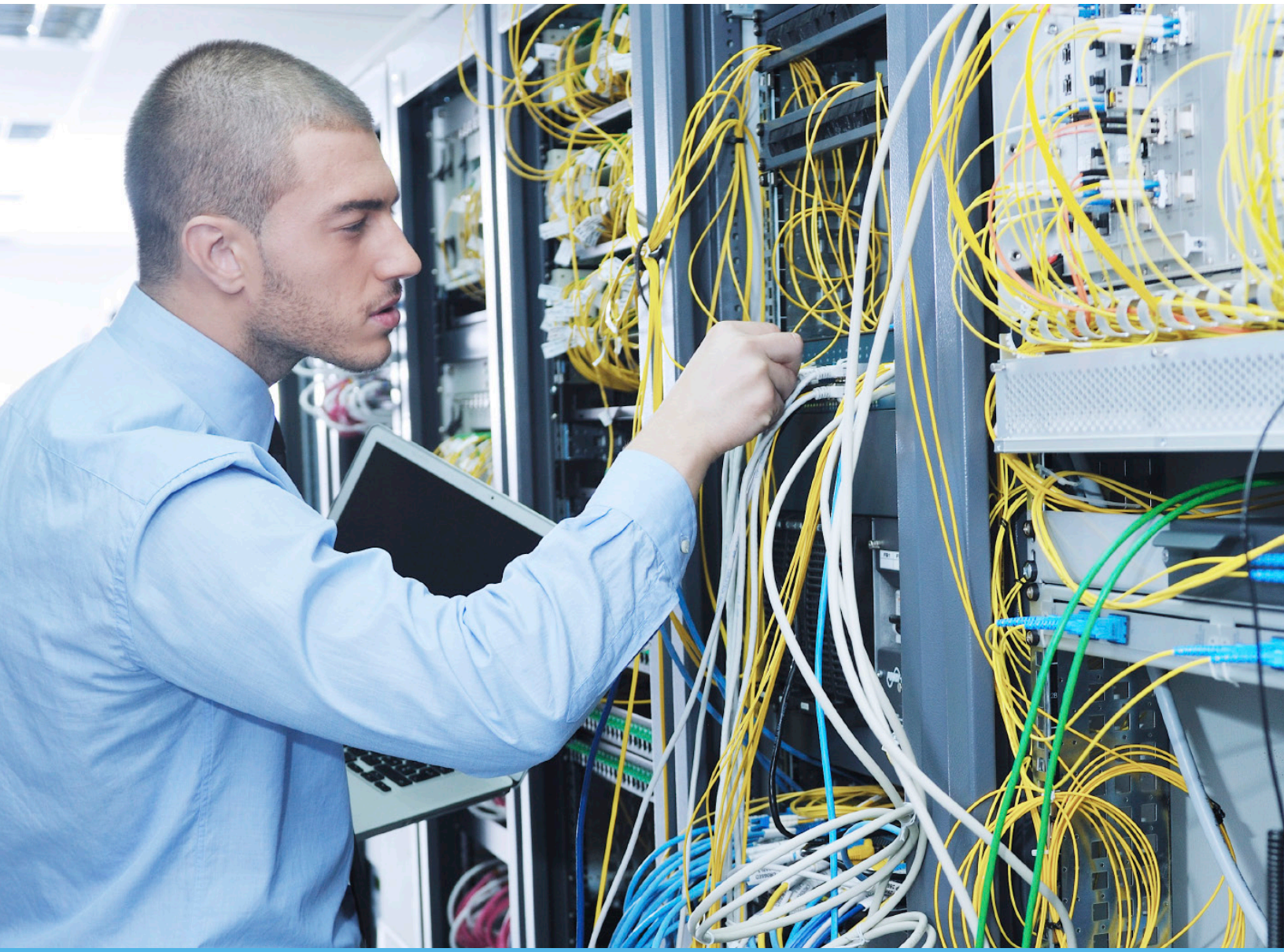
Rescue by LogMeIn

ARQUITECTURA Y SEGURIDAD DE RESCUE

Folleto de descripción general



Índice

INTRODUCCIÓN

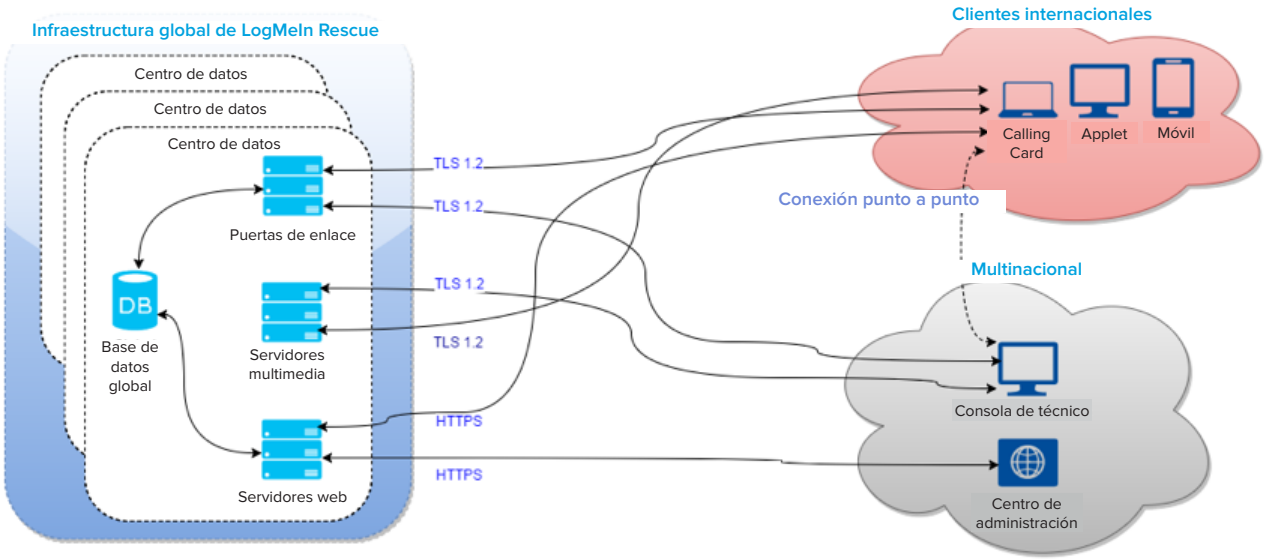
Escalabilidad, seguridad, fiabilidad, facilidad de uso. Estas cuatro características describen una buena solución de asistencia técnica remota, pero no siempre van de la mano. Resulta sencillo encontrar una solución de asistencia