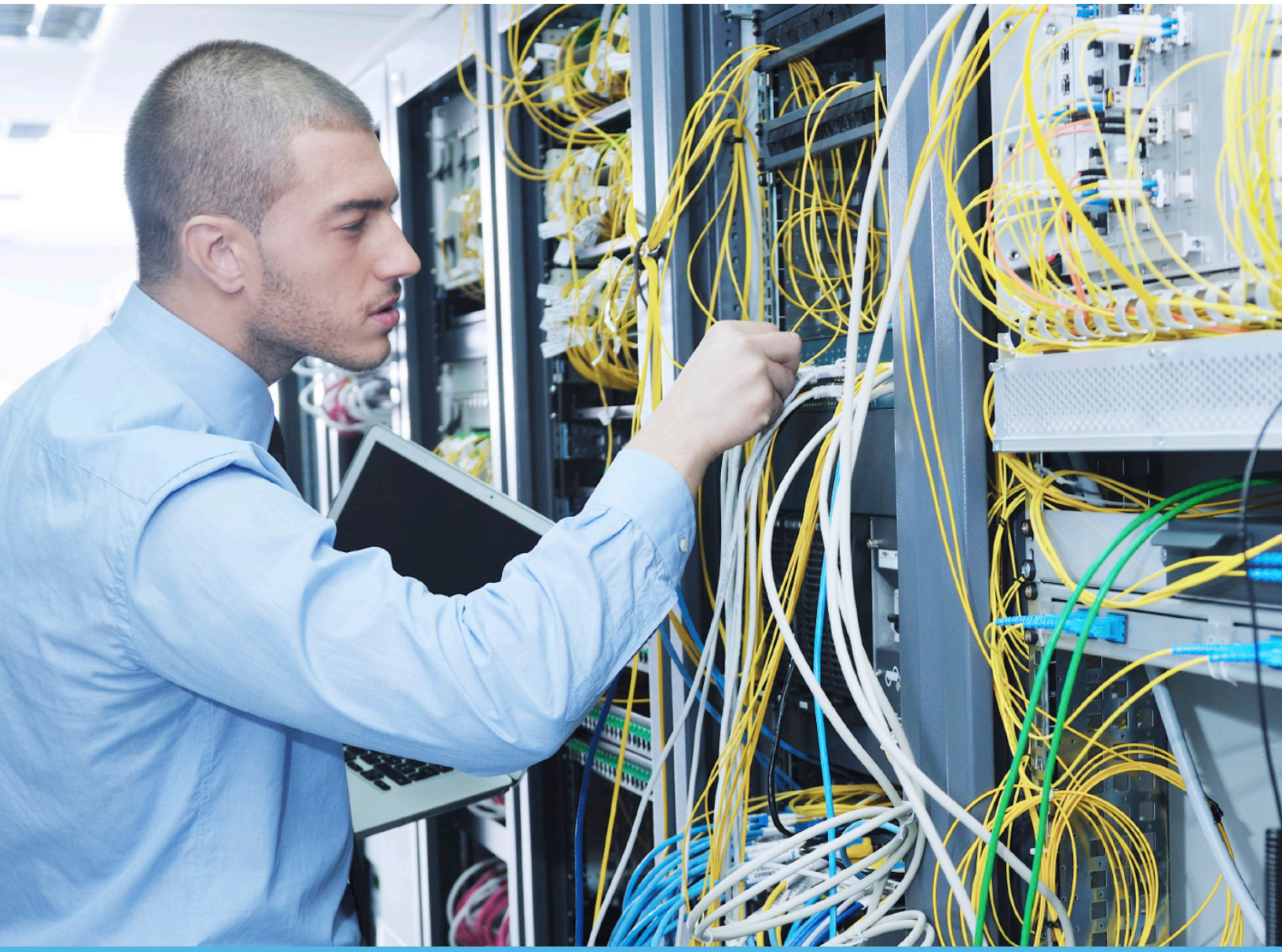
Rescue by LogMeIn

L'ARCHITETTURA E LA SICUREZZA DI RESCUE

Brochure informativa



Indice

INTRODUZIONE

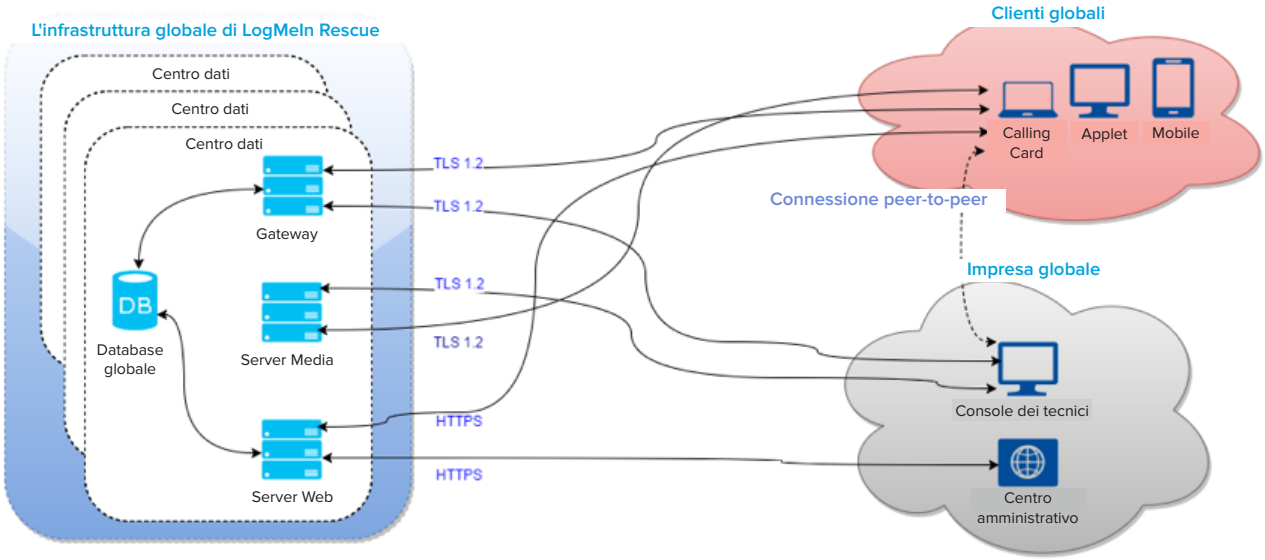
Scalabilità, sicurezza, affidabilità e facilità d'uso. Queste quattro caratteristiche descrivono al meglio una soluzione di supporto remoto ottimale, ma non sempre si trovano combinate in un'unica soluzione. È facile