Guía de referencia rápida de recomendaciones de infraestructura para distribuidores STAR

2025

Índice

Introducción

Descripción general

Este breve documento de referencia está destinado para usarse en conjunto con las Recomendaciones de infraestructura para los distribuidores (DIG) de STAR. Para obtener más información sobre cualquier tema tratado en esta guía de referencia, consulte STAR DIG.

Exención de responsabilidad

Cualquier nombre de empresa, aplicación, enlace a sitio web o referencia tecnológica mencionada en este documento no debe considerarse un aval de los fabricantes de equipos originales o de STAR, a menos que dicho aval se indique expresamente.

En este documento se proporciona una especificación o directriz básica para que los distribuidores establezcan una comunicación por Internet. Es importante señalar que la infraestructura de red, los datos del distribuidor y la seguridad del sistema son responsabilidad de la distribuidora. Las organizaciones de terceros, como proveedores de servicios y socios, pueden proporcionar 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 a la gestión de la red.

Recomendaciones de hardware

Computadoras de escritorio, portátiles y tabletas

Las recomendaciones STAR para computadoras de escritorio, portátiles y tabletas de los distribuidores se han alejado de las especificaciones generales de hardware. Esto se debe principalmente a los avances en la potencia de procesamiento del hardware, el paso a la computación en la nube y la ubicuidad de la movilidad. STAR recomienda que las necesidades de hardware se determinen en relación con una hipótesis de caso de uso según la función del trabajo. A la hora de adquirir dispositivos nuevos, tenga en cuenta los factores a continuación:

1. **Movilidad:** Algunas funciones dentro de una distribuidora exigen movilidad. Otras funciones del puesto se efectúan, en principio, en un lugar físico. Tenga en cuenta las necesidades de movilidad a la hora de adquirir un dispositivo nuevo. Recuerde también que muchos dispositivos móviles, como las tabletas, funcionan con un software específico que puede no ser compatible con todo el hardware y el software necesarios. Considere los requisitos de hardware y software antes de decidir si una tableta, una portátil o una computadora de escritorio es la mejor opción para esa función laboral.
2. **Requisitos de software:** Las funciones en la distribuidora necesitarán la interacción con softwares diferentes. El software suele estar escrito para sistemas operativos y navegadores de Internet específicos. Las aplicaciones de software también pueden necesitar una especificación mínima de hardware. Cuando adquiera un dispositivo nuevo, familiarícese con el software que ejecutará y los requisitos necesarios para ejecutarlo.
3. **Requisitos de los accesorios de hardware.** A menudo, los distribuidores necesitan accesorios específicos para desempeñar una función laboral. Se necesitan ayudas a la venta, diagnósticos de servicio y otros adaptadores físicos para casos de uso específicos. Estos accesorios suelen fabricarse teniendo en cuenta especificaciones concretas de software y hardware. Si la función

de robo exige un accesorio específico, consulte los requisitos con el proveedor antes de adquirir un equipo nuevo.

4. **Requisitos de OEM, DSP y terceros:** Los fabricantes de equipos originales, los proveedores de servicios para distribuidores y otros proveedores externos suelen implantar tecnologías específicas para distribuidoras. Estas tecnologías (hardware o software) pueden demandar especificaciones concretas para funcionar con eficiencia. Si un dispositivo del distribuidor utiliza tecnologías específicas, consulte al proveedor de la tecnología.
5. **Confiabilidad:** Se debe tener en cuenta la confiabilidad de los dispositivos a la hora de comprar hardware. Algunas áreas de la distribuidora, como el entorno de servicio, son más propensas a fallos de dispositivos. Algunas funciones laborales están más limitadas por el tiempo de inactividad de los dispositivos. Al considerar cuándo y qué comprar, tenga en cuenta la probabilidad de fallos del dispositivo y el impacto que un fallo puede tener en esa función laboral y en las operaciones comerciales de la distribuidora.

