Les modules SISR de deuxième année

Description de la ressource

Propriétés	Description
Intitulé long	Grille de lecture des modules SISR3 SISR4 et SISR5
Formation concernée	BTS SIO
Matière	SISR3 SISR4 et SISR5
Présentation	Ce document présente une aide à la compréhension des modules SISR3 SISR4 et SISR5 avec des propositions non détailles de progression. 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.
Outils	Les outils sont laissés au libre choix des professeurs.
Mots-clés	SISR3 SISR4 SISR5 BTS SIO services qualité sécurité continuité
Auteur(es)	Roger Sanchez (avec l'aide précieuse d'Apollonie Raffalli et la relecture avisée d'Alain Van Sante et Fabio Pasqualini)
Version	v 1.1
Date de publication	Juin 2012

1 - Préalables

Comme en première année, les modules se veulent opérationnels :

- Les modules d'enseignement sont orientés compétences (une compétence est construite sur des savoirs et des savoir-faire) ;
- les modules participent à la construction progressive de compétences techniques exploitant des concepts compris : on n'enseigne pas de mode opératoire ;
- on n'enseigne pas des savoirs académiques (la sécurité en générale, la haute disponibilité, la sauvegarde, etc.) : pour construire les compétences, les modules s'appuient toujours sur des objets métiers (la sécurité d'un système serveur, la sécurité mise en œuvre sur un élément d'interconnexion réseau, la sécurisation d'un service, la continuité de service d'un serveur, la haute disponibilité d'un service, la qualité d'un service, etc.) ; chaque concept est donc, en règle générale, abordé dans chaque module ;
- qualité, sécurité et continuité doivent être vus comme des objectifs à atteindre sur chaque objet d'étude (serveurs, services et infrastructures réseaux) à partir d'actions précises (exploitation, administration, supervision) ;
- les compétences techniques construites dans les modules SISR sont mobilisées en PPE dans des situations complexes (les contextes) afin d'aboutir aux compétences professionnelles attendues.

2 – Compréhension des modules SISR deuxième année

SISR3 – Qu'est ce qu'un service ?

Il est important de bien comprendre le concept de service comme « **service perçu par l'utilisateur** » et non comme un service au sens technique d'un processus serveur.

Prenons un exemple simple (et provocateur ;-)), l'accès à internet.

« Accéder à la ressource internet » c'est le service perçu par l'utilisateur, mais pour un administrateur réseau ce service peut se décomposer ainsi :

- un FAI ;
- un routeur ADSL ;
- un Proxy (habilitations, filtrage de site, logs …) ;
- un DNS ;
- la bande passante nécessaire et la priorité associée (VLAN ?, QOS ? …) ;
- le mode d'accès à la ressource Internet (filaire, WIFI, fixes, mobile, smartphone, tablette, etc.) ;
- l'adressage permettant la sortie vers Internet (DHCP, NAT) ;
- le contrôle de l'activité en sortie (logs, problèmes juridiques associés, archivage des logs…) ;
- le contrôle de l'activité en entrée (filtrage, anti virus …) ;
- l'administration sécurisée locale ou distante des éléments participant au service.

On doit pouvoir répondre aux types de questions suivants :

- Pourquoi l'accès à Internet « rame » ?
- Pourquoi ne suis-je pas autoriser à aller sur internet, ou sur certains sites ?
- Qui a accédé à tel site tel jour ?
- etc.

La perception du service par l'utilisateur donne une cohérence et un sens à ce qu'on fait.

C'est parce qu'on veut fournir l'accès à la ressource Internet qu'on met en place, qu'on utilise ou qu'on modifie une solution d'infrastructure.

Il ne faut donc pas confondre services techniques, (nécessaires par ailleurs, avec le service rendu à l'utilisateur.

Ainsi dans l'exemple précédent DNS, DHCP sont des services techniques mais en aucun cas des objets d'étude particuliers pour SISR3 ; ce sont des services orientés réseau qui ont plutôt vocation à être étudiés (ou approfondis) en SISR5.

