



FlashStack Virtual Server Infrastructure with Commvault for Data Protection

FlashStack VSI for VMware vSphere 6.0 U2 with Commvault
Modern Data Protection with Cisco UCS S3260 Design and
Deployment Guide

Last Updated: March 7, 2017



About Cisco Validated Designs

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit

<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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2017 Cisco Systems, Inc. All rights reserved.

Table of Contents

Executive Summary	6
Solution Overview	7
Introduction	7
Audience	7
Purpose of this Document.....	7
Solution Summary.....	7
FlashStack Program Benefits	9
Technology Overview	11
FlashStack VSI for VMware vSphere	11
FlashStack VSI Components	11
Cisco UCS 6332-16UP Fabric Interconnect.....	12
Cisco UCS 2304 Fabric Extender.....	12
Cisco UCS 5108 Blade Server Chassis	12
Cisco UCS B200 M4 Blade Server	12
FlashStack VSI with Commvault Modern Data Protection	14
Commvault Data Platform Overview.....	14
Commvault IntelliSnap Technology Overview.....	17
Deduplication	18
Recovery and Access	19
VM Lifecycle Management.....	19
VM Archiving	20
Cisco UCS S3260 Storage Server	20
Cisco UCS C240.....	22
Solution Design.....	24
Requirements	24
Physical Topology.....	24
Logical Topology	25
Considerations.....	26
Deployment Hardware and Software	27
Connecting the Cisco UCS S3260 Storage Server and the Cisco UCS C240 Rack Server	27
Cisco UCS S3260 Insertion into FlashStack VSI	28
Cisco UCS S3260 Chassis Setup.....	30
Cisco UCS S3260 Server Node Setup	38

Cisco UCS S3260 Storage Profile.....	40
Cisco UCS S3260 Service Profile	48
Cisco UCS C240 Insertion to FlashStack.....	63
Cisco UCS C240 Storage Profile.....	65
Cisco UCS C240 Service Profile	70
OS Installation for MediaAgent and CommServe.....	80
S3260 MDS Zoning and Host Group addition on the FlashArray//M.....	95
OS Follow-up for the CommServe and the MediaAgent	99
Commvault Deployment for FlashStack.....	105
Commvault Data Platform Installation Process	105
CommServe Installation	105
CommCell Console Overview	110
Setup CommServe Software Cache.....	110
Remote Installation of MediaAgent on S3260	111
Commvault Data Platform Configuration	112
Creating Storage Policies	114
Creating Schedule Policies	118
Configure Virtual Machine Protection for VMware.....	121
Operating Within the Commvault Environment	128
Admin Console Overview.....	128
Admin Console Dashboard	128
Customizing the Administrative Console.....	129
VM Recovery Operations	131
Validation.....	136
Validate Hardware and Software.....	136
Testing Methodology	137
Summary	138
Reference Sources for Components in this Design	139
Products and Solutions.....	139
Appendix	141
Commvault Reference Architectures.....	141
Commvault Configuration Details	142
Server Roles and Architectures.....	142
Storage Pool Information	143
Policy Information	143

Hypervisor Information.....	145
Subclient Information.....	146
Commvault Software Offline Installation.....	146
FlashArray API Token Lookup	151
Live Sync.....	153
About the Authors.....	155
Acknowledgements	155

Executive Summary

Cisco Validated Designs consist of 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 our customers.

This document expands the FlashStack VSI (Virtual Server Infrastructure) for VMware vSphere 6.0 U2 Design and Deployment Guides, which covers the FlashStack Converged Infrastructure consisting of:

- Pure Storage FlashArray//M all flash array
- Cisco Unified Computing System
- Cisco Nexus® 9000 family of switches
- Cisco MDS 9000 family of Fibre Channel switches

The expansion of the FlashStack VSI solution adds holistic data protection from Commvault. Commvault software adds snapshot management, secondary storage with Cisco UCS S3260 Storage Servers, Replication, Active Copy Management, and virtual machine (VM) archiving. Commvault's automated approach to snapshot management adds application consistent controls to the FlashArray, exponentially accelerating data protection and recovery operations. The tight integration of management snapshots with data protection, recovery, and copy management functions provide a complete data management of the virtual server infrastructure with a complete view into data across applications, devices, operating systems and locations. This comprehensive solution cuts administrative overhead while improving access and availability, and improving IT efficiency.

With the data center rapidly transforming, the need for convergence is greater than ever to maximize the value of the equipment on the floor. Combining compute and storage with intelligent data management allows for deeper integration into the applications and data itself. This also creates a seamless path for data to flow between sites, geographies, and between on premise locations and the cloud as required. The use cases vary and can include development a test, disaster recovery (DR), or simply long term data retention. Merging availability and recoverability has never been so important nor so simple to achieve.

Commvault, Cisco, and Pure Storage are all leaders in their respective markets. Using these positions of excellence, a combined solution linking best in breed solutions makes for a compelling tactical and strategic solution. Data Protection for FlashStack VSI with the Commvault Data Platform provides a validated solution build on a modern approach to data protection that delivers enterprise level recovery for today's data center environments.

Solution Overview

Introduction

FlashStack is a partnership between Cisco and Pure Storage, which uses best of breed storage, server and network components to serve as the foundation for virtualized workloads, enabling efficient architectural designs that can be quickly and confidently deployed.

It is a pre-engineered solution to deliver a standardized data center infrastructure, to serve diverse applications with increased efficiency and reduced risk. To expand on reducing risk, Cisco and Pure Storage have brought in Commvault to deliver data protection.

In this document we will describe the integration and use of the Commvault Data Platform deployed with Cisco UCS S3260 Storage Server, as well as Cisco UCS C240 Rack Servers. The Commvault solution provides modern data protection for FlashStack virtual machines and integrates directly with Pure Storage **and VMware vSphere to incorporate snapshot management as part of the protection policies. The solution's** modern approach offers application consistent snapshot integration, creation of efficient secondary protection copies, replication, secure end user access, and VM lifecycle management.

Audience

The audience for this document includes, but is not limited to; sales engineers, field consultants, professional services, IT managers, partner engineers, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

Purpose of this Document

This document provides an overview of Commvault's modern data protection of FlashStack VSI for VMware vSphere 6.0, initial configuration of the FlashArray//M array within Commvault software, and highlights various recovery use cases. The deployment scenarios such Single Site, Multi Site across different data centers and centralized replication for Remote Office and Branch Offices.

This document provides a detailed description of implementing the Cisco UCS S3260 Storage Server as a local and remote data protection element within the Commvault solution. The document will also cover the configuration **of Pure Storage's FlashRecover** hardware based snapshot protection for FlashStack VSI with the Commvault Data Platform. This document covers the validation of simulated disaster recovery scenarios, the associated architecture, features, and configuration requirements to integrate these controls with Commvault.

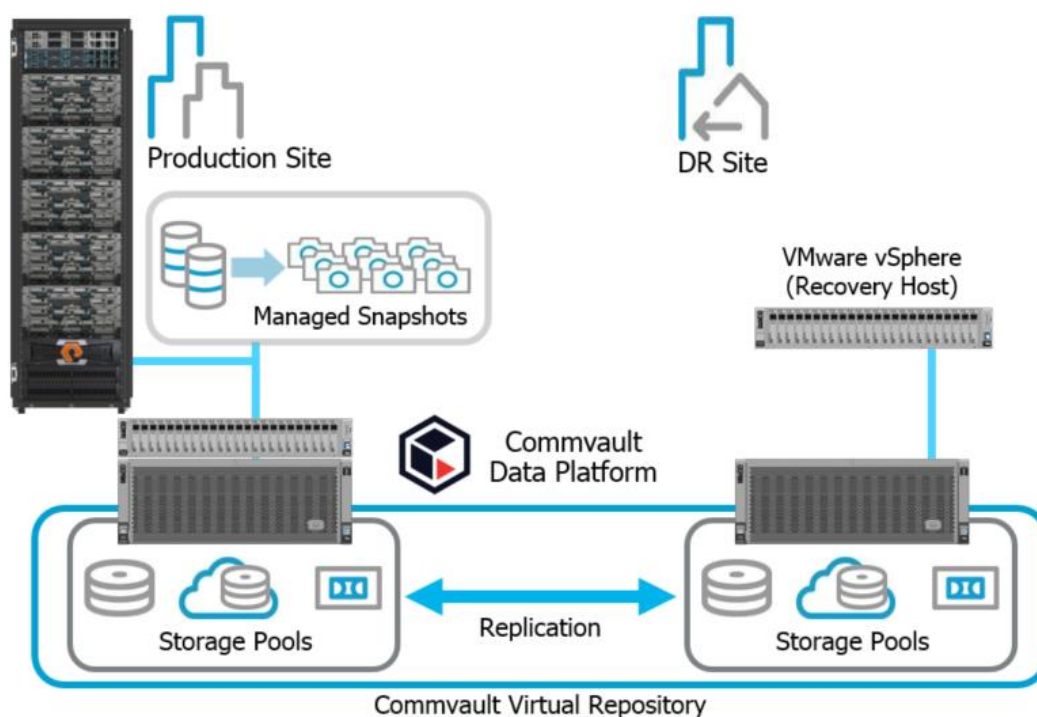
Solution Summary

This solution provides modern data protection, recovery, and replication of VMs on FlashStack VSI located in the same Data Center or Campus through the Commvault Data Platform. The Commvault Data Platform components reside on the Cisco UCS C240 and the Cisco UCS S3260 servers based on the Cisco and Commvault reference architecture. Disaster Recovery to a remote site is simulated through Commvault replication to the simulated remote Cisco UCS S3260 and recover to a separate ESXi cluster. The

Commvault Data Platform can be extended across heterogeneous data center environments comprising both converged, hyperconverged, and 3rd party infrastructure.

Modern data centers have a variety of configurations for virtualized environments, and even with FlashStack VSI there are configuration options that are not covered in this solution document. The current deployment scenarios covered in this guide are as follows:

- Protection and recovery of the FlashStack VSI environment(s) in a single data center. The single site solution focuses on protection of data in the same data center through the Commvault Data Platform. **Commvault's IntelliSnap technology integrates with Pure Storage snapshots to provide rapid lightweight protection copies on array.** These integrated snapshots are then offload to secondary storage, the Cisco UCS S3260 Storage Server, which provide an off array retention copy for recovery purposes.
- Multi-Site protection and recovery of the FlashStack VSI environment. The above single site solution is **expanded with Commvault's efficient deduplicated replication technology to offer recovery and access to data in an alternate campus or data center.** Commvault's solution can be seamless expanded to manage multiple sites and location from a single management console that mitigates the challenges of utilizing multiple tools and technologies for modern data protection.



Commvault and Cisco can provide multi-site protection that integrates with Pure Storage replication, however, this is beyond the scope of this CVD.

FlashStack Program Benefits

FlashStack brings a carefully validated architecture built on superior compute, world class networking, and the leading innovations in all flash storage. The added integration of Commvault covered in this CVD brings the assurance of data protection to the highly resilient architecture.



- Consistent performance: FlashStack provides higher, more consistent performance than disk-based solutions and delivers a con-verged infrastructure based on all-flash that provides non-disruptive upgrades and scalability.
- Cost savings: FlashStack uses less power, cooling, and data center space when compared to legacy disk/hybrid storage. It provides industry-leading storage data reduction and exceptional storage density.
- Simplicity: FlashStack requires low ongoing maintenance, and reduces operational overhead. It also scales simply and smoothly in step with business requirements.
- **Deployment choices:** It's available as a custom-built single unit from FlashStack partners, but organizations can also deploy using equipment from multiple sources, including equipment they already own.
- Unique business model: The Pure Storage Evergreen Storage Model enables companies to keep their storage investments forever, which means no more forklift upgrades and no more downtime.

- Mission-critical resiliency: FlashStack offers best in class performance by providing active-active resiliency, no single point of failure, and non-disruptive operations, enabling organizations to maximize productivity.
- Support choices: Focused, high-quality single-number FlashStack support is available from FlashStack Authorized Support Partners. Single-number support is also available directly from Cisco Systems as part of their Data Center Critical Infrastructure services offering. Support for FlashStack components is available from Cisco, VMware, and Pure Storage individually and leverages TSAnet for resolution of support queries between vendors.

Technology Overview

This section describes the FlashStack Architecture.

FlashStack VSI for VMware vSphere

The FlashStack architecture is composed of leading edge product lines from Cisco and Pure Storage and were detailed in a pair of companion Design and Deployment Guides that are available at:

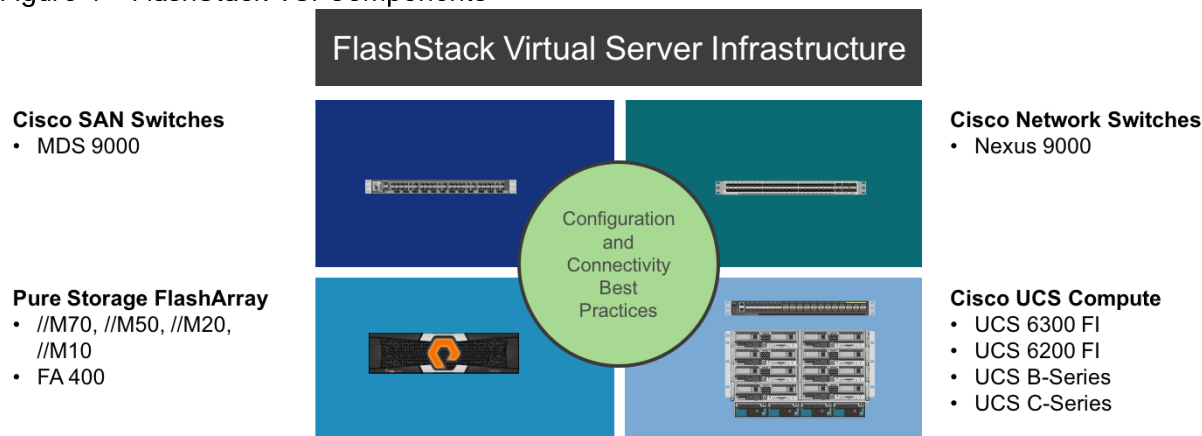
Design Guide:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_flashstack_vsi_vm6_design_s.html

Deployment Guide:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_flashstack_vsi_vm6.html

Figure 1 FlashStack VSI Components



The FlashStack VSI design features a subset of components, centered on the Cisco UCS 6332-16UP and the FlashArray//M70 within a fibre channel implementation for storage communication. A pair of Cisco MDS 9148S SAN switches are positioned between these two main components. This managed compute and storage is delivered to UCS B200 M4 servers, with all of this extended to the network via a pair of Cisco Nexus 93180YC-EX switches.

FlashStack VSI Components

The primary components of the FlashStack VSI are detailed in the following sections.

Cisco Unified Computing System

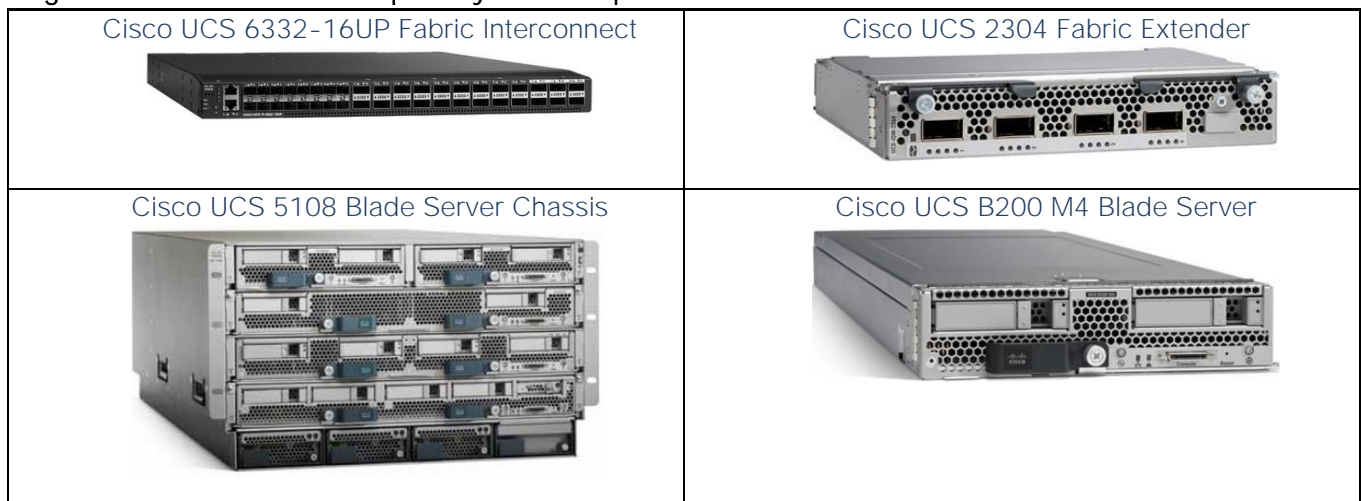
[The Cisco Unified Computing System](#) is a next-generation solution for blade and rack server computing. The system integrates a low-latency, lossless 40 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform in which all resources participate in a unified management domain. The Cisco Unified Computing System accelerates the delivery of new services simply, reliably, and securely through end-to-end provisioning and migration support for both virtualized and non-virtualized systems.

The main components of the Cisco UCS are:

- **Compute** –The system is based on the industry leading data center computing system that incorporates rack mount and blade servers based on Intel processors.
- **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** –Cisco UCS system provides consolidated access to both SAN storage and Network Attached Storage over the unified fabric. This provides customers with storage choices and investment protection. Also, the server administrators can pre-assign storage-access policies to storage resources, for simplified storage connectivity and management leading to increased productivity.
- **Management**–The system uniquely integrates all system components to enable the entire solution to be managed as a single entity by the Cisco UCS Manager. The Cisco UCS Manager has an intuitive graphical user interface (GUI), a command-line interface (CLI), and a powerful scripting library module for Microsoft PowerShell built on a robust application programming interface (API) to manage all system configuration and operations.

Cisco Unified Computing System (Cisco UCS) fuses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability.

Figure 2 Cisco Unified Compute System components in FlashStack VSI



Cisco Nexus

The [Cisco Nexus 93180YC-EX](#) is one option among many from the Cisco Nexus 9000 Series Switches viable for FlashStack. These switches are ACI and Tetration ready, offer both modular and fixed 10/25/40/50/100

Gigabit Ethernet switch configurations with scalability up to 60 Tbps of non-blocking performance with less than five-microsecond latency, implementing Layer 2 and Layer 3 Ethernet ports and wire speed VXLAN gateway, bridging, and routing support.

Figure 3 Cisco Nexus 93180-YC-EX Switch



Cisco MDS

The [Cisco MDS 9148S](#) 16G Multilayer Fabric Switch is the next generation of options available within the highly reliable Cisco MDS 9100 Series Switches. It includes up to 48 auto-sensing line-rate 16-Gbps Fibre Channel ports in a compact easy to deploy and manage 1-rack-unit (1RU) form factor. In all, the Cisco MDS 9148S is a powerful and flexible switch that delivers high performance and comprehensive Enterprise-class features at an affordable price.

Figure 4 Cisco MDS 9148S Fabric Switch

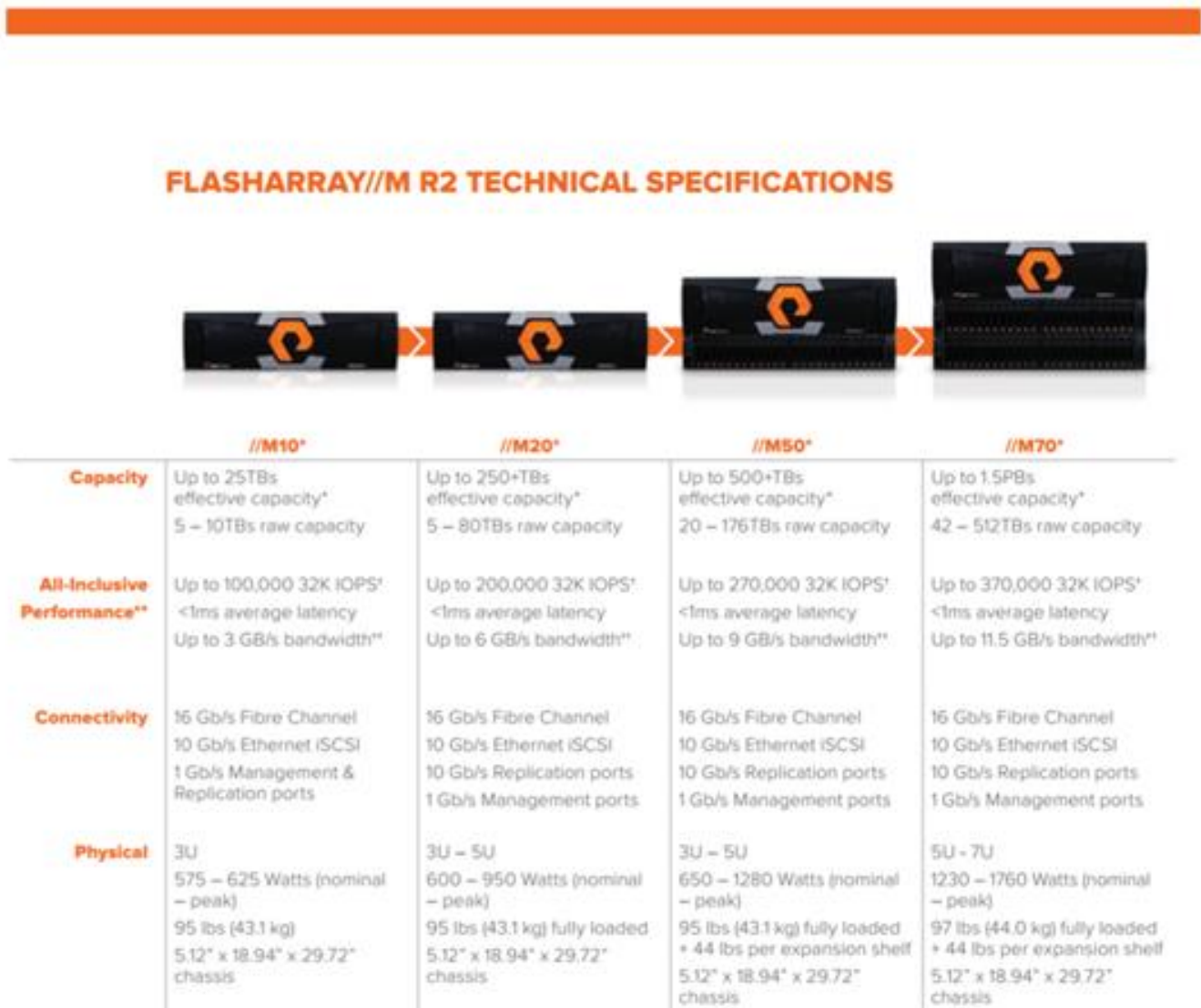


Pure Storage FlashArray//M

The FlashArray//M **expands upon the FlashArray's modular, stateless architecture, designed to enable** expandability and upgradability for generations. The FlashArray//M leverages a chassis-based design with customizable modules, enabling both capacity and performance to be independently improved over time **with advances in compute and flash, to meet your business' needs today and tomorrow.** FlashArray//M delivers the following:

- Consistent Performance FlashArray delivers consistent <1ms average latency. Performance is optimized for the real-world applications workloads that are dominated by I/O sizes of 32K or larger vs. 4K/8K hero performance benchmarks. Full performance is maintained even under failures/updates.
- Less Cost than Disk, with inline de-duplication and compression deliver 5 – 10x space savings across a broad set of I/O workloads including Databases, Virtual Machines and Virtual Desktop Infrastructure. With VDI workloads data reduction is typically > 10:1.
- Mission-Critical Resiliency FlashArray delivers >99.999% proven availability, as measured across the Pure Storage installed base and does so with non-disruptive everything without performance impact.
- Disaster Recovery Built-In FlashArray offers native, fully-integrated, data reduction-optimized backup and disaster recovery at no additional cost. Setup disaster recovery with policy-based automation within minutes. And, recover instantly from local, space-efficient snapshots or remote replicas.
- Simplicity Built-In FlashArray offers game-changing management simplicity that makes storage installation, configuration, provisioning and migration a snap. No more managing performance, RAID, tiers or caching. Achieve optimal application performance without any tuning at any layer. Manage the FlashArray the way you like it: Web-based GUI, CLI, VMware vCenter, Windows PowerShell, Python, REST API, or OpenStack.

Figure 5 Pure Storage FlashArray//M Portfolio



FlashStack VSI with Commvault Modern Data Protection

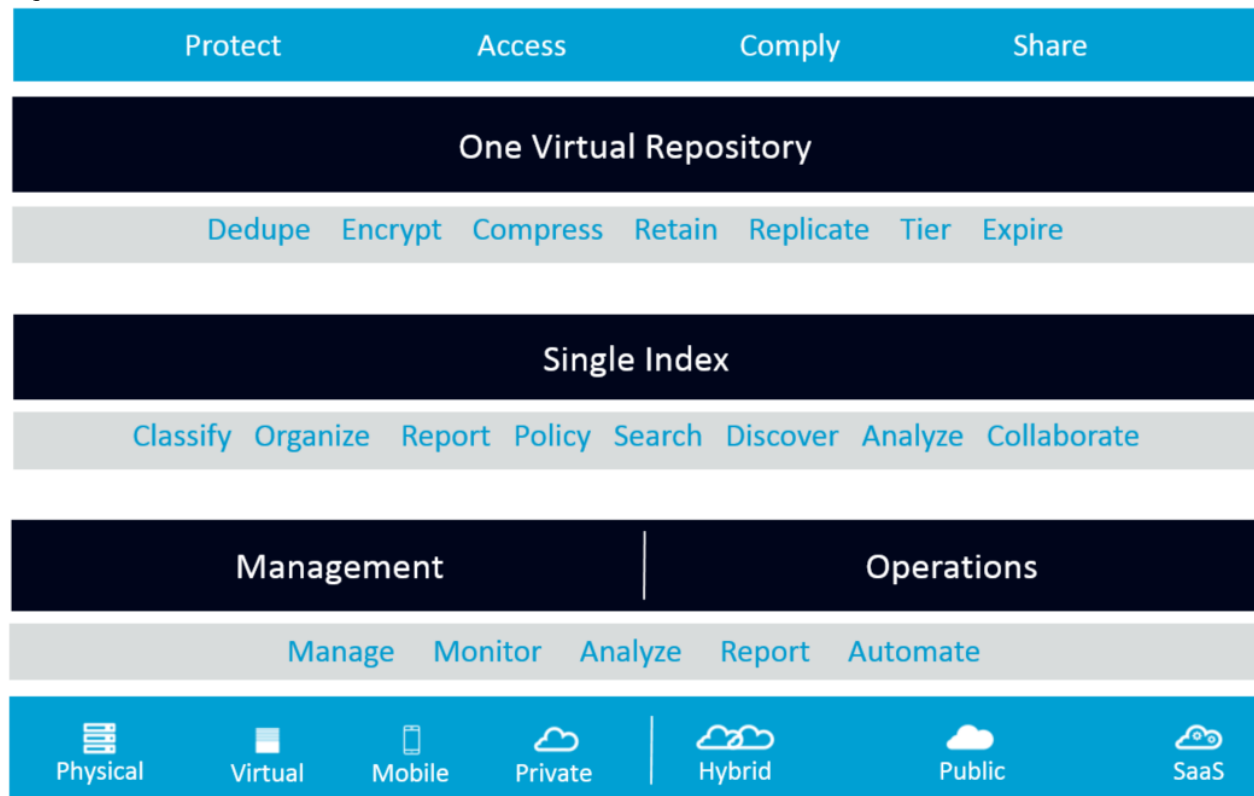
Commvault Data Platform Overview

Commvault software is built on a common platform with shared services to meet the burgeoning data protection and management needs of today's modern infrastructures. The Commvault Data Platform converges all the needs of a modern data management solution in one place to seamlessly integrate protection, management, and access in one solution.

Commvault drives unprecedented efficiency and cost reduction while driving out complexity; modern data management solutions are more than just a point solution or tool. Commvault's solution enables our customers to:

- **Protect** - Commvault likes to keep it simple, all customer data is protected and secure, whether it is in a physical, virtual or cloud environment, whether on desktops, servers, or endpoints. Focus on the right technology for the right protection, everything from native hardware snapshot integration with IntelliSnap technology, to direct cloud integration for both storage and compute, protection isn't just about streaming data but ensure that all the data is protected and indexed to provide insight about the data and eliminate redundant and dark data copies.
- **Access** - What good is protecting the data across the platform without the ability to know what is being protected, where it is location, who owns it, when it was last protected, and much more. Providing direct access to end users and application owners is the requirement for today's modern solutions. Commvault's targeted administrative console makes it simple and personalized for users to securely access their data regardless of the underlying technology or location it is stored in.
- **Comply** - Commvault solutions enable customers to produce, retrieve, and review all discoverable information, on demand. No waiting. Leveraging powerful indexed search across multiple data types with a single platform not only saves time and money, it minimizes risk and exposure.
- **Share** - Sharing and collaboration can increase productivity it shouldn't be at the risk of security and protection of the data and information. Commvault brings control back to the enterprise with data management controls that provide secure sharing, and anytime/anywhere access, all powered from the platform. Users get powerful sharing and access, IT gets a comprehensive solution that includes security and protection.

Figure 6 Commvault Data Platform



Commvault's software underlying foundation is the platform that creates a single virtual repository to delivery on the need to protect, access, comply and share data. The virtual repository is extremely storage and

network efficient, using technology like global deduplication, replication, bandwidth throttling, plus application awareness to ensure that only the minimum amount of data is stored and the fewest number of copies are retained. In fact, the virtual repository can repurpose copies of data for different needs - such as utilize a protection copy to provide access for development and test use cases, without creating additional copies of the data. The virtual repository is extremely secure, with built-in encryption for data on the moved, and at rest with complete key management. Regardless of the data location Commvault ensures the data is never exposed to unauthorized parties, whether it is on-site or in the cloud.

The single index is unique for Commvault for three reasons. First it is the only software that encompasses all secondary copies of the data, whether the data is in snapshots, backups, archive, mobile, cloud, or compliance. Multiple different tools can't provide a single unified view across all of the data, regardless of format. Second, the index is independent of data, providing the singular view to know who owns the data, who created, when it was created, and most importantly what to do with it. Finally third, it provides access to the content, what's inside your data which is critical to activating your data. Activating data means extracting more value and providing deeper insights to drive better results.

Bringing this all together, the Commvault Data Platform's architecture is unique in the data management industry. The industry-leading management also provides unparalleled management and operation capabilities. Commvault can replace up to 20 individual products and reduce the infrastructure associated with the data repositories, however it does that all while decreasing the administrative burden and allow direct access for users and administrators alike.

The key features of Commvault software are:

- Complete modern data protection solution supporting all major hypervisors, operating systems, applications, and databases on virtual and physical servers, NAS shares, cloud-based infrastructures, remote offices, and mobile devices.
- Policy based data management, transcending limitations of legacy backup products by managing data based on business needs and not physical location.
- Data protected by Commvault software resides in a single, virtual data repository that support multi-vendor storage (physical, virtual, cloud, hybrid). Data can be quickly recovered access and leveraged in a single step.
- Active Copy Management provides instant availability of secondary copies for Development/Test purposes to reduce the Copy Data Management struggles and enable end-users access to critical datasets on demand.
- Cutting edge user experience empowering end users to manage, protect, find, and recovery their own data use customizable web portals allowing focused self-service options to empower end user direct access.
- **IntelliSnap technology integrates with the industry's top storage arrays, such as Pure Storage, to automate the creation and use of indexed, application aware hardware snapshots for use with modern data protection and active copy management.**
- Simplified management through a single console; view, manage, and access all functions and all data and information across the enterprise.

- Integrated deduplication technology to provide significant data reduction at the source and globally across sites and servers, without the need for costly deduplication appliances.
- Native cloud support, with over 25 cloud storage platforms, makes it easy to backup workloads, VMs, and applications directly to the cloud with no additional appliances.
- Advanced security capabilities for role-based access to critical data, granular management capabilities, and single sign on access for Active Directory users.
- **Commvault's open API framework and built in orchestration engine allow for broad integration and interaction with other 3rd party tools to drive increased automation across data management operations**

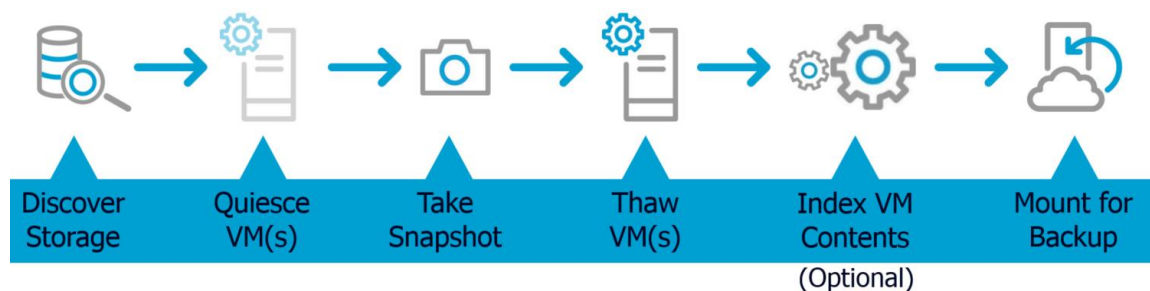
Commvault IntelliSnap Technology Overview

Commvault IntelliSnap technology provides hardware based snapshot management that simplifies and accelerates operational recovery and extends active copy management with array based snapshot technology. Unlike traditional snapshot solutions IntelliSnap technology dramatically simplifies management and access since administrators can initiate snapshots using a consistent process and user interface regardless of application, hypervisor, or storage platform.

IntelliSnap technology integrates with leading storage arrays, such as Pure Storage, to provide consistent point-in time recovery copies integrated into the data protection process. Unlike many other hardware-based copy management approaches, IntelliSnap extends beyond just creating or deleting snapshots. Snapshot contents are indexed to enable simple, granular object recovery. Snapshots are integrated into virtual machine, database and application protection schemes, enabling granular, partial, and point-in-time recoveries from snapshot.

Integrating snapshots into recovery operations leads to shorter recovery times and lower recovery costs. Commvault software can instruct storage arrays to roll back production volumes to snapshot recovery points, while managing application state, and then applying database logs to reach a more granular recovery point. Virtual machines and virtual machine files can be accessed and recovered directly out of snapshots. The entire recovery process is orchestrated based on simple criteria, with no manual intervention from storage, application or backup administrators. IntelliSnap technology manages the hardware copy lifecycle from creation through backup, replication, reuse, and finally deletion.

IntelliSnap technology works directly with VMware vSphere to provide off-host protection for VMs. This greatly reduces the impact of protection on both VMs and the physical hypervisor by rapidly creating application-consistent recovery copies. Large and/or busy VMs, which traditionally have challenges due to delta files being generated during protection operations, are easily protected in a fraction of the time while mitigating the impact to those VMs. Application awareness ensures data consistency and recoverability, with capabilities such as log truncation for Microsoft SQL Server and Microsoft Exchange.



Commvault software not only provides automated orchestration of snapshots with IntelliSnap technology, but it ensures that new VMs and Datastores are automatically protection. Commvault's automated discovery rules can detect and discover new storage and automatically assign it to the appropriate protection policy.

Key benefits of IntelliSnap technology with VMware vSphere:

- Auto-discovery of new VMs and Datastores, and automatic protection under existing protection policies
- Automated snapshot management function eliminate snapshot-based scripts
- **Commvault Data Platform's index spans all snapshot copies under management, enabling quick, intuitive search and granular recovery within and across all snapshots**
- Accelerating recovery, while reducing administrative overhead, by providing a consistent process for administrators and end-users to recover data using the same process. Recovery data from snapshot, secondary replica, deduplicated disk, cloud, or tape are rolled into a secure unified view
- Leveraging snapshots to create secondary retention copies away from production resources further reducing impact during the creation of disk, cloud tape copies.
- Commvault's workflow technology can extend into custom protection operations for operations that are unique to the environment (for example, Custom DBA scripts can be incorporated into the protection policy to ensure automation while preserving DBA independence for customer routines).

Deduplication

Commvault software integrates deduplication functionality directly into the platform for a flexible backup and recovery approach that is both scalable and cost effective. Deduplication can be deployed where it makes most sense, at the source, at the target or both, this flexibility is critical, as no two environments are identical. Deduplication technology helps reduce network backup traffic by as much as 90% by only sending unique data during the backup operations; these savings can be compounded with off-site data storage in alternate data centers or directly in the cloud.

Commvault directly integrates with VMware vSphere's Change Block Tracking (CBT), a native feature in VMware that provides an index of data that has changed since the last protection operation. Commvault directly integrates with this functionality and utilizes an incremental forever approach for data protection. **Commvault's incremental forever approach always presents a full view of the data for recovery there-by** eliminating the need to perform traditional full backups in the environment. Utilizing IntelliSnap technology does not exclude the use of incremental forever streaming support with Commvault deduplication; in fact it enhances it by shifting the source for secondary copies to the snapshot instead of production.

Recovery and Access

Commvault offers a number of options to recover and access the data that is being managed within the platform. Recovery requirements differ depending on the situation, and Commvault offers multiple options from a single protection policy:

- **Full virtual machine** – Provides integrated recovery of the entire virtual machine directly back to the original or alternate VMware vSphere environment.
- **Virtual machine files** – Provides the ability to recover individual VMDK and configuration files directly to the vSphere or a filesystem location.
- **Granular File & Application Recovery** – Provides the ability to recovery individual data and applications from within the virtual machines themselves. Oftentimes, the recovery demands more than simple restoration of the entire hypervisor, it is the database or files and directories that are needed in specific states. The ability to extract and recover those data sets from the hypervisor to another location (physical, virtual, or cloud) is a powerful asset to any organization.
- **Cross Hypervisor Recovery** – Provides the ability to recover virtual machines directly into another hypervisor that differs from the source configuration.

Providing direct access to the virtual machine in different scenarios provides different recovery options that **are required to meet today's stringent SLA policies.**

- **Live Recovery** – Provides the functionality for VMs to be recovered and powered on from a protection copy without waiting for a full restore of the VM. This can be utilized to provide instant access to a VM that has failed and needs to be placed back into production quickly, or to validate a backup can be used in a disaster recovery scenario.
- **Live Sync** – Provides VM level replication by incorporating block changes captured during protection operations to a copy on a warm standby VM at an alternate location or cluster. Live Sync can be used to create and maintain warm recovery sites for VMs running critical business applications.
- **Live Mount** – Enables a virtual machine to be powered on and run directly from a protection copy. This feature can be used to validate backups and applications are useable for a disaster recovery scenario, to validate the content of the VM, perform additional development and test procedures without creating another copy of the VM, or to access data directly from the VM instead of restoring guest files.

VM Lifecycle Management

Controlling VM sprawl and ensuring that VM usage does not create unwanted risks is a paramount concern **of IT departments.** Commvault's VM Lifecycle Management provides self-service admin management access for provisioning, backup, and recovery of VMs with customizable configuration limits, expiration dates, and more. VM Lifecycle Management enables accelerated Test/Dev by providing self-service resource provisioning and management with automated VM retirement to ensure that the continual sprawl of VM proliferation is brought under control easily and effectively.

Automation is a key benefit, enable IT to simplify testing and development, and leaving no VM unprotected thanks to automated discovery. It also allows IT to identify idle or stale VMs thus automatically reclaiming

wasted resources. Commvault also delivers “IT as a service” with chargeback reporting, workflow automation, and self-service access, providing even more efficiencies for IT managers.

VM Archiving

The proliferation of virtual infrastructure across the enterprise is a reality, vSphere environments are growing at an astounding rate. End users request VMs for any number of reasons outside of production, and left unchecked can consume resources and have adverse environmental effects in the data center, let alone the **IT budgets. Commvault’s VM archiving provides a comprehensive approach to mitigate VM sprawl and** ensuring that unused resources are not consuming valuable resources.

Selective operations that include shutting down idle resources, relocating them to lower tiers of storage, and ultimately archiving virtual machines out of the infrastructure automate the reclamation of resources.

Archived VMs are still protected in Commvault’s Virtual Repository, and with end user lifecycle management can automatically be re-activated should they become required.

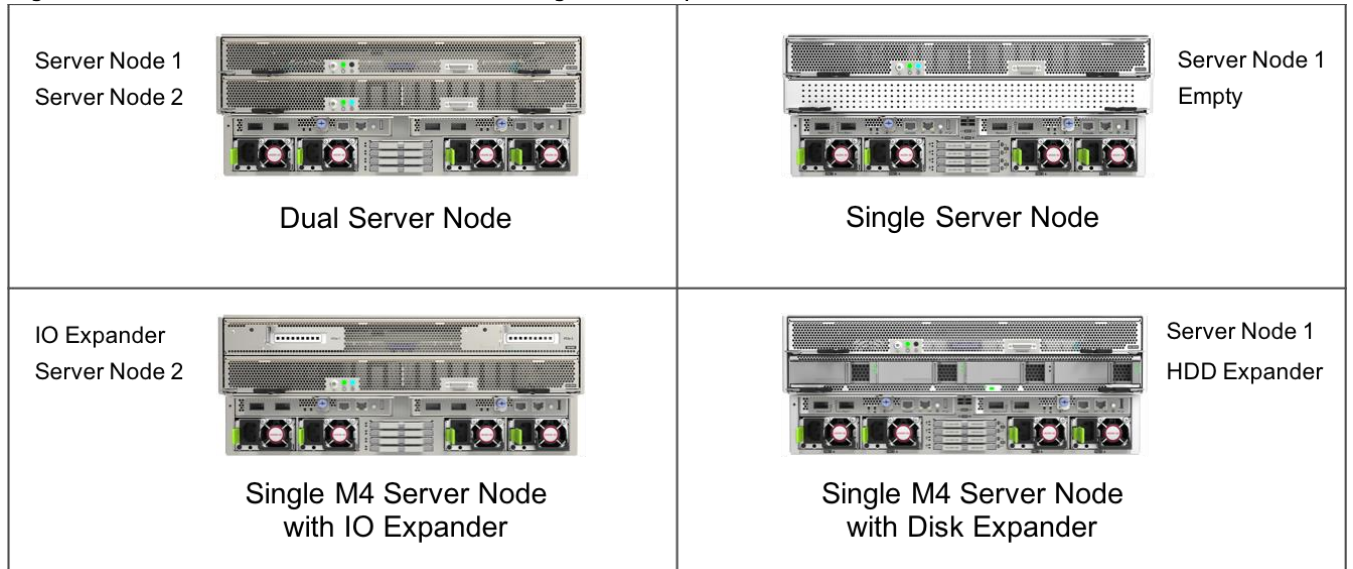
Cisco UCS S3260 Storage Server

The [Cisco UCS S3260 M4 Storage Server](#) is a high performance, dual node x86 server that delivers high capacity storage for enterprise needs. The storage is configured with the Cisco UCS C3X60 12G SAS RAID Controller card using a thorough range of RAID options (0,1,5,6,10,50,60), or as JBOD resources in pass-through mode. To present this high performance and high capacity, the S3260 comes equipped with:

- Dual two-socket server nodes based on Intel E5-2600 v2 or v4 CPUs with up to 36 cores per server node
- Up to 512GB of DDR3/DDR4 memory per server node (1 terabyte [TB] total)
- Support for high performance NVMe and Flash Memory
- Massive 600TB data storage capacity that easily scales to Petabytes with Cisco UCS Manager
- Policy driven storage management framework for zero-touch capacity on demand
- Dual-port 40Gbps System I/O Controllers with Cisco VIC 1300 Series Embedded Chip
- Unified I/O for Ethernet or Fiber Channel to existing NAS or SAN storage environments
- Support for Cisco BIDI transceivers, 40G connectivity over existing 10G cabling infrastructure

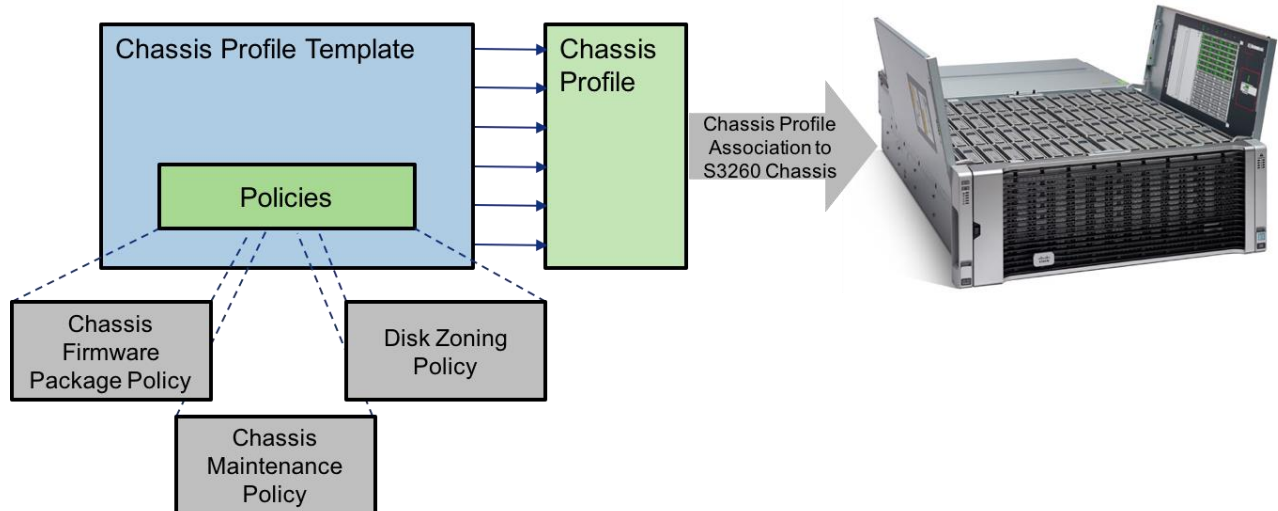
Configuring the Cisco UCS S3260 can include multiple node and expansion options:

Figure 7 Cisco UCS S3260 Chassis Configuration Options



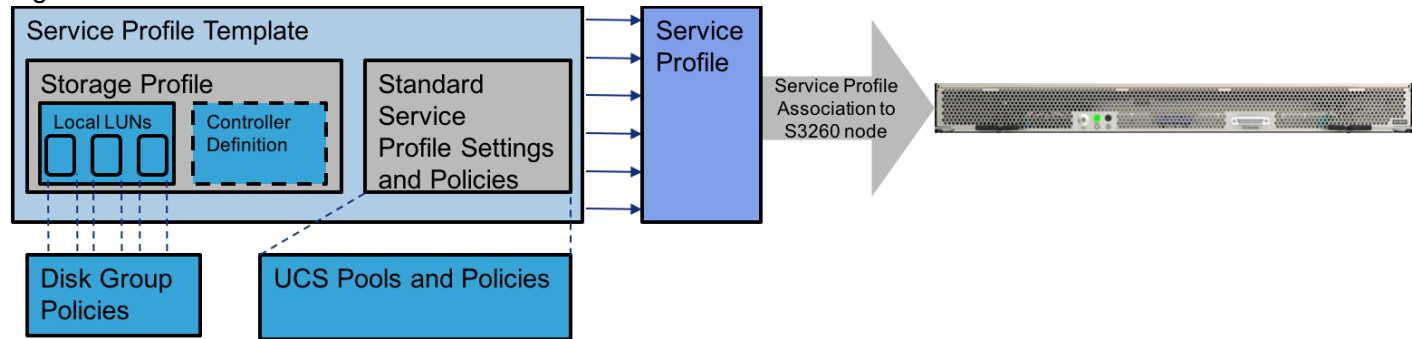
The S3260 can be CIMC managed, or Cisco UCS Manager managed as a registered Chassis with the Cisco UCS Fabric Interconnects. When the S3260 is Cisco UCS Manager managed, the Chassis will use a Chassis Profile can be generated from template, and will contain specifications for Firmware and Maintenance 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 8 Cisco UCS S3260 Chassis Profile Association



Server Nodes in a Cisco UCS Manager managed 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 will use Service Profiles that can be provisioned from template, but will need to have a Storage Profile set within the Service Profile to be able to access the disk slots made available to it by the Disk Zoning Policy set within the Chassis Profile of the Chassis the Node is hosted within.

