HPE PRESENTS

THE GORILLA GUIDE to...

Hyperconverged Infrastructure Technical Overview

Scott D. Lowe

INSIDE THE GUIDE:

• Discover the five key architectural elements you need to consider before you adopt a hyperconverged data center
• Learn how software defined networking and hyperconverged infrastructure have come together to power modern enterprises
• Get answers to your most pressing data center challenges
ENTERING THE JUNGLE

Chapter 1: Introduction to Hyperconverged Infrastructure

Hyperconverged Infrastructure from 30,000 Feet ......................................................... 9
Resources to Consolidate ................................................................................................. 11

Chapter 2: Architecting the Hyperconverged Data Center

Decision 1: Server Support ............................................................................................... 16
Decision 2: The Storage Layer ....................................................................................... 16
Decision 3: Data Protection Services ............................................................................ 23
Decision 4: The Management Layer ............................................................................. 23
Decision 5: The Network ................................................................................................. 25

Chapter 3: Exploring the Intersection of Software-Defined Networking and Hyperconverged Infrastructure

How Hyperconvergence Leverages the Network .......................................................... 27
The Result of Network-Centric Data Protection ......................................................... 28
Latency Origination Points ............................................................................................ 29
Traditional Network Designs and Hyperconvergence ................................................ 30
Enter Software-Defined Networking ......................................................................... 31
SDN and Hyperconverged Infrastructure ..................................................................... 36

Chapter 4: Addressing Data Center Pain Points

The Relationship Between Performance & VM Density ............................................. 38
Storage Performance in a Hyperconverged Infrastructure ....................................... 39
Chapter 5: Ensuring Availability, Data Protection and Disaster Recovery

The Data Protection and Disaster Recovery Spectrum

End Results: High Availability, Architectural Resiliency, Data Protection, and Disaster Recovery

Chapter 6: Hyperconverged Infrastructure in a Hybrid Cloud World

Why Is Cloud So Desirable?

The Public Cloud

On-Premises Reality

Private Clouds

Hybrid Cloud & Multi-Cloud

The Intersection of Cloud and Hyperconverged Infrastructure
The Gorilla is the professorial sort that enjoys helping people learn. In the School House callout, you’ll gain insight into topics that may be outside the main subject but are still important.

This is a special place where you can learn a bit more about ancillary topics presented in the book.

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

Takes you into the deep, dark depths of a particular topic.

Discusses items of strategic interest to business leaders.
ICONS USED IN THIS BOOK

DEFINITION
Defines a word, phrase, or concept.

KNOWLEDGE CHECK
Tests your knowledge of what you’ve read.

PAY ATTENTION
We want to make sure you see this!

GPS
We’ll help you navigate your knowledge to the right place.

WATCH OUT!
Make sure you read this so you don’t make a critical error!
CHAPTER 1

Introduction to Hyperconverged Infrastructure

The world of technology is changing at both a broader and faster pace than ever before. In years past, IT practitioners and decision makers might have had to deal with a few new hardware options and some software upgrades. Today, changes come every day as companies break the data center walls in favor of hybrid cloud, as cloud providers continue to grow, and as software updates deploy silently behind the scenes.

As employees devour technologies such as smartphones, tablets, wearables, and other devices, and as they become more comfortable with solutions such as Slack, Dropbox, and Zoom, their demands on enterprise IT intensify. On top of this, management and other decision makers are also increasing their demands on enterprise IT to provide application environments that have higher levels of availability and easier growth capability, but with the kinds of pay-as-you-grow economics that they see from the cloud. Unfortunately, enterprise IT organizations often don’t see much, if any, associated increases in funding to accommodate these demands, particularly as spending increases on other business priorities, such as improved security, analytics, and digital transformation efforts.

These demands have resulted in the need for IT organizations to attempt to mimic NASA’s much-heralded “Faster, Better, Cheaper” operational campaign. As the name suggests, NASA made great attempts to build new missions far more quickly than was possible in the past, with greater levels of success, and with costs that were dramatically...
lower than previous missions. NASA was largely successful in its efforts, but the new missions tended to look very different from the ones in the past. For example, the early missions were big and complicated with a ton of moving parts, while modern missions have been much smaller in scale with far more focused mission deliverables.

The same “Faster, Better, Cheaper” challenge is hitting enterprise IT, although even the hardest-working IT pros don’t usually have to make robots rove the surface of an inhospitable planet! Today’s IT departments must meet a quickly growing list of business needs while, at the same time, appeasing the decision makers who demand far more positive economic outcomes, either by cutting costs overall or doing more work within the existing budget.

Even as the public cloud continues to gain favor for certain workloads, the real center of workload action remains the on-premises data center. Unfortunately, traditional data center architectures actively work against modern goals, because with increasing complexity comes increased costs—and things have definitely become more complex. Virtualization was a fantastic opportunity for companies, but with virtualization came new challenges, including major issues with storage. With virtualization, enterprise IT moved from physical servers, where storage services could be configured on a per-server basis, to shared storage systems. These shared storage systems, while offering plenty of capacity, have often not been able to keep up in terms of performance, forcing IT departments to take corrective actions that don’t always align with good economic practices.

These are just some of the challenges that administrators of legacy data centers need to consider as well:

- **Hardware sprawl.** Data centers are littered with separate infrastructure silos that are all painstakingly cobbled together to form a complete solution. This hardware sprawl results in a data center that’s increasingly complex, decreasingly flexible, and expensive to maintain.
• **Policy sprawl.** The more variety of solutions in the data center, the more touch points that exist when it comes to applying consistent policies across all workloads.

• **Scaling Challenges.** Predictability is becoming extremely important. That is, being able to predict ongoing budgetary costs and how well a solution will perform after purchase are important. Legacy infrastructure and its lack of inherent feature-like scaling capability make both predictability metrics very difficult to achieve.

• **Desire for less technical overhead.** Businesses want analysts and employees that can help drive top-line revenue growth. Purely technical staff are often considered expenses that must be minimized. Businesses today are looking for ways to make the IT function easier to manage overall so that they can redeploy technical personnel to more business-facing needs. Legacy data centers are a major hurdle in this transition.

• **A focus on security.** Security has always been important, but never more than it is today. Increasingly a boardroom issue, security spending is accelerating, sometimes at the expense of other areas of IT, a situation that data center architects need to accommodate.

So, with all of this in mind, what are you to do?

**Hyperconverged Infrastructure from 30,000 Feet**

A number of years ago, a new data center architectural option, dubbed hyperconverged infrastructure, came on the scene and exploded faster than anyone could have imagined. Hyperconvergence is a way to reduce your costs and better align enterprise IT with business needs. At its most basic, hyperconverged infrastructure is the conglomeration of the servers and storage devices that comprise the data center with modern iterations of the technology also swallowing up complex networking components. These systems are wrapped in comprehensive...
and easy-to-use management tools designed to help shield the administrator from much of the underlying architectural complexity while providing an infrastructure that’s self-managing.

Why are storage and compute at the core of hyperconverged infrastructure? Simply put, storage has become an incredible challenge for many companies. It’s one of—if not the—most expensive resources in the data center and often requires a highly skilled person or team to keep it running. Moreover, for many companies, it’s a single point of failure. When storage fails, swaths of services are negatively impacted. Finally, with the increase in the growth of data volume, legacy storage architectures were beginning to crumble.

Combining storage with compute is in many ways a return to the past, but this time serious brains have been wrapped around it. Before virtualization and before SANs, many companies ran physical servers with direct-attached storage systems, and they tailored these storage systems to meet the unique needs for whatever applications might have been running on the physical servers. The problem with this approach was it created numerous “islands” of storage and compute resources without a centralized coordinating mechanism. Virtualization solved this resource-sharing problem, but introduced its own problems previously described.

Hyperconverged infrastructure distributes the storage resource among the various nodes that comprise a cluster. Built using standard server chasses and hardware, hyperconverged infrastructure nodes and appliances are bound together via Ethernet and a powerful software layer. The software layer often includes what is termed as a virtual storage appliance (VSA) that runs on each cluster node. Each VSA communicates with all of the other VSAs in the cluster over an Ethernet link, thus forming a distributed file system across which VMs (VMs) are run.

If you reread that last paragraph, you’ll note that the network plays a critical supporting role in every hyperconverged solution on the market. However, few hyperconverged vendors treat the network as more
than a support infrastructure. Today, as organizations scale beyond single racks, overlooking the criticality of the network introduces serious scaling limitations. Later in this book, you’ll discover how HPE has solved this challenge through the introduction of the HPE Composable Fabric, a software-defined networking solution that eliminates scaling challenges in hyperconverged infrastructure (and other) scenarios.

The fact that hyperconverged systems leverage standard off-the-shelf hardware is critical. The power behind hyperconverged infrastructure lies in its ability to corral resources—RAM, compute, data storage, and networking—from hardware that doesn’t all have to be custom-engineered. This is the basis for hyperconverged infrastructure’s ability to scale granularly and the beginnings of cost reduction processes.

**Resources to Consolidate**

The basic combination of storage, servers, and networking is a good start, but once you look beyond the confines of this baseline definition, hyperconverged infrastructure begins to reveal its true power. The more hardware devices and software systems that can be collapsed into a hyperconverged solution, the easier it becomes to manage the solution and the less expensive it becomes to operate.
Here are some data center elements that can be integrated in a hyper-converged infrastructure.

**Deduplication Appliances**

In order to achieve the most storage capacity, deduplication technologies are common in today’s data center. Dedicated appliances are now available that handle complex and CPU-intensive deduplication tasks, ultimately reducing the amount of data that has to be housed on primary storage.

Deduplication services are also included with storage arrays in many cases. However, deduplication in both cases is not as comprehensive as it could be. As data moves around the organization, data is rehydrated into its original form and may or may not be reduced via deduplication as it moves between services.

**SSD Caches/All-Flash Arrays**

To address storage performance issues, companies increasingly deploy either solid-state disk (SSD)-based caching systems or full SSD/flash-based storage arrays. However, both solutions have the potential to increase complexity as well as cost. When server-side PCI-e SSD cards are deployed, there also has to be a third-party software layer that allows them to act as a cache, if that’s the desire. With all-flash arrays or flash-based stand-alone caching systems, administrators are asked to support new hardware in addition to everything else in the data center.

