Nexsan VHR Appliance
+
Veeam Integration v13



Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

Contents

Document Information 3
Vendor Recommended Configuration 3
Nexsan Support 3
Stage One: Nexsan VHR Unpack, Connect, Power-on 4
1. Pre-Unpacking Safety Checks 4
2. Unpacking the Nexsan VHR 4
3. Rack Mounting 4
4. Power Connectivity 5
5. IPMI / BMC Out-of-Band Connectivity 5
6. Core Network Connectivity 6
7. Power-on Nexsan VHR and Configure 7
Stage Two: Veeam Host, Backup, Replication 10
1. Sign in to Veeam Host Management 10
2. Integrate Nexsan VHR into Veeam Backup v13 12
3. Authorise SSH request as Security Officer 13
4. Veeam Backup & Replication Management 14
5. Assigning the Backup Repository role 17

Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

Document Information

Alliance Partner	NEXSAN
Alliance Product	NEXSAN VHR Appliance Integration into Veeam
Program Category	Veeam Ready – Appliance
Category Description	User guide
Article ID	NEXSAN VHR & VEEAM BACKUP INTERGRATION
Features and attributes	Hardened repository Immutability Integration
Publication Date	31st March 2026
Part number	P0450195 rev A
Product details	NEXSAN VHR Appliance
Product name and Version	NEXSAN VHR Appliance + Veeam Integration v13

Vendor Recommended Configuration

Readers are strongly advised to have a basic level of hands-on experience in administering Veeam Backup.

IMPORTANT: After unpacking the Nexsan VHR and installing it in the designated location, please ensure that all steps in Stage One are fully completed before proceeding to the integration workflow in Stage Two.

Nexsan Support

Global:

- Web: Nexsan.com/support
- Email: support@nexsan.com

UK Office:

- Phone: +44 (0)1332 596 900
- Email: support@nexsan.com

North America Office:

- Toll-free: +1 866-263-9726
- Phone: +1 760-690-1111
- Email: support@nexsan.com

Nexsan® and the Nexsan logo are trademarks or registered trademarks of Nexsan. All other trademarks and registered trademarks are the property of their respective owners.

Stage One: Nexsan VHR Unpack, Connect, Power-on

1. Pre-Unpacking Safety Checks

Before opening the box, ensure the following:

A. Confirm the installation rack is ready:

- Adequate space (2U or as required)
- Front and rear access
- PDUs powered and reachable

B. Ensure at least **two people** are available for lifting—**the chassis is heavy**.

C. Inspect the packaging for visible damage before opening.

2. Unpacking the Nexsan VHR

A. Place the shipping box on a stable surface near the rack.

B. Use a knife or cutter to remove the packing tape—avoid cutting too deep.

C. Remove the top foam insert.

D. Remove accessories:

- Rail kit
- Power cables
- Screws & cage nuts
- Documentation / quick start cards

E. With two persons, lift the chassis out of the box using the side handles.

F. Place the chassis on a sturdy table or directly in front of the rack.

3. Rack Mounting

NOTE: Two-Person Lift Required

A. Install the Rails

a. Remove the VHR Server rail kit from the accessories box.

b. Install inner rails on the chassis sides.

c. Install outer rails in the rack:

d. Ensure both sides are level.

e. Lock each end securely with rack screws.

B. Slide the Unit into the Rack

a. With two people, lift the unit and align the inner rails with the outer rails.

b. Slide the chassis into the rack until it clicks or locks into place.

c. Use front panel locking screws to secure the unit.

Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

4. Power Connectivity

The Nexsan VHR system usually includes dual redundant power supplies.

A. Identify PSU1 and PSU2 on the rear.

B. Connect each PSU to separate PDUs for redundancy.

C. Avoid using the same power strip or UPS unless that UPS is redundant.

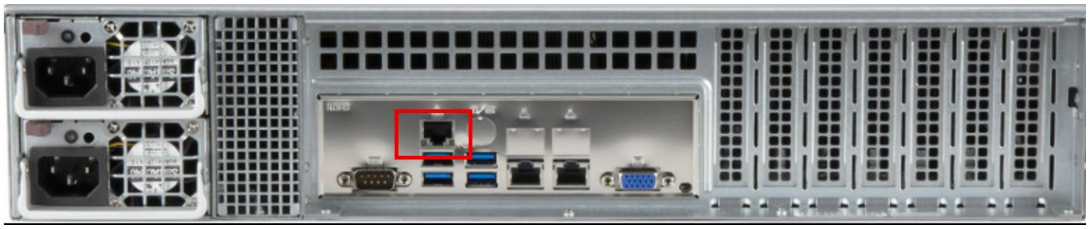
D. Confirm both PSU LEDs turn green once powered.

5. IPMI / BMC Out-of-Band Connectivity

The IPMI (Intelligent Platform Management Interface) port allows remote hardware management.

A. Identify the IPMI Port

This is usually a dedicated RJ45 port, often labelled IPMI or BMC.



B. Connect IPMI to Management Network

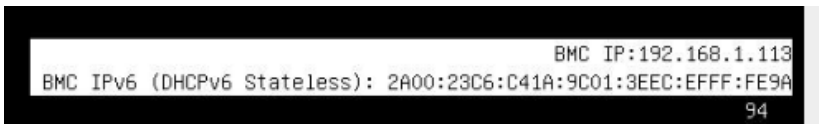
a. Use a standard Cat5e/6 cable.

b. Best practice, connect IPMI to the management VLAN or isolated admin network. Ensure the port is not exposed to public networks.

C. Locate the Default IPMI IP Address

BMC IP address appears in the bottom right during POST.

IP address located in 'IPMI > BMC Network Configuration' in the BIOS



User: ADMIN Password: CAN BE LOCATED ON THE FRONT PULL OUT TAB



Use your laptop/desktop with an IP in the same range to connect initially if required

D. Login and Configure Permanent IP

a. Open browser → http://IPMI-IP

b. Log in as ADMIN + “Password”

c. Go to Configuration → Network.

d. Set: i. Static IP address + Subnet mask

ii. Gateway + VLAN (optional)

e. Save and reboot BMC if prompted.

Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

6. Core Network Connectivity

Once the system is racked and powered, connect the primary network ports.

A. Identify NIC Ports

Nexsan VHR platforms typically include:

- 2 × 10GbE / 25GbE ports
- 2 × 1GbE ports
- Optional OCP or add-on NICs



B. Connect Production Network

Connect the 10/25GbE ports to your core switching fabric.

C. Verify Link Activity

Check:

a. Switchport link lights

b. NIC LEDs on the server

High-speed NICs must negotiate correctly (auto-negotiation enabled).

