
# Directives relatives à l'infrastructure des concessionnaires STAR
# Guide de référence rapide
**2020**

## Sommaire

# Introduction

## Vue d'ensemble

Ce court document de référence qui est destiné à être associé aux lignes directrices de l'infrastructure des concessionnaires STAR (DIG). Veuillez consulter le STAR DIG pour plus d'informations sur tout sujet abordé dans ce guide de référence.

## Décharge de responsabilité

Tout nom de société, application, lien de site web ou référence technologique mentionné dans ce document ne doit pas être considéré comme une approbation par les OEM ou par STAR, sauf si cette approbation est expressément mentionnée.

Ce document fournit une spécification de base ou une ligne directrice aux concessionnaires pour établir une communication sur Internet. Il est important de noter que l'infrastructure du réseau, les données des concessionnaires et la sécurité du système sont de la responsabilité du concessionnaire. Des organisations tierces telles que des prestataires de services et des partenaires peuvent fournir des conseils et des recommandations. Certaines entreprises peuvent fournir des logiciels, du matériel ou des éléments de réseau propriétaires pour aider à rationaliser les opérations du réseau. Toutefois, ces applications, recommandations ou outils ne remplacent pas la gestion du réseau.

# Recommandations sur le matériel informatique

| Ordinateurs de bureau | |
|---|---|
| **Composant** | **Spécifications** |
| **Processeur** | Intel Core i5 et au-dessus, ou équivalent AMD |
| **Mémoire (RAM)** | 4 GB ou plus |
| **Disque dur** | 500 GB ou plus |
| **Lecteur de CD/DVD** | Lecteur CD/DVD, ou lecteur externe |
| **Port de série** | 1 (Adaptateur USB facultatif) |
| **Ports USB** | 2 ou plus |
| **Adaptateur Audio** | 16 bit |
| **Haut-parleur** | Facultatif |
| **Affichage** | 1280x768 résolution minimum |
| **Adaptateur réseau** | Câblé: Gigabit (ou plus grand) Ethernet<br>Sans fil: 802.11 n ou ac |
| **Garantie** | 3 ans sur place |
| **Système d'exploitation** | Les systèmes d'exploitation Windows sont compatibles avec la plupart des applications des concessionnaires. Veuillez consulter vos partenaires OEM et technologiques lors du choix d'un système d'exploitation. |

| Ordinateurs portables | |
|---|---|
| **Composant** | **Spécifications** |
| **Processeur** | Intel Core i5 ou au-dessus, ou équivalent AMD |
| **Mémoire (RAM)** | 4 GB ou plus |
| **Disque dur** | 320 GB ou plus |
| **Lecteur CD/ DVD** | Lecteur CD/DVD, ou lecteur externe |
| **Ports USB** | 2 |
| **Haut-parleur** | facultatif |
| **Affichage** | 1280x768 résolution minimum |
| **Adaptateur réseau** | Câblé: Gigabit (ou plus grand) Ethernet<br>Sans fil: 802.11 n ou ac |
| **Garantie** | 3 ans sur place |
| **Système d'exploitation** | Les systèmes d'exploitation Windows sont compatibles avec la plupart des applications des concessionnaires. Veuillez consulter vos partenaires OEM et technologiques lors du choix d'un système d'exploitation. |

| Routeurs et commutateurs | |
|---|---|
| **Composant** | **Spécifications** |
| **Spécification Standard Ethernet** | IEEE 802.3 100baseT ou 1000baseT |
| **Redondance** | La connexion de plusieurs commutateurs ensemble devrait utiliser des liens redondants de la plus haute vitesse disponible, en utilisant STP ou rSTP pour assurer une topologie sans boucle. |
| **Alimentation électrique** | Les alimentations électriques redondantes sont recommandées pour réduire les temps d'arrêt. |
| **Vitesse** | 100 ou 1000 Mbps |
| **VLAN** | Les commutateurs avec VLAN et la technologie 802.1Q trunk doivent être utilisés pour les réseaux routés avec plusieurs sous-réseaux ou VLAN. |
| **Protocoles de gestion** | Les appareils gérés doivent prendre en charge les normes industrielles de gestion à distance telles que le protocole SNMP (Simple Network Management Protocol) et le RMON (Remote Network Monitoring). |
| **Commutateurs sans fil** | Les appareils sans fil doivent être à double bande et compatibles avec la norme IEEE 802.11b/g/n. |

