Rescue by LogMeIn

ARCHITECTURE ET SÉCURITÉ DE RESCUE

Fiche de présentation

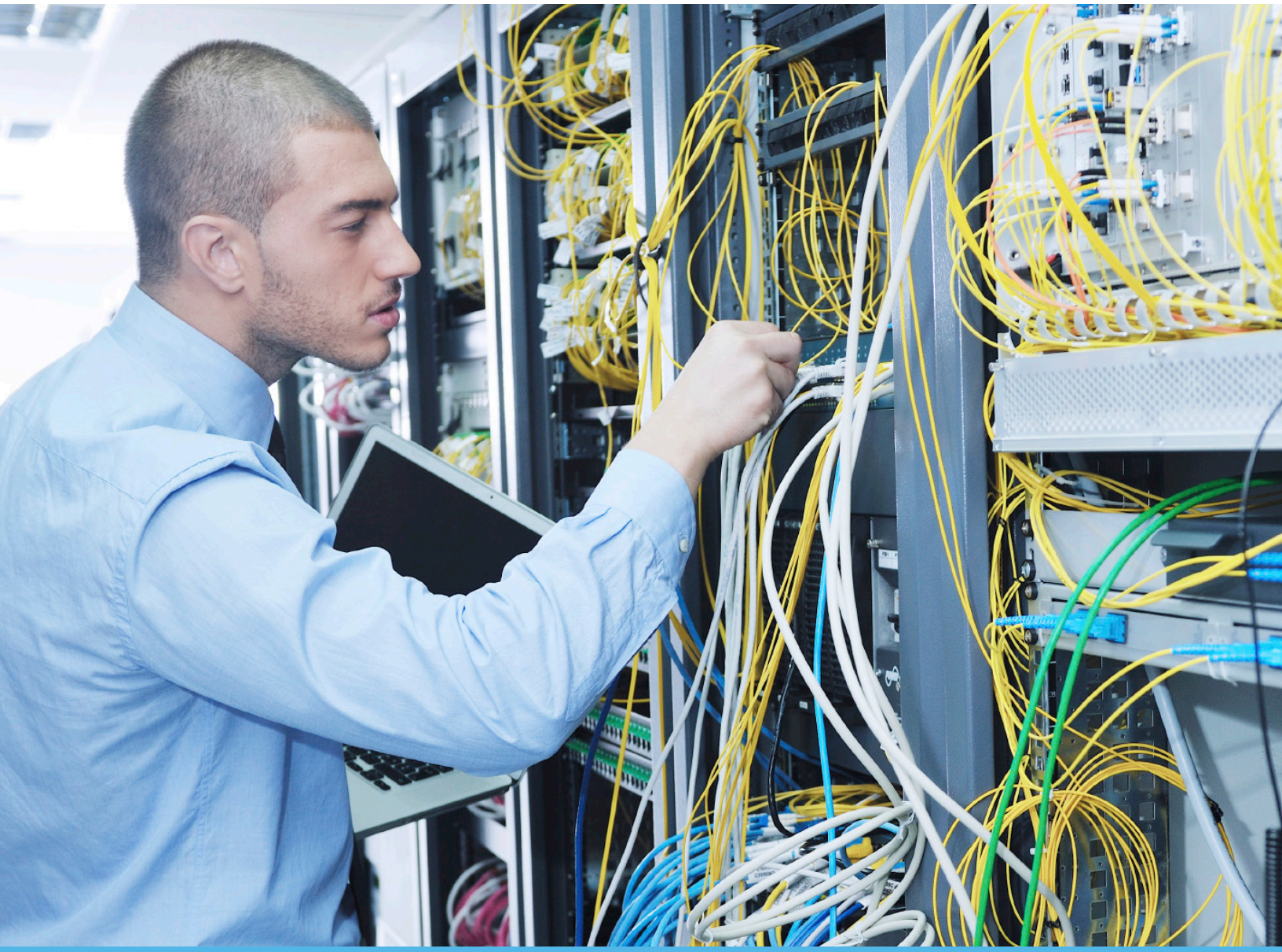


Table des matières

INTRODUCTION

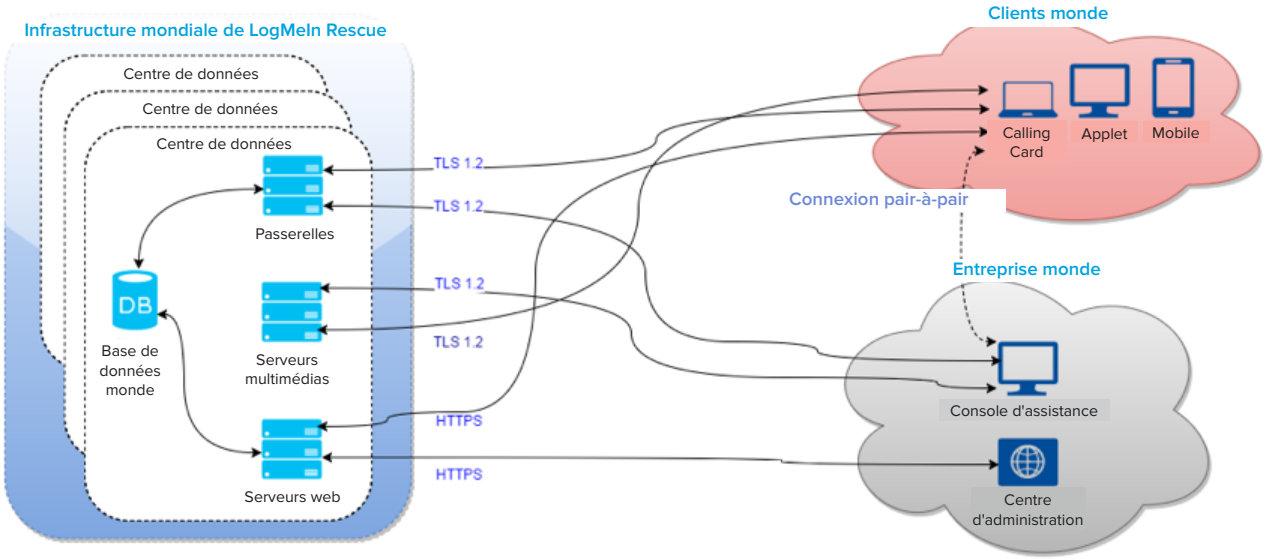
Évolutivité, sécurité, fiabilité, convivialité. Ce sont ces quatre caractéristiques qui définissent une solution d'assistance à distance d'exception, bien qu'elles ne soient pas toujours compatibles. Vous