trovare una soluzione di supporto remoto che offra due o forse tre di queste caratteristiche, ma una soluzione che le offra tutte e quattro è rara. LogMeIn, Inc., invece, offre proprio questo tipo di soluzione completa con LogMeIn Rescue.

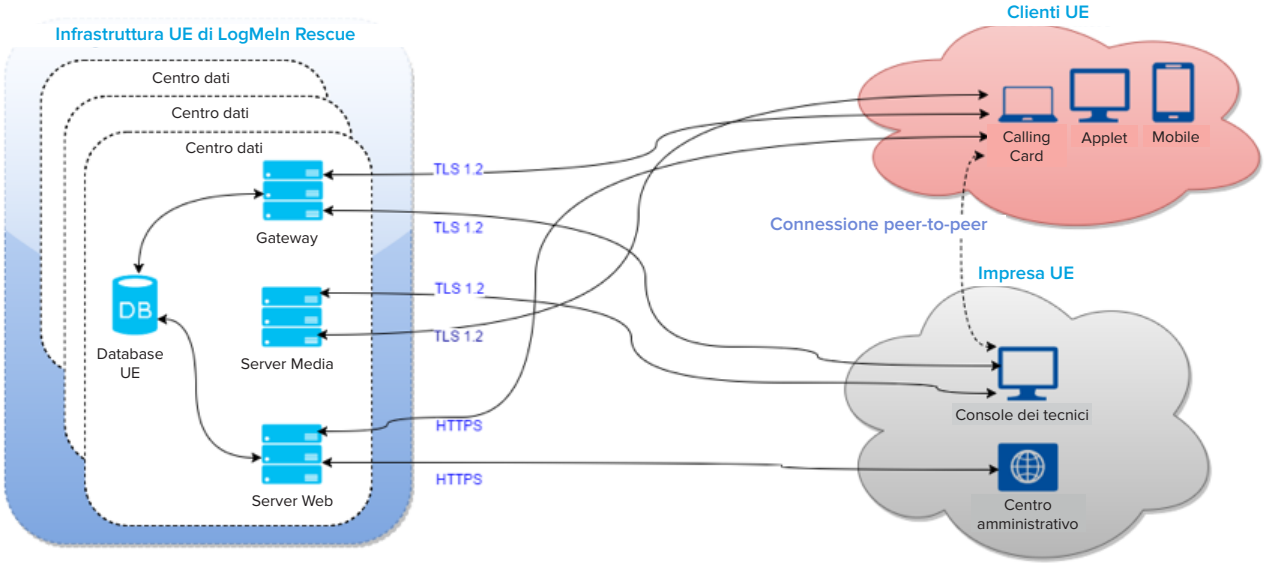
Scalabilità. Rescue è la soluzione perfetta sia per un solo tecnico che per i call center con migliaia di dipendenti.

