



Version 1.1

July 2024

Restore Active Directory Domain Controller with Cohesity

Domain Controller Recovery for AD with Cohesity

ABSTRACT

You could lose the Domain Controller (DC), the server that runs Active Directory, due to accidental deletion. This concise guide can help you restore an Active Directory Domain Controller from a Cohesity backup.

Table of Contents

The Case for Domain Controller Restore 3

The Recovery Workflow 4

Recover Your Active Directory Domain Controller 5

 Microsoft Limitations5

Install the Cohesity Windows Agent 6

Directory Services Repair Mode..... 9

Configure the Domain Controller to boot in DSRM using MSConfig..... 9

Recover the Domain Controller 10

 Instant Volume Mount.....10

Appendix A: Product Documentation 13

Your Feedback 14

About the Authors..... 14

Document Version History..... 14

Figures

Figure 1: Domain Controller Restore Sequence 4

The Case for Domain Controller Restore

Having a secure Domain Controller (DC) is not enough. Your DC could be hacked, become a target of a cyber attack, or could go down due to other reasons.

Imagine you've lost your DC to accidental deletion. Your old host is still up and running and now you want to restore the DC as quickly as possible.

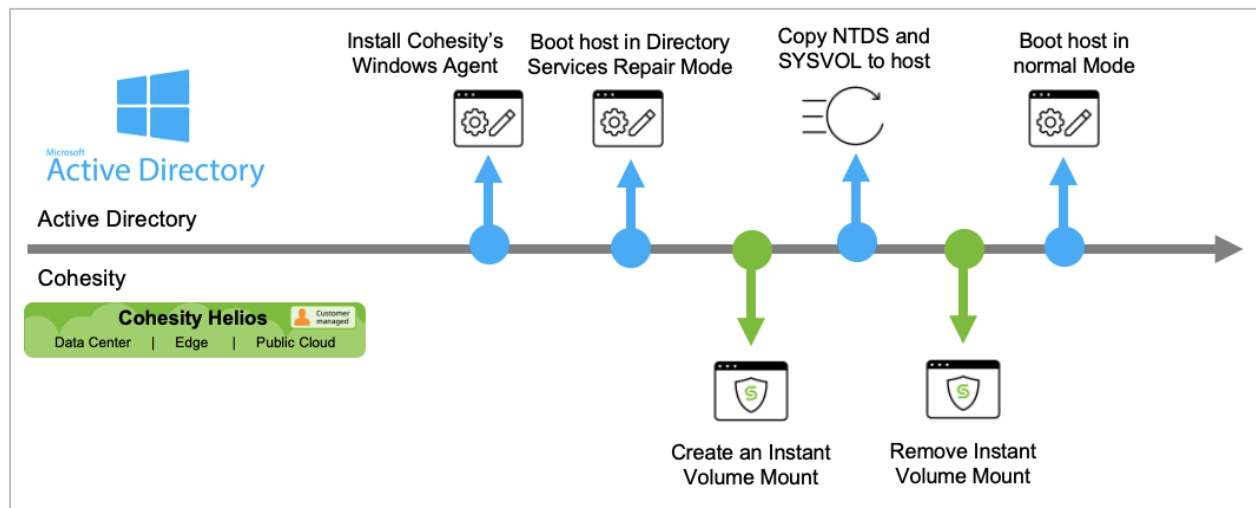
NOTE: Use the Domain Control restore procedure mentioned in the document is the *last* option because it may cause damage to your Active Directory.

The Domain Controller is one of several services that operate together within Active Directory. This workflow assumes that you've installed all Active Directory services together on the same host; and the host is not replicated.

The Recovery Workflow

1. [Install the Cohesity Agent if not already installed.](#)
2. [Configure the Domain Controller to boot in Directory Services Repair Mode.](#)
3. [Recover Domain Controller:](#)
 - Run Instant Volume Mount (IVM).
 - Copy the folders from the IVM.
 - Tear down the IVM.
 - Restart the Domain Controller in normal mode.
4. Login as domain administrator. Make sure that Active Directory services are running.
5. Verify the deleted Organizational Unit (OU) and all users under it are restored.

Figure 1: Domain Controller Restore Sequence



Recover Your Active Directory Domain Controller

We recommend backing up your domain regularly, so you have several backups to choose from depending on your requirements.

