**Dr.SNS RAJALAKSHIMI COLLEGE OF ARTS AND SCIENCE**



**VIRTUALIZATION TECHNOLOGY FUNDAMENTALS**

**UNIT-V**

**CHAPTER- 5**

###### **5.1. To copy text from your local computer to a VM using the VM clipboard**

1. Highlight the text on your local computer. Right-click and select **Copy** or press Ctrl+C to copy the text. This places the text on your local clipboard.
2. In the VM browser window, click clipboard to open the **VM Clipboard** view.
3. Right-click and select **Paste** or press Ctrl+V (⌘+V if you’re using macOS) to paste the text into the **VM Clipboard**. A **Success** message displays in the **VM Clipboard** window.
4. In the VM, click where you want to paste the text.
5. Right-click and select **Paste** or press Ctrl+V (⌘+V if you’re using macOS).

Vim doesn’t use the system clipboard—to paste text into vim, press Ctrl+Shift+V (⌘+Shift+V).

**5.2 Cloning a Virtual Machine**

The cloning process in VMware is a process in which you create an exact copy of your original virtual machine (VM). A VMware clone has the same hardware, software, and other configurations as the original VM.

Cloning is useful when deploying several virtual machines with the same resource allocation and configurations. The cloning process saves you a lot of time in situations that require new, similar machines fast.

In this article, we will explain how to use the VMware cloning VM function.

**Benefits of Cloning a Virtual Machine**

The speed and simplicity of the VMware cloning VM process are its biggest advantage. The process of new VM creation can be quite long sometimes because of the OS installation. With cloning, you can quickly deploy multiple virtual machines with the same setup.

Cloning is handy when you’ve just started a new quality assurance (QA) team, and they all need to run tests in the same environment. They can all get their environment in just a few clicks.

## 5.2.1. Drawbacks of Cloning a Virtual Machine

The only real drawback is that eventually, you may run out of resources. It is easy to create new

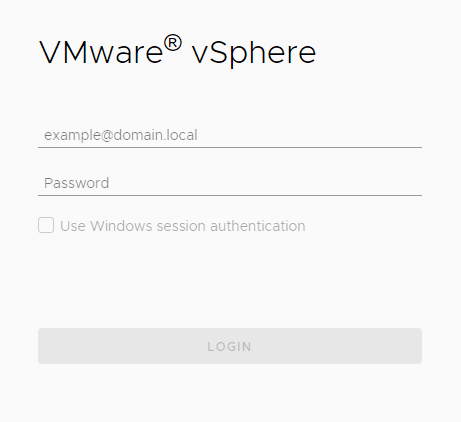
Clones, and you may run out of resources faster than you realize.

When creating many VM clones, you will overload your RAM and CPU at some point. It happens because you will have many virtual CPUs and virtual memory allocated to your virtual machines, not to mention storage space. So just keep in mind how many resources you have at your disposal when you are cloning virtual machines.

**5.2.2 How to Clone a Virtual Machine**

**Step 1**

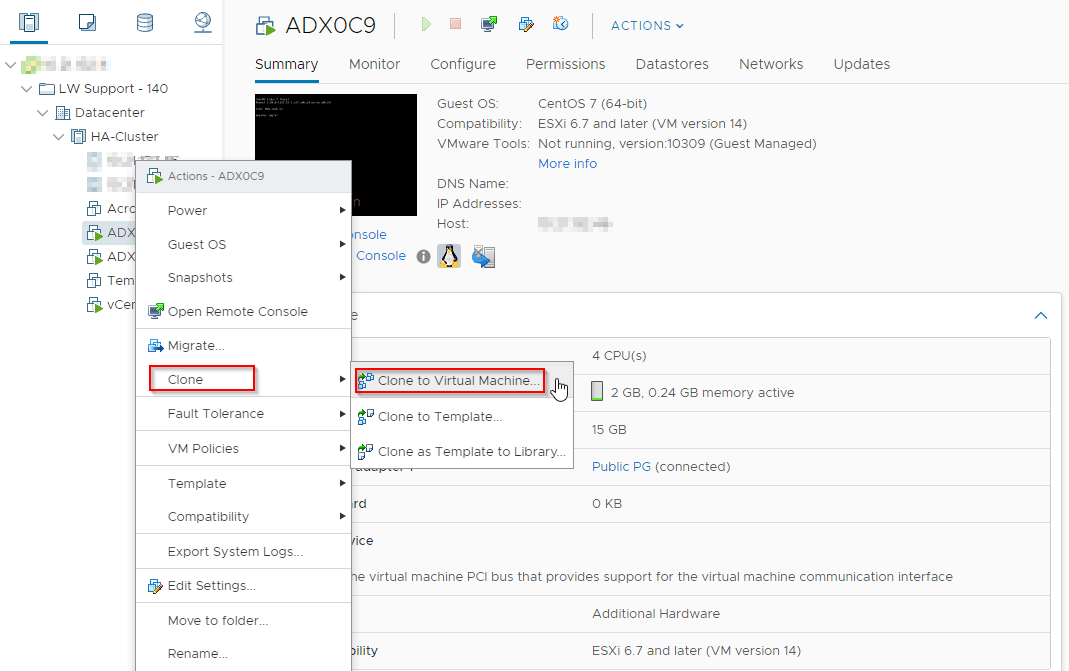
Log in to your vSphere client. Each managed VMware cloud hosting here at Liquid Web comes with vSphere. Enter the IP address of the host on which has your vSphere installation. The login page will load. Enter your credentials and click **login**.



**Figure 5.1**

### Step 2

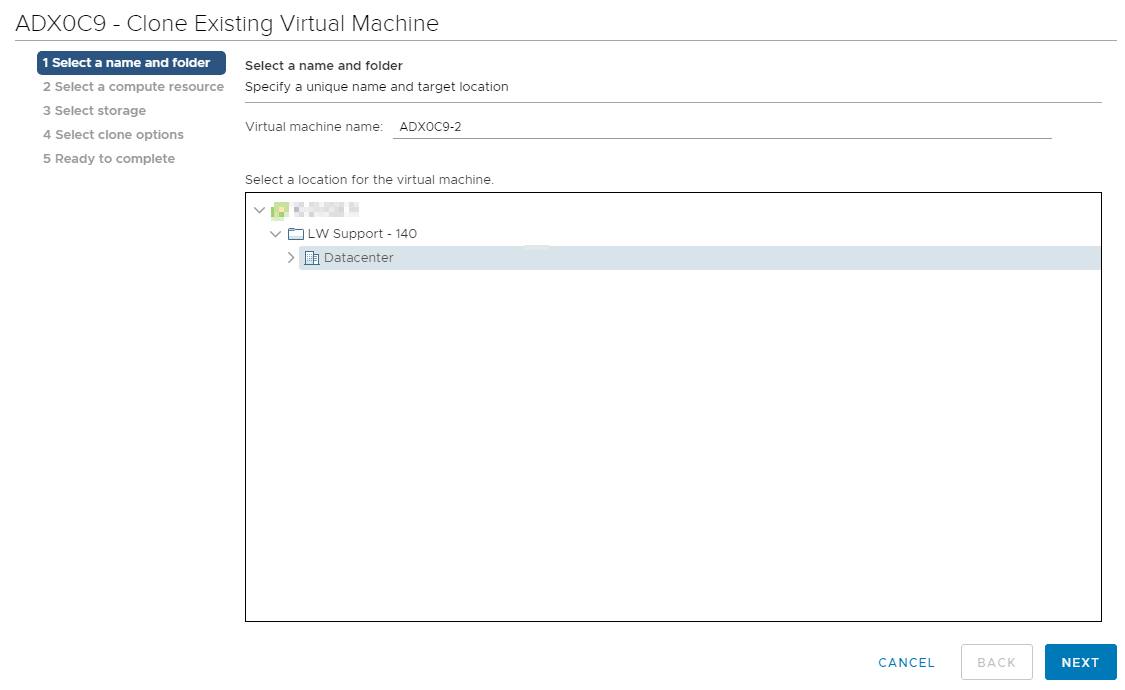
Once logged in, navigate to your virtual machines. Choose a VM you wish to clone and right-click on it with your mouse. A menu will appear, and you can hover your mouse pointer over the Clone option. Finally, click on **Clone to Virtual Machine**.



