QuickFile

Guide d'administration

Version 1.1

QuickFile

Guide d'administration

Version 1.1

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 101.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Chapitre 1. Déploiement de IBM QuickFile en tant que dispositif virtuel

Si vous déployez IBM® QuickFile, veuillez lire les rubriques d'installation et de configuration avant de commencer le processus de déploiement.

QuickFile est déployé en tant que dispositif virtuel. L'avantage de cette approche est la facilité de distribuer, d'installer et de configurer le système. Après le déploiement, vous disposez d'une machine virtuelle qui peut être mise en fonction et utilisée pour héberger QuickFile. Une base de données est nécessaire pour utiliser le produit. La base de données par défaut est Derby et elle ne nécessite aucune configuration spéciale. Vous pouvez également utiliser IBM DB2 ou Oracle.

Si vous utilisez QuickFile dans un environnement hébergé, il n'y a pas besoin de déploiement. Un environnement hébergé est également connu comme étant un logiciel sous forme de services (SaaS).

Présentation de la haute disponibilité

La haute disponibilité est la configuration de deux instances QuickFile derrière un équilibreur de charge.

La haute disponibilité consiste en deux instances QuickFile contrôlées par un équilibreur de charge. L'équilibreur de charge est une méthode de mise en réseau d'ordinateurs qui distribue la charge de travail sur plusieurs ordinateurs. Cette méthode permet une utilisation optimale des ressources et maximise la capacité de traitement. Le service d'équilibrage de charge est fourni par un matériel ou un logiciel dédié, tel qu'un commutateur multicouches ou un serveur DNS. QuickFile prend en charge la configuration d'une haute disponibilité active et passive. Lorsque vous configurez l'équilibreur de charge, une instance est configurée comme instance primaire (active) et une autre configurée en tant qu'instance secondaire (passive). La primaire est pondérée plus lourdement pour qu'elle accepte tout le trafic à moins qu'elle ne soit marquée comme inactive par l'équilibreur de charge.

Restriction : QuickFile ne prend pas en charge les paramètres de sessions difficiles ou de persistance des sessions.

Configurez l'équilibreur de charge et identifiez les instances primaire et secondaire. Dans un environnement de production, l'instance primaire envoie et reçoit des fichiers. Si l'instance primaire n'est pas disponible, l'équilibreur de charge bascule immédiatement le travail sur l'instance secondaire.

Les comportements spécifiques suivants ont lieu comme résultat du basculement d'une instance primaire à une instance secondaire :

- Si vous utilisez la fonction Advanced File Transfer, les instances de haute disponibilité répondent de la façon suivante :
  - Si l'instance primaire perd sa connexion, le transfert de fichier est interrompu. Le transfert est disponible sur l'instance secondaire et s'affiche comme étant en pause sur cette instance. Vous pouvez reprendre le transfert de fichier à partir de l'instance secondaire après vous être connecté.

- Si l'instance primaire devient disponible lorsque le transfert sur l'instance secondaire est en cours, il est interrompu. L'état du transfert sur l'instance primaire s'affiche comme étant en pause. Après la connexion de l'utilisateur, il peut reprendre le transfert.

- Si vous utilisez le transfert de fichier de base, les instances répondent de la façon suivante :
  - Si l'utilisateur envoie un transfert et l'instance primaire perd sa connexion avant la fin du transfert, l'instance primaire n'est pas disponible. L'utilisateur doit se connecter sur l'instance secondaire et renvoyer le transfert de fichier.
  - Si l'instance primaire devient disponible, le transfert de fichier qui a commencé sur l'instance secondaire se termine. L'utilisateur doit redémarrer l'instance primaire et se connecter pour l'utiliser.

Configuration de QuickFile pour la haute disponibilité

Utilisez les informations pour configurer la haute disponibilité de QuickFile. La haute disponibilité correspond a deux ou plusieurs dispositifs QuickFile qui partagent une base de données externe et un système de fichiers NFS, derrière un équilibreur de charge. Déployez deux fichiers OVA. Ensuite, configurez les deux instances de la haute disponibilité.

Avant de commencer

Pour configurer la haute disponibilité pour QuickFile, les deux instances doivent être configurées avec les mêmes informations, identifiées dans la liste suivante :

- Une base de données externe que les deux instances QuickFile partagent
- Un serveur NFS pour le stockage de fichiers que les deux instances partagent
- L'adresse IP externe et le port de l'équilibreur de charge

L'équilibreur de charge achemine le trafic sur le noeud primaire. Si le noeud primaire tombe, l'équilibreur de charge bascule sur le noeud secondaire et y achemine le trafic. Lorsque l'équilibreur de charge détecte que le noeud primaire est sauvegarder, il réachemine le trafic sur le noeud primaire. Utilisez le même fichier de propriétés pour chaque déploiement.

Important : Lorsque vous effectuez des modifications dans la configuration de QuickFile, vous devez vous connecter directement sur chaque instance. Ne vous connectez pas via l'équilibreur de charge. Les mêmes modifications doivent être effectuées sur les deux instances

Pourquoi et quand exécuter cette tâche

Complétez la procédure suivante pour définir les instances de QuickFile pour la haute disponibilité :

Procédure

1. Téléchargez le fichier OVA.
2. Téléchargez les scripts de base de données pour le fichier OVA.
3. Utilisez le logiciel client de base de données, tel que dbWiz ou Squirrel, pour exécuter les scripts 0, 1, 2 et 3. Les scripts créent les tables de base de données et chargent les données par défaut.

4. Sur un système auquel OVA peut accéder, créez un fichier de propriétés avec la configuration de votre instance de base de données. Incluez la configuration NFS, l'adresse IP externe et le port utilisé dans la configuration de l'équilibreur de charge.
5. Déployez OVA.
6. Connectez-vous à l'appareil.
7. Entrez **Y** pour définir l'adresse IP.
8. Entrez **Y** pour définir le DNS.
9. Entrez **Y** pour importez le fichier de propriétés que vous avez créé.
10. Si vous le souhaitez, modifiez le mot de passe de l'administrateur. Ce mot de passe s'applique seulement à cette instance. Vous devez modifier le mot de passe de la seconde instance pour conserver la synchronisation des deux emplacements.

Résultats

La configuration prend quelques minutes. Puis, QuickFile est disponible.

Planification de votre déploiement

Lors de la phase de planification de votre déploiement, vous devez impérativement définir le type de système de fichiers. Vous pouvez planifier un système de fichiers local ou une implémentation du système NFS. Vous ne pouvez pas modifier le type de système de fichiers après le déploiement. Vous devez effectuer un nouveau déploiement.

Lors de la phase de planification de votre déploiement, vous devez sélectionner l'un des types de systèmes de fichiers suivants :

- Système de fichiers local
- Système NFS (Network file System)

Vous ne pouvez pas modifier le type de système de fichiers une fois le déploiement terminé car certains fichiers risqueraient de ne pas pouvoir être extraits ou supprimés.

Pour bénéficier d'une haute disponibilité, vous devez disposer d'un serveur NFS pour le stockage des fichiers partagés entre les deux instances.

Préparation pour l'utilisation de la base de données IBM DB2

Vous pouvez utiliser la base de données DB2 à la place de la base de données par défaut lorsque vous déployez QuickFile. Pour utiliser DB2, vous devez créer un espace table temporaire. Ensuite, déployez le logiciel, exécutez les scripts et créez le fichier de propriétés.

Pour configurer la base de données DB2 pour l'utiliser avec QuickFile, complétez les tâches suivantes dans l'instance DB2 :

- Créez un espace table temporaire système de 32 Ko
- Créez un pool de mémoire tampon système de 32 Ko
- Créez un pool de mémoire tampon de 16 Ko
- Créez un espace table de 16 Ko

Pour configurer QuickFile pour utiliser DB2, complétez les tâches suivantes après avoir déployé le produit :

1. Téléchargez les scripts de la base de données à partir du site suivant : IBM QuickFile Database Scripts.
2. Exécutez les scripts suivants, dans l'ordre dans lequel ils sont répertoriés dans le tableau suivant :

Script	Description
`0_createSchemaObjects.sql`	Crée des tables, des index et des contraintes
`1_loadDefaultSystemData.sql`	Charge les enregistrements de données système
`2_loadDefaultGroupsAndUsers.sql`	Charge les enregistrements de données de support des groupes et des utilisateurs
`3_loadDefaultConfigurationData_ova.sql`	Charge les enregistrements des données de configuration

3. Personnalisez le fichier de propriétés pour spécifier que DB2 est utilisé comme base de données. Voir «Personnalisation de votre déploiement avec un fichier de propriétés», à la page 8 pour les instructions.
4. Déployez le produit. Voir «Déploiement de QuickFile en tant que dispositif virtuel», à la page 5.

Conseil : Si vous ne souhaitez pas utiliser cette base de données, exécutez le script appelé **`9_dropSchemaObjects.sql`**. Il supprime toutes les tables, les index et les données QuickFile. Assurez-vous que vous n'avez pas besoin des données avant d'exécuter ce script.

Préparation pour l'utilisation de la base de données Oracle

Vous pouvez utiliser Oracle comme base de données à la place d'une base de données par défaut lorsque vous déployez QuickFile. Pour utiliser Oracle, activez l'utilisation des autorisations spéciales, exécutez les scripts de base de données et personnalisez les fichiers de propriétés.

Pour configurer Oracle afin d'utiliser les autorisations spéciales avec QuickFile, exécutez les commandes suivantes en tant qu'utilisateur SYS. Remplacez *<myOracleUserId>* avec l'ID utilisateur de la connexion Oracle.

- grant select on `pending_trans$` to *<myOracleUserId>*;
- grant select on `pending_trans$` to *<myOracleUserId>*;
- grant select on `dba_2pc_pending` to *<myOracleUserId>*;
- grant execute on `dbms_xa` to *<myOracleUserId>*;

Pour configurer QuickFile pour utiliser la base de données Oracle, complétez les tâches suivantes après avoir déployé le produit :

1. Téléchargez les scripts de la base de données à partir du site suivant : IBM QuickFile Database Scripts.
2. Exécutez les scripts suivants, dans l'ordre dans lequel ils sont répertoriés dans le tableau suivant :

Script	Description
`0_createSchemaObjects.sql`	Crée les tables, les index et les contraintes.

Script	Description
1_loadDefaultSystemData.sql	Charge les enregistrements de données système.
2_loadDefaultGroupsAndUsers.sql	Charge les enregistrements de données de support des groupes et des utilisateurs.
3_loadDefaultConfigurationData_ova.sql	Charge les enregistrements des données de configuration.

3. Personnalisez le fichier de propriétés pour spécifier qu'Oracle est utilisé comme base de données. Voir «Personnalisation de votre déploiement avec un fichier de propriétés», à la page 8 pour les instructions.

Conseil : Si vous déterminez que vous ne souhaitez pas utiliser cette base de données, exécutez le script appelé **9_dropSchemaObjects.sql**. Il supprime toutes les tables, les index et les données QuickFile. Assurez-vous que vous n'avez pas besoin des données avant d'exécuter ce script.

Déploiement de QuickFile en tant que dispositif virtuel

Pour simplifier le déploiement et l'administration, QuickFile est livré en tant que dispositif virtuel et est déployé sur l'hyperviseur VMware vSphere (ESXi).

Avant de commencer

Avant de déployer QuickFile, installez un hyperviseur ESXi. ESXi est un hyperviseur complet qui s'exécute directement sur le matériel. Le guide de compatibilité VMware répertorie les systèmes d'exploitation pris en charge pour ESXi. Assurez-vous que la version vSphere que vous utilisez pour le déploiement correspond à la version ESXi.

Important : Assurez-vous que votre hyperviseur est configuré pour s'exécuter sur un serveur NTP.

Pour déployer un dispositif virtuel, vous avez besoin du client VMware vSphere. Le client se connecte à l'hyperviseur ou au groupe d'hyperviseurs, géré par un centre virtuel. Allez sur le site Web de VMware et téléchargez le client VMware vSphere. Suivez les instructions du site Web pour installer le client.

Restriction : Les magasins de données ESXi doivent prendre en charge au moins 2 To de stockage. L'espace disque minimal requis pour l'hôte ESXi est de 100 Go. Si les magasins de données ne prennent pas en charge 2 To de stockage avec un déploiement interne (pas de serveur NFS), un risque de surcharge de VMware existe. Vous devez vérifier que QuickFile ne dépasse pas la capacité de votre magasin de données.

Pour déployer un dispositif virtuel de 2 To, la taille de bloc du magasin de données doit prendre en charge 2 To, même en cas d'allocation de ressources à la demande. Pour modifier la taille de bloc, supprimez le magasin de données et créez-en un nouveau. Les tailles de bloc suivantes sont requises :

- Pour ESXi 5.0 et 5.1 avec un magasin de données VMFS5, la taille de bloc est de 1 Mo
- Pour ESX/ESXi 4.1 et ESXi 5.*x* avec un magasin de données VMFS3, la taille de bloc est de 8 Mo.

Important : Les ports suivants sont ouverts sur un dispositif virtuel QuickFile :

Protocole	Port
WebSphere MQ	1414
HTTP	9080
HTTPS	9443 : ce port est ouvert seulement si la connexion SSL est activée.

Pourquoi et quand exécuter cette tâche

Après avoir installé le client VMware vSphere, complétez la procédure suivante pour commencer votre déploiement :

Procédure

1. Rassemblez les informations suivantes :
   - Adresse IP à utiliser pour le dispositif
   - Si vous le souhaitez, le nom d'hôte complet à utiliser pour le dispositif

     ATTENTION :
     Si vous indiquez un nom d'hôte, il doit être enregistré avec votre serveur DNS. Enregistrer le nom d'hôte permet aux clients distants et au dispositif de trouver le nom d'hôte.
   - Adresse IP de votre passerelle
   - Adresse IP de votre serveur DNS
   - Masque sous-réseau au format CIDR (par exemple, 24 est le format CIDR du sous-réseau 255.255.255.0)
   - Adresse IP de votre serveur NTP. Vous devez indiquer le même serveur NTP que celui qui est utilisé par l'hyperviseur sous-jacent.
   - Fuseau horaire au format POSIX (par exemple, `EST5EDT` est l'heure normale de l'est américain au format POSIX)
   - Nom de serveur SMTP ou adresse IP du serveur à utiliser pour envoyer un e-mail. L'e-mail notifie les utilisateurs quand les fichiers sont envoyés ou reçus.
   - Mot de passe à utiliser pour administrer le dispositif
2. Téléchargez l'archive nommée **`QuickFile-1.1.zip`**.
3. Procédez à l'extraction de l'archive. Le fichier nommé **`QuickFile-1.1.ova`** est extrait. Le fichier contient le dispositif QuickFile.
4. Démarrez le serveur ESXi.
5. Pour vous connecter à l'hyperviseur ou à vCenter, complétez les étapes suivantes :
   a. Démarrez le client VMware vSphere
   b. Entrez l'adresse IP hôte
   c. Entrez un nom d'utilisateur avec les droits d'accès complet et le mot de passe
   d. Cliquez sur **Connexion**.
6. Choisissez **Fichier** > **Déployer modèle OVF** du menu principal du client vSphere.
7. Lorsque vous y êtes invité, entrez l'emplacement du fichier que vous avez extrait.

8. Cliquez sur **Suivant** et acceptez les valeurs par défaut sur les pages suivantes avec les exceptions suivantes :
   - Sur la page Format de disque, sélectionnez **Allocation de ressources à la demande**
   - Sur la dernière page, cochez **Mettre sous tension après déploiement** et cliquez sur **Terminer**.
9. Attendez que le déploiement et la mise sous tension se terminent. Le processus prend plusieurs minutes. Le fichier OVA est déployé.
10. À l'aide du client vSphere, allez dans l'onglet **Console** pour voir la ligne de commande QuickFile. Sur cette ligne de commande, une invite de connexion s'affiche. Si ce n'est pas le cas, appuyez sur Entrée.
11. Lorsque vous êtes invité à vous connecter, entrez `admin` pour le nom d'utilisateur et `admin` pour le mot de passe. Lorsque vous y êtes invité, indiquez les informations que vous avez récupérées à l'étape 1 dans les zones suivantes.
    - Adresse IP à utiliser pour le dispositif
    - Le masque de sous-réseau du dispositif
    - La passerelle par défaut du dispositif
12. Confirmez les valeurs saisies.
13. Lorsque vous êtes invité à définir le serveur DNS, entrez `Y`, entrez l'adresse IP du serveur DNS. Pour spécifier plusieurs serveurs DNS, séparez chaque adresse IP avec un espace. Confirmez votre saisie.
14. Pour modifier la base de données en DB2 ou Oracle, ou pour indiquer un système de fichiers NFS, téléchargez un fichier de propriétés. Pour personnaliser l'une de ces variables, entrez `Y`. Voir «Personnalisation de votre déploiement avec un fichier de propriétés», à la page 8. Sinon, entrez `N`.

    Une fois que vous avez fourni toutes les informations, le dispositif se configure lui-même. Ce processus prend plusieurs minutes. Un message s'affiche indiquant que l'application est disponible à l'adresse `http://`*`ip address`*`:9080/quickfile/login.html`. Attendez quelques minutes avant d'utiliser le dispositif.
15. Lorsque vous êtes invité à modifier le mot de passe administrateur, entrez le nouveau mot de passe.

    Important : Pour protéger le système contre un accès externe, définissez un mot de passe fiable.
16. Démarrez un navigateur Web et entrez `http://`*`ip address`*`:9080/quickfile/login.html`
17. Connectez-vous à QuickFile en tant qu'administrateur.

    Important : Le nom de l'administrateur par défaut est `admin` et le mot de passe est `admin`. Si vous avez modifié le mot de passe dans une des étapes précédentes, entrez le nouveau mot de passe dans cette zone.
18. Accédez aux pages de configuration administrative du dispositif en cliquant sur **Configuration** dans le menu.
19. Si vous utilisez la base de données par défaut, définissez votre fuseau horaire dans l'onglet **Paramètres régionaux**. Cliquez sur **Enregistrer**.
20. Si vous avez modifié le fuseau horaire, vous êtes invité à redémarrer l'application. Cliquez sur **Oui** pour redémarrer le dispositif.

ATTENTION :
Ne manipulez pas la base de données en dehors de l'application. Manipuler la base de données en dehors de QuickFile menace l'intégrité et la sécurité des données du produit.

Personnalisation de votre déploiement avec un fichier de propriétés

Dans le processus de déploiement, vous pouvez télécharger un fichier de propriétés pour personnaliser votre déploiement.

Le fichier de propriétés peut personnaliser QuickFile avec les actions suivantes :

- Activer une base de données DB2 ou Oracle à la place de la base de données par défaut
- Configurer l'utilisation d'un système de fichiers NFS externe
- Configurer un serveur de messagerie
- Modifier le fuseau horaire
- Configurer LDAP dans QuickFile

Vous pouvez créer plus d'un fichier de propriétés pour définir plus d'une configuration. Pour personnaliser une fonction, modifiez les valeurs des propriétés appropriées et enregistrez le fichier.

Le fichier de propriétés doit présenter les caractéristiques suivantes :

- Un fichier en texte uniquement sans retour masqué ou autre caractère
- Stocké dans un emplacement auquel l'ordinateur sur lequel vous déployez le dispositif peut accéder
- codé UTF-8
- Accessible pour FTP, SCP ou HTTP

Vous pouvez préciser l'emplacement d'un fichier de propriétés pendant le déploiement.

A faire : Toutes les lignes qui commencent par # sont traitées comme des commentaires.

Le tableau suivant identifie les propriétés de configuration :

Tableau 1. Propriétés du serveur de messagerie électronique

Propriété	Description	Relancer
`smtp.server`	Nom d'hôte ou adresse IP du serveur SMTP.	oui
`smtp.port`	Numéro de port du serveur SMTP.	oui
`smtp.user`	Nom d'utilisateur SMTP.	oui
`smtp.password`	Mot de passe SMTP.	oui
`smtp.secure.mode`	Mode de sécurité des sessions SMTP. Les valeurs valides sont SSL, TLS ou laissez vide pour les sessions non chiffrées.	oui

Tableau 2. Propriétés du nom d'hôte

Propriété	Description	Relancer
`external.server.host`	Nom d'hôte externe ou adresse IP du dispositif. Utilisé avec des équilibreurs de charge ou des proxys VMware.	non

Tableau 2. Propriétés du nom d'hôte (suite)

Propriété	Description	Relancer
`external.server.port`	Port externe du dispositif. Utilisé avec des équilibreurs de charge ou des proxys VMware.	non
`external.server.port.ssl`	Port SSL externe du dispositif. Utilisé avec des équilibreurs de charge ou des proxys VMware.	non

Tableau 3. Propriétés du serveur

Propriété	Description	Relancer
`dns.servers`	Adresses IP pour les serveurs DNS. Adresses multiples sont délimitées par des points-virgules.	non
`ntp.servers`	Adresses IP du serveur NTP. Seul un serveur NTP est pris en charge. **Important :** Indiquez le même serveur NTP utilisé par l'hyperviseur sous-jacent.	non
`timezone`	Fuseau horaire du dispositif en cours.	oui

Tableau 4. Propriétés du système NFS

Propriété	Description	Relancer
`nfs.server`	Nom d'hôte ou adresse IP du serveur NFS. **Important :** Ne remplacez pas une implémentation en système de fichiers local existante par une implémentation en système NFS.	oui
`nfs.directory`	Chemin du répertoire exporté du système distant à monter comme un système de fichiers sur le dispositif.	oui
`nfs.reset`	S'il est défini sur `true`, démontez l'annuaire NFS et réinitialisez les zones de DB suivantes sur les valeurs par défaut du système local : • `app.repository.dir` • `app.photos.dir` • `app.email.template.dir` Si défini sur `false`, entraîne l'annuaire exporté à être monté sur NFS.	oui

Tableau 5. Propriétés de la base de données

Propriété	Description	Relancer
`db.type`	Type de base de données (DB2 ou Oracle). Si vous utilisez la base de données Derby par défaut, aucun type de base de données n'est requis. Les valeurs par défaut de l'application s'appliquent à Derby, à moins que vous ne définissiez cette valeur.	oui
`db.userid`	Données d'identification utilisateur pour connexion à la BD.	oui
`db.password`	Données d'identification pour ouverture de session BD - mot de passe.	oui
`db.db2.server`	DB2 uniquement. Nom d'hôte ou adresse IP pour le serveur de base de données.	oui
`db.db2.port`	DB2 uniquement. Numéro de port du serveur de base de données.	oui
`db.db2.name`	DB2 uniquement. Nom de base de données.	oui
`db.db2.schema`	DB2 uniquement. Schéma.	oui

Tableau 5. Propriétés de la base de données (suite)

Propriété	Description	Relancer
db.oracle.url	Oracle uniquement. Chaîne URL de connexion	oui

Tableau 6. Propriétés LDAP

Propriété	Description	Relancer
ldap.enabled	true = LDAP activé; false = LDAP désactivé.	non
ldap.server.host	Nom d'hôte ou adresse IP du serveur LDAP. Zone de texte. Obligatoire (non implicite).	non
ldap.server.port	Numéro de port du serveur LDAP. Champ de texte numérique. Par défaut = 636. Les valeurs admises sont comprises entre 1 et 65535.	non
ldap.user.base.dn	Noeud parent où les utilisateurs sont stockés dans le serveur LDAP. Zone de texte. Obligatoire (non implicite).	non
ldap.group.base.dn	Noeud parent où les groupes sont stockés dans le serveur LDAP. Zone de texte. Obligatoire (non implicite).	non
ldap.user.search.filter	Filtre de recherche pour les utilisateurs. Zone de texte. La valeur par défaut est (|(objectClass=user) (objectClass=person) (objectClass=inetOrgPerson) (objectClass=organizationalPerson))	non
ldap.group.search.filter	Filtre de recherche pour les groupes. Zone de texte. La valeur par défaut est (|(objectClass=group) (objectClass=groupOfNames) (objectClass=groupOfUniqueNames))	non
ldap.protocol	Protocole SSL. Obligatoire. Valeurs admises : ldap pour créer une connexion claire au serveur LDAP, ldaps pour créer une connexion SSL au serveur LDAP.	non
ldap.member.attribute	Chaîne représentant une matrice des noms d'attribut. Chaque chaîne indique le nom d'un attribut dénotant l'appartenance au groupe.	non
ldap.service.principal	Nom distinct complet d'un serveur LDAP qui peut chercher dans l'annulaire. Zone de texte. Obligatoire (non implicite).	non
ldap.service.principal.password	Mot de passe du nom principal de service. Zone de texte. Obligatoire (non implicite).	non
ldap.authorized.groups	Chaîne représentant une matrice de chaînes. Chaque chaîne indique le nom distinctif d'un groupe LDAP qui contient les utilisateurs autorisés à accéder au système QuickFile. Par exemple : ["cn=Testers,ou=User Groups,ou=QFad,DC=AIXTST,DC=LDAP"]	non
ldap.email.attribute	Chaîne représentant une matrice des noms d'attribut. Chaque chaîne spécifie le nom d'un attribut dans une classe d'utilisateur qui indique une adresse e-mail. Obligatoire. La valeur par défaut est ["mail","userPrincipalName", "email","emailAddress"].	non

Tableau 7. Propriétés de l'application

Propriété	Description	Relancer
sys.admin.email	Adresse e-mail de l'administrateur système.	non

Tableau 7. Propriétés de l'application (suite)

Propriété	Description	Relancer
app.sender.email	Adresse e-mail du compte « sans réponse ». Cette adresse e-mail est utilisée pour les notifications par e-mail envoyées par QuickFile.	non
sessioninvalidationtimeout	Définissez le temps d'inactivité d'une session avant qu'elle ne soit fermée. Définissez les valeurs entre 2 et 1440 minutes. La valeur par défaut de 30 minutes est utilisée si aucune valeur n'est fournie. Elle est également utilisée si une valeur non valide, comme un nombre en dehors de la plage valide ou un valeur non numérique, est fournie.	oui

Exemple de fichier de propriétés

L'exemple de fichier de propriétés suivant indique l'emplacement d'un système de fichiers NFS et l'emplacement d'une base de données DB2. Les informations de la base de données Oracle sont mis en commentaire. Définissez votre fichier de propriétés avec les valeurs adaptées à votre déploiement.

```
nfs.server=myserver.example.org
nfs.directory=/localhome/bsmith/NFSdatadirectory
nfs.reset=false

db.type=DB2
db.userid=bsmith
db.password=password
db.db2.server=myDB2server.example.org
db.db2.port=50001
db.db2.name=QUICKFILE
db.db2.schema=QUICKFILE

#db.type=Oracle
#db.userid=cjones
#db.password=password2
#db.oracle.url=jdbc:oracle:thin:@myOracleDBserver.example.org:1522/DEV11R1
```

Pour indiquer un serveur NFS, supprimez le # au début de chaque ligne du premier paragraphe. Indiquez le nom de votre serveur NFS avec le répertoire dans lequel les données NFS doivent être stockées. Si vous ne souhaitez pas spécifier de serveur NFS, mettez ces lignes en commentaire en ajoutant un # au début de chaque ligne.

