Cloud Virtual Machine

소식 및 공지 사항

제품 문서

목록:

소식 및 공지 사항
릴리스 노트

최종 업데이트 날짜: : 2024-04-26 16:46:23

2024년 4월

업데이트 명칭	업데이트 설명	관련 문서
CVM은 정액 과금제를 지원	정액 과금제는 1개월 또는 몇개월, 몇년의 요금을 사전에 일시불로 결제하는 일종의 CVM 선불 방식으로, 가격이 종량제 과금 방식에 비해 더 저렴하고, 인스턴스가 만료되기 전에 사전 환불이 지원되지 않습니다.	과금 방식

공용 이미지 릴리스 노트

최종 업데이트 날짜: : 2024-03-22 15:26:12

주의 :

실제 이미지 업데이트 시간은 리전에 따라 다를 수 있습니다. 여기에 제공된 업데이트 날짜는 모든 Tencent Cloud 리전에서 이미지 업데이트가 완료된 시간입니다.

Tencent Cloud가 제공하는 공용 이미지 유지보수 주기는 공식 유지보수 주기와 같습니다. 자세한 내용은 Official Maintenance End Plans of Operating Systems을 참고하십시오.

OpenCloudOS

OpenCloudOS 업데이트 기록은 OpenCloudOS 이미지 업데이트 로그를 참고하십시오.

CentOS

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
CentOS Stream 9x86_64	이미지 ID: img-9xqekomx현재 커널 버전: 5.14.0-202.el9.x86_64	2022. 12. 19.	최신 시스템 패치 업데이트.
CentOS Stream 8x86_64	이미지 ID: img-8m9ugrip현재 커널 버전: 4.18.0-348.7.1.el8_5.x86_64	2022. 9. 16.	최신 시스템 패치 업데이트.
Centos 8.5x86_64	이미지 ID: img-es95t8wj현재 커널 버전: 4.18.0-348.7.1.el8_5.x86_64	2022. 11. 23.	최신 시스템 패치 업데이트.
CentOS 8.4x86_64	이미지 ID: img-l5eqiljn현재 커널 버전: 4.18.0-348.7.1.el8_5.x86_64	2022. 11. 7.	최신 시스템 패치 업데이트.
CentOS 8.3x86_64	이미지 ID: img-5w4qozfr현재 커널 버전: 4.18.0-348.7.1.el8_5.x86_64	2022. 11. 7.	최신 시스템 패치 업데이트.
CentOS 8.2x86_64	이미지 ID: img-n7nyt2d7현재 커널 버전: 4.18.0-348.7.1.el8_5.x86_64	2022. 8. 24.	최신 시스템 패치 업데이트.
CentOS 8.0x86_64	이미지 ID: img-25szkc8t현재 커널 버전: 4.18.0-348.7.1.el8_5.x86_64	2022. 3. 17.	최신 시스템 패치 업데이트.

CentOS 7.9x86_64	이미지 ID: img-l8og963d현재 커널 버전: 3.10.0-1160.71.1.el7.x86_64	2023. 3. 6.	최신 시스템 패치 업데이트.
CentOS 7.8x86_64	이미지 ID: img-3la7wgnt현재 커널 버전: 3.10.0-1160.62.1.el7.x86_64	2022. 4. 19.	최신 시스템 패치 업데이트.
CentOS 7.7x86_64	이미지 ID: img-1u6l2i9l현재 커널 버전: 3.10.0-1160.62.1.el7.x86_64	2022. 4. 22.	최신 시스템 패치 업데이트.
CentOS 7.6x86_64	이미지 ID: img-9qabwvbn현재 커널 버전: 3.10.0-1160.62.1.el7.x86_64	2022. 4. 28.	최신 시스템 패치 업데이트.
CentOS 7.5x86_64	이미지 ID: img-oikl1tzv현재 커널 버전: 3.10.0-1160.71.1.el7.x86_64	2022. 12. 2.	최신 시스템 패치 업데이트.
CentOS 7.4x86_64	이미지 ID: img-8toqc6s3현재 커널 버전: 3.10.0-1160.62.1.el7.x86_64	2022. 4. 19.	최신 시스템 패치 업데이트.
CentOS 7.3x86_64	이미지 ID: img-dkwyg6sr현재 커널 버전: 3.10.0-1160.62.1.el7.x86_64	2022. 4. 22.	최신 시스템 패치 업데이트.
CentOS 7.2x86_64	이미지 ID: img-31tjrtph현재 커널 버전: 3.10.0-1160.83.1.el7.x86_64	2023. 3. 6.	최신 시스템 패치 업데이트.
CentOS 6.10x86_64	이미지 ID: img-fizif873현재 커널 버전: 2.6.32-754.35.1.el6.x86_64	2022. 1. 17.	최신 시스템 패치 업데이트.
CentOS 6.9x86_64	이미지 ID: img-i5u2lkoz현재 커널 버전: 2.6.32-754.30.2.el6.x86_64	2022. 1. 18.	최신 시스템 패치 업데이트.

Ubuntu

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
Ubuntu 22.04x86_64	이미지 ID: img-487zeit5현재 커널 버전: 5.15.0-56-generic	2022. 12. 8.	최신 시스템 패치 업데이트.
Ubuntu 20.04x86_64	이미지 ID: img-22trbn9x현재 커널 버전: 5.4.0-126-generic	2022. 9. 20.	최신 시스템 패치 업데이트.
Ubuntu 18.04x86_64	이미지 ID: img-pi0ii46r현재 커널 버전: 4.15.0-193-generic	2022. 11. 3.	최신 시스템 패치 업데이트.

Ubuntu 16.04x86_64	이미지 ID: img-pyqx34y1현재 커널 버전: 4.4.0-210-generic	2022. 3. 21.	최신 시스템 패치 업데이트.

Debian

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
Debian 11.4x86_64	이미지 ID: img-btz2mndd현재 커널 버전: 5.10.0-16-amd64	2022. 9. 8.	최신 시스템 패치 업데이트.
Debian 11.1x86_64	이미지 ID: img-4cmp1f33현재 커널 버전: 5.10.0-19-amd64	2022. 11. 3.	최신 시스템 패치 업데이트.
Debian 10.12x86_64	이미지 ID: img-7ay90qj7현재 커널 버전: 4.19.0-21-amd64	2022. 9. 23.	최신 시스템 패치 업데이트.
Debian 10.11x86_64	이미지 ID: img-h1yvvfw1현재 커널 버전: 4.19.0-22-amd64	2022. 11. 1.	최신 시스템 패치 업데이트.
Debian 10.2x86_64	이미지 ID: img-qhtfjw1d현재 커널 버전: 4.19.0-19-amd64	2022. 11. 1.	최신 시스템 패치 업데이트.
Debian 9.13x86_64	이미지 ID: img-5k0ys7jp현재 커널 버전: 4.9.0-19-amd64	2022. 9. 30.	최신 시스템 패치 업데이트.
Debian 9.0x86_64	이미지 ID: img-6rrx0ymd현재 커널 버전: 4.9.0-19-amd64	2022. 11. 3.	최신 시스템 패치 업데이트.
Debian 8.11x86_64	이미지 ID: img-2lj11q1f 현재 커널 버전: 3.16.0-11-amd64	2022. 11. 7.	최신 시스템 패치 업데이트.