Pour plus d'informations sur les recommandations en matière de matériel des concessionnaires, veuillez consulter la section 2.2 de la directive sur l'infrastructure des concessionnaires STAR (DIG)

# Recommandations sur les logiciels

## Systèmes d'exploitation

Vous trouverez ci-dessous une liste des systèmes d'exploitation les plus courants sur le marché actuel. Certaines applications ne sont pas compatibles avec des systèmes d'exploitation spécifiques. Il est recommandé aux concessionnaires de vérifier auprès de leurs OEM, DSP et autres vendeurs pour déterminer les systèmes d'exploitation à utiliser. Veuillez noter qu'à partir d'avril 2014, Microsoft a cessé de prendre en charge les systèmes d'exploitation XP. Cela inclut les mises à jour de sécurité critiques. STAR recommande aux concessionnaires de ne pas utiliser Windows XP.

| Systèmes d'exploitation clients communs actuels | Dernière mise à jour ou Service Pack*. | Fin d'assistance générale | Fin de l'assistance prolongée |
|---|---|---|---|
| **Windows XP** | Service Pack 3 | 14-Apr-09 | 8-Apr-14 |
| **Windows Vista** | Service Pack 2 | 10-Apr-12 | 11-Apr-17 |
| **Windows 7** | Service Pack 1 | 13-Jan-15 | 14-Jan-20 |
| **Windows 8** | Windows 8.1 | 9-Jan-18 | 10-Jan-23 |
| **Windows 10,** | N/A | 13-Oct-20 | 14-Oct-25 |
| **MAC OS X** | 10.9 (ou supérieur pris en charge) 10.11 | Versions 10.8 (Mountain Lion) et antérieurs ne sont plus pris en charge | Versions 10.8 (Mountain Lion) et antérieurs ne sont plus pris en charge |
| **IOS (pour iPad et iPhone)** | 9.1 | | |
| **Android** | 5 | | |

**** Dernières mises à jour / Service Pack en novembre 2015***

## Navigateurs Internet

Vous trouverez ci-dessous une liste des navigateurs internet les plus courants sur le marché actuel. Certaines applications ne sont pas compatibles avec des navigateurs spécifiques. D'autres applications nécessitent des paramètres de navigateur spécifiques, tels que le mode de compatibilité. Il est recommandé aux concessionnaires de vérifier auprès de leurs OEM, DSP et autres vendeurs pour déterminer les systèmes d'exploitation à utiliser.

**** Dernières mises à jour / Service Pack en janvier 2019***

| Navigateur | Dernière mise à jour ou service pack* | Remarques |
|---|---|---|
| **Google Chrome** | 71 | |
| **Mozilla Firefox** | 64 | |
| **Internet Explorer** | 11 | |
| **Apple Safari** | 12 | Utilisation non recommandée sur les systèmes d'exploitation Microsoft |
| **Opera** | 57 | |
| **Edge** | 18 | |

Pour plus d'informations sur les recommandations en matière de logiciels pour distributeurs, veuillez consulter la section 2.3 de la directive STAR sur l'infrastructure des concessionnaires (DIG)

