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

BTS Services informatiques aux organisations

Session 2019 • Code sujet : **SI5SISR** • Durée : **4 heures** • Coefficient : **5**

Sommaire

Cliquez sur une partie pour y accéder directement

1. Refonte de l'infrastructure (10 questions) **Page 3**

2. Intégration dans l'équipe support (11 questions) **Page 8**

3. Migration vers le cloud (8 questions) **Page 12**

4. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 16**

Sujet officiel (PDF) : https://coursbtssio.fr/assets/annales/bts-sio/E5 - Administration des systèmes et des réseaux (spécifique à l'option)/2019/BTS SIO - E5 - Administration des systèmes et des réseaux (spécifique à l'option) - Session 2019 - 1-Sujet.pdf

1. Refonte de l’infrastructure

La plateforme de développement et de tests du site C doit se rapprocher de l’architecture de production, notamment en séparant les serveurs Web des serveurs de bases de données dans des VLAN distincts. Le dossier porte aussi sur le remplacement d’équipements réseau, la mise en service sécurisée du nouveau commutateur et son intégration à la supervision.

Mission A.1

Question A.1.1. Indiquer, en argumentant, en quoi le commutateur présélectionné permet de prendre en charge les mêmes fonctionnalités que le routeur RT-1 et le commutateur SW2-1 à remplacer.

Le Catalyst 3850-24T-S réunit commutation de niveau 2 et routage de niveau 3. Ses 24 ports Gigabit Ethernet permettent de raccorder les équipements prévus, tandis que la prise en charge des VLAN et des trunks 802.1Q reprend les fonctions de commutation de SW2-1. Ses interfaces virtuelles commutées (SVI) et sa capacité de routage IPv4 permettent le routage inter-VLAN assuré par RT-1. Le port relié à FW-1 peut aussi être raccordé au nouveau commutateur. Il peut donc remplacer ces équipements pour les fonctions décrites.

> **✓ RÉPONSE À RETENIR**
>
> Le Catalyst 3850 assure la commutation des VLAN et le routage inter-VLAN nécessaires au remplacement de SW2-1 et RT-1.

Question A.1.2. Proposer, pour le nouveau VLAN destiné aux serveurs Web, un numéro de VLAN, une adresse de sous-réseau et un masque, puis justifier la réponse.

Paramètre	Proposition
Numéro et nom	VLAN 80, serveurs_Web
Sous-réseau	172.29.80.0/22
Masque	255.255.252.0

Le VLAN 80 est distinct des VLAN existants. Le sous-réseau 172.29.80.0/22 suit les blocs commençant par 172.29.64.0, 68.0, 72.0 et 76.0. Le préfixe /22 conserve la capacité des sous-réseaux actuels : 10 bits sont disponibles pour les hôtes, soit 1 022 adresses utilisables après retrait des adresses réseau et de diffusion.

> **✓ RÉPONSE À RETENIR**
>
> VLAN 80, sous-réseau 172.29.80.0/22, masque 255.255.252.0, avec 1 022 adresses hôtes utilisables.

Question A.1.3. **Indiquer si la configuration IP des serveurs SRV-IIS-1 et SRV-IIS-2 doit être modifiée après l'implantation du nouveau VLAN. Proposer, si nécessaire, les paramètres des autres VLAN en conformité avec l'existant.**

Oui. Les serveurs Web changent de sous-réseau, car ils passent du VLAN 72 au VLAN 80. Ils gardent leurs derniers octets actuels et le masque /22. Les serveurs SQL restent dans le VLAN 72. La passerelle de chaque VLAN conserve la convention indiquée : dernière adresse IP utilisable.

Équipement ou VLAN	Adresse ou passerelle
SRV-IIS-1, VLAN 80	172.29.80.203/22, passerelle 172.29.83.254
SRV-IIS-2, VLAN 80	172.29.80.204/22, passerelle 172.29.83.254
VLAN 64, 68, 72 et 76	Passerelles inchangées : 172.29.67.254, 172.29.71.254, 172.29.75.254 et 172.29.79.254

Les autres adresses IP restent inchangées.

> ✓ **RÉPONSE À RETENIR**
>
> SRV-IIS-1 : 172.29.80.203/22. SRV-IIS-2 : 172.29.80.204/22. Passerelle : 172.29.83.254. Les autres adresses IP restent inchangées.

