Symantec Enterprise Vault™ Best Practice Guide – Implementing Enterprise Vault on Hyper-V

Who should read this paper

This Whitepaper is intended to assist customers, partners and service providers as they plan to implement Enterprise Vault on Microsoft Hyper-V.

If you have any feedback or questions about this document please email them to **iig-tfe@symantec.com** stating the document title.

This document applies to the following version(s) of Enterprise Vault:

10.0.3 and later

Table of Contents

Document Control

Contributors

Who	Contribution
Dan Strydom	Author

Revision History

Version	Date	Changes
1.0	June 2013	Published

Related Documents

Document Title	Document Location	Version
Symantec Enterprise Vault Administrator's Guide	www.symantec.com/docs/DOC2200	10.0.4
Enterprise Vault 10 Performance Guide	www.symantec.com/docs/DOC4553	10.0.4
Enterprise Vault 10 – Best Practices for Indexing	www.symantec.com/docs/DOC4250	Dec 2011
Enterprise Vault 10 – Best Practice Guide for SQL	www.symantec.com/docs/DOC5365	Jan 2013

Scope of Document

This document aims to provide guidance on designing and deploying Enterprise Vault 10 on the Microsoft Hyper-V 2012 platform. The recommendations in this document do not apply to earlier versions of Enterprise Vault or Hyper-V.

This document should be used in conjunction with other performance and best practice guides as outlined in the "Related Documents" section of this document.

Intended Audience

This document is aimed at Enterprise Vault customers, partners and service providers. It is assumed that the reader has a thorough understanding of the architecture and operational aspects of Enterprise Vault 10. It is also assumed that the reader has experience and understanding of Microsoft Hyper-V 2012.

Terminology Used In This Document

Term	Description
Virtual Machine	A virtual machine is an isolated software container that can run its own operating systems and applications as if it were a physical computer
Hypervisor	A hypervisor, also called a virtual machine manager (VMM), is a program that allows multiple operating systems to share a single hardware host
HBA	Host Bus Adapter, normally associated with a Fibre Channel Storage Connectivity
CSV	Cluster Shared Volumes, a feature of Failover Clustering in Hyper-V
NIC	Network Interface Card
IOPs	Input/Output operations per second, used when measuring performance
MPIO	Multi-path Input/Output is a protocol used to provide redundant paths and load-balancing features to storage devices
Snapshot	Virtual machine snapshots are file-based snapshots of the state, disk data and configuration of a virtual machine at a specific point in time
VHD	Fixed Virtual Hard Disks
VHDX	Newer version of VHD. The new format disk supports storage capacity of up to 64TB, provides improved protection against power failures and improved alignment of the virtual hard disk format to work on large sector disks

Benefits of Using Enterprise Vault on Hyper-V

Virtualization technology introduces many benefits to IT organizations around the world, including cost savings both in terms of lowered data center power consumption and cooling requirements. Virtualization typically also simplifies the datacenter landscape through server consolidation, requiring less hardware to provide the same service to end users with the added benefit of application independent high availability.

With a virtual infrastructure deployment, the architecture can be as modular as is appropriate, without expanding the hardware footprint. While it is important to accurately design your environment, the dynamic nature of virtual machines mean that the design can grow and adapt as required, without the need for an initial "perfect" design. Virtual deployments typically take minutes, can share currently deployed hardware, and can be adjusted "on the fly" when more resources are required.

Certain server applications however are less suitable for virtualization, especially those requiring extensive use of physical server resources such as CPU and memory. Traditionally customers have been reluctant to place applications with high service level agreements such as Microsoft Exchange Server and SQL Server on a virtual platform, not only because the application's demand on resources meant that only one or two virtual machines could co-exist on a single server, but also because the server could not offer the same performance it would have on a physical machine.

More powerful hardware, enhancements in virtualization technology and better support from application vendors now mean that customers are looking to virtualize all the traditional Enterprise applications.

Considerations before deploying Enterprise Vault on Hyper-V

A number of factors should be considered before deploying Enterprise Vault in a Hyper-V environment:

1. Enterprise Vault is heavily dependent on CPU resources. In a typical physical server configuration it is not unusual for the CPU to run at 80% or higher utilization during scheduled archiving. Generally the CPU has the greatest impact on archive ingestion rates and index search performance, and therefore a less powerful CPU would impact archiving and search performance.
2. The recommended CPU and memory configuration for Enterprise Vault 10 is 8 CPU cores and 16GB RAM. Consider therefore the number of virtual machines you plan to deploy on a single physical server, and decide whether deploying Enterprise Vault in your virtual environment will be a cost effective option.
3. It is recommended that CPU and Memory resources are dedicated (reserved) to the Enterprise Vault server, and not shared with other virtual machines on the host. This aligns with Hyper-V recommendations for virtualizing enterprise applications such as Microsoft Exchange Server.

