Backup Security & Compliance

This report details the configurations of all backup servers. It checks alignment with security best practices for the operating system and Veeam backup components. Use this report for a direct overview of your backup infrastructure's security compliance.

Report Parameters

Infrastructure objects:	Veeam Backup & Replication
Best practices types:	All items
Check result:	All items

Summary

Backup Server Security & Compliance Status

Total backup servers:	4
Passed:	0
Not implemented:	4
Unable to detect:	0
Other:	0

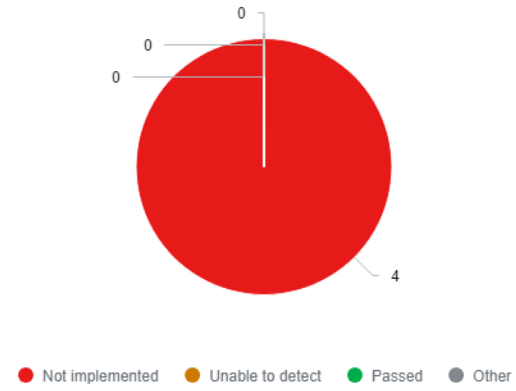
Missed Security & Compliance Checks

Unable to detect:	7
Not implemented:	85
Suppressed:	0
Not checked:	0

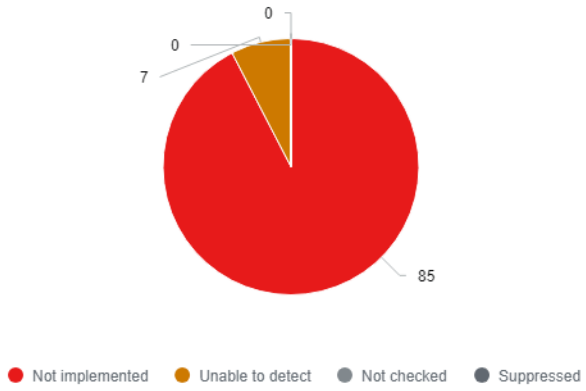
Security & Compliance Last Check

Less than a week:	4
From week to a month:	0
More than a month:	0

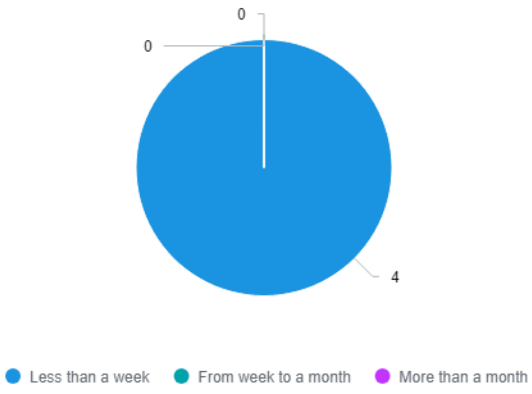
Backup Server Security & Compliance Status



Missed Security & Compliance Checks



Security & Compliance Last Check



Overview

Not implemented

Backup Server	Security & Compliance Last Check	Backup Infrastructure Security Best Practices	Product Configuration Best Practices	Best Practices Suppressed	Backup Server Security & Compliance Status
ahvbackupsrv60.tech.local	12/14/2025 11:00 PM	2 of 15	12 of 23	0	Not implemented
ccsrv.tech.local	12/13/2025 11:00 PM	3 of 15	12 of 23	0	Not implemented
vbrsrv1.tech.local	12/13/2025 11:00 PM	3 of 15	12 of 23	0	Not implemented
winsrv31.tech.local	12/13/2025 11:00 PM	3 of 15	13 of 23	0	Not implemented