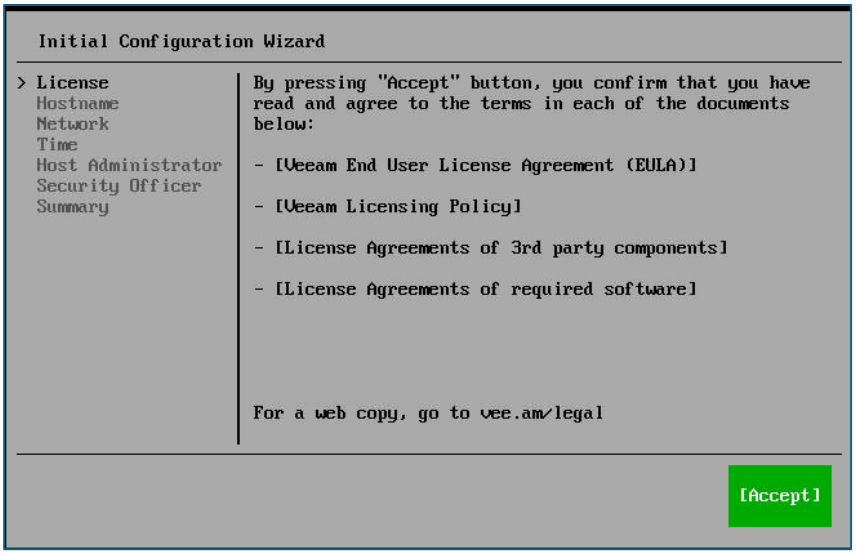
D. Readiness Confirmation

Once all above items are complete, you have completed Stage One.

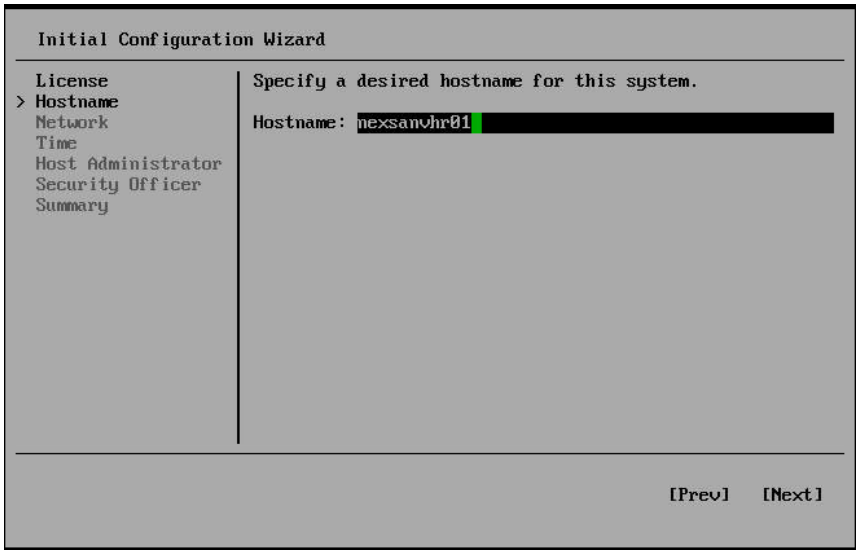
Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

7. Power-on Nexsan VHR and Configure

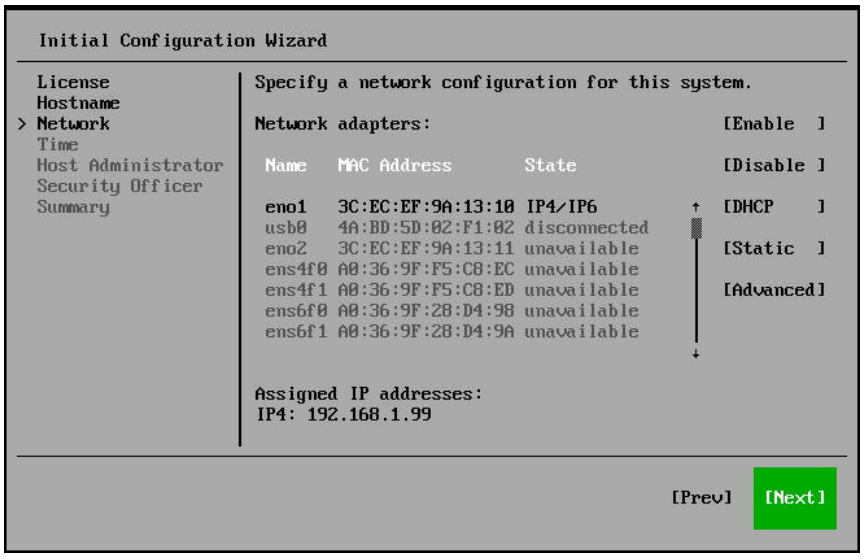
A. Read and **Accept** the **EULA**.



