Guide de Durcissement Proxmox VE 9

Référence Francophone — CIS Benchmark · MITRE ATT&CK v16 · ISO 27001:2022

CIS Benchmark Debian 13 v1.0.0 | MITRE ATT&CK v16 | ISO 27001:2022 | PCI DSS v4.0 | CC BY-SA 4.0

77	9	10	3
Contrôles CIS	Phases	Scénarios	Profils

Ayi NEDJIMI — Expert Cybersécurité & IA — Mars 2026

ayinedjimi-consultants.fr

CHAPITRE 1 SUR 5

Threat Model & Pré-Installation

🛡️ Guide de Durcissement Proxmox VE 9 — Référence Francophone

Présentation

Ce guide fournit des recommandations de durcissement **prescriptives, vérifiables et opérationnelles** pour Proxmox Virtual Environment 9.x (Debian 13 "Trixie"). Il est conçu pour les administrateurs systèmes, ingénieurs sécurité et auditeurs.

Ce qui le différencie

CARACTÉRISTIQUE	CE GUIDE	GUIDES EXISTANTS
Format CIS hybride	Chaque contrôle suit la structure CIS (Audit/ Remediation/Default Value) + mappings compliance	Formats variés, rarement alignés CIS
Mappings compliance intégrés	CIS Controls v8, MITRE ATT&CK, ISO 27001:2022, PCI DSS v4.0	Peu ou pas de mappings
Threat model explicite	10 scénarios d'attaque rattachés à chaque contrôle	Pas de threat model
3 profils d'environnement	🏠 Homelab, 🏢 Production, 🌐 Exposé internet	Pas de distinction
Contrôles validés	Testé sur PVE 9.x — pas de "non validé" dans le guide principal	Contrôles souvent non validés
Corrections d'erreurs	Corrige les erreurs des guides existants (syntaxe 2FA, Fail2Ban regex, firewall defaults, LUKS)	Erreurs propagées
Rollback documenté	Chaque contrôle risqué a sa procédure de retour arrière	Jamais documenté
Couverture hyperviseur	Isolation VM (seccomp, KSM, IOMMU), pas juste l'OS	Focalisé OS uniquement

Base de référence

- **CIS Debian Linux 13 Benchmark** v1.0.0 (2025-12-16)
- **MITRE ATT&CK** v16
- **CIS Controls** v8
- **ISO/IEC 27001:2022** Annex A
- **PCI DSS** v4.0
- **BSI** — Sicherheitsanalyse von KVM (KVMSec) v1.0.1
- **QEMU Project** — Security Documentation

Structure du guide

#	FICHIER	PHASE	DESCRIPTION	CONTRÔLES
01	01-threat-model.md	—	Modèle de menaces (10 scénarios MITRE ATT&CK)	—
02	02-pre-installation.md	Phase 0	Avant l'installation (matériel, BIOS, chiffrement, réseau)	8
03	03-os-debian-durci.md	Phase 1	Durcissement OS Debian 13 (kernel, comptes, audit, services)	15
04	04-proxmox-specifique.md	Phase 2	Durcissement Proxmox (pveproxy, cluster, API, mises à jour)	12
05	05-acces-authentification.md	Phase 3	Accès et authentification (SSH, 2FA, RBAC, Fail2Ban, VPN)	12
06	06-reseau-segmentation.md	Phase 4	Réseau et segmentation (VLAN, firewall PVE, security groups)	8
07	07-stockage-chiffrement.md	Phase 5	Stockage et chiffrement (LUKS, ZFS, Ceph, NFS/iSCSI)	5
08	08-isolation-vm-ct.md	Phase 6	Isolation VM/CT (seccomp, KSM, IOMMU, LXC)	6
09	09-monitoring-detection.md	Phase 7	Monitoring et détection (AIDE, logs centralisés, audit)	3
10	10-maintenance-backup.md	Phase 8+9	Maintenance, backup, reprise d'activité (PBS, DR drills)	8

Quickstart

Prérequis

- Proxmox VE 9.x installé (Debian 13 "Trixie")
- Accès root au(x) nœud(s)
- Accès console hors-bande (IPMI/iDRAC/KVM) ou physique
- Sauvegardes fonctionnelles des VM et du nœud

Par où commencer ?

🏠 **Homelab** — Top 5 actions à impact maximal :

1. SSH : clés uniquement + Fail2Ban → Phase 3

2. Mises à jour auto sécurité Debian → Phase 1
3. 2FA sur le web UI → Phase 3
4. Backups PBS chiffrées → Phase 9
5. Firewall PVE activé → Phase 4

🏢 **Production** — Parcours recommandé :

1. Lire le threat model (30 min)
2. Appliquer la Phase 0 (pré-installation) si nouveau déploiement
3. Phases 1 → 4 dans l'ordre (Level 1 d'abord)
4. Phase 9 (backup) en priorité si pas encore fait
5. Phases 5 → 8 pour la défense en profondeur
6. Revenir sur les contrôles Level 2

🌐 **Exposé internet** — Ajouts critiques :

- VPN comme unique entrée management → Phase 3, 3.5
- WebAuthn/FIDO2 → Phase 3, 3.2.2
- LUKS full-disk encryption → Phase 0, 0.2.3

Règles d'or

1. **Toujours tester en lab** avant d'appliquer en production
2. **Ne jamais fermer votre session SSH** avant d'avoir testé la nouvelle configuration dans un second terminal
3. **Garder un accès console OOB** en cas de lock-out
4. **Appliquer Level 1 d'abord**, puis Level 2 quand Level 1 est stabilisé
5. **Documenter chaque déviation** par rapport au guide (justification + acceptation du risque)

Corrections notables vs guides existants

ERREUR COURANTE	NOTRE CORRECTION	PHASE
`pveum realm modify <<pam>> --tfa type=<<oath>>` (syntaxe invalide)	Procédure via interface web documentée	3 (3.2.1)
Fail2Ban pointe vers `/var/log/syslog` (absent PVE 9)	Backend systemd + `journalmatch = _SYSTEMD_UNIT=pvedaemon.service`	3 (3.4.2)
`PermitRootLogin no` (casse le cluster)	`PermitRootLogin prohibit-password` + Match Address cluster	3 (3.1.1)
`lockdown=integrity` en production (casse ZFS/Ceph/GPU)	Classé expérimental, exclu du guide principal	1 (1.2.5)
Firewall PVE "INPUT=DROP par défaut" (faux)	Explication complète des règles anti-lockout cachées	4 (4.2.1)
LUKS via installateur PVE (non disponible pour ext4)	Tableau comparatif ISO PVE vs Debian-first	0 (0.2.1)
KSM `echo 2 > run` (incomplet)	Désactivation KSM + ksmtuned	6 (6.1.2)
FORWARD=DROP sans règles cluster (casse les migrations)	Avertissement + prérequis réseau dédié	4 (4.2.4)

Format des contrôles

Chaque contrôle suit le format CIS Benchmark enrichi :

X.Y.Z — Titre du contrôle

PROFILE APPLICABILITY	LEVEL 1/2 — SERVER
Applicabilité PVE	🏠🏢🌐
Réf. CIS Debian 13	X.Y.Z
CIS Controls v8	Safeguard mappé
MITRE ATT&CK	Techniques + Mitigations
ISO 27001:2022	Annex A
PCI DSS v4.0	Exigence
Scénario threat model	S1-S10
Statut PVE 9	✅ Validé / ⚠️ Partiel / 🧪 Expérimental

Description / Rationale / Impact / Audit / Remédiation

Valeur par défaut / Rollback / Spécificité PVE

Avertissements

⚠️ Ce guide est fourni « en l'état », sans garantie. Vous êtes seul responsable de l'évaluation, du test et de la validation de chaque recommandation dans votre environnement.

⚠️ Certaines procédures ne sont pas officiellement supportées par Proxmox GmbH. Tester et maintenir à vos propres risques.

⚠️ Ce guide ne constitue pas une certification de conformité. Il est conçu pour aider à la préparation d'audits et à l'amélioration de la posture de sécurité.

Contribuer

Les contributions sont bienvenues. Voir CONTRIBUTING.md.

Licence

Ce guide est publié sous licence Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).

Vous pouvez copier, modifier et distribuer le contenu à condition de conserver l'attribution et de partager sous la même licence.

-e

---

01 — Modèle de menaces Proxmox VE

> **Version** : 0.2.0 **Date** : 2026-03-20 **Statut** : Rédaction initiale — Format normalisé **Licence** : CC BY-SA 4.0 **Base de référence** : CIS Debian Linux 13 Benchmark v1.0.0, MITRE ATT&CK v16, CIS Controls v8 **Sources** : BSI KVMSec v1.0.1, QEMU Security Documentation, Proxmox Forum, CVE databases

---

1.1 — Objectif et portée

Pourquoi un modèle de menaces ?

La plupart des guides de durcissement démarrent par « exécutez ces commandes ». Sans modèle de menaces, on applique des contrôles au hasard — on chiffre des disques pendant que SSH accepte les mots de passe, on active auditd sur un nœud dont le BMC a encore le mot de passe usine.

Ce chapitre identifie :

- Les **surfaces d'attaque** spécifiques à un hyperviseur Proxmox VE
- Les **scénarios d'attaque** réalistes, classés par probabilité
- Les **mappings** vers les cadres de référence (MITRE ATT&CK, CIS Controls v8, ISO 27001, PCI DSS)
- Les **contrôles préventifs et détectifs** de ce guide rattachés à chaque scénario

Chaque contrôle des phases suivantes référence un ou plusieurs scénarios de ce chapitre. Si un scénario ne vous concerne pas, les contrôles associés deviennent optionnels. Si un scénario est votre cauchemar, vous savez exactement quoi prioriser.

Portée

ÉLÉMENT	INCLUS	EXCLU
Hyperviseur Proxmox VE 9.x	✅	
OS hôte Debian 13	✅	
Infrastructure réseau PVE (bridges, VLAN, firewall)	✅	
Stockage PVE (local, Ceph, NFS/iSCSI)	✅	
BMC/IPMI/iDRAC	✅	
Proxmox Backup Server	✅ (interactions)	Guide dédié PBS hors périmètre
Sécurité des OS guests (VM/CT internes)		❌
Sécurité applicative des workloads		❌
Sécurité physique des locaux		❌ (mentionnée, non couverte)

1.2 — Surfaces d'attaque

Un hyperviseur est le **pire point de compromission possible** dans une infrastructure. Compromettre un hyperviseur donne accès simultanément à toutes les VM hébergées, à leur mémoire vive, à leurs disques, à leur trafic réseau. Proxmox VE expose quatre plans d'attaque distincts :

1.2.1 Plan de management (contrôle)

COMPOSANT	Port/Protocole
PVEPROXY (WEB UI + API REST)	TCP 8006
SSH	TCP 22
VNC/SPICE/NOVNC	Tunnelés via pveproxy
PVEDAEMON	TCP 85 (local)

Criticité : Quiconque contrôle le plan de management contrôle tout — création/destruction de VM, accès backups, lecture mémoire des VM, modification de la configuration cluster.

1.2.2 Plan de données (workloads)

COMPOSANT	Port/Protocole
BRIDGES LINUX (VMBR*)	Variable
STOCKAGE NFS	TCP 2049
STOCKAGE ISCSI	TCP 3260
CEPH PUBLIC	TCP 6789, 6800-7300
MIGRATION LIVE	TCP 60000-60050

Criticité : Une VM compromise peut tenter de pivoter via le réseau partagé ou tenter une évasion vers l'hôte via les devices émulés QEMU.

Référence : La documentation officielle de sécurité QEMU définit explicitement les guests, les interfaces utilisateur (VNC, SPICE), les protocoles réseau (NBD, migration) et les fichiers fournis par l'utilisateur comme des entités **non fiables** (untrusted).

1.2.3 Plan cluster

COMPOSANT	Port/Protocole
COROSYNC	UDP 5405
PMXCFS	—
SSH INTER-NŒUDS	TCP 22

Criticité : Compromettre un nœud = accès au filesystem cluster partagé (configurations, certificats, tokens de tous les nœuds).

1.2.4 Plan physique

COMPOSANT	Accès
BMC/IPMI/IDRAC/ILO	Réseau OOB (TCP 443, UDP 623)
CONSOLE PHYSIQUE	Local
DISQUES PHYSIQUES	Local
PORTS USB	Local

Criticité : Un BMC compromis donne un accès console virtuel complet, invisible depuis l'OS. Des cas de ransomware via BMC vulnérable sont documentés dans la communauté Proxmox.

1.3 — Profils d'environnement

PROFIL	SYMBOLE	DESCRIPTION	MENACES PRINCIPALES
Homelab	🏠	Nœud unique ou petit cluster, réseau local, pas d'exposition internet directe	Rebond depuis poste LAN compromis, erreur de config, accès physique accidentel
Production	🏢	Cluster multi-nœuds, réseau d'entreprise segmenté, SLA internes, multi-administrateurs	Mouvement latéral, insider malveillant, ransomware, non-conformité réglementaire
Exposé internet	🌐	Nœuds accessibles depuis internet (hébergeur, cloud privé, VPS)	Brute-force, exploitation CVE, compromission BMC, attaques ciblées, supply chain

Règle : en cas de doute entre deux profils, choisir le plus restrictif.

1.4 — Scénarios d'attaque

Chaque scénario suit un format normalisé avec mappings compliance intégrés. Les scénarios sont ordonnés par probabilité décroissante.

S1 Compromission via SSH ou l'interface web

PROBABILITÉ	🔴 Très élevée
IMPACT	Critique — contrôle total de l'hyperviseur
PROFILS	🏠🏢🌐
VECTEUR	Réseau — plan de management

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Accès initial	Initial Access	Exploit Public-Facing Application	T1190
Accès initial	Initial Access	Valid Accounts	T1078
Accès initial	Initial Access	Brute Force	T1110
Exécution	Execution	Command and Scripting Interpreter	T1059
Persistance	Persistence	Account Manipulation	T1098

CIS Controls v8 : 4.1, 5.2, 5.4, 6.3, 6.4, 6.5, 13.1

ISO 27001:2022 : A.5.15, A.5.17, A.8.5, A.8.20

PCI DSS v4.0 : 2.2.1, 6.3.3, 8.2.1, 8.3.1, 8.3.6

DESCRIPTION :

Description :

Chaîne d'attaque type :

1. Scan de ports → détection SSH (22) et/ou pveproxy (8006)
2. Brute-force ou credential stuffing sur SSH/web UI
3. Ou : exploitation d'une CVE pveproxy (ex : CVE-2023-43320 bypass 2FA, CVE-2025-57538/39/40 XSS stocké)
4. Obtention d'un shell root ou d'une session web admin
5. Contrôle total : création/suppression VM, accès backups, modification cluster

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
Désactivation auth par mot de passe SSH	3	3.1.1	🔴 Critique
2FA obligatoire (TOTP ou WebAuthn)	3	3.2	🔴 Critique
Fail2Ban SSH + Web UI (regex corrigé)	3	3.4	🔴 Critique
Restriction IP sur pveproxy :8006	2	2.1.3	🔴 Critique
VPN comme unique entrée management	3	3.5	🟡 Important (🌐)
Mise à jour régulière PVE	2	2.4	🔴 Critique
RBAC moindre privilège	3	3.3	🟡 Important

Contrôles détectifs :

CONTRÔLE	PHASE	RÉF.
Centralisation logs auth	7	7.2.3
Alerting échecs auth multiples	7	7.1.3
Audit appels API	2	2.2.3

CVE historiques pertinentes :

CVE	ANNÉE	TYPE	CVSS
CVE-2023-43320	2023	Bypass 2FA (PVE 5.4–8.0)	N/A
CVE-2025-57538/39/40	2025	XSS stocké config Datacenter	N/A
CVE-2022-31358	2022	XSS stocké	N/A

S2 Ransomware ciblant l'hyperviseur et les backups

PROBABILITÉ	🔴 Élevée
IMPACT	Critique — perte totale des données et des VM
PROFILS	🏠🏢🌐
VECTEUR	Post-compromission (rebond après S1 ou poste admin compromis)

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Impact	Impact	Data Encrypted for Impact	T1486
Impact	Impact	Inhibit System Recovery	T1490
Impact	Impact	Data Destruction	T1485
Mouvement	Lateral Movement	Remote Services: SSH	T1021.004
Collection	Collection	Data from Local System	T1005

CIS Controls v8 : 3.4, 11.1, 11.2, 11.3, 11.4, 11.5

ISO 27001:2022 : A.8.13 (Information backup), A.8.14 (Redundancy), A.5.29 (Business continuity)

PCI DSS v4.0 : 3.5.1, 9.4.1, 12.10.1

DESCRIPTION :

Description :

Chaîne d'attaque type :

1. Compromission initiale (S1, phishing admin, rebond LAN)
2. Reconnaissance : stockage, backups PBS, snapshots
3. Suppression des snapshots ZFS/LVM
4. Suppression ou chiffrement des backups PBS
5. Chiffrement des images disque VM
6. Demande de rançon

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
Backups PBS chiffrés client-side + clé escrow hors ligne	9	9.1.2, 9.1.3	🔴 Critique
Immutabilité backups (retention lock PBS)	9	9.1.3	🔴 Critique
Tokens PBS avec privilèges minimaux (pas de suppression)	9	9.1.2	🔴 Critique
Backup hors site / hors ligne (3-2-1-1-0)	9	9.1.1	🔴 Critique
Snapshots ZFS out-of-band	5	5.3	🟡 Important
RBAC : séparer admin-VM et admin-backup	3	3.3	🟡 Important

Contrôles détectifs :

CONTRÔLE	PHASE	RÉF.
Monitoring espace stockage (suppression massive = alerte)	7	7.1
AIDE (intégrité fichiers)	7	7.2.1
Alerting suppression backups PBS	7	7.1.3

S3 Évasion de VM (VM escape)

PROBABILITÉ	🟡 Moyenne (en augmentation)
IMPACT	Critique — compromission de l'hôte depuis un guest
PROFILS	🏢🌐
VECTEUR	VM compromise → exploitation QEMU/KVM → accès hôte

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Évasion	Privilege Escalation	Escape to Host	T1611
Exploitation	Execution	Exploitation for Client Execution	T1203
Découverte	Discovery	System Information Discovery	T1082
Accès	Privilege Escalation	Exploitation for Privilege Escalation	T1068

CIS Controls v8 : 4.1, 7.1, 7.3, 10.5, 16.13

ISO 27001:2022 : A.8.7, A.8.8, A.8.9

PCI DSS v4.0 : 6.2.4, 6.3.3, 11.3.1

DESCRIPTION :

Description :

Particularité Proxmox : Contrairement à libvirt/sVirt qui confine chaque processus QEMU avec des labels SELinux automatiques, Proxmox **ne génère pas de profils AppArmor par VM automatiquement**. Les processus QEMU tournent en tant que root sans confinement mandatory access control par défaut. C'est une différence architecturale majeure documentée par le BSI.

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
Profils AppArmor pour QEMU	6	6.1.1	🟡 Important
Filtres seccomp QEMU	6	6.1.2	🟡 Important
Suppression devices émulés inutiles	6	6.1.5	🟡 Important
Machine type q35 (meilleure isolation)	6	6.1.5	🟡 Important
KSM désactivé (side-channel multi-tenant)	6	6.1.4	🟡 Important
IOMMU vérifié pour PCI passthrough	6	6.1.3	🔴 Critique si passthrough
Mise à jour kernel + QEMU prioritaire	2	2.4	🔴 Critique
Paramètres boot kernel durcis	1	1.2.5	🟡 Important

Contrôles détectifs :

CONTRÔLE	PHASE	RÉF.
auditd modules kernel + syscalls	1	1.4.1
Monitoring processus anormaux sur l'hôte	7	7.2

Références :

- BSI — Sicherheitsanalyse von KVM (KVMSec) v1.0.1, 2017
- QEMU Project — Security Documentation (modèle d'entités non fiables)
- Red Hat — Hardening QEMU through continuous security testing

S4 Mouvement latéral via le cluster

PROBABILITÉ	🟡 Moyenne
IMPACT	Critique — compromission de tous les nœuds
PROFILS	🏢🌐
VECTEUR	Réseau interne — plan cluster

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Mouvement	Lateral Movement	Remote Services: SSH	T1021.004
Mouvement	Lateral Movement	Exploitation of Remote Services	T1210
Collecte	Credential Access	Unsecured Credentials: Private Keys	T1552.004
Collecte	Collection	Data from Information Repositories	T1213

CIS Controls v8 : 4.1, 6.1, 6.4, 12.2, 13.1

ISO 27001:2022 : A.8.20, A.8.22, A.8.24

PCI DSS v4.0 : 1.2.1, 1.3.1, 4.2.1

DESCRIPTION :

Description :

Chaîne d'attaque type :

1. Compromission d'un nœud (via S1 ou S3)
2. Lecture `/etc/pve` → certificats cluster, clés SSH, tokens API
3. SSH root vers les autres nœuds (confiance implicite)
4. Interception/injection Corosync si non chiffré
5. Contrôle de l'ensemble du cluster

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
Réseau dédié Corosync (VLAN isolé)	4	4.1.1	🔴 Critique
Chiffrement Corosync	2	2.3.1	🔴 Critique
Segmentation VLAN management/cluster/VM	4	4.1	🔴 Critique
Restriction SSH inter-nœuds au réseau cluster	3	3.1.1	🟡 Important
Firewall PVE FORWARD=DROP + règles explicites	4	4.2	🟡 Important

Contrôles détectifs :

CONTRÔLE	PHASE	RÉF.
Monitoring connexions SSH inter-nœuds	7	7.2.4
Alerting changements config cluster	7	7.2
auditd sur /etc/pve	1	1.4.1

S5 Compromission du BMC/IPMI

PROBABILITÉ	🟡 Moyenne (🔴 si BMC exposé internet)
IMPACT	Critique — contrôle physique total du serveur
PROFILS	🏢🌐
VECTEUR	Réseau — plan physique/OOB

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Accès initial	Initial Access	External Remote Services	T1133
Accès initial	Initial Access	Valid Accounts: Default Accounts	T1078.001
Persistance	Persistence	Pre-OS Boot: Component Firmware	T1542.002
Accès	Privilege Escalation	Hardware Additions	T1200

CIS Controls v8 : 1.1, 2.2, 4.1, 4.6, 12.2

ISO 27001:2022 : A.5.15, A.7.2, A.8.9, A.8.20

PCI DSS v4.0 : 2.2.1, 9.2.1, 11.3.1

DESCRIPTION :

Description :

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
Isolation BMC sur VLAN OOB dédié	0	0.1.2	🔴 Critique
Changement credentials par défaut	0	0.1.2	🔴 Critique
Désactivation protocoles non chiffrés	0	0.1.2	🔴 Critique
Mise à jour firmware BMC	0	0.1.1	🔴 Critique
Certificats TLS sur interface web BMC	0	0.1.2	🟡 Important

S6 Insider malveillant ou négligent

PROBABILITÉ	🟡 Moyenne
IMPACT	Variable — fuite de données à destruction
PROFILS	🏢
VECTEUR	Accès légitime — plan de management

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Collection	Collection	Data from Local System	T1005
Exfiltration	Exfiltration	Exfiltration Over Web Service	T1567
Impact	Impact	Data Destruction	T1485
Évasion	Defense Evasion	Indicator Removal: Clear Linux Logs	T1070.002

CIS Controls v8 : 3.3, 5.3, 5.4, 6.1, 6.2, 8.2, 8.5

ISO 27001:2022 : A.5.10, A.5.15, A.6.1, A.8.15

PCI DSS v4.0 : 7.2.1, 8.2.1, 10.2.1

DESCRIPTION :

Description :

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
RBAC strict moindre privilège	3	3.3	🔴 Critique
Comptes nommés individuels	3	3.3.1	🔴 Critique
2FA sur tous les comptes	3	3.2.3	🔴 Critique
Séparation des rôles	3	3.3.2	🟡 Important
Revue trimestrielle des accès	8	8.2.1	🟡 Important

Contrôles détectifs :

CONTRÔLE	PHASE	RÉF.
Journalisation appels API	2	2.2.3
auditd fichiers sensibles	1	1.4.1
Logs centralisés hors contrôle admin PVE	7	7.2.3

S7 Attaque supply chain (dépôts, paquets)

PROBABILITÉ	🟠 Faible-Moyenne
IMPACT	Critique — backdoor persistante sur tous les nœuds
PROFILS	🏠🏢🌐
VECTEUR	Réseau — mises à jour

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Accès initial	Initial Access	Supply Chain Compromise: Software	T1195.002
Exécution	Execution	System Services: Service Execution	T1569.002
Persistance	Persistence	Compromise Client Software Binary	T1554

CIS Controls v8 : 2.2, 2.5, 7.3, 16.4

ISO 27001:2022 : A.8.8, A.8.10

PCI DSS v4.0 : 6.3.2, 6.3.3

DESCRIPTION :

Description :

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
Vérification signatures GPG (ne pas désactiver)	1	1.1.1	🔴 Critique
Dépôt enterprise (signé Proxmox GmbH)	1	1.1.1	🟡 Important
Vérification intégrité paquets installés	1	1.1.3	🟡 Important
Pas de dépôts tiers non vérifiés	1	1.1.1	🔴 Critique

Contrôles détectifs :

CONTRÔLE	PHASE	RÉF.
Vérification périodique intégrité (debsums)	7	7.2
AIDE (changements binaires)	7	7.2.1

S8 Exploitation du PCI passthrough / accès DMA

PROBABILITÉ	🟠 Faible
IMPACT	Critique — accès mémoire hôte
PROFILS	🏢🌐
VECTEUR	VM compromise + device passthrough → DMA → mémoire hôte

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Évasion	Privilege Escalation	Escape to Host	T1611
Accès	Privilege Escalation	Exploitation for Privilege Escalation	T1068

CIS Controls v8 : 4.1, 4.8

ISO 27001:2022 : A.8.9

DESCRIPTION :

Description :

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
IOMMU activé et vérifié (VT-d / AMD-Vi)	6	6.1.3	🔴 Critique
IOMMU groups isolés	6	6.1.3	🔴 Critique
Pas de passthrough vers VM non fiables	6	6.1.3	🔴 Critique
Paramètres kernel `intel_iommu=on iommu=pt`	1	1.2.5	🔴 Critique

S9 Interception du trafic inter-nœuds

PROBABILITÉ	🟠 Faible (accès réseau interne requis)
IMPACT	Élevé — vol de données, injection
PROFILS	🏢
VECTEUR	Réseau interne — plan données/cluster

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Collecte	Credential Access	Adversary-in-the-Middle	T1557
Collecte	Collection	Data from Network Shared Drive	T1039

CIS Controls v8 : 3.10, 12.2, 12.6

ISO 27001:2022 : A.8.20, A.8.24

PCI DSS v4.0 : 4.2.1

DESCRIPTION :

Description :

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
Réseaux dédiés Ceph et migration	4	4.1.1	🔴 Critique
Chiffrement Ceph en transit (Messenger v2)	5	5.2.1	🟡 Important
Migration chiffrée	2	2.3.3	🟡 Important
VLAN isolation stricte	4	4.1	🔴 Critique

S10 Accès physique non autorisé

PROBABILITÉ	Variable
IMPACT	Critique — compromission totale
PROFILS	🏠🏢
VECTEUR	Physique

MITRE ATT&CK :

PHASE	TACTIQUE	TECHNIQUE	ID
Accès initial	Initial Access	Hardware Additions	T1200
Accès initial	Initial Access	Replication Through Removable Media	T1091
Persistance	Persistence	Pre-OS Boot	T1542
Collecte	Collection	Data from Local System	T1005

CIS Controls v8 : 3.6, 4.1, 4.6

ISO 27001:2022 : A.7.1, A.7.2, A.7.4, A.8.24

PCI DSS v4.0 : 9.1.1, 9.2.1, 9.4.1

DESCRIPTION :

Description :

Contrôles préventifs :

CONTRÔLE	PHASE	RÉF.	PRIORITÉ
Chiffrement disques (LUKS2 / ZFS encryption)	0	0.2.3	🔴 Critique (🌐)
Mot de passe GRUB	1	1.2.1	🟡 Important
Secure Boot	0	0.1.3	🟡 Important
Désactivation boot USB dans BIOS	0	0.1.1	🟡 Important
TPM 2.0 pour scellement clés	0	0.1.4	🟡 Important

1.5 — Matrice menaces ↔ phases du guide

SCÉNARIO	PH.0	PH.1	PH.2	PH.3	PH.4	PH.5	PH.6	PH.7	PH.8	PH.9
S1 SSH/Web			●	●●●	●			●●	●	
S2 Ransomware			●	●●		●		●●		●●●
S3 VM escape		●	●●				●●●	●		
S4 Cluster			●●	●	●●●			●●		
S5 BMC	●●●							●		
S6 Insider				●●●				●●●	●●	●
S7 Supply chain		●●●	●					●●		
S8 PCI/DMA		●					●●●			
S9 Interception			●●		●●●	●●				
S10 Physique	●●●	●				●●				

Légende : ● pertinent, ●● important, ●●● critique pour ce scénario

1.6 — Priorisation par profil

🏠 Homelab — Top 5 actions

#	ACTION	SCÉNARIO	PHASE
1	SSH clés uniquement + Fail2Ban	S1	3
2	Mises à jour auto sécurité Debian	S7	1
3	2FA sur le web UI	S1, S6	3
4	Backups PBS chiffrées + hors site	S2	9
5	Firewall PVE politique restrictive	S1	4

🏢 Production — Top 10

#	ACTION	SCÉNARIO	PHASE
1-5	Tout le Top 5 homelab	—	—
6	RBAC strict comptes nommés	S6	3
7	Segmentation VLAN complète	S4, S9	4
8	Chiffrement Corosync	S4	2
9	Logs centralisés hors contrôle admin PVE	S6	7
10	BMC isolé VLAN OOB	S5	0

🌐 Exposé internet — Ajouts critiques

#	ACTION	SCÉNARIO	PHASE
11	VPN unique entrée management	S1	3
12	WebAuthn/FIDO2 (résistant phishing)	S1	3
13	Profils AppArmor QEMU	S3	6
14	BMC jamais exposé internet	S5	0
15	Chiffrement disques complet (LUKS2)	S10	0
16	Secure Boot	S10	0
17	IOMMU vérifié pour tout passthrough	S8	6

1.7 — Références

SOURCE	DESCRIPTION	DATE
BSI — Sicherheitsanalyse von KVM (KVMSec) v1.0.1	Analyse de sécurité KVM/QEMU avec recommandations (AppArmor/sVirt, seccomp, devices)	2017
QEMU Project — Security Documentation	Modèle de sécurité QEMU, entités non fiables, principe de moindre privilège	En cours
Red Hat — Hardening QEMU through continuous security testing	Mécanismes de durcissement continu (fuzzing, Coverity, analyse statique)	2025
OpenStack Security Guide — Hardening the Virtualization Layers	Recommandations minimisation QEMU, compiler hardening, sVirt/AppArmor	En cours
CIS — Debian Linux 13 Benchmark v1.0.0	Benchmark de configuration sécurisée Debian 13	2025-12-16
MITRE — ATT&CK Framework v16	Tactiques, techniques et procédures adversaires	2025
CIS — Controls v8	Contrôles de sécurité prioritisés	2021
Proxmox Forum — Security Hardening threads	Retours communautaires, cas BMC/ ransomware	2021-2026
CVE databases (OpenCVE, CVEDetails, Akaoma)	Vulnérabilités Proxmox VE documentées	Continu

Navigation : ← 00-introduction.md | 02-pre-installation.md →

-e

02 — Phase 0 : Avant l'installation

> **Version** : 0.2.0 **Date** : 2026-03-20 **Statut** : Rédaction initiale — Format CIS hybride **Licence** : CC BY-SA 4.0 **Base de référence** : CIS Debian Linux 13 Benchmark v1.0.0 (2025-12-16) **Scénarios du threat model** : S5, S7, S10

Conventions du format

Chaque contrôle suit la structure du CIS Benchmark, enrichie de champs spécifiques à Proxmox VE :

CHAMP	DESCRIPTION
Profile Applicability	Level 1 (baseline) / Level 2 (defense-in-depth) — conforme au CIS
Applicabilité PVE	🏠 Homelab / 🏢 Production / 🌐 Exposé internet
Réf. CIS Debian 13	Numéro de section CIS correspondant (si applicable)
CIS Controls v8	Safeguard CIS Controls v8 mappé
MITRE ATT&CK	Techniques / Tactics / Mitigations
ISO 27001:2022	Contrôle Annex A mappé
PCI DSS v4.0	Exigence PCI DSS mappée
Scénario threat model	Référence S1-S10 du chapitre 01
Statut PVE 9	✅ Validé / ⚠️ Partiel / 🧪 Expérimental
Description	Ce que fait le contrôle
Rationale	Pourquoi ce contrôle est nécessaire
Impact	Conséquences opérationnelles
Audit	Commande(s) de vérification + résultat attendu
Remédiation	Commande(s) d'application
Valeur par défaut	Valeur sur une installation fraîche
Rollback	Procédure de retour arrière (ajout Proxmox)
Spécificité PVE	Notes spécifiques à Proxmox (ajout Proxmox)
Références	Sources additionnelles

0.1 — Préparation matérielle

0.1.1 Mise à jour firmware, BIOS et microcode CPU Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	Hors périmètre CIS (prérequis matériel)
CIS CONTROLS V8	2.2 — Ensure Authorized Software is Currently Supported
MITRE ATT&CK	T1542 (Pre-OS Boot), T1195 (Supply Chain Compromise)
ISO 27001:2022	A.8.8 — Management of technical vulnerabilities
PCI DSS V4.0	6.3.3 — Install security patches within one month
SCÉNARIO THREAT MODEL	S5 (BMC), S10 (accès physique)
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

Reboot nécessaire. Un flash de BIOS raté peut bricker le serveur — prévoir un accès console physique ou IPMI. Certaines mises à jour de microcode peuvent réduire très légèrement les performances (~1-3%) sur les workloads affectés par les mitigations Spectre.

🔍 AUDIT

Audit :

Version BIOS/UEFI

dmidecode -t bios | grep -E "Vendor|Version|Release Date"

Résultat attendu : version correspondant à la dernière release constructeur

Version microcode CPU

journalctl -k | grep -i microcode

ou :

cat /proc/cpuinfo | grep -m1 microcode

Résultat attendu : version récente (comparer avec les advisories Intel/AMD)

Vérification des mitigations CPU actives

cat /sys/devices/system/cpu/vulnerabilities/*

Résultat attendu : "Mitigation:" sur chaque ligne (pas "Vulnerable")

```
**Remédiation** :
```

1. Firmware BIOS : procédure constructeur (Dell, HP, Lenovo, Supermicro)

Télécharger depuis le site officiel, vérifier le checksum, appliquer

2. Microcode CPU via paquets Debian :

apt update

Intel

apt install -y intel-microcode

AMD

apt install -y amd64-microcode

3. Redémarrer pour appliquer

reboot

```
**Valeur par défaut** : Microcode distribué avec le kernel Debian. Peut ne pas être la

**Rollback** : Pour le microcode Debian : `apt purge intel-microcode` ou `amd64-microco

**Spécificité PVE** : Le kernel Proxmox (basé sur Ubuntu) charge le microcode depuis l'

---
```

0.1.2 Sécurisation BMC / IPMI / iDRAC / iLO

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏢🌐 (N/A si matériel sans BMC)
RÉF. CIS DEBIAN 13	Hors périmètre CIS (couche matérielle)
CIS CONTROLS V8	4.1 — Establish and Maintain a Secure Configuration Process
MITRE ATT&CK	T1200 (Hardware Additions), T1133 (External Remote Services), T1078 (Valid Accounts)
ISO 27001:2022	A.8.9 — Configuration management, A.5.15 — Access control
PCI DSS V4.0	2.2.1 — Develop configuration standards for system components
SCÉNARIO THREAT MODEL	S5 (Compromission BMC)
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

Faible. Nécessite un accès au réseau BMC pour la configuration initiale.

🔍 AUDIT

Audit :

Vérifier que le BMC N'EST PAS accessible depuis le réseau management PVE

(exécuter depuis un hôte sur le réseau management, PAS le réseau OOB)

nmap -sV <adresse_IP_BMC> -p 80,443,623,5900 --max-retries 1

Résultat attendu : tous les ports filtrés ou host unreachable

(le BMC ne doit être joignable QUE depuis le VLAN OOB)

Vérifier les protocoles actifs (depuis le réseau OOB)

ipmitool -I lanplus -H <BMC_IP> -U admin -P <password> lan print 1

Vérifier : Auth Type = PASSWORD uniquement n'est pas acceptable

Résultat attendu : des méthodes d'authentification fortes

```
**Remédiation** :

| Action | Priorité | Détail |
|--------|----------|--------|
| Changer les credentials par défaut | 🔴 Critique | Mot de passe ≥ 16 caractères
| Isoler sur VLAN OOB dédié | 🔴 Critique | VLAN non routable vers internet ni ve
| Désactiver HTTP (forcer HTTPS) | 🔴 Critique | Via l'interface web BMC ou CLI i
| Désactiver SNMP v1/v2c | 🟡 Important | Migrer vers SNMPv3 si monitoring nécess
| Désactiver Telnet | 🔴 Critique | Via l'interface web BMC |
| Désactiver IPMI-over-LAN | 🟡 Important | Si non utilisé pour le monitoring |
| Mettre à jour le firmware BMC | 🔴 Critique | Depuis le site constructeur |
| Installer certificat TLS | 🟡 Important | Si le BMC supporte l'import de certif
| Activer le System Event Log | 🟡 Important | Pour la traçabilité des accès BMC

**Valeur par défaut** : Credentials usine (`admin`/`admin`, `ADMIN`/`ADMIN`, ou s

**Rollback** : Reset usine du BMC via le bouton physique ou la procédure construc

**Spécificité PVE** : Proxmox n'a aucune interaction directe avec le BMC. La sécu

**Références** :
- Forum Proxmox — cas documentés de ransomware via BMC
- NIST SP 800-123 — Guide to General Server Security

---
```

0.1.3 Activer Secure Boot (UEFI) Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Hors périmètre CIS
CIS CONTROLS V8	4.1 — Establish and Maintain a Secure Configuration Process
MITRE ATT&CK	T1542.003 (Bootkit), T1014 (Rootkit)
ISO 27001:2022	A.8.9 — Configuration management
PCI DSS V4.0	2.2.1
SCÉNARIO THREAT MODEL	S10 (accès physique)
STATUT PVE 9	⚠️ Partiel — fonctionnel mais incompatible avec certains modules tiers

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

Moyen à élevé. Les modules kernel non signés ne se chargeront pas. Cela affecte :

- Drivers NVIDIA propriétaires (GPU passthrough) — ❌ ne fonctionneront pas sans signature personnalisée
- Certains modules DRBD — ⚠️ vérifier la compatibilité
- Modules kernel out-of-tree tiers — ❌ bloqués
- ZFS (inclus dans le kernel PVE) — ✅ fonctionne
- Modules kernel Proxmox standard — ✅ fonctionnent

🔍 AUDIT

Audit :

```
mokutil --sb-state
```

Résultat attendu : "SecureBoot enabled"

Alternative si mokutil non installé :

dmesg | grep -i "secure boot"

Résultat attendu : "Secure boot enabled"

```
**Remédiation** :
1. Activer Secure Boot dans le BIOS/UEFI
2. Installer PVE normalement (ou redémarrer si déjà installé)
3. Vérifier que le système démarre et que tous les modules nécessaires se ch
```

lsmod | grep -E "zfs|kvm|vhost"

Résultat attendu : modules présents et chargés

```
**Valeur par défaut** : Dépend du matériel et du BIOS. Souvent désactivé sur

**Rollback** : Désactiver Secure Boot dans le BIOS/UEFI.

**Spécificité PVE** : Proxmox VE 9 supporte Secure Boot. Le kernel PVE et se

---
```

0.1.4 Activer et configurer TPM 2.0 Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Hors périmètre CIS
CIS CONTROLS V8	3.6 — Encrypt Data on End-User Devices
MITRE ATT&CK	T1542 (Pre-OS Boot), M1026 (Privileged Account Management)
ISO 27001:2022	A.8.24 — Use of cryptography
PCI DSS V4.0	3.5.1
SCÉNARIO THREAT MODEL	S10 (accès physique)
STATUT PVE 9	✅ Validé (vTPM pour VM), ⚠️ Partiel (auto-unlock LUKS)

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

Faible. Le TPM est transparent une fois configuré. L'auto-unlock via TPM protège contre le vol de disques mais PAS contre un attaquant ayant accès à l'ensemble du serveur (le TPM est sur la carte mère).

🔍 AUDIT

Audit :

cat /sys/class/tpm/tpm0/tpm_version_major 2>/dev/null

Résultat attendu : 2

dmesg | grep -i tpm

Résultat attendu : lignes indiquant un TPM détecté et initialisé

```
**Remédiation** :
1. Activer le TPM 2.0 dans le BIOS/UEFI
2. Vérifier la détection par le kernel

Pour l'auto-unlock LUKS via TPM (si LUKS est utilisé) :
```

apt install -y systemd-cryptenroll tpm2-tools

Enregistrer la clé TPM pour un volume LUKS

systemd-cryptenroll /dev/sdX3 --tpm2-device=auto --tpm2-pcrs=0+1+7

PCR 0 = firmware, PCR 1 = firmware config, PCR 7 = Secure Boot state

Générer une clé de récupération (IMPÉRATIF)

systemd-cryptenroll /dev/sdX3 --recovery-key

STOCKER CETTE CLÉ HORS LIGNE (password manager, coffre-fort)

```
**Valeur par défaut** : TPM souvent désactivé dans le BIOS par défaut

**Rollback** : Supprimer l'enrollment TPM : `systemd-cryptenroll /dev/

**Spécificité PVE** :
- PVE 9 supporte le vTPM (TPM virtuel) pour les VM guests — utile pour
- L'auto-unlock LUKS via TPM est une fonctionnalité Debian/systemd sta
- **Alternatives sans TPM** : `dropbear-initramfs` (unlock SSH dans l'

---
```

0.1.5 Documenter l'inventaire matériel Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	Hors périmètre CIS
CIS CONTROLS V8	1.1 — Establish and Maintain Detailed Enterprise Asset Inventory
MITRE ATT&CK	T1082 (System Information Discovery) — contrôle défensif
ISO 27001:2022	A.5.9 — Inventory of information and other associated assets
PCI DSS V4.0	9.9.1 — Maintain a listing of devices
SCÉNARIO THREAT MODEL	Tous
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact : Nul.

🔍 **AUDIT**

Audit :

Script de génération d'inventaire rapide

```
echo "=== SYSTEM ===" && dmidecode -t system | grep -E "Manufacturer|Product|Serial" && \

echo "=== BIOS ===" && dmidecode -t bios | grep -E "Vendor|Version|Release" && \

echo "=== CPU ===" && lscpu | grep -E "Model name|Socket|Thread" && \

echo "=== RAM ===" && free -h | grep Mem && \
```

```
echo "=== STORAGE ===" && lsblk -d -o
NAME,SIZE,MODEL,SERIAL && \

echo "=== NETWORK ===" && ip -br link show && \

echo "=== PVE ===" && pveversion -v 2>/dev/null && \

echo "=== KERNEL ===" && uname -r
```

Résultat attendu : informations complètes pour alimenter le tableau d'inventaire

```
**Remédiation** :

Créer et maintenir un fichier d'inventaire par nœud. Modèle :
```

CHAMP	VALEUR
Hostname	pve-node01
Modèle	Dell PowerEdge R750
N° série	XXXXXXX
CPU	2x Intel Xeon Gold 6338
RAM	256 Go DDR4 ECC
Disques OS	2× 480 Go SSD SATA (RAID1)
Disques VM	4× 1.92 To NVMe
Réseau	2× 25 GbE + 2× 1 GbE
BIOS	v2.12.2 (2025-10-15)
BMC	iLO 5 v3.10
PVE	9.1-3
Kernel	6.12.6-1-pve
Emplacement	Rack A, U12-14
VLAN Mgmt	10 — 10.0.10.11/24
VLAN BMC	99 — 10.0.99.11/24
Dernier audit	2026-03-20

```
Mettre à jour après **chaque** changement de matériel ou de conf

**Valeur par défaut** : Aucun inventaire.

---
```

0.2 — Choix d'installation

0.2.1 Sélectionner la méthode d'installation

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	Prérequis global (conditionne 1.1.x partitionnement)
CIS CONTROLS V8	4.1 — Establish and Maintain a Secure Configuration Process
ISO 27001:2022	A.8.9 — Configuration management
SCÉNARIO THREAT MODEL	S7 (supply chain), S10 (accès physique)
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

Décision architecturale irréversible. L'installateur ISO Proxmox ne propose pas d'option LUKS pour ext4/XFS. Les options de chiffrement dans l'installateur PVE n'existent que pour ZFS.

CRITÈRE	ISO PROXMOX	DEBIAN 13 + DÉPÔT PVE
Simplicité	✅ Assistée	❌ Manuelle
Support Proxmox GmbH	✅ Méthode principale	⚠️ Supportée
Partitionnement CIS (1.1.x)	❌ Schéma fixe	✅ Contrôle total
LUKS sur ext4/LVM	❌ Non disponible	✅ Via installateur Debian
ZFS encryption	✅ Disponible	⚠️ Installation manuelle
Conformité CIS complète	❌ Partitions non séparées	✅ Possible
Risque opérationnel	Faible	Moyen

Remédiation (recommandation par profil) :

PROFIL	RECOMMANDATION
🏠 Homelab	ISO Proxmox — simple, fiable
🏢 Prod sans exigence CIS strict	ISO Proxmox + ZFS encryption si chiffrement requis
🏢🌐 Prod avec conformité CIS ou LUKS obligatoire	Debian 13 + dépôt Proxmox

Si Debian 13 + dépôt PVE : suivre https://pve.proxmox.com/wiki/Install_Proxmox_VE_on_Debian_13_Trixie

Pièges documentés :

- Ne PAS installer d'environnement de bureau
- Sélectionner uniquement `Standard system utilities` + `SSH server`
- Configurer un hostname FQDN résolvable (requis par Proxmox)
- Retirer le kernel Debian APRÈS vérification du boot sur kernel PVE

Valeur par défaut : N/A (choix initial).

Spécificité PVE : L'installateur ISO PVE utilise un partitionnement prédéfini : une partition EFI, un VG LVM avec root + swap (ou ZFS avec root pool + data pool). Ce schéma ne crée PAS de partitions séparées pour `/tmp`, `/var`, `/var/log`, `/var/log/audit`, `/home`.

0.2.2 Configurer le partitionnement selon CIS

Level 1

PROFILE APPLICABILITY	Level 1 — Server (partitions de base), Level 2 — Server (toutes)
APPLICABILITÉ PVE	🏠 (simplifié) 🏢🌐 (complet)
RÉF. CIS DEBIAN 13	1.1.2.1 à 1.1.2.7
CIS CONTROLS V8	4.8 — Uninstall or Disable Unnecessary Services
MITRE ATT&CK	T1499.001 (OS Exhaustion Flood), M1022 (Restrict File and Directory Permissions)
ISO 27001:2022	A.8.9 — Configuration management
PCI DSS V4.0	2.2.1, 2.2.4
SCÉNARIO THREAT MODEL	S2 (ransomware), S7 (supply chain)
STATUT PVE 9	✅ Validé (si Debian-first) / ⚠️ Non conforme (si ISO PVE)

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

Nul si fait à l'installation. Irréversible après installation (réinstallation nécessaire pour le partitionnement, options de montage modifiables à chaud).

🔍 AUDIT

Audit :

Vérifier que les partitions existent

for mp in /tmp /var /var/log /var/log/audit /home /var/tmp; do

```
findmnt -n "$mp" > /dev/null 2>&1 && echo "PASS: $mp est une partition séparée" \
  echo "FAIL: $mp n'est PAS une partition séparée"
done
```

Vérifier les options de montage

```
for mp in /tmp /dev/shm /var/tmp; do
opts=$(findmnt -n -o OPTIONS "$mp" 2>/dev/null)
echo "$mp: $opts"
echo "$opts" | grep -q "nosuid" && echo " nosuid: PASS" || echo " nosuid: FAIL"
echo "$opts" | grep -q "nodev" && echo " nodev: PASS" || echo " nodev: FAIL"
echo "$opts" | grep -q "noexec" && echo " noexec: PASS" || echo " noexec: FAIL"
done
```

```
**Remédiation** :

Schéma complet (installateur Debian, conformité CIS L

| Point de montage | CIS | Level | Taille recommandée
|------------------|-----|-------|--------------------
| `/` | — | — | 20-50 Go | `defaults` |
| `/boot` | — | — | 1 Go | `defaults,nosuid,nodev,noe
| `/boot/efi` | — | — | 512 Mo | `defaults,nosuid,nod
| `/tmp` | 1.1.2.1 | L1 | 5-10 Go | `defaults,nosuid,
| `/dev/shm` | 1.1.2.2 | L1 | tmpfs | `defaults,nosui
| `/home` | 1.1.2.3 | L1 | 5-10 Go | `defaults,nosuid
| `/var` | 1.1.2.4 | L1 | 20-50 Go | `defaults,nosuid
| `/var/tmp` | 1.1.2.5 | L1 | 5-10 Go | `defaults,nos
| `/var/log` | 1.1.2.6 | L1 | 10-20 Go | `defaults,no
| `/var/log/audit` | 1.1.2.7 | L1 | 5-10 Go | `defaul
| `/var/lib/vz` | PVE | — | Max ou volume dédié | `de
| swap | — | — | 1-2x RAM (max 32 Go) | `sw` |

**Valeur par défaut** : L'installateur ISO PVE crée u

**Rollback** : Les options de montage sont modifiable

**Spécificité PVE** : `/var/lib/vz` est le répertoire

---
```

0.2.3 Chiffrer les disques à l'installation

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Hors périmètre CIS (recommandation complémentaire)
CIS CONTROLS V8	3.6 — Encrypt Data on End-User Devices, 3.9 — Encrypt Data on Removable Media
MITRE ATT&CK	T1005 (Data from Local System), T1025 (Data from Removable Media), M1041 (Encrypt Sensitive Information)
ISO 27001:2022	A.8.24 — Use of cryptography
PCI DSS V4.0	3.5.1 — Render PAN unreadable anywhere it is stored
SCÉNARIO THREAT MODEL	S10 (accès physique)
STATUT PVE 9	⚠️ Partiel — ZFS encryption natif dans l'installateur, LUKS uniquement via Debian-first

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

- Surcoût performance : 3-5% (LUKS2 + AES-NI), 5-8% (ZFS encryption) sur I/O séquentiel
- Nécessite une intervention au boot (saisie de passphrase) ou une configuration auto-unlock (TPM, dropbear, tang/clevis)
- Complexité accrue de la gestion des clés et de la recovery

🔍 AUDIT

Audit :

Vérifier le chiffrement LUKS

lsblk -f | grep -i crypt

Résultat attendu : volumes de type "crypt" visibles

Vérifier le chiffrement ZFS

zfs get encryption -r rpool 2>/dev/null | grep -v off

Résultat attendu : datasets avec encryption=aes-256-gcm

Vérifier l'état global

cryptsetup status cryptlvm 2>/dev/null || echo "Pas de LUKS actif"

```
**Remédiation** :

Trois options (voir 0.2.1 pour le choix d'insta

**Option A — ZFS native encryption (via install
Sélectionner ZFS dans l'installateur et activer
```

zfs create -o encryption=aes-256-gcm \

-o keylocation=prompt \

-o keyformat=passphrase \

rpool/encrypted-vms

```
**Option B — LUKS2 (via installateur Debian)**
Choisir « Guided — use entire disk and set up e

**Option C — LUKS sous ZFS (post-installation,
Conversion in-place via live boot. Réservé aux

**Impératifs communs** :
```

Sauvegarder l'en-tête LUKS (si LUKS)

cryptsetup luksHeaderBackup /dev/sdX3 --header-backup-file /root/luks-header-sdX3.img

STOCKER HORS SITE

Générer et stocker une clé de récupération

systemd-cryptenroll /dev/sdX3 --recovery-key 2>/dev/null

ou noter la passphrase dans un gestionnaire de MDP hors ligne

```
**Valeur par défaut** : Aucun chiffrement.

**Rollback** : Le chiffrement une fois appliqué

**Spécificité PVE** :
- L'installateur ISO PVE **ne propose PAS LUKS
- ZFS native encryption ne chiffre pas le root
- Pour un chiffrement total (full disk encrypti
- Le déverrouillage distant via `dropbear-initr
```

apt install dropbear-initramfs

echo 'DROPBEAR_OPTIONS="-s -c cryptroot-unlock"' > /etc/dropbear/initramfs/dropbear.conf

Ajouter votre clé publique SSH dans /etc/dropbear/initramfs/authorized_keys

update-initramfs -u

```
---
```

0.2.4 Planifier l'architecture réseau

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠 (simplifié) 🏢🌐 (complet)
RÉF. CIS DEBIAN 13	Hors périmètre CIS (architecture)
CIS CONTROLS V8	12.2 — Establish and Maintain a Secure Network Architecture
MITRE ATT&CK	T1557 (Adversary-in-the-Middle), T1021 (Remote Services), M1030 (Network Segmentation)
ISO 27001:2022	A.8.22 — Segregation of networks
PCI DSS V4.0	1.2.1 — Restrict inbound and outbound traffic
SCÉNARIO THREAT MODEL	S1, S4, S5, S9
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact : Nul (planification uniquement).

🔧 REMÉDIATION

Remédiation :

Architecture VLAN de référence (🏢🌐) :

VLAN	NOM	RÔLE	PLAGE EXEMPLE	PORTS PVE
10	Management	Web UI :8006, SSH, API	10.0.10.0/24	8006/tcp, 22/tcp
20	VM/CT	Trafic applicatif guests	10.0.20.0/24+	Variable
30	Stockage	NFS, iSCSI, Ceph public	10.0.30.0/24	2049, 3260, 6789
40	Cluster	Corosync, migration, réplication	10.0.40.0/24	5405/udp, 60000-60050/tcp
41	Ceph cluster	Réplication OSD (si Ceph)	10.0.41.0/24	6800-7300/tcp
99	OOB	BMC/IPMI	10.0.99.0/24	443/tcp (BMC web)

Architecture simplifiée (🏠) :

Réseau plat avec firewall PVE pour restreindre l'accès aux ports management. Pas de VLAN nécessaire.

Valeur par défaut : Pas de segmentation. Un seul bridge `vmbr0` sur l'interface principale.

Spécificité PVE : Proxmox utilise des bridges Linux (`vmbr0` , `vmbr1` ...) pour la connectivité réseau. Chaque VLAN peut être associé à un bridge dédié ou utiliser des VLAN-aware bridges. La configuration détaillée est couverte en Phase 4.

0.3 — Checklist pré-installation

```
MATÉRIEL
[ ] 0.1.1 — Firmware/BIOS à jour
[ ] 0.1.1 — Microcode CPU installé
[ ] 0.1.2 — Credentials BMC changés
[ ] 0.1.2 — BMC isolé sur VLAN OOB
[ ] 0.1.2 — Protocoles non chiffrés BMC dé
[ ] 0.1.3 — Secure Boot : décision documer
[ ] 0.1.4 — TPM 2.0 : décision documentée
[ ] 0.1.5 — Inventaire matériel rempli

ARCHITECTURE
[ ] 0.2.1 — Méthode d'installation choisie
[ ] 0.2.2 — Schéma de partitionnement défi
[ ] 0.2.3 — Stratégie de chiffrement défir
[ ] 0.2.4 — Architecture réseau VLAN plani

PRÉREQUIS
[ ] Accès console hors-bande vérifié
[ ] ISO d'installation préparée (checksum
[ ] Procédure de déverrouillage distant pl
```

Navigation : ← 01-threat-model.md | 03-os-debian-durci.md →

-e

CHAPITRE 2 SUR 5

Phase 1 — OS Debian Durci

03 — Phase 1 : Durcissement OS Debian 13

> **Version** : 0.2.0 **Date** : 2026-03-20 **Statut** : Rédaction initiale — Format CIS hybride **Licence** : CC BY-SA 4.0 **Base de référence** : CIS Debian Linux 13 Benchmark v1.0.0 (2025-12-16) **Scénarios du threat model** : S1, S2, S3, S6, S7

1.1 — Gestion des paquets et dépôts

1.1.1 Configurer les dépôts Proxmox et vérifier les signatures GPG

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	1.2.1.1 — Ensure GPG keys are configured
CIS CONTROLS V8	2.2 — Ensure Authorized Software is Currently Supported
MITRE ATT&CK	T1195.002 (Compromise Software Supply Chain), M1051 (Update Software)
ISO 27001:2022	A.8.8 — Management of technical vulnerabilities, A.8.10 — Information deletion
PCI DSS V4.0	6.3.3
SCÉNARIO THREAT MODEL	S7 (supply chain)
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact : Faible. Sans abonnement, les mises à jour via le dépôt no-subscription sont fonctionnelles mais n'ont pas le même niveau de test que le dépôt enterprise.

🔍 AUDIT

Audit :

Vérifier que apt update fonctionne sans erreur

```
apt update 2>&1 | grep -E "Err:|401|
Failed"
```

Résultat attendu : aucune sortie (pas d'erreurs)

Vérifier les clés GPG Proxmox

```
apt-key list 2>/dev/null | grep -A1
"proxmox" || \

ls /etc/apt/trusted.gpg.d/proxmox-*
```

Résultat attendu : clé Proxmox Release Key présente

Vérifier qu'aucun dépôt n'a AllowUnauthenticated

```
grep -r "AllowUnauthenticated\|
AllowInsecureRepositories" /etc/apt/ 2>/
dev/null
```

Résultat attendu : aucune sortie

```
**Remédiation** :

Avec abonnement enterprise (🏢🌐 recomman
```

Vérifier /etc/apt/sources.list.d/pve-enterprise.list

cat /etc/apt/sources.list.d/pve-enterprise.list

Doit contenir : deb https://enterprise.proxmox.com/debian/pve trixie pve-enterprise

apt update # Doit fonctionner sans erreur 401

```
Sans abonnement (🏠) :
```

Désactiver le dépôt enterprise

sed -i 's/^deb/#deb/' /etc/apt/sources.list.d/pve-enterprise.list

Ajouter le dépôt no-subscription

echo "deb http://
download.proxmox.com/debian/pve
trixie pve-no-subscription" \

> /etc/apt/sources.list.d/pve-no-subscription.list

apt update

```
**Valeur par défaut** : Dépôt enterprise

**Rollback** :
```

sed -i 's/^#deb/deb/' /etc/apt/
sources.list.d/pve-enterprise.list

rm -f /etc/apt/sources.list.d/pve-no-subscription.list

```
**Spécificité PVE** : Ne jamais ajouter d

---
```

1.1.2

Configurer les mises à jour automatiques de sécurité

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	1.2.2.1 — Ensure updates, patches, and additional security software are installed
CIS CONTROLS V8	7.3 — Perform Automated Operating System Patch Management
MITRE ATT&CK	T1190 (Exploit Public-Facing Application), M1051 (Update Software)
ISO 27001:2022	A.8.8 — Management of technical vulnerabilities
PCI DSS V4.0	6.3.3 — Install security patches within one month
SCÉNARIO THREAT MODEL	S3 (VM escape via CVE QEMU), S7 (supply chain)
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact : Faible. Les correctifs de sécurité Debian sont stables. Un reboot peut être nécessaire (kernel) mais `Automatic-Reboot` est désactivé.

🔍 **AUDIT**

Audit :

dpkg -l unattended-upgrades | grep -q "^ii" && echo "PASS: installé" || echo "FAIL: non installé"

systemctl is-enabled unattended-upgrades && echo "PASS: activé" || echo "FAIL: désactivé"

grep -v "^//" /etc/apt/apt.conf.d/50unattended-upgrades | grep -q "Debian-Security" \

&& echo "PASS: sécurité Debian configurée" || echo "FAIL: non configuré"

```
**Remédiation** :
```

apt install -y unattended-upgrades apt-listchanges

dpkg-reconfigure -plow unattended-upgrades

```
Contenu de `/etc/apt/apt.conf.d/50ur
```

Unattended-Upgrade::Origins-Pattern {

"origin=Debian,codename=${distro_codename}-security,label=Debian-Security";

// NE PAS ajouter de ligne pour les dépôts Proxmox

};

Unattended-Upgrade::Mail "admin@example.com";

Unattended-Upgrade::MailReport "on-change";

Unattended-Upgrade::Automatic-Reboot "false";

Unattended-Upgrade::Remove-Unused-Dependencies "true";

Unattended-Upgrade::Remove-New-Unused-Dependencies "true";

```
Contenu de `/etc/apt/apt.conf.d/20au
```

APT::Periodic::Update-Package-Lists "1";

APT::Periodic::Unattended-Upgrade "1";

APT::Periodic::Download-Upgradeable-Packages "1";

APT::Periodic::AutocleanInterval "7";

```
**Valeur par défaut** : `unattended-

**Rollback** : `apt purge unattended

**Spécificité PVE** : **Ne JAMAIS in

---
```

1.1.3 Supprimer les paquets inutiles

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	2.1.x — Ensure [service] is not installed
CIS CONTROLS V8	4.8 — Uninstall or Disable Unnecessary Services
MITRE ATT&CK	T1543 (Create or Modify System Process), M1042 (Disable or Remove Feature or Program)
ISO 27001:2022	A.8.9 — Configuration management
PCI DSS V4.0	2.2.4 — Only necessary services are enabled
SCÉNARIO THREAT MODEL	S1, S3
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact : Faible.

🔍 **AUDIT**

Audit :

for pkg in telnet rsh-client rsh-server xinetd tftp-server nis \

avahi-daemon cups talk inetutils-talk postfix exim4; do

dpkg -l "$pkg" 2>/dev/null | grep -q "^ii" && echo "FAIL: $pkg installé" \

echo "PASS: $pkg absent"

done

```
**Remédiation** :
```

apt purge -y telnet rsh-client rsh-server xinetd tftp-server nis \

avahi-daemon cups cups-client talk inetutils-talk 2>/dev/null

apt autoremove -y

```
**Valeur par défaut** : Varie

---
```

1.2 — Noyau et paramètres de démarrage

1.2.1 Configurer un mot de passe GRUB

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	1.4.1 — Ensure bootloader password is set
CIS CONTROLS V8	4.1
MITRE ATT&CK	T1542.003 (Bootkit), M1046 (Boot Integrity)
ISO 27001:2022	A.8.5 — Secure authentication
PCI DSS V4.0	2.2.1
SCÉNARIO THREAT MODEL	S10 (accès physique)
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact : Faible. Le boot normal ne demande pas le mot de passe (paramètre `--unrestricted`). Le mot de passe n'est demandé que pour l'édition des entrées GRUB.

🔍 AUDIT

Audit :

grep -q "^set superusers" /boot/grub/grub.cfg && echo "PASS" || echo "FAIL"

grep -q "^password_pbkdf2" /boot/grub/grub.cfg && echo "PASS" || echo "FAIL"

```
**Remédiation** :
```

Générer le hash

grub-mkpasswd-pbkdf2

(saisir le mot de passe, noter le hash grub.pbkdf2.sha512.10000.XXXXX)

Configurer dans /etc/grub.d/40_custom :

cat >> /etc/grub.d/40_custom << 'EOF'

set
superusers="grubadmin"

password_pbkdf2
grubadmin
grub.pbkdf2.sha512.10000.<VOTRE_HASH>

EOF

Permettre le boot normal sans mot de passe

sed -i 's/class gnu-linux/
class gnu-linux --
unrestricted/' /etc/
grub.d/10_linux

update-grub

```
**Valeur par défaut** :

**Rollback** : Supprimer

---
```

1.2.2 Appliquer les paramètres sysctl réseau

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	3.3.1 à 3.3.11
CIS CONTROLS V8	4.1, 4.8
MITRE ATT&CK	T1557 (AitM), T1499 (Endpoint DoS), M1037 (Filter Network Traffic)
ISO 27001:2022	A.8.20 — Network security, A.8.22 — Segregation of networks
PCI DSS V4.0	1.2.1, 1.3.1
SCÉNARIO THREAT MODEL	S1, S4, S9
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact : Faible.
Exception critique :
`net.ipv4.ip_forward`

est nécessaire pour le réseau des VM. Ne PAS le désactiver si des VM ont un accès réseau.

