Deployment and Configuration

Dell Technologies Cloud Storage Hybrid Disaster Recovery as a Service

Abstract

This document details the Dell Technologies™ Cloud Storage Hybrid Disaster Recovery as a Service (DRaaS) solution with Dell EMC™ Unity and PowerStore™. This offering provides organizations with an automated, enterprise-grade DRaaS solution in VMware® Cloud on Amazon Web Services.

June 2020

Revisions

Date	Description
December 2019	Initial release
June 2020	Offering updates

Acknowledgements

Author: Jason Boche

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Table of contents

Executive summary

Dell Technologies™ customers of any size, type, and vertical need a business-continuation plan that is fully tested and ready to execute if a disaster or unplanned outage occurs. A typical plan involves recovering applications and the associated data at a remote site as quickly as possible so that business can resume. However, disaster recovery planning and execution is challenged by factors such as growing data footprints, recovery time, recovery asset management, and cost.

Data center virtualization and Dell EMC storage-array-based replication opens the door to more modern and efficient opportunities in disaster recovery planning. For example, virtual-machine-level images can be replicated to a remote site at regular intervals to meet a predetermined recovery point objective (RPO). VMware® vSphere® Site Recovery Manager (SRM) orchestration can be added to the same solution to provide turnkey operations that meet a predetermined recovery time objective (RTO). Having the plans in place to meet service level agreements (SLAs) in terms of RPO and RTO is a primary objective of disaster recovery planning. However, maintaining a recovery site owned or leased by the customer, along with scalable recovery infrastructure in that site, is an ongoing challenge.

Dell Technologies Cloud Storage is a cloud-based solution that fits a variety of business needs. Dell EMC Unity and PowerStore™ storage consumed as a managed service and VMware Cloud™ (VMC) on Amazon Web Services (AWS), can help organizations realize and augment a modernized, cloud-based, disaster recovery strategy.

1 Enterprise services for multi-cloud environments

Dell Technologies Cloud Storage enables connecting file and block storage, consumed as a service, directly to a public cloud including VMC on AWS, AWS, Microsoft® Azure®, and Google Cloud. This is achieved through native replication from on-premises Dell EMC storage—including Dell EMC Unity, Dell EMC Unity XT, PowerStore, PowerMax™, or Isilon storage—to a managed service provider location. Dell Technologies has partnered with Faction Inc. to deliver a fully managed, cloud-based service for Dell EMC storage to address a variety of cloud use cases.

Faction, Inc. is a Dell Technologies Gold Cloud Service Provider (CSP) and Tech Connect Select partner founded in 2006 and headquartered in Denver, Colorado. Faction is a multi-cloud platform-as-a-service provider and VMware partner that offers multi-cloud-attached storage from a variety of colocations (Equinix, Coresite, and Digital Reality). Faction has expanded globally to London and Frankfurt.

Faction has two storage-based offerings available: Cloud Control Volumes (CCVs) and Hybrid Disaster Recovery as a Service (HDRaaS).

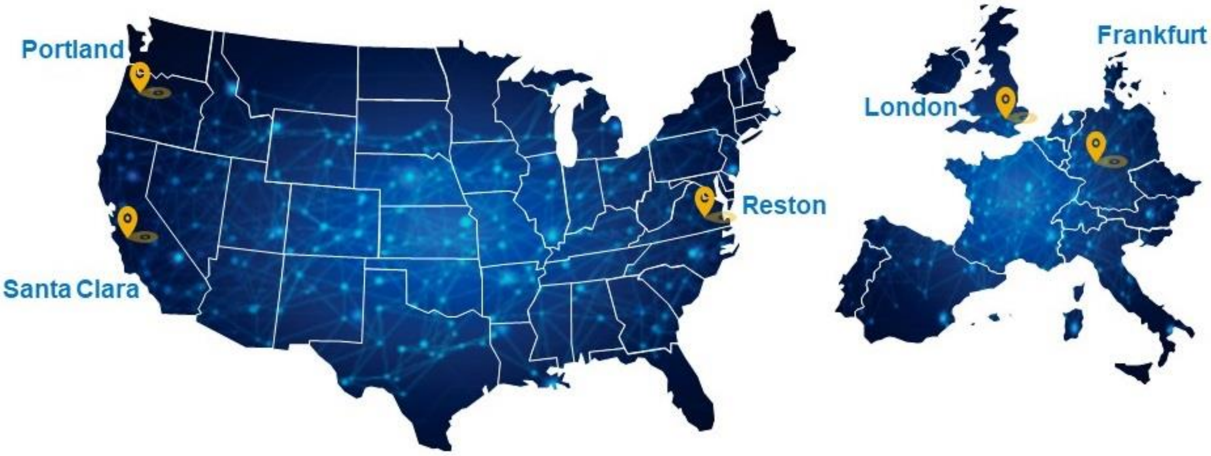


Figure 1 Faction locations which offer Dell Technologies Cloud Storage

2 Faction Cloud Control Volumes

Cloud Control Volumes (CCVs) provide durable, persistent, cloud-attached, and cloud-adjacent storage directly connected to the cloud of choice (VMC on AWS, AWS, Azure, and Google Cloud). CCVs allow leveraging multiple clouds and quickly switching clouds based on business needs.

Although this document focuses on HDRaaS with Dell EMC Unity and PowerStore, this section addresses CCVs because they are often added to an HDRaaS solution if there is a need for direct-attached storage from VMware Cloud on AWS. In addition, most of the technical underpinnings of CCVs commonly apply to HDRaaS.

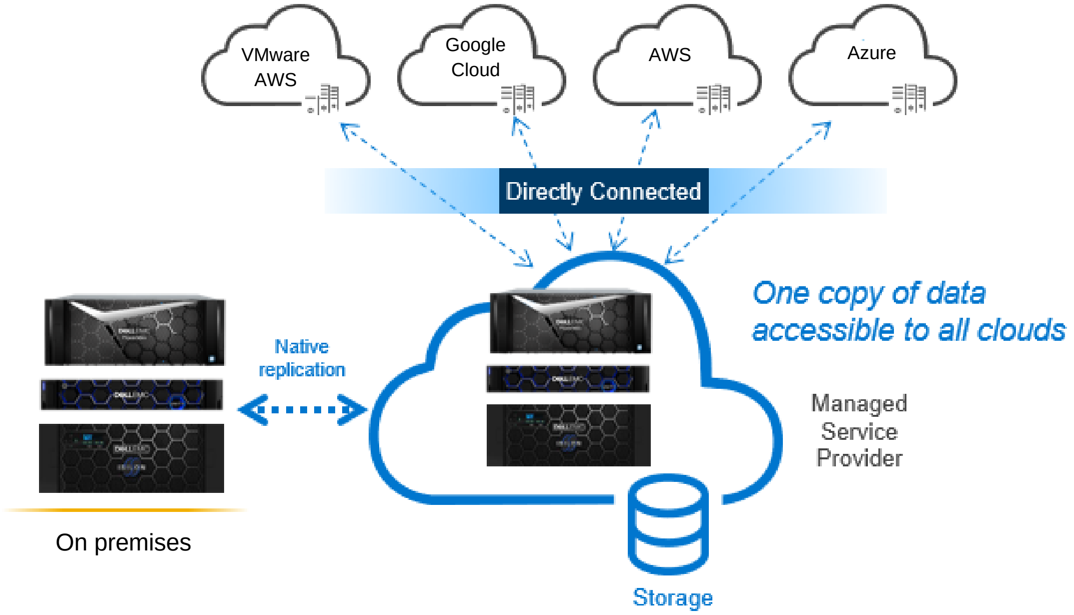
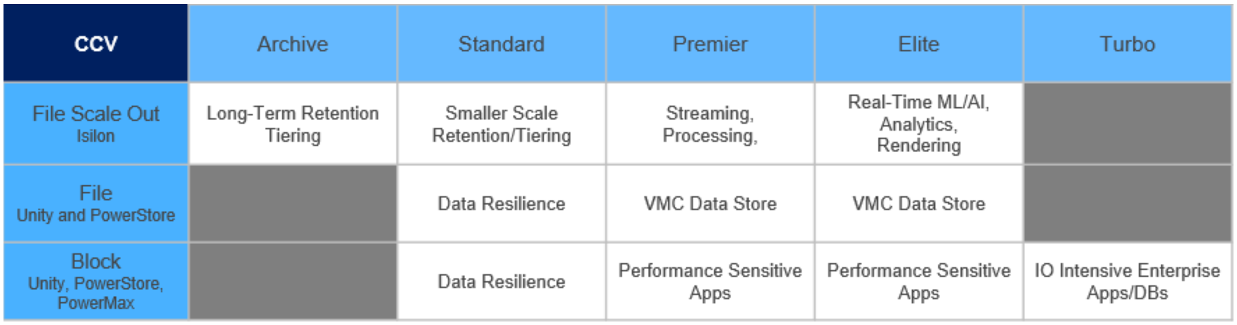


