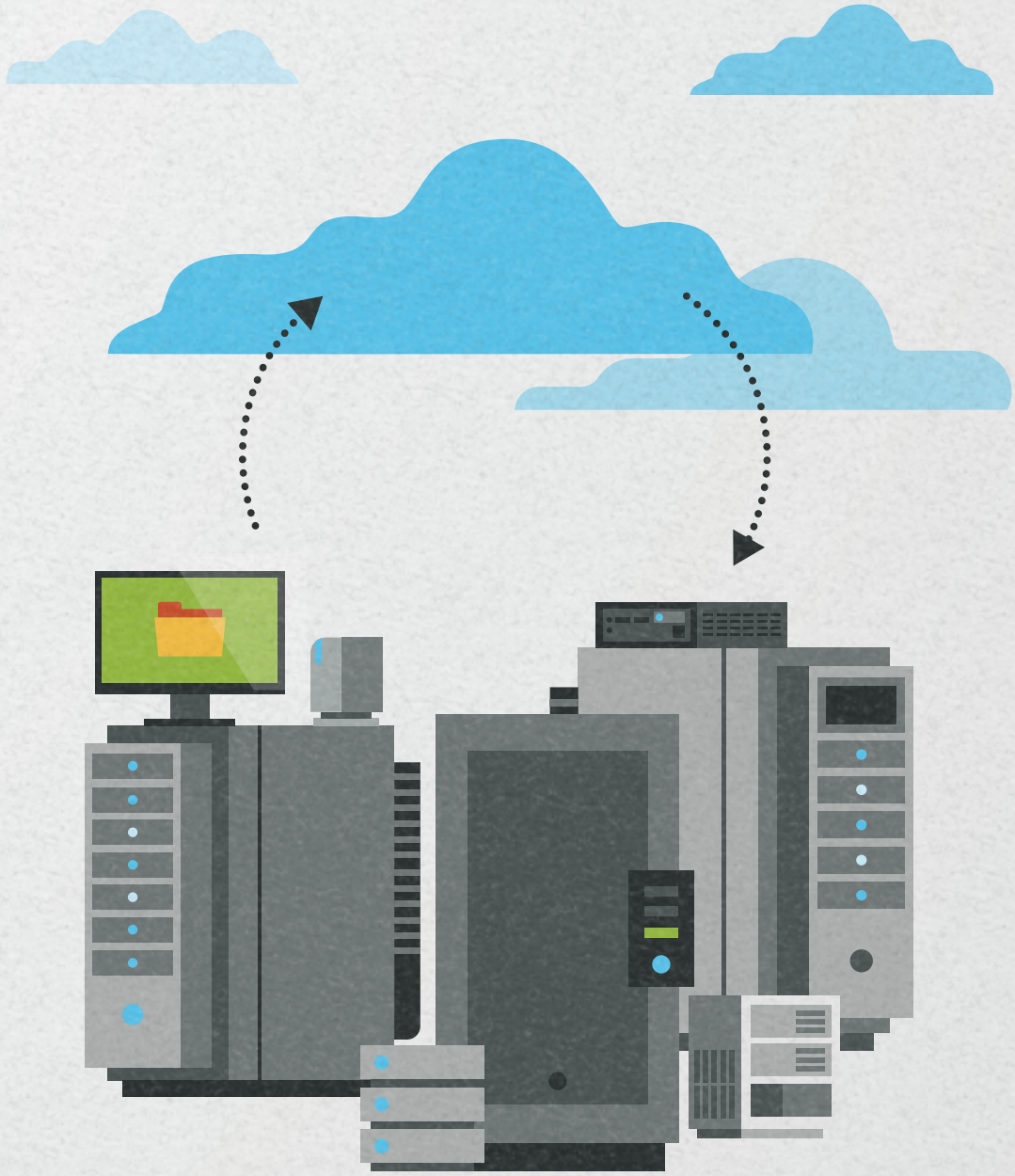
CARBONITE

Carbonite Availability onboarding overview

What to expect in the first 30 days with our high availability solution.



Carbonite Availability onboarding overview

It's easy to focus on the technology side of data protection while overlooking the importance of service and support. Carbonite Availability *Powered by DoubleTake* is more than just speeds and feeds. Our solutions are backed by a team of highly trained data protection experts who have deployed high availability in thousands of environments, each uniquely configured for the needs of that organization. In addition to phone support, there's also a comprehensive collection of helpful resources in our online support center. These resources are designed to get your high availability solution up and running without hassle.