If the above considerations are acceptable and supported by the Hyper-V environment then it is likely that virtualizing the Enterprise Vault environment will be a good fit for the organization.

Sizing Enterprise Vault for Hyper-V

One of the most important considerations when sizing Enterprise Vault is a thorough understanding of the expected workload on each of the Enterprise Vault servers. The initial design of Enterprise Vault should be done independent of whether it will run on physical servers or virtual machines - with the main consideration being the customer requirements for archiving and eDiscovery. It is expected that if the Hyper-V environment is optimally configured the performance of the virtual machine should have no more than 15% reduction in performance when compared a similarly specified physical server.

It is outside the scope of this document to provide a design and sizing introduction to Enterprise Vault, but in general terms, once the customer requirements are understood, a closer look at the archive targets will help determine what server resources will be required to not only archive the backlog (based on the archiving policy) but also keep up with the daily change (also known as the “steady-state”).

Enterprise Vault sizing utilities such as Exchange Mailbox Analyzer, Domino Mail File Reporter, File System Analyzer, SharePoint Analyzer and PST Analyzer will help provide a better understanding of what data is held within the archive targets and what the impact of different archiving policies will be. A qualified Symantec Professional Services Partner will have access to these utilities, and the data collected from these sizing utilities can then be used in the Enterprise Vault 10 Sizing Estimator Tool.

From here the tool will provide a number of recommendations, including number of Enterprise Vault servers, expected performance for different CPU configurations, SQL database recommendations and estimated Vault Store and Index storage figures over a 3 year period. This overview represents an over simplified view of the design process as there will be many environment specific factors that will affect a design.

The following sections in this guide will provide detail on how to configure the various Hyper-V components for optimal performance.

Hyper-V Host Considerations

Windows Server 2012 provides two different deployment options for Hyper-V – the Server with a GUI and the Server Core installation. The Server Core version is recommended as it requires less disk space, reduces the potential security vulnerabilities on an Operating System level and requires less frequent restarts (due to fewer software updates). Both versions are supported by Enterprise Vault although the Server Core version is recommended.

The following best practices apply to the Hyper-V host:

- Confirm that the host hardware supports the Hyper-V features you wish to use – specifically hardware-enforced Data Execution Prevention must be available and enabled. On Intel servers the XS bit (execute disable bit) and on AMD servers the AMD NX bit (not execute bit) should be enabled

- Ensure that hosts are running the latest BIOS version, and all hardware devices such as Fiber Channel Host Bus Adapters (HBA) and Network Interface Cards (NIC) also have the latest firmware installed
- Ensure that Hyper-V hosts are up to date with recommended Microsoft updates
- Hosts should be joined to a domain to provide centralized management of policies, security and auditing.

The host Anti-virus software should exclude Hyper-V specific files such as:

- All folders containing VHD, VHDX, AVHD, VSV and ISO files
- Default virtual machine configuration directory (C:\ProgramData\Microsoft\Windows\Hyper-V)
- Default Snapshot directory (%systemdrive%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots)
- Default virtual machine disk drive directory
- Any Snapshot directories
- Cluster Shared Volume directory (C:\ClusterStorage)
- Hyper-V Program Files "vmms.exe" and "vmwp.exe".

It is recommended that periodic performance counters are run on the host, with specific focus on CPU, memory and disk latency issues. Appendix B contains in-guest Windows performance counters relevant to Enterprise Vault.

CPU

One of the key decisions for Enterprise Vault deployments on Hyper-V is how many vCPU cores to assign to each of the Enterprise Vault servers. The CPU component is the biggest driving factor in determining archive rates and search throughput. As with most other virtual components you can add or remove resources after the server is configured – with Enterprise Vault this is especially useful as you may wish to allocate more CPU resources early on in a new deployment to help archive the backlog faster. Once archiving has "caught up" with the specified policy it is likely that fewer resources are required to keep up with the daily change of data to be processed. Resources can also be added for specific purposes, such as increasing the archive ingestion rates during a PST Migration. The 64-bit indexing architecture of Enterprise Vault can make full use of the high resource ceiling in Hyper-V 2012 - Windows 2012 Hyper-V supports virtual machines with up to 64 virtual processors and 1TB of memory.

