Client: Creative IT

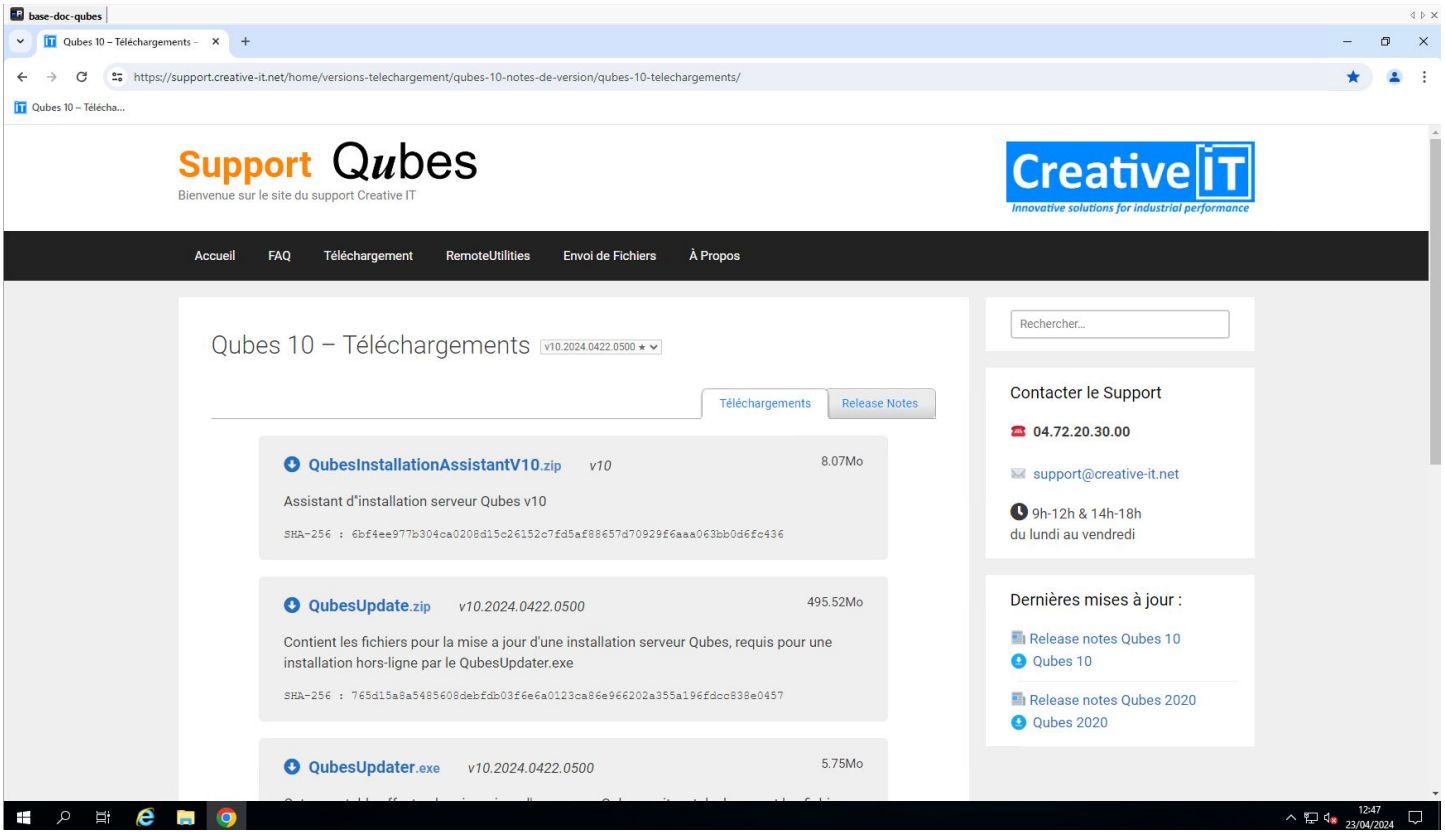
Prérequis : Avoir un accès au serveur Qubes

