

CHECKLIST QUOTIDIENNE - ADMINISTRATEUR RHEL 9.4

Objectif: Stabilité, Sécurité & Haute Disponibilité

I. SURVEILLANCE DES SYSTÈMES

Tâches (08h00 - 08h20)

1. État global des serveurs

Bash: **uptime && cat /proc/loadavg**: Charge système

2. Santé du stockage

Bash: **df -Th --exclude-type=tmpfs** : Espace disque

Bash: **vgs && pvs** : Santé LVM

3. Performance mémoire

Bash: **free -h && vmstat 2 5** : Utilisation RAM/Swap

II. SÉCURITÉ

Tâches (08h20 - 08h40)

1. Audit d'authentification

Bash: **grep -i "failed" /var/log/secure**

Bash: **lastb | head -20** : Tentatives échouées

2. Vérification SELinux

Bash: **sealert -a** : Alertes de sécurité

Bash: **sestatus** : État global

3. Contrôle des accès

Bash: **sudo ausearch -m USER_ACCT** : Audit des comptes

III. MISES À JOUR & CORRECTIFS

Tâches (08h40 - 09h00)

1. Gestion des paquets

Bash: **sudo dnf check-update** : Mises à jour en attente

Bash: **rpm -Va --nofiledigest** : Vérification d'intégrité

2. Kernel actif

Bash: **uname -r && rpm -q kernel** : Version du noyau

3. Nettoyage automatique

Bash: **sudo dnf autoremove** : Paquets obsolètes

IV. SAUVEGARDES

Tâches (09h00 - 09h15)

1. Vérification des sauvegardes

Bash: **tail -n 50 /var/log/backup.log | grep "SUCCESS"**

2. Test de restauration

Bash: **tar -tf /backups/app_\$(date +%F).tar.gz | head** : Sample

3. Intégrité RAID

Bash: **cat /proc/mdstat && smartctl -a /dev/sda**

V. PERFORMANCE

Tâches (09h15 - 09h30)

1. Diagnostic I/O

Bash: **iostat -dxm 2 3** : Performance disque

2. Processus critiques

Bash: **pidstat -d -u -h 1 5** : Charge CPU/mémoire

3. Optimisation réseau

Bash: **nethogs -d 5 -t** : Bandwidth par processus

VI. JOURNAUX (LOGS)

Tâches (09h30 - 09h45)

1. Erreurs système

Bash: **journalctl -p 3 -xb --since "today"** : Critical errors

2. Surveillance centralisée

Bash: **grep -r "ERROR" /var/log/rsyslog/ # Si ELK/Splunk**

3. Rotation des logs

Bash: **ls -lh /var/log/*.log** : Taille des fichiers

VII. AUTOMATISATION

Tâches (09h45 - 10h00)

1. Vérification cron/Ansible

Bash: **crontab -l | grep -v "^#" : Tâches planifiées**

Bash: **ansible-playbook --check site.yml : Dry-run**

2. Maintenance des scripts

Bash: **git -C /scripts/ pull** : Mise à jour des outils

VIII. DOCUMENTATION & CONFORMITÉ

Tâches (10h00 - 10h15)

1. Rapport quotidien

- Incidents traités
- Changements effectués

2. Audit de conformité

Bash: **oscap xccdf eval --profile stig-rhel9
/usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml**

IX. BONNES PRATIQUES & RÉFÉRENCES

Workflow Recommandé :

mermaid

graph LR

A[Surveillance] --> B[Sécurité]

B --> C[Mises à jour]

C --> D[Sauvegardes]

D --> E[Documentation]

X. OUTILS ESSENTIELS :

Catégorie	Outils
Monitoring	Nagios, Prometheus, Grafana
Sécurité	OpenSCAP, AIDE, SELinux
Backup	Bacula, Rclone, Duplicity

Temps Estimé : 1h30/jour



Personnaliser selon :

- Politiques de l'entreprise
- Criticité des services
- Environnements (Cloud/On-prem)