Hyper-V provides a *Weights* and *Reserves* feature to help fine-tune CPU allocation to virtual machines:

- Weights are assigned to a virtual processor to guarantee a larger or smaller share of CPU cycles than the average cycle share
- Reserves on the other hand are set for a virtual processor to ensure it gets a minimum specified percentage of the total possible CPU use when there is contention on the host.

Weights and reserves can be used to control how each vCPU in a virtual machine uses physical logical processors. For example a 100% reserve will give a vCPU 100% use of a logical processor. This is especially useful for applications with CPU intensive workloads such as Enterprise Vault to guarantee a certain service level for application performance.

It is recommended that at least 8 vCPU cores are dedicated to the Enterprise Vault server. **For optimum performance Symantec recommends that the vCPU cores assigned to Enterprise Vault servers are set with a 100% reserve.** Increasing the number ofv CPU cores available to an Enterprise Vault server has by far the greatest impact on ingestion performance.

Avoid the use of hyper-threading by the hyper-visor as this provides no performance benefit to Enterprise Vault. Review the CPU section of the Enterprise Vault 10 Performance Guide for more information.

Figure 1 shows an example of this configuration.

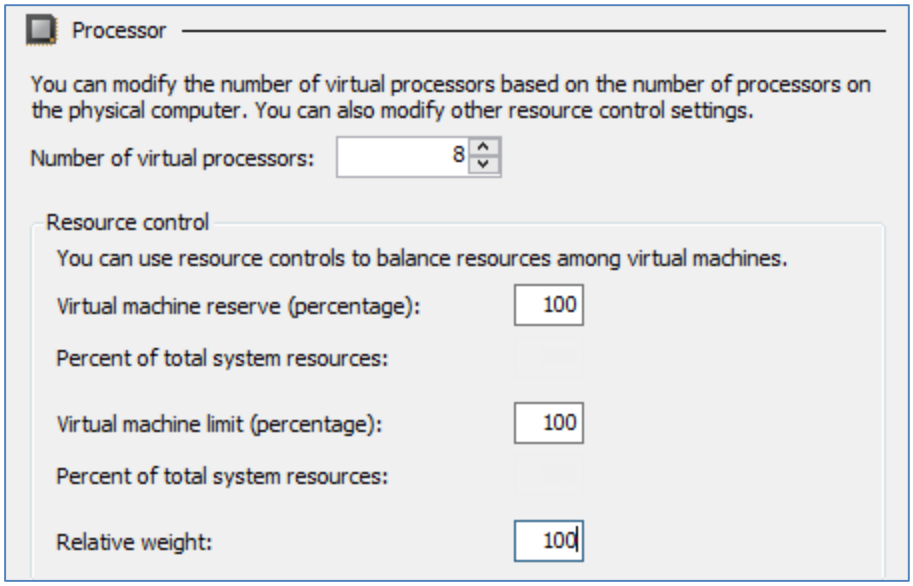

Figure 1 Recommended CPU weight and reserve settings

Memory

Hyper-V provides the ability to oversubscribe or dynamically adjust the memory available to a virtual machine. This technology works very well for machine workloads that require the memory for a brief period of time, however it is not suitable for virtual machines that require the memory on an ongoing basis.

Enterprise Vault index operations require the server to cache data in memory, and is therefore susceptible to poor performance and unacceptable client response times if it doesn't have full control over the memory allocated to the virtual machine. **As a result the Dynamic Memory features are not recommended for Enterprise Vault.**

Figure 2 shows a screenshot of the New Virtual Machine Wizard – do not tick the box "Use Dynamic Virtual Memory for this machine".