Pour spécifier une base de données Oracle, mettez les lignes DB2 en commentaire. Ensuite, supprimez la mise en commentaire pour les lignes de la base de données Oracle et donnez les valeurs qui appartiennent à votre base de données Oracle.

Réglage de l'environnement

Réglez votre environnement de manière à améliorer les performances en fonction du type de transactions que vous prenez en charge et des exigences de votre société. Réglez certaines fonctions en modifiant les valeurs dans le fichier de propriétés.

Surveillez les performances de votre système et les caractéristiques des fichiers transférés. Pour régler une fonction, modifiez les valeurs des propriétés appropriées et enregistrez le fichier.

Un fichier de propriétés doit être un fichier texte uniquement sans renvoi masqué ou d'autres caractères. Il doit être stocké sur un emplacement auquel l'ordinateur sur lequel vous déployez le dispositif peut accéder. Il doit être codé en UTF-8 et accessible pour FTP, SCP ou HTTP. Vous pouvez préciser l'emplacement d'un fichier de propriétés pendant le déploiement.

A faire : Toutes les lignes qui commencent par # sont traitées comme des commentaires.

Le tableau suivant identifie les propriétés de configuration :

Propriété	Description
`channel.http.inbound.readtimeout`	Combien de secondes le canal de transport HTTP attend pour qu'une demande de lecture se termine sur un connecteur après la première lecture. La lecture a lieu dans le corps de la demande de lecture, telle qu'un POST. Elle peut avoir lieu dans les en-têtes, si tous les en-têtes ne sont pas lus lors de la première lecture. Par défaut, la valeur est 60 secondes.
`channel.http.inbound.writetimeout`	Combien de secondes le canal de transport HTTP attend pour chaque portion de données de réponse à transmettre. Ce délai d'attente a lieu seulement dans les cas où les écritures se décalent sur les nouvelles demandes. Cette situation peut avoir lieu lorsqu'un client a un débit de données bas ou la carte d'interface réseau est saturée avec un trafic E/S. Si les clients nécessitent plus de 300 secondes pour recevoir des données en cours d'écriture, modifiez la valeur spécifiée de ce paramètre. Certains clients nécessitent plus de 300 secondes pour recevoir les données qui leur sont envoyées. Pour vous assurer qu'ils peuvent recevoir toutes les données, modifiez la valeur de ce paramètre. Assurez-vous que la longueur est suffisante pour toutes les données à recevoir. Si vous modifiez la valeur de ce paramètre, assurez-vous que la nouvelle valeur protège toujours le serveur des clients malveillants. Par défaut, la valeur est 60 secondes.
`channel.http.inbound.persistenttimeout`	Combien de secondes le canal de transport HTTP octroie à un connecteur pour qu'il reste en veille entre les demandes. La valeur par défaut est de 30 secondes

Activation de la purge d'événements

Activez la purge d'événements pour conserver la performance de votre système.

Pourquoi et quand exécuter cette tâche

La purge des événements est suspendue par défaut. Pour conserver la performance, reprenez **PurgeEvents** quand vous définissez initialement votre installation :

Procédure

1. Dans le menu **Administration**, sélectionnez **Règles** et cliquez sur l'onglet **Plannings**.
2. Cliquez sur **Afficher toutes les tâches**. Quand vous installez QuickFile pour la première fois, le statut de la tâche **PurgeEvents** est défini sur **Suspendu**.
3. Pour lancer la purge des événements système, sélectionnez **Reprendre** dans la case de sélection pour **PurgeEvents**. Par défaut, la tâche s'exécute toutes les semaines le dimanche à minuit pour purger les événements antérieurs à 30 jours. L'étiquette est modifiée sur **Planifiée**.

Que faire ensuite

Pour plus d'options, voir «Configuration de la purge des événements», à la page 64.

Personnalisation de l'image de marque du produit pour afficher les informations de la société

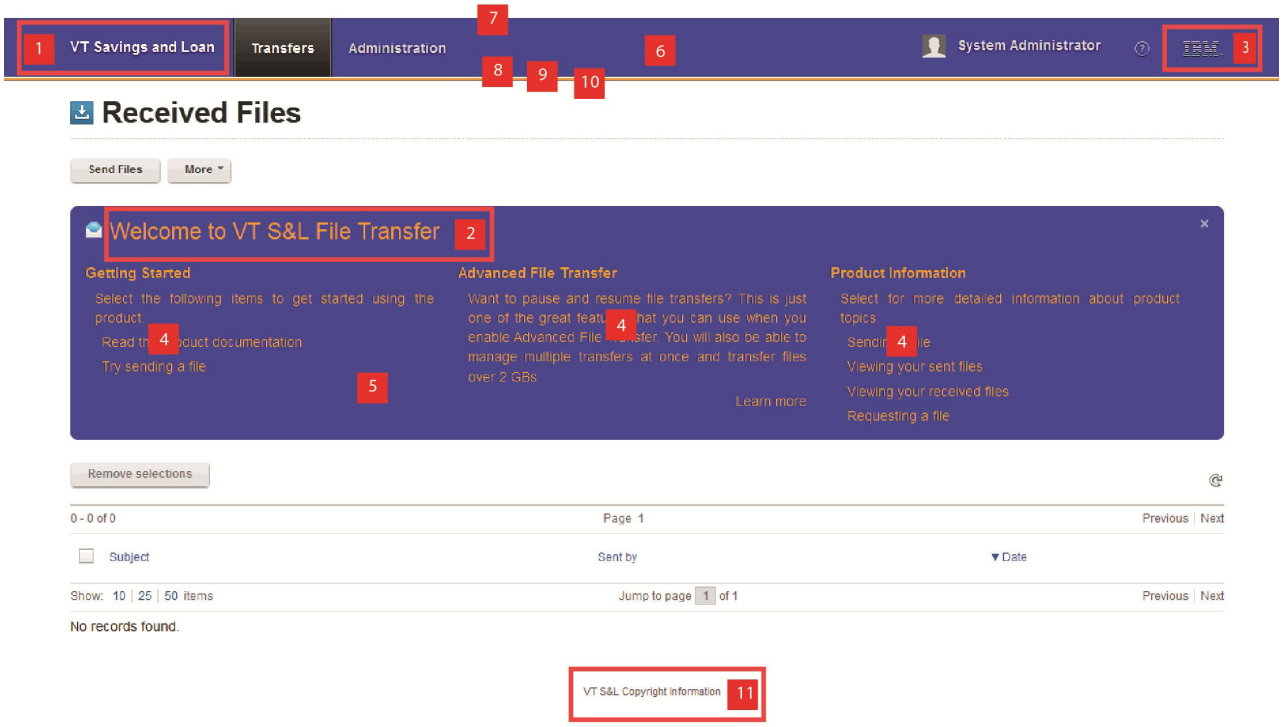
Vous pouvez personnaliser QuickFile pour afficher les informations de votre société sur les pages et les notifications par e-mail de QuickFile. Vous pouvez personnaliser le nom de la société, le message de bienvenue, les couleurs, le logo et la déclaration de la marque.

Complétez les étapes suivantes pour personnaliser chaque page et notification par e-mail de QuickFile pour afficher les informations de votre société :

1. Créez un fichier texte appelé `ui-branding_en_US.properties` et ajoutez les propriétés suivantes :

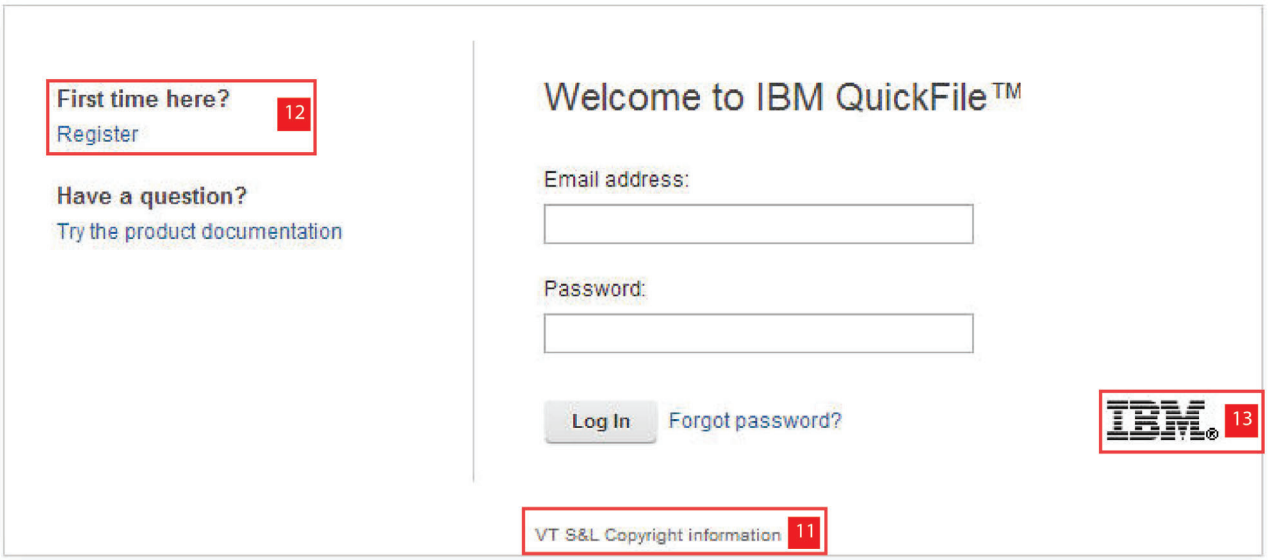
   Conseil : Si vous ne souhaitez pas personnaliser une propriété, laissez vide la valeur de la propriété. Par exemple, pour utiliser la couleur par défaut de la couleur du diviseur Bienvenue, définissez **`welcomeDividerColor=`**. La valeur par défaut, noire, est utilisée.

   Conseil : Pour supprimer toute référence à la marque sur la page, ne définissez aucune valeur du fichier`ui-branding_en_US.properties`.



Propriété	Valeurs valides
1 **productLongName**	Nom complet du produit à afficher dans l'interface, par exemple, IBM QuickFile.
12 **showRegistration**	Détermine si le lien d'inscription est affiché sur la page de connexion. Les valeurs valides sont true pour afficher le lien d'inscription ou false pour supprimer le lien d'inscription de la page de connexion. Entrez la valeur de cette zone, true ou false, en minuscules.
2 **welcomeMessage**	Message de bienvenue qui s'affiche sur la page Login et la bannière Welcome (par exemple : Welcome to VT S&L File Transfer).
3 **bannerLogoImage**	Graphique s'affichant dans le bannière de chaque page. Le logo de la bannière peut comporter jusqu'à 60 pixels en hauteur et 300 pixels en largeur. Spécifiez le nom du fichier graphique pour cette valeur. Les types de fichiers graphique sont : .jpg, .gif, ou .png.
13 **welcomeLogoImage**	Graphiques à afficher comme logo de la société. Le logo d'accueil peut comporter jusqu'à 60 pixels en hauteur et 200 pixels en largeur. Spécifiez le nom du fichier graphique pour cette valeur. Les types de fichiers graphique sont : .jpg, .gif, ou .png.
4 **welcomeDividerTextColor**	Couleur du texte sur la bannière de bienvenue et initialement affichée sur la fiche Transferts. Utilisez une valeur hexadécimale (par exemple : #ED7818) ou un nom de couleur (par exemple : vert).
5 **welcomeDividerColor**	La couleur d'arrière-plan sur la bannière de bienvenue ou le diviseur de page affichée au-dessus de la fiche de fichiers. Utilisez une valeur hexadécimale (par exemple : #ED7818) ou un nom de couleur (par exemple : vert).
6 **mainBannerColor**	Couleur utilisée sur la bannière. Utilisez une valeur hexadécimale (par exemple : #ED7818) ou un nom de couleur (par exemple : vert).
7 **mainBannerTopBorderColor**	Couleur utilisée pour la bordure supérieure de la bannière. Utilisez une valeur hexadécimale (par exemple : #ED7818) ou un nom de couleur (par exemple : vert).
8 **mainBannerBottomBorderColor**	Couleur utilisée pour la bordure inférieure de la bannière. Utilisez une valeur hexadécimale (par exemple : #ED7818) ou un nom de couleur (par exemple : vert).

Propriété	Valeurs valides
9 **subBannerColor**	Couleur utilisée sur la sous-bannière, la petite bannière sous la bannière principale. Utilisez une valeur hexadécimale (par exemple : #ED7818) ou un nom de couleur (par exemple : vert).
10 **subBannerBottomBorderColor**	Couleur utilisée sur la bordure inférieure de la petite bannière affichée sous la bannière principale. Utilisez une valeur hexadécimale (par exemple : #ED7818) ou un nom de couleur (par exemple : vert).
11 **copyright**	Texte à afficher dans la propriété du copyright, par exemple, (C) COPYRIGHT Zeta Hospital 2012. Ce texte apparaît sur chaque page de l'interface, y compris su r la page d'accueil.



2. Pour personnaliser les notifications par e-mail avec les informations de votre société, créez un fichier texte appelé `email_defaults_en_US.properties` et ajoutez les propriétés suivantes :

   Conseil : Pour utiliser les valeurs par défaut d'une propriété, laissez la valeur vide. Par exemple, pour utiliser la couleur par défaut sur le nom de votre société, définissez **companyNameColor=**. La valeur par défaut, noire, est utilisée.

   Conseil : Pour supprimer toute référence à la marque dans les notifications par e-mail, ne définissez aucune valeur dans le fichier `email_defaults_en_US.properties`.

Propriété	Description
companyName	Nom de la société à afficher dans la notification par e-mail. La valeur par défaut est IBM QuickFile.
companyLogo	Fichier graphique, au format jpeg, à afficher au dessus du sujet de l'e-mail. La valeur par défaut est `company.jpeg`. La taille maximum permise est 25K.
companyNameColor	Couleur de police à utiliser pour le nom de la société. Indiquez les couleurs à l'aide des codes couleur HTML (par exemple : #E01B6A) ou en spécifiant le nom de la couleur (par exemple : bleu).
emailTitle	Le titre de toutes les notifications par e-mail.

Propriété	Description
iHeight	Hauteur du logo de la société. La valeur est définie en pixels.
iWidth	Largeur du logo de la société. La valeur est définie en pixels.

3. Connectez-vous à QuickFile en tant qu'administrateur.
4. Dans la page QuickFile **Bienvenue**, cliquez sur **Envoyer fichiers**.
5. Dans la zone **Envoyer à**, entrez le nom d'un destinataire. Utilisez le format : `username@domainname`, par exemple `john.doe@company.com`.

   Remarque : Le nom du destinataire n'est pas utilisé. Les fichiers sont envoyés vers un emplacement local lorsque vous entrez personnalisation comme valeur dans la zone Sujet.
6. Dans la zone **Sujet**, entrez personnalisation.
7. Sélectionnez les fichiers `.properties` que vous avez créés et les fichiers graphiques à utiliser pour la page d'accueil, le logo de la bannière et le logo de la société.
8. Cliquez sur **Envoyer**. Les fichiers que vous avez créés et les fichiers graphiques du logo sont envoyés au serveur et définissent la personnalisation des pages du produit et des notifications par e-mail.

Conseil : Les modifications apportées prennent effet une fois les fichiers `.properties` et les fichiers graphiques envoyés au serveur. Vous n'avez pas besoin de fermer et rouvrir votre navigateur.

Affichage de la licence

La licence est téléchargée comme composante du déploiement. Si votre société requière que la licence soit révisée avant d'utiliser l'application, déployez d'abord l'application. Ensuite, utilisez l'utilitaire de licence pour réviser la licence.

Avant de commencer

Avertissement : Une licence est installée lorsque vous déployez l'application. Pour afficher le contenu de la licence, vous devez d'abord déployer l'application.

Pourquoi et quand exécuter cette tâche

Pour télécharger et afficher les informations relatives à la licence à partir de la console :

Procédure

1. Entrez `wizard getLicense.xml`. L'assistant prépare les fichiers de licence en un fichier compressé.
2. Vous pouvez ensuite envoyer le fichier à un autre hôte sur lequel vous décompressez et affichez les fichiers de licence.
3. Vous pouvez également imprimer les fichiers de licence.

Mise à niveau de QuickFile version 1.1 en tant que dispositif virtuel

Si vous déployez QuickFile en tant que dispositif virtuel, mettez à niveau le produit dès qu'une nouvelle version est disponible. Si vous utilisez QuickFile dans un environnement (SaaS) hébergé, vous n'êtes pas obligé de mettre à niveau le dispositif.

Avant de commencer

Pour mettre à jour avec succès QuickFile vers la version 1.1, votre dispositif virtuel doit être configuré avec un minimum de 8 Go de mémoire. Vérifiez la mémoire disponible configurée pour votre instance QuickFile avant de poursuivre. Pour plus d'informations, consultez la documentation VMware.

Téléchargez le fichier de mise à niveau du microprogramme depuis le site Web IBM Fix Central. Le fichier de mise à niveau du microprogramme possède une extension de `vcrypt2`. Si vous déployez QuickFile avec une base de données externe, téléchargez le fichier de mise à niveau de la version 1.1.0.0 de QuickFile SQL pour votre base de données (Oracle ou DB2).Copiez le fichier de mise à niveau du microprogramme et le script de mise à niveau de la base de données vers un serveur FTP, SCP, ou HTTP accessible depuis QuickFile.

Pourquoi et quand exécuter cette tâche

Pour mettre à niveau un dispositif virtuel, utilisez le client de l'infrastructure VMware à connecter à un hyperviseur ou un groupe d'hyperviseurs (géré par un centre virtuel).

Complétez la procédure suivante pour mettre à niveau votre déploiement :

Procédure

1. Arrêtez toutes les connexions au serveur sur lequel QuickFile est en cours d'exécution.

   ATTENTION :
   Avant de mettre à niveau la base de données QuickFile et pour éviter toute instabilité, vous devez arrêter les connexions.
2. Exécutez la commande suivante depuis votre console de ligne de commande QuickFile pour récupérer le fichier de mise à niveau du microprogramme à partir du serveur sur lequel vous avez téléchargé le fichier :

Nom de la commande	Description de variable	Exemples

`file get` *`URL nom de fichier`*	• *URL* est le nom du fichier, de l'hôte et du chemin du fichier de mise à niveau du microprogramme.
	• *nom de fichier* est le nom pour enregistrer le fichier en tant que dispositif. Ce nom de fichier peut être n'importe quel nom valide, sans chemin (par exemple : fw)
		FTP
		`file get ftp://user1@dallas. ibm.com:/downloads/upgrade/ 091112.vcrypt2 fw`
		SCP:
		`file get scp://user1@dallas. ibm.com:/downloads/upgrade/ 091112.vcrypt2 fw`
		HTTP:
		`file get http://user1@dallas. ibm.com:/downloads/upgrade/ 091112.vcrypt2 fw`

A faire : Si vous mettez le dispositif hors tension, le fichier de mise à niveau est supprimé. Mettez à niveau le dispositif avant de le mettre hors tension.

3. Prenez une image instantanée de la machine virtuelle du serveur QuickFile. Cette image peut être utilisée pour restaurer l'instance si la mise à niveau du microprogramme échoue et que la restauration automatique qui s'effectue après un échec de mise à niveau échoue également. Pour plus d'informations, consultez la documentation VMware.
4. Si vous utilisez une base de données externe Oracle ou DB2, sauvegarder la base de données QuickFile.

   Important : Si votre mise à niveau échoue, vous devez posséder une sauvegarde de votre base de données pour restaurer. Pour plus d'informations, voir la documentation DBMS.
5. Si vous utilisez une base de données externe Oracle ou DB2, mettez à niveau la base de données en exécutant le script SQL QuickFile version 1.1.0.0 sur le serveur de la base de données. Pour plus d'informations, voir la documentation DBMS.
6. Réorganisez toutes les tables QuickFile. Pour plus d'informations, voir la documentation DBMS.
7. Après avoir récupéré le fichier, exécutez la commande suivante à partir de votre console pour mettre QuickFile à niveau :

Nom de la commande	Description de variable	Exemple
`firmware upgrade` *`nom de fichier`*	*nom de fichier* : nom utilisé dans la commande file get.	`mise à niveau de microprogramme (fw)`

8. Attendez que la commande de mise à niveau du microprogramme se termine. La commande peut être longue. Le dispositif redémarre quand la commande est terminée.
9. Lorsque le dispositif redémarre, connectez-vous à la console avec les données d'identification administratives.
10. Lorsque le contrat de licence s'affiche, lisez les conditions et acceptez la licence en appuyant sur 1 à l'invite.

    Important : Vous devez accepter la licence avant de pouvoir accéder au dispositif. Si vous ne l'avez pas accepter, le dispositif s'arrête.
11. Suivez les invites pour compléter le processus de démarrage. Pour utiliser les paramètres en cours, entrez `N` lorsqu'on vous invite à modifier les propriétés. Voir «Personnalisation de votre déploiement avec un fichier de propriétés», à la page 8 pour les instructions sur les propriétés de modification.

Que faire ensuite

Si la mise à niveau a échoué, le dispositif annule automatiquement la mise à niveau du microprogramme et restaure la version d'origine de celui-ci. Si vous utilisez une base de données externe Oracle ou DB2, vous devez restaurer manuellement la base de données vers sa version d'origine à partir de la sauvegarde de l'étape 4.

Pour déterminer la raison de l'échec, exportez les fichiers journal QuickFile en exécutant la commande de plateforme `must-gather` à partir de la console de ligne de commande QuickFile. Copiez les fichiers journal sur un serveur pour qu'ils puissent être envoyés pour révision à IBM Support.

Pour exportez les journaux, procédez comme suit :

```
platform must-gather logs.tgz
```

Pour copier les journaux sur un autre serveur, exécutez la commande d'insertion des fichiers. Vous pouvez utiliser FTP ou SCP, mais pas HTTP :

```
file put logs.tgz ftp://user1@dallas.ibm.com:/uploads/logs.tgz
file put logs.tgz scp://user1@dallas.ibm.com:/uploads/logs.tgz
```

Redémarrez le dispositif avec la commande de redémarrage du périphérique pour restaurer l'opération :

```
device restart
```

Si le dispositif ne démarre pas après une annulation du microprogramme automatique, vous devez le restaurez manuellement à partir de l'image instantanée de la machine virtuelle.

Chapitre 2. Questions liées à l'administration

En tant qu'administrateur, vous êtes responsable de nombreuses tâches. Ces tâches sont les suivantes : ajout des utilisateurs et des groupes, configuration de la sécurité des utilisateurs et détermination du moment de la purge des fichiers du serveur.

Utilisez le tableau suivant pour répondre aux questions que vous vous posez sur les tâches administratives :

Question	Réponse
Comment puis-je m'assurer que mon serveur dispose d'espace disque suffisant pour ajouter plus de fichiers ?	Pour vous assurer que votre serveur dispose d'espace disque suffisant pour télécharger des fichiers à transférer, définissez un planning pour purger les fichiers et les événements système. Vous définissez les conditions sous lesquelles les fichiers sont supprimés du serveur, y compris les fichiers qui sont abandonnés pendant le téléchargement. Dans le menu **Administration**, sélectionnez **Règles**. Cliquez sur l'onglet **Planifications**, puis sur **Purger** pour définir quand les fichiers sont supprimés du système. Sélectionnez **PurgeEvents** pour définir quand les événements système sont supprimés du système.
Puis-je modifier le nombre de tentative de connexion d'un utilisateur avant qu'il ne soit verrouillé ?	Oui. Vous pouvez modifier le nombre de fois qu'un utilisateur peut se tromper en se connectant avant d'être verrouillé. Cliquez sur **Administration** dans le menu et sélectionnez **Règles**. Cliquez sur l'onglet **Mot de passe** pour définir les options de mot de passe.
Puis-je contrôler les règles nécessaires pour les mots de passe utilisateur ?	Oui, vous pouvez définir le niveau de sécurité du mot de passe, la durée de validité du mot de passe, la fréquence à laquelle le mot de passe doit être modifiée et le nombre de caractères requis. Cliquez sur **Administration** dans le menu et sélectionnez **Règles**. Cliquez sur l'onglet **Mot de passe** pour définir les options de mot de passe.
Puis-je configurer le produit pour qu'il fonctionne avec Sterling Secure Proxy?	Oui. Ce produit fonctionne en arrière de Sterling Secure Proxy. Pour que les deux produits fonctionnent ensemble, définissez la configuration réseau pour prendre en charge Sterling Secure Proxy. Consultez «Protection de QuickFile avec Sterling Secure Proxy», à la page 30
Est-ce que quelqu'un peut déchiffrer le disque du dispositif ?	Non. Accès direct au disque virtuel dans le dispositif non disponible. Déchiffrement du contenu impossible.

