

Projet SWITCH – Stream HPC

Intégration EXALEAD à la **3DEXPERIENCE**

PI6/Lot1/Stream HPC



3DEXPERIENCE®

Sommaire

1. Validation et historique des versions.....	3
Validation.....	3
Principaux changements.....	3
2. Périmètre du document.....	4
3. Introduction.....	5
3.1. Mashup Builder.....	5
3.2. 3DEXPERIENCE	5
3.3. Communication entre CloudView et 3DDashboard	5
4. Communication entre EXALEAD CloudView et 3DDashboard	6
4.1. Installation d'une application Mashup.....	6
4.1.1. Pré-requis.....	6
4.1.2. Installation du plugin 3DEXPERIENCE dans le Mashup Builder.....	6
4.1.3. Génération des Widgets UWA.....	7
4.1.4. Configuration du reverse proxy.....	7
4.1.5. Création de l'application Mashup dans le 3DDashboard	7
5. Administration 3DDashboard	9
5.1.1. Création du Rôle HPC 3DDashboard	9
5.1.2. Rattachement du Rôle HPC avec le Dashboard Portail HPC.....	9
6. Interactions entre les widgets.....	11
7. Sécurité.....	13
7.1. Authentification Utilisateur à partir du 3DPassport	13
7.1.1. Configuration du « Security Provider ».....	13
7.2. Ajout du certificat SSL 3DPassport à CloudView.....	14

1. Validation et historique des versions

Validation

Version	Date	Etat	Responsable	Relecteur	Approbateur
V1.0	22/08/2019	Terminée	Yohan CLECH LE	Xavier BUSSENAULT	Oussama ABDALA
V1.1	23/08/2019	Terminée	Yohan CLECH LE	Xavier BUSSENAULT	Oussama ABDALA
V1.1	02/09/2019	En cours	Yohan CLECH LE	Xavier BUSSENAULT	Oussama ABDALA

Remarques :

- Les états possibles sont « En cours », « Validé »
- Le responsable est l'architecte solution du stream/lot
- Le relecteur est le consultant métier du stream/lot
- L'approbateur est l'architecte solution global du programme

Principaux changements

Version	Description des évolutions
V1.0	Version initiale
V1.1	Version validée

2. Périmètre du document

Le présent document a pour objectif de décrire comment intégrer la solution EXALEAD dans la 3DEXPERIENCE via le 3D Dashboard pour le stream HPC. Il ne se substitue pas à la Spécification Technique HPC mais représente une préconisation d'intégration DS.

Ce document traite des sujets suivants :

Type du sujet	Intitulé	Date de publication	Cadrage
Introduction	Introduction	23/08/2019	Terminé
Communication	Communication entre EXALEAD CloudView et 3DDashboard	02/09/2019	Terminé
Administration	Administration 3DDashboard	02/09/2019	Terminé
Interaction	Interactions entre les widgets	23/08/2019	1D 2D Terminé
Sécurité	Sécurité	23/08/2019	Terminé

Si nécessaire mentionner les documents de références et les documents applicables.

3. Introduction

3.1. Mashup Builder

Le Mashup Builder EXALEAD permet de créer des applications de type « Recherche & Analytiques ». Il représente le Front End de la solution EXALEAD CloudView.