Carbonite Availability onboarding overview

Configuring protection

The Carbonite replication console is the central management tool where administrators configure data-only or full server protection workflows between any combination of physical, virtual or cloud servers. Full server protection is most commonly configured as it offers a simple and streamlined way to protect and restore the entire state of the system, including operating system, registry entries, host name, Security ID (SID), Global ID's (GUID), applications, services and settings.

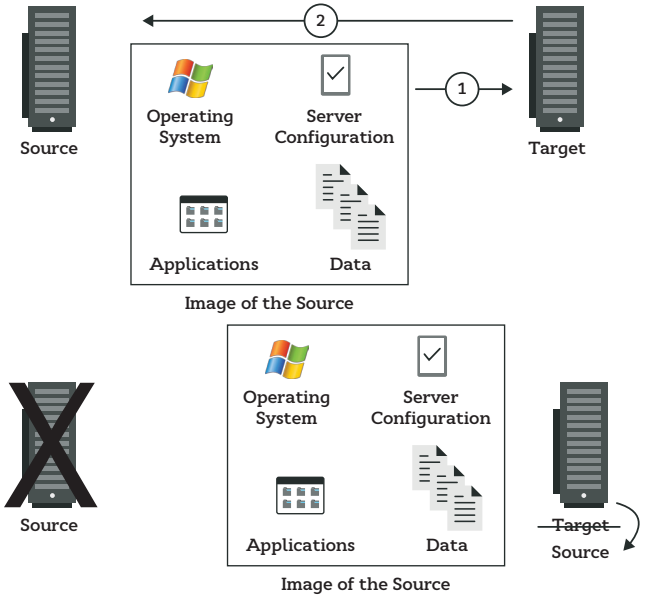
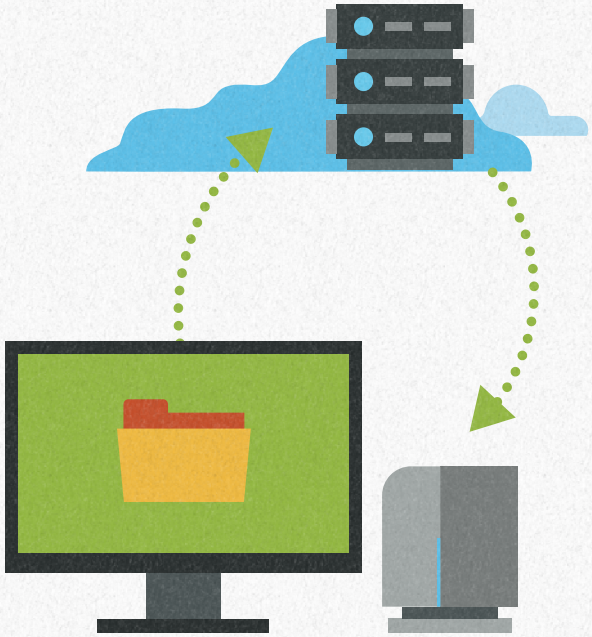
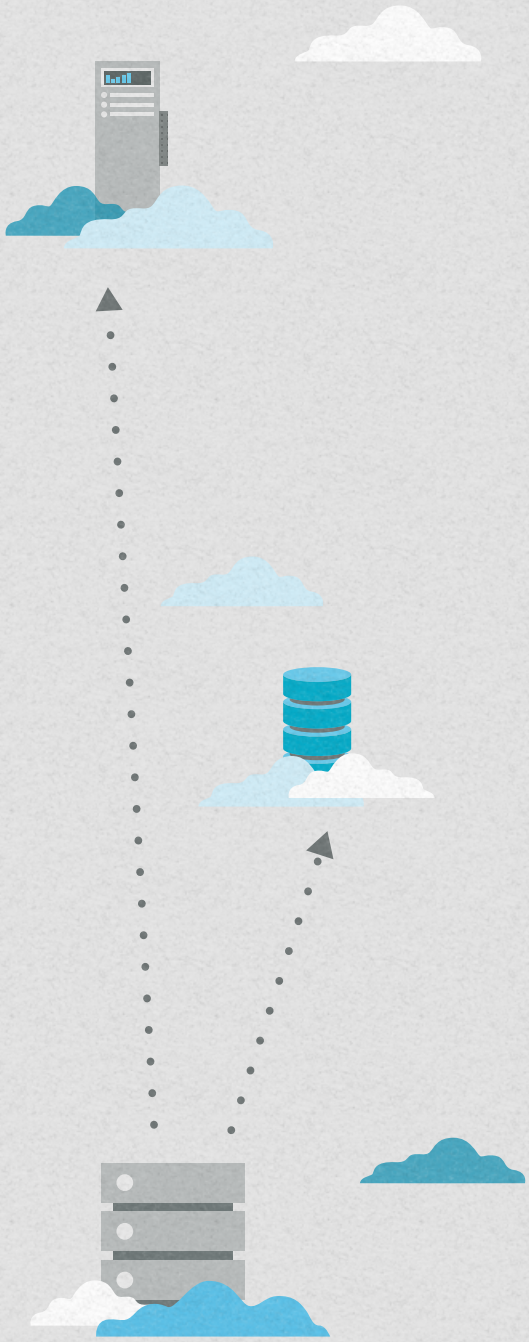


Figure 1: Full server protection captures everything on the system you need to restore service from the replication environment including operating system, system state, applications and settings.