Question	Réponse
Puis-je utiliser l'utilitaire de verrouillage PI (Program Isolation) du système d'information de gestion de la capacité pour extraire un fichier appartenant à quelqu'un d'autre ?	Oui. Vous pouvez utiliser l'utilitaire de verrouillage PI (Program Isolation) du système d'information de gestion de la capacité pour extraire des fichiers. Il se peut que vous souhaitiez utiliser l'utilitaire de verrouillage PI du système d'information de gestion de la capacité pour archiver des fichiers si vous n'utilisez pas FileNet.
Quand les fichiers sont-ils archivés ?	Si vous avez configuré l'archivage, les fichiers sont mis en file d'attente pour archivage après le téléchargement du fichier. Les fichiers mis en file d'attente pour archivage sont traités sur la base du premier entré, premier sorti.
Est-ce que les fichiers sont supprimés après leur archivage ?	Non. Une copie du fichier est déplacée dans la file d'attente d'archivage. Le fichier original est traité par QuickFile. Si vous configurez la tâche de maintenance de purge, les fichiers sont supprimés en fonction de la planification définie.
Si le système NFS n'est pas chiffré, est-ce que l'environnement n'est plus du tout sécurisé ?	Correct. Pour maintenir un environnement sécurisé, chiffrez le matériel du système NFS.
Puis-je modifier le nom d'utilisateur et le mot de passe par défaut utilisés pour se connecter à WebSphere MQ ?	Vous ne pouvez pas modifier le nom d'utilisateur et le mot de passe par défaut.
Puis-je configurer la notification de téléchargement de fichier pour supprimer le lien d'enregistrement ?	Oui. Si vous configurez la règle de transfert de fichier et restreignez les utilisateurs à inviter d'autres utilisateurs à s'enregistrer, l'option d'enregistrement est supprimée de la page de connexion. Reportez-vous à la rubrique • «Définition des restrictions de transfert de fichier», à la page 71 • «Définition des utilisateurs autorisés à envoyer des invitations d'enregistrement», à la page 71
Combien de fois un utilisateur peut-il télécharger un fichier ?	Un utilisateur peut télécharger un fichier autant de fois que nécessaire jusqu'à ce que le téléchargement du fichier expire. «Règles pour la date d'expiration et la taille de fichier des transferts», à la page 70
Quand et à quelle fréquence les événements sont-ils purgés ?	La tâche **PurgeEvents** doit d'abord être reprise afin qu'elle soit planifiée. Par défaut, la tâche s'exécute toutes les semaines le dimanche à minuit pour purger les événements antérieurs à 30 jours. Vous pouvez définir l'intervalle et planifier **PurgeEvents** pour qu'il s'exécute en fonction de vos besoins d'affaires. Voir«Configuration de la purge des événements», à la page 64.

Question	Réponse
Pourquoi mon système accumule un tel nombre d'événements ?	La tâche **PurgeEvents** doit d'abord être reprise afin qu'elle soit planifiée. Le nombre de transactions de votre système entraînant les événements peut être supérieur à la moyenne. Modifiez les paramètres de **PurgeEvents**. Voir : • «Activation de la purge d'événements», à la page 12 • «Configuration de la purge des événements», à la page 64

Chapitre 3. Utilisation d'IBM Sterling Control Center pour contrôler les événements de transfert QuickFile

IBM Sterling Control Center peut être utilisé pour contrôler les activités économiques de QuickFile.

QuickFile est un système de contrôle et de gestion centralisé qui donne la possibilité au personnel des opérations de contrôler continuellement les activités économiques de IBM Sterling Connect:Direct, IBM Sterling Connect:Direct File Agent, IBM Sterling Connect:Enterprise, IBM Sterling Connect:Enterprise Gateway, IBM Sterling B2B Integrator, QuickFile et de nombreux serveurs FTP au sein de l'entreprise.

Sterling Control Center prend en charge les événements suivants à partir de QuickFile

- Stockage des fichiers
- Evénements utilisateur et groupes
- Messagerie pour les éléments d'exception
- Evénements relatifs au dispositif
- Configuration SSL

Chapitre 4. Configuration ou modification des paramètres de l'application

Les options de configuration sont disponibles pour contrôler la configuration de QuickFile. De nombreuses options de configuration sont définies lors du déploiement du produit. Utilisez les options de configuration pour modifier ou ajouter de nouveaux paramètres.

Au besoin, modifiez la configuration de QuickFile. Vous pouvez modifier la configuration de QuickFile dans les zones suivantes :

- **Réseau** : modifiez les paramètres de base du réseau, y compris le réseau ou l'adresse DNS, ou le nom d'hôte (nom de domaine complet). Vérifiez les paramètres de base après le déploiement du produit.
- Si vous disposez d'un pare-feu, modifiez les paramètres réseau avancés. Vous pouvez également identifier un utilisateur sur un domaine d'e-mail spécifique en tant qu'utilisateur interne.
- **Paramètres régionaux** : configurez les adresses serveur NTP, modifiez le fuseau horaire du serveur ou modifiez les paramètres régionaux du serveur.
- **Système** : identifiez la durée d'attente avant qu'une session expire, après une période d'inactivité, et que l'utilisateur soit déconnecté. La valeur par défaut est 30 minutes. La valeur maximum est 1 440 minutes ou 24 heures.
- **Alimentation** : ferme ou redémarre QuickFile.
- **Serveur ICAP** : configurez le serveur ICAP à utiliser pour l'analyse antivirus et la prévention de perte de données (DLP)
- **LDAP** : utilisez cette option pour configurer le protocole LDAP.
- **Archivage** : permet l'archivage et configure IBM FileNet.
- **SSL** : active l'authentification SSL.

Quand configurer les options réseau

Les options réseau sont définies lorsque vous déployez le produit. Affichez les options réseau de base après l'installation pour valider les paramètres. Si nécessaire, modifiez les valeurs réseau de base. Pour certains environnements réseau, tels que la présence d'un pare-feu ou l'identification des utilisateurs internes, configurez les paramètres réseau avancés.

- Utilisez la procédure appelée «Configuration des options de configuration de réseau de base», à la page 28 pour valider l'adresse réseau définie pour l'installation. Vous pouvez également désactiver la connexion Ethernet.
- Utilisez la procédure appelée «Configuration des options de configuration de réseau de base», à la page 28 pour configurer les exigences réseau spécifiques à votre environnement. Les options sont les suivantes : ajouter ou supprimer la définition d'un serveur DNS, ou définir le domaine sur lequel les utilisateurs internes sont stockés. Ou encore définir un serveur de messagerie SMTP, modifier la définition du serveur de messagerie ou configurer la prise en charge d'un pare-feu.

Si vous modifiez le domaine de messagerie utilisé par le réseau, tous les utilisateurs du nouveau domaine sont désignés comme des utilisateurs internes. Si

vous supprimez un domaine de messagerie de la définition du réseau, tous les utilisateurs du domaine que vous avez supprimés sont définis en tant qu'utilisateurs externes.

Configuration des options de configuration de réseau de base

Les paramètres réseau sont d'abord configurés lorsque le produit est installé. Après avoir installé QuickFile, utilisez cette procédure pour valider les paramètres réseau de base et modifiez-les si nécessaire.

Avant de commencer

Pour afficher et modifier les paramètres réseau de base :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Sur l'onglet **Réseau**, cliquez sur **Adresses réseau** pour afficher les options d'adresse.
3. Pour modifier l'interface Ethernet, complétez les étapes suivantes :
   a. Cochez **eth0** pour activer l'interface Ethernet.
   b. Entrez l'adresse IP pour l'interface Ethernet dans la zone **Adresse IP**.
   c. Entrez la valeur appropriée du **Masque** au format CIDR.
   d. Entrez l'adresse de la **Passerelle par défaut** pour l'interface.
4. Pour désactiver une interface Ethernet, décochez la case à côté de son nom.
5. Pour ajouter l'adresse de serveur DNS avec le nom de domaine, cliquez sur **Cliquer pour ajouter**, entrez le nom DNS et appuyez sur Entrée.
6. Pour supprimer un serveur DNS, cliquez sur **x**.
7. Pour activer le nom d'hôte défini pour le réseau, complétez les étapes suivantes :
   a. Cliquez sur **Noms d'hôte** pour afficher l'option du nom d'hôte.
   b. Entrez le nom d'hôte dans la zone **Nom d'hôte**.
8. Pour configurer le serveur NTP et le fuseau horaire du serveur, complétez les étapes suivantes :
   a. Cliquez sur l'onglet **Environnement local**.
   b. Pour ajouter une adresse de serveur NTP, cliquez sur **Cliquer pour ajouter** et entrez une nouvelle adresse.
   c. Pour supprimer la définition d'une adresse de serveur NTP, cliquez sur **x** à côté de son nom.
   d. Pour modifier le fuseau horaire du serveur, sélectionnez le fuseau horaire à utiliser à partir de la liste.
9. Cliquez sur **Enregistrer**.

Configuration des options réseau avancées pour définir les utilisateurs internes

Configurez les paramètres réseau avancés pour préparer les environnements spécifiques. Définissez les domaines dans lesquels les utilisateurs sont stockés en plus de l'adresse définie lors de l'installation. Configurez les noms du domaine d'e-mail utilisés pour identifier les utilisateurs internes. Jusqu'à ce que vous définissiez un domaine d'e-mail, tous les utilisateurs sont créés en tant qu'utilisateurs externes. Définissez les options réseau destinées au public pour configurer un pare-feu.

Avant de commencer

Pour afficher et modifier les paramètres réseau pour les exigences d'environnement, complétez les étapes suivantes :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Si nécessaire, cliquez sur l'onglet **Réseau**.
3. Pour définir les domaines de messagerie dans lesquels les utilisateurs internes sont stockés, complétez les étapes suivantes :
   a. Cliquez sur **Domaines de messagerie** pour afficher les options de domaine de messagerie.
   b. Pour ajouter un domaine d'e-mail interne, cliquez sur **Cliquer pour ajouter**.
   c. Entrez le domaine de messagerie dans lequel les utilisateurs internes sont stockés et appuyez sur Entrée.

      A faire : Si vous modifiez le domaine de messagerie utilisé par le réseau, tous les utilisateurs du nouveau domaine sont désignés comme des utilisateurs internes. Si vous supprimez un domaine de messagerie de la définition du réseau, tous les utilisateurs du domaine que vous avez supprimés sont définis en tant qu'utilisateurs externes.
4. Pour cela, procédez comme suit :
   a. Sélectionnez **SSL** ou **Démarrer TLS** dans la zone **Sécurité**.
   b. Ajoutez le certificat du serveur SMTP au magasin de clés de confiance.
5. Pour modifier le serveur de messagerie SMTP, complétez les étapes suivantes :
   a. Cliquez sur **Serveurs de messagerie**.
   b. Entrez un nom de serveur dans la zone **Nom de serveur SMTP** et un port dans la zone **Port de serveur SMPT**.
   c. Pour activer la sécurité, sélectionnez **SSL ou Start TLS** dans la zone **Sécurité**. Ajoutez le certificat du serveur SMTP au magasin de clés de confiance.
6. Pour authentifier l'accès au serveur SMTP, cliquez sur **Utiliser les données d'authentification avec le serveur smtp**, puis donnez le nom d'utilisateur autorisé et le mot de passe autorisé.
7. Pour configurer la prise en change d'un pare-feu, complétez les étapes suivantes :
   a. Cochez **Utiliser un nom d'hôte (nom de domaine complet - FQDN) ou l'adresse IP** pour sélectionner la méthode de connexion au serveur.
   b. Entrez le nom d'hôte à utiliser pour vous connecter à QuickFile dans la zone **Nom d'hôte destiné au public**.
   c. Entrez le **Numéro de port** pour ce nom d'hôte.
8. Cliquez sur **Enregistrer**.

   Restriction : Vous ne pouvez pas passer un utilisateur d'un utilisateur interne en utilisateur externe. Pour faire passer un utilisateur d'un utilisateur interne en utilisateur externe, supprimez le compte utilisateur. Puis, demandez à l'utilisateur de s'enregistrer à nouveau. Par défaut, les utilisateurs sont définis comme des utilisateurs externes

Protection de QuickFile avec Sterling Secure Proxy

Vous pouvez utiliser IBM Sterling Secure Proxy pour protéger QuickFile dans le réseau interne.

Avant de commencer

Configurez HTTP dans Sterling Secure Proxy. Pour plus d'informations, consultez le centre de documentation de Sterling Secure Proxy.

Important : Les connexions HTTP entrantes et sortantes peuvent être sécurisées ou non sécurisées, mais elles doivent correspondre. Si la connexion netmap entrante est sécurisée, la connexion netmap sortante sur QuickFile doit également être sécurisée.

Complétez la procédure suivante pour configurer QuickFile pour qu'il fonctionne avec Sterling Secure Proxy:

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Si nécessaire, cliquez sur l'onglet **Réseau**.
3. Pour configurer le produit afin qu'il prenne en charge Sterling Secure Proxy, complétez les étapes suivantes :
   - Entrez le nom d'hôte ou l'adresse IP de l'adaptateur HTTP Sterling Secure Proxy dans la zone **Nom d'hôte** destiné au public.
   - Entrez le **Numéro de port** de l'adaptateur HTTP Sterling Secure Proxy pour ce nom d'hôte.
4. Cliquez sur **Enregistrer**.

   Important : Si vous avez configuré QuickFile pour qu'il utilise un certificat autosigné pour SSL, vous devez exporter le certificat racine. Configurez le netmap HTTP Sterling Secure Proxy avec ce certificat. Pour plus d'informations, consultez le centre de documentation de Sterling Secure Proxy.

Résolution d'incidents réseau

Résolvez des incidents réseau identifiés par les utilisateurs et comment chaque incident a été résolu.

Tableau 8. incidents réseau

Incident	Solution
Alors qu'un utilisateur testait le dispositif, l'utilisateur n'a pas configuré le réseau correctement. Le réseau a rencontré des erreurs et je n'ai pas pu me connecter pour corriger le problème. Existe-t-il une commande pour réinitialiser le dispositif pour que je puisse corriger la configuration ?	Dans la vue console du dispositif, exécutez l'assistant de configuration à nouveau pour entrer la commande suivante sur la ligne de commande : **wizard startup.xml** Réinitialisez seulement le réseau en entrant la commande suivante : **netif set eth0 IPAddress=** *youripaddress***DefaultGateway=***yourdefaultgateway*Remplacez *youripaddress* par votre adresse IP et *yourdefaultgateway* par votre adresse de passerelle.

Définitions de zone Configuration de réseau

Définissez les zones suivantes dans l'onglet **Réseau** des paramètres de configuration pour configurer les paramètres réseau avancés et de base :

Nom de zone	Description
Interface Ethernet (`eth`*x*)	L'interface Ethernet définie. Une interface Ethernet (`eth0`) est requise. Seule une interface Ethernet est prise en charge.
Adresse IP	Adresse IP ou masque de l'interface Ethernet. Obligatoire.
Masque	Masque de sous-réseau pour cette adresse IP. Il doit être dans la notation du routage CIDR. (CIDR), un moyen de spécifier les adresses IP et leur préfixe de routage. Il fournit le nombre décimal des bits d'interlignage du préfixe de routage. Par exemple : 24. Obligatoire.
Passerelle par défaut	Adresse de passerelle par défaut de l'interface Ethernet. Obligatoire.
Adresse du serveur DNS	Adresse du serveur DNS.
Domaines d'e-mail interne	Serveurs de noms de domaine (DNS) du dispositif. Au moins 1 domaine est requis.
Nom du serveur SMTP	Protocole SMTP ou serveur de messagerie à utiliser pour acheminer les e-mails pour le dispositif. Obligatoire.
Port du serveur SMTP	Protocole SMTP ou port du serveur de messagerie à utiliser pour acheminer les e-mails. Obligatoire.
Sécurité	Sécurité utilisée par le serveur SMTP : les valeurs valides sont aucune, SSL ou Start TLS.
Données d'identification pour l'authentification utilisateur avec serveur smtp	Active l'utilisation des données d'identification pour l'authentification avec serveur SMTP
Nom d'utilisateur autorisé	Un nom d'utilisateur avec l'autorisation d'accéder au serveur SMTP. Facultatif.
Mot de passe autorisé	Mot de passe de l'utilisateur autorisé à accéder au serveur SMTP. Requis si l'option **Nom d'utilisateur autorisé** est spécifiée.
Utilisation d'un nom d'hôte (nom de domaine complet - FQDN) pour l'application	Activez cette option seulement lorsqu'un nom d'hôte est affecté au dispositif QuickFile, et que le nom d'hôte du mappage de l'adresse IP est ajouté au serveur de noms de domaine (DNS). Lorsque cette zone est activée, vous pouvez accéder à QuickFile en utilisant le nom distinctif complet. Le nom distinctif est plus facile à mémoriser que l'adresse IP. Si vous définissez cette zone sur un nom d'hôte qui ne peut pas être résolu par le serveur de noms de domaine (DNS), une erreur se produit.

Nom de zone	Description
Nom d'hôte	Nom d'hôte du DNS du dispositif QuickFile. Si aucun nom d'hôte n'est affecté, la zone affiche l'adresse IP du premier réseau configuré.
Utilisation d'un nom de domaine complet destiné au public ou d'une adresse IP	Cochez cette zone lorsque QuickFile est déployé en arrière d'un proxy inverse ou d'un équilibreur de charge. Si cette option est activée, entrez le nom et le port de domaine complet destiné au public à utiliser pour accéder au proxy ou à l'équilibreur de charge. Le proxy ou l'équilibreur de charge achemine les demandes qu'il reçoit vers QuickFile
Nom d'hôte destiné au public	Si l'option **Utilisation d'un nom de domaine complet destiné au public** est cochée, entrez le proxy ou le nom d'hôte de l'équilibreur de charge, ou l'adresse IP sur laquelle le trafic client est acheminé.
Numéro de port destiné au public	Port à utiliser pour accéder au proxy ou à l'équilibreur de charge. • Si vous configurez un équilibreur de charge et SSL, définissez la valeur du port sur 9443. Pour un équilibreur de charge non sécurisé, définissez le port sur 9080. • Si vous configurez Sterling Secure Proxy, définissez le port sur la valeur définie dans l'adaptateur HTTP Sterling Secure Proxy. Consultez «Protection de QuickFile avec Sterling Secure Proxy», à la page 30.

Configuration de la valeur du délai d'expiration d'une session

Vous pouvez modifier la valeur du délai d'expiration. La valeur du délai d'expiration identifie la durée pendant laquelle une session inactive reste valide.

Pourquoi et quand exécuter cette tâche

Avertissement : La règle système de la section Configuration identifie la durée pendant laquelle une session inactive reste valide, en minutes. La valeur par défaut est de 30 minutes. La valeur maximum est 1 440 minutes ou 24 heures.

Utilisez cette procédure pour définir la valeur du délai d'expiration.

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **Système**.
3. Sélectionnez une valeur dans la zone **Durée des sessions utilisateur avant expiration**. Cette valeur définie le nombre de minutes avant qu'une session inactive n'expire.
4. Cliquez sur **Enregistrer**.
5. Redémarrez QuickFile pour que vos modifications prennent effet.

Arrêt ou redémarrage de QuickFile

Vous pouvez redémarrer ou arrêter QuickFile.

Avant de commencer

Quand c'est possible, alertez les utilisateurs à l'avance lorsque vous planifiez de redémarrer ou d'arrêter QuickFile.

Pourquoi et quand exécuter cette tâche

Pour la maintenance ou pour d'autres raisons, il est possible que vous soyez invité à redémarrer QuickFile ou à l'arrêter. L'administration vous donne la possibilité d'accomplir cette tâche dans le bon ordre. Lorsque c'est possible, assurez-vous que les utilisateurs sont notifiés avant que vous n'arrêtiez le serveur. Donnez du temps aux utilisateurs pour qu'ils se préparent à une impossibilité temporaire d'accès et pour éviter que les transferts de fichiers ne soient affectés.

Pour arrêter ou redémarrer le dispositif, effectuez les étapes suivantes :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **Power**.
3. Pour redémarrer QuickFile, cliquez sur **Redémarrer le dispositif**.
4. Pour arrêter QuickFile, cliquez sur **Arrêter le dispositif**. Si vous arrêtez le dispositif, vous devez redémarrer QuickFile en utilisant le client VMware vSphere.

Utilisation du protocole LDAP pour gérer les utilisateurs et les mots de passe

Utilisez QuickFile avec votre serveur LDAP. Il simplifie les tâches d'ajout et de suppression d'utilisateurs. L'utilisation de définitions d'utilisateur LDAP intègre mieux l'acquis utilisateur de QuickFile dans leur flux de travail.

LDAP est un protocole Internet au norme de l'industrie. Il stocke et accède aux informations utilisateur relatives à un serveur. LDAP est largement utilisé dans les programmes de messagerie et autres logiciels pour gérer les informations relatives à l'adresse utilisateur.

Si votre société utilise le protocole LDAP pour gérer les utilisateurs, vous pouvez l'utiliser pour gérer les utilisateurs QuickFile. Avec une connexion LDAP, vous pouvez éliminer la plupart des conditions requises pour ajouter des utilisateurs ou des groupes d'utilisateurs à QuickFile.

Si vous activez LDAP, n'utilisez pas QuickFile pour gérer les utilisateurs LDAP. Utilisez plutôt les outils LDAP. Si un utilisateur essaie de se connecter à QuickFile avec un mot de passe LDAP expiré, l'utilisateur est invité à contacter l'administrateur. En tant qu'administrateur, assurez-vous que l'utilisateur réinitialise le mot de passe dans le répertoire LDAP de la société.

Restriction : Vous pouvez définir les utilisateurs à la fois dans le protocole LDAP et dans QuickFile. Cependant, les utilisateurs créés dans le protocole LDAP ne peuvent pas être gérés dans QuickFile et les utilisateurs créés dans QuickFile doivent être gérés via QuickFile.

Après avoir créé un utilisateur dans le LDAP, demandez que l'utilisateur se connecte à QuickFile. Le profil utilisateur s'affiche lorsque l'utilisateur passe la souris sur l'image et clique sur **Profil**. Les utilisateurs peuvent modifier leur profil, y compris leur nom. Il n'est pas obligatoire que cette valeur corresponde à celle définie dans LDAP. Les utilisateurs ne peuvent pas utiliser le produit pour modifier leur mot de passe. Il est modifié dans LDAP.

Configuration d'un serveur LDAP avec QuickFile

En tant qu'administrateur, vous pouvez configurer QuickFile pour utiliser votre serveur LDAP. Utiliser un serveur LDAP élimine la nécessité d'ajouter et de maintenir des utilisateur dans QuickFile. Les informations relatives aux utilisateurs et au mot de passe sont déjà créés dans LDAP ; par conséquent, vous n'avez pas besoin de créer ces informations dans QuickFile. Vous pouvez définir les utilisateurs à la fois dans LDAP et QuickFile.

Avant de commencer

Pour utiliser SSL avec LDAP, activez SSL dans la configuration LDAP. Ensuite, importez le certificat du serveur LDAP dans la base de données du magasin de clés de confiance dans QuickFile à partir du menu **Configuration** dans l'onglet **SSL**. Définissez également le port de serveur LDAP sur le port SSL utilisé par le serveur.

Pourquoi et quand exécuter cette tâche

Complétez les étapes suivantes pour configurer QuickFile pour utiliser votre répertoire LDAP.

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **LDAP**.
3. Pour configurer la connexion LDAP, cliquez sur **Informations de connexion** > **Activer l'intégration LDAP**, et entrez les informations dans les zones suivantes.
   a. Nom du serveur
   b. Numéro de port
   c. ID principal
   d. Mot de passe principal
4. Pour activer la connexion Secure Sockets Layer (SSL) pour l'authentification d'utilisateur, cochez **Activer SSL**. Assurez-vous d'importer le certificat dans le magasin de clés de confiance.
5. Pour tester la validité de vos entrées de connexion LDAP, cliquez sur **Tester la connexion**.
6. Cliquez sur **Informations de base** et fournissez les informations suivantes :
   a. Entrez le **Nom distinctif de la base de groupe** pour identifier les informations du groupe indiquées dans la base de données LDAP
   b. Entrez le Type the **Nom distinct de la base utilisateur** pour identifier les informations utilisateur indiquées dans la base de données LDAP

c. Pour mieux identifier un groupe dans le groupe du nom distinct de base, entrez les informations dans cette zone de texte et cliquez sur **Entrer**.

7. Pour ajouter des groupes LDAP que vous souhaitez que QuickFile reconnaisse, cliquez sur **Cliquer pour ajouter**.
8. Cliquez sur **Enregistrer**.

Définitions de zone Configuration LDAP

Les définitions suivantes décrivent les zones dans l'onglet **LDAP** de la page Configuration de QuickFile.