Figure 9 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. The secondary function for a Storage Profile is a Controller Definition used by S3260 M3 server nodes, which sets how the PCH Controller should handle the rear facing SSDs of the S3260 Chassis. The Controller Definition is specific to the SSD drives allocated to the node by the PCH Controller and will have valid settings of RAID 0, 1, or no RAID.



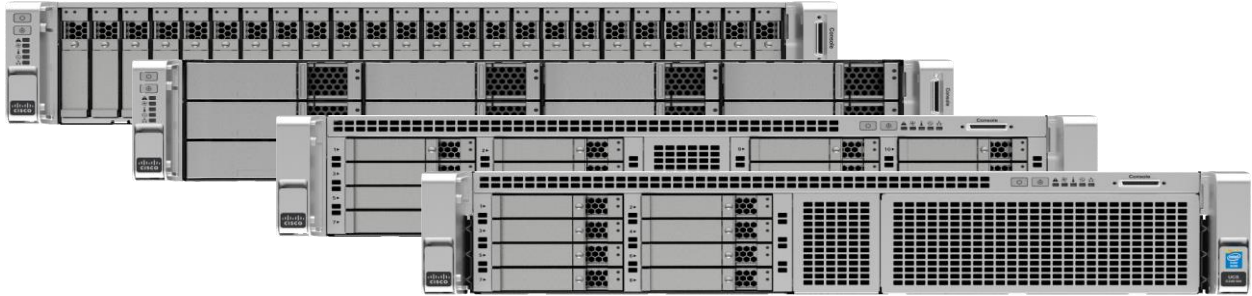
S3260 M4 server nodes do not use a Controller Definition, and will have their allocated rear facing SSD drives configured by a Disk Group Policy specified by a manual slot specification for the LUN.

Cisco UCS C240

The Cisco UCS C240 M4 Rack Server is a modular blend of CPU, Memory, Storage, IO, and expansion capabilities in a 2RU form-factor. This delivers exceptional performance and expandability to workloads such as big data analytics, virtualization, GPU intensive, and bare-metal applications. The C240 comes equipped with:

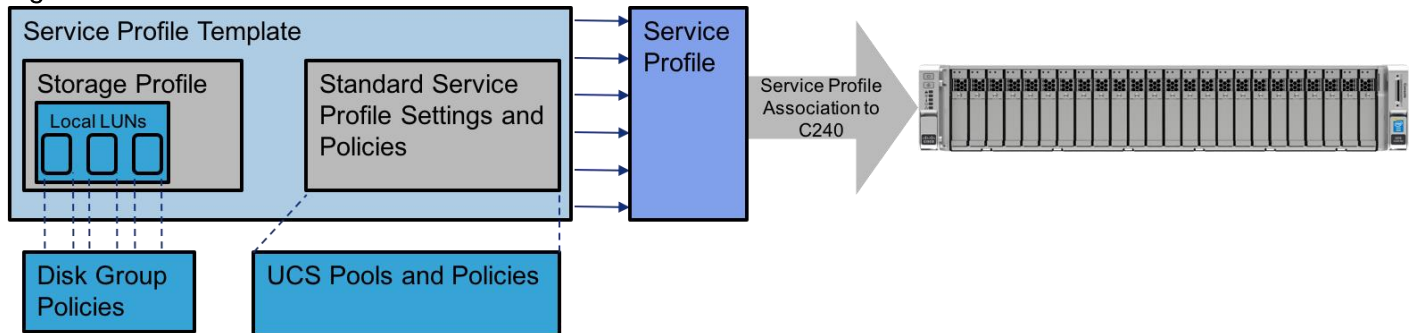
- Dual Intel® Xeon® E5-2600 v3 or v4 processors for improved performance suitable for nearly all two-socket applications
- Next-generation double-data-rate 4 (DDR4) memory, 12-Gbps SAS throughput, and NVMe PCIe SSD support
- Innovative Cisco UCS virtual interface card (VIC) support in PCIe or modular LAN-on-motherboard (mLOM) form factor for dual port 10Gb or 40Gb adapters.
- Graphics-rich experiences to more virtual users with support for the latest NVIDIA graphics processing units (GPUs)

Figure 10 Cisco UCS C240 M4 in Multiple Backplane Options



Much like the Service Profile association of the S3260 server nodes, the Cisco UCS C240 will be configured with a Cisco UCS Manager Service Profile, and will use a Storage Profile within that Service Profile to utilize the front facing disk slots of the Cisco UCS C240. The front facing disk slots are managed by a SAS controller in the Cisco UCS C240, and will only need Disk Group Policies to create the Local LUNs to be set up for the Cisco UCS C240 within the Storage Profile.

Figure 11 Cisco UCS C240 Service Profile Association

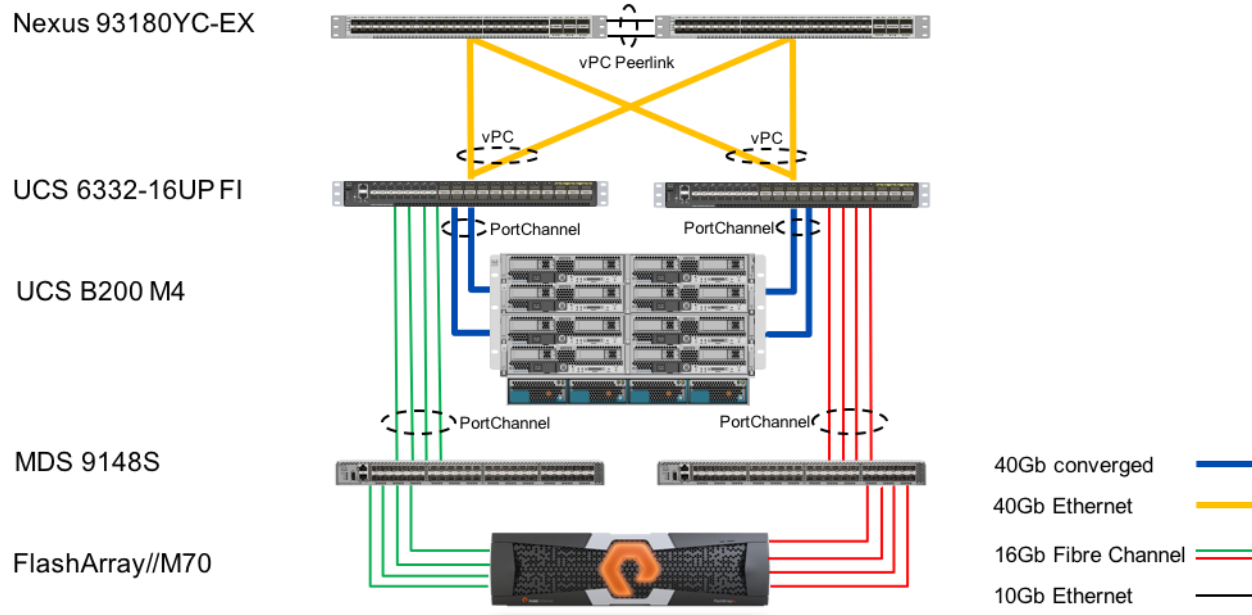


Solution Design

Requirements

The FlashStack VSI with Modern Data Protection architecture builds off of the design covered in the FlashStack VSI for VMware vSphere 6.0 U2 Design Guide.

Figure 12 FlashStack Virtual Server Infrastructure Architectural Diagram



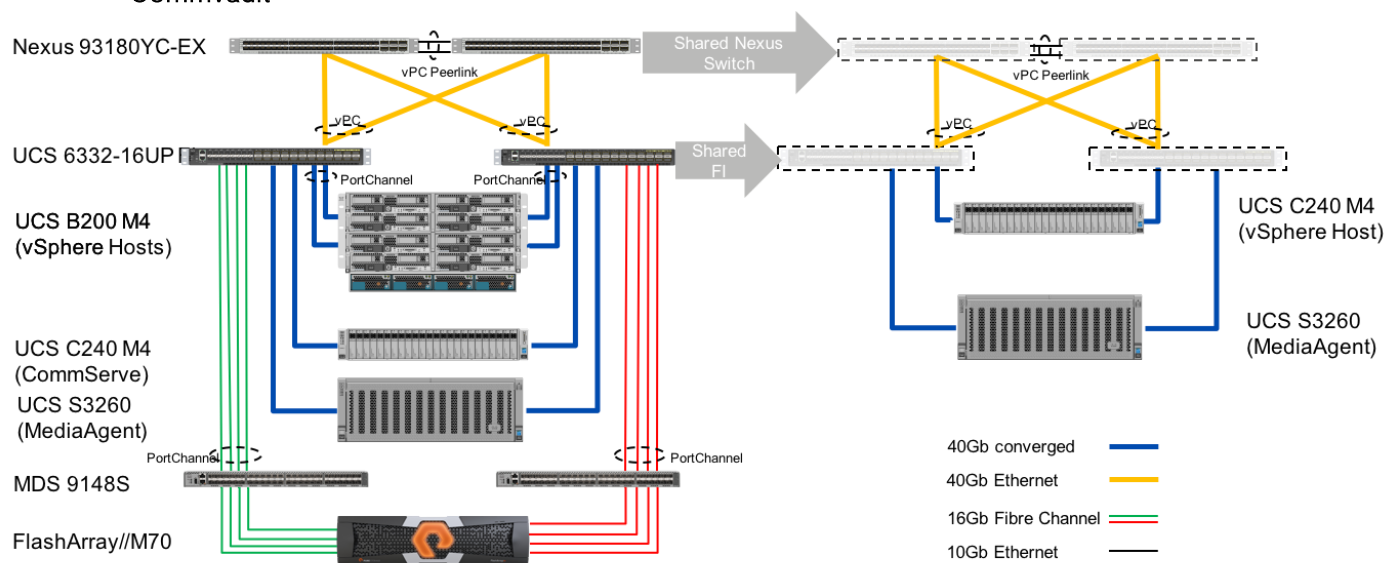
The full design will not be discussed in this document and should be referenced from here:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_flashstack_vsi_vm6_design_s.html

Physical Topology

The insertion of Cisco UCS S3260 and Cisco UCS C240 servers builds off of the original architecture as Cisco UCS Manager managed components. The S3260 with its large disk capacity was used as the Commvault MediaAgent for streaming backups off of the FlashArray//M, and the Cisco UCS C240 served as the Commvault CommServe and a remote independent ESXi instance using its own storage for restoration testing.

Figure 13 Components Added to the FlashStack VSI Architecture in the Validation of Data Protection with Commvault

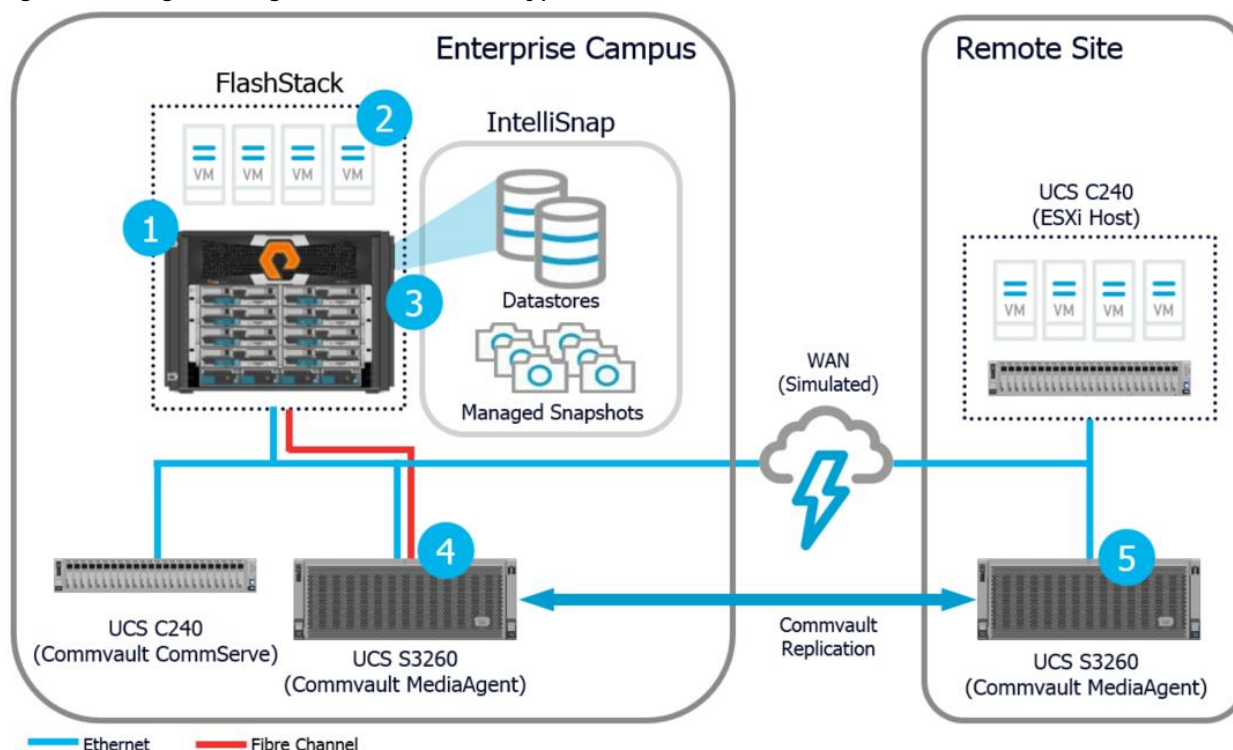


Cisco UCS Manager management, network, and SAN connectivity are brought into the S3260 through their dual-port 40Gb System I/O Controller (SIOC) modules. The SIOC incorporate the VIC 1300 architecture within them allowing the configuration flexibility of multiple virtual NICs, and vHBAs as is common in Cisco UCS VIC converged network adapters.

Logical Topology

The solutions logical topology shows both single site protection and (simulated) secondary site disaster recovery requirements. Figure 14 shows the automated steps that the Commvault Data Platform will perform for FlashStack VSI.

Figure 14 Logical Diagram of the Traffic Types within FlashStack VSI with Data Protection



1. Commvault performs auto-discovery against VMware vCenter to discover new datastores and virtual machines.
2. Commvault, in conjunction with VMware vCenter, synchronizes VMs to ensure application consistent images on the Pure Storage FlashArray are ready for protection.
3. IntelliSnap technology communicates with the Pure Storage FlashArray to take snapshot(s).
4. Snapshot(s) are mounted for incremental forever secondary copy creation on MediaAgent for longer term retention.
5. Commvault deduplicated replication transfers data to secondary location for disaster recovery.

Considerations

Customer environments and the number of FlashStack VSI components will vary from site to site; Commvault and Cisco reference architectures are included in the Appendix for comparison purposes.

The CommServe can reside on a virtual or physical server. Customers may choose to deploy the CommServe on a physical Cisco UCS server or as a VM within the FlashStack VSI. This design physically separates the data protection layer from the production layer (FlashStack VSI). This ensures that data protection and recover operations do not have dependencies and minimizes workload imposed on the FlashStack VSI.

Deployment Hardware and Software

The deployment of hardware and software for FlashStack VSI with Data Protection covers the following:

- Connecting the Cisco UCS S3260 Storage Server and the Cisco UCS C240 Rack Server to the FlashStack VSI
- The setup of the Cisco UCS S3260 Storage Server
- The setup of a Cisco UCS C240 Rack Server
- The installation of Commvault CommServe on the Cisco UCS C240 Rack Server and the installation of Commvault MediaAgent on the Cisco UCS S3260 Storage Server

The existing deployment of the FlashStack VSI architecture is assumed, and the setup of these resources will have dependencies covered in the FlashStack VSI for VMware vSphere 6.0 U2 Deployment Guide that is available at:

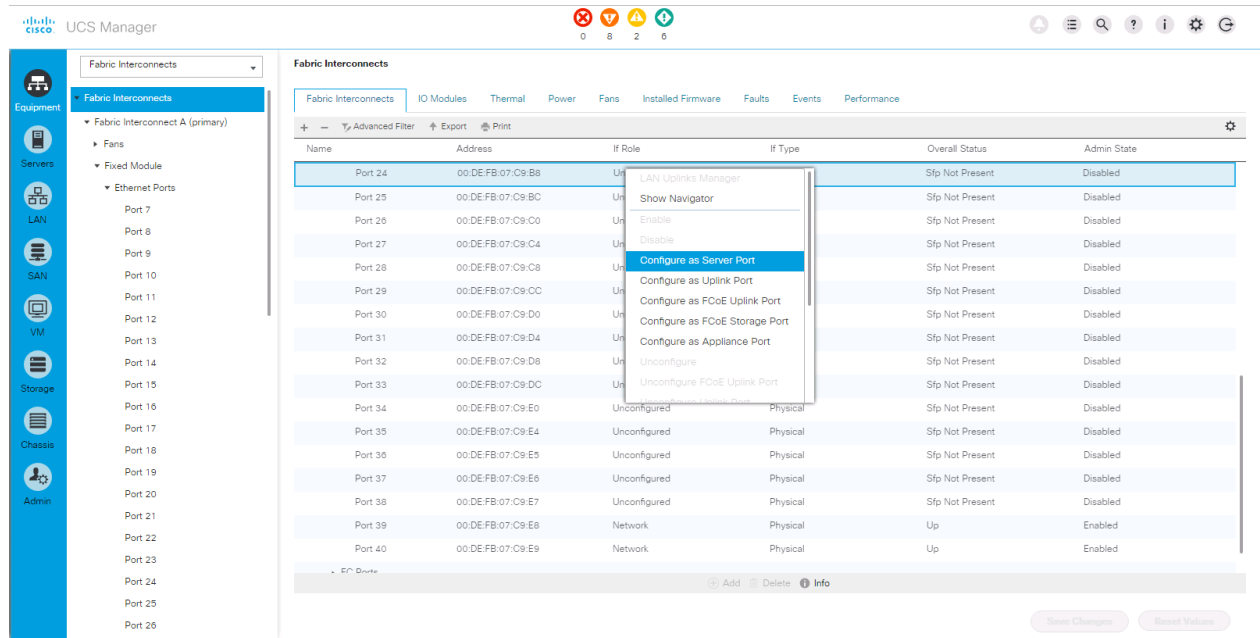
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_flashstack_vsi_vm6.html

Connecting the Cisco UCS S3260 Storage Server and the Cisco UCS C240 Rack Server

The Cisco UCS S3260 (S3260) rack servers and Cisco UCS C240 (C240) rack servers connect to each 6332-16UP Fabric Interconnect in the FlashStack VSI using available 40Gb ports. For 40Gb connectivity, the Cisco UCS S3260 uses an SIOC (one per equipped server node), and the Cisco UCS C240 will use a VIC 1387(mLOM) or VIC 1385(PCIe) Converged Network Adapter. For each adapter type, the QSFP+ port labeled Port 1 should go into an available 40Gb port of the A side Fabric Interconnect, and the port labeled Port 2 should go into an available 40Gb port of the B side Fabric Interconnect.

To set the selected 40Gb ports used on each Fabric Interconnect as Server Ports, complete the following steps:

1. In Cisco UCS Manager, click Equipment within the Navigation Pane and select Fabric Interconnects from within the Equipment drop-down options.
2. Within the Fabric Interconnect tab, find the available port the S3260 or C240 is connecting to and right-click it, selecting Configure as Server Port.



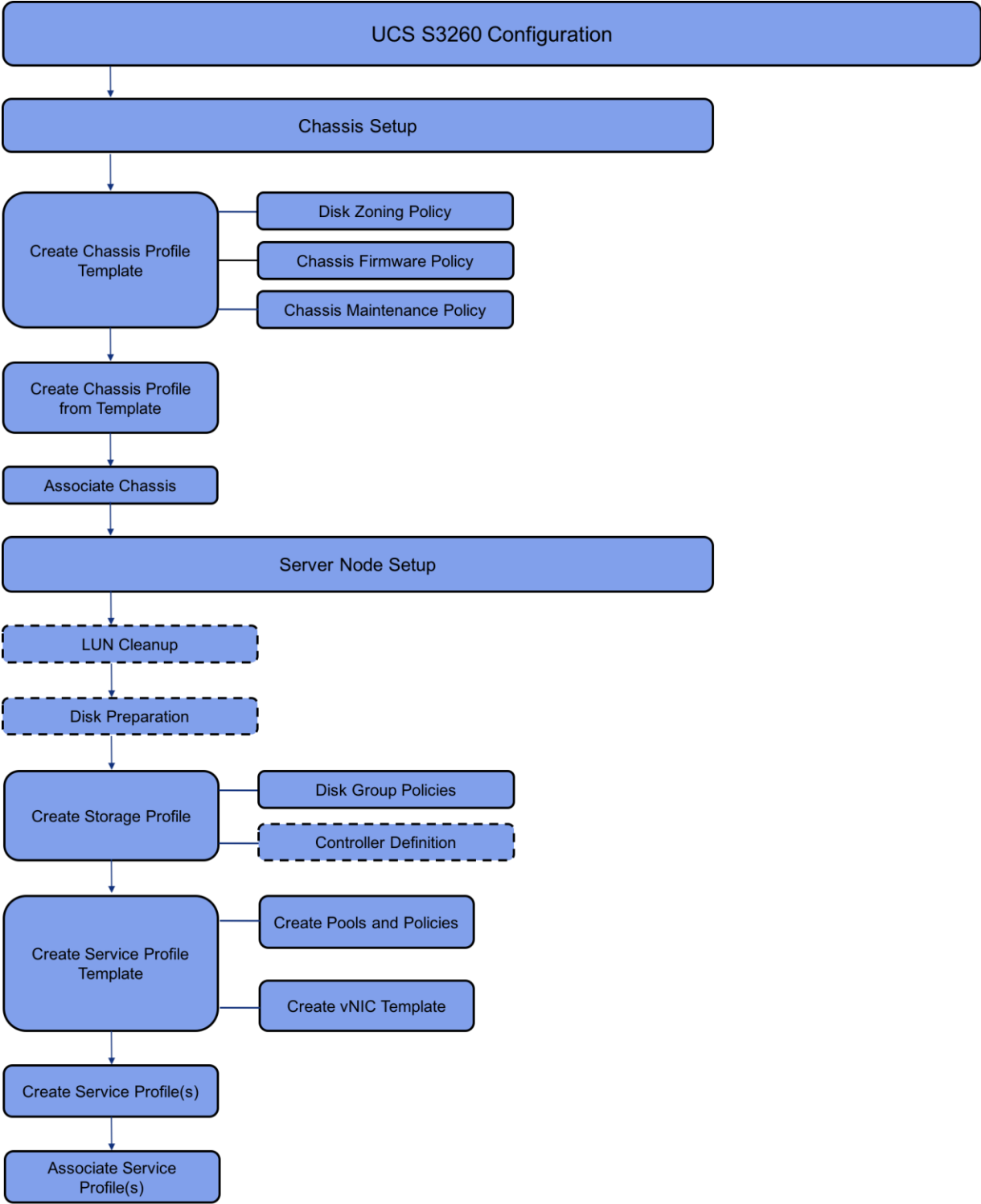
3. Click Save Changes to apply.
4. Repeat these steps for each Fabric Interconnect and each server being added.



Previously unmanaged Cisco UCS S3260 Rack Servers will need to run a minimum of Cisco IMC release 2.0(13). Upgrade instructions for this can be found [here](#).

Cisco UCS S3260 Insertion into FlashStack VSI

The S3260 configuration has two main components, the creating and associating the S3260 Chassis Profile, and the S3260 Server Node Setup which will involve Service Profile creation and association using a Storage Profile.



Cisco UCS S3260 Chassis Setup

Chassis Profile Template

The Chassis Profile can be deployed independently, but to maximize consistency allowed within Cisco UCS, the Chassis Profiles can be generated from the Chassis Profile Templates. To create a Chassis Profile Template, three policies are used:

- Disk Zoning Policy
- Chassis Maintenance Policy
- Chassis Firmware Policy

Disk Zoning Policy

The Disk Zoning Policy allocates disk slots between server nodes in the chassis. To create a Disk Zoning Policy, complete the following steps:

1. In Cisco UCS Manager, click Chassis within the Navigation Pane and select Policies from within the Chassis drop-down options.
2. Right-click Disk Zoning Policies and select Create Disk Zoning Policy.
3. Provide an appropriate Name for the Disk Zoning Policy, leave Preserve Config unselected.

Create Disk Zoning Policy

?

×

Name : CVLT-MA-Zoning

Description :

Preserve Config : ☐

Disk Zoning Information

+ - Advanced Filter Export Print

Name	Slot Number	Ownership	Assigned to Ser...	Assigned to Con...	Controller Type
No data available					

+ Add

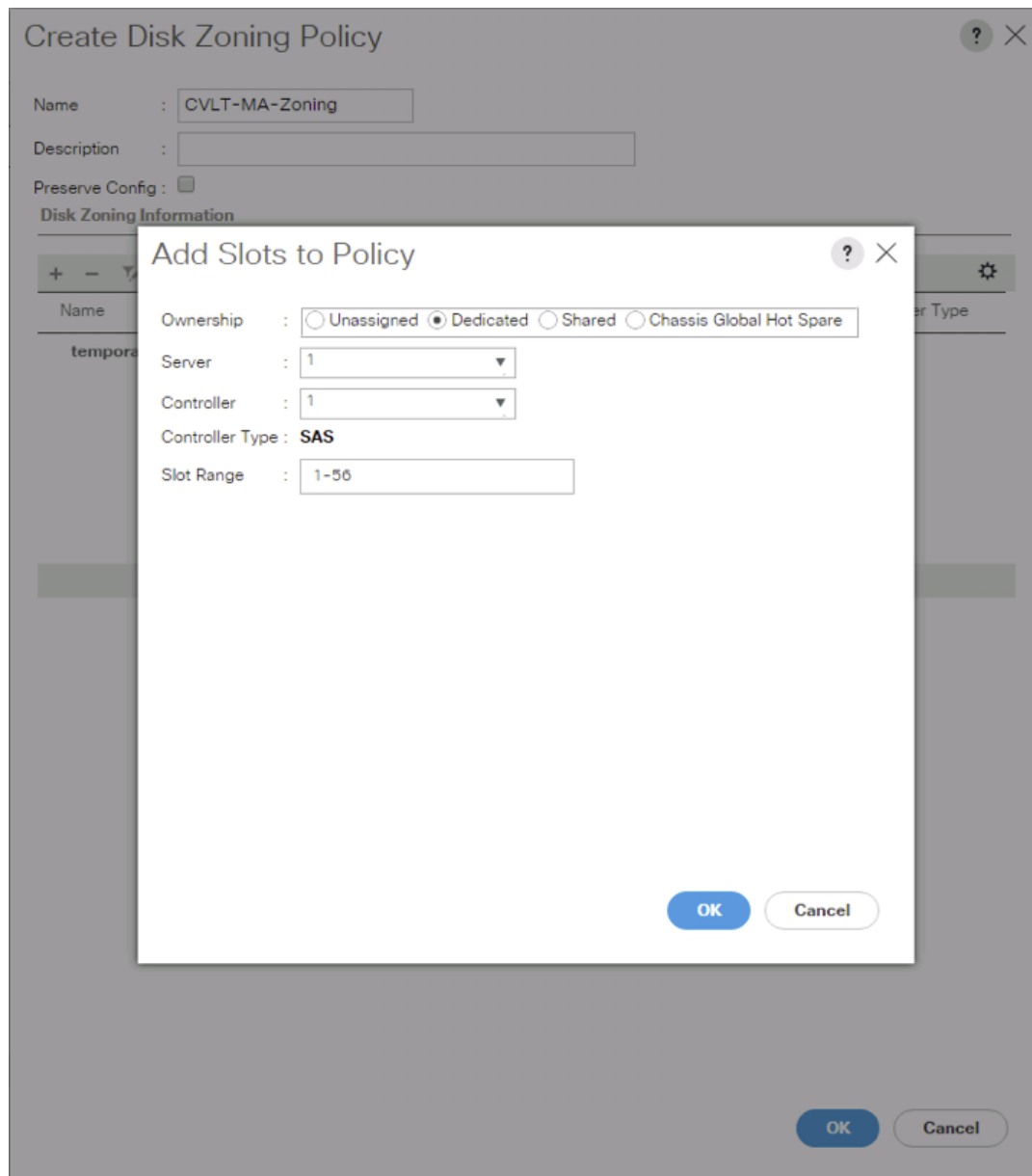
Delete

Modify

OK

Cancel

4. Click Add within the Disk Zoning Information section to set the disk slot associations for the chassis.



5. For this deployment, the S3260 is utilizing one node, so within the Add Slots to Policy dialogue:
 - a. Click the Dedicated option for Ownership.
 - b. Select 1 for the Server.
 - c. Select 1 for the Controller.
 - d. Enter 1-56 for the Slot Range.
6. Click OK to confirm the Add Slots to Policy options.
7. Click OK to create the Disk Zoning Policy.

Chassis Maintenance Policy

The available policy is the Default Chassis Maintenance Policy and it is set for User Ack for Reboot.

Chassis Firmware Policy

The Chassis Firmware Policy applies the appropriate firmware package to the chassis. To create a Chassis Firmware Policy, complete the following steps:

1. In Cisco UCS Manager, click Chassis within the Navigation Pane and select Policies from within the Chassis drop-down options.
2. Right-click the Chassis Firmware Packages, and select Create Chassis Firmware Package.
3. Provide the Chassis Firmware Package with an appropriate name (UCS-3260), select the 3.1(2b)C Chassis Package, and leave Local Disk as the only option selected under Excluded Components.

The screenshot shows the 'Create Chassis Firmware Package' dialog box. The 'Name' field is filled with 'UCS-3260'. The 'Description' field is empty. The 'Chassis Package' dropdown is set to '3.1(2b)C'. The 'Excluded Components' section has a list of checkboxes: 'Chassis Board' (unchecked), 'Chassis Manager' (unchecked), 'Chassis Adapter' (unchecked), 'Local Disk' (checked), and 'SAS Expander' (unchecked). The 'OK' button is highlighted in blue.

4. Click OK to create the Chassis Firmware Package policy.

Create the Chassis Profile Template

With the Policies used by the Chassis Profile in place, to create the Chassis Profile Template complete the following steps:

1. In Cisco UCS Manager, click Chassis within the Navigation Pane and select Chassis Profile Templates from within the Chassis drop-down options.
2. Right-click and select Create Chassis Profile Template.
3. Provide a name for the Chassis Profile Template and for Type select Updating Template.

1

Identify Chassis Profile Template

2

Chassis Maintenance Policy

3

Policies

4

Disk Zoning Policy

Create Chassis Profile Template

?

×

You must enter a name for the chassis profile template and specify the template type. You can also enter a description of the template.

Name : S3260-1node

The template will be created in the following organization. Its name must be unique within this organization.
Where : org-root

Type : ☐ Initial Template ☒ Updating Template

Optionally enter a description for the template. The description can contain information about when and where the chassis profile template should be used.

< Prev

Next >

Finish

Cancel

4. Select the default Chassis Maintenance Policy.

1

Identify Chassis Profile Template

2

Chassis Maintenance Policy

3

Policies

4

Disk Zoning Policy

Create Chassis Profile Template

?

×

Specify how disruptive changes (such as reboot, network interruptions, firmware upgrades) should be applied to the system.

⊖ Chassis Maintenance Policy

Select a maintenance policy to include with this chassis profile template or create a new maintenance policy that will be accessible to all chassis profile templates.

Chassis Maintenance Policy: Select (no policy used by default) Create Chassis Maintenance Policy

Select (no policy used by default)

Domain Policies

default

No maintenance policy is selected. The chassis profile will inherit the default policy.

< Prev

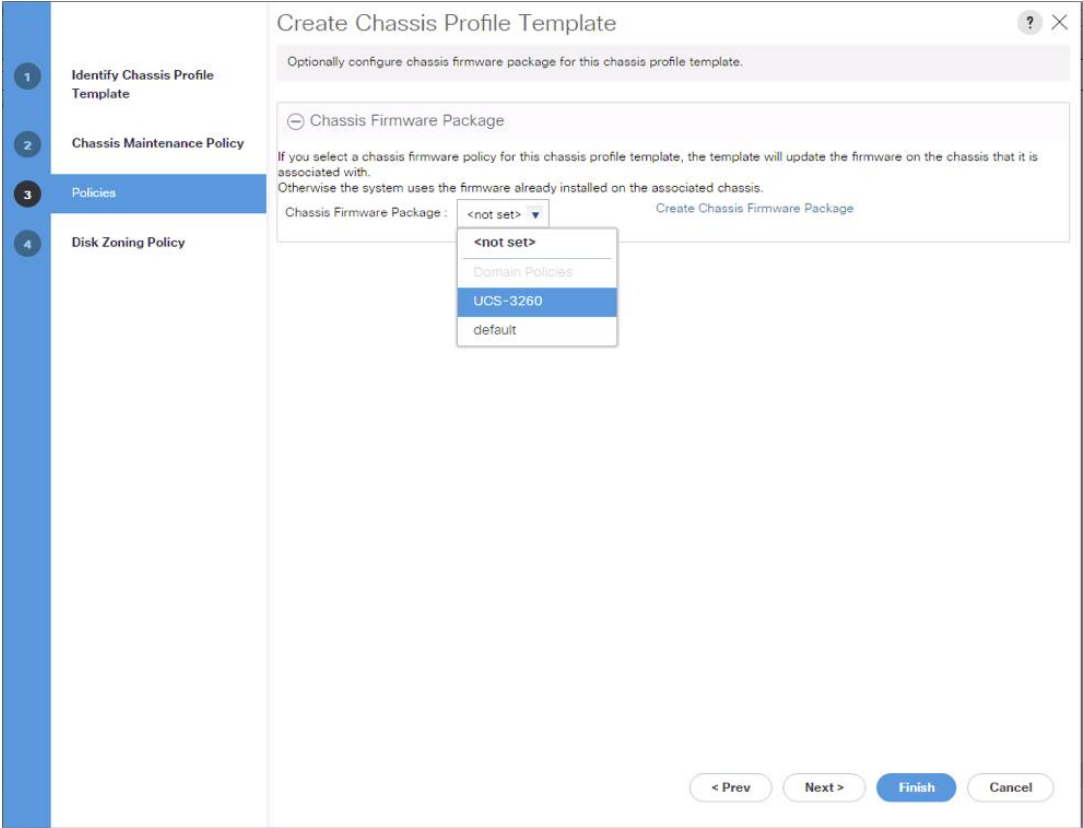
Next >

Finish

Cancel

5. Set the Chassis Firmware Package to the UCS-3260 package previously created.

34



6. Select the CVLT-MA-Zoning Disk Zoning Policy that was previously created.

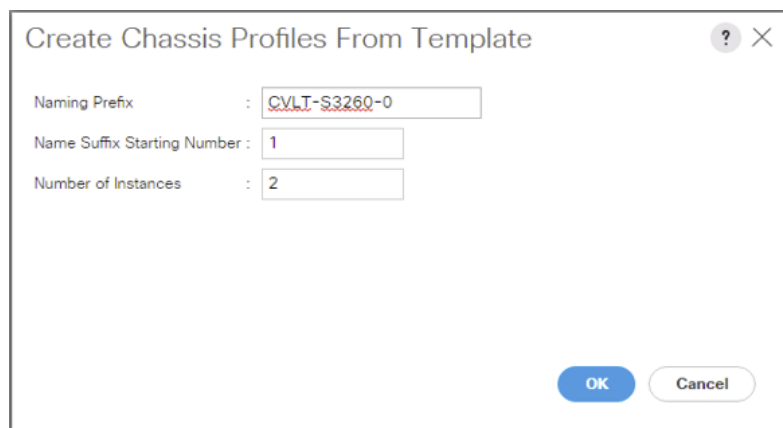
7. Click Finish to create the Chassis Profile Template.

Create Chassis Profile(s) from Template

The Chassis Profile Template has been created with policies appropriate for both S3260 Storage Servers used in the environment, so as a result there will be two Chassis Profiles created in this section.

To create chassis profiles, complete the following steps:

1. In Cisco UCS Manager, click Chassis within the Navigation Pane and select Chassis Profile Templates from within the Chassis drop-down options.
2. Right-click the newly created Chassis Profile Template and select the Create Chassis Profiles from Template option.
3. Specify a Naming Prefix, the Name Suffix Starting Number, and the Number of Instances of Chassis Profiles to be created from the template.



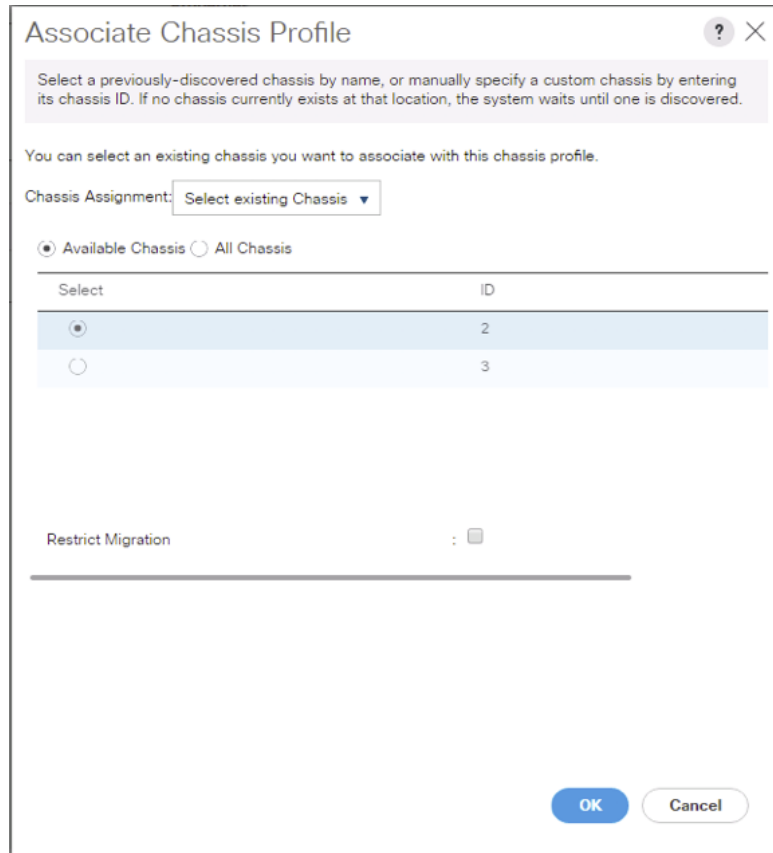
The image shows a dialog box titled "Create Chassis Profiles From Template". It has a question mark icon and a close button (X) in the top right corner. The dialog contains three input fields: "Naming Prefix" with the value "CVLT-S3260-0", "Name Suffix Starting Number" with the value "1", and "Number of Instances" with the value "2". At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

4. Click OK to create the Chassis Profiles.

Associate Chassis Profiles

Each Chassis Profile created can be associated to one of the connected S3260 Storage Servers. To associate the chassis profiles, complete the following steps:

1. In Cisco UCS Manager, click Chassis within the Navigation Pane and select Chassis Profiles from within the Chassis drop-down options.
2. Right-click one of the newly created Chassis Profiles and select Change Chassis Profile Association.
3. Choose Select the existing Chassis from the Chassis Assignment drop-down, and pick the appropriate Chassis ID to use.



Associate Chassis Profile [?] [X]

Select a previously-discovered chassis by name, or manually specify a custom chassis by entering its chassis ID. If no chassis currently exists at that location, the system waits until one is discovered.

You can select an existing chassis you want to associate with this chassis profile.

Chassis Assignment:

☒ Available Chassis ☐ All Chassis

Select	ID
<input checked="" type="radio"/>	2
<input type="radio"/>	3

Restrict Migration : ☐

OK Cancel

4. Click OK to associate the Chassis.
5. Repeat these steps for the second S3260s.

Cisco UCS S3260 Server Node Setup

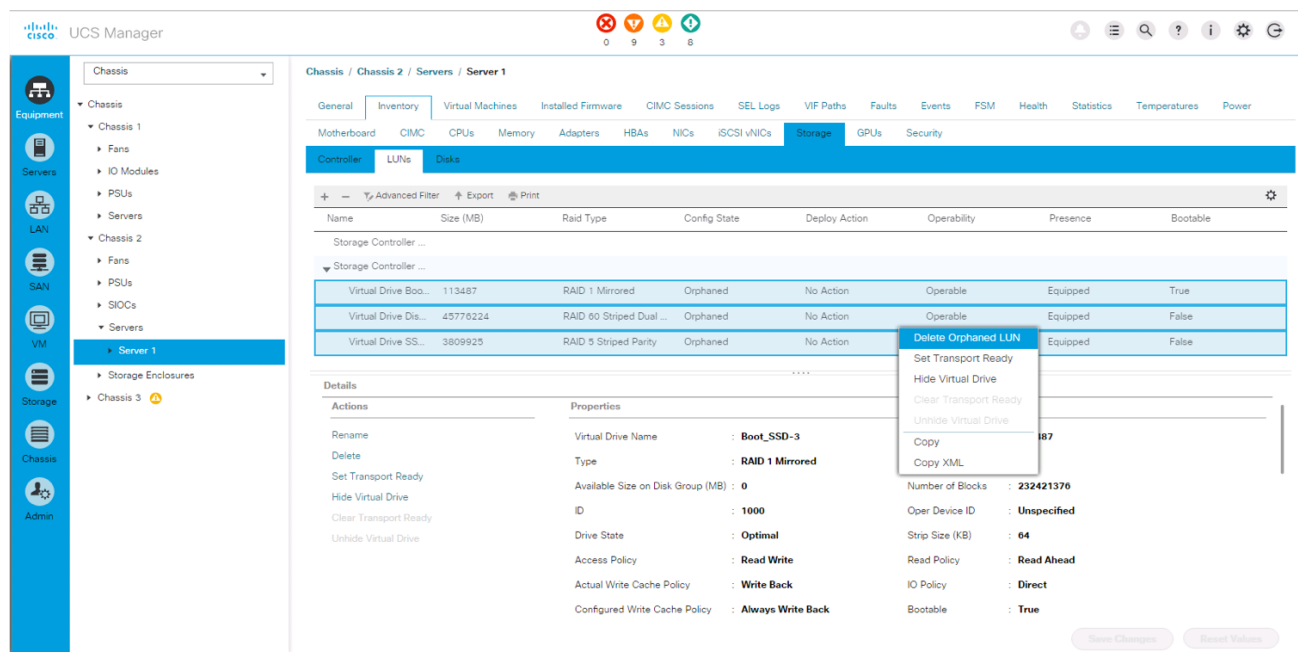
The server nodes will be configured using Service Profiles like other Cisco UCS Manager managed server resources, but will require a Storage Profile to use disks made available to them by disk slots designated for the server in the Disk Zoning Policy of Chassis Profile associated to the Chassis.

