Tintri

TECHNICAL WHITE PAPER

# Data Protection Overview and Best Practices

With Tintri VMstore and Tintri Global Center

## Revision History

| Version | Date | Description | Author |
|---|---|---|---|
| 1.1 | 02/03/2017 | Update | Bill Roth |
| 1.0 | 04/10/2014 | Previously known as Backup and Recovery Best Practices with Tintri VMstore | Previous Contributor |

Table 1 - Revision history

# Contents

# Introduction

The Tintri VMstore features significant data protection and disaster recovery capabilities. Built-in features such as snapshots and replication form the basis for creating recovery points, and disaster recovery copies of recovery points on different VMstore arrays. Data recovery functions include the automated ability to restore an entire virtual machine, a specific virtual disk, and granular folder and file recovery. Cloning, the ability to create a new virtual machine from a local or replicated snapshot, adds to the recovery options available to meet business objectives.

Deep analytic capabilities are also built-in to the Tintri VMstore. Critical data points are clearly presented to assist in gaining a comprehensive understanding data protection, replication, and disaster recovery preparedness.

By design, the VMstore data protection architecture operates at a virtual machine level. This advanced approach to managing data protection and disaster recovery simplifies planning, implementation, monitoring, and the ongoing administration of a comprehensive data protection and disaster recovery deployment.

# Intended Audience

Focused on building a successful data protection solution, this document targets key best practices and known challenges. Hypervisor administrators and staff members associated with architecting, deploying, and administering a data protection and disaster recovery solution are encouraged to read this document.

## Prerequisites

General knowledge of and familiarity with the Tintri VMstore is highly advised prior to architecting or implementing a data protection and disaster recovery solution. It is also important to have a comprehensive understanding of service level agreements as they relate to data protection and disaster recovery within your organization.

## Considerations & Limitations

Product compatibility and support matrices should be referenced to confirm that a given configuration is supported prior to implementation. This includes but is not limited to Tintri products, VMware products, and Microsoft products.

For Tintri support information please visit http://support.tintri.com. The Tintri support site requires access credentials.

Descriptions provided and examples depicted within this document are based on Tintri Operating System version 4.3 and higher.

# Consolidated List of Practices

The table below includes the recommended practices in this document. Click the text on any of the recommendations to jump to the section that corresponds to each recommendation for additional information.

**DO:** When using the default protection policy, specify the use of “Crash-consistent” snapshots.

**DON’T:** Avoid scheduling all snapshots to occur at the exact same point in time.

**DO:** Select VM-consistent snapshots for specific virtual machines that require virtual machine level consistency.

**DO:** Assure that VMware tools are installed and up to date on VMware virtual machines when creating VM-consistent snapshots.

**DO:** When configuring outbound replication paths, be sure to test the settings with the “Test paths” function.

**DO:** Augment “Snap and replicate every minute” replication with additional replication schedules when additional recovery points are required.

**DO:** When restoring virtual machine files or folders, leave the “Auto detach disks in 48 hours” function enabled.

## Data Protection & Disaster Recovery

This section takes a deep look at constructing a data protection and disaster recovery solution using the key technologies discussed in the overview section; snapshots, replication, data restoration, and cloning.

### Snapshots

A snapshot is a point in time copy of an individual virtual machine stored on a VMstore (the entire virtual machine must reside on the same VMstore). The snapshot retains the state of the virtual machine and its files at the time the snapshot was created.

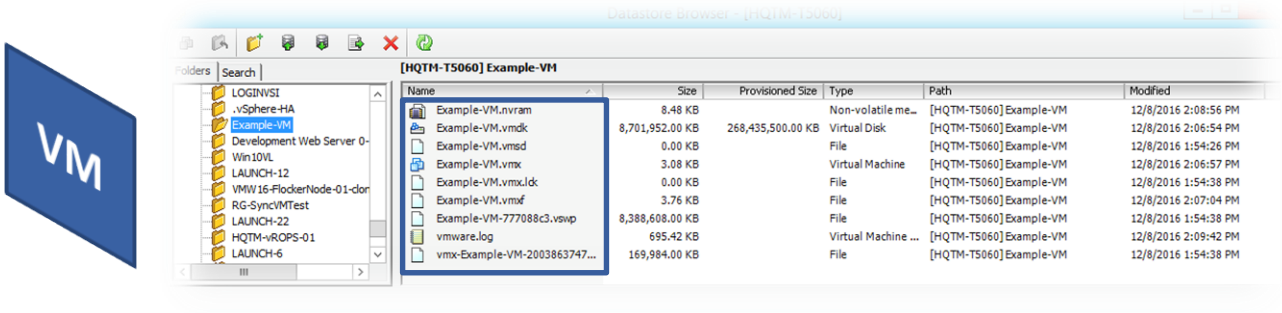



Figure 1: The files associated with a virtual machine named “Example-VM”

Snapshots form the basis of a data protection strategy for a given virtual machine in that they can be used as recovery points, replicated to a different VMstore, or cloned to create a new virtual machine. Virtual machine snapshots can be created manually, automatically by means of a schedule, or triggered through the Tintri RESTful API.

Snapshot schedules are typically configured to achieve a required RPO (Recovery Point Objective). RPO is usually defined as a maximum time period during which data may be lost. For instance, an RPO value of one hour implies that up to one hour of data loss is acceptable. The frequency at which scheduled snapshots are created dictates the recovery point objective that will be achieved. For example, a snapshot schedule that creates daily snapshots results in a maximum RPO of 24 hours. The retention period for a given virtual machines snapshots is also configurable such that the RPO can be achieved over the duration of a timeframe, one week for example.

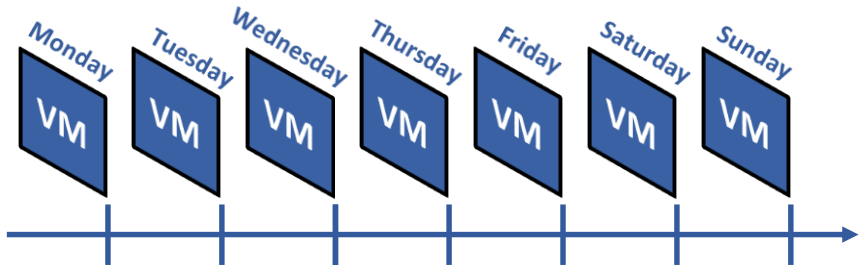



Figure 2: Scheduled virtual machine snapshots with a 24 hour RPO retained for 1 week

A snapshot includes references to the data blocks in use by the virtual machine at the time the snapshot was taken. At the point where a given block is referenced by a snapshot, it cannot be modified. Modification to data within a block referenced by a snapshot will be written to a new block.

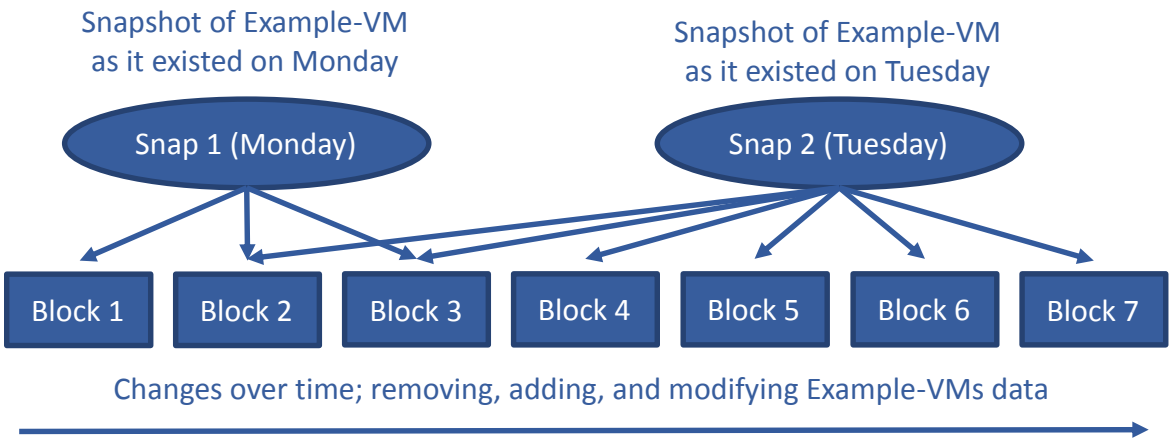



Figure 3: Basic snapshot "block pointer" diagram

Snapshot space consumption is an important factor that should be taken into consideration when using array based snapshots for data protection and disaster recovery. Any performance impact that may be introduced with an array based snapshot solution is also important to understand. VMstore snapshots are efficient for a number of reasons:

- **VM Level Snapshots** - The ability to snapshot only the virtual machines that require protection also eliminates wasted snapshot space. Without this capability, users are forced to snapshot all of the virtual machines within a LUN, for example. The alternative is deciding not to protect a LUN with snapshots, making virtual machine placement decisions a pre-requisite to deployment.
- **Block size** - The Tintri file system uses a block size of 8 KB. When updating a single byte of data in a block referenced by a snapshot, the Tintri file system will create a new 8 KB block. File systems with a larger block size, 16 KB for example, will create a new 16 KB block effectively consuming additional file system space.
- **Compression** –Tintri T800 and T5000 series products feature data compression, further increasing efficiency by reducing the space consumed by snapshots.
- **Deduplication** - Tintri T5000 series VMstore products deduplicate blocks with the same content, extending efficiency by reducing the space consumed by snapshots.

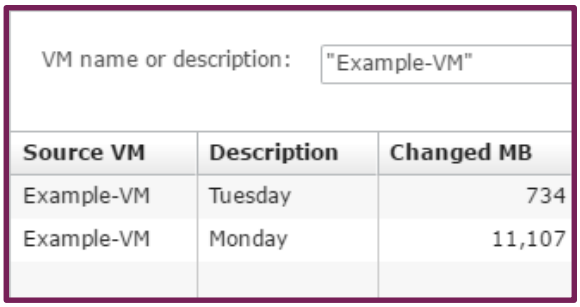



Figure 4: Example-VM snapshot space consumption

- **VM Level Retention** - The ability to retain only the required number of snapshots for an individual virtual machine further eliminates wasted snapshot space. Without this capability, users are forced to group virtual machines with the same data protection characteristics into the same LUN, for example. Snapshots at the virtual machine level eliminate the pre-requisite decision making process of determining the LUN on which a particular virtual machine should be deployed.
- **Zero Performance Impact** – Retained snapshots do not impose a performance penalty on a running virtual machine. Automatic snapshot deletion that occurs when a snapshot expires, also imposes no performance penalty on a running virtual machine.

### *Snapshot Consistency*

There are two types of snapshots that can be created for a virtual machine:

- **Crash-consistent**: Creates a snapshot of a virtual machine without taking extra measures to coordinate the snapshot with the virtual machines guest operating system and any applications it may be running. When powering on a virtual machine recovered from a Crash-consistent snapshot, the virtual machine will boot as if it was abruptly powered off.
- **VM-consistent**: Creates a snapshot while also taking further steps to coordinate the construction of the snapshot with the hypervisor, the guest operating system, and any applications it may be running.
    - In the case of VMware, a VM-consistent snapshot will create a vSphere snapshot, invoke VMware tools if installed in the virtual machine, create a VMstore snapshot of the virtual machine, and then remove the vSphere snapshot.

Snapshots can be created manually through an on-demand process, or created automatically by means of a schedule. Snapshot schedules can be implemented for an individual virtual machine, multiple virtual machines, a Tintri Global Center service group, or through the use of the VMstore default protection policy.

### *Manual Snapshots*

Manual snapshots can be used to create a recovery point prior to a known event. For example, some users may decide to create a snapshot prior to installing operating system updates, or prior to updating a database schema.

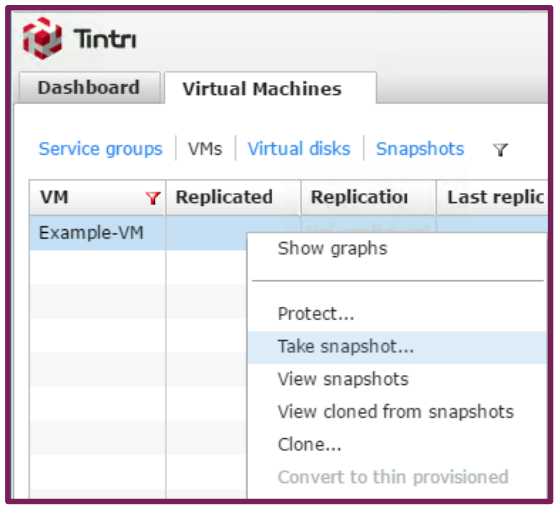



Figure 5: On-demand manual snapshot creation

Snapshots are easily created on-demand by right-clicking a virtual machine and selecting “Take snapshot” from the pop-up menu.

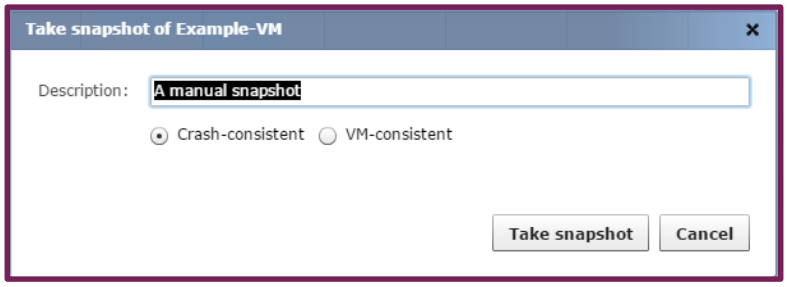



Figure 6: "Take snapshot" dialog window

The “Take snapshot” dialog window includes an editable description field, and the ability to select the creation of a Crash-consistent or VM-consistent snapshot.

Manual snapshots have an infinite retention period, and should be manually deleted when no longer required.

### *Scheduled Snapshots*

A variety of intuitive methods are available for use in creating scheduled snapshots. Among them are the “Default Protection Policy”, “Custom Protection Policies”, and “Tintri Global Center Service Groups”. All scheduling methods contain a collection of similar attributes:

- The frequency at which snapshots should be created; hourly, daily, weekly, monthly, and quarterly for example.
- The length of time that snapshots are retained locally.
- Consistency setting; Crash-consistent or VM-consistent.
- Replication settings
    - Whether or not replication is enabled.
    - At least one replication destination when replication is enabled.
    - The retention period replica for remote snapshots when replication is enabled.