## Configuration et gestion du réseau

| | Spécifications LAN |
|---|---|
| **Réseau local** | Gigabit Ethernet |
| **Câblage de données** | Le câblage des réseaux de données existants devrait être - au minimum - conforme aux normes TIA-568-A Catégorie 5e. La catégorie 6a doit être utilisée pour le nouveau câblage. Aucun câble horizontal ne doit dépasser 90 mètres (295 pieds). Il est fortement recommandé d'utiliser des câbles en fibre optique au lieu de câbles de données lorsque la longueur dépasse 295 pieds. |
| **Emplacement de l'équipement** | L'équipement LAN doit être logé dans un placard de câblage ou une salle de communication. Tous les équipements doivent être montés ou fixés sur un rack ou une étagère. |
| **Adressage IP** | Le fournisseur d'accès Internet du concessionnaire doit fournir une adresse IP routable. Pour le réseau local du concessionnaire, l'adressage dynamique (DHCP) doit être utilisé pour faciliter le support. |
| **Adaptateur réseau** | Gigabit Ethernet |
| **Commutation Ethernet** | Commutateur géré Gigabit. Étiqueter chaque interface et chaque câble. Cela permettra de gagner du temps lors du suivi des câbles réseau pour le support ou une nouvelle installation. |
| **Routeurs** | Routeur de qualité professionnelle. Les routeurs doivent prendre en charge la technologie NAT/PAT (Network Address Translation/Process Analytical Technology). Les routeurs doivent également prendre en charge le routage dynamique utilisant RIPv2, OSPF et BGP.<br>- Changez le mot de passe de l'appareil au moment de l'installation et de façon continue et régulière.<br>- Conserver une configuration de sauvegarde dans un fichier en cas de panne de logiciel ou de remplacement de matériel. |
| **Firewall** | Un dispositif de sécurité entièrement géré qui surveille en permanence les menaces par le biais du système de détection des intrusions "IDS" et du système de prévention des intrusions "IPS" et d'autres mécanismes tels que le filtrage des paquets, l'antivirus et l'inspection des paquets par état.<br>- Les firewalls doivent prendre en charge la technologie NAT/PAT (Network Address Translation/Process Analytical Technology). Les firewalls doivent également prendre en charge le routage dynamique en utilisant RIPv2, OSPF et BGP.<br>- Changez le mot de passe de l'appareil au moment de l'installation et de façon continue et régulière.<br>- Conserver une configuration de sauvegarde dans un fichier en cas de panne de logiciel ou de remplacement de matériel.<br>- Pour plus d'informations sur les firewalls et la sécurité des réseaux, voir la section 2.6. |
| **Services de noms de domaine (DNS)** | Utilisez le DNS public, sauf si vous utilisez Windows Active Directory. (Dans ce cas, il est nécessaire de disposer d'un serveur DNS interne). |

| Configuration de réseaux sans fil | |
|---|---|
| **Recommandation** | **Spécification** |
| **Matériel sans fil** | Seuls les points d'accès de niveau professionnel doivent être utilisés. Les points d'accès de niveau professionnel sont conçus pour fournir l'itinérance et d'autres fonctionnalités de qualité professionnelle (telles que les VLAN et/ou les SSID multiples) nécessaires à la prise en charge des appareils sans fil pour les applications. Les points d'accès sans fil de niveau professionnel sont également conçus pour accueillir un plus grand nombre de connexions que le matériel de niveau consommateur. |
| **Segmentation du réseau** | Les concessionnaires doivent veiller à ce que le trafic des visiteurs soit segmenté à partir du réseau du concessionnaire par le biais de réseaux locaux virtuels ou d'une connexion internet distincte. |
| **SSIDs** | Il est recommandé aux concessionnaire d'utiliser des SSID distincts pour les différentes fonctions commerciales (c'est-à-dire la vente, le service et l'administration). Toutefois, les concessionnaires ne doivent pas confondre les SSID avec la segmentation du réseau. Les SSID ne séparent généralement pas le trafic du réseau, mais fournissent seulement un moyen différent de rejoindre le réseau. |
| **Couverture** | Déployer des points d'accès sans fil pour assurer une couverture adéquate. Les outils sans fil peuvent fournir une puissance de signal autour du bâtiment. Faites attention aux structures ou aux objets qui peuvent interférer avec la couverture sans fil (interférences électriques, interférences de radiofréquence ou matériaux physiques tels que les métaux ou le béton). |
| **Authentification et cryptage** | Authentification WPA2 avec RADIUS et cryptage AES |
| **Norme de réseau** | 802.11n or 802.11ac |
| **Détection des réseaux sans fil malveillants** | Scanner, identifier et supprimer tout point d'accès sans fil malveillant qui pourrait se trouver sur le réseau du distributeur.<br>-Un point d'accès sans fil malveillant est défini comme un point d'entrée sans fil dans le réseau de le réseau du concessionnaire qui n'a pas été autorisé ou sécurisé par le concessionnaire, la direction informatique et le propriétaire.<br>-Tous les réseaux sans fil malveillants doivent être détectés, trouvés et supprimés immédiatement.<br>-STAR recommande l'utilisation d'un service de détection sans fil géré qui analyse en permanence le réseau à la recherche de menaces sans fil. |

