OPAL – proposition de politique d’accès croisés

V0.9 – 2018-08-06

Table des matières

1 - Introduction

Le groupe de travail “accès croisés” de OPAL a été créé par le Comité Technique OPAL (compte rendu de réunion du 17/01/2018) pour proposer **une évolution des modalités d’accès à OPAL et mettre en oeuvre la solution retenue**, dans le cadre de la création du méso-centre distribué OPAL.

OPAL est une ***plateforme*** mutualisée incluant plusieurs ***équipements*** (ressources de calcul, visualisation), mise en œuvre par un groupement de ***membres*** (UNS, OCA, Mines ParisTech, Inria) à destination d’une communauté d’***ayants droit*** (utilisateurs avec autorisation d’accès aux équipements [i]).

La notion d’***accès croisés*** recouvre :

- L’accès par les ayants droit d’un membre de OPAL aux équipements des autres membres de OPAL,
- L’accès à la plateforme OPAL pour l’ensemble des ayants droit.

Un premier document fait un état des lieux des modalités d'accès actuelles aux ressources de calcul existantes des partenaires du CPER OPAL (UNS, OCA, Mines ParisTech, , Inria).

Ce document, qui s'appuie en très grande partie sur les travaux du groupe de travail accès croisés, propose une cible pour les modalités d'accès à la plateforme OPAL.
La cible prend notamment en compte les objectifs de :

1. Simplicité d'usage pour l'utilisateur OPAL : faciliter l'accès croisé aux différents équipements de OPAL pour contribuer à l'adoption du méso-centre distribué ;
2. Continuité pour l'utilisateur actuel : minimiser les changements d'utilisation imposés aux utilisateurs des équipements existants inclus dans OPAL ;
3. Délai court de mise en oeuvre par des équipes techniques réduites ;
4. Viabilité des choix effectués : passage à l'échelle des membres de OPAL et de UCA/UCA^{jedi} avec un coût opérationnel raisonnable.

2 - Ayants droit OPAL : qui ? comment ?

Pour mettre en oeuvre les accès croisés OPAL, deux préalables nécessaires sont de savoir :

- Qui sont les ayants droit OPAL ?
- Comment est validée une demande d'accès à OPAL ?

Les ayants droit OPAL sont les personnels (y compris les stagiaires) rattachés à un membre de OPAL (UNS, OCA, Mines ParisTech, Inria) ou de UCA ou de UCA^{jedi} :

1. **soit au titre de leur appartenance à une structure locale** à la zone géographique d'implantation de UCA. Exemples : une UMR locale, une équipe de recherche locale d'un établissement membre de UCA.
2. **soit au titre de leur participation à un projet :**
    a. **validé par une structure transverse de UCA** (MSI, Centre de référence,...)
    b. **en collaboration avec un ayant droit appartenant à une structure locale** (pour les projets qui ne sont pas portés par une structure transverse UCA, type MSI).

Le droit d'accès à OPAL s'entend dans le cadre des activités donnant droit et pour la durée de ces activités.

Les industriels, les personnels des membres de OPAL non affectés dans la zone géographique d'implantation de UCA, les invités et les collaborateurs externes des ayants droit OPAL, etc. **peuvent donc accéder à OPAL au titre de leur participation à un projet éligible à OPAL et uniquement à ce titre** (donc dans le cadre des activités du projet et pour la durée de ce projet).

L’accès par les étudiants dans le cadre de cours est possible sur **certaines plateformes** de OPAL sous supervision d’un enseignant. **Ces accès sont élargis à OPAL dans le cadre de formations validées par le Comité Scientifique OPAL** (toujours sous encadrement d'un enseignant).

OPAL s’ajoute aux usages actuels des équipements sans les remettre en cause :
l’usage d’un équipement inclus dans OPAL est mutualisé avec la communauté des ayants droit OPAL ; mais simultanément l’équipement reste la propriété d’un membre de OPAL qui peut accorder des accès additionnels à cet équipement selon ses critères, en plus des accès des ayants droit OPAL.

L’***accréditation* OPAL** est la procédure par laquelle une ***autorité d’accréditation*** valide une demande d’accès à OPAL.
Un utilisateur qui souhaite accéder à OPAL dépose une demande d’accès. La demande est examinée par une autorité d’accréditation car une liste a priori des ayants droit OPAL n’est pas définie.

