# Les modules SI5 et PPE2

## Description de la ressource

| Propriétés | Description |
|---|---|
| **Intitulé long** | Les modules SI5 et PPE2 |
| **Formation concernée** | BTS SIO |
| **Matière** | SI5 PPE2 |
| **Présentation** | Ce document présente une approche du module SI5 du BTS SIO en proposant un bornage des savoirs ainsi que des exemples d'activités pouvant être réalisées en parallèles en TP et dans le module PPE 2.<br><br>Ces propositions, cohérentes avec le référentiel du diplôme, sont fournies uniquement à titre indicatif, elles n'ont aucun caractère contraignant pour les enseignants qui peuvent choisir de s'en inspirer ou pas. |
| **Notions** | Les savoirs-faire du référentiel sont présentés dans la première colonne de ce document, des exemples de notions à aborder et de technologies à présenter sont cités dans la quatrième colonne. |
| **Outils** | Les outils sont laissés au libre choix des professeurs. |
| **Mots-clés** | SI5 PPE2 BTS SIO |
| **Auteur(es)** | Apollonie Raffalli, Éric Deschaintre et l'équipe SIO du réseau CERTA |
| **Version** | v 1.0 |
| **Date de publication** | Décembre 2011 |

# Les module SI5 et PPE2

*Ce document présente une approche du module SI5 du BTS SIO en proposant un bornage des savoirs ainsi que des exemples d'activités pouvant être réalisées en parallèles en TP et dans le module PPE 2.*

*Ces propositions, cohérentes avec le référentiel du diplôme, sont fournies uniquement à titre indicatif, elles n'ont aucun caractère contraignant pour les enseignants qui peuvent choisir de s'en inspirer ou pas.*

## SI5 - Support des services et des serveurs

Ce module permet de construire les savoirs et savoir-faire liés au support et au maintien en condition opérationnelle de services et de serveurs.

On entend par service tout composant logiciel participant au transport, au partage et au traitement de données numériques à travers un réseau.

**Remarques :**

- ce module reprend quasiment toutes les notions vues en SI1 (composants matériels et performances associées, architectures d'un système d'exploitation, applications, langage de commande, sauvegarde, etc) mais dans leurs spécificités côté "serveur" ;
- ce module s'appuie aussi sur les savoirs et savoir-faire du module SI2, en particulier en lien avec "Exploiter un service de base" ; ces notions sont reprises et mises en œuvre ici mais en se limitant aux **principes de base** car :
  - ➔ il s'agit d'un module commun,
  - ➔ ils seront largement approfondis en SISR3 pour la partie "services" et SISR4 pour la partie "systèmes"
- tous les services ne peuvent pas être décrits et étudiés en détail, aussi nous faisons ici le choix de mettre l'accent sur les services orientés utilisateurs "emblématiques" qui ont, de plus, déjà été rencontrés au premier semestre (comme le SGBD, le WEB ou le partage de fichiers) ;
- les services orientés réseau sont seulement décrits dans leur rôle car ils seront approfondis dans les modules de spécialité SISR de deuxième année.

## Le module PPE du deuxième semestre

À partir de différentes situations professionnelles définies par l'équipe pédagogique, ce module amène les étudiants à fournir (*c'est-à-dire maintenir en bon état de fonctionnement*) un service défini par un contrat de service.

Il place les étudiants en situation d'acteurs au sein du processus « P2 - Fourniture de services » afin d'assurer la maintenance d'un service, de répondre à des incidents et à des demandes d'assistance, d'identifier des problèmes et de proposer des pistes d'amélioration du service rendu.

Il invite à contribuer également au processus « P5 - Gestion du patrimoine informatique » avec pour objectif d'étudier une proposition de contrat de service sur les plans technique, financier et juridique.
Le travail demandé doit solliciter des compétences associées aux deux processus « P3 – Conception et maintenance des solutions d'infrastructure » et « P4 - Conception et maintenance des solutions applicatives » avec une dominante correspondant au parcours des étudiants concernés.

