Guide de référence rapide sur les lignes directrices de STAR relatives à l'infrastructure des concessionnaires

2025

Table des matières

Introduction

Aperçu

Ce document de référence abrégé est destiné à être jumelé avec le document intitulé *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires*. Pour plus d'informations sur l'un ou l'autre des sujets abordés dans ce guide de référence, veuillez vous référer aux *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires*.

Avis de non-responsabilité

Tout nom d'entreprise, application, lien de site Web ou référence technologique figurant dans le présent document ne doit pas être considéré comme une approbation par les fabricants d'équipement d'origine ou par STAR, à moins que cette approbation ne soit expressément mentionnée.

Le présent document fournit une spécification de base ou une ligne directrice pour les concessionnaires afin de leur permettre d'établir la communication par Internet. Il est important de noter que l'infrastructure du réseau, les données du concessionnaire et la sécurité du système relèvent de la responsabilité de la concession. Des organisations tierces, telles que des prestataires de services et des partenaires, peuvent fournir des conseils et des recommandations. Certaines organisations peuvent fournir des logiciels, du matériel ou des éléments de réseau propriétaires pour aider à simplifier les opérations du réseau. Toutefois, ces applications, recommandations ou outils ne remplacent pas la gestion du réseau.

Recommandations matérielles

Ordinateurs de bureau, ordinateurs portables et tablettes

Les recommandations de STAR pour les ordinateurs de bureau, les ordinateurs portables et les tablettes des concessionnaires ne sont plus axées sur des exigences matérielles globales. Cette évolution s'explique principalement par les progrès de la puissance de traitement du matériel, le passage à l'informatique en nuage et l'omniprésence de la mobilité. STAR recommande que les besoins matériels soient déterminés sur la base d'un scénario d'utilisation fondé sur les tâches à accomplir. Lors de l'achat de nouveaux appareils, il faut tenir compte des facteurs suivants :

1. **Mobilité :** certaines fonctions au sein d'une concession requièrent de la mobilité. D'autres fonctions sont exercées principalement dans un seul lieu. Tenez compte des besoins en matière de mobilité lors de l'achat d'un nouvel appareil. Gardez également à l'esprit que de nombreux appareils mobiles, tels que les tablettes, fonctionnent avec des logiciels particuliers qui peuvent ne pas être compatibles avec l'ensemble du matériel et des logiciels requis. Il faut tenir compte des exigences matérielles et logicielles avant de décider si une tablette, un ordinateur portable ou un ordinateur de bureau est le meilleur choix pour une fonction donnée.
2. **Exigences logicielles :** les fonctions exercées au sein de la concession nécessitent une interaction avec différents logiciels. Les logiciels sont souvent conçus pour des systèmes d'exploitation et des navigateurs Internet précis. Les applications logicielles peuvent également exiger une configuration matérielle de base. Lors de l'achat d'un nouvel appareil, il faut comprendre le logiciel qu'il utilisera et les exigences requises pour le faire fonctionner.
3. **Exigences relatives aux accessoires matériels :** les concessionnaires ont souvent besoin d'accessoires particuliers pour remplir une fonction. Des outils d'aide à la vente, des diagnostics de service et d'autres adaptateurs physiques sont nécessaires pour des cas d'utilisation précis. Ces accessoires sont souvent conçus en fonction de spécifications logicielles et matérielles particulières. Si la fonction d'antivol nécessite un accessoire particulier, il faut vérifier les exigences auprès du fournisseur avant d'acheter un nouvel équipement.
4. **Exigences des fabricants d'équipement d'origine, des fournisseurs de systèmes pour les concessionnaires et des tiers :** les fabricants d'équipement d'origine, les fournisseurs de services aux concessionnaires et d'autres fournisseurs tiers déploient souvent des technologies propres aux concessions. Ces technologies (matériel ou logiciel) peuvent nécessiter des caractéristiques précises pour fonctionner de manière efficace. Si un appareil de concession utilise des technologies particulières, il faut vérifier auprès du fournisseur de ces technologies.
5. **Fiabilité :** la fiabilité des appareils doit être prise en compte lors de l'achat de matériel. Certaines activités de la concession, telles que l'environnement de service, sont plus sujettes aux défaillances des appareils. Certaines fonctions sont plus sensibles aux temps d'arrêt des appareils. Pour déterminer quoi acheter et à quel moment, il faut tenir compte de la probabilité d'une défaillance de l'appareil et des conséquences qu'une telle défaillance peut avoir sur la fonction concernée et sur les activités de la concession.