| Mobilité des concessionnaires | |
|---|---|
| **Recommandations** | **Spécification** |
| **Mobilité au sein de la société du concessionnaire** | Utiliser un réseau maillé sans fil pour s'assurer que les utilisateurs finaux peuvent naviguer dans le lieu sans perdre la connexion ou 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 les points d'accès légers sur le réseau de la société du concessionnaire. Cela permettra d'assurer une couverture adéquate, la fiabilité et l'efficacité du réseau. |

| Accès des clients | |
|---|---|
| **Recommandations** | **Spécification** |
| Hiérarchisation des priorités en matière de trafic | Les concessionnaires devraient utiliser un firewall ou un autre mécanisme pour limiter la consommation de bande passante des visiteurs. Cela empêchera l'accès des visiteurs d'interférer avec les opérations commerciales en consommant trop de bande passante. |
| Authentification des invités/ Conditions d'utilisation | STAR recommande aux concessionnaires d'utiliser un portail captif exigeant des invités qu'ils acceptent les conditions d'utilisation de la société du concessionnaire. Ces conditions peuvent inclure des restrictions de contenu, des limitations de bande passante et des accords d'utilisation. |
| Bande passante Internet | Pour s'assurer que la société du concessionnaire dispose d'une largeur de bande suffisante, le concessionnaire doit choisir la bonne technologie et la bonne vitesse. (Voir les sections 2.5a et 2.5b dans le STAR DIG pour plus d'informations sur les technologies et la bande passante internet).<br>-STAR recommande également à chaque concessionnaire de disposer d'une connexion de secours à un fournisseur d'accès Internet, utilisant une technologie différente.<br>-Voir la section 2.5c pour les recommandations sur les connexions de sauvegarde sur Internet. |

Pour plus d'informations sur la configuration et la gestion du réseau, veuillez consulter la section 2.4 du guide de l'infrastructure des concessionnaires STAR (DIG))

## Sécurité

| | Sécurité du réseau |
|---|---|
| **Firewall/ UTM** | Un dispositif de sécurité entièrement géré qui surveille en permanence les menaces par le biais du système de détection des intrusions "IDS" et du système de prévention des intrusions "IPS" et d'autres mécanismes.<br><br>Le dispositif doit également présenter les caractéristiques suivantes :<br>• Des mécanismes tels que le filtrage des paquets, l'antivirus et l'inspection des paquets par état.<br>• Filtrage des paquets et des protocoles (par exemple IP, ICMP)<br>• Analyse antivirus<br>• Effectuer une inspection officielle des connexions<br>• Effectuer des opérations proxy sur des demandes sélectionnées<br>• Signaler régulièrement (c'est-à-dire tous les mois) le trafic autorisé et refusé par le dispositif de sécurité |
| **Segmentation du réseau** | Les informations sur les cartes de paiement, les informations sur les clients, le trafic des concessionnaires et le trafic des clients doivent être segmentées par le biais d'une segmentation du réseau (comme le VLAN) ou d'un réseau différent (comme un circuit dédié aux clients) pour garantir la sécurité des données. |

