OBJECT FIRST

2026

Early Threat Detection for Veeam Backups:

Object First Honeypot Feature

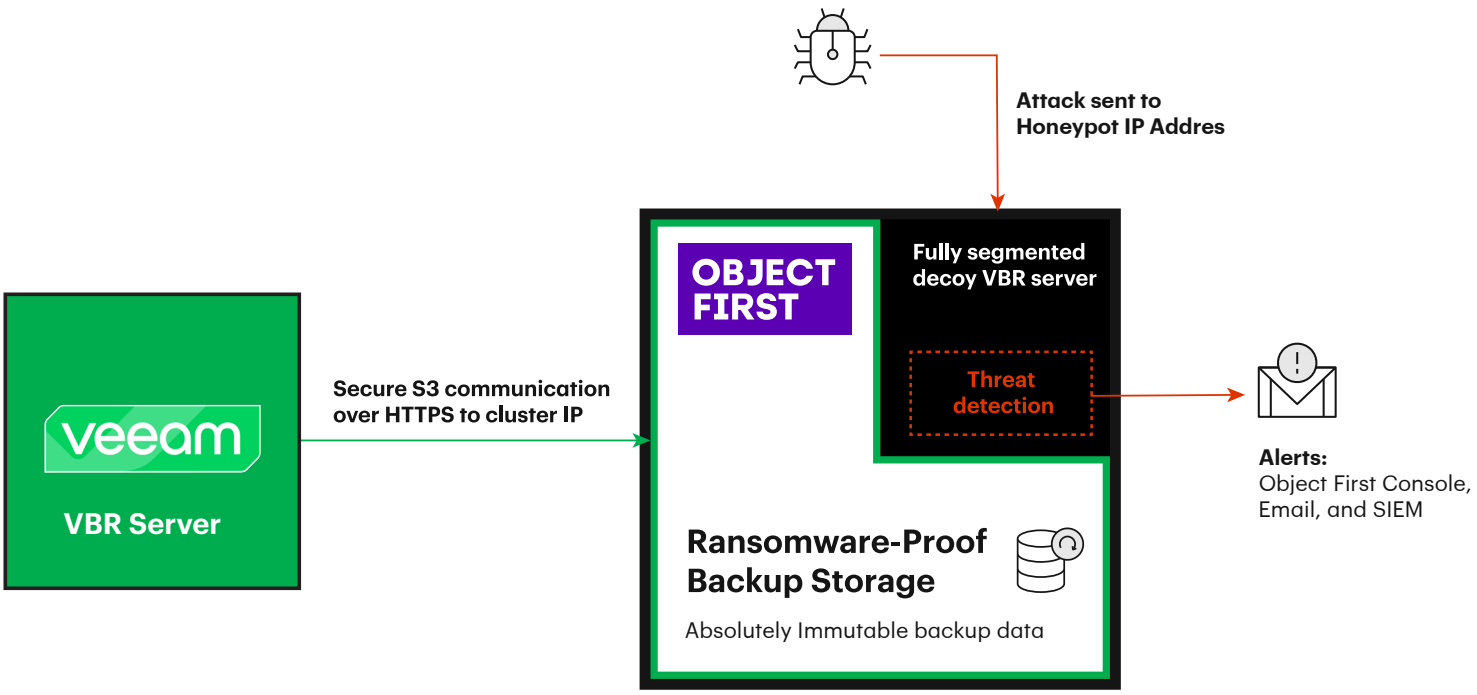
Ransomware attackers know your backups are your last line of defense. If your Veeam backups survive, you won't pay the ransom. That's why backup servers are often the first target.

Object First's Honeypot feature, included in the Object First 1.7 release, helps you detect suspicious activity targeting your backup environment, enabling you to be resilient and ransomware-proof when attacks, disasters, accidents, or insider threats occur.

What Is a Honeypot—and Why Should You Care?

A honeypot acts like a **tripwire for cyber threats**. It's a decoy system that attracts attackers and alerts you when someone is probing your environment.

