

Business Continuity Disaster Recovery

vDR FAQ

www.voffice.net.nz

What is the vDR product?

vDR (vOffice Disaster Recovery) comprises an onsite vDR appliance which participates on the Company network. The appliance takes snapshots of selected servers and stores them on the local appliance and also replicates these snapshots to cloud storage in a geographically different location to the appliance.

What exactly does the onsite vDR Appliance do?

The vDR appliance is responsible for several tasks:

- **Snapshot Backups:** The appliance takes continuous snapshots of agreed selected servers at an agreed frequency.
- **Exports:** Once an evening the appliance exports the backup snapshots to virtual servers on the vDR appliance.
- **Off Site Replication:** The backup snapshots are replicated to cloud storage in a geographically different location. Once an evening the backup snapshots are exported to virtual servers
- **Near Instant File Recovery:** Using a locally installed tool you can access stored backups to recover single or multiple files and emails.
- **Business Continuity:** Should a single production server (that is being backed up) fail on the company network, the server export can be mounted as a fully functional virtual server to take place of the failed server while a replacement server is sourced for the failed production server.

If I need to use Business Continuity what happens to my snapshot/backups?

All Snapshot Backups and Off Site Replication continue as normal.

Is there an impact running Business Continuity on the vDR appliance?

- **Performance:** As the vDR Appliance is still performing Snapshot Backups, Exports and Offsite Replication while running a Production Virtual Machine, it is likely the Production Virtual Server will perform slower than the actual Production Server it is replacing.
- **Microsoft Licensing:** Microsoft will only allow you to run the Production Virtual Machine on the vDR Appliance using License Mobility (provided by Microsoft Volume Licensing with Software Assurance). Charges may apply if Microsoft licensing is not to this level.

How much Internet traffic will the vOffice vDR Replication service use?

Your internet usage will increase with the vDR service. By how much is dependent upon the nature of your current server environment.

The primary parameters that affect your replication traffic are:

- Rate of data change per server (NB: transactional servers have a higher rate of change than file based servers)
- Frequency of snapshots
- Type of data (compressible or not)

Estimating Internet Traffic usage is not an exact science and is dependent on a number of factors. vOffice vDR uses backup technology that is highly efficient in maximizing your WAN usage when compared with other similar technologies and includes features such as global de-duplication and compression, which can reduce your backup WAN traffic by 60% or more.

How much Internet Bandwidth does vDR come with?

vDR300 and vDR600 come with a 5Mb Internet Bandwidth while the vDR1200 comes with 10Mb Internet Bandwidth. Increased performance can be obtained by purchasing dedicated pipe(s) at additional cost. These would need to be discussed and quoted on a case by case basis.

Will I need to purchase extra software or hardware?

No. Once you have settled on your individual configuration requirements you will be billed a monthly amount which includes the backup appliance and all the software required. Additional charges may be incurred for Business Continuity (see 'Is there an impact running Business Continuity on the vDR appliance?') or Disaster Recovery (see 'What, if any, charges come into effect when DR is invoked?').

Where is my data held and is it secure?

Primarily your data is stored on-premise inside the vDR Appliance (which is protected by your encryption key) and is replicated to the 'cloud' (our New Zealand datacentre).

Data is secured via encryption between your premises and our datacentre.

vOffice uses a secured Enterprise level Tier-3 datacentre to ensure your data is secure. Your data will reside in New Zealand and will never be sent off shore.

To protect backups from unauthorized access, use and to ensure data privacy, our backup agent provides 256-Bit Advanced Encryption Standard (AES) encryption, compliant with SHA-3.

Who has access to my data?

vDR is a fully managed service. Only you and vOffice authorised personnel have access to your data.

Do I need to install anything on my servers?

Yes, the vDR backup agent will be required to be installed on each protected server. The agent is a very small footprint software agent that will have little or no impact on the Server performance.

Can I recover files from the backup?

Yes, using a locally installed console tool you can access the stored backups on the local appliance and recover files. Alternatively vOffice can assist.

Do I need to keep using my current backup system?

No, vDR can replace your current backup solution. In fact vDR works best when it's the only backup solution on a server. vDR utilises Microsoft's VSS snapshotting technologies and has been known not work with other backup vendors using their own, or Microsoft's VSS technology. Multiple backup solutions may be supported but care is needed to avoid the systems conflicting.

You may need to retain your old backup tapes and equipment for archive compliancy purposes.

How do I know that it is working?

vDR uses a technology called 'Recovery Assure' which performs automated recovery testing and verification of backups.

Recovery Assure includes, but is not limited to, Microsoft Exchange 2007/2010, different versions of Microsoft SQL 2005, 2008, 2008 R2 and 2012 provides 100% recoverability of applications and backups in both virtual and physical environments. vDR features a comprehensive integrity checking algorithm based on 256-bit SHA keys that check the correctness of each disk block in the backup during archiving, replication, and data seeding operations. This ensures that data corruption is identified early and prevents corrupted data blocks from being maintained or transferred during the backup process.

In addition to this we implement a nightly process that tests the exports of your system to ensure that you have a working backup and a recoverable server.

Systems are proactively monitored from our central console and any issues are rapidly revealed.

What about Restore of an Exchange email / mailbox / mail database?

Yes, unlike other 'cloud' based systems, vDR uses Universal Recovery which allows you restore individual mail items or complete mailboxes.

Can I test my DR plan?

Yes. We would recommend that you test your DR plan at least once a year.