Details

ahvbackupsrv60.tech.local

Backup Server	Best Practice Name	Best Practice Check Result	Recommendation
ahvbackupsrv60.tech.local	All backups should have at least one copy (the 3-2-1 backup rule)	Not implemented	To be compliant with the 3-2-1 rule, at least one backup copy job should be created or a scale-out backup repository with the copy mode or archive tier should be added.
ahvbackupsrv60.tech.local	Backup encryption passwords should follow length and complexity recommendations	Passed	To minimize the possibility of unauthorized access, passwords should meet Veeam requirements for password complexity. The password is at least 12 characters long. The password contains at least one uppercase character, one lowercase character, one special character and one numeric character.
ahvbackupsrv60.tech.local	Backup jobs to cloud repositories should use encryption	Passed	To reduce the cloud attack surface, job-level encryption should be enabled.
ahvbackupsrv60.tech.local	Backup server should not be a part of the production domain	Unable to detect	Adding the backup server and other backup infrastructure components to a management domain in a separate Active Directory forest is the best practice for building the most secure infrastructure. For medium-sized and small environments, backup infrastructure components can be placed to a separate workgroup.
ahvbackupsrv60.tech.local	Backup services should be running under the LocalSystem account	Passed	The account used to run Veeam services must be a LocalSystem account.
ahvbackupsrv60.tech.local	Compliance mode should be used for repositories with backup immutability enabled	Passed	The Compliance retention mode should be used for object storage repositories with immutability enabled. This is a more secure option compared to the Governance retention mode.
ahvbackupsrv60.tech.local	Configuration backup should be enabled and use encryption	Not implemented	Configuration backup should be enabled to reduce the risk of data loss and manage the Veeam Backup & Replication configuration database easier. Data encryption for configuration backup should be enabled to secure sensitive data stored in the configuration database.
ahvbackupsrv60.tech.local	Credential Guard should be enabled	Not implemented	Credential Guard should be configured properly to prevent credential theft attacks.
ahvbackupsrv60.tech.local	Credentials and encryption passwords should be rotated at least annually	Passed	For all user accounts added to the Credentials Manager, Cloud Credentials Manager, and Password Manager, passwords should be changed at least once a year.
ahvbackupsrv60.tech.local	Deprecated versions of SSL and TLS should be disabled	Not implemented	Outdated network protocols SSL 2.0 and 3.0 should be disabled as they have well-known security vulnerabilities and are not NIST-approved. Also, TLS 1.0 and 1.1 should be disabled if they are not needed.
ahvbackupsrv60.tech.local	Email notifications should be enabled	Not implemented	Email notifications should be enabled to monitor job statuses.
ahvbackupsrv60.tech.local	Firewall should be enabled	Not implemented	For Windows: Microsoft Defender Firewall with Advanced Security should be turned on. Also, rules for inbound and outbound connections should be set up according to your infrastructure and Microsoft best practices. For Linux: The firewall should be turned on. Also, rules for inbound and outbound connections should be configured according to your infrastructure and security best practices.
ahvbackupsrv60.tech.local	Hardened repositories should have the SSH Server disabled	Passed	SSH connection is necessary only for the deployment and upgrade of Veeam Data Mover. For security purposes, after adding the hardened repository to the backup infrastructure, the SSH connection should be disabled for the user account used to connect to the Linux server or for the server itself.
ahvbackupsrv60.tech.local	Hardened repositories should not be hosted in virtual machines	Passed	To reduce the attack surface, the hardened repository should be hosted on a physical machine with local storage.
ahvbackupsrv60.tech.local	Hardened repositories should not be used as backup proxy servers due to expanded attack surface	Passed	A VMware backup proxy requires VMware VDDK components to be installed. To reduce the risk of

