04 - Maintenance

1) Diagnostic et dépannage

Commandes de diagnostic Asterisk

Commande	Usage
asterisk -rx "pjsip show contacts"	État des enregistrements : Avail/NonQual/Unreachable + RTT
asterisk -rx "pjsip show endpoints"	État global des endpoints configurés
asterisk -rx "pjsip show endpoint 1000"	Détail d'un endpoint spécifique
asterisk -rx "core show channels"	Appels actifs en cours
asterisk -rx "dialplan show interne"	Afficher le contexte du dial plan
asterisk -rx "module reload res_pjsip.so"	Recharger PJSIP à chaud
asterisk -rx "dialplan reload"	Recharger extensions.conf
asterisk -rvvvv	Console interactive avec niveau de verbosité 4

Activation des logs SIP et RTP

Depuis la console Asterisk (asterisk -rvvvv) :

```
pjsip set logger on    ; Active les logs SIP complets (INVITE, OPTIONS, 200 OK...)
rtp set debug on       ; Active les logs RTP (flux audio)
pjsip set logger off   ; Désactive (important en prod, très verbeux)
rtp set debug off
```

Vérification réseau

```
# Vérifier qu'Asterisk écoute sur le bon port
sudo ss -ulnp | grep 5160

# Tester la connectivité vers les téléphones
ping -c 4 192.168.10.67   # Yealink T41P
ping -c 4 192.168.10.66   # Yealink T31P

# Vérifier les logs Asterisk
sudo tail -f /var/log/asterisk/full
sudo tail -f /var/log/asterisk/messages
```

Problème fréquent

Symptôme	Cause probable	Solution
"Provisoirement indisponible"	Contact en état NonQual — téléphone non qualifié	Ajouter qualify_frequency=30 dans la section AOR. Vérifier DHCP/IP du téléphone.
Pas de son (audio absent)	external_signaling_address manquant ? Asterisk annonce 127.0.0.1	Ajouter external_signaling_address et external_media_address dans le transport. Redémarrer Asterisk.
Audio unidirectionnel	direct_media=yes ? bypass RTP échoue	Ajouter direct_media=no dans chaque endpoint.
Appel en absence sans sonnerie	DND activé sur le téléphone destinataire	Désactiver DND dans Features ? Forward & DND ? Etat NPD ? "de".
Téléphone non enregistré (croix rouge)	Port SIP incorrect, mauvaise IP serveur, ou mot de passe erroné	Vérifier la config du téléphone : IP Asterisk, port 5160, username/password.
Contact Unavail après redémarrage VM	Téléphone garde l'ancienne IP du serveur en cache	Redémarrer le téléphone. Vérifier que la réservation DHCP d'Asterisk est correcte.
Module reload sans effet sur le transport	Le transport PJSIP ne se recharge pas à chaud	sudo systemctl restart asterisk
Appels impossibles, pas de connectivité VM	VM attachée au mauvais bridge Proxmox	Changer vmbr0 ? vmbr1 dans les paramètres réseau de la VM Proxmox.

2) Sécurité de l'infrastructure VoIP

Menaces courantes

Menace	Description	Impact
Scan SIP (SIPVicious)	Robots qui scannent le port 5060 à la recherche de serveurs Asterisk	Tentatives d'enregistrement non autorisé
Brute force	Attaque par dictionnaire sur les credentials SIP	Accès non autorisé, frais téléphoniques
Toll fraud	Utilisation du serveur pour passer des appels internationaux payants	Factures exorbitantes
Écoute RTP	Capture des flux audio RTP sur le réseau	Violation de la confidentialité
Déni de service (DoS)	Flood de paquets SIP pour saturer le serveur	Interruption de service

Mesures de sécurité recommandées

- (5060 → 5160 ou autre) pour réduire les scans automatisés.Changer le port SIP par défaut
- Minimum 16 caractères, mélange de lettres, chiffres et symboles.Mots de passe complexes
- Bloquer automatiquement les IPs effectuant trop de tentatives d'authentification.Fail2ban
- Utiliser les listes de contrôle d'accès du Cisco ISR pour n'autoriser le trafic SIP qu'en provenance du VLAN 20.ACL réseau
- Isoler les téléphones du reste du réseau — déjà en place dans ce projet.VLAN dédié
- Chiffrer le flux audio RTP avec SRTP pour les environnements sensibles.SRTP
- Modules Asterisk non utilisés (DAHDI, chan_skinny…) doivent être désactivés.Désactiver les services inutiles

Installation de Fail2ban pour Asterisk

Fail2ban est un outil qui surveille les fichiers de logs d'Asterisk et bloque automatiquement les adresses IP qui font trop de tentatives d'authentification SIP échouées (brute force sur les mots de passe des postes).

```
sudo apt install -y fail2ban

# Créer /etc/fail2ban/jail.local
[asterisk]
enabled = true
port = 5160
filter = asterisk
logpath = /var/log/asterisk/full
maxretry = 5
bantime = 3600

sudo systemctl restart fail2ban
sudo fail2ban-client status asterisk
```

3) Supervision avec Zabbix

Éléments à superviser

Élément	Méthode	Seuil d'alerte
Service Asterisk	Check process "asterisk"	Alerte si arrêté > 1 min
Nombre d'appels actifs	AMI ou script	Alerte si > seuil configuré
Enregistrements SIP	Script pjsip show contacts	Alerte si endpoint Unreachable
Connectivité téléphones	ICMP ping	Alerte si téléphone injoignable
Logs d'erreurs	Log monitoring	Alerte sur ERROR/WARNING répétés

Revision #3
Created 19 March 2026 10:26:20 by Mathéo
Updated 1 June 2026 08:55:13 by Mathéo