Ce module peut inclure des activités de type jeux de rôle permettant de travailler la communication professionnelle.

**Remarques** :

- les activités proposées ici (colonnes 2 et 3) ne sont ni obligatoires, ni exhaustives et ne sont pas décrites dans une logique de progression ;
- les activités proposées ici en PPE viennent en complément d'activités liées aux autres modules et être réalisées dans le cadre de projets ou missions ; aussi le contexte fourni peut inclure un contrat de service et l'**activité de PPE peut consister à vérifier la validité du service fourni au regard du contrat et procéder éventuellement aux corrections ;**
- les PPE ne sont pas nécessairement identiques pour tous pour tenir compte des acquis et de la spécialité de chacun ;
- les "savoirs associés" en italique pourront faire l'objet d'apprentissage directement en PPE aussi bien qu'en module de formation.

## Exemples d'activités et de technologies pour le module SI5 - Support des services et des serveurs -

| Savoir-faire tirés du référentiel | Activités possibles dans le cadre de travaux dirigés | Activités possibles dans le cadre des PPE | Exemples de notions à aborder et de technologies à présenter |
|---|---|---|---|
| **Caractériser** un service et le serveur associé | **À partir d'une observation du réel :**<br>• **décrire** la configuration matérielle d'une machine physique de type "serveur ",<br>• **décrire** les services qu'elle propose | **En observant le fonctionnement d'un service fourni et défini par un contrat de service** :<br>• **identifier** le matériel utilisé selon plusieurs critères définis (performances, budget, etc.),<br>• **justifier** ce choix à travers un argumentaire précis. | **Typologie des serveurs**<br>Architecture, composants matériels des serveurs et critères de performance (types de mémoire, nombre de processeurs, familles de puces, redondances de matériel, type de disques, boîtiers, etc).<br>**Mise en évidence** des différences entre serveur et STA (en gros, quelles différences entre la machine à 1 000 € et celle à 10 000 voire à 100 000 € ?) |
| **Justifier** le choix d'une solution technique | **À partir d'une documentation technologique ou d'une documentation technique fournie ou obtenue à partir d'une recherche documentaire en autonomie :**<br>• **recenser** les serveurs et leurs composants,<br>• **étudier** plusieurs configurations matérielles complètes,<br>• **comparer** les éléments matériels des différents types de serveurs | **Dans le cadre du contexte fourni et notamment du contrat de service** :<br>• **choisir** le matériel permettant le redimensionnement d'un serveur<br>• **justifier** le choix à travers un argumentaire précis. | **Typologies des services et des protocoles associés** : services rendus par le système d'exploitation (gestion du matériel, gestion des processus, gestion des utilisateurs, système de stockage, système de fichier), services orientés utilisateurs (SMTP, POP, HTTP, FTP, SGBD), services réseaux (DNS, DHCP), etc)<br>**Remarque** : la typologie des services orientés utilisateurs et réseaux (ainsi que leur rôle et les protocoles associés) a déjà été vue en SI2, il s'agit juste d'un rappel ici. |
| **Installer** un composant matériel et logiciel. | **À partir d'une procédure d'installation :**<br>• **ajouter ou participer à l'ajout** d'une unité de stockage (isolée ou en RAID), un onduleur, une alimentation redondante, une deuxième carte réseau, etc.,<br>• **installer** éventuellement le logiciel (et/ou pilote) associé au matériel,<br>• **configurer** le nouveau matériel,<br>• **tester** la performance et/ou le bon fonctionnement du matériel | **En analysant les dysfonctionnements d'un service fourni et défini par un contrat de service :**<br>• **choisir** une configuration matérielle mieux adaptée<br>• **installer ou participer à l'installation** d'une configuration matérielle,<br>• **configurer** le matériel<br><br>**À partir d'une procédure de tests (fournie ou élaborée par le groupe)**<br>• **tester** la performance et/ou le bon fonctionnement du matériel | **Procédure d'installation**.<br>**Typologie des tests** pour les serveurs<br><br>RAID – SCSI – Onduleur – Redondance matérielle<br><br>Gestionnaire de paquetage<br><br>**Outils de diagnostics.** |