Más allá de las recomendaciones sobre casos de uso, STAR puede orientar sobre cuándo adquirir nuevo hardware y qué comprar cuando llegue ese momento. STAR brinda orientación sobre "cuándo comprar hardware nuevo" en las Recomendaciones de infraestructura para distribuidores STAR en la sección 2.2.a. A la hora de determinar qué comprar, STAR ofrece orientación sobre las compras de hardware diseñado para el consumidor frente al hardware de calidad empresarial en la sección 2.2.b., y una guía para tabletas y dispositivos móviles en la sección2.2.d.

STAR también proporciona orientación y especificaciones sobre enrutadores y conmutadores para conectar el hardware de red en la sección 2.2.c de las Recomendaciones de infraestructura para distribuidores.

Para obtener más información sobre las recomendaciones de hardware para distribuidoras, incluso tabletas, la movilidad y el retiro del servicio y reciclaje de hardware, consulte la sección 2.2 de las Recomendaciones de infraestructura para distribuidores (DIG) de STAR

Recomendaciones de software

Sistemas operativos

A continuación encontrará una lista de los sistemas operativos más comunes en el mercado actual. Algunas aplicaciones no son compatibles con sistemas operativos específicos. Se recomienda a los distribuidores que consulten a sus OEM, DSP y otros proveedores para determinar qué sistemas operativos deben utilizar. Tenga en cuenta que Microsoft ha finalizado la asistencia técnica para los sistemas operativos Windows XP, Vista y Windows 7. Esto incluye actualizaciones de seguridad críticas. STAR recomienda a las distribuidoras no utilizar Windows XP, Vista ni Windows 7.

Sistemas operativos comunes actuales de clientes	Última actualización o Service Pack*	Fin de la asistencia estándar	Fin de la asistencia ampliada
Windows XP	Service Pack 3	14 abril 09	8 abril 14
Windows Vista	Service Pack 2	10 abril 12	11 abril 17
Windows 7	Service Pack 1	13 enero 15	14 enero 20
Windows 8	Windows 8.1	9 enero 18	10 enero 23
Windows 10	22H2	13 octubre 20	14 octubre 25
Windows 11	24H2		
MAC OS X	15.1.1	Las versiones 14 e inferiores ya no tienen asistencia.	Las versiones 14 e inferiores ya no tienen asistencia.
IOS (para iPad y iPhone)	18.2		
Android	15		

Últimas actualizaciones/service pack a partir de enero de 2025

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 determinados navegadores. Otras aplicaciones demandan una configuración específica del navegador, como el modo de compatibilidad. Se recomienda a los distribuidores que consulten a sus OEM, DSP y otros proveedores para determinar qué sistemas operativos deben utilizar.

Navegador	Última actualización o Service Pack*	Notas
Safari de Apple	17	No se recomienda su uso en sistemas operativos de Microsoft
Google Chrome	131	
Internet Explorer	11	Internet Explorer se retiró en junio de 2022. Microsoft Edge es el navegador que recomienda Microsoft.
Microsoft Edge	1131	
Mozilla Firefox	133	

Últimas actualizaciones/service pack a partir de enero de 2020

Para más información sobre las recomendaciones de software para distribuidoras, consulte la sección 2.3 de las Recomendaciones de infraestructura para disbribuidores (DIG) de STAR.