Au-delà des recommandations relatives aux cas d'utilisation, STAR peut fournir des conseils sur le choix du matériel à acheter et sur le moment de l'achat. STAR fournit des conseils sur le moment où il convient d'acheter du nouveau matériel à la section 2.2.a du document *Lignes directrices de STAR sur l'infrastructure des concessionnaires*. Pour déterminer ce qu'il convient d'acheter, STAR fournit des conseils sur les achats de matériel destiné aux consommateurs ou aux entreprises à la section 2.2.b. et un guide pour les tablettes et les appareils mobiles à la section 2.2.d.

STAR fournit également à la section 2.2.c des lignes directrices sur l'infrastructure des concessionnaires, et des conseils et des spécifications concernant les routeurs et les commutateurs qui permettent de connecter le matériel du réseau.

Pour plus de renseignements sur les recommandations relatives au matériel des concessionnaires, y compris les tablettes, la mobilité, la mise hors service et le recyclage du matériel, veuillez consulter la section 2.2. des *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires.*

Recommandations logicielles

Systèmes d'exploitation

Vous trouverez ci-dessous une liste des systèmes d'exploitation les plus courants sur le marché. Certaines applications ne sont pas compatibles avec des systèmes d'exploitation particuliers. Il est recommandé aux concessionnaires de consulter leurs fabricants d'équipement d'origine, leurs fournisseurs de systèmes pour les concessionnaires et d'autres fournisseurs pour déterminer quel navigateur utiliser. Veuillez noter que Microsoft a mis fin au soutien des systèmes d'exploitation XP, Vista et Windows 7, y compris les mises à jour de sécurité critiques. STAR recommande aux concessions de ne pas utiliser Windows XP, Vista ou Windows 7.

Systèmes d'exploitation clients courants	**Dernière mise à jour ou ensemble de modifications provisoires* (Service Pack)**	**Fin du soutien général**	**Fin du soutien prolongé**
Windows XP	Service pack 3	14 avril 2009	8 avril 2014
Windows Vista	Service pack 2	10 avril 2012	11 avril 2017
Windows 7	Service pack 1	13 janvier 2015	14 janvier 2020
Windows 8	Windows 8.1	9 janvier 2018	10 janvier 2023
Windows 10	22H2	13 octobre 2020	14 octobre 2025
Windows 11	24H2		
MAC OS X	15.1.1	Les versions 14 et inférieures ne sont plus prises en charge	Les versions 14 et inférieures ne sont plus prises en charge
iOS (pour iPad et iPhone)	18.2		
Android	15		

**** Dernières mises à jour/Service Pack en date de janvier 2025***

Navigateurs Internet

Vous trouverez ci-dessous une liste des navigateurs Internet les plus courants sur le marché actuellement. Certaines applications ne sont pas compatibles avec des navigateurs spécifiques. D'autres applications nécessitent des paramètres de navigateur précis, tels que le mode de compatibilité. Il est recommandé aux concessionnaires de consulter leurs fabricants d'équipement d'origine, leurs fournisseurs de systèmes pour les concessionnaires et d'autres fournisseurs pour déterminer quel navigateur utiliser.

Navigateur	Dernière mise à jour ou Service Pack*	Remarques
Apple Safari	17	Non recommandé pour les systèmes d'exploitation Microsoft
Google Chrome	131	
Internet Explorer	11	Internet Explorer a été retiré en juin 2022 Microsoft Edge est le navigateur recommandé par Microsoft
Microsoft Edge	1131	
Mozilla Firefox	133	

**** Dernières mises à jour/Service Pack en date de janvier 2020***

Pour plus d'informations sur les recommandations relatives aux logiciels des concessions, veuillez consulter la section 2.3 des *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires*.