When a scheduled snapshot is created, the retention period of the snapshot is used to calculate an expiration timestamp. At the point in time where the expiration timestamp equals the current time of the

VMstore, the snapshot is deleted. The expiration timestamp is part of the snapshot, and it can be displayed within the VMstore user interface. Note that altering the retention period within an existing schedule will not retroactively alter the retention period for snapshots created prior to the alteration, but will apply the modified retention period to new snapshots.

### *Default Protection Policy*

The VMstore default protection policy can serve as a failsafe mechanism, ensuring that each virtual machine residing on a given array has a basic level of data protection.

To view or configure the default protection policy click the "Settings" button on the VMstore user interface menu bar.


Figure 7: Settings button

The "Settings" dialog window will appear. Within the dialog window select the "Protection" menu item.

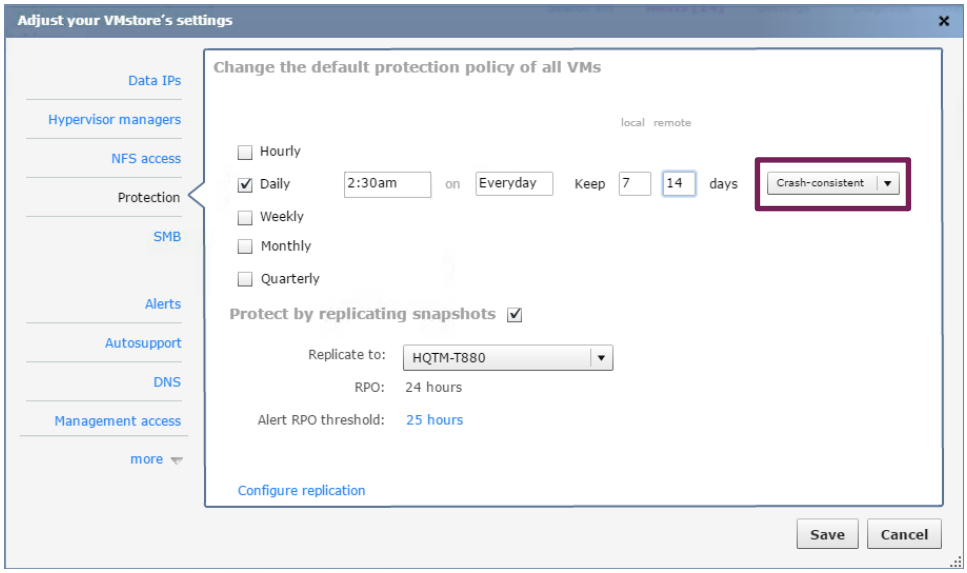



Figure 8: Default protection policy

The example depicted above is a default protection policy for all virtual machines residing on a given VMstore. The default protection policy has been configured to:

- Take daily snapshots at 2:30 AM everyday
- Retain 7 days of local snapshots
- Replicate snapshots
- Retain 14 days of remote snapshots
- Create "Crash-consistent" snapshots

Importantly, snapshot consistency has been set to "Crash-consistent", which is the recommended practice when configuring a default protection policy.

---

***DO:*** *When using the default protection policy, specify the use of "Crash-consistent" snapshots.*

---

Crash-consistency is a recommended practice because it eliminates the possibility that a large number of virtual machines protected by the default protection policy execute hypervisor coordinated snapshots at the same point in time.

Many users prefer to configure a default protection policy which assures that all virtual machines will be protected based on the organizations minimum protection requirements. Other users may prefer to leave the default protection policy in a non-configured state because they have a number of of virtual machines that do not require protection. The non-configured state may also be utilized in cases where virtual machines are being protected by means of a third party backup application.

A wide variety of scheduling options are available to fine tune schedules to meet business requirements.

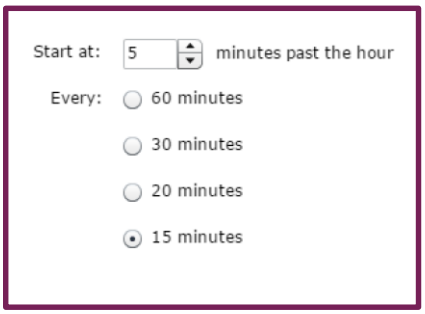



Figure 9: Hourly snapshot options

Hourly snapshot schedules can optionally be configured to occur at a specified number of minutes after the hour, and to repeat at different intervals within the hour. For example, the “Start at 5 minutes past the hour” setting combined with the “15 minutes” radio button depicted in the graphic would result in the creation individual virtual machine snapshots at 5, 20, 35, and 50 minutes after the beginning of the hour.

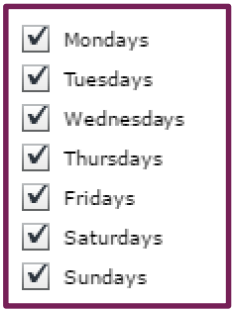



Figure 10: Hourly and daily optional settings

Hourly, daily, and weekly snapshot schedules can optionally be configured to occur only on specific days of the week.

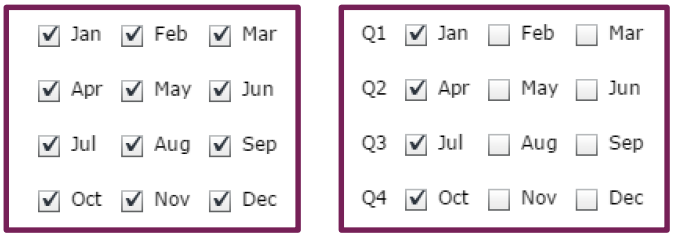



Figure 11: Monthly and quarterly optional settings

Monthly and quarterly schedules provide additional scheduling flexibility, where specific months can be selected, and where specific quarters can be selected.

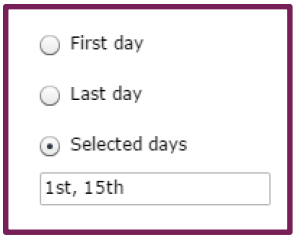



Figure 12: Additional monthly and quarterly options

Monthly and quarterly schedules can be configured to execute on the first day, last day, or specific days.

### *Custom Protection Policies*

Administration of data protection for one or more virtual machines from within the Tintri VMstore user interface is accomplished by right-clicking the virtual machine or a selection of machines, and then selecting “Protect” from the pop-up menu.

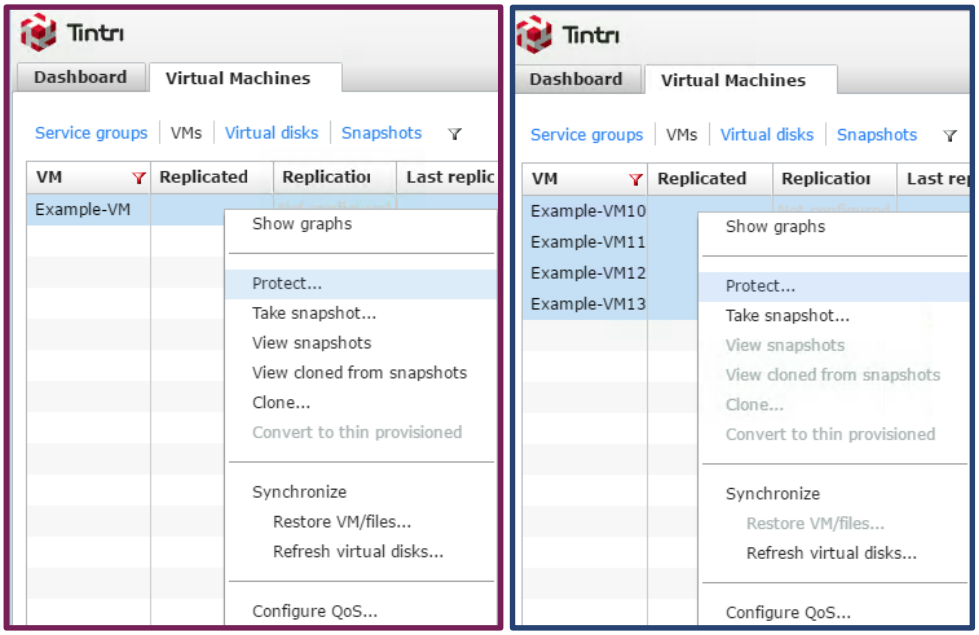



Figure 13: Selecting "Protect" from the pop-up menu

After selecting “Protect” from the pop-up menu, the “Protect” dialog window will appear. At this point the user can add hourly, daily, weekly, monthly, and quarterly snapshot schedules as required to meet organizational requirements.

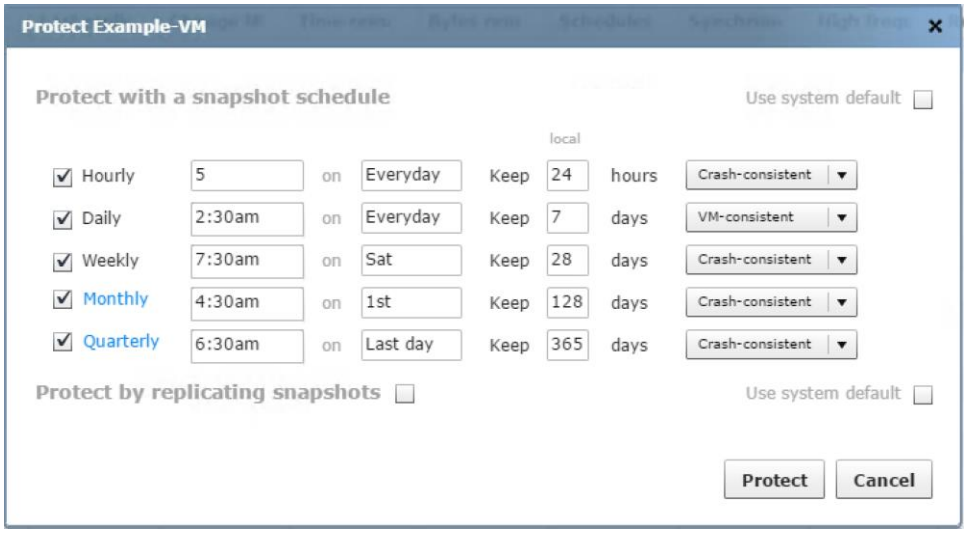



Figure 14: Protect dialog window

As shown, the "Protect" dialog window provides the ability to override use of the default protection policy and to create a variety of schedules; hourly, daily, weekly, monthly, and quarterly. Snapshot retention is specified separately for each schedule, as is snapshot consistency.

---

***DON'T:*** *Avoid scheduling all snapshots to occur at the exact same point in time.*

---

Scheduling the snapshots of hundreds or thousands of virtual machines to occur at the same point in time, 5 minutes past the hour for example, is not recommended. Consider using a variety of offset values for hourly schedules. Similarly, the time at which daily, weekly, monthly, or quarterly snapshots are scheduled to occur can be customized to avoid a scenario where hundreds or thousands of virtual machines are scheduled for snapshot creation at the same point in time. This consideration is particularly important in cases where VM-consistent snapshots are being scheduled, as there is a possibility that the hypervisor may not be able to accommodate the simultaneous creation of a large number of snapshots.

---

***DO:*** *Select VM-consistent snapshots for specific virtual machines that require virtual machine level consistency.*

***DO:*** *Assure that VMware tools are installed and up to date on VMware virtual machines when creating VM-consistent snapshots.*

---

### *Tintri Global Center Service Groups*

Tintri Global Center can also be used to administer snapshot schedules. One advantage of using Tintri Global Center is that a Service Group can be used to manage protection of one or more virtual machines simultaneously. This mitigates any challenge of managing protection for large numbers of virtual machines.

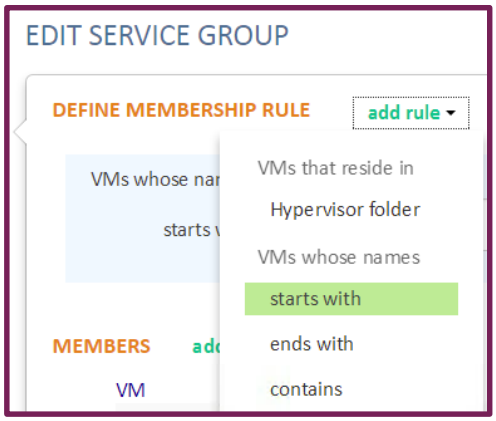



Figure 15: Service Group membership rules

Tintri Global Center Service Groups have membership rules that define which virtual machines will be members of a given group. For instance, a rule can include virtual machine names that start with, end with, or contain a specific character pattern.

The protection characteristics of a given Tintri Global Center Service Group are easily managed. The protection characteristics can be viewed by selecting a Service Group.

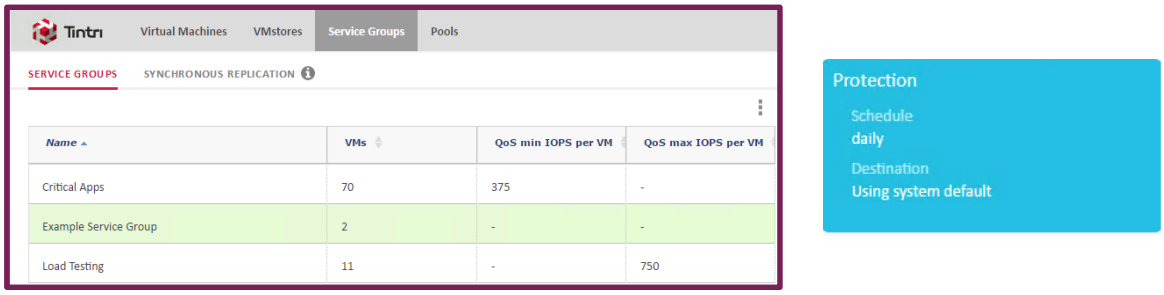



Figure 16: Tintri Global Center Service Group protection

Altering Tintri Global Center Service Group protection properties is accomplished by means of an intuitive interface.

