aws

用户指南

Amazon Lightsail



Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Lightsail: 用户指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 Lightsail？ 1
特征 1
Lightsail 是为谁准备的？ 2
开始使用 3
相关服务 3
估算、账单和成本优化 4
设置 5
注册获取 AWS 账户 5
创建具有管理访问权限的用户 5
访问 Lightsail 7
Lightsail 服务接口 7
Lightsail 服务端点 8
IPv4 端点 8
双栈（IPv4 和 IPv6）端点 8
各区域的服务终端节点 9
指定端点的示例 10
入门 13
步骤 1：完成先决条件 13
第 2 步：创建实例 13
步骤 3：连接到您的实例 14
步骤 4：向您的实例添加存储 17
步骤 5：创建快照 17
步骤 6：清除 18
后续步骤 19
将 Lightsail 与 AWS CLI 19
先决条件 19
生成 SSH 密钥对 20
创建和管理实例 21
连接到您的实例 24
向您的实例添加存储空间 26
创建和使用快照 28
清理资源 30
后续步骤 33
Lightsail 经销商 34

转售 Lightsail 的好处 34
Lightsail 经销商权益和增加的默认配额如何适用于您的账户 34
如何成为 Lightsail 经销商 37
成为 Lightsail 经销商 37
成为 Lightsail 经销商所需的信息 38
申请成为 Lightsail 经销商 38
申请其他账户成为 Lightsail 经销商 40
服务配额增加 42
以经销商身份联系 Lightsail 43
实例 46
创建实例 46
Linux 实例 46
Windows 实例 50
蓝图 57
操作系统 58
数据库应用程序 61
CMS 应用程序 62
应用程序堆栈和服务器 64
电子商务应用程序 66
项目管理应用程序 66
实例防火墙 67
Lightsail 防火墙 67
创建防火墙规则 68
指定协议 69
指定端口 69
指定应用层协议类型 70
指定源 IP 地址 71
Lightsail 的默认防火墙规则 72
添加防火墙规则 74
删除防火墙规则 75
实例防火墙规则 76
容量爆增和性能 79
CPU 性能 80
突增容量累积 82
识别实例爆增 83
监控容量爆增 84

查看容量爆增 86
排查高 CPU 问题 89
实例菜单 89
启动、停止或重启实例 89
强制停止实例 92
增强联网 94
在 Lightsail 中扩展 Windows 服务器文件系统 95
Linux Shell 脚本 99
PowerShell 脚本 101
Windows 安全最佳实践 103
删除实例 107
从 Lightsail 控制台主页中删除实例 107
从 Lightsail 控制台的实例管理页面中删除实例 108
使用删除实例 AWS CLI 108
后续步骤 110
SSH 和连接到您的实例 111
选择密钥对选项 111
连接到您的实例 112
管理存储在实例上的密钥 113
设置 SSH 密钥 113
管理 SSH 密钥 116
管理实例 SSH 密钥 130
连接到 Linux 实例 134
连接到 Windows 实例 153
实例元数据服务 167
使用实例元数据服务 168
其他 IMDS 文档 168
配置 IMDS 169
磁盘 175
数据块存储磁盘 175
磁盘配额 175
将磁盘附加到 Linux 实例 176
步骤 1：创建新磁盘并将其连接到您的实例 176
步骤 2：连接到您的实例以格式化并装载磁盘 177
步骤 3：每次重启您的实例时装载磁盘 182
将磁盘附加到 Windows 实例 183

步骤 1：创建新的数据块存储磁盘并将其连接到您的实例 183
步骤 2：连接到您的实例并将数据块存储磁盘联机 185
步骤 3：初始化数据块存储磁盘 187
步骤 4：通过系统文件格式化磁盘 189
分离并删除磁盘 191
先决条件 191
断开连接并删除您的磁盘 191
快照 193
手动快照 193
自动快照 193
系统磁盘快照 194
根据快照创建新资源 194
复制快照 195
将快照导出到亚马逊 EC2 195
删除快照 195
自动快照 195
自动快照限制 196
自动快照保留 196
使用 Lightsail 控制台启用或禁用自动实例快照 196
使用启用或禁用实例或块存储磁盘的自动快照 AWS CLI 198
更改快照时间 201
删除自动快照 205
保留自动快照 209
Linux 快照 214
Windows 快照和 sysprep 215
步骤 1：在运行 Sysprep 之前创建备份快照 216
步骤 2：连接到您的实例并使用 Sysprep 将其关闭 217
步骤 3：运行 Sysprep 之后创建快照 219
后续步骤 220
创建块存储磁盘的快照 221
从快照中创建磁盘 221
步骤 1：查找您的磁盘快照并选择创建新磁盘 222
步骤 2：通过磁盘快照创建新磁盘 223
创建根卷快照 225
步骤 1：完成先决条件 225
步骤 2：创建实例根卷快照 225

步骤 3：从快照创建数据块存储磁盘并将其连接到实例 227
步骤 4：从实例访问数据块存储磁盘 229
从快照创建实例 233
从快照创建更大的资源 235
先决条件 235
创建您的资源 235
使用快照创建更大的资源 AWS CLI 236
先决条件 237
步骤 1：获取您的快照名称 237
步骤 2：选择套装 237
第 3 步：编写 AWS CLI 命令并创建新实例 240
后续步骤 241
删除快照 242
跨区域复制快照 243
先决条件 243
复制快照 243
后续步骤 245
将快照导出到 EC2 245
根据导出的 Lightsail 快照创建亚马逊 EC2 资源 247
选择 Amazon EC2 实例类型 248
Connect 到亚马逊 EC2 实例 248
保护 Amazon EC2 实例 249
如何导出快照 249
监控导出 253
使用导出的快照创建 EC2 实例 254
从导出的快照创建 EBS 卷 261
连接到 Linux EC2 实例 263
安全的 Linux 或 Uni EC2 x 270
Connect 到 Windows EC2 实例 278
安全 Windows EC2 实例 284
AWS CloudFormation 堆栈 285
域和 DNS 288
域注册的工作原理 288
你可以在 Lightsail 中注册的域名 289
域注册定价 289
有关域的其他信息 289

Lightsail 中的 DNS 290
DNS 术语 290
Lightsail DNS 区域支持的 DNS 记录类型 292
创建一个 DNS 区域 294
编辑 DNS 区域 300
删除 DNS 区域 300
互联网流量路由 301
将域指向实例 303
将域指向负载均衡器 305
转移 DNS 管理 308
使用 Route 53 309
注册域 313
使用 Lightsail 注册一个新域名 314
域的详细信息 317
设置域名格式 318
为域名注册设置域名格式 318
为 DNS 区域和记录设置域名格式 318
在 DNS 区域和记录的名称中使用星号（*） 318
后续步骤 319
管理 R53 中的域 320
查看域注册的状态 320
锁定域以防止未经授权转移到另一个注册商 320
恢复已到期或已删除的域 321
转移域注册 321
删除域名注册 321
注册信息 321
租期 322
自动域续订 322
注册人、管理、技术和账单联系人 322
Contact type（联系人类型） 323
名字、姓氏 323
组织 323
电子邮件 324
电话 324
Address 1（地址 1） 324
Address 2（地址 2） 324

国家/地区 324
州/省 325
城市 325
邮政编码 325
Privacy protection（隐私保护） 325
注册续订 326
Automatic renewal（自动续订） 326
在域注册期间为域配置自动续订 327
为已注册的域配置自动续订 328
Privacy protection（隐私保护） 328
完成 先决条件 328
管理域的隐私保护 329
更新域名联系人信息 329
Who is the owner of a domain?（域的所有者是谁？） 329
更新域的联系信息 329
数据库 331
比较数据库 331
比较 Lightsail 中的托管数据库 331
优化数据导入 333
高可用性数据库 333
创建 数据库 333
后续步骤 336
连接到 MySQL 337
步骤 1：获取 MySQL 数据库连接详细信息 337
步骤 2：配置 MySQL 数据库的公有可用性 338
步骤 3：将数据库客户端配置为连接到 MySQL 数据库 338
后续步骤 341
使用 SSL 连接到 MySQL 341
支持的连接 342
先决条件 342
使用 SSL 连接到 MySQL 数据库 342
连接到 PostgreSQL 344
步骤 1：获取 PostgreSQL 数据库连接详细信息 345
步骤 2：配置 PostgreSQL 数据库的公有可用性 345
步骤 3：将数据库客户端配置为连接到 PostgreSQL 数据库 346
后续步骤 348

使用 SSL 连接到 PostgreSQL 348
先决条件 349
使用 SSL 连接到您的 Postgres 数据库 349
删除数据库 350
数据导入模式 351
导入 SQL 数据 352
将数据导入 PostgreSQL 354
数据库日志 356
MySQL 查询日志 358
禁用 point-in-time-backups 361
先决条件 361
禁用数据库 point-in-time备份 361
数据库快照 363
后续步骤 364
还原数据库 364
从快照创建数据库 367
下载 SSL 证书 369
所有 AWS 区域 s 的证书捆绑包 370
特定 AWS 区域的证书捆绑包 370
更新 CA 证书 370
维护和备份时段 373
先决条件 374
更改数据库维护时段 374
后续步骤 377
管理数据库密码 377
后续步骤 379
公有模式 379
后续步骤 380
更新参数 380
先决条件 380
获取可用数据库参数的列表 380
更新数据库参数 382
升级主要版本 384
先决条件 384
更新数据库主要版本 384
后续步骤 387

