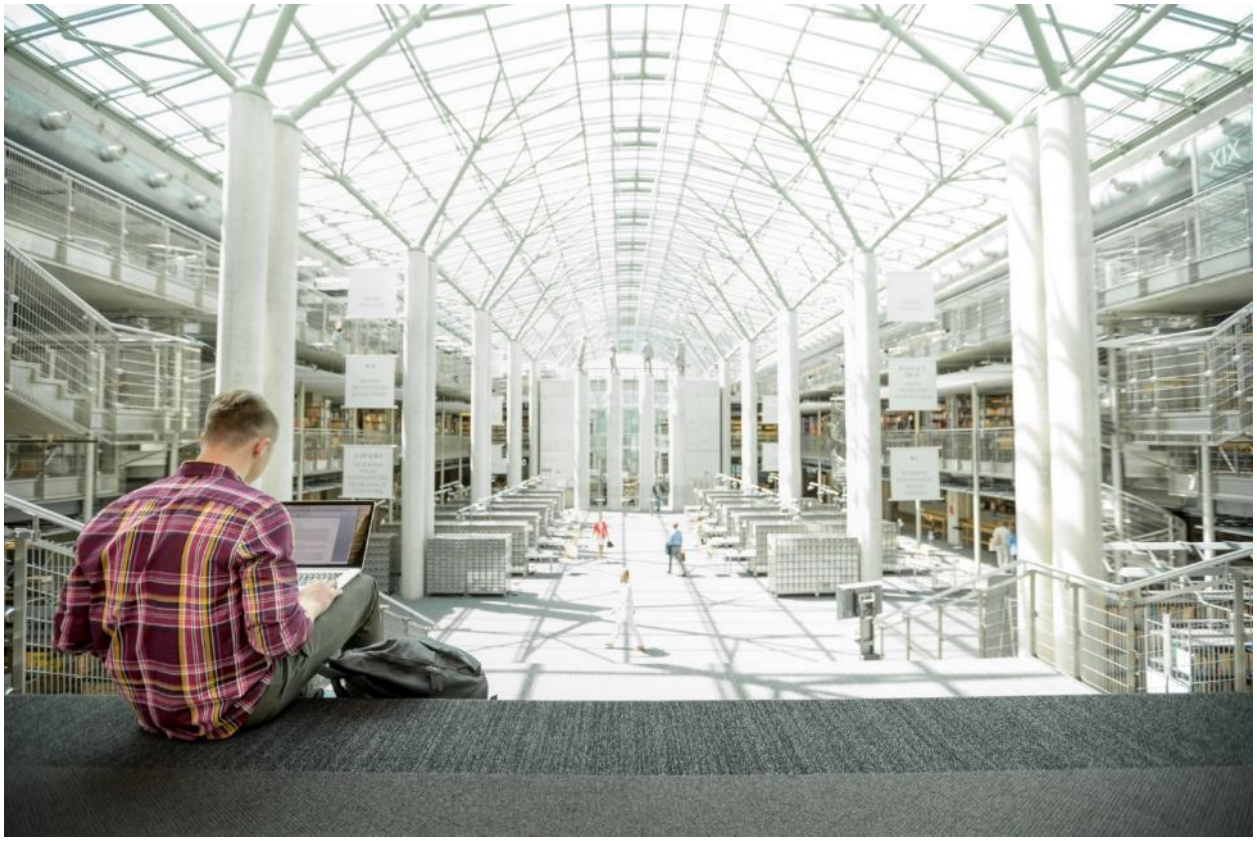


Cisco Design Guide for ScaleProtect™ with Cisco UCS®

Last Updated: December 12, 2018

About the Cisco Validated Design Program

The Cisco Validated Design (CVD) program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, see:

http://www.cisco.com/go/designzone.

Table of Contents

Executive Summary

Cisco Validated Designs (CVDs) deliver systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of the customers and to guide them from design to deployment. Cisco and Commvault have partnered to deliver a series of data protection solutions that provide customers with a new level of management simplicity and scale for managing secondary data on premises.

As organizations continue to innovate their businesses through digital transformation, it is clear that data has become the new currency. Successful organizations must harness the power of data to drive competitive differentiation and provide value to their customers.

Secondary storage and their associated workloads account for the vast majority of storage today. Enterprises face increasing demands to store and protect data while addressing the need to find new value in these secondary storage locations as a means to drive key business and IT transformation initiatives. ScaleProtect™ with Cisco Unified Computing System (Cisco UCS) supports these initiatives by providing a unified modern data protection and management platform that delivers cloud-scalable services on-premises. The solution drives down costs across the enterprise by eliminating costly point solutions that do not scale and lack visibility into secondary data.

This CVD provides design details for the ScaleProtect with Cisco UCS solution, specifically focusing on the Cisco UCS S3260 Storage Server. ScaleProtect with Cisco UCS is deployed as a single cohesive system, which is made up of Commvault® Software and Cisco UCS infrastructure. Cisco UCS infrastructure provides the compute, storage, and networking, while Commvault Software provides the data protection and software designed scale-out platform.

Solution Overview

Introduction

This design document outlines the principles that comprise the ScaleProtect with Cisco UCS solution, which is a validated architecture jointly developed by Cisco and Commvault. This solution is a pre-designed, integrated, and validated architecture for modern data protection that combines Cisco UCS servers, Cisco Nexus switches, Commvault Complete™ Backup & Recovery, and Commvault HyperScale™ Software into a single software-defined scale-out flexible architecture. ScaleProtect with Cisco UCS is designed for high availability and resiliency, with no single points of failure, while maintaining cost-effectiveness and flexibility in design to support secondary storage workloads (for example; backup and recovery, disaster recovery, dev/test copies, etc.).

ScaleProtect design discussed in this document has been validated for resiliency and fault tolerance during system upgrades, component failures, and partial as well as complete loss of power scenarios.

This design guide focuses on the architecture and design of the Cisco UCS S3260 M5 Storage Servers for use with ScaleProtect for Cisco UCS. The design guide is a living document; as such, the addition of new designs or updates will be incorporated as Cisco and Commvault work together to enhance this solution offering to meet market requirements.

Audience

The audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineers, IT architects, and customers who want to take advantage of an infrastructure that is built to deliver IT efficiency and enable IT innovation. The reader of this document is expected to have the necessary training and background to install and configure Cisco UCS, Cisco Nexus, and Cisco UCS Manager as well as a high-level understanding of Commvault Software and its components. External references are provided where applicable and it is recommended that the reader be familiar with these documents.

Purpose of this Document

This document describes the best practices to design a ScaleProtect with Cisco UCS solution.

Solution Summary

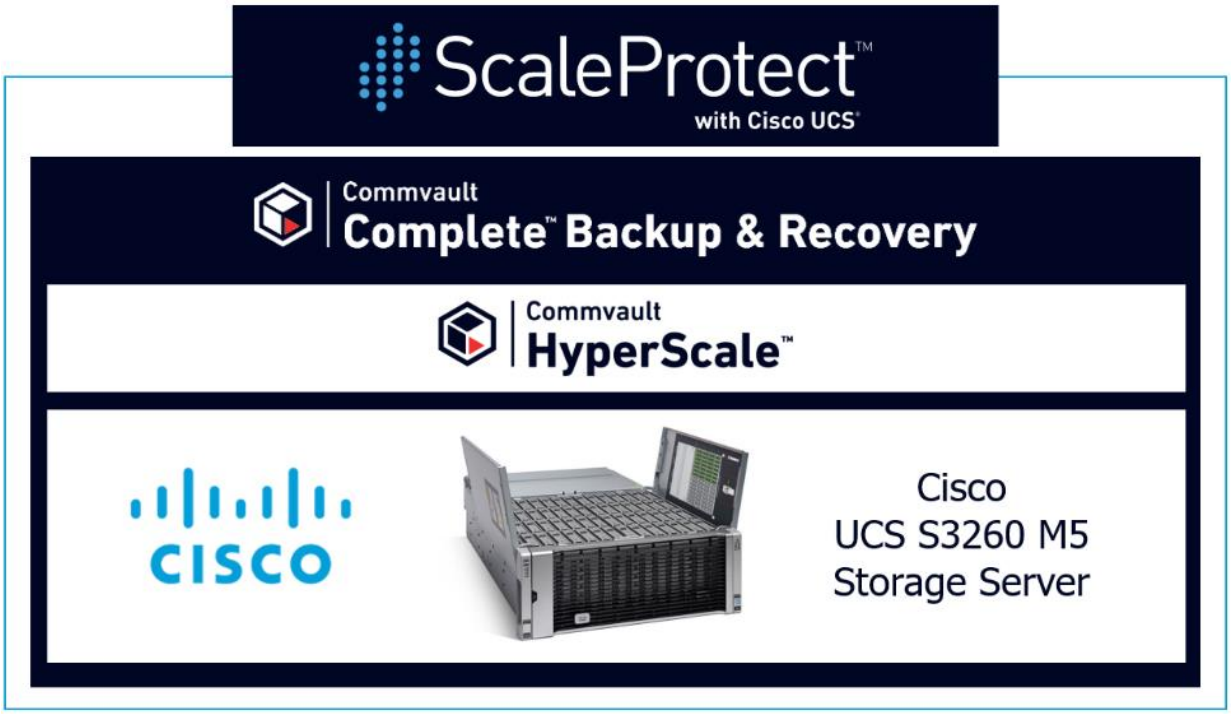
Cisco UCS revolutionized the server market through its programmable fabric and automated management that simplify application and service deployment. Commvault HyperScale™ Software provides the software-defined scale-out architecture that is fully integrated and includes true hybrid cloud capabilities. Commvault Complete Backup & Recovery provides a full suite of functionality for protecting, recovering, indexing, securing, automating, reporting, and natively accessing data. Cisco UCS, along with Commvault Software delivers an integrated software defined scale-out solution called ScaleProtect with Cisco UCS.

It is the only solution available with enterprise-class data management services that takes full advantage of industry-standard scale-out infrastructure together with Cisco UCS. ScaleProtect with Cisco UCS tightly integrates with Cisco UCS compute, storage and offers full life cycle data management and analytics into a single platform across both on-premises and the cloud. This turnkey Hyperconverged data management solution provides ease of use, greater resiliency, availability, scalability, and services for applications and data in an on-premises structure.

ScaleProtect with Cisco UCS consolidates multiple different point solutions and disparate architectures that are found in traditional data protection solutions into a single software-defined stack running on Cisco UCS. This

solution scales from terabytes to petabytes that eliminate the need for dedicated and proprietary infrastructure, which dramatically reduces complexity and infrastructure costs while ensuring the enterprise is more agile for data protection, recovery, and new secondary workloads.

Figure 1 ScaleProtect with Cisco UCS Solution Summary



The configuration uses the following components for the deployment:

- Cisco Unified Computing System (Cisco UCS)
  - Cisco UCS Manager
  - Cisco UCS 6332 Series Fabric Interconnects
  - Cisco UCS S3260 Storage Server
  - Cisco UCS S3260 M5 Server Node
  - Cisco S3260 system IO controller with VIC 1380
- Cisco Nexus C9332PQ Series Switches
- Commvault Complete™ Backup and Recovery v11
- Commvault HyperScale Software

Solution Benefits

ScaleProtect with Cisco UCS improves efficiency and reduces downtime with modern data protection and live recovery. It helps you improve your data backup and recovery processes regardless of where your workloads and data are located. Protection spans the entire system, from the data center to the hybrid or public cloud. This comprehensive enterprise backup solution reduces risk by making data backup and recovery easy, with less operational complexity. You gain long-term value with modular scalability that lets the solution grow with your

business. Increase your infrastructure flexibility, remove data silos and costly appliances and introduce elastic economics for your data. ScaleProtect with Cisco UCS delivers the powerful simplicity of the Commvault Software but in a highly available integrated scale-out solution. This solution delivers a modern approach to data management and provides organizations even greater choice for solving data protection and management challenges. ScaleProtect with Cisco UCS allows organizations to decouple their data strategy from their infrastructure strategy.

This joint solution offers the following benefits:

- Scale - Cut costs and reduce your hardware footprint by breaking down data silos — incrementally adding storage capacity as needed instead of a forklift upgrade of current appliances. Plan for the future with an easily scalable single core platform, which delivers feature-for-feature performance and enables you to analyze, replicate, protect, archive, and search your enterprise data and information.
- Manage - Remove operational complexity and gain more value from your data with native automation and orchestration capabilities — from on-premises to and from the cloud. Manage rapidly growing data storage demand by utilizing a single platform to simplify backup, storage, and recovery.
- Optimize - Use operational metrics to tailor your service level agreements to your business demands and take advantage of hybrid cloud integration capabilities with no added hardware or appliances. Streamline backup using one platform, which provides the flexibility to maintain copies of your data on different storage tiers. This allows you to meet different retention and recovery needs, helps ensure appropriate levels of protection over time, and enhances overall efficiency.

This solution provides data protection for all your data and applications in both physical and virtual environments, and provides a holistic approach to data protection. With ScaleProtect with Cisco UCS, you also benefit from:

- Better, more secure data protection, utilization and movement by eliminating point products and data silos.
- Cutting costs of data management by managing and scaling the data within your infrastructures as needed and use existing investments more efficiently.
- Expedited recovery and operate with less downtime since you have the ability to efficiently capture, move, retain, find, and recover data from any storage tier
- Greater resiliency and availability for more predictable performance and improved service level agreements (SLAs)
- Ending costly and complex forklift upgrades
- Understanding your data better in order to reduce redundancy and optimize data movement, storage, protection, and recovery.

Technology Overview

ScaleProtect with Cisco UCS includes the following components:

- Cisco UCS 6332 Fabric Interconnects
- Cisco UCS S3260 M5 Servers
- Cisco Nexus 9332PQ switches
- Commvault Complete™ Backup and Recovery
- Commvault HyperScale Software

These components are connected and configured according to the best practices of both Cisco and Commvault to provide an ideal platform for data protection to enterprise workloads. ScaleProtect with Cisco UCS can scale out for greater performance and capacity for environments that require consistent deployment with unified management without impacting the availability of service.

Cisco Unified Computing System

Cisco Unified Computing System (Cisco UCS) is a state-of-the-art data center platform that unites computing, network, storage access, and virtualization into a single cohesive system.