**Figure 5.2**

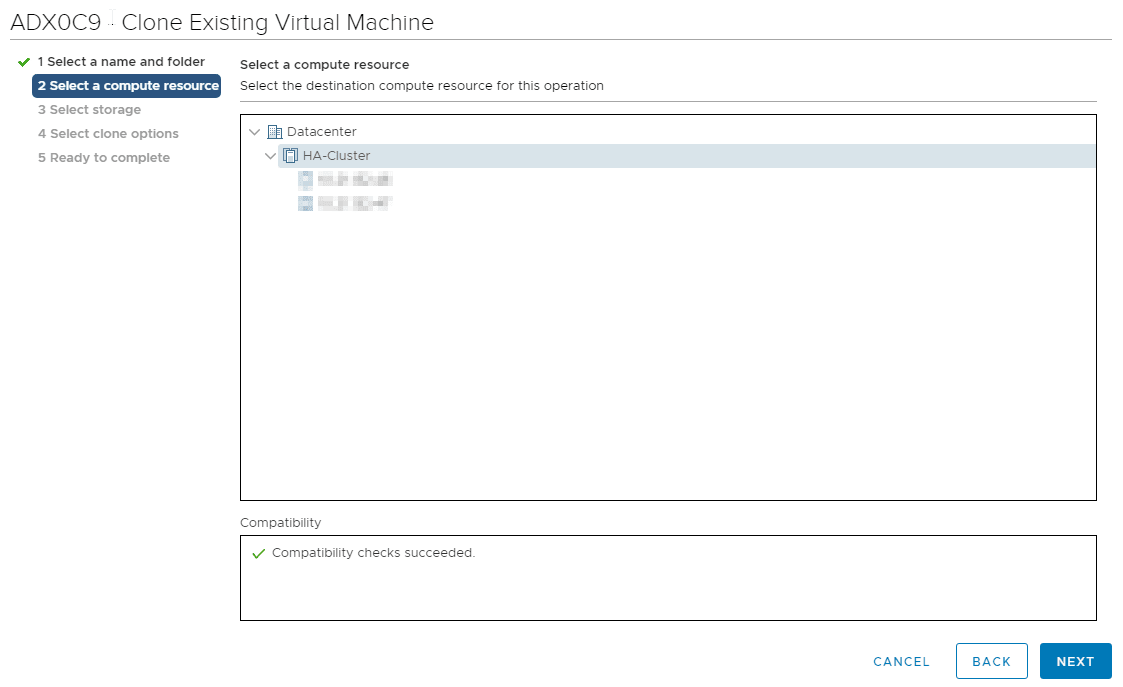
### Step 3

Once you go through the process in step 2, a new window will appear. You need to name your VM clone and choose a location for it. Type in the name and select the location of your preference. Once done, click on the **Next** button in the lower right corner.



**Figure 5.3**

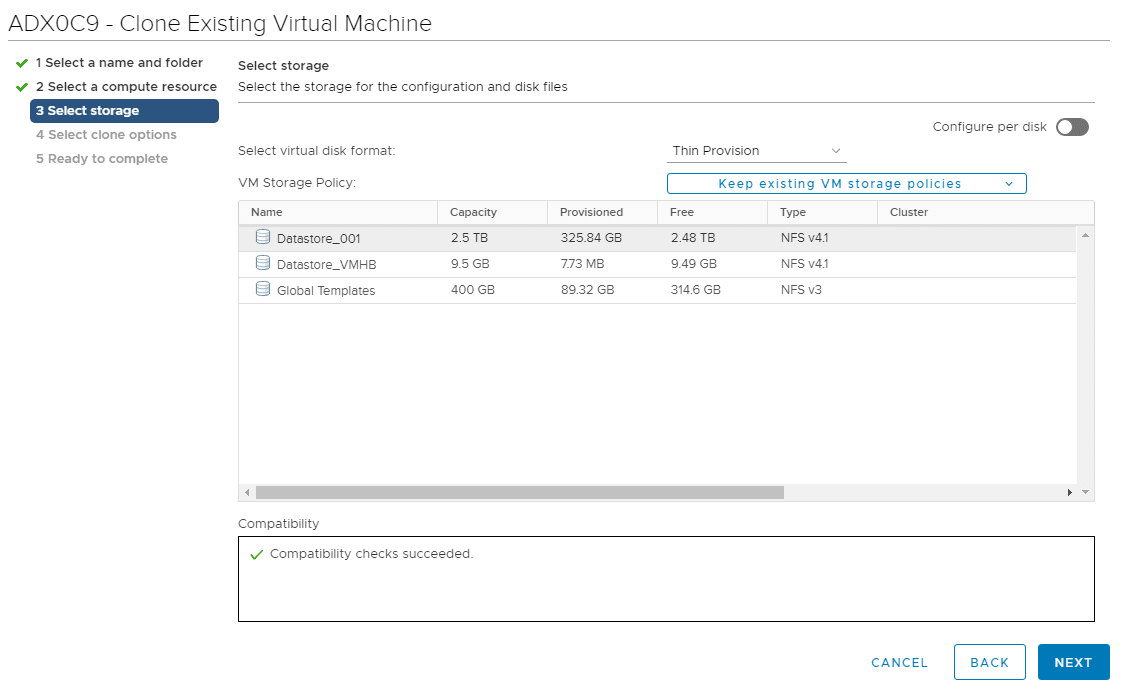
### Step 4:Select the destination compute resource for our VMware cloning VM operation and the host for the clone. Once completed, click the **Next**button again.



**Figure 5.4**

### Step 5

Now we are going to select the storage for our VMware clone machine. Choose the disk on which you want to keep configuration files for this VM and click **Next**when you are ready.

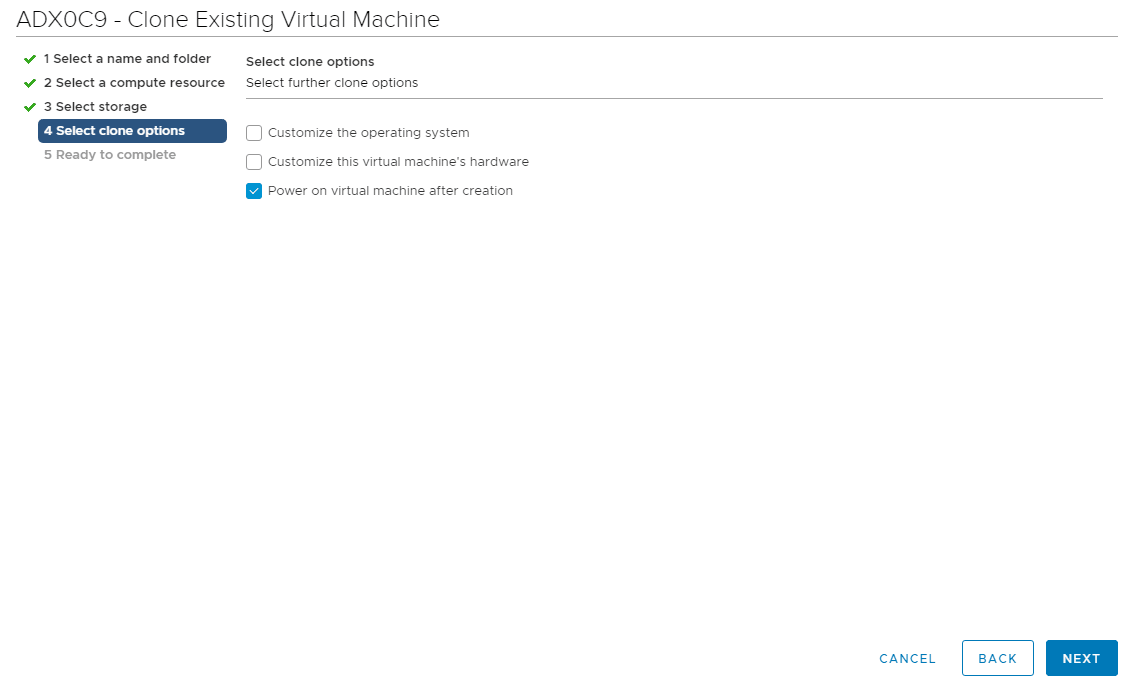


**Figure 5.5**

### Step 6

You will have a couple of options from which to choose. However, it is worth noting that if you want the exact copy of the original VM, you only need to select **Power on virtual machines after creation.** It will boot up your freshly cloned VM.