从 MySQL 5.6 迁移 387
步骤 1：了解更改 388
步骤 2：完成先决条件 388
步骤 3：连接到 MySQL 5.6 数据库并导出数据 388
步骤 4：连接到 MySQL 5.7 数据库并导入数据 392
步骤 5：测试您的应用程序并完成迁移 395
负载均衡器 396
负载均衡器功能 396
何时使用负载均衡器 396
建议进行负载均衡的应用程序 397
开始使用负载均衡器 397
创建负载均衡器 397
先决条件 397
创建负载均衡器 397
将实例附加到您的负载均衡器 399
后续步骤 399
更新 负载均衡器设置 399
运行状况检查 400
加密的流量 (HTTPS) 400
会话持久性 401
实例负载均衡 401
一般准则：使用数据库的应用程序 401
WordPress 401
Node.js 401
Magento 402
GitLab 402
Drupal 403
LAMP 堆栈 403
MEAN 堆栈 403
Redmine 404
Nginx 404
Joomla! 404
配置 TLS 安全策略 405
安全策略概述 405
支持的安全策略和协议 405
完成先决条件 407

使用 Lightsail 控制台配置安全策略 407
使用配置安全策略 AWS CLI 407
HTTP 到 HTTPS 重新导向 408
完成先决条件 408
使用 Lightsail 控制台在您的负载均衡器上配置 HTTPS 重定向 409
使用以下命令为负载均衡器配置 HTTP 到 HTTPS 重定向 AWS CLI 409
会话持久性 411
启用会话持久性 411
调整 Cookie 持续时间 411
运行状况检查 412
自定义运行状况检查路径 413
运行状况检查指标 414
运行状况检查 415
分离实例 416
删除 负载均衡器 417
分配 418
使用案例 420
配置您的分配 421
边缘站点和 IP 地址范围 422
创建分配 422
先决条件 423
源资源 423
源协议策略 424
缓存行为和缓存预设 425
最适合 WordPress 缓存预设 425
默认行为 426
目录和文件覆盖 426
高级缓存设置 427
分配计划 430
创建分配 430
后续步骤 433
删除分配 433
删除分配 434
缓存行为 434
缓存预设 434
最适合 WordPress缓存预设 435

默认行为 435
目录和文件覆盖 436
高级缓存设置 437
更改分配的缓存行为 439
重置缓存 440
更改源 441
源协议策略 441
更改分配的源 441
将存储桶与分配结合使用 443
步骤 1：完成先决条件 443
步骤 2：修改存储桶权限 444
步骤 3：创建使用存储桶作为源的分配 447
步骤 4：启用分配的自定义子域 449
第 5 步：在你的 WordPress 网站上安装 WP Offload Media Lite 插件 449
第 6 步：测试你的 WordPress 网站与 Lightsail 存储桶和发行版之间的连接 455
管理存储桶和对象 458
更改套餐 460
更改分配计划 460
分配自定义域 460
先决条件 461
启用分配的自定义域 461
将域指向分配 462
更改自定义域 464
禁用分配自定义域 464
将分配域添加到容器服务 465
请求和响应行为 467
分配如何处理请求并将请求转发到源 467
分配如何处理来自源的响应 480
POST 分配 484
测试您的分配。 484
网络连接 486
负载均衡器 486
静态 IPs 486
IP 地址 486
实例的私有 IPv4 地址和公有地址 486
实例的静态 IPv4 地址 488

IPv6 用于实例、容器服务、CDN 分发和负载均衡器 490
静态 IP 地址 492
双堆栈联网 497
IPv6-仅限联网 500
区域和可用区 504
SSH 密钥和 Lightsail 区域 505
使用 Lightsail 区域的技巧 505
Lightsail 可用区 505
可用区和你的 Lightsail 应用程序 506
VPC 对等连接 506
允许与其他 AWS 服务通信 507
SSL/TLS 证书 507
为什么使用 HTTPS？ 508
过程概述 508
将 SSL/TLS 证书与分配和容器服务结合使用 509
将 SSL/TLS 证书与负载均衡器结合使用 510
容器证书 510
分配证书 515
负载均衡器证书 525
配置反向 DNS 533
先决条件 534
向 Amazon Web Services Support 提交请求以配置反向 DNS 534
存储桶 536
对象存储概念 536
管理存储桶和对象 538
创建存储桶 538
创建存储桶 538
管理存储桶和对象 539
删除存储桶 541
强制删除存储桶 541
使用 Lightsail 控制台删除你的存储桶 541
使用删除您的存储桶 AWS CLI 542
管理存储桶和对象 543
创建访问密钥 545
为存储桶创建访问密钥 546
删除访问密钥 546

删除存储桶的访问密钥 547
阻止公有访问 547
为您的账户配置屏蔽公共访问权限设置 548
管理存储桶和对象 550
存储桶访问日志 552
启用日志传输需要哪些操作？ 552
日志对象密钥格式 553
如何传输日志？ 553
尽量访问日志传输 553
存储桶日志记录状态更改将逐渐生效 554
访问日志格式 554
管理访问日志 566
使用访问日志 570
存储桶对象 574
使用 Lightsail 控制台过滤对象 575
使用查看对象 AWS CLI 577
管理存储桶和对象 579
复制和移动对象 581
删除对象 585
下载对象 592
筛选对象 596
管理对象版本控制 600
还原对象版本 605
为对象添加标签 609
存储桶资源访问权限 613
配置存储桶的资源访问权限 613
更改存储桶套餐 614
使用 Lightsail 控制台更改存储分区的存储计划 614
使用更改存储桶的存储计划 AWS CLI 614
配置访问权限 616
配置存储桶访问权限 617
跨账户访问 618
配置存储桶的跨账户存取 618
个别对象访问权限 619
配置个别对象访问权限 619
分段上传 620

分段上传流程 621
并发分段上传操作 623
分段上传保留 623
Amazon Simple Storage Service 分段上传限制 624
拆分要上传的文件 624
使用 AWS CLI启动分段上传 624
使用上传分段 AWS CLI 625
使用 Amazon CLI 列出分段上传的分段 626
创建分段上传 .json 文件 628
使用 Amazon CLI 完成分段上传 630
使用 Amazon CLI 列出存储桶分段上传 631
使用 Amazon CLI 停止分段上传 632
命名规则 633
示例存储桶名称 634
对象键名称 634
键名称 635
对象键命名准则 635
XML 相关的对象键约束 637
对象存储安全最佳实践 638
预防性安全最佳实践 639
监测和审计最佳实践 643
存储桶权限 644
存储桶访问权限 645
个别对象访问权限 645
跨账户访问 646
访问密钥 646
资源访问权限 646
Amazon S3 屏蔽公共访问权限 646
将文件上传到存储桶 647
对象键名称和版本控制 647
使用 Lightsail 控制台将文件上传到存储桶 648
使用 AWS CLI将文件上传到存储桶 648
为 IPv6仅限请求配置 AWS CLI 650
在 Lightsail 中管理存储桶和对象 651
容器服务 653
容器 653

Lightsail 容器服务元素 654
Lightsail 容器服务 654
容器服务容量（规模和功率） 655
定价 656
部署 656
部署版本 657
容器镜像源 657
容器服务 ARN 657
公有端点和默认域 658
自定义域和 SSL/TLS 证书 659
容器日志 659
Metrics 659
使用 Lightsail 容器服务 659
创建容器 660
容器服务容量（规模和功率） 661
定价 661
容器服务节点 661
创建容器服务 662
容器映像 664
步骤 1：完成先决条件 665
步骤 2：创建 Docker 文件并构建容器镜像 665
步骤 3：运行新容器镜像 667
（可选）步骤 4：清除本地机器上运行的容器 668
创建容器镜像后的后续步骤 668
管理容器映像 669
安装容器服务插件 673
ECR 私有存储库访问权限 679
管理容器和部署 695
先决条件 696
部署参数 696
容器之间的通信 700
容器日志 700
部署版本 700
部署状态 701
部署失败 701
查看当前的容器服务部署 701

创建或修改容器服务部署 701
更改容器容量 704
管理部署版本 705
查看容器日志 706
容器服务自定义域 709
容器服务自定义域限制 709
先决条件 709
查看容器服务的自定义域 710
为容器服务启用自定义域 710
禁用容器服务的自定义域 711
将 Lightsail 域指向容器 712
将 Route 53 域指向容器 714
删除容器 719
删除容器服务 719
安全性 720
基础结构安全性 720
恢复能力 720
身份和访问管理 721
受众 721
使用身份进行身份验证 721
使用策略管理访问 725
AWS 托管策略 728
Lightsail 的政策和角色 730
管理 IAM 用户的访问权限 749
更新管理 755
实例蓝图软件支持 755
合规性验证 756
AWS PrivateLink 757
注意事项 757
创建接口端点 757
AWS CLI 例子 758
创建端点策略 758
监控性能 760
有效地监控您的资源 760
指标的概念和术语 760
Metrics 761