Nom de zone	Description
Activer l'intégration LDAP	Cochez cette case pour permettre l'utilisation du serveur LDAP. Décochez la case pour désactiver l'option. Facultatif. La valeur par défaut est supprimée. Si vous activez l'intégration LDAP et que vous la configurer, les utilisateurs LDAP peuvent utiliser leurs données d'identification LDAP pour se connecter à QuickFile.
Nom du serveur	Nom d'hôte ou adresse IP du serveur LDAP. Il doit être un nom de serveur LDAP valide dans votre réseau. (IPv6 n'est pas pris en charge.) Obligatoire.
Numéro de port	Numéro de port à utiliser pour accéder au serveur LDAP. Intervalle de valeurs valides entre 1 et 65535. Obligatoire.
ID principal	Nom distinctif complet d'un utilisateur LDAP autorisé à chercher dans le répertoire LDAP. Obligatoire.
Mot de passe principal	Mot de passe pour l'ID principal. Obligatoire.
Activer SSL	Cochez pour activer la sécurité de la connexion Secure Sockets Layer (SSL). Si cette option est activée, vous devez importer le certificat de serveur LDAP dans le magasin de clés de confiance QuickFile. Facultatif.
Nom distinctif (DN) de base de groupe	Nom distinctif de la base de groupe. Le noeud parent dans lequel les groupes sont stockés dans la zone **LDAP**. Entrez le noeud en tant que nom distinctif complet (ex: `OU=Users,O=IBM,C=US`). Obligatoire.
Nom distinctif de base utilisateur	Nom distinct de base utilisateur. Entrez le noeud en tant que nom distinctif complet (ex: `OU=Users,O=IBM,C=US`). Obligatoire.
Groupe	Cliquez sur **Cliquer pour ajouter** et définissez les groupes autorisés à accéder à QuickFile. Entrez le groupe en tant que nom distinct complet (ex: `CN=QuickFile Users, OU=Users,O=IBM,C=US`). Obligatoire.
Classe du filtre de recherche de groupe	Filtre de recherche pour les groupes. Ne modifiez pas cette valeur à moins que le support ne vous demande de le faire. Valeur par défaut : `(|(objectClass=group)(objectClass=groupOfNames)(objectClass=groupOfUniqueNames))`.Obligatoire.
Attributs des membres	Matrice des noms d'attribut. Ne modifiez pas cette valeur à moins que le support ne vous demande de le faire.
Classe du filtre de recherche utilisateur	Filtre de recherche pour les utilisateurs. Ne modifiez pas cette valeur à moins que le support ne vous demande de le faire. Obligatoire. Valeur par défaut : `(|(objectClass=user)(objectClass=person)(objectClass=inetOrgPerson)(objectClass=organizationalPerson))`
Attributs de courrier électronique	Matrice des noms d'attribut d'e-mail. Ne modifiez pas cette valeur à moins que le support ne vous demande de le faire.

Configuration de l'archivage

En tant qu'administrateur, vous pouvez configurer QuickFile pour archiver toutes les activités de transferts de fichiers pour vous assurer qu'un enregistrement de toutes les activités est conservé.

Avant de commencer

La configuration de l'archivage nécessite FileNet. Il est également nécessaire de configurer un type de document FileNet approprié pour l'archive. Enfin, obtenez l'URL du document de service CMIS utilisé pour accéder au système de fichier archive. Obtenez le nom du dossier de niveau supérieur de l'archive. Pour plus d'informations, consultez la documentation FileNet.

Important : Activer l'archivage peut avoir un impact sérieux sur les performances.

Pourquoi et quand exécuter cette tâche

Pour configurer l'archivage, complétez les étapes suivantes:

Procédure

1. Dans le menu, cliquez sur **Configuration**.
2. Cliquez sur l'onglet **Archivage**.
3. Cochez l'option **Activer l'intégration d'un système d'archivage**. Les zones pour l'indication des informations d'archivage sont activées
4. Sélectionnez **FileNet** en tant que fournisseur d'archives.
5. Entrez l'**URL du document de service** du système de fichier archive.
6. Entrez le nom de l'utilisateur autorisé à accéder au système d'archive.
7. Entrez le mot de passe utilisateur pour accéder au système de fichiers.
8. Entrez le **Dossier d'archivage de niveau supérieur** du système de fichiers.
9. Cliquez sur **Enregistrer**. L'archivage est activé. Aucun redémarrage système n'est requis.

Archivage des définitions de zone

Le tableau suivant décrit les zones que vous définissez pour configurer l'archivage sur l'onglet Archivage des fonctions de configuration.

Nom de zone	Description
Activer l'intégration d'un système d'archivage	Vérifiez cette option pour activer l'archivage et les zones restantes sur cette page.
Fournisseur d'archivage	Sélectionnez l'application de base de données à utiliser pour archiver les fichiers. Étant donné que FileNet est le seul fournisseur disponible, seule cette zone.
Document de service (URL)	URL où se trouve le document de service du système d'archivage sélectionné. La zone est limitée à 255 caractères.
ID de référentiel	ID de référentiel sur lequel les fichiers et les modules sont archivés.
Nom d'utilisateur autorisé	Utilisateur autorisé à accéder au système de fichier archive. Obligatoire.

Nom de zone	Description
Mot de passe autorisé	Mot de passe autorisé de l'utilisateur pour accéder au système de fichier archive.
Dossier d'archivage de niveau supérieur	Dossier de niveau supérieur dans lequel les fichiers et les modules archivés sont stockés.

Présentation de la configuration SSL

QuickFile utilise les certificats numériques pour authentifier l'identité du serveur à l'utilisateur qui s'y connecte. SSL est un protocole permettant d'activer des sessions de communication sécurisées sur un réseau non protégé, tel qu'Internet. Pour authentifier le serveur aux utilisateurs, obtenez et vérifiez les certificats numériques. Les certificats du serveur sont stockés dans le magasin de clés.

Les certificats sont utilisés pour sécuriser les communications, chiffrer et déchiffrer les données. Chaque certificat est fait de la clé publique et d'une clé privée. La clé publique contient les informations que vous avez envoyées à votre partenaire. La clé privée est enregistrée sur votre site et confirme votre identité. Elle doit restée secrète.

Comme mesure supplémentaire de sécurité, obtenez votre certificat d'une autorité de certification (CA). Une autorité de certification CA vérifie toutes les informations d'identité de votre certificat, puis ajoute sa signature. Dans une transaction SSL, votre certificat est présenté à chaque utilisateur qui se connecte à votre serveur. Le serveur reconnaît la signature de l'autorité de certification qui signe le certificat racine de l'autorité de certification. Avant de commencer à communiquer avec l'utilisateur, assurez-vous que le site de l'utilisateur a une copie du certificat racine de l'autorité de certification. Le fait que l'utilisateur reconnaît votre certificat racine de l'autorité de certification assure à l'utilisateur que vous êtes bien celui que vous dites être.

Si vous utilisez un certificat qui n'est pas validé par une autorité de certification, il s'agit d'un certificat autosigné. Utilisez des certificats autosignés lorsque la vérification d'identité n'est pas requise, comme les communications dans votre société ou pendant le test d'un produit.

Pour implémenter SSL lorsque la transaction utilise un certificat de l'autorité de certification, importez le certificat racine de l'autorité de certification dans votre magasin de clés de confiance. Si nécessaire, envoyez le certificat racine de l'autorité de certification à l'utilisateur, pour l'inclure dans le magasin de clés de confiance de l'utilisateur. Stockez votre clé privée et le certificat de l'autorité de certification dans le magasin de clés. Il est disponible pour vérification lorsque vous le stockez dans le magasin de clés.

Méthodes de configuration SSL

Sélectionnez la méthode à utiliser pour configurer SSL. Les méthodes comprennent l'utilisation d'un nouveau certificat de l'autorité de certification, un certificat de l'autorité de certification existant, un certificat chaîné ou un certificat autosigné.

- Si votre certificat signé par l'autorité de certification est utilisé avec une autre application, vous pouvez l'importer dans QuickFile.
- Si vous ne disposez pas d'un certificat signé par l'autorité de certification, complétez une demande de signature pour en demander un. Extrayez les informations de QuickFile et envoyez-les à l'autorité de certification. Après que

l'autorité de certification a renvoyé le certificat signé, importez-le dans QuickFile. Activez la connexion SSL en identifiant le certificat du serveur et lancez SSL. Toutes les futures connexions authentifient le serveur sur la connexion entrante.

- Pour utiliser un certificat chaîné, complétez la configuration du certificat chaîné. Activez la connexion SSL en identifiant le certificat du serveur et lancez SSL. Toutes les futures connexions authentifient le serveur sur la connexion entrante.
- En ce qui concerne la méthode la moins sécurisée, comme lorsque vous communiquez avec des utilisateurs externes ou lorsque vous testez une application, utilisez un certificat autosigné pour l'authentification SSL.

Configuration de SSL en créant un certificat signé par l'autorité de certification

Pour activer l'authentification SSL, utilisez l'une des méthodes suivantes : demandez un nouveau certificat à l'autorité de certification ou utilisez un certificat signé par l'autorité de certification existant pour configurer l'authentification SSL.

Pour demander un nouveau certificat auprès de l'autorité de certification, puis configurer une authentification SSL dans QuickFile:

- «Ajout d'une demande de signature de certificat»
- «Extraction d'un certificat à partir d'une demande de signature», à la page 39
- «Sélection du certificat à utiliser pour l'authentification de serveur», à la page 40
- «Configuration des options de configuration de réseau de base», à la page 28

Ajout d'une demande de signature de certificat

Pour demander un certificat signé par l'autorité de certification, complétez une demande de signature. Ensuite, envoyez la demande à l'autorité de certification qui la signe.

Pourquoi et quand exécuter cette tâche

A faire : Consultez la documentation de l'autorité de certification qui signe votre demande de signature de certificat (CSR) pour comprendre les exigences de la CSR. Si la demande de signature ne répond pas aux exigences de l'autorité de certification, elle peut être rejetée.

Complétez les étapes suivantes pour créer une demande de signature et l'ajouter au magasin de demandes signées :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'**onglet SSL**.
3. Cliquez sur **Gestion de certificats** pour développer la section.
4. Cliquez sur le nom du magasin de demandes signées pour l'ouvrir.
5. Cliquez sur **Nouvelle**. La page Demande de signature de certificat s'affiche.
6. Entrez le libellé de clé à utiliser lorsque vous faites référence à cette demande dans la zone **Libellé de clé**.
7. Entrez le nom usuel utilisé pour faire référence à la société ou l'URL qui est validée dans la zone **Nom usuel**.
8. Entrez les informations dans les zones facultatives restantes, le cas échéant.
9. Cliquez sur **Créer**.

Définitions de zone Nouvelle demande de signature

Créez une demande de signature pour créer un certificat et envoyez-le sur une autorité de certification pour signature. Le tableau suivant identifie les zones à définir lors de la création d'une demande de signature.

Zone	Description
Libellé de clé	Libellé à affecter à la demande de signature du certificat que vous créez.
Taille de clé	Longueur de clé requise pour la clé publique permettant de valider la clé.
Nom usuel (CN)	Nom de domaine complet (FQDN), nom d'hôte ou URL sur lequel vous avez l'intention d'appliquer votre certificat. Si le nom usuel du certificat ne correspond pas à la valeur définie dans cette zone, la session échoue.
Organisation	Nom sous lequel votre entreprise est légalement enregistrée. L'organisation répertoriée doit être la personne juridique enregistrée du nom de domaine dans la demande de certificat. Si vous vous inscrivez en tant qu'individu, entrez le nom du demandeur de certificat dans la zone **Organisation**. Entrez le nom de l'administrateur de base de données (faisant des affaires en tant que) dans la zone **Unité organisationnelle**.
Unité d'organisation	Définissez cette zone pour différencier les divisions d'une organisation. Par exemple, « Ingénierie » ou « Ressources humaines ». Le cas échéant, entrez le nom de l'administrateur de base de données (faisant des affaires en tant que) dans cette zone.
Localisation	Nom de la ville dans laquelle se trouve ou est enregistrée votre organisation. Épelez le nom de la ville. Aucune abréviation.
Région/Département	Nom de la région ou du département dans laquelle se trouve votre organisation. Entrez le nom complet. Aucune abréviation.
Code postal	Code postal de la ville dans laquelle se trouve votre organisation.
Pays ou région	L'indicatif de pays à deux lettres au format ISO (Organisation internationale de normalisation) du pays ou de la région où votre organisation est légalement enregistrée.

Extraction d'un certificat à partir d'une demande de signature

Après avoir créé une demande de signature, extrayez le certificat et envoyez les informations sur l'autorité de certification (CA).

Pourquoi et quand exécuter cette tâche

Complétez les étapes suivantes pour extraire le certificat à partir de la demande de signature. Vous pouvez ensuite l'envoyer sur l'autorité de certification.

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **SSL**.
3. Cliquez sur **Gestion de certificats** pour développer la section.
4. Cliquez sur le nom du magasin de la demande de signature où la CSR est stockée.
5. Sélectionnez la demande de signature pour l'extraire et cliquez sur **Extraire**.
6. Copiez le texte à partir de la boîte de dialogue et collez-le dans un autre fichier. Enregistrez le fichier.
7. Cliquez sur **Fermer**.
8. Envoyez le fichier sur votre autorité de certification et demandez qu'il soit signé et vous soit renvoyé.

Téléchargement d'un fichier de clés reçu d'une autorité de certification

Téléchargez un fichier de clés reçu d'une autorité de certification pour le rendre disponible sur QuickFile.

Pourquoi et quand exécuter cette tâche

Pour télécharger un fichier de clés à partir d'une autorité de certification :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **SSL**.
3. Cliquez sur **Gestion de certificats** pour développer la section.
4. Cliquez sur le nom du magasin de clés à ouvrir.
5. Cliquez sur **Télécharger le fichier de clés**.
6. Activez **Importer à partir d'un fichier de clés** et cliquez sur **Naviguer** pour localiser le fichier.
7. Cliquez sur **Télécharger**.

Activation ou désactivation de SSL

Après avoir configuré et vérifié vos certificats dans la base de données, vous pouvez alors activer SSL. Si vous souhaitez désactiver l'authentification SSL, vous pouvez le faire.

Procédure

1. Cliquez sur **Configuration**.
2. Cliquez sur l'onglet **SSL**.
3. Si nécessaire, cliquez sur **Configuration** pour afficher les options de configuration SSL.
4. Cochez l'option **Activer les connexions sécurisées (SSL)**.
5. Pour désactiver SSL, décochez l'option **Activer les connexions sécurisées (SSL)**.
6. Cliquez sur **Enregistrer**. Redémarrez votre navigateur pour activer les modifications que vous avez faites.

Sélection du certificat à utiliser pour l'authentification de serveur

Vous pouvez sélectionner le certificat utilisé pour authentifier le serveur. Si le certificat change, modifiez la configuration du certificat.

Avant de commencer

Pour activer le certificat à utiliser pour authentifier le serveur pour les utilisateurs qui se connectent à l'application :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **SSL**.
3. Sélectionnez le certificat à utiliser pour l'authentification dans la zone **Certificat du serveur**.
4. Cliquez sur **Enregistrer**.

Configuration de SSL en utilisant un certificat autosigné existant

Pour activer l'authentification SSL, utilisez l'une des méthodes suivantes. Vous pouvez demander un nouveau certificat, générer un certificat chaîné ou utiliser un certificat existant pour configurer l'authentification SSL.

Complétez les procédures suivantes pour utiliser un certificat signé par l'autorité de certification existant pour authentifier une connexion et configurer QuickFile pour qu'il soit authentifié par les connexions entrantes :

- «Téléchargement d'un fichier de clés et importation d'un certificat»
- «Activation ou désactivation de SSL», à la page 40
- «Sélection du certificat à utiliser pour l'authentification de serveur», à la page 40
- «Configuration des options de configuration de réseau de base», à la page 28

Téléchargement d'un fichier de clés et importation d'un certificat

Pour authentifier le serveur QuickFile avec un certificat obtenu d'une autorité de certification, téléchargez le fichier de clés de l'autorité de certification sur la base de données.

Pourquoi et quand exécuter cette tâche

Pour télécharger un fichier de clés :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **SSL**.
3. Cliquez sur **Gestion de certificats** pour développer la section.
4. Cliquez sur le nom du magasin de clés sur lequel le certificat est importé.
5. Cliquez sur **Télécharger le fichier de clés**. La boîte de dialogue Télécharger le fichier de clés s'affiche.
6. Activez **Importer à partir d'un fichier de clés** et cliquez sur **Naviguer** pour localiser le fichier.
7. Cliquez sur **Télécharger**. La page **Importation de certificat** s'affiche.
8. Entrez les informations sur le certificat, y compris le nom du fichier de clés et l'alias du certificat importé.
9. Cliquez sur **Importer**.

Configuration de SSL avec un certificat chaîné

Pour activer l'authentification SSL avec un certificat chaîné, créez un certificat chaîné et signez-le avec un certificat racine de l'autorité de certification. Ensuite, vous êtes prêt à activer la sécurité avec le certificat chaîné.

Complétez les procédures suivantes pour créer un nouveau certificat chaîné et configurer une authentification SSL dans QuickFile:

- «Configuration des certificats chaînés»
- «Activation ou désactivation de SSL», à la page 40
- «Sélection du certificat à utiliser pour l'authentification de serveur», à la page 40
- «Configuration des options de configuration de réseau de base», à la page 28

Utilisation des certificats chaînés

Pour augmenter la sécurité, vous pouvez utiliser le chaînage du certificat de l'autorité de certification.

Dans le chaînage de certificat, deux ou plusieurs certificats de l'autorité de certification sont liés à une chaîne de certificats. Le certificat de l'autorité de certification principal est le certificat racine à la fin de la chaîne de certificat de l'autorité de certification. Il doit être présent pour vérifier l'authenticité du certificat reçu. Une chaîne de certificats peut être stockée dans un fichier unique, tel qu'un fichier `.pem`. Elle peut être stockée dans des fichiers séparés, où chaque fichier contient un certificat de l'autorité de certification dans une chaîne. Si vous envisagez d'utiliser une hiérarchie de certificats, veillez à installer chaque certificat CA de la hiérarchie dans le magasin sécurisé.

Configuration des certificats chaînés

Pour augmenter la sécurité, utilisez un certificat chaîné de l'autorité de certification. Avant de créer un certificat chaîné, importez la clé du certificat racine dans le fichier de clés certifiées. Le certificat racine est utilisé pour signer le certificat chaîné.

Pourquoi et quand exécuter cette tâche

Pour configurer un certificat chaîné, complétez les étapes suivantes :

Procédure

1. Cliquez sur **Configuration** dans le menu.
2. Cliquez sur l'onglet **SSL**.
3. Cliquez sur **Gestion de certificats** pour développer la section.
4. Cliquez sur le nom du magasin de clés à ouvrir.
5. Cliquez sur **Créer** > **Certificat chaîné**. La page Créer un certificat chaîné s'affiche.
6. Entrez l'alias utilisé pour ce certificat dans la zone **Alias**.
7. Sélectionnez le certificat racine utilisé pour signer le certificat.
8. Entrez le nom usuel à utiliser pour le certificat chaîné.
9. Sélectionnez la taille de la clé du certificat racine dans la liste.
10. Entrez le nom usuel à utiliser pour le certificat chaîné.
11. Entrez le nombre de jours pendant lesquels le certificat est valide dans la zone **Période de validité**.
12. Si nécessaire, entrez les informations relatives au serveur à valider dans les zones restantes.

13. Cliquez sur **Créer**.

Définitions de zone Certificat chaîné

Lorsque vous recevez le certificat d'une autre entité, il se peut que vous ayez à utiliser une chaîne de certificats pour obtenir le certificat racine de l'autorité de certification. La chaîne de certificats est la liste des certificats qui sont utilisés pour authentifier une entité. La chaîne commence avec le certificat de cette entité. Chaque certificat d'une chaîne est signé par l'entité identifiée par le certificat suivant dans la chaîne. La chaîne se termine avec un certificat racine de l'autorité de certification. Le certificat racine de l'autorité de certification est toujours signé par l'autorité de certification elle-même. Les signatures de tous les certificats de la chaîne doivent être vérifiées jusqu'à ce que le certificat racine de l'autorité de certification soit atteint. Le tableau suivant identifie les zones que vous définissez lorsque vous configurez un certificat chaîné dans QuickFile.

Zone	Description
Alias	Alias associé au certificat. Les définitions de la connexion et du programme d'écoute sécurisés qui spécifient la connexion SSL utilisent l'alias pour faire référence au certificat.
Certificat racine utilisé pour signer le certificat	Nom du certificat racine. Si la demande ne comprend pas la chaîne complète de certificats, les certificats d'émetteur sont recherchés dans le magasin de clés de confiance.
Taille de clé	Taille de clé utilisée pour signer le certificat. Les valeurs suivantes sont valides : 512, 1024 et 2048. La plupart des fournisseurs de certificat se tournent vers des tailles de clés de 2048 octets.
Nom usuel (CN)	Nom de domaine complet (FQDN), nom d'hôte ou URL sur lequel vous avez l'intention d'appliquer votre certificat. Si le nom usuel du certificat ne correspond pas à la valeur définie dans cette zone, la session échoue.
Période de validité	Temps d'utilisation du certificat pour authentification. Entrez le nombre de jours, jusqu'à 356 jours.
Organisation	Nom sous lequel votre entreprise est légalement enregistrée. L'organisation répertoriée doit être la personne juridique enregistrée du nom de domaine dans la demande de certificat. Si vous vous inscrivez en tant qu'individu, entrez le nom du demandeur de certificat dans la zone **Organisation**. Entrez le nom de l'administrateur de base de données (faisant des affaires en tant que) dans la zone **Unité organisationnelle**.

Zone	Description
Unité organisationnelle	Définissez cette zone pour différencier les divisions d'une organisation. Par exemple, « Ingénierie » ou « Ressources humaines ». Le cas échéant, entrez le nom de l'administrateur de base de données (faisant des affaires en tant que) dans cette zone.
Localisation	Nom de la ville dans laquelle se trouve ou est enregistrée votre organisation. Épelez le nom de la ville. Aucune abréviation.
Région/Département	Nom de la région ou du département dans laquelle se trouve votre organisation. Entrez le nom complet. Aucune abréviation.
Code postal	Code postal de la ville dans laquelle se trouve votre organisation.
Pays ou région	L'indicatif de pays à deux lettres au format ISO (Organisation internationale de normalisation) du pays ou de la région où votre organisation est légalement enregistrée.

Configuration de SSL à l'aide d'un certificat autosigné

Pour activer l'authentification SSL à l'aide d'un certificat autosigné, vous créez un certificat autosigné.

Pour créer un certificat autosigné et configurer une authentification SSL dans QuickFile :

- «Création d'un certificat autosigné»
- «Activation ou désactivation de SSL», à la page 40
- «Sélection du certificat à utiliser pour l'authentification de serveur», à la page 40
- «Configuration des options de configuration de réseau de base», à la page 28

Création d'un certificat autosigné

pour tester rapidement votre environnement, utilisez un certificat autosigné. Il n'est pas signé par une autorité de certification et ne fournit pas la sécurité requise dans un environnement de production. Si vous utilisez un certificat autosigné pour tester votre environnement, assurez-vous de le remplacer avant d'utiliser le produit.

Pourquoi et quand exécuter cette tâche

Pour configurer un certificat autosigné, complétez les étapes suivantes :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **SSL**.
3. Cliquez sur **Gestion de certificats** pour développer la section.
4. Cliquez sur le nom du magasin de clés à ouvrir.
5. Cliquez sur **Créer > Certificat autosigné**. La page Créer un certificat autosigné s'affiche.
6. Entrez l'alias à utiliser pour ce certificat dans la zone **Alias**.
7. Sélectionnez le nom usuel identifié dans le certificat dans la zone **Nom usuel**.

8. Entrez le nombre de jours pendant lesquels le certificat est valide dans la zone **Période de validité**.
9. Si vous le souhaitez, entrez les informations relatives au serveur dans les zones restantes.
10. Cliquez sur **Créer**.

Définitions de zone de certificat autosigné

Créez un certificat autosigné pour activer la connexion SSL d'un environnement interne. Un certificat autosigné n'est pas aussi sécurisé que l'utilisation d'un certificat de l'autorité de certification. Cependant, il fournit un niveau de sécurité qui peut être utilisé pour tester ou valider le serveur pour les utilisateurs au sein de l'entreprise.

Zone	Description
Alias	Alias associé au certificat. Les définitions de la connexion et du programme d'écoute sécurisés qui spécifient la connexion SSL utilisent l'alias pour faire référence au certificat.
Version	Version utilisée pour créer le certificat autosigné : `X509v3` ou `IBMX509`
Taille de clé	Longueur de clé requise pour la clé publique permettant de valider le certificat.
Nom usuel (CN)	Nom de domaine complet (FQDN), nom d'hôte ou URL sur lequel vous avez l'intention d'appliquer votre certificat. Si le nom usuel du certificat ne correspond pas à la valeur définie dans cette zone, la session échoue.
Période de validité	Temps d'utilisation du certificat pour authentification. Entrez le nombre de jours, jusqu'à 356 jours.
Organisation	Nom sous lequel votre entreprise est légalement enregistrée. L'organisation répertoriée doit être la personne juridique enregistrée du nom de domaine dans la demande de certificat. Si vous vous inscrivez en tant qu'individu, entrez le nom du demandeur de certificat dans la zone **Organisation**. Entrez le nom de l'administrateur de base de données (faisant des affaires en tant que) dans la zone **Unité organisationnelle**.
Unité organisationnelle	Définissez cette zone pour différencier les divisions d'une organisation. Par exemple, « Ingénierie » ou « Ressources humaines ». Le cas échéant, entrez le nom de l'administrateur de base de données (faisant des affaires en tant que) dans cette zone.
Localisation	Nom de la ville dans laquelle se trouve ou est enregistrée votre organisation. Épelez le nom de la ville. Aucune abréviation.
Région/Département	Nom de la région ou du département dans laquelle se trouve votre organisation. Entrez le nom complet. Aucune abréviation.

