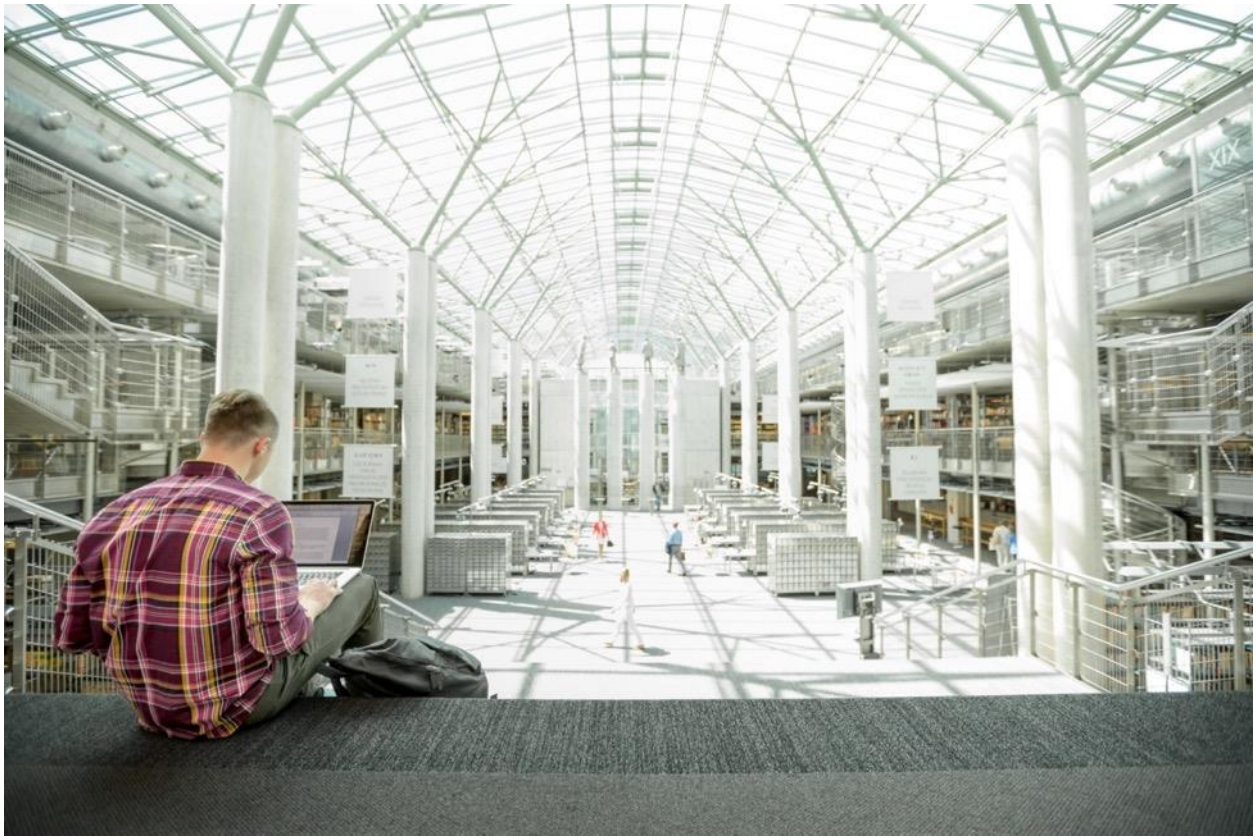


Cisco UCS for ScaleProtect with Cisco UCS Servers Design Guide

Last Updated: October 8, 2019

CISCO VALIDATED DESIGN

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, go to:

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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Table of Contents

Executive Summary 5

Solution Overview 6

- Introduction 6
- Audience 6
- Purpose of this Document 6
- Solution Summary 6
- What's New? 7
- Solution Benefits 8

Technology Overview 9

- Cisco Unified Computing System 10
  - Cisco UCS Manager 10
  - Cisco UCS Fabric Interconnects 10
  - 2nd Generation Intel® Xeon® Scalable processors 12
  - Cisco UCS S3260 Storage Server ScaleProtect Node 12
  - Cisco UCS C-Series ScaleProtect Nodes 12
  - Cisco UCS Virtual Interface Card 1387 and 1457 13
- Cisco Nexus 9300 Switches 13
- Commvault® Software 14
  - Commvault Complete™ Backup & Recovery 14
  - Commvault HyperScale™ Software 15

Solution Design 18

- Design Overview with Cisco UCS S3260 Storage Servers 18
  - Cisco UCS S3260 Node Hardware Overview 20
- Design Overview with Cisco UCS C-Series Rack Servers 21
- ScaleProtect with Cisco UCS Site Configuration Options 23
- Resiliency 24
  - ScaleProtect Fabric Resiliency 24
  - Compute Resiliency 24
  - Commvault ScaleProtect Storage Resiliency 24
- Scalability 25
- ScaleProtect with Cisco UCS Sizing 26
- Physical Topology and Configuration 27
  - Network Fabric 27
  - ScaleProtect with Cisco UCS S3260 Physical Topology 28
  - ScaleProtect with Cisco UCS C-Series Physical Topology 30
  - Cisco UCS Network Interface Configuration 31

Fabric Failover for Ethernet: High-Availability vNIC 32
ScaleProtect with Cisco UCS Node Disk Layout 33
Other Design Considerations 35
Cisco UCS Management Connectivity 36
Cisco UCS Fabric Interconnects 36
Jumbo Frames 36
Network Uplinks 36
Deployment Hardware and Software 38
ScaleProtect with Cisco UCS Servers Software Revisions 38
Bill of Materials 38
Validation 40
Test Plan 40
Validation 40
References 41
Products and Solutions 41
Summary 42
About the Authors 43
Acknowledgements 43

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, focusing on the Cisco UCS S3260 Storage Server and Cisco UCS C-Series platforms. 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, and so on).

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, Cisco UCS C240 M5 LLF and Cisco UCS C220 M5 LLF servers for use with ScaleProtect for Cisco UCS. The design guide will be 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 design details and best practices to design a ScaleProtect with Cisco UCS solution.

Solution Summary

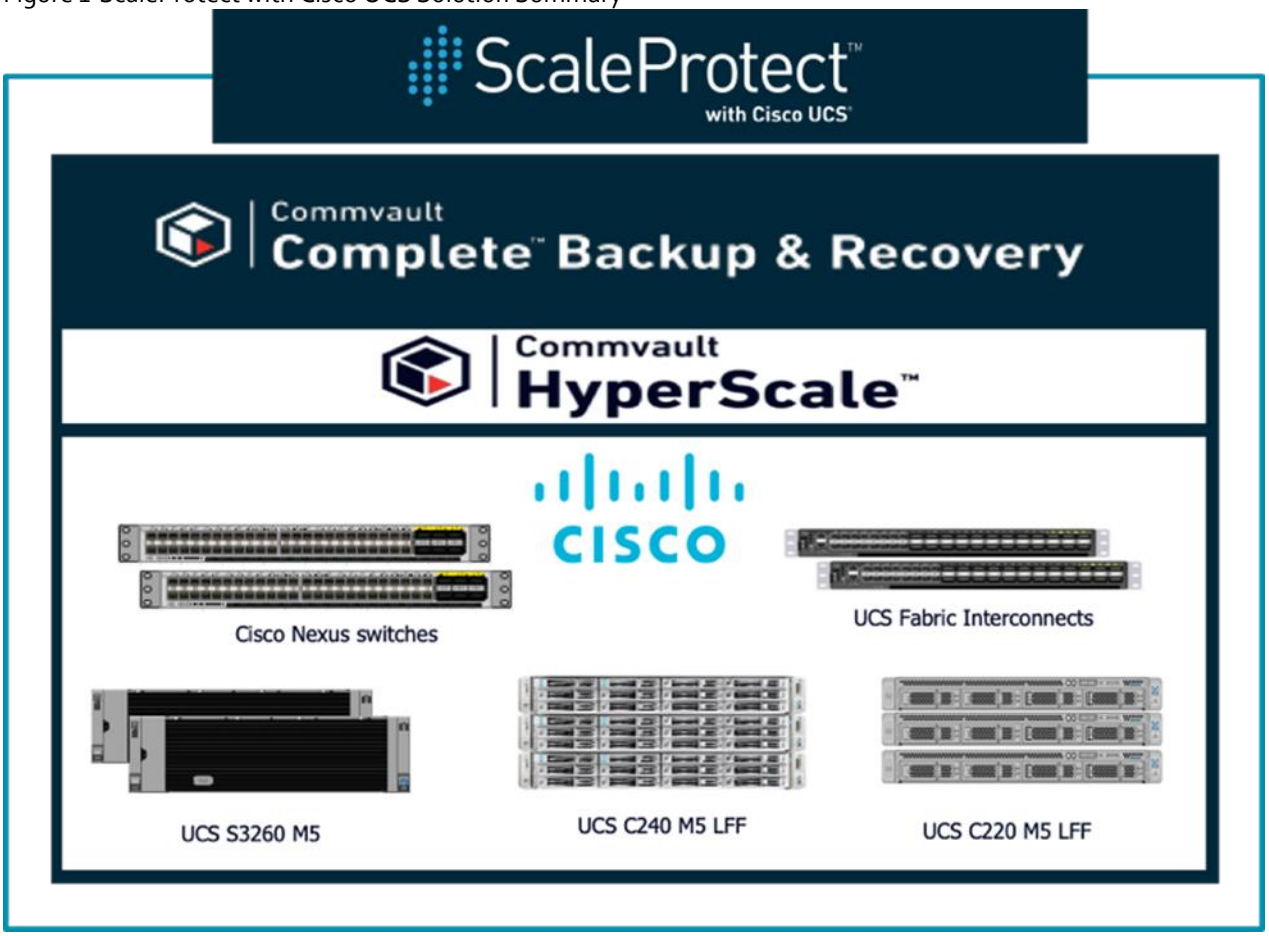
Cisco UCS revolutionized the server market through its programmable fabric and automated management that simplify application and service deployment. Commvault HyperScale™ Software provides the software-defined scale-out architecture that is fully integrated and includes true hybrid cloud capabilities. 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



What's New?

The addition of the following design elements distinguishes this version of ScaleProtect with Cisco UCS from previous models:

- Cisco UCS release 4.0(4b)
- Commvault Hyperscale release 11 SP16
- Cisco UCS C240 M5 Servers
- Cisco UCS C220 M5 Servers
- Cisco UCS 6454 Fabric Interconnects
- Second-generation Intel Xeon Scalable processors

Solution Benefits

ScaleProtect with Cisco UCS improves efficiency and reduces downtime with modern data protection and live recovery. It helps improve data backup and recovery processes regardless of where the 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. The solution enables customers to gain long-term value with modular scalability that lets the solution grow with their business. Increases infrastructure flexibility, removes data silos and costly appliances and introduce elastic economics for customers 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 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 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

This section provides a technical overview of the compute, network, storage and management components in this solution.

