Contents

Réseau des Centres de Calcul FRançais

Un réseau très haut débit dédié interconnecte les trois centres de calcul nationaux : le Très Grand Centre de Calcul du CEA (TGCC) à Bruyères-le-Châtel, l'Institut du développement et des ressources en informatique scientifique (Idris) du CNRS à Orsay et le Centre informatique national de l'enseignement supérieur (Cines) à Montpellier.

Ce réseau des Centres de Calcul FRançais (CCFR) est mis à la disposition des utilisateurs pour faciliter leurs transferts de données entre les centres. Outre le transfert de données, l'accès interactif aux machines des centres via le réseau CCFR est proposé. Sont raccordées sur le réseau, les machines Irene au TGCC, Jean-Zay à l'Idris et Occigen au Cines.

Demande d'accès au réseau CCFR

L'accès au réseau CCFR nécessite une demande. Cette demande doit être portée par le responsable projet DARI auquel vous êtes rattaché. La demande est à déposer auprès de l'un des centres sur lequel vous disposez ou demandez un compte utilisateur. Toute demande d'accès au réseau CCFR déposée auprès d'un centre est automatiquement diffusée aux autres centres.

À la constitution de votre demande de création de compte utilisateur, via le portail DCC (https://www-dcc.extra.cea.fr/CCFR/), vous pouvez demander l'accès au réseau CCFR en cochant à l'étape 2 la case *Je souhaite utiliser CCFR.*

Si vous disposez déjà d'un compte actif sur l'un des centres, votre responsable projet DARI doit contacter le support du centre de calcul pour demander l'accès au réseau CCFR pour votre compte utilisateur.

La demande d'accès à CCFR est permanente dans le temps. Dès lors qu'un nouveau compte utilisateur vous est associé sur un centre, les autorisations d'accès sont mises à jour sur les centres pour vous permettre l'usage de CCFR entre les centres sur lesquels vous disposez d'un compte.

Pré-requis et authentification

Outre la demande d'accès au réseau, il est nécessaire de disposer d'un compte utilisateur valide sur les centres entre lesquels les échanges de données doivent avoir lieu. Les accès aux ressources du réseau sont authentifiés au même titre que les accès aux centres de calcul. Deux modes d'authentification sont proposés : l'authentification unique (Single Sign-On) par certificat X.509, communes aux centres, et l'authentification basique traditionnellement en vigueur sur les centres (mot de passe, etc). Nous vous préconisons l'authentification par certificat X.509 qui, après génération d'un jeton initial valide durant plusieurs heures, permet un accès automatisé aux ressources de site en site.

Demander un certificat X.509

Les certificats X.509 délivrés par l'autorité de certification GRID-FR de l'IGC MENESR sont reconnus pour l'authentification sur le réseau CCFR. Si vous ne bénéficiez pas d'ores et déjà d'un certificat délivré par cette autorité dans le cadre d'un autre projet, vous pouvez faire une demande de certificat personnel à l'adresse :

https://services.renater.fr/ssi/grid-fr/vos_certificats/demande/certificat_personnel

Vous devrez contacter le correspondant GRID-FR local de l'unité à laquelle vous êtes rattaché administrativement (l'unité mentionnée dans votre contrat de travail), afin qu'il enregistre votre profil par courriel signé. Si vous ne connaissez pas le correspondant GRID-FR de votre unité, veuillez contacter GRID-FR, à l'adresse grid-fr@renater.fr.

Associer son certificat à ses comptes utilisateurs

Une fois le certificat délivré par l'autorité de certification, il est nécessaire de communiquer son identification aux centres afin de le faire associer à ses comptes utilisateurs. Cette association permet l'authentification sur ces comptes à l'aide du certificat.

