Pautas de Infraestructura para Distribuidores STAR
Guía de Referencia Rápida
2020

Contenidos

Introducción

Descripción General

Este breve documento de referencia está destinado a ser emparejado con las Pautas de Infraestructura de Vendedores STAR (DIG). Consulte el STAR DIG para obtener más información sobre cualquier tema descrito en esta guía de referencia.

Descargo de Responsabilidad

Cualquier nombre de la empresa, aplicación, enlace al sitio web o referencia tecnológica mencionada en este documento no debe considerarse como un aval por parte de los OEM o de STAR a menos que dicho aval sea indicado de forma expresa.

Este documento proporciona una especificación básica o una guía para que los vendedores puedan establecer sus comunicaciones por Internet. Es importante tener en cuenta que la infraestructura de la red, los datos del vendedor y la seguridad del sistema son responsabilidad de la concesionaria. Las organizaciones de terceros, como proveedores de servicios y socios, pueden brindar orientación y recomendaciones. Algunas organizaciones pueden proporcionar software, hardware o elementos de red patentados para ayudar a racionalizar las operaciones de red. Sin embargo, estas aplicaciones, recomendaciones o herramientas no sustituyen la administración de la red.

Recomendaciones de Hardware

PCs de Escritorio	
Componentes	**Especificaciones**
Procesadores	Intel Core i5 o superior, o su equivalente de AMD
Memoria (RAM)	4 GB o más
Disco Rígido	500 GB o más
Unidad de CD/DVD	CD/DVD combo, o unidad externa
Puerto Serial	1 (Adaptador USB opcional)
Puertos USB	2 o más
Adaptador de Audio	16 bit
Parlante de Audio	Opcional
Pantalla	Resolución mínima de 1280x768
Adaptador de Red	Cableado: Gigabit (o superior) Ethernet Inalámbrico: 802.11 n o ac
Garantía	3 años en el sitio
Sistema Operativo	Los sistemas operativos Windows son compatibles con la mayoría de los aplicativos de la concesionaria. Consulte a su OEM y socios tecnológicos al elegir un sistema operativo.

Laptops	
Componentes	**Especificaciones**
Procesadores	Intel Core i5 o superior, o su equivalente de AMD
Memoria (RAM)	4 GB o más
Disco Rígido	500 GB o más
Unidad de CD/DVD	CD/DVD combo, o unidad externa
Puertos USB	2
Parlante de Audio	Opcional
Pantalla	Resolución mínima de 1280x768
Adaptador de Red	Cableado: Gigabit (o superior) Ethernet Inalámbrico: 802.11 n o ac
Garantía	3 años en el sitio
Sistema Operativo	Los sistemas operativos Windows son compatibles con la mayoría de los aplicativos de la concesionaria. Consulte a su OEM y socios tecnológicos al elegir un sistema operativo.

Ruteadores & Conmutadores	
Componentes	**Especificaciones**
Especificación estándar de Ethernet	IEEE 802.3 100baseT o 1000baseT
Redundancia	La conexión de varios conmutadores juntos debería usar enlaces redundantes de la velocidad más alta disponible, utilizando STP o rSTP para garantizar una topología sin bucles.
Fuente de alimentación	Se recomiendan fuentes de alimentación redundantes para reducir el tiempo de inactividad.
Velocidad	100 o 1000 Mbps
VLAN	Los swtiches con tecnología troncal VLAN y 802.1Q deben usarse para redes enrutadas con múltiples subredes o VLANs.
Protocolos de gestión	Los dispositivos administrados deben ser compatibles con los estándares de administración remota de la industria, como el Protocolo Simple de Administración de Redes (SNMP) y el Monitoreo Remoto de Redes (RMON).
Conmutadores inalámbricos	Los dispositivos inalámbricos deben ser de doble banda y compatibles con IEEE 802.11b/g/n.

Para obtener más información sobre las recomendaciones de hardware de la concesionaria, consulte la sección 2.2 de la Guía de Infraestructura del Vendedor STAR (DIG)

Recomendaciones de Software

Sistemas Operativos

A continuación se muestra una lista de los sistemas operativos más comunes en el mercado actual. Algunas aplicaciones no son compatibles con sistemas operativos específicos. Se recomienda que los vendedores verifiquen con sus OEM, DSP y otros proveedores para determinar qué Sistemas Operativos usarán. Tenga en cuenta que, a partir de abril de 2014, Microsoft finalizó el soporte para sistemas operativos XP. Esto incluye actualizaciones críticas de Seguridad. STAR recomienda que las concesionarias no utilicen Windows XP.

