

Deploy Veeam Backup & Replication with Scality RING on Cisco UCS to Protect Large Data Sets

This document introduces the expansion of Veeam Backup & Replication with Scality RING as a capacity tier to protect large data sets.

Contents

Introduction	3
Purpose of this document	3
Test environment	3
Cisco Unified Computing System	4
Cisco Nexus 9000 Series Switches	11
Veeam Availability Suite	12
Scality RING	16
Solution design	29
Configuring Scality RING	30
Configure Veeam Backup & Replication	35
Test the new configuration	51
Conclusion	53
For more information	53

Introduction

The amount of data that organizations need to protect continues to grow, while at the same time the time frame for restoring critical workloads is shrinking. This challenge is hard to resolve with traditional systems for data protection. Either the solution cannot scale to provide the capacity needed for the amount of data, or the solution becomes too expensive, or the restoration of critical workloads runs outside the requirements defined by the business. In Veeam Backup & Replication Release 9.5 Update 4, Veeam introduced the option to use object storage solutions through the Amazon Web Services (AWS) Simple Storage Service (S3) protocol as a capacity tier. With this option, organizations can build a performance tier within a Veeam environment to meet the recovery-time objective (RTO) and recovery-point objective (RPO) requirements of the business for fast storage and then migrate older data sets or less important data sets through the S3 protocol to cloud storage or to on-premises object storage, such as Scalify RING on Cisco UCS® S3260 Storage Servers. Organizations can meet the RPO and RTO requirements of the business by restoring the data or virtual machines from the performance tier and at the same time scaling the capacity tier on object storage nearly limitlessly at an affordable cost.

Purpose of this document

This document describes the configuration of Veeam Backup & Replication on the Cisco Unified Computing System™ (Cisco UCS) as a performance tier connected to Scalify RING on Cisco UCS as a capacity tier.

The document does not cover the installation of Veeam Backup & Replication or Scalify RING on Cisco UCS C240 rack servers. Please use the published documents for the initial installation.

This document covers these topics:

- Configuration in Scalify RING: Users, buckets, and access keys
- Configuration in Veeam Backup & Replication: Backup repository on S3, scale-out backup repository, and backup jobs

Test environment

This section introduces the components and technologies used in the lab to test the processes described in this document.

The setup used in the lab for this document uses one Cisco UCS 240 M5 Rack Server to run Veeam Backup & Replication and three Cisco UCS C240 M5 Rack Servers to run Scalify RING. This is just one out of many configuration options, and the combination will also work with Cisco UCS S3260 Storage Servers or a combination of Cisco UCS C240 and S3260 servers.

Table 1 lists the hardware and software versions used in the test environment described in this document.

Table 1. Test environment details

Layer	Component	Image or version
Computing	Cisco UCS 6332-16UP Fabric Interconnect pair	Release 4.0(1b)
	Cisco UCS C240 M5 Rack Server	Release 4.0(1b)
Network	Cisco Nexus® 9372PX Switch pair	Release 7.0(3)I2(2d)
Software	Cisco UCS Manager	Release 4.0(1b)
	Veeam Availability Suite	Release 9.5 Update 4
	Scality RING	Release 7.4

Cisco Unified Computing System

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

Cisco UCS consists of these main resources:

- **Computing:** The system is based on an entirely new class of computing system that incorporates rack-mount and blade servers using Intel® Xeon® processor CPUs. The Cisco UCS servers offer patented Cisco® Extended Memory Technology to support applications with large data sets and allow more virtual machines per server.
- **Network:** The system is integrated onto a low-latency, lossless, 10- or 40-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing (HPC) networks, which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- **Virtualization:** The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage access:** The system provides consolidated access to both SAN storage and network-attached storage (NAS) over the unified fabric. By unifying the storage access layer, Cisco UCS can access storage over Ethernet (with Network File System [NFS] or Small Computer System Interface over IP [iSCSI]), Fibre Channel, and Fibre Channel over Ethernet (FCoE). This approach provides customers with a choice for 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.

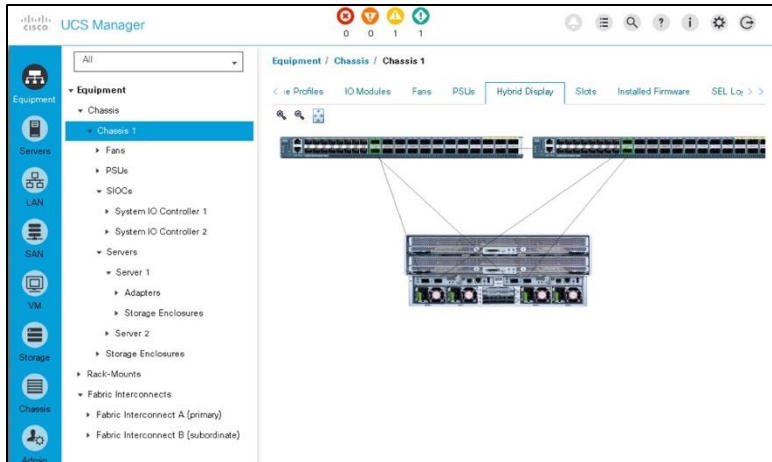


Figure 1.
Cisco UCS Manager

Cisco UCS consists of the following components:

- [Cisco UCS Manager](#) provides unified, embedded management of all software and hardware components in the Cisco Unified Computing System (Figure 1).
- [Cisco UCS 6000 Series Fabric Interconnects](#) are line-rate, low-latency, lossless, 10- or 40-Gbps Ethernet and FCoE interconnect switches that provide the management and communication backbone for Cisco UCS.
- [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 total cost of ownership (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 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
- Industry standards supported by a partner ecosystem of industry leaders
- Unified, embedded management for easy-to-scale infrastructure

Cisco UCS C240 M5 Rack Server

The Cisco UCS C240 M5 Rack Server (Figure 2) is a two-socket, 2RU rack server offering industry-leading performance and expandability. It supports a wide range of storage and I/O-intensive infrastructure workloads, from big data and analytics to collaboration. 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 their business agility.



Figure 2.
Cisco UCS C240 M5 Rack Server

In response to ever-increasing computing and data-intensive real-time workloads, the enterprise-class Cisco UCS C240 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 Non-Volatile Memory Express (NVMe) PCI Express (PCIe) solid-state disks (SSDs) than the previous generation of servers. These improvements deliver significant performance and efficiency gains that will improve your application performance. The Cisco UCS C240 M5 delivers outstanding levels of storage expandability with exceptional performance. The servers offer the following features:

- Latest Intel Xeon Scalable CPUs with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- 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-, 25- 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

The Cisco UCS C240 M5 server is well suited for a wide range of enterprise workloads, including the following:

- Object storage
- Big data and analytics
- Collaboration
- Small and medium-sized business databases

-
- Virtualization and consolidation
 - Storage servers
 - High-performance appliances

Cisco UCS C240 servers can be deployed as standalone servers or in a Cisco UCS managed environment. When used in combination with Cisco UCS Manager, the Cisco UCS C240 brings the power and automation of unified computing to enterprise applications, including Cisco SingleConnect technology, drastically reducing switching and cabling requirements.

Cisco UCS Manager uses service profiles, templates, and policy-based management to enable rapid deployment and help ensure deployment consistency. It also enables end-to-end server visibility, management, and control in both virtualized and bare-metal environments.

The Cisco Integrated Management Controller (IMC) delivers comprehensive out-of-band server management with support for many industry standards, including the following:

- Redfish Version 1.01 (v1.01)
- Intelligent Platform Management Interface (IPMI) v2.0
- Simple Network Management Protocol (SNMP) v2 and v3
- Syslog
- Simple Mail Transfer Protocol (SMTP)
- Key Management Interoperability Protocol (KMIP)
- HTML5 GUI
- HTML5 virtual keyboard, video, and mouse (vKVM)
- Command-line interface (CLI)
- XML API

Management software development kits (SDKs) and DevOps integrations exist for Python, Microsoft PowerShell, Ansible, Puppet, Chef, and more. For more information about integrations, see Cisco DevNet (<https://developer.cisco.com/site/ucs-dev-center/>).

The Cisco UCS C240 is Cisco Intersight™ ready. The Cisco Intersight solution is a new cloud-based management platform that uses analytics to deliver proactive automation and support. By combining intelligence with automated actions, you can reduce costs dramatically and resolve problems more quickly.

Cisco UCS Virtual Interface Card 1387

The Cisco UCS VIC 1387 (Figure 3) offers dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP+) 40 Gigabit Ethernet and FCoE in an mLOM form factor. The mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, providing greater I/O expandability.



Figure 3.
Cisco UCS Virtual Interface Card 1387

The Cisco UCS VIC 1387 provides high network performance and low latency for the most demanding applications, including the following:

- Big data, HPC, and high-performance trading (HPT)
- Large-scale virtual machine deployments
- High-bandwidth storage targets and archives

The card is designed for the M5 generation of Cisco UCS C-Series Rack Servers and Cisco UCS S3260 dense storage servers. It includes Cisco's next-generation converged network adapter (CNA) technology and offers a comprehensive feature set, so you gain investment protection for future software feature releases.

The card can present more than 256 PCIe standards-compliant interfaces to its host. These can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs).

This engine provides support for advanced data center requirements, including stateless network offloads for the following:

- Network Virtualization Using Generic Routing Encapsulation (NVGRE)
- Virtual extensible LAN (VXLAN)
- Remote direct memory access (RDMA)

The engine also offers support for performance optimization applications such as the following:

- Server Message Block (SMB) Direct
- Virtual Machine Queue (VMQ)
- Data Plane Development Kit (DPDK)
- Cisco NetFlow

Cisco UCS 6300 Series Fabric Interconnects

The Cisco UCS 6300 Series Fabric Interconnects are a core part of Cisco UCS, providing both network connectivity and management capabilities for the system (Figure 4.). The Cisco UCS 6300 Series offers line-rate, low-latency, lossless 10 and 40 Gigabit Ethernet, FCoE, and Fibre Channel functions.



Figure 4.
Cisco UCS 6300 Series Fabric Interconnects

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

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

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

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

Cisco UCS Manager

Cisco UCS Manager (Figure 5.) provides unified, embedded management of all software and hardware components of Cisco UCS across multiple chassis and rack servers and thousands of virtual machines. It supports all Cisco UCS product models, including Cisco UCS B-Series Blade Servers, C-Series Rack Servers, and S- and M-Series composable infrastructure and Cisco UCS Mini, as well as the associated storage resources and networks. Cisco UCS Manager is embedded on a pair of Cisco UCS 6300 or 6200 Series Fabric Interconnects using a clustered, active-standby configuration for high availability. The manager participates in server provisioning, device discovery, inventory, configuration, diagnostics, monitoring, fault detection, auditing, and statistics collection.

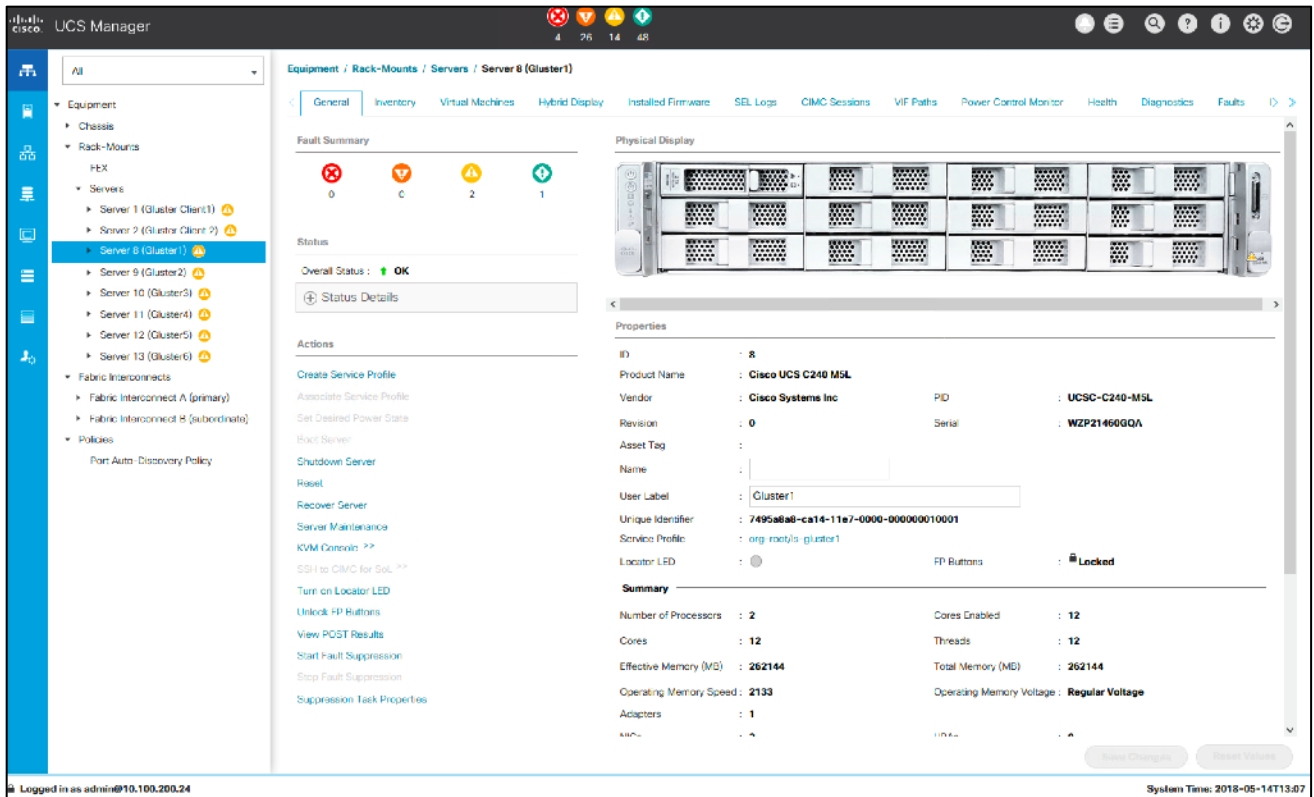


Figure 5.
Cisco UCS Manager

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

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

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

Cisco Nexus 9000 Series Switches

Based on [Cisco Cloud Scale technology](#), the Cisco Nexus 9300-EX and 9300-FX platforms (Figure 6) are the next generation of fixed Cisco Nexus 9000 Series Switches. The new platforms support cost-effective cloud-scale deployments, an increased number of endpoints, and cloud services with wire-rate security and telemetry. The platforms are built on modern system architecture designed to provide high performance and meet the evolving needs of highly scalable data centers and growing enterprises.



Figure 6.
Cisco Nexus 9336C-FX2 Switch

Cisco Nexus 9300-EX and 9300-FX platform switches offer a variety of interface options to transparently migrate existing data centers from 100-Mbps, 1-Gbps, and 10-Gbps speeds to 25 Gbps at the server, and from 10- and 40-Gbps speeds to 50 and 100 Gbps at the aggregation layer. The platforms provide investment protection for customers, delivering large buffers, highly flexible Layer 2 and Layer 3 scalability, and performance to meet the changing needs of virtualized data centers and automated cloud environments.

The Cisco Nexus 9336C-FX2 Switch is a 1RU switch that supports 7.2 Tbps of bandwidth and over 2.8 Bpps. The switch can be configured to work at 1, 10, 25, 40, and 100 Gbps, offering flexible options in a compact form factor. All ports support wire-rate MAC Security (MACsec) encryption. Breakout is supported on all ports.

The platform hardware is capable of collecting comprehensive Cisco Tetration Analytics™ telemetry information at line rate across all the ports without adding any latency to the packets or negatively affecting switch performance. This telemetry information is exported every 100 milliseconds (ms) by default directly from the switch's application-specific integrated circuit (ASIC). This information consists of three types of data:

- Flow information: This information contains information about endpoints, protocols, ports, when the flow started, how long the flow was active, and so on.
- Interpacket variation: This information captures any interpacket variations within the flow. Examples include variation in time to live (TTL), IP and TCP flags, and payload length.
- Context details: Context information is derived outside the packet header, including variation in buffer utilization, packet drops within a flow, and association with tunnel endpoints.

The Cisco Tetration Analytics platform consumes this telemetry data, and by using unsupervised machine learning and behavior analysis it can provide outstanding pervasive visibility across everything in your data center in real time. By using algorithmic approaches, the Cisco Tetration Analytics platform provides deep application insights and interactions, enabling dramatically simplified operations, a zero-trust model, and migration of applications to any programmable infrastructure. To learn more, go to <https://www.cisco.com/go/tetration>.

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

Veeam Availability Suite

Veeam Availability Suite combines the backup, restore, and replication capabilities of Veeam Backup & Replication with the advanced monitoring, reporting, and capacity planning functions of Veeam ONE.