trouverez aisément des solutions d'assistance à distance qui répondent à deux ou trois de ces critères, mais les solutions qui réussissent sur ces quatre fronts sont rares. LogMeIn, Inc. offre une telle solution sous la forme de LogMeIn Rescue.

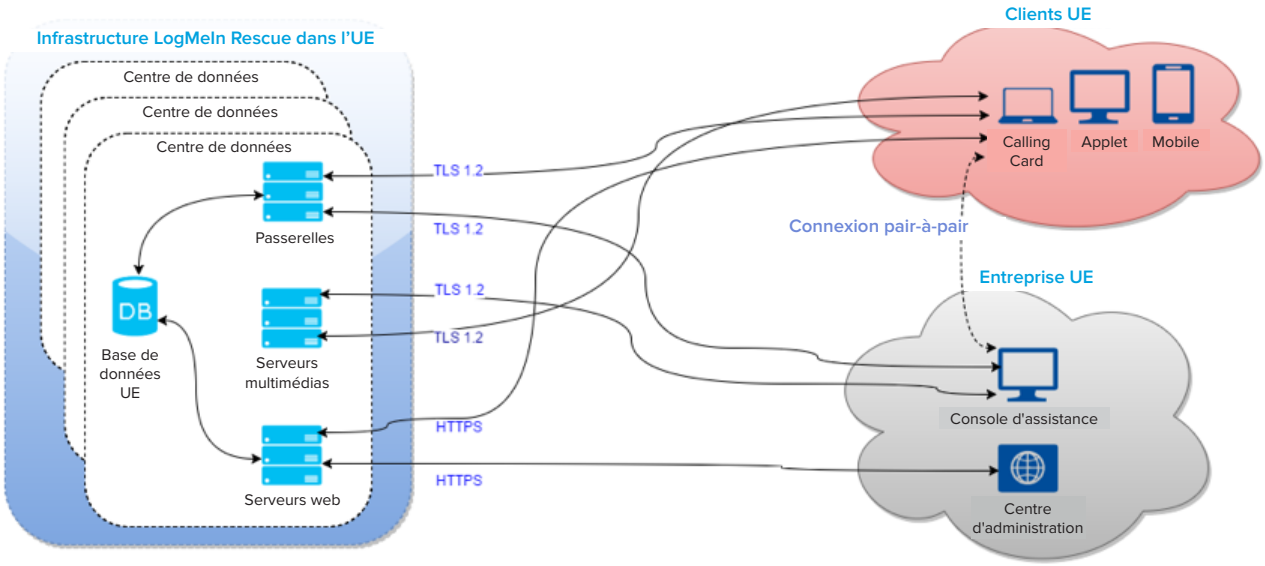
Évolutivité. Que vous ayez un seul technicien ou un centre d'appel de dix milles employés, Rescue est à la hauteur.