Configuración y gestión de redes

Especificaciones LAN	
Red de área local	Gigabit Ethernet
Cableado de datos	El cableado de red de datos existente debe ser, como mínimo, de categoría 5e según las normas TIA-568-A. La categoría 6a debe utilizarse para el cableado nuevo. Los tramos horizontales de cable no deben superar los 90 metros (295 pies). El cable de fibra óptica es muy recomendable en lugar de los tendidos de cable de datos cuando la longitud supera los 90 metros (295 pies).
Ubicación del equipo	Los equipos LAN deben alojarse en un armario de cableado o en una sala de comunicaciones. Todos los equipos deben montarse en un bastidor o estante o fijarse a un bastidor o estante.
Direccionamiento IP	El ISP de la distribuidora debe proporcionar un direccionamiento IP enrutable. En el caso de la LAN del distribuidor, debe utilizarse el direccionamiento dinámico (DHCP) para facilitar la asistencia.
Adaptador de red	Gigabit Ethernet
Conmutación Ethernet	Conmutador Gigabit gestionado. Etiquete cada interfaz y cable. Esto ahorrará tiempo a la hora de localizar cables de red para asistencia o instalaciones nuevas.
Enrutadores	Enrutador para empresas. Los enrutadores deben ser compatibles con 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 en el momento de la instalación y de forma continua y periódica. - Guarde una copia de seguridad de la configuración en caso de fallo del software o de sustitución del hardware.
Firewall	Dispositivo de seguridad totalmente gestionado que ejecuta una supervisión continua de las amenazas mediante el sistema de detección de intrusiones "IDS" y el sistema de prevención de intrusiones "IPS" y otros mecanismos como el filtrado de paquetes, el antivirus y la inspección de paquetes con estado.
	Los firewalls deben ser compatibles con la traducción de direcciones de red/tecnología analítica de procesos (NAT/PAT). Los firewalls también deben admitir el enrutamiento dinámico mediante RIPv2, OSPF y BGP.
	- Cambie la contraseña del dispositivo en el momento de la instalación y de forma continua y periódica .
	- Guarde una copia de seguridad de la configuración en caso de fallo del software o de sustitución del hardware.
	- Para más información sobre firewalls y seguridad de la red, consulte el apartado 2.6.

Servicios de nombres de dominio (DNS)	Utilice DNS público excepto cuando utilice Windows Active Directory. (En cuyo caso, es necesario disponer de un servidor DNS interno).

Diseño de redes inalámbricas	
Recomendación	**Especificación**
Hardware inalámbrico	Sólo deben utilizarse puntos de acceso de nivel empresarial. Los puntos de acceso de nivel empresarial están diseñados para proporcionar itinerancia y otras funciones de clase empresarial (como VLAN y/o múltiples SSID) necesarias para admitir los dispositivos inalámbricos para aplicaciones. Los puntos de acceso inalámbricos para empresas también están diseñados para admitir un mayor número de conexiones que el hardware el consumidor.
Segmentación de la red	Las distribuidoras deben asegurarse de que el tráfico de invitados está segmentado de la red de la distribuidora mediante VLAN o una conexión a Internet independiente.
SSIDs	Se recomienda a las distribuidoras que utilicen SSID distintos para las diferentes funciones empresariales (es decir, ventas, servicio y administración). Sin embargo, las distribuidoras no deben confundir los SSID con la segmentación de la red. Por lo general, los SSID no separan el tráfico de red, sino que solo proporcionan una forma diferente de unirse a la red.
Cobertura	Despliegue puntos de acceso inalámbricos para garantizar una cobertura adecuada. Las herramientas inalámbricas pueden proporcionar intensidad de señal en todo el edificio. Tenga cuidado con las estructuras u objetos que puedan interferir en la cobertura inalámbrica (interferencias eléctricas, interferencias de radiofrecuencia o materiales físicos como metales u hormigón).
Autenticación y cifrado	WPA2 con autenticación RADIUS y cifrado AES. Nota: Consulte las recomendaciones del OEM para obtener orientación sobre la compatibilidad de las tecnologías específicas del OEM.
Norma de red	802.11ax o 802.11ac
Detección de redes inalámbricas no autorizadas	Escanee, identifique y elimine cualquier punto de acceso inalámbrico no autorizado que pueda haber en la red de la distribuidora . -Un punto de acceso inalámbrico no autorizado se define como un punto de entrada inalámbrico a la red de la distribuidora que no ha sido autorizado o protegido por el distribuidor, la dirección de TI y el propietario. -Todas las redes inalámbricas fraudulentas deben detectarse, encontrarse y eliminarse de inmediato. STAR recomienda el uso de un servicio gestionado de detección inalámbrica que ejecute un escaneo continuo de la red en busca de amenazas inalámbricas.