técnica que ofrezca dos o tres de los criterios anteriormente mencionados, pero es más complicado encontrar una que presente los cuatro. LogMeIn, Inc. ofrece este tipo de solución con LogMeIn Rescue.

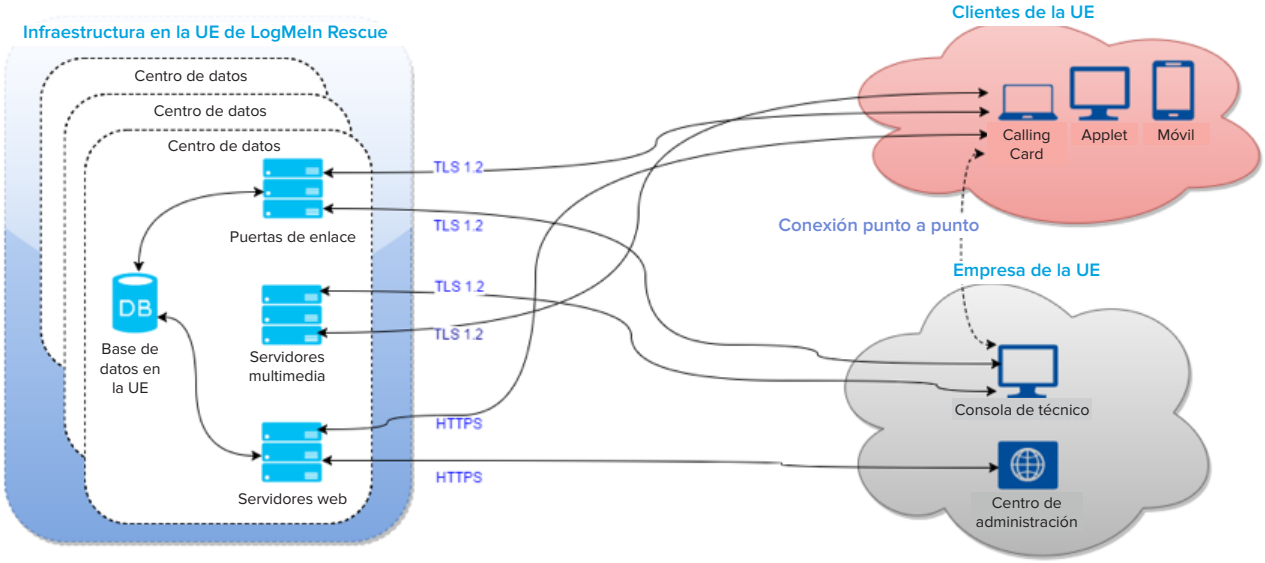
Escalabilidad. Tanto si es un técnico que trabaja solo como si se trata de un centro de atención al cliente con diez mil empleados, Rescue le permitirá hacer lo que necesita.

