

Architecture et prérequis Qubes v10



DATE DE DIFFUSION : 09/11/2022

REFERENCE : SUP0237 v1.00

Prérequis Qubes v10

Creative IT | 28 Avenue René Cassin - 69009 Lyon - FRANCE

+33 (0)4 78 83 19 90 | www.qubes.com

SOMMAIRE

1. Introduction.....	5
2. Prérequis technique pour les serveurs.....	5
2.1. Gestion des environnements.....	5
2.2. Configuration minimale requise.....	6
2.2.1 Types d'application	6
2.2.2 Environnement	8
2.2.3 Virtualisation	8
2.2.4 Stockage	8
2.3. Bases de données	9
2.3.1 Firebird.....	9
2.3.2 PostgreSQL	9
2.3.3 Oracle.....	9
2.3.4 MS SQL Server	9
3. Prérequis techniques pour les postes utilisateur	11
3.1. Configuration minimale pour les postes fixes.....	11
3.2. Configuration minimale pour les terminaux mobiles.....	12
3.3. Cas des serveurs CITRIX ou TSE	12
3.4. Mots de passe Qubes.....	13
4. Réseau.....	13
5. Sécurité	13
6. Compatibilités logicielles.....	14
6.1. Outils bureautiques via l'application	14
6.2. Outils bureautiques en intranet via WebDAV.....	14
6.3. Messagerie électronique.....	14
6.4. Serveur d'impression	15
6.4.1 Cas général	15
6.4.2 Avec Qubes i4	15
6.4.3 Conversion PDF.....	15
6.5. Serveur OPC.....	15
6.6. Bases de données tierces	16



6.7. Autres logiciels.....	16
6.8. Logiciels antivirus.....	16

1. Introduction

L'objectif de ce document est de vous accompagner dans votre démarche de recherche de matériels (serveurs, poste de travail utilisateur, réseaux ...) et de préparer au mieux votre infrastructure informatique pour l'installation et le déploiement du logiciel Qubes.

Les recommandations proposées dans ce document ont été rédigées pour des installations typiques de Qubes. En fonction des spécificités de votre projet, des configurations plus puissantes peuvent s'avérer nécessaires.

Les choix pour le matériel et l'infrastructure sont bien sûr sous la responsabilité du client.

2. Prérequis technique pour les serveurs

2.1. Gestion des environnements

Nous préconisons pour tout projet Qubes de disposer d'un environnement de développement, d'un environnement de tests (ou pré-production) et d'un environnement de production.

Environnement de développement : environnement indépendant utilisé pour réaliser les développements et les paramétrages nécessaires au projet, que ce soit au début du projet ou tout au long de la vie de l'application dans l'entreprise.

Environnement de tests (ou pré-production) : environnement qui dans l'idéal est relié à un serveur de tests ERP et à un serveur de données process, permettant de jouer les paramétrages pour les tester avec des données réelles.

Environnement de production : environnement stabilisé utilisé par les opérateurs lors de leurs actions dans Qubes. Seul cet environnement doit répondre aux configurations minimales ci-après.

Pour gérer correctement une installation comprenant plusieurs environnements (environnements de production, de test, de formation, d'intégration...), il est recommandé d'installer un serveur par site, pour chaque environnement.

Nous recommandons également une base de données Qubes par site, pour chaque environnement.

Il est préférable de stocker les bases de données de développement et de test sur un serveur distinct de celui de la production. Dans le cas d'Oracle, définir une instance spécifique pour chaque environnement permet d'assurer l'indépendance des bases entre elles.

2.2. Configuration minimale requise

2.2.1 Types d'application

Afin de déterminer l'architecture à mettre en place, il convient d'identifier le type d'application qui sera déployée.

Type d'application	Small	Standard	Premium
Base de données	Firebird, PostgreSQL, MSSQL	Firebird, PostgreSQL, Oracle	PostgreSQL, Oracle
Mémoire vive	6 Go min	12 Go min*	24 Go min*
Processeur	x86-64 cadencé à 3 GHz ou plus		
Nb cœurs physiques	2	4	
Nb serveurs	1 (Qubes + Firebird)	1 (Qubes + BDD) ou 2 (si BDD séparée)	
Stockage	Classe SSD		Classe NVMe
Taille disques BDD	5 Go/an	10 Go/an/site**	15 Go/an/site**

* dans le cas d'une configuration à deux serveurs, il s'agit de la mémoire totale

** un espace disque supplémentaire devra être alloué pour la journalisation pour les BDD concernées. Les chiffres indiqués sont des chiffres moyens. La taille de la BDD est fortement variable d'un client à l'autre selon les types de données que doit historiser l'application.

