



Linux 64-bit: RedHat 6 & 7, CentOS 6 & 7, SLES 11, Ubuntu 12-14, Debian 6 & 7

Revision: 149670 Generated: 10/24/2017 12:54

Sommaire

Introduction.....	3
Configuration système requise.....	4
Paramétrage de Connect.....	5
Partie 1 : Installation.....	5
Partie 2 : Environnement réseau.....	6
Partie 3 : Configuration de base.....	10
Partie 4 : Configuration de la sécurité.....	13
Fonctionnalité Connect.....	21
Lancement d'un transfert de fichier.....	21
Le Gestionnaire des transferts.....	22
Contrôle des transferts.....	23
Déchiffrement des fichiers chiffrés.....	23
Désinstallation.....	28
Appendice.....	29
Fichiers journaux.....	29
Dépannage.....	30
SELinux empêche l'accès au plug-in Connect.....	30
Problèmes de connectivité.....	30
Support technique.....	32
Commentaires.....	33
Mentions légales.....	34

Introduction

Présentation du plug-in de navigateur Web installé à la demande Aspera Connect

Aspera Connect est un plug-in de navigateur Web installé à la demande qui permet des chargements et téléchargements en vitesse accélérée avec un serveur Aspera. Compatible avec la plupart des navigateurs standard quel que soit votre système d'exploitation, Aspera Connect intègre toute la haute technologie Aspera en matière de transport dans un petit package, facile à utiliser, offrant un contrôle inégalé sur les paramètres de transfert. Aspera Connect comprend les fonctionnalités suivantes :

Fonctionnalité	Description
Transport de fichier <i>fasp</i>	Haute technologie en matière de transport.
Plug-in de navigateur	Les chargements et les téléchargements sont lancés par un navigateur Web en toute transparence.
Types de transfert flexibles	Transférer facilement de simples fichiers, plusieurs dossiers ou des répertoires entiers.
Reprise des transferts	Retente et reprend automatiquement les transferts partiellement exécutés ou ayant échoué.
Transfert indépendant du navigateur	Le navigateur Web peut être fermé pendant l'opération de transfert.
Moniteur des transferts	Moniteur des transferts intégré pour la visualisation, le contrôle de la vitesse et le suivi.
Traitement de secours HTTP	Mode de traitement de secours HTTP pour les environnements réseau très restrictifs.
Prise en charge de proxy	Saisie des paramètres du traitement de secours HTTP et du proxy <i>fasp</i> .
Protection du contenu	Les fichiers protégés par un mot de passe qui sont transférés et stockés sur le serveur distant.
Mise en file d'attente	Autoriser un nombre fixe de transferts simultanés et mettre le reste en file d'attente.

Configuration système requise

Configuration système requise pour l'installation/l'utilisation de Connect.

Les configurations suivantes sont applicables lors de l'installation et de l'exécution de l'application Connect :

- (*GLIB 2.9 et versions supérieures*) Debian 6 & 7, RHEL/Centos 6 & 7, SLES 11, Ubuntu 12-14, ou Ubuntu 12-14.
- Firefox 27+

Paramétrage de Connect

Installez Aspera Connect et configurez votre ordinateur pour les transferts de fichiers *fasp*.

Partie 1 : Installation

Instructions pour l'installation de Aspera Connect sur votre système.

Cette rubrique explique le processus d'installation de Aspera Connect sur votre système. Connect peut être installé sur votre système via le programme d'installation Web ou un package téléchargeable. Veuillez vous référer aux sections correspondantes ci-dessous.



Avertissement :

Avant d'installer Connect, assurez-vous que vous exécutez Debian 6.0+, RHEL/Centos 6.0+ ou Ubuntu 8.04+. Connect 3.X prend en charge GLib 2.9 et versions supérieures.



Important :

Pour que Connect fonctionne correctement, vous devez activer les *cookies* dans votre navigateur. Veuillez vous référer à l'aide de votre navigateur pour obtenir des instructions sur la vérification de ce paramètre.

Programme d'installation Web de Aspera Connect

Utilisez votre navigateur pour accéder à votre application Web Aspera (c'est-à-dire Faspex Server, Connect Server ou Shares). Une fois que vous avez atteint la page Web du serveur, vous visualisez le bouton **Installer maintenant** (ou le bouton **Mettre à jour maintenant** si une ancienne version de Connect est installée sur votre système). En fonction de votre système d'exploitation et de votre navigateur, cliquer sur ce bouton lancera l'installation automatique ou vous redirigera vers la page de téléchargement de Aspera Connect (pour une *installation manuelle*). Suivez les instructions affichées à l'écran pour terminer le processus d'installation. Si votre navigateur affiche une invite ou un avertissement de sécurité, cliquez sur **Autoriser** ou **Continuer** pour poursuivre le processus.

Programme d'installation de bureau d'Aspera

Vous pouvez télécharger le package Aspera Connect directement depuis http://www.asperasoft.com/download_connect/. Une fois téléchargé, fermez votre navigateur Web et exécutez les commandes suivantes dans le répertoire du programme d'installation (remplacez le numéro de version en conséquence) :

```
# tar -zxvf aspera-connect-<version>.tar.gz
# sh aspera-connect-<version>.sh
```

Post-installation

Une fois l'installation de Aspera Connect terminée, l'application s'exécute automatiquement lors de la connexion à la page Web du serveur Connect, Faspex ou Shares. Cherchez l'icône Connect dans votre barre d'état système pour confirmer qu'elle est en cours d'exécution.



Si Connect ne s'est pas lancé automatiquement (ou si vous avez besoin de le redémarrer), vous pouvez exécuter l'application manuellement avec la commande suivante :

```
# ~/.aspera/connect/bin/asperaconnect
```

Partie 2 : Environnement réseau

Configurez si nécessaire des proxy réseau ou remplacez les vitesses du réseau via le GUI Aspera Connect.

Si vous devez configurer un proxy réseau quel qu'il soit ou remplacer les vitesses du réseau, vous pouvez le faire via l'option **Réseau** de Aspera Connect. Avant de modifier la configuration réseau de Connect, veuillez examiner les conditions requises pour le réseau, énumérées ci-dessous et décrivant les ports dont l'ouverture peut être nécessaire sur votre réseau (par exemple, 22, 33001, etc.).

Conditions requises pour le réseau

Votre connexion SSH peut différer en fonction des paramètres réseau uniques de votre entreprise. Bien que **TCP/22** soit le paramètre par défaut, consultez votre service informatique pour des questions relatives aux ports SSH ouverts pour le transfert de fichier. Veuillez également consulter la documentation d'aide spécifique à votre système d'exploitation pour obtenir des instructions spécifiques sur la configuration de votre pare-feu. Si l'hôte de votre client se trouve derrière un pare-feu qui n'autorise pas les connexions sortantes, vous devez autoriser les éléments suivants :

- Les connexions sortantes pour SSH, qui est paramétré par défaut sur **TCP/22**, bien que le serveur puisse exécuter SSH sur un autre port (veuillez consulter votre service informatique pour des questions relatives aux ports SSH ouverts pour le transfert de fichier).
- Les connexions sortantes pour les transferts *fasp*, dont le paramètre par défaut est **UDP/33001**, bien que le serveur puisse exécuter les transferts *fasp* sur un ou plusieurs autres ports (veuillez consulter votre service informatique pour des questions relatives aux ports ouverts pour les transferts *fasp*).

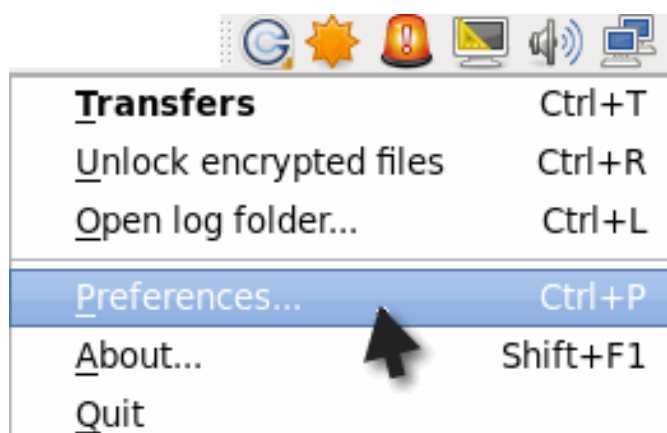
Limiter la vitesse de transfert

Important :

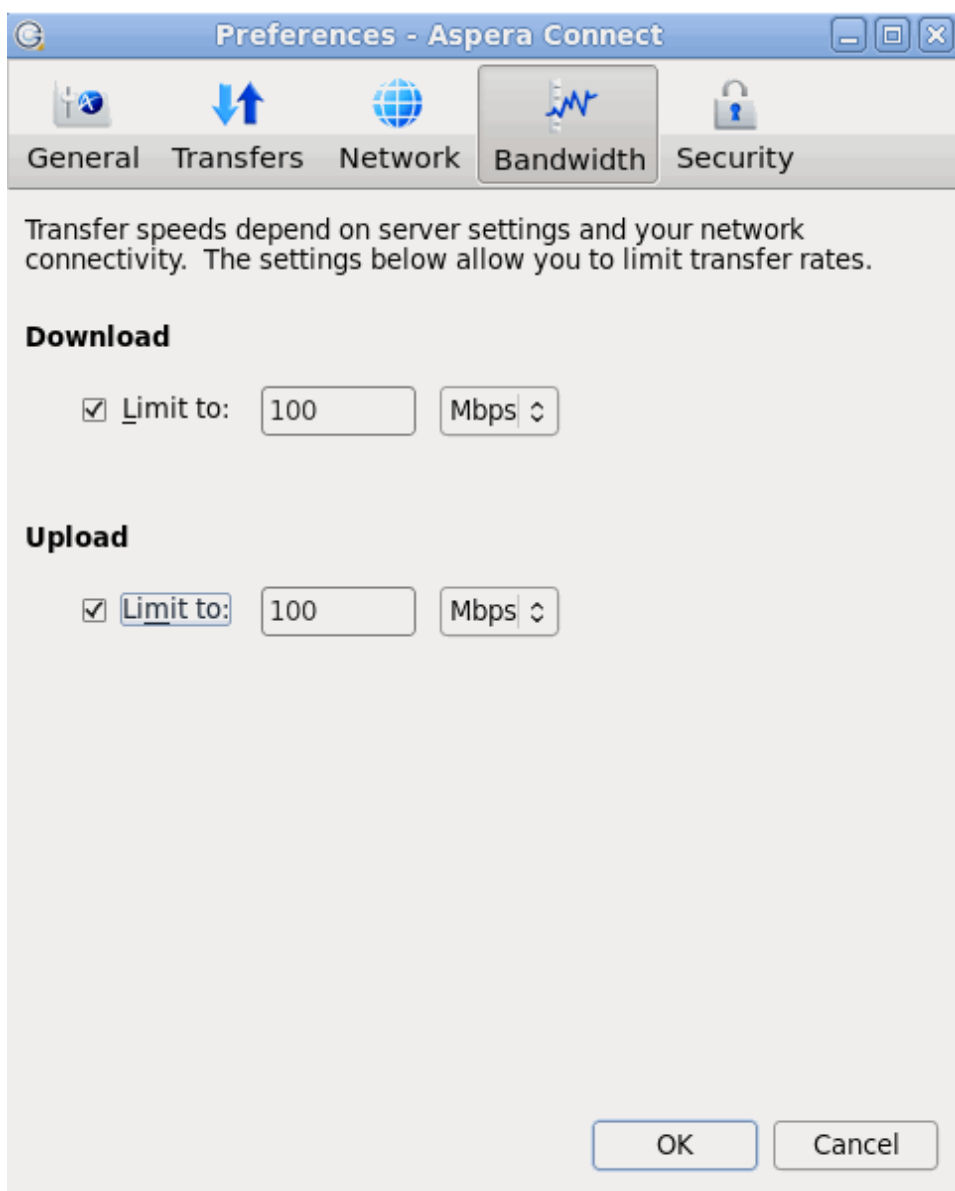
Sauf si vous devez limiter la bande passante utilisée par Aspera Connect, vous n'avez pas à définir de valeurs pour ces champs.

