Cisco Integrated System for Microsoft Azure Stack with Commvault

This document provides an introduction to the Commvault® Data Platform deployment on ScaleProtect™ with Cisco UCS® to protect and recover tenant data and applications running on Cisco® Integrated System for Microsoft® Azure Stack.
Contents

Introduction ................................................................................................................................................. 4
Purpose of this document .......................................................................................................................... 5
Document reference .................................................................................................................................. 5
Solution overview ....................................................................................................................................... 5
Technology overview ............................................................................................................................... 7
Cisco Integrated System for Microsoft Azure Stack .................................................................................. 7
Cisco Unified Computing System .......................................................................................................... 9
   Cisco UCS C240 M5 Rack Server ........................................................................................................ 10
   Cisco UCS C220 M5 Rack Server ........................................................................................................ 11
Commvault Data Platform ...................................................................................................................... 12
Commvault protection and recovery for Microsoft Azure Stack .............................................................. 13
Scalability ................................................................................................................................................ 14
   Commvault HyperScale Software ......................................................................................................... 15
Configuration and validation .................................................................................................................... 17
   Physical topology ................................................................................................................................ 17
   Logical topology ................................................................................................................................... 17
Cisco Integrated System for Microsoft Azure Stack configuration ....................................................... 19
Commvault Data Platform configuration ............................................................................................... 19
Configuring CommServe ....................................................................................................................... 20
   Reference architecture ....................................................................................................................... 20
Configuring ScaleProtect with Cisco UCS ............................................................................................ 20
   Reference architecture ....................................................................................................................... 21
Configuring the VSA for Azure Stack ...................................................................................................... 22
   Install the VSA for Azure Stack .......................................................................................................... 23
   Install Azure PowerShell ................................................................................................................... 26
   Configure registry settings on the VSA for Azure Stack .................................................................... 27
   Configure the application and tenant for Azure Stack ....................................................................... 29
   Get the tenant ID from Azure Active Directory .................................................................................. 32
Configure the application or service principal for the tenant subscription.................................................................32
Add a Microsoft Azure Stack client for Azure Active Directory or ADFS .................................................................33
Configure a subclient for Azure Stack virtual machine protection ...........................................................................34
Configure the Azure Blob virtual client ....................................................................................................................35
Configuring Azure Stack protection ........................................................................................................................36
Admin Console overview .................................................................................................................................................36
Data protection plans .......................................................................................................................................................38
Configure a virtualization plan for Azure Stack protection ......................................................................................38
Set up a subclient for Azure Stack virtual machine protection ..................................................................................41
Manually back up a virtual machine ...........................................................................................................................43
Restore a virtual machine ..............................................................................................................................................44
Conclusion .................................................................................................................................................................47
For more information................................................................................................................................................47
**Introduction**

Enterprise IT is being transformed with the maturing of cloud providers that offer computing, storage, and application services with exceptional elasticity, scale, resiliency, and availability on a consumption-based economic model. However, the choice between public cloud and on-premises infrastructure is not a binary one. As some workloads shift to the cloud, enterprises are also seeking to transform their internal data centers and services into offerings that provide cloud-like scale, flexibility, resiliency, and operational methods, with similar positive economic outcomes. To this end, architects are augmenting or replacing traditional, proprietary, and single-purpose IT infrastructure and applications with software-defined services, distributed processing, big data applications, and hyperconverged architectures.

The Cisco® Integrated System for Microsoft® Azure Stack enables your organization to access development tools, data repositories, and related Azure services to reinvent your applications and gain new information from your secured data. Azure Stack provides the same APIs and user interface as the Azure public cloud. An integrated system enables your team to save time building cloud-enabled applications, even when disconnected from Azure, and manage customer data while adhering to regulations on data location and accessibility. Cisco’s infrastructure builds on the key automation benefits of the Cisco Unified Computing System™ (Cisco UCS®) with leading Cisco Nexus® networking and data security technology, while helping ensure the highest performing design to meet your future hybrid cloud growth requirements. Azure Stack opens the door to new hybrid cloud possibilities. When you use the Cisco Integrated System for Microsoft Azure Stack, you gain high-performance networking and industry-leading versatility for virtualized environments with Cisco Unified Fabric. You also automate infrastructure management with Cisco UCS Manager and help ensure consistency with policy-based management.

Data protection is an essential component of business continuity and helps protect an organization from human error, data corruption, ransomware, etc. Figure 1 shows the data protection responsibilities of an Azure Stack environment.

**Figure 1. Azure Stack data protection responsibilities**

<table>
<thead>
<tr>
<th>Data protection responsibilities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Human error</td>
<td>• Hardware failure</td>
</tr>
<tr>
<td>• Programmatic errors</td>
<td>• Software failure</td>
</tr>
<tr>
<td>• Malicious insiders</td>
<td></td>
</tr>
<tr>
<td>• External hackers</td>
<td></td>
</tr>
<tr>
<td>• Viruses and malware</td>
<td></td>
</tr>
<tr>
<td>• Natural disasters</td>
<td></td>
</tr>
<tr>
<td>• Power outages</td>
<td></td>
</tr>
</tbody>
</table>

Customer \ Microsoft and original equipment manufacturer (OEM) hardware vendor
Data protection—no matter where your data lives—is a real concern, including in Microsoft Azure Stack. Microsoft supports the Azure Stack software and Cisco supports the hardware components, but it is up to you to protect your data in Azure Stack. The Commvault Data Platform and Cisco provide a comprehensive data management solution for protection and recovery of Azure Stack virtual machines, applications, databases, and Blob storage. Transforming mission-critical applications and workloads can be difficult and disruptive, but transforming secondary infrastructure is less risky. By some estimates, 50 to 70 percent of infrastructure capacity is used for secondary workloads and storage. Cisco enables this shift in secondary storage and workloads, supporting cloud-like economics and critical services using secondary data and extending these services into Microsoft Azure Stack. ScaleProtect™ with Cisco UCS® is a powerful, unique scale-out data protection solution combining Commvault data protection including Commvault HyperScale™ Software with Cisco UCS. ScaleProtect with Cisco UCS provides enterprises with a single, integrated solution that delivers infrastructure simplicity, elasticity, resiliency, flexibility, and scale for managing primary and secondary data, while replacing traditional backup tools with a modern cloud-enabled data management solution.

**Purpose of this document**

This document describes the reference architecture and use cases for tenant data protection on the Cisco Integrated System for Microsoft Azure Stack with ScaleProtect with Cisco UCS on Cisco UCS C240 M5 Rack Servers. It provides an overview of Commvault Data Platform technical capabilities, best practices, and validation for data protection of tenants in a Cisco Integrated System for Microsoft Azure Stack environment.

**Document reference**

Please refer to [Cisco Integrated System for Microsoft Azure Stack Solution Overview](#) for details for Cisco Integrated System for Microsoft Azure Stack. This document builds on this design and incorporates the Commvault data protection solution for systems and applications running on Cisco Integrated System for Microsoft Azure Stack together with Commvault.

The configuration guidelines and best practices documented here serve as a reference for implementation of backup and recovery on the Cisco Integrated System for Microsoft Azure Stack. Please refer to the Cisco white paper [ScaleProtect with Cisco UCS S3260 Storage Server](#) published in January 2018 for a more comprehensive understanding of ScaleProtect with Cisco UCS.

