

Votre feuille de route Jitsi Meet sans compte, sous votre contrôle

Préparez, déployez et sécurisez une instance Jitsi Meet auto-hébergée pour inviter vos participants par simple lien web. Suivez cette feuille de route avant votre première visioconférence.

Au sommaire

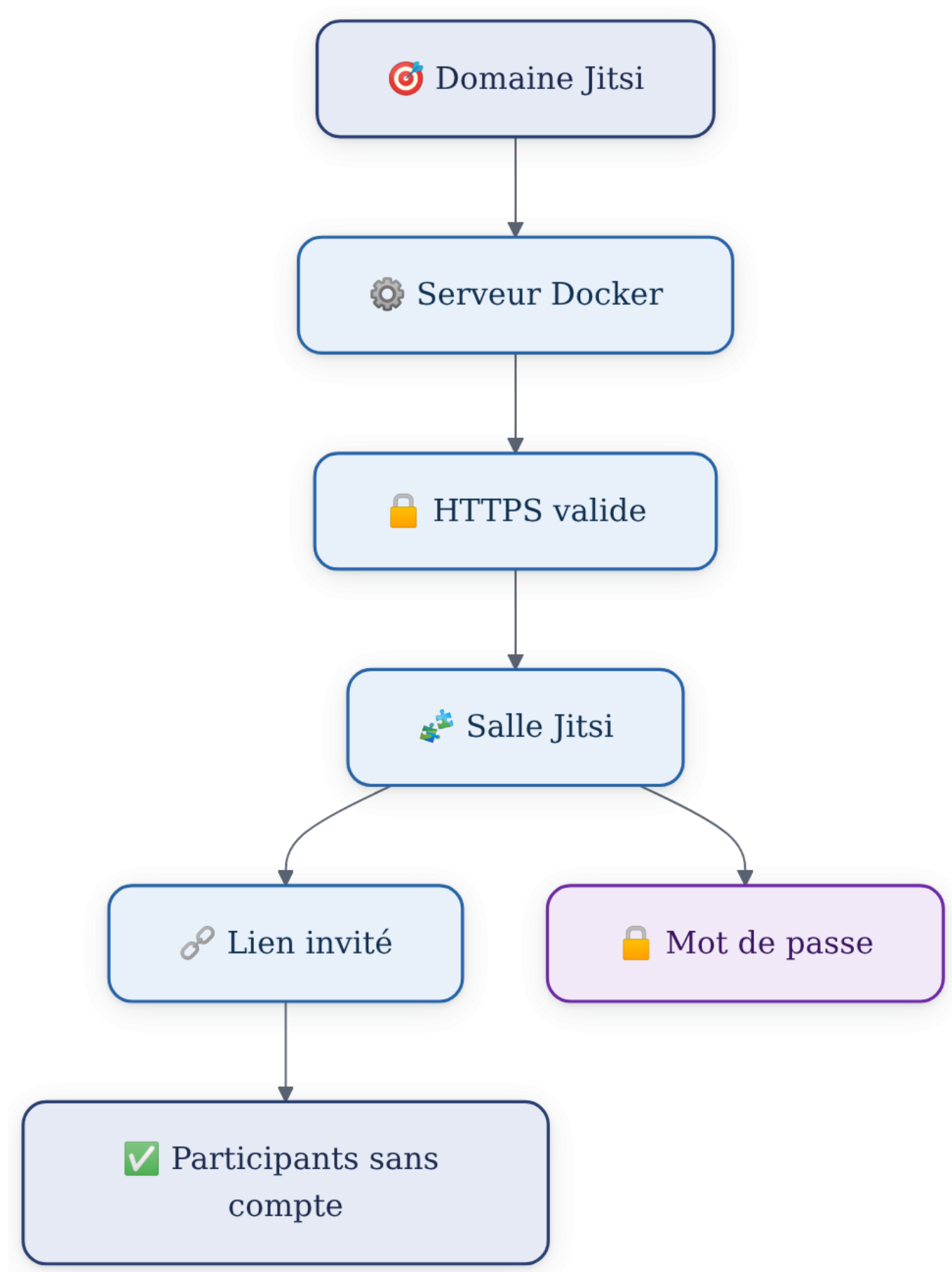
- 1 Le principe à retenir
- 2 Choisir le mode de déploiement
- 3 Préparer l'infrastructure avant l'installation
- 4 Déployer Jitsi Meet avec Docker
- 5 Contrôle final avant d'envoyer le lien

