003     HP EG000300JWSJP   98W0A0SHF2QG HDD         True    OK                Healthy      Auto-Select  279.4 GB
507      HP EG000300JWSJP   98J0A0HVF2QG HDD         True    OK                Healthy      Auto-Select  279.4 GB
1005     HP EG001200JWJNQ   WFK1PWRQ     HDD         True    OK                Healthy      Auto-Select   1.09 TB
502      HP EG001200JWJNQ   WFK26MKH     HDD         True    OK                Healthy      Auto-Select   1.09 TB
1006     HP EG001200JWJNQ   WFK1YS7L     HDD         True    OK                Healthy      Auto-Select   1.09 TB
1007     HP EG001200JWJNQ   WFK1W7L1     HDD         True    OK                Healthy      Auto-Select   1.09 TB
509      ATA MK000480GWUGF  18361EE3E994 SSD         True    OK                Healthy      Auto-Select 447.13 GB
505      HP EG001200JWJNQ   WFK26L7Y     HDD         True    OK                Healthy      Auto-Select   1.09 TB
1002     HP EG000300JWSJP   98F0A0UWF2QG HDD         True    OK                Healthy      Auto-Select  279.4 GB
1008     ATA MK000480GWUGF  18341EA275E1 SSD         True    OK                Healthy      Auto-Select 447.13 GB
1009     ATA MK000480GWUGF  18341EA27ADB SSD         True    OK                Healthy      Auto-Select 447.13 GB


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

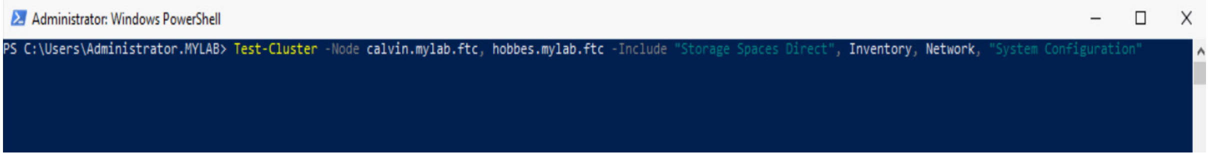
Test the cluster

Once Storage Spaces Direct has been successfully created, it can be tested using the PowerShell command:

`Test-Cluster -Node <server1_name>.<domain_name>, <server2_name>.<domain_name> -Include “Storage Spaces Direct”, Inventory, Network, “System Configuration”.`

NOTE

It is important that all the tests pass before moving forward with the next steps. Any failures in the tests need to be resolved before proceeding.



```
PS C:\Users\Administrator.MYLAB> Test-Cluster -Node calvin.mylab.ftc, hobbes.mylab.ftc -Include "Storage Spaces Direct", Inventory, Network, "System Configuration"
```

Create volumes

Once Storage Spaces Direct has been successfully enabled, the volumes (LUNs) can be carved out of the storage pool formed from the combined raw disk drives from all the nodes in the cluster.

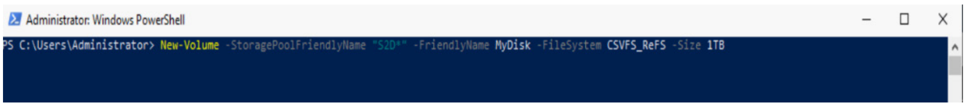
For information about planning and creating volumes in Storage Spaces Direct, see the following documentation from Microsoft:

- Planning volumes in Storage Spaces Direct
- Creating volumes in Storage Spaces Direct

To create a volume, run the PowerShell command:

```
New-Volume -StoragePoolFriendlyName “S2D*” -FriendlyName <volume_name> -FileSystem CSVFS_ReFS |
CSVFS_NTFS -Size <number>TB
```

Refer to the New-Volume PowerShell command line document reference at Microsoft website for more details on the usage.



```
PS C:\Users\Administrator> New-Volume -StoragePoolFriendlyName "S2D*" -FriendlyName MyDisk -FileSystem CSVFS_ReFS -Size 1TB
```

Additional resources

This document is not intended to replace the Storage Spaces Direct deployment guides from Microsoft and other related PowerShell reference documentation. It is intended to capture the experiences of deploying Storage Spaces Direct on Windows Server 2019 using the two-node cluster configuration as provided by the HPE Small Business Solution for HCI. Please refer to the following links for more details:

- Deploying Storage Spaces Direct from Microsoft
- Overview of Azure Stack HCI from Microsoft
- HPE and Microsoft Alliance—Azure Stack HCI Solutions
- Technical white paper from HPE on Implementing Azure Stack HCI with Windows Server 2019
- Creating Volumes in Storage Spaces Direct from Microsoft
- HPE iLO 5 User Guide
- HPE Service Pack for ProLiant (SPP)
- PowerShell cmdlet reference guide from Microsoft

SUPPORT AND OTHER RESOURCES

HPE enterprise support

- For live assistance, go to the contact HPE website: hpe.com/assistance.
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website: hpe.com/support/hpesc.

