COHESITY

Version 1.2

July 2024

Protect Microsoft Active Directory with Cohesity

Backup and Granular Recovery for AD with Cohesity

ABSTRACT

In today's large organizations and enterprises, Active Directory is an increasingly critical component of your growing data infrastructure. Therefore, it is essential to protect that infrastructure efficiently and reliably. Read these practical recommendations for configuring Cohesity protection for Active Directory, with a focus on in-place granular recovery. You will find descriptions, technical recommendations, and notes describing the common mistakes to avoid.

Table of Contents

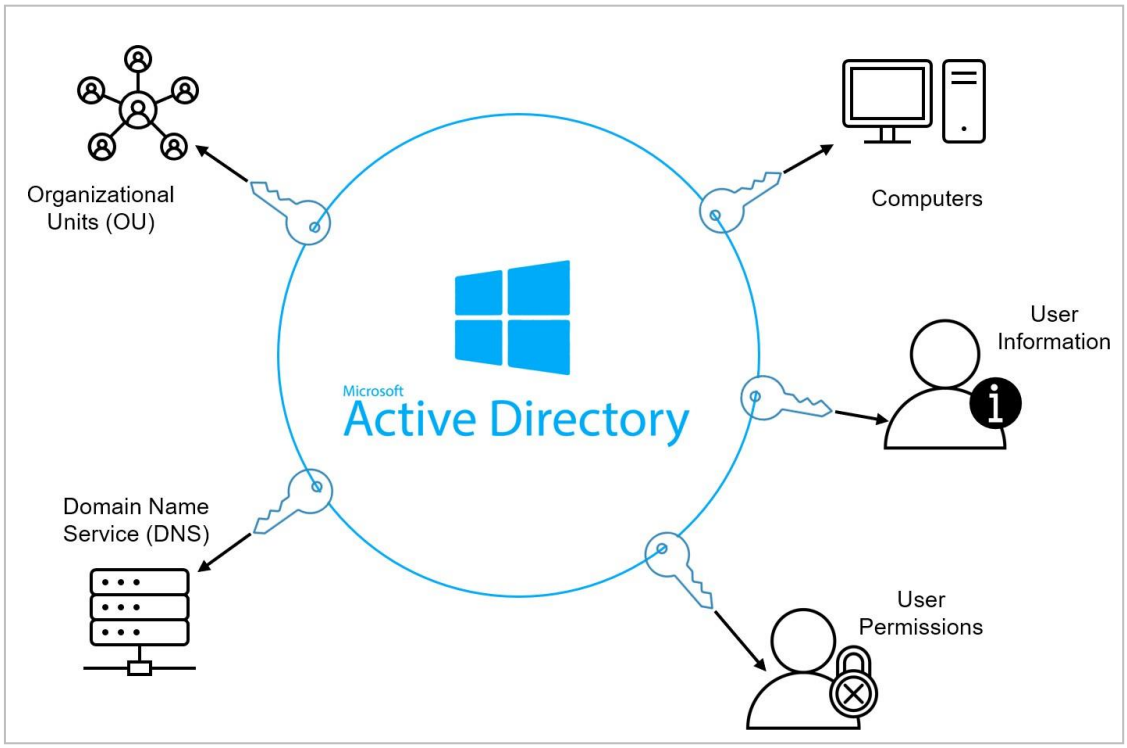
Figures

Use Active Directory to Protect Your Data Kingdom

Active Directory (AD) enables administrators to manage enterprise-wide information and role-based user access to data efficiently from a central repository. It governs the information about users and groups, computers, printers, applications, and services across your enterprise. As an AD administrator, you can make those resources available to the right users throughout the entire enterprise, to as many or as few people as is appropriate for each resource.

To achieve this, Active Directory resolves IP addresses through its own DNS service and is the central location for authenticating passwords — it quite literally holds the keys to the kingdom.

Figure 1: Active Directory Holds the Keys to Your Data Kingdom



Given its central and growing role in managing and protecting your organization's information and resources, it is critical to protect your Active Directory from any number of today's data threats:

- Accidental data deletion
- Insider attack
- Security breaches
- Administrative error
- Ransomware and malware attacks

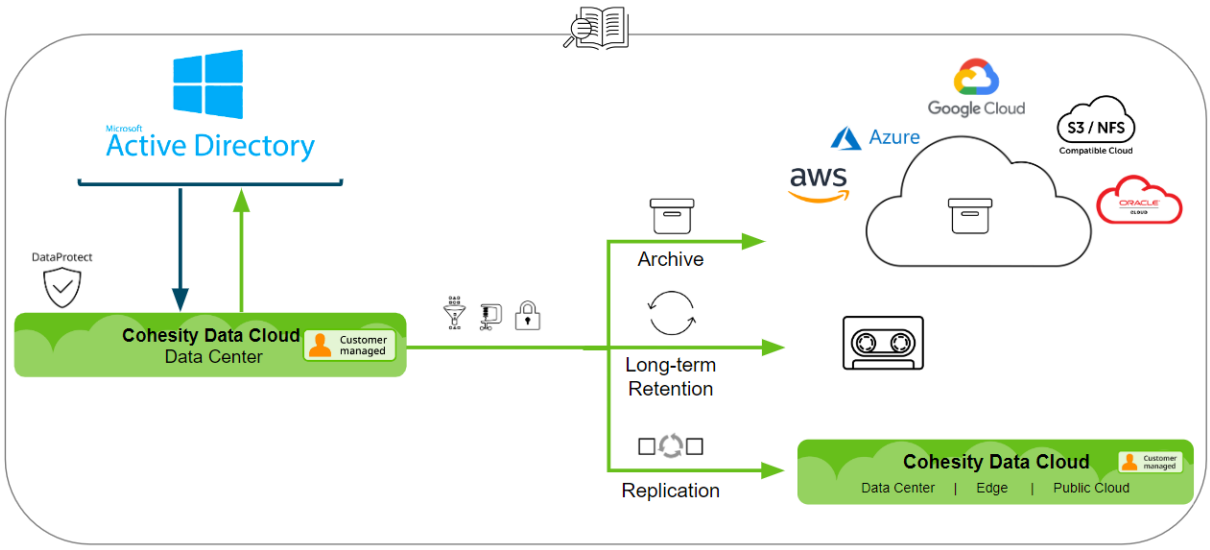
Cohesity provides a web-scale, space-efficient, highly available, and robust platform to back up and protect your AD universe from these threats, with extensive features to help you meet your business and compliance needs, your SLAs, and your long-term retention, recovery, and preparedness requirements.

Cohesity's Advanced Protection for Active Directory

Cohesity is a modern, software-defined platform for data management. Taking inspiration from its web-scale architecture and leveraging its unique distributed file system (SpanFS®), Cohesity offers high-scalability and reliability.

Cohesity's flexible architecture allows easy expansion, increasing operational simplicity and improving TCO. Cohesity's solution for Active Directory works on-premises, in the public cloud, and in your remote and branch offices. You choose how to back up your data and where to keep your backups, and for how long.

Figure 2: Cohesity's Advanced Data Protection for Active Directory



Features and Benefits of Cohesity Protection

Cohesity's solution for AD includes many features that make your backups much more valuable, including:

- **Granular Object Restore**. Once your Active Directory is protected, Cohesity gives you the flexibility to restore everything from an entire snapshot to a whole Microsoft Organizational Unit (OU), a specific user, or even a specific email.

  In addition, Cohesity's granular object restore uses a comparison of your live Active Directory with a mounted backup, which allows you to identify the differences between live data and protected data quickly. You can easily spot the difference and then restore just the objects and attributes you need.

- **Flexibility**. Cohesity gives you the ability to browse and search across all your snapshots, and to restore to different locations on different servers.

- **Performance to Meet Your SLAs**. Cohesity gives you the backup performance you need to protect your Active Directory objects efficiently and securely.

- **Scalability**. Cohesity protection for AD is scalable from a single domain controller to an AD tree and even an entire AD forest across multiple hosts.
- **Compression**. Data compression significantly reduces storage usage and data transmission. Efficient storage means you have room for more backups and other important data. By default, Cohesity performs compression on all the data it stores.

  If you also enable *inline* compression, the process occurs as Cohesity is saving the data to storage, instead of after saving it.
- **Encryption at rest, in flight, and in the cloud**. Active Directory governs access to data and resources across your organization and, as such, it is vital to protect that data from unauthorized access.
  - **Data-at-Rest**. The Cohesity SpanFS® file system provides full at-rest encryption based on the strong AES-256 CBC (Cipher Block Chaining) standard.
  - **Data-in-Flight**. Cohesity can encrypt all data that is transmitted.
  - **Data-in-Cloud**. Cohesity's CloudArchive provides encryption for data stored in the cloud.

For details, see Cohesity Security Features in the online Help.

- **Archive to cloud**. Cohesity's policy-based ability to archive to public clouds like AWS, Azure, and Google Cloud, as well as to any S3-compatible storage, makes it easy to leverage lower-cost long-term retention and protect your data from regional disasters. Cohesity makes it easy to retrieve your organization's information to different geographical locations, whenever you need to.
- **Disaster Recovery**. Protect your Active Directory universe from disaster by replicating your Cohesity backups to another location that can be ready to failover (and failback, after repairs) as soon as disaster strikes.

In addition, Active Directory can be deployed to provide services across multiple hosts. Active Directory might be replicated between data centers on multiple hosts. In such cases, you can use Cohesity *for other Active Directory backups* and even *create new backup strategies*. For example, you can protect just one AD replica or all the AD replicas across the business.