Sistema operativos actuales típicos del cliente	Última actualización o *service pack**	Fin del soporte estándar	Fin del soporte extendido
Windows XP	Service Pack 3	14-Abr-09	8-Abr-14
Windows Vista	Service Pack 2	10-Abr-12	11-Abr-17
Windows 7	Service Pack 1	13-Ene-15	14-Ene-20
Windows 8	Windows 8.1	9-Ene-18	10-Ene-23
Windows 10,	N/A	13-Oct-20	14-Oct-25
MAC OS X	10.9 (o superior soportado) 10.11	Versiones 10.8 (Mountain Lion) e inferiores ya no son soportadas.	Versiones 10.8 (Mountain Lion) e inferiores ya no son soportadas.
IOS (para iPad y iPhone)	9.1		
Android	5		

**** Últimas actualizaciones / service pack a partir de noviembre de 2015***

Navegadores de Internet

A continuación se muestra una lista de los navegadores de internet más comunes en el mercado actual. Algunas aplicaciones no son compatibles con navegadores específicos. Otras aplicaciones requieren configuraciones específicas del navegador, como el modo de compatibilidad. Se recomienda que los vendedores verifiquen con sus OEM, DSP y otros proveedores para determinar qué sistemas operativos usarán.

Navegador	Última actualización o service pack*	Notas
Google Chrome	71	
Mozilla Firefox	64	
Internet Explorer	11	
Apple Safari	12	No recomendado para sistemas operativos de Microsoft
Opera	57	
Edge	18	

**** Últimas actualizaciones / service pack a partir de enero de 2019***

Para obtener más información sobre las recomendaciones de software de la concesionaria, consulte la sección 2.3 de la Guía de Infraestructura del Vendedor STAR (DIG)

Configuración de Redes & Gestión

	Especificaciones de LAN
Red de área local (LAN)	Gigabit Ethernet
Cableado de datos	El cableado de red de datos existente debe ser, como mínimo, los estándares TIA-568-A Categoría 5e. La categoría 6a debe usarse para cableado nuevo. Ningún cable horizontal debe exceder los 90 metros (295 pies). Se recomienda encarecidamente el uso de cables de fibra óptica en lugar de los cables de datos cuando la longitud exceda los 295 pies.
Ubicación del equipo	El equipo LAN debe estar alojado en un armario de cableado o sala de comunicaciones. Todo el equipo debe estar montado o asegurado a un estante o estante.
Direccionamiento IP	El ISP de la concesionaria debe proporcionar direccionamiento IP enrutable. Para la LAN del distribuidor, debe utilizarse el direccionamiento dinámico (DHCP) para facilitar el soporte.
Adaptador de red	Gigabit Ethernet
Conmutador de Ethernet	Conmutador gestionado por Gigabit. Etiquete cada interfaz y cable. Esto ahorrará tiempo al rastrear los cables de red para soporte o instalación nueva.
Ruteadores	Enrutador de tipo empresarial. Los enrutadores deben admitir la traducción de direcciones de red / tecnología analítica de procesos (NAT / PAT). Los enrutadores también deben admitir el enrutamiento dinámico mediante RIPv2, OSPF y BGP. - Cambie la contraseña del dispositivo al momento de la instalación y de manera continua y regular. - Mantenga la configuración de la copia de seguridad en archivos en caso de una falla de software o reemplazo de hardware.
Cortafuegos	Un dispositivo de Seguridad completamente administrado que monitorea continuamente las amenazas a través del Sistema de Detección de Intrusos "IDS", el Sistema de Prevención de Intrusos "IPS" y otros mecanismos como el filtrado de paquetes, antivirus e inspección de paquetes con estado. - Los firewalls deben admitir la traducción de direcciones de red / tecnología analítica de procesos (NAT / PAT). Los cortafuegos también deberían admitir el enrutamiento dinámico mediante RIPv2, OSPF y BGP. - Cambie la contraseña del dispositivo al momento de la instalación y de manera continua y regular. - Mantenga la configuración de la copia de seguridad en archivos en caso de una falla de software o reemplazo de hardware. - Para obtener más información sobre firewalls y Seguridad de Redes, consulte la sección 2.6.
Servicios de nombres de dominio (DNS)	Use DNS público, excepto cuando use Windows Active Directory. (En cuyo caso, se requerirá que tenga un servidor DNS interno).

