Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour en savoir plus sur nos formations disponibles, veuillez visiter :
formav.co/explorer

BTS SIO

# E5 : Production et fourniture de services

**Session 2016** • Code sujet : **SI5SISR** • Durée : **4 heures** • Coefficient : **5**

## Sommaire

Cliquez sur une partie pour y accéder directement

**1. Conception et maintenance de services** (14 questions) **Page 3**

**2. Production de services et gestion du patrimoine** (8 questions) **Page 8**

**3. Ce qu'il faut retenir & Questions fréquentes (FAQ)** (Synthèse & Q&A Examen) **Page 11**

**Sujet officiel (PDF) :** https://coursbtssio.fr/assets/annales/bts-sio/E5 - Administration des systèmes et des réseaux (spécifique à l'option)/2016/BTS SIO - E5 - Administration des systèmes et des réseaux (spécifique à l'option) - Session 2016 - 1-Sujet.pdf

# 1. Conception et maintenance de services

La société RIOCA fait auditer son système d'information afin d'améliorer l'organisation de son infrastructure, sa disponibilité et sa sécurité. Le dossier traite aussi de la supervision, de la sauvegarde des journaux de connexion et de l'évolution vers une infrastructure virtualisée.

## Mission 1 : Analyse et maintenance de l'infrastructure

**Question A.1.1. Pour chaque constat de la FRAP n° 1 relatif à l'organisation et à la gestion de l'infrastructure informatique, détailler les conséquences possibles sur le fonctionnement du réseau.**

Les quatre constats entraînent des risques distincts :

- Sans alerte, une panne ou une saturation peut durer avant d'être détectée.
- Sans compte rendu, les interventions sont mal suivies et les mêmes erreurs peuvent se reproduire.
- Sans identification préalable, le diagnostic ne commence qu'à l'arrivée des techniciens, ce qui allonge l'interruption.
- L'examen manuel quotidien des journaux retarde le repérage des anomalies et mobilise du temps d'administration.

Au total, la réactivité et la disponibilité du réseau diminuent.

> **✓ RÉPONSE À RETENIR**
>
> Détection tardive, diagnostics plus longs, incidents répétitifs et disponibilité du réseau réduite.

**Question A.1.2. Recommander des solutions techniques susceptibles de résoudre durablement l'ensemble des problèmes décrits dans la FRAP n° 1.**

Déployer une supervision centralisée des serveurs et équipements réseau, avec alertes automatiques sur les pannes et seuils critiques. Centraliser les journaux afin de faciliter les recherches et le diagnostic. Enregistrer chaque incident dans un outil de suivi avec ses symptômes, sa cause et sa résolution. Tenir à jour la documentation de l'architecture, des configurations et des procédures de dépannage. Enfin, planifier les évolutions de l'infrastructure et organiser le partage des responsabilités pour limiter la dépendance à quelques techniciens.

> **✓ RÉPONSE À RETENIR**
>
> Supervision avec alertes, journaux centralisés, suivi documenté des incidents et planification de l'infrastructure.

## Mission 2 : Définition des éléments nécessaires à la continuité de service

**Question A.2.1. Donner le principe d'une gestion des SLA (Service Level Agreement) et présenter les avantages qu'elle apporte.**

Un SLA définit les niveaux de service attendus entre les utilisateurs et le service informatique, par exemple la disponibilité d'un serveur ou le délai de réponse. Sa gestion consiste à mesurer les indicateurs, à les comparer aux objectifs convenus et à signaler les écarts. Elle apporte une mesure objective de la qualité du service, aide à repérer les services insuffisamment disponibles et permet de prioriser les corrections. Les engagements deviennent plus clairs et le dialogue entre utilisateurs et informaticiens est facilité.

> ✓ **RÉPONSE À RETENIR**
>
> Mesurer les niveaux de service, les comparer aux objectifs et corriger les écarts.