**Backup Software**

Data protection in the form of backup and recovery remains a critical service provided by IT and is one that’s often not meeting organizational needs. Recovery time objectives (RTO) and recovery point objectives (RPO)—both described in the deep-dive section, “The Ins and Outs of Backup and Recovery”—are both shrinking metrics upon which IT needs to improve.
Using traditional hardware and software solutions to meet this need has been increasingly challenging. As RPO and RTO needs get shorter, costs get higher with traditional solutions.

With the right hyperconverged infrastructure solution, the picture changes a bit. In fact, some baseline solutions include comprehensive backup and recovery capability that can enable extremely short RTO windows, enabling very small RPO metrics—both very good characteristics!

**Data Replication**

Data protection is about far more than just backup and recovery. What happens if the primary data center is lost? This is where replication comes into play. By making copies of data and replicating that data to remote sites, companies can rest assured that critical data won’t be lost.

To enable these data replication services in traditional scenarios, companies implement a variety of other data center services. For example, to minimize replication impact on bandwidth, companies deploy WAN-acceleration devices intended to reduce the volume of data traversing the Internet to a secondary site. WAN accelerators are yet another device that needs to be managed, monitored, and maintained.
There are acquisition costs to procure these devices; there are operation costs in the form of staff time and training; and there are annual maintenance costs to make sure that these devices remain supported by the vendor.

**Up Next**

With an understanding of hyperconverged infrastructure and knowledge about many of the resources that can be consolidated into such solutions, let’s move on to discuss some specific data center architectural elements and options that comprise a hyperconverged environment.
Architecting the Hyperconverged Data Center

Data centers are dynamic, complex, and sometimes even chaotic. As business needs evolve, so does the data center, with IT staff working hard to ensure that the operating environment is sufficiently robust. Today, the term “data center” is coming to mean something completely new, too, as organizations look for ways to comingle public cloud and on-premises environments to operate their mission-critical workloads.

Hyperconverged infrastructure starts to change the mechanics behind how these efforts are carried out. With regard to hyperconvergence, there are a number of architectural elements that must be considered in order to determine the best path forward. But always remember: One of the primary goals of hyperconvergence is to simplify data center and hybrid cloud infrastructure.

You don’t need to worry about buying all kinds of different hardware, because with hyperconvergence the traditional silos of compute and storage resources have been merged into a single hyperconverged appliance. Moreover, the more sophisticated hyperconverged infrastructure solutions converge far more than just servers and storage. These appliances can also include your entire backup-and-recovery process, your deduplication and WAN acceleration appliances, and much more. Your architectural decisions can revolve around higher-order items, such as those described in the following sections.
Decision 1: Server Support

Not all hyperconverged solutions ship in the same kind of packaging. For example, there are appliance-based hyperconverged solutions from companies such as HPE, Nutanix, Scale Computing, and NetApp. And then there are software-only solutions that you install yourself.

With an appliance-based solution, you’re buying the full package, and you just need to plug everything in and turn it on. These are really easy to get going since most things are already done for you. Even better, when you combine your hyperconverged solution with a software-defined networking component, such as HPE Composable Infrastructure, things get even more plug-and-play since the network can self-configure based on the kind of network traffic that it sees.

Perhaps the biggest downside to an appliance-based solution is that you generally have to live with whatever constraints the vendor has placed on you. You need to remain within its hardware specifications. That said, today, there’s generally more than sufficient configurability so that this is mostly a non-issue.

Decision 2: The Storage Layer

Let’s face facts. One of the main reasons people are dissatisfied with their data centers is because their storage solution has failed to keep pace with the needs of the business. It’s either too slow to support mission-critical applications or it doesn’t have data-efficiency features (deduplication and compression), thus forcing the company to buy terabyte after terabyte of new capacity. Or, the company is falling victim to a data tsunami and can’t keep up with the old ways of adding storage all the time.

Many storage devices aren’t well-designed when it comes to supporting virtualized workloads, either. Traditional SANs are challenged when attempting to support the wide array of I/O types that are inherent in heavily virtualized environments. At the same time, storage has
become more complex, often requiring specialized skill sets to keep things running. For some systems, it’s not easy to do the basics, which can include managing LUNs, RAID groups, aggregates, and more. Some storage solutions also impose complex storage requirements, which can further muddy the infrastructure waters.

As companies grow and become more dependent on IT, they also start to have more reliance on data-mobility services. Legacy storage systems don’t always do a great job enabling data mobility and often don’t even support services like remote replication and cloning or, if they do, it’s a paid upgrade service. Without good local and remote cloning and replication capabilities, ancillary needs like data protection take on new challenges, too.

None of these situations are sustainable for the long term, but companies have spent inordinate sums of cash dragging inadequate storage devices into the future.

Hyperconverged infrastructure aims to solve this storage challenge once and for all. At the most basic level, hyperconverged infrastructure unifies the compute and storage layers and effectively eliminates the need for a monolithic storage array and SAN.

How does the storage component actually work if there’s no more SAN? Let’s unveil the storage secrets you’ve been dying to know!

**Software-Defined Storage Defined**

Abstract. Pool. Automate. That’s the mantra by which the software-defined movement attains its success. Consider the traditional SAN. It can be a huge and expensive device. Software-defined storage (SDS) works in a vastly different way. With SDS, storage resources are abstracted from the underlying hardware. In essence, physical storage resources are logically separated from the system via a software layer.

Hyperconverged infrastructure systems operate by returning to an IT environment that leverages direct-attached storage running on
standard server hardware, but many solutions go far beyond this baseline. In these baseline systems, there are a multitude of hard drives and SSDs installed in each of the x86-based server nodes that comprise the environment.

Installed on each of these nodes is the traditional hypervisor, along with software to create a shared resource pool of compute and storage. Increasingly, hyperconverged vendors are either eliminating disks from their product lineup and moving to flash-only configurations, or they’re adding all-flash variations to their existing product portfolios.

What’s more is that there are vendors who collapse data protection, cloud gateway technologies, and services such as deduplication, compression, and WAN optimization into their solutions. In essence, hyperconverged infrastructure leverages the concepts behind SDS systems in order to modernize and simplify the data center environment.

With storage hardware fully abstracted into software, it becomes possible to bring policy-based management and APIs to bear in ways that focus efforts on management on the VM rather than the LUN. The VM is really the administrative target of interest, whereas a LUN is just a supporting element that contributes to how the VM functions. By moving administration up to the VM level, policies can be applied more evenly across the infrastructure.

**To VSA or Not to VSA?**

Much has been written about why virtual storage appliances, or VSAs, (which run in user space) are terrible, why VSAs are awesome, why hypervisor-converged (kernel space) storage management is terrible, and why hypervisor-converged storage management is awesome. In short, should storage-management services run in user space (VSA) or kernel space (kernel-integrated)?
Defining VSA and Kernel-Integrated Management

Before examining the facts behind these opinions, let’s take a minute to make sure you understand what constitutes a VSA versus a kernel-integrated storage management system. Bear in mind that both VSAs and kernel-integrated management systems are part of the SDS family of storage systems in which storage resides in the server, not on SANs or separate arrays—at least in general.

A VSA is a VM that runs on a host computer. This VM’s purpose is to manage the storage that is local to that host. The VSAs on individual hosts work together to create a shared storage pool and global namespace. This storage is then presented back to the virtual hosts and used to support VMs in the environment. HPE’s SimpliVity platform is among a number of offerings from various companies that use a VSA to support the storage element of the solution.

Figure 2–1 provides a conceptual look at how VSAs operate. The key point here is to understand that the VSA is a VM just like any other.

Most hyperconverged systems on the market use this VSA method for handling storage abstraction.

Figure 2-1: This is the general architecture that includes a VSA
However, kernel-integrated storage is another method you should understand. Referred to as either kernel-integrated storage management or hypervisor-converged storage, this non-VSA storage management method operates through the implementation of a kernel-based module that resides in the hypervisor. In other words, instead of a VM handling local storage management, this hypervisor kernel handles the job. The most well-known kernel-integrated hyperconverged infrastructure solutions is VMware VSAN, which uses an operating system driver to handle storage needs.

There are other significant players in this space as well, such as Microsoft with Storage Spaces Direct (S2D). This feature is built right into the Windows Server Datacenter edition. Users can either build their own architecture and manage it or they can partner with a vendor such as HPE if they prefer to have a fully supported S2D experience. Regardless of how it’s supported, S2D is a kernel-driven service that requires Windows at the core.

Choosing a Method

So, which method is better? Let’s take a look at both options and how they align with needs around hyperconverged infrastructure.

First, recall the discussion around hypervisor choice. If you don’t need multi-hypervisor support, then either a VSA or a kernel-integrated kernel module will work equally well. Remember that multi-hypervisor choice is often not a major requirement as long as the intended solution supports the hypervisor you want to use, or plan to use in the future.

As soon as you introduce a need for multi-hypervisor support, your only choice is to work with a VSA. Because a VSA is just another VM running on the host, that VSA can be transitioned to run on any other hypervisor. When it comes to portability, VSA is king. There are far more VSA-based hyperconverged infrastructure solutions available on the market than non-VSA ones.
Hypervisor-integrated systems will lock you into the hypervisor to which the kernel module is tied. For some, that’s a big downside. For others, it’s not a problem since they don’t have any plans or desire to move to a different hypervisor.

All this said, let’s talk reality. VMware has spent years tuning the general hypervisor for performance and has told its customers that it’s more than sufficient for running even their most performance-sensitive applications, including monster databases on Oracle and SQL Server, Exchange, SAP and SAP HANA. It boils down to this: If it’s good enough for those kinds of really I/O-heavy applications, why can’t it support storage and hyperconvergence?

Proponents for VSA-based systems say they are designed from the ground up to support storage and hyperconverged infrastructure running a variety of workloads and applications. In fact, some of these appliances are certified to support Microsoft and high-impact SAP apps, without being tied to a single hypervisor. That kind of flexibility can’t be overstated.

It’s hard to say that one solution is “better” than the other. Instead, they’re just different ways to achieve the same goal, which is to abstract storage, pool it, and present it back to the hypervisor as a single shared resource pool. The choice really comes down to other goals you may have for your environment.

The Role of Custom Hardware in a Commodity Infrastructure

The first S in SDS stands for software. SDS is very much a software-driven storage architecture. However, this doesn’t mean that custom hardware has no place in the solution. For software-defined purists, having any custom or proprietary hardware anywhere in the software-defined data center might be considered blasphemous. However, don’t forget that we live in a world where not all is black and white. Shades of gray permeate everything we do.
The purists are right to a point. Proprietary hardware that doesn’t serve a strategic purpose doesn’t belong in a software-defined data center. However, when proprietary hardware provides a value-add that significantly differentiates a solution, it’s worth a hard look. The vendor isn’t creating that proprietary hardware for no reason.

