QBR *Knowledge base*

QBR Disaster Recovery Guide

What To Do During a Disaster Recovery

Establish the Scenario

It is most important to first establish and note the parameters of the disaster scenario

How does the outage impact client business continuity?

- Do recovery operations need to proceed carefully to avoid disrupting ongoing client business?
- Does the outage impact client business continuity such that the recovery takes priority over ongoing business?

What happened to the original protected system?

- Physical hardware failures are important to note, especially if failure involved the disks, RAID, SAN Corruption, etc.
- OS corruption such as Windows errors, registry corruption, infection by viruses or malware
- Application corruption, such as a problematic software update
- What precipitated the failure - are there ongoing issues that led to the current failure?

What date would you like to restore from?

- Depending on the nature of the failure, the most recent available recovery point might not be the best option
- If full restore is only available from an earlier date, can we still retrieve data from more recent points, or from other sources?

What kind of recovery do we need to perform?

- If only data recovery is necessary, a file-level restore is the most direct approach, or an application restore (such as email).
- If system recovery is necessary, local virtualization may be the client's quickest route to business continuity.
- If the local site is compromised, reach out to QBR Tech Support as soon as possible to establish networking provisions for an offsite virtualization.
- If operational hardware is available, Bare Metal Restore is an option. However, remember that data transfer takes time - establish that file restore and/or local virtualization are viable first.

- If virtual hosting resources are available, Virtual Machine Restore is an option. However, remember that data transfer takes time - establish what can be restored directly from the QBR environment before investing time to migrate it.
- If restoring the full backup with all volumes is problematic in any way, consider restoring the OS Volume separately from storage volumes. This can save time in troubleshooting, and may serve as a work around for storage compatibility issues.

ADDITIONAL INFORMATION TO CONSIDER:

- Have screenshot verifications come through successfully for this protected system?
- When mounting a file restore, are files on all volumes accessible?
- What kind of server are we restoring? Web or IIS, Application, File, Print, Exchange, SQL, Domain Controller? This is important to prioritizing restoration of the system and the data.
- Has network infrastructure been compromised? Domain Controlller, Active Directory, DNS server, or DHCP server? A compromised network may present issues beyond the scope of data recovery and must be addressed separately or identified as obstacles.

CAN WORK BE DONE TO RESTORE THE ORIGINAL MACHINE?

- If possible, work to restore the original machine to a functional state.
- Don't rely on a single path to restoration if several are available.
- Depending on the error, get necessary hardware/software vendors involved to troubleshoot.

ESTABLISH RECOVERY GOALS

WHAT DO THEY NEED BACK - THE SYSTEM, THE DATA, OR BOTH?

- If both, would it be useful to restore the data first if necessary?
- Considering the parameters gathered above: what must be done first?
- Create a plan of action and make it known and available to all parties working on the issue.

ONSITE TECH RECOVERY KIT (THINGS TO BRING TO A DISASTER RECOVERY):

- Original OS Installation or Recovery disks if available
- Any proprietary RAID drivers in .INF format, including a 32-bit version as many Recovery Environments do not include 64-bit support (Contact hardware manufacturer to get exactly the right drivers for your hardware platform, many times the drivers downloads page will provide drivers in .exe format, which does not work when attempting to slipstream drivers in during the restore process.)
- Network drivers relevant to the manufacturer of the network card. These may need to be reinstalled after the restore.
- ShadowProtect Boot ISO

- USB Flash drive (4 GB Minimum, if drivers or other data needs to be pre-loaded during the restore)
- Partition sizes of original machine (for the purposes of sizing the partitions correctly)
- Network configurations/map/dependencies to test access after the restore is complete.

LOCAL VIRTUALIZATION

- Which recovery point are we using? Most recent point / recovery point from a previous date that may have escaped corruption.
- Select the appropriate amount of resources for the virtual machine.
- 32 bit machines max out at 4 GB RAM.
- Use of more than 2 CPU's is not recommended, start with 2 and then if necessary increase performance (virtual machine will need to be turned off to reconfigure the network resources as necessary).
- More resources doesn't necessarily mean better performance
- Check the networking settings
- In Local Virtualization, select Bridge to the primary NIC. Longer deployments may need to be Bridged to Secondary NIC - this can be modified later if no second NIC is immediately available.
- Boot the virtual machine
- Log in to virtual machine using Local Virtualization Connect via RDP
- Allow drivers to be installed upon boot up. Some drivers that fail to install may be benign, so note the drivers but proceed with the installation.
- Reboot the virtual machine.
- Assign networking for the virtual machine - be sure to take any compromised network infrastructure into account.
- Test network connectivity. Connect to the assigned IP using RDP, ping the gateway, try Google, etc.
- Make sure clients can access resources and operate applications on the virtual machine, especially database applications.
- If the virtual machine fails to virtualize right away, investigate error and call QBR technical support for assistance.
- If troubleshooting steps to recover from the virtual machine are unsuccessful, consider trying another recovery point
- If troubleshooting steps to recover from the virtual machine compromise virtual machine data in some way, consider simply unmounting the virtual machine and remounting from the same point

OFF-SITE RECOVERY

Call QBR right away at (450) 681-3009 or submit an urgent ticket if the local device cannot be used for restore and we need to virtualize in the cloud, please be sure to specify whether the situation is a disaster scenario.
Have the information requested in our Offsite Virtualization Test Form ready to ensure fastest possible recovery.

QBR *Knowledge base*

BARE METAL RESTORE: NETWORK BMR

- Determine the hardware we are performing the BMR to. Note specifics in case of the need to call support.
- Ensure that the target hardware is healthy (BMR to bad disks will guarantee failure)
- Always use Firefox or Chrome (Internet Explorer does not properly capture BMR interface)
- Don't use the auto partition editor, always partition manually.

After BMR is performed, verify the restored system is viable.

- Get client verification that system is functional
- If BMR boots into a failed boot environment, use the ShadowProtect recovery environment to investigate the bootability of the volumes.
- Prepare and Launch a Virtual Machine with the ShadowProtect ISO
- Check boot configuration utility; make sure appropriate volumes are marked as active and primary.

BARE METAL RESTORE: USB BMR

If restoring to 64-bit hardware, the USB BMR is a viable option as well.

BARE METAL RESTORE (SHADOWPROTECT METHOD)

First, take the ShadowProtect backup to a NAS share on the QBR device:

- Fastest method is to restore the OS volume and confirm bootability before attempting the restore of data volumes.
- Check partition tables for the size of the restore to ensure that you have the space necessary.
- Create the partition with ShadowProtect or any other disk utility, format NTFS and validate the disk is ready for transfer.

VIRTUAL MACHINE RESTORE

Determine the host of the machine (Hyper-V, VSphere, VirtualBox, etc)

- The share created by an image export should automatically be a public share.
- Consider beginning with the OS volume to confirm bootability:
    - Copy the OS Volume over to hypervisor datastore
    - Start transfer of other data volumes
    - Then work to confirm the bootability of the OS volume