| | | | |
|---|---|---|---|
| **Installer, configurer et administrer un** système d'exploitation<br><br>**Exploiter** les fonctions de base d'un langage de commandes. | **Configurer** et **administrer** un ou plusieurs systèmes d'exploitation déjà installés.<br><br>**À partir d'une procédure d'installation :**<br>**Installer** un système d'exploitation serveur sur une machine virtuelle ou réelle :<br>• **formater** un DD (technique classique et LVM – avantages et inconvénients),<br>• **installer** un ou plusieurs systèmes d'exploitation,<br>• **administrer** le système,<br>• **mettre à jour** le système | **En analysant l'architecture technique d'un service fourni et défini par un contrat de service :**<br>• **décrire** son implantation système (un système pour un serveur physique, un système virtualisé),<br>• **installer** éventuellement un nouveau système,<br>• **configurer** le système,<br>• **tester** les installations,<br>• **automatiser** la mise à jour du système et des applications,<br>• **documenter** l'installation<br><br>**Dans le cadre du contexte fourni :**<br>• **installer et/ou migrer** une machine virtuelle<br>• **sauvegarder** une machine virtuelle<br>• **exploiter** une machine virtuelle | **Architecture et fonctions générales** d'un système d'exploitation (gestion du matériel, gestion des processus, gestion des utilisateurs, système de stockage, système de fichiers…)<br><br>**Typologie des systèmes d'exploitation**<br><br>***Techniques de virtualisation*** *des serveurs (problématique différente de la virtualisation des STA, installation, sauvegarde et migration de machines virtuelles).*<br><br>**Techniques d'accès (simple et sécurisée) à un serveur à distance** (type d'accès à privilégier)<br><br>**Langage de commandes** (à privilégier : ne doit pas faire seulement l'objet d'un cours ou d'un TP mais on doit utiliser le langage de commande au quotidien). |
| **Gérer** les habilitations d'accès aux ressources d'un serveur et d'un service (accès locaux et distants) | **À partir d'un service déjà installé :**<br>**Observer** le comportement et la configuration d'un serveur d'authentification<br><br>**Installer, configurer et paramétrer** un serveur d'authentification ainsi que les utilisateurs et/ou les machines associées | **En analysant les habilitations d'accès à un service définies par le contrat de service :**<br>• **installer, configurer** et **paramétrer** un serveur d'authentification<br>• **gérer** les utilisateurs et/ou les machines et/ou les processus<br>• **gérer** les habilitations des utilisateurs et/ou les machines et/ou les processus à accéder aux ressources du système et/ou des services<br>• **tester** les habilitations | **Notions d'authentification** en différenciant authentification locale et authentification distante.<br>*Problématique liée à l'authentification multiple (sans pour autant forcément la résoudre)*<br><br>**Protocoles** associés à l'authentification (LDAP, Kerberos, etc.)<br><br>**Typologies des risques et des dispositifs de sécurité** liés à un service et à un serveur<br><br>**Typologie des habilitations** (utilisateurs, machines, processus - Système de droits et ACL) |
| **Installer**, **configurer** et **administrer** un service | **À partir d'un service déjà installé et/ou à partir d'un simulateur :**<br>**Observer** le comportement et la configuration par défaut du service | **En analysant l'architecture technique d'un service fourni et défini par un contrat de service :**<br>• **choisir** le(s) service(s) et protocole(s) réseau à installer<br>• **choisir** le(s) composant(s) logiciel(s) correspondant (s) | **Rôles**, **architectures** et **protocoles** associés aux principaux services orientés utilisateurs (SMTP, POP, WEB, FTP, SGBD, etc.)<br><br>**Rôle** des principaux services réseaux (DNS, DHCP, etc.). |

