VMware Cloud Disaster Recovery: Using Quiescing to improve VM snapshot consistency

VMware Architecture

Table of contents

VMware Cloud Disaster Recovery: Using Quiescing to improve VM snapshot consistency

Introduction

VMware Cloud Disaster Recovery uses VMware Snapshots on the Protected Site to preserve all the Virtual Machine data at the time you take the snapshot. Changed block tracking allows the changes since the last snapshot to be determined and the VMware Cloud DR connectors use this to send the incremental changes to the Scaleout Cloud File System - providing an immutable space efficient recovery point which remains until the retention period expires. Quiescing wraps around the taking of a snapshot with pre & post steps that give additional control to interact with applications and improve data consistency.

Quiescing the virtual machine, co-ordinates these actions with taking the snapshot:
- Place the file system in a consistent state on disk
- Run custom scripts before and after the snapshot
- (for Windows) Invoke Volume Shadow Services writers for registered applications

This quiescing option has been available VCDR Protection Groups leveraging vSphere Storage APIs for Data Protection (VADP) snapshots since the first release of VCDR, but with the update in February 2024 quiescing is also available in Protection Groups that are using High Frequency Snapshots (HFS). The minimum Protected Site vSphere version requirements are 7.0U3c for HFS and 8.0U1 for quiescing + HFS (which for a VMC on AWS SDDC equates to 1.16 and 1.20v6 respectively).

This is a guide provided as is, not support documentation.

Configuring Protection Groups

In VMware Cloud DR create a Protection Group either:

1. With standard snapshots and select the Quiesce option – this will use VADP to create & then consolidate snapshot files and can have a significant source site infrastructure overhead, particularly in terms of additional storage i/o on larger and fast changing VMs . Minimum supported RPO is 4 hours with VADP snapshots.
2. With high frequency snapshots provided that the source site meets the minimum vSphere requirements to support quiescing with HFS. Minimum RPO is 30 minutes for schedules including quiescing and 15mins without as frequent quiescing can be onerous on some applications. HFS uses memory based change tracking avoiding the need for snapshot files and the associated overhead.

Enabling quiescing in VCDR is via a checkbox in the Protection Group configuration & is optional for each PG schedule. Eligibility of protected sites and hosts is checked and presented automatically. Quiescing compatibility can also be checked via a compatibility check button in the first PG setup screen. As usual configure membership to include the required VMs and specify desired scheduling/retention noting that 15min RPOs are not supported for quiescing,

Because quiescing is a Protection Group setting if you have an application or requirement for a set of VMs where some must be quiesced and others not quiesced then these VMs need to be divided between two separate Protection Groups.