**Solution overview**

Azure Stack is Microsoft’s hybrid cloud solution for on-premises data centers. Azure Stack provides an organization with three core benefits: Azure services on the premises, a consistent application development environment, and a predictable delivery experience. This solution provides modern data protection, recovery, and replication of systems and applications hosted on the Cisco Integrated System for Microsoft Azure Stack through the Commvault Data Platform. ScaleProtect with Cisco UCS on Cisco UCS C240 M5 large-form-factor (LFF) servers enables this shift for secondary storage and workloads, supporting cloud-like economics and critical services using secondary data and extending these services into the public cloud. ScaleProtect with Cisco UCS delivers web-scale data services for data protection using industry-standard x86 servers while providing best-in-class data management. By combining Cisco UCS servers with industry-leading Commvault HyperScale™ Software, customers gain exceptional scale-out flexibility and agility with uncompromised data management, all with cloud-like economics and true hybrid cloud capabilities. Cisco UCS revolutionized the server market through its programmable fabric and automated management that simplify application and service deployment. Figure 2 provides an overview of the solution.
ScaleProtect with Cisco UCS provides a full suite of data services for protecting, indexing, securing, automating, reporting, and natively accessing data. In addition, ScaleProtect with Cisco UCS provides insight into the data, thereby creating the value that business demands.

The deployment scenarios detailed in this document enable the protection and recovery of tenant resource data on the Cisco Integrated System on Microsoft Azure Stack with ScaleProtect with Cisco UCS through the Commvault Data Platform. Commvault’s components are hosted on Cisco UCS C-Series Rack Servers and S-Series Storage Servers using the predefined reference architectures. The Commvault Data Platform can be extended across heterogeneous data center environments comprising converged traditional and cloud infrastructures.

The main data protection and recovery use cases are as follows:

- **Protection in Microsoft Azure Stack**: Commvault provides operational recovery for active workloads and data within Microsoft Azure Stack, including the Cisco Integrated System for Microsoft Azure Stack. Commvault can provide agentless instance protection, DASH Copy data to another Azure Stack region or to an on-premise system, and protection for Blob storage in Microsoft Azure Stack.

- **Migration to Microsoft Azure Stack**: Commvault orchestrates the migration of application workloads across Azure Stack instances, either at the virtual machine container level or the application level, while providing protection during the migration lifecycle while workloads are in a transition phase between an on-premises system and Azure Stack or between an Azure Stack scale unit and a destination Azure Stack scale unit.

- **Disaster recovery to Microsoft Azure Stack**: Commvault Data Platform can automate the creation and replication of virtual machine replicas from a source Azure Stack scale unit to a destination Azure Stack for warm recovery.
For application and data consistency, database plug-ins or Intelligent Data Agents (iDAs) can be deployed within virtual machines to provide integrated application and database recovery as required.

Commvault offers the following advantages with benefits for protecting Azure Stack virtual machines:

- Native Azure Stack API integration to protect an Azure Stack virtual machine
- Full virtual machine restoration of an Azure Stack virtual machine
- Recovery of specific files and folders in a virtual machine
- Migration from on-premises hypervisors to Azure Stack
- Disaster recovery (warm) with live synchronization (using the Live Sync feature) to an Azure Stack virtual machine

To back up virtual machines using virtual machine disk snapshots, Commvault software does not require access to the Azure Stack hypervisor. Instead, it uses representational state transfer (REST) APIs to create snapshots of each block volume. Every snapshot is then mapped to a nominated proxy virtual machine (Commvault Virtual Server Agent [VSA] for Azure Stack) to perform deduplication before writing to ScaleProtect with Cisco UCS on Cisco UCS servers or the public Azure cloud.

**Technology overview**

This section introduces the technologies used in the solution described in this document.

**Cisco Integrated System for Microsoft Azure Stack**

The Cisco Integrated System for Microsoft Azure Stack enables your organization to access the development tools, data repositories, and related Azure services to reinvent your applications and gain new information from your secured data (Figure 3). Azure Stack provides the same APIs and user interface as the Azure public cloud. This integrated system enables your team to save time building cloud-enabled applications, even when disconnected from Azure, and manage customer data while adhering to regulations about data location and accessibility. Cisco’s infrastructure builds on the key automation benefits of the Cisco UCS with leading Cisco Nexus networking and data security technology, while helping ensure that you deploy the highest performing design to meet your future hybrid cloud growth requirements.

This solution offers the following benefits:

- Design by Cisco: All major system components are designed, developed, and manufactured by Cisco, which simplifies system management, enables single-source support, and helps you avoid unforeseen product roadmap issues.
- Leading system performance: The latest Intel® Xeon® Scalable processors, up to 1536 GB of memory per server, Non-Volatile Memory Express (NVMe) standard storage cache, and optional solid-state disk (SSD) drives are part of the package.
- Capability to maintain your data center standards for system racks and networking: Maintain your IT organization’s data center standards for Cisco Nexus switching and system racks by installing all system components in your racks and using your networking team’s existing expertise.
- Freedom to choose: Purchase Azure services from any vendor.
- Proven tools: Cisco UCS Central Software enables easy management of multiple locations or regions from a single screen on your desktop.
The Cisco solution starts with rack-optimized Cisco UCS C240 M5 Rack Servers. These models house two Intel Xeon processors, up to 1.5 terabytes (TB) of memory, and up to 96 TB of storage. You can select from several different processors, provided that each server is configured with exactly the same processors, memory, and storage. The servers drive the Azure Stack software and house all the virtual machines and data.

Each server is connected to two third-generation fabric interconnects, avoiding any single point of failure. Cisco UCS Manager resides on the Cisco UCS fabric interconnects. These fabric interconnects are connected to two Cisco Nexus 9000 Series Switches to enable connectivity to the data center’s border switches. Each switch and fabric interconnect maintains a copy of the other’s configuration to help enable easy replacement should replacement be required. Each server is configured with NVMe cache storage and 40 Gigabit Ethernet, which is managed by a Cisco Nexus 2000 Series Fabric Extender (FEX). The unified fabric that connects the system enables 40 Gigabit Ethernet traffic, which is an important benefit as the system configuration grows over time to a multiscale unit (cluster) configuration, and the customer may choose to back up multiple scale units simultaneously.

Azure Stack installation services managed by Cisco Advanced Services are included (typical installation takes only three days). Cisco can configure any node increment from four up to the limit supported by Azure Stack.

Cisco Solutions Support is also included. Solutions Support is the highest level of Cisco support and provides up to 24 x 7 x 4-hour onsite repair. In addition, your support calls are automatically routed to a team specially trained on Azure Stack. This team can also
move a support call to the Microsoft Case Exchange system to enable Microsoft support to engage as needed. This way, human error in reentering call details is avoided. The call flow works in reverse should you choose to contact Microsoft support initially.

For additional information about the Cisco Integrated System for Azure Stack, see [https://www.cisco.com/go/microsoft-azure-stack](https://www.cisco.com/go/microsoft-azure-stack).

**Cisco Unified Computing System**

Cisco brings 30 years of broad experience, leadership, and vision to guide businesses through networking and infrastructure challenges. Cisco UCS continues Cisco's long history of innovation in providing integrated systems that deliver business results. Cisco UCS Integrated Infrastructure solutions accelerate IT operations today and create the modern technology foundation needed for the critical business initiatives of tomorrow.

Cisco UCS is a next-generation data center platform that unites computing, networking, and storage access. The platform, optimized for virtual environments, is designed using open industry-standard technologies and aims to reduce total cost of ownership (TCO) and increase business agility. The system integrates a low-latency, lossless 10 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. It is an integrated, scalable, multichassis platform in which all resources participate in a unified management domain.

