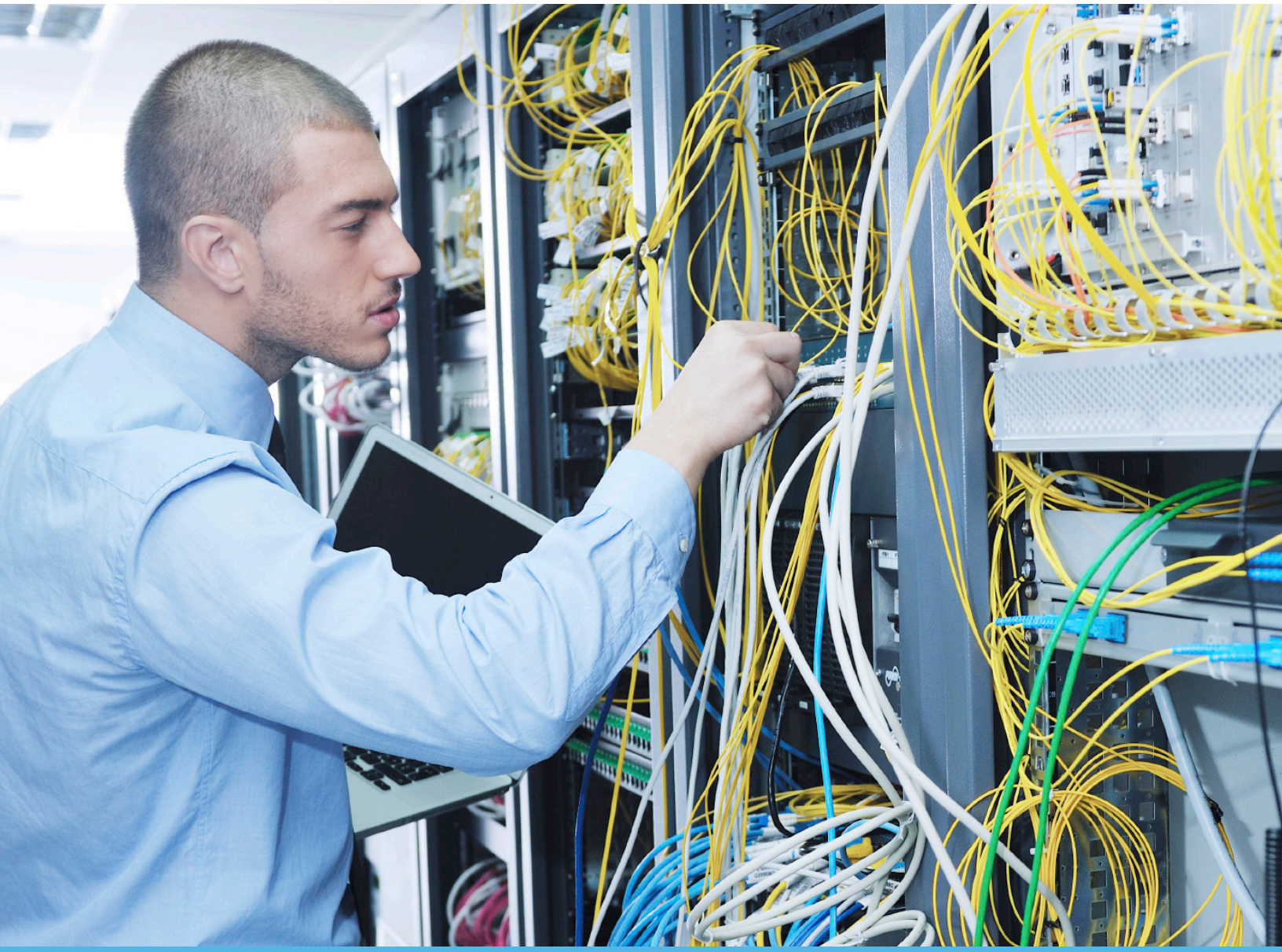
Rescue by LogMeIn

ARQUITETURA E SEGURANÇA DO RESCUE

Brochura de visão geral



Índice

INTRODUÇÃO

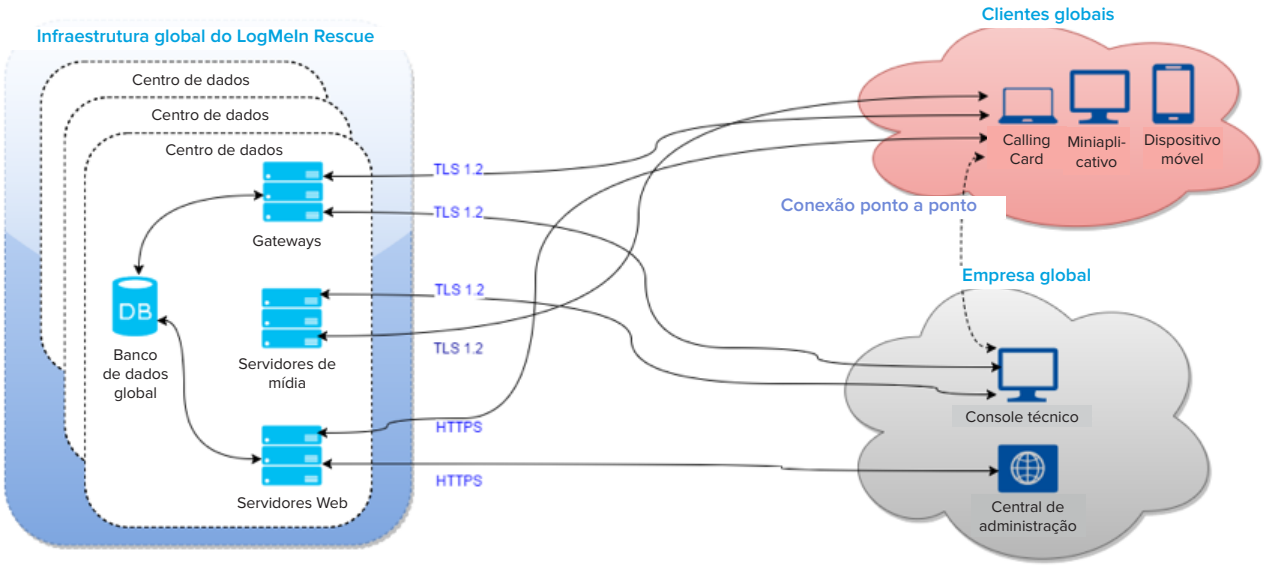
Capacidade de dimensionamento, segurança, confiabilidade e facilidade de uso. Essas quatro características descrevem uma ótima solução de suporte remoto, mas nem sempre andam juntas. É comum encontrar uma solução de suporte