指标保留 761
统计信息 761
单位 761
时间段 762
警报 762
Lightsail 中提供的指标 762
实例指标 762
数据库指标 763
分配指标 764
负载均衡器指标 764
容器服务指标 765
存储桶指标 765
资源运行状况指标 766
实例指标 766
数据库指标 767
分配指标 767
负载均衡器指标 767
容器服务指标 768
存储桶指标 769
指标通知 769
查看 实例指标 770
指标警报 773
创建实例警报 783
删除或禁用警报 787
存储桶指标 788
存储桶指标 789
在 Lightsail 控制台中查看存储桶指标 789
管理存储桶和对象 790
创建警报 791
容器指标 795
容器服务指标 795
在 Lightsail 控制台中查看容器服务指标 795
数据库指标 796
数据库指标 796
在 Lightsail 控制台中查看数据库指标 797
查看数据库指标后的后续步骤 797

创建数据库警报 ... 798
分配指标 ... 802
分配指标 ... 803
在 Lightsail 控制台中查看分发指标 ... 803
查看分配指标后的后续步骤 ... 804
创建分配警报 ... 804
负载均衡器指标 ... 808
负载均衡器指标 ... 809
查看负载均衡器指标 ... 810
后续步骤 ... 810
负载均衡器警报 ... 811
添加通知联系人 ... 815
区域通知联系人限制 ... 816
SMS 文本消息收发支持 ... 816
电子邮件联系人验证 ... 817
使用 Lightsail 控制台添加通知联系人 ... 818
使用 AWS CLI添加通知联系人 ... 823
添加通知联系人后的后续步骤 ... 825
删除通知联系人 ... 825
使用 Lightsail 控制台删除通知联系人 ... 825
使用 AWS CLI删除通知联系人 ... 826
删除通知联系人后的后续步骤 ... 827
查看 Lightsail 警报通知 ... 827
查看警报通知以了解活动警报 ... 827
查看待验证的电子邮件联系人 ... 828
标签 ... 829
使用标签整理账单并控制访问 ... 829
支持标记的 Lightsail 资源 ... 829
标签限制 ... 831
添加标签 ... 831
后续步骤 ... 833
删除标签 ... 833
基于标签的权限和授权 ... 835
使用标签控制访问 ... 835
步骤 1：创建 IAM policy ... 835
步骤 2：将策略附加到用户或组 ... 837

使用标签整理成本 837
步骤 1：向资源添加键值标签 837
步骤 2：激活用户定义的成本分配标签 838
步骤 3：设置成本分配报告并进行查看 838
使用标签整理资源 838
查看资源的标签 839
使用标签筛选资源 839
故障排除 841
WordPress 设置 841
常见错误 842
设置失败 845
403 错误（未经授权） 849
数据块存储磁盘 850
常规磁盘错误 850
基于浏览器的 SSH 或 RDP 客户端 851
错误消息：Can’t connect (无法连接) 851
错误消息：Can’t connect right now (无法立即连接) 853
Ghost 服务不可用 854
启动 Ghost 服务 854
IAM 问题 856
我无权在 Lightsail 中执行任何操作 857
我无权执行 iam：PassRole 857
我想要查看我的访问密钥 858
我是一名管理员，想允许其他人访问 Lightsail 858
我想允许 AWS 账户之外的人访问我的 Lightsail 资源 859
IPv6 可达性 859
IPv6 为双栈实例启用 859
配置实例的防火墙 861
测试您实例的可达性 861
实例容量不足错误 864
启动新实例时容量不足 864
启动已停止的实例时容量不足 864
相关信息 865
负载均衡器 865
常规负载均衡器错误 865
通知 866

SSL/TLS 证书 867
教程 869
快速入门指南 870
AlmaLinux 870
cPanel 和 WHM 878
Drupal 890
Ghost 899
GitLab CE 910
Joomla! 919
LAMP 929
Magento 931
Nginx 946
Node.js 948
Plesk 950
PrestaShop 954
Redmine 968
WordPress 977
WordPress 多站点 982
Bitnami 989
Bitnami 用户名和密码 989
删除 Bitnami 横幅 997
WordPress 1000
配置 WordPress 1001
连接到 Amazon S3 1008
连接到 Aurora 数据库 1017
连接到 MySQL 1024
连接到存储桶 1028
配置 CDN 1043
启用电子邮件 1047
启用 HTTPS 1057
迁移到 Lightsail 1067
WordPress 多站点 1074
WordPress 多站点：将博客添加为域名 1074
WordPress 多站点：将博客添加为子域名 1081
WordPress 多站点：定义域名 1084
Let's Encrypt 1086

LAMP Let's Encrypt 证书 1087
Nginx Let's Encrypt 证书 1100
WordPress 让我们加密证书 1115
IPv6 联网 1130
IPv6 适用于 cPanel 和 WHM 1130
IPv6 对于 GitLab 1136
IPv6 对于 Nginx 1139
IPv6 给 Plesk 1143
AWS CLI 适用于 Lightsail 1146
步骤 1：安装 AWS CLI 1147
步骤 2：创建新的访问密钥 1147
步骤 3：配置 AWS CLI 1148
后续步骤 1148
AWS CloudShell 1149
持久性存储 1149
AWS 区域 1149
启动和使用 AWS CloudShell 1150
其他信息 1153
启动和配置 LAMP 1153
步骤 1：注册亚马逊云科技 1154
步骤 2：创建 LAMP 实例 1154
步骤 3：通过 SSH 连接到您的实例并获取 LAMP 实例的应用程序密码 1157
步骤 4：在您的 LAMP 实例上安装应用程序 1158
步骤 5：创建静态 IP 地址并将其附加到 LAMP 实例 1158
步骤 6：创建 DNS 区域并将域映射到 LAMP 实例 1160
后续步骤 1161
将 LAMP 实例连接到 Aurora 数据库 1161
启动并配置 Windows Server 2016 1166
步骤 1：注册亚马逊云科技 1166
第 2 步：在 Lightsail 中创建 Windows Server 2016 实例 1166
步骤 3：通过 RDP 连接到 Windows Server 2016 实例 1169
步骤 4：创建静态 IP 地址并将其附加到 Windows Server 2016 实例 1170
步骤 5：创建 DNS 区域并将域映射到 Windows Server 2016 实例 1173
后续步骤 1174
CloudTrail 日志记录 1174
Lightsail 中的信息 CloudTrail 1174

了解 Lightsail 日志文件条目 1175
创建 HAR 文件 1175
步骤 1：在浏览器中创建 HAR 文件 1176
步骤 2：编辑 HAR 文件以删除敏感信息 1178
步骤 3：提交 HAR 文件以供审核 1178
安装 Prometheus 1178
步骤 1：完成先决条件 1178
步骤 2：将用户和本地系统目录添加到 Lightsail 实例 1179
步骤 3：下载 Prometheus 二进制包 1180
步骤 4：配置 Prometheus 1183
步骤 5：启动 Prometheus 1185
步骤 6：启动 Node Exporter 1187
步骤 7：使用 Node Exporter 数据收集器配置 Prometheus 1188
使用 scp 传输文件 1191
前提条件 1191
步骤 1：将私有密钥（.pem）文件保存到本地计算机 1192
步骤 2：更改私有密钥的权限 1192
步骤 3：将私有密钥传输到您的实例 1193
第 4 步：在 Lightsail Linux 和 Unix 实例之间安全地传输文件 1194
使用其他亚马逊云科技服务 1195
虚拟机（虚拟私有服务器） 1196
无服务器计算 1196
数据库 1197
负载均衡器 1198
大数据 1198
存储 1199
监控和警报 1200
应用程序部署 1200
应用程序容器 1200
安全性和用户登录 1201
源代码控制和应用程序生命周期管理 1201
队列和消息收发 1201
工作流 1202
流式处理应用程序 1203
AWS CloudFormation 资源 1203
Lightsail 和模板 AWS CloudFormation 1203

了解更多关于 AWS CloudFormation 1203
有关 Lightsail 的其他信息 1204
博客 1204
教程 1207
视频 1208
计费 1211
查看你的详细的 Lightsail 账单 1211
账单使用类型 1212
账单中的区域代码 1213
FAQs 1215
关于 Lightsail 1215
什么是 Amazon Lightsail？ 1215
我能用 Lightsail 做什么？ 1216
Lightsail 是否提供 API？ 1216
如何注册 Lightsail？ 1216
Light AWS 区域 sail 在哪个版本中可用？ 1216
什么是可用区？ 1217
Lightsail 的服务配额是多少？ 1217
我如何获得更多帮助？ 1217
账单和账户管理 1217
Lightsail 计划的费用是多少？ 1217
计划在什么情况下计费？ 1218
我可以免费试用 Lightsail 实例吗？ 1218
Lightsail 免费试用什么时候开始？ 1218
Lightsail 托管数据库的成本是多少？ 1218
我可以免费试用 Lightsail 托管数据库吗？ 1219
Lightsail 区块存储的成本是多少？ 1219
Lightsail 负载均衡器的费用是多少？ 1219
证书管理如何收费？ 1219
Lightsail 静态 IPv4地址的费用是多少？ 1219
数据传输如何收费？ 1219
我针对实例的数据传输限额如何运作？ 1219
如何在我的负载均衡器中使用数据传输限额？ 1221
如果我超出我的数据传输计划限额该怎么办？ 1221
我需要为哪些类型的数据传输付费？ 1221
各 AWS 区域的实例数据传输限额有何差异？ 1222