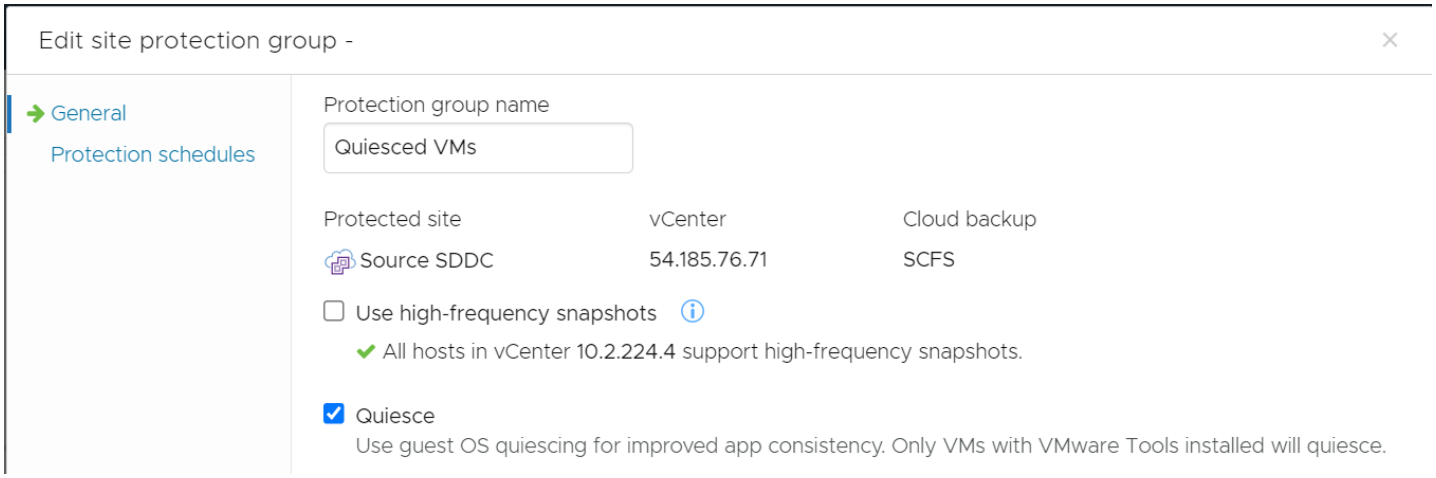

Image 1 - VADP snapshot with quiescing

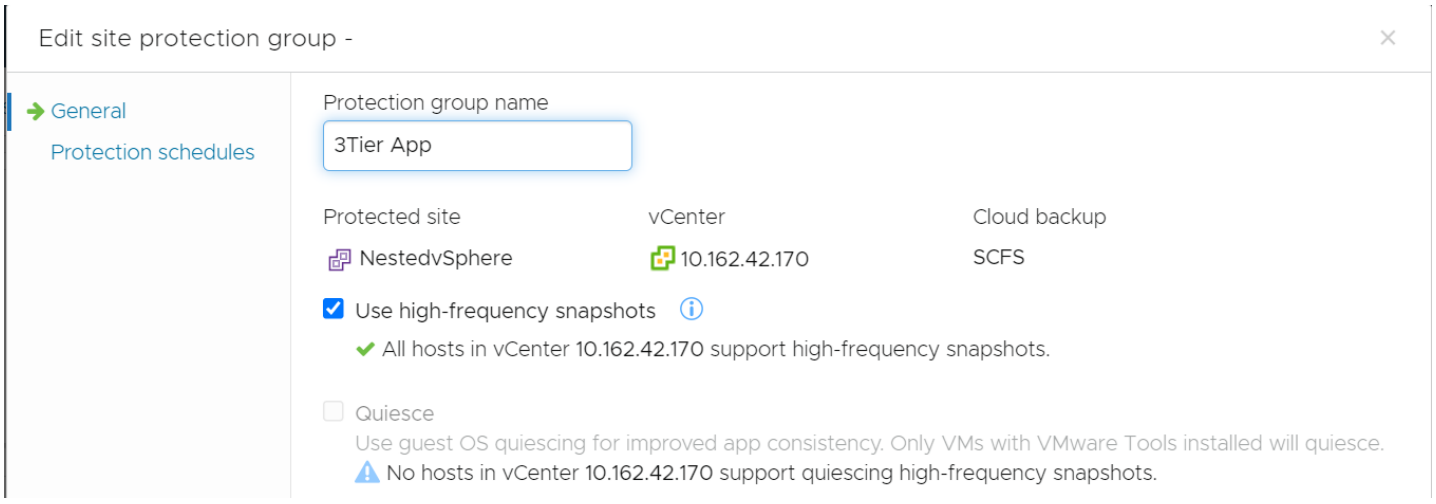

Image 2 – Source site requirements not met for HFS with quiescing

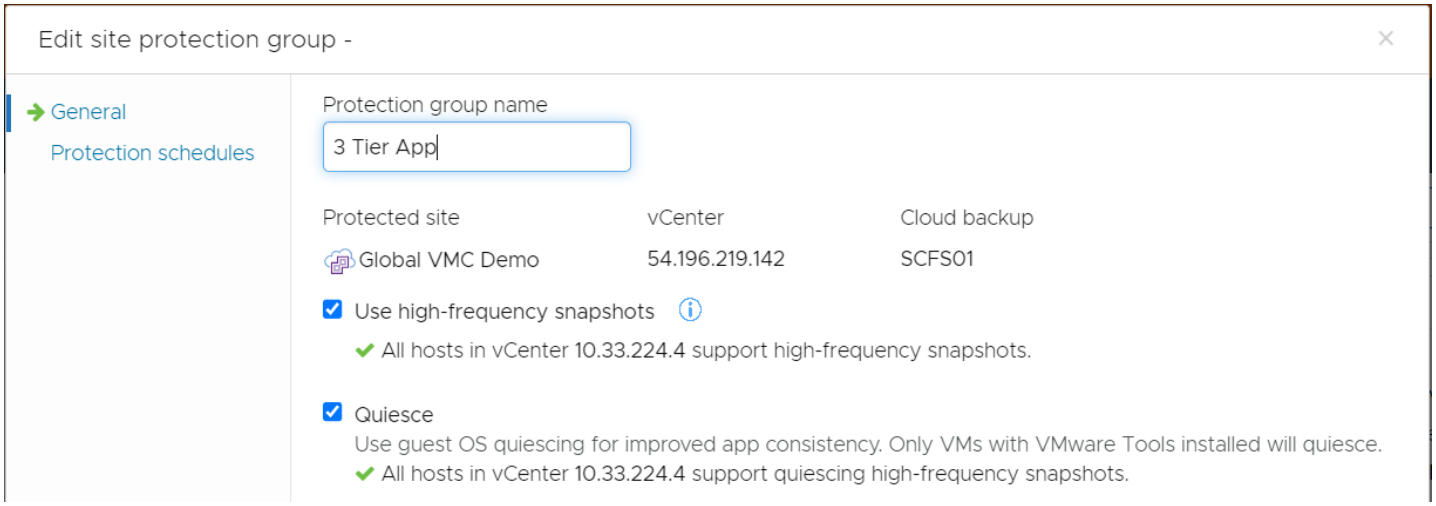

Image 3 – Source site supports HFS and quiescing

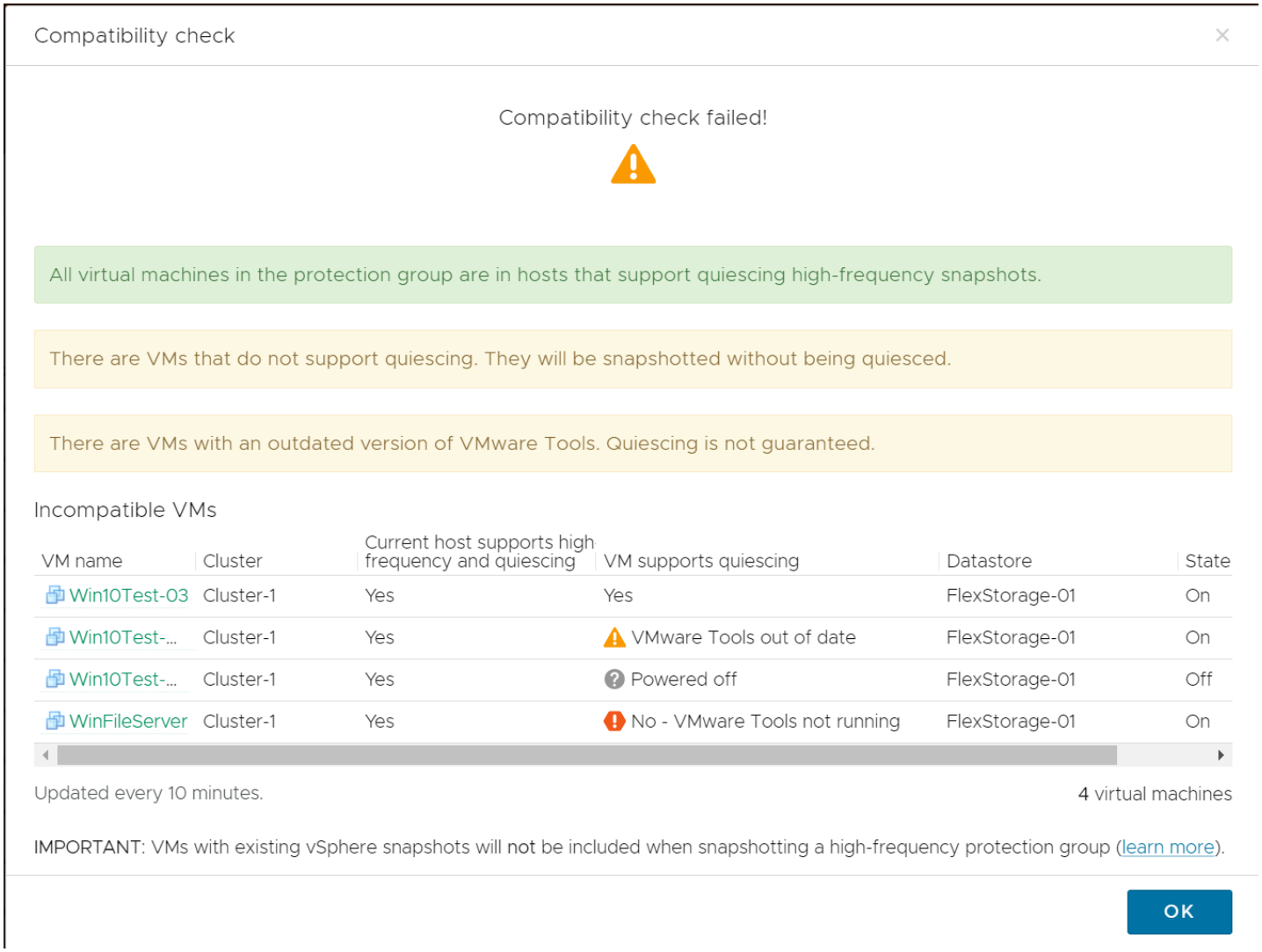