Question A.1.4. **Expliquer pourquoi les tests de connectivité ont échoué et proposer une solution pour remédier au problème, en s'appuyant sur les tests et la configuration de SW3-1.**

La passerelle du nouveau VLAN répond au ping depuis SRV-SQL-1 : la SVI est active. En revanche, les trunks vers ESX-1 à ESX-4 n'autorisent que les VLAN 64, 68, 72 et 76. Le VLAN 80 n'est donc pas transporté jusqu'aux machines virtuelles. Cela explique l'échec du ping entre SRV-SQL-1 et SRV-IIS-1, ainsi que l'impossibilité pour SRV-IIS-1 de joindre sa passerelle.

Ajouter le VLAN 80 aux VLAN autorisés sur les ports G1/0/1 à G1/0/4, en conservant les VLAN déjà autorisés, puis retester la passerelle et la communication entre serveurs.

> ✓ **RÉPONSE À RETENIR**
>
> Autoriser le VLAN 80 sur les trunks G1/0/1 à G1/0/4, puis vérifier les pings vers la passerelle et entre serveurs.

a.

Question A.2.1. **Argumenter le choix d'un protocole sécurisé d'accès à distance compatible avec le nouveau commutateur.**

Utiliser SSH pour l'administration à distance du Catalyst 3850. Le commutateur prend en charge SSH, contrairement à une solution limitée à Telnet. SSH chiffre la session, notamment les identifiants et les commandes échangées. Telnet les transmet en clair, ce qui permettrait leur interception sur le réseau. SSH répond ainsi au

besoin d’accès distant tout en protégeant les informations d’administration du commutateur.

> **✓ RÉPONSE À RETENIR**
>
> Choisir SSH : il chiffre les identifiants et les commandes d’administration, contrairement à Telnet.

---

b.

Question A.2.1. Lister et justifier les points à vérifier lors de la configuration du protocole d’accès à distance afin d’obtenir le meilleur niveau de sécurité.

Configurer SSH v2 et désactiver Telnet afin d’éviter un accès distant non chiffré. Restreindre l’administration aux seuls postes ou réseaux autorisés et appliquer les mesures suivantes :

- Utiliser des clés cryptographiques robustes : limiter le risque de déchiffrement ou d’usurpation.
- Créer des comptes nominatifs avec des mots de passe robustes et des privilèges adaptés : limiter les abus et les erreurs.
- Appliquer une ACL aux connexions d’administration : bloquer les sources non autorisées.
- Prévoir une durée d’inactivité courte : éviter qu’une session ouverte soit utilisée sans autorisation.

> **✓ RÉPONSE À RETENIR**
>
> SSH v2, clés et mots de passe robustes, comptes nominatifs à privilèges minimaux, ACL d’administration, délai d’inactivité et Telnet désactivé.

---

a.

Question A.2.2. Argumenter l’importance de centraliser les journaux des événements système sur un serveur et de synchroniser les horloges de tous les appareils.

La centralisation permet de consulter les événements depuis un serveur unique, de les corréler entre appareils et de conserver des traces même si un équipement tombe en panne ou est compromis. Elle facilite le diagnostic et l’analyse de sécurité. Synchroniser les horloges, par exemple avec NTP, garantit des horodatages cohérents. On peut alors reconstituer l’ordre des événements provenant de plusieurs systèmes, sans décalage horaire susceptible de fausser l’analyse.

> **✓ RÉPONSE À RETENIR**
>
> La centralisation facilite la conservation et la corrélation des journaux. La synchronisation des horloges garantit une chronologie fiable.

b.

Question A.2.2. Vérifier si le commutateur retenu peut répondre aux besoins de centralisation des journaux et de synchronisation des horloges.

Besoin	Fonction prise en charge
Centraliser les journaux	Syslog
Synchroniser les horloges	NTP

Les caractéristiques du Catalyst 3850 mentionnent explicitement la prise en charge de Syslog et de NTP. Le commutateur peut donc envoyer ses journaux au serveur central et synchroniser son horloge avec le serveur de temps configuré. Il faut renseigner les destinations correspondantes lors de sa mise en service.

> **✓ RÉPONSE À RETENIR**
>
> Oui. Le Catalyst 3850 prend en charge Syslog pour centraliser les journaux et NTP pour synchroniser les horloges.

Mission A.2

Question A.2.3. Lister les principaux paramétrages à réaliser lors de la configuration de l'agent SNMP sur le commutateur. Pour chaque paramétrage, argumenter en termes de risques potentiels et de sécurisation.