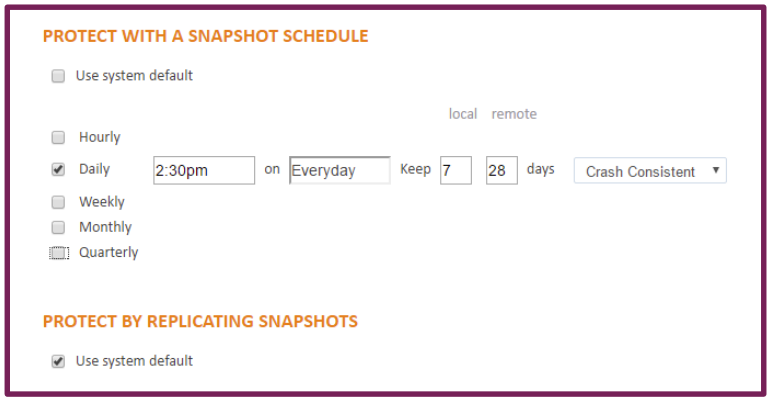



Figure 17: Tintri Global Center Service Group protection properties

The example depicted above includes a daily snapshot schedule and uses the system default replication properties.

Importantly, there exists a chance that a virtual machine may have been configured to be protected using more than a single methodology. For this reason, a policy application model is used to determine which protection methodology will take precedence over another methodology.

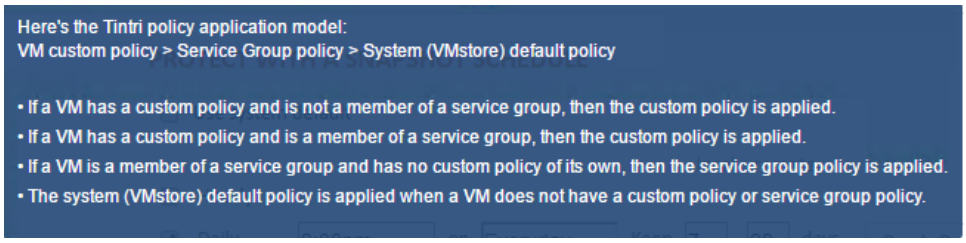



Figure 18: Tintri Global Center policy application model

The policy application model shown in the graphic defines the action that will be taken when a virtual machine has been configured with multiple protection methodologies:

- If a virtual machine has a custom policy and is not a member of a Tintri Global Center Service Group, then the custom policy is applied.
- If a virtual machine has a custom policy and is a member of a Tintri Global Center Service Group, then the custom policy is applied.
- If a virtual machine is a member of a Tintri Global Center Service Group and has no custom policy of its own, then the Service Group policy is applied.
- The system (VMstore) default policy is applied when a virtual machine does not have a custom policy or Tintri Global Center Service Group policy.

## Replication

Tintri VMstore products simultaneously support asynchronous and synchronous replication. This subsection focuses on asynchronous replication. Tintri replication is trademarked as “ReplicateVM”. Replication occurs at the virtual machine level, and is based on individual virtual machine snapshots. “ReplicateVM” is a licensed feature that requires enablement through the use of a license key.

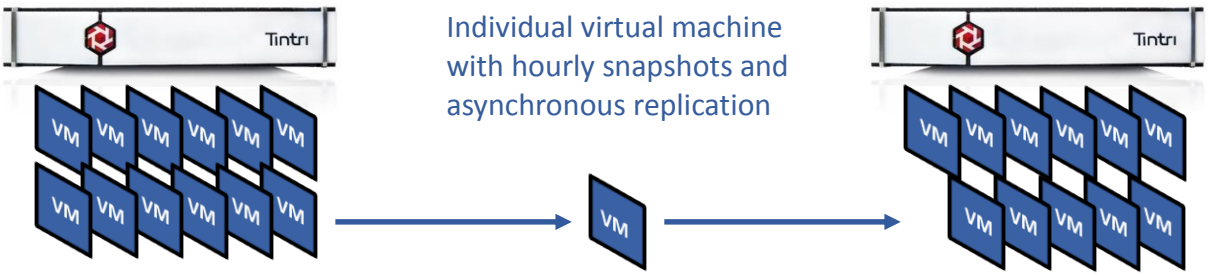



Figure 19: Individual virtual machine replication

Replication efficiency is important from a number of perspectives. One perspective deals with the fact that a replicated snapshot becomes a recovery point for an individual virtual machine on a destination VMstore. It represents a disaster recovery copy of the virtual machine, and the point at which the replication operation completes becomes the point at which the virtual machines enters a “disaster recovery ready” state. Another perspective involves network bandwidth usage. Tintri replication sends only changed blocks between snapshots after deduplication and compression to dramatically reduce the amount of data sent over a WAN connection by up to 95 percent.

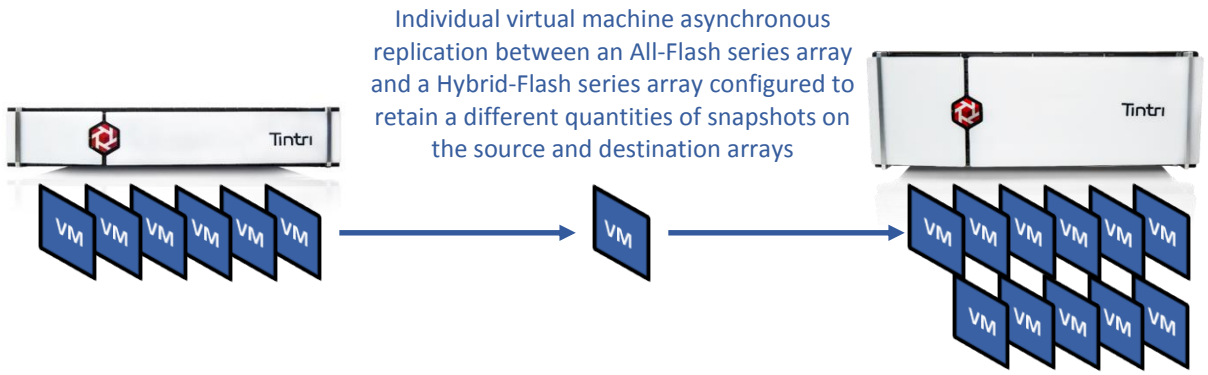



Figure 20: Replication from an All-Flash series array to a Hybrid-Flash series array

The benefits of Tintri replication are:

- Easily replicate only the individual virtual machines that need to be replicated. Unlike LUN based replication where all of virtual machines residing within a LUN are replicated, Tintri replication increases efficiency because only the required virtual machines are replicated to a destination VMstore.
- Replicating only changed blocks between snapshots after deduplication and compression increases efficiency and consume less network bandwidth.
- Easily configure the number of snapshots retained on a destination Tintri VMstore. This capability increases efficiency because only the required number of snapshots are retained on a destination VMstore.
- Replicate individual virtual machines from an all-flash series VMstore to a hybrid-series VMstore. This economical solution reduces cost when fewer snapshots are retained locally on flash and more snapshots are retained remotely on disk.

### *Array Replication Paths*

A single VMstore can be configured with a maximum of 64 outbound replication paths. The same VMstore can simultaneously act as a replication target for other VMstore arrays.

### *Virtual Machine Level Replication*

With Tintri asynchronous replication, a single virtual machine can be replicated outbound to anywhere from 1 to 4 different replication destinations. Replication between different Tintri VMstore array series is also supported, for example replicating from a T5000 All-Flash series array to a T500, T600, or T800 Hybrid-Flash series array.

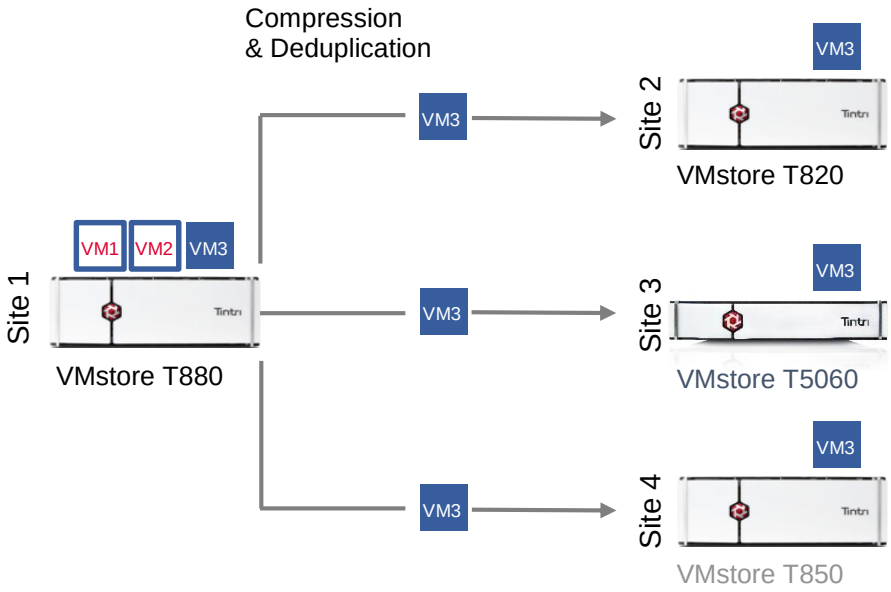



Figure 21: A single virtual machine replicated to 3 different destinations

### *Outbound Replication Paths*

Note: Replication settings are administered from the VMstore user interface by clicking on the “Settings” button on the menu bar. This will open a “Settings” dialog window.


Figure 22: Settings button

From within the “Settings” dialog window, clicking on “more” and then selecting “Replication” will enable the configuration of replication settings.

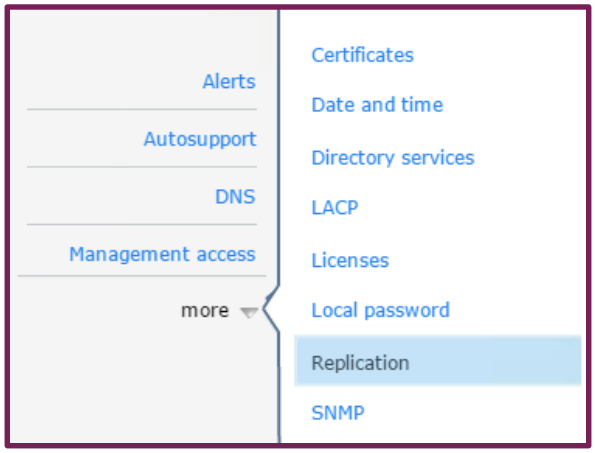



Figure 23: Selecting replication settings

Replication paths are defined on a source VMstore by specifying parameters associated with a given replication destination:

- “Replicate to” is the FQDN (Fully Qualified Domain Name) or IP address of the destination Tintri VMstore array, and the listening port number.

- “Display name” is a user supplied value that identifies the replication target, usually a hostname.
- “Destination passphrase” is the local passphrase of the destination Tintri VMstore array.
- “Replication IP” is the outgoing replication IP address of the local Tintri VMstore.

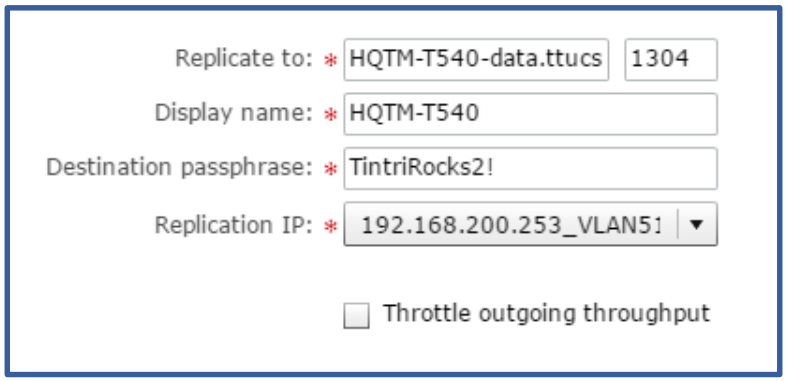



Figure 24: Outbound replication path

It is also possible to create a new replication IP on the local Tintri VMstore. This is accomplished by means of the Replication IP pull-down menu.

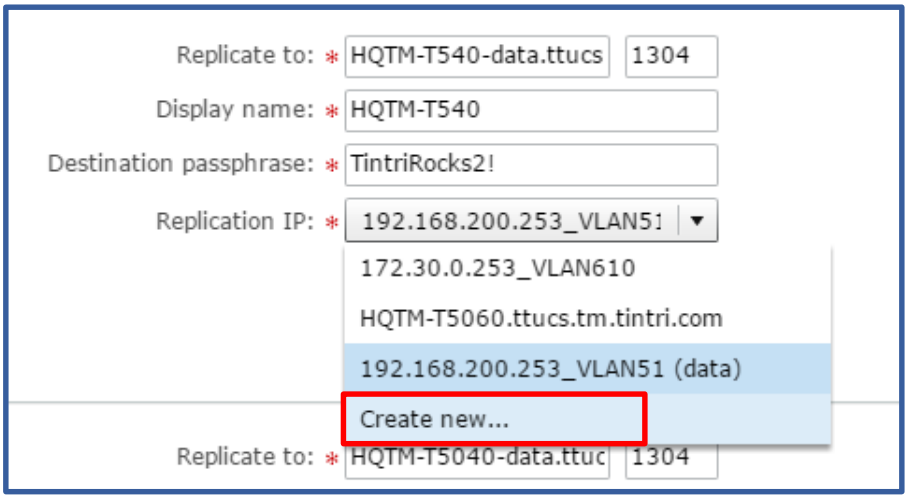



Figure 25: Create new replication IP

Selecting the “Create new” menu item will launch the “Create Replication IP” dialog window.