Backup

Veeam Backup & Replication operates at the virtualization layer and uses an image-based approach for virtual machine backup. To retrieve virtual machine data, no agent software needs to be installed in the guest OS. Instead, Veeam Backup & Replication uses VMware vSphere snapshot capabilities and application-aware processing. When a new backup session starts, a snapshot is taken to create a cohesive point-in-time copy of a virtual machine, including its configuration, OS, applications, associated data, and system state. Veeam Backup & Replication uses this point-in-time copy to retrieve virtual machine data. Image-based backups can be used for different types of recovery, including full virtual machine recovery, virtual machine file recovery, instant virtual machine recovery, and file-level recovery.

Use of the image-based approach allows Veeam Backup & Replication to overcome the limitations of traditional backup processes. It also helps simplify recovery verification and the restore process: to recover a single virtual machine, you do not need to perform multiple restore operations. Veeam Backup & Replication uses a cohesive virtual machine image from the backup repository to restore a virtual machine to the required state without the need for any manual reconfiguration or adjustment.

With Veeam Backup & Replication, backup is a job-driven process in which one backup job can be used to process one or more virtual machines. The job is the configuration unit for the backup activity. Essentially, a job defines when, what, how, and where data is backed up. It indicates what virtual machines should be processed, what components should be used to retrieve and process virtual machine data, what backup options should be enabled, and where the resulting backup file should be saved. Jobs can be started manually by the user or scheduled to run automatically. The resulting backup file stores compressed and deduplicated virtual machine data. Compression and deduplication are performed by the Veeam proxy server.

Regardless of the backup method you use, the first run of a job creates a full backup of the virtual machine image. Subsequent job runs are incremental: Veeam Backup & Replication copies only those data blocks that have changed since the last backup job was run. To keep track of changed data blocks, Veeam Backup & Replication uses several approaches, including VMware's Changed Block Tracking (CBT) technology.

Restore

Veeam Backup & Replication offers a number of recovery options for a variety of disaster-recovery scenarios:

- Veeam Explorer enables you to restore single application items.
- Instant virtual machine recovery enables you to instantly start a virtual machine directly from a backup file.
- Full virtual machine recovery enables you to recover a virtual machine from a backup file to its original or another location.
- Virtual machine file recovery enables you to recover separate virtual machine files (virtual disks, configuration files, and so on).
- Virtual drive restoration enables you to recover a specific hard drive of a virtual machine from the backup file and attach it to the original virtual machine or to a new virtual machine.

- Microsoft Windows file-level recovery enables you to recover individual Windows guest OS files (from the File Allocation Table [FAT], New Technology File System [NTFS], and Resilient File System [ReFS] file systems).
- Multiple-OS file-level recovery enables you to recover files from 15 different guest OS file systems.

Veeam Backup & Replication uses the same image-level backup process for all data-recovery operations. You can restore virtual machines, virtual machine files and drives, application objects, and individual guest OS files to the most recent state or to any available restore point.

Instant virtual machine recovery

With instant virtual machine recovery, you can immediately restore a virtual machine to your production environment by running it directly from the backup file. Instant virtual machine recovery helps improve your RTO and reduce disruption and downtime on production virtual machines. It is like having a temporary clone of a virtual machine. Users can remain productive while you troubleshoot the problem in the failed virtual machine.

When instant virtual machine recovery is performed, Veeam Backup & Replication uses the Veeam vPower technology to mount a virtual machine image on a VMware ESXi host directly from a compressed and deduplicated backup file. Because you do not need to extract the virtual machine from the backup file and copy it to production storage, you can restart a virtual machine from any restore point (incremental or full) in minutes.

After the virtual machine is back online, you can use VMware Storage vMotion to migrate the virtual machine back to production storage.

Virtual machine object recovery

Veeam Backup & Replication can help you restore specific virtual machine files (.vmdk, .vmx, and others) if any of these files are deleted or the datastore is corrupted. This option provides an excellent alternative to full virtual machine restoration: for example, when your virtual machine configuration file is missing and you need to restore it. Instead of restoring the whole virtual machine image to production storage, you can restore only the specific virtual machine file.

Another data-recovery option provided by Veeam Backup & Replication is the restoration of a specific hard drive of a virtual machine. If a virtual machine hard drive becomes corrupted for some reason (for example, by a virus), you can restore it from the image-based backup file to any known good point in time.

Components

Veeam Availability Suite provides backup, restore, and replication capabilities plus advanced monitoring, reporting, and capacity planning functions. Veeam Availability Suite delivers everything you need to reliably ensure and manage your environment. Veeam Backup & Replication is a modular solution that lets you build a scalable backup infrastructure for environments of different sizes and configurations. The installation package of Veeam Backup & Replication includes a set of components that you can use to configure the backup infrastructure. Some components are mandatory and provide core functions, and some components are optional and can be installed to provide additional features to meet your particular business and deployment needs. You can co-install all Veeam Backup & Replication components on the same machine, physical or virtual, or you can set them up separately for a more scalable approach.

Figure 7 provides an overview of the main Veeam components.

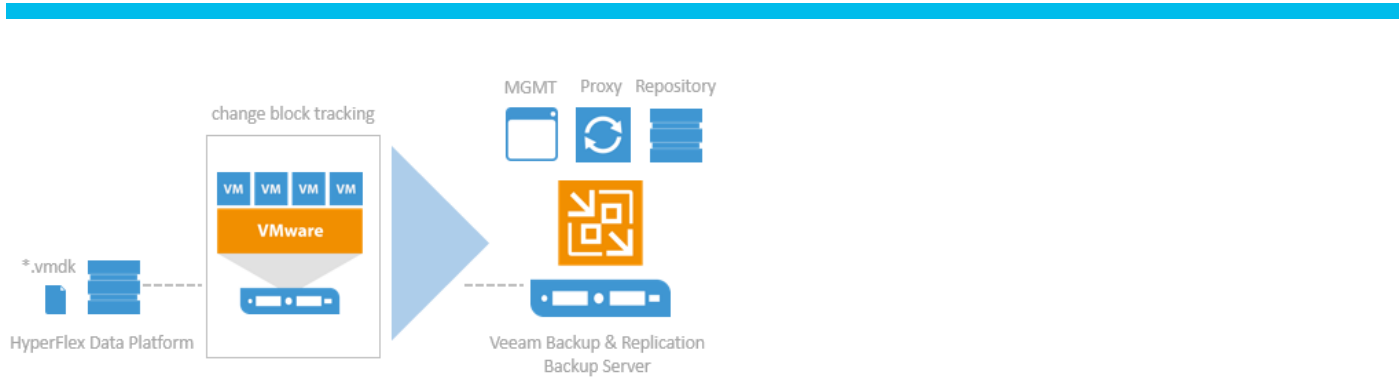


Figure 7.
Veeam Backup & Replication components

Backup server

The backup server is a Microsoft Windows-based physical or virtual machine on which Veeam Backup & Replication is installed. It is the core component in the backup infrastructure, filling the role of configuration and control center. The backup server performs all types of administrative activities:

- It coordinates backup, replication, recovery verification, and restore tasks.
- It controls job scheduling and resource allocation.
- It manages all proxy and repository servers.

It is used to set up and manage backup infrastructure components as well as specify global settings for the backup infrastructure (Figure 8).

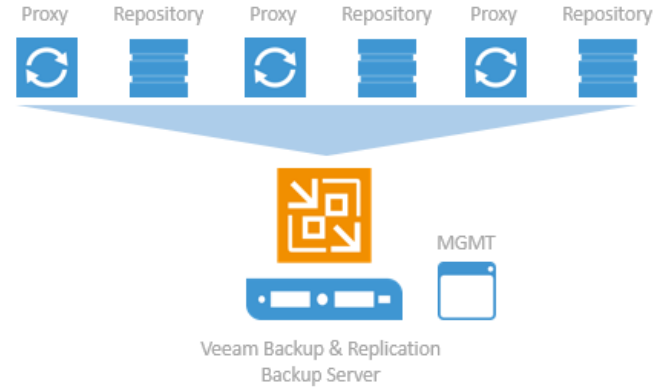


Figure 8.
Veeam backup server management

In addition to its primary functions, a newly deployed backup server also performs the roles of default backup proxy and backup repository.

The backup server uses the following services and components:

- Veeam Backup Service is a Windows service that coordinates all operations performed by Veeam Backup & Replication, such as backup, replication, recovery verification and restore tasks. The Veeam Backup Service runs under the local system account or the account that has local administrator permissions on the backup server.

-
- Veeam Backup Shell provides the application user interface and allows access to the application's functions.
 - Veeam Guest Catalog Service is a Windows service that manages guest OS file system indexing for virtual machines and replicates system index data files to enable searches through guest OS files. Index data is stored in the Veeam backup catalog: a folder on the backup server. The Veeam Guest Catalog Service running on the backup server works in conjunction with search components installed on Veeam Backup Enterprise Manager and (optionally) a dedicated Microsoft search server.
 - Veeam Backup SQL Database is used by Veeam Backup Service, Backup Shell, and Guest Catalog Service to store data about the backup infrastructure, jobs, sessions, and so on. The database instance can be located on a Microsoft SQL Server installed either locally (on the same machine on which the backup server is running) or remotely.
 - Veeam Backup PowerShell Snap-In is an extension to Microsoft Windows PowerShell 2.0. Veeam Backup PowerShell adds a set of cmdlets to allow users to perform backup, replication, and recovery tasks through the PowerShell CLI or run custom scripts for fully automated operation of Veeam Backup & Replication.
 - Backup Proxy Services are a set of data movement services. The backup server runs these services in addition to dedicated services.

Veeam repository sizing

To estimate the amount of required disk space, you should know the following:

- The total size of the virtual machines being backed up
- Frequency of backup operations
- The retention period for backup files
- Whether jobs will use forward or reverse incremental backup processes

In addition, when testing is not possible beforehand, you should make assumptions about compression and deduplication ratios, change rate, and other factors. The following figures are typical for most deployments; however, you need to understand the specific environment to identify possible exceptions:

- Data reduction from compression and deduplication is usually 2:1 or greater. A ratio of 3:1 or greater is common, but you should always be conservative when estimating required space.
- The typical daily change rate is between 2 and 5 percent in a midsize or enterprise environment. However, this rate can vary greatly among servers, with some servers showing much higher values. If possible, run monitoring tools such as Veeam ONE to gain a better understanding of the actual change rates in your system.
- Include additional space for occasional full backups.
- Include additional space for backup chain transformation (forward forever incremental to reverse incremental backups).
- Include space equal to at least the size of a full backup multiplied by 1.25.

Using these numbers, you can estimate the required disk space for any job. In addition, you always should leave plenty of headroom for future growth, additional full backups, movement of virtual machines, and restoration of virtual machines from tape.

Note: A repository sizing tool that can be used for estimation is available at <http://vee.am/rps>. Note that this tool is not officially supported by Veeam. Nonetheless, it is heavily used by Veeam architects. The tool is regularly updated.

Scality RING

Scality RING (Figure 9) is a cloud-scale, distributed software solution for petabyte-scale unstructured data storage. It is designed to create unbounded scale-out storage systems for the many petabyte-scale applications and use cases, both object and file, that are deployed in today's enterprise data centers. RING is a fully distributed system deployed on industry-standard hardware, starting with a minimum of three storage servers. The system can be seamlessly scaled to thousands of servers with hundreds of petabytes of storage capacity. RING has no single points of failure and requires no downtime during any upgrades, scaling, planned maintenance, or unplanned system events. With self-healing capabilities, it continues operating normally throughout these events.

To match performance to increasing capacity, RING can also independently scale out its access layer of protocol connectors, to enable an even match of aggregate performance to the application load. RING provides data protection and resiliency through local or geographically distributed erasure coding and replication, with services for continuous self-healing to resolve expected failures in platform components such as servers and disk drives. RING is fundamentally built on a scale-out object-storage layer that employs a second-generation peer-to-peer architecture. This approach uniquely distributes both the user data and the associated metadata across the underlying nodes to eliminate the typical central metadata database bottleneck. To enable file and object data in the same system, RING integrates a virtual file system layer through an internal NoSQL scale-out database system, which provides Portable Operating System Interface (POSIX)-based access semantics using standard NFS, SMB, and Filesystem in Userspace (FUSE) protocols with shared access to the files as objects using the representational state transfer (REST) protocol.

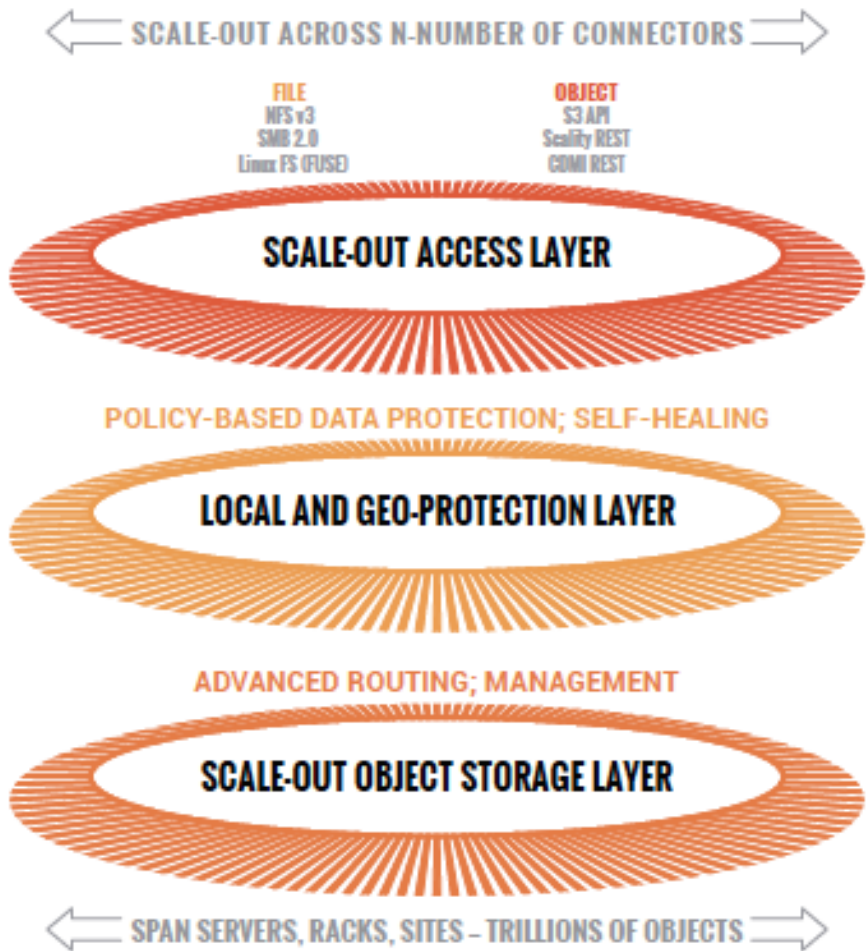


Figure 9.
Scality RING overview

Scality designed RING using the design criteria implemented by leading cloud-scale service providers, such as Google, Facebook, and Amazon. RING uses a loosely coupled, distributed systems design that uses mainstream commodity hardware and supports these main principles:

100 percent parallel design for metadata and data, to enable scaling of capacity and performance to unbounded numbers of objects, with no single points of failures, service disruptions, or major equipment upgrades as the system grows.

Multiprotocol data access, to allow the widest variety of object-based, file-based, and host-based applications to use RING storage.

Flexible data protection mechanisms, to efficiently and durably protect a wide range of data types and sizes.

Self-healing after component failures, to provide high levels of data durability; the system expects and tolerates failures and automatically resolves them.

Hardware freedom, to provide optimal platform flexibility, eliminate lock-in, and reduce TCO.

RING incorporates these design principles at multiple levels to deliver the highest levels of data durability at the highest levels of scale for the most optimal economics.

Scality RING architecture

To scale both storage capacity and performance to massive levels, the Scality RING software is designed as a distributed, parallel, scale-out architecture with a set of intelligent services for data access and presentation, data protection, and systems management. To implement these capabilities, RING provides a set of fully abstracted software services including a top layer of scalable access services (connectors) that provide storage protocols for applications. The middle layers consists of a distributed virtual file system, a set of data protection mechanisms to help ensure data durability and integrity, self-healing processes, and a set of systems management and monitoring services. At the bottom of the stack, the system is built on a distributed storage layer that consists of virtual storage nodes and underlying I/O daemons that abstract the physical storage servers and disk-drive interfaces. Figure 10 shows the architecture.

At the core of the storage layer is a scalable, distributed object key-value store based on a second-generation peer-to-peer routing protocol. This routing protocol helps ensure that store and lookup operations scale efficiently to very high numbers of nodes.