Microsoft recommends that you restore the DCs by using backups that you had taken a few days before the failure. In general, you must determine a tradeoff between the recency and the safeness of the restored data. Choosing a more recent backup recovers more useful data, but it might increase the risk of reintroducing dangerous data into the restored forest¹.

Microsoft Limitations

Restoring system state backups depends on the original operating system and server of the backup. For example, you should not restore a system state backup to a different server. In this case, you may see the following warning: “The specified backup is of a different server than the current one.”

Consider the following Microsoft limitations and recommendations before you proceed with the DC recovery procedure:

- Microsoft does not recommend performing a system state recovery with the backup to an alternate server because the server might become unusable.
- Microsoft recommends that If you need to restore Active Directory to different hardware, create full server backups and plan to perform a full server recovery.

NOTE: You cannot use the backup of a read-only Domain Controller (RODC) to restore a writeable DC.

- Microsoft states that beginning with Windows Server 2008, it is not supported to restore system state backup to a new installation of Windows Server on new hardware or the same hardware.

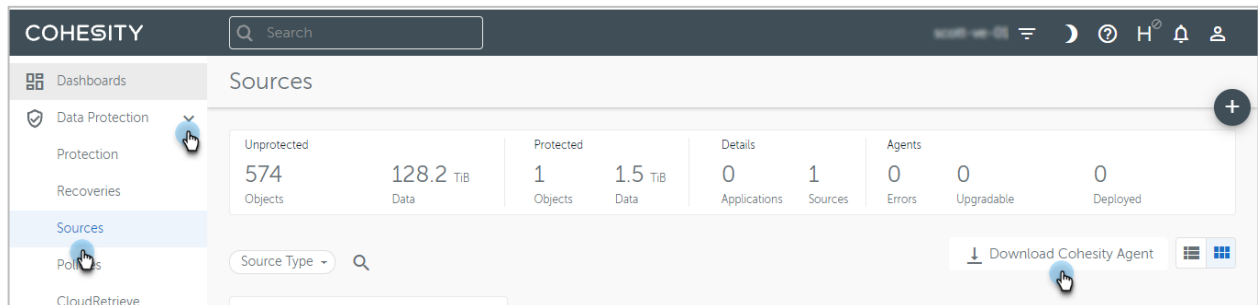
¹ [“Determining which backups to use”, Microsoft Documentation.](#)

Install the Cohesity Windows Agent

If the Cohesity Windows Agent is not already installed, you must install it on the Active Directory host. The Windows agent is designed to work specifically with the Windows operating system and is compatible with Windows versions 2008R2 and above. If there are multiple Active Directory hosts, you will need to install the agent on each host that you wish to protect.

To install the agent:

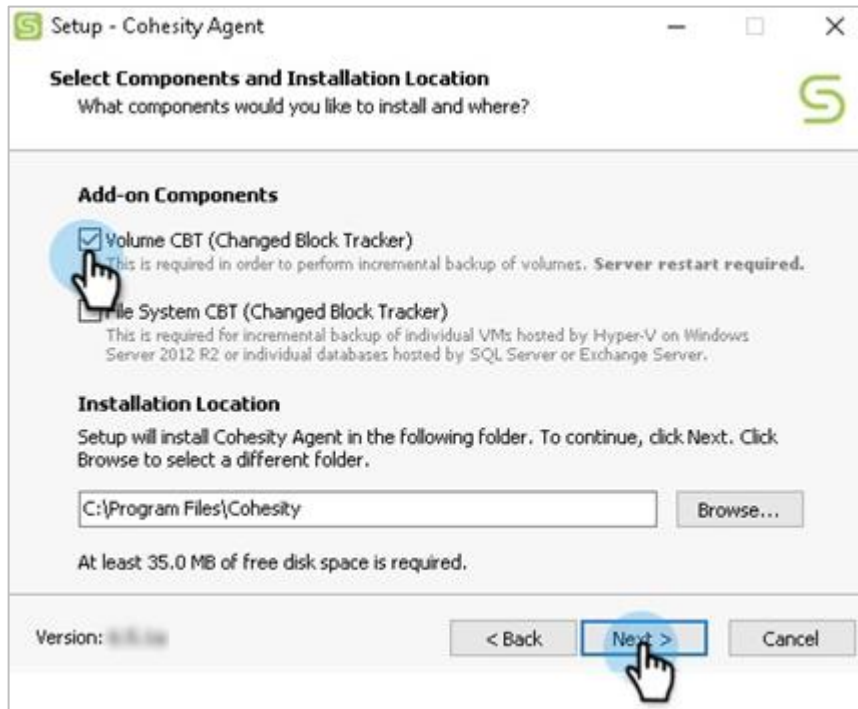
1. Log in to Cohesity and navigate to **Data Protection > Sources** and click **Download Cohesity Agent**.



