Gestion et Réglages des ACLs dans onEye 0.8

Vous vous interrogez sur les Contrôles d'Accès dans onEye et n'êtes pas sûr de savoir comment les utiliser? Ne vous interrogez pas plus longtemps! Lisez ce qui suit.

Dans ce guide, nous allons voir comment utiliser les Listes de Contrôle d'Accès (ACLs) pour interdire l'accès à un programme installé, par défaut, sur tous les systèmes oneye, le Tableau public, ou Public Board. Nous allons créer une règle ACL puis l'appliquer à un utilisateur spécifique. Ensuite, nous verrons comment l'éditer et l'appliquer à un groupe d'utilisateur. Pour les besoins de ce guide, nous avons créé un utilisateur appelé User-Test et l'avons assigné au groupe appelé Groupe-Test.

Que sont les ACLs?

Les ACLs, de l'anglais "Access Control Lists", sont les Listes de Contrôles d'Accès qui permettent de définir certaines restrictions d'utilisation du système à des utilisateurs ou/et des groupes spécifiques.

Pourquoi utiliser les ACLs?

Si vous souhaitez éviter que vos utilisateurs effectuent certaines actions vous pouvez utiliser une ACL pour cela. Si vous désirez restreindre l'utilisation d'un programme, vous pouvez définir une ACL. Bien sûr, vous pourriez simplement supprimer le programme mais, alors, plus aucun utilisateur ne pourrait s'en servir. Les ACLs permettent d'affecter cette restriction à des utilisateurs spécifiques.

Important

Avant d'aller plus loin, assurez-vous que votre installation est à jour. À l'heure où nous rédigeons ce tutoriel, il y a eu quelques corrections des fonctionnalités de l'ACL sur lesquelles les paragraphes suivant s'appuient. Rendez-vous sur http://lars-sh.de/2011/09/22/how-to-download-the-latest-oneye-svn/ pour avoir les informations concernant le téléchargement et l'installation de la dernière révision svn.

Créer une règle ACL

Tout d'abord, identifiez-vous en tant que root. À l'heure actuelle, les ACLs ne peuvent être réglées que par l'administrateur du système, root.

Maintenant que vous êtes identifié, jetons un oeil à l'application que nous allons bloquer. Ouvrons-la pour en avoir un bon aperçu (figure 1). Le Tableau Public fournit un service de chat de style IRC à vos utilisateurs.

Figure 1

Veuillez toutefois noter qu'il n'est pas nécessaire que l'application soit lancée pour lui définir une règle ACL, vous pouvez donc la fermer. Par contre, il vous faut connaitre le nom de son package: il s'agit du nom réel de l'application contrairement l'étiquette plus conviviale lui est assignée dans l'interface utilisateur.

Sachant cela, ouvrez les Préférences Système.

Si nous cliquons sur "Contrôle d'accès" sous l'entête "Administration", nous pouvons voir toutes les ACLs du système (figure 2).

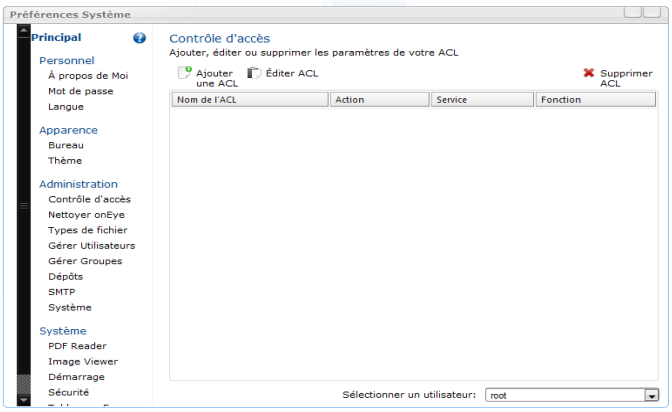

Figure 2

Pour créer une nouvelle ACL, choisissez "Ajouter une ACL". Vous serez en présence de 4 champs qui devront tous être remplie (figure 3).

