STAS EUPCloud

Spécifications Techniques d'Accès au Service

1. État du service

Une page d'information en temps réel sur l'état opérationnel de la plateforme est disponible ici :
https://status.eupcloud.io

2. Portail Opérationnel

Un portail opérationnel (boite à outils) est accessible à l'adresse:
https://ops.e4sp.cloud

Et met à disposition un ensemble d'outils de diagnostic et d'exploitation, notamment :

Outil	Description
Speedtest	Test autonome (basé sur librespeed.org) permettant de mesurer la bande passante entre un site externe et le datacenter EUPCloud afin de valider la compatibilité VoIP.
Network QT	Suite de tests autonome permettant de valider l'installation réseau sur site client.
PVS ACL	Configuration de la liste blanche d'accès pour PVS Legacy.
Out PSTN GW	Configuration des préfixes de numérotation sortants pour les entreprises (scénarios multi interconnexions-).
VoIP Monitor	Recherche de traces d'appels SIP par date et numéros appelant/appelé ; téléchargement des fichiers PCAP (SIP uniquement).
Data Dashboard	Affichage des statistiques d'appels et indicateurs d'activité basés sur Prometheus.
PVS Log	Recherche et visualisation des logs Traefik relatifs aux requêtes PVS.
Audit	Audit des licences par entreprise ou fournisseur de services, exportable en XLS.

4.Réseau et Protocoles

4.1 Exigences Firewall (traffic sortant de l'equipement CPE –egress-)

Ports	Protocol	Vers IPv4	Vers IPv6	Comment
*	TCP/UDP	5.144.142.32/27	2a00:e00:0:8::/64	EUPCloud DATA
*	TCP/UDP	195.200.102.96/27	2a00:e00:0:9::/64	EUPCloud VOIP
19302	TCP	*	*	WebRTC STUN/TURN
443	TCP	*	*	Coligo Collab service
5223, 2197	TCP	*	*	Apple Push Service
5235, 5222, 5228, 853	TCP	*	*	Google Firebase push

4.2 Sous--réseaux Publics

- DATA : **5.144.142.32/27** – **2a00:e00:0:8::/64**
- VOICE : **195.200.102.96/27** – **2a00:e00:0:9::/64**

4.3 Allocation IP/Ports

DATA NETWORK

Source / Destination IP(s)	FQDN	Protocol	Ports	Comment
5.144.142.36 (GS) / 5.144.142.37 (PAR3) 2a00:e00:0:8::36/37	*.eupcloud.io inservice.webapps.eupcloud.io mtx.eupchat.online	HTTP/HTTPS	80 / 443	Wildcard for DATA services (mytelephony, myistra, cdr...). mtx.eupchat.online only for group chat. DNSbased load

				balancing. HTTP 80 redirected to HTTPS 443.-based load balancing.
5.144.142.38 (GS) / 5.144.142.39 (PAR3) 2a00:e00:0:8::38/39	pvsx1.eucloud.io	HTTPS (mTLS)	443	Provisioning for certified IP Phones only.
5.144.142.36 (GS) / 5.144.142.37 (PAR3) 2a00:e00:0:8::36/37	pvsxlegacyonly.eupcloud.io (restricted)	HTTPS (IP validation)	443	Legacy provisioning — ticket and IP declaration required.

SBC – VOIP ACCESS (IP Phones, Softphones, PBX Trunking)

IP (GS/PAR3)	FQDN	Protocol	Ports	Comment
195.200.102.110 / 2a00:e00:0:9::110	cprx1.eupcloud.io → inservice.access.eupcloud.io	SIP (UDP/TCP), RTP	6060 / 16000–65535	Unsecured SIP/RTP for IP Phones without TLS.
195.200.102.111 / 2a00:e00:0:9::111	cprx1soft.eupcloud.io → inservice.access-sp.eupcloud.io	SIP (UDP/TCP), RTP	6060 / 16000–65535	Unsecured SIP/RTP for softphones (myistra, mobiis).
195.200.102.112 / 2a00:e00:0:9::112	routing.eupcloud.io → inservice.pbxtrunking.eupcloud.io	SIP (UDP/TCP), RTP	6060 / 16000–65535	Unsecured PBX trunking.
195.200.102.113 / 2a00:e00:0:9::113	cprx1s.eupcloud.io → inservice.access-tls.eupcloud.io	SIPTLS, SRTP-TLS, SRTP	5061 / 16000–65535	Secured SIP/RTP for TLScapable IP Phones.-capable IP Phones.
195.200.102.114 / 2a00:e00:0:9::114	cprx1softs.eupcloud.io → inservice.access-sp-tls.eupcloud.io	SIPTLS, SRTP-TLS, SRTP	5061 / 16000–65535	Secured SIP/RTP for TLS softphones.

195.200.102.115 / 2a00:e00:0:9::115	routings.eupcloud.io → inservice.pbxtrunking-tls.eupcloud.io	SIPTLS, SRTP-TLS, SRTP	5061 / 16000–65535	Secured PBX trunking.

MBC – WebRTC Media Relays

IP (PAR3 / GS)	FQDN	Protocol	Ports	Comment
195.200.102.105 / 106 2a00:e00:0:9::105/106	mbc1.eupcloud.io mbc2.eupcloud.io	WebRTC (UDP)	10000–60000	WebRTC relay for softphones; load balancing by app.

External Services

IP / FQDN	Protocol	Ports	Comment
stun.l.google.com stun1.l.google.com	STUN/TURN	19302	Browser WebRTC capability tests.
iam.voipoperator.eu www.mymeetings.cloud	HTTPS	443	Coligo Istra Collab service.
* or 17.0.0.0/8	TCP	5223 / 2197	Apple push notifications.
xmpp.googleapis.com	HTTPS	5235 / 5222 / 5228 / 853	Google Firebase push services.