The solution consists of three different designs options, which are based on Cisco UCS S3260 M5 Storage Servers and Cisco UCS C-Series M5 server models. Customers can choose the solution design based on the storage capacity needs they have for backup infrastructure and future expansions. Following are the three ScaleProtect with Cisco UCS Servers design options:

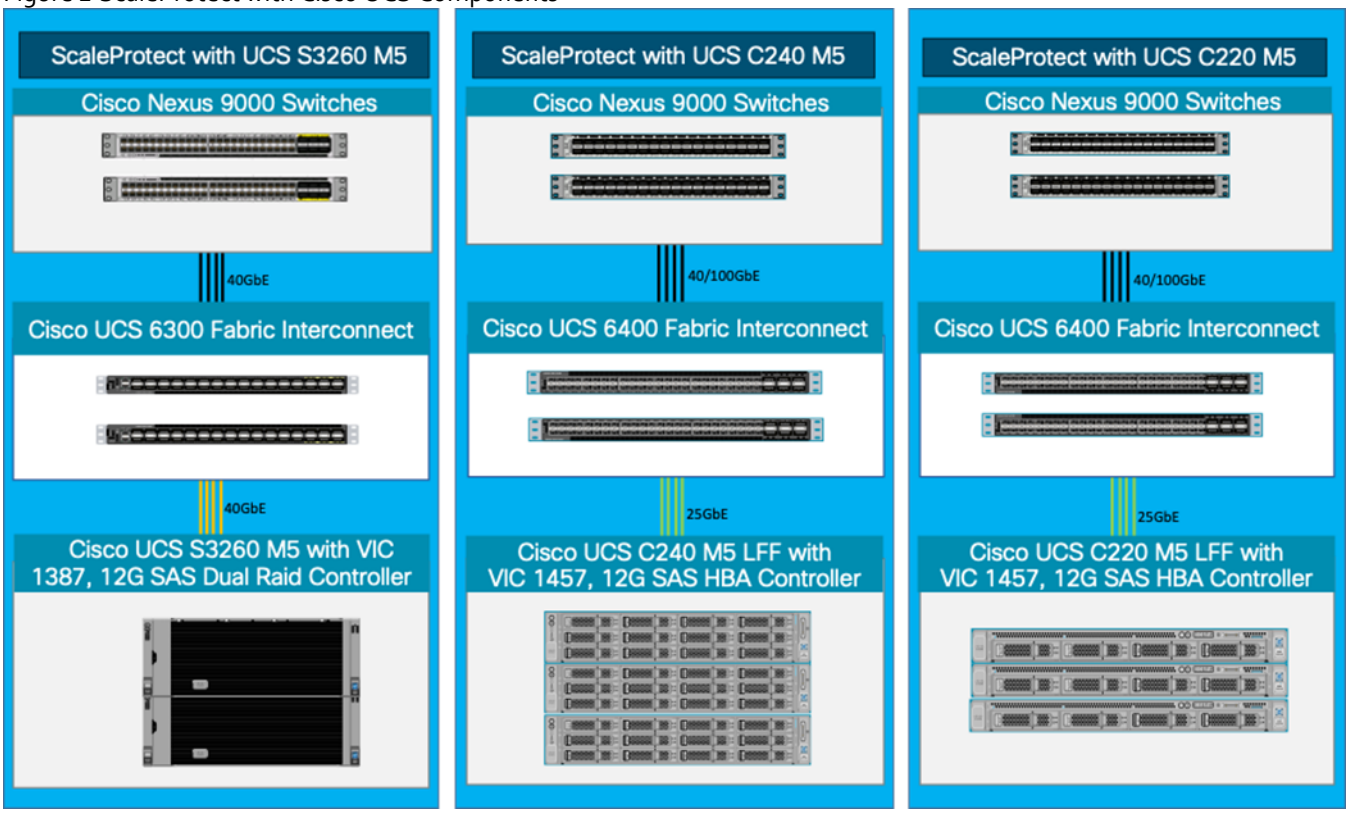
- ScaleProtect with Cisco UCS S3260 M5 Storage Servers
- ScaleProtect with Cisco UCS C240 M5 LFF Servers
- ScaleProtect with Cisco UCS C220 M5 LFF Servers

ScaleProtect with Cisco UCS includes the following components:

- Cisco UCS 6332 and Cisco UCS 6454 Fabric Interconnects
- Cisco UCS S3260 M5 Servers, Cisco UCS C240 M5 LFF Servers and Cisco UCS C220 LFF Servers
- Cisco S3260 system IO controller with VIC 1380
- Cisco VIC 1400 Series
- Cisco Nexus 9000 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.

Figure 2 ScaleProtect with Cisco UCS Components



Cisco Unified Computing System

Cisco Unified Computing System™ (Cisco UCS) is a next-generation data center platform that integrates computing, networking, storage access, and virtualization resources into a cohesive system designed to reduce total cost of ownership and increase business agility. The system integrates a low-latency, lossless unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform with a unified management domain for managing all resources.

Cisco UCS Manager

Cisco UCS® Manager (UCSM) provides unified, integrated management for all software and hardware components in Cisco UCS. UCSM manages, controls, and administers multiple blades and chassis enabling administrators to manage the entire Cisco Unified Computing System as a single logical entity through an intuitive GUI, a CLI, as well as a robust API. Cisco UCS Manager is embedded into the Cisco UCS Fabric Interconnects and offers a comprehensive set of XML API for third party application integration. Cisco UCS Manager exposes thousands of integration points to facilitates custom development for automation, orchestration, and to achieve new levels of system visibility and control.

Cisco UCS Fabric Interconnects

The Cisco UCS Fabric Interconnects (FIs) provide a single point for connectivity and management for the entire Cisco Unified Computing System. Typically deployed as an active-active pair, the system's fabric interconnects integrate all components into a single, highly-available management domain controlled by the Cisco UCS Manager. Cisco UCS FIs provide a single unified fabric for the system, with low-latency, lossless, cut-through switching that supports LAN, SAN and management traffic using a single set of cables. ScaleProtect with Cisco UCS leverages 6300 and 6400 series Fabric Interconnects in the solution designs.

Cisco UCS 6300 Fabric Interconnects

The Cisco UCS 6300 Series Fabric Interconnects are featured in ScaleProtect with Cisco UCS S3260 Storage Servers Design. The Cisco UCS 6300 Series are 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.

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.

The Cisco 6332-16UP Fabric Interconnect offers 40 ports in one rack unit (RU), including:

- 24 40-Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)
- 16 1- and 10-Gbps and FCoE or 4-,8-, and 16-Gbps Fibre Channel unified ports

Figure 3 Cisco UCS 6332 and 6332-16UP Fabric Interconnects

Cisco UCS 6332 Fabric Interconnect	Cisco UCS 6332-16UP Fabric Interconnect
	

Cisco UCS 6454 Fabric Interconnects

The 4th generation (6400) Fabric delivers options for both high workload density, as well as high port count, with both supporting either Cisco UCS B-Series blade servers, or Cisco UCS C-Series rack mount servers. The UCS 6400 Fabric Interconnects are used in the ScaleProtect with Cisco UCS C-Series designs.

Figure 4 Cisco UCS 6454 Fabric Interconnect

The Cisco UCS 6454 Fabric Interconnect is a 54 port 1/10/25/40/100GbE/FCoE switch, supporting 8/16/32Gbps FC ports and up to 3.82Tbps throughput. This model is aimed at higher port count environments that can be configured with 32Gbps FC connectivity to Cisco MDS switches or FC direct attached storage.

Table 1 lists the comparison of the port capabilities of the different Fabric Interconnect models that are part of ScaleProtect with Cisco UCS designs.

Table 1 Cisco UCS 6300 and 6400 Series Fabric Interconnects

Features	UCS FI 6332	UCS FI 6332-16UP	UCS FI 6454
Max 10G ports	96* + 2**	72* + 16	48
Max 25G ports	N/A	N/A	48
Max 40G ports	32	24	6
Max 100G ports	N/A	N/A	6
Max unified ports	N/A	16	8
Max FC ports	N/A	16x 4/8/16G	8x 8/16/32G

* Using 40G to 4x10G breakout cables ** Requires QSA module

2nd Generation Intel® Xeon® Scalable processors

The ScaleProtect with Cisco UCS solution supports 2nd generation Intel Xeon Scalable processors in all the Cisco UCS M5 server models used in this design. These processors provide a foundation for powerful data center platforms with an evolutionary leap in agility and scalability. Disruptive by design, this innovative processor family supports new levels of platform convergence and capabilities across computing, storage, memory, network, and security resources.

Cascade Lake (CLX-SP) is the code name for the next-generation Intel Xeon Scalable processor family that is supported on the Purley platform serving as the successor to Skylake SP. These chips support up to eight-way multiprocessing, use up to 28 cores, incorporate a new AVX512 x86 extension for neural-network and deep-learning workloads, and introduce persistent memory support. Cascade Lake SP–based chips are manufactured in an enhanced 14-nanometer (14-nm++) process and use the Lewisburg chip set.

Cisco UCS S3260 Storage Server ScaleProtect Node

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 5 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 2nd Gen Intel® Xeon® Scalable and Intel Xeon Scalable processor, it features up to 840 TB of local storage in a compact 4-Rack-Unit (4RU) form factor. The drives can be configured with enterprise-class Redundant Array of Independent Disks (RAID) redundancy or with a pass-through Host Bus Adapter (HBA) controller. Network connectivity is provided with dual-port 40-Gbps nodes in each server, with expanded unified I/O capabilities for data migration between Network-Attached Storage (NAS) and SAN environments. This storage-optimized server comfortably fits in a standard 32-inch-depth rack, such as the Cisco® R 42610 Rack.

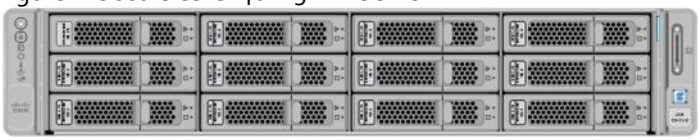
Cisco UCS C-Series ScaleProtect Nodes

A ScaleProtect cluster with C-Series servers requires a minimum of three Cisco UCS C-Series "converged" nodes (with disk storage). The solution consists of two designs with UCS C-series servers; one with Cisco UCS C240 M5 LFF server and the other with Cisco UCS C220 M5 LFF server.

Cisco UCS C240 M5 LFF Server

This two-rack-unit (2RU) Cisco C240 M5 Large Form Factor (LFF) model server contains a pair of 240/480/960 GB M.2 form factor solid-state disk (SSD) that acts as the boot drives, a pair of 1.6 TB or 3.2 TB NVMe SSD drives installed in the rear drive slots, and twelve 4 TB to 12 TB SATA HDD drives for storage capacity. The UCS C240 M5 LFF server extends the capabilities of Cisco's Unified Computing System portfolio in a 2U form factor with the addition of the Intel® Xeon® Processor Scalable Family, 24 DIMM slots for 2666-MHz or 2933-MHz DIMMs with capacity points up to 128 GB, 2666-MHz DCPMMs with capacity points up to 512 GB, up to 6 PCI Express (PCIe) 3.0 slots, and up to 12 front-facing internal LFF drives.

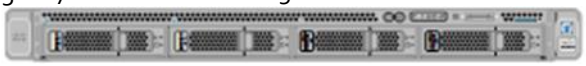
Figure 6 Cisco UCS C240 M5 LFF Server



Cisco UCS C220 M5 LFF Server

The enterprise-class Cisco UCS C220 M5 Rack Server extends the Cisco UCS portfolio in a 1RU rack server. This M5 server uses the latest Intel® Xeon® Scalable processors with up to 28 cores per processor, 3TB of RAM (using 24 x128GB DIMMs), 10 drives (SSD, HDD or NVMe), 2 GPUs and up to 200Gbps of unified I/o to the server. It supports a variety of other PCIe options.

Figure 7 Cisco UCS C220 M5 LFF Server



Cisco UCS Virtual Interface Card 1387 and 1457

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 **Cisco UCS VIC 1457** Card is a quad-port Enhanced Small Form-Factor Pluggable (SFP+) 10/25-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter installed in the Cisco UCS C-Series Rack Servers.

Cisco Nexus 9300 Switches

The Cisco Nexus® 9000 Series Switches offer both modular and fixed 10/40/100 Gigabit Ethernet switch configurations with scalability up to 60 Tbps of non-blocking performance with less than five-microsecond latency, wire speed VXLAN gateway, bridging, and routing support.

Supporting either Cisco ACI or NX-OS, the Nexus delivers a powerful 40/100Gbps platform offering up to 7.2 TBps of bandwidth in a compact 1RU TOR switch.

Figure 8 and Figure 9 are the two Cisco Nexus Switch models used in ScaleProtect with Cisco UCS Solution:

Figure 8 Cisco Nexus 9332 Switch

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.

Figure 9 Cisco Nexus 9336C-FX2 Switch

The Cisco Nexus 9336C-FX2 offers flexible port speeds supporting 1/10/25/40/100 Gbps in a compact 1 RU form factor.