Les autorités d’accréditation OPAL sont :

1. **les membres de OPAL** (UNS, OCA, Mines ParisTech, Inria)
    a. qui conservent les comités et procédures en place pour leurs équipements actuels, et les adaptent pour s’aligner sur la cible définie dans ce document (ex: prise en compte de la définition des ayants droit) ;
    b. qui traitent les demandes émanant des projets et des structures rattachées à leur entité.
2. **une ou plusieurs autorités additionnelles à créer**, pour traiter les demandes issues des autres projets et structures de UCA / UCA^{jedi}
    Le Comité Scientifique OPAL désigne une autorité déléguée pour chaque membre de UCA (autre que les membres de OPAL), ainsi que pour chaque structure transverse de UCA (ex : MSI, Centres de référence, ...). Cette autorité déléguée traite les demandes d’accès issues du périmètre délégué.

Une autorité d’accréditation OPAL :

- a la responsabilité de s’assurer du respect des règles définissant les ayants droit pour son entité (ex: elle ne valide que des demandes éligibles à OPAL et leur adjoint une date d’échéance adaptée) ;
- peut mettre en œuvre des critères additionnels de sélection des projets ou des structures afin de contribuer à une utilisation optimale des ressources ;
- a la responsabilité de s’assurer du respect de la “charte d’utilisation de OPAL” (voir après) par les ayants droit qu’elle accrédite. Elle

vérifie notamment la signature préalable d'une charte informatique par le demandeur et lui communique les règles de citation de OPAL ;
- ajoute au référentiel OPAL les ayants droits qu'elle accrédite en renseignant pleinement leur entrée (ex : contact du responsable sécurité et du support technique) et maintient à jour ces informations.

Le portail utilisateur commun OPAL décrit les différents cas et fournit les liens pour déposer une demande d'accès à OPAL.

3 - Engagements des utilisateurs OPAL : charte, citation

Une charte d'utilisation de OPAL :
- sera écrite (proposition à fournir par le GT "accès croisés") ;
- et publiée sur le portail utilisateur commun OPAL (accessible depuis Internet sans authentification).

La charte d'utilisation de OPAL contient initialement :

1) Les principaux éléments de ce document :
   a) introduction ("OPAL est une plateforme mutualisée", etc.), rôles et responsabilités (Comités, utilisateurs) ;
   b) définition des ayants droit, de l'accréditation et des autorités d'accréditation ;
   c) règles de citation.
2) **Le lien entre un ayant droit OPAL et une charte informatique :** préalablement à leur accréditation, les ayants droit OPAL signent avec leur autorité d'accréditation un document tenant lieu de charte informatique**. Cette charte informatique s'applique de fait pour l'ensemble de leurs activités sur OPAL, complétée par la charte OPAL :**
   a) charte d'établissement (de leur entité de rattachement) ;
   b) charte de plateforme (de l'équipement OPAL qui les héberge) ;
   c) contrat (avec leur entité de rattachement).
3) **Le lien entre un équipement OPAL et des règles de gestion :** l'activité sur chacun des équipements composant la plateforme OPAL reste régie par les règles, chartes, conditions techniques spécifiques à cet équipement (fournir les liens pour chacun des équipements).

Discussion : l'articulation de la charte décrite ci-dessus signifie que chaque équipement de OPAL "fait confiance" à la charte informatique qu'un ayant droit a signé dans son établissement de rattachement, ce qui évite de lui faire signer d'autres chartes pour accéder à OPAL (zéro papier supplémentaire).
Cela évite également de perturber les règles de fonctionnement des équipements existants de OPAL (ex: niveau de service, mesures conservatoires, paramétrage technique, etc.).

Cette articulation permet donc de simplifier la mise en œuvre de OPAL. Sa viabilité juridique pourra être ré-examinée dans un second temps.

Les règles de citation pour les ayants droit OPAL évoluent afin de favoriser la visibilité de la plateforme mutualisée.

Tout ayant droit OPAL :

a) **remercie systématiquement OPAL**[1] dans ses publications scientifiques et ses communications portant sur des travaux qui ont utilisé des ressources de OPAL **même lorsque ces ressources OPAL sont situées dans son établissement de rattachement** ;
b) signale ses publications par mail (voir ci-dessous).

Éléments à fournir pour la mise en œuvre des règles de citation :

- éléments de citation : paragraphe Latex, mots-clés (ex: OPAL, UCA) ;
- tampon HAL OPAL et lien vers le portail HAL UCA ;
- adresse mail opal-publications@univ-cotedazur.fr pour signaler les publications.