---

5. Service VoIP

Codecs & DTMF

Usage	Codecs préférés	Notes
Passerelle PSTN	G.711A (principal), OPUS (à la demande)	DTMF via SIP INFO (préféré), fallback RFC2833

Téléphones IP	G.711A, G.722, OPUS	Sélection optimisée selon modèle
Mobiis	iLBC, OPUS, G.722, G.711A	Appels internes → OPUS/G722 ; Mobiis ↔ Mobiis → iLBC ; PSTN → G711A
myIstra Multi	iLBC, OPUS, G.722, G.711A	SIP INFO privilégié
myIstra WebRTC	WebRTC	Softphone basé navigateur (WebRTC)

---

6. Hébergement & Redondance

La plateforme est hébergée dans trois datacenters **Tier 3+** en région parisienne :

Datacenter	Nom	Adresse	Usage
Digital Realty	PAR3	Saint-Denis	Moitié de l'infrastructure + firewalls
Global Switch Paris Est	GS	Clichy	Moitié de l'infrastructure + firewalls
Equinix	PA7	Courbevoie	Noeud témoin pour la redondance

Un test annuel de continuité est réalisé avec les partenaires.

---

7. Limitations du Service

Sécurité et contrôle d'accès

• Compte de type "SIP générique" est non autorisé (exceptions possibles via PSE).
• Provisioning sécurisé uniquement (mTLS pour les équipements compatible).
• Mise en autoblacklist temporaire en cas de provisioning non déclaré ou autorisé (30 min).

Connectivité et réseau
• IPv6: le provisioning mTLS est disponible uniquement en IPv6, pas de mode "legacy whitelist" possible.

• Les équipements « legacy » ou ne supportant pas un échange TLS avec un certificat valide, signé par une autorité de certification constructeur reconnue, ne sont pas pris en charge en IPv6, mais seulement en IPv4.
• Mobiis fonctionne de manière optimale dans un environnement mobile 4G/5G ou sur un réseau WiFi principalement en 5 GHz. Le WiFi 2,4 GHz est généralement trop perturbé par des éléments extérieurs (réseaux WiFi concurrents, téléphones DECT, Bluetooth, fours micro-ondes, etc.) pour garantir une liaison stable et pérenne. Il est donc aussi recommandé d'éviter les réseaux WiFi avec SSID dual-band (2,4 GHz + 5 GHz) et de privilégier un réseau 5 GHz exclusivement.

Téléphonie et numérotation
• Numérotation obligatoire au format E.164.
• Les utilisateurs myIstra peuvent composer en format national.

Services non supportés
• Pas de Fax2Mail (ATA requis).

Sessions et expirations
• Expiration de session myTelephony : 8h.
• Expiration de session myIstra : 12h.

Bonnes pratiques d'usage
• Déconseillé d'utiliser plusieurs appareils Mobiis par extension.

8. Implémentation SIP

La plateforme supporte un ensemble étendu de RFC SIP couvrant :

- **RFC 3261**: SIP: The main SIP RFC.
- RFC 2617: HTTP Digest Authentication: The digest authentication used by SIP is defined in this RFC.
- RFC 2976: SIP Info Method: Generic INFO message to convey information such as the dtmf send or received (today we use this message to send/receive dtmf encoded in the format: "application/vnd.nortelnetworks.digits" or "application/dtmf-relay" (Cisco proprietary).
- RFC 3262: SIP Reliability of Provisional Response : This RFC defines how to send reliably the provisional SIP responses (response of range 1XX).
- RFC 3263: Locating SIP Servers (SRV resolutions only) : This RFC defines how to locate a SIP server through the use of the DNS NAPTR/SRV/A record entries.
- RFC 3264: Offer Answer Model SDP for SIP : This RFC defines the SDP negotiation process in SIP for establishing audio/video format.
- RFC 3265: Specific Event Notifications : SUBSCRIBE and NOTIFY
- RFC 3323: A Privacy Mechanism for the Session Initiation Protocol (SIP) : This RFC specify the usage of the header Privacy.
- RFC 3324: Short Term Requirements for Network Asserted Identity : This RFC specify the notion of Trusted Network.
- RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks: This RFC specify the usage of the header P-Asserted-Identiy and the value "id" of header Privacy.
- RFC 3515: Refer Method: The REFER method is used for transfering SIP calls.
- RFC 3581: Symmetric Response Routing: This describe a method to be able to route responses through NAT. (parameter rport)
- RFC 3761: ENUM: PSTN number resolution:
- RFC 3842: A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3891: Replaces Header : The replaces header is used on one leg of a transfered call (in a two steps transfer).
- RFC 3892: Referred-By Mechanism : The referred-by mechanism is also used in redirected/transfered calls.
- RFC 4028: Session Timers for SIP
- RFC 4235: An INVITE-Initiated Dialog Event Package for SIP. These events are used for the BLF implementation (notification of change on call state).
- RFC 5806: Diversion Info (http://www.softarmor.com/wgdb/docs/draft-levy-sip-diversion-08.txt) : Allow to convey in the SIP messages the history of the call (history of diversion that have happened on this call like a forward, transfer, redirect...).

- SIP RemotePartyID to convey privacy data, expired draft: http://www.iptel.org/ietf/security/identity/draft-ietf-sip-privacy-04.txt
- Comedia direction in SDP: expired draft ietf-mmusic-sdp-comedia-04.txt (have been replaced by RFC4145) : allow to specifiy in the SDP if the RTP IP destination is updated using source IP address of received RTP packets (mode passive).