Si Aspera Connect est déjà en cours d'utilisation, allez dans **Barre d'état système > Clic droit sur Aspera Connect > Préférences**. Si elle n'est pas en cours d'utilisation, vous pouvez exécuter l'application manuellement avec la commande suivante :

```
# ~/.aspera/connect/bin/asperaconnect
```



Vous pouvez limiter la vitesse de transfert de Aspera Connect via l'option **Bande passante**.



Vous pouvez limiter la vitesse de transfert de téléchargement et/ou de chargement en cochant les cases concernées et en saisissant une vitesse, soit en Mbps soit en Kbps. Notez que votre capacité à limiter ces vitesses dépend des facteurs suivants :

1. La bande passante de votre réseau : La bande passante disponible sur votre réseau peut limiter la vitesse de transfert, même si vous avez entré des nombres élevés dans ces champs.
2. Vos paramètres de transfert du serveur Aspera : Les paramètres de votre serveur peuvent limiter la vitesse de transfert, même si la bande passante et les nombres entrés sont supérieurs.

Proxy HTTP de traitement de secours

Le proxy HTTP de traitement de secours ne doit être utilisé que pour les transferts de traitement de secours, et **non** pour les transferts *fast*. Pour paramétrer un proxy HTTP de traitement de secours, allez dans Aspera Connect **Préférences > Réseau**.

Preferences - Aspera Connect

General Transfers **Network** Bandwidth Security

Configure how Aspera Connect connects to the Internet.

HTTP Proxy

☒ Use HTT**P** Fallback Proxy

Username: user1

Password: *****

Address: 10.0.0.1 Port: 3866

FASP Proxy

☐ Use FASP Proxy (DNAT)

☐ Secure (DNATS)

Username:

Password:

Address: Port: 0

OK Cancel

Dans la section **Proxy HTTP**, vous pouvez modifier la configuration du proxy pour le serveur gérant le traitement de secours. Le traitement de secours HTTP sert de méthode de transfert secondaire lorsque la connectivité Internet requise pour les transferts accélérés Aspera (c'est-à-dire, le port UDP 33001, par défaut) n'est pas disponible. Si la connectivité UDP est perdue ou ne peut pas être établie, le transfert continuera alors sur le protocole HTTP selon la configuration de ce proxy.

Pour configurer un proxy HTTP de traitement de secours, cochez la case **Utiliser le proxy http de traitement de secours** et saisissez vos paramètres. Ces paramètres incluent les informations d'identification de l'authentification à NTLM (nom d'utilisateur et mot de passe), ainsi que le nom de l'hôte/l'adresse IP et le numéro du port.

HTTP Proxy

☒ Use HHTTP Fallback Proxy

Username:

Password:

Address: Port:

Proxy FASP

Lorsque le proxy *fasp* est activé, Aspera transmet le nom d'utilisateur, l'adresse du serveur et le port DNAT ou DNATS (sécurisé), à **ascp**. Pour paramétrer un proxy *fasp*, allez dans Aspera Connect **Préférences > Réseau**.

Preferences - Aspera Connect

General Transfers **Network** Bandwidth Security

Configure how Aspera Connect connects to the Internet.

HTTP Proxy

☒ Use HHTTP Fallback Proxy

Username:

Password:

Address: Port:

FASP Proxy

☐ Use FASP Proxy (DNAT)

☐ Secure (DNATS)

Username:

Password:

Address: Port:

OK Cancel

Pour configurer un proxy *fasp*, activez les cases à cocher suivantes :

- Utiliser le proxy FASP (DNAT)
- Sécurisé (DNATS)

Après avoir coché les cases, saisissez vos nom d'utilisateur, mot de passe, adresse et numéro de port du serveur proxy.

FASP Proxy

☒ Use FASP Proxy (DNAT)

☒ Secure (DNATS)

Username:

Password:

Address: Port:

Partie 3 : Configuration de base

Modification des paramètres par défaut de Aspera Connect via l'option « Préférences ».

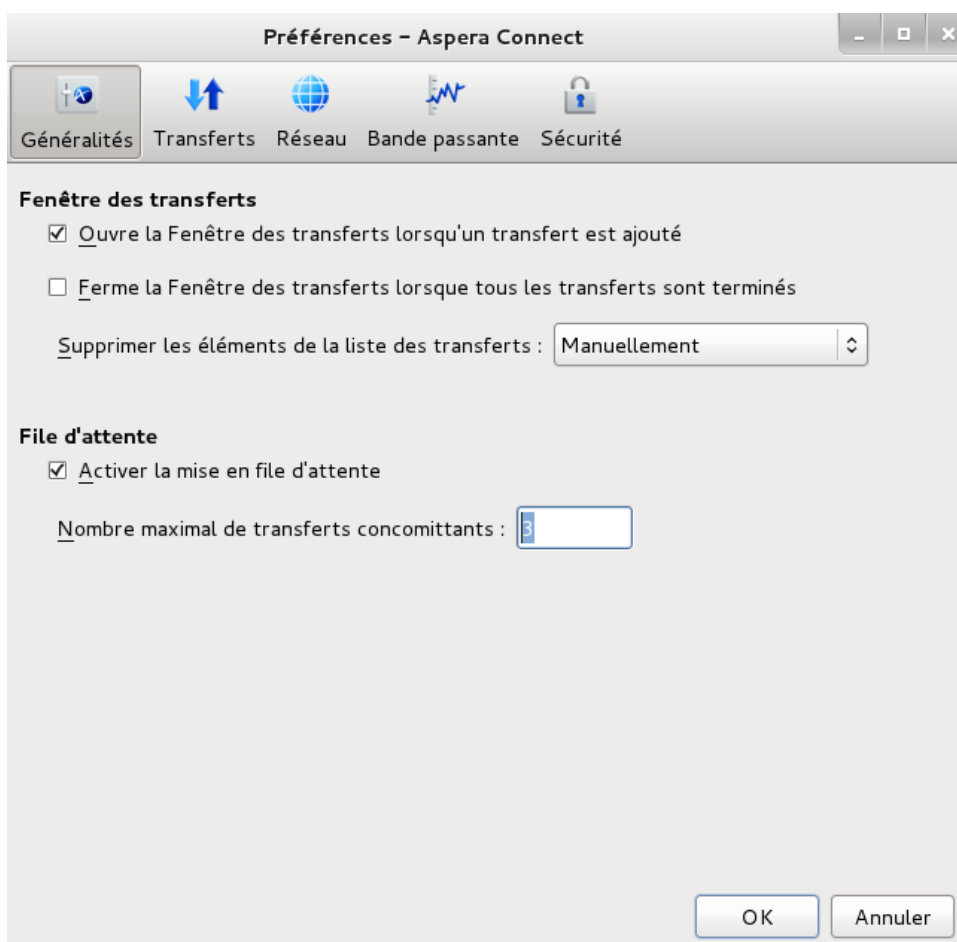
Si Aspera Connect est déjà en cours d'utilisation, allez dans **Barre d'état système > Clic droit sur Aspera Connect > Préférences**. Si elle n'est pas en cours d'utilisation, vous pouvez exécuter l'application manuellement avec la commande suivante :

```
# ~/.aspera/connect/bin/asperaconnect
```

<u>T</u> ransferts	Ctrl+T
<u>D</u> éverrouiller les fichiers chiffrés	Ctrl+R
<u>O</u> uvrir le dossier des journaux	Ctrl+L
<u>P</u> références...	Ctrl+P
<u>À</u> propos de...	Maj+F1
<u>Q</u> uitter	

Préférences générales

Le comportement général de l'application Aspera Connect peut être configuré via l'option **Généralités**.