Figure 2 Array-based replication of volumes to Faction directly attached as CCVs across one or more clouds through NFS or iSCSI

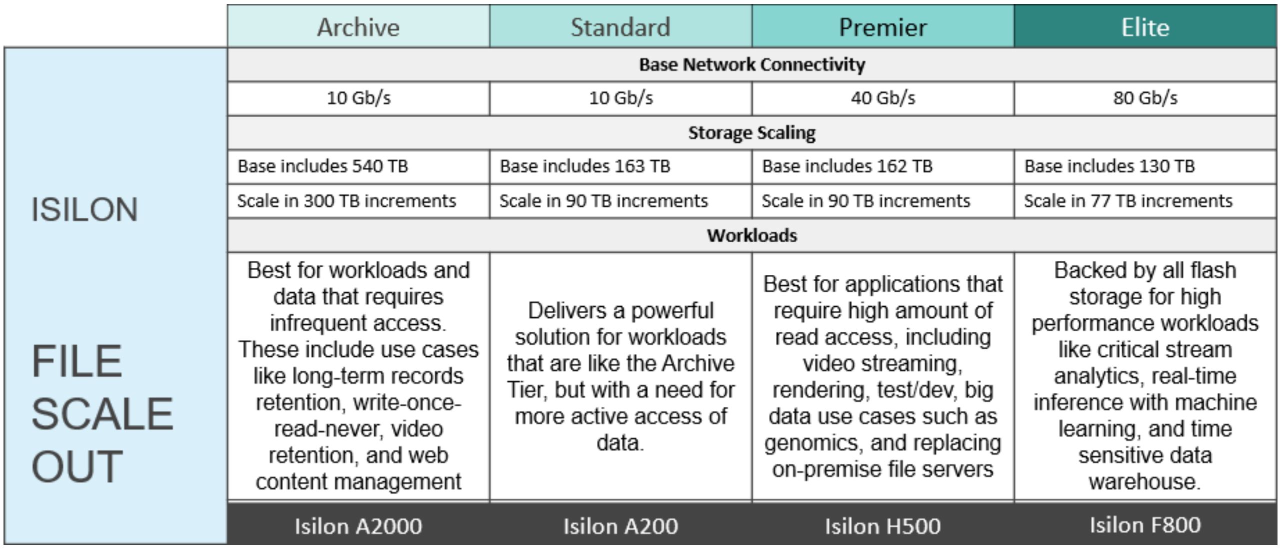
Use cases for CCVs could be transient in nature, such as performing data analytics on a large or complex data footprint. Another use case may be locating or migrating an application to the cloud, and leaving it there permanently while leveraging one or more CCVs in a nearby Faction data center.

A variety of tiers of CCV storage are available in the Faction data center. Storage tier specifics are ultimately determined by the Dell EMC array and use case. CCVs are multi-cloud available with Dell EMC Unity/Unity XT (shared and dedicated), PowerStore, Isilon™ (dedicated), and PowerMax (dedicated).



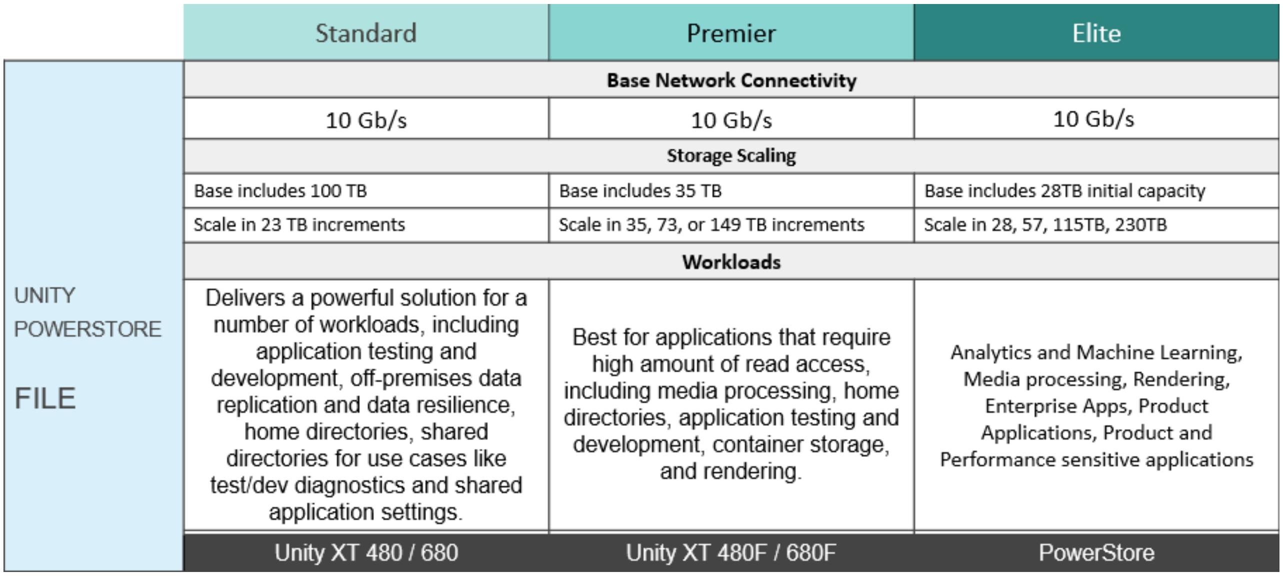
CCV	Archive	Standard	Premier	Elite	Turbo
File Scale Out Isilon	Long-Term Retention Tiering	Smaller Scale Retention/Tiering	Streaming, Processing,	Real-Time ML/AI, Analytics, Rendering	
File Unity and PowerStore		Data Resilience	VMC Data Store	VMC Data Store	
Block Unity, PowerStore, PowerMax		Data Resilience	Performance Sensitive Apps	Performance Sensitive Apps	IO Intensive Enterprise Apps/DBs