The main components of Cisco Unified Computing System are:

- Computing - The system is based on an entirely new class of computing system that incorporates rack-mount and blade servers based on Intel Xeon Scalable Processor family. The Cisco UCS servers offer the patented Cisco Extended Memory Technology to support applications with large datasets and allow more virtual machines (VM) per server.
- Network - The system is integrated onto a low-latency, lossless, 40-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- Virtualization - The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- Storage access - The system provides consolidated access to both SAN storage and Network Attached Storage (NAS) over the unified fabric. By unifying the storage access, the Cisco Unified Computing System can access storage over Ethernet (NFS or iSCSI), Fibre Channel, and Fibre Channel over Ethernet (FCoE). This provides customers with choice for storage access and investment protection. In addition, the server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity, and management for increased productivity.

Cisco Unified Computing System is designed to deliver:

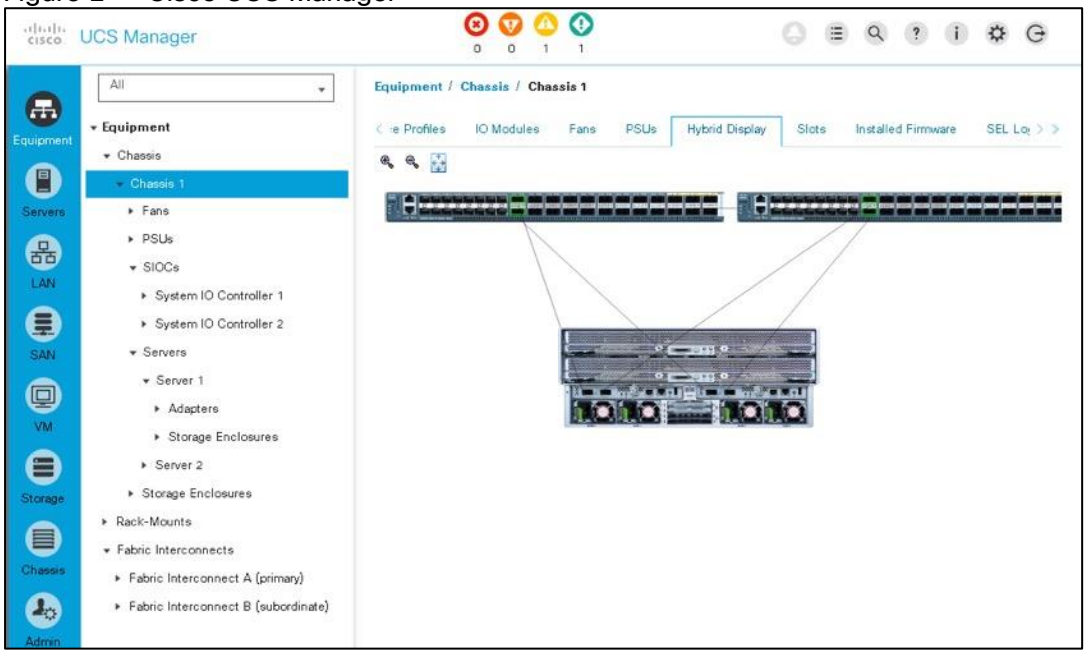
- A reduced Total Cost of Ownership (TCO) and increased business agility.
- Increased IT staff productivity through just-in-time provisioning and mobility support.
- A cohesive, integrated system that unifies the technology in the data center.

- Industry standards supported by a partner ecosystem of industry leaders.

Cisco UCS Manager

Cisco UCS® Manager (UCSM) provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ across multiple chassis, rack servers and thousands of virtual machines. It supports all Cisco UCS product models, including Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack-Mount Servers, and Cisco UCS Mini, as well as the associated storage resources and networks. Cisco UCS Manager is embedded on a pair of Cisco UCS 6300 or 6200 Series Fabric Interconnects using a clustered, active-standby configuration for high availability. The manager participates in server provisioning, device discovery, inventory, configuration, diagnostics, monitoring, fault detection, auditing, and statistics collection.

Figure 2 Cisco UCS Manager



An instance of Cisco UCS Manager with all Cisco UCS components managed by it forms a Cisco UCS domain, which can include up to 160 servers. In addition to provisioning Cisco UCS resources, this infrastructure management software provides a model-based foundation for streamlining the day-to-day processes of updating, monitoring, and managing computing resources, local storage, storage connections, and network connections. By enabling better automation of processes, Cisco UCS Manager allows IT organizations to achieve greater agility and scale in their infrastructure operations while reducing complexity and risk. Cisco Manager provides flexible role and policy-based management using service profiles and templates.

Cisco UCS Manager manages Cisco UCS systems through an intuitive HTML 5 or Java user interface and a command-line interface (CLI). It can register with Cisco UCS Central Software in a multi-domain Cisco UCS environment, enabling centralized management of distributed systems scaling to thousands of servers. Cisco UCS Manager can be integrated with Cisco UCS Director to facilitate orchestration and to provide support for converged infrastructure and Infrastructure as a Service (IaaS).

The Cisco UCS XML API provides comprehensive access to all Cisco UCS Manager Functions. The API provides Cisco UCS system visibility to higher-level systems management tools from independent software vendors (ISVs) such as VMware, Microsoft, and Splunk as well as tools from BMC, CA, HP, IBM, and others. ISVs and in-house developers can use the XML API to enhance the value of the Cisco UCS platform according to their unique

requirements. Cisco UCS PowerTool for Cisco UCS Manager and the Python Software Development Kit (SDK) help automate and manage configurations within Cisco UCS Manager.

Cisco UCS 6300 Fabric Interconnects

The Cisco UCS 6300 Series Fabric Interconnects are a core part of Cisco UCS, providing both network connectivity and management capabilities for the system. The Cisco UCS 6300 Series offers line-rate, low-latency, lossless 10 and 40 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and Fibre Channel functions.

Figure 3 Cisco UCS 6300 Fabric Interconnect

The Cisco UCS 6300 Series provides the management and communication backbone for the Cisco UCS B-Series Blade Servers, 5100 Series Blade Server Chassis, and C-Series Rack Servers managed by Cisco UCS. All servers attached to the fabric interconnects become part of a single, highly available management domain. In addition, by supporting unified fabric, the Cisco UCS 6300 Series provides both LAN and SAN connectivity for all servers within its domain.

From a networking perspective, the Cisco UCS 6300 Series uses a cut-through architecture, supporting deterministic, low-latency, line-rate 10 and 40 Gigabit Ethernet ports, switching capacity of 2.56 terabits per second (Tbps), and 320 Gbps of bandwidth per chassis, independent of packet size and enabled services. The product family supports Cisco® low-latency, lossless 10 and 40 Gigabit Ethernet unified network fabric capabilities, which increase the reliability, efficiency, and scalability of Ethernet networks. The fabric interconnect supports multiple traffic classes over a lossless Ethernet fabric from the server through the fabric interconnect. Significant TCO savings can be achieved with an FCoE optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

The Cisco UCS 6332 32-Port Fabric Interconnect is a 1-rack-unit (1RU) Gigabit Ethernet, and FCoE switch offering up to 2.56 Tbps throughput and up to 32 ports. The switch has 32 fixed 40-Gbps Ethernet and FCoE ports.

Both the Cisco UCS 6332UP 32-Port Fabric Interconnect and the Cisco UCS 6332 16-UP 40-Port Fabric Interconnect have ports that can be configured for the breakout feature that supports connectivity between 40 Gigabit Ethernet ports and 10 Gigabit Ethernet ports. This feature provides backward compatibility to existing hardware that supports 10 Gigabit Ethernet. A 40 Gigabit Ethernet port can be used as four 10 Gigabit Ethernet ports. Using a 40 Gigabit Ethernet SFP, these ports on a Cisco UCS 6300 Series Fabric Interconnect can connect to another fabric interconnect that has four 10 Gigabit Ethernet SFPs. The breakout feature can be configured on ports 1 to 12 and ports 15 to 26 on the Cisco UCS 6332UP Fabric Interconnect. Ports 17 to 34 on the Cisco UCS 6332 16-UP Fabric Interconnect support the breakout feature.

Cisco UCS S3260 Storage Server

The Cisco UCS® S3260 Storage Server is a modular, high-density, high-availability dual node rack server well suited for service providers, enterprises, and industry-specific environments. It addresses the need for dense cost effective storage for the ever-growing data needs. Designed for a new class of cloud-scale applications, it is simple to deploy and excellent for big data applications, Software-Defined Storage environments and other unstructured data repositories, media streaming, and content distribution.

Figure 4 Cisco UCS S3260 Storage Server

Extending the capability of the Cisco UCS C3000 portfolio, the Cisco UCS S3260 helps you achieve the highest levels of data availability. With dual-node capability that is based on the Intel® Xeon® scalable processors, it features up to 720 TB of local storage in a compact 4-rack-unit (4RU) form factor. All hard-disk drives can be asymmetrically split between the dual-nodes and are individually hot-swappable. The drives can be built in to an enterprise-class Redundant Array of Independent Disks (RAID) redundancy configuration or they can be configured in JBOD architecture in pass-through mode.

This high-density rack server comfortably fits in a standard 32-inch depth rack, such as the Cisco® R42610 Rack.

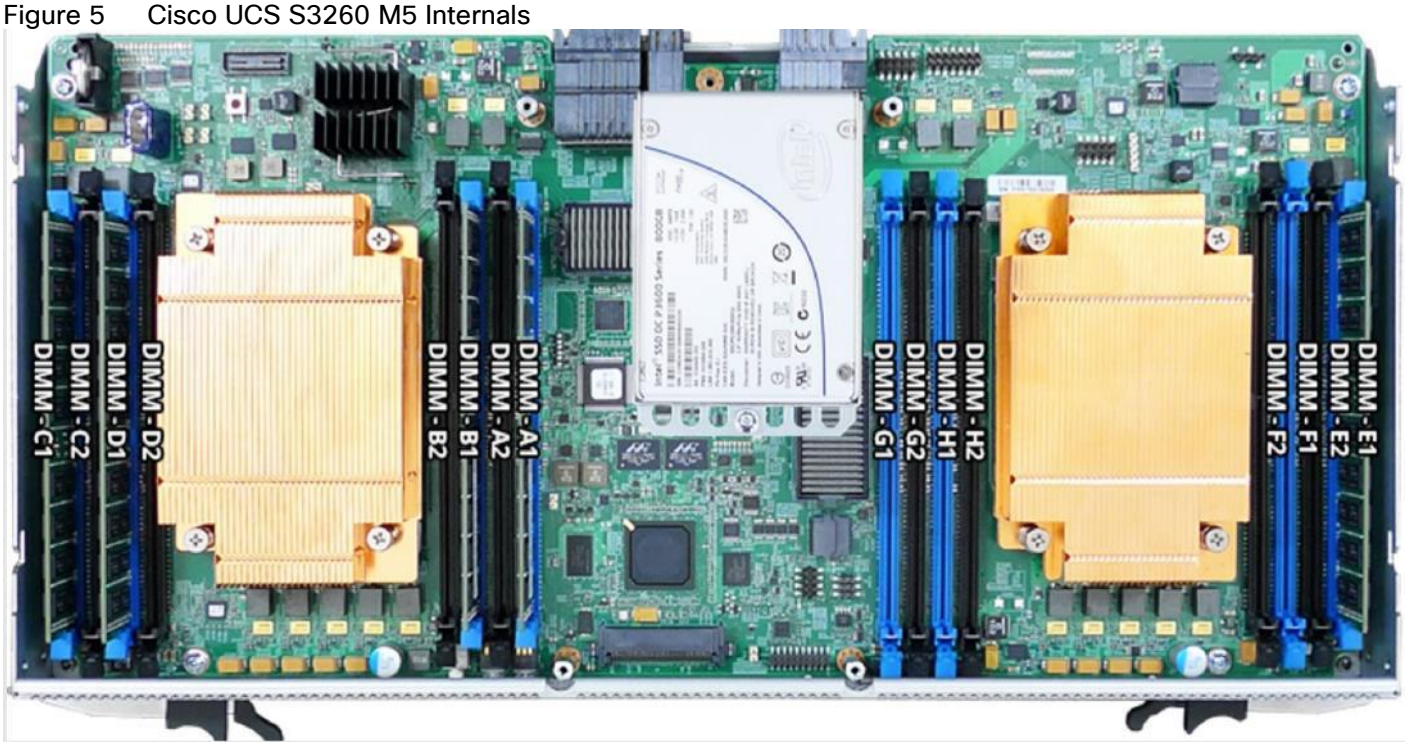
The Cisco UCS S3260 is deployed as a standalone server in both bare-metal or virtualized environments. Its modular architecture reduces TCO by allowing you to upgrade individual components over time and as use cases evolve, without having to replace the entire system.