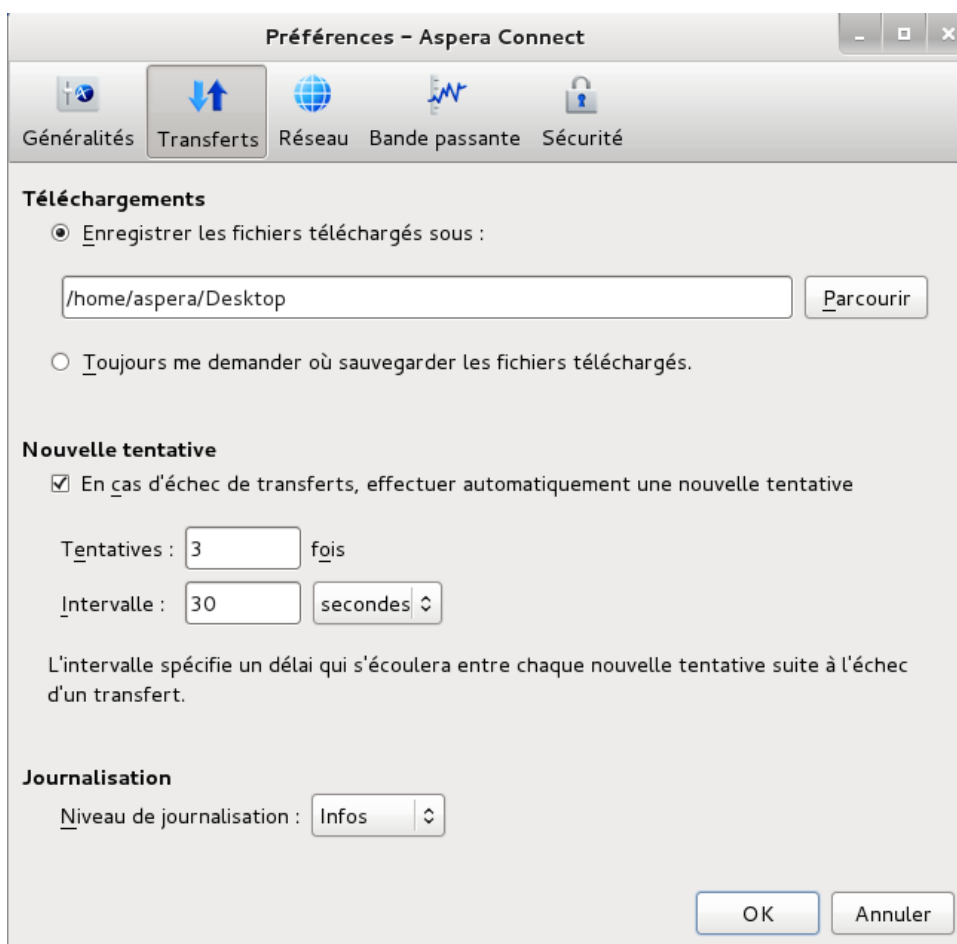


Sous l'option **Généralités**, vous pouvez modifier les paramètres suivants :

- Indiquer le comportement de la fenêtre *Transferts* lorsqu'un transfert commence et se termine (via les cases à cocher).
- Indiquer comment les éléments de la liste de transfert doivent être supprimés de la fenêtre *Transferts* (via la liste déroulante).
- Activer ou désactiver la mise en file d'attente des transferts via la case à cocher (qui autorise un nombre fixe de transferts simultanés et met le reste en file d'attente) et définir le nombre maximum de transferts simultanés via la zone de texte.

Préférences de transfert

Le comportement du transfert Aspera Connect peut être configuré sous l'option de préférence **Transferts**.



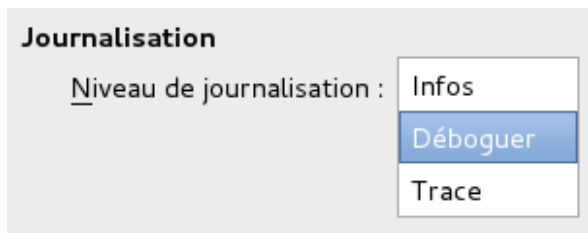
Par défaut, Connect télécharge les fichiers sur le bureau de l'utilisateur en cours. Pour modifier ce paramètre, définissez la règle de téléchargement dans la section *Téléchargements* de la façon suivante :

- **Enregistrer les fichiers téléchargés sous** : Indiquez le chemin d'accès pour enregistrer les fichiers téléchargés.
- **Toujours me demander où sauvegarder les fichiers téléchargés** : Sélectionnez un emplacement ad-hoc pour chaque téléchargement.

Vous pouvez également définir une règle de nouvelle tentative si le transfert échoue. Définissez la règle de nouvelle tentative dans la section *Nouvelle tentative* de la façon suivante :

- **En cas d'échec de transferts, effectuer automatiquement une nouvelle tentative** : Activez ou désactivez.
- **Tentatives** : Indiquez combien de fois Connect devra tenter de recommencer le transfert.
- **Intervalle** : Indiquez le délai qui doit s'écouler entre chaque tentative (en secondes, minutes ou heures).

Enfin, vous pouvez configurer un niveau de journalisation qui peut être utilisé pour contrôler la sortie de journalisation lors de la résolution d'un problème de transfert.



Notez que cette fonctionnalité n'est généralement utilisée que lorsque vous contactez le [support technique Aspera](#). Sélectionnez l'une des options suivantes :

- **Infos** : Affiche des messages généraux concernant les demandes, les options de génération *ascp* et les modifications de statut de transfert.
- **Déboguer** : Les commentaires (c'est-à-dire, les messages de validation de demande et de gestion *fasp*). -D sera également transmis à ascp.
- **Trace** : Commentaires supplémentaires. -DD sera également transmis à ascp.

Partie 4 : Configuration de la sécurité

Configuration des préférences de sécurité de Aspera Connect.

Aspera Connect présente les fonctionnalités suivantes pour la minimisation des risques de sécurité lors du chargement ou du téléchargement de fichiers :

- Vous pouvez ajouter les serveurs Aspera aux **hôtes de confiance** pour éviter les invites de sécurité récurrentes, ou ajouter des serveurs à la liste des **hôtes soumis à restrictions** pour recevoir une demande de confirmation à chaque fois que vous essayez de lancer un transfert avec cet hôte.
- Vous avez la possibilité d'enregistrer vos informations d'identification lorsque vous vous connectez à un serveur, ainsi que de les supprimer de l'onglet **Mots de passe**.
- La **protection du contenu** est une fonctionnalité qui permet le chiffage des fichiers chargés pendant un transfert, dans le but de les protéger lorsqu'ils sont stockés sur un serveur distant. Le téléchargeur définit un mot de passe lors du téléchargement du fichier, et le mot de passe est requis pour déchiffrer le fichier protégé.

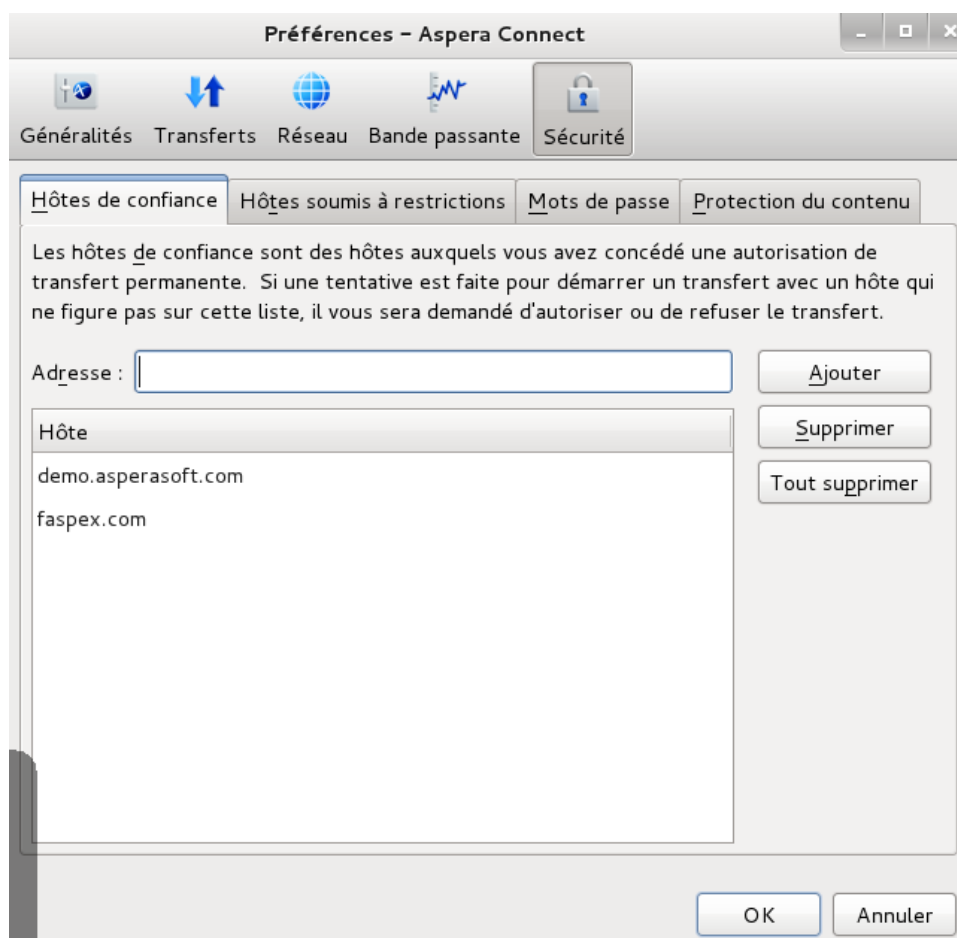
Les paramètres ci-dessus peuvent être configurés dans la boîte de dialogue **Préférences** de Aspera Connect. Si Aspera Connect est déjà en cours d'utilisation, allez dans **Barre d'état système > Clic droit sur Aspera Connect > Préférences**. Si elle n'est pas en cours d'utilisation, vous pouvez exécuter l'application manuellement avec la commande suivante :

```
# ~/.aspera/connect/bin/asperaconnect
```