Sécurité. Les sessions d'assistance sont protégées par un chiffrement de bout en bout AES sur 256 bits. L'utilisateur doit autoriser les opérations d'assistance avant que le technicien ne puisse les entreprendre. Les journaux des séances d'assistance sont stockés dans un format chiffré dans une base de données interrogeable plus tard. Les sessions de contrôle à distance peuvent être enregistrées dans un fichier vidéo.

Fiabilité. Rescue est hébergé dans six centres de données de classe transporteur dotés d'infrastructures totalement redondantes.

Convivialité. Il suffira de quelques heures pour que vos techniciens soient opérationnels. Vos utilisateurs finaux peuvent obtenir de l'aide en quelques clics. Aucune installation logicielle n'est requise de part et d'autre.





CONFIDENTIALITÉ DES DONNÉES

L'on associe généralement la sécurité à la confidentialité des données, la confidentialité des données au chiffrement, et le chiffrement est généralement caractérisé par le chiffrement symétrique et la longueur de clé. Ces idées fausses conduisent à des expressions malheureuses comme « sécurité AES 256 bits ». Car il s'agit bien d'une notion trompeuse.

Un système en ligne sécurisé doit toujours répondre aux conditions suivantes :

- Authentification des parties communicantes
- Négociation des clés de chiffrement sans possibilité d'interception par un intermédiaire
- Échange confidentiel des messages
- Possibilité de détecter la modification éventuelle d'un message en transit

SSL/TLS (Secure Sockets Layer / Transport Layer Security) a été conçu pour la prise en charge des étapes ci-dessus. Créé par Netscape Communications Corporation au milieu des années 90, ce protocole s'est imposé comme le standard de fait pour les communications sécurisées sur Internet. Il est notamment utilisé par Visa, MasterCard et American Express.

LogMeIn Rescue utilise la version OpenSSL (http://www.openssl.org) du SSL. LogMeIn utilise systématiquement la dernière version. Au moment de la publication, Rescue utilise la version 1.0.2j.

NÉGOCIATION DES CLÉS

Lorsqu'une session d'assistance démarre et qu'une connexion est établie entre l'utilisateur et le technicien, leurs ordinateurs doivent s'accorder sur l'algorithme de chiffrement et la clé associée qui seront utilisés durant la session. L'importance de cette étape est souvent sous-estimée, ce qui peut se comprendre. Il s'agit à priori d'une tâche routinière des plus banales.

Or, elle est tout sauf simple. Pour contrer une attaque par un intermédiaire (où un ordinateur C se positionne entre les ordinateurs A et B pour se faire passer pour l'autre partie auprès de A et B), il faut utiliser un certificat. Puisque ni le technicien, ni l'utilisateur final n'ont de logiciel serveur ou de certificat SSL installés sur leurs ordinateurs, ils doivent se tourner vers un des serveurs LogMeIn Rescue et effectuer cette phase initiale de négociation de clés avec cet ordinateur. La vérification du certificat par la console d'assistance et par l'applet de l'utilisateur final garantit que seul un ordinateur Rescue peut négocier ce processus.