**Question A.2.2. Identifier les points faibles de l'infrastructure réseau actuelle de RIOCA concernant la disponibilité des systèmes et des applications.**

Plusieurs éléments constituent des points de défaillance uniques :

- Le PGI et l'annuaire LDAP sont hébergés sur un seul serveur physique ESXi : sa panne peut interrompre les deux services.
- La panne LDAP a déjà bloqué le fonctionnement normal de l'entreprise pendant deux jours.
- DHCP, DNS, proxy, serveur web et NAS sont décrits comme des serveurs uniques, sans redondance indiquée.
- Le cœur de réseau et l'accès Internet ADSL n'ont pas de secours mentionné.

Les SLA confirment une disponibilité faible des serveurs web et d'authentification.

> ✓ **RÉPONSE À RETENIR**
>
> Services centraux et équipements sans redondance : une panne peut interrompre plusieurs systèmes et applications.

**Question A.2.3. Démontrer qu'en cas d'arrêt planifié d'un serveur ESXi, les modules de la solution de base permettent d'assurer la continuité de service.**

Les deux hôtes ESXi sont administrés comme un cluster par vCenter. Les machines virtuelles résident sur le stockage partagé VMFS, accessible en lecture et en écriture par plusieurs hôtes. Avant la maintenance, l'administrateur utilise vMotion pour migrer à chaud les machines virtuelles actives vers l'autre ESXi. Le sujet précise que cette migration s'effectue sans interruption et préserve l'intégrité des transactions. L'hôte initial peut alors être arrêté pour maintenance.

✓ RÉPONSE À RETENIR

vMotion migre à chaud les machines virtuelles vers l'autre ESXi grâce au stockage partagé VMFS, sans interruption de service.

---

**Question A.2.4. Préciser en quoi la solution de base améliore également le plan de reprise d'activité (PRA) de RIOCA en cas de panne brutale de l'un des serveurs ESXi.**

En cas de panne brutale d'un ESXi, VMFS partagé permet à l'autre hôte d'accéder aux fichiers des machines virtuelles. L'administrateur peut alors les enregistrer ou les redémarrer sur cet hôte, sans reconstruire les serveurs virtuels ni restaurer immédiatement toutes leurs données. vCenter facilite la gestion centralisée du cluster, mais le redémarrage automatique après panne relève du module optionnel HA, absent de la solution de base. La reprise est donc facilitée, sans être instantanée ni automatique.

✓ RÉPONSE À RETENIR

VMFS partagé permet de relancer manuellement les machines virtuelles sur l'autre ESXi et facilite la reprise après panne.

---

**Question A.2.5. Expliquer comment les modules optionnels pourraient améliorer le taux de disponibilité du serveur d'authentification une fois virtualisé.**

Le module HA redémarre automatiquement la machine virtuelle d'authentification sur un autre ESXi en cas de panne de l'hôte. Fault Tolerance maintient une seconde machine virtuelle synchronisée : si la principale devient indisponible, la copie prend le relais sans interruption perceptible du service. DRS équilibre les ressources entre les hôtes et contribue à réserver la capacité nécessaire. HA et FT réduisent directement la durée d'interruption, tandis que DRS aide à maintenir les performances du serveur d'authentification.

✓ RÉPONSE À RETENIR

HA redémarre automatiquement la machine virtuelle, FT assure un relais continu et DRS équilibre les ressources disponibles.

---

**Question A.2.6. Montrer que la virtualisation et la haute disponibilité peuvent avoir un impact positif sur le TCO (coût total de possession).**

La virtualisation consolide plusieurs serveurs sur moins d'hôtes physiques : elle peut réduire les achats de matériel, l'espace occupé, la consommation électrique et la maintenance. La gestion centralisée peut aussi diminuer le temps d'administration. La migration à chaud et la haute disponibilité limitent les interruptions, donc les pertes de productivité et les coûts d'incident. Enfin, DRS répartit les charges et sa fonction DPM peut réduire la consommation d'énergie. Ces économies sont à mettre en balance avec le coût de la plateforme et des licences.

✓ RÉPONSE À RETENIR

La réduction du matériel, de l'énergie, de la maintenance et des interruptions peut abaisser le TCO.