Sicurezza. Le sessioni di supporto sono protette da crittografia AES end-to-end a 256 bit. Le operazioni di supporto devono essere autorizzate dall'utente finale prima che il tecnico le possa eseguire. I registri delle sessioni di supporto vengono memorizzati in un database in formato crittografato e possono essere sottoposti a query in un secondo momento. È possibile inoltre registrare le sessioni di supporto remoto in un file video.

Affidabilità. Rescue è ospitato su sei centri dati carrier-grade dotati di un'infrastruttura completamente ridondante.

Facilità d'uso. I tecnici possono iniziare a usare Rescue nel giro di poche ore, gli utenti finali ricevono il supporto di cui hanno bisogno in pochi clic e tutto questo senza che nessuno debba installare alcun software.





RISERVATEZZA DEI DATI

Spesso per sicurezza si intende riservatezza dei dati, per riservatezza dei dati si intente crittografia e la crittografia è caratterizzata dall'algoritmo simmetrico utilizzato e dalla lunghezza della sua chiave. Queste convinzioni errate hanno portato a espressioni improprie quali "protetto con AES a 256 bit". È superfluo sottolineare quanto questo sia fuorviante.

Un sistema online sicuro dovrebbe sempre soddisfare i seguenti requisiti:

- autenticazione delle parti comunicanti;
- negoziazione delle chiavi di crittografia senza che queste vengano intercettate da terzi (attacchi man-in-the-middle);
- scambio riservato di messaggi;
- capacità di rilevare eventuali modifiche dei messaggi in transito.

SSL/TLS, ovvero Secure Sockets Layer/Transport Layer Security, è un protocollo sviluppato proprio per supportare queste caratteristiche. Originariamente creato da Netscape Communication Corporation intorno alla metà degli anni '90, si è in seguito affermato come standard de facto per la protezione delle comunicazioni su Internet ed è stato approvato da Visa, MasterCard e American Express.

L'implementazione SSL utilizzata da LogMeIn Rescue è OpenSSL (https://www.openssl.org). LogMeIn utilizza sempre la versione più recente disponibile. Al momento della pubblicazione, la versione utilizzata da Rescue è la 1.0.2j.

CHIAVE CONCORDATA

Quando ha inizio una sessione di supporto e viene stabilita la connessione tra l'utente e il tecnico, i rispettivi computer devono concordare un algoritmo di crittografia e la chiave corrispondente da utilizzare per la durata della sessione. L'importanza di questo passaggio è spesso sottovalutata e ciò, in una certa misura, è comprensibile, in quanto può sembrare un'attività ordinaria che dovrebbe essere semplice e priva di complicazioni.

Invece, è tutt'altro che semplice: è infatti necessario l'impiego di certificati per contrastare i cosiddetti attacchi MITM, nei quali il computer C si posiziona fra il computer A e il computer B fingendo di essere l'altra parte sia con A che con B. Dal momento che il software del server e il certificato SSL non sono installati né nel computer del tecnico né in quello dell'utente finale, entrambi si rivolgono a uno dei server di LogMeIn Rescue per eseguire la fase iniziale in cui viene concordata la chiave da utilizzare durante la sessione corrente. La verifica del certificato sia da parte della Console dei tecnici che dell'applet dell'utente finale assicura che il processo possa essere mediato soltanto da un server Rescue.

SCAMBIO DEI MESSAGGI

Il protocollo TLS consente l'utilizzo di una vasta gamma di pacchetti di crittografia, permettendo alle parti comunicanti di concordare uno schema di crittografia supportato da entrambe. Ciò ha due scopi principali: il primo è che il protocollo può essere ampliato con nuovi pacchetti di crittografia senza compromettere la compatibilità con le versioni precedenti, e il secondo è che implementazioni più nuove possono eliminare il supporto per pacchetti di cui sia nota la debolezza crittografica.