Lightsail 域名的费用是多少？ 1222
Lightsail DNS 的管理费用是多少？ 1223
Lightsail 快照的费用是多少？ 1223
如何管理我的 AWS 账户？ 1223
Lightsail 的法律使用条款是什么？ 1223
我怎样才能支付我的 Lightsail 账单？ 1223
数据传输 1224
如果我超过了实例的数据传输计划限额怎么办？ 1224
对于哪些类型的数据传输，我需要为实例付费？ 1224
我针对实例的数据传输限额如何运作？ 1225
我的实例数据传输限额有何不同 AWS 区域？ 1226
数据传输如何收费？ 1226
如何在我的负载均衡器中使用数据传输限额？ 1226
对象存储如何使用我的数据传输限额？ 1227
我需要为哪些类型的数据传输收取分发费用？ 1227
Lightsail 的实例数据传输配额和分布式数据传输配额有什么区别？ 1227
我需要为进出容器服务的数据传输付费吗？ 1228
数据块存储（磁盘） 1228
我能用 Lightsail 区块存储做什么？ 1228
连接的磁盘与我的 Lightsail 套餐中包含的存储空间有何不同？ 1229
我可以连接多大的磁盘？ 1229
每个 Lightsail 实例可以连接多少个磁盘？ 1229
我是否可以将一个磁盘连接到多个实例？ 1229
是否需要将我的磁盘连接到实例上？ 1229
我是否可以增加连接的磁盘大小？ 1229
Lightsail 区块存储是否提供加密？ 1229
我可以期待 Lightsail 区块存储提供什么可用性？ 1229
我如何备份连接的磁盘？ 1230
证书 1230
如何使用 LightSail 提供的证书？ 1230
如何验证我的证书？ 1230
如果无法验证我的域，会发生什么情况？ 1230
可以将多少个域和子域添加到我的证书中？ 1230
如何更改与我的证书关联的域？ 1230
如何续订我的证书？ 1231
在删除负载均衡器时，我的证书会发生什么情况？ 1231

我能否下载 Lightsail 提供的证书？ 1231
联系人和监控通知 1231
什么是通知？ 1231
我可以添加多少个联系人？ 1231
容器服务 1231
我可以用 Lightsail 容器服务做什么？ 1231
Lightsail 容器服务能否运行 Docker 容器？ 1232
如何在 Lightsail 容器服务中使用我的公共容器镜像？ 1232
我可以从私有容器注册表中提取容器镜像吗？ 1232
我可以根据需求更改服务的功率和规模吗？ 1232
我能否自定义 Lightsail 容器服务创建的 HTTPS 终端节点的名称？ 1232
我能否将自定义域名用作 Lightsail 容器服务的 HTTPS 终端节点？ 1232
Lightsail 集装箱服务的费用是多少？ 1232
如果我只是运行了几天的容器服务，会向我收取整个月的费用吗？ 1233
我需要为进出容器服务的数据传输付费吗？ 1233
停止和删除容器服务之间有何区别？ 1234
如果我的容器服务处于禁用状态，会向我收取费用吗？ 1234
我能否使用容器服务作为我的 Lightsail 内容分发网络 (CDN) 发行版的来源？ 1234
我能否使用容器服务作为 Lightsail 负载均衡器的目标？ 1234
是否可以将容器服务的公有端点配置为将 HTTP 请求重新导向到 HTTPS？ 1234
容器服务是否支持监控和提醒？ 1234
Lightsail 容器服务支持吗？ IPv6 1234
内容分发网络分配 1235
我能用 Lightsail CDN 发行版做什么？ 1235
我可以使用哪些类型的资源作为分配的源？ 1235
我是否需要将静态 IPv4地址附加到我的 Lightsail 实例才能将其用作 Lightsail 发行版的来源？ 1235
如何在我的 WordPress 网站上设置 Lightsail 发行版？ 1235
我可以附加多个源吗？ 1235
Lightsail 发行版是否支持证书创建？ 1235
是否需要证书？ 1235
可以创建的证书数量有限制吗？ 1236
如何配置我的分配以将 HTTP 请求重新导向到 HTTPS？ 1236
如何将我的顶点域名配置为指向我的 Lightsail 发行版？ 1236
Lightsail 的实例数据传输配额和分布式数据传输配额有什么区别？ 1236
我可以更改与分配关联的计划吗？ 1236

如何知道我的分配是否正常工作？ 1236
我能否删除 Lightsail 发行版中的缓存内容？ 1236
与亚马逊 CloudFront 发行版相比，我什么时候应该使用 Lightsail 发行版？ 1236
我能否将我的 Lightsail 内容分发网络 (CDN) 分发转移到亚马逊？ CloudFront 1237
Lightsail CDN 打算如何使用？ 1237
Lightsail CDN 发行版是否支持？ IPv6 1238
是否需要 IPv6 启用源代码才能与 Lightsail CDN 发行版配合使用？ 1238
数据库 1238
什么是 Lightsail 托管数据库？ 1238
我可以用 Lightsail 托管的数据库做什么？ 1238
Lightsail 能为我管理什么？ 1238
Lightsail 支持哪些类型的数据库以及这些数据库的哪些版本？ 1239
Lightsail 提供哪些托管数据库计划？ 1239
什么是高可用性计划？ 1239
如何扩大或缩小我的 Lightsail 托管数据库？ 1239
如何备份我的 Lightsail 托管数据库？ 1239
如果我删除我的 Lightsail 托管数据库，我的数据会怎样？ 1240
我能否将我的实例连接到在不同 AWS 区域 或不同可用区中运行的 Lightsail 托管数据库？ . 1240
如何将数据加载到我的 Lightsail 托管数据库中？ 1240
如何访问我的 Lightsail 托管数据库中的数据？ 1240
Lightsail 托管数据库如何与我的 Lightsail 实例配合使用？ 1240
如何将 Lightsail 托管数据库连接到我的 AWS 账户中运行的 EC2 实例？ 1241
我的 Lightsail 托管数据库的公共模式和私有模式有什么区别？ 1241
我能否管理我的 Lightsail 托管数据库使用的端口？ 1241
Lightsail 托管数据库服务是否支持？ IPv6 1241
域 1241
我能用 Lightsail 域名做什么？ 1241
我可以使用哪些顶级域名 (TLDs)？ 1241
我能否将 Lightsail 作为我现有域名的 DNS 服务？ 1242
如何开始在 Lightsail 中注册域名？ 1242
与 Route 53 相比，我什么时候应该在 Lightsail 中注册域名？ 1242
我可以将我的域名转移到 Lightsail 吗？ 1242
我可以将哪些 Lightsail 资源用于域？ 1242
将资源导出到 Amazon EC2 1242
什么是向亚马逊出口 EC2？ 1242
我为什么要出口到 Amazon EC2？ 1242

出口到亚马逊是如何 EC2 运作的？ 1243
如何计费？ 1243
我是否可导出托管数据库或磁盘快照？ 1243
我可以导出哪些 Lightsail 资源？ 1243
实例 1243
什么是 Lightsail 实例？ 1243
什么是 Lightsail 计划？ 1244
我可以在我的实例上运行什么软件？ 1244
我可以在 Lightsail 上使用哪些操作系统？ 1244
我需要自带许可证才能使用 Lightsail 实例吗？ 1244
如何创建 Lightsail 实例？ 1244
Lightsail 实例的性能如何？ 1244
如何知道我的实例何时突增？ 1245
如何连接到 Lightsail 实例？ 1245
如何备份我的实例？ 1245
我能否升级我的计划？ 1245
如何将 Lightsail 实例连接到我 AWS 账户中的其他资源？ 1245
停止实例和删除实例有何区别？ 1246
负载均衡器 1246
我可以用 Lightsail 负载均衡器做什么？ 1246
我能否将负载均衡器用于不同 AWS 区域 或不同可用区的实例？ 1246
我的 Lightsail 负载均衡器如何应对流量峰值？ 1247
Lightsail 负载均衡器如何将流量路由到我的目标实例？ 1247
Lightsail 如何知道我的目标实例是否运行正常？ 1247
我可以将多少个实例连接到负载均衡器？ 1247
我是否可以将一个实例分配给多个负载均衡器？ 1247
在删除负载均衡器时，我的目标实例会发生什么情况？ 1247
什么是会话持久性？ 1247
Lightsail 负载均衡器支持哪种连接？ 1248
Lightsail 负载均衡器是否支持？ IPv6 1248
是否需要启用负载均衡器后面的实例才能使用 IPv6 已启用的负载均 IPv6 衡器？ 1248
快照 1248
什么是快照 1248
什么是自动快照？ 1248
手动快照与自动快照之间有什么区别？ 1249
哪些资源支持快照？ 1249