Figure 3 CCVs by tier and platform overview



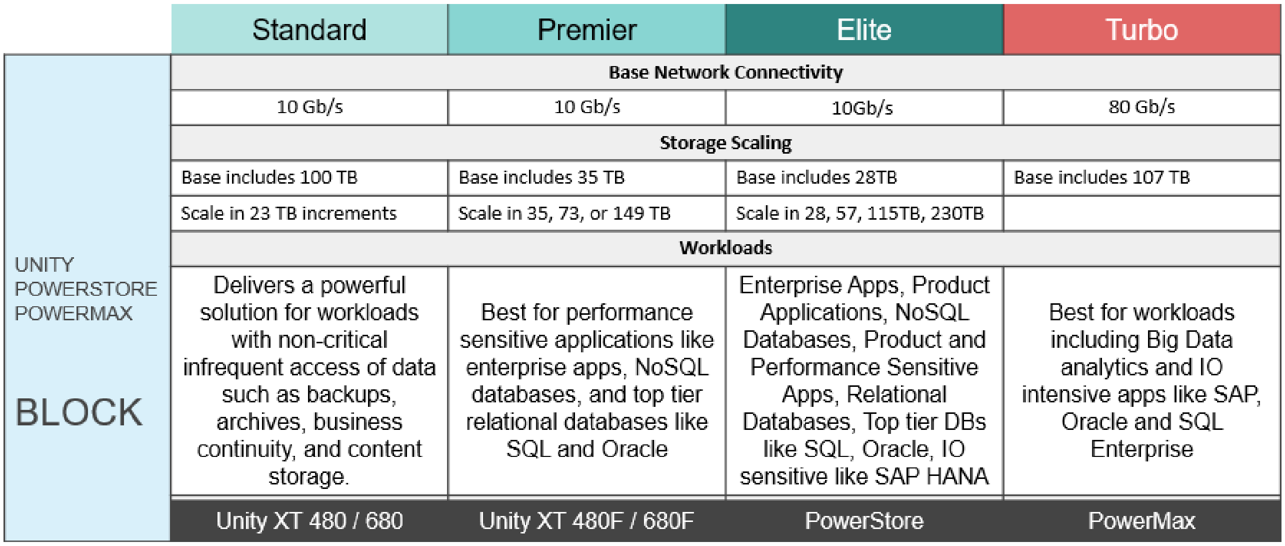
	Archive	Standard	Premier	Elite
ISILON FILE SCALE OUT	**Base Network Connectivity**			
	10 Gb/s	10 Gb/s	40 Gb/s	80 Gb/s
	Storage Scaling			
	Base includes 540 TB	Base includes 163 TB	Base includes 162 TB	Base includes 130 TB
	Scale in 300 TB increments	Scale in 90 TB increments	Scale in 90 TB increments	Scale in 77 TB increments
	Workloads			
	Best for workloads and data that requires infrequent access. These include use cases like long-term records retention, write-once-read-never, video retention, and web content management	Delivers a powerful solution for workloads that are like the Archive Tier, but with a need for more active access of data.	Best for applications that require high amount of read access, including video streaming, rendering, test/dev, big data use cases such as genomics, and replacing on-premise file servers	Backed by all flash storage for high performance workloads like critical stream analytics, real-time inference with machine learning, and time sensitive data warehouse.
	Isilon A2000	Isilon A200	Isilon H500	Isilon F800

Figure 4 File Scale Out CCV details



	Standard	Premier	Elite
UNITY POWERSTORE FILE	**Base Network Connectivity**		
	10 Gb/s	10 Gb/s	10 Gb/s
	Storage Scaling		
	Base includes 100 TB	Base includes 35 TB	Base includes 28TB initial capacity
	Scale in 23 TB increments	Scale in 35, 73, or 149 TB increments	Scale in 28, 57, 115TB, 230TB
	Workloads		
	Delivers a powerful solution for a number of workloads, including application testing and development, off-premises data replication and data resilience, home directories, shared directories for use cases like test/dev diagnostics and shared application settings.	Best for applications that require high amount of read access, including media processing, home directories, application testing and development, container storage, and rendering.	Analytics and Machine Learning, Media processing, Rendering, Enterprise Apps, Product Applications, Product and Performance sensitive applications
	Unity XT 480 / 680	Unity XT 480F / 680F	PowerStore

Figure 5 File CCV details



	Standard	Premier	Elite	Turbo
UNITY POWERSTORE POWERMAX BLOCK	**Base Network Connectivity**			
	10 Gb/s	10 Gb/s	10Gb/s	80 Gb/s
	Storage Scaling			
	Base includes 100 TB	Base includes 35 TB	Base includes 28TB	Base includes 107 TB
	Scale in 23 TB increments	Scale in 35, 73, or 149 TB	Scale in 28, 57, 115TB, 230TB	
	Workloads			
	Delivers a powerful solution for workloads with non-critical infrequent access of data such as backups, archives, business continuity, and content storage.	Best for performance sensitive applications like enterprise apps, NoSQL databases, and top tier relational databases like SQL and Oracle	Enterprise Apps, Product Applications, NoSQL Databases, Product and Performance Sensitive Apps, Relational Databases, Top tier DBs like SQL, Oracle, IO sensitive like SAP HANA	Best for workloads including Big Data analytics and IO intensive apps like SAP, Oracle and SQL Enterprise
	Unity XT 480 / 680	Unity XT 480F / 680F	PowerStore	PowerMax

Figure 6 Block CCV details

Organizations wanting to new cloud-based applications or service can deploy into the cloud on net-new CCVs. Alternately, existing application volume data may be migrated from an on-premises data center to a Faction data center. In the latter case, asynchronous array-based replication is configured between on-premises storage and a similar storage array owned and managed by Faction in the Faction data center.

Note: Dell EMC documentation (see appendix A.1) covers installation and configuration of array-based replication.

It is the customer's responsibility to manage the network between their on-premises data center and the Faction data center. Faction can terminate both Fibre Channel and copper cross-connects in the supported facilities, and most other common connections. There are two replication transport options to move data from a customer's on-premises datacenter to the Faction datacenter:

- VPN: Faction can supply an internet endpoint for replication and client network connectivity over VPN. In addition, Faction can terminate IPsec VPNs from compatible equipment for encryption in transit. The VPN must be managed by Faction if the customer does not have a compute environment within the Faction cloud. Compute environment examples would be permanent colocation services or transient DR/test-activation capacity offered in the HDRaaS solution.
- Dedicated circuit: Large-scale customers can opt for a dedicated connection for replication traffic between their facility and Faction, perhaps leveraging a VPN temporarily since lead times for dedicated circuits can be in the 90+ day range. Customers may also use a VPN as redundancy to a dedicated link. Faction can source and manage the dedicated link or the client can work with their carrier directly.

CCVs are presented in close proximity to public cloud providers while leveraging redundant connectivity with multiple 10 Gb Ethernet connections and redundant switches to provide highly available connections. Link Aggregation Groups (LAGs) are used to scale to higher levels of bandwidth into public clouds.

