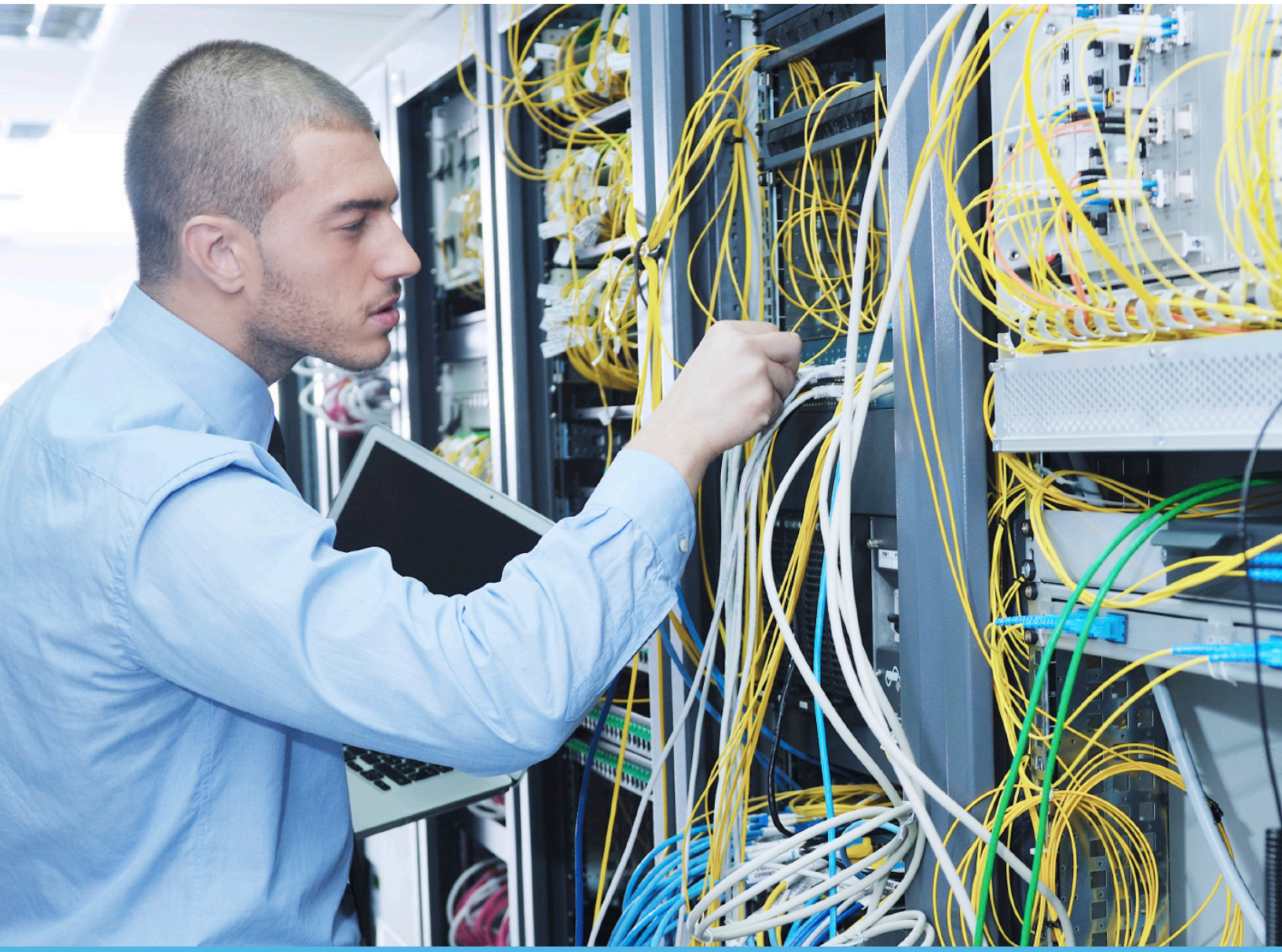
Rescue by LogMeIn

RESCUE – ARCHITECTUUR EN BEVEILIGING

Overzichtsbrochure



Inhoudsopgave

INLEIDING

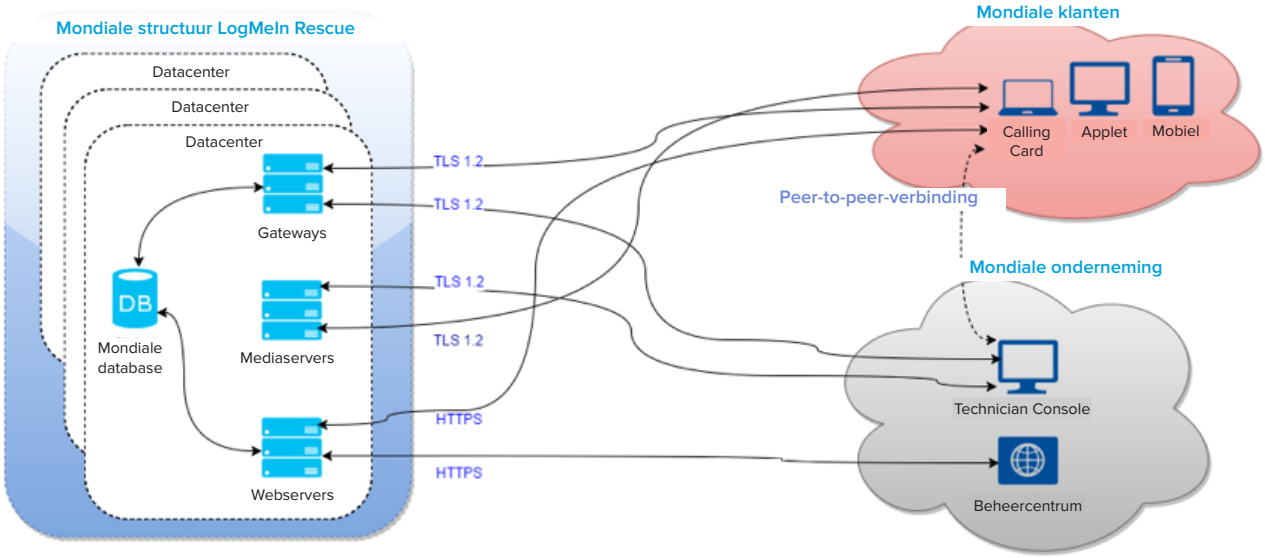
Schaalbaarheid, veiligheid, betrouwbaarheid, gebruiksgemak. Een goede oplossing voor ondersteuning op afstand zou aan deze vier kenmerken moeten voldoen, maar ze gaan helaas niet altijd goed samen. Het is niet moeilijk om een