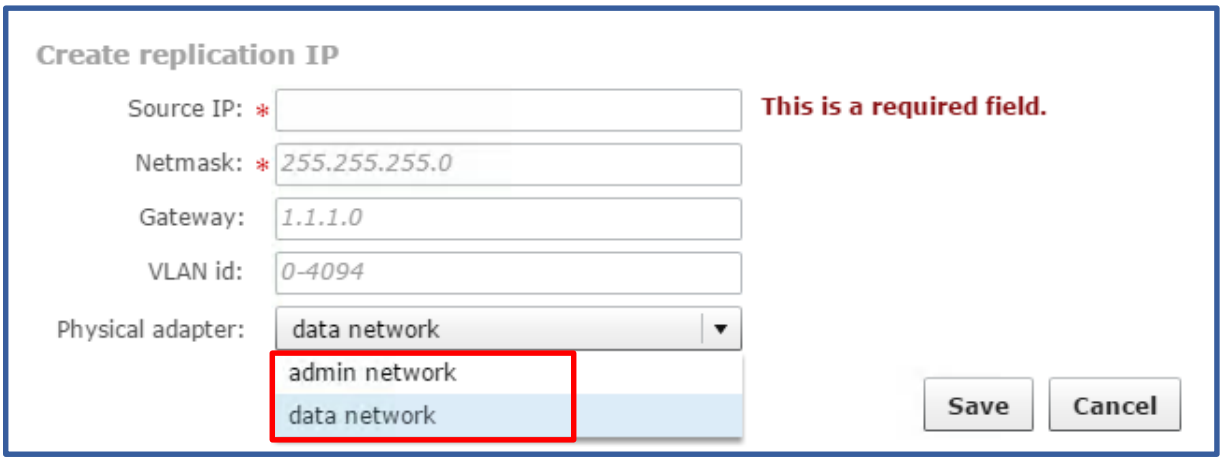



Figure 26: Create Replication IP

Within the “Create Replication IP” dialog window, the source IP, netmask, gateway, and VLAN ID values can be entered. Importantly, the physical adapter is also selected, by means of a pull-down menu. A choice of available physical adapters allows the user to select the desired outgoing replication adapter.

Tintri T800 Hybrid-Flash and T5000 All-Flash series products support an optional replication NIC (Network Interface Controller). The replication NIC can be used to segregate replication traffic, virtual machine traffic, and administrative traffic onto specific networks.

The state of a replication NIC can be determined by viewing controllers from within the hardware tab of the user interface. Clicking on the “Hardware” button on the menu bar will open the hardware tab.


Figure 27: Hardware button

On T800 series products, each controller will include replication network interface status regardless of whether the optional replication NIC is installed.


Figure 28: T800 Series replication network status

On T5000 series products, each controller will indicate the presence of a replication network interface only when the optional replication NIC is installed.


Figure 29: T5000 Series – Optional replication NIC present

T5000 series products also provide replication network interface status for each controller.

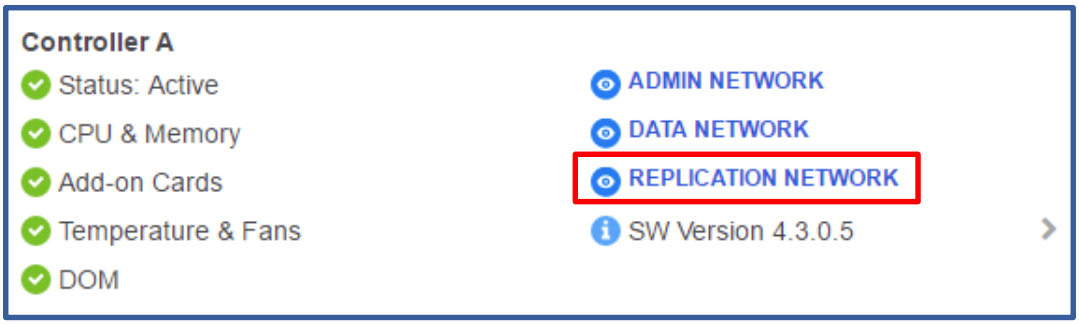



Figure 30: T5000 Series - Replication network

Configuring the optional replication NIC is accomplished by clicking the “Assign IP to replication card” button.

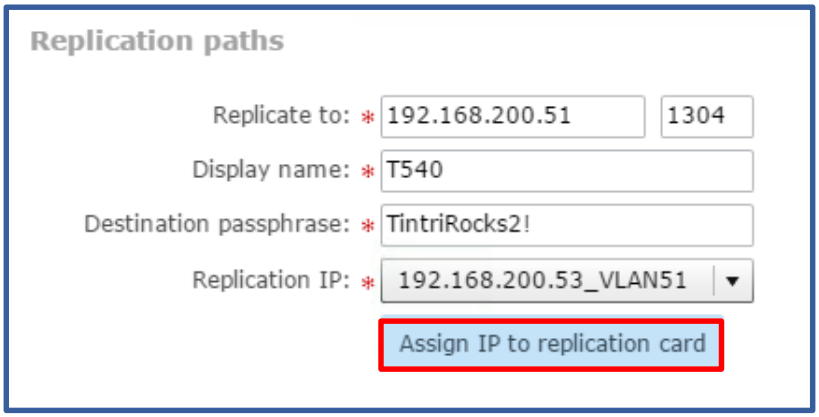



Figure 31: Assign IP to replication card

After clicking the “Assign IP to replication card” button, the “Create replication IP” dialog window will appear.

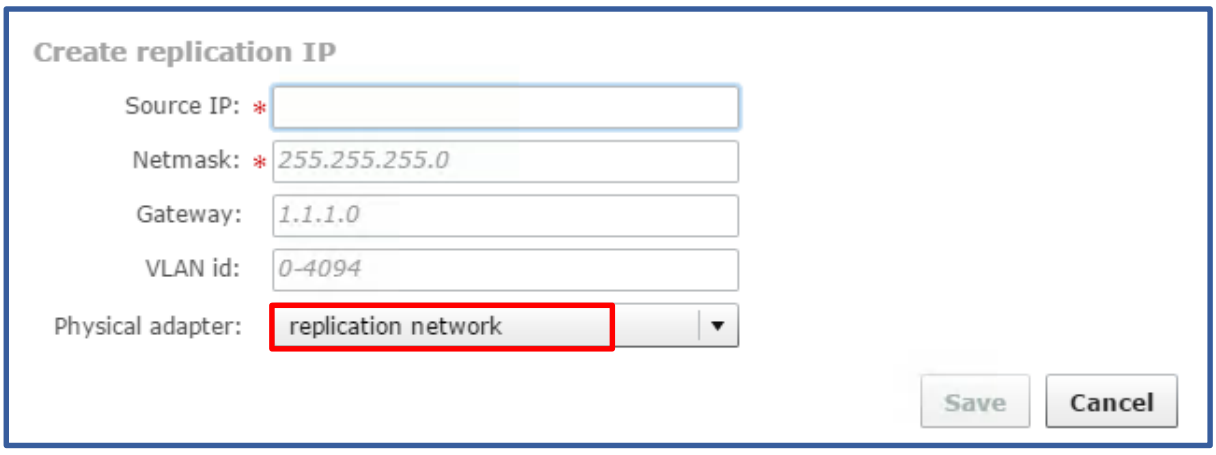



Figure 32: Create Replication IP - Replication Network

Within the “Create Replication IP” dialog window, the source IP, netmask, gateway, and VLAN ID values can be entered. Importantly, the physical adapter is also selected, by means of a pull-down menu. When configuring the optional replication NIC, the replication network physical adapter should be selected.

Also note that outbound data transfer rate can be throttled. Throttling can be customized to occur on specific days of the week and during specific timeframes.


Figure 33: Throttling outbound replication throughput

Business hours can also be customized by clicking on the highlighted “Business hours” link.

The destination port number and passphrase can be determined by viewing replication properties on the destination VMstore.

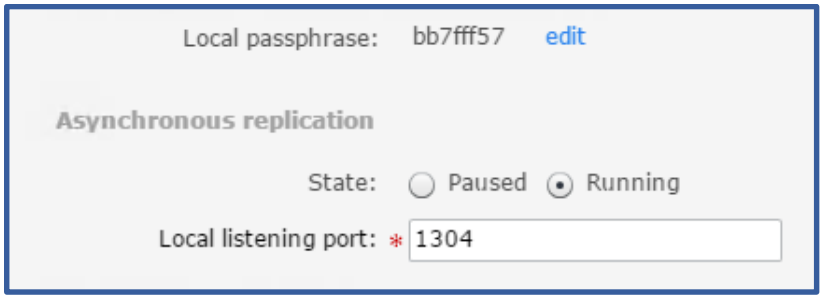



Figure 34: Destination replication properties

In addition to the passphrase and listening port number properties, replication can also be paused.

Once outbound replication paths have been configured, they should be tested in advance of using replication within the default protection policy, a custom policy, or within a Tintri Global Center Service Group.

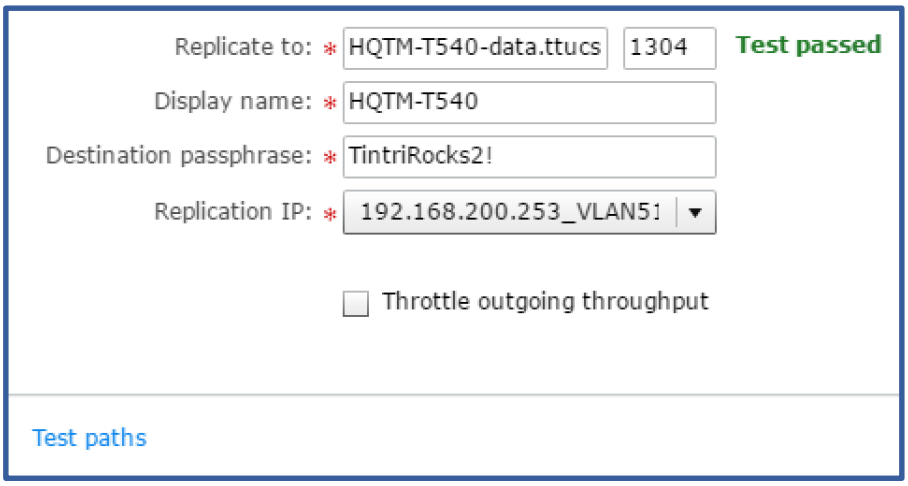



Figure 35: Replication "Test paths"

The replication “Test Paths” function confirms that replication has been configured properly on all outbound replication destinations. When all outbound replication paths are tested, a “Test passed” indicator will be displayed next to each successful path.

***DO:*** *When configuring outbound replication paths, be sure to test the settings with the "Test paths" function.*

### *Adding Replication to Protection*

Replication can be applied to a Tintri VMstore default protection policy, a custom protection policy, or to a Tintri Global Center Service Group.

Note that configuring the replication of an individual machine to more than a single destination requires the use of Tintri Global Center. The ability to replicate a single virtual machine to multiple destination is referred to as "one to many replication".

Adding replication to the default protection policy is accomplished by selecting the "Protect by replicating snapshots" checkbox.

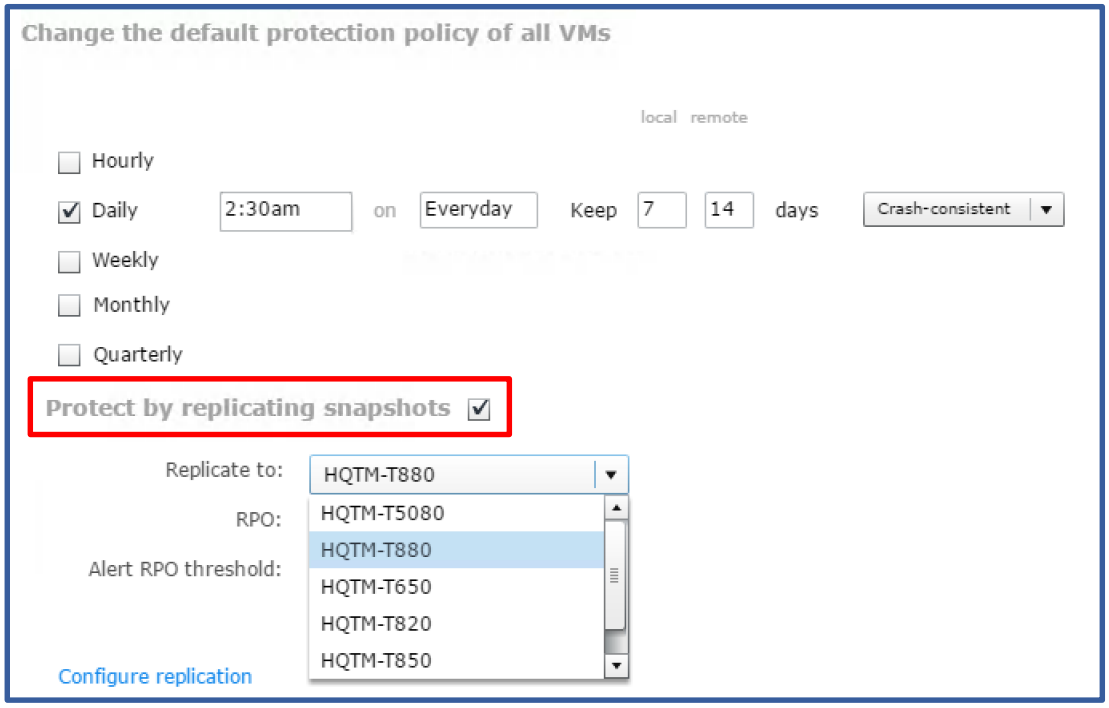



Figure 36: Enabling replication in the default protection policy

The "Replicate to" pull-down menu can be used to select the desired outbound replication destination. Note that the "remote" retention field is also enabled for editing. In addition to retaining local snapshots, replicated snapshot retention is also configured at this time.

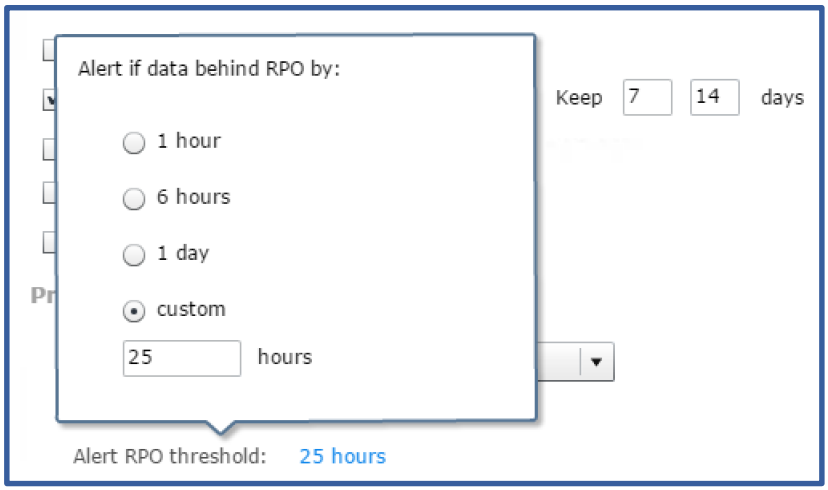



Figure 37: Alert RPO threshold

If desired, the default “Alert RPO threshold” can be altered. Clicking on the current value (25 hours in this example) will cause a pop-up menu to appear. Within the popup menu, a new “Alert RPO threshold” value can be selected or manually entered.