Seguridad. Las sesiones de asistencia están protegidas con cifrado AES integral de 256 bits. El usuario final debe permitir las operaciones de asistencia para que los técnicos puedan realizarlas. Los registros de las sesiones de asistencia técnica se guardan en una base de datos en formato cifrado para poder realizar consultas posteriormente. Las sesiones de control remoto pueden grabarse en un archivo de vídeo.

Fiabilidad. Rescue está alojado en seis centros de datos extremadamente fiables con una infraestructura completamente redundante.

Facilidad de uso. Sus técnicos estarán en marcha en cuestión de horas. El grupo de usuarios finales a los que presta asistencia técnica recibirán ayuda con tan solo unos clics. Ninguna de las partes tiene que instalar software.





CONFIDENCIALIDAD DE LOS DATOS

A menudo la seguridad se equipara a la confidencialidad de los datos, la confidencialidad de los datos al cifrado y el cifrado se caracteriza por el cifrado simétrico utilizado y la longitud de su clave. Estas concepciones erróneas llevan a denominaciones incorrectas como “seguridad AES de 256 bits”. No hace falta decir que esto es engañoso.

Un sistema en línea seguro debe cumplir siempre los siguientes objetivos:

- Autenticación de las partes que intervienen en la comunicación
- Negociación de las claves de cifrado sin intrusiones
- Intercambio confidencial de mensajes
- Capacidad de detectar si un mensaje se ha modificado durante la transmisión

La tecnología SSL/TLS, siglas de Secure Sockets Layer y Transport Layer Security, se ha diseñado para ofrecer asistencia técnica durante los pasos mencionados. Originalmente creados por Netscape Communications Corporation a mediados de los noventa, se ha convertido en el estándar de comunicaciones seguras a través de Internet y lo apoyan empresas como Visa, MasterCard y American Express.

La implementación de SSL empleada por LogMeIn Rescue es OpenSSL (http://www.openssl.org). LogMeIn utiliza siempre la versión más reciente. A fecha de publicación de este documento, la versión que utiliza Rescue es la 1.0.2j.

ACUERDO DE CLAVES

Cuando se inicia una sesión de asistencia técnica y se establece una conexión entre el usuario al que se presta asistencia y el técnico, sus ordenadores deben acordar un algoritmo de cifrado y la clave correspondiente que se va a utilizar durante la sesión. La importancia de este paso suele infravalorarse, lo que es bastante comprensible, ya que parece una tarea común que debería ser sencilla y clara.

Sin embargo, es de todo menos simple: para contrarrestar los ataques denominados de hombre en el medio (en el que el ordenador C se sitúa entre el ordenador A y B y se hace pasar por la otra parte a A y B), deben emplearse certificados. Como ni el técnico ni el usuario final tienen software de servidor y un certificado SSL instalado en sus ordenadores, ambos se ponen en contacto con unos de los servidores de LogMeIn Rescue y realizan la fase inicial del acuerdo de claves con este ordenador. La verificación del certificado por parte de la Consola de técnico y del applet del usuario final garantiza que solo un servidor de Rescue pueda participar en el proceso.

INTERCAMBIO DE MENSAJES

La tecnología TLS permite utilizar una mayor variedad de conjuntos de cifrado, y las partes que se comunican pueden acordar un esquema de cifrado compatible para ambas. Esto tiene dos objetivos principales: en primer lugar, el protocolo puede ampliarse con nuevos conjuntos de cifrado sin perder la compatibilidad con versiones anteriores y, en segundo lugar, las implementaciones más recientes pueden eliminar conjuntos de cifrado conocidos por sus debilidades criptográficas.