---

### Mission 3 : Définition des éléments nécessaires à la sécurité de l'infrastructure

**Question A.3.1. À la suite de l'incident ayant endommagé des disques et une alimentation, citer deux éléments matériels indispensables permettant de sécuriser un serveur physique.**

L'incident a détruit deux disques et une alimentation. Pour les disques, un RAID 6 est adapté, car il peut tolérer la défaillance simultanée de deux disques et maintenir l'accès aux données. Pour l'alimentation, installer deux blocs redondants permet au serveur de rester alimenté si l'un tombe en panne. Si possible, raccorder ces blocs à des circuits électriques distincts pour réduire le risque d'une coupure commune.

✓ RÉPONSE À RETENIR

Disques en RAID 6 et alimentation électrique redondante.

---

**Question A.3.2. Indiquer trois autres dispositifs permettant de mieux sécuriser la salle serveur.**

Trois dispositifs complémentaires réduisent les risques observés et protègent les équipements :

- Surveillance de la température et climatisation redondante, avec alerte en cas de défaillance.
- Détection incendie adaptée à une salle informatique et extinction sans projection d'eau.
- Contrôle d'accès physique par badge ou serrure sécurisée, avec suivi des entrées.

Un onduleur constitue aussi une protection utile contre les coupures électriques et permet un arrêt maîtrisé.

✓ RÉPONSE À RETENIR

Climatisation surveillée, détection et extinction incendie adaptées, contrôle des accès physiques.

---

**Question A.3.3. Donner deux arguments permettant de justifier la mise en place de mod_security, pare-feu applicatif web, en complément du pare-feu actuel de l'entreprise.**

Le pare-feu réseau filtre principalement les flux selon des critères tels que les adresses IP et les ports. mod_security complète cette protection en analysant le contenu des requêtes et réponses HTTP échangées avec le portail, afin de détecter ou bloquer des attaques visant l'application web. Il peut aussi journaliser les requêtes suspectes. En cas de violations répétées depuis une même adresse, il peut exécuter un script demandant au pare-feu réseau de bloquer cette adresse.

✓ RÉPONSE À RETENIR

Analyse et filtrage des échanges HTTP, journalisation des requêtes suspectes et possible blocage des adresses malveillantes.

### Mission 4 : Amélioration du trafic réseau

**Question A.4.1. Expliquer en quoi la mise en place de notifications (traps) SNMP pourrait résoudre le problème de lenteur sur le réseau.**

La supervision actuelle interroge les équipements à intervalles réguliers, ce qui génère de nombreuses trames SNMP. Avec les traps, un équipement envoie une notification seulement lorsqu'un événement prédéfini survient, par exemple un seuil de disque ou de trafic dépassé. Cette approche réduit les interrogations périodiques et le volume de trafic SNMP, tout en alertant rapidement l'administrateur. Le serveur de supervision doit disposer des MIB correspondantes pour interpréter les notifications reçues.

> ✓ **RÉPONSE À RETENIR**
>
> Les traps événementiels réduisent les interrogations périodiques et le trafic SNMP associé.

### Mission 5 : Planification des sauvegardes

**Question A.5.1. Proposer une solution permettant la réplication quotidienne, sur le serveur NAS, des fichiers contenant les connexions internet.**

Programmer chaque jour, sur le proxy, la copie du journal de connexions vers un répertoire dédié du NAS. Le N8500 accepte notamment NFS, CIFS et FTP : choisir un protocole adapté et utiliser un compte réservé à cette tâche, avec des droits limités. Dater les fichiers pour éviter leur écrasement, vérifier automatiquement le résultat de la copie et appliquer une politique de conservation d'au moins un an. La réplication doit être contrôlée afin de détecter rapidement un échec.

> ✓ **RÉPONSE À RETENIR**
>
> Copie quotidienne contrôlée des journaux proxy vers le NAS, avec une conservation d'au moins un an.