For example, HPE includes a proprietary hardware card, called an accelerator card, in one of its hyperconverged models to handle much of the heavy lifting when it comes to complex storage operations.

In the modern data center, some storage truths must be observed. The first is that latency is **enemy No. 1**. The more latency that’s introduced into the equation, the slower that workloads will operate. HPE SimpliVity’s accelerator card is inserted into a commodity server and uses custom-engineered chips to provide ultra-fast write caching services that don’t rely on commodity CPUs. Moreover, the accelerator card enables comprehensive data reduction technologies (deduplication and compression) to take place in real time with no performance penalty in order to massively reduce the total amount of data that has to be stored to disk and the I/O that it takes to carry out operations.

Of course, it wouldn’t be a complete modern solution if this card was an absolute requirement. To that end, HPE also makes available SimpliVity node options in which the heavy lifting around deduplication and compression are wholly handled by increasingly powerful commodity CPUs. Modern CPUs have incredible horsepower, some of which can be sliced away and used to improve overall data efficiency. HPE’s software-optimized stack (read: no physical accelerator card) allows more adaptation of HPE server platforms from high performance computing to edge computing to match customer’s use cases.

Regardless of which way you go, remember this: Even when there’s some custom hardware, “software-defined” has nothing to do with hardware. “Software-defined” is about abstraction from the underlying hardware, thereby allowing software to present all services to applications.
Decision 3: Data Protection Services

Data protection shouldn’t be considered an afterthought in your data center. It should be considered a core service that’s central to how IT operates. RTOs and RPOs should be a key discussion point as you’re considering hyperconverged infrastructure solutions. Bear in mind that not all hyperconverged products come with the same levels of data protection.

Decision 4: The Management Layer

The data center has become an ugly place when it comes to management. There are separate administrative consoles for everything in the environment. The result is that administrators have no consistency in their work and are burdened with inefficiencies. To simplify management in the data center, admins need as few interfaces as possible. Here are the most common options that you need to be aware of when considering a hyperconverged virtual infrastructure:

Virtualization Layer Management

For those using VMware vSphere, vCenter is already in place.

Organizations using Microsoft Hyper-V likely use System Center Virtual Machine Manager (SCVMM).

Dot Your RPOs and Your RTOs

We haven’t ignored how important RTOs and RPOs are in this book. In fact, we have a whole chapter on data protection! To learn everything you’ve ever wanted to know about data protection as it relates to hyperconverged infrastructure, head on over to Chapter 5.
Orchestration and Automation Layer Management

Once the hyperconverged infrastructure is running, common tasks must be automated to gain efficiencies. Common orchestration and automation tools are:

- **VMware vRealize Automation (vRA).** Provides automated provisioning through a service catalog. With the ability to deploy across multi-vendor cloud and virtual infrastructures, vRA allows you to provide applications to the business as needed.

- **HPE OneView.** HPE OneView is an integrated management platform that brings together compute, storage, networking, and the public cloud into a singly managed hybrid cloud platform. In a hyperconverged scenario, OneView provides a management and orchestration layer that includes a complete API for automation.

- **Containers.** Containers have become a key player in the infrastructure space as have software management and orchestration layers, including the massively popular Kubernetes. Containers run atop a virtualized environment allow for increased workload flexibility, just like traditional applications.

Vendor-Supplied Management

Many hyperconvergence solutions provide you with a whole new management interface for your virtual infrastructure. With most hyperconverged solutions running vSphere today, this idea of creating a whole new management tool for the virtual infrastructure disregards that fact that you already have one—VMware vCenter.

REST APIs

A Relative State Transition Application Programming Interface (REST API) provides you with the entry point required to integrate multiple management points and automate your data center.
You should ensure that the hyperconvergence solution you choose offers compatibility with the virtualization management, automation, orchestration, and API tools discussed here. Also, ensure that your hyperconvergence solution does whatever is possible to reduce the number of management points and tools that are required for administration and troubleshooting.

**Decision 5: The Network**

As was mentioned earlier in this book, the network has become a more important consideration than it was in the past. Today, your hyperconverged infrastructure platform choice needs to include an evaluation of what you need in terms of networking. If you’re a smaller environment, a run-of-the-mill 10Gb Ethernet network may be just fine. But, as you scale, you need to seriously consider software-defined options, such as HPE Composable Fabric. See Chapter 3 for more information about software-defined networking and how it intersects with hyperconvergence.

With virtualization forming the core for hyperconverged infrastructure solutions, the question naturally turns to one of hypervisor choice. If there’s one thing IT administrators try to avoid, it’s a lack of choice.

**Hypervisor Support**

By its very nature, hyperconverged infrastructure requires using some kind of hypervisor. The hypervisor has become the standard layer on which most new business applications are deployed. Although there are still services deployed on bare metal servers, they’re becoming far less common as virtualization assimilates more and bigger workloads and as Kubernetes-powered containerized applications hit the scene.
Organizations demand choice, and this is also true when considering the server virtualization component of the data center.

Just keep in mind a few key facts when choosing hypervisor support:

- First, although variety in choice is highly desired, it’s not always required for individual hyperconverged infrastructure solutions. There are options on the market today that each support vSphere, KVM, and Hyper-V. If you absolutely demand to be able to use a particular hypervisor, there is likely a solution waiting for you. However, not every hyperconvergence vendor supports every hypervisor.

- Second, for the hyperconverged infrastructure vendors that do support multiple hypervisors, the customer (that’s you!) gets to decide which hypervisor to run on that platform.

In terms of popularity, it’s pretty common knowledge that the most popular hypervisor on the market today is VMware’s vSphere. With a formidable command of the hypervisor market, vSphere is offered as a primary hypervisor choice on a number of hyperconverged platforms.

Therefore, your decision concerning hypervisor support is really simple: For which hypervisor do you require support?

Up Next

Overall data center architecture includes a number of critical decision points, as described in this chapter. You were briefly introduced to one decision point: hardware acceleration. In the context of hyperconvergence, acceleration has to do with storage capacity and performance—efficiency. There is a third critical resource that was briefly mentioned in this chapter but that deserves more attention and, so, it gets a chapter all to itself. Chapter 3 delves deep into the world of software-defined networking.
Exploring the Intersection of Software-Defined Networking and Hyperconverged Infrastructure

In considering the history of hyperconverged infrastructure, it becomes clear that the foundations of the technology focus squarely on the storage and compute portions of the data center triad, leaving the networking leg as nothing more than a supporting element. The result has been a series of hyperconverged infrastructure deployments that may operate atop networks that were never really designed with the unique needs of hyperconvergence in mind.

How Hyperconvergence Leverages the Network

Much more than other storage technologies, hyperconvergence relies on the network as a fundamental part of its capabilities. Consider this: in any storage system that uses multiple copies of data as a part of the overall data protection scheme, data has to be written to two or more locations. When the storage system is self-contained, as is the case with more traditional SAN and NAS devices, these write operations can take place, sometimes, within the confines of a single chassis or across a dedicated storage fabric.

In contrast, most hyperconverged infrastructure solutions rely on simple Ethernet as the glue that binds the nodes to one another. And, as a part of the data protection algorithm in these solutions, there has
to be the ability for the cluster of nodes to withstand the loss of any one node. As such, with every write operation comes a need to write data to multiple nodes, each separated by an Ethernet link.

The Result of Network-Centric Data Protection

Early iterations of hyperconverged infrastructure didn’t enable the kinds of scaling opportunities we see from modern products. They were local affairs, keeping traffic within the confines of a single rack, with no need for storage traffic to traverse top-of-rack switches to other racks. Of course, this was severely limiting; so, over time, hyper-convergence vendors worked hard to improve the scaling capabilities of their products.

Traditional networking topologies introduce some significant challenges in terms of hyperconvergence. To start with, distributed hyperconverged infrastructure storage systems are inherently latency-sensitive. This is especially true when considering intra-cluster metadata, such as heartbeat and state change traffic. Anything that introduces additional latency impacts the overall performance and reliability of the entire system.

Why?

Let’s take a step back and look at hyperconvergence from the 100,000-foot view. What is it, really? At its core, hyperconverged infrastructure features a software-defined storage element. Software-defined storage systems typically have the ability to be highly distributed, just like a lot of other kinds of workloads that exist in today’s enterprise IT market. Think of file-systems such as Hadoop, vSAN or high-performance computing environments. All these designs rely on a software-defined data management layer and require infrastructures capable of supporting a lot of nodes, with minimal latency between them.
Latency Origination Points

Software defined storage is somewhat unique, though. There are several opportunities to introduce latency into a distributed storage service. There are three specific primary latency triggers that contribute to the total latency experienced by storage traffic in a distributed software-defined storage system.

The first contributor is network congestion. As more and more traffic traverses a given network link, the network experiences an increased level of congestion. At some point, this congestion slows down all network traffic and latency increases, which, for any storage traffic operating on that network, means that storage operations will suffer. Of course, this outcome isn’t specific to storage alone, but high storage latency can quickly impact users.

Another type of latency that can impact distributed storage solutions is hop latency, which is the latency introduced during packet and traffic processing on networking devices. The more devices there are between nodes, increased hop latency may be experienced.

And, finally, we have the primary contributor to latency in a network-centric storage stack: the storage protocol stack itself. Whenever storage traffic has to be moved across a network, there are various points at which data has to be encapsulated on the sending host and then de-encapsulated on the receiving host. For IP-based Ethernet networks, storage traffic has to first be placed inside an IP packet, which is then itself encapsulated into an Ethernet frame.

A newer approach to moving large amount of data across Ethernet with low latency is RDMA over Converged Ethernet (RoCE) in which remote direct memory access (RDMA) over an Ethernet network is enabled. While emerging standards like RoCE promises to reduce server-to-server latency by streamlining the protocol stack, this approach is still in early stages of adoption.
TCP-offload engines have also attempted to accelerate the processing time in the host protocol stack. While such approaches help accelerate these processes, they add cost. In the end, host-to-host traffic still needs to undergo this transformation to be sent across the network. This adds latency to the overall storage equation.