我可以存储快照多长时间？ 1249
如何启用自动快照？ 1249
何时创建自动快照？ 1249
我可以存储多少个快照？ 1249
快照如何计费？ 1250
如果禁用自动快照，是否会丢失快照？ 1250
如果我不想替换自动快照该怎么办？ 1250
我是否可以删除自动快照？ 1250
如何使用快照？ 1250
指标和警报 1250
什么是指标？ 1250
什么是警报？ 1251
我可以添加多少个警报？ 1251
网络连接 1251
如何在 Lightsail 中使用 IP 地址？ 1251
Lightsail 是否支持仅限实 IPv6例？ 1251
什么是静态 IP？ 1251
我 IPs 可以将多少静态实例附加到一个实例？ 1251
什么是 DNS 记录？ 1252
我能否管理我的实例的防火墙设置？ 1252
对象存储（存储桶） 1252
我可以使用 Lightsail 对象存储执行哪些操作？ 1252
Lightsail 对象存储如何收费？ 1252
Lightsail 对象存储是否有超额费用？ 1252
对象存储如何使用我的数据传输限额？ 1253
我可以更改与我的 Lightsail 存储桶关联的计划吗？ 1253
是否可以将对象从 Lightsail 对象存储复制到 Amazon S3？ 1253
如何开始使用 Lightsail 对象存储？ 1253
如何将对象上传到我的存储桶？ 1253
可以阻止对存储桶的公有访问吗？ 1253
如何提供存储桶的编程访问权限？ 1254
如何与其他 AWS 账户共享存储桶？ 1254
什么是版本控制？ 1254
如何将我的 Lightsail 存储桶关联到我的 Lightsail CDN 分配？ 1254
Lightsail 对象存储服务有什么限制？ 1254
Lightsail 对象存储是否支持监控和提醒？ 1254

Lightsail 中的标签 1255
标签是什么？ 1255
如何在 Lightsail 中使用标签？ 1255
什么资源可以标记？ 1255
如何标记我的 Lightsail 快照？ 1256
键-值和仅键标签之间有什么差别？ 1256
获取帮助 1257
上下文相关的帮助面板 1257
关于本用户指南 1257
使用搜索 1258
使用 Lightsail CLI 和 API 1258
AWS 论坛和其他社区资源 1258
..... mcclix

什么是 Amazon Lightsail？

对于任何需要构建网站或网络应用程序的人来说，Amazon Lightsail 是开始使用亚马逊网络服务 (AWS) 的最简单方法。它包括快速启动项目所需的一切内容 — 实例（虚拟专用服务器）、容器服务、托管式数据库、内容分发网络 (CDN) 分配、负载均衡器、基于 SSD 的块存储、静态 IP 地址、注册域的 DNS 管理以及资源快照（备份），并且每月的费用少且可预测。

Lightsail 还提供用于研究的亚马逊 Lightsail。借助 Lightsail for Research，学者和研究人员可以在其中创建强大的虚拟计算机。 AWS Cloud这些虚拟计算机预装了研究应用程序，例如 RStudio 和Scilab。有关更多信息，请参阅 Amazon Lightsail 研究版用户指南。

主题

- Lightsail 的特点
- Lightsail 是为谁准备的？
- 开始使用 Lightsail
- 相关服务
- 估算、账单和成本优化

Lightsail 的特点

Lightsail 提供了以下高级功能：

实例

Lightsail提供易于设置的虚拟专用服务器（实例），并由的强大功能和可靠性提供支持。 AWS您可以在几分钟内启动您的网站、Web 应用程序或项目，并通过直观的 Lightsail 控制台或 API 管理您的实例。

在创建实例时，你需要 click-to-launch一个简单的操作系统 (OS)、一个预先配置的应用程序或开发堆栈，例如 Windows、Plesk WordPress、LAMP、Nginx 等。每个 Lightsail 实例都带有内置防火墙，您可以使用该防火墙根据源 IP、端口和协议来允许或限制实例的流量。了解更多

容器

在云中运行并安全访问容器化应用程序。容器是将代码和依赖关系打包在一起的软件标准单位，这样应用程序就可以从一个计算环境快速可靠地转到另一个计算环境运行。了解更多

负载均衡器

在您的实例之间路由 Web 流量，以便您的网站和应用程序可以适应流量的变化，防止中断，并提供无缝的访客体验。了解更多

托管数据库

Lightsail 提供完全配置的 MySQL 或 PostgreSQL 数据库计划，其中包括内存、处理、存储和传输限额。借助 Lightsail 托管数据库，您可以独立于虚拟服务器轻松扩展数据库、提高应用程序可用性或在云中运行独立数据库。了解更多

块和对象存储

Lightsail 同时提供区块和对象存储。借助适用于 Linux 或 Windows 虚拟服务器的高可用性 SSD 存储器，您可以快速轻松地扩展存储。了解更多

借助 Lightsail Object 存储桶，您可以随时随地从互联网上的任何地方存储和检索对象。您还可以在云上托管静态内容。了解更多

CDN 分配

Lightsail 支持内容分发网络 (CDN) 分发，这些分发建立在与亚马逊相同的基础设施之上。CloudFront通过在世界各地设置代理服务器，您可以轻松地将内容分配给全球受众，从而用户可以在距离他们更近的地理位置访问您的网站以减少延迟。了解更多

访问 AWS 服务

Lightsail 使用了一组重点功能，例如实例、托管数据库和负载均衡器，以简化入门流程。但这并不意味着你只能选择这些选项，你可以通过 AWS Amazon VPC 对等互连将你的 Lightsail 项目与其他 90 多种服务中的一些集成。了解更多

有关 Lightsail 的更多详情，请参阅亚马逊 Lights ail。

Lightsail 是为谁准备的？

Lightsail 适合所有人。您可以为 Lightsail 实例选择一个可以快速启动项目的映像，这样您就不必花费太多时间安装软件或框架。

如果您是从事个人项目的个人开发者或业余爱好者，Lightsail 可以帮助您部署和管理基本的云资源。您可能还对学习或尝试云服务感兴趣，例如虚拟机、域或网络。Lightsail 提供了一种快速入门的方法。

Lightsail 包含基本操作系统的映像、LAMP、LEMP（Nginx）和 SQL Server Express 等开发堆栈以及 Drupal 和 Magento 等 WordPress应用程序。有关安装在每个映像上的软件的更多详细信息，请参阅选择 Lightsail 实例映像。

随着项目的发展，您可以添加块存储磁盘并将其连接到您的 Lightsail 实例。您可以拍摄这些实例和磁盘的快照，并通过这些快照轻松创建新的实例。您还可以对您的 VPC 进行对等，这样您的 Lightsail 实例就可以使用 Lightsail 之外的其他 AWS 资源。

您还可以创建 Lightsail 负载均衡器并连接目标实例，以创建高度可用的应用程序。您还可以配置负载均衡器以处理加密的 (HTTPS) 流量、会话持久性、运行状况检查，等等。

开始使用 Lightsail

设置使用 Lightsail 后，您可以Lightsail 上的虚拟专用服务器入门逐步启动、连接和清理实例。有关如何访问 Lightsail 的更多信息，请参阅。访问 Lightsail

相关服务

您可以直接使用 Lightsail 预配置 Lightsail 资源，例如实例和磁盘。此外，您还可以使用其他 AWS 服务来配置资源，例如：

- Amazon EC2

  提供可调节的计算容量 (简单来说，就是 Amazon 数据中心的服务器)，您可以使用它构建和托管您的软件系统。要比较 Lightsail 和亚马逊 EC2，请参阅亚马逊 Light sail 或亚马逊。 EC2
- Amazon A EC2 uto Scaling

  有助于确保您有正确数量的 Amazon EC2 实例来处理应用程序的负载。
- Elastic Load Balancing

  可在多个实例间自动分配传入的应用程序流量。
- Amazon Relational Database Service (Amazon RDS)

  在云中设置、操作和扩展托管式关系数据库。
- Amazon Elastic Container Service（Amazon ECS）

  在 Ama EC2 zon 实例集群上部署、管理和扩展容器化应用程序。

估算、账单和成本优化

要为您的 AWS 用例创建估算值，请使用AWS 定价计算器。

若要查看您的账单，请转到 AWS 账单与成本管理 控制台中的账单和成本管理控制面板。您的账单中包含了提供您的账单详情的使用情况报告的链接。要了解有关 AWS 账户账单的更多信息，请参阅《AWS 账单与成本管理用户指南》。

如果您对 AWS 账单、账户和活动有疑问，请联系 Su AWS pport。

您可以使用来优化 AWS 环境的成本、安全性和性能AWS Trusted Advisor。

为 Lightsail 设置 AWS 账户 和管理用户

如果您是新 AWS 客户，请在开始使用 Amazon Lightsail 之前完成本页列出的设置先决条件。对于这些设置过程，您可以使用 AWS Identity and Access Management （ IAM ）服务。有关 IAM 的完整信息，请参阅《IAM 用户指南》。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in as the root user。
2. 为您的根用户启用多重身份验证（ MFA ）。

有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Enabling AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Add groups。

访问 Lightsail

您可以使用各种接口和服务终端节点访问 Amazon Lightsail。

主题

- Lightsail 服务接口
- Lightsail 服务端点
- 指定端点的示例

Lightsail 服务接口

您可以使用以下界面创建和管理 Lightsail 资源。

亚马逊 Lightsail 游戏机

一个用于创建和管理 Lightsail 实例和资源的简单网页界面。如果您已注册 AWS 帐户，则可以直接访问 Lightsail 控制台，也可以登录 AWS Management Console 并从主机主页选择 Lights ail。

AWS Command Line Interface

使您能够使用命令行 shell 中的命令与 AWS 服务进行交互。它在 Windows、Mac 和 Linux 上受支持。有关更多信息 AWS CLI，请参阅《AWS Command Line Interface 用户指南》。你可以在 C AWS LI 命令参考的 Lightsail 部分找到 Lightsail 命令。