3.2. 3DEXPERIENCE

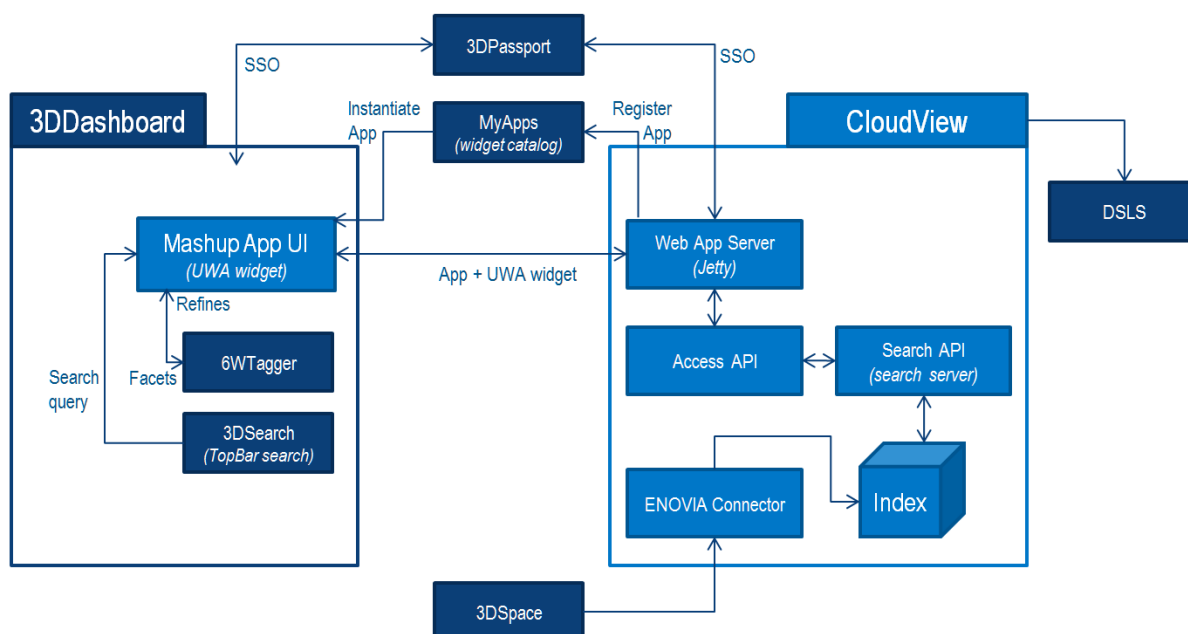
La plateforme 3DEXPERIENCE fournit de nombreux services collaboratifs à travers l'ensemble des applications Dassault Systèmes. Elle permet ainsi une expérience client unifiée unique.

Parmi ces services, on peut retrouver :

- 3DDashboard : Outil de création et d'administration de tableau de bord. Il fournit un ensemble de Widgets permettant d'accéder simplement aux informations gérées dans les différentes applications
- 3DSpace : Gestion de données et contenus simplifié et performant
- 3DSearch : Moteur de recherche de données aussi bien structurées que non structurées
- 3DPassport : Fournit un « single sign-on » pour tous les services/applications

3.3. Communication entre CloudView et 3DDashboard

Le diagramme ci-dessous présente comment les composants 3DEXPERIENCE (en bleu foncé) et les composants CloudView (en bleu clair) interagissent :



4. Communication entre EXALEAD CloudView et 3DDashboard

Il existe de 2 méthodes d'exposer les pages du Mashup dans le 3DDashboard :

- Via le Widget UWA : Intégration à travers une application Mashup CloudView
- Via le Web Page Reader : Redirige vers une page du Mashup (iFrame)

Dans le cadre du Projet HPC, la première méthode sera utilisée car elle garantit une intégration complète des pages du Mashup en incluant ses différents contextes (dont la sécurité).

Cette méthode est décrite dans la section suivante.

4.1. Installation d'une application Mashup

4.1.1. Pré-requis

Vous devez avoir accès au 3DDashboard avec les droits d'administration (n'importe quel utilisateur avec les droits d'administration dans le 3DSpace) afin de déclarer une nouvelle application.

4.1.2. Installation du plugin **3DEXPERIENCE** dans le Mashup Builder

Marche à suivre :

- Dans le Mashup Builder, sélectionner le menu « Application » en haut à gauche
- Sélectionner « Manage Component » puis cliquer sur « Plugins » [1]
- Cliquer sur « Upload plugin » [2]
- Une boîte de dialogue s'affiche, cliquer sur « Browse » puis sélectionner le plugin *experience-api.zip* [3]
- Répéter l'opération pour le plugin *experiment-ui.zip* [3]
- Redémarrer le « Search server process » comme demandé par l'application