**Question A.5.2. Donner les caractéristiques techniques du serveur NAS permettant de répondre aux critères de confidentialité des données et de disponibilité des données.**

Pour la confidentialité, le schéma prévoit l'intégration du NAS au domaine : les groupes et comptes du domaine permettent de contrôler les droits d'accès aux fichiers. Pour la disponibilité, le N8500 possède une architecture en cluster actif-actif à deux nœuds. Ses niveaux RAID comprennent le RAID 6, qui tolère la perte de deux disques. Les fonctions de mise en miroir, d'instantané et de réplication apportent des protections complémentaires pour restaurer les données, sans remplacer le contrôle des accès.

> ✓ **RÉPONSE À RETENIR**
>
> Confidentialité : droits liés aux utilisateurs et groupes du domaine. Disponibilité : cluster actif-actif à deux nœuds et RAID 6.

## 2. Production de services et gestion du patrimoine

RIOCA étudie le déploiement d'un accès Wi-Fi destiné aux appareils personnels des salariés, ainsi que le recyclage de postes informatiques sous forme de clients légers LTSP. Les tâches portent sur les équipements et configurations réseau, puis sur l'analyse d'un problème de démarrage à partir d'un fichier DHCP et de résultats de tests.

### Mission 1 : Préparation d'une solution d'infrastructure

**Question B.1.1. Justifier que la borne d'accès sans fil choisie respecte les conditions de mise en œuvre définies avec le DSI.**

La WAP371 répond aux contraintes principales : son port Ethernet Gigabit s'intègre au réseau, son alimentation PoE évite de tirer des câbles électriques et elle prend en charge WPA2 et RADIUS. Sa portée minimale de 100 m est cohérente avec le choix de deux bornes pour l'atelier de 20 m sur 80 m. La pose en hauteur, hors d'accès, répond à la demande de protection contre le vol et les incidents. Elle permet aussi la segmentation VLAN.

> ✓ **RÉPONSE À RETENIR**
>
> La WAP371 convient : Gigabit, PoE, WPA2/RADIUS et VLAN, avec deux bornes prévues pour l'atelier.

**Question B.1.2. Proposer des éléments de réponse permettant de valider ou d'invalider chacun des choix de configuration proposés pour le déploiement de la nouvelle zone Wi-Fi : modifier le SSID, cacher le SSID, configurer des adresses IP statiques avec une plage limitée, choisir un mot de passe fort pour l'administration du point d'accès, filtrer les clients par adresse MAC et choisir une méthode d'authentification par portail captif ou serveur RADIUS.**

| Choix | Décision et justification |
|---|---|
| Modifier le SSID | Oui : remplacer le nom par défaut, sans en faire une protection suffisante. |
| Cacher le SSID | Non : le masquage n'empêche pas sa détection et complique la connexion. |
| IP statiques à plage limitée | Non : DHCP convient mieux aux appareils personnels et aux connexions temporaires. |
| Mot de passe d'administration fort | Oui : il protège la configuration du point d'accès. |
| Filtrage MAC | Non comme protection principale : une adresse MAC peut être usurpée. |
| Portail captif ou RADIUS | Oui : privilégier RADIUS avec WPA2 pour authentifier les utilisateurs. |

La sécurité doit reposer principalement sur un chiffrement et une authentification robustes.

> ✓ **RÉPONSE À RETENIR**
>
> Valider le SSID personnalisé, le mot de passe d'administration fort et l'authentification RADIUS/WPA2. Ne pas retenir le masquage SSID, les IP statiques ou le filtrage MAC comme protections principales.

**Question B.1.3.** **Proposer la nouvelle configuration du commutateur de l'atelier afin d'intégrer la nouvelle zone dans le VLAN Wi-Fi.**

1. Créer ou activer le VLAN 50, nommé `WIFI`, déjà défini dans le plan d'adressage en `172.20.0.0/24`.
2. Raccorder les deux bornes à deux ports PoE libres parmi `Fa0/25` à `Fa0/28`, configurés en ports d'accès du VLAN 50.
3. Sur le port de cascade `Gi0/25`, transporter le VLAN 50 vers le cœur de réseau, en conservant le VLAN 20. Vérifier que le relais DHCP et le serveur DHCP prennent en charge le VLAN Wi-Fi.