Red Hat Enterprise Linux

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용

Red Hat Enterprise Linux 8.5	이미지 ID: img-r5xber0b현재 커널 버전: 4.18.0-425.19.2.el8_7.x86_64	2023-04-27	최신 시스템 패치 업데이트.
Red Hat Enterprise Linux 7.9	이미지ID: img-0qhxz7dl현재 커널 버전: 3.10.0-1160.88.1.el7.x86_64	2023-04-27	최신 시스템 패치 업데이트.

설명：
CVM 구입 시 Red Hat Enterprise Linux 인증을 통과한 인스턴스 유형을 선택한 경우 Red Hat Enterprise Linux 이미지를 사용할 수 있습니다. 지원되는 이미지 태그 및 인스턴스 모델은 FAQs about Red Hat Enterprise Linux Image를 참고하십시오.

AlmaLinux

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
AlmaLinux 9.0x86_64	이미지 ID: img-f089mf4l현재 커널 버전: 5.14.0-70.13.1.el9_0.x86_64	2022. 10. 27.	이미지 릴리스.
AlmaLinux 8.6x86_64	이미지 ID: img-jy2bb29p현재 커널 버전: 4.18.0-372.19.1.el8_6.x86_64	2022. 10. 25.	최신 시스템 패치 업데이트.
AlmaLinux 8.5x86_64	이미지 ID: img-4ogcw28j현재 커널 버전: 4.18.0-348.20.1.el8_5.x86_64	2022. 9. 30.	최신 시스템 패치 업데이트.

Fedora

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
Fedora36x86_64	이미지 ID: img-ge141oql현재 커널 버전: 5.19.14-200.fc36.x86_64	2022. 11. 7.	최신 시스템 패치 업데이트.
Fedora 37x86_64	이미지 ID: img-d7j9x59z현재 커널 버전: 6.0.7-301.fc37.x86_64	2022. 11. 30.	이미지 릴리스.

FreeBSD

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
FreeBSD 13.1x86_64	이미지 ID: img-ng3lehjp현재 커널 버전: 13.1-RELEASE	2022. 9. 16.	최신 시스템 패치 업데이트.
FreeBSD 13.0x86_64	이미지 ID: img-1lkqxofp현재 커널 버전: 13.0-RELEASE	2022. 9. 2.	최신 시스템 패치 업데이트.
FreeBSD 12.3x86_64	이미지 ID: img-j9m732cx현재 커널 버전: 12.3-RELEAS	2022. 1. 20.	최신 시스템 패치 업데이트.
FreeBSD 12.2x86_64	이미지 ID: img-pi37fg9j현재 커널 버전: 12.2-RELEAS	2022. 1. 20.	최신 시스템 패치 업데이트.
FreeBSD 11.4x86_64	이미지 ID: img-aif2u6pf현재 커널 버전: 11.4-RELEASE	2022. 10. 27.	최신 시스템 패치 업데이트.

Rocky Linux

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
Rocky Linux 9.0x86_64	이미지 ID: img-k1g1wwy9현재 커널 버전: 5.14.0-70.13.1.el9_0.x86_64	2022. 11. 25.	이미지 릴리스.
Rocky Linux 8.6x86_64	이미지 ID: img-no575grb현재 커널 버전: 4.18.0-372.9.1.el8.x86_64	2022. 11. 25.	최신 시스템 패치 업데이트.
Rocky Linux 8.5x86_64	이미지 ID: img-qd4bf0jb현재 커널 버전: 4.18.0-348.20.1.el8_5.x86_64	2022. 10. 10.	최신 시스템 패치 업데이트.

OpenSUSE

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
OpenSUSE Leap 15.4	이미지 ID: img-aaa4d8d1현재 커널 버전: 5.14.21-150400.22-default	2022. 8. 31.	이미지 릴리스.
OpenSUSE Leap 15.3	이미지 ID: img-1e4uwwol현재 커널 버전: 5.3.18-59.27-default	2022. 11. 2.	최신 시스템 패치 업데이트.
OpenSUSE Leap 15.2	이미지 ID: img-i6u3kbtj현재 커널 버전: 5.3.18-lp152.106-default	2022. 1. 7.	최신 시스템 패치 업데이트.
OpenSUSE Leap 15.1	이미지 ID: img-4orfgj3l현재 커널 버전: 4.12.14-lp151.28.91-default	2021-12-21	최신 시스템 패치 업데이트.

Windows

이미지 태그	이미지 세부정보	마지막 업데이트 날짜	마지막 업데이트 내용
Windows Server 2022 데이터센터 버전의 64비트 중국어 버전	이미지 ID: img-9lw52tbx	2023. 1. 6.	최신 시스템 패치 업데이트.
Windows Server 2022 데이터센터 버전의 64비트 영어 버전	이미지 ID: img-cg67n3n9	2023. 1. 6.	최신 시스템 패치 업데이트.
Windows Server 2019 데이터센터 버전의 64비트 중국어 버전	이미지 ID: img-perxw61f	2023. 3. 9.	최신 시스템 패치 업데이트.
Windows Server 2019 데이터센터 버전의 64비트 영어 버전	이미지 ID: img-1dmc4wwp	2023. 3. 9.	최신 시스템 패치 업데이트.
Windows Server 2016 데이터센터 버전의 64비트 중국어 버전	이미지 ID: img-gu1nmb8d	2023. 3. 9.	최신 시스템 패치 업데이트.
Windows Server 2016 데이터센터 버전의 64비트 영어 버전	이미지 ID: img-6fp83vpb	2023. 3. 9.	최신 시스템 패치 업데이트.
Windows Server 2012 R2 데이터센터 버전의 64비트 중국어 버전	이미지 ID: img-ixj8o53x	2023. 1. 6.	최신 시스템 패치 업데이트.

Windows Server 2012 R2 데이터센터 버전의 64비트 영어 버전	이미지 ID: img-bpsjtw7n	2023. 1. 6.	최신 시스템 패치 업데이트.

공지
CentOS 8 유지보수 종료 공지

최종 업데이트 날짜: : 2023-08-07 09:59:43

CentOS는 공식적으로 CentOS Linux 프로젝트 유지 보수를 중단하고 2022년 01월 01일 CentOS 8 유지 보수 지원을 중단할 계획입니다. CentOS 7도 2024년 06월 30일에 유지 보수를 중단합니다. 자세한 사항은 CentOS 공식 발표를 참고하십시오.

관련 설명

Tencent Cloud는 CentOS 8 시리즈 이미지를 비활성화하지 않지만 CentOS 8 시리즈 이미지 및 OS 소프트웨어 버전 업데이트를 중지합니다. 비즈니스가 영향을 받지 않도록 Tencent Cloud는 사용자가 선택할 수 있는 다양한 이미지 버전을 제공합니다.