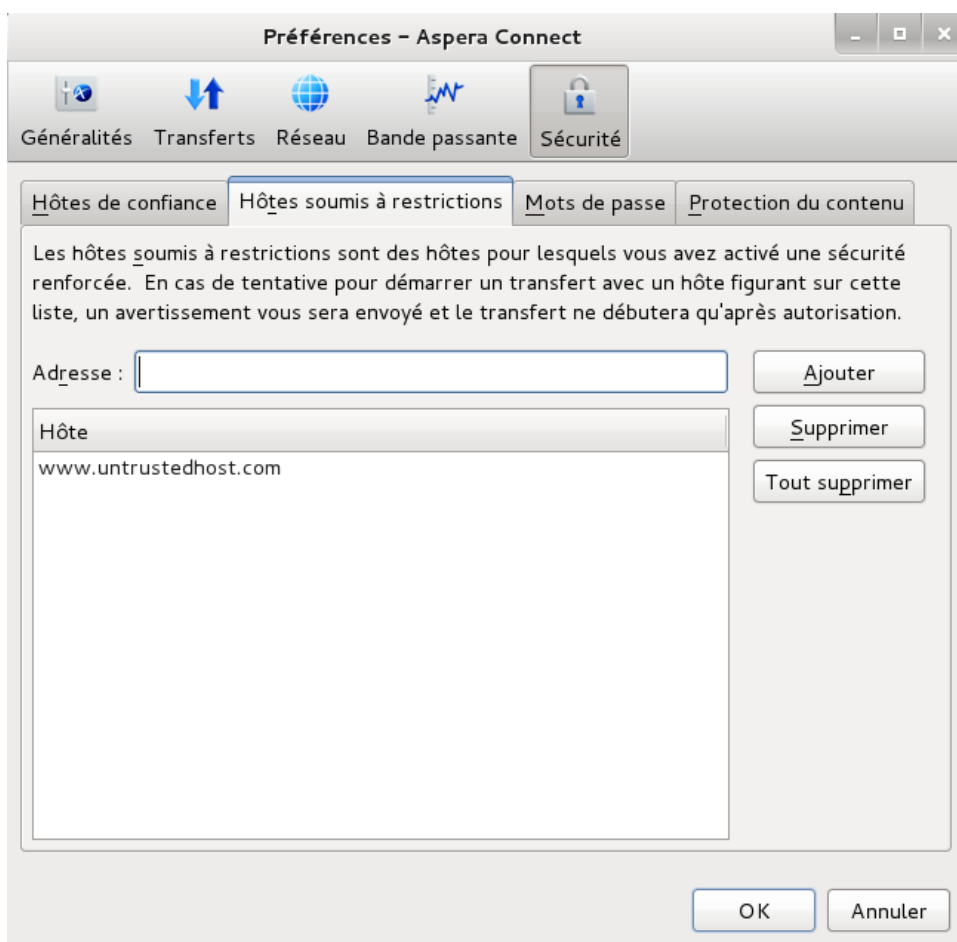
<u>T</u>ransferts	Ctrl+T
<u>D</u>éverrouiller les fichiers chiffrés	Ctrl+R
<u>O</u>uvrir le dossier des journaux	Ctrl+L
<u>P</u>références...	Ctrl+P
<u>À</u> propos de...	Maj+F1
<u>Q</u>uitter	

Gestion des hôtes

Lorsqu'un transfert est lancé et que l'option **Utiliser mon choix pour tous les transferts effectués avec cet hôte** est activée dans la boîte de dialogue de confirmation, le serveur que vous autorisez ou refusez sera ajouté à la liste **Hôtes de confiance** ou **Hôtes soumis à restrictions**, respectivement. Pour afficher, ajouter ou supprimer des hôtes de confiance supplémentaires, allez dans **Sécurité > Hôtes de confiance**. Saisissez l'adresse de l'hôte dans la zone de texte indiquée et cliquez sur **Ajouter**.



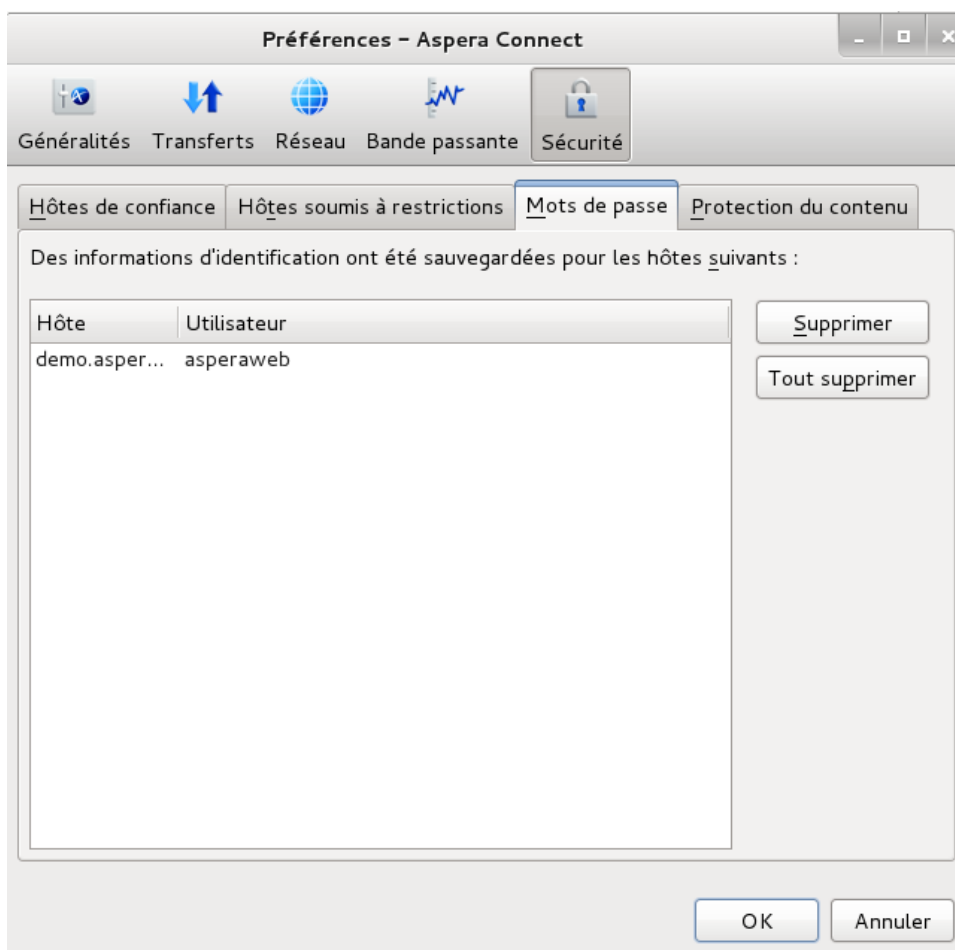
Pour afficher, ajouter ou supprimer des hôtes soumis à restrictions supplémentaires, allez dans **Sécurité > Hôtes soumis à restrictions**. Saisissez ici l'adresse de l'hôte dans la zone de texte indiquée et cliquez sur **Ajouter**.



Important:

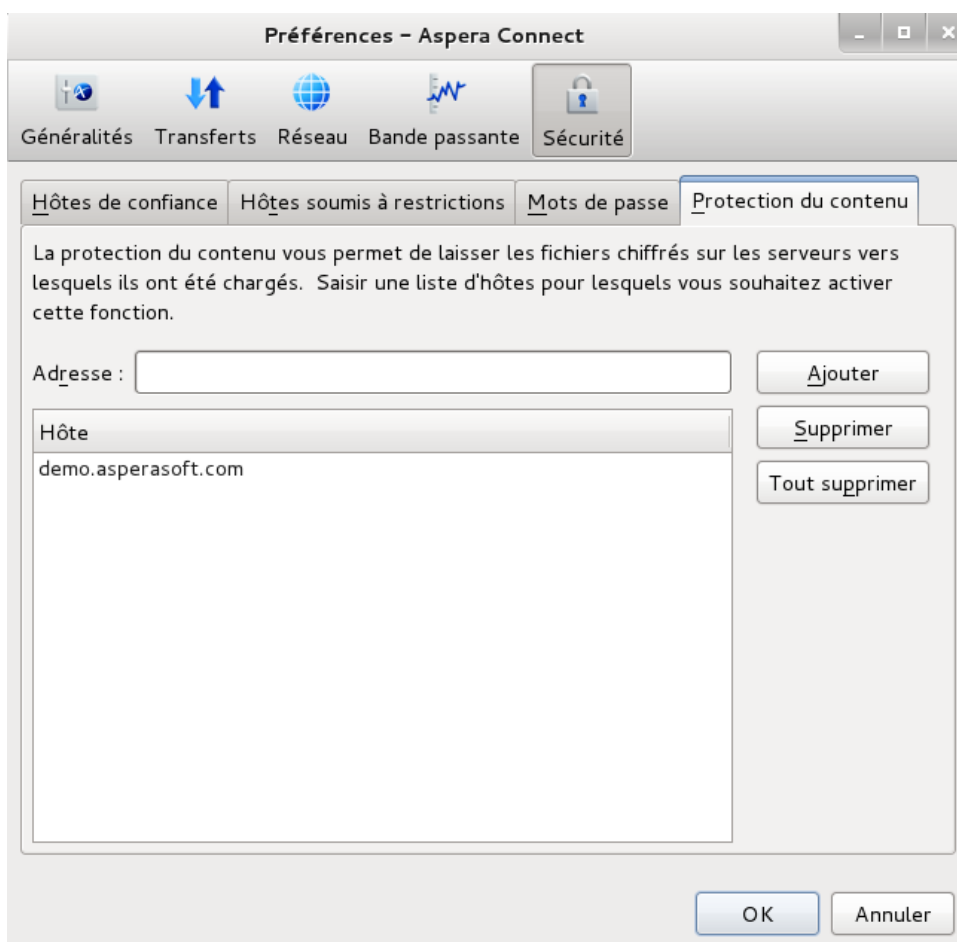
Après avoir ajouté un hôte à la liste des hôtes soumis à restrictions, une confirmation vous sera demandée à chaque fois que vous essaieriez de lancer un transfert avec cet hôte.

Pour afficher, ajouter ou supprimer des informations enregistrées pour un hôte, allez dans **Sécurité > Mots de passe**. Ici, vous pouvez supprimer les informations d'identification enregistrées.