Como los tres componentes del sistema de comunicaciones de LogMeIn Rescue están controlados por LogMeIn, el conjunto de cifrado utilizado por estos componentes es siempre el mismo: AES256-SHA en modo de encadenamiento de bloques cifrados (CBC) con acuerdo de claves RSA. Esto significa lo siguiente:

- Las claves de cifrado se intercambian utilizando pares de claves RSA privadas/públicas, tal y como se ha descrito en la sección anterior.
- AES, siglas de Advanced Encryption Standard, se utiliza como algoritmo de cifrado/descifrado.
- La clave de cifrado tiene una longitud de 256 bits.
- SHA-2 se utiliza como base de los códigos de autenticación de mensajes (MAC). Un MAC es una porción de información que se utiliza para autenticar un mensaje. El valor del MAC protege tanto la integridad de un mensaje como su autenticidad, pues permite que las partes que establecen comunicación detecten cualquier cambio en el mensaje.
- El modo de encadenamiento de bloques cifrados (CBC) garantiza que cada bloque de texto cifrado dependa de los bloques de texto plano hasta ese punto, de forma que los mensajes similares no se puedan identificar como tales.

Esto, a su vez, garantiza que la transmisión de datos entre el usuario final al que se presta asistencia y el técnico esté completamente cifrada y que solo estas partes tengan acceso a la información contenida en el flujo de mensajes.

AUTENTICACIÓN Y AUTORIZACIÓN

La autenticación y la autorización en LogMeIn Rescue tienen dos objetivos diferentes.

La autenticación garantiza que el técnico o el administrador que inicia sesión en el sistema de Rescue sea quien dice ser. En Rescue, la autenticación se realiza de una forma muy clara: Los administradores asignan a los técnicos sus ID de inicio de sesión (que suelen ser sus direcciones de correo electrónico) y las contraseñas correspondientes. Estas credenciales se introducen en el formulario de inicio de sesión del sitio web de LogMeIn Rescue al comenzar la jornada de trabajo del técnico.

En LogMeIn Rescue, el sistema de Rescue se autentica en primer lugar con el técnico (o, más bien, con el navegador web del técnico) con su certificado SSL RSA de 2048 bits. Esto garantiza que el técnico introduzca su nombre de usuario y contraseña en el sitio web correcto. A continuación, el técnico inicia sesión en el sistema con sus credenciales.

LogMeIn Rescue no almacena ninguna contraseña sino que utiliza scrypt para crear algoritmos hash de las contraseñas que posteriormente se almacenan en la base de datos de Rescue. El algoritmo hash utiliza una cadena de 24 caracteres como "sal", generada por CSPRNG para cada contraseña exclusiva.

LogMeIn Rescue ofrece a los administradores distintas opciones para la política de contraseñas:

- Los administradores pueden exigir una fortaleza de contraseña mínima y un periodo de uso máximo de la contraseña (un medidor integrado muestra a administradores y técnicos la fortaleza de la contraseña elegida).
- Se puede obligar a los técnicos a cambiar su contraseña de Rescue la próxima vez que inicien sesión.
- Los administradores maestros pueden exigir a los miembros de su organización que utilicen la verificación en dos pasos para iniciar sesión en Rescue.

LogMeIn Rescue también permite a los administradores implementar una política de inicio de sesión único (SSO). Se utiliza Security Assertion Markup Language (SAML), un estándar XML para el intercambio de datos de autenticación y autorización entre dominios de seguridad (entre un proveedor de identidades y un proveedor de servicios). Por lo tanto, los técnicos solo tienen acceso a las aplicaciones predefinidas y utilizan un ID de SSO para iniciar sesión en esas aplicaciones. Con solo pulsar un botón puede desactivarse el ID de SSO de un técnico.

La función de verificación en dos pasos utiliza LastPass Authenticator para dotar de una segunda capa de protección a las cuentas de Rescue, ya que se les pedirá a ciertos miembros de la organización que establezcan una forma adicional de verificar su identidad. La configuración de la aplicación de autenticación se activa en cualquiera de los siguientes casos:

- El miembro seleccionado intenta iniciar sesión en la cuenta de Rescue en el sitio web seguro.
- El miembro seleccionado intenta iniciar sesión en la versión para ordenador de la Consola de técnico.
- El miembro seleccionado intenta cambiar su contraseña de Rescue.