LUN Cleanup

For any S3260 server nodes that had LUNs created from previous Service Profile associations, there will be LUNs existing on those server nodes in an orphaned state preventing use of the disks from those LUNs to a new Service Profile association.

To clear up orphaned LUNs, complete the following steps:

1. In Cisco UCS Manager, click Equipment within the Navigation Pane and select Chassis from within the Equipment drop-down options.
2. Select the Chassis of the S3260 and click the server node within that chassis to clear LUNs from.
3. Within that server node, click the Inventory tab, then the Storage tab within that, and finally the LUNs tab of the Storage tab of the server node.



4. Select each of the Orphaned LUNs, and right-click the Delete Orphaned LUN option.

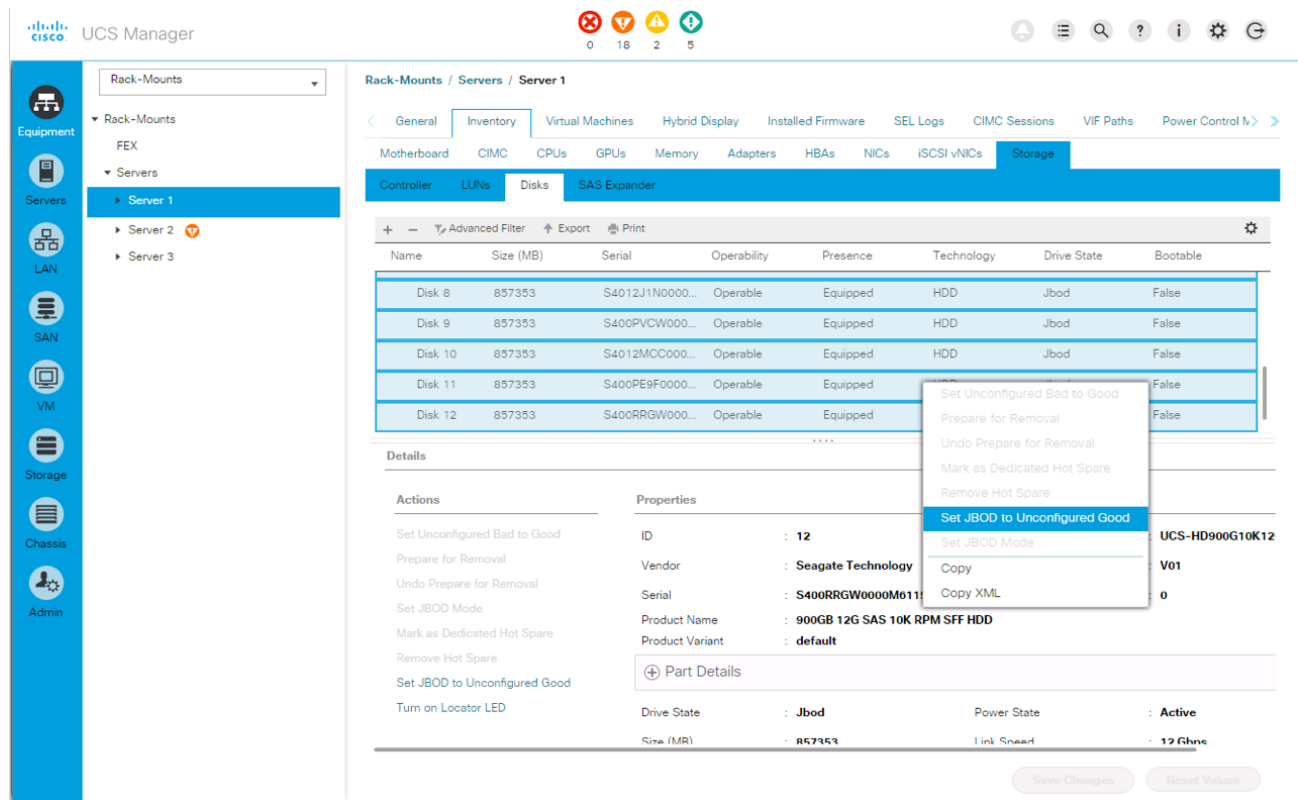
5. Click Yes to confirm the action, and OK to continue.

Disk Preparation

After the S3260 server nodes have had disks allocated to them through the Chassis Profile Association, new S3260s, as well as when newly inserted disks into an S3260, there will be disks set as Jbod within the Disks view of the Storage tab.

To set new disks to be available, complete the following steps:

1. In Cisco UCS Manager, click Equipment within the Navigation Pane and select Chassis from within the Equipment drop-down options.
2. Select the Chassis of the S3260 and click the server node within the chassis to prepare disks from.
3. Click the Inventory tab, then the Storage tab within that, and finally the Disks tab of the Storage tab of the server.



- Highlight each disk set as Jbod, and right-click Set JBOD to Unconfigured Good.



For setting a large number of disks from Jbod to Unconfigured Good, it might take some time, and the best view of the status will be in the FSM tab of the server node.

Cisco UCS S3260 Storage Profile

The Storage Profile consists of Storage Policies used for creating Local LUNs out of allocated disks (Disk Group Policies).



For Cisco UCS S3260 M3 server nodes, a Controller Definition of the Embedded RAID Controller or PCH (Platform Controller HUB) used by the rear panel SSD of the S3260 is created within the Storage Profile, instead of a Local LUN Disk Group Policy for those SSDs.

Disk Group Policies

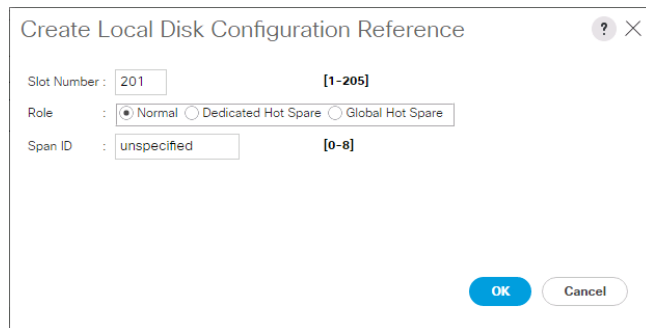
Three Disk Group Policies were created for the MediaAgent deployment on the Cisco UCS S3260 based on the Medium MediaAgent configuration options specified in Table 3

- Boot_SSD_rear1 – Boot LUN of the rear SSD slots in a RAID 1 configuration.
- S3260-SSD_Cache – SSD Cache used by the MediaAgent consisting of 6xSSD in RAID 5 with one hot spare.
- S3260-Disk_Lib – Disk Library of the MediaAgent using 16xHDD in RAID 60 with two hot spares.

Each of these Disk Group Policies will create Local LUNs for the S3260 server nodes, utilizing available disks of specific types, or from manual slot specification.

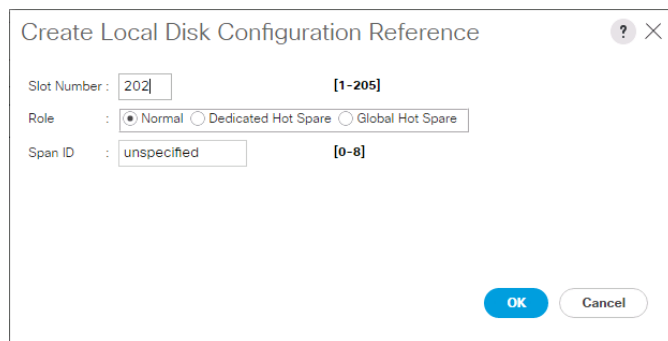
To create the Boot_SSD_rear1 Disk Group Policy, complete the following steps:

1. In Cisco UCS Manager, click Storage within the Navigation Pane, and select Storage Policies from within the Storage drop-down options.
2. Right-click and select Create Disk Group Policy.
3. Provide the following:
 - a. An appropriate Name (Boot_SSD_rear1)
 - b. Select RAID 1 Mirrored
 - c. Select Disk Group Configuration (Manual)
 - d. Click Add and enter 201 for the Slot Number



The screenshot shows a dialog box titled "Create Local Disk Configuration Reference". It contains three input fields: "Slot Number" with the value "201" and a range "[1-205]", "Role" with radio buttons for "Normal" (selected), "Dedicated Hot Spare", and "Global Hot Spare", and "Span ID" with the value "unspecified" and a range "[0-8]". At the bottom right, there are "OK" and "Cancel" buttons. The "OK" button is highlighted in blue.

4. Click OK.
5. Click Add again and enter 202 for the Slot Number.



The screenshot shows the same dialog box as before, but with the "Slot Number" field now containing the value "202". The "OK" button remains highlighted in blue.

6. For the Virtual Drive Configuration:
 - a. Set Stripe Size to 64KB
 - b. Set Read Policy to Read Ahead
 - c. Set Write Cache Policy to Always Write Back

Create Disk Group Policy ? ×

RAID Level : RAID 1 Mirrored

☐ Disk Group Configuration (Automatic) ☒ Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Advanced Filter Export Print ⚙️

Slot Number	Role	Span ID
201	Normal	Unspecified
202	Normal	Unspecified

+ Add - Delete i Info

Virtual Drive Configuration

Strip Size (KB) : 64KB

Access Policy : Platform Default

Read Policy : ☐ Platform Default ☒ Read Ahead ☐ Normal

Write Cache Policy : ☐ Platform Default ☐ Write Through ☐ Write Back Good Bbu ☒ Always Write Back

OK Cancel

7. Click OK to create the Disk Group Policy.



Manual slot number specifications for the rear SSD can be found in Cisco UCS Manager -> Equipment -> Chassis -> Chassis [chassis #] -> Servers -> Server [server #] -> Storage Enclosures -> Storage Enclosure 3, but should be 201-202 for server node 1 and 203-204 for server node 2.

To create the S3260-SSD-Cache Disk Group Policy, complete the following steps:

1. In Cisco UCS Manager, click Storage within the Navigation Pane, and select Storage Policies from within the Storage drop-down options.
2. Right-click and select Create Disk Group Policy.
3. Provide the following:
 - a. An appropriate Name (S3260-SSD-Cache)
 - b. Select RAID 5 Striped Parity
 - c. Specify Number of Drives to 6
 - d. Set Drive Type to SSD
 - e. Set a Dedicated Hot Spare if available
 - f. Set Stripe Size to 64KB
 - g. Set Read Policy to Normal
 - h. Set Write Cache Policy to Write Through

Create Disk Group Policy

Name : S3260-SSD-Cache

Description :

RAID Level : RAID 5 Striped Parity

☒ Disk Group Configuration (Automatic) ☐ Disk Group Configuration (Manual)

Disk Group Configuration (Automatic)

Number of drives : 6 [0-60]

Drive Type : ☐ Unspecified ☐ HDD ☒ SSD

Number of Dedicated Hot Spares : 1 [0-60]

Number of Global Hot Spares : unspecified [0-60]

Min Drive Size (GB) : unspecified [0-10240]

Use Remaining Disks : ☒

Virtual Drive Configuration

Strip Size (KB) : 64KB

Access Policy : Platform Default

Read Policy : ☐ Platform Default ☐ Read Ahead ☒ Normal

Write Cache Policy : ☐ Platform Default ☒ Write Through ☐ Write Back Good Bbu ☐ Always Write Back

OK Cancel

4. Click OK to create the Disk Group Policy.

To create the S3260-Disk-Lib Disk Group Policy, complete the following steps:

1. In Cisco UCS Manager, click Storage within the Navigation Pane, and select Storage Policies from within the Storage drop-down options.
2. Right-click and select Create Disk Group Policy.
3. Provide the following:
 - a. An appropriate Name (S3260-Disk-Lib)
 - b. Select RAID 60 Striped Dual Parity
 - c. Specify Number of Drives to 16
 - d. Set Drive Type to HDD
 - e. Set 2 Dedicated Hot Spares
 - f. Set Stripe Size to 512KB
 - g. Set Read Policy to Read Ahead
 - h. Set Write Cache Policy to Always Write Back

?

×

Create Disk Group Policy

Name : S3260-Disk-Lib

Description :

RAID Level : RAID 60 Striped Dual Parity ▾

☒ Disk Group Configuration (Automatic)
 ☐ Disk Group Configuration (Manual)

Disk Group Configuration (Automatic)

Number of drives : 16 [0-60]

Drive Type : ☐ Unspecified ☒ HDD ☐ SSD

Number of Dedicated Hot Spares : 2 [0-60]

Number of Global Hot Spares : unspecified [0-60]

Min Drive Size (GB) : unspecified [0-10240]

Use Remaining Disks : ☐

Virtual Drive Configuration

Strip Size (KB) : 512KB ▾

Access Policy : Platform Default ▾

Read Policy : ☐ Platform Default ☒ Read Ahead ☐ Normal

Write Cache Policy : ☐ Platform Default ☐ Write Through ☐ Write Back Good Bbu ☒ Always Write Back

OK

Cancel

- Click OK to create the Disk Group Policy.

Create the Media Agent Storage Profile

To create the MediaAgent Storage Profile, complete the following steps:

- In Cisco UCS Manager, click Storage within the Navigation Pane, and select Storage Profiles from within the Storage drop-down options.
- Right-click and select Create Storage Profile.
- Provide a name for the Storage Profile (S3260-MediaAgent).

Create Storage Profile [?] [X]

Name :

Description :

LUNs

Local LUNs | Controller Definitions

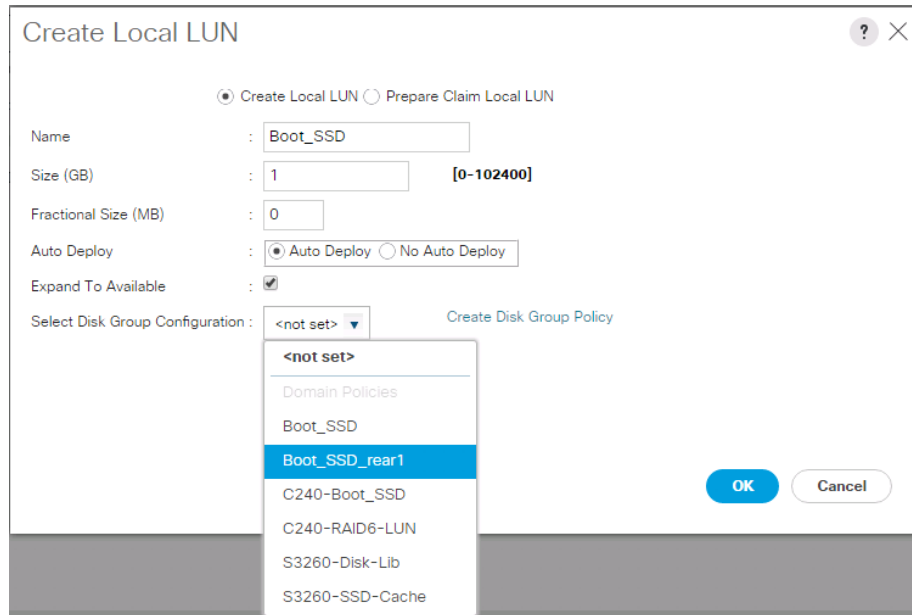
Advanced Filter | Export | Print | [Settings]

Name	Size (GB)	Order	Fractional Size (MB)
No data available			

[+ Add] [Delete] [Info]

[OK] [Cancel]

4. Select Add within the Local LUNs tab to add a LUN that will be created from the Boot_SSD_rear1 Disk Group Policy.
5. Provide the following in the Create Local LUN dialogue:
 - a. Name: Boot_SSD
 - b. Leave the Size at 1
 - c. Leave Auto Deploy selected as Auto Deploy
 - d. Click Expand to Available
 - e. Select the Boot_SSD_rear1 Disk Group Policy from the Select Disk Group Configuration drop-down

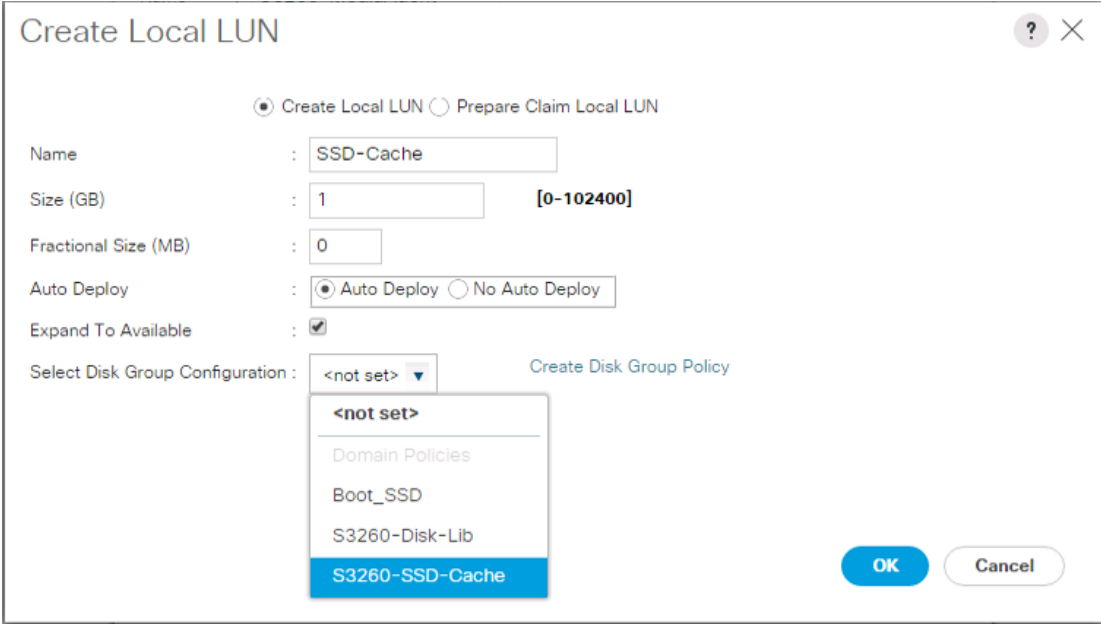


The image shows a 'Create Local LUN' dialog box with the following fields and options:

- Name:** Boot_SSD
- Size (GB):** 1 (range [0-102400])
- Fractional Size (MB):** 0
- Auto Deploy:** ☒ Auto Deploy ☐ No Auto Deploy
- Expand To Available:** ☒
- Select Disk Group Configuration:** A dropdown menu is open, showing the following options:
 - <not set>
 - Domain Policies
 - Boot_SSD
 - Boot_SSD_rear1** (highlighted)
 - C240-Boot_SSD
 - C240-RAID6-LUN
 - S3260-Disk-Lib
 - S3260-SSD-Cache

Buttons: OK, Cancel

6. Click OK to add the Local LUN.
7. Select Add within the Local LUNs tab to add a LUN that will be created from the SSD-Cache Disk Group policy.
8. Provide the following in the Create Local LUN dialogue:
 - a. Name: SSD-Cache
 - b. Leave the Size at 1
 - c. Leave Auto Deploy selected as Auto Deploy
 - d. Click Expand to Available
 - e. Select the S3260-SSD-Cache Disk Group Policy from the Select Disk Group Configuration drop-down



The image shows a 'Create Local LUN' dialog box with the following fields and options:

- Radio Buttons:** ☒ Create Local LUN, ☐ Prepare Claim Local LUN
- Name:** Text field containing 'SSD-Cache'
- Size (GB):** Text field containing '1', with a range indicator '[0-102400]' to its right.
- Fractional Size (MB):** Text field containing '0'.
- Auto Deploy:** Radio buttons for ☒ Auto Deploy and ☐ No Auto Deploy.
- Expand To Available:** Checkmark icon.
- Select Disk Group Configuration:** A dropdown menu currently showing '<not set>'. A tooltip is open, showing a list of policies: '<not set>', 'Domain Policies', 'Boot_SSD', 'S3260-Disk-Lib', and 'S3260-SSD-Cache' (which is highlighted in blue). A link 'Create Disk Group Policy' is visible to the right of the dropdown.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

9. Click OK to add the Local LUN.
10. Select Add within the Local LUNs tab to add a LUN that will be created from the Disk-Lib Disk Group policy
11. Provide the following in the Create Local LUN dialogue:
 - a. Name: Disk-Lib
 - b. Leave the Size at 1
 - c. Leave Auto Deploy selected as Auto Deploy
 - d. Click Expand to Available
 - e. Select the S3260-Disk-Lib Disk Group Policy from the Select Disk Group Configuration drop-down

Create Local LUN

☒ Create Local LUN
 ☐ Prepare Claim Local LUN

Name :

Size (GB) : **[0-102400]**

Fractional Size (MB) :

Auto Deploy : ☒ Auto Deploy ☐ No Auto Deploy

Expand To Available : ☒

Select Disk Group Configuration : [Create Disk Group Policy](#)

<not set>
 Domain Policies
 Boot_SSD
S3260-Disk-Lib
 S3260-SSD-Cache

OK Cancel

12. Click OK to add the Local LUN.

13. Click OK to create the Storage Profile.

Cisco UCS S3260 Service Profile

In addition to the Storage Profile, a couple of new policies and pools will need to be made before a Service Profile can be created for the S3260 Server Node.

Cisco UCS S3260 Server Pool

The S3260 Server Pool will contain S3260 Server Nodes to be used for the MediaAgent. To create the Server Pool to use, complete the following steps:

1. In Cisco UCS Manager, click Server within the Servers Pane, and select Pools from within the Server drop-down options.
2. Right-click Server Pools and select Create Server Pool.
3. Enter an appropriate name for the Server Pool (S3260-MediaAgent), and click Next.

1

Set Name and Description

2

Add Servers

Create Server Pool

?

×

Name

:

S3260-MediaAgent

Description


:

< Prev

Next >

Finish

Cancel

 The S3260 were acknowledged in this environment as chassis 2 and chassis 3, so select these numbers, or the appropriate chassis number in your environment if they differ, and click the >> button between the Servers list and the Pooled Servers list.

Create Server Pool

1 Set Name and Description

2 Add Servers

Servers

Chassi...	P...
2	F...
1	F...
3	1	...	F...	24	...
2	1	...	F...	24	...
1	1	...	F...	28	...
1	2	...	F...	28	...
1	3	...	F...	16	...
1	4	...	F...	16	...
1	5	...	F...	16	...
1	6	...	F...	20	...
1	7	...	F...	12	...
1	8	...	F...	20	...

Model: UCSC-C3K-M4SRB
Serial Number: FCH2033JEFF
Vendor: Cisco Systems Inc

Pooled Servers

... SL... R... U... PID A... S... C...

No data available

Model:
Serial Number:
Vendor:

< Prev Next > Finish Cancel

4. Click Finish to create the server pool.

Create Boot Policy

A boot policy will be needed to boot from the Boot_SSD_rear1 Local LUN created during the Disk Group Policy party of the Storage Profile. To create the Boot Policy complete the following steps:

1. In Cisco UCS Manager, click Server within the Navigation Pane, and select Policies from within the Server drop-down options.
2. Right-click Boot Policies under root, and select Create Boot Policy.
3. Provide a name for the policy (Boot_SSD), and add a Remote CD/DVD (used for KVM vMedia booting) under Local Devices.

Create Boot Policy

Name

: Boot_SSD

Description

:

Reboot on Boot Order Change

:

☐

Enforce vNIC/vHBA/iSCSI Name

:

☒

Boot Mode

:

☒ Legacy

☐ Uefi

WARNINGS:

The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Local Devices

Add Local Disk

Add Local LUN

Add Local JBOD

Add SD Card

Add Internal USB

Add External USB

Add Embedded Local LUN

Add Embedded Local Disk

Add CD/DVD

Add Local CD/DVD

Add Remote CD/DVD

Add Floppy

Boot Order

+ - Advanced Filter Export Print

Name	Order	vNIC/v...	Type	WWN	LUN N...	Slot N...	Boot ...	Boot P...	Descri...
Remote CD/DVD	1								

Move Up Move Down Delete

Set Disk Boot Parameters

OK

Cancel

4. Click Add Local LUN to reference the Boot_SSD LUN created by the Boot_SSD_rear1 Disk Group Policy.

Create Boot Policy

Name

: Boot_SSD

Description

:

Reboot on Boot Order Change

:

☐

Enforce vNIC/vHBA/iSCSI Name

:

☒

Boot Mode

:

☒ Legacy

☐ Uefi

WARNINGS:

The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Local Devices

Add Local Disk

Add Local LUN

Add Local JBOD

Add SD Card

Add Internal USB

Add External USB

Add Embedded Local LUN

Add Embedded Local Disk

Add CD/DVD

Add Local CD/DVD

Add Remote CD/DVD

Add Floppy

Add Local Floppy

Add Remote Floppy

Boot Order

+ - Advanced Filter Export Print

Name	Order	vNIC/v...	Type	WWN	LUN N...	Slot N...	Boot ...	Boot P...	Descri...
Remote CD/DVD	1								

Move Up Move Down Delete

Set Disk Boot Parameters

OK

Cancel

Add Local LUN Image Path

Type

:

☒ Primary

☐ Secondary

☐ Any

LUN Name

:

Boot_SSD

OK

Cancel

5. Click OK, and click OK again to create the Boot Policy.

51

Create Windows 40Gb Adapter Policy

Some Ring Size adjustments and a Receive Side Scaling enablement will be set for a Windows specific adapter for increased performance using 40Gb NICs. To create the Adapter Policy complete the following steps:

1. In Cisco UCS Manager, click Server within the Navigation Pane, and select Policies from within the Server drop-down options.
2. Right-click Adapter Policies and select Create Ethernet Adapter Policy.
3. Provide a name (Windows-40G) for the Adapter Policy and specify the following options:
 - a. Transmit Queues: 8
 - b. Ring Size: 4096
 - c. Receive Queues: 8
 - d. Ring Size: 4096
 - e. Completion Queues: 16
 - f. Interrupts: 32
 - g. Receive Side Scaling(RSS): Enabled

Create Ethernet Adapter Policy

Name :

Description :

Resources

Transmit Queues	: <input type="text" value="8"/>	[1-1000]
Ring Size	: <input type="text" value="4096"/>	[64-4096]
Receive Queues	: <input type="text" value="8"/>	[1-1000]
Ring Size	: <input type="text" value="4096"/>	[64-4096]
Completion Queues	: <input type="text" value="16"/>	[1-2000]
Interrupts	: <input type="text" value="32"/>	[1-1024]

Options

Transmit Checksum Offload	: <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Receive Checksum Offload	: <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
TCP Segmentation Offload	: <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
TCP Large Receive Offload	: <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Receive Side Scaling (RSS)	: <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Accelerated Receive Flow Steering	: <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Network Virtualization using Generic Routing Encapsulation	: <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Virtual Extensible LAN	: <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

OK **Cancel**

4. Click OK to create the Adapter Policy.

Create vNIC Template

The MediaAgent and the CommServe could use the LAN Connectivity Policy and vNIC Templates that the vSphere hosts use in the FlashStack VSI architecture, but only the In-Band Management Network is needed. Other vNICs would go unused by the Windows OS, and we can also setup A-B fabric failover within a new vNIC Template that will save us the steps of configuring NIC Teaming within the Windows OS.

To create a vNIC Template that will be used by the MediaAgent and the CommServe, complete the following steps:

1. In Cisco UCS Manager, click LAN within the Navigation Pane, and select Policies from within the Network drop-down options.
2. Right-click vNIC Templates under the root Org, and select Create vNIC Template.
3. Provide a Name for the vNIC Template and set the following options:
 - a. Fabric ID: Enable Failover
 - b. Template Type: Updating Template
 - c. VLANs: IB-Mgmt with Native VLAN selected

Create vNIC Template

Name

: vNIC_IB-Mgmt_AB

Description

:

Fabric ID

: ☒ Fabric A ☐ Fabric B ☒ Enable Failover

Redundancy

Redundancy Type

: ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Target

☒ Adapter ☐ VM

Warning

If **VM** is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type

: ☐ Initial Template ☒ Updating Template

VLANs

Advanced Filter

Export

Print

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-Branch	<input type="radio"/>
<input checked="" type="checkbox"/>	IB-Mgmt	<input checked="" type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input type="checkbox"/>	...	<input type="radio"/>

OK

Cancel

4. Scroll down to the second half of the window and select these additional options:

- d. MAC Pool: MAC_Pool_A
- e. Network Control Policy: Enable_CDP

Create vNIC Template

VLANs

Advanced Filter Export Print

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-Branch	<input type="radio"/>
<input checked="" type="checkbox"/>	IB-Mgmt	<input checked="" type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-App-1	<input type="radio"/>
<input type="checkbox"/>	VM-App-2	<input type="radio"/>

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 1500

MAC Pool : MAC_Pool_A(35/64)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set>

OK Cancel

5. Click OK to create the vNIC Template.

Create Service Profile Template

With the Storage Profile ready and the vNIC Template prepared the Service Profile Template can be created; complete the following steps:

1. In Cisco UCS Manager, click Servers within the Navigation Pane, and select Service Profile Templates from within the Server drop-down options.
2. Right-click root and select Create Service Profile Template to open the Create Service Profile Template wizard.
3. Enter an appropriate name (S3260-MediaAgent) as the name of the service profile template.
4. Select the “Updating Template” option.

- Under UUID, select UUID_Pool as the UUID pool.

Create Service Profile Template

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.

Name :

The template will be created in the following organization. Its name must be unique within this organization.
Where : **org-root**

The template will be created in the following organization. Its name must be unique within this organization.
Type : ☐ Initial Template ☒ Updating Template

Specify how the UUID will be assigned to the server associated with the service generated by this template.
UUID

UUID Assignment:

The UUID will be assigned from the selected pool.
The available/total UUIDs are displayed after the pool name.

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

< Prev Next > **Finish** Cancel

- Click Next.

- Configure Storage Provisioning:

- Click the Storage Profile Policy tab within Storage Provisioning, and select the Storage Profile previously created (S3260-MediaAgent).

Create Service Profile Template

Optionally specify or create a Storage Profile, and select a local disk configuration policy.

Specific Storage Profile | **Storage Profile Policy** | Local Disk Configuration Policy

Storage Profile: Select Storage Profile to use Create Storage Profile

No Storage P

Select Storage Profile to use

- No Storage Profile
- Storage Profiles
- Boot_SSD
- ESXi_Local_Disk
- S3260-MA-2
- S3260-MediaAgent**
- test

< Prev Next > **Finish** Cancel

b. Click Next.

8. Configure Networking:

- Keep the default setting for Dynamic vNIC Connection Policy.
- Select the “Expert” option** to configure the LAN connectivity.
- Click Add to add the vNIC.
- Click “Use vNIC Template”** in the Create vNIC window.

Create vNIC

Name :

MAC Address :

The Value is null, which is invalid for this field.

MAC Address Assignment :

Select (pool default used by default)

Create MAC Pool

Select MAC address assignment option.
If nothing is selected, the MAC address will be assigned from the default pool.

WARNING: The selected pool does not contain any available entities.
You can select it, but it is recommended that you add entities to it.

Use vNIC Template :

Fabric ID :

Fabric A

Fabric B

Enable Failover

VLAN in LAN cloud will take the precedence over the Appliance Cloud when there is a name clash.

VLANs

Advanced Filter

Export

Print

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-Branch	<input type="radio"/>
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-App-1	<input type="radio"/>
<input type="checkbox"/>	VM-App-2	<input type="radio"/>

Create VLAN

CDN Source :

vNIC Name

User Defined

OK

Cancel

e. Add an Appropriate name for the vNIC to create (vNIC-IB-Mgmt), select the vNIC_IB-Mgmt_AB for the vNIC Template, and select the Windows-40G policy from the Adapter Policy drop-down.

Create vNIC

Name :

vNIC-IB-Mgmt

Use vNIC Template :

☒

Redundancy Pair :

☐

Peer Name :

vNIC Template :

vNIC_IB-Mgmt_AB

Create vNIC Template

Adapter Performance Profile

Adapter Policy :

<not set>

Create Ethernet Adapter Policy

<not set>

Domain Policies

Linux

SMBClient

SMBServer

SRIOV

Solaris

VMWare

VMWarePassThru

Windows

Windows-40G

default

usNIC

usNICOracleRAC

OK

Cancel

- f. Click OK to add the vNIC.
- g. Click Next.

9. Configure Storage Options:

- a. **Select the Use Connectivity Policy option for the “How would you like to configure SAN connectivity?” field.**
- b. Pick the Infra-SAN-Policy option from the SAN Connectivity Policy drop-down menu.

Create Service Profile Template

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

☐ Simple
 ☐ Expert
 ☐ No vHBA
 ☒ Use Connectivity Policy

SAN Connectivity Policy : <not set> [Create SAN Connectivity Policy](#)

<not set>
 Domain Policies
Infra-SAN-Policy

< Prev Next > **Finish** Cancel

- c. Click Next.

10. Configure Zoning Options:

- a. Set no Zoning options and click Next. The next step in this process is to configure the vNIC/HBA placement.

11. Configure vNIC/HBA Placement:

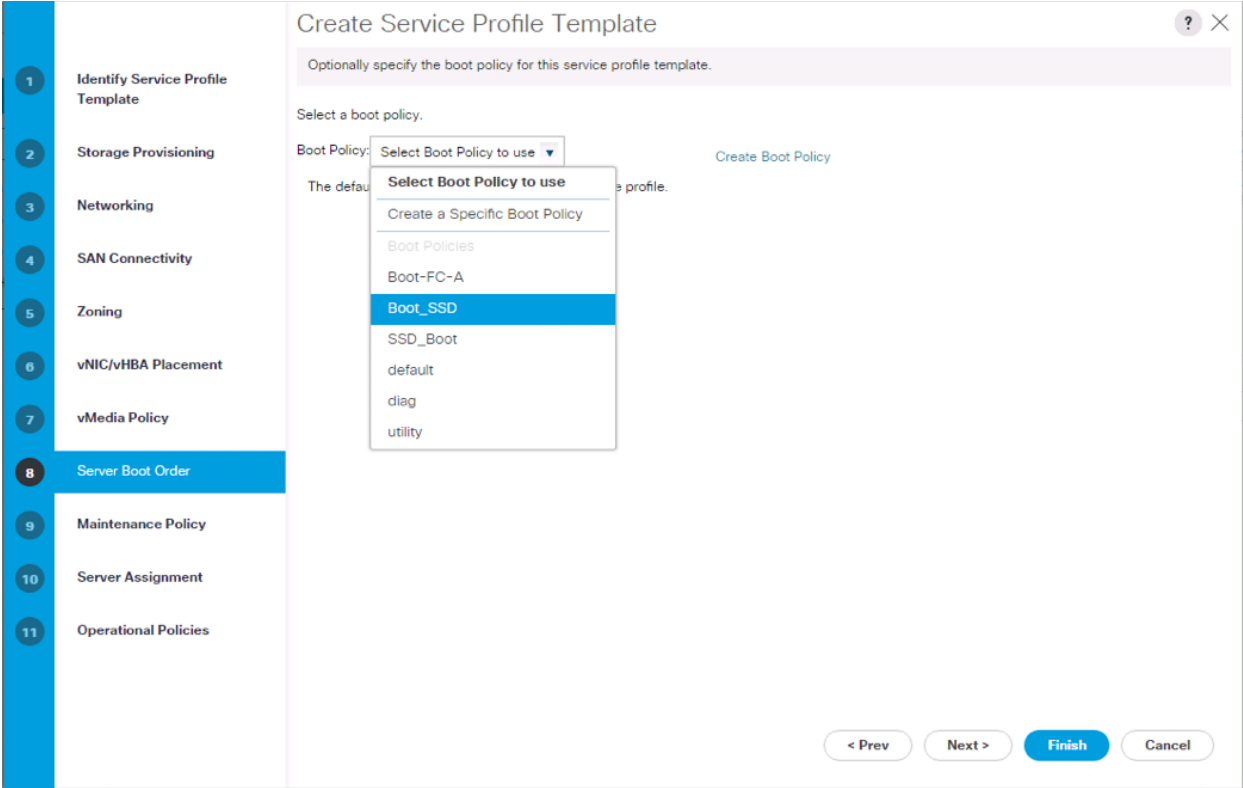
- a. In the “Select Placement” list, leave the placement policy as “Let System Perform Placement”.
- b. Click Next. The next step in this process is to configure the vMedia policy.

12. Configure vMedia Policy:

- a. Leave the vMedia Policy unselected.
- b. Click Next.

13. Configure Server Boot Order:

a. Select Boot_SSD for Boot Policy.



b. Click Next.

14. Configure Maintenance Policy:

a. Change the Maintenance Policy to default.

1

Identify Service Profile Template

2

Storage Provisioning

3

Networking

4

SAN Connectivity

5

Zoning

6

vNIC/vHBA Placement

7

vMedia Policy

8

Server Boot Order

9

Maintenance Policy

10

Server Assignment

11

Operational Policies

?

×

Create Service Profile Template

Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.

⊖

Maintenance Policy

Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

Maintenance Policy:

Select (no policy used by default)

Create Maintenance Policy

Select (no policy used by default)

Domain Policies

default

No maintenance policy is selected by default.

The service profile will immediately reboot when disruptive changes are applied.

< Prev

Next >

Finish

Cancel

b. Click Next.

15. Configure Server Assignment:

a. In the Pool Assignment list, select s3260-MediaAgent.

60

Create Service Profile Template

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment: S3260-MediaAgent Create Server Pool

Select the power state to be applied when this profile is associated with the server.

☒ Up ☐ Down

The service profile will be associated with one of the servers in the selected pool. If desired, you can select a pool policy qualification that the selected server must meet. To do so, select the qualification from the list.

Server Pool Qualification: **S3260-MediaAgent**

Restrict Migration: default

+ Firmware Management (BIOS, Disk Controller, Adapter)

< Prev Next > Finish Cancel

- b. Firmware Management at the bottom of the page can be left alone as it will use default from the Host Firmware list.
- c. Click Next.

16. Configure Operational Policies:

- a. In the BIOS Policy list, select VM-Host-Infra.
- b. Expand Power Control Policy Configuration and select **No-Power-Cap** in the Power Control Policy list.

Create Service Profile Template

Optionally specify information that affects how the system operates.

BIOS Configuration

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile

BIOS Policy : VM-Host-Infra

External IPMI Management Configuration

Management IP Address

Monitoring Configuration (Thresholds)

Power Control Policy Configuration

Power control policy determines power allocation for a server in a given power group.

Power Control Policy : default [Create Power Control Policy](#)

Scrub Policy

KVM Management

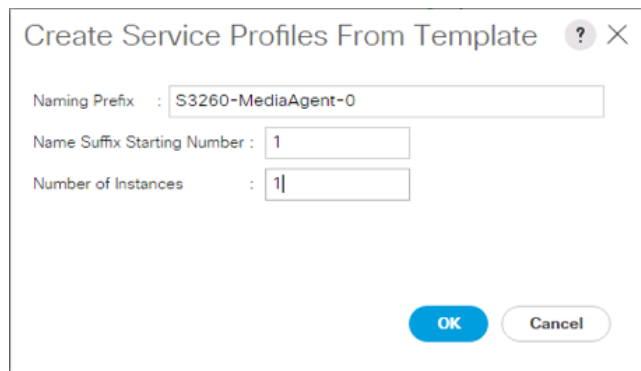
< Prev Next > **Finish** Cancel

- c. Click Finish to create the service profile template.
- d. Click OK in the confirmation message.
- e. Click Finish.

Create Service Profiles

To create a service profile from the service profile template, complete the following steps:

1. Connect to the UCS 6332-16UP Fabric Interconnect Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Template S3260-MediaAgent.
3. Right-click S3260-MediaAgent and select Create Service Profiles from Template.
4. Enter S3260-MediaAgent-0 as the service profile prefix.
5. Leave 1 as “Name Suffix Starting Number.”
6. Set 1 as the “Number of Instances.”
7. Click OK to create the service profiles.



Create Service Profiles From Template ? X

Naming Prefix : S3260-MediaAgent-0

Name Suffix Starting Number : 1

Number of Instances : 1

OK Cancel

8. Click OK in the confirmation message to provision the MediaAgent Service Profile.



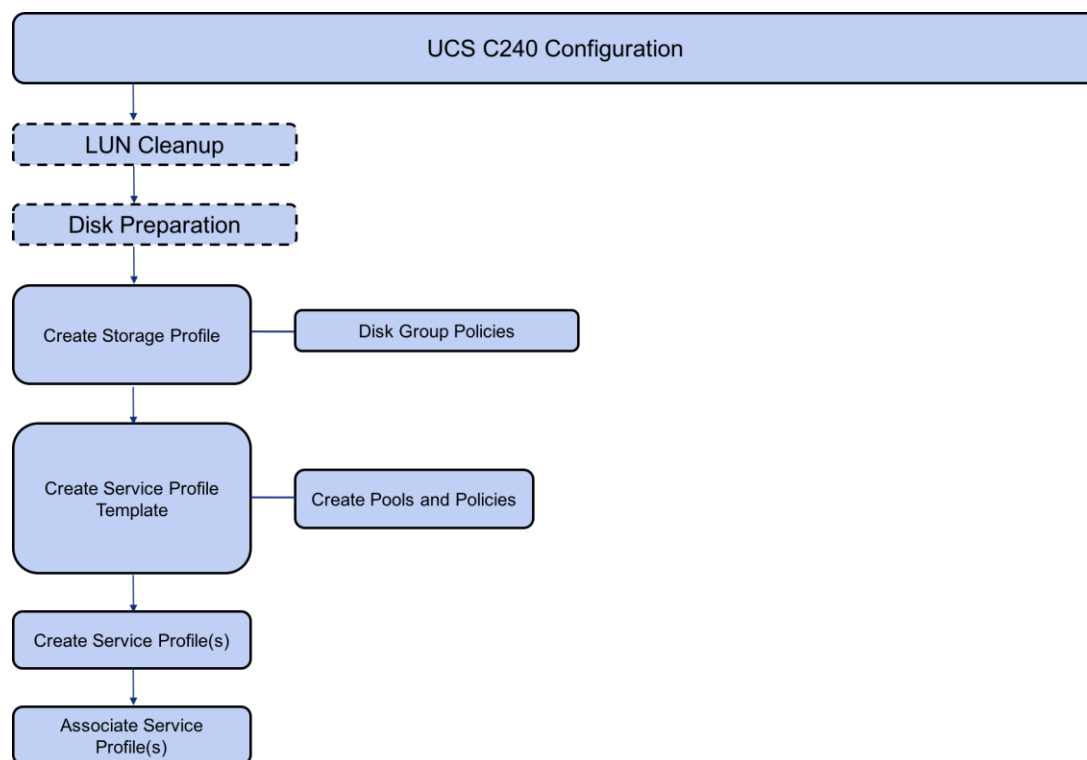
To create the second MediaAgent used in testing, a new vNIC template was created that was valid for the simulated secondary data center network. With the new vNIC template available, the S3260-MediaAgent Service Profile Template was cloned, and the secondary data center network appropriate vNIC template was swapped in for the vNIC_IB-Mgmt_AB vNIC template, and the simulated secondary data center MediaAgent was deployed from that cloned Service Profile Template.



In a real deployment to a secondary data center, this kind of uniformity for the configuration could be enabled with Cisco UCS Central managing the central and secondary data center Cisco UCS Domains. (Cisco UCS Central is not covered in this CVD).

Cisco UCS C240 Insertion to FlashStack

The Cisco UCS C240 will use a Storage Profile like the S3260, but will not need a Controller Definition, as the C240 in the environment had all disks in front facing drive slots. The Disk Policy created will be for a Local LUN to use as a boot device for CommServe, but others could be created if additional Local LUNs are needed.



LUN Cleanup

Like the S3260s, for C240 servers that had LUNs created from previous Service Profile associations, there will be LUNs existing on those servers in an orphaned state preventing use of the disks from those LUNs to a new Service Profile association.