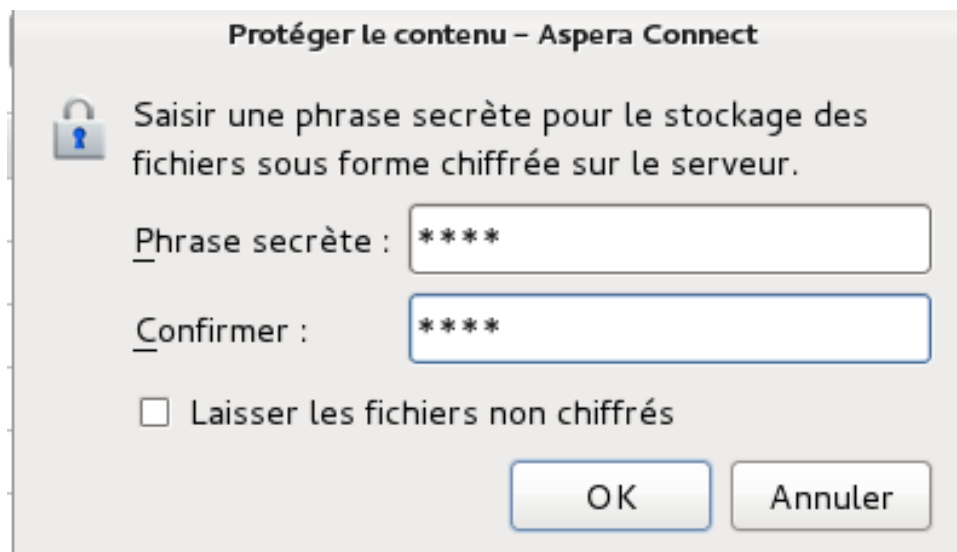


Protection du contenu

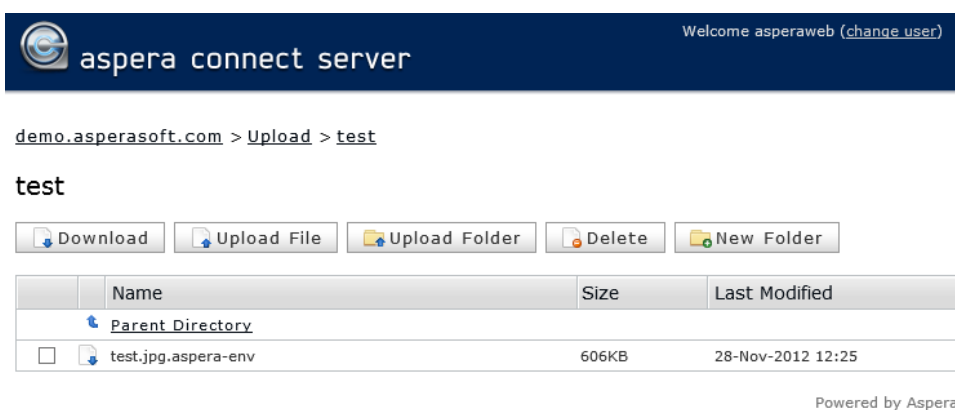
Pour ajouter des hôtes exigeant le chiffrement des fichiers chargés pendant un transfert, cliquez sur l'onglet **Protection du contenu** sous l'option **Sécurité**. Saisissez l'adresse de votre serveur Aspera dans la zone de texte Adresse et cliquez sur **Ajouter**. Le serveur sera ajouté à la liste des hôtes.



Lors du chargement de fichiers sur un serveur configuré comme hôte au contenu protégé, une fenêtre de confirmation apparaît et vous demande une phrase secrète pour chiffrer le fichier. Vous pouvez saisir la phrase secrète dans la zone de texte, ou cocher la case **Laisser les fichiers chargés non chiffrés** (si le serveur le permet) pour continuer sans utiliser cette fonctionnalité. Cliquez sur **OK** pour commencer le transfert.

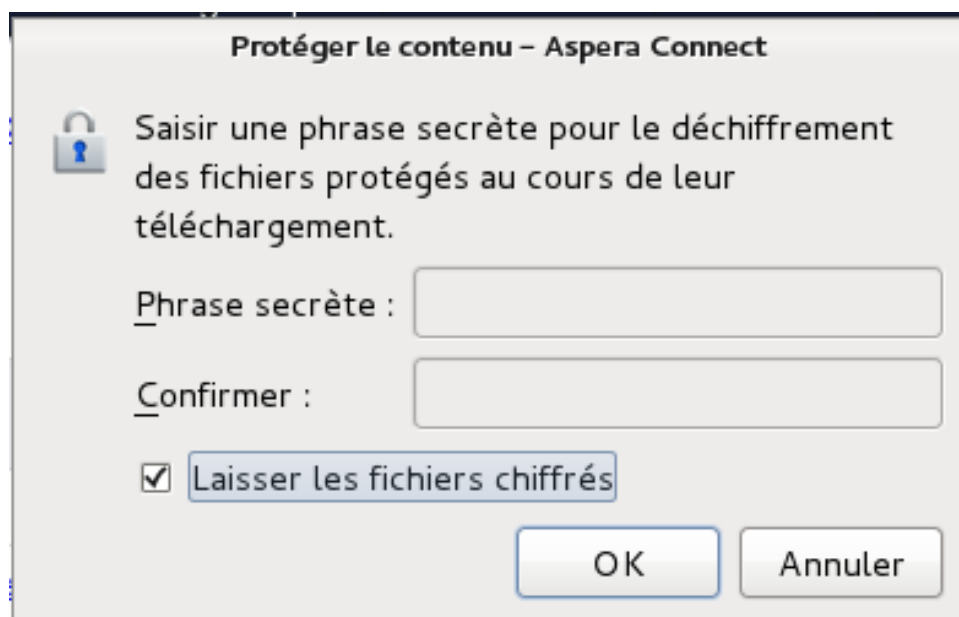


Une fois que les fichiers au contenu protégé ont été chargés sur votre serveur, ils apparaissent avec le suffixe *aspera-env* (Enveloppe de sécurité Aspera).

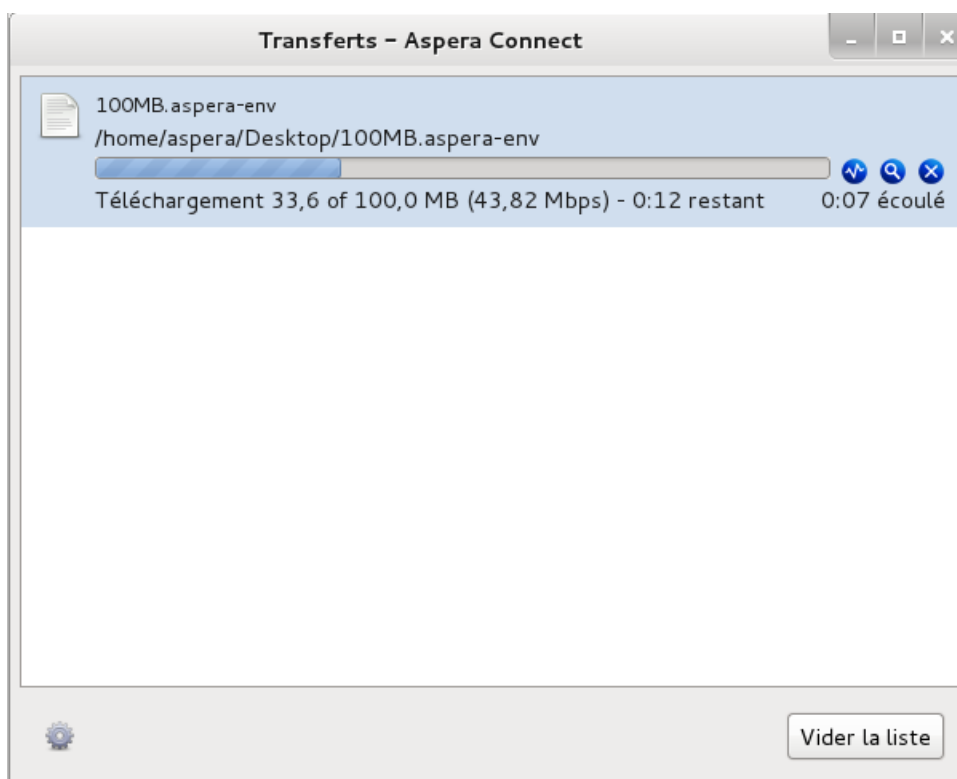


Lors de l'utilisation de Aspera Connect pour télécharger un fichier au contenu protégé, vous avez deux options de déchiffrement.

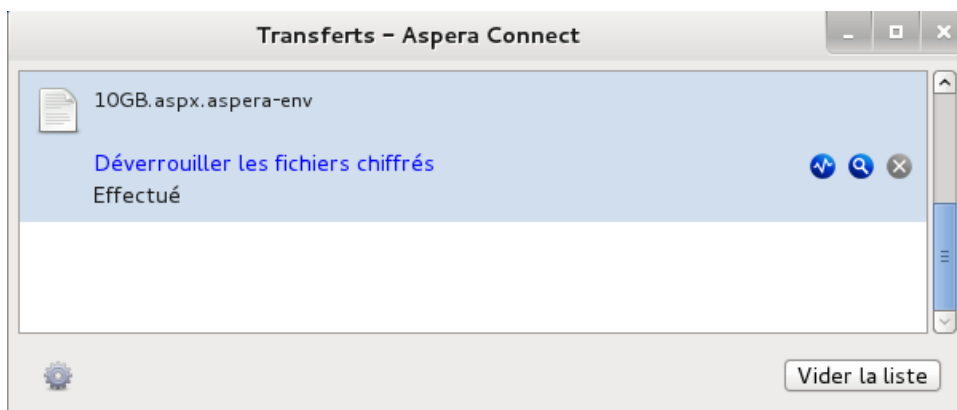
1. Vous pouvez saisir et confirmer votre phrase secrète pour déchiffrer les fichiers *pendant* le téléchargement.
2. **OU**, vous pouvez activer la case **Laisser les fichiers téléchargés chiffrés** pour télécharger les fichiers au contenu protégé, et les déchiffrer *après* le téléchargement. Lorsque vous sélectionnez cette option, vous n'avez pas besoin de saisir votre phrase secrète dans la boîte de dialogue ; cependant, vous aurez des étapes supplémentaires à effectuer pour déchiffrer les fichiers sur votre ordinateur local. Pour plus d'informations, consultez la rubrique « [Déchiffrement](#) ».



Lorsque le fichier au contenu protégé est téléchargé sur votre ordinateur, le suffixe du fichier *aspera-env* est affiché dans la fenêtre **Transferts** de Aspera Connect.



Une fois que le téléchargement est terminé, vérifiez votre fenêtre **Transferts** Aspera Connect. Si vous avez saisi votre phrase secrète pour déchiffrer les fichiers *pendant* le téléchargement (*Option 1*, ci-dessus), vous serez en mesure d'ouvrir immédiatement les fichiers déverrouillés. Si vous choisissez de télécharger les fichiers au contenu protégé et de les déchiffrer *après* le téléchargement, vous recevrez un message d'état vous indiquant de **Déverrouiller les fichiers chiffrés**, ainsi qu'un lien vers l'utilitaire de déchiffrement Aspera.



Notez que vous pouvez également déverrouiller les fichiers chiffrés depuis le menu application de Aspera Connect (sélectionnez l'option **Déverrouiller les fichiers chiffrés** présentée ci-dessous).

<u>T</u>ransferts	Ctrl+T
<u>D</u> éverrouiller les fichiers chiffrés	Ctrl+R
<u>O</u> uvrir le dossier des journaux	Ctrl+L
<u>P</u> références...	Ctrl+P
<u>À</u> propos de...	Maj+F1
<u>Q</u> uitter	

Pour obtenir des instructions sur l'utilisation de l'utilitaire de déchiffrement, veuillez consulter la rubrique « [Déchiffrement](#) ».