Updates

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

- To download product updates:
  - Hewlett Packard Enterprise Support Center: hpe.com/support/hpesc.
  - Hewlett Packard Enterprise Support Center, software downloads: hpe.com/support/downloads.
  - Software Depot: hpe.com/support/softwaredepot.
- To subscribe to eNewsletters and alerts: hpe.com/support/e-updates.
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center, More Information on Access to Support Materials page: hpe.com/support/accesstosupportmaterials.

IMPORTANT
Access to some updates might require product entitlement when accessed through the HPE Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website: support.hpe.com/hpesc/public/home.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

- HPE Get Connected: hpe.com/services/getconnected
- HPE Proactive Care Services: hpe.com/services/proactivecare
- HPE Proactive Care Services, supported products list: hpe.com/services/proactivecaresupportedproducts
- HPE Proactive Care Advanced service, supported products list: hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

- Proactive Care Central: hpe.com/services/proactivecarecentral
- Proactive Care Central—Get Started: hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below.

- HPE ProLiant and IA-32 servers and options: hpe.com/support/proliantservers-warranties
- HPE Storage products: hpe.com/support/storage-warranties
- HPE Networking products: hpe.com/support/networking-warranties

Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center.

Documentation feedback

HPE is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

APPENDIX A: MIGRATING TO MICROSOFT WINDOWS SERVER 2019

Microsoft Windows Server 2008 is reaching end of support (EoS) in 2019, and Windows Server 2012 will also be reaching EoS before long. SMBs need a strategy for migrating existing applications and data that are running on older hardware and older versions of Windows Server. This section discusses some of the strategies and details for migrating to Windows Server 2019 with a focus on resolving some issues specific to SMBs.

Migration considerations

For most SMBs there are three types of data to consider when migrating to new server platforms:

- Migrating Active Directory-Directory Services (ADDS)
- Migrating file storage data
- Migrating applications and databases

There are two primary methods used to migrate these data types:

- Upgrade in place—HPE does not recommend upgrade in place, especially if running older versions of applications on old hardware.
    a. Old hardware will not likely meet system requirements for upgrade in place to new operating system or new application
    b. Old applications may not be compatible with new operating systems
    c. Even if it is possible (and supported) to upgrade in place, the chances are high that you will simply be rolling old digital artifacts that have accumulated over the years into your upgraded deployment, increasing the chances of support calls that you were trying to avoid by not migrating in the first place
- Physical to Physical (P2P) migration—deploy the latest version of the application on new hardware running a new operating system and then migrating the application data from the old system to the new system.
- Physical to Virtual (P2V) migration—similar to P2P, but the target system is a virtual machine running the latest application on new hardware running a new operating system and then migrating the application data from the old system to the new system.
- Physical to Virtual (P2V) conversion—a temporary “stop-gap” solution where a conversion utility is run on the old server to convert it to a format that can be run on a new virtualization host.

This section covers the considerations and steps for migrating the three data types using both migration methods, with links to outside resources where appropriate.

Migrating ADDS (P2P or P2V)

1. Deploy a physical server with the Windows Server 2019 operating system (OS) as noted in this document or provision a virtual server with the Windows Server 2019 OS.
2. Install ADDS and promote the server to a Domain controller, thus synchronizing it to the existing domain.
3. Transfer the Active Directory Flexible Single Master Operations (FSMO) roles from the old server to the new server.
4. **IMPORTANT:** If the old server is to be decommissioned, uninstall ADDS from the old server while it is still on the network and connected to the new ADDS server. This will ensure the best possible cleanup of ADDS database objects. If the old server is decommissioned or re-purposed without this step you must manually clean Active Directory which requires very specialized skills and could negatively impact Active Directory.
5. **Recommended:** If the old server will be decommissioned after uninstalling ADDS:
    a. Reset the password for the local administrator account
    b. Unjoin the domain using the System Properties settings
    c. Reboot the server and log in with the local administrator account

6. **Recommended:** Set the Active Directory Functional Level to the highest level appropriate for your environment, which is the oldest version of Windows still running ADDS. Note that if you leave the old server running ADDS until a later date, the Active Directory Functional Level must remain at the level of the old server.

   For more details on the established procedures for this step, refer to the Microsoft documentation.