The Cisco UCS S3260 uses a modular server architecture that, using Cisco's blade technology expertise, allows you to upgrade the computing or network nodes in the system without the need to migrate data migration from one system to another. It delivers the following:

- Dual server nodes, Cisco UCS S3260 chassis fits in two types of server nodes:
  - M5 server nodes based on Intel Xeon Scalable Processors
  - M4 server nodes based on Intel Xeon processor E5-2600 v4 CPUs
- Up to 44 computing cores per server node
- Up to 60 drives mixing a large form factor (LFF) with up to 28 solid-state disk (SSD) drives plus 2 SSD SATA boot drives per server node
- Up to 1.5 TB of memory per server node (3 TB Total) with 128GB DIMMs
- Support for 12-Gbps serial-attached SCSI (SAS) drives
- System I/O controller with a Cisco UCS Virtual Interface Card (VIC) 1300 platform embedded chip supporting dual-port 40 Gbps connectivity
- Enterprise-class redundancy with full-featured RAID plus JBOD
- Standalone management interface (Cisco Integrated Management Controller [CIMC])
- No data migration required when replacing or upgrading server nodes
- No need for extended-depth racks

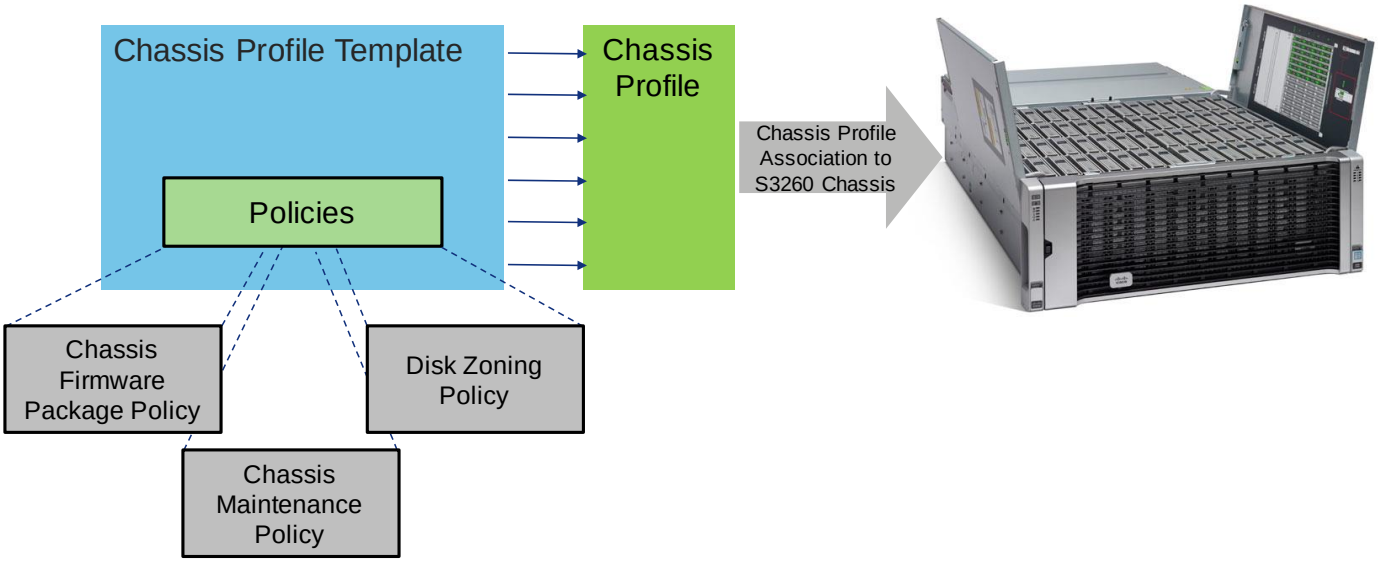
- High reliability, availability, and serviceability (RAS) features with tool-free server nodes, system I/O controller, easy-to-use latching lid, and hot-swappable and hot-pluggable components
- Dual 7mm NVMe - Capacity points: 512G, 1TB and 2TB
- 1G Host Management Port

Figure 5 Cisco UCS S3260 M5 Internals



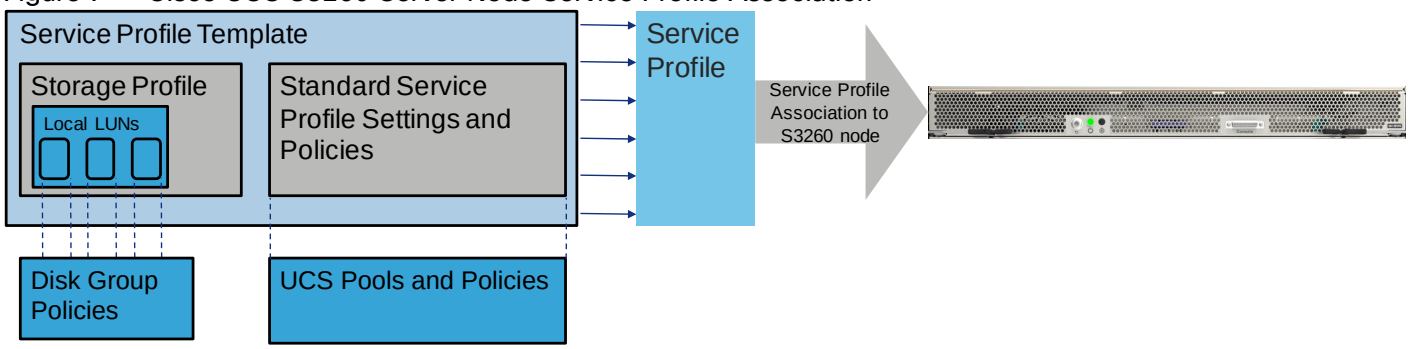
The Cisco UCS S3260 can be CIMC managed, or Cisco UCS Manager managed as a registered Chassis with the Cisco UCS Fabric Interconnects. When the Cisco UCS S3260 is Cisco UCS Manager managed, the Chassis will use a Chassis Profile can be generated from template, and will contain specifications for Firmware and Maintenance policies as well as the Disk Zoning Policy. The Disk Zoning Policy will be used to set how disk slot allocation occurs between server nodes.

Figure 6 Cisco UCS S3260 Chassis Profile Association



Server Nodes in a Cisco UCS Manager managed Cisco UCS S3260 are configured in nearly the same manner as standard Cisco UCS B-Series and Cisco UCS Manager managed Cisco UCS C-Series servers. The Server Nodes use Service Profiles that can be provisioned from templates, but need to have a Storage Profile set within the Service Profile. This enables access to the disk slots made available to it by the Disk Zoning Policy set within the chassis profile of the chassis in which the node is hosted.

Figure 7 Cisco UCS S3260 Server Node Service Profile Association



Within the Storage Profile there are two main functions, Local LUN creation that will be specified by Disk Group Policies, which are set within the Storage Profile. The LUNs created from the Disk Group Policies will have options of RAID 0, 1, 5, 6, 10, 50, or 60 and will allow the selection of type, quantity, or manual specification of slot the disk should be used from, as well as drive configuration policies of the LUN.

Cisco UCS Virtual Interface Card 1387

The Cisco UCS Virtual Interface Card (VIC) 1387 is a Cisco® innovation. It provides a policy-based, stateless, agile server infrastructure for your data center. This dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP) half-height PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter is designed exclusively for Cisco UCS C-Series and UCS S3260 Rack Servers. The card supports 40 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE). It incorporates Cisco's next-generation converged network adapter (CNA) technology and offers a comprehensive feature set, providing investment protection for future feature software releases. The card can present more than 256 PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the VIC supports

Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology. This technology extends the Cisco UCS Fabric Interconnect ports to virtual machines, simplifying server virtualization deployment.

Figure 8 Cisco UCS VIC 1387

The Cisco UCS VIC 1387 provides the following features and benefits:

- Stateless and agile platform: The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile. The capability to define, create, and use interfaces on demand provides a stateless and agile server infrastructure.
- Network interface virtualization: Each PCIe interface created on the VIC is associated with an interface on the Cisco UCS fabric interconnect, providing complete network separation for each virtual cable between a PCIe device on the VIC and the interface on the fabric interconnect.

Cisco Nexus 9300 Switches

The Cisco Nexus® 9000 Series Switches include both modular and fixed-port switches that are designed to overcome these challenges with a flexible, agile, low-cost, application-centric infrastructure.

Figure 9 Cisco Nexus 9332 Switch

The Cisco Nexus 9300 platform consists of fixed-port switches designed for top-of-rack (ToR) and middle-of-row (MoR) deployment in data centers that support enterprise applications, service provider hosting, and cloud computing environments. They are Layer 2 and 3 non-blocking 10 and 40 Gigabit Ethernet switches with up to 2.56 terabits per second (Tbps) of internal bandwidth.

The Cisco Nexus 9332PQ Switch is a 1-rack-unit (1RU) switch that supports 2.56 Tbps of bandwidth and over 720 million packets per second (mpps) across thirty-two 40-Gbps Enhanced QSFP+ ports.

All the Cisco Nexus 9300 platform switches use dual- core 2.5-GHz x86 CPUs with 64-GB solid-state disk (SSD) drives and 16 GB of memory for enhanced network performance.

With the Cisco Nexus 9000 Series, organizations can quickly and easily upgrade existing data centers to carry 40 Gigabit Ethernet to the aggregation layer or to the spine (in a leaf-and-spine configuration) through advanced and cost-effective optics that enable the use of existing 10 Gigabit Ethernet fiber (a pair of multimode fiber strands).

Cisco provides two modes of operation for the Cisco Nexus 9000 Series. Organizations can use Cisco® NX-OS Software to deploy the Cisco Nexus 9000 Series in standard Cisco Nexus switch environments. Organizations also can use a hardware infrastructure that is ready to support Cisco Application Centric Infrastructure (Cisco ACI™) to take full advantage of an automated, policy-based, systems management approach.

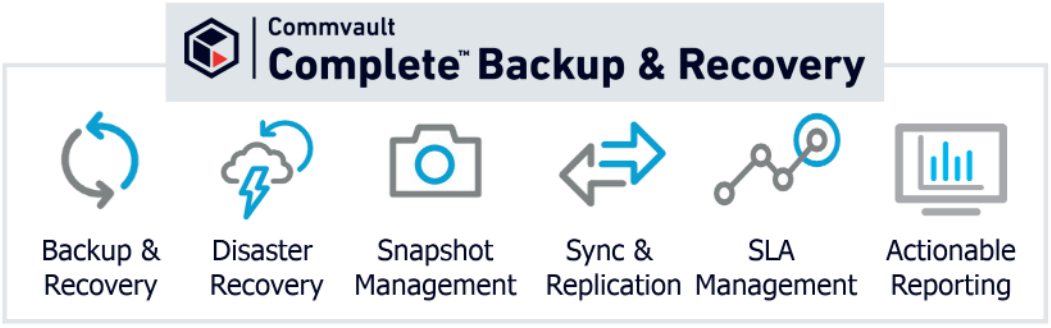
Commvault® Software

Commvault Software is a single platform for automated global protection, retention, and recovery. Commvault enterprise data protection and recovery software automates global data protection, accelerates recovery, reduces costs, and simplifies operations. A comprehensive data protection and management strategy offers seamless and efficient backup, archiving, storage, and recovery of data in your enterprise from any operating system, virtual machine, database, and application. Commvault Software converges all the needs of a modern data management solution in one place to seamlessly integrate protection, management, and access in one solution.

Commvault™ Complete Backup & Recovery

Commvault Complete Backup & Recovery software is an enterprise level, integrated data and information management solution, built from the ground up on a single platform and unified code base. All functions share the same back-end technologies to deliver the unparalleled advantages and benefits of a truly holistic approach to protecting, managing, and accessing data. Commvault Complete Backup & Recovery integrates application awareness with hardware snapshots, indexing, global deduplication, replication, search, and reporting.

Figure 10 Commvault Complete Backup & Recovery



The software contains modules to protect and archive, analyze, replicate, and search your data, which all share a common set of back-end services and advanced capabilities, seamlessly interacting with one another. This addresses all aspects of data management in the enterprise, while providing infinite scalability and unprecedented control of data and information. Built on a common platform with shared services to meet the burgeoning data protection and management needs of today's modern infrastructures. Commvault Complete Backup & Recovery converges all the needs of a modern data management solution in one place to seamlessly integrate protection, management, and access in one solution.

Commvault Complete benefits:

- Full support for all file systems, applications, and virtual platforms is included.

- Backup and recovery functionality to store protected data on disk/cloud/tape media, including deduplication and encryption capabilities.
- Store protected data with common cloud storage providers without the use of gateways or appliances.
- Replicate copies of live data in secondary (or more) locations.
- Integrate with an industry leading number of hardware arrays to orchestrate snapshot and backup operations from those snapshots without the use of scripts.
- Endpoint protection, with user self-service to directly protect and recover data, and even share data with others.
- Intelligently archive data, while keeping it protected, from both on-premises and cloud locations.
- Utilize machine-learning algorithms to optimize performance, analyze patterns, and report on anomalies.
- Actionable reporting to drive better SLA outcomes, targeted dashboard for application and virtualization owners, readiness reports to ensure the preparation for the unexpected is easy, and more.

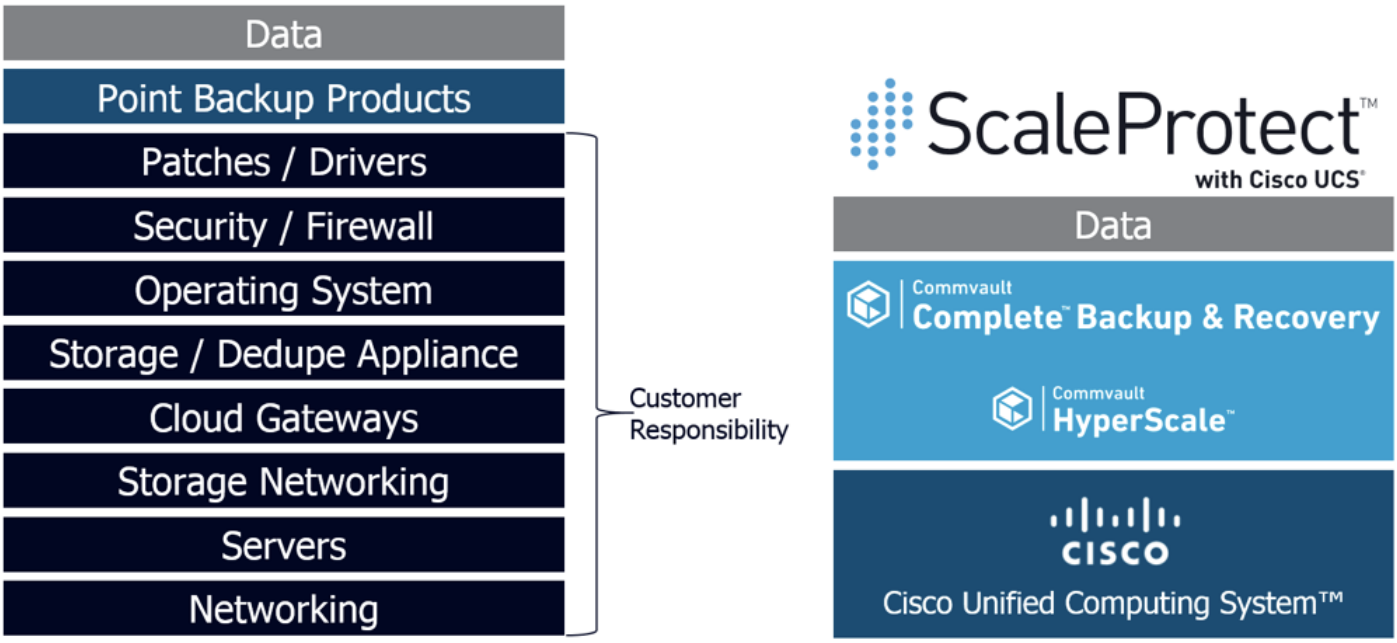
Commvault HyperScale™ Software

Commvault HyperScale™ Software combines data protection software, operating system, compute and storage in one integrated solution pre-configured for Cisco UCS infrastructure. Commvault HyperScale Software provides greater benefits over traditional software and hardware-based solutions taking the guesswork out of scale-out data protection with a single easy-to-use software package that simplifies and accelerates deployment, management, and support.