AWS CloudShell

CloudShell 是一个基于浏览器、经过预先验证的 shell，您可以直接从启动。 AWS Management Console你可以使用你喜欢的外壳来运行 AWS CLI 命令，比如 Bash PowerShell、或 Z shell。有关如何使用 AWS CloudShell 来管理 Lightsail 资源的示例，请参阅。使用管理 Lightsail 资源 AWS CloudShell

查询 API

Lightsail 提供了一个查询 API。这些请求属于 HTTP 或 HTTPS 请求，需要使用 HTTP 动词 GET 或 POST 以及一个名为 `Action` 的查询参数。有关 Lightsail 的 API 操作的更多信息，请参阅《亚马逊 Lightsail API 参考》中的操作。

AWS SDKs

如果您更喜欢使用特定语言构建应用程序， APIs 而不是通过 HTTP 或 HTTPS 提交请求，请为软件开发人员 AWS 提供库、示例代码、教程和其他资源。这些库文件提供可自动执行任务的基本功

能，例如以加密方式对请求签名、重试请求和处理错误响应，以便您可以更轻松地上手。有关更多信息，请参阅用于在 AWS上进行构建的工具。

AWS Tools for PowerShell

一组基于公开的功能构建的 PowerShell 模块 适用于 .NET 的 SDK。这些工具 PowerShell 使您能够通过 PowerShell 命令行编写 AWS 资源操作脚本。要开始使用，请参阅 AWS Tools for PowerShell 用户指南。你可以在 Cmdlet 参考中找到 Lightsail 的 cmdlet。AWS Tools for PowerShell

Lightsail 服务端点

端点是用作 AWS Web 服务入口点的 URL。对于前面描述的接口中的编程访问方法，Lightsail 支持以下端点类型：

- IPv4 端点
- 双栈端点（同时支持 IPv4 和 IPv6）

当您发出请求时，您可以指定要使用的端点。如果您未指定终端节点，则默认使用该 IPv4 终端节点。要使用不同的端点类型，您必须在请求中指定。

IPv4 端点

IPv4 端点仅支持 IPv4 流量。 IPv4 终端节点适用于所有区域。有关区域服务终端节点的更多信息，请参阅各区域的服务终端节点。

IPv4 端点名称使用以下命名约定：

- *service*.*region*.amazonaws.com

例如，该us-east-2区域的 IPv4 终端节点名称为lightsail.us-east-2.amazonaws.com。

双栈（IPv4 和 IPv6）端点

双栈端点同时支持 IPv4 和 IPv6 流量。当您向双栈终端节点发出请求时，终端节点 URL 会解析为 IPv6 或 IPv4 地址，具体取决于您的网络和客户端使用的协议。

- lightsail.*region*.api.aws

例如，us-east-2 区域的双堆栈端点名称是 lightsail.us-east-2.api.aws。

各区域的服务终端节点

以下是 Lightsail 的服务端点。有关 Lightsail 可用区域的更多信息，请参阅。Lightsail 的区域和可用区

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	lightsail.us-east-2.amazonaws.com lightsail.us-east-2.api.aws	HTTPS HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	lightsail.us-east-1.amazonaws.com lightsail.us-east-1.api.aws	HTTPS HTTPS
美国西部（俄勒冈州）	us-west-2	lightsail.us-west-2.amazonaws.com lightsail.us-west-2.api.aws	HTTPS HTTPS
亚太地区（孟买）	ap-south-1	lightsail.ap-south-1.amazonaws.com lightsail.ap-south-1.api.aws	HTTPS HTTPS
亚太地区（首尔）	ap-northeast-2	lightsail.ap-northeast-2.amazonaws.com lightsail.ap-northeast-2.api.aws	HTTPS HTTPS
亚太地区（新加坡）	ap-southeast-1	lightsail.ap-southeast-1.amazonaws.com lightsail.ap-southeast-1.api.aws	HTTPS HTTPS
亚太地区（悉尼）	ap-southeast-2	lightsail.ap-southeast-2.amazonaws.com lightsail.ap-southeast-2.api.aws	HTTPS HTTPS
亚太地区（东京）	ap-northeast-1	lightsail.ap-northeast-1.amazonaws.com lightsail.ap-northeast-1.api.aws	HTTPS HTTPS

区域名称	区域	端点	协议
加拿大（中部）	ca-central-1	lightsail.ca-central-1.amazonaws.com	HTTPS
		lightsail.ca-central-1.api.aws	HTTPS
欧洲地区（法兰克福）	eu-central-1	lightsail.eu-central-1.amazonaws.com	HTTPS
		lightsail.eu-central-1.api.aws	HTTPS
欧洲地区（爱尔兰）	eu-west-1	lightsail.eu-west-1.amazonaws.com	HTTPS
		lightsail.eu-west-1.api.aws	HTTPS
欧洲地区（伦敦）	eu-west-2	lightsail.eu-west-2.amazonaws.com	HTTPS
		lightsail.eu-west-2.api.aws	HTTPS
欧洲地区（巴黎）	eu-west-3	lightsail.eu-west-3.amazonaws.com	HTTPS
		lightsail.eu-west-3.api.aws	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	lightsail.eu-north-1.amazonaws.com	HTTPS
		lightsail.eu-north-1.api.aws	HTTPS

指定端点的示例

本节提供了一些在发出请求时如何指定端点的示例。

> **Note**
>
> 如果您未指定终端节点，则默认使用该 IPv4 终端节点。

AWS CLI

以下示例说明如何使用为该`us-east-2`区域指定终端节点 AWS CLI。

- IPv4

```
aws lightsail get-regions --region us-east-2 --endpoint-url https://lightsail.us-east-2.amazonaws.com
```

- 双堆栈

```
aws lightsail get-regions --region us-east-2 --endpoint-url https://lightsail.us-east-2.api.aws
```

AWS SDK for Java 2.x

以下示例说明如何使用为该us-east-2区域指定终端节点 AWS SDK for Java 2.x。

- IPv4

```
LightsailClient client = LightsailClient.builder()
    .region(Region.US_EAST_2)
    .endpointOverride(URI.create("https://lightsail.us-east-2.amazonaws.com"))
    .build();
```

- 双堆栈

```
LightsailClient client = LightsailClient.builder()
    .region(Region.US_EAST_2)
    .endpointOverride(URI.create("https://lightsail.us-east-2.api.aws"))
    .build();
```

适用于 Java 的 AWS SDK 1.x

以下示例说明如何使用 适用于 Java 的 AWS SDK 1.x 为该us-east-2区域指定终端节点。

- IPv4

```
AmazonLightsail lightsail = AmazonLightsailClientBuilder.standard()
     .withEndpointConfiguration(new EndpointConfiguration(
          "https://lightsail.us-east-2.amazonaws.com",
          "us-east-2"))
     .build();
```

- 双堆栈

```
AmazonLightsail lightsail = AmazonLightsailClientBuilder.standard()
     .withEndpointConfiguration(new EndpointConfiguration(
          "https://lightsail.us-east-2.api.aws",
          "us-east-2"))
     .build();
```

AWS SDK for Go

以下示例说明如何使用为该us-east-2区域指定终端节点 适用于 Go 的 AWS SDK。

- IPv4

```
sess := session.Must(session.NewSession())
svc := lightsail.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast2RegionID),
    Endpoint: aws.String("https://lightsail.us-east-2.amazonaws.com")
})
```

- 双堆栈

```
sess := session.Must(session.NewSession())
svc := lightsail.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast2RegionID),
    Endpoint: aws.String("https://lightsail.us-east-2.api.aws")
})
```

Lightsail 上的虚拟专用服务器入门

在 Lightsail 中，实例是虚拟专用服务器（也称为虚拟机）。您可以在中创建和管理 Lightsail 实例。AWS Cloud在创建您的实例时，选择包含操作系统（OS）的映像。您也可以选择包含应用程序或开发堆栈 (包括基础 OS) 的实例映像。

您在本教程中创建的实例从您创建实例之时起一直产生使用费，直到您将其删除。删除是本教程的最后一步。有关定价的更多信息，请参阅 Lightsail 定价。

主题

- 步骤 1：完成先决条件
- 第 2 步：创建实例
- 步骤 3：连接到您的实例
- 步骤 4：向您的实例添加存储
- 步骤 5：创建快照
- 步骤 6：清除
- 后续步骤
- 将 Amazon Lightsail 与 AWS CLI

步骤 1：完成先决条件

如果您是新 AWS 客户，请在开始使用 Amazon Lightsail 之前完成设置前提条件。有关更多信息，请参阅 为 Lightsail 设置 AWS 账户 和管理用户。

第 2 步：创建实例

您可以使用 Lightsail 控制台创建实例，如以下过程所述。本教程旨在帮助您快速启动第一个实例。我们还建议您探索可用的应用程序和硬件计划。有关更多信息，请参阅 查看 Lightsail 实例蓝图产品。

1. 登录 Lightsail 控制台。
2. 在主页上，选择 Create instance（创建实例）。
3. 为您的实例选择一个位置（ AWS 区域 和可用区）。选择离您的实际位置最近的，以减少延迟。
   AWS 区域