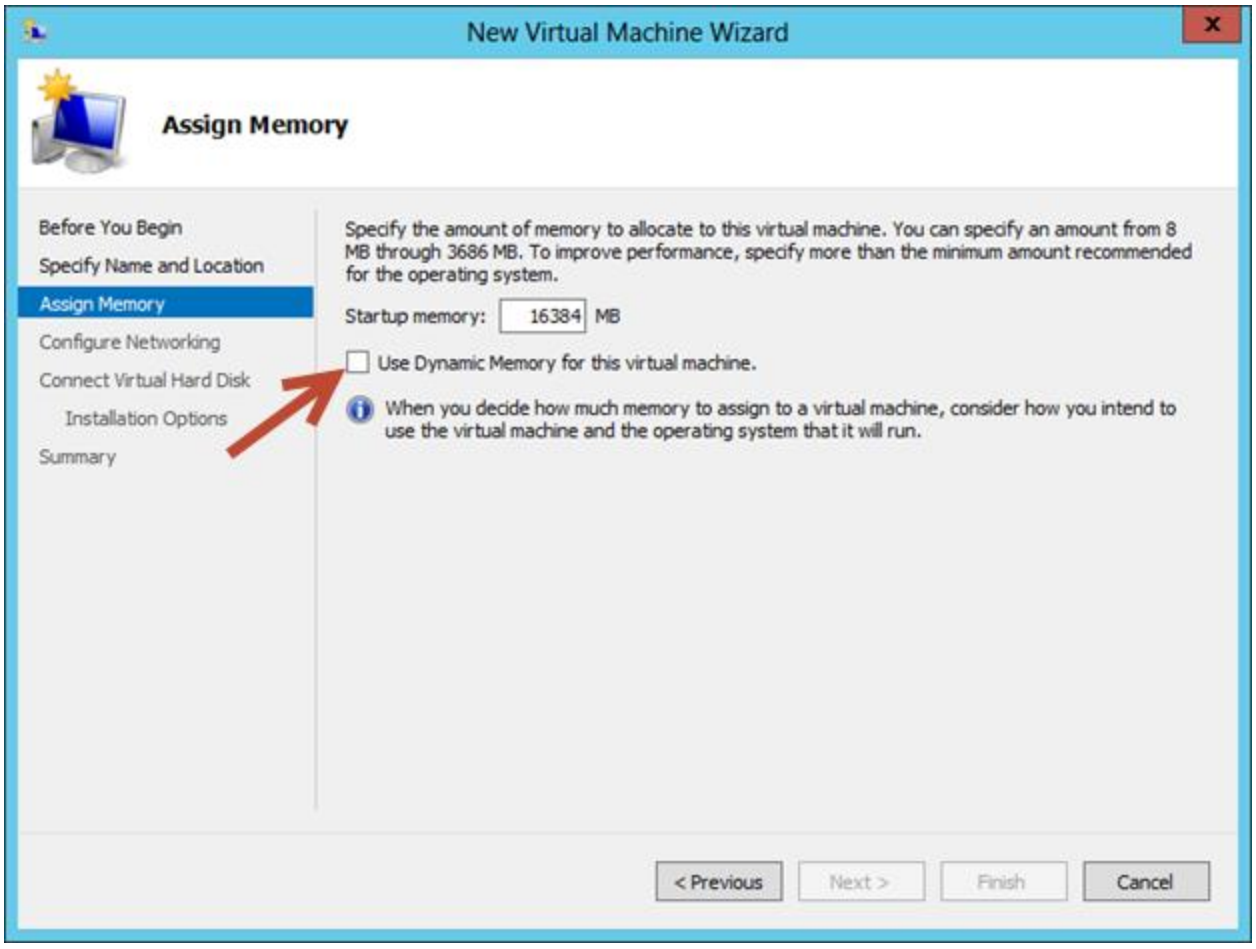

Figure 2 New Virtual Machine Wizard

The virtual machine memory size should always be set to a value greater than the average memory usage of the Enterprise Vault server. This will avoid guest operating system swapping. In a typical Enterprise Vault environment around 6GB of RAM will be used in core activities during the day, increasing to 16GB+ recommended memory with journaling and searching (end user searches, Virtual Vault activity, etc.).

It is therefore recommended that a minimum 16GB of memory is dedicated to the Enterprise Vault server.

To find out more about expected server performance for different CPU and memory configurations please refer to the Enterprise Vault 10 Performance Guide.

Figure 3 shows an example configuration for an Enterprise Vault server. Note that the weight slider is set to provide the server with full priority use of the assigned memory.