Poiché tutti e tre i componenti del sistema di comunicazione di LogMeIn Rescue sono sotto il controllo di LogMeIn, il pacchetto di crittografia utilizzato da tali componenti è sempre lo stesso: AES256-SHA in modalità Cipher Block Chaining con chiave concordata RSA. Ciò significa quanto segue:

- le chiavi di crittografia vengono scambiate utilizzando coppie di chiavi RSA private e pubbliche, come descritto nella sezione precedente;
- l'algoritmo di crittografia e decrittografia utilizzato è lo standard AES (Advanced Encryption Standard);
- la lunghezza della chiave di crittografia è di 256 bit;
- come base dei codici di autenticazione dei messaggi (MAC) è utilizzata la funzione SHA-2. Il valore MAC è una breve unità di dati utilizzata per l'autenticazione di un messaggio. Il valore MAC protegge sia l'integrità del messaggio che la sua autenticità, consentendo alle parti comunicanti di rilevare eventuali modifiche al messaggio;
- la modalità CBC (Cipher Block Chaining) assicura che ciascun blocco di testo crittografato dipenda dai blocchi di testo normale fino a quel punto e che messaggi simili non possano essere distinti sulla rete.

Questo assicura che i dati trasmessi tra l'utente finale a cui viene fornito supporto e il tecnico siano crittografati end-to-end e che solo le parti comunicanti abbiano accesso alle informazioni contenute nel flusso di messaggi.

AUTENTICAZIONE E AUTORIZZAZIONE

L'autenticazione e l'autorizzazione in LogMeIn Rescue hanno due scopi distinti.

L'autenticazione serve a garantire che il tecnico o l'amministratore che accede al sistema Rescue sia di fatto chi afferma di essere. Su Rescue, l'autenticazione viene gestita in modo molto semplice: gli amministratori assegnano ai tecnici degli ID di accesso (generalmente corrispondenti ai loro indirizzi e-mail) e le password corrispondenti. All'inizio della giornata di lavoro, il tecnico deve inserire tali credenziali nel modulo di accesso che si trova sul sito Web di LogMeIn Rescue.

Su LogMeIn Rescue, il sistema Rescue viene prima autenticato al tecnico, o meglio sul suo browser Web, mediante il suo avanzato certificato SSL con chiave RSA a 2048 bit. Ciò assicura che il tecnico inserisca nome utente e password sul sito Web corretto. Il tecnico accede quindi al sistema con le proprie credenziali.

LogMeIn Rescue non memorizza le password, bensì usa scrypt per creare hash dalle password e memorizzarli nel database di Rescue. Effettuiamo un processo di hashing usando una stringa di 24 caratteri generata da CSPRNG per ciascuna password univoca.

LogMeIn Rescue offre agli amministratori una scelta di criteri per le password:

- gli amministratori possono imporre un livello minimo di complessità delle password (un indicatore incorporato mostra il livello della scelta effettuata) e una durata massima della loro validità;
- i tecnici possono essere costretti a cambiare la password di Rescue all'accesso successivo;
- gli amministratori principali possono imporre ai membri della propria azienda di utilizzare la verifica in due passaggi per l'accesso a Rescue.

LogMeIn Rescue consente inoltre agli amministratori di implementare un metodo Single-Sign-On (SSO). Viene utilizzato il Security Assertion Markup Language (SAML), che è uno standard XML per lo scambio di dati di autenticazione e autorizzazione tra domini di sicurezza, ovvero tra un fornitore di identità e un fornitore di servizi. I tecnici hanno così accesso soltanto ad applicazioni predefinite e dispongono di un solo ID SSO per accedervi. In questo modo, l'ID SSO di un tecnico può essere disabilitato in un clic.

La verifica in due passaggi è una funzione che ricorre a LastPass Authenticator per aggiungere un secondo livello di protezione agli account Rescue, richiedendo a membri selezionati dell'azienda di impostare un metodo aggiuntivo per verificare la propria identità. La configurazione dell'app di autenticazione è richiesta nei seguenti casi:

- quando un membro selezionato tenta di accedere al proprio account Rescue dal sito Web sicuro;
- quando un membro selezionato tenta di accedere alla Console dei tecnici per computer;
- quando un membro selezionato tenta di cambiare la proprio password Rescue.