remoto que ofereça dois ou três desses critérios, mas uma solução que dê conta de todos os quatro ao mesmo tempo é rara. A LogMeIn, Inc. oferece exatamente esse tipo de solução com o LogMeIn Rescue.

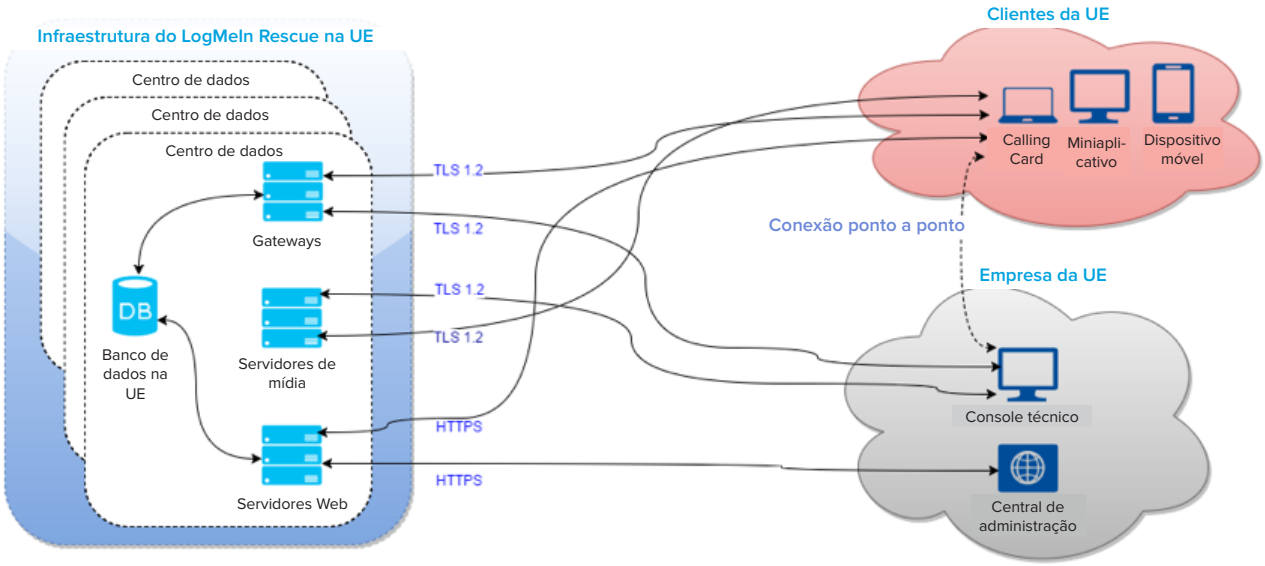
Capacidade de dimensionamento. Não importa se você tem um único técnico ou uma central de atendimento com dez mil funcionários, o Rescue vai dar conta do serviço.