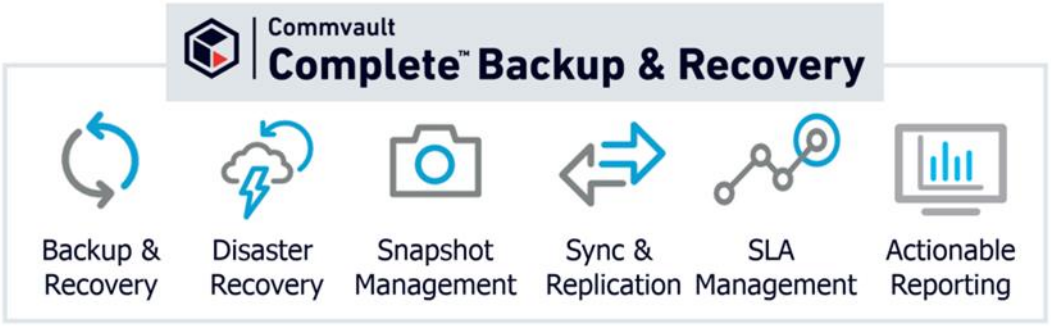
Commvault® Software

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.

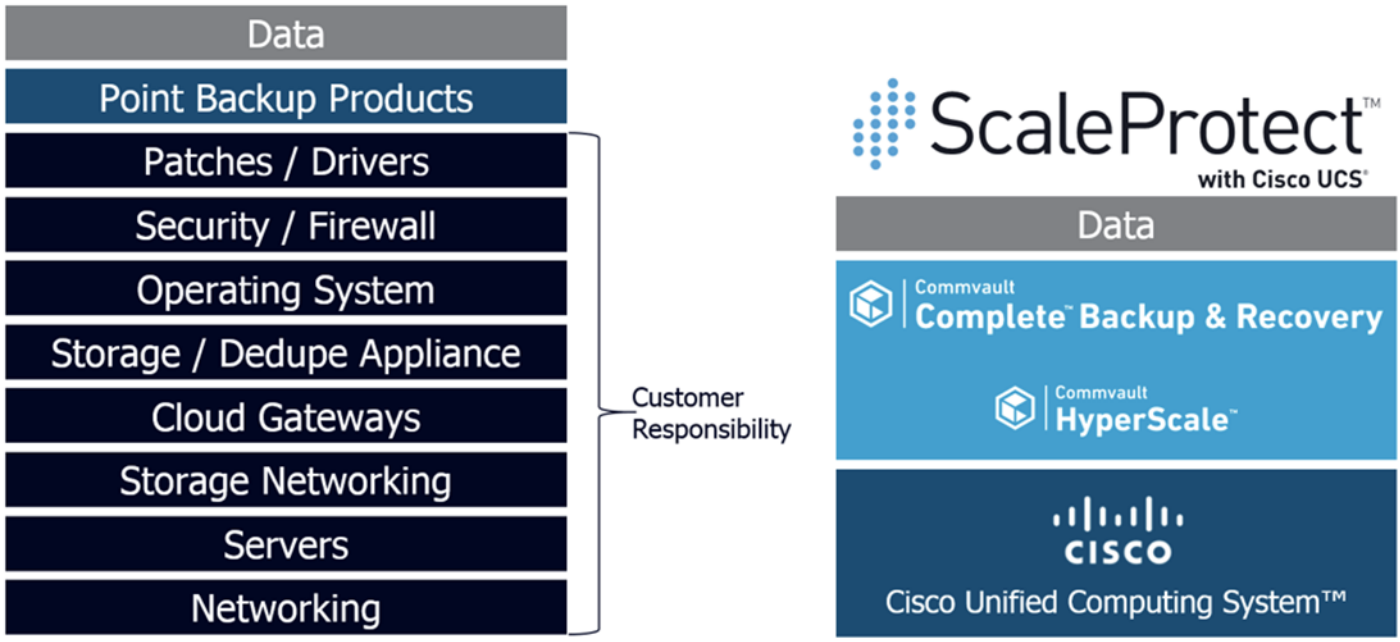
Commvault HyperScale™ Software

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 helping to ensure that scaling 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:

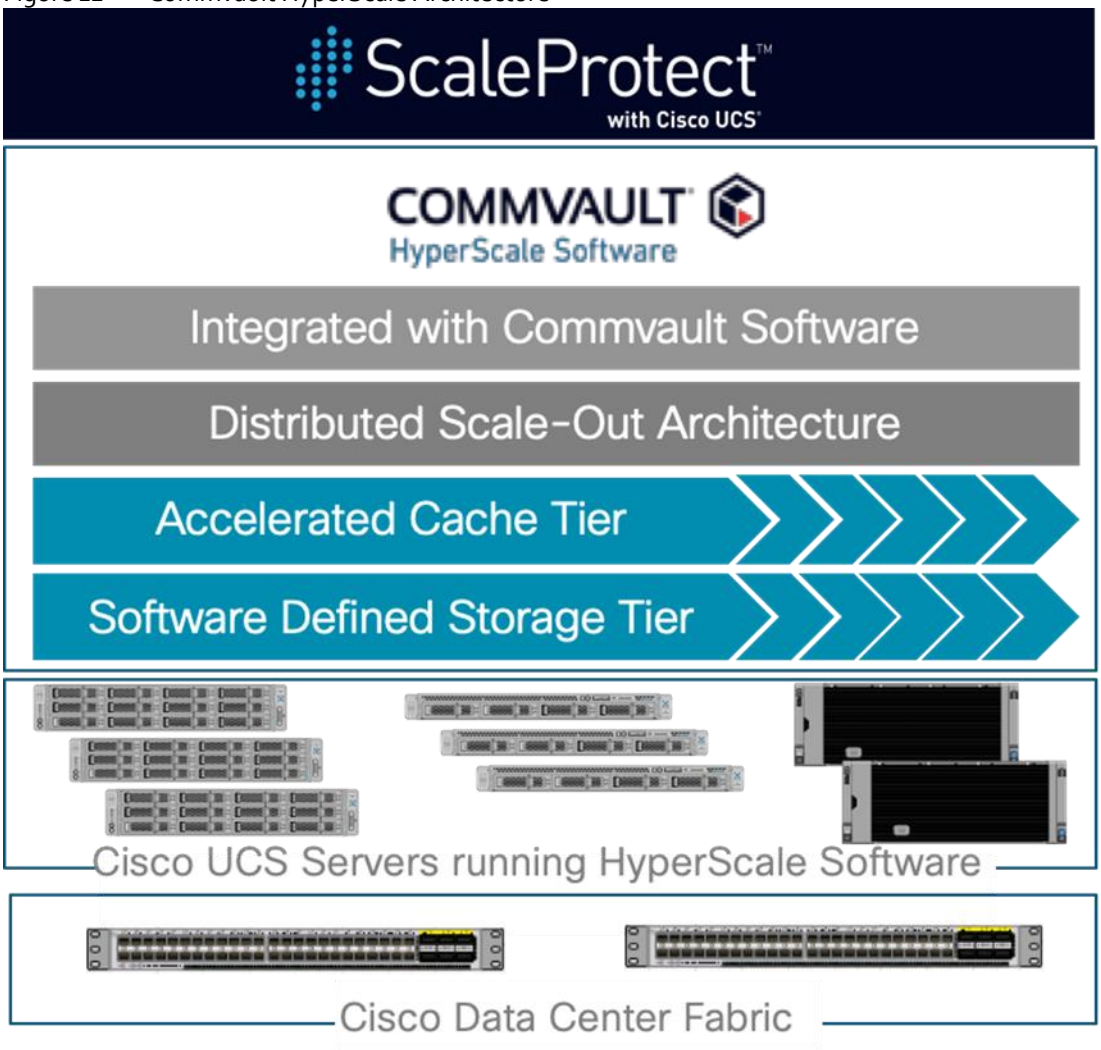
- Ease of Acquisition: an integrated solution including pre-installed data protection software, operating system, and compute and storage that is pre-configured and validated for the specific workload, available in a single package for easy procurement.
- Simple Installation and Integration: a single 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 are no utilization issues when growing the solution. Distribution of data, resiliency and redundancy are built-in and scale as the solution does.

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, cohesive, highly available solution.

A typical ScaleProtect with Cisco UCS deployment starts with a 3-node or a 6-node block with all servers in a block having similar resources of CPU, memory, storage and network. The 3-node block model scales in increments of 3: to 3, 6, 9, 12, or more nodes. The 6-node block model scales in increments of 6: to 6, 12, 18, 24, or more nodes. The solution can be scaled-out by adding additional nodes without service disruption. Separate node blocks in the same ScaleProtect cluster can use different HDDs (for example, a 3-node 6-TB block can be mixed with a second 3-node 10-TB block in the same grid).

There are three design options available within the solution and each of these designs have different Cisco UCS servers used as ScaleProtect server nodes and the solution provides choice to the customers in selecting a specific design based on the needs for secondary backup infrastructure. The considerations include the starting storage capacity needed and the projected scale required to support the growing backup and recovery needs.

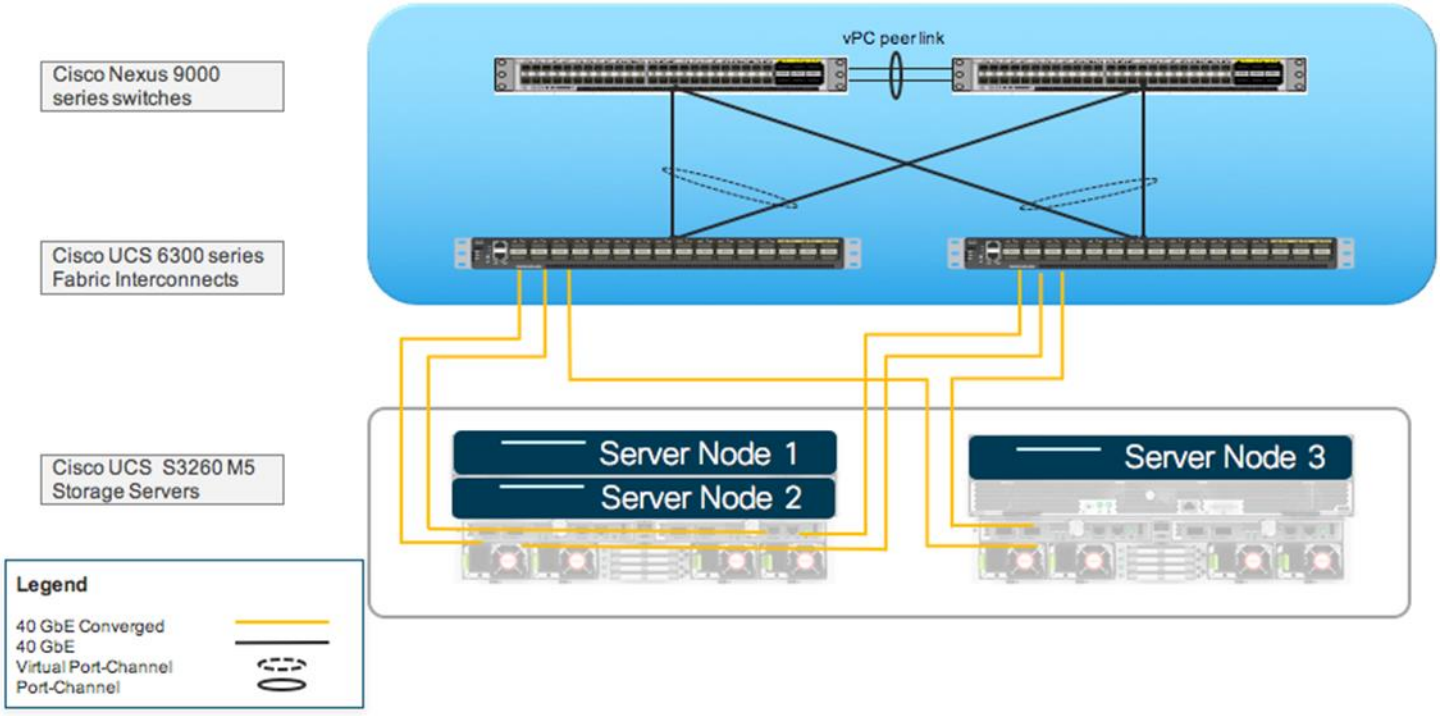
The following are the design options available with ScaleProtect with Cisco UCS Servers. Each of these designs are discussed in detail in the following sections of the document:

- ScaleProtect with Cisco UCS S3260 M5 Storage Servers
- ScaleProtect with Cisco UCS C240 M5 LFF Servers
- ScaleProtect with Cisco UCS C220 M5 LFF Servers

Design Overview with Cisco UCS S3260 Storage Servers

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 9000 upstream network switches.

