Compliance Audit Report

Customer Node: Customer A Node

Report generated: 2026-02-01 12:15 UTC

ProxSecure Audit — Compliance automation for Proxmox infrastructure

Executive Summary

Overall compliance score: **40%**. Total checks: 10 (Passed: 4, Failed: 6).

Critical findings: 4. See Detailed Findings and Remediation Roadmap below.

Detailed Findings

Check Name	Category	Status	Severity	ISO 27001 / BSI
SSH root login disabled	ACCESS CONTROL	FAIL	CRITICAL	A.8.2 SYS.1.3.A14
Firewall enabled	NETWORK SECURITY	FAIL	CRITICAL	A.8.20, A.8.21 NET.1.1.A5
Backup schedule configured	STORAGE BACKUP	FAIL	CRITICAL	A.8.13 CON.3.1.A1
Backup retention at least 7 days	STORAGE BACKUP	FAIL	HIGH	A.8.13 CON.3.1.A1
Two-factor authentication enabled	ACCESS CONTROL	FAIL	CRITICAL	A.8.5 APP.4.2.A3
Syslog forwarding enabled	LOGGING MONITORING	FAIL	HIGH	A.8.15 SYS.1.1.A18
SNMP configured for monitoring	LOGGING MONITORING	PASS	MEDIUM	A.8.15 SYS.1.1.A18
VM network segmentation	VIRTUALIZATION SECURITY	PASS	HIGH	A.8.20 NET.1.1.A5
VM resource limits configured	VIRTUALIZATION SECURITY	PASS	MEDIUM	A.8.31 SYS.1.2.A2
Privileged access logging enabled	LOGGING MONITORING	PASS	HIGH	A.5.18, A.8.15 APP.4.2.A5

Remediation Roadmap

HIGH priority

• SSH root login disabled (ACCESS_CONTROL)

```
- name: Disable SSH root login
ansible.builtin.lineinfile:
path: /etc/ssh/sshd_config
regexp: '^#?PermitRootLogin'
line: 'PermitRootLogin no'
notify: restart sshd
```

• Firewall enabled (NETWORK_SECURITY)

```
- name: Enable firewall
ansible.builtin.systemd:
name: '{{ proxmox_firewall_service }}'
state: started
enabled: true
```

• Backup schedule configured (STORAGE_BACKUP)

```
- name: Configure backup schedule
community.general.cron:
name: 'Proxmox backup'
minute: '0'
hour: '2'
job: '/usr/bin/vzdump --compress zstd --mode snapshot'
user: root
state: present
```

• Two-factor authentication enabled (ACCESS_CONTROL)

```
- name: Enable 2FA for Proxmox users
ansible.builtin.shell: |
pveum user modify {{ proxmox_user }}@pam -otp {{ totp_secret }}
# Note: 2FA configuration requires manual TOTP setup per user via Proxmox GUI
# or pveum CLI. This snippet demonstrates the concept; actual implementation
# requires user-specific TOTP secret generation and QR code distribution.
```

MEDIUM priority

• Backup retention at least 7 days (STORAGE_BACKUP)

```
- name: Set backup retention
ansible.builtin.lineinfile:
path: /etc/pve/storage.cfg
regexp: '^prune-backups: keep-last='
line: 'prune-backups: keep-last=7'
insertafter: '^dir:'
# Note: For Proxmox VE 7.1+, configure via GUI (Datacenter > Storage > Backup Retention)
# or use /etc/pve/jobs.cfg for backup job definitions
```

• Syslog forwarding enabled (LOGGING_MONITORING)

```
- name: Configure syslog forwarding
ansible.builtin.lineinfile:
path: /etc/rsyslog.d/50-forward.conf
line: '*.* @{{ syslog_server }}:514'
create: true
notify: restart rsyslog
```

Compliance Trend Summary

Based on the last 5 days: minimum compliance **30%**, average **36.6%**, maximum **40%**.

Overall trend: **+10%** versus start of period (improving).