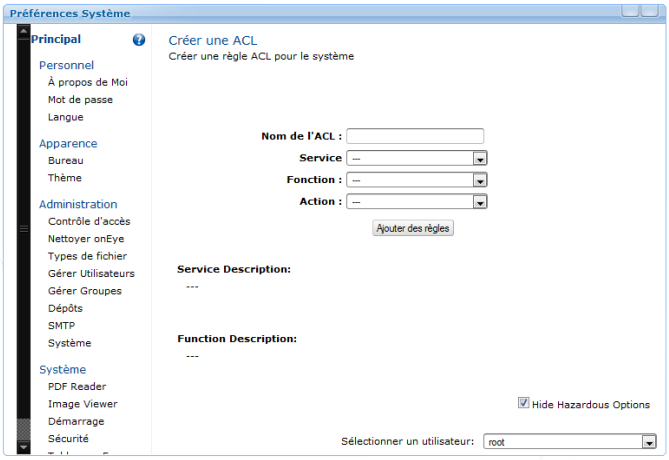

Figure 3

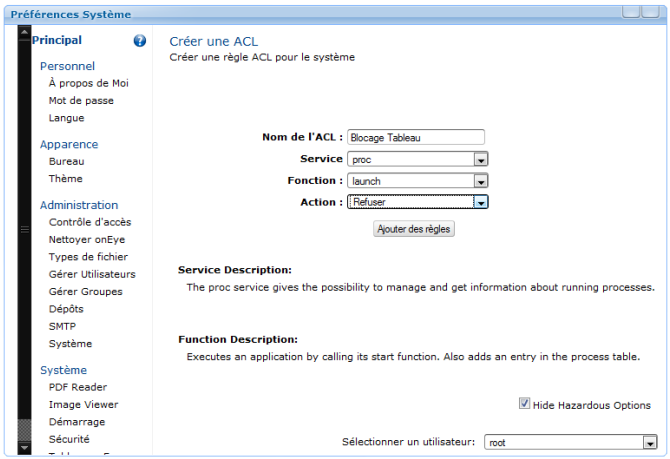

Figure 4

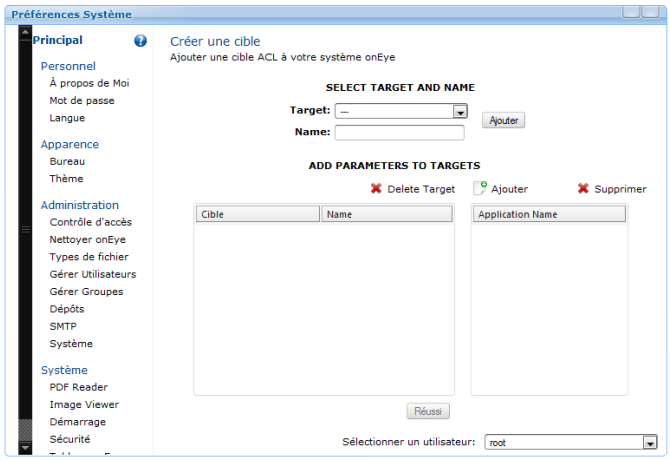

Figure 5

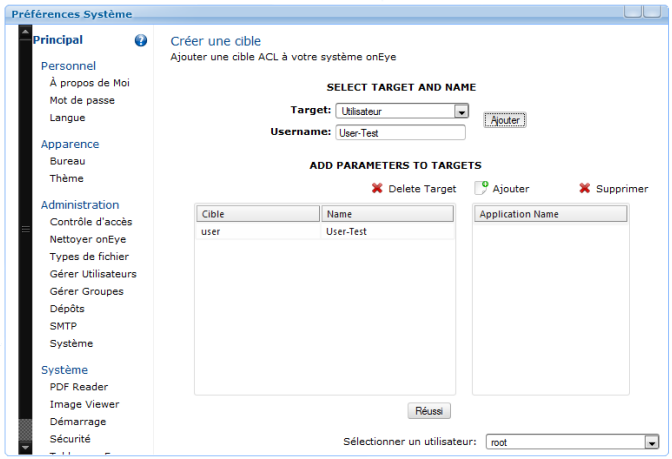

Figure 6

Dans le 1er champ, Nom de l'ACL, saisissez un nom pour votre ACL. C'est le nom que le système utilisera dans votre liste d'ACL, assurez-vous donc qu'il soit évocateur pour vous. Je vais nommer cette nouvelle ACL “Blocage Tableau”.