ÉCHANGE DE MESSAGES

TLS autorise l'utilisation d'un vaste éventail de suites de chiffrement, et les parties en communication peuvent s'accorder sur un type de chiffrement pris en charge par les deux ordinateurs. Cette stratégie à deux principaux objectifs. Tout d'abord, le protocole peut être enrichi par de nouvelles suites de chiffrement sans entraîner des problèmes de rétrocompatibilité. Ensuite, ces versions plus récentes peuvent abandonner la prise en charge de types de chiffrement connus pour leurs faiblesses cryptographiques.

Puisque tous les composants du système de communication LogMeIn Rescue sont contrôlés par LogMeIn, le type de chiffrement utilisé par ces composants est invariable : AES256-SHA en mode CBC (cipher-block chaining) avec négociation de clé RSA. Les implications sont les suivantes :

- Les clés de chiffrement sont échangées sous forme de paires de clés RSA privées/publiques, comme décrit à la section précédente
- L'algorithme de chiffrement/déchiffrement AES (Advanced Encryption Standard) est utilisé
- La clé de chiffrement a une longueur de 256 bits
- SHA-2 sert de base aux codes d'authentification des messages (MAC). Un MAC est un court segment de données servant à l'authentification d'un message. La valeur de MAC garantit l'intégrité du message ainsi que son authenticité en permettant aux parties en communication de détecter toute modification éventuelle du message.
- Le mode CBC (cipher-block chaining) permet d'assurer que chaque bloc de texte chiffré est dépendant des blocs de texte en clair jusqu'à ce point, et que des messages similaires ne peuvent pas être identifiés sur le réseau.

Tout cela permet d'assurer que les données transmises entre l'utilisateur final et le technicien sont chiffrées de bout en bout, et que seules les parties respectives ont accès aux informations contenues dans le flux des messages.

AUTHENTIFICATION ET AUTORISATION

L'authentification et les autorisations ont deux objectifs distincts dans LogMeIn Rescue.

L'authentification garantit que le technicien ou l'administrateur qui se connecte au système Rescue est bien la personne qu'elle prétend être. L'authentification est gérée de façon très simple : les techniciens reçoivent leurs identifiants de connexion (généralement leur adresse e-mail) et les mots de passe correspondants de leur administrateur. Le technicien entre ces données d'identification dans le formulaire de connexion de LogMeIn Rescue au début de sa journée de travail.

Sous LogMeIn Rescue, le système Rescue s'authentifie d'abord auprès du technicien (plus précisément de son navigateur web) avec son certificat SSL RSA haut de gamme sur 2048 bits. Cela permet d'assurer que le technicien saisit son nom d'utilisateur et mot de passe sur le bon site web. Le technicien se connecte alors au système avec ses identifiants.

LogMeIn Rescue ne stocke pas les mots de passe, mais utilise scrypt pour créer des hachages des mots de passe qui sont stockés dans la base de données Rescue. Les hachages sont ensuite salés avec une chaîne de 24 caractères générée par CSPRNG pour chaque mot de passe unique.

LogMeIn Rescue offre plusieurs options de règles de mots de passe aux administrateurs :

- Les administrateurs peuvent imposer une fiabilité minimale du mot de passe ainsi que sa durée de vie – une jauge indique aux administrateurs et techniciens la fiabilité du mot de passe choisi.
- Les techniciens peuvent être obligés à changer de mot de passe lors de la connexion suivante
- L'administrateur principal peut forcer les membres de son organisation à utiliser la vérification en deux étapes pour la connexion à Rescue.

LogMeIn Rescue permet également aux administrateurs de mettre en œuvre un système de connexion unique. Le langage SAML (Security Assertion Markup Language) est utilisé à cette fin. Il s'agit d'une norme XML d'échange de données d'authentification et d'autorisation entre domaines de sécurité (comme entre un fournisseur d'identité et un fournisseur de services). Les techniciens n'ont alors accès qu'à des applications prédéfinies, par le biais d'un identifiant de connexion unique. L'identifiant unique d'un technicien peut être désactivé en un clic.

