Welcome to the VCE VxRail Appliance  Data Protection Administration.
The objectives of this module are to discuss considerations for backup and recovery related to business continuity. We will review products offered by the Market tab in VxRail reviewing, Cloud Array, RecoverPoint for VMs and vSphere Data Protection.
VCE provides solutions to meet all VxRail Appliance data protection requirements

Focus is on integrating industry leading technologies into a strategic platform offered by VCE to simplify data protection
Enterprise backups are outdated and need to evolve to keep pace with the latest advancements in Cloud infrastructure. The backup process has changed very little. There have been improvements along the way with the speed and capabilities, but it’s the fundamental way we backup that has not evolved with the way IT is run in the datacenters. With no visibility, or control of backups, each team rolls its own solution. VxRail integrates VMware and EMC backup and recovery technologies creating solutions to have more frequent backups with reduced backup windows.
With data protection there are different levels of requirements. Some need a very stringent recover point objective and others may need continuous uptime with no downtime. To start with the basics all data should have some kind of daily backup even if it’s only changed data. With this approach a daily backup can provide a business with a maximum loss of 24 hours’ worth of lost data. Moving up the stack other applications may need special interim snapshots of the data. This is where local replication and snapshots come in. Becoming more stringent could be a continuous point in time snapshots at very tight intervals. This is where RecoverPoint comes in. Finally for those that require no downtime vMotion can be used to move VMs to another location for continuous availability. Note none of these are fault tolerant, but rather fault resilient. It is very important to understand the recovery time objective and recovery point objective.
Today’s businesses need to keep a backup copy of their local data on-site to follow industry regulations or to ensure business continuity. Some organizations also need to replicate their local servers and applications to external locations to guarantee minimal Recovery Time Objective (RTO) in case of a disaster. Deploying a VxRail Appliance is the perfect time to transform backups and disaster recovery!
Data protection these days is not just a backup of data as rapid data restoration is essential to fast paced business environments. The first layer of protection should be where the data lives on disk. This can be accomplished with keeping multiple copies on disk. VxRail does this with its use of the Virtual SAN and its storage policies. The next layer of protection is using snapshot/snaps or clones to make an immediate backup. This would be used to take an immediate copy prior to applying updates to a VM and its environment.

The next layer of protection are local backups using VMware vSphere Data Protection (VMware VDP) and/or RecoverPoint for VMs both protecting against physical and logical failures. We will be looking at these options in this module.
4 nodes had advantages over 3 nodes. Customers are often surprised by limitations of using a 3 node solution. 4 node provides full protection when a node is lost as the virtual SAN can then tolerate another failure. Another use is during rolling upgrades where a 4 node cluster would give you full data migration and protection during the upgrade.

If you want VMs to remain highly available during failure, maintenance or upgrades, buffered capacity and a minimum 4 nodes are needed by VSAN.
Checksum is enabled as a cluster wide setting (Default is on). It can be disabled on a per object basis using storage policies.

During the read/write operations VSAN will check for the validity of the data based on checksum. If the data is not valid then it should take the necessary steps to either correct the data or report it to the user to take action. These actions could be:

- Fetch the data from other copy of the data for RAID1, RAID5/6, etc.
  - This is what we call recoverable data.
- If there is no valid copy of the data the error SHOULD be returned
  - This is what we call Non-recoverable errors

Reporting:

- In case of errors the issues will be reported in the UI and logs. This will include impacted blocks and their associated VMs.
- A customer will be able to see the list of the VMs/Blocks that are hit by non-recoverable errors.
- A customer will be able to see the historical/trending errors on each drive

CRC32 is the algorithm used (CPU offload support reduces overhead)

There will be two level of scrubbing:

Component level scrubbing: every block of each component is checked. If checksum mismatch, the scrubber tries to repair the block by reading other components.

Object level scrubbing: for every block of the object, data of each mirror (or the parity blocks in RAID-5/6) is read and checked. For inconsistent data, mark all data in this stripe as bad.

Repair can happen during normal I/O at DOM Owner or by scrubber.

The repair path for mirror and RAID-5/6 are different. When checksum verification fails, the scrubber or DOM Owner will read the other copy of the data (or other data in the same stripe in case of RAID-5/6), rebuild the correct data and write it out to the bad location.

End-to-end checksum of the data to detect and resolve silent disk errors
- Checksum is enabled by default as a cluster wide setting
- Fetch the data from another copy in case of checksum verification failures
- Disk scrubbing will run in the background

Benefits
- Provide additional level of data integrity
- Automatic detection and resolution of silent disk errors
The `NumberOfFailuresToTolerate` policy setting is an availability capability that can be applied to all virtual machines or individual VMDKs.

- The setting defined in a virtual machine storage policy can lead to the consumption of as many as four times the capacity of the virtual machine.

- The value refers to the number of replica copies of the virtual machine’s data.
  - The default value for is 1 (max value 3).

- For VxRail Virtual SAN the `NumberOfFailuresToTolerate` is set to 1, two replica mirror copies of the virtual machine or individual VMDKs are created across the cluster.