Privilégier SNMPv3, disponible sur le commutateur, avec authentification et chiffrement : SNMPv1 et SNMPv2c reposent sur une communauté qui ne chiffre pas les échanges. Pour l'intégration, vérifier les points suivants :

- Créer un utilisateur SNMPv3 et lui attribuer une vue en lecture seule : limiter les modifications possibles.
- Autoriser uniquement l'adresse du serveur Centreon, par ACL : réduire les requêtes non autorisées.
- Configurer la destination des traps si les alertes SNMP sont utilisées : recevoir les notifications sur le bon serveur.
- Configurer Centreon avec la même version et les mêmes paramètres SNMPv3. Si l'environnement reste en SNMPv2c, utiliser une communauté robuste et limiter son accès par ACL.

> **✓ RÉPONSE À RETENIR**
>
> SNMPv3 avec authentification, chiffrement, droits en lecture seule et accès limité à Centreon. Adapter Centreon à la même version.

Question A.2.4. Proposer deux commandes de vérification pertinentes pour superviser la disponibilité réseau du commutateur et la bande passante de ses interfaces. Préciser les valeurs des paramètres et justifier les choix.

Le contrôle ping vérifie la disponibilité IP du commutateur. Le contrôle de trafic mesure la charge d'une interface en pourcentage. Dans la commande de trafic, sélectionner l'index SNMP correspondant à G1/0/1, à relever sur le commutateur : le sujet ne fournit pas cet index. Les seuils de 80 % et 90 % sont des valeurs de configuration proposées pour l'avertissement et l'état critique. Les paramètres SNMP ci-dessous reprennent ceux déjà configurés dans Centreon.

```
/usr/lib/nagios/plugins/check_icmp -H $HOSTADDRESS$ -n 5
/usr/lib/nagios/plugins/check_centreon_traffic -H $HOSTADDRESS$ -n -i <ifIndex_de_G1/0/1> -w
80 -c 90 -v 2c -C $_HOSTSNMPCOMMUNITY$ -- 64-bits
```

Le ping utilise cinq sondes. Si SNMPv3 est retenu, il faut aussi adapter la commande et la configuration de Centreon.

> **✓ RÉPONSE À RETENIR**
>
> Disponibilité : ping avec 5 sondes. Trafic de G1/0/1 : index SNMP de l'interface, warning 80 %, critical 90 %, compteurs 64 bits.

2. Intégration dans l’équipe support

L’équipe support doit traiter la saturation d’un lien réseau, puis analyser une activité anormale repérée dans les journaux d’un serveur Web. Le dossier demande aussi de qualifier une alerte de RAID dégradé, de préparer une intervention et d’appliquer la démarche ITIL de gestion des incidents et des problèmes.

Mission B.1

Question B.1.1. Proposer une solution permettant d’augmenter le débit du lien saturé, en vous appuyant sur le graphe de supervision et les spécifications des cartes réseau des serveurs ESX et du commutateur.

Le graphe indique pour G1/0/1 un débit entrant moyen de 873,66 Mbit/s et un maximum de 990,39 Mbit/s, proche de la capacité d’un lien Gigabit. Cette interface relie ESX-1 à SW3-1. La carte réseau d’ESX-1 possède quatre ports Gigabit et prend en charge LACP. Ajouter des liens Gigabit entre ces équipements et les agréger avec LACP aux deux extrémités augmente le débit cumulé. L’équilibrage répartit les flux, mais le débit d’un flux unique reste limité à un lien.

> ✓ **RÉPONSE À RETENIR**
>
> Ajouter et agréger en LACP des liens Gigabit entre ESX-1 et SW3-1 pour augmenter le débit cumulé disponible.

Mission B.2

Question B.2.1. À partir de l’extrait du journal fourni pour SRV-IIS-1, argumenter pour confirmer qu’il s’agit d’une activité suspecte.

Les lignes montrent des requêtes GET répétées depuis la même adresse, 180.222.224.52, et horodatées à la même seconde. Le journal complet contient plusieurs milliers de requêtes de même nature. Les paramètres des URL paraissent aléatoires et les référents comme les agents utilisateurs varient fortement. Ce profil est peu compatible avec une navigation ordinaire et évoque un trafic automatisé. Les réponses HTTP 200 montrent que le serveur traite les requêtes, sans suffire à prouver à elles seules une attaque.