To clear up orphaned LUNs, complete the following steps:

1. In Cisco UCS Manager, click Equipment within the Navigation Pane and select Rack-Mounts from within the Equipment drop-down options.
2. Select the server to clear LUNs from.
3. Within that server, click the Inventory tab, then the Storage tab within that, and finally the LUNs tab of the Storage tab of the server.
4. Select each of the Orphaned LUNs, and right-click the Delete Orphaned LUN option.
5. Click Yes to confirm the action, and OK to continue.

Disk Preparation

As with the S3260, for new C240s systems and newly inserted disks, the disks are set as Jbod within the Disks view of the Storage tab within the C240s.

To set new disks to be available, complete the following steps:

1. In Cisco UCS Manager, click Equipment within the Navigation Pane and select Rack-Mounts from within the Equipment drop-down options.

2. Click the server to prepare disks on from the list, click the Inventory tab, then the Storage tab within that, and finally the Disks tab of the Storage tab of the server.
3. Highlight each disk set as Jbod, and right-click Set JBOD to Unconfigured Good.



For setting a large number of disks from Jbod to Unconfigured Good, it might take some time, and the best view of the status will be in the FSM tab of the server.

Cisco UCS C240 Storage Profile

The Storage Profile will consist of Storage Policies used for the creation of a boot LUN out of SSD and a SQL database LUN created out of normal HDD, all coming out of the front facing slots of the Cisco UCS C240.

Disk Group Policies

To create the C240-Boot_SSD Disk Group Policy, complete the following steps:

1. In Cisco UCS Manager, click Storage within the Navigation Pane, and select Storage Policies from within the Storage drop-down options.
2. Right-click and select Create Disk Group Policy.
3. Provide the following:
 - a. An appropriate Name (C240-Boot_SSD)
 - b. Select RAID 1 Mirrored
 - c. Specify Number of Drives to 2
 - d. Set Drive Type to SSD
 - e. Set Stripe Size to 64KB
 - f. Set Read Policy to Read Ahead
 - g. Set Write Cache Policy to Always Write Back

Create Disk Group Policy

Name : C240-Boot_SSD

Description :

RAID Level : RAID 1 Mirrored

☒ Disk Group Configuration (Automatic) ☐ Disk Group Configuration (Manual)

Disk Group Configuration (Automatic)

Number of drives : 2 [0-60]

Drive Type : ☐ Unspecified ☐ HDD ☒ SSD

Number of Dedicated Hot Spares : unspecified [0-60]

Number of Global Hot Spares : unspecified [0-60]

Min Drive Size (GB) : unspecified [0-10240]

Use Remaining Disks : ☐

Virtual Drive Configuration

Strip Size (KB) : 64KB

Access Policy : Platform Default

Read Policy : ☐ Platform Default ☒ Read Ahead ☐ Normal

Write Cache Policy : ☐ Platform Default ☐ Write Through ☐ Write Back Good Bbu ☒ Always Write Back

OK Cancel

4. Click OK to create the Disk Group Policy.

To create the SQL-DB Disk Group Policy for the SQL database LUN, complete the following steps:

1. In Cisco UCS Manager, click Storage within the Navigation Pane, and select Storage Policies from within the Storage drop-down options.
2. Right-click and select Create Disk Group Policy.
3. Provide the following:
 - a. An appropriate Name (SQL-DB)
 - b. Select RAID 1 Mirrored
 - c. Specify Number of Drives to 2
 - d. Set Drive Type to HDD
 - e. Set Stripe Size to 64KB
 - f. Set Read Policy to Normal
 - g. Set Write Cache Policy to Always Write Back

?

×

Create Disk Group Policy

Name : SQL-DB

Description :

RAID Level : RAID 1 Mirrored

☒ Disk Group Configuration (Automatic)
 ☐ Disk Group Configuration (Manual)

Disk Group Configuration (Automatic)

Number of drives : 2 [0-60]

Drive Type : ☐ Unspecified ☒ HDD ☐ SSD

Number of Dedicated Hot Spares : unspecified [0-60]

Number of Global Hot Spares : unspecified [0-60]

Min Drive Size (GB) : unspecified [0-10240]

Use Remaining Disks : ☐

Virtual Drive Configuration

Strip Size (KB) : 64KB

Access Policy : Platform Default

Read Policy : ☐ Platform Default ☐ Read Ahead ☒ Normal

Write Cache Policy : ☐ Platform Default ☐ Write Through ☐ Write Back Good Bbu ☒ Always Write Back

OK

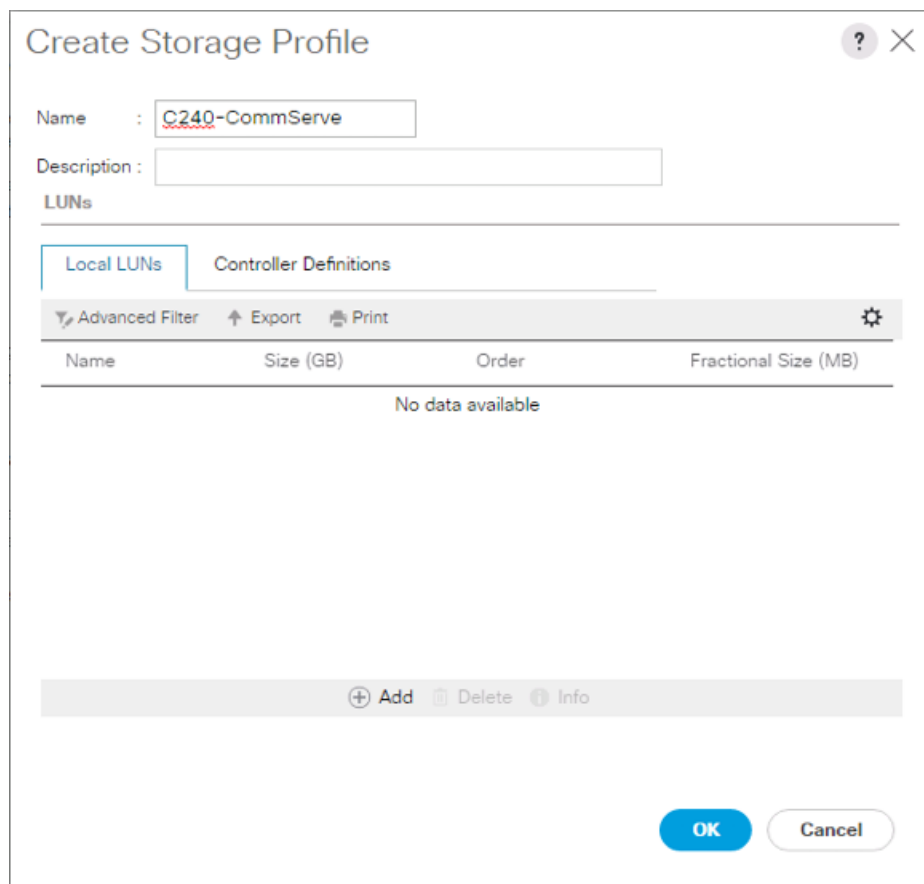
Cancel

4. Click OK to create the Disk Group Policy.

Create the CommServe Storage Profile

To create the CommServe Storage Profile, complete the following steps:

1. In Cisco UCS Manager, click Storage within the Navigation Pane, and select Storage Profiles from within the Storage drop-down options.
2. Right-click and select Create Storage Profile.
3. Provide a name for the Storage Profile (C240-CommServe).



The image shows a 'Create Storage Profile' dialog box. At the top, there is a title bar with a question mark icon and a close button. Below the title bar, there are two input fields: 'Name' with the value 'C240-CommServe' and 'Description' which is empty. Underneath these fields is a section titled 'LUNs'. This section contains two tabs: 'Local LUNs' (which is selected) and 'Controller Definitions'. Below the tabs is a toolbar with three icons: 'Advanced Filter', 'Export', and 'Print', followed by a settings gear icon. Below the toolbar is a table with four columns: 'Name', 'Size (GB)', 'Order', and 'Fractional Size (MB)'. The table is currently empty, with the text 'No data available' centered below the column headers. At the bottom of the 'LUNs' section is a bar with three icons: a plus sign for 'Add', a trash can for 'Delete', and an information icon for 'Info'. At the bottom right of the dialog box are two buttons: 'OK' and 'Cancel'.

4. Select Add within the Local LUNs tab to add a LUN that will be created from the C240-Boot_SSD Disk Group policy.
5. Provide the following in the Create Local LUN dialogue:
 - a. Name: Boot_SSD
 - b. Leave the Size at 1
 - c. Leave Auto Deploy selected as Auto Deploy
 - d. Click Expand to Available
 - e. Select the C240-Boot_SSD Disk Group Policy from the Select Disk Group Configuration drop-down

Create Local LUN

☒ Create Local LUN ☐ Prepare Claim Local LUN

Name :

Size (GB) : [0-102400]

Fractional Size (MB) :

Auto Deploy : ☒ Auto Deploy ☐ No Auto Deploy

Expand To Available : ☒

Select Disk Group Configuration : [Create Disk Group Policy](#)

Domain Policies

Boot_SSD

Boot_SSD_rear1

C240-Boot_SSD

C240-RAID6-LUN

S3260-Disk-Lib

S3260-SSD-Cache

OK Cancel

6. Click OK to add the Local LUN.
7. Select Add once again within the Local LUNs tab to add a LUN that will be created from the SQL-DB Disk Group policy.
8. Provide the following in the Create Local LUN dialogue:
 - a. Name: SQL-DB
 - b. Leave the Size at 1
 - c. Leave Auto Deploy selected as Auto Deploy
 - d. Click Expand to Available
 - e. Select the SQL-DB Disk Group Policy from the Select Disk Group Configuration drop-down

9. Click OK to add the Local LUN.
10. Click OK again to create the Storage Profile.



Since the Local LUN in this Storage Profile for the C240-Boot_SSD Disk Group Policy was named Boot_SSD, the Boot Policy used by the S3260 MediaAgent is reusable.

Cisco UCS C240 Service Profile

The Cisco UCS C240 Service Profile will use the Storage Profile created in the previous step, and will only need a dedicated Server Pool defined for it outside of the Pools and Policies defined by the base FlashStack VSI deployment, and the previous S3260 deployment steps.

Cisco UCS C240 Server Pool

The C240 Server Pool will contain C240 Rack Mount Servers that can be used for the CommServe. To create the Server Pool to use, complete the following steps:

1. In Cisco UCS Manager, click Server within the Servers Pane, and select Pools from within the Server drop-down options.
2. Right-click Server Pools and select Create Server Pool.
3. Enter an appropriate name for the Server Pool (C240-CommServe), and click Next.

1

Set Name and Description

2

Add Servers

Create Server Pool

?

×

Name

:

C240-CommServe

Description

:

< Prev

Next >

Finish

Cancel

4. Select the Rack IDs numbers for the appropriate C240s in your environment, and click the >> button between the Servers list and the Pooled Servers list.

1

Set Name and Description

2

Add Servers

Create Server Pool

?

×

Servers

⚙

Chassis ID ▲	Slot ID	Rack ID
	3	1 1 1
	2	1 1 1
	1	1 1 1
1	8	1 1 1 2
1	7	1 1 1 1
1	6	1 1 1 2
1	5	1 1 1 1
1	4	1 1 1 1
1	3	1 1 1 1
1	2	1 1 1 2
1	1	1 1 1 2
2	1	1 1 1 2

Model: UCSC-C240-M4SX
Serial Number: FCH1944V0E2
Vendor: Cisco Systems Inc

>>

<<

Pooled Servers

⚙

...	SL...	R...	U...	PID	A...	S...	C...
No data available							

Model:
Serial Number:
Vendor:

< Prev

Next >

Finish

Cancel

- Click Finish to create the server pool.

Create Service Profile Template

To create the C240 CommServe Service Profile Template, complete the following steps:

- In Cisco UCS Manager, click Servers within the Navigation Pane, and select Service Profile Templates from within the Server drop-down options.
- Right-click root and select Create Service Profile Template to open the Create Service Profile Template wizard.
- Enter an appropriate name (C240-CommServe) as the name of the service profile template.
- Select the “Updating Template” option.
- Under UUID, select UUID_Pool as the UUID pool.

Create Service Profile Template

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.

Name :

The template will be created in the following organization. Its name must be unique within this organization.
Where : **org-root**

The template will be created in the following organization. Its name must be unique within this organization.
Type : ☐ Initial Template ☒ Updating Template

Specify how the UUID will be assigned to the server associated with the service generated by this template.
UUID

UUID Assignment:

The UUID will be assigned from the selected pool.
The available/total UUIDs are displayed after the pool name.

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

< Previous Next > **Finish** Cancel

- Click Next.
- Configure Storage Provisioning:
 - Click the Storage Profile Policy tab within Storage Provisioning, and select the Storage Profile previously created (C240-CommServe).

Create Service Profile Template

Optionally specify or create a Storage Profile, and select a local disk configuration policy.

Specific Storage Profile | **Storage Profile Policy** | Local Disk Configuration Policy

Storage Profile: Select Storage Profile to use Create Storage Profile

No Storage Profile

Select Storage Profile to use

- No Storage Profile
- Storage Profiles
- Boot_SSD
- C240-CommServe**
- ESXi_Local_Disk
- S3260-MA-2
- S3260-MediaAgent
- test

< Prev Next > **Finish** Cancel

b. Click Next.

8. Configure Networking:

- Keep the default setting for Dynamic vNIC Connection Policy.
- Select the “Expert” option to configure the LAN connectivity.
- Click the Add to add the vNIC.
- Click “Use vNIC Template” within the resulting Create vNIC window.

Create vNIC

Name :

MAC Address :

The Value is null, which is invalid for this field.

MAC Address Assignment :

Select (pool default used by default)

Create MAC Pool

Select MAC address assignment option.
If nothing is selected, the MAC address will be assigned from the default pool.

WARNING: The selected pool does not contain any available entities.
You can select it, but it is recommended that you add entities to it.

Use vNIC Template :

Fabric ID :

☒ Fabric A

☐ Fabric B

☐ Enable Failover

VLAN in LAN cloud will take the precedence over the Appliance Cloud when there is a name clash.

VLANs

Advanced Filter

Export

Print

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-Branch	<input type="radio"/>
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-App-1	<input type="radio"/>
<input type="checkbox"/>	VM-App-2	<input type="radio"/>

Create VLAN

CDN Source :

☒ vNIC Name

☐ User Defined

OK

Cancel

- e. Add an Appropriate name for the vNIC to create (vNIC-IB-Mgmt), select the vNIC_IB-Mgmt_AB for the vNIC Template, and select the Windows-40G policy from the Adapter Policy drop-down.

Create vNIC

Name :

vNIC-IB-Mgmt

Use vNIC Template :

☒

Redundancy Pair :

☐

Peer Name :

vNIC Template :

vNIC_IB-Mgmt_AB

Create vNIC Template

Adapter Performance Profile

Adapter Policy :

<not set>

Create Ethernet Adapter Policy

<not set>

Domain Policies

Linux

SMBClient

SMBServer

SRIOV

Solaris

VMWare

VMWarePassThru

Windows

Windows-40G

default

usNIC

usNICOracleRAC

OK

Cancel

f. Click OK to add the vNIC.

g. Click Next.

9. Configure Storage Options:

a. Select the No vHBAs option for the “How would you like to configure SAN connectivity?” field.

Create Service Profile Template

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

☐ Simple ☐ Expert ☒ No vHBAs ☐ Use Connectivity Policy

This server associated with this service profile will not be connected to a storage area network.

< Prev Next > **Finish** Cancel

b. Click Next.

10. Configure Zoning Options:

a. Set no Zoning options and click Next.

11. Configure vNIC/HBA Placement:

a. In the “Select Placement” list, leave the placement policy as “Let System Perform Placement”.

b. Click Next.

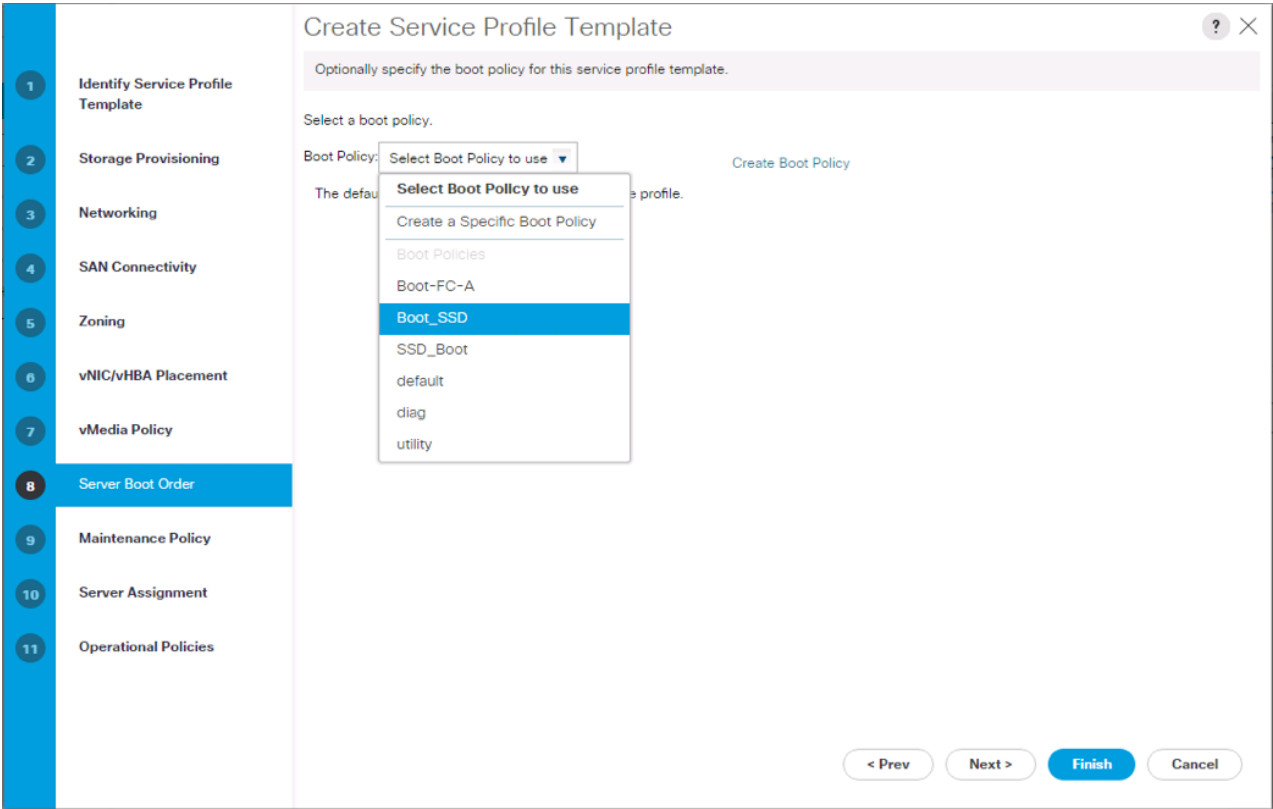
12. Configure vMedia Policy:

a. Leave the vMedia Policy unselected.

b. Click Next.

13. Configure Server Boot Order:

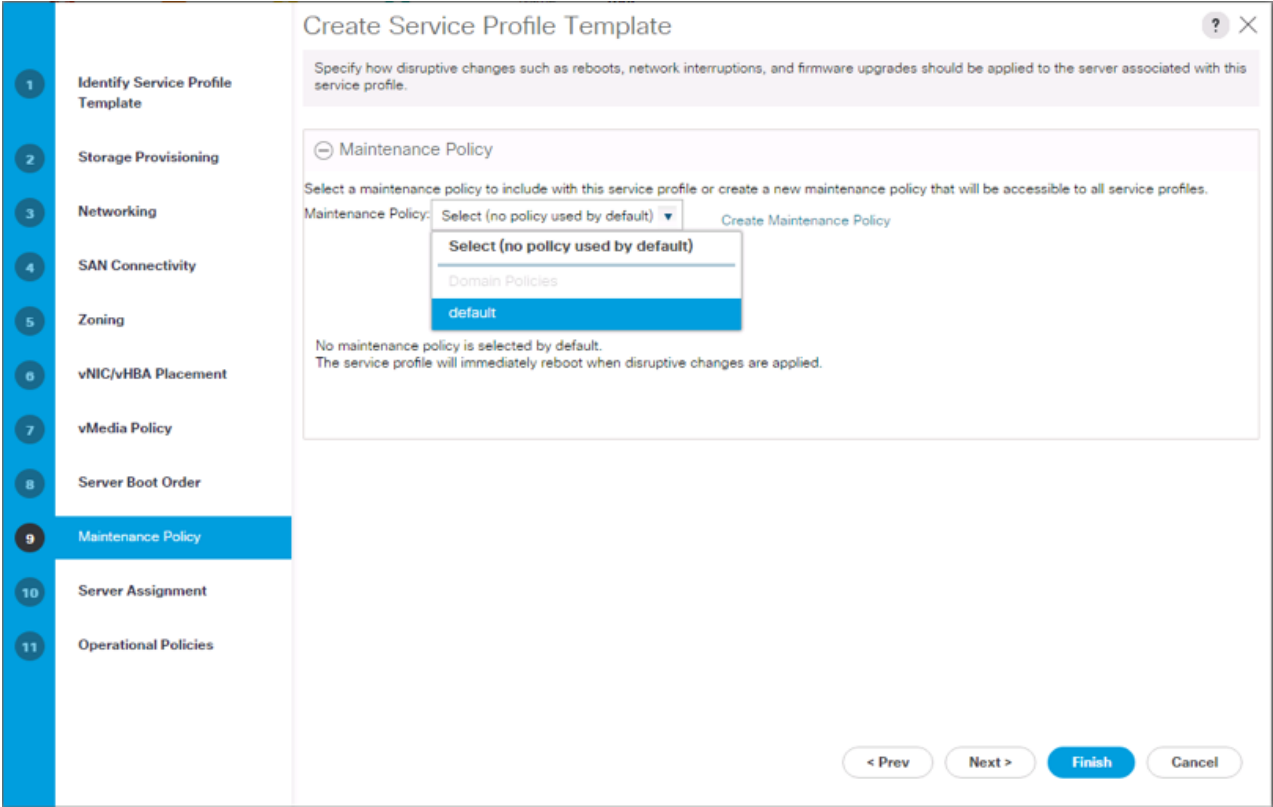
a. Select Boot_SSD for Boot Policy.



b. Click Next to continue to the next section.

14. Configure Maintenance Policy:

a. Change the Maintenance Policy to default.



b. Click Next.

15. Configure Server Assignment:

a. In the Pool Assignment list, select C240-CommServe.

Create Service Profile Template

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment: **Assign Later** [Create Server Pool](#)

Assign Later

Select from a Pool

- 3260
- Branch_C240_ESXi
- C240-CommServe**
- CommServe
- Infra_Pool
- S3260-MediaAgent
- Test_Harness_Pool
- default

The service profile manually later.

Firmware

Select the power state to be applied when this profile is associated with the server.

☒ Up ☐ Down

associated with a server. Either select a server from the list or associate the service profile

Controller, Adapter)

< Prev Next > **Finish** Cancel

- b. Firmware Management at the bottom of the page can be left alone as it will use default from the Host Firmware list.
- c. Click Next.

16. Configure Operational Policies:

- a. In the BIOS Policy list, select VM-Host-Infra.
- b. Expand Power Control Policy Configuration and select **No-Power-Cap** in the Power Control Policy list.

Create Service Profile Template

Optionally specify information that affects how the system operates.

BIOS Configuration

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile

BIOS Policy : VM-Host-Infra

External IPMI Management Configuration

Management IP Address

Monitoring Configuration (Thresholds)

Power Control Policy Configuration

Power control policy determines power allocation for a server in a given power group.

Power Control Policy : default [Create Power Control Policy](#)

Scrub Policy

KVM Management

Operational Policies

< Prev Next > **Finish** Cancel

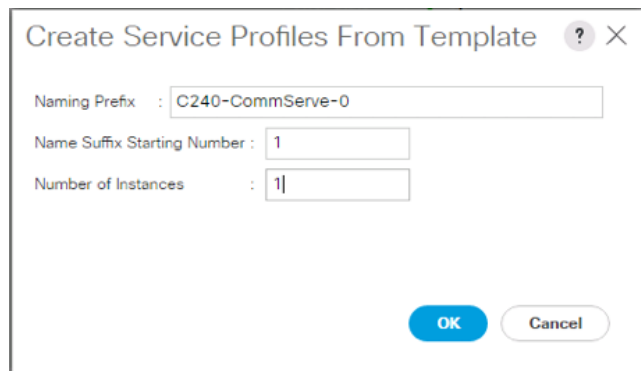
17. Click Finish to create the service profile template.

18. Click OK in the confirmation message.

Create Service Profiles

To create a service profile from the service profile template, complete the following steps:

1. Connect to the UCS 6332-16UP Fabric Interconnect UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Template S3260-MediaAgent.
3. Right-click S3260-MediaAgent and select Create Service Profiles from Template.
4. Enter C240-CommServe-0 as the service profile prefix.
5. Leave 1 as “Name Suffix Starting Number.”
6. Set 1 as the “Number of Instances.”
7. Click OK to create the service profiles.



Create Service Profiles From Template ? X

Naming Prefix : C240-CommServe-0

Name Suffix Starting Number : 1

Number of Instances : 1

OK Cancel

8. Click OK in the confirmation message to provision the CommServe Service Profile.



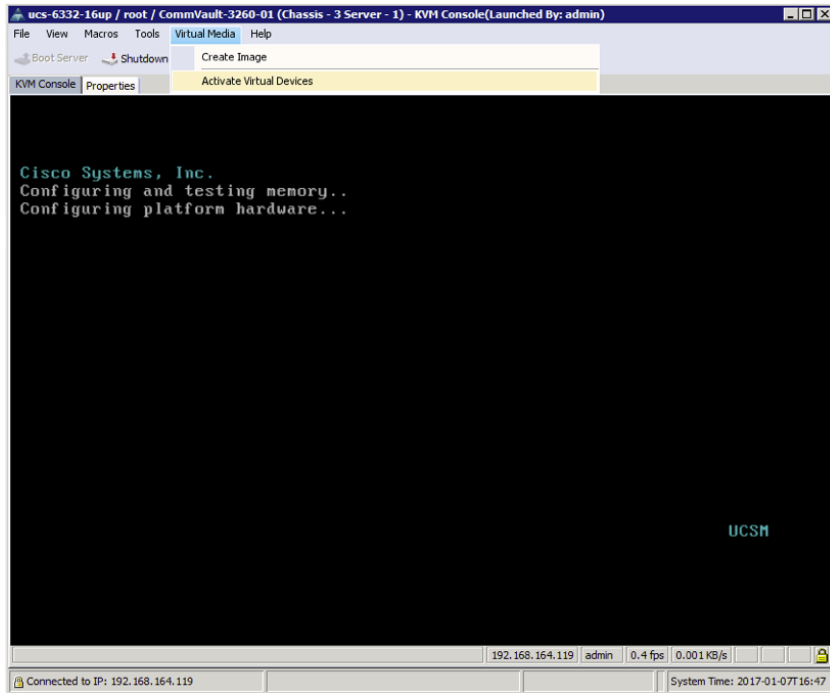
A Cisco UCS C240 was also used in the test environment of the simulated secondary data center. The steps involved for its creation are not covered in this CVD, but involved using the IB-Secondary appropriate vNIC Template used for the secondary data center Media Agent, and an expansion of the Storage Profile used to include an additional Local LUN created for a local datastore.

OS Installation for MediaAgent and CommServe

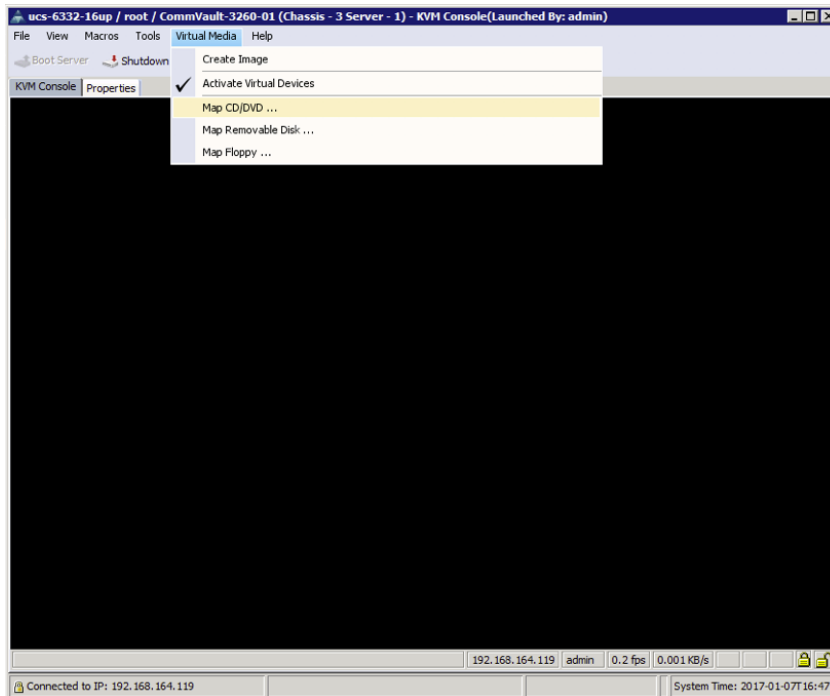
The installation steps for the S3260 MediaAgent and the C240 CommServe are similar; both install Microsoft Windows Server 2012 R2, and use a Cisco UCS Manager KVM installation process from locally accessed vMedia mapping.

To install the OS for MediaAgent and CommServe, complete the following steps:

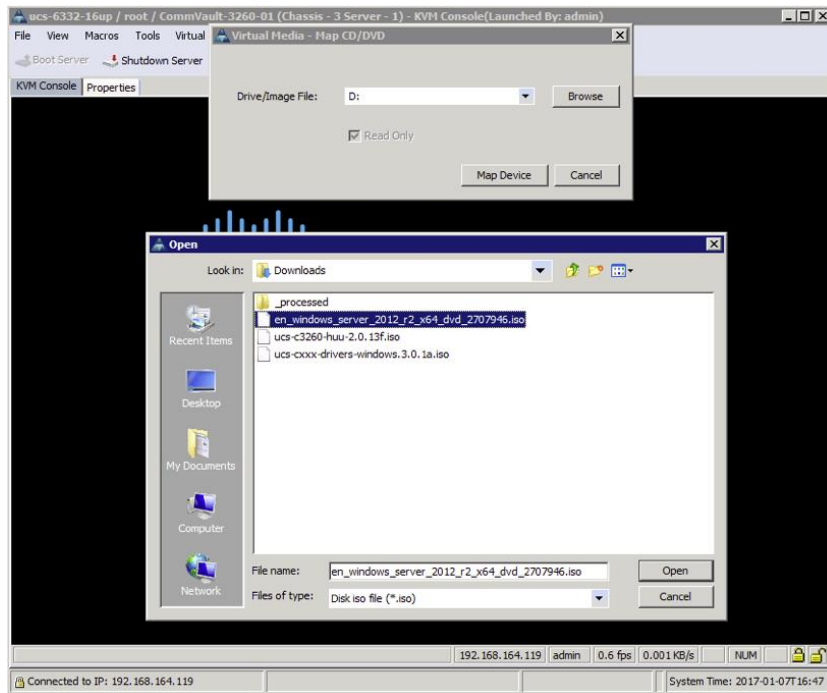
1. To begin the installation, a Cisco UCS Manager KVM Console needs to be opened from the General tab of the associated Service Profile of the first server to install.
2. With the KVM Console open, click Virtual Media and select Activate Virtual Devices from the dropdown.



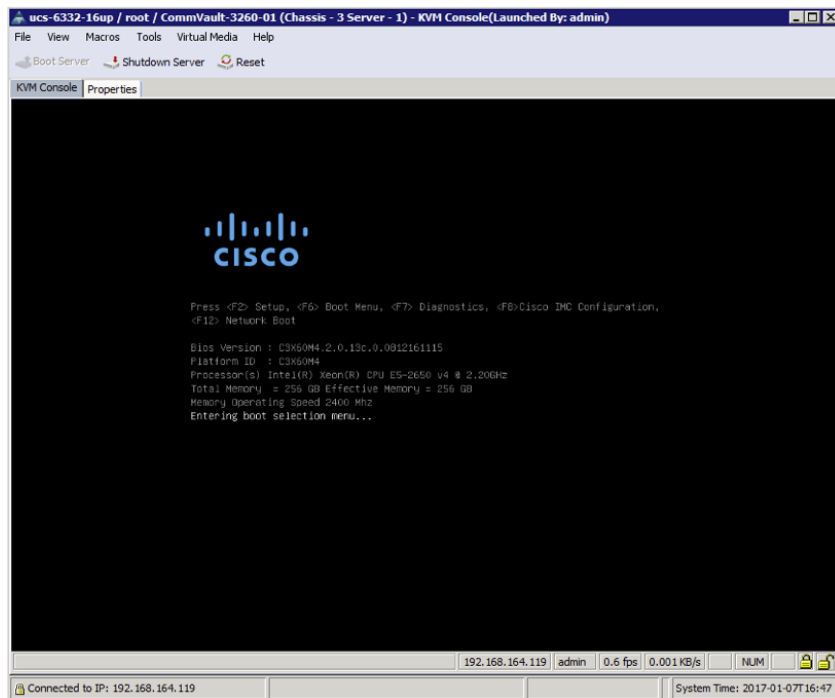
3. Click Virtual Media again, and select **Map CD/DVD ...** from the drop-down.



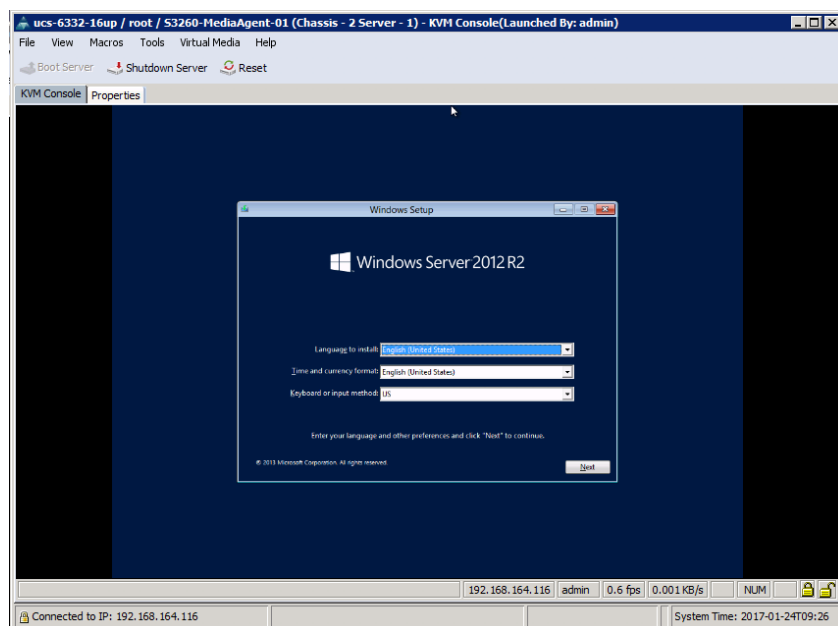
4. Click Browse within the Virtual Media pop-up window, and find the location of the OS installation ISO within the resulting pop-up window. Select the file and click Open.



- Click Reset if the system has progressed past the boot selection menu prior to mapping of the Windows ISO through KVM vMedia.



- Boot order will initiate the OS installation automatically, click Next on the OS installation start screen.

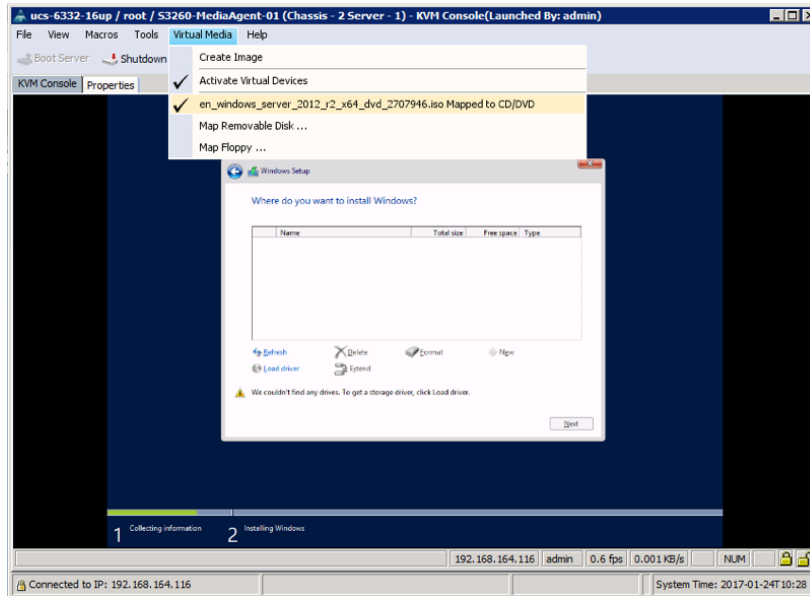


7. Proceed with the start of the installation entering a valid Windows license key and selecting the mode (GUI mode will be used in our example.)
8. Accept the License and select Custom: Install Windows only (advanced).
9. When the installation destination screen appears, for the S3260, no suitable drives are available. The Windows Driver ISO should be download from software.cisco.com at <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286281356&flowid=71443&softwareid=283853158>

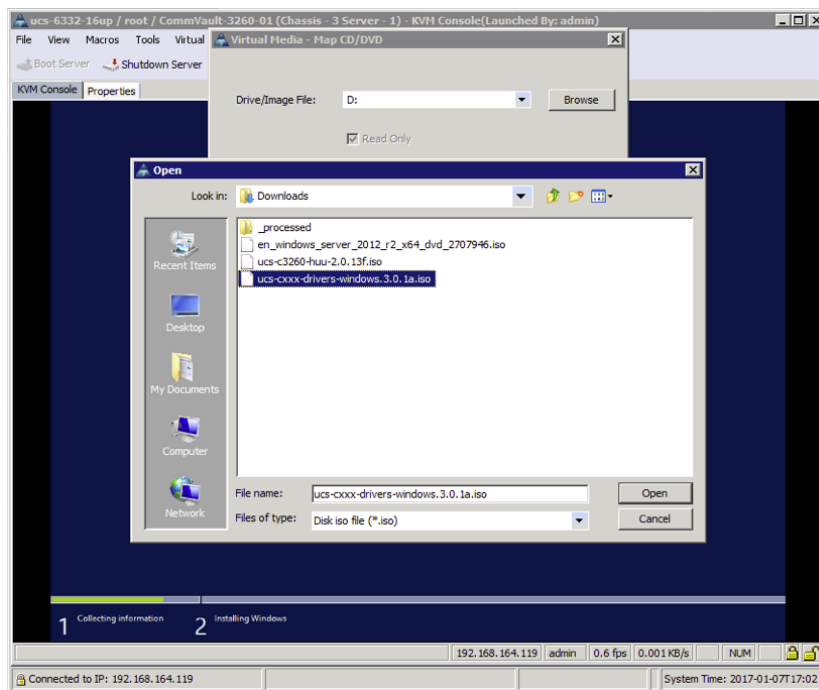


The Load Driver steps can be skipped for the C240 Windows OS Setup.

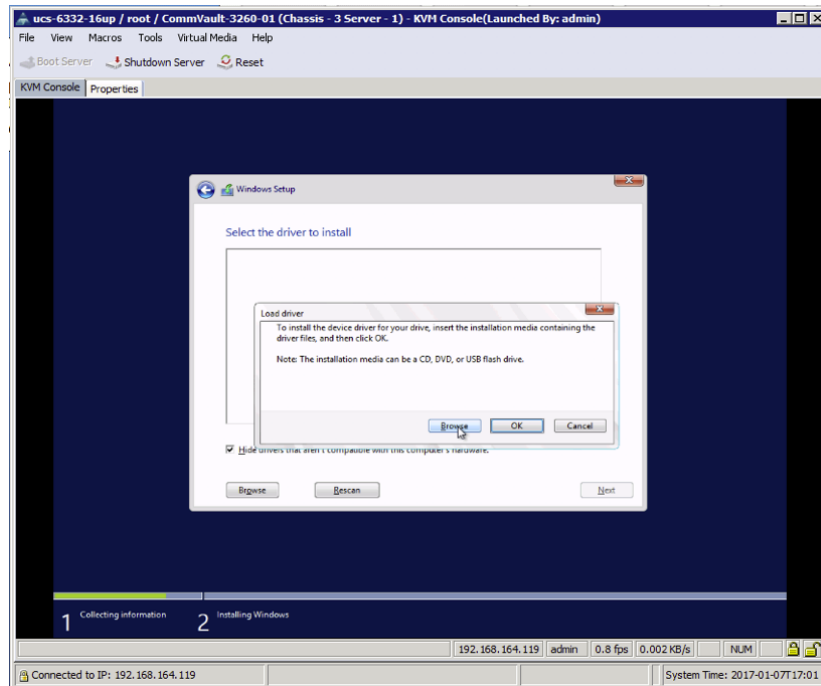
10. Un-map the Windows OS installation ISO as vMedia.



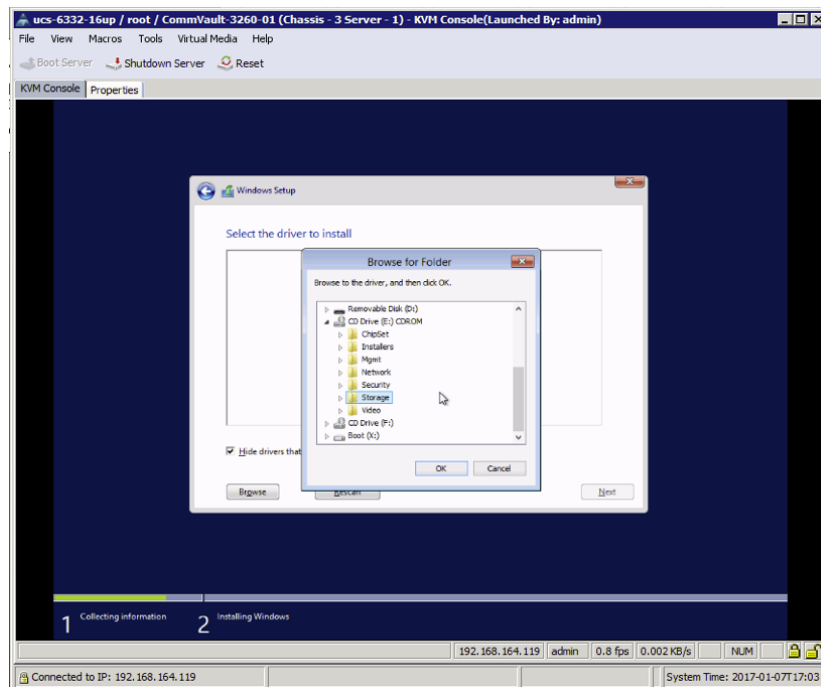
11. Click Yes to confirm the un-map drive request.
12. Re-select the Virtual Media drop-down, selecting **Map CD/DVD ...** , and find the downloaded Cisco UCS Driver ISO using the Browse option.



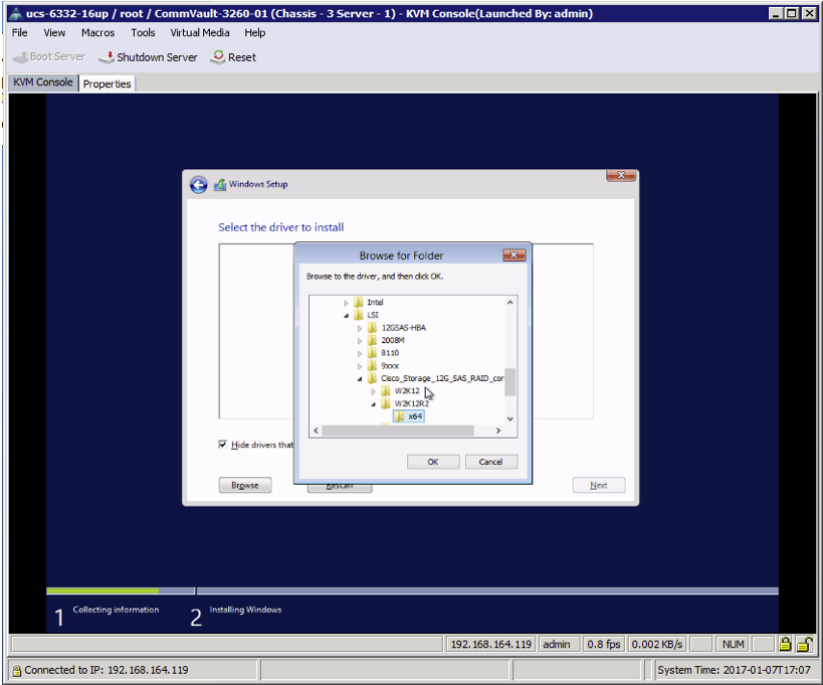
13. Click Open, and then choose Map Device.
14. Click Load Driver and select Browse within the pop-up window that appears.