Le principe à retenir

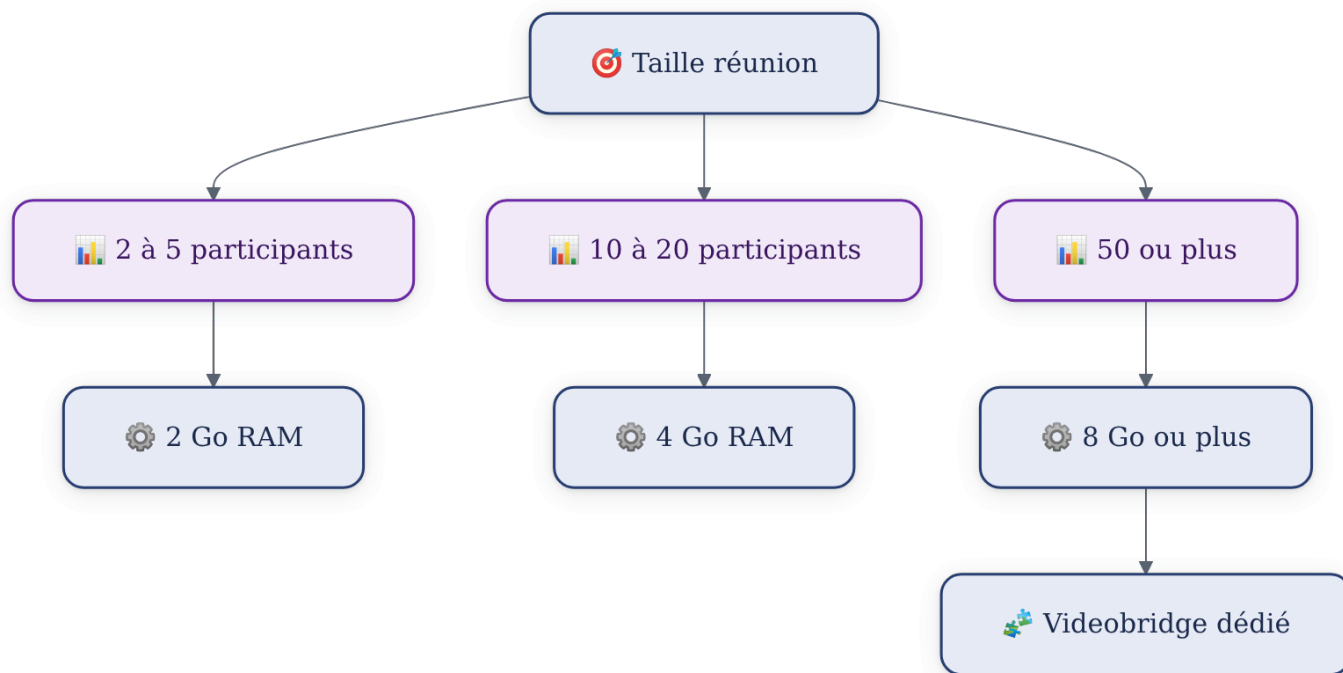
Les invités peuvent rejoindre une réunion Jitsi Meet depuis leur navigateur, sans créer de compte.

L'auto-hébergement donne la maîtrise du domaine, des règles d'accès, des mises à jour et de l'infrastructure, mais implique aussi leur administration.

L'accès sans compte ne rend pas une salle privée : un nom difficile à deviner, un mot de passe et la modération restent essentiels.



INFOGRAPHIE Schéma du déploiement Jitsi Meet auto-hébergé avec Docker et accès sans compte



INFOGRAPHIE Infographie des ressources serveur pour Jitsi Meet sans compte auto-hébergé

Choisir le mode de déploiement

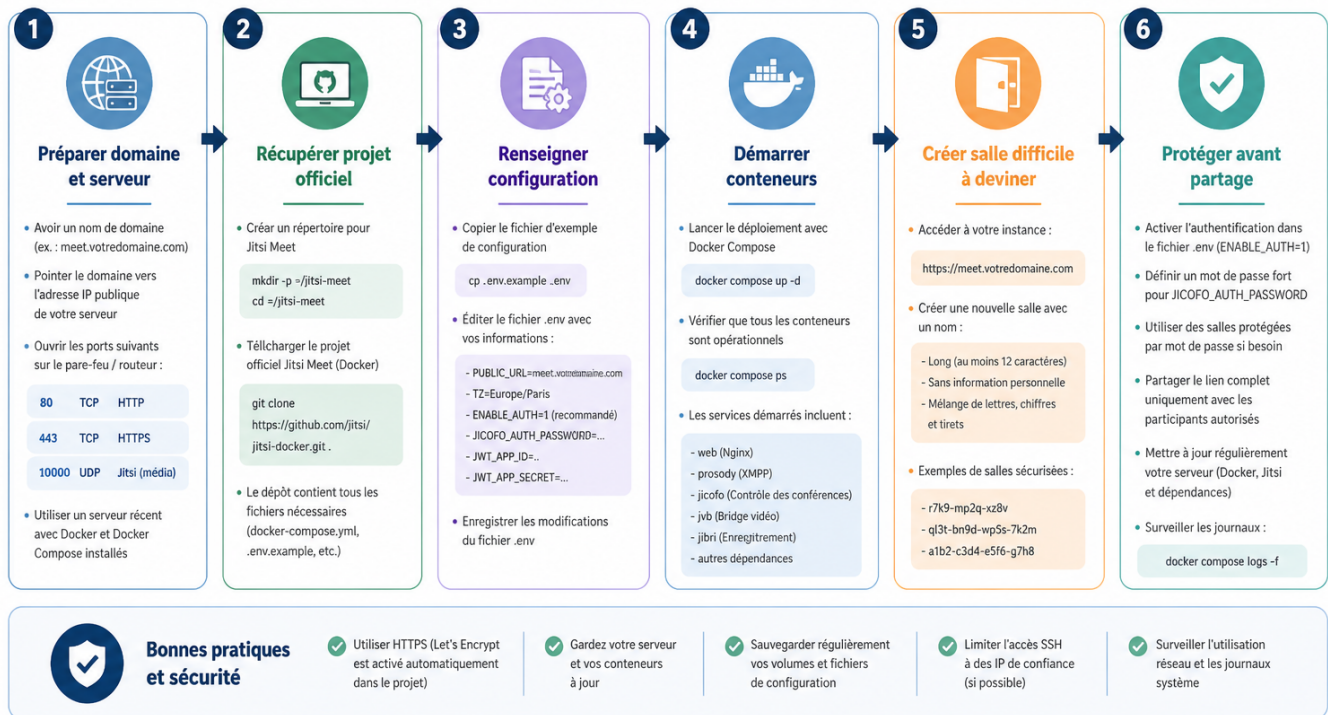
Option	À privilégier si...	Point de vigilance
Instance publique	Vous avez un besoin ponctuel ou souhaitez tester rapidement.	Les règles, la disponibilité et la politique de données dépendent de l'opérateur.
Jitsi Meet auto-hébergé avec Docker	Vous disposez d'un administrateur et voulez un déploiement reproductible.	Vous prenez en charge le DNS, la sécurité, la supervision et les incidents.
Installation Linux classique	Vous administrez déjà une infrastructure Debian et recherchez une intégration directe.	La maintenance dépend davantage de la configuration locale.