Commvault HyperScale Software addresses the data protection needs of modern data centers. The increasing percentage of virtualized workloads, the dramatic increase in the size and amount of data, and the changes in the ways that companies do business and work with data have had an immense impact on data protection solutions. With the time requirement for backup operations reduced to minutes, and with recovery point objective (RPO) and recovery time objective (RTO) requirements in the range of minutes to one hour, technologies such as compression, encryption, deduplication, replication, and backup to disk are essential in every design. The second-tier storage must be able to scale as quickly as the protected data grows, but the traditional silo-based approach has too many limitations to be effective. The Commvault HyperScale architecture introduces a modern way to perform second-tier data management by breaking down the silos and reducing the management overhead in second-tier environments.

The main objective of Commvault HyperScale Software is to simplify the management and scale of modern data protection. By transitioning from individual islands of storage devices, processors, networking, operating systems, and patching to a converged approached it allows the entire stack to be managed as a single platform. Compute capacity, memory, network, and storage are managed together allowing for an almost linear increase in of performance and capacity that cater to the needs of any enterprise. Commvault HyperScale Software forms a software-defined storage pool that is abstracted from the underlying hardware helps ensure that scale and hardware refreshes are no longer a monumental undertaking. The result is a data protection platform that can scale as required while meeting the Service Level Agreement (SLA) of any business.

Figure 11 Traditional Data Management Stack Compared to ScaleProtect with Cisco UCS



With Commvault HyperScale Software running on Cisco UCS, this in-depth integration enables enterprises to realize time savings in the following areas:

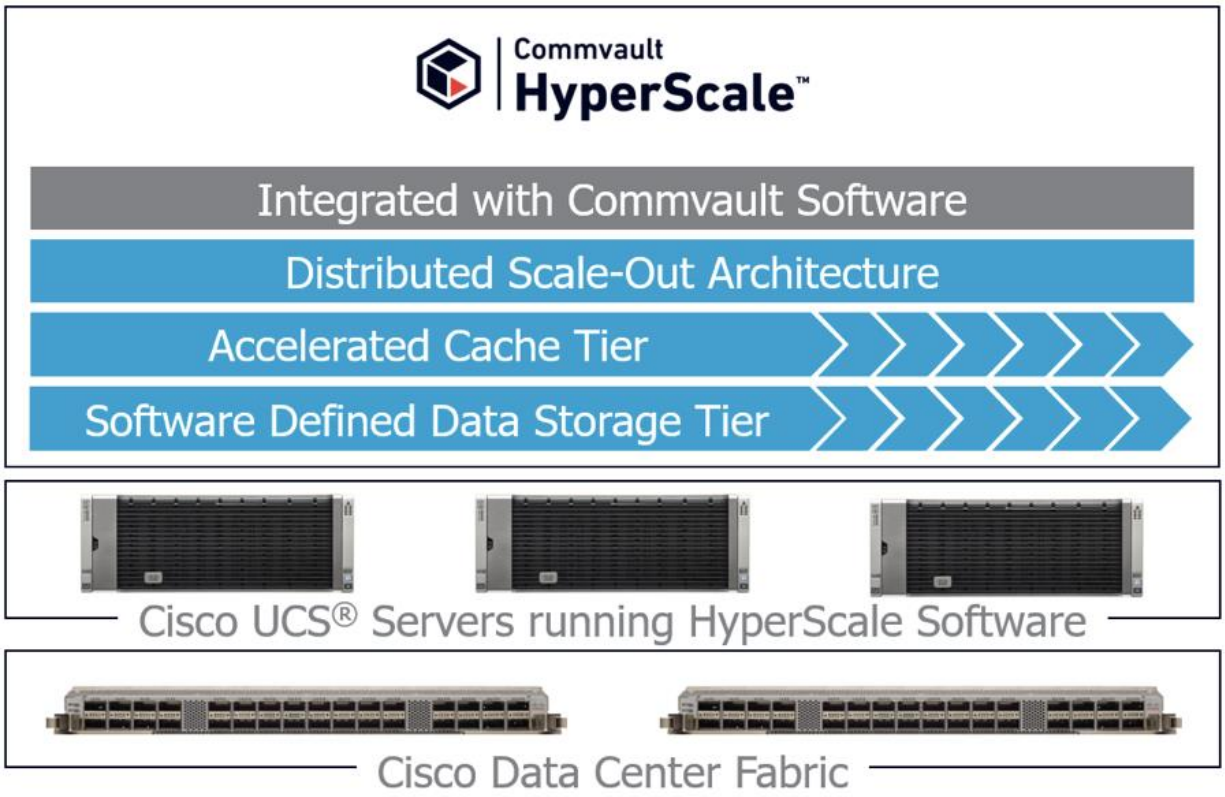
- Ease of Acquisition: an integrated solution including pre-installed data protection software, operating system, and compute and storage that is pre-configured and validated for the specific workload, available in a single package for easy procurement.
- Simple Installation and Integration: a single software package eliminates loading the OS, data protection software, and drivers separately. An installation guide and documented processes saves time and eliminates complexity.
- Centralized Manageability: conserve valuable IT staff resources and time with centralized management and reporting via an easy-to-use console for the entire solution. No longer manage the OS, compute, storage, and data protection separately.
- Single Patch and Driver Update: save time and minimize risk of patching individual software components and updating hardware drivers separately. A single, comprehensive patch, and updates the entire solution to ensure you are always running the current software and driver versions.

The features and functions provided by ScaleProtect with Cisco UCS create a powerful solution for backup and recovery operations that is simple to implement and easy to scale and upgrade. With the combination of Cisco and Commvault technologies, you can easily scale from tens of terabytes up to hundreds of petabytes (PB) of protected data.

Commvault HyperScale Architecture

Commvault HyperScale Software is integrated with Commvault Software to create an architecture that is highly available with no single point of failure. HyperScale Software nodes house all of the components required for data protection, recovery, deduplication, encryption, etc. Additionally, the architecture is integrated with Cisco UCS infrastructure to ensure that the hardware and software house create a software-defined scale out platform with built-in resiliency and redundancy.

Figure 12 Commvault HyperScale Architecture



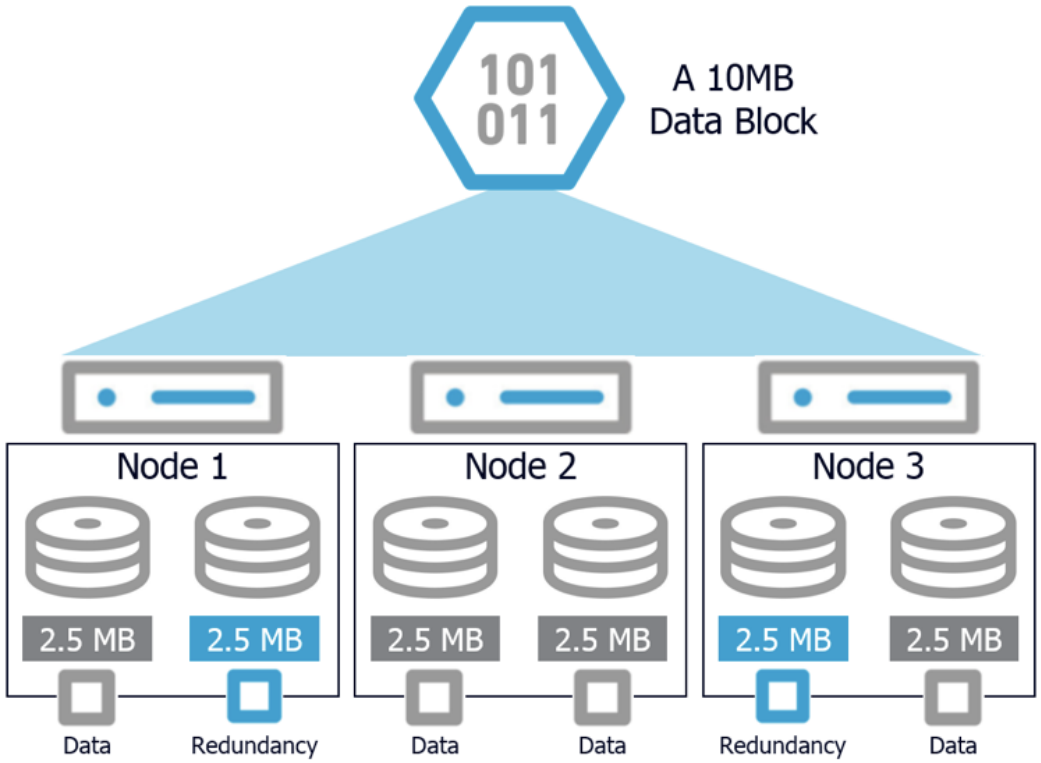
Logically the architecture converges multiple different functions into the stack:

- Distributed Scale-Out Architecture – replaces the need for standalone dedicated Media Management devices for accessing physical media, access to disk, cloud, or even tape are built-in. Services for data protection operations are embedded in each node of the architecture and scales with the solution.
- Accelerated Cache Tier – replaces the need for deduplication appliances or acceleration gateways for secondary operations.
- Software Defined Data Storage Tier – automatically scales with each node and ensure there is no utilization issues when growing the solution. Distribution of data, resiliency and redundancy are built-in and scale as the solution does.

Commvault HyperScale Storage Resiliency

Disk and node level resiliency for the data storage tier is a function of erasure coding and the block size of the cluster. Erasure coding is a method of data resiliency that splits data into fragments, encodes them, and redundantly disperses them across different disks within the grid. These dispersed volumes distribute the coded fragments across multiple nodes as a way to ensure the resiliency of stored data. Erasure coding is similar in a way to RAID which pools storage in a single system and fragments the data to be able to sustain drive failures. Unlike RAID, erasure coding fragments the data not just across drives, but across nodes as well, extending the failure tolerances to entire nodes without impacting the integrity of the overall grid.

Figure 13 Erasure Coding using Dispersed Volumes



Erasure coding uses multiple disk groups, called sub-volumes, to distribute the data across smaller subsets of disks in each block. In the above figure, the sub-volume is 6 hard drives (HDDs) which are housed in 3 nodes in the block. The standard HyperScale Software configuration consists of 3 nodes in a block, and sub-volumes which are based on 4+2 erasure coding. The numeric values of erasure coding provides the resiliency inside of the system, 4+2 represents that it requires 4 blocks of data to read a segment of information, and 2 represents the tolerance for failure, therefore 4+2 resiliency for any one node failure, or any two hard drives per sub-volume. Alternate block-size and erasure code configurations are available which change the resilience against failure.

Table 1 Erasure Coding Configuration Choices

Erasure Code	Block Size (Nodes / Block)	Sub- Volume Size	Erasure Coding Overhead	Node Failure Tolerance	HDD Failure Tolerance
(4 + 2)	3 Nodes	6 HDDs	**33%**	1 node per block	2 HDD's per sub-volume
	6 Nodes	6 HDDs	**33%**	2 nodes per block	2 HDD's per sub-volume
(8 + 4)	3 Nodes	12 HDDs	**33%**	1 node per block	4 HDD's per sub-volume
	6 Nodes	12 HDDs	**33%**	2 nodes per block	4 HDD's per sub-volume
	12 Nodes	12 HDDs	**33%**	4 nodes per block	4 HDD's per sub-volume

Choosing a larger erasure code method and block size can increase the resiliency, however it also alters the scaling metric. For instance, if an 8 + 4 erasure coding method is chosen, with a block size of 6 nodes, it increases the tolerance for node failure to any 2 nodes per block and any 4 HDDs per sub-volume. This increase

in tolerance requires that the scalability also shift from a 3 node increase in scaling, to a 6 node increase to help ensure that the tolerance levels are intact as the solution to scales.

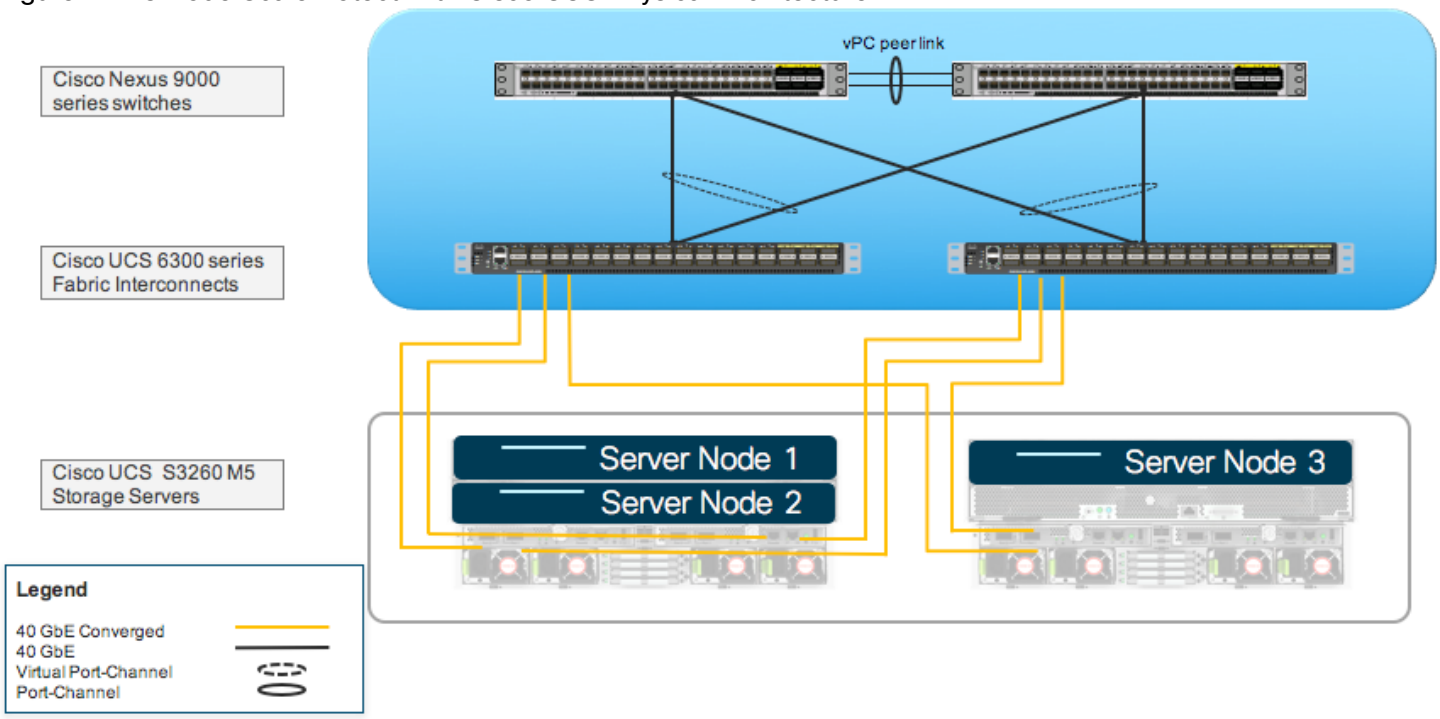
Solution Design

This section provides an overview of the hardware and software components used in this solution, as well as the design factors to be considered in order to make the system work as a single, highly available solution.