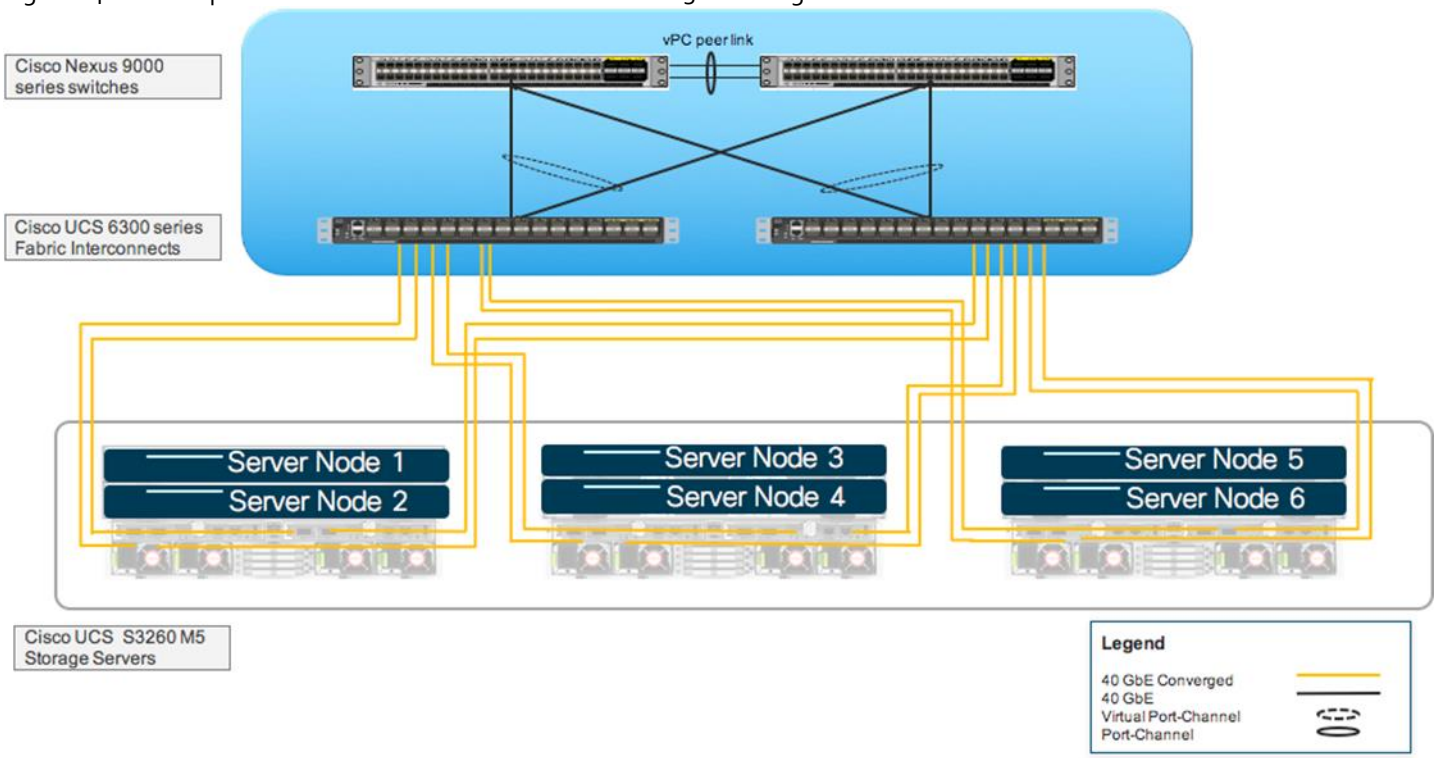
Figure 13 3 Node ScaleProtect with Cisco UCS S3260 Design



ScaleProtect with Cisco UCS can start with more nodes than 3 as mentioned earlier, 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 Cisco UCS S3260 M5. In the 3-node starting block, there is a dual node Cisco UCS S3260 and a single node Cisco UCS S3260, while in the 6-node configuration there are 3 dual nodes.

Figure 14 outlines an example of a 6-node starting architecture.

Figure 14 Example – 6 Node ScaleProtect with Cisco UCS S3260 Design



Cisco UCS S3260 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 15 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.

This section describes some of the optional deployment considerations for 3-node and 6-node ScaleProtect configurations.

To avoid service disruptions due to Cisco UCS S3260 chassis failure, solution can be deployed with a single server node per chassis. This will prevent the cluster failure if a chassis goes down due to any reason with the 3-node ScaleProtect cluster, since the configuration will only loose one node in the cluster and the other two surviving nodes will provide full functionality with access to storage pool. The same is applicable to a 6-node block deployment, the configuration loses one server node only in the ScaleProtect cluster if a chassis fails.

Along with providing enhanced high availability, this deployment model allows easy scalability with addition of 3 or 6 nodes to the empty available slots in the existing S3260 chassis for cluster expansion with additional blocks.

When expanding an existing ScaleProtect Cluster, please consider the following limitation with the Cisco UCS S3260 Chassis. Cisco UCS S3260 M4 and M5 server nodes cannot be mixed in the same Cisco UCS S3260 chassis. If there is an existing chassis with a M4 node, the other available slot cannot be used to populate an Cisco UCS M5 S3260 server node.

Table 2 Cisco UCS S3260 M5 Server Node Configuration

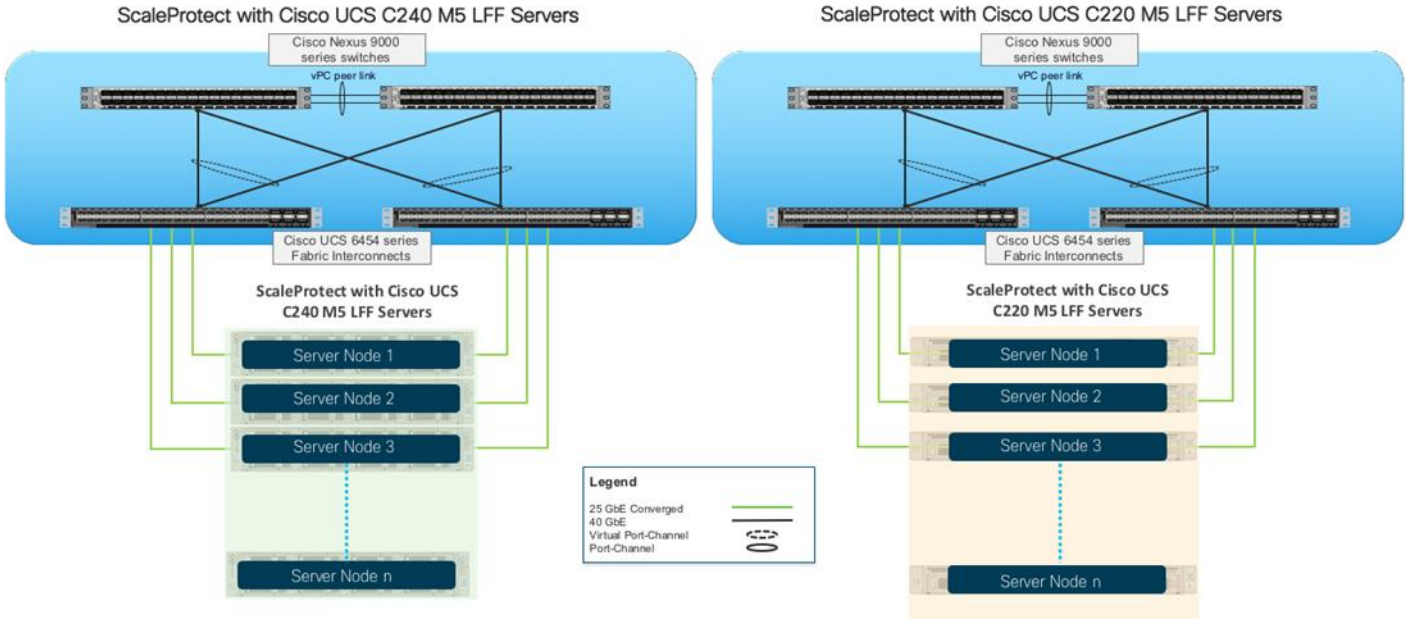
	S3260 M5 Dual Node		S3260 M5 Single Node
	Node 1	Node 2	Node 1
CPU	2x 2nd Gen Intel® Xeon® Scalable Silver 4214 52.8GHz (24 Cores)	2x 2nd Gen Intel® Xeon® Scalable Silver 4214 52.8GHz (24 Cores)	2x 2nd Gen Intel® Xeon® Scalable Silver 4214 52.8GHz (24 Cores)
Memory	256GB DDR4	256GB DDR4	256GB DDR4
Storage	**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

Design Overview with Cisco UCS C-Series Rack Servers

The solution design with the Cisco UCS C-Series servers is similar to the Cisco UCS S3260 solution architecture in terms of connectivity and the number of nodes per block. Connectivity within the Cisco UCS C-Series solution architecture is provided via a pair of Cisco UCS 6454 Fabric Interconnects and the server nodes with in the ScaleProtect block are either Cisco UCS C240 M5 LFF or Cisco UCS C220 M5 LFF servers.

Two individual ScaleProtect Clusters were independently deployed during solution validation, one with three Cisco UCS C240 M5 LFF servers and the other with three Cisco UCS C220 M5 LFF servers. Both designs including the Cisco UCS C-Series servers provide different starting storage capacity options and scale to multiple nodes seamlessly with the addition of new Cisco UCS C-Series servers.