Exemples de configurations en fonction du type d'application :

Small :

- **Utilisateurs simultanés** : 10
- **Un des périmètres suivants** : Suivi des OF, et / ou suivi des contrôles qualité, ou gestion documentaire (avec quelques processus qualité)
- **Nombre de sites** : 1
- **Volumétrie** : exemple d'une laiterie industrielle
 - 100 000 enregistrements de contrôles / an
 - 20 000 lots / an
 - Taille de disque : 25 Go pour 5 ans de fonctionnement

Standard :

- **Utilisateurs simultanés** : 25 par site
- **Deux ou 3 des périmètres suivants** : suivi du TRS (connecté aux équipements ou non), suivi des OF, suivi des contrôles qualité, gestion documentaire (avec quelques processus qualité)
- **Nombre de sites** : 1 à 4
- **Volumétrie** : exemple d'un groupe de maroquinerie industrielle
 - 20 points d'acquisition automatique toutes les 60s, soit 28 800 / jour
 - 20 000 OFs /an
 - 60 000 lots /an
 - Taille de disque : 50 Go par site pour 5 ans de fonctionnement

Premium :

- **Utilisateurs simultanés** : 50 par site
- **Périmètre** : l'intégralité du périmètre couvert par Qubes, c'est à dire suivi du TRS (connecté aux équipements ou non), suivi des OF, suivi des contrôles qualité, SPC (Historian), logistique atelier, gestion documentaire, processus qualité...
- **Nombre de sites** : 5 à 20 sites

- **Volumétrie** : exemple d'un groupe de boulangerie industrielle
 - 60 points d'acquisition automatique toutes les minutes soit 86 400 / jour
 - 100 000 lots /an
 - Taille de disque : 100 Go par site pour 5 ans de fonctionnement

2.2.2 Environnement

Les systèmes d'exploitation requis pour l'utilisation de Qubes sont :

- Serveur Applicatif Qubes : Microsoft Windows 2016, 2019, 2022
- Serveur base de données : Linux ou OS alternatifs, si géré par le client

Il est indispensable de disposer sur le serveur d'un navigateur HTML5 compatible avec Qubes (cf. prérequis du poste utilisateur, plus loin dans le document). NB : L'installation standard de Microsoft Internet Explorer sur le serveur n'est pas compatible avec Qubes.

2.2.3 Virtualisation

La plupart des serveurs étant aujourd'hui virtualisés, il convient de faire attention à ce que chaque cœur de CPU virtuel utilise bien un cœur CPU physique et non pas un cœur hyperthreadé (HT chez Intel ou SMT chez AMD). Les ressources du serveur physique doivent impérativement être dédiées à la machine virtuelle.

Aussi il faudra faire en sorte que la somme des cœurs virtuels de toutes les machines virtuelles hébergées sur l'hyperviseur ne dépasse pas le nombre de cœurs physiques totaux.

Les applications de virtualisation compatibles sont : VMWare, KVM, Hyper-V.

2.2.4 Stockage

Les niveaux de performances s'entendent comme :

- « Classe SSD » : minimum 300 Mo/s et 30k IOPS
- « Classe NVMe » : minimum 1 Go/s et 100k IOPS

La partie serveur de l'application requiert 10 Go, elle contient environ 1 Go de binaires de l'application (exe, dll, ...) et de ressources, ainsi que des logs et cache applicatifs, de taille variable.

Cet espace sera à surveiller et doit offrir des performances d'accès de « classe SSD ».

Ne pas négliger l'espace de stockage pour la sauvegarde de la BDD, qui selon les configurations sera au minimum deux fois plus important que la BDD (taille de la sauvegarde J-1, plus espace pour la sauvegarde J).

2.3. Bases de données

2.3.1 Firebird



Firebird : 3.X (en version 64 bits)

Firebird est une base de données Open Source gratuite avec des options de support payant. Cette base de données n'est pas recommandée en cas de forte volumétrie cible mais ne requiert pas de maintenance.

2.3.2 PostgreSQL



PostgreSQL : 12.2, 15 (en version 64 bits)

PostgreSQL est « la base de données Open Source la plus avancée au monde ».

2.3.3 Oracle



Oracle : 19.X

Les clients disposant de compétences Oracle et ayant déjà des serveurs Oracle installés peuvent choisir de les utiliser comme système de base de données pour Qubes. Dans ce cas, c'est au gestionnaire de la base de données de faire les choix opportuns pour l'installation.