> ✓ **RÉPONSE À RETENIR**
>
> Créer le VLAN 50 WIFI, affecter deux ports PoE libres à ce VLAN et transporter le VLAN 50 sur la cascade Gi0/25 vers le cœur.

## Mission 2 : Recyclage de solutions techniques d'accès

**Question B.2.1.** **Donner trois avantages apportés par une architecture LTSP utilisant des clients légers.**

LTSP permet de réutiliser les anciens ordinateurs comme clients légers, sans stockage local nécessaire au démarrage. Les applications et l'authentification étant traitées sur le serveur, les clients peuvent avoir une configuration matérielle minimale. Enfin, l'absence de logiciel à installer sur chaque client et la centralisation des applications et des opérations simplifient la maintenance et l'administration du parc.

> ✓ **RÉPONSE À RETENIR**
>
> LTSP réduit les achats de matériel, simplifie la maintenance des clients et centralise applications et authentification sur le serveur.

**Question B.2.2.** **Montrer, en utilisant le critère du TCO, que le recyclage est plus intéressant que l'achat de nouveaux postes.**

Le TCO prend en compte l'achat, l'installation, la maintenance et l'exploitation. Le recyclage évite l'achat de dix postes neufs et limite les interventions sur les clients, qui n'ont ni stockage local ni logiciel spécifique à maintenir. LTSP centralise applications et administration sur le serveur hébergé dans le cluster ESX. Il faut néanmoins intégrer au TCO la mise en place et l'exploitation du serveur, ainsi que les éventuels coûts de licences et de capacité. À service comparable, la réutilisation des postes et la maintenance centralisée rendent cette solution moins coûteuse que l'achat de dix postes neufs.

> ✓ **RÉPONSE À RETENIR**
>
> Le recyclage sous LTSP réduit le TCO en évitant l'achat de dix postes et en centralisant leur maintenance.

**Question B.2.3. Indiquer s'il est possible d'ajouter les dix clients légers sans modification du réseau, du point de vue physique comme logique, et justifier la réponse.**

**Physiquement :** oui, sous réserve de ports libres. Le commutateur de zone dispose d'au moins 24 ports ; les équipements actuels laissent la capacité nécessaire pour raccorder dix clients supplémentaires. **Logiquement :** non, le sous-réseau Garage `172.20.1.128/28` offre 14 adresses d'hôtes. Il faut en prévoir 22 pour les 20 postes, l'imprimante et la passerelle. Le sous-réseau doit donc être agrandi, par exemple en /27 si l'espace d'adressage est disponible, puis l'étendue DHCP et la configuration de la passerelle doivent être adaptées.

> **✓ RÉPONSE À RETENIR**
>
> Le raccordement physique est possible avec des ports libres. Le /28 est insuffisant : 22 adresses sont nécessaires ; prévoir au minimum un /27 disponible et adapter DHCP.

**Question B.2.4. À partir du fichier de configuration du serveur DHCP et des résultats des tests, identifier la raison pour laquelle le client léger ne récupère pas de session.**

Le client reçoit bien une configuration DHCP et commence le chargement PXE ; le ping confirme que le serveur LTSP `172.20.2.13` est joignable. Cependant, l'option `next-server` indique `172.20.2.12`. Le client tente donc de charger `pxelinux.0` depuis une adresse erronée, ce qui explique le message « No server found ». Le problème se situe dans l'adresse du serveur d'amorçage communiquée par DHCP, pas dans la connectivité générale.

> **✓ RÉPONSE À RETENIR**
>
> L'option DHCP `next-server` pointe vers `172.20.2.12` au lieu de l'adresse réelle du serveur LTSP, `172.20.2.13`.

