Axcient Fusion FAQs

Environment Support

Which operating systems are supported?

Axcient Fusion can protect systems running a range of operating systems, including Microsoft Windows and various Linux distributions. Refer to the Axcient Fusion Compatibility Matrix for details about current operating systems support.

Which VMware versions are supported?

Refer to the Axcient Fusion Compatibility Matrix for details about current VMware version support, including minimum versions and necessary configuration options.

What VMware disk formats and protocols are supported?

Supported VMware disk formats include VMDK, NFS, and VMFS. Refer to the Axcient Fusion Compatibility Matrix for the latest details about supported formats and protocols.

Are large file stores supported?

Yes, Axcient Fusion can handle file stores that are multiple terabytes in size. Refer to the Axcient Fusion Compatibility Matrix for the latest details about supported storage configurations.

Are there any volume size limitations?

Although any size server can be protected and recovered, each individual volume should be less than 4 TB. Otherwise, recovery options are limited. Refer to the Axcient Fusion Compatibility Matrix for details about volume sizes and recovery options.

Are physical servers supported?

Not yet. In the meantime, the Axcient Business Recovery Cloud, which can be used in conjunction with Fusion, might be a good alternative solution.

Is Hyper-V supported?

Not yet. In the meantime, the Axcient Business Recovery Cloud, which can be used in conjunction with Fusion, might be a good alternative solution.

Which software-defined VMware stacks are supported?

Axcient Fusion supports VM migration. Other stacks, such vSAN, NSX, and VVol are not supported.

Are hyper-converged stacks supported?

No, currently hyper-converged stacks such as Nutanix and Simplivity are not supported.

Setup

What components comprise Axcient Fusion?

Axcient Fusion is a cloud service that delivers IT resiliency. The cloud portion of Fusion runs on elastic, cloud infrastructure. Users interact with Fusion via a web application that runs in the cloud, behind which is all the automation for protection and recovery.

Fusion also includes a component called the Axcient Virtual Manager (AVM), which is downloaded and installed by the user into the IT environment to be protected.

How much time does it take to set up Axcient Fusion?

Setting up the Fusion service in the Axcient web application takes less than five minutes.

After that, it’s just another 10 minutes to download and install the Axcient Virtual Manager (AVM) on the local host.

What is the Axcient Virtual Manager (AVM)?

The AVM is a virtual machine template (OVF file) that is part of the Axcient Fusion service. The AVM protects the virtual machines on a particular host by replicating data to the Axcient cloud.

What resources are required by the AVM?

There are no minimum requirements associated with an AVM in terms of CPU cores and RAM. However, there are best practice guidelines for the allocation of cores and RAM to an AVM, depending upon the number of virtual machines that are being protected. Refer to the Axcient Virtual Manager Tech Overview for specifics.

What is the size of the AVM?

The OVF file for the AVM is around 650 MB in size.

Protection

Does Axcient Fusion take application-aware snapshots?

Yes, the snapshots are application-aware. Axcient Fusion uses VMware Change Block Tracking (CBT) to extract snapshots of virtual machine images.

In the very rare situations where the load on the ESXi host is too high and VMware returns a quiescing error, Axcient Fusion extracts a crash-consistent snapshot.

Refer to VMWare Knowledgebase for more details about virtual machine snapshots in VMware.

What Recovery Point Objective (RPO) is provided?

Axcient Fusion can provide consistent sub-hour RPO for any type of server it protects. The replication interval is user configurable.

Note that replication times will vary depending on the uplink bandwidth to the Axcient cloud, network contention, load on the host, amount of data change, and size of the server being protected.

What data retention options are offered?

For disaster recovery and business continuity, retention options of 30 days and 90 days are offered. Longer-term options for data archival include 1, 3 and 7 years.

What is manage-by-exception?

Manage-by-exception is a philosophy based on the idea that the user be notified of important activities and alerts that are outside of normal, healthy operations. In the Axcient web application, all activities and devices that need immediate attention are displayed highest in the dashboard so that the user can quickly take action to resolve any issues.

What is WAN optimization in Axcient Fusion?

The WAN optimization technology in Axcient Fusion ensures that only the latest changed data is replicated to the Axcient cloud. Since only incremental changes are transmitted, WAN optimization increases replication speeds (thereby reducing RPOs), consumes less networking bandwidth, and minimizes storage footprint.

What kind of deduplication is supported?