2. Click the **Download** (↓) button for **Windows**.

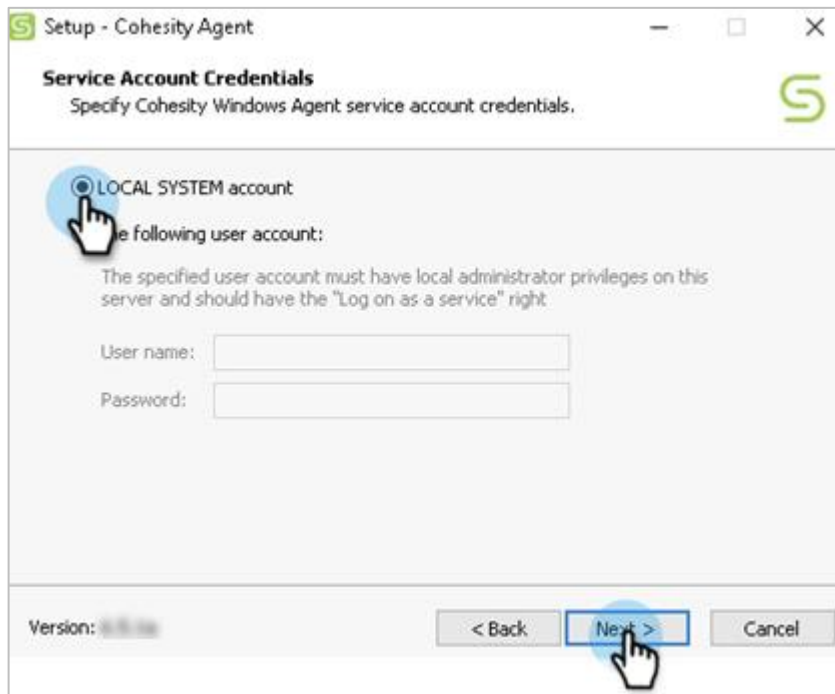


- When you launch the Cohesity Windows Agent installer, under **Add-on Components**, ensure that **Volume CBT** (the default) is selected and click **Next**.



You need to install the Volume CBT (Changed Block Tracker) component to perform incremental backups, and reboot the system. Until you reboot, you can only perform volume-based *full* backups.

4. Select the type of service account to use for control over your systems. The **LOCAL SYSTEM account** gives you direct control, but you can also enter your Active Directory domain admin user account.



TIP: If you are unsure which account to use, don't let that slow you down—choose the **LOCAL SYSTEM account**. This account already has most of the required permissions. You can change the agent service account later if you change your mind.