Objectifs: Faire la MAJ mineure d’un serveur Qubes

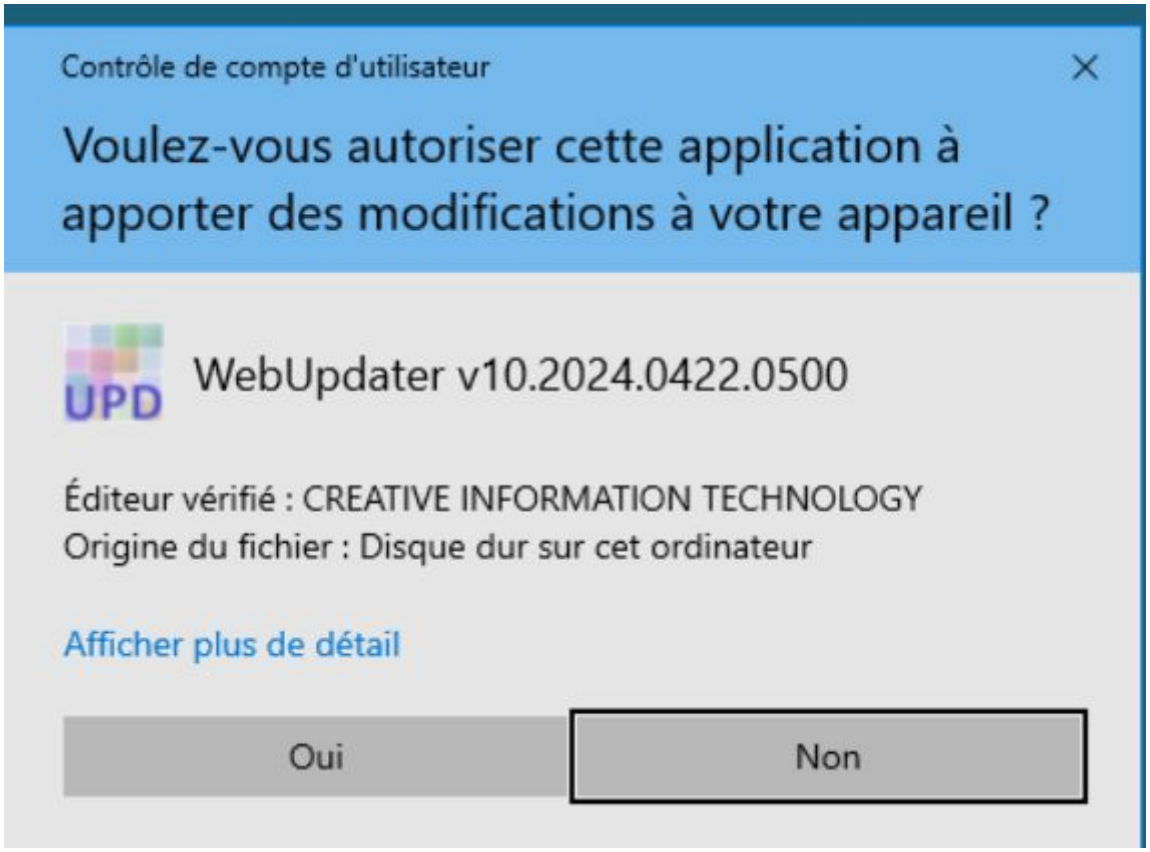
Destinataires: Support, Clients

Actions

1. Ouvrir un navigateur sur le serveur Qubes si vous avez un accès internet, sinon depuis un poste et accéder à la page de téléchargement de notre site support comme ci-dessous. https://V10.qubes.com/Télécharger le fichier « QubesUpdate.zip et QubesUpdater.exe en vous assurant que vous êtes bien sur la version adéquate comme ici la dernière publiée avec (*) qui la symbolise