Fonctionnalité Connect

Transférez des fichiers en utilisant Aspera Connect.

Lancement d'un transfert de fichier

Test et lancement de transferts de fichiers avec Aspera Connect.

Les étapes suivantes décrivent (1) comment effectuer un test de téléchargement à l'aide du serveur de test de Aspera et (2) comment lancer un transfert de fichier courant à l'aide de Aspera Connect.

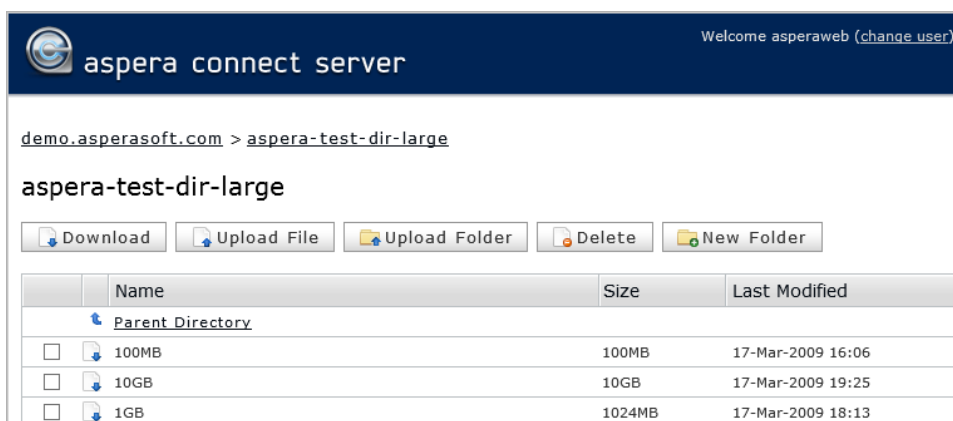
1. Ouvrez votre navigateur Web et connectez-vous au serveur de test de Aspera à l'adresse <http://demo.asperasoft.com/aspera/user>.

Lorsqu'elles vous sont demandées, saisissez les informations d'identification suivantes :

- **Utilisateur** : asperaweb
- **Mot de passe** : demoaspera

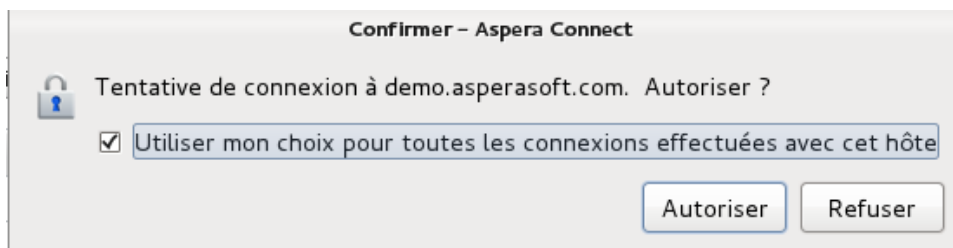
2. Sur la page Web du serveur Aspera Connect, accédez au dossier */aspera-test-dir-large*

Cliquez sur une icône pour télécharger le fichier ou le dossier correspondant. Vous pouvez aussi cocher plusieurs cases et cliquer sur **Télécharger** pour télécharger plus d'un fichier ou dossier à la fois.



3. Confirmez le transfert.

Cliquez sur **Autoriser** pour commencer. Activez la case **Utiliser mon choix pour toutes les connexions effectuées avec cet hôte** pour ne plus visualiser cette boîte de dialogue à l'avenir.



Une fois que vous avez confirmé que les paramètres de configuration sont exacts et que Aspera Connect fonctionne correctement, vous pouvez commencer les transferts avec le serveur Aspera de votre organisation. Il vous suffit de vous rendre sur l'adresse de votre serveur (par exemple, <http://nomentreprise.com/aspera/utilisateur>) pour commencer.

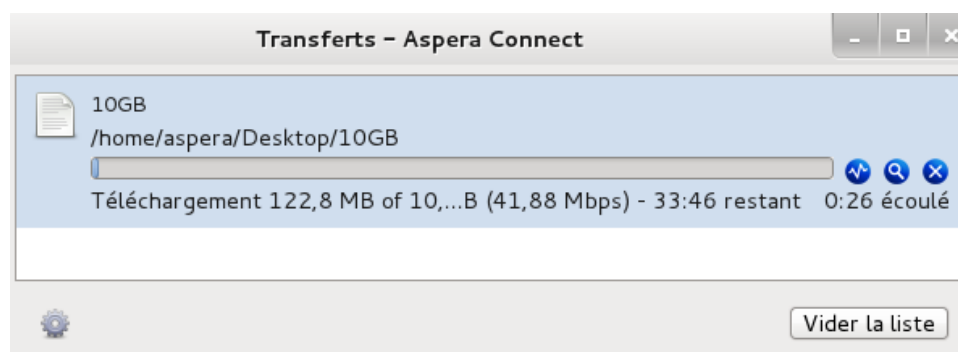
Notez que lors du téléchargement, il est conseillé **d'éviter de transférer des fichiers contenant les caractères suivants** dans leur nom de fichier :

Caractères à éviter : / \ " : ' ? > < & * |






Le Gestionnaire des transferts

Un aperçu détaillé du « Gestionnaire des transferts » de Aspera Connect.


Vous pouvez afficher et gérer toutes les sessions de transfert dans la fenêtre **Transferts** de Aspera Connect.

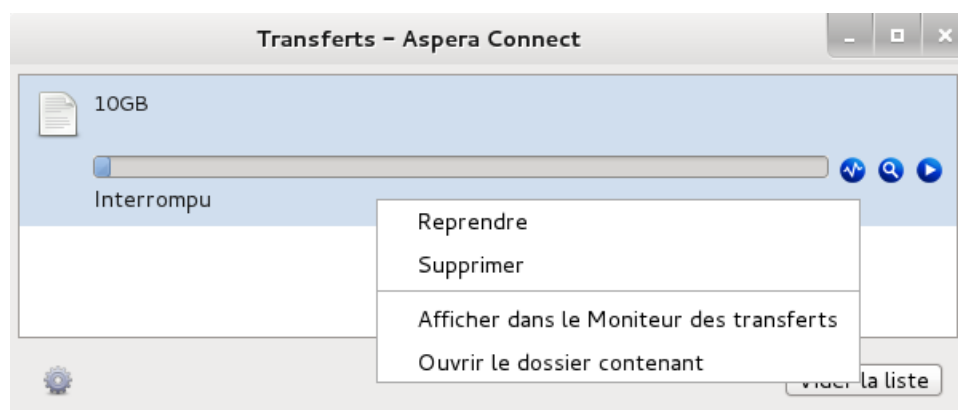


La fenêtre **Transferts** de Aspera Connect contient les commandes suivantes :


-  Ouvrir le Moniteur des transferts. Pour plus d'informations sur l'utilisation de cette fonctionnalité, veuillez vous référer à la rubrique « [Moniteur des transferts](#) ».
-  Afficher le fichier sur votre ordinateur.
-  Arrêter la session de transfert.
-  Reprendre le transfert.
-  Recommencer un transfert ayant échoué.



Lorsque l'option de mise en file d'attente est activée, seul un certain nombre de transferts simultanés sont autorisés. Les autres transferts sont mis en file d'attente dans la fenêtre **Transferts** et sont lancés lorsqu'un transfert se termine.


Vous pouvez lancer manuellement un transfert mis en file d'attente en cliquant sur le bouton . Vous pouvez également faire un clic droit sur un transfert en cours ou arrêté pour accéder à plusieurs commandes. L'exemple ci-dessous présente les options de clic droit pour un transfert arrêté.



Contrôle des transferts


Vous pouvez contrôler et ajuster la vitesse de transfert d'un fichier en cliquant sur le bouton  pour ouvrir la boîte de dialogue Aspera Connect **Moniteur des transferts**. Si vous disposez des autorisations serveur nécessaires et que la configuration de votre serveur de transfert vous le permet, vous pouvez modifier les éléments suivants dans cette boîte de dialogue :

Champ	Valeur
Barre de progression du transfert	Ajustez la vitesse de transfert du fichier en cliquant sur la barre de progression du transfert et en la faisant glisser.
	Cliquez pour afficher le dossier de destination des fichiers transférés.
	Cliquez pour arrêter la session de transfert.
Stratégie de transfert : <ul style="list-style-type: none"> • Fixe • Élevée • Moyenne • Faible 	Sélectionnez la stratégie de transfert dans la liste déroulante : <ul style="list-style-type: none"> • Le transfert transmet les données à une vitesse égale à la vitesse cible bien que cela puisse affecter la performance du reste du trafic présent sur le réseau. • La vitesse de transfert est ajustée pour utiliser la bande passante disponible à la vitesse maximum. • Le transfert tente de transmettre les données à une vitesse égale à la vitesse cible. Si les conditions du réseau ne le permettent pas, il transfère à une vitesse inférieure à la vitesse cible, mais supérieure à la vitesse minimum. • La vitesse de transfert est moins agressive que sous la stratégie Moyenne lors du partage de la bande passante avec le reste du trafic sur le réseau. Lorsqu'une surcharge se produit, la vitesse de transfert baisse jusqu'à la vitesse minimum, dans l'attente de la diminution du trafic.

 **Remarque :** Vous ne pouvez passer de la stratégie de transfert Élevée à la stratégie de transfert Moyenne que si l'hôte est Enterprise Server v3.0 ou versions ultérieures.