The Carbonite Availability user manual details each step for configuring protection for all the major server platforms commonly used in today's IT environments.





Carbonite Availability onboarding overview

Here's what to expect after installing the Carbonite replication console:

1. From the console, identify the source system(s) you want to protect as well as the target system(s) to which you'll failover in a disaster or outage. An SDK is also available if you wish to automate the process of creating replication jobs.
2. Deploy the agents to the source machine and configure the target systems.
3. Select a protection workflow and configure and start the jobs to begin replication.
4. Replication occurs continuously at the byte level, with no performance impact, keeping the source and target in sync.
5. Carbonite Availability monitors the source for a failure, using configurable thresholds.
6. If the source fails, the target will spin up either automatically or manually, depending on how you configure it in the console, bringing online an identical copy of the source within a few minutes.
7. Once online, the target acts as the primary system and users are routed to it via a DNS update.

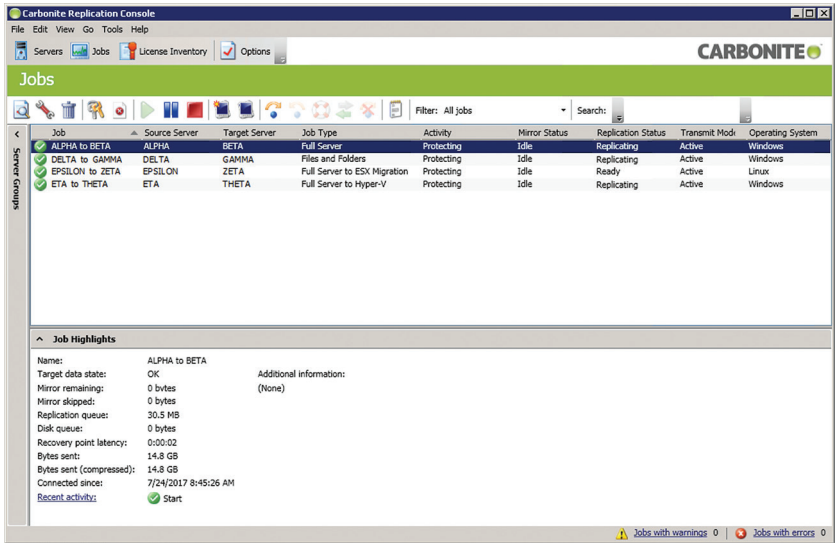


Figure 2: The Carbonite replication console is the central management tool for configuring and monitoring protection.

Carbonite Availability onboarding overview

Expectations for the initial replica

Carbonite Availability will replicate all data on the source system to the target and simultaneously replicate any changes being made to the source. Your network bandwidth and overall network utilization will have an impact on the amount of time required to synchronize the source and target. Using a dedicated replication link would increase replication speed without impacting business traffic on the network.

Carbonite Availability replicates over standard TCP/IP connections and can compress data in transit. If you are using a compression router, turning on compression is not recommended due to slight compression overhead.

In many cases, you can pre-seed the target system by restoring a backup of the source. Carbonite Availability will identify that the target has existing data and replicate only the differences, rather than mirroring the full source system. This option can significantly reduce the time required to synchronize the two systems.

Virtual protection

Carbonite Availability also delivers high availability with integrated support for Hyper-V and vSphere hypervisors. This virtual protection model provides simple and efficient protection of physical or virtual environments to a virtual target in a many-to-one configuration, including auto-provisioning of the target virtual machine.

To configure virtual protection, first identify your source, which is the server you want to protect. The source can be a physical server or a virtual machine. The target can be in a Hyper-V or vSphere environment. The administrator defines what constitutes a failure when configuring protection in the console. Carbonite Availability then monitors the source. In the event of a failure, the replica virtual machine on the target will fail over and become the source, allowing end-users to continue accessing data and applications seamlessly. The Carbonite Availability user manual has step-by-step instructions for configuring virtual protection, testing and failing over for both Hyper-V and vSphere environments.