Toutes les publications incluant des travaux sur un équipement OPAL seront saisies par leurs auteurs scientifiques ou par leur entité dans HAL, puis tamponnées OPAL, afin de faciliter la communication sur la production scientifique de la plateforme mais aussi la valorisation de cette production pour OPAL ou UCA. Il reviendra au Comité Scientifique de gérer manuellement le tamponnage et les éventuels manquements aux règles de saisie.

4 - Gestion technique des comptes OPAL

On constate :
- une hétérogénéité de la gestion des comptes, et en particulier un recouvrement des plans UID/GID des utilisateurs sur les différents équipements de OPAL
- des modes d'authentification variés

Afin de permettre l'ouverture des accès croisés dans des délais assez brefs, nous préférons ne pas homogénéiser cette gestion des comptes : un même utilisateur n'aura pas forcément le même login ni le même numéro UID sur les différents équipements.
En revanche, au vu de la partie sur les "ayants droit" la création d'un référentiel regroupant l'ensemble des données de référence OPAL est nécessaire pour gérer les différents utilisateurs en plus des annuaires/référentiels des membres et des équipements.

---

1 Le remerciement OPAL n'est bien sûr pas exclusif : il peut y avoir des remerciements additionnels pour un équipement de OPAL, pour un établissement, une équipe, etc.

4.1 - Le référentiel OPAL

Quelles données ?

- **l'autorité d'accréditation qui a validé le compte OPAL** (pourra être présenté à l'utilisateur comme "quel cluster d'origine" - quand il en a un) => nomenclature des identifiants d'autorité à établir (string ou code ?)
- **identifiant de l'ayant droit OPAL** :
    - adresse mail (celle communiquée sur cluster d'origine)
- **autres informations d'identification** de l'ayant droit :
    - login de préférence (a priori celui sur cluster d'origine, pas forcément possible d'utiliser le même login sur les autres équipements)
    - Nom
    - Prénom
- **contact du support technique** de l'entité d'origine : adresse mail (ou URL d'un helpdesk avec accès public)
- **contact du responsable sécurité** (SSI) de l'entité d'origine : adresse mail
- **date d'expiration des droits** (mise à jour à la modification des droits)
- **titre d'ayant droit** : par exemple laboratoire d'appartenance, collaboration avec une structure UCA, équipe, parrain (format libre, informatif et utile pour le support, mais ne doit pas être impératif au fonctionnement technique ou utilisé pour des extractions de statistiques)
- **champ commentaire** : pas d'utilisation prévue pour le moment

Quel format ?
- un annuaire LDAP ? => choix à défaut de motivation spécifique
- une base de données ?

Remarque : Dans un deuxième temps nous pourrions être amenés à normaliser (nomenclature) les caractéristiques précisant à quel titre l'ayant droit est autorisé afin de permettre des extractions, des statistiques,… Par exemple en s'appuyant sur l'annuaire UCA.

Respect du RGPD :
Le référentiel OPAL sera une base contenant des informations personnelles il est important de respecter le RGPD lors de sa mise en œuvre. A réaliser en collaboration avec les Délégués à la Protection des Données des membres.

4.2 - Processus d'accréditation et de création du compte d'un utilisateur

Ce paragraphe décrit les processus d'accréditation et de création des comptes utilisateur en particulier :

- quand et comment accrédite-t-on un utilisateur ?
- quand crée-t-on le compte utilisateur sur un équipement ?

4.2.1 - Accréditation d’un utilisateur auprès du projet OPAL

Un utilisateur accrédité a le droit d’accéder à l’ensemble des équipements.
Rappel : comme défini dans le paragraphe sur « l’autorité d’accréditation OPAL », accréditer un utilisateur implique notamment de :

- vérifier la signature préalable d’une charte informatique par le demandeur ;
- lui communiquer les règles de citation de OPAL ;
- le rajouter au référentiel OPAL.

Les utilisateurs éligibles le sont à plusieurs titres par ordre de précédence :

Cas 1 : appartenance à un membre OPAL

L’autorité d’accréditation du membre OPAL prend en charge le processus d’accréditation. Elle s’assure notamment de l’éligibilité de la demande (ex : appartenance à une structure locale ou projet en collaboration avec un ayant droit appartenant à une structure locale).