oplossing voor ondersteuning op afstand te vinden die voldoet aan twee van de criteria, misschien lukt drie ook nog, maar een oplossing die voldoet aan alle vier is zeldzaam. Met LogMeIn Rescue biedt LogMeIn, Inc. precies zo'n oplossing.

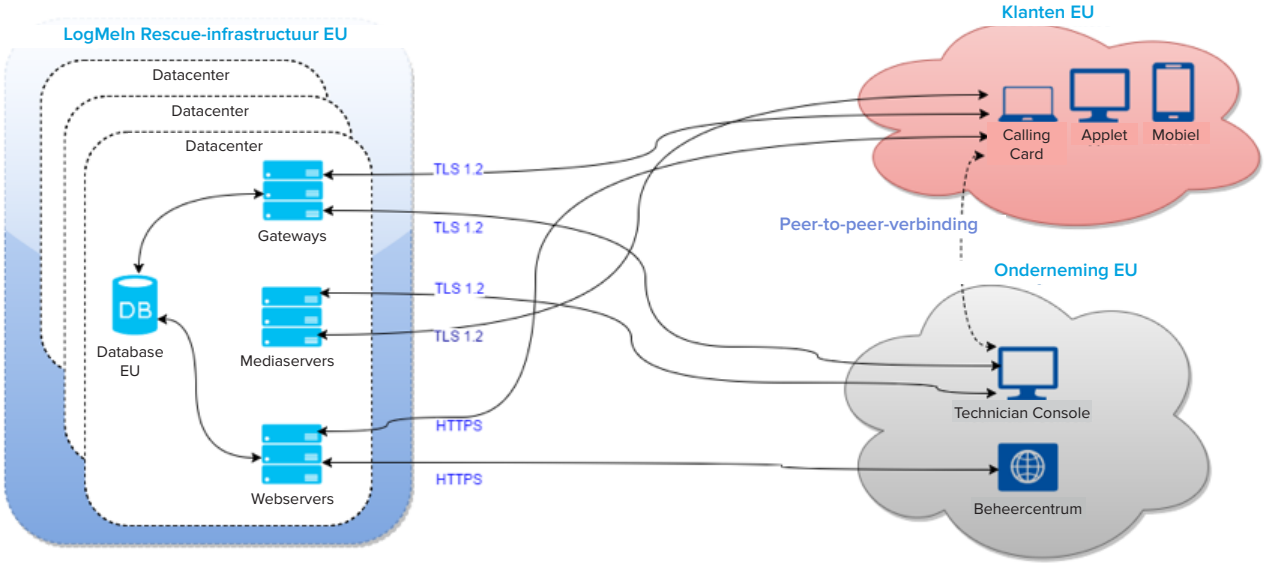
Schaalbaarheid. Of u nu één enkele technicus hebt, of een callcenter met tienduizend medewerkers, Rescue krijgt de klus geklaard.