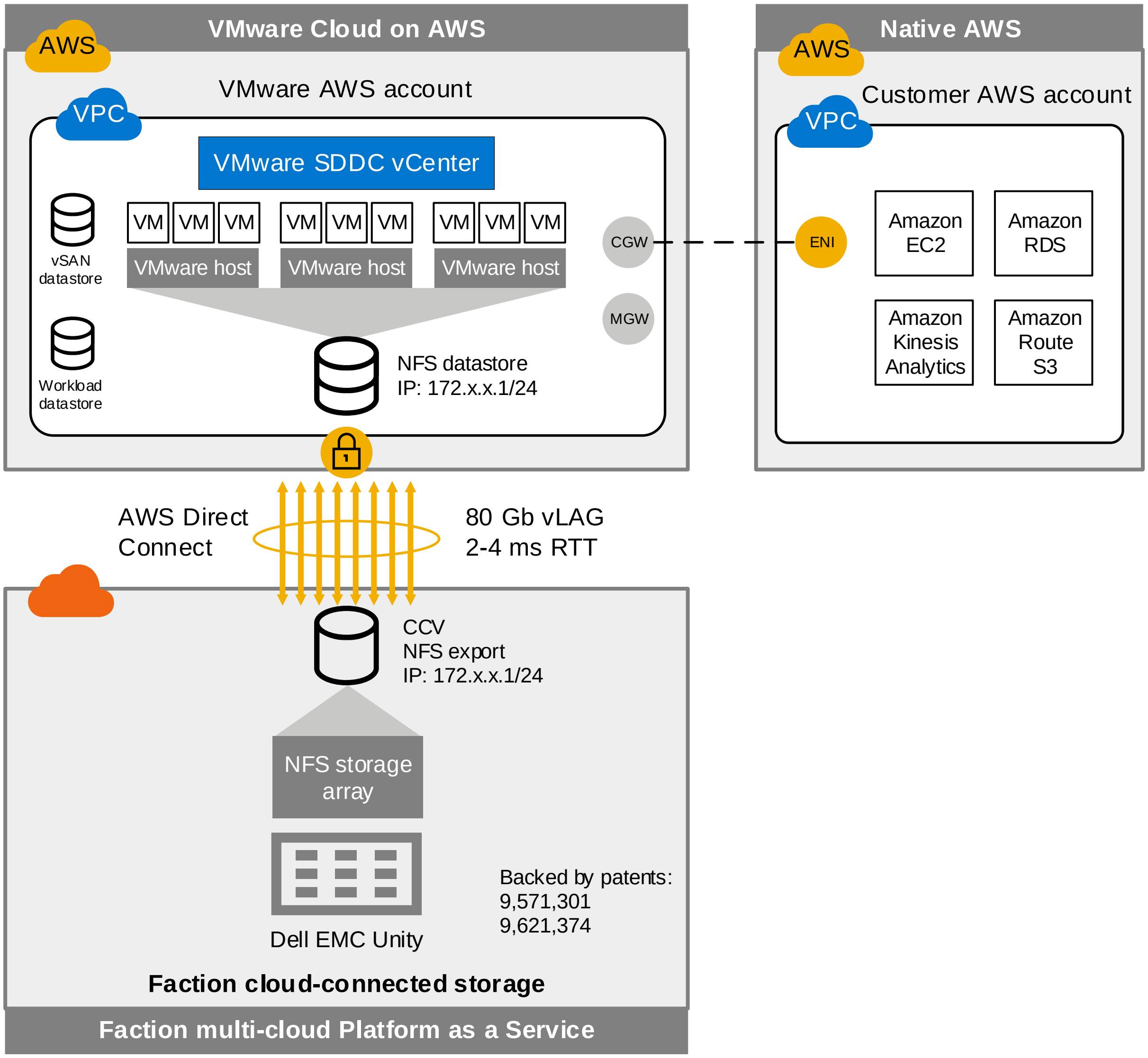


Figure 7 Link Aggregation Groups yield higher levels of bandwidth into public clouds

Note: AWS has limits per flow (source, destination, SRC IP, DST IP, port) on connections that are in the 3–4 Gbps range. As a result, any individual instance can only drive about that amount of maximum throughput per volume/LUN. Public cloud providers also have per-instance rate limitations. For example, AWS has limits where any given EC2 instance, even with enhanced networking and much faster adapters, can only drive a certain throughput (1.5 Gbps for example) although that rate is typically burstable (4 Gbps for example) and the rate is higher with larger instances (for example, an m4.16xl will have ~8x the throughput limits of an m4.large).

The Faction network infrastructure provides full layer-2 and layer-3 isolation between the storage service and the public cloud infrastructures. Public clouds provide the following dedicated network connections for data to flow ingress and egress:

- AWS Direct Connect
- Azure ExpressRoute
- Google Cloud Platform Dedicated Interconnect

Egress traffic charges typically apply at a rate of $.02/GB (USD). Write I/O stemming from a public cloud provider to a direct attached CCV would count as egress traffic.

Latency between the Faction data center and the public cloud providers varies by public cloud and region. Faction provides the current latency numbers at the page Faction Latency Information. The latency numbers can be used for planning and comparison purposes.

It is not uncommon to connect additional data services to storage beyond providing basic availability, scalability, performance, and replication. When moving data into the cloud, these services should be taken into consideration. Faction supports Quality of Service (QoS) as well as compression and deduplication if these services are enabled and in use within the customer's data center. On shared solutions (such as Dell EMC Unity CCVs), storage efficiencies do not affect capacity to the customer. On dedicated platforms (such as PowerMax and Isilon CCVs) storage efficiencies can be enabled to increase effective capacity.

Dell EMC Data at Rest Encryption (D@RE) can also be enabled within the Faction data center. Faction leverages D@RE for Dell EMC Unity, PowerStore, and PowerMax platforms. Isilon systems with self-encrypting drives are also offered in the service. Faction can support external key-management servers over KMIP for Dell EMC Unity and PowerMax storage. This capability is only available on dedicated storage platforms. The customer is responsible for management and availability of the key server. Faction generally does not support customer-managed keys, though exceptions may be made for very large environments.

With regards to data security and compliance in the public cloud, Faction services and data centers undergo annual Type II SOC1 and SOC2 and HIPAA compliance audits, with independent outside auditor attestations available under NDA. Faction can execute BAA agreements with customers subject to HIPAA.

3 Faction Hybrid Disaster Recovery as a Service

Faction Hybrid Disaster Recovery as a Service (HDRaaS) offers disaster recovery from Dell EMC storage into VMware Cloud on AWS by incorporating a variety of technologies as needed in the customer's design. These technologies are covered in the following subsections.

3.1 VMware Cloud on AWS

VMware Cloud on AWS (VMC) is a cloud-based infrastructure service offered and operated by VMware. The solution features one or more VMware Software-Defined Datacenters (SDDCs) deployed on top of Amazon Web Services bare metal instances. The bundle includes vSphere Hyperconverged Infrastructure (HCI) constructs. Each vSphere hypervisor host is configured with the following components:

- Amazon EC2 I3 bare metal instance (currently a three-host minimum configuration)
- Compute: Intel® Xeon® E5-2686 v4 (Broadwell) processors with 36 hyper-threaded cores
- Memory: 512 GiB
- Network: 25 Gbps of aggregate network bandwidth
- Storage: NVMe SSD-backed instance storage (5–7 TB usable internal vSAN storage per host with examples below)
  - 3-host cluster storage 15 TB
  - 4-host cluster storage 21 TB

The vSphere data center resources are managed as a cluster by vCenter Server. Hybrid Linked Mode allows customers to link their VMware Cloud on AWS vCenter Server instance with their on-premises vCenter single sign-on domain. VMC on AWS is a familiar go-to-cloud strategy for VMware customers. VMC on AWS is similar to the vSphere infrastructure in a customer data center. Because the platform components between the two sites are the same, applications and services can easily migrate between a private cloud and the public cloud.

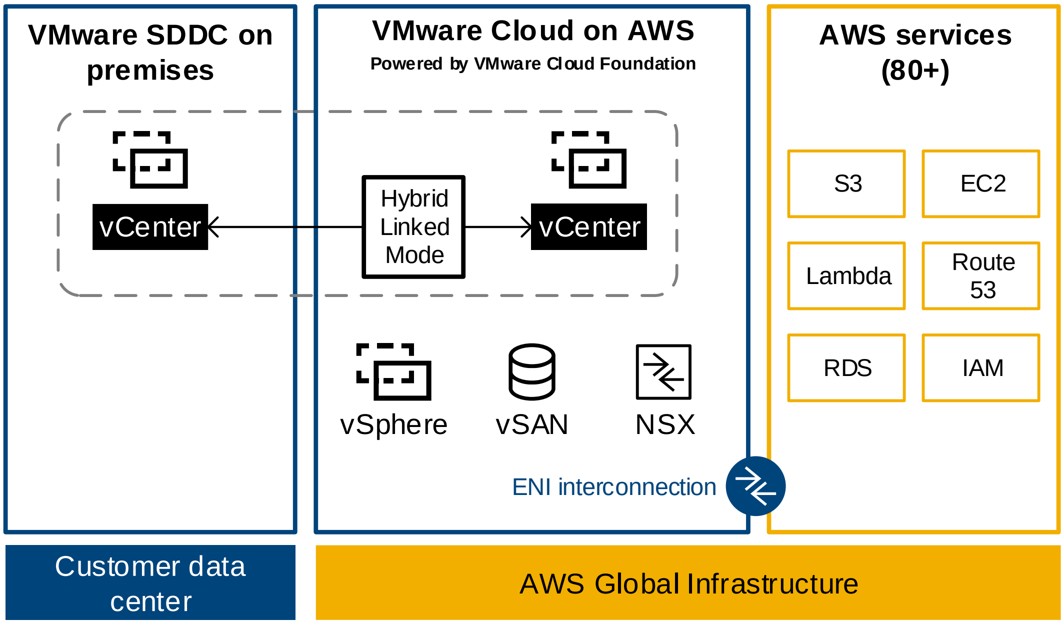


Figure 8 VMware Cloud on AWS architecture

3.2 VMware Cloud on AWS Site Recovery

For rapid recovery and turnkey operations, Site Recovery can be added to both the VMC on AWS SDDC, as well as the customer on-premises SDDC. Site Recovery works like VMware vSphere Site Recovery Manager except it is offered as a fully managed service by VMware. VMware manages components in the VMC on AWS recovery site while customers maintain the protected site within their on-premises data center. The two sites are paired, and data is replicated asynchronously from the on-premises data center to the cloud with vSphere replication. On-premises virtual machines are placed in protection groups and associated with recovery plans. Customers can then activate the protected virtual machines in the cloud by testing or running the recovery plans.