Par exemple, le processus d’accréditation peut être pris en charge par l’équipe du membre qui opère un équipement OPAL.

Cas 2 : appartenance à un membre de UCA (autre que les membres OPAL)

L’autorité d’accréditation déléguée (définie par le Comité Scientifique) associée à son institution prend en charge le processus d’accréditation.

Le portail OPAL contient les liens vers les procédures d’accréditation associées à chaque institution.

Cette autorité d’accréditation déléguée jouera également un rôle de conseil et pourra orienter l’utilisateur vers l’équipement le plus adapté à son besoin.

Cas 3 : via un projet porté par une structure transverse de UCA (ex : MSI, Centres de référence,...)

Le projet devra être préalablement validé par cette structure transverse.

L’autorité d’accréditation déléguée (définie par le Comité Scientifique) associée à cette structure transverse prend en charge le processus d’accréditation.

Le portail OPAL contient les liens vers les procédures d’accréditation associées à chaque structure transverse.

Cette autorité d'accréditation déléguée jouera également un rôle de conseil et pourra orienter l'utilisateur vers l'équipement le plus adapté à son besoin.

4.2.2 - Création du compte d'un utilisateur sur un équipement

L'équipe du membre OPAL opérant l'équipement prend en charge la création des comptes des ayants droit accrédités. Il lui revient de vérifier cette accréditation en consultant le référentiel OPAL.

Dans le cas particulier où ce membre OPAL est également autorité d'accréditation de l'utilisateur, il a la possibilité d'articuler les deux procédures d'accréditation et de création de compte comme il l'entend. Ce membre OPAL peut également choisir de faire suivre aux utilisateurs disposant déjà d'un compte sur leur équipement et dont il est autorité d'accréditation le processus d'accréditation OPAL.

Conséquence : tous les ayants droit OPAL qui ont déjà un compte sur un équipement existant à inclure dans OPAL pourront être ajoutés au référentiel dans la phase d'initialisation sans refaire une procédure administrative. En revanche ils devront prendre connaissance des nouvelles obligations : charte, règles de citation,...

5 - Gestion technique des accès

Les différents équipements ont leurs propres politiques de sécurité pour protéger les accès à l'équipement. Il faut faciliter les accès croisés, sans remettre en cause ces politiques (simplifier la mise en œuvre).
Ce paragraphe décrit les configurations qui sont mises en œuvre pour autoriser les accès aux équipements pour les utilisateurs.

La suite de ce paragraphe est spécifique aux 3 équipements initiaux de OPAL de type cluster : clusters OCA, Mines ParisTech, Inria.

Terminologie des machines sur un équipement de type cluster :
- *bastion* : serveur permettant l'accès (ssh) depuis l'extérieur
- *frontal* : serveur permettant la compilation, la gestion des jobs, l'accès interactif, la copie de fichier, la visualisation de données
- *noeud* : ressource de calcul

Cas 1 : accès depuis le frontal du cluster A vers le frontal du cluster B ?

intérêt : faciliter les connexions des utilisateurs, les calculs et expérimentations croisées, etc.

choix de mise en œuvre : ajout d'autorisations croisées sur les firewalls des 3 équipements : ouverture des accès ssh (entrant sur 3 équipements + sortant chez OCA). A voir dans le futur si on peut avoir besoin d'autres protocoles.

Cas 2 : accès depuis une machine (cluster ou poste de travail) connectée sur le site du membre A à un nœud du cluster B ?

intérêt : pas d'intérêt clairement identifié (couplage de ressource ?)

choix de mise en œuvre : non déployé au moins en phase 1 : complexité car les nœuds en adresses IP privées sont non accessibles sans mise en place de NAT

Cas 3 : accès depuis un poste de travail connecté sur le site du membre A vers le frontal du cluster B ?

intérêt : faciliter les connexions des utilisateurs depuis les machines connectées sur les sites des membres OPAL

choix de mise en œuvre : non déployé :
- liste potentiellement complexe et changeante de préfixes IP à gérer de manière coordonnée
- pas d'homogénéité sur les politiques de gestion des postes de travail

Cas 4 : accès depuis le VPN d'une entité ayant droit A vers le frontal du cluster B ?

intérêt : faciliter les connexions des utilisateurs des principales entités des ayants droit

choix de mise en œuvre : ajout d'autorisations croisées sur les firewalls des 3 équipements : ouverture des accès ssh.