选择变更 AWS 区域 和可用区在其他位置创建您的实例。

4. 选取一个应用程序（应用程序 + 操作系统）或操作系统（仅限操作系统）。

   要了解有关 Lightsail 实例图像的更多信息，请参阅。查看 Lightsail 实例蓝图产品

5. 选择实例计划。

   选择您的实例是使用双堆栈（IPv4 和 IPv6）还是 IPv6仅使用双堆栈（和）网络。有些 Lightsail 蓝图目前不支持 IPv6仅限联网。要查看哪些蓝图支持 IPv6仅限网络连接，请参阅。查看 Lightsail 实例蓝图产品

   你可以免费试用 5 美元的 Lightsail 套餐一个月（最长 750 小时）。我们将向您的账户免费提供一个月的积分。查看我们的 Lightsail 定价页面以了解更多信息。

6. 输入实例的名称。

   资源名称：

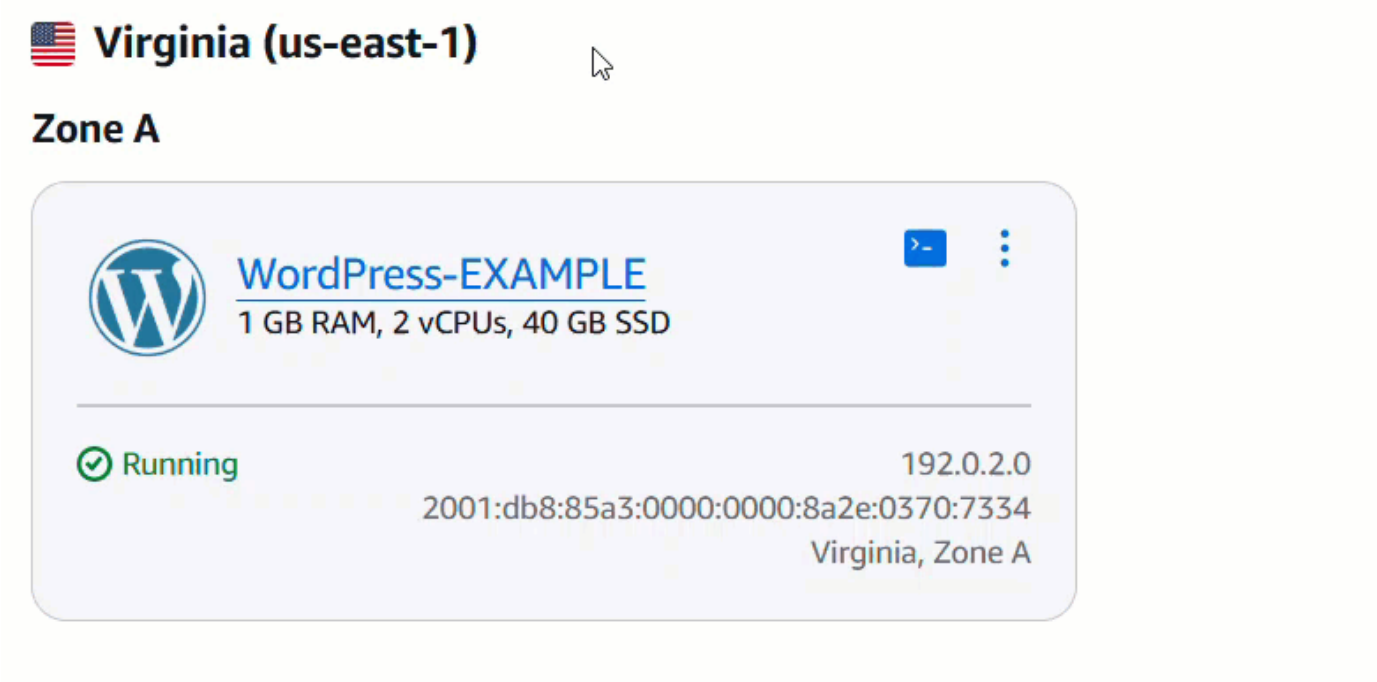
   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