Architectural Overview

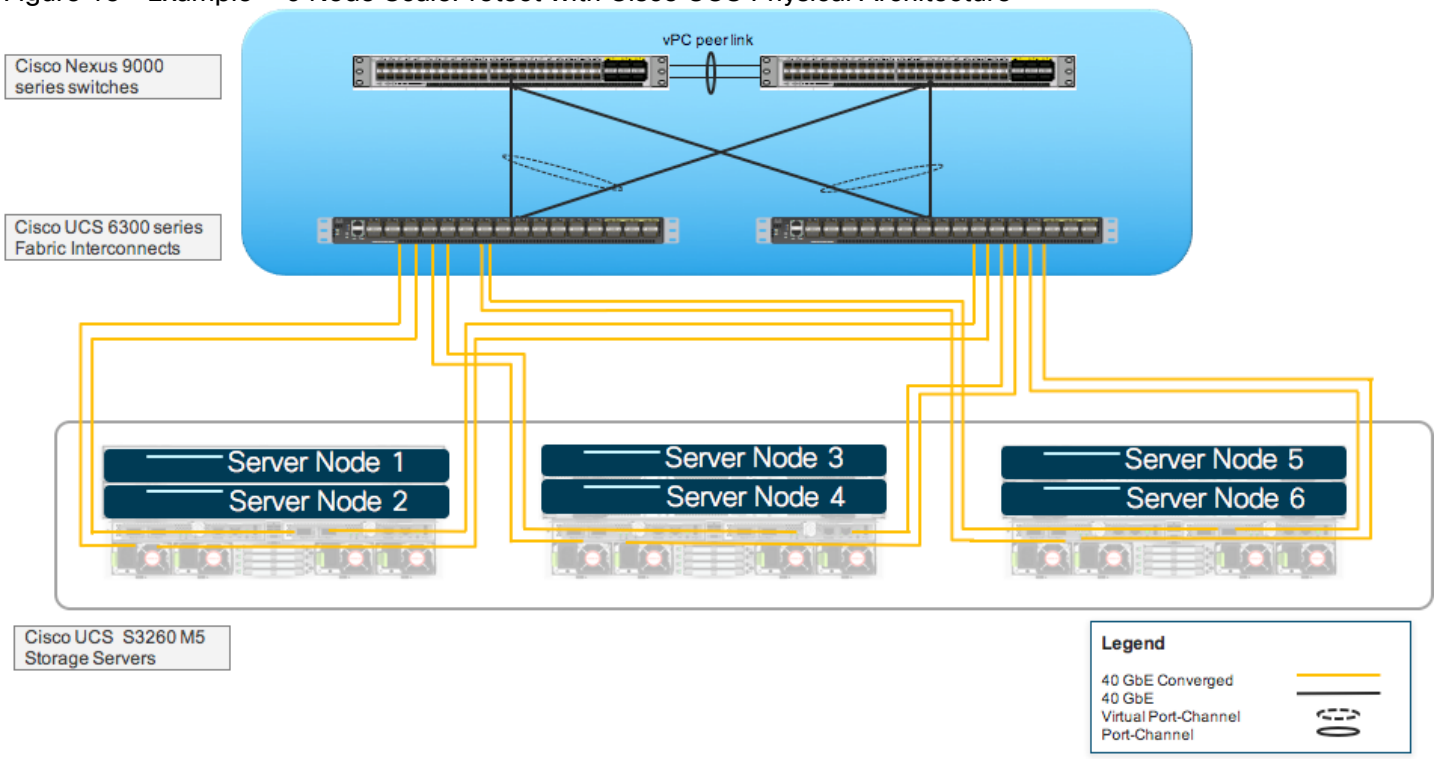
A typical ScaleProtect with Cisco UCS deployment starts with a 3 node block. The solution has been validated with three Cisco UCS S3260 M5 server nodes spread across two Cisco UCS S3260 Storage Server Chassis with built-in storage that consists of top-loaded Large Form Factor (LFF) HDDs for the software defined data storage tier, top-loaded Solid State Drives (SSDs) for the accelerated cache tier, and rear mounted SSDs for the operating system and associated binaries. Connectivity for the solution is provided via a pair of Cisco UCS 6332 Fabric Interconnects and to a pair of Cisco Nexus 9332PQ upstream network switches.

Figure 14 3 Node ScaleProtect with Cisco UCS Physical Architecture



ScaleProtect with Cisco UCS can start with more nodes than 3, the additional nodes are simply added to the Cisco UCS 6300 Series Fabric Interconnects for linear scalability. The only difference between a 3 or 6 node configuration is the chassis configuration of the S3260 M5. In the 3 node starting block, there is a dual node S3260 and a single node S3260, while in the 6 node configuration there are 3 dual nodes. Figure 15 outlines an example of a 6 node starting architecture.

Figure 15 Example – 6 Node ScaleProtect with Cisco UCS Physical Architecture



Node Hardware Overview

The Cisco UCS S3260 Storage Server can house single or dual nodes in a ScaleProtect with Cisco UCS configuration. The four rack unit (4RU) chassis can house two fully populated nodes in a single Chassis. A single node configuration can be expanded to a dual node configuration by adding the secondary node into the chassis and expanding the appropriate storage tiers.

Figure 16 Single and Dual Node Rear Chassis View

The hardware for each node is standardized for ease of deployment and configuration. There are two configurable components in the solution, the size of the NL-SAS drives in the Software Defined Data Storage Tier which determines the overall size of solution, and the Optional Cloud Cache.

Table 2 Cisco UCS S3260 M5 Server Node Configuration

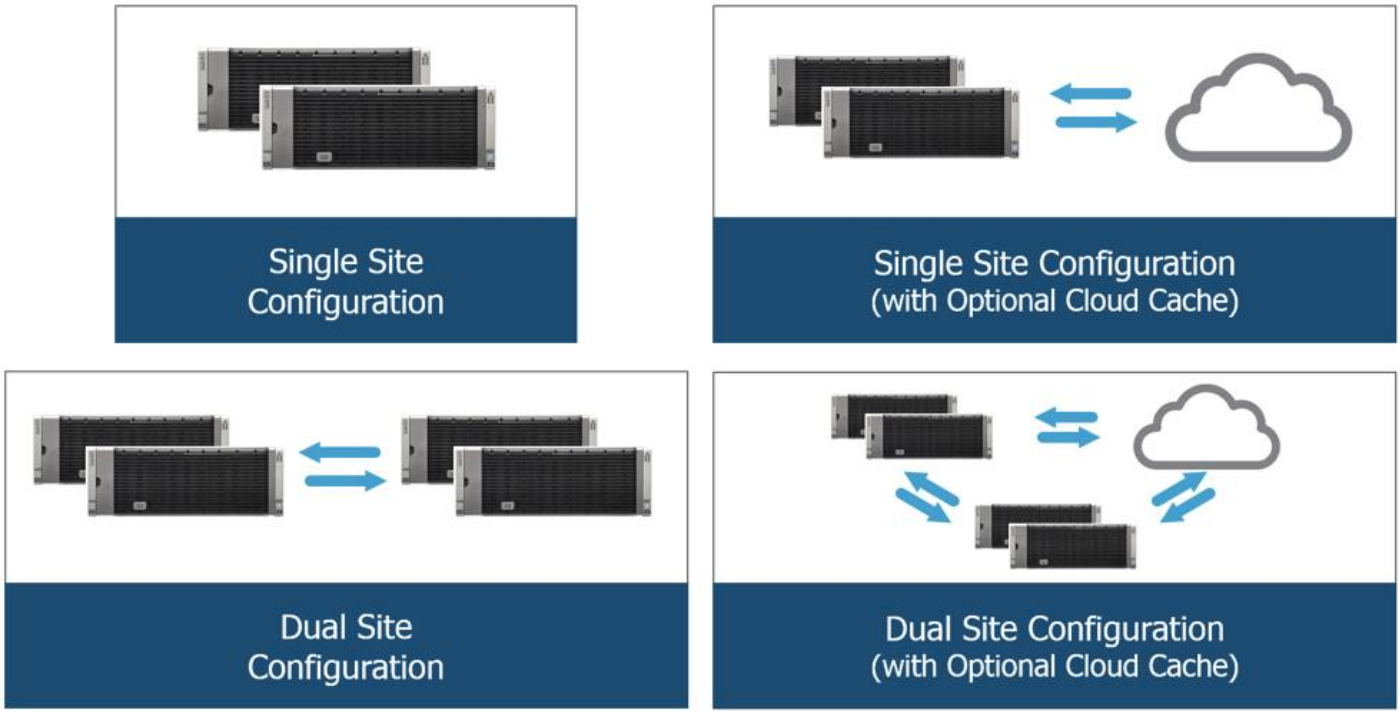
	S3260 M5 Dual Node		S3260 M5 Single Node
	Node 1	Node 2	Node 1
CPU	2x Intel® Xeon® Silver 4114 44.0GHz (20 Cores)	2x Intel® Xeon® Silver 4114 44.0GHz (20 Cores)	2x Intel® Xeon® Silver 4114 44.0GHz (20 Cores)

Memory	256GB DDR4	256GB DDR4	256GB DDR4
Storage	Boot Drives		
	(2) 480GB SSD – RAID1	(2) 480GB SSD – RAID1	(2) 480GB SSD – RAID1
	Accelerated Cache Tier		
	(4) 1.6TB SSD	(4) 1.6TB SSD	(4) 1.6TB SSD
	Optional Cloud Cache		
	(1) 2TB NVMe	(1) 2TB NVMe	(1) 2TB NVMe
	Software Defined Data Storage Tier		
	(24) 4/6/8/10/12TB HDD	(24) 4/6/8/10/12TB HDD	(24) 4/6/8/10/12TB HDD
Storage Controller	SAS 12G RAID	SAS 12G RAID	SAS 12G RAID
Network	(2) 40Gbps	(2) 40Gbps	(2) 40Gbps

Site Configuration Options

ScaleProtect with Cisco UCS can be utilized for data protection across multiple different sites and locations, from a single site to multi-site with cloud extensions. These configurations do not require external gateways or appliances, as outlined in the previous section is determining the amount of storage required for specific configurations, and the Optional Cloud Cache.

Figure 17 Example Site Configurations with ScaleProtect with Cisco UCS



There are multiple configurations that are possible, beyond the ones listed in the above figure, these examples highlight some of the common deployment scenarios. It also highlights when the Cloud Cache should be utilized.

Architecture for a single site with no other replication copies being generated is a simple configuration, simply size the require amount of storage to house the data protection workload and deploy the node combination. All of the relevant hardware is in the solution, and the optional Cloud Cache is not required.

Dual site configurations, similar to single site configurations do not require the Cloud Cache, however the sizing of the solution assumes that some or all of the copies in each site will be copied, therefore the sizing of the solution in each site must include enough to maintain dual copies.

The optional Cloud Cache adds the ability to add an independently maintained copy of deduplicated data in a supported cloud provider. There are typically two main use cases for this copy, long term retention of data for compliance or regulatory requirements, or as part of a disaster recovery strategy to the cloud. This optional cache is sized to match the primary workload so there are no additional sizing considerations required to manage the footprint.

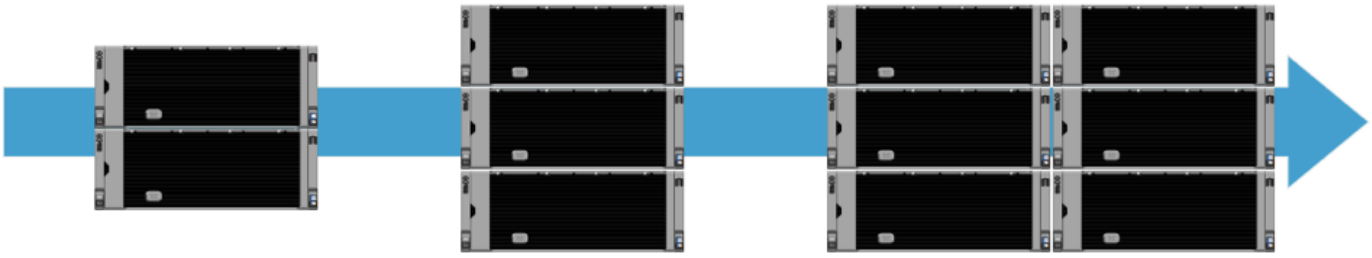
Scalability

Deployment of ScaleProtect with Cisco UCS solution can be easily scaled with additional UCS servers. Cisco UCS S3260 chassis can be physically connected to any of the open ports on the Cisco UCS 6300 Series Fabric Interconnects. When connected, the new Cisco UCS servers can be seamlessly deployed in to the architecture by creating additional Cisco UCS service profiles using Cisco UCS Manager. All the identity of the servers is stored through Service Profiles that are cloned from templates. When a template is created, a new Service Profile for the additional server can be created and easily applied on the newly added hardware. Addition of new nodes requires racking the nodes physically, connecting the cables and then cloning and applying the Service Profiles.