Access privileges

To ensure the confidentiality of data, Carbonite Availability offers multi-level security using native operating system security features. Privileges are granted through membership in user groups defined on each machine. To gain access to a source or target, the user must provide a valid operating system user name and password, and the specified user name must be a member of one of the approved security groups. Once a valid user name and password have been provided and the source or target has verified membership in one of the security groups, the user is granted appropriate access to the source or target and the corresponding features are enabled in the client. Access is granted on one of the following three levels:

- **Administrator access** – All features are available for that machine.
- **Monitor access** – Servers and statistics can be viewed, but management and configuration functionality is not available.
- **No access** – Servers appear in the clients, but no access to view the server details is available.

Carbonite Availability onboarding overview

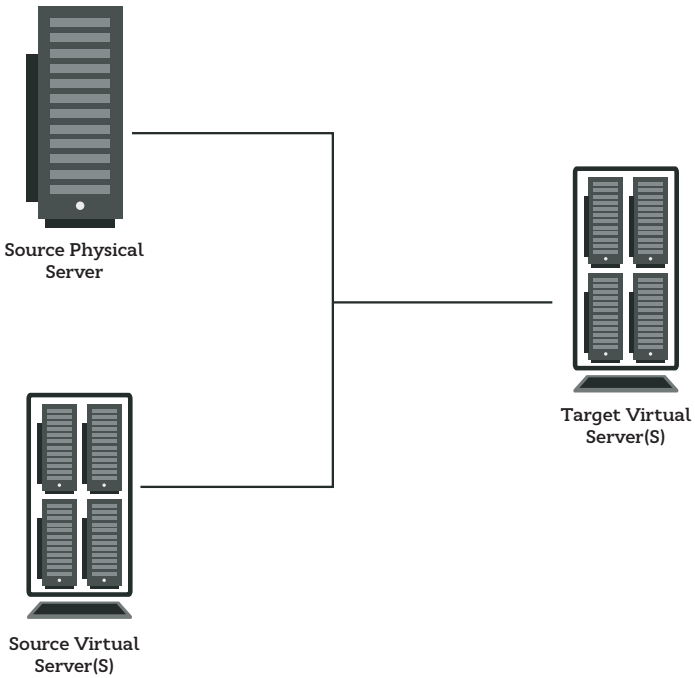


Figure 3: Carbonite Availability protects both physical and virtual servers with a perfectly mirrored replica running in either Hyper-V or vSphere.

Failover testing

Carbonite Availability enables administrators to perform non-disruptive test failovers using a snapshot of the target data to ensure the source is properly synchronized, including cross-dependencies that need to be preserved to maintain interoperability. A test failover includes all the steps that would be performed during an actual failover except the source is never taken offline and users are never rerouted to the target.

Carbonite recommends failover testing as soon as the initial mirror of the source is complete on the target, or no later than 90 days after deploying the solution. Additionally, anytime there's a change to network topology, a test failover should be performed to ensure cross-dependent systems are unaffected.

Carbonite Availability onboarding overview

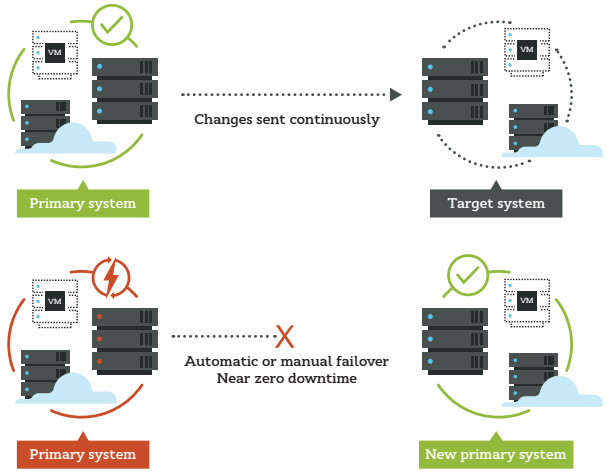


Figure 4: Carbonite Availability replicates changes between the source and target, creating a bit-perfect mirror for immediate failover in the event of a disruption at the source.

Service and Support

Our professional services team is comprised of knowledgeable, helpful experts who configure and troubleshoot data protection environments on a daily basis. They can guide you through the process of configuring the solution for your environment either on-site or remotely. They can also teach you how to monitor the data protection environment, perform test failovers and give you best practice recommendations for ensuring your disaster recovery plan will meet the needs of the organization(s) you support.

In addition to our professional services team, we offer multiple support resources for answering any questions that may arise while configuring or using Carbonite Availability. Our online support center has a complete knowledge base with how-to articles and instructions for virtually any process or procedure supported by the solution. The console also offers contextual tips depending on where you are and what you're doing within it.

Contact Us

Phone: 800-683-4667
Email: DataProtectionSales@carbonite.com