RING software includes the following main components: RING connectors, a distributed internal NoSQL database called MESA, RING storage nodes and I/O daemons, and a web-based Supervisor management portal. The MESA database is used to provide object indexing. RING also includes the integral Scale-Out File System (SOFS) abstraction layer, the underlying core routing protocol, and keyspaces mechanisms.

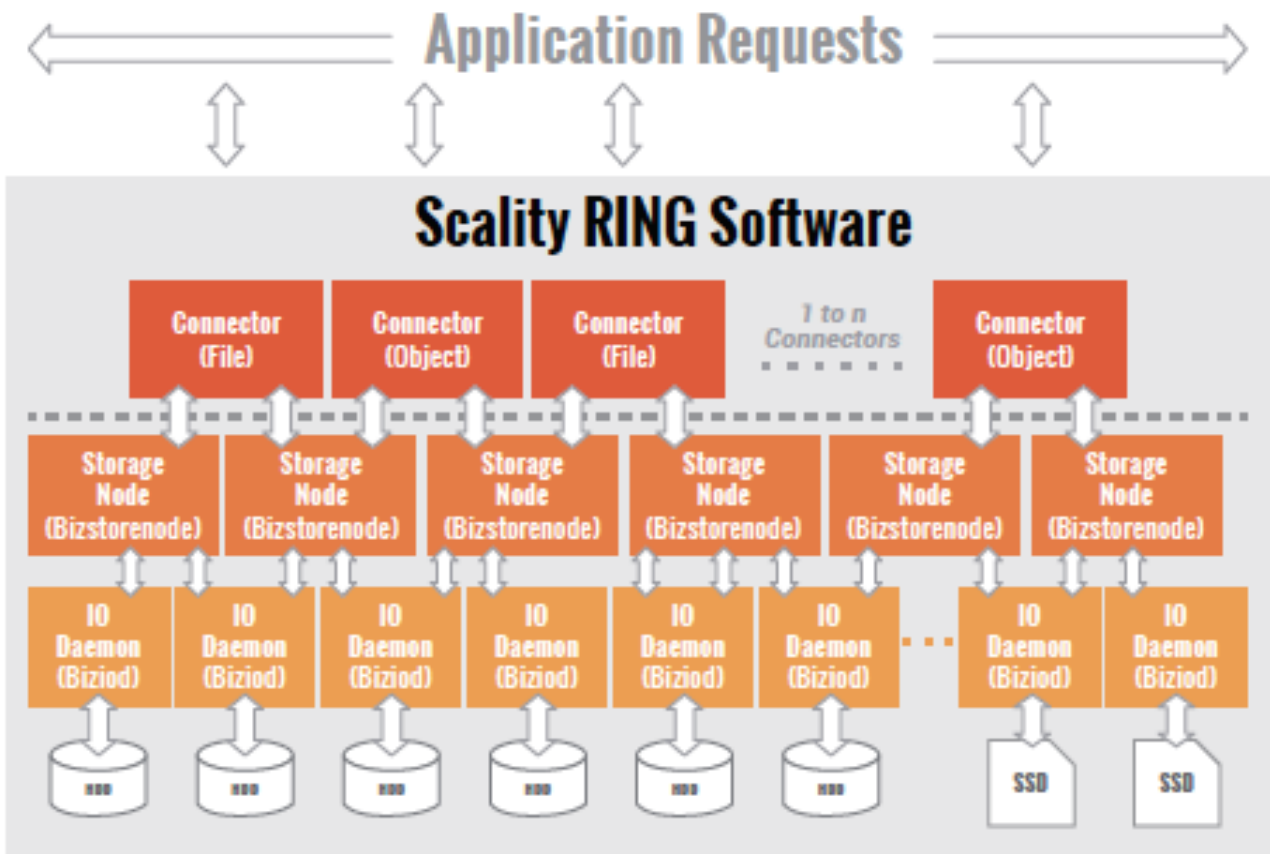


Figure 10.
Scality scale-out architecture

Scality RING connectors

RING connectors provide the data access endpoints and protocol services for applications that use Scality RING for data storage. As a scale-out system, RING supports any number of connectors and endpoints to service large and growing application workloads. RING Release 7 provides a group of object and file interfaces:

- **AWS S3 API:** A comprehensive implementation of the AWS S3 REST API provides support for the bucket and object data model, AWS Signature Version 4 and Version 2 (v4 and v2)-style authentication, and the AWS model of identity and access management (IAM).
- **HTTP and REST (sproxyd):** RING's native key-value REST API provides a flat object storage name space with direct access to RING objects.
- **NFSv3:** SOFS volumes are presented as standard NFSv3 mount points.
- **SMB 2.0:** SOFS volumes are presented as SMB shares to Microsoft Windows clients. Several SMB 3.0 features are currently supported; a later release will provide full SMB 3.0 support.
- **FUSE:** SOFS volumes are presented as a local Linux file system.
- **Cloud Data Management Interface (CDMI) and REST:** The Storage Networking Industry Association (SNIA) CDMI REST interface is supported, with full compatibility with SOFS file data.
- **S3 on SOFS:** SOFS volumes can be accessed in read-only mode over the S3 protocol for name space and data sharing between objects and files.
- **NFSv4 and v3 on S3:** S3 buckets can be exported as NFSv4 and v3 mount points.

Connectors provide storage services for reading, writing, deleting, and looking up objects and files stored in RING based on either object or POSIX (file) semantics. Applications can use multiple connectors in parallel to scale out the number of operations per second, or the aggregate throughput of RING. A RING deployment can be designed to provide a mix of file access and object access (over NFS and S3, for example), simultaneously, to support multiple application use cases.

Storage nodes and I/O daemons

The core of the RING solution are the storage nodes: virtual processes that own and store a range of objects associated with their portion of the RING keyspace. Each physical storage server (host) typically is configured with six storage nodes (called bizstorenodes). Under the storage nodes are the storage daemons (called biziods), which are responsible for the persistence of the data on disk in an underlying local standard disk file system. Each biziod instance is a low-level software process that manages the I/O operations to a particular physical disk drive and maintains the mapping of object keys to the actual object locations on disk. Biziod processes are local to a given server, managing only local, direct-attached storage and communicating only with storage nodes on the same server. The typical configuration is one biziod per physical disk drive, with support for up to hundreds of daemons per server, so the system can support very large, high-density storage servers.

Each biziod stores object payloads and metadata in a set of fixed-size container files on the disk it is managing. With such containerization, the system can maintain high-performance access even to small files without any storage overhead. The biziod daemons typically use low-latency flash (SSD or NVMe) devices to store the index files for faster lookup performance. The system provides data integrity assurance and validation through the use of stored checksums on the index and data container files, which are validated upon read access to the data. The use of a standard file system underneath biziod helps

ensure that administrators can use normal operating system utilities and tools to copy, migrate, repair, and maintain the disk files if required.

The recommended deployment for systems that have both hard-disk drive (HDD) and SSD media on the storage servers is to deploy a data RING on the HDD, and to deploy the associated metadata in a separate RING on the SSD. Typically, the requirements for metadata are approximately 2 percent of the storage capacity of the actual data, so the sizing of the SSD should reflect that percentage for best effectiveness. Scality can provide specific sizing recommendations based on the expected average file sizes and the number of files for a given application.

Scality RING systems management

RING management and monitoring is achieved through a cohesive suite of user interfaces, built on top of a set of REST interfaces called the Supervisor API (SupAPI). The SupAPI provides an API-based method that can be accessed from scripts, tools, and frameworks to gather statistics, metrics, health check probes, and alerts and to provision new services on the RING. The SupAPI also supports role-based access control (RBAC), using the administrator identity to provide access privileges for super-admin and monitor-admin user roles.

RING provides a set of tools that use the SupAPI to access the same information and services. RING 7 includes the new Scality Supervisor, a browser-based portal for both systems monitoring and management of Scality components. In RING 7, the Supervisor provides capabilities across object (S3) and file (NFS, SMB, and FUSE) connectors, with integrated dashboards that include key performance indicators (KPIs) with trend information such as global health, performance, availability, and forecast metrics. The Supervisor also includes provisioning capabilities to add new servers in the system and a new zone management module to handle customer failure domains for multisite deployments. Figure 11 shows the Supervisor GUI.



Figure 11. Supervisor web GUI

RING Supervisor also includes an advanced monitoring dashboard on which all collected metrics can be graphed and analyzed by component and by server. This feature is based on a powerful graphing engine that has access to thousands of metrics.

A new S3 service management console portal is provided to manage the integrated AWS IAM model of S3 multitenancy in the RING (Figure 12). This console provides two-level management of accounts, users and groups, and IAM access-control policies. The S3 console also can easily be customized for white-labeling purposes.

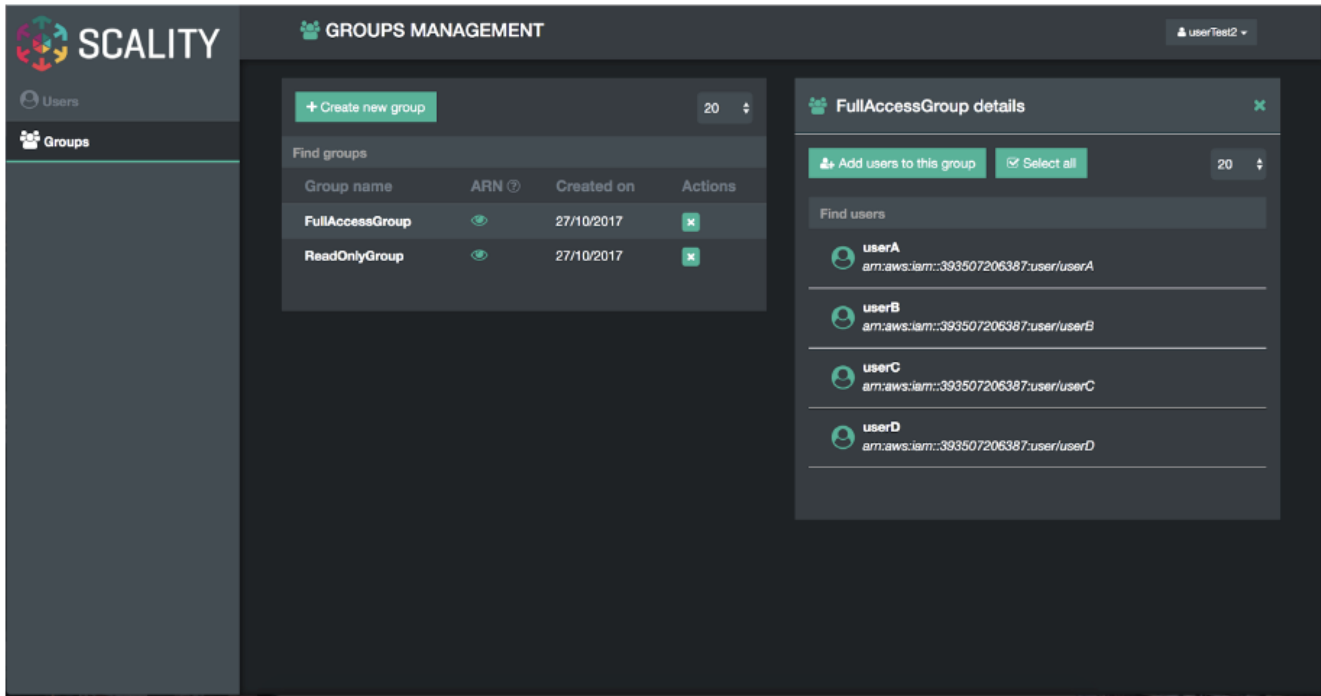


Figure 12.
AWS S3 service management console

A new Scality S3 browser (Figure 13) is provided to browse S3 buckets, upload and download object data, and manage important S3 features such as bucket versioning, cross-origin resource sharing (CORS), editing of metadata attributes, and tagging. The S3 browser is an S3 API client that runs on the S3 user browser and is accessible to both the storage administrator and the S3 end user.

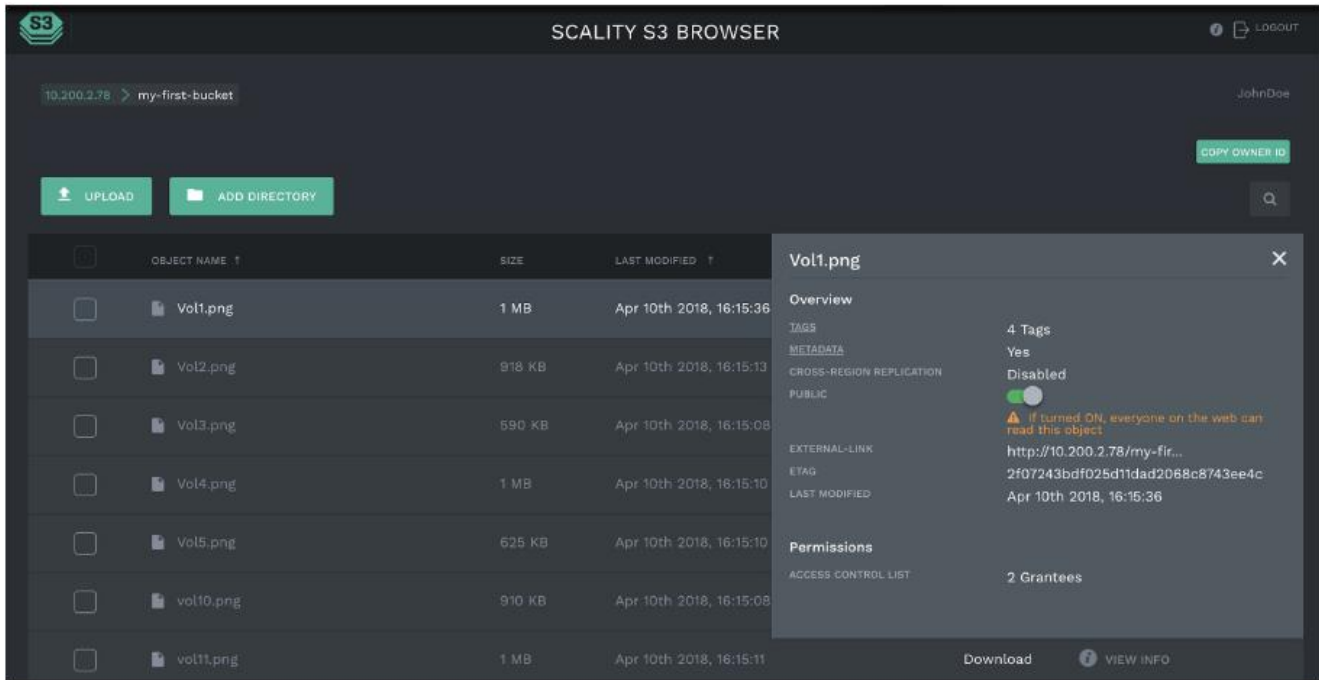


Figure 13.
Scality S3 browser

A scriptable CLI, called RingSH, is also provided, as well as an SNMP-compatible management information base (MIB) and traps interface for monitoring from standard SNMP consoles. RING is designed to be self-managing and autonomous to free administrators to work on other value-added tasks without having to worry about the component-level management tasks common in traditional array-based storage solutions.

AWS S3 connector: AWS S3 storage with identity and access management

The Scality S3 connector provides a modern S3-compatible application interface to RING. The AWS S3 API has become the industry's default cloud storage API and has emerged as the standard REST dialect for object storage, as NFS was for the network-attached storage (NAS) generation of solutions. The S3 connector is built on a distributed scale-out architecture to support heavy application workloads and high concurrent user access. It is based on a highly available, high-performance metadata engine that can also be scaled out for increased performance. Deployments can be geographically replicated deployments to enable highly available disaster-recovery solutions for metro-area network (MAN) environments (stretched deployments) and for cross-region replication (CRR) asynchronous replication of individual S3 buckets or a full site.

The Scality S3 connector also provides a full implementation of the AWS multitenancy IAM model, with federated authentication to Lightweight Directory Access Protocol (LDAP) and Active Directory for integration with enterprise deployment environments. In addition to the RING Supervisor management user interface, the S3 connector offers an S3 service provider user interface, which is a web-based user interface for managing multitenancy accounts, users, groups, and policies. To support enterprise security, development, and operational methodologies, the S3 connector on RING provides the following capabilities:

- Integration with enterprise directory and security servers: The most common integrations is with Microsoft Active Directory and LDAP servers. Federated authentication integration is supported through a Security Assertion Markup Language (SAML) 2.0-compatible identity provider such as

Microsoft Active Directory Federation Services (ADFS), and many other SAML-compatible products, to enable a complete single sign-on (SSO) solution.