> ✓ **RÉPONSE À RETENIR**
>
> Le trafic est suspect et automatisé : des milliers de requêtes GET proviennent de 180.222.224.52.

a.

Question B.2.2. À court terme, indiquer sur quel appareil de l’infrastructure intervenir et quel type de configuration réaliser pour bloquer l’activité suspecte toujours en cours.

Pour bloquer l’activité en cours, intervenir sur le pare-feu FW-1, qui filtre les échanges entre le réseau du serveur Web et les réseaux externes. Ajouter une règle de refus ciblant l’adresse source 180.222.224.52 et la destination SRV-IIS-1, sur les ports HTTP et HTTPS concernés. Journaliser les blocages, puis vérifier que les requêtes suspectes cessent tout en maintenant l’accès légitime au site. La règle doit être limitée à cette source et à cette destination.

✓ RÉPONSE À RETENIR

Sur FW-1, refuser et journaliser les connexions de 180.222.224.52 vers SRV-IIS-1 sur les ports Web.

b.

Question B.2.2. À plus long terme, proposer une solution matérielle et/ou logicielle permettant d'automatiser la détection et le blocage de ce type d'activité.

Déployer un pare-feu applicatif Web (WAF), ou un système de prévention d'intrusion configuré pour analyser le trafic HTTP. Il peut repérer les volumes ou motifs anormaux, puis bloquer automatiquement les requêtes ou adresses sources concernées. Des seuils de fréquence, une durée de blocage limitée et des alertes à l'équipe support facilitent la réponse. Il faut ajuster et surveiller les règles afin de réduire le risque de bloquer des utilisateurs légitimes.

✓ RÉPONSE À RETENIR

Mettre en place un WAF ou un IPS qui détecte les requêtes anormales et bloque automatiquement les sources suspectes.

a.

Question B.3.1. À la lecture du courriel d'alerte envoyé par la plateforme de supervision, identifier le ou les composants concernés.

L'alerte identifie l'hôte SRV-SQL-1 et son stockage RAID. Le disque physique 1I:1:4, situé dans le groupe miroir 1, est signalé en échec. Le contrôleur Smart Array P840 et sa batterie ou son condensateur sont indiqués comme opérationnels. Le volume logique 1 de l'array A, de 3,6 To, est en mode « Interim Recovery ». Les composants concernés sont donc le serveur, son array RAID et le disque défaillant.

✓ RÉPONSE À RETENIR

Composants concernés : SRV-SQL-1, l'array RAID A et le disque physique 1I:1:4 du groupe miroir 1.

b.

Question B.3.1. Proposer une catégorie pour cet événement en vous appuyant sur la liste des catégories et sous-catégories fournie.

L'événement concerne une panne physique de stockage sur un serveur, et non une erreur logicielle ou un problème d'accès. Dans l'arborescence du document B6, la catégorie la plus précise correspond au matériel de type serveur, sous-catégorie disque. Cette qualification décrit directement le composant déclaré en échec dans l'alerte et facilite le classement ainsi que le suivi du ticket.

✓ RÉPONSE À RETENIR

Catégorie à enregistrer : Matériel > Serveur > Disque.

---

c.

Question B.3.1. Proposer une priorité pour cet événement et argumenter ce choix à l'aide de la matrice de priorisation des incidents.

Le disque est en panne et le RAID fonctionne en mode « Interim Recovery », mais l'alerte ne signale pas d'interruption du serveur SQL : le contrôleur et les autres disques sont opérationnels. L'impact est donc moyen, car l'incident touche un composant important sans indisponibilité avérée du service. L'urgence est élevée : une autre défaillance pourrait aggraver la situation et menacer les données. Dans la matrice, urgence élevée et impact moyen correspondent à la priorité 2.

✓ RÉPONSE À RETENIR

Priorité 2 : impact moyen, car le service reste actif, et urgence élevée en raison du risque d'aggravation.

---

a.

Question B.3.2. Indiquer les informations à rechercher dans la base de données de gestion de configuration pour préparer l'intervention.

Consulter la CMDB pour connaître les éléments nécessaires à l'identification du matériel, aux précautions de l'intervention et à l'évaluation de ses conséquences.

- Serveur concerné : modèle, numéro de série, emplacement et contacts responsables.
- Disque : baie, référence compatible, garantie et modalités de remplacement à chaud.
- Relations avec le volume RAID, les services hébergés et les autres composants.
- Criticité, sauvegardes, fenêtre de maintenance, interventions et incidents précédents.