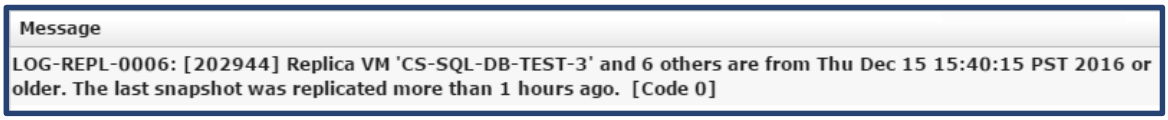



Figure 38: Alert RPO threshold event message

Alert messages are logged to the “Alerts” section of the VMstore user interface. Alerts can also be emailed to serve as a real time notification of a replication (or other) issue.

Applying replication to a custom protection policy is also accomplished by selecting the “Protect by replicating snapshots” checkbox.

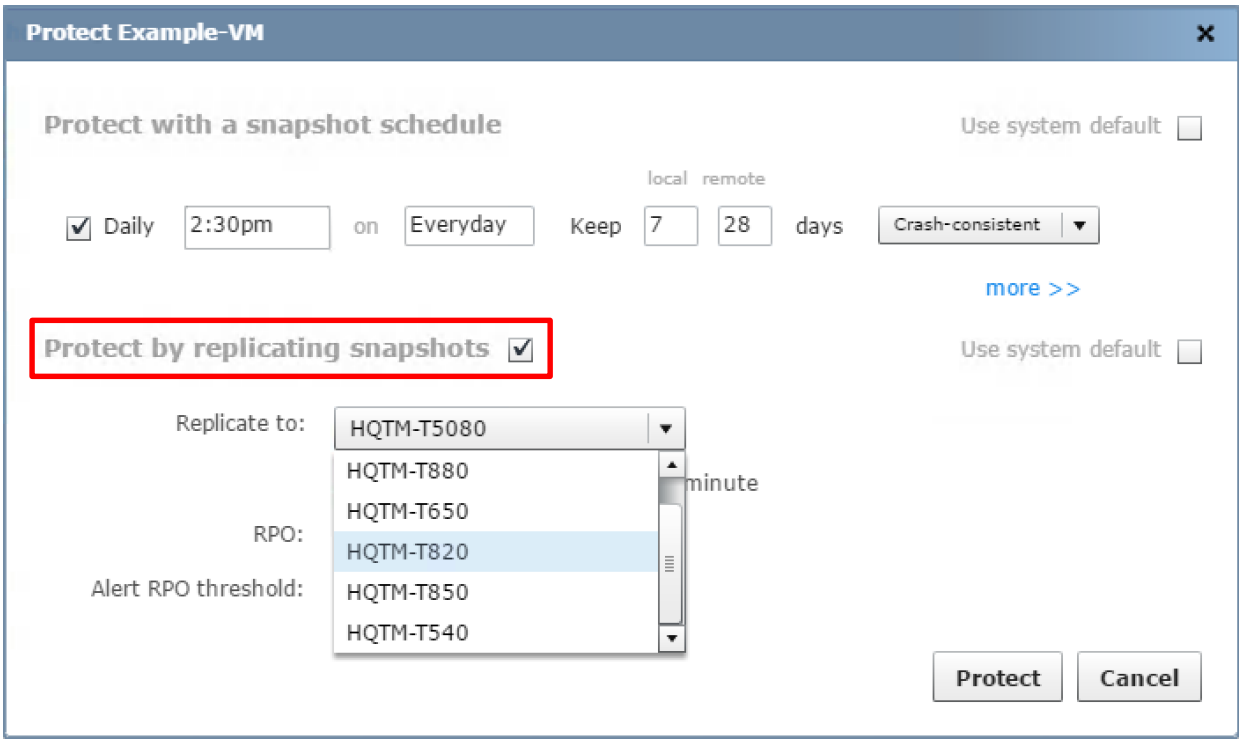



Figure 39: Enabling replication in a custom protection policy

Similar to configuring replication within the default protection policy, the "Replicate to" pull-down menu can be used to select the desired outbound replication destination. Note that the "remote" retention field is also enabled for editing.

Applying replication to a Tintri Global Center Service Group, or to an individual virtual machine within Tintri Global Center is also simple and straightforward.

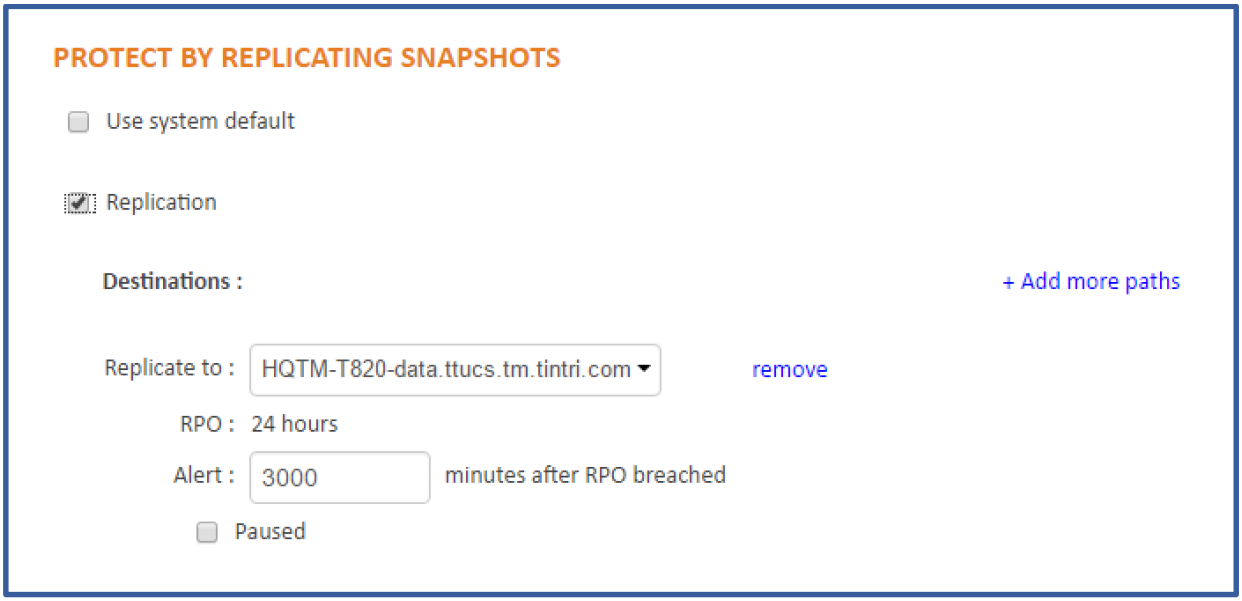



Figure 40: Tintri Global Center replication

Note that the "Use system default" checkbox was disabled by selecting the "Replication" checkbox. At that point the "+ Add more paths" button becomes active and enables the ability to add one or more destination paths.

Configuring the replication of an individual virtual machine to multiple VMstore destinations is configured using this technique, and up to four replication destinations can be configured.

In this example two replication destination have been configured.

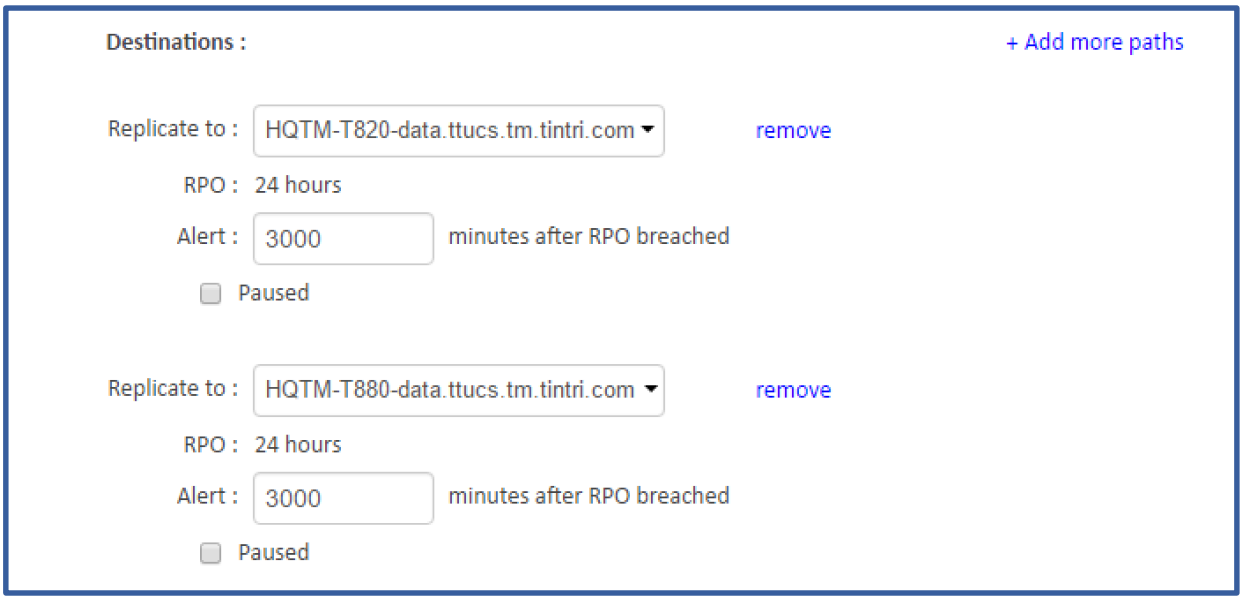



Figure 41: Tintri Global Center replication configuration with 2 destinations

### *Snapshot and Replicate Every Minute – High Frequency Snapshots*

The ability to snapshot and replicate an individual virtual machine every minute is another feature available with replication. This replication methodology retains a single snapshot on the local VMstore, and a single replica of that snapshot on the remote VMstore.

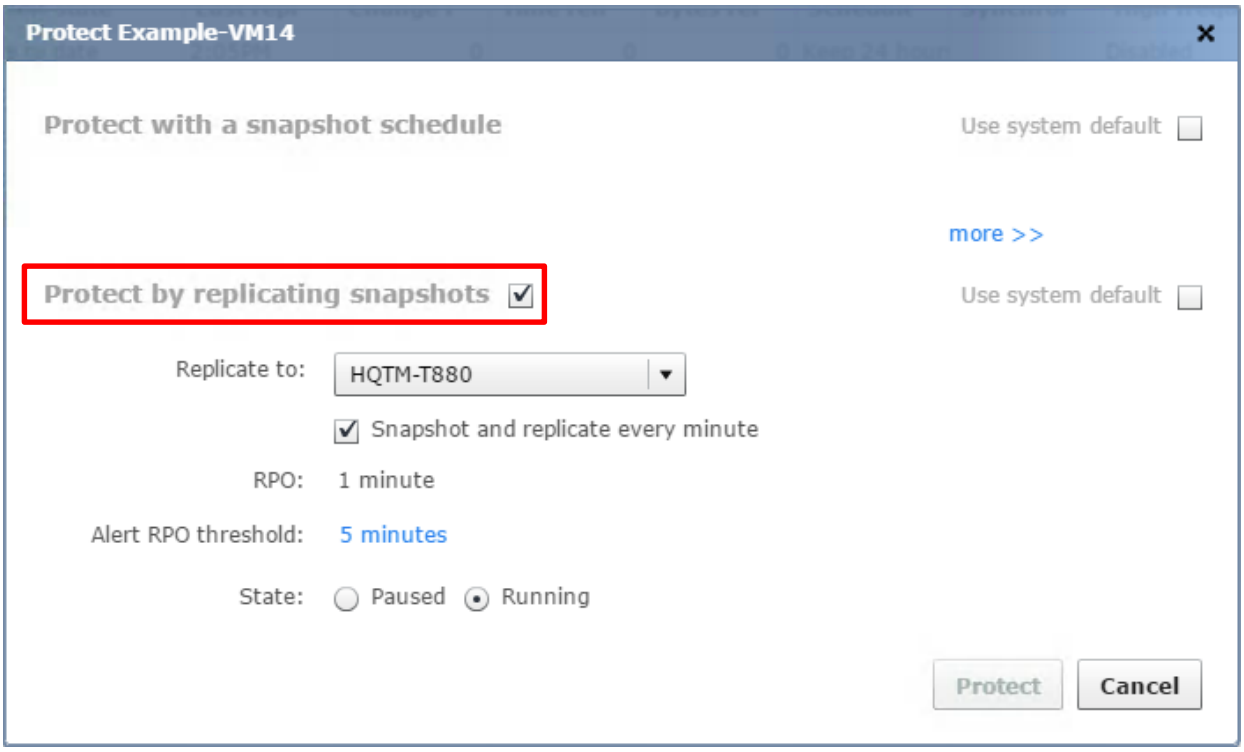



Figure 42: Snapshot and replicate every minute

Note that when using “Snapshot and replicate every minute”, there is no ability to configure the number of snapshots retained locally or remotely. This effectively limits the number of available recovery points to 1. When additional recovery points are required, high frequency snapshots should be augmented with an hourly, daily, or other snapshot schedule.

---

***DO:*** *Augment “Snap and replicate every minute” replication with additional replication schedules when additional recovery points are required.*

---

# Recovery

Restoring an entire virtual machine, virtual disk, or a guest OS folder or file, requires the use of a snapshot from which to restore the data. Creating a clone of a virtual machine also requires the use of a snapshot from which to create the clone.

## Viewing Snapshots

Snapshots are associated with individual virtual machines. Viewing, or locating snapshots associated with a given virtual machine require locating the virtual machine first. From within the VMstore user interface, click the “Search VM” button on the menu bar. This will create a “Virtual Machines” tab within the user interface that displays a list of the virtual machines residing on the VMstore.


Figure 43: Search VM

Users can manually navigate to locate the desired virtual machine, or they can click the “Search VM” button a second time at which point the name of a specific virtual machine can be input as search criteria.

Once the correct virtual machine has been located, right-clicking the virtual machine and selecting “View snapshots” from the pop-up menu displays the snapshots of the virtual machine.