| | | | |
|---|---|---|---|
| | **À partir d'un mode opératoire fourni :**<br>• **installer** un service<br>• **procéder** à une configuration de base<br>• **tester** la configuration | • **installer** le(s) service(s)<br>• **configurer** le(s) service(s)<br>• **tester** le(s) service(s)<br>• **mettre à disposition** de l'utilisateur le(s) service(s)<br>• **documenter** l'installation et la configuration (du serveur et des clients)<br>• **rédiger** éventuellement un mode opératoire pour un service orienté utilisateurs | **Architecture d'un service** : fichiers de configuration, fichiers de données, comptes systèmes associés, fichiers d'activité (logs), protocoles associés. On se limite à quelques services orientés utilisateurs pour une description détaillée.<br><br>**Outils d'analyse et de tests** de bon fonctionnement (trame, scanneur de port, fichiers d'activités, commandes et outils divers associés aux services et processus, etc) |
| **Mettre en œuvre** un protocole sécurisé associé à un service | **À partir d'un mode opératoire fourni :**<br>• **créer** des paires de clés,<br>• **déposer** des clés notamment sur un serveur de clés,<br>• **récupérer** des clés notamment sur un serveur de clés,<br>• **gérer** des clés,<br>• **exploiter** les clés (configuration d'un serveur SSH, chiffrement et signature de méls, chiffrement de fichiers)<br><br>**À partir d'un mode opératoire fourni :**<br>• **créer** des certificats,<br>• **gérer** des certificats<br><br>**À partir d'un service non sécurisé déjà installé et configuré (HTTP par exemple) et d'un mode opératoire fourni :**<br>• **configurer le service** avec un protocole sécurisé<br>• **configurer l'accès** au service sécurisé<br>• **tester** le bon fonctionnement | **En analysant les contraintes de sécurité définies dans un contrat de service :**<br>• **installer** les composants nécessaires à la mise en œuvre d'un protocole sécurisé<br>• **configurer** un service avec un protocole sécurisé<br>• **configurer l'accès** au service sécurisé<br>• **tester** le bon fonctionnement | **Typologies des risques et des dispositifs de sécurité** liés à un service et à un serveur<br><br>**Le chiffrement** :définition, méthodes (symétrique et asymétrique – notions de clé publique et clé privée), objectifs (confidentialité et intégrité des données, authentification et non-répudiation – notions de signature électronique et d'horodatage) - algorithmes de chiffrage et de hachage<br><br>**Le certificat** (définition, rôle, formes, autorités de certification, etc.)<br><br>**Typologie des protocoles** sécurisés et services associés |

| | | | |
|---|---|---|---|
| | **À partir d'un analyseur de trame**<br>• **comparer** les trames échangées quand un service est non-sécurisé avec celles quand le service est sécurisé | | |
| **Installer** une solution de sauvegarde et de restauration des données. | **À partir d'un mode opératoire fourni :**<br>• **Installer** et **configurer** une solution de sauvegarde des données<br>• **Sauvegarder** des données<br>• **Restaurer** des données | **En analysant les contraintes de continuité d'un service à fournir définies dans un contrat de service :**<br>• **installer** et **configurer** un outil de sauvegarde et de restauration<br>• **appliquer une procédure** de sauvegarde<br>• **en guise de test, appliquer une procédure** de restauration<br>• **automatiser** une sauvegarde<br><br>**En fonction de différents critères (taux de transfert, volume de données, etc) :**<br>• **choisir** un système de sauvegarde<br>• **justifier** son choix | **Typologie des données à sauvegarder** : (données utilisateurs, données d'un service, données de configuration du système)<br>==> Solutions de sauvegarde des données d'un serveur (y compris externalisation). On se limite ici à la sauvegarde des données.<br><br>**Types de sauvegarde** (totale, incrémentielle, différentielle) a probablement déjà été vu en SI1, auquel cas il s'agit juste d'un rappel ici.<br><br>**Typologies des risques et des dispositifs de sécurité** liés à un service et à un serveur<br>==> Différencier les types de sécurisation (différences entre sauvegarde et disponibilité ==> par exemple différence entre sauvegarde et utilisation d'un système RAID)<br><br>Matériel associé aux solutions de sauvegarde (robot de sauvegarde, NAS, SAN, etc) |
| **Valider et documenter** un service | | **En observant le fonctionnement d'un service fourni définit par un contrat de service :** (mais pas forcément conforme au contrat de service) **:**<br>• **vérifier** la conformité du service fourni<br>• **rédiger** le rapport correspondant<br>• **procéder** éventuellement aux corrections nécessaires<br><br>**Remarque** : cette activité a sa place au niveau de **chaque savoir-faire.** | *Notions sur le contrat de service*<br><br>*Méthode pour vérifier la conformité d'un service à un contrat* |