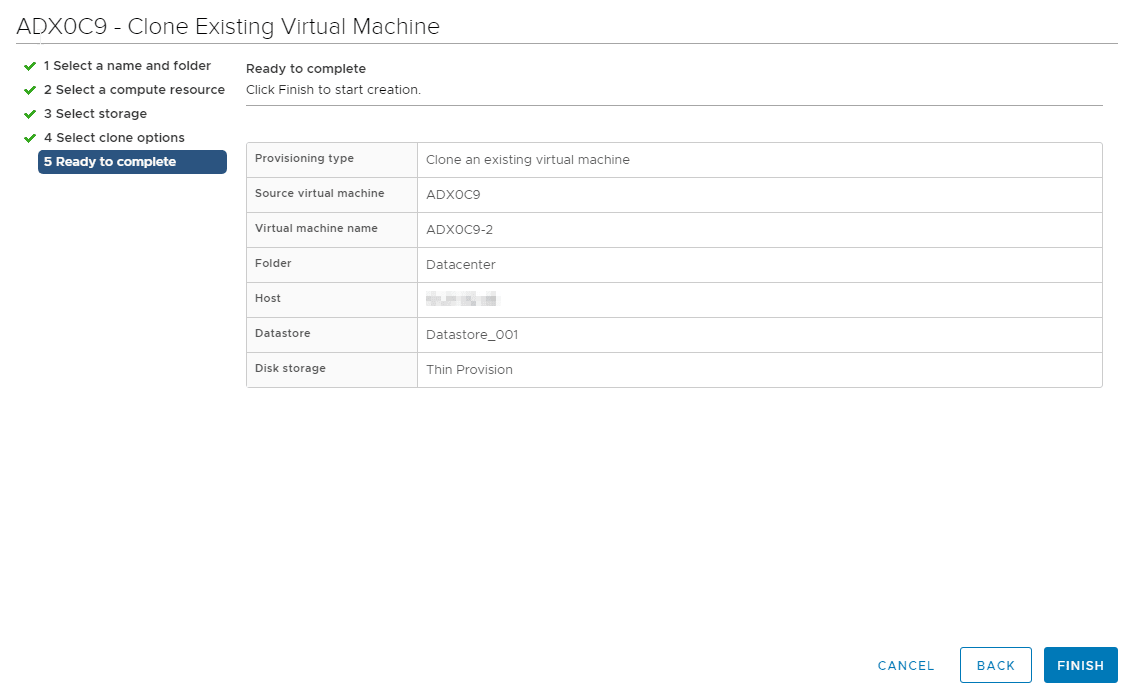
Click **Next**when ready.



**Figure 5.6**

### Step 7

Here you see an overview of the previously selected options. Go through them once more, and if everything is correct, click the **Finish** button. If you want to change something, you can click the **Back** button to get back to one of the previous steps and make the necessary changes.



**Figure 5.6**

Congratulations! You successfully completed the VMware cloning VM process.

**5.3. Working with template:**

You must create a virtual machine template before you can create an automated pool that contains full virtual machines.

A virtual machine template is a main copy of a virtual machine that can be used to create and provision new virtual machines. Typically, a template includes an installed guest operating system and a set of applications.

You create virtual machine templates in vSphere Client. You can create a virtual machine template from a previously configured virtual machine, or you can convert a previously configured virtual machine to a virtual machine template.

See the vSphere Basic System Administration guide for information on using vSphere Client to create virtual machine templates. See Automated Pools That Contain Full Virtual Machines for information on creating automated pools.

In vSphere 7.0, you can manage VM templates in an efficient and flexible manner. You can edit the contents of the VM templates by checking them out, making the necessary changes, and checking them in.

You can track history of changes over time by using the vertical timeline view. The vertical timeline view provides you with detailed information about the different VM template versions, the updates that privileged users have made, and when the last change was made. By using the vertical timeline, you can revert VM templates back to their previous state or delete the previous version of a VM template.

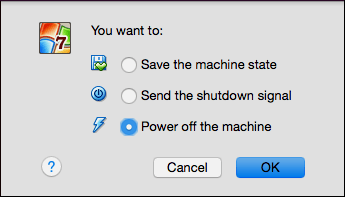
In addition, you can deploy a virtual machine from the latest version of the VM template without any disruptions while it is checked out for update. You can update the virtual machine and check it back in into the same VM template.

* Templates in Content Libraries  
  Templates are primary copies of virtual machines that you can use to deploy virtual machines that are customized and ready for use. Templates promote consistency throughout your vSphere environment. You can use the content library to store and manage templates of virtual machines and vApps. You can use VM templates and vApp templates to deploy virtual machines and vApps to a destination object, such as a host or a cluster
* **Check Out a Virtual Machine from a Template**  
  In the vSphere Client, you can edit the VM templates and monitor the changes that have been made by other privileged users. You can perform the checkout operation to update a virtual machine from the VM template. During this process, the VM template is not available for checkout from other users, but they can deploy a virtual machine from the VM template without any disruptions.
* **Check In a Virtual Machine to a Template**  
  After you check out a virtual machine from a template and update the virtual machine, you must check the virtual machine back into the VM template. When you check in the virtual machine to a template, you create a new version of the VM template containing the updated state of the virtual machine.
* Discard a Checked Out Virtual Machine  
  If you check out a VM template and make no updates to the virtual machine or perform an update that you do not want to keep, you can discard the checked out virtual machine. Each time you check in the virtual machine back to the template, you create a new version of the VM template. You can discard the checked out virtual machine to avoid creating new versions or to prevent other users from using a faulty version.
* Revert to a Previous Version of a Template:  
  If the latest VM template contains changes that you no longer want to keep or you made a mistake during your last check-in, you can revert the VM template to the previous version.
* Delete a previous version of a VM template if you no longer want to allow the use of the template. Deleting a VM template removes the template and its content from the inventory.

**5.4. Saving a Virtual Machine State**

When you click on the ***Close*** button of your virtual machine window, at the top right of the window, just like you would close any other window on your system, Oracle VM VirtualBox asks you whether you want to save or power off the VM. As a shortcut, you can also press ***Host key + Q***.

**Figure 5.7  Save a Virtual Machine**



The difference between the three options is crucial. They mean the following:

* ***Save the machine state:*** With this option, Oracle VM VirtualBox freezes the virtual machine by completely saving its state to your local disk.

When you start the VM again later, you will find that the VM continues exactly where it was left off. All your programs will still be open, and your computer resumes operation. Saving the state of a virtual machine is thus in some ways similar to suspending a laptop computer by closing its lid.

* ***Send the shutdown signal.*** This will send an ACPI shutdown signal to the virtual machine, which has the same effect as if you had pressed the power button on a real computer. This should trigger a proper shutdown mechanism from within the VM.
* ***Power off the machine:*** With this option, Oracle VM VirtualBox also stops running the virtual machine, but without saving its state.

**Warning**

This is equivalent to pulling the power plug on a real computer without shutting it down properly. If you start the machine again after powering it off, your OS will have to reboot completely and may begin a lengthy check of its virtual system disks. As a result, this should not normally be done, since it can potentially cause data loss or an inconsistent state of the guest system on disk.

As an exception, if your virtual machine has any snapshots, you can use this option to quickly ***restore the current snapshot*** of the virtual machine. In that case, powering off the machine will not disrupt its state, but any changes made since that snapshot was taken will be lost.

The ***Discard*** button in the VirtualBox Manager window discards a virtual machine's saved state. This has the same effect as powering it off, and the same warnings apply.

**5.5. Creating a Snapshot**

Create a Snapshot to learn about those fine details of what is happening on an individual page. By default, a Snapshot tracks every visit and visitors' clicks and scrolls on your page. The click Heatmap report, Scrollmap report, and our five other reports, all come from creating snapshots.

## 5.5.1. Creating a Standard Snapshot - Step by Step

Here is a recommended process to help you create a single snapshot.

**Step 1**

Click on + Create New Snapshot

**Step 2**

Click on Sclick on Snapshot for a single page.

**Step 3**

Enter the URL from your webpage that you want to track. The Snapshot Name will fill in automatically.    
**Note:** If the Snapshot Name does not fill in, hit the Next button.  An error message will appear under the URL field to provide more information.