Beveiliging. Ondersteuningssessies worden beveiligd met end-to-end 256-bit AES-encryptie. De eindgebruikers moeten toestemming geven voor ondersteuningswerkzaamheden voordat de technicus deze kan uitvoeren. Logbestanden van ondersteuningssessies worden versleuteld opgeslagen in een database en kunnen later worden opgevraagd. Sessies met bediening op afstand kunnen in een videobestand worden opgeslagen.

Betrouwbaarheid. Rescue wordt gehost in zes carrier-grade datacenters met een volledig redundante infrastructuur.

Gebruiksgemak. Uw technici kunnen binnen enkele uren aan de slag. Uw ondersteunde eindgebruikers worden geholpen met een paar drukken op de knop. Er hoeft door geen van de partijen software te worden geïnstalleerd.





VERTROUWELIJKHEID VAN GEGEVENS

Vaak wordt 'beveiliging' gelijkgesteld aan 'vertrouwelijkheid van gegevens', wat weer wordt gelijkgesteld aan 'encryptie'. De encryptie wordt dan gekenmerkt door de gebruikte symmetrische versleuteling en de bijbehorende sleutellengte. Deze misvattingen leiden tot foutieve benamingen als '256-bit AES veilig'. Dit is misleidend.

Een veilig online systeem moet altijd voldoen aan de volgende doelstellingen:

- Authenticatie van de communicerende partijen
- Uitwisseling van encryptiesleutels zonder een tussenpersoon die ze kan onderscheppen
- Vertrouwelijke uitwisseling van berichten
- Het vermogen tot detectie als een bericht tijdens de overdracht is bewerkt

SSL/TLS, dat staat voor Secure Sockets Layer & Transport Layer Security, is ontworpen om ondersteuning te bieden voor de bovenstaande stappen. Het is oorspronkelijk halverwege de jaren '90 ontworpen door Netscape Communications Corporation en is sindsdien de standaard voor veilige communicatie via internet. SSL/TLS is geschikt bevonden door Visa, MasterCard en American Express.

De SSL-implementatie die LogMeIn Rescue gebruikt, is OpenSSL (http://www.openssl.org). LogMeIn gebruikt altijd de nieuwste beschikbare versie. Ten tijde van publicatie maakt Rescue gebruik van versie 1.0.2j.

SLEUTELOVEREENKOMST

Als een ondersteuningssessie start en er een verbinding wordt gemaakt tussen de ondersteunde gebruiker en de technicus, moeten hun computers een encryptiealgoritme en een corresponderende sleutel overeenkomen die gedurende de sessie worden gebruikt. Het belang van deze stap wordt vaak over het hoofd gezien. Dit is enigszins begrijpelijk: het lijkt een duidelijke en eenvoudige routinetaak.

Het is evenwel allesbehalve eenvoudig: om zogenaamde man-in-the-middle-aanvallen tegen te gaan (waarbij een computer C zichzelf tussen computer A en B plaatst en zich tegenover B uitgeeft als A en vice versa), moeten certificaten worden gebruikt. Aangezien de technicus en de eindgebruiker beiden geen serversoftware hebben en er een SSL-certificaat is geïnstalleerd op hun computers, maken ze beiden gebruik van de LogMeIn Rescue-servers en voeren ze de eerste fase van de sleutelovereenkomst uit met deze computer. Door verificatie van het certificaat door zowel de Technician Console als de applet van de eindgebruiker, kan alleen een Rescue-server bemiddelen in het proces.

BERICHTEN UITWISSELEN

TLS biedt een breed aanbod aan versleutelingssuites waarvan gebruik kan worden gemaakt. De communicerende partijen kunnen het eens worden over een encryptieschema dat ze beide ondersteunen. Dit heeft twee hoofddoelen: ten eerste kan het protocol worden uitgebreid met nieuwe versleutelingssuites zonder de compatibiliteit met eerdere versies te verbreken en ten tweede kunnen nieuwere implementaties ondersteuning voor suites laten vallen als bekend is dat deze bepaalde cryptografische zwakheden hebben.