1. Télécharger le fichier « QubesUpdate.zip » et « QubesUpdater.exe »
2. Déplacer les fichiers sur le bureau du serveur Qubes
3. Exécuter le fichier « QubesUpdater.exe » en tant qu'administrateur
4. Si vous avez ce message ci-dessous, il faut cliquer sur « Oui »



5. Sur cet écran comme ci-dessous, il faut cocher « Ne pas télécharger la mise à jour… »

6. Laisser se dérouler l'update, à la fin vous devez avoir ce type de message

24/04/2024 10:56:26 – Qubes Update Start
24/04/2024 10:56:26 – Check if Qubes is running.
24/04/2024 10:56:26 – Check QubesRelease.zip content.
24/04/2024 10:56:26 – Stop Qubes Services
24/04/2024 10:56:26 – Query service stop: SEQubesGuardian
24/04/2024 10:56:29 – Query service stop: SEWebService

24/04/2024 10:56:34 – Backup current Qubes.
24/04/2024 10:57:22 – Apply update.
24/04/2024 10:57:53 – Unable to extract file LDAPTest.exe from fullrelease.zip -> skipped.
24/04/2024 10:57:53 – Unable to extract file SMTPTester.exe from fullrelease.zip -> skipped.
24/04/2024 10:58:29 – Query service start: SEQubesGuardian
24/04/2024 10:58:53 – Query service start: SEP2PProxyService
24/04/2024 10:58:53 – Query service start: SEWebService
24/04/2024 10:58:54 – Query service start: SEQuBESIndexer
24/04/2024 10:58:55 – Query service start: SEPeonService
24/04/2024 10:58:58 – Update Finished

7. Afin de ne pas encombrer votre serveur, il est conseiller de supprimer les versions précédentes et de conserver que celle que vous aviez avant cette MAJ mineure au cas où il faille revenir en arrière. le chemin par défaut du répertoire Update de Qubes est:
D:\Qubes\Bin\Updates

Client: Creative IT, clients et prestataires

Prérequis : Être un utilisateur confirmer de Qubes

Objectifs: Désactiver des fonctions de scripts en mode web

Destinataires: Creative IT, clients et prestataires

Les fonctions suivantes ont été désactivés en mode Web, dans les versions 2018 et >. :

StartNewFormularInstance

StartNewProcessInstance

TOFExecution.ExecuteOrContinue

Ce sont des fonctions dont il est documenté depuis longtemps qu'elle ne doivent être utilisés qu'en mode Client/Serveur, et celles-ci provoquent des blocages du service en mode web

Sur certains projet, pour pouvoir faire passer certains process, il est possible de les réactiver temporairement de la manière suivante :

Cela ne doit pas être utilisé au delà d'un déblocage et il est nécessaire d'adapter le code sous peine de toujours subir des blocages intempestifs.

Pour réactiver TOFExecution.ExecuteOrContinue, dans le fichier ini du meme nom que l'exécutable ajouter :

[LEGACY]

ExecOpe=Y

Pour réactiver les fonction StartNewFormularInstance et StartNewProcessInstance, dans le fichier ini du meme nom que l'exécutable ajouter :

[LEGACY]

StartNewFormular=Y

Client: Creative IT, clients et partenaires

Prérequis : Avec Teams

Objectifs: Savoir réparer quand Microsoft Teams est très lent avec écrans noirs

Destinataires: Creative IT, clients et partenaires

L'application Microsoft Teams peut devenir très lente, avec des écrans noirs intermédiaires affichés plusieurs secondes à plusieurs minutes.

Ce problèmes est signalé chez Microsoft mais non résolu depuis 2019, le contournement est de purger les caches.

Aller dans **%appdata%\Microsoft\teams**, puis supprimer les caches suivant:

1. In **Application Cache > Cache** folder, delete all files in it.
2. In **Blob_storage** folder, delete all files.
3. In **Cache** folder, delete all files.
4. In **databases** folder, delete all files.
5. In **GPUCache** folder, delete all files.
6. In **IndexedDB** folder, delete the .db file.
7. In **Local** Storage folder, delete all files.
8. In **tmp** folder, delete all files.