On peut bien sûr imaginer un service DNS qui fasse du « round robin » pour répartir la charge sur des services perçus par l'utilisateur, mais ce n'est que la conséquence de la mise ne place du service perçu et non l'objet principal d'étude.

Dans la même ligne d'idée, pour accéder à ce service on traverse un ensemble d'éléments d'interconnexion installés (commutateurs, routeurs, etc.), configurés et optimisés en SISR5 (car objets principaux d'étude dans ce module).

Pour préciser encore cette approche, on considère que la téléphonie sur IP est un service perçu par l'utilisateur (le téléphone) alors que l'accès Wifi est un moyen d'accéder à un service. Donc on étudiera plutôt la VOIP dans SISR3 et le Wifi dans SISR5. Ceci est bien sûr discutable.

Le positionnement des Modules SISR de deuxième année

SISR3 se situe clairement dans le *front office* alors que SISR4 et SISR5 se situe dans le *back office*.

La cohérence est donnée par l'objet d'étude : le service, le système et le réseau. Il y a forcément des éléments communs à chaque module mais l'approche de ceux-ci est différente.

L'activité métier principale associée à chaque module

Le choix du nom des modules repose évidemment sur la volonté d'utiliser les termes emblématiques du métier mais oriente aussi les enseignements.

Exploitation ➔ On insiste sur le respect d'un contrat de service explicite ou implicite. Le service est rendu, il fonctionne selon un contrat de service explicite ou implicite, il est contrôlé et un dysfonctionnement quel qu'il soit (panne, dégradation, sécurité, etc.) doit être pris en charge sous peine de ne plus rendre le service prévu dans le contrat.

Ceci implique une certaine expertise technique du service, une compréhension de son fonctionnement, la mise en place d'outils de mesure et de contrôle de l'activité, des solutions de continuité de service et de reprise d'activité en cas d'arrêt de fonctionnement.

Administration ➔ On insiste sur l'administration des éléments systèmes utilisés par l'ensemble des services. On fournit l'infrastructure mutualisée technique et administrative nécessaire à l'exécution et à l'utilisation des services perçus par l'utilisateur. Il s'agit de la gestion centralisée

- des solutions techniques d'accès ;
- des supports de stockage ;
- des habilitations ;
- des serveurs supportant l'ensemble des services techniques ;
- des éléments communs de qualité de service, de continuité de service et de sécurité ;

L'administration système mutualise les ressources systèmes utilisés par les services perçus par les utilisateurs.

Un dysfonctionnement à ce niveau n'est perçu que s'il a des conséquences directes sur un service utilisateur. Il ne sera jamais signalé par l'utilisateur comme se produisant à ce niveau.

Supervision ➔ On insiste sur le contrôle de l'activité réseau. L'infrastructure réseau (c'est-à-dire l'ensemble des éléments d'interconnexion permettant un accès aux services perçus par l'utilisateur) est opérationnelle et doit être contrôlé. On a mis en place les éléments permettant de vérifier l'activité « normale » et « anormale ». On a mis en place des solutions de continuité de service, de qualité de service et de sécurité.

La supervision des réseaux mutualise les ressources « réseaux » utilisés par les services perçus par les utilisateurs.

Un dysfonctionnement à ce niveau n'est perçu que s'il a des conséquences directes sur un service utilisateur. Il ne sera jamais signalé par l'utilisateur comme se produisant à ce niveau.

L'interdépendance des modules

Les systèmes et le réseau n'ont d'intérêt que par rapport aux services qu'ils supportent mais aucun service ne peut-être rendu sans une administration système et réseau performante et rigoureuse.

SISR3 demande des services abordés en SISR4 (en matière de support serveur) et en SISR5 (en matière de connexion réseau), on peut donc mettre en place des stratégies pédagogiques communes sans exclure une relative autonomie de chaque module.