Diseño de Redes Inalámbricas	
Recomendación	**Especificación**
Hardware inalámbrico	Solo se deben utilizar puntos de acceso de tipo empresarial. Los puntos de acceso de tipo empresarial están diseñados para proporcionar *roaming* y otras características de clase empresarial (como VLAN y / o SSID múltiples) necesarios para admitir dispositivos inalámbricos para sus aplicaciones. Los puntos de acceso inalámbrico de tipo empresarial también están diseñados para acomodar una mayor cantidad de conexiones que el hardware a nivel de consumidor.
Segmentación de red	Las concesionarias deben garantizar que el tráfico de invitados esté segmentado desde la red de la concesionaria a través de VLANs o una conexión a Internet separada.
SSIDs	Se recomienda que las concesionarias utilicen SSID separados para diferentes funciones comerciales (por ejemplo: ventas, servicio y administración). Sin embargo, las concesionarias no deben confundir los SSID con la segmentación de la red. Los SSID generalmente no separan el tráfico de red, sino que solo proporcionan una forma diferente de unirse a la red.
Cobertura	Implemente puntos de acceso inalámbrico para garantizar una cobertura adecuada. Las herramientas inalámbricas pueden proporcionar intensidad en la señal de todo el edificio. Tenga en cuenta las estructuras u objetos que puedan interferir con la cobertura inalámbrica (interferencia eléctrica, interferencia de radiofrecuencia o materiales físicos como metales u hormigón).
Autenticación & Cifrado	WPA2 con autenticación RADIUS y cifrado AES
Estándar de red	802.11n o 802.11ac
Detección inalámbrica no autorizada	Escanee, identifique y elimine cualquier punto de acceso inalámbrico no autorizado que pueda estar en la red de la concesionaria. -Un punto de acceso inalámbrico no autorizado se define como un punto de entrada inalámbrico en la red de la concesionaria que no ha sido autorizado o asegurado por la concesionaria, la administración de TI y tampoco es propio. -Todas las redes inalámbricas no autorizadas se deben detectar, encontrar y eliminar de inmediato. -STAR recomienda el uso de un servicio de detección inalámbrica administrada que esté continuamente escaneando la red en busca de amenazas inalámbricas.

Movilidad de la Concesionaria	
Recomendaciones	**Especificación**
Movilidad dentro de la concesionaria	Utilice una red de malla inalámbrica para garantizar que los usuarios finales puedan navegar en las instalaciones sin perder la conexión o sin necesidad de autenticarse de nuevo.
Controladores inalámbricos	Se puede usar un controlador de LAN inalámbrica en combinación con el Protocolo ligero de puntos de acceso (LWAPP) para administrar puntos de acceso ligeros en toda la red de la concesionaria. Esto ayudará a garantizar una cobertura, confiabilidad y eficiencia de red adecuadas.

Acceso de los Clientes	
Recomendaciones	**Especificación**
Priorización de tráfico	Las concesionarias deben utilizar un cortafuego u otro mecanismo para limitar el consumo de ancho de banda del invitado. Esto evitará que el acceso de los invitados interfiera con las operaciones comerciales al consumir demasiado ancho de banda.
Autenticación de invitados / Términos de uso	STAR recomienda que las concesionarias utilicen un portal cautivo que requiera que los invitados acepten los términos y condiciones de uso en la concesionaria. Esto puede incluir restricciones de contenido, limitaciones de ancho de banda y acuerdos de uso.
Ancho de banda de internet	Para garantizar que la concesionaria tenga suficiente ancho de banda, una concesionaria debe elegir la tecnología y la velocidad adecuadas. (Consulte la Sección 2.5a y 2.5b en STAR DIG para obtener más información sobre tecnologías y ancho de banda de Internet). -STAR también recomienda que cada concesionario tenga una conexión ISP de respaldo de un proveedor diferente, utilizando una tecnología diferente. -Ver sección 2.5c para recomendaciones sobre conexiones de respaldo de internet.

Para obtener más información sobre la configuración y administración de la red, consulte la sección 2.4 de la Guía de Infraestructura del Distribuidor STAR (DIG)

Seguridad

	Seguridad de Redes
Cortafuegos / UTM	Un dispositivo de Seguridad totalmente administrado que monitorea continuamente las amenazas a través del sistema de detección de intrusos "IDS" y el Sistema de prevención de intrusiones "IPS" y otros mecanismos. El dispositivo también debe tener las siguientes características: ● Mecanismos tales como filtrado de paquetes, antivirus e inspección de paquetes *stateful*. ● Filtrar paquetes y protocolos (por ejemplo, IP, ICMP) ● Escaneo antivirus ● Realizar una inspección *stateful* de las conexiones. ● Realizar operaciones *proxy* en aplicaciones seleccionadas ● Informar sobre el tráfico permitido y denegado por el dispositivo de Seguridad de forma regular (por ejemplo: mensual)
Segmentación de red	La información de la tarjeta de pago, la información del cliente, el tráfico de la concesionaria y el tráfico del cliente deben segmentarse a través de la segmentación de red (como VLAN) o una red diferente (como un circuito dedicado para invitados) para garantizar la seguridad de los datos.
Filtrado de contenido	La pérdida de datos puede ocurrir por empleados que navegan por la web para actividades no relacionadas con el negocio. STAR recomienda que las concesionarias filtren contenido de la red para eliminar el posible tráfico nocivo, inapropiado u otro tráfico no relacionado con el negocio.