Segurança. As sessões de suporte são protegidas com criptografia AES de 256 bits completa. As operações de suporte devem ser autorizadas pelo usuário final antes que o técnico possa executá-las. Os registros das sessões de suporte são armazenados em um banco de dados de maneira criptografada e podem ser consultados posteriormente. As sessões de controle remoto podem ser gravadas em um arquivo de vídeo.

Confiabilidade. O Rescue é hospedado em seis centros de dados altamente confiáveis com uma infraestrutura totalmente redundante.

Facilidade de uso. Seus técnicos estarão prontos para operar em questão de horas. Seus usuários finais receberão suporte com apenas alguns cliques. Nenhuma das partes precisa instalar qualquer tipo software.





CONFIDENCIALIDADE DOS DADOS

Em geral, a segurança é associada à confidencialidade dos dados, a confidencialidade dos dados é associada à criptografia e a criptografia é caracterizada pela codificação simétrica usada e seu comprimento de chave. Essas concepções errôneas levam a designações erradas, como "segurança garantida por AES de 256 bits". Obviamente, isso está equivocado.

Um sistema online seguro deve sempre cumprir os seguintes objetivos:

- Autenticação das partes que se comunicam;
- Negociação das chaves de criptografia sem possibilidade de interceptação man-in-the-middle;
- Troca confidencial de mensagens;
- Capacidade de detectar se uma mensagem foi modificada em trânsito.

O SSL/TLS, abreviatura de Camada de soquete seguro (Secure Sockets Layer) e Segurança da camada de transporte (Transport Layer Security), foi projetado para oferecer suporte para as etapas listadas acima. Originalmente criado pela Netscape Communication Corporation na metade dos anos 1990, ele se tornou, na prática, o padrão para comunicações seguras pela Internet e foi endossado pela Visa, Mastercard e American Express.

A implementação de SSL utilizada pelo LogMeIn Rescue é a OpenSSL (http://www.openssl.org). A LogMeIn sempre utiliza a versão mais recente disponível. No momento da publicação, a versão utilizada pelo Rescue era a 1.0.2j.

ACORDO DE CHAVE

Quando uma sessão de suporte é iniciada e se estabelece uma conexão entre o usuário que está recebendo suporte e o técnico, seus computadores devem entrar em acordo quanto a um algoritmo de criptografia e uma chave correspondente, que serão utilizados durante a sessão. A importância dessa etapa costuma ser negligenciada, o que é, de certa forma, compreensível: parece se tratar de uma tarefa trivial, supostamente simples e direta.

Ela é, no entanto, tudo menos simples: para combater os, assim chamados, ataques de um espião intermediário (man-in-the-middle) (em que o computador C se posiciona entre os computadores A e B e se faz passar pela contraparte correspondente para A e B), novamente, devem ser empregados certificados. Uma vez que nem o técnico nem o usuário final têm um software de servidor ou um certificado SSL instalados em seus computadores, ambos se direcionam para um dos servidores LogMeIn Rescue e executam a fase inicial do acordo de chave com esse computador. A verificação do certificado, tanto por parte do console técnico como pelo miniaplicativo do usuário final, assegura que apenas um servidor Rescue possa mediar o processo.