B. Enter your hostname, then select **Next**.

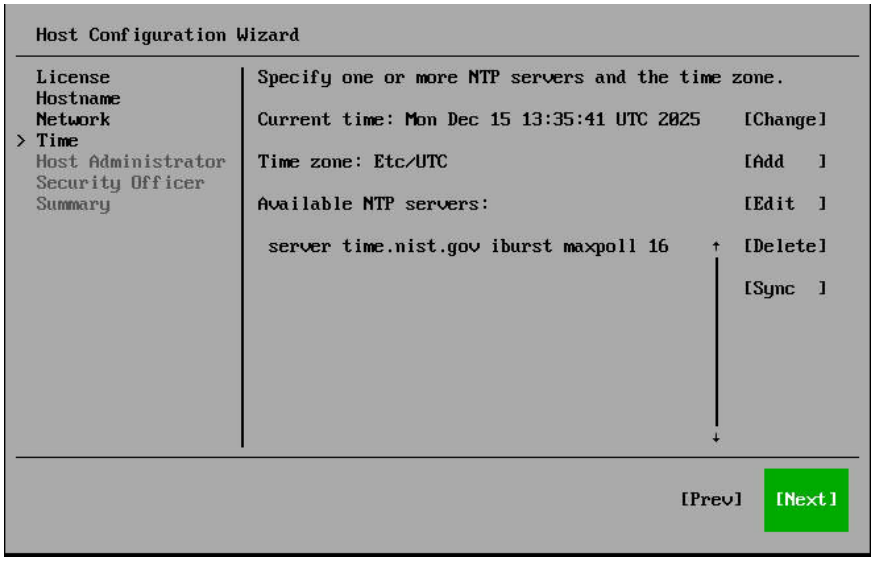


C. Set **Network** as required, then select **Next**.

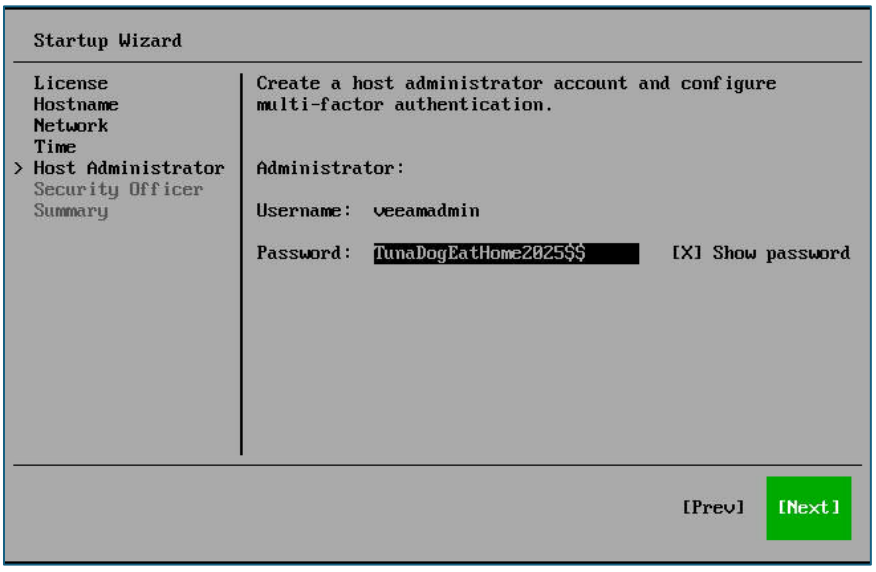


Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

D. Set **NTP** as required, then select **Next**.

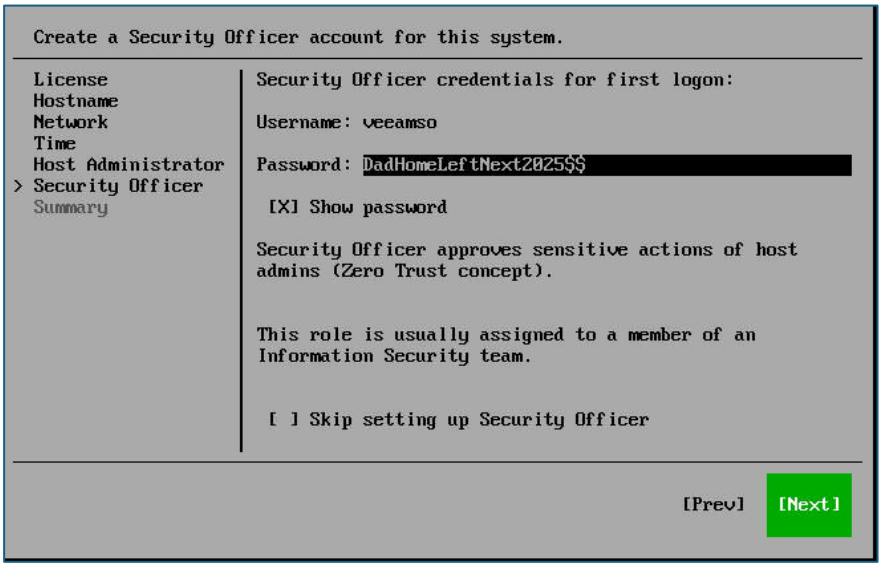


E. Configure the **veeamadmin** password, then select **Next**.



F. Set your MFA

Either follow onscreen instructions, or press Enter if the Show QR code option is selected.

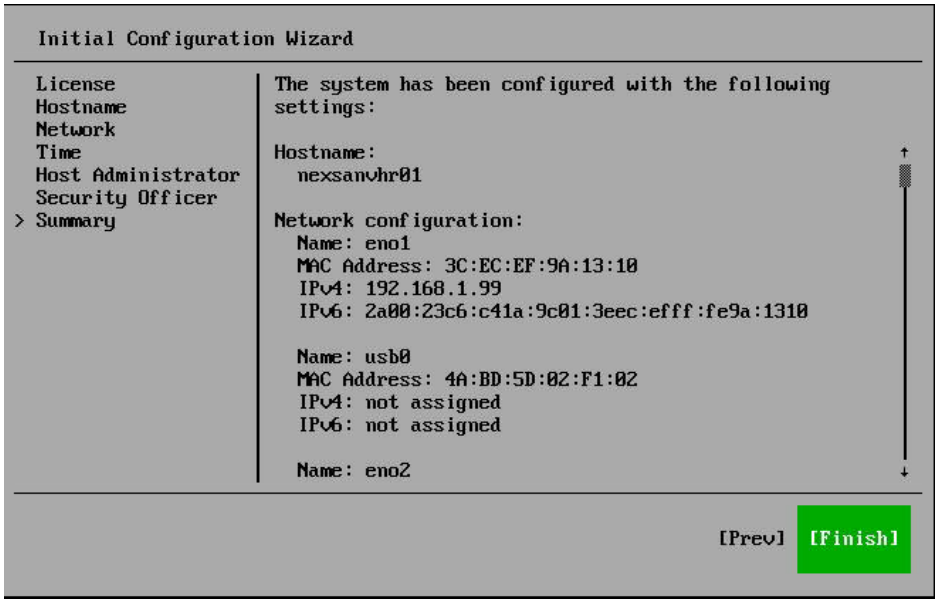


Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

G. Enter the code from your authenticator app and select **OK**.
Select **Next** to continue.

H. Enter the password for the **Security Officer**.
This account must be a different person to veeamadmin, providing an additional layer of protection for the VHR by enforcing the 4-eyes rule.
The **Security Officer role** is designed to ensure that no single administrator can make critical or destructive changes. Certain actions require approval from both veeamadmin and the Security Officer, significantly increasing security and preventing unauthorised modifications.

I. **Review** the setting and select **Finish.**



J. Select **OK** when the Security Officer prompt appears.



Stage One of the installation is complete.

Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

Stage Two: Veeam Host, Backup, Replication

1. Sign in to Veeam Host Management

NOTE: you are signing in as the Security Officer.

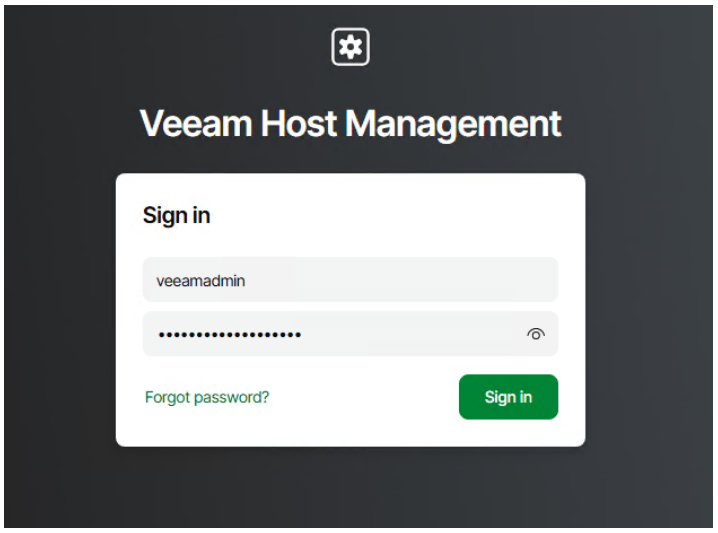
A. Open your Veeam Infrastructure Appliance http management page,