SISR3 VS SISR4 : tout ce qui est mutualisé par les systèmes est approfondi et détaillé par SISR4. Ça n'empêche bien sûr pas SISR3 de mobiliser des savoirs et savoir faire SISR4 mais toujours en relation avec un service. Au démarrage du module la connaissance des systèmes donnés par SI1, SI5 et SISR1 doit suffire.

SISR3 VS SISR5 : tous les éléments d'interconnexion et leur supervision sont vus dans SISR5. Encore une fois SISR3 utilise des éléments d'interconnexion (et on peut être amené à en configurer dans ce module) mais ce n'est pas un objet d'étude. La connaissance du réseau donnée par SI2, SISR1 et SISR2 doit suffire.

SISR4 VS SISR5 : SISR5 se préoccupe des éléments d'interconnexion mais utilise forcément des services techniques associés à des systèmes (autorité de certification, RADIUS, etc.) de la même manière que les serveurs et les solutions techniques d'accès sont connectés au réseau via des éléments d'interconnexion.

L'interdépendance ne doit pas constituer un frein. Il faut voir chaque module comme un ensemble cohérent et autonome même si on peut étudier des progressions communes cohérentes. Si on utilise par exemple une autorité de certification dans SISR5, on a deux solutions : soit elle a déjà été vue dans SISR4 (surtout) ou SISR3 et dans ce cas on ira plus vite soit elle n'a pas été vue, et on voit alors dans le module les éléments nécessaires à l'objectif fixé.

Un autre exemple est le système de log : il est théoriquement défini, installé et configuré en SISR4 et utilisé par les services en SISR3, voire par l'infrastructure en SISR5. Mais si le système n'a pas été configuré en SISR4 ou s'il n'est pas adapté, rien n'empêche de l'installer et de le configurer dans les autres modules.

Techniquement chaque module doit pouvoir progresser de façon indépendante. Par exemple, autant que faire se peut, SISR3 disposera de ses systèmes et gérera le matériel d'interconnexion nécessaire.

Les éléments communs

Les services, les systèmes et les réseaux doivent pouvoir être contrôlés localement ou à distance de façon sécurisée.

Il y a forcément des concepts et des éléments techniques communs à la réalisation de cela (les VPN notamment). Encore une fois, on ne bloque pas la progression dans les modules dans l'attente d'un

autre module. Même si on peut considérer que les VPN sont davantage du ressort de SIR4 ou SISR5 ; de toute façon ces modules n'en feront pas un tour exhaustif, et le VPN devra donc être vu aussi dans SISR3 en relation avec un service.

Pour continuer sur cet exemple, c'est cette approche qu'il faut privilégier : généralités ou rappels sur les VPN, puis VPN adapté à l'objectif dans le module considéré.

De même un certain nombre de services techniques comme les autorités de certification, les annuaires, DNS ou encore DHCP sont nécessaires à chaque module et seront donc utilisés et configurés dans chaque module.

D'un point de vue plus général, c'est ainsi qu'il faut aussi traiter la continuité de service, la qualité de service ou la sécurité dans chaque module.

On utilise des concepts communs mais adaptés à des objets différents et donc techniquement les mises en œuvre sont différentes. La haute disponibilité d'un service WEB, d'un serveur, (virtualisé ou non), d'un routeur poursuit le même objectif général mais s'implémente de façon différente.

3 – Proposition non détaillée de progression

SISR3 – Exploitation des services

Ce module permet de construire les savoirs et savoir-faire liés à l'exploitation des services.

Un service est entendu ici comme le résultat d'une action qui répond à un besoin. Il est mis en œuvre par des composants logiciels ou matériels.

L'exploitation des services implique de gérer leur qualité, d'assurer leur continuité et leur sécurité. Elle participe à la détection des problèmes et peut être à l'origine d'une demande de changement.