**Traditional Network Designs and Hyperconvergence**

All networks have inherent scaling limitations. Both traditional three tier and leaf-and-spine networking topologies rely on one or more layers of routers to overcome this challenge. In addition, most traditional networks were designed primarily to deliver connectivity, not performance. To keep cost under control, cross-network bandwidth typically received minimal attention. As a result, these kinds of fabrics hit a wall at some point where lots of network lanes are reduced to just a few. This often happens where top-of-rack switches are uplinked to other switches. It is not uncommon to see whole racks of 30 to 40 servers sharing only a few uplinks to the data center fabric at large. Blocking ratio of 10:1 is all too common. Such designed-in bottlenecks hurts and effectively discourages rack-to-rack traffic. While it’s possible to build non-blocking architectures, it gets expensive and can be complex.

![Figure 3-1: Traditional leaf-and-spine fabric](image-url)
While these types of architectures and hyperconvergence aren’t directly related to the network, a hyperconvergence/software-defined storage system looks just like any other workload. At some point, an unsuitable network design will catch up to it and it will become a limiting factor in terms of continued expansion of the storage cluster.

In essence, hyperconverged solutions are exposing the data center network to new traffic patterns and cross-rack bandwidth demands which forces re-thinking of network design. In fact, many of today’s workloads benefit from a new approach to the top-of-rack switches – where hyperconverged servers are connecting as part of an overall multi-rack system strategy. Ideally the top-of-rack switches would form their own intelligent cross-rack system backplane. There needs to be a new network strategy that works for all workloads, including these server-to-server workloads, a design that supports the overall fabric.

Enter Software-Defined Networking

Software-defined networking (SDN) isn’t a new technology, but it is constantly and quickly evolving. And, based on some of the articles that have been written about it, you’d be forgiven if you were under the impression that this technology has magical properties that imbue your network with fairy dust!

What, exactly, is SDN? Like so many other technologies that used to rely solely on hardware, networking has made the jump into software. In essence, with an SDN infrastructure, what used to be fused control planes and data planes are torn asunder and kept separate.

With traditional networking devices, both the brains and the brawn exist on the same device. The brain is the control plane, while the brawn – the ability to process networking traffic and pass it along to the next device that the brain directs it to – is the data plane.
There are a couple of problems inherent in this structure:

- **Visibility.** The brains are limited in terms of insight. They can see only what’s on their local device, and what certain protocols, such as spanning tree, provide to them. They don’t have a comprehensive view of the network.

- **Coordination.** With so many brains across so many devices, there isn’t a central authority. Sure, there are tools that can act as a central authority, but they’re often bolt-ons that don’t always enable a true real-time view of the network.

As more workloads, in terms of both quantity and diversity, hit the network, the rigidity of traditional networking structures has begun to show its weaknesses more clearly. As workloads continued to become more variable, it’s clear that the network was having issues keeping up, even with the Herculean efforts of highly skilled administrators tending to it.

**It’s Not Just Software: It’s a Reimagining of the Network**

At this point, you might be thinking, “There is still just physical Ethernet under all of this. How does software-defined networking actually make things better?”

Don’t fall into the trap of thinking that SDN is the beginning and the end of solving your networking challenges. In reality, the move to an SDN infrastructure should be seen as an opportunity to fundamentally transform how your infrastructure operates. And it’s not just a matter of installing new code on a few switches: you’ll need to rethink everything, from the cabling plant to the hardware.

The end result will be a fabric with an overarching view of the network and of the workloads operating on that network. The brains, formerly distributed to lots of switches with little external visibility, are now centralized, with a master view of everything. The brawn is still...
distributed. The centralized controller tells individual devices what should happen with traffic based on the brain’s detailed understanding of what’s happening across the network.

In essence, one of the things that SDN brings to the table is deep insight into the entire environment, allowing the automation of traffic decisions that takes everything into consideration. Better yet, this can happen more quickly than would be possible under the old model.

The traditional layered approach to networking results in bottlenecks that can be difficult to manage around. It’s the network reimagined.

The Cabling Plant

Cabling is rarely seen as strategic. But, with the deployment of SDN, it’s time for data center architects to rethink the role that cabling plays.

Let’s start with the basics. Under traditional networking environments, top-of-rack switches were cabled to uplink switches. Every server in the rack connects to the top-of-rack switch, which then typically has just a few ports connected to the next-higher switch in the pyramid. This creates bottlenecks when a lot of traffic has to exit the rack.

SDN changes the game, as you’ll learn shortly.
Scaling in the Software Defined Networking World

Traditional meshed topologies are not new. But they have historically been limited in scale. It is easy to see how: if, for example, a given top-of-rack switch has 8 fabric ports by which to connect out of the rack, a fully connected mesh will be limited to \( 8 + 1 \) switches. If we further set that each switch has 48 ports, the maximum fabric size possible with this particular switch is \( 9 \times 48 = 432 \) network ports.

For smaller data centers, 400+ ports may be enough. However, for larger data center fabrics, we need to scale larger. Again, this is where a software driven approach to networking unlocks new capabilities. With a software-defined solution such as the HPE Composable Fabric, it’s possible to build an \( n \) dimensional mesh that enables tremendous scalability. If we again use the 8-fabric port switch, we can now use the 8 ports to build a two-dimensional fabric. Here 4 ports are used in a horizontal dimension and 4 ports are used in a vertical dimension. Think of the network topology as a kind of chess board with \( 4 + 1 \) switches in each direction for a total of 25 switches and \( 25 \times 48 = 1,200 \) ports. We now have retained to any-any properties of a meshed fabric yet crated a fabric that is 170% larger than before.

Continuing with the 8-fabric port example. The largest \( n \)-dimensional fabric with 8 fabric ports per switch is a fabric in 4 dimensions: \( 3 \times 3 \times 3 \times 3 = 81 \) switches and \( 81 \times 48 = 3,888 \) ports. 9 times larger than the traditional single dimensional mesh.

Even larger fabrics can be build using switches with more fabric ports. With the HPE Composable Fabric, data center network scalability is determined by:

a. The number of fabric ports on each switch, and

b. The number of meshed dimensions selected.
Meshes Lead to Messes? Not with Software-Defined Networking

Imagine, if you will, a traditional environment. What happens when you try to use multiple links? Either you use some protocol that enables link aggregation, or you run into a mess from spanning tree protocol. Remember: Spanning Tree Protocol was developed as a way to prevent network loops from bringing down entire swaths of infrastructure courtesy of the unregulated network broadcast traffic that is generated by such loops.

Simply put, routing method drives network layout (topology). While the Spanning Tree Protocol works well in hierarchical networks, it completely undermines fully meshed topologies. Yet, a meshed network is exactly what we want when traffic flows from machine to machine. That’s where SDN comes in. With the right solution, a top-of-rack switch can be connected directly to other top-of-rack switches – forming a fully connected mesh, allowing everyone to talk to everyone at the same time. Furthermore, each top-of-rack switch can now contribute part of its ports and bandwidth to the resilience and overall throughput of the network. If a given path is disconnected, there are many path alternatives to route around the failing link.

Once a mesh has been created, the next step is to bring it under the auspices of a controller that can manage and monitor potentially thousands of nodes simultaneously. This controller needs to have the brains to dynamically identify the kinds of workloads operating on that mesh, and to automatically reconfigure nodes to provide the best possible support for those workloads. This all has to be automatic and real-time. If a human has to get involved, it won’t scale.

In terms of the network, the software-defined storage system is just another workload that operates on a cluster. The network controller needs to identify this workload so that it can automate configuration and segment traffic as needed.
Solving Latency

While SDN effectively pools the bandwidth available in each switch, the simple introduction of software doesn’t eliminate latency. There will still be congestion latency. There will still be hop latency. There will still be latency imposed by the storage stack.

But let’s put latency into some perspective in the context of HPE’s Composable Fabric technology. Congestion latency points to some kind of a bandwidth constraint. With a full mesh, that shouldn’t be a routine occurrence; since the fabric is controlling all switches as a single pool of resources. If the addition of new workloads creates a need for more bandwidth, you can add more switches to the mesh. The bandwidth of each additional switch adds to the total bandwidth budget of the overall fabric. Finally, if the node bandwidth is too low, you may elect to upgrade the speed of the top-of-rack switches. 25GbE is becoming more common on servers these days, with high-performance servers using 100GbE.

As with a traditional switch, there will still be some hop latency; the switches in an SDN scenario still need to process packets. But that processing time is minimal: with HPE’s Composable Fabric, hop latency can be as low as 0.5 microseconds.

And, SDN provides more pathways for your workloads, because as you add more ports to the mesh, you also add more potential pathways. Even if they have to traverse a bunch of switches, with each hop imposing additional latency of 0.5 microseconds per switch, it will take a lot of switches for hop latency to have a noticeable impact on total latency.

SDN and Hyperconverged Infrastructure

What does all of this SDN goodness have to do with hyperconverged infrastructure? First, as mentioned earlier in the chapter, keep in mind that hyperconvergence is highly network dependent since hyperconverged infrastructure workloads depends on unrestricted
server-to-server data flows. A poor network infrastructure will have noticeably negative outcomes. A well-designed network will have good outcomes, but a well-designed software-defined network can deliver fantastic outcomes.

HPE Composable Fabric provides an architecture that’s self-managing and can adapt as the underlying mix of workloads drives new demands. By watching the kinds of workloads that operate on the fabric and automatically tuning the network to prioritize, for example, latency sensitive workloads such as HPE SimpliVity cluster traffic, the network controller makes sure that the network is adjusted to support low latency and at the same time provide high bandwidth for high throughput workloads.

On the ongoing operational front, the intelligent networking fabric can also automate VLAN configuration after automatically identifying the workloads running on the network. This eases administration and ensures that human error is kept to a minimum.

The end result is a highly scalable environment that provides the performance necessary for even the most demanding workloads. Even as your workloads scale beyond the rack, a well-designed SDN underpinning will help ensure that your hyperconverged infrastructure traffic doesn’t suffer due to legacy constraints.

**Up Next**

Software defined networking has emerged as a critical player in hyperconvergence, as described in this chapter. While SDN needs to be a more engrained component of the modern data center, compute and storage are still often top of mind. Chapter 4 goes into some details around how you can address key pain points in these realms.
Addressing Data Center Pain Points

As much as IT pros hate to be told, “We have to do more with less,” it’s doubtful that this directive will die in the near future. The unfortunate truth is that IT has to continue to do more with either no increase or with decreases in overall resources. This comes at the same time that increasing attention is being paid to other technology-centric needs, including increasing security and undertaking digital transformation initiatives.

That means that organizations need to reconsider how they operate underlying infrastructure to make sure that it’s cost effective and can allow staff time to work on these other needs. In this chapter, you’ll learn about how hyperconverged infrastructure can be leveraged to help address these needs.