Step 4

Option 1- Device Tracking is set by default and will create 3 separate Snapshots for each device type: Desktop, Tablet, and Mobile visitors.

Option 2 - Tick the Custom Tracking box if your mobile visitor volume is less than 25% of your overall visitor traffic to your site or a given page.

Step 5

By default, the Start and End Duration settings are set for you. A snapshot will start tracking immediately. A snapshot will stop tracking after 60 days **OR** when it has tracked 25,000 visits.

**Step 6**

At this point, you can click on the **Review**button in the bottom right-hand corner. By default, we track every visit to the page and do not block pop-ups.

**Step 7**

The thumbnail images will start to load. You can wait until you see them or click on the **Create # Snapshots** button in the bottom right-hand corner.

**Step 8**

Congratulations!  You have created your snapshots. Now click on **Return to Dashboard**.

**5.6 Merging Snapshots**

There are times when you need to install OS updates or security patches on one of your guest virtual machines (VMs). However, the update process can sometimes go wrong, resulting in a system failure, loss of configuration data, or the uninstallation of certain programs. Microsoft Hyper-V has provided the opportunity to create Hyper-V snapshots, which allow you to save the VM state at a particular point in time and roll back the system to its previous state if a system error occurs.

In this blog post, we will describe how to merge Hyper-V snapshots using Hyper-V Manager or PowerShell and how they can be used. However, to learn how to manage Hyper-V snapshots, you first need to understand the technology behind them.

## **5.6.1 How to Merge Hyper-V Snapshots**

In one of our previous blog posts, we have covered how to manage Hyper-V snapshots (create, apply, rename, enable/disable, etc.). However, today’s blog post serves as a guide to manually merging Hyper-V snapshots.

In order to merge Hyper-V snapshots, you need to use either Hyper-V Manager or PowerShell. Both of these approaches will be described below.

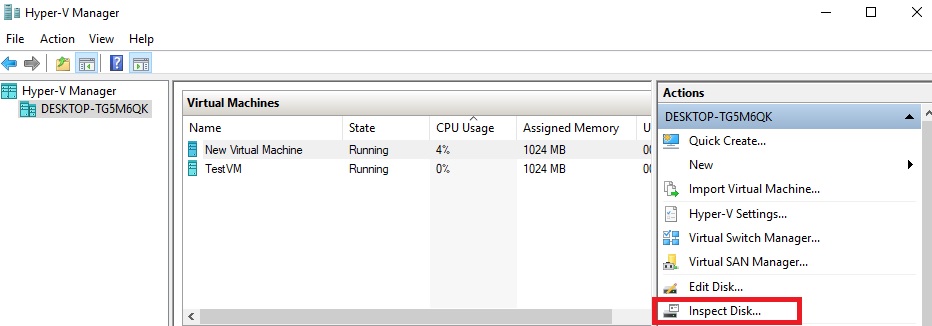
### **5.7. Using Hyper-V Manager**

Before we start to describe how to merge Hyper-V snapshots, we should first determine which snapshots will be merged. Hyper-V snapshots should be merged in a specific order: from child to parent. Therefore, it is important to establish the structure of the checkpoint tree by establishing the order of their creation: from the newest to the oldest ones.

As mentioned above, each snapshot has a parent-child relationship with another snapshot that was created before it. All of them combined can be represented in the form of a chain. For example, 3 snapshots were created for 1 virtual hard disk. The main virtual disk on which the VM is running acts as a parent of the first checkpoint, this checkpoint acts as a parent of the second checkpoint, and the second checkpoint acts as a parent of the third checkpoint.

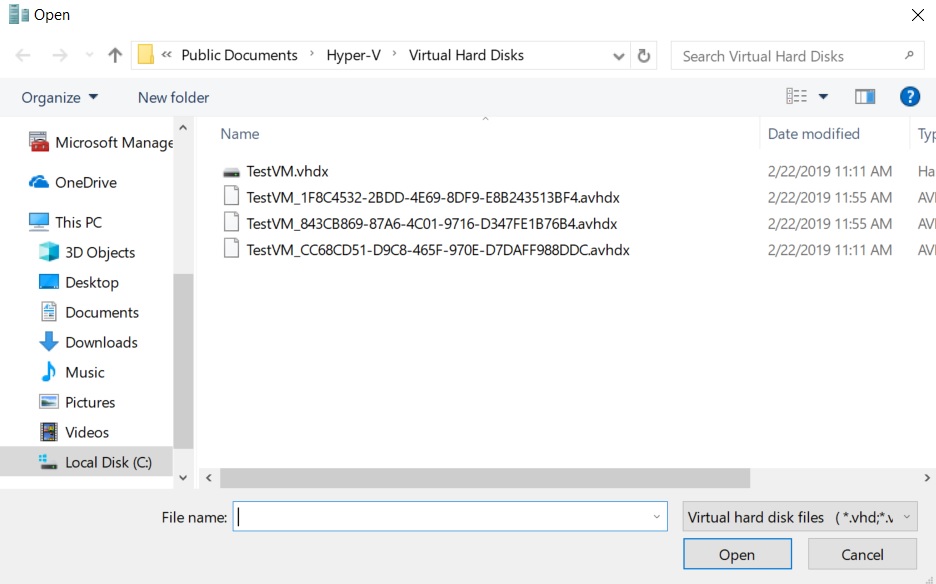
To establish the checkpoint structure, take the following steps:

1. Open Hyper-V Manager.
2. In the center pane, select the VM whose snapshots you want to be merged.
3. In the Actions section on the right, click **Inspect Disk.**



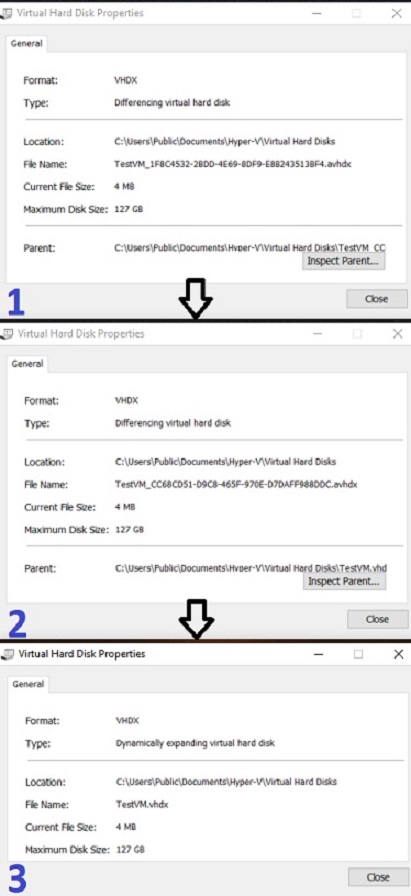
**Figure 5.7**

1. Select the .avhd(x) file and click **OK**.



**Figure 5.8**

1. Next, you should see a general overview of the virtual hard disk properties, including its name, location, and the parent’s name. Determine the parent of the selected .avhd(x) file.
2. Repeat steps 3-5 for each .avhd(x) file and identify their order for merging.



**Figure 5.9**

1. After that, you can start the process of merging Hyper-V snapshots. Note that your VM must be turned off to avoid any issues during the merging operation.