La fonctionnalité de vérification en deux étapes utilise LastPass Authenticator pour fournir une deuxième couche de protection aux comptes Rescue en obligeant les membres sélectionnés à configurer un moyen supplémentaire de vérification de leur identité. La configuration de l'app Authenticator est déclenchée dans les cas suivants :

- Le membre sélectionné essaie de se connecter à son compte Rescue sur le site web sécurisé.
- Le membre sélectionné essaie de se connecter à la console d'assistance de bureau.
- Le membre sélectionné essaie de changer son mot de passe Rescue.

Livre blanc technique sur LastPass : https://enterprise.lastpass.com/wp-content/uploads/LastPass-Technical-Whitepaper-3.pdf

L'autorisation, quant à elle, survient très fréquemment, au moins une fois par session d'assistance à distance. Lorsque l'utilisateur final a téléchargé et lancé l'applet d'assistance, il est contacté par un technicien. Le technicien peut chatter avec l'utilisateur via l'applet, mais toute autre action, comme l'envoi d'un fichier ou l'affichage de l'écran de l'utilisateur, requiert l'autorisation explicite de l'utilisateur. Une « invite unique » peut également être mise en œuvre. Elle est conçue pour les interventions à distance prolongées, lorsque le client peut ne pas être présent durant toute la session. Lorsque cette option est activée pour un groupe de techniciens, les techniciens peuvent demander une autorisation « globale » de la part du client, ce qui lui permettra d'effectuer des tâches comme afficher des informations

système ou initier une session de contrôle à distance sans autorisation supplémentaire de l'utilisateur final.

Les administrateurs peuvent également appliquer des restrictions d'adresses IP à leurs techniciens. Dans ce cas, les adresses IP disponibles peuvent être limitées à une liste très restreinte. Les techniciens affectés à une tâche particulière ne peuvent alors accéder à Rescue que depuis des adresses IP validées pour cette tâche.

L'administrateur d'un groupe de techniciens peut également désactiver certaines fonctionnalités dans le Centre d'administration. Par exemple, il peut empêcher que les membres d'un groupe de techniciens puissent recevoir des fichiers de la part des utilisateurs finaux. Voici des autorisations que les administrateurs peuvent accorder ou refuser :

- Lancer le contrôle à distance
- Redémarrer
- Lancer l'affichage du bureau
- Enregistrer les sessions
- Envoyer et recevoir des fichiers
- Démarrer des sessions privées
- Lancer le gestionnaire de fichiers
- Demander les identifiants Windows
- Envoyer des URL
- Autoriser la synchronisation du presse-papiers
- Afficher les informations système
- Déployer des scripts
- Utiliser une invite unique pour toutes les autorisations
- Transférer des sessions
- Autoriser le partage d'écran avec les clients

Le système Rescue s'authentifie également auprès de l'utilisateur final. L'applet téléchargée et exécutée par l'utilisateur est signée avec le certificat de signature de code de LogMeIn (basé sur une clé RSA de 2048 bits), et cette information est généralement présentée à l'utilisateur dans son navigateur web avant de lancer le logiciel.

L'utilisateur qui reçoit l'assistance n'est pas authentifié. Il incombe au technicien de déterminer l'identité de l'utilisateur, par chat ou par conversation téléphonique. Toutefois, le système Rescue fournit des mécanismes apparentés à l'authentification comme les codes PIN uniques, mais ils servent à acheminer la session d'assistance à la file d'attente privée ou partagée pertinente, et ne doivent pas être considérés comme un système d'authentification.

AUDIT ET JOURNALISATION

Toute solution d'assistance à distance doit mettre l'accent sur la responsabilité. LogMeIn Rescue offre deux fonctions d'audit distinctes :

Tout d'abord, un « journal de chat » est enregistré dans la base de données de Rescue. Le journal de chat est transmis aux serveurs de Rescue en temps réel par la console d'assistance. Il contient les événements et les messages associés à une session d'assistance donnée. Un fichier journal est par exemple affiché au démarrage ou à la fermeture d'une session de contrôle à distance, ou lorsqu'un fichier est envoyé par le technicien à l'utilisateur final. Les métadonnées associées, comme le nom et le hachage MD5 d'un fichier transféré, sont également consignées dans le journal. La base de données du journal de chat peut être interrogée depuis le Centre d'administration. Au moment de la publication de ce document, les règles de conservation de données de LogMeIn stipulent que les journaux restent disponibles en ligne pendant deux années à compter de la fermeture d'une session d'assistance à distance, puis sont archivées pendant deux années supplémentaires. Pour simplifier l'intégration avec les systèmes de gestion de la relation client, LogMeIn Rescue peut envoyer des informations de session via une URL. L'administrateur a l'option d'exclure le contenu du chat de ces informations. En outre, tous les enregistrements des messages de chat entre techniciens et clients peuvent être automatiquement omis des informations de session stockées dans le centre de données Rescue.