Use Cohesity to Protect Your Active Directory

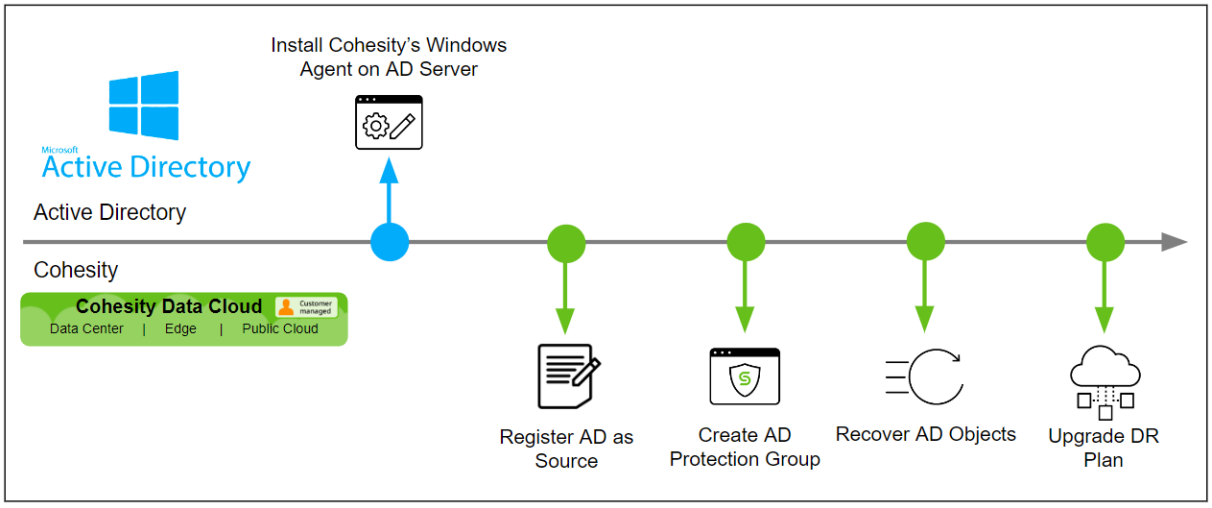
Cohesity offers a policy-based, highly-scalable data protection infrastructure for your Active Directory data. With a few steps, you can set up Cohesity to meet all your data protection requirements.

Implementing any enterprise technology is always a process. It is important to understand what makes a backup strategy successful. For example, it is important to have a second copy of backup data in case the original copy fails. But that is only part of the story. When you need to recover your AD objects, it is crucial that you be able to find those objects and restore them quickly. To take full advantage of the many features of Cohesity's solution, be sure you understand each step of the implementation.

To protect your Active Directory using Cohesity:

1. Install Cohesity's Windows Agent on your AD server.
2. Register Active Directory as a Cohesity source.
3. Create a Cohesity Protection Group to specify the AD data you need to protect.
4. Recover protected Active Directory objects.
5. Upgrade your disaster recovery (DR) plan to improve your enterprise's readiness and resilience.

Figure 3: Set Up Active Directory Data Protection with Cohesity



Complete these steps to protect your Active Directory data. Get started by deploying Cohesity's Windows Agent next!

NOTE: For more background, see Appendix A: Terminology and Appendix B: Product Documentation.

Deploy the Cohesity Windows Agent

To start, you need to install the Cohesity Windows Agent 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 you wish to protect.

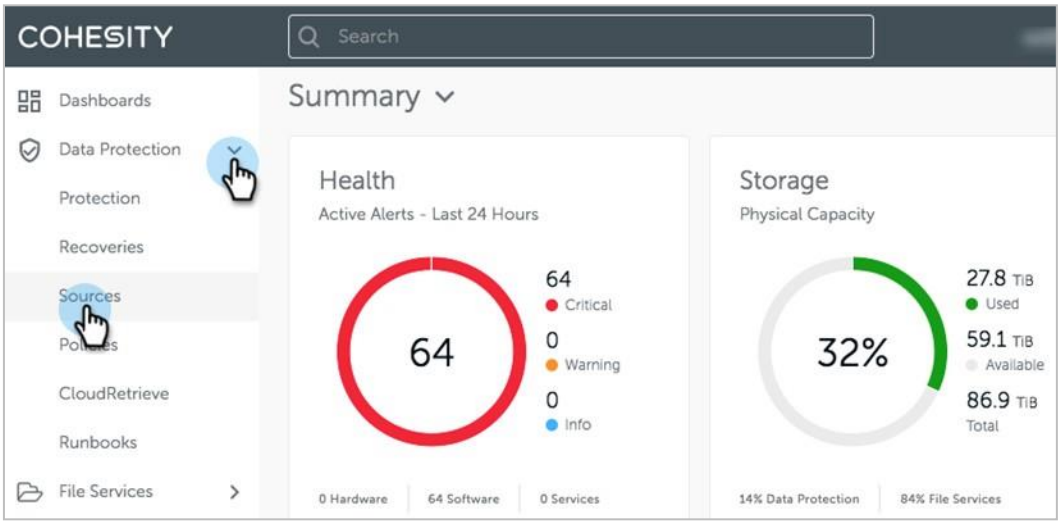
The agent is lightweight and has a small memory footprint. The agent carries out the tasks you define in the Cohesity Protection Group. It ties together technologies and capabilities already in Windows, like Windows VSS, and new technologies, like Cohesity Changed Block Tracker (CBT), so that you can tackle data management efficiently.

You manage the Cohesity Agent through the Sources page in Cohesity. When an upgrade becomes available for any agent you've installed, an **Upgrade Agent** button appears next to your Active Directory source. You can upgrade the agent from there.

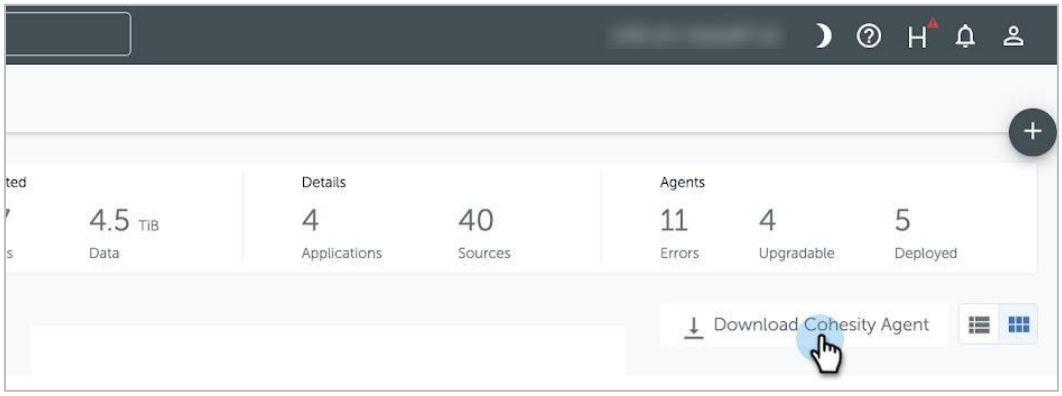
IMPORTANT: You need to install the agent on each Active Directory host you wish to protect.

To install the agent:

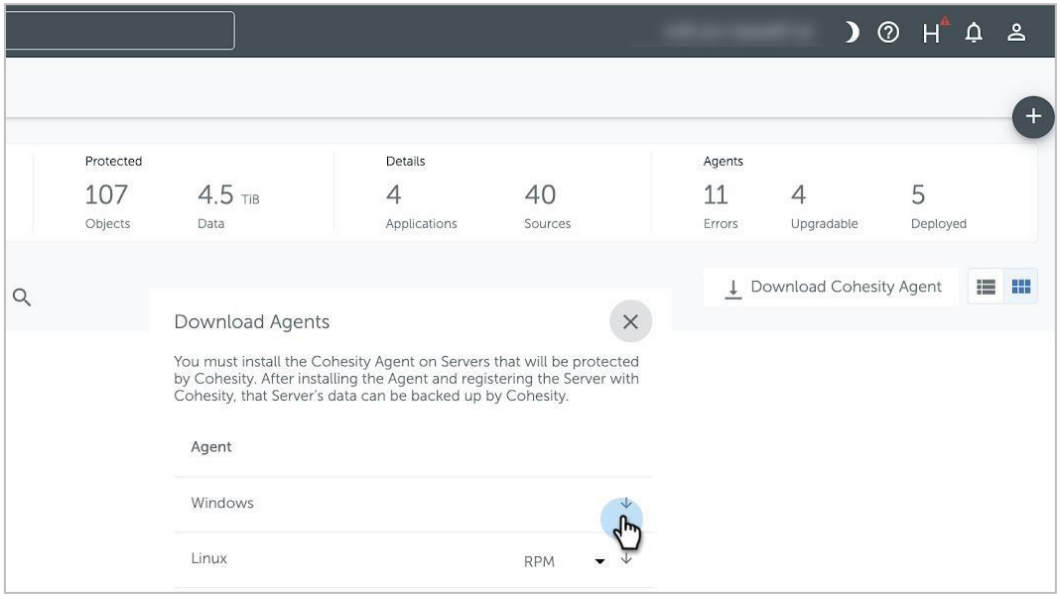
1. Log in to Cohesity and navigate to **Data Protection** > **Sources**.



