لشف إعادة تعيين كلمة مرور نظام التشغيل "pwrecovery" عملية مع CUMA

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
المشكلة
الحل 1
الحل 2
معلومات ذات صلة

المقدمة

تعد ميزة التنقل الموحد (CUMA) من Cisco جزءا من مجموعة منتجات الاتصالات الموحدة من Cisco. CUMA هو برنامج خادم تم نشره خلف جدار حماية المؤسسة الذي يربط هواتف الموظفين المحمولة بخوادم الدليل ونظام إتصالات IP وبرامج المجموعات وخوادم المؤتمرات، بالإضافة إلى موارد الشركة الأخرى. ويعمل هذا على زيادة إمكانات الاتصالات الحيوية للشركات إلى أجهزة الهاتف المحمولة، كما يتيح للجميع إمكانية الاتصال بشكل أكثر فعالية.

يقدم هذا المستند الإرشادات لاستكشاف أخطاء إسترداد كلمة المرور وإصلاحها في خادم ميزة التنقل الموحد من Cisco.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 7.1.2.3 من خادم CUMA.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

المشكلة

المشكلة هي أنه لا يمكنك تسجيل الدخول باستخدام SSH أو CLI، أو صفحة النظام الأساسي. تم تجربة إجراء إسترداد البيانات، ولكن لا يمكنك تسجيل الدخول إلى وحدة التحكم. إذا تم إدخال كلمة مرور غير مقبولة أثناء الاسترداد، فإن كلمة المرور غير قابلة للاستخدام. هناك ثلاثة أنواع على الأقل من كلمات المرور غير المقبولة أثناء إعادة تعيين كلمة المرور:

- كلمة المرور قصيرة جدا
- كلمات المرور غير متطابقة
- كلمة المرور في القاموس

ملاحظة: في حالة إستخدام أي من هذه الأنواع، يتم عرض خطأ. بعد ذلك إذا تم إدخال كلمة مرور صحيحة، فيبدو أنه قد تمت إعادة تعيين كلمة المرور. ومع ذلك، فإن كلمة المرور غير قابلة للاستخدام. لن تعمل أي محاولة لإجراء إسترداد كلمة المرور في هذه الحالة. لن تتمكن من تسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) للنظام الأساسي أو واجهة سطر الأوامر (CLI).

الحل 1

إذا كنت لا تتذكر كلمة مرور المسؤول، فإليك الإجراء لإعادة تعيينها. هناك طريقتان لإعادة ضبط كلمة المرور. الأول بدون إستخدام قرص إستعادة والآخر بقرص مضغوط.

1. قم بتسجيل الدخول إلى مربع لينوكس باستخدام الحساب الجذر (هذا مربع لينوكس قياسي).
2. تأكد من تشغيل هذه الخدمات:/sbin/service cuma_db start بدء sbin/service/ cuma_admin/sbin/service cuma_nm start
3. قم بتحرير الملف باستخدام محرر VI: **/opt/cuma/conf/admin/admin.xml**.
4. البحث عن هذا السطر:
```
<name>admin_password</name>

<value>{MD5}xxxxxxxxxxxxxxxxxxxxxxxxxxxx</value>
```
وتغييرها إلى:
```
<name>admin_password</name>

<value>{plain}new_password</value>
```
5. أستخدم هذا الأمر لإعادة تشغيل الخدمة:
```
sbin/service cuma_admin restart/
```
6. قم بتسجيل الدخول باستخدام "admin" و"new_password".

الحل 2

المشكلة هي أنه لا يمكنك إعادة ضبط كلمة مرور مسؤول OS عند إستخدام عملية **pwrecovery**. أتمت هذا steps in order to حللت الإصدار:

1. قم بتمهيد النظام باستخدام القرص المضغوط الخاص بالاسترداد (يوصى باستخدام الإصدار 7.1.2 أو إصدار أحدث).
2. تأكد من أنه يمكنه الكشف عن التثبيت (الذي تتم طباعته باستخدام القائمة الرئيسية لقرص الاسترداد المضغوط).
3. اضغط على **Alt+F2** للوصول إلى صدفة الجذر لقرص الاسترداد المضغوط.
4. يجب أن يكون القسم النشط على **/mnt/part1**. تأكد من أنه تم تحميله بشكل صحيح.
5. قم بتشغيل الأوامر الرئيسية **chroot /mnt/part1 rpm -q master** و**chroot /mnt/part2 rpm -q** للعثور على القسم النشط.
6. بعد تشغيل هذه الأوامر والعثور على إصدار العمل للخادم من النتائج المرتجعة، تحتاج إلى إستخدامه كقسم عامل.

7. أدخل القسم النشط بواسطة **chroot /mnt/part1**، إذا كان تثبيتا جديدا.
8. في حالة ترقية الخادم، أستخدم رقم الجزء المحدد هذا (**<chroot /mnt/part<no>**).
9. في الإصدارات السابقة، قم بتشغيل **root/.security/unimmunize.sh/** لإزالة وحدة بت ثابتة من **etc/password/**.
10. قم بتحرير **etc/password/** وتغيير **الجذر:x:0:0:root:/root:/sbin/nologin** إلى **الجذر:x:0:0:root:/bin/bash**، ثم احفظ التغييرات.
11. قم بتشغيل الأمر **password root** وأعط كلمة مرور في موجه الأمر، ثم قم بالتأكيد. سيكون لديك الآن الوصول الجذر عند التمهيد في القسم النشط.
12. اضغط على **Alt+F1** للحصول على قائمة قرص الاسترداد المضغوط الرئيسية وإدخال **Q** للإنهاء. بعد ذلك، قم بإخراج القرص.
13. اضغط على **Ctrl+Alt+Delete** لإعادة التمهيد.
14. بعد ذلك، يدخل **SSH** كجذر ويعين كلمة مرور مؤقتة لمسؤول نظام التشغيل باستخدام هذا الأمر: **password admin**، حيث يكون المسؤول اسم تسجيل دخول المستخدم لمسؤول نظام التشغيل الخاص بك.**ملاحظة:** هنا، يتم إستخدام كلمة المرور مؤقتا فقط. عليك أن تفعل ذلك مرة أخرى.
15. ابدأ تشغيل واجهة سطر الأوامر (CLI) باستخدام الأمر **su -admin**، حيث يكون المسؤول اسم تسجيل الدخول الخاص بمسؤول نظام التشغيل.
16. قم بتغيير كلمة المرور في قاعدة البيانات باستخدام أمر CLI الخاص **بتعيين كلمة المرور للمستخدم<*admin* *id*>**.
17. الخروج من واجهة سطر الأوامر.
18. قم بتعيين كلمة مرور نظام مسؤول OS لمطابقة كلمة مرور قاعدة البيانات مع هذا الأمر: **password admin**، حيث يكون admin هو اسم تسجيل الدخول لمسؤول OS.**ملاحظة:** يتم توثيق ذلك بواسطة معرف تصحيح الأخطاء من CSCtf25554 Cisco (للعملاء المسجلين فقط).

معلومات ذات صلة

- إستخدام معالج التكوين في ميزة التنقل الموحد من Cisco
- مشكلة شهادة خادم ميزة التنقل الموحد من Cisco مع ASA
- دعم تقنية الصوت
- دعم منتجات الاتصالات الصوتية والاتصالات الموحّدة
- استكشاف أخطاء خدمة IP الهاتفية من Cisco وإصلاحها
- 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).