Configuration et gestion du réseau

Caractéristiques du réseau local	
Réseau local	Gigabit Ethernet
Câblage de données	Le câblage du réseau de données existant doit être de catégorie 5e, au minimum, et être conforme à la norme TIA-568-A. La catégorie 6a doit être utilisée pour le câblage neuf. Les câbles horizontaux ne doivent pas dépasser 90 mètres (295 pieds). Il est fortement recommandé de remplacer les câbles de données par des câbles en fibre optique lorsque la longueur dépasse 295 pieds.
Emplacement de l'équipement	L'équipement utilisé pour le réseau local doit être installé dans une armoire de câblage ou dans une salle de communication. Tous les équipements doivent être montés ou fixés sur un support ou une étagère.
Adressage IP	Le fournisseur de services Internet de la concession doit fournir un adressage IP pouvant être acheminé (« routable »). Pour le réseau local du concessionnaire, l'adressage dynamique (DHCP) doit être utilisé pour faciliter l'assistance.
Adaptateur de réseau	Gigabit Ethernet
Commutation Ethernet	Commutateur gigabit géré. Étiquetez chaque interface et chaque câble. Vous gagnerez ainsi du temps lorsque vous devrez retrouver des câbles de réseau dans le cadre d'une demande d'assistance ou d'une nouvelle installation.
Routeurs	Routeur professionnel. Les routeurs doivent prendre en charge la traduction d'adresses de réseau (NAT) et la technologie d'analyse de procédé (TAP). Les routeurs doivent également prendre en charge le routage dynamique à l'aide de RIPv2, OSPF et BGP. - Modifiez le mot de passe de l'appareil au moment de l'installation et de façon régulière. - Conservez une configuration de sauvegarde dans vos dossiers en cas de défaillance du logiciel ou de remplacement du matériel.
Pare-feu	Dispositif de sécurité entièrement géré qui surveille en permanence les menaces par le biais d'un système de détection d'intrusion (SDI) et d'un système de prévention d'intrusion (IPS), et d'autres mécanismes, tels que le filtrage des paquets, l'antivirus et l'inspection dynamique des paquets.
	– Les pare-feu doivent prendre en charge la traduction d'adresses de réseau (NAT) et la technologie d'analyse de procédé (TAP). Les pare-feu doivent également prendre en charge le routage dynamique à l'aide des protocoles RIPv2, OSPF et BGP.
	– Modifiez le mot de passe de l'appareil au moment de l'installation et de façon régulière.
	– Conservez une configuration de sauvegarde dans vos dossiers en cas de défaillance du logiciel ou de remplacement du matériel.
	– Pour en savoir plus sur les pare-feu et la sécurité du réseau, consultez la section 2.6.

Services de noms de domaine (DNS)	Utilisez le service DNS public, sauf lorsque vous utilisez Windows Active Directory (dans ce cas, il est nécessaire de disposer d'un serveur DNS interne).

Conception de réseaux sans fil	
Recommandation	**Caractéristiques**
Matériel sans fil	Seuls des points d'accès de qualité professionnelle doivent être utilisés. Les points d'accès de qualité professionnelle sont conçus pour offrir des fonctions d'itinérance et d'autres fonctions professionnelles (telles que les VLAN ou les identifiants SSID multiples) nécessaires à la prise en charge des dispositifs sans fil pour les applications. Les points d'accès sans fil de qualité professionnelle sont également conçus pour accueillir un plus grand nombre de connexions que le matériel de qualité grand public.
Segmentation du réseau	Les concessions doivent s'assurer que le trafic des invités est séparé du réseau de la concession par des VLAN ou une connexion Internet distincte.
Identifiants SSID	Il est recommandé aux concessions d'utiliser des identifiants SSID distincts pour les différentes fonctions de l'entreprise (c.-à-d. ventes, service après-vente et administration). Toutefois, les concessions ne doivent pas confondre les identifiants SSID avec la segmentation du réseau. En général, les identifiants SSID ne séparent pas le trafic du réseau, mais fournissent seulement un moyen différent de se connecter au réseau.
Couverture	Déployez des points d'accès sans fil pour assurer une couverture adéquate. Les outils sans fil peuvent fournir la puissance du signal autour du bâtiment. Faites attention aux structures ou aux objets qui peuvent interférer avec la couverture sans fil (interférences électriques, interférences de fréquence radio ou matériaux physiques, tels que les métaux ou le béton).
Authentification et chiffrement	Liaison WPA2 (Wi-Fi Protected Access II) avec authentification RADIUS et chiffrement AES. Remarque : consultez les recommandations du fabricant d'équipement d'origine pour obtenir des conseils sur la compatibilité avec les technologies propres au fabricant d'équipement d'origine.
Norme de réseau	802.11ax ou 802.11ac
Détection sans fil indésirable	Analysez, identifiez et supprimez tous les points d'accès sans fil indésirables qui pourraient se trouver sur le réseau de la concession. – Un point d'accès sans fil indésirable est défini comme un point d'entrée sans fil dans le réseau de la concession qui n'a pas été autorisé ou sécurisé par le concessionnaire, la direction des TI et le propriétaire. – Tous les réseaux sans fil indésirables doivent être détectés, repérés et supprimés immédiatement. – STAR recommande l'utilisation d'un service de détection sans fil géré qui analyse en permanence le réseau pour détecter les menaces liées au réseau sans fil.