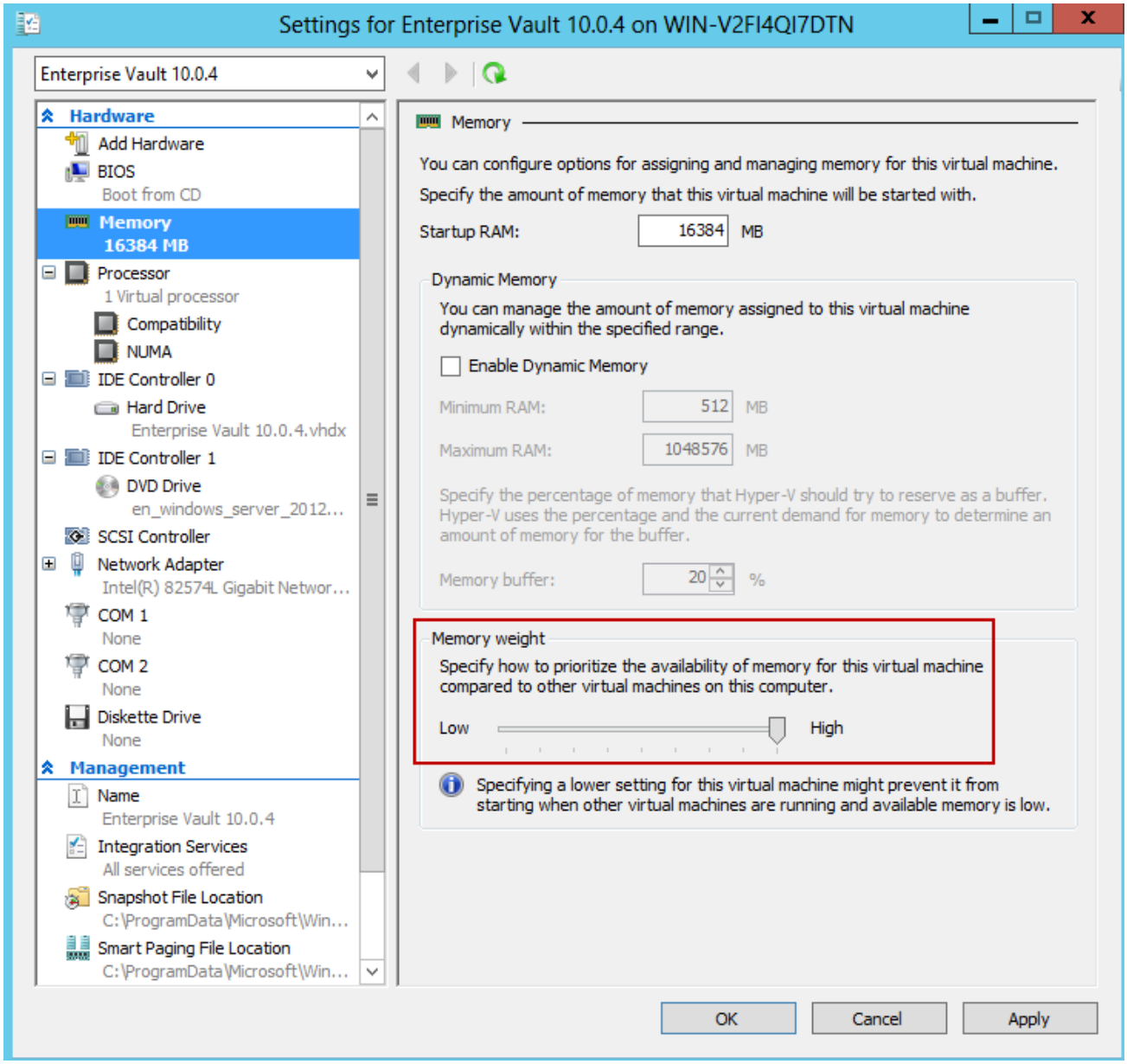

Figure 3 - Memory Weight value recommended to High

When setting the page file size it is best to allow Windows 2012 to handle the page file sizing. It is recommended that the page file is moved to a high performing storage device – make sure it does not share the same storage device as the operating system files.

Storage

Depending on the customer requirements for archiving and search it is likely that a number of different storage areas with varying performance requirements will be needed.

The storage used for Enterprise Vault can be virtual storage of a fixed size (for example, fixed virtual hard disks (VHDs) in a Hyper-V environment), SCSI pass-through storage, or Internet SCSI (iSCSI) storage. Pass-through storage is configured at the host level, and typically dedicated to one guest machine.

All storage for Enterprise Vault should be block-level storage – with the exception of Vault Store Partitions. While Enterprise Vault supports network attached storage (NAS) for Index Volumes, typically the performance from these devices is not sufficient for anything other than Enterprise Vault saveset storage.