SIEM	Monitoreo proactivo de eventos en tiempo real que utiliza un servicio SIEM. SIEM necesita poder recopilar datos con capacidad para agregar y correlacionar datos variables de Seguridad de la red en tiempo real. El proveedor de servicios SIEM debe poder notificar al administrador de la red en el caso de un evento de Seguridad, así como proporcionar la documentación adecuada para fines de cumplimiento. El objetivo final de un servicio SIEM es ayudar a identificar o prevenir una intrusión en su red. La respuesta inmediata a una violación puede reducir o prevenir en gran medida la pérdida de datos.
Sistema de detección inalámbrico	Escanee, identifique y elimine cualquier punto de acceso inalámbrico no autorizado que pueda estar en la red de minoristas. Un punto de acceso inalámbrico no autorizado se define como un punto de entrada inalámbrico en la red de la concesionaria que no cuenta con autorización, seguridad o conocimiento del departamento de TI, administración y que ni es propiedad de la concesionaria. ○ Todas las redes inalámbricas no autorizadas se deben detectar, encontrar y eliminar de inmediato. ○ STAR recomienda el uso de un servicio de detección inalámbrico administrado que esté continuamente escaneando la red en busca de amenazas inalámbricas.
Pruebas de Penetración y Escaneo de Vulnerabilidades	Se recomienda realizar pruebas anuales de penetración interna y externa de la red de distribuidores. Una prueba de penetración ("*pen test*") es un método para evaluar la seguridad de un sistema informático o red mediante la simulación de un ataque de una fuente maliciosa. Se debe realizar una prueba de penetración en cualquier sistema informático que vaya a implementarse en un entorno de red, en particular, aquellos con cualquier sistema que fuera expuesto a Internet. Los trabajos de prueba de penetración pueden realizarse externamente (simulación de un ataque desde fuera de su red y exactamente como si se lanzara un intento de hackeo desde un país extranjero), o puede realizarse internamente (desde dentro de su red para ver qué acceso y vulnerabilidades existen).

Recomendación	Seguridad del Escritorio
Monitoreo de Virus de PC	Los productos antivirus de tipo empresarial deben instalarse en todas las PC y deben configurarse para realizar automáticamente lo siguiente: ● Descargar e instalar las actualizaciones de firmas de virus más recientes ● Monitorear activamente los virus ● Poner en cuarentena y erradicar archivos infectados ● El paquete de antivirus debe incluir antivirus, antispyware, prevención de intrusiones, control de aplicaciones, control de spam y detección de rootkits.
Manejo de parches	STAR recomienda que la administración de parches se realice en cada PC para garantizar que cada estación de trabajo tenga los parches actuales de Microsoft. La Administración de la Estación de Trabajo debe incluir monitoreo remoto de fallas de hardware/software, servidores inactivos, poco espacio en disco, uso excesivo de CPU y uso excesivo de la memoria.

Protección de contraseña	Las contraseñas se deben configurar para que caduquen cada 60 días o menos. Como mínimo, las concesionarias deben usar "contraseñas seguras" que contengan un mínimo de 8 caracteres compuesto por 3 de los siguientes 4 requisitos: 1) Mayúsculas 2) Minúsculas 3) Números 4) Caracteres especiales.
Detección y Respuesta *Endpoint*	El servicio de detección y respuesta *Endpoint* de tipo empresarial debe instalarse en todos los *endpoints* y servidores críticos. La oferta de servicios debe proporcionar visibilidad multiplataforma de las actividades del servidor/*endpoint*. La solución debería poder proporcionar: • Detección de amenazas a través de motores de IA estáticos y de comportamiento y HIDS dentro del agente *endpoint* • Contención de Amenazas y Orientación de Remediación • Informes de Actividad y Búsqueda de Amenazas • Visibilidad multiplataforma en la ejecución de procesos, comunicaciones de red, acceso a archivos, aplicaciones, solicitudes de DNS y tráfico web cifrado

Para obtener más información sobre las recomendaciones de seguridad de la concesionaria, consulte la sección 2.6 de la Guía de Infraestructura del Vendedor STAR (DIG)