To merge Hyper-V snapshots, do the following:

1. Open Hyper-V Manager.
2. Select the required VM.
3. Click **Edit Disk.**The Edit Virtual Hard Disk Wizard will open**.** Click **Next.**
4. Click **Browse** to select the latest .avhdx file. Click **Next.**

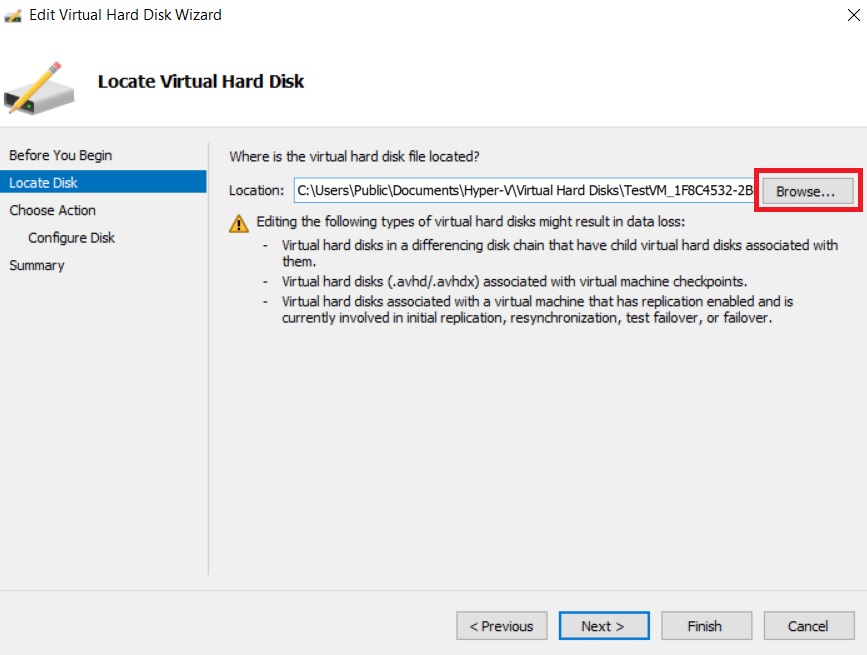
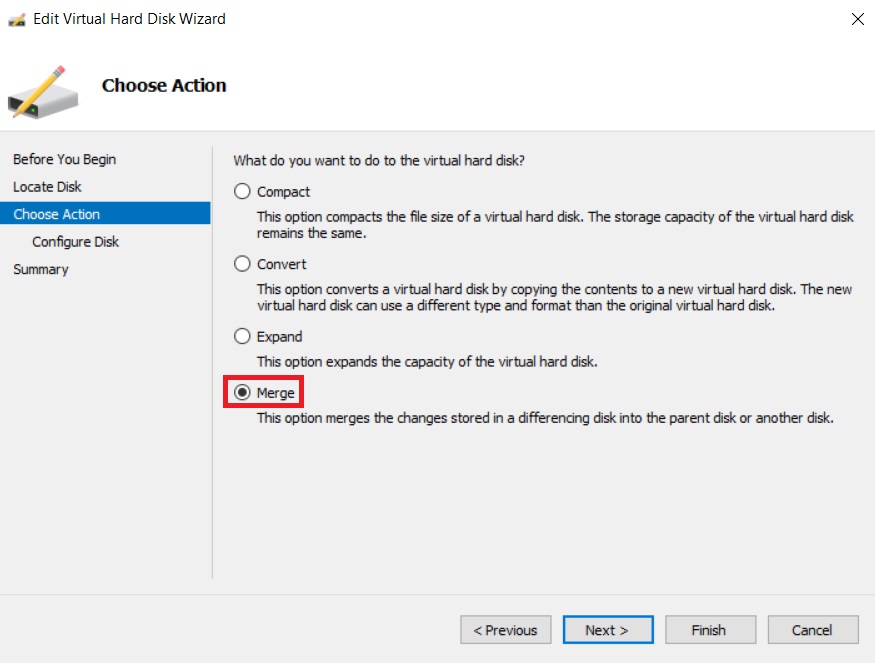
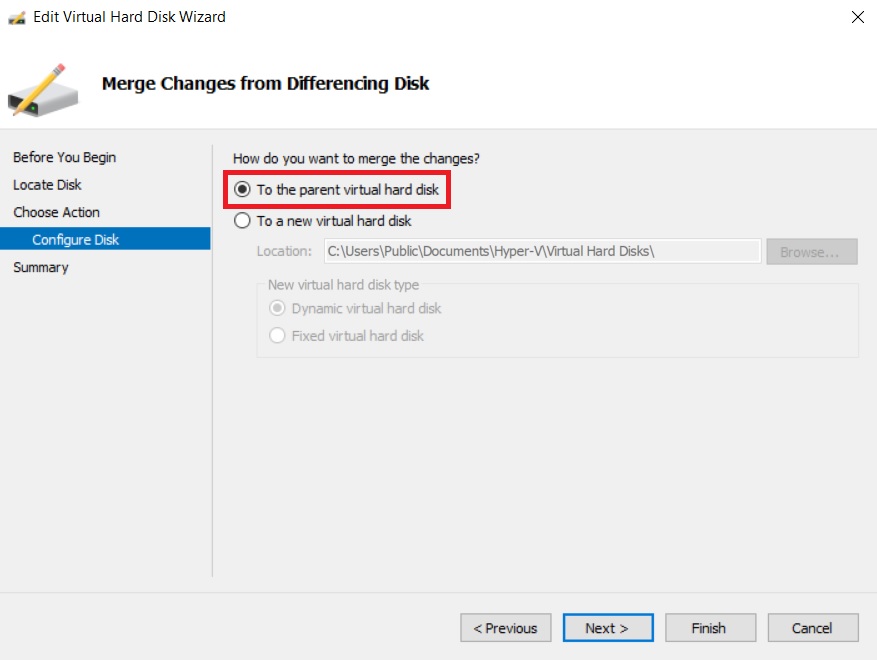


Figure 5.10

1. Select **Merge**to merge the changes stored in a differencing disk into the parent or another disk. Click **Next.**



1. Select **To the parent virtual hard disk** and click **Finish.**



**Figure 5.11**

1. To fully complete the process of merging Hyper-V snapshots, repeat steps 1-5 for each .avhd(x) file, until all of the changes have merged into the original parent disk.
2. The final step is to reboot the VM to adopt the implemented changes.

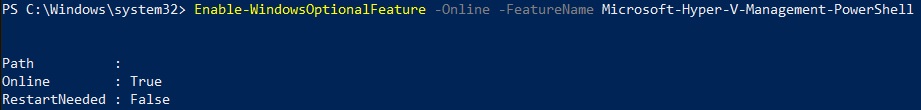
### **Using PowerShell**

Before you can start to merge Hyper-V snapshots, ensure that your computer has the Merge-VHD cmdlet enabled. If not, the following error will appear on the screen:  
The term 'Merge-VHD' is not recognized as the name of a cmdlet, function, script file, or operable program.  
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

To remove this issue, open PowerShell as an Administrator and run the following command:

Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V-Management-PowerShell

If everything is correct, you should see the following:



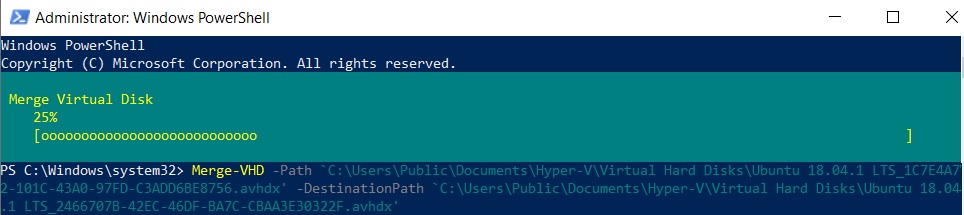
**Figure 5.12**

Now, you are ready to run the Merge-VHD cmdlet. Note that this operation is conducted offline.

To merge Hyper-V snapshots, run this cmdlet:

Merge-VHD Path = '' DestinationPath = ''

In this case, the data from several child disks, beginning from the newest one, can be merged into the oldest parent disk. On the screen, you will see the following:



**Figure 5.13**

After the operation is complete, shut down the guest VM and reboot the system. Unlike Hyper-V Manager, which requires you to merge each layer of the disk chain separately, PowerShell allows you to perform such a complex operation with a single command.

**5.8. Understanding Availability**

When learning something new there are a lot of phrases, terms and theory to learn and when learning Azure the same is true. One of the things you should be aware of within Azure is the difference and use cases of [Availability Zones and Availability Sets](https://docs.microsoft.com/azure/availability-zones/az-overview?WT.mc_id=modinfra-11089-salean).

When we are architecting workloads we see availability is making sure the resources or workloads are there when you need them.

**Virtual Machines in Azure**

Within Azure when you spin up a virtual machine it gives you an availability of either 95%, 99.5% or 99.9% depending on how you configure your disks with that virtual machine.  When you think about it in monthly terms a 95% Service Level Agreement (SLA) allows for around one and half days downtime. For a lot of workload cases and organisations these availability numbers will be more than adequate.  If you need more then that’s where Availability Zone and Sets can help.

**Availability Sets**

An Availability Set  lets you spread your virtual machines across physical hardware in different fault domains and update domains, in one location. This reduces the risk of a hardware failure or update failure impacting the availability of all of your VMs at the same time. Fault domains share common storage as well as a power source and a network switch. An updated domain contains physical hardware that can be rebooted at the same time. Without visibility down at that hardware level, you can benefit from deploying your VMs into an Availability Set, to spread them across fault domains and update domains.

