Axcient

Virtualization Best Practices for x360Recover

The Ps of Successful Virtualization

- ***Plan*** your disaster recovery process ***prior*** to a real-life disaster recovery situation.
- ***Practice*** test cloud failover events to give your staff the experience they need.
- ***Prepare*** a documented disaster recovery plan. Detail how you intend to handle various types of potential disasters.
- ***Provide*** efficient access to client services in the cloud

What should you include in each plan?

A single generic document is often sufficient to guide your technical staff in meeting various case requirements. However, detailed and customized plans may be necessary for large clients to understand every server, service, and system involved and to explain all requirements needed to recover efficiently.

Be sure your plan addresses the different situations each client may potentially experience. Use cases typically boil down to a few recurring considerations, regardless of whether the underlying cause of the disaster involves hardware failure, software corruption, or ransomware:

- A single server fails at one site
- Multiple servers fail at one or more sites
- A total loss of site facilities occurs at one or more locations (fire, flood, power outage, etc.)

To virtualize effectively with x360Recover

Plan your network topology to include Virtual Office

Treat the Axcient Virtual Office as a separate remote site in your overall network topology. This is helpful when planning your process, whether you need to recover a single server or an entire site.

For example, Customer 1 has a main office and a secondary remote office location with site-to-site VPN connections linking them together.

- When planning for potential recovery to the cloud, treat the Virtual Office as a new site on your network plan, with its own unique LAN IP subnet.
- When virtualizing a failed server in the cloud, simply change its IP address to the new subnet in Virtual Office.
- For Windows environments, define this environment in Active Directory Sites and Services. Also, if you virtualize a Windows domain controller, remember to update its location in Sites and Services. This will optimize Windows synchronization of Active Directory between sites.

Use Runbooks Effectively

Runbooks allow you to thoroughly pre-plan your disaster recovery scenarios. With a runbook, you can select and configure protected systems, organize network settings, set up port forwarding, arrange public IP addresses, and configure client and/or site-to-site VPN settings, among other tasks. Also, a runbook allows you to start up a Virtual Office and boot the most recent recovery point for each protected system with just a few clicks of the mouse.

Runbook does have its limitations. While runbooks are undeniably convenient, there are a few things that runbooks can’t fully automate. Also, IPv4 Addresses are a limited commodity in the modern world. Unfortunately, Axcient doesn’t possess a limitless amount of IP space, so we cannot assign dedicated IP addresses to each partner. This means that each time you start Virtual Office (whether manually or via a runbook), you will be assigned random IP address(es) from the available pool.

- When starting a test or live disaster recovery operation, you must update your VPN connections with the new peer IP address and the randomly generated pre-shared encryption key.
- If you are performing a failover for servers hosting publicly accessible services (such as mail or web servers), you must update your DNS ‘A’ records for such services to point to your Virtual Office IP address(es).

Provide Efficient Access to Client Services in the Cloud

One of the most important aspects to consider when planning and performing a disaster recovery is how your clients will access their services when running in the cloud.

Here are three options, along with a discussion of why/when to choose each:

1 Site-to-site VPN – When the Environment is Intact

Site-to-site VPN is often the best option when the physical location and the user environments are still intact, and you simply need to fail over one or more servers.

In this scenario, you relocate one or more servers to a different site. If your internet bandwidth is sufficient, users may not even notice that servers are physically running somewhere else.

Steps for Site-to-site VPN:

- Launch a runbook
- Update your VPN connections with the new Peer IP address and password
- Change the IP address of the virtual machine Server to match the new LAN subnet.
- You may also need to update and sync Windows DNS, and Active Directory changes across all domain controllers.

2 Client VPN - When Users Connect from Another Location

When an entire site outage occurs, no services such as internet connectivity or power are usually unavailable. Your users must relocate to another location with access to such services. Typically, this relocation involves going to a home office or other area where power and internet can be found. Roaming users will need to connect without the benefit of IT-managed infrastructure (such as routers and site-to-site VPN tunnels.)

One method of providing this access is client VPN. It is important to note that while a client VPN connection provides flexibility, this method can be somewhat slower, depending on the applications used.

Axcient Virtual Office provides client VPN via web browser and VPN client software.
When (Client) VPN services are enabled in Virtual Office, a web-based URL will be created for the users to follow to get connected. For details, please see Configure VPN for Virtual Office.

Steps for connecting to client VPN:

1. Roaming users connect via web browser to Virtual Office
2. Then, they log in with user credentials and connect over client VPN software installed directly onto their computers.

Note: if the user has never connected before, they must download and install the client software from the Virtual Office login page.

