Veracity Admin Guide

Chapter 1

Administration

Topics:

Installing Cloud Backup

Install on cloud platforms.

These steps are intended for administrators only.

1. Log into the cloud console at .
2. Navigate to the Backup section and select version .
3. Click **Install** and follow the prompts to complete setup.

   Tip: If you're not an administrator, please contact your IT team to perform the installation.

Installing On-Prem Backup

Install on on-premises systems for secure local backups.

Choose the appropriate procedure based on your operating system.

1. Download the Windows installer from .
2. Double-click the downloaded `.exe` file to launch the installer.
3. Follow the installation wizard and select a local backup destination.
4. Download the Linux installer package (.rpm or .deb) from .
5. Open a terminal and run:

   ```
   sudo dpkg -i veracity-agent.deb
   ```

6. Start the backup service with:

   ```
   sudo systemctl start veracity-agent
   ```

Tip: Ensure your firewall settings allow port 443 for secure agent communication.

Configuring Retention Policies

Set data retention periods to match your compliance and storage needs.

Retention policies determine how long backup data is stored before being purged.

As an **Enterprise** user, you can create granular retention rules by workload, location, or policy tag.

In the **Standard** edition, you can choose from predefined policies: *30 Days*, *90 Days*, or *1 Year*.

1. Log in to the admin dashboard.
2. Navigate to **Policies** > **Retention**.
3. Click **Create New Policy** and define scope, duration, and deletion rules.

   Select one of the predefined retention options and click **Apply**.
4. Click **Save** to finalize your changes.

Important: Retention settings directly impact your storage usage and compliance posture.

Managing Users and Roles

Control access to by managing user accounts and permissions.

Only users with administrative privileges can manage accounts and assign roles in .

1. Log in to the admin console.

2. Navigate to **Settings** > **User Management**.
3. Click **Add User** and enter the user's details.
4. Select a role such as *Backup Operator*, *Auditor*, or *Administrator*.
5. Click **Save** to apply changes.

CAUTION: Assigning Administrator roles grants full access to all system settings. Use with caution.

Monitoring Backup Jobs

Track the status of active and completed backup operations in .

Use the **Cloud Dashboard** to monitor job activity in real time. Navigate to and log in to your administrator account.

Use the **On-Prem Monitor** from your local management console. Access it from the Control Panel.

1. Go to **Job Monitor** in the main navigation.
2. Filter jobs by status: *Running*, *Completed*, or *Failed*.
3. Click on a job to view detailed logs and resource usage.

Note: Both platforms allow exporting job logs for troubleshooting or auditing purposes.

Chapter 2

Knox Recovery Feature

Topics:

Installing Knox Recovery

Steps to Install

1. Download the latest Knox installer from Veracity Downloads.
2. Run the installer using the following command:

```
sudo ./install-knox.sh
```

3. Review the following settings before proceeding:

Field	Description	Default Value
Port	Port Knox listens on	9443
Data Directory	Location for backup metadata	/var/knox
Enable Logs	Whether to enable debug logging	true

Knox Compatibility and Support Matrix

Hardware Compatibility

The following table is updated from the latest NIC Compatibility Matrix:

NIC Model	Supported OS	Notes
Intel X520	RHEL 8, Ubuntu 22	Requires firmware upgrade
Broadcom 57810	Windows Server 2022	Tested with driver v2.14

This table is maintained as a shared reference. Copy and paste from GDocs is supported.

Advanced Knox Configuration

Configure Multi-node Deployment

1. Setup the primary Knox node.
2. Configure secondary nodes:
   - Set static IP address for each node.
   - Verify cluster synchronization:
     - Run: `knox-cluster status`
     - Confirm output shows "All nodes synced"
3. Apply the configuration to all nodes.

   Tip: Ensure all nodes are on the same firmware version.

Knox Version and Edition-Specific Notes

Feature Behavior by Version

:::dita

Self-managed deployments require manual key rotation every 90 days.

SaaS version handles key rotation automatically via the Knox Control Plane.

Advanced recovery scripts are available for Linux admins only.

Some features may be unavailable on Windows desktop clients.

Reusing Knox Procedures and Snippets

Adding Active Directory as a Source

To add Active Directory:

```
knox-auth add-ad --domain corp.local --admin user1

See [Mount ISO Procedure](../shared/mount-iso.md)
```