When you create your virtual machine you can specify the Availability Set, you can’t change it or move it in or out of an Availability Set after creation.  If you wanted to make changes you would need to start again and recreate the virtual machine.   And Availability Sets only apply to virtual machines, they can’t be used for any other type of resource within Azure.

Using an Availability Set takes the acceptable downtime to around 22 minutes a month, which is a vast improvement over a single virtual machine deployment. Note: While an availability set will decrease the risk of all of your VMs being unavailable at the same time, you will still need to architect your application or solution to fail over to non-impacted VMs for redundancy/business continuity.

**Availability Zone**

The next level of availability for your virtual machines within Azure is Availability Zones.  With Availability Zones utilised your acceptable downtime a month moves to less than 5 minutes as you’ve got a 99.99% SLA.

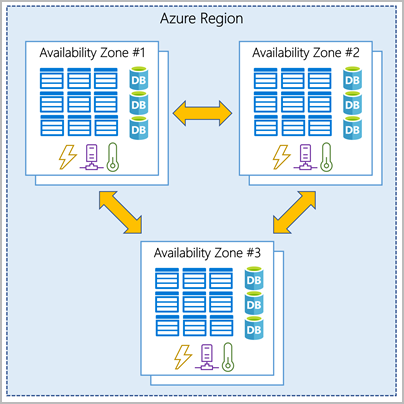


Figure 5.13 Availability Zone

With Availability Zones you are starting to use zone aware services. Your workload will be spread out across the different zones that make up an Azure region.  An Azure region is made up of multiple datacentres and each zone is made up of one or more datacentres.  Each datacentre is equipped with independent power, cooling and networking.

**When do use them?**

There can be a few deciding factors around Availability Zones versus Availability Sets, you should be thinking about these questions when designing your workloads in Azure:

 Are Availability Zones available in the region I want to use? You can find out which regions support them and which services are support [here](https://docs.microsoft.com/azure/availability-zones/az-region?WT.mc_id=modinfra-11089-salean).

* What SLA or availability does this workload really need? Make sure you really understand the business needs versus the wants.  Each configuration will offer you the following:
  + 99.9% = Single VM (with Premium SSD or Ultra Disk)
  + 99.95% = Availability Set
  + 99.99% = Availability Zones

**5.9. Protecting a Virtual Machine**

* Install only what you need on the host machine. Keep your OS and applications current for both virtual and host machines.
* Isolate each virtual machine you have by installing a firewall. Only allow approved protocols to be deployed.
* Ensure that antivirus programs are installed on the virtual machines and kept current with updates. Virtual machines, like physical machines are at risk for viruses and worms.
* Utilize strong encryption between the host and virtual machines.
* Avoid internet surfing from the host computer. Spyware and malware could easily infiltrate through the the host computer and spread to the virtual machines.
* Prevent unauthorized access by securing accounts on the host machine.
* Only use what you need. If you're not utilizing a virtual machine, shut it down.
* If a virtual machine does not need to connect with each other, isolate it. Use a separate network card on a different network range.
* Monitor the event log and security events on both the host machine and on the virtual machine. These logs need to be stored in your log vault for security and for auditing purposes at a later date.
* Ensure that any hardware you use is designed for VM usage.
* Strictly manage remote access to virtual machines and especially to the host machine, this will make exposure less likely.
* Remember, the host machine represents a single point of failure. Technologies like replication and continuity help with reducing this risk.
* Avoid sharing IP addresses. Again this is typical of sharing a resource and will attract problems and vulnerabilities.
* Using these tips will help you make the most of your physical and virtual environments so if anything interrupts your business, you are prepared.

**5.10. Protecting Multiple Virtual Machines**

**5.10.1 Protecting Datacenters.**

Modern companies use computers in almost all aspects of doing business—communication, information storage, accounting, and day-to-day business functions. This includes data centers and virtual machines.

A **data center** is a centralized physical facility where corporate computers, networks, storage, and other IT equipment that support business operations live. The computers in a data center contain or facilitate business-critical applications, services, and data. Windows Server Datacenter is often seen as the ultimate powerhouse for high-level computing, with its wide array of features and functionality that make handling high levels easier.But are data centers the same as virtual machines? What is their difference? How do they work?This guide looks at the difference between data centers and virtual machines and how they work.



Figure 5.14

The purpose of the data center is to host business-critical applications for the enterprise. Each role in the data center is designed and configured to ensure the highest quality user experience possible. This document describes the critical role that security play in the virtualized IT data center architecture.

Security

Security is a vital component of any network architecture and the virtualized IT data center is no exception. There are various areas within the data center where security is essential. At the perimeter, security is focused on securing the edge of the data center from external threats and with providing a secure gateway to the Internet. Remote access is another area where security is vital in the data center. Operators often require remote access to the data center to perform maintenance or new service activations. This remote access must be secured and monitored to ensure that only authorized users are permitted access. Robust authentication, authorization and accounting (AAA) mechanisms should be in place to ensure that only authorized operators are allowed access. Given that the data center is a cost and revenue center that can house the critical data and applications of many different enterprises, multi-factor authentication is an absolute necessity to properly secure remote access.

Software application security in the virtualized IT data center is security that is provided between VMs. A great deal of inter-VM communication occurs in the data center and controlling this interactivity is a crucial security concern. If a server is supposed to access a database residing on another server, or on a storage array, a virtual security appliance should be configured to limit the communication between those resources to allow only those protocols that are necessary for operation. Limiting the communication between resources prevents security breaches in the data center and might be a requirement depending on the regulatory requirements of the hosted applications (HIPPA, for instance, can dictate security safeguards that must exist between patient and business data). Security in the virtual network, or between VMs, differs from security that can be implemented on a physical network. In a physical network, a hardware firewall can connect to different subnets, security zones, or servers and provide security between those devices (see [Figure 5.1](https://www.juniper.net/documentation/en_US/release-independent/solutions/topics/concept/security-virtual-it-dc-overview.html#fig-physical-vs-virtual-security)5). In the virtual network, the physical firewall does not have the ability to see traffic between the VMs. In these cases, a virtual hypervisor security appliance should be installed to enable security between VMs.

[Figure 5.1](https://www.juniper.net/documentation/en_US/release-independent/solutions/topics/concept/security-virtual-it-dc-overview.html#fig-physical-vs-virtual-security)5  illustrates physical security compared to virtual network security.

Physical Security
Compared to Virtual Network Security

Figure 5.15

**5.11 Application Security**

When securing VMs, you need a comprehensive virtualization security solution that implements hypervisor security with full introspection; includes a high-performance, hypervisor-based stateful firewall; uses an integrated intrusion detection system (IDS); provides virtualization-specific antivirus protection; and offers unrivaled scalability for managing multitenant cloud data center security. The Juniper Networks Firefly Host (formerly vGW) offers all these features and enables the operator to monitor software, patches, and files installed on a VM from a central location. Firefly Host is designed to be centrally managed from a single-pane view, giving administrators a comprehensive view of virtual network security and VM inventory.

Table 5.2 shows the relative merits of three application security design options: vSRX, SRX, and Firefly Host. Because other choices lack intrusion detection and prevention, quarantine capabilities, and mission-critical line-rate performance and scalability, Firefly Host is the preferred choice for this solution. Additionally, Firefly Host is integrated into all VMs and provides every endpoint with its own virtual firewall.

Table 5.2  shows the application security options.

Table 5.1: Application Security Options

| **Requirement** | **vSRX** | **SRX** | **Firefly Host** |
| --- | --- | --- | --- |
| **Stateful security policies** | **Yes** | **Yes** | **Yes** |
| **Centralized management** | **Yes** | **Yes** | **Yes** |
| Intrusion detection and prevention | Yes | Yes | Yes |
| Quarantine | No | No | Yes |
| 10G line-rate performance at scale | No | No | Yes |

**Table 5.1**

To provide application security in the virtualized IT data center, this solution uses the Juniper Networks Firefly Host to provide VM-to-VM application security. Firefly Host integrates with VMware vCenter for comprehensive VM security and management.

Figure 5.16 shows the design for application security.