- TencentOS Server: 10년 이상 운영 체제 분야에서 Tencent의 기술을 축적했으며, 수년간 Tencent 내 대규모 비즈니스에 의해 검증 및 최적화 되었습니다. Tencent 내 운영 체제의 99% 이상을 차지하며, 모든 Tencent 비즈니스를 포괄합니다.
- OpenCloudOS: OpenCloudOS의 기본 라이브러리 및 사용자 상태 컴포넌트는 CentOS 8과 완벽하게 호환됩니다. 또한 커널 수준의 최적화 및 강화를 통해 1000만+노드의 대규모 검증을 거쳐 안정성이 70% 향상되고 특정 시나리오의 성능이 50% 향상되었습니다. 사용자에게 CentOS 8보다 더 나은 솔루션을 제공할 수 있습니다.
- CentOS Stream 버전 및 Ubuntu와 같은 기타 릴리스 버전

CentOS를 사용 중인 경우 해당 OpenCloudOS 또는 TencentOS Server 버전으로 최대한 빨리 마이그레이션하는 것이 좋습니다. 자세한 마이그레이션 작업은 CentOS를 TencentOS Server로 마이그레이션을 참고하십시오.

SUSE 프로 버전 이미지 지원 중단 공지

최종 업데이트 날짜: : 2022-05-07 16:03:45

Tencent Cloud는 2022년 1월 1일부터 SUSE 프로 버전 공용 이미지 및 해당 인증 서비스에 대한 새로운 지원 추가를 중단합니다. 버전은 다음과 같습니다.

- SUSE Linux Enterprise Server 12 SP3
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 10

공용 SUSE 이미지를 계속 사용하려는 기존 사용자는 SUSE 고객서비스에 연락하시기 바랍니다. SUSE 업체에서 해당 기술 지원을 제공할 것입니다. 연락처는 다음과 같습니다.

- 전화: +86-10-6533-9000
- 이메일: sales-inquiries-apac@suse.com

여러 가용존의 CVM 가격 인하 공지

최종 업데이트 날짜: : 2022-12-14 10:22:32

Tencent Cloud CVM은 2021년 3월 10일부터 일부 서비스 가격을 인하합니다. 중국 내 주요 리전, 가용존 및 온라인에서 90%가 넘는 인스턴스 유형에 적용됩니다. 구체적인 인하율은 가용존과 인스턴스 사양에 따라 다르며, 최대 인하율은 10%입니다.

커버 범위	설명
가용존	광저우 6존, 베이징 6존, 난징 1존, 난징 2존, 난징 3존
인스턴스 유형	표준형 S5, 표준형 SA2, 표준형 S4, 표준 스토리지 확장형 S5se, 메모리형 M5, 컴퓨팅형 C5, 컴퓨팅형 C4, 빅 데이터형 D3, 빅 데이터형 D2, 고성능 I/O IT5, 고성능 I/O IT3

조정 상세 내용

- 2021년 3월 10일부터 최신 가격이 적용됩니다. 본 문서는 가격 조정에 대한 안내입니다. 구체적인 가격은 공식 홈페이지 가격 센터, 구매 페이지, 가격 계산기의 최신 가격 기준입니다.
- 2021년 3월 10일 이후 가격 인하되는, 종량제 CVM을 **구매/연장**하면 혜택가가 적용됩니다.

설명 사항

- 이번 가격 인하에는 CVM 인스턴스 사양 관련 연산 능력 리소스 요금만 포함되며, 네트워크 및 클라우드 디스크 요금은 포함되지 않습니다.
- 본 공지는 2021년 3월 10일부터 다음 CVM 가격 조정 전까지 적용됩니다.
- CVM의 최신 가격은 가격 센터에서 조회할 수 있으며, 클라우드 디스크와 네트워크 과금에 대한 상세 가격은 CVM 가격 계산기에서 추산해볼 수 있습니다.
- CVM 인스턴스 유형 관련 정보에 대한 자세한 내용은 인스턴스 사양에서 확인할 수 있습니다.

관련 문제

현재 계정에 종량제 CVM이 있습니다. 2021년 3월 10일부터 최신 혜택가로 적용되나요?

그렇습니다. 종량제 CVM은 시간제 요금이므로, 계정에 이미 종량제 CVM이 있는 경우 공식 홈페이지에서 새로운 가격을 정식으로 공지한 1시간 후부터 혜택가로 청구서에 적용됩니다. 가격 공지 시간은 공식 홈페이지 및 청구서 적용

시간 기준입니다.

이벤트로 구매한 CVM도 혜택가로 적용되나요?

다른 이벤트를 통해 구매한 CVM은 별도의 혜택이 적용되므로 가격 인하가 적용되지 않습니다. CVM 구매 페이지나 API를 통해 구매한 인스턴스만 가격 인하가 적용되며, 이벤트 등 다른 경로를 통해 구매한 CVM은 적용되지 않습니다.

고객센터

- 기타 궁금한 점이 있으시면 고객센터를 통해 문의 바랍니다. 오랫동안 Tencent Cloud를 이용해주셔서 감사드리며, 앞으로도 다양한 제품을 효율적인 비용으로 제공하도록 노력하겠습니다.

OrcaTerm 프록시 IP 주소 변경 공지

최종 업데이트 날짜: : 2023-07-07 15:34:55

배경 정보

Orcaterm 서버 용량 확장 및 업데이트로 인해 2021년 4월 1일부터 orcaterm 프록시 IP 주소에 신규 IP 대역이 추가됩니다. 보안 그룹에서 새로 추가된 orcaterm 프록시 IP 대역 및 원격 로그인 포트(기본값: 22 포트)를 개방할 수 있습니다.

> 설명 :
> Orcaterm 로그인 방식은 표준 로그인 방식을 사용한 Linux 인스턴스 로그인(권장)을 참조하십시오.

조정 상세 내용

- 신규 프록시 IP 대역은 다음과 같습니다.

81.69.102.0/24
106.55.203.0/24
101.33.121.0/24
101.32.250.0/24

- 신규 및 기존 프록시 IP 주소/대역은 병행 사용됩니다. 아래 IP 주소/대역이 포함됩니다.

> 설명 :
> 인스턴스가 orcaterm에 정상적으로 로그인할 수 있도록 보안 그룹의 소스(인바운드)인 신규 및 기존 프록시 IP 대역 및 원격 로그인 포트를 개방하십시오.

81.69.102.0/24
106.55.203.0/24
101.33.121.0/24
101.32.250.0/24
115.159.198.247
115.159.211.178

119.28.7.195
119.28.22.215
119.29.96.147
211.159.185.38

관련 작업

- 표준 방식으로 Linux 인스턴스 로그인(권장)
- 보안 그룹 규칙 추가

실리콘밸리 리전 표준형 S3의 가격 변동에 대한 공지

최종 업데이트 날짜: : 2020-08-25 14:24:51

Tencent Cloud 실리콘밸리 리전 **표준형 S3**의 종량제 가격 변동:

운영 체제	하락 폭
Linux	종량제 모두 21% 하락
Windows	종량제 모두 10% 하락

설명 사항

- 조정 후의 가격은 2020년 7월 24일부터 적용됩니다.
- 본 문서는 가격 조정에 대한 안내입니다. 구체적인 가격은 CVM 가격 계산기를 통해 계산 바랍니다.
- 기타 궁금한 점이 있으시면 영업 지원을 통해 문의 바랍니다.