Ensuite, LogMeIn Rescue permet aux techniciens de consigner les événements qui surviennent lors d'une session d'affichage de bureau ou de contrôle à distance dans un fichier vidéo. Cette option est particulièrement importante en matière de responsabilité ou en cas de litige. Les enregistrements sont stockés dans un répertoire spécifié par le technicien. Les organisations d'assistance de taille importante ont intérêt à les stocker sur un serveur. L'espace

disque occupé par ces enregistrements est très variable et dépend du contenu (et de la possibilité de plus ou moins le compacter) qui s'affiche sur l'écran de l'utilisateur final. Toutefois, une analyse de millions de sessions de contrôle à distance exploitant les technologies LogMeIn indique que l'espace disque moyen requis pour stocker une minute de données de contrôle à distance varie entre 372 et 1024 Ko. Les enregistrements sont stockés directement au format AVI ou dans un format intermédiaire propriétaire de LogMeIn, convertible en fichiers AVI standard avec l'application « Rescue AVI Converter » proposée au téléchargement sur help.logmein.com. Le format propriétaire de LogMeIn, appelé RCREC, peut réduire la taille des enregistrements d'environ 10 %.

ARCHITECTURE DU CENTRE DE DONNÉES

LogMeIn Rescue est hébergé dans des centres de données sécurisés haut de gamme dotés des caractéristiques suivantes :

- Procédures de contrôle à plusieurs niveaux, systèmes d'accès biométriques, vidéosurveillance 24x7 et surveillance des alarmes
- Alimentation CA et CC sur onduleur avec générateurs de secours sur site
- Système de refroidissement redondant avec distribution d'air sous planchers surélevés pour un contrôle optimal de la température
- Système de détection de fumée au dessus et en dessous du plancher surélevé, double sas et extincteurs d'incendie

L'infrastructure LogMeIn Rescue est elle-même hautement sécurisée et fiable :

- Redondance au niveau des composants des serveurs : alimentation et ventilateurs redondants, disques durs RAID-1 en miroir
- Redondance au niveau des serveurs : grappes actifs/passifs ou actifs/actifs, selon les rôles
- Redondance au niveau du centre de données : Six centres de données (côte ouest, centre, sud et côte est des États-Unis, Londres au Royaume-Uni et Francfort en Allemagne), avec capacité de basculement quasi instantané
- Double pare-feu redondant (seuls les ports 80 et 443 sont ouverts)
- Grappes de bases de données actives/passives
- Équilibreurs de charge redondants, y compris SSL
- Grappes de serveurs d'applications et de services web redondants à charge équilibrée
- Grappes de serveurs passerelle redondants à charge équilibrée

PRÉSENTATION DU PROCESSUS DE TRANSMISSION DE LA PASSERELLE LOGMEIN RESCUE

Lorsqu'une applet Rescue signée est lancée sur un ordinateur :

- Elle contient un identifiant unique global (GUID) d'authentification de session intégré au fichier .exe sous forme de ressource par le site au moment du téléchargement
- Elle télécharge ensuite une liste des passerelles disponibles depuis secure.logmeinrescue.com
- Elle choisit une passerelle dans la liste et s'y connecte par TSL ; la passerelle est authentifiée par l'applet avec son certificat SSL
- La passerelle authentifie l'applet dans la base de données avec le GUID et spécifie que l'utilisateur est en attente d'un technicien

Lorsqu'une session est activée dans la console d'assistance du technicien :

- Une demande est envoyée à la passerelle avec le GUID d'authentification de session à des connexions relais entre la console d'assistance et l'applet client
- La passerelle authentifie la connexion et se met à relayer les données au niveau du transport de données (elle ne déchiffre pas les données relayées)

Lorsqu'un relais de connexion est démarré, les parties tentent d'établir une connexion point à point (P2P) :