Axcient Fusion provides end-to-end data deduplication. This means the AVM performs deduplication on the client side and only sends unique data to the Axcient cloud. Once data reaches the cloud, another deduplication takes place to provide storage efficiency.

Is encryption supported?

Yes, Axcient Fusion supports TLS encryption for data in transit and 256-bit AES encryption for data at rest in the cloud.

Is there a limit on the number of servers that can be protected?

No, there is no limit on the number of servers that Axcient Fusion can protect.

What compliance standards apply to Axcient Fusion?

The infrastructure on which Axcient Fusion runs meets a number of compliance standards, including:

- HIPAA
- SOC 1, SOC 2, SOC 3
- PCI DSS Level 1
- FIPS
- ISP 9001, 27001, 27017, 27018

- MLPS
- MTCS
- ITAR
- HITECH

Recovery

What use cases does Axcient Fusion support?

Axcient Fusion consolidates workloads to support the following use cases:

- Disaster recovery testing
- Disaster recovery production (actual DR event)
- Testing and development
- Data recovery (files and folders)
- Data archival (for compliance)
- Business continuity (recover servers, not entire site)

What recovery options are provided?

The following types of recovery are provided:

- Virtual machine failover
- File and folder recovery
- VMDK export
- Granular recovery of Microsoft Exchange and Microsoft SQL Server using the Axcient DirectRestore application

What Recovery Time Objective (RTO) is provided?

Axcient Fusion is capable of providing consistent sub-hour RTO for any type of server it protects.

Note that RTO will vary depending on the size of the server being recovered.

What is a virtual office?

A virtual office is a virtual private cloud, which a user can create using Axcient Fusion for:

- Disaster recovery testing
- Disaster recovery production (actual DR event)
- Testing and development
- Business continuity (recover servers, not entire site)

What is the management IP address when creating a virtual office?

The management IP address is the address of the service VM that runs in the virtual office. The service VM is a router in the virtual office, which allows network communication with the outside world.

The user configures the management IP address when creating a virtual office. The address should belong to a unique subnet and should be unique itself from any other subnets or servers present in the user's environment.

Are there any IP address limitations in the virtual office?

The first four IP addresses and the last IP address in each subnet CIDR block are reserved for use by the virtual office. They cannot be used by VMs running in the virtual office. For example, in a subnet 10.0.0.0/24, the reserved addresses are 10.0.0.0, 10.0.0.1, 10.0.0.2, 10.0.0.3, and 10.0.0.255. Refer to VPCs and Subnets for more details on this topic.

It is advisable to avoid IP address collisions between VMs running in the primary environment and the reserved IP addresses in the corresponding virtual office. Furthermore, it is recommended to run a disaster recovery test to confirm there are no VMs with IP addresses that collide with reserved IP addresses.

Are orchestration and automation provided for recovering servers?

Yes, orchestration and automation are provided for the creation of a virtual office, orchestrating networks, sequencing VM start-up, and more. Orchestration and automation are achieved through reusable templates called "runbooks".

What is a runbook?

A runbook is a template that defines the orchestration and automation rules for a virtual office. A runbook contains networking details, a list of servers participating in the runbook, cores and RAM to be allocated to each server, priority ordering for servers, and wait time for each server.

Once created, a runbook can be selected and executed to stand up a virtual office in the event of a disaster. Additionally, runbooks let users carry out disaster recovery testing or perform testing and development activities.

Does Axcient Fusion support multi-tenancy?

Yes, every user who starts a virtual office is running in a containerized environment (i.e., a virtual private cloud). This ensures complete security and privacy.

What networking options are provided for an Axcient virtual office in the cloud?

Axcient Fusion provides the ability to configure the network in the following ways:

- Network configuration – gateway IP, netmask, and management IP address
- Multiple subnets inside the virtual office
- Public IP and port forwarding for one or more servers
- VPN client for one or more servers and for one or more users

- Site-to-site VPN (bridging of two networks) for business continuity
- A single virtual office from multiple Axcient Fusion services belonging to one primary site

What connectivity options are available for servers running in an Axcient virtual office?

Servers running in an Axcient virtual office can be accessed in the following ways:

- VPN client, such as open VPN or Cisco VPN client
- Remote Desktop Connection (RDP)
- Site-to-site VPN (bridging of two networks between a user's data center and the virtual office in the Axcient cloud)
- Public IP and port forwarding

How does failback work?

Axcient provides an automated failback feature that allows a user to stop a failover VM and convert it into an OVA, which can then be downloaded.