2.3.4 MS SQL Server



MS SQL Server : 2016, 2017

Les clients disposant de compétences MS SQL Server et ayant déjà des serveurs MS SQL Server installés peuvent choisir de les utiliser comme système de base de données pour Qubes. Dans ce cas, c'est au gestionnaire de la base de données de faire les choix opportuns pour l'installation. Cette base de données n'est pas recommandée en cas de nombreux accès concurrents.



La gestion, le monitoring et le contrôle périodique de l'intégrité des sauvegardes sont à la charge du client. NB : Creative IT propose aussi une prestation de service de monitoring du bon fonctionnement de l'application Qubes afin d'anticiper les éventuelles dérives des services Qubes sur vos serveurs.



Pour accéder à la base de données Qubes, on recommande d'utiliser la version 64 bits du service P2PProxy (un des services compris dans l'installation de Qubes).

3. Prérequis techniques pour les postes utilisateur

3.1. Configuration minimale pour les postes fixes

Les utilisateurs ont accès l'application Qubes :

- **En mode web** : dit intranet, via les navigateurs Web compatibles listés ci-après
- **En Client /serveur** : dit application Qubes.exe, pour les administrateurs Qubes et certaines fonctionnalités de consultation avancées

Type d'application	Application Qubes.exe	Intranet
Système Client	Windows 8.1, 10, 11	Windows 8.1, 10, 11 Linux, Android 9+
Mémoire vive	4 Go	4 Go
Nb cœurs	2	2
Résolution Ecran mini	1280*1024	1024*768

Les navigateurs HTML 5 supportés sont :

- **Chromium (Chrome, Brave, New Edge)** : version publique courante



Attention : le navigateur Microsoft IE 11 n'est plus supporté ni pour les [postes fixes](#) ni pour les [terminaux portables](#) (Pocket PC, ...)

Pour l'utilisation de l'application Qubes.exe, nous recommandons les OS Windows 10 Pro.

Pour l'utilisation de Qubes, il faut prévoir que les postes clients soient pourvus des logiciels adaptés à la consultation ou à l'édition des formats stockés par Qubes dans le cadre du projet (exemple : lecteur PDF, MS Office, LibreOffice, ...).

3.2. Configuration minimale pour les terminaux mobiles

Les configurations minimales valent pour les terminaux mobiles Android utilisant le navigateur intégré.

Type de matériel	Pocket PC mode portrait	Tablette mode paysage
Système client	Android 9+	Android 9+
Mémoire vive	2 Go	4 Go
Nb cœurs	2	2
Résolution Ecran mini	480*800	1024*768

3.3. Cas des serveurs CITRIX ou TSE

Type d'application	Application sous TSE/Citrix	Intranet sous TSE/Citrix
Système Client	2016/2019	2016/2019
Mémoire vive	1 Go / session	2 Go / session
Nb cœurs	1/2 par session	1 par session
Résolution Ecran mini	1280*1024	1280*1024



Pour des raisons de performances, il faut séparer le serveur CITRIX/TSE du serveur Qubes. Les configurations s'entendent si le serveur CITRIX/TSE est **dédié** et non partagé avec d'autres applications.

3.4. Mots de passe Qubes

Nous attirons votre attention sur le fait que certains utilisateurs ont pu activer les fonctions de mémorisation de mots de passe de leur navigateur. Cela provoquera l'initialisation du mot de passe Qubes dans les fenêtres de signature électronique, ce qui pourra être une cause de non-conformité en cas d'audit externe (exigences Bonnes Pratiques de Fabrication, exigences 21-CFR-11 de la FDA ...).

4. Réseau

Il est difficile d'établir une évaluation de la bande passante tant que le périmètre et l'implémentation du projet n'auront pas été finalisés (ex : utilisation ou non de modes opératoires vidéo, utilisation ou non des clusters Qubes i4, types de données synchronisées...).

Il conviendra de minimiser la latence entre le serveur Qubes et les postes clients (application Qubes ou navigateur HTML5). L'infrastructure Qubes i4 cluster est une solution possible pour minimiser la latence et augmenter la disponibilité.

5. Sécurité

Il est essentiel de protéger les machines de production de toute attaque informatique visant à prendre le contrôle des données ou des systèmes (virus, ransomware, hacking).

Nous préconisons donc que le réseau usine (qui assure la communication entre les machines de production) soit désolidarisé du réseau bureautique (qui a généralement accès à Internet et donc potentiellement attaquant).