The following general storage recommendations apply:

- Storage used by Enterprise Vault should be hosted in disk spindles that are separate from the storage that's hosting the guest virtual machine's operating system
- Configuring iSCSI storage to use an iSCSI initiator inside an Enterprise Vault guest virtual machine is supported. However, there is reduced performance in this configuration if the network stack inside a virtual machine isn't full-featured (for example, not all virtual network stacks support jumbo frames)
- Any new disk should be created in the VHDX format – disks created in earlier versions of Hyper-V should be converted to VHDX. The new format disk supports storage capacity of up to 64TB, provides improved protection against power failures and improved alignment of the virtual hard disk format to work on large sector disks
- Disks should be of the fixed format in production environment to provide increased disk throughput. Differencing and Dynamic disks are not recommended for production due to increased disk read/write latency times[1]
- Loopback configurations (where the computer that is running Hyper-V is used as the file server for virtual machine storage) should be avoided
- Confirm that the depth of the queue of outstanding commands on the SCSI adapter is set to the manufacturer's recommended setting. A queue depth that is too small limits the disk bandwidth that can be pushed through the virtual machine – this is a very common performance bottleneck
- Virtual hard disks with paging files should be excluded from replication, unless the page file is on the same disk as the operating system (not recommended).

[1] For more information see **http://technet.microsoft.com/en-us/library/cc720381(v=WS.10).aspx**

Pass-Through Disks

Pass-through disks are LUNs or physical disks attached to a virtual machine. Pass-through disks provide slightly better performance when compared to using VHDX files – Pass-through disks however do not offer the same level of flexibility found with VHDX disks. Carefully consider the performance requirement and the ongoing management of the solution before deciding which option is suitable for your environment.

Virtual IDE vs. Virtual SCSI

Virtual machines can use either virtual IDE device controllers or virtual SCSI device controllers. When starting a virtual machine the virtual IDE controller is used as the virtual SCSI drivers cannot be loaded until the operating system is started. The Virtual IDE controller is limited to 3 connected disks, where the virtual SCSI can have 4 controllers with 64 disks per controller. It is therefore recommended that Enterprise Vault drives are attached to the Virtual SCSI controller for more flexibility.

Enterprise Vault Storage Locations

Table 1 - Enterprise Vault per Server Storage Locationsdetails the storage requirements of Enterprise Vault. For optimal performance, each of the storage areas should be treated as a separate storage areas.

Per server storage area	Type of access	Expected Size	Recommendation
Index Locations	Sequential Access. Large flat file area consisting of many small files	Depending on Indexing Level – Brief 3% of total information archived, Full Indexing will require 12%	Fast SAN based storage – FC or iSCSI. Storage should be capable of supporting 400+ IOPS, 2000+ IOPS for eDiscovery environments. NAS storage not considered appropriate in most scenarios (refer to Indexing Best Practice paper for more information)
Vault Store Partitions	Random Access. Large flat file area consisting of many small files	Very large but split up in smaller "vault partitions"	Slower, lower tier storage such as NAS is appropriate. Low IOPS requirement
MSMQ Data and Log Folder	Data and Log locations will be random access, and log location sequential	40GB	Fast SAN based or local RAID1 disk. Ideally split onto a different spindle set from MSMQ Log area for optimum performance
Vault Server Cache Area	Random Access	50GB	Fast SAN based disk, RAID1 or better performing stripe. Storage should be capable of supporting 400 IOPS for typical environment. Virtual Vault environments can expect up to 1,000 IOPS during busy periods
Windows Temp Directory	Random Access	Minimum 2GB	Fast SAN based disk, used for temporary EV operations RAID1 or better performing stripe. Used during archiving to process large files

Table 1 - Enterprise Vault per Server Storage Locations

Storage performance depends on many factors, including the workload, hardware, RAID level, cache size, stripe size, etc. The storage vendor documentation should always be consulted along with Microsoft Hyper-V recommendations.

Choosing Suitable Storage for Index Locations

When choosing a suitable storage device the whole storage solution should be considered. The supported IOPs is just one aspect of performance and other areas should also be looked at such as connectivity – for example Fiber and iSCSI are preferred over CIFS.

A high speed storage device is recommended for Index locations. Lower tier NAS devices are generally not recommended for index locations, and should definitely not be used to host indexes where any type of eDiscovery search is used. NAS devices connected over CIFS shares are not suitable to host index volumes for certain environments due to the slower connectivity speed. The best devices are local storage, direct attached storage[2], or SAN LUNs.

In the case of local or direct attached storage:

- Use multiple controllers supporting multiple channels to distribute the load between index file locations and provide sufficient throughput
- Provide battery-backed read and write cache to aid performance.

Before using partitions on a SAN, consider the I/O load together with any other applications that are already using the SAN to ensure that the performance can be maintained. Ideally, the implementation should be discussed with the SAN hardware vendor to ensure that optimum performance is achieved. Typically LUNs should be created across as many suitable disks as possible, using entire disks rather than partial disks to prevent multiple I/O-intensive applications from using the same disks.