✓ RÉPONSE À RETENIR

Vérifier l'identification et l'emplacement du serveur, le disque et sa baie, les dépendances, les sauvegardes et l'historique des interventions.

---

b.

Question B.3.2. Rédiger un courriel à destination de l'administrateur système présentant le diagnostic ainsi que les conséquences et les risques prévisibles, afin de planifier une intervention.

Objet : Intervention sur le RAID dégradé de SRV-SQL-1
Bonjour,
Centreon signale un disque défaillant, le 1I:1:4, dans l'array RAID A de SRV-SQL-1. Le volume logique est en

mode « Interim Recovery » ; le contrôleur et sa batterie sont opérationnels. Merci de prévoir rapidement le remplacement du disque et le contrôle de la reconstruction du RAID. Une nouvelle défaillance pourrait entraîner une indisponibilité des données ou du service SQL. Pouvez-vous vérifier les sauvegardes et proposer un créneau d'intervention ?
Cordialement,
Équipe support

> ✓ **RÉPONSE À RETENIR**
>
> Demander à l'administrateur de planifier le remplacement rapide du disque 1I:1:4 et de vérifier la reconstruction RAID.

---

a.

Question B.3.3. Justifier la qualification de cet incident récurrent en problème, au sens du référentiel ITIL.

En ITIL, un incident correspond à une interruption ou à une dégradation d'un service ; un problème désigne la cause, connue ou à rechercher, d'un ou plusieurs incidents. Ici, un événement similaire s'est produit quatre fois en six mois sur le même appareil. Cette récurrence justifie d'ouvrir un problème pour rechercher une cause commune, au lieu de se limiter au rétablissement ponctuel après chaque incident.

> ✓ **RÉPONSE À RETENIR**
>
> Ouvrir un problème ITIL : quatre incidents similaires en six mois sur le même appareil indiquent une cause récurrente à rechercher.

---

b.

Question B.3.3. Lister les recherches à réaliser et les étapes nécessaires pour résoudre durablement le problème.

Rechercher la cause racine à partir des incidents récurrents, puis valider et documenter une correction durable.

1. Comparer les tickets, journaux RAID, diagnostics matériels et changements antérieurs.
2. Examiner les disques, le contrôleur, le câblage et les conditions de fonctionnement pour identifier une cause commune.
3. Vérifier les sauvegardes, choisir une solution, puis planifier et réaliser le changement selon la procédure.
4. Contrôler la reconstruction et la stabilité du RAID, surveiller l'équipement, puis mettre à jour la CMDB et la base de connaissances.

> ✓ **RÉPONSE À RETENIR**
>
> Analyser les incidents et les journaux, trouver la cause racine, appliquer puis vérifier une correction permanente et documenter le résultat.

3. Migration vers le cloud

La DSI compare la location actuelle d'une armoire technique au centre de données avec l'hébergement des machines virtuelles dans le cloud, en analysant les coûts et les conséquences pour l'administration et l'exploitation. Une machine virtuelle Web a déjà été créée dans le cloud, et il faut choisir comment rendre rapidement le site accessible aux personnes chargées des tests.

Mission C.1

Question C.1.1. Expliquer pourquoi certains coûts relatifs à la location de l'armoire technique ne sont pas facturés à ModePrivee.Shopping par le centre de données.

Le document indique que les liens fibre optique et le service « gestes de proximité » ne sont pas facturés. Les cross-connects servent notamment à relier des armoires ou des partenaires : aucun coût de ce type n'est donc ajouté ici. De plus, la DSI est située à moins de 2 km du centre de données et peut intervenir rapidement sur ses équipements. Elle n'a donc pas besoin de demander au personnel du centre de données les manipulations facturables de proximité.

> ✓ **RÉPONSE À RETENIR**
>
> Aucun coût de cross-connect ni de gestes de proximité : les liens sont indiqués « néant » et la DSI intervient elle-même.

Question C.1.2. Calculer le coût de revient total de l'armoire technique sur cinq ans, en prenant en compte les éléments facturés par le centre de données et le matériel renouvelé tous les cinq ans.