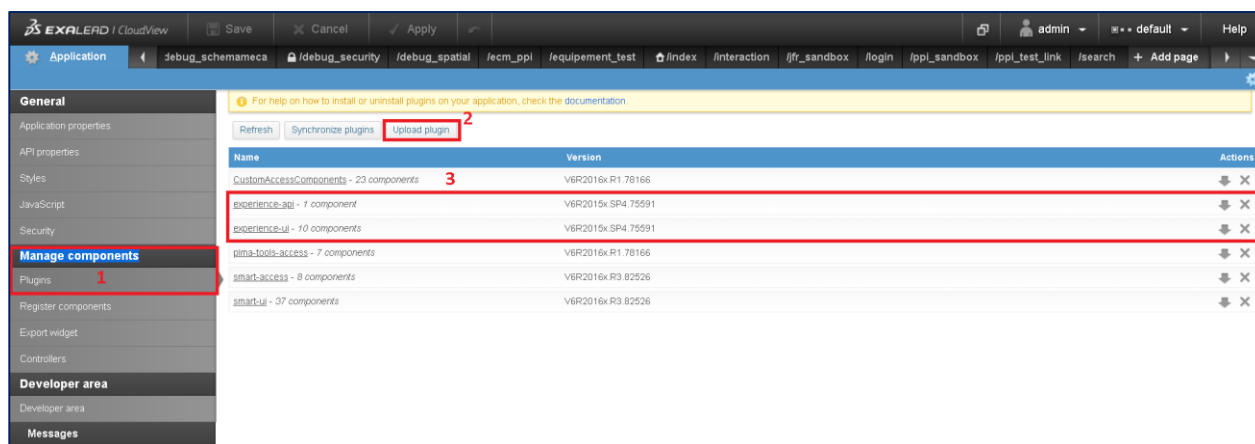


Figure 1 : Screenshot du Mashup Builder

4.1.3. Génération des Widgets UWA

Marche à suivre :

- Dans le Mashup Builder, sélectionner le menu « Application » en haut à gauche
- Sélectionner « Manage Component » puis cliquer sur « Controllers »
- Dans **3DEXPERIENCE** – Widget Builder :
 - Sélectionner « Enable »
 - Dans « Page prefix » :
 - Entrer « /page » si les pages sont accessibles via l'URL « .../page/[nom de la page] »
 - Laisser vie si les pages sont accessibles via l'URL « ...[nom de la page] »
 - Dans « Start Page », préciser la page du Mashup à afficher quand le Widget est lancé
 - Dans « Title », préciser le titre pour le Header du widget
- Cliquer sur « Save » puis « Apply » fin d'enregistrer la configuration