The Relationship Between Performance & VM Density

Return on investment. Total cost of ownership. These are phrases used to describe the economic impact of technology investments—or expenses—depending on your perspective. Regardless of the perspective, though, businesses want to squeeze as much return as possible out of their technology investments while spending as little as reasonably possible on those investments.

You might be wondering what this quick economic discussion has to do with workload performance in the data center. There’s actually a direct link between these two topics and it revolves around overall VM density.
VM density refers to the number of VMs that you can cram onto a single host. The more VMs that you can fit onto a host, the fewer hosts you need to buy. Obviously, fewer hosts means having to spend less money on hardware, but the potential savings go far beyond that measure.

When you have fewer hosts, you also spend less on licensing. For example, you don’t need to buy hypervisor licenses for hosts that don’t exist!

The savings don’t stop there. Fewer hosts means less electricity is needed to operate the data center environment. Fewer hosts means there’s less cooling needed in the data center environment. Fewer hosts means that you free up rack space in the data center environment.

However, these benefits cannot come at the expense of workload performance. When workloads perform poorly, they actively cost the company money, such as lost efficiency and customer dissatisfaction.

How do you maximize VM density without impacting workload performance? First of all, it’s a balance that you need to find, but when you’re initially specifying hardware for a new environment, you won’t necessarily know how your workloads will function in that new environment, so things can be tough to predict. Instead, you need to look at the inputs, or the resources atop which the new environment is built. Storage is one of these key resources.

**Storage Performance in a Hyperconverged Infrastructure**

In a hyperconverged infrastructure environment, one of the primary resources that must be considered is storage, and not just from a capacity perspective. Remember that storage and compute are combined in hyperconvergence, so that becomes a factor that’s not present in more traditional environments. In a traditional environment, 100 percent of the available CPU and memory resources are dedicated to serving the needs of running VMs. In a hyperconverged infrastructure environment,
some of those resources must be diverted to support the needs of the storage management function, usually in the form of a VSA. This is one of the core trade-offs to consider when adopting a hyperconverged infrastructure.

**Data Deduplication Explained**

Consider this scenario: Your organization is running a virtual desktop environment with hundreds of identical workstations all stored on an expensive storage array purchased specifically to support this initiative. That means you’re running hundreds of copies of Windows, Office, ERP software, and any other tools that users require.

Let’s say that each workstation image consumes 25GB of disk space. With just 200 such workstations, these images alone would consume 5TB of capacity.

With deduplication, you can store just one copy of these individual VMs and then allow the storage array to place pointers to the rest. Each time the deduplication engine comes across a piece of data that’s already stored somewhere in the environment, rather than write that full copy of data all over again, the system instead saves a small pointer in the data copy’s place, thus freeing up the blocks that would’ve otherwise been occupied.

In the figure “Deduplication vs. No Deduplication,” the graphic on the left shows what happens without deduplication. The graphic on the right shows deduplication in action. In this example, there are four copies of the blue block and two copies of the green block stored on this array. Deduplication enables just one block to be written for each block, thus freeing up those other four blocks.

Now, let’s expand this example to a real-world environment. Imagine the deduplication possibilities present in a VDI scenario: With hundreds of
identical or close-to-identical desktop images, deduplication has the potential to significantly reduce the capacity needed to store all of those VMs.

Deduplication works by creating a data fingerprint for each object that’s written to the storage array. As new data is written to the array, additional data copies beyond the first are saved as tiny pointers. If a completely new data item is written—one that the array hasn’t seen before—the full copy of the data is stored.

Different vendors handle deduplication in different ways. In fact, there are two primary deduplication techniques that deserve discussion: inline deduplication and post-process deduplication.

**Inline Deduplication**

Inline deduplication takes place at the moment in which data is written to the storage device. While the data is in transit, the deduplication engine fingerprints the data on the fly. As you might expect, this deduplication process does create some overhead.

First, the system has to constantly fingerprint incoming data and then quickly identify whether that new fingerprint already matches something in the system. If it does, a pointer to the existing fingerprint is written. If it does not, the block is saved as is. This process introduces the need to have processors that can keep up with what might be a tremendous workload. Further, there’s the possibility that latency could be introduced into the storage I/O stream due to this process.

<table>
<thead>
<tr>
<th>Deduplication vs. No Deduplication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DATA ELEMENTS</strong></td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Data</td>
</tr>
</tbody>
</table>

Without Deduplication               With Deduplication
A few years ago, this might have been a showstopper since some storage controllers may not have been able to keep up with the workload need. Today, though, processors have evolved far beyond what they were just a few years ago. These kinds of workloads don’t have the same negative performance impact that they might’ve once had. In fact, inline deduplication is a cornerstone feature for most of the new storage devices released in the past few years and, while it may introduce some overhead, it often provides far more benefits than costs. With a hardware-accelerated or software-optimized hyperconverged infrastructure, inline deduplication is not only the norm, it’s a key cornerstone for the value that’s derived from the infrastructure.

**Post-Process Deduplication**

As mentioned, inline deduplication imposes the potential for some processing overhead and potential latency. The problem with some deduplication engines is that they have to run constantly, which means that the system needs to be adequately configured with constant deduplication in mind. Making matters worse, it can be difficult to predict exactly how much processing power will be needed to achieve the deduplication goal. As such, it’s not always possible to perfectly plan overhead requirements.

This is where post-process deduplication comes into play. Whereas inline deduplication processes deduplication entries as the data flows through the storage controllers, post-process deduplication happens on a regular schedule, perhaps overnight. With post-process deduplication, all data is written in its full form—copies and all—on that regular schedule. The system then fingerprints all new data and removes multiple copies, replacing them with pointers to the original copy of the data.

Post-process deduplication enables organizations to utilize this data reduction service without having to worry about the constant processing overhead involved with inline deduplication. This process can take a significant amount of time and overhead, especially if you have large amounts of data, which is why many organizations schedule dedupe (deduplication) to take place during off hours.
The biggest downside to post-process deduplication is the fact that all data is stored fully hydrated—a technical term that means that the data hasn’t been deduplicated—and, as such, requires all of the space that non-deduplicated data needs. It’s only after the scheduled process that the data is shrunk. For those using post-process dedupe, bear in mind that, at least temporarily, you’ll need to plan on having extra capacity. There are a number of hyperconverged infrastructure systems that use post-process deduplication while others don’t do deduplication at all. Lack of full inline deduplication increases costs and reduces efficiency.

**Hardware Acceleration and Software Optimization to the Rescue**

Hardware-accelerated and software-optimized hyperconverged infrastructure solutions completely solve the overhead challenges inherent in those systems. All deduplication tasks are delegated to the accelerator card or the software-defined accelerator, thereby negating the need for the system to consume processor resources that are also needed by the VMs.

**Tiering and Deduplication**

In order to match storage performance needs with storage solutions, many companies turn to what are known as tiered storage solutions. They run, for example, hard disk-based arrays for archival data and they run flash systems for performance needs and they manage these resources separately. This also means that deduplication is handled separately per tier. Each time dedupe is duplicated, there are additional CPU resources that must be brought to bear and there are multiple copies of deduplicated data. Neither is efficient. Hyperconverged systems that include comprehensive inline deduplication services carry with them incredibly efficient outcomes.
This is where hardware acceleration can be a boon when it’s selected. Most hyperconverged infrastructure systems rely on the commodity hardware to carry out all functions. With a system that uses hardware acceleration, more Intel CPU horsepower can be directed at running VMs while the acceleration hardware handles processor-intensive data reduction operations, such as deduplication and compression.

Don’t underestimate the benefits of data reduction! These services have far more impact on the environment than might be obvious at first glance and the benefits go far beyond simple capacity gains, although capacity efficiency is important.

There are several metrics that benefit when dedicated and specialized hardware is brought to bear.

Capacity

“Data Deduplication Explained” discusses generalized capacity benefits of deduplication, but let’s now consider this in the world of hyperconverged infrastructure. In order to do this, you need to consider your organization’s holistic data needs:

- **Primary storage.** This is the storage that’s user- or application-facing. It’s where your users store their stuff, where email servers store your messages, and where your ERP’s database is housed. It’s the lifeblood for your day-to-day business operations.

- **Backup.** An important pillar of the storage environment revolves around storage needs related to backup. As the primary storage environment grows, more storage has to be added to the backup environment, too.

- **Disaster recovery.** For companies that have disaster recovery systems in place in which data is replicated to secondary data centers, there’s continued need to grow disaster recovery-focused storage systems.
When people think about storage, they often focus just on primary storage, especially as users and applications demand more capacity. But when you look at the storage environment from the top down, storage growth happens across all of these storage tiers, not just the primary storage environment. In fact, these secondary storage needs are growing faster than any other segment.

In other words, your capacity needs are growing far faster than it might appear. Hardware acceleration, when applied to all of the storage domains in aggregate, can have a tremendous impact on capacity. By treating all of these individual domains as one, and deduplicating across all of them, you can achieve pretty big capacity savings.

But deduplication, as mentioned before, can be CPU-intensive. By leveraging hardware acceleration, you can deduplicate all of this without taking CPU resources away from running workloads. By infusing the entire storage environment with global deduplication capabilities via hardware or software-optimized acceleration, you can get capacity benefits that were only the stuff of dreams just a few years ago. Hyperconvergence with great deduplication technology can attain great results while also simplifying the overall management needs in the data center.

**IOPS**

Imagine a world in which you don’t actually have to write 75 percent of the data that’s injected into a system. Very often, we see solutions screaming “one million IOPS!” when they should be screaming “we get stuff done!”

What does this mean? IOPS shouldn’t be the sole direct measure of performance. More doesn’t mean better. IOPS is a reflection of how hard your system is working. If you can make your system do more with less, then you don’t need crazy IOPS metrics to begin with. You get the job done more efficiently, without impacting performance of your workloads/applications.
That world becomes possible when acceleration is used so that all workloads benefit from inline deduplication, not just some workloads.

The more that data can be deduplicated, the fewer write operations that have to take place. For example, a deduplication ratio of 5-to-1 means that there would only be one actual write-to-storage operation that takes place for every five attempted write operations.

Hardware and software-optimized acceleration allow this comprehensive data reduction process to take place in a way that doesn’t divert workload CPU resources. As a result, you continue to enjoy the IOPS benefits without having to give up workload density.