Object First's Honeypot simulates a Veeam Backup & Replication (VBR) server. If attackers scan or attempt access, you get an immediate alert.



Business Benefits

- **Early Warning:** Detect threats before ransomware strikes.
- **Peace of Mind:** Adds security without complexity or extra tools.
- **Faster Response:** Alerts help you act before backups are compromised.
- **Compliance and Confidence:** Demonstrates proactive defense to auditors and stakeholders.
- **Zero Risk:** Enabling Honeypot introduces no risk to the security or integrity of the cluster or the immutable data stored within. Proven by the latest 3rd-party penetration testing.

Why Object First Honeypot Is Different

- **Built-In:** No extra software or hardware.
- **Simple Setup:** Enable in five clicks from the Object First Cluster Management dashboard.
- **No Expertise Required:** Perfect for IT teams of any size.

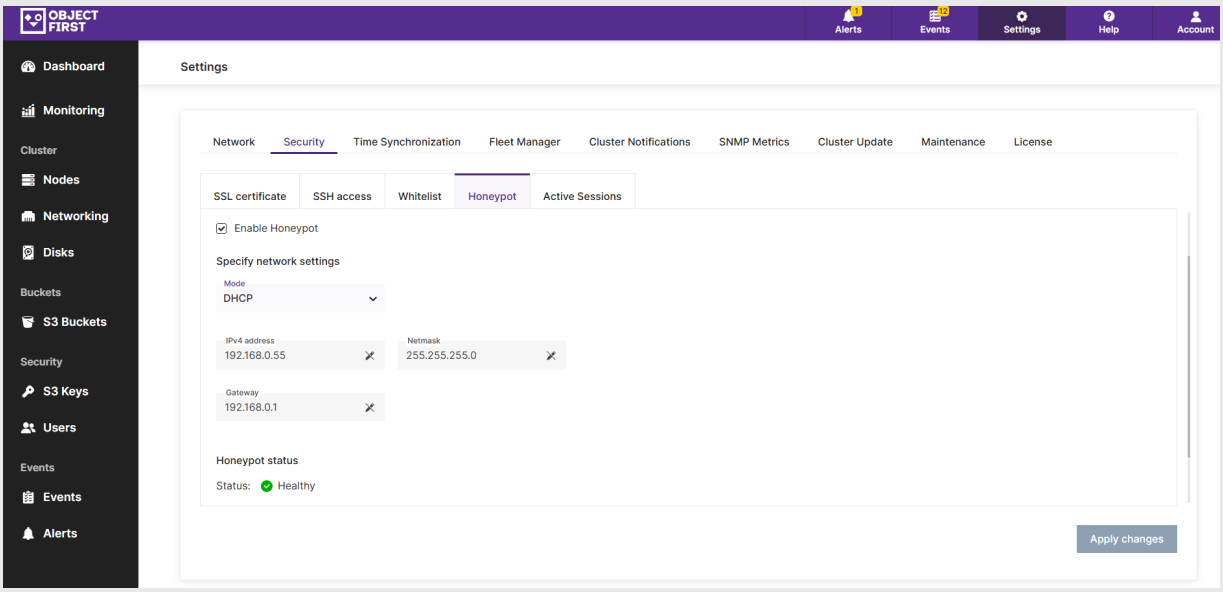
How It Works

Once enabled, Honeypot monitors for:

- Multiple login attempts
- Port scans
- Probing sensitive protocols
- Unauthorized Veeam console access

Alerts appear in the Object First dashboard and are sent via email or through syslog forwarding to SIEM.

How to Activate Honeypot in your Object First cluster



1. **Log in** to the Cluster Manager UI.