a. https://nexsanvhr01:10443

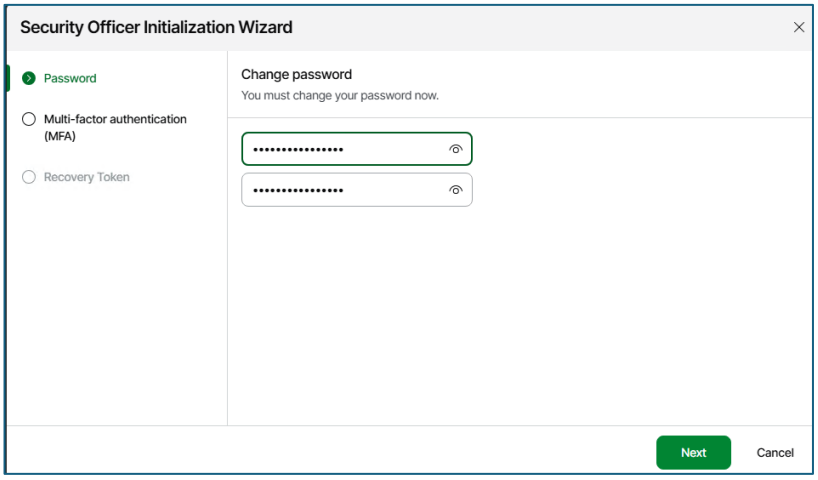
b. login with:

i. veeamso

ii. Password used

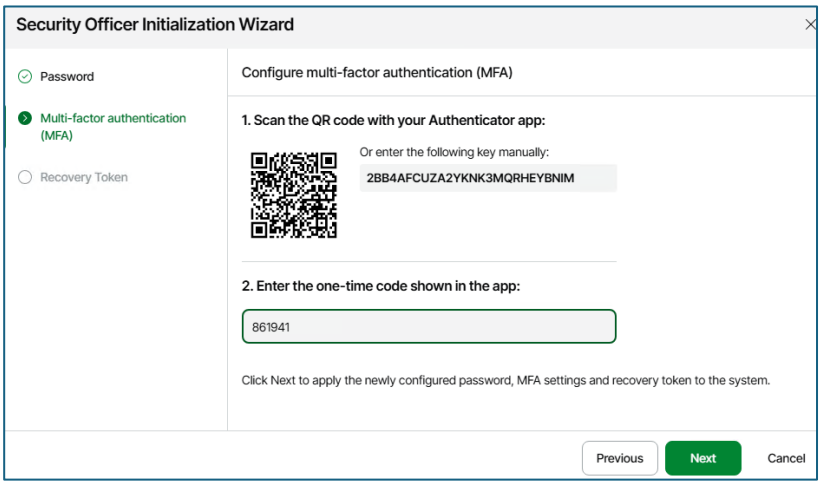


B. Change the password

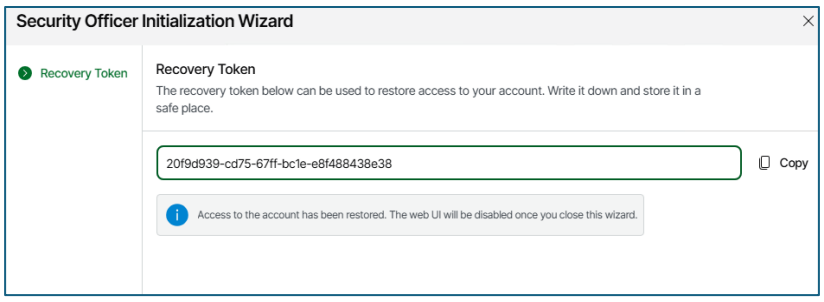


Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

C. Configure **MFA** for the Security Officer.



D. Save your **Recovery Token**.



NOTE

- Once the above Host Management steps (1. A - D) are complete, the **management console is disabled**.
- To re-enable the management console, you need to use the IPMI console and log in as veeamadmin, then turn access back on. The procedure is detailed in the following, step 2.

Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

2. Integrate Nexsan VHR into Veeam Backup v13

NOTE: All required settings must be configured before integration of Nexsan VHR into Veeam Backup.

Use the following procedure to temporarily enable SSH access for up to 8 hours:

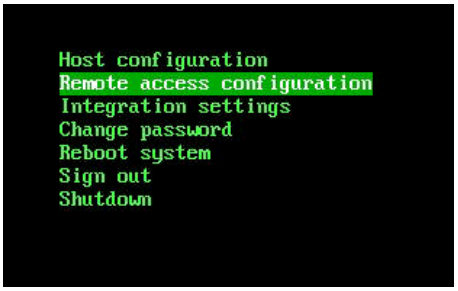
A. From the IPMI console, select **Sign In** from the bottom of the console screen.



B. Enter **veeamadmin** as Username, your Password, and your MFA code.



C. Select **Remote access configuration**.



D. Select **Enable SSH server**. Press **Enter** to request SSH access, status indicated **Awaiting Security Officer approval**..





Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

3. Authorise SSH request as Security Officer

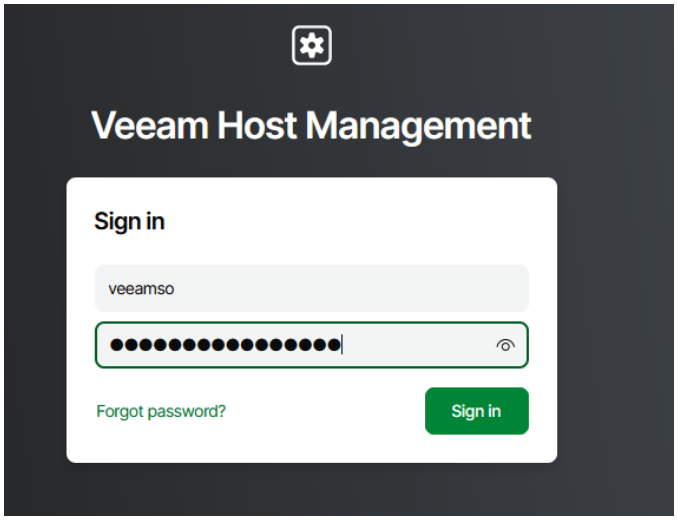
A. Open your Veeam Infrastructure Appliance http management page,

a. https://nexsanvhr01:10443

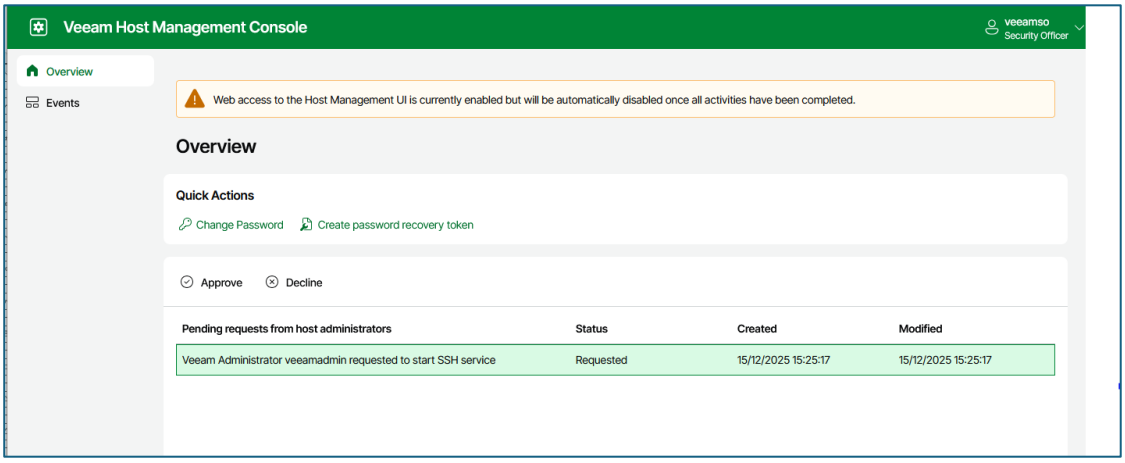
b. login with:

i. **veeamso**

ii. **Password used + MFA when promoted**



B. Proceed to **Approve the SSH**.



C. Proceed to create a **Veeam Hardened Repository** in Veeam v13.

Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

4. Veeam Backup & Replication Management

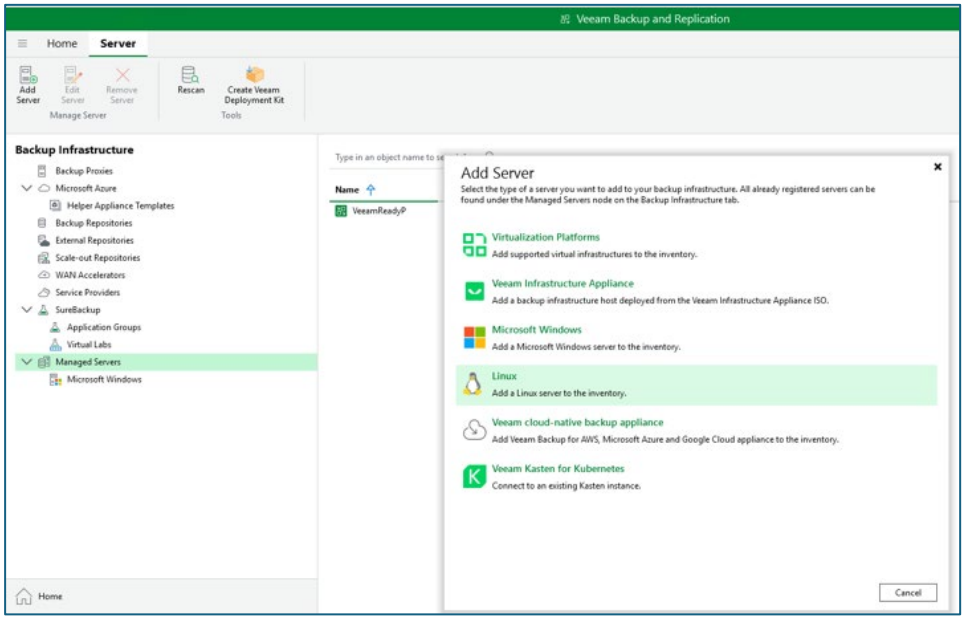
To complete the integration, open your **Veeam Backup & Replication 13** management console and proceed with the remaining steps:



A. Launch **Veeam Backup & Replication**.

B. Go to **Backup Infrastructure** from bottom left of interface.

C. Select **Managed Servers**.

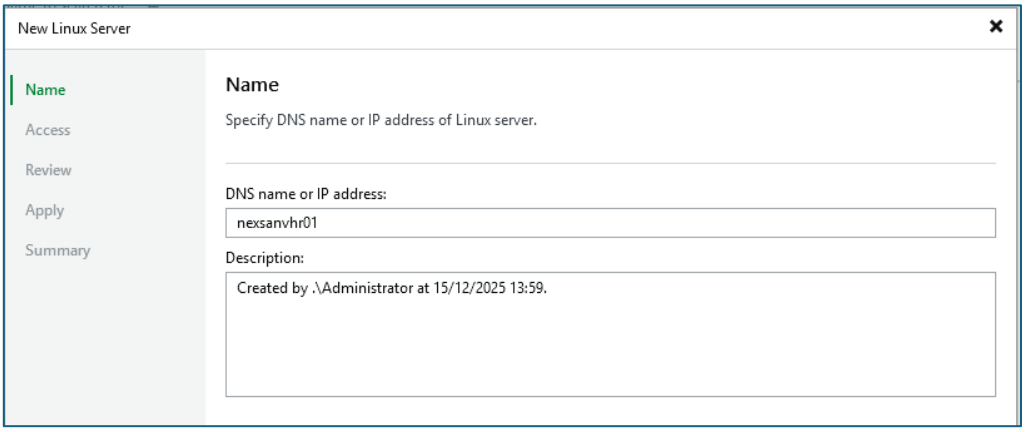


D. Select **Add Server** from top right-hand corner of interface.

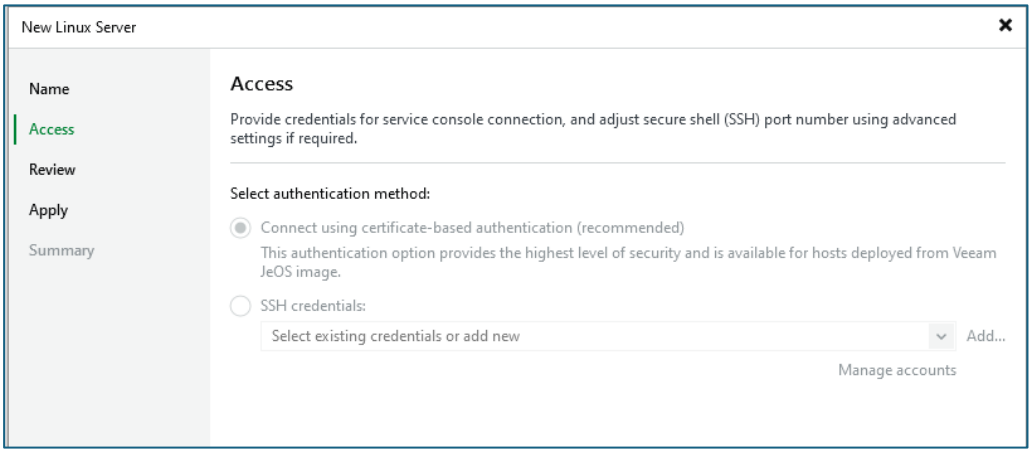
E. Select **Linux**.

Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

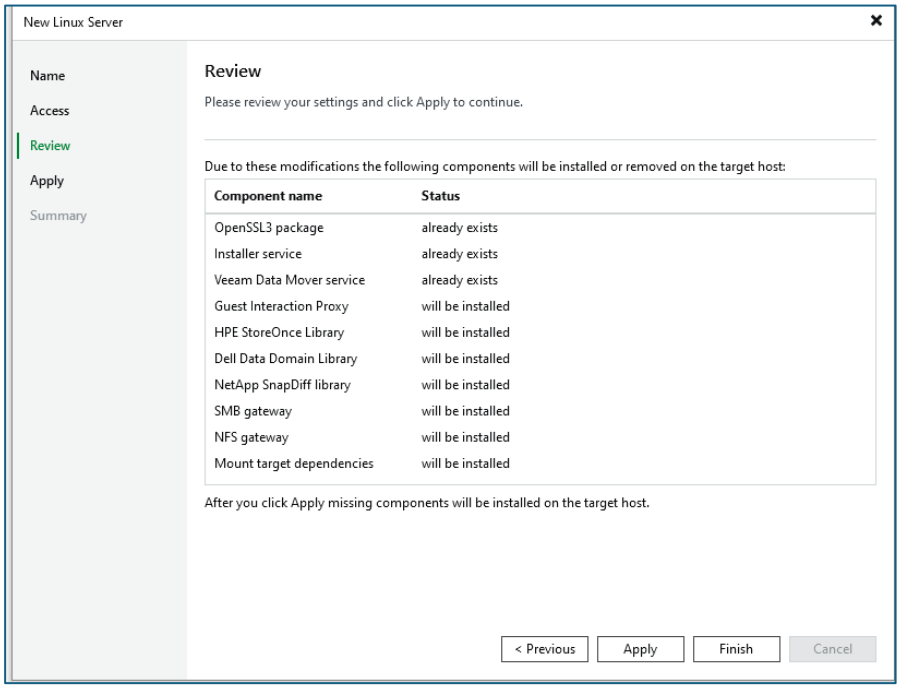
F. Enter the **DNS name** or **IP address**, then select **Next**.



G. Select **Connect using certificate-based authentication (recommend)**, then the **Add Next** button.

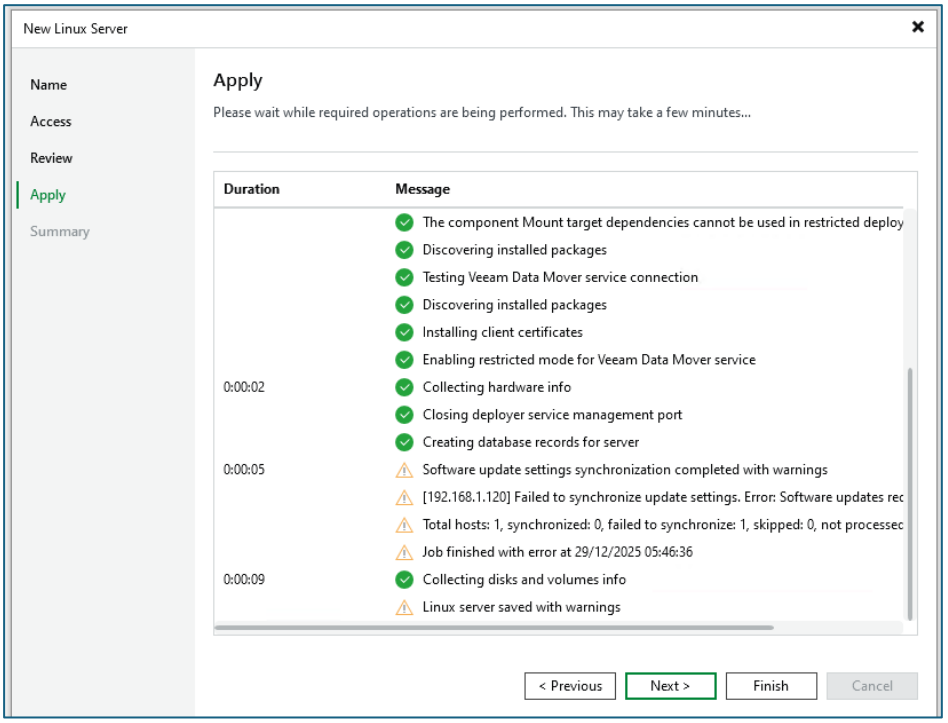


H. Select **Next** to install the required packages.



Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

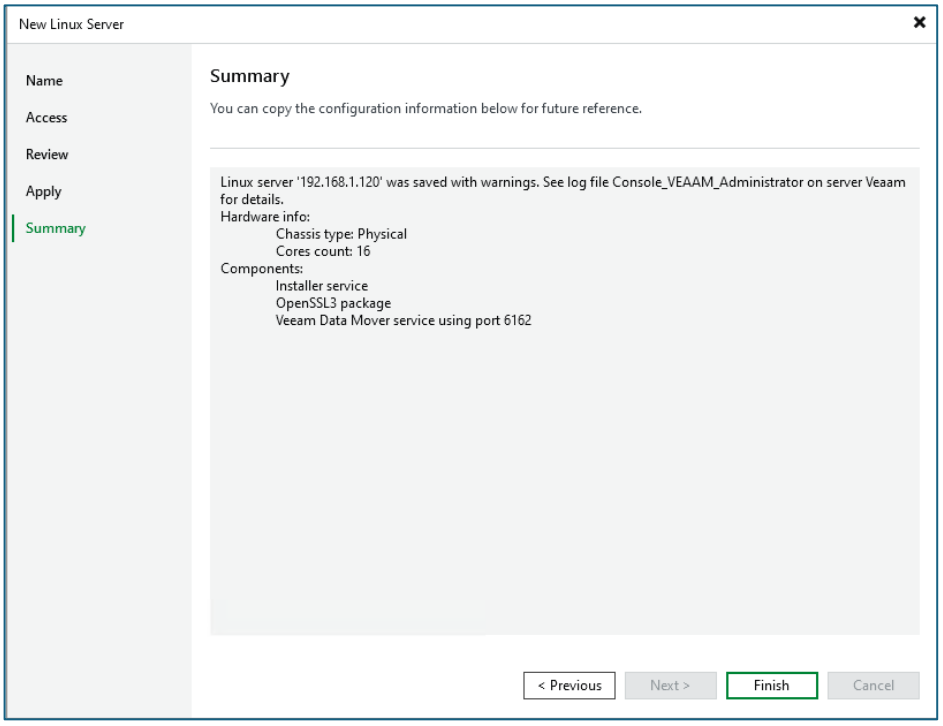
I. Select **Next** once you have reviewed the warnings.



NOTE:

Warnings related to software update synchronization are expected when deploying a hardened repository in a restricted or offline environment. These warnings do not impact backup functionality or immutability.

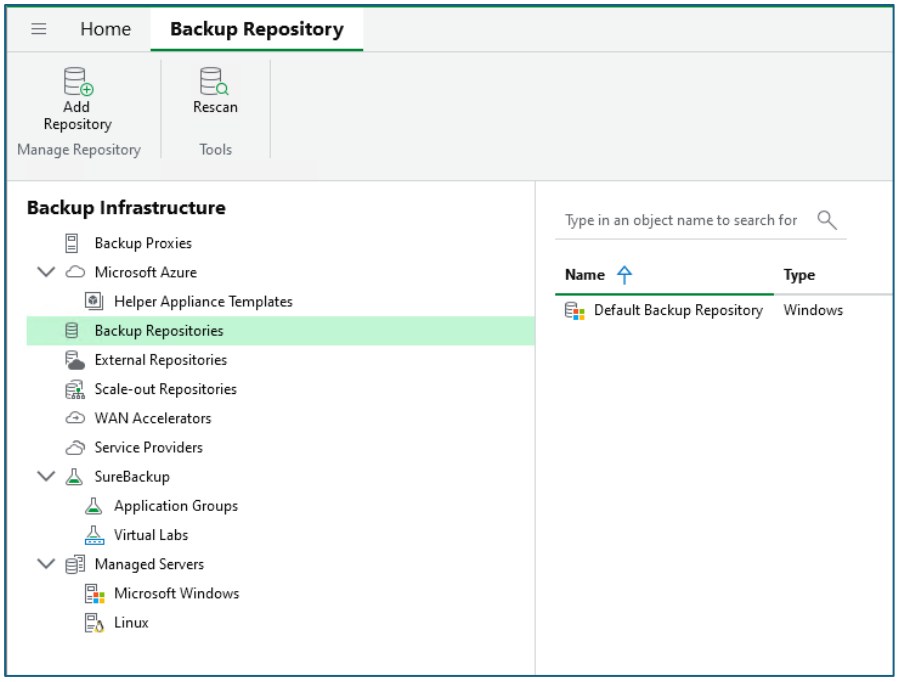
J. Select **Finish**.