**Latency**

Latency is the enemy of data center performance. By offloading intensive tasks to a custom-developed component that specifically handles these kinds of tasks, latency can be reduced to a point where it doesn’t affect application performance.
Application Performance

At the end of the day, all that matters is application performance. That’s the primary need in the data center environment and, while it can be difficult to measure, you’ll know very quickly if you’ve failed to hit this metric. The phones will start to ring off the hook. Hardware and software-optimized acceleration help you to keep this metric in the green.

Linear Scalability

Businesses grow all the time. The data center has to grow along with it. Scaling “up” has been one of the primary accepted ways to grow, but it carries some risks. Remember, in the world of storage, scaling up occurs when you add additional capacity without also adding more CPU and networking capacity at the same time. The problem here is that

Scale-up Architecture Increases Burden on Shared Components and Single Points of Failure

With a reasonable number of disks to support, the storage processor and storage network uplinks operate well.

As additional disk shelves are added, the storage head/processor begins to assume yet more responsibility and additional burden is placed on the uplinks to the storage network.

Eventually, too many disk shelves are added and a shared component somewhere in the stack fails to keep up, slowing everything down or risking widespread failure.

Figure 4-1: A scale-up environment relies on shared components.
you run the risk of eventually overwhelming the shared resources that exist. **Figure 4–1** shows an example of a scale–up environment.

Scale–out has become a more popular option because it expands all resources at the same time. With hyperconverged infrastructure, the scaling method is referred to as linear scalability. Each node has all of the resources it needs—CPU, RAM, and storage—in order to stand alone. **Figure 4–2** gives you a look at this kind of scalability.

For solutions that use them, accelerators are a critical part of the scaling capabilities as they offload intensive functionality that can be workload–impacting. This increases density, but more importantly, by freeing up resources, it adds more predictability to the overall performance of applications, even while maintaining high levels of density.

**Up Next**

The items discussed in this chapter are critically important to ensuring that the data center adequately (maybe even excellently!) supports business needs, but these metrics are just the very tip of the iceberg.

Under the waterline are other requirements that can’t be ignored. In the next chapter, we’ll discuss one really important requirement that’s often quite challenging: data protection.
Even the smallest of small businesses today depend on their IT resources being available on a 24/7 basis. Even short periods of downtime can wreak havoc, impact the bottom line, and mean having to cancel going out to lunch. Maintaining an agreed-upon level of infrastructure availability is critically important. On top of that, outages or other events resulting in loss of data can be a death knell for the business. Many businesses that suffer major data loss fail to recover in the long-term and eventually make their way down the drain. Data protection is one of IT’s core services. Unfortunately, it’s also a hard service to provide at times, or at least, it was. There are now some hyperconverged infrastructure solutions that are uniquely positioned to solve, once and for all, the challenges across the entire data protection spectrum.

The Data Protection and Disaster Recovery Spectrum

Let’s talk a bit about data protection as a whole. When you really look at it, data protection is a spectrum of features and services. If you assume that data protection means “ensuring that data is available when it’s needed,” the spectrum also includes high availability for individual workloads. Figure 5-1 provides you with a look at this spectrum.
The Ins & Outs of Backup & Recovery

There are two primary metrics to consider when it comes to disaster recovery.

**Recovery Point Objective (RPO)**

If you’re using a nightly backup system, you’re implicitly adhering to a 24-hour RPO. You’re basically saying that losing up to 24 hours worth of data is acceptable to the business. RPO is the metric that defines how much data your organization is willing to lose in the event of a failure that has the potential to result in data loss. To reduce RPO, you need to back data up more often.

**Recovery Time Objective (RTO)**

RPO is critically important as it defines just how much data you’re willing to lose. Once you’ve suffered a data loss, the critical metric shifts. Now, you’re more interested in how long it takes you to recover from that failure. How long is your organization willing to be without data while you work to recover it from backup systems? This metric is often used to support such statements as, “For every minute we’re down, the company loses $X.”

The RTO is the formal name for this metric and is one that companies will go to great lengths to minimize. As is the case with RPO, the closer to zero that you attempt to get to RTO—that is, the less time that you’re willing to be down—the more it costs to support.

To achieve very low RTO values, companies will often implement multi-pronged solutions, such as disaster recovery sites, fault tolerant VMs, clustered systems, and more.
RAID

Yes, RAID is a part of your availability strategy, but it’s also a big part of your data protection strategy. IT pros have been using RAID for decades. For the most part, it has proven to be very reliable and has enabled companies to deploy servers without much fear of negative consequences in the event of a hard drive or two failing. Over the years, companies have changed their default RAID levels as the business needs have changed, but the fact is that RAID remains a key component in even the most modern arrays.

The RAID level you choose is really important, but you shouldn’t have to worry about it! The solution should do it for you. That said, don’t forget that it’s pretty well-known that today’s really large storage devices have made traditional RAID systems really tough to support. When drives fail in a traditional RAID array, it can take hours or even days to fully rebuild that drive. Don’t forget this as you read on; we’ll be back to this shortly.

RAID is also leveraged in some hyperconverged infrastructure systems; however, with these systems, administrators are shielded from some of the complexity and configuration options that they used to work with on stand-alone storage arrays. Bear in mind that one of the tenets of hyperconverged infrastructure is simplicity. As such, you don’t have to go through a lot of effort to manage RAID in a hyperconverged system. It’s simply leveraged behind the scenes by the system itself. In Figure 5–2, you get a look at how RAID protects data.
Replication/RAIN/Disaster Recovery

RAID means you can lose a drive and still continue to operate, but what happens if you happen to lose an entire node in a hyperconverged infrastructure cluster? That’s where replication jumps in to save the day. Many hyperconverged infrastructure solutions on the market leverage replication as a method for ensuring ongoing availability and data protection in the event that something takes down a node, such as a hardware failure or an administrator accidentally pulling the wrong power cord.

This is possible because replication means “making multiple copies of data and storing them on different nodes in the cluster.”

Therefore, if a node is wiped off the face of the earth, there are one or more copies of that data stored on other cluster nodes.

In some hyperconverged infrastructure solutions, like those shown in Figure 5-3, you can configure what’s known as the replication factor (RF). The replication factor is just a fancy way of telling the system how many copies of your data you’d like to have. For example, if you specify a Replication Factor of 3 (RF3), there will be three copies of your data created and stored across disparate nodes. You’ll sometimes see replication-based availability mechanisms referred to as RAIN, which stands for Redundant Arrays of Independent Nodes.
Besides helping you to make sure that your services remain available, replication goes way beyond just allowing you to withstand the loss of a node, too. When replication is taken beyond the data center to other sites, you suddenly gain disaster recovery capability, too. In fact, in some hyperconverged systems that leverage inline deduplication across primary and secondary storage tiers, that’s exactly what happens. After deduplication, data is replicated to other nodes and to other data centers, forming the basis for incredibly efficient availability and disaster recovery.

**How About Both: RAID and RAIN Combined**

Let’s go a little deeper into the RAID/RAIN discussion with an eye on hyperconverged infrastructure solutions that provide both. First, there are some downsides to just RAIN-based replication (Replication Factor 2 or RF2). There are solutions on the market that provide RF2. Systems based on RF2 will lose data if any two nodes or disks in a cluster fail, or if even just one node should fail while any other node is down for maintenance.

To make things a bit more resilient, you could bump up to RF3, but this replication factor then requires a minimum of five nodes at each site.
that uses RF3 and imposes an additional 50 percent penalty on capacity. With RF3, you can also start to think about using erasure coding, but this requires RF3 and carries with it a lot of CPU overhead due to the way that erasure coding works. This may not be suitable when trying to support high-performance applications.

How about combining RAID and RAIN into a single solution? Maybe you combine the use of local RAID 6 on individual nodes so that any node can tolerate double disk failures and keep VMs up and running. With each individual node very well protected, the likelihood of losing an entire node is reduced. From there, you apply RAIN so that, in the event that a complete node is lost, you can tolerate that, too. The strategic combination of RAID and RAIN enables tolerance against a broad set of failure scenarios.

**What Is Erasure Coding?**

Erasure coding is usually specified in an N+M format: 10+6, a common choice, means that data and erasure codes are spread over 16 (N+M) drives, and that any 10 of those can recover data. That means any six drives can fail. If the drives are on different appliances, the protection includes appliance failures, so six appliance boxes could go down without stopping operations.

Backup and Recovery

Despite your best efforts, there will probably come a day when you need to recover data lost from production. Data losses can happen for a variety of reasons:

- **Human error.** People make mistakes. Users accidentally delete files. Administrators accidentally delete VMs. IT pros can sometimes accidentally pull the wrong disk from a storage system or unplug the wrong server’s power cord.

- **Hardware failure.** When hardware fails, sometimes it fails spectacularly. In fact, hardware failure may not even be the result of failed IT hardware. You may end up in a situation, for example, in which the data center cooling systems fail and the server automatically shuts down as the temperature rises. This could be considered a server hardware failure because of the outcome (the server going down), when in fact the server is actually doing exactly what it’s supposed to do in this case.

- **Disasters.** Hurricanes, tornados, floods, a new “Terminator” movie. Disasters come in all kinds of forms and can result in data loss.

Disaster Recovery

Disaster recovery takes backup one step further than the basics. Whereas backup and recovery are terms that generally refer to backing up data and, when something happens, recovering that data, disaster recovery instead focuses on recovery beyond just the data.

Disaster recovery demands that you think about the eventual needs by starting at the end and working backward. For example, if your data center is hit by an errant meteor (and assuming that this meteor hasn’t also caused the extinction of the human race), recovering your data alone will be insufficient. You won’t have anything onto which to recover your data if your data center is obliterated.
Before we get too fatalistic, let’s understand what the word disaster really means in the context of the data center. It’s actually kind of an unfortunate term since it immediately brings to mind extinction-level events, but this is not always the case for disaster recovery.

There are really two kinds of disasters on which you need to focus:

- **Micro-level disasters.** These are the kinds of events that are relatively common, such as losing a server or portion of a data center. In general, you can quickly recover in the same data center and keep on processing. Often, recovery from these kinds of disasters can be achieved through backup and recovery tools. With that said, these events will probably still result in downtime.