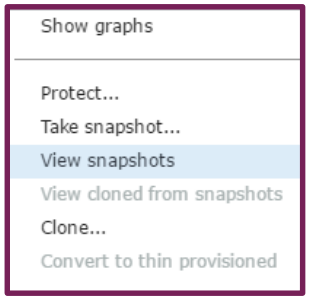
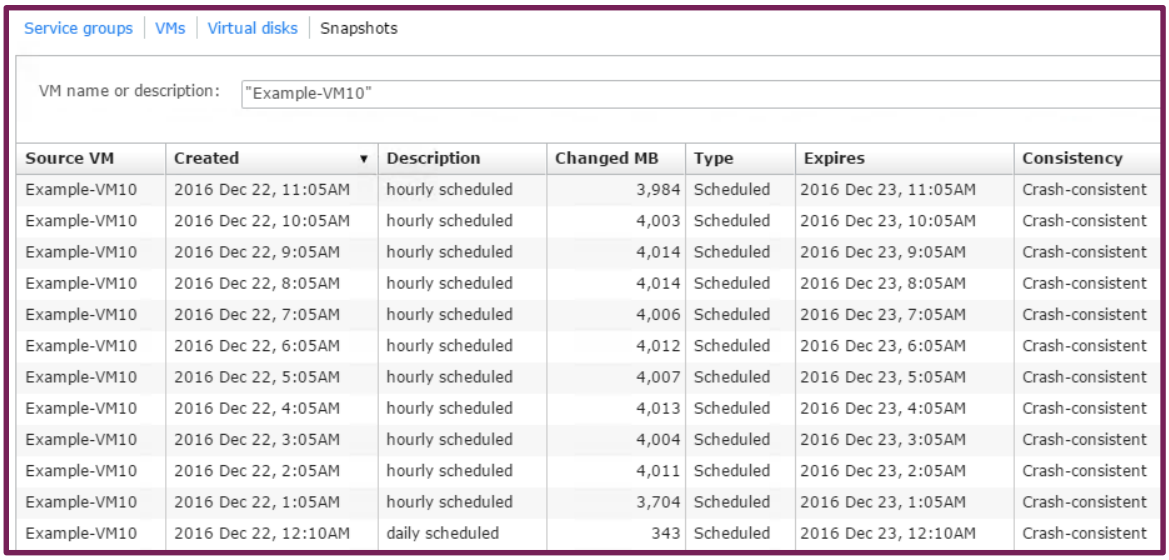



Figure 44: View snapshots

Each snapshot represents a recovery point from a specific time and date.




| Source VM | Created | Description | Changed MB | Type | Expires | Consistency |
|---|---|---|---|---|---|---|
| Example-VM10 | 2016 Dec 22, 11:05AM | hourly scheduled | 3,984 | Scheduled | 2016 Dec 23, 11:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 10:05AM | hourly scheduled | 4,003 | Scheduled | 2016 Dec 23, 10:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 9:05AM | hourly scheduled | 4,014 | Scheduled | 2016 Dec 23, 9:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 8:05AM | hourly scheduled | 4,014 | Scheduled | 2016 Dec 23, 8:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 7:05AM | hourly scheduled | 4,006 | Scheduled | 2016 Dec 23, 7:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 6:05AM | hourly scheduled | 4,012 | Scheduled | 2016 Dec 23, 6:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 5:05AM | hourly scheduled | 4,007 | Scheduled | 2016 Dec 23, 5:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 4:05AM | hourly scheduled | 4,013 | Scheduled | 2016 Dec 23, 4:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 3:05AM | hourly scheduled | 4,004 | Scheduled | 2016 Dec 23, 3:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 2:05AM | hourly scheduled | 4,011 | Scheduled | 2016 Dec 23, 2:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 1:05AM | hourly scheduled | 3,704 | Scheduled | 2016 Dec 23, 1:05AM | Crash-consistent |
| Example-VM10 | 2016 Dec 22, 12:10AM | daily scheduled | 343 | Scheduled | 2016 Dec 23, 12:10AM | Crash-consistent |

Figure 45: Snapshots

Within the snapshot view, a variety of optional fields can be added to the display. Right-clicking within an existing column header row will launch a pop-up menu where additional fields can be selected.

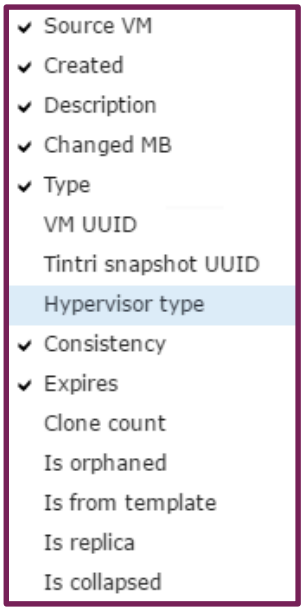



Figure 46: Optional fields

## Cloning

Cloning is the process by which one or more new virtual machines can be created using the virtual machine retained in a snapshot as the basis or starting point for the new virtual machine(s). Cloned virtual machines operate as independent virtual machines with their own identity.

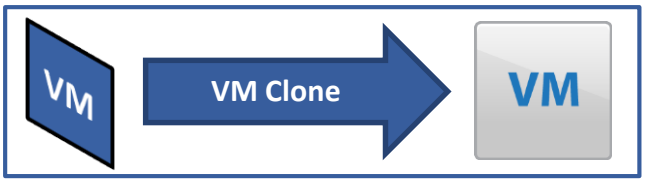



Figure 47: Cloning a virtual machine snapshot to create a new virtual machine

Cloning can be used for a number of data protection and disaster recovery situations. Common use cases include:

- Creating a new virtual machine from a snapshot of a virtual machine that was accidentally deleted from disk.
- Creating a new virtual machine from a snapshot for the purpose of testing local disaster recovery.
- Creating a new virtual machine from a replicated snapshot for the purpose of testing remote disaster recovery.

In the event of a disaster, where cloning a new virtual machine from a snapshot is required, Tintri clones can be instantaneously created without data movement. Because cloning results in new virtual machine creation on a VMstore, the clone is production ready on primary storage without any need to use VMware “Instant Recovery”, and without any need to perform a “Storage VMotion” operation. The elimination of “Instant Recovery” and “Storage VMotion” operations removes virtual machine stun and high latency I/O from disaster recovery operations.

Tintri clones are space efficient as they initially consume no additional space. As snapshot based blocks are updated, the updates are written to new data blocks, at which point a cloned virtual machine begins to consume additional space.

Cloned virtual machines can be created from a snapshot on a local VMstore, or on a remote VMstore.

Creating a clone of a virtual machine based on a snapshot of the original virtual machine is easily accomplished by right-clicking the virtual machine itself, or a specific snapshot of the virtual machine.

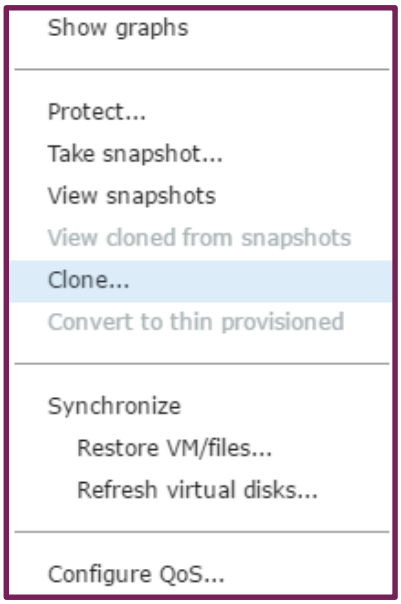



Figure 48: Clone

When cloning from the virtual machine view, the user must select a specific snapshot from which to create the clone.

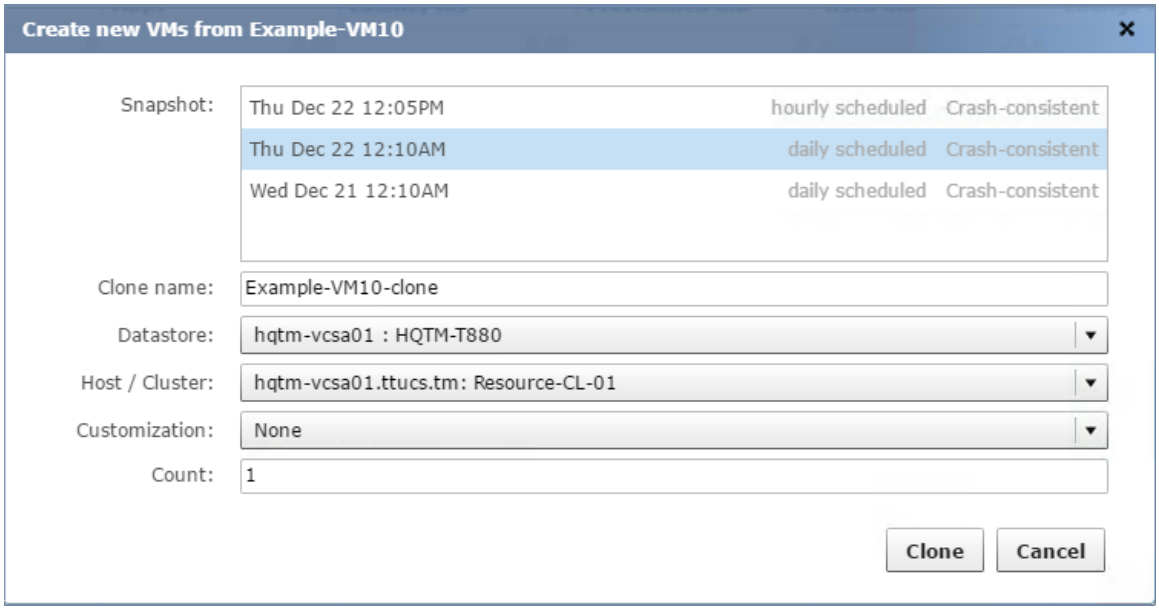



Figure 49: Create clone

By default, the name of a clone will include the suffix “-clone”, which is appended to the name of the original virtual machine on which the clone will be based. The “Datastore” selection dictates which datastore the clone will be created on. The “Host / Cluster” selection dictates the host or cluster resource on which the cloned virtual machine will execute. Note that the “Customization” and “Count” parameters are typically not used for data protection or disaster recovery purposes.

The clone operation will add the cloned virtual machine to inventory on the specified hypervisor manager. The cloned virtual machine will appear within the VMstore user interface.

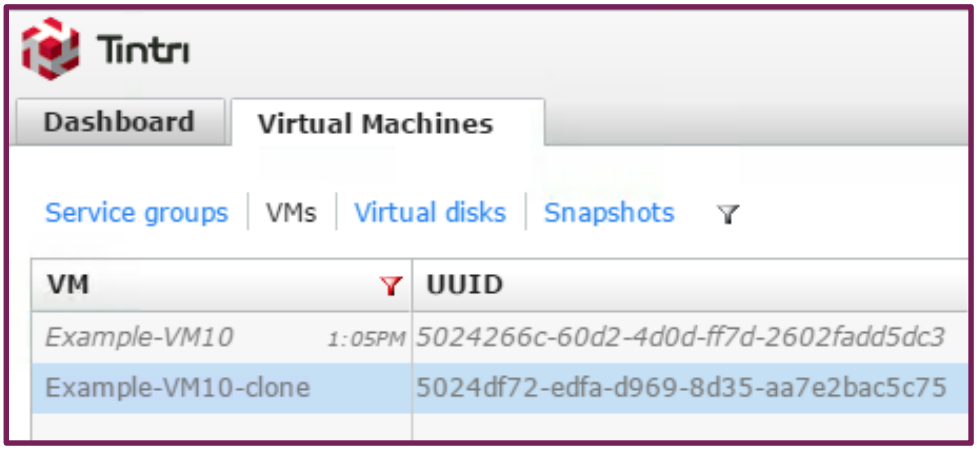



Figure 50: Cloned virtual machine

Note that the cloned virtual machine will have a different “UUID” when compared to the original virtual machine.

The cloned virtual machine can be deleted by means of the hypervisor manager when it is no longer needed.

## Restoring

Tintri uses an individual virtual machine snapshot as the recovery point for a variety of recovery scenarios. Tintri restore functionality is trademarked as “SyncVM”, which can also be used to synchronize disks for test and development purposes. This subsection focuses on the use of this technology for the purpose of data recovery. “SyncVM” is a licensed feature that requires enablement through the use of a license key.

Recovery is automated in the sense that the user only needs to select what needs to be recovered by means of an easy to use interface. There are no pre-requisite tasks involving the cloning of a LUN from a snapshot, adding cloned LUNs as hypervisor storage, adding a virtual machine to hypervisor inventory, or manually adding a virtual disk to a guest. Additionally, there are no post-recovery clean-up operations required, such as removing a virtual disk or deleting a cloned LUN.


Figure 51: Full virtual machine recovery

Full virtual machine recovery is accomplished with a simple process where the snapshot to restore from is selected by means of a pull down menu, and clicking the “Restore” button initiates the restore process.


Figure 52: Virtual disk recovery

Virtual disk recovery, where one or more virtual machine disks are restored, is also accomplished by means of a simple process where the snapshot to restore from and specific disk or disks to recover are selected.


Figure 53: Granular folder / file recovery

The intuitive workflow employed for granular folder and file level recovery adds the appropriate snapshot based virtual disk image as a new drive to the specified virtual machine. Within the guest operating system the new drive is manually brought online and then assigned a drive letter. Drag and drop folder and file level recovery is then easily accomplished. By default, any added drives are automatically disconnected after 48 hours.

Tintri restore technology simplifies the administrative overhead routinely associated with data recovery at a full virtual machine, virtual disk, or granular folder and file level.

The following subsections describe features supported with VMware and Hyper-V. Feature support requires that the virtual machine is not a linked clone, and that the virtual machine does not have any VMware vSphere snapshots.

Restore operations are performed using a local snapshot as a recovery point.

### *Full VM Restore*

When performing a full virtual machine restore, any existing snapshot schedules, replication, or QoS (Quality of Service) settings remain the intact after the restore completes. Performance history also remains intact.

The restore process is initiated by right-clicking the virtual machine, and selecting “Restore VM/files” from the pop-up menu.