Source:
https://answers.microsoft.com/en-us/msoffice/forum/msoffice_o365admin-mso_teams-mso_o365b/teams-hogging-memory-running-slowly/3a5ddd1a-e4b0-41be-881d-c0d46b9abe23

Client: Creative IT

Prérequis : Avoir un admin qui puisse se connecter au serveur de la BDD, avoir un accès en VPN ou avec un partage d'écran

Objectifs: Rétablir la connexion à une base de données externe sous oracle 64 bits en Qubes 2020

Destinataires: Support

Information

Une application 32 bits (resp 64 bits) ne peut pas accéder à une source de données 64 bits (resp 32 bits). Or, Qubes.exe est une application 32 bits. Il ne peut donc pas accéder aux sources de données ODBC 64 bits.
Par contre, P2PProxy est une application 64 bits et pourra donc y accéder.

Le problème vient donc essentiellement du faite que vous ne pouvez pas utiliser l'écran de paramétrage de

Qubes.exe pour définir la source de données SQL de cette façon.
Cependant, c'est une très mauvaise pratique de définir une source de données SQL en indiquant son driver et les paramètres associés. Car cela obligera toutes les applications (Qubes, QubesExpress, QubesPeon) à être sur des machines pour lesquelles ce driver est installé et réglé de la même façon.

C'est pour éviter cela qu'on a développé le P2PProxy. Ainsi, il suffit de paramétrer les réglages de connexion via un nouvel alias dans le fichier SDBAliases.ini du P2PProxy (64 bits) et de dire que la source de données SQL passe par cet alias de ce P2Pproxy.

Astuce

Pour récupérer les informations que vous devez renseigner dans le SDBAliases.ini Vous pouvez utiliser l'utilitaire UDL.

-Pour ce faire il faut créé un fichier texte
-Renommer ce fichier en lui donnant l'extension UDL

Action 1

-Il est maintenant possible de double-cliquer sur le fichier pour exécuter l'application, le premier onglet Fournisseur afin de sélectionner le fournisseur.

-Rentrer les informations de connexion à votre serveur

-Editer le fichier UDL avec Bloc-Notes ou Notepad

Ses informations peuvent être utilisé pour remplir le SDBAliases.ini

Présentation

Depuis Qubes 2018, le système d'authentification a évolué pour supporter aussi une authentification de type TOTP, spécifique à chaque serveur Qubes.
Il est ainsi possible d'autoriser des clients ou des partenaires à accéder aux pages d'administration des installations Qubes qui les concernent.
Le protocole TOPT étant basé sur l'heure courante, l'utilisation de ce moyen d'authentification impose que le serveur concerné et l'application qui génère les OTP soient à l'heure.

Procédure client pour activer l'administration OTP

Pour chaque serveur concerné, l'administrateur doit envoyer un mail au support Creative IT avec :

- le nom du serveur
- la liste des identifiants autorisés à administrer les OTP de ce serveur
    - Il s'agit d'identifiants entre 3 et 10 caractères, choisis librement par le client
- la clé serveur générée par ServerKey.bat :
    - Télécharger le zip ServerKey.zip
    - Le dézipper et lancer ServerKey.bat
    - Copier la clé indiquée

Pour chaque serveur concerné, le support Creative IT renverra alors :

- un fichier « otp.key »
- une liste d'URL de paramétrage des secrets utilisateurs (un par identifiant administrateur)

Le fichier « otp.key » devra être copié dans le dossier « Creative IT » du serveur concerné.
Pour que les exécutables Creative IT utilisent ce fichier, ils doivent être redémarrés.
Le plus simple est donc de redémarrer le service QubesGuardian une fois que le fichier est en place pour que les services Qubes l'utilisent.

Chaque administrateur a 24H pour accéder à son URL, qui lui affichera un QRCode permettant de

paramétrer son application de gestion des OTP.