Mobilité de la concession	
Recommandations	**Caractéristiques**
Mobilité au sein de la concession	Utilisez un réseau maillé sans fil pour que les utilisateurs finaux puissent se déplacer sur le site sans perdre la connexion et sans avoir à s'authentifier à nouveau.
Contrôleurs sans fil	Un contrôleur de réseau local sans fil peut être utilisé en combinaison avec le protocole LWAPP (Lightweight Access Point Protocol) pour gérer des points d'accès allégés sur le réseau de la concession. La couverture, la fiabilité et l'efficacité du réseau s'en trouveront renforcées.

Accès des clients	
Recommandations	**Caractéristiques**
Priorisation du trafic	Les concessions doivent utiliser un pare-feu ou un autre mécanisme pour limiter la consommation de bande passante des invités. Ainsi, l'accès des visiteurs n'interfère pas avec les activités de l'entreprise en consommant trop de bande passante.
Authentification des invités et conditions d'utilisation	STAR recommande aux concessions d'utiliser un portail captif exigeant des invités qu'ils acceptent les conditions d'utilisation de la concession. Il peut s'agir de restrictions de contenu, de limitations de la bande passante et d'accords d'utilisation.
Bande passante Internet	Pour s'assurer que la concession dispose d'une largeur de bande passante suffisante, le concessionnaire doit choisir la bonne technologie et la bonne vitesse. (Pour en savoir plus sur les technologies et la bande passante Internet, consultez les sections 2.5.a et 2.5.b des *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires.*) – STAR recommande également à chaque concession de disposer d'une connexion Internet de secours provenant d'un autre fournisseur et utilisant une technologie différente. – Voir la section 2.5.c pour des recommandations sur les connexions de sauvegarde Internet.

Pour plus d'informations sur la gestion et la configuration des réseaux, veuillez consulter la section 2.4 des *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires*.

Sécurité

	Sécurité du réseau
Pare-feu/UTM (gestion unifiée des menaces)	Dispositif de sécurité entièrement géré qui surveille en permanence les menaces par le biais d'un système de détection d'intrusion (SDI), d'un système de prévention d'intrusion (IPS) et d'autres mécanismes. L'appareil doit également présenter les caractéristiques suivantes : • Des mécanismes, comme le filtrage de paquets, l'antivirus et l'inspection dynamique de paquets; • Le filtrage des paquets et des protocoles (p. ex. IP, ICMP); • L'analyse de l'antivirus; • L'inspection des connexions en fonction de leur état; • L'exécution d'opérations mandataires sur les applications sélectionnées; • Les rapports sur le trafic autorisé et refusé par le dispositif de sécurité sur une base régulière (c.-à-d. mensuellement). En raison de l'importance du pare-feu et du fait qu'il se trouve souvent sur le chemin des données pour la plupart du trafic de la concession, STAR recommande l'utilisation d'un dispositif de secours en cas de défaillance. Pour limiter les temps d'arrêt, les concessionnaires doivent envisager une solution de basculement automatique vers le dispositif de secours en cas de défaillance matérielle.
Segmentation du réseau	Les informations relatives aux cartes de paiement, aux clients, au trafic de la concession et au trafic des clients doivent être séparées par le biais d'une segmentation du réseau (telle que le VLAN) ou d'un réseau différent (comme un circuit dédié pour les invités) afin de garantir la sécurité des données.
Filtrage de contenu	La perte de données peut résulter du fait que les employés naviguent sur Internet pour des activités non liées à l'entreprise. STAR recommande aux concessions de filtrer le contenu du réseau afin d'éliminer tout trafic potentiellement nuisible, inapproprié ou non lié aux activités de l'entreprise.
Gestion des informations et des événements de sécurité (GIES)	Surveillance proactive des événements en temps réel qui utilise un service GIES. La GIES doit être en mesure de recueillir des données et avoir la capacité d'agréger et de mettre en corrélation des données de sécurité variables provenant du réseau en temps réel. Le fournisseur de services de GIES doit être en mesure d'avertir l'administrateur du réseau en cas d'événement de sécurité et de fournir la documentation appropriée à des fins de conformité. L'objectif fondamental d'un service de GIES est de contribuer à l'identification ou à la prévention d'une intrusion dans un réseau. Une réponse immédiate à une violation peut réduire ou prévenir la perte de données de manière significative.
Système de détection sans fil	Analysez, identifiez et supprimez les points d'accès sans fil indésirables qui pourraient se trouver sur le réseau du détaillant. Un point d'accès sans fil indésirable est défini comme un point d'entrée sans fil dans le réseau de la concession qui n'est pas autorisé, sécurisé ou connu des services informatiques, de la direction et des propriétaires du concessionnaire. ○ Tous les réseaux sans fil indésirables doivent être détectés, repérés et supprimés sans délai. ○ STAR recommande l'utilisation d'un service de détection sans fil géré qui analyse en permanence le réseau pour détecter les menaces liées au réseau sans fil.