For VxRail Virtual SAN the `NumberOfFailuresToTolerate` is set to 1. This means there are two replica mirror copies of the virtual machine or individual VMDKs across the cluster. If the number is set to 2, three mirror copies are created; if the number is set to 3, four copies are created. You need consider the number of replica copies when sizing storage resources.
Organizations are now required to keep information applications online 7x24x365. When there is an outage or a disruption, service time to recovery has a real cost to the business. In the event of a catastrophic failure data loss can not only have an impact to the business operations but to the organizations very existence. Having secondary copies is a necessity. Maintaining a consistent restartable copy of production applications is part of normal business practices.

Recovery Point Objective is how much data a company afford to lose in the event of an outage or disaster. Recovery Time Objective is how long a company can be without access to applications and data. Both of these need to be considered carefully. Although we’d all like to never lose data and never be down there are real business costs to achieve this. One has to weigh the pros and cons and find a good balance between RTO and RPO.
VMware vSphere Data Protection (VMware VDP) is a backup management, recovery and replication utility for virtual machines and applications that is based on EMC Avamar deduplication technology. VDP is a Linux-based virtual appliance for backup and recovery that is included as part of the VxRail solution.

VDP can perform agent-less image backup, replication and restore, individual disk backup, variable-length deduplication, changed block tracking restore and file-level recovery.

Powered by EMC Avamar, vSphere Data Protection provides disk-based backup and recover via simple wizards. VDP backups can be stored on EMC Data Domain systems.

Included with VxRail is vSphere Data Protection which is deployed as a virtual appliance on the VxRail system, and provides up to 8 TB of backup capacity.

VDP features built-in deduplication for rapid backups and reduced network bandwidth when replicating to EMC Data Domain systems. This deduplication also reduces the backup window by 90%, and significantly reduces the required capacity for backup storage.

If restoration is needed, VDP features a one-step recovery process that is highly efficient, secure, and fast.
EMC RecoverPoint for Virtual Machines is a business continuity solution that is incredibly simple to use yet gives you peace of mind by protecting your virtual machines at a granular level.

RecoverPoint for VMs will protect the virtual machines deployed on VxRail by providing continuous data protection. The software has built-in orchestration and automation to streamline your protection schemes.

With RecoverPoint for Virtual Machines protecting VxRail Appliance resources, administrators can easily replicate data to and from remote offices in the event of a disaster ensuring that the business suffers no downtime. VMs can be rolled back to a known good point in time and resume operations quickly and efficiently. RecoverPoint for VMs is closely integrated with VMware vSphere so that management can be done from within vSphere’s management interface.
RecoverPoint splitters for ESXi reside on all servers with protected workloads, allowing replication and recovery at the virtual disk (VMDK and RDM) granularity level. Since the I/O splitter resides within the vSphere hypervisor, RecoverPoint for VMs can replicate VMs to and from any storage array supported by VMware: SAN, NAS, DAS, and VSAN.

RecoverPoint architecture uses an advanced journaling system to track changes. This allows for replication across a WAN, and extremely granular recovery point options.

After being deployed from the VxRail Market, provisioning of replication tasks can be performed with a simple wizard from vSphere Web Client. Administrators can conduct automated disaster recovery tasks from within the RecoverPoint for VMs vCenter plug-in.

Standard VxRail licensing includes a 15-VM license for RecoverPoint for Virtual Machines.
To install RecoverPoint for VMs first download the manual from support.emc.com. You want to get RecoverPoint for Virtual Machines Installation and Deployment Guide and then follow the procedures within the guide.
EMC CloudArray, EMC’s cloud storage gateway, is integrated into VxRail Appliances and it seamlessly extends the appliance to public and private clouds to securely expand managed storage capacity. Cloud-storage gateways make it possible to take advantage of storage services from both public and private cloud storage providers while maintaining predictable performance behavior. EMC CloudArray is accessed through VxRail Manager and provides an additional 10TB of on-demand cloud storage per appliance. EMC CloudArray currently provides connections (APIs) to over 20 different public and private clouds. VxRail Appliance CloudArray can provide an elegant, seamless solution for cost-efficient cold (inactive) data storage or an easily accessible online archive with predictable performance behavior.

VxRail Appliance deploys CloudArray as a virtual appliance, a preconfigured, ready-to-run VM packaged with an operating system and a software application. Self-contained virtual appliances make it simpler to acquire, deploy, and manage applications. The CloudArray virtual appliance is essentially a VM already
installed with and running the EMC CloudArray software application. The communication between the VxRail VMs and the CloudArray VM takes place through the VM IP network. An iSCSI initiator is configured on the VM’s guest OS to connect it to the CloudArray VM, and the IP address of the CloudArray VM is defined as the iSCSI target.
Shown here is a simple diagram of CloudArray’s architecture. As users and applications access data on CloudArray, they write and read against CloudArray’s cache. The data then is reduced in sized, encrypted, and stored on private or public Cloud storage.
In summary, we’ve discussed some considerations for business continuity, backup, and recovery. You’ve learned it’s important to understand the RTO and RPO for the application environment being backed up knowing that there are tradeoffs that must be decided. One has to also consider how much data, growth rate and how backups could affect performance. We explained the VxRail options to address business continuity looking at CloudArray, RecoverPoint for VMs, and vSphere Data Protection.
Thank you.