- moins de préfixes IP à gérer que pour les postes de travail, plus stable, plus de confiance dans les personnes qui ont un compte VPN (au moins car l'expiration du compte utilisateur dans l'entité provoque l'expiration du compte VPN).
- attention : il est nécessaire d'avoir un contact à la DSI de l'entité ayant droit. Initialement les accès seront donc ouverts pour OCA, Mines, Inria et UNS.

Cas 5 : accès depuis Internet vers le frontal du cluster B ?

intérêt : faciliter la connexion de tous les ayants droit OPAL : domicile, les accès d'un collaborateur distant sur projet (hors site et sans VPN), ...

choix de mise en œuvre : à effectuer par chaque membre OPAL pour l'équipement qu'il gère (conserver ou adapter la mise en œuvre actuelle)

Les 3 équipements envisagent de conserver leur mise en œuvre actuelle :
- OCA : conserve la procédure d'accès actuelle : ouverture depuis des préfixes IP (laboratoires partenaires) ou depuis des adresses IP spécifiques (collaborateurs externes avec contact SSI) ou depuis les préfixes IP des clients VPN de partenaires autorisés
- Mines : via le bastion ssh Mines ParisTech Sophia (compte créé à la demande pour les utilisateurs du cluster)
- Inria : via le bastion ssh du cluster (compte créé systématiquement pour les utilisateurs du cluster)

6 - Support technique aux utilisateurs OPAL

Le support à l'utilisation d'un équipement est plutôt géré par **l'équipe technique de l'équipement**. On reste dans le cadre des procédures et pratiques habituelles de l'équipement (ex: utilisation du helpdesk de l'équipement ; l 'équipe technique peut ne pas installer un outil demandé par un utilisateur si trop spécifique, complexe, pas la compétence dans l'équipe technique).

Le support aux outils métiers et aux outils spécifiques à l'entité d'origine est plutôt géré par **l'équipe technique de l'entité d'origine de l'utilisateur**. L'équipe technique de l'entité d'origine est référencée dans le référentiel OPAL

Le support au développement est géré par **l'équipe technique de l'entité d'origine de l'utilisateur ou par la MSI**.

Comment un utilisateur fait-il remonter ses demandes de support ?
Réponse : par un ticket de support en suivant la procédure de l'équipement sur lequel il rencontre le problème (helpdesk de l'équipement).

Si l'équipe technique d'un équipement estime que la demande est du ressort d'une autre équipe technique (entité d'origine ou MSI), elle réoriente la demande de l'utilisateur.

7 - Les outils transverses à déployer

7.1 - Listes de diffusion

Les listes de diffusions suivantes doivent être créées :

- opal-admin@univ-cotedazur.fr : échange entre les équipes techniques des équipements de OPAL. Ne pas communiquer cette

adresse à des tiers risque de dérive rapide (demande de support hors helpdesk)

- opal-users@univ-cotedazur.fr : construite (et maintenue à jour) à partir du référentiel des accrédités. Elle permet de diffuser des informations aux utilisateurs OPAL. Liste modérée dans un premier temps, permettant uniquement une information descendante car contenant potentiellement un grand nombre d'abonnés

7.2 - Le référentiel

Le référentiel s'exécute sur une machine virtuelle hébergée :
- soit par un des membres qui gèrent les équipements OPAL (OCA, Mines ParisTech, Inria)
- soit par UCA (solution préconisée si possibilité)

Il est géré par les membres du comité technique OPAL.

Les autorités d'accréditation saisissent et mettent à jour les données du référentiel.

Dans un premier temps le référentiel OPAL n'est pas un référentiel d'authentification.
L'authentification sur les équipements se fait avec des comptes locaux.

7.3 - Le portail Web

Le « portail utilisateur commun OPAL » (ex: http://opal.univ-cotedazur.fr) est un portail Web qui s'exécute sur une machine virtuelle hébergée :
- soit par un des membres qui gèrent les équipements OPAL (OCA, Mines ParisTech, Inria)
- soit par UCA (solution préconisée si possibilité)

Il est maintenu à jour par les membres du comité technique OPAL.

Les informations du portail (charte, contacts, lien vers les helpdesks, liens vers les sites web des différents équipements) sont généralement accessibles en lecture depuis tout Internet sans authentification.
Les accès authentifiés (modification) sur ce portail web peuvent se faire via la fédération d'identités UCA.