🔍 AUDIT

Audit :

Vérifier les paramètres critiques

```
declare -A expected=(
["net.ipv4.conf.all.rp_filter"]="1"
["net.ipv4.conf.all.accept_redirects"]="0"
["net.ipv4.conf.all.send_redirects"]="0"
["net.ipv4.conf.all.accept_source_route"]="0"
["net.ipv4.conf.all.log_martians"]="1"
["net.ipv4.tcp_syncookies"]="1"
["net.ipv4.icmp_echo_ignore_broadcasts"]="1"
["net.ipv6.conf.all.accept_redirects"]="0"
["net.ipv6.conf.all.accept_source_route"]="0"
)
for key in "${!expected[@]}"; do
val=$(sysctl -n "$key" 2>/dev/null)
```

```
[ "$val" = "$
{expected[$key]}" ]
&& echo "PASS:
$key = $val" \

  echo "FAIL: $key =
  $val (attendu: $
  {expected[$key]})"

done
```

```
**Remédiation** :

Créer `/etc/sysctl.
```

CIS 3.3.1 — Source routed packets

```
net.ipv4.conf.all.accept_source_route
= 0

net.ipv4.conf.default.accept_source_route
= 0

net.ipv6.conf.all.accept_source_route
= 0

net.ipv6.conf.default.accept_source_route
= 0
```

CIS 3.3.2 — ICMP redirects

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

CIS 3.3.3 — Secure ICMP redirects

net.ipv4.conf.all.secure_redirects = 0

net.ipv4.conf.default.secure_redirects = 0

CIS 3.3.4 — Suspicious packets logged

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians
= 1

CIS 3.3.5 — Broadcast ICMP requests

net.ipv4.icmp_echo_ignore_broadcasts
= 1

CIS 3.3.6 — Bogus ICMP responses

net.ipv4.icmp_ignore_bogus_error_responses
= 1

CIS 3.3.7 — Reverse path filtering

net.ipv4.conf.all.rp_filter
= 1

net.ipv4.conf.default.rp_filter
= 1

CIS 3.3.8 — TCP SYN cookies

net.ipv4.tcp_syncookies = 1

CIS 3.3.9 — IPv6 router advertisements

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

CIS 3.3.10 — Do not send ICMP redirects (not a router)

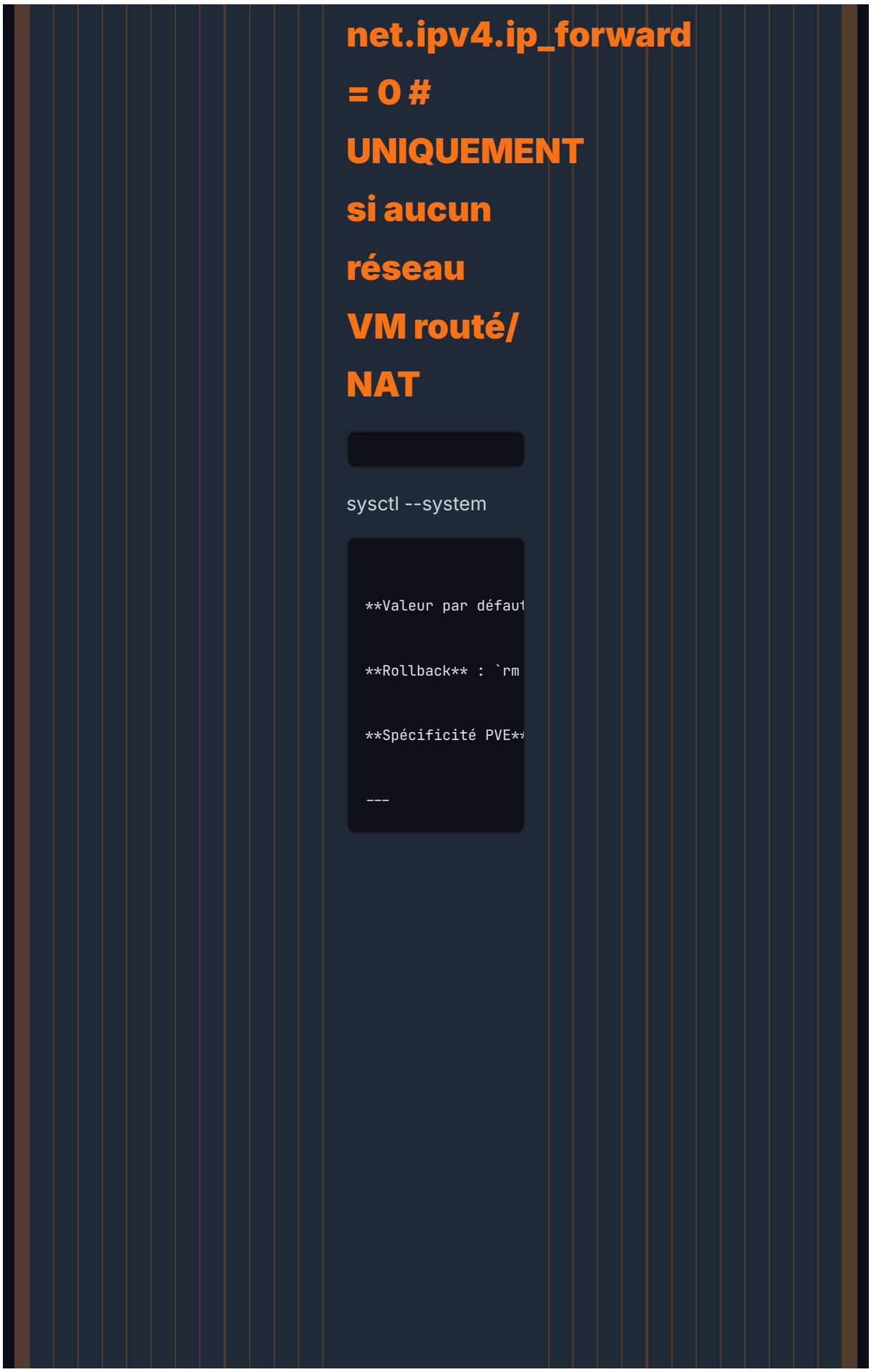
net.ipv4.conf.all.send_redirects = 0

```
net.ipv4.conf.default.send_redirects
= 0
```

CIS 3.3.11 — IP forwarding

ATTENTION PVE : NE PAS DÉSACTIVER si les VM ont un accès réseau !

Proxmox gère ce paramètre — il DOIT être à 1 pour le réseau VM


net.ipv4.ip_forward = 0 # UNIQUEMENT si aucun réseau VM routé/ NAT
sysctl --system
**Valeur par défaut
Rollback : `rm
Spécificité PVE

1.2.3 Appliquer les paramètres sysctl kernel

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	1.5.1 à 1.5.4
CIS CONTROLS V8	4.1
MITRE ATT&CK	T1068 (Exploitation for Privilege Escalation), M1050 (Exploit Protection)
ISO 27001:2022	A.8.9 — Configuration management
PCI DSS V4.0	2.2.1
SCÉNARIO THREAT MODEL	S3 (VM escape), S6 (insider)
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Faible pour la plupart des workloads. `ptrace_scope=2` empêche `strace` et `gdb` pour les

utilisateurs
non-root.

🔍 AUDIT

Audit :

```
declare -A
expected=(

["kernel.kptr_restrict"]="2"

["kernel.dmesg_restrict"]="1"

["kernel.perf_event_paranoid"]="3"

["kernel.yama.ptrace_scope"]="2"

["kernel.unprivileged_bpf_disabled"]="1"

["kernel.kexec_load_disabled"]="1"

["fs.suid_dumpable"]="0"

)

for key in "${!
expected[@]}";
do

val=$(sysctl
-n "$key" 2>/
dev/null)

[ "$val" = "$
{expected[$key]}" ]
&& echo
"PASS: $key
= $val" \

  echo "FAIL: $key =
  $val (attendu: $
  {expected[$key]})"

done
```

```
**Remédiation

Créer `/etc/s
```

Masquer les pointeurs kernel (prévient KASLR bypass)

kernel.kptr_restrict
= 2

Restreindre dmesg aux privilégiés

kernel.dmesg_restrict
= 1

Restreindre perf_event (profilage)

kernel.perf_event_paranoid
= 3

Restreindre ptrace (debugging inter-processus)

kernel.yama.ptrace_scope = 2

Désactiver BPF non privilégié

kernel.unprivileged_bpf_disabled = 1

Durcir BPF JIT

net.core.bpf_jit_harden = 2

Désactiver kexec (chargement kernel à chaud)

```
kernel.kexec_load_disabled = 1
```

Restreindre userfaultfd

```
vm.unprivileged_userfaultfd = 0
```

Pas de core dumps des processus setuid

```
fs.suid_dumpable = 0
```

```
sysctl --system
```

```
**Valeur par

**Rollback**

---
```

1.2.4

Désactiver les modules kernel inutiles

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	1.1.1.1 à 1.1.1.8
CIS CONTROLS V8	4.8
MITRE ATT&CK	T1068 (Exploitation for Privilege Escalation), M1042 (Disable or Remove Feature)
ISO 27001:2022	A.8.9
PCI DSS V4.0	2.2.4
SCÉNARIO THREAT MODEL	S3, S10
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Faible. Ces modules ne sont pas utilisés sur un

hyperviseur standard.

🔍 AUDIT

Audit :

```
for mod in cramfs freevxfs hfs hfsplus jffs2 udf dccp sctp rds tipc; do

result=$(modprobe -n -v "$mod" 2>&1)

echo "$result" | grep -q "install /bin/true\|install /bin/false" \

&& echo "PASS: $mod désactivé" || echo "FAIL: $mod chargeable"

done
```

```
**Remed

Créer `
```

CIS 1.1.1.1 — cramfs

install cramfs /bin/false

blacklist cramfs

CIS 1.1.1.2 — freevxfs

install freevxfs /bin/false

blacklist freevxfs

CIS 1.1.1.3 — hfs

```
install hfs /bin/false

blacklist hfs
```

CIS 1.1.1.4 — hfsplus

```
install hfsplus /bin/false

blacklist hfsplus
```

CIS 1.1.1.5 — jffs2

```
install jffs2 /bin/false
```

```
blacklist
jffs2
```

CIS 1.1.1.7 — udf

```
install
udf /bin/
false

blacklist
udf
```

Protocoles réseau obsolètes

```
install
dccp /
bin/false

blacklist
dccp

install
sctp /
bin/false

blacklist
sctp

install
rds /bin/
false

blacklist
rds
```

install tipc /bin/ false

blacklist tipc

Bluetooth (inutile sur un serveur)

install bluetooth /bin/ false

blacklist bluetooth

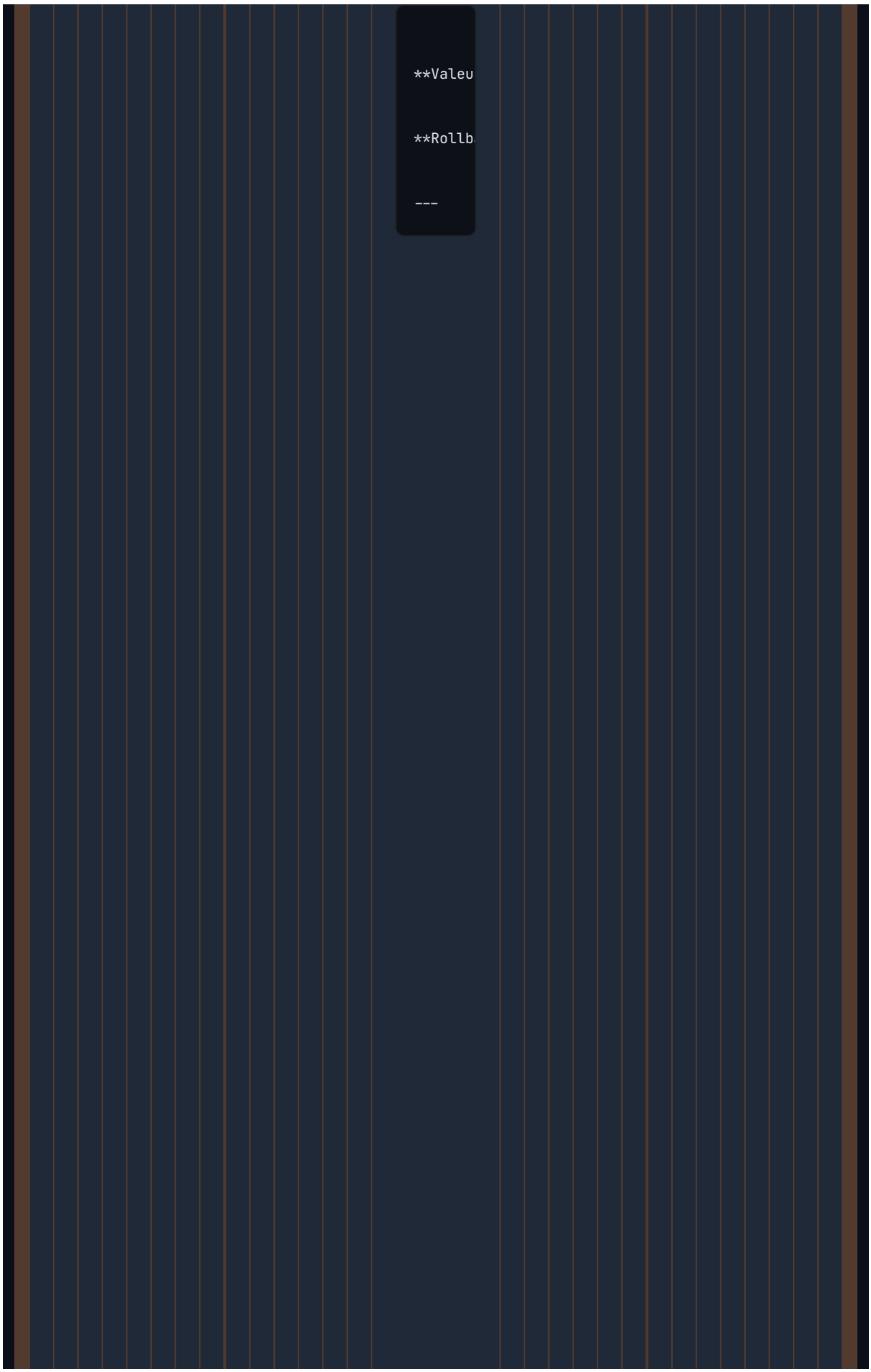
Firewire

install firewire-core /bin/false

blacklist firewire-core

[redacted]

update-initramfs -u


**Valeu
**Rollb

1.2.5

Appliquer les paramètres de démarrage kernel

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Complémentaire (hardening kernel avancé)
CIS CONTROLS V8	4.1
MITRE ATT&CK	T1068, T1014 (Rootkit), M1050 (Exploit Protection)
ISO 27001:2022	A.8.9
SCÉNARIO THREAT MODEL	S3
STATUT PVE 9	✅ Validé (paramètres listés), 🧪 Expérimental (`lockdown=integrity`)

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Surcoût performance ~1-5% selon le workload (principalement `init_on_alloc/free`).

🔧 REMÉDIATION

Remédiation :

Dans `/etc/default/grub` :

```
GR
```

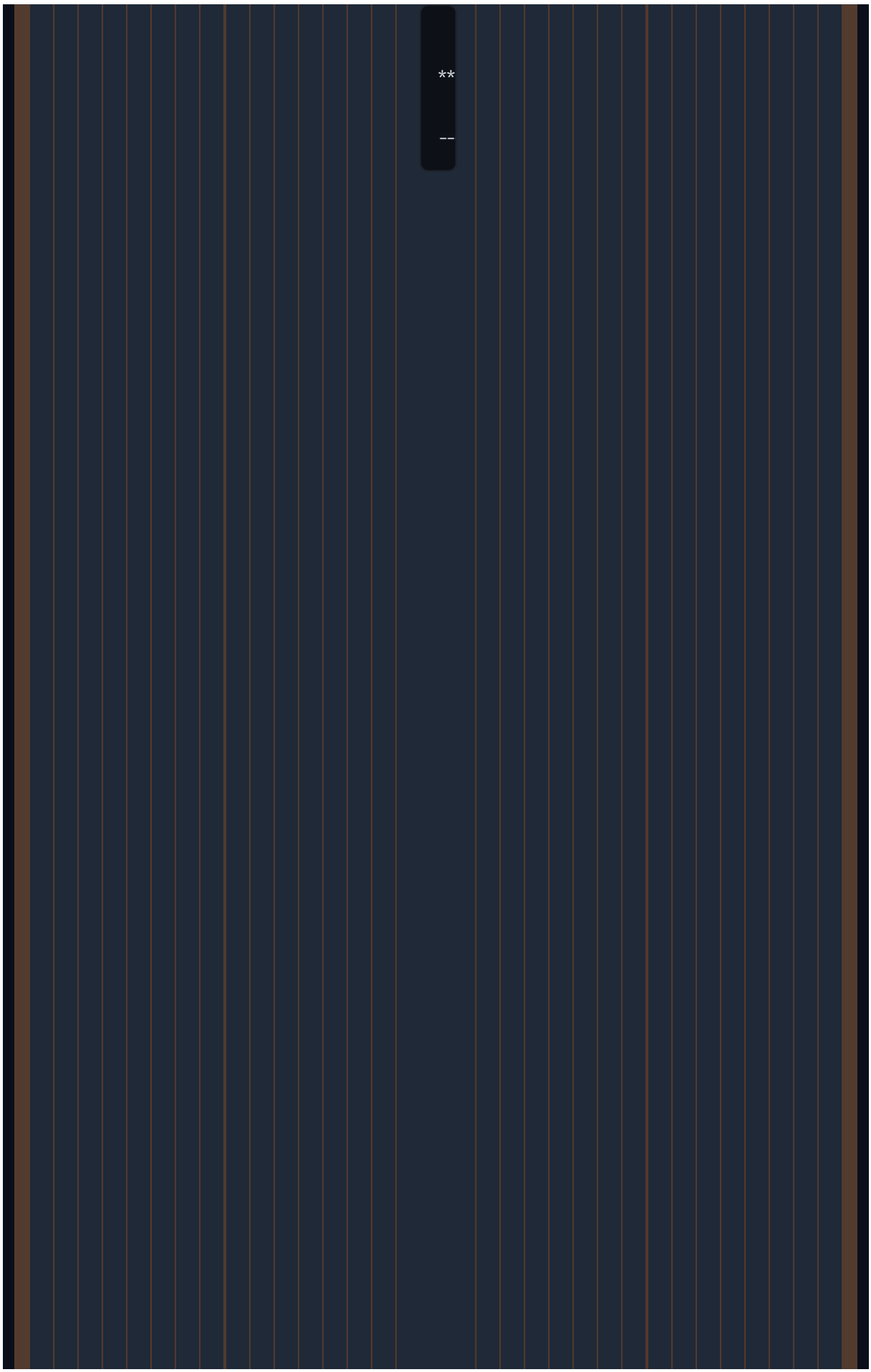
⚠️ **NE PAS AJOUTER** `lockdown=integrity` — ce paramètre empêche le chargement de modules kernel même par root. Il casse ZFS, Ceph, GPU passthrough et d'autres fonctionnalités Proxmox. Voir `12-experimental.md`.

up

NE PAS redémarrer immédiatement — tester d'abord les autres modifications

**

```
cat /proc/cmdline | grep -o "init_on_alloc=1" && echo "PASS" || echo "FAIL"
```



1.3 — Comptes et authentification locale

1.3.1 Configurer la politique de mots de passe

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	5.3.1 — Configure PAM software packages, 5.4.1 — Ensure password creation requirements
CIS CONTROLS V8	5.2 — Use Unique Passwords
MITRE ATT&CK	T1110 (Brute Force), M1027 (Password Policies)
ISO 27001:2022	A.5.17 — Authentication information
PCI DSS V4.0	8.3.6 — Minimum password complexity
SCÉNARIO THREAT MODEL	S1, S6
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

🔍
AUDIT

Audit :

```
grep
-E
"^minlen|
^minclass|
^dcredit|
^ucredit"
/
etc/
security/
pwquality.conf
2>/
dev/
null
```

Résultat attendu : minlen = 14, minclass = 3

**

```
apt
install
-y
libpam-
pwquality
```

```
Co

minlen
=
14

minclass
=
3

maxrepeat
=
3

dictcheck
=
1

dcredit
=
-1

ucredit
=
-1

lcredit
=
-1

ocredit
=
-1

**

--
```

1.3.2

Configurer le verrouillage après échecs d'authentification

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	5.3.2 — Ensure lockout for failed password attempts
CIS CONTROLS V8	5.6 — Centralize Account Management
MITRE ATT&CK	T1110 (Brute Force), M1036 (Account Use Policies)
ISO 27001:2022	A.8.5 — Secure authentication
PCI DSS V4.0	8.3.4 — Lockout after 10 invalid attempts
SCÉNARIO THREAT MODEL	S1
STATUT PVE 9	✅ Validé

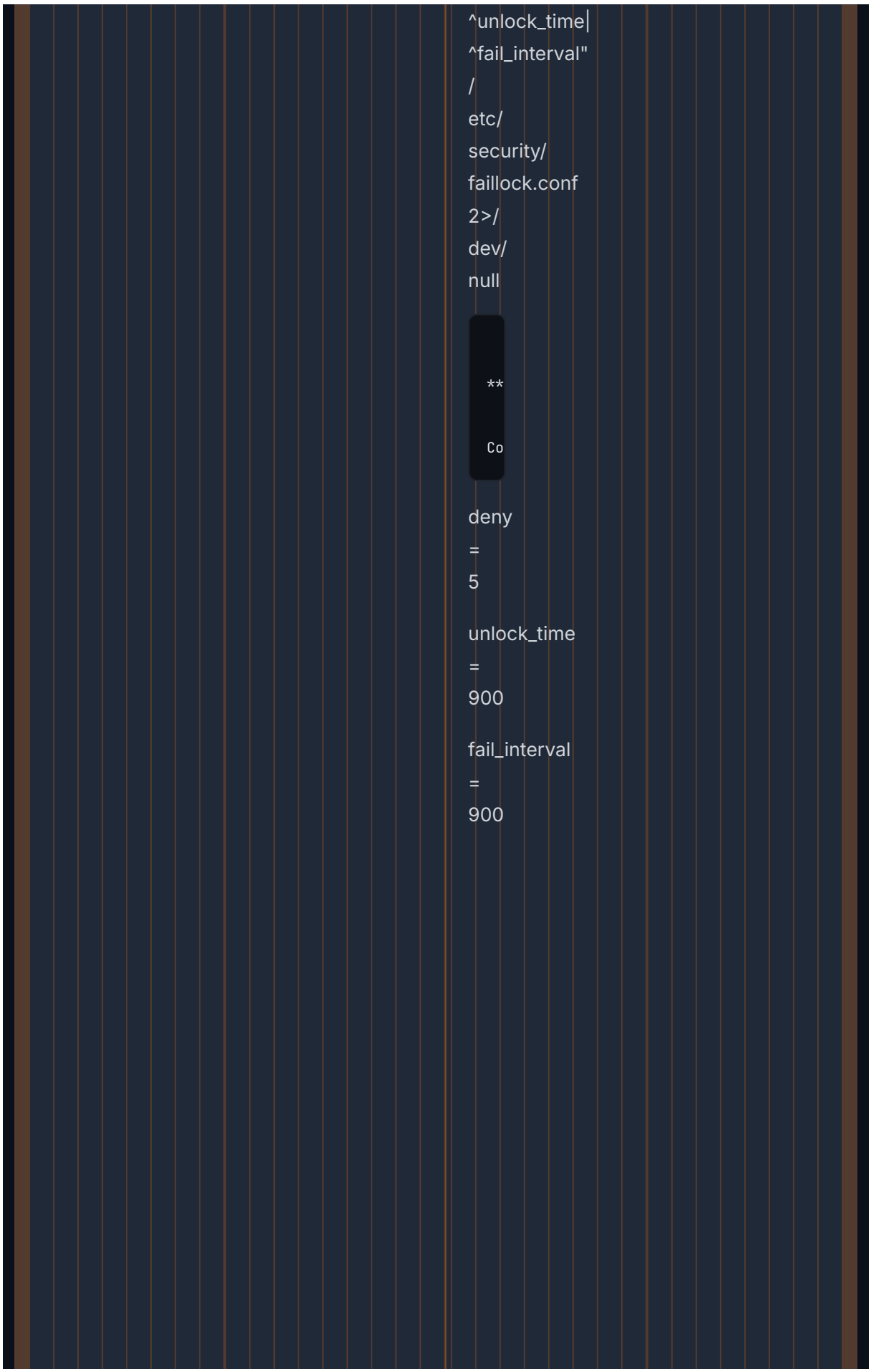
DESCRIPTION :

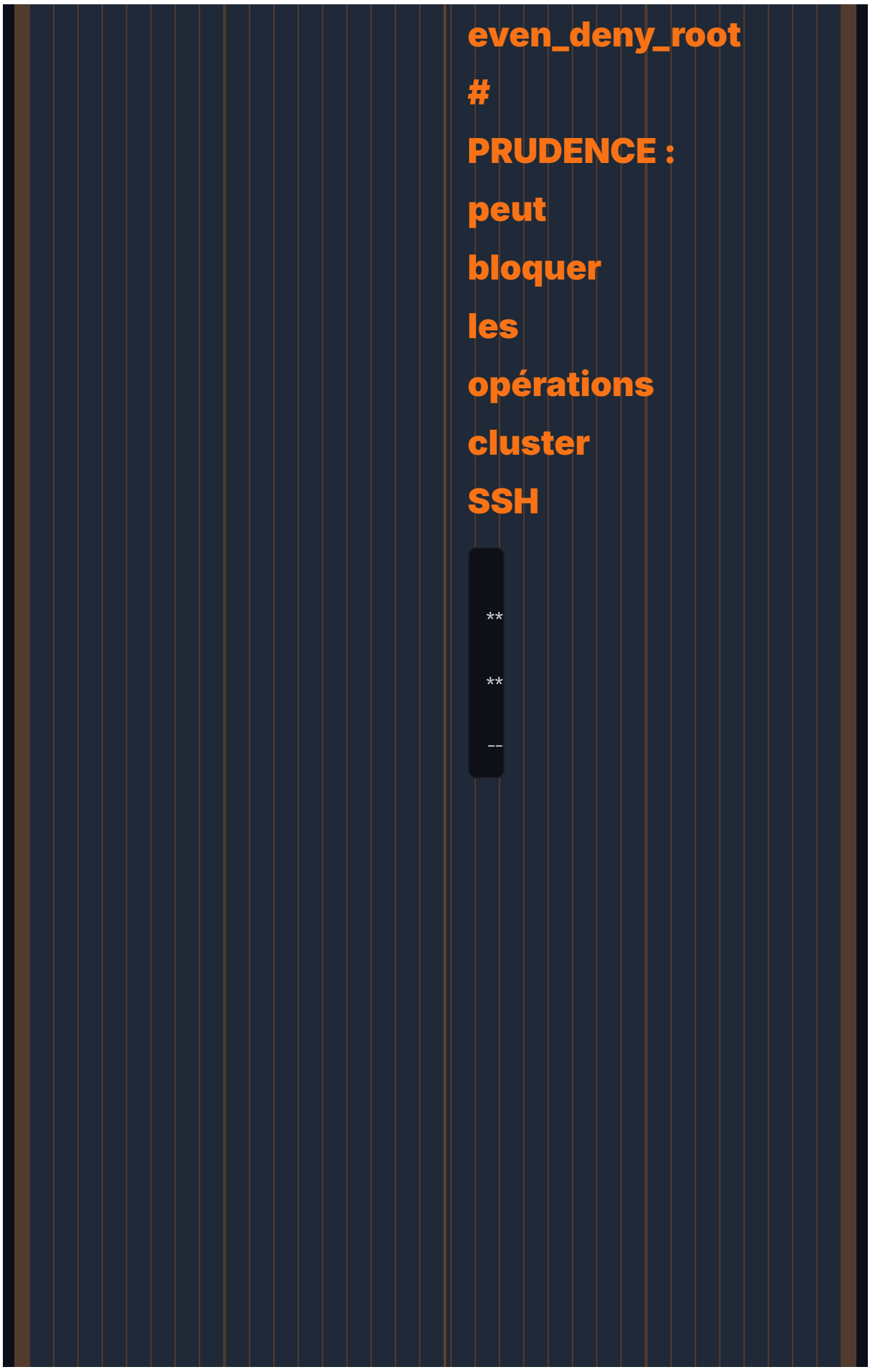
Description :

🔍
AUDIT

Audit :

```
grep
-E
"^deny|
```


^unlock_time|
^fail_interval"
/
etc/
security/
faillock.conf
2>/
dev/
null
**
Co
deny
=
5
unlock_time
=
900
fail_interval
=
900


even_deny_root
#
PRUDENCE :
peut
bloquer
les
opérations
cluster
SSH
**
**
--

1.3.3 Configurer le timeout d'inactivité shell

Level 1

PROFILE APPLICABILITY	Level 1 — Server
RÉF. CIS DEBIAN 13	5.5.5 — Ensure default user shell timeout is configured
CIS CONTROLS V8	4.3 — Configure Automatic Session Locking
MITRE ATT&CK	T1078 (Valid Accounts)
ISO 27001:2022	A.8.5
SCÉNARIO THREAT MODEL	S6
STATUT PVE 9	✅ Validé

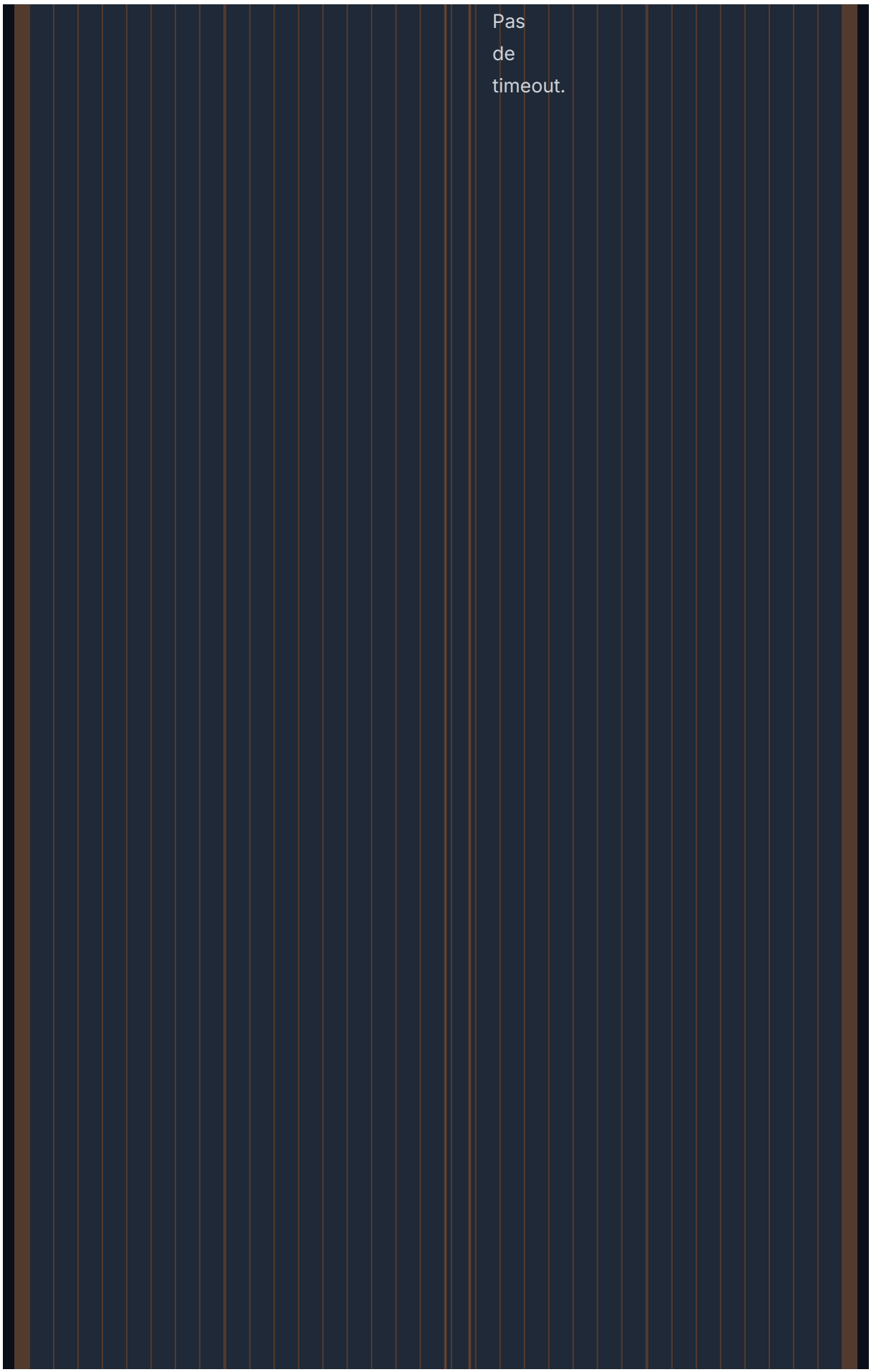
🔧 REMÉDIATION

Remédiation :

Créer `/etc/profile.d/cis-timeout.sh` :

```
re
ex
```

Valeur par défaut :


Pas
de
timeout.

1.3.4 Configurer la bannière de connexion

Level 1

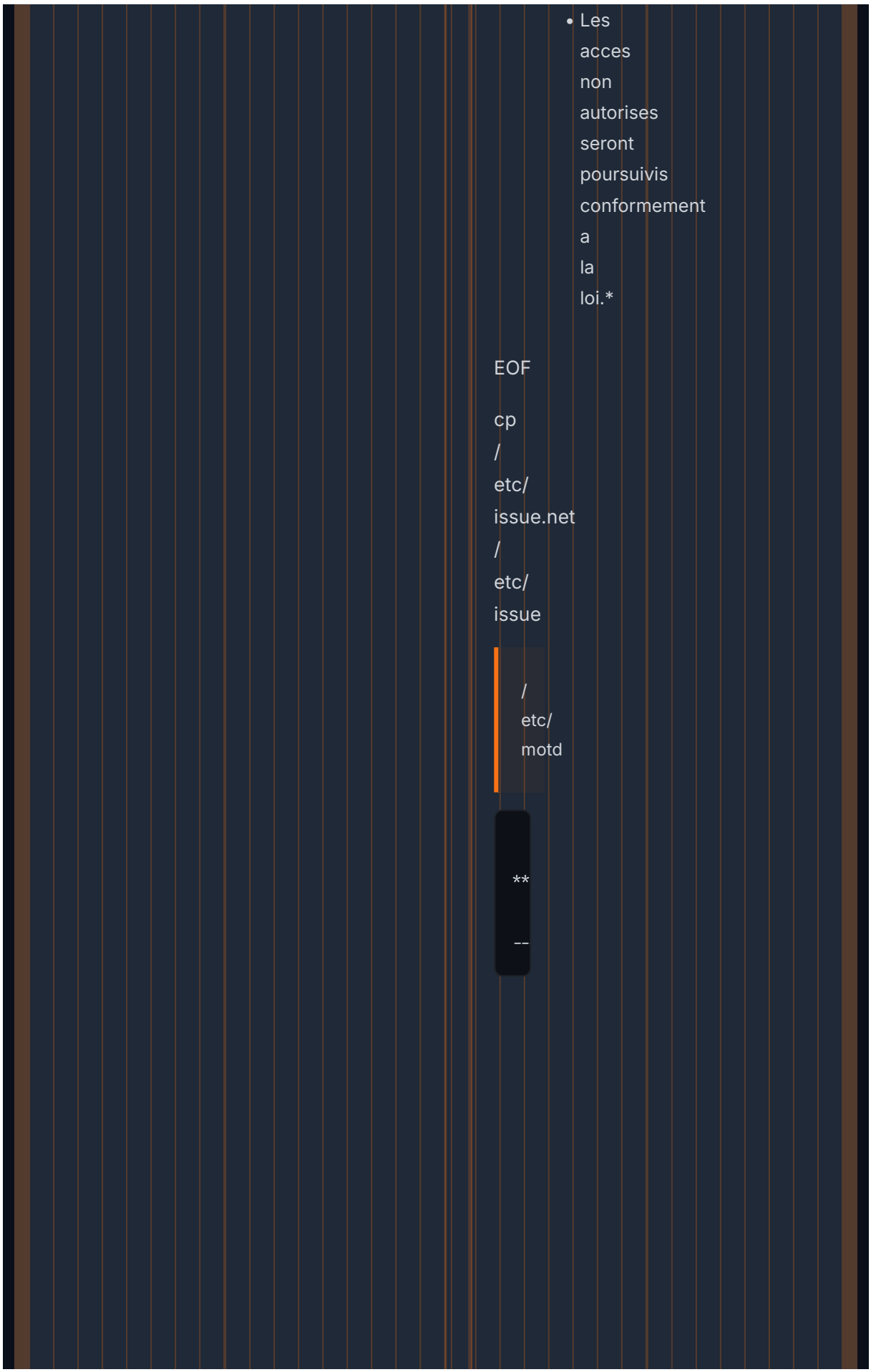
PROFILE APPLICABILITY	Level 1 — Server
RÉF. CIS DEBIAN 13	1.7.1 à 1.7.6
CIS CONTROLS V8	N/A
MITRE ATT&CK	N/A (contrôle juridique, pas technique)
ISO 27001:2022	A.8.5
PCI DSS V4.0	2.2.1
STATUT PVE 9	✅ Validé

🔧 REMÉDIATION

Remédiation :

cat > /etc/issue.net << 'EOF'

- Acces autorise uniquement. Toute activite est journalisee. *


• Les acces non autorises seront poursuivis conformement a la loi.*
EOF
cp / etc/ issue.net / etc/ issue
/ etc/ motd
** --

1.4 — Journalisation et audit

1.4.1

Installer et configurer auditd

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐 (🟡 N2 pour 🏠)
RÉF. CIS DEBIAN 13	6.2.1 à 6.2.4
CIS CONTROLS V8	8.2 — Collect Audit Logs, 8.5 — Collect Detailed Audit Logs
MITRE ATT&CK	T1070 (Indicator Removal), T1078 (Valid Accounts), M1028 (Operating System Configuration)
ISO 27001:2022	A.8.15 — Logging
PCI DSS V4.0	10.2.1 — Audit logs capture defined events
SCÉNARIO THREAT MODEL	S1, S3, S6
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

Surcoût CPU ~2-4%,

I/O supplémentaire selon le volume de logs. Surveiller la taille de `/var/log/audit`.

🔍 AUDIT

Audit :

```
systemctl is-active auditd && echo "PASS" || echo "FAIL"

auditctl -l | wc -l
```

Résultat attendu :

> 0

```
**
```

```
apt
install
-y
auditd
audispd-
plugins

systemctl
enable
--
now
auditd
```

```
Cr
```

Purge des règles existantes

```
-D
```

Buffer

```
-b
8192
```

Action en cas d'erreur

```
-f
1
```

=== CIS 6.2.3.1-4 : Fichiers d'identité ===

```
-w
/
etc/
passwd
-p
wa
-k
identity

-w
/
etc/
shadow
-p
```

```
wa
-k
identity

-w
/
etc/
group
-p
wa
-k
identity

-w
/
etc/
gshadow
-p
wa
-k
identity

-w
/
etc/
security/
opasswd
-p
wa
-k
identity
```

```
=== CIS 6.2.3.5 : Réseau ===

-w /etc/hosts -p wa -k network

-w /etc/network/ -p wa -k network

=== CIS 6.2.3.6 : Sysctl ===

-w /etc/sysctl.conf -p
```

```
wa
-k
sysctl

-w
/
etc/
sysctl.d/
-p
wa
-k
sysctl

=== CIS 6.2.3.7 : SSH ===

-w
/
etc/
ssh/
sshd_config
-p
wa
-k
sshd

-w
/
etc/
ssh/
sshd_config.d/
-p
wa
-k
sshd
```

```
=== CIS 6.2.3.8 : PAM ===

-w /etc/pam.d/ -p wa -k pam

-w /etc/security/ -p wa -k pam

=== CIS 6.2.3.9 : Heure système ===

-a always,exit -F
```

```
arch=b64
-S
adjtimex,settimeofday,clock_settime
-k
time-
change

=== CIS 6.2.3.10 : Cron ===

-w
/
etc/
crontab
-p
wa
-k
cron

-w
/
etc/
cron.d/
-p
wa
-k
cron

-w
/
etc/
cron.daily/
-p
wa
-k
cron
```

```
-w
/
etc/
cron.hourly/
-p
wa
-k
cron

-w
/
etc/
cron.weekly/
-p
wa
-k
cron

-w
/
etc/
cron.monthly/
-p
wa
-k
cron
```

CIS 6.2.3.14 : Élévation de privilèges

```
-a
always,exit
```

```
-F
arch=b64
-S
execve
-F
euid=0
-F
auid>=1000
-F
auid!
=4294967295
-k
privilege_escalation
```

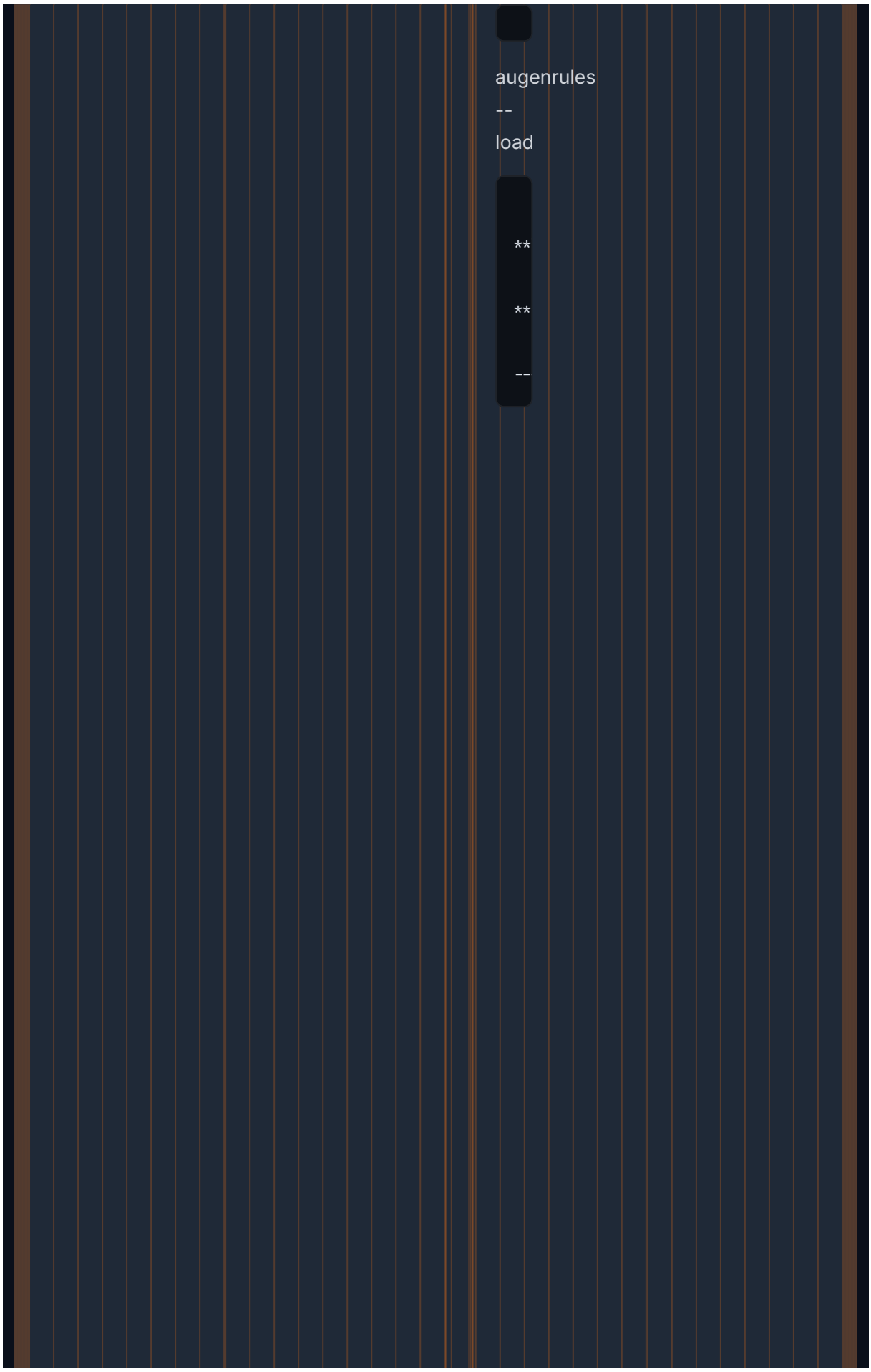
=== CIS 6.2.3.15 : Montage de filesystems ===

```
-a
always,exit
-F
arch=b64
-S
mount,umount2
-F
auid>=1000
-F
auid!
=4294967295
-k
mounts
```

```
===
CIS
6.2.3.17 :
Suppression
de
fichiers
===

-a
always,exit
-F
arch=b64
-S
unlink,unlinkat,rename,renameat
-F
auid>=1000
-F
auid!
=4294967295
-k
delete

===
CIS
6.2.3.19 :
Modules
kernel
===

-a
always,exit
-F
```

```
arch=b64
-S
init_module,finit_module,delete_module
-k
modules

-w
/
sbin/
insmod
-p
x
-k
modules

-w
/
sbin/
modprobe
-p
x
-k
modules

-w
/
sbin/
rmmod
-p
x
-k
modules
```

```
=== SPÉCIFIQUE PROXMOX : Configuration PVE ===
-w /etc/pve/ -p wa -k proxmox-config

=== Verrouillage des règles (reboot requis pour modifier) ===
-e 2
```


augenrules
--
load
**
**
--

1.4.2

Configurer journald en mode persistant

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	6.1.1 à 6.1.3
CIS CONTROLS V8	8.2
MITRE ATT&CK	T1070.002 (Clear Linux Logs)
ISO 27001:2022	A.8.15
PCI DSS V4.0	10.2.1
SCÉNARIO THREAT MODEL	S6
STATUT PVE 9	✅ Validé

🔧 REMÉDIATION

Remédiation :

Dans `/etc/systemd/journald.conf` :

```
[J
St
Co
Sy
Sy
Fo
```

```
sy
```

Valeur par défaut : `Storage=auto` (persistant si `/var/log/journal` existe, sinon volatile).

1.5 — Services et processus

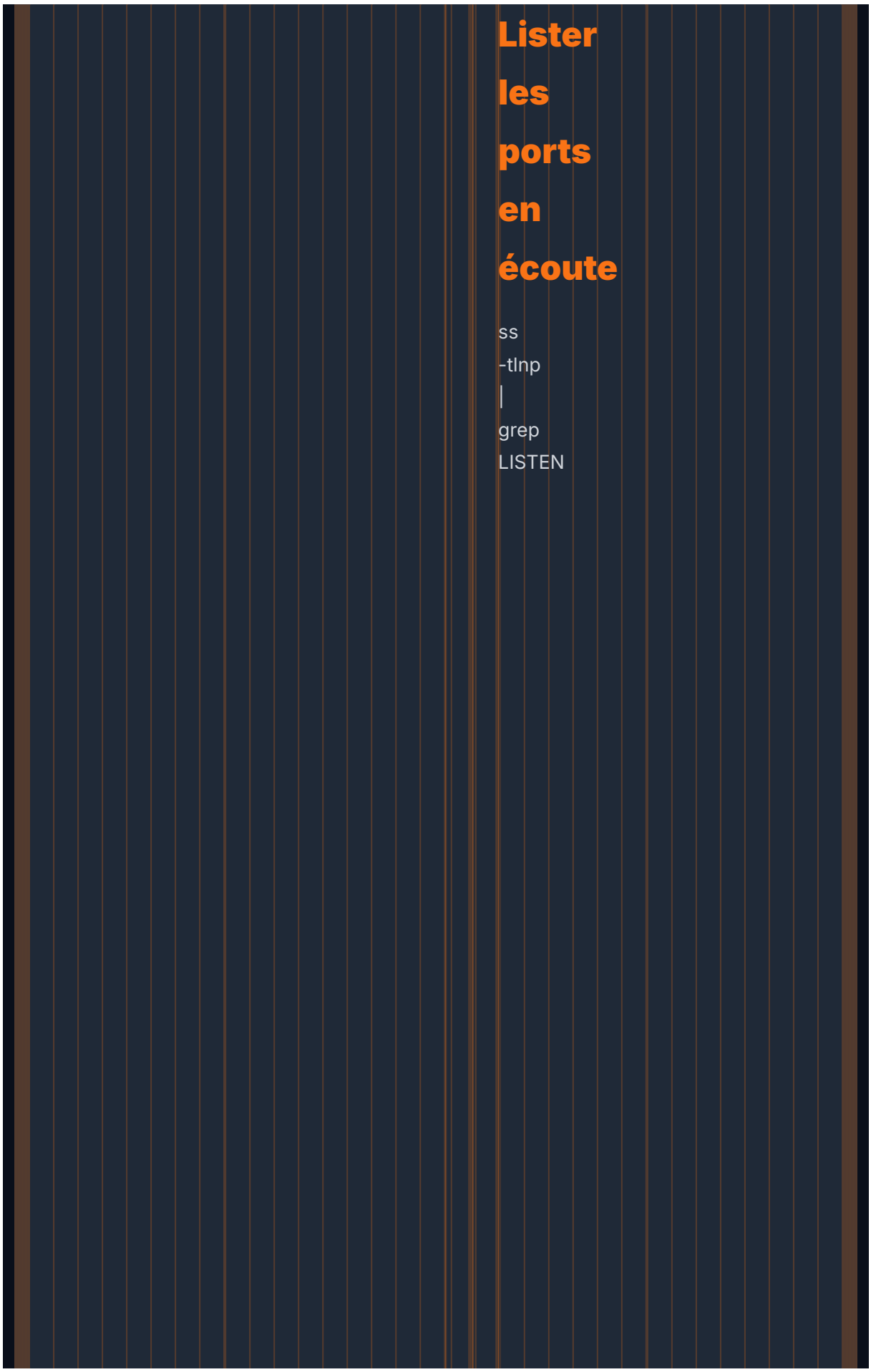
1.5.1 Désactiver les services inutiles

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	2.1.x à 2.3.x
CIS CONTROLS V8	4.8
MITRE ATT&CK	T1543 (Create or Modify System Process), M1042
ISO 27001:2022	A.8.9
PCI DSS V4.0	2.2.4
SCÉNARIO THREAT MODEL	S1, S3
STATUT PVE 9	✅ Validé

🔍 AUDIT

Audit :



Lister les ports en écoute

```
ss
-tlnp
|
grep
LISTEN
```

Résultat attendu : uniquement les ports PVE nécessaires (22, 8006, 85, et selon le cas : 3128, 5405, 6789, 6800-7300)

**

systemctl disable --now

```
avahi-
daemon.service
2>/
dev/
null

systemctl
disable
--
now
cups.service
2>/
dev/
null

systemctl
disable
--
now
rpcbind.service
rpcbind.socket
2>/
dev/
null
```

1.5.2

Masquer les services Proxmox non utilisés

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox (hors CIS)
CIS CONTROLS V8	4.8
MITRE ATT&CK	M1042
SCÉNARIO THREAT MODEL	S1, S3
STATUT PVE 9	✅ Validé

DESCRIPTION :

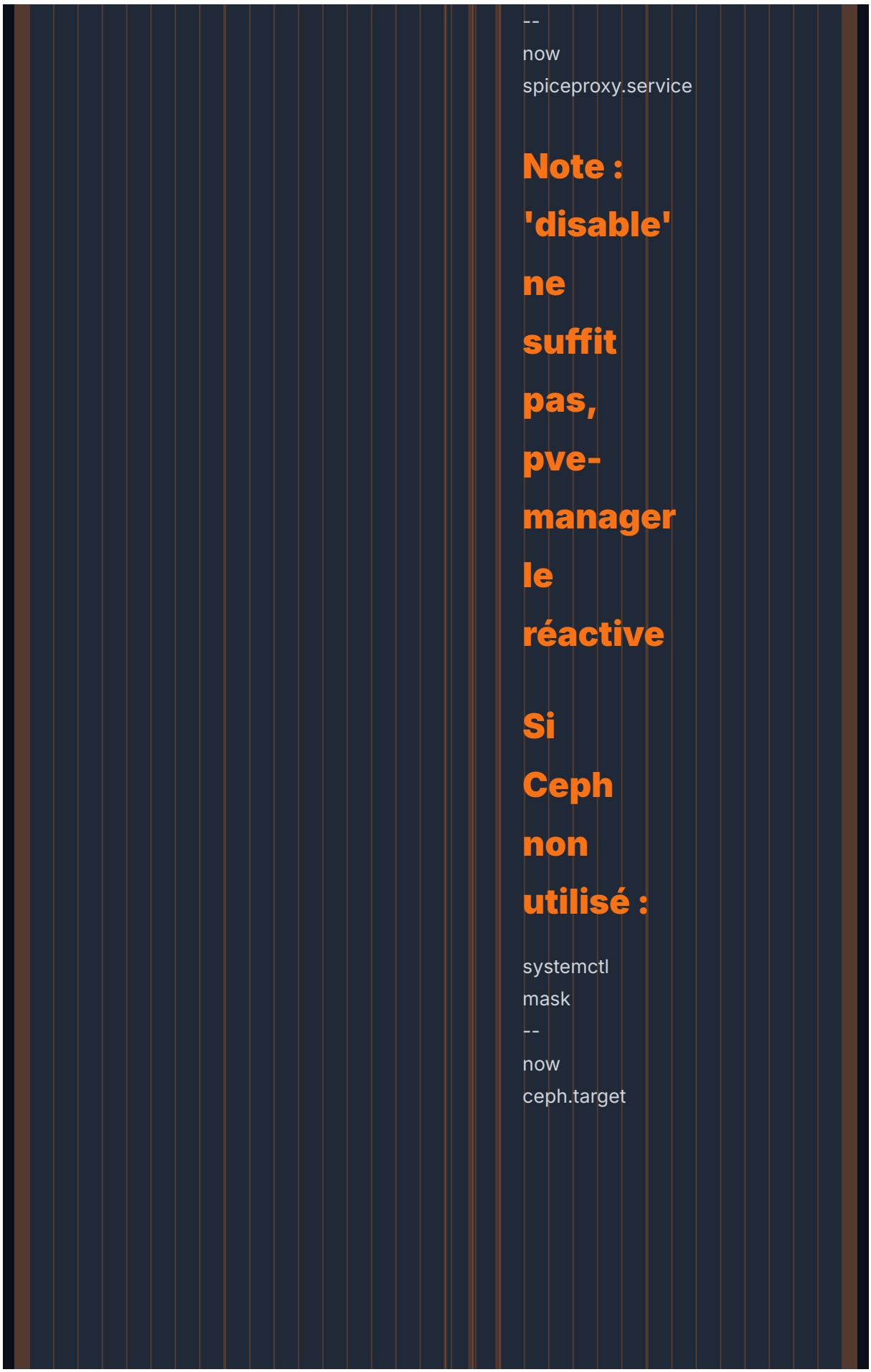
Description :

🔧 REMÉDIATION

Remédiation :

Si SPICE non utilisé (consoles VM) :

systemctl mask



```
--
now
spiceproxy.service
```

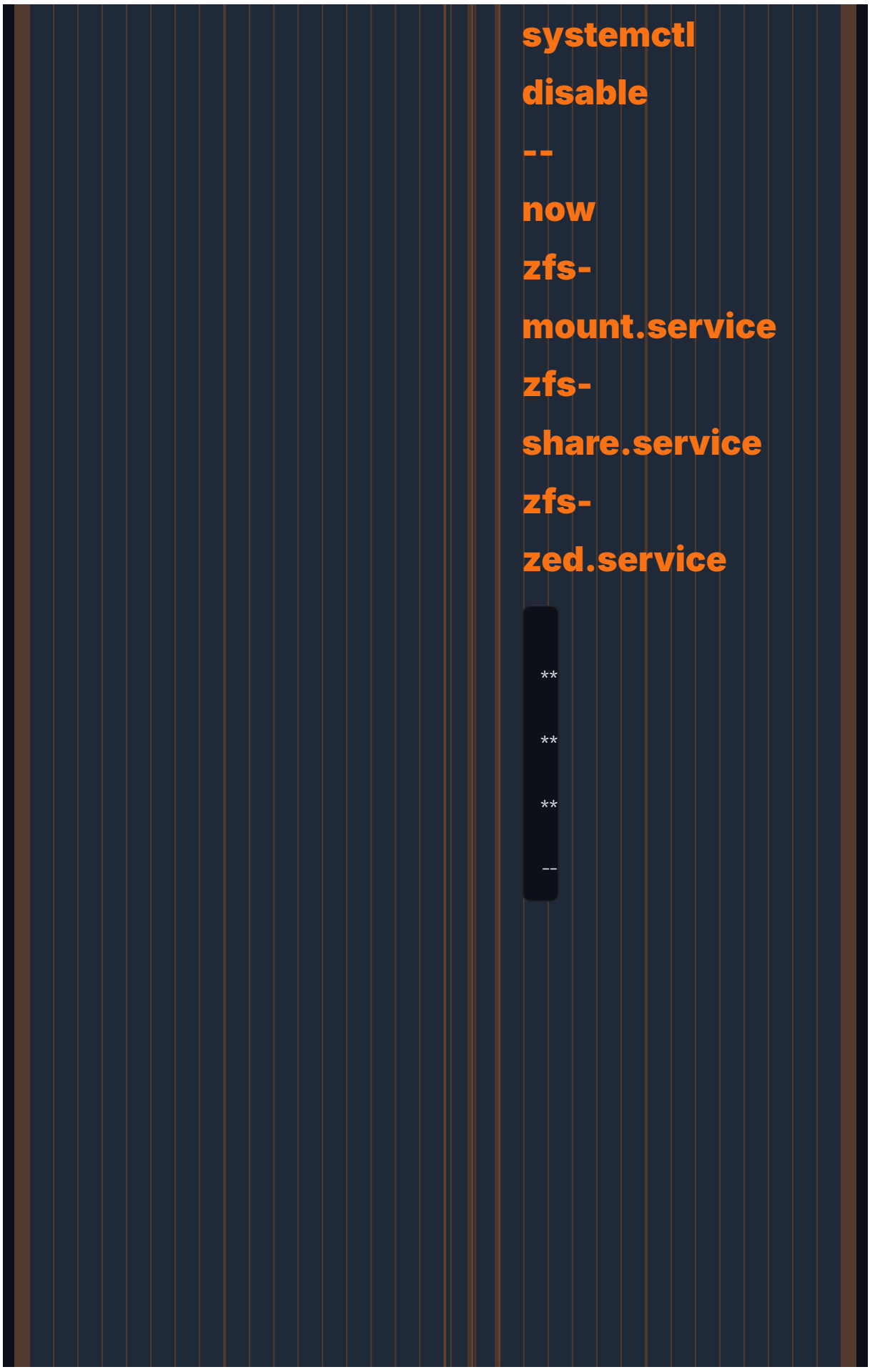
Note : 'disable' ne suffit pas, pve-manager le réactive

Si Ceph non utilisé :

```
systemctl
mask
--
now
ceph.target
```

Note : 'disable' ne suffit pas, le service se réactive au reboot

Si ZFS non utilisé :


systemctl
disable
--
now
zfs-
mount.service
zfs-
share.service
zfs-
zed.service
**
**
**
--

1.6 — AppArmor

1.6.1 Vérifier qu'AppArmor est actif

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	1.3.1.1 — Ensure AppArmor is installed, 1.3.1.2 — Ensure AppArmor is enabled
CIS CONTROLS V8	4.1, 10.5
MITRE ATT&CK	T1068 (Exploitation for Privilege Escalation), M1050 (Exploit Protection)
ISO 27001:2022	A.8.7 — Protection against malware
PCI DSS V4.0	2.2.1
SCÉNARIO THREAT MODEL	S3 (VM escape)
STATUT PVE 9	✅ Validé

🔍 AUDIT

Audit :

```
aa-status --enabled && echo "PASS"
```

```
|| echo "FAIL"

aa-status 2>/dev/null | head -5
```

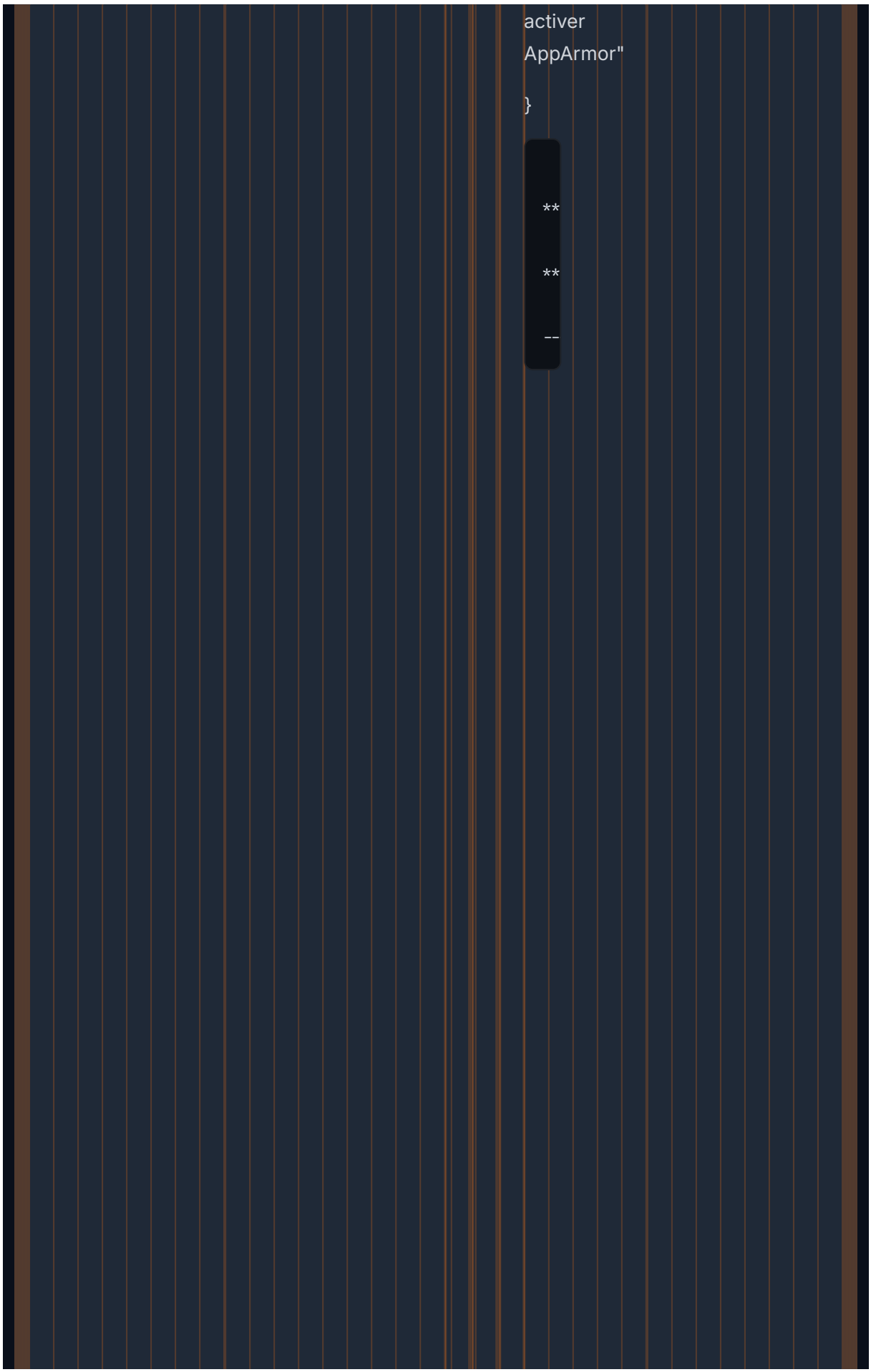
Résultat attendu : "apparmor module is loaded", X profiles, Y enforce

```
**

apt install -y apparmor
```

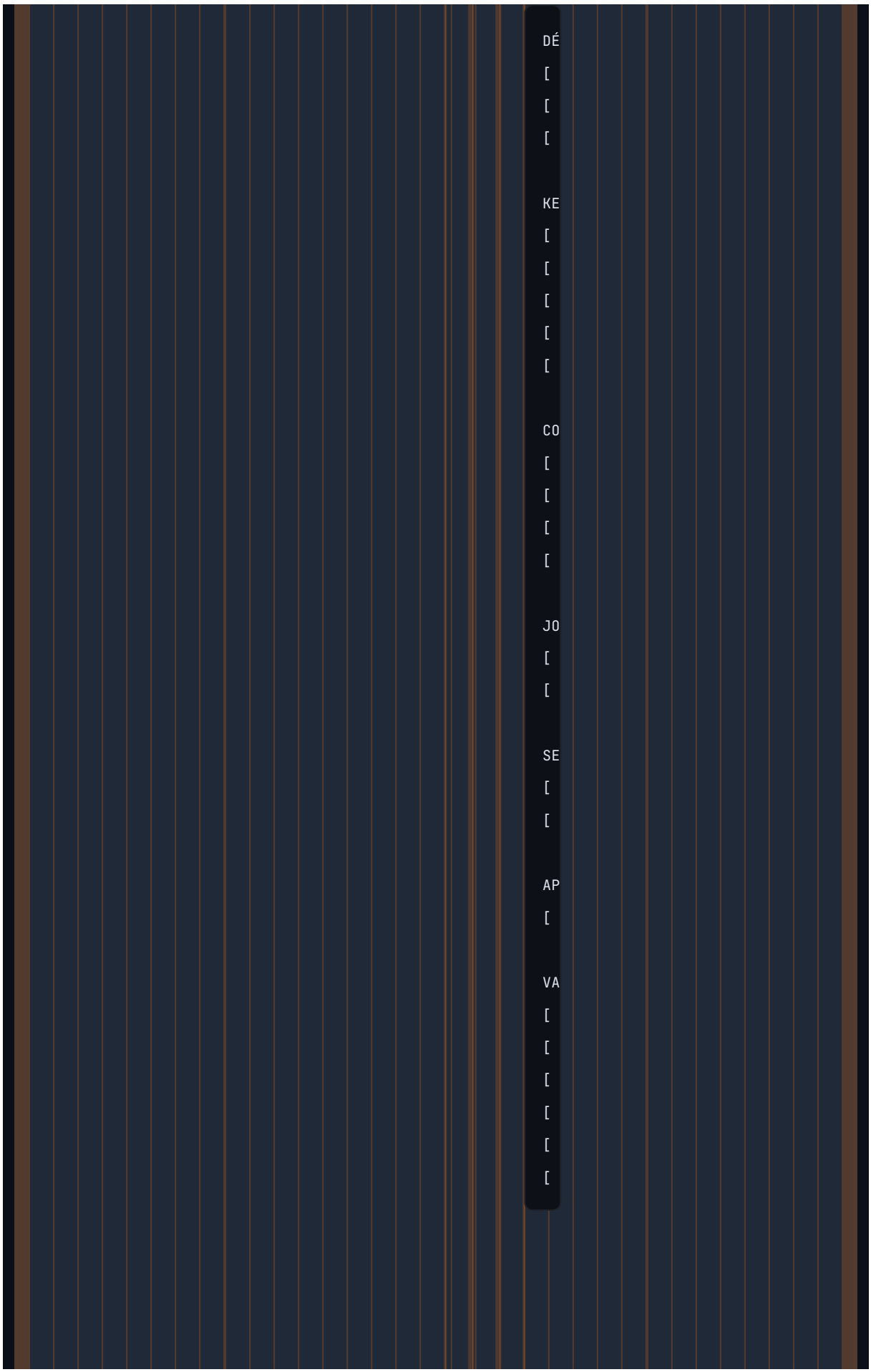
```
apparmor-
utils
```

Vérifier la ligne de commande kernel

```
grep
-qE
"apparmor=1|
security=apparmor"
/
proc/
cmdline
||
{

sed
-i
's/
GRUB_CMDLINE_LINUX_DEFAULT="/
GRUB_CMDLINE_LINUX_DEFAULT="apparmor=1
security=apparmor /'
/
etc/
default/
grub

update-
grub

echo
"Reboot
nécessaire
pour
```


activer
AppArmor"
}
**
**
--

1.7 — Checklist post-Phase 1


DÉ
[
[
[
KE
[
[
[
[
[
CO
[
[
[
[
JO
[
[
SE
[
[
AP
[
VA
[
[
[
[
[
[

Navigation : ← 02-pre-installation.md | 04-proxmox-specifique.md →

-e

CHAPITRE
3
SUR
5

Phase 2 & 3 — Proxmox & Authentification

04 — Phase 2 : Durcissement spécifique Proxmox VE

Version : 0.2.0
Date : 2026-03-20
Statut : Rédaction initiale — Format CIS hybride
Licence : CC BY-SA 4.0
Base de référence : CIS Debian Linux 13 Benchmark v1.0.0, Documentation Proxmox VE 9

Scénarios du threat model : S1, S3, S4, S6, S9

2.1 — Interface web (pveproxy)

2.1.1 Durcir la configuration TLS de pveproxy

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox (hors CIS)
CIS CONTROLS V8	3.10 — Encrypt Sensitive Data in Transit
MITRE ATT&CK	T1557 (Adversary-in-the-Middle), T1040 (Network Sniffing), M1041 (Encrypt Sensitive Information)
ISO 27001:2022	A.8.24 — Use of cryptography
PCI DSS V4.0	4.2.1 — Strong cryptography for transmission
SCÉNARIO THREAT MODEL	S1, S9
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :

Faible. Les navigateurs modernes supportent tous TLS 1.2+ avec AES-GCM et ChaCha20. Seuls les clients très anciens (IE < 11, Android < 5) seraient affectés.