Il white paper tecnico di LastPass è disponibile all'indirizzo https://enterprise.lastpass.com/wp-content/uploads/LastPass-Technical-Whitepaper-3.pdf

L'autorizzazione invece avviene molto spesso, almeno una volta nel corso di ciascuna sessione di supporto remoto. L'utente finale supportato, dopo aver scaricato ed eseguito l'applet per il supporto, verrà contattato da un tecnico. Il tecnico può chattare con l'utente finale tramite l'applet, ma qualsiasi altra sua azione, come l'invio di un file o la visualizzazione del desktop dell'utente, richiede l'esplicita autorizzazione dell'utente stesso. È possibile anche implementare una "richiesta singola". Questa è intesa per interventi di supporto prolungati, nei quali il cliente potrebbe non essere presente per l'intera durata della sessione. Abilitando questa opzione per un gruppo di tecnici, i tecnici di tale gruppo possono richiedere al cliente un'autorizzazione "globale", che, se concessa, consentirà loro di eseguire azioni quali la visualizzazione delle informazioni di sistema o l'accesso a una sessione di controllo remoto senza ulteriori autorizzazioni da parte dell'utente finale.

Gli amministratori possono inoltre imporre ai tecnici delle limitazioni relative agli indirizzi IP. Con questa funzione è possibile limitare gli indirizzi IP disponibili a un elenco molto ristretto. I tecnici assegnati a una particolare attività, potranno eseguirla quindi accedendo a Rescue solamente da un elenco di indirizzi IP approvati in precedenza.

L'amministratore di un gruppo di tecnici può anche disattivare determinate funzioni nel Centro amministrativo. È possibile, ad esempio, impedire ai membri di un gruppo di tecnici di ricevere file dagli utenti finali. Le seguenti sono alcune delle autorizzazioni che un amministratore può concedere o negare:

- avvio del controllo remoto;
- riavvio;
- avvio della visualizzazione desktop;
- registrazione delle sessioni;
- invio e ricezione di file;
- avvio di sessioni private;
- avvio di Gestione file;
- richiesta delle credenziali Windows;
- invio di URL;
- sincronizzazione degli Appunti;
- visualizzazione delle informazioni di sistema;
- distribuzione di script;
- uso di una richiesta singola per tutte le autorizzazioni;
- trasferimento delle sessioni;
- condivisione dello schermo con i clienti.

Il sistema Rescue viene autenticato anche all'utente finale al quale viene fornito supporto. L'applet, scaricata ed eseguita dall'utente, è firmata con il certificato di firma del codice di LogMeIn (basato su una chiave RSA a 2048 bit), e questa informazione viene generalmente visualizzata all'utente nel browser Web quando l'utente sta per eseguire il software.

L'utente a cui viene fornito supporto non è autenticato. È compito del tecnico verificare l'identità dell'utente, tramite chat o telefonicamente. Il sistema Rescue offre meccanismi analoghi all'autenticazione, quali i codici PIN univoci, ma questi servono per indirizzare la sessione di supporto alla coda privata o condivisa di competenza e non dovrebbero essere considerati un sistema di autenticazione.

AUDIT E REGISTRAZIONE DEGLI EVENTI

Qualsiasi soluzione di supporto remoto deve porre un forte accento sul concetto di responsabilizzazione, altrimenti noto come "accountability". LogMeIn Rescue offre due funzioni di audit distinte.

La prima è il "Registro di chat", che viene salvato nel database di Rescue. Il Registro di chat viene trasmesso dalla Console dei tecnici ai server Rescue in tempo reale e contiene sia gli eventi che i messaggi di chat di una data sessione di supporto. Un file di registro indica, ad esempio, l'ora di inizio e di fine di una sessione di controllo remoto, oppure l'ora in cui il tecnico ha inviato un file all'utente finale. Laddove applicabile, il registro può includere anche eventuali metadati associati, quali il nome e l'identificazione digitale dell'hash MD5 del file trasmesso. Il database dei Registri di chat può essere sottoposto a query dal Centro amministrativo. Al momento della pubblicazione del presente documento, i criteri di conservazione dei dati di LogMeIn prevedono che i contenuti dei registri vengano resi disponibili online per due anni dalla fine di una sessione di supporto remoto e successivamente archiviati per ulteriori due anni. Per agevolare l'integrazione con i sistemi CRM, LogMeIn Rescue può inviare i dettagli delle sessioni a un URL. Gli amministratori hanno la facoltà di scegliere se escludere o meno i testi delle chat da tali dettagli. I testi delle chat tra i tecnici e i clienti possono inoltre essere omessi automaticamente dai dettagli delle sessioni memorizzati nel Centro dati Rescue.