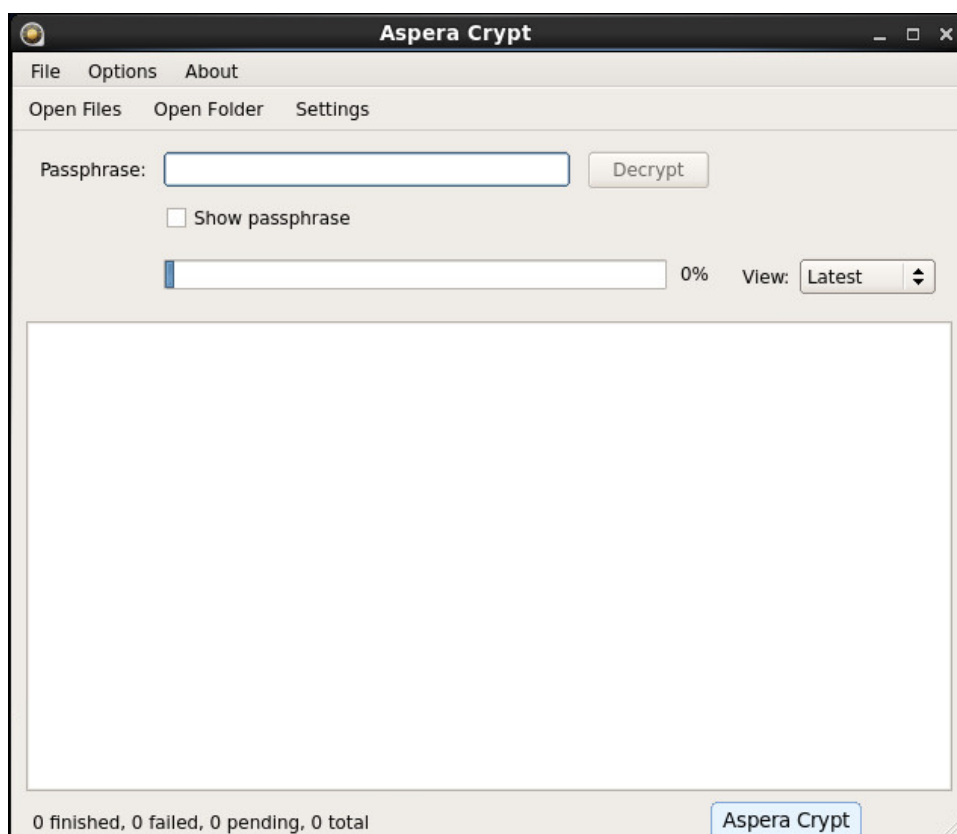
Déchiffrement des fichiers chiffrés

Une fois que vous avez téléchargé un package, fichier ou répertoire chiffré, Aspera Crypt vous permet de facilement le retrouver dans votre système de fichiers, de saisir votre phrase secrète et de déchiffrer le contenu.

 **Remarque :** Une fois qu'un élément chiffré a été téléchargé sur votre ordinateur, il a l'extension **.aspera-env** (Enveloppe de sécurité Aspera).

1. Lancez Aspera Crypt et recherchez votre package, fichier ou répertoire.

Pour lancer Aspera Crypt, allez dans le menu de l'application Aspera Connect et sélectionnez **Windows > Déverrouiller les fichiers chiffrés**.



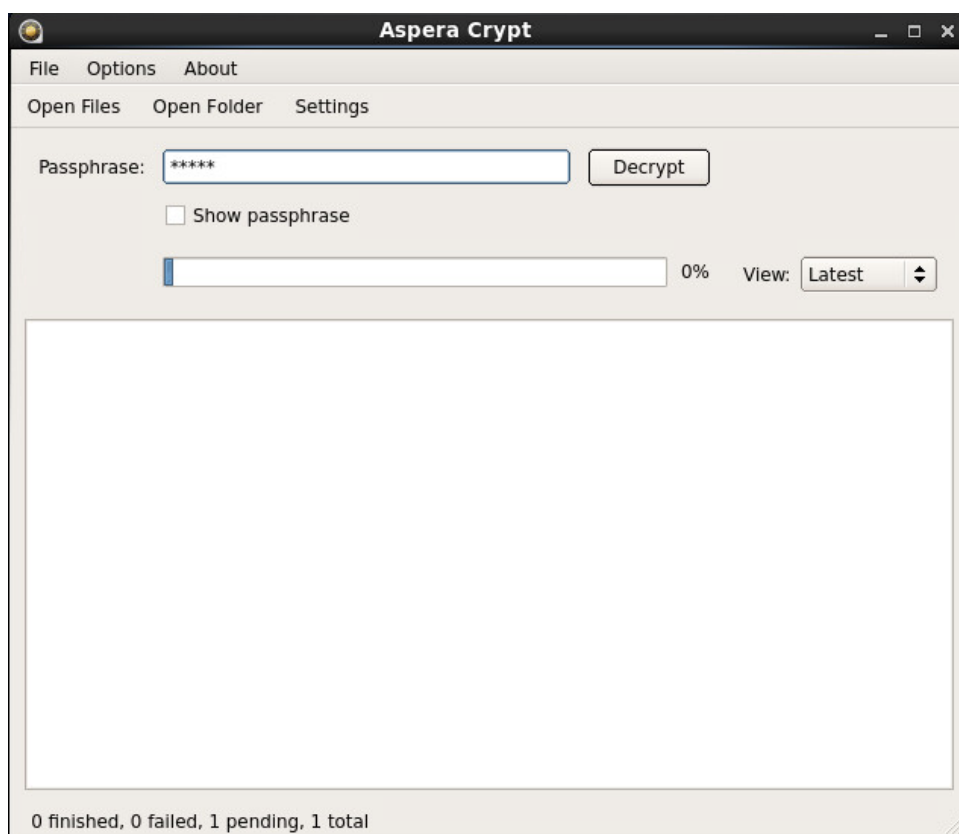
2. Recherchez votre package, fichier ou répertoire.

- Cliquez sur **Open Files** (Ouvrir fichiers) pour localiser un package Faspex ou un fichier du serveur Enterprise ou Connect.
- Cliquez sur **Open Folder** (Ouvrir dossier) pour localiser un dossier du serveur Enterprise ou Connect.

Lorsque vos contenus chiffrés sont chargés dans Crypt, un message d'état s'affiche en bas de l'application indiquant le nombre d'éléments prêts pour le déchiffrement.

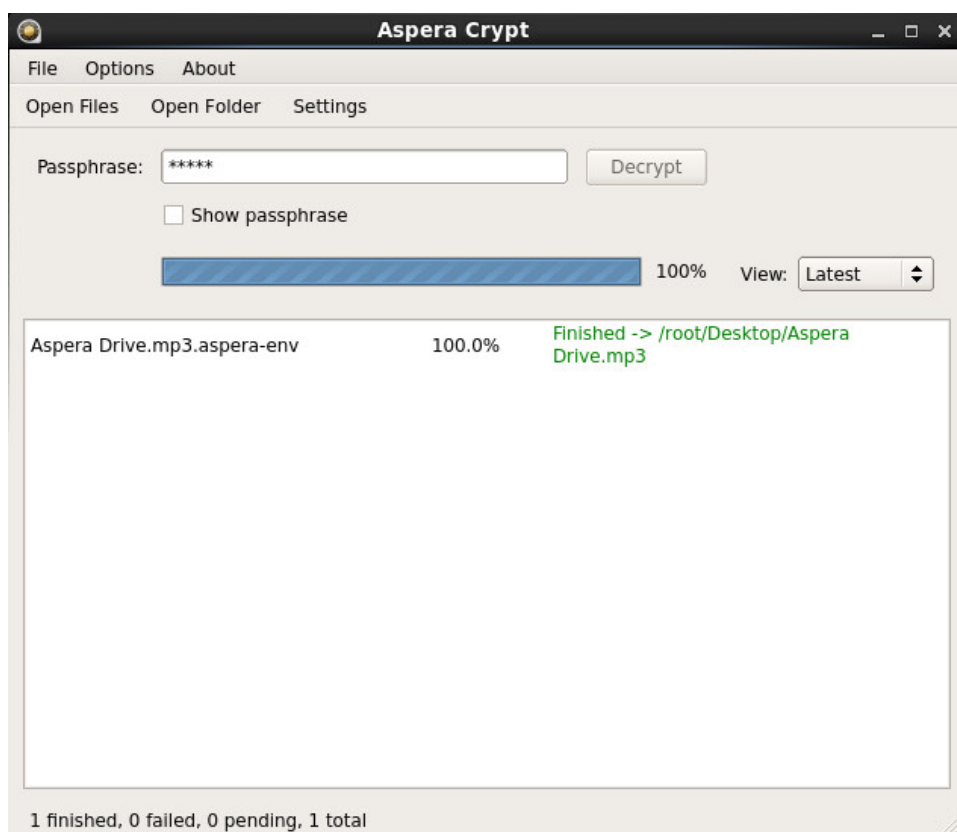
3. Saisissez votre phrase secrète et cliquez sur le bouton **Decrypt** (Déchiffrer).

Après avoir recherché vos contenus, entrez votre phrase secrète dans la zone de texte. Votre phrase secrète sera masquée sauf si vous cochez la case **Show Passphrase** (Afficher phrase secrète). Notez que vous devez saisir la phrase secrète correcte pour que le bouton **Decrypt** (Déchiffrer) soit activé. Une fois les fichiers chargés et le bouton **Decrypt** (Déchiffrer) activé, cliquez sur ce bouton pour déchiffrer votre package, fichier ou dossier.

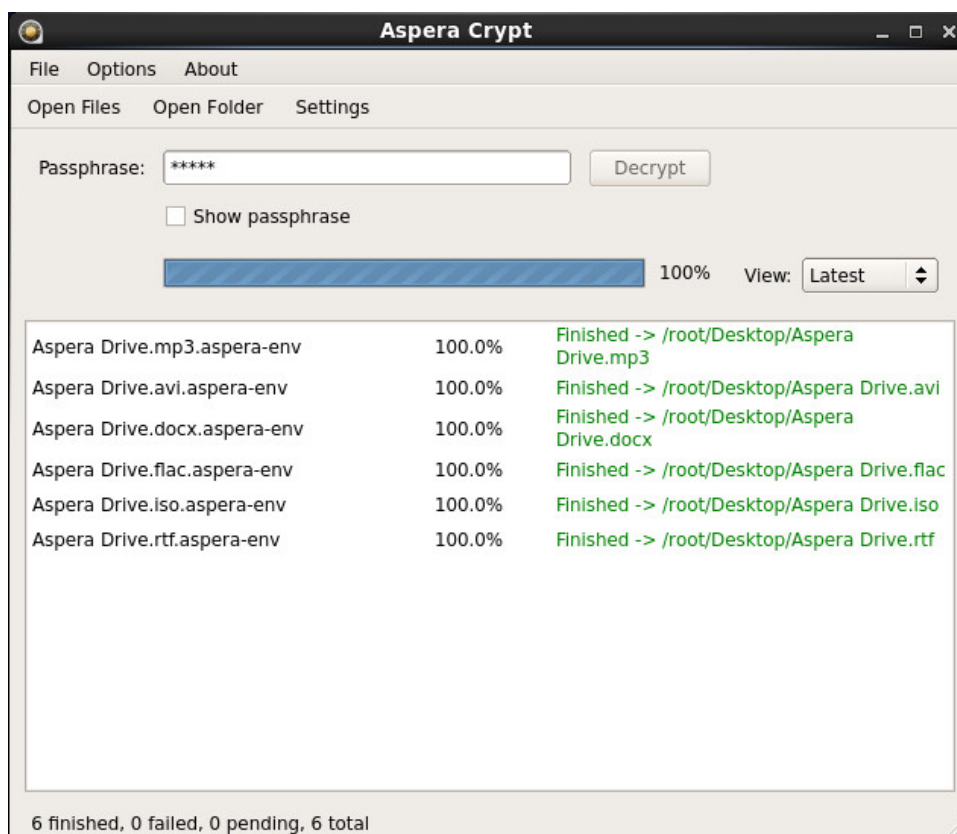


4. Affichez le résultat et confirmez le déchiffrement

Lorsque les contenus de votre package, fichier ou dossier ont été déchiffrés, vous pouvez visualiser le résultat dans la fenêtre d'affichage Aspera Crypt.



