يتم حظر الملاحظات من نقطة نهاية MXP الخاصة بي إلى TMS بواسطة الشبكة أو خادم الويب - ماذا يعني هذا؟

المحتويات

المقدمة

تتعلق هذه المقالة بمجموعة إدارة نظام TelePresence من Cisco.

س. الملاحظات من نقطة نهاية MXP إلى TMS تم حظرها بواسطة الشبكة أو خادم الويب - ماذا يعني هذا؟

ألف - تعتمد نظم إدارة الدعم التقني على التغذية المرتدة المرسلة من النظم. تقوم معظم أنظمة TANDBERG و Polycom بإرسال هذه الملاحظات باستخدام إتصالات HTTP أو HTTPS مجهولة. يمكن حظر هذا الاتصال إذا كان هناك وكيل ويب على الشبكة يتطلب المصادقة. في هذه الحالة، يجب التحدث إلى مسؤول الوكيل حول إضافة إستثناء لحركة المرور الموجهة ل TMS.

هناك فشل شائع آخر وهو منع جدران الحماية للطلبات الواردة إلى TMS. يوضح مستند دعم منتجات TMS المنافذ والبروتوكولات التي يجب أن تكون متوفرة لكل نوع من أنواع النظام.

الفشل الشائع الأخير هو قيام المسؤول بتعديل تكوين IIS يدويا بعد تثبيت TMS وتعطيل الوصول المجهول إلى أدلة الويب. الوصول المجهول مفتوح لأجزاء معينة من TMS فقط ولا يمكن تعطيله لأن الأنظمة لا تستخدم أسماء المستخدمين وكلمات المرور عند إرسال الملاحظات.

لتصحيح أي تكوين غير صحيح ل IIS، قم بإزالة تثبيت TMS وأعد تثبيته. لن يتم فقد أي بيانات عميل طالما لم يتم ترك قاعدة البيانات كما هي، وسيقوم المثبت بإعادة إنشاء خصائص موقع الويب بشكل صحيح.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).