- Secure multitenancy support: Secure multitenancy is supported through IAM accounts, secure access keys, users, groups, access-control policies, Signature v4 authentication per tenant, bucket encryption (integrated with corporate AWS Key Management Service [KMS] solutions), and auditing.
- Utilization reporting to enable chargeback: The S3 connector utilization API provides an extended API for reporting on comprehensive use metrics, including capacity, number of objects, bandwidth, and S3 operations (per unit of time). This API provides all the metrics required for consumption by corporate tools for chargeback calculations.
- Cloud-based S3 monitoring: Cloud-based monitoring is integrated through Scality's upcoming cloud monitoring console and load-balancer-driven health checks.
- High-performance, scale-out access: Many corporate applications and workloads can simultaneously read and write to the S3 service.
- Highly-available disaster-recovery solutions: Multiple-data center deployments provide availability in the event of a site failure.

In RING 7, the feature set for the S3 connector now supports bucket versioning through the S3 API. For CRR of buckets through the S3 API, it provides bucket-level asynchronous replication to another S3 RING deployment.

SOFS: Scality Scale-Out File System

RING supports native file system access to RING storage through the integrated SOFS file system, with NFS, SMB, and FUSE connectors for access over these well-known file protocols. SOFS is a POSIX-compatible, parallel file system that provides file storage services on RING without the need for external gateways.

SOFS is more precisely a virtual file system based on an internal distributed database, MESA (meaning "table" in Spanish), on top of the RING storage services. MESA is a distributed, semistructured database that is used to store the file system directories and file index node (inode) structures. It provides a virtual file system hierarchical view with the consistency required for file system data by making sure that file system updates always are atomic. This means that updates are either committed or rolled back entirely, thus guaranteeing that the file system is never left in an intermediate or inconsistent state. An important advantage for scaling is that MESA is itself distributed as a set of objects across all the RING storage nodes in a shared-nothing manner to eliminate any bottlenecks or limitations.

File system lookups are performed using RING's standard peer-to-peer routing protocol. For fast access performance, SOFS metadata should be stored in flash storage, typically on its own dedicated SSD drives in the storage servers, with the SOFS file payloads stored in the data RING on HDDs. SOFS works directly with the data protection and durability mechanisms present in RING, including replication and configurable erasure-coding schemas.

SOFS can be provisioned into one or more volumes, and capacity can be scaled as needed to support application requirements. Each volume can be accessed by any number of connectors to support the incoming workload, even with mixed protocols (NFS, SMB, and FUSE). RING can support up to 232 volumes and can grow to billions of files per volume. You do not need to preconfigure volumes for capacity (RING effectively supports thin provisioning of volumes). Volumes will use the RING storage pool to expand

as needed when files are created and updated. For efficient storage of very large files, RING supports the concept of sparse files: effectively files combined from multiple individual data stripes.

Multiple connectors can be used to simultaneously access a volume. RING also currently supports scale-out access for multiple concurrent readers and a new file-access coordination mode that allows multiple readers on a file while it is being written from another connector. This feature is useful in use cases such as video streaming in which very large video files are written over the course of minutes or hours, but the file must be accessed for content distribution before the write process is complete. When multiple connectors attempt to write to the same directory or one per file within a directory, SOFS maintains view consistency across multiple connectors. By supporting a scale-out design across any number of connectors, SOFS throughput can be scaled to support increasing workload demands. When performance saturation is reached, you always can add more connectors or storage nodes (and disk spindles) to RING to increase throughput to the system further. The system can achieve tens of gigabytes per second of aggregate throughput for parallel workloads through this architecture.

SOFS provides volume-level utilization metering and quota support, in addition to user and group (UID and GID) quotas. This feature allows administrators to use the concept of volumes to meter, report, and limit space (capacity) use at the volume level. This capability is useful in a multitenant environment, in which multiple applications or use cases share the same RING, but each accesses data stored in its own volume.

SOFS also provides integrated failover and load-balancing services for the NFS and SMB connectors. The load balancer uses an integrated Domain Name System (DNS) service to expose one or more service names (for example, sofs1.companyname.com) on virtual IP addresses, which can be mounted as NFS mount points or SMB shares. The load balancer can be configured with multiple underlying NFS or SMB connector real IP addresses, and it load-balances file traffic across these SOFS connectors. In combination with the RING 6.0 folder scale-out feature, the load balancer provides transparent multiconnector access to a single folder and enables failover. If one of the underlying NFS or SMB connectors becomes nonresponsive, the load balancer can select another connector IP address as the access point for the request.

Intelligent data durability and self-healing

RING is designed to expect and manage a wide range of component failures, including failures of disks and server networks and even across multiple data centers, while helping ensure that data remains durable and available during these conditions. RING provides data durability through a set of flexible data protection mechanisms optimized for distributed systems, including replication, erasure coding, and geographically distributed replication, that allow applications to select the best protection strategies for their data. These flexible data protection mechanisms implement Scality's design principle of addressing a wide spectrum (80 percent) of storage workloads and data sizes. Multisite data protection is discussed in detail later in this document, in the section "Scality RING multisite deployments."

Replication class of service

To optimize data durability in a distributed system, RING employs local replication, or the storage of multiple copies of an object within the RING. RING will attempt to spread these replicas across multiple storage nodes and across multiple disk drives to separate them from common failures (assuming sufficient numbers of servers and disks are available). RING supports six class-of-service (CoS) levels for replication (0 through 5), indicating that the system can maintain from 0 to 5 replicas (or 1 to 6 copies) of an object. This approach allows the system to tolerate up to five simultaneous disk failures, while still preserving access to and storage of the original object. Note that any failure will cause the system to self-heal the lost replica, to automatically bring the object back up to its original CoS as fast as possible.

Although replication is well suited to many use cases in which the objects are small and access performance is critical, it does impose a high storage overhead penalty compared to the original data. For example, a 100-KB object being stored with a CoS of 2 (2 extra copies, so 3 total), will therefore consume $3 \times 100 \text{ KB} = 300 \text{ KB}$ of actual physical capacity on RING to maintain its 3 replicas. This overhead is acceptable in many cases for small objects, but it can become a costly burden for megabyte- or gigabyte-level video and image objects. For example, a penalty of 200 percent is exacted to store a 1-GB object, because 3 GB of underlying raw storage capacity are required for the 3 replicas. When measured across objects totaling petabytes of data, this penalty becomes a significant cost burden for many businesses, requiring a more efficient data protection mechanism.

Flexible erasure coding

Scality's erasure-coding (EC) data protection mechanism provides an alternative to replication that is optimized for large objects and files. RING implements Reed-Solomon erasure-coding techniques to store large objects with an extended set of parity chunks instead of multiple copies of the original object. The basic approach of erasure coding is to break an object into multiple chunks (m) and apply mathematical encoding to produce an additional set of parity chunks (k). A description of the mathematical encoding is beyond the scope of this document, but EC can be simply explained as an extension of the XOR parity calculations used in traditional RAID. The resulting set of chunks, $(m + k)$ are then distributed across the RING nodes, providing the capability to access the original object as long as any subset of m data or parity chunks is available. Stated another way, EC provides a way to store an object with protection against k failures with only k/m overhead in storage space.

Many commercial storage solutions impose a performance penalty on the reading of objects stored through erasure coding, because all the chunks, including the original data, are encoded before they are stored. This characteristic requires mandatory decoding on all access to the objects, even when there are no failure conditions on the main data chunks. With Scality's EC mechanism, the data chunks are stored in the clear, without any encoding, so this performance penalty is not present during normal read accesses. This approach means that EC data can be accessed as quickly as other data, unless a data chunk is missing, in which case a parity chunk must be accessed and decoded.

Use of replication and erasure coding together

In summary, for single-site data protection, Scality's replication and EC data protection mechanisms can provide very high-levels of data durability, with the capability to trade off performance and space characteristics for different data types.

Note that replication and EC can be combined, even on a single connector, by configuring a policy for the connector to store objects below a certain size threshold with a replication CoS, and to store files above the file size limit with a specific EC schema. This capability allows the application to simply store objects, without the need for the administrator to consider the optimal storage strategy for each object because the system manages that automatically.

Note also that RING does not employ traditional RAID-based data protection techniques. Although RAID served the industry well in traditional NAS and SAN systems, industry experts have written about the inadequacies of classical RAID technologies when employed on high-density disk drives and in capacity-optimized and distributed storage systems. These deficiencies include higher probabilities of data loss due to long RAID rebuild times, and the capability to protect against only a limited set of failure conditions (for example, only two simultaneous disk failures per RAID 6 group). Additional information about the limitations of RAID as a data protection mechanism on high-capacity disk drives is widely available.

Self-healing capability

RING provides self-healing processes that monitor and automatically resolve component failures. These processes include the capability to rebuild missing data chunks resulting from disk drive and server failures, rebalance data when nodes leave and join the RING, and serve proxy requests related to component failures. If a disk drive or even a full server fails, background rebuild operations are spawned to restore the missing object data from its surviving replicas or EC chunks. The rebuild process is complete when it has restored the original CoS: either the full number of replicas or the original number of EC data and parity chunks. A local disk failure can also be repaired quickly on a node (distinct from a full distributed rebuild) through the use of an in-memory key map maintained on each node. Nodes are also responsible for automatically detecting mismatches in their own keyspaces, rebalancing keys and establishing and removing proxies during node addition and departure operations. Self-healing provides RING with the resiliency required to maintain data availability and durability in the event of a wide set of failure conditions, including multiple simultaneous component failures at the hardware and software levels.

To optimize rebuild as well as main-line I/O performance during rebuild operations, RING uses the distributed power of the entire storage pool. The parallelism of the underlying architecture pays dividends by eliminating any central bottlenecks that might otherwise limit performance or cause contention between processes servicing application requests and normal background operations such as rebuilding, especially when the system is under load. To further optimize rebuild operations, the system repairs only the affected object data, not the entire set of disk blocks, as is commonly the case in RAID arrays. Rebuild operations are distributed across multiple servers and disks in the system to use the aggregate processing power and available I/O of multiple resources in parallel, rather than serializing the rebuild operations on a single disk drive.

By using the entire pool, the impact of rebuilding data stored either with replication or EC is reduced, because there will be relatively little overlap between the disks involved in servicing data requests and those involved in the rebuild operation.

Scality RING multisite deployments

To support deployments that span multiple data centers with site protection and complete data consistency between all sites, RING natively supports a stretched (synchronous) deployment mode across sites. In this mode, a single logical RING is deployed across multiple data centers, with all nodes participating in the standard RING protocols as if they were local to one site.

When a stretched RING is deployed with EC, it provides multiple benefits, including full site-level failure protection, active-active access from both data centers, and dramatically reduced storage overhead compared to a mirrored RING. An EC schema for a three-site stretched RING of EC (7,5) provides protection against one complete site failure, or up to four disk or server failures per site plus one additional disk or server failure in another site, with approximately 70 percent space overhead. This approach compares favorably to a replication policy, which might require 300 to 400 percent space overhead for a similar level of protection across these sites.

Multisite deployments are supported for both the SOFS file system and SWS S3 objects.

SOFS multisite geographical distribution

Scality RING can be stretched across two or three sites within a MAN to provide full site failover when the latency between the several sites exceeds 10 ms. The stretched architecture provides RTO and RPO values of 0, because the failover is automated. This is also true for the failback procedure, because when the lost site is recovered, the system recovers the data automatically. For the two-site stretched architecture only, to manage the migration between the two sites, two witness servers are needed.

The two stretched sites and the witness site form an active-active replication system using synchronous replication (Figure 14).

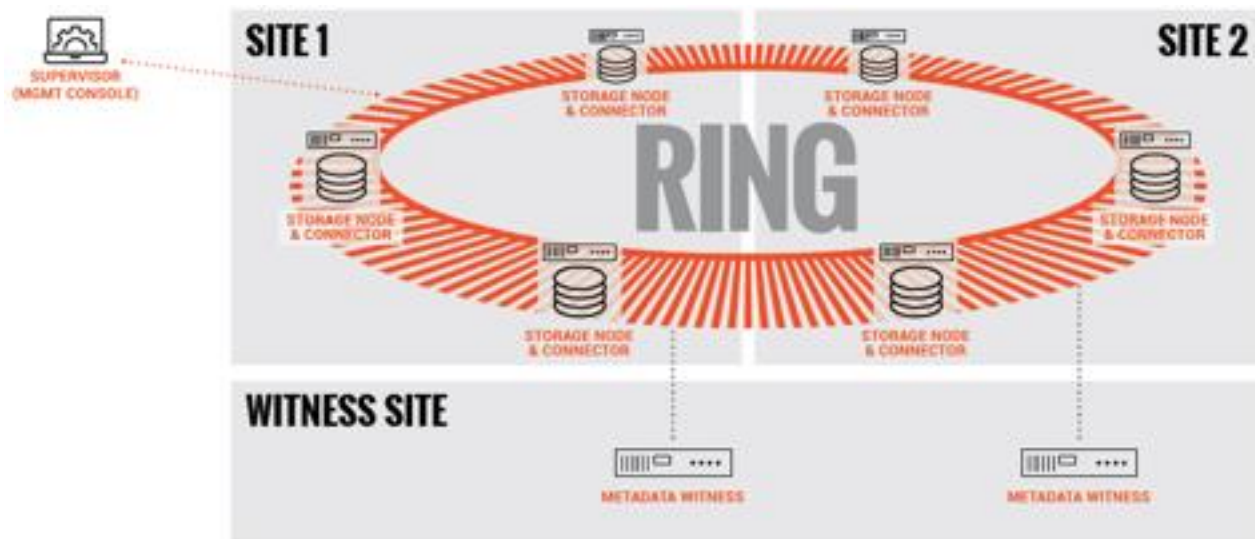


Figure 14.
SOFS: Two-site stretched

The three stretched sites form an active-active replication system using synchronous replication (Figure 15).

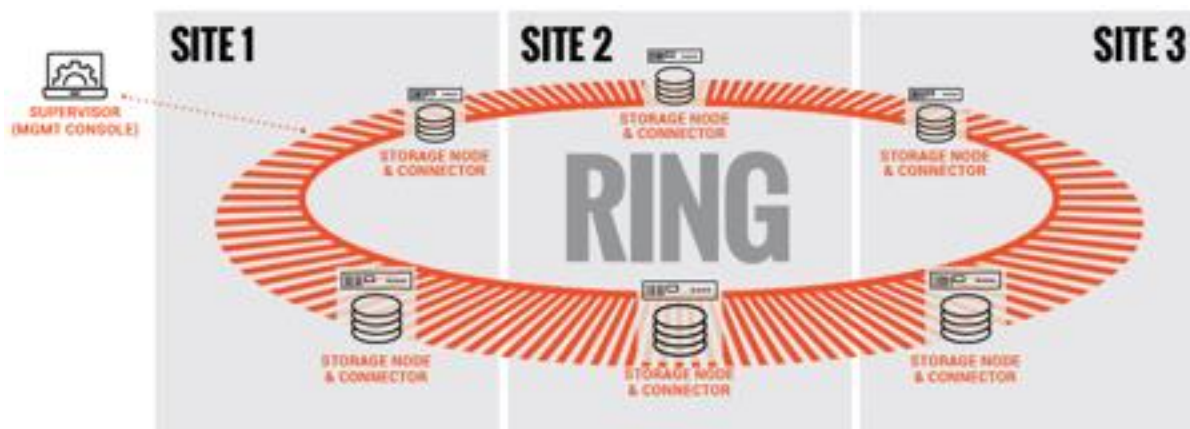


Figure 15.
SOFS: Three-site stretched

For high latency between sites, Scality supports an SOFS two-site full asynchronous replication mechanism at scale to enable the replication of massive amounts of file data across the two sites. Scality also supports a full differential mechanism that can compare at scale the content of the two sites to help ensure that the data is effectively replicated. If one site is fully lost, Scality provides a mechanism to fully reconstruct the lost site.

To manage the replication traffic burst, Scality integrates a back-pressure system to help ensure that the production network link isn't overloaded by the replication process itself and at the same time respects the RPO defined during the installation setup process. This feature enables disaster recovery by providing failover and enabling the failback system to recover in the case of a partial or full loss.

The two sites with high latency between them form an active-standby replication system using asynchronous replication (Figure 16).



Figure 16.
SOFS: Two-site asynchronous replication

AWS S3 object multisite geographic distribution

The same multisite architectures are supported for S3 as for SOFS: both synchronous and asynchronous. A stretched solution on two or three sites has RPO and RTO values of 0. As for SOFS, a stretched architecture is available within a MAN to provide full site failover when the latency between the several sites exceeds 10 ms. For the two-site stretched architecture only, to manage the migration between the two sites, two witness servers are needed.

The two stretched sites and witness site form an active-active replication system using synchronous replication (Figure 17).