The main components of Cisco UCS are as follows:

- **Computing**: The system is based on an entirely new class of computing system that incorporates rack-mount and blade servers based on Intel Xeon processors.
- **Network**: The system is integrated onto a low-latency, lossless, 10-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks, which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables and by decreasing the power and cooling requirements.
- **Virtualization**: The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage access**: The system provides consolidated access to both SAN storage and network-attached storage (NAS) over the unified fabric. By unifying storage access, Cisco UCS can access storage over Ethernet, Fibre Channel, Fibre Channel over Ethernet (FCoE), and Small Computer System Interface over IP (iSCSI). This approach provides customers with choice of storage access and investment protection. In addition, server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity and management for increased productivity.
- **Management**: The system uniquely integrates all system components, which enables the entire solution to be managed as a single entity by Cisco UCS Manager. Cisco UCS Manager has an intuitive GUI, a command-line interface (CLI), and a robust API to manage all system configuration and operations.

Cisco UCS is designed to deliver:

- Reduced TCO and increased business agility
- Increased IT staff productivity through just-in-time provisioning and mobility support
- A cohesive, integrated system that unifies the technology in the data center and is managed, serviced, and tested as a whole
- Scalability through a design for hundreds of discrete servers and thousands of virtual machines and the capability to scale I/O bandwidth to match demand
- Industry standards supported by a partner ecosystem of industry leaders
The Cisco UCS product family (Figure 4) consists of the following components:

Note: As Azure Stack evolves over time, these components may be incorporated into future designs.

- **Cisco UCS Manager** provides unified, embedded management of all software and hardware components in the Cisco Unified Computing System.
- **Cisco UCS 6300 Series Fabric Interconnects** offer several features and benefits that can lower TCO. Some examples include:
  - Bandwidth up to 2.56 Tbps
  - Centralized unified management with Cisco UCS Manager software
  - High-performance ports capable of line-rate, low-latency, lossless 10 and 40 Gigabit Ethernet (varies by model) and FCoE and 4-, 8-, and 16-Gbps Fibre Channel
- **Cisco UCS 5100 Series Blade Server Chassis** supports up to eight blade servers and up to two fabric extenders in a 6-rack-unit (6RU) enclosure.
- **Cisco UCS B-Series Blade Servers** are Intel-based blade servers that increase performance, efficiency, versatility, and productivity.
- **Cisco UCS C-Series Rack Servers** deliver unified computing in an industry-standard form factor to reduce TCO and increase agility.
- **Cisco UCS S-Series Storage Servers** deliver unified computing in an industry-standard form factor to address data-intensive workloads with reduced TCO and increased agility.
- **Cisco UCS adapters** with wire-once architecture offer a range of options to converge the fabric, optimize virtualization, and simplify management.

**Cisco UCS C240 M5 Rack Server**

The Cisco UCS C240 M5 Rack Server (Figure 5) is a 2-socket, 2RU rack server offering industry-leading performance and expandability. It supports a wide range of storage and I/O-intensive infrastructure workloads, including big data and analytics, data protection, and collaboration workloads. Cisco UCS C-Series Rack Servers can be deployed as standalone servers or as part of a Cisco UCS managed environment to take advantage of Cisco’s standards-based unified computing innovations that help reduce customers’ TCO and increase business agility.
In response to ever-increasing computing and data-intensive real-time workloads, the enterprise-class Cisco UCS C240 M5 server extends the capabilities of the Cisco UCS portfolio in a 2RU form factor. It incorporates the Intel Xeon Scalable processors, supporting up to 20 percent more cores per socket, twice the memory capacity, and five times more NVMe PCI Express (PCIe) SSDs than the previous generation of servers. These improvements deliver significant performance and efficiency gains that will improve your application performance. The C240 M5 delivers outstanding levels of storage expandability and exceptional performance, with:

- The latest Intel Xeon Scalable CPUs, with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Intel 3D XPoint-ready support, with built-in support for next-generation nonvolatile memory technology
- Up to 26 hot-swappable small-form-factor (SFF) 2.5-inch drives, including 2 rear hot-swappable SFF drives (up to 10 support NVMe PCIe SSDs on the NVMe-optimized chassis version), or 12 large-form-factor (LFF) 3.5-inch drives plus 2 rear hot-swappable SFF drives
- Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- Modular LAN-on-motherboard (mLOM) slot that can be used to install a Cisco UCS virtual interface card (VIC) without consuming a PCIe slot, supporting dual 10- or 40-Gbps network connectivity
- Dual embedded Intel x550 10GBASE-T LAN-on-motherboard (LOM) ports
- Modular M.2 or Secure Digital (SD) cards that can be used for boot

Cisco UCS C220 M5 Rack Server

The Cisco UCS C220 M5 Rack Server (Figure 6) is among the most versatile general-purpose enterprise infrastructure and application servers in the industry. It is a high-density 2-socket rack server that delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications. The Cisco UCS C-Series Rack Servers can be deployed as standalone servers or as part of Cisco UCS to take advantage of Cisco’s standards-based unified computing innovations that help reduce customers’ TCO and increase their business agility.

The Cisco UCS C220 M5 server extends the capabilities of the Cisco UCS portfolio in a 1RU form factor. It incorporates the Intel Xeon Scalable processors, supporting up to 20 percent more cores per socket, twice the memory capacity, 20 percent greater storage density, and five times more PCIe NVMe SSDs than the previous generation of servers. These improvements deliver significant performance and efficiency gains that will improve your application performance. The C220 M5 delivers outstanding levels of expandability and performance in a compact package, with:

- The latest Intel Xeon Scalable CPUs, with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Up to 10 SFF 2.5-inch drives or 4 LFF 3.5-inch drives (77 TB storage capacity with all NVMe PCIe SSDs)
- Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- mLOM slot that can be used to install a Cisco UCS VIC without consuming a PCIe slot
- Dual embedded Intel x550 10GBASE-T LOM ports

In the present solution for the Cisco Integrated System for Azure Stack with Commvault, the CommServe® and VSA proxy for Azure Stack are deployed on the Cisco UCS C220 M5 Rack Server.

**Commvault Data Platform**

The Commvault Data Platform is a single platform for automated global protection, retention, and recovery. Commvault enterprise data protection and recovery software automates global data protection, accelerates recovery, reduces costs, and simplifies operations. Commvault integrates application awareness with hardware snapshots, indexing, global deduplication, replication, search, and reporting. The Commvault Data Platform converges all the needs of a modern data management solution into one place to seamlessly integrate protection, management, and access in one solution.

A comprehensive data protection and management strategy offers smooth and efficient backup, archiving, storage, and recovery of data in your enterprise from any operating system, database, and application. To protect and manage data in your environment, the Commvault software must be distributed to systems that you want to protect. CommServe, MediaAgent, and protected systems constitute a CommCell® environment, and each protected system is referred to as a client (Figure 7).

**Figure 7. Commvault Data Platform overview**

The CommServe server is the command and control center of the CommCell architecture. It coordinates and performs all CommCell operations, maintaining Microsoft SQL Server databases that contain all configuration, security, and operational history for the CommCell environment. A CommCell environment can contain only one CommServe host. The CommServe software can be installed in physical, virtual, and clustered environments.
MediaAgent is the data transmission manager. It provides high-performance data movement and manages the data storage pools. When installed on a client system, it also manages Commvault IntelliSnap® snapshot integration with the underlying storage.

A client is any system within a CommCell environment to be protected. Intelligent Data Agents, or iDAs, are software modules that are installed on computers to access and protect data. The backup and recovery system uses agents to interface with file systems, applications, and databases to facilitate the protection of data on production systems. By default, a file system iDA module is installed when the Commvault software is added to a system. If the client hosts specific applications or databases, additional iDAs are required.