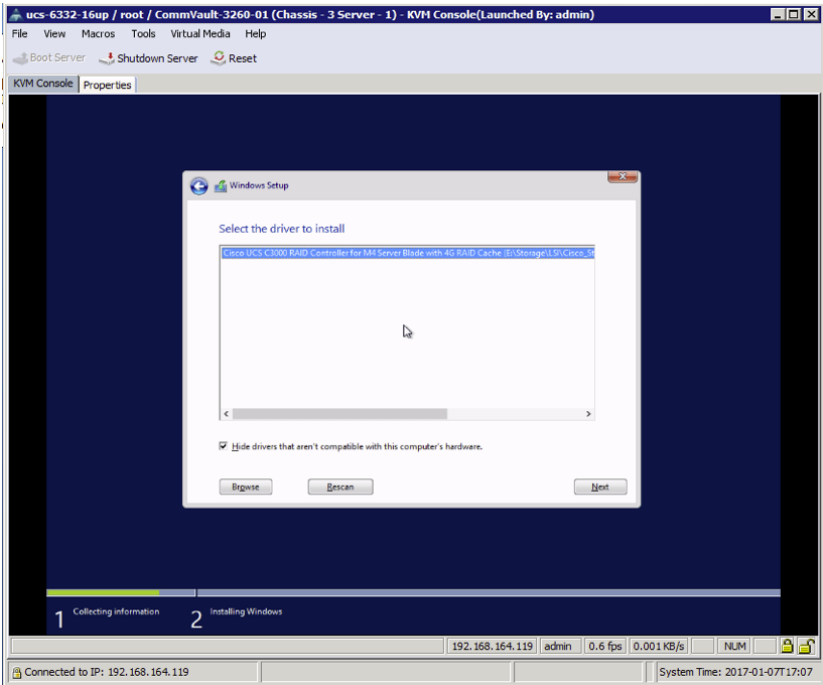
15. Select the Storage directory within the mapped CDROM drive.



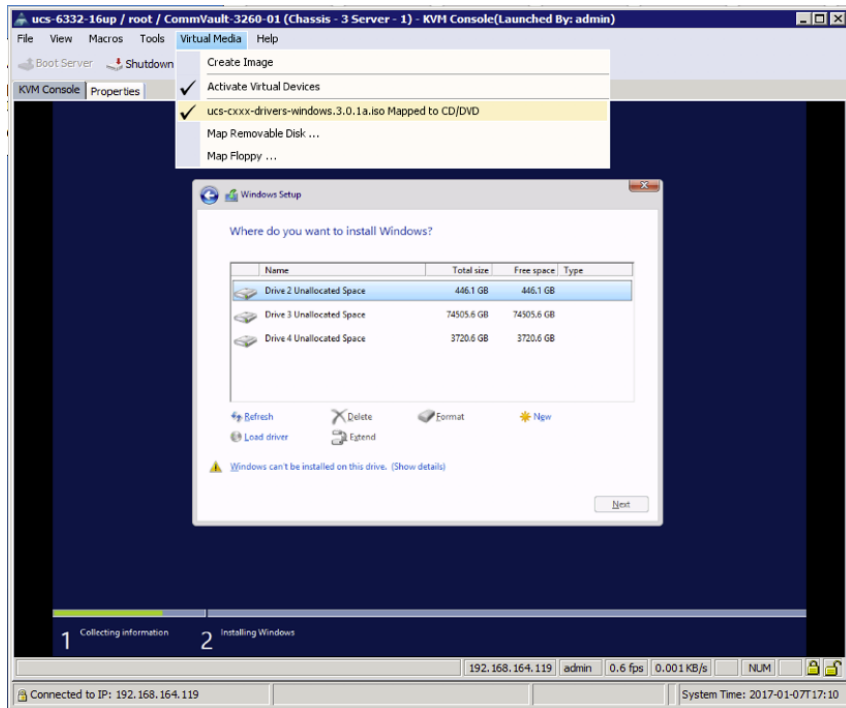
16. Drill further down within the Storage directory to -> LSI -> Cisco_Storage_12G_SAS_RAID_controller -> W2K12R2 -> x64 and click OK.



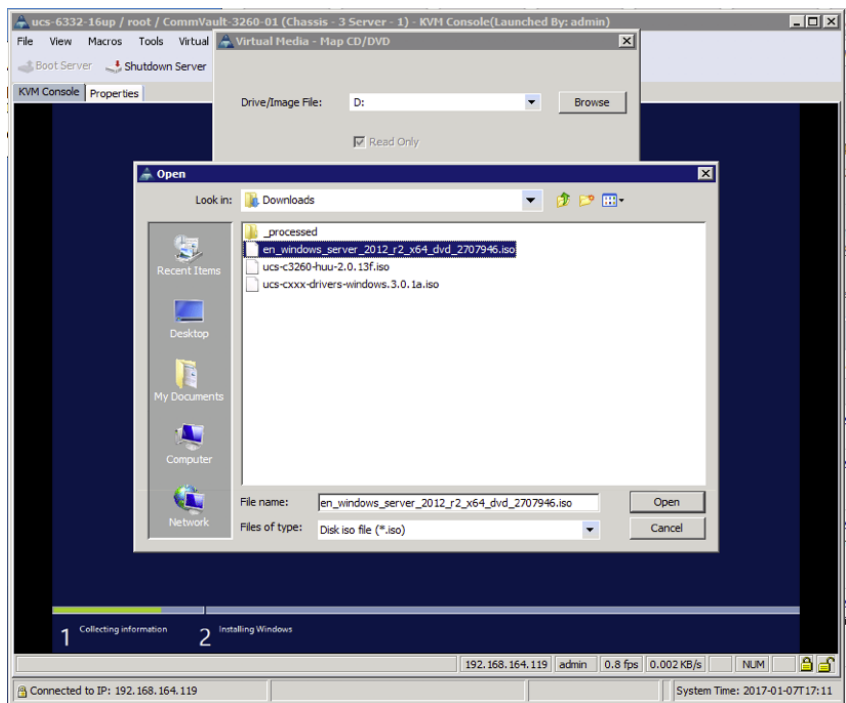
17. Select the driver that is found and click Next.



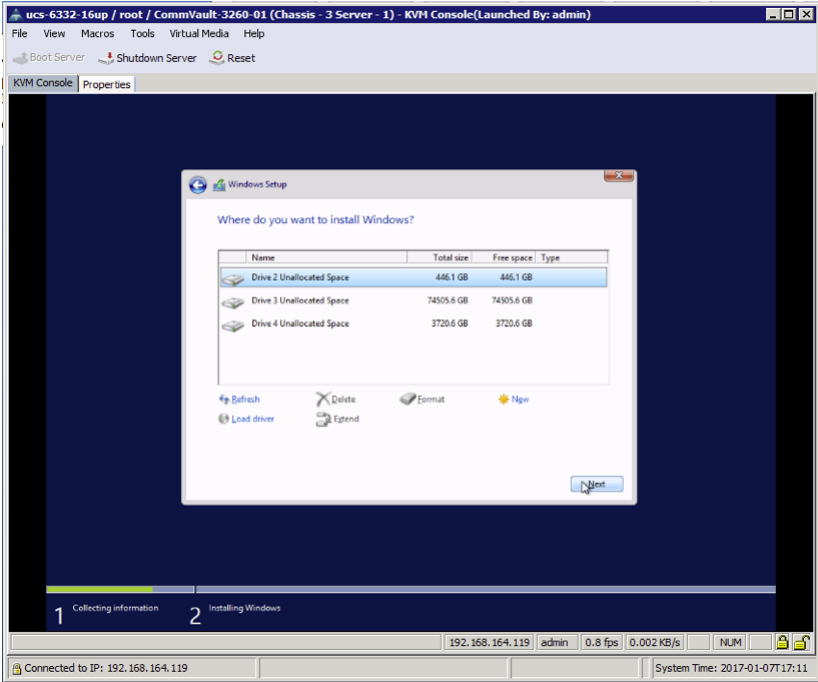
18. Select the drive to install the Windows OS to, and re-select the Virtual Media drop-down to un-map the Cisco Windows Drivers ISO.



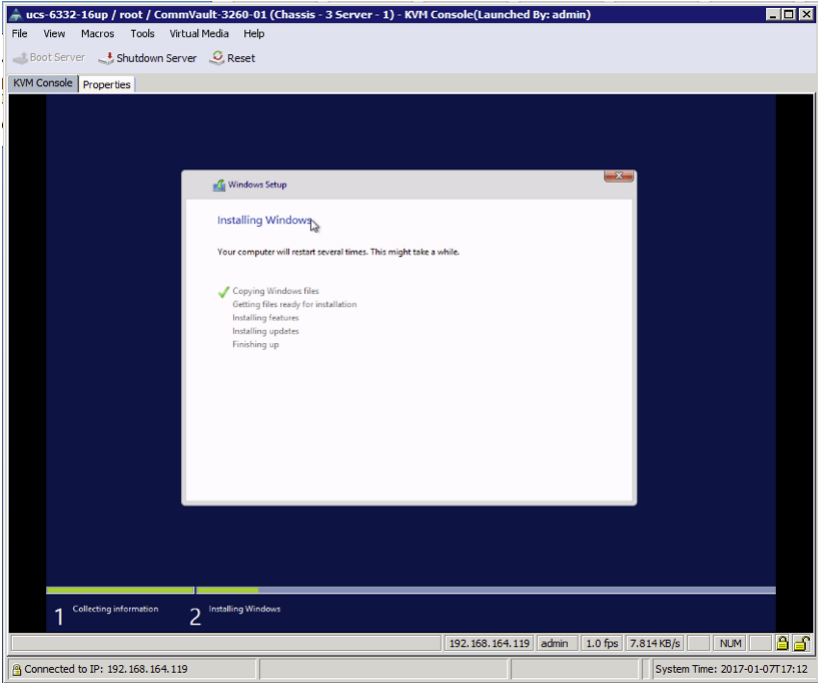
19. Click Yes to confirm the un-mapping of the ISO, and re-select the Virtual Media drop-down to re-map the Windows OS installation ISO.



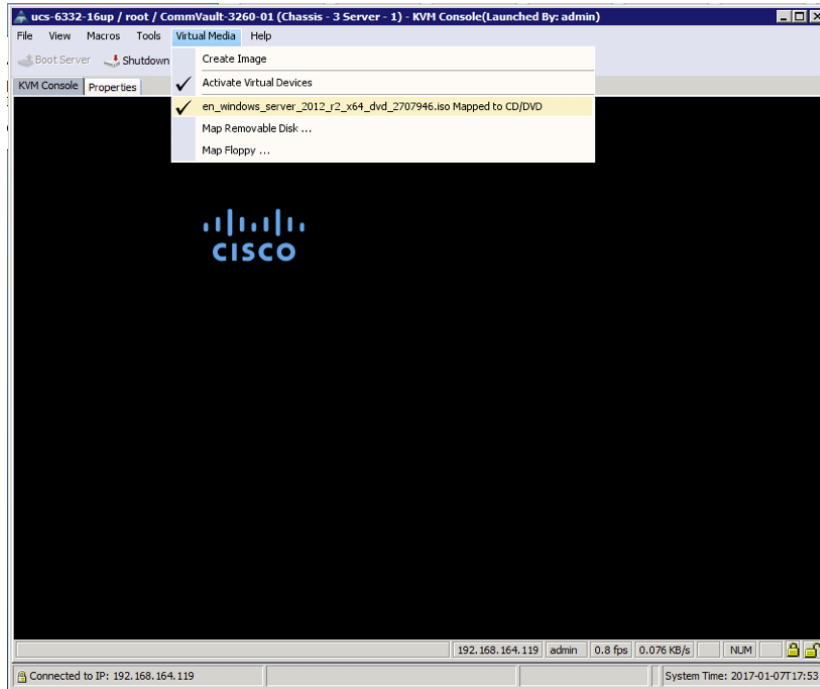
20. Click Next to begin the installation.



21. Wait for the Windows Setup to complete.

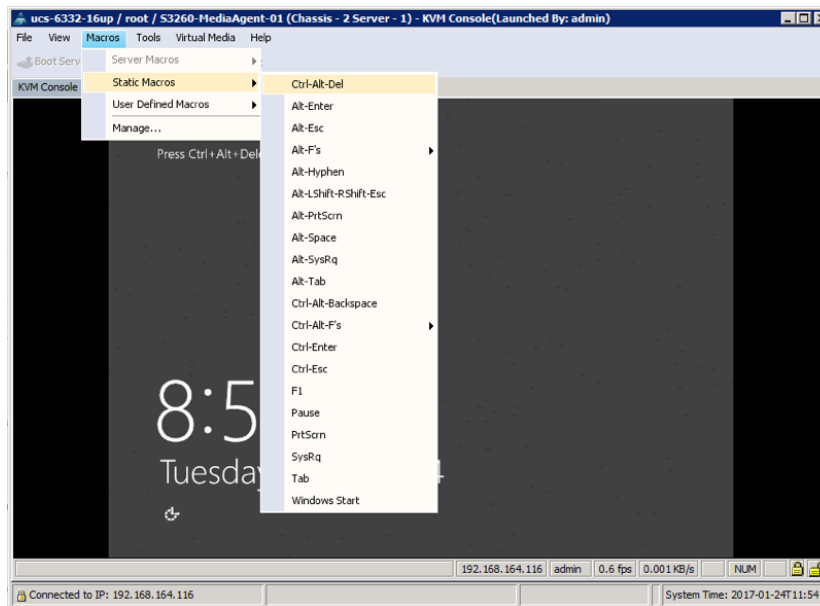


22. Un-map the Windows OS installation ISO after completion.

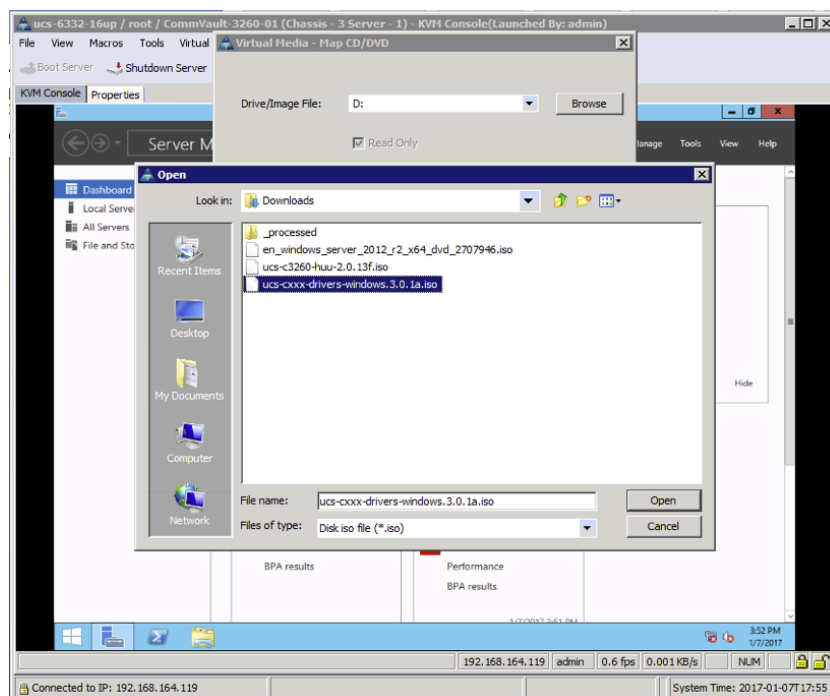


23. Provide an Administrator password and click Finish.

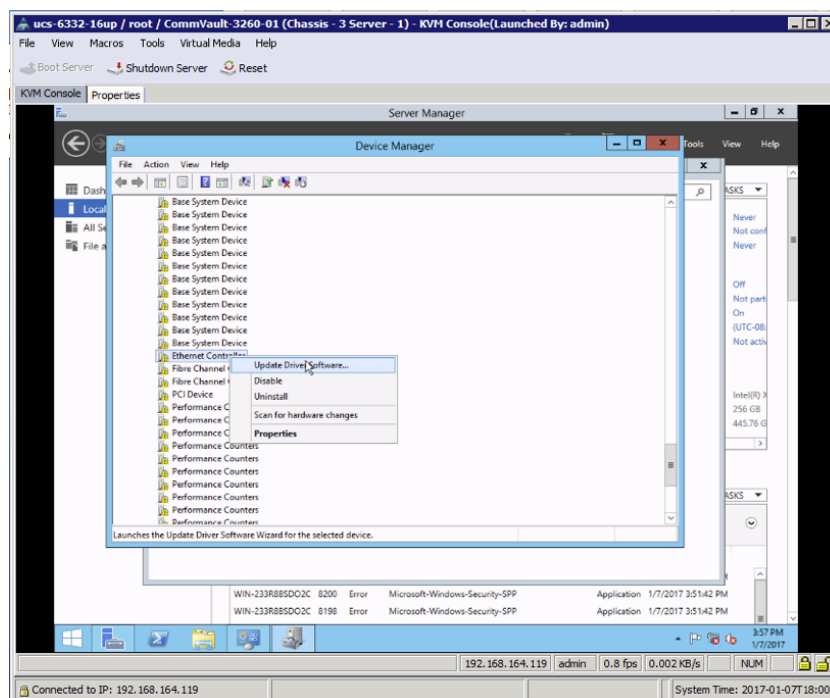
24. Use the Static Macro for Ctrl-Alt-Del to login to the system.



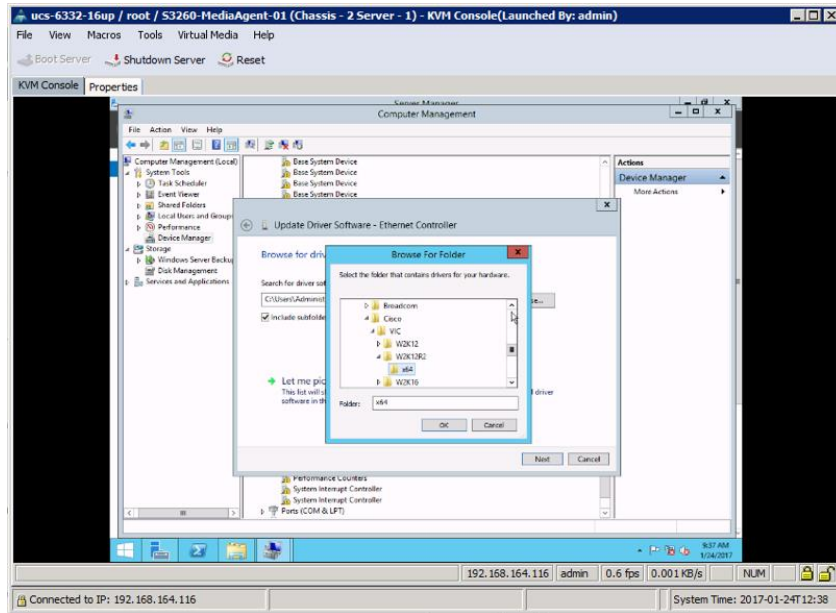
25. Re-select the Virtual Media drop-down and go through the steps to re-map the Cisco UCS Windows Drivers ISO.



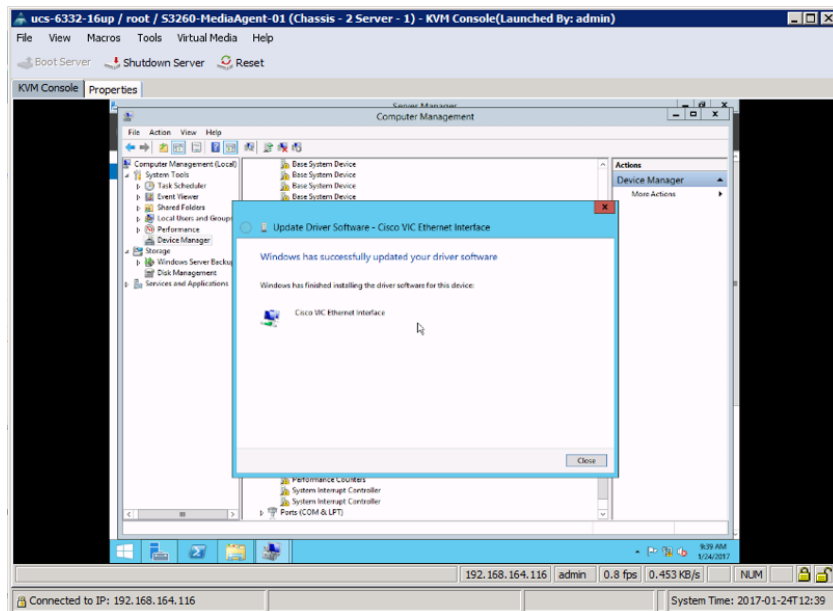
26. Open the Device Manager and find the unidentified Ethernet Controller Device within Other Devices, and right-click to select **Update Driver Software ...**.



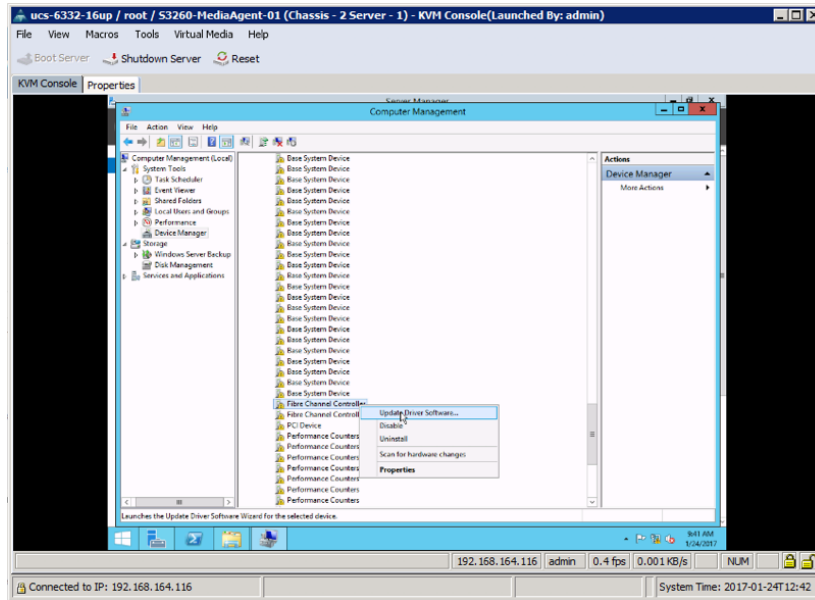
27. Select Browse my computer for driver software within the resulting pop-up window.
28. Click Browse in the Update Driver Software - Ethernet Controller window, and navigate from the mapped CD Drive -> Network -> Cisco -> VIC -> W2K12R2 -> x64 and click OK.



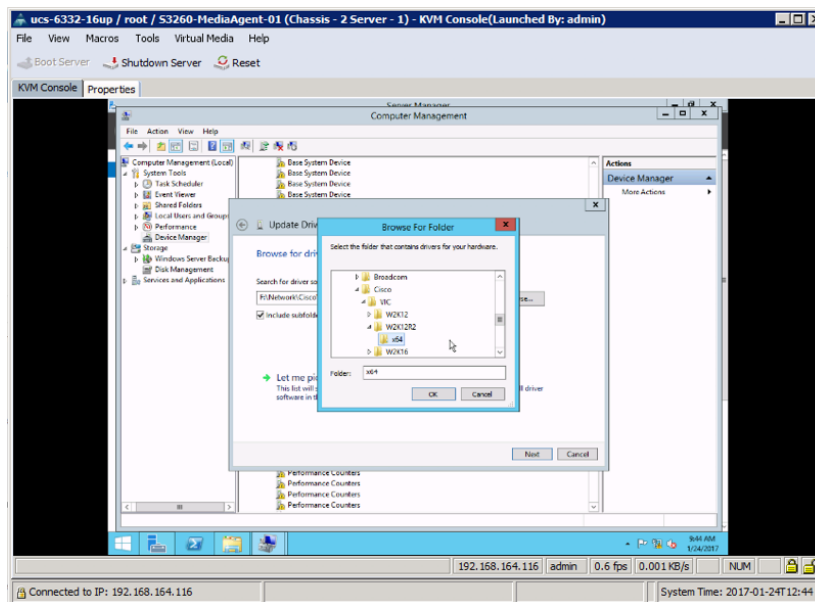
29. Click Next to update the driver.



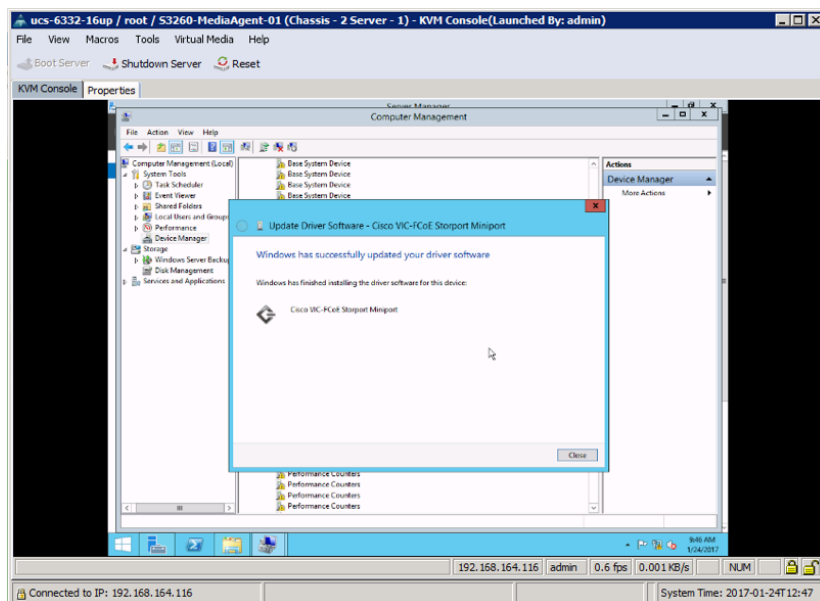
30. Click Close, and with the Device Manager still open, scroll down within Other Devices and find an entry for the first Fibre Channel Controller, right-click and select **Update Driver Software ...**



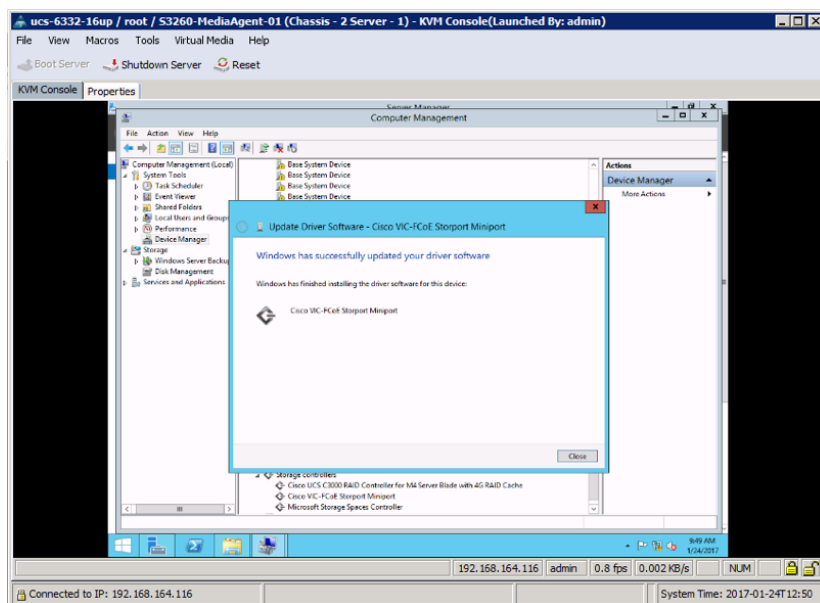
31. Repeating the similar process followed for the Ethernet Controller, select Browse my computer for driver software.
32. Select Browse, and drill down from the mapped CD Drive -> Storage -> Cisco -> VIC -> W2K12R2 -> x64 and click OK.



33. Click Next to update the driver.
34. Click Close.

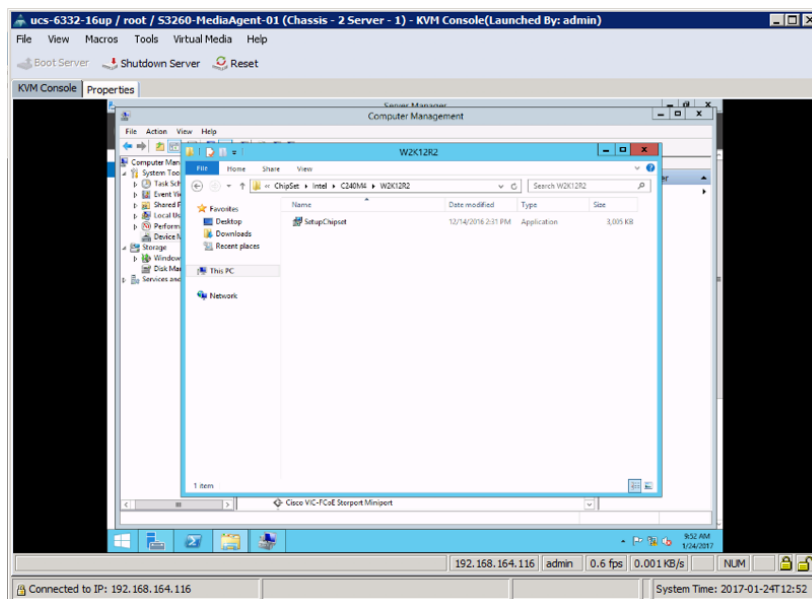


35. Repeat these steps for the second Fibre Channel Controller.

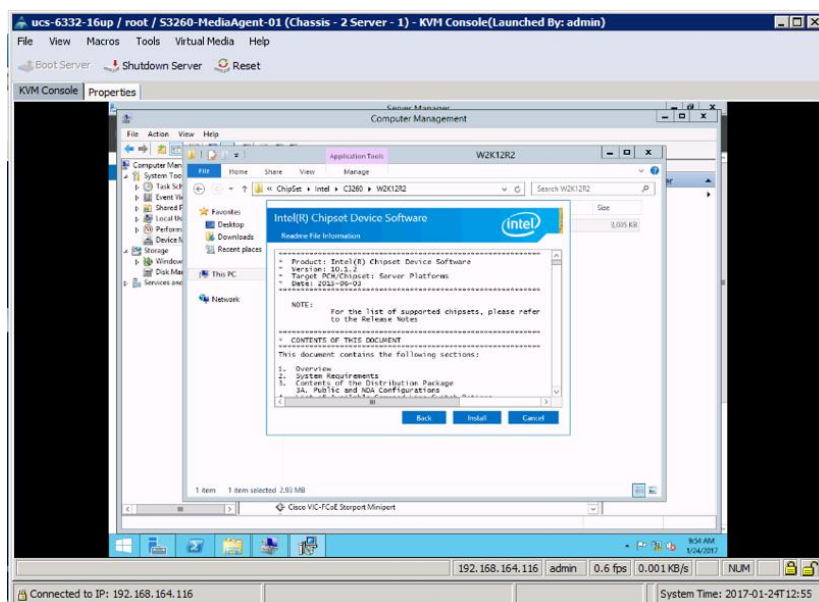


36. Click Close.

37. Open up a Windows File Explorer, and drill down from the mapped CD Drive -> Chipset -> Intel -> [C240M4 or C3260] -> W2K12R2, and open the SetupChipset application.



38. Click Next at the Welcome window, click accept to get past the EULA, and click Install.



39. Click Restart Later when finished.

40. Configure the network interface with an IP and enable Remote Desktop.

41. Complete OS updates and join it to an appropriate domain.

42. Disconnect the Virtual Media as the system reboots.

S3260 MDS Zoning and Host Group addition on the FlashArray//M

The S3260 MediaAgent will access the FlashArray//M snapshots, and will need zoning within the MDS as well as membership in the Host Group on the FlashArray//M that has access to the datastores being backed up.



The CommServe does not need fibre channel access, so you will not need to follow the steps in this section for the C240.

To setup the S3260 MediaAgent, complete the following steps:

1. Access the Service Profile the S3260 MediaAgent is associate to and select Storage -> vHBAs within the Service Profile.

The screenshot shows the UCS Manager interface for Service Profile S3260-MediaAgent-01. The 'vHBAs' tab is active, showing a table of vHBA configurations. The WWPNs for vHBA Fabric-A and vHBA Fabric-B are highlighted with red boxes.

Name	WWPN	Desired Order	Actual Order	Fabric ID	Desired Placement	Actual Placement	Admin Host Port	Actual Host Port
vHBA Fabric-A	20:00:00:25:B5:01:0A:00	1	2	A	Any	1	ANY	NONE
vHBA Fabric-B	20:00:00:25:B5:01:0B:00	2	3	B	Any	1	ANY	NONE

2. The WWPNs will be used for the SAN zoning, and later for the Host Groups on the FlashArray//M. Connect to the MDS Switches.

3. Device Alias Creation:

- a. Create device alias database entries for each of the WWPN/PWWNs mapping them to their human readable Source names:

```
mds-9148s-a(config-if)# device-alias database
```

```
mds-9148s-a(config-device-alias-db)# device-alias name S3260-MediaAgent-1A pwwn
20:00:00:25:b5:01:0a:0d
```

```
mds-9148s-a(config-device-alias-db)# exit
```

```
mds-9148s-a(config)# device-alias commit
```

- b. Repeat these steps on MDS 9148S B:

```

mds-9148s-b(config-if)# device-alias database

mds-9148s-b(config-device-alias-db)# device-alias name S3260-MediaAgent-1B pwnn
20:00:00:25:b5:01:0b:0d

mds-9148s-b(config-device-alias-db)# exit

mds-9148s-b(config)# device-alias commit

```

MDS VSAN Zones

To create the MDS VSAN zones, complete the following steps:

1. Create zones on each MDS for the S3260 using the device aliases created in the previous step, associating them with device aliases for the FlashArray//M created during the initial FlashStack VSI deployment:

```

mds-9148s-a(config)# zone name S3260-MediaAgent-1A vsan 101

mds-9148s-a(config-zone)# member device-alias S3260-MediaAgent-1A

mds-9148s-a(config-zone)# member device-alias FlashArray-CT0FC0-fabricA

mds-9148s-a(config-zone)# member device-alias FlashArray-CT0FC2-fabricA

mds-9148s-a(config-zone)# member device-alias FlashArray-CT1FC0-fabricA

mds-9148s-a(config-zone)# member device-alias FlashArray-CT1FC2-fabricA

```

2. Create a similar zone on MDS 9148S B:

```

mds-9148s-b(config)# zone name S3260-MediaAgent-1B vsan 102

mds-9148s-b(config-zone)# member device-alias S3260-MediaAgent-1B

mds-9148s-b(config-zone)# member device-alias FlashArray-CT0FC1-fabricB

mds-9148s-b(config-zone)# member device-alias FlashArray-CT0FC3-fabricB

mds-9148s-b(config-zone)# member device-alias FlashArray-CT1FC1-fabricB

mds-9148s-b(config-zone)# member device-alias FlashArray-CT1FC3-fabricB

```

3. Add the zones to a zoneset on each MDS switch:

- a. zoneset for MDS A

```

mds-9148s-a(config-zone)# zoneset name flashstack-zoneset vsan 101

mds-9148s-a(config-zoneset)# member S3260-MediaAgent-1A

```

- b. zoneset for MDS B

```

mds-9148s-b(config-zone)# zoneset name flashstack-zoneset vsan 102

mds-9148s-b(config-zoneset)# member S3260-MediaAgent-1B

```

4. Activate the zonesets and save the configuration:

- a. zoneset for MDS A


```
mds-9148s-a(config-zoneset)# zoneset activate name flashstack-zoneset vsan 101

mds-9148s-a(config)# copy run start
```

b. zoneset for MDS B

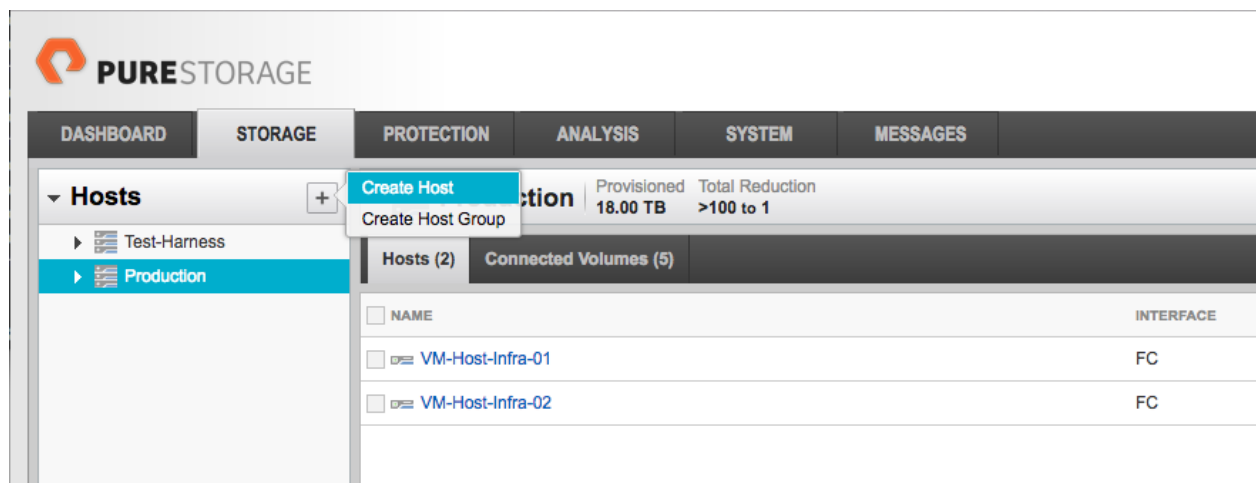
```
mds-9148s-b(config-zoneset)# zoneset activate name flashstack-zoneset vsan 102

mds-9148s-b(config)# copy run start
```

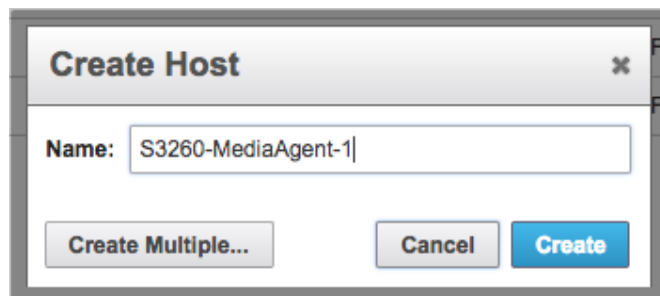
FlashArray//M Host Registration

For Host registration, complete the following steps:

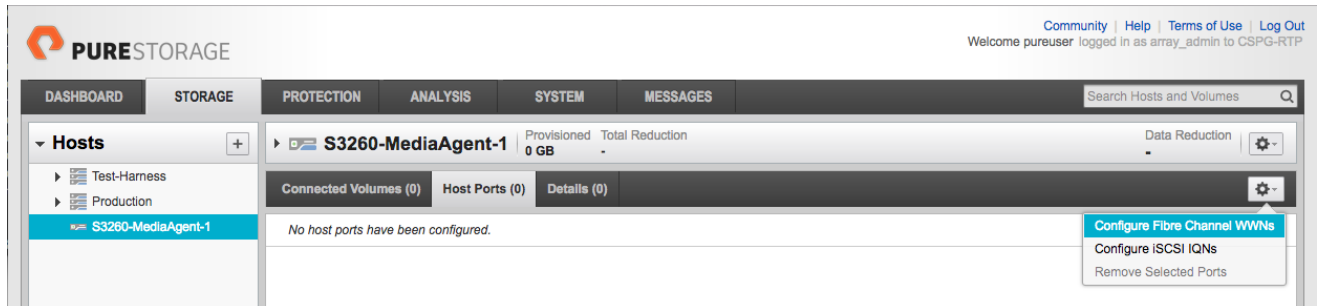
1. Create host entries from the Pure Storage Web Portal from the STORAGE tab, by selecting the + box next to Hosts appearing in the left side column.



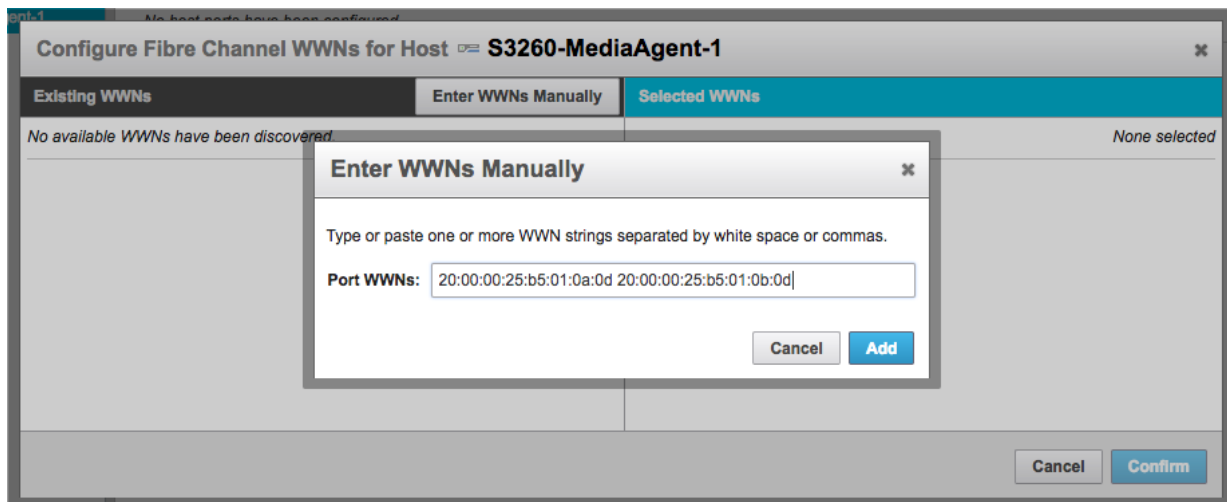
2. After clicking the Create Host option, a pop-up will appear to create an individual host entry on the FlashArray//M. Provide the name for the MediaAgent in that pop-up:



3. Click Create to add the host.
4. For the host created, select the host from within the STORAGE tab, and click the Host Ports tab within the individual host view. Select the Configure Fibre Channel WWNs menu option from the Host Ports tab menu drop-down:



5. A pop-up will appear for Configure Fibre Channel WWNs for Host <host being configured>. Within this pop-up, click the Enter WWNs Manually button and enter in the WWNs (WWPN) found at the beginning of this section through the MediaAgent's Service Profile:



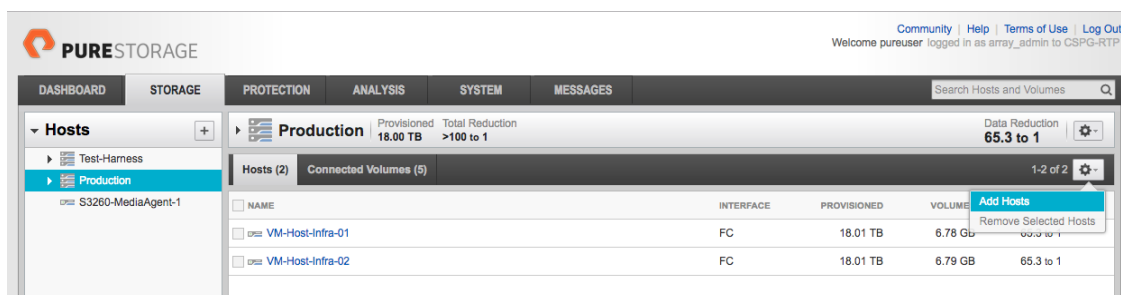
6. After adding the WWNs, click Confirm to add the Host Ports.

FlashArray//M Host Groups

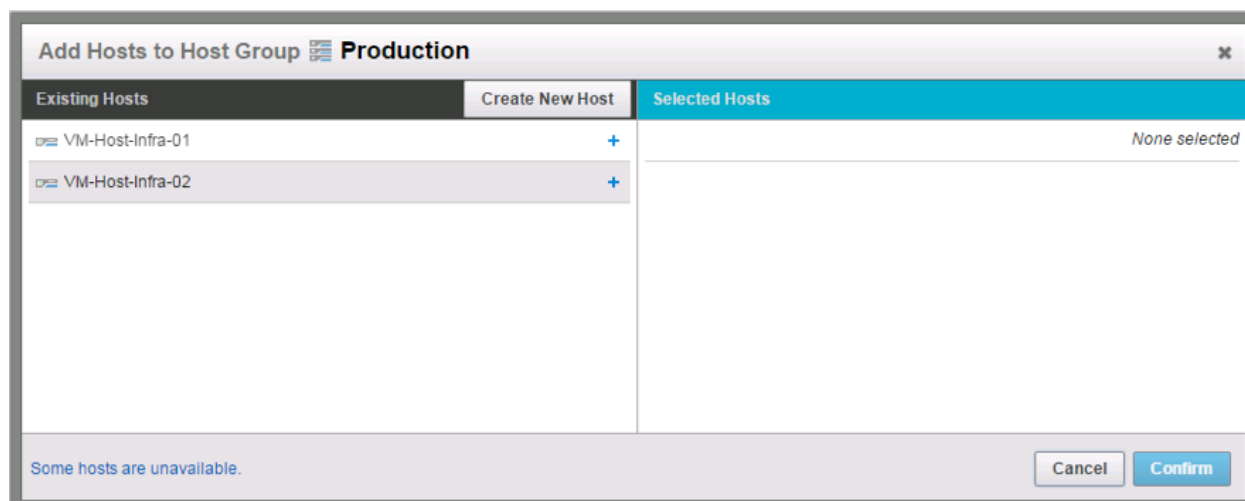
The S3260 MediaAgent will need access to the shared volumes used as VM datastores. To get this access it will need to be added to the Host Groups associated with the volumes used as datastores.