Pour générer des OTP, les utilisateurs peuvent utiliser l'application de leur choix, pourvu qu'elle soit compatible avec le protocole T-OTP.
Nous recommandons d'utiliser une application connue de gestion des OTP sur téléphone (ex : Google Authenticator, Free OTP, Authy, ...), dans laquelle il suffira de photographier le QRCode pour paramétrer une nouvelle authentification.

Pour accéder à un utilitaire d'administration protégé par AdminSec, il suffit de saisir son identifiant et le code OTP généré par l'application en utilisant l'authentification associé au serveur concerné (NB : dans ce cas, le challenge ne sert à rien).

Procédure pour gérer des administrateurs locaux

Un administrateur qui a un code OTP valide (ou un mastercode) peut gérer manuellement une liste d'identifiants autorisés pour l'administration d'un service donné.
Il faut se connecter sur la page http d'administration du service (généralement **/admin.sys**) puis cliquer sur *Configure OTP for admin pages*.
On peut alors ajouter/modifier/supprimer un identifiant autorisé à se connecter aux pages d'administration de ce service.

Quand on ajoute un identifiant, si on veut utiliser le même secret pour plusieurs services, on peut le préciser.
Sinon, si on ne précise pas de secret, le service en génère un automatiquement.

Il faut valider avec le service support le niveau de sécurité que vous souhaité :

- sécurité simple : un même utilisateur aura une seule authentification pour tous les serveurs sur lesquels il est déclaré
- sécurité normale : un même utilisateur aura une authentification différente pour les serveurs de PROD et de TEST
- sécurité renforcée : un même utilisateur aura des authentifications différentes pour chaque serveur

NB : il faut renforcer la sécurité si ne veut pas qu'un vol de secret d'un utilisateur sur un serveur ne compromette les autres serveurs.

Client: Créative IT

Prérequis : Être un admin qui puisse se connecter au serveur de Qubes

Objectifs: Personnaliser l'icône d'un site Qubes

Destinataires: Clients et prestataires

L'îcone d'un site web peut se configurer avec le « favicon ».

Dans le fichier de configuration server.cfg, ajuster l'option HTTPDirectory et la faire pointer vers un dossier local.
Dans ce dossier placer le fichier favicon.ico

Pour plus de détails voir

- Favicon sur wikipedia
- Favicon sur MDN (référence des outils de création d'un fichier favicon.ico)

A partir des versions datées 2022, les tâches dont la taille d'historique en HTML est trop importante ne sont plus affichées par défaut.

Il est possible d'ajuster la limite dans le fichier ini du Qubes.exe ou du QubesExpress.exe, cette limite est prise en compte tâche par tâche.

```
[Processes]
MaxPresentationHtmlSize=65536
```

Cette limite a été intégré comme mitigation de certains historiques de tâche intégrant des enregistrements de très gros fichier dans des variables, ce qui conduit à un HTML très complexe pouvant entraîner un blocage au niveau des navigateurs web, voire des crash.

Les variables restes accessibles en consultant par l'écran « consulter les variables ».

QubesExpress supporte le HTTP/2 à partir de Windows 2016, et le HTTP/3 à partir de Windows 2022, sous réserve des conditions suivantes:

- Le TLS (SSL) doit être actif, voir (Activer HTTPS pour Qubes)
- le SSO (si utilisé) doit être configuré sur un sous-domaine, avec le paramètre SSOBindDomain du server.cfg

Par exemple si le domaine principal est qubes.domain.net, le paramètre SSOBindDomain peut être défini à sso.qubes.domain.net

Le HTTP/2 et le HTTP/3 permettent d'améliorer les performances réseau du HTTP en introduisant le multiplexage et de optimisations au niveau de la latence (cf. HTTP/2 et HTTP/3)

- Ouvrir le gestionnaire de taches sur le serveur Qubes
- Aller sur l'onglet Détails
- Rechercher le service voulu (ex: QubesExpress.exe, QubesPeon.exe…)
- Faire un clique droit sur le service sélectionné, propriété et Détails
- Vous trouverez la version du fichier…

Le HTTPS est un prérequis pour activer les protocoles HTTP modernes, voir l'article support de HTTP/2 et HTTP/3.