- L'applet se met à l'écoute d'une connexion TCP sur un port attribué par Windows
- Si la connexion TCP n'est pas établie sous un délai prédéfini (10 secondes), une tentative de connexion UDP est lancée, à l'aide de la passerelle
- Lorsqu'une connexion TCP ou UDP est établie, les parties authentifient le canal P2P (avec le GUID d'authentification des sessions) qui prend alors le contrôle du trafic
- Lorsqu'une connexion UDP est configurée, TCP est émulé sur les datagrammes UDP avec XTCP, un protocole propriétaire de LogMeIn basé sur la pile TCP BSD

Chaque connexion est sécurisée avec le protocole TLS (avec chiffrement AES256 avec MAC SHA256). Le GUID d'authentification des sessions est une valeur d'entier aléatoire chiffrée de 128 bits.

BDD

- Toutes les données sensibles sont protégées par chiffrement AES sur 256 bits (journal de chat et champs personnalisés).
- La base de données Rescue est automatiquement sauvegardée toutes les 24 heures. La base de données de sauvegarde est stockée dans le centre de données avec le même chiffrement que l'original.
- L'option de résidence des données de Rescue vous permet de choisir la destination des données des utilisateurs finaux : en Europe (Francfort, Londres), ou aux États-Unis. LogMeIn garantit que ceux qui choisissent de faire résider les données dans l'UE ne se connecteront qu'aux centres de données dans l'UE et que les données des clients resteront dans la région choisie. Nos centres de données dans l'UE et aux USA ne sont pas connectés.

ARCHITECTURE MULTIMÉDIA DE RESCUE

Le service multimédia de Rescue est un service autonome basé sur WebRTC qui régit le streaming vidéo dans Rescue Lens. Il gère les « conférences » des sessions Rescue qui utilisent la fonctionnalité Lens. Les participants aux conférences (les pairs) rejoignent et quittent les conférences et les clients envoient des flux audio et vidéo aux autres participants. Lens envoie du contenu vidéo sous forme de flux unidirectionnel depuis l'app Lens vers la Console d'assistance.

Le service multimédia a trois composants principaux : le SDK multimédia, le gestionnaire de session et le gestionnaire de streaming. Ces composants gèrent les processus de création/destruction et de connexion/déconnexion des conférences. Ces composants communiquent via les canaux de communication sécurisés existants entre la Console d'assistance et le site web, et entre l'app Lens et le site web.

MediaSDK

Le service multimédia est bâti sur WebRTC, avec une fine couche autour du code WebRTC. Ce « SDK multimédia » est utilisé par la Console d'assistance et l'app mobile Lens.

Gestionnaires de session

Le gestionnaire de session est un simple site web avec équilibrage de charge qui fournit une API REST pour gérer (créer/détruire/rejoindre/quitter) les conférences. Le gestionnaire de session n'accepte des requêtes que de la part du site web.

Serveurs de streaming

Le service multimédia utilise la solution de serveur de streaming open source Jitsi pour la gestion des flux entre les pairs (la Console d'assistance et l'app Lens). La Console d'assistance et l'app Lens sont tous deux connectés au serveur de streaming. L'app Lens diffuse son contenu vidéo vers le serveur de streaming. La Console d'assistance

récupère le flux vidéo depuis le serveur. Jitsi fonctionne comme un serveur relais entre les pairs. Les sessions Lens exploitent deux flux (l'un est envoyé et l'autre est reçu).

NORMES ET LOGMEIN RESCUE

SOC 2

LogMeIn Rescue est certifié SOC 2 (Service Organization Control 2), ce qui garantit aux clients que nous effectuons les contrôles nécessaires pour protéger leurs données importantes.

SOC 2 est une procédure d'audit exhaustive, basée sur de nombreux principes et critères, testant les systèmes de contrôle utilisés pour traiter les données et la confidentialité des informations traitées par ces systèmes. Une évaluation annuelle est nécessaire pour conserver la certification SOC 2. Nous soumettre au processus SOC 2, un « étalon-or » reconnu dans le monde entier et sur de nombreux secteurs d'activité, est une illustration supplémentaire de notre engagement en faveur de la sécurité et de la confidentialité.