			attacks through VMware VDDK vulnerabilities, a hardened repository should have only one role assigned.
ahvbackupsrv60.tech.local	Host to proxy traffic encryption should be enabled for the Network transport mode	Not implemented	If a VMware backup proxy uses the Network transport mode, it is recommended to transfer VM data over an encrypted TLS connection.
ahvbackupsrv60.tech.local	Immutable or offline (air gapped) media should be used	Not implemented	Immutable repositories should be used to protect backup files from being modified or deleted. Offline media should be used to keep backup files in addition to virtual storage devices.
ahvbackupsrv60.tech.local	Latest software updates should be installed	Passed	Veeam Software Appliance components should be updated regularly. Major releases, cumulative patches, and security updates usually contain new features, performance enhancements, and bug fixes that reduce the risk of compromise. If this check fails, a list of pending updates can be found in the log files. For more information, see Managing Logs.
ahvbackupsrv60.tech.local	Link-Local Multicast Name Resolution (LLMNR) should be disabled	Not implemented	Outdated broadcast protocol Link-Local Multicast Name Resolution (LLMNR) should be disabled to prevent spoofing and man-in-the-middle (MITM) attacks.
ahvbackupsrv60.tech.local	Linux servers should have password-based authentication disabled	Passed	Using key-based SSH authentication is generally considered more secure than using password authentication and helps averting man-in-the-middle (MITM) attacks. The private key is not passed to the server and cannot be captured even if a user connects to a fake server and accepts a bad fingerprint.
ahvbackupsrv60.tech.local	Local Security Authority Server Service (LSASS) should be set to run as a protected process	Not implemented	The protection for the Local Security Authority (LSA) process should be configured properly to prevent code injection and credential theft attacks.
ahvbackupsrv60.tech.local	MFA for the backup console should be enabled	Not implemented	Multi-factor authentication (MFA) should be enabled for the Veeam Backup & Replication console to protect user accounts with additional user verification.
ahvbackupsrv60.tech.local	NetBIOS protocol should be disabled on all network interfaces	Not implemented	NetBIOS should be disabled to reduce the risk of data theft attacks through shared folders.
ahvbackupsrv60.tech.local	Network traffic encryption should be enabled in the backup network	Passed	Network traffic encryption should be enabled in the backup network to ensure secure communication of sensitive data not only between public networks but also between private ones.
ahvbackupsrv60.tech.local	Password loss protection should be enabled	Not implemented	Password loss protection should be enabled on Veeam Backup Enterprise Manager to provide an alternative way to decrypt the data if a password for encrypted backup or tape is lost.
ahvbackupsrv60.tech.local	PostgreSQL server should be configured with recommended settings	Passed	PostgreSQL should have optimal run-time settings to operate correctly.
ahvbackupsrv60.tech.local	Remote Desktop Service (TermService) should be disabled	Not implemented	Remote services should be disabled if they are not needed. Note that for the Veeam Cloud Connect infrastructure, this parameter must be enabled if the SP uses Remote Desktop Protocol (RDP) to connect to the tenant backup server.
ahvbackupsrv60.tech.local	Remote Registry service (RemoteRegistry) should be disabled	Not implemented	Remote services should be disabled if they are not needed.
ahvbackupsrv60.tech.local	Reverse incremental backup mode is deprecated and should be avoided	Passed	The reverse incremental backup method should not be used as it produces the heaviest I/O impact on the backup storage compared to other backup methods.
ahvbackupsrv60.tech.local	Saved credentials should follow password length and complexity recommendations	Not implemented	To minimize the possibility of unauthorized access, passwords should meet Veeam requirements for password complexity. The password is at least 12 characters long. The password contains at least one uppercase character, one lowercase character, one special character and one numeric character.
ahvbackupsrv60.tech.local	SMBv1 protocol should be disabled	Not implemented	Outdated network protocol SMB 1.0 should be disabled as it has a number of serious security vulnerabilities including remote code execution.
ahvbackupsrv60.tech.local	SMBv3 signing and encryption should be enabled	Not implemented	If SMB shares are used in the backup infrastructure, SMB signing and encryption should be enabled to prevent NTLMv2 relay attacks.
ahvbackupsrv60.tech.local	The configuration backup must not be stored on the backup server	Not implemented	The configuration backup must not be stored on the backup server or on the default backup repository to be able to recover its configuration in case of failure.
ahvbackupsrv60.tech.local	Unknown Linux servers should not be trusted automatically	Not implemented	Untrusted Linux VMs and Linux servers must be allowed to connect to the backup server only using manual SSH fingerprint verification.
ahvbackupsrv60.tech.local	WDigest credentials caching should be disabled	Passed	WDigest credentials caching stores cleartext credentials in Windows RAM. To reduce the risk of credential dumping attacks, the setting should be disabled with a registry value.