Ceci est à adapter en fonction de la stratégie de sécurité de votre service informatique.

6. Compatibilités logicielles

Qubes est compatible à sa date de sortie initiale avec les versions des logiciels tiers ci-dessous.

Durant la période standard où la version de Qubes v10 est maintenue, celui-ci restera compatible avec ces versions logicielles même si celles-ci cessent d'être maintenues par leur éditeur durant cette période.

6.1. Outils bureautiques via l'application

- **Microsoft Office** : 2016, 2019, 2021. Qubes a conservé ses interfaces avec d'autres versions obsolètes de Microsoft Office, mais la compatibilité n'est plus garantie (ex : 2003 SP3, 2007 SP3, 2010 SP2)
- **LibreOffice** : 7.x

6.2. Outils bureautiques en intranet via WebDAV

- **Microsoft Office** : 2016, 2019, 2021
- **LibreOffice** : 7.x (nécessité d'ajouter une entrée dans la base de registre)

6.3. Messagerie électronique

Qubes peut envoyer des emails via le protocole **SMTP** (soit depuis le serveur Qubes, soit depuis l'application Qubes).

Le port 25 devra être ouvert dans le firewall du serveur Qubes, ainsi que des postes Qubes susceptibles d'envoyer des messages.

Les protocoles SSL et TLS ne sont pas supportés nativement par Qubes, mais il est possible de le faire via l'installation d'un logiciel de relais SMTP tiers.



En fonction des réglages, Qubes peut envoyer un grand nombre de messages automatiques (en lien avec le cycle de vie des documents, les processus qualité, les processus de production, ...). Or, certains fournisseurs SMTP imposent des limites (c'est le cas de Microsoft Office 365). Dans ce cas, il faudra souscrire un compte adéquat auprès du fournisseur SMTP, ou se tourner vers un fournisseur de mail transactionnel.

6.4. Serveur d'impression

6.4.1 Cas général

Pour l'impression des étiquettes nous préconisons l'utilisation d'un serveur d'impression dédié. Pour une haute disponibilité des impressions, nous recommandons que le serveur d'impression soit installé en local sur chaque site.

Les imprimantes doivent impérativement être connectées sur le réseau Ethernet. Les imprimantes en port série sur un PC ne pourront pas être adressées par le serveur.

Qubes possède un connecteur NiceLabel. Il existe différentes versions du serveur NiceLabel. Merci de vérifier que la version que vous allez acquérir correspond à votre projet (nombre d'imprimantes, ...).

6.4.2 Avec Qubes i4

Pour l'impression de documents à partir d'imprimantes bureautiques, il est nécessaire que le serveur d'impression « Qubes i4 Print » soit installé sur un poste bureautique incluant Foxit Serveur (version 9.0). Dans ce cas particulier, Qubes i4, le PC bureautique et l'imprimante bureautique doivent être sur le même réseau. Dans le cas contraire il sera nécessaire de paramétrer les règles de flux dans la passerelle inter-réseau.

6.4.3 Conversion PDF

En Intranet, il est possible de convertir au format PDF un document Word ou Libre office sans passer par une opération d'import du document au format PDF. Pour cela il faut installer Libre Office 6.3 sur le serveur (la conformité de la version PDF au document original dépendra donc de la capacité du moteur de conversion de LibreOffice).

Il est aussi possible de publier l'export PDF d'un document Word directement dans la vue PDF de Qubes (Export / PDF / Enregistrer).

6.5. Serveur OPC

Qubes étant client OPC nativement, il peut se connecter avec n'importe quel serveur OPC DA ou OPC UA, dans la limite des fonctionnalités supportées par Qubes. Merci de nous contacter au préalable si votre serveur OPC est autre que KEPWare OPC Server.

6.6. Bases de données tierces

Qubes possède des connecteurs Firebird, PostgreSQL, MS SQL Server, Oracle, SQLite et ODBC.

Pour se connecter aux bases de données tierces, on recommande de passer par la version 64 bits du service P2PProxy. Dans le cas d'une connexion ODBC, cela imposera d'utiliser un driver ODBC 64 bits.

6.7. Autres logiciels

Qubes s'interface avec un certain nombre d'applications tierces dont les ERP.

Pour connaître les ERP avec lesquels Qubes est compatible et les protocoles d'échange, voir la fiche : **Qubes connecteurs ERP**.

6.8. Logiciels antivirus

Des configurations spécifiques des logiciels antivirus peuvent être nécessaires.

Exemple : McAfee nécessite de mettre Qubes en liste blanche pour l'envoi SMTP.