Figure 5.16 Application Security Design

Application Security
Design

**Figure 5.16**

In Figure 5.16 , the following sequence occurs for VM-to-VM traffic:

A VM sends traffic to a destination VM.

The Firefly Host appliance inspects the traffic.

The traffic matches the security policy.

The ESXi host transmits the traffic.

The second ESXi host receives the traffic.

Firefly Host inspects the traffic.

The traffic matches the security policy and permits the traffic to continue to the destination.

The destination VM receives the traffic.

**5.11.1 Perimeter Security**

Edge firewalls handle security functions such as Network Address Translation (NAT), intrusion detection and prevention (IDP), security policy enforcement, and virtual private network (VPN) services.

As shown in Figure 5.17, there are four locations where you could provide security services for the physical devices in your data center:

Firewall filters in the QFabric system PODs

Firewall filters in the core switches

Dedicated, stateful firewalls (such as the SRX3600)

Physical firewalls connected to the QFabric system PODs

Physical Security
Design

Figure 5.17 : Physical Security Design

For example, location 3 in Figure 5.17 uses a stateful firewall to protect traffic flows travelling between the edge routers and core switches. Anything below the POD level is protected by the Firefly Host application.

To provide perimeter security in the virtualized IT data center, this solution uses the SRX3600 Services Gateway as an edge firewall. This firewall offers up to 55-Gbps of firewall performance, which can easily support the VM traffic generated by this solution.

5.11.2. Secure Remote Access

The virtualized IT data center solution requires secure remote access into the data center environment. Such access must provide multifactor authentication, granular security controls, and usher scale that give multitenant data centers the ability to provide access to administrators and access to many thousands of users.

The secure remote access application must be accessible through the Internet; capable of providing encryption, Role-Based Access Control (RBAC), and two-factor authentication services; able to access a virtualized environment; and scale to 10,000 users.

Table 5.3  shows a comparison of the MAG Series gateway and the Junos Pulse gateway options. For the virtualized IT data center solution, the Junos Pulse gateway is superior because it offers all the capabilities of the MAG Series gateway as well as being a virtualized application.

Table 5.3 : Data Center Remote Access Options

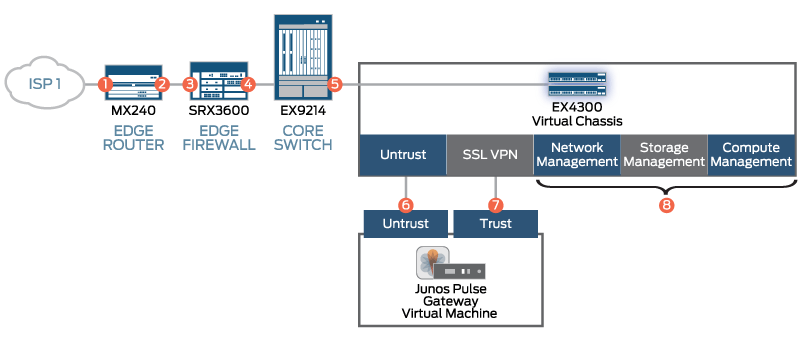
| Requirement | MAG Gateway | Virtual Pulse Gateway |
| --- | --- | --- |
| Internet accessible | Yes | Yes |
| Encryption | Yes | Yes |
| Two-factor authentication | Yes | Yes |
| Scale to 10,000 users | Yes | Yes |
| Virtualized | No | Yes |

Table 5.3

To provide secure remote access to and from the virtualized IT data center, this solution uses the Juniper Networks SA Series SSL VPN Appliances as remote access systems and the Junos Pulse gateway.

Figure 5.18 shows the remote access flow.

Figure 5.18 Remote Access Flow



As shown in [Figure](https://www.juniper.net/documentation/en_US/release-independent/solutions/topics/concept/security-virtual-it-dc-overview.html#fig-remote-access-flow)5.18, the remote access flow in the virtualized IT data center happens as follows:

The user logs in from the Internet.

The user session is routed to the firewall.

Destination NAT is performed on the session.

The authorized user matches the security policy.

The traffic is forwarded to the Junos Pulse gateway.

Traffic arrives on the Untrust interface.

Trusted traffic permits a local address to be assigned to the user.

The user is authenticated and granted access through RBAC.

5.13 .Understanding Applications in a Virtual Machine

## **The multiplicity of Operating Systems**

A Virtual Machine enables the running of operating systems (OS) that would not normally be compatible with your host system (e.g., Windows on a Mac or an Apple overlay on a Linux configuration).  By simulating multiple computer systems from one console users are able to toggle amongst systems and displays from a single workstation. Thus VMs provide the experience of using multiple computers at the same time; ideal for creating complex servers with multisystem needs.   An added advantage of this type of overlay is that users who are comfortable with one OS, perhaps an older non-supported version of Windows, can have their preference available, regardless of the overall company OS, thus aiding them to work efficiently.

## **Reduced Overhead**

Overhead comes in many forms: salaries, benefits, hardware purchases, software licensing, etc. The ability to run multiple OS on a single piece of hardware reduces the need for office machinery as well as its upkeep and operational costs (say a utility bill for electricity to power and cool the machinery).  Fewer physical servers due to running more systems on each one also reduce costs via a reduction in floor space required!

## **Safety Net for Data – Rapid Disaster Recovery and Auto Backups**

Since virtual machines are set up using a hypervisor (a piece of hardware, firmware, or software that creates your virtual machines, allocates resources to them, and then manages them) or similar technology which creates a layer between your physical computer and your virtual machine, the various systems remain entirely separate from each other; this adds an important layer of security to your operations which can help prevent faulty applications or corrupted files from infecting your host machine. For example, if you download a corrupted or infected file on your Virtual Machine, the hypervisor will prevent the file from getting to your host machine.

In addition, since Virtual Machines make regular copies/snapshots of their operations history there is little risk of data loss – making for a highly effective disaster recovery solution as these copies can be revisited as necessary or, in more severe recovery scenarios, moved to another device.  Further, the negligible hardware overhead of your virtual environment poses a lower risk of system failure to your server in the first place.  Finally a Virtual Machine set-up allows you to various applications while you determine what works best for your business needs during development.

## **Scalability**

Since physical space for as well as maintenance costs of additional hardware are not a factor in a Virtual Machine environment, your company and its systems can grow and change more easily. Virtual Machines enable you to add and remove applications with no physical overhead, so that an expanding virtual infrastructure doesn’t require complex budgets for hardware resources. This simulated hardware is a flexible solution to an expanding company server, with multi-application, multi-user needs.

## **Centralization**

The use of virtual machine environments can allow for the consolidation and more efficient management of your IT needs via a single console with commercially available Virtual Machine software helping to monitor all of your systems, applications, and OSs from a single dashboard. Additionally, use of a Virtual Machine performance monitoring tool to collect data and metrics for your network on a regular basis can help to ensure the system is functioning well and there are no impending issues. With proper centralization and monitoring you will be able to track trends (such as which Virtual Machines are consistently reaching resource limits), more effectively approach capacity planning and disk space usage as well as flag any VMs regularly experiencing crashes, delays, or application issues.

**Before we conclude, note needs to be made of a**special virtue of the flexibility of Virtual Machines, one highlighting many of the benefits noted above, which is their usefulness for **Software Development and Testing. T**esting in-development software is enhanced as applications can be installed on the Virtual Machine and then reset to a saved state whenever needed. Also, if you are trying out a new application and aren’t sure how it will perform under certain conditions, you can test it on a virtual machine and then reset it to a particular state if it crashes or you want to try something new. This is a definite advantage as doing this on a physical machine may leave you with unexpected crashes and issues even after you uninstall the test software. The isolation from the host OS of the test software on a [virtual machine](https://en.wikipedia.org/wiki/Virtual_machine) creates a much safer test environment. Plus, you can determine whether an application you are developing works well on all OSs or has bugs in some operating systems but not others.

**5.12. Deploying Applications in a Virtual Environment**

When you use Configuration Manager to manage virtual applications, you gain the following benefits:

* A single management infrastructure
* Scalability, deployment, and content distribution features, like collections and user device affinity
* Advanced application management features
* Operating system deployment, software and hardware inventory, software metering, and asset intelligence to support virtual applications

For more information about how to create and sequence applications with Microsoft Application Virtualization (App-V), see Application Virtualization 4 documentation.