Préparer l'infrastructure avant l'installation

- ☐ **Prévoir un serveur Linux accessible depuis Internet avec un accès administrateur.**
- ☐ **Créer un domaine ou sous-domaine dédié à la visioconférence.**
Son enregistrement DNS doit pointer vers l'adresse publique du serveur.
- ☐ **Installer et vérifier Docker ainsi que Docker Compose.**
- ☐ **Prévoir un certificat TLS valide pour le domaine.**
Il évite les alertes de sécurité dans le navigateur.
- ☐ **Documenter les règles de pare-feu et les tester depuis un réseau externe.**
- ☐ **Évaluer le besoin d'un serveur TURN.**
Il améliore la fiabilité pour les réseaux avec NAT ou pare-feu restrictif.

Installation de Jitsi Meet auto-hébergé avec Docker

Guide pas à pas pour déployer votre propre solution de visioconférence sécurisée



📌 Votre instance Jitsi Meet auto-hébergée est prête ! Profitez de visioconférences libres, privées et sous votre contrôle.

SCHÉMA Vue d'ensemble des étapes d'installation de Jitsi Meet avec Docker.

Déployer Jitsi Meet avec Docker



1. Valider le domaine et le serveur

Faites pointer le DNS vers le serveur, appliquez les mises à jour système et confirmez que Docker et Docker Compose fonctionnent. Attendez que le DNS soit propagé avant de poursuivre.

2. Récupérer le projet officiel

Clonez ou téléchargez le dépôt officiel docker-jitsi-meet dans un répertoire dédié. Consultez sa documentation pour choisir la version et les variables de configuration adaptées.

3. Configurer l'instance

Renseignez le nom de domaine et les paramètres d'environnement dans le fichier de configuration fourni par le projet. Évitez les fichiers .env non vérifiés provenant de forums.

4. Démarrer les conteneurs

Lancez les services avec Docker Compose, puis ouvrez l'adresse HTTPS de votre domaine pour vérifier que l'interface Jitsi Meet est accessible.

5. Tester une réunion réelle

Testez l'audio, la vidéo et le partage d'écran avec un participant externe, idéalement depuis un réseau différent du vôtre.

6. Protéger la salle avant l'invitation

Créez une salle au nom imprévisible, activez un mot de passe et appliquez la modération avant de partager le lien.

! N'ouvrez pas des ports sans vérification

Les déploiements mentionnent souvent 443/TCP, 4443/TCP et la plage 10000-20000 pour les flux média. Vérifiez impérativement les paramètres de la version installée et les règles de votre hébergeur avant toute ouverture.

Contrôle final avant d'envoyer le lien

- ☐ Vérifier que l'URL utilise bien HTTPS et ne déclenche aucune alerte de navigateur.
- ☐ Donner à la salle un nom non prévisible.
- ☐ Définir un mot de passe de réunion et le transmettre séparément si nécessaire.
- ☐ Prévoir la modération de la salle pendant la réunion.
- ☐ Tester l'accès depuis un navigateur et un réseau externes.
- ☐ Contrôler audio, vidéo et partage d'écran avant l'horaire prévu.
- ☐ Prévoir une solution de relais TURN si certains invités se connectent depuis des réseaux restrictifs.

La capacité et la qualité d'une visioconférence dépendent aussi du réseau, du navigateur, du pare-feu et des réglages de l'instance. Consultez la documentation officielle de Jitsi et du projet docker-jitsi-meet avant toute mise en production.