Image 4 – HFS and quiescing compatibility check example

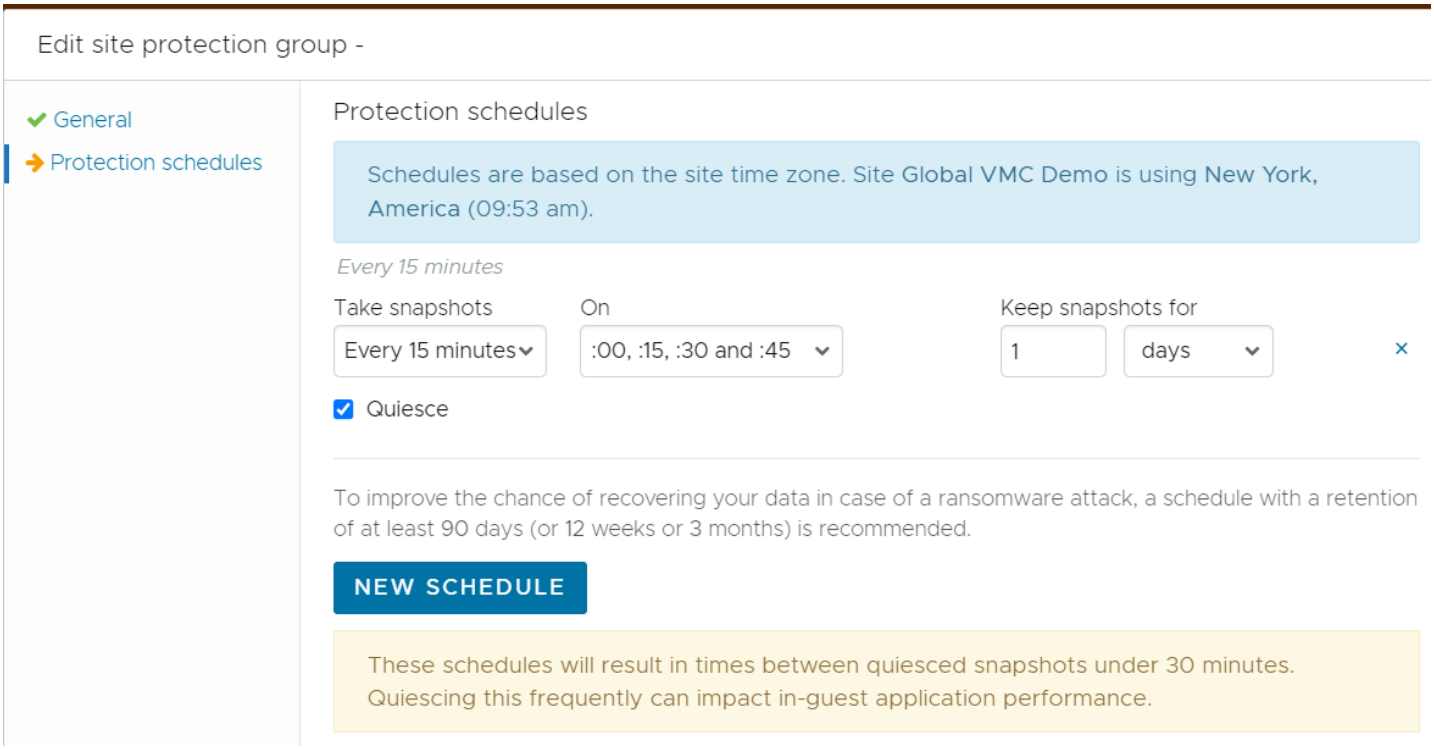

Image 5 – HFS and quiescing minimum recommended RPO is 30mins

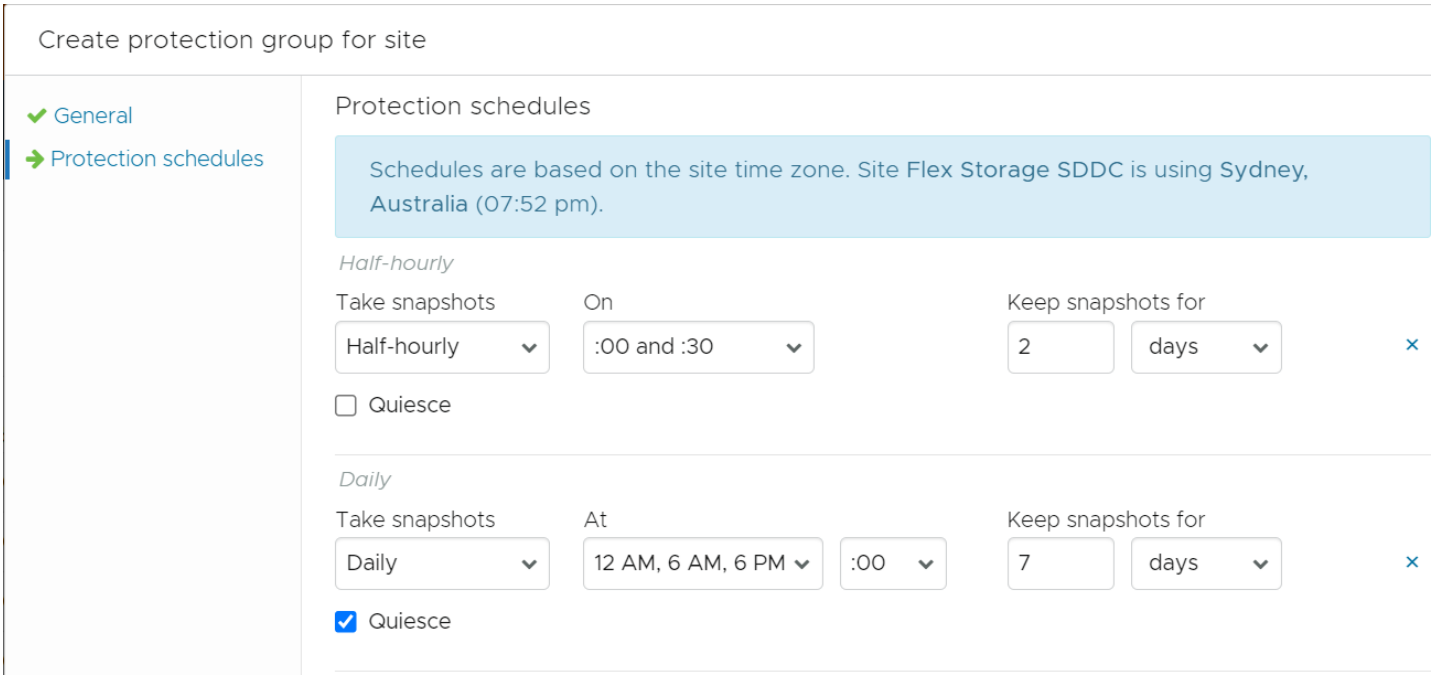

Image 6 – HFS and selective quiescing

Setting Quiesce behaviour within Windows Virtual Machines

VMware Tools version 10.2 or higher must be installed on the VMs to use quiescing.
If the VM is powered off then it will have no in-memory file data and the pre & post backup actions will not be carried out, if it was a graceful shutdown of the VM then it is likely in a clean state for restoration similar to a quiesced running snap.

There are two routes for controlling behaviour around snapshots with Windows VMs:

Windows VMs - Scripts

Scripts should be saved in Program Files\VMware\VMware Tools\backupScripts.d (legacy location c:\windows) specifically named 'pre-freeze-script.bat' and 'post-thaw-script.bat'.