TROCA DE MENSAGENS

O TLS possibilita o uso de uma grande variedade de pacotes de codificação. Assim, as partes envolvidas na comunicação podem entrar em acordo quanto a um esquema de criptografia compatível com ambas. Esse procedimento tem dois propósitos principais: primeiro, o protocolo pode ser estendido com novos pacotes de codificação sem romper compatibilidades anteriores e, segundo, novas implementações podem reduzir a necessidade de suporte para pacotes que, notoriamente, apresentam deficiências na criptografia.

Uma vez que os três componentes do sistema de comunicação do LogMeIn Rescue estão sob o controle da LogMeIn, o pacote de codificação utilizado por esses componentes é sempre o mesmo: AES256-SHA no modo de encadeamento de blocos de codificação com acordo de chave RSA. Isso significa o seguinte:

- As chaves de criptografia são intercambiadas usando pares de chaves RSA privadas/públicas, como descrito na seção anterior.
- O AES, abreviatura de Padrão de Criptografia Avançada (Advanced Encryption Standard), é utilizado como o algoritmo de criptografia e descriptografia;
- A chave de criptografia tem comprimento de 256 bits;
- O SHA-2 é utilizado como a base dos Códigos de autenticação de mensagem (MACs, Message Authentication Codes). Um MAC é um fragmento pequeno de informação utilizado para autenticar uma mensagem. O valor do MAC protege a integridade e a autenticidade da mensagem, pois permite que as partes envolvidas na comunicação possam detectar qualquer alteração feita na mensagem;

- O modo de Encadeamento de blocos de criptografia (CBC, Cipher-block chaining) assegura que cada bloco de texto codificado dependa dos blocos de texto não criptografados acumulados até aquele ponto, e que mensagens similares não possam ser identificadas como tal na rede.

O processo descrito acima garante que os dados sendo transmitidos entre o usuário final que está recebendo suporte e o técnico sejam totalmente criptografados, e que apenas as respectivas partes tenham acesso às informações contidas na transmissão de mensagens.

AUTENTICAÇÃO E AUTORIZAÇÃO

A autenticação e a autorização no LogMeIn Rescue servem a dois propósitos distintos.

A autenticação assegura que o técnico ou administrador fazendo login no sistema do Rescue seja, de fato, quem ele afirma ser. No Rescue, a autenticação é tratada de uma maneira bem direta: os técnicos recebem IDs de login (que geralmente coincidem com seus endereços de e-mail) e senhas correspondentes de seus administradores. Essas credenciais são inseridas no formulário de login no site do LogMeIn Rescue no início do dia de trabalho de um técnico.

No LogMeIn Rescue, o sistema Rescue é primeiro autenticado para o técnico (ou melhor, o navegador de Internet do técnico) com o certificado SSL RSA premium de 2048 bits. Isso garante que o técnico insira seu nome de usuário e senha no site correto. Em seguida, o técnico faz o login no sistema com suas credenciais.

O LogMeIn Rescue não armazena senhas. Em vez disso, ele usa scrypt para criar hashes de senhas que estão armazenadas no banco de dados do Rescue. Os hashes recebem um sal com uma cadeia de 24 caracteres gerada por CSPRNG para cada senha única.

O LogMeIn Rescue também garante aos administradores algumas opções de política de senha:

- Os administradores podem exigir um grau mínimo de segurança de senha e um prazo de validade máximo. Um medidor integrado mostra aos administradores e técnicos o grau de segurança da senha escolhida;
- É possível exigir que os técnicos alterem sua senha do Rescue no login seguinte.
- Os administradores principais podem exigir que os membros da sua organização usem a verificação em duas etapas para fazer login no Rescue.

O LogMeIn Rescue também permite aos administradores implementar uma política de Logon único. Emprega-se a Linguagem de marcação de declaração de segurança (SAML, Security Assertion Markup Language), que é um padrão XML para a troca de dados de autenticação e autorização entre domínios de segurança (entre um provedor de identidade e um provedor de serviço). Os técnicos têm, então, acesso apenas a aplicativos predefinidos e um único ID de logon único para fazer login nesses aplicativos. O ID de logon único de um técnico pode ser desabilitado com facilidade.

O recurso de verificação em duas etapas usa o LastPass Authenticator para oferecer uma segunda camada de proteção para uma conta Rescue exigindo que membros selecionados da organização configurem uma maneira adicional de verificar sua identidade. A configuração do LastPass Authenticator é acionada em qualquer um dos seguintes casos:

- O membro selecionado tenta efetuar login na sua conta do Rescue em um site seguro;
- O membro selecionado tenta efetuar login no Console técnico para desktop;
- O membro selecionado tenta alterar sua senha do Rescue.