Documentos técnicos de LastPass: https://enterprise.lastpass.com/wp-content/uploads/LastPass-Technical-Whitepaper-3.pdf

Por su parte, la autorización se realiza con mucha frecuencia: al menos una vez durante cada sesión de asistencia técnica remota. Un técnico se pondrá en contacto con el usuario final al que se presta asistencia después de que este descargue y ejecute el applet de asistencia técnica. El técnico podrá chatear con el usuario final a través del applet, pero cualquier otra acción, como enviar un archivo o ver el ordenador del usuario, necesitará el permiso expreso del usuario. También puede implementarse una “petición única”. Esto resulta útil en tareas de asistencia técnica remota largas, en las que el cliente podría no estar presente durante toda la sesión. Si se habilita este marcador para un grupo de técnicos, los técnicos de dicho grupo

podrán solicitar un permiso “global” al cliente y, si este lo concede, podrán realizar acciones como ver información del sistema o iniciar una sesión de control remoto sin que el usuario final tenga que autorizarlas.

Además, los administradores pueden imponer restricciones de dirección IP a sus técnicos. En este caso, las direcciones IP disponibles pueden restringirse a una lista muy reducida. De esta forma, los técnicos asignados a una tarea determinada solo podrán acceder a Rescue desde direcciones IP previamente aprobadas para esa tarea.

Además, el administrador de un grupo de técnicos puede deshabilitar determinadas funciones en el Centro de administración. Por ejemplo, puede impedirse que los miembros de un grupo de técnicos reciban archivos de los usuarios finales. Estos son algunos de los permisos que un administrador puede conceder o denegar:

- Iniciar el control remoto
- Reiniciar
- Iniciar la visualización del escritorio
- Grabar sesiones
- Enviar y recibir archivos
- Iniciar sesiones privadas
- Iniciar el Gestor de archivos
- Solicitar credenciales de Windows
- Enviar URL
- Permitir sincronización con portapapeles
- Ver información del sistema
- Implementar scripts
- Utilizar la petición única para todos los permisos
- Transferir sesiones
- Permitir las pantallas compartidas con los clientes

El sistema de Rescue se autentica también con el usuario final al que se presta asistencia técnica. El applet, descargado y ejecutado por el usuario, se firma con el certificado de firma de código de LogMeIn (basado en una clave RSA de 2048 bits), y esta información suele mostrarla al usuario su navegador web cuando va a ejecutar el software.

El usuario al que se presta asistencia técnica no se autentica. El técnico es quien debe determinar quién es el usuario, ya sea a través del chat o con una conversación telefónica.

El sistema de Rescue ofrece mecanismos similares a la autenticación, como códigos PIN únicos, pero se utilizan para redirigir la sesión de asistencia técnica a la cola privada o compartida correcta y no deben considerarse un sistema de autenticación.

AUDITORÍA Y REGISTRO

Toda solución de asistencia técnica remota debe conceder gran importancia a la responsabilidad. LogMeIn Rescue ofrece dos funciones de auditoría diferentes.

En primer lugar, el llamado “registro de chat” se guarda en la base de datos de Rescue. La Consola de técnico envía este registro de la conversación en tiempo real a los servidores de Rescue; el registro contiene sucesos y mensajes de chat de una sesión de asistencia técnica determinada. Por ejemplo, se mostraría un archivo de registro al iniciar o finalizar una sesión de control remoto o cuando el técnico envía al usuario final un archivo. Los metadatos correspondientes, como el nombre y la huella digital (hash) MD5 de un archivo transmitido, también se incluyen en el registro si procede. Desde el Centro de administración pueden realizarse consultas de la base de datos de registros de conversaciones. A fecha de publicación del presente documento, las políticas de retención de datos de LogMeIn estipulan que el contenido de los registros estará disponible en línea durante dos años tras el final de una sesión de asistencia técnica remota, y archivado durante dos años más. Para facilitar la integración con sistemas de CRM, LogMeIn Rescue puede publicar los datos de las sesiones en una URL. Los administradores pueden permitir que se excluya el texto de los chats de estos datos. Además, todos los registros del texto de los chats mantenidos entre técnicos y clientes pueden omitirse automáticamente de los datos de la sesión almacenados en el Centro de datos de Rescue.