These three Commvault components combined offer the most comprehensive and flexible data protection solution on the market today. The Commvault Data Platform is designed as an orchestrated, hardware- and cloud-independent, highly modular, distributed solution that conforms to this new architecture reality, allowing flexible data management solutions to be built to support a highly distributed infrastructure.

Commvault protection and recovery for Microsoft Azure Stack

Commvault provides a comprehensive data management solution for protecting and recovering Azure Stack virtual machines, applications, databases, and Blob storage. Commvault provides two methods for data protection and recovery of Azure Stack tenant data: the Virtual Server Agent (VSA) for Azure Stack, and application and database plug-ins. The VSA for Azure Stack provides agentless backup and recovery of Azure Stack virtual machines. Application and database iDAs can be deployed within virtual machines to provide integrated application and database recovery as required.

The following approaches support multiple use cases for Microsoft Azure Stack:

- Agentless virtual machine protection and Azure Blob storage (native Azure Stack integration)
- Snapshot support for Azure Stack
- Agent-in-guest protection
- Application and virtual machine migration
- Disaster recovery for Azure Stack using Live Sync

Figure 8 summarizes the data protection capabilities for Microsoft Azure Stack tenant data with Commvault.

**Figure 8.** High-level overview of Microsoft Azure Stack protection
• **Agentless virtual machine and Blob storage protection:** the VSA for Azure Stack delivers an agentless, block-level capture of Azure Stack virtual machine instances and their attached block volumes. The VSA for Azure Stack uses Azure Stack’s APIs and provides a simplified data protection approach to quickly and easily protect and recover Azure Stack virtual machines, including the OS and data disks, and network configuration. In addition, the Commvault Cloud Apps plug-in can be deployed to back up and recover underlying Azure Stack Blob storage. Restoration options include full virtual machine, full container, and specific-level file recovery.

• **Snapshot support for Azure Stack:** The VSA for Azure Stack orchestrates Azure Stack snapshots, allowing creation of a crash-consistent point-in-time copy of an Azure Stack disk through virtualization services from the Azure Stack portal. This snapshot management is provided through the IntelliSnap technology framework and enables organizations to quickly back up large numbers of virtual machines, perform multiple backups daily, and recover full instances.

• **Agent-in-guest (streaming):** An agent-in-guest approach can be used to protect a wide variety of operating systems and applications. Agents back up the production workload and use compression and client-side deduplication to reduce network consumption.

• **Application and virtual machine migration:** Commvault® can assist in application migration efforts when shifting from traditional workloads to private and public cloud providers. By leveraging the power of the Commvault Data Platform, workloads can be migrated through a number of methods.
  - **Virtual machine migration:** The VSA can capture virtual machines from VMware based-platforms in an application-consistent method (Microsoft Volume Shadow Copy Service [VSS] call and VMware Tools) to help ensure that a consistent image of the guest, and the applications residing within it, are captured correctly. With this image, the VSA can then restore and convert the virtual machines to Azure or Azure Stack virtual machines directly, and the process can handle single or multiple virtual machines. This process is performed interactively through the CommCell Console, using the Commvault workflow or API calls.
  - **Application out-of-place restore:** All Application iDataAgents support the capability to restore a given source dataset out-of-place to an alternate location. In this method, the data is captured from the source system (physical, or virtual), and then either directly from the source copy or replicated to cloud (DASH Copy), a restore to the destination is submitted.

• **Disaster recovery for Microsoft Azure Stack using Live Sync:** The Live Sync feature enables incremental replication from a streaming backup of an Azure Stack virtual machine to a synced copy of the virtual machine (destination Azure Stack scale unit virtual machine). The Live Sync operation applies incremental changes to the destination virtual machine from the source virtual machine backups since the last sync point. Live Sync replication delivers a warm-recovery disaster recovery strategy and provides a low recovery-point objective (RPO) and recovery-time objective (RTO) for the replicated virtual machines.

**Scalability**

Application environments and their data grow over time, and a data management solution needs to quickly and efficiently adapt to these changes, while maintaining economy of scale. Data growth is fueled by larger virtualized workloads, substantial increases in application sizes and data, and data retention requirements mandated by government policies. These changes affect data protection solutions, because backup operations now need to complete processing within shorter backup windows, and organizations require lower RPOs and RTOs to meet business service-level agreements (SLAs) and backup policies. A data management solution must be able to meet these demanding requirements.

Commvault addresses scalability by providing these constructs:

• **Native Azure Stack and cloud connectivity:** The cloud connector is the native integration within the Commvault MediaAgent module that directly communicates with object storage providers such as Amazon Web Service (AWS) Simple Storage Service (S3), Azure Blob, Azure Stack Blob, Google Cloud Storage, and Oracle Cloud Infrastructure Classic, without requiring translation devices, gateways, hardware appliances, or virtual tape libraries (VTLs).
• Application consistency: Although crash-consistency within a recovery point may be sufficient for a file-based data set or Azure Stack instance, it is not generally appropriate for an application such as Microsoft SQL Server, for which the database instance needs to be quiesced to help ensure that the database is valid at time of backup. Commvault software supports both crash- and application-consistent backups, providing flexibility in your design while assuring instance recoverability.

• Deduplication building blocks: Commvault software maintains a building block approach for protecting data sets, regardless of the origin or type of data. Deduplication building blocks may be grouped together in a grid, providing further deduplication scale, load balancing, and redundancy across all nodes within the grid. The use of client-side deduplication can reduce backup windows and increase scale, freeing bandwidth for both production and backup network traffic.

• Automation: The cloud encourages automation because the infrastructure is programmable. Furthermore, the benefits of having repeatable actions reduces operation overhead, bolsters resilience through the availability of known good configurations, and allows greater scale. Commvault software provides automation through three main capabilities:
  ◦ Programmatic data management: Commvault software provides a robust API that allows automated control over deployment, configuration, backup, and restore activities within the solution.
  ◦ Workload autodetection and autoprotection: The Commvault iDAs—whether the VSA for Azure Stack, the SQL Server iDA, or Oracle Database iDA—provide autodetection capabilities to reduce administrative load. For example, when fresh instances occur, new volumes are attached to a virtual machine, or databases are imported and created in a database instance, Commvault software automatically detects new data sets for inclusion in the next data-protection window, without manual intervention. As a result of this autodetection and autoprotection capability, the backup or cloud administrator does not need to manually update the solution to protect newly created data sets. The result is improved operational excellence and resiliency within your cloud infrastructure and the assurance that new data is protected and recovery points maintained.
  ◦ Self-service access and restore: Commvault’s self-service interfaces empower users to access their data sets through a Web-based interface, allowing security-mapped access to individual files and folders within the protected data set and freeing administrators to work on critical tasks. Commvault’s robust role-based security function provides assurance that self-service users have access to only their data assets, and custom auditory reporting capabilities capture the way that these users access those data assets.

Commvault HyperScale Software

The features and functions provided by Commvault Data Protection with Commvault HyperScale Software, combined with the features and functions provided by Cisco UCS, create a powerful solution for fast backup and fast restore operations that is simple to implement and easy to scale and upgrade: ScaleProtect with Cisco UCS. ScaleProtect with Cisco UCS addresses the data protection needs of modern data centers. Second-tier storage must be able to scale as quickly as the protected data grows, but the traditional silo-based approach has too many limitations to be effective. The Commvault HyperScale Software architecture introduces a modern way to perform second-tier data management by breaking down the silos and reducing the management overhead in second-tier environments (Figure 9).
With the combination of Cisco and Commvault technologies, you can easily scale from tens of terabytes up to multiple petabytes (PBs) of protected data (Figure 10).