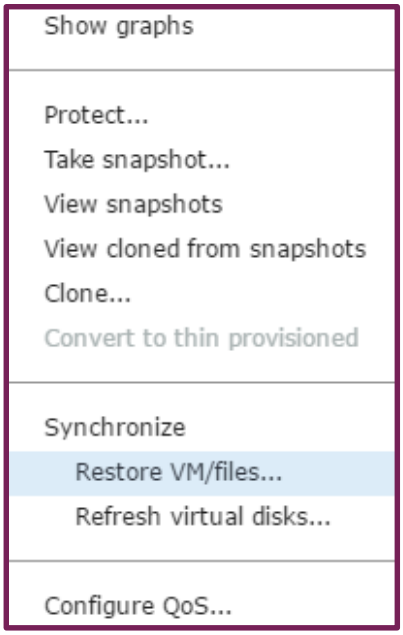



Figure 54: Restore VM/files

The “Restore VM” dialog window will appear. At this point a snapshot to restore from can be selected.

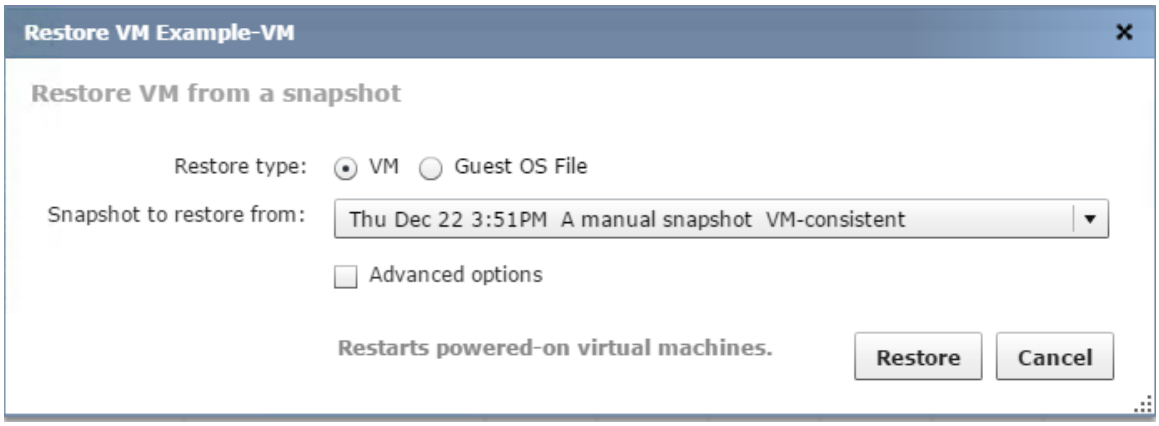



Figure 55: Restore VM

The automated restore process consists of a number of steps that occur behind the scenes, and can be monitored from the hypervisor.

When restoring a VMware virtual machine from a VM-consistent snapshot, advanced options are available to specify the datastore and host/cluster where the temporary clone is placed.

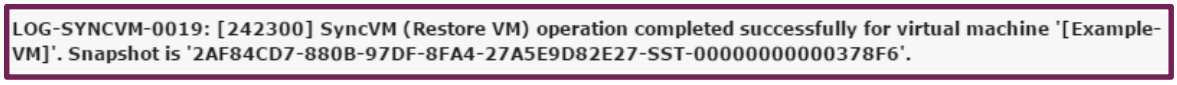



Figure 56: Restore virtual machine event

Alert messages are logged to the “Alerts” section of the VMstore user interface. The alert depicted above indicates that the operation was completed successfully.

### *Virtual Disk Restore*

The process of restoring one or more virtual disks is initiated by right-clicking the virtual machine, and selecting “Refresh virtual disks” from the pop-up menu.

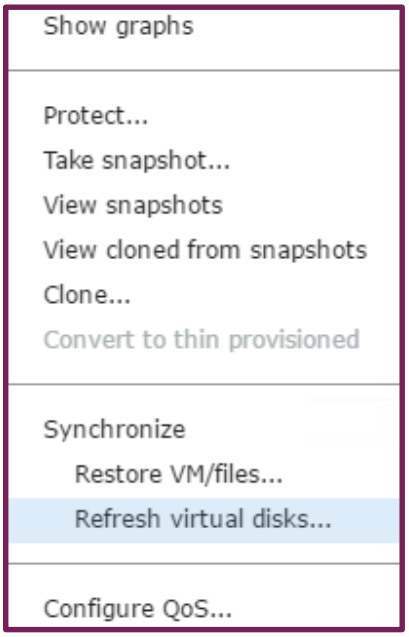



Figure 57: Refresh virtual disks

The “Refresh vDisks” dialog window will appear. At this point a virtual machine to refresh from can be selected. In most virtual disk recovery scenarios, the “VM to refresh from” should be the same virtual machine that was selected and right-clicked earlier in this subsection.

Note that the “VM to refresh from” pull-down menu will allow the user to recover a virtual disk from a different virtual machine than the virtual machine being recovered. This use case is typically reserved for test and development workloads.

Next, select the snapshot to refresh (recover) from. The target virtual disks of the virtual machine being recovered appear as SCSI devices. Each SCSI device corresponds to a virtual disk configured within the selected virtual machine.

In this example “SCSI 0:0” is a VMware virtual device node for hard disk 1, and “SCSI 0:1” is a VMware virtual device node for hard disk 2. To refresh (recover) hard disk 2 select “SCSI 0:1” from the pull-down menu for target virtual disk “SCSI 0:1”.

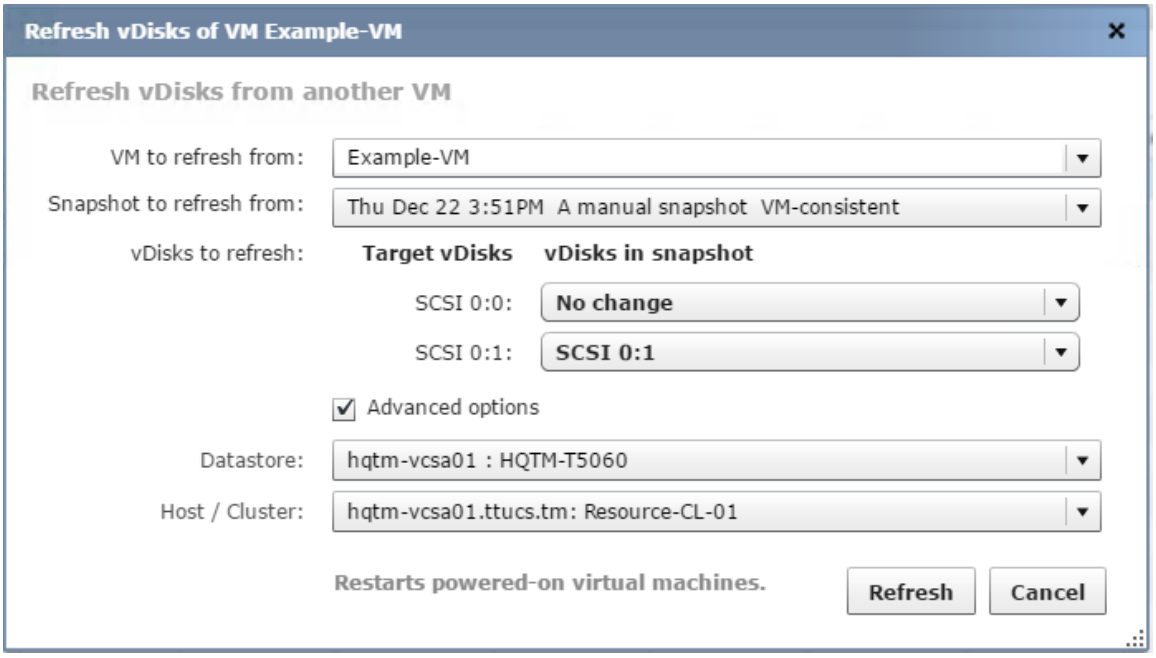



Figure 58: Refresh vDisks

The automated virtual disk restore process consists of a number of steps that occur behind the scenes, and can be monitored from the hypervisor.

When restoring a VMware virtual machine from a VM-consistent snapshot, advanced options are available to specify the datastore and host/cluster where the temporary clone is placed.

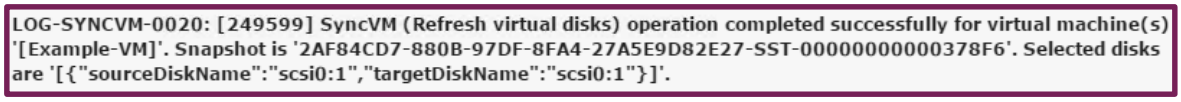



Figure 59: Refresh virtual disk event

Alert messages are logged to the “Alerts” section of the VMstore user interface. The alert depicted above indicates that the operation was completed successfully.

### *Guest OS File Restore*

The restore process is initiated by right-clicking the virtual machine, and selecting “Restore VM/files” from the pop-up menu.

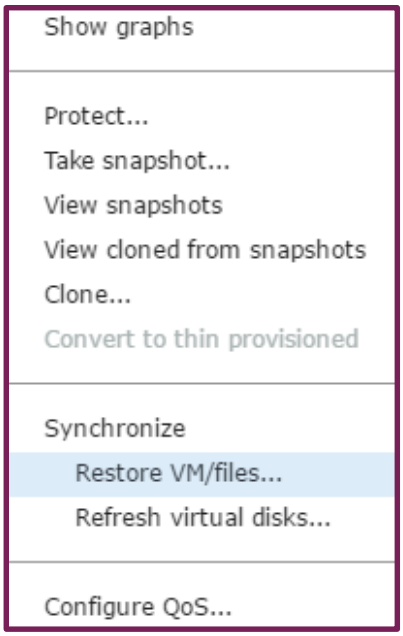



Figure 60: Restore VM/files

The “Restore VM” dialog window will appear. Click the “Guest OS File” radio-button, and select a snapshot to recover from.

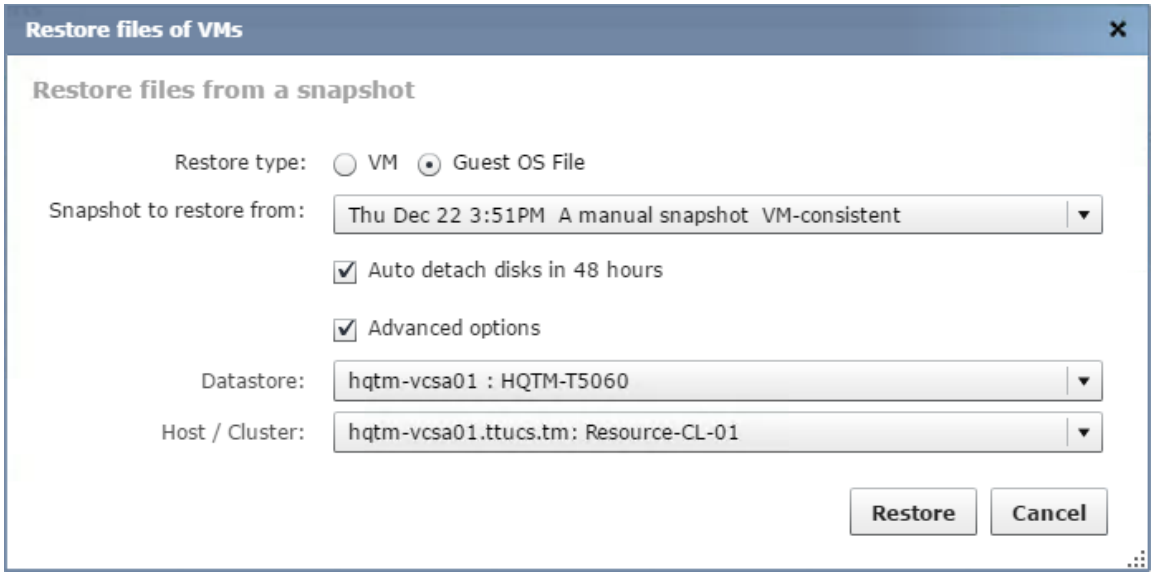



Figure 61: Restore files of virtual machine

By default, the “Auto detach disk in 48 hours” check-box is enabled. This eliminates any administrative requirement to manually detach disks that have been added to the virtual machine after recovery has been completed.

---

***DO:*** *When restoring virtual machine files or folders, leave the “Auto detach disks in 48 hours” function enabled.*

---

The automated restore process consists of a number of steps that occur behind the scenes, and can be monitored from the hypervisor.

When restoring a VMware virtual machine from a VM-consistent snapshot, advanced options are available to specify the datastore and host/cluster where the temporary clone is placed.

LOG-SYNCVM-0024: [249753] SyncVM (File-Level Restore) operation completed successfully for virtual machine(s) '[Example-VM]'. Snapshot is '2AF84CD7-880B-97DF-8FA4-27A5E9D82E27-SST-00000000000378F6'.

Figure 62: File restore event

Alert messages are logged to the “Alerts” section of the VMstore user interface. The alert depicted above indicates that the operation was completed successfully.

Within the virtual machine guest operating system, the virtual disks present in the snapshot selected to recover from appear as offline disks.

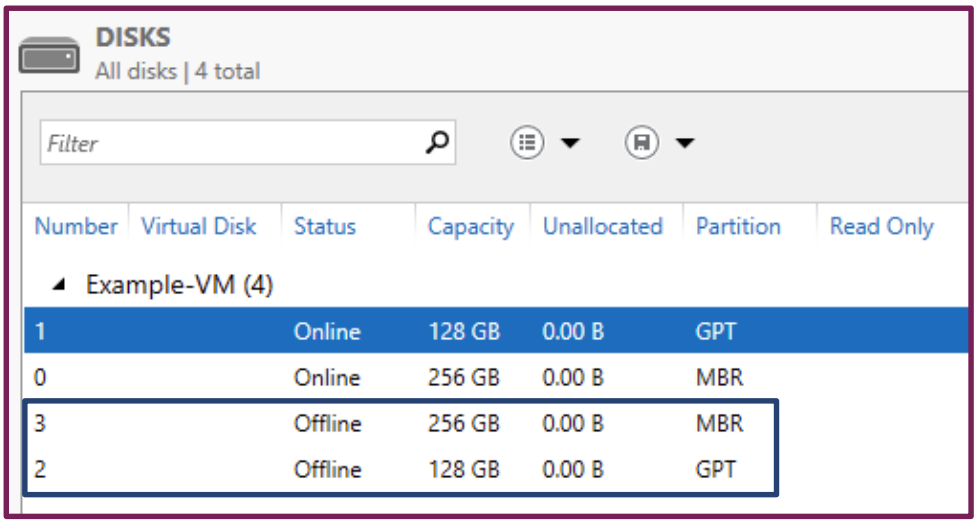



Figure 63: Offline disks

One or more of the offline disks can be set to online. At this point the online drive appears as a volume within the virtual machine guest operating system.