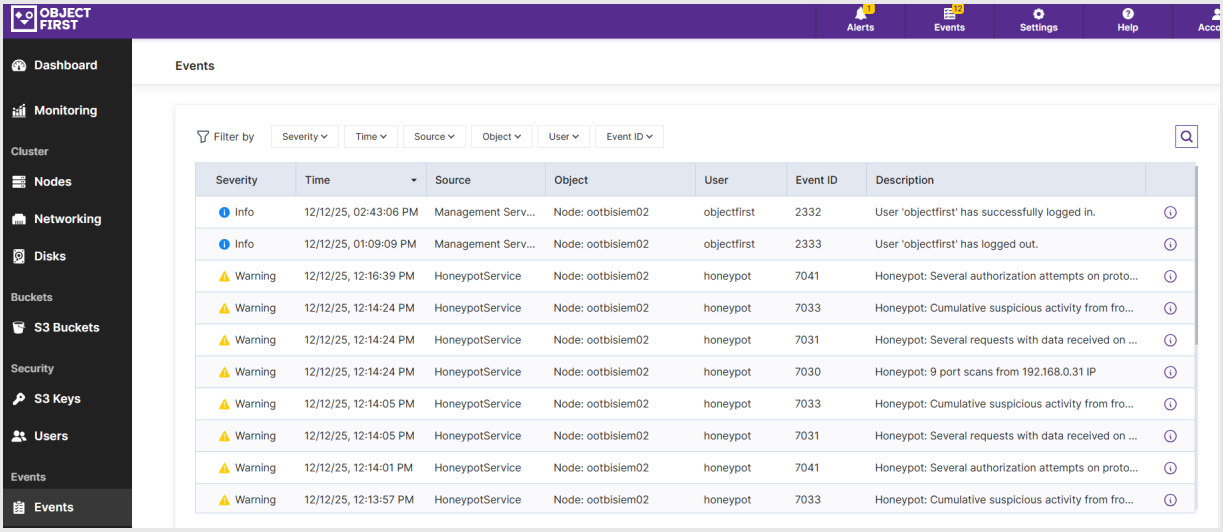
2. Go to **Settings > Security > Honeypot**.

3. **Check the box** to enable Honeypot.

4. Choose IP mode:
   a. **DHCP:** Auto-assigns IP.
   b. **Static:** Manually set IP and netmask.

5. Click **Apply Changes**.

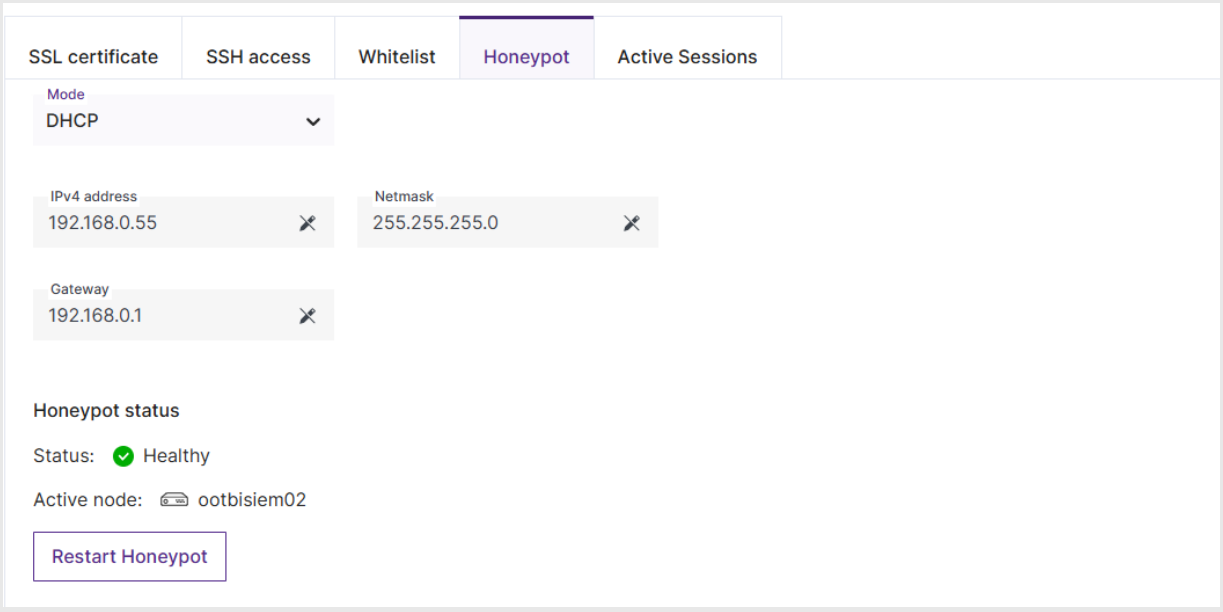
Honeypot is now live and monitoring for suspicious activity.