# Exemple d'un service orienté utilisateurs : une application WEB

## Remarques préalables

Le choix fait ici d'une application web s'appuie sur le fait qu'il s'agit d'un service emblématique du métier qui aura probablement été abordé au premier semestre.

Ce service rendu aux utilisateurs s'appuie sur des services réseaux comme le service DNS. Le rôle de ces services est explicité autant que nécessaire en fonction de la progression choisie par l'enseignant.

La recherche de complémentarités entre les deux parcours plaide pour que ce service soit étudié en parallèle ,du point de vue développeur, en SI6 afin de pouvoir placer les étudiants des deux parcours sur des projets communs en PPE.

## En SI5

- Installation par le professeur dans le laboratoire informatique d'une application web opérationnelle. Il peut s'agit d'un logiciel *open source* donnant accès à son code et/ou permettant de développer des modules spécifiques (CMS Joomla, Drupal.., logiciel de gestion OpenConcerto, OpenERP, logiciel de gestion de parc, etc...)
- Présentation par le professeur du contrat de service contenant : son utilité pour une organisation client, la description des utilisateurs concernés, leur rôles et leurs habilitations, les cas d'utilisation qui seront étudiés, les conditions de performance et de sécurité du service fourni.
- Description de l'architecture de l'application web et des protocoles associés :
  - ➔ observation (comportement et fichier de configuration) à partir d'un service déjà installé
  - ➔ analyse de trame, etc
- Installation du service (par exemple Apache ou IIS) sur un système serveur Linux ou Windows
- Configuration et/ou analyse de la configuration du service :
  - ➔ comprendre le paramétrage par défaut et mettre en ligne un premier site WEB
  - ➔ configuration de base (alias, serveur web pour chaque utilisateur, serveur virtuel, etc...)
  - ➔ une première gestion des logs (en cas de problème au niveau de la configuration, pages visitées, nombre de connexion, utilisateurs rejetés, etc...)
- Analyse et mise en œuvre des conditions d'authentification des utilisateurs (qui a le droit de se connecter à quoi ?) → simple en SI5 (par exemple fichiers "htaccess" ou utilisation d'un serveur d'authentification déjà installé et configuré)
- Analyse et mise en œuvre des conditions d'authentification du serveur et cryptage des échanges (assurer au client l'identité valide du serveur + chiffrement des échanges) → privilégier, dans la mesure du possible, une application qui nécessite de configurer le protocole HTTPS)
- Observation, éventuellement, d'une architecture n tiers avec SGBD déporté sur un autre serveur

## En PPE2

Le service étudié en cours et en TP dans le module SI5 peut également servir de support à la réalisation de projets dans le cadre du module PPE2. Voici quelques thèmes de projets possibles :