2. Click **Download Cohesity Agent**.

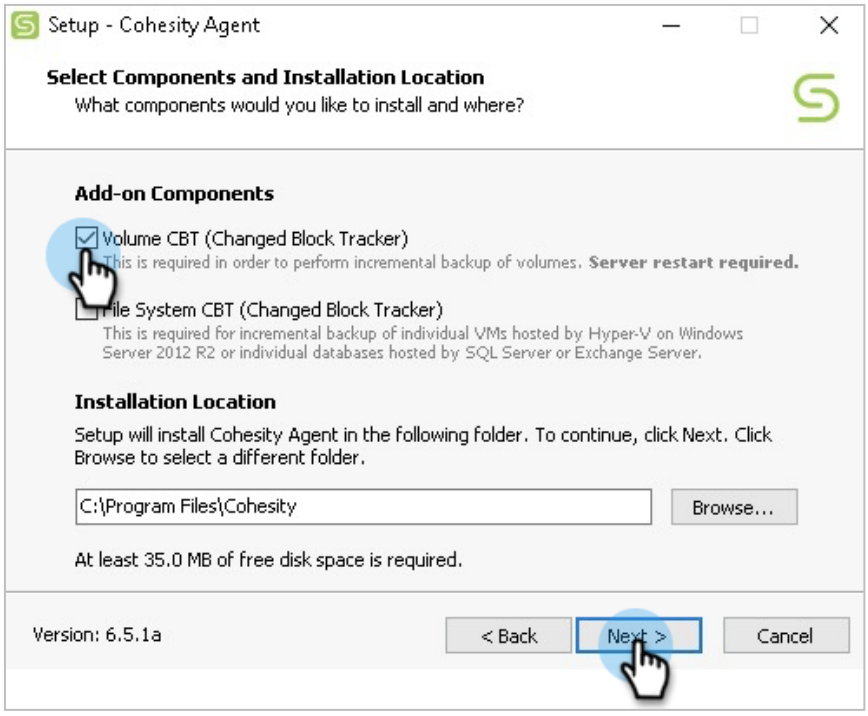


3. Click the **Download** (↓) button for **Windows**.



4. Download or copy the agent to all AD hosts you want to protect. On each AD host, install the agent and run the installer.

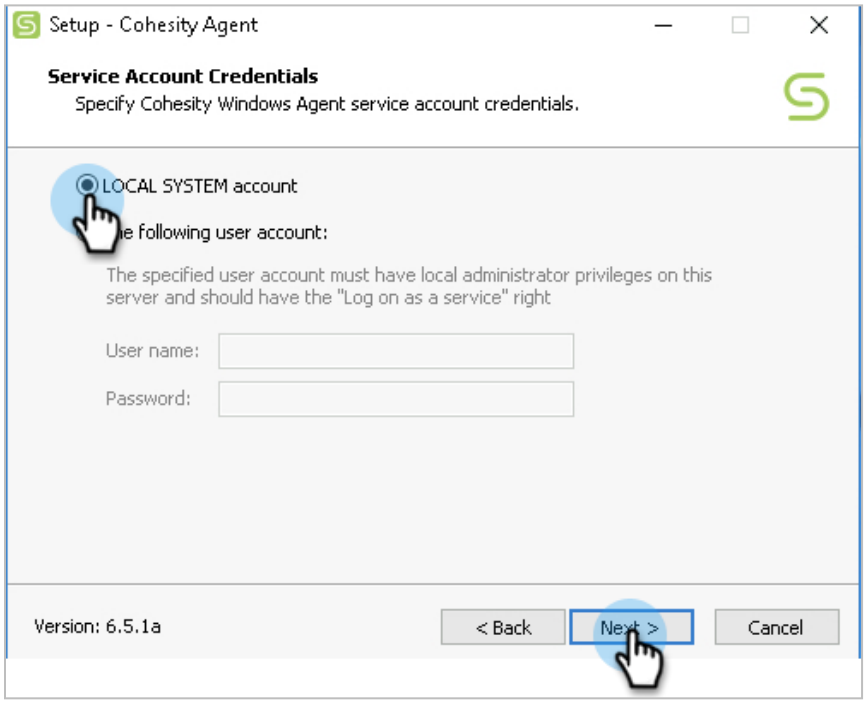
5. When you launch the Cohesity Windows Agent installer, under **Add-on Components**, ensure that **Volume CBT** (the default) is selected and click **Next**.



The Volume CBT (Changed Block Tracker) component is required to perform incremental backups and requires a reboot. Until you reboot, you can only perform volume-based *full* backups .

> **TIP**: The Cohesity snapshot captures all the data on the AD host. That means it captures all the changes to AD-related files *and* to other, non-AD files. To keep your AD backups running efficiently, keep the volume that AD is using clear of lower-priority and unrelated files.

6. 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.

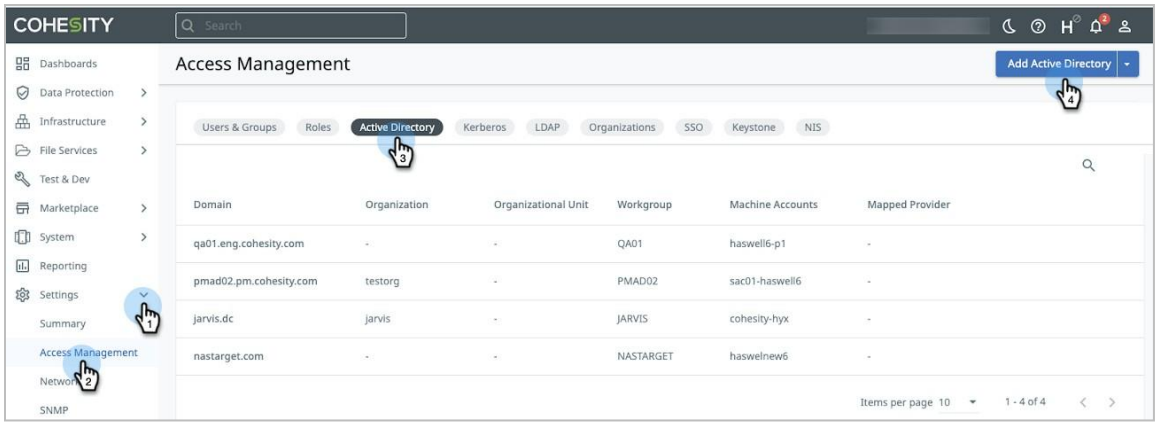
Your AD host is now ready to be registered as a Cohesity source in the next chapter.

Register Active Directory in Cohesity

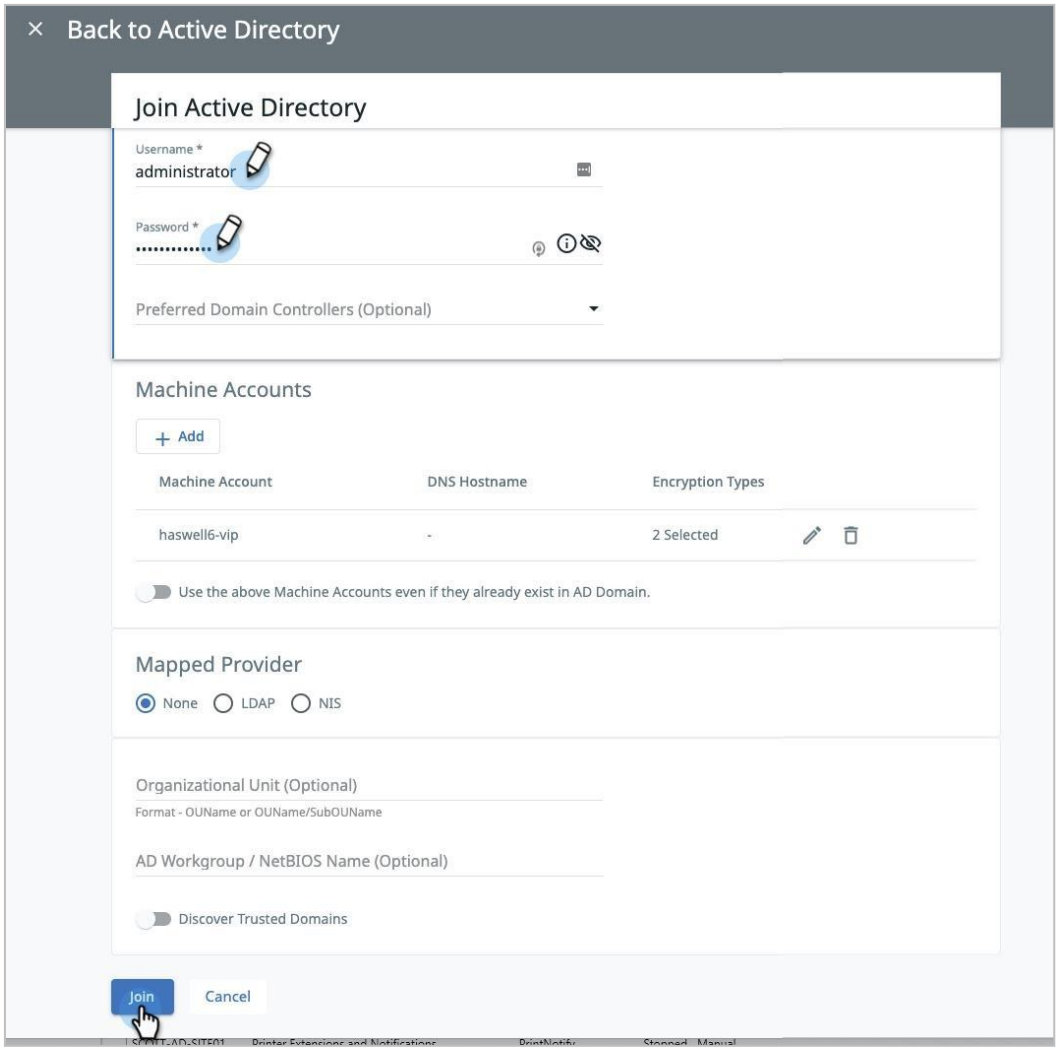
To protect your Active Directory with Cohesity and take advantage of its many features, you need to register it as a Cohesity source. Once it's registered in Cohesity, you will be able to add it to a Protection Group and configure the settings for your environment.