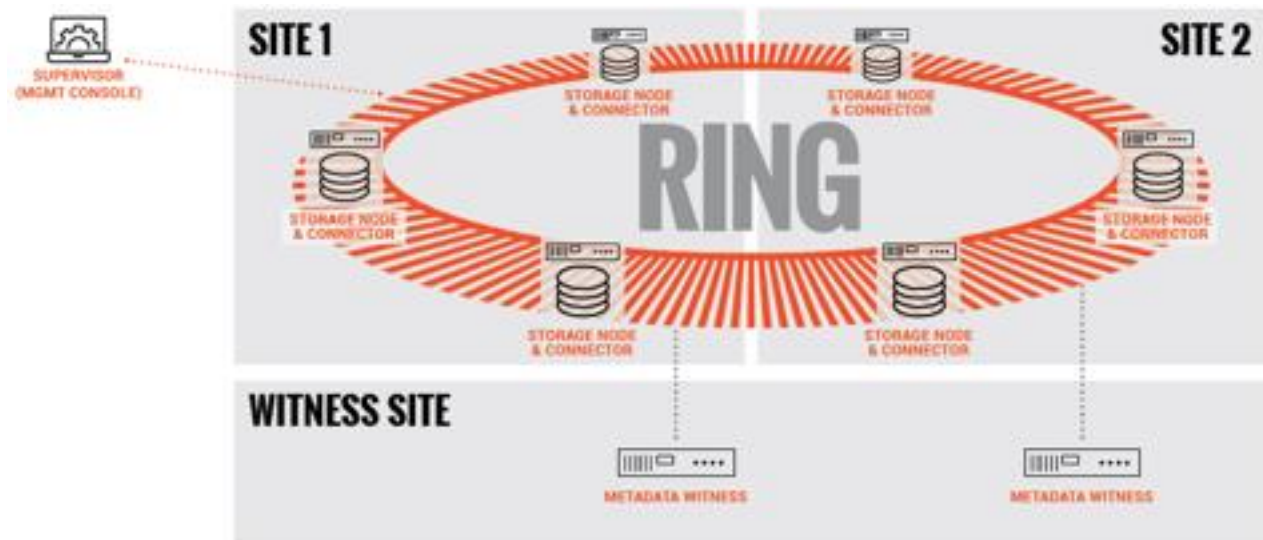


Figure 17.
AWS S3: Two-site stretched

The three stretched sites form an active-active replication system using synchronous replication (Figure 18).

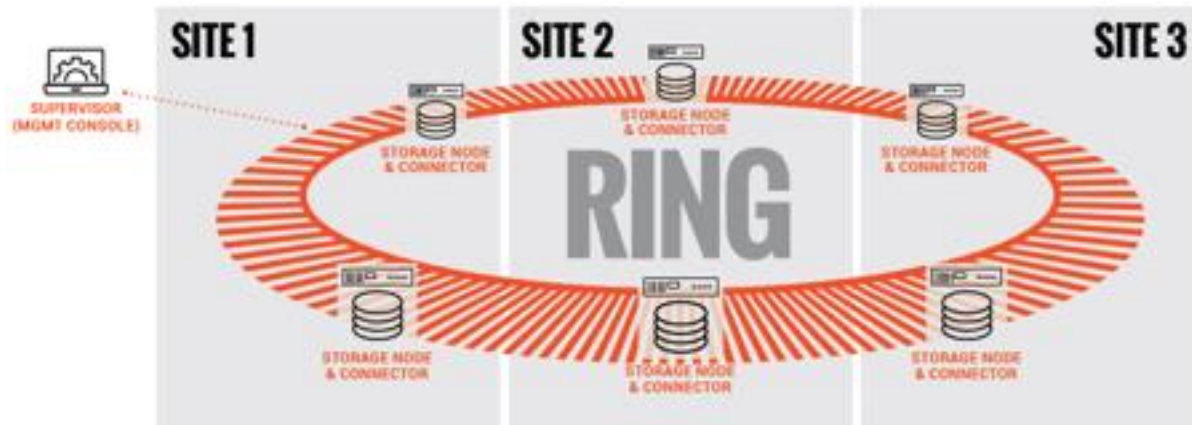


Figure 18.
AWS S3: Three-site stretched

For high latency between sites (such as sites on a WAN), Scality supports an S3 two-site full asynchronous replication mechanism at scale to enable the replication of massive amounts of data across the two sites. This system is based on the S3 CRR design to replicate a bucket between two sites. For site replication, Scality developed its own system to support site replication instead of replication of just a bucket. This feature enables disaster recovery by providing failover and enabling the failback system to recover in the case of a partial or full loss (from flooding, fire, etc.).

The two sites with high latency between them form an active-standby replication system using asynchronous replication (Figure 19).



Figure 19.
AWS S3: Two-site asynchronous replication

Solution design

For you to follow the configuration steps in this document, your system must have the following components installed and configured:

- Veeam Backup & Replication installed on Cisco UCS C240 M5 Rack Server or Cisco UCS S3260 Storage Server
- Scality RING installed on Cisco UCS C240 M5 Rack Server or Cisco UCS S3260 Storage Server

Documents for installing the components

Consult the following documents for detailed guidance in installing the components:

- Installing Veeam on Cisco UCS: <https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/whitepaper-c11-741589.pdf>
- Installing Scality RING on Cisco UCS: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_c240m5_scalityring.pdf

Configuring Scality RING

To connect Veeam Backup & Replication to Scality RING, you first need to perform some configuration steps, such as creating a user. This section presents these configuration steps.

These are the main steps:

- Create an account for Veeam in the S3 console and create an access key and secret access key.
- Create a bucket.

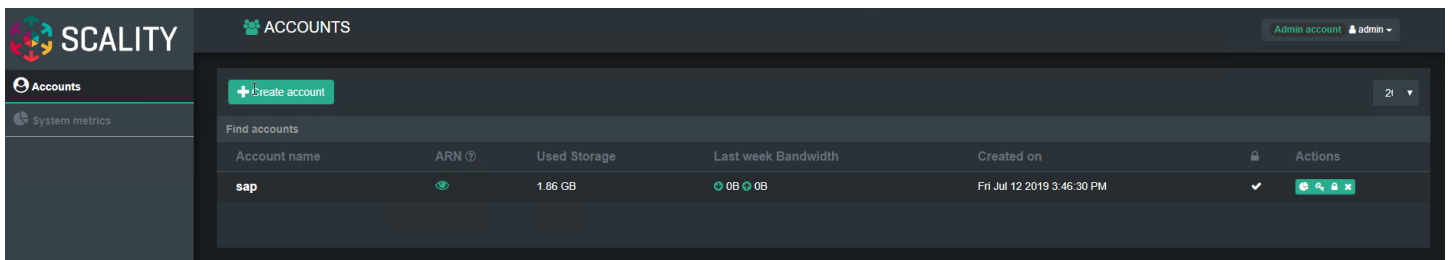
Create an account

You first create an account in the S3 console of Scality RING.

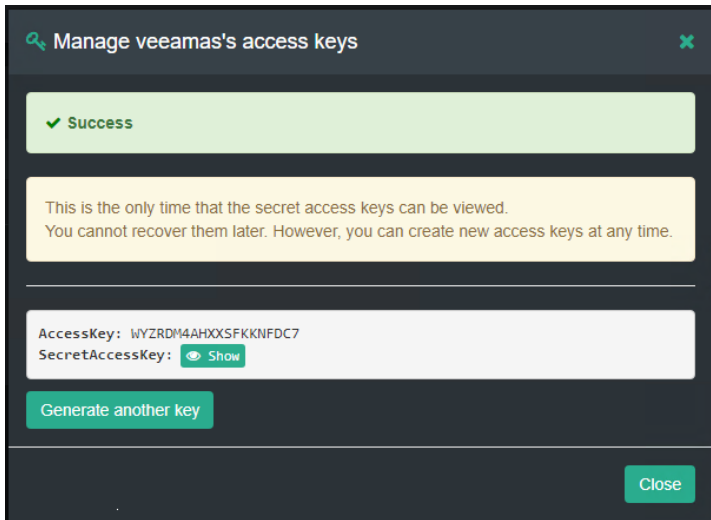
1. Connect to the S3 console as admin.



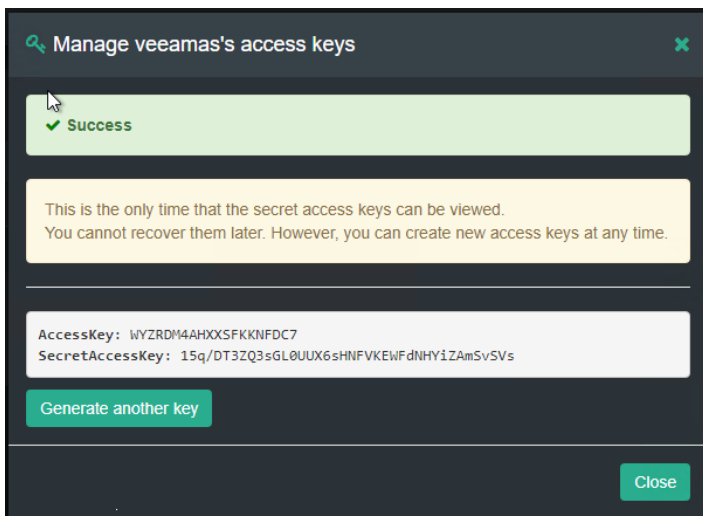
2. Click Create Account.



7. Click Show to see the secret access key.



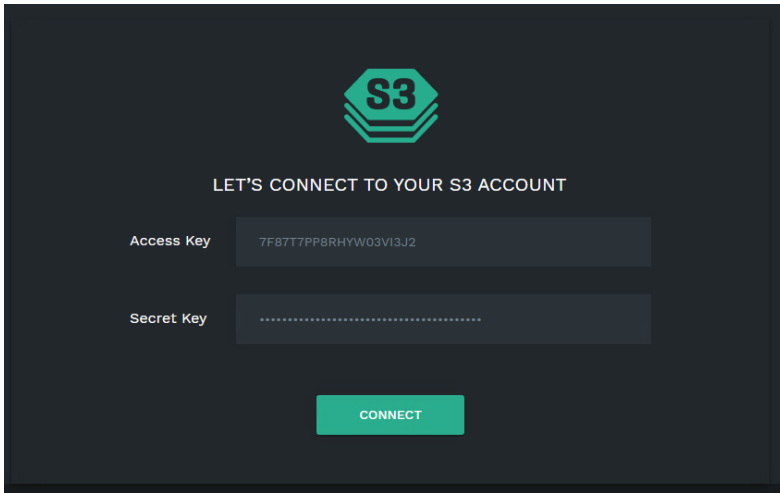
8. Copy the access key and secret access key to a secure place. This information is required to configure Veeam Backup & Replication. Then click Close.



Create an AWS S3 bucket

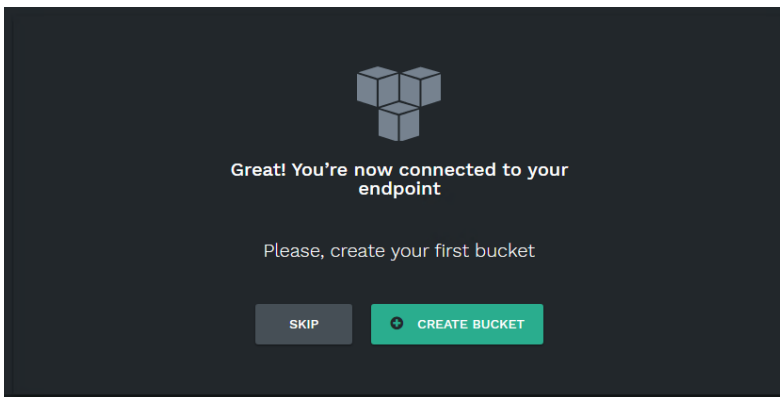
Within the created account, you need to create an S3 bucket for use by Veeam Backup & Replication.

1. Log on to the S3 browser with the new access key and secret key.



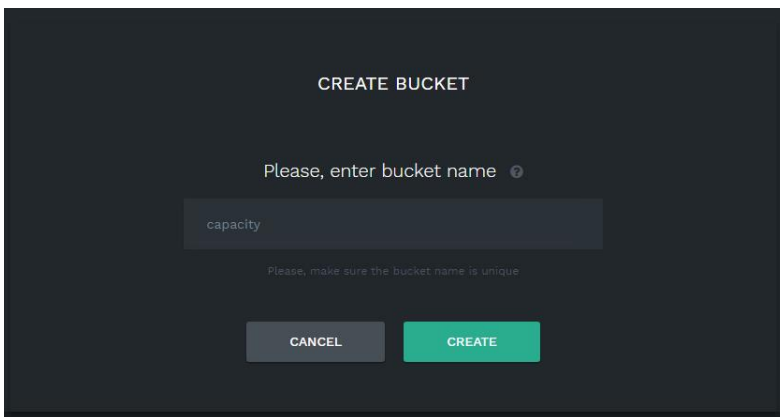
The screenshot shows a dark-themed interface for connecting to an S3 account. At the top center is a logo consisting of a green hexagon with the letters 'S3' inside, and three horizontal lines below it. Below the logo, the text 'LET'S CONNECT TO YOUR S3 ACCOUNT' is displayed. There are two input fields: 'Access Key' with the value '7F8T7PP8RHYW03V13J2' and 'Secret Key' with a masked value of dots. A green 'CONNECT' button is positioned at the bottom center.

2. Click Create Bucket.



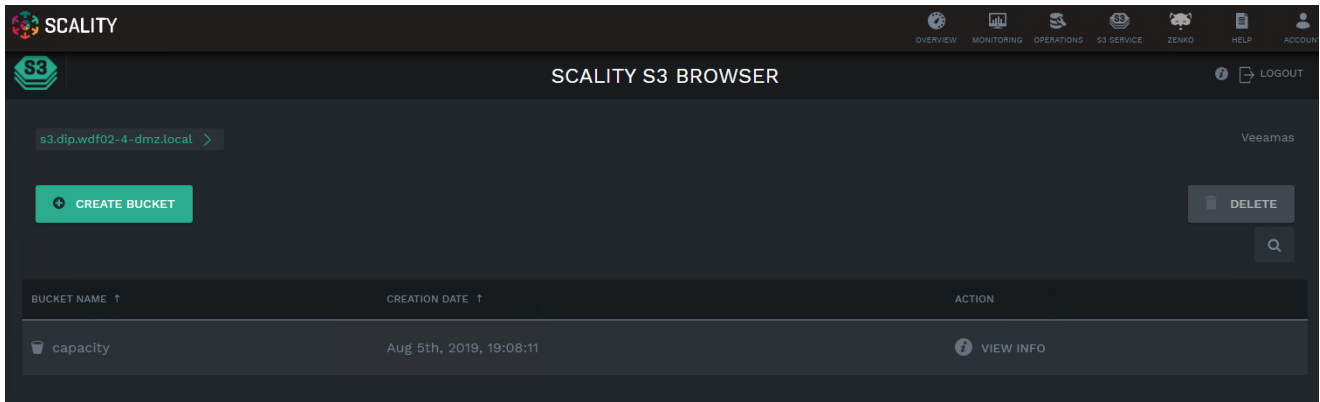
The screenshot shows a dark-themed interface with a confirmation message. At the top center is a logo of three stacked cubes. Below it, the text reads 'Great! You're now connected to your endpoint'. Underneath, it says 'Please, create your first bucket'. At the bottom, there are two buttons: a grey 'SKIP' button and a green 'CREATE BUCKET' button with a plus icon.

3. Enter a name and click Create.



The screenshot shows a dark-themed interface for creating a bucket. The title 'CREATE BUCKET' is at the top. Below it, the text says 'Please, enter bucket name' with a help icon. There is a text input field containing the word 'capacity'. Below the input field, a small note reads 'Please, make sure the bucket name is unique'. At the bottom, there are two buttons: a grey 'CANCEL' button and a green 'CREATE' button.