Zone	Description
Code postal	Code postal de la ville dans laquelle se trouve votre organisation.
Pays ou région	L'indicatif de pays à deux lettres au format ISO (Organisation internationale de normalisation) du pays ou de la région où votre organisation est légalement enregistrée.

Importation d'un certificat dans le magasin de clés

Indiquez un certificat personnel à importer à partir d'un magasin de clés ou d'un fichier de clés. Téléchargez le fichier de clés avant d'importer un certificat.

Pourquoi et quand exécuter cette tâche

Pour importer un certificat dans le magasin de clés :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **SSL**.
3. Cliquez sur **Gestions de certificats** pour afficher le magasin de clés et le magasin de clés de confiance.
4. Cliquez sur **Plus** > **Importation**. La page **Importation de certificat** s'affiche.
5. Entrez les informations dans les zones requises suivantes :
   - Nom du fichier de clés
   - Mot de passe de fichier de clés
   - Alias de certificat importé
6. Cliquez sur **Importer**.

Définitions de zone Importer un certificat

Lorsque vous importez un fichier de clés à partir d'un fichier, utilisez les zones du tableau suivant pour importez le certificat :

Zone	Description
Nom du fichier de clés	Nom du fichier de clés qui contient la clé publique et la clé privée.
Type	Sélectionnez le type de clé à importer : `JKS` ou `PKCS12`
Mot de passe de fichier de clés	Le mot de passe qui verrouille le fichier de clés et est utilisé pour importer le certificat.
Obtenir des alias pour les fichiers de clés	Cliquez pour interroger le fichier de clés pour obtenir les alias de tous les certificats personnels dans le magasin de clés.
Alias de certificat à importer	Alias de certificat qui est identifié comme nom du fichier de clés que vous souhaitez importer dans le magasin de clés en cours.
Alias de certificat importé	Nouvel alias que vous souhaitez donner au certificat dans le magasin de clés.

Téléchargement d'un fichier certificat pour stockage

Téléchargez un fichier dans le magasin de clés. Le fichier n'est pas disponible pour être utilisé avec l'application. Il est seulement stocké pour une utilisation ultérieure.

Pourquoi et quand exécuter cette tâche

Pour télécharger un fichier certificat pour le stockage, complétez la procédure suivante :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **SSL**.
3. Cliquez sur **Gestion de certificats** pour développer la section.
4. Cliquez sur le nom du magasin de clés sur lequel le fichier est téléchargé.
5. Cliquez sur **Télécharger le fichier de clés**. La page Télécharger le fichier de clés s'affiche.
6. Activer **Télécharger simplement le fichier** et cliquez sur **Naviguer** pour localiser le fichier.
7. Cliquez sur **Télécharger**.

Définitions de zone Télécharger un fichier de clés

Utilisez la fenêtre Télécharger un fichier de clés pour définir comment télécharger les fichiers dans un magasin de clés ou à partir des fichiers reçus d'une autorité de certification. Les zones sont décrites dans le tableau.

Zone	Définition
Joindre un fichier à télécharger	Pour télécharger, exécutez l'une des actions suivantes : • Faites glisser le fichier de clés dans la case **Joindre** • **Parcourir** pour sélectionner le fichier de clés
Sélectionnez ce que vous souhaitez faire avec le fichier	Sélectionnez l'action à prendre avec le fichier que vous téléchargez : • Recevoir d'une autorité de certification • Importer à partir d'un fichier de clés • Télécharger le fichier

Suppression d'un certificat à partir du magasin de clés

Vous pouvez supprimer un certificat à partir du magasin de clés.

Pourquoi et quand exécuter cette tâche

Pour supprimer un certificat à partir du magasin de clés :

Procédure

1. Cliquez sur **Configuration** à partir du menu.
2. Cliquez sur l'onglet **SSL**.
3. Cliquez sur le nom du magasin de clés qui contient le certificat à supprimer.
4. Cliquez sur le certificat à supprimer.

5. Cliquez sur **Plus** > **Supprimer**. La page Supprimer certificat s'affiche.
6. Cliquez sur **Supprimer**.

Chapitre 5. Utilisation de l'analyse DLP pour éviter la perte des données

La prévention des pertes de données (DLP) est le processus de surveillance et d'empêchement que les données sensibles sortent du serveur de votre société. Obtenez des services de la part d'un fournisseur de services et configurez un serveur ICAP conformément aux spécifications de ce fournisseur. Utilisez ce serveur pour implémenter des règles d'analyse des fichiers qui sont transférés à l'aide de QuickFile.

QuickFile peut analyser les fichiers téléchargés pour la DLP. Pour analyser des fichiers, procédez comme suit :

- Configurez le serveur ICAP. Le serveur peut être configuré pour l'analyse DLP, l'analyse antivirus ou les deux.

  Pour configurer le serveur, identifiez les informations suivantes :

  – Le nom du serveur sur lequel le logiciel DLP est installé.
  – Le fournisseur du logiciel DLP.
  – L'application installée sur le serveur. Les options comprennent la prévention des pertes de données (DLP) ou l'antivirus et DLP.

    Restriction : Des serveurs ICAP dupliqués ne peuvent pas être configurés. Si un serveur est configuré pour antivirus et DLP, vous ne pouvez pas ajouter un antivirus unique ou une configuration unique de DLP.
  – Les informations sur le serveur comprennent le nom d'hôte, le nom du service et le numéro de port.

  Voir Chapitre 6, «Activation d'une analyse antivirus ou du serveur pour la prévention des pertes de données», à la page 51 pour les instructions sur la configuration du serveur ICAP.
- Testez la configuration du serveur pour déterminer si la définition se connecte au serveur ICAP.
- Avant de configurer une règle, activez le serveur.
- Pour configurer un exemple de règle sans l'appliquer, n'activez pas le serveur.
- Configurez une règle pour définir les fichiers à analyser. Vous pouvez analyser tous les fichiers téléchargés ou seulement les fichiers téléchargés à partir d'utilisateurs externes.

  Restriction : Si le serveur n'est pas configuré, vous ne pouvez pas définir de règle.
  Voir «Règle pour les analyses de prévention des pertes de données (DLP)», à la page 59 pour obtenir des instructions de définition des règles.
- Après avoir configuré un serveur et défini une règle, les fichiers sont analysés selon la règle que vous avez définie (tous les fichiers ou seulement les fichiers provenant d'utilisateurs externes). Si l'analyse détecte des données sensibles d'entreprise dans un fichier, la séquence suivante se produit :

  – Le transfert de fichiers est annulé.
  – Un statut **Package failed** (Echec du package) s'affiche sur la page Sent files (Fichiers envoyés) en regard du transfert annulé.

– Les journaux indiquent les transferts qui ont été annulés en raison d'un échec de l'analyse des données sensibles.

Chapitre 6. Activation d'une analyse antivirus ou du serveur pour la prévention des pertes de données

Configurez les serveurs ICAP à utiliser pour l'analyse antivirus et la prévention des pertes de données.

Avant de commencer

Le protocole ICAP est un protocole HTTP simple qui implémente l'analyse antivirus et la prévention des pertes de données. Les éléments prérequis suivants s'appliquent :

- Obtenir des services de la part d'un fournisseur ICAP pris en charge.
- Déterminer les paramètres de configuration dont votre fournisseur de services a besoin.
- Configurer QuickFile de manière à respecter la configuration de votre fournisseur pour les serveurs ICAP utilisés pour l'analyse antivirus et la prévention des pertes de données (DLP). Vous pouvez configurer un serveur ICAP pour traiter les deux services ou un serveur pour chaque service implémenté, selon votre fournisseur de services. Par exemple, certains fournisseurs configurent l'antivirus et la DLP sur le même serveur. Pour ces fournisseurs, vous configurez seulement un serveur ICAP.

Lorsque vous configurez le serveur, identifiez les services qui sont fournis :

- Analyse antivirus
- DLP
- Analyse antivirus et DLP

Pourquoi et quand exécuter cette tâche

Pour configurer les services requis pour votre environnement :

Procédure

1. Cliquez sur **Configuration** à partir du menu de navigation.
2. Cliquez sur l'onglet **Serveurs ICAP**.
3. Cliquez sur le bouton **Ajouter serveur ICAP** pour ouvrir la page et définir un nouveau serveur.
4. Pour activer l'utilisation du serveur configuré, vérifiez que la case **Activer serveur ICAP** est cochée.
5. Renseignez les zones en vous référant à leur définition. Pour plus d'informations, voir la rubrique «Zones de configuration du serveur ICAP», à la page 52.
6. Pour tester la connexion du serveur QuickFile au serveur ICAP, cliquez sur **Tester la connexion**.
7. Cliquez sur **Enregistrer**.

Que faire ensuite

Définissez une règle qui utilise le serveur que vous avez configuré. Voir :

- «Règle pour les analyses antivirus», à la page 58

- «Règle pour les analyses de prévention des pertes de données (DLP)», à la page 59

Zones de configuration du serveur ICAP

Lorsque vous configurez ou modifiez une définition de serveur ICAP, complétez les zones suivantes :

Zone	Description
Nom du serveur	Nom affecté au serveur ICAP. Toutes les mises à jour de valeur jusqu'à 100 caractères. Obligatoire.
Nom du fournisseur	Nom du fournisseur du logiciel antivirus ou DLP. Sélectionnez un fournisseur dans la liste suivante : • Prévention des pertes de données Symantec • Passerelle Web McAfee • Moteur de protection Symantec Obligatoire.
Type de serveur	Les services qui sont fournis par le serveur que vous configurez. Sélectionnez un type dans la liste suivante : • Analyse antivirus • Prévention des pertes de données (DLP) • Analyse antivirus et DLP Obligatoire. **Conseil :** Vous avez accès uniquement aux options valides selon le fournisseur sélectionné.
Nom d'hôte (Adresse IP)	Nom d'hôte ou adresse IP utilisé pour se connecter au serveur ICAP. Le nombre maximum de caractères autorisé pour un nom d'hôte est de 255 caractères. Chaque segment séparé d'un point ne peut pas dépasser 63 caractères. Le dernier segment doit dépasser deux caractères. Pour une adresse IP, la valeur peut contenir jusqu'à 15 caractères et doit inclure 4 segments de chiffres uniquement séparés par un point. Chaque segment comprend une valeur allant de 0 à 255. Les valeurs exemple comprennent les valeurs suivantes : `myhost`, `myhost.ompany.domain.com` ou 192.168.1.1.Obligatoire.

Zone	Description
Nom du service	Nom du service ICAP à utiliser sur le serveur que vous configurez. Il est également utilisé dans le chemin URL de ICAP. Par exemple : `icap://server:port/serviceName` est la valeur URL. Cette zone comprend jusqu'à 255 caractères. La valeur doit commencer par un caractère alphanumérique. Les caractères suivants sont autorisés : • Alphanumérique • / (barre oblique) • _ (trait de soulignement) • - (trait d'union) Voici quelques exemples : • Passerelle Web McAfee - `RESPMOD` • Analyse antivirus Symantec - `SYMCSCANRESPEX-AV` • Prévention des pertes de données Symantec - `reqmod` **Conseil :** Les valeurs de la zone **Service name** sont définies par votre fournisseur de services.Obligatoire.
Numéro de port	Port sur lequel le serveur ICAP pour accepter les connexions. Les valeurs autorisées sont des nombres entiers entre 1025 et 65536. La valeur par défaut est 1344. Obligatoire.
Analyse taille de bloc	Valeur indiquant comment interrompre la transmission de fichiers vers ou à partir du serveur. Cette valeur doit être un multiple de 1024, dont le maximum est défini sur 1048576 (1024 X 1024). La valeur par défaut est 8192. Obligatoire.
Test de la configuration	Cliquez sur **Tester la configuration** pour contrôler que le serveur QuickFile peut se connecter au serveur ICAP.

Chapitre 7. Règles de définition des paramètres de tous les utilisateurs

Définissez les règles utilisateur globales pour identifier comment les utilisateurs adaptent QuickFile lors de votre installation.

En tant qu'administrateur, vous pouvez définir les règles pour configurer les paramètres utilisateur sur l'ensemble du système et définir comment QuickFile fonctionne pour tous les utilisateurs. Vous pouvez également définir les groupes et appliquer les règles sur un ensemble d'utilisateurs avec les mêmes exigences.

Restriction : Il n'est pas possible d'appliquer toutes les règles sur un groupe d'utilisateurs.

Vous pouvez configurer les règles suivantes :

- Comment configurer les expirations de compte utilisateur externe
- Comment gérer les utilisateurs qui ne saisissent pas correctement les informations de connexion et sont verrouillés sur le système
- Options de réinitialisation de mot de passe
- Le niveau de sécurité du mot de passe nécessaire et la durée de validité d'un mot de passe
- Exécutez, modifiez, interrompez et reprenez les planifications administratives communes de la même façon que la suppression de la base de données et des transferts expirés
- Le type d'utilisateurs qui peut inviter des utilisateurs externes à s'enregistrer
- Le type d'utilisateurs qui est autorisé à envoyer des fichiers à des utilisateurs internes et externes
- Taille maximale de fichier qui peut être téléchargée

Règle pour la date d'expiration des comptes externes

Définissez une règle d'expiration du compte pour identifier si les comptes utilisateur externe expirent. Si la règle d'expiration d'un compte est définie, tous les utilisateurs externes expirent après la durée définie dans la zone Durée.

En tant qu'administrateur, vous pouvez définir une règle pour déterminer si les comptes utilisateur externe expirent et la durée pendant laquelle les comptes sont actifs. Prenez les informations suivantes en compte lorsque vous configurez une règle de compte utilisateur :

- Un domaine de messagerie doit être défini dans les options avancées réseau avant que vous ne configuriez cette règle.
- Si aucune règle d'expiration de compte n'est définie, les comptes des utilisateurs externes n'expirent pas.
- Si une règle d'expiration est définie, le compte d'un utilisateur externe est valide à partir du moment où le compte est créé jusqu'à la date d'expiration.
- La première règle d'expiration définie est appliquée à tous les comptes d'utilisateurs externes existants.

- Cette règle s'applique à tous les utilisateurs externes à qui un fichier a été envoyé, qui ont été invité à envoyer un fichier et qui ont fait une demande de fichier.
- Les utilisateurs sont notifiés sept jours avant que le compte n'expire.
- Si la période d'expiration du compte est inférieure à sept jours, l'e-mail d'expiration est envoyé immédiatement.
- Vous pouvez modifier la date d'expiration de tous les comptes utilisateur. Par exemple, si les comptes expirent dans 30 jours et que 20 jours se sont écoulés, vous pouvez modifier le délai d'expiration à 60 jours. Le compte expire alors dans 60 jours.
- Lorsqu'un compte externe expire, l'utilisateur ne peut plus se connecter à QuickFile
- Les utilisateurs internes n'expirent pas.
- Lorsque le compte d'un utilisateur externe expire, tous les utilisateurs qui ont reçu des fichiers de la part d'un utilisateur expiré ont accès aux fichiers reçus jusqu'à ce que le fichier expire.
- À l'expiration du compte d'un utilisateur externe, le compte n'est pas disponible. Cependant, l'utilisateur externe peut s'enregistrer avec les mêmes données d'identification et commencer à envoyer et à recevoir à nouveau des fichiers. L'utilisateur externe nouvellement activé ne peut pas accéder aux fichiers qui ont été envoyés avant l'expiration du compte.
- Les comptes d'administration sont exempts de cette règle et n'expirent pas.

Assurez-vous que vous définissez un serveur de domaine de messagerie interne. Sinon, vous ne pouvez pas définir une règle de gestion des comptes

Création de la règle d'expiration d'un compte utilisateur

Utilisez la règle d'expiration d'un compte utilisateur pour définir si les comptes des utilisateurs externes expirent. Commencez par activer l'option. Puis, définissez la durée d'expiration. Utilisez cette règle pour définir le temps d'activité d'un compte utilisateur avant son expiration.

Pourquoi et quand exécuter cette tâche

A faire : Définissez au moins un serveur du domaine de messagerie avant de créer la règle d'expiration de compte. Utilisez la configuration de réseau pour définir le serveur du domaine de messagerie. Consultez «Configuration des options réseau avancées pour définir les utilisateurs internes», à la page 28.

Pour configurer la règle d'expiration du compte utilisateur :

Procédure

1. À partir du menu de navigation, cliquez sur **Règles**.
2. Cliquez sur l'onglet **Gestion des comptes**.
3. Développez la section Expirations de compte.
4. Cochez la zone **Activer l'expiration des comptes des utilisateurs externes**.
5. Dans la zone **Durée avant que les comptes des utilisateurs externes n'expirent**, sélectionnez une valeur d'expiration entre 1 et 999, puis sélectionnez l'unité. La valeur par défaut est 30 jours.
6. Cliquez sur **Enregistrer**.

Désactivation des règles d'expiration des comptes d'utilisateurs externes

Après avoir défini les règles d'expirations d'un compte, vous pouvez désactiver l'option si vous ne souhaitez plus que les comptes utilisateur expirent. Si un compte a été configuré pour expirer, désactiver la règle empêche tous les comptes des utilisateurs externes d'expirer.

Pourquoi et quand exécuter cette tâche

Pour désactiver la règle d'expiration du compte utilisateur :

Procédure

1. À partir du menu de navigation, cliquez sur **Règles**.
2. Cliquez sur l'onglet **Gestion des comptes**.
3. Développez la section Expirations de compte.
4. Décochez l'option **Activer l'expiration des comptes des utilisateurs externes**.
5. Cliquez sur **Enregistrer**.

Définition de zone Expiration de compte

Les zones d'expiration de compte de l'onglet **Gestion des comptes** donnent les informations définies pour configurer la durée d'expiration des comptes des utilisateurs externes.

Nom de zone	Description
Activer l'expiration des comptes des utilisateurs externes	Sélectionnez cette option pour activer l'expiration d'un compte d'utilisateur externe.
Durée avant l'expiration des comptes des utilisateurs externes	Dans la première case, définissez la durée pendant laquelle un compte externe reste actif. Les valeurs admises sont comprises entre 1 et 999. Dans la deuxième case, définissez l'unité de mesure en jours, mois et années. Si cette définition est la première définition de règle d'administration, elle est immédiatement appliquée à tous les comptes des utilisateurs externes. La règle du compte utilisateur est appliquée à chaque compte utilisateur externe nouvellement créé.

Règle de verrouillage de compte

En tant qu'administrateur, vous pouvez définir une règle pour définir si les utilisateurs sont temporairement bloqués pour se connecter. La règle est imposée lorsque l'utilisateur n'a pas réussi à se connecter correctement après un nombre d'essais défini.

Vous définissez le nombre de tentatives de connexions échouées qu'un utilisateur peut essayer avant d'être verrouillé. Vous pouvez définir la durée pendant laquelle l'utilisateur est bloqué.

Configuration des règles de verrouillage utilisateur

Définissez une règle de verrouillage de compte utilisateur temporaire pour définir quand un utilisateur est verrouillé. Le verrouillage a lieu après qu'un utilisateur tente de se connecter à plusieurs reprises avec des données d'identification non valides.

Pourquoi et quand exécuter cette tâche

Pour des raisons de sécurité, vous pouvez verrouiller temporairement un utilisateur de QuickFile. Le verrouillage a lieu si l'utilisateur ne réussit pas à fournir un ID utilisateur et un mot de passe valides. Vous définissez le nombre de tentatives où l'utilisateur est autorisé à fournir des données d'identification non valides avant d'être verrouillé. Cette pratique décourage les tiers malveillants de deviner les mots de passe possibles pour accéder à un compte.

Pour définir les règles de verrouillage :

Procédure

1. Cliquez sur **Règles**.
2. Cliquez sur l'onglet **Verrouillage de compte**.
3. Sélectionnez **Verrouillage de mot de passe** pour activer le verrouillage.
4. Définissez les valeurs dans les zones suivantes :
   - **Nombre d'échecs de connexion avant le verrouillage**
   - **Durée du verrouillage temporaire**
   - **Temps avant que le compteur d'échecs de connexion se réinitialise**
5. Cliquez sur **Enregistrer**.

Définitions de zone Verrouillages temporaires

Pour définir quand un utilisateur est verrouillé de QuickFile après avoir entré des informations de connexion incorrectes, configurez la page Verrouillage de compte.

Nom de zone	Description
Verrouillages de mot de passe	Activez ou désactivez le verrouillage de mot de passe. Facultatif.
Nombre d'échecs de connexion avant le verrouillage	Combien de fois l'utilisateur peut essayer de se connecter sans réussir avant d'être verrouillé. Si l'option **Verrouillage de mot de passe** est activée, sélectionnez un chiffre entre 1 et 99 dans cette zone.
Durée du verrouillage temporaire	Temps qui doit s'écouler avant que l'utilisateur puisse tenter une nouvelle connexion après le verrouillage. Sélectionnez une valeur entre 1 et 9 et des unités en minutes ou en heures pour la durée.
Temps avant que le compteur d'échecs de connexion se réinitialise	Temps pendant le lequel les échecs de connexion sont comptabilisés, en commençant par le premier échec. Le compteur d'échec de connexion se remet à zéro lorsque cette période s'est écoulée. Sélectionnez une valeur entre 1 et 99 et des unités en minutes ou en heures pour la durée.

Règle pour les analyses antivirus

Après avoir configuré le logiciel antivirus, définissez les fichiers à analyser pour les virus. Après l'analyse des fichiers, tout transfert qui contient un fichier infecté est annulé.

Avant de commencer

D'abord, définissez le serveur ICAP. Les informations requises pour configurer la règle peuvent changer en fonction des options que vous avez définies dans la configuration du serveur ICAP. Vous pouvez créer une règle lorsque le serveur et le fournisseur sont configurés mais que le fournisseur n'est pas activé. Cependant, l'analyse antivirus n'est pas activée jusqu'à ce que le fournisseur soit activé. Voir Chapitre 6, «Activation d'une analyse antivirus ou du serveur pour la prévention des pertes de données», à la page 51 pour les instructions sur l'activation du serveur ICAP.

- Si un fournisseur et les serveurs sont définis mais que le fournisseur n'est pas actif, vous pouvez définir la règle mais aucune analyse n'a lieu. L'analyse démarre après l'activation des fournisseurs.
- Si un fournisseur n'est pas défini, ou qu'un fournisseur est défini mais aucun serveur n'est configuré, les paramètres des règles ne s'affichent pas. Vous ne pouvez pas définir une règle.

Pourquoi et quand exécuter cette tâche

Pour définir les fichiers à analyser pour les virus, complétez les étapes suivantes :

Procédure

1. Cliquez sur **Règles** à partir du menu de navigation.
2. Cliquez sur l'onglet **ICAP**.
3. Dans **Antivirus**, cochez l'option **Activer l'analyse antivirus pour les transferts de fichiers**, si vous souhaitez implémenter cette règle immédiatement.
4. Activez une des options suivantes pour définir les fichiers à analyser pour les virus :
   - **Analyser tous les fichiers entrants** pour analyser tous les fichiers entrants
   - **Analyser seulement les fichiers entrants provenant d'utilisateurs externes** pour analyser seulement les fichiers reçus d'utilisateurs externes
5. Cliquez sur **Enregistrer**.

Règle pour les analyses de prévention des pertes de données (DLP)

Après avoir configuré le serveur de prévention contre les pertes de données (DLP), définissez les fichiers à analyser pour l'intégrité des données. Lorsque les fichiers sont analysés, tout transfert qui contient des informations sensibles est annulé. Seuls les fichiers téléchargés peuvent être analysés.

Avant de commencer

Configurez le serveur ICAP avant de définir une règle. Le fournisseur doit être activé avant que vous puissiez définir la règle. Voir Chapitre 6, «Activation d'une analyse antivirus ou du serveur pour la prévention des pertes de données», à la page 51 pour les instructions sur l'activation du serveur ICAP.

Pourquoi et quand exécuter cette tâche

Pour définir les fichiers à analyser pour la prévention des pertes de données, procédez comme suit :

Procédure

1. Cliquez sur **Règles** à partir du menu de navigation.
2. Cliquez sur l'onglet **ICAP**.
3. Développez la section **DLP**.
4. Dans la sous-section **DLP**, cochez l'option **Activer l'analyse DLP pour les transferts de fichiers**, pour activer cette règle immédiatement.
5. Sélectionnez une règle d'analyse pour les transferts de fichiers :
   - **Scan all uploaded files** (Analyser tous les fichiers téléchargés) pour analyser tous les fichiers pour la prévention contre la perte de données.
   - **Only scan uploaded files from internal users** (Analyser uniquement les fichiers téléchargés provenant d'utilisateurs externes) pour analyser tous les fichiers téléchargés provenant de tous les utilisateurs externes.

   Restriction : Aucune option d'analyse des fichiers entrant provenant d'une source externe.
6. Cliquez sur **Enregistrer**.

Règle pour la planification des tâches de maintenance

En tant qu'administrateur, vous pouvez planifier des tâches prédéfinies pour qu'elles s'exécutent régulièrement. Ces tâches continuent à exécuter QuickFile efficacement pour répondre aux exigences des affaires.

