



Introducing CA ARCserve Central Host-Based VM Backup

CA ARCserve Central Host-Based Backup allows an installation CA ARCserve D2D to protect multiple VMware Windows virtual machines. Also, these recovery points support the Recover VM recovery type, allowing the process to restore a complete virtual machine. In fact, since CA ARCserve D2D is used to create the recovery point, albeit remotely, the destination data fully supports all CA ARCserve D2D recovery methods. Keep in mind, that while CA ARCserve D2D is not required to be installed on the virtual machines being protected, it is required for restore types other than Recover VM.

OVERVIEW

One to Many — By using CA ARCserve D2D installed on one server to protect more than one virtual machine, the backup overhead on the virtual machine is almost nonexistent.

Auto Discovery — Use your ESX or Virtual Center to discover and optionally add the virtual machines to backup policy.

Backup Policy — All backup settings are configured and deployed as policy to one or more nodes, and nodes can be added and associated with policy.

Scalable — Based on the role, amount of data and rate of change there is no magic number of virtual machines that can be protected by a single CA ARCserve Host-Based Backup server. Installing more than one CA ARCserve Host-Based Backup Server provides a simple way to extend protection.

Recover VM — CA ARCserve Central Host Based Backup creates CA ARCserve D2D recovery points that support an additional recovery type, Recover VM. This method can be used to restore the entire virtual machine to the original or alternate ESX location.

Standard Recovery Points — The recovery points created on disk are standard CA ARCserve D2D recovery points, so all of the standard CA ARCserve D2D recovery types are supported as well.

Tape Integration — The CA ARCserve Central Host-Based Backup server can be added to the CA ARCserve Backup source tree as a CA ARCserve D2D Proxy Server. All virtual machines being protected will auto populate below and can be selected for backup. The actual source for the backup is the last CA ARCserve D2D recovery point on disk, not the virtual machine itself.

BENEFITS

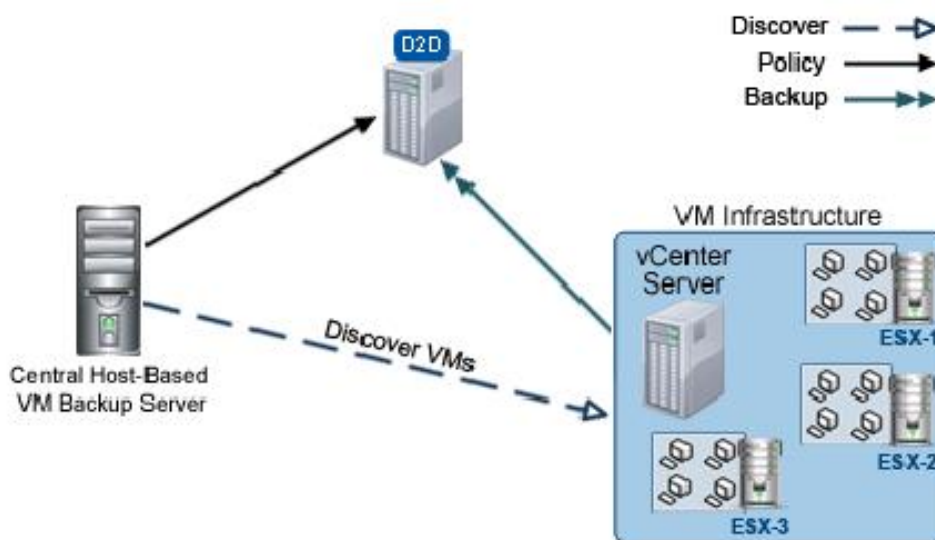
- Dedicating a server to perform backups of other machines alleviates much of the load from production and shifts it to a system tuned for backups
- Creating policies that can be shared across appropriate servers allows faster initial deployment, and subsequent deployments are just as fast. Adding discovered nodes to existing backup policy also decreases the change of user error, as only the assigned nodes change, not the actual policy.
- How many virtual machines can be protected with one CA ARCserve Central Host-Based installation? It depends. There are so many variables between the server and the virtual machines, there is no right number. However; the architecture is such that if a limit is reached, another CA ARCserve Central Host-Based Backup server can be used to split the virtual machines being protected.
- Recover VM is a great time saver. As an alternative to BMR to recover a server, Recover VM. The Recover VM method quickly and consistently creates a virtual machine from a CA ARCserve Central Host-Based Backup recovery point on an ESX server. It can then simply be started to complete the recovery.
- Since CA ARCserve Central Host-Based Backup uses CA ARCserve D2D to create the recovery points, all of the standard recovery methods are supported, in exactly the same way. This allows for a consistent recovery process with familiar user interfaces.
- While there are methods to retain recovery points on disk, long term data storage is probably best suited for tape. All virtual machines can be easily selected for tape backup from the CA ARCserve Backup source tree. Individual files can be restored from tape, or the entire recovery point for BMR, SQL or Exchange recovery.