Tencent Cloud 미러 상시 허점 복구 정책 공지

최종 업데이트 날짜: : 2020-05-19 15:03:02

Tencent Cloud 보안 센터는 각종 보안 취약점에 즉각 대응합니다. 공식 홈페이지에서 중요 보안 취약점을 배포하면, Tencent Cloud 보안 센터가 취약점을 즉시 추적하여 사용자에게 취약점 정보를 전송하고 취약점 복구 솔루션을 제공합니다.

Tencent Cloud의 공식 이미지 복구 주기

- 취약점 정기 복구: Tencent Cloud의 공식 이미지는 취약점 정기 복구를 매년 2회씩 진행합니다.
- 고위험 취약점 복구: Tencent Cloud는 고위험 취약점에 대해 긴급 복구를 진행하며 고객에게 신속한 서비스를 제공합니다.

취약점 복구에 포함되는 이미지 범위

이미지의 보안에 있어 Tencent Cloud와 업스트림 이미지 공식 릴리스 버전의 점검 원칙이 일치하므로, 공식 점검 주기에 해당하는 시스템 버전의 보안 점검을 진행합니다.

CentOS

CentOS 공식 홈페이지는 현재 배포된 메이저 버전의 최신 마이너 버전 점검 소프트웨어 및 취약점만 업데이트하며, Tencent Cloud와 CentOS 공식 홈페이지의 점검 원칙이 일치합니다. 따라서 공식 점검 주기에 해당하는 각 메이저 버전의 최신 마이너 버전에 대해 정기적인 취약점 복구 및 고위험 취약점 긴급 복구를 진행합니다.

Tencent Cloud의 기존 CentOS 버전 이미지 점검 설명:

- CentOS 7.6 64비트 (CentOS 공식 홈페이지에서 지원 유지)
- CentOS 7.5 64비트 (CentOS 공식 홈페이지에서 지원 유지)
- CentOS 7.4 64비트 (CentOS 공식 홈페이지에서 지원 유지)
- CentOS 7.3 64비트 (CentOS 공식 홈페이지에서 지원 유지)
- CentOS 7.2 64비트 (CentOS 공식 홈페이지에서 지원 유지)
- CentOS 7.1 64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 7.0 64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 6.9 32/64비트 (CentOS 공식 홈페이지에서 다음 버전 배포까지 지원합니다)
- CentOS 6.8 32/64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 6.7 32/64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 6.6 32/64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 6.5 32/64비트 (CentOS 공식 홈페이지에서 지원 중단)

- CentOS 6.4 32/64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 6.3 32/64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 6.2 64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 5.11 32/64비트 (CentOS 공식 홈페이지에서 지원 중단)
- CentOS 5.8 32/64비트 (CentOS 공식 홈페이지에서 지원 중단)

Ubuntu

Ubuntu 공식 홈페이지는 LTS 버전 시스템의 소프트웨어와 취약점을 장기적으로 업데이트 및 점검하며, 각 LTS 시스템의 서버 버전의 경우 5년 동안 업데이트가 유지됩니다. Tencent Cloud 운영사는 각 LTS 버전의 서버 시스템을 제공하며, Ubuntu의 공식 배포와 일치하므로 점검 주기에 해당하는 이미지의 취약점 업데이트 및 고위험 취약점 긴급 복구를 진행합니다.

Tencent Cloud의 기존 Ubuntu 버전 이미지 점검 설명:

- Ubuntu 18.04 LTS 64비트 (Ubuntu 공식 홈페이지에서 점검 지원)
- Ubuntu 16.04 LTS 64비트 (Ubuntu 공식 홈페이지에서 점검 지원)
- Ubuntu 14.04 LTS 32/64비트 (Ubuntu 공식 홈페이지에서 점검 지원)
- Ubuntu 12.04 LTS 64비트 (Ubuntu 공식 홈페이지에서 점검 중단)
- Ubuntu 10.04 LTS 32/64비트 (Ubuntu 공식 홈페이지에서 점검 중단)

Debian

Debian 공식 홈페이지는 stable과 oldstable 두 가지의 주요 branch 시스템을 점검합니다. stable은 현재의 안정 버전이고 oldstable은 옛 안정 버전입니다. Debian 공식 홈페이지는 stable 시스템의 소프트웨어 점검과 취약점 업데이트를 진행하고, oldstable은 자원 봉사 및 커뮤니티에서 제공하는 장기 지원(Long Term Support, LTS)로 점검합니다. Tencent Cloud와 업스트림 공식 점검 정책이 일치하므로 Debian 공식 홈페이지에서 점검하는 stable branch 시스템의 취약점을 정기적으로 복구합니다.

Tencent Cloud의 기존 Debian 버전 이미지 점검 설명:

- Debian 9.0 64비트 (Debian 공식 홈페이지에서 점검 지원)
- Debian 8.2 32/64비트 (2019년 6월 점검 중단 예정)
- Debian 7.8 32/64비트 (Debian 공식 홈페이지에서 점검 중단함)
- Debian 7.4 64비트 (Debian 공식 홈페이지에서 점검 중단함)

openSUSE

Tencent Cloud는 openSUSE 시스템의 라이프사이클에 따라, 공식 홈페이지에서 지원하는 시스템의 이미지 취약점을 정기적으로 복구합니다.

Tencent Cloud의 기존 openSUSE 버전 이미지 점검 설명:

- openSUSE 42.3 openSUSE 공식 홈페이지에서 점검 지원)

- openSUSE 13.2 openSUSE 공식 홈페이지에서 점검 중단함)
- openSUSE 12.3 32/64비트 openSUSE 공식 홈페이지에서 점검 중단함)

FreeBSD

FreeBSD 11.0-RELEASE 이후, FreeBSD는 stable branch에 5년의 점검 주기를 제공하며, 11.0-RELEASE 이전 버전은 유형에 따라 점검 주기가 제공됩니다. 또한, Tencent Cloud와 FreeBSD 와 공식 홈페이지의 점검 원칙이 일치합니다.

Tencent Cloud의 기존 FreeBSD 버전 이미지 점검 설명:

- FreeBSD 11.1 64비트 (FreeBSD 공식 홈페이지에서 점검 지원)
- FreeBSD 10.1 64비트 (FreeBSD 공식 홈페이지에서 점검 중단함)

비즈니스 버전 시스템

Tencent Cloud는 비즈니스 버전 시스템의 취약점 업데이트 및 점검을 지원하지 않습니다.

Ubuntu10.04 미러 이미지 비활성화 및 인벤토리 소프트웨어 소스 구성에 관한 공지

최종 업데이트 날짜: : 2020-04-16 15:33:41

Ubuntu에서 Ubuntu 10.04 LTS의 점검을 종료하여, 더불어 Tencent Cloud에서도 Ubuntu 10.04버전의 공용 이미지 운영을 정지하였습니다.

최근 공식 리소스 웨어하우스에서 Ubuntu10.04 LTS 관련 디렉터리 트리가 삭제되었습니다. Tencent Cloud의 소프트웨어 웨어하우스는 공식 데이터와 일치하므로, 아울러 공식 소스 디렉터리 트리에서도 Ubuntu 10.04 LTS 에 대해 더는 지원하지 않으니 미러 이미지를 더 높은 버전으로 교체해 주시기 바랍니다.