Aangezien de drie onderdelen van het LogMeIn Rescue-communicatiesysteem onder controle van LogMeIn vallen, is de versleutelingssuite die door deze onderdelen wordt gebruikt altijd dezelfde: AES256-SHA in cipher-block chaining-modus met RSA-sleutelovereenkomst. Dat betekent:

- De encryptiesleutels worden uitgewisseld met privé- en algemene RSA-sleutelparen, zoals beschreven in het vorige gedeelte
- Als encryptie-/decryptiealgoritme wordt AES (Advanced Encryption Standard) gebruikt
- De encryptiesleutel is 256 bits lang
- Als basis van MAC's (berichtverificatiecodes) wordt SHA-2 gebruikt. Een MAC is een kort stukje informatie dat wordt gebruikt om een bericht te verifiëren. De MAC-waarde beschermt zowel de integriteit van een bericht als de authenticiteit ervan, doordat communicerende partijen alle wijzigingen aan het bericht kunnen detecteren.
- De cipher-block chaining-modus (CBC) zorgt dat ieder versleuteld tekstblok afhankelijk is van de leesbare tekstblokken tot op dat punt. Soortgelijke berichten kunnen niet worden onderscheiden op het netwerk.

Dit zorgt ervoor dat gegevens die tussen de ondersteunde gebruiker en de technicus worden overgedragen end-to-end zijn versleuteld en dat alleen de betrokken partijen toegang hebben tot de informatie binnen de berichtenstroom.

VERIFICATIE EN AUTORISATIE

Verificatie en autorisatie dienen in LogMeIn Rescue twee specifieke doelen.

Verificatie is de bevestiging dat de technicus of beheerder die is ingelogd bij het Rescue-systeem echt is wie hij zegt dat hij is. Verificatie in Rescue is eenvoudig. Technici krijgen een ID om zich aan te melden (doorgaans is dit hun e-mailadres) en een bijbehorend wachtwoord van hun beheerders. Deze aanmeldgegevens worden bij het begin van de werkdag van een technicus ingevoerd op het aanmeldformulier op de LogMeIn Rescue-website.

In LogMeIn Rescue wordt het Rescue-systeem eerst geverifieerd door de technicus (of beter gezegd, de webbrowser van de technicus) met het 2048-bit premium RSA SSL-certificaat. Zo wordt gegarandeerd dat de technicus zijn gebruikersnaam/wachtwoord op de juiste website invoert. De technicus logt vervolgens in op het systeem met zijn aanmeldgegevens.

LogMeIn Rescue slaat geen wachtwoorden op. In plaats daarvan maakt gebruik van het scrypt-algoritme om hashes van wachtwoorden te maken. Alleen deze hashes worden opgeslagen in de Rescue-database. Hashes van wachtwoorden worden aangemaakt nadat een met CSPRNG gegenereerde tekenreeks van 24 tekens aan elk uniek wachtwoord wordt toegevoegd (salting).

LogMeIn Rescue biedt beheerders een aantal opties voor het wachtwoordbeleid:

- Beheerders kunnen een vereiste wachtwoordsterkte en maximale houdbaarheid afdwingen – een ingebouwde meter laat beheerders en technici de sterkte van het gekozen wachtwoord zien
- Technici kunnen worden gedwongen om hun Rescue-wachtwoord bij hun volgende aanmelding te vernieuwen
- Hoofdbeheerders kunnen afdwingen dat gebruikers binnen hun organisatie tweeledige verificatie gebruiken voor hun aanmelding bij Rescue.

In LogMeIn Rescue kunnen beheerders ook een Single Sign-On-beleid (SSO) implementeren. Er wordt gebruikgemaakt van SAML (Security Assertion Markup Language), een XML-standaard voor het uitwisselen van verificatie- en autorisatiegegevens tussen beveiligingsdomeinen, dus tussen een identiteitsleverancier en een serviceprovider. Technici hebben vervolgens alleen toegang tot van tevoren opgegeven applicaties en één SSO-ID om op deze applicaties in te loggen. Met één druk op de knop kan het SSO-ID van een technicus worden uitgeschakeld.

De tweeledige verificatie maakt gebruik van de LastPass Authenticator om een tweede beveiligingslaag aan te brengen voor een Rescue-account. Geselecteerde leden van de organisatie worden hierbij verplicht een extra methode in te stellen om hun identiteit te verifiëren. Het instellen van de authenticator-app wordt geactiveerd in de volgende gevallen:

- Het geselecteerde lid probeert om zich bij zijn Rescue-account aan te melden op de beveiligde website.
- Het geselecteerde lid probeert om zich bij de Technician Console op het bureaublad aan te melden.
- Het geselecteerde lid probeert zijn of haar Rescue-wachtwoord te veranderen.