   IMPORTANT
   Never perform P2V conversion on a Windows server that is running ADDS. If you need to migrate a server that is running ADDS, perform the ADDS migration procedure noted above, then demote the old ADDS server and uninstall ADDS before performing a P2V conversion of other applications and data on the old server. It is extremely vital that you plan ahead for ADDS migration. For more details, refer to the Microsoft documentation.

Migrating file storage data (P2P or P2V migration)

In many cases, file migration provides a "clean" migration of file storage and an opportunity to archive very old files that are no longer used. When migrating file storage data, both manual and automated methods are available. The Microsoft Storage Migration Service can be used to aid in migration of files on Windows Server 2003 and later, as well as some Linux file storage running on Samba. For more details on the established procedures for migrating file storage data, refer to the Microsoft article.

Migrating applications and databases (P2P or P2V migration)

The steps for migrating applications and/or databases to a new physical server or OS are highly dependent on application compatibility and vendor requirements. HPE recommends that you work with your application or database vendor for a successful migration.

Converting applications and databases (P2V conversion)

Using the P2V conversion method enables you to continue running an application or database on the older OS. This is particularly useful when the application is not supported on newer OS or hardware. This method enables you to run the application on a new server running Windows Server 2019 right away while giving you more time to evaluate a migration plan for your unsupported application. This method can also help protect against failure of older hardware during an "upgrade in place."

IMPORTANT
Never perform P2V conversion on a Windows server that is running ADDS. If you need to migrate a server that is running ADDS, perform the ADDS migration procedure noted above, then demote the old ADDS server and uninstall ADDS before performing a P2V conversion of other applications and data on the old server. It is extremely vital that you plan ahead for ADDS migration. For more details, refer to the Microsoft documentation.

1. Prepare a new Windows Server 2019 Hyper-V virtual machine (VM).
   a. If not already completed, install Windows Server 2019 on new server and add the Hyper-V role.
   b. Optional: create a shared folder to serve as a temporary repository for the VHD/VHDX files that will be created by the conversion utility.
   c. In the Hyper-V manager, configure the storage location for VHD/VHDX disks.
   d. In the Hyper-V manager, create a VM that will replace the old server. When creating the VM, select "Attach a virtual hard disk later." Do not configure disks for this VM—they will be added later in this procedure.
2. Prepare the old server to be converted to a virtual machine.
   a. Optional: map a network drive to the temporary VHD/VHDX repository on the Windows Server 2019 server.
   b. Recommended: quiesce any transactional services (such as databases or logging services) prior to running the conversion utility. Consider safely shutting down these services because they could potentially create a transactional-consistency issue. These services will start up according to their default settings when the server boots up in the VM.

3. Convert disks to VHDXs.
   a. Download, install, and run the Microsoft Sysinternals Disk2vhd conversion utility on the machine to be converted to VHDX.
   b. In the utility, set the "VHD File name:" to the path for storing the virtual disk files that will be created. Best practice is to choose a storage location that is not on the same physical disk being converted. The fastest method would be to select a different physical disk on the same system. Or, use the optional mapped network drive created on the new Windows Server 2019 server.
   c. Select VHD or VHDX virtual disk type. Choose VHDX unless your application does not support VHDX; check your app's requirements to be sure you are selecting the correct format.
   d. Decide whether you will use Volume Snapshot Service (VSS). Choose VSS unless your application does not support VSS. Check your app's requirements to determine if VSS is supported.
   e. Select the physical disk(s) to be converted. Also select the System Reserved disk if the disk to be virtualized is the boot disk.
   f. Click "Create" to start the conversion.
4. Add converted VHD(X) disks to the new VM.
   a. Move the newly created virtual disks to the folder defined in the Hyper-V settings as the home folder for the new VM, if necessary.
   b. Open the Hyper-V manager, right-click the VM that will host the new disks, and select "Settings."
   c. Select "IDE Controller" in the navigation pane and then "Hard Drive" in the settings pane, then click "Add."
   d. Browse to the VHD(X) disk file and click "Apply," then "OK."
   e. Repeat these steps for additional drives as needed.
5. Shut down the old machine.

IMPORTANT
Shut down and disconnect the old machine from the network to prevent a Domain Account conflict.

6. Boot the new VM.
   a. Verify data and services are present and functioning correctly.
   b. Verify the new VM is running satisfactorily and the application data is correct.
7. Decommission the old server.

IMPORTANT
Do not run the old server on the network once the converted VM is started, unless you are rolling back to the old server, in which case ensure that the new VM is not running before starting the old server.

LEARN MORE AT

hpe.com/info/smb

Our solution partner

Microsoft

Make the right purchase decision.
Contact our presales specialists.

Chat Email Call

Get updates

a00070770ENW, April 2020, Rev. 9

Hewlett Packard
Enterprise