To add the S3260 to a Host Group in the Pure Storage Web Portal, complete the following steps:

1. Select the STORAGE tab select the appropriate Host group on the left and select the Add Hosts option within the menu drop-down within the Hosts tab of the Host Group created:



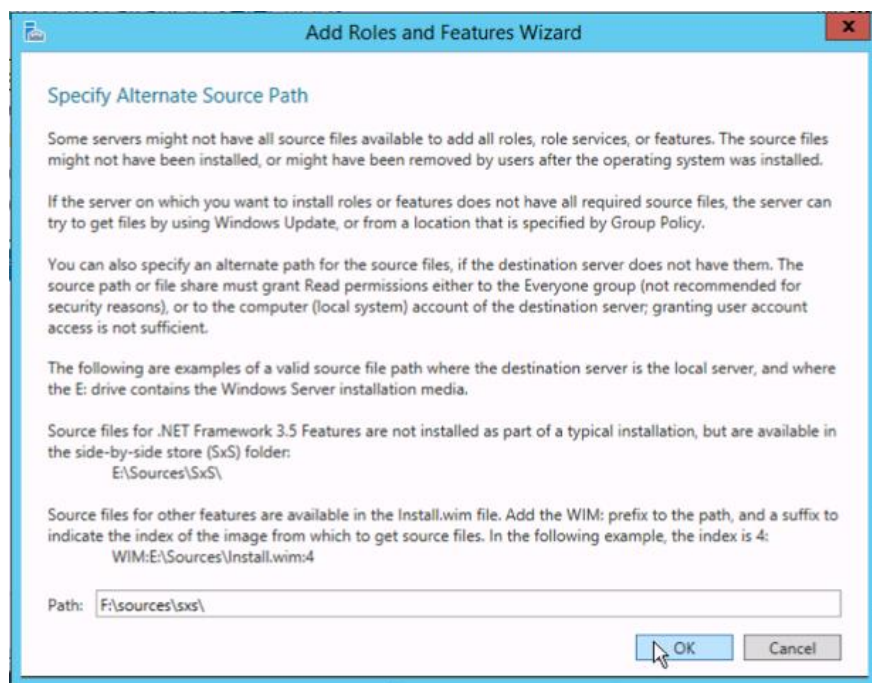
2. Select the + icon next to the S3260, and click Confirm to add to the Host Group:



OS Follow-up for the CommServe and the MediaAgent

To perform a follow-up for the CommServe and MediaAgent, complete the following steps:

1. Connect back to each system.
2. For the CommServe, add the IIS role and the .NET Framework 3.5 Features through Server Manager.
3. Map the OS installation ISO back to the CommServe via the KVM Virtual Media
4. During the .NET 3.5 install, select Specify Alternate Source Path, and use "F:\sources\sxs\" for the Path:



5. Un-map the install ISO from Virtual Media when complete.

6. For the MediaAgent, add the Multi-Path I/O feature through Server Manager.
7. Open a Command Prompt with administrator privileges. type diskpart command and hit Enter, type the automount disable command and hit Enter, type automount scrub command and hit Enter and close the Command Prompt.



Automatic drive-letter assignment to new volumes is disabled and cleared-out any entries previously mounted to volumes from the windows registry. Procedures were taken from KB:

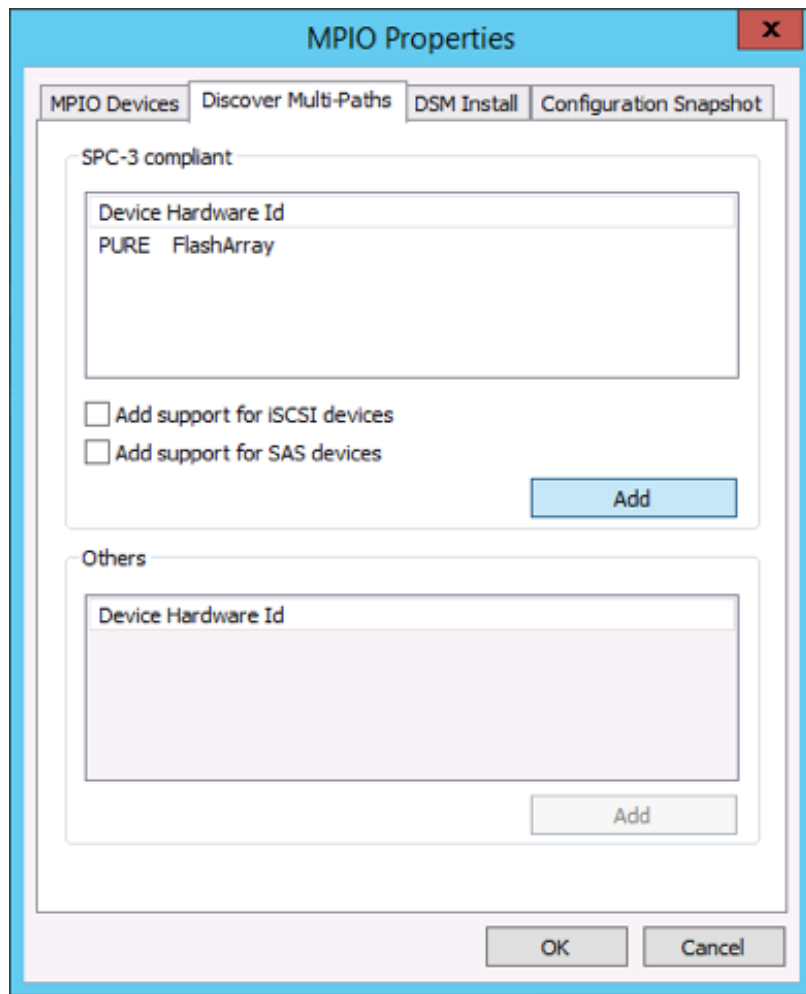
<https://kb.vmware.com/kb/2002227>



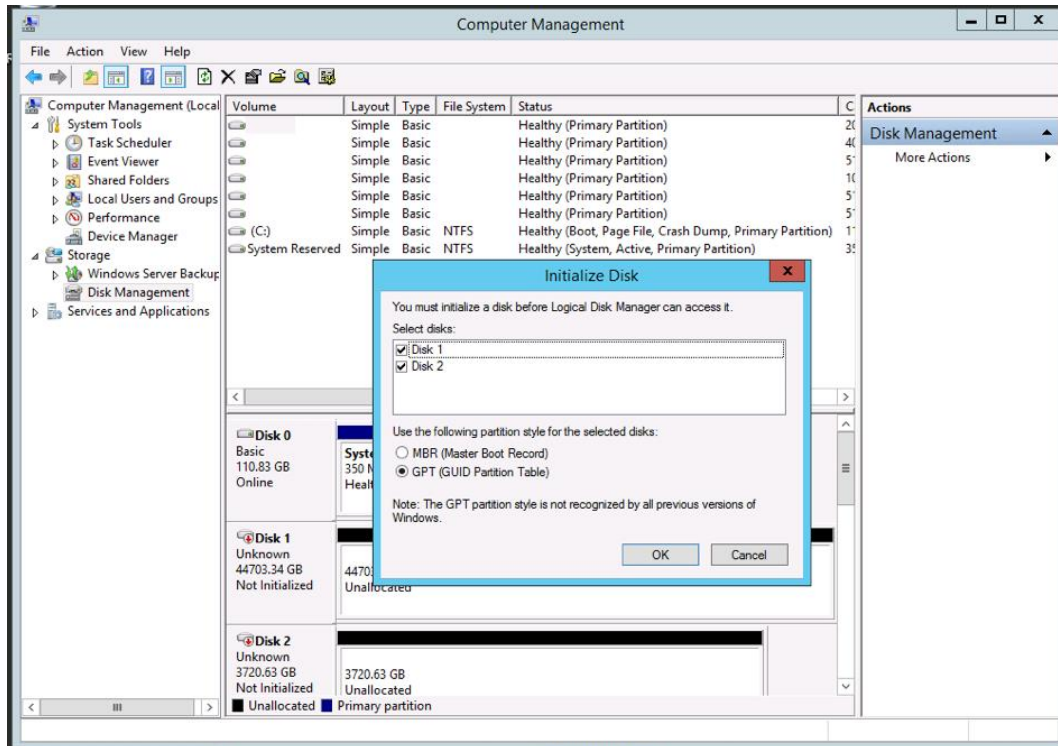
With the Multi-Path I/O feature installed, follow the steps in this support document from Pure Storage:

https://support.purestorage.com/?title=Solutions/Operating_Systems/Microsoft_Windows/Windows_Configuration:_Configuring_MPIO_%26_Adding_LUNs_to_Windows_Hosts

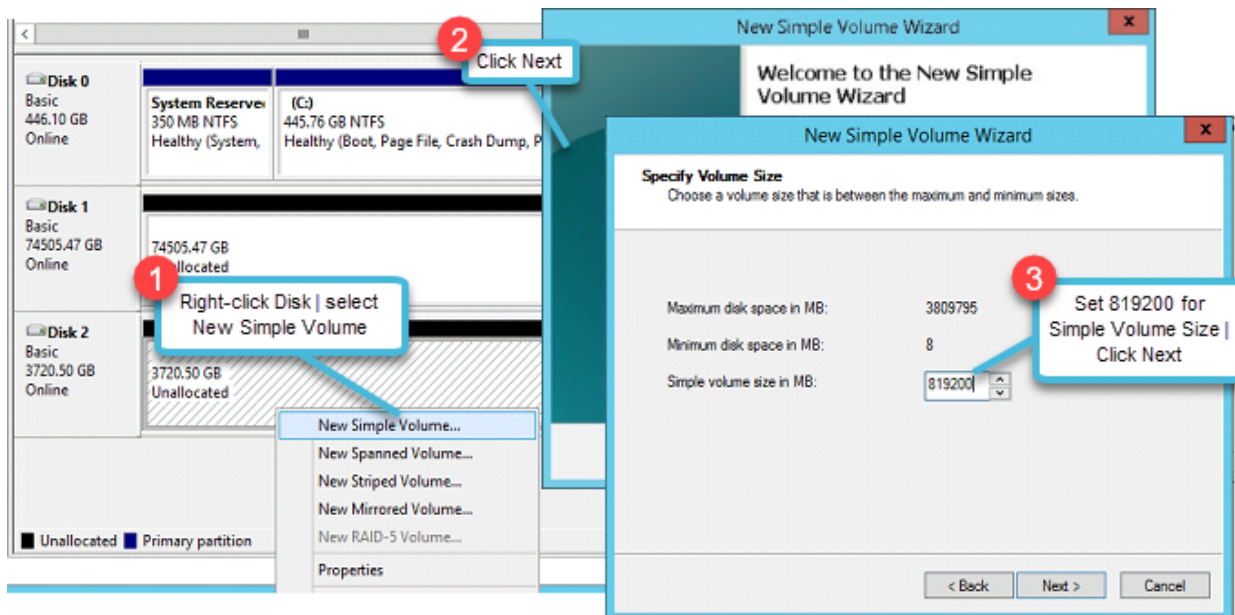
8. Run “mpiocpl” to configure MPIO Properties.
9. Select the Discover Multi-Paths tab and click Add for the identified PURE FlashArray.



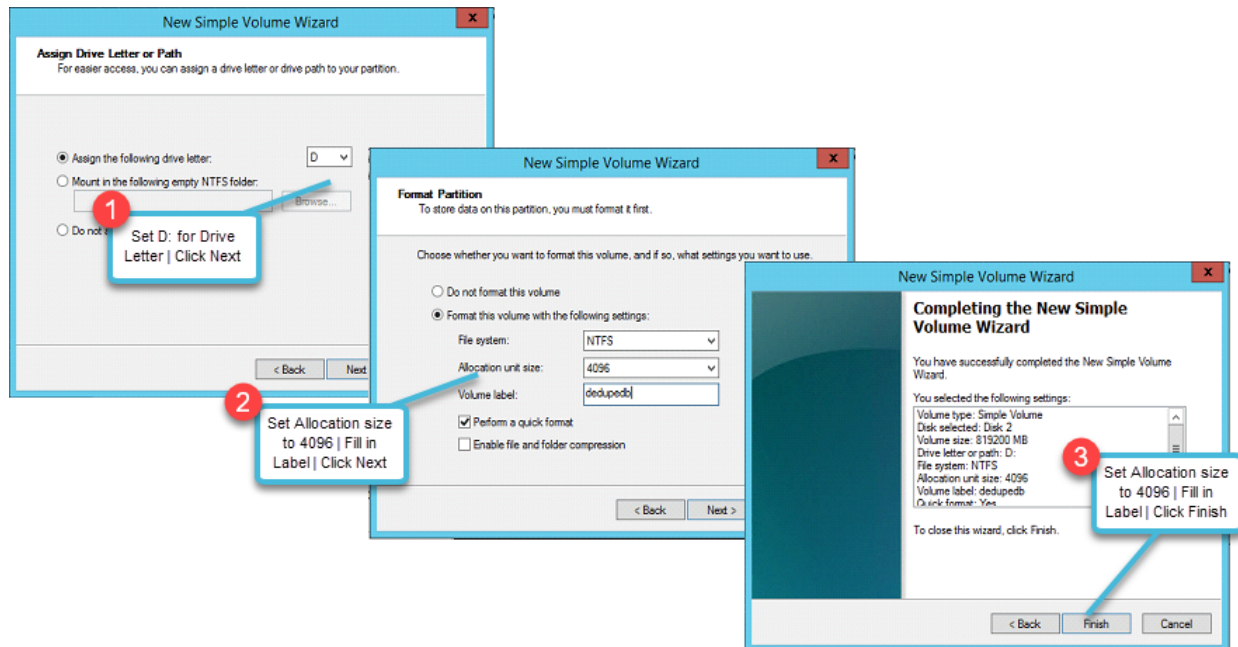
10. Reboot the system to apply changes.
11. From Server Manager, open up Tools -> Computer Management, and select Disk Management within Computer Management. The two local LUNs of the S3260 for the Disk Library and the SSD Cache have not been initialized yet, so click OK at the pop-up to initialize them.



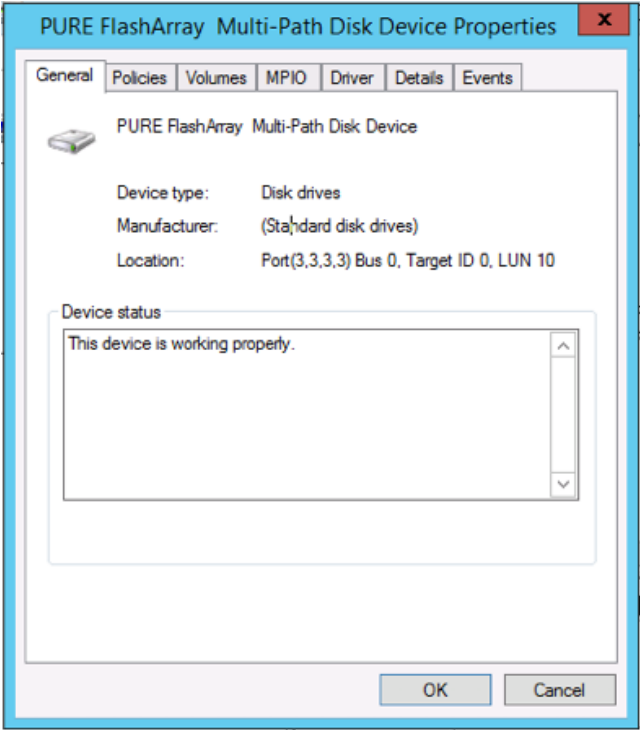
12. Configure the mount paths for the D: (dedupedb) and I: (indexcache) from SSD Cache disk (Disk 2)
13. Right-click the Disk 2 > select New Simple Volume > Click Next on Welcome to the New Simple Volume Wizard > click Next.
14. Set the Simple volume size in MB: to 819200 (800 GB) and click Next.
15. Once the volume has been created and assigned a drive letter D > click Next.



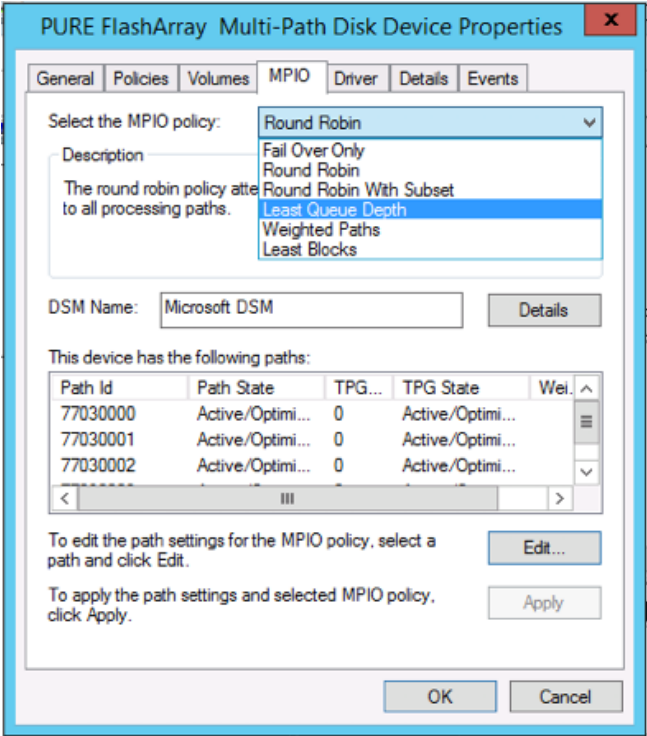
16. The next screen will have the format and file system options. Select Allocation unit size of 4096 and enter in a volume label dedupedb > click Next > click Finish.



17. Repeat steps a-b for unallocated space on Disk 2 > assigned a drive letter I: > click Next.
18. The next screen will have the format and file system options. Select Allocation unit size of 4096 and enter in a volume label index. Click **Next** > click Finish.
19. Configure the mount path L: Disk Library (Disk 1).
20. Right-click the Disk 1 > select New Simple Volume > Click Next on Welcome to the New Simple Volume Wizard > click Next > click Next on Specify Volume Size.
21. Once the volume has been created and assigned a drive letter L > click Next.
22. The next screen will have the format and file system options. Select Allocation unit size of 64k and enter in a volume label library_01. Click **Next** > click Finish.
23. Find the first Disk showing up that is a zoned resource from the FlashArray//M.
24. After the local LUNs to the S3260 are initialized, find the first Disk showing up that is a zoned resource from the FlashArray//M.



25. Click the MPIO tab and set the MPIO policy to Least Queue Depth, and click OK to set the policy change.



26. Repeat this step for each Disk in inventory from the FlashArray//M.

Commvault Deployment for FlashStack

This section describes how to create a Commvault environment consisting of a CommServe, MediaAgent and protected VMs. The VMs will be protected daily with hardware-based snapshots on the FlashArray//M and backups to the Cisco UCS S3260. VM lifecycle management policies will define user capabilities for creating VMs, as well as the rules for archiving idle VMs.

Commvault Data Platform Installation Process

To protect and manage data in your environment, the Commvault software must be distributed to the systems that you want to protect. The CommServe, MediaAgent and protected systems constitute a CommCell environment, while each protected system is referred to as a client. Virtualization management systems such as VMware vCenter and Microsoft Hyper-V clusters are also considered clients within a CommCell.

Use the Commvault installation package to set up a CommCell environment for protecting virtual machines. This package includes software for the Commvault CommServe, Admin Console, Virtual Server Agent, MediaAgent, CommCell Console, Web Server, Web Console, and Workflow Engine.

The CommCell environment installation will proceed in the following order:

1. CommServe software installation on Cisco UCS C240
2. MediaAgent software installation on Cisco UCS S3260
3. Storage Pool(s) configuration
4. Storage Array configuration
5. Policy configuration(s):
 - a. Storage Policies
 - b. Schedule Policies
6. Configure VM Protection for VMware

Before You Begin

Download the Commvault installation package from <http://cloud.commvault.com> and save it in a location accessible to the Cisco UCS C240 server.

CommServe Installation

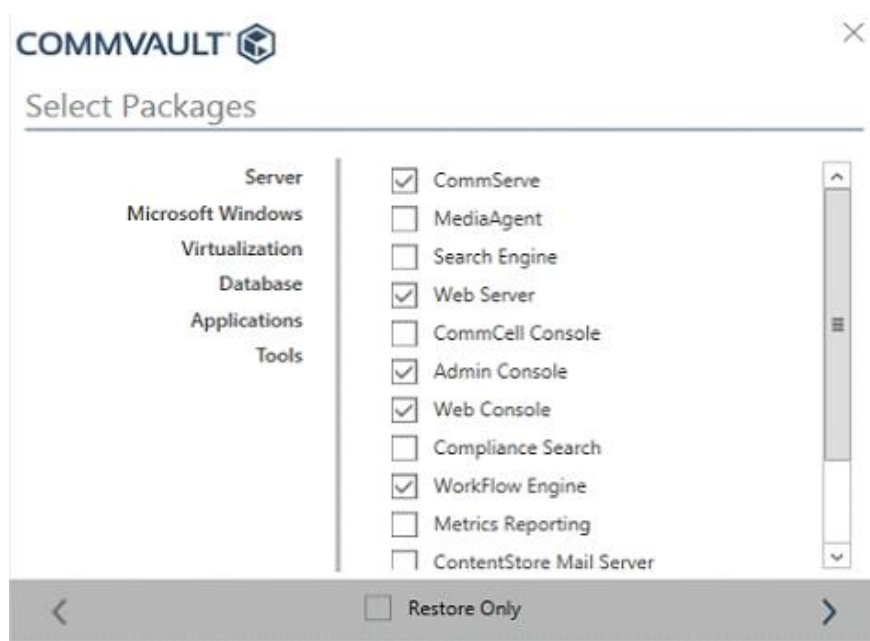
This procedure assumes the Cisco UCS C240 has an Internet connection. If an Internet connection is not available from the Cisco UCS C240, the complete installation source must be downloaded first. See the Appendix: Commvault Software Offline Installation for detail on how to download the complete installation source.

To install CommServe, complete the following steps:

1. Log on to the C240 with a user account with local administrator privileges.
2. In File Explorer, navigate to the downloaded installation package. Run setup.exe.

The Commvault Installer wizard opens.

3. On the welcome page, select the I Agree check box to accept the license agreement. Click the right arrow button to proceed to the next page.
4. On the Choose the Installation Type page, select Install packages on this computer and proceed to the next page.
5. On the Select Packages page, select the CommServe, and Admin Console checkboxes, and proceed to the next page.



The **Web Server**, **Web Console** and **Workflow Engine** packages are required for the CommServe and will be automatically selected.

6. On the Installation Path page, select the D:\ from the Drive list drop-down menu, and proceed to the next page.

COMMVAULT

Installation Path

Installation Path

C:\Program Files\Commvault\ContentStore

Drive List

C:\

C:\

D:\

Space Required / Available

3998 MB / 402457 MB

7. On the Database Engine Installation Path page, select the D:\ from the Drive list dropdown box, and proceed to the next page.
8. On the CommServe Database Installation Path page accept default selection, proceed to the next page.
9. On the Disaster Recovery Path page, select Use Local Path, enter D:\CSDR in the Disaster Recovery Backup Files Path and proceed to the next page.

COMMVAULT

Disaster Recovery Path

☐ Use Network Path

☒ Use Local Path

Disaster Recovery Backup Files Path

D:\CSDR

Drive List

D:\

Space Available

858275 MB



The best practice is to use a network path. The solution validation occurred in an isolated lab with no suitable network location.

10. Review the Installation Summary and proceed to next page.
11. On the Client Computer Information page verify Host Name shows the correct IP address or FQDN (fully qualified domain name) then proceed to next page.

12. On the Firewall Configuration page accept default selection, proceed to next page.



Disabling Windows firewall on the CommServe and MediaAgents is recommended.

13. On Database Installation Option, proceed to next page.
14. On the Database Install Option page, accept Create New Database and proceed to the next page.



To help you troubleshoot errors that occur before the installation summary page, check the %allusersprofile%\Commvault Systems\Galaxy\LogFiles\Install.log. If the error occurs after the summary page, check the installation logs in the *Software_Installation_Directory*\Log Files directory.

15. On the Commvault ID page, enter an email address to be used for alert notifications in the Email field. In the Password and Confirm Password fields, enter a password. This information will create a local user within the Commvault Data Platform with full access to the CommCell. The email address will be used for alert notifications. Proceed to the next page.



COMMVAULT 

Commvault ID

Email

Password

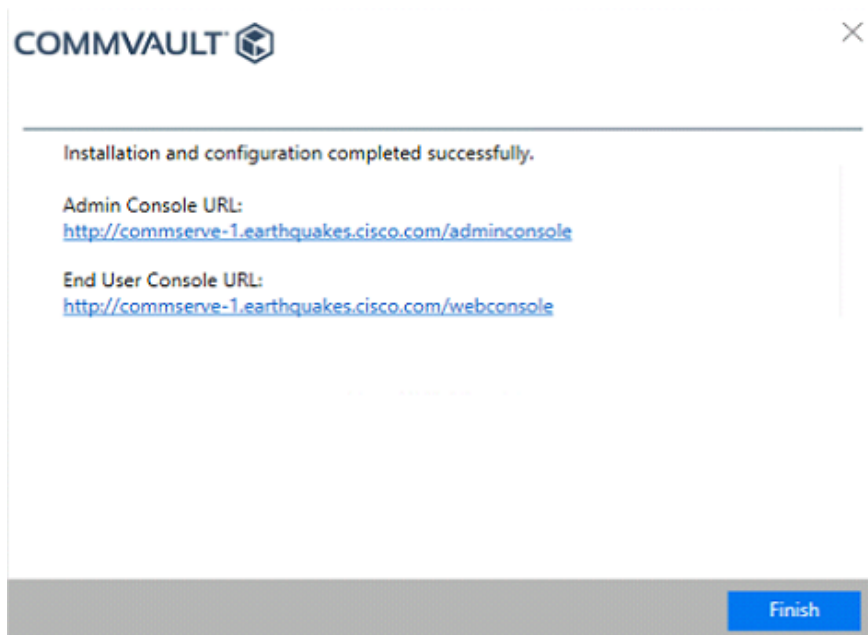
Confirm Password


< >

16. When the installation is complete, click Finish to exit the setup wizard.



Record the Admin Console URL and End User Console URL for later access.



COMMVAULT 

Installation and configuration completed successfully.

Admin Console URL:
<http://commserve-1.earthquakes.cisco.com/adminconsole>

End User Console URL:
<http://commserve-1.earthquakes.cisco.com/webconsole>

Finish

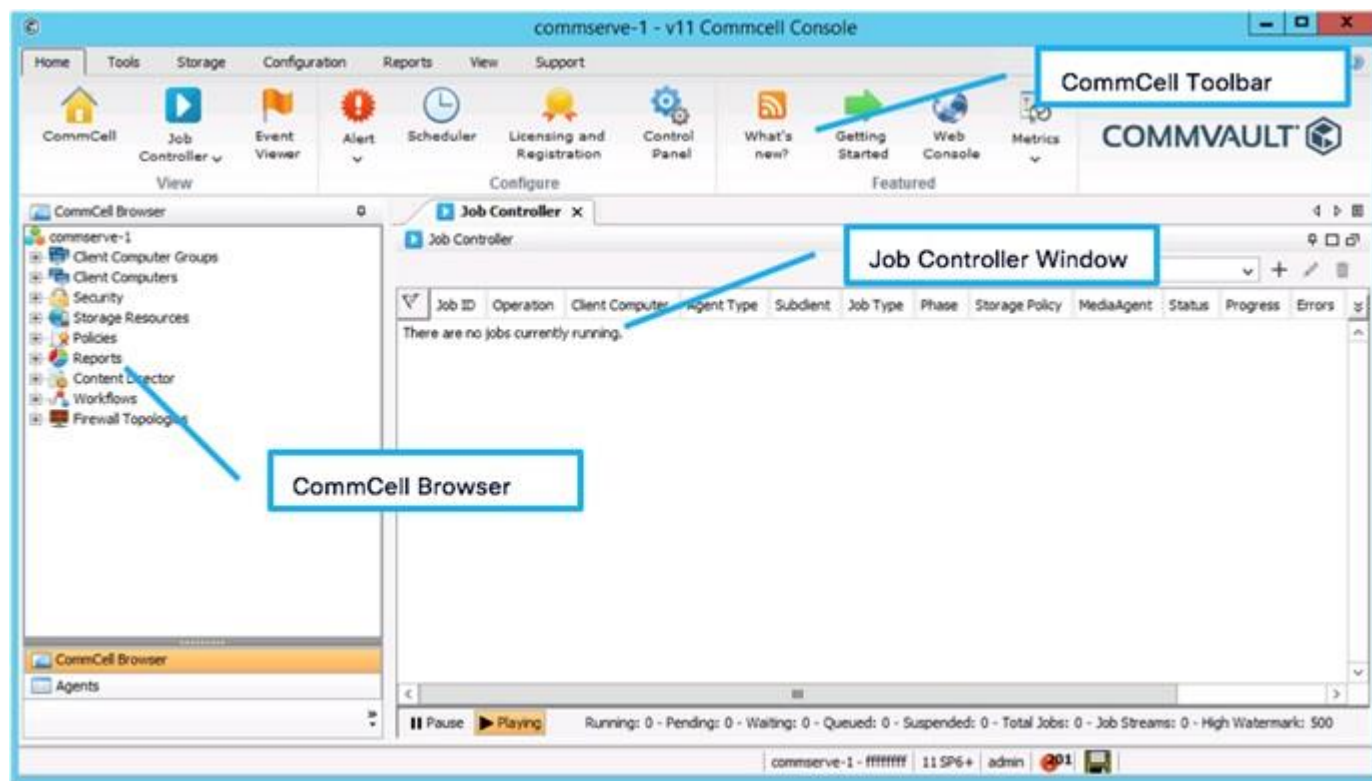
Post-installation Tasks

The post-installation tasks, advanced configurations, and features will use the CommCell Console. General administration and recovery tasks will be performed with the Admin Console. The CommCell Console can be accessed from a web browser at <http://<CommServe Hostname>/console>.

CommCell Console Overview

The CommCell Console is the graphical user interface used for advanced management of the CommCell environment, with more detail and options available than in the Admin Console. The CommCell Console is made up of the following elements:

- CommCell Toolbar: An easy to navigate "ribbon" used to access global configuration elements in the CommCell environment.
- CommCell Browser: The main navigation window which contains a hierarchical structure of all components within the CommCell environment.
- Job Controller Window: Management screen for all active and recent jobs in the CommCell environment.

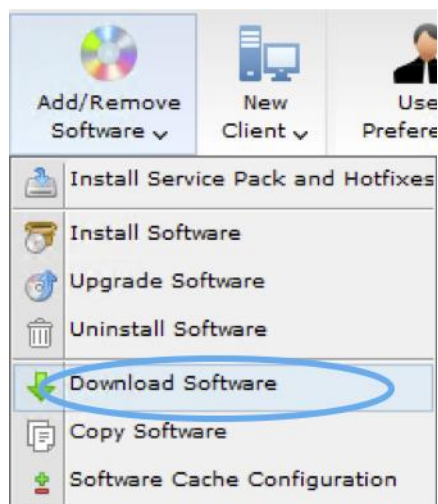


Setup CommServe Software Cache

The CommServe software cache stores the Commvault software media needed to perform remote installations and upgrades from the CommCell Console. By default, software is downloaded from the Internet to the CommServe software cache directory via FTP through the CommCell Console. If Internet connectivity is not available, the CommServe cache can be populated manually using the installation media.

To setup the CommServe Software Cache, complete the following steps:

1. From the CommCell Console ribbon, on the Tools tab, click Add/Remove Software, then select Download Software from the drop-down menu.



2. In the Download and Sync Cache Options dialog box, ensure the Latest Service Pack option is selected, then click OK. A Download Software job will initiate to obtain the packages. Wait for the job to complete before attempting any remote agent installations.



By default only packages for Microsoft Windows (including the Virtual Server Agent) are downloaded. Linux and Unix packages are available but must be selected using the Advanced button.

Remote Installation of MediaAgent on S3260

To perform a remote installation of MediaAgent on S3260, complete the following steps:

1. From the CommCell Console ribbon, on the Tools tab, click Add/Remove Software, then select Install Software from the drop-down menu.
2. The Installer Wizard will appear, click Next.
3. **On Select the computer's operating system page, select Windows, click Next.**
4. On Select how to discover the computers for installing the software page, click Next.
5. **On Select the computer's operating system page, select Windows, click Next.**
6. On the Enter the host names of the computers page, enter the hostnames or IP addresses of all S3260 servers that will host the MediaAgent role, click Next.
7. On the Enter Account Information page, enter credentials for a user with local administrator privileges on the S3260 and click Next.
8. On the Select Package(s) to install page, select MediaAgent and Virtual Server packages > click Next
9. On the Optional Settings page, select the Index cache to this folder checkbox and enter I:\indexcache in the Index Cache path field > click Next.
10. On the Firewall Configuration page, click Next.

11. On the Please Select When to Run the Job page, click Next
12. On the Summary page, click Finish. An Install Software job will be initiated. Monitor this job in the Job Controller window.



Make sure the MediaAgent installation is complete before proceeding.

Commvault Data Platform Configuration

Deduplicated storage pools and snapshot management for the FlashArray//M need to be configured before data protection and recovery operations can take place. The full details of the policies configured in this design are shown in the Appendix: Commvault Configuration Details.

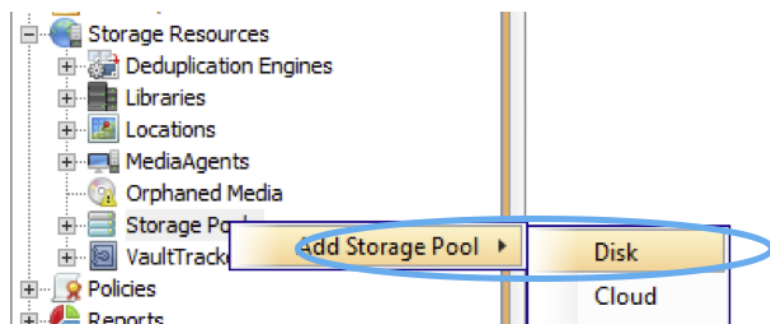
Configuring Disk Storage Pool

- Storage Pools provide a scalable and easy to manage storage target. Multiple cross-platform MediaAgents can share a storage pool. Storage capacity can be scaled on demand by adding more storage paths.
- When configuring a storage pool, depending on the selection of disk, tape or cloud, the following entities are created:
- Disk Storage Pool, a Global Deduplication policy and a dependent storage policy, and the associated disk storage
- Cloud Storage Pool, a Global Deduplication policy and a dependent storage policy, and the associated cloud storage
- Tape Storage Pool and a Global Secondary Copy Policy

In this solution a disk storage pool per site will be created using the S3260 as a target. For a single-site solution only one pool is created, and for a multi-site solution a storage pool is created in each site.

To configure the disk storage pool, complete the following steps:

1. From the CommCell Browser, expand to Storage Resources > Storage Pools.
2. Right-click the Storage Pools and click Disk. The Create New Storage Pool Wizard opens.



3. On the Enter the Storage Pool Name page, enter the Storage Pool Name. For this example the storage pool name is `gdsp_prod_01`.
4. On the Configure storage page, set options as follows:

Select the MediaAgent with the disk storage, in this case `mediaagent-1`.

Enter or browse to the desired folder on the L: drive, in this case `L:\dl_prod_01`. The folder does not need to exist.

5. On the Specify the location to store the Deduplication Database page, select the MediaAgent, select the Location of the deduplication database, and click Next.

The default name is typically sufficient.

Select the MediaAgent hosting the database, in this case `mediaagent-1`.

Enter or browse to the desired folder on the D: drive, in this case `D:\gdsp_prod_01`. The folder does not need to exist.

6. Click Finish to create the Disk Storage Pool.



Repeat this procedure to create a storage pool for each location/campus MediaAgent in a multi-site solution.

FlashArray//M Integration

The Array Management tool in the CommCell Console records the configuration details for all arrays that will be utilized with IntelliSnap technology. This configuration is performed only one time per array, and all clients

will inherit this configuration. IntelliSnap software will automatically detect the array on each client at the time of execution to ensure maximum flexibility in the configuration

To integrate FlashArray//M, complete the following steps:

1. From the CommCell Console ribbon, on the Storage tab, click Array Management.
2. The Array Management menu will appear. Click Add.
3. The Array Properties menu will appear. Set options as follows to configure the FlashArray//M:

The screenshot shows the 'Array Properties' dialog box with the 'General' tab selected. The 'Snap Vendor' dropdown is set to 'PURE Storage'. The 'Name' field contains 'pure.isl.commvault.lab'. The 'Control Host' field is empty. The 'User Account' field contains 'pureuser' and has a 'Change' button next to it. The 'Description' field contains 'Pure Storage Array Optional Description Location, Rack, Use Cases, etc.'. Four blue callout boxes with arrows point to specific fields: 'Select **PURE Storage**' points to the 'Snap Vendor' dropdown; 'Hostname or IP Address of Pure Storage FlashArray//M' points to the 'Control Host' field; 'Provide user credentials for the Pure Storage FlashArray//M. For the password use the **API Token**. Do not utilize the user's password.' points to the 'User Account' field; and 'Provide an optional description for the array. Useful for recording additional information about the Pure Storage FlashArray//M.' points to the 'Description' field.

4. Click OK to save the Pure Storage array configurations and click OK again to exit the Array Management screen. The array is now configured in Commvault.



The FlashArray//M user account requires “storage administrator” privileges. Please refer to the Appendix: FlashArray API Token Lookup for procedures to obtain the API token.

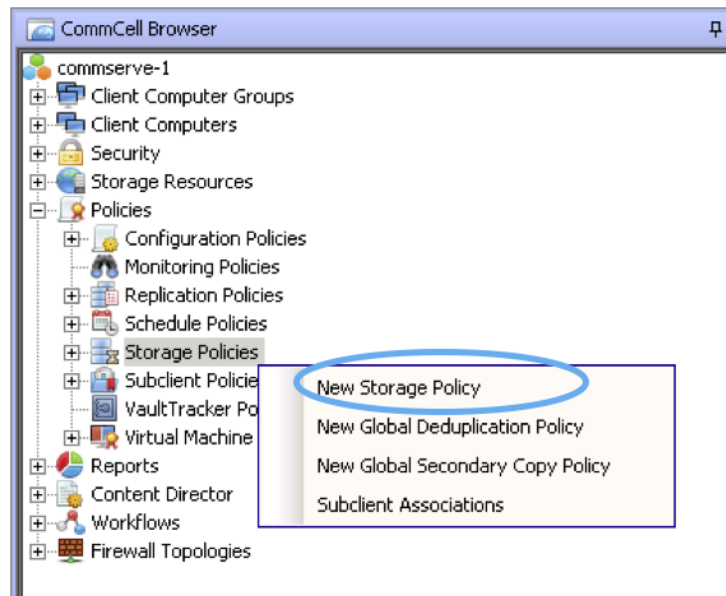
Creating Storage Policies

Storage policies act as a channel for backup and restore operations. Its chief function is to map data from its original location to physical media and define retention. This procedure will create a storage policy called “**plan_gold_vm_01**” using **global deduplication**, with 30-day retention and snapshot management capabilities. For a multi-site solution, the resulting configuration will also replicate protected data to a second site, also with 30-day retention.

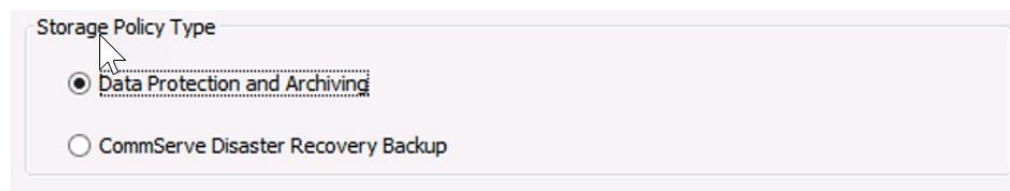
Create Storage Policy

To create the storage policy, complete the following steps:

1. From CommCell Browser, expand Policies > right-click Storage Policies > click New Storage Policy.



2. The Create Storage Policy Wizard will open. Select the default Storage Policy type of Data Protection and Archiving. Click Next to continue.



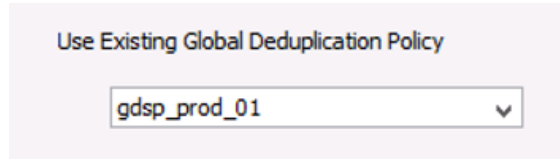
3. Enter the Storage Policy Name, in this case “plan_gold_vm_01”, and click Next.



4. On the global deduplication policy page, click Yes and select Enable Client Side Deduplication. Click Next.



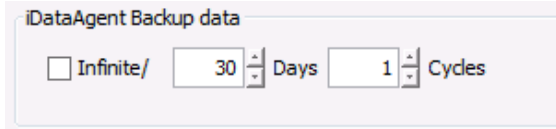
- On the global deduplication policy selection page, select the Global Deduplication Policy created from the storage pool, in this case “gdsp_prod_01”. Click Next.



Use Existing Global Deduplication Policy

gdsp_prod_01

- Enter the Retention Information, in this case 30 days and 1 cycle. Click Next.



iDataAgent Backup data

☐ Infinite/ 30 Days 1 Cycles

- Click Finish to close Create Storage Policy Wizard.



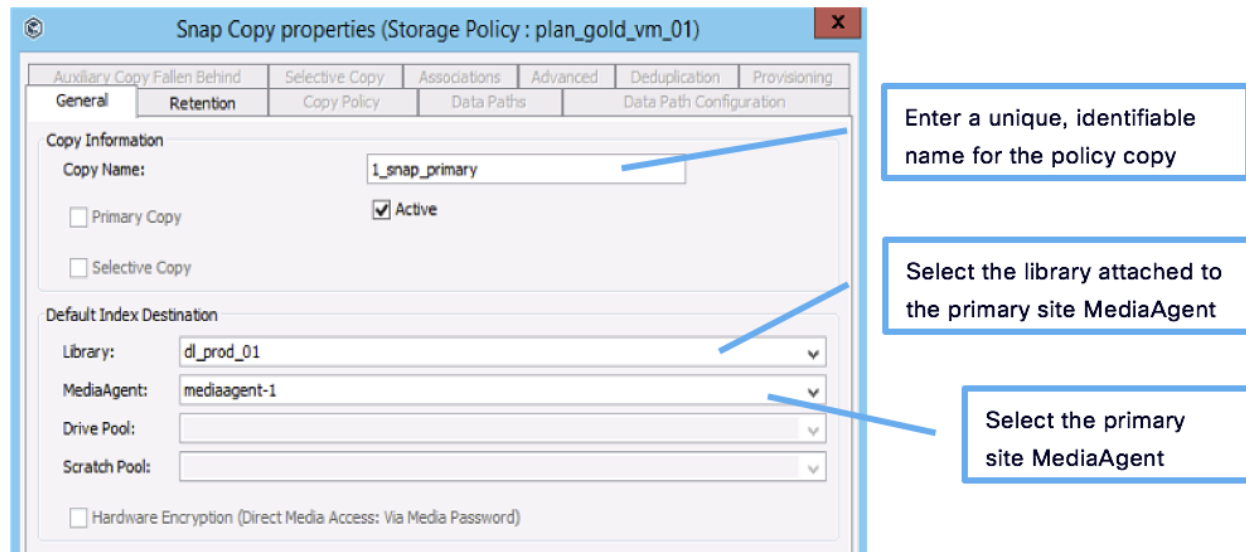
In the example above, the retention is set to 30 days, but the policy can be tailored to whatever the recovery SLA dictates. Most deployments will have multiple storage policies to service different SLAs for different data.

Create Snapshot Copy (IntelliSnap® Technology)

IntelliSnap software operations require a snapshot copy to house the indexing information and define the retention on the snapshots. Any currently defined storage or newly created data protection Storage Policy supports the addition of a snapshot copy.

To create a Snapshot copy, complete the following steps:

- Right-click the plan_gold_vm_01 Storage Policy, select All Tasks, and then click Create New Snapshot Copy.
- The Snap Copy Properties dialog opens for the newly created Snapshot Copy in the Storage Policy.



