

Spécification filtres d'identification

Spécification filtres d'identification

**

Auteur : Raymond Bourges (Université de Rennes1) (<http://http://www.raymond-bourges.fr>)

- [Spécification filtres d'identification](#)
- [Introduction](#)
- [Principe de fonctionnement](#)
- [Le filtre d'aiguillage](#)
 - [Classe](#)
 - [Paramètres](#)
 - [Mode de fonctionnement](#)
- [Le filtre d'identification Trusted](#)
 - [Classe](#)
 - [Paramètres](#)
- [Le filtre d'identification LDAP](#)
 - [Classe](#)
 - [Paramètres](#)
- [Le filtre d'identification CAS](#)

Introduction

Ce document a pour but de spécifier le mode de fonctionnement, à base de filtre J2EE, de l'identification des serveurs Slide et Cocoon utilisés dans le cadre d'Injac.

Principe de fonctionnement

On utilise une cascade de 4 filtres. Le premier d'entre eux sert uniquement à l'aiguiller vers les trois autres filtres. Ces trois autres filtres gèrent les différents modes d'identification du serveur. A savoir : LDAP, TRUSTED ou CAS. Les filtres utilisent log4j pour les logs. Les filtres vont chercher leurs paramètres directement dans le fichier web.xml de l'application conformément à la norme sur les filtres J2EE.

Le filtre d'aiguillage

Classe

- `org.esupportail.filter.AuthenticationRouter`

Paramètres

- `org.esupportail.filter.AuthenticationRouter.filterList` ** Obligatoire, valeur par défaut : aucune
 - Donne la liste des filtres d'identification (séparées par un espace) que le filtre d'aiguillage doit savoir gérer.
 - Ex : "TRUSTED LDAP CAS"
 - Dans la suite de ce document <NOM> représente un nom quelconque dans cette liste.
- `org.esupportail.filter.AuthenticationRouter.allowClientIP<NOM>` ** Non obligatoire, valeur par défaut : aucune
 - Donne la liste des adresses IP (séparées par un espace) des machines autorisées à se connecter via le filtre <NOM>
- `org.esupportail.filter.AuthenticationRouter.useSecureRequest<NOM>` ** Non obligatoire, valeur par défaut : false
 - Permet de savoir si l'on autorise l'utilisation du filtre <NOM> avec une connexion http ou https.
- `org.esupportail.filter.AuthenticationRouter.agent<NOM>` ** Non obligatoire, valeur par défaut : aucune
 - Donne une liste *d'expressions régulières - type PERL* (séparées par un espace) des types d'agent (clients http) autorisée à se connecter via le filtre <NOM>.
 - Ex : `(.)mozilla(.)`
- `org.esupportail.filter.AuthenticationRouter.httpRequestParameter<NOM>` ** Non obligatoire, valeur par défaut : aucune

- Donne une liste de paramètres de la requête http et de la valeur associée. La valeur associée prend la forme *d'une expression régulière - type PERL* et est séparé du paramètre par "=". Les différents éléments de la liste sont séparés par un espace.
 - Ex : "(.)*identLDAP=true(.)* (.)*ident=LDAP(.)*".
 - Le requête devra correspondre à au moins un de ces paramètres pour faire appel au filtre d'identification <NOM>.
- org.esupportail.filter.AuthenticationRouter.destinationHost<NOM> ** Non obligatoire, valeur par défaut : aucune
 - Donne une liste de noms de sites virtuels et du port associé à chacun. Le port associé est séparé du nom du site virtuel par ":". Les différents éléments de la liste* (expression s régulières - type PERL) *sont séparés par un espace.
 - Ex : "(.)*univ.fr:80(.)* (.)*localhost(.)*".
 - Le requête devra correspondre à au moins un de ces paramètres pour faire appel au filtre d'identification <NOM>.
- org.esupportail.filter.AuthenticationRouter.defaultAuthenticationFilter ** Non obligatoire, valeur par défaut : première entrée de org.esupportail.filter.AuthenticationRouter.filterList
 - Contient une des valeurs de org.esupportail.filter.AuthenticationRouter.filterList
 - Permet de définir le filtre à utiliser par défaut.

Mode de fonctionnement

- Positionne une variable session (org.esupportail.filter.AuthenticationRouter.selectFilter) qui peut une des valeurs de org.esupportail.filter.AuthenticationRouter.filterList.
- Cette variable session sera testée en début de chacun des filtres suivants pour savoir s'ils doivent opérer ou pas.
- Chaque filtre définit un wrapper de request pour redéfinir la fonction getUserPrincipal() et getRemoreUser()

Le filtre d'identification Trusted

Classe

- org.esupportail.filter.AuthenticationTrusted

Paramètres

- org.esupportail.filter.AuthenticationTrusted.TrustedPassword ** Non obligatoire, valeur par défaut : trusted
 - Donne une liste d'expressions régulières (séparées par un espace) des password autorisés pour se connecter en mode trusted.

Le filtre d'identification LDAP

Classe

- org.esupportail.filter.AuthenticationLDAP

Paramètres

- org.esupportail.filter.AuthenticationLDAP.connectionURL ** Obligatoire, valeur par défaut : aucune
 - URL du serveur LDAP principal
- org.esupportail.filter.AuthenticationLDAP.alternateURL ** Non Obligatoire, valeur par défaut : aucune
 - URL du serveur LDAP secondaire
- org.esupportail.filter.AuthenticationLDAP.bindType ** Non obligatoire, valeur par défaut : FASTBIND
 - Contient FASTBIND ou SEARCHBIND.
- org.esupportail.filter.AuthenticationLDAP.fastBindUserPattern ** Obligatoire si bindType=FASTBIND, valeur par défaut : aucune
 - Chaîne permettant de construire un DN LDAP à partir du nom de connexion. Exemple : uid=

Unknown macro: {0}

,ou=people,dc=univ,dc=fr

- org.esupportail.filter.AuthenticationLDAP.searchBindConnectionName ** Non obligatoire, valeur par défaut : aucune
 - Nom d'utilisateur pour lancer la recherche LDAP en cas de SEARCHBIND. Si le nom est vide cette recherche est faite en mode anonyme.
- org.esupportail.filter.AuthenticationLDAP.searchBindConnectionPassword ** Non obligatoire, valeur par défaut : aucune
 - Mot de passe de l'utilisateur qui lance la recherche LDAP en cas de SEARCHBIND.
- org.esupportail.filter.AuthenticationLDAP.searchBindBaseDN ** Obligatoire si bindType=SEARCHBIND, valeur par défaut : aucune
 - Base DN utilisée pour lancer la recherche LDAP. Exemple : ou=people,dc=univ,dc=fr
- org.esupportail.filter.AuthenticationLDAP.searchBindScope ** Obligatoire si bindType=SEARCHBIND, valeur par défaut : SUBTREE
 - Scope utilisée pour lancer la recherche LDAP.
 - Valeurs possible : SUBTREE, ONE, BASE
- org.esupportail.filter.AuthenticationLDAP.searchBindFilter ** Obligatoire si bindType= SEARCHBIND, valeur par défaut : uid=
- Cette fonction permet de construire un RDN LDAP à partir du nom de connexion. Exemple : uid=

Unknown macro: {0}

Le filtre d'identification CAS

Il s'agit ici en fait n'y plus ni moins du filtre CAS. A ceci près que :

- L'on a adapté le wrapper de request pour redéfinir la fonction getUserPrincipal()
- On teste en début de filtre la variable session org.esupportail.filter.AuthenticationRouter.selectFilter