Whitepaper técnico do LastPass: https://enterprise.lastpass.com/wp-content/uploads/LastPass-Technical-Whitepaper-3.pdf

A autorização, por outro lado, ocorre com bastante frequência: ao menos uma vez durante cada sessão de suporte remoto. O usuário final que está recebendo suporte, após baixar e executar o miniaplicativo de suporte, será contatado pelo técnico. O técnico pode conversar com o usuário final pelo bate-papo do miniaplicativo, mas qualquer ação além dessa, como enviar um arquivo ou visualizar a área de trabalho do usuário final, exige a permissão expressa por parte do usuário. Uma “solicitação única” também pode ser implementada. Ela é destinada a trabalhos de suporte remoto mais demorados, em que o cliente pode não es-

tar presente durante toda a sessão. Se esse sinalizador for habilitado para um grupo de técnicos, os técnicos desse grupo poderão solicitar uma permissão "global" ao cliente. Se esta for concedida, eles poderão executar ações como visualizar informações do sistema ou ingressar em uma sessão de controle remoto sem precisar de autorizações subsequentes do usuário final.

Os administradores também podem impor restrições de endereço IP aos técnicos. Quando selecionados, os endereços IP disponíveis podem ser restringidos a uma lista bem limitada. Os técnicos designados para uma tarefa específica só podem, então, acessar o Rescue a partir de endereços de IP pré-aprovados para aquela tarefa.

O administrador de um grupo de técnicos também pode desabilitar determinados recursos na Central de administração. Por exemplo, os membros de um grupo de técnicos podem ser impedidos de receber arquivos de usuários finais. A seguir, você encontra algumas permissões que um administrador pode conceder ou negar:

- Iniciar o controle remoto;
- Reinicializar;
- Iniciar a visualização da área de trabalho;
- Gravar sessões;
- Enviar e receber arquivos;
- Iniciar sessões privadas;
- Iniciar o gerenciador de arquivos;
- Solicitar credenciais do Windows;
- Enviar URLs;
- Permitir a sincronização da área de transferência;
- Exibir informações do sistema;
- Implantar scripts;
- Usar uma solicitação única para todas as permissões;
- Transferir sessões;
- Permitir compartilhamento de tela com clientes.

O sistema Rescue também é autenticado para o usuário final que está recebendo suporte. O miniaplicativo, baixado e executado pelo usuário, é assinado com o certificado de assinatura de código da LogMeIn (baseado em uma chave RSA de 2048 bits). Essa informação costuma ser exibida ao usuário em seu navegador de Internet quando ele está prestes a executar o software.

O usuário que está recebendo suporte não é autenticado. Cabe ao técnico determinar quem é o usuário, seja por bate-papo, seja por conversa telefônica. O sistema Rescue oferece mecanismos semelhantes à autenticação, como códigos PIN exclusivos, mas estes são utilizados para direcionar a sessão de suporte para a fila correta, privada ou compartilhada, não devendo ser compreendidos como um sistema de autenticação.

AUDITORIA E REGISTRO

Qualquer solução de suporte remoto deve colocar muita ênfase na responsabilidade pela prestação de contas. O LogMeIn Rescue oferece dois recursos de auditoria distintos.

Primeiro, o chamado "registro do bate-papo" é salvo no banco de dados do Rescue. O registro do bate-papo é transmitido aos servidores do Rescue pelo console técnico em tempo real. Ele contém eventos e mensagens do bate-papo relativos a uma determinada sessão de suporte. Por exemplo, um arquivo de registro pode exibir um evento em que uma sessão de controle remoto é iniciada ou encerrada, ou quando um arquivo é enviado pelo técnico para o usuário final. Os metadados que acompanham as ações, como o nome e a impressão digital de Hash MD5 de um arquivo transmitido, também são incluídos no registro quando aplicável. O banco de dados do registro do bate-papo pode ser consultado a partir da Central de administração. No momento da publicação, as políticas de retenção de dados da LogMeIn estabelecem que o conteúdo dos registros estará disponível online por dois anos após o fim de uma sessão de suporte remoto e será arquivado por mais dois anos depois disso. Para facilitar a integração com sistemas CRM, o LogMeIn Rescue pode publicar detalhes de uma sessão em um URL. Os administradores podem optar por permitir que o texto do bate-papo seja excluído desses detalhes. Além disso, todos os registros de textos de bate-papo entre técnicos e clientes podem ser automaticamente omitidos dos detalhes da sessão armazenados no centro de dados do Rescue.