Snap Copy properties (Storage Policy : plan_gold_vm_01)

General Retention Copy Policy Data Paths Data Path Configuration

Copy Information

Copy Name: i_snap_primary

☐ Primary Copy ☒ Active

☐ Selective Copy

Default Index Destination

Library: dl_prod_01

MediaAgent: mediaagent-1

Drive Pool:

Scratch Pool:

☐ Hardware Encryption (Direct Media Access: Via Media Password)

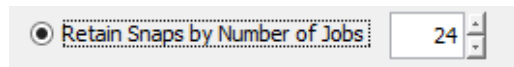
Enter a unique, identifiable name for the policy copy

Select the library attached to the primary site MediaAgent

Select the primary site MediaAgent

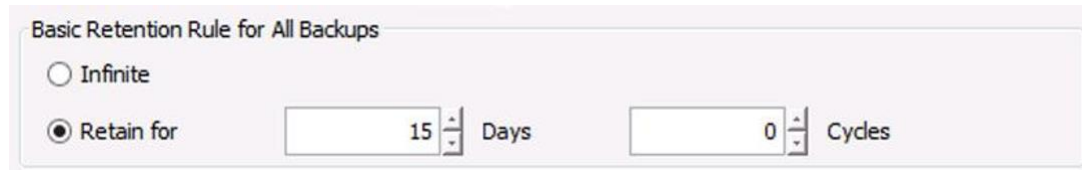
3. Select the “Retention” Tab.

4. To store snapshots solely based on the number of jobs under retention, regardless of time passed, select the “Retain Snaps by Number of Jobs” setting:



☒ Retain Snaps by Number of Jobs: 24

5. To store snapshots based on days, set the amount of days under the Basic Retention Rule for All Backups, and set the Cycles to 0:



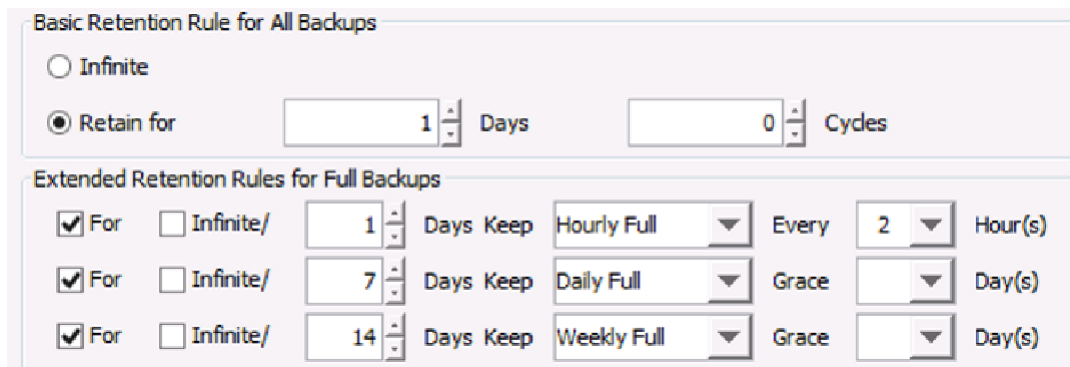
Basic Retention Rule for All Backups

☐ Infinite

☒ Retain for 15 Days 0 Cycles



Extended snapshot retention configurations can be enabled from this screen also. In the below configuration, the last snapshot from every 2 hour period is kept for one day, the last snapshot each day is retained for 7 days, and finally, the last snapshot of the week is retained for 14 days.



Basic Retention Rule for All Backups

☐ Infinite

☒ Retain for 1 Days 0 Cycles

Extended Retention Rules for Full Backups

For	Infinite/	Days	Keep	Every	Hour(s)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	Hourly Full	2	Hour(s)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	7	Daily Full		Day(s)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	14	Weekly Full		Day(s)

6. Click OK to create the Snapshot Copy in the Storage Policy



Make sure the snapshot retention will not overrun the capabilities of the array based on the planned protection schedule.

Create Storage Policy Copy with Deduplication (Replication to Remote Site)

A secondary storage policy copy provides the means to make additional copies of the data in a separate site and/or with different retention. An auxiliary copy operation must be performed to replicate the data to the secondary copy. DASH (Deduplication Accelerate Streaming Hash) Copy, is an option for a deduplication-enabled storage policy copy (auxiliary copy), to send only unique data to that copy. DASH Copy uses network bandwidth efficiently and minimizes the use of storage resources.

To create a storage policy copy with deduplication, complete the following steps:

1. In the CommCell Browser window, expand Policies and Storage Policies. Right-click the plan_gold_vm_01 Storage Policy, select All Tasks, and then click Create New Copy.

2. The Copy Properties dialog appears for the new storage policy copy. Set the options as follows:

Enter a unique, identifiable name, in this case 3_auxcopy_dr.

Enable global deduplication.

Select the global deduplication policy for the secondary site.

3. Select the Retention tab. Set Days to 30 and Cycles to 1:

4. Click OK to create the Storage Policy Copy.



The Storage Policy should now have 3 storage policy copies: a snapshot copy, a primary copy to disk and auxiliary copy to remote site/DR datacenter.

commserve-1 > Policies > Storage Policies > plan_prod_01_vm_gold >

Copy	Copy Type	Status	Default Library	MediaAgent	Retain For	Deduplication	Precedence
1_snap_primary	Snap Primary	✓	dl_prod_01	mediaagent-1	1 days, 0 cycles	<input type="checkbox"/>	1
2_primary	Primary	✓	dl_prod_01	mediaagent-1	30 days, 1 cycles	<input checked="" type="checkbox"/>	2
3_dr_copy	Synchronous	✓	dl_dr_01	mediaagent-2	30 days, 1 cycles	<input checked="" type="checkbox"/>	3

Creating Schedule Policies

A Schedule Policy provides a single management point for scheduling multiple protection jobs within a CommCell. Schedule policies give the flexibility to modify or alter job schedules for multiple data sets from one central location. The modifications are automatically reflected in the associated schedules.



The following example will create a schedule policy called vsa_gold, targeted at VM protection. The schedule consists of daily snapshots and incremental backups and weekly synthetic full backups to enable an incremental forever strategy. Movement of data from snapshot to media and auxiliary copy are managed separately.

To create schedule policies, complete the following steps:

1. From the CommCell Browser, navigate to Policies.
2. Right-click Schedule Policies and click New Schedule Policy.
3. The New Schedule Policy dialog opens. Fill in the following information:

The screenshot shows the 'New Schedule Policy' dialog box with the following fields and annotations:

- Name:** (Annotation: Schedule policy name, in)
- Type:** (Annotation: Type of schedule: Auxiliary Copy, Backup Copy, Content Indexing, Data Protection, DDB Verification)
- Agent Type:** (Annotation: Agent type(s) to manage, in this case Virtual Server)
- Description:** (Annotation: Appropriate description for the policy)
- Tasks:** A table with columns: Schedule N..., Job Type, Pattern, Time Zone. (Annotation: Click to create schedule patterns pointing to the 'Add' button)
- Buttons:** Add, Edit, Delete, OK, Cancel, Save As Script, Help.

4. Click Add to create a pattern.
5. The Backup Task Options dialog opens. Fill in the following information on the Schedule Pattern tab:

Schedule Pattern | **Backup Options**

Schedule Name: Weekly Synthetic Full

Schedule frequency: Weekly

Start Time: 7:00 PM

On these days: ☐ Monday, ☐ Tuesday, ☐ Wednesday, ☐ Thursday, ☒ Friday, ☐ Saturday, ☐ Sunday

Repeat: Every 01 Week(s) **Exceptions**

☐ Repeat every 8 hr(s) 0 min(s) until 11:59 PM

Options>>

Descriptive name for the pattern

Job start time for the pattern

Granular scheduling options based on selected frequency

- Patterns in a schedule policy with the Data Protection type will have a Backup Options tab to configure job type and specific configuration options. On the Backup Options tab select the options that apply to your environment. In this example the backup type is synthetic full. Other options can be set by clicking the Advanced button; these options are not covered in detail in this document.

Schedule Pattern | **Backup Options**

Select Backup Type

☐ Full

☐ Incremental

☐ Differential

☒ Synthetic Full

☒ Run Incremental Backup

☒ Before Synthetic Full

☐ After Synthetic Full

- Click OK.
- Repeat for each additional desired schedule pattern.



The options shown will create a pattern that runs a weekly synthetic full backup, starting at 7:00 PM every Friday. For design validation a second pattern was created to execute two incremental backups per day. The incremental backup pattern includes the advanced options to run backup copy with the snap backup and to index the backup copy for granular recovery.

- Click OK to commit the schedule policy.

Configure Virtual Machine Protection for VMware

The Virtual Server Agent (VSA) for VMware provides a unified protection and recovery vehicle for all virtual machine data in your vCenter. In addition to complete protection of entire virtual machines for disaster recovery, the Virtual Server Agent provides granular backup and recovery options. Options such as customized automatic discovery, deduplication, and reporting ensure all your virtual machine data is easily traceable and retrievable whenever the need arises.

The VSA for VMware enables you to perform backup and restores and manage virtual machine data in complex virtualized environments. VSA uses vStorage APIs for Data Protection (VADP), with support for all guest operating systems supported by VADP.

Commvault software uses VSA proxies to facilitate the movement of virtual machine data during backup and recovery operations. The VSA proxies are identified in the virtualization instance properties. For Microsoft Hyper-V, each VSA proxy will be designated to protect virtual machines hosted on the physical Hyper-V server. For VMware, the VSA proxies will be used as a pooled resource. This means that depending on resource availability different proxies may be used to backup VSA sub-clients each time a job runs. This method of backing up virtual machines provides for higher scalability and resiliency.

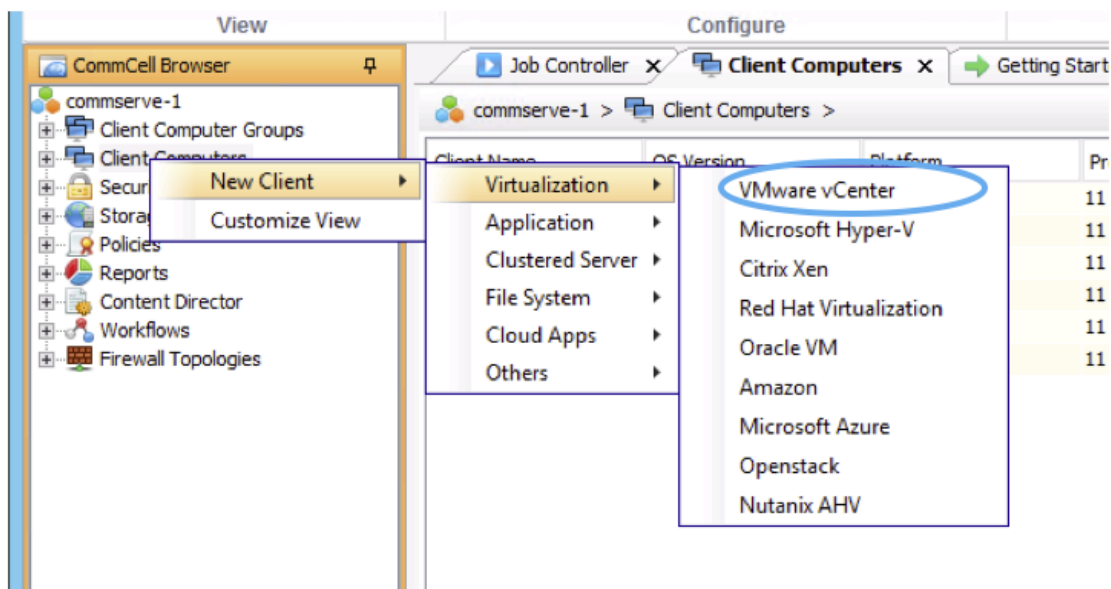


In this solution, the VSA proxy coexists with the MediaAgent.

Creating a Virtualization Client for the VMware vCenter

To create a virtualization client for each vCenter instance, complete the following steps:

- From the CommCell Console, right-click Client Computers > select New Client > select Virtualization and select VMware vCenter.



- In the Create VMware vCenter Client dialog, enter the appropriate vCenter information:

Create VMware vCenter Client

Client Name :

vCenter Server Name:

User Name:

Password:

Confirm Password:

Proxies: Add... Remove

Clients / Client Groups

mediaagent-1

OK Cancel Save As Script Help

Display name to assign to the new client

DNS hostname or IP address of vCenter server

vCenter login credentials

Click Add to associate a VSA proxy

3. Select the VSA Proxy server, in this case mediaagent-1, and click Include. Click OK to close the Select Clients / Client Groups window.

Select Clients / Client Groups

Clients / Client Groups

Exclude

plan_prod_01_vm_silver clients

plan_vm_gold clients

Proxy Clients

Solr Servers

vc-branch.earthquakes.cisco.com

vc.earthquakes.cisco.com

vc_prod_01

mediaagent-2

< Exclude

<< Exclude All

Include >

Include All >>

Include

mediaagent-1

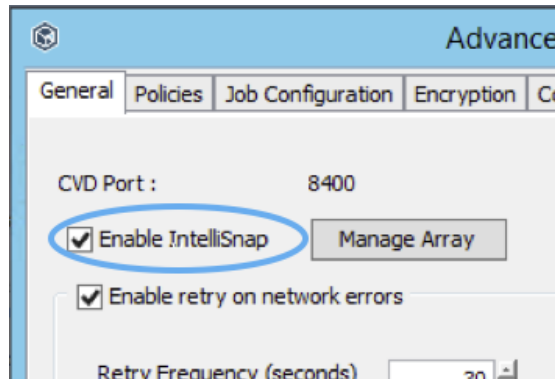
OK Cancel Help

4. Click OK to close the Create VMware vCenter Client wizard.



A VMware vCenter client is created and displayed under the Client Computers node in the CommCell Console.

5. From the CommCell browser, expand Client Computers, then right-click the new vCenter client and select Properties.
6. Click the Advanced button on the Client Computer Properties dialog.
7. Click the Enable IntelliSnap checkbox and click OK to close the Advanced Client Properties for vCenter dialog.

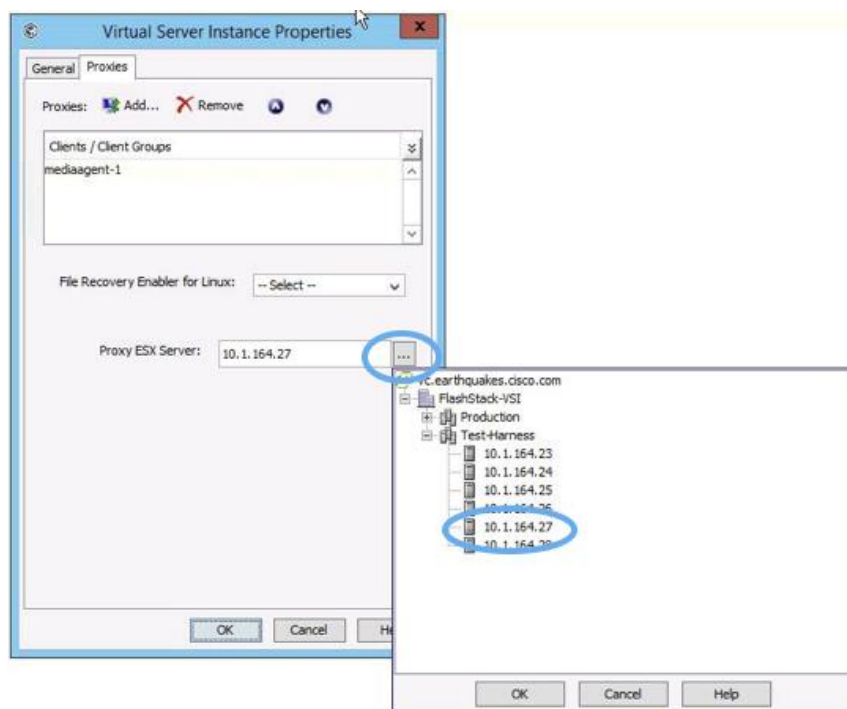


8. Click OK to close the Client Properties for the vCenter client.
9. The vCenter instance needs to have a default ESXi host specified for VADP snapshot mount operations.
10. From the CommCell browser, expand the new vCenter client and Virtual Server until VMware is visible. Right-click VMware and select Properties.



vCenter details such as hostname and credentials can be changed in the VMware instance properties.

11. The Virtual Server Instance Properties dialog appears. On the Proxies tab, click the Browse (ellipsis) button next to Proxy ESX Server. In the popup inventory screen, located and select the desired ESXi host, then click OK. In this example, ESXi host 10.1.164.27 is selected.



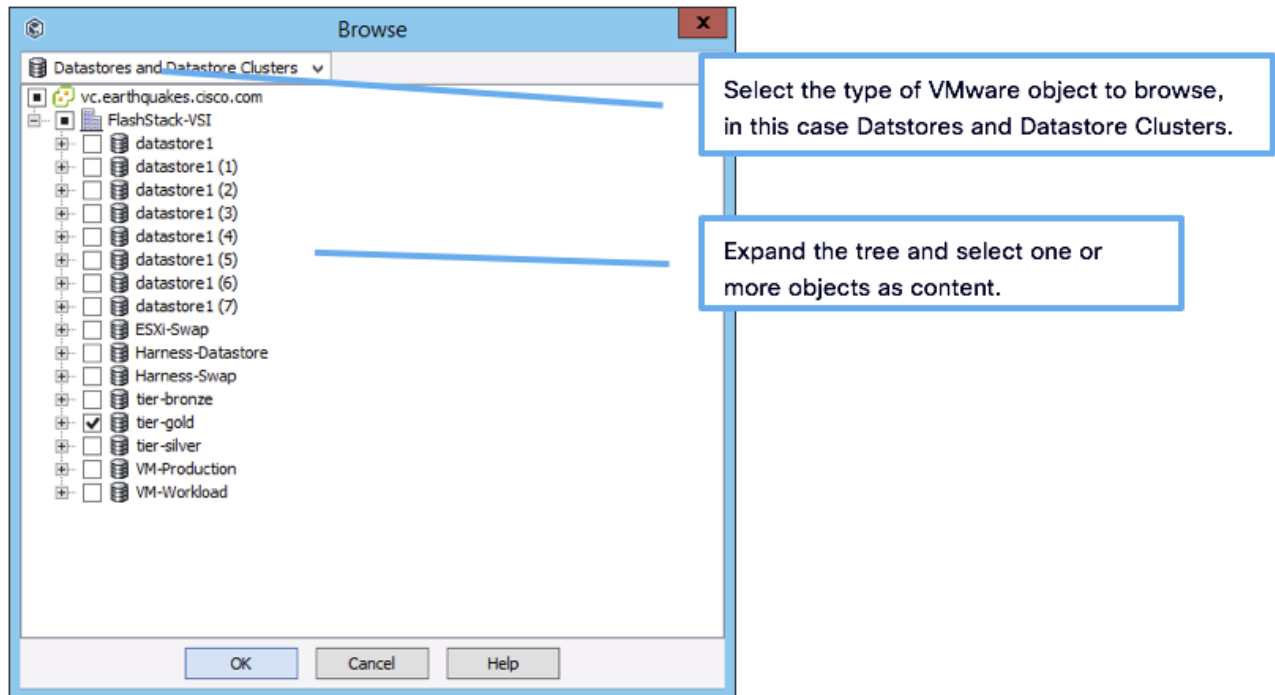
12. Locate and select the ESXi host to be used for VADP snapshot mount operations.

Configure Subclient for VM Protection

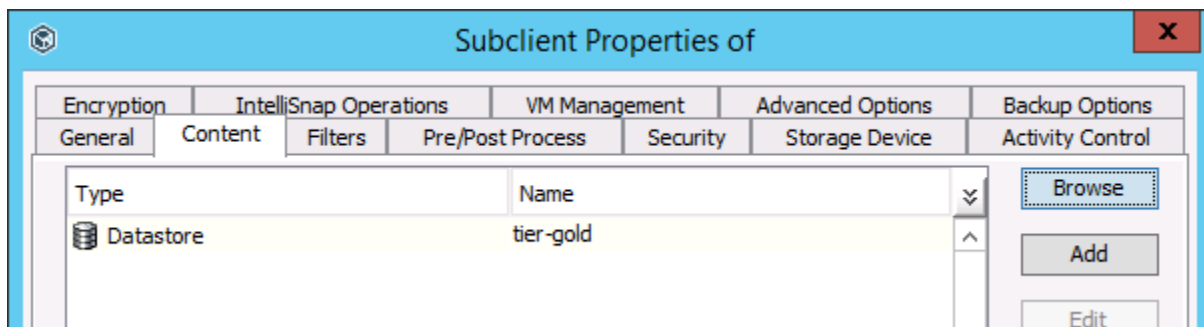
To provide protection for a specific set of virtual machines, create a subclient. A user-defined subclient can identify virtual machines that have the same Service Level Agreement (SLA), that reside on the same datastore, or that otherwise need to be backed up on the same schedule. This example will create a subclient for protecting VMs in a gold tier datastore on a FlashArray//M volume.

To create a subclient, complete the following steps:

1. From the CommCell Browser, navigate to Client Computers > Virtualization_Client (for example, vc.earthquakes.cisco.com) > Virtual Server > VMware.
2. Right-click a backup set and click New Subclient. The Subclient Properties dialog appears.
3. On the General tab, enter a name for the subclient. In this example, the subclient is named vm_gold_vmfs.
4. On the Content tab, click Browse to select contents from vCenter inventory. Click OK to close the Browse window.



5. The selected objects will be listed as subclient content.

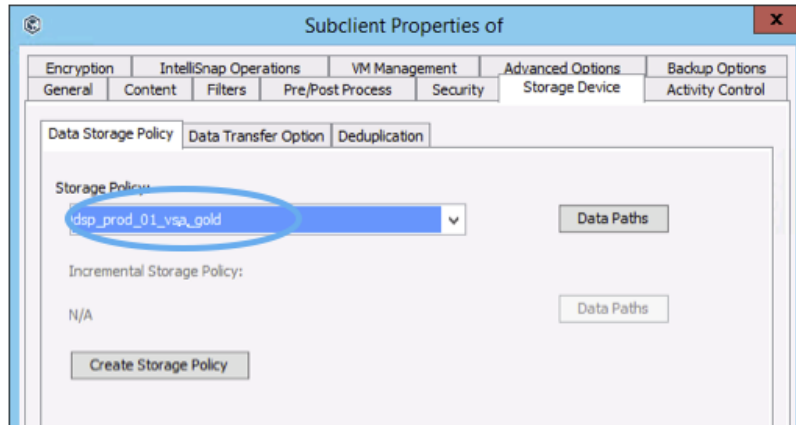


If you have deployed MediaAgents, VSA proxies, or vCenter on virtual machines, [filter those virtual machines](#) from VSA backups. (If you need to protect files on those virtual machines, install in-guest agents on those virtual machine to perform file backups.)

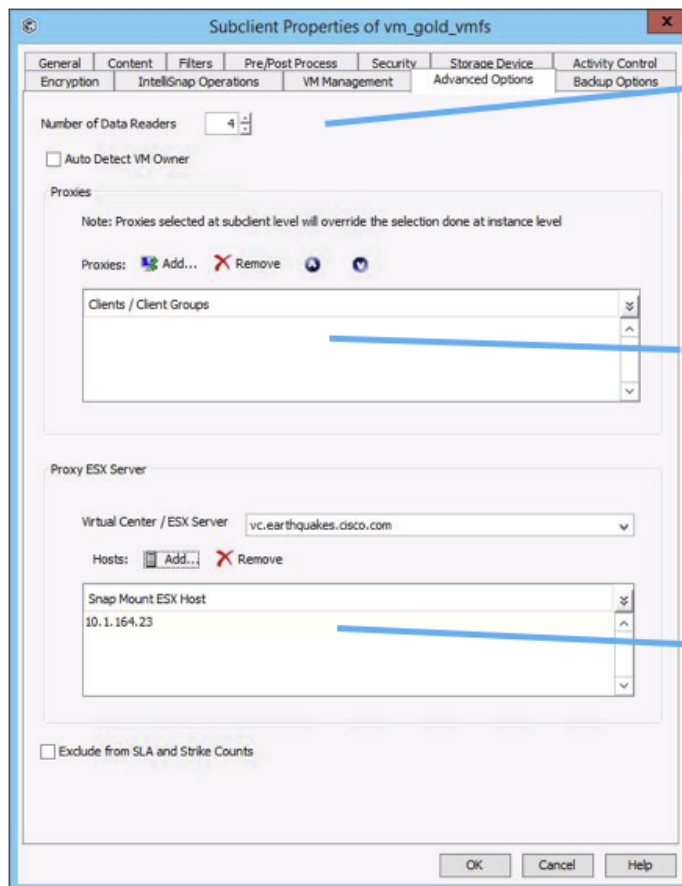


Subclients can contain a mix of content types. If the subclient content includes containers such as datastores, the virtual machines in those containers will be discovered during protection jobs.

6. On the Storage Device tab, select the **appropriate** storage policy, in this case “dsp_prod_01_vsa_gold”, then click OK.



7. On the IntelliSnap tab, select the Enable IntelliSnap Checkbox. Select PURE Storage Snap in the Snap Engine dropdown.
8. On the Advanced Options tab, subclient settings can optionally be tuned to optimize backups based on the environment.

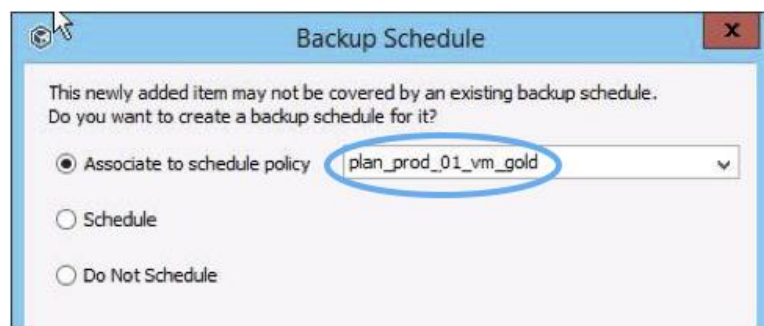


Data Readers controls how many VMs can be backed up in parallel.

Alternate VSA proxies can be selected for a subclient.

ESXi hosts can be overridden for a subclient. Multiple hosts can be selected by clicking Add.

9. Click OK to create the subclient.
10. In the Backup Schedule dialog box, select Associate to schedule policy and select the appropriate policy, in this case plan_prod_01_vm_gold, and then click OK.



The Commvault Data Platform deployment and configuration is complete. FlashStack VSI Virtual Machines will be protected by automated discovery rules and scheduling. The next section will cover operational monitoring and recovery operations.

11. Repeat the above process for additional subclients, for example, VMs in lower recovery tiers.

Operating Within the Commvault Environment

Admin Console Overview

The Admin Console is a web-based user interface for administration that is streamlined for routine data protection and recovery tasks. The Admin Console enables administrators and application owners provides streamlined administrative tasks including policy management, operations, analytics, and monitoring.

To access the Admin Console, complete the following steps:

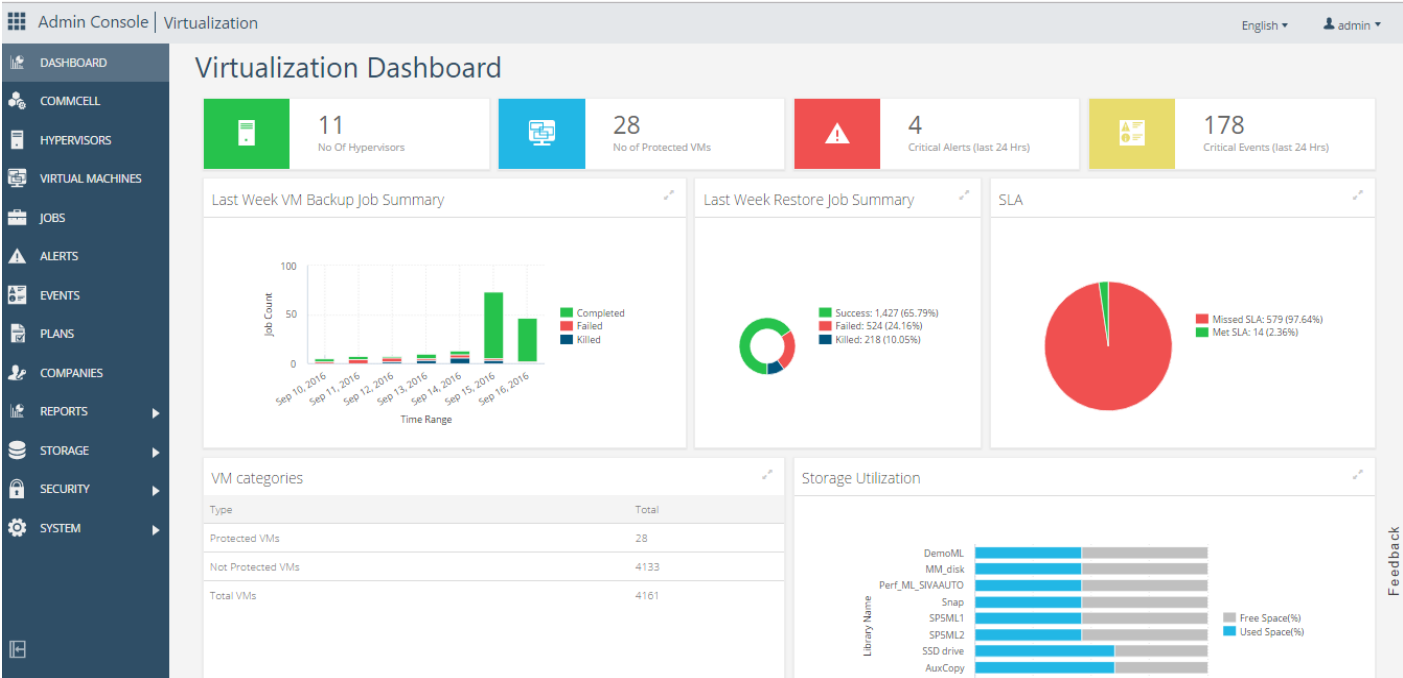
1. Go to the Admin Console URL: <http://<webhost>/adminconsole/>. In this example the URL is <http://commserve-1/adminconsole>.
2. Type your user name and password, and then click Login.



The first time you log in, the software prompts you to do some basic setup for your environment, including product registration and adding email server information for alerting purposes. This setup process is not covered in this document.

Admin Console Dashboard

Provides a quick overview of managed assets, alerts, and SLA target.

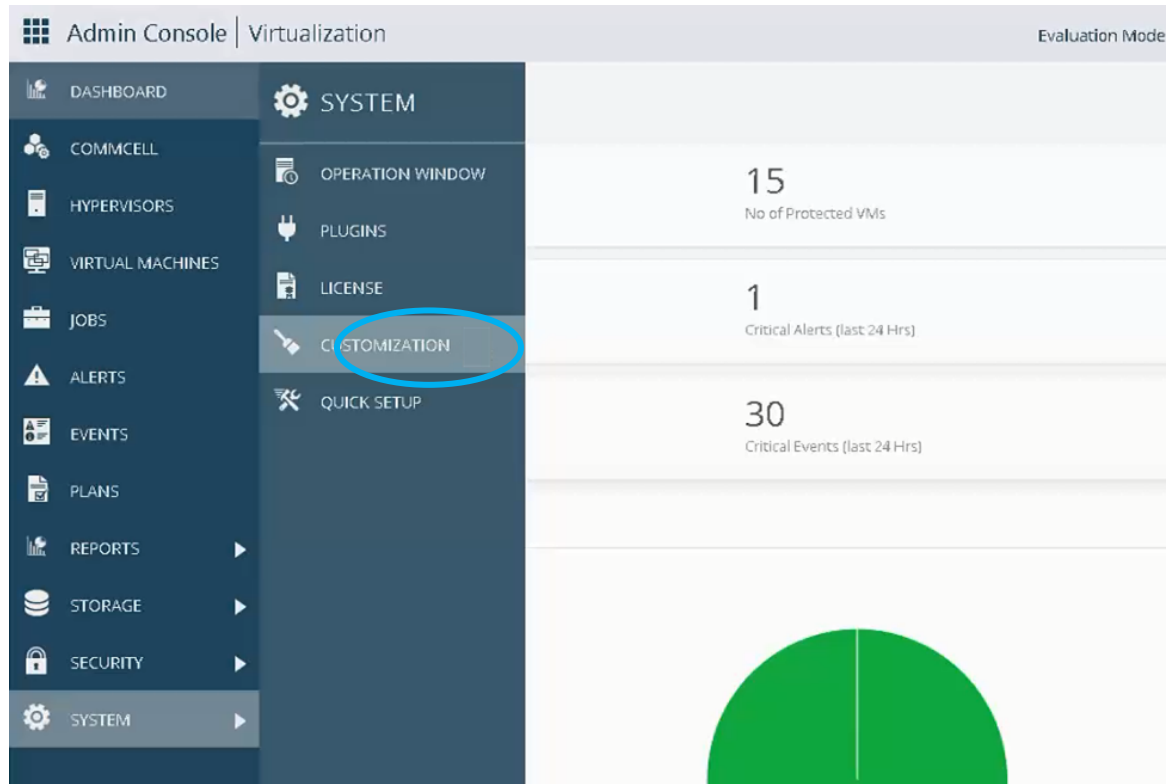


Customizing the Administrative Console

The Admin Console can be customized to your preferences, as well as the ability to upload brand/logos.

To customize the Admin Console, complete the following steps:

- 1. From Admin Console > Virtualization, click SYSTEM, and click CUSTOMIZATION.



- From the Customization window, select options. Options include color scheme and a custom logo that appears in the header bar. The options shown will change the interface to include a FlashStack logo and coordinating colors. Click Save to apply changes.

Customization

Primary color
This is your brand color. Changes the color of the side column, all header text and action buttons.

Header color
Changes the top bar color.

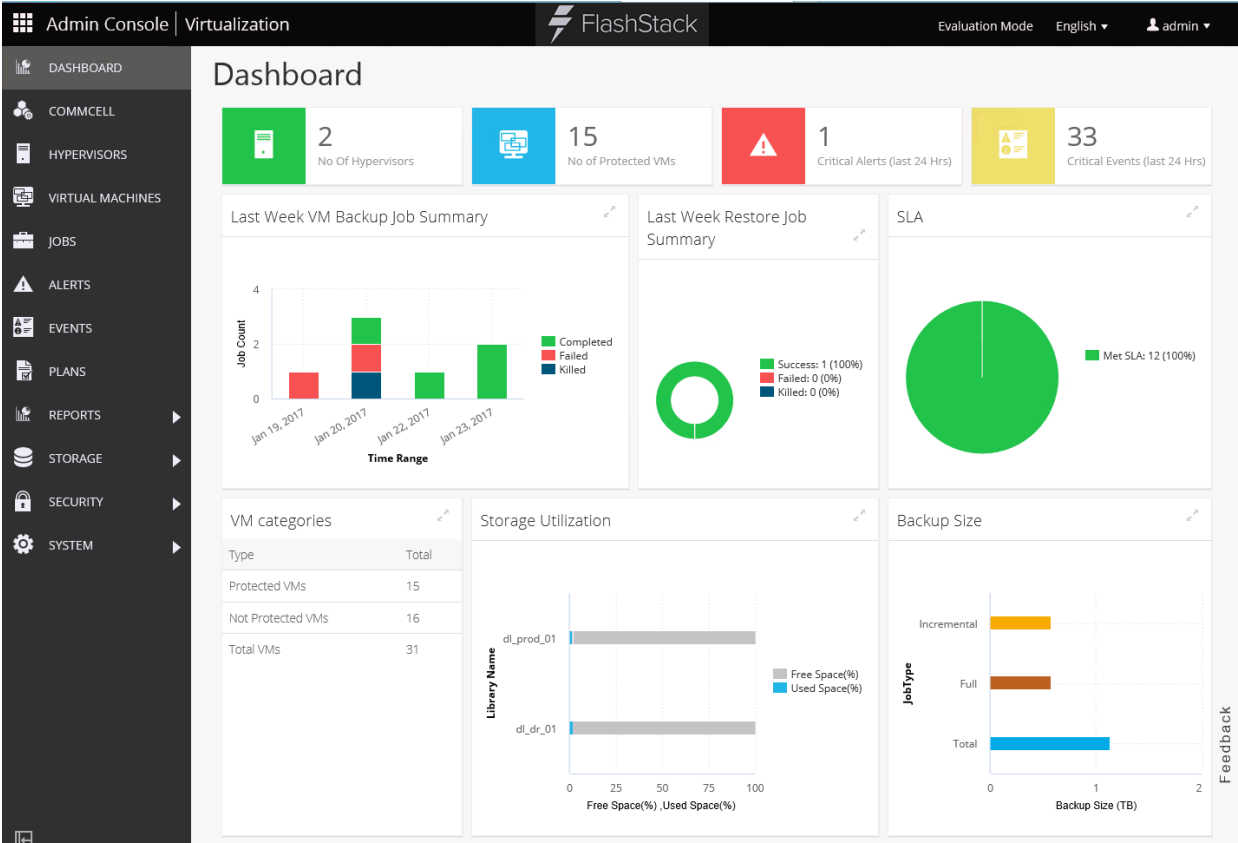
Header text color
Changes the top bar text color.

Select custom logo
Image requirements: 200 x 50 pixels in JPG, JPEG, PNG or GIF format. No larger than 10 KB.

Navigation icon color
Changes the color of the navigation icon on the side column.

Link color
Changes the [color of links across all pages](#). Can be the same as the primary color.

The interface is now customized.



VM Recovery Operations

Application owners and administrators can perform VM restore operations from the Admin Console. This example will show the recovery of a file from one VM to another VM.



Backup operations, either using the schedules configured earlier or run on demand, need to complete before data can be restored.

To recover a file from a VM, complete the following steps:

1. From the Admin Console Virtualization view, click Virtual Machines, then click the name of the VM with the data being restored, in this case IOM-CTRL.

The screenshot shows the FlashStack Admin Console interface. The left sidebar contains navigation links: DASHBOARD, COMMCELL, HYPERVISORS, VIRTUAL MACHINES, JOBS, ALERTS, EVENTS, PLANS, and REPORTS. The main content area is titled 'VMs' and displays a table of virtual machines. The 'IOM-CTRL' VM is highlighted with a blue circle.

Name	Hypervisor	Backup size	Last backup time	Host	Proxy
VM-04	vc.earthquakes.cisco...	120.13 GB	Jan 22, 2017 9:45:36...	10.1.164.23	mediaagent-1
VM-03	vc.earthquakes.cisco...	120.12 GB	Jan 22, 2017 9:45:35...	10.1.164.24	mediaagent-1
VM-02	vc.earthquakes.cisco...	120.12 GB	Jan 22, 2017 9:45:37...	10.1.164.23	mediaagent-1
VM-01	vc.earthquakes.cisco...	120.12 GB	Jan 22, 2017 9:45:37...	10.1.164.23	mediaagent-1
vdbench-06	vc.earthquakes.cisco...	0 B	Jan 13, 2017 7:58:50...	10.1.164.25	mediaagent-1
IOM-CTRL	vc.earthquakes.cisco...	100.02 GB	Jan 23, 2017 7:44:17...	10.1.164.25	mediaagent-1

2. The focus changes to the VM details. Click the Restore link to start the restore process.

The screenshot shows the FlashStack Admin Console interface with the 'IOM-CTRL' VM details page. The left sidebar is the same as the previous screenshot. The main content area is titled 'IOM-CTRL' and includes a 'Summary' section and a 'Security' section. The 'Restore' link in the top right corner is highlighted with a blue circle.

Virtual machines >

IOM-CTRL

Backup now Last backup Jobs **Restore**

Summary

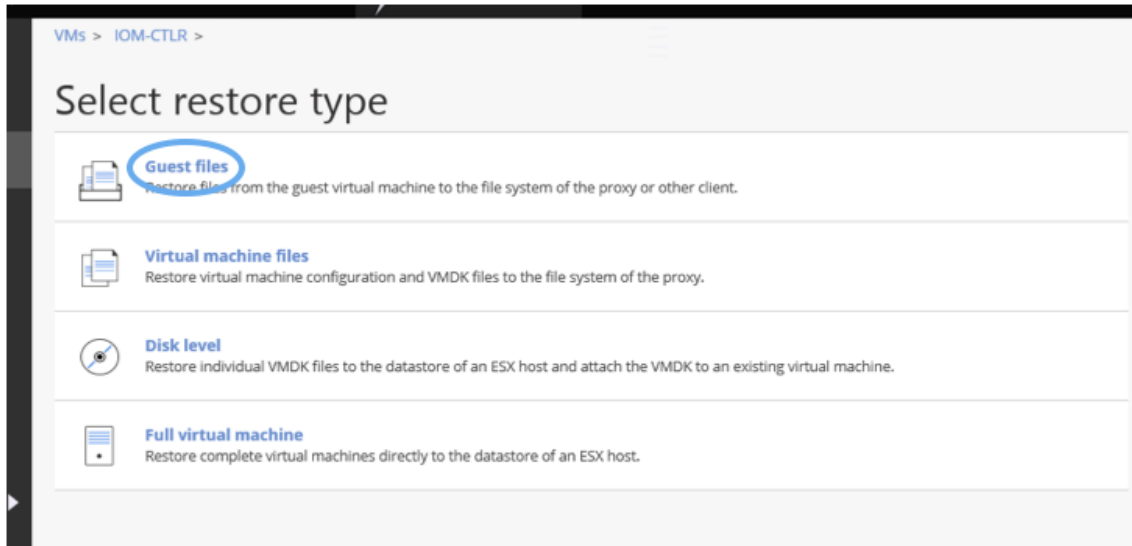
Backup status	Backed up with error
Hypervisor	vc.earthquakes.cisco.com
Subclient	SQL Application Aware Backups
Proxy	mediaagent-1
VM size	100.01 GB
Backup size	100.02 GB
Last backup time	Jan 23, 2017 7:44:17 AM
Guest OS	Microsoft Windows Server 2008 R2 (64-bit)
Guest size	100.02 GB
Host	10.1.164.25
Total backup time	2 sec

Security

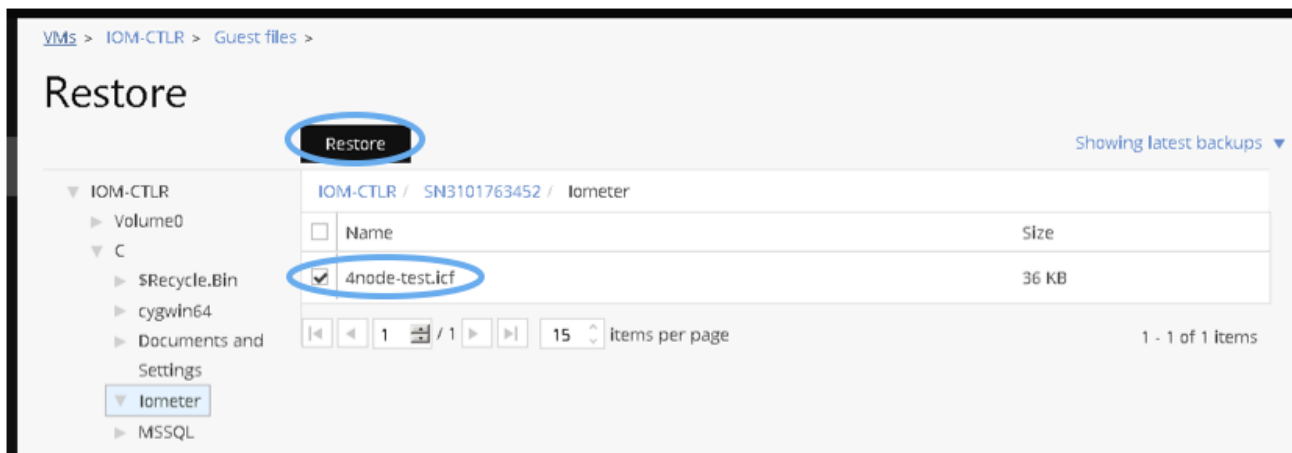
Associations Owners

No owners configured

3. From the Select Restore Type, choose the type of data to be restored, whether guest files, virtual machine files, virtual disks, or full VM. This example shows the guest files option.



4. Locate and select the file(s) to be restored. In this case the file being recovered is C:\lometer\4node-test.icf. Click the Restore button when all desired files have been selected.



5. Select the restore destination options as follows:

Restore to

☐ My VM
 ☒ Other VM
 ☐ Guest agent

Proxy: mediaagent-1

Destination hypervisor: vc.earthquakes.cisco.com

- 10.1.164.27
- 10.1.164.28
- IOM-CTRL
- IOM-WKR
- VM-01
- VM-02
- VM-03
- VM-04
- VM-05
- VM-06
- VM-07
- VM-08

Virtual machine login:

Username: flashstack/flashstack

Password:

Path: C:\TEMP [Browse](#)

☒ Overwrite if it already exists

Cancel Submit

Select the target type:

My VM – protected virtual machine owned by the current user

Other VM – select VMs through a hypervisor inventory (used in example).