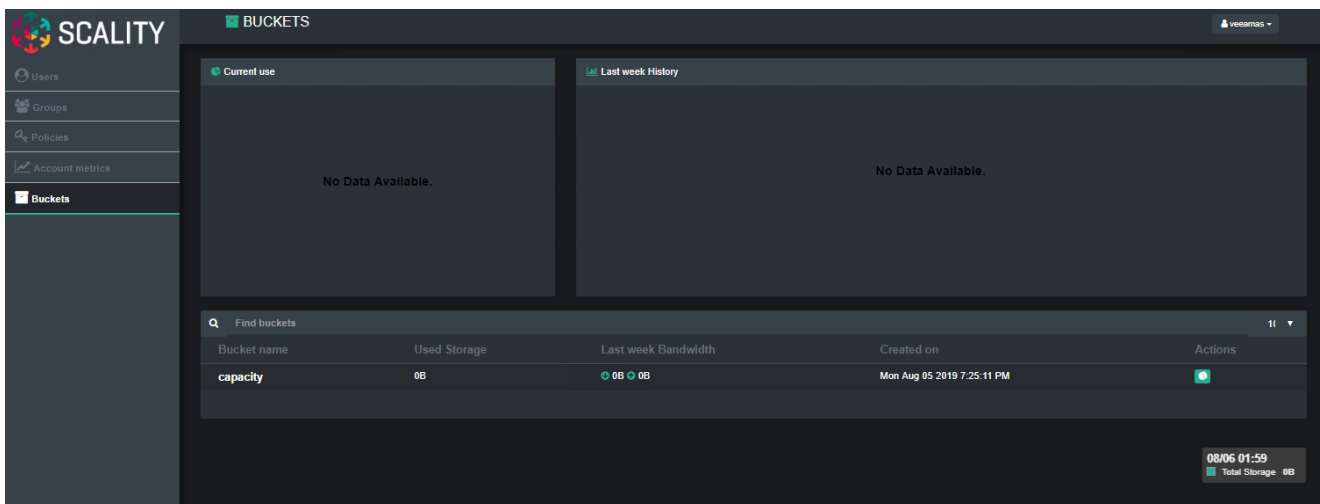
4. Log out of the S3 browser.



5. To monitor the use of the S3 bucket you created, log on to the S3 console with the created user name and password. In this example, the user is veeamas.



6. Click Buckets.



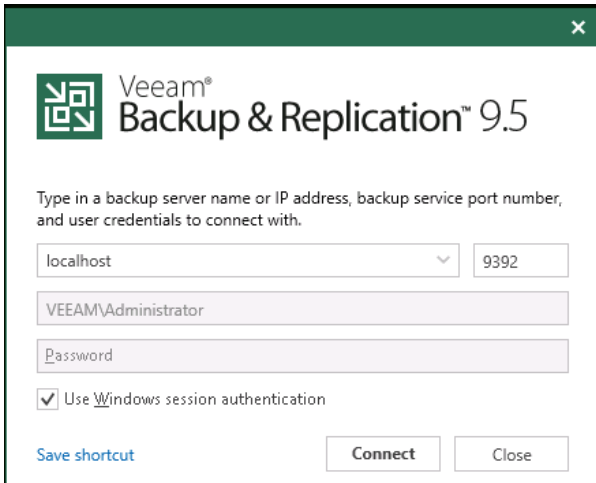
Configure Veeam Backup & Replication

With Scalify RING now prepared to accept connections and data from Veeam Backup & Replication, you can configure Veeam.

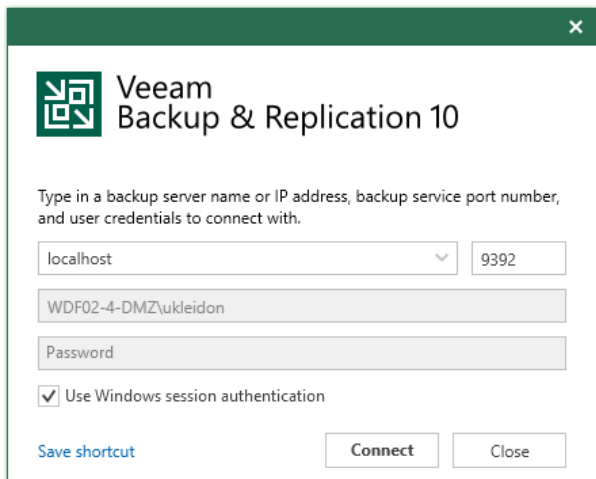
Create a backup repository

The first step is to configure a backup repository for the Scalify RING bucket.

1. Open the Veeam Backup & Replication console. The screen you see depends whether you are using Veeam 9.5 or Veeam 10. In either case, click Connect.



The screenshot shows the Veeam Backup & Replication 9.5 connection dialog. It features a green header with the Veeam logo and the text "Veeam Backup & Replication 9.5". Below the header, there is a prompt: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." The form includes a dropdown menu for the server name (set to "localhost"), a text box for the port number (set to "9392"), a text box for the user name (set to "VEEAM\Administrator"), and a password field. A checkbox labeled "Use Windows session authentication" is checked. At the bottom, there are three buttons: "Save shortcut", "Connect", and "Close".



The screenshot shows the Veeam Backup & Replication 10 connection dialog. It features a green header with the Veeam logo and the text "Veeam Backup & Replication 10". Below the header, there is a prompt: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." The form includes a dropdown menu for the server name (set to "localhost"), a text box for the port number (set to "9392"), a text box for the user name (set to "WDF02-4-DMZ\ukleidon"), and a password field. A checkbox labeled "Use Windows session authentication" is checked. At the bottom, there are three buttons: "Save shortcut", "Connect", and "Close".

2. Click Backup Infrastructure, Backup Repositories, and Add Repository.

veeam1.pod6.wdf02--

REPOSITORY TOOLS

HOME

BACKUP REPOSITORY

Add Repository Manage Repository Edit Repository Rescan Tools Upgrade

BACKUP INFRASTRUCTURE

Backup Proxies

Backup Repositories

External Repositories

Scale-out Repositories

Scale-Out-BR

WAN Accelerators

Service Providers

SureBackup

Application Groups

Virtual Labs

Managed Servers

VMware vSphere

Microsoft Windows

HOME

INVENTORY

BACKUP INFRASTRUCTURE

STORAGE INFRASTRUCTURE

TAPE INFRASTRUCTURE

FILES





Type in an object name to search for

NAME ↑	TYPE	HOST	PATH
Default Backu...	Windows	veeam1.pod...	D:\Backup
veeam1-br	Windows	veeam1.pod...	D:\Repository
veeam2-br	Windows	veeam2.pod...	D:\Repository
veeam3-br	Windows	veeam3.pod...	D:\Repository
veeam4-br	Windows	veeam4.pod...	D:\Repository

3. Click Object Storage.

Add Backup Repository

Select the type of backup repository you want to add.





-  **Direct attached storage**
Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.
-  **Network attached storage**
Network share on a file server or a NAS system. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.
-  **Deduplicating storage appliance**
Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.
-  **Object storage**
On-prem object storage system or a cloud object storage provider. Object storage based repositories can only be used for Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

Cancel

4. Click S3 Compatible.

Object Storage

Select the type of object storage you want to use as a backup repository.

-  **S3 Compatible**
Adds an on-premises object storage system, or a cloud object storage provider.
-  **Amazon S3**
Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.
-  **Microsoft Azure Blob Storage**
Adds Microsoft Azure blob storage. Both hot and cold storage tiers are supported.
-  **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.

Cancel

5. Enter a name for the backup repository and, optionally, a description. Then click Next.

The screenshot shows the 'New Object Storage Repository' dialog box with the 'Name' step selected. The 'Name' field contains 'Scality-RING' and the 'Description' field contains 'Scality RING on Cisco UCS C240 M5'. The 'Next >' button is highlighted.

6. Enter the HTTP address of Scality RING as the service point and click Add beside the Credentials field.

The screenshot shows the 'New Object Storage Repository' dialog box with the 'Account' step selected. The 'Service point' field contains 'https://s3.dip.wdf02-4-dmz.local/'. The 'Region' field contains 'us-east-1'. The 'Credentials' field is empty, and the 'Add...' button is visible. The 'Use the following gateway server' checkbox is unchecked, and the 'veeam1.pod6.wdf02-4-dmz.local' gateway server is listed below.

7. Enter the access key and secret access key you previously created in Scalify RING and click OK.

Access key: 7F87T7PP8RHYW03V13J2
Secret key:
Description:
Access Key for veeamas on the Scalify RING
OK Cancel

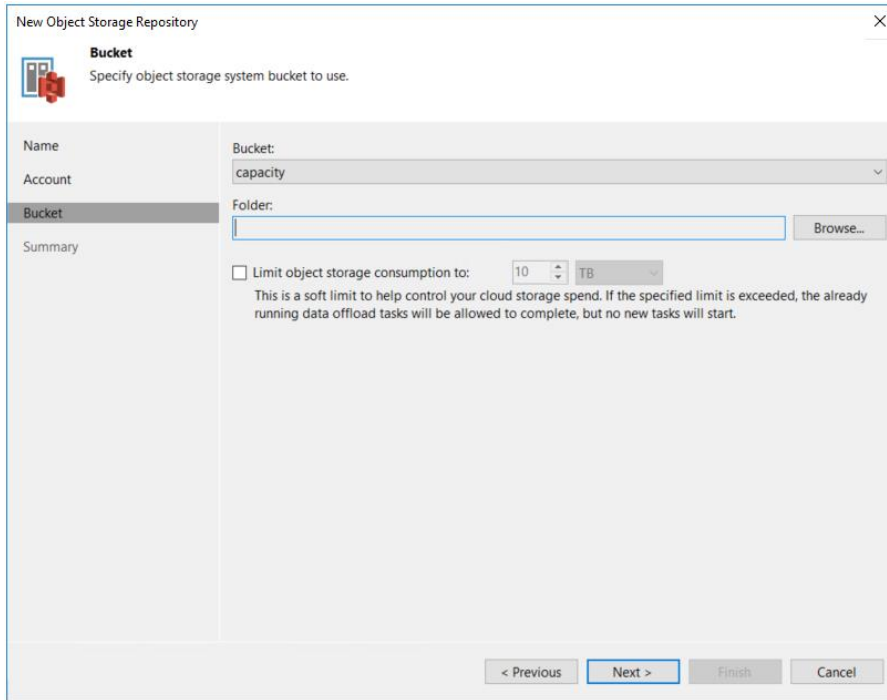
8. Click Next.

New Object Storage Repository
Account
Specify account to use for connecting to S3 compatible storage system.
Name
Account
Bucket
Summary
Service point:
https://s3.dip.wdf02-4-dmz.local/
Region:
us-east-1
Credentials:
7F87T7PP8RHYW03V13J2 (Access Key for veeamas on the Scalify RING, last edited: less) Add...
Manage cloud accounts
Use the following gateway server:
veeam1.pod6.wdf02-4-dmz.local
Select a gateway server to proxy access to the object storage system. If no gateway server is specified, all scale-out backup repository extents must have direct network access to the storage system.
< Previous Next > Finish Cancel

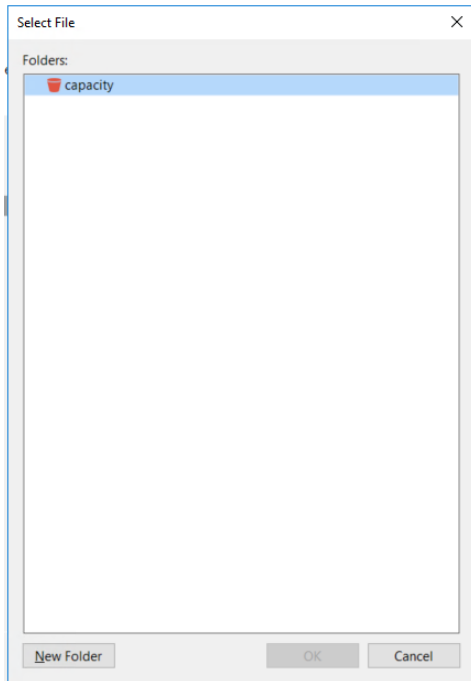
9. If the security certificate used in Scalify RING is not an official one, you will be prompted to accept the insecure certificate by clicking Continue.

Certificate Security Alert
Site certificate cannot be verified. Continue anyway?
Remote certificate chain errors:
UntrustedRoot (A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.)
View... Continue Cancel

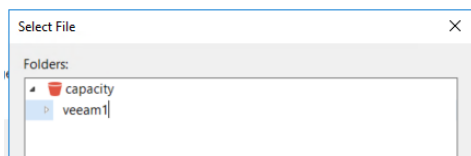
10. The bucket created in Scalify RING is automatically picked. Click Browse beside the Folder field.



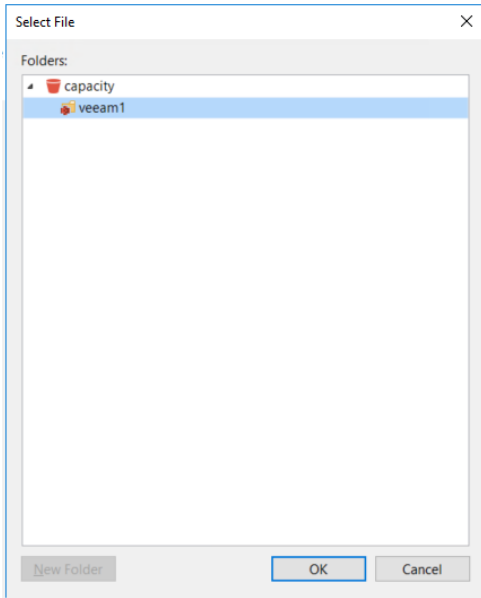
11. Click New Folder.



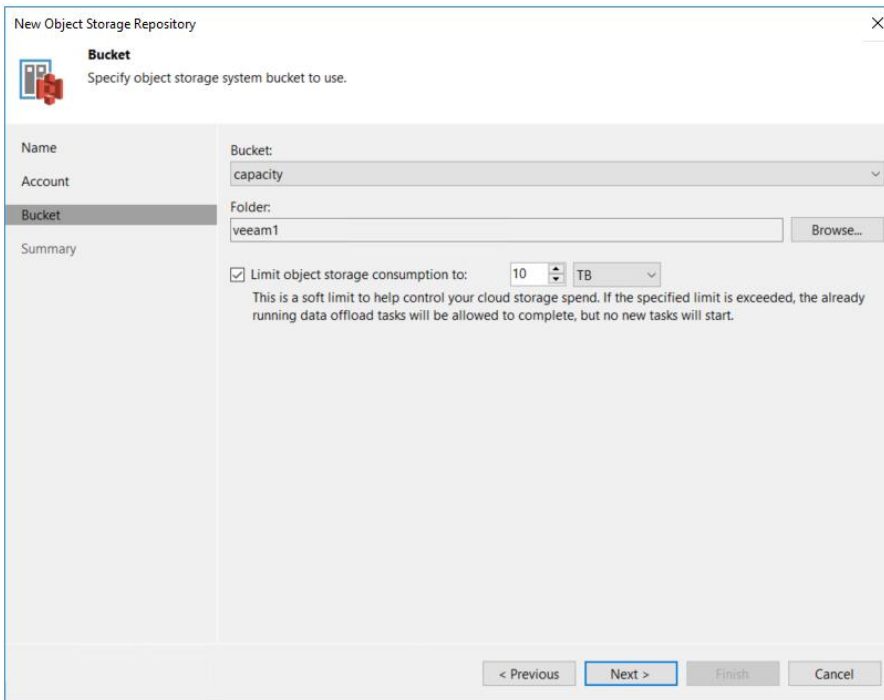
12. Enter a name for the folder and press Return.



13. Click OK.



14. As a best practice, limit the storage used for each backup repository. For example, you can limit the capacity to 10 TB as shown here. Click Next.



15. Click New.

New Object Storage Repository
✕

Summary
You can copy the configuration information below for future reference.

Name

Account

Bucket

Summary

Summary:

Object storage repository was successfully created.

