COVID-19のパンデミック時のビジネス継続性の サポート – モバイルおよびリモートアクセスソ リューションリソース

内容

概要

<u>SIZE</u>

設定

トラブルシュート

概要

このドキュメントでは、Cisco Expresswayを介したモバイルおよびリモートアクセス(MRA)ソリューションのサイズ設定、トラブルシューティング方法について説明します。

SIZE

MRA Scale Application Noteは、Cisco MRAの導入で既存の容量を最適化する方法と、追加の容量を評価する方法に関するガイダンスを示しています。

さらに、Cisco Expresswayのサイジング情報は、<u>Preferred Architecture for Cisco Collaboration</u> 12.x Enterprise On-Premises Deployments、CVD、表9-8および9-9で入手できます。

設定

- <u>Cisco Expresswayを使用したモバイルおよびリモートアクセス導入ガイド(X12.5)</u>と <u>Expressway MRA基本設定</u>(ビデオ)では、MRAソリューションの設定方法を段階的に説明 しています。
- ファイアウォールの要件については、「<u>Cisco ExpresswayのIPポートの使用</u>」を参照<u>してく</u> ださい。
- 導入によっては、内部ドメインと外部ドメインが異なる場合があります。MRAの設定方法<u>については、「マルチドメイン展開でのExpressway/VCSを介したモバイルおよびリモートアクセスの設定</u>」を参照してください。

トラブルシュート

MRA経由でのJabberログインに失敗した場合は、次の手順を実行して問題をトラブルシューティングします。

ステップ1:一連のテスト<u>認証情報を使用し</u>て、Collaboration Solutions Analyzer(CSA)を実行します。

CSAは、コラボレーションソリューションのツールスイートです。CSAは、コラボレーションソ

リューションのライフサイクルのさまざまなフェーズ、特にMRAのコラボレーションエッジ (CollabEdge)検証を支援し、ソリューションのトラブルシューティングに必要な時間を大幅に短縮します。

CollabEdge validatorは、クライアントログインプロセスをシミュレートしてMRA展開を検証するツールです。いくつかのチェックが完了しました。

- パブリックドメインネームシステム(DNS)エントリの検証
- 外部接続チェック
- Expressway-E(Exp-E)SSL証明書
- Unified Communications Manager(UCM)およびIM & Presence Server(IM&P)関連のアプリケーションフローチェック ユーザデータサービス(UDS)eXtensible Messaging and Presence Protocol (XMPP) Session Initiation Protocol(SIP)登録

入力

少なくとも、このツールでは、ドメインがDNS設定、Exp-E検出、接続、およびExp-E SSL証明書を確認する必要があります。テストユーザ名とパスワードを指定すると、ツールはUCMからユーザとデバイスの設定を取得し、IM&Pに対して認証を試み、関連付けられたデバイスを登録できます。電話機のみの導入の場合は、チェックボックスをオンにすると、IM&Pチェックがスキップされます。

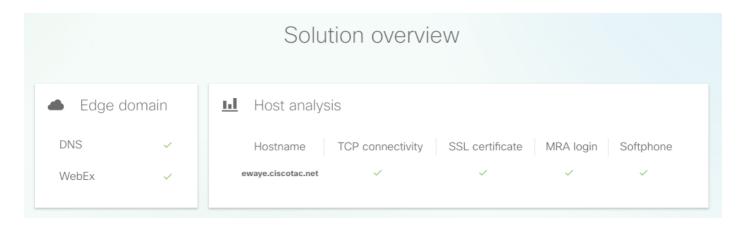
/ Fill in below details



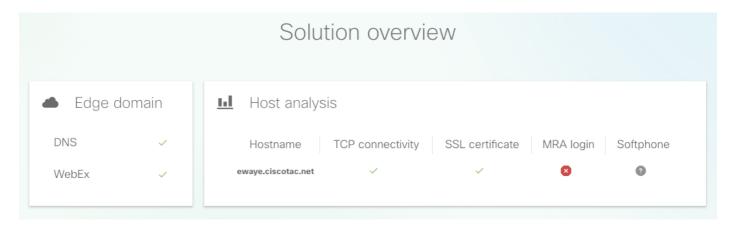
Validate MRA deployment

出力例

最初に表示されるのは、ログイン試行の概要です。このログには、動作の概要と失敗の概要が示されます。すべてが正しく動作する例:

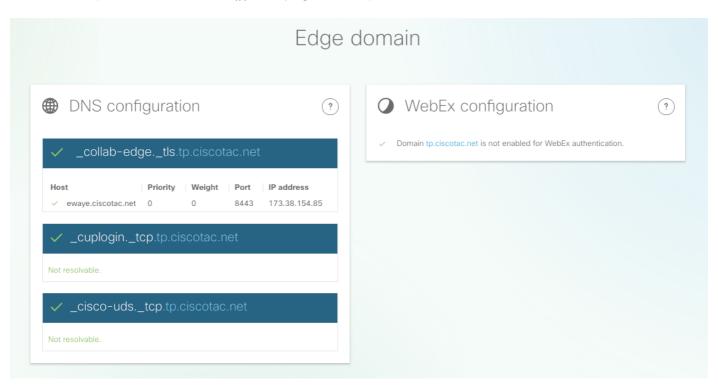


何かが機能しない場合は、障害が発生したセクションにすぐに表示されます。詳細については、 このドキュメントの特定のセクションを参照してください。



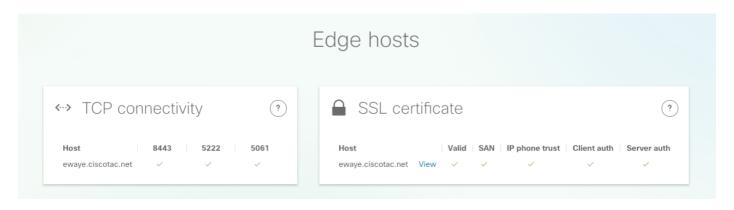
エッジドメインの検証

エッジドメイン検証では、DNSレコードに関するすべての詳細が表示されます。チェックマークをクリックすると、チェックの詳細が表示されます。



外部接続とExp-E SSL証明書のチェック

このセクションでは、DNSレコードで検出された各ホストの接続とExp-E証明書チェックの詳細を示します。疑問符は、チェックの内容と理由の詳細を確認するためにも使用できます。



証明書の詳細ビューを開き、チェーン全体のすべての詳細を使用可能にするには、ホスト名の横にある[View]をクリックします。

SSL certificate ewaye.tp.ciscotac.net Certificate chain Full chain available ▼ CN: Go Daddy Root Certificate Authority - G2 ▼ CN: Go Daddy Secure Certificate Authority - G2 CN: ewaye.ciscotac.net Summary ewaye.ciscotac.net Subject: OU=Domain Control Validated, CN=ewaye.ciscotac.net C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2 Detail Certificate: Data: Version: 3 (0x2)

Serial Number: 13402504543026767831 (0xb9ff42df53ab67d7)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go

Daddy Secure Certificate Authority - G2

Validity

Not Before: Aug 18 13:44:01 2017 GMT Not After: Mar 21 16:19:00 2019 GMT

Subject: OU=Domain Control Validated, CN=ewaye.ciscotac.net

エッジサーバ

このセクションでは、エッジ設定の詳細を示します。これは、DNSによって検出されたすべての Exp-Eに対して実行されます。

Tested edge servers

?

ewaye.ciscotac.net

- ▲ Single sign-on (SSO)
- Domain tp.ciscotac.net is not enabled for SSO.
- OAuth token with refresh is not enabled.

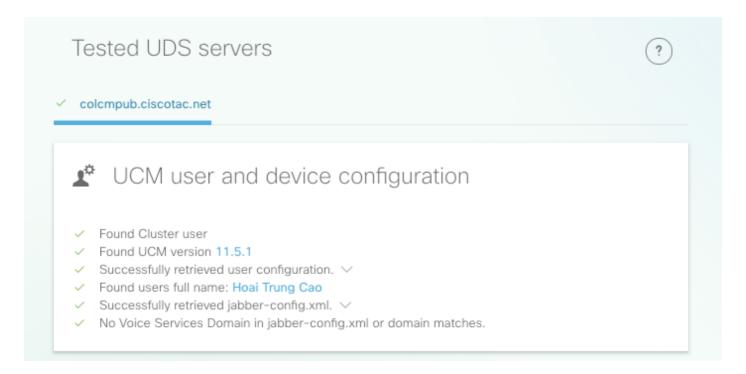
- ✓ Successfully retrieved edge config. ✓
- Found _cisco-uds SRV record in edge config: colcmpub.ciscotac.net:8443 colcmsub.ciscotac.net:8443
- Found user home cluster: 192.168.0.50:8443
- Found SIP edge server: ewaye.ciscotac.net:5061
- Found XMPP edge server: ewaye.ciscotac.net:5222
- ✓ Found HTTP edge server: ewaye.ciscotac.net:8443

回答の内容を拡張することもできます。

Successfully retrieved edge config.