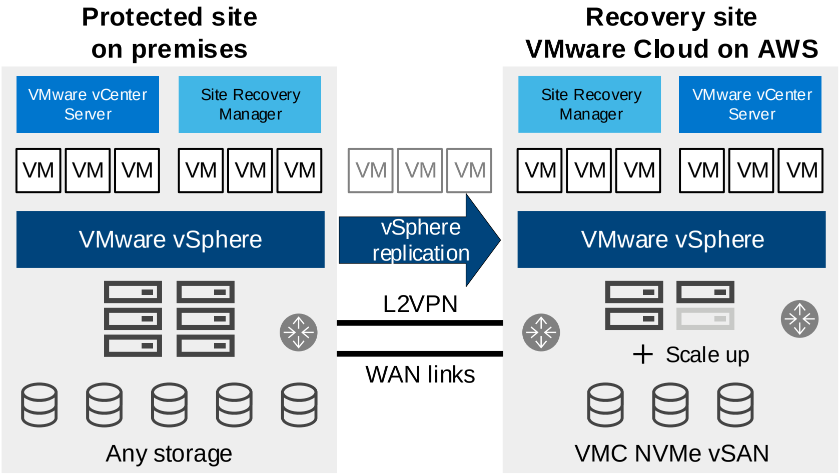


Figure 9 VMware Cloud on AWS with Site Recovery architecture

Recovery to VMware Cloud on AWS offers unique advantages compared to traditional DR methods. Customers do not need to finance and maintain their own building or infrastructure for DR. A broad set of AWS Global Infrastructure services such as Route 53, a highly available and scalable cloud Domain Name Service (DNS) web service, are available to VMC on AWS through the Elastic Network Interface (ENI) in the customer's virtual private cloud (VPC). Accommodating growth and scale is easy because DR infrastructure in the cloud SDDC can be scaled out by adding an additional vSphere host in less than 15 minutes. The environment can also be scaled back as needed with host removal. Host-removal timings vary depending on the amount of vSAN data that must be migrated off the host. On-demand elasticity of resources is a fundamental principle of cloud strategy and it is realized in this solution.

3.3 HDRaaS solution

Faction HDRaaS augments VMware Cloud on AWS Site Recovery in a few ways. The HDRaaS solution provides Dell EMC Unity/Unity XT as well as PowerStore and PowerMax customers with the option of leveraging native storage array based replication or vSphere replication into a Faction Bloc where the initial disaster recovery failover takes place. Additional storage capacity can be added to the VMC on AWS SDDC with Cloud Control Volumes (CCVs). VMware Cloud on AWS integration with Faction is called **External Storage as a Service through MSP** by VMware.

The HDRaaS solution is offered in two packages:

3-Node VMware Cloud on AWS + DRaaS:

- 100 virtual machines, 50TB storage
- Three dedicated VMC on AWS SDDC hosts
- Replication to Faction Bloc or directly to VMC on AWS
- Two failover tests per year included (full or partial)
- Lowest RTO (15 mins) & RPO for production workloads supporting always-on replication

On Demand DR as a Service:

- 100 virtual machines, 25TB storage
- Replication to Faction Bloc only (there are no dedicated hosts in VMC on AWS)
- Failover tests performed as needed but not included in the package
- Cost Effective DR for Tier 2-4 workloads. RTO 4-8 hours

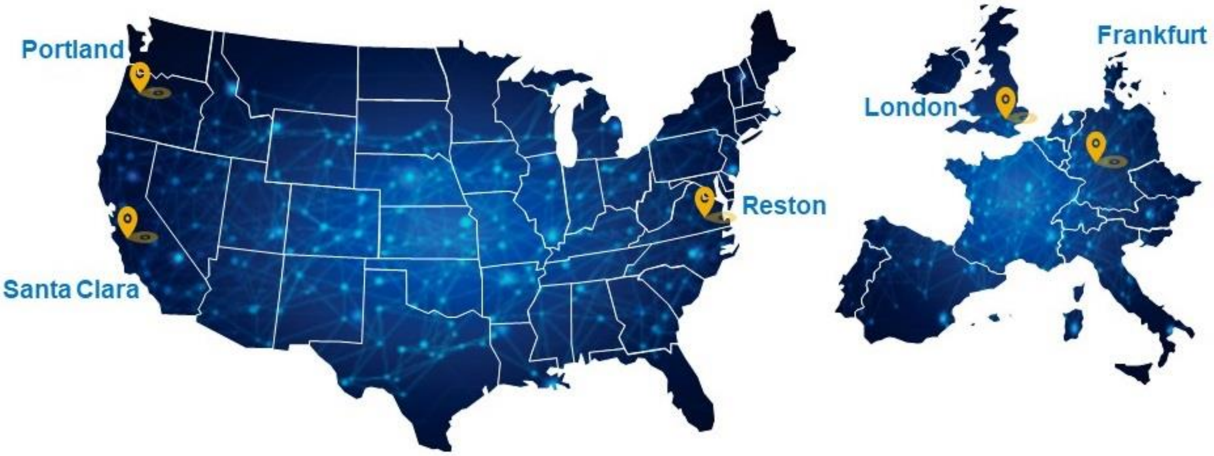


Figure 10 Faction HDRaaS available locations (refer to the Faction Latency Information URL provided earlier for region-specific latency planning)

3.3.1 Storage

When considering native VMware Cloud on AWS with Site Recovery, one may wonder why there is a need for additional externally attached storage from another cloud provider beyond VMC on AWS. This need is supported by economics and how VMC on AWS resources combine to scale as a single unit.

VMware Cloud on AWS uses a hyperconverged architecture based on the VMware SDDC stack. A VMware Cloud on AWS SDDC stack is deployed on AWS Dedicated Bare Metal instances. The dedicated instances are not virtualized; they are essentially dedicated servers deployed from the AWS portal in minutes.

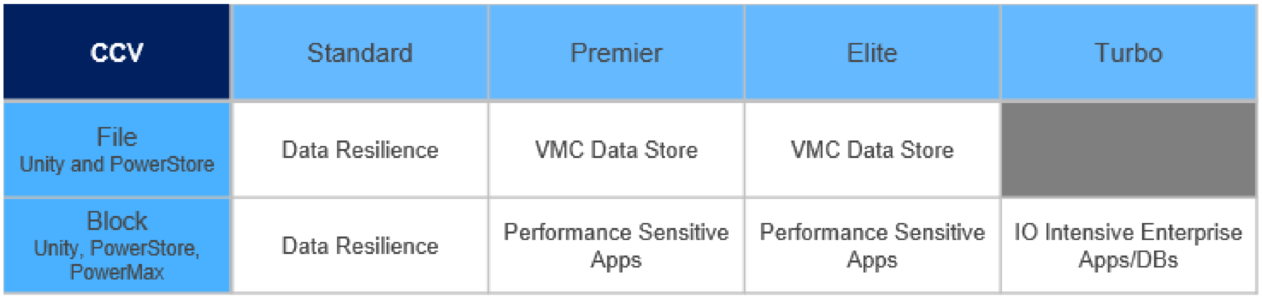
VMware Cloud on AWS automates the deployment of the SDDC stack, which includes NVMe-backed vSAN for storage, NSX for networking, and the vSphere (ESXi) hypervisor for compute. The HDRaaS bundle includes three vSphere nodes in VMC on AWS. vSAN combines the internal storage capacity from all deployed vSphere hosts in the SDDC into a vSphere-consumable datastore. Because this is a hyperconverged architecture, storage is tied to each host in the SDDC and cannot be added independently. If additional storage is needed in this model, customers must add another host into the SDDC, expanding the vSAN storage capacity.