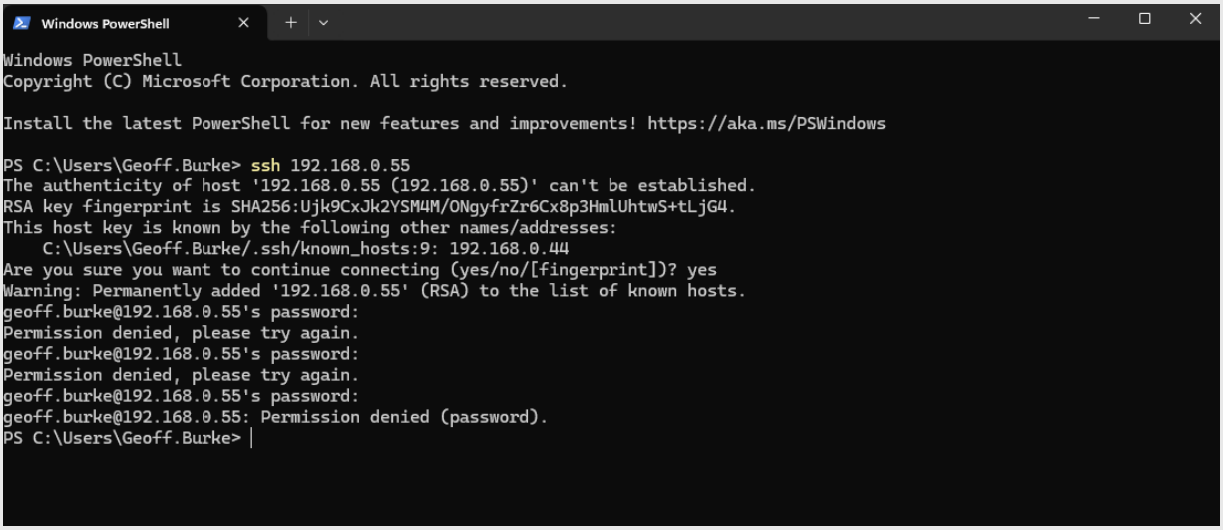
Hands-On Testing

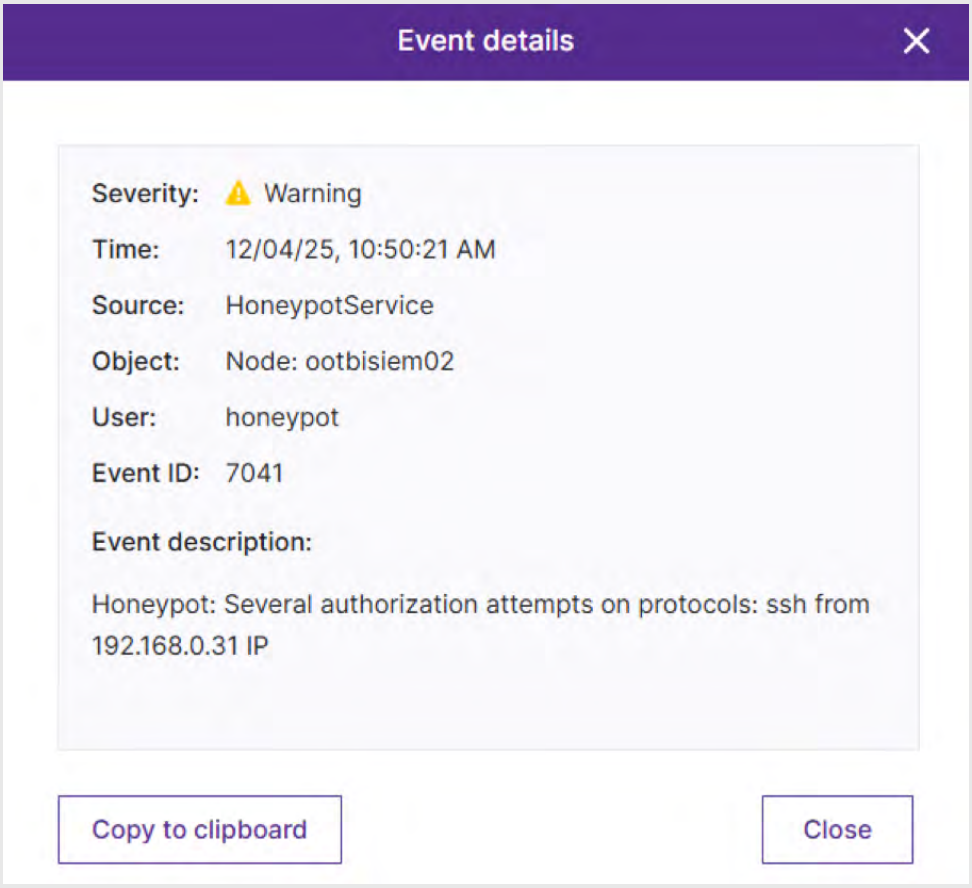
These quick, controlled tests help to demonstrate the Object First Honeypot feature's detection capabilities in a lab setup.