ScaleProtect with Cisco UCS architecture scales linearly with the addition of new nodes. ScaleProtect linear expansion adds predictable compute and storage capacity and can be done in-line non-disruptively. The data on the existing nodes is automatically redistributed on the new nodes to maintain optimal capacity and performance on the entire cluster. Users can also mix and match multiple generations of hardware for maximum flexibility.

These new nodes distribute the data and services across an increasing amount of nodes. These nodes form together into blocks, and they communicate and expand as the solution criteria requires. Blocks are deployed and expanded in 3, 6, or 12 node configurations which can change the resiliency.

Figure 18 Linear Scale with ScaleProtect with Cisco UCS



ScaleProtect with Cisco UCS Sizing

The ScaleProtect with Cisco UCS solution is a rapidly scalable solution that can start small and incrementally scale as required. As outlined in the Commvault HyperScale Storage Resiliency section, the choice of erasure coding and resiliency schemes will determine the deployment and scaling method for the cluster. Choosing a resiliency scheme based on 3 node increments the solution scales in increments of 3 – 3, 6, 9, 12, etc. Alternatively,

selecting a resiliency scheme based on 6 node increments the solution scales in increments of 6 – 6, 12, 18, 24, etc.

When sizing an initial ScaleProtect for Cisco UCS it is best practice to utilize the same node type and size in the configuration. This will help ensure the even distribution of the data across nodes and minimize additional overhead. There is no requirement to go with the same HDD sizes inside of the same tier, it can be mixed and matched inside a configuration it will just mean that the HDDs with the larger capacity will have additional utilization versus the smaller drivers.

Sizing a ScaleProtect with Cisco UCS solution is simple, the table below shows sizing up to the first 15 nodes, simply size the required amount of storage for the data protection solution. Keep in mind it's always a good idea to size for some additional expansion of the solution as data sets continue to grow.

With the addition of the optional Cloud Cache deduplicating data into a supported cloud provider is added directly from the ScaleProtect with Cisco UCS nodes. These copies can be used for long term retention or as part of a disaster recovery strategy. The nodes provide the ability to deduplicate data into the cloud for these secondary copies with the addition of optional Cloud Cache.

Table 3 **ScaleProtect with Cisco UCS Hardware Solution Sizing**

Cisco UCS Model	HDD Size[1]	3 Node Usable[2]	6 Node Usable[2]	9 Node Usable[2]	12 Node Usable[2]	15 Node Usable[2]
Cisco UCS S3260 M5 (24 Drives per node)	4 TB	174 TiB	349 TiB	523 TiB	698 TiB	873 TiB
	6 TB	261 TiB	523 TiB	785 TiB	1047 TiB	1309 TiB
	8 TB	349 TiB	698 TiB	1047 TiB	1396 TiB	1746 TiB
	10 TB	436 TiB	873 TiB	1309 TiB	1746 TiB	2182 TiB
	12 TB	523 TiB	1047 TiB	1571 TiB	2095 TiB	2619 TiB
Optional Cloud Cache[3]	N/A	600 TiB	1200 TiB	1800 TiB	2400 TiB	3000 TiB

1. HDD capacity values are calculated using Base10 (e.g. 1TB = 1,000,000,000,000 bytes)
2. Usable capacity values are calculated using Base2 (e.g. 1TiB = 1,099,511,627,776 bytes), post erasure coding
3. Optional cloud capacity is in addition to the ScaleProtect with Cisco UCS on-premises architecture.

Physical Topology and Configuration

This section describe the physical design of the validated solution and the configuration of each component.

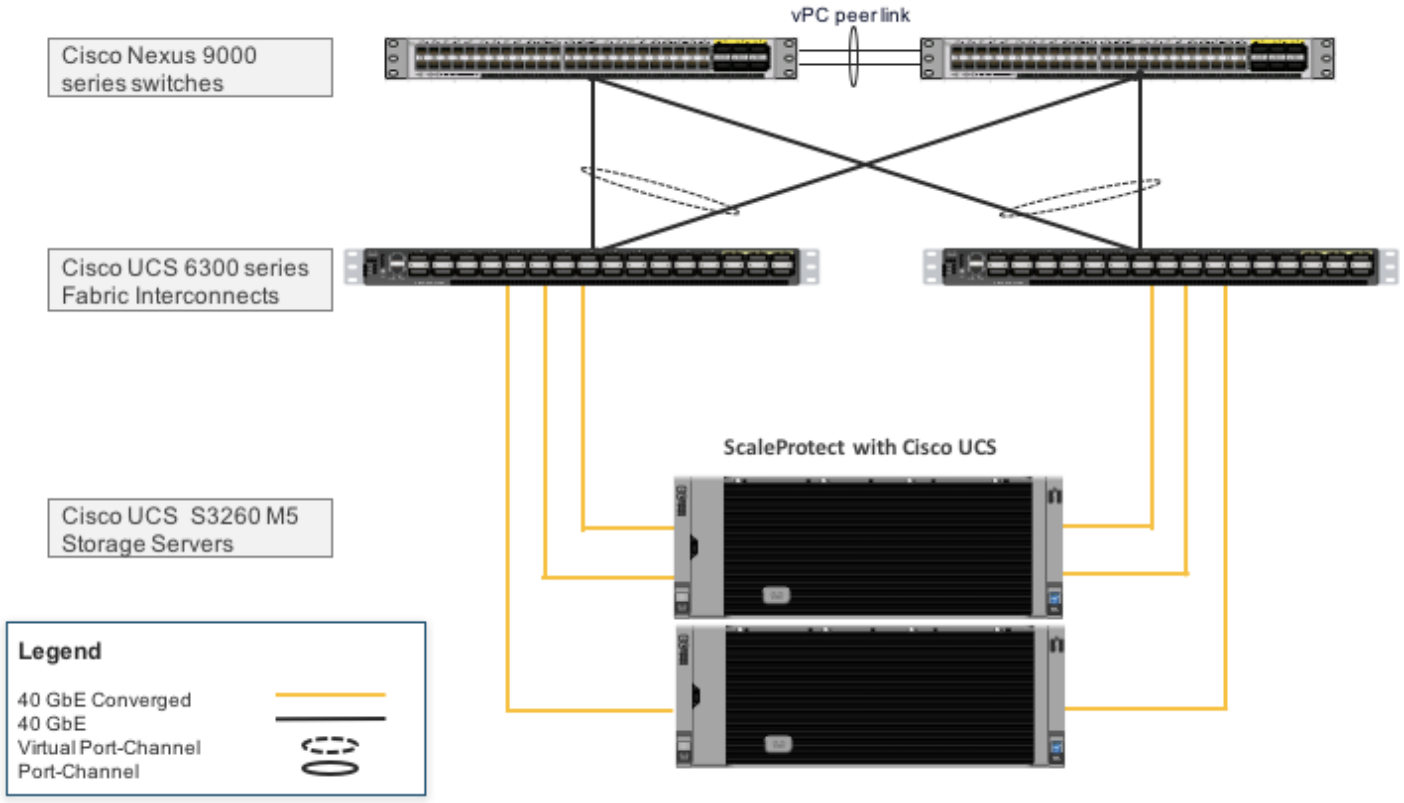
The detailed configuration is as follows:

- 2 x Cisco Nexus 9332PQ Switches
- 2 x Cisco UCS 6332 Fabric Interconnects
- 2 x Cisco UCS S3260 Storage Servers with 3 x Cisco UCS S3260 M5 Server Nodes

Physical Topology

This design deploys a single pair of Nexus 9000 top-of-rack switches, using the traditional standalone mode running NX-OS and has end-to-end 40 Gb Ethernet connections between the Cisco UCS Storage Servers and the Cisco UCS Fabric Interconnects, and between the Cisco UCS Fabric Interconnect and Cisco Nexus 9000. Cisco Nexus 9000 provides Ethernet switching fabric for communications between the ScaleProtect with Cisco UCS environment and the enterprise network. In this design, Cisco UCS Fabric Interconnects are connected to the Cisco Nexus 9000 switches using virtual Port Channels (vPC).

Figure 19 ScaleProtect with Cisco UCS S3260 – 3 Node Physical Topology



For validation, Cisco UCS S3260 M5 servers with VIC 1380 adapters included with System I/O Controller (SIOC) were connected to 2 x Cisco UCS 6332 Fabric Interconnects. Each Cisco UCS S3260 server node is deployed with a single SIOC to connect to the UCS fabric interconnects. Two 40GbE links were used for SIOC to FI connectivity, one from port-0 to FI-A and one from port-1 to FI-B, for an aggregate access bandwidth of 80Gbps from the blade server chassis to the unified fabric.

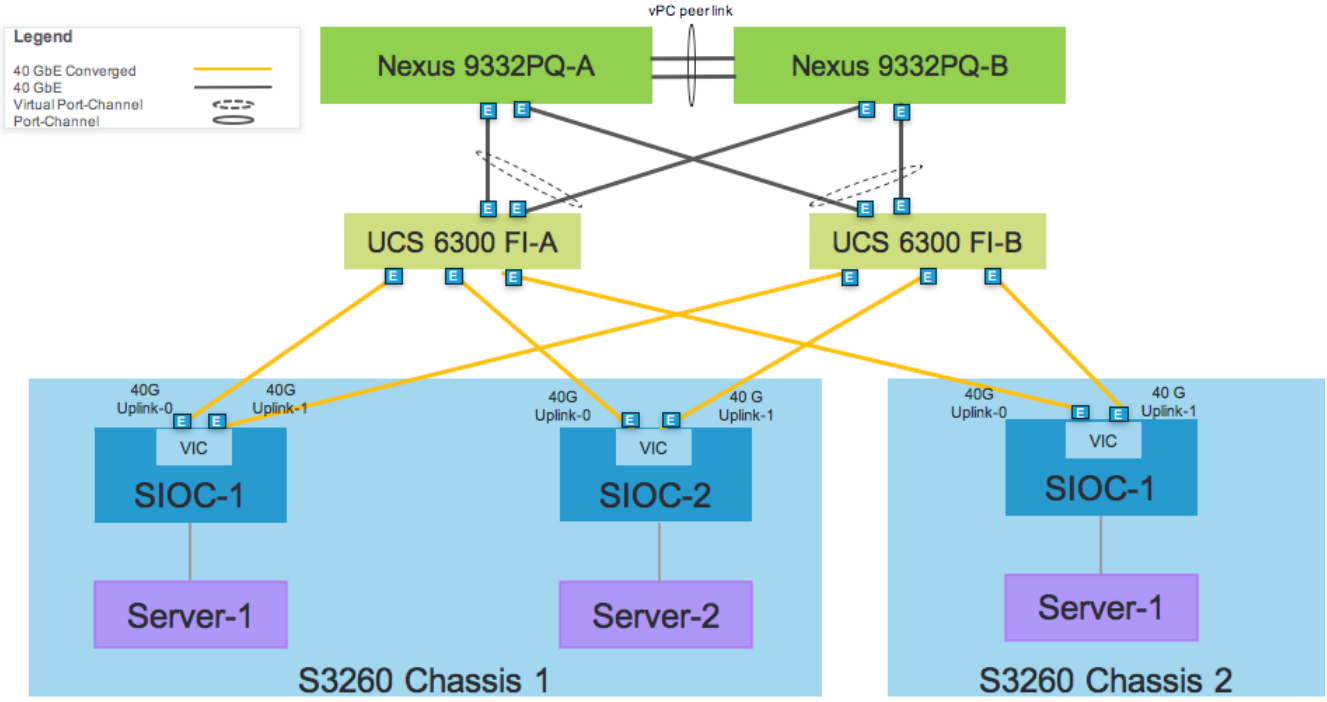
Connectivity from each individual UCS fabric interconnect, to all upstream or northbound (NB) networks is provided by 2 x 40G links to each of the top-of-rack Cisco Nexus switches as follows:

- 2 x 40G uplinks from FI-A to Nexus-A and Nexus-B respectively
- 2 x 40G uplinks from FI-B to Nexus-A and Nexus-B respectively

Both uplinks are configured into a single port channel, making the total aggregate bandwidth to the core switching infrastructure 80Gbps per UCS fabric interconnect. Each port designated as a core switch connection is designated as an uplink port within Cisco UCS Manager.

The switches are configured as vPC peers. vPCs are used to provide switch-level redundancy to the Cisco UCS fabric interconnects and S3260 servers without requiring special configuration on those devices. The switches in this solution are operating in NX-OS mode but could also be configured as leaves in an ACI network.

Figure 20 ScaleProtect with Cisco UCS S3260 Physical Connectivity



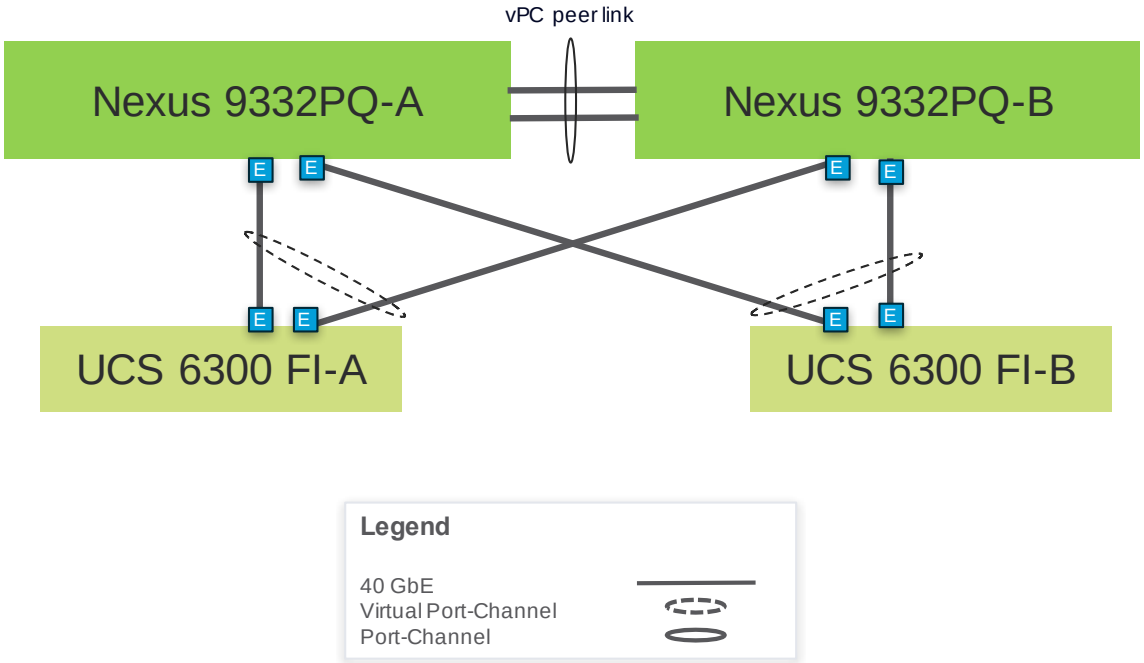
Network Design

In this ScaleProtect with Cisco UCS design, a pair of redundant Cisco Nexus 9332 switches provide Ethernet switching fabric for communication with the production infrastructure for data protection in existing enterprise networks.