Pourquoi et quand exécuter cette tâche

Configurez QuickFile pour utiliser les tâches de maintenance prédéfinies selon un calendrier régulier. La liste des tâches est définie par QuickFile. Vous configurez les tâches de maintenance à planifier pour votre environnement. Vous pouvez démarrer une tâche manuellement, définir un planning d'exécution d'une tâche, et interrompre et reprendre les tâches. L'état par défaut de toutes les tâches est Planifié.

Procédure

1. Cliquez sur **Règles** à partir du menu de navigation.
2. Cliquez sur l'onglet **Planification**.
3. Sélectionnez **Afficher toutes les tâches**. QuickFile fournit les méthodes suivantes pour définir les plannings :

Tableau 9. Méthodes de planification des tâches de maintenance

Méthode de planification	Description
Prédéfini	Utilisez les intervalles prédéfinis comme méthode simple pour définir un planning. Sélectionnez un des intervalles prédéfinis suivants : • Annuellement pour planifier une tâche une fois par an à midi le 1er janvier • Mensuellement pour exécuter une tâche le premier jour de chaque mois à midi • Chaque semaine pour exécuter une tâche tous les dimanches à midi • Quotidiennement pour planifier la tâche à midi tous les jours • Toutes les heures pour planifier la tâche au début de chaque heure
Intervalle	Options qui permettent un contrôle plus minutieux sur la planification. Vous pouvez exécuter une tâche toutes les x minutes ou heures, et chaque jour ou une fois par semaine.
Date et heure	Identifie les jours spécifiques de la semaine où la tâche est exécutée. Vous choisissez les jours de la semaine et les heures pour exécuter la tâche. Par exemple, définissez une tâche pour qu'elle s'exécute tous les mardis et jeudis à 6h00 et 18h00
CRON	Une méthode de notation qui utilise un ensemble limité de caractères dans une syntaxe particulière pour exprimer les heures de planification. Cette application prend en charge la notation CRON pour définir les intervalles de date et d'heure, et indique six termes pour définir l'expression. Alors que les autres approches de CRON utilisent cinq termes, cette application nécessite six termes et ne prend pas en charge cinq termes. Consultez la documentation de WebSphere Application Server et recherchez le titre de la rubrique : Interface User Calendar. **Important :** Parce que les expressions CRON sont complexes, QuickFile utilise seulement une validation limitée de vos entrées.

4. Cliquez sur **Enregistrer**.

Tâches disponibles à planifier

Définissez les règles de QuickFile pour compléter les tâches de maintenance prédéfinies sur l'ensemble du système selon un planning normal. La liste des tâches est définie par QuickFile.

L'état par défaut de toutes les tâches est **Planifié**, avec un intervalle par défaut.

Un menu déroulant à côté de **État** indique les choix suivants :

- Exécuter : pour démarrer une tâche manuellement
- Modifier : pour modifier le planning
- Interrompre : pour arrêter une tâche en cours d'exécution et la reprendre plus tard
- Reprendre : si vous interrompez une tâche, vous devez la reprendre manuellement.

Le tableau suivant décrit les tâches planifiées pour s'exécuter. Modifiez la valeur de chaque tâche pour empêcher la tâche de s'exécuter :

Tâche	Description
Cycle de vie	Mise à jour de l'état des transferts de fichier via les états suivants : • En cours • Nombre de fichiers envoyés ou reçus (indique un transfert réussi) • Echec du transfert (indique qu'une analyse de virus ou une analyse préventive de perte de données a trouvé un problème dans un fichier dans un package) L'intervalle par défaut est toutes les 30 secondes.
Notification	Met en file d'attente toutes les notifications d'e-mail en attente et les prépare à être envoyées. L'intervalle par défaut est toutes les 30 secondes.
Purger	Marque tous les modules qui ont expiré et tous les modules de transfert de fichiers incomplets et les rend disponible pour la suppression. Un package incomplet est celui qui a été envoyé mais qui a été interrompu et qui n'a pas terminé le transfert dans l'intervalle de sept jours. Il ne peut pas être téléchargé. Tous les modules marqués pour être supprimés le sont à partir de la base de données. L'intervalle par défaut est toutes les heures.
PurgeEvents	Supprime les événements système des journaux selon la configuration de l'option **Purge des événements système**. Un fichier CSV contenant la liste des événements purgés est envoyé à tous les administrateurs système. Une notification indiquant que la tâche **PurgeEvents** est terminée est envoyée par e-mail à tous les administrateurs système. L'intervalle par défaut est tous les jours. Voir«Configuration de la purge des événements», à la page 64.
Mémento	Met en file d'attente tous les messages électroniques de rappel en suspens et les rend disponibles pour l'envoi. L'intervalle par défaut est toutes les 30 minutes.

Tâche	Description
Etat	Suppression par lot des enregistrements de base de données une fois qu'ils ne sont plus utiles. L'intervalle par défaut est toutes les 5 minutes.
Utilisateur	Effectue la maintenance des enregistrements utilisateur et de groupe. Les types de maintenance des enregistrements comprennent les exemples suivants : • Suppression des enregistrements en cours d'expiration • Identification des certificats SSL en cours d'expiration L'intervalle par défaut est chaque jour à 4h00 du matin.

Planification des tâches de maintenance

Utilisez l'onglet **Planification** sous Règles pour définir les plannings pour répondre à vos exigences pour les tâches que QuickFile doit compléter régulièrement.

Pourquoi et quand exécuter cette tâche

QuickFile doit effectuer systématiquement certaines tâches pour que le système puisse fonctionner facilement et garder ses performances. Les tâches de maintenance sont planifiées pour s'exécuter selon un planning par défaut. Le planificateur de tâches peut configurer un planning personnalisé pour chaque tâche. Vous pouvez également interrompre ou reprendre une tâche, ou la définir pour qu'elle s'exécute immédiatement.

Pour définir la planification ou exécuter une tâche manuellement :

Procédure

1. Cliquez sur **Règles** dans le menu.
2. Cliquez sur l'onglet **Planification**.
3. Par défaut, seules les tâches planifiées sont affichées dans la liste de planification. Cliquez sur **Afficher toutes les tâches** pour afficher l'ensemble complet des tâches.
4. Pour exécuter immédiatement une tâche, sélectionnez la tâche et cliquez sur **Exécuter**.
5. Pour définir un planning personnalisé pour utiliser une tâche de la liste, complétez les étapes suivantes :
   a. Activez la tâche et cliquez sur **Modifier**.
   b. Cliquez sur l'onglet de la méthode de planification à utiliser.
   c. Configurez l'intervalle à utiliser pour exécuter la tâche. Voir «Règle pour la planification des tâches de maintenance», à la page 60 pour plus d'informations sur les méthodes de planification et les options.
   d. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

      Conseil : Vous n'avez pas besoin de redémarrer QuickFile pour que les modifications soient appliquées.

Que faire ensuite

Si vous détectez que les tâches planifiées ne s'exécutent pas ou s'exécutent à des intervalles imprévisibles et que l'hyperviseur est ESXi5, effectuez les actions suivantes :

- Assurez-vous que l'hyperviseur du serveur NTP est configuré et fonctionne.
- Vérifiez que le serveur NTP QuickFile et l'hyperviseur sous-jacent utilisent le même serveur NTP.

Interruption ou reprise d'une tâche

Vous pouvez interrompre une tâche qui est en cours d'exécution ou redémarrer une tâche interrompue.

Pourquoi et quand exécuter cette tâche

QuickFile doit compléter systématiquement certaines tâches pour que le système fonctionne facilement. Après avoir planifié les tâches à exécuter régulièrement, vous pouvez interrompre une tâche et la reprendre plus tard.

Pour interrompre une tâche et la redémarrer plus tard, complétez la procédure suivante :

Procédure

1. Cliquez sur **Règles** dans le menu.
2. Cliquez sur l'onglet **Planification**.
3. Permettez à la tâche de s'interrompre et cliquez sur **Interrompre**.
4. Pour redémarrer la tâche, complétez les étapes suivantes :
   a. Cliquez sur **Afficher toutes les tâches** pour afficher toutes les tâches.
   b. Permettez à la tâche de redémarrer et cliquez sur **Reprendre**.

Configuration de la purge des événements

Les événements système peuvent être purgés et exportés pour réduire le nombre d'événements répertoriés dans les journaux et maintenir les performances de votre système.

Pourquoi et quand exécuter cette tâche

La purge des événements est suspendue par défaut. Pour relancer **PurgeEvents** ou modifier la durée pendant laquelle les événements sont conservés, procédez comme suit :

Procédure

1. Dans le menu **Administration**, sélectionnez **Règles** et cliquez sur l'onglet **Plannings**.
2. Cliquez sur **Afficher toutes les tâches**. Quand vous installez QuickFile pour la première fois, le statut de la tâche **PurgeEvents** est défini sur **Suspendu**.
3. Pour lancer la purge des événements système, sélectionnez **Reprendre** dans la case de sélection pour **PurgeEvents**. L'étiquette est modifiée sur **Planifiée**.
4. Quand **PurgeEvents** est défini sur **Planifié**, dans le menu **Administration**, sélectionnez **Configuration** et clqiuez sur l'onglet **Système**.
5. Pour modifier la durée de conservation des événements, sélectionnez l'une des valeurs suivantes, en nombre de jours :

- 15
- 30 (valeur par défaut)
- 60
- 90

La tâche **PurgeEvents** purge les événements en fonction de l'intervalle que vous avez défini. La tâche purge les événements du système pendant un nombre de jours qui dépasse le paramètre du temps de conservation. Par défaut, la tâche s'exécute toutes les semaines le dimanche à minuit pour purger les événements antérieurs à 30 jours. Consultez «Planification des tâches de maintenance», à la page 63.

6. Cliquez sur **Enregistrer**.

   Conseil : Vous n'avez pas besoin de redémarrer QuickFile pour que les modifications soient appliquées.
7. Vous pouvez définir la tâche **PurgeEvents** pour exécuter une seule fois et immédiatement en sélectionnant **Exécuter**.

Résultats

Une notification par e-mail est envoyée à tous les administrateurs système lorsque **PurgeEvents** se termine, si les conditions suivantes sont réunies :

- Le compte de messagerie de l'administrateur est valide et configuré
- Les notifications par e-mail sont activées dans le profil utilisateur de l'administrateur

L'e-mail de notification contient un lien permettant de télécharger un fichier CSV des événements exportés. Vous pouvez également télécharger les fichiers journaux exportés depuis la liste Received files (Fichiers reçus) pour tous les administrateurs. Les fichiers journaux exportés ont les caractéristiques suivantes :

- Une taille de fichier maximale (100 Mo). Si la liste des événements purgés dépasse la taille de fichier maximale, plusieurs fichiers générés. Chaque fichier est répertorié séparément dans la liste Received files (Fichiers reçus) et génère un e-mail de notification séparé.

  Restriction : La taille de fichier maximale pour la liste des événements purgés n'estpas gérée par le paramètre de taille maximale du fichier système.
- Format CSV
- Une durée d'expiration définie sur 90 jours.

  Restriction : Après 90 jours, les fichiers ne sont plus récupérables, sauf les archives (si l'archivage est activé).
- Le nom de fichier est `archived-events-`*`timestamp`*`.csv`, où *timestamp* est au format `aaaaMMjj_HHmmss`

Important : Lorsque vous mettez une version précédente à niveau, les événements de la version précédente sont déplacés sur la nouvelle installation. Les mêmes paramètres pour **PurgeEvents** s'appliquent à ces événements. En fonction de l'âge des événements de votre système, la première exécution de la tâche **PurgeEvents** purge les événements déplacés.

Définition de zone Planificateur de tâches

Définissez les zones dans l'onglet Planification de Règles d'administration pour définir les tâches affichées et à quelle fréquence la planification est exécutée.

Nom de zone	Définition
Afficher seulement les tâches planifiées	Cliquez sur cette option pour afficher seulement les tâches avec une planification établie. Valeur implicite.
Afficher toutes les tâches	Cliquez sur cette option pour afficher toutes les tâches indépendamment de leur planification. Facultatif.
Nom	Nom de la tâche. Les tâches de cette liste sont déterminées par le serveur et ne sont pas modifiables. Les tâches ne peuvent pas être ajoutées ou supprimées. Cliquez sur le nom de la tâche pour modifier sa planification. Les valeurs suivantes sont valides : • **Cycle de vie** • **Notification** • **Purge** • **PurgeEvents** • **Mémento** • **Etat** • **Utilisateur**
Etat	Indique si un planning est mis en place pour la tâche et si la tâche est en cours d'exécution ou interrompue. Les valeurs suivantes sont valides : • **Planifiée** • **Non planifiée** • **Exécution en cours** • **Interrompue**
Intervalle	Intervalle de planification. Voir «Règle pour la planification des tâches de maintenance», à la page 60 pour les valeurs possibles pour cette zone. Affichage uniquement.
Exécution suivante	Date et heure auxquelles la tâche est planifiée pour s'exécuter. Exprimé en date (ou Aujourd'hui si planifiée ainsi) et en heure. Affichage uniquement.

Règle pour les exigences liées aux mots de passe

En tant qu'administrateur, vous pouvez définir une règle qui définit les exigences relatives à un mot de passe valide.

Vous pouvez inclure une ou plusieurs exigences de mot de passe suivantes :

- Vulnérabilité des mots de passe
- Définition de la complexité des mots de passe
- Durée minimum et maximum

- Nombre de mots de passe dans l'historique qui ne peuvent pas être utilisés dans la réinitialisation du mot de passe
- Si un utilisateur est autorisé à réinitialiser un mot de passe et pour combien de temps

Définition d'une règle sur les mots de passe

En tant qu'administrateur, vous pouvez définir les règles utilisées pour définir les mots de passe.

Pourquoi et quand exécuter cette tâche

QuickFile fournit la méthode pour définir les règles sur l'accès sécurisé de l'utilisateur. Les paramètres des règles sur les mots de passe gèrent les exigences pour le niveau de sécurité et la durée du mot de passe et définissent les paramètres à utiliser pour réinitialiser les mots de passe.

Si votre environnement utilise le protocole LDAP pour gérer les utilisateurs et les mots de passe, utilisez pour configurer les utilisateurs de QuickFile. Les utilisateurs qui se connectent à l'aide des données d'identification LDAP sont gérés par LDAP et pas par les règles de QuickFile. Par conséquent, les utilisateurs LDAP doivent utiliser LDAP pour réinitialiser leur mot de passe. Si un utilisateur LDAP se connecte avec un mot de passe expiré, l'utilisateur est notifié par QuickFile et invité à contacter l'administrateur LDAP.

Complétez la procédure suivante pour définir les règles sur les mots de passe :

Procédure

1. Cliquez sur **Règles** dans le menu.
2. Cliquez sur l'onglet **Mot de passe**.
3. Pour définir les exigences du niveau de sécurité du mot de passe :
   a. Cliquez sur **Niveau de sécurité** pour afficher les options du niveau de sécurité.
   b. Entrez une valeur dans la zone **Nombre minimum de caractère dans les mots de passe**.
   c. Définissez les types de caractère que les utilisateurs doivent inclure dans un mot de passe valide dans les options de caractère.
   d. Si nécessaire, entrez une valeur dans les zones **Nombre maximum de caractère identique autorisé consécutivement** et **Nombre maximum d'occurrence du même caractère** pour définir une limite de caractère consécutif et des limites de caractère total.
4. Complétez les étapes suivantes pour définir la durée de validité d'un mot de passe :
   a. Cliquez sur **Durée**.
   b. Définissez les limites de changement minimum, le temps minimum entre les changements de mot de passe et le nombre de mots de passe à conserver dans l'historique.
   c. Définissez les exigences de durée maximum dans les expirations de mot de passe, au cours de laquelle le mot de passe expire. Définissez les avertissements d'expiration de mot de passe.
5. Pour définir les exigences de réinitialisation de mot de passe, cliquez sur **Réinitialiser** et définissez une ou plusieurs exigences de réinitialisation suivantes :

a. Pour permettre aux utilisateurs de réinitialiser leur mot de passe, cochez **Permettre aux utilisateurs de réinitialiser les mots de passe**.
b. Pour empêcher les utilisateurs de réinitialiser leur mot de passe, décochez **Permettre aux utilisateurs de réinitialiser les mots de passe**.
c. Pour définir **Durée avant que la demande de réinitialisation de mot de passe expire**, sélectionnez la durée et le nombre d'unités de temps.

6. Cliquez sur **Enregistrer**.

Définitions de zone Règles sur les mots de passe

Utilisez les définitions suivantes sur la page **Règles sur les mots de passe**. Entrez un zéro dans une zone si vous ne souhaitez pas demander cette définition dans le mot de passe.

Nom de zone	Description
Nombre minimal de caractères dans les mots de passe	Nombre minimal de caractères qu'un mot de passe peut contenir. L'intervalle est entre 6 et 128. Le nombre total de caractères minuscules, majuscules, numériques et spéciaux indiqués dans les quatre zones suivantes dépassent cette valeur. Obligatoire.
Nombre minimal de caractères minuscules	Nombre minimal de caractères minuscules qu'un mot de passe peut contenir. L'intervalle est entre 0 et 128. Facultatif.
Nombre minimal de caractères majuscules	Nombre minimal de caractères majuscules qu'un mot de passe peut contenir. L'intervalle est entre 0 et 128. Facultatif.
Nombre minimal de caractères numériques	Nombre minimal de caractères numériques qu'un mot de passe peut contenir. L'intervalle est entre 0 et 128. Facultatif.
Nombre minimal de caractères spéciaux	Nombre minimal de caractères spéciaux qu'un mot de passe peut contenir. L'intervalle est entre 0 et 128. Les caractères suivants sont considérés comme des caractères spéciaux : ~ `! @ # $ % ^ & * ( ) - _ + = { } [ ] | \: ; " ' < >,. ? / Facultatif.
Nombre maximal de caractères identiques autorisés consécutivement	Nombre maximal d'instances consécutives d'un même caractère autorisé dans un mot de passe. L'intervalle est entre 0 et 128. Zéro indique qu'il n'y a aucune limite relative aux caractères consécutifs. Facultatif.

Nom de zone	Description
Nombre maximal d'occurrences du même caractère	Le nombre maximal de caractère que le mot de passe peut contenir. L'intervalle est entre 0 et 128. Zéro indique qu'il n'y a pas de limite quant aux répétitions d'un caractère. Facultatif.
Nombre minimal des limites de changement	Cocher cette case permet de définir une durée minimale entre les changements du mot de passe de l'utilisateur et active l'historique de mot de passe. Facultatif.
Durée minimale entre les changements de mot de passe	Durée minimale qui doit s'écouler entre les changements de mot de passe d'un utilisateur. Sélectionnez le chiffre (1 - 100) et les unités (minutes, heures, jours, semaines, mois, années). Si l'option **Expirations de mot de passe** est cochée, la valeur spécifiée ici ne peut pas dépasser la valeur de la zone **Le mot de passe expire le**. Si l'option **Expirations de mot de passe** n'est pas cochée, la valeur spécifiée ici ne peut pas dépasser 30 jours. Facultatif.
Nombre de mots de passe conservés dans l'historique	Combien d'anciens mots de passe sont conservés dans l'historique. L'intervalle est entre 0 et 99. Facultatif.
Expirations de mot de passe	Durée maximale autorisée entre les changements de mot de passe. Facultatif
Le mot de passe expire le	Durée pendant laquelle les utilisateurs doivent changer leur mot de passe. Sélectionnez un chiffre entre 1 et 365 et les unités en heures, jours, semaines, mois et années.
Avertir les utilisateurs avant l'expiration du mot de passe	Générez un avertissement avant l'expiration du mot de passe d'un utilisateur (en fonction du paramètre Le mot de passe expire le). Sélectionnez 1-30 jours.
Permettre aux utilisateurs de réinitialiser les mots de passe	Cochez cette case pour permettre aux utilisateurs de réinitialiser leur mot de passe. Facultatif.
Durée avant que la demande de réinitialisation du mot de passe expire	Durée après laquelle la demande de réinitialisation du mot de passe d'un utilisateur expire. Lorsqu'un utilisateur clique sur **J'ai oublié mon mot de passe** sur la page Connexion, QuickFile envoie un code d'accès à l'utilisateur. L'utilisateur doit cliquer sur le lien dans l'e-mail et modifier le mot de passe pendant ce laps de temps et fournir le code d'accès pour réinitialiser le mot de passe. Sélectionnez un chiffre (1-100) et les unités (minutes, heures). Facultatif.

Règles pour la date d'expiration et la taille de fichier des transferts

En tant qu'administrateur, vous pouvez définir les règles sur l'ensemble du système qui affectent le moment où le transfert de fichiers expire. Vous pouvez également définir si les notifications sont envoyées aux utilisateurs lorsque leurs fichiers sont sur le point d'expirer. Vous pouvez définir si les utilisateurs peuvent choisir d'être notifiés lorsqu'ils reçoivent les fichiers. Vous pouvez également définir une taille maximale pour les fichiers individuels que les utilisateurs sont autorisés à envoyer.

Pourquoi et quand exécuter cette tâche

Pour définir les règles de gestion des systèmes, complétez la procédure suivante :

Procédure

1. Sélectionnez **Règles** à partir du menu.
2. Cliquez sur l'onglet **Gestion des systèmes**.
3. Pour gérer les expirations de fichier :
   a. Cliquez sur **Expirations** pour développer la section.
   b. Définissez la période d'expiration de fichier par défaut en sélectionnant le chiffre et les unités pour l'option **Expiration par défaut de tous les fichiers envoyés par les utilisateurs système**.
   c. Pour permettre aux utilisateurs de redéfinir l'expiration par défaut, cochez l'option **Permettre aux utilisateurs finaux de redéfinir la durée d'expiration du fichier par défaut**.
4. Complétez les étapes suivantes pour définir le moment où les notifications d'expiration sont envoyées :
   a. Cliquez sur **Notifications d'expiration** pour développer la section.
   b. Définissez une notification finale en cochant l'option **Envoyer une notification d'avertissement finale avant l'expiration du transfert**. Sélectionnez combien de temps avant l'expiration d'un transfert de fichier la notification finale est envoyée.
   c. Définissez une notification initiale en cochant l'option **Envoyer une notification d'avertissement finale avant l'expiration du transfert**. Sélectionnez combien de temps avant l'expiration la notification initiale est envoyée.
   d. Pour modifier la fréquence des notifications, cliquez sur **Modifier le rappel de la planification de tâche**. Voir «Règle pour la planification des tâches de maintenance», à la page 60.
5. Pour définir la taille maximale de fichier qui peut être transmise, cliquez sur **Taille de fichier** et entrez une taille maximale en mégaoctets.
6. Cliquez sur **Enregistrer**.

Gestion des règles utilisateur

Gérez les règles utilisateur, y compris qui peut envoyer des fichiers à un utilisateur non enregistré, si un utilisateur non enregistré peut recevoir des fichiers et qui peut inviter un utilisateur non enregistré à s'enregistrer.

Utilisez les procédures suivantes pour gérer les règles utilisateur :

- «Définition des restrictions de transfert de fichier», à la page 71

- «Définition des utilisateurs autorisés à envoyer des invitations d'enregistrement»

Définition des restrictions de transfert de fichier

Définissez le type d'utilisateurs qui peut envoyer un transfert de fichiers et le type d'utilisateurs qui peut recevoir les fichiers.

Pourquoi et quand exécuter cette tâche

Utilisez cette procédure pour définir qui peut transférer les fichiers et demander les fichiers à partir d'utilisateurs non enregistrés. Vous pouvez empêcher les utilisateurs externes de recevoir des fichiers. La valeur par défaut permet à tout le monde d'envoyer et de recevoir des fichiers. Vous pouvez empêcher les utilisateurs externes d'envoyer et de recevoir des fichiers.

Complétez la procédure suivante pour définir les restrictions de transfert de fichier :

Procédure

1. Cliquez sur **Règles** à partir du menu.
2. Cliquez sur l'onglet **Gestion des utilisateurs**.
3. Cliquez sur **Transferts de fichiers**.
4. Pour définir qui est autorisé à envoyer des fichiers aux utilisateurs externes, sélectionnez l'une des options suivantes :
   - Pour empêcher les utilisateurs externes d'envoyer des fichiers à d'autres utilisateurs, sélectionnez **Seuls les utilisateurs internes peuvent envoyer des fichiers aux utilisateurs externes**.
   - Pour autoriser tout utilisateur enregistré à envoyer des fichiers à tout le monde, sélectionnez **Utilisateurs internes et externes peuvent envoyer des fichiers à tout le monde**.
5. Pour définir qui est autorisé à recevoir des transferts de fichiers, activez l'une des options suivantes :
   - Pour empêcher les utilisateurs non enregistrés de recevoir des fichiers, activez **Les fichiers de transfert ne peuvent pas être envoyés aux utilisateurs non enregistrés**.
   - Pour autoriser tous les utilisateurs à envoyer des transferts de fichiers, activez **Les transferts de fichiers peuvent être envoyés à tout le monde**.
6. Cliquez sur **Enregistrer**.

Définition des utilisateurs autorisés à envoyer des invitations d'enregistrement

Définissez les utilisateurs qui peuvent envoyer des invitations d'enregistrement en les définissant dans la règle Gestion des utilisateurs. Un utilisateur enregistré est autorisé à envoyer et à recevoir des fichiers, si l'administrateur active les autorisations. Un utilisateur enregistré peut également voir les informations relatives au nombre de transferts de fichiers qui ont été envoyés et reçus.