Il est aussi recommandé très fortement d'avoir suivi une formation sécurité internet, et de ne pas juste dérouler une procédure d'installation de certificat HTTPS.
Toute erreur dans la manipulation d'un certificate peut entraîner de graves manquement à la sécurité, et de fait, invalider tout l'interêt d'utiliser un certificat.
Si les termes si dessous vous interpellent ou vous semblent être du chinois, n'allez pas plus long et contactez votre administrateur web.

Paramètres du serveur Qubes relatif à HTTPS

Le paramètres du server.cfg relatif à HTTPS sont les suivant.

- SSLEnabled=Y active le HTTPS
- SSLPort (optionnel) spécifié le port du HTTPS (par défaut 443, il est recommandé de ne pas le modifier)
- BindDomain spécifie le domaine du certificat HTTPS, il est recommandé de le définir afin de ne pas servir de certificat en « catch all » sur un port et une IP
- SSOBindDomain permet de spécifier un sous domaine pour le SSO s'il est utilisé (sans quoi HTTP/2 et HTTP/3 seront non disponibles)
- BindRelativeURI permet de spécifier un sous-chemin et une priorité pour le serveur web. Ce réglage permet à plusieurs serveurs web d'opérer sur le même domaine.

Il est aussi possible de spécifier plusieurs domaines, plusieurs sous chemins et plusieurs certificats avec l'option BindURLACLs, en indiquant une ou plusieurs urlacl séparées par des virgules.
Il est alors possible d'établir une hiérarchie de services QubesExpress, en configuration de failover ou de load balancing, au niveau domaine ou chemin d'URL.

Pour plus de détails, une documentation Microsoft est disponibles à Configuring HTTP and HTTPS.

Les modifications du server.cfg ne seront prise en compte qu'au redémarrage du service.

Installation du certificat en ligne de commande

Qubes utilise la même couche Microsoft http.sys que IIS et WCF.
La procédure officielle Microsoft en ligne de commande utilise netsh et httpcfg, elle est décrite sur

https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-configure-a-port-with-an-ssl-certificate

Cette approche est a préférer pour les déploiements, car elle evite d'exposer le certificat dans une fichier en clair.

Il n'est pas nécessaire de redémarrer les services Qubes pour une mise à jour de certificat.

Installation avec IIS Manager

Il est possible d'utiliser IIS Manager inclus dans Windows (cf. Installation Certificat SSL Cloudflare Origin qui décrit la procédure similaire pour l'intégration du certificat).
Il ne faut pas activer le site dans IIS (sans quoi il prendrait le pas sur QubesExpress), mais uniquement définir et paramétrer le site.

Il n'est pas nécessaire de redémarrer les services Qubes pour une mise à jour de certificat.

Installation historique avec httpsysmanager

La procédure ci-dessous est historique et utilise httpsysmanager (qui est un outils non maintenu)***, elle n'est pas recommandée pour les serveurs Windows 2016 et ultérieurs.***

1. Récupérer le fichier QubesUpdate.zip
2. Ouvrir le fichier zip, et aller dans le dossier httpsysmanager-bin-1.5 et copier le contenu de ce dossier dans Qubes\Bin\Tools
3. Lancer httpsysmanager.exe
4. Saisir l'IP du serveur dans la zone IP, ou 0.0.0.0 si le serveur doit être exposé sur toute les IPs.
5. Saisir le port (pour connaitre le port aller dans Qubes\Bin\=>qubesexpress, lancer maincfgfileditor.exe, saisir ssl dans la zone de texte et sélectionner sslenabled, puis cliquer sur la case à cocher, puis aller dans l'onglet sslport et voir le port renseigné (si le port est 0 donc ça sera le port par défaut))
6. sélectionner le certificat qui doit être au format .pfx
7. cliquer sur add certificat
8. redémarrer les services lorsque le certificat est en place