En segundo lugar, LogMeIn Rescue permite a los técnicos grabar en un archivo de vídeo los sucesos que tienen lugar cuando ven un ordenador o realizan una sesión de control remoto. Esta es una función muy importante, por motivos de responsabilidad. Los archivos grabados se almacenan en un directorio especificado por el técnico. En las grandes organizaciones de asistencia técnica este directorio debe encontrarse en un servidor de red. El espacio de disco que ocupan estas grabaciones varía mucho, y depende total-

mente del contenido y las posibilidades de compresión del escritorio del usuario final al que se presta asistencia técnica. Basándonos en el análisis de millones de sesiones de control remoto en las que se ha utilizado la tecnología de LogMeIn, podemos decir que la media de espacio de disco necesario para un minuto de datos de control remoto oscila entre los 372 y los 1024 kbytes. Las grabaciones se almacenan directamente en AVI o en un formato intermedio propiedad de LogMeIn que puede convertirse en AVI con la aplicación "Rescue AVI Converter" disponible para descargar de help.logmein.com. El formato propiedad de LogMeIn, llamado RCREC, puede reducir el tamaño de la grabación aproximadamente un 10%.

ARQUITECTURA DEL CENTRO DE DATOS

LogMeIn Rescue está alojado en centros de datos modernos y seguros con las siguientes características:

- Procedimientos de control de seguridad multinivel, sistemas de acceso biométricos, sistema de circuito cerrado de televisión permanente y supervisión mediante alarmas.
- Alimentación de CA y CC redundante ininterrumpida, generadores de alimentación de reserva en las instalaciones.
- Diseño de acondicionamiento de aire redundante bajo suelos elevados para optimizar el control de temperatura.
- Sistema de detección de humos por encima y por debajo del suelo elevado, enclavamiento doble, acción previa, supresión de incendios mediante conductos secos.

La infraestructura de LogMeIn Rescue es, por sí sola, segura y fiable:

- Redundancia a nivel de componentes del servidor: fuentes de alimentación y ventiladores redundantes, discos duros con duplicación en espejo RAID-1
- Redundancia a nivel de servidor: dependiendo de la función, clústeres activos/pasivos o activos/activos
- Redundancia a nivel de centro de datos: Seis centros de datos (costa oeste de EE. UU., centro de EE. UU., centro-sur de EE. UU., costa este de EE. UU., Londres en el Reino Unido y Fráncfort en Alemania), con capacidad de conmutación por error casi instantánea
- Firewalls redundantes duales que solo tienen abiertos los puertos 80 y 443
- Clústeres de base de datos activos/pasivos
- Equilibradores de carga redundantes, con SSL incluido
- Clústeres de servidores web y de aplicaciones redundantes y con equilibrado de carga
- Clústeres de servidores de puerta de enlace redundantes y con equilibrado de carga

DESCRIPCIÓN GENERAL DEL PROCESO DE CONEXIÓN DE LA PUERTA DE ENLACE DE RESCUE

Cuando el applet de Rescue, firmado digitalmente, se inicia en un equipo:

- Contiene un GUID (Identificador único global) de autenticación de la sesión, que el sitio incrustó como recurso en el archivo .exe cuando se descargó.
- A continuación, descarga una lista de puertas de enlace disponibles de secure.logmeinrescue.com.
- Elige una puerta de enlace de la lista y se conecta a ella utilizando TLS. El applet autentica la puerta de enlace utilizando su certificado SSL.
- La puerta de enlace autentica el applet en la base de datos con el GUID y registra que el usuario está esperando a un técnico.

Cuando se elige una sesión en la Consola de técnico de Rescue:

- Se envía una solicitud a la puerta de enlace con el GUID de autenticación de la sesión para retransmitir las conexiones entre la Consola de técnico y el applet cliente.
- La puerta de enlace autentica la conexión y empieza a retransmitir los datos a nivel de transporte (no descifra los datos retransmitidos).

Cuando se inicia una retransmisión de conexión, las partes intentan establecer una conexión punto a punto (P2P):

- El applet comienza a recibir datos de una conexión TCP en un puerto asignado por Windows.