🔍 AUDIT

Audit :

Vérifier la configuration existante

cat /

```
etc/
default/
pveproxy
2>/
dev/
null
```

Résultat attendu : fichier présent avec CIPHERS et HONOR_CIPHER_ORDER

Tester les ciphers acceptés (depuis un autre hôte)

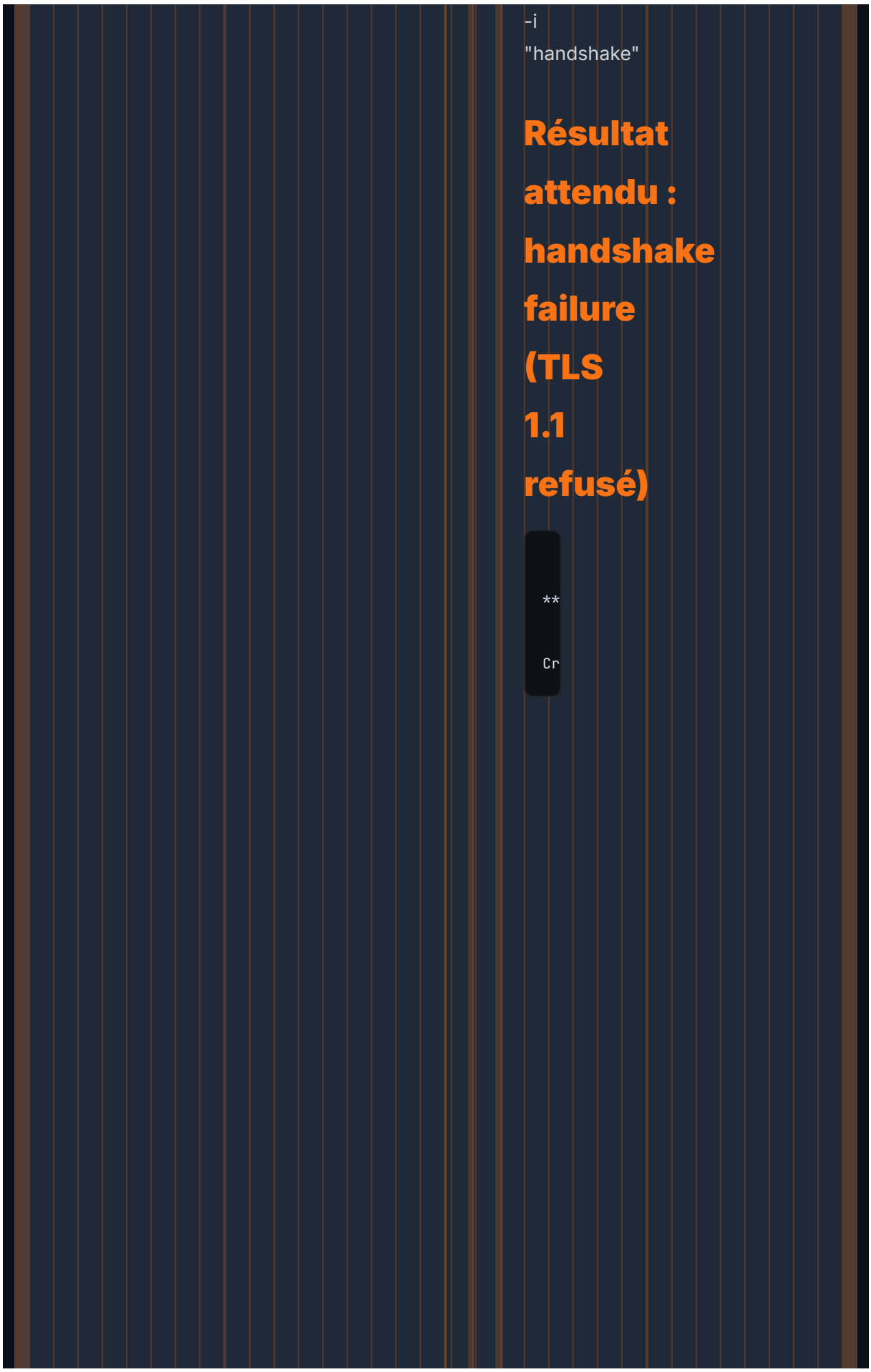
```
nmap
--
script
ssl-
```

```
enum-
ciphers
-p
8006
<PVE_IP>
```

Résultat attendu : uniquement TLS 1.2 et 1.3, pas de ciphers CBC

Alternative avec openssl

```
openssl
s_client
-connect
<PVE_IP>:8006
-tls1_1
2>&1
|
grep
```


-i
"handshake"
Résultat attendu : handshake failure (TLS 1.1 refusé)
**
Cr

Ciphers TLS 1.2 — uniquement AEAD (GCM, ChaCha20), pas de CBC

```
CIPHERS="ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
```

GCM-
SHA256"

Ciphers TLS 1.3 (défauts OpenSSL, déjà sécurisés)

CIPHERSUITES="TLS_AES_256_GCM_SHA384:TLS_C

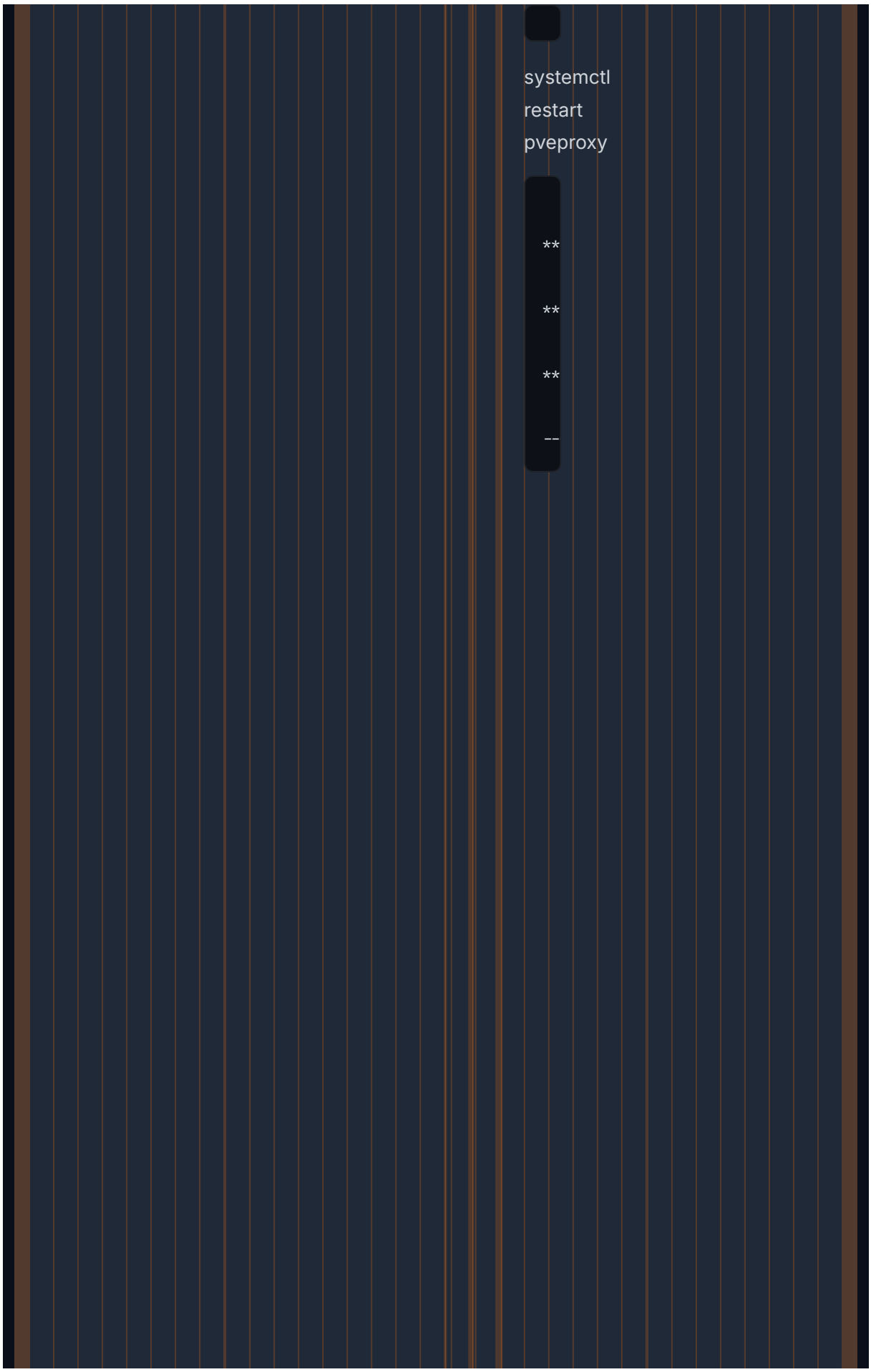
Le serveur choisit le cipher (pas le client)

HONOR_CIPHER_ORDER=1

Désactiver TLS < 1.2 explicitement

(normalement déjà désactivé via OpenSSL sur Debian 13, mais par sécurité)

Note : pveproxy désactive SSL 2/3 inconditionnellement


systemctl
restart
pveproxy
**
**
**
--

2.1.2

Configurer des certificats Let's Encrypt / ACME

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	3.10
MITRE ATT&CK	T1557, M1041
ISO 27001:2022	A.8.24
PCI DSS V4.0	4.2.1
SCÉNARIO THREAT MODEL	S1
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Faible. Nécessite un FQDN résolvable et un accès réseau pour la

validation ACME (HTTP-01 ou DNS-01).

🔍 AUDIT

Audit :

Vérifier le certificat actuel

```
openssl x509 -in /etc/pve/local/pve-ssl.pem -text -noout | grep -E "Issuer:|Not After"
```

Résultat attendu : Issuer != "Proxmox Virtual Environment" (pas auto-signé)

Not After : date dans le futur

Vérifier la configuration ACME

```
pvenode
acme
account
list
2>/
dev/
null
```

**

1. Enregistrer un compte ACME

```
pvenode
acme
account
register
default
<email@example.com>
--
directory
https://
acme-
v02.api.letsencrypt.org/
directory
```

2. Configurer le challenge (HTTP-01 ou DNS-01)

HTTP-01 (le port 80 doit être accessible depuis internet) :

```
pvenode
config
set
--
acme
domains=<fqdn>

pvenode
acme
cert
order
```

DNS-01 (recommandé si le serveur n'est pas directement accessible) :

Configurer le plugin DNS dans Datacenter > ACME

```
**
**
--
```

2.1.3

Restreindre l'accès au Web UI par IP

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	4.2 — Establish and Maintain a Firewall Rule Set, 13.1 — Centralize Security Event Alerting
MITRE ATT&CK	T1190 (Exploit Public-Facing Application), M1030 (Network Segmentation), M1035 (Limit Access to Resource)
ISO 27001:2022	A.8.20 — Network security
PCI DSS V4.0	1.2.1
SCÉNARIO THREAT MODEL	S1
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Faible, mais

risque de lock-out si l'IP d'administration change. Toujours conserver un accès console hors-bande.

🔍 AUDIT

Audit :

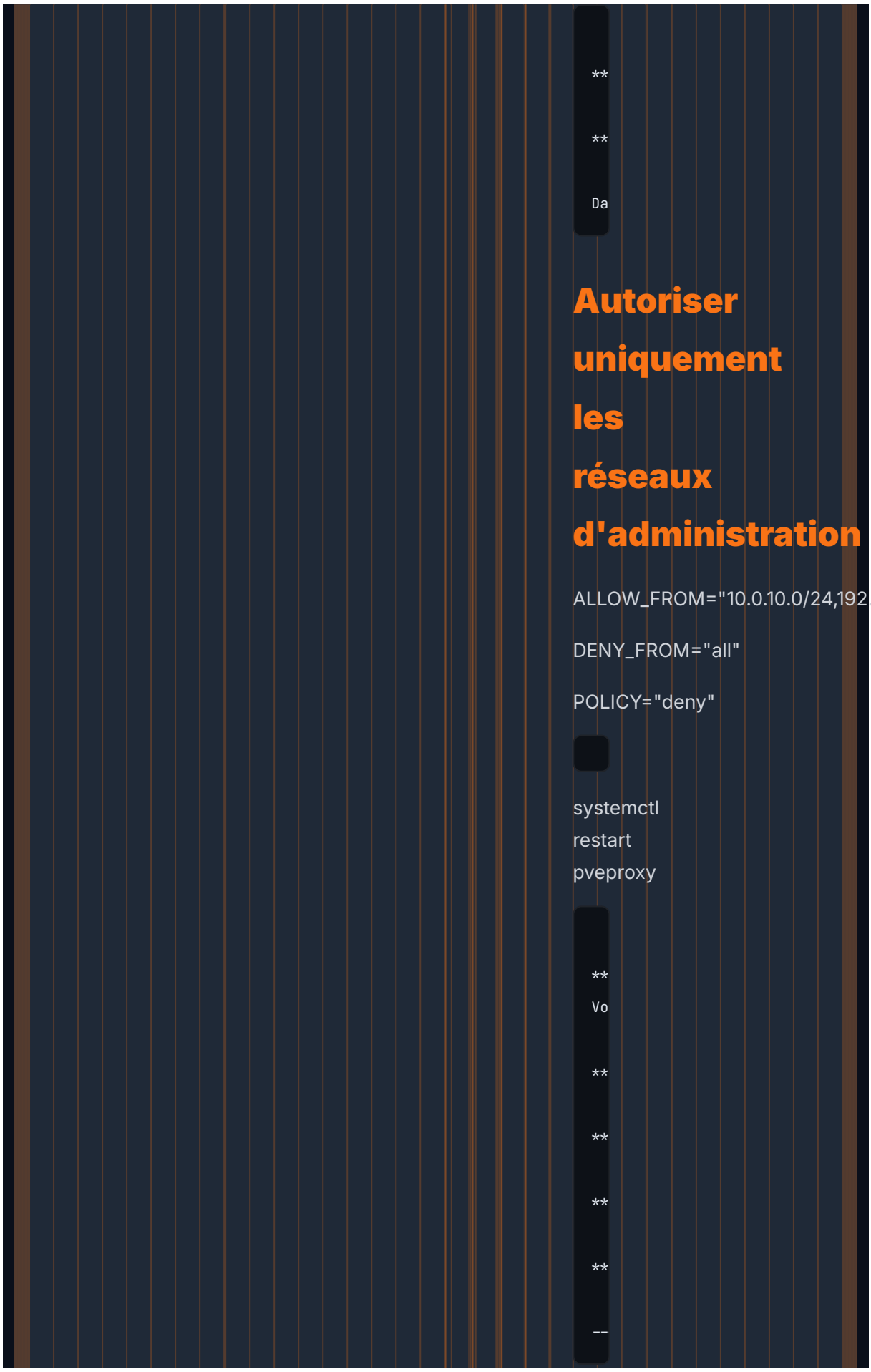
Vérifier la configuration ACL pveproxy

```
grep -E "ALLOW_FROM|DENY_FROM|POLICY" /etc/default/pveproxy 2>/dev/null
```

Résultat attendu : ALLOW_FROM configuré, DENY_FROM="all", POLICY="deny"

Vérifier les règles firewall PVE pour le port 8006

```
pvesh
get
/
cluster/
firewall/
rules
2>/
dev/
null
|
grep
8006
```


**
**
Da
Autoriser uniquement les réseaux d'administration
ALLOW_FROM="10.0.10.0/24,192.168.1.0/24"
DENY_FROM="all"
POLICY="deny"
systemctl
restart
pveproxy
**
Vo
**
**
**
**
--

2.1.4 Désactiver la console noVNC si non utilisée

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	4.8
MITRE ATT&CK	T1021.005 (VNC), M1042 (Disable or Remove Feature)
ISO 27001:2022	A.8.9
SCÉNARIO THREAT MODEL	S1, S3
STATUT PVE 9	⚠️ Partiel — spiceproxy masquable, noVNC intégré à pveproxy

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Moyen. Plus de console graphique

pour les VM depuis l'interface web PVE. L'accès SSH aux VM reste fonctionnel.

🔧 REMÉDIATION

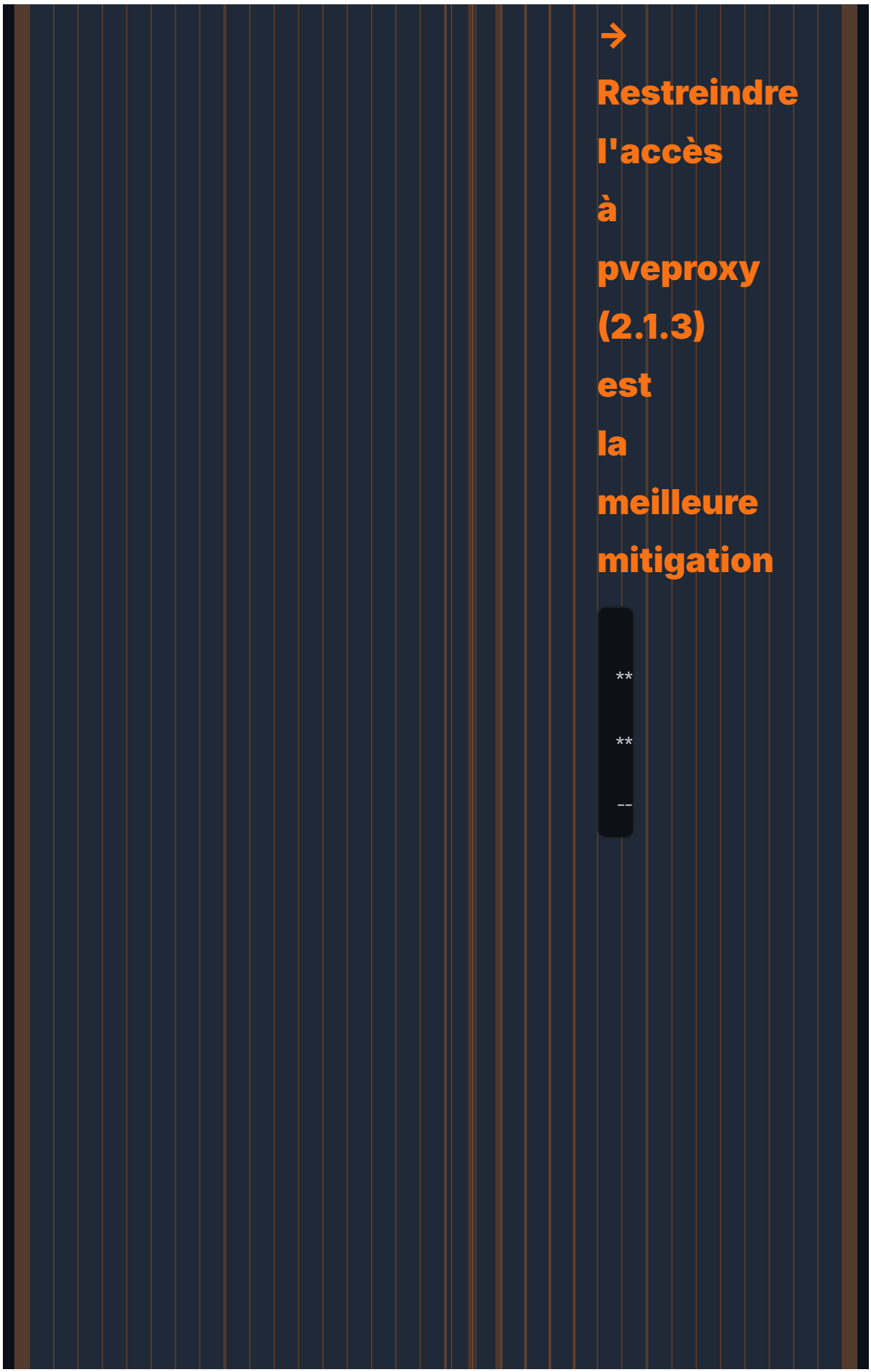
Remédiation :

Désactiver SPICE proxy (port 3128)

systemctl mask --now spiceproxy.service

Note : utiliser 'mask' car pve-manager le réactive avec 'disable'

noVNC est intégré dans pveproxy et ne peut pas être désactivé séparément


→
Restreindre
l'accès
à
pveproxy
(2.1.3)
est
la
meilleure
mitigation
**
**
--

2.2 — API Proxmox

2.2.1 Préférer les tokens API aux mots de passe

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	5.2 — Use Unique Passwords, 5.4 — Restrict Administrator Privileges
MITRE ATT&CK	T1078 (Valid Accounts), T1552 (Unsecured Credentials), M1026 (Privileged Account Management)
ISO 27001:2022	A.5.17, A.8.5
PCI DSS V4.0	8.3.1, 8.6.1
SCÉNARIO THREAT MODEL	S1, S6
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

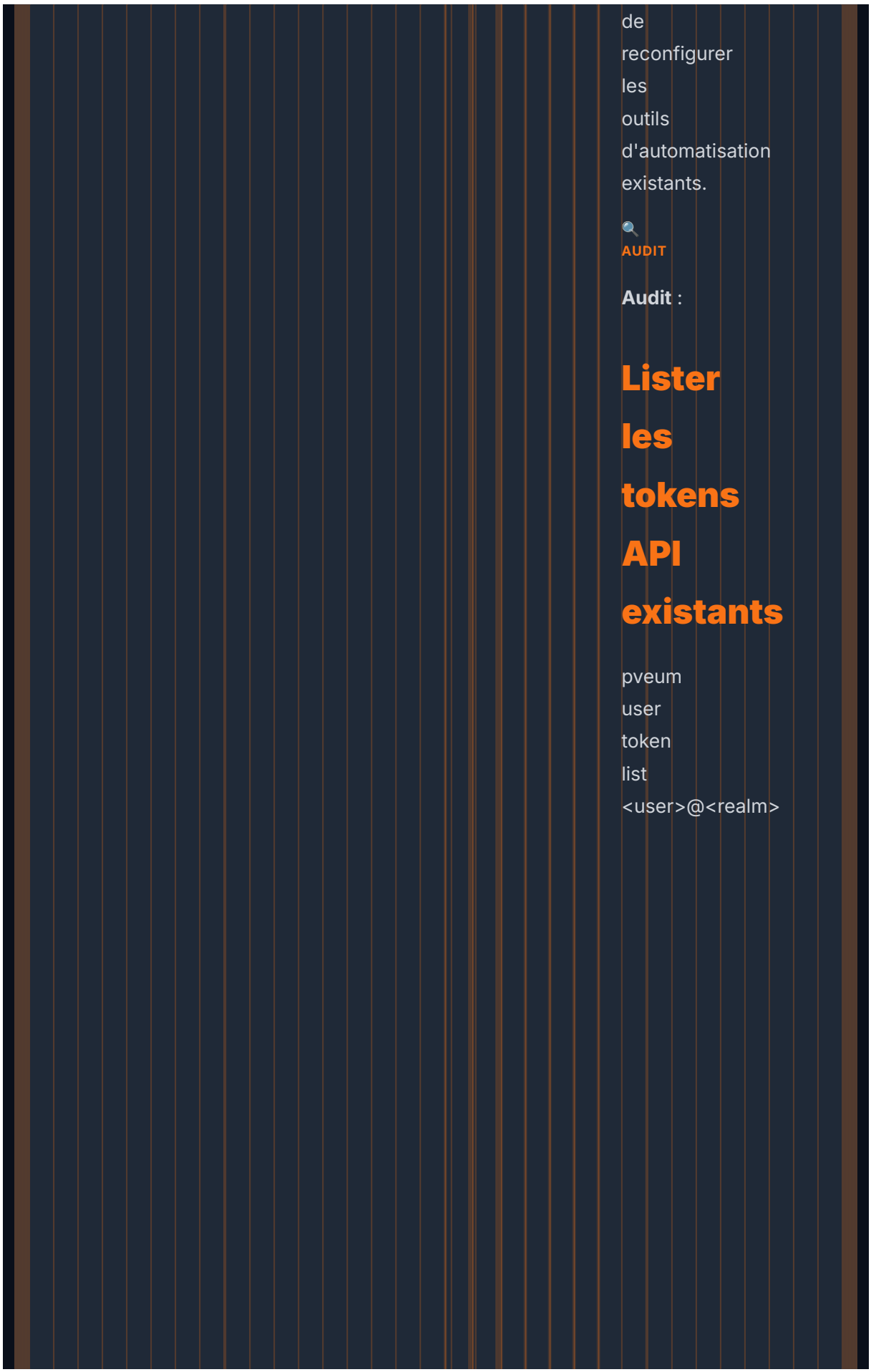
RATIONALE :

Rationale :

Impact :

Faible.

Nécessite



de reconfigurer les outils d'automatisation existants.

🔍 AUDIT

Audit :

Lister les tokens API existants

pveum user token list <user>@<realm>

Résultat attendu : tokens dédiés par outil/service

Vérifier qu'aucun script n'utilise de mot de passe en dur

```
grep
-rn
"password\|
PVE_PASSWORD"
/
root/
/
home/
/
```

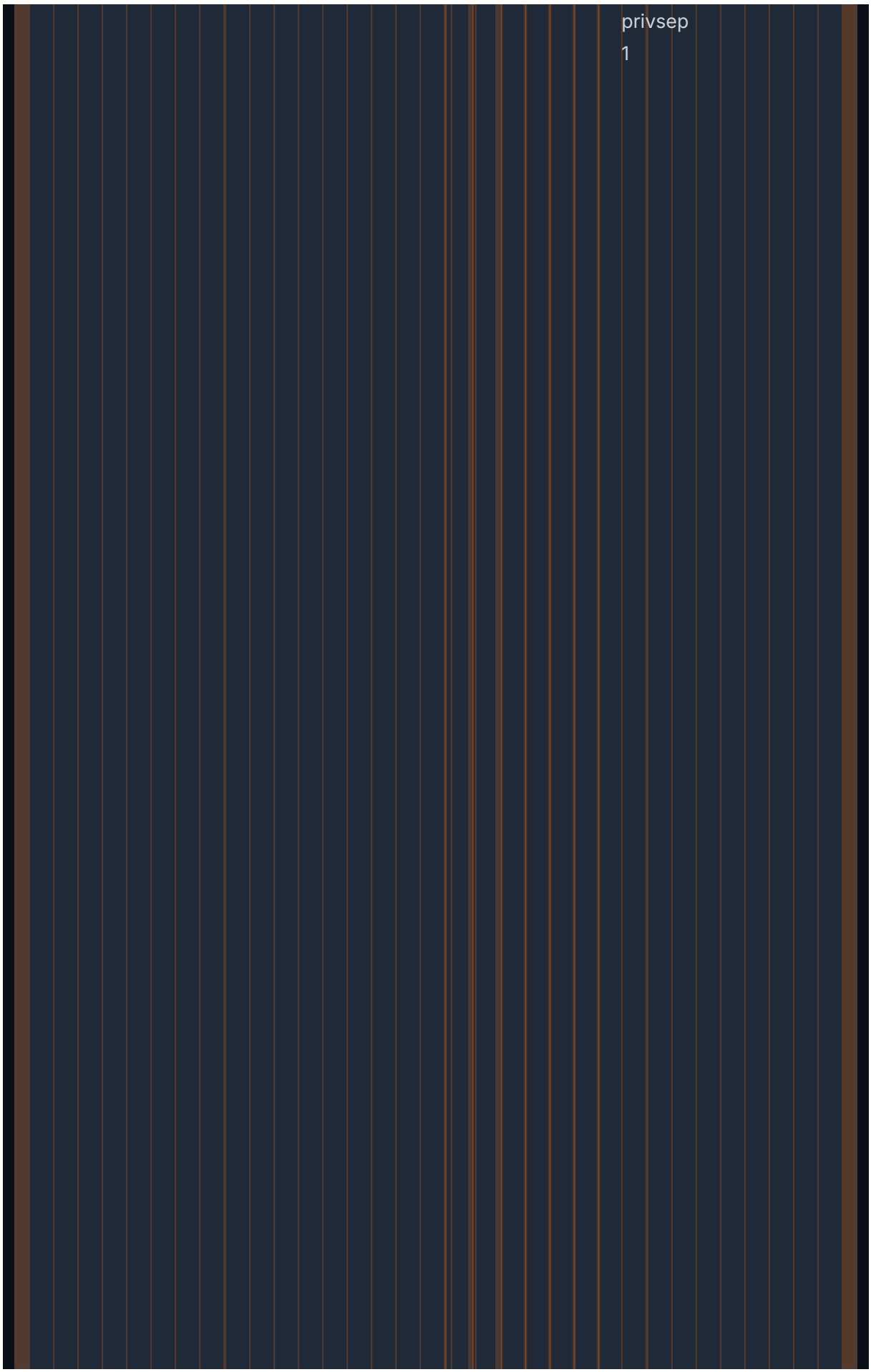
opt/
/
etc/
cron*
2>/
dev/
null

Résultat attendu : aucune correspondance

**

Créer un token API pour Ansible (exemple)

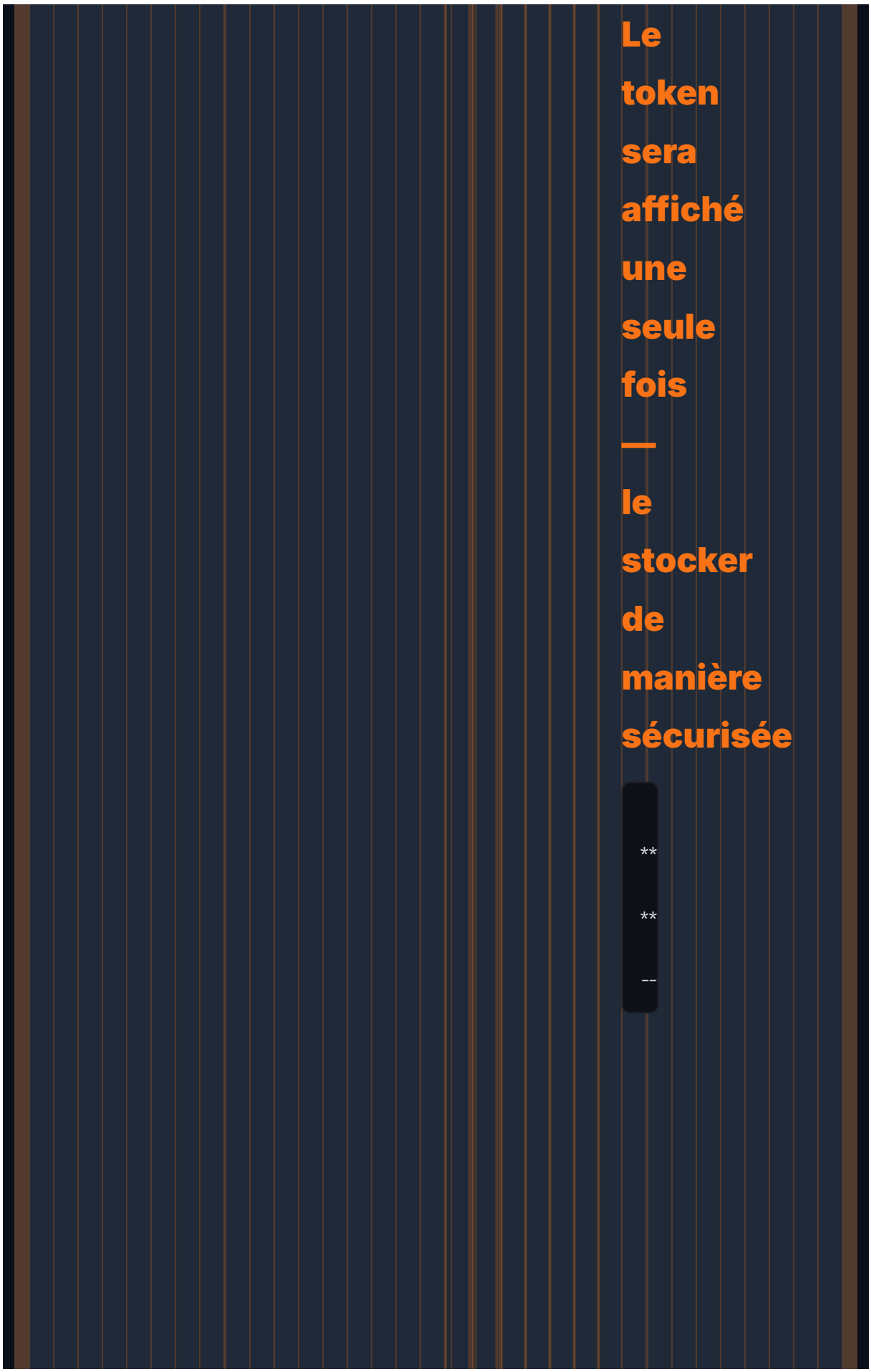
pveum
user
token
add
ansible@pve
ansible-
token
--


privsep
1


privsep=1 : le token a ses propres privilèges (séparés de l'utilisateur)
privsep=0 : le token hérite des privilèges de l'utilisateur

Attribuer uniquement les privilèges nécessaires

```
pveum
acl
modify /
--
token
'ansible@pve!
ansible-
token'
--
role
PVEVMAdmin
```


Le
token
sera
affiché
une
seule
fois
—
le
stocker
de
manière
sécurisée
**
**

2.2.2 Restreindre l'accès API par IP

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	4.2, 13.1
MITRE ATT&CK	T1190, M1030
ISO 27001:2022	A.8.20
PCI DSS V4.0	1.2.1
SCÉNARIO THREAT MODEL	S1
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

Remédiation :
Voir 2.1.3 (même mécanisme ALLOW_FROM/ DENY_FROM).

2.2.3 Activer l'audit des appels API

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	8.2, 8.5
MITRE ATT&CK	T1070 (Indicator Removal), M1028 (OS Configuration)
ISO 27001:2022	A.8.15
PCI DSS V4.0	10.2.1
SCÉNARIO THREAT MODEL	S6 (insider)
STATUT PVE 9	✅ Validé (logs pveproxy natifs)

DESCRIPTION :

Description :

RATIONALE :

Rationale :

🔍
AUDIT

Audit :

Vérifier que les logs API existent et sont alimentés

```
ls
-la
/
var/
log/
pveproxy/
access.log
```

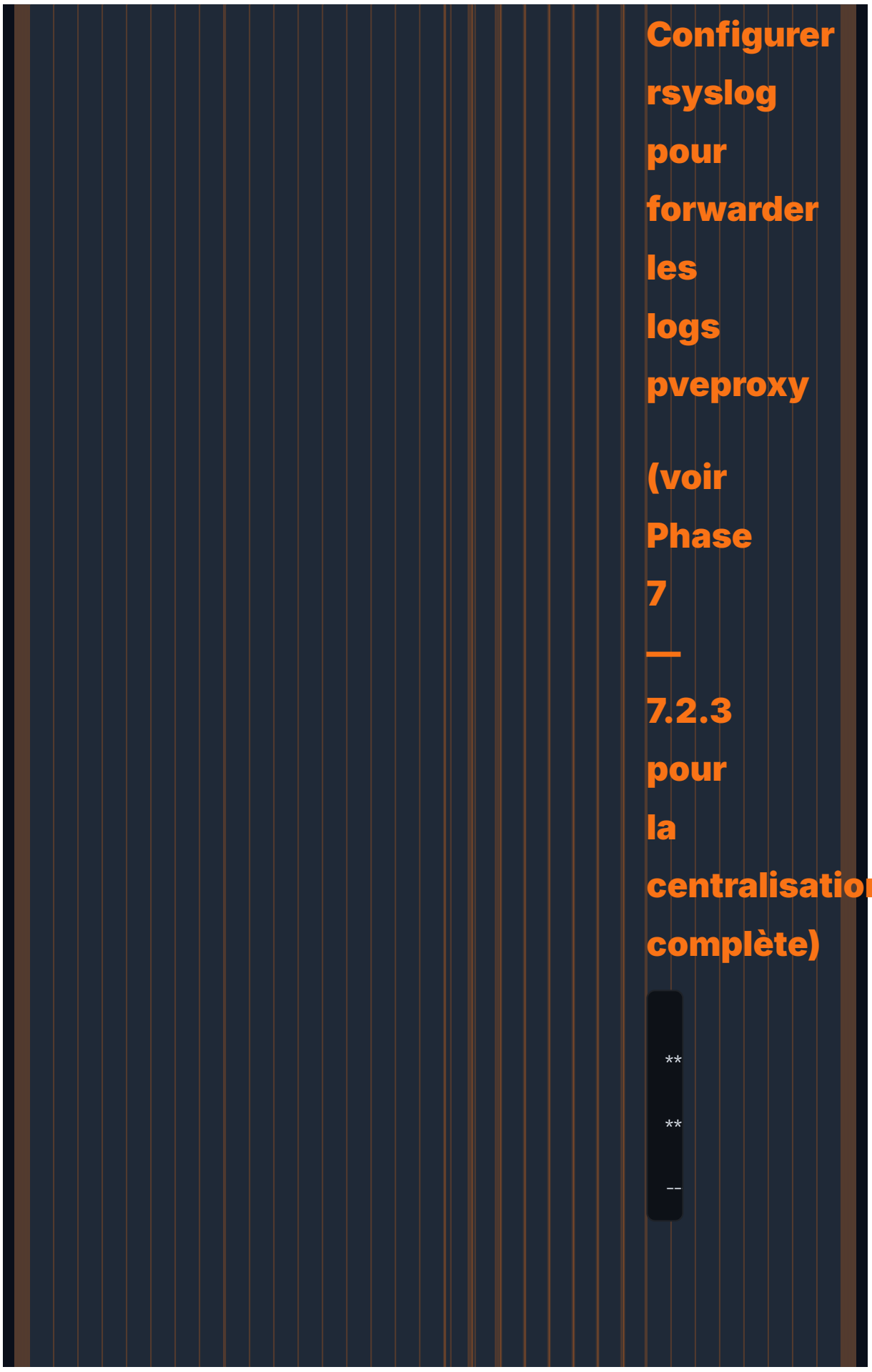
```
tail
-5
/
var/
log/
pveproxy/
access.log
```

Résultat attendu : fichier existant avec des entrées récentes

Vérifier la rotation des logs

```
cat /etc/logrotate.d/pveproxy 2>/dev/null
```

**
Le



Configurer rsyslog pour forwarder les logs pveproxy (voir Phase 7 — 7.2.3 pour la centralisation complète)

```
**
**
--
```

2.3 — Cluster Proxmox

2.3.1

Chiffrer les communications Corosync

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏢 (clusters uniquement)
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	3.10, 12.6
MITRE ATT&CK	T1557 (AitM), T1040 (Network Sniffing), M1041 (Encrypt Sensitive Information)
ISO 27001:2022	A.8.24
PCI DSS V4.0	4.2.1
SCÉNARIO THREAT MODEL	S4 (mouvement latéral cluster)
STATUT PVE 9	✅ Validé

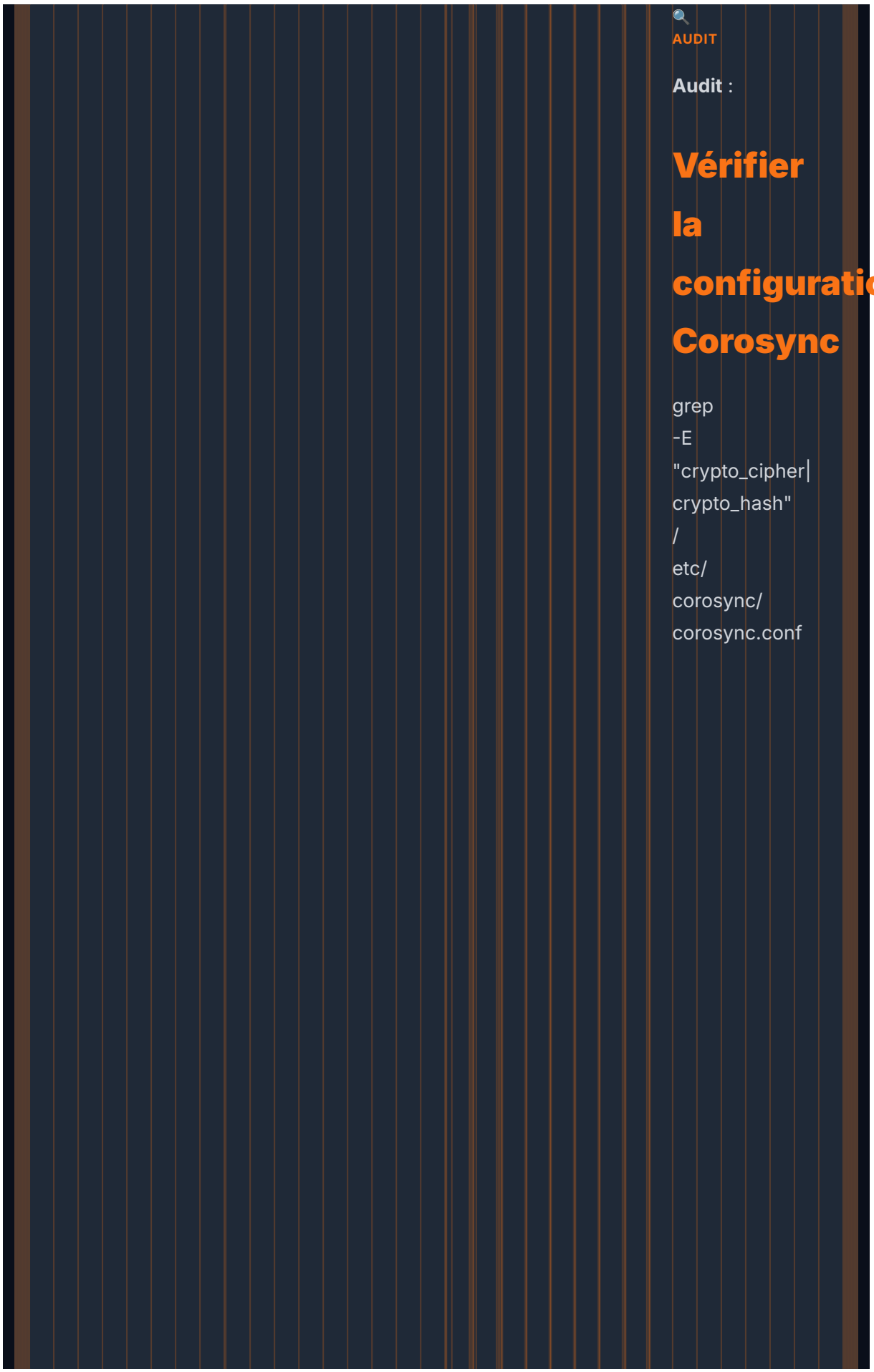
DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Faible. Surcoût CPU négligeable avec AES-NI.

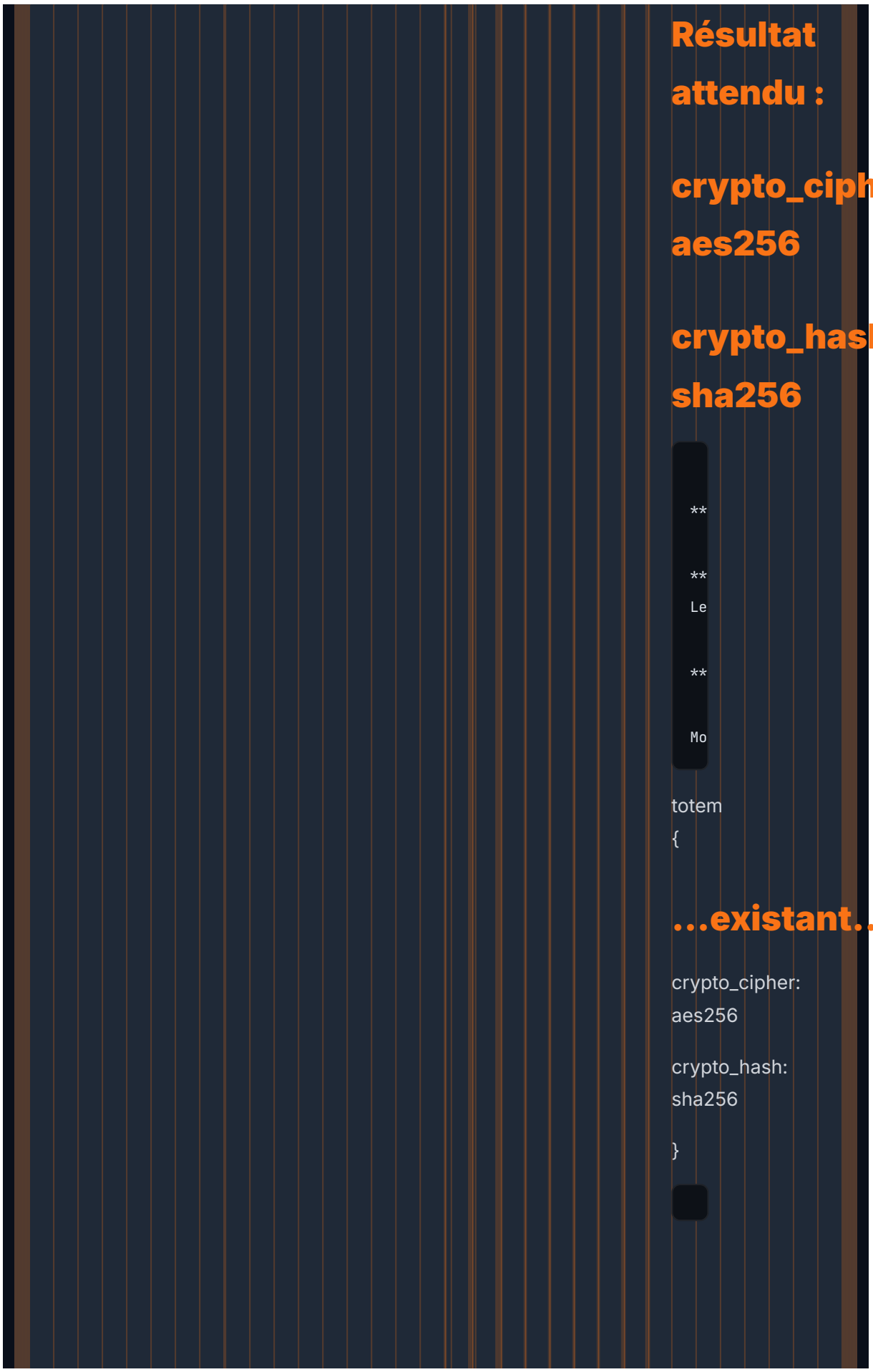


🔍
AUDIT

Audit :

Vérifier la configuration Corosync

```
grep
-E
"crypto_cipher|
crypto_hash"
/
etc/
corosync/
corosync.conf
```



Résultat attendu :

crypto_cipher: aes256

crypto_hash: sha256

```
**
**
Le
**
Mo
```

totem
{

...existant...

crypto_cipher: aes256

crypto_hash: sha256

}

Appliquer sur TOUS les nœuds simultanément (fenêtre de maintenance)

systemctl
restart
corosync

```
**
**
**
--
```

2.3.2

Sécuriser le filesystem cluster /etc/pve

Level 1

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏢
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	3.3, 4.1
MITRE ATT&CK	T1552.004 (Private Keys), T1213 (Data from Information Repositories)
ISO 27001:2022	A.8.3, A.8.12
PCI DSS V4.0	3.5.1, 7.2.1
SCÉNARIO THREAT MODEL	S4, S6
STATUT PVE 9	✅ Validé

DESCRIPTION :

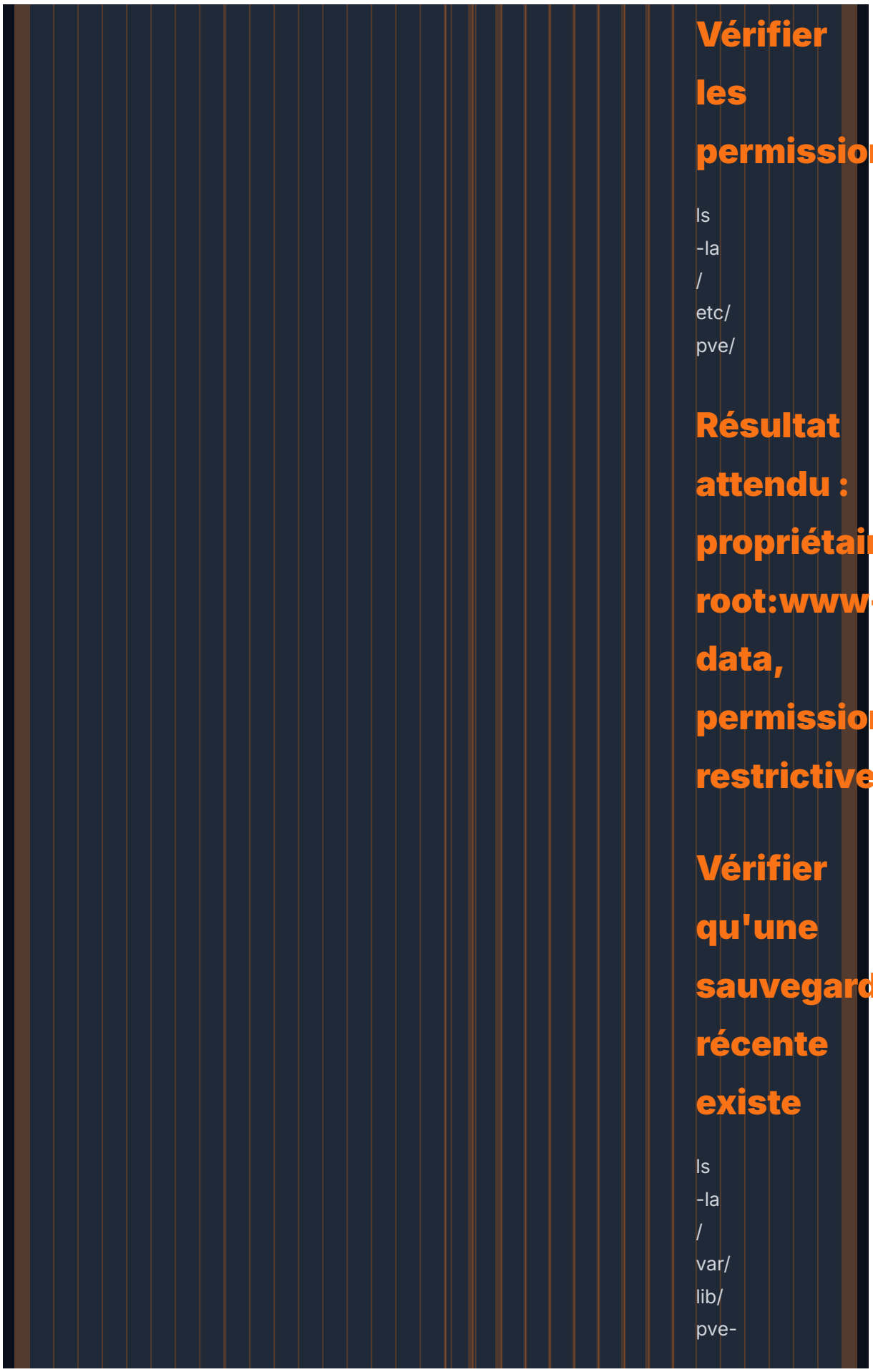
Description :

RATIONALE :

Rationale :

🔍
AUDIT

Audit :



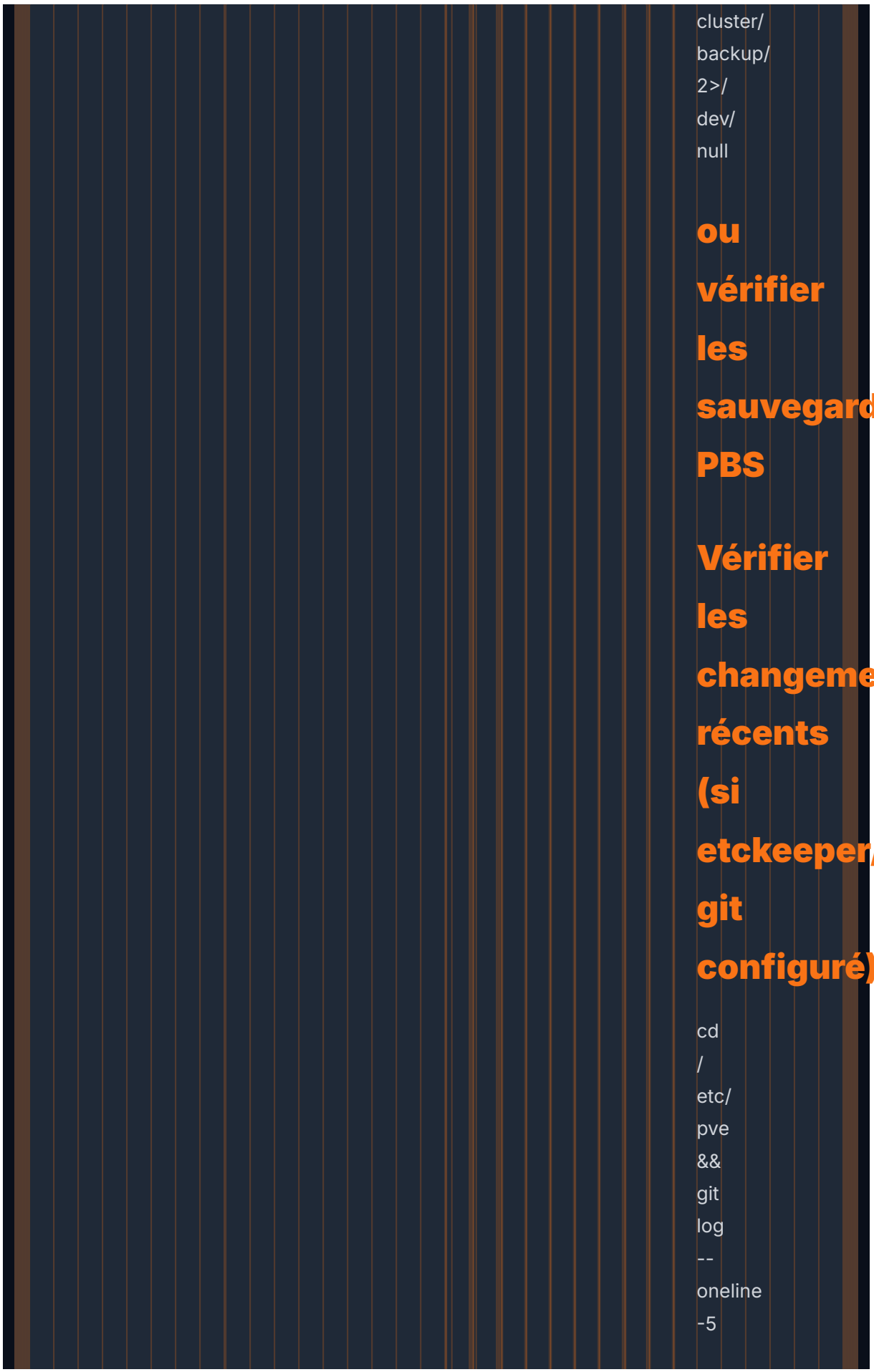
Vérifier les permissions

```
ls
-la
/
etc/
pve/
```

Résultat attendu : propriétaire root:www-data, permissions restrictives

Vérifier qu'une sauvegarde récente existe

```
ls
-la
/
var/
lib/
pve-
```



```
cluster/
backup/
2>/
dev/
null
```

ou vérifier les sauvegardes PBS

Vérifier les changements récents (si etckeeper/ git configuré)

```
cd
/
etc/
pve
&&
git
log
--
oneline
-5
```

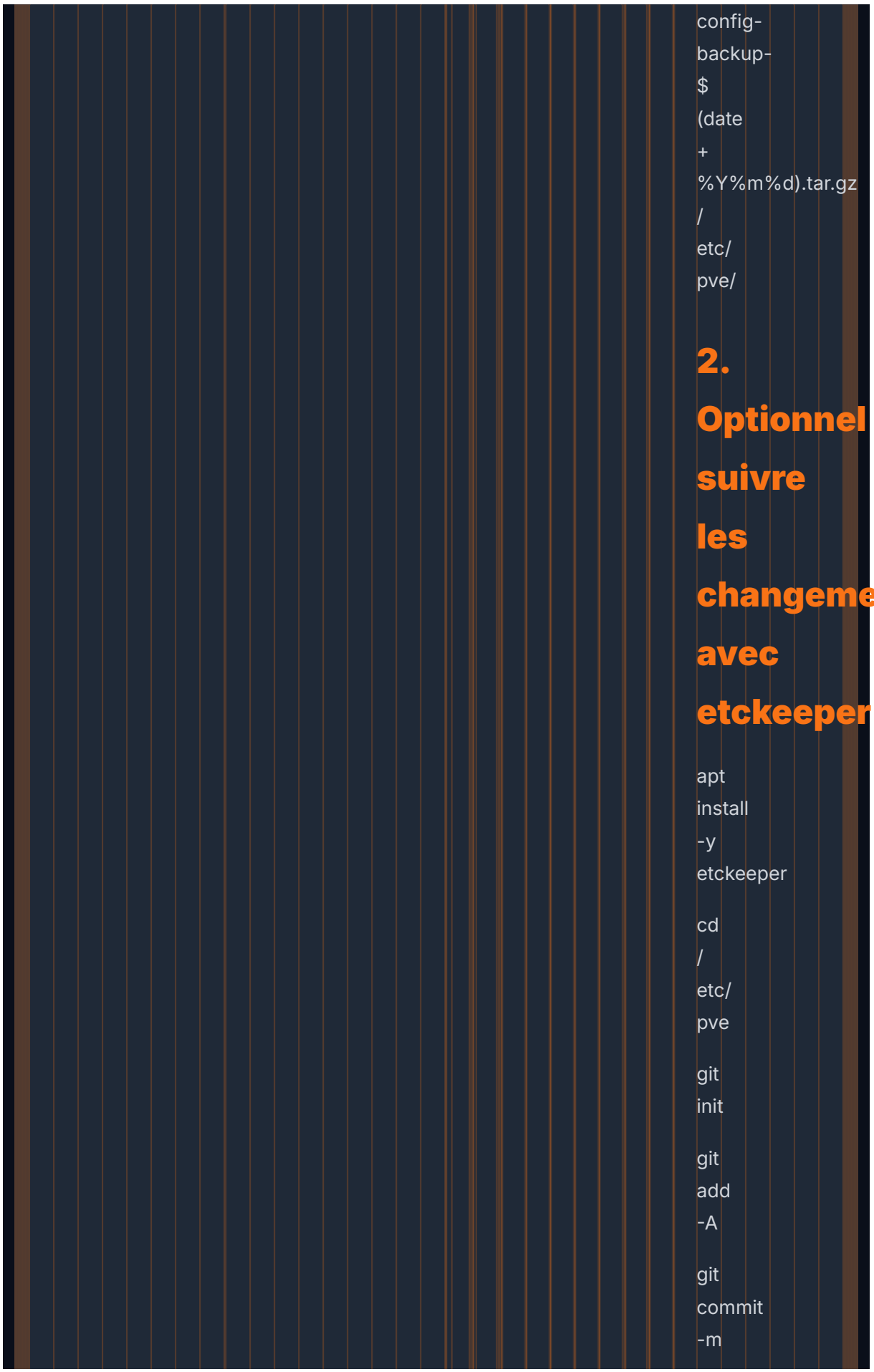
2>/
dev/
null

**

1. Sauvegarder régulièrement /etc/pve

Via vzdump (inclus dans les backups PVE) ou manuellement :

tar
czf
/
root/
pve-



```
config-
backup-
$
(date
+
%Y%m%d).tar.gz
/
etc/
pve/
```

2. Optionnel : suivre les changements avec etckeeper

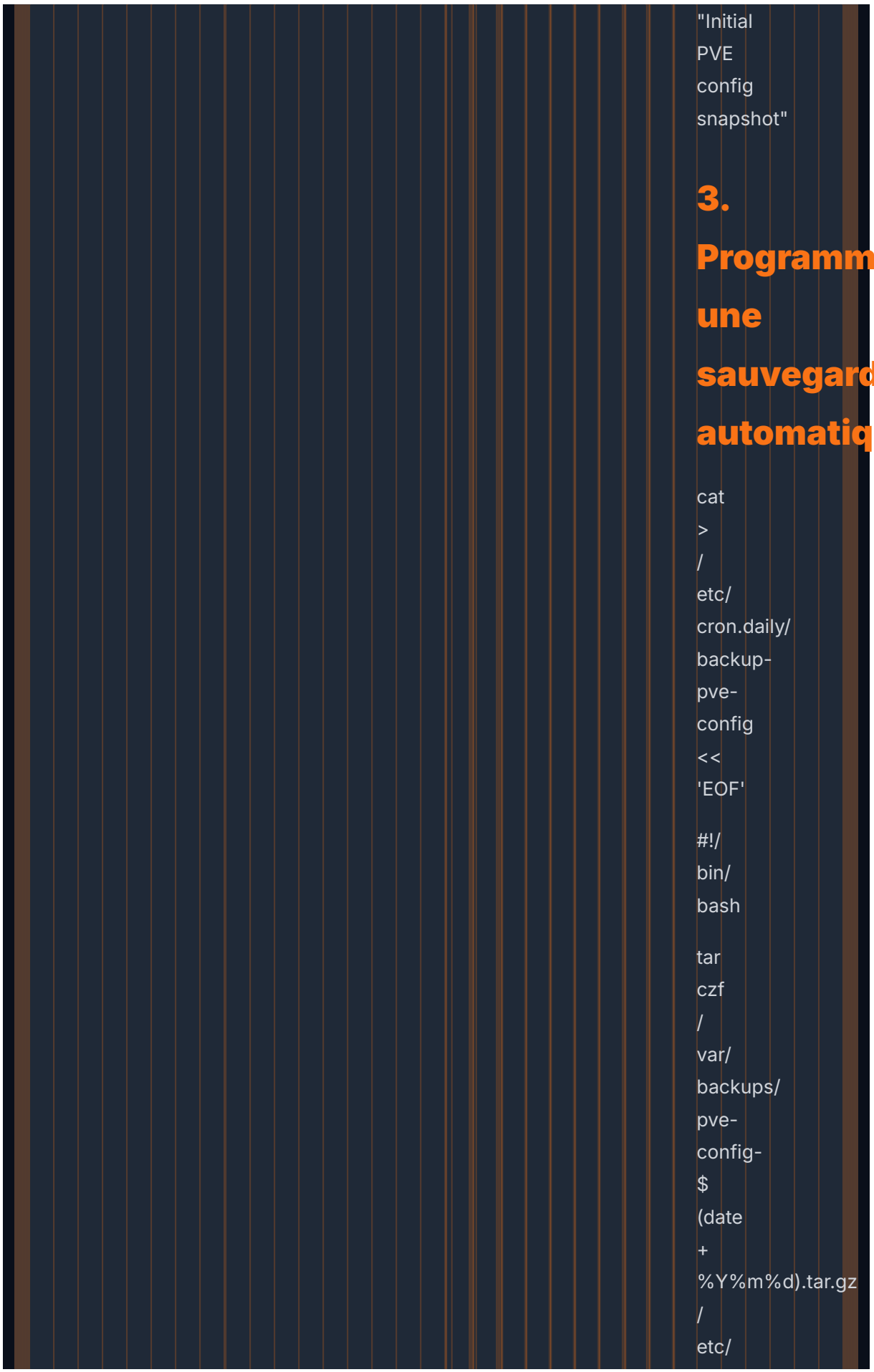
```
apt
install
-y
etckeeper
```

```
cd
/
etc/
pve
```

```
git
init
```

```
git
add
-A
```

```
git
commit
-m
```



```
"Initial
PVE
config
snapshot"
```

3. Programmer une sauvegarde automatique

```
cat
>
/
etc/
cron.daily/
backup-
pve-
config
<<
'EOF'

#!/
bin/
bash

tar
czf
/
var/
backups/
pve-
config-
$
(date
+
%Y%m%d).tar.gz
/
etc/
```

```
pve/
2>/
dev/
null

find
/
var/
backups/
-name
"pve-
config-
*.tar.gz"
-mtime
+30
-delete

EOF

chmod
+x
/
etc/
cron.daily/
backup-
pve-
config
```

**

**

--

2.3.3

Sécuriser les migrations live

Level 2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	3.10
MITRE ATT&CK	T1557, T1040
ISO 27001:2022	A.8.24
PCI DSS V4.0	4.2.1
SCÉNARIO THREAT MODEL	S9 (interception trafic)
STATUT PVE 9	✅ Validé

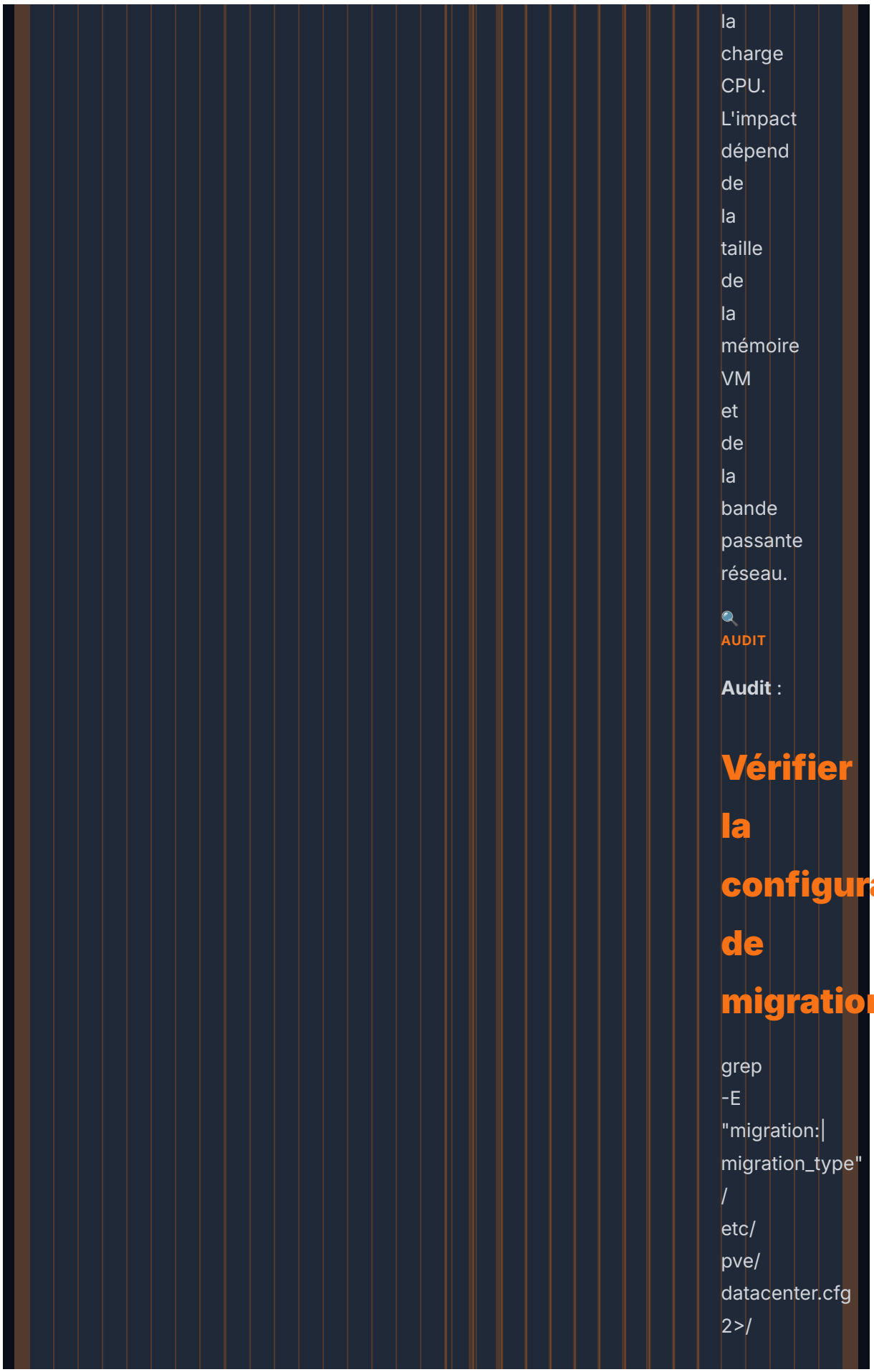
DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Moyen. Le chiffrement de la migration augmente la durée de migration et



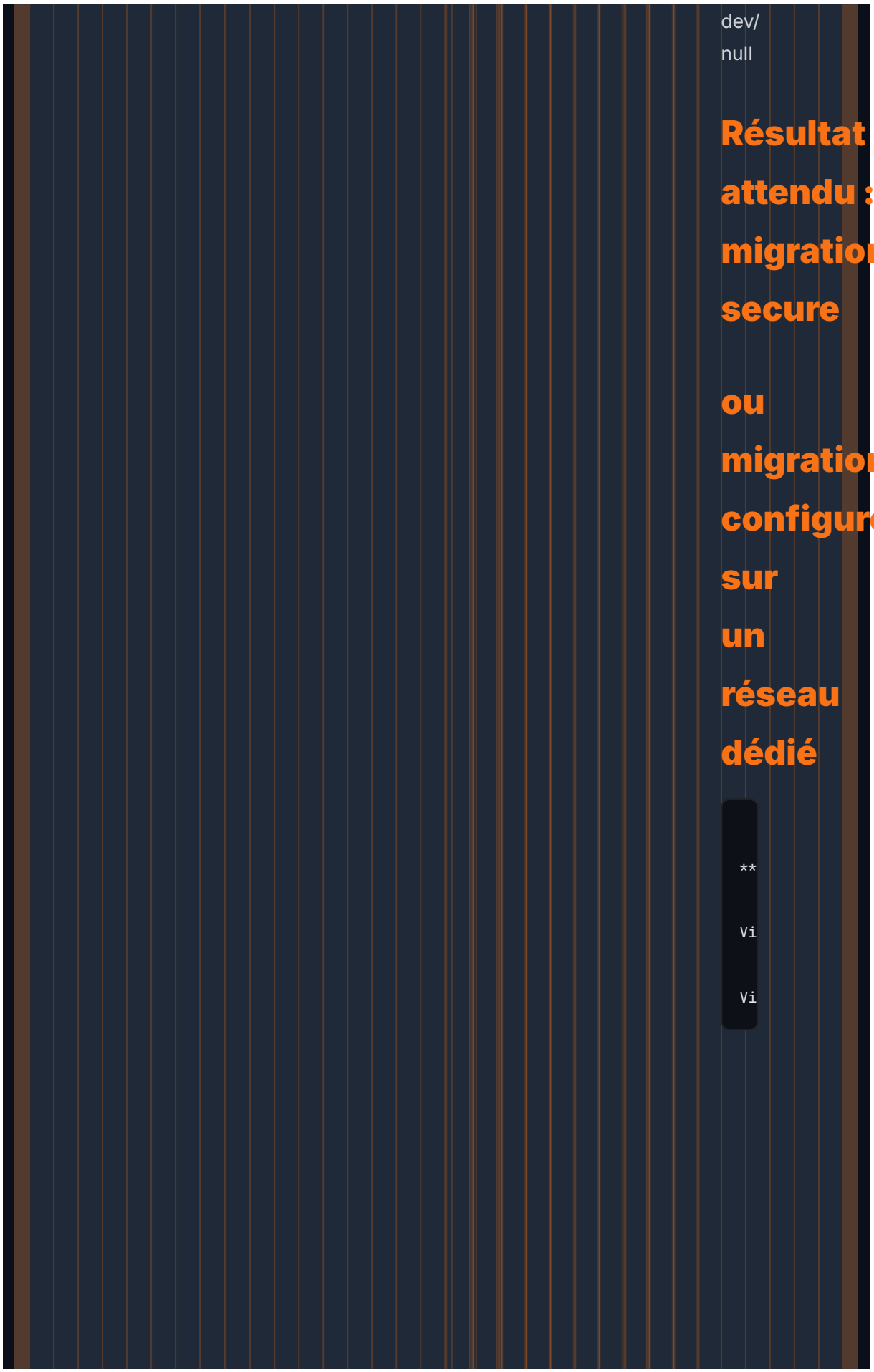
la charge CPU. L'impact dépend de la taille de la mémoire VM et de la bande passante réseau.