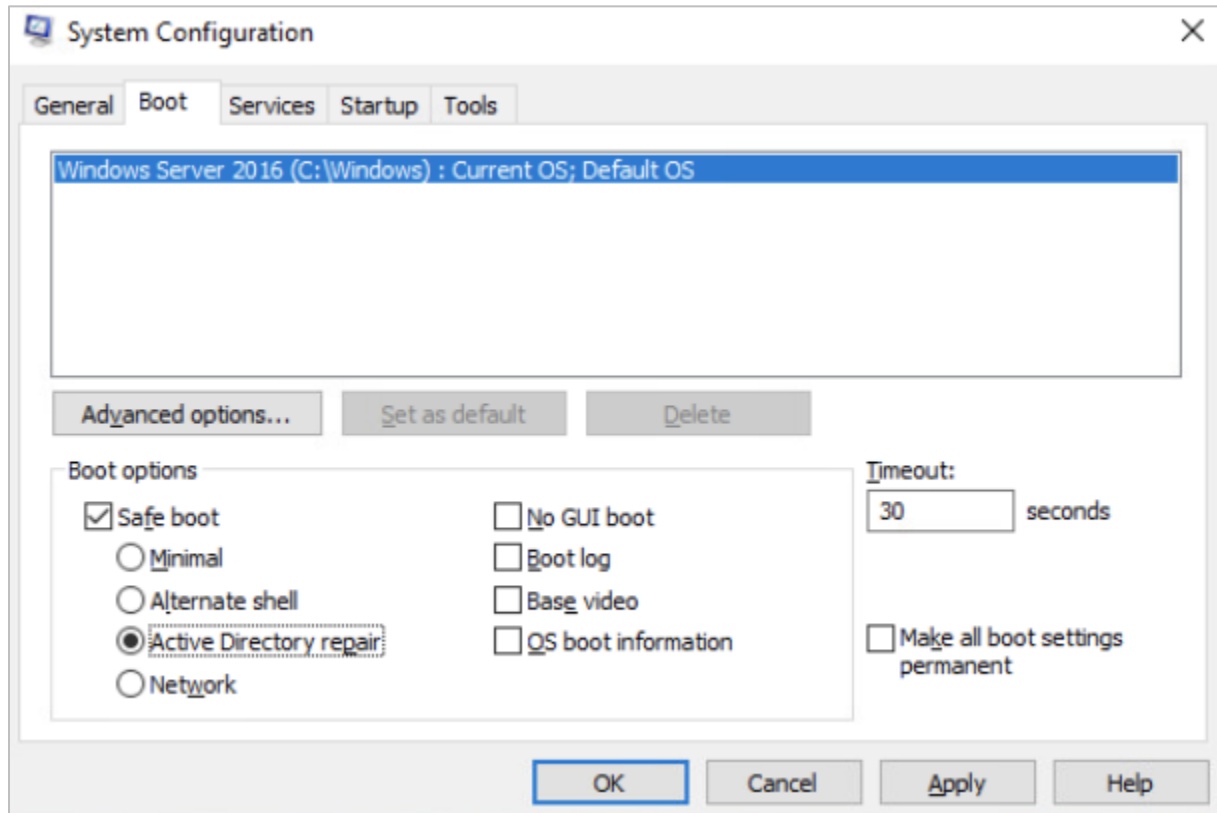
Now you are ready to put the host in Directory Services Repair Mode (DSRM).

Directory Services Repair Mode

The DSRM function on Active Directory Domain Controllers helps you take the server offline to restore AD backups.

Configure the Domain Controller to boot in DSRM using MSConfig

1. On the **Start** menu, type msconfig and press **Enter**.



2. Restart the Domain Controller. The server should now be running in safe mode.
3. Login as a local administrator. Verify that Active Directory services are not running.