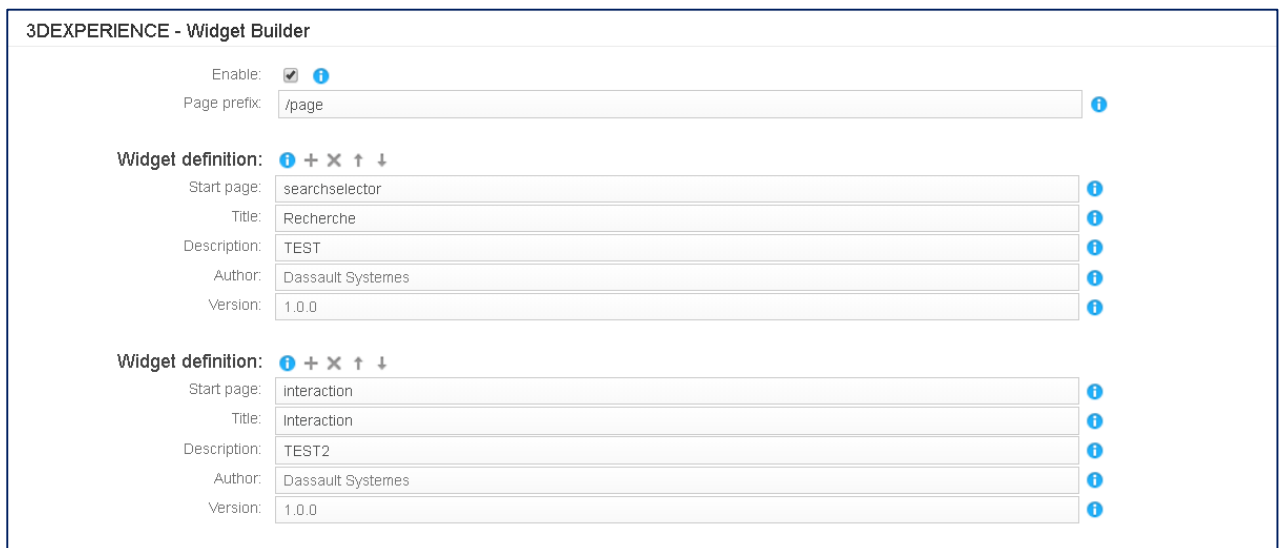


Figure 2 : Screenshot du paramétrage du 3DEXPERIENCE - Widget Builder

4.1.4. Configuration du reverse proxy

Marche à suivre :

- Se connecter en SSH avec le « root user » de la **3DEXPERIENCE**
- Editer le fichier reverse proxy httpd.conf sur l'host virtuel * :433
- Ajouter "ProxyPass /mashup-ui http://cloudview:port/mashup-ui"
- Ajouter "ProxyPassReverse /mashup-ui http://cloudview:port/mashup-ui"
- Ajouter le protocole HTTPS suivant : RequestHeader set x-forwarded-port "443"
- Redémarrer le reverse proxy

4.1.5. Création de l'application Mashup dans le 3DDashboard

Marche à suivre :

- Dans le **3DDashboard**, accéder au Dashboard « Platform Manager »

- Dans l'onglet « Members & Roles », accéder à la section « Third Party Apps » en bas de l'onglet
- Cliquer sur « Create Third Party Apps »
- Dans la pop-up :
 - Entrer le nom du Widget *Search & Display*
 - Spécifier le cadran du compass *My Information Intelligence Apps*
 - Sélectionner une icône pour le Widget
 - Sélectionner le type *Widget*
 - Entrer l'URL cible EXALEAD sous la forme suivante :
<https://HOST/mashup-ui/uwa/widget/homepage>
 - Cliquer sur Save

Afin de vérifier la création du Widget, vous pouvez vous rendre sur le compass dans le cadran *My Information Intelligence Apps* (cadran droit) et vérifier la présence de votre Widget Cuso.

5. Administration 3DDashboard

5.1.1. Création du Rôle HPC 3DDashboard

Une fois le Widget Custo EXALEAD créé, il est nécessaire de le lier à un rôle spécifique afin que tous les utilisateurs HPC ayant ce rôle puisse accéder en lecture au Portail HPC.

Marche à suivre :

- Dans le **3DDashboard**, accéder au Dashboard « Platform Manager »
- Dans l'onglet « Members & Roles », accéder à la section « Roles »
- Cliquer sur « Create Custom Role »
- Dans la pop-up :
 - Entrer le nom du role *ROLE_HPC*
 - Entrer la Description *Role for HPC User*
 - Cocher le Widget custom *Search & Display*

Créer un rôle personnalisé

Nom (s'affiche dans le Compass) *

ROLE_SMART

Icône du rôle

Description *

Rôle de SMART

Ajouter des applications à...