1. Open PowerShell and attempt to SSH into Honeypot (using the IP address displayed in your Honeypot).

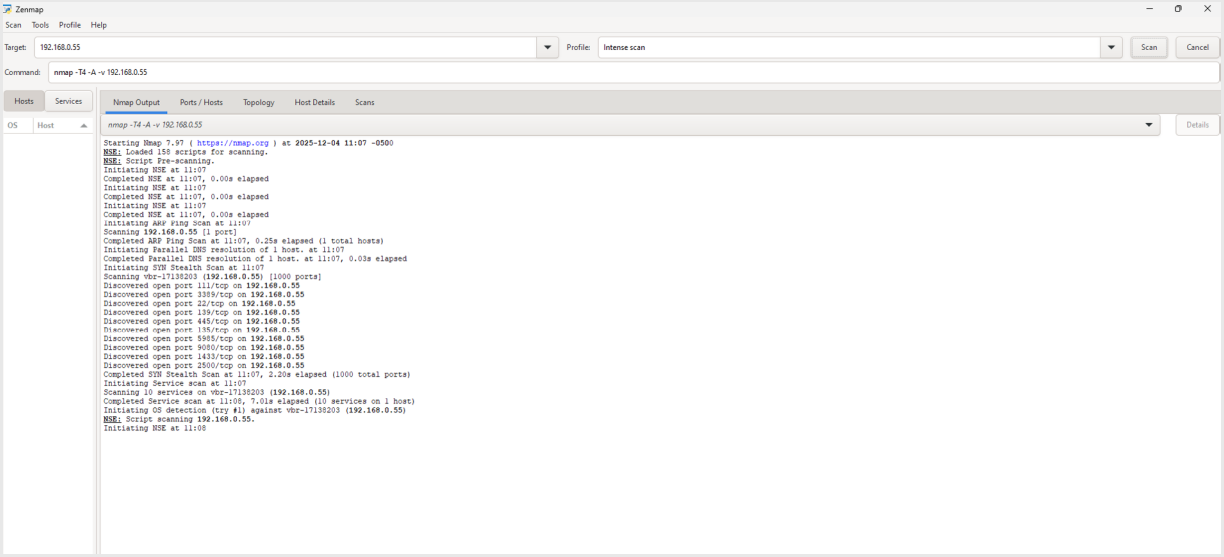


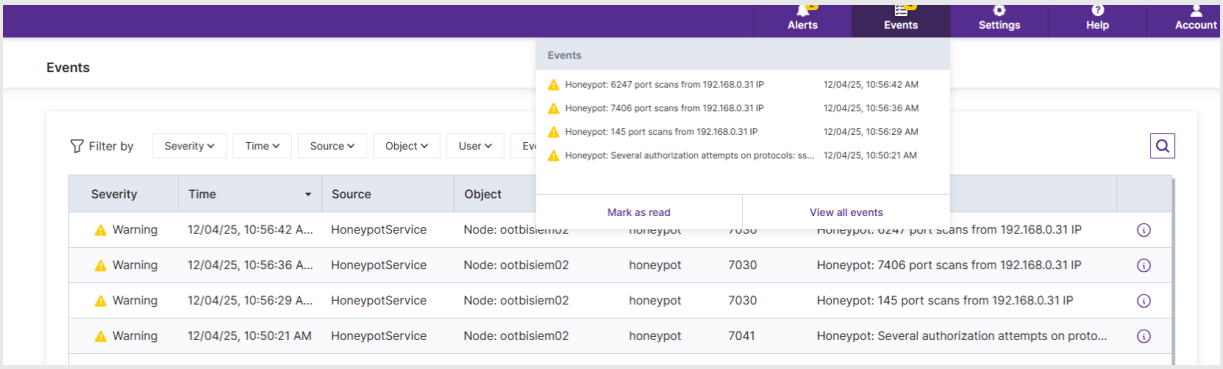
2. Enter any password; all attempts will be rejected.



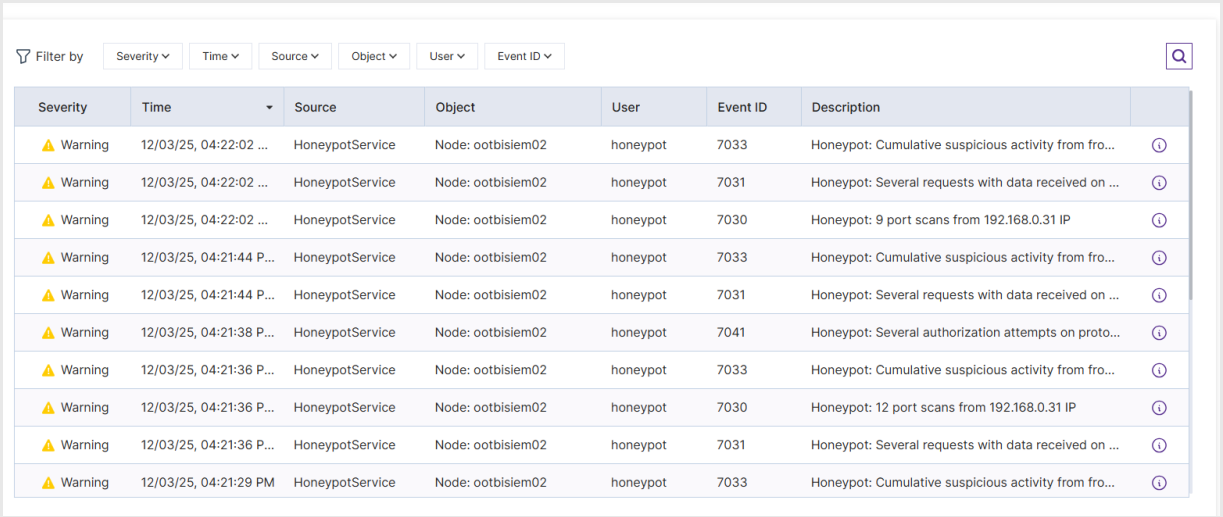


3. Use an authorized in-house security scanner—such as Zenmap—to test Honeypot.





4. Honeypot immediately flags the activity and displays an alert in the Object First dashboard.



Have Additional Questions?

For a complete list of Event IDs, including messages, severity, and source, please refer the Object First Help Center. For more information about Honeypot, please contact us directly or reach out to Object First Support.

OBJECT FIRST

Simply Resilient for Veeam

Learn More at ObjectFirst.com