Tests d'intrusion et analyse des vulnérabilités	Il est vivement recommandé d'effectuer chaque année des tests d'intrusion internes et externes sur le réseau des concessionnaires. Un test d'intrusion est une méthode d'évaluation de la sécurité d'un système informatique ou d'un réseau qui consiste à simuler une attaque provenant d'une source malveillante. Un test d'intrusion doit être effectué sur tout système informatique destiné à être déployé dans un environnement en réseau, en particulier ceux qui possèdent un accès à Internet ou qui sont exposés. Les activités de test d'intrusion peuvent être réalisées en externe (simulation d'une attaque depuis l'extérieur de votre réseau, exactement comme une tentative de piratage lancée depuis un pays étranger), ou en interne (depuis l'intérieur de votre réseau pour voir quels sont les accès et les vulnérabilités).

Recommandation	Sécurité des postes de travail
Surveillance des virus sur les ordinateurs	Des produits antivirus de qualité professionnelle doivent être installés sur tous les ordinateurs et configurés pour effectuer automatiquement les opérations suivantes : • Téléchargement et installation des mises à jour les plus récentes des signatures de virus; • Surveillance active des virus; • Mise en quarantaine et suppression des fichiers infectés; • La solution antivirus doit comprendre un antivirus, un logiciel-antiespion, une prévention d'intrusion, un contrôle d'application, un antipourriel et une détection de trousse administrateur pirate.
Gestion des correctifs	STAR recommande que la gestion des correctifs soit effectuée sur chaque ordinateur afin de s'assurer que tous les postes de travail disposent des correctifs Microsoft les plus récents. La gestion des postes de travail doit inclure la surveillance à distance des défaillances matérielles et logicielles, des pannes de serveurs, du manque d'espace disque, de l'utilisation excessive de l'unité centrale et de la mémoire.
Protection par mot de passe	Les mots de passe doivent expirer tous les 60 jours ou moins. Les concessions doivent au moins utiliser des « mots de passe forts » contenant un minimum de huit caractères et comprenant trois des quatre exigences suivantes : 1) Une majuscule; 2) Une minuscule; 3) Un caractère numérique; 4) Des caractères spéciaux.
Détection des points d'extrémité et plateforme d'intervention	• Une plateforme de protection des points d'extrémité et une solution de détection et d'intervention sur les terminaux doivent être déployées sur les points d'extrémité afin de prévenir les attaques de logiciels malveillants à partir de fichiers, de détecter les activités malveillantes et de fournir les capacités d'investigation et de remise en état nécessaires pour répondre aux incidents et aux alertes de sécurité actives. Les alertes émises par ce service doivent être traitées immédiatement afin de limiter les risques et les pertes potentielles de données. L'offre de services doit permettre une visibilité multiplateforme des activités des points d'extrémité et des serveurs, ainsi que des activités suivantes : une détection des menaces grâce à des moteurs d'IA statiques et comportementaux, et un système de détection des intrusions sur l'hôte (SDIH) au sein de l'agent du point d'extrémité; • Un confinement des menaces et un guide de remédiation; • Les rapports sur les activités et la chasse aux menaces; • La visibilité multiplateforme sur l'exécution des processus, les communications réseau, l'accès aux fichiers, les applications, les requêtes DNS et le trafic Web chiffré.

Pour plus d'informations sur les recommandations relatives aux logiciels des concessions, veuillez consulter la section 2.6 des *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires*.