Figure 16 ScaleProtect with Cisco UCS C-Series Design



The following is the hardware configuration of Cisco UCS C-Series nodes with standard and configurable components:

Table 3 Cisco UCS C-Series Server Node Configuration

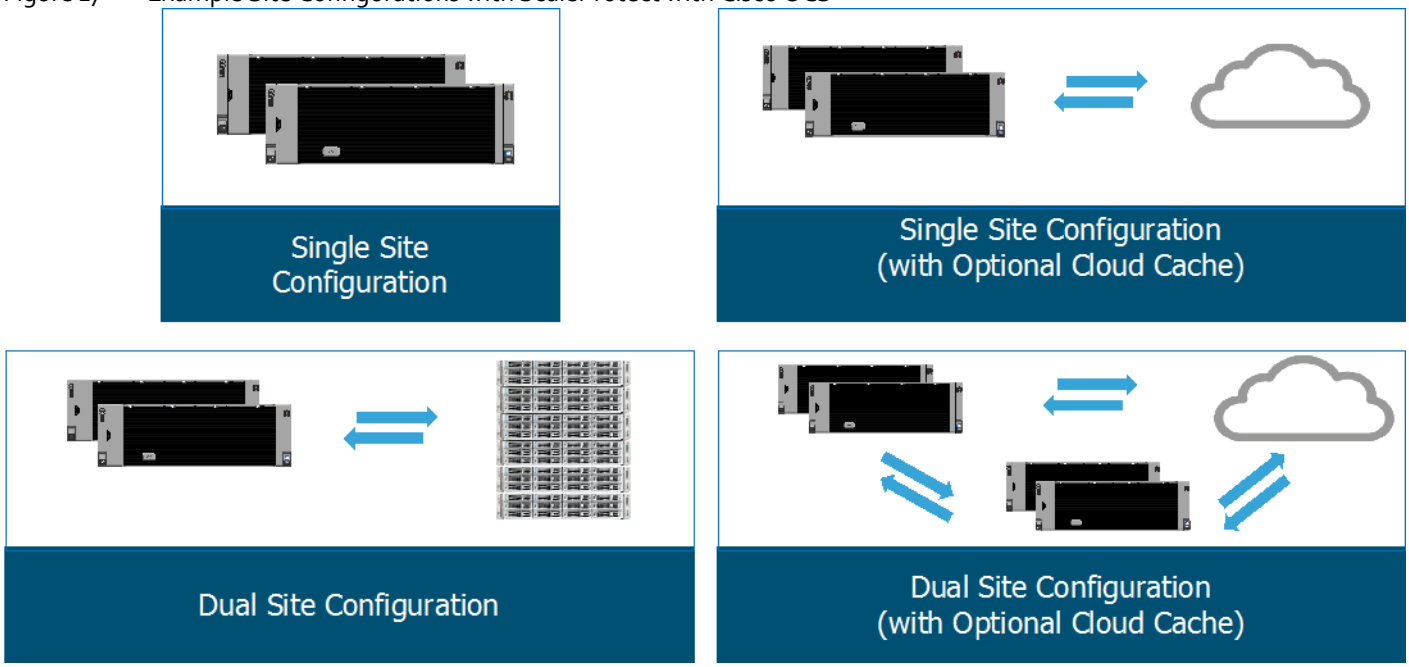
Resources	Cisco UCS C240 M5 LFF	Cisco UCS C220 M5 LFF
CPU	2x 2nd Gen Intel® Xeon® Scalable Silver 4214 52.8GHz (24 Cores)	2x 2nd Gen Intel® Xeon® Scalable Silver 4214 52.8GHz (24 Cores)
Memory	256GB DDR4	96GB DDR4
Storage	**Boot Drives**	
	(2) 960GB SSD – RAID1	(2) 960GB SSD – RAID1
	Accelerated Cache Tier	
	(1) 3.2TB NVMe	(1) 1.6TB NVMe
	Software Defined Data Storage Tier	
	(12) 4/6/8/10/12TB HDD	(4) 4/6/8/10/12TB HDD
Storage Controller	12G SAS HBA	SAS 12G RAID
Network	(2/4) 25Gbps	(2/4) 25Gbps

ScaleProtect with Cisco UCS 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 with support for different Cisco UCS hardware platforms across the locations providing flexibility. These configurations do not require external gateways or appliances, as outlined in the previous section the solution deployment requires determining the amount of storage required for specific configurations, and the Optional Cloud Cache.

With the Cisco UCS C-Series ScaleProtect design; dedicated Cloud Cache Tier is not a requirement. The Accelerated Cache Tier can support additional storage capacity required for deduplication database to support cloud copies.

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. In a multi-site deployment, the source and destination locations can have ScaleProtect clusters deployed using different Cisco UCS Server models.

Architecture for a single site with no other replication copies being generated is a simple configuration, simply size the required 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.

Resiliency

The ScaleProtect solution addresses infrastructure resiliency by including redundancy in its design and implementation at the level of each component (compute, network, and storage).

ScaleProtect Fabric Resiliency

ScaleProtect is a highly available and scalable infrastructure that IT can evolve over time to support any application backup needs. ScaleProtect has no single point of failure at any level, from the server through the network, to the internal storage. The fabric is fully redundant and scalable and provides seamless traffic failover should any individual component fail at the physical or virtual layer. Link aggregation using port channels and virtual port channels have been used throughout the design for higher bandwidth and availability.

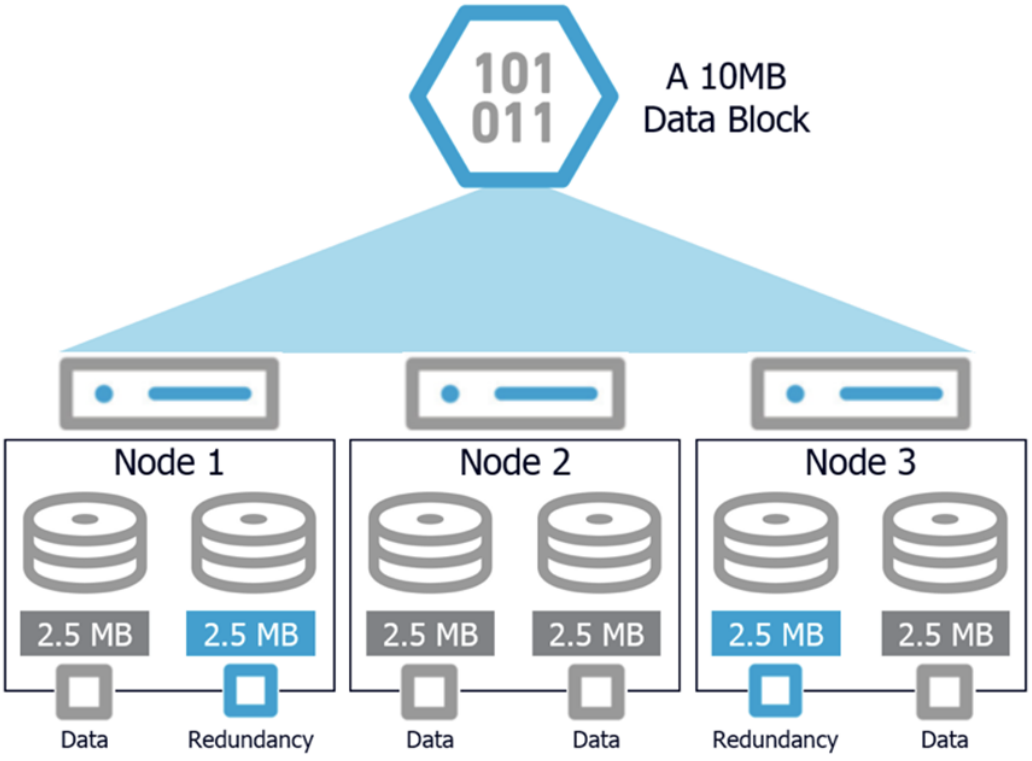
Compute Resiliency

Cisco UCS provides redundancy at the component and link level and end-to-end path redundancy to the LAN network. Cisco UCS servers are highly redundant with redundant power supplies and fans. Each server is deployed using vNICs that provide redundant connectivity within the unified fabric using NIC failover.

Commvault ScaleProtect 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 18 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 4 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.

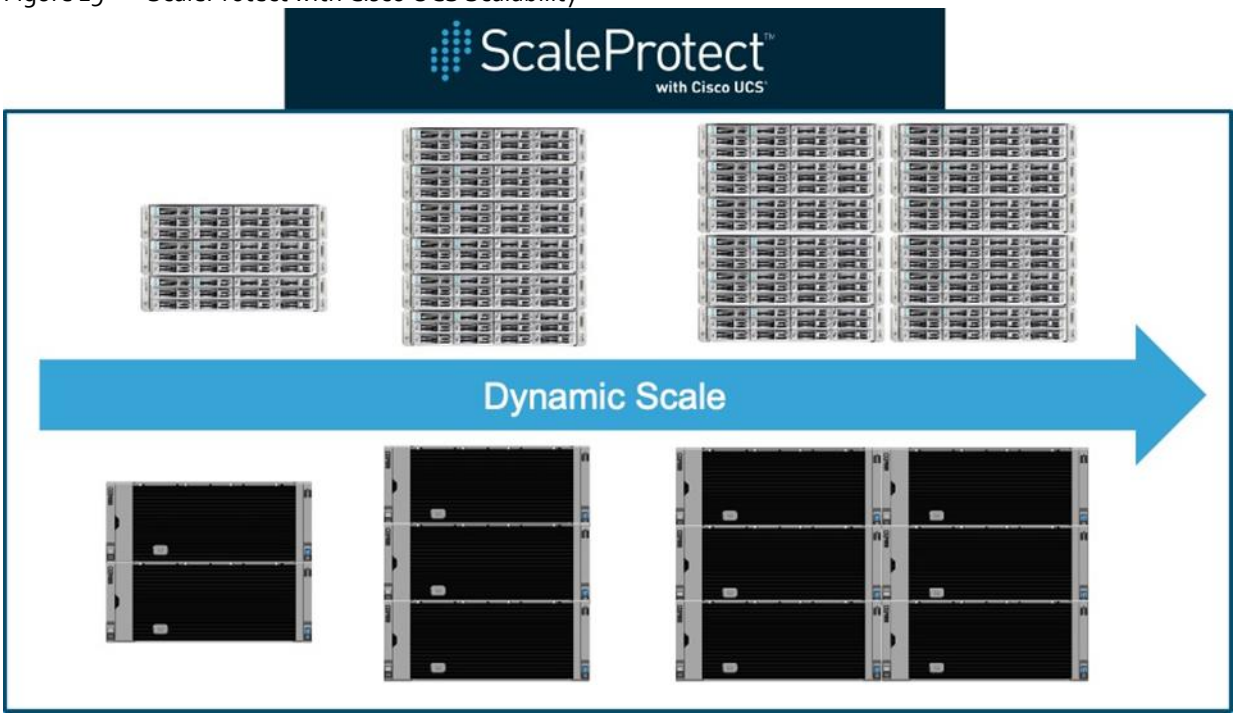
Scalability

Deployment of ScaleProtect with Cisco UCS solution can be easily scaled with additional Cisco UCS servers. Cisco UCS servers can be physically connected to any of the open ports on the Cisco UCS Fabric Interconnects. When connected, the new Cisco UCS servers can be seamlessly deployed into 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 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.

ScaleProtect with Cisco UCS architecture scales linearly with the addition of new nodes. These new nodes distribute the data and services across an increasing number 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 19 ScaleProtect with Cisco UCS Scalability



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

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 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 secondary location or 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 target location or cloud for these secondary copies with the addition of optional Cloud Cache.

Table 5 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	4 TB	174 TiB	349 TiB	523 TiB	698 TiB	873 TiB
	6 TB	261 TiB	523 TiB	785 TiB	1047 TiB	1309 TiB

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]
node)	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
Cisco UCS C240 M5 (12 Drives per node)	4 TB	87 TiB	174 TiB	261 TiB	349 TiB	436 TiB
	6 TB	130 TiB	261 TiB	392 TiB	523 TiB	654 TiB
	8 TB	174 TiB	349 TiB	523 TiB	698 TiB	873 TiB
	10 TB	218 TiB	436 TiB	654 TiB	873 TiB	1091 TiB
	12 TB	261 TiB	523 TiB	785 TiB	1047 TiB	1309 TiB
Cisco UCS C220 M5 (4 Drives per node)	4 TB	29 TiB	58 TiB	87 TiB	116 TiB	145 TiB
	6 TB	44 TiB	88 TiB	132 TiB	176 TiB	220 TiB
	8 TB	58 TiB	116 TiB	174 TiB	232 TiB	290 TiB
	10 TB	72 TiB	144 TiB	222 TiB	296 TiB	370 TiB
	12 TB	87 TiB	174 TiB	261 TiB	348 TiB	435 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 for the UCS S3260 design.