Poste sur 5 ans	Calcul	Coût
Loyer	2 500 × 12 × 5	150 000 €
Électricité	1 000 × 5	5 000 €
Matériel	15 000 + 5 000 + 3 000 + 2 000	25 000 €
Total	150 000 + 5 000 + 25 000	180 000 €

Le loyer est mensuel et l'électricité est chiffrée à l'année : chacun est donc multiplié par sa durée sur cinq ans. Le matériel acheté par l'entreprise comprend quatre serveurs de virtualisation, une baie de stockage, un commutateur et un pare-feu. Ces montants représentent le coût de revient sur la période, avec le renouvellement du matériel prévu au terme des cinq ans.

> ✓ **RÉPONSE À RETENIR**
>
> Coût de revient total de l'armoire technique sur cinq ans, matériel inclus : 180 000 €.

Question C.1.3. Calculer le coût d'hébergement sur cinq ans des machines virtuelles dans le cloud, en incluant les serveurs Web, les serveurs de bases de données et le serveur d'authentification nécessaire.

Le parc actuel comporte deux serveurs SQL et deux serveurs Web IIS. Le coût annuel est donc de 2 × 12 000 € pour SQL, 2 × 5 000 € pour IIS et 1 000 € pour le contrôleur de domaine nécessaire. Le total annuel atteint 35 000 €. Sur cinq ans, le coût d'hébergement des machines virtuelles est calculé ainsi : (2 × 12 000 + 2 × 5 000 + 1 000) × 5.

> ✓ RÉPONSE À RETENIR
>
> Le coût estimé d'hébergement des cinq machines virtuelles dans le cloud sur cinq ans est de 175 000 €.

a.

Question C.1.4. Identifier les avantages et les inconvénients de la solution cloud d'un point de vue économique et financier.

Sur cinq ans, l'estimation cloud atteint 175 000 €, contre 180 000 € pour l'armoire et le matériel : l'écart calculé est faible et favorable au cloud. La comparaison repose sur les postes chiffrés dans le sujet et ne permet pas d'évaluer d'éventuels frais supplémentaires liés au contrat ou à la migration.

- **Avantage :** pas d'investissement initial à renouveler pour le matériel de l'armoire.
- **Inconvénient :** coût récurrent d'hébergement, susceptible d'évoluer avec les tarifs et les ressources consommées.

> ✓ RÉPONSE À RETENIR
>
> Le cloud est estimé 5 000 € moins cher sur cinq ans, mais ses frais récurrents et leurs évolutions restent à surveiller.

b.

Question C.1.4. Identifier les avantages et les inconvénients de la solution cloud en termes d'administration des serveurs.

La migration réduit les interventions de la DSI sur les équipements physiques, ce qui répond à l'objectif de recentrer l'équipe sur le développement. Le fournisseur prend en charge l'infrastructure physique nécessaire à l'hébergement. En revanche, l'offre décrite porte sur des machines virtuelles : il faut donc toujours administrer les systèmes d'exploitation, les serveurs Web et SQL, leurs mises à jour et leur sécurité. La répartition exacte des tâches dépend du service inclus dans le contrat cloud.

> ✓ RÉPONSE À RETENIR
>
> La gestion du matériel physique diminue, mais l'administration des systèmes et des applications reste nécessaire selon le contrat cloud.

c.

Question C.1.4. Identifier les avantages et les inconvénients de la solution cloud en termes de fonctionnement, notamment pour la disponibilité des ressources et les performances.

Le cloud peut fournir des ressources hébergées par un opérateur spécialisé, mais le sujet ne précise ni niveau de disponibilité garanti ni performance contractuelle. Il faut donc distinguer les possibilités de la solution des engagements réellement souscrits.

- **Avantage :** les ressources peuvent être accessibles depuis le siège sans intervention sur les serveurs du centre de données.
- **Inconvénients :** l'accès dépend de la connexion réseau et du fournisseur ; les performances dépendent des ressources allouées et de la latence. Disponibilité et capacité doivent être vérifiées dans le contrat.

> **✓ RÉPONSE À RETENIR**
>
> Le cloud peut faciliter l'accès aux ressources, mais disponibilité et performances dépendent du réseau, des ressources allouées et des engagements du fournisseur.

d.

Question C.1.4. Identifier les avantages et les inconvénients de la solution cloud en termes d'évolutivité de l'infrastructure.

Pour une plateforme de développement et de tests, le cloud permet généralement de créer ou d'ajuster des machines virtuelles sans acheter et installer de nouveaux serveurs physiques. Cette souplesse facilite l'adaptation de la capacité aux besoins. Elle n'est toutefois pas illimitée : les ressources disponibles, les quotas et les conditions tarifaires dépendent de l'offre souscrite. Une dépendance forte à la plateforme peut aussi rendre une migration vers un autre fournisseur plus complexe.