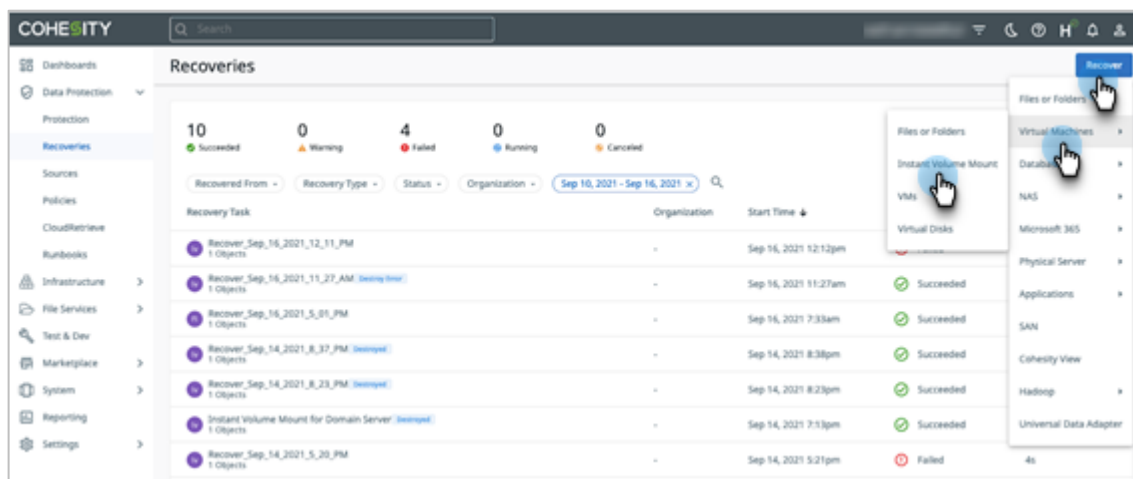
Recover the Domain Controller

Cohesity's IVM feature allows you to make selected backup volumes available at a target location. Instant mounting is available only for backup volumes stored locally. You can mount the volume to its original location or to a new location. For more information, see [our IVM documentation](#).

Here is how you recover your Domain Controller using Cohesity Instant Volume Mount.