For more information about ScaleProtect with Cisco UCS, please refer to ScaleProtect with Cisco UCS on the Cisco UCS C240 M5 Rack Server.
**Configuration and validation**

The following section outlines the configuration and validation of backup and recovery for tenant applications on the Cisco Integrated System for Microsoft Azure Stack with Commvault Data Platform.

**Physical topology**

The backup and restoration of tenant virtual machines hosted on the Cisco Integrated System for Microsoft Azure Stack is managed by the Commvault Data Platform. The Cisco UCS solution that hosts Commvault Data Platform is connected to the same border switch as Azure Stack. This configuration provides 40 Gbps of backup network bandwidth to the Commvault VSA and MediaAgents through the border switch. ScaleProtect with Cisco UCS is hosted on Cisco UCS C240 M5 LFF servers and is used as a scale-out storage target to stream backups from the Cisco Integrated System for Azure Stack. The CommServe and VSA components are hosted on Cisco UCS C220 M5 servers. Figure 11 shows the validation environment for the Cisco Integrated System for Azure Stack with Commvault.

**Figure 11.** Cisco Integrated System for Azure Stack with Commvault validation environment

**Logical topology**

The logical topology shows the required infrastructure for protection of tenant data in the Cisco Integrated Infrastructure for Azure Stack. The flexible architecture of Commvault Data Platform supports multiple protection methods and deployment configurations to protect tenant data within an Azure Stack. The virtual server proxy for Azure Stack can be deployed on an instance within the Azure Stack scale unit or external to the Azure Stack scale unit. Figure 12 depicts the logical topology for protection of the VSA for Azure Stack within the Azure Stack scale unit for agentless protection and recovery of Azure Stack instances and Azure Blob storage containers.
Customers can deploy the Commvault VSA either external to the Azure Stack scale unit or within the Azure Stack environment. Some of the main considerations for deploying the VSA are listed here:

- The border switch (Cisco Nexus 9000 Series) provides 40 Gigabit Ethernet connectivity to the Commvault VSA for backup of tenant virtual machine. Moreover, Cisco’s fully integrated Azure Stack is designed to deliver industry-leading performance by using 40 Gigabit Ethernet across the entire system. This approach provides customers with higher network throughput with lower latency for backup of tenant virtual machines deployed within Azure Stack.

- If you choose to provision the Commvault VSA within Azure Stack, then the VSA running as an Azure Stack virtual machine is charged as an Azure service by Microsoft. This approach also leads to sharing of Azure Stack resources with tenant virtual machines and the Commvault VSA. Azure Stack virtual machine instances (as of May 2018) are also network bound, with expected maximum network bandwidth of 12,000 Mbps. Moreover, to enable greater concurrency of backup operations, you may need to require multiple VSAs to meet SLAs. In addition, this approach requires greater computing and memory resources to optimize network bandwidth for data protection SLAs.

- With Commvault VSA deployed on a Cisco UCS C220 M5 Rack Server outside Azure Stack, you benefit from greater concurrency of backup operations without the need to consume the computing resources of the Azure Stack environment. This approach physically separates the data protection infrastructure from the protected Azure Stack scale unit production resource consumption and dependencies in disaster recovery scenarios.

- If multiple VSAs for Azure are required to meet business requirements, such as resiliency and concurrency requirements, Commvault supports a hybrid approach of managing internal and external VSA for Azure Stack proxy servers for an Azure Stack scale unit.

Figure 13 depicts the validation environment components used for agentless protection and recovery of Azure Stack instances and Blob storage containers.
The following section describes the components and configuration required to protect tenant data hosted on the Cisco Integrated System for Azure Stack.

**Cisco Integrated System for Microsoft Azure Stack configuration**

Cisco Integrated System for Azure Stack was deployed in a 4-node C240 M5 configuration. For more details about configurations and server specifications and deployment guides, please refer to [Cisco Integrated System for Microsoft Azure Stack](#).

**Commvault Data Platform configuration**

The Commvault Installation package was used to set up the CommCell environment for protecting data on the Cisco Integrated System for Microsoft Azure Stack. This package includes software for the Commvault CommServe, Admin Console, MediaAgent, VSA, Cloud Apps, CommCell Console, Web Server, Web Console, File System iDAs, and Workflow Engine and Analytics.
The CommCell environment installation proceeds in the following order:

1. Configure the CommServe server.
2. Configure ScaleProtect with Cisco UCS.
3. Configure the VSA for Azure Stack.

**Configuring CommServe**

As a deployment option, you can virtualize CommServe. For validation, an existing CommCell environment based on the Commvault reference architecture on Cisco UCS was used. The following procedure assumes that the CommServe server has been configured, CommServe software installed and the CommServe Software cache set up for remote deployment.

**Reference architecture**

Cisco and Commvault tested configurations using the Cisco UCS C220 M5 server and CommServe (command and control software). Table 1 summarizes the suggested CommServe configurations for Medium, Large, and Extra Large deployments.

<table>
<thead>
<tr>
<th>Table 1. CommServe configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco UCS rack servers</strong></td>
</tr>
<tr>
<td>CommServe C220 M5 Medium</td>
</tr>
<tr>
<td>C220 M5SX</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
</tr>
<tr>
<td>1 x Intel Xeon processor 4108 (8 cores at 1.8 GHz)</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
</tr>
<tr>
<td>32 GB</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
</tr>
<tr>
<td>4 x 240 GB SSD</td>
</tr>
<tr>
<td><strong>RAID cache</strong></td>
</tr>
<tr>
<td>2 GB</td>
</tr>
<tr>
<td><strong>RAID</strong></td>
</tr>
<tr>
<td>RAID 5 with hot spare for OS and data</td>
</tr>
<tr>
<td><strong>Network</strong></td>
</tr>
<tr>
<td>2 x 10 Gbps or 2x 40 Gbps</td>
</tr>
<tr>
<td><strong>Sizing</strong></td>
</tr>
<tr>
<td>Up to 5000 clients</td>
</tr>
</tbody>
</table>

**Notes:**

For requirements for deploying a virtualized or nonvirtualized CommServe server, please refer to: Hardware Specifications for the CommServe Server.

For more information about installing CommServe software, please refer to Installing the CommServe Software.

**Configuring ScaleProtect with Cisco UCS**

The ScaleProtect with Cisco UCS solution within the existing CommCell environment was used for validation.
Reference architecture

Tables 2 and 3 summarize the individual MediaAgent server configurations available. You can choose a configuration and sizing based on your data protection requirements.