While this is an option, there are economic drawbacks because the price of the storage expansion includes unnecessary networking, hypervisor, and compute costs. The SDDC itself also has cluster-scaling limits which currently caps the total number of vSAN hosts at 16. Limiting vSphere hosts places a limit on the amount of native vSAN storage capacity that can be achieved across the cluster of hosts. Lastly, usable vSAN capacity is also dependent on the failures to tolerate (FTT) and RAID configuration.

Faction CCVs in the HDRaaS solution are a natural fit in this scenario. Faction is able to deploy best of breed Dell EMC storage separately from the SDDC construct and attach it to the VMware Cloud on AWS environment through NFS over AWS Direct Connect. This allows storage to scale independently of the compute, memory, and networking building blocks and achieve much higher storage-to-compute ratios.

Note: At the time of publication, VMware does not support NFS v4.1 nor Kerberos 5p (k5p) in VMC on AWS. Also, a minimum and maximum of three NFS datastores that are backed by Faction Managed Service Provider (MSP) cloud storage can be externally attached to the SDDC. In the event there is not a use for all three datastores, Faction will add **stub** datastores consisting of minimal usable space as placeholders to satisfy VMC on AWS requirements.

Four tiers of CCV storage are available with the Dell Technologies and Faction HDRaaS offering: Standard, Premier, Elite, and Turbo. CCV storage capacity is measured in usable TB. A summary of these tiers by storage platform is shown below. CCV details can be found in an earlier section of this guide.



CCV	Standard	Premier	Elite	Turbo
File Unity and PowerStore	Data Resilience	VMC Data Store	VMC Data Store	
Block Unity, PowerStore, PowerMax	Data Resilience	Performance Sensitive Apps	Performance Sensitive Apps	IO Intensive Enterprise Apps/DBs

Figure 11 CCV storage tiers available through Direct Connect NFS with Dell EMC storage

Attaching external storage to the SDDC in VMware Cloud on AWS requires NFS. If the on-premises storage array is NFS based, it can be replicated to the storage array in the Faction data center and presented to VMC on AWS. Direct attachment of block LUNs as datastores or raw device mappings (RDMs) to VMware Cloud on AWS is not supported. However, block LUNs can still be used in an on-premises data center and block LUN replication into the Faction datacenter is supported.

On-premises block LUNs can be recovered as NFS datastores with the HDRaaS service using VMware vSphere Storage vMotion or a Faction proprietary appliance called the Storage Gateway Handler (SGH). Therefore, If the on-premises storage array is block based, it can be replicated to the storage array in the Faction data center. The vSphere data on the block LUN is either migrated to NFS or converted by the Storage Gateway Handler and presented as an NFS export to VMC on AWS.

The Storage Gateway Handler is also used to preserve file-level QoS for customers on shared multi-tenant storage within the Faction datacenter. The Storage Gateway Handler is built and maintained for high availability and leverages a variety of purpose-integrated technologies in its active/passive redundant architecture.

The Faction HDRaaS solution distinguishes itself from native VMware Cloud on AWS Site Recovery in a few ways:

- Instead of using vSphere replication from on-premises storage to VMC on AWS, customer data is asynchronously replicated from on-premises storage to the Faction data center. This may be array-based replication or vSphere replication.
- HDRaaS introduces an interim landing site that is used for disaster recovery testing and failover.
- Faction HDRaaS can fail over and recover customer workloads with disaster recovery products such as VMware vSphere Site Recovery Manager.
- Alternatively, Faction can fail over and recover customer workloads without disaster recovery products by manually registering virtual machines from array-based replicated volumes in the Faction Bloc and powering them on.

3.3.2 Recovery sites

Typical HDRaaS deployments incorporate Dell EMC array-based replication from the customer on-premises site to the Faction site. These deployments optionally include three CCVs to be attached externally into VMC on AWS. The use of CCVs depends on a storage need beyond what is already available from the VMC on AWS vSAN cluster capacity.

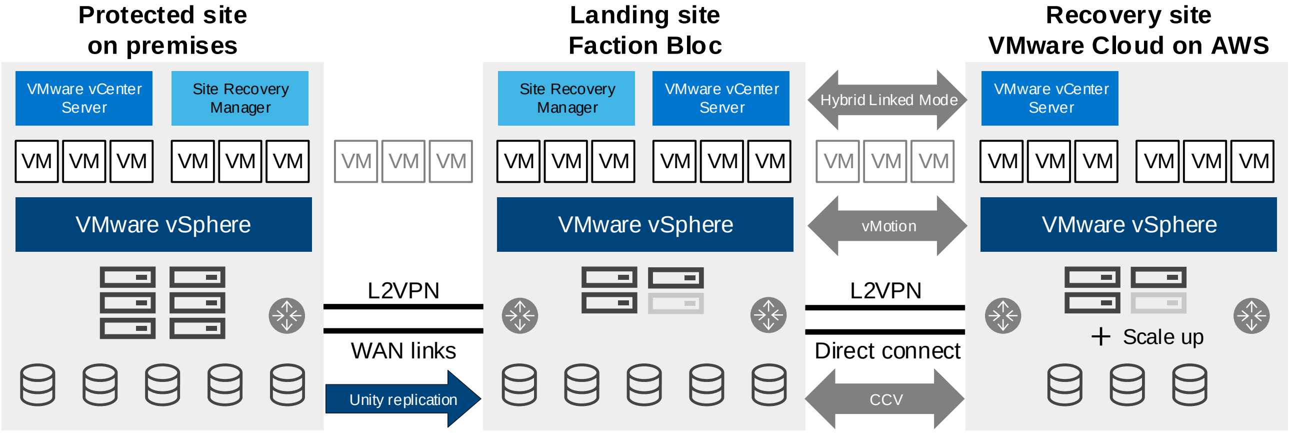


Figure 12 Faction HDRaaS with Hybrid Linked Mode and CCV architecture

Note: A Faction Bloc is isolated infrastructure consisting of compute, network, and storage, within a Faction data center. A Faction Bloc is typically used as permanent colocation services or transient DR/test activation capacity offered in the HDRaaS solution. Each Faction Bloc is sized and built appropriately to fit specific needs and use cases.

Looking at the HDRaaS solution and starting from the customer on-premises site, customer data is replicated to the Faction data center, Site Recovery Manager is paired with the Faction data center, and disaster recovery testing/failover initially occurs within the Faction data center to meet RTO and RPO needs. After applications and services are brought online within the Faction data center, they are migrated to the SDDC within VMware Cloud on AWS using vMotion and Storage vMotion. This migration occurs live with no downtime or disruption, providing the customer has the necessary network connectivity from their client recovery site to both the Faction data center and the VMC on AWS SDDC.

Customers may also choose to replicate on-premises data directly to VMware Cloud on AWS and pair their local Site Recovery Manager instance for failover directly with VMC on AWS. In this design, the customer’s datastores can be backed by any VMware-supported brand, make, or model of storage. VM-level vSphere replication is used to replicate customer data from abstracted block or file datastores into VMC on AWS vSAN cluster capacity. Available storage in VMC on AWS can be scaled by adding cluster nodes to the SDDC (maximum of 16 per cluster) or by attaching three external CCVs from the adjacent Faction data center through NFS.