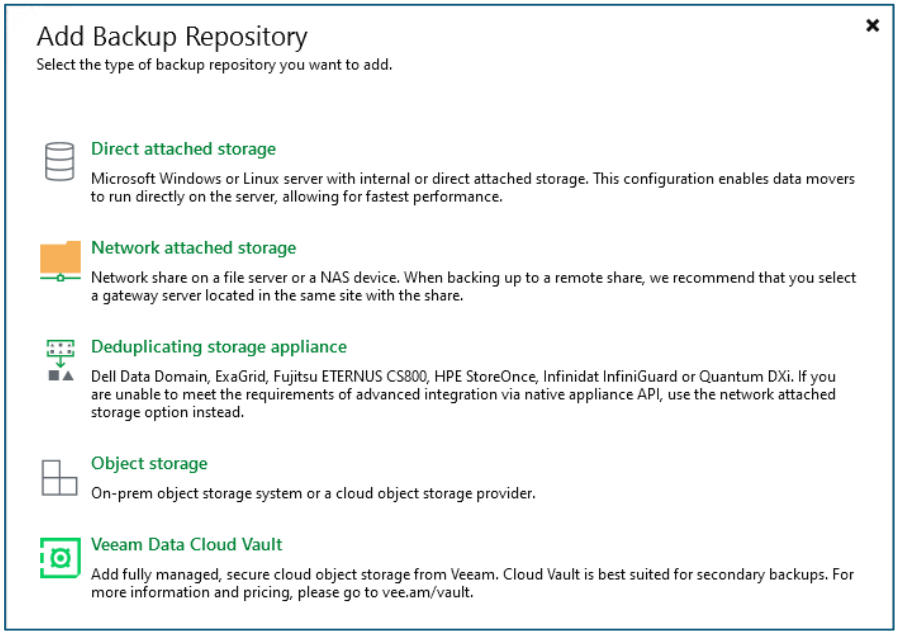
Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

5. Assigning the Backup Repository role

A. From the **Backup Repository** tab, select **Backup Repositories**, then click **Add Repository** in the top-left corner of the window.

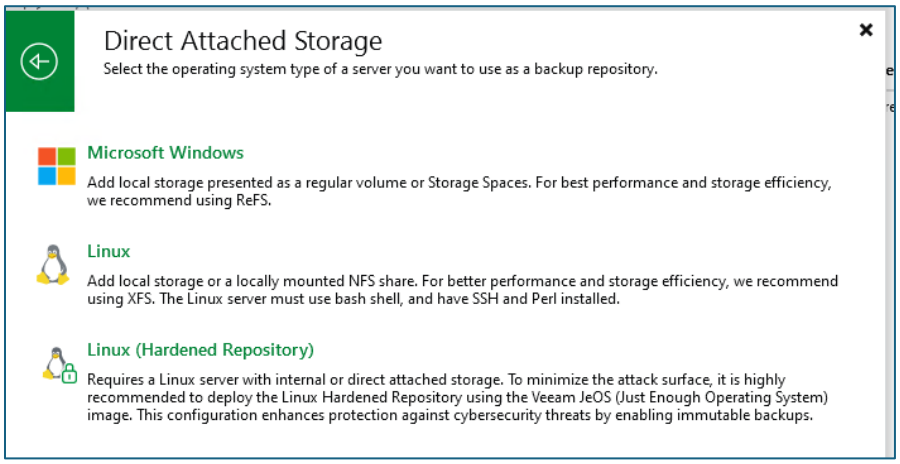


B. Select **Direct attached storage** as the repository type.

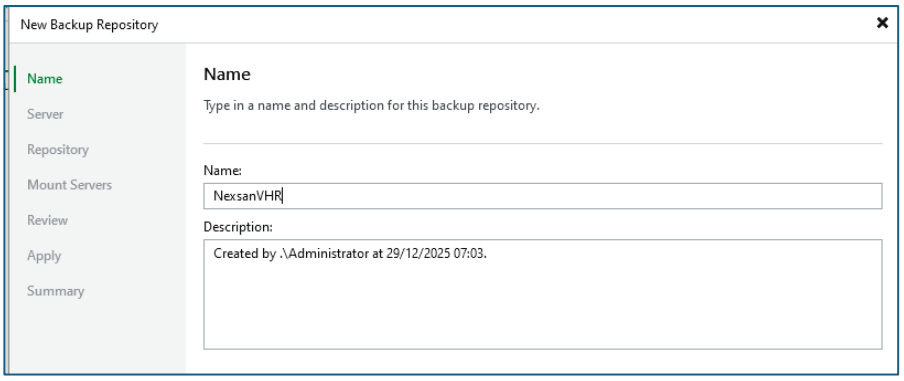


Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

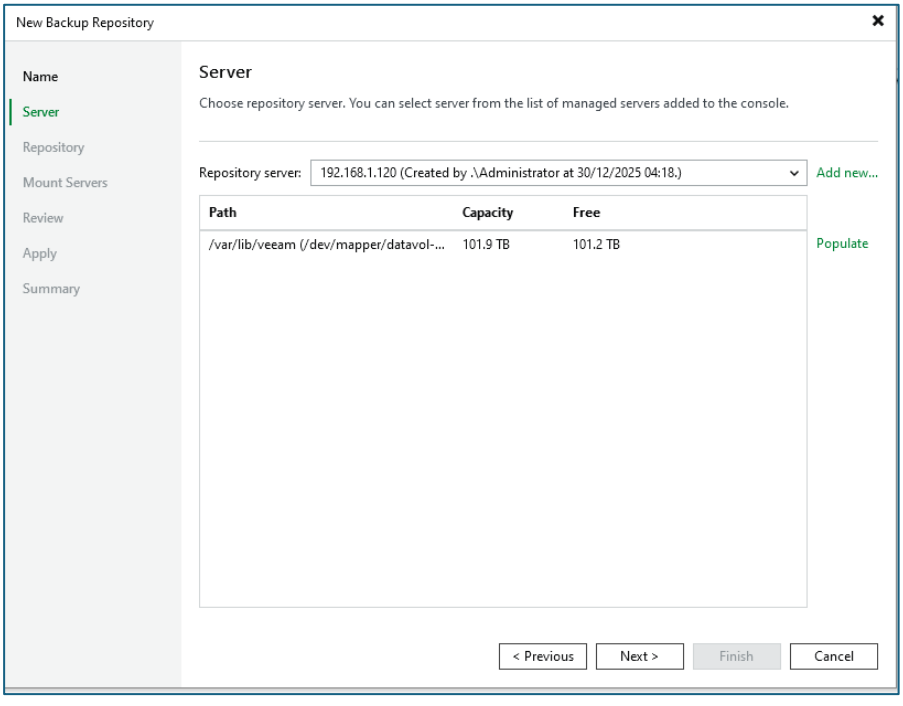
C. Select **Linux (Hardened Repository)**.