Name: Scality-RING

Description: Scality RING on Cisco UCS C240M5

Type: S3-compatible

Gateway server: not selected

Service point: https://s3.dip.wdf02-4-dmz.local/

Region: us-east-1

Bucket: capacity

Storage consumption limit: 10.0 TB

< Previous
Next >
Finish
Cancel

16. The new backup repository is now listed.

veeam1.pod6.wdf02-4-dmz.local - VEEAM BACKUP AND REPLICATION

Add Repository
Edit Repository
Rescan
Upgrade

BACKUP INFRASTRUCTURE

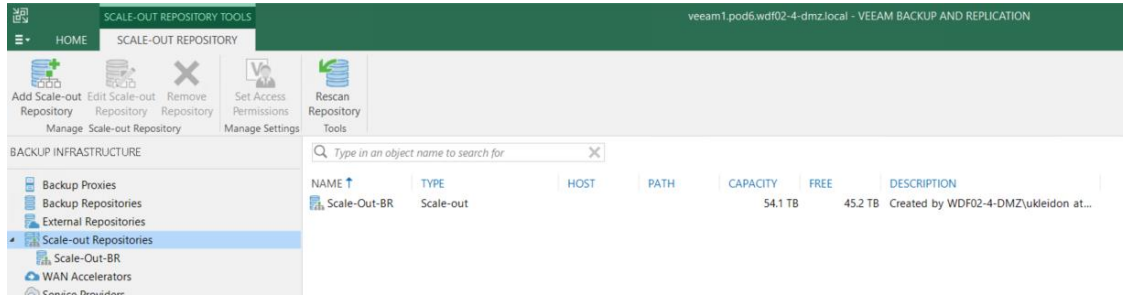
- Backup Proxies
- Backup Repositories**
- External Repositories
- Scale-out Repositories
- Scale-Out-BR
- WAN Accelerators
- Service Providers
- SureBackup
 - Application Groups
 - Virtual Labs
- Managed Servers
 - VMware vSphere
 - Microsoft Windows

NAME ↑	TYPE	HOST	PATH	CAPACITY	FREE	USED SPACE	DESCRIPTION
Default Backu...	Windows	veeam1.pod...	D:\Backup	54.1 TB	45.2 TB	0.0 B	Created by Veeam Backup
Scality-RING	S3-compatible		amazonS3://s3.dip.wdf02-4-dmz.local/capacity/Vee...	N/A	N/A	0.0 B	Scality RING on Cisco UCS C240M5
veeam1-br	Windows	veeam1.pod...	D:\Repository	54.1 TB	45.2 TB	9.9 TB	Created by WDF02-4-DMZ\ukleidon at...
veeam2-br	Windows	veeam2.pod...	D:\Repository	49.1 TB	49.0 TB	0.0 B	Created by WDF02-4-DMZ\ukleidon at...
veeam3-br	Windows	veeam3.pod...	D:\Repository	49.1 TB	49.0 TB	0.0 B	Created by WDF02-4-DMZ\ukleidon at...
veeam4-br	Windows	veeam4.pod...	D:\Repository	54.1 TB	53.9 TB	0.0 B	Created by WDF02-4-DMZ\ukleidon at...

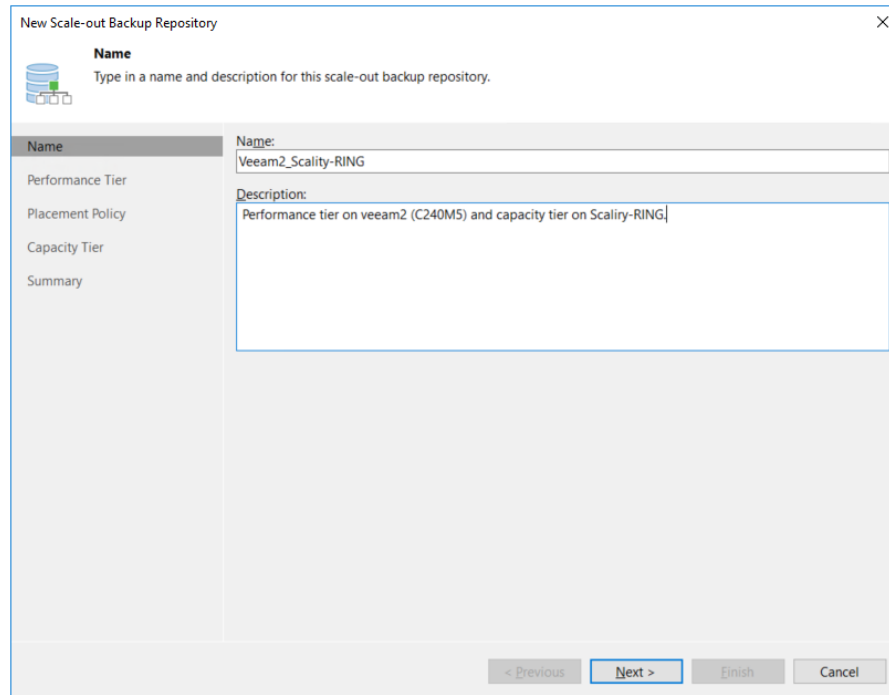
Create a scale-out repository

A Veeam scale-out backup repository is a logical entity consisting of multiple repositories grouped into a single abstracted object. It can be used as a target for any backup job operation and provides an easy way to extend repositories when you run out of space. Backup files are then moved to the capacity tier according to age requirements that you set. Follow these steps to create a scale-out repository.

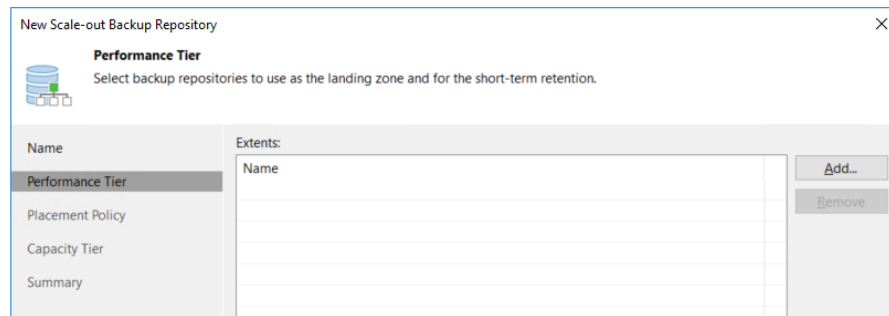
1. Click Scale-Out Repositories and Add Scale-Out Repository.



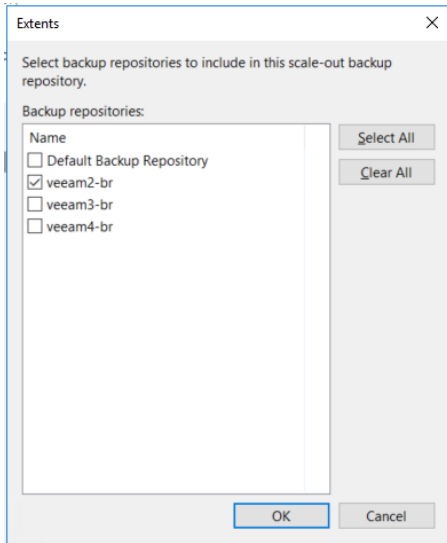
2. Enter a name and description for the repository and click Next.



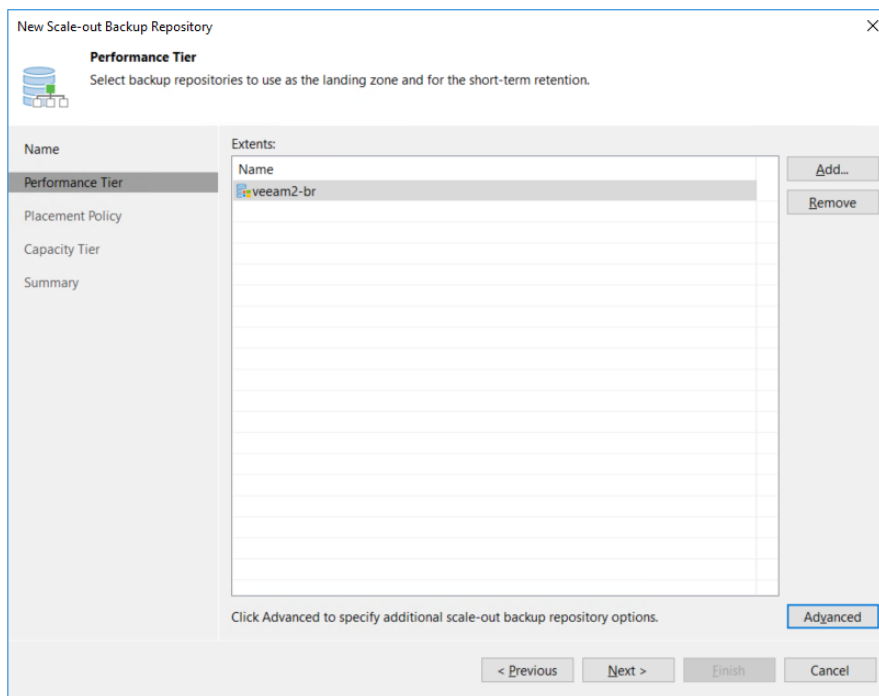
3. Click Add.



4. Select the backup repository used as the performance tier and click OK.



5. Click Next.



6. Select the placement policy that best fits for your use case. In this example, Data Locality is selected. Click Next.

New Scale-out Backup Repository

Placement Policy
Choose a backup files placement policy for this performance tier. When more than one extent matches the placement policy, backup job will chose extent with the most free disk space available.

Name

Performance Tier

Placement Policy

Capacity Tier

Summary

Data locality
All dependent backup files are placed on the same extent. For example, incremental backup files will be stored together with the corresponding full backup file. However, the next full backup file can be created on another extent (except extents backed by a deduplicating storage).

Performance
Incremental backup files are placed on a different extent from the corresponding full backup file, providing for better backup file transformation performance with raw storage devices. Note that losing an extent with a full backup makes restoring from increments impossible.

Specify the placement policy for full and incremental backup files. Customize...

< Previous Next > Finish Cancel

7. Select the box to enable extend the scale-out backup repository and enter the number of days before data is moved to the capacity tier. Click Apply.

You see this screen if you are using Veeam 9.5:

New Scale-out Backup Repository

Capacity Tier
Specify object storage to move your backup files to as they age out of your operational restores window. This reduces your long-term retention costs without sacrificing the ability to perform restore from offloaded backup files.

Name

Performance Tier

Placement Policy

Capacity Tier

Summary

Extend scale-out backup repository capacity with object storage:
Scality-RING Add...

Define time windows when uploading to object storage is allowed Window...

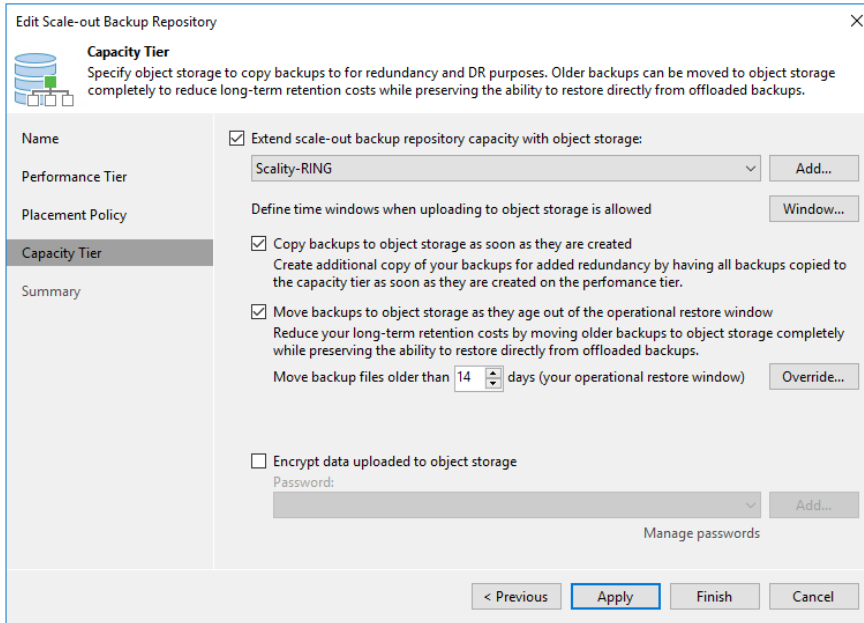
Move backups to object storage as they age out of the operational restores window
Reduce your long-term retention costs by moving older backups to object storage while preserving the ability to restore directly from offloaded backups.

Move backup files older than 7 days (your operational restores window) Override...

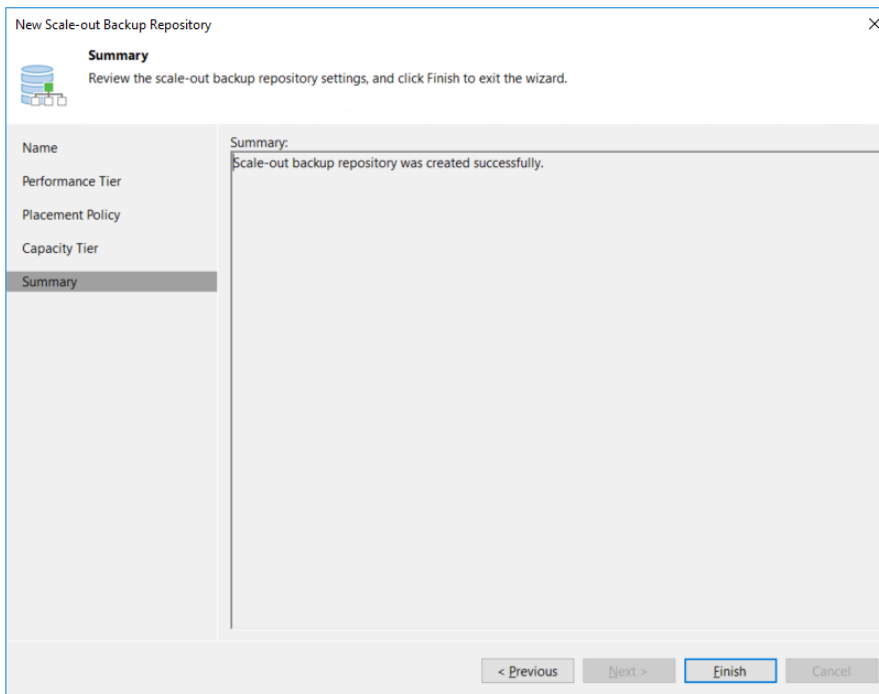
Encrypt data uploaded to object storage
Password: Add...
Manage passwords

< Previous Apply Finish Cancel

You see this screen if you are using Veeam 10:



8. Click Finish.



Veeam also supports the addition of a capacity tier to existing scale-out repositories, not only to new ones.

Configure a backup job

Next you need to configure a backup job using the new scale-out repository.

1. Click Home and then Jobs and then Backup Job and choose Virtual Machine.

The screenshot shows the Veeam Backup and Replication console interface. The top navigation bar includes 'HOME' and 'VIEW'. Below the navigation bar are several icons for 'Backup Job', 'Replication Job', 'Backup Copy Job', 'Restore', 'Failover Plan', 'Import Backup', and 'Export Backup'. The main area displays a list of backup jobs under the 'Jobs' category. The left sidebar shows a tree view with 'Jobs' expanded, and 'Backup' selected. The bottom navigation bar includes 'HOME', 'INVENTORY', 'BACKUP INFRASTRUCTURE', 'STORAGE INFRASTRUCTURE', 'TAPE INFRASTRUCTURE', and 'FILES'.

NAME ↑	TYPE	STATUS	LAST RUN	LAST RESULT	NEXT RUN	DESCRIPTION
__TEST__	VMware Backup	Stopped	127 days a...	Success	<not schedul...	Created by WDF02-4-DMZ\ukleidon at...
POD2-HX-Demo	VMware Backup	Stopped	7 hours ago	Success	8/7/2019 4:0...	Created by WDF02-4-DMZ\ukleidon at...
POD2-HX-Demo_every_2hr	VMware Backup	Stopped	1 hour ago	Success	8/6/2019 12:...	Created by WDF02-4-DMZ\ukleidon at...
POD3-Datahub	VMware Backup	Stopped	12 days ago	Failed	<not schedul...	Created by WDF02-4-DMZ\ukleidon at...
POD3-Infrastructure_VMs	VMware Backup	Stopped	11 hours a...	Success	8/7/2019 12:...	Created by WDF02-4-DMZ\ukleidon at...
RACK5-DMZ	VMware Backup	Stopped	6 days ago	Failed	<Disabled>	Created by WDF02-4-DMZ\ukleidon at...
vhana-cockpit SAP backint backup (Scale-Out-BR)	SAP HANA Backup	Stopped	77 days ago	Success	<not schedul...	SAP HANA backint job
vhana-h01 SAP backint backup (Scale-Out-BR)	SAP HANA Backup	Stopped	50 days ago	Success	<not schedul...	SAP HANA backint job
vhana-h02 SAP backint backup (Scale-Out-BR)	SAP HANA Backup	Stopped	50 days ago	Success	<not schedul...	SAP HANA backint job
vhana-hi3 SAP backint backup (Scale-Out-BR)	SAP HANA Backup	Stopped	19 hours a...	Success	<not schedul...	SAP HANA backint job

2. Enter a name and description and click Next.

The screenshot shows the 'New Backup Job' dialog box with the 'Name' step selected. The 'Name' field contains 'SAP_PRD_Daily_Scale-Out_90days' and the 'Description' field contains 'SAP production systems. Daily backup. Stored on Scale-Out repository. Retention period of 90 days'. The 'Next >' button is highlighted.

Name	Description
SAP_PRD_Daily_Scale-Out_90days	SAP production systems. Daily backup Stored on Scale-Out repository Retention period of 90 days

3. Add the virtual machines protected by this backup job and click Next.

The screenshot shows the 'New Backup Job' dialog box with the 'Virtual Machines' step selected. A table lists the virtual machines to be backed up. The 'Total size' is 820 GB.