To register AD as a Source in Cohesity:

1. Before you can register AD as a source, you need to add AD to your Cohesity cluster. Log in to Cohesity and navigate to **Settings** > **Access Management** > **Active Directory** and click **Add Active Directory**.

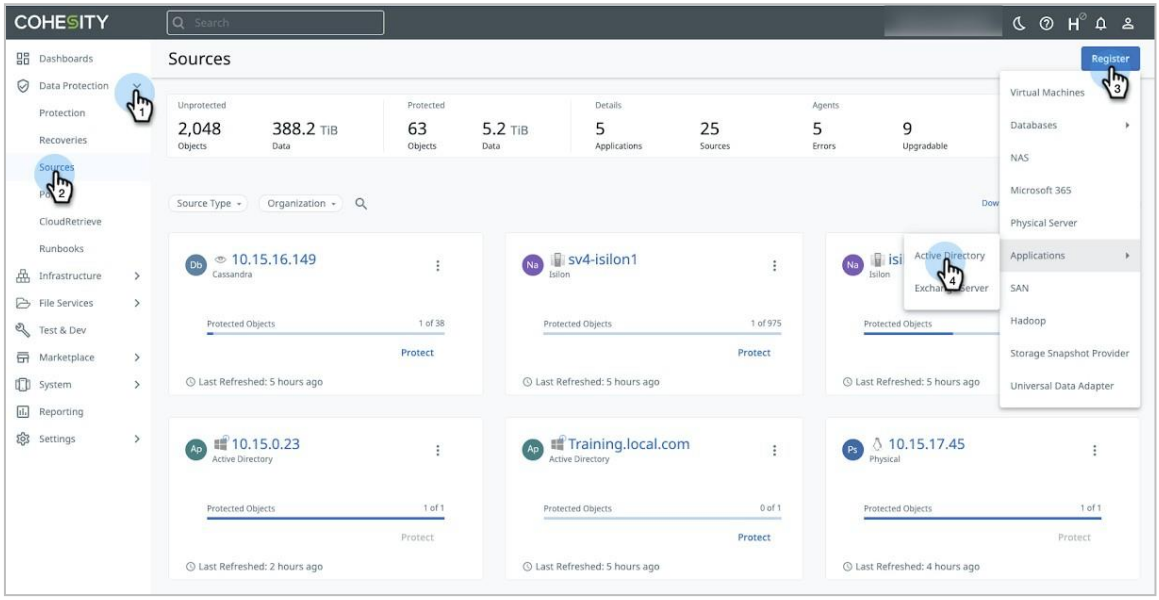


2. In the **Join Active Directory** form, enter the AD administrator **Username** and **Password** and click **Join**.



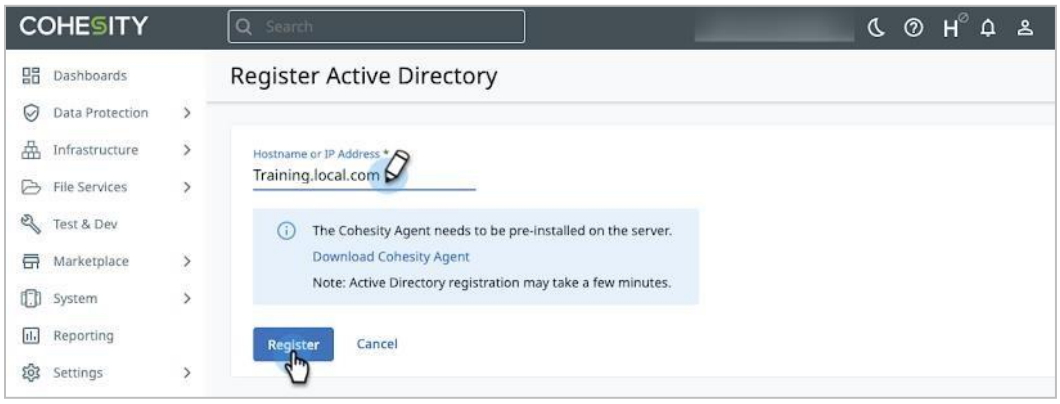
For details on the other options here, see Join the Cluster to an AD Domain in the online Help.

3. Navigate to **Data Protection** > **Sources** > **Register** > **Applications** > **Active Directory**.

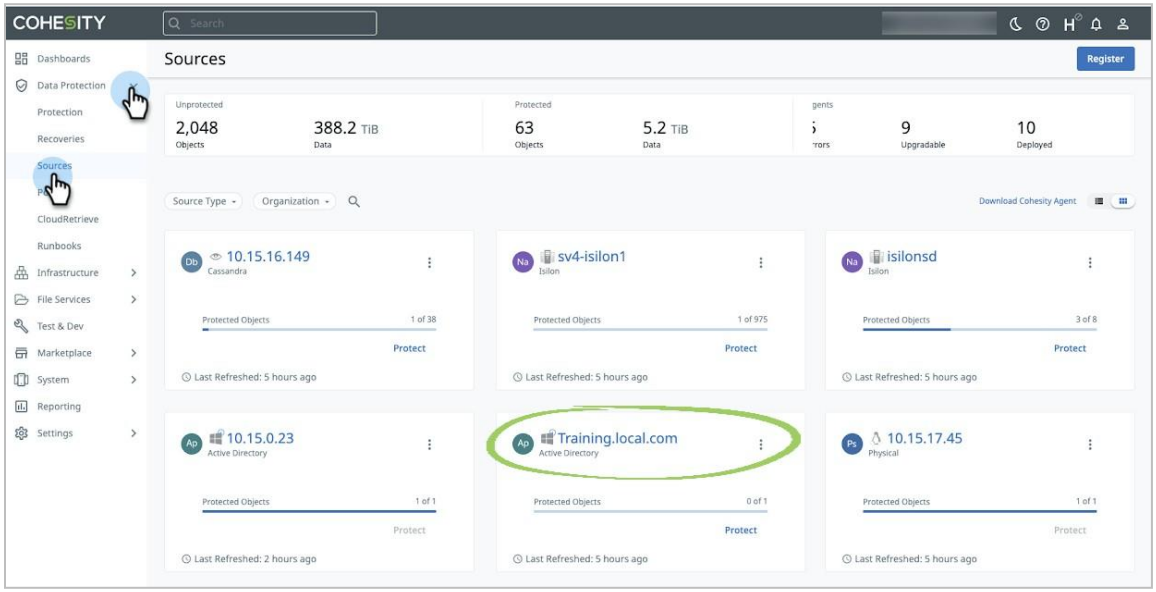


NOTE: When you register AD, Cohesity registers both the host and the application. Cohesity sees the host and the AD application so that it has full application awareness.

4. In the **Register Active Directory** form, enter the AD FQDN or IP address and click **Register**.



5. The **Sources** page now includes your Active Directory (in our example, **Training.local.com**), available for immediate protection.



To protect your newly registered AD source, you'll create a Cohesity Protection Group for it in the next chapter.

Create a Protection Group

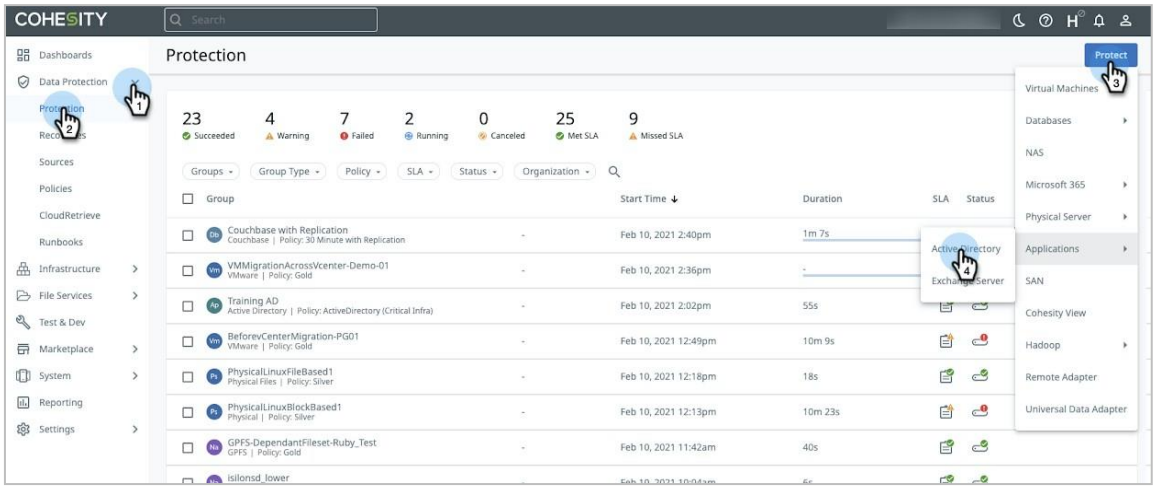
Automation is the only way to stay ahead of the demand for backups and data management. In Cohesity, Protection Groups combine operational requirements (which objects to protect, indexing, alerts, exclusions, inclusions, etc.) with the business requirements that are defined in a Protection Policy (scheduling, retention, etc.). Multiple Protection Groups can use the same Protection Policy, but each Group can have only one Policy. For more, see About Policies and Protection Groups in the online Help.

Automate your Active Directory backups by building a Protection Group and assigning the AD host you registered earlier and applying the Protection Policy that meets your business requirements.

NOTE: Because Active Directory services can be implemented across multiple hosts, or can be part of a larger domain tree or forest, it's important that you identify all the Active Directory hosts so that they can be included in your Protection Group.