☒	Exalead - 1D	Type - Widget, disponible à tous les membres
☒	Exalead - Interaction	Type - Widget, disponible à tous les membres
☒	Hybrid Structure	Type - Widget, disponible à tous les membres

Enregistrer Annuler

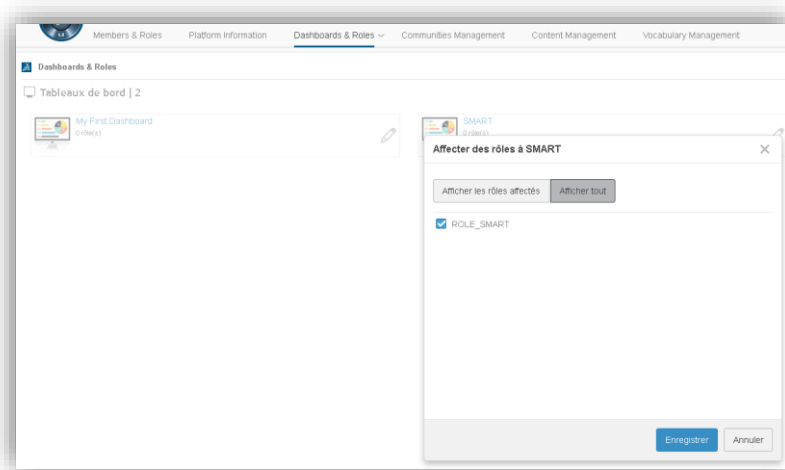
- Cliquer sur Save

5.1.2. Rattachement du Rôle HPC avec le Dashboard Portail HPC

Pré-requis : Dashboard Portail HPC & Rôle *ROLE_HPC* créés

Marche à suivre :

- Dans le **3DDashboard**, accéder au Dashboard « Platform Manager »
- Dans l'onglet « Dashboards & Roles », éditer le Dashboard *Portail HPC*
- Ajouter le rôle *ROLE_HPC*



- Cliquer sur Save

Une fois la manipulation effectuée, l'ensemble des utilisateurs ayant le rôle **3DDashboard HPC_ROLE** auront accès en lecture au Dashboard *Portail HPC*.

NB : Afin d'affecter le rôle **ROLE_HPC** en masse aux utilisateurs, il est possible de passer par des commandes serveur. Vous trouverez ci-dessous les commandes permettant d'effectuer cette affectation unitairement :

Commande 1 : Récupération de l'**ID technique** du rôle **ROLE_HPC**

```
list product RAP-* select title;
```

Résultat 1

```
product RAP-XXXXXXXXX
```

```
title = ROLE_HPC
```

Commande 2 : Affectation du rôle **ROLE_HPC** à l'utilisateur **YYY**

```
mod product RAP-XXXXXXXXX add person YYY;
```

6. Interactions entre les widgets

Afin d'assurer la communication et l'interopérabilité entre les widgets, plusieurs bus de données doivent être créés.