O LogMeIn Rescue também permite que os técnicos gravem os eventos transcorridos durante uma visualização da área de trabalho ou uma sessão de controle remoto em um arquivo de vídeo. Esse é um recurso muito importante para questões ligadas à prestação de contas e responsabilidade. Os arquivos de gravação são armazenados em um

diretório especificado pelo técnico. No caso de uma grande organização de suporte, o local deve ser um servidor de rede. O espaço em disco ocupado por essas gravações varia bastante e depende inteiramente dos conteúdos e da capacidade de compactação do computador do usuário final que está recebendo suporte. Com base em uma análise de milhões de sessões de controle remoto utilizando a tecnologia da LogMeIn, o requisito médio de espaço em disco para um minuto de dados de controle remoto fica entre 372 e 1.024 Kbytes. As gravações são armazenadas diretamente em AVI ou em um formato proprietário intermediário da LogMeIn, que pode ser convertido para arquivos padrão AVI pelo aplicativo "Rescue AVI Converter", que pode ser baixado do site help.logmein.com. O formato proprietário da LogMeIn, chamado RCREC, pode reduzir o tamanho da gravação em cerca de 10%.

ARQUITETURA DO CENTRO DE DADOS

O LogMeIn Rescue é hospedado em centros de dados seguros e modernos que contam com os seguintes recursos:

- Procedimentos multicamadas de controle de segurança, sistemas biométricos de entrada, vigilância por circuito fechado de vídeo em tempo integral e monitoramento com alarme;
- Energia redundante ininterrupta CA e CC, geradores de energia de backup no local;
- Design AVAC redundante com distribuição de ar sob pavimento elevado para maior controle de temperatura;
- Sistema de detecção de fumaça por cima e por baixo do piso elevado, além de tubo seco de supressão de fogo com duplo bloqueio e pré-ação.

A infraestrutura do LogMeIn Rescue em si é altamente segura e confiável:

- Redundância no nível de componentes do servidor: fontes de energia e ventiladores redundantes, discos rígidos espelhados RAID-1;
- Redundância no nível do servidor: dependendo da função, clusters ativo/passivo ou ativo/ativo;
- Redundância no nível do centro de dados: Seis centros de dados [Costas oeste e leste dos EUA, centro dos EUA, centro-sul dos EUA, Londres (Reino Unido) e Frankfurt (Alemanha)] com recursos de fail-over quase instantâneos;
- Firewalls redundantes duplos, com apenas as portas 80 e 443 abertas;
- Clusters de banco de dados ativo/passivo;
- Balanceadores de carga redundantes, incluindo SSL;
- Clusters de servidor de aplicativo e web redundantes e com balanceamento de carga;
- Clusters de servidor de gateway redundantes e com balanceamento de carga.

VISÃO GERAL DO PROCESSO DE TRANSFERÊNCIA PARA O GATEWAY DO RESCUE

Quando o miniaplicativo com assinatura digital do Rescue é iniciado em uma máquina:

- Ele contém um Identificador global exclusivo (GUID, Globally Unique Identifier) de autenticação de sessão, que foi inserido no arquivo .exe como um recurso pelo site ao ser baixado;
- Ele, então, baixa uma lista de gateways disponíveis a partir de secure.logmeinrescue.com;
- O miniaplicativo elege um gateway da lista e se conecta a ele usando TLS; o gateway é autenticado pelo miniaplicativo usando seu certificado SSL;
- O gateway autentica o miniaplicativo no banco de dados com o GUID e registra que o usuário está esperando um técnico.

Quando uma sessão é capturada no console técnico do Rescue:

- Uma solicitação é enviada ao gateway com o GUID de autenticação da sessão para que transmita as conexões entre o console técnico e o miniaplicativo do cliente;
- O gateway autentica a conexão e inicia a transmissão de dados no nível de transporte (ele não descriptografa os dados transmitidos).