Virtual Port Channel Configuration

Network reliability is attained through the configuration of virtual Port Channels within the design as shown in Figure 21.

Figure 21 Network Design – vPC Enabled Connections



Virtual Port Channel allows Ethernet links that are physically connected to two different Cisco Nexus 9000 Series devices to appear as a single Port Channel. vPC provides a loop-free topology and enables fast convergence if either one of the physical links or a device fails. In the design, when possible, vPC is a preferred mode of Port Channel configuration.

vPC on Nexus switches running in NXOS mode requires a peer-link to be explicitly connected and configured between peer-devices (Nexus 9332 switch pair). In addition to the vPC peer-link, the vPC peer keepalive link is a required component of a vPC configuration. The peer keepalive link allows each vPC enabled switch to monitor the health of its peer. This link accelerates convergence and reduces the occurrence of split-brain scenarios. In this validated solution, the vPC peer keepalive link uses the out-of-band management network.

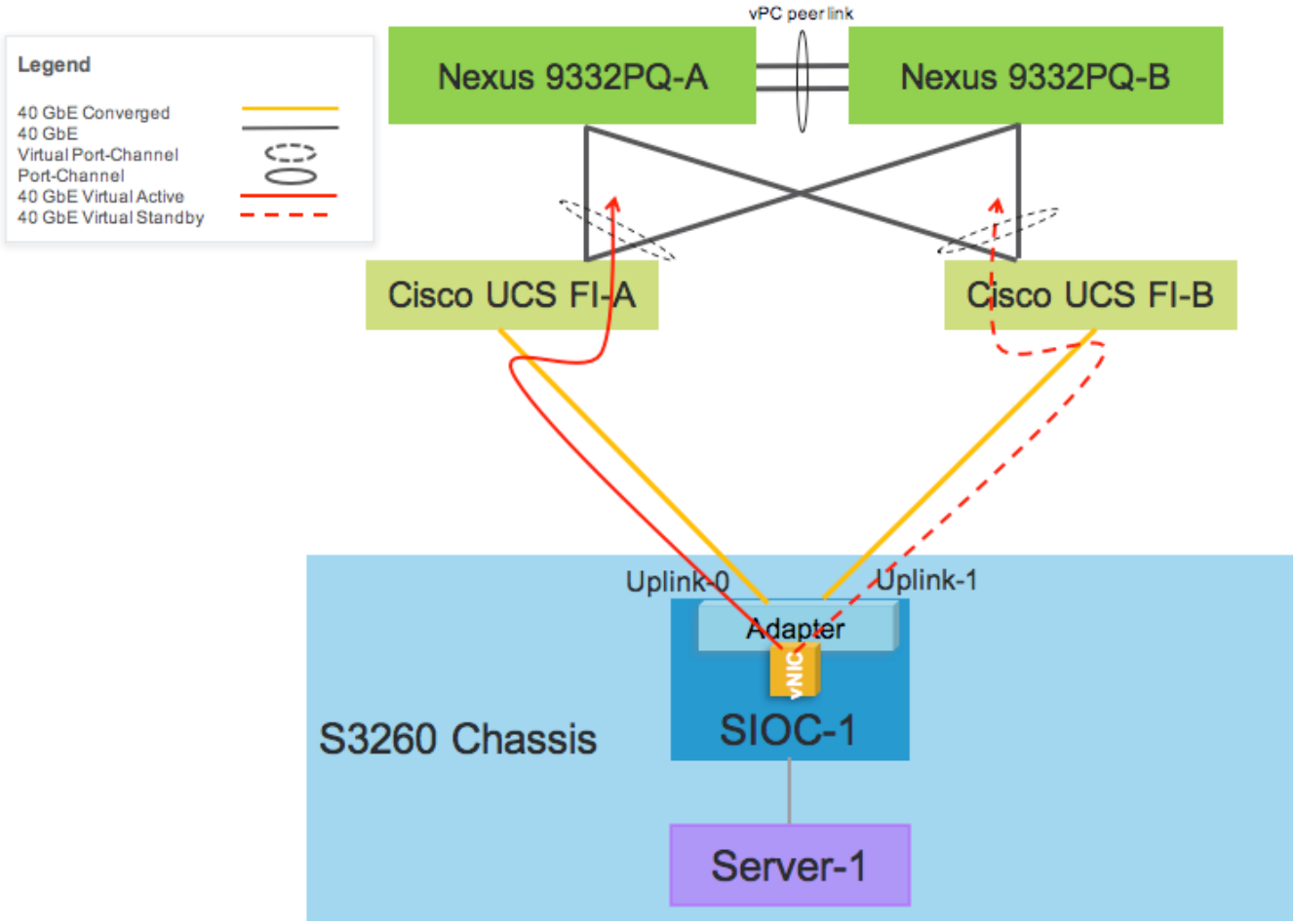
Fabric Failover for Ethernet: High-Availability vNIC

Each adapter in Cisco UCS is a dual-port adapter that connects to both fabrics (A and B). The two fabrics in Cisco UCS provide failover protection in the event of planned or unplanned component downtime in one of the fabrics.

A vNIC in Cisco UCS is a host-presented PCI device that is centrally managed by Cisco UCS Manager. The fabric-based failover feature, which is enabled by selecting the high-availability vNIC option in the service profile definition, allows Cisco Virtual Interface Card (VIC) cards and the fabric interconnects to provide active-standby failover for Ethernet vNICs without any NIC-teaming software on the host. Host software (MPIO) is still required to handle failover for Fibre Channel virtual HBAs (vHBAs).

Cisco UCS fabric failover is an important feature because it reduces the complexity of defining NIC teaming software for failover on the host. It does this transparently in the fabric based on the network property that is defined in the service profile. For traffic failover, the fabric interconnect in the new path sends gratuitous Address Resolution Protocols (gARPs). This process refreshes the forwarding tables on the upstream switches.

Figure 22 Cisco UCS vNIC Fabric Failover



ScaleProtect with Cisco UCS Server Configuration

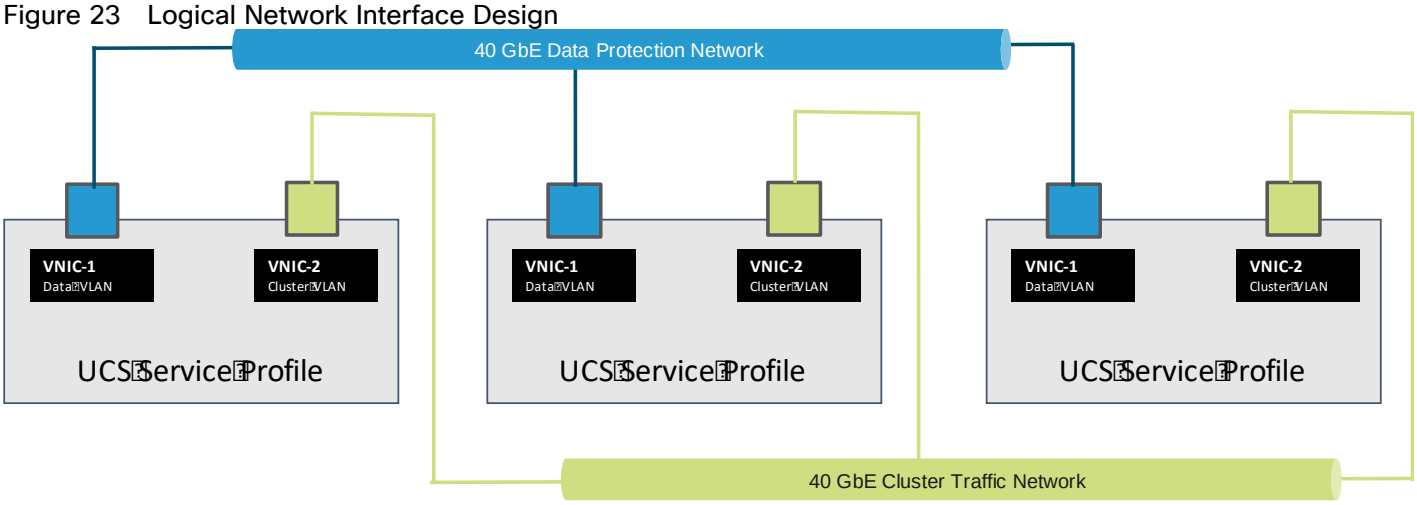
The ScaleProtect with Cisco UCS nodes consist of Cisco UCS S3260 M5 servers with Cisco 1380 VIC included with the SIOC. These nodes are allocated to the cluster. At the server level, the Cisco 1380 VIC presents multiple virtual PCIe devices to the UCS node and the operating system identifies these interfaces as VMnics or VMhbas. The operating system is unaware of the fact that the NICs or HBAs are virtual adapters.

In the ScaleProtect with Cisco UCS design, two vNICs are created and utilized as follows:

- One vNIC for data protection traffic
  - Primary fabric A, with failover to fabric B
- One vNIC for cluster traffic
  - Primary fabric B, with failover to fabric A

Each node has a cluster VLAN and a data protection VLAN. The cluster VLAN deals with inter-node traffic while the data protection VLAN is used for communication with the Commvault management server and the enterprise infrastructure. Resilience is ensured by enabling Cisco UCS fabric failover for the vNICs within Cisco UCS service profiles.

Figure 23 Logical Network Interface Design



ScaleProtect with Cisco UCS Node Disk Layout

A ScaleProtect with Cisco UCS node can houses the processing capability at the node level for all data protection functionality, including deduplication, indexing, storage resiliency, and for accepting client data. The layout of the nodes is as follows:

- Boot Volume – 2x 480GB SSDs
  - Configured in RAID 1
- Accelerated Cache Volume – 4x 1.6TB SSDs
  - Configured in RAID 5
- Software Defined Storage Tier – 24x NL-SAS HDDs (Option of 4/6/8/12 TB sizes)
  - Configured in Pass-through (JBOD) mode

The following diagrams depict the disk layout of single server node and dual server nodes respectively:

Figure 24 Single Node Disk Layout

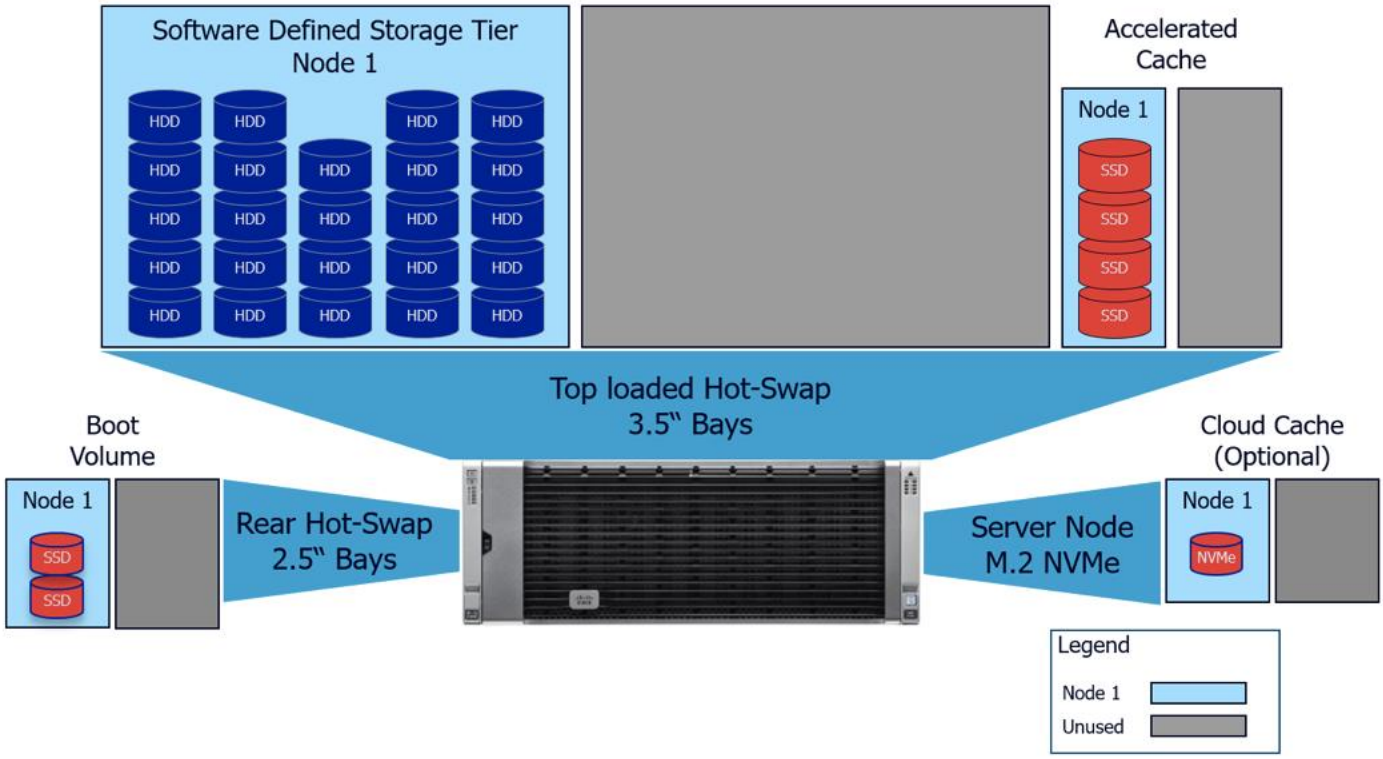
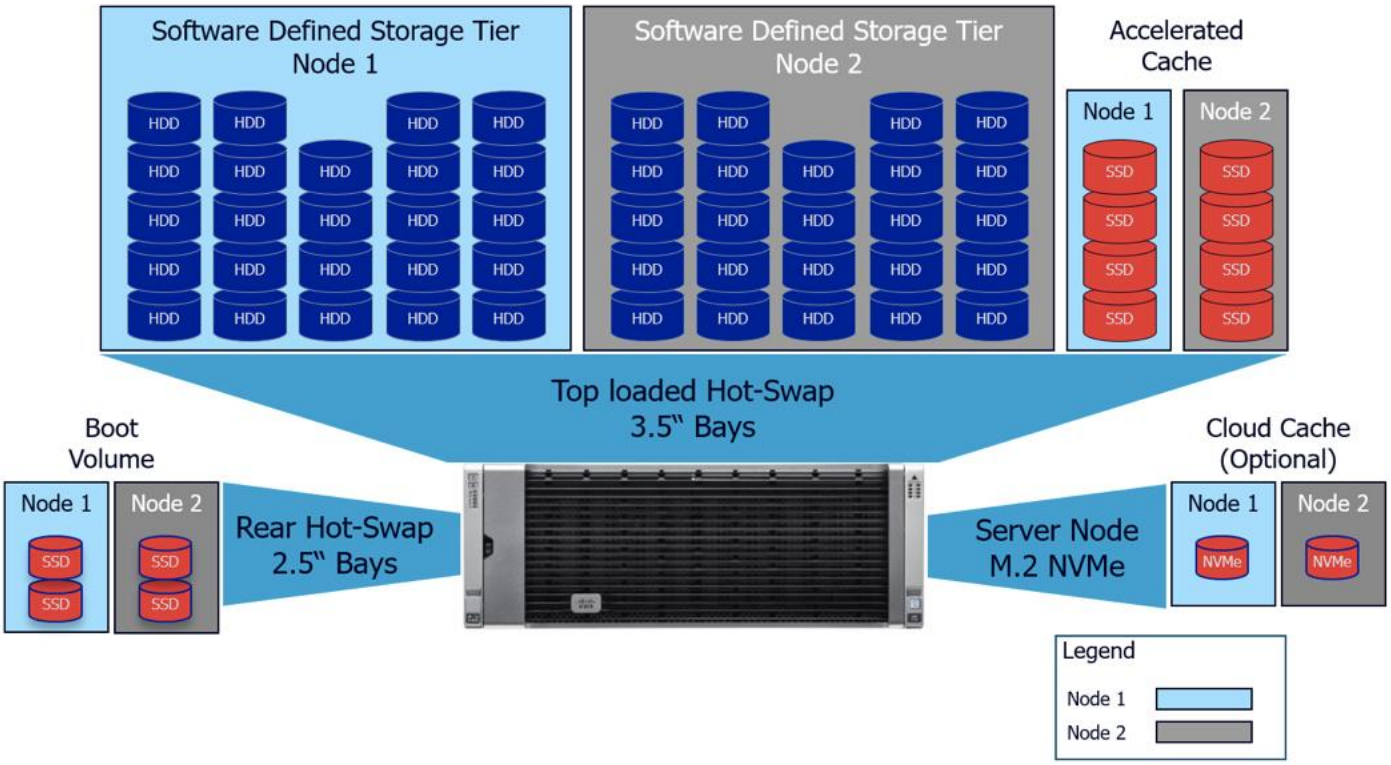


Figure 25 Dual Node Disk Layout



Other Design Considerations

The following sections outline other design considerations for the ScaleProtect with Cisco UCS solution and a few additional design selection options available to the customers.

Cisco UCS Management Connectivity

The ScaleProtect with Cisco UCS design uses a separate out-of-band management network to configure and manage compute and network components in the solution. Management ports on each physical device (Cisco UCS FI and Cisco Nexus switches) in the solution are connected to a separate, dedicated management switch.

Cisco UCS 6300 Fabric Interconnects

The third generation of Cisco Unified Fabric used in this solution is designed to fit easily into a Cisco UCS environment comprising Cisco UCS fabric extenders, VICs, and Cisco Nexus 9300 platform switches. Cisco UCS 6300 Series Fabric Interconnects have been carefully designed to combine the cost-saving advantages of merchant silicon with custom Cisco innovations. They provide an intelligent progression from previous-generation fabric interconnects. Two Cisco UCS 6332 models; Cisco UCS 6332 and Cisco UCS 6332-16UP are offered to provide deployment flexibility. The specific switch model has to be selected based on the customers' requirements in having connectivity to SAN fabrics.

The Cisco UCS 6332 32-Port Fabric Interconnect is a one-rack-unit (1RU) 40-GbE switch offering up to 2.56 Tbps full-duplex throughput. The switch has 32 40-Gbps QSFP+ ports and should be deployed with ScaleProtect with Cisco UCS when fibre channel connectivity to the existing SAN is not a requirement.

Other Design Considerations

The following sections outline other design considerations for the ScaleProtect with Cisco UCS solution and a few additional design selection options available to the customers.

Cisco UCS Management Connectivity

The ScaleProtect with Cisco UCS design uses a separate out-of-band management network to configure and manage compute and network components in the solution. Management ports on each physical device (Cisco UCS FI and Cisco Nexus switches) in the solution are connected to a separate, dedicated management switch.

Cisco UCS 6300 Fabric Interconnects

The third generation of Cisco Unified Fabric used in this solution is designed to fit easily into a Cisco UCS environment comprising Cisco UCS fabric extenders, VICs, and Cisco Nexus 9300 platform switches. Cisco UCS 6300 Series Fabric Interconnects have been carefully designed to combine the cost-saving advantages of merchant silicon with custom Cisco innovations. They provide an intelligent progression from previous-generation fabric interconnects. Two Cisco UCS 6332 models; Cisco UCS 6332 and Cisco UCS 6332-16UP are offered to provide deployment flexibility. The specific switch model has to be selected based on the customers' requirements in having connectivity to SAN fabrics.

The Cisco UCS 6332 32-Port Fabric Interconnect is a one-rack-unit (1RU) 40-GbE switch offering up to 2.56 Tbps full-duplex throughput. The switch has 32 40-Gbps QSFP+ ports and should be deployed with ScaleProtect with Cisco UCS when fibre channel connectivity to the existing SAN is not a requirement.

The Cisco UCS 6332-16UP 40-Port Fabric Interconnect is a 1RU 10-GbE, 40-GbE, and native fibre channel switch offering up to 2.43-Tbps full-duplex throughput. The ScaleProtect with Cisco UCS design should include this switch model when connectivity to existing SAN fabrics is a requirement. Fibre channel connectivity is used

mainly for backup to fibre channel tape or when IntelliSnap™ technology will be used for LAN-free backup directly from storage snapshots.

Jumbo Frames

Jumbo frames are a standard recommendation across Cisco designs to help leverage the increased bandwidth availability of modern networks. To take advantage of the bandwidth optimization and reduced consumption of CPU resources gained through jumbo frames, all networks in this design can have jumbo frames enabled across the entire path of all network components and the backup clients if supported. Use standard 1500 MTU if any connections or devices are not configured to support a larger MTU to prevent drops.

Check with your network administrator and server administrator to determine which MTU value is ideal for your deployment.

Network Uplinks

Depending on the available network infrastructure, several methods and features can be used to uplink the ScaleProtect environment to customers' existing infrastructure. If an existing Cisco Nexus environment is present, its recommended using vPCs to uplink the Cisco Nexus 9332 switches included in the ScaleProtect environment into the infrastructure. The network uplinks from fabric interconnects provide upstream connectivity to the Nexus switches and to the existing customer's infrastructure.

While there is a complete high availability built in the ScaleProtect infrastructure, the performance may degrade during device failures or maintenance activities depending on the uplink connections from each FI to the Nexus switches, in the case of such failures or reboots, increase the uplink connections as well to ensure proper bandwidth is available.

NIC Bonding versus Cisco UCS Fabric Failover

ScaleProtect with Cisco UCS network requirements are standard Ethernet only, while Commvault HyperScale Software can work with two network interfaces in bonded mode for each traffic type (data protection VLAN and cluster VLAN), it is recommended to use a single network interface for each traffic type and enable Cisco UCS Fabric Failover for resiliency versus NIC bonding in the operating system. With Cisco UCS Fabric Failover the management and operation of failover and link aggregation is handled in the networking fabric. The Fabric Failover is enabled in the vNIC templates with in the Cisco UCS service profiles which makes it easy to implement NIC resiliency across any number of servers managed by Cisco UCS, this eliminates the need to configure every server individually.

NIC teaming is often implemented to aggregate lower-speed NICs in order to gain throughput. Since ScaleProtect with Cisco UCS leverages 40GbE connections, aggregation is generally not required.

Deployment Hardware and Software

The deployment of hardware and software for ScaleProtect with Cisco UCS is detailed in the following sections.

ScaleProtect with Cisco UCS on S3260 Servers and Software Revisions

Table 4 Hardware and Software Revisions Validated

Layer	Device	Image
Compute	Cisco UCS 6300 Series Fabric Interconnects	4.0(1a)
	Cisco UCS S3260 Storage Server	4.0(1a)
Network	Cisco Nexus 9332PQ NX-OS	9.2(1)
Software	Cisco UCS Manager	4.0(1a)
	Commvault Complete Backup and Recovery	v11 Service Pack 13
	Commvault HyperScale Software	v11 Service Pack 13

Bill of Materials

To find various components of ScaleProtect with Cisco UCS system, complete the following steps:

1. Go to the Main CCW page: https://apps.cisco.com/Commerce/home.
2. Under Find Products and Solutions, click the Search for solutions.
3. Type Commvault. System will pull all the Commvault data protection solution variations.
4. Select one of the solutions and click View Components.

Refer to Error! Reference source not found. for key solution components:

Table 5 ScaleProtect with Cisco UCS S3260 Bill of Materials

Component	Model	Quantity	Comments
UCS Fabric Interconnects	Cisco UCS 6332 Fabric Interconnects	2	
Network Switches	Cisco Nexus 9332PQ Switches	2	
Cisco UCS S3260 Storage Servers	Cisco UCS S3260 Chassis & M5 Server Nodes	2	3 X UCS S3260 M5 Server Nodes (1 X Single Node UCS S3260 Chassis and 2 X Dual Node UCS S3260 Chassis)

Validation

Test Plan

This section provides the details about the tests conducted by the team, validating the design, and the implementation aspects of this solution.

A high-level summary of the ScaleProtect with Cisco UCS on S3260 M5 Storage Servers validation is provided in this section.

Validation

The system was validated for resiliency by failing various aspects of the system under load. Examples of the types of tests executed include:

- Failure and recovery of links from Cisco UCS S3260 Chassis to FI-A and FI-B, one at a time
- Failure and recovery of links with in vPC from Cisco UCS FI and Cisco Nexus 9332 switches
- Fail/power off both Cisco 9332 switches, one after other
- Failure and recovery of Cisco UCS S3260 M5 server node
- Failure and recovery of SSD and capacity HDD
- Backup and recovery of VMs, physical clients and applications.

More information regarding deployment guidelines, sizing practices and high availability about the deployment steps with any other best practices discovered as part of the setup will be documented in the Deployment guide.

References

Products and Solutions

Cisco Unified Computing System:

http://www.cisco.com/en/US/products/ps10265/index.html

Cisco UCS 6300 Series Fabric Interconnects:

https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-6300-series-fabric-interconnects/index.html

Cisco UCS S-Series Storage Servers

https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-s-series-storage-servers/index.html

Cisco UCS C-Series Rack Servers:

http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html

Cisco UCS Adapters:

http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html

Cisco UCS Manager:

http://www.cisco.com/en/US/products/ps10281/index.html

Cisco Nexus 9000 Series Switches:

http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

Commvault Complete Backup and Recovery:

https://www.commvault.com/solutions/by-function/data-protection-backup-and-recovery

Commvault HyperScale Software:

https://www.commvault.com/solutions/by-function/cloud-and-infrastructure-management/hyperscale

ScaleProtect with Cisco UCS:

https://www.commvault.com/solutions/by-technology/infrastructure/cisco-ucs/scaleprotect

Summary

ScaleProtect with Cisco UCS provides enterprises a single, hyperconverged solution that delivers infrastructure simplicity, elasticity, resiliency, flexibility and scale for managing secondary data, while replacing legacy back-up tools with a modern cloud-enabled data management solution. ScaleProtect with Cisco UCS delivers these benefits as well as seamless integration with storage arrays, hypervisors, applications and the full range of cloud provider solutions to support the most diverse and dynamic enterprise and hybrid cloud environments.

ScaleProtect with Cisco UCS delivers the powerful simplicity of Commvault Complete Backup & Recovery in a highly available, scale-out integrated solution. With ScaleProtect with Cisco UCS today, you can build a fully modern data protection solution with cloud-like services in an easy-to-use unified platform. It is simple to buy, install, manage, upgrade, and support. Cisco and Commvault are delivering a modern approach to data management and providing Customers even greater choice for solving their data protection and management challenges. ScaleProtect with Cisco UCS allows customers to decouple their data strategy from their storage infrastructure strategy.

About the Authors

Sreenivasa Edula, Technical Marketing Engineer, Cisco UCS Data Center Solutions Engineering, Cisco Systems, Inc.

Sreeni is a Technical Marketing Engineer in the Cisco UCS Data Center Solutions Engineering team focusing on converged and hyper-converged infrastructure solutions, prior to that he worked as a Solutions Architect at EMC Corporation. He has experience in Information Systems with expertise across Cisco Data Center technology portfolio, including DC architecture design, virtualization, compute, network, storage and cloud computing.

Jonathan Howard, Director, Commvault Systems, Inc.

Acknowledgements

- Ulrich Kleidon, Cisco Systems, Inc.
- Nivas Iyer, Cisco Systems, Inc.
- Bryan Clarke, Commvault Systems, Inc.
- John Pham, Commvault Systems, Inc.