Le 2ème champ, Service, est une liste des services disponibles dans le système. Lorsque vous sélectionnez un service, une brève description vous est proposée. Pour notre exemple, sélectionnons proc.

Le 3ème champ, Fonction, adapte automatiquement son contenu selon le Service précédemment sélectionné car les fonctions diffèrent selon les services. Ici aussi, lorsque vous sélectionnez une option, une brève description vous en est proposée. Pour notre exemple, sélectionnons launch.

Le 4ème champ, Action, est un simple choix booléen: Autoriser ou Refuser. C'est à dire: voulez-vous d'autoriser ou refuser l'accès à la fonction précédemment choisie dans Fonction. Pour notre exemple, sélectionnons Refuser (figure 4).

Avant d'aller plus loin, nous aimerions attirer votre attention sur la case à cocher situé dans le coin inférieur droit. La plupart des fonctions sélectionnables sur cette page sont essentielles au fonctionnement d'onEye. Si elles sont refusées, cela pourrait causer de sérieux problèmes. Pour éviter que cela se produise par accident, ces fonctions particulières sont masquées par défaut. Décocher cette case les fera réapparaitre. Soyez très prudent avec cela.

Après avoir rempli les champs, sélectionnez Ajouter des règles.

Cibler un utilisateur

L'écran suivant (figure 5) présente plus d'options et celles-ci peuvent être un peu obscure.

Ces options vous permettent de cibler la règle sur quelqu'un, qu'il s'agisse d'un utilisateur ou un groupe. Sans ce ciblage, la règle serait assez inutile.

La 1ère option, Target, vous permet de choisir entre Utilisateur, Groupe et Admin. Pour notre exemple, sélectionnons Utilisateur.

Vous remarquerez que, comme vous avez choisi une option, l'étiquette de la boîte suivante a changé. Maintenant, affiche Username. Donc, saisissez le Nom de l'utilisateur auquel vous souhaitez appliquer la règle et cliquez sur Ajouter. Vous noterez qu'il est ajouté dans le tableau de gauche situé en dessous (figure 6).

À partir de ce moment, la règle est définie pour interdire le lancement de toutes les applications par l'utilisateur "User-Test". Cela inclut aussi les applications nécessaires au fonctionnement de base d'onEye. De ce fait, et parce que nous ne souhaitons interdire l'accès qu'à "eyeBoard", tournons-nous vers le tableau de droite. Comme son titre "Application Name" vous le laisse entendre, il s'agit de la liste des Applications à bloquer.

Pour créer un entrée, sélectionnez l'utilisateur précédemment ajouté dans le tableau de droite puis cliquez sur "Ajouter" situé au-dessus du tableau de droite. Une boîte de dialogue vous invite à saisir un paramètre. Ce 'paramètre' est le nom de package de l'application. Pour notre exemple, saisissons "eyeBoard" et cliquons sur Ajouter (figure 7).

Cela fait, cliquons sur Réussi et nous retournerons à la liste des ACL.

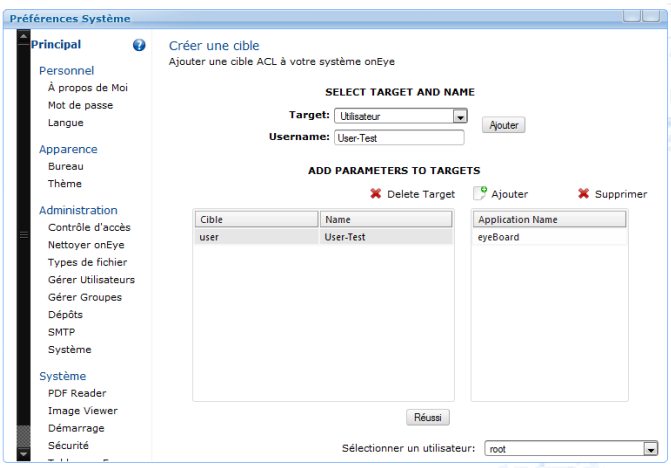

Figure 7

Tester la règle ACL

Testons! Fermez votre session pour revenir à l'écran de connexion. Cette fois-ci, connectez-vous en tant que l'utilisateur que vous avez précédemment ciblé (dans notre exemple, User-Test).