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

Autorisatie gebeurt echter zeer frequent: ten minste één keer tijdens elke ondersteuningssessie op afstand. Een technicus neemt na het downloaden en uitvoeren van de ondersteuningsapplet contact op met de ondersteunde eindgebruiker. De technicus kan via de applet chatten met de eindgebruiker, maar iedere verdere actie, zoals het verzenden van een bestand of het weergeven van het bureaublad van de eindgebruiker, vereist specifieke toestemming van de gebruiker. Het is ook mogelijk om een 'eenmalige vraag' te implementeren. Deze is bedoeld voor langdurig werken met ondersteuning op afstand waarbij de klant mogelijk niet aanwezig is gedurende de hele sessie. Als deze vlag is ingeschakeld voor een technicusgroep, kunnen de

gebruikers in deze groep een 'algemene' toestemming aanvragen bij de klant. Als deze wordt verleend, kunnen ze acties uitvoeren zoals systeeminformatie weergeven of een sessie met besturing op afstand openen zonder dat daarvoor toestemming van de eindgebruiker nodig is.

Beheerders kunnen ook IP-adresbeperkingen aan hun technici opleggen. De beschikbare IP-adressen kunnen, als ze zijn geselecteerd, worden beperkt tot een zeer korte lijst. Technici die een bepaalde taak toegewezen hebben gekregen kunnen Rescue dan alleen openen vanaf van tevoren voor die taak goedgekeurde IP-adressen.

De beheerder van een groep technici kan ook bepaalde functies in het beheercentrum uitschakelen. De beheerder kan bijvoorbeeld instellen dat leden van een bepaalde Technicusgroep geen bestanden van eindgebruikers kunnen ontvangen. Dit zijn enkele handelingen waarvoor de beheerder toestemming kan verlenen of weigeren:

- Besturing op afstand starten
- Opnieuw opstarten
- Bureaubladweergave starten
- Sessies opnemen
- Bestanden verzenden en ontvangen
- Privésessies starten
- Bestandsbeheer starten
- Verzoeken om Windows-aanmeldingsgegevens
- URL's versturen
- Synchronisatie van Klembord toestaan
- Systeeminformatie bekijken
- Scripts uitvoeren
- Eenmalige vraag voor alle toegangsrechten gebruiken
- Sessies overdragen
- Schermen delen met klanten toestaan

Het Rescue-systeem wordt ook geverifieerd voor de ondersteunde eindgebruiker. De applet die wordt gedownload en door de gebruiker wordt ondertekend met het code signing-certificaat van LogMeIn (op basis van een 2048-bit RSA-sleutel). Deze informatie wordt doorgaans in de webbrowser voor de gebruiker weergegeven wanneer deze de software gaat uitvoeren.

De ondersteunde gebruiker wordt niet geverifieerd. Het is de taak van de technicus om te bepalen wie de gebruiker is, via chat of via een telefoongesprek. Het Rescue-systeem biedt mechanismen die op verificatie lijken, zoals unieke pincodes, maar deze worden gebruikt voor routering van de ondersteuningssessies naar de juiste privé- of gedeelde rij en mogen niet worden beschouwd als verificatiesysteem.

CONTROLE EN LOGBOEKEN

Elke oplossing voor ondersteuning op afstand moet sterk de nadruk leggen op verantwoordelijkheid. LogMeIn Rescue biedt twee specifieke controlefuncties.

Ten eerste wordt het zogenaamde 'chatlogboek' opgeslagen in de Rescue-database. Het chatlogboek wordt door de Technician Console in realtime overgedragen aan de Rescue-servers en bevat zowel gebeurtenissen als chatberichten die bij een bepaalde ondersteuningssessie horen. Er wordt bijvoorbeeld een logbestand weergegeven als er een sessie met besturing op afstand wordt gestart of beëindigd, of als een technicus een bestand naar de eindgebruiker stuurt. Als ze van toepassing zijn, worden bijbehorende metagegevens, zoals de naam en MD5 Hash-vingerafdruk van een overgedragen bestand, ook opgenomen in het logbestand. De chatlogboekdatabase kan worden geraadpleegd via het beheercentrum. Ten tijde van publicatie van dit artikel is in het bewaarbeleid voor gegevens van LogMeIn vastgelegd dat de inhoud van de logbestanden tot twee jaar na het einde van een ondersteuningssessie online beschikbaar moet zijn en het daarna nog twee jaar in het archief moet worden bewaard. LogMeIn Rescue kan sessie-informatie aan een URL toevoegen om integratie met CRM-systemen te faciliteren. Beheerders kunnen kiezen of ze chatberichten uit deze informatie willen weglaten. Daarnaast kunnen alle chatberichten tussen technici en klanten automatisch worden weggelaten uit de sessie-informatie die op het Rescue-datacenter wordt opgeslagen.