**Question B.2.5. Proposer une solution afin de résoudre le problème empêchant le client léger de récupérer une session.**

1. Corriger dans la configuration DHCP l'option `next-server` et y indiquer `172.20.2.13`, adresse relevée sur l'interface du serveur LTSP.
2. Recharger le service DHCP pour appliquer la modification, puis renouveler le bail du client si nécessaire.
3. Relancer le démarrage PXE et vérifier le chargement de `/ltsp/lightclient/pxelinux.0` depuis le serveur, puis l'ouverture de session.

> **✓ RÉPONSE À RETENIR**
>
> Remplacer `next-server 172.20.2.12` par `next-server 172.20.2.13`, recharger DHCP et retester le démarrage PXE.

# Ce qu'il faut retenir de ce sujet (Session 2016)

**Bilan de l'épreuve :** Épreuve E5 du BTS Services informatiques aux organisations, option SISR, session 2016, code SI5SISR, d'une durée de quatre heures et de coefficient 5. Le cas RIOCA évalue l'analyse et la maintenance d'une infrastructure informatique, la continuité et la sécurité des services, la sauvegarde, la configuration Wi-Fi et VLAN, ainsi que le recyclage de postes en clients légers LTSP.

### Notions-clés, formules & règles à maîtriser

- Un SLA formalise les niveaux de service attendus et permet de comparer les résultats mesurés aux objectifs convenus.
- vMotion migre une machine virtuelle en fonctionnement; HA la redémarre automatiquement sur un autre hôte après une panne.
- Un trap SNMP signale un événement à la supervision sans attendre une interrogation périodique de l'équipement.
- LTSP exécute les applications sur le serveur; le client démarre par PXE et dépend notamment des paramètres DHCP.

### Points de vigilance & attentes du jury

- Distinguer la migration planifiée par vMotion du redémarrage automatique après panne fourni par HA.
- Justifier les choix de sécurité Wi-Fi au regard des contraintes pratiques et ne pas confondre masquage du SSID et authentification.
- Vérifier les correspondances entre VLAN, ports, plage DHCP, passerelle, adresse du serveur LTSP et chemins PXE.
- Pour le NAS, relier chaque critère aux fonctions adaptées : droits d'accès pour la confidentialité, redondance et réplication pour la disponibilité.

## Questions fréquentes sur cette épreuve (Q&A Examen)

**Q : Quelle différence faut-il retenir entre vMotion et HA dans ce sujet ?**

vMotion déplace à chaud une machine virtuelle vers un autre serveur pour permettre une maintenance planifiée sans interruption. HA intervient après une panne d'hôte et redémarre automatiquement les machines virtuelles affectées sur un autre serveur disponible.

**Q : Pourquoi le client léger affiche-t-il « No server found » malgré le ping réussi ?**

Le ping confirme la connectivité IP, mais pas le bon fonctionnement du service LTSP. Il faut vérifier que l'adresse du serveur LTSP indiquée par next-server correspond à son adresse réelle, puis contrôler la configuration PXE et le service de démarrage.

**Q : Comment organiser son temps et lire le barème de cette épreuve ?**

L'épreuve dure quatre heures et totalise 100 points : 60 pour le dossier A et 40 pour le dossier B. Parcourez les deux dossiers, répartissez le temps selon leur poids, puis gardez quelques minutes pour vérifier les réponses et les configurations.

**Q : Quels critères le jury attend-il dans les réponses techniques ?**

Les réponses doivent s'appuyer sur les documents et relier chaque recommandation à la contrainte ou au problème posé. Pour une configuration, indiquez les éléments utiles et cohérents, notamment les adresses, VLAN, ports, services ou mécanismes de disponibilité concernés.

**Sujet officiel associé (PDF) :** https://coursbtssio.fr/assets/annales/bts-sio/E5 - Administration des systèmes et des réseaux (spécifique à l'option)/2016/BTS SIO - E5 - Administration des systèmes et des réseaux (spécifique à l'option) - Session 2016 - 1-Sujet.pdf
**Ressources BTS Services Informatiques aux Organisations :** Toutes les annales & corrigés • Fiches de révision complètes • Simulateur de notes d'examen

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.