Physical Topology and Configuration

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

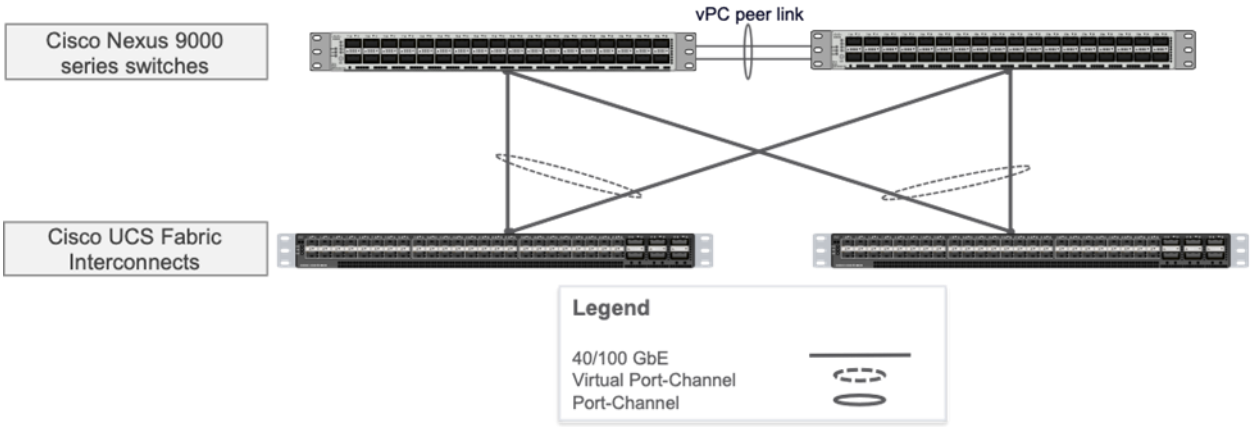
Network Fabric

In this ScaleProtect with Cisco UCS design, a pair of redundant Cisco Nexus 9000 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 20.

Figure 20 Network Design – vPC Enabled Connections



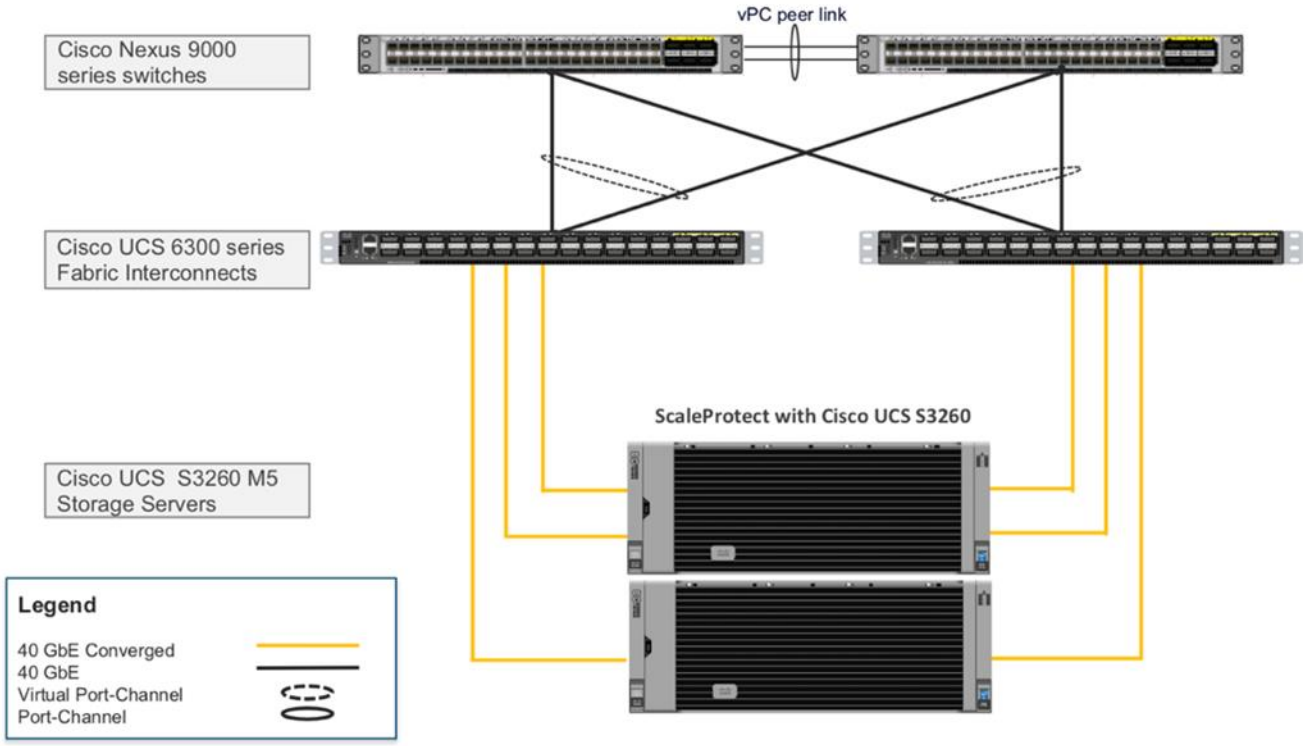
Virtual Port Channel allows Ethernet links that are physically connected to two different Cisco Nexus 9000 Series devices to appear as a single Port Channel. vPC provides a loop-free topology and enables fast convergence if either one of the physical links or a device fails. In the design, when possible,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

ScaleProtect with Cisco UCS S3260 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 21 ScaleProtect with Cisco UCS S3260 M5– 3 Node Physical Topology



For validation, Cisco UCS S3260 M5 servers with VIC 1387 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.

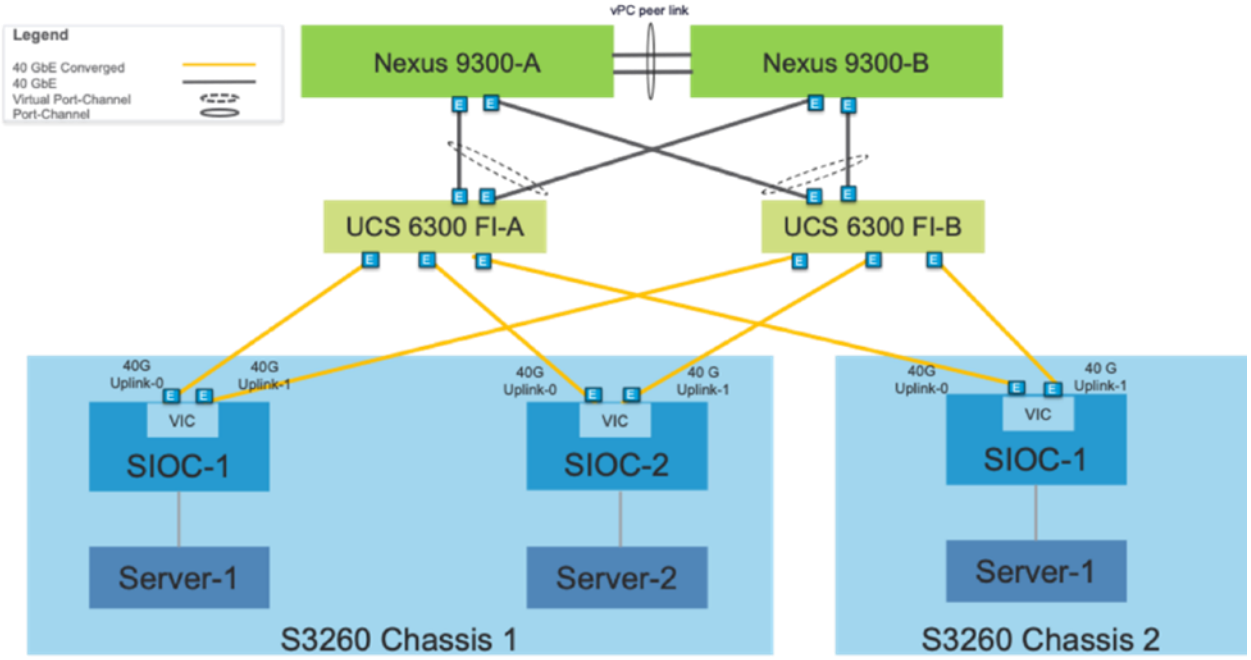
Connectivity from each individual UCS fabric interconnect, to all upstream or northbound (NB) networks is provided by 2 x 40G links to each of the top-of-rack Cisco Nexus switches as follows:

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

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 for 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.

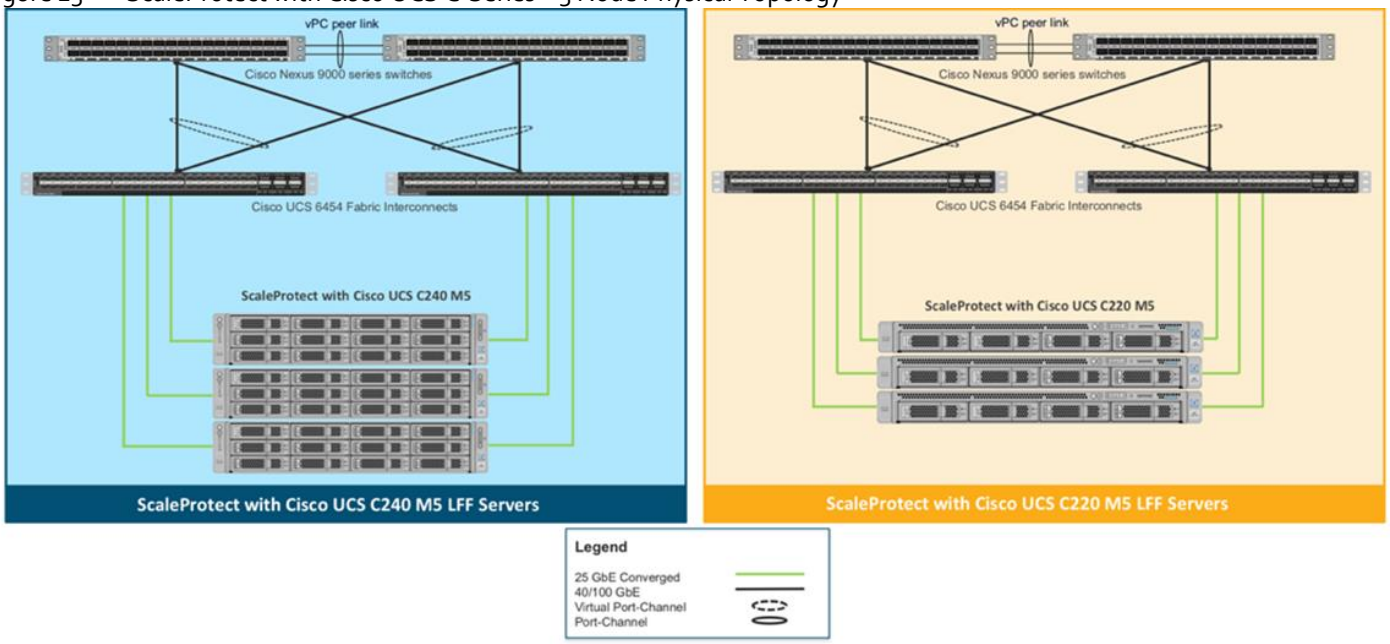
Figure 22 ScaleProtect with Cisco UCS S3260 M5 Logical Connectivity



ScaleProtect with Cisco UCS C-Series Physical Topology

ScaleProtect with Cisco UCS C-Series requires a minimum of three (3) Cisco UCS C240 M5 LFF Rack-Mount Servers or three (3) Cisco UCS C220 M5 LFF Rack-Mount Servers. The Cisco UCS C-Series Rack-Mount Servers are connected directly to the Cisco UCS Fabric Interconnects in Direct Connect mode.

Figure 23 ScaleProtect with Cisco UCS C-Series – 3 Node Physical Topology



Internally, the Cisco UCS C-Series servers are configured with the Cisco UCS VIC 1457 network interface card (NIC) installed in a modular LAN on motherboard (MLOM) slot, which has quad 10/25 Gigabit Ethernet (GbE) ports. The standard and redundant connection practice is to connect port 1 of each server's VIC card to a numbered port on FI A, and port 3 of each

server's VIC card to the same numbered port on FI B. The use of ports 1 and 3 are due to the fact that ports 1 and 2 form an internal port-channel, as does ports 3 and 4. This allows an optional 4 cable connection method, which is not used in this design but is a valid option if more bandwidth is required.