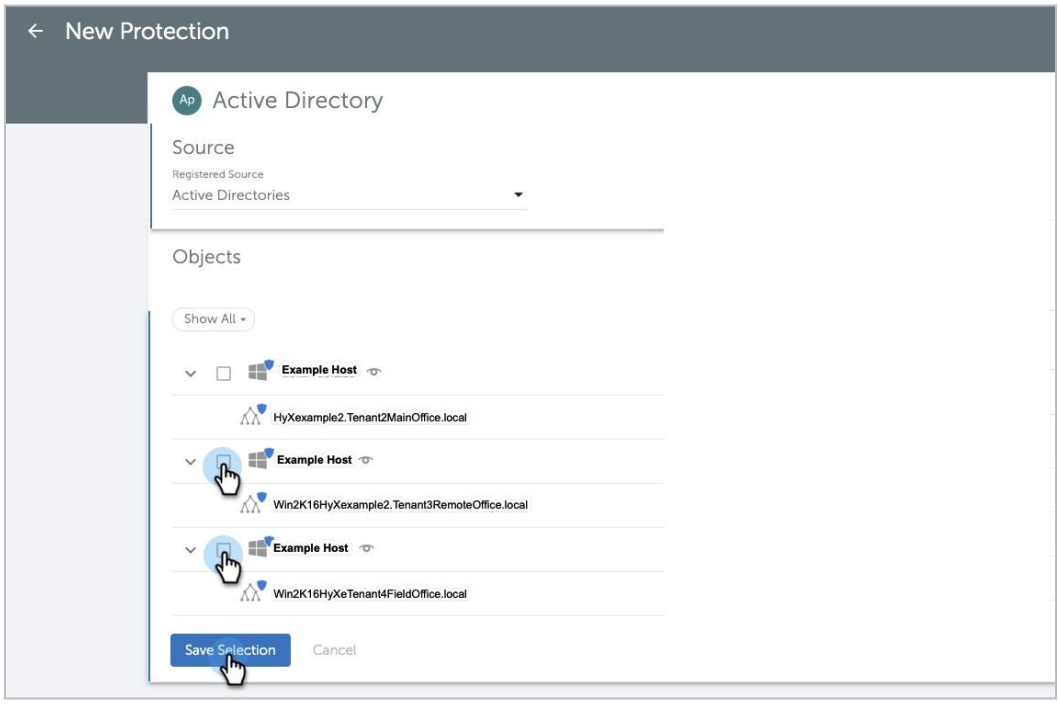
To create a Protection Group:

1. Log in to Cohesity and navigate to **Data Protection** > **Protection**. Then click **Protect** and select **Applications** > **Active Directory**.

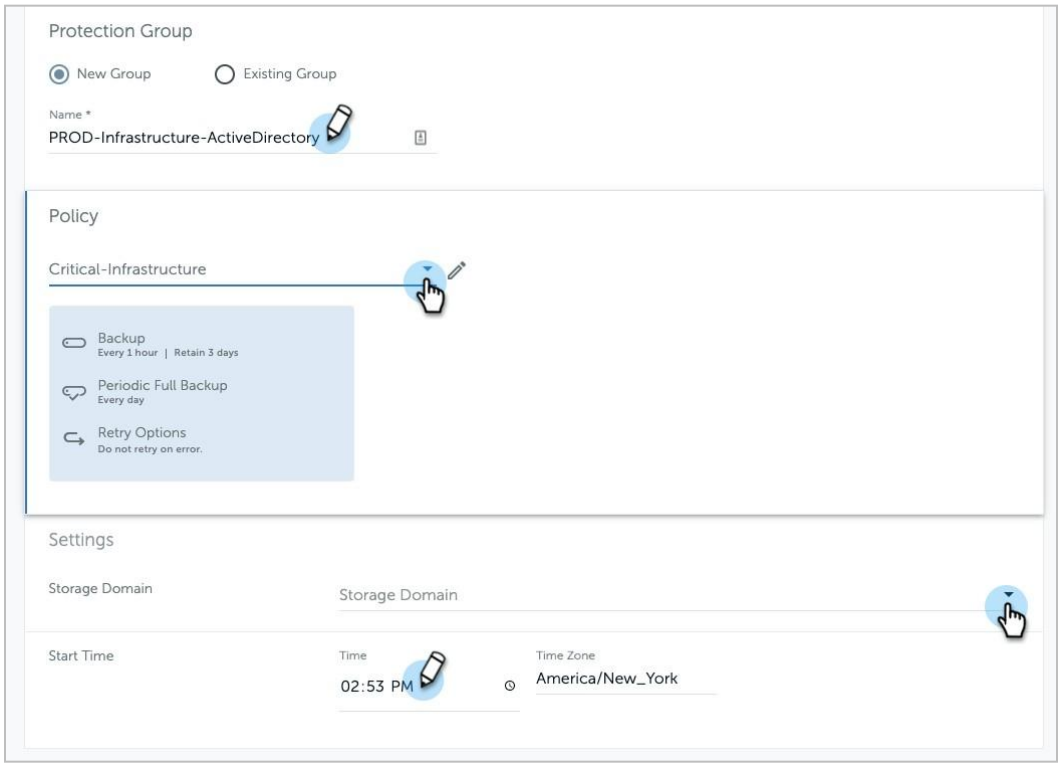


TIP: You can add or remove more AD sources to the Protection Group later if you like. In this way, you can build onto the Protection Group to manage all your Active Directory servers.

2. In the **New Protection** form, under **Source**, select the AD host(s) you registered earlier, and click **Save Selection**.



3. In the same form, enter a Protection Group **Name** and select the appropriate **Policy**. Under **Settings**, select the **Storage Domain** and set the **Start Time**.



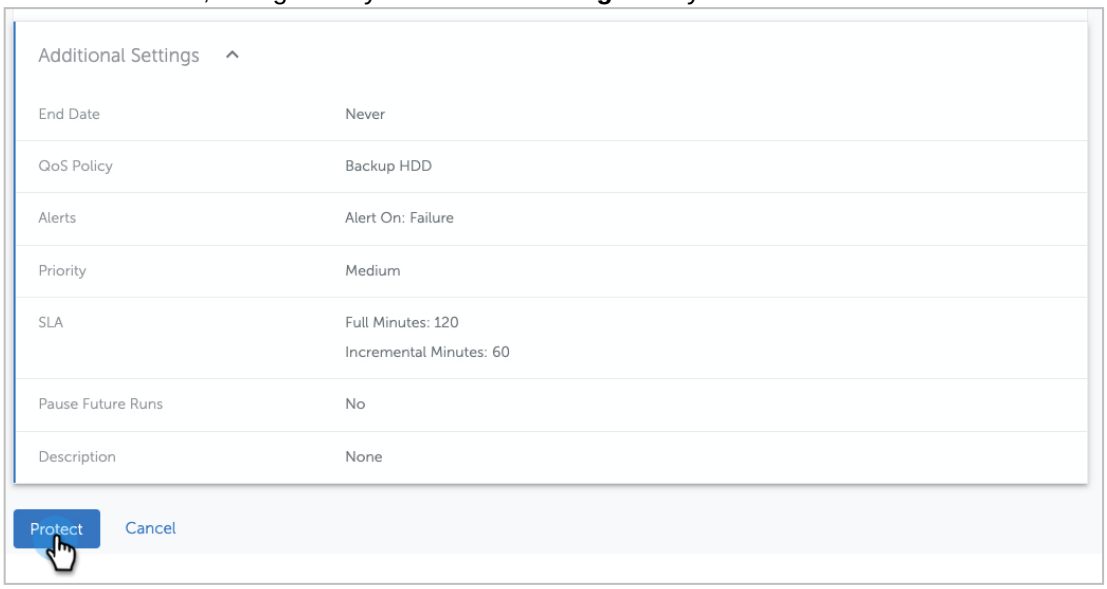
TIPS:

- Give your Protection Group a descriptive name that identifies the kind of data being protected and how it is managed. This will help you identify and manage your AD backups as your environment grows. Use descriptors like: production (PROD), critical, infrastructure (INFRA), financial, sales, primary, secondary, and employees (EMP). For example:

Production_ActiveDirectory	DataCenter_Dallas_Production
Critical_Infrastructure	Production_ReplicatedTo_DRsite
Archive_LongRetention	Development_User_Data

- Once you set the Policy for a Protection Group, all the sources assigned to that Protection Group will be conveniently managed the same way.
- To create a custom Protection Policy to meet specific scheduling, retry options, log backup, replication, and archiving needs, learn how to Create or Edit a Standard Policy in the online Help.
- For maximum space savings and security, choose a Storage Domain with compression, deduplication, and encryption enabled. For details, see Create or Edit Storage Domains in the online Help.

4. In the same form, configure any **Additional Settings** that you need to and then click **Protect**.



NOTE: For details on the **Additional Settings**, see Create an AD Protection Group in the online Help.

Your new AD Protection Group is now active and running and appears on the **Protection** page. For more on optimizing your protection, see Cohesity Best Practices for AD Protection below.

Now that you have created a Protection Group for your Active Directory, you can add other Active Directory sources, or change the Protection Policy and settings. In this way, all your Active Directory sources in this Protection Group will be managed the same way. For example, to replicate all the backups to an off-site target, simply add replication to the Policy that is assigned to this Protection Group.

TIP: In larger environments, build two or three different Protection Groups with different configurations to manage several Active Directory hosts. This helps keep your data management simpler even as your environment grows.

Recover Active Directory Objects

"A needle in a haystack" **—** Try finding the erased email address for an employee among a thousand other employees in Active Directory. This is not an unusual request for an Active Directory administrator. It is often like looking for a needle in a haystack.