Les contenus déchiffrés s'affichent dans le même répertoire que celui des contenus chiffrés.



Si votre fenêtre d'affichage Crypt comporte plusieurs éléments déchiffrés répertoriés, vous pouvez utiliser la liste déroulante **View** (Afficher) pour trier les éléments par *dernière version*, *terminé* ou *échec*.

Désinstallation

Supprimez Aspera Connect de votre ordinateur.



Important :

Avant de procéder à la désinstallation de Aspera Connect, veuillez **quitter** tous les navigateurs ouverts.

Aspera Connect installe sur votre ordinateur les fichiers et dossiers suivants :

- `~/.mozilla/plugins/libnpasperaweb.so` Plug-in du navigateur Firefox
- `~/.aspera/connect` Fichiers d'application files, Préférences

Pour désinstaller Aspera Connect, commencez par sortir de l'application Aspera Connect et de tout autre navigateur Web ouvert. Ensuite, exécutez les commandes suivantes pour supprimer les fichiers installés :

```
# rm ~/.mozilla/plugins/libnpasperaweb_{connect build #}.so
# yes|rm -r ~/.aspera/connect
```

Appendice

Fichiers journaux

Recherchez les fichiers journaux de Aspera Connect.

Fichiers journaux

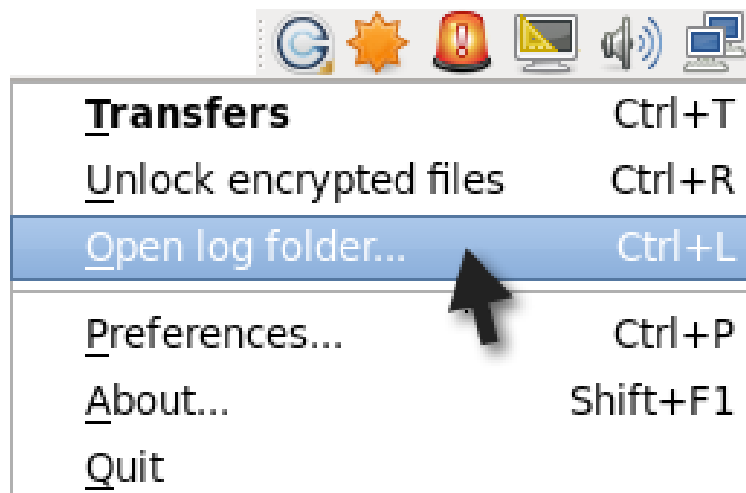
- aspera-connect.log
- aspera-connect-browser-plugin.log
- aspera-scp-transfer.log
- aspera-webinstaller-plugin.log

Emplacement du fichier journal

Les fichiers journaux sont situés dans le répertoire suivant :

```
~/.aspera/connect/var/log
```

Vous pouvez aussi utiliser le raccourci vers le dossier des journaux Connect en allant dans **Barre d'état système** > **Clic droit sur Aspera Connect** > **Ouvrir le dossier des journaux...** .



Dépannage

SELinux empêche l'accès au plug-in Connect

(RedHat, CentOS et Fedora uniquement)

Dans certains cas, SELinux (Security-Enhanced Linux) empêche l'accès au plug-in internet Aspera Connect. Le journal des messages sous `/var/log/messages` indique :

```
SELinux is preventing /usr/bin/bash from execute access on the file
asperaconnect. (SELinus refuse à /usr/bin/bash l'accès en exécution au
fichier asperaconnect.)
```

Pour résoudre ce problème, désactivez SELinux sur votre ordinateur en exécutant la ligne de commande suivante, qui ouvre le service et le désactive :

```
$ system-config-securitylevel
```

Si cette action ne désactive pas SELinux, modifiez le fichier de configuration suivant (accès superutilisateur requis) :


```
/etc/selinux/config
```

Dans **config**, localisez la ligne suivante :

```
SELINUX=enforcing
```

Modifiez la valeur du paramètre en **disabled**, comme indiqué ci-dessous.

```
SELINUX=disabled
```

 **Important :** Vous devez redémarrer le X-Server ou relancer le système après avoir modifié le fichier **config** SELinux. Si cette opération n'est pas effectuée, les modifications apportées à SELinux ne seront pas validées.

Problèmes de connectivité

Erreurs de connectivité et solutions potentielles.

Erreurs de connectivité SSH

Cette section s'applique aux délais d'attente qui surviennent pendant les transferts (codes d'erreur 13, 15 ou 40). Elle concerne le cas dans lequel Aspera Connect ne parvient pas à se connecter au serveur et reçoit le message d'erreur « Le délai d'établissement de la connexion a expiré ». Cette situation est causée par le blocage de la connectivité TCP. Aspera Connect tente de contacter le serveur sur le port TCP désigné (généralement configuré pour être 33001) et soit le pare-feu côté client interdit l'accès du TCP sortant, soit une configuration incorrecte du pare-feu côté serveur n'autorise pas le trafic TCP sortant vers le serveur Aspera. Pour résoudre ce problème, essayez de vous connecter au port TCP du serveur via le terminal de ligne de commande de votre ordinateur client (l'ordinateur sur lequel est installé Aspera Connect). Pour ce faire, exécutez la commande suivante pour vous connecter au serveur avec le **port 33001** (ou le port TCP configuré, si autre que 33001).

```
# telnet server-ip-address 33001
```

Notez que vous devrez remplacer `server-ip-address` par l'adresse IP du serveur Aspera.

Si le message d'erreur reçu est « Connexion refusée », le serveur Aspera n'exécute pas le service SSHD et vous devrez contacter votre administrateur de serveur. Si le message d'erreur reçu est « Délai expiré », le problème provient du pare-feu côté client, qui interdit probablement le trafic TCP sortant. Vérifiez que le pare-feu côté client autorise le **trafic TCP sortant avec le port 33001** (ou le port TCP configuré, si autre que 33001).

Erreurs de connectivité UDP

Cette section s'applique lorsque Aspera Connect semble se connecter correctement au serveur ; cependant, la progression du transfert indique 0 %, puis le message d'erreur « Expiration du délai de transfert des données » est reçu (codes d'erreur 14, 15 ou 18). Même si les fichiers à transférer apparaissent dans le répertoire de destination, ils ont une taille de 0 octet. Cette situation est due au blocage de la connectivité UDP. La connexion de contrôle via TCP est établie, mais la connexion de données (avec UDP) ne peut pas être établie. Les problèmes liés à l'UDP sont généralement causés par la configuration du pare-feu. Pour résoudre ce problème, vérifiez que le **port UDP 33001** est ouvert au trafic sortant.

Support technique

Pour obtenir une assistance complémentaire, vous pouvez nous contacter des manières suivantes :

Informations de contact	
E-mail	support@asperasoft.com
Téléphone	+1 (510) 849-2386
Formulaire de demande de renseignements	http://support.asperasoft.com/home

Horaires du service de support technique :

Type de support	Heure (heure standard du Pacifique, GMT-8)
Standard	8 h 00 – 18 h 00
Premium	8 h 00 – 12 h 00

Nous sommes fermés les jours suivants :

Dates d'indisponibilité du support technique	
Week-ends	Samedi, dimanche
Vacances Aspera	Veuillez consulter notre site Web .

Commentaires

Le service des publications techniques d'Aspera est à l'écoute de vos suggestions pour améliorer la documentation client Aspera. Pour nous soumettre un commentaire sur ce guide, ou sur tout autre document concernant un produit Aspera, veuillez visiter le [Forum des commentaires sur la documentation des produits Aspera](#).

Sur ce forum, vous pouvez nous signaler tout contenu que vous ne trouvez pas très clair ou qui vous paraît erroné. Nous vous invitons également à nous faire des suggestions pour de nouvelles rubriques, ainsi que sur des moyens d'améliorer la documentation pour la rendre plus lisible et plus facile à mettre en œuvre. Lors de votre visite sur le Forum des commentaires sur la documentation des produits Aspera, n'oubliez pas les éléments suivants :

- Vous devez être enregistré pour utiliser le site Web du support technique Aspera à l'adresse <https://support.asperasoft.com/>.
- Veuillez lire les instructions concernant le forum avant d'envoyer une demande.

Mentions légales

© 2008-2014 Aspera, Inc., une société du groupe IBM. Tous droits réservés.

Contenu sous licence - Propriété d'IBM

© Copyright IBM Corp. 2008, 2014. Utilisé sous licence

Droits restreints pour les utilisateurs du gouvernement américain - l'utilisation, la duplication ou la divulgation sont soumises aux restrictions visées dans le contrat GSA ADP Schedule conclu avec IBM Corp.

Aspera, le logo Aspera et la technologie de transfert *fasp* sont des marques déposées de l'entreprise Aspera Inc., enregistrée aux États-Unis. Aspera Connect Server, Aspera Drive, Aspera Enterprise Server, AsperaPoint-to-Point, Aspera Client, Aspera Connect, Aspera Cargo, Aspera Console, AsperaOrchestrator, Aspera Crypt, Aspera Shares, le module complémentaire Aspera pour Microsoft Outlook et Aspera Faspex sont des marques déposées de l'entreprise Aspera, Inc. Toutes les autres marques mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs. Toutes mentions à des produits tiers dans ce document sont faites uniquement à titre informatif. Toute entente, tout accord ou toute garantie, le cas échéant, s'effectue directement entre les vendeurs et les utilisateurs potentiels.