Movilidad de las distribuidoras	
Recomendaciones	**Especificación**
Movilidad dentro del concesionario	Utilice una red de malla inalámbrica para garantizar que los usuarios finales puedan desplazarse por el lugar sin perder la conexión ni tener que autenticarse de nuevo.
Mandos inalámbricos	Un controlador de LAN inalámbrica puede utilizarse en combinación con el protocolo de punto de acceso ligero (LWAPP) para gestionar puntos de acceso ligeros en toda la red de la distribuidora. Esto ayudará a garantizar una cobertura adecuada, confiabilidad y eficiencia de la red.

Acceso de clientes	
Recomendaciones	**Especificación**
Priorización del tráfico	Las distribuidoras deberían utilizar un firewall u otro mecanismo para limitar el consumo de ancho de banda de los invitados. Esto evitará que el acceso de invitados interfiera en las operaciones de la empresa al consumir demasiado ancho de banda.
Autenticación de invitados/ Términos y condiciones de uso	STAR recomienda a las distribuidoras que utilicen un portal cautivo que obligue a los clientes a aceptar los términos y condiciones de uso en la distribuidora. Esto puede incluir restricciones de contenido, limitaciones de ancho de banda y acuerdos de uso.
Ancho de banda de Internet	Para asegurarse de que la distribuidoras dispone de suficiente ancho de banda, debe elegir la tecnología y la velocidad adecuadas. (Para más información sobre tecnologías y ancho de banda de Internet, véanse los apartados 2.5a y 2.5b del STAR DIG). -STAR también recomienda que cada distribuidora tenga una conexión ISP de reserva de un proveedor diferente, que utilice una tecnología distinta. -Vea la sección 2.5c para recomendaciones sobre las conexiones de respaldo a Internet .

Para más información sobre la configuración y la gestión de la red, consulte la sección 2.4 de las Recomendaciones de infraestructura para distribuidores (DIG) de STAR.

Seguridad

	Seguridad de las redes
Firewall/UTM	Dispositivo de seguridad totalmente gestionado que ejecuta supervisión continua de las amenazas mediante el sistema de detección de intrusiones "IDS", el sistema de prevención de intrusiones "IPS" y otros mecanismos. El dispositivo también debe tener las siguientes características: • Mecanismos como el filtrado de paquetes, el antivirus y la inspección de paquetes con estado . • Filtrar paquetes y protocolos (por ejemplo, IP, ICMP) • Escaneo con antivirus • Inspección de estado de las conexiones • Realizar operaciones proxy en las aplicaciones seleccionadas • Informar del tráfico permitido y denegado por el dispositivo de seguridad de forma periódica (por ejemplo, mensualmente) Debido a la importancia del firewall y al hecho de que a menudo se encuentra en la ruta de datos de la mayor parte del tráfico de las distribuidoras, STAR recomienda un dispositivo de reserva en caso de fallo. Para limitar el tiempo de inactividad, los distribuidores deben considerar una solución de conmutación automática al dispositivo de reserva en caso de fallo del hardware .
Segmentación de la red	La información de las tarjetas de pago, la información de los clientes, el tráfico de la distribuidora y el tráfico de los clientes deben segmentarse mediante una segmentación de red (como VLAN) o una red diferente (como un circuito dedicado para invitados) para garantizar la seguridad de los datos.
Filtrado de contenidos	La pérdida de datos puede deberse a que los empleados naveguen por Internet para actividades no relacionadas con la empresa. STAR recomienda a las distribuidoras filtrar el contenido de la red para eliminar el tráfico potencialmente dañino, inapropiado o no relacionado con el negocio.
SIEM	Supervisión proactiva de eventos en tiempo real que utiliza un servicio SIEM. SIEM debe ser capaz de recopilar datos con capacidad para agregar y correlacionar datos de seguridad variables de la red en tiempo real. El proveedor de servicios SIEM debe ser capaz de notificar al administrador de la red en caso de que se produzca un incidente de seguridad, así como de proporcionar la documentación adecuada a efectos de cumplimiento de la normativa. El objetivo último de un servicio SIEM es ayudar a identificar o prevenir una intrusión en su red. La respuesta inmediata a una violación puede reducir en gran medida o evitar la pérdida de datos.
Sistema de detección inalámbrico	Escanee, identifique y elimine cualquier punto de acceso inalámbrico fraudulento que pueda haber en la red del minorista. Un punto de acceso inalámbrico no autorizado se define como un punto de entrada inalámbrico a la red del concesionario que no está autorizado, protegido o conocido por el departamento de TI, la dirección y los propietarios de la distribuidora. o Todas las redes inalámbricas no autorizadas deben detectarse, encontrarse y eliminarse de inmediato. o STAR recomienda el uso de un servicio gestionado de detección inalámbrica que ejecute un escaneo continuo de la red en busca de amenazas inalámbricas.