Table 2. ScaleProtect with Cisco UCS server node configurations

<table>
<thead>
<tr>
<th></th>
<th>ScaleProtect with Cisco UCS C240 M5 server node</th>
<th>ScaleProtect with Cisco UCS S3260 single server node</th>
<th>ScaleProtect with Cisco UCS S3260 dual server node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot disks</td>
<td>2 x 960-GB M.2 SSDs</td>
<td>2 x 480-GB SSDs</td>
<td>4 x 480-GB SSDs</td>
</tr>
<tr>
<td>Data disks</td>
<td>12 x 4-TB SAS</td>
<td>24 x 4-TB SAS</td>
<td>48 x 4-TB SAS</td>
</tr>
<tr>
<td></td>
<td>12 x 6-TB SAS</td>
<td>24 x 6-TB SAS</td>
<td>48 x 6-TB SAS</td>
</tr>
<tr>
<td></td>
<td>12 x 8-TB SAS</td>
<td>24 x 8-TB SAS</td>
<td>48 x 8-TB SAS</td>
</tr>
<tr>
<td></td>
<td>12 x 10-TB SAS</td>
<td>24 x 10-TB SAS</td>
<td>48 x 10-TB SAS</td>
</tr>
<tr>
<td></td>
<td>12 x 12-TB SAS</td>
<td>24 x 12-TB SAS</td>
<td>48 x 12-TB SAS</td>
</tr>
<tr>
<td>Flash storage</td>
<td>1 x 3.2-TB NVMe</td>
<td>4 x 1.6-TB SSD</td>
<td>8 x 1.6-TB SSD</td>
</tr>
<tr>
<td>Cisco UCS rack servers</td>
<td>C240 M5 LFF</td>
<td>S3260 M4</td>
<td>S3260 M4</td>
</tr>
<tr>
<td>CPU</td>
<td>2 x Intel Xeon processor 4114 (10 cores, 2.2 GHz, and 85W)</td>
<td>2 x Intel Xeon processor E5-2650 v4 (12 cores, 2.2 GHz, and 105W)</td>
<td>2 x Intel Xeon processor E5-2650 v4 (12 cores, 2.2 GHz, and 105W)</td>
</tr>
<tr>
<td>Memory</td>
<td>256 GB</td>
<td>256 GB</td>
<td>2 x 256 GB</td>
</tr>
<tr>
<td>RAID cache</td>
<td>1 GB</td>
<td></td>
<td>2 x 4 GB</td>
</tr>
<tr>
<td>RAID</td>
<td>RAID 1 for OS and JBOD for SAS</td>
<td>RAID 1 for OS, RAID 5 for SSD, and JBOD for HDD</td>
<td>RAID 1 for OS, RAID 5 for SSD, and JBOD for HDD</td>
</tr>
<tr>
<td>Maximum Fibre Channel ports:</td>
<td>4 x 16 Gbps</td>
<td>None; FCoE through fabric interconnect</td>
<td>None; FCoE through fabric interconnect</td>
</tr>
<tr>
<td>Network ports</td>
<td>2 x 10 Gbps or 2 x 40 Gbps</td>
<td>2 x 40 Gbps</td>
<td>4 x 40 Gbps</td>
</tr>
</tbody>
</table>

Table 3. ScaleProtect with Cisco UCS sizing and node counts

<table>
<thead>
<tr>
<th>Cisco UCS model</th>
<th>HDD size¹</th>
<th>3 nodes usable²</th>
<th>6 nodes usable²</th>
<th>9 nodes usable²</th>
<th>12 nodes usable²</th>
<th>15 nodes usable²</th>
<th>18 nodes usable²</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS C240</td>
<td>4 TB</td>
<td>87 TB</td>
<td>174 TB</td>
<td>261 TB</td>
<td>349 TB</td>
<td>436 TB</td>
<td>523 TB</td>
</tr>
<tr>
<td></td>
<td>6 TB</td>
<td>130 TB</td>
<td>261 TB</td>
<td>392 TB</td>
<td>523 TB</td>
<td>654 TB</td>
<td>785 TB</td>
</tr>
<tr>
<td></td>
<td>8 TB</td>
<td>174 TB</td>
<td>349 TB</td>
<td>523 TB</td>
<td>698 TB</td>
<td>873 TB</td>
<td>1047 TB</td>
</tr>
<tr>
<td></td>
<td>10 TB</td>
<td>218 TB</td>
<td>436 TB</td>
<td>654 TB</td>
<td>873 TB</td>
<td>1091 TB</td>
<td>1309 TB</td>
</tr>
<tr>
<td></td>
<td>12 TB</td>
<td>261 TB</td>
<td>523 TB</td>
<td>785 TB</td>
<td>1047 TB</td>
<td>1309 TB</td>
<td>1571 TB</td>
</tr>
<tr>
<td>Cisco UCS S3260</td>
<td>4 TB</td>
<td>174 TB</td>
<td>349 TB</td>
<td>523 TB</td>
<td>698 TB</td>
<td>873 TB</td>
<td>1047 TB</td>
</tr>
<tr>
<td></td>
<td>6 TB</td>
<td>261 TB</td>
<td>523 TB</td>
<td>785 TB</td>
<td>1047 TB</td>
<td>1309 TB</td>
<td>1571 TB</td>
</tr>
<tr>
<td></td>
<td>8 TB</td>
<td>349 TB</td>
<td>698 TB</td>
<td>1047 TB</td>
<td>1396 TB</td>
<td>1746 TB</td>
<td>2095 TB</td>
</tr>
<tr>
<td></td>
<td>10 TB</td>
<td>436 TB</td>
<td>873 TB</td>
<td>1309 TB</td>
<td>1746 TB</td>
<td>2182 TB</td>
<td>2619 TB</td>
</tr>
<tr>
<td></td>
<td>12 TB</td>
<td>523 TB</td>
<td>1047 TB</td>
<td>1571 TB</td>
<td>2095 TB</td>
<td>2619 TB</td>
<td>3143 TB</td>
</tr>
</tbody>
</table>

Notes:

1. HDD capacity values are calculated using base 10 (for example, 1 TB = 1,000,000,000,000 bytes).
2. Capacity values are calculated using base 2 (for example, 1 TB = 1,099,511,627,776 bytes).

For more information about ScaleProtect with Cisco UCS on the C240 M5, please refer to ScaleProtect with Cisco UCS on the Cisco UCS C240 M5 Rack Server.
Configuring the VSA for Azure Stack

A physical machine or a virtual machine with the VSA installed can act as a VSA proxy to perform agentless backup and restore operations for Azure Stack virtual machines and Blob storage. The VSA for Azure Stack can protect Azure Stack environments that are deployed using Azure Active Directory (Azure AD) or Active Directory Federation Services (ADFS) in a connected or disconnected environment.

A minimum of one VSA is required for the Azure Stack proxy server:

- The OS must be Microsoft Windows Server 2012 or later.
- Commvault VSA, Cloud Apps, and MediaAgent modules must be deployed.
- The VSA for Azure Stack can be installed on a physical or virtual machine and can reside within the Azure Stack scale unit or external to the scale unit.
- Install Azure PowerShell and download Azure Stack tools as described in Install PowerShell for Azure Stack.
- A VSA proxy deployed on a virtual machine in Azure Stack must have a public IP address.

A VSA proxy deployed outside Azure Stack must be able to connect to the following Azure Stack endpoints:

- Required endpoint access for VSA proxy with ADFS:
  - Azure Stack Resource Manager endpoint: management.$(Azure Stack domain)
  - Storage endpoint suffix: $(Azure Stack domain)/adfs
  - Active Directory authority endpoint: adfs.$(Azure Stack domain)/adfs
  - Active Directory service endpoint: adfs.$(Azure Stack domain)/${TenantID}

- Required endpoint access for VSA proxy with Azure Active Directory:
  - Azure Stack Resource Manager endpoint: management.$(Azure Stack domain)
  - Storage endpoint suffix: $(Azure Stack domain)
  - Active Directory endpoint: graph.$(Azure Stack domain)
  - Active Directory endpoint: graph.$(Azure Stack domain)/${Tenant ID}

Table 4 summarizes the configuration for the VSA proxy used in the validation lab.