Pourquoi et quand exécuter cette tâche

La règle Gestion des utilisateurs identifie :

- Les utilisateurs qui peuvent envoyer des invitations d'enregistrement
- Si les utilisateurs peuvent envoyer des fichiers à des utilisateurs externes

- Si les transferts de fichiers peuvent être demandés ou envoyés à partir des utilisateurs non enregistrés
- Combien de temps un utilisateur non enregistré est autorisé à s'enregistrer après que l'utilisateur a reçu une invitation

Pour définir la règle Gestion des utilisateurs :

Procédure

1. Cliquez sur **Règles** à partir du menu.
2. Cliquez sur l'onglet **Gestion des utilisateurs**.
3. Cliquez sur **Invitation à s'enregistrer**.
4. Activez l'une des options suivantes
   - Pour empêcher les utilisateurs d'envoyer des invitations d'enregistrement, activez **Interdire aux utilisateurs d'inviter d'autres utilisateurs à s'enregistrer**.
   - Pour autoriser seulement à les utilisateurs internes à envoyer des invitations d'enregistrement, activez **Seuls les utilisateurs internes peuvent inviter d'autres utilisateurs à s'enregistrer**.
   - Pour autoriser tous les utilisateurs à envoyer des invitations d'enregistrement, activez **Autoriser les utilisateurs à inviter d'autres utilisateurs à s'enregistrer**.
5. Définissez le nombre de jours pendant lesquels une invitation est active dans la zone **Les invitations pour s'enregistrer expirent dans**.
6. Cliquez sur **Enregistrer**.

Définitions de zone des règles de transfert de fichier

La définition du transfert de fichier sur la page **Règles de gestion des utilisateurs** définit qui peut envoyer des transferts de fichiers à des utilisateurs externes.

Nom de zone	Description
Seuls les utilisateurs internes peuvent envoyer des fichiers aux utilisateurs externes	Sélectionnez cette option pour permettre seulement aux utilisateurs internes d'envoyer des fichiers aux utilisateurs hors de la société.
Les utilisateurs internes et externes peuvent envoyer des fichiers à tout le monde	Sélectionnez cette option pour permettre à la fois aux utilisateurs internes et externes d'envoyer des fichiers les uns aux autres. Un utilisateur interne est défini sur le domaine de la société. Un utilisateur externe est un utilisateur hors du serveur de la société.
Les transferts de fichiers ne peuvent pas être envoyés aux utilisateurs non enregistrés	Sélectionnez cette option pour empêcher les transferts de fichiers d'être envoyés aux utilisateurs non enregistrés.
Les transferts peuvent être envoyés à tout le monde	Sélectionnez cette option pour permettre à tous les utilisateurs d'envoyer des fichiers aux utilisateurs non enregistrés.

Définitions de zone Règles relatives aux invitations à s'enregistrer

Vous pouvez configurer les zones de la règle relative aux invitations à s'enregistrer pour définir qui peut inviter un utilisateur externe à s'enregistrer.

Nom de zone	Description
Interdire aux utilisateurs d'inviter d'autres utilisateurs à s'enregistrer	Empêche tous les utilisateurs de demander aux autres utilisateurs de s'enregistrer.
Seuls les utilisateurs internes peuvent inviter d'autres utilisateurs à s'enregistrer	Permet aux utilisateurs internes seulement d'envoyer une demande d'enregistrement à un utilisateur externe.
Les utilisateurs internes et externes peuvent inviter d'autres utilisateurs à s'enregistrer	Permet à tous les utilisateurs d'inviter d'autres utilisateurs à s'enregistrer.
Les invitations à s'enregistrer expirent le	Identifiez quand une invitation expire. La valeur par défaut est de 7 jours. Entrez le nombre d'unités et sélectionnez l'unité de mesure : heures, jours, semaines, mois, années.

Chapitre 8. Gestion des comptes utilisateur

En tant qu'administrateur, utilisez la page Utilisateurs pour ajouter des utilisateurs et verrouiller de façon permanente des utilisateurs du système. Vous pouvez également réinitialiser l'enregistrement d'un utilisateur, affecter des droits administratifs, définir un type d'authentification et supprimer un utilisateur.

Vous pouvez ajouter des utilisateurs individuels à QuickFile. Définissez si l'utilisateur est un administrateur ou un utilisateur standard. Vous pouvez également définir si l'utilisateur est authentifié via QuickFile ou via une annuaire de société. Vous pouvez empêcher un utilisateur d'utiliser ses données d'identification pour se connecter au système.

Vous pouvez configurer un utilisateur pour qu'il soit authentifié via l'annuaire de société du protocole LDAP. Commencez par configurer un serveur avec le protocole LDAP. Puis, demandez à l'utilisateur de se connecter à QuickFile. L'utilisateur est ensuite ajouté à la liste des utilisateurs et est identifié comme un utilisateur du protocole LDAP.

Lorsque vous authentifier des utilisateurs via le serveur LDAP, ils ne peuvent pas modifier leur mot de passe QuickFile via QuickFile. Les utilisateurs du protocole LDAP doivent modifier leur mot de passe via l'annuaire de société.

Création ou modification d'un compte utilisateur

Utilisez QuickFile pour ajouter un utilisateur au système. Après l'ajout de l'utilisateur, il reçoit un avis Enregistrement d'un nouvel utilisateur. L'utilisateur doit cliquer sur le lien de l'avertissement par e-mail et définir un mot de passe dans un laps de temps de 7 jours. Si ce n'est pas le cas, l'enregistrement expire. Vous pouvez réinitialiser un compte utilisateur pour donner plus de temps à l'utilisateur pour s'enregistrer. Après avoir créé un compte utilisateur, vous pouvez modifier le compte et modifier n'importe quel paramètre. L'accès aux outils d'administration est limité aux administrateurs.

Avant de commencer

Pour créer un compte utilisateur :

Procédure

1. Cliquez sur **Utilisateurs** à partir du menu. La liste des utilisateurs en cours s'affiche.

   Les colonnes répertorient le nom d'utilisateur, le rôle, les groupes auxquels l'utilisateur est affecté, le type d'utilisateur et l'état du compte de l'utilisateur.
2. Cliquez sur **Créer**.
3. Entrez l'**Adresse e-mail** de l'utilisateur. Entrez la même adresse dans la zone **Confirmer l'adresse e-mail**.
4. Entrez le **Nom complet** de l'utilisateur.
5. Cliquez sur **Créer**.

Que faire ensuite

Pour modifier un profil existant, cliquez sur le nom d'utilisateur dans la liste des utilisateurs.

Suppression d'un compte utilisateur

Vous pouvez ajouter un compte utilisateur ou un compte utilisateur peut être ajouté lorsqu'un utilisateur s'enregistre. Utilisez la page **Utilisateur** pour supprimer un compte utilisateur qui n'est plus nécessaire.

Pourquoi et quand exécuter cette tâche

Pour supprimer un compte utilisateur, complétez la procédure suivante :

Procédure

1. Cliquez sur **Utilisateurs** à partir du menu. La liste des utilisateurs en cours s'affiche.
2. Pour supprimer un utilisateur, cochez la case à côté du nom d'utilisateur à modifier et cliquez sur **Supprimer**.
3. Cliquez sur **Supprimer** pour confirmer la suppression.

   Avertissement : Après la suppression d'un compte utilisateur, cet utilisateur ne peut plus se connecter à nouveau et l'activité n'est plus disponible. L'utilisateur doit s'enregistrer pour utiliser le système.

Réinitialisation de la configuration d'un compte utilisateur

Lorsque vous créez un compte utilisateur, un avis d'enregistrement d'un nouveau utilisateur est envoyé à l'utilisateur. Pour compléter la configuration d'un compte utilisateur, l'utilisateur doit cliquer sur le lien dans l'avis et définir un mot de passe. Le processus doit être complété dans une période de sept jours ou la configuration du compte utilisateur expire.

Avant de commencer

Si la configuration utilisateur expire, l'administrateur peut réinitialiser le compte utilisateur. L'utilisateur a ensuite sept jours supplémentaires pour mettre à jour le mot de passe.

Pour réinitialiser la configuration du compte utilisateur :

Procédure

1. Cliquez sur **Utilisateurs** à partir du menu. La liste des utilisateurs en cours s'affiche.
2. Cochez la case à côté du nom d'utilisateur à réinitialiser.
3. Cliquez sur **Plus** > **Réinitialiser**.

Extension d'un compte utilisateur

Les administrateurs système définissent le temps pendant lequel le compte d'un utilisateur externe est actif dans la règle d'expiration des comptes utilisateur.

Pourquoi et quand exécuter cette tâche

Les comptes des utilisateurs externes expirent après une certaine période. Sept jours avant l'expiration du compte, l'utilisateur reçoit une notification d'expiration de compte. L'utilisateur peut demander une extension en cliquant sur le lien dans l'e-mail de notification. Lorsque l'utilisateur demande une extension, vous pouvez étendre le compte.

Pour étendre le compte utilisateur et affecter une nouvelle date d'expiration :

Procédure

1. Cochez la case que vous souhaitez modifier.
2. Cliquez sur **Utilisateurs** à partir du menu de navigation.
3. Cliquez sur **Plus** > **Réinitialiser** > **Expirations de compte**.
4. Sélectionnez la nouvelle date d'expiration et cliquez sur **Enregistrer**.

   Restriction : Si l'administrateur n'est pas défini avec une adresse électronique valide, les utilisateurs externes en cours d'expiration ne peuvent pas étendre le compte à partir de la notification d'expiration.

Verrouiller ou déverrouiller un utilisateur

Utilisez QuickFile pour verrouiller un utilisateur et lui empêcher l'accès au système. Vous pouvez également déverrouiller un utilisateur que vous avez verrouillé.

Avant de commencer

Pour verrouiller un utilisateur ou déverrouiller un utilisateur :

Procédure

1. Cliquez sur **Utilisateurs** à partir du menu. La liste des utilisateurs en cours s'affiche.
2. Pour empêcher un utilisateur de se connecter à QuickFile, cochez la case à côté du nom d'utilisateur et cliquez sur **Plus** > **Verrouillage**.
3. Pour déverrouiller un compte utilisateur, cochez la case à côté du nom d'utilisateur et cliquez sur **Plus** > **Déverrouillage**.

Changement du rôle affecté à un utilisateur

En tant qu'administrateur, vous pouvez changer les responsabilités d'un utilisateur. Par défaut, un utilisateur est défini comme un utilisateur de base. L'utilisateur peut envoyer un fichier et en recevoir mais il ne peut pas modifier les règles, les paramètres d'environnement ou ajouter des utilisateurs. Les administrateurs peuvent effectuer toutes les fonctions qu'un utilisateur peut effectuer et il peut également définir des règles, configurer l'environnement et ajouter des utilisateurs. L'accès aux outils d'administration est limité aux administrateurs.

Avant de commencer

Complétez les étapes suivantes pour changer le rôle d'un utilisateur :

Procédure

1. Cliquez sur **Utilisateurs** à partir du menu.
2. Cochez la case de l'utilisateur à modifier.
3. Cliquez sur **Plus** > **Rôle de l'utilisateur** et sélectionnez le rôle à affecter à l'utilisateur :
   - Administrateur
   - Utilisateur

Modification du type d'authentification d'un compte utilisateur

Configurez QuickFile pour identifier comment un utilisateur est authentifié. Sélectionnez QuickFile ou LDAP pour gérer les données d'identification de l'utilisateur de chaque utilisateur. Les utilisateurs authentifiés par LDAP sont définis par le serveur LDAP. Les utilisateurs LDAP se connectent à QuickFile avec leurs données d'identification LDAP. Les utilisateurs LDAP n'ont pas besoin de s'enregistrer avec QuickFile.

Avant de commencer

Le protocole LDAP est un protocole Internet au norme de l'industrie. Il stocke les informations de l'utilisateur et y accède à partir d'un serveur LDAP. Si votre société utilise LDAP, vous pouvez rendre ces données disponibles sur QuickFile.

Restriction : L'option LDAP pour la société est active seulement si vous établissez une connexion entre QuickFile et votre serveur LDAP.

Avec une connexion LDAP, vous pouvez définir les utilisateurs et les groupes d'utilisateurs avec un protocole LDAP et éliminer le besoin de définir les utilisateurs dans QuickFile.

Si vous activez le protocole LDAP, n'utilisez pas QuickFile pour ajouter et gérer les données d'identification de l'utilisateur. Utilisez plutôt les outils LDAP. Si un utilisateur essaie de se connecter à QuickFile avec un mot de passe LDAP expiré, l'utilisateur est notifié de l'expiration du mot de passe. L'utilisateur ou l'administrateur LDAP doit modifier ou réinitialiser le mot de passe dans l'annuaire LDAP. L'annuaire LDAP est créé et géré séparément à partir de QuickFile.

Pour modifier le type d'authentification d'un utilisateur :

Procédure

1. Cliquez sur **Utilisateurs** à partir du menu. La liste des utilisateurs en cours s'affiche.
2. Cochez la case à côté du nom d'utilisateur à modifier et cliquez sur **Plus** > **Type d'authentification** et sélectionnez le type d'authentification :
   - LDAP société : pour utiliser LDAP
   - Application : pour utiliser QuickFile

   Avertissement : Si vous basculez le type d'authentification de LDAP société à Application, l'utilisateur reçoit un e-mail avec un code d'accès et des instructions pour configurer son mot de passe dans QuickFile.

Définitions de zone Liste de compte utilisateur

Utilisez la page Liste de compte utilisateur pour afficher les informations utilisateur de chaque utilisateur défini.

Nom de zone	Description
Nom	Nom complet de l'utilisateur, comme indiqué lorsque le compte utilisateur a été créé, ou modifié par l'utilisateur ou l'administrateur. Obligatoire.
Rôle	Type d'utilisateur Un Utilisateur est un utilisateur régulier qui peut envoyer et recevoir des fichiers mais qui ne peut pas ajouter des utilisateurs ou des règles. Un Admin peut ajouter des règles, ajouter et modifier les utilisateurs, verrouiller et déverrouiller les utilisateurs, supprimer les utilisateurs et modifier les paramètres de configuration.
Groupes	Le groupe QuickFile sur lequel l'utilisateur est assigné. L'utilisateur peut être affecté seulement à 1 groupe. Les utilisateurs administrateur ne peuvent pas être ajoutés à un groupe lorsque vous définissez l'utilisateur. Cependant, les utilisateurs administrateur sont ajoutés à un groupe par défaut, s'il en existe un.
Type	Identifie un utilisateur comme étant interne ou externe. Un utilisateur interne est défini sur le domaine de la société. Un utilisateur externe est un utilisateur hors du serveur de la société.
Etat	Etat du compte utilisateur. Les valeurs suivantes sont valides : • lock • unlock • delete • pending registration • registration expired • departed Departed est un utilisateur qui est supprimé du protocole LDAP et tente de se reconnecter au système.

Définitions de zone Compte utilisateur

Utilisez la page Compte utilisateur pour créer et afficher les informations utilisateur. Vous pouvez créer un compte utilisateur ou afficher les informations relatives à un compte existant. Vous pouvez supprimer un compte utilisateur. Vous pouvez modifier le type de compte, le rôle de l'utilisateur et la méthode d'authentification. En cliquant sur le nom d'un utilisateur, vous pouvez afficher et modifier des informations sur la page Profil de l'utilisateur.

Nom de zone	Description
Adresse e-mail	Adresse e-mail utilisée pour envoyer et recevoir des fichiers. Indiquez cette valeur lorsque vous créez un utilisateur via la boîte de dialogue Créer utilisateur.
Confirmer l'adresse électronique	Lorsque vous ajoutez le compte utilisateur, entrez à nouveau l'adresse e-mail pour vérification. Obligatoire.
Nom complet	Le nom complet. Obligatoire.

Chapitre 9. Utilisation des groupes pour gérer les paramètres utilisateur

Créez un groupe et ajoutez des utilisateurs au groupe pour affecter rapidement les mêmes règles à un groupe d'utilisateurs.

Assurez-vous de définir les règles par défaut avant de définir un groupe. Vous pouvez ensuite affecter les règles par défaut, y compris la gestion des fichiers, le mot de passe et les règles de verrouillage au groupe. En fonction des exigences utilisateur, vous pouvez créer un groupe et définir une règle personnalisée pour une ou plusieurs règles. Un utilisateur peut être affecté à un groupe seulement.

Création d'un groupe

Vous pouvez définir rapidement les fonctions qu'un utilisateur peut effectuer en créant un groupe, en associant des règles au groupe et en ajoutant des utilisateurs au groupe. Au besoin, vous pouvez modifier et supprimer des groupes.

Pourquoi et quand exécuter cette tâche

Pour créer un groupe et ajouter des utilisateurs et des règles au groupe :

Procédure

1. Cliquez sur **Groupes** à partir du panneau de navigation.
2. Pour créer un groupe, cliquez sur **Création**.
3. Saisissez un nom et une description pour le groupe.
4. Pour utiliser ce groupe comme le groupe par défaut pour tout nouvel utilisateur enregistré, cliquez sur **En faire le groupe par défaut pour les utilisateurs nouvellement enregistrés**.
5. Cliquez sur **Suivant**.
6. Pour utiliser les règles par défaut, cochez **Utiliser les règles par défaut pour le groupe**.
7. Pour définir les paramètres personnalisés pour l'une des régions suivantes, cliquez sur **Définir une règle personnalisés pour ce groupe**. Définissez les paramètres pour la définition de règle en fonction des instructions répertoriées dans le tableau suivant :

Règle à personnaliser	**Lien vers la procédure**
Règles de verrouillage temporaire	«Configuration des règles de verrouillage utilisateur», à la page 57 **Restriction :** Les expirations de compte ne peuvent pas être définies au niveau du groupe. Elles sont activées ou désactivées pour tous les utilisateurs.
Règles sur les mots de passe	«Définition d'une règle sur les mots de passe», à la page 67
Règles sur la gestion des systèmes	«Règles pour la date d'expiration et la taille de fichier des transferts», à la page 70

Règle à personnaliser	Lien vers la procédure
Règles sur la gestion des utilisateurs	«Définition des utilisateurs autorisés à envoyer des invitations d'enregistrement», à la page 71 «Définition des restrictions de transfert de fichier», à la page 71

8. Cliquez sur **Suivant** pour avancer dans l'assistant.
9. Pour ajouter un utilisateur au groupe, procédez comme suit :
   a. Sélectionnez l'utilisateurs dans le panneau **Utilisateurs disponibles**.
   b. Cliquez sur **Ajouter les utilisateurs sélectionnés au groupe** (flèche de droite) pour déplacer l'utilisateur dans le panneau **Utilisateurs sélectionnés**.
   c. Cliquez sur **Suivant**.
10. Sur la page **Récapitulatif**, confirmez que tous les paramètres sont valides et cliquez sur **Terminer**.

Modification d'un groupe

Vous pouvez modifier un groupe pour changer les informations, y compris les utilisateurs affectés à un groupe et les règles qui y sont associées.

Pourquoi et quand exécuter cette tâche

Pour modifier un groupe, complétez les étapes suivantes :

Procédure

1. Cliquez sur **Groupes** à partir du panneau de navigation.
2. Pour modifier un groupe existant, cliquez sur le nom du groupe dans la liste.
3. Si vous le souhaitez, modifiez le nom, la description ou si ce groupe doit s'appliquer aux utilisateurs nouvellement enregistrés.
4. Pour modifier les règles associées au groupe, cliquez sur l'onglet **Règles** et modifiez un ou plusieurs paramètres :
   - Pour modifier les paramètres des règles de verrouillage, utilisez cette procédure «Configuration des règles de verrouillage utilisateur», à la page 57.
   - Pour modifier les règles de gestion des fichiers, utilisez cette procédure «Définition des restrictions de transfert de fichier», à la page 71
   - Pour modifier les règles sur les mots de passe, utilisez cette procédure «Définition d'une règle sur les mots de passe», à la page 67
   - Pour modifier les règles de gestion des systèmes, utilisez cette procédure «Règles pour la date d'expiration et la taille de fichier des transferts», à la page 70
5. Pour ajouter des utilisateurs au groupe, procédez comme suit :
   a. Cliquez sur l'onglet **Membres**.
   b. Sélectionnez les utilisateurs dans le panneau **Utilisateurs disponibles**.
   c. Cliquez sur **Ajouter les utilisateurs sélectionnés au groupe** (flèche de droite) pour déplacer les utilisateurs dans le panneau **Utilisateurs sélectionnés**.
   d. Cliquez sur **Suivant**.

6. Pour supprimer des utilisateurs d'un groupe, procédez comme suit :
   a. Cliquez sur l'onglet **Membres**.
   b. Sélectionnez les utilisateurs dans le panneau **Utilisateurs sélectionnés**.
   c. Cliquez sur **Supprimer les utilisateurs sélectionnés au groupe** (flèche de gauche) pour déplacer les utilisateurs dans le panneau **Utilisateurs disponibles**.
   d. Cliquez sur **Suivant**.
7. Sur la page **Récapitulatif**, confirmez que tous les paramètres sont valides et cliquez sur **Enregistrer**.

Suppression d'un groupe

Vous pouvez supprimer les groupes dont vous n'avez plus besoin. Vous pouvez supprimer plusieurs groupes en une seule fois.

Pourquoi et quand exécuter cette tâche

Pour supprimer un groupe :

Procédure

1. Cliquez sur **Groupes** à partir du panneau de navigation.
2. Sélectionnez les groupes à supprimer et cliquez sur **Supprimer**.
3. Cliquez sur **Supprimer** pour confirmer la suppression.

Définitions de zone Groupes

Le tableau suivant répertorie les zones de la page **Groupes** et leurs définitions :

Zone	Définition
Nom	Nom affecté au groupe.
Description	Description du groupe.
Faire de ce groupe le groupe par défaut pour les utilisateurs nouvellement enregistrés	Sélectionnez cette option pour utiliser les paramètres du groupe définis pour tous les nouveaux utilisateurs enregistrés avec QuickFile.
Définir des règles personnalisées pour ce groupe	Sélectionnez cette option pour définir les nouvelles règles personnalisées du groupe. Vous pouvez définir les paramètres pour un ou plusieurs types de règle.
Onglet Règles	Cliquez sur cet onglet pour afficher les règles que vous pouvez définir. Consultez «Configuration des règles de verrouillage utilisateur», à la page 57 pour définir les règles de verrouillage, «Définition d'une règle sur les mots de passe», à la page 67 pour configurer les règles sur les mots de passe, «Règles pour la date d'expiration et la taille de fichier des transferts», à la page 70 pour configurer les règles sur les transferts de fichiers, «Définition des restrictions de transfert de fichier», à la page 71 pour configurer les règles utilisateur et

Zone	Définition
Membres	Sélectionnez cet onglet pour définir les utilisateurs associés au groupe. Pour ajouter des utilisateurs au groupe, mettez les utilisateurs en évidence dans le panneau **Utilisateurs disponibles** et cliquez sur **Ajouter les utilisateur sélectionnés au groupe** (flèche de droite). Les utilisateurs dans le panneau **Utilisateurs sélectionnés** sont les membres du groupe.
Récapitulatif	La page du récapitulatif affiche la définition du groupe, y compris le nom et la description du groupe. Elle identifie également les règles qui sont des règles personnalisées, et combien d'utilisateurs se trouvent dans la définition du groupe.

Chapitre 10. Affichage des utilisateurs actifs

Vous pouvez afficher le nombre d'utilisateurs actifs définis dans QuickFile. Les utilisateurs sont tous les utilisateurs définis et qui ne sont pas supprimés.

Avant de commencer

Les utilisateurs actifs sont tous les utilisateurs définis dans le système. Les utilisateurs actifs comprennent les utilisateurs internes définis dans le domaine de messagerie et les utilisateurs externes définis dans le domaine de messagerie. Ils comprennent également les utilisateurs enregistrés qui se sont inscrits sur QuickFile et les utilisateurs non enregistrés.

Les données sont mises à jour lorsque vous ouvrez la page. Pour actualiser les données, fermez la page et ouvrez-la à nouveau.

Pour afficher la liste des utilisateurs actifs, sélectionnez **Administration** > **Informations système**.

Chapitre 11. Performances

Les performances de votre système QuickFile doivent être gérées en fonction des exigences de votre entreprise.

Les performances de votre système QuickFile peuvent être réduites à cause des éléments suivants :

- Nombre d'utilisateurs actifs
- Volume des transferts de fichiers
- Taille de fichier des transferts
- Activité de charge en heures pleines
- Archivage
- Purge
- Journalisation

Surveillez vos performances et comparez les performances actuelles aux critères définis pour les exigences de votre entreprise. Pour plus d'informations, consultez les rubriques suivantes :

- «Collecte et contrôle des données de performance»«Gestion et amélioration des performances», à la page 88

Collecte et contrôle des données de performance

Utilisez l'utilitaire **nmon** pour collecter et contrôler les données de performance.

Les données collectées comprennent l'utilisation du processeur, l'utilisation de la mémoire et les informations sur la file d'attente d'exécution. C'est également l'analyse des taux d'entrée et de sortie du disque, les transferts, les rapports lecture/écriture et l'espace libre disponible sur les systèmes de fichiers.

L'outil collecte et affiche les informations importantes relatives à l'utilisation des ressources système et les met à jour de façon dynamique. Entrez les commandes dans la procédure sur la console QuickFile. Vous devez avoir les droits ADMIN. Pour déplacer le fichier de collecte de données sur un autre serveur distant, celui-ci doit avoir un serveur SSH installé pour que la commande **file put** fonctionne.

Complétez les étapes suivantes pour démarrer l'utilitaire en mode collecte de données et arrêtez-le.

1. Entrez **wizard startNmon.xml** à l'invite de commande.
2. Donnez le nom du fichier de sortie sur lequel sont écrites les données.