Remarques :

- Ce module s'inscrit soit dans le processus « Production de services » (P1) soit dans le processus « fourniture de services » (P2) en prenant appui sur le processus « Conception et maintenance des solutions d'infrastructures ».
- Ce module s'appuie sur les savoirs et savoir-faire vus dans les modules SI1, SI2, SI5, SISR1 et SISR2.
- Même si l'on peut s'en inspirer avec profit, ce module n'est pas une réplique du processus « Exploitation des services » d'ITIL V3.
- L'exploitation des services va au-delà de l'installation et de la configuration de base d'un service. Les notions de base ont été vues en SI5 : il s'agit donc bien ici d'un approfondissement.
- On prend en compte la performance d'un service (qui peut-être mesurée en fonction d'un contrat de service), la continuité et la sécurité du service.
- Le mot service est polysémique. On entend ici le service rendu et perçu par l'utilisateur. Le service ne se réduit donc pas à un simple processus « serveur ». Par exemple la téléphonie sur IP peut-être considérée comme un service ou bien encore la « messagerie » ou le « serveur web » associé à un ou plusieurs sites. Par contre le DNS ou le DHCP ne sont pas des services perçus par l'utilisateur. On peut prendre un exemple caractéristique, l'accès internet est aujourd'hui un service perçu par l'utilisateur, quand celui-ci tombe on a immédiatement des appels. C'est donc le service perçu, mais pas le service réel, en effet un accès internet défaillant peut être la conséquence de nombreuses causes de dysfonctionnement.
- La notion de *cloud computing* peut-être étudiée ici dans la mesure où celle-ci distingue « l'application » en contact avec la client, la « plateforme » sur laquelle elle s'exécute et « l'infrastructure » qui supporte l'ensemble. Dans le module SISR3 le service est proche de la notion d'application.
- Dans tous les cas il faudra choisir un ou plusieurs services comme support d'apprentissage.
- On peut avoir différentes stratégies d'apprentissage, soit étudier un service en recherchant presque « l'expertise » soit étudier plusieurs services.
- Quel que soit le choix didactique, il faudra essayer de dissocier ce qui est spécifique à un service et ce qui est commun à l'ensemble des services, pour toujours essayer de fournir un savoir qui soit à la fois opérationnel et pérenne.
- Les normes et standard associés à la gestion des services (quand ils existent) doivent être étudiés.

.

La construction proposée ici est la suivante :

- **Mettre en production**
- **Exploiter**
- **Gérer les incidents et les problèmes**

Mettre en production est un approfondissement des notions vues en SI1 et SI5. Ici on doit s'intéresser de façon détaillée à l'architecture d'un service dans toutes ses composantes (intégration dans un environnement, installation, configuration, tests, scripts d'installation .etc.)

Exploiter met en place et utilise tous les éléments permettant de mesurer la qualité de service, d'optimiser le service, de tolérer la panne, et de sécuriser un service. C'est ici qu'on met en place les éléments permettant de contrôler l'accès au service. On peut ici s'intéresser aussi aux phases préalables d'authentification réseau (SISR5) et système (SISR4) avant même la phase d'authentification par le service qui est pris en charge par les habilitations. Les habilitations sont pris en charge par le service ou déléguées à un annuaire, dans ce cas la globalité est vue dans le module. Ici le service ne dysfonctionne pas et on vérifie en permanence son «opérationnalité ».

Gérer les incidents et les problèmes insiste sur toutes les procédures associés à la reprise de service et au fonctionnement dégradé mais étudie aussi les difficultés d'une migration vers une nouvelle version sur un service en exploitation (lien avec SI7). Ici le service dysfonctionne et on réagit par rapport à ce dysfonctionnement. On s'appuie bien évidemment sur les éléments vus en SISR1 mais en les 'associant à un service déterminé pour lequel des éléments de configuration de qualité, continuité et sécurité ont été configurés. Pour les problèmes de migration, il faudra certainement s'appuyer sur la virtualisation. On s'intéressera aux failles de sécurité connues de certains services.