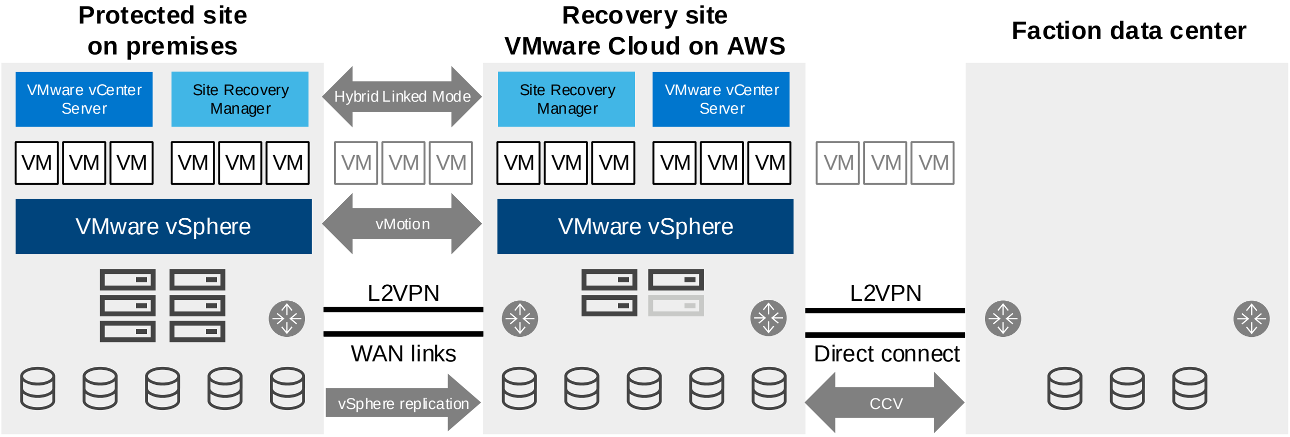


Figure 13 VMware Cloud on AWS Site Recovery with Faction CCV architecture

Looking at the VMware Cloud on AWS Site Recovery solution and starting from the customer on-premises site, customer data is replicated to the SDDC within VMC on AWS, Site Recovery Manager is paired with VMC on AWS, and DR testing/failover occurs directly within VMC on AWS to meet RTO and RPO requirements.

Both solutions offer disaster recovery into VMware Cloud on AWS. Later sections in this document explain the differences in replication technology, SRM pairing, interim landing site, storage capacity scaling, and operational behavior.

Note: Cloud provider egress charges always apply. A replication strategy should be considered when using CCVs with the HDRaaS solution. If replicating to the Faction Bloc, only the delta storage changes made in VMC on AWS (write I/O) will constitute egress back to the CCV(s) in the Faction Bloc. If replicating directly to VMC on AWS, the entire volume(s) will need to egress to the CCV(s) in the Faction Bloc, plus delta storage changes made afterwards.

3.3.3 Networking and client connectivity

Connectivity between the customer site and the Faction Bloc is needed for both array-based replication as well as network connectivity to support DR testing and DR activation. It is the customer's responsibility to manage the network between their on-premises data center and the Faction data center. Faction can terminate both Fibre Channel and copper cross-connects in the supported facilities, and most other common connections.

There are two options for providing secure network connectivity between a customer on-premises protected site and the Faction Bloc/VMC on AWS recovery site:

- VPN: Faction can supply an Internet endpoint for replication and client network connectivity over VPN. In addition, Faction can terminate IPsec VPNs from compatible equipment for encryption in transit. The VPN must be managed by Faction if the customer does not have a compute environment within the Faction Cloud. Compute environment examples would be permanent colocation services or transient DR/test activation capacity offered in the HDRaaS solution.

- Dedicated circuit: Larger scale customers can opt for a dedicated connection for replication traffic between their facility and Faction. Customers can leverage a VPN temporarily because lead times for dedicated circuits can be 90 days or more. Customers may also use a VPN as redundancy to a dedicated link. Faction can source and manage the dedicated link or the client can work with their carrier directly.

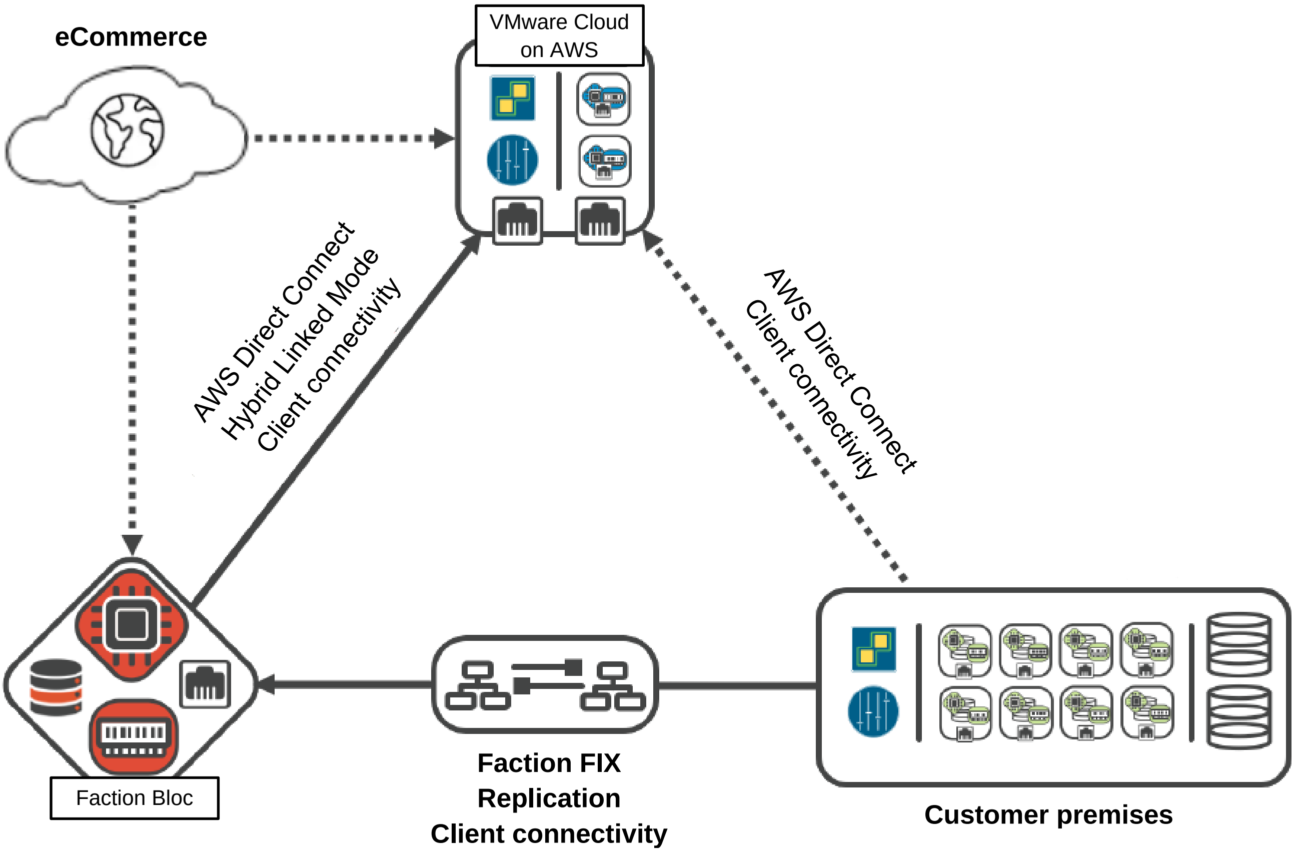


Figure 14 Client connectivity to Faction Bloc and VMC on AWS

Note: A Faction Internetwork Exchange (FIX) is a Faction cloud-node endpoint which customer environments communicate with over a private connection (such as cross-connect, VPN, or a third-party circuit).