The following general recommendations apply to Enterprise Vault index locations:

- If indexes are stored on NetApp devices, and possibly other NAS systems, opportunistic locking must be turned off for volumes that contain indexes
- Disable Windows file indexing on the drives that contain Enterprise Vault indexes.

Make sure to give thought to the growth strategy up front. As the Vault Store and Index volume grows, how will the growth of data files / LUNs / RAID groups be managed? It is much better to design for this up front than to rebalance data files or LUN(s) later in a production deployment.

[2] Local storage and direct attached storage may restrict the high availability options for the server. Normally a SAN or NAS device is more suitable to provide failover capability.

The index files can quickly become fragmented on disk, even if there is a large volume of free storage capacity. This file fragmentation can cause severe performance problems which need to be managed on any index storage device. Either an automated background file defragmentation product or scheduled device defragmentation must be employed.

For more information please see the Enterprise Vault 10 – Best Practices for Indexing[3] document.

Snapshots

Hyper-V includes the ability to take snapshots of virtual machines. The snapshots captures the state of a virtual machine while it's running, but as the snapshot processes are not application aware using them can cause unexpected consequences - especially in environments where multiple EV servers can have dependencies on other servers (such as a remote storage service). Snapshots can however be useful when making changes to the server that will only affect the local machine, such as testing a hotfix. Additional care should be taken when doing snapshots during an Enterprise Vault upgrade, as the Enterprise Vault server version should be kept in step with the SQL database schema version. Snapshots can have a considerable impact on server performance and should therefore only be used outside of normal business hours.

Network

The following best practices apply to the network configuration of the Enterprise Vault virtual machine:

- Ensure NIC adapters have the latest firmware, as this often addresses known issues with hardware
- Ensure that the latest network interface drivers have been installed on the host
- Network interface cards used for iSCSI communication should have "All Networking protocols" (on the Local Area Connection Properties) unchecked, with the exception of:
    - Manufacturers protocol (if applicable)
    - Internet Protocol Version 4
    - Internet Protocol Version 6
    - Unbinding other protocols (not listed above) helps eliminate non-iSCSI traffic/chatter on the network adapters.
- Do not use NIC teaming on adapters used for iSCSI – use MPIO instead. Teaming can be used on Management, Production, CSV Heartbeat and Live Migration adapters. Also check that the "Do not

[3] www.symantec.com/docs/DOC4250

allow cluster network communication on this network" setting is enabled to prevent cluster traffic on the iSCSI adapter

- Turn off VLAN filters on teamed NICs. It is preferred to let the teaming software or the Hyper-V switch (if present) do the filtering
- Where possible use Single Root I/O Virtualization (SR-IOV). This will give the highest network performance possible by giving the virtual machines direct access to the network adapter hardware, bypassing the virtual networking stack
- Ensure that there are enough network adapters in the failover cluster to support each traffic type – this is especially important when you need to isolate traffic types from each other.

General Best Practice Recommendations

The following general best practices apply to running Enterprise Vault in a Hyper-V environment:

- Schedule backups and virus scanning programs[4] in virtual machines to run at off-peak hours, outside of the archiving schedule. Avoid scheduling them to run simultaneously in multiple virtual machines on the same Hyper-V host
- Unused or unnecessary virtual hardware devices can impact performance and should be disabled. For example, Windows guest operating systems poll optical drives (that is, CD or DVD drives) quite frequently. When virtual machines are configured to use a physical drive, and multiple guest operating systems simultaneously try to access that drive, performance could suffer. This can be reduced by configuring the virtual machines to use ISO images instead of physical drives, and can be avoided entirely by disabling optical drives in virtual machines when the devices are not needed
- Ensure that that the version of Integration Services on the guest virtual machine matches that of the host where possible. Note that when a host version is updated the client virtual machines does not automatically get up dated. To find out if the guest Integration Services are out of date look for 4010 events logged in the Windows Event Viewer.

The following in-guest Windows 2012 server tweaks are recommended for Enterprise Vault servers:

- Disable, throttle, or stagger periodic activity such as backup and defragmentation
- Review the scheduled tasks and services that are enabled by default

[4] Refer to www.symantec.com/docs/TECH48856 for a recommended list of anti-virus exclusions applicable to Enterprise Vault

- Disable background services such as SuperFetch and Windows Search
- Disable visual user interface enhancements.