Une fois identifié, vous trouverez que tout fonctionne normalement... Jusqu'à ce vous tentiez de lancer le Tableau public: rien ne se passe, comme il se doit. Après tout, vous venez d'en refuser l'accès!

N'hésitez pas à vous connecter en tant que n'importe quel autre utilisateur pour vous assurer qu'aucun autre utilisateur ne se voit refuser l'accès au Tableau public, mais pour les fins de ce guide, nous allons passer à l'édition de la règle ACL.

Éditer une règle ACL

Que se passe-t-il si nous voulons éditer une règle ACL?

Identifions-nous à nouveau en tant que root et retournons à la liste des règles ACL.

Sélectionnons la règle ACL que nous voulons éditer puis cliquons sur Éditer ACL (figure 8).

Ici, nous pouvons renommer la règle dans "Nom de l'ACL" ou modifier la façon dont la règle Accepte ou Refuse la Fonction dans "Action". Comme nous n'avons besoin de faire ni l'un ni l'autre, nous allons plutôt choisir l'option "Edit Targets" (Éditer les cibles).

Un problème?

Un problème peut survenir. Si vous vous connectez avec succès, mais vous retrouvez face au papier peint sans dock ni icônes de bureau, vous avez dû oublier de mettre les paramètres pour la cible. Vous devrez supprimer votre cookie de session et rafraîchir la page manuellement. Cela vous ramènera à l'écran de connexion. Connectez-vous en tant que root et vérifiez votre règle ACL, modifiez-la et testez à nouveau.

Le programme fonctionne toujours

Si le programme fonctionne toujours veuillez commencer par vérifier que vous avez défini la règle correctement. Si cela ne fonctionne toujours pas, assurez-vous que vous utilisez un système à jour.