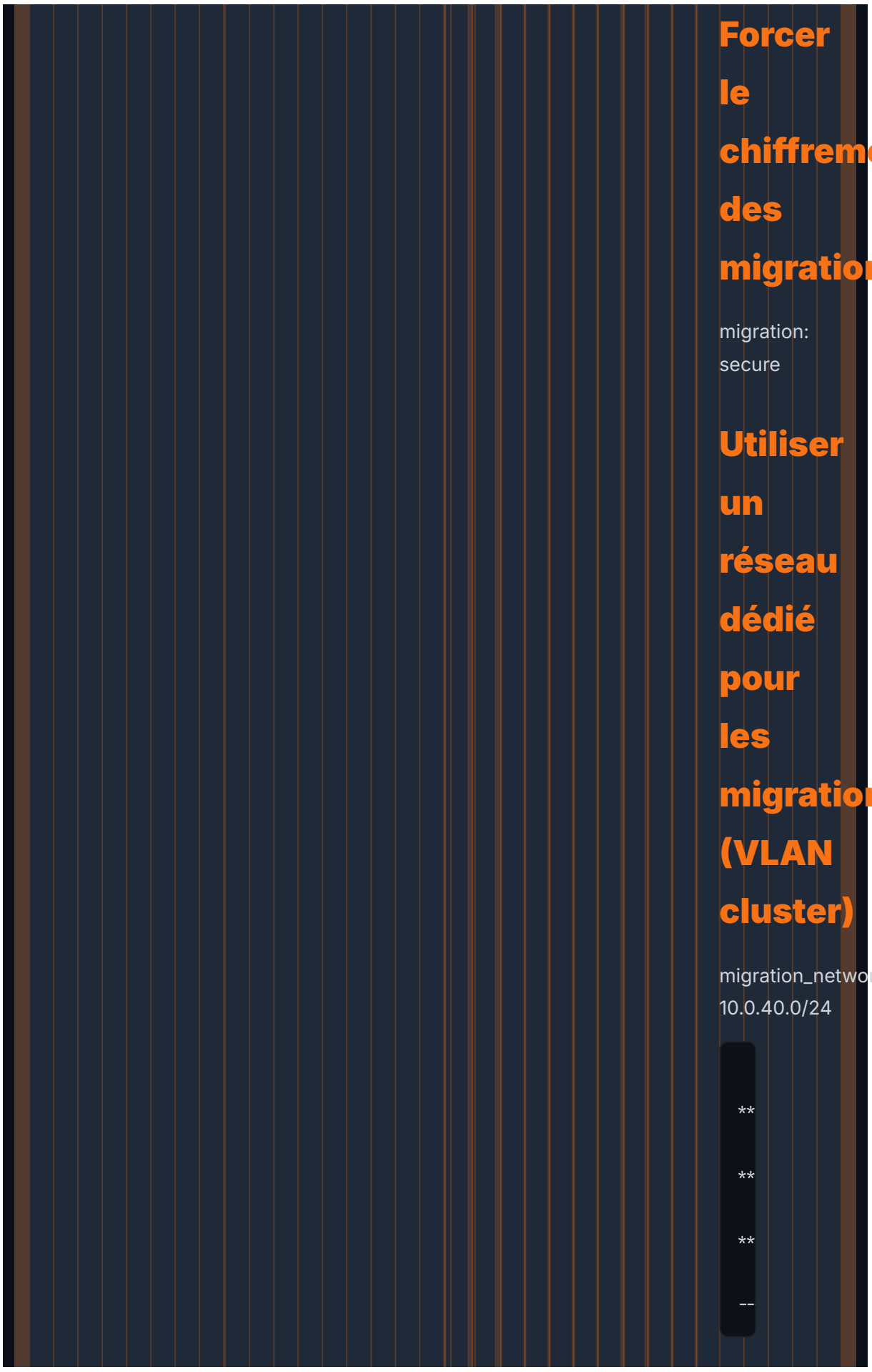
🔍 AUDIT

Audit :

Vérifier la configuration de migration

```
grep -E "migration:|migration_type" /etc/pve/datacenter.cfg 2>/
```


dev/
null
Résultat attendu : migration: secure
ou migration_netwo
configuré sur un réseau dédié
**
Vi
Vi



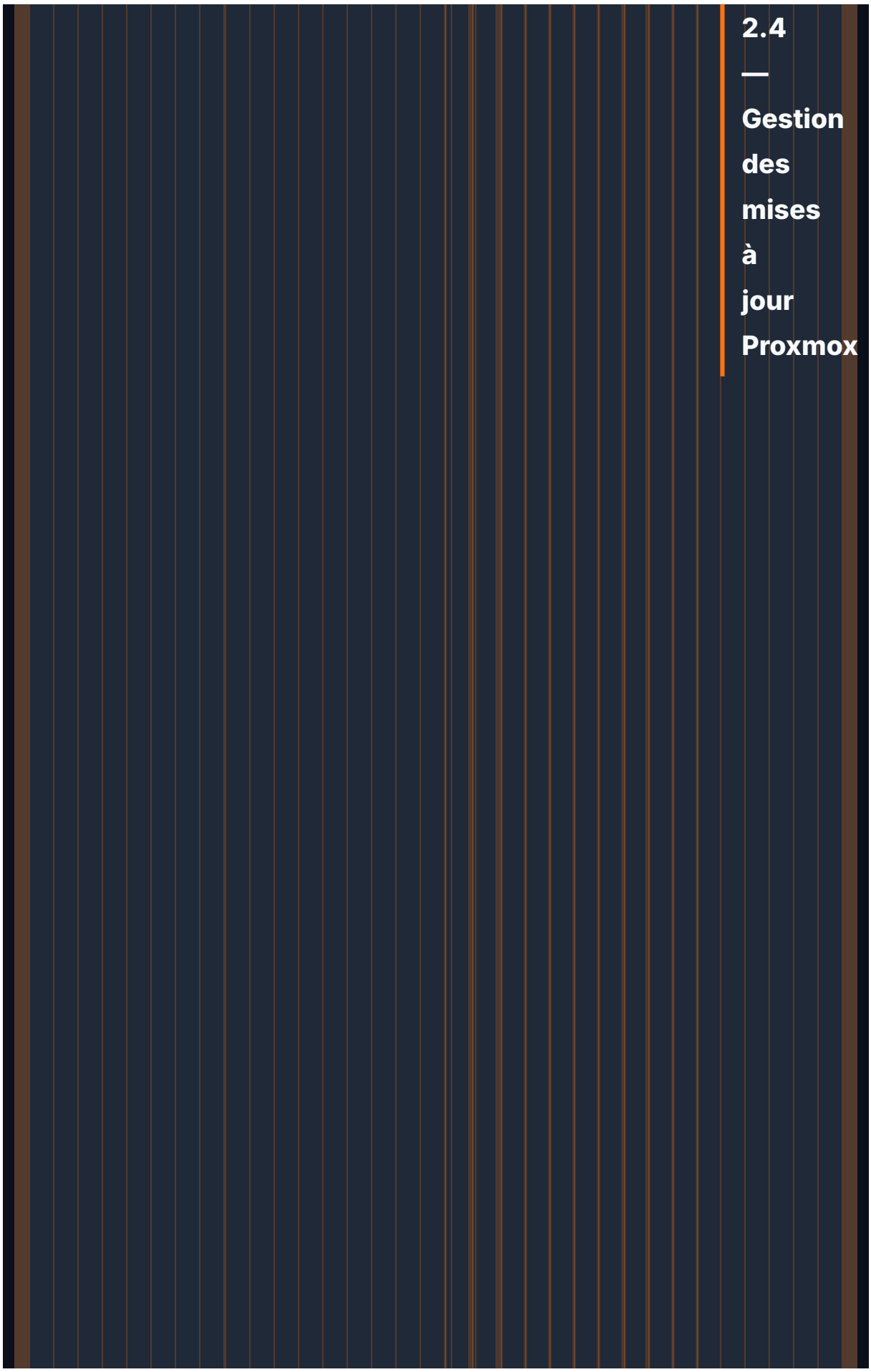
Forcer le chiffrement des migrations

migration: secure

Utiliser un réseau dédié pour les migrations (VLAN cluster)

migration_network: 10.0.40.0/24

```
**
**
**
--
```



2.4 — Gestion des mises à jour Proxmox

2.4.1

Définir une stratégie de mise à jour PVE

Level

PROFILE APPLICABILITY	Level 1 — Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	1.2.2.1 (complémentaire)
CIS CONTROLS V8	7.1, 7.3, 7.4
MITRE ATT&CK	T1190, T1068, M1051 (Update Software)
ISO 27001:2022	A.8.8
PCI DSS V4.0	6.3.3
SCÉNARIO THREAT MODEL	S1, S3
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
La procédure elle-même n'a pas d'impact. L'application des mises

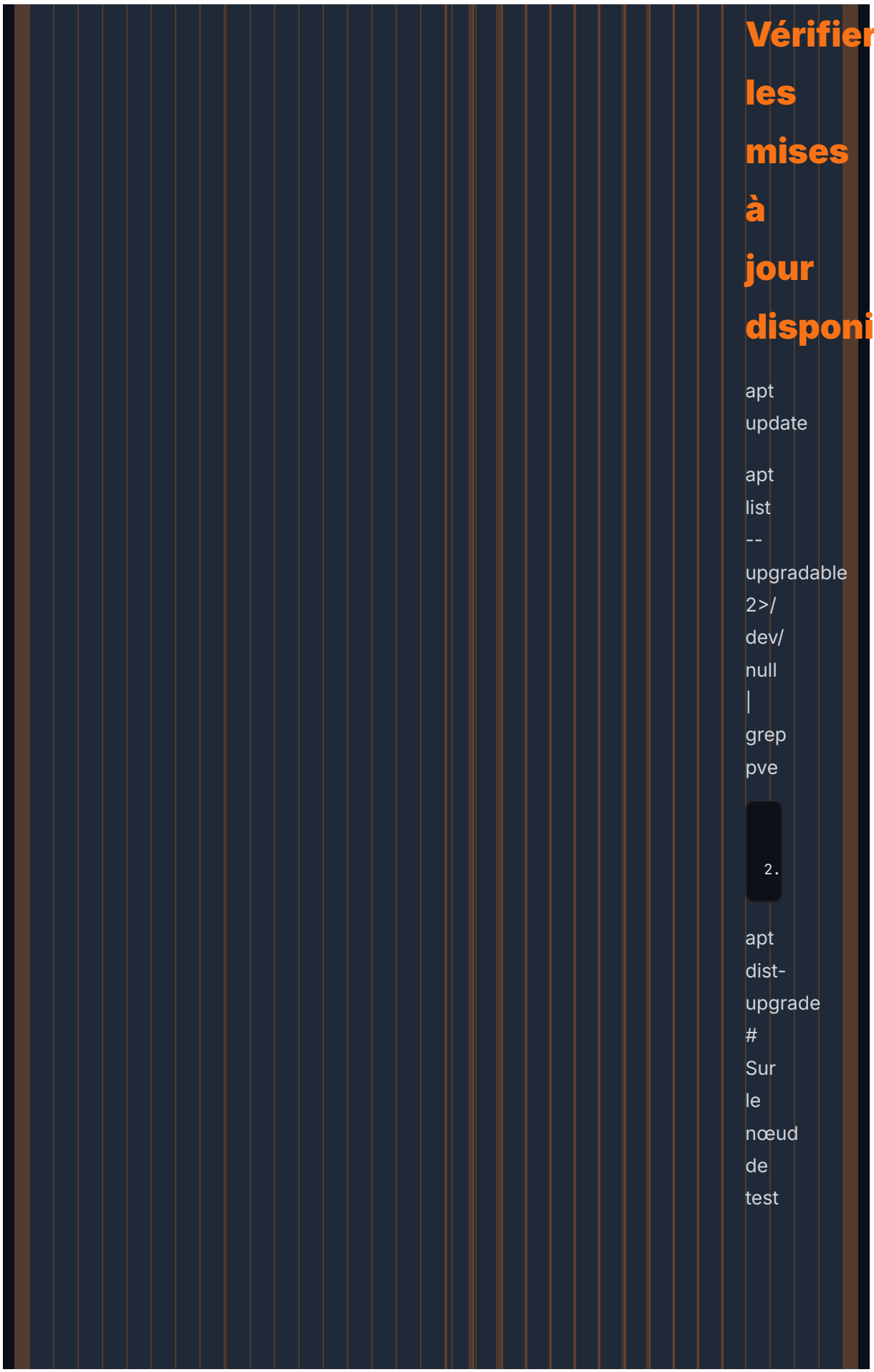
à jour nécessite une fenêtre de maintenance avec reboot potentiel.

🔧 REMÉDIATION

Remédiation :

Procédure de mise à jour recommandée :

1. **Veille** : s'abonner aux listes de diffusion Proxmox et surveiller les advisories

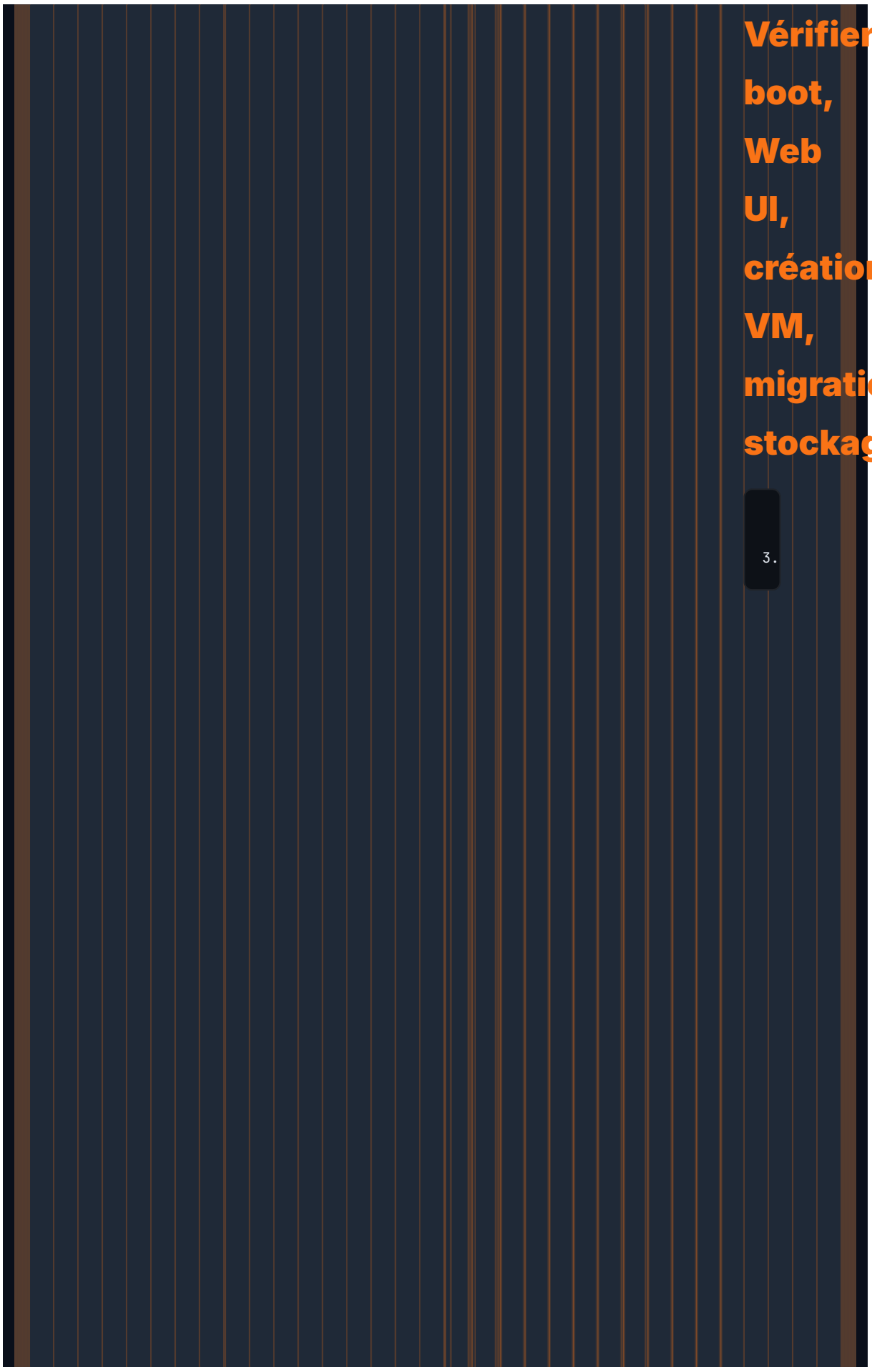


Vérifier les mises à jour disponibles

```
apt update

apt list --upgradable 2>/dev/null | grep pve
```

2.

```
apt dist-upgrade
# Sur le nœud de test
```



Vérifier : boot, Web UI, création VM, migration, stockage

3.

Sur chaque nœud, un par un :

a) Migrer les VM critiques vers un autre nœud

b) Appliquer les mises à jour

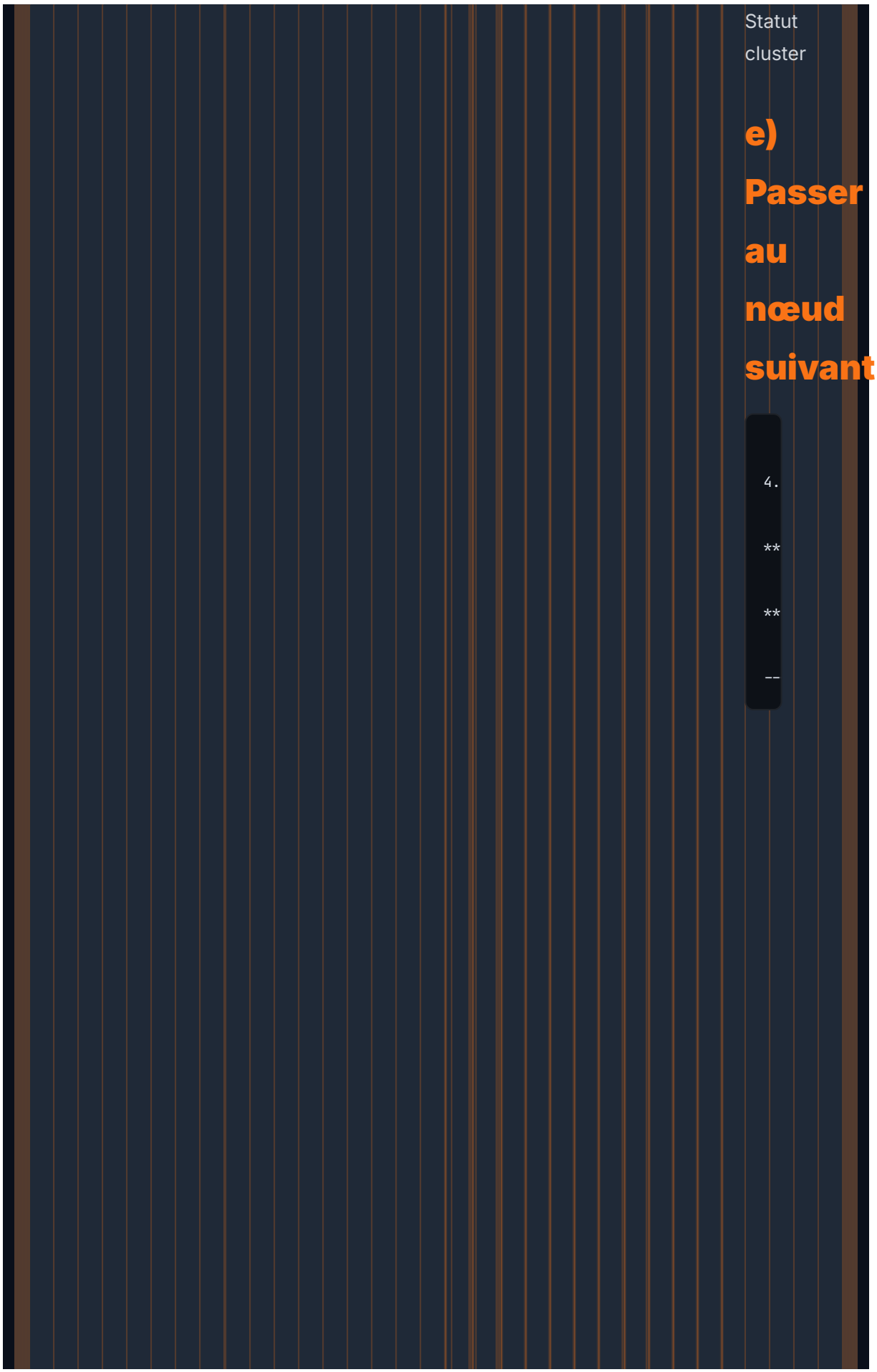
```
apt
dist-
upgrade
```

c) Redémarrer si nécessaire (nouveau kernel)

```
reboot
```

d) Vérifier :

```
pveversion
-v
#
Version
PVE

uname
-r
#
Kernel

systemctl
status
pveproxy
pvedaemon
corosync

pvecm
status
#
```


Statut
cluster
e) Passer au nœud suivant
4.
**
**
--

2.4.2

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	2.2
MITRE ATT&CK	T1068, M1051
ISO 27001:2022	A.8.8
SCÉNARIO THREAT MODEL	S3
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

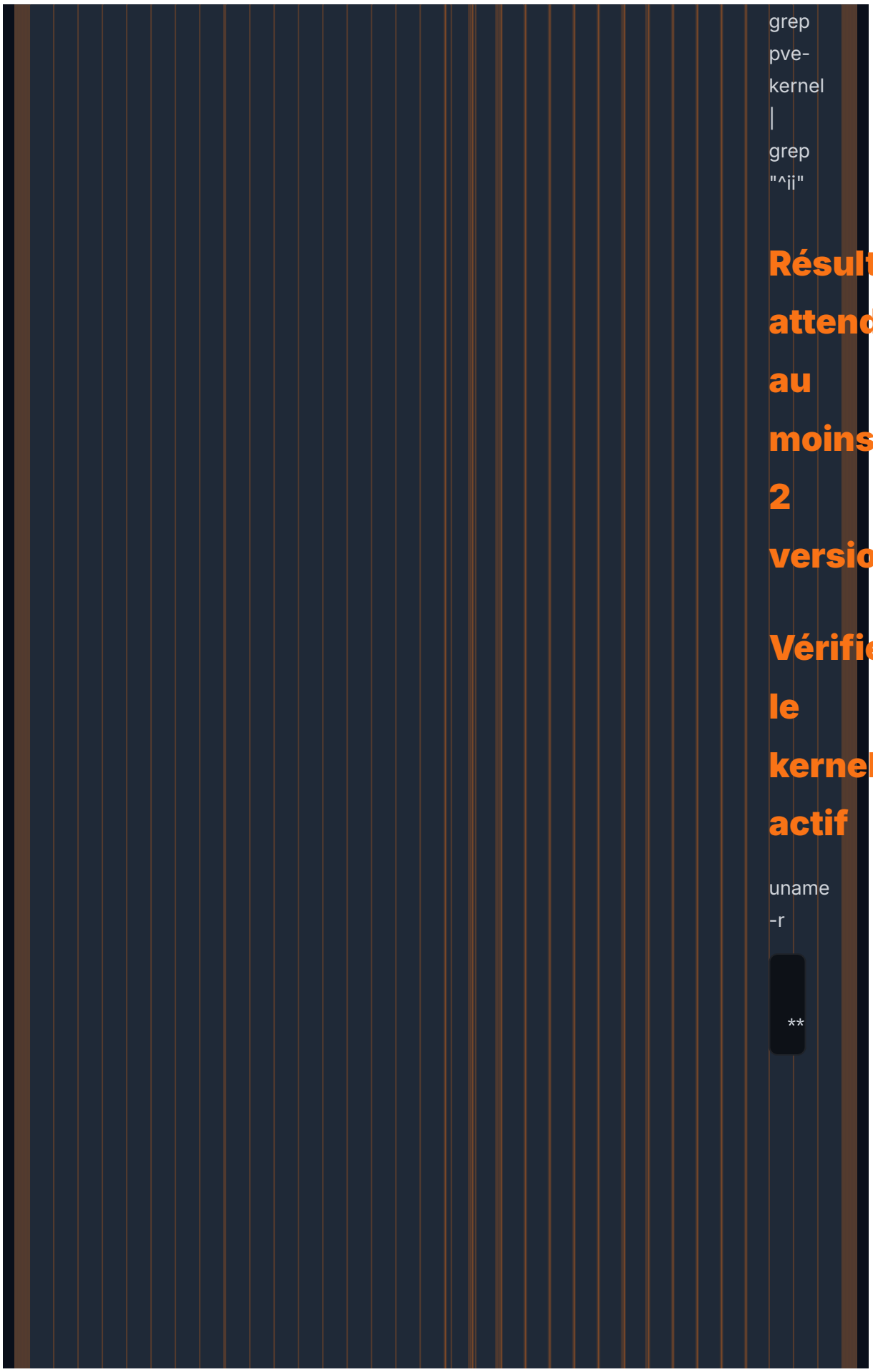
Rationale :

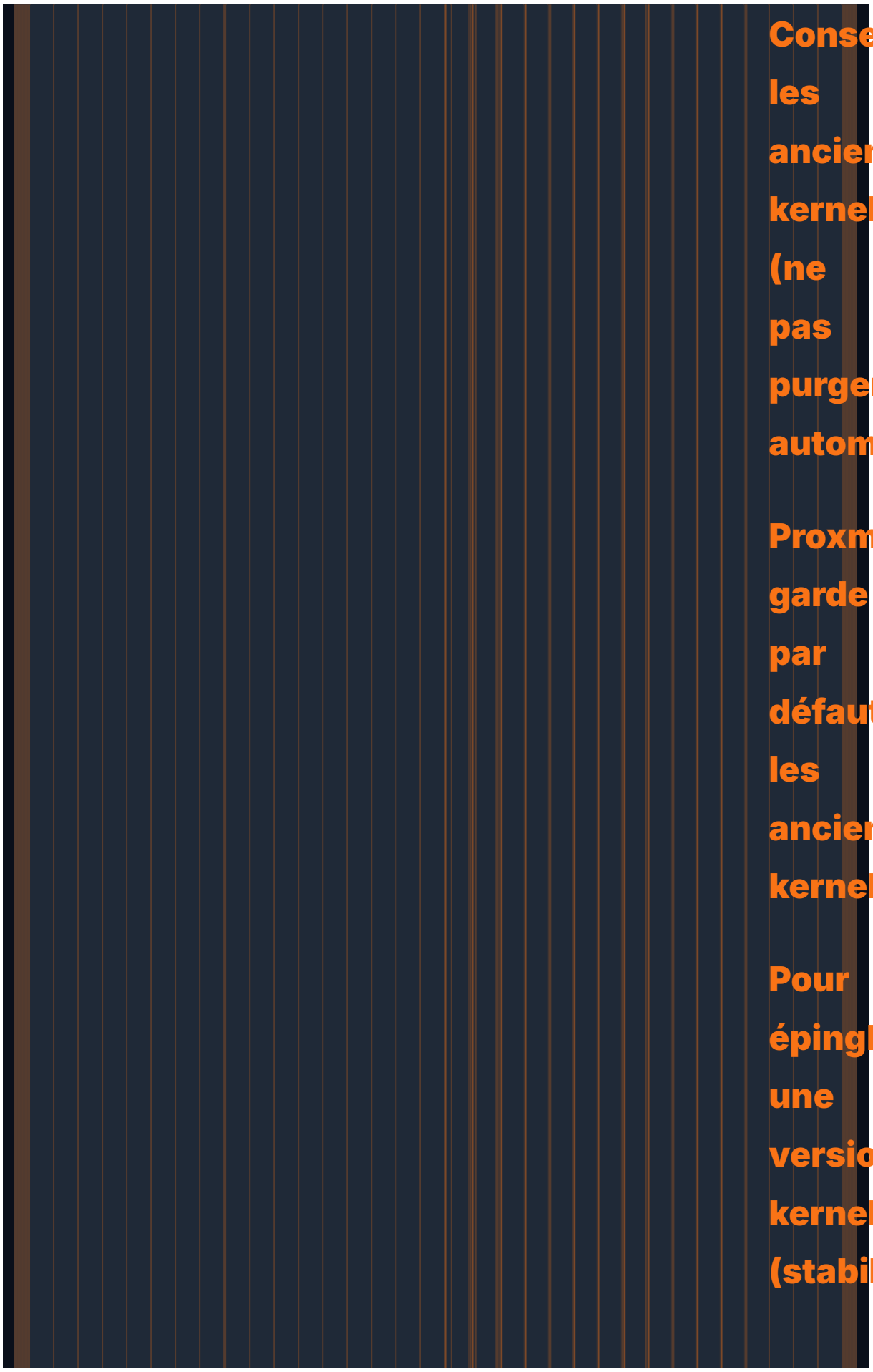
🔍 AUDIT

Audit :

Lister les kernels installés

```
dpkg
-l
|
```

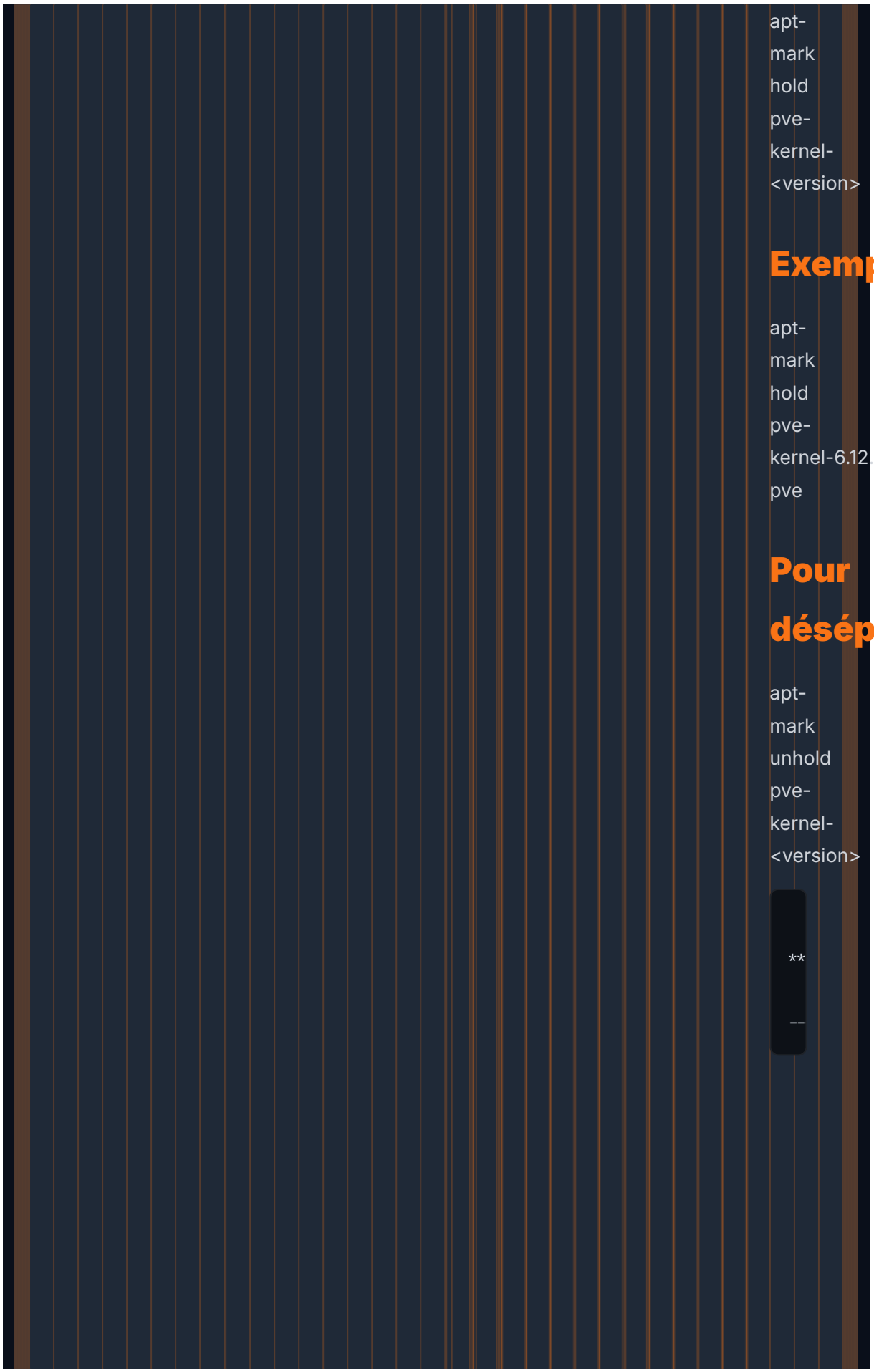

grep
pve-
kernel
|
grep
"^ii"
Résultat attendu : au moins 2 versions
Vérifier le kernel actif
uname
-r
**

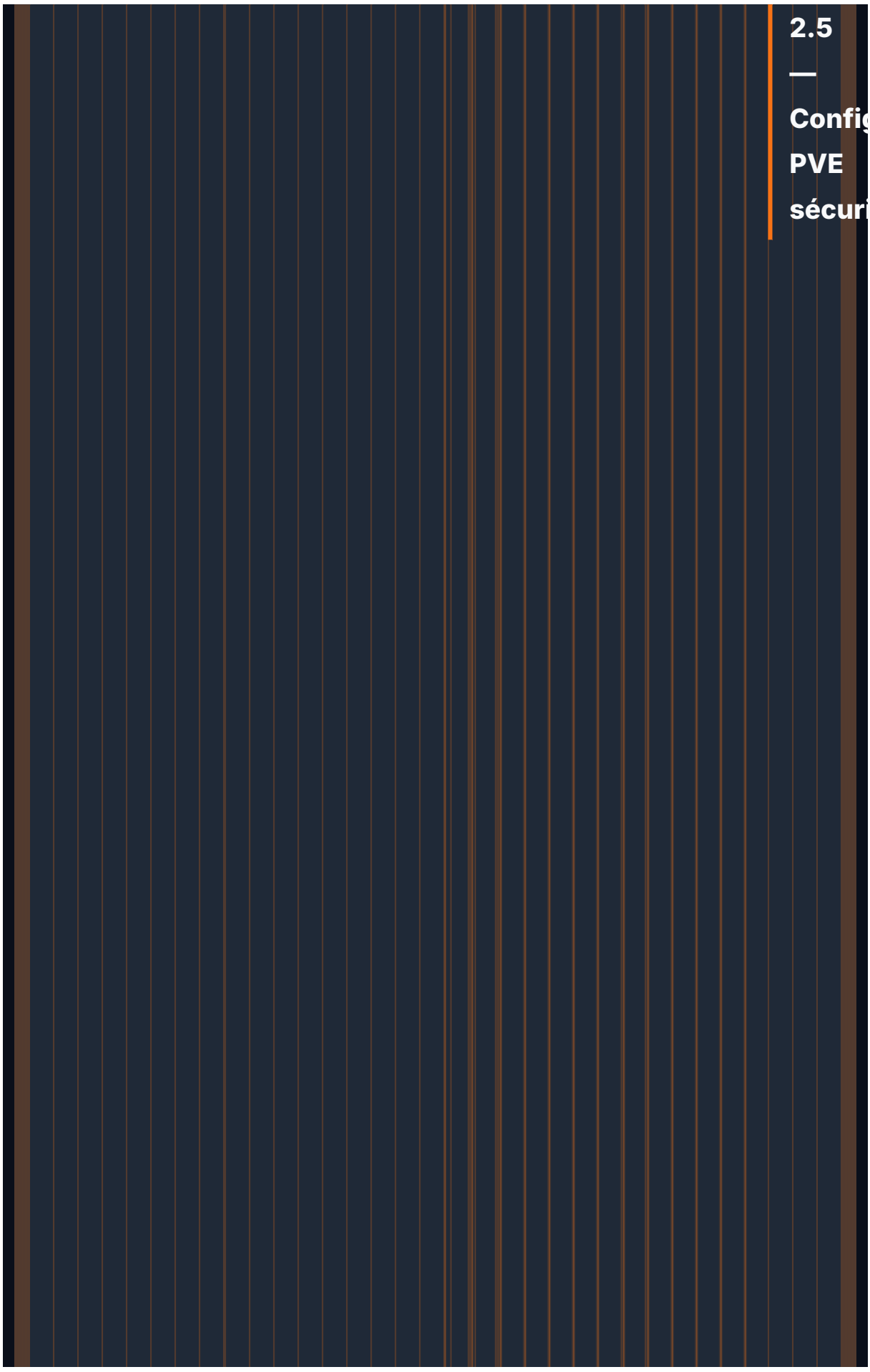


Conserver les anciens kernels (ne pas purger automatiquen

Proxmox garde par défaut les anciens kernels

Pour épingler une version kernel (stabilité) :


apt-mark hold pve-kernel-<version>
Exemple :
apt-mark hold pve-kernel-6.12.6-1-pve
Pour désépingler :
apt-mark unhold pve-kernel-<version>
**
--



2.5 — Configuration PVE sécurisée

2.5.1

Suivre les modificatio de configurati avec etckeeper

PROFILE APPLICABILITY	Level 2 — Server
APPLICABILITÉ PVE	🏢🌐
RÉF. CIS DEBIAN 13	Spécifique Proxmox
CIS CONTROLS V8	4.1, 8.2
MITRE ATT&CK	T1070 (Indicator Removal), M1028
ISO 27001:2022	A.8.9, A.8.15
PCI DSS V4.0	10.2.1
SCÉNARIO THREAT MODEL	S6
STATUT PVE 9	✅ Validé

DESCRIPTION :

Description :

RATIONALE :

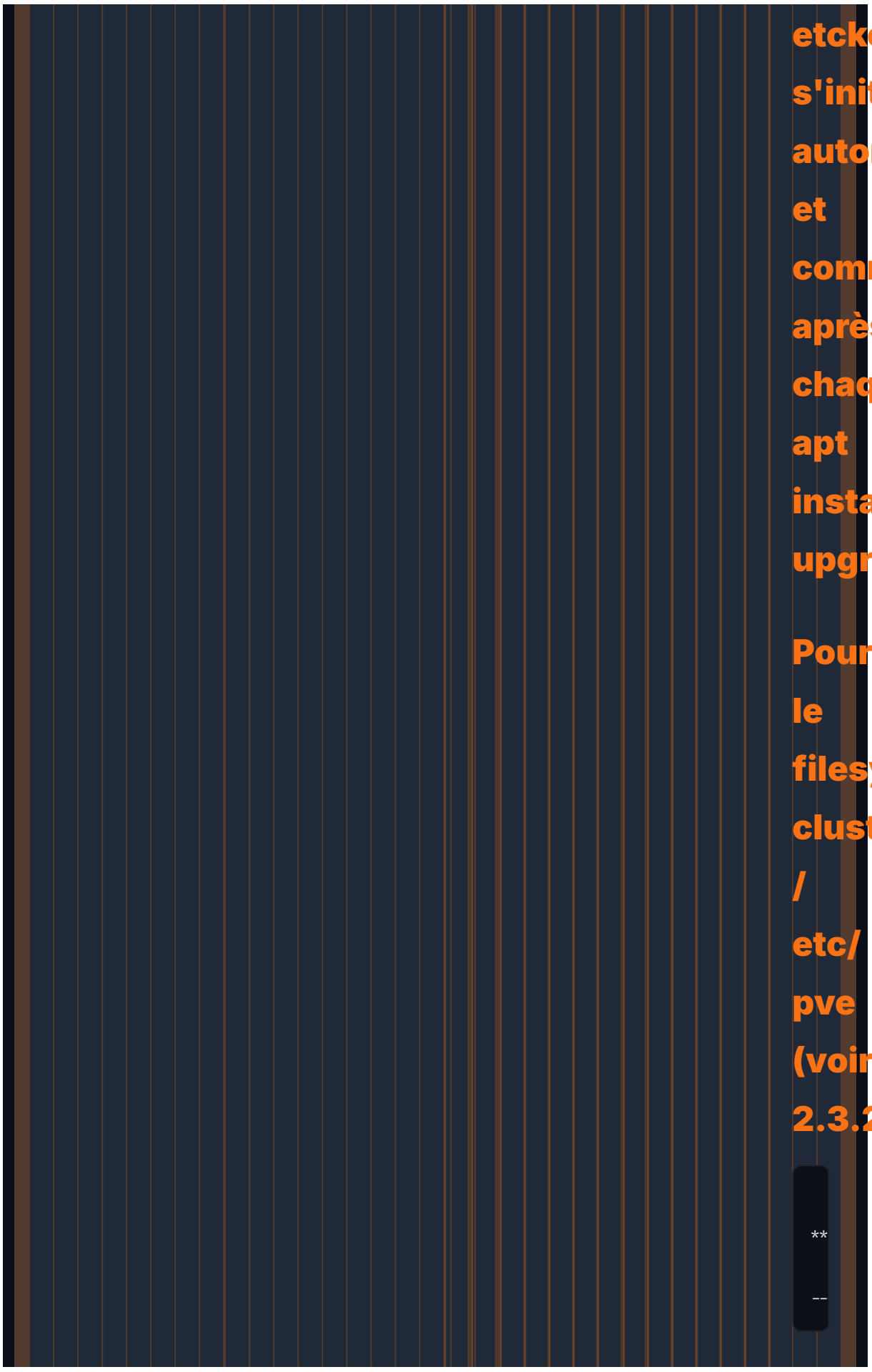
Rationale :

🔍 AUDIT

Audit :

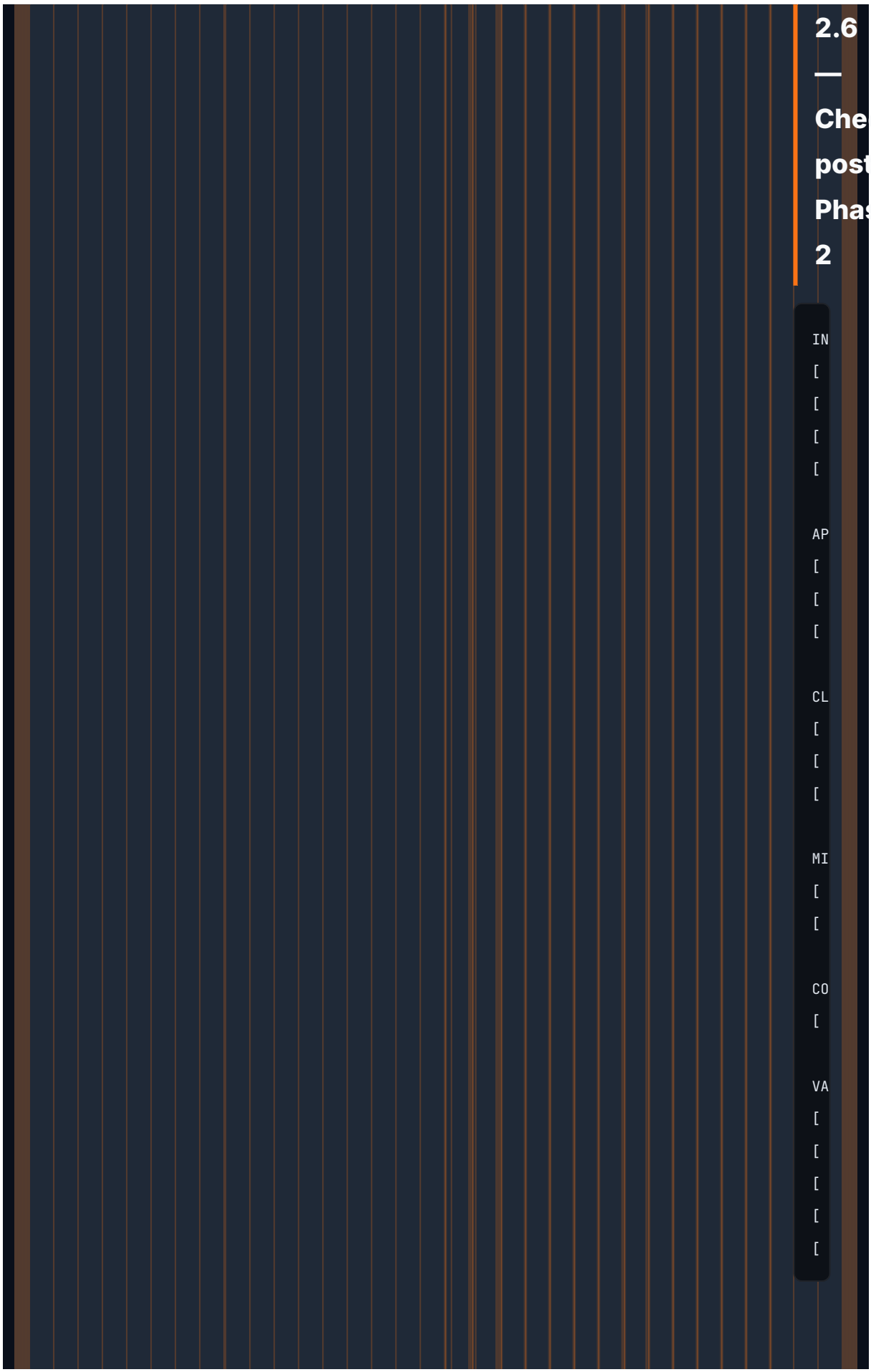
```
dpkg -l etckeeper | grep -q "^ii"
```

```
&& echo "PASS" || echo "FAIL"

cd /etc && git log --oneline -3 2>/dev/null && echo "PASS: historique git" || echo "FAIL: pas d'historique"

**

apt install -y etckeeper
```



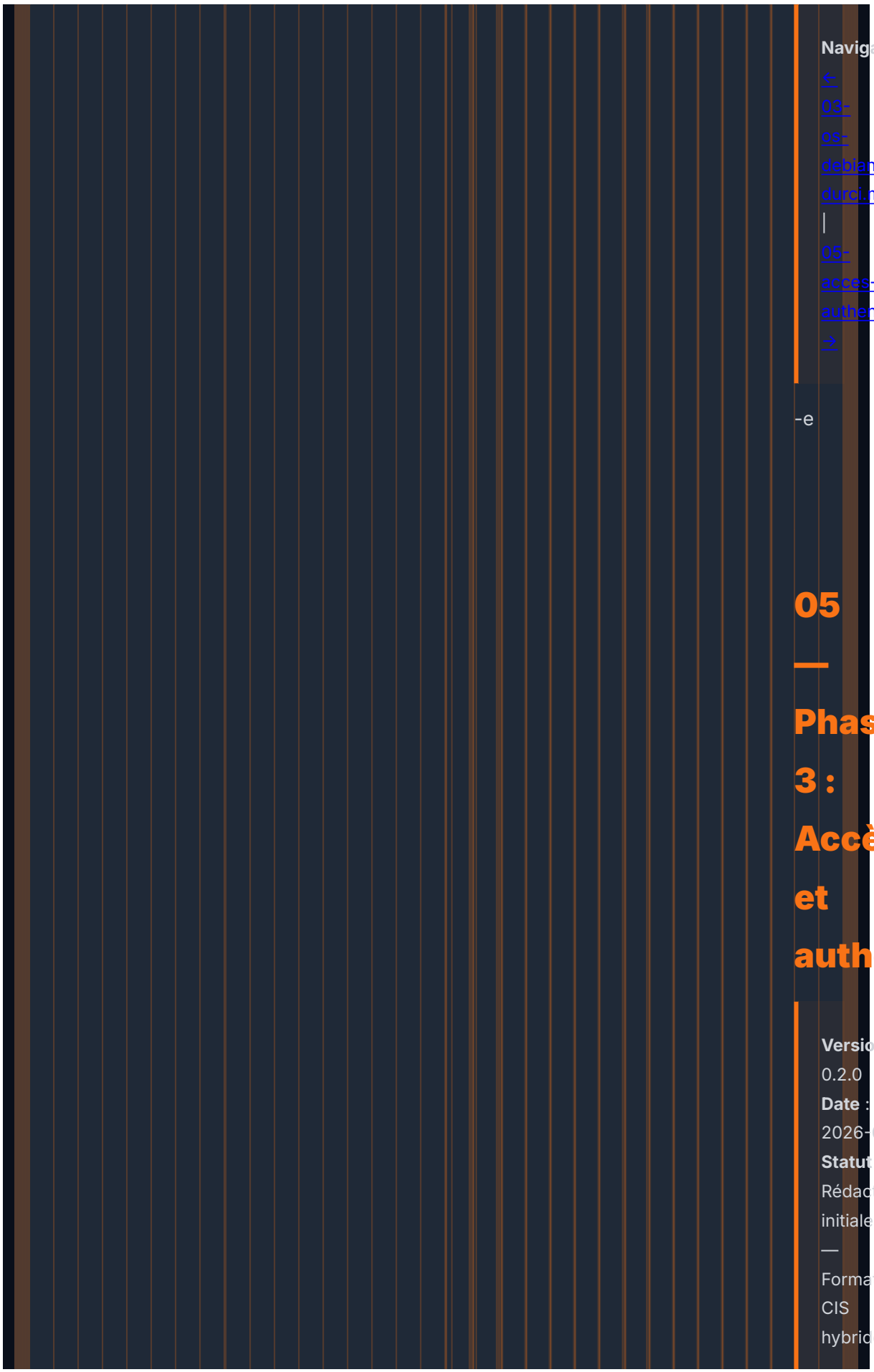
etckeeper s'initialise automatiquement et commite après chaque apt install/upgrade

Pour le filesystem cluster /etc/pve (voir 2.3.2)



2.6 — Checklist post-Phase 2

```
IN
[
[
[
[

AP
[
[
[

CL
[
[
[

MI
[
[

CO
[

VA
[
[
[
[
[
```

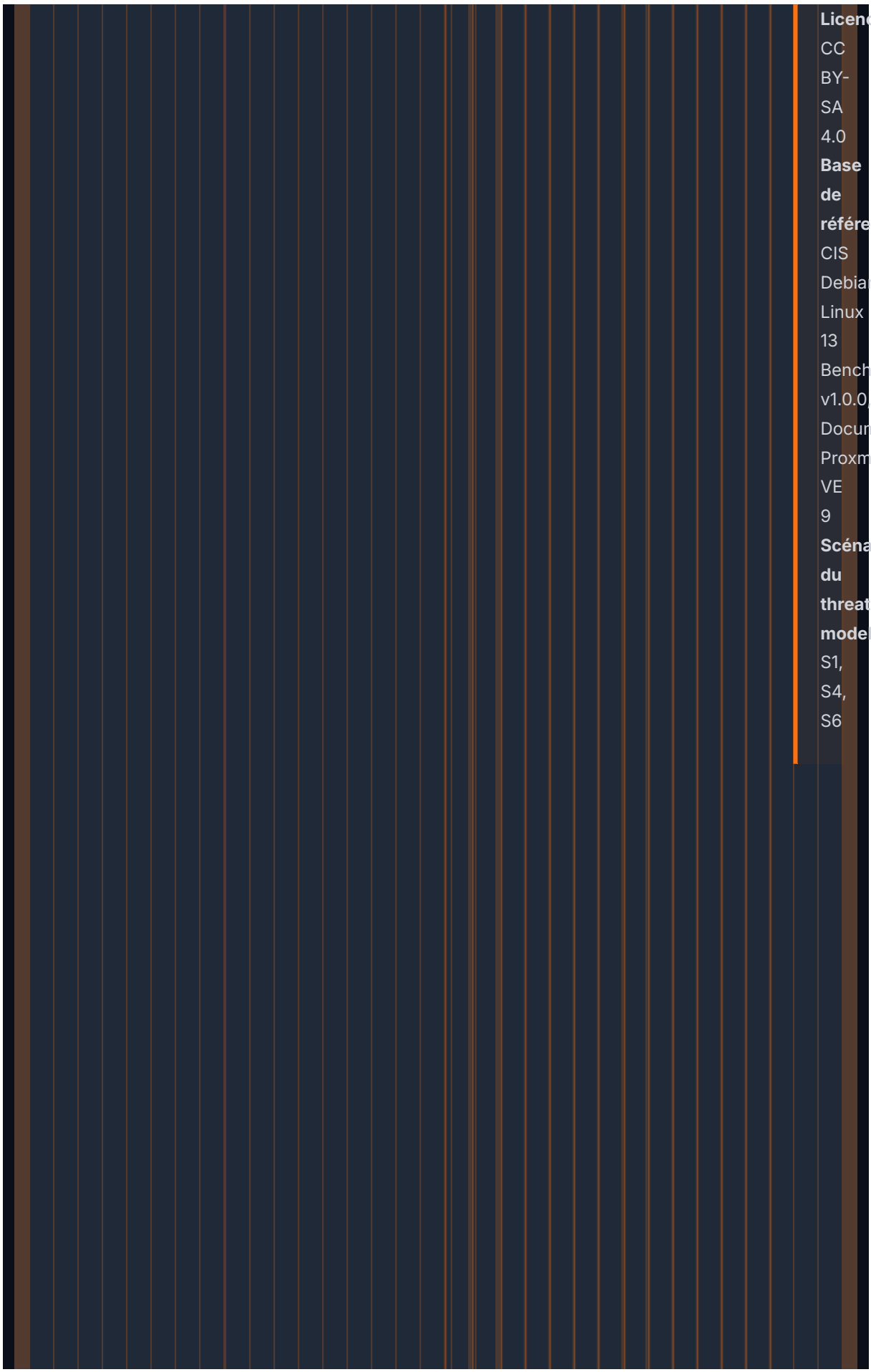


Navigation : ← 03-os-debian-durci.md | 05-acces-authentification.md →

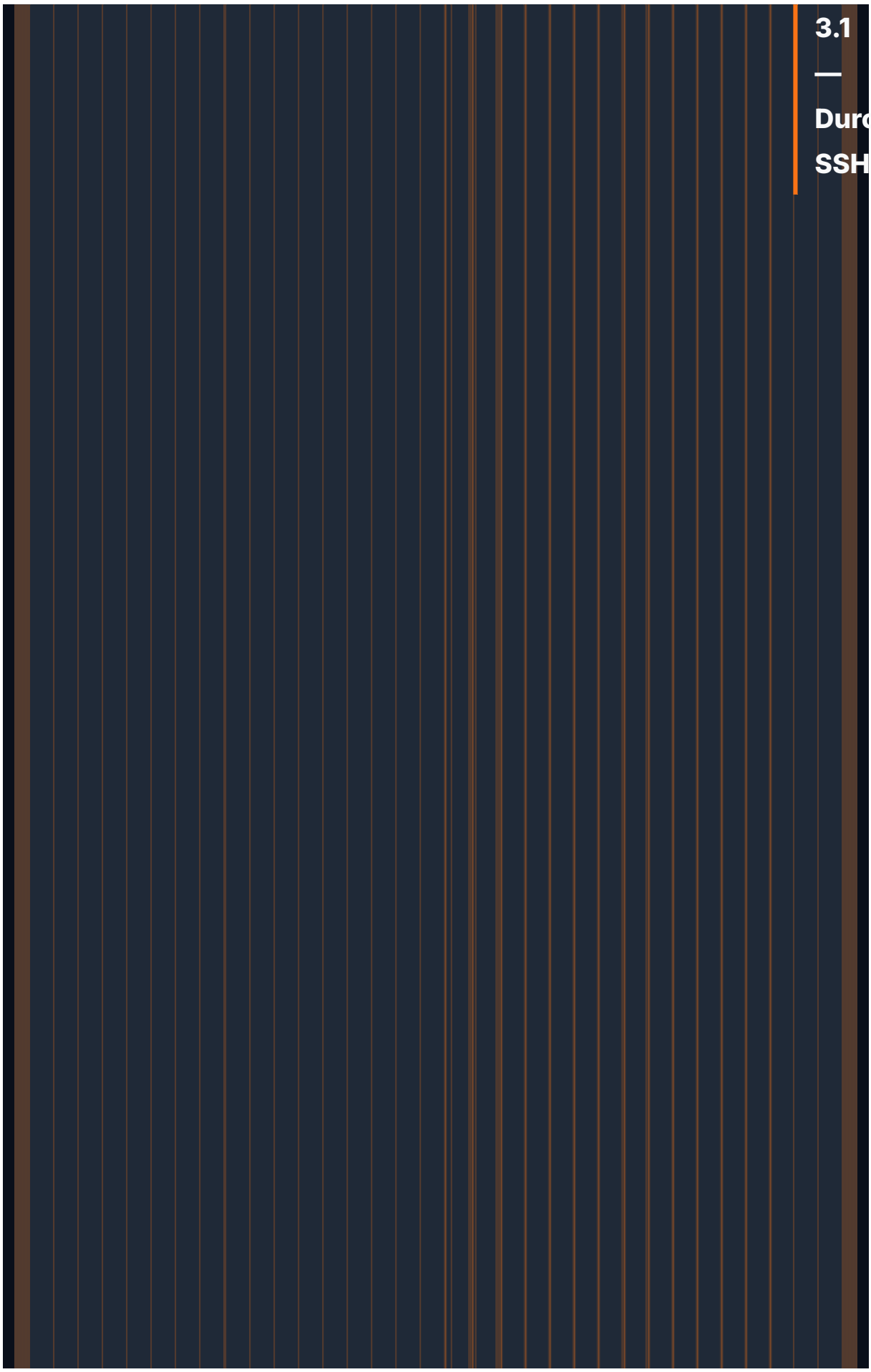
-e

05 — Phase 3 : Accès et authentifica

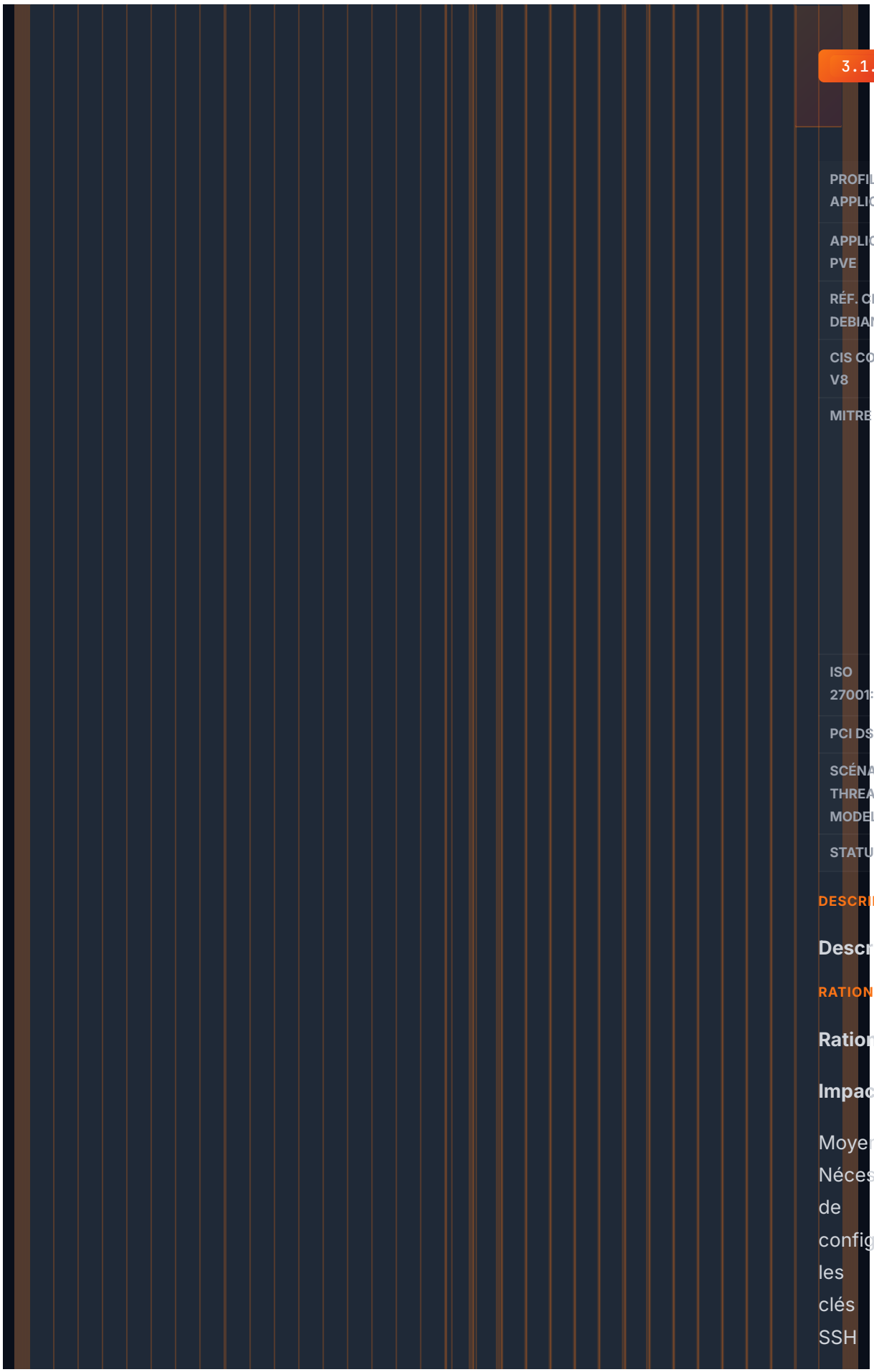
Version : 0.2.0
Date : 2026-03-20
Statut : Rédaction initiale — Format CIS hybride