User accounts for Client VPN logins may be pre-created within a runbook, or you may configure Active Directory LDAP authentication to leverage your existing Active Directory user accounts. (Configuration of LDAP integration is beyond the scope of this document.)

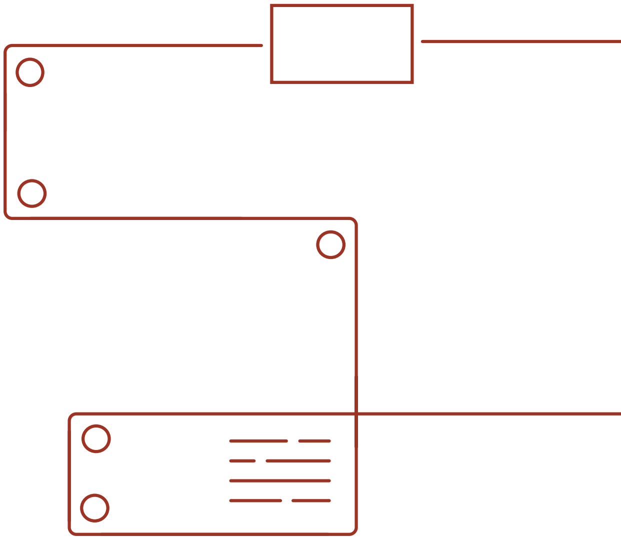
3 Remote Desktop Services (RDS)

Many clients prefer the flexibility of supporting remote and roaming workers in their everyday working environment. One of the best ways to provide seamless remote accessibility to users is via Windows Remote Desktop Services (sometimes referred to as either Terminal Services or RDS.)

If your client's environment already includes servers supporting Remote Desktop Services, it is straightforward to enable these servers to run in Virtual Office:

- Allocate an IP address for the Remote Desktop Services server virtual machine
- Port forward the required ports (typically 80, 443, and 3389)
- Update the DNS 'A' records (if you have one) to point to the IP address in Virtual Office.

Once DNS changes are propagated, clients can connect to their normal remote access address as usual.



Supporting Virtualized Protected Desktops

In some situations, you may have a client with complex vertical software environments - and such applications may not run well over a VPN. Or you might have some specialized users with vastly different application requirements than typical users. Another possibility is that you could have cases where it is imperative that user desktops be individually backed up and ready for recovery.

Typically, in these scenarios, your clients would use an alternate computer, perhaps a home or personal system, to connect to a virtual machine copy of their regular work computer. In these cases, it may be best to use a client VPN to connect the alternate computer system to Virtual Office and then use Remote Desktop Services over the VPN to connect each user to their own workstation machine.

Note: While it is possible to use port forwarding to allow direct Remote Desktop connections to multiple running workstation virtual machines, this is a poor practice. This exposes each machine to direct access over the internet. Connecting over a client VPN first adds an extra layer of security to your environment.

Example: Let’s assume that your client has a Remote Desktop Services server, as described above, which is used by most users working remotely. But your client also has a few users with sensitive data or vertical applications on their work computers that other users should not have access to. How could you best support this? Users with special needs would access an existing tablet, home PC, or personal laptop to connect to Virtual Office.

They could then either:

- Directly connect to the Remote Desktop Services server for typical user access or
- Connect via client VPN and then access the virtual image of their work computer using Remote Desktop Protocol. (RDP) RDP provides a rich, responsive remote desktop experience, up to and including support for sound if needed.

The Ps of Virtualization Best Practices

Being ready is the key to good virtualization; remember - proper prior planning prevents poor performance.

Want to learn more about virtualization? Visit the Axcient Knowledgebase.

Unified Data Security with Unmatched Flexibility

If you're not an Axcient partner, use the options below to see how your MSP can can get best-in-class virtualization with any deployment method.

Schedule Your 1:1 Demo

Try Axcient Free for 14 Days

Get a BCDR Quote

Additonal Free Resources for MSPs:

- Recovery Playbook for Axcient x360Recover
- QBR Handbook for MSPs
- MSP Blueprint for Profitably Selling Bundled Services
- DR Planning and Testing Best Practices for MSPs
- 5 Critical Pieces of a Good Security Playbook

About Axcient

Axcient is an award-winning leader in business continuity and disaster recovery for Managed Service Providers (MSPs). Axcient x360 provides one platform for MSPs to Protect Everything™, and includes BCDR, Microsoft 365 and Google Workspace backup, and secure sync and share. Trusted by more than 4,800 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

Axcient

Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202
Tel: 720-204-4500 | axcient.com