In the case of HDRaaS, the Faction Bloc is a temporary landing spot for virtual machines to be powered on in a DR test or activation, and migrated to VMC on AWS afterwards. With this in mind, customers need network client connectivity to both the Faction Bloc as well as VMC on AWS. Both recovery-site network endpoints can be facilitated with a L2VPN or dedicated circuit between the Faction Bloc and the customer data center. During a DR test or activation, the customer has client connectivity to their virtual machines powered on within the Faction Bloc. Activated virtual machines in the Faction Bloc are exposed as necessary to support inbound network connectivity. After these virtual machines are migrated to VMC on AWS, customer network traffic is passed through the Faction data center to the SDDC in VMC on AWS through the AWS Direct Connect established between Faction and VMC on AWS.

3.3.4 Failback scenarios

After recovering from a disaster or unplanned outage in VMware Cloud on AWS, customers should consider how and when to resume business within their own on-premises data center. Disaster recovery planning should include not only data center failover, but failback specifics as well. What site is targeted for failback? How will the data be moved? How long will it take? How much will it cost? Failback operations almost always involve migrating customer data out of VMC on AWS. This constitutes egress traffic and is subject to egress fees of $.02/GB. Failback specifics will largely depend on the disaster scenario and the impact it has made. Disaster events come in a variety of shapes and sizes. Most often, there is some sort of natural disaster or disruption the impacts the integrity of the production data center. These are unplanned situations where a customer makes a “war room” decision to declare a disaster and to initiate the disaster recovery plan. Planned disaster avoidance may also arise where a client declares because of a known situation that will put the production data center at risk (i.e. a hurricane projected to hit the area). In this situation, the customer may initiate a declaration to move production for a period of days or weeks until the risk has been mitigated.

Faction will support a couple of base cases with no or nominal professional services fees for its Managed HDRaaS offering(s). Customers who choose an “Assisted Recovery” or DIY DRaaS solution will be required to leverage Faction Professional Services to support a failback procedure. The reason for this delineation is that in the later cases, Faction will have very limited knowledge of the customer production environment, replication tools, RPTO targets and network design. Faction will be required to start the engagement with an assessment in order to make any kind of recommendation of failback operations and procedures. The Managed HDRaaS service will have a couple of base-case fail back solutions which can be offered. Each is specific to a HDRaaS standard offer that is supported by the Managed Services team. Custom solutions may be supported as a Professional Services Statement of Work.

3.3.4.1 VMware SRS/SRM failback directly to an existing customer data center

In this scenario, the VMware Site Recovery (VSR) solution pairs the VMC on AWS SDDC with the Site Recovery Manager installation in the customer data center. VMware vSphere replication is used to copy virtual machines from VMC on AWS vSAN back to the customer data center. Whether fully managed or delivered as an assisted recovery instance, the provisioning of the service establishes the necessary protection groups and recovery plans. When the customer is ready to fail back, the customer or Faction Managed Services can initiate the planned migration of workloads from VMC on AWS to the customer data center. During the failback, the environments will checksum data to validate everything synchronized correctly ensuring data consistency between sites. The duration of this process will vary based on the size of the environment and the amount of data being moved back to the customer data center. This failback solution is provided as part of the managed solution for one declaration per year. Incremental professional services may be required for source environments that have changed during the recovery or experience data replication failures.

3.3.4.2 Managed HDRaaS failback to Faction Bloc

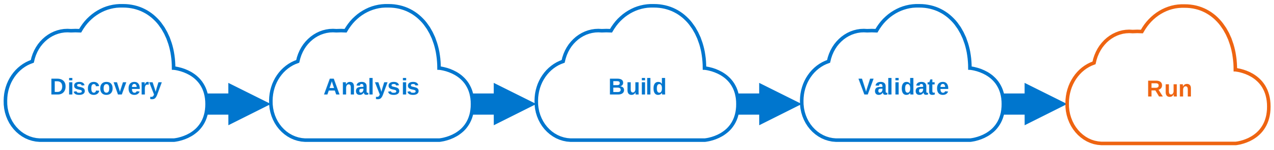
This scenario is only available with fully managed HDRaaS with an annual failback option of once per calendar year. When a customer declares with this product, VMs are powered up in the Faction Bloc and vMotioned to the VMC on AWS SDDC which then becomes a production deployment for a period of time. The failback operations for this solution would be the exact same recovery operation, but back to a Faction Bloc environment. When a customer is ready to fail back, workloads are live migrated from VMC on AWS back to the Faction Bloc using vMotion and Storage vMotion through Hybrid Linked Mode. If a customer chooses to utilize Faction Bloc as a failback landing zone, the customer must pay for those resources on a month to month basis until they move the environment to a customer owned data center. This solution is not as conducive to temporary DR events since the failback operations are to a third environment. There would be another failback required to get the customer back to the customer owned data center. That effort would not be included in the MRR of the Managed Service and would require a Professional Services engagement. However, if the original source environment did not change, the Professional Services engagement would be primarily focused on the replication effort back to the customer data center.

3.3.4.3 Original data center not viable

In the event that the original customer data center is no longer a viable option for a failback operation, Faction would require a Professional Services engagement to assess whatever new environment is being deployed to become the new failback data center. This scenario will require that Faction oversees the replication of data to the new customer data center and conduct a thorough assessment of the environment before data replication commences. This would be a fairly involved engagement and the variables are so unpredictable, Faction cannot forecast what that effort may entail. For that reason, the Statement of Work and associated costs cannot be estimated. Larger and more complex environments would involve a commensurate Professional Services engagement. Once the failback data center is online, Faction oversees the replication of data back to this new environment.

3.4 Faction Managed Services engagement, onboarding, and operations

Faction provides a fully managed HDRaaS offering and works with your business to assess, onboard, manage, monitor, and maintain the disaster recovery solution. Experts at Faction provide assistance from interest to implementation, operations, and recovery.



- Migration and recovery planning
- Storage sizing
- Cloud account(s)
- Network discovery

- Application dependencies
- RTO/RPO SLA tiers
- Network connectivity

- Configure network, applications, storage
- Seed data
- Establish connectivity
- Initial testing

- Recovery and test runbooks
- Validate data seeding
- Confirm RACI matrix
- Verify customer satisfaction

- 24x7 support and monitoring
- Annual testing (2)
- Recovery
- Failback services

Figure 15 Faction onboarding and provisioning

3.4.1 Faction HDRaaS onboarding process

As part of the onboarding process, a Faction solution engineer works to understand your business use case, collect environment information, and capture the proposed solution design. After this is reviewed by the Faction consulting cloud architect, the process proceeds as follows:

- Discovery: The Onboarding project manager helps you define acceptance criteria, migration and recovery planning, and network connectivity to create the project timeline and assign the primary Faction engineer. This may require multiple engagements with key technical subject matter experts.
- Consultation: Faction works with your stakeholders to identify application, systems, resources, and external dependencies. Faction then helps you define and establish Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) to meet business requirements while optimizing the recovery solution.

- Design and build: Faction builds the recovery environment and works with you to link it with the production environment. Replication links are built, and all necessary network, system, storage, and appliance configurations are created. Depending on the replication method, various optimization methods are used to ensure minimal impact to the production environment and ensure the most rapid replication of data. Initial data seeding can be completed over the network or with a shippable drive.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.

A.1 Related resources

- Amazon EC2 I3 Instances
- AWS Global Infrastructures Regions and AZs
- VMware Cloud on AWS product documentation
- VMware Cloud on AWS – Quick Reference Poster
- Configuration Maximums for VMware Cloud on AWS
- VMware Cloud on AWS Release Notes
- Service Level Agreement for VMware Cloud on AWS
- Faction VMware Cloud on AWS Cheat Sheet
- Faction White Paper: Recovery to the Cloud with VMware Cloud on AWS
- Dell EMC Unity: Replication Technologies White Paper
- Dell EMC Unity: Configuring Replication
- Dell EMC PowerStore: Replication Technologies
- Dell EMC PowerStore: Snapshots and Thin Clones

For additional technical information, please contact cloudstorageservices@dell.com.