   L'utilitaire démarre en arrière-plan.
3. Pour arrêter l'outil, entrez **wizard stopNmon.xml**.

   Conseil : Il est recommandé d'arrêter un processus **nmon** existant avant d'en démarrer un autre. Entrez **file list** pour afficher le contenu de `/tmp/userfiles`.
4. Une fois les données collectées, entrez

   `file put` *`file name protocol://user@host/path`*

pour copier les données collectées à un emplacement. Les valeurs variables sont définies dans le tableau suivant :

Tableau 10. Variables de l'utilitaire **nmon**

Variable	Définition
file name	Nom du fichier de sortie contenant les données créées par l'outil de collecte.
protocol	SCP ou FTP.
user	ID utilisateur qui peut se connecter à un hôte distant.
host	Nom d'hôte ou adresse IP du serveur distant où le fichier est copié.
path	Chemin sur l'hôte distant sur lequel le fichier est copié
Exemple de commande	**file put quickfile.nmon scp://root@192.168.60.128:/nmon-data/**

5. Si plusieurs instances de l'outil sont en cours d'exécution, entrez * pour arrêter toutes les instances.

Conseil : Pour plus d'informations sur l'utilitaire et plus d'options, voir developerWorks.

Gestion et amélioration des performances

Chapitre 12. Affichage du journal des événements système

En tant qu'administrateur, vous pouvez afficher le journal des événements qui sont générés par QuickFile.

Pourquoi et quand exécuter cette tâche

Vous pouvez afficher le journal des événements qui sont générés par QuickFile. Vous déterminez le nombre d'événements à afficher par page et triez la liste par type ou date d'événement. Par défaut, les événements sont triés d'abord par date et heure, puis par nom de l'événement.

Pour afficher les événements système :

Procédure

1. Cliquez sur **Rapports de journalisation** à partir du menu.
2. Assurez-vous que l'onglet **Evénements système** est sélectionné.
3. Pour trier la liste des événements par événement ou par date d'événement, cliquez sur l'en-tête approprié.
4. Si plus d'une page d'événements est disponible dans un rapport, cliquez sur **Suivant** pour afficher la page suivante du rapport.
5. Pour revenir à la page précédente dans le rapport d'événements, cliquez sur **Précédent**.
6. Pour afficher la dernière page des événements, cliquez sur le numéro de la dernière page dans la liste **Page**.
7. Pour afficher la première page des événements, cliquez sur le numéro de la première page dans la liste **Page**.
8. Pour passer à une page spécifique, entrez le numéro de la page dans la zone de texte **Aller à la page** ou cliquez sur le numéro de page dans la liste **Page**.

Explication du journal des événements

Les événements système peuvent être consultés par les administrateurs seulement et décrivent les événements qui se produisent dans QuickFile. Chaque message utilise le format de code `CIVxx`*`nnnn`*`T`, où *nnnn* est un numéro de message unique et *T* est le type de message. Consultez les tableaux suivants pour la description des composants de code message et des messages qui se produisent :

Composant code message	Description
xx	Préfixe du code message. Les préfixes disponibles comprennent : • ST : stockage • ID : identité • MB : boîte aux lettres • VI : visibilité • MS : messagerie • CF : configuration • CN : communication • SC : planification • CC : composants communs
H	Type de message. Les types de message disponibles comprennent : • E = erreur • I = information • W = avertissement

Descriptions des codes d'événement

Le tableau suivant identifie les messages créés dans QuickFile.

Événement	Code d'événement	Message	Description
User self registered	CIVID1001I	*user* self registered	Utilisateur qui a complété le formulaire d'inscription de la page de connexion. L'utilisateur doit cliquer sur l'e-mail d'enregistrement pour compléter le processus.
User registration expired	CIVID1002I	*user* self registration expired	Un utilisateur a complété le formulaire d'inscription de la page de connexion mais n'a pas cliqué sur le lien de l'e-mail d'enregistrement pour compléter le processus.
User invited	CIVID1003I	*user1* invited *user2* to register	*user1* a envoyé une invitation à un autre utilisateur pour qu'il s'enregistre. Pour compléter l'invitation, *user2* doit cliquer sur un lien dans l'e-mail pour terminer le processus.
User invitation declined	CIVID1004I	*user* declined to register	Un utilisateur a décliné une invitation pour s'enregistrer.
User created	CIVID1005I	*user* created by administrator	Un administrateur a ajouté un utilisateur. L'utilisateur doit cliquer sur le lien dans un e-mail pour compléter l'enregistrement d'utilisateur.
User register confirmed	CIVID1006I	*user* confirmed registration	L'utilisateur a cliqué sur un lien dans l'e-mail d'enregistrement pour terminer l'enregistrement.
User login	CIVID1007I	*user* logged in	L'utilisateur est connecté.
User logout	CIVID1008I	*user* logged out	L'utilisateur est déconnecté.
User password change	CIVID1009I	*user* changed password	L'utilisateur a modifié les mots de passe.

Événement	Code d'événement	Message	Description
User login failed	CIVID1010I	*user* failed to login; forgot password	L'utilisateur n'a pas pu se connecter car l'utilisateur a fourni un mot de passe non valide.
User AFT enabled	CIVID1011I	*user* enabled Advanced File Transfer	L'utilisateur a activé l'option AFT (Advanced File Transfer) pour permettre le transfert de gros fichiers et pour pouvoir mettre en pause et reprendre.
User AFT disable	CIVID1012I	*user* disabled Advanced File Transfer	L'utilisateur a désactivé l'option Advanced File Transfer.
User locked	CIVID1013I	*user* locked by administrator	L'utilisateur ne peut pas se connecter à QuickFile car l'administrateur a verrouillé l'utilisateur.
User unlocked	CIVID1014I	*user* unlocked by administrator	L'administrateur a déverrouillé l'utilisateur.
User locked failure	CIVID1015I	*user* locked; repeated login failures	L'utilisateur ne peut pas se connecter car il a dépassé le nombre maximum de tentatives de connexion défini par l'administrateur.
User deleted	CIVID1016I	*user* deleted by administrator	L'utilisateur a été supprimé de la base de données par l'administrateur. **A faire :** Les enregistrements utilisateur ne sont jamais supprimés de la base de données. Ils sont marqués comme supprimés et l'utilisateur ne peut plus se connecter.
User profile updated	CIVID1017I	*user* updated profile	L'utilisateur a modifié son profil.
User added to group	CIVID1018I	*user* was added to *groupn* by administrator	L'administrateur a ajouté un utilisateur à une définition de groupe. La définition de groupe détermine la règle imposée à tous les utilisateurs du groupe.
User removed from group	CIVID1019I	*user* was removed from *groupn* by administrator	L'administrateur a supprimé l'utilisateur de la définition de groupe. Les règles utilisateur imposées lorsqu'un utilisateur ne fait pas partie d'un groupe sont les paramètres par défaut.
User assigned role	CIVID1020I	*user* assigned the role of *administrator or user* by administrator	L'administrateur a modifié le rôle de l'utilisateur identifié. Les rôles disponibles sont utilisateur ou administrateur.
Group created	CIVID1021I	*group* created by administrator	L'administrateur a créé un groupe.
Group deleted	CIVID1022I	*group* deleted by administrator	L'administrateur a supprimé le groupe nommé *group*.
Group modified	CIVID1023I	*group* modified by administrator	L'administrateur a modifié le groupe.
User forgot password	CIVID1024I	*user* requested a password reset	L'utilisateur a demandé une réinitialisation du mot de passe certainement car il l'a oublié.
User authorization failed	CIVID1025I	*user* failed to login	L'utilisateur n'a pas réussi à se connecter en raison d'un mot de passe erroné.
File sent	CIVCC1001I	*user1* sent file *f* in package *p* to *user2*	L'utilisateur 1 a envoyé un fichier nommé *f* dans le package *p* à l'utilisateur 2. Le fichier est enregistré sur le serveur. L'utilisateur 2 peut maintenant télécharger le fichier.

Événement	Code d'événement	Message	Description
File resent	CIVCC1002I	*user1* resent file *f* with package subject *p* to *user2user2*	*user1* a renvoyé un fichier nommé *f* à *user2*. Le fichier est envoyé au même utilisateur que celui qui a reçu le fichier lors du premier transfert. Le fichier est enregistré sur le serveur. L'utilisateur 2 peut maintenant télécharger le fichier.
File forwarded	CIVCC1003I	*user1* forwarded file *f* with package subject *p* to *user2*	*user1* a transféré un package nommé *p* à *user2*. Le fichier est enregistré sur le serveur. L'utilisateur 2 peut maintenant télécharger le fichier.
File downloaded	CIVCC1004I	*user* downloaded a file *f*	Un utilisateur a téléchargé un fichier nommé *f*.
File requested	CIVCC1005I	*user1* requested *user2* to send file with package subject	Un utilisateur a demandé à un autre utilisateur d'envoyer un fichier.
File deleted	CIVCC1006I	*user* deleted file *f* with package subject *p*	Un utilisateur a supprimé un fichier de la liste de fichiers. Le fichier est stocké sur le serveur et est marqué pour être supprimé.
File expired	CIVCC1007I	*f* with package subject *p* sent to *user2* expired and will be deleted	Un fichier nommé *f* du package *p* a expiré
Antivirus scan fail	CIVCC1008E	*f* with package subject *p* from *sending user* contains a virus and will not be transferred.	Le fichier indiqué avec l'objet de package *p* provenant de l'expéditeur contient un virus et ne sera pas transféré.
Antivirus scan success	CIVCC1009I	*f* with package subject *p* from *sending user* was successfully scanned for viruses.	Le fichier indiqué avec l'objet de package *p* provenant de l'expéditeur a été analysé avec succès et aucun virus n'a été détecté ; le fichier sera transféré.
File removed	CIVCC1010I	*f* in *p* for *user* were abandoned after 7 days and will be removed	Le package identifié a été mis en pause et n'a pas été redémarré avant l'écoulement de la période de 7 jours. Le package est marqué pour être supprimé.
File archived	CIVCC1011I	*f* in *p* for *user* were archived	Les fichiers d'un utilisateur ont été archivés.
AFT uploaded	CIVCC1012I	*user1* uploaded *n* out of *x* bytes of *f* with package subject *p* to *user2*	*user1* a utilisé la fonctionnalité AFT (Advanced File Transfer) pour envoyer une partie d'un fichier comme indiqué dans la définition de *n* octets sur *x*. Le fichier est envoyé à *user2*.
AFT downloaded	CIVCC1013I	*user1* downloaded *n* out of *x* bytes of *f* with package subject *p* to *user2*	*user1* a utilisé Advanced File Transfer pour téléchargé une partie du fichier identifié dans la définition de *n* sur *x* octets. Le fichier est envoyé à *user2*.
File upload exceeded limit	CIVCC1014W	Upload failed because *file1* with package subject exceeds required limit	Le fichier envoyé par l'utilisateur dépasse la taille limite de fichier et n'est pas transféré.
File transfer started	CIVCC1015I	Transfer file *f* with package subject *p* started	Le transfert du fichier *f* a commencé.
File transfer ended	CIVCC1016I	Transfer file *f* with package subject *p* ended	Le transfert du fichier *f* est terminé.
Transfer package started	CIVCC1017I	Transfer package with subject *p* started	Le transfert avec l'objet de package *p* a commencé.
Transfer package ended	CIVCC1018I	Transfer package with subject *p* ended	Le transfert avec l'objet de package *p* est terminé.

Événement	Code d'événement	Message	Description
Package summary	CIVCC1019I	Summary for package with subject *p*	Récapitulatif de l'objet de package *p*.
Delete recipient	CIVCC1020I	*user* deleted recipient *user* of file *f* with package subject *p*	Un utilisateur a supprimé un destinataire du fichier *f* avec l'objet de package *p*.
File expiration updated	CIVCC1021I	*user* updated expiration date of a file with package subject *p*	Un utilisateur a mis à jour la date d'expiration d'un fichier dans un package
DLP detected	CIVCC1022E	*f* with package subject *p* from *user* contains sensitive information (DLP) and will not be transferred	Le fichier *f* de l'objet de package *p* provenant de l'utilisateur contient des informations sensibles et le package ne sera pas transféré dans son intégralité. Supprimez les informations sensibles et soumettez de nouveau le package.
DLP scanned	CIVCC1023I	*f* with package subject *p* from *user* was successfully scanned for sensitive information (DLP)	Le fichier *f* de l'objet de package *p* provenant de l'utilisateur a correctement été analysé pour les informations sensibles et le transfert s'effectue.
Appliance Powered Down	CIVCF1001I	*admin* powered down the server	Un administrateur est en train de fermer le serveur.
Appliance Restarted	CIVCF1002I	*admin* restarting the appliance	Un administrateur redémarre le serveur.
Appliance Powering Down	CIVCF1003I	The server is powering down.	Le dispositif est arrêté.
Appliance Started	CIVCF1004I	The server has been started	Un administrateur a démarré le dispositif.
NFS Configured	CIVCF1005I	Application is configured to use NFS with *nfs configuration*	L'application utilise NFS.
Database Configured	CIVCF1006I	Application is configured to use external database with *db configuration*	L'application utilise la base de données externe.
LDAP Configured	CIVCF1007I	Application is configured to use external directory with *LDAP configuration*	L'application utilise LDAP.
Archive Configured	CIVCF1008I	Application has been configured to use archiving *FileNet*	L'application utilise *FileNet* pour archiver les fichiers.
SMTP Configured	CIVCF1009I	Application is configured to use the SMTP server with *SMTP server*	L'application utilise un serveur SMTP *SMTP server*.
Backup SMTP configured	CIVCF1010I	Application has been configured to use backup SMTP server - *SMTP server*	L'application utilise un serveur SMTP de sauvegarde - *SMTP server*.
IP Configured	CIVCF1011I	Application is configured to use IP address with *ip address*	L'application utilise une adresse IP.
Gateway Configured	CIVCF1012I	Application is configured to use Gateway server with *gateway configuration*	L'application utilise un serveur de passerelle.
Mask Configured	CIVCF1013I	Application has been configured to use subnet mask with *CIDR mask configuration*	L'application utilise un masque de sous-réseau.

Événement	Code d'événement	Message	Description
Fix applied	CIVCF1014I	Fix pack applied to the application *fix pack*	Le groupe de correctifs *fix pack* est appliqué à l'application.
Task policy configured	CIVCF1015I	Application has been configured to use task *task* with initial state *state* and repeat interval *interval*	L'application est configurée pour exécuter la tâche de maintenance *task* au statut initial *state* selon l'intervalle *interval*.
Antivirus configured	CIVCF1016I	Application has been configured to use *provider name* for antivirus.	L'application est configurée pour utiliser le fournisseur ICAP nommé *provider name* pour l'analyse antivirus.
ICAP server enabled	CIVCF1017I	*admin* successfully enabled ICAP server *server name*	Un administrateur a activé un serveur ICAP nommé *server name*.
ICAP server disabled	CIVCF1018I	*admin* successfully disabled ICAP server *server name*	Un administrateur a désactiver un serveur ICAP nommé *server name*.
DNS server enabled	CIVCF1019I	Application has been configured to use DNS server *server name*	Un administrateur a activé un serveur DNS nommé *server name*.
ICAP server deleted	CIVCF1020I	*admin* deleted ICAP server *server name*	Un administrateur a supprimé un serveur ICAP nommé *server name*. L'analyse par ce serveur est désactivée.
DNS server deleted	CIVCF1021I	*admin* deleted DNS server *server name*	Un administrateur a supprimé un serveur DNS nommé *server name*. La gestion des connexions par ce serveur est désactivée.
NFS Connection Failed	CIVCF1020E	NFS with *nfs configuration* failed to connect	NFS n'a pas réussi à se connecter au serveur.
Database Connection Failed	CIVCF1021E	External database with *db configuration* failed to connect	La base de données externe n'a pas réussi à se connecter au serveur.
LDAP Connection Failed	CIVCF1022E	LDAP with *ldap configuration* failed to connect	LDAP n'a pas réussi à se connecter au serveur.
Archive Connection Failed	CIVCF1023E	Archive with *archive configuration* failed to connect	L'outil d'archivage n'a pas réussi à se connecter au serveur.
DNS Connection Failed	CIVCF1024E	The Gateway server using the *gateway configuration* failed to connect	Le serveur de passerelle n'a pas réussi à se connecter.
SMTP Failed	CIVCF1025E	SMTP server connection failed.	La connexion au serveur SMTP a échoué.
Fix Pack Failed	CIVCF1026E	Fix pack updates with *update info* failed	Le groupe de correctifs ne s'est pas installé correctement.
No SMTP Server	CIVCF1027E	No SMTP server configured	Aucun serveur SMTP n'est configuré.
SMTP Server Failed	CIVCF1028E	Failed to connect to the SMTP server	L'application n'a pas réussi à se connecter au serveur SMTP.
Out of Disk Space	CIVCF1029E	Appliance ran out of disk space	Le dispositif manque d'espace disque et par conséquent les modules ne peuvent plus être téléchargés.
System policy update	CIVCF1029I	*admin* successfully updated policy *policy*	Un administrateur a mis à jour une règle système.

Événement	Code d'événement	Message	Description
System policy enabled	CIVCF1030I	*admin* successfully enabled system policy *policy*	Une règle système pour *policy* a été activée avec succès par un utilisateur. Les valeurs suivantes pour *policy* sont possibles : • Règles sur l'analyse antivirus • Règles sur la prévention des pertes de données • Règles sur la notification par e-mail • Règles sur la conservation d'événement • Règles sur la notification d'expiration • Règles sur les mots de passe • Règles sur la réinitialisation des mots de passe • Règles sur l'expiration du compte utilisateur
System policy disabled	CIVCF1031I	*admin* successfully disabled system policy *policy*	Une règle système pour *policy* a été désactivée par un administrateur.
Temp suspend task	CIVSC1001I	Application has temporarily suspended task name *task*	L'application a interrompu temporairement la tâche nommée *task*.
Temp resume task	CIVSC1002I	Application has temporarily resumed task name *task*	L'application a relancé la tâche nommée *task* qui avait été interrompue.
Run now task	CIVSC1003I	*admin* has requested the immediate execution of task name *task*	Un administrateur a demandé l'exécution immédiate de la tâche nommée *task*.
Internal email domains added		*admin* added internal email domain *domain name*	Un administrateur a ajouté un domaine de messagerie électronique interne nommé *domain name*.
Internal email domains deleted		*admin* deleted internal email domain *domain name*	Un administrateur a supprimé un domaine de messagerie électronique interne nommé *domain name*.
SSL Expired	CIVSE1001I	SSL certificate *alias* expired	Le certificat SSL a expiré. Demandez-en un nouveau à votre autorité de certification.
SSL Imported	CIVSE1002I	SSL certificate *alias* imported by *admin*	Un administrateur a importé un certificat SSL.
SSL Exported	CIVSE1003I	SSL certificate *alias* exported by *admin*	Un administrateur a exporté un certificat SSL.
SSL Enabled	CIVSE1004I	SSL enabled	Un administrateur a activé le protocole SSL.
SSL Disabled	CIVSE1005I	SSL disabled	Un administrateur a désactivé le protocole SSL.
SSL certificates added		*admin* added SSL certificate *cert name*	Un administrateur a ajouté un certificat SSL nommé *cert name*.
SSL certificates deleted		*admin* deleted SSL certificate *cert name*	Un administrateur a supprimé un certificat SSL nommé *cert name*.
User expirations updated	CIVSE1006I	*user* expirations updated	La date d'expiration du compte utilisateur a été modifiée.
User expirations notified	CIVSE1007I	*user* notified of upcoming account expiration	L'utilisateur reçoit une notification indiquant que son compte arrive bientôt à expiration.

Événement	Code d'événement	Message	Description
User expirations processed	CIVSE1008I	*user* accounts expired	Le compte utilisateur a expiré.
Email failed	CIVMS0001E	Email notification for *user* could not be delivered	Un e-mail de notification n'a pas pu être envoyé à l'utilisateur.

Génération d'un journal de support

Si le support vous demande de générer un journal de support, utilisez QuickFile pour le générer.

Pourquoi et quand exécuter cette tâche

Lors de l'identification et de la résolution d'un problème lié à QuickFile, le support peut vous demander d'activer le journal de support. QuickFile simplifie cette tâche grâce aux rapports de journalisation (Log Reports).

L'un des onglets Log Reports vous permet d'activer le journal de support. À l'aide du journal de support, vous pouvez générer les informations de journalisation et exporter les informations sur un fichier que le support pourra utiliser. À cause de l'impact temporaire que cette journalisation a sur les performances du système, activez la journalisation seulement si le support vous y invite.

Pour activer la journalisation, complétez la procédure suivante :

Procédure

1. Cliquez sur **Rapports de journalisation** à partir du menu.
2. Cliquez sur l'onglet **Rapports de journalisation**.
3. Sélectionnez **Activer la journalisation de support**.
4. Sélectionnez un des journaux d'application suivants pour afficher :
   - Serveur d'application
   - Base de données
   - Messagerie
   - Systèmes d'exploitation
5. Si vous sélectionnez **Serveur d'application** en tant que journal à afficher, entrez les informations exactes relatives au journal comme indiqué par le support.
6. Si vous sélectionnez **Base de données**, fournissez les informations dans les zones suivantes :
   - **Niveau de gravité du journal**
   - **Plan de requête du journal** - True ou False
   - **Texte d'instruction du journal** - True ou False
   - **Trace des interblocages** - True ou False
7. Si vous sélectionnez **Messagerie** comme type de journal, sélectionnez une ou plusieurs des zones suivantes pour définir les niveaux de journalisation à afficher :
   - **traçage**
   - **cluster**

- **defs**
- **noyau**
- **dap**
- **rubrique**
- **programme de consignation**

8. Si vous sélectionnez **Système d'exploitation**, sélectionnez un des niveaux d'erreur suivants pour consigner :
   - **Débogage**
   - **Informations**
   - **Avert**
   - **Erreur**
   - **Message**
   - **Erreur bloquante**
9. Une fois la journalisation activée, vous devez provoquer de nouveau les événements pour qu'ils apparaissent dans le journal. Sous les instructions du support, créez à nouveau le problème d'origine. Après avoir recréé le problème, retournez sur la page **Rapports de journalisation** .
10. Exportez le journal des événements dans un fichier en procédant comme suit :
    - Sélectionnez les fichiers de vidage à exporter, activez les fichiers de **vidage Java** ou de **cliché de pile**, ou les deux.
    - Cliquez sur **Exporter**. Un fichier est téléchargé sur votre ordinateur.
    - Ouvrez ou enregistrez le fichier, le cas échéant.
11. Cliquez sur **Enregistrer**.
12. Envoyez les fichiers journaux au support pour analyse.

Que faire ensuite

Une fois le problème résolu, retournez sur la page **Rapports de journalisation** pour désactiver la journalisation du support. Sinon, cela peut nuire aux performances du système.

Affichage des événements qui ne sont pas dans le journal

Vous pouvez utiliser le journal d'événement pour générer une liste des tâches qui ont lieu fréquemment. Cependant, tous les événements et toutes les erreurs ne sont pas disponibles dans le journal. Regroupez et téléchargez tous les journaux système pour obtenir tous les événements.

Avant de commencer

Complétez les étapes suivantes pour regrouper et télécharger tous les journaux système :

Procédure

1. Entrez l'url suivante dans votre navigateur : `http://`*`ip address`*`:9080/quickfile/rest/admin/mustgather`
2. Entrez votre ID et votre mot de passe administrateur.
3. Enregistrez le fichier appelé `quickfileMustGather.tgz`.
4. Extrayez le fichier pour afficher tous les journaux de QuickFile.

Chapitre 13. Identification et résolution des problèmes

Lorsqu'un transfert de fichiers échoue, suivez des procédures vous permettant d'identifier la source du problème et de le résoudre.

Pourquoi et quand exécuter cette tâche

Pour identifier et résoudre les problèmes liés à QuickFile, procédez comme suit :

Procédure

1. Identifiez les types de transferts dont le statut est à l'échec.
2. Consultez les journaux pour déterminer les caractéristiques communes aux transferts ayant échoué.
3. Suivez la procédure de correction permettant résoudre l'échec des transferts.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : LE PRÉSENT DOCUMENT EST LIVRÉ "EN L'ÉTAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DÉCLINE NOTAMMENT TOUTE RESPONSABILITÉ RELATIVE À CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DÉFAUT D'APTITUDE À L'EXÉCUTION D'UN TRAVAIL DONNÉ. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci) et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Les résultats peuvent donc varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. IBM ne peut donc pas garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les programmes exemples sont fournis "en l'état", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation de ces programmes exemples.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© IBM 2013. Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. 2013.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web “Copyright and trademark information” à l'adresse http://www.ibm.com/legal/copytrade.shtml.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux États-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux États-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux États-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis et/ou dans certains autres pays.

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

UNIX est une marque enregistrée de The Open Group aux États-Unis et/ou dans certains autres pays.

Java™ ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc. aux États-Unis et/ou dans certains autres pays et est utilisée sous licence.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logo Ultrium sont des marques de HP, IBM Corp. et Quantum aux États-Unis et/ou dans certains autres pays.

Connect Control Center, Connect:Direct, Connect:Enterprise, Gentran, Gentran:Basic, Gentran:Control, Gentran:Director, Gentran:Plus, Gentran:Realtime, Gentran:Server, Gentran:Viewpoint, Sterling Commerce, Sterling Information Broker et Sterling Integrator sont des marques de Sterling Commerce, Inc., une filiale d'IBM Company.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Index

J

L

M

N

O

P

Q

R

S

T

U

V

Z

Numéro de programme : 5725-F81

Imprimé en France