Licence : CC BY-SA 4.0
Base de référence : CIS Debian Linux 13 Benchmark v1.0.0, Documentation Proxmox VE 9
Scénarios du threat model : S1, S4, S6



3.1 — Durcissement SSH



3.1.1

Durcir la configuration sshd

PROFILE APPLICABILITY	Level 1 - Server
APPLICABILITÉ PVE	🏠🏢🌐
RÉF. CIS DEBIAN 13	5.1.1 à 5.
CIS CONTROLS V8	4.1, 5.2,
MITRE ATT&CK	T1021.0 (SSH), T (Brute F T1078 (Accoun M1032 factor Authent M1035 Access)
ISO 27001:2022	A.5.17, A A.8.20
PCI DSS V4.0	2.2.1, 8.
SCÉNARIO THREAT MODEL	S1
STATUT PVE 9	✅ Valid

DESCRIPTION :

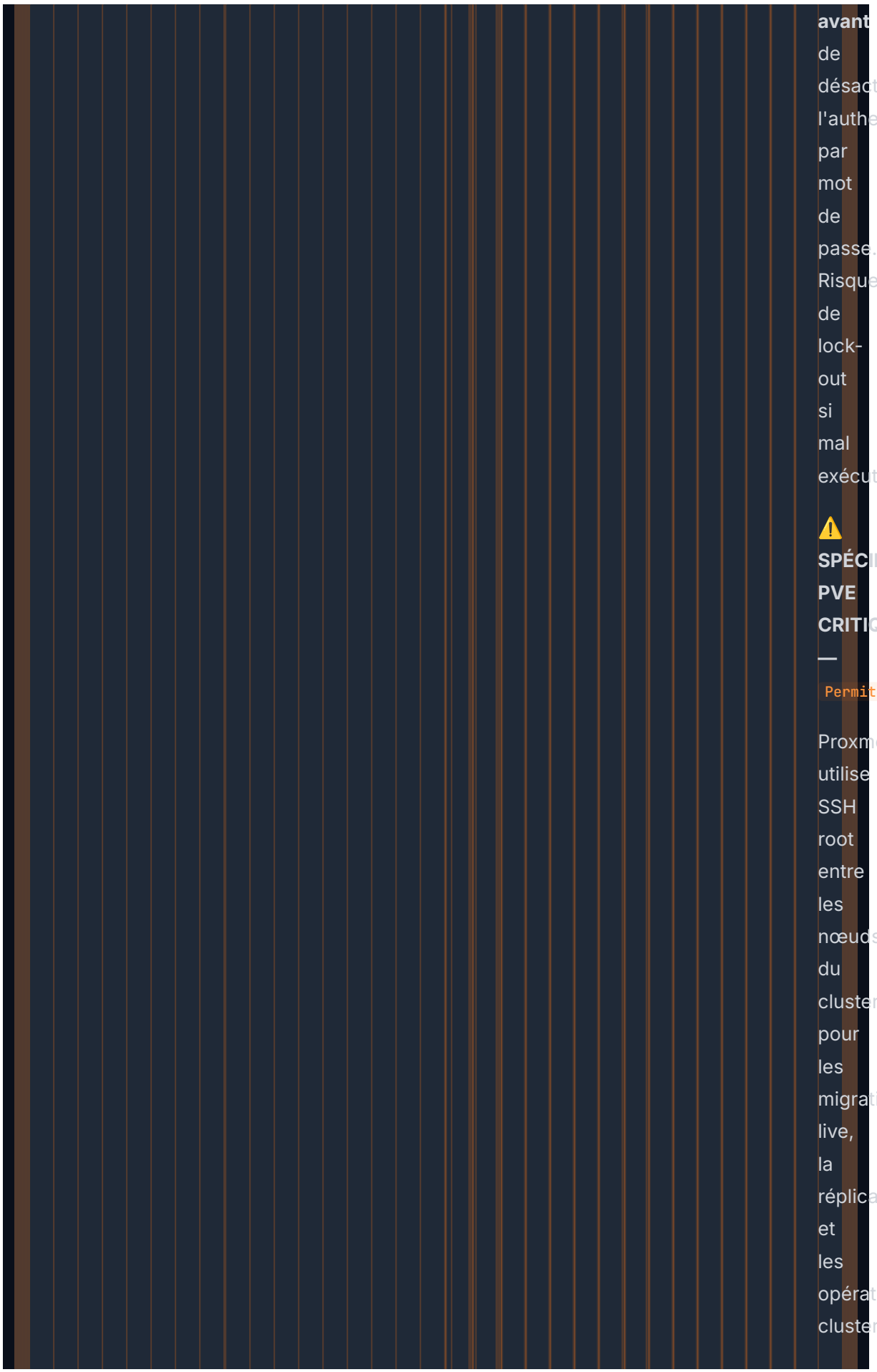
Description :

RATIONALE :

Rationale :

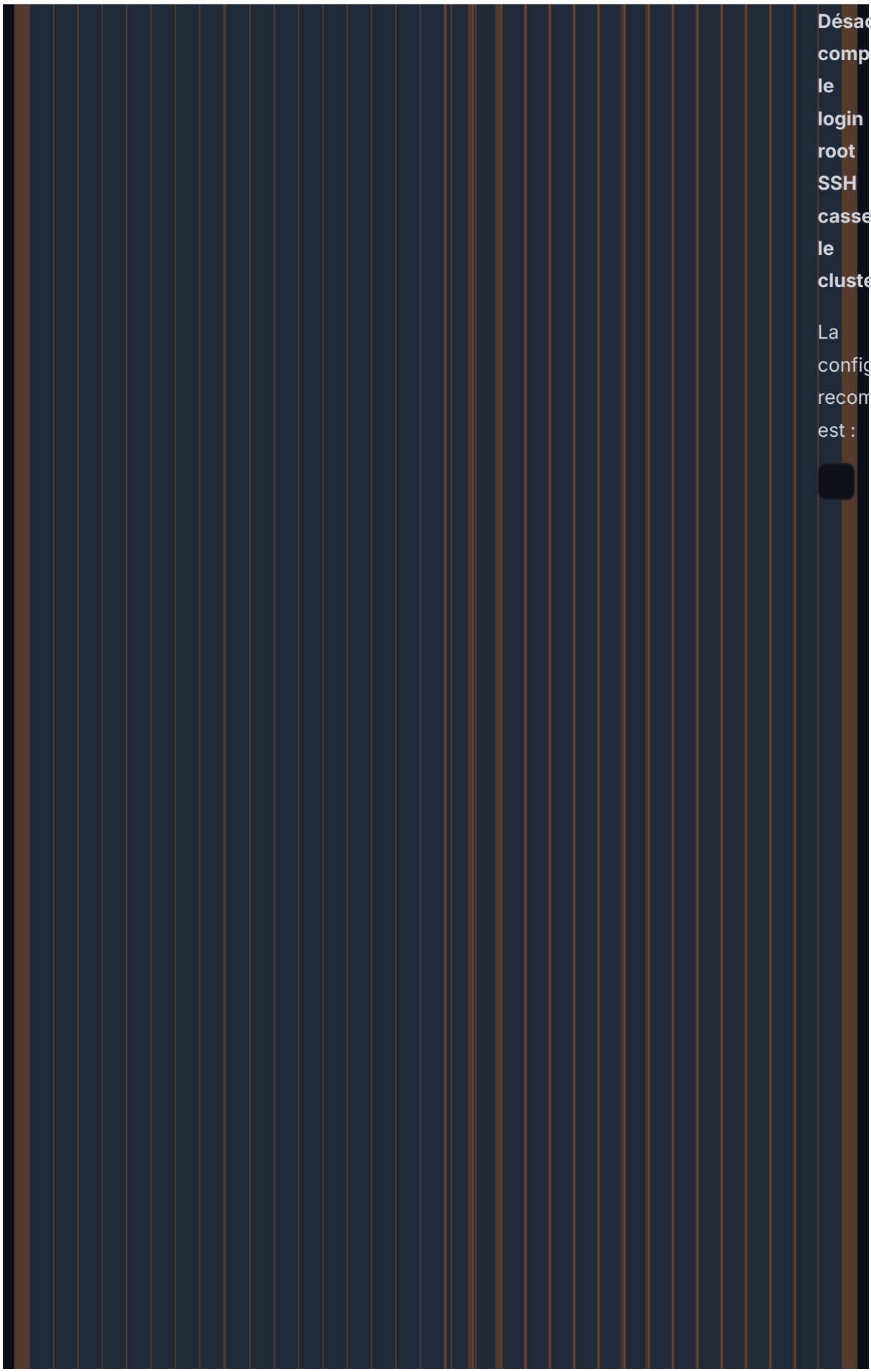
Impact :

Moyen. Nécessite de configurer les clés SSH



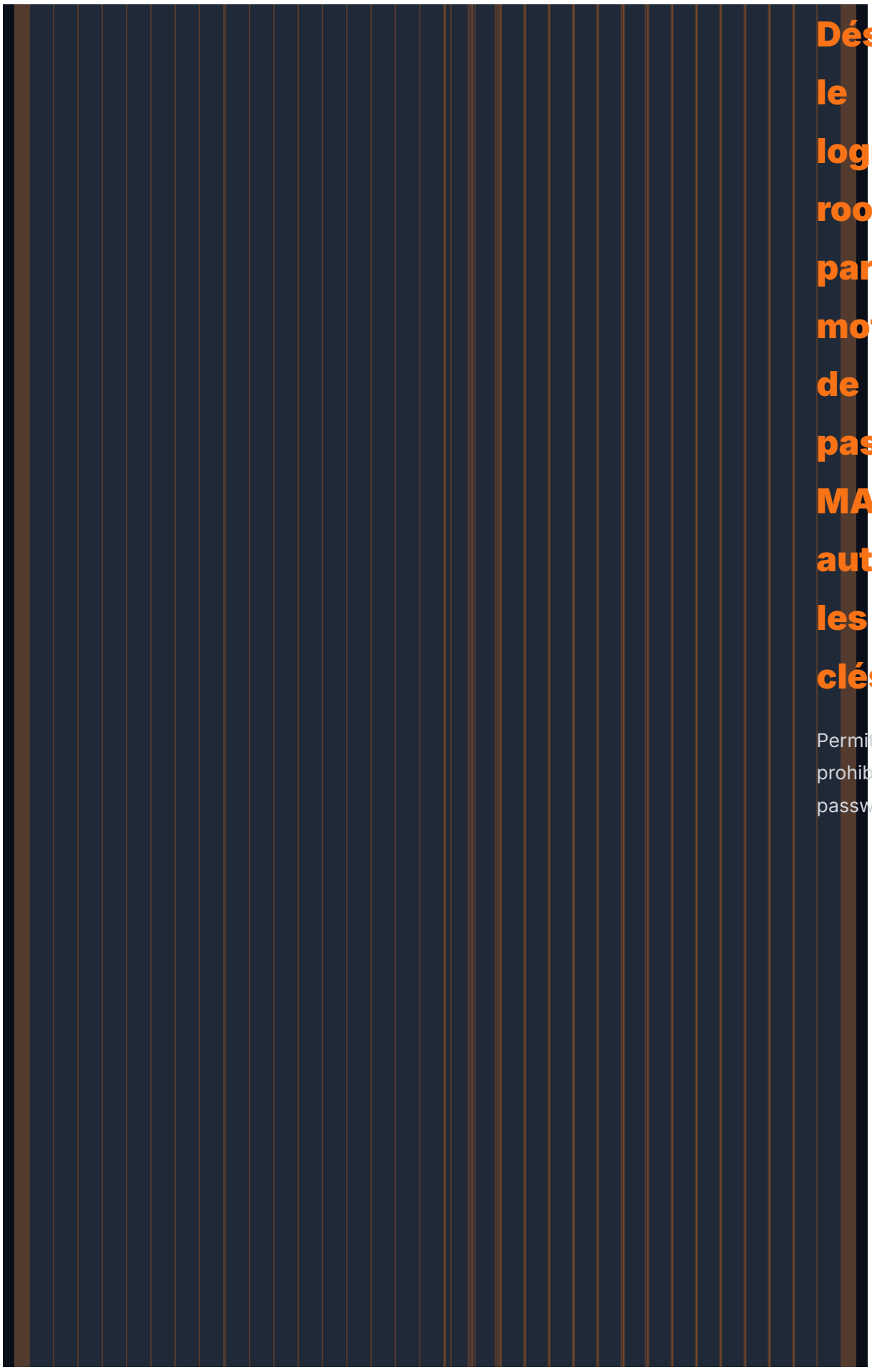
avant de désactiver l'authentification par mot de passe. Risque de lock-out si mal exécuté.

⚠️ **SPÉCIFICITÉ PVE CRITIQUE** — `PermitRootLogin` : Proxmox utilise SSH root entre les nœuds du cluster pour les migrations live, la réplication, et les opérations cluster.



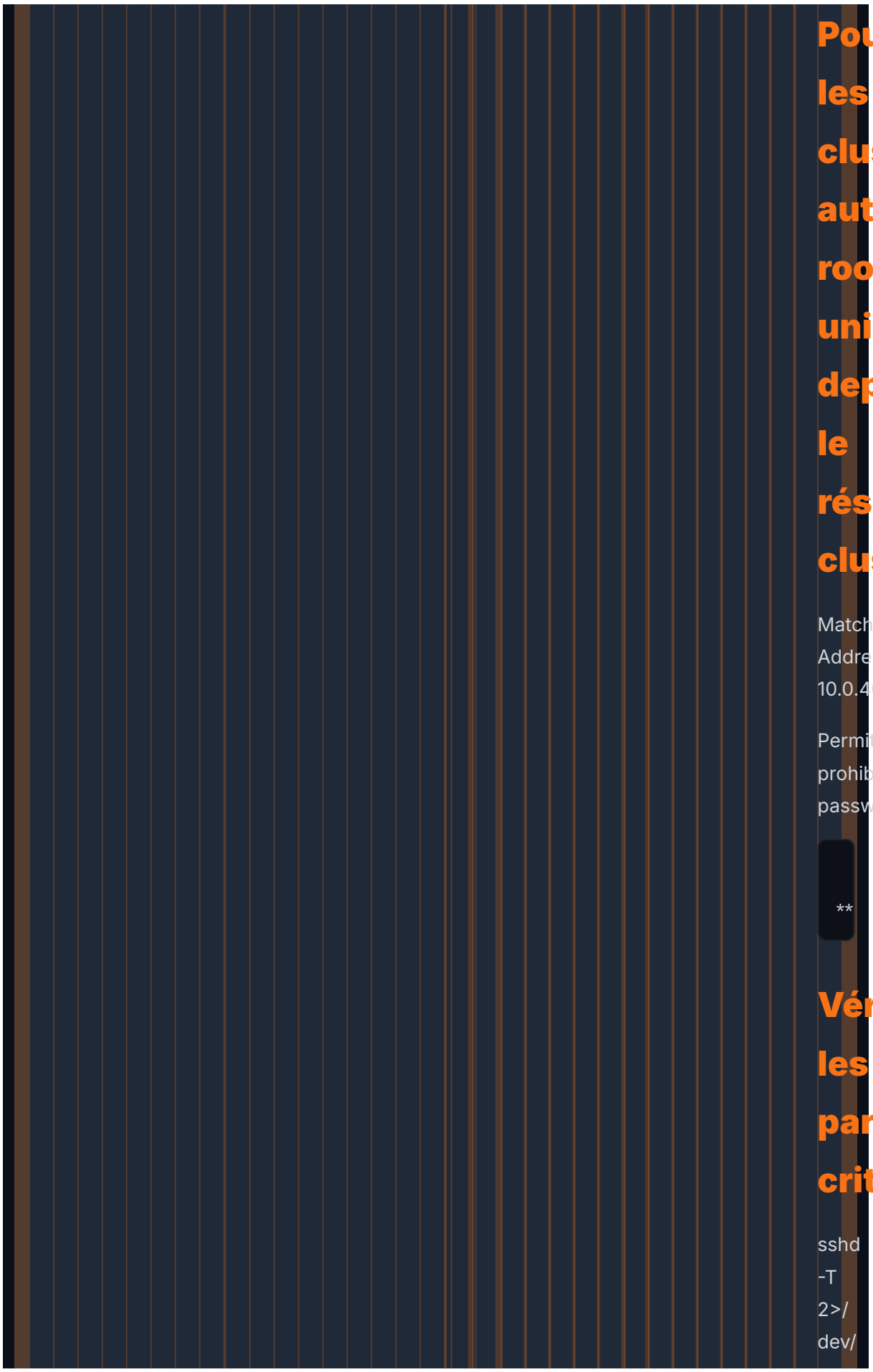
Désactiver complètement le login root SSH casse le cluster.

La configuration recommandée est :



Désactiver le login root par mot de passe MAIS autoriser les clés

PermitRootLogin prohibit-password

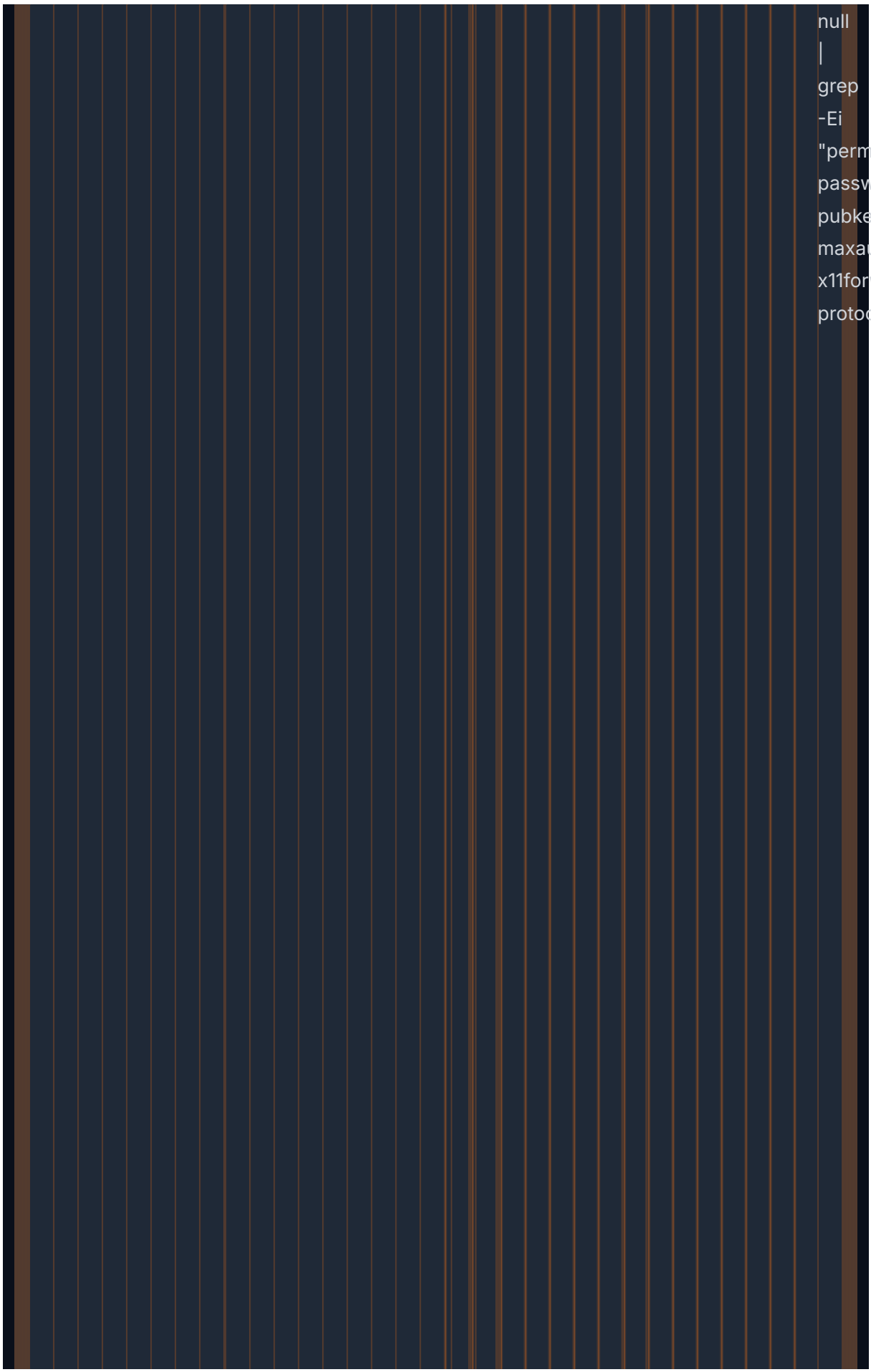


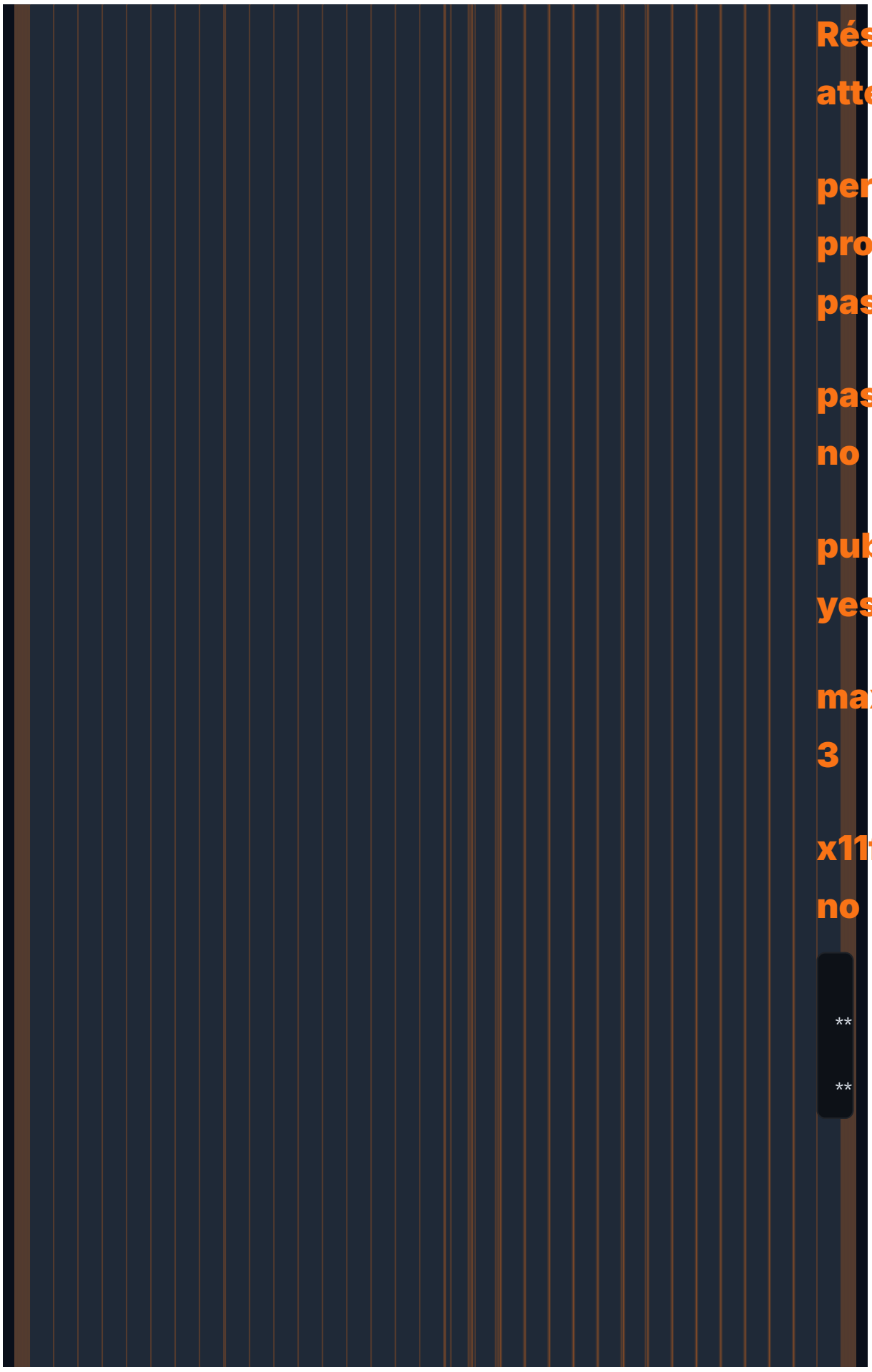
Pour les clusters : autoriser root uniquemer depuis le réseau cluster

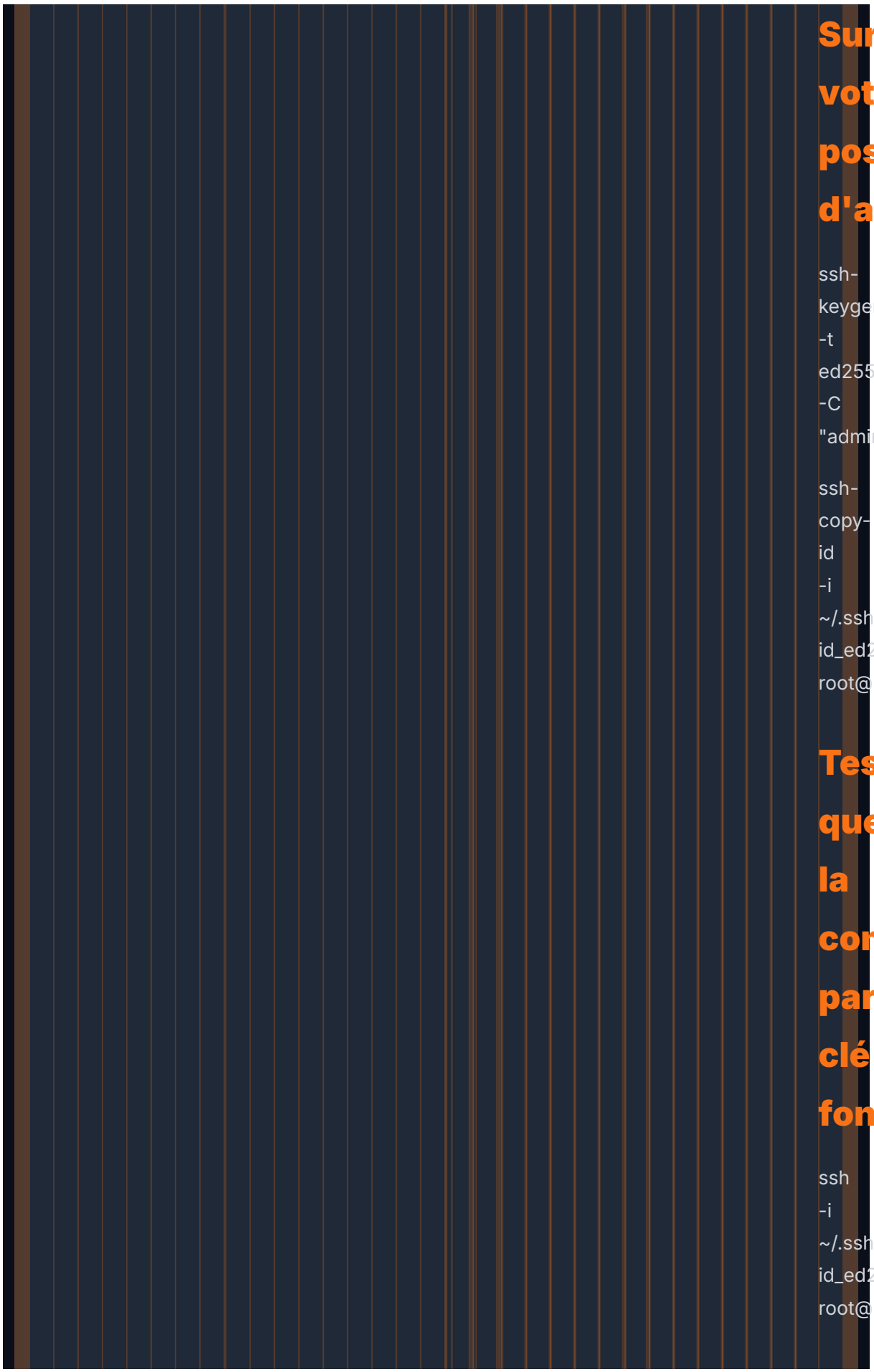
```
Match
Address
10.0.40.0/24

PermitRootLogin
prohibit-
password

**
```

Vérifier les paramètres critiques

```
sshd
-T
2>/
dev/
```


null
|
grep
-Ei
"permitrootlogin|
passwordauthenticat
pubkeyauthentication
maxauthtries|
x11forwarding|
protocol"


Résultat attendu :
permitroot
prohibit-
password
passworda
no
pubkeyaut
yes
maxauthtri
3
x11forward
no
**
**



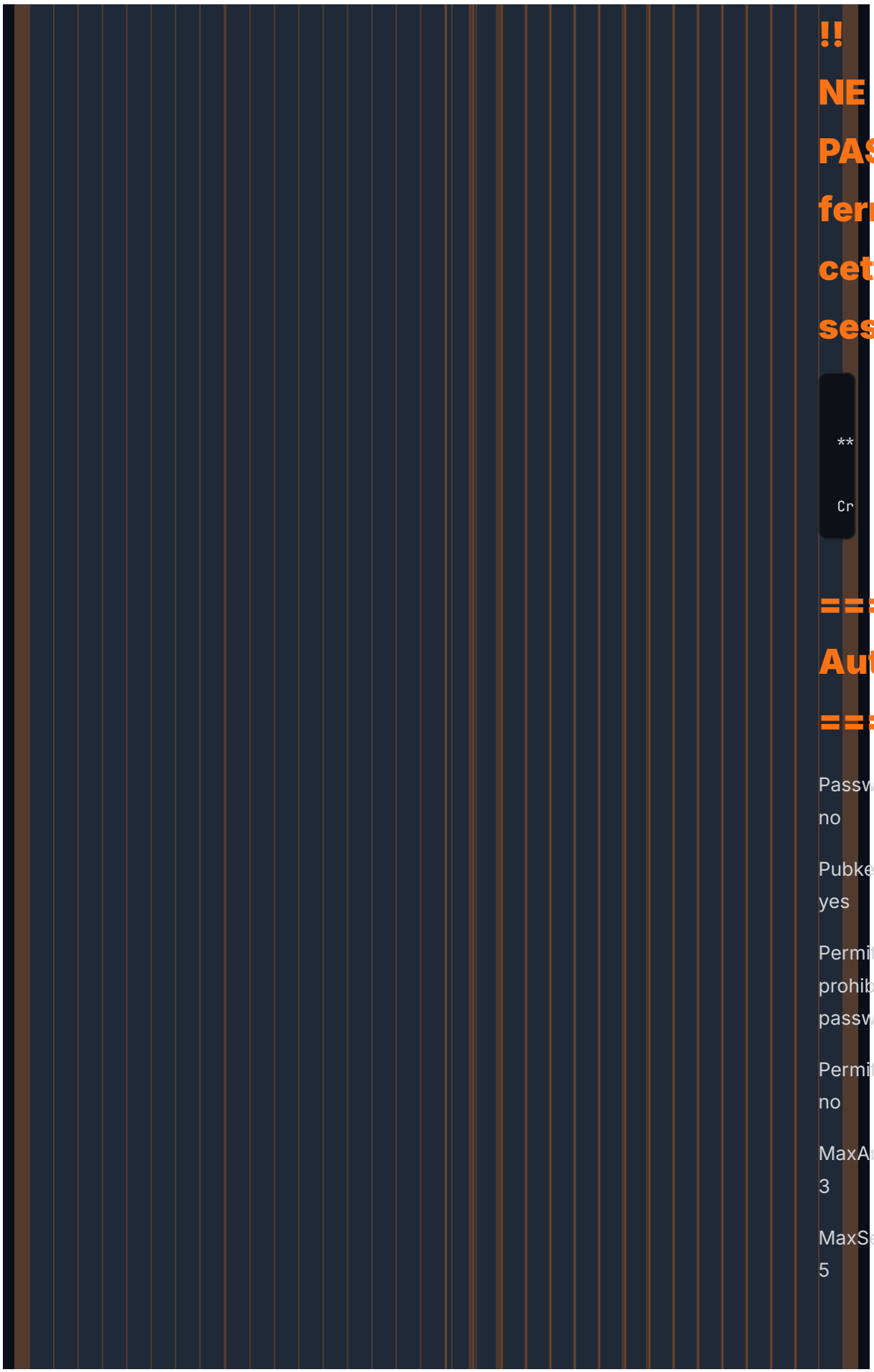
Sur votre poste d'administ

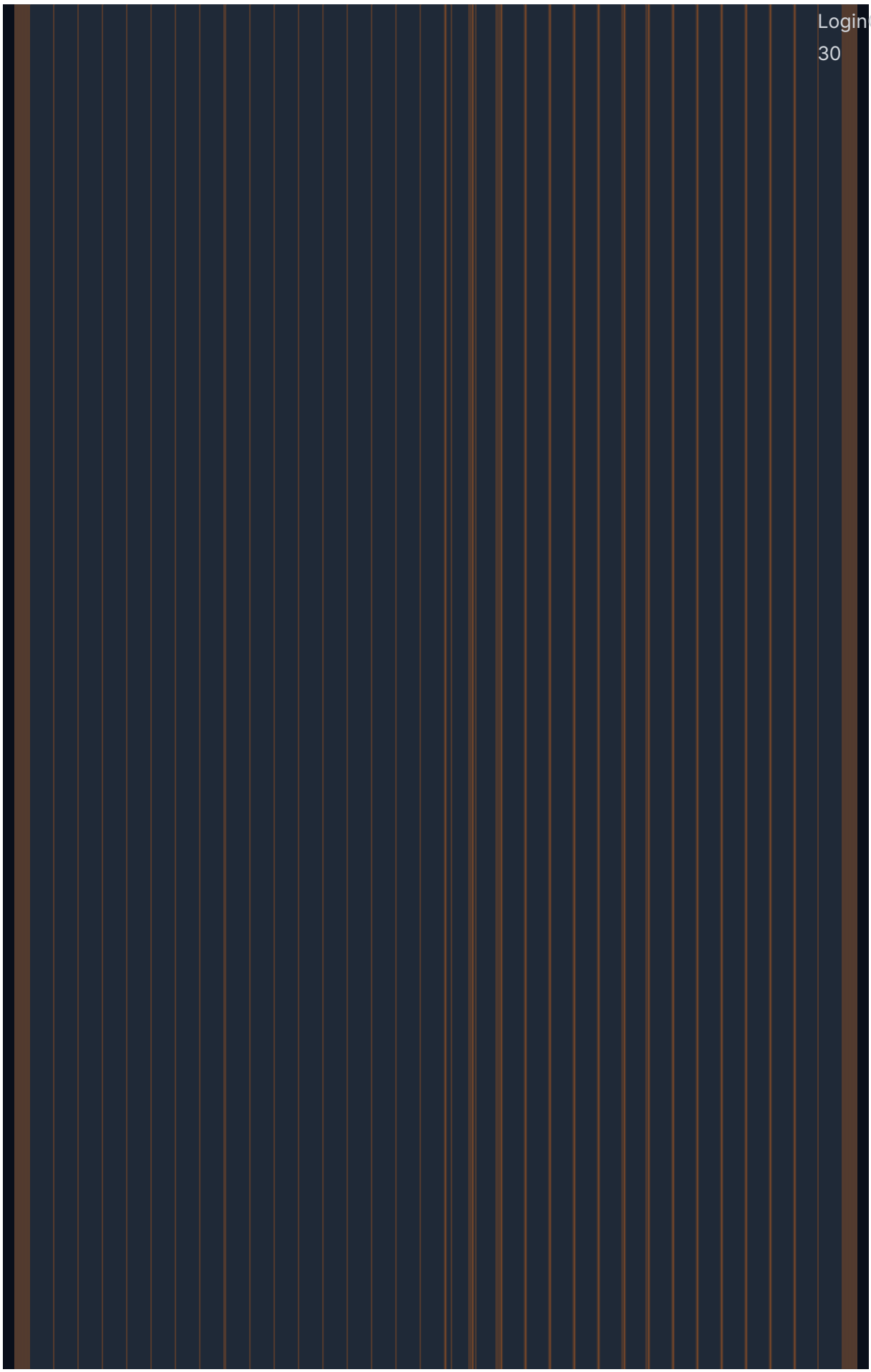
```
ssh-keygen -t ed25519 -C "admin@pve"
```

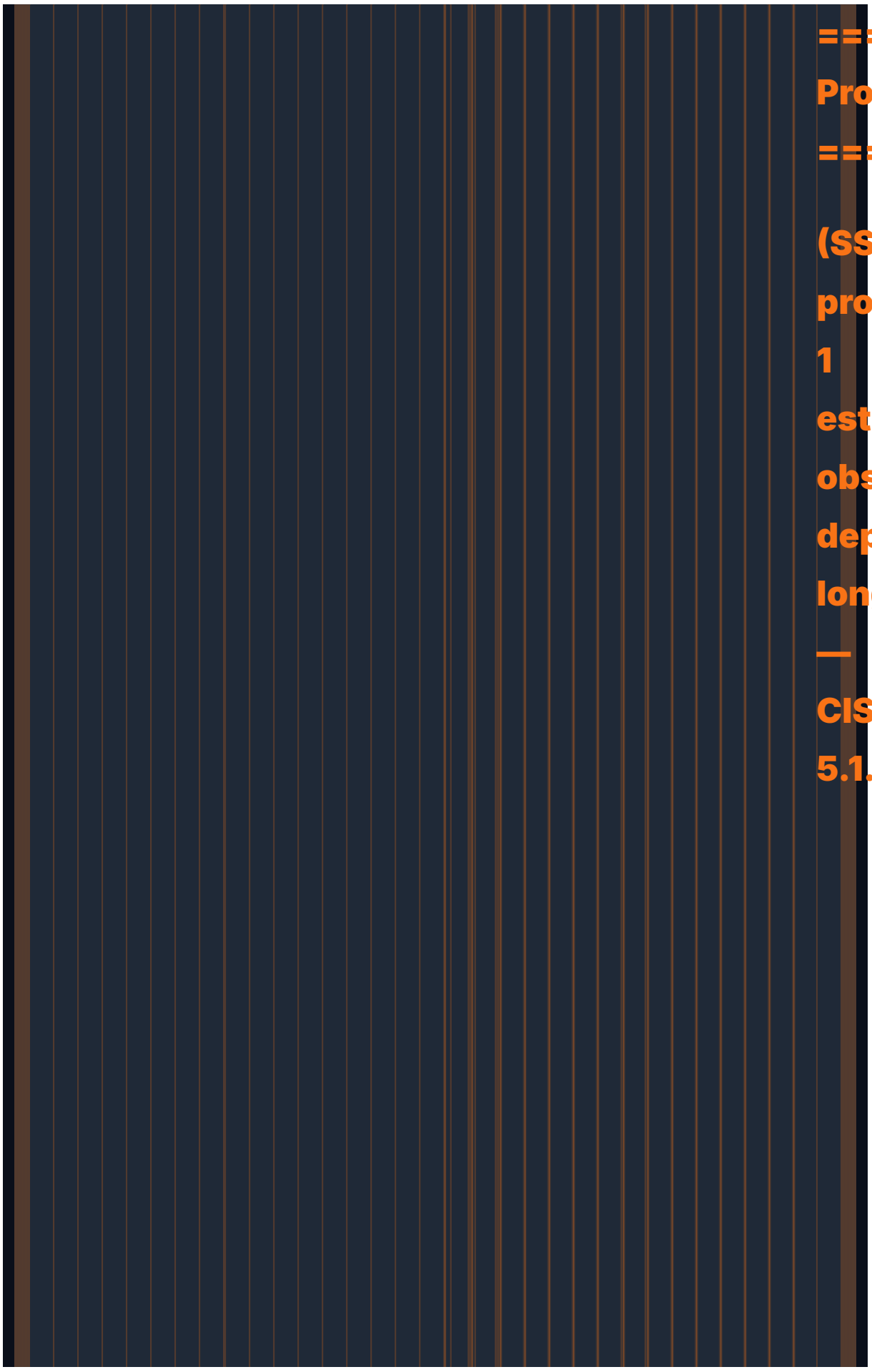
```
ssh-copy-id -i ~/.ssh/id_ed25519.pub root@<PVE_IP>
```

Tester que la connexion par clé fonctionne

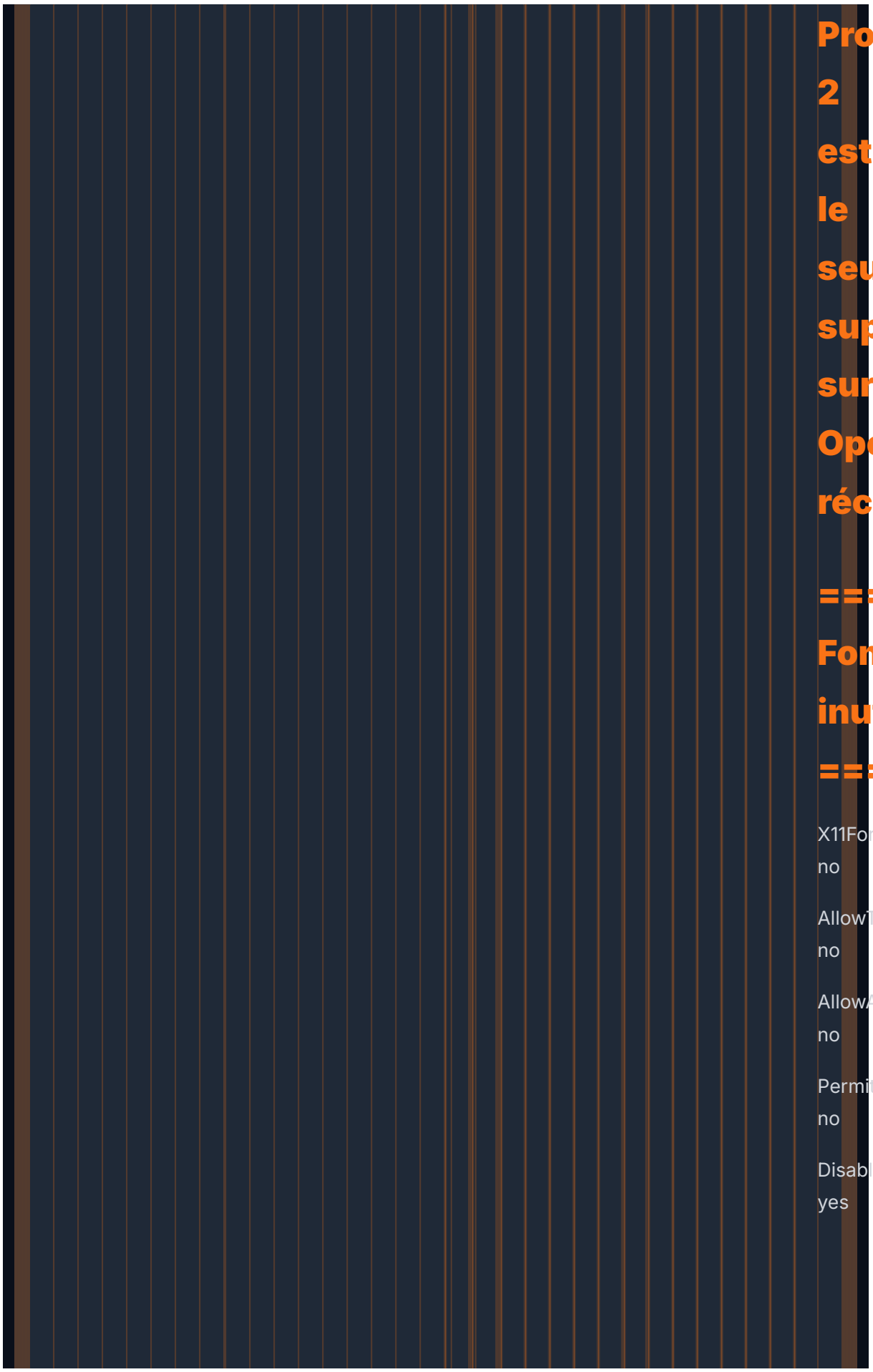
```
ssh -i ~/.ssh/id_ed25519 root@<PVE_IP>
```


!!
NE
PAS
fermer
cette
session !!
**
Cr
===
Authentifi
===
PasswordAuthentica
no
PubkeyAuthenticatio
yes
PermitRootLogin
prohibit-
password
PermitEmptyPasswo
no
MaxAuthTries
3
MaxSessions
5


LoginGraceTime
30



=== Protocole === (SSH protocol 1 est obsolète depuis longtemps — CIS 5.1.1)



Protocol 2 est le seul supporté sur OpenSSH récent

=== Fonctionna inutiles ===

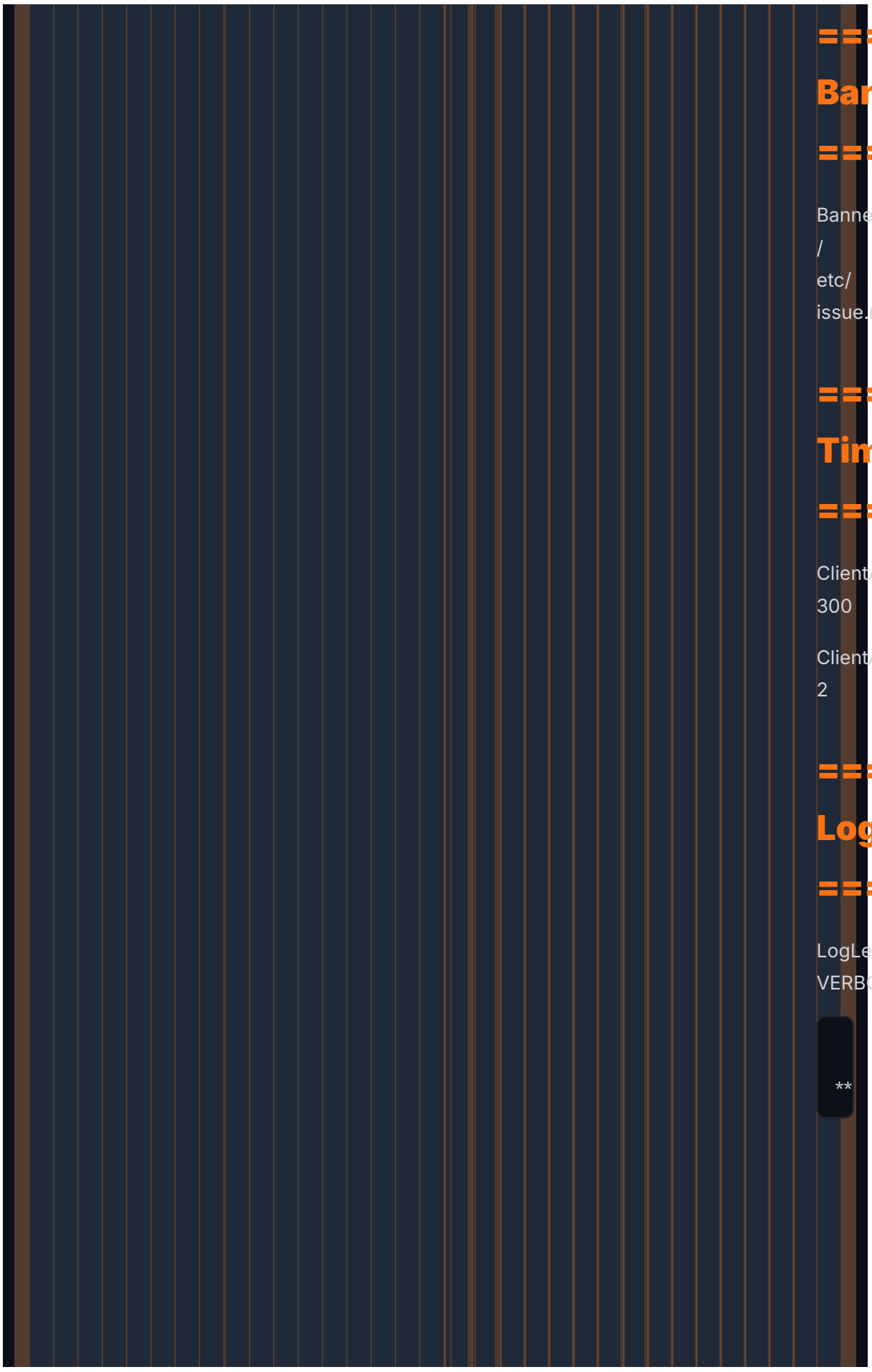
X11Forwarding no

AllowTcpForwarding no

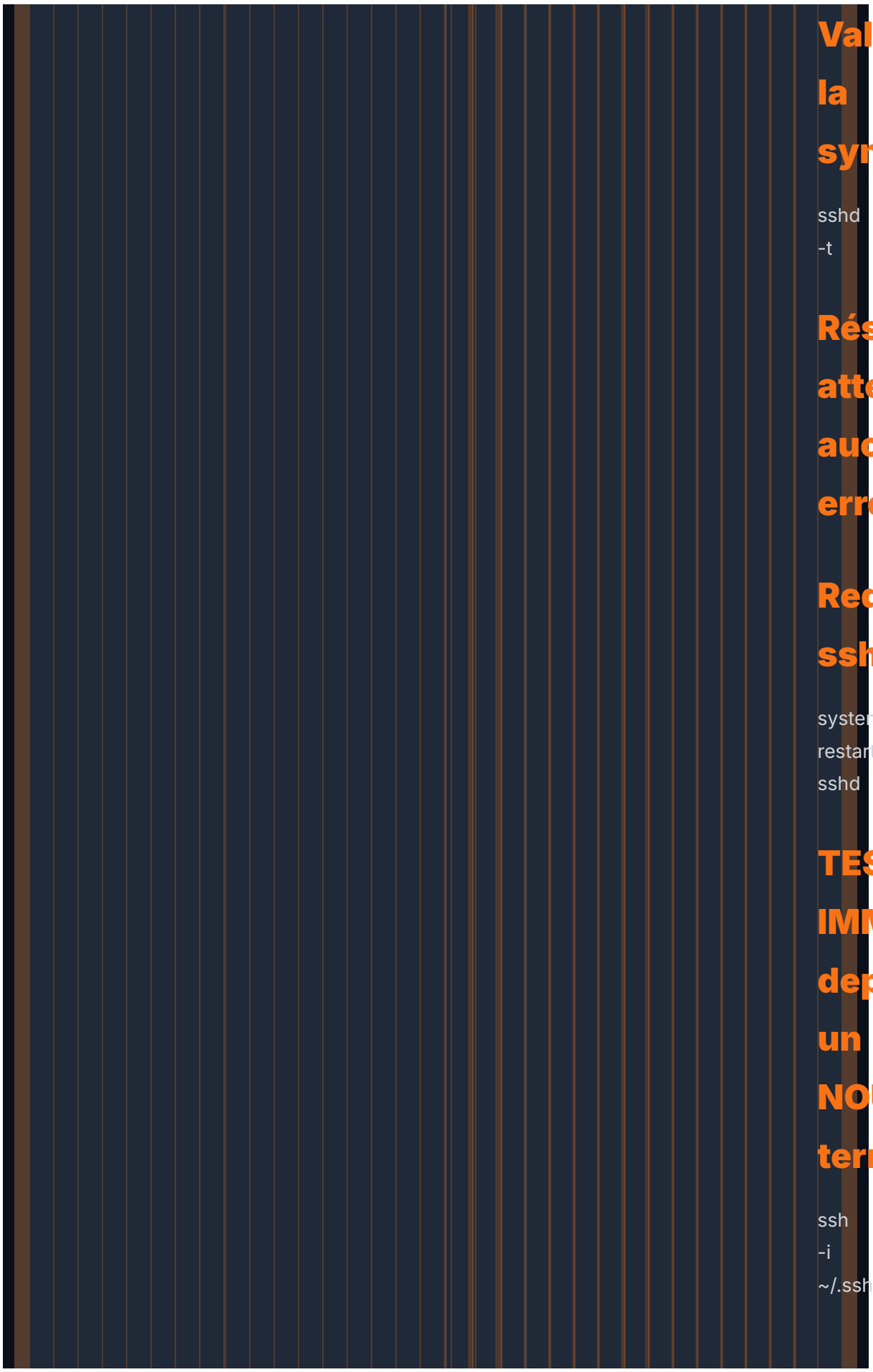
AllowAgentForwardi no

PermitUserEnvironm no

DisableForwarding yes



```
# ===
# Bannière
# ===
Banner /etc/issue.net

# ===
# Timeouts
# ===
ClientAliveInterval 300
ClientAliveCountMax 2

# ===
# Logging
# ===
LogLevel VERBOSE

**
```



Valider la syntaxe

```
sshd
-t
```

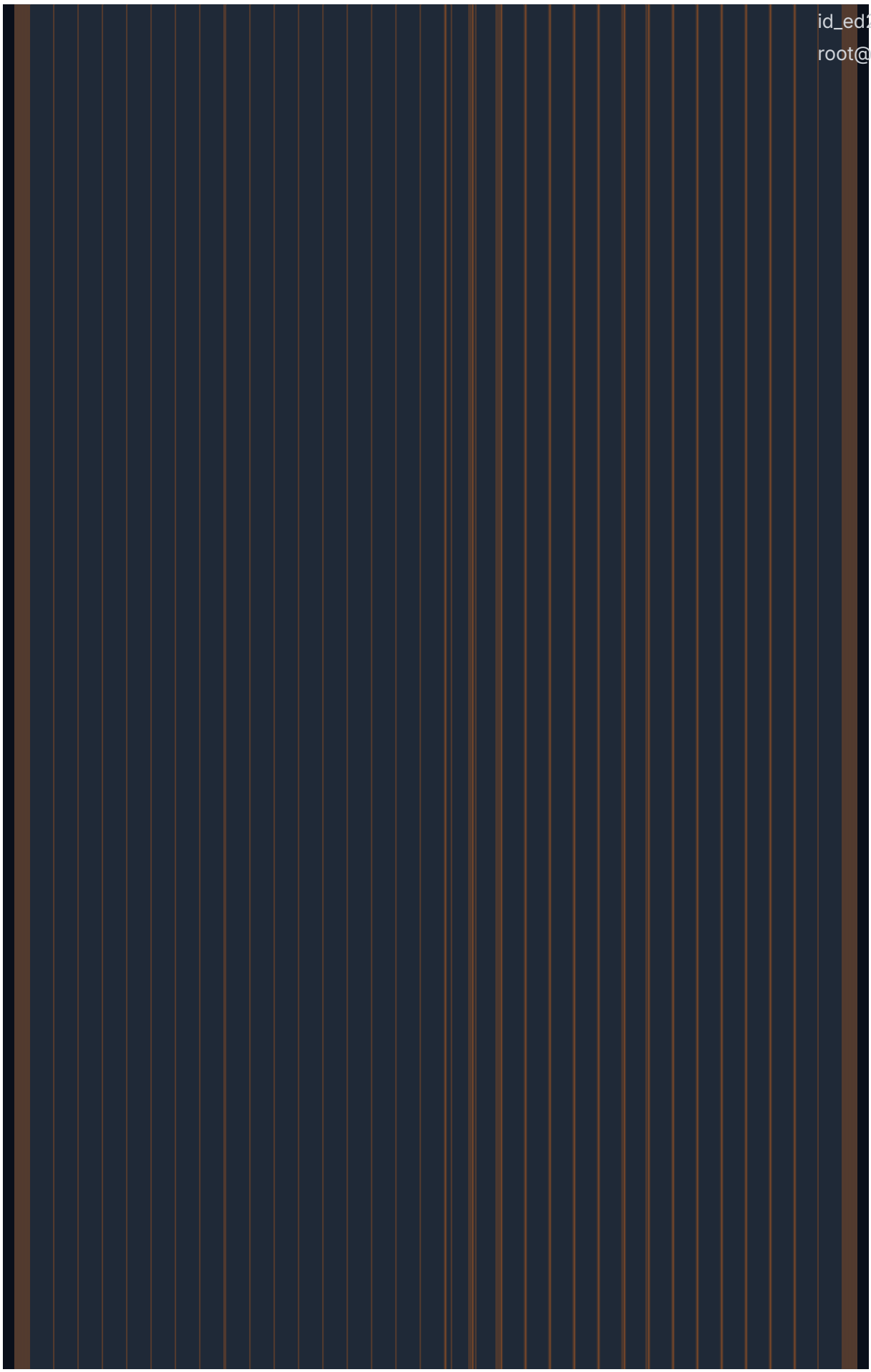
Résultat attendu : aucune erreur

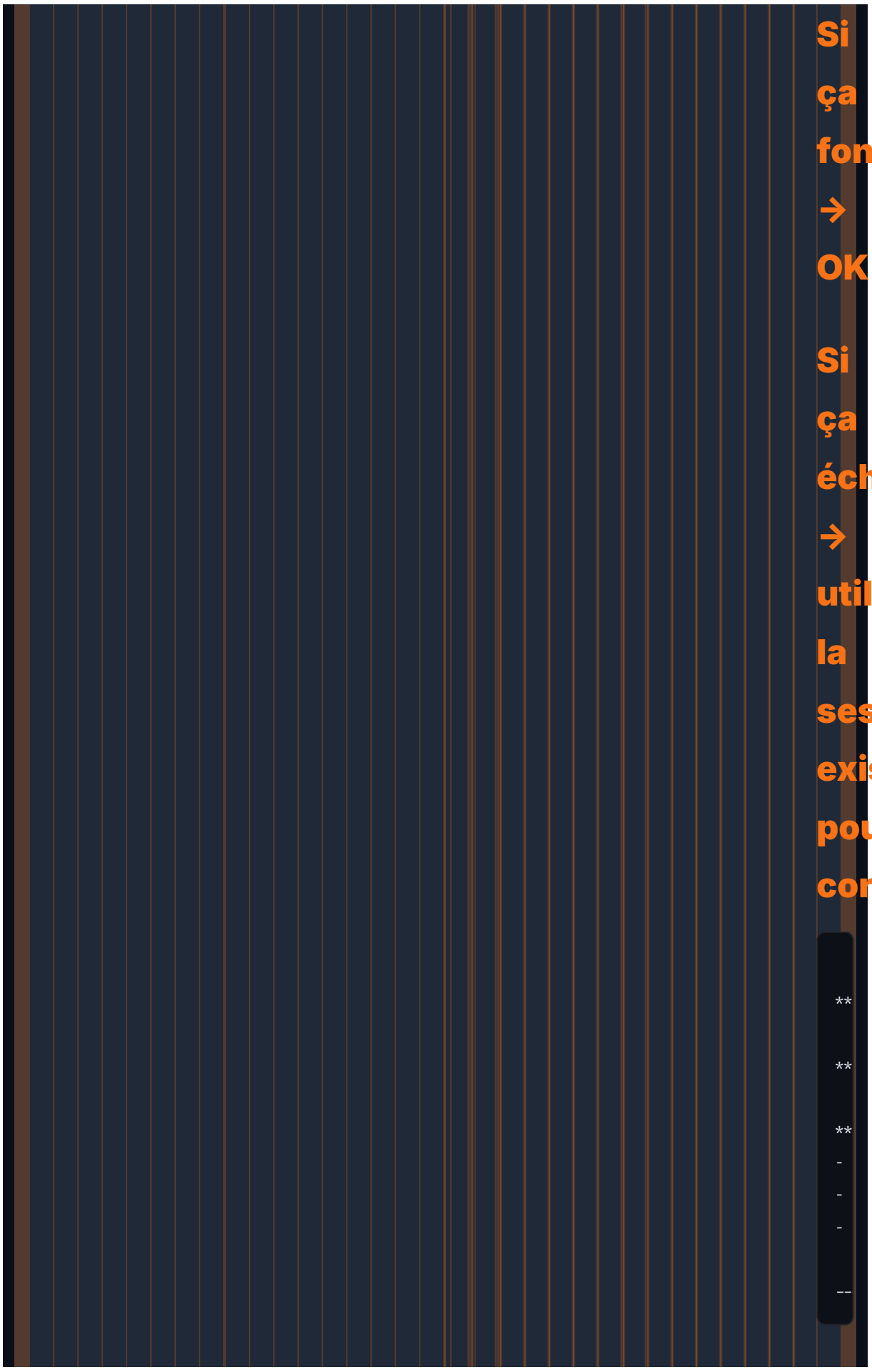
Redémarre sshd

```
systemctl
restart
sshd
```

TESTER IMMÉDIATI depuis un NOUVEAU terminal

```
ssh
-i
~/.ssh/
```

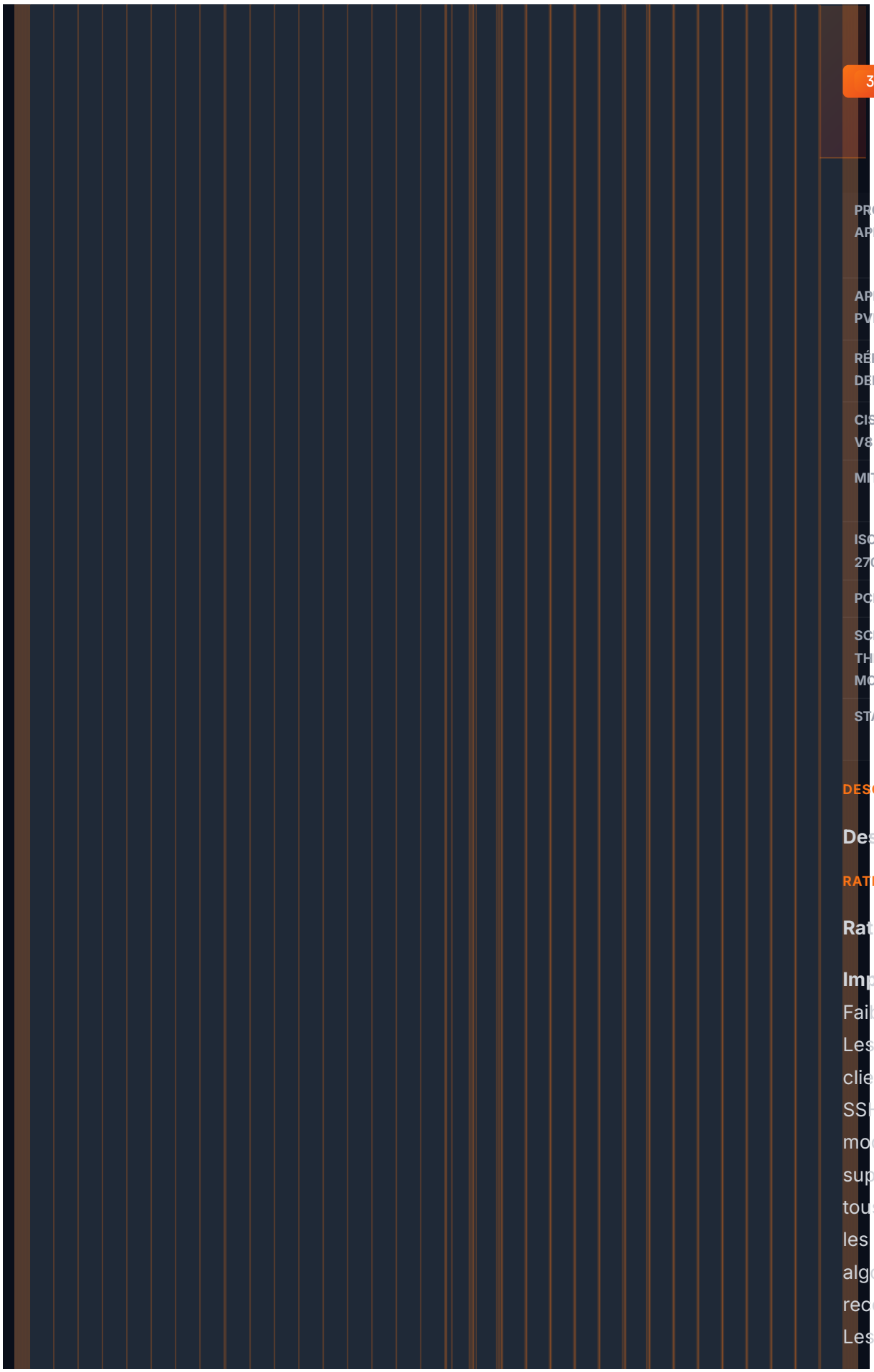

id_ed25519
root@<PVE_IP>



Si ça fonctionne → OK

Si ça échoue → utiliser la session existante pour corriger

```
**
**
**
-
-
-
--
```



3.1.2

PROFILE APPLICABILITY	Leve 1 — Serv
APPLICABILITÉ PVE	🏠🏢 🌐
RÉF. CIS DEBIAN 13	5.1.6 5.1.1
CIS CONTROLS V8	3.10
MITRE ATT&CK	T155 M10
ISO 27001:2022	A.8.
PCI DSS V4.0	4.2.1
SCÉNARIO THREAT MODEL	S1, S
STATUT PVE 9	✅ Valid

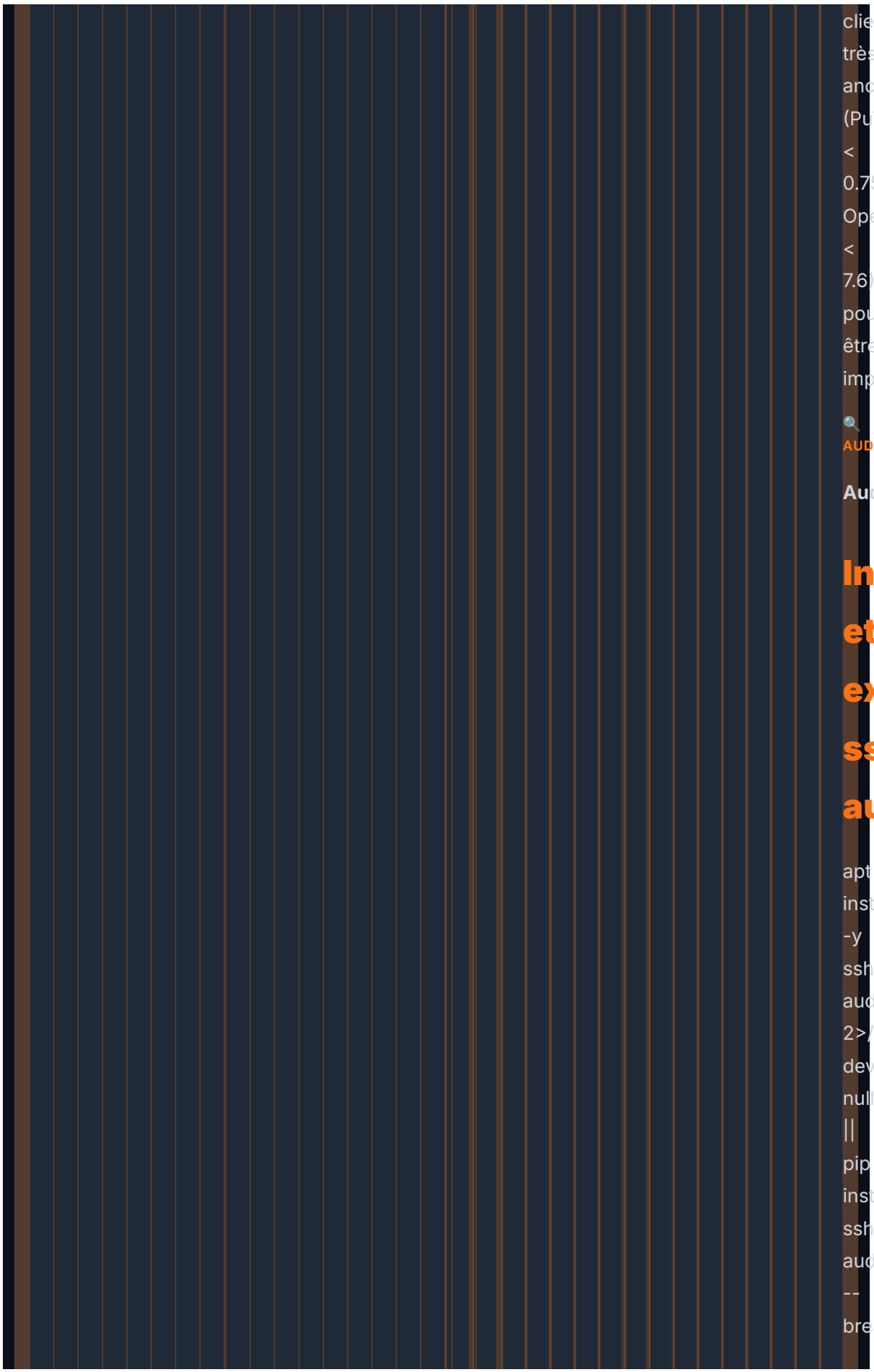
DESCRIPTION :

Description :

RATIONALE :

Rationale :

Impact :
Faible. Les clients SSH modernes supportent tous les algorithmes recommandés. Les



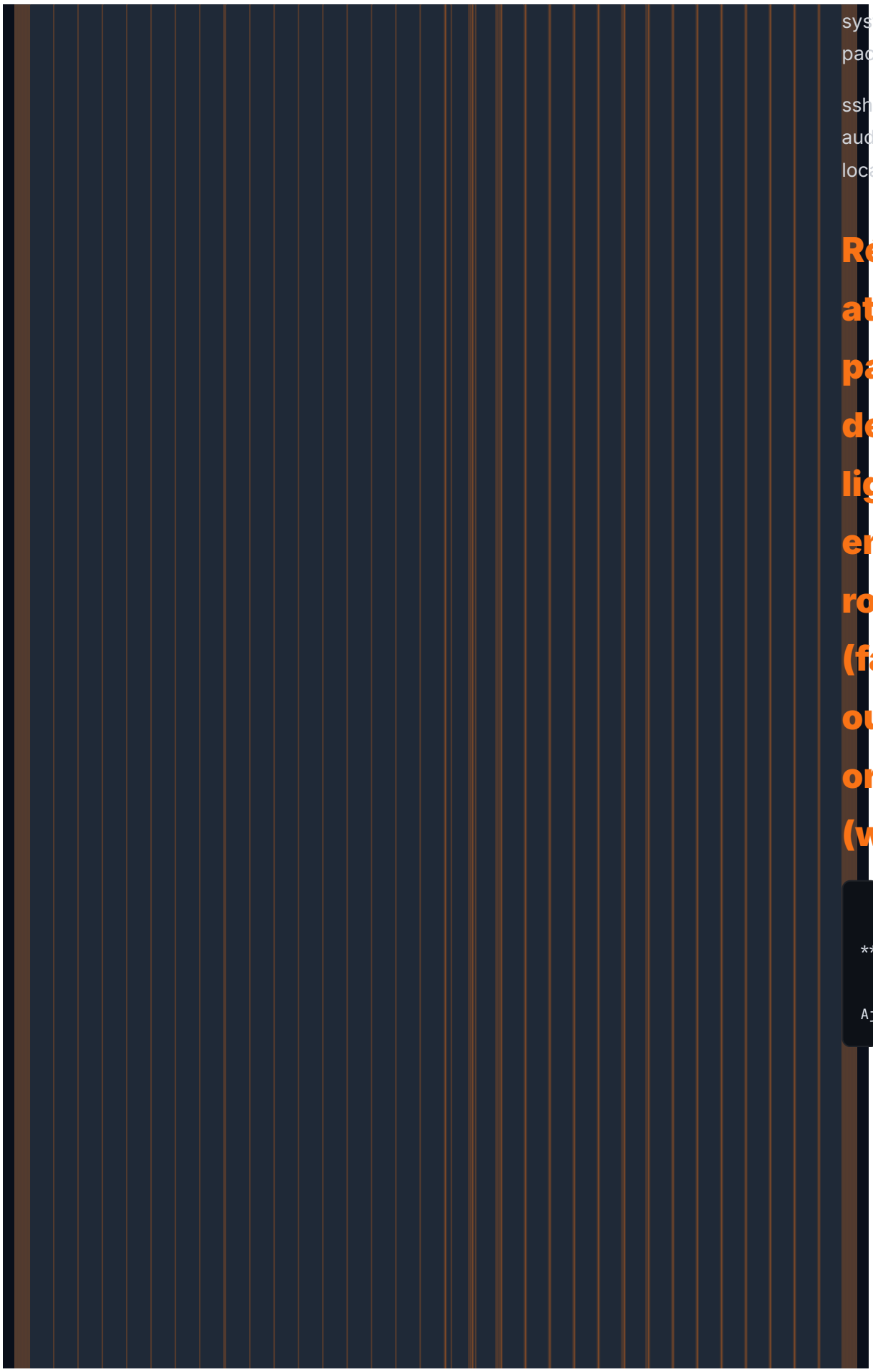
clients très anciens (PuTTY < 0.75, OpenSSH < 7.6) pourraient être impactés.