L'information d'identification à transmettre aux centres est le sujet du certificat (ou "Subject DN"). Lorsque le certificat est remis par l'autorité de certification, celui-ci est automatiquement installé dans votre navigateur Web. Vous pouvez obtenir le sujet du certificat en visualisant ses propriétés dans votre navigateur ou en l'exportant au format PKCS12, puis en interrogeant son contenu à l'aide de la commande openssl :

```
$ openssl pkcs12 -in cert.p12 -clcerts -nokeys | grep ^subject
```

Le sujet d'un certificat GRID-FR a généralement pour forme : **/O=GRID-FR/C=FR/O=Institut/OU=Unite/CN=Prenom Nom**.

Une demande d'accès au réseau CCFR est à transmettre à chacun des centres sur lesquels vous bénéficiez d'un accès, en précisant le sujet de votre certificat et le nom du compte utilisateur auquel l'associer. Contactez hotline.tgcc@cea.fr pour le TGCC, assist@idris.fr pour l'Idris et svp@cines.fr pour le Cines.

Configurer son certificat sur son centre primaire

Pour bénéficier de l'authentification unique par certificat X.509, il est recommandé d'installer votre certificat sur votre centre de travail principal. Pour ce faire, exportez votre certificat de votre navigateur au format PKCS12, puis copiez le fichier exporté sur le centre de votre choix. La commande suivante vous permet d'installer votre certificat sur votre compte :

```
$ module load ccfr
$ ccfr_mycert install cert.p12
```

Afin de protéger la clé privée associée à votre certificat, un mot de passe est à saisir. Ce mot de passe sera nécessaire à chaque utilisation initiale du certificat, afin de générer un certificat proxy temporaire qui sera utilisé pour s'authentifier sur les services du réseau. Le mot de passe protégeant la clé doit utiliser au moins trois classes de caractères différentes et contenir au minimum douze caractères.

Une fois le certificat installé sur votre compte, il est recommandé de supprimer de votre compte le fichier PKCS12 qui vous a permis de réaliser l'installation. Vous pouvez consulter le statut de votre certificat avec la commande `ccfr_mycert`.

Accès interactif

L'accès interactif aux machines des centres via le réseau CCFR est proposé. Une commande wrapper est fournie pour simplifier les usages :

```
$ module load ccfr
$ ccfr_ssh <machine>
```

Cette commande `ccfr_ssh`, basée sur le protocole SSH, récupère automatiquement les informations de connexion à la machine spécifiée (nom de domaine, port spécifique) et détecte les possibilités d'authentification. Si un certificat X.509 est installé dans votre compte et que la machine ciblée supporte ce mécanisme d'authentification, alors une authentification par certificat sera réalisée. Dans le cas contraire, la commande optera pour une authentification basique, utilisant les modalités traditionnelles en vigueur sur la machine ciblée.

Le détail de la commande, ainsi que la liste des machines accessibles sur le réseau CCFR sont disponibles en précisant l'option `-h` à la commande `ccfr_ssh`.

Transfert de données

Le transfert de données entre les machines des centres via le réseau CCFR constitue le service principal sur le réseau. Une commande wrapper est fournie pour simplifier les usages :

```
$ module load ccfr
$ ccfr_cp <src> <machine>:<dst>
```

Comme pour `ccfr_ssh`, la commande `ccfr_cp` récupère automatiquement les informations de connexion à la machine spécifiée et détecte les possibilités d'authentification pour réaliser, si possible, une authentification par certificat. La commande `ccfr_cp` est basée sur l'outil rsync, configuré pour faire transiter les données sur le protocole SSH. La copie réalisée est récursive et préserve les liens symboliques, les droits d'accès ainsi que les dates de modification des fichiers.

Le détail de la commande, ainsi que la liste des machines accessibles sur le réseau CCFR sont disponibles en précisant l'option `-h` à la commande `ccfr_cp`.

Une commande `ccfr_sync`, variante de `ccfr_cp`, permet une synchronisation forte entre la source et la destination en ajoutant, par rapport à la commande `ccfr_cp`, la suppression des fichiers de la destination non présent dans la source.