- Si no puede establecerse la conexión TCP en un periodo de tiempo establecido (10 segundos), se intenta establecer una conexión UDP con ayuda de la puerta de enlace.
- Si se establece una conexión TCP o UDP, las partes autentican el canal P2P (utilizando el GUID de autenticación de la sesión) y se asume el tráfico de la conexión retransmitida.
- Si se ha establecido una conexión UDP, se emula el TCP sobre los datagramas de UDP con XTCP, un protocolo propiedad de LogMeIn basado en la pila TCP BSD.

Todas las conexiones se protegen con el protocolo TLS (utilizando cifrado AES256 con MAC SHA256). El GUID de autenticación de la sesión es un valor entero criptográficamente aleatorio de 128 bits.

BASE DE DATOS

- Todos los datos almacenados en la base de datos y que contienen información confidencial (el registro de la conversación y los campos personalizados) se protegen mediante cifrado AES de 256 bits.
- Se realiza una copia de seguridad automática de la base de datos de Rescue cada 24 horas. La copia de seguridad de la base de datos se almacena en el centro de datos con el mismo cifrado que la versión original.
- La opción de residencia de datos de Rescue le permite elegir dónde desea guardar los datos de los usuarios finales: en la Unión Europea (Fráncfort, Londres) o en los Estados Unidos. LogMeIn garantiza que al elegir la residencia de datos en la Unión Europea solo se establecerá conexión con centros de datos de la Unión Europea, y que los datos del cliente permanecerán exclusivamente dentro de la región seleccionada. No hay ninguna conexión entre nuestros centros de datos de la Unión Europea y de los Estados Unidos.

LA ARQUITECTURA MULTIMEDIA DE RESCUE

El servicio multimedia de Rescue es un servicio independiente basado en WebRTC que gestiona las transmisiones de vídeo de Rescue Lens. Gestiona las denominadas conferencias de las sesiones de Rescue en las que se utiliza la función Lens. Los participantes de la conferencia (interlocutores) se unen a las conferencias y salen de ellas, mientras que los clientes envían secuencias de vídeo y audio para que otros participantes las reciban. Lens envía el contenido de vídeo en un flujo unidireccional desde la aplicación Rescue Lens hasta la Consola de técnico.

El servicio multimedia tiene tres componentes principales: MediaSDK, el Gestor de sesiones y el Servidor de transmisión. Estos componentes gestionan el proceso de crear/eliminar conferencias, y de unirse a ellas/salir de ellas. Se comunican por medio de las conexiones seguras existentes entre la Consola de técnico y el sitio web y entre la aplicación Lens y el sitio web.

MediaSDK

El servicio multimedia está basado en WebRTC con una fina capa creada en torno a la base de código de WebRTC. La tecnología MediaSDK se utiliza en la Consola de técnico y en las aplicaciones Lens para móviles.

Gestores de sesiones

El Gestor de sesiones es un sitio web con carga equilibrada sencilla que proporciona una API REST para gestionar (crear/eliminar/unirse/salir) las conferencias. El Gestor de sesiones solo acepta solicitudes procedentes del sitio web.

Servidores de transmisión

El servicio multimedia utiliza el servidor de transmisión de código abierto Jitsi para gestionar las transmisiones entre interlocutores (la Consola de técnico y la aplicación Lens). Tanto la Consola de técnico como la aplicación Lens se conectan al servidor de transmisión. La aplicación Lens transmite su contenido de vídeo al servidor de transmisión. La

Consola de técnico transmite el contenido de vídeo desde el servidor. Jitsi actúa como servidor de retransmisión entre los interlocutores. Una sesión de Lens engloba dos transmisiones (una que se envía y otra que se recibe).

ESTÁNDARES DEL SECTOR DE LOGMEIN RESCUE

SOC 2

LogMeIn Rescue tiene la certificación Service Organization Control 2 (SOC 2), lo que garantiza a los clientes que utilizamos los controles adecuados para proteger sus datos importantes.

SOC 2 es un procedimiento de auditoría exhaustivo que se basa en distintos principios y criterios. Somete a pruebas los sistemas de control utilizados para procesar datos y la confidencialidad de la información procesada por estos sistemas. Es necesario realizar una revisión anual para mantener la certificación SOC 2. Teniendo en cuenta que se trata de la referencia número uno empresas de software, con un amplio reconocimiento en los Estados Unidos en numerosos sectores, la obtención de la certificación SOC 2 ratifica nuestro compromiso con la seguridad y la privacidad.