Bovendien staat LogMeIn Rescue technici toe om de gebeurtenissen die zich voordoen tijdens een bureaubladweergave of een sessie met besturing op afstand in een videobestand op te nemen. Dit is een zeer belangrijke functie vanwege verantwoordelijkheid en aansprakelijkheid.

De opnamebestanden worden in een map opgeslagen die door de technicus wordt opgegeven. In het geval van een grote ondersteunende organisatie moet deze locatie zich op een netwerkserver bevinden. De schijfruimte die door deze opnames wordt gebruikt kan zeer uiteenlopen en is geheel afhankelijk van de inhoud (en comprimeerbaarheid) van het bureaublad van de ondersteunde eindgebruiker. Op basis van een analyse van miljoenen sessies met besturing op afstand met de technologie van LogMeIn, is de gemiddelde vereiste schijfruimte voor de gegevens van één minuut ondersteuning op afstand tussen de 372 en 1024 Kb. De opnames worden direct als AVI opgeslagen of in een tussenliggende indeling van LogMeIn die met de applicatie 'Rescue AVI Converter' kan worden omgezet naar standaard AVI-bestanden. Deze applicatie kan worden gedownload van help.logmein.com. De indeling van LogMeIn (RCREC) kan de bestandsgrootte van de opnames met ongeveer 10% verkleinen.

ARCHITECTUUR VAN DATACENTER

LogMeIn wordt gehost in hypermoderne, veilige datacenters die beschikken over:

- Meerlaagse procedures voor veiligheidscontrole, biometrische toegangssystemen, 24/7 CCTV en alarmbewaking
- Niet-onderbreekbare redundante stroomvoorziening (wissel- en gelijkstroom), noodstroomaggregaten op locatie
- Redundant HVAC-ontwerp met luchtdistributie onder een verhoogde vloer voor maximale controle over de temperatuur
- Rookdetectiesysteem boven en onder de verhoogde vloer en dubbel-gekoppelde, anticiperende brandbeveiliging met droge blusleidingen

De LogMeIn Rescue-infrastructuur zelf is zeer veilig en betrouwbaar:

- Redundantie op serveronderdeelniveau: redundante voeding en ventilatoren, RAID-1 gespiegelde harde schijven
- Redundantie op serverniveau: afhankelijk van rol, actieve-/passieve of actieve-/actieve clusters
- Redundantie op datacenterniveau: Zes datacenters (westkust VS, midden VS, zuiden VS, oostkust VS, Londen en Frankfurt) met vrijwel onmiddellijke failovercapaciteit
- Dubbele redundante firewalls waarvan alleen poorten 80 en 443 zijn geopend
- Actieve-/passieve databaseclusters
- Redundante load balancers inclusief SSL
- Load-balanced en redundante web- en applicatieserverclusters
- Load-balanced en redundante gatewayserverclusters

OVERZICHT VAN HET HAND-OFFPROCES VAN DE RESCUE GATEWAY

De digitaal ondertekende Rescue-applet wordt gestart op een computer:

- Deze bevat een sessieverificatie-GUID (Globally Unique Identifier) die is genest in het .exe-bestand als bron van de site waarvan het is gedownload.
- Er wordt een lijst met beschikbare gateways gedownload van secure.logmeinrescue.com.
- Hierna wordt er een gateway uit de lijst gekozen en hiermee wordt met TLS verbinding gemaakt; de gateway wordt geverifieerd door de applet met het SSL-certificaat.
- De gateway verifieert de applet in de database met de GUID en registreert dat de gebruiker op een technicus wacht.

Een sessie wordt opgepakt in de Technician Console van Rescue:

- Er wordt een aanvraag naar de gateway verzonden met de sessieverificatie-GUID om verbinding te maken tussen de Technician Console en de applet van de klant.
- De gateway verifieert de verbinding en geeft gegevens door op transportniveau (het codeert de doorgegeven gegevens niet).

