2020 年 5 月 11 日

Cygnus での JLDG 利用規則

筑波大学計算科学研究センター
計算機システム運用委員会
JLDG 筑波大拠点管理者グループ

(適用範囲)

1. 本規則は、計算科学研究センタースーパーコンピュータ cygnus のログインノードで、JLDG ファイルシステムにアクセスするユーザに適用する。以下、cygnus ログインノードを Cygnus と略称する。

(利用資格)

2. Cygnus, JLDG 両システムでアカウントを有するユーザは、『Cygnus での JLDG 利用』を申請できる。
3. Cygnus のユーザ ID と JLDG で有効なグリッド証明書サブジェクトの組を申請し、両システムの管理者の確認を経て、利用資格を得る。手順の詳細は、別途定める。

(グリッド証明書の取り扱い)

4. Cygnus へは、グリッド証明書に基づく GSI 認証 SSH ログインを許可する。
5. Cygnus での JLDG 利用に必要な代理証明書の生成は以下の方法を許可する。
   ① GSI 認証 SSH ログインの際の代理証明書委譲
   ② 証明書のリポジトリサーバからの myproxy-logon による代理証明書のダウンロード
   ③ 他のシステムで生成した代理証明書の scp(公開鍵認証)によるリモートコピー
6. Cygnus に、認証局発行の証明書や鍵を置くことは禁止する。従って、Cygnus では、証明書・鍵から代理証明書を生成することはできない。

Cygnus での JLDG 利用手順

2020 年 5 月 18 日改訂

(適用範囲)

1. 本文書は、『Cygnus での JLDG 利用』の手順を纏めたもので、『Cygnus での JLDG 利用規則』(以下、規則)を補完するためのものです。

(利用資格)

2. 規則第 3 条の利用資格は、Cygnus のファイル /etc/grid-security/grid-mapfile.jldg で管理されます。このファイルに、"JLDG グリッド証明書のサブジェクトと cygnus の user ID の組"が登録されると、利用資格が生じます。
3. 利用申請では、申請者の Cygnus の user ID と JLDG グリッド証明書が、共に、申請者自身のものであることを検証します。申請の過程で、以下の 2 点がチェエックされます。
   - ✓ Cygnus での申請者の本名と、JLDG グリッド証明書サブジェクト内の本名が一致すること
   - ✓ Cygnus での申請者が JLDG の自身のホームディレクトリに書き込みできること
     (これは、申請者が、対応する JLDG グリッド証明書を所持し使用できる事を意味します。)
4. 利用申請手順は以下の通りです。
   - ✓ 事前に、Cygnus で、コマンドパスの先頭に /usr/local/JLDG/bin を加えてください
   - ✓ Cygnus で **jldg-map-key.sh** (引数なし) を実行します。表示内容を確認の上、JLDG グリッド証明書サブジェクトを入力します。
   - ✓ JLDG 側でのユーザの確認が済むと、jldg-map-1234-567-8901 の形式の jldg-map-から始まり 3 つの数値をハイフン(-)で繋いだ文字列が提示されます。
   - ✓ 提示された文字列をファイル名とするファイルを、Cygnus と JLDG のホームディレクトリに作成して下さい。ファイルの中身は空でかまいません。
   - ✓ 再び Cygnus に戻り、**jldg-map-req.sh jldg-map-1234-567-8901** を実行します。(引数はファイル名)
   - ✓ JLDG 側でファイルの存在がチェックされると制御はユーザーに戻されます。
   - ✓ 手続き終了後 30 分以内に、管理簿 /etc/grecurity/grid-mapfile.jldg に反映されます

(GSI 認証 SSH ログインと利用法)

5. 利用登録終了後、Cygnus に GSI 認証で ssh ログインすると、ログイン元の証明書に基づき、Cygnus に代理証明書がつくられます。ログイン元端末の設定、ログイン方法、ログイン後の JLDG ファイルシステムのマウント方法などは、基本的に、『JLDG-HPCI 連携システムホスト』利用の場合と同じです。ただし、以下の点が異なっています。
   - ✓ Cygnus のホスト証明書は HPCI 発行のものです。ログイン元端末の /etc/grid-security/certificates に HPCI CA 局証明書を配置して下さい。(JLDG-HPCI 連携システムホスト(jldghpci)のホスト証明書は KEK CA 局発行です。)
   - ✓ Cygnus の gsissh の待ち受け port は、2222 です。(HPCI 資源と同一です。22 番 port は通常の sshd が待ち受けています。jldghpci では 22 番 port に gsisshd が立っていて、gsi 認証以外の認証は停止しています。従って、cygnus01 へのログインは、
     % gsissh -p 2222 -l user cygnus01.ccs.tsukuba.ac.jp
   - ✓ 筑波大 JLDG クライアント jldg-fr3 には、gsissh がインストールされています。