Quando uma transmissão de conexão é iniciada, as partes tentam estabelecer uma conexão ponto a ponto (P2P):

- O miniaplicativo começa a aguardar uma conexão TCP em uma porta designada pelo Windows;
- Se a conexão TCP não puder ser estabelecida dentro de um limite de tempo (10 segundos), é feita uma tentativa de estabelecer uma conexão UDP com a ajuda do gateway;
- Se não for possível estabelecer uma conexão TCP ou UDP, as partes autenticam o canal P2P (usando o GUID de autenticação da sessão), que assume o tráfego da conexão transmitida;
- Se uma conexão UDP tiver sido configurada, o TCP é simulado sobre os datagramas de UDP usando XTCP, um protocolo proprietário da LogMeIn baseado na pilha TCP da BSD.

Todas as conexões são protegidas pelo protocolo TLS (usando criptografia AES256 com MAC SHA256). O GUID de autenticação da sessão é um valor inteiro de 128 bits randomizado por criptografia.

BANCO DE DADOS

- Todos os dados contendo informações confidenciais estão protegidos com criptografia AES de 256 bits (registro de bate-papo e campos personalizados);
- Um backup do banco de dados do Rescue é feito a cada 24 horas. O backup do banco de dados é armazenado no centro de dados com a mesma criptografia do original.
- A opção de residência de dados do Rescue permite que você escolha onde armazenar os dados do usuário final: na União Europeia (Frankfurt ou Londres) ou nos EUA. A LogMeIn garante que as pessoas que escolhem a residência de dados na UE somente se conectarão a centros de dados dentro da UE, e que os dados do cliente permanecerão apenas na região escolhida. Não há conexão entre nossos centros de dados baseados na UE e nos EUA.

ARQUITETURA DO SERVIÇO DE MÍDIA DO RESCUE

O serviço de mídia do Rescue é um serviço baseado em WebRTC independente que permite a transmissão de vídeo no Rescue Lens. Ele gerencia as chamadas "conferências" das sessões do Rescue que usam o recurso do Lens. Os participantes da conferência (pares) entram e saem das conferências, e os clientes enviam transmissões de vídeo e áudio para que os outros participantes os recebam. O Lens envia conteúdo de vídeo em uma transmissão unidirecional do aplicativo do Lens para o console técnico.

Existem três principais componentes do serviço de mídia: o MediaSDK, o gerenciador de sessões e o servidor de transmissões. Esses componentes gerenciam o processo de criar/excluir e de entrar/sair de conferências. Esses componentes comunicam-se por meio das conexões seguras existentes entre o console técnico e o site e entre o aplicativo do Lens e o site.

MediaSDK

O serviço de mídia foi desenvolvido sobre um WebRTC com um wrapper fino em torno da base do código do WebRTC. Esse MediaSDK é usado no console técnico e nos aplicativos móveis do Lens.

Gerenciadores de sessão

O gerenciador de sessões é um site com balanceamento de carga simples que fornece uma API REST para gerenciar conferências (criar/excluir e entrar/sair). O gerenciador de sessões aceita apenas solicitações do site do Rescue.

Servidores de transmissão

O serviço de mídia está usando a solução de servidor de código aberto Jitsi para lidar com os fluxos entre os pares (o console técnico e o aplicativo Lens). Tanto o console técnico quanto o aplicativo Lens estão conectados ao servidor de transmissão. O aplicativo Lens transmite seu conteúdo de vídeo para o servidor de transmissão. O console técnico

transmite o conteúdo de vídeo que vem do servidor. O Jitsi funciona como um servidor de transmissão entre os pares. A sessão do Lens tem dois fluxos (o que é enviado e o que é recebido).

PADRÕES DA INDÚSTRIA DO LOGMEIN RESCUE

SOC 2

O LogMeIn Rescue é atestado para Controle de Organização de Serviço 2 (SOC 2), o que garante que os clientes estão usando os controles adequados para proteger seus dados importantes.

SOC 2 é um procedimento de auditoria extenso, baseado em vários princípios e critérios, testando os sistemas de controle usados para processar dados e a confidencialidade das informações processadas por esses sistemas. Uma revisão anual deve ser concluída para manter a conformidade com o SOC 2. Como "padrão de excelência" para empresas de software, amplamente reconhecido em vários países por diversos setores, a conclusão e manutenção do atestado SOC 2 é apenas mais uma forma de demonstrar nosso compromisso com a segurança e a privacidade.