RGPD

El Reglamento General de Protección de Datos (RGPD) es una ley de la Unión Europea (UE) que rige la protección y privacidad de los datos de los residentes en la Unión Europea. El objetivo principal del RGPD es ceder el control de sus datos personales a los ciudadanos y residentes, y también simplificar el entorno reglamentario en la UE. LogMeIn Rescue ofrece a sus usuarios control de los datos que almacenamos en su nombre (Contenido, según se define en los Términos del servicio) para ayudarles a centrarse en el desarrollo de su actividad empresarial al tiempo que se preparan para el RGPD de una manera eficiente.

- Los usuarios de Rescue pueden exportar sus datos con la funcionalidad de informes del Centro de administración de las API de Rescue.
- Los usuarios de Rescue pueden eliminar sus datos almacenados en los servidores de LogMeIn Rescue.
  - Eliminar todos los datos relacionados con un técnico de asistencia técnica.
  - Eliminar todos los datos relacionados con una sesión de asistencia técnica, incluidos los datos personales y vinculados a sus clientes.

Mediante estas funcionalidades, LogMeIn Rescue permite a sus usuarios cumplir los estándares y los requisitos del RGPD.

Si desea obtener información detallada sobre el RGPD, visite el sitio web del RGPD de LogMeIn.

HIPAA

Aunque LogMeIn no puede controlar el contenido que comparten los usuarios durante una sesión de asistencia técnica, el servicio de LogMeIn Rescue está diseñado para cumplir unas estrictas normas de seguridad y ayudar a que las entidades reguladas por la normativa HIPAA cumplan las directrices reguladoras correspondientes.

Controles de acceso

- Definir el acceso basado en permisos con todo detalle (por ejemplo, permitir que algunos técnicos utilicen la visión remota, pero no el control remoto).
- Los datos de los dispositivos remotos no se almacenan en los servidores del centro de datos de LogMeIn (como se ha indicado anteriormente, solo se almacenan datos de sesiones y conversaciones). Además, los registros del texto de los chats pueden eliminarse de los datos de la sesión.
- Es posible configurar los permisos para impedir que los técnicos transfieran archivos, por lo que no podrán extraer archivos de dispositivos remotos.

- El usuario final debe encontrarse en el dispositivo remoto y permitir el acceso remoto.
- El usuario final mantiene el control, y puede finalizar la sesión en cualquier momento.
- Se puede impedir que los técnicos accedan a determinadas funciones hasta que el usuario final les haya concedido permiso explícito (ejemplo: control remoto, vista del escritorio, transferencia de archivos, información del sistema, reinicio y reconexión).
- Los derechos de acceso se revocan automáticamente al terminar la sesión.
- Un tiempo de inactividad predeterminado fuerza el cierre automático de la sesión
- Alojamiento en centros de datos Carrier Grade redundantes, con acceso seguro y restringido.

Controles de auditoría

- Opción de forzar la grabación de sesiones, con capacidad para almacenar archivos de auditoría en un recurso compartido de la red seguro.
- La actividad de las sesiones remotas y las sesiones del técnico se registra en el ordenador host para garantizar la seguridad y mantener el control de calidad (inicios de sesión correctos, inicios de sesión erróneos, inicio de control remoto, fin de control remoto, comienzo del reinicio, cierre de sesión).
- Autenticación de personas o entidades.
- La identidad del técnico se define mediante una dirección de correo electrónico exclusiva o un ID de SSO. El técnico debe autenticarse.
- Un número excesivo de intentos de inicio de sesión incorrectos bloqueará la cuenta.
- Solo se permite que los técnicos inicien sesión desde las direcciones IP autorizadas.

Seguridad de transmisión

- Cifrado AES de 256 bits integral de todos los datos
- Hash MD5 para mejorar la trazabilidad de las transferencias de archivos

CONCLUSIÓN

La elección de una solución de asistencia técnica remota suele basarse en funciones y precios. Si está leyendo este documento, lo más probable es que LogMeIn Rescue se haya adaptado a sus necesidades en estas categorías. Con la anterior información creemos haber demostrado que la arquitectura que está detrás de Rescue proporciona los niveles adecuados de escalabilidad, seguridad, fiabilidad y facilidad de uso.