Als een verbindingsrelais wordt gestart proberen de partijen een peer-to-peer-verbinding (P2P) te maken:

- De applet zoekt naar een TCP-verbinding op een door Windows toegewezen poort.
- Als de TCP-connectie niet kan worden gemaakt binnen een bepaalde tijd (10 seconden), wordt er een poging gedaan om een UDP-verbinding te maken met hulp van de gateway.
- Als er een TCP- of UDP-verbinding wordt gemaakt, verifiëren de partijen het P2P-kanaal (met behulp van de sessieverificatie-GUID) en neemt deze het verkeer over van de doorgegeven verbinding.
- Als er een UDP-verbinding is gemaakt, wordt TCP met XTCP (een eigen protocol van LogMeIn op basis van de BSD TCP-stack) geëmuleerd bovenop de UDP-datagrammen.

Iedere verbinding wordt beveiligd met het TLS-protocol (met AES256-encryptie met SHA256 MAC). De sessieverificatie-GUID is een 128-bit waarde van een geheel getal dat willekeurig is gecodeerd.

DATABASE

- Alle gegevens die gevoelige informatie bevatten, zijn beveiligd met 256-bits AES-encryptie (chatlogs en aangepaste velden).
- Iedere 24 uur wordt automatisch een back-up gemaakt van de Rescue-database. De back-updatabase wordt opgeslagen in het datacenter, met dezelfde encryptie als het origineel.
- Met de Data Residency-optie kunt u een locatie kiezen voor de opslag van gegevens van eindgebruikers: binnen de EU (Frankfurt, Londen) of in de VS. LogMeIn garandeert dat diegenen die kiezen voor gegevensopslag binnen de EU exclusief verbinding maken met datacenters binnen de EU, en dat gebruikersgegevens uitsluitend binnen de gekozen regio worden bewaard. Er bestaat geen verbinding tussen onze datacenters in de EU en de datacenters in de VS.

DE ARCHITECTUUR VAN RESCUE MEDIA

De Rescue Media Service is een op zichzelf staande service op basis van WebRTC, die videostreaming mogelijk maakt voor Rescue Lens. Deze service beheert de zogeheten 'vergaderingen' voor Rescue-sessies waarbij de Lens-functie wordt ingezet. Deelnemers aan de vergadering (peers) kunnen vergaderingen binnengaan en ze verlaten en clients kunnen video- en audiostreams verzenden, die andere deelnemers kunnen ontvangen. Lens verstuurt videocontent als éénrichtingsstream vanuit de Lens-app naar de Technician Console.

De Media Service bestaat uit drie hoofdcomponenten: de MediaSDK, de Sessiebeheerder en de streamingserver. Deze componenten beheren het proces van het aanmaken en verwijderen en binnengaan en verlaten van vergaderingen. De componenten communiceren via de bestaande beveiligde verbindingen tussen de Technician Console en de website en tussen de Lens-app en de website.

MediaSDK

De Media Service is opgebouwd op basis van WebRTC met een dunne schil rond de WebRTC-code. De zogeheten MediaSDK wordt gebruikt in de Technician Console en de Lens-apps voor mobiel gebruik.

Sessiebeheerders

De Sessiebeheerder is een eenvoudige load-balanced website met een REST-API voor het beheren (aanmaken/verwijderen/deelnemen/verlaten) van vergaderingen. De Sessiebeheerder accepteert alleen verzoeken van de website.

Streamingservers

De Media Service gebruikt een Jitsi open source-oplossing voor de streamingserver om de streams tussen peers (de Technician Console en de Lens-app) af te handelen. De Technician Console en de Lens-app zijn allebei verbonden met de streamingserver. De Lens-app streamt de videocontent naar de streamingserver. De Technician Console streamt videocontent van de server. Jitsi fungeert als

relayserver tussen de peers. Een Lens-sessie heeft twee streams: één wordt verzonden, de ander ontvangen.

NORMEN IN DE SECTOR VAN LOGMEIN RESCUE

SOC 2

LogMeIn Rescue voldoet aan alle eisen van Service Organization Control 2 (SOC 2). Hierdoor kunnen klanten erop vertrouwen dat we de juiste controlemechanismen toepassen om hun belangrijke gegevens te beschermen.

SOC 2 is een uitgebreide auditing-procedure op basis van meerdere principes en criteria en omvat het testen van alle controlesystemen voor gegevensverwerking en de vertrouwelijkheid die deze systemen bieden. Voor SOC 2-compliance is een jaarlijkse audit vereist. SOC 2 geldt als de gouden standaard voor softwarebedrijven. Onze compliance met SOC 2 is slechts één van de manieren waarop we laten zien dat we extreem zorgvuldig omgaan met beveiliging en privacy.