In addition to the other Configuration Manager requirements and procedures for creating an application, you must take the following considerations into account when you create and deploy virtual applications:

* To deploy virtual applications to computers, you must have the Configuration Manager client and App-V Client installed on your computers. Client devices can include desktop and portable computers, and Virtual Desktop Infrastructure (VDI) clients. The Configuration Manager and App-V Client software work together to deliver, locate, and launch virtual application packages. The Configuration Manager client manages the delivery of virtual application packages to the App-V Client. The App-V Client runs the virtual application on the client.
* To deploy a virtual application, you must first create the virtual application by using the App-V Application Virtualization Sequencer. The sequencer monitors the installation and setup process for an application and records the information that is needed for the application to run in a virtual environment. You can also use the sequencer to set which files and configurations apply to all users, and which configurations users can customize.
* When you sequence an application, you must save the package to a location that Configuration Manager can access. You can then create an application deployment that contains this virtual application.
* Configuration Manager does not support the use of the shared read-only cache feature of App-V 4.6.
* Configuration Manager supports the Shared Content Store feature in App-V 5.
* When you create a deployment type for a virtual application, Configuration Manager creates the deployment type by using the contents of the application manifest file. This is an XML file that has information about the virtual application. Additionally, Configuration Manager creates requirements for the deployment type based on the contents of the App-V .osd file that has information about the supported operating systems for the virtual application.
* To deploy virtual applications in Configuration Manager, client computers must have at minimum the App-V 4.6 SP1 or a later version of the client installed.
* Before you can successfully deploy virtual applications, update the App-V client with the latest hotfix.
* When you use connection groups in App-V 5.0, your deployed virtual applications can share the same file system and registry on client computers. Unlike standard virtual applications, these applications can share data with one another. Additionally, connection groups preserve user settings for the applications that they contain. App-V virtual environments in Configuration Manager are used to set up connection groups on client computers. Virtual environments are created or changed on client computers when the application is installed or when clients next evaluate their installed applications. You can prioritize these applications so that when multiple applications try to change a file system or registry value, the application that has the highest priority takes precedence.

### 5.13 What is a virtual appliance (VA)?

Considered a software equivalent of a hardware device, a virtual appliance (VA) is a preconfigured software solution. It contains an operating system (OS) and a customized application to perform a fixed set of functions. When a software appliance is installed on a virtual machine (VM), it creates a virtual appliance, which is nothing but a VM image file.

### 5.13.1 Virtual appliance explained

A virtual appliance is a subset of the broader class of software applications. Thus, it is an application and its OS packaged together for use in a virtualized environment. Simply put, it is a software appliance installed on a virtual machine.

A VA does not require locally installed hardware and can be remotely accessed by users. Its purpose is to simplify the delivery and operation of an application, so only the OS components required to support the application's functions are included. This type of specialized OS is known as a "just enough operating system" (JeOS).

VAs usually come in the Open Virtualization Format (OVF). Because this format is vendor-independent, the appliance can be easily packaged and distributed in a single-file format. OVF is also beneficial for customers because it allows them to deploy, manage and update complex solutions easily.

Virtual appliances play a major role in cloud computing and cloud-based software as a service ([SaaS](https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service)) because they support the model's key USP: the delivery of software remotely through a user's web browser. VAs are also useful for quickly provisioning OSes and applications in the platform as a service ([PaaS](https://www.techtarget.com/searchcloudcomputing/definition/Platform-as-a-Service-PaaS)) model.

### 5.13.2.Types of virtual appliances

There are two types of virtual appliances:

* closed virtual appliance, which is always packaged, distributed, maintained, updated and managed as a unit; and
* open virtual appliance, which allows to customers to make modifications.

Developers can include a web interface to allow customers to make custom configurations, or to deliver patches and updates for the VA.

### 5.13.3. How a virtual appliance is deployed

A VA can be deployed as a VM or a subset of a VM running atop virtualization technology, such as VMware vSphere. This makes it possible to package, maintain and manage multiple VMs as a single unit.

Deploying an application as a VA can eliminate problems with installation and configuration, such as software or driver compatibility issues. Users can simply download a single file and run the application. Resources required for maintenance are also reduced.

### 5.13.4.Virtual appliance use cases

Virtual appliances have proved useful for deploying network applications. They are also helpful in grid computing, where they can solve problems introduced by heterogeneous hardware and operating systems, and in the SaaS delivery model, where the simplicity of the virtual appliance can help improve economies of scale.

### 5.13.5. Virtual appliance vs. virtual machine

While a VM offers significant advantages over physical machines, it can be operated only when the virtual hardware, guest OS and guest application are fully configured.

A VA, however, is a "turnkey" solution that's delivered to users in a preconfigured format. It simplifies deployment and saves time because it eliminates the need to manually configure different components, such as its VM and OS. It also minimizes the risk of configuration errors. Finally, because the application and OS are pretested, it's less likely that errors will be encountered when running the software.

### 5.13.6. Benefits of virtual appliances

Virtual appliances deliver numerous benefits for developers, vendors and customers, including:

**Reduced costs for developers, vendors and customers.** For developers and appliance vendors, virtual appliances help lower development and distribution costs. This is achieved by reducing the need for hardware testing and decreasing the number of platforms that need to be supported.

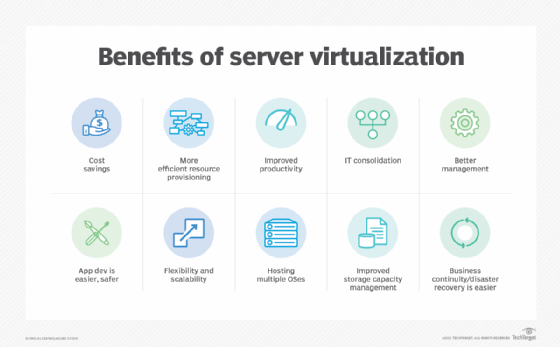
For vendors, VAs are a cheaper alternative to hardware appliances because they don't have to manage inventory or support hardware components. They can also distribute VAs online.

For customers, a VA reduces the cost of owning, operating and managing the software.

**Easier IT management.** With a VA, users have to manage a single solution instead of multiple applications, OS and server hardware. Moreover, they can get support from a single vendor for all components in the VA. All of this simplifies IT management, administration and maintenance.

**Accelerated time-to-market and time-to-value.** A VA reduces the time required for product evaluation, configuration, packaging and deployment, accelerating time-to-value for customers. It also shortens the sales cycles for vendors, accelerating their time-to-market. Further, vendors can expand customer reach by targeting potential customers they would not be able to target with hardware appliances.

**Enhanced security with isolation.** Virtual appliances run in an isolated environment, with different appliances shielded from each other. With that arrangement, if the security of any VA is compromised, other VAs will not be affected and can continue functioning.



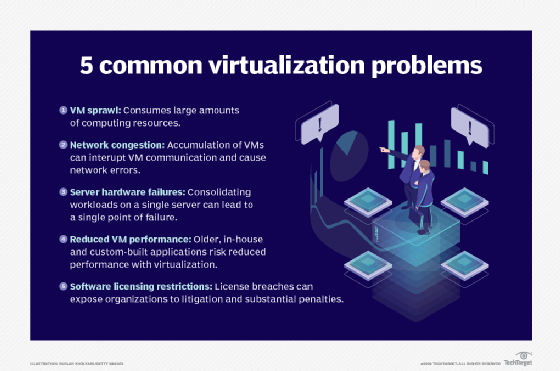
Typical advantages of server virtualization

### 5.13.7. Challenges in upgrading virtual appliances

Like other software products, a virtual appliance also needs upgrades to fix errors/[bugs](https://www.techtarget.com/searchsoftwarequality/definition/bug) or to add more features. However, because it is preconfigured and self-contained, upgrading a VA can be a complex endeavor.

Upgrading involves two main aspects: the application software and the running environment. The approach to upgrading depends on the types of changes that need to be made. If the upgrade is required to change the application's features/requirements, it should be modified first. However, if the upgrade is primarily aimed at fixing a bug or security issue in the running environment, it's crucial to first consider the implications of these changes on the application.

For instance, if a new OS creates the need for a new language environment, then the target application must also be modified.



One possible issue during upgrades is that the OS may be past its support period. If the OS vendor no longer provides security updates or fixes bugs, users must upgrade to a newer version. They may also have to update link libraries and use a newer programming environment to build the VA application.