인벤토리 사용자가 Ubuntu 10.04의 소프트웨어 소스를 계속 사용하려면 다음과 같은 2가지 방법이 있습니다.

방법1: 환경 설정 파일을 수동 업데이트

사용자의 사용 퀄리티를 높이기 위해 Tencent Cloud의 소프트웨어 웨어하우스에서는 Ubuntu 10.04 LTS의 공식 보관 소스 `http://old-releases.ubuntu.com/ubuntu/` 를 불러와 사용자에게 제공하고 있으며, 사용자는 환경 설정 파일을 수동으로 수정하여 해당 웨어하우스를 정상적으로 사용할 수 있습니다.

apt원본 설정 파일 'vi /etc/apt/sources.list' 를 열고 아래의 코드를 수정합니다.

```
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted u
niverse multiverse
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main rest
ricted universe multiverse
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main res
tricted universe multiverse
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main re
stricted universe multiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted unive
rse multiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main restrict
ed universe multiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restric
ted universe multiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main restri
cted universe multiverse
```

방법2: 오토 스크립트 실행

Tencent Cloud에서 제공하는 스크립트 old-archive.run 를 통해 설정하고 해당 파일을 Ubuntu 10.04 CVM 내부에 다운로드한 다음, 아래의 명령어를 실행합니다.

```
chmod +x old-archive.run
./old-archive.run
```

Ubuntu14.04에서 Tomcat 작동 불가 솔루션에 대해

최종 업데이트 날짜: : 2023-03-28 09:47:01

고객님께:
안녕하세요. 고객님께서 Tencent Cloud 공식 홈페이지에서 Ubuntu14.04 CVM apt-get을 구매하여 Tomcat 및 Hadoop을 설치할 때 정상적으로 포트를 리슨할 수는 있지만, 요청에는 무응답인 것으로 감지되었습니다. Tecent Cloud에서 관련 해결 조치를 제안해드리오니, 이와 같은 상황이 발생하면 해당 조치에 따라 문제를 해결하시기 바랍니다.

문제 원인

Java Runtime Environment의 기존 문제에 의해 발생했습니다.

문제 분석

Tomcat 및 Hadoop은 Java로 개발되어 java.security.SecureRandom API를 사용했습니다.
해당 API는 JRE에서 `/dev/random` 을 사용하여 생성되도록 기본 설정되어 있는데, `/dev/random` 은 CPU 온도, 키보드 등 하드웨어 노이즈에 따라 엔트로피를 생성합니다. CVM은 가상화 기술이 적용된 환경이므로 CPU 온도와 같은 신호를 감지하기 어려워 엔트로피를 생성할 수 없습니다. 따라서 `cat /dev/random` 이 대부분 차단되어 Tomcat 및 Hadoop을 실행할 수 없게 됩니다.

해결 조치

JRE 설정 변경

기존 `/etc/java-7-openjdk/security/java.security` (URL은 실제 상황에 따라 다름) 중의 `securerandom.source=file:/dev/urandom` 을 `securerandom.source=file:/dev/./urandom` 으로 변경하면 위와 같은 문제를 해결할 수 있습니다.

Windows CVM Virtio 랜카드 드라이브를 업그레이드할데 대한 공지

최종 업데이트 날짜: : 2020-01-02 16:43:31

2016년 6월부터 8월 중순에 생성된 Windows CVM의 극단적인 상황 시 나타나는 네트워크 끊김 문제와 정상 서비스 운행에 영향을 주는 상황을 방지하기 위해, Virtio ENI 드라이버 업그레이드 프로그램을 제공합니다. 업그레이드 제안에 따라 프로그램을 설치하길 권장합니다. 재시작 후 해당 문제는 즉시 해결됩니다.

Tencent Cloud 사용자는 다음 개인 네트워크 주소를 통해 업그레이드 프로그램을 다운로드한 뒤, 원클릭으로 업그레이드가 완료됩니다. 사용자는 Windows CVM 로그인해야 하며, 내부의 미러 이미지 사이트 'http://mirrors.tencentyun.com/install/windows/update_netkvm.exe'로 액세스한 뒤 다운로드 후 직접 업그레이드 프로그램을 실행하거나 저장 후 실행할 수 있습니다.

다음의 정보가 표시되는 경우: 드라이버의 업그레이드가 성공했으며, 시스템 재시작 후 새 드라이버가 작동되는 것을 나타냅니다.
다음의 정보가 표시되는 경우: 기존 드라이버에 문제가 없으며, 업그레이드가 필요하지 않다는 것을 나타냅니다.

보안 그룹 53 포트 설정 관련 공지

최종 업데이트 날짜: : 2022-04-25 19:02:02

개요

53 포트는 DNS(Domain Name Server, 도메인 네임 서버) 서버를 위해 오픈되어 주로 도메인 이름의 리졸브에 사용되며, DNS 서버를 통해 도메인 이름을 IP 주소로 전환하여 도메인만 기억해도 웹 사이트에 빠르게 액세스할 수 있습니다.

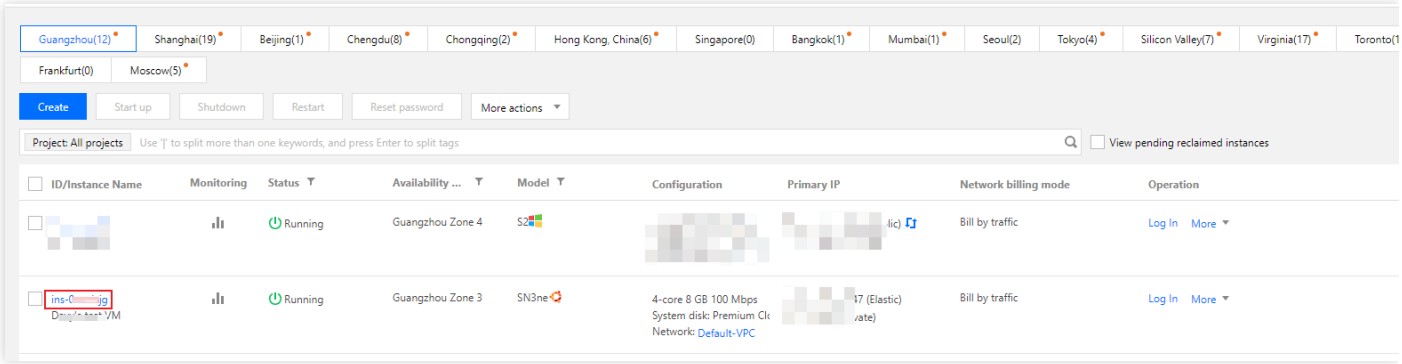
<통신 비즈니스 분류 목록>(2015 버전)부터 인터넷 도메인 재귀적 리졸브 서비스가 통신 비즈니스(코드번호 B26-1)에 포함되었습니다. 즉 도메인 재귀적 서비스에 종사하려면 해당 비즈니스 종류의 부가 통신 비즈니스 라이선스를 취득해야 합니다.