The HPE SimpliVity Story on Protecting Production Data and Availability

Being a hyperconvergence platform, HPE SimpliVity first provides the compute and storage infrastructure for customers’ production applications. As data is ingested from the hypervisor, we stage the VM data into DRAM on the HPE SimpliVity Accelerator Card (or software-optimized accelerator) across two of our nodes within a single data center. With data now protected across multiple nodes, in addition to supercapacitor and flash storage protecting the DRAM on each HPE SimpliVity Accelerator Card, we acknowledge a successful write back to the VM and process the data for deduplication, compression and optimization to permanent storage on both nodes. Once this process is complete, every VM in an HPE SimpliVity data center can survive the loss of at least two disks in every node, in a data center, and the loss of a full hyperconverged node.
• **Macro-level disasters.** These are the kind of life-altering events that keep IT pros awake at night and include things like fires, acts of {insert deity here}, or rampaging hippos.

Recovery from these disasters will mean much more than just restoring data.

Thinking about the disaster recovery process with the end in mind requires that you think about what it would take to have everything back up and running—hardware, software, and data—before disaster strikes.

Yes, your existing backup and recovery tools probably play a big role in your disaster recovery plan, but that’s only the very beginning of the process.

Disaster recovery plans also need to include, at a bare minimum:

• **Alternate physical locations.** If your primary site is gone, you need to have other locations at which your people can work.

• **Secondary data centers.** In these locations, or in the cloud, you need to have data centers that can handle the designated workloads from the original site. This includes a space for the hardware, the hardware itself, and all of the software necessary to run the workloads.

---

**Business Continuity**

Since disaster recovery is kind of a loaded term, a lot of people prefer to think about the disaster recovery process as “business continuity” instead. However, that’s not all that accurate. Business continuity is about all the aspects to a business continuing after a disaster. For example, where are the tellers going to report after the fire? How are the phone lines going to be routed? Disaster recovery is an IT plan that’s a part of business continuity.
• **Ongoing replication.** In some way, the data from your primary site needs to make its way to your secondary site. This is a process that needs to happen as often as possible in order to achieve desirable RTOs and RPOs. In an ideal world, you would have systems in place that can replicate data in minutes after it has been handled in the primary data center. The right hyperconverged infrastructure solution can help you achieve these time goals.

• **Post-disaster recovery processes.** Getting a VM back up and running is just the very first step in a disaster recovery process. RTO is a measure of more than just the restoration of the VM. From there, processes need to kick off that include all the steps required to get the application and data available to the end user. These processes include IP address changes, DNS updates, re-establishment of communication paths between parts of an n-tier application stack and other non-infrastructure items.

**HPE SimpliVity’s Answer to Full-Spectrum Disaster Recovery**

HPE SimpliVity alone makes it simple for you to achieve the first part of disaster recovery, which is making sure that VMs are always available, even if a data center is lost.

Along with their 1-click SimpliVity RapidDR solution, HPE has focused on providing integration into other tools that can help automate and orchestrate all of the remaining steps of the disaster recovery process, including pre-built packages of HPE SimpliVity functionality within VMware’s vRealize Automation and Cisco’s UCS Director, and supporting partners in the development of tools on top of HPE SimpliVity APIs like VM2020’s EZ-DR.
Data Reduction in the World of Data Protection

We’re going to be talking a lot about data reduction—deduplication and compression—in this book. They’re a huge part of the hyperconverged infrastructure value proposition and, when done right, can help IT address problems far more comprehensively than when it’s done piecemeal.

When it comes to data protection, data reduction can be really important, especially if that data reduction survives across different time
periods—production, backup, and disaster recovery. If that data can stay reduced and deduplicated, some very cool possibilities emerge. The sidebar, The Data Virtualization Platform and Disaster Recovery highlights one such solution.

Fault Tolerance

Availability is very much a direct result of the kinds of fault tolerance features built into the infrastructure as a whole. Data center administrators have traditionally taken a lot of steps to achieve availability, with each step intended to reduce the risk of a fault in various areas of the infrastructure. These can include:

- **Using RAID.** As previously mentioned, RAID allows you to experience drive failures within a hyperconverged node and keep operating.

- **Redundant power supplies.** Extra power supplies are, indeed, a part of your availability strategy, because they allow you to experience a fault with your power system and still keep servers operating.

- **Multiple network adapters.** Even network devices can fail, and when they do, communications between servers and users and between servers and other servers can be lost. Unless you’ve deployed multiple switches into your environment and multiple network adapters into your servers, you can’t survive a network fault. Network redundancy helps you make your environment resilient to network-related outages. A software-defined network with automation and workload intent-based principles provides even more protection, as the intelligence recognizes faults and automatically adjusts network paths.

- **Virtualization layer.** The virtualization layer includes its own fault-tolerance mechanisms, some of which are transparent, and others that require a quick reboot. For example, VMware’s High Availability (HA) service continuously monitors all of your
vSphere hosts. If one fails, workloads are automatically restarted on another node. There is some downtime, but it’s minimal. In addition to HA, VMware makes available a fault-tolerance feature. With FT, you actually run multiple VMs. One is the production system and the second is a live shadow VM that springs into action in the event that the production system becomes unavailable. However, with all that said, there are some limitations inherent in hypervisor-based fault tolerance technology, described in the sidebar, “Fault Tolerance Improvements in vSphere 6+.” This is why some hyperconverged infrastructure vendors eschew hypervisor-based fault-tolerance mechanisms in favor of building their own solutions.

**End Results: High Availability, Architectural Resiliency, Data Protection, and Disaster Recovery**

No one wants downtime. It’s expensive and stressful and can even be career-impacting. Most organizations would be thrilled if IT could guarantee that there would be no more downtime ever again. Of course, there’s no way to absolutely guarantee that availability will always be 100 percent, but organizations do strive to hit 99 percent to 99.999 percent (and even higher) availability as much as possible.

**Simplified Storage Systems**

Bear in mind that RAID, and storage in general, becomes far simpler to manage in a hyperconverged infrastructure scenario. There’s no more SAN and, in most cases, RAID configuration is an “under the hood” element that you don’t need to worry about. This is one less component that you have to worry about in your data center.
High availability is really the result of a combination of capabilities in an environment. In order to enable a highly available application environment, you need to have individual nodes that can continue to work even if certain hardware components fail and you need to have a cluster that can continue to operate even if one of the member nodes bites it.

Hyperconverged infrastructure helps you to achieve your availability and data protection goals in a number of different ways. First, the linear scale-out nature of hyperconverged infrastructure (in other words, as you add nodes, you add all resources, including compute, storage, and RAM), means that you can withstand the loss of a node because data is replicated across multiple nodes with RAIN. Plus, for some hyperconverged solutions, internal use of RAID means that you can withstand the loss of a drive or two in a single node. With the combination of

---

### Fault Tolerance Improvements in vSphere 6+

Frankly, vSphere Fault Tolerance used to be all but useless, except for the smallest VMs. Here’s an excerpt from VMware’s documentation explaining the limitations of vSphere Fault Tolerance: “Only VMs with a single vCPU are compatible with Fault Tolerance.” This limitation was one of the many items that held back vSphere Fault Tolerance from being truly usable across the board.

vSphere 6 increased Fault Tolerance capabilities to VMs with up to four vCPUs. This is still a significant limitation when you consider that many VMs are deployed with eight vCPUs or more, particularly for large workloads. And, only machines with 64GB or less of RAM were supported by Fault Tolerance in vSphere 6.0 and 6.5.

Fortunately, VMware keeps moving ahead. vSphere 6.7 further increases the vCPU limit for Fault Tolerance to eight vCPUs and on the RAM front, VMs with up to 128GB of RAM are supported.
RAIN+RAID providing the most comprehensive disaster recovery capabilities, you can withstand the loss of an entire data center and keep on operating with little to no loss of data.

As you research hyperconverged infrastructure solutions, it’s important to make sure that you ask a lot of questions about how vendors provide availability and data protection in their products. The answers to these questions will make or break your purchase.

**Up Next**

It’s clear that data protection and high availability are key components in any data center today. The cloud has become another way that companies can improve their availability and data protection systems. Of course, cloud can do a lot more as well, which is why it’s the topic of our next chapter.
Hyperconverged Infrastructure in a Hybrid Cloud World

This chapter will help you understand the ways by which you can leverage cloud services as part of your hyperconverged infrastructure solutions. It will also help you better understand the private cloud and how that fits with hyperconvergence. Can a hyperconverged solution deliver some of the things that organizational leadership has come to expect from the cloud? Can public and private cloud deployments co-exist in harmony?

Why Is Cloud So Desirable?

You’ll learn more about what defines cloud a little later in this chapter. Before getting into the various definitions, though, let’s discuss the inherent cloud traits that make this destination a popular and desirable choice for service deployment.

The Economic Model

Everything in business eventually comes down to money. Decision makers are constantly on the lookout for ways to reduce costs while also boosting efficiency and outcomes. This is often a seemingly impossible task described as “doing more with less.” IT was supposed to be an enabler, but for many companies, it has become a money pit—an expense center to be minimized. Obviously, when leveraged properly, IT can be an incredible enabling function, but even in these cases, no one wants to spend more than they have to.
When you buy your own data center hardware and software, you incur pretty significant capital costs. This initial cash outlay, necessary to procure a solution, can be pretty high and can result in the need to cut corners or even delay upgrades if there’s not enough cash available or if management won’t make sufficient cash available.

When you decide to start consuming resources from the public cloud, there’s no initial cash outlay necessary. You don’t incur capital expenses. Sure, you might have to pay a bit in the way of startup costs, but you don’t have to buy hardware and software. You simply rent space on someone else’s servers and storage.

Business decision makers love this shift. They don’t need to worry about huge capital expenditures, and they know that they’re paying for what they use. They’re not paying for extra hardware that may never end up actually being leveraged to help solve business needs.

**Scale**

Your business isn’t a static entity. It grows. It changes over time. At some point, that may mean needing to scale the data center environment. When you build your own data center, you have to do all the work yourself. Sometimes, you can scale in increments that make financial sense, while other times you have to add more than you might like due to predefined requirements from your vendors. It’s an inexact science.

When you use the public cloud, you don’t have to worry about inherent scaling limits or increments. Remember, you pay for what you use. As your usage grows, so does your bill, but you don’t generally need to manually add new resources to your account. It can happen automatically.

Scalability granularity often isn’t a problem with the public cloud, either. You grow as you need to in the increments that you need. There’s no practical limit to how far you can grow as long as the cloud provider still has resources.
Geographic Diversity and Disaster Recovery

Building multiple data centers can be an expensive undertaking, but it’s one that’s often executed as companies seek ways to protect their data and ensure continuity of their business in the event of a disaster striking the primary data center. The separate data centers are generally geographically diverse so that a single natural disaster can’t take out both sites at the same time.