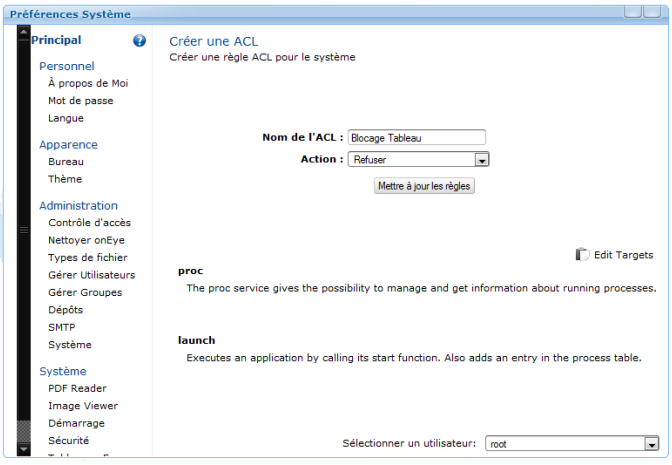

Figure 8

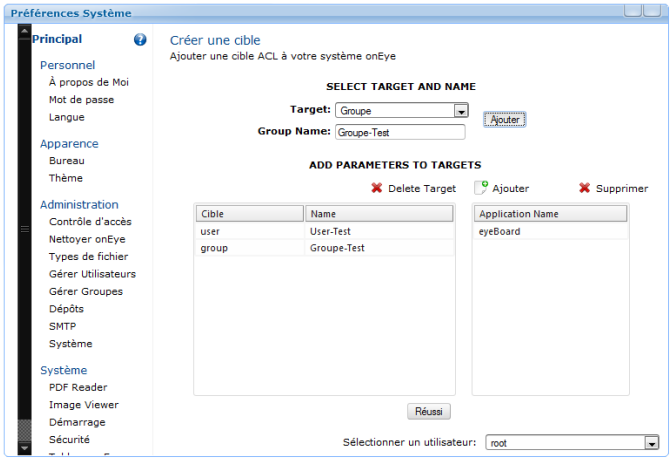

Figure 9

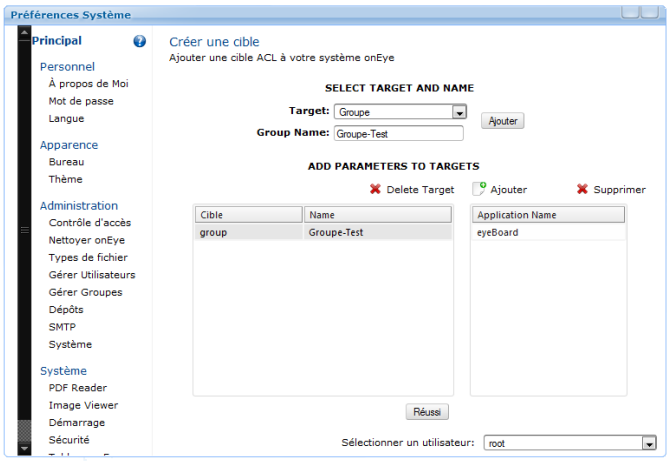

Figure 10

Une remarque à propos du Root

Ne vous inquiétez pas l'utilisateur root se trouve être un membre d'un groupe ciblé par une ACL - root est immunisé contre elle. Cela signifie également que de tenter de cibler spécifiquement le root en tant qu'utilisateur échouera également. C'est ainsi qu'il doit être et qu'il sera toujours.

Comment trouver le nom du package?

Le moyen le plus simple (mais pas le plus rapide) est, avec l'application fermée, d'ouvrir le Gestionnaire de Processus et d'aller à l'onglet Processus. Démarrer l'application qui vous intéresse et notez le Nom du processus de la ligne qui vient d'être ajouté (c'est généralement celle du bas, juste en dessous de eyeProcess).

Cibler un groupe

Depuis l'écran précédent, nous allons choisir "Groupe" dans le champ "Target". Le champ du dessous se renomme automatiquement "Group Name". Saisissons "Groupe-Test" et cliquons sur "Ajouter" (figure 9).

Ici, 2 choses sont à noter. D'abord nous avons toujours la cible "User-Test" que nous allons retirer en la sélectionnant puis en cliquant sur "Delete Target" (Supprimer la cible). Ensuite, si vous sélectionnez la nouvelle cible crée, vous noterez qu'elle n'a aucun paramètre défini sous "Application Name".

La raison de ceci est que vous pouvez utiliser la même fonction sur les différents utilisateurs et groupes, mais en spécifiant des paramètres différents pour chaque cible. (nous pourrions, par exemple, utiliser cette règle pour empêcher un autre utilisateur de lancer eyeNav tout en empêchant User-Test de lancer eyeBoard - User-Test pourra toujours exécuter eyeNav et l'autre utilisateur faire fonctionner eyeBoard).

Sachant cela, sélectionnons notre nouvelle cible, cliquons sur "Ajouter" et saisissons "eyeBoard" dans la boîte de dialogue qui s'affiche.

Après avoir vérifier que tout est comme nous le voulions (figure 10), cliquons sur "Réussi", et retournerons à la liste des ACL.

Tester la règle ACL

Testons! Sortons de la session root et identifions-nous comme un utilisateur appartenant au groupe "Groupe-Test": nous pouvons lancer n'importe quelle application sauf le Tableau public, comme nous le voulions.

Important

Soyez, SVP, très très prudent avec les ACLs. La plupart des fonctions susceptibles d'être bloquées sont essentielles pour le bon fonctionnement d'onEye. Si vous bloquez l'une d'elles pour un utilisateur, cela signifie qu'onEye sera incapable d'utiliser cette fonction - même en arrière-plan - lors de la session de cet utilisateur. Cela risquerait non seulement de perturber le fonctionnement d'onEye mais aussi d'affecter votre base d'utilisateurs.