- Rédiger la documentation utilisateur du service
- Rédiger la documentation technique du service
- Rédiger un rapport d'audit du service en vérifiant point par point sa conformité au contrat de service
- Prendre en charge tout ou partie de l'installation du service (sur d'autres équipements)
- Assurer une présentation orale du service du point de vue de l'utilisateur (fonctionnalités, usages) et du point de vue de l'informaticien (architecture, technologies)
- Jeu de rôles "dépannage" à trois équipes : une première équipe dégrade intentionnellement le service rendu en veillant à la réversibilité de cette dégradation et en notant précisément ce qui a été

dégradé et comment ; une deuxième équipe audite le service et note les manquements ou les dysfonctionnements en adoptant le point de vue des utilisateurs ; elle rapporte ses constatations à une troisième équipe ; à partir des indications de la deuxième équipe, la troisième équipe est chargée de restaurer le fonctionnement nominal du service tel qu'il est prévu dans le contrat de service. On peut prévoir que la première équipe observe la deuxième et prenne note du déroulement des opérations, ceci permet de faire éventuellement un compte rendu en cours pour illustrer les apports sur les stratégies de détection et de correction de pannes.

- Restituer le schéma de tout ou partie de la base de données ; repérer où sont enregistrées certaines informations
- Étudier tout ou partie d'un module de l'application ; expliciter son rôle
- Jeu de rôle "formation" : un étudiant joue le rôle d'un formateur chargé d'expliquer le fonctionnement et l'architecture technique du service à ses collègues. Ceci peut être utile notamment si différentes applications web sont proposées à différents groupes d'étudiants.
- À partir d'un besoin utilisateur (un forum, un wiki, une FAQ, un besoin de gestion, un besoin de communication) faire une étude des solutions *open source* existantes et rédiger un document qui présente les solutions en les comparant sur différents critères ; étudier la pertinence et le coût d'un développement spécifique intégral ou adapté à partir d'une solution *open source* existante.

## Proposition de bornage

- Il peut ne pas être nécessaire de détailler chaque service ou protocole réseau dans la mesure où ceux-ci pourront être approfondis plus tard
- On peut rester sur des configurations de base

## Approfondissements possibles dans les semestres 3 et 4

À titre indicatif, est décrit ci-après un approfondissement possible en deuxième année :

- **Exploitation du service en SISR3**
  - ➔ Approfondissement de la sécurisation
    - ✔ authentification des utilisateurs (installation et configuration d'un service d'authentification spécifique ou d'un système d'authentification unique : SSO)
    - ✔ authentification du serveur et cryptage des échanges (assurer au client l'identité valide du serveur + chiffrement des échanges) --> configuration d'une Infrastructure à clé publique
  - ➔ Administration du service : gestion des logs, mise à jour du service, surveillance du service, résolution des problèmes, etc
  - ➔ Gestion de la qualité du service WEB : contrôler (tester la montée en charge – par exemple avec jmeter), gérer et améliorer les performances du service WEB (répartition de charges – par exemple avec le module d'apache mod_proxy_balancer, configuration poussée pour des performances maximales)
  - ➔ Gestion de la continuité du service WEB : outils mis en place à l'avance afin de gérer des situations de crise selon la stratégie du plan de reprise ; par exemple :
    - ✔ mise en place d'une haute disponibilité si le service est critique (par exemple : deuxième serveur avec le service installé dans les mêmes conditions de sécurité et de qualité en capacité de prendre le relais automatiquement si le service tombe) ;
    - ✔ sauvegarde + restauration si le service est non critique ;
    - ✔ tests réguliers du plan de reprise.

- **Exploitation de l'application WEB étudiée en SI5 et SI6 dans le module SI7 des semestres 3 et 4.**
  - ➔ Étude et comparaison des différents outils de mise à disposition de page web et de mise en production du service
  - ➔ Étude de l'impact de l'intégration du service sur le système informatique (dont l'impact financier de la consommation du service)
  - ➔ Test d'intégration et d'acceptation de la nouvelle application web
  - ➔ Accompagnement de la mise en place du nouveau service