En fonction des objectifs qu'on se fixe, les séquences peuvent être plus ou moins approfondies, on peut ainsi vouloir passer plus de temps sur certaines parties. On peut par exemple, prendre comme point de départ un service déjà configuré de façon basique et travailler à son optimisation dans le cadre d'un contrat professionnel : **en fait il faut que l'étudiant saisisse bien la différence entre un service installé sans enjeu professionnel, et le service installé dans un cadre professionnel exigeant.**

On peut sur chaque service distinguer 2 aspects : les aspects généraux et les aspects spécifiques dans le but de dégager des notions pérennes et opérationnelles.

- ⇨ Aspect généraux contrat de service, éléments de configuration, principe de disponibilité, principes de sécurité .etc.
- ⇨ Aspectes spécifiques : fichiers de configuration, processus, fichiers de données, fichiers d'activité .etc.

La meilleure progression pour SISR3 est de choisir un ou plusieurs services et de se situer dans le cadre d'un contrat de service.

Prenons l'exemple de 2 services de nature différente :

- la téléphonie sur IP
- le *web*

Téléphonie sur IP :

- Étude du concept
- Protocoles associés (SIP, RTP)
- Matériels spécifiques (téléphone IP, *softPhone,* etc.)
- Service (PABX logiciel ASTERISK, etc.)
- Services offerts (Audioconférence, visioconférence, etc.)
- Contrôles (habilitations, log, etc.)
- Bande passante (VLAN, QOS)
- Haute disponibilité du service (tolérance de pannes, répartition de charges, etc.)
- Sécurité du service (DOS, utilisation frauduleuse, espionnage, etc .)
- Supervision du service
- etc.

WEB :

- Protocoles associés (HTTP, HTTPS)
- Service (IIS, Apache, etc.)
- Optimisation (processus, thread, requêtes, etc.)

- Contrôles (habilitations, log, etc.)
- Bande passante (VLAN, QOS)
- Haute disponibilité du service
- Sécurité du service (DOS, utilisation frauduleuse, espionnage, etc .)
- Supervision du service
- etc.

Remarques :

- on est donc amené à travailler ici sur les VLAN et la QOS mais en consolidation sur des concepts acquis en SISR5 ;
- la haute disponibilité (comme, dans la mesure du possible, la supervision) de chaque service est configurée dans ce module.

SISR4 – Administration des systèmes

Ce module aborde les savoirs et savoir-faire liés à l'administration des systèmes.

On définit comme système un système serveur ou tout système associé à des solutions techniques d'accès. On se préoccupe ici de la mise en production, de l'administration sécurisée, de la gestion des performances, de la sécurité et de la disponibilité des systèmes, ainsi que de l'automatisation des tâches d'administration

Remarques :

- Ce module s'inscrit soit dans le processus « Production de services » (P1) soit dans le processus « fourniture de services » (P2) en prenant appui sur le processus « Conception et maintenance des solutions d'infrastructures ».
- Ce module s'appuie sur les savoirs et savoir-faire vus dans les modules SI1, SI5 et SISR1
- Par rapport à SI1 on se préoccupe ici du déploiement des solutions techniques d'accès et de la diffusion des mises à jours.
- Par rapport à SI5 on de préoccupe ici de qualité de service de continuité de service et de sécurité .dans la mise en place des serveurs.
- Les serveurs peuvent être des serveurs simples supportant un service mais ce type de serveur est plutôt utilisé par le module SISR3..
- Les serveurs du point de vue SISR4 sont plutôt les serveurs qui mutualisent les ressources nécessaires à l'exécution des services comme par exemple les annuaires, les autorités de certification, les baies de stockage, les solutions de sauvegarde, etc.
- SISR4 est le module principal où s'étudie les solutions de virtualisation et toutes les solutions de continuité de service et de répartition de charge qui en dépendent.
- SISR4 est le module principal où s'étudient les outils d'automatisation et donc le *scripting*.
- SISR4 est le module principal où s'étudient les services techniques orientés système.