RGPD

O Regulamento Geral de Proteção de Dados (RGPD) é uma legislação da União Europeia (UE) sobre a proteção de dados e a privacidade das pessoas físicas dentro da União Europeia. O objetivo do RGPD é principalmente dar controle aos seus cidadãos e residentes sobre seus próprios dados pessoais e simplificar o ambiente regulador na UE. O LogMeIn Rescue fornece aos seus usuários controle sobre os dados que armazenamos em seu nome (Conteúdo - conforme definido nos Termos de Serviço) para ajudá-los a manter o foco em seu negócio principal enquanto se preparam com eficiência para o RGPD.

- Os usuários do Rescue podem exportar seus dados usando o recurso de relatórios da Central de Administração ou os APIs do Rescue.
- Os usuários do Rescue podem excluir seus dados armazenados pelos servidores do LogMeIn Rescue.
  - Excluir todos os dados ligados a um técnico de suporte.
  - Excluir todos os dados conectados a uma sessão de suporte, incluindo dados pessoais relacionados e vinculados aos seus clientes.

Com esses recursos, o LogMeIn Rescue permite que seus usuários atendam aos padrões e requisitos do RGPD.

Para obter informações detalhadas sobre o RGPD, visite o site de RGPD do LogMeIn.

HIPAA

Apesar de a LogMeIn não poder controlar o conteúdo compartilhado por usuários durante uma sessão de suporte, o serviço LogMeIn Rescue é projetado para atender a normas de segurança rigorosas e ajudar as entidades reguladas pela Lei de responsabilidade e portabilidade de seguros de saúde dos Estados Unidos (HIPAA, Health Insurance Portability and Accountability Act) a atender às diretrizes regulatórias estabelecidas pela HIPAA.

Controles de acesso

- Possibilidade de definir o acesso baseado em permissão em um nível granular (como permitir a alguns técnicos apenas a visualização remota, mas não o controle remoto);
- Nenhum dado dos dispositivos remotos é armazenado nos servidores do centro de dados da LogMeIn (conforme indicado anteriormente, apenas os dados da sessão e do bate-papo são armazenados). Além disso, os registros de textos de bate-papo podem ser removidos dos detalhes da sessão;

- As permissões podem ser configuradas de maneira que os técnicos não possuam o direito de transferir arquivos, eliminando a possibilidade de retirarem arquivos dos dispositivos remotos;
- O usuário final deve estar presente no dispositivo remoto e permitir o acesso remoto;
- O usuário final mantém o controle e pode encerrar a sessão a qualquer momento;
- Os técnicos podem ser impedidos de usar certos recursos até que o usuário final conceda explicitamente a permissão (exemplos: controle remoto, visualização da área de trabalho, transferência de arquivos, informações do sistema, reinicialização e reconexão);
- Os direitos de acesso são automaticamente revogados quando a sessão é encerrada;
- O tempo predeterminado de inatividade força automaticamente o logoff;
- Hospedado em centros de dados redundantes que contam com acesso restrito e seguro.

Controles de auditoria

- Opção de gravação forçada da sessão, com capacidade para armazenar arquivos de auditoria em uma rede compartilhada segura;
- A atividade das sessões dos técnicos e das sessões remotas é registrada no computador host para garantir a segurança e manter o controle de qualidade (logins feitos com sucesso, logins malsucedidos, controle remoto iniciado, controle remoto encerrado, reinicialização efetuada, logout);
- Autenticação de pessoa ou entidade;
- A identidade do técnico é definida por um endereço de e-mail único ou por meio de um ID de logon único; além disso, o técnico deve ser autenticado;
- Um número excessivo de tentativas de login malsucedidas ocasiona o bloqueio da conta;
- Os técnicos podem receber permissão para fazer login a partir de endereços IP aprovados.

Segurança de transmissão

- Criptografia AES completa de 256 bits para todos os dados;
- Hash MD5 para garantir rastreabilidade aprimorada das transferências de arquivos.

CONCLUSÃO

Optar por uma solução de suporte remoto costuma ser uma decisão baseada em recursos e preços. Se você está lendo este documento, é provável que o LogMeIn Rescue tenha atendido às suas necessidades nessas categorias. Com as informações disponibilizadas acima, acreditamos que foi possível provar que a arquitetura por trás do Rescue oferece os níveis adequados de dimensionamento, segurança, confiabilidade e facilidade de uso.