Name	Type	Size
SAP Applications	Resource Pool	723 GB
vHANA-H01	Virtual Machine	58.9 GB
vHANA-H02	Virtual Machine	37.1 GB

Total size: **820 GB**

4. Select the scale-out repository you created and enter the number of restore points to keep on disk.

The placement of restore points is defined in the scale-out repository configuration you created earlier. In this example, data will be retained for 7 days on the performance tier and for the remaining 83 days on the capacity tier.

Click Advanced and configure the advanced options for this backup job based on your own best practices and requirements.

You see this screen if you are using Veeam 9.5:

The screenshot shows the 'New Backup Job' dialog box in Veeam 9.5. The 'Storage' tab is selected in the left-hand navigation pane. The main area contains the following settings:

- Backup proxy:** Automatic selection (with a 'Choose...' button).
- Backup repository:** Veeam2_Scality-RING (Performance tier on veeam2 (C240M5) and capacity tier on Scaliry-RING) (with a 'Map backup' link).
- Free space:** 48.9 TB free of 49.1 TB.
- Restore points to keep on disk:** 90 (with an information icon).
- Configure secondary destinations for this job:** An unchecked checkbox with a note: 'Copy backups produced by this job to another backup repository, or to tape. Best practices recommend maintaining at least 2 backups of production data, with one of them being off-site.'
- Advanced settings:** A link labeled 'Advanced' with a gear icon.

At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

You see this screen if you are using Veeam 10:

The screenshot shows the 'New Backup Job' dialog box in Veeam 10. The 'Storage' tab is selected in the left-hand navigation pane. The main area contains the following settings:

- Backup proxy:** VMware Backup Proxy (with a 'Choose...' button).
- Backup repository:** Veeam2-Scalify-RING (Created by WDF02-4-DMZ\ukleidon at 4/21/2020 4:25 PM.) (with a 'Map backup' link).
- Free space:** 36.0 TB free of 54.0 TB.
- Retention policy:** 7 restore points (with an information icon).
- Keep certain full backups longer for archival purposes:** An unchecked checkbox with a 'Configure...' button and a note: 'GFS retention policy is not configured'.
- Configure secondary backup destinations for this job:** An unchecked checkbox with a note: 'Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.'
- Advanced settings:** A link labeled 'Advanced' with a gear icon.

At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

5. Click Next.

6. Configure guest processing as required. In this example, guest processing is enabled. Click Next.

New Backup Job [Close]

Guest Processing
Choose guest OS processing options available for running VMs.

Name **Enable application-aware processing**
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot. Applications...

Virtual Machines

Storage Customize application handling options for individual items and applications Applications...

Guest Processing **Enable guest file system indexing**
Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries. Indexing...

Schedule Customize advanced guest file system indexing options for individual items Indexing...

Summary Guest OS credentials

veeam (veeam, last edited: 96 days ago) Add... [Manage accounts](#)

Customize guest OS credentials for individual items and operating systems Credentials...

Guest interaction proxy:
Automatic selection Choose... Test Now

< Previous **Next >** Finish Cancel

7. Configure the backup schedule as required. In this example, the schedule for backup is daily at 10 pm. Click Apply.

New Backup Job [Close]

Schedule
Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Name **Run the job automatically**

Daily at this time: 10:00 PM Everyday Days...

Monthly at this time: 10:00 PM Fourth Saturday Mgnths...

Periodically every: 1 Hours Schedule...

After this job: __TEST__ (Created by WDF02-4-DMZ\ukleidon at 4/1/2019 10:43 PM.)

Schedule Automatic retry

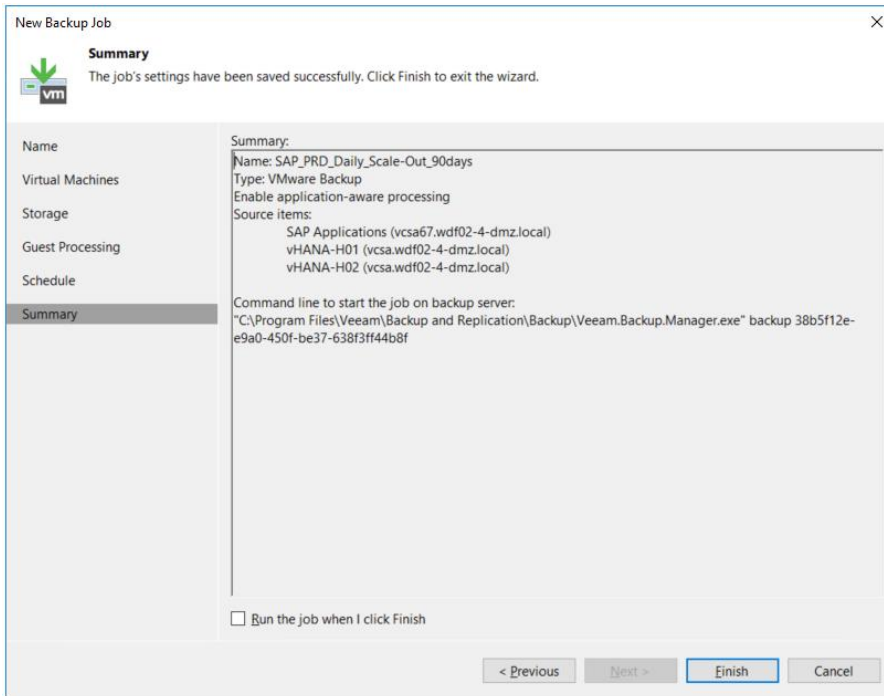
Retry failed items processing: 3 times
Wait before each retry attempt for: 10 minutes

Summary Backup window

Terminate job if it exceeds allowed backup window Window...
If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

< Previous **Apply** Finish Cancel

8. Click Finish.



Test the new configuration

Now test your new configuration.

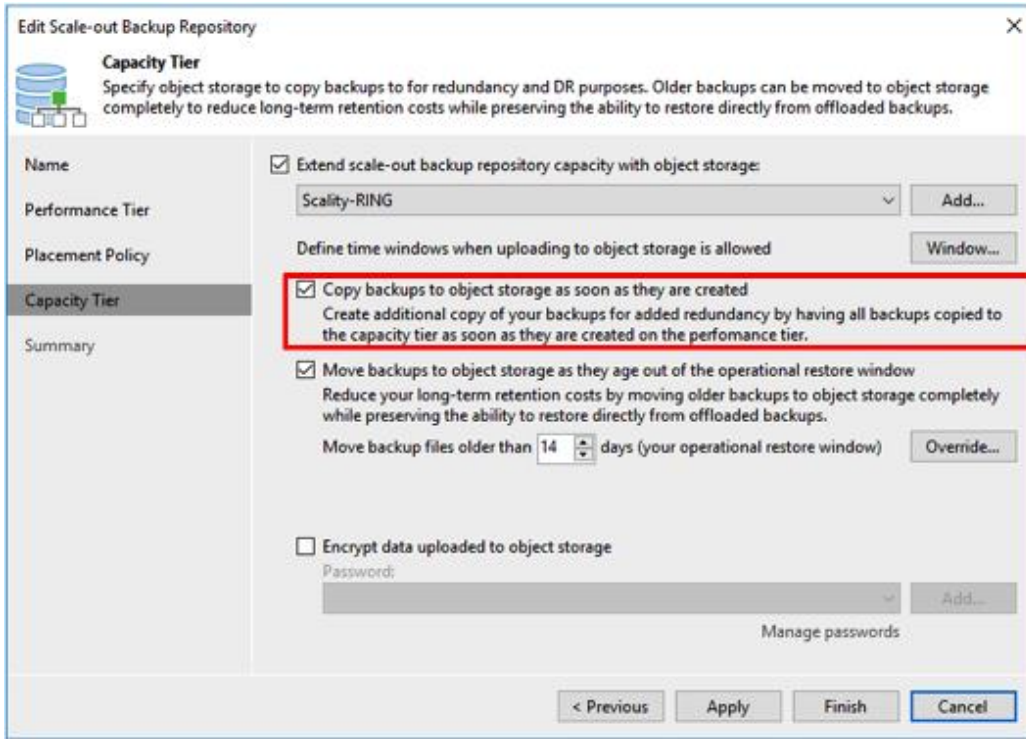
To test the configuration, you should initiate an active full backup process with a small number of source virtual machines.

NAME	TYPE	OBJECTS	STATUS	LAST RUN	LAST RESULT	NEXT RUN	TARGET	DESCRIPTION
TEST	VMware Backup	2	Stopped			<not scheduled>	Scale-Out-BR	Created by WDF02-4-DMZ\ukleidon at 4/1/2019 1...
Backup_2_RING	VMware Backup	1	Stopped	22 minutes ago	Success	4/21/2020 10:00...	Veeam-Scalby-RING	Created by WDF02-4-DMZ\ukleidon at 4/21/2020...
PODS-Datahub	VMware Backup	6	Stopped	14 hours ago	Failed	4/22/2020 2:00 AM	Scale-Out-BR	Created by WDF02-4-DMZ\ukleidon at 4/9/2019 6...
RACK2-HX_Demo	VMware Backup	2	Stopped	14 hours ago	Success	4/22/2020 3:00 AM	Scale-Out-BR	Created by WDF02-4-DMZ\ukleidon at 8/9/2019 5...
RACKS_Infrastructure_VMs	VMware Backup	1	Stopped	17 hours ago	Success	4/22/2020 12:00...	Scale-Out-BR	Created by WDF02-4-DMZ\ukleidon at 7/15/2019...
RACKS-DMZ	VMware Backup	1	Stopped	21 days ago	Failed	<Disabled>	Scale-Out-BR	Created by WDF02-4-DMZ\ukleidon at 7/15/2019...

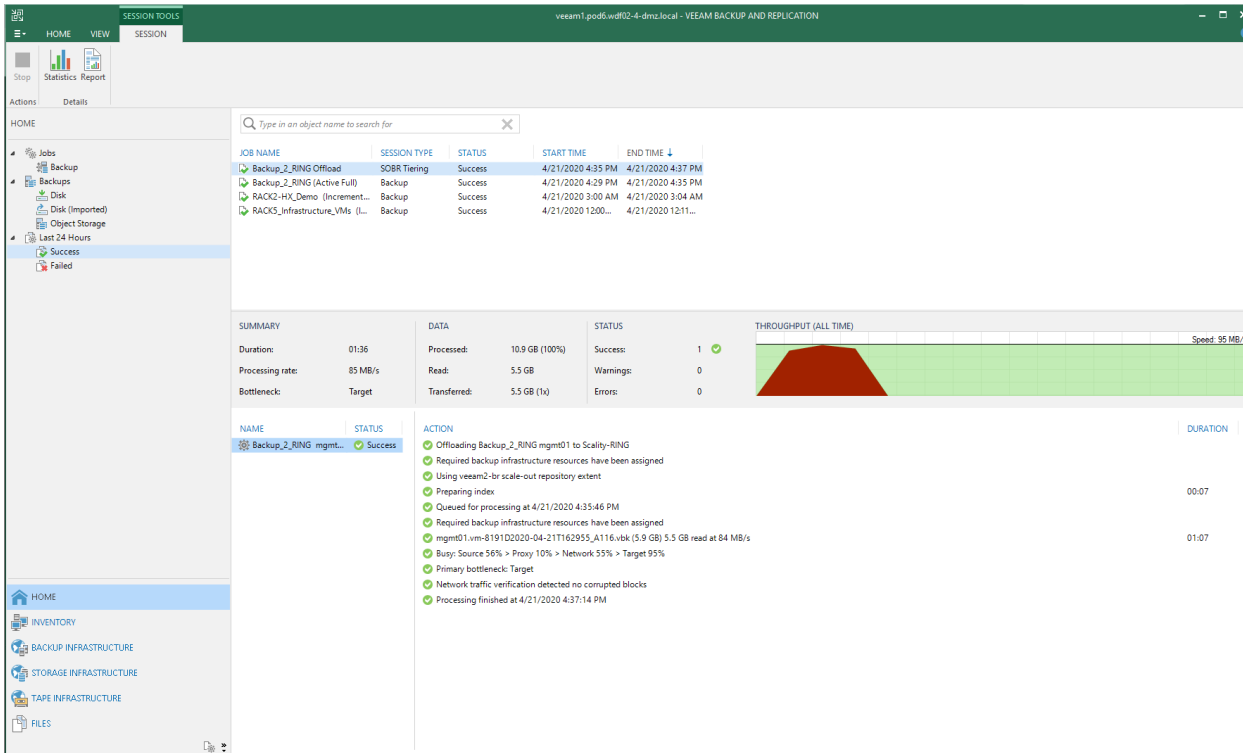
SUMMARY	DATA	STATUS	THROUGHPUT (ALL TIME)
Duration: 05:40	Processed: 160 GB (100%)	Success: 1	
Processing rate: 641 MB/s	Read: 160 GB	Warnings: 0	
Bottleneck: Source	Transferred: 5.5 GB (29.1%)	Errors: 0	

NAME	STATUS	ACTION	DURATION
mgm01	Success	<ul style="list-style-type: none"> Job started at 4/21/2020 4:29:44 PM Building list of machines to process VM size: 160 GB Changed block tracking is enabled Processing mgm01 All VMs have been queued for processing Load: Source 91% > Proxy 18% > Network 42% > Target 0% Primary bottleneck: Source Job finished at 4/21/2020 4:35:24 PM 	00:03

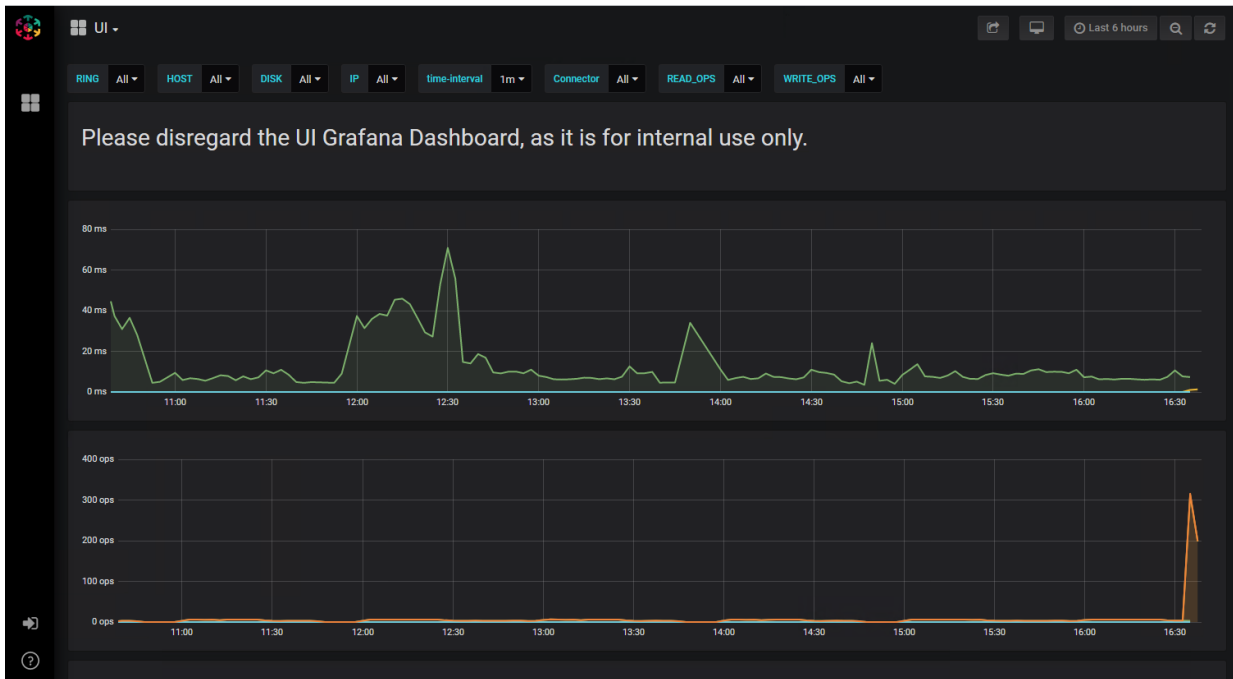
If the option “Copy backups to object storage as soon as they are created” is selected in the scale-out backup repository configuration, a new offload job is initiated directly after the primary backup job is finished.



You can monitor this offload job in the Veeam console just as you can every other job.



The related traffic is also shown in the Scalify RING performance monitoring user interface.



Conclusion

With the introduction of the AWS S3 destination in Veeam Backup & Replication software, you can easily extend the capacity of the backup system to tens or hundreds of petabytes of data. This solution provides cost optimization, serves multiple use cases, and can span multiple sites.

For more information

Cisco-Veeam Solutions at:

<https://www.veeam.com/cisco-storage-solutions.html>

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)