RGPD

Le Règlement général sur la protection des données (RGPD) est une législation de l'Union européenne (UE) portant sur la protection et la confidentialité des données de tous les résidents de l'UE. Le RGPD vise principalement à donner à ses citoyens et résidents le contrôle de leurs données personnelles et à simplifier l'environnement réglementaire à l'échelle de l'UE. LogMeIn Rescue permet à ses utilisateurs de contrôler les données que nous stockons en leur nom (le Contenu, tel que défini dans les Conditions générales) pour qu'ils puissent se concentrer sur leur cœur de métier tout en se conformant efficacement au RGPD.

- Les utilisateurs de Rescue peuvent exporter leurs données existantes à l'aide des fonctions de reporting disponibles dans le Centre d'administration ou via les API Rescue.
- Les utilisateurs de Rescue peuvent supprimer leurs données des serveurs LogMeIn Rescue.
  - Supprimer toutes les données liées à un technicien d'assistance.
  - Supprimer toutes les données liées à une session d'assistance, y compris les données personnelles et les données associées à leurs clients.

Grâce à ces fonctionnalités, LogMeIn Rescue permet à ses utilisateurs de respecter les normes et exigences du RGPD.

Pour des informations détaillées sur le RGPD, visitez le site RGPD de LogMeIn.

HIPAA

Bien que LogMeIn ne puisse pas contrôler le contenu échangé entre les utilisateurs lors d'une session à distance, le service LogMeIn Rescue est conçu pour répondre aux exigences de sécurité strictes qui permet aux entités soumises à la réglementation HIPAA de se conformer à ses exigences.

Contrôle des accès

- Définition d'accès spécifiques à base d'autorisations (comme limiter certains techniciens à l'utilisation de l'affichage à distance sans prise de contrôle)
- Aucune donnée provenant d'appareils distants n'est stockée sur les serveurs du centre de données LogMeIn (encore une fois, seules les données de session et journaux de chat sont stockés). En outre, les messages de chat peuvent être exclus des détails de session.
- Les autorisations peuvent bloquer les transferts de fichiers par les techniciens, afin de les empêcher de récupérer des fichiers sur les appareils distants.

- L'utilisateur final doit être présent auprès de l'appareil distant et autoriser l'accès à distance
- L'utilisateur final garde le contrôle, et peut terminer la session à tout instant
- Les techniciens peuvent être empêchés d'utiliser certaines fonctionnalités tant que l'utilisateur final n'a pas accordé explicitement son autorisation (comme le contrôle à distance, l'affichage du bureau, le transfert de fichiers, la récupération d'informations système ou le redémarrage et la reconnexion)
- Les droits d'accès sont automatiquement révoqués à la clôture de la session
- Un délai d'inactivité prédéfini entraîne une déconnexion automatique
- Hébergement dans des centres de données redondants de classe transporteur avec accès sécurisé restreint

Contrôles d'audit

- Option pour forcer l'enregistrement des sessions, avec possibilité de stocker les fichiers d'audit sur des partages réseau sécurisés
- Les sessions de techniciens et l'activité des sessions à distance sont consignées sur l'ordinateur hôte à des fins de sécurité et de contrôle qualité (connexions réussies, échecs de connexion, contrôle à distance lancé, contrôle à distance terminé, redémarrage initié, déconnexion)
- Authentification de personnes ou d'entités
- L'identité du technicien est définie par une adresse e-mail unique ou par un identifiant à connexion unique, et le technicien doit être authentifié
- Un certain nombre de tentatives de connexion infructueuses entraîne le verrouillage du compte
- La connexion des techniciens peut être limitée à des adresses IP approuvées

Sécurité des transmissions

- Chiffrement AES sur 256 bits de bout en bout de toutes les données
- Hachage MD5 pour une plus grande traçabilité des transferts de fichiers

CONCLUSION

Le choix d'une solution d'assistance à distance s'appuie généralement sur les fonctionnalités et le prix. Si vous lisez ce document, cela signifie sans doute que LogMeIn Rescue répond à vos exigences en la matière. Nous espérons en outre que les informations présentées ci-dessus prouvent que l'architecture de Rescue offre un niveau optimal d'évolutivité, de sécurité, de fiabilité et de convivialité.