أستكشاف أخطاء اتصال Azure Virtual Desktop وإصلاحها

المحتويات

مسألة

تفشل إتصالات Azure Virtual Desktop (AVD) عندما يصل المستخدمون إلى AVD من شبكة المكتب مع تمكين Cisco Secure Access. ولوحظ هذا السلوك المحدد:

- يعمل AVD بشكل جيد عند الوصول إليه من شبكة شخصية مع تعطيل الوصول الآمن.
- يعمل AVD بشكل جيد عند الوصول إليه من شبكة المكتب دون الوصول الآمن.
- لا يعمل AVD عند الوصول إليه من أي شبكة مع تمكين الوصول الآمن.

يؤثر هذا الفشل في الاتصال على قدرة المستخدمين على الوصول إلى أجهزة الكمبيوتر المكتبية الافتراضية الخاصة بهم، كما يؤثر على عمليات أعمال الإنتاج. أظهر تحليل التقاط الحزمة حركة مرور ثنائية الإتجاه في كل من سيناريوهات العمل وغير العمل مع عدم وجود برامج TCP أو مؤشرات أخرى على مستوى الشبكة تقوم Secure Access بإنهاء اتصال AVD.

البيئة

- الوصول الآمن من Cisco مع تمكين الوصول إلى الشبكة دون ثقة (ZTNA)
- تم تكوين ملف تعريف ZTNA لاستخدام ZTA لجميع وجهات الإنترنت
- تم الوصول إلى نشر Azure Virtual Desktop (AVD) من خلال نقاط النهاية من Microsoft
- Secure Access عميل نشر مع Office شبكة بيئة
- المستخدمون الذين يصلون إلى AVD من كل من شبكات المكتب والشبكات الشخصية

رارق

تم حل المشكلة بإضافة المجالات المرتبطة ب Microsoft AVD إلى قائمة إستثناءات ZTA، مما يسمح لعميل Secure Access بتجاوز ZTNA لحركة مرور AVD.

تحليل تشخيصي

حدد التحليل المشترك لاستكشاف الأخطاء وإصلاحها أن تم تكوين ملف تعريف ZTNA بشكل صحيح، ولكن حركة مرور الوصول الآمن إلى جميع وجهات الإنترنت، وهو ما تسبب في خلل كبير لمستخدمي ZTA. وقد أدى هذا إلى عمليات إسقاط الجلسة لأن "سطح المكتب الظاهري Azure" يستخدم حركة WebSocket المستمرة للتوجيه AVD من خلال الشبكة للوصول الآمن. يعتمد السلوك على تدفق جلسات سطح المكتب في الوقت الفعلي، كما تم تصميم وكلاء السحابة لفحص صفحات الويب القياسية بدلا من معالجة بروتوكولات الدفق.

تغيير التكوين

تمت إضافة المجالات المرتبطة ب AVD من Microsoft إلى قائمة إستثناءات ZTA:

```
*.wvd.microsoft.com
*.core.windows.net
*.servicebus.windows.net
*.events.data.microsoft.com
```

بإضافة هذه المجالات إلى قائمة إستثناءات ZTA، تم توجيه عميل الوصول الآمن إلى تجاوز حركة مرور البيانات الخاصة ب AVD بالكامل. وهذا يسمح لحركة مرور AVD بالانتقال مباشرة إلى Microsoft، بتجاوز وكيل ZTNA بالكامل، وهذا هو بالضبط ما تتطلبه Microsoft لكي يعمل AVD بشكل صحيح.

التحقق من الصحة

بعد تطبيق تكوين إستثناءات ZTA، تم الإبلاغ عن اتصال AVD بأنه يعمل بشكل طبيعي. تمكن المستخدمون من الوصول بنجاح إلى أجهزة الكمبيوتر أثناء فترة المراقبة.

المكتبية الافتراضية الخاصة بهم من شبكة المكتب مع تمكين ميزة Secure Access.

السبب

كان السبب الجذري هو تكوين ملف تعريف ZTNA الذي اعترض حركة مرور البيانات المرتبطة بالإنترنت، بما في ذلك إتصالات Azure Virtual Desktop. عندما تم توجيه حركة مرور (Secure Access) للتفتيش، من خلال وكيل شبكة الوصول الآمن ب AVD الخاصة WebSocket تسببت في حالات قطع الاتصال لأن الوكيل لم يتم تصميمه للتعامل مع طبيعة الدفق المستمر لجلسات عمل AVD. يتطلب AVD اتصالا مباشرا بنقاط نهاية Microsoft للحفاظ على إستقرار جلسات تدفق سطح المكتب.

المحتوى ذي الصلة

- نقاط نهاية FQDN المطلوبة ل Microsoft Azure Virtual Desktop
- أستكشاف الأخطاء وإصلاحها وتجميع المعلومات الأساسية ل Cisco Secure Access
- الدعم الفني والتنزيلات من Cisco

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).