How does it work with Cohesity? Once you have started protecting your AD data in Cohesity, you select the backup to restore and Cohesity presents it to the Active Directory host as a mount. Then the contents of the mount are brought up under an Active Directory service, enabling the administrator to do a side-by-side comparison of the contents in the backup against the live AD service. This allows the administrator to locate the missing email, or any other information that has been modified or deleted from the live AD service, quickly.

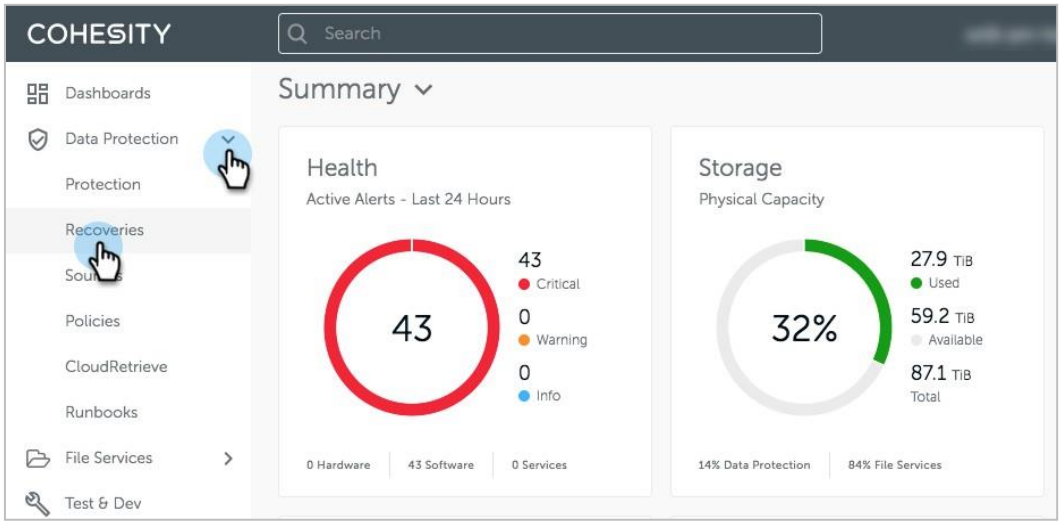
In Cohesity, the sequence of recovery events is simple:

1. Cohesity performs an Instant Volume Mount of your AD backup.
2. Cohesity instructs the Cohesity Windows Agent to stand up the AD backup alongside current, live AD, using an `NTDS.dit` file (which contains all the AD data) from the Instant Volume Mount.
3. You view a side-by-side comparison of the AD backup against the live AD objects.
4. You select the objects to recover and recover them.

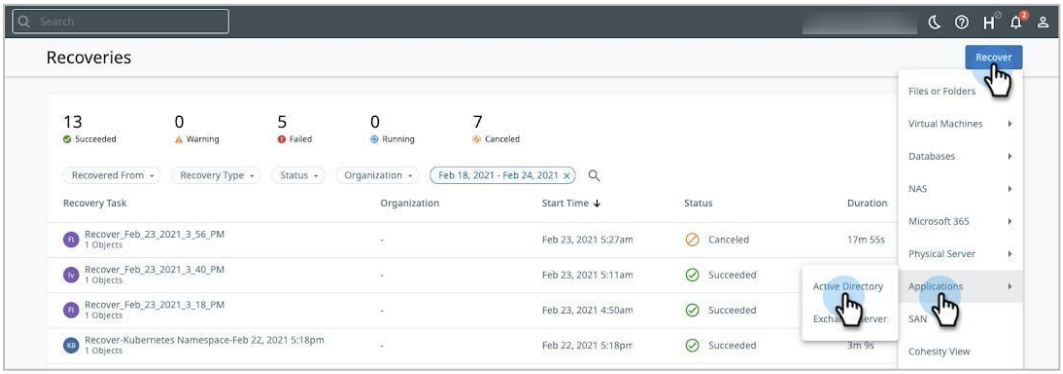
TIP: If they choose to, advanced Active Directory administrators can access this Instant Volume Mount to run their own scripts and perform their own search.

To recover Active Directory objects:

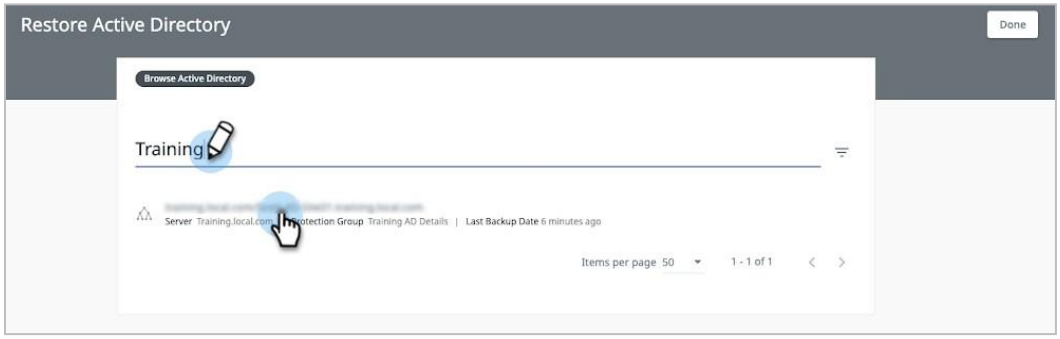
1. Log in to Cohesity and navigate to **Data Protection > Recoveries**.



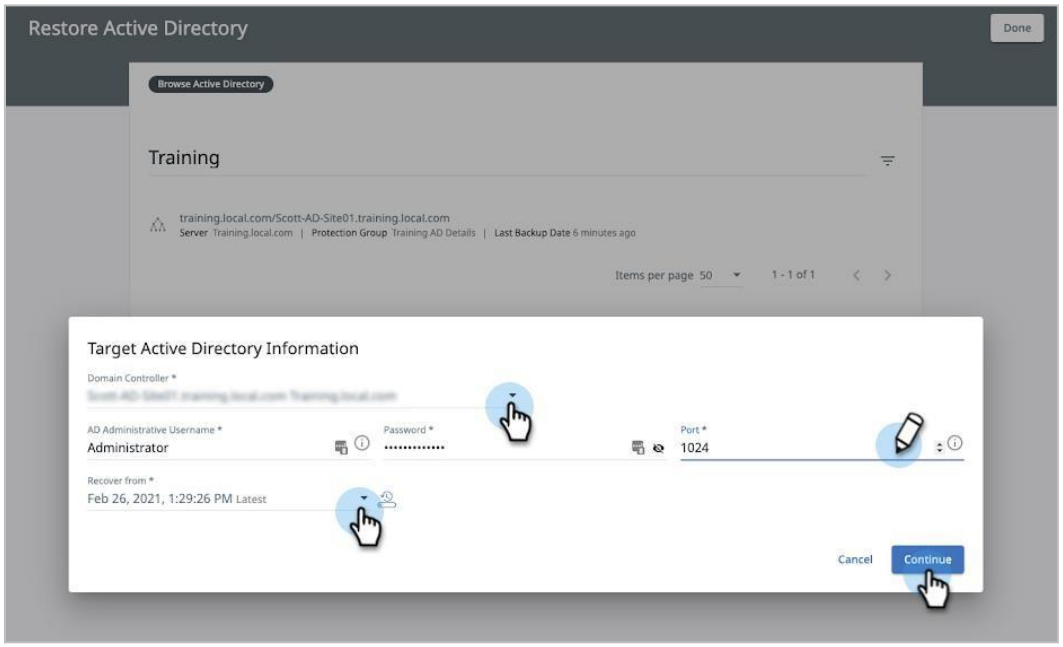
2. On the **Recoveries** page, click the **Protect** and select **Active Directory**.



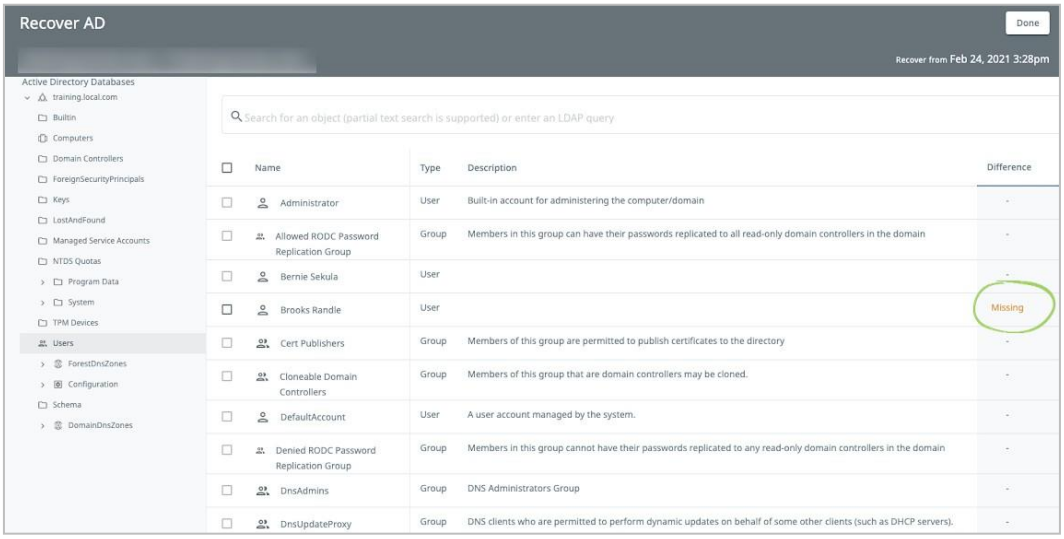
3. In the **Restore Active Directory** form, enter a search term to locate your protected AD. When you do, click it.