<table>
<thead>
<tr>
<th>Platform</th>
<th>External VSA for Azure Stack</th>
<th>Internal VSA for Azure Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>C220 M5SX</td>
<td>1 x Intel Xeon processor 4108 (8 cores at 1.8 GHz)</td>
<td>Standard_DS4_v2</td>
</tr>
<tr>
<td>CPU</td>
<td>32 GB</td>
<td>28 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>4 x 240 GB SSD</td>
<td>300 GB</td>
</tr>
<tr>
<td>RAID cache</td>
<td>2 GB</td>
<td>-</td>
</tr>
<tr>
<td>RAID</td>
<td>RAID 5 with hot spare for OS and data</td>
<td>-</td>
</tr>
<tr>
<td>Network</td>
<td>2 x 10 Gbps or 2 x 40 Gbps</td>
<td>Up to 6 Gbps</td>
</tr>
</tbody>
</table>

Notes:

- For more information about Azure Stack instance sizing, refer to [Microsoft Azure Stack VM Sizes](#).
- For more information about Commvault VSA sizing, refer to [CommCell sizing for Virtual Server Agent](#).
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.

The procedures for deploying the VSA proxy are presented here.

**Install the VSA for Azure Stack**

Use the following steps to install the VSA for Azure Stack.

1. From the CommCell Console ribbon, on the Tools tab, click Add/Remove Software. From the drop-down menu, choose Install Software.

   ![Click the Tools tab.](image)

2. The Installer Wizard will appear. Click Next.


4. On the Select How to Discover the Computers for Installing the Software page, click Next.

5. On the Select the Computer’s Operating System page, select Windows. Click Next.
6. On the Enter the Host Names of the Computers page, enter the host names or IP addresses of the VSA proxy servers that you will use. Click Next.

7. On the Enter Account Information page, enter credentials for a user with local administrator privileges on the server. Click Next.
8. On the Select Package(s) to Install page, under Server, select MediaAgent; under Virtualization, select Virtual Server; and under Applications, select Cloud Apps. Click Next.


10. On the Please Select When to Run the Job page, click Next.

11. On the Summary page, click Finish. A software installation job will be initiated. Monitor this job in the Job Controller window.
Install Azure PowerShell

Use the following steps to install Azure PowerShell.


   ```powershell
   Administrator: Windows PowerShell
   Windows PowerShell
   Copyright (C) 2016 Microsoft Corporation. All rights reserved.
   PS C:\Windows\system32> # Set the module repository and the execution policy.
   PS C:\Windows\system32> Set-PSRepository 'Name':'Azure', 'Source': 'https://azure-core-tools.s3.amazonaws.com/','Default' 'false','AllowCerts': 'true'
   PS C:\Windows\system32> # Install Azure Stack PowerShell modules.
   PS C:\Windows\system32> Install-Module 'Name': 'AzureStackTools', 'Repository': 'https://azuresdkcoretools.blob.core.windows.net/', 'Source': 'https://azuresdkcoretools.s3.amazonaws.com/','Default' 'false','AllowCerts': 'true'
   PS C:\Windows\system32> # Use Azure Stack PowerShell modules.
   PS C:\Windows\system32> Use-AzureStackProfile 'Name': 'AzureStackTools', 'Profile': 'https://azuresdkcoretools.s3.amazonaws.com/','Default' 'false','AllowCerts': 'true'
   PS C:\Windows\system32> # Uninstall any existing Azure PowerShell modules. To uninstall, close all the active PowerShells.
   PS C:\Windows\system32> Get-Module -ListAvailable -Name Azure | 'Uninstall-Module'
   PS C:\Windows\system32> # Install PowerShell for Azure Stack.
   PS C:\Windows\system32> Install-Module 'Name': 'AzureStack', 'Version': '1.2.11'...
   ```


   ```powershell
   Administrator: Windows PowerShell
   PS C:\Windows\system32> $To = [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
   PS C:\Windows\system32> Invoke-WebRequest -Uri 'https://github.com/Azure/AzureStack-Tools/archive/master.zip' -OutFile master.zip
   PS C:\Windows\system32> Expand-Archive master.zip
   PS C:\Windows\system32> cd AzureStack-Tools-master
   PS C:\AzureStack-Tools-master> ...
   ```
3. Configure the Azure Stack user environment.

Configure registry settings on the VSA for Azure Stack

The following procedures require the Azure Stack endpoints.

1. Run the following PowerShell command to get the Azure Stack endpoints for the Azure instance named Azure StackUser on the VSA for Azure Stack: `Get-AzureRmEnvironment -Name Azure StackUser`

2. Record the output <Azure Stack endpoints>.

3. Add the sResourceManagerURL additional setting on the VSA for Azure Stack proxy:
   a. From the CommCell Console, expand Clients, right-click VSA for Azure Stack, and choose Properties.
b. Click the Advanced button and click Additional Settings.
c. In the Additional Settings window, enter the following values:
   - Name: sResourceManagerURL
   - Category: VirtualServer
   - Type: String
   - Value: Endpoint URL from step 2
4. Click OK to close the Advanced Properties window and click OK to close the Properties window for the VSA for Azure Stack.

Configure the application and tenant for Azure Stack

The Azure application must be created in Azure and must be added to the Azure Stack tenant subscription.

1. In the Azure portal, select All Services. Select Identity and then select App Registrations.
2. Create a new application registration.

To view and manage your registration, enter the name of the application to be created in Azure Active Directory, select Web App/API native, and create a URL for the application. For example, use the name MyWebApp and the URL https://MyWebApp.
3. Update the application permissions by selecting the application, selecting Settings, and selecting Required Permissions. Then click Add.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Required permissions</th>
<th>Add API access</th>
<th>Enable Access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

| Select an API (for example, the Windows Azure Service Management API). |
| Select the Delegated Permissions option to access Azure service management as organization users. |
| Click Done. |

4. Get the application ID for the Azure Stack client. Select the application registrations in the navigation pane.

<table>
<thead>
<tr>
<th>Settings</th>
<th>API keys</th>
<th><strong>Keys</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Keep this key. This key will be used to configure the Azure Stack pseudo-client.

For more information, refer to Create a Service Principal for Azure AD.
Get the tenant ID from Azure Active Directory

The tenant ID is required to configure the Azure Stack client in Commvault. Use the following procedure to get the tenant ID from the Azure portal.

In the Azure portal, select Azure Active Directory select Properties. Note that the directory ID is the same as the tenant ID.

![Image of Azure portal with highlighted Directory ID]

Directory ID = tenant ID

Configure the application or service principal for the tenant subscription

Use the following procedures to configure the application or service principal for the tenant subscription.

1. In the Azure Stack portal, select Subscriptions. Then select the subscription.
2. Select Access Control (IAM). Then add the application or service principal to the subscription and click Save.

Add a Microsoft Azure Stack client for Azure Active Directory or ADFS

The following procedures are run from the CommCell Console and will be used to add a Microsoft Azure Stack hypervisor to support data protection operations for all virtual machines hosted.

Use Table 5 for the input values for the following procedures.

Table 5. Variables for adding a Microsoft Azure Stack client

<table>
<thead>
<tr>
<th>Variable</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Enter the client name.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select Azure Active Directory or Active Directory Federation Services.</td>
</tr>
<tr>
<td>Resource Manager URL (ADFS only)</td>
<td>Enter the Azure Stack Resource Manager endpoint.</td>
</tr>
<tr>
<td>Subscription ID</td>
<td>Enter the Azure Stack subscription ID.</td>
</tr>
<tr>
<td>Tenant ID (Azure AD only)</td>
<td>Enter the Azure Active Directory ID.</td>
</tr>
<tr>
<td>Application ID</td>
<td>Enter the Azure Active Directory or the ADFS service principal application ID.</td>
</tr>
<tr>
<td>Thumbprint: (ADFS only)</td>
<td>Enter the service principal certificate thumbprint.</td>
</tr>
<tr>
<td>Proxies</td>
<td>Add the VSA proxy or proxies that are configured for the Azure Stack environment.</td>
</tr>
</tbody>
</table>

2. Click Virtualization and click Azure Stack.
3. Enter the Azure Stack environment information.

![Create Azure Stack Client](image)

**Configure a subclient for Azure Stack virtual machine protection**

Use the following steps to configure a subclient for Azure Stack virtual machine protection.