> **✓ RÉPONSE À RETENIR**
>
> Le cloud facilite l'ajustement de la capacité, dans les limites des ressources, des quotas et des conditions du fournisseur.

Mission C.2

Question C.2.1. Choisir entre intervenir sur le serveur DNS hébergeant la zone ModePrivee.Shopping et configurer une redirection HTTP sur l'ancien serveur Web. Justifier la solution retenue au regard de la contrainte de mise à disposition rapide du site sur la nouvelle machine virtuelle.

Pour rendre le site rapidement accessible, configurer une redirection HTTP sur l'ancien serveur Web vers la nouvelle machine virtuelle cloud. Les testeurs conservent ainsi l'adresse habituelle et la modification agit sans attendre la mise à jour des caches DNS. Cette solution exige que l'ancien serveur reste disponible pour recevoir les demandes et transmettre les visiteurs vers le nouveau site. Elle répond donc plus directement à la contrainte de mise à disposition rapide que la modification DNS.

✓ RÉPONSE À RETENIR

Configurer une redirection HTTP sur l’ancien serveur Web vers le site de la nouvelle machine virtuelle dans le cloud.

Ce qu'il faut retenir de ce sujet (Session 2019)

Bilan de l'épreuve : Épreuve BTS Services informatiques aux organisations, E5, session 2019, code SI5SISR, durée quatre heures, coefficient 5. Le cas ModePrivee.Shopping étudie la refonte d'une plateforme de développement et de tests, son support opérationnel et une migration vers le cloud. Les compétences évaluées couvrent les réseaux, la sécurité, la supervision, ITIL, l'analyse des coûts et le choix de solutions.

Notions-clés, formules & règles à maîtriser

- Un VLAN sépare logiquement des équipements ; chaque sous-réseau doit disposer d'un plan d'adressage et d'une passerelle cohérents.
- Un trunk 802.1Q transporte plusieurs VLAN ; les VLAN autorisés doivent être configurés de façon cohérente sur les liens.
- La priorité d'un incident se détermine en croisant son urgence et son impact selon la matrice fournie.
- Comparer des coûts sur cinq ans suppose de cumuler les dépenses récurrentes et les investissements matériels concernés.

Points de vigilance & attentes du jury

- Distinguer les fonctions de commutation et de routage pour justifier le remplacement des équipements.
- Vérifier les sous-réseaux, masques, passerelles et VLAN autorisés sur les trunks avant de diagnostiquer les pings.
- Appuyer le diagnostic d'activité suspecte sur des éléments observables des journaux, sans présenter un indice comme une preuve définitive.
- Pour les calculs de coût, expliciter les quantités, la durée retenue et les coûts inclus ou non facturés.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment organiser un calcul de coût sur cinq ans ?

Séparez les dépenses ponctuelles des dépenses récurrentes. Multipliez les tarifs mensuels ou annuels par la durée correspondante, ajoutez les achats matériels concernés et vérifiez quelles prestations sont explicitement facturées.

Q : Comment repérer une erreur de configuration VLAN à partir de tests réseau ?

Comparez les tests entre hôtes et passerelles, puis vérifiez l'appartenance des ports, l'encapsulation 802.1Q et la liste des VLAN autorisés sur chaque trunk. Contrôlez également l'état des interfaces virtuelles commutées.

Q : Comment gérer le temps dans cette épreuve de quatre heures ?

Les trois dossiers indépendants valent respectivement 45, 35 et 20 points. Répartissez le temps selon leur poids, répondez à chaque question et gardez quelques minutes pour vérifier les calculs, les justifications et les réponses rédigées.

Q : Quels critères faut-il respecter pour qualifier et prioriser un incident ?

Identifiez les composants concernés et sélectionnez une catégorie dans la nomenclature fournie. Évaluez séparément l'urgence et l'impact, croisez-les dans la matrice, puis justifiez la priorité avec les informations de l'alerte.

Sujet officiel associé (PDF) : https://coursbtssio.fr/assets/annales/bts-sio/E5 - Administration des systèmes et des réseaux (spécifique à l'option)/2019/BTS SIO - E5 - Administration des systèmes et des réseaux (spécifique à l'option) - Session 2019 - 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.