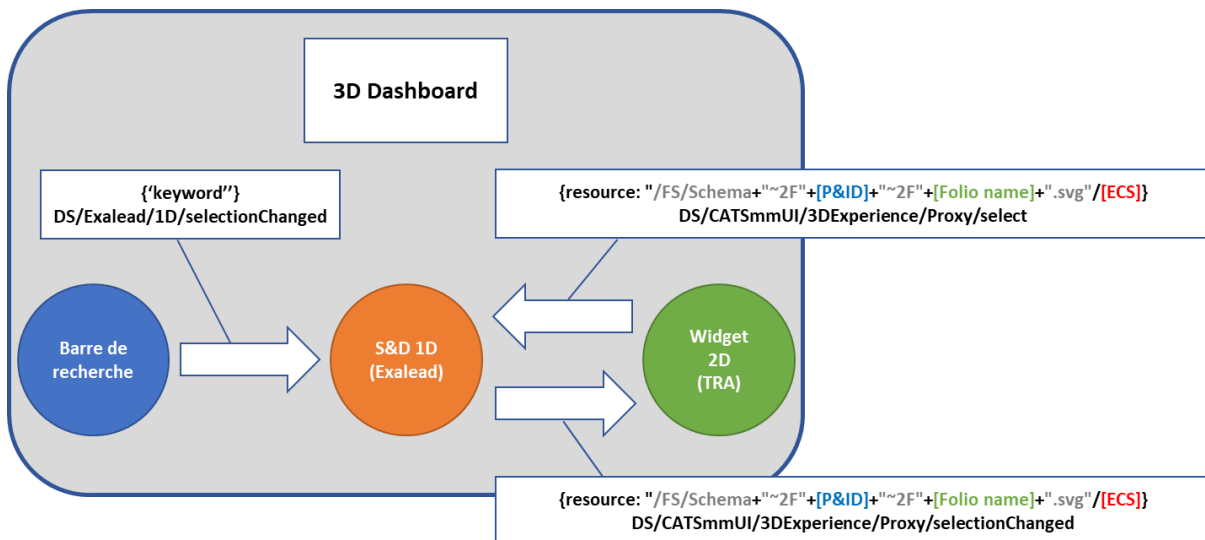


Figure 3 : Schéma des interactions Portail HPC

La communication par bus de données entre les Widgets est développée en Javascript en utilisant des fonctions du 3DDashboard.

Cette communication est divisée en 2 types :

1. Envoie du message depuis le Widget A dans le bus (Publish)
2. Réception du message par le Widget B à partir de l'écoute du bus (Subscribe)

```
// 3DDashboard - Utils
function subscribeTopic(topicName, callBackFunction) {
  parent.require(["DS/PlatformAPI/PlatformAPI"], function(PlatformAPI) {
    PlatformAPI.subscribe(topicName, function(data, eventObj) {
      console.log(location.pathname + " - Received message from topic : ");
      console.log(eventObj);
      callBackFunction(data);
    });
    console.log(location.pathname + " - Subscribed to topic : " + topicName);
  });
};

function publishToTopic(topicName, message) {
  parent.require(["DS/PlatformAPI/PlatformAPI"], function(PlatformAPI) {
    PlatformAPI.publish(topicName, message);
    console.log(location.pathname + " - Published message : " + JSON.stringify(message) + " to topic : " + topicName);
  });
};
```

Figure 4 : Exemple de fonctions de Subscribe/Publish

Ci-dessous la liste des topics :

- TOPIC_PUBLISH_TO_1D : Permet de notifier le Widget 1D avec la page de référence
- TOPIC_SUBSCRIBE_FROM_1D : Capte le message du Widget 1D
- TOPIC_PUBLISH_TO_2D : Permet de notifier le Widget 2D en cas de changement
- TOPIC_SUBSCRIBE_FROM_2D : Capte le message du Widget 2D

Ci-dessous un exemple de message envoyé par un Widget A (1D) vers un Widget B (Interaction) :

```
/mashup-ui/page/ci_equipement - Subscribed to topic : DS/CAT5mmUI/3DEXperience/Proxy/selectionChanged
/mashup-ui/page/ci_equipement - Subscribed to topic : SMT/HybridMockup/Equipment/selectedIn3D
/mashup-ui/page/ci_equipement - Published message : {"equipmentId":"CPY-JPT-001-BA"} to topic : DS/Exalead/1D/selectionChanged
```

Ci-dessous un exemple de réception de message par un Widget B (Interaction) :

```
/mashup-ui/page/interaction - Received message from topic :
» {channel: "Widgets", topic: "DS/Exalead/1D/selectionChanged", timestamp: Tue Jul 17 2018 10:13:20 GMT+0200 (Central European Summer Time), data: "{"equipmentId":"CPY-HK-0204-GS"}"}
Parsed equipmentId = CPY-HK-0204-GS
targetUrl = /mashup-ui/page/interaction?generic_equipment_id=CPY-HK-0204-GS
```

7. Sécurité

Les contrôles de sécurité se base sur l'infrastructure CloudView (« Security Providers » pour l'autorisation d'accès au Mashup et « Security Source » pour l'autorisation d'accès au serveur de recherche).

7.1. Authentification Utilisateur à partir du 3DPassport

Afin d'avoir une authentification utilisateur basé sur le mécanisme SSO du 3DPassport, il est nécessaire de configurer les « Security Source » dans le Mashup Builder et ensuite d'ajouter le certificat 3DPassport SSL au « CloudView trusted keystore ».