6. Cygnus で gfarm コマンドを実行する前に、/usr/local/JLDG/bin がコマンドパスの先頭にある事を、再度確認してください。理由は以下の通りです。HPCI の採択課題で cygnus を利用するユーザに HPCI 共用ストレージへのアクセスを提供するため、Cygnus には、gfarm が install されていますが、JLDG の gfarm と版が異なり、互換性がありません。JLDG 用 gfarm は /usr/local/JLDG 以下にインストールされており、コマンド群は、その下の bin/ にある為です。JLDG 用の gfarm コマンド（gfls, gfwhere 等 gf で始まるコマンド)は、JLDG 用 gfarm の設定ファイル /usr/local/JLDG/etc/gfarm2.conf を default で参照する様になっていますので、コマンドパスさえ正しく設定してあれば、他のクライアントと違いはありません。但し、設定ファイルを指定する必要があるコマンドには注意が必要です。次項を参照下さい。

7. JLDG ファイルシステムのマウントには、幾つか方法があります。汎用性が高い方法は、
   % mount.gfarm2fs /usr/local/JLDG/etc/gfarm2.conf /tmp/yoshie gfarmfs_root=/
   です。第 1 引数は JLDG 用 gfarm の設定ファイルです。第 2 引数はマウントポイントで、あらかじめ作成しておくことを推奨します。[この例の通りにしないで下さい。] 第 3 引数は マウントする JLDG ファイルシステムツリーのトップディレクトリで、この例では、JLDG の root (/) が Cygnus の /tmp/yoshie にマウントされます。対応するアンマウントは、% umount.gfarm2fs /tmp/yoshie です。
   - ✓ mount.gfarm2fs の第 2 引数のマウントポイントを NFS ファイルシステム上に取るのは､非推奨です。/tmp/`whoami` 又は /tmp/`gfwhoami` をお勧めします。
   - ✓ Cygnus のログインノードは cygnus0[123].ccs.tsukuba.ac.jp の 3 台で、 JLDG ファイルシステムのマウントは独立です。ホームディレクトリは共有ですが、ホームディレクトリ下のマウントポイントに JLDG ファイルシステムをマウントしても、別ログインノードからは参照できません。cygnus.ccs.tsukuba.ac.jp への gsissh では、3 台の何れかに、ラウンドロビンでログインします。

8. Shell script 等のバックグラウンド実行と、代理証明書の取り扱い
   gfarm コマンド（マウントした JLDG ファイルシステムに対するファイル操作を含む)を実行する shell script 等をバックグラウンドで実行し、login shell を抜ける (logout)場合、『gfarm コマンドが実行される時点で、gfarm コマンドが有効な代理証明書を参照できる』様に、工夫する必要があります。ポイントは、
   - ✓ gsissh login で生成される代理証明書の有効期限は、ログイン元の代理証明書の有効期限と同じ
   - ✓ gsissh login では、代理証明書のファイル名がランダムに生成され、ファイル名は、環境変数 X509_USER_PROXY にセットされる。Gfarm コマンドは、この環境変数を参照している。
   - ✓ gsissh login shell からログアウトすると、代理証明書ファイルは消される。Shell script では、起動時の環境変数が有効であり続けるので、gfarm コマンドが代理証明書を見つけられず、認証に失敗する。
   - ✓ gfarm コマンドは、環境変数 X509_USER_PROXY が無い場合、標準のファイル
     /tmp/x509up_u`id -u` を参照する。 (`id -u` は、Cygnus 上の user id 番号です)

   以上の事から、以下の手順で対応できる事がわかります。
   - ✓ gsissh で Cygnus に作られた代理証明書 $X509_USER_PROXY を、標準のファイル名ファイルにコピーし、X509_USER_PROX を unset して、shell script を開始する
   - ✓ 代理証明書の有効期限内に、ログイン元で期限が先の代理証明書を作り、Cygnus に gsissh ログインし、代理証明書を標準の場所にコピーする

   なお、mount.gfarm2fs は、gfarm2fs 実行前処理で、代理証明書の標準場所へのコピーを行っています。また、JLDG ファイルシステムがマウント済みの場合、mount.gfarm2fs は代理証明書のコピーのみ行います。従って、『mount.gfarm2fs, unset X509…, shellScript.sh &, (gsissh), mount.gfarm2fs』も可能です。