🔍 AUDIT

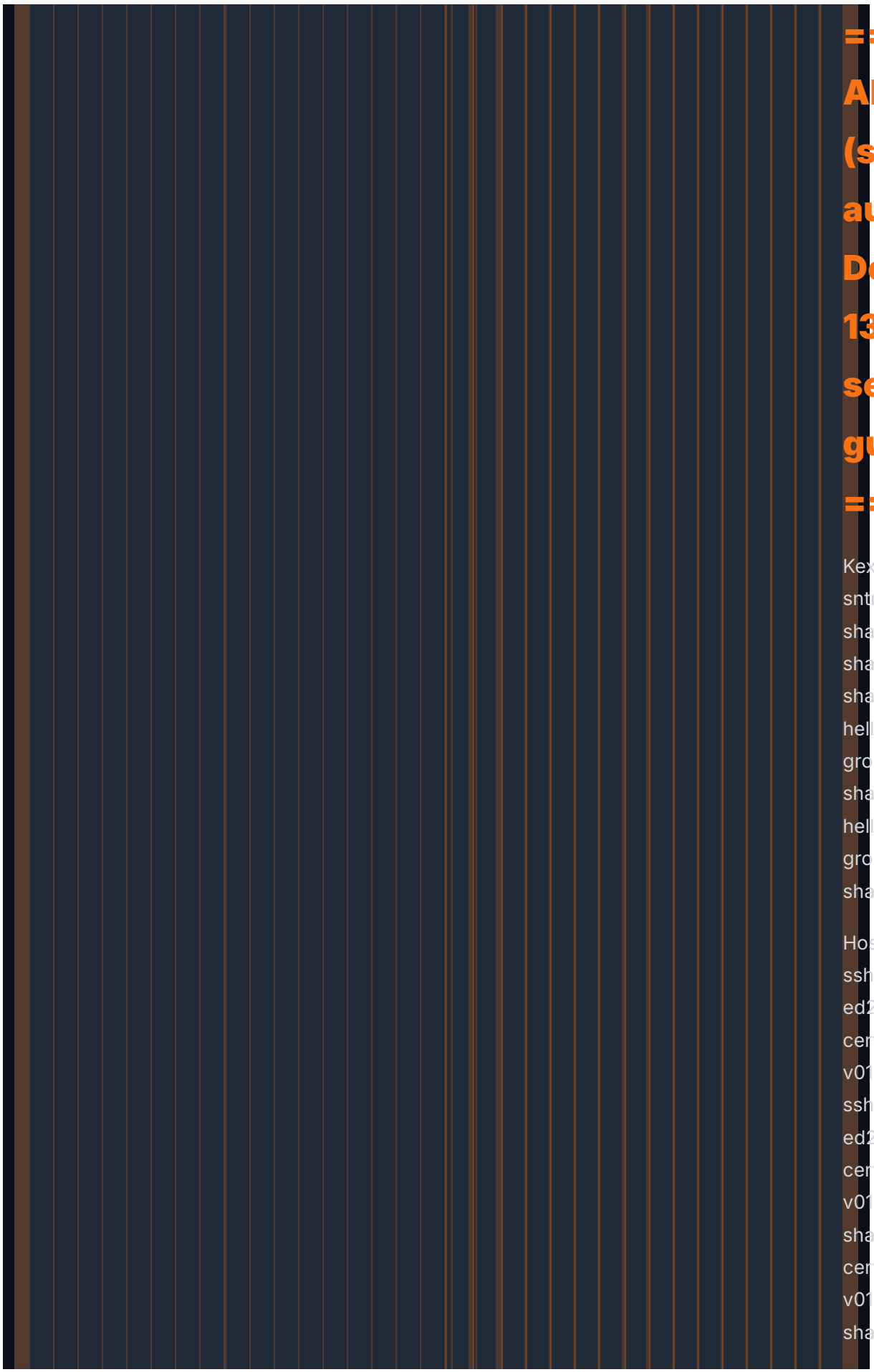
Audit :

Installer et exécuter ssh-audit

```
apt install -y ssh-audit 2>/dev/null || pip install ssh-audit --break-
```



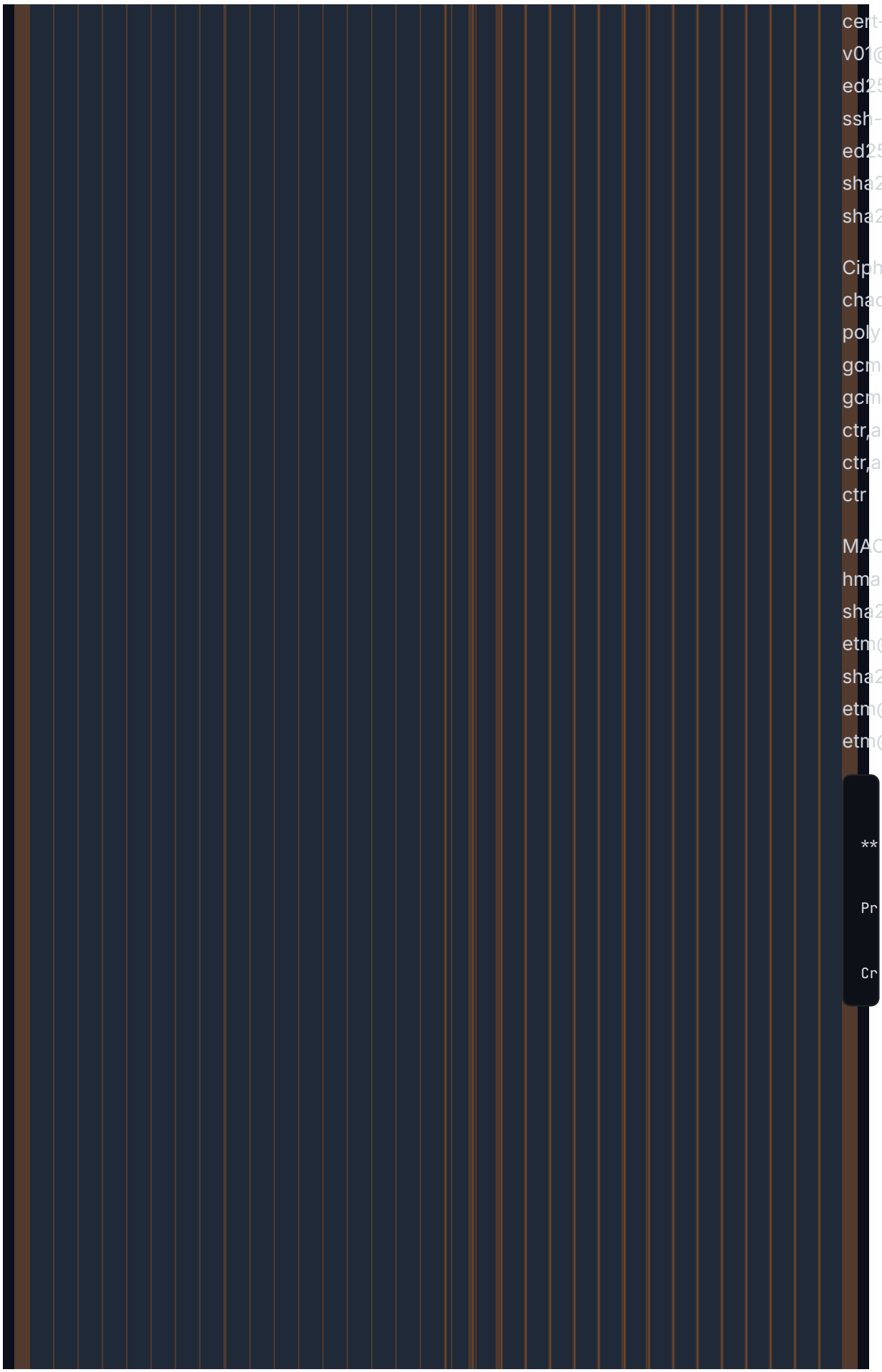
Résultat attendu : pas de lignes en rouge (fail) ou orange (warn)

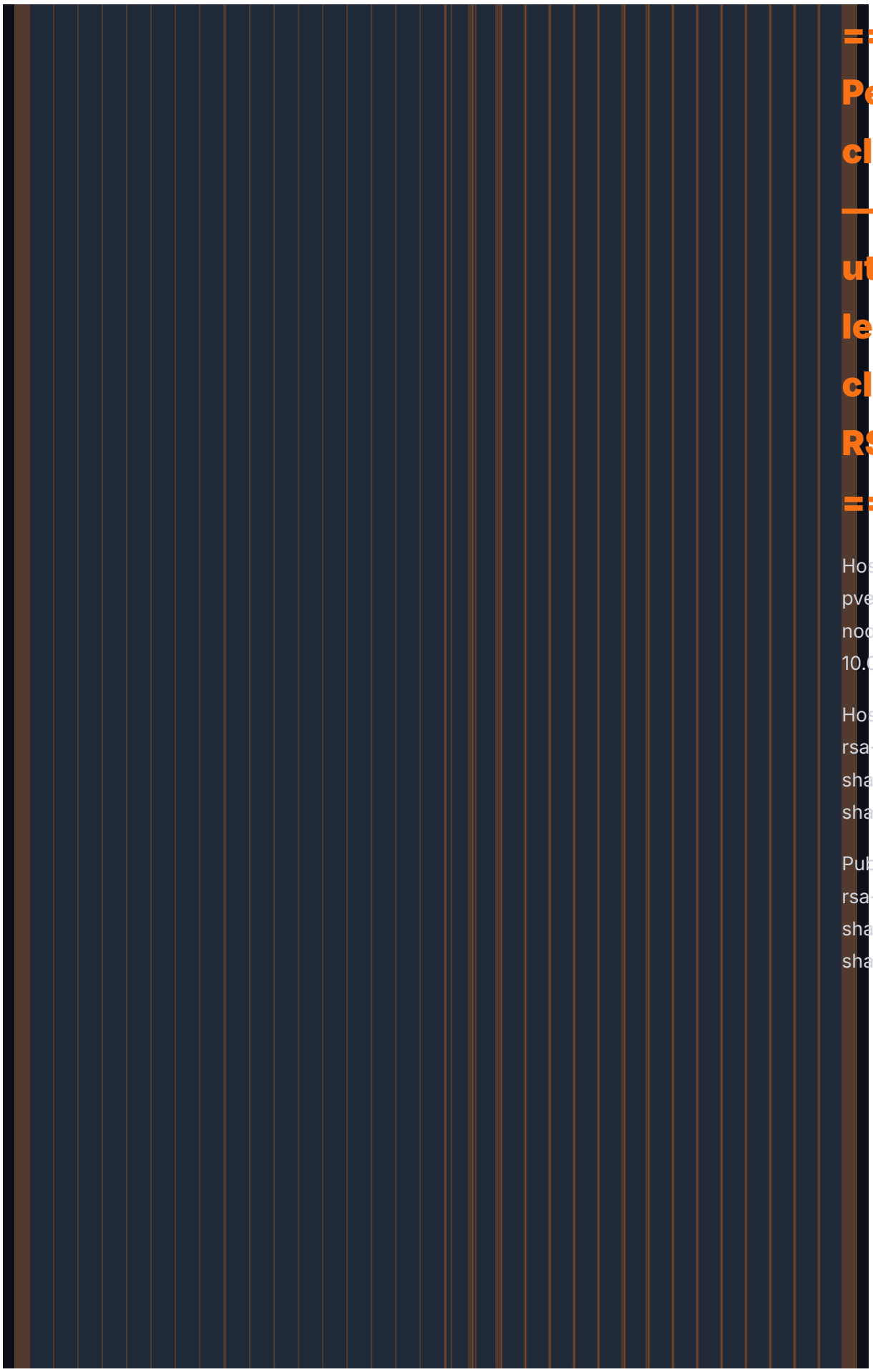


=== Algorithm (ssh-audit Debian 13 server guide) ===

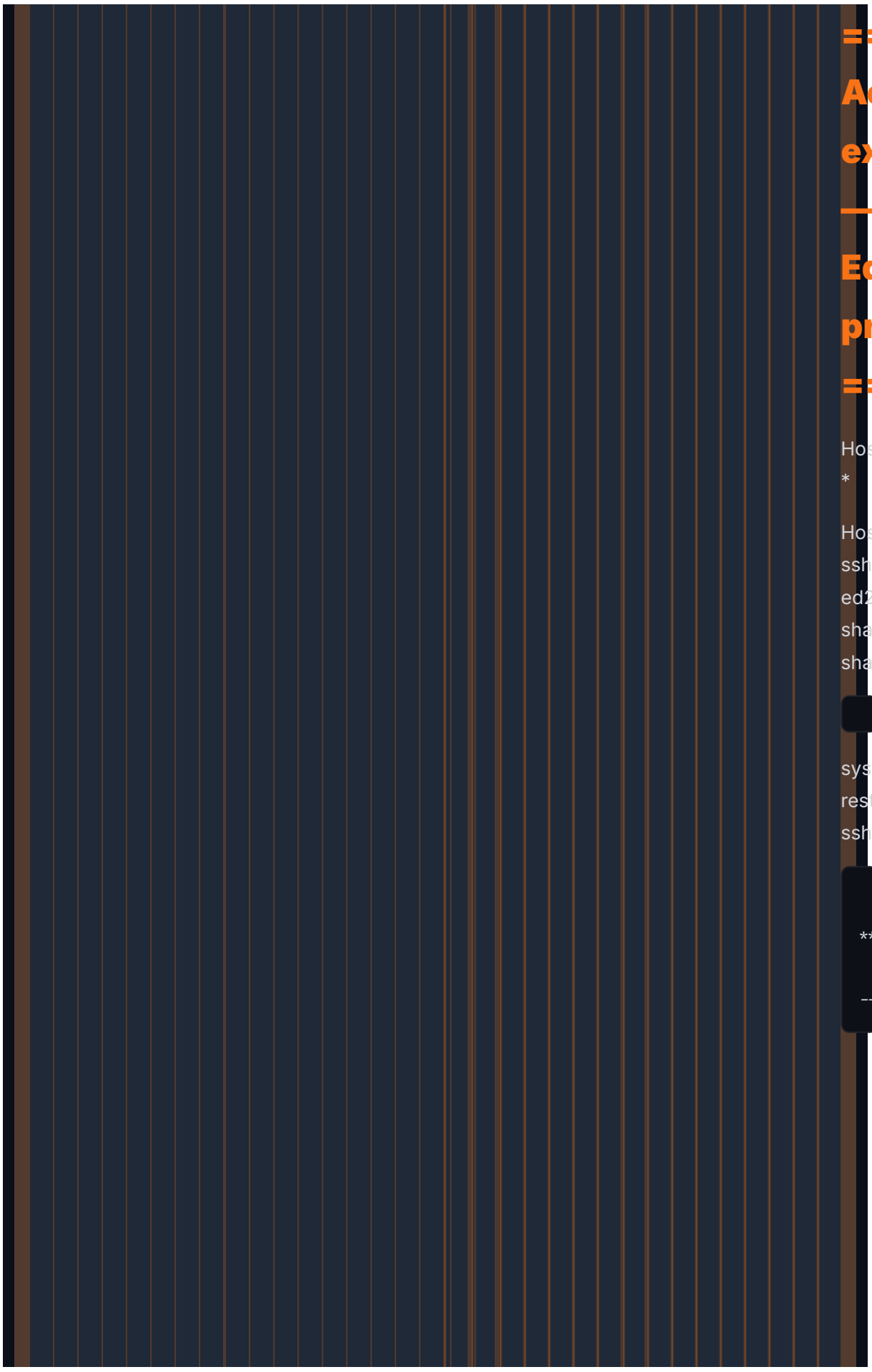
KexAlgorithms
sntrup761×25519-
sha512@openssh.
sha256,curve2551
sha256@libssh.or
hellman-
group18-
sha512,diffie-
hellman-
group16-
sha512

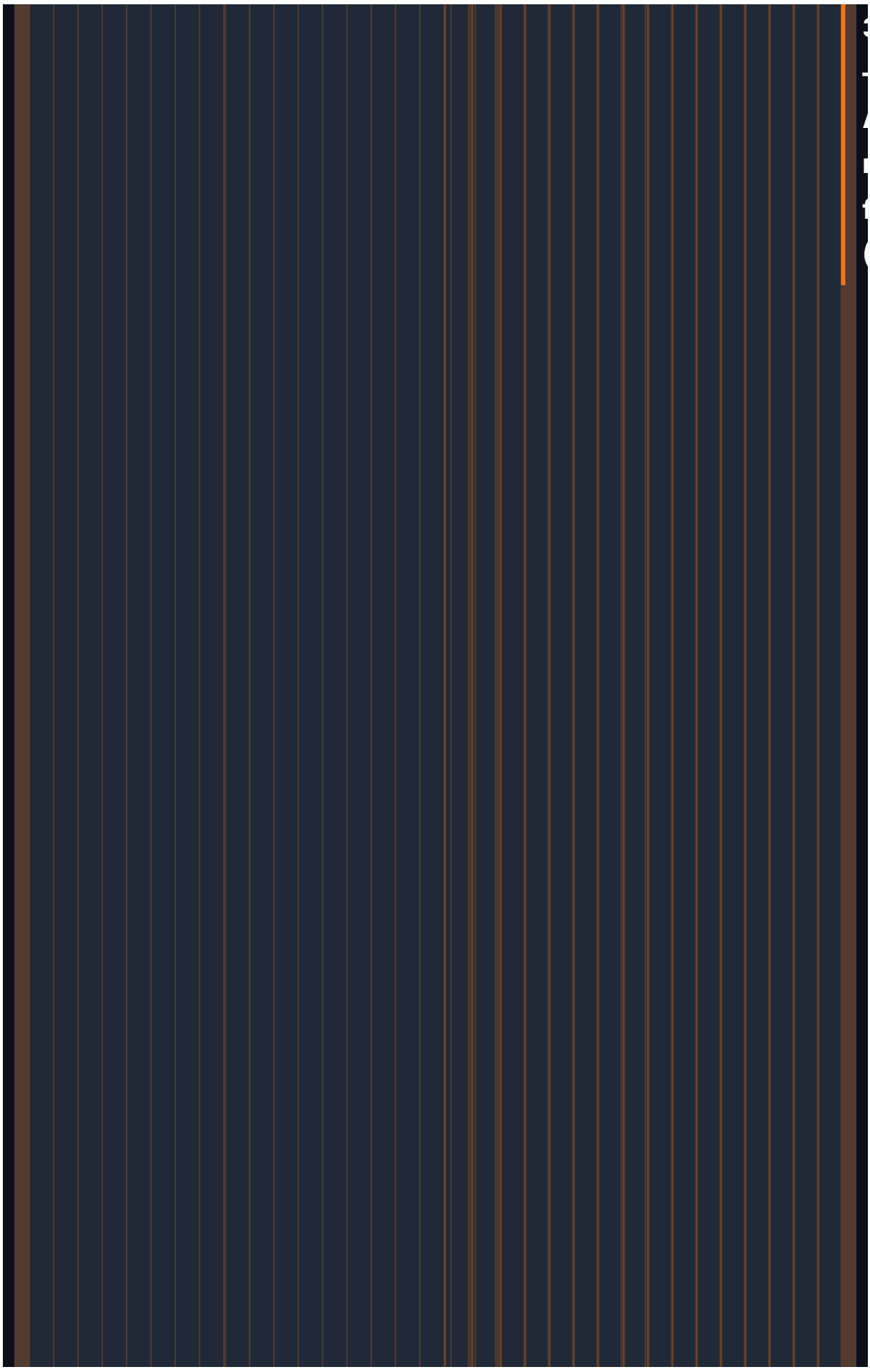
HostKeyAlgorithm
ssh-
ed25519-
cert-
v01@openssh.com
ssh-
ed25519-
cert-
v01@openssh.com
sha2-512-
cert-
v01@openssh.com
sha2-256-

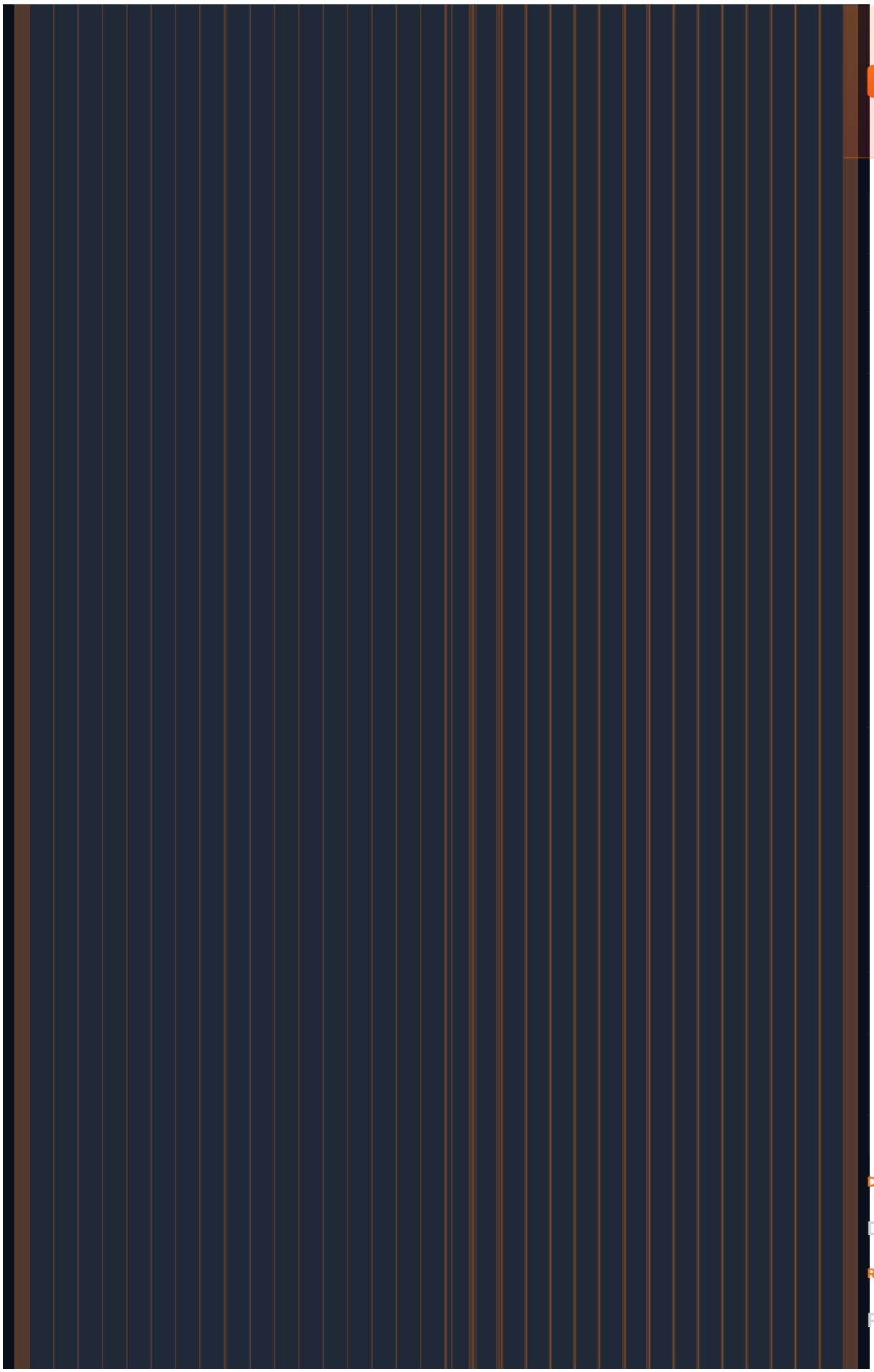

cert-
v01@openssh.com
ed25519,sk-
ssh-
ed25519@openss
sha2-512,rsa-
sha2-256
Ciphers
chacha20-
poly1305@openss
gcm@openssh.co
gcm@openssh.co
ctr,aes192-
ctr,aes128-
ctr
MACs
hmac-
sha2-512-
etm@openssh.com
sha2-256-
etm@openssh.com
etm@openssh.com
**
Pr
Cr



```
=== Peers cluster — utiliser les clés RSA ===

Host pve-node 10.0.40.

HostKeyAlgorithm rsa-sha2-512,rsa-sha2-256

PubkeyAcceptedA rsa-sha2-512,rsa-sha2-256
```


===
Accès
externe
—
Ed25519
préféré
===
Host
*
HostKeyAlgorithm
ssh-
ed25519,rsa-
sha2-512,rsa-
sha2-256
systemctl
restart
sshd
**
--





3.2.1

PROFILE APPLICABILITY

APPLICABILITÉ PVE

RÉF. CIS DEBIAN 13

CIS CONTROLS V8

MITRE ATT&CK

ISO 27001:2022

PCI DSS V4.0

SCÉNARIO THREAT MODEL

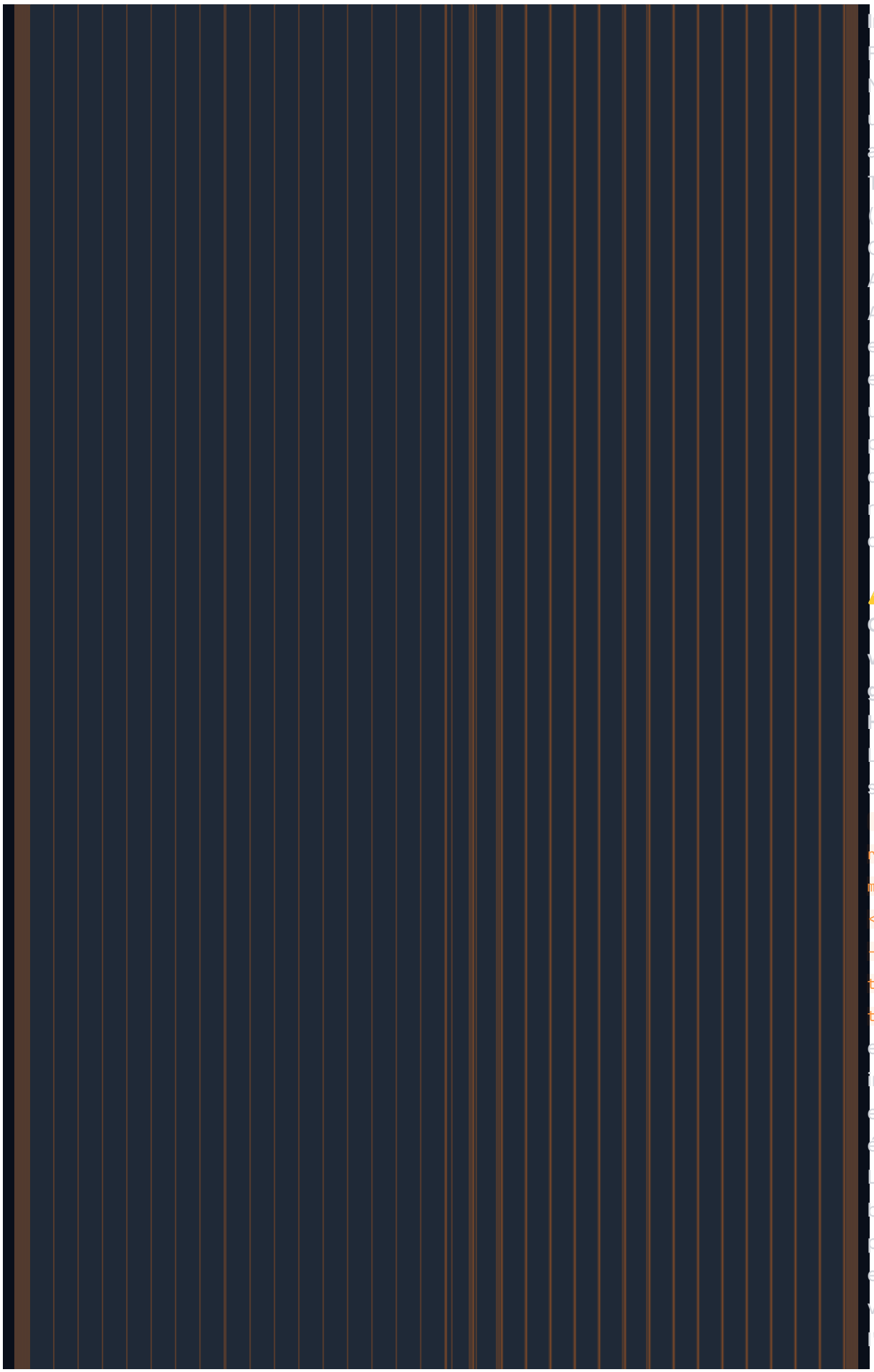
STATUT PVE 9

DESCRIPTION :

Description :

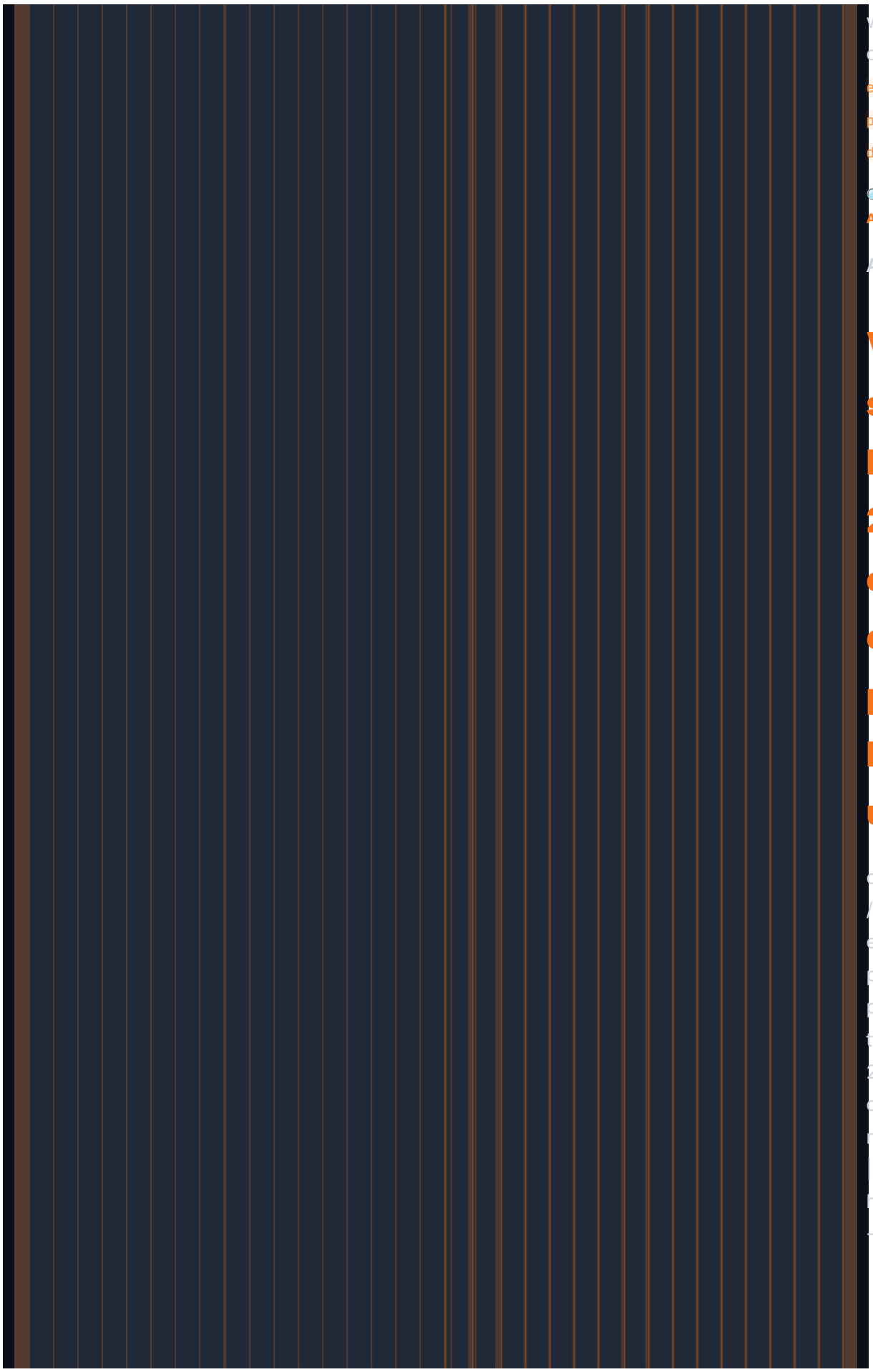
RATIONALE :

Rationale :



Impact : Faible. Nécessite une app TOTP (FreeOTP, Google Authenticator, Aegis, etc.) et une procédure de récupération documentée.

⚠️ **CORRECTION vs guide HomeSecExplo** La syntaxe `pveum realm modify <<pam>> --tfa type=<<oath>>` est incorrecte et échoue. La bonne procédure est via l'interface



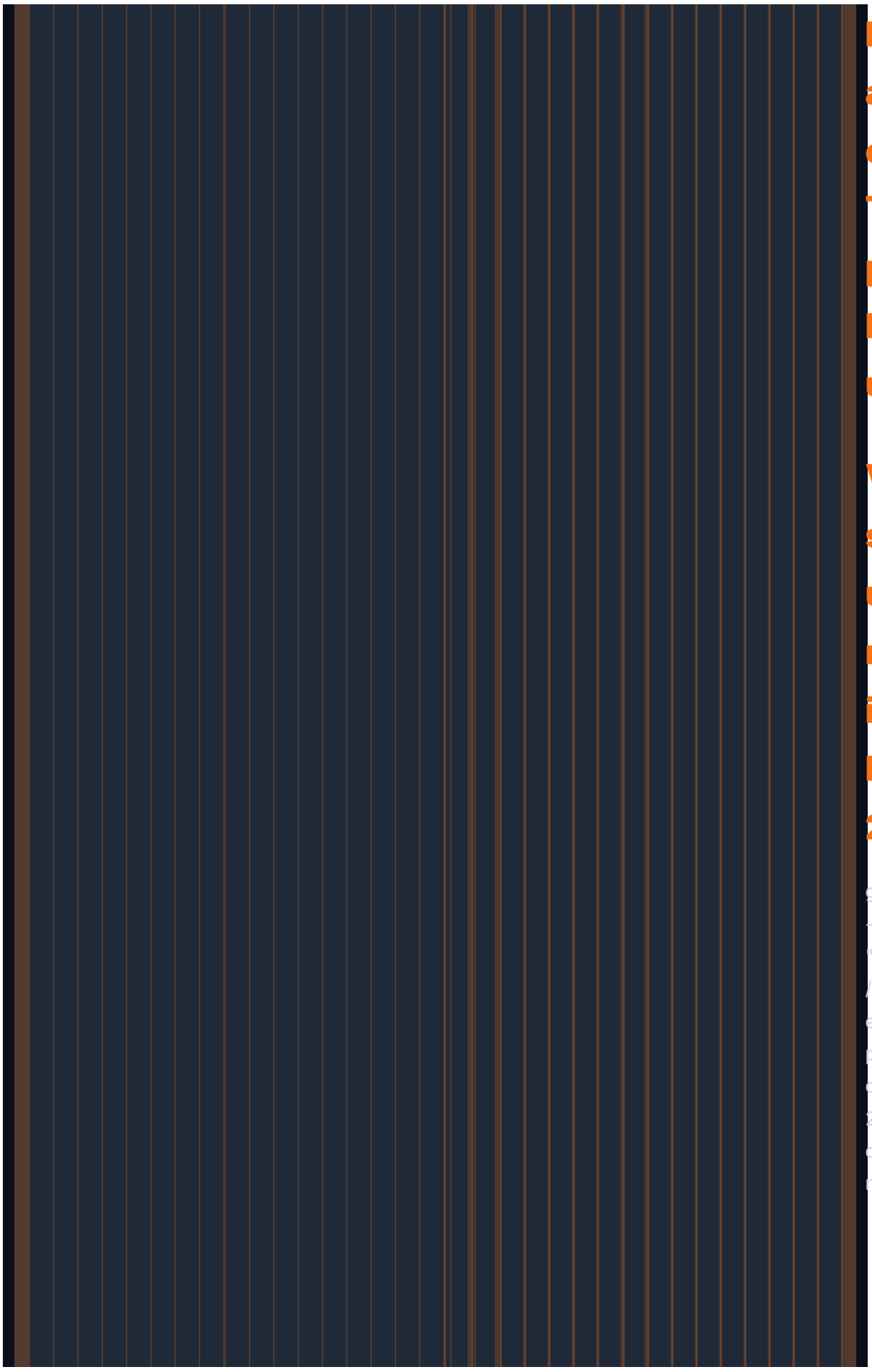
web ou `/etc/pve/domains.cfg`.

🔍 AUDIT

Audit :

Vérifier si le 2FA est configu pour les utilisate

```
cat /etc/pve/priv/tfa.cfg 2>/dev/null | head -5
```

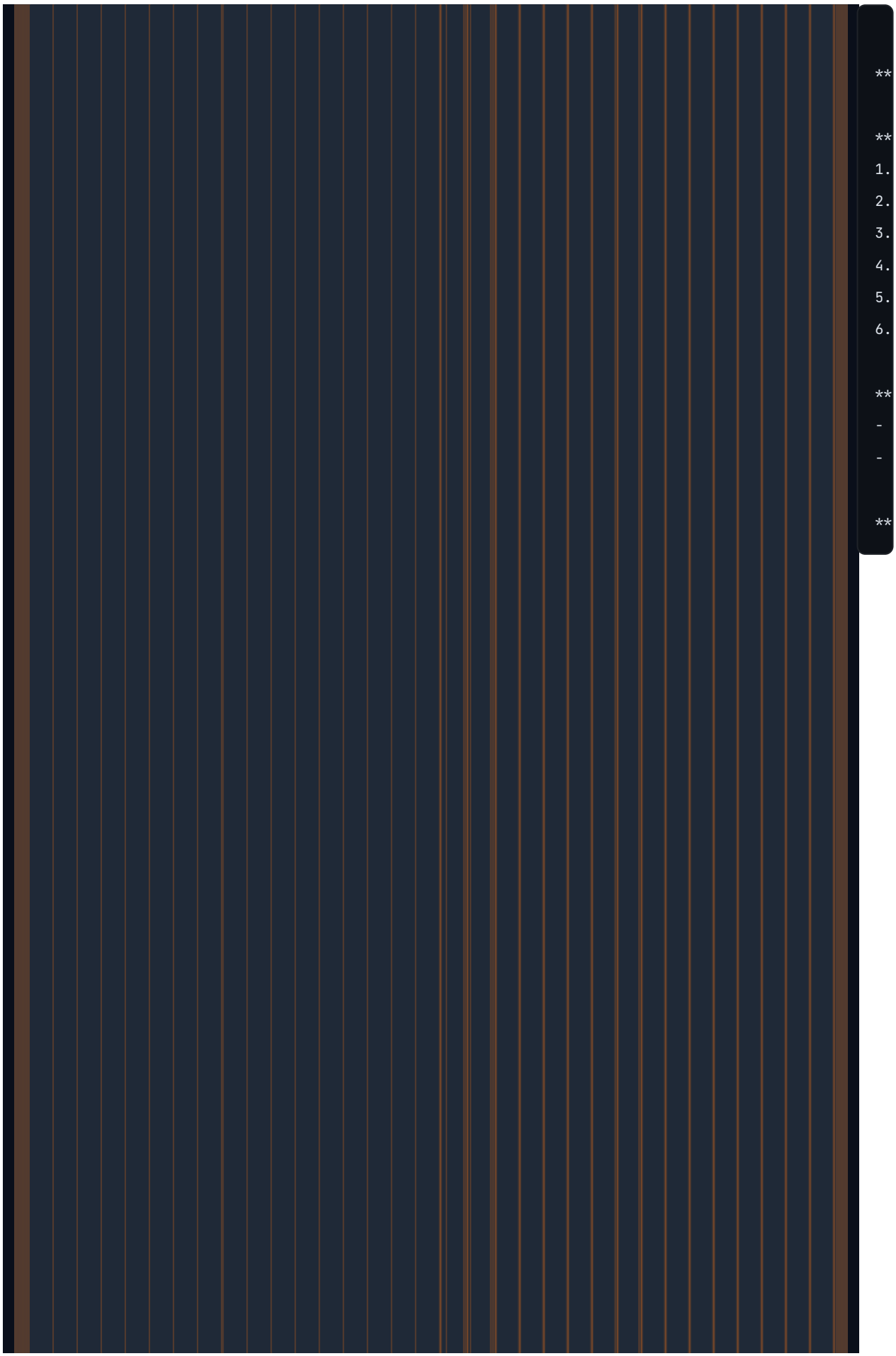


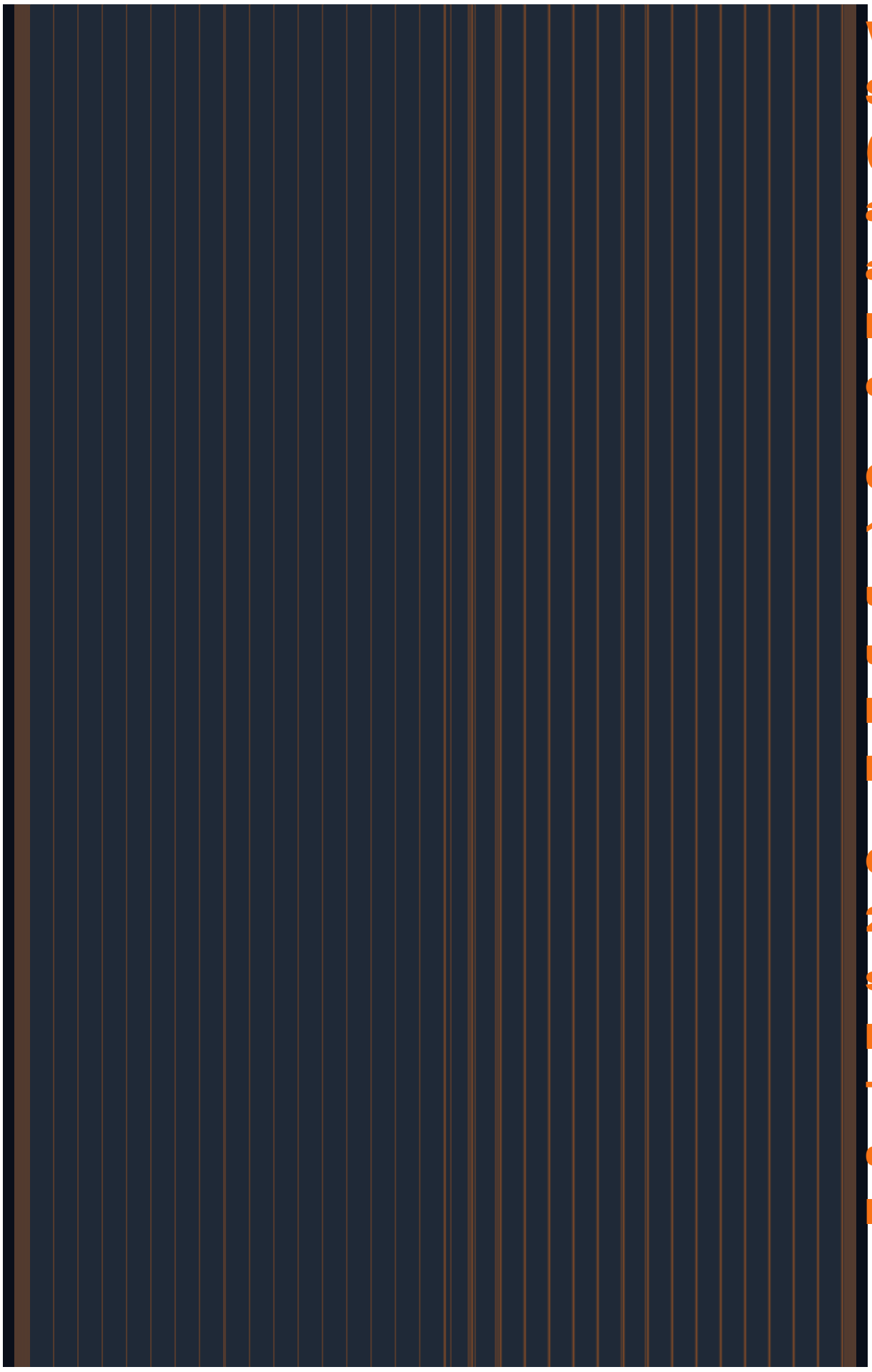
Résultat attendu

entrées TFA pour les utilisate

Vérifier si un realm impose le 2FA

```
grep -i "tfa" /etc/pve/domains.cfg 2>/dev/null
```

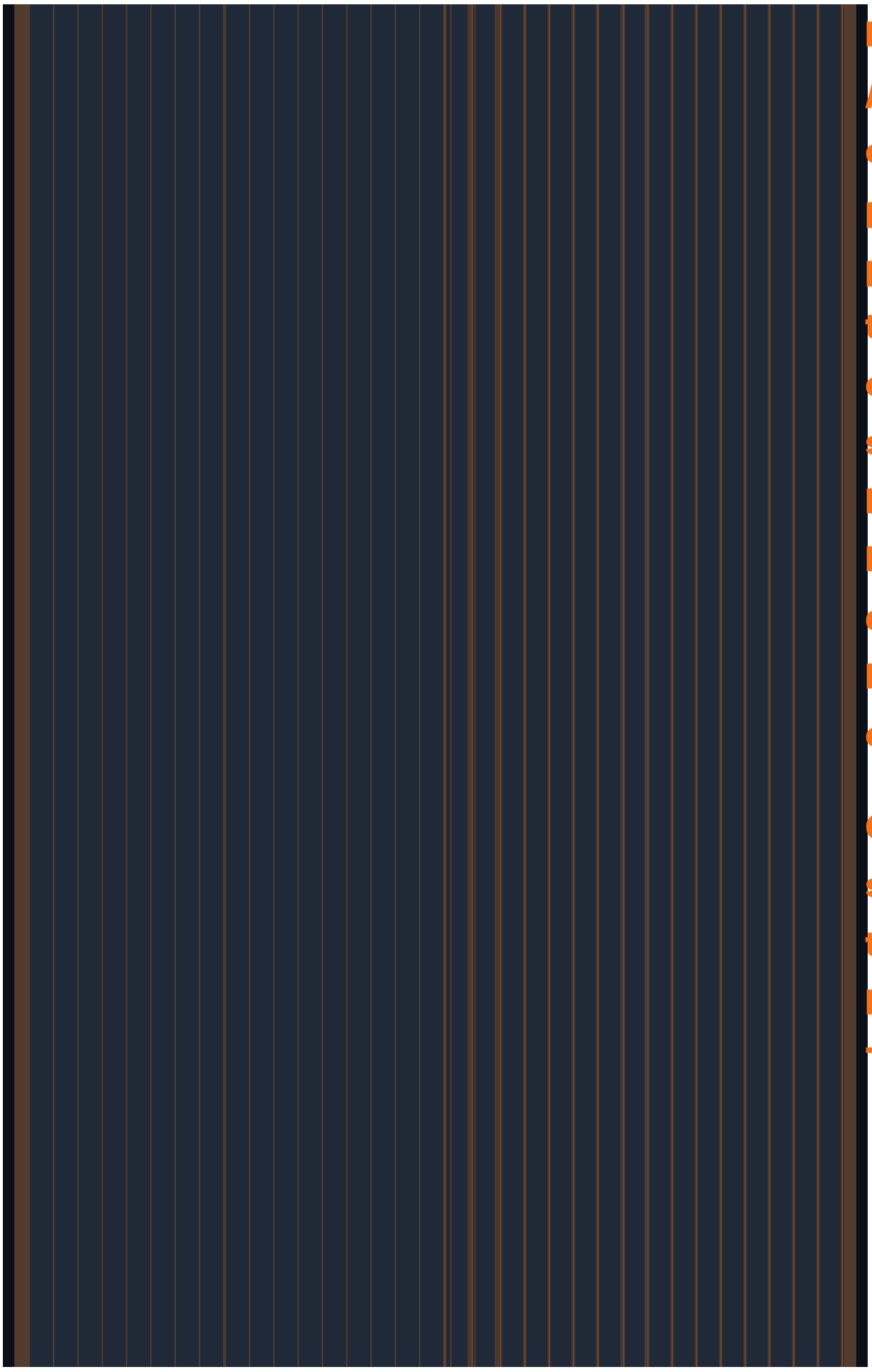

**
**
1.
2.
3.
4.
5.
6.
**
-
-
**



Via SSH (toujour accessil avec les clés) :

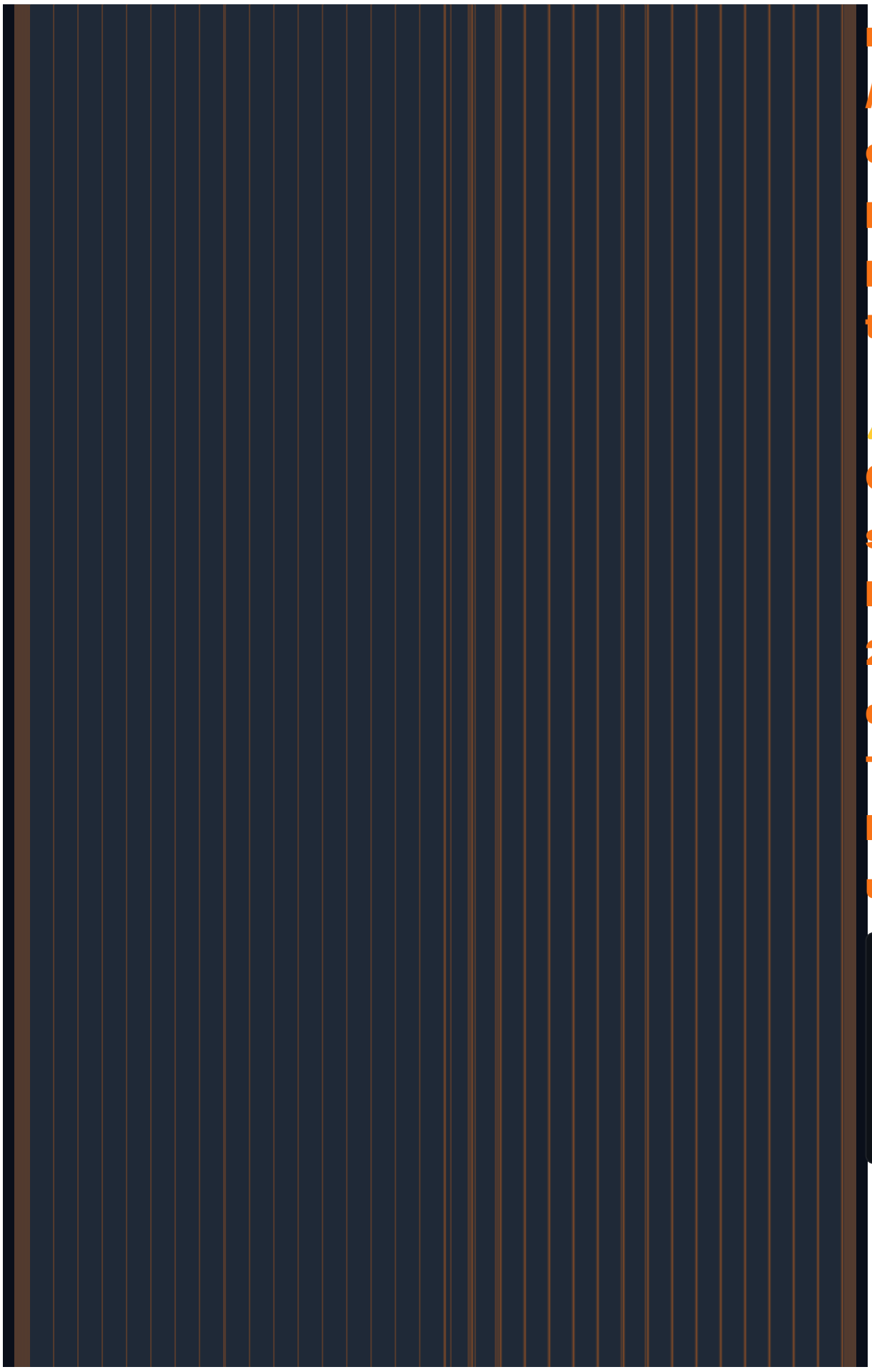
Option 1 : utiliser une Recover Key

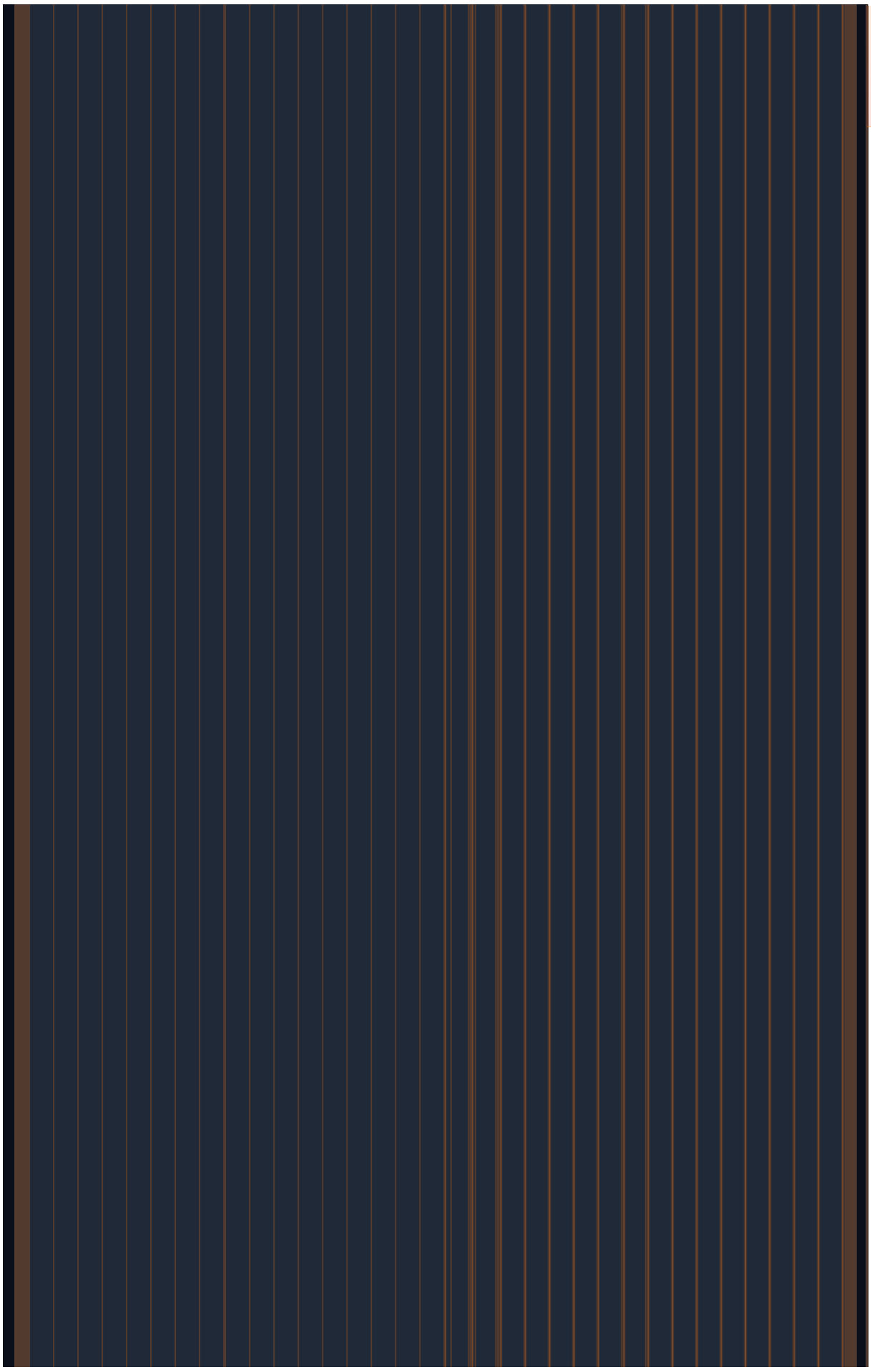
Option 2 : supprim le TFA de l'utilisat



Éditer / etc/ pve/ priv/ tfa.cfg et supprim la ligne de l'utilisat concern

Ou supprim tout le TFA :


rm
/
etc/
pve/
priv/
tfa.cfg
⚠️
Ceci
supprim
le
2FA
de
TOUS
les
utilisate
**
**
--



3.2.2

PROFILE APPLICABILITY

APPLICABILITÉ PVE

RÉF. CIS DEBIAN 13

CIS CONTROLS V8

MITRE ATT&CK

ISO 27001:2022

PCI DSS V4.0

SCÉNARIO THREAT MODEL

STATUT PVE 9

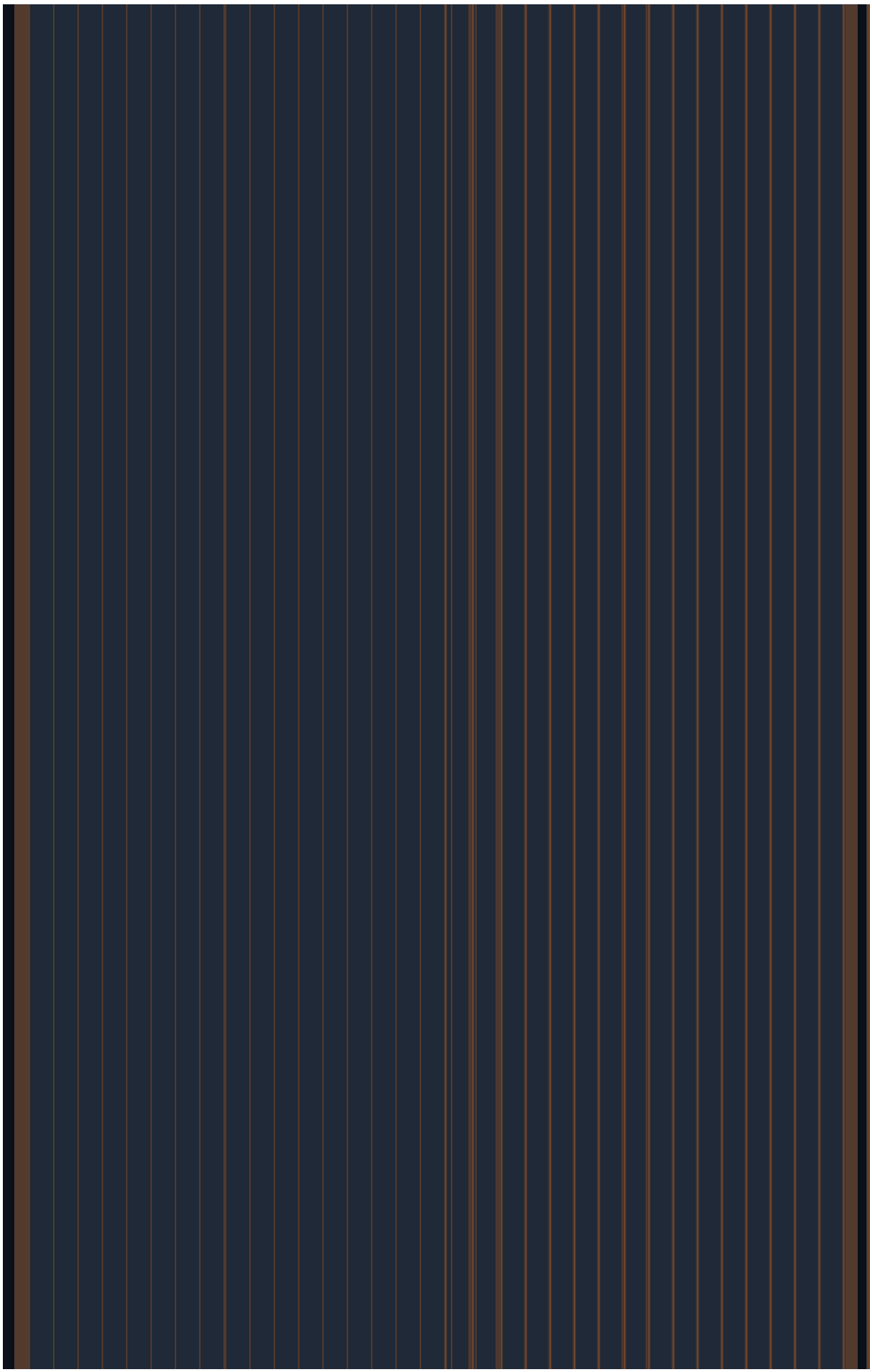
DESCRIPTION :

Description

RATIONALE :

Rationale :

Impact :
Nécessite un certificat TLS valide (pas auto-signé) et la configuration



WebAuthn dans PVE.