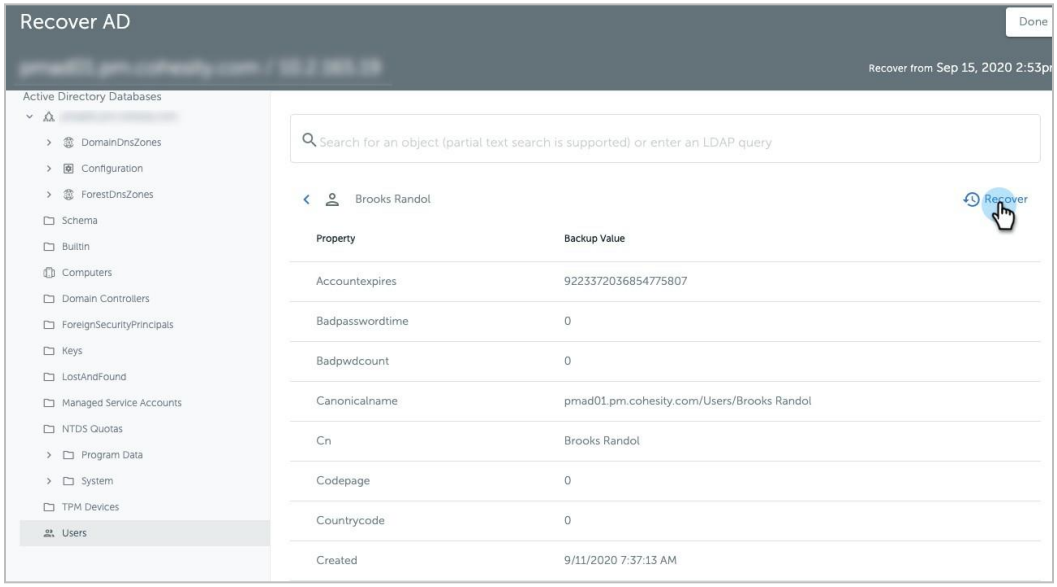
4. In **Target Active Directory Information**, select the target **Domain Controller** and enter the **AD Administrative Username** and **Password** that you need to mount the snapshot on the target host, and the **Port** number (defaults to port 1024 otherwise). If you need a different snapshot (point in time), click the snapshot listed under **Recover from** to select an earlier snapshot. Click **Continue**.



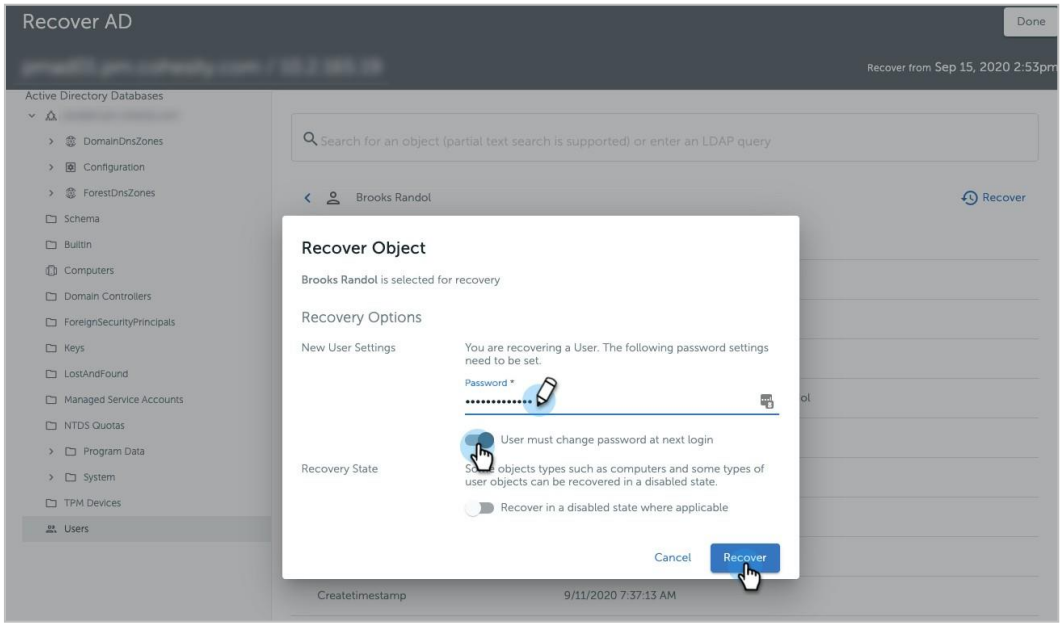
5. In the **Recover AD** comparison list, locate the missing or changed objects under **Difference**. Click into an object to explore its details.



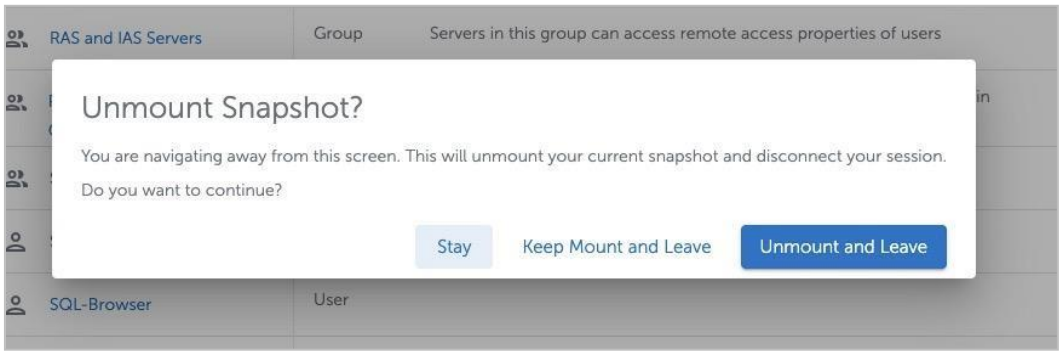
6. Examine the object's details. If it's an object you need, click **Recover**.



7. Configure any additional **Recovery Options** (like **New User Settings** and **Recovery State** in this example) for the object and then click **Recover**.



8. Next, click:
   - **Stay** to recover more objects.
   - **Keep Mount and Leave** to be able to resume the granular recovery later.
   - **Unmount and Leave** to remove the snapshot from the host.



Upgrade Your Disaster Recovery Preparedness

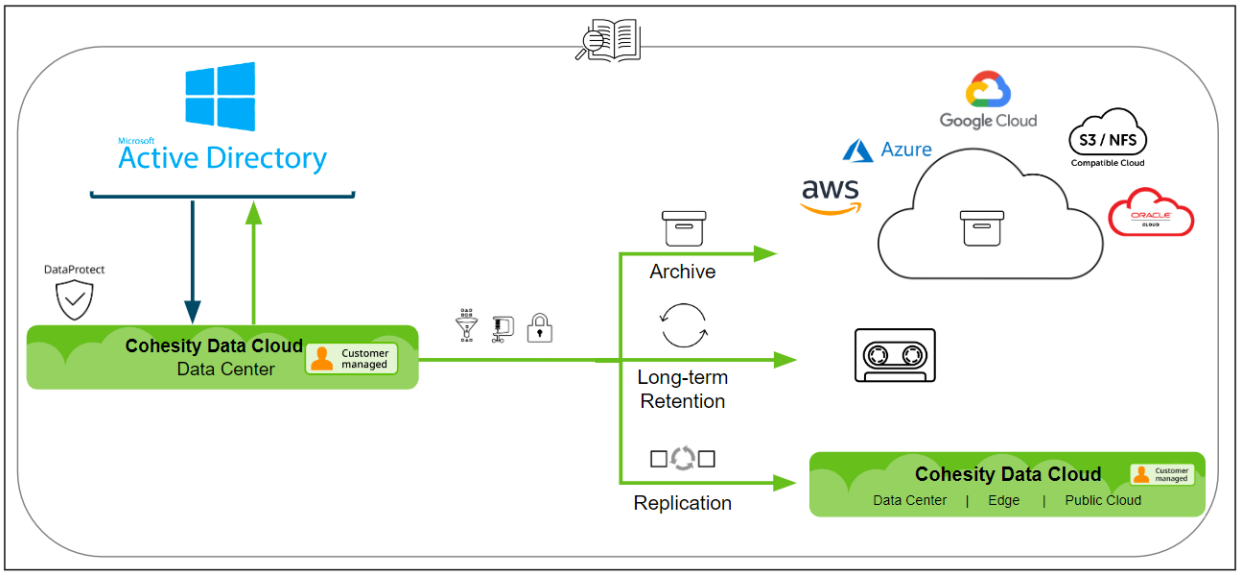
Disaster Recovery (DR) and business continuity are closely related plans designed to proactively protect a business's infrastructure and data. Taking an AD backup is only one part of protecting your business; you must also protect the data from corruption and catastrophic disaster. You can achieve this by keeping a series of backups replicating those backups off-site and archiving them under a long-term retention plan.

Cohesity gives you the foundation to build a DR plan to protect your business:

- **Capture and Store**. Protect your Active Directory from loss and corruption with regularly scheduled backups.
- **Geo-redundancy**. Replicate your AD backups to an off-site location to protect from catastrophic loss and disaster.
- **Cost-effective Archival**. Archive your AD backups to the cloud and store them on lower-cost storage tiers for long-term retention.

Use a Protection Group to schedule regular AD backups and assign a Protection Policy to include archiving and replicating those backups for long-term retention and disaster recovery.

Figure 4: Active Directory Backups in Cohesity are Available to Replicate and Archive



Take Local Snapshots

Protect your AD backups over time by maintaining a series of local Cohesity snapshots.

Use Cohesity Protection Groups to schedule and automate AD backup management.

