TrueNAS + HYCU®
Immutability Solution Guide

Introduction

TrueNAS Enterprise systems can be deployed as an immutable backup target for HYCU data protection workflows. Immutability is a capability of HYCU backup platforms (in combination with suitably configured storage systems) that prevents backup data from being modified or deleted for a user-defined retention period. This protects your backup data from threats such as ransomware, malicious insider actions, or accidental deletion.

What's Required to Configure TrueNAS + HYCU Immutability

Below is a summary of what needs to be in place on the TrueNAS side, and what configuration is required in HYCU.

TrueNAS Side

1. Ensure you are running TrueNAS Enterprise with support for S3-compatible object storage with an appropriate license for VM & Apps.
2. On TrueNAS, deploy the S3 compatible service - for example, the MinIO App.
3. Create the bucket for HYCU with both Versioning and Object Locking enabled.
4. Secure the TrueNAS appliance: enable strong access controls, separate networks for backup traffic, ensure TLS certs, isolate the object endpoint, and maintain audit logs. See Security Recommendations on docs.truenas.com for more information

HYCU Side

1. In HYCU's console, configure a backup target pointing to the TrueNAS object storage endpoint. Provide the service endpoint, credentials, region, certificate (if self-signed), etc.
2. In the HYCU policy/target settings, enable the immutability/WORM retention mode (if supported) and set the "immutable retention period" (e.g., 30/60/90 days).
3. Confirm that HYCU sees the storage target as supporting immutability (object-lock enabled).
4. Create or modify backup jobs to write to that target. HYCU will then land the data into the immutable area, and enforce the retention/lock window.
5. Test restore operations from the immutable target to verify full chain recoverability.
6. Test deletion operations to ensure that they fail as designed.

Configuring TrueNAS (S3-Compatible Object Storage)

1. On the TrueNAS appliance, install and activate the MinIO App per the TrueNAS documentation.
2. Create a storage bucket in MinIO for the HYCU target. When creating the bucket, enable **Versioning**, **Object Lock**, and **Retention** to "WORM" or "Compliance" mode and select the required retention period.
3. Ensure bucket permissions restrict deletion/modification of objects once locked.
4. On the HYCU side: in Targets → Add → S3 Compatible, provide the TrueNAS endpoint (IP:port or hostname), specify region, upload the CA certificate (if non-trusted), choose Direct or Gateway mode as appropriate.
5. Select the bucket in question, and enable "Immutable retention" or "Make recent backups immutable for X days" (terminology may vary).
6. Once configured, perform a HYCU backup job to this target, then review via TrueNAS that the objects are under the retention/lock period and cannot be removed until expiry.

Configuring HYCU for Immutability

1. From the HYCU dashboard, navigate to Backup Targets and add the TrueNAS S3 endpoint. Use credential access that has sufficient rights to write, list, and read, but limit deletion rights to protect the bucket.
2. In backup policy settings, enable “immutable retention” or “object-lock enabled” and specify the retention window (for example 30 days).
3. Schedule backup jobs to that target. HYCU will write the data into TrueNAS’s locked bucket.
4. Monitor dashboard/alerts to ensure HYCU reports successful writes and immutability status.
5. Periodically test restore from the immutable target to validate end-to-end recoverability and that the lock did not impede restores.

Why This Matters (Benefits)

Ransomware Defense: An immutable copy means attackers cannot encrypt or delete your backup landing zone until the retention period ends.

Accidental Deletion Protections: Human or operational mistakes cannot remove locked data prematurely.

Compliance & Audit: Many regulations (e.g., finance, healthcare) require unalterable backup retention or WORM-style storage.

Recovery Confidence: With HYCU + TrueNAS immutability you bolster the backup chain integrity and can confidently restore clean data even after a breach.

Example Use Case

- A customer has 200 VMs (each 1 TB) and uses HYCU to back them up daily to a TrueNAS-based object store.
- They configure the bucket with a 90 day immutability window.
- Each day, HYCU writes ~1.2 TB of data to the TrueNAS MinIO bucket. Objects written are locked and cannot be deleted/modified for 90 days.
- Even if their primary infrastructure is compromised by ransomware on Day 35, they still have 35 days of clean backups locked and fully recoverable.
- After Day 90 elapses for a given object, it becomes eligible for deletion per the retention policy. Until that time, the WORM lock enforces immutability.

Best Practices and Considerations

- Use Pull rather than push replication when possible (i.e., backup target cannot initiate inbound connections) to reduce attack surface.
- Isolate the backup endpoint network (dedicated VLAN, firewall rules) so that only HYCU writes are permitted.
- Use strong IAM/Access keys with least privilege for bucket write operations—do not use root-level keys.
- Regularly test restore operations to validate the immutable target can actually restore the backup data when needed.
- Monitor expiration of immutability windows and ensure retained data volumes align with capacity planning.
- Factor in capacity, throughput, and retention duration when sizing your TrueNAS appliance (pool size, number of nodes in cluster, etc).
- Educate operations team on the difference between “locked” (immutable) and “deleted/expired” states for data objects.

Summary

Combining TrueNAS Enterprise (as an object target) with HYCU’s immutability-capable backup workflow delivers a robust ransomware-resistant, compliance-friendly backup landing zone. With correct configuration of object lock retention on TrueNAS, and HYCU policies pointing to that target, you ensure that your backup chain is locked for a defined period, thwarting deletion or modification by attackers or mis-operation.