D. **Name** your repository (example: NexsanVHR), then select **Next**.

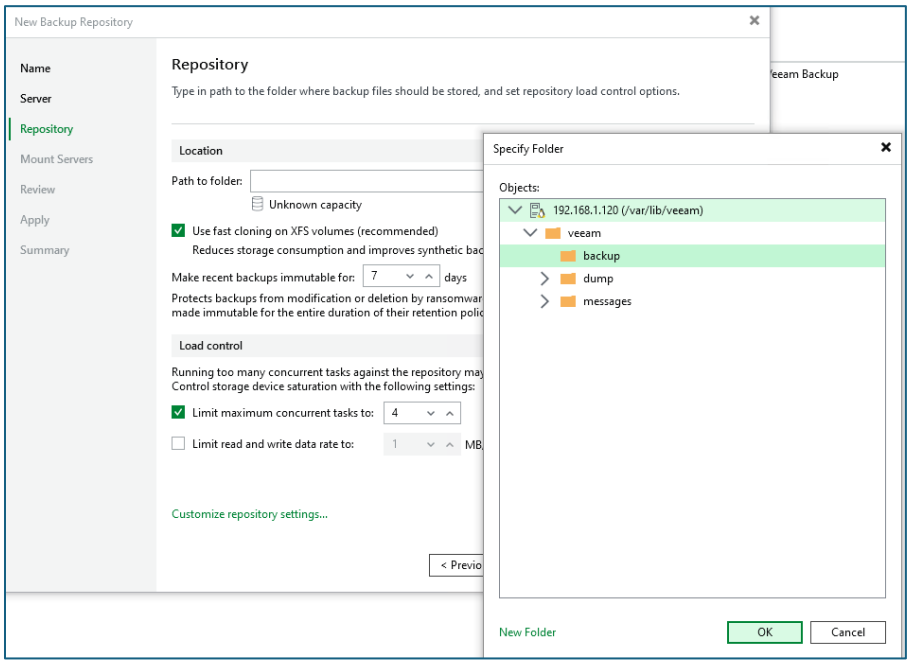


E. Select the **Repository server** that was added in the previous steps, then select **Populate**.



Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

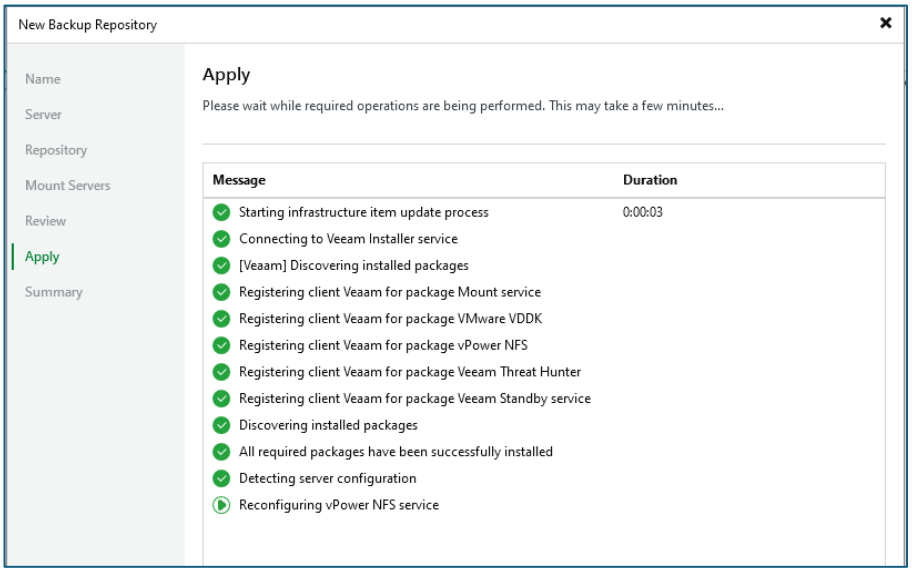
F. Select the **Path to folder location** for the **Backup** and select **OK**.



G. **Review** and confirm the **retention requirements**, then select **Next** to continue.

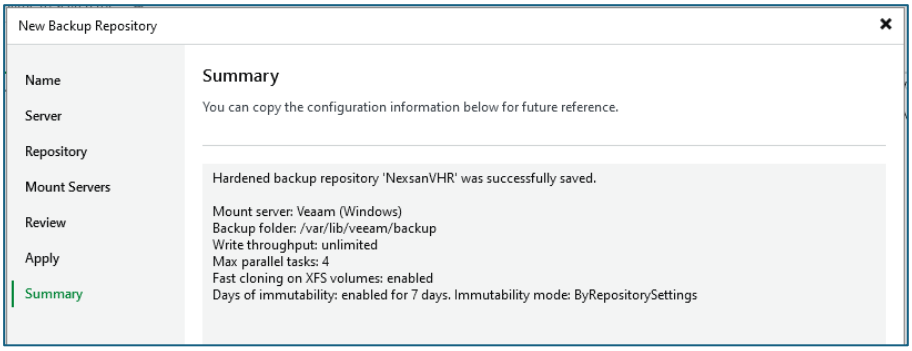
H. Confirm the **Mount Server**, **Review** the settings, then **Apply** the configuration.

I. Wait for settings to be applied, then select **Next**.

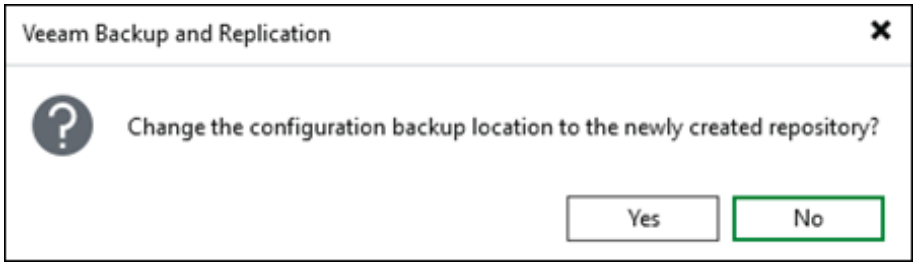


Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved

J. Review your configuration in the **Summary** and run a backup job to ensure all items are working as expected.



K. Confirm the change of the default backup location with **Yes** and then click **Finish**.



Stage Two of the installation is complete.



Copyright © 2010-2026 Nexsan Technologies, Inc. All Rights Reserved