GDPR

De General Data Protection Regulation (GDPR), in het Nederlands de Algemene Verordening Gegevensbescherming (AVG), is de Europese wet om de privacy en gegevens van alle EU-ingezetenen te beschermen. De GDPR is voornamelijk bedoeld om burgers en ingezetenen controle te geven over hun persoonlijke gegevens en om het regelgevingskader EU-breed te vereenvoudigen. LogMeIn Rescue biedt zijn gebruikers controle over de gegevens die we namens hen opslaan (Content – zoals gedefinieerd in de Dienstverleningsvoorwaarden) zodat ze zich op hun kerntaken kunnen concentreren, terwijl ze zich efficiënt voorbereiden op de GDPR.

- Gebruikers van Rescue kunnen hun gegevens exporteren via de rapportagefunctie in het Beheercentrum of via de Rescue-API's.
- Gebruikers van Rescue kunnen hun gegevens die opgeslagen zijn op servers van LogMeIn Rescue verwijderen.
  - Verwijder alle gegevens die gekoppeld zijn aan een supporttechnicus.
  - Verwijder alle gegevens die gekoppeld zijn aan een supportsessie, inclusief persoonlijke gegevens met betrekking tot hun klanten.

Met behulp van deze functies stelt LogMeIn Rescue zijn gebruikers in staat om te voldoen aan de standaarden en vereisten van de GDPR.

Ga voor meer informatie over GDPR naar de LogMeIn GDPR-pagina.

HIPAA

Hoewel LogMeIn geen controle heeft over de content die door gebruikers wordt gedeeld tijdens een ondersteuningssessie is de LogMeIn Rescue-service ontworpen volgens strenge beveiligingsnormen, waarmee door HIPAA gereguleerde entiteiten kunnen voldoen aan de relevante regelgeving.

Toegangscontrole

- Op toestemming gebaseerde toegang kan tot op detailniveau worden geregeld (bijvoorbeeld om sommige technici toegang te geven tot weergave op afstand maar niet tot besturing op afstand)
- Er worden geen gegevens van externe apparaten opgeslagen op servers in LogMeIn-datacenters (zoals hierboven vermeld worden alleen sessie- en chatgegevens opgeslagen). Daarnaast kunnen chatlogboeken worden verwijderd uit de sessie-informatie.
- Machtigingen kunnen zo worden ingesteld dat technici geen overdrachtsrechten hebben. Zo kunnen ze geen bestanden van externe apparaten halen.
- De eindgebruiker moet aanwezig zijn bij het externe apparaat en moet externe toegang toestaan

- De eindgebruiker behoudt de controle en kan de sessie op elk moment beëindigen
- De toegang tot bepaalde voorzieningen kan technici worden geweigerd totdat de eindgebruiker expliciet toestemming geeft (bijvoorbeeld besturing op afstand, bureaubladweergave, bestandsoverdracht, systeeminformatie en opnieuw opstarten en verbinden)
- Toegangsrechten worden automatisch herroepen wanneer de sessie is beëindigd
- Van tevoren bepaalde periode van inactiviteit forceert automatisch afmelden
- Gehost op redundante, carrier-grade datacenters met beperkte, beveiligde toegang

Controlebeheer

- Optie voor geforceerde sessie-opname met de mogelijkheid controlebestanden op te slaan op een veilige gedeelde netwerklocatie
- Sessies met technici en activiteiten van sessies op afstand worden bijgehouden op de hostcomputer om de beveiliging te garanderen en kwaliteitscontrole te behouden (succesvolle aanmeldingen, mislukte aanmeldingen, start van besturing op afstand, einde van besturing op afstand, start van opnieuw starten, uitloggen)
- Verificatie van persoon of entiteit
- De identiteit van de technicus wordt bepaald door een uniek e-mailadres of via een SSO-ID, en de technicus moet worden geverifieerd
- Bij hoge aantallen mislukte aanmeldpogingen wordt de account geblokkeerd
- Optie om technici uitsluitend vanaf goedgekeurde IP-adressen te laten inloggen

Overdrachtsbeveiliging

- End-to-end, 256-bit AES-encryptie van alle gegevens
- MD5 Hash voor betere traceerbaarheid van bestandsoverdrachten

CONCLUSIE

De keuze voor een oplossing voor ondersteuning op afstand wordt vaak gebaseerd op de functies en de prijs. Als u dit document leest, is het waarschijnlijk dat LogMeIn Rescue voldoet aan uw eisen binnen deze categorieën. Met de informatie die hier is gegeven, zijn wij ervan overtuigd dat we u hebben kunnen bewijzen dat de architectuur achter Rescue de juiste niveaus in schaalbaarheid, veiligheid, betrouwbaarheid en gebruiksgemak kan bieden.