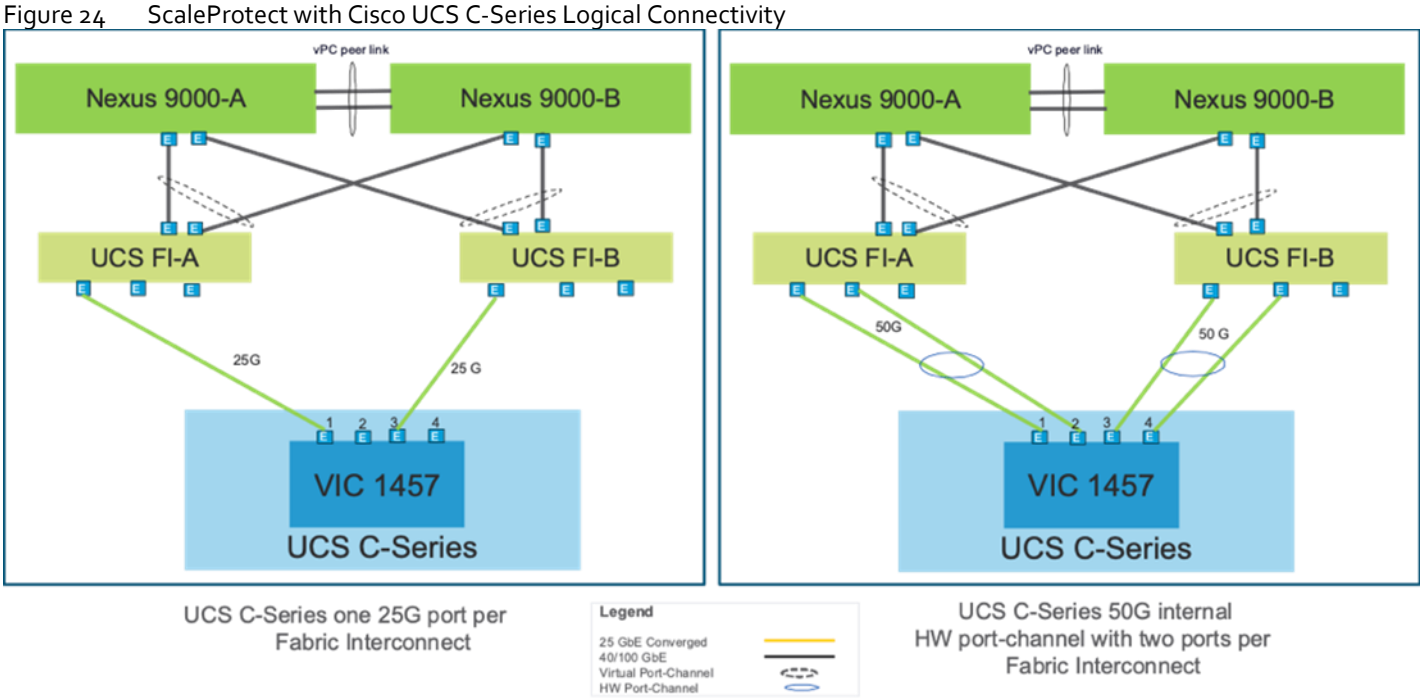
The Connectivity from each individual UCS fabric interconnect, to all upstream or northbound (NB) networks is provided by 2 x 40G links to each of the top-of-rack Cisco Nexus switches as follows:

- 2 x 40/100 G uplinks from FI-A to Nexus-A and Nexus-B
- 2 x 40/100 G uplinks from FI-B to Nexus-A and Nexus-B

Both uplinks are configured into a single port channel, making the total aggregate bandwidth to the core switching infrastructure 80/200 Gbps per Cisco 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 and are operating in NX-OS mode.

Figure 24 illustrates the 2-port and 4-port connectivity from the Cisco UCS C-Series servers to Fabric Interconnects.

Figure 24 ScaleProtect with Cisco UCS C-Series Logical Connectivity



Cisco UCS Network Interface Configuration

The ScaleProtect with Cisco UCS nodes consist of Cisco UCS S3260 M5 servers with Cisco UCS 1387 VIC included with the SIOC or Cisco UCS C-Series servers, either the Cisco UCS C240 M5 LFF or the Cisco UCS C220 M5 LFF with mLOM 1457. These nodes are allocated to the ScaleProtect cluster. At the server level, the Cisco VIC presents multiple virtual PCIe devices to the Cisco 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.

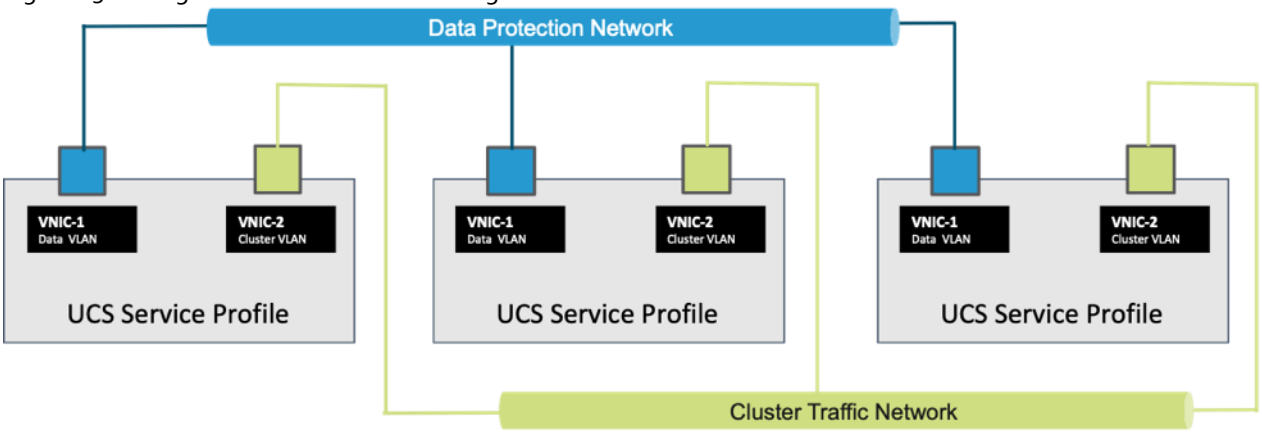
In the ScaleProtect with Cisco UCS design, two vNICs are created and utilized as follows:

- 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 25 Logical Network Interface Design



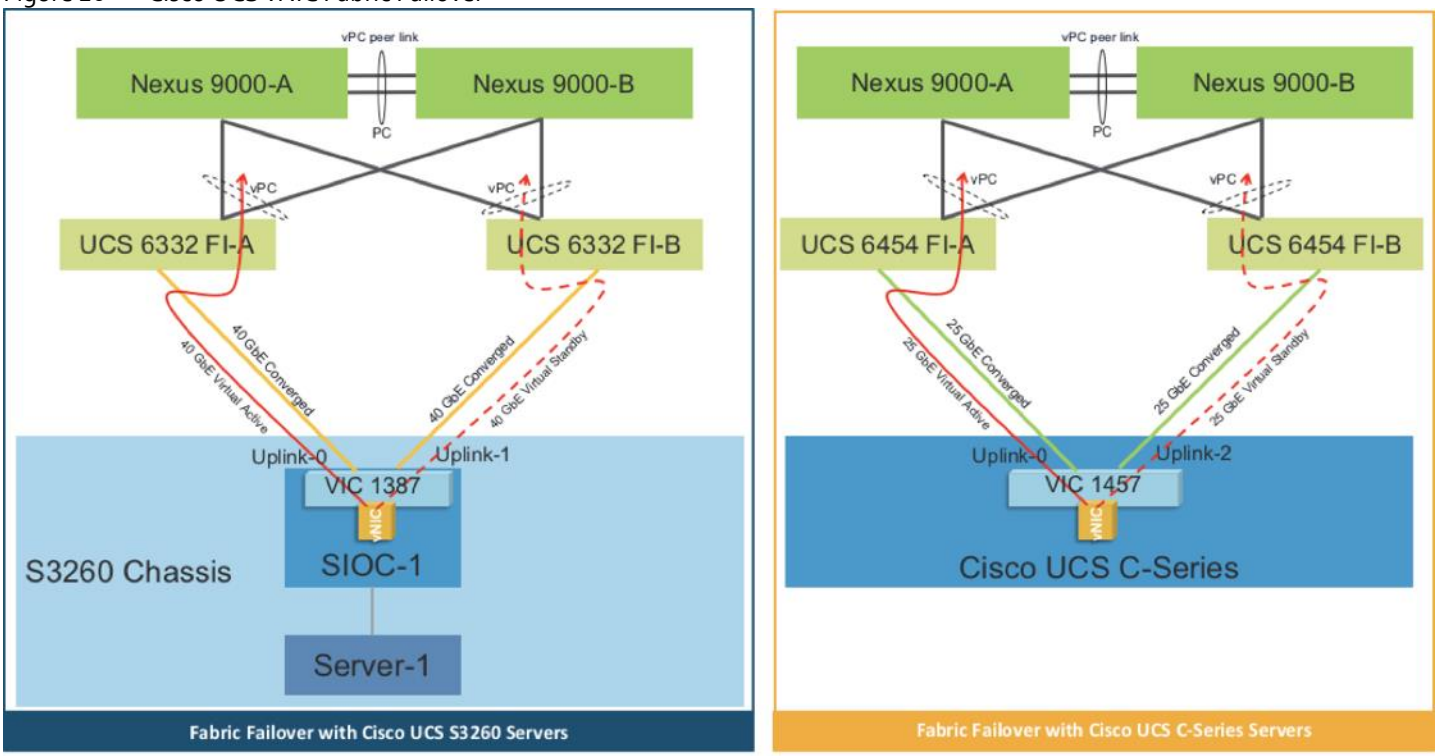
Fabric Failover for Ethernet: High-Availability vNIC

Each adapter in Cisco UCS is a dual-port 40 GbE (UCS S3260) or quad-port 25 GbE (UCS C-Series) 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 26 Cisco UCS vNIC Fabric Failover



ScaleProtect with Cisco UCS Node Disk Layout

A ScaleProtect with Cisco UCS node can house 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 Cisco UCS S3260 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

Figure 27 and Figure 28 depict the disk layout of single server node and dual server nodes:

Figure 27 Cisco UCS S3260 Single Node Disk Layout

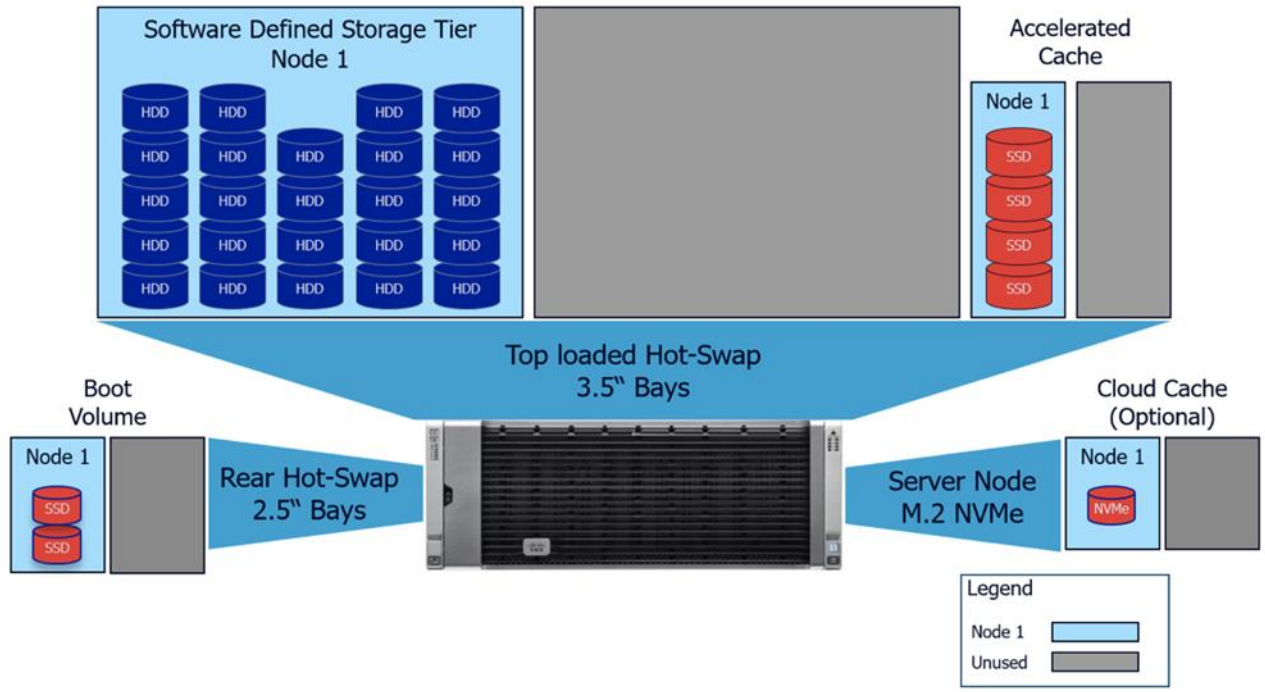
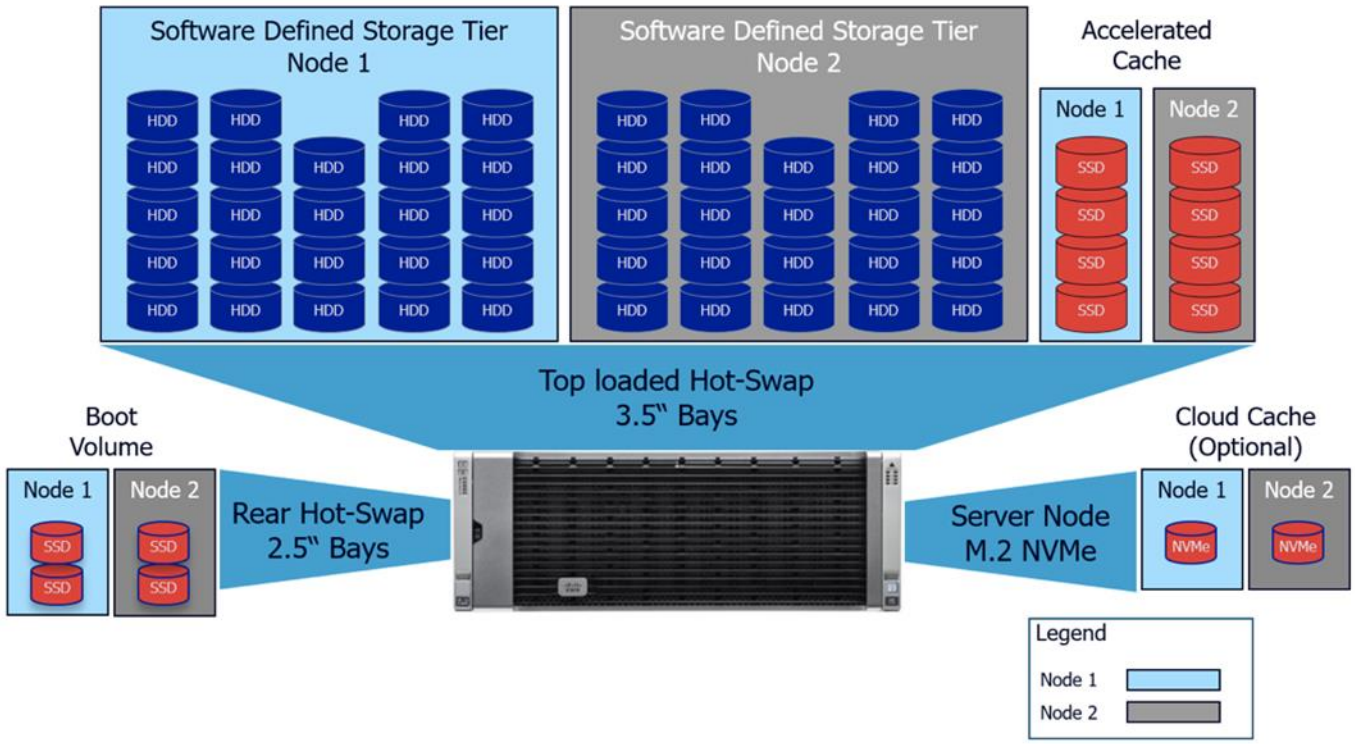


Figure 28 Cisco UCS S3260 Dual Node Disk Layout



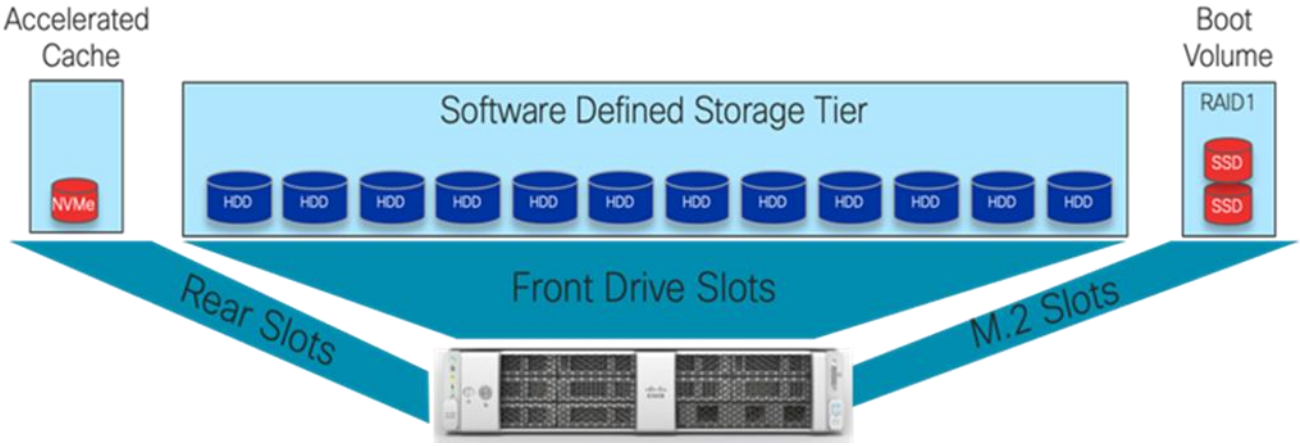
The layout of the Cisco UCS C240 M5 LFF nodes is as follows:

- Boot Volume – 2x 960GB M.2 SSDs
  - Configured in RAID 1 using Software Raid

- Accelerated Cache Volume – 1x 3.2TB NVMe SSD
- Software Defined Storage Tier – 12x NL-SAS HDDs (Option of 4/6/8/12 TB sizes)
  - Configured in Pass-through (JBOD) mode

Figure 29 illustrates the disk layout of Cisco UCS C240 M5 LLF server node:

Figure 29 UCS C240M5 LFF Disk Layout

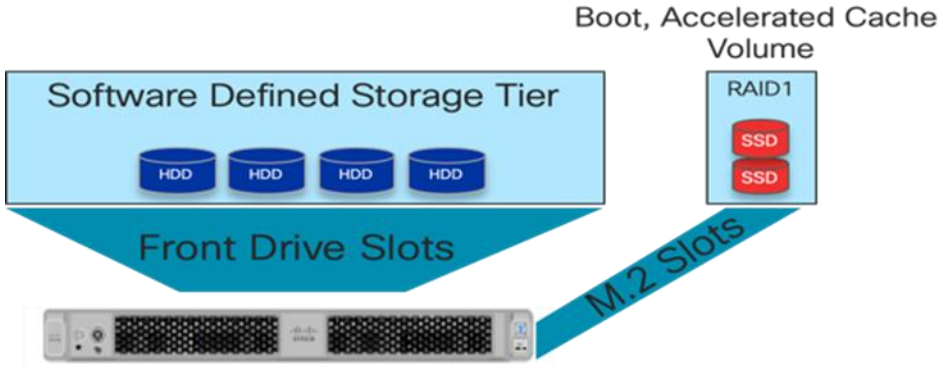


The layout of the UCS C220 M5 LFF nodes is as follows:

- Boot Volume – 2x 960GB M.2 SSDs
  - Configured in RAID 1 using Software Raid
- Accelerated Cache Volume – 1x 1.6TB NVMe SSD
- Software Defined Storage Tier – 4x NL-SAS HDDs (Option of 4/6/8/12 TB sizes)
  - Configured in Pass-through (JBOD) mode

Figure 30 illustrates the disk layout of Cisco UCS C220 M5 LFF server node:

Figure 30 Cisco UCS C220M5 LFF 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 Fabric Interconnects

The 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.

The Cisco UCS Fabric Interconnects are deployed in the default ethernet end-host mode, in this mode the FI will only learn MAC addresses from devices connected on server and appliance ports. In this mode, the FI does not run spanning-tree and handles loop avoidance using a combination of Deja-Vu check and Reverse Path Forwarding (RFP)

The ScaleProtect with Cisco UCS design should include Cisco UCS 6332-16UP Fabric Interconnect with Cisco UCS S3260 design and the Cisco UCS 6454 Fabric Interconnect with the C-Series design 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 9000 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 by default, 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 25/40GbE connections, aggregation is generally not required.

Commvault HyperScale

- Make sure that all the nodes in the HyperScale storage pool are identical including the following:
  - Same version and updates in all the nodes, which includes the Operating System, Gluster File system and Commvault software.
  - Firmware on all the HyperScale are the same and match the latest firmware version provided by Cisco.
- Upgrading to the Latest Service Pack
  - Commvault Service Pack installation on the HyperScale devices includes security and kernel patches for the Operating System, if there are any available. A reboot may be required as a result, hence it is recommended that the Service Pack installation on these devices is performed or scheduled at a convenient time.
- Adding disks
  - While adding disks, it is recommended that the number of disks (bricks) on each Cisco UCS node should ideally be a multiple of the redundancy factor for better usage of disk storage.

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 Servers Software Revisions

Table 6 Hardware and Software Revisions Validated

Layer	Device	Image
Compute	Cisco UCS 6454 Series Fabric Interconnects	4.0(4b)
	Cisco UCS C240M5 LFF Storage Server	4.0(4b)
	Cisco UCS 6300 Series Fabric Interconnects	4.0(4b)
	Cisco UCS S3260 Storage Server	4.0(4b)
Network	Cisco Nexus 9336C-FX2 NX-OS	nxos.7.0.3.I7.6.bin
	Cisco Nexus 9332PQ NX-OS	nxos.7.0.3.I7.6.bin
Software	Cisco UCS Manager	4.0(4b)
	Commvault Complete Backup and Recovery	v11 Service Pack 16
	Commvault HyperScale Software	v11 Service Pack 16

Bill of Materials

To find the various components of ScaleProtect with Cisco UCS system, follow these 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**.

Table 7 lists the key solution components, the detailed component list for each specific design has also been covered in the earlier design section of the document.

The components in the below table represent all the Cisco UCS platforms that are part of ScaleProtect solution designs.

Table 7 ScaleProtect with Cisco UCS Bill of Materials

Component	Model	Quantity	Comments
Cisco UCS Fabric Interconnects	Cisco UCS 6332 Fabric Interconnects	2	

Component	Model	Quantity	Comments
	Cisco UCS 6454 Fabric Interconnects	2	
Network Switches	Cisco Nexus 9332PQ Switches	2	
	Cisco Nexus 9336C-FX2	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)
Cisco UCS C-Series Servers	Cisco UCS C240 M5 LFF Servers	3	
Cisco UCS C-Series Servers	Cisco UCS C220 M5 LFF Servers	3	

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 and Cisco UCS C-Series 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 from Cisco UCS C240 M5 LFF to FI-A and FI-B, one at a time
- Failure and recovery of links from Cisco UCS C220 M5 LFF 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 9000 switches
- Fail/power off both Cisco 9000 switches, one after other
- Failure and recovery of Cisco UCS server nodes
- 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 is 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 Fabric Interconnects:

https://www.cisco.com/c/en/us/products/servers-unified-computing/fabric-interconnects.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, 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.

Acknowledgements

- Ulrich Kleidon, Cisco Systems, Inc.
- Bryan Clarke, Commvault Systems, Inc.
- Julio Calderon, Commvault Systems, Inc.