La seconda funzione di audit offerta da LogMeIn Rescue consente ai tecnici di registrare in un file video gli eventi che avvengono durante una visualizzazione del desktop o una sessione di controllo remoto. Questa funzione è molto importante ai fini dell'accountability e della responsabilità. I file di registrazione vengono memorizzati in una directory specificata dal tecnico. Nel caso di un'organizzazione di supporto di grandi dimensioni, tale directory dovrebbe trovarsi su un server di rete. Lo spazio su disco occupato da queste registrazioni varia in misura considerevole e dipende interamente dai contenuti e dalla comprimibilità del desktop dell'utente finale a cui viene fornito supporto. Tut-

tavia, secondo un'analisi svolta su milioni di sessioni di controllo remoto con la tecnologia LogMeIn, lo spazio su disco medio richiesto per un minuto di dati di controllo remoto è compreso tra 372 e 1024 Kbyte. Le registrazioni vengono memorizzate direttamente in formato AVI, oppure in un formato intermedio proprietario di LogMeIn, convertibile in file AVI standard mediante l'applicazione "Rescue AVI Converter", scaricabile da help.logmein.com. Il vantaggio dell'uso del formato proprietario di LogMeIn, chiamato RCREC, è che può ridurre le dimensioni delle registrazioni del 10% circa.

L'ARCHITETTURA DEI CENTRI DATI

LogMeIn Rescue è ospitato su centri dati sicuri e all'avanguardia dotati delle seguenti caratteristiche:

- procedure di controllo della sicurezza a più livelli, sistemi di accesso biometrici nonché monitoraggio degli allarmi e videosorveglianza a circuito chiuso costanti;
- gruppi di continuità CA e CC ridondanti, generatori elettrici di riserva sul posto;
- sistema HVAC con struttura ridondante e distribuzione dell'aria sotto il pavimento sopraelevato, per il massimo controllo della temperatura;
- sistema di rilevamento del fumo sopra e sotto il pavimento sopraelevato, impianto antincendio a secco a preazione con doppio interblocco.

L'infrastruttura stessa di LogMeIn Rescue è altamente sicura e affidabile:

- ridondanza a livello di componenti dei server: fonti di alimentazione e ventole ridondanti, dischi rigidi configurati in RAID 1 (volumi con mirroring);
- ridondanza a livello di server: cluster attivi/passivi o attivi/attivi, a seconda della funzione;
- ridondanza a livello di centri dati: sei centri dati (costa occidentale USA, area centrale USA, area centromeridionale USA, costa orientale USA, Londra nel Regno Unito e Francoforte in Germania) con funzionalità di failover quasi istantanee;
- doppi firewall ridondanti, con le sole porte 80 e 443 aperte;
- cluster di database attivi/passivi;
- bilanciamenti del carico ridondanti con protocollo SSL;
- cluster di server Web e server applicazioni ridondanti e con bilanciamento del carico;
- cluster di server gateway ridondanti e con bilanciamento del carico.

PANORAMICA SUL PROCESSO DI HANDOFF DEL GATEWAY DI RESCUE

All'avvio in un computer dell'applet firmata digitalmente di Rescue:

- l'applet contiene un GUID (Globally Unique Identifier) di autenticazione della sessione, che è stato incorporato nel file .exe come risorsa da parte del sito quando è stato scaricato;
- l'applet scarica quindi l'elenco dei gateway disponibili da secure.logmeinrescue.com;
- l'applet sceglie un gateway dall'elenco, vi si connette tramite TLS e il gateway viene autenticato dall'applet con il suo certificato SSL;
- il gateway autentica l'applet con il GUID e registra nel database il fatto che l'utente sia in attesa di un tecnico

Al prelievo di una sessione dalla Console dei tecnici di Rescue:

- al gateway con il GUID di autenticazione della sessione viene inviata la richiesta di inoltrare le connessioni tra la Console dei tecnici e l'applet del cliente;
- il gateway autentica la connessione e inizia a inoltrare i dati a livello di trasporto (non decrittografa i dati inoltrati).