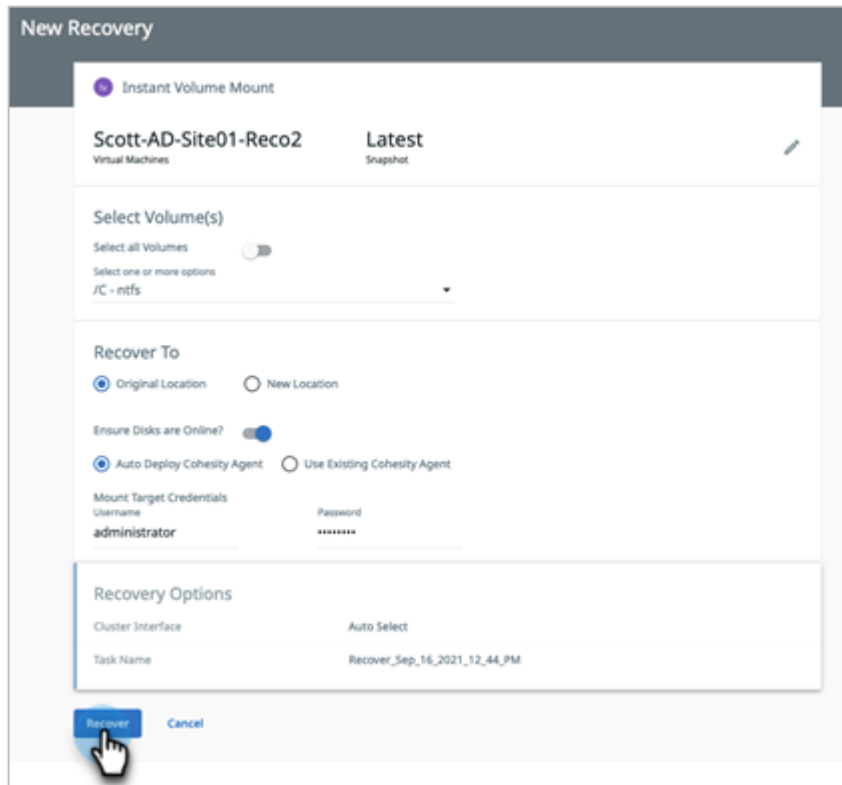
Instant Volume Mount

1. Navigate to the **Recoveries** sidebar and click **Recover > Virtual Machines > Instant Volume Mount**.

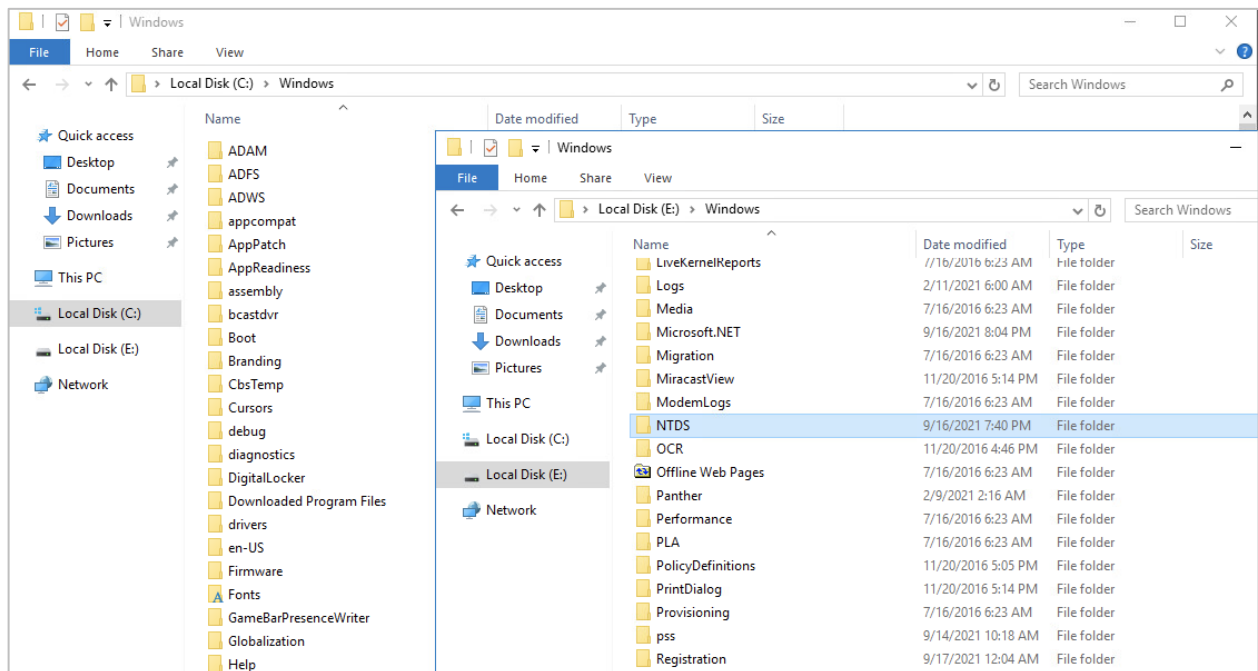


2. Use the search field to find and select the backup of your server.
3. Click **Next: Recovery Options**.

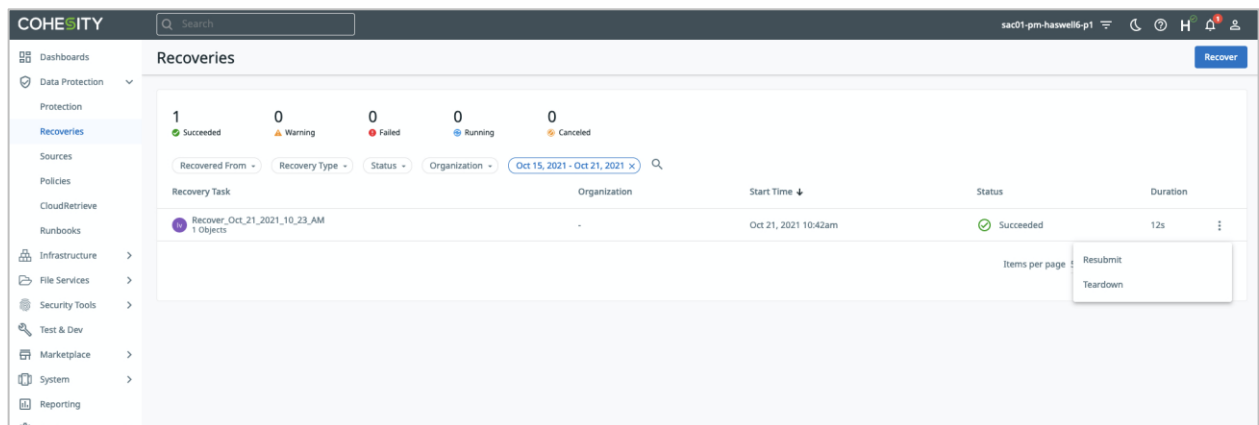
4. Select volumes and recovery options, and click **Recover**. The instant volume mount is presented to the host as a drive.