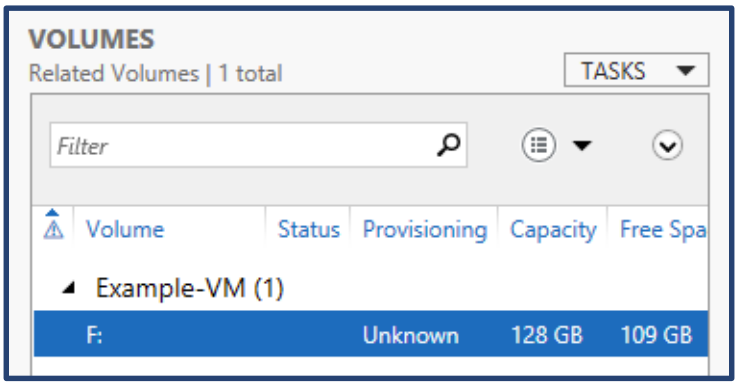



Figure 64: Volume

At this point, files and folders from the online volume can be copied to a different volume on the virtual machine. Familiar “drag and drop” or “copy and paste” tasks are then used to recover the desired folders or files.

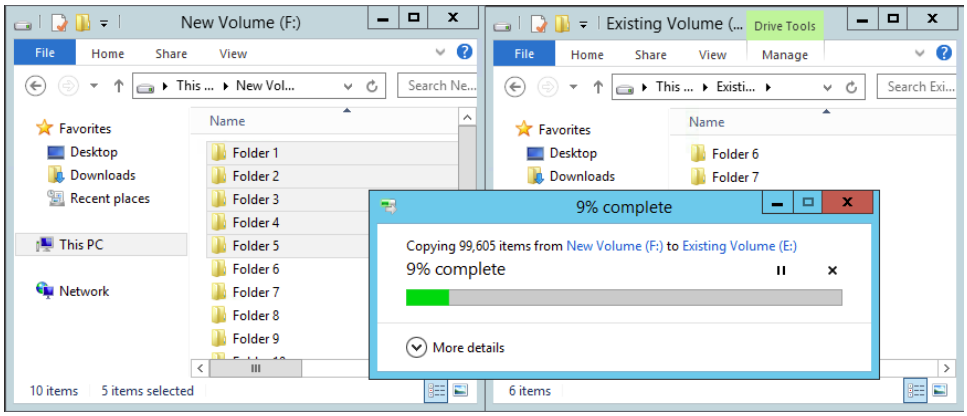



Figure 65: Granular folder / file restore

The recovery disks will be automatically detached from the virtual machine after 48 hours if the default setting “Auto detach disk in 48 hours” was left in an enabled state.

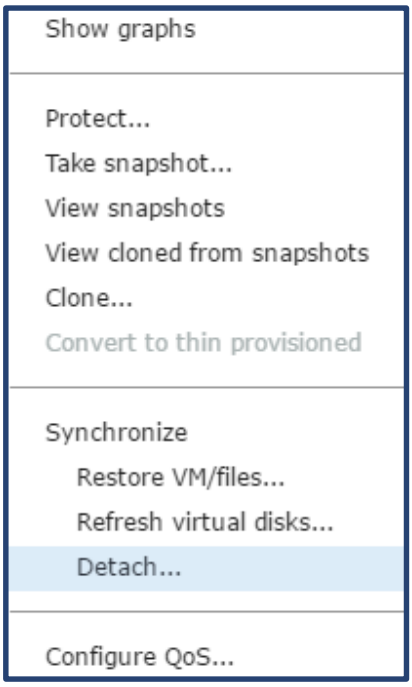



Figure 66: Detach

Alternatively, the recovery disks can be manually detached by right-clicking the virtual machine from within the VMstore user interface, and selecting “Detach” from the pop-up menu.

## Analytics

Real time and historical analysis of operations is usually performed as the result of a performance issue or outright failure. The VMstore includes industry leading analytics that assist in analyzing a challenge or failure. Tintri Global Center extends this capability by automatically maintaining the most recent 30 days of analysis data for the VMstore arrays being managed.

Replication is one area that may require analysis based on factors such as a slow replication link, attempting to replicate more data than network bandwidth can reasonably accommodate, or a network outage.

The VMstore provides clear and concise tools that assist in analyzing replication operations. The first is the ability to view replication data waiting to be replicated. This correlates to new snapshot resident data that became eligible for replication at the time a snapshot was created. Ideally, all eligible snapshot data is replicated in a timely manner and prior to the creation of a subsequent snapshot.

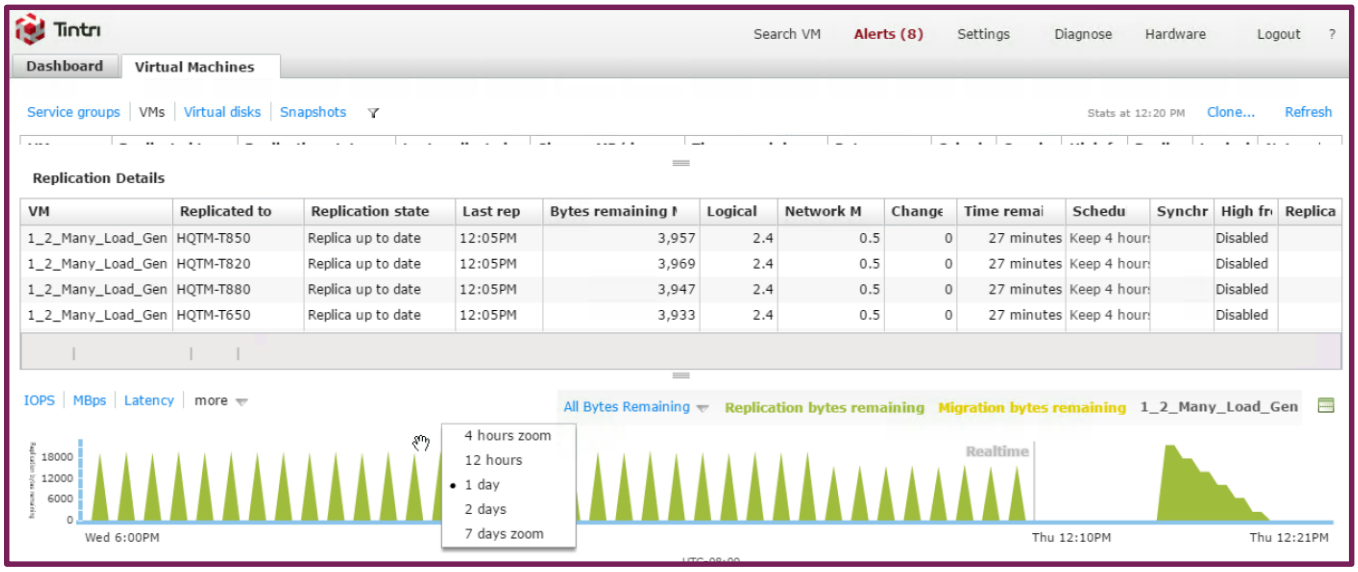



Figure 67: Replication bytes remaining

The graphic depicts asynchronous replication of a single virtual machine to 4 different destinations. Analytics are available in tabular format, and in graphical format. “Replication bytes remaining”, or data yet to be replicated, is easy to view as it occurs in real time, or at a user selectable level of granularity over the most recent 7 days.

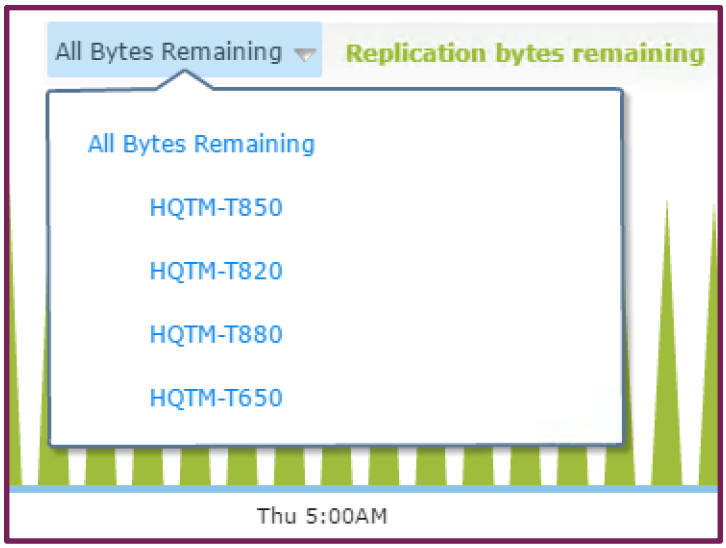



Figure 68: Filters for a single replication destination

Drilling down to view the replication analytics for a single destination is as simple as clicking on a pull-down menu, where the desired destination can be selected.

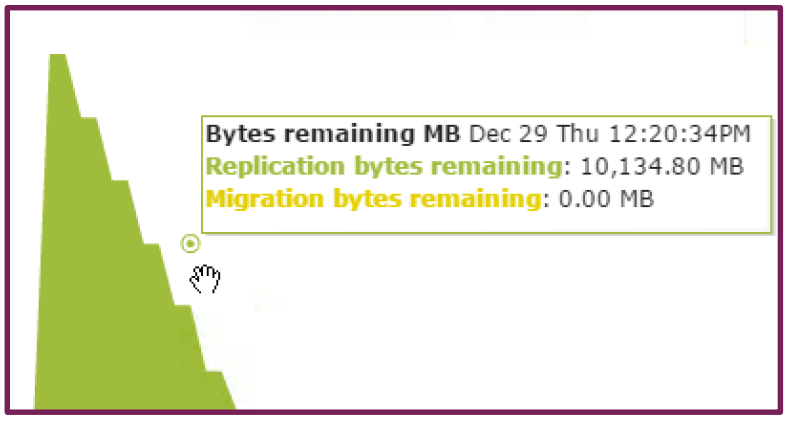



Figure 69: Detailed analytics

Hovering over a specific point in the graphical portion of the user interface provides detailed analytic data to assist in forensic analysis.

Large or excessive amounts of data not yet replicated may be the result of many factors, such as a replication link that was down for a period of time, abnormally large data change rates between snapshots, or a heavily congested replication network, for example.

Another tool provides the ability to view the replication rate for a virtual machine. The rate is expressed in MB/s and includes both logical and network data transfer rates.

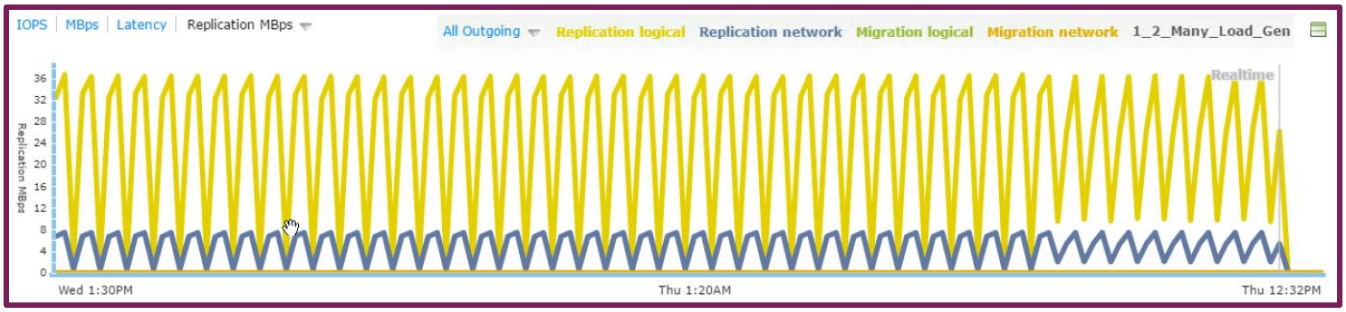



Figure 70: Replication MB/s

The logical replication rate is typically greater than the network replication rate, the result of efficiency based on replicating only unique deduplicated and compressed data blocks. Similar to when viewing “replicated bytes remaining”, “replication MB/s” allows drilling down to view a specific replication destination by means of a pull-down menu.

Tintri Global Center provides access to the same comprehensive suite of analytics. Tintri Global Center provides access to the last 30 days of analytics, and also enables downloading data to a CSV file.

## Summary

The goal of a data protection and disaster recovery solution that meets service level agreements has long been a business requirement. Ongoing challenges such as total cost of ownership, reliability, and performance continue to make this goal difficult to achieve. Organizations are under constant pressure to reduce cost, eliminate failures, and at the same time, enhance performance.

Tintri assists users in achieving these goals in a tangible way with advanced technology:

- Virtual machine level protection; snapshot only the virtual machines requiring protection, retain only the required number of snapshots for a virtual machine, and replicate snapshots of only the virtual machines that require it.
- Space efficient snapshots that invoke no data movement at creation time. Array based snapshot creation does not involve the moving or copying of a backup payload to a backup device. Forget about backup streams, transport modes, and backup storage devices.
- Bandwidth efficient replication, where only unique deduplicated and compressed blocks are transmitted to one or more destinations, and only for the virtual machines that need to be replicated.
- Replication from All-Flash series products to Hybrid-Flash series products further improves cost efficiency. Forget about retaining large numbers of recovery points on expensive flash media.
- Test data recovery and disaster recovery easily, before a data loss or disaster event strikes to reduce failure rates. Perform testing as frequently as required, without impact to production workload or ongoing data protection activity.
- Recover from a disaster faster with individual virtual machine cloning where there is no data movement at recovery time. Forget about VMware “Instant Recovery” and “Storage VMotion”. Stop worrying about stunned virtual machines and high latency I/O during “Storage VMotion” operations. Individual virtual machine clones are instantaneously created on primary storage in a production ready state.

## References

Tintri VMstore All Flash/Hybrid System Administration Manual

Tintri Global Center System Administration Guide

303 Ravendale Drive
Mountain View CA 94043
+1 650.810.8200
info@tintri.com