7.1.1. Configuration du « Security Provider »

- Dans le Mashup Builder, accéder au menu Application > General select Security
- Ajouter un « Security Provider »
- Sélectionner « CAS Security Provider »
- Dans la section « CAS Security Provider », configurer les paramètres suivants :
 - Authenticate to : Sélectionner *None*
 - Allow proxy ticket validation : Sélectionner *True*
 - CAS Server login URL : <https://HOST/3dpassport/cas/login>
 - CAS Server URL prefix : <https://HOST/3dpassport/cas>
 - CAS Server logout URL : <https://HOST:PORT/iam/logout>
 - Server Name : Entrer <https://HOST>
 - CAS Attribute(s) for displayName : Entrer *name*

CAS Security Provider

Uses standard CloudView security sources or CAS Single Sign On. If parameters are defined in CustomConfigs.xml, they replace this configuration.

API Config:	sapi0	i
API Endpoints:		i + x ↑ ↓
Command:	security	i
Source:		i + x ↑ ↓
Authenticate to:	NONE	i
CAS ticket validation filter:	Cas20	i
Allow proxy ticket validation:	true	i
CAS Server login URL:	https://3dpassport.smart-dev15.fr/3dpassport/cas/login	i
CAS Server URL Prefix:	https://3dpassport.smart-dev15.fr/3dpassport/cas	i
CAS Server logout URL:	https://3dpassport.smart-dev15.fr/3dpassport/cas/logout	i
Server name:	http://vmedfsmart05dsy.ux.dsone.3ds.com	i
CAS attribute(s) for displayName:	name	i

Remove security provider

Figure 5 : Screenshot du CAS Security Provider

- Dans la section page Mashup, sélectionner la check box correspondant à la page de recherche

Mashup pages

Enables the security on the following Mashup pages:

ci_affaire:	☐	ci_affaire_old:	☐	ci_equipement:	☐	ci_local:	☐	ci_tcdi:	☐	debug_3dmodel:	☐
debug_cartorad:	☐	debug_equipement:	☐	debug_export:	☐	debug_requirement:	☐	debug_schemameca:	☐	debug_security:	☒
debug_spatial:	☐	ecm_ppi:	☐	equipement_test:	☐	index:	☐	interaction:	☐	jfr_sandbox:	☐

Figure 6 : Screenshot du « Mashup pages »

- Cliquer sur « Save » puis « Apply » fin d'enregistrer la configuration

7.2. Ajout du certificat SSL 3DPassport à CloudView

Marche à suivre :

- Vérifier le format du certificat en utilisant la commande suivante :
openssl x509 -in <infile.cert> -text -inform <format>
→ Le format doit être DER ou PEM suivant les besoins
- Les clés privées sont généralement stockées dans des fichiers PEM encryptés. Il est nécessaire les convertir en fichiers non cryptés. Cela peut être réalisé en utilisant openssl via la commande suivante :
openssl pkcs8 -topk8 -in <key> -out <hostname>-<instance>.key -nocrypt
- Vérifier que le certificat est stocké en utilisant les caractères « Unix LF » en fin de ligne :
 - Sous Windows, l'outil suivant peut-être utilisé :
<http://www.thefreecountry.com/tofrodo/index.shtml>
 - Sous Unix, dos2unix peut être utilisé
- Surcharer la clé et les fichiers de certificat générés à la date d'installation dans ***DATADIR/security***. Si vous utiliser un alias, le nom de la clé privée doit utiliser l'alias et pas le défaut ***<hostname>-<instance>***. Cette étape doit être réalisée sur chaque instance. Les fichiers sont localisés dans :
 - Le certificat publique : ***DATADIR/security/<hostname>-<instance>.cert***
 - La clé privée : ***DATADIR/security/<hostname>-<instance>.key***
- Ajouter le certificat du server au « Truststore » sur chaque instance en utilisant la commande suivante :
keytool -import -file <.cert file (DER)> -alias <jetty> -keystore DATADIR/security/trusted.servers.ks -storepass <exalead>
- Redémarrer CloudView

NB : Voir « Securing your installation with HTTPS and SSL » dans la documentation CloudView pour plus de détails.