Virtualizing SQL Server

Follow the recommendations of Microsoft when you size and configure the environment for SQL Server. The following general recommendations can be made when virtualizing SQL for Enterprise Vault:

- Virtual hard disks should be created as fixed size and not dynamic
- The required memory capacity should be dedicated and prioritized to the virtual machine to prevent dynamic allocation or sharing
- Avoid the use of hyper-threading by the hyper-visor
- The processor cores should be exclusively dedicated to the virtual machine, and the processor weights and reserves set to provide the virtual machine with full utilization of the selected vCPUs.

For more information please refer to the Enterprise Vault 10 Best Practices for SQL document[5].

Performance Impact of Upgrading to Enterprise Vault 10 from Earlier Versions

Enterprise Vault 10 introduces a new 64-bit indexing engine, offering many advantages over the 32-bit engine found in earlier versions. The new indexing engine is more scalable and provides better performance but, as is common with any 64-bit application, it requires more powerful hardware – the recommended CPU and memory requirements have increased to 8 CPU cores and 16GB of RAM as mentioned earlier in this document. If you are upgrading from Enterprise Vault 9 on an existing virtual environment it is important that these requirements are met, and supported by the version of Hyper-V. Customers using this recommended hardware should expect to see equal or better archiving performance when compared to a server running EV9 on the recommended hardware specified for that version. Please refer to the EV10 Performance guide for more information[6].

[5] **www.symantec.com/docs/DOC5365**

[6] **www.symantec.com/docs/DOC4553**

Appendix A: Checklist: Enterprise Vault on Hyper-V

Item	Check
CPU	
Minimum 8 CPU cores assigned to the virtual machine	
CPU reserve set to 100%	
Hyper-V Host is not oversubscribed	
Memory	
Check that virtual machine is not enabled for Dynamic Memory	
Minimum 16GB RAM assigned to the virtual machine	
Page File moved to high performance storage device, not sharing with OS	
Storage	
All disks are VHDX or Pass-through	
Disks are fixed size format	
Index volumes are on high performing disk	
MSMQ Data/Log split off to dedicated spindle set	
Vault Server Cache area moved to fast performing spindle set	
Windows Temp Directory to fast performing spindle set	
If using NetApp for Index volumes – disable opportunistic locking	
Disable Windows Indexing on EV Index volumes	
Scheduled defragging is configured on EV Index volumes	
Network	
Adapters are using latest drivers and firmware	
Protocols checked for iSCSI adapters	
General	
Backup and anti-virus schedules are appropriately configured	
Unused virtual devices are disabled	
Guest Integration Services are the same version as the host	

Appendix B - Windows Performance Counters

The following counters may be useful to monitor within the virtual machine:

Objects and Counters	Description
Processor	
% Processor Time	Shows processor usage over a period of time. If this counter is consistently too high it is likely that the system performance will be impacted. You can measure the utilization on each processor to achive balanced performance between cores.
Disk	
Avg. Disk Queue Length	Shows the average number of read and write requests that were queued for the selected disk during the sample interval. A bigger disk queue length may not be a problem as long as disk reads/writes are not suffering and the system is working in a steady state without expanding queuing.
Avg. Disk Read Queue Length	The average number of read requests that are queued.
Avg. Disk Write Queue Length	The average number of write requests that are queued.
Disk Reads/sec	The number of reads to disk per second.
Disk Wites/sec	The number of writes to disk per second.
Memory	
Available Mbytes	Shows the amount of physical memory available for allocation. Insufficient memory is likely to cause excessive use of the page file and an increase in the number of page faults per second.
Cache Faults/sec	Shows the rate at which faults occur when a page is sought in the file system cache and is not found. This may be a soft fault, when the page is found in memory or a hard fault when the page is on disk. The use of cache for read and write operations can have a significant impact on server performance. Monitor for increased cache failures, indicated by a reduction in the Async Fast Reads/sec or Read Aheads/sec.

Pages/sec	Shows the rate at which pages are read from or written to disk to resolve hard page faults. If this rises, it indicates system-wire performance problems.

Objects and Counters	Description
Paging File	
% Used and % Used Peak	The server paging file holds “virtual” memory addresses on disk. Page faults occur when a process has to stop and wait while required “virtual” resources are retrieved from disk into memory. These are more frequent if the physical memory is inadequate.
Network	
Total Bytes/sec	The rate at which data is sent and received on the network interface. If the rate is over 50% capacity you should investigate for issues. To troubleshoot monitor Bytes Received/sec and Bytes Sent/sec.
Avg. Disk Read Queue Length	The average number of read requests that are queued.
Avg. Disk Write Queue Length	The average number of write requests that are queued.
Disk Reads/sec	The number of reads to disk per second.
Disk Wites/sec	The number of writes to disk per second.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at **www.symantec.com**.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com