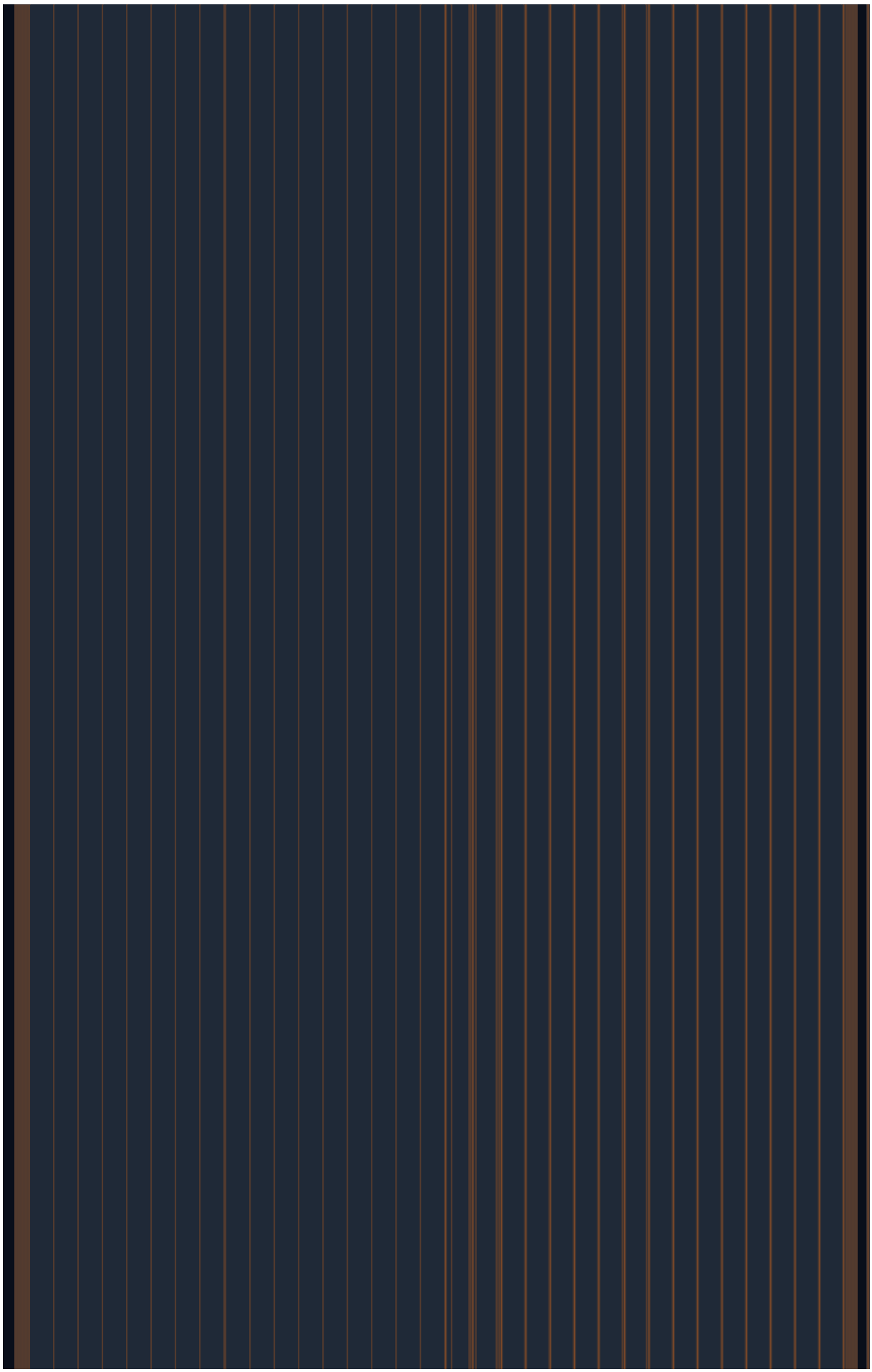
Prérequis :

- Cer TLS vali sur le nœ PVE (vo Pha 2, 2.1.
- Har key (Yu Sol ou pla aut (To ID, Wir Hel And

🔧 **REMÉDIATION**

Remédiation

- Ori `htt` `<vo` `fqd`
- Rel Par `<vo` `fqd`



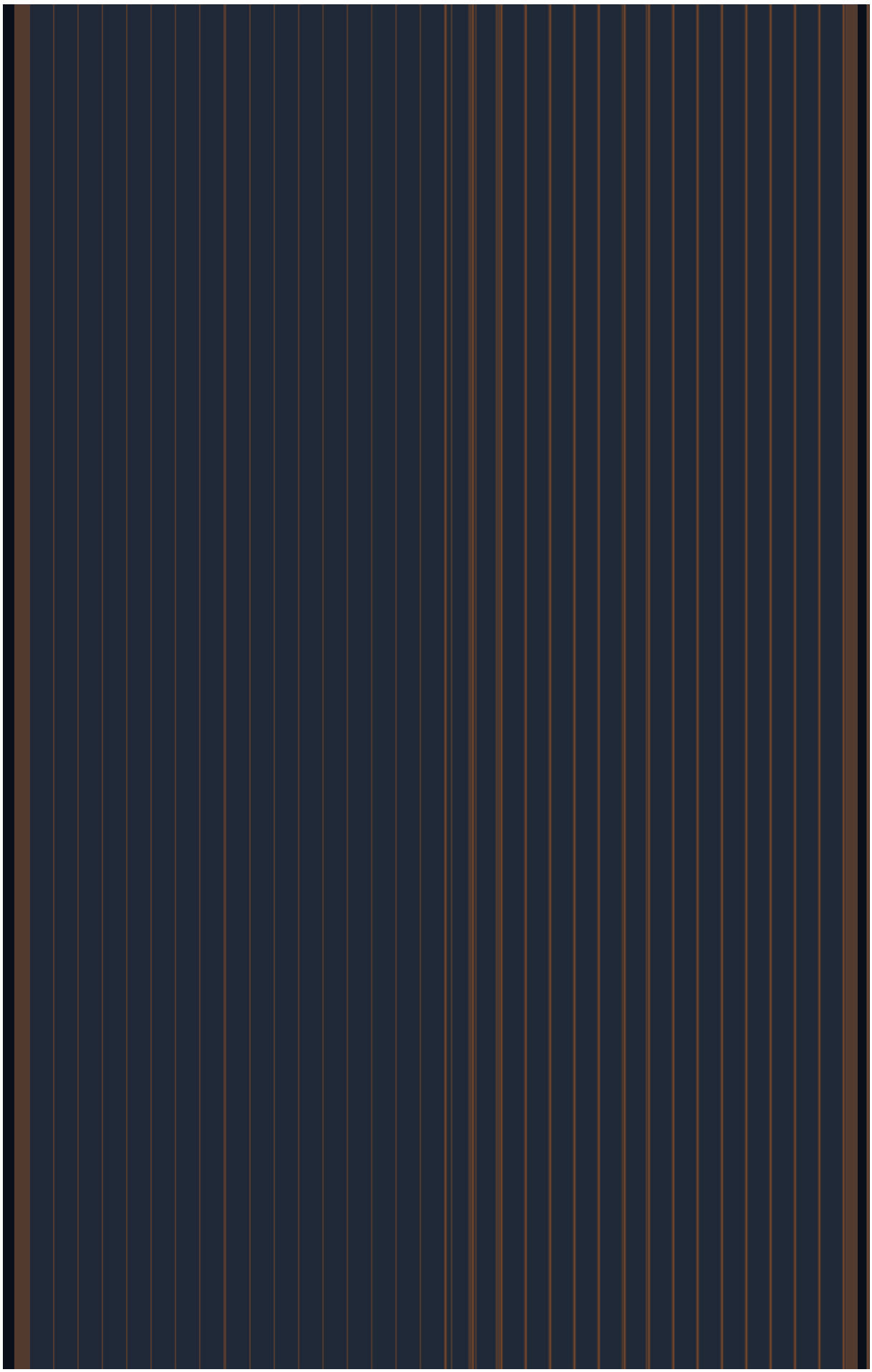
- ID :
  <v
  dom

1. **Dat**
   >
   Per
   >
   Tw
   Fac
   >
   Ad
   >
   We

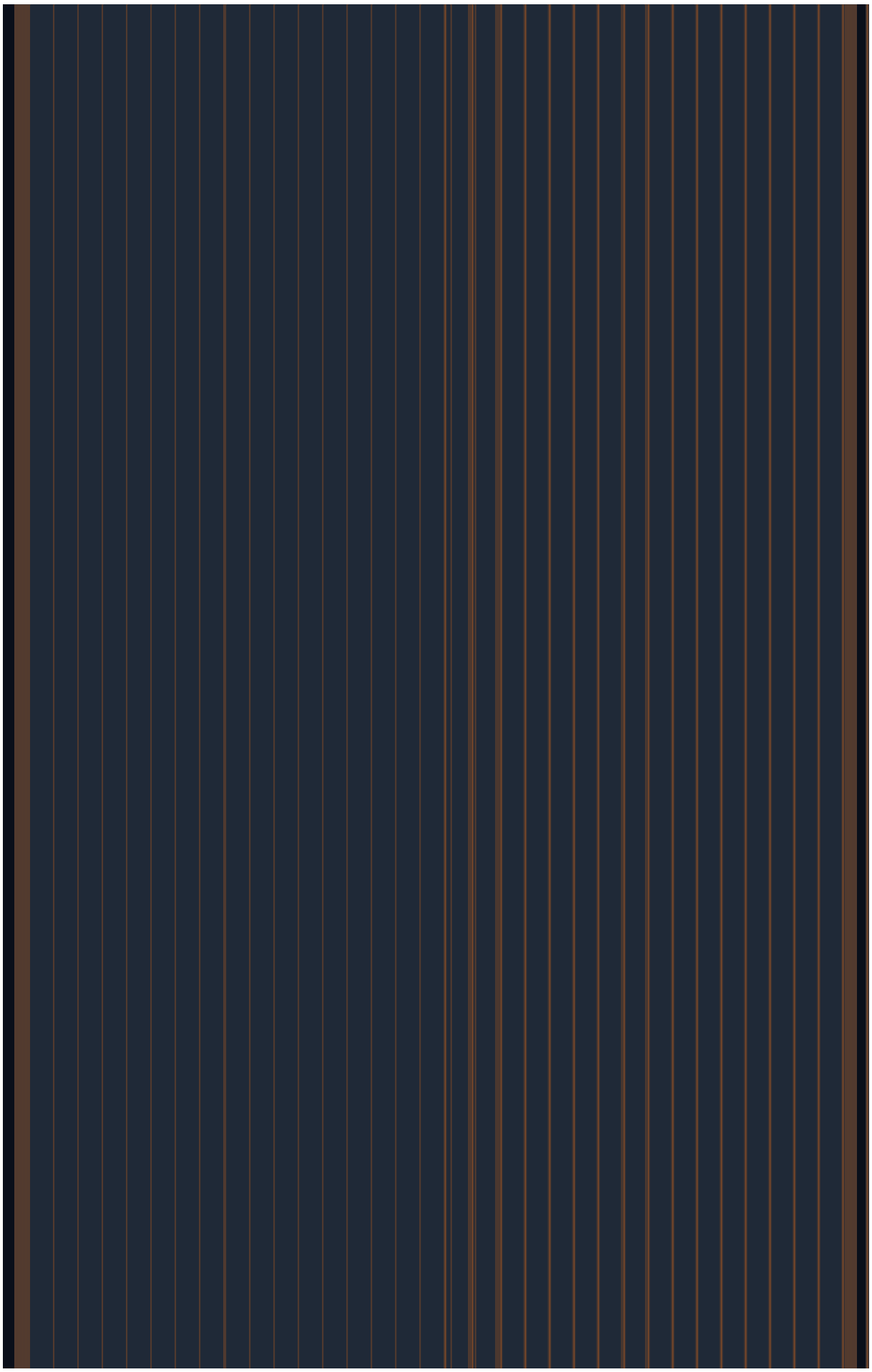
1. Enr
   vot
   clé
   ou
   aut

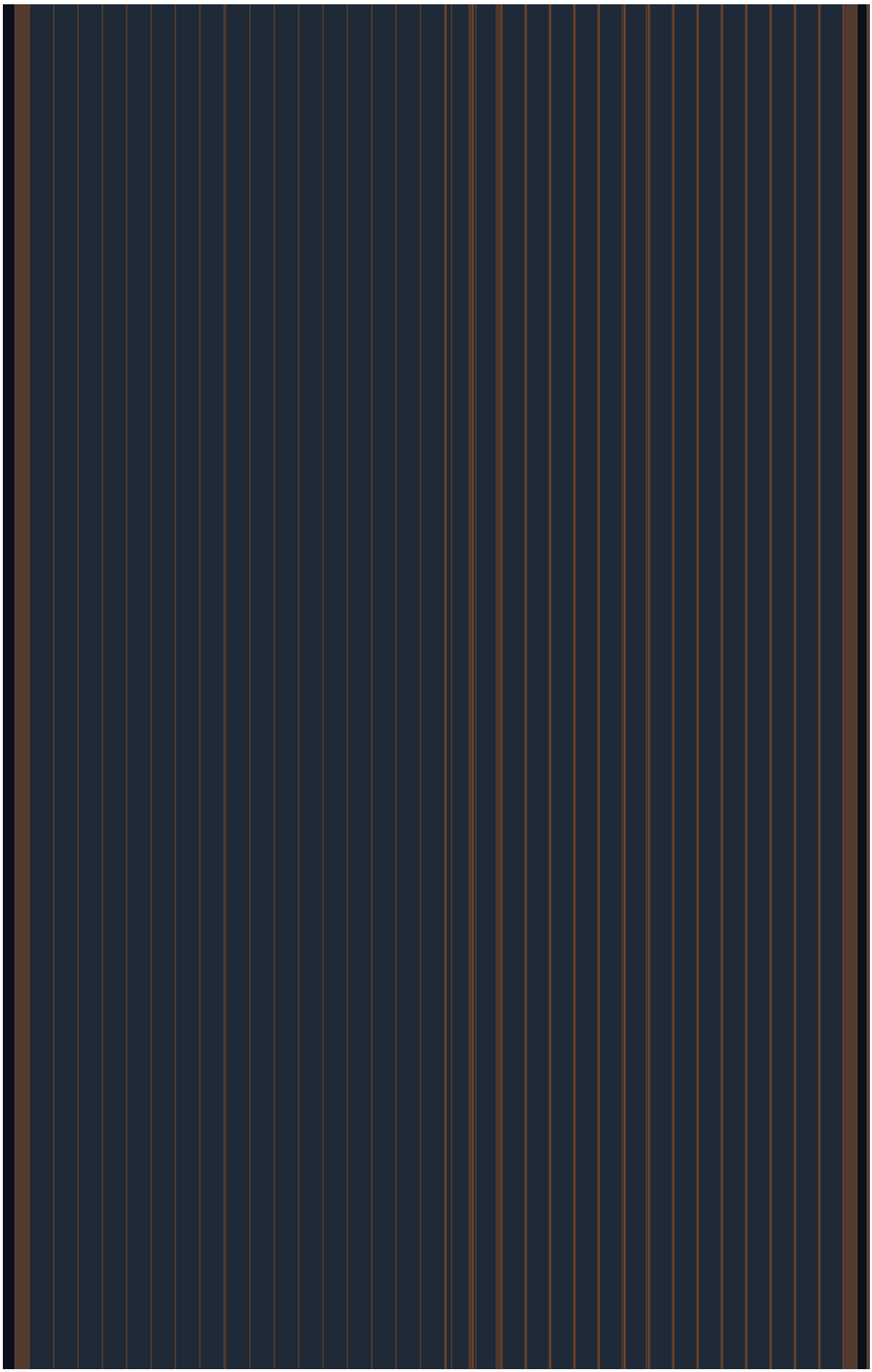
Valeur par défaut : WebAuthn non configuré.

Spécificité PVE : En cluster, le WebAuthn Relying Party doit correspondre au domaine par lequel vous accédez



au cluster. Si vous accédez via des noms différents par nœud, WebAuthn ne fonctionnera que pour le domaine configuré. Un load balancer ou DNS round-robin avec un FQDN unique est recommandé





3.3.1

PROFILE APPLICABIL

APPLICABIL PVE

RÉF. CIS DEBIAN 13

CIS CONTRO V8

MITRE ATT&

ISO 27001:2022

PCI DSS V4.

SCÉNARIO THREAT MODEL

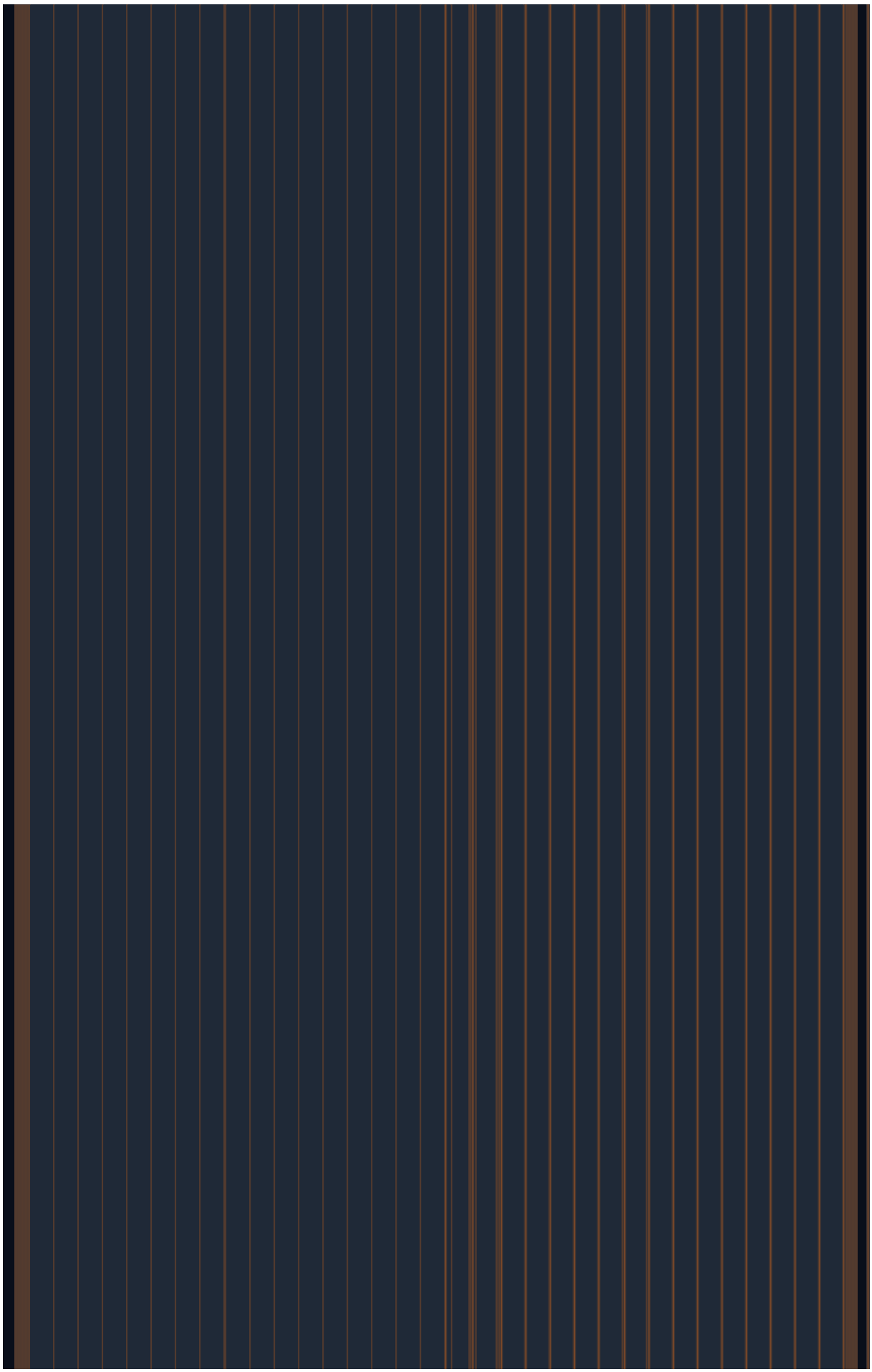
STATUT PVE

DESCRIPTIO

Descripti

RATIONALE

Rationale



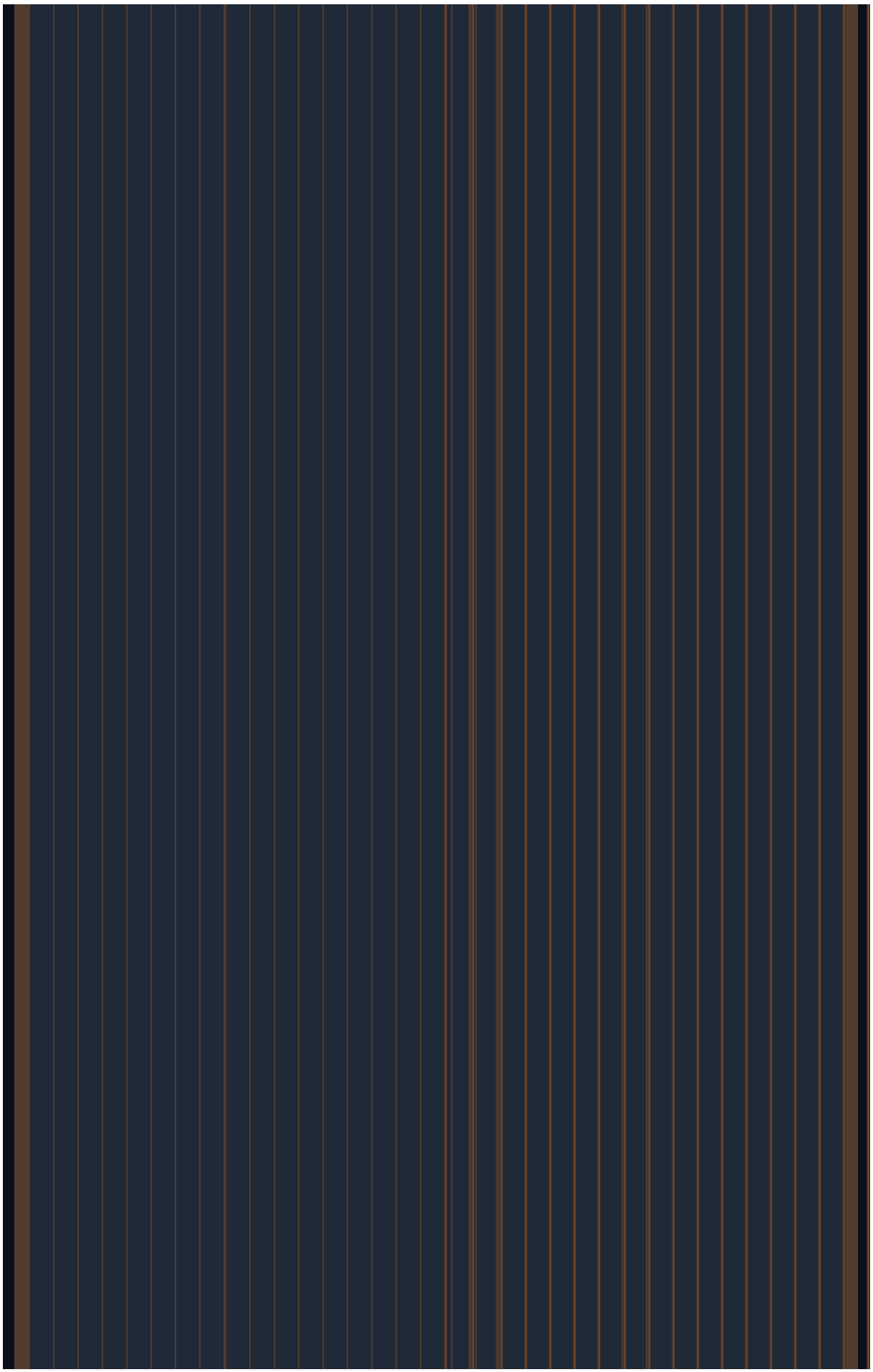
Impact : Faible. Nécessite la création de comptes et l'attributio de rôles.

🔍 **AUDIT**

Audit :

Liste les utilis

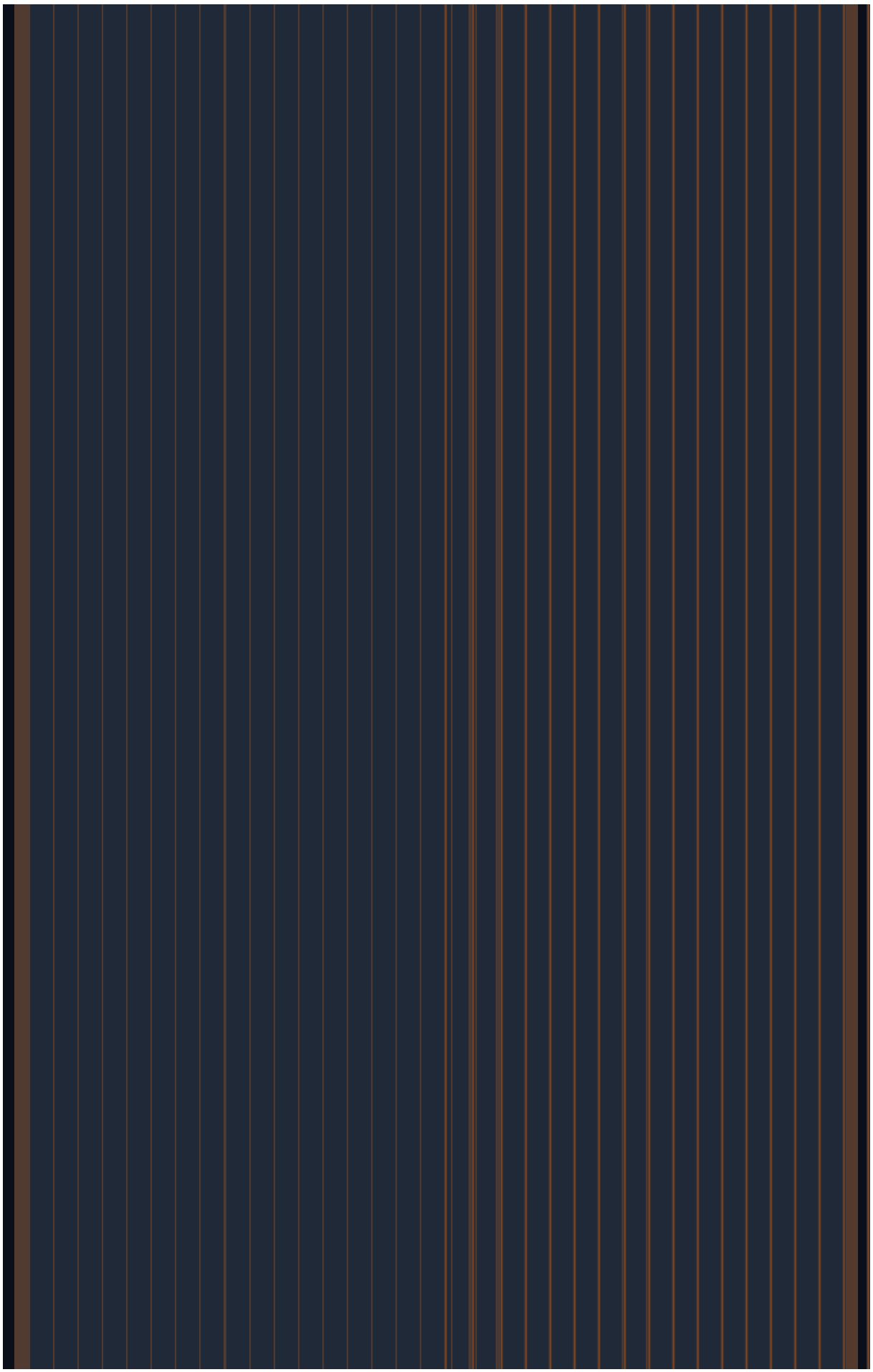
pveum user list



Résul
atten
des
comp
nomi
en
plus
de
root@

Vérifi
les
ACL

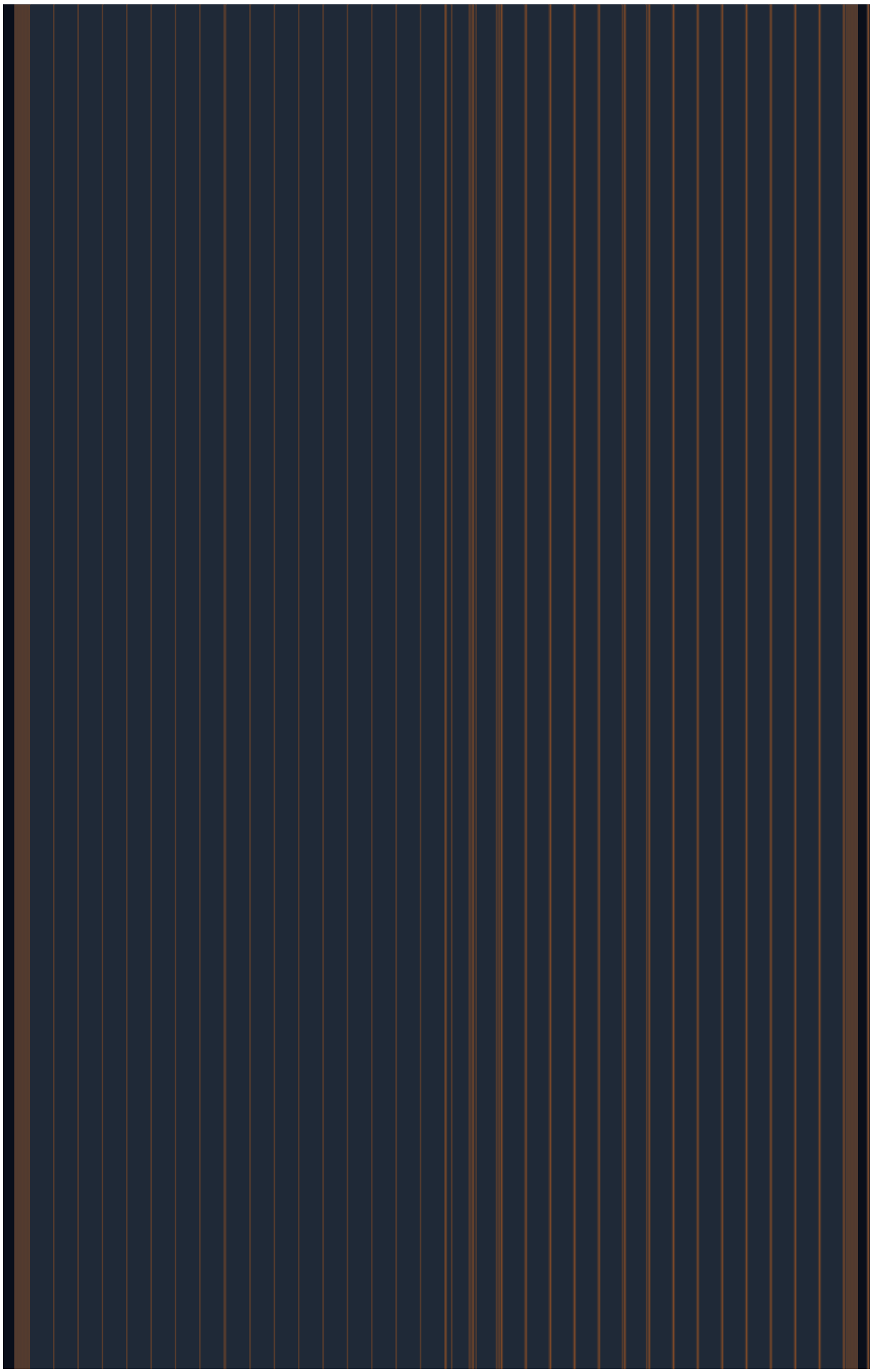
pveum
acl
list



Résul
atten
ACL
par
utilis
group
pas
de
'/'
attrib
à
tout
le
monc

Vérifi
les
conn
récer
avec
root@

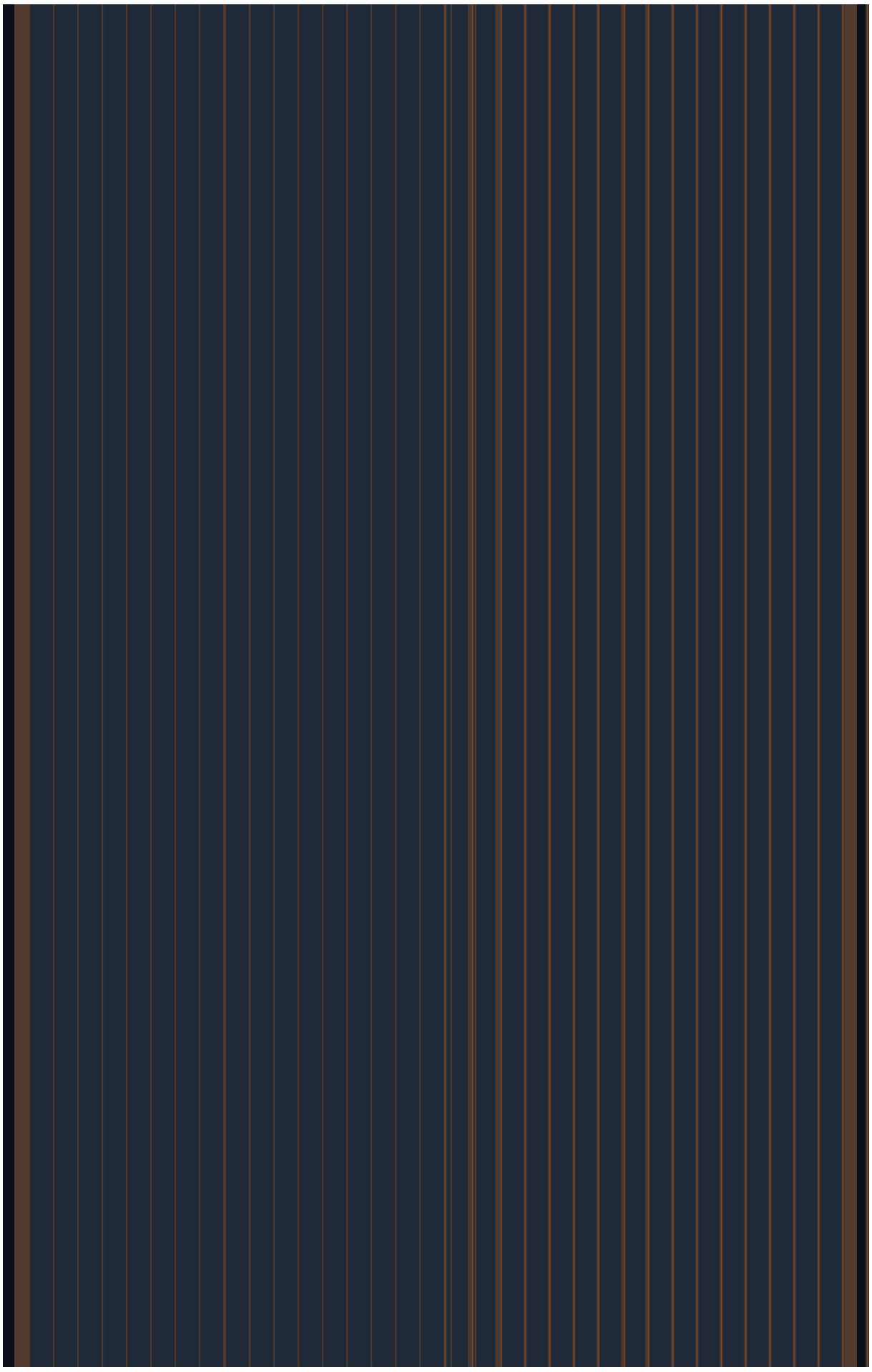
journalctl
-u
pvedaemo
--



since
"7
days
ago"
|
grep
"root@pa
|
grep
"successf
|
tail
-5

**Résul
atten
minin
(root
ne
devra
pas
être
utilis
quoti

**

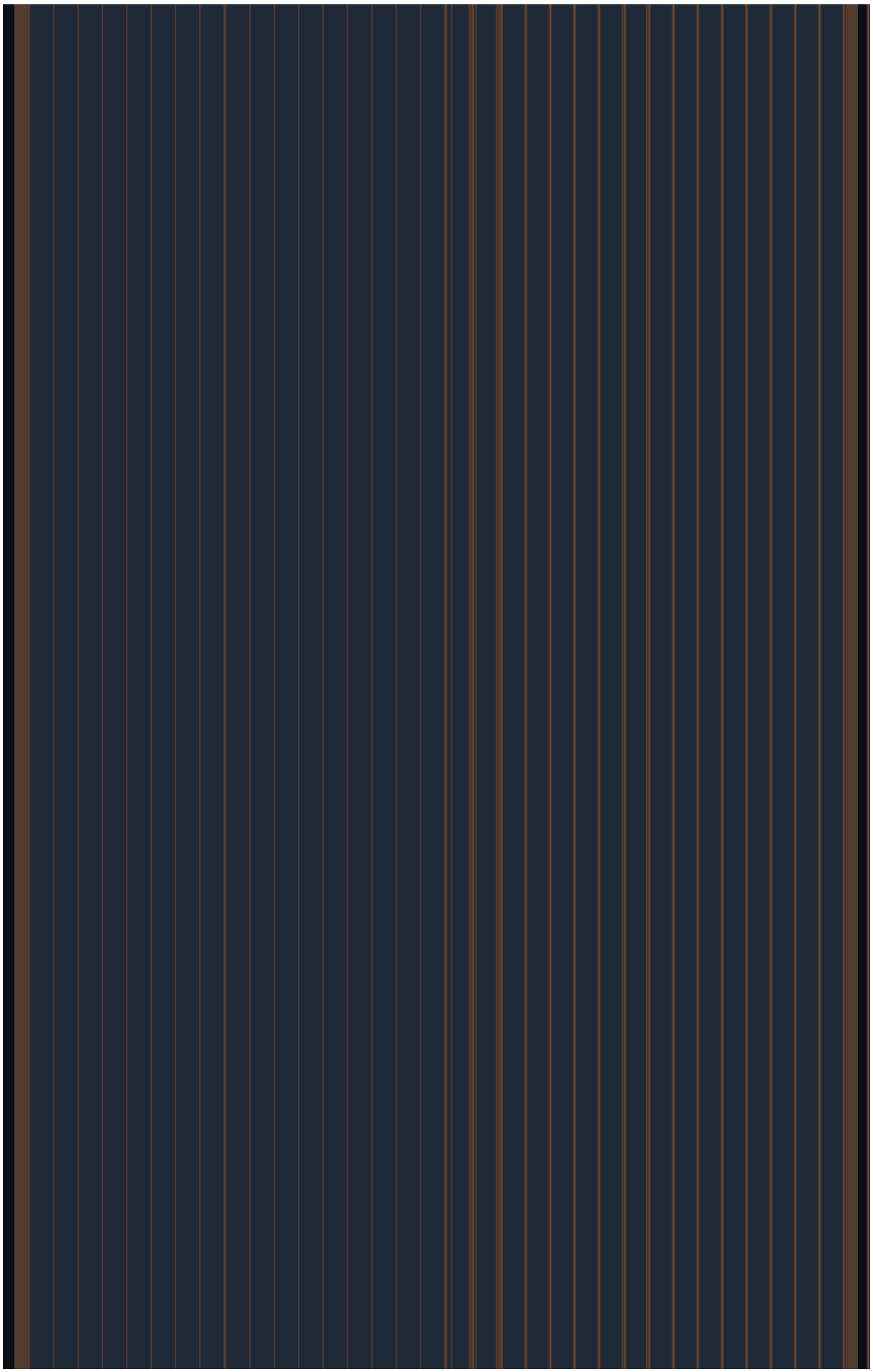


1. Créer un group d'adr

```
pveum
group
add
admins
--
comment
"Administr
PVE"
```

2. Créer des comp nomi

```
pveum
user
add
alice@pve
--
firstname
Alice
--
lastname
Dupont
--
email
alice@exa
```

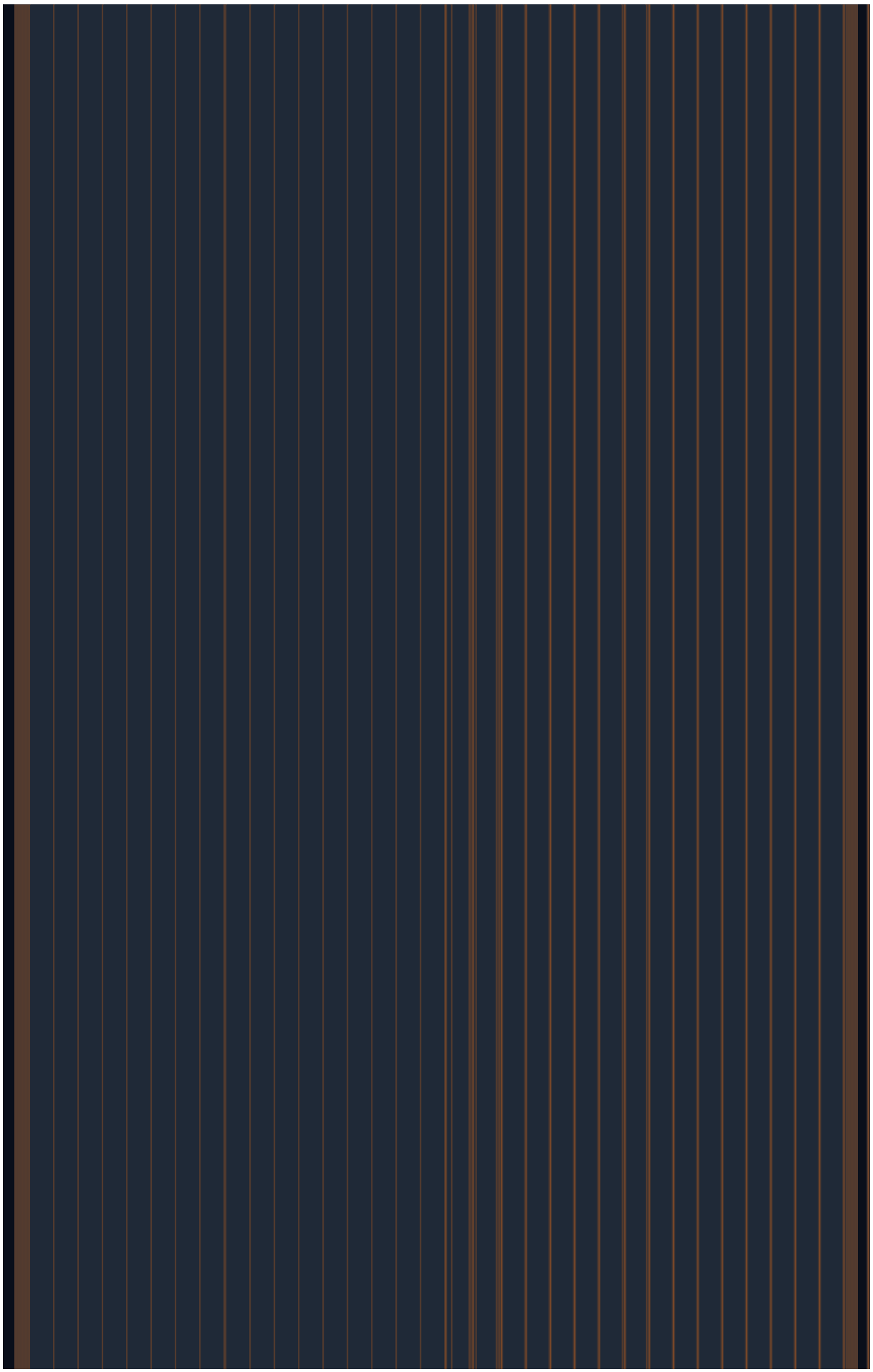


--
groups
admins

pveum
passwd
alice@pve

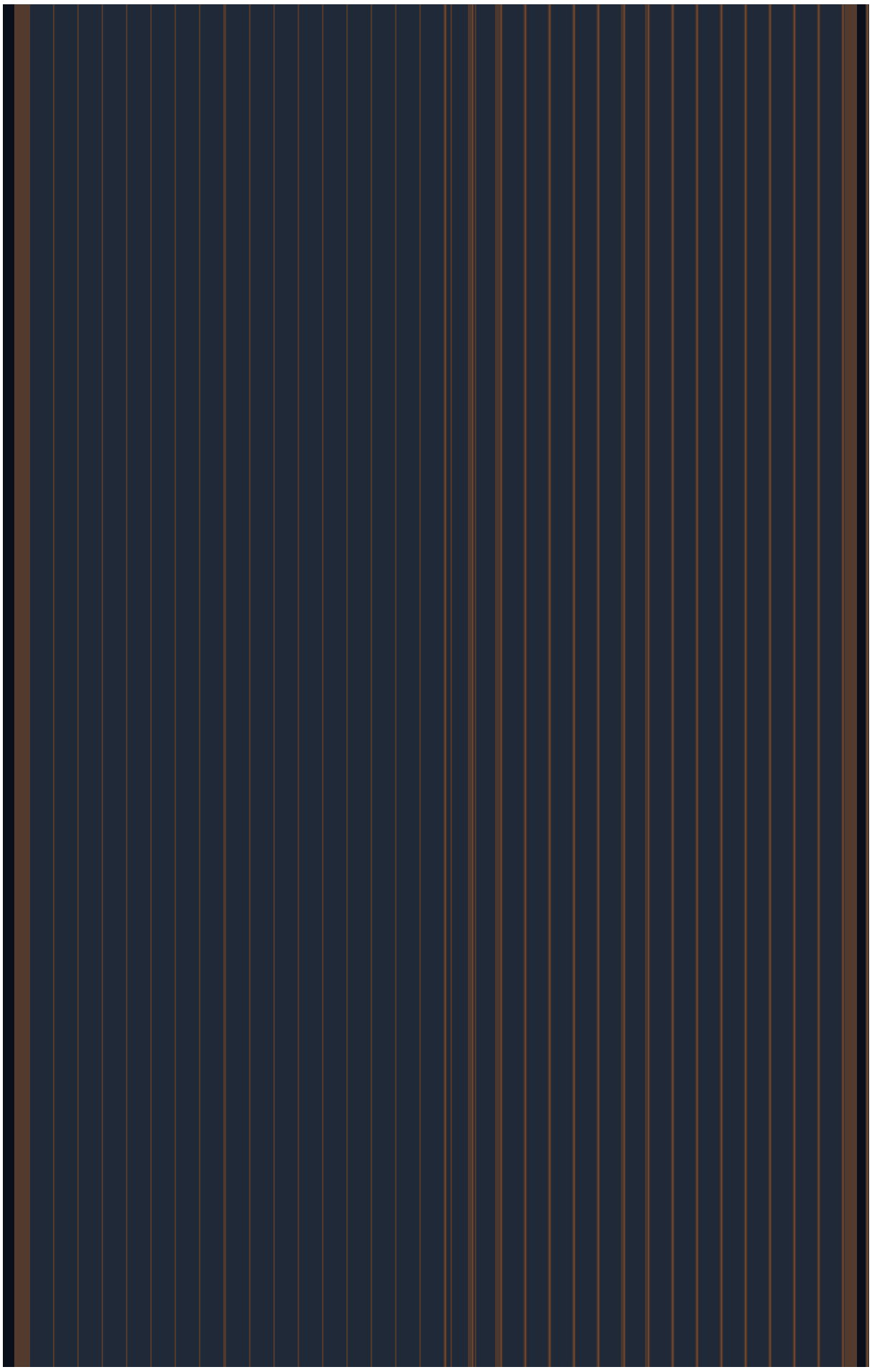
3. Attrib
le
rôle
Admi
au
group
sur /

pveum
acl
modify /
--
group
admins
--
role
Administra



4. Impos
le
2FA
pour
ces
comp
(voir
3.2.1)

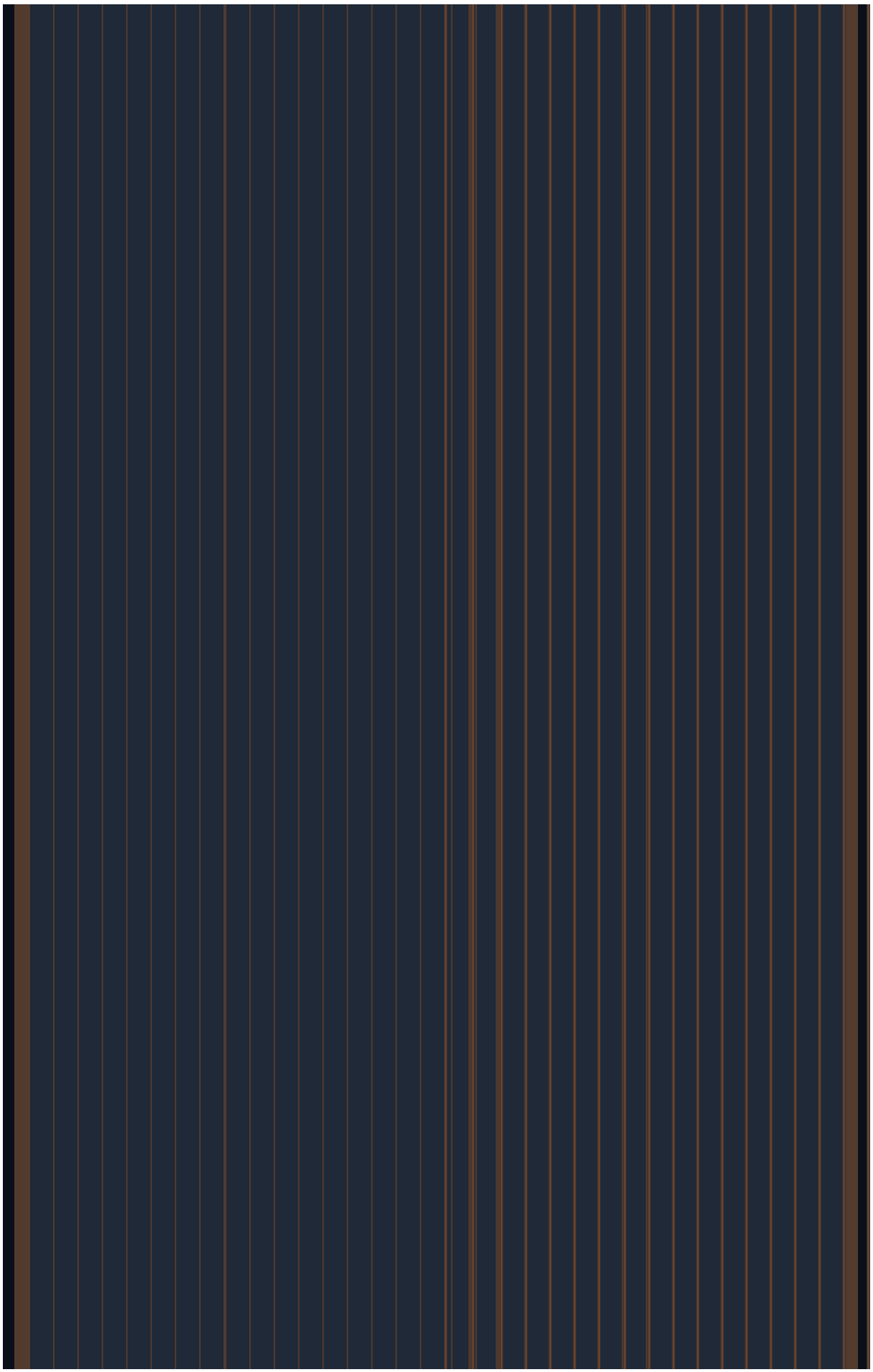
5. Docu
la
procé
d'util
de
root@

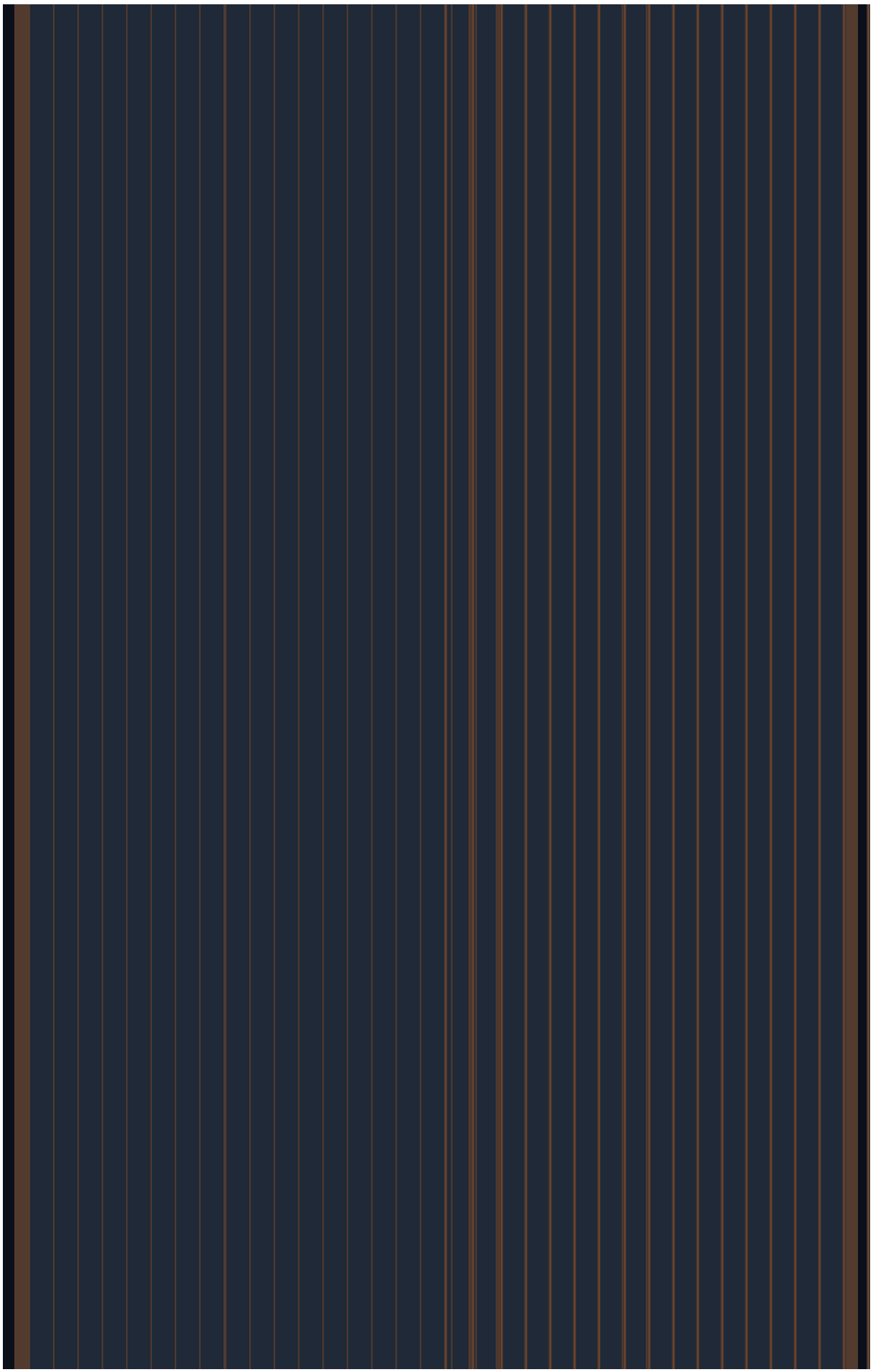


→ uniqu
pour
les
opéra
de
maint
systè

→ uniqu
via
SSH
avec
clé

→ jamai
via
l'inte
web
en
usag
quoti





3.3.2

PROFILE
APPLICA

APPLICA
PVE

CIS CON
V8

MITRE A

ISO
27001:2

PCI DSS

SCÉNAR
THREAT
MODEL

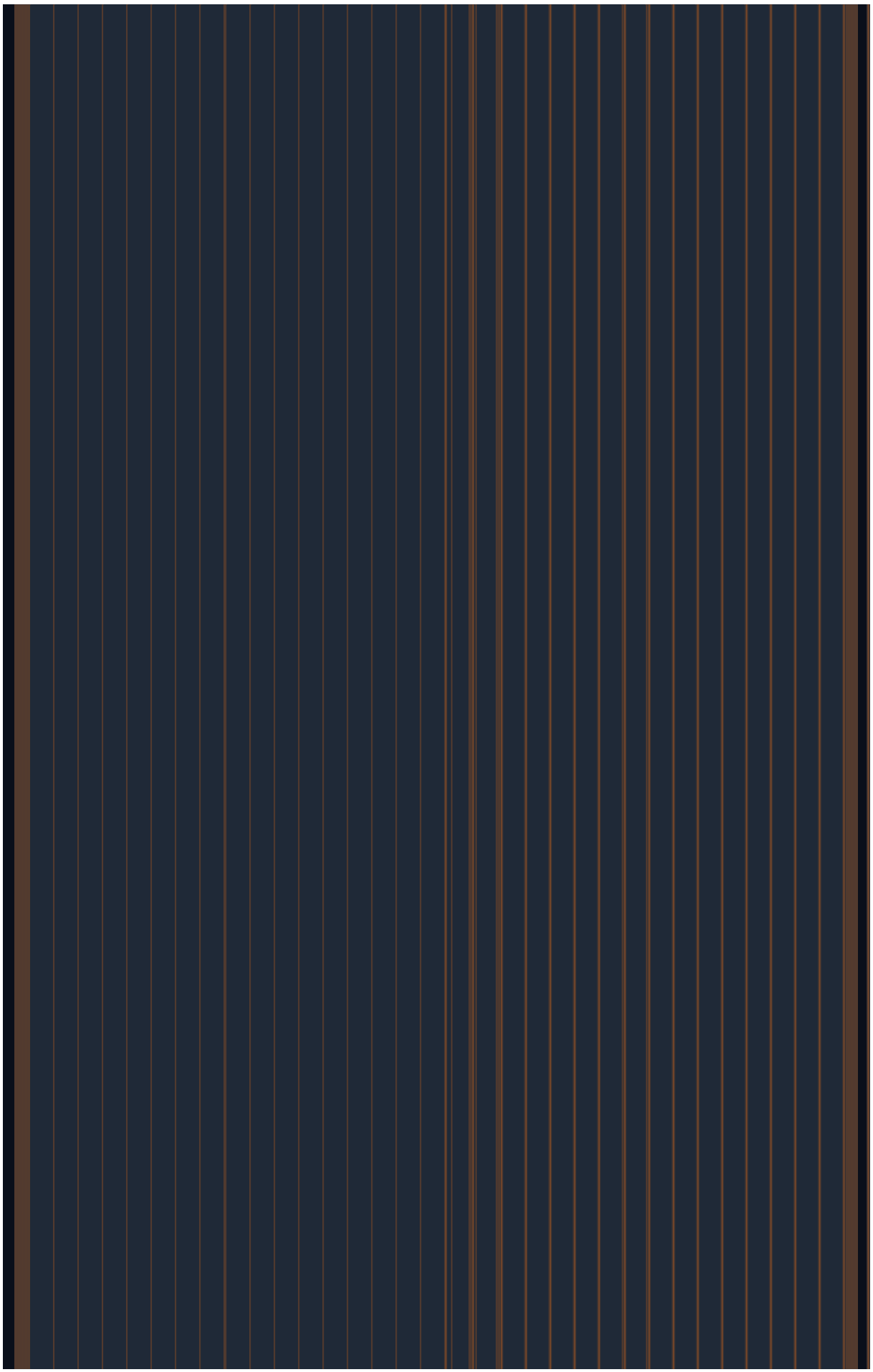
STATUT

DESCRIP

Descrip

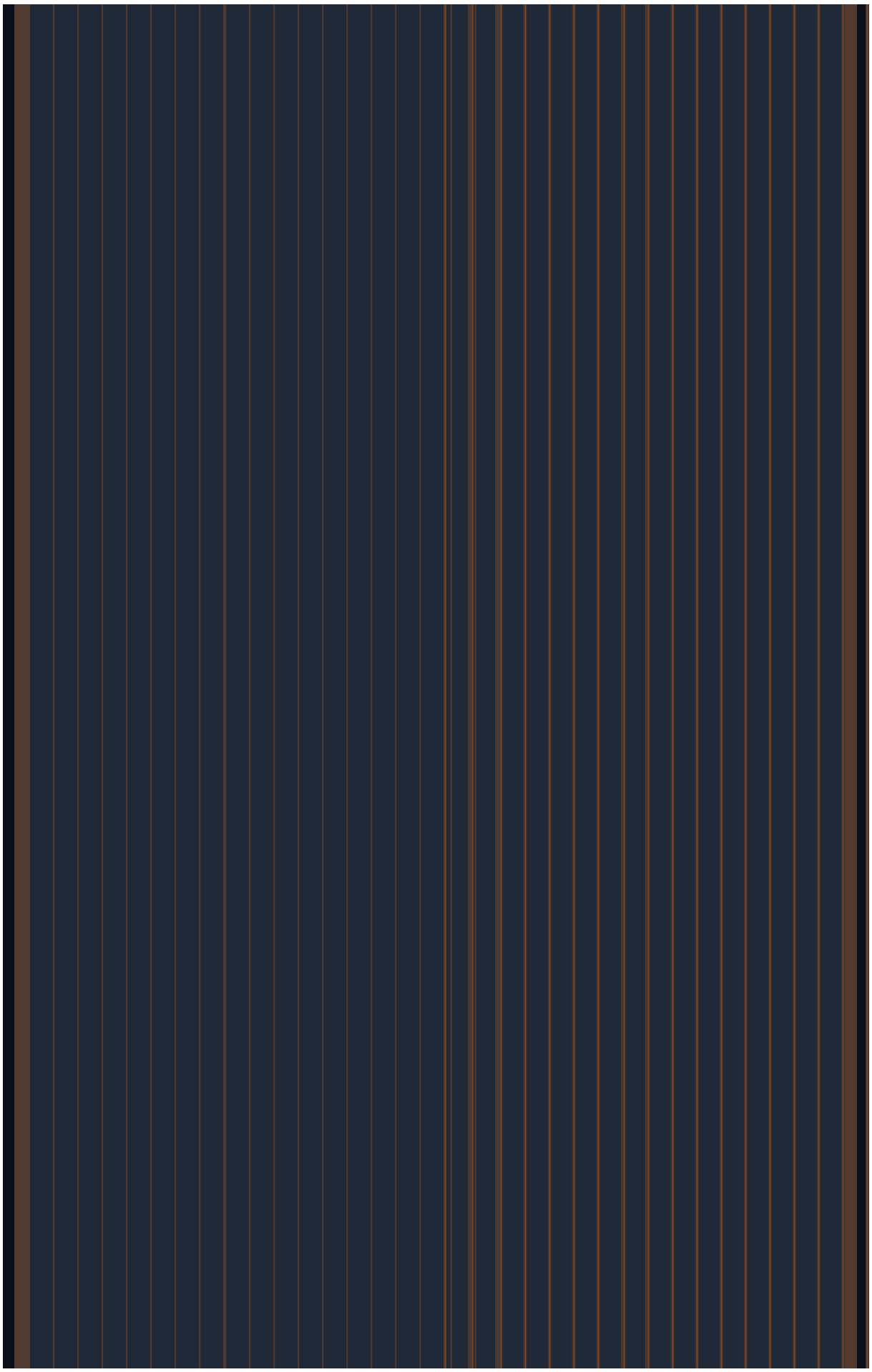
REMÉDIA

Reméd



Rôle "op VM" (sta stop con pas de crea dele

pveum
role
add
VMOpe
--
privs
"VM.Co
VM.Pov
VM.Mo
VM.Auc

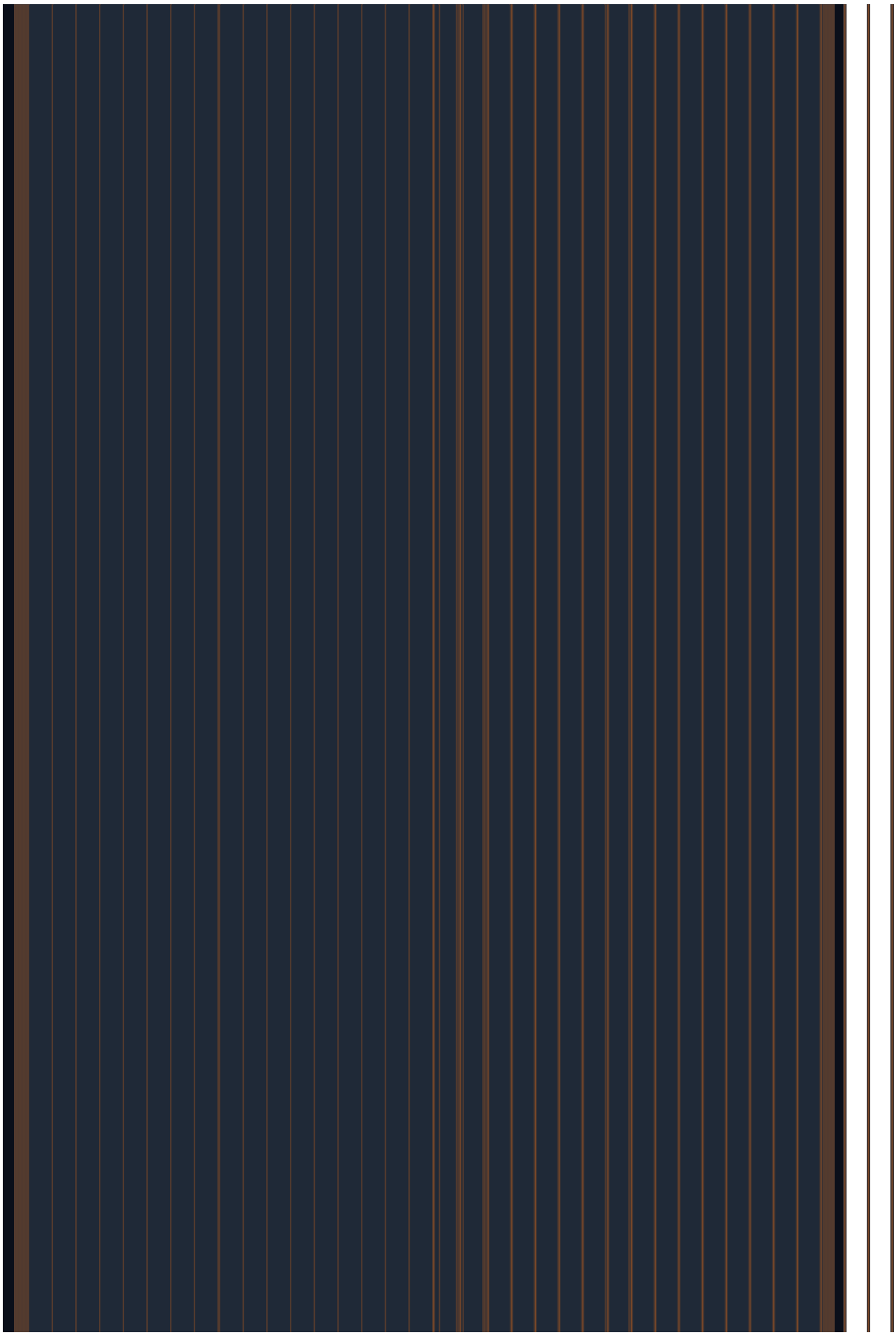


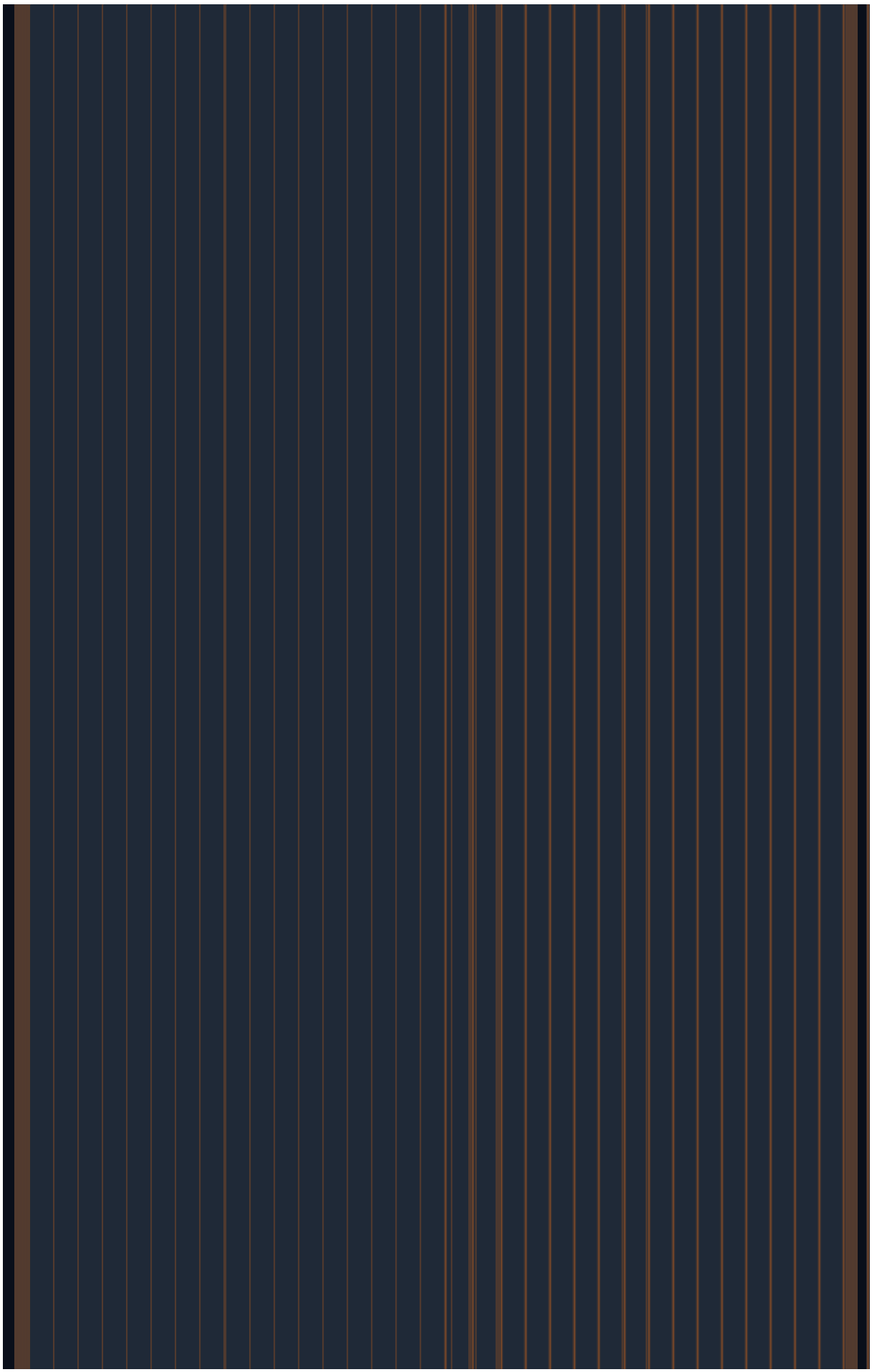
Rôle "ad bac (bac rest unic

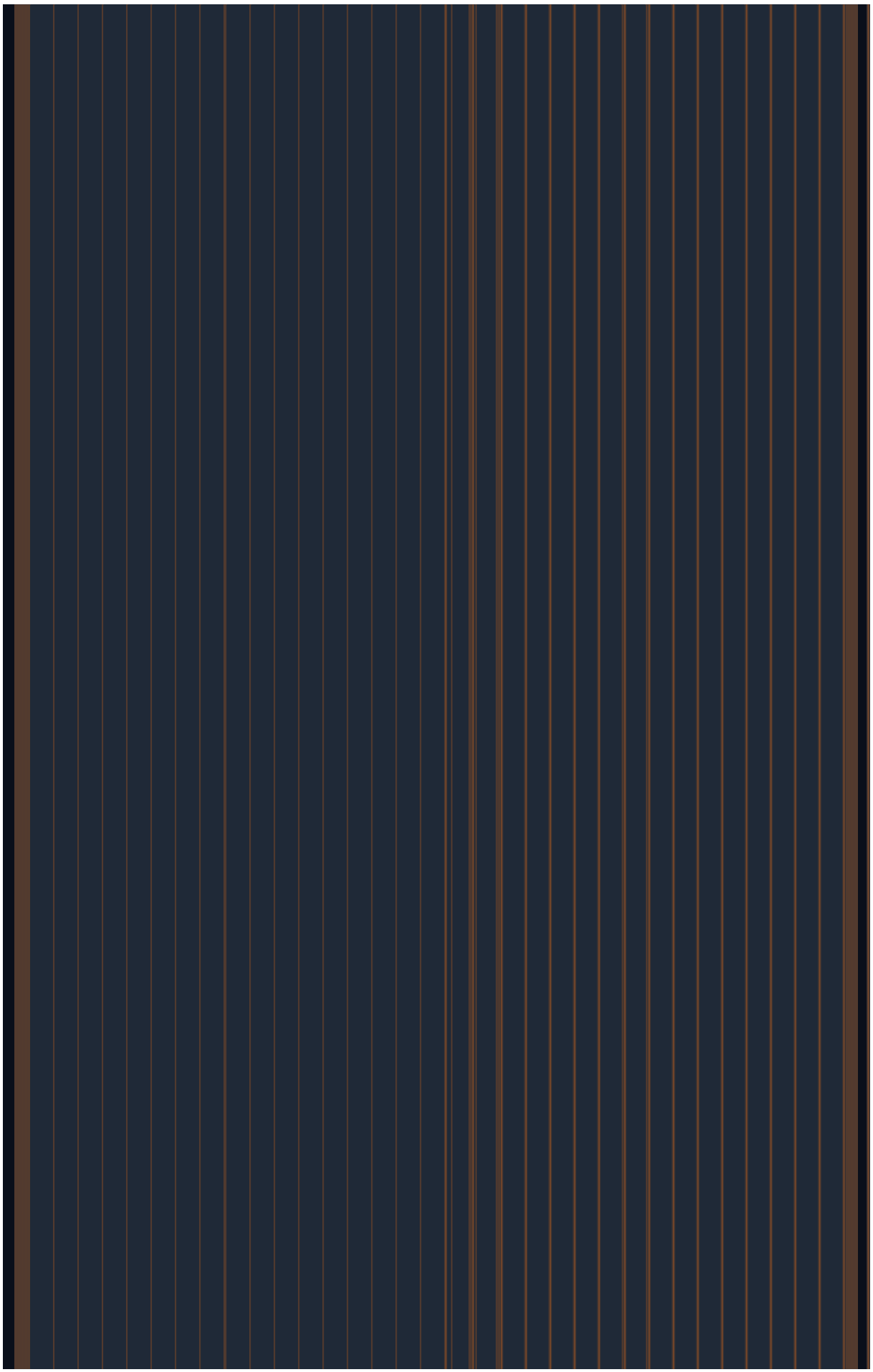
```
pveum
role
add
Backup
--
privs
"Datast
Datasto
VM.Bac
```