With “My VM” and “Other VM” options, choose the VSA proxy to use for the hypervisor communication during the restore.

With the “Other VM” option, choose the hypervisor to query for VM targets.

With the “Other VM” option, select a VM as the restore target.

Enter user credentials with access to the restore target. (Optional with the “Guest agent” option.)

Enter or browse to the desired destination. folder

Enable to force overwrite of existing files with the same name.

- The Restore to dialog will close and a pop up containing the restore job information will appear. Click the Jobs or View jobs link to see a list of running jobs.

Admin Console | Virtualization | FlashStack | Evaluation Mode | English | admin

VMs > IOM-CTRL > Guest files >

Restore

Restore

IOM-CTRL / SN3101763452 / Iometer

Name	Size
4node-test.icf	36 KB

Showing latest backups

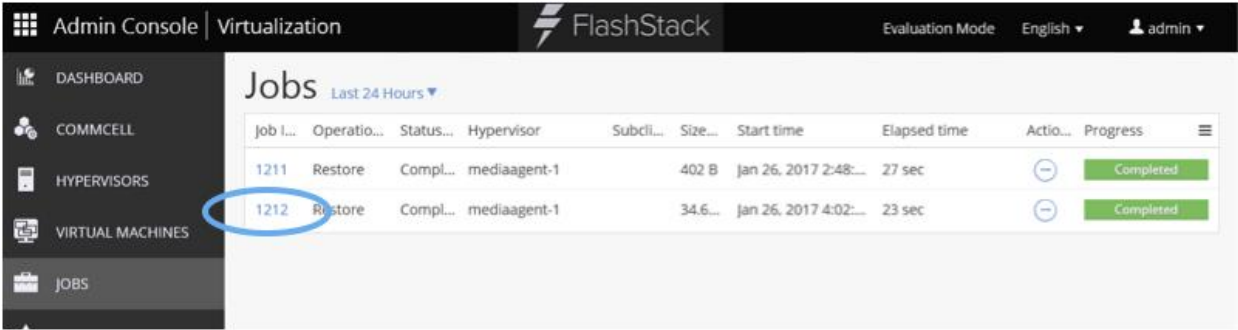
1 - 1 of 1 items

Restore requested - Job ID: 1212

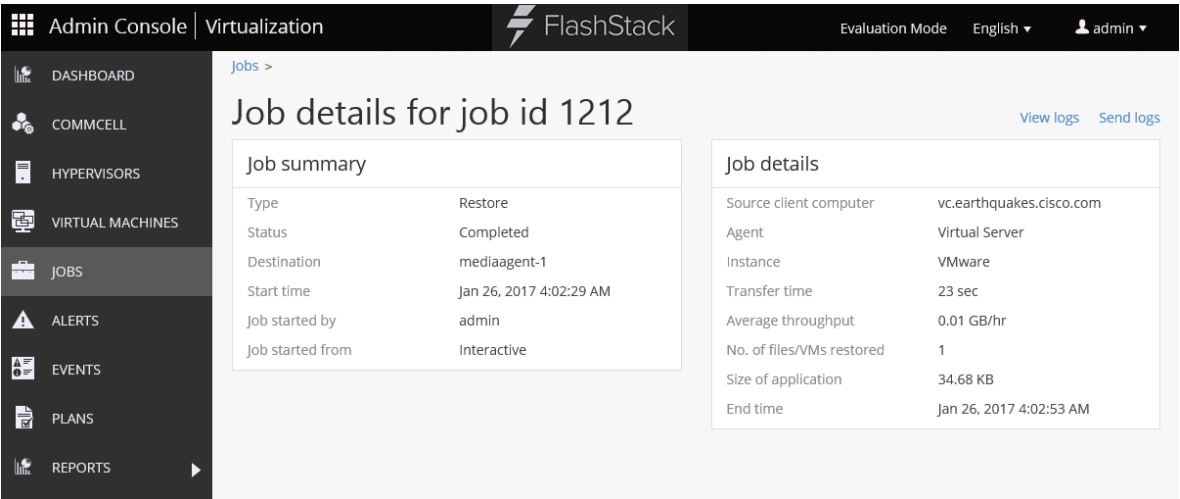
[View jobs](#)

[JOBS](#)

- The focus changes to the jobs view. Information will update as the job progresses. To see details for the selected job, click the job ID.



8. The focus changes to the details for the restore job. The information will update as the job progresses. When the job is complete the file has been restored to the selected path on the target VM.



Validation

Validate Hardware and Software

Table 1 lists the hardware and software versions used during solution validation. Each of versions have been used have been certified within interoperability matrixes supported by Cisco, Pure Storage and VMware. For more current supported version information, consult the following sources:

- Cisco UCS Hardware and Software Interoperability Tool: <http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html>
- Commvault Support Compatibility Matrix: <https://ma.commvault.com/Support/CompatibilityMatrices>
- Pure Storage Interoperability (note, this interoperability list will require a support login from Pure Storage): https://support.purestorage.com/FlashArray/Getting_Started/Compatibility_Matrix
- VMware Compatibility Guide: <http://www.vmware.com/resources/compatibility/search.php>

Table 1 Hardware and Software Used in this Solution

Layer	Device	Image
Compute	Cisco UCS 6332-16UP Fabric Interconnect	3.1(2b)
	Cisco UCS B-200 M4	3.1(2b)
	Cisco UCS S3260	3.1(2b)
	Cisco UCS C240 M4	3.1(2b)
	Cisco eNIC	2.3.0.10
	Cisco fNIC	1.6.0.28
	Cisco Windows drivers	3.0.1a
	Cisco Nexus 93180YC-EX NX-OS	7.0(3)I4(2)
Storage	Cisco MDS 9148S	7.3(0)D1(1)
	Pure Storage FlashArray //m70 (Purity)	4.7.4
Software	Cisco UCS Manager	3.1(2b)
	Commvault Data Platform	V11
	VMware vSphere ESXi	6.0 U2
	VMware vCenter	6.0 U2
	Pure Storage vSphere Web Client Plugin	2.1.0

Testing Methodology

Testing FlashStack VSI with Data Protection covered this CVD performed the following use cases:

- Local FlashArray//M snapshot management through IntelliSnap
- Streaming Backup to an S3260 MediaAgent
- Backup Replication to secondary data center S3260 MediaAgent
- Application Aware backup of MS SQL
- Live Sync of VMs to a simulated secondary data center
- VM Archiving to a simulated secondary data center

Testing was functional in nature, extending into browsing and restoring of VMs in the environment. Scale testing was not performed, but resiliency testing of the Microsoft multi-**pathing within the MediaAgent's** access to the SAN was conducted.

Summary

FlashStack delivers a platform for Enterprise and cloud datacenters using Cisco UCS Blade Servers, Cisco Fabric Interconnects, Cisco Nexus 9000 switches, Cisco MDS switches and fibre channel-attached Pure Storage FlashArray//M. FlashStack is designed and validated using compute, network and storage best practices for high performance, high availability, and simplicity in implementation and management.

FlashStack with Modern Data Protection adds onto the platform, with in-depth data assurance for virtualized environments. This integration with Commvault works with the volume snapshot management with Pure Storage FlashArray//M to expand backups to the Cisco UCS S3260 Storage Server, allowing for secondary site backups, VM archiving, and multiple options for restoration, all within a single management interface.

The FlashStack with Modern Data Protection architecture delivered by Cisco, Pure Storage, and Commvault, presents a total solution for our customers, that is scalable in both size and feature set, and brings together the critical elements of performance, efficiency, automation, availability, and recoverability. This grants peace of mind and helps drive simplicity and security into what is otherwise a disruptive and complex digital transformation.

Reference Sources for Components in this Design

Products and Solutions

Cisco Unified Computing System:

<http://www.cisco.com/c/en/us/products/servers-unified-computing/index.html>

Cisco UCS 6300 Series Fabric Interconnects:

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

Cisco UCS 5100 Series Blade Server Chassis:

<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-5100-series-blade-server-chassis/index.html>

Cisco UCS B-Series Blade Servers:

<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/index.html>

Cisco UCS C-Series Blade Servers:

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

Cisco UCS S3260 Storage Servers:

<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-s3260-storage-server/index.html>

Cisco UCS Adapters:

<http://www.cisco.com/c/en/us/products/interfaces-modules/unified-computing-system-adapters/index.html>

Cisco UCS Manager:

<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-manager/index.html>

Cisco Nexus 9000 Series Switches:

<http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html>

Cisco MDS 9000 Series Multilayer Switches:

<http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html>

Pure Storage FlashArray//M:

<https://www.purestorage.com/products/flash-array-m.html>

Commvault Data Platform:

<http://www.commvault.com/commvault-next-generation>

Appendix

Commvault Reference Architectures

Table 2 and Table 3 show Cisco and Commvault tested reference architecture configurations using Cisco UCS, Commvault CommServe (command and control software), and Commvault MediaAgent (manages data transmission between clients and Cisco storage) components.

Table 2 CommServe Architecture

	Cisco UCS C220 M4 Express	Cisco UCS C220 M4 Work Group	Cisco UCS C240 M4 Data Center	Cisco UCS C240 M4 Enterprise
CPU	12GHz Across 4 Cores	24GHz Across 8 Cores	28.8GHz Across 12 Cores	33.6GHz Across 16 Cores
Memory	16GB DDR4	32GB DDR4	32GB DDR4	64GB DDR4
Storage	600GB Useable Boot / Binaries / DB RAID 10 – 4x 300GB 10k SAS	Boot – 300GB 10k SAS (RAID1)	Boot – 300GB 10k SAS (RAID1)	Boot – 300GB 10k SAS (RAID1)
		Binaries / DB – 600GB 15k (RAID 10 – 4x 300GB Drives)	Binaries / DB – 480GB SSD (RAID 5 – 3x 240GB Drives)	Binaries / DB – 480GB SSD (RAID 5 – 3x 240GB Drives)
Storage Controller	SAS 6G RAID 512MB Flash Backed Cache	SAS 6Gbps RAID 1GB Flash Backed Cache	SAS 6Gbps RAID 1GB Flash Backed Cache	SAS 6Gbps RAID 1GB Flash Backed Cache
Network	2x 1Gbps	2x 1Gbps	2x 1Gbps	4x 1Gbps

Table 3 MediaAgent Architecture

	Cisco UCS C240 Small	Cisco UCS S3260 Medium	Cisco UCS S3260 Large	Cisco UCS S3260 Extra-Large
CPU	14.4 GHz Across 6 Cores	52.8GHz Across 24 Cores	52.8GHz Across 24 Cores	52.8GHz Across 24 Cores
Memory	32 GB DDR4	128 GB DDR4	128 GB DDR4	128 GB DDR4
Storage	Boot - 120 GB SSD	Boot - 480 GB SSD	Boot - 480 GB SSD	Boot - 480 GB SSD
	SSD Cache - 1 TB	SSD Cache - 1.6 TB	SSD Cache - 2 TB	SSD Cache - 4 TB
	BET - 30 TB usable	BET - 64 TB usable	BET - 144 TB usable	BET - 216 TB useable
Storage Controller	SAS 12G RAID 1GB Flash Backed Cache	SAS 12Gbps RAID 4GB Flash Backed Cache	SAS 12Gbps RAID 4GB Flash Backed Cache	SAS 12Gbps RAID 4GB Flash Backed Cache
		16gb FC HBA	16gb FC HBA	16gb FC HBA
Network	6x 1Gbps	2x 40Gbps (Both Ethernet & FCoE)	2x 40Gbps (Both Ethernet & FCoE)	2x 40Gbps (Both Ethernet & FCoE)

Commvault Configuration Details

The configuration details listed in this section are based on a multi-site deployment with a MediaAgent in each of two sites. For single-site deployments, ignore any elements related to mediaagent-2.

Server Roles and Architectures

Table 4 lists the sites, names, roles and reference architectures for the Cisco UCS C240 and Cisco UCS S3260 servers.

Table 4 Server Roles and Architecture

Site	Role	Reference Architecture	Hostname
prod	CommServe	Data Center UCS C240	commserve-1
prod	MediaAgent	Medium UCS S3260	mediaagent-1
dr	MediaAgent	Medium UCS S3260	mediaagent-2

Storage Pool Information

Table 5 lists the storage pool configurations.

Table 5 Storage Pool Configuration

MediaAgent	Library Name	Library Mount Path	Deduplication DB path
mediaagent-1	gdsp_prod_01	L:\dl_prod_01	D:\gdsp_prod_01\
mediaagent-2	gdsp_dr_01	L:\dl_dr_01_01	D:\gdsp_dr_01\

Policy Information

Table 6 is an example of a service level agreement. Policies have been defined within Commvault software to meet these criteria.

Table 6 Serve Level Agreement Details

Tier	RPO	Onsite Retention	Offsite Retention	RTO
Gold	8 hours	30 days	30 days	1 hour
Silver	24 hours	30 days	30 days	4 hours
Bronze	24 hours	30 days	30 days	Best Effort

Storage Policy Details

Table 7 details the storage policies created to meet the SLAs.

Table 7 Storage Policy Details

Storage Policy	SLA Tier	Storage Policy Copy Copy Type	Copy Type	Retention
plan_gold_vm_01	Gold	1_snap_primary Snap Primary	Snap Primary	7 day / 0 cycles
		2_primary Primary	Primary	30 days/1 cycle
		3_dr_copy Synchronous	Synchronous	30 days/1 cycle
plan_silver_vm_01	Silver	1_snap_primary Snap Primary	Snap Primary	1 days / 0 cycles
		2_Primary Primary	Primary	30 days/1 cycle
		3_dr copy Synchronous	Synchronous	30 days/1 cycles
plan_bronze_vm_01	Bronze	1_primary Primary	Primary	30 days/1 cycle
		2_dr copy Synchronous	Synchronous	30 days/4 cycles

Schedule Policy Details

Table 8 details the schedule policies created to meet the defined SLAs.

Table 8 Schedule Policy Details

Schedule Policy Name	Type	Agent Types	Occurrence	Time	Additional Options
vsa_gold	Incremental	All Agents	Daily	00:00:00	Run backup copy

Schedule Policy Name	Type	Agent Types	Occurrence	Time	Additional Options
				Repeat every 8 hours	Indexing for granular recovery on backup copy
	Full		Monthly	Last Saturday at 20:00:00	Run backup copy Indexing for granular recovery on backup copy
	Synthetic Full		Weekly	Friday 20:00:00	
vsa_silver	Incremental	All Agents	Daily	00:00:00	Run backup copy Indexing for granular recovery on backup copy
	Full		Monthly	Last Saturday at 20:00:00	Run backup copy Indexing for granular recovery on backup copy
	Synthetic Full		Weekly	Friday 20:00:00	
vsa_bronze	Incremental	All Agents	Daily	00:00:00	
	Full		Monthly	Last Saturday at 20:00:00	
	Synthetic Full		Weekly	Friday 20:00:00	

Auxiliary copy from the primary site to the secondary site uses automated scheduling, enabled by default, and does not require a schedule policy.

Hypervisor Information

Table 9 details the hypervisor details from the virtualization clients.

Table 9 Hypervisor Information

Site	Hypervisor	Hostname	VSA Proxy	ESXi Proxy
Prod	VMware	vc.earthquakes.cisco.com	mediaagent-1	10.1.164.27
DR	VMware	vc-branch.earthquakes.cisco.com	mediaagent-2	10.2.164.21

Subclient Information

Table 10 details key information for the virtualization subclients on virtualization client vc.earthquakes.cisco.com. There are no VMs running in the DR site, so no subclients are configured on vc-branch.earthquakes.cisco.com.

Table 10 Virtualization Subclient

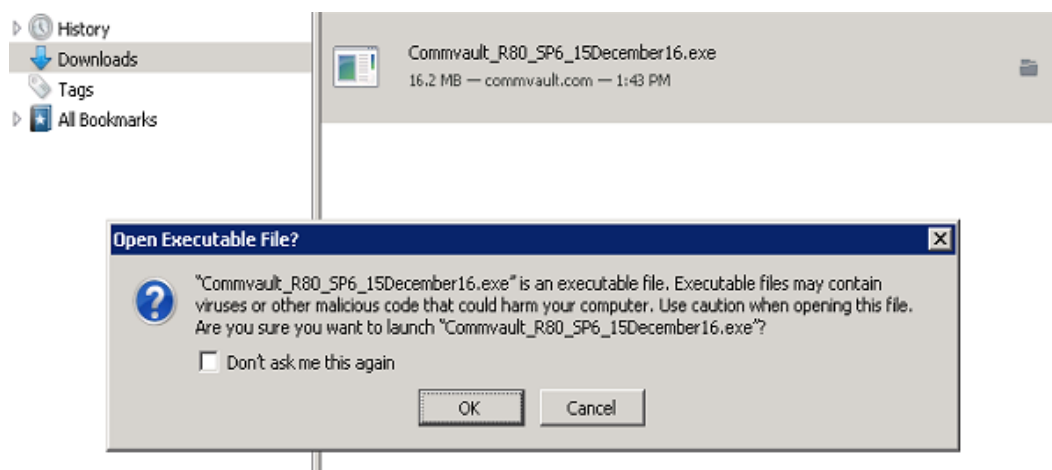
Backup Set	Subclient Name	Content	Storage Policy	Schedule Policy
defaultBackup Set	ds_gold	Datastore: tier_gold	plan_prod_01_vm_gold	plan_prod_01_vm_gold
defaultBackup Set	ds_silver	Datastore: tier_silver	plan_prod_01_vm_silver	plan_prod_01_vm_silver
defaultBackup Set	ds_bronze	Datastore: tier_bronze	plan_prod_01_vm_bronze	plan_prod_01_vm_bronze

Commvault Software Offline Installation

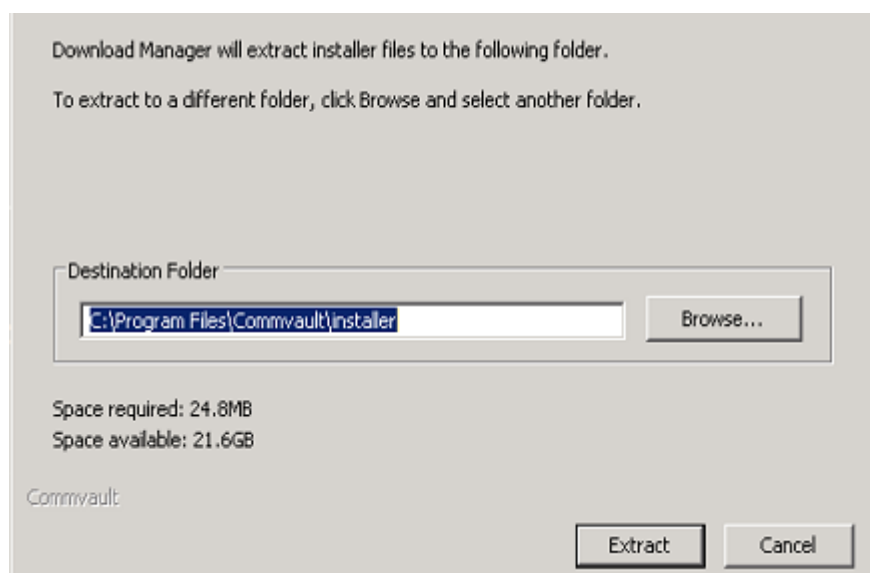
If the CommServe does not have an Internet connection, Commvault software must be downloaded and made available to the CommServe. The Commvault software installer includes an option to download packages rather than install locally. This section details the download process.

To install Commvault software, complete the following steps:

1. Download and execute the latest version of the Commvault Download Manager from cloud.commvault.com. The exact filename may differ from the image based on the latest service pack release.



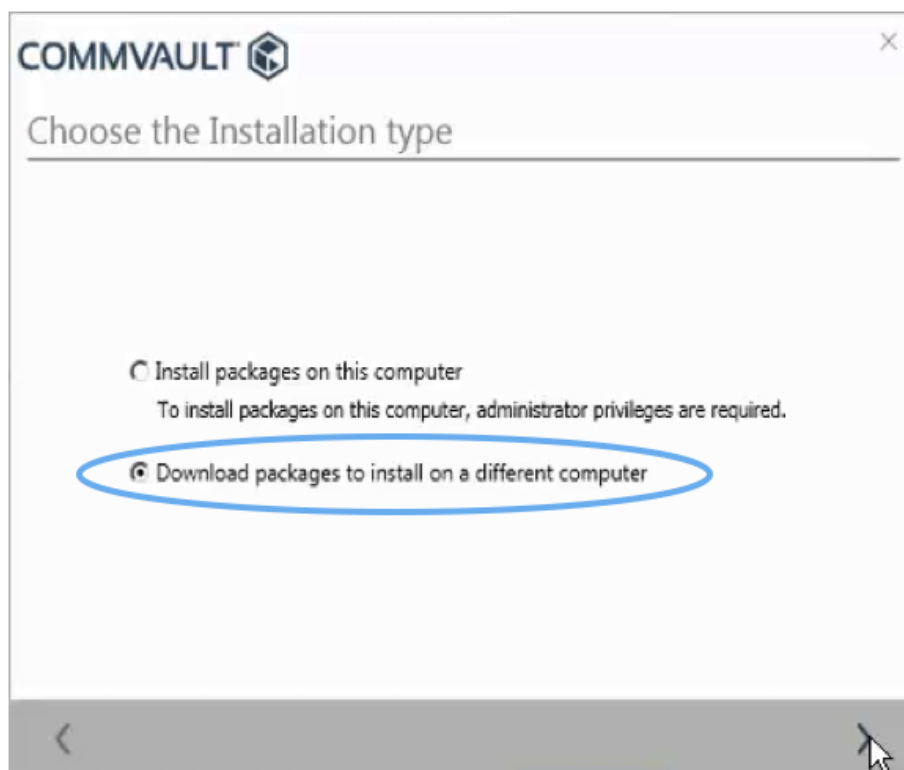
2. Enter or browse to a folder to extract the installer to, or accept the default. This is not the location where the full software download will occur.



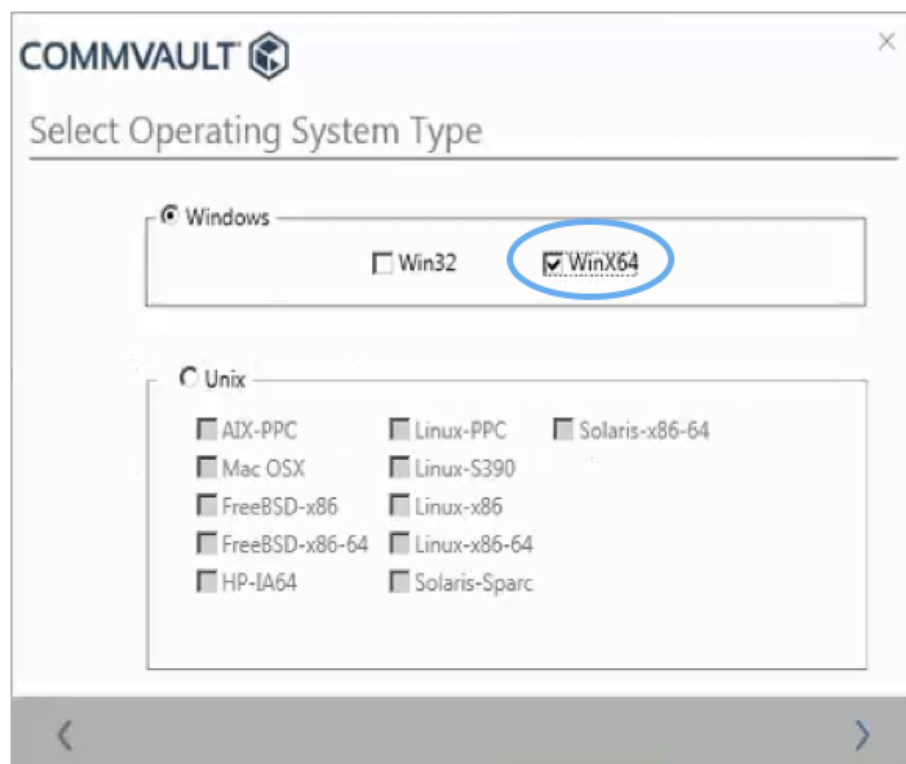
3. Accept the license agreement. Click the right arrow button to continue to the next screen.



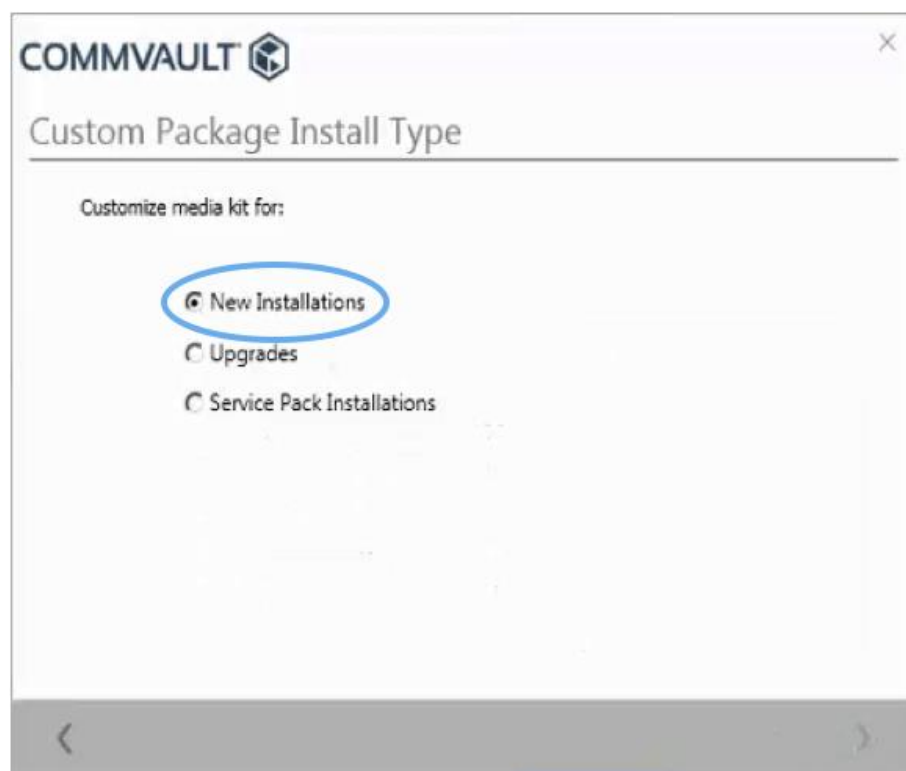
4. Select the option to download packages, then continue to the next screen.



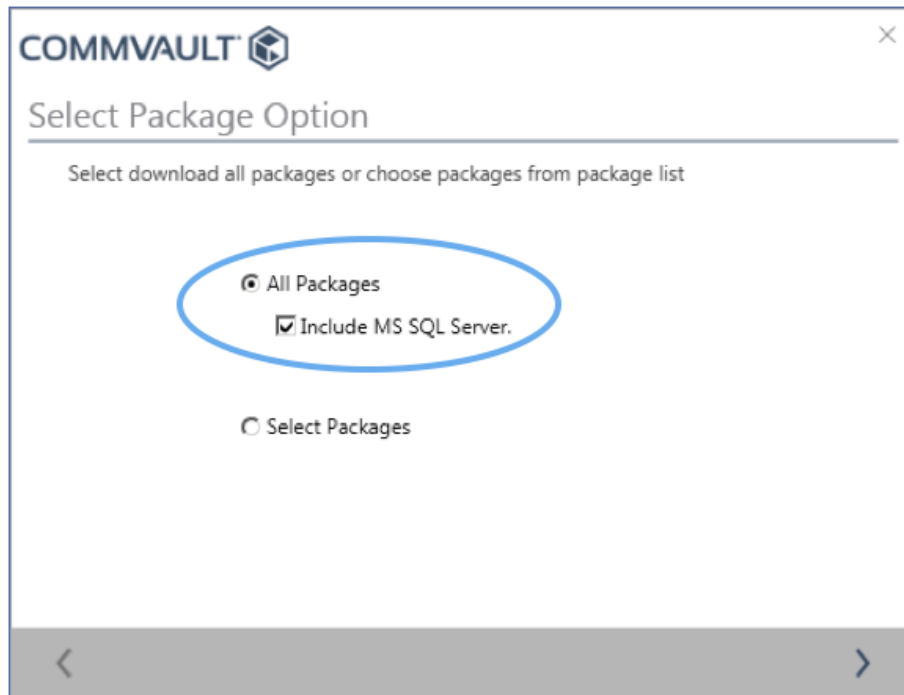
5. Select the platforms to download, then continue to the next screen. Only WinX64 is required for VSI protection.



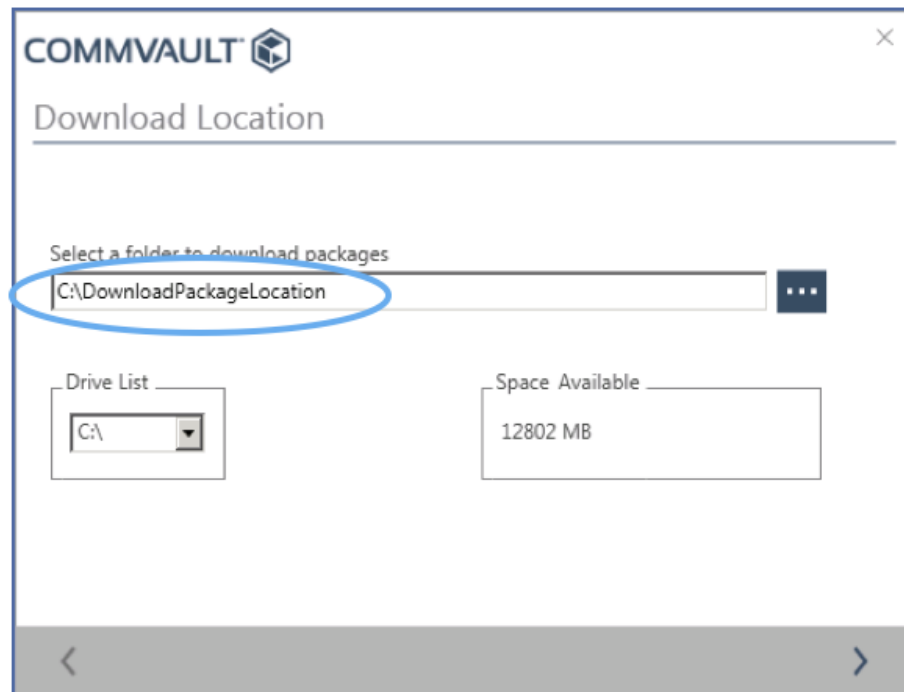
6. Select the option to customize the media kit for new installations and continue to the next screen.



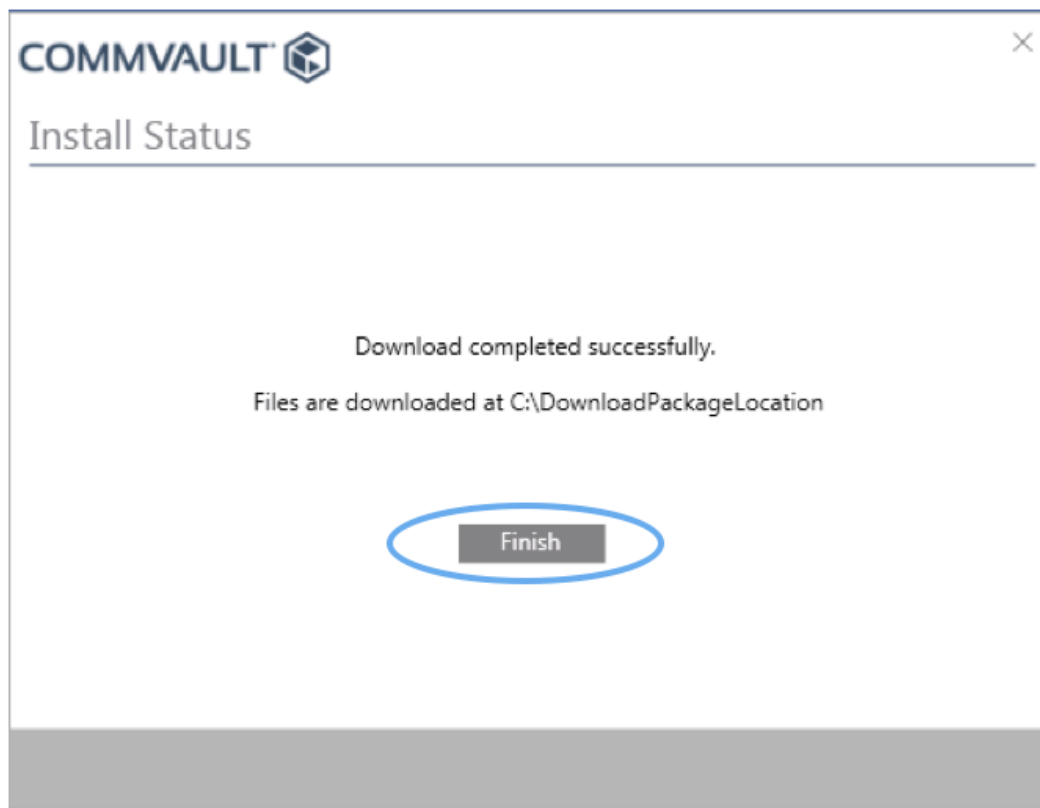
7. Select the option to download all packages, including MS SQL Server. Continue to the next screen.



8. Select a location to download the installation packages. To use a network location, map a network drive first. Continue to the next screen.



9. The installer will download packages to the specified location and display a completion screen when finished. Click Finish to exit the installer.



The downloaded packages may now be used to install the CommServe without an Internet connection.

FlashArray API Token Lookup

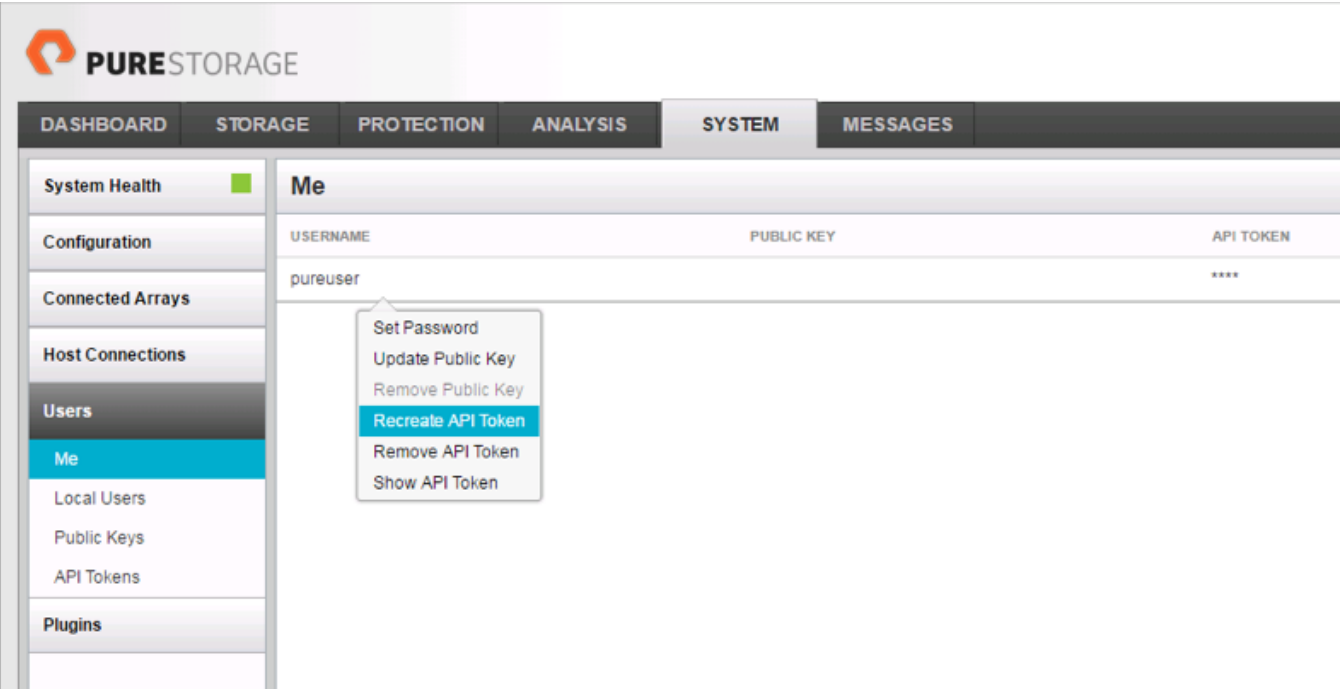
To perform the FlashArray API Token Lookup, complete the following steps:



Determine the proper user account to authorize the FlashArray. The user account must have “storage admin” privileges or higher.

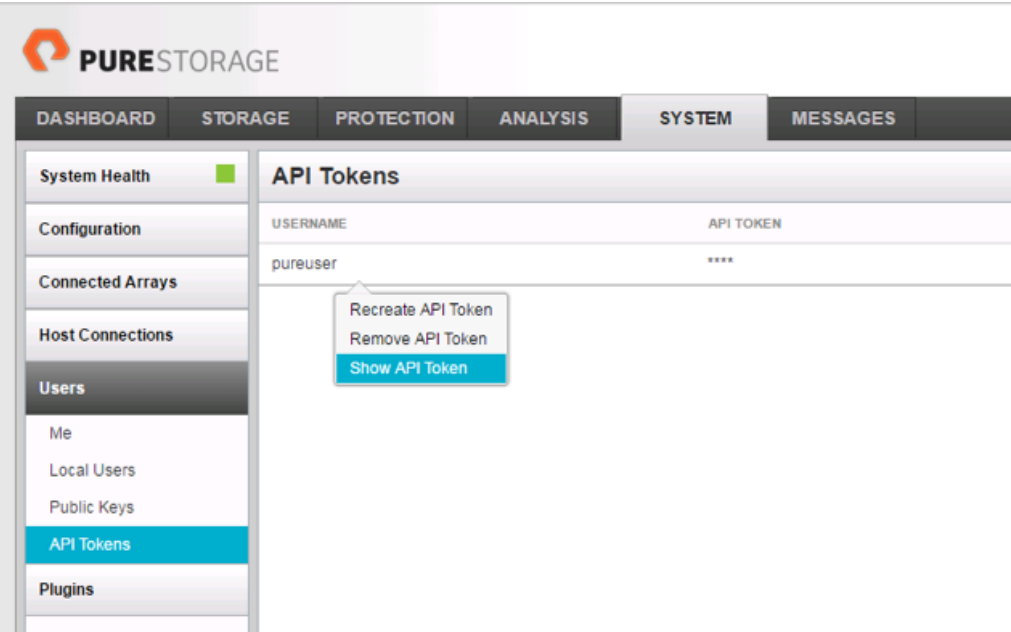
1. To add a FlashArray object into the IntelliSnap software, you must know the username and the API token. If an API token for the user account does not exist, it must be created. The token can be created by logging into the FlashArray GUI with the target account and then navigating to the System tab then Users > Me.
2. Hover **to the right of the username with your mouse and select “Create API Token”** from the menu drop-down (shown as Recreate API Token in the below screenshot as the token exists).

Figure 15 Create API Token



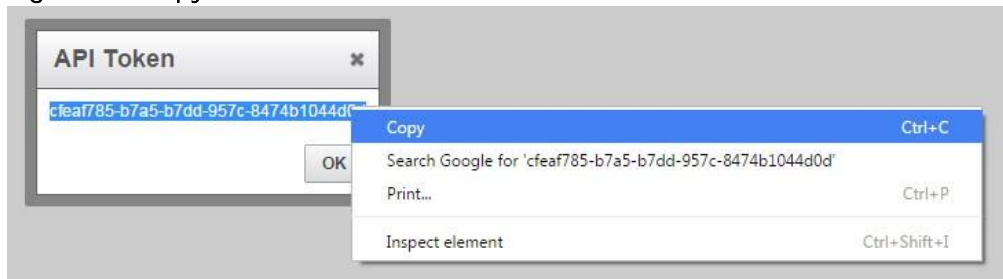
- 3. With the token created, select the pulldown of the user from within the Users sub-menu of the System tab, or from within the API Tokens listing as shown below, and pick the Show API Token:

Figure 16 Obtain API Token



- 4. Copy the token to your clipboard.

Figure 17 Copy API Token



Live Sync

The Live Sync feature enables you to use backup data to create and maintain a warm disaster recovery site for virtual machines (VMs) running critical business applications. Live Sync provides software-based replication for source VMs. By using backup data and performing replication using backup infrastructure, you can minimize the impact on production systems.

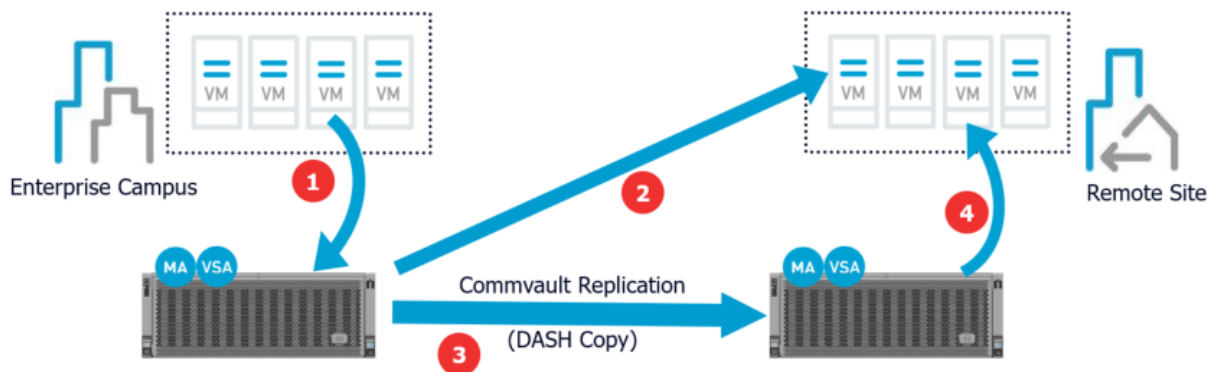
Live Sync uses a full or synthetic full backup to create each destination VM and updates destination VMs from subsequent incremental backups of the source VMs. You can configure Live Sync schedules to create multiple Live Sync jobs for each schedule, with each job using its own stream for a subset of virtual machines; this approach dramatically reduces the amount of time required to replicate large numbers of virtual machines.

The recovery time objective (RTO), the time interval between a service interruption and the restoration of services from the recovery site, is the time needed to power on the virtual machines at the recovery site. Automated validation and the ability to specify new network connections and IP addresses at the recovery site ensure that startup time is minimized.

Because Live Sync is based on backups the recovery point objective (RPO), the acceptable time interval within which virtual machine data must be recoverable, is determined by the frequency of backups. In the event of corrupted data in source VMs, you can recover source VMs from any stable recovery point that is available in backup history, and then use Live Sync to resync VMs from the recovered source VM.

In the event of a disaster, you can power on the destination virtual machines for minimal disruption of vital business applications.

Live Sync provides quick recovery capability for critical applications running on virtual machines. And as always, Commvault data protection enables recovery of less critical virtual machines from backups as needed.



1 VSA Protection Operation is run against VMs to be replicated: This will be a low impact incremental backup.

2 After Protection Operation is Complete Changed Blocks are Shipped to Standby VMs: This can be a synchronous or asynchronous operation.

3 OR DASH Copy is Performed to Secondary Site:

4 Then Changed Blocks are Overlaid on Replicated VMs:

About the Authors

Ramesh Isaac, Technical Marketing Engineer, Cisco Systems, Inc.

Ramesh Isaac is a Technical Marketing Engineer in the Cisco UCS Data Center Solutions Group. Ramesh has worked in data center and mixed-use lab settings since 1995. He started in information technology supporting UNIX environments and focused on designing and implementing multi-tenant virtualization solutions in Cisco labs before entering Technical Marketing. Ramesh holds certifications from Cisco, VMware, and Red Hat.

John Pham, Systems Engineer, Commvault Systems, Inc.

John Pham is a Systems Engineer in the Commvault World Wide Alliances Architecture Group. He has over 14 years of experience in architecting and engineering data management and security solutions across the federal, public, and private sectors. John has a deep background in data protection, information security, information life-cycle management, disaster recovery, business continuity, compliance, and hybrid cloud strategies. John holds a Certified Information Systems Security Professional (CISSP), Commvault Solutions Architect (CVSA), and Commvault Certified Master (CVCN) certifications.

Acknowledgements

- Craig Ashapa, Technical Marketing Engineer, Cisco Systems, Inc.
- Ann Rondinone, Product Specialist, Commvault Systems, Inc.