1. From the CommCell browser, navigate to Client Computers > virtualization_client > Virtual Server > Azure Stack.
2. Right-click a backup set and click New Subclient.
3. On the General tab, enter the subclient name.
4. Identify virtual machines to back up:
   a. Click the Content tab.
   b. Click Browse.
   c. From the list at the top left, select a view to browse by virtual machines or other categories.
   d. Navigate to one or more virtual machines and select them.
   e. Click OK.

   The selected virtual machines are displayed in the Contents of Subclient list.

   **Note:** For other methods of identifying virtual machines for a subclient, see Adding Subclient Content.

5. Click the Storage Device tab.
6. Select a storage policy.
7. To specify proxies to be used to back up the subclient, click the Advanced Options tab and add the proxies to be used.
   If you do not specify proxies at the subclient level, the proxies specified at the instance level are used.

   **Note:** If you have existing VSA proxies that are used to support Azure Classic or Azure Resource Manager, use different proxies for Azure Stack.

8. Click OK.
9. In the Backup Schedule dialog box, click Do Not Schedule. Then click OK.
Configure the Azure Blob virtual client

Use the following procedures to create a virtual client for Azure or Azure Stack Blob storage to perform backup and restore operations.

1. From the CommCell browser, right-click Client Computers and then choose New Client > Cloud Storage > Azure BLOB.

2. On the General tab, fill in the fields as shown in the following screenshot.
3. Click the Connection Details tab and provide the details as shown in the following screenshot.

![New Azure Storage Client](image)

- **Enter the Azure Stack Blob storage service account URL.**
- **Enter the name of the Azure Stack Blob storage service account.**
- **Enter the secret access key for the Azure Stack Blob storage service.**
- **Re-enter the secret access key for the Azure Stack Blob storage service account.**

4. Click OK.

For more information about setting up Azure Blob storage protection, refer to [Azure Blob Storage](#).

**Configuring Azure Stack protection**

The next step is to configure Azure Stack protection.

**Admin Console overview**

The Admin Console is a powerful web-based user interface that provides a simplified, service-oriented approach to managing on-premises and cloud infrastructure. It is streamlined for routine data protection and recovery tasks. With an easy-to-use and flexible interface, you can configure and manage a broad range of solutions, including file systems, databases, and hypervisors. The Admin Console provides administrators and application owners with an interface to simplify administrative tasks, including policy management, operations, analytics, and monitoring. The Admin Console is built on a self-service, solution-based architecture that adapts to your environment without the need for complicated administration. After the initial deployment and configuration of the console is completed, solutions can be added with ease.

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

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

The Admin Console dashboard provides a quick overview of managed assets, alerts, and SLA targets.
Data protection plans

The Admin Console greatly simplifies the configuration of data protection. Simplification is achieved by creating a protection plan, which consists of several configuration options easily set in a single wizard. Options include storage pool, retention, backup schedule, content to protect, and offsite copy configurations.

You create backup plans to protect data by defining what to back up, where to back up data, and how often to run the backup job. The Admin Console provides predefined plan types, and these include the data protection parameters that apply to the type of data you want to protect. Plans are created during configuration; however, you can also later define additional backup plans.

Configure a virtualization plan for Azure Stack protection

A virtualization plan is used to protect virtual machines using the VSA. After protection is implemented, several recovery options are available: for example, you can restore an entire virtual machine, files within a virtual machine, a virtual machine disk, and more.

When you configure a plan, you must specify a plan type. The following types are available:

- Backup
- Backup and replication

A backup plan simply protects the virtual machines at the set frequency and sends the backup data to primary storage. The primary copy can be copied and replicated in a secondary storage pool if needed.

The backup and replication plan not only protects the virtual machine in storage, but also restores the virtual machine in a secondary virtualization environment. This restoration process can be implemented at a set frequency that can be scheduled, or it can be performed as soon as the backup operation is complete. This approach helps ensure that if a disaster occurs, the virtual machines are ready to be powered on. This feature of the Commvault software is referred to as Live Sync.

The following procedures provide an example showing how to create a plan.

1. Log in to the Admin Console. Click Plans.
2. Click Create Plan and then click Virtualization.
3. Select Backup.

4. Enter the plan name, select Storage Pool, set the retention period, set the Backup SLA time, click Add Schedule, and click Next.
5. It is recommended to create another copy, click "I want to create another copy."

6. Enter the Storage copy name, select Storage pool, set the retention period, set the Backup SLA time, and click Next.
7. The window displays the plan created and provides option for medication if needed.

Set up a subclient for Azure Stack virtual machine protection

Add a subclient to identify a specific set of virtual machines to back up or restore from Azure Stack.

1. From the navigation pane, navigate to Solutions > Virtualization > Hypervisors.
2. Click the name of the Azure Stack hypervisor.
3. Click Add Subclient
4. Enter the information in the Add Subclient pop-up window. Then click Save to save the subclient.

Subclients are created with default settings for backup options. To change the default settings, see Editing Subclient Options.
Manually back up a virtual machine

The following procedures show how to perform a manual backup operation from the Admin Console.

1. Select the subclient in the Hypervisors view. Then choose Back Up Now.

2. Choose the backup option and click OK.
3. Monitor the backup job in the Jobs monitor.

![Image of backup job in Jobs monitor]

**Restore a virtual machine**

The following procedures show how to restore a virtual machine.

1. Select the ellipsis for a subclient in the Hypervisors view. Then choose Restore.

![Image of selecting ellipsis and choosing Restore]
2. Select the restore type (either Guest Files or Full Virtual Machine).

For a Guest Files restore operation:

a. Select the file that you want to restore. Then select Restore.

b. Select the restore destination. Then click Submit.
● For a Full Virtual Machine restore operation:
  a. Select the virtual machine. Then click Restore.

b. Enter the Restore options, then click Submit.
Conclusion

The Cisco Integrated System for Microsoft Azure Stack and Commvault Data Protection through ScaleProtect with Cisco UCS provides a complete multicloud solution engineered to perform, scale, protect, and optimize to meet your “always-on” business demands. Backup and restore operations can be initiated from a single GUI, and the complexity of the underlying system can be hidden from daily operators. The seamless integration of Commvault and Cisco UCS server platforms make this a best-in-class solution for secondary-site backup operations and virtual machine archiving, with multiple options for restoration—all within a single management interface. The solution is designed to accelerate Azure Stack and cloud adoption through policy-based management tools that provide automation and orchestration for existing workloads. Deploy with confidence a flexible and scalable solution to meet your critical data, services, and application needs today as well as your evolving needs in the future.

For more information

For additional information, see the following:

- Cisco Integrated System for Microsoft Azure Stack Solution Overview
- Cisco Integrated System for Microsoft Azure Stack Data Sheet
- Cisco UCS C240 M5 Rack Server
- Cisco UCS 6000 Series Fabric Interconnects
- Cisco UCS Manager
- Cisco white paper: ScaleProtect with Cisco UCS on the Cisco UCS C240 M5 Rack Server
- ScaleProtect with Cisco UCS (solution brief)
- Commvault Software Offline Installation
- Commvault Cloud Storage Support
- Commvault Support for Azure Stack