Rôle "lec rése (auc rése unic

```
pveum
role
add
NetAuc
--
privs
"SDN.A
Sys.Au
```

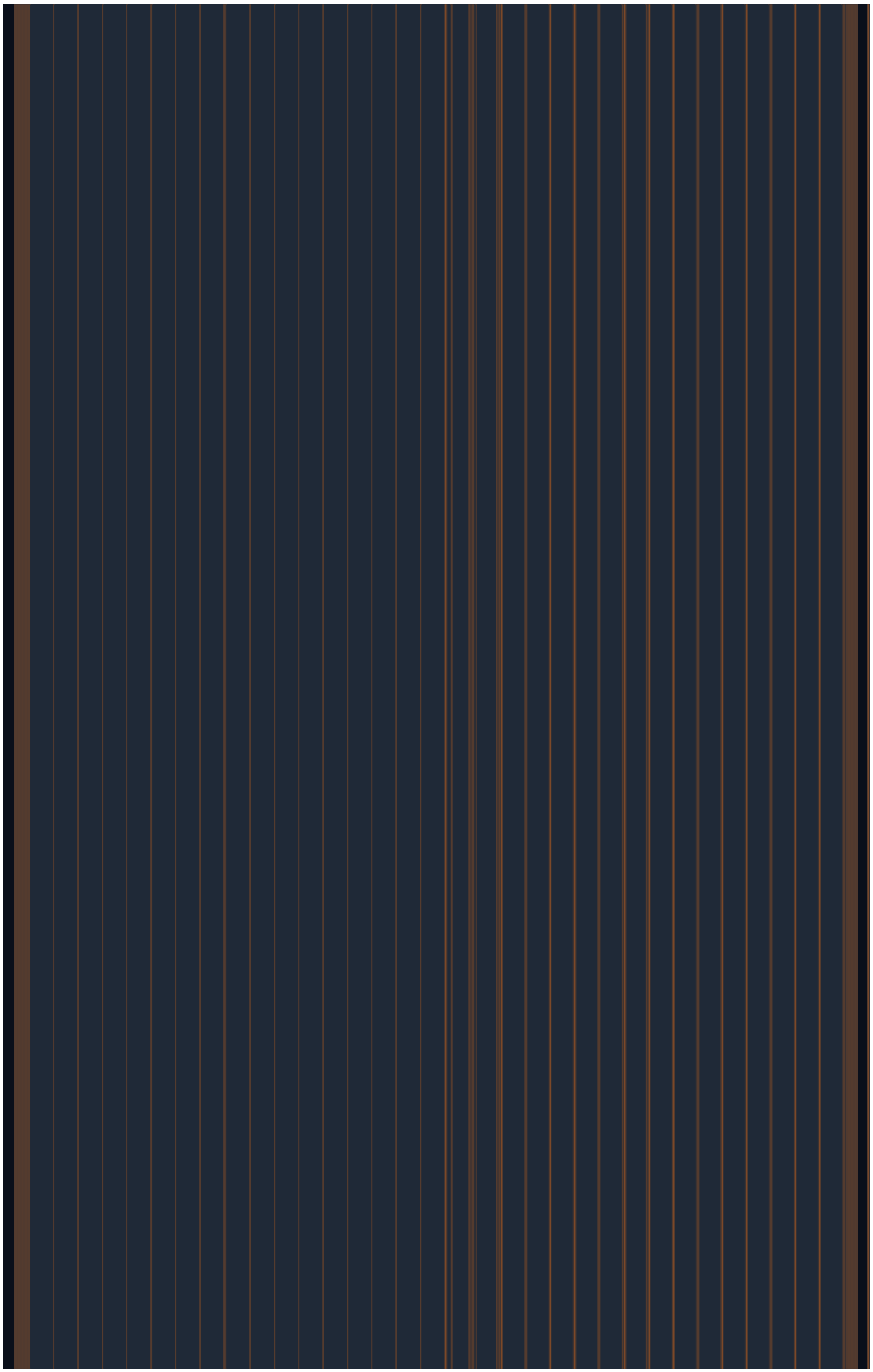


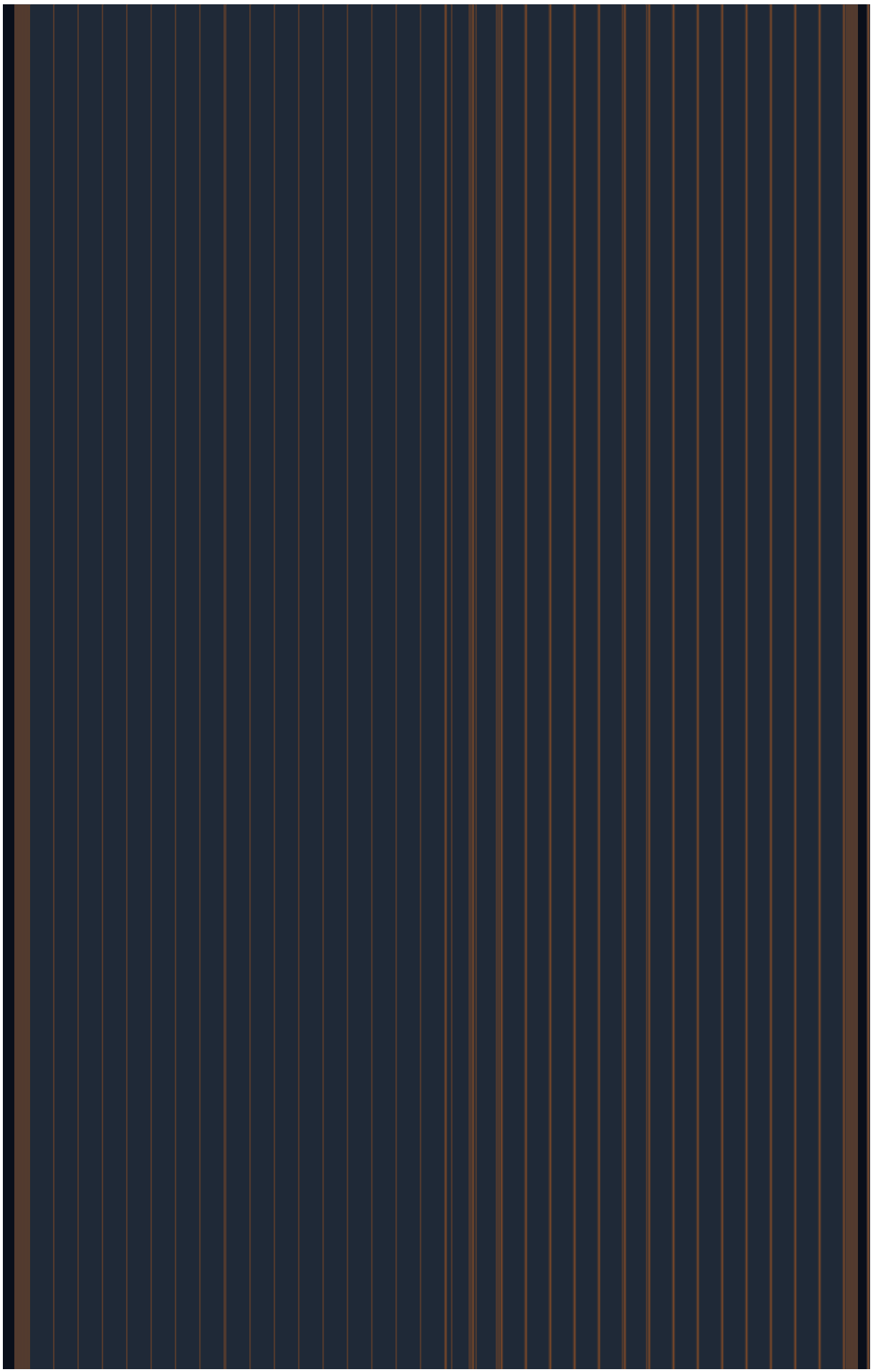




Aj
un
rea
LD

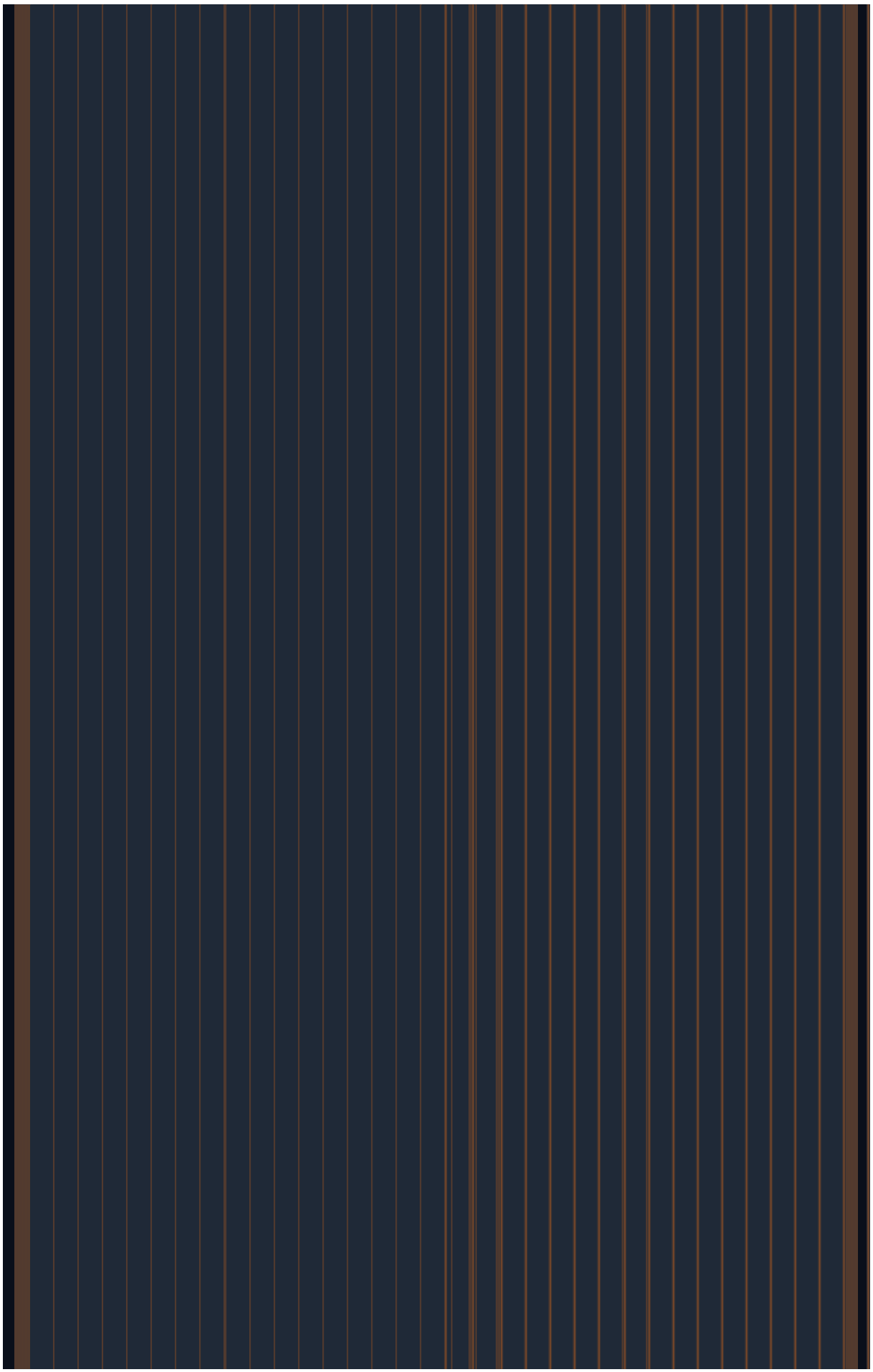
```
pveu
realm
add
mylo
--
type
ldap
\
--
base
dn
"ou=
\
--
bind
dn
"cn=
read
\
--
serv
ldap
\
--
port
636
\
--
secu
```





⚠️
TC
uti
LD
(p
63
ou
St

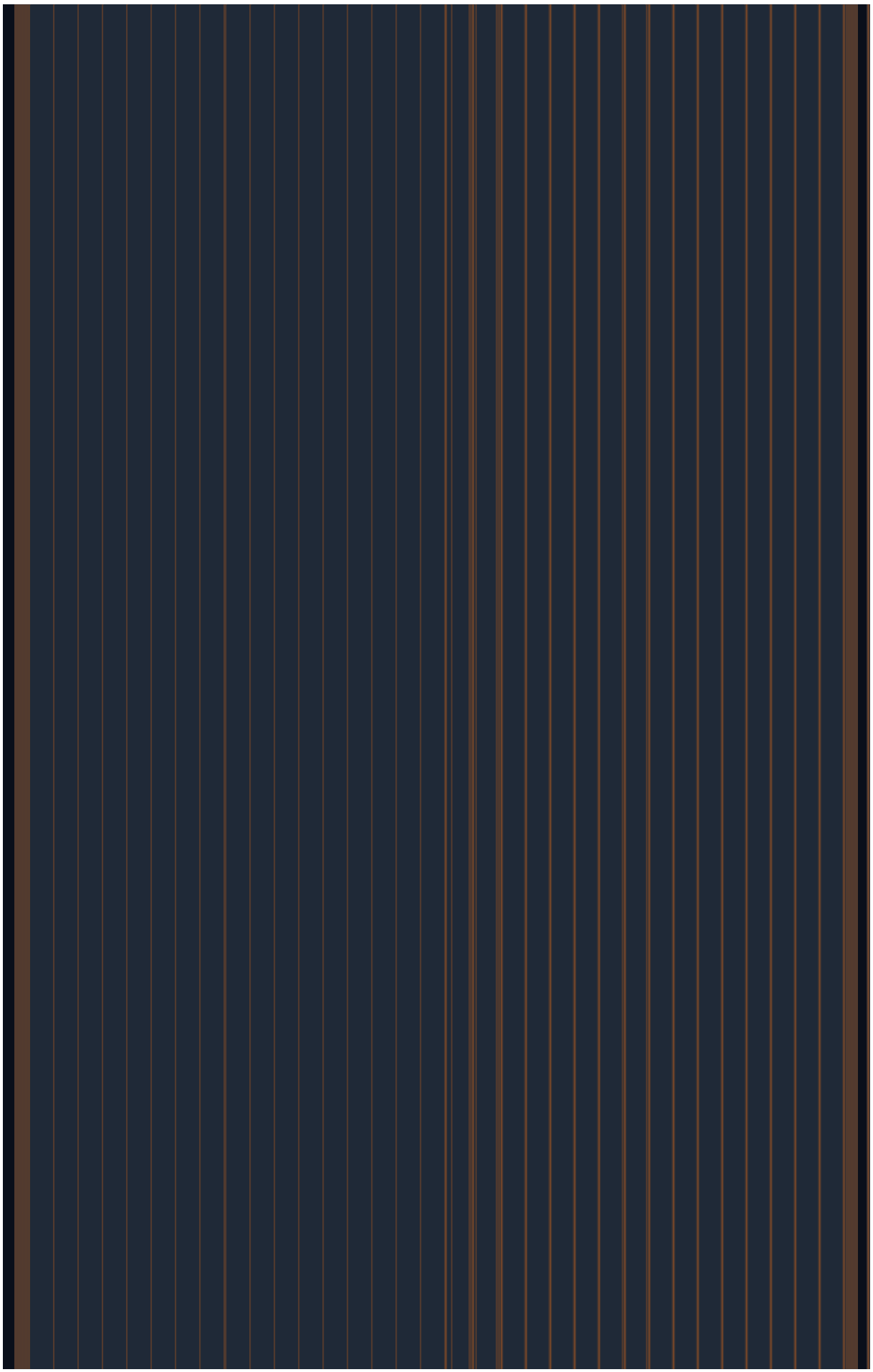
Ne
JA
uti
LD
en
cla
(p
38
→
cr
tra
en
cla

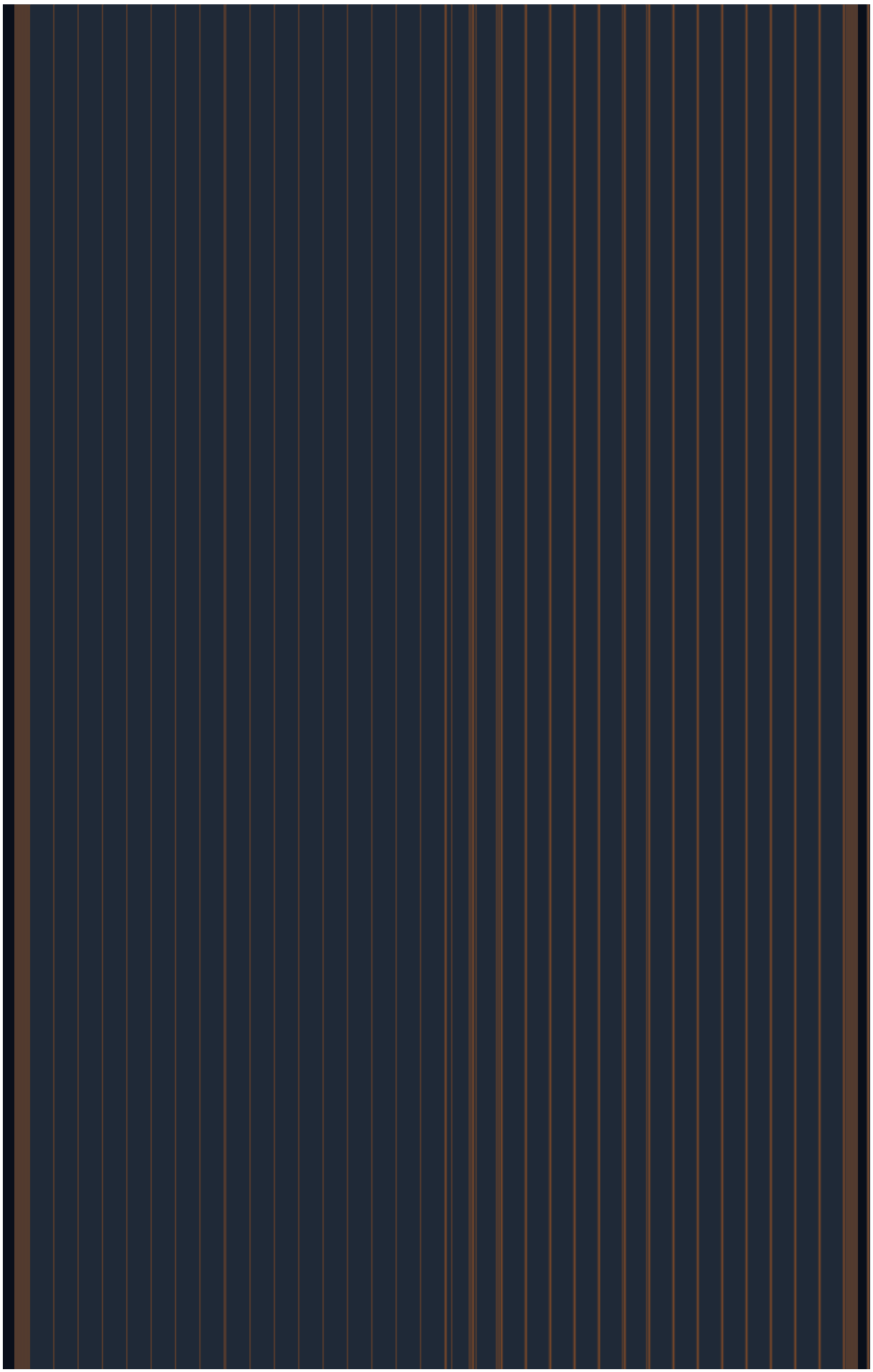


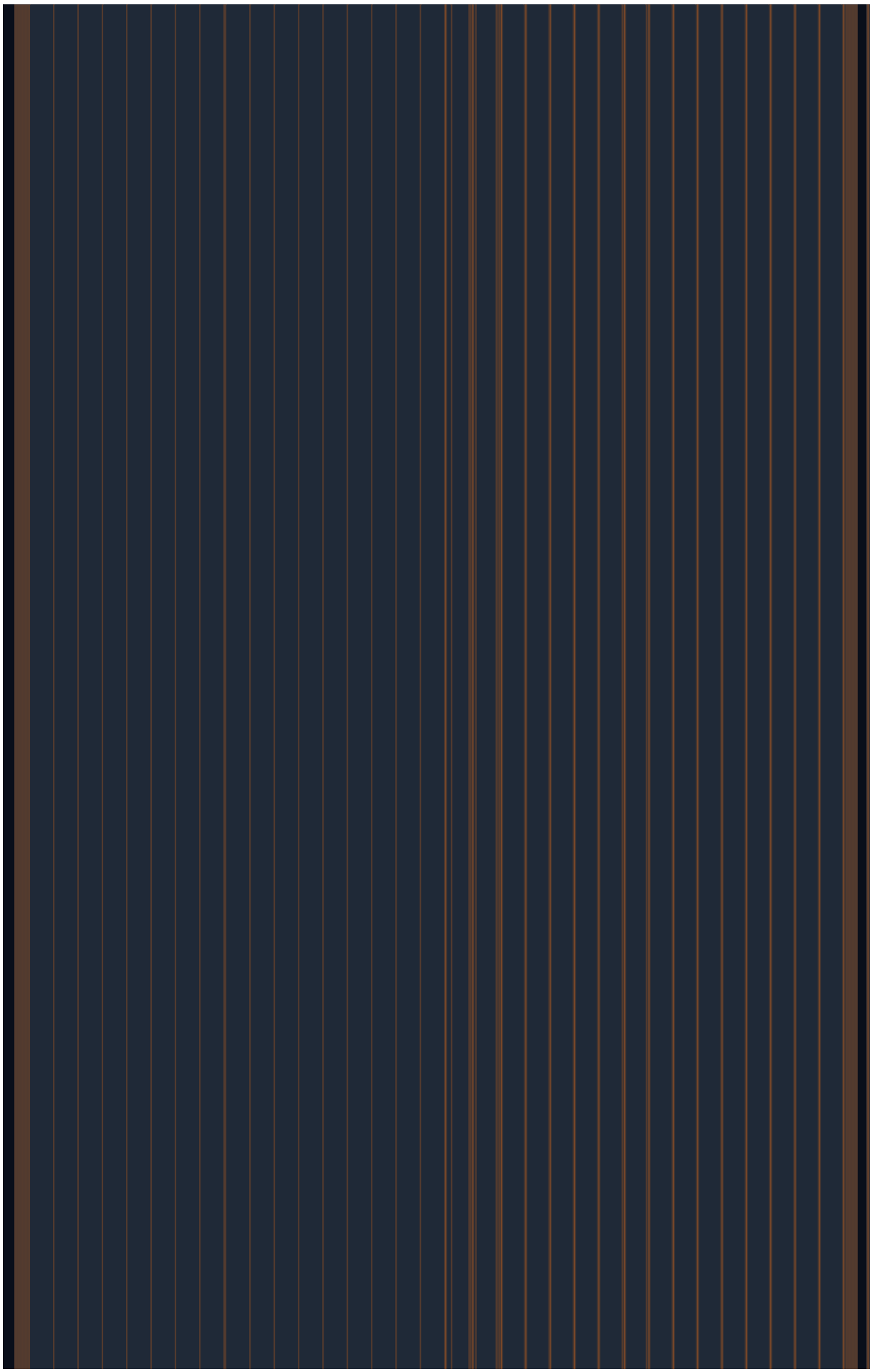
Sy
les
gr

pveu
realr
sync
mylo

```
**
**
--
```

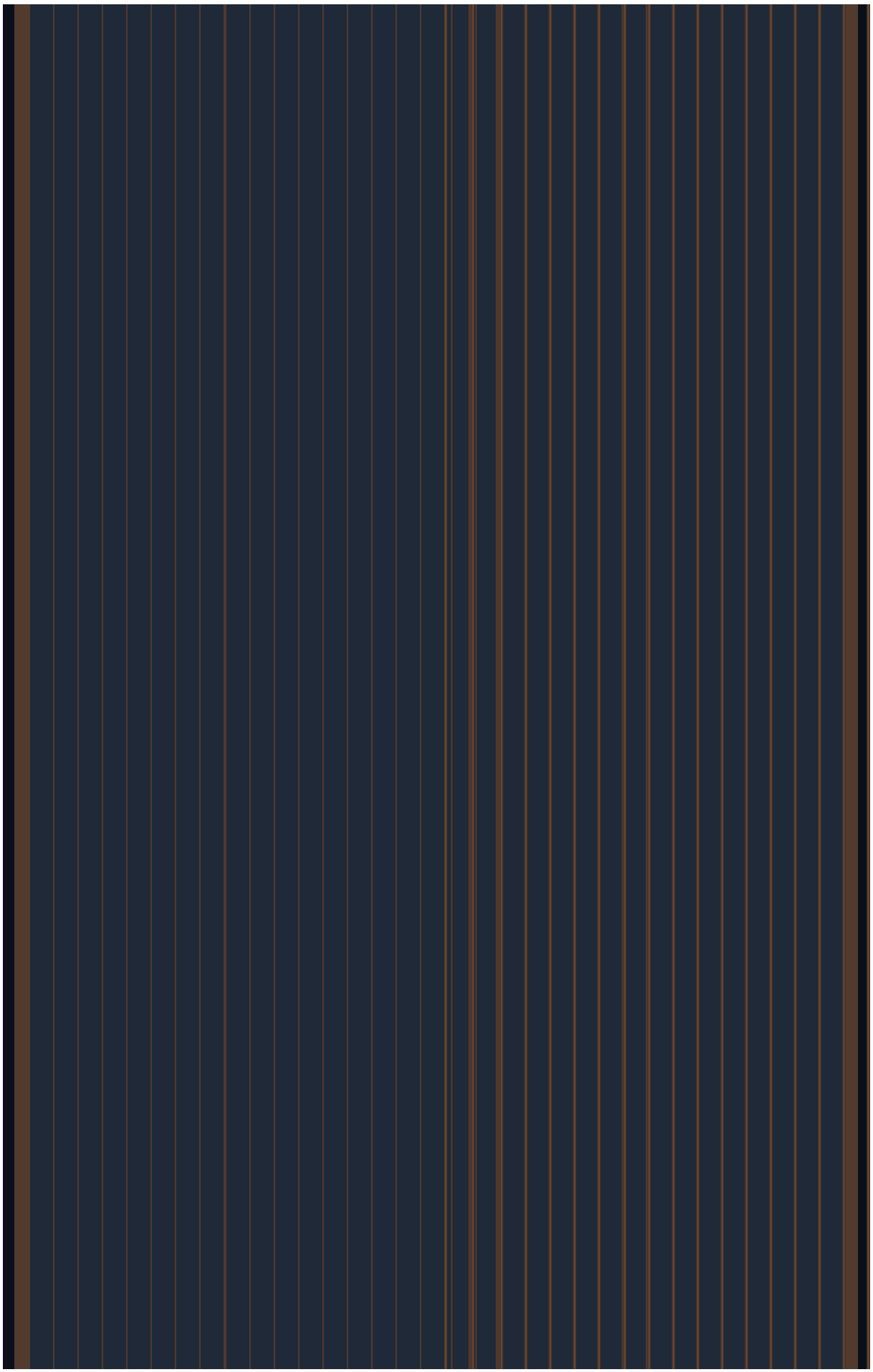


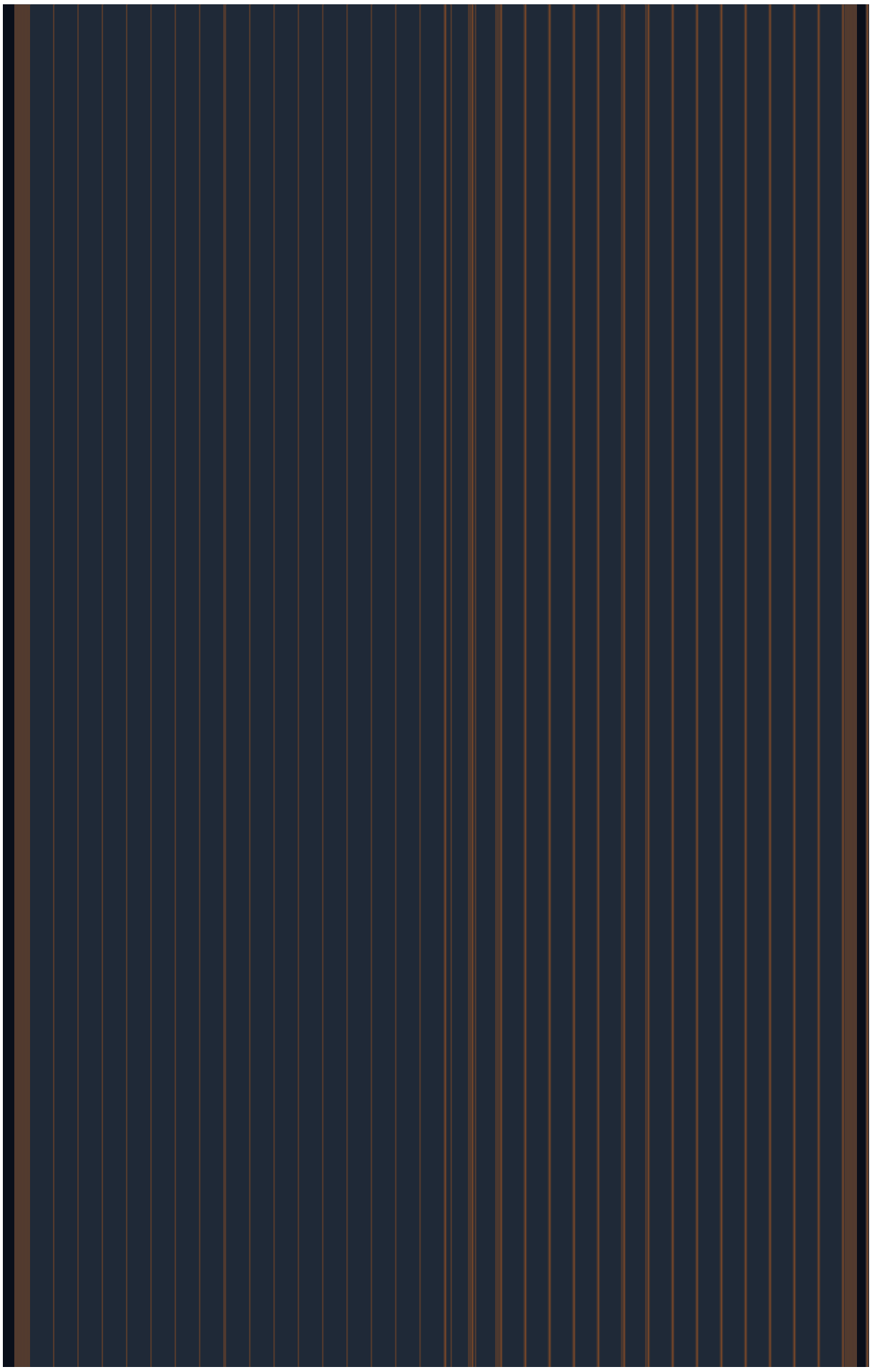


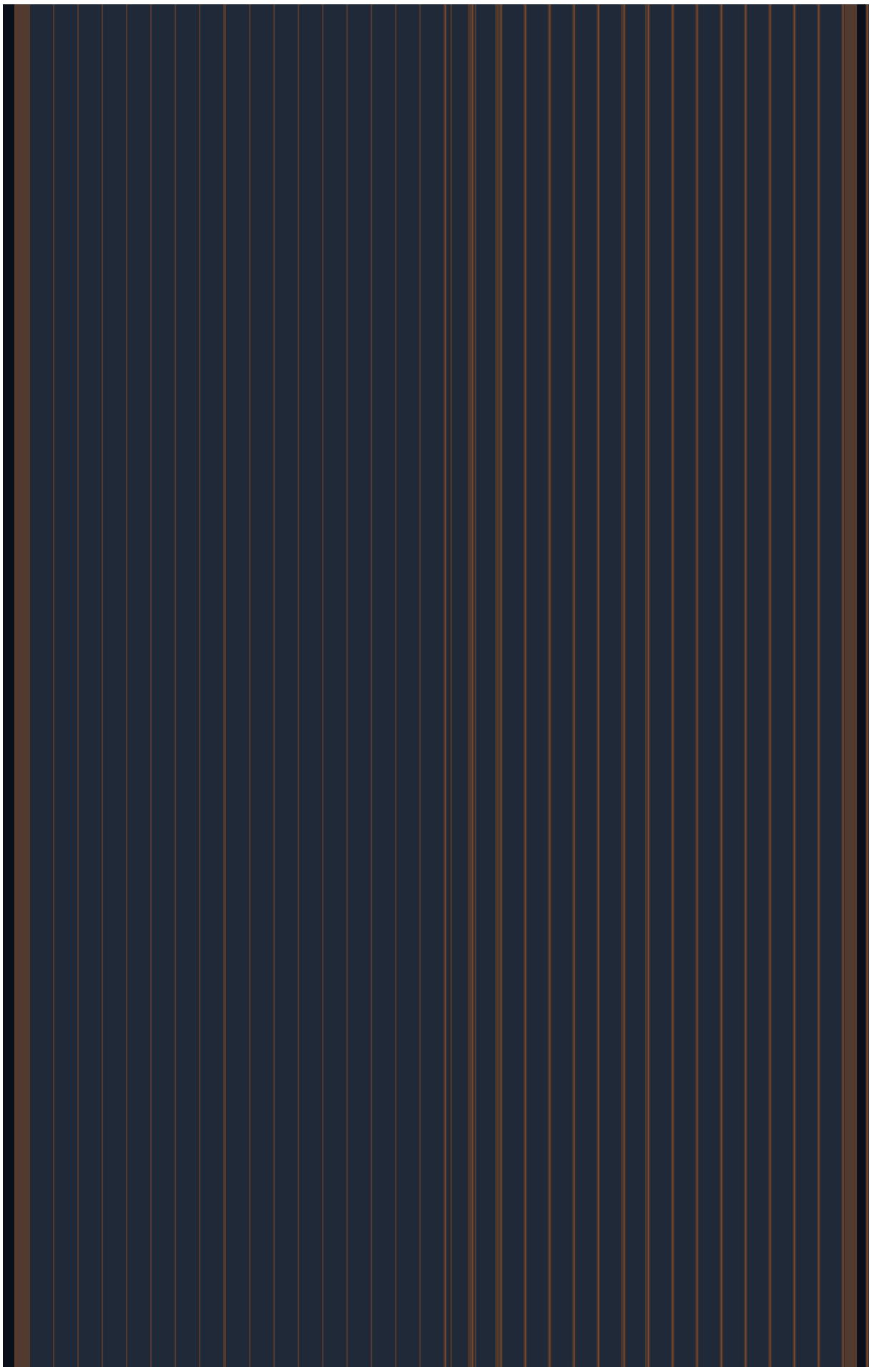


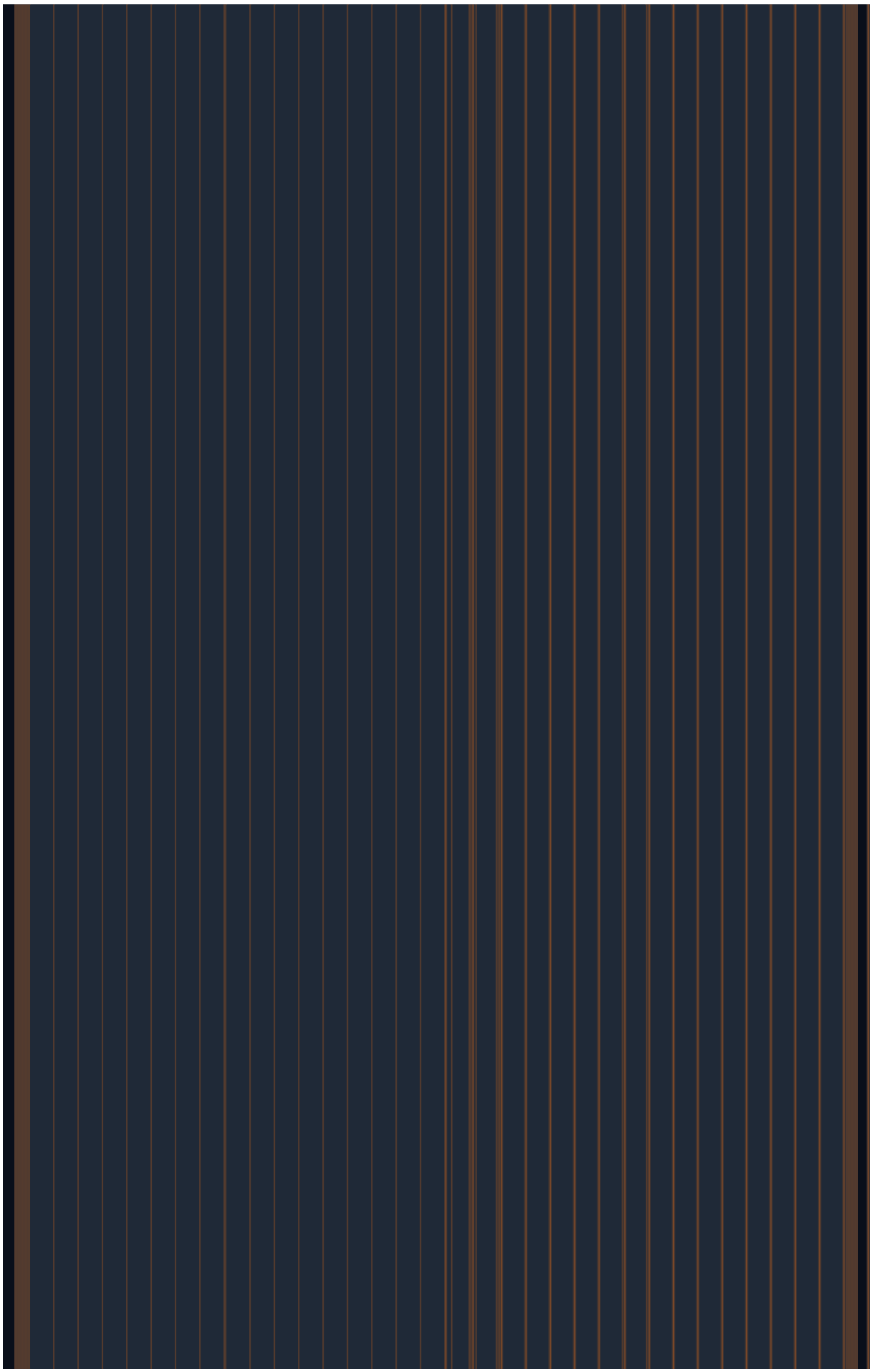
La
jai
ss
es
pr
il
su
de
l'a

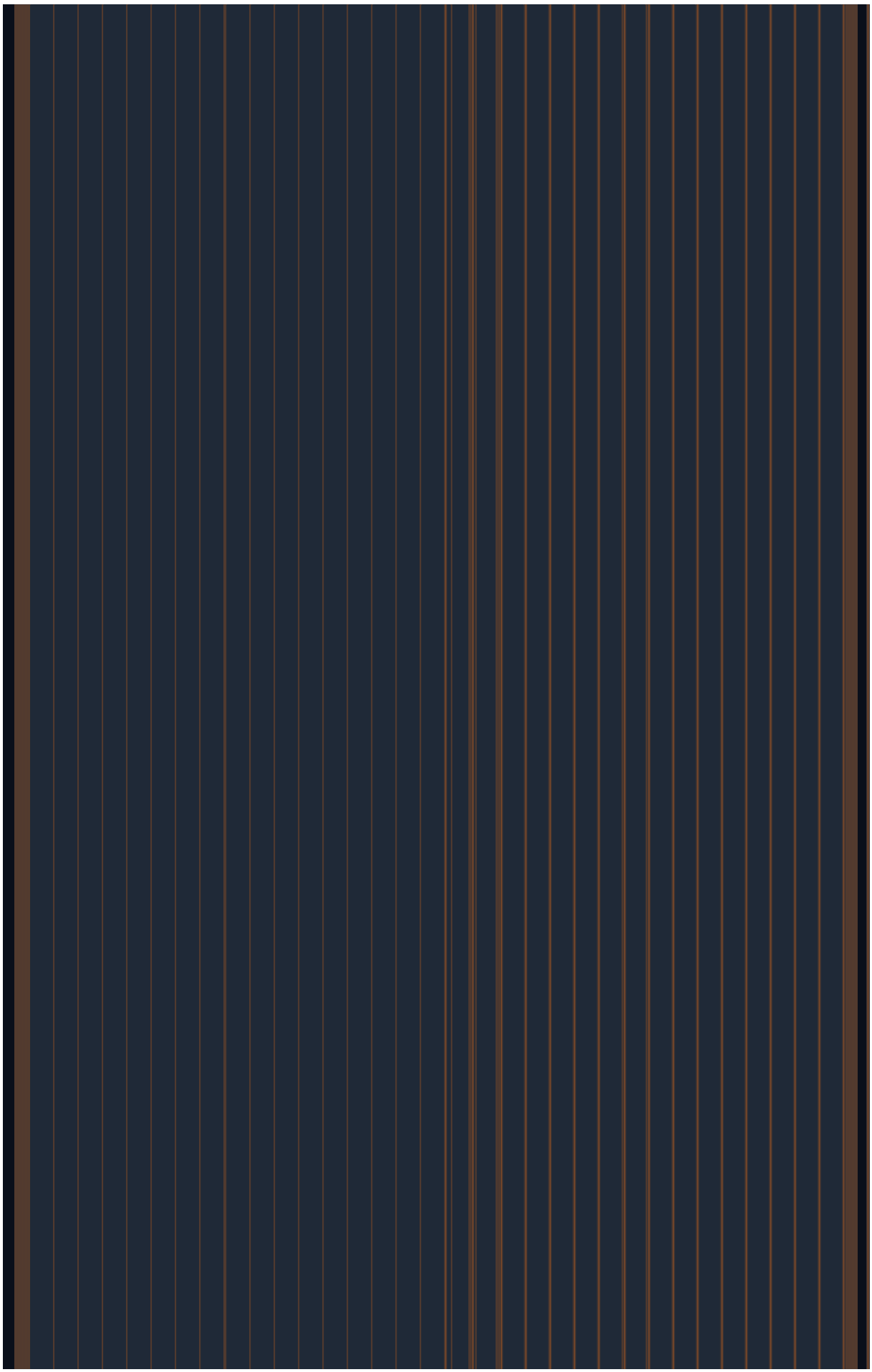
```
cat
>
/
etc/
fail2
jail.d
sshd
<<
'EOF
[ssh
enab
=
true
max
=
3
findt
=
2d
```

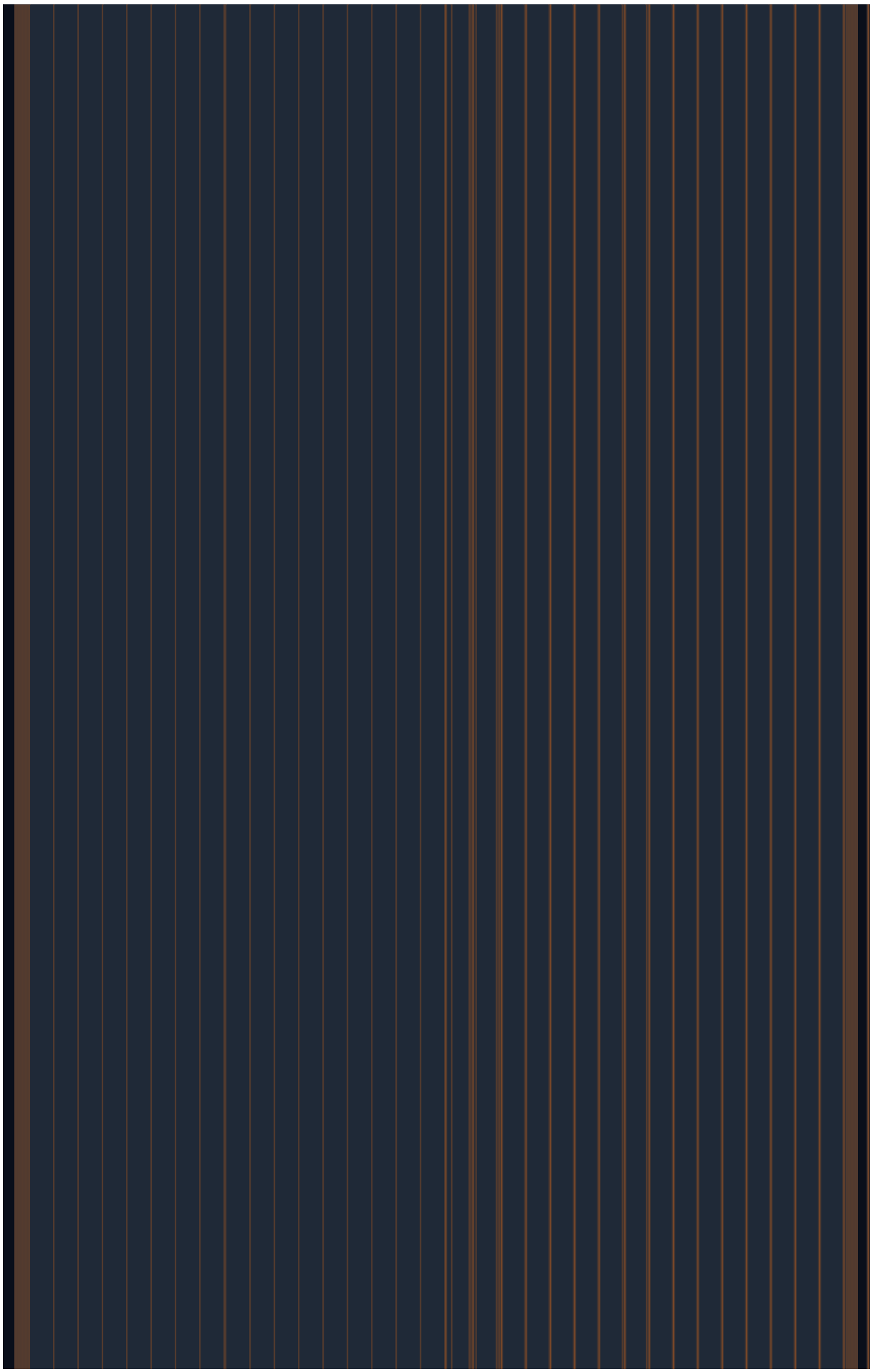


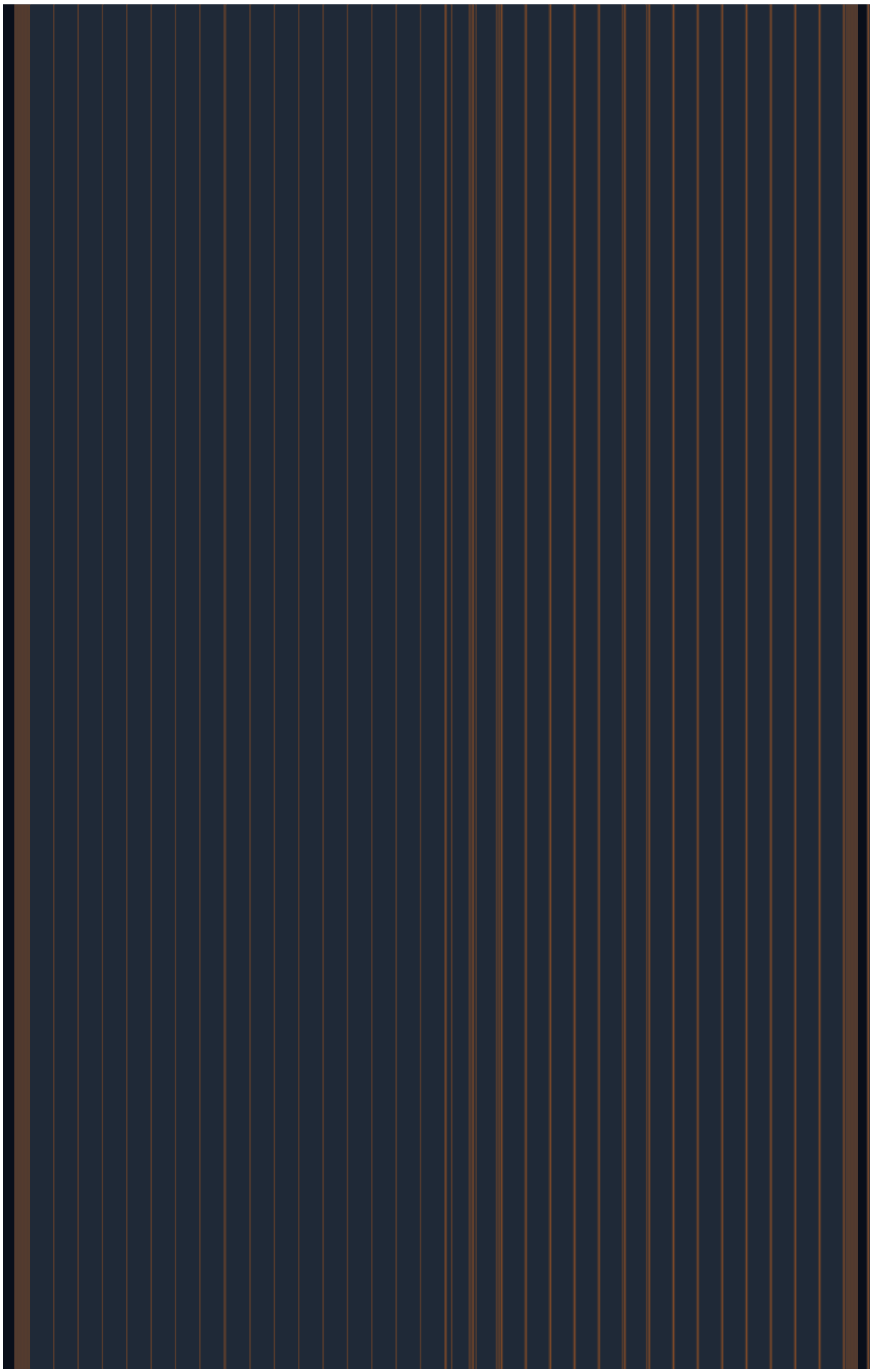


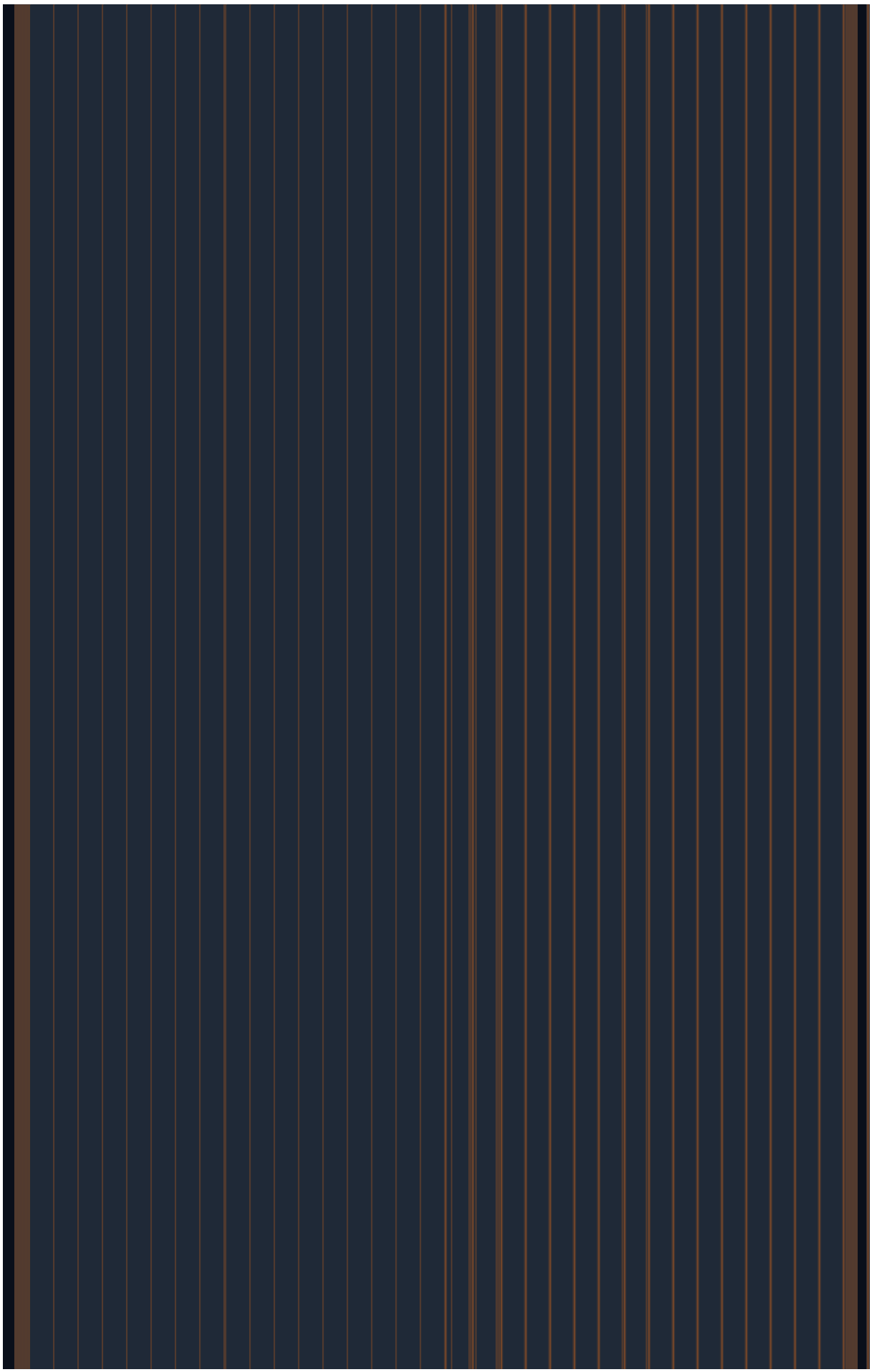


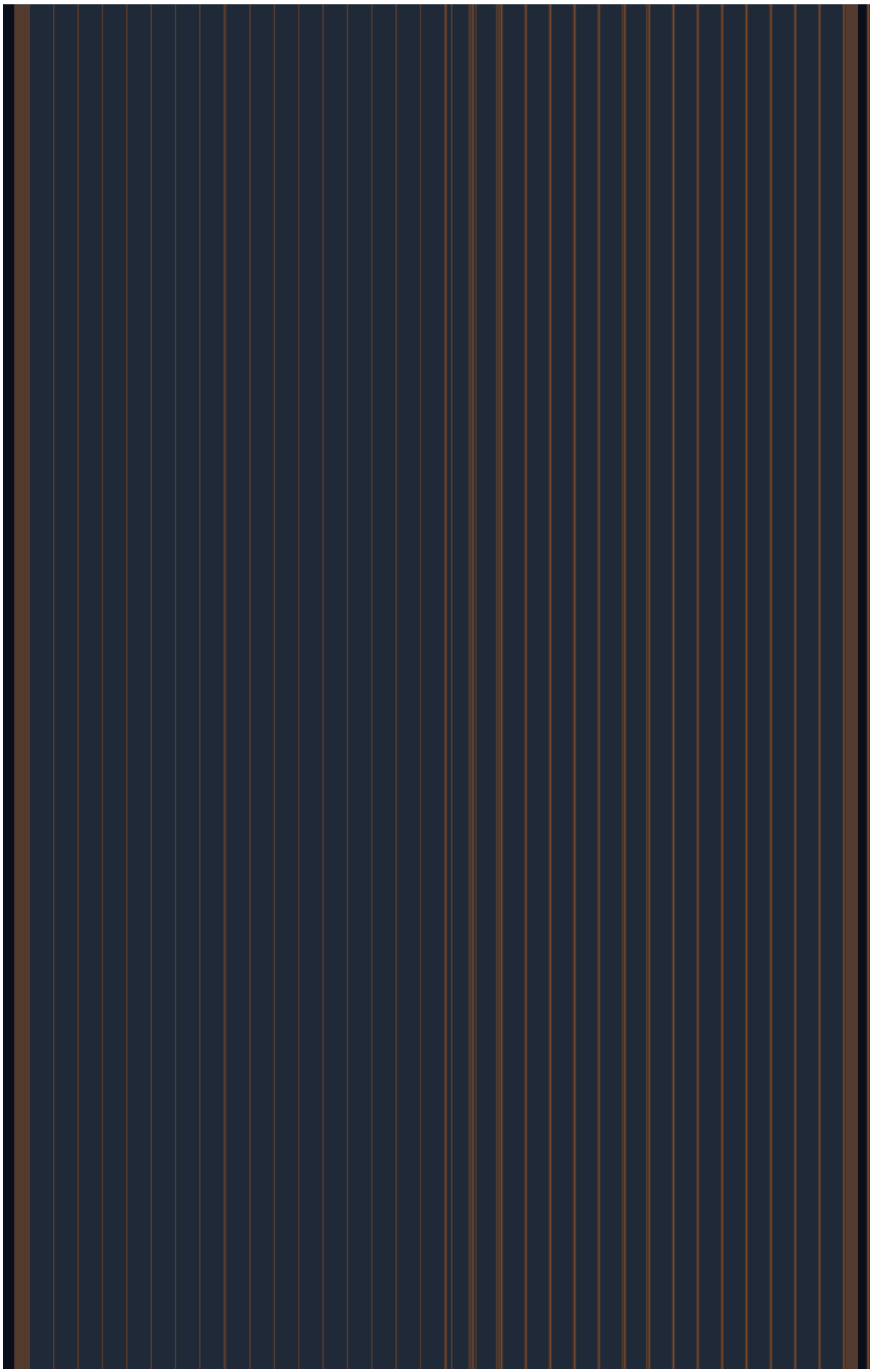












P
u
é
d
v
v
l'
v

(
n
d
p
p
v

fa
re
sy
jo
/
et
fa
fi
pr