All'inizio dell'inoltro di una connessione, le parti tentano di stabilire una connessione peer-to-peer (P2P):

- l'applet attende una connessione TCP su una porta assegnata da Windows;

- se non è possibile stabilire una connessione TCP entro un dato limite di tempo (10 secondi), viene tentata una connessione UDP con l'ausilio del gateway;
- se viene stabilita una connessione TCP o UDP, la parti autenticano il canale P2P (utilizzando il GUID di autenticazione della sessione) e il traffico proveniente dalla connessione inoltrata viene trasferito su tale canale;
- se è stata stabilita una connessione UDP, sui datagrammi UDP viene emulato il protocollo TCP utilizzando XTCP, un protocollo proprietario di LogMeIn basato sullo stack TCP di BSD.

Tutte le connessioni sono protette con il protocollo TLS (utilizzando la crittografia AES-256 con MAC SHA-256). Il GUID di autenticazione delle sessioni è un valore intero, crittograficamente casuale, a 128 bit.

DATABASE

- Tutti i dati che contengono informazioni riservate sono protetti con crittografia AES a 256 bit (registro di chat e campi personalizzati).
- Il backup del database di Rescue viene eseguito automaticamente ogni 24 ore e poi memorizzato nel centro dati con la stessa crittografia dell'originale.
- L'opzione per la residenza dei dati di Rescue consente di scegliere dove archiviare i dati dell'utente finale: nell'Unione Europea (Francoforte, Londra) o negli USA. LogMeIn garantisce che chi sceglie la residenza dei dati nell'Unione Europea si connetterà solamente ai centri dati nell'Unione Europea e che i dati dei clienti rimarranno esclusivamente nella regione da loro scelta. Non vi è alcuna connessione tra i centri dati nell'Unione Europea e i centri dati negli USA.

L'ARCHITETTURA DEL SERVIZIO MEDIA DI RESCUE

Il servizio Media di Rescue è un servizio indipendente basato su WebRTC che fornisce lo streaming video per Rescue Lens. Gestisce le cosiddette "conferenze" per le sessioni di Rescue che utilizzano la funzione Lens. Gli utenti (peer) partecipano alle conferenze e le abbandonano, e i client inviano gli streaming video e audio agli altri partecipanti. Lens invia contenuti video in streaming unidirezionale dall'applet Lens alla Console dei tecnici.

Il servizio Media ha tre componenti principali: MediaSDK, il Gestore sessioni e il server di streaming. Questi componenti gestiscono il processo per creare le conferenze o eliminarle e per parteciparvi o abbandonarle. Essi comunicano tramite le stesse connessioni sicure esistenti tra la Console dei tecnici e il sito Web e tra l'app Lens e il sito Web.

MediaSDK

Il servizio Media è basato sul progetto open-source WebRTC, con un leggero wrapper sulla base del codice WebRTC. MediaSDK è utilizzato nella Console dei tecnici e nelle app per dispositivi mobili di Lens.

Gestori sessione

Il Gestore sessioni è un semplice sito Web con bilanciamento del carico che fornisce un'API REST per la gestione (creazione/eliminazione/partecipazione/abbandono) delle conferenze. Il Gestore sessioni accetta richieste solo dal sito Web.

Server di streaming

Il servizio Media impiega il server di streaming open source Jitsi per gestire gli streaming tra i peer (la Console dei tecnici e l'app Lens). Sia la Console dei tecnici sia l'app Lens sono connesse al server di streaming. L'app Lens invia i propri contenuti video in streaming al server di streaming,

mentre la Console dei tecnici li riceve. Jitsi funge da server di inoltro tra i peer. Una sessione di Lens ha quindi due stream, uno inviato e uno ricevuto.

STANDARD DI SETTORE DI LOGMEIN RESCUE

SOC 2

LogMeIn Rescue ha la certificazione Service Organization Control 2 (SOC 2), che assicura ai clienti il nostro impegno nell'eseguire i controlli necessari a proteggere i loro preziosi dati.

La certificazione SOC 2 è un'approfondita procedura di esame, basata su molteplici principi e criteri, dei sistemi di controllo impiegati per elaborare i dati e della riservatezza dei dati elaborati mediante tali sistemi. Per mantenere la conformità al SOC 2, questo esame va ripetuto ogni anno. Poiché si tratta di uno standard di riferimento per le aziende di software ed essendo ampiamente riconosciuto dalle imprese statunitensi di ogni settore, il conseguimento e il mantenimento della certificazione SOC 2 è soltanto un altro modo in cui dimostriamo il nostro impegno nei confronti della sicurezza e della privacy.