관련 정책 법규 요구 사항

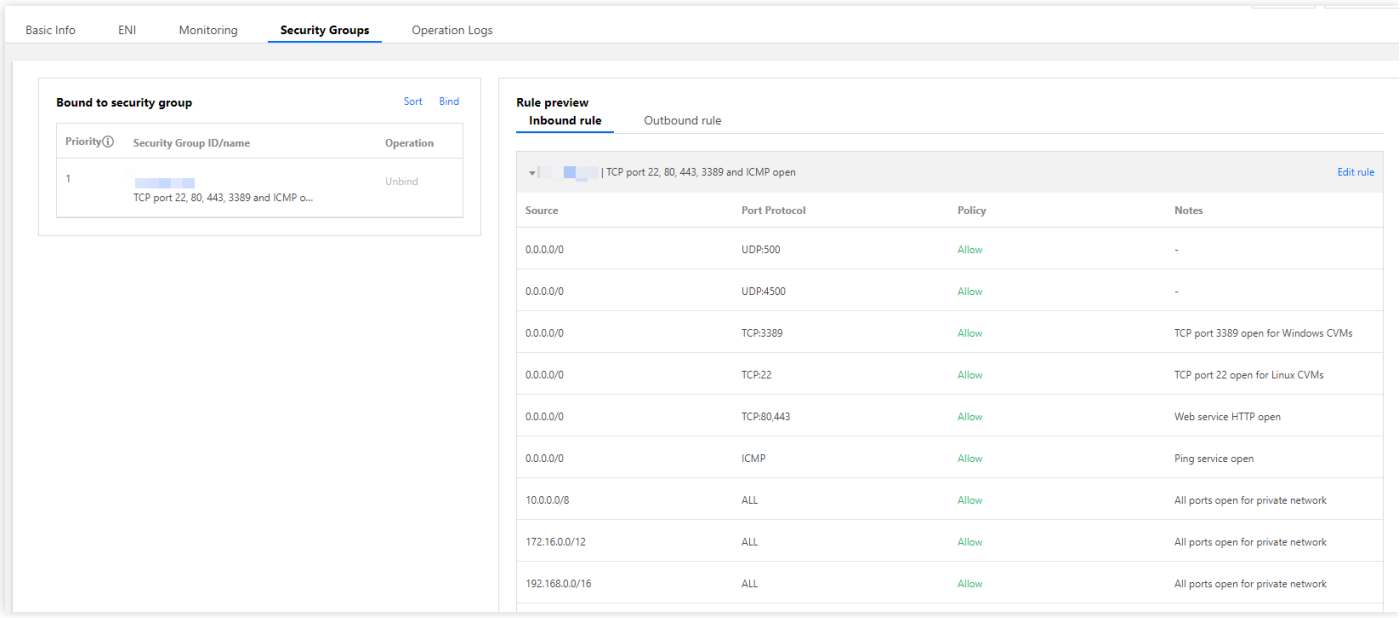
1. 경영 허가증 취득 없이 인터넷 도메인 이름 리졸브 서비스 비즈니스에 종사할 수 없습니다.
귀사(귀하)가 이와 같은 비즈니스에 연관될 경우, "코딩 및 규정 전환 비즈니스 허가증"을 취득해야 하며 자세한 취득 방법은 귀하가 소재한 성 통신관리국에 문의하시기 바랍니다.
<통신 비즈니스 경영 허가 관리 방법> 제46조: **본 방법 제16조 제1항, 제28조 제1항 규정을 위반하여 통신 비즈니스를 무단으로 경영하거나 범위를 벗어나 통신 비즈니스를 경영할 경우, <중화인민공화국 통신조례> 제69조 규정에 근거하여 처벌하고, 그중 상황의 심각성에 따라 영업정지 및 정리 처벌을 받을 경우, 즉시 통신 비즈니스 경영 신용 상실 명단에 추가됩니다.
****중국 공업정보화부 <인터넷 도메인 관리 방법> 제36조: **도메인 이름 리졸브 서비스를 제공하려면 관련 법률, 법규 및 표준을 따라야 하고, 관련 기술, 서비스 및 네트워크와 정보 보안 능력을 갖춰 네트워크와 정보의 보안을 보장해야 합니다. 또한, 법에 따라 도메인 이름 리졸브 로그, 유지 보수 로그 및 변경 이력을 기록 및 보존하여 확인 서비스 퀄리티와 확인 시스템 보안을 보장해야 합니다. 통신 비즈니스 경영에 연관될 경우, 법에 따라 통신 비즈니스 경영 라이선스를 취득해야 합니다.**
****2. Tencent Cloud는 법에 따라 경영 허가증을 취득하지 않았거나 비영리성 인터넷 정보 서비스 ICP비안 등록을 하지 않은 업체 또는 개인에게 액세스 또는 과금 대행 등 서비스를 제공할 수 없습니다.**
<통신 비즈니스 경영 허가 관리 방법>: 제24조 액세스 서비스를 제공하는 부가 통신 비즈니스 경영자는 다음의 규정을 따라야 합니다.(3) 법에 따라 경영 허가증을 취득하지 않았거나 비영리성 인터넷 정보 서비스 ICP비안 등록을 하지 않은 업체 또는 개인에게 액세스 또는 과금 대행 등 서비스를 제공할 수 없습니다.
귀하(귀사)가 **인터넷 도메인 이름 리졸브 서비스 비즈니스**에 연관되지 않은 경우, 서버의 보안 그룹 정책을 조정하고 인바운드 규칙의 53 포트를 차단할 것을 권장합니다.