.

La construction proposée ici est la suivante :

- **Déployer les installations et diffuser les mises à jour**
- **Mutualiser les ressources systèmes et assurer la qualité de service des serveurs**
- **Automatiser les tâches d'administration**

Déployer les installations et diffuser les mises à jour : on étudie ici une ou plusieurs solutions de déploiement avec les technologies associes (PXE, *multicast,* etc.). On étudie aussi les serveurs de mises à jour système ou antivirus par exemple. On peut aussi étudier les techniques de client légers ou de virtualisation des postes de travail (complément avec SI1).

Mutualiser les ressources systèmes et assurer la qualité de service des serveurs : Ici aujourd'hui on étudie clairement les solutions de virtualisation de serveur (HyperV, ESX, XEN, etc.) et les baies de stockage sécurisées de type NAS. On s'intéresse bien sûr aux solutions d'hyper disponibilité et de répartition de charges. On s'intéressera aussi aux problèmes de sécurité associés aux serveurs ainsi qu'aux problèmes d'authentification.

Automatiser les tâches d'administration : on étudie les langages de commandes orientés « scripting ».

SISR5 – Supervision des réseaux

Ce module aborde les savoirs et savoir-faire liés à la supervision des réseaux.

On se préoccupe en priorité ici de performance, de disponibilité et de sécurité au niveau des éléments d'interconnexion du réseau.

Remarques :

- Ce module s'inscrit soit dans le processus « Production de services » (P1) soit dans le processus « fourniture de services » (P2) en prenant appui sur le processus « Conception et maintenance des solutions d'infrastructures ».
- Ce module s'appuie sur les savoirs et savoir-faire vus dans les modules SI2, SISR1 et SISR2
- Par rapport à SI2 et SISR2 on étudiera des infrastructures réseaux complexes intégrant la qualité de service et la continuité de service. On pourra regarder par exemple avec intérêt l'architecture CISCO (*access layer, distribution layer* et *core layer*).
- On s'appuiera autant se faire que peut sur des infrastructures d'entreprise.
- Ce module se préoccupe essentiellement des matériels d'interconnexion mais peut utiliser des services techniques comme par exemple une autorité de certification, des annuaires, RADIUS, etc.
- Pour les matériels d'interconnexion on se préoccupera de la qualité de service de la continuité de service et de la sécurité.
- SISR5 est le module principal où s'étudie les solutions de supervision avec prise en charge des alertes.
- SISR5 est le module principal où s'étudient les solutions de sécurité orientées infrastructures (couche 2 et couche 3).
- SISR5 est le module principal où s'étudient les services techniques orientés réseau.

.

La construction proposée ici est la suivante :

- **Assurer la qualité et la continuité de service**
- **Administrer et Superviser**
- **Sécuriser l'accès au réseau et détecter l'activité anormale**

Assurer la qualité et la continuité de service : on étudiera ici des solutions au niveau de la couche 2 comme par exemple le *spanning tree* ou la QOS associée aux VLAN. On étudiera aussi des solutions pour la couche 3 comme HSRP ou VRRP.

Administrer et superviser : on étudiera des solutions de configuration dynamique comme les GVRP (2) ou OSPF (3) par exemple. On mettra en œuvre une solution de supervision en étudiant les protocoles associés (SNMP par exemple). On mettra en place des solutions de métrologie au niveau des matériels d'interconnexion et des solutions permettant de contrôler les flux.

Sécuriser l'accès au réseau et détecter l'activité anormale : on mettra en place des architectures sécurisées (VLAN, DMZ, etc.) dans la continuité de SISR2. On étudiera des protocoles sécurisés d'accès au réseau comme 802.1X, EAP, PEAP RADIUS, WPA par exemple. On étudiera quelques failles de sécurité standard. On mettra en œuvre éventuellement des outils de détection d'intrusion.