Pruebas de penetración y exploración de vulnerabilidades	Se recomienda encarecidamente realizar pruebas anuales de penetración internas y externas de la red de concesionarios. Una prueba de penetración ("pen test") es un método de evaluación de la seguridad de un sistema informático o de una red mediante la simulación de un ataque procedente de una fuente maliciosa. Se debe realizar una prueba de penetración en cualquier sistema informático que se vaya a implantar en un entorno de red, en particular, en aquellos con cualquier sistema expuesto o orientado a Internet. Los compromisos de pruebas de penetración se pueden realizar externamente (simulación de un ataque desde fuera de su red y exactamente igual que si se lanzara un intento de pirateo desde un país extranjero), o se pueden realizar internamente (desde dentro de su red para ver qué accesos y vulnerabilidades existen).

Recomendación	Seguridad de las computadoras de escritorio
Supervisión de virus de PC	Los productos antivirus de nivel empresarial deben instalarse en todos los PC y configurarse para que realicen automáticamente las siguientes acciones: • Descargue e instale las actualizaciones de firmas de virus más recientes • Control activo de virus • Ponga en cuarentena y erradique los archivos infectados • La solución antivirus debe incluir antivirus, antispyware, prevención de intrusiones, control de aplicaciones, control de spam y detección de rootkits.
Gestión de parches	STAR recomienda que la gestión de parches se realice en cada PC para asegurar que cada estación de trabajo tiene los parches de Microsoft actualizados. La gestión de estaciones de trabajo debe incluir la supervisión remota de fallos de hardware o software, servidores inactivos, poco espacio en disco, uso excesivo de CPU y uso excesivo de memoria.
Protección por contraseña	Las contraseñas deben caducar cada 60 días o menos. Como mínimo, las distribuidoras deben utilizar "contraseñas seguras" que contengan un mínimo de 8 caracteres compuestos por 3 de los 4 requisitos siguientes: 1) Mayúsculas 2) Minúsculas 3) Numérico 4) Caracteres especiales.
Plataforma de detección y respuesta a puntos finales	• Una plataforma de protección de puntos finales (EPP) y una solución de detección y respuesta de puntos finales (EDR) singulares deben desplegarse en los dispositivos de puntos finales para prevenir los ataques de malware basados en archivos, detectar la actividad maliciosa y proporcionar las capacidades de investigación y reparación necesarias para responder a incidentes y alertas de seguridad dinámicos. Se debe responder de inmediato a las alertas de este servicio para mitigar el riesgo y la posible pérdida de datos. La oferta de servicios debe proporcionar visibilidad multiplataforma de las actividades del punto final/servidor, así como: Detección de amenazas mediante motores de IA estáticos y de comportamiento y HIDS dentro del agente de punto final • Orientación para la contención y corrección de amenazas • Informes de actividad y caza de amenazas • Visibilidad multiplataforma de la ejecución de procesos, las comunicaciones de red, el acceso a archivos, las aplicaciones, las solicitudes DNS y el tráfico web cifrado

Para más información sobre las recomendaciones de software para distribuidoras, consulte la sección 2.6 de las Recomendaciones de infraestructura para distribuidores (DIG) de STAR.