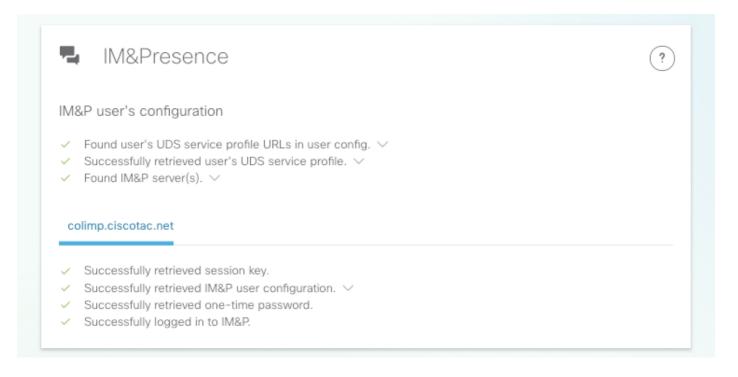
UDSサーバ

選択できる各エッジサーバについて、get_edge_configで返されたUDSサーバは、動作中のサーバが見つかるか、すべてが失敗するまで、1つずつテストされます。



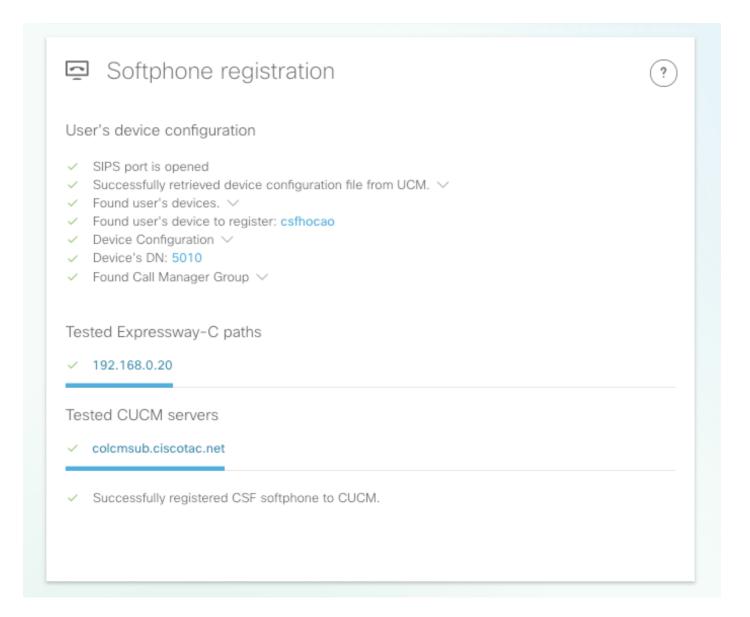
IM&Pサーバ

[エッジサーバ(Edge Servers)]セクションで選択できる各エッジサーバに対して、動作中のサーバが見つかるか、すべてが失敗するまで、IM&Pサーバ(サービスプロファイルからフェッチ)が1つずつテストされます。



ソフトフォンの登録

[Edge Servers]セクションで選択できる各エッジサーバについて、ソフトフォンの登録がテストされます。テストするソフトフォンのタイプは、ユーザに関連付けられているデバイスによって異なり、優先順位リストに従います。CSF、BOT、TCT、TAB。選択したエッジサーバに対して、Exp-Cサーバ(get_edge_configによって返される)とUnified CMサーバ(CUCMグループで設定される)は、組み合わせが機能するか、またはすべてが失敗するまでテストされます。



ステップ2:ログインプロセスが失敗した場所を確認したら、<u>Collaboration Edgeの最も一般的な</u> <u>問題を使用して</u>き、既知の問題の1つと一致するかどうかを確認します。

CSAで証明書の問題が見つかった場合<u>は、「Collaboration Edge(MRA)証明書の設定とトラブルシューティン</u>グ」または「<u>Expresswayへのサーバ証明書のインストール</u>」(ビデオ)を参照してください。

Exp-EでスタティックNetwork Address Translation(NAT;ネットワークアドレス変換)を使用する単一のネットワークインターフェイスコントローラ(NIC)を使用し、適応型セキュリティアプライアンス(ASA)を使用する場合は、「<u>VCS Expressway TelePresenceデバイスのNATリフレクションのの設定」を</u>を参照正しく設定されています。

ステップ3:問題を解決できなかった場合は、Expresswayログと問題レポートを含むTechnical Assistance Center(TAC)ケースをオープンします。

- Expressway診断ログおよびパケットキャプチャのダウンロード(ビデオ)
- Jabberデスクトップ問題レポートの入手(ビデオ)