Example windows files

pre-freeze-script.bat

```
set /p count=<quiesce.count
set /a count=count+1
echo ¦ set  /p="Starting pre-freeze scripts, run count ref is %count%, ">>quiesce.log
>quiesce.count echo %count%
set d=%date%
set t=%time%
REM Commands to perform specific app preparation for snapshot
echo %t% : %d% : Quiesce prep exit code: %errorlevel% >>quiesce.log
```

post-thaw-script.bat

```
REM Commands to perform specific app thawing after snapshot
echo "Post-thaw scripts complete with exit code %errorlevel% at %time% " >>quiesce.log
```

Windows VMs - Volume Shadow Copy Service (VSS)

The VSS service is installed and starts on demand by default in most modern Windows Server distributions. As a minimum this flushes all I/O buffers and then creates a shadow copy of the VM disks which improves the file system consistency by ensuring all files including open files are included. VSS aware applications can further co-ordinate their actions via VSS writers (EG Exchange, SQL Server, Active Directory, Sharepoint) – this can be particularly useful for log management You can use 'vssadmin list writers' to see the available writers and their state.

Setting Quiesce behaviour within Linux Virtual Machines

VMware Tools version 10.2 or higher must be installed on the VMs to use quiescing.
If the VM is powered off then it will have no in-memory file data and the pre & post backup actions will not be carried out, if it was a graceful shutdown of the VM then it is likely in a clean state for restoration similar to a quiesced running snap.

For Linux VMs quiescing behaviour is solely managed through scripts to run pre-freeze and post-thaw commands.

The scripts have to be located in /etc/vmware-tools/backupScripts.d directory on Linux VMs. The directory can contain one or multiple scripts executed in alphabetical order sequence for freeze and reverse alphabetical order for thaw. Each script must be able to handle freeze, freezeFail and thaw arguments passed by VMware Tools during the different phases. Legacy location for scripts is /usr/sbin with single script files named pre-freeze-script and post-thaw-script. Irrespective of location the scripts should be owned by root with execute bit set.

Example Linux scripts:

Legacy style pre-freeze-script in /usr/sbin

```
#!/bin/sh
if [ "$(id -u)" -eq "0" ]; then
#commands to flush data & pause writes to the database / pause operations
fi
```

Legacy style post-thaw-script in /usr/sbin

```
#!/bin/sh
if [ "$(id -u)" -eq "0" ]; then
#commands to resume writes to the database / unpause operations
fi
```

Example script in /etc/vmware-tools/backupScripts.d

```
#!/bin/bash
if [[ $1 == "freeze" ]]
then
  echo "This section is executed before the Snapshot is created"
  #commands to flush data & pause writes to the database / pause operations
elif [[ $1 == "freezeFail" ]]
then
  echo "This section is executed when a problem occurs during snapshot creation and cleanup is needed since thaw is not executed"
elif [[ $1 == "thaw" ]]
then
  echo "This section is executed when the Snapshot is removed"
  #commands to resume writes to the database / unpause operations
else
  echo "Usage: `/bin/basename $0` [ freeze | freezeFail | thaw ]"
  exit 1
fi
```

Caveats, Testing and Validation

When implementing any backup solution it is critical to thoroughly test not just the backups are successful but that restores are successful too! Similarly when using quiescing you should verify not just the script logic and operation but that the desired state changes occur and the resulting restores enjoy the expected benefits.

The operations triggered when using the quiescing feature will add some level of additional load and depending on what the scripts and/or VSS writers do may cause slowdown or disruption to the application that users may notice – if this is the case then you may want to use a mixed schedule of crash and application consistent backups and only run the latter outside of peak or working hours such as the schedule in Image 6 above.

Revisiting testing is important when significant upgrades or changes occur, particularly of the application/database but also when data and usage increases to ensure continued correct & timely functioning.

Lastly the consistency that quiescing brings is only within the VM – it does not guarantee any consistency across VMs, even when VMs are scheduled to be protected at the same time there is no expectation that they will be snapshotted at exactly the same time as there may be queuing of backup jobs either by VCDR or by vCenter.

This is a guide provided as is, not support documentation.

Further Reading

Taking Snapshots of a Virtual Machine

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-64B866EF-7636-401C-A8FF-2B4584D9CA72.html

Enabling Quiescing for Linux VMs:

https://docs.vmware.com/en/VMware-Cloud-Disaster-Recovery/services/vmware-cloud-disaster-recovery/GUID-DBF1DFD5-F956-4ED9-AF06-95664D3AA89D.html

Volume Shadow Copy Service Overview:

https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service