What happens if I have a 'protected' server fail on my network?

The vDR appliance is designed to cater for an unexpected server failure. The exported image of the server on your local vDR appliance can be rapidly mounted as a virtual server and continue to perform its functions on the production network, although this may be at a reduced performance.

Will testing the DR cost me more?

No, your vDR service contains a time allocation for spinning up your servers in the

'Cloud' at our datacentre providing the tests involve five users or less. This is currently 3 hours/quarter/server. Should you require additional testing spin-ups of your environment can be booked at \$150 per server per hour.

What is meant by RPO. and RTO.?

The Recovery Time Objective (RTO) is how quickly you need to have that application's information back and available after downtime has occurred.

The Recovery Point Objective (RPO) is the point in time to which data must be restored to successfully resume processing (often thought of as time between last backup and when an 'event' occurred).



Every comprehensive Business Continuity or Disaster Recovery Plan should have RPO and RTO objectives set for each application.

Is this all I need for my DR plan?

No, the vDR appliance and its two levels of backup protection only forms part of a DR plan. A DR plan has to be a robust construct and cover all aspects of your business including phones, staff, local devices, communications, web systems etc. A VPN connection and an IP range are generally required as a base minimum, however, there are many other design issues to cover. vOffice can assist with the planning your DR requirements at an additional consulting charge.

Will I lose emails if my email server fails?

Generally you will lose some emails between the time of the last backup (replicated in DR) and the time your email server fails (RPO). If you have an extended outage (RTO) then new emails sent after the failure may get bounced back to the sender.

How long is my backup retained?

This is dependent on the frequency of your backups and the amount of storage they consume.

There are a number of archiving options available which can extend this period for longer term retention and/or compliancy at additional cost. The options can be explored once the storage requirements have been assessed from historical data.

How often are my servers backed up (RPO)?

This can vary and is set after the initial consultation and the completion of the Server Survey conducted as part of the setup period of the onsite vDR appliance.

Servers can be backed up every 15 minutes, or more frequently, if required, although this may impact overall performance of the onsite vDR appliance. However, many server C: drives (for example) are relatively static and only need backing up once a day.

This may require review once the change rate of your server(s) and storage requirements has been established.

Do my staff need to be involved with the new vDR backup?

The service is highly automated and was designed to be completely hands off for customers.

What, if any, charges come into effect when DR is invoked?

Microsoft License Mobility does not apply to mounting the company's server(s) in DR. Instead Microsoft SPLA licensing applies. Under Microsoft SPLA each user able to access the system whilst in DR is charged for. We would propose that you recover these charges from the Company's insurance company.

What are the factors that impact DR performance?

- **Internet Bandwidth:** A contended internet connection is provided as standard. Increased performance can be obtained by purchasing dedicated pipe(s) at additional cost. These would need to be quoted on a case by case basis.
- **Number of users accessing DR:** The number of users accessing the Company under DR will have an impact on the usability of the system. Traditionally the number of users is reduced to those deemed essential to running the business while DR is invoked.
- **Server Resource Allocation:** The Standard Server in DR is scoped to be a dedicated CPU core plus 4GB RAM. Additional Resource units (CPU core plus 4GB RAM) can be purchased to increase the performance of Servers on a Server by Server basis. Normally this is a contended service, however, Cloud Server reservations can be purchased
- **Virtual Machine Storage:** As standard, Replicated Servers are provided on Tier-2 SAN storage. Tier-1 SAN storage is available at an additional cost for faster performance.

Is there a limit to the number of servers or the amount of data I want to back-up?

No, the amount of 'cloud' storage allocated can be increased in 50GB 'chunks'. If your onsite appliance proves to be too small for your expanding needs then you can upgrade to a higher level or multiple vDR appliance(s).

What if I use the vDR300 now but need to upgrade to the vDR600 or vDR1200 solutions later?

If the onsite vDR appliance is too small for your growing needs, you can upgrade to a larger vDR appliance that will meet your new requirements.

How do I know which vDR appliance I require?

We base the initial deployment on the used disk space and number of protected servers. This should offer reasonable retention of your protected data.

What is a Cloud Priority Reservation?

Cloud DR services in the Data Centre are provided on a contention ratio basis, unless a 'Priority Reservation' is taken up. The standard Cloud Priority Reservation consists of a Server Resource Unit (dedicated CPU core plus 4GB RAM) connected to Tier-2 SAN storage.

Additional Server Resource units can be purchased and added to the Cloud Priority Reservation to increase the performance of Servers on a Server by Server basis. These reservations can also include High Speed SAN connectivity at additional cost.

What happens to my backups if the Internet fails?

Your local backups are not affected by the Internet and continue to function as normal, however replication to our hosted service will be queued and will resume once the Internet link is available.

When I am in DR are my DR Servers being backed up?

Replication to another DataCentre can be arranged at additional cost.

What happens if I require more resources that the vDR1200 can supply?

In some exceptional cases the resources required to run a large Server and Application in Business Continuity mode may exceed the resources of the vDR1200. In such cases a custom built vDR can be quoted to meet requirements.

Are there Maintenance windows that might affect my services?

- Service availability of the vDR appliance, subject to any local power outages or hardware issues, is 7x24x365.
- Service availability of the Data Centre is 7x24x365 subject to any required maintenance outages. Bulletins will be issued prior to scheduling any maintenance windows, however, if the window is inconvenient for any reason the maintenance window will be shifted.