| | |
|---|---|
| **Filtrage du contenu** | La perte de données peut être due au fait que des employés naviguent sur le web pour des activités non liées à l'entreprise. STAR recommande aux concessionnaires de filtrer le contenu du réseau afin de supprimer tout trafic potentiellement préjudiciable, inapproprié ou autre trafic non lié à l'activité professionnelle. |
| **SIEM** | Une surveillance proactive et en temps réel des événements qui utilise un service SIEM. Le SIEM doit pouvoir collecter des données avec la possibilité d'agréger et de corréler en temps réel les différentes données de sécurité du réseau. Le fournisseur de services SIEM doit être en mesure d'informer l'administrateur du réseau en cas d'événement de sécurité et de fournir la documentation appropriée à des fins de conformité. Le but ultime d'un service SIEM est d'aider à identifier ou à prévenir une intrusion dans votre réseau. Une réponse immédiate à une violation peut réduire ou prévenir considérablement la perte de données. |
| **Système de détection sans fil** | Scannez, identifiez et supprimez tous les points d'accès sans fil malveillants qui pourraient se trouver sur le réseau du détaillant. Un point d'accès sans fil malveillant est défini comme un point d'entrée sans fil dans le réseau du concessionnaire qui n'a pas été autorisé, sécurisé ou connu par les services informatiques, la direction et les propriétaires du concessionnaire.<br>○ Tous les réseaux sans fil malveillants doivent être détectés, trouvés et supprimés immédiatement.<br>○ STAR recommande l'utilisation d'un service de détection sans fil géré qui analyse en permanence le réseau à la recherche de menaces sans fil. |
| **Test de pénétration et analyse de vulnérabilité** | Il est fortement recommandé de procéder à des tests de pénétration internes et externes annuels du réseau du concessionnaire. Un test de pénétration ("pen test") est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique en simulant une attaque provenant d'une source malveillante. Un test de pénétration doit être effectué sur tout système informatique qui doit être déployé dans un environnement en réseau, en particulier ceux dont le système est exposé à Internet. Le test de pénétration peut être effectué en externe (simulation d'une attaque depuis l'extérieur de votre réseau et exactement comme une tentative de piratage lancée depuis un pays étranger), ou il peut être effectué en interne (depuis l'intérieur de votre réseau pour voir quels accès et quelles vulnérabilités existent). |

| **Recommandation** | Sécurité des ordinateurs de bureau |
|---|---|
| **Surveillance des virus informatiques** | Des produits antivirus de qualité professionnelle doivent être installés sur tous les PC et configurés pour effectuer automatiquement les opérations suivantes :<br>• Télécharger et installer les mises à jour les plus récentes des signatures de virus<br>• Surveiller activement les virus<br>• Mettre en quarantaine et éradiquer les fichiers infectés<br>• La solution antivirus doit comprendre un antivirus, un antispyware, la prévention des intrusions, le contrôle des applications, le contrôle du spam et la détection des rootkits |
| **Gestion des patchs** | STAR recommande que la gestion des patchs soit effectuée sur chaque PC afin de s'assurer que chaque poste de travail dispose des patchs Microsoft actuels. La gestion des postes de travail doit inclure la surveillance à distance des défaillances matérielles/logicielles, des serveurs en panne, du manque d'espace disque, de l'utilisation excessive des processeurs et de la mémoire. |

| | |
|---|---|
| **Protection des mots de passe** | Les mots de passe doivent expirer tous les 60 jours ou moins.<br><br>Les concessionnaires doivent utiliser des "mots de passe forts" contenant au minimum 8 caractères et comprenant 3 des 4 exigences suivantes:<br>1) Majuscules<br>2) Minuscules<br>3) Numéros<br>4) Caractères spéciaux. |
| Détection des points terminaux et réponse | Le service de détection et de réponse des points terminaux de niveau entreprise doit être installé sur tous les points terminaux et les serveurs critiques. L'offre de service doit fournir une visibilité multiplateforme des activités des points d'extrémité/serveurs. La solution doit être capable de fournir :<br><br>• Détection des menaces par le biais de moteurs d'IA statiques et comportementaux et de HIDS dans l'agent terminal<br>• Confinement de la menace et orientation en matière d'assainissement<br>• Rapports d'activité et chasse aux menaces<br>• Visibilité multiplateforme sur l'exécution des processus, les communications réseau, l'accès aux fichiers, les applications, les demandes DNS et le trafic web crypté |

Pour plus d'informations sur les recommandations en matière de sécurité des concessionnaires, veuillez consulter la section 2.6 du guide de l'infrastructure des concessionnaires STAR (DIG)