인바운드 규칙 53 포트를 비활성화하는 작업 순서

1. Tencent Cloud CVM 콘솔에 로그인합니다.
2. 인스턴스의 관리 페이지에서 53 포트를 차단할 예정인 인스턴스를 선택하고 해당 인스턴스의 "ID/인스턴스 이름"을 클릭합니다. 아래 이미지 참조

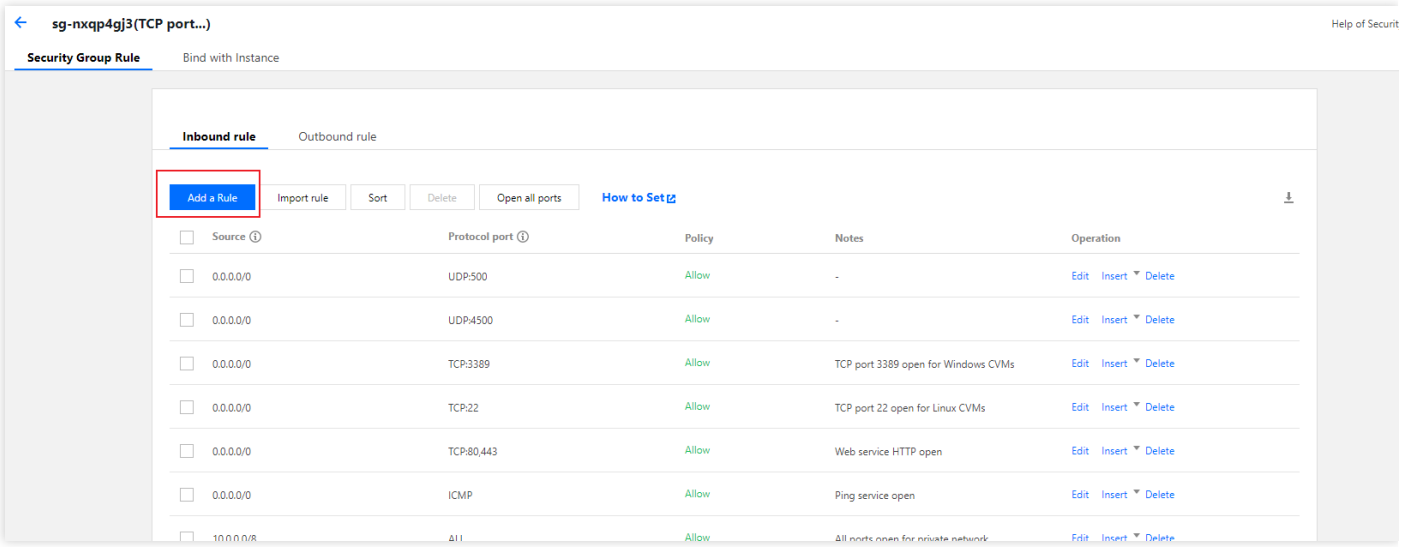


3. 인스턴스의 상세 페이지에서 [Security Group] 탭을 선택하여 해당 인스턴스의 보안 그룹 관리 페이지에 접속합니다. 아래 이미지 참조

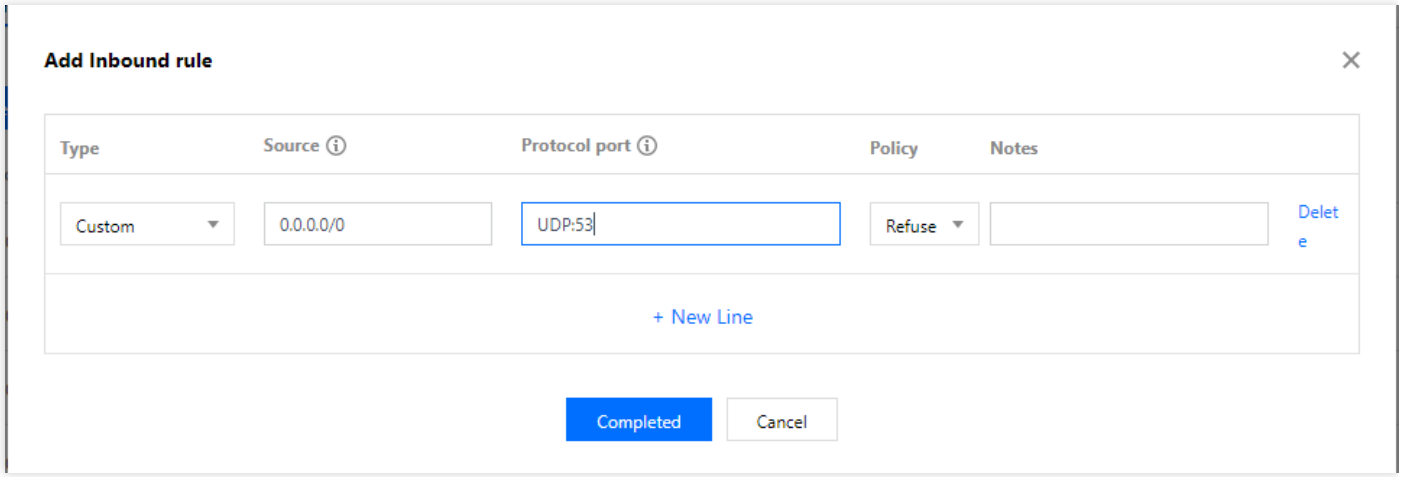


4. [바인딩 완료한 보안 그룹] 창에서 수정 예정인 인바운드 규칙의 "보안 그룹 ID/이름"을 선택합니다.

5. "보안 그룹 규칙" 페이지에서 [Inbound rule]을 선택하고 [Add a Rule]를 클릭합니다. 아래 이미지 참조



6. 팝업된 "인바운드 규칙 추가" 창에서 아래의 정보를 입력합니다. 아래 이미지 참조



- 유형: "사용자 정의"를 선택합니다.
- 소스: "0.0.0.0/0"을 입력합니다.
- 프로토콜 포트: "UDP:53"을 입력합니다.
- 정책: "거부를 선택합니다.

7. [Completed]를 클릭하면 바로 53 포트를 차단화할 수 있습니다.

FAQ

인터넷 도메인 이름 리졸브 서비스란?

인터넷 도메인 이름 리졸브은 인터넷 도메인과 IP 주소의 상호 대응 관계를 구현하는 과정입니다.
인터넷 도메인 이름 리졸브 서비스 비즈니스는 인터넷상에 도메인 이름 리졸브 서버와 상응하는 프로그램을 구축함으로써 인터넷 도메인과 IP 주소를 서로 전환하는 서비스를 가리킵니다. 도메인 이름 리졸브 서비스엔 권한 서비스와 재귀적 서비스 두 가지가 포함됩니다.

- 권한 확인: 루트 도메인, 최상위 도메인 및 기타 각 레벨 도메인을 위해 도메인 이름 리졸브을 제공하는 서비스를 가리킵니다.
- 재귀적 확인: 로컬 캐시 조회 또는 권한 확인 서비스 시스템을 통해 도메인과 IP 주소 간 대응 관계를 구현하는 서비스를 가리킵니다.

여기에서 인터넷 도메인 이름 리졸브 서비스는 재귀적 확인 서비스를 가리킵니다. 더 자세한 내용은 <통신 비즈니스 분류 목록(2015년 버전)>: B26-1 인터넷 도메인 이름 리졸브 서비스 비즈니스를 참조 바랍니다.

인바운드 규칙에서 53 포트를 차단하면 사용자의 서버에 어떤 영향을 미칩니까?

사용자가 인터넷 도메인 이름 리졸브 서비스 비즈니스를 진행하지 않은 경우, 인바운드 규칙 53 포트를 차단해도 사용자의 서버, 비즈니스에 영향을 미치지 않습니다.

개인이 인터넷 도메인 이름 리졸브 서비스 비즈니스에 종사할 수 있습니까?

통신 비즈니스 경영자는 합법적으로 설립된 회사여야 하고, 개인은 해당 비즈니스에 종사할 수 없습니다. 사용자는 회사의 명의로 "코딩 및 규정 전환 비즈니스 허가증"을 취득해야만 인터넷 도메인 이름 리졸브 서비스 비즈니스를 시작할 수 있습니다. 허가증의 자세한 취득 방법은 귀하가 소재한 성 통신관리국에 문의할 수 있습니다.

관련 허가증을 취득하지 않은 채 인터넷 도메인 이름 리졸브 서비스 비즈니스를 시작할 경우 어떤 영향이 있습니까?

<중화인민공화국 통신조례> 제69조: (1) 본 조례 제7조 제3항의 규정을 위반하거나 본 조례 제58조 제(1)항에서 나열한 행위를 한 경우, 무단으로 통신 비즈니스를 경영한 경우 또는 범위를 벗어나 통신 비즈니스를 경영한 경우, 국무원 정보산업 주관부서 또는 성, 자치구, 직할시 통신관리기관은 직권에 의해 시정을 명령하고 불법소득을 몰수하며 불법소득의 3배 이상 5배 이하의 과태료를 부과합니다. 불법소득이 없거나 불법소득이 5만 위안 이하일 경우, 10만 위안 이상 100만 위안 이하의 과태료를 부과합니다. 상황이 심각한 경우, 영업정지 및 정리를 명령합니다.