Introducing CA ARCserve Central Host-Based Backup

Introducing CA ARCserve Central Host-Based Backup, a web-based solution designed protect Windows based virtual machines in a VMware hypervisor environment. Using a common policy interfaced, backup policy can be created quickly and applied consistently to individual or groups of virtual machines.

The CA ARCserve Central Host-Based Backup server initiates the backup and a snapshot of the virtual machine is taken. The virtual machine meta data, including the virtual machine name and number of VMDKs, is saved. Then the VMDK file is opened for read, and the data is copied to the destination, creating the recovery point.

When using Recover VM, an empty VMDK file is created on the specified ESX server, and the data is read from the recovery point and written to the virtual machine. This machine is then started to complete the recovery.



Frequently Asked Questions

Q: Does CA ARCserve Central Host-Based Backup require a license?

A: Yes, CA ARCserve Central Host-Based Backup requires a license.

Q: How can I discover the virtual machines in CA ARCserve Backup in order to move the recovery point data to tape?

A: Install the CA ARCserve Backup Client Agent for Windows on the CA ARCserve Host-Based Backup server. Then discover the server using the CA ARCserve Backup, and the virtual machines will populate under the CA ARCserve Host-Based Backup server.

Q: Can CA ARCserve D2D be used to Recover VM?

A: Yes, as long as the recovery point data was created by a CA ARCserve Central Host-Based Backup server. However; all of the VMware ESX information would have to be manually added during the process. When using CA ARCserve Central Host-Based Backup to perform Recover VM, this VMware information is known and automatically populated in the user interface.

Q: What hypervisors does CA ARCserve Central Host-Based Backup currently support?

A: At this time only VMware is supported, however; CA ARCserve Central Virtual Standby can convert CA ARCserve Central Host-Based Backup as well as CA ARCserve D2D recovery points to Microsoft Hyper-V virtual machines.

Q: Why am I only able to use Recover VM?

A: Check that VMware VIX is installed on the CA ARCserve Central Host-Based VM Backup server for file, application and email recovery.

- Q: What impact does CA ARCserve Central Host-Based Backup on the virtual machines during backup?
- A: Since the backup is snapshot based, the initial impact is the snapshot itself. The next consideration would be disk IO and network traffic which would depend on the configuration. Separating disk IO and network segmentation from the virtual machines would be the recommended configuration.

Summary

CA ARCserve Central Host-Based Backup allows instance of CA ARCserve D2D to efficiently protect one or more VMware windows based virtual machines. The familiar interfaces makes discovery and policy creation for multiple virtual machines as easy as a few clicks. The additional recovery type, Recover VM, is also supported when the repository data was created by CA ARCserve Central Host-Based Backup. This recovery method creates an empty VMDK file on the specified ESX server, and then copy the data from the recovery point into the VMDK. When complete the virtual machine can be started to complete the full system recovery using Recover VM. So once again it is clear how the CA ARCserve Central Applications continue to extend the base functionality of CA ARCserve D2D to provide the flexibility to create just the right data protection.

For more information about the CA ARCserve Family of products, please visit arcserve.com/products or test drive our products at arcserve.com/software-trials.