Public cloud providers almost always have native systems that can quickly enable geographic diversity for applications that are already running on their systems. Enabling geographic diversity is often as simple as clicking a mouse button and, most likely, paying some additional money to the cloud provider.

The Public Cloud

The cloud is everywhere. For many, the term itself has become synonymous with “Internet” or is just another way to describe what used to be called “hosted services.” However, there are a number of traits that make a public cloud a public cloud.

First, in general, public cloud systems are comprised of multi-tenant environments operated by a service provider with the hardware and software located in the provider’s data center. As the saying goes, it’s someone else’s computer. In these environments, the customer may not always even be aware in which provider data center the services reside, nor does the customer have to be aware in some cases (although it’s good practice to know where your data lives). The beauty of these systems is that workloads can move around as necessary to maintain SLAs.

Cloud service providers generally build their systems with the assumption that hardware will ultimately fail, which means the you, as the customer, can avoid the need to buy expensive failover and availability systems on your own since the provider’s already doing it.
The Faces of the Public Cloud

Here’s a brief look at the different kinds of public cloud services that are available on the market.

**Software-as-a-Service (SaaS)**

From a customer perspective, SaaS is the simplest kind of cloud service to consume as it’s basically an application all wrapped up and ready to go. Common SaaS applications include Salesforce and Office 365.

With SaaS applications, the provider controls everything and provides to the customer an application layer interface that only controls very specific configuration items. Because all of the infrastructure and the fact that most of the software is hidden from the you as the customer, you don’t need to worry about any underlying services except those that may extend the service, such as integrating Office 365 with your on-premises Active Directory environment.

**Platform-as-a-Service (PaaS)**

Sometimes, you don’t need or want a complete application. In many cases, you just need a place to install your own applications but you don’t want to have to worry at all about the underlying infrastructure or virtualization layers. This is where PaaS comes into play.

PaaS provides you with infrastructure and an application development platform that gives you the ability to automate and deploy applications including your own databases, tools, and services. As a customer, you simply manage the application and data layers.

**Infrastructure-as-a-Service (IaaS)**

In other cases, you need a bit more control, but you still may not want to have to directly manage the virtualization, storage, and networking layers. However, you need the ability to deploy your own operating systems inside
vendor-provided VMs. Plus, you want to have the ability to manage operating systems, security, databases, and applications.

For some, IaaS makes the most sense since the provider offers the network, storage, compute resources, and virtualization technology while you manage everything else.

For scale, the cloud provider can provide grid-like scalability so that you don’t need to worry about how to grow when the time comes.

For public cloud, there are a number of pros and cons to consider. On the plus side, cloud will:

- Enable immediate implementation
- Carry low to no initial deployment costs
- Provide a consumption-based utility cost model

However, there are definitely some downsides to cloud as well, which include:

- Provide more cost-effective scale than would be feasible in a private data center
- Potentially unpredictable ongoing usage charges
- Concerns around data location; many don’t want data stored in U.S.-based data centers due to concerns around the NSA and PATRIOT Act and GDPR; this issue is now referred to as ensuring an understanding of data sovereignty
- Charges across every aspect of the environment, from data storage to data transfer and more
- No control over underlying infrastructure
- Care needs to be taken to avoid lock-in
On-Premises Reality

Even though public cloud has a number of desirable traits, there are some harsh realities with which CIOs and IT pros need to contend:

- **Security.** For some, particularly those in highly regulated or highly secure environments, the idea of moving to a multi-tenant public cloud is simply not feasible, although cloud providers have added, and continue to enhance, versions of their services to meet specific compliance requirements.

- **Bandwidth.** Many areas of the world remain underserved when it comes to bandwidth, and some companies can’t get sufficient bandwidth or link redundancy with sufficiently low latency to make cloud a feasible option at scale.

- **Cost.** There may come a point at which cloud may become more expensive than simply building your own environment. This is an increasingly common scenario. For example, unused instances, reserved compute, and instances that are turned off all lead to unexpected costs and stranded capacity. A survey performed by RightScale estimates that up to 35% of public cloud spend is wasted due to these issues.

- **Comfort level to meet service levels.** Let’s face it, in spite of everything that public cloud has to offer, it’s hard to trust having all of your apps and data live offsite. Most IT organizations opt to keep some business-critical data on-premises to meet business service level agreements (SLAs).

These challenges are reasons that many organizations are turning to private cloud environments.
Private Clouds

The term private cloud is often, well, clouded in confusion as people try to apply the term to a broad swath of data center architectures. So, let’s try to clear up some of the confusion.

First and foremost, a private cloud environment generally resides in a single tenant environment that is built out in an on-premises data center, but it can sometimes consist of a single tenant environment in a public data center. For the purposes of this chapter, we’ll focus on the on-premises use case.

Private cloud environments are characterized by heavy virtualization, which fully abstracts the applications from underlying hardware components. Virtualization is absolutely key to these kinds of environments. Some companies go so far as to offer internal SLAs to internal clients in a cloud-like manner. The key phrase there is “internal clients”—that’s the customer in a private cloud environment. For such environments, being able to provide service-level guarantees may mean that multiple geographically dispersed data centers need to be built in order to replicate this feature of public cloud providers.

Heavy use of virtualization coupled with comprehensive automation, orchestration, and intelligent reporting tools enables an additional benefit of private cloud: self-service. Moving to more of a self-service model has several benefits:

- Users get their needs serviced faster
- IT is forced to build or deploy automation tools to enable self-service functionality, thereby streamlining the administrative experience
- Reporting and analytics gives ability to charge-back and show-back usage as well as optimize the infrastructure with predictive analytics and monitoring to avoid stranded capacity.
As mentioned before, many companies want to keep their data center assets close at hand and in their full control, but they want to be able to gain some cloud-like attributes, hence the overall interest in private cloud. As is the case with public cloud, there are a number of pros and cons that need to be considered when building a private cloud.

In the pros column, private cloud:

- Provides an opportunity to shift workloads between servers to best manage spikes in utilization in a more automated fashion
- Enables the ability to deploy new workloads on a common infrastructure. Again, this comes courtesy of the virtualization layer
- Provides full control of the entire environment, from hardware to storage to software in a way that enables operational efficiency. In other words, routine tasks are automated and repeatable
- Allows customers to customize the environment since they own everything
- Provides additional levels of security and compliance due to the single tenant nature of the infrastructure. Private cloud-type environments are often the default due to security concerns

As with everything, not all is a perfect picture. Private clouds do have a number of drawbacks, including:

- Requiring customers to build, buy, and manage hardware. This is often something that many companies want to reduce or eliminate
- They don’t always result in operational efficiency gains
- Not really providing what’s considered a cloud-computing economic model. You still have to buy and maintain everything
- Potentially carrying very high acquisition costs
In short, private clouds are intended to have some of the architectural characteristics of public clouds while offering internal clients cloud-like economic outcomes when chargeback processes are implemented.

Even if the central IT department providing the service doesn’t really use “the cloud,” as internal clients are able to provision and consume resources on demand—at least to a reasonable point—there’s the beginning of a private cloud taking shape.

**Hybrid Cloud & Multi-Cloud**

Increasingly, people are choosing both cloud options—public and private—to meet their needs and are even adopting multiple public cloud offerings. In these hybrid and multi-cloud scenarios, the company builds its own on-premises private cloud infrastructure to meet local application needs and also leverage one or more public clouds where reasonable and possible. In this way, the company gets to pick and choose which services run where and can also move between them at will.

**The Intersection of Cloud and Hyperconverged Infrastructure**

If you’re wondering what all of this talk about cloud has to do with hyperconverged infrastructure, wonder no more! Depending on the hyperconverged infrastructure solution you’re considering, there are varying degrees of association between the hyperconverged infrastructure product and both public and private clouds.

**Economics**

Everything you’ve read so far leads to money. The potential to completely transform the data center funding model is one of the key outcomes when you consider hyperconverged infrastructure. With easier administration comes lower staffing costs. With the use of
commodity hardware comes lower acquisition costs. With the ability to scale linearly in bite-size chunks, companies can get the beginnings of a consumption-based data center equipment acquisition model that enables closer pay-as-you-go growth than traditional data center architectural models allow. As your environment needs to grow and as users demand new services, you can easily grow by adding new hyper-converged systems.

**Scale**

Agility implies some level of predictability in how workloads will function. Public cloud provides this capability. For those wishing to deploy a private cloud environment, these needs can be met by leveraging hyperconvergence’s inherent ability to scale linearly. In other words, you scale all resources simultaneously, including compute, storage, and networking in small increments to large scale. In this way, you avoid potential resource constraint issues that can come from trying to manually adjust individual resources and you begin to achieve some of the economic benefits that have made public cloud a desirable option.

Scaling the data center shouldn’t result in scaling the complexity. In order to attain the full breadth of economic benefits that go with cloud, you have to make sure that the environment is very easy to manage or, at the very least, that management is efficient. This means that you need to automate what can be automated and try to reduce the number of consoles that it takes to get things done.

With hyperconverged infrastructure, management efficiency—even at scale—is a core feature of the solution. You’re able to manage all of the elements included in the product from a single console; to apply a breadth of consolidated policies to VMs; and leverage robust APIs for orchestration and automation.
Geographic Diversity and Disaster Recovery

Also on the economics front, the value of resiliency and disaster recovery cannot be overstated. One of the benefits of the cloud is the geographic diversity that can be achieved to protect against natural disasters. With a hyperconverged infrastructure solution that has resiliency and data replication as a part of the core offering, multisite redundancy capability is baked in as part of the solution.

For those that have opted to build hybrid clouds, some hyperconverged infrastructure solutions can leverage that public cloud deployment as a replication target. In other words, rather than going to the expense of building out a second physical site, the public cloud can be used to achieve data protection goals.

Hyperconvergence and the Private Cloud

Building a traditional private cloud can be hard work. It takes a lot of effort to get all of the pieces aligned. Hyperconverged infrastructure makes it possible to deploy private clouds in a fraction of the time it would normally take. Everything is built into the individual appliances, including centralized management, data efficiency, replication, and the ability to scale in incremental units. These are core needs in building an agile private cloud environment.

Next Steps

You’ve now completed your introductory journey into the technical world of hyperconverged infrastructure. To learn more about hyperconverged infrastructure, look for The Gorilla Guide to Hyperconverged Infrastructure Implementation Strategies where you’ll learn about key uses cases and how hyperconvergence is affecting the role of the IT pro.