Windows Server 2003 시스템 미러를 지원 불가한데 대한 공지

최종 업데이트 날짜: : 2020-01-02 16:43:05

사용 설명

Microsoft는 2015년 7월 14일 Windows Server 2003 및 Windows Server 2003 R2에 대한 확장 지원 서비스를 공식적으로 중지했습니다. 동시에 Windows Server 2003 시스템의 Tencent CVM 또한 이 날짜 이후에 Microsoft의 업데이트 및 패치를 얻을 수 없게 되며 프로그램 호환성, 불안정성, 보안 등의 문제와 위험에 직면하게 되었습니다.
안정적인 보안 서비스를 보장하기 위해, 기존의 Windows Server 2003의 CVM을 Windows Server 2008 R2 및 Windows Server 2012 등의 보다 높은 버전으으로 마이그레이션하는 것을 권장합니다.

위험 알림

Microsoft에서 Windows Server 2003의 업데이트 및 패치 프로그램을 가져올 수 없기 때문에, Tencent Cloud는 운영 체제의 문제를 해결할 수 없습니다. 만약 Windows Server 2003 사용을 계속 유지할 경우, 다음 위험이 발생할 수 있습니다.

1. 2015년 7월 14일 이후 Windows Server 2003 운영 체제의 Tencent CVM을 계속 사용할 경우, Microsoft 제공의 업데이트 및 패치를 얻지 못합니다. 동시에 애플리케이션과 서비스가 각종 위험에 직면할 수 있으며, 보안 문제에 국한하지 않고 애플리케이션 비호환, 요청 불이행 및 기타 비기능성 문제로 확인할 수 없는 보안 위험을 일으킬 수 있습니다.
2. 2015년 7월 14일 이후에도 Windows Server 2003의 Tencent CVM을 계속 사용할 경우, Microsoft의 지원 결여로 인한 운영 체제의 장애, 보안 문제, 비호환성 또는 확인 불가능한 위험성이 높아지는 것에 대해 Tencent Cloud는 책임지지 않습니다. 상응하는 위험의 결과 및 책임은 스스로 부담해야 합니다.

서비스 공지

Microsoft에서 Windows Server 2003의 업데이트 및 패치를 가져올 수 없기 때문에, Tencent Cloud는 관련 운영 체제의 문제를 해결할 수 없습니다. 아래의 상황은 Tencent Cloud 서비스의 품질 미달, 장애 혹은 책임에 속하지 않습니다.

1. Windows Server 2003 인스턴스는 장애 위험이 높아지고, 각종 보안 문제가 생기며 비호환성 상황이 발생하거나 정상적인 작동히 불가해 완전히 마비될 수 있습니다.
2. Windows Server 2003 인스턴스에서 실행 중인 애플리케이션에 장애가 발생해 Microsoft의 패치 설치가 필요하거나 Microsoft가 제공하는 운영 체제급의 지원이 있어야만 장애가 제거될 수 있을 경우, Tencent는 장애 해결에 대한

협조를 제공합니다. 하지만 완전한 문제 해결 방안은 제공하지 못할 수 있습니다.

3. 하드드웨어 호환성 및 드라이버 프로그램 관련 문제에 대해 제한을 받습니다. 새로운 Tencent CVM은 조만간 Windows 2003 미러 이미지의 운영을 지원하지 않을 수 있습니다.

Windows Server 2008 R2 기업용 SP1 64비트 시스템 이미지 지원 중단에 관한 공지

최종 업데이트 날짜: : 2023-02-01 10:21:53

사용 설명

Microsoft는 2020년 1월 14일부터 Windows Server 2008에 대한 지원을 공식적으로 종료했기 때문에 Tencent Cloud도 2020년 3월 16일에 Windows Server 2008 R2 엔터프라이즈 버전 SP1 64비트 공개 이미지를 비활성화했습니다. 이 이미지를 사용하는 Tencent Cloud CVM은 더 이상 Microsoft로부터 보안 업데이트 및 패치를 받을 수 없으며 프로그램 호환성, 안정성 및 보안 위험에 노출될 수 있습니다.

비즈니스의 보안과 안정성을 보장하기 위해 Windows Server 2008 R2 엔터프라이즈 버전 CVM 인스턴스를 최신 버전의 Windows Server로 마이그레이션하는 것이 좋습니다.

리스크 안내를 충분히 이해하고 이에 동의하는 경우 사용자 정의 이미지를 가져와서 Windows Server 2008 R2 엔터프라이즈 버전을 사용하여 인스턴스를 생성하거나 다시 설치할 수 있습니다.

위험 알림

Microsoft는 더 이상 보안 업데이트 및 패치를 제공하지 않기 때문에 운영 체제 문제를 해결할 수 없습니다. Windows Server 2008 R2 엔터프라이즈 버전 SP1 64비트 운영 체제를 계속 사용할 경우 다음 위험에 유의하십시오.

1. 2020년 3월 16일 이후 Windows Server 2008 R2 엔터프라이즈 버전 SP1 64비트 운영 체제를 사용하는 Tencent Cloud CVM은 더 이상 Microsoft로부터 업데이트 및 패치를 받을 수 없습니다. 이 운영 체제를 계속 사용하면 애플리케이션과 비즈니스가 애플리케이션 비호환성, 비준수 및 비기능적 보안 문제를 포함하되 이에 국한되지 않는 다양한 위험에 노출될 수 있습니다.
2. 2020년 3월 16일 이후에도 Windows Server 2008의 Tencent CVM을 계속 사용할 경우, Microsoft의 지원 결여로 인한 운영 체제의 장애, 보안 문제, 비호환성 또는 확인 불가능한 위험성이 높아지는 것에 대해 Tencent Cloud는 책임지지 않습니다. 상응하는 위험의 결과 및 책임은 스스로 부담해야 합니다.

서비스 공지

Microsoft는 더 이상 Windows Server 2008에 대한 보안 업데이트 및 패치를 제공하지 않기 때문에 Tencent Cloud는 운영 체제 문제를 해결할 수 없습니다. 다음 상황은 Tencent Cloud의 서비스 품질 또는 책임과 관련이 없습니다.

1. Windows Server 2008 R2 엔터프라이즈 버전 SP1 64비트 운영 체제를 사용하는 인스턴스는 장애, 보안 문제, 비호환성, 작업 예외 또는 시스템 충돌에 노출될 수 있습니다.
2. Windows Server 2008 R2 엔터프라이즈 버전 SP1 64비트 인스턴스에서 실행 중인 애플리케이션에 예외가 있고 Microsoft의 패치 또는 OS 지원이 필요한 경우 문제 해결 지원만 제공할 수 있지만 완전한 솔루션은 제공할 수 없습니다.
3. 하드웨어 호환성 및 드라이버 관련 제한으로 인해 새로운 Tencent Cloud CVM은 Windows Server 2008 이미지 실행을 지원하지 못할 수 있습니다.