GDPR

Il regolamento generale sulla protezione dei dati (General Data Protection Regulation o GDPR, in inglese) è una legge dell'Unione Europea (UE) finalizzata alla protezione e alla riservatezza dei dati delle persone che risiedono nell'Unione Europea. Lo scopo principale del GDPR è di dare a cittadini e residenti il controllo dei propri dati personali e di semplificare l'ambiente normativo nell'UE. LogMeIn Rescue offre ai propri utenti il controllo sui dati che conserva per loro conto (Contenuti, come definito nelle Condizioni per l'utilizzo), per consentire loro di concentrarsi sulla propria attività principale preparandosi allo stesso tempo in modo efficiente per il GDPR.

- Gli utenti Rescue possono esportare i propri dati usando la funzionalità di reporting del Centro amministrativo oppure le API di Rescue.
- Gli utenti Rescue possono rimuovere i propri dati conservati nei server di LogMeIn Rescue.
  - Rimuovere tutti i dati associati a un tecnico del supporto.
  - Rimuovere tutti i dati associati a una sessione di supporto, inclusi i dati personali correlati, e associati ai loro clienti.

Grazie a queste funzionalità, LogMeIn Rescue consente ai propri utenti di soddisfare gli standard e io requisiti del GDPR.

Per informazioni dettagliate sul GDPR, visitare il sito sul GDPR di LogMeIn.

HIPAA

Benché LogMeIn non possa controllare i contenuti condivisi dagli utenti durante le sessioni di supporto, il servizio di LogMeIn Rescue è progettato per soddisfare rigorosi standard di sicurezza e per assicurare alle organizzazioni soggette a HIPAA l'osservanza delle relative indicazioni normative.

Controlli degli accessi

- Possibilità di definire a livello capillare l'accesso basato su autorizzazioni (consentendo, ad esempio, ad alcuni tecnici la sola visualizzazione remota ma non il controllo remoto).
- Sui server dei centri dati di LogMeIn non viene archiviato alcun dato dei dispositivi remoti ma, come illustrato in precedenza, vengono conservati solo i dati delle sessioni e delle chat. È inoltre possibile rimuovere dai dettagli delle sessioni i registri dei testi di chat.
- Possibilità di impostare le autorizzazioni in modo da impedire ai tecnici di trasferire file, rendendo così impossibile ai tecnici prelevare file dai dispositivi remoti.

- L’utente finale deve essere presente presso il dispositivo remoto e deve consentire l’accesso remoto.
- L’utente finale mantiene il controllo e può terminare la sessione in qualsiasi momento.
- Ai tecnici può essere impedito l'utilizzo di determinate funzioni finché l'utente finale stesso non conceda loro l'autorizzazione esplicita (ad esempio: controllo remoto, visualizzazione del desktop, trasferimento di file, informazioni di sistema, riavvio e riconnessione).
- Revoca automatica dei diritti d'accesso al termine della sessione.
- Disconnessione automatica dopo un tempo di inattività predeterminato.
- Hosting presso centri dati carrier-grade con accesso protetto e limitato.

Controlli di audit

- Opzione per la registrazione forzata delle sessioni, con la possibilità di memorizzare i file di audit su una rete condivisa protetta.
- Le sessioni dei tecnici e l’attività delle sessioni remote vengono registrate sul computer host per garantire la sicurezza e il controllo qualitativo (accessi riusciti, accessi non riusciti, inizio del controllo remoto, fine del controllo remoto, riavvio, disconnessione).
- Autenticazione delle persone o delle organizzazioni.
- L’identità del tecnico è definita da un indirizzo e-mail univoco o da un ID SSO, e il tecnico deve autenticarsi.
- Blocco dell’account nel caso di un numero eccessivo di tentativi di accesso non riusciti.
- L'accesso ai tecnici può essere consentito solo da indirizzi IP approvati.

Sicurezza delle trasmissioni

- Crittografia AES end-to-end a 256 bit per tutti i dati.
- Hash MD5 per una maggiore tracciabilità dei trasferimenti di file.

CONCLUSIONE

La scelta di una soluzione di supporto remoto è una decisione che spesso dipende dalle funzioni offerte e dal prezzo. LogMeIn Rescue è una soluzione ottimale da entrambi questi punti di vista. Con le informazioni fornite nel presente documento, riteniamo di aver dimostrato come l'architettura su cui si basa Rescue offra adeguati livelli di scalabilità, sicurezza, affidabilità e facilità d'uso.