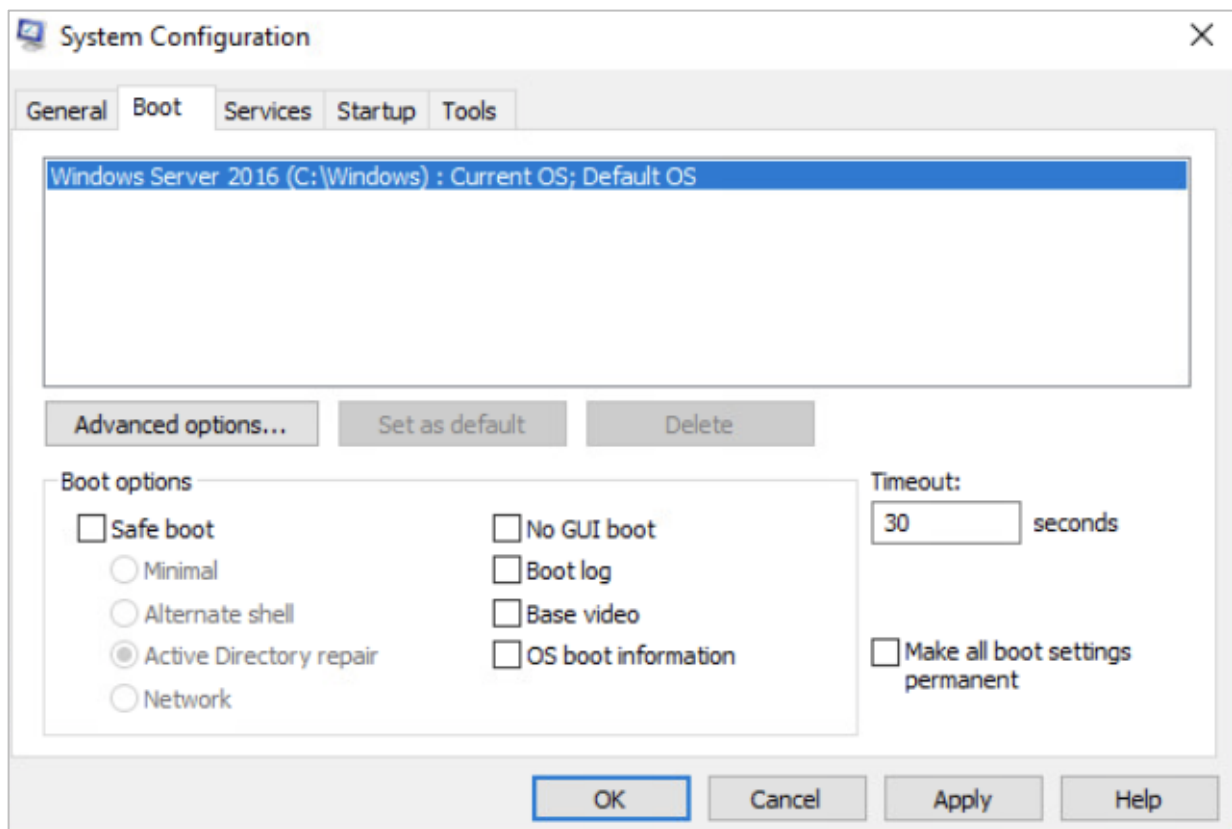
5. Copy the folders NTDS and SYSVOL from the IVM over to their location on the local C:\ drive.



6. Tear down the IVM once you complete copying over the files.



7. Use msconfig to uncheck **Safe boot**, and then reboot the host.



8. Login as domain administrator. Make sure that Active Directory services are running.
9. Verify the deleted OU and all users under it are restored.

Appendix A: Product Documentation

Review our Active Directory product documentation for an in-depth understanding of Active Directory concepts and procedures:

- [Active Directory Protection Requirements](#)
- [Active Directory Non-Cohesity-Specific Information](#)
- [MS Active Directory Key Concepts](#)
- [Set Up Active Directory for Data Protection](#)
- [Protect Active Directory](#)
- [Recover Active Directory Objects](#)
- [Active Directory Data Protection FAQs](#)

Your Feedback

Was this document helpful? [Send us your feedback!](#)

About the Authors

Scott Lorenz is a SQL Solutions Engineer at Cohesity. In his role, Scott focuses on business-critical applications, MS SQL Server databases, cloud storage, and enterprise data protection. Scott has over 26 years' experience as an enterprise DBA.

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.1	July 2024	Publishing
1.0	Nov 2021	Original Document

ABOUT COHESITY

[Cohesity](#) is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our [website](#) and [blog](#), follow us on [Twitter](#) and [LinkedIn](#) and like us on [Facebook](#).

© 2024. Cohesity, Inc. All Rights Reserved. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.