Replicate Backups Off-Site

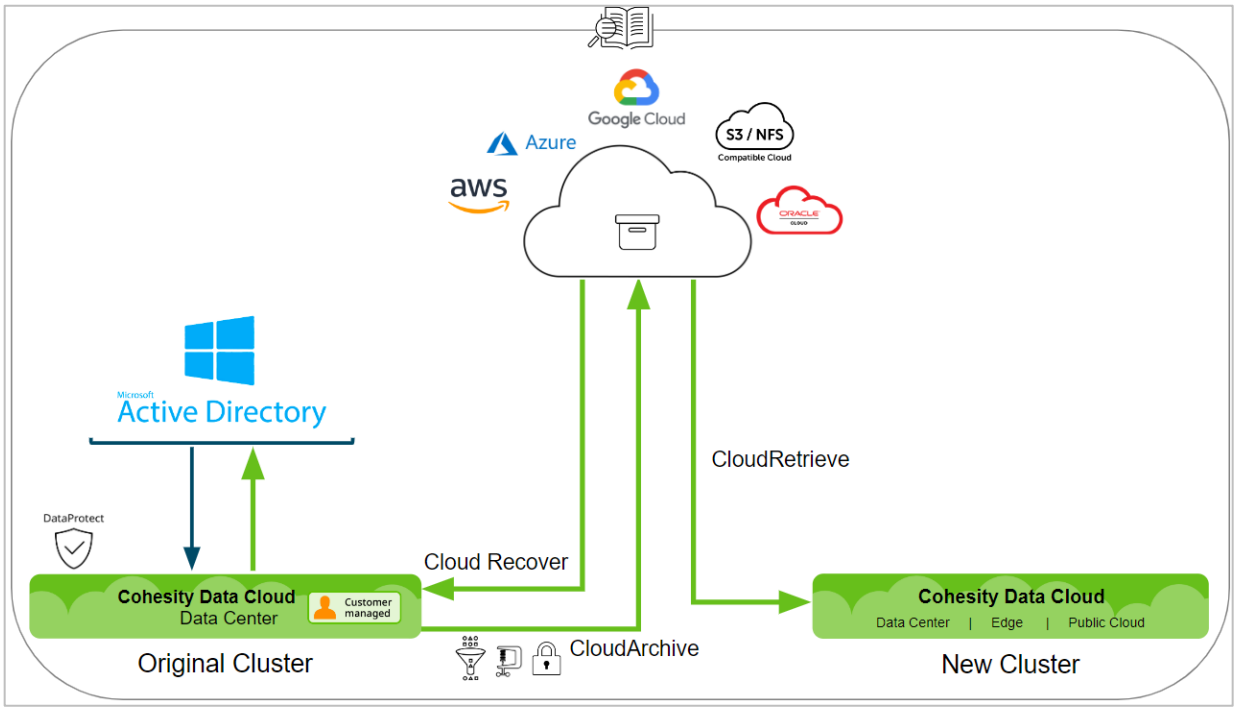
Protect your entire set of AD backups from catastrophic loss by replicating your AD backups to an off-site location. Choose a Protection Policy for your Protection Group that automatically copies the AD backups to a second, off-site Cohesity cluster. By default, source-side deduplication and compression are enabled for replication, so that Cohesity sends *only the changed data* over the network, producing a significant reduction in network traffic and cost.

Archive Backups to the Cloud

Archive your AD backups to the cloud as a way to address long-term data retention requirements and simultaneously lower the cost of storage. Cohesity provides a policy-based method to archive to public clouds (AWS, Azure, and GCP), as well as to any S3-compatible storage.

With Cohesity CloudArchive, Cloud Recover, and CloudRetrieve, your AD backups are available for recovery to their original Cohesity cluster or onto a different Cohesity cluster, for geo-redundancy and disaster recovery.

Figure 5: Cohesity CloudArchive, Cloud Recover, and CloudRetrieve Provide Disaster Recovery



Cohesity Best Practices for AD Protection

Configuring the right Cohesity settings dramatically improves the performance of your backups, and the efficiency of your storage and archives. Manage your backups by choosing the optimal settings for deduplication, compression, and encryption.

- **Use inline deduplication**. *Deduplication* (enabled by default) prevents duplicate blocks of repeated data from being stored, dramatically reducing your storage consumption.

  With *inline deduplication*, the process occurs as Cohesity is saving the blocks, instead of waiting until *after* Cohesity has written the data to its Storage Domain. We recommend that you use deduplication and wherever possible, enable inline deduplication.

- **Use inline compression**. Compressing your data significantly reduces the space needed to store your backups and frees up space for more backups and other important data.

  With inline compression, the process occurs as Cohesity is saving the blocks, instead of waiting until *after* Cohesity has written the data to its Storage Domain. Both compression and inline compression are enabled by default, and we recommend that you take advantage of them. For details, see Create or Edit Storage Domains in the online Help.

- **Use encryption**. When a platform governs access to data across the systems in your environment, it is crucial to protect the data it manages. We recommend that you enable encryption — at rest, in flight, and in the cloud — for all your Active Directory backups. For more, see Cohesity Security Features in the online Help.

- **Keep multiple snapshots to guard against corruption**. We recommend you maintain five to seven local snapshots of your backups.

  When you capture and store your backups like this, you protect your data from corruption over time. By taking and maintaining several snapshots, you are in position to recover data from its state *prior* to being corrupted. Snapshots are efficient because they capture just the changed blocks of data, and then use deduplication and compression.

  We recommend protecting all your Active Directory servers with regularly scheduled backups, and then in turn moving some of those backups off-site and archiving them under a long-term retention plan for disaster recovery.

- **Protect all domain controllers that have FSMO roles**. Should you experience a role failover, this helps ensure that a backup (snapshot) is available even if a backup domain controller (DC) becomes primary at some point.

- **Protect high-latency AD sites individually**. If you have two AD sites with high latency between them, it might be better to protect each site so that you are protecting latent or out-of-sync data.

- **Validate the backups**. We recommend a periodic restore of Active Directory objects in a test environment from its backup. This is an important step in the overall backup strategy because it tests, verifies, and validates the integrity of the backup. Restore a sample from the snapshot set to a non-production server and evaluate it. In addition to confirming that the right data is backed up properly, this practice also ensures that you have already validated your method of restoring objects *before* a critical event necessitates it.

- **Verify logging and auditing operations**. It is very important to log and audit changes on an Active Directory server. Cohesity logs its recovery process as it mounts the snapshot and works to present

the saved Active Directory data. In Cohesity, navigate to **Data Protection > Recoveries** and click into your AD recovery task to view detailed logs.

- **Shelter in the cloud**. We recommend archiving to the cloud for low-cost, long-term storage and protection from regional disasters.

  Cohesity provides a policy-based method to archive to public clouds (AWS, Azure, Google Cloud Platform) or any S3-compatible storage. This makes it easy to change policies, meet regulatory requirements, and retrieve your data to different geographical locations.

- **Use replication to defend against site disaster loss**. Protect your entire set of Active Directory backups from catastrophic loss by replicating them to a different geographical site. Cohesity can automatically replicate the Active Directory backups stored in the Cohesity cluster to a second, off-site Cohesity cluster.

  Cohesity replication always performs source-side deduplication and compression first and sends only the changed data over the network for cost-effective disaster recovery. As such, Cohesity replication is an essential part of every disaster recovery (DR) plan.

- **Be prepared *before* disaster hits with a DR plan**. One of the best things you can do to protect your Active Directory is to include it when you create your DR plans.

Appendix A: Terminology

There are several concepts and terms that are important to understand as you learn how to take advantage of all of Cohesity's features for Active Directory protection.

- **Protection Group**. A collection of objects from your registered sources that share a recurring backup schedule of Protection Runs. Use a Protection Group to identify which Active Directories to protect. When you create a Protection Group, you associate it with a Cohesity Protection Policy.
- **Protection Policy**. A reusable collection of settings that define how and when objects are backed up, replicated, and archived.
- **Cohesity Replication**. Replication automatically makes copies of snapshots captured by Protection Runs on one Cohesity cluster and puts the copies on a second Cohesity cluster.
- **Domain Controller**. Active Directory's logical structure is built around the concept of domains. A domain *controller* (DC) can be authoritative for one and *only one* domain.

  This is the most common implementation of Active Directory.
- **Domain Tree**. A domain *tree* is a hierarchy of several domains.

  All the domains in the domain tree trust one another implicitly with *transitive trusts* — that is, the America domain trusts the Asia and Europe domains, therefore Asia trusts Europe also.

  Put simply, the administrator of asia.mycorp.com can allow any user in the entire domain tree (Asia, America, or Europe) access to any of the resources in the Asia domain that the administrator wishes.
- **Domain Forest**. Where a domain tree is a collection of domains, a domain *forest* is a collection of one or more domain trees.

  A forest trust allows an administrator to create a single transitive one-way or two-way trust between two root domains. This allows all the domains in one forest to trust all the domains in another forest, and vice versa.
- **Primary Domain Controller (PDC)**. Controls all access to the enterprise and manages access to other domains in your organization.
- **Backup Domain Controller (BDC)**. Controls the host(s) where backups are stored. Many times, this is read-only.
- **Flexible Single Master Operation (FSMO)**. FSMO roles prevent conflicts in an Active Directory and, at the same time, give you the flexibility to handle different operations within the same Active Directory.

Appendix B: Product Documentation

Review our Active Directory product documentation for in-depth details:

- 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.

Other essential contributors included:

- Bart Abicht, Senior Technology Writer and Editor at Cohesity

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.2	July 2024	Republishing
1.1	Feb 2023	Rebranding updates
1.0	Feb 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.