7. 选择创建实例。

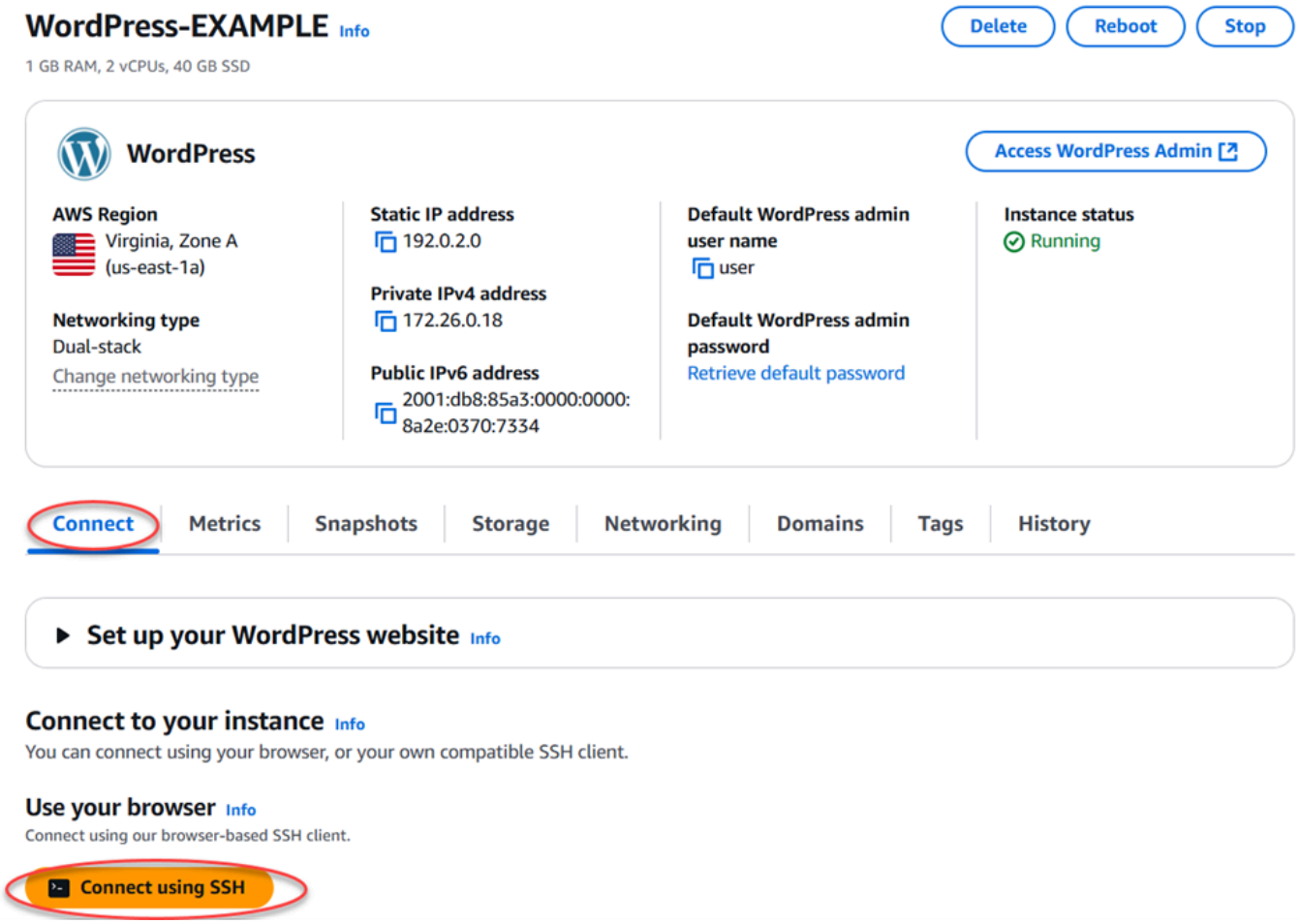
几分钟之内，你的 Lightsail 实例就准备好了，你可以连接到它了。

步骤 3：连接到您的实例

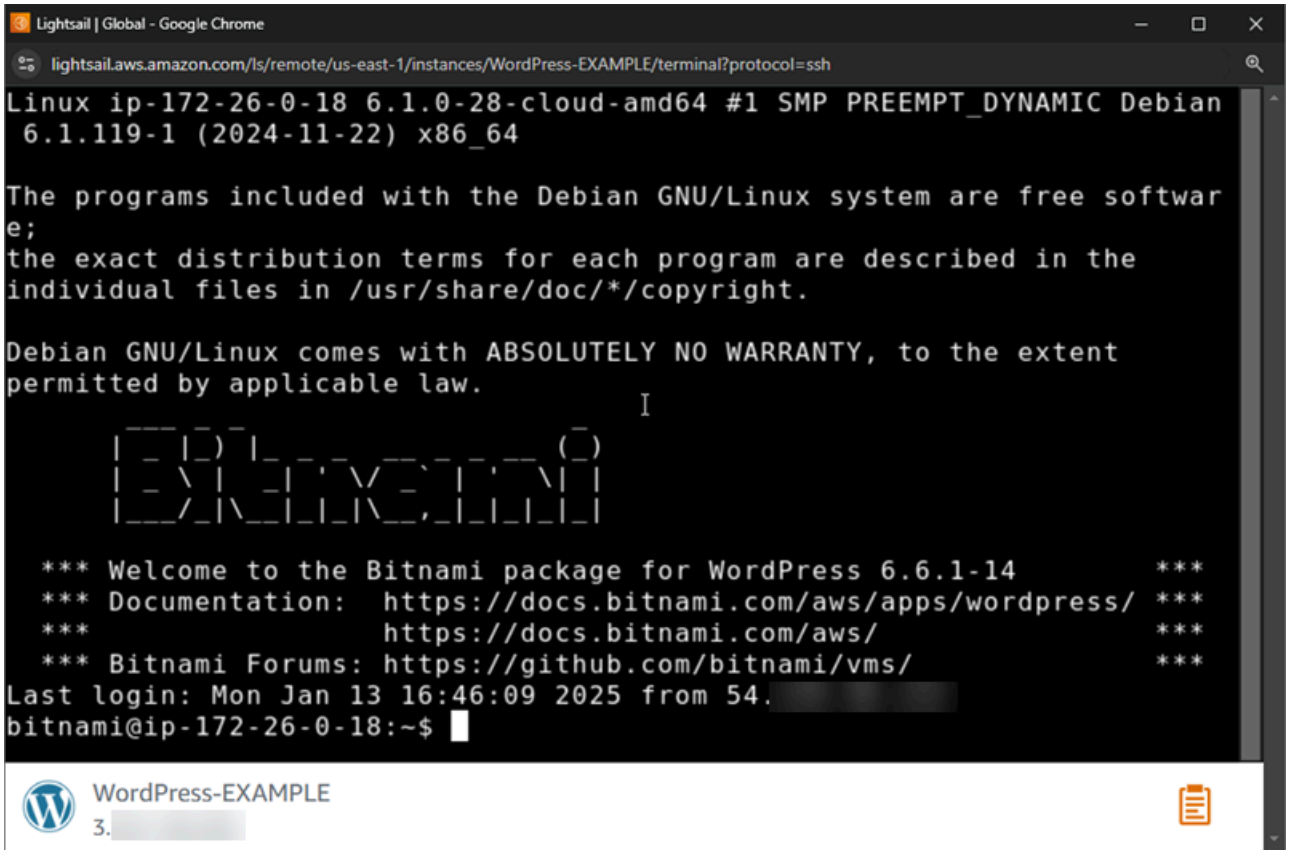
1. 在 Lightsail 主页上，选择操作菜单图标 ()，然后选择 Connect。



或者，您可以从实例的管理页面进行连接。选择您的实例名称，选择 Connect 选项卡，然后选择使用 SSH 连接。



2. 现在，您无需设置 SSH 客户端即可在终端中键入命令并管理 Lightsail 实例。



要了解如何连接虚拟计算机以添加额外的存储，请继续执行本教程的下一步骤。

步骤 4：向您的实例添加存储

Lightsail 提供了您可以连接到实例的块级存储卷（磁盘）。即使您的实例附带系统磁盘，您也可以根据需求的变化附加其他存储磁盘。您也可将磁盘从实例中分离，并将其附加到另一个实例。

创建其他磁盘后，您需要连接到 Lightsail 实例以格式化和装载该磁盘。

有关创建、附加和管理磁盘的更多信息，请参阅 创建 Lightsail 块存储磁盘并将其连接到 Linux 实例。

要了解备份虚拟计算机的信息，请继续执行本教程的下一步。

步骤 5：创建快照

快照是您的数据的 point-in-time副本。您可以创建实例的快照，并将其用作创建新实例或备份数据的基准。快照包含恢复实例所需的所有数据（从拍摄快照的那一刻开始）。

有关创建和管理快照的更多信息，请参阅 使用快照备份 Linux/Unix Lightsail 实例。

要了解清理虚拟计算机资源的信息，请继续执行本教程的下一步。

步骤 6：清除

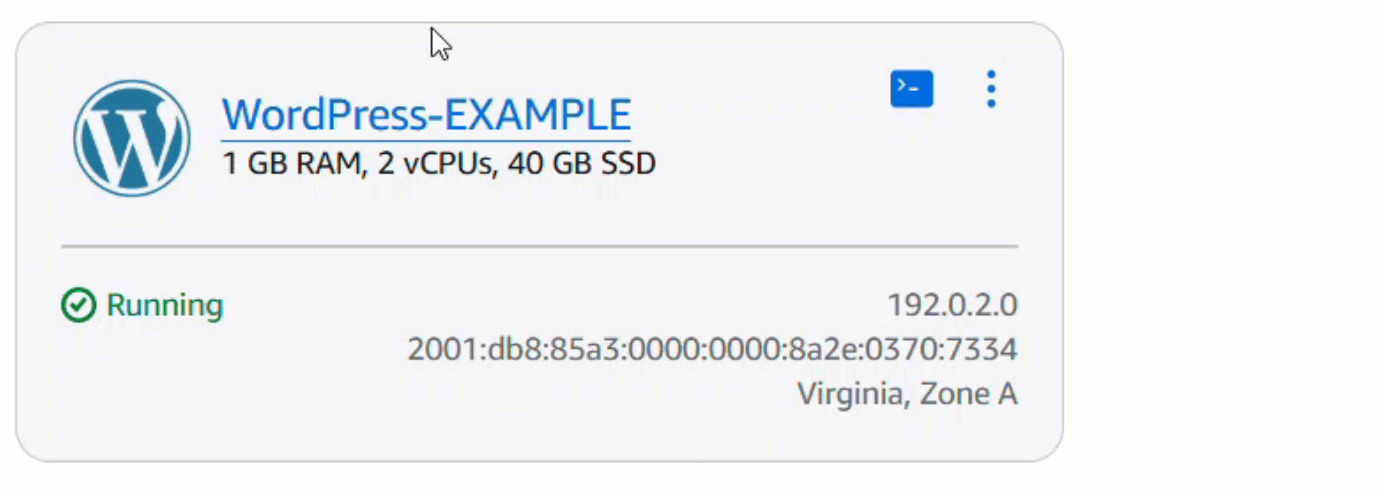
在完成使用为本教程创建的实例后，请将其删除。如果您不需要使用该实例，则删除实例后将不会产生费用。

删除实例并不会删除其关联的快照或附加磁盘。如果您为本教程创建了快照和磁盘，则还应将其删除。

为了保存实例以供将来使用但避免产生费用，您可以停止该实例，而不是删除它。稍后您可以重新启动。有关定价的更多信息，请参阅 Lightsail 定价。

> **Important**
>
> 删除 Lightsail 资源是一项永久性操作。删除的数据无法恢复。如果以后可能需要数据，请先创建虚拟计算机的快照，然后再删除它。有关更多信息，请参阅 使用快照备份 Linux/Unix Lightsail 实例。

1. 登录 Lightsail 控制台。
2. 在导航窗格中选择实例。
3. 针对要删除的实例，选择操作菜单图标 (⋮)，然后选择 Delete (删除)。



4. 选择是，删除以确认删除。

后续步骤

使用以下主题开始使用基于 Amazon Lightsail Linux 和 Windows 的实例。

- 在 Lightsail 上使用应用程序创建 Linux/Unix 实例
- 在 Lightsail 中创建 Windows 服务器实例

将 Amazon Lightsail 与 AWS CLI

本教程将指导你使用 AWS Command Line Interface ()AWS CLI完成常见的 Amazon Lightsail 操作。您将学习如何创建和管理 Lightsail 资源，包括密钥对、实例、存储和快照。

主题

- 先决条件
- 生成 SSH 密钥对
- 创建和管理实例
- 连接到您的实例
- 向您的实例添加存储空间
- 创建和使用快照
- 清理资源
- 后续步骤

先决条件

在开始本教程之前，请确保您已具备以下内容。

1. 的 AWS CLI。如果需要安装，请按照AWS CLI 安装指南进行操作。您也可以使用 AWS CloudShell，其中包括 AWS CLI。
2. 为你配置 AWS CLI 了相应的凭证。`aws configure`如果您尚未设置凭据，请运行。
3. 基本熟悉命令行界面和 SSH 概念。
4. 在您的 AWS 账户中创建和管理 Lightsail 资源的@@ 足够权限。

在开始之前，请将`AWS_REGION`环境变量设置为与您配置为使用的相同区域（如果尚未设置）。此环境变量用于在示例命令中为 Lightsail 资源指定可用区。 AWS CLI

```
$ [ -z "${AWS_REGION}" ] && export AWS_REGION=$(aws configure get region)
```

让我们开始使用 CLI 创建和管理 Amazon Lightsail 资源。

生成 SSH 密钥对

SSH 密钥对允许您在不使用密码的情况下安全地连接到 Lightsail 实例。在本节中，您将创建一个新的密钥对并检索其信息。

Example — 创建新的密钥对

以下命令创建一个名为 “cli-tutorial-keys” 的新 SSH 密钥对，并将私钥保存到本地计算机。

```
$ aws lightsail create-key-pair --key-pair-name cli-tutorial-keys \
        --query privateKeyBase64 --output text > ~/.ssh/cli-tutorial-keys.pem
$ chmod 400 ~/.ssh/cli-tutorial-keys.pem
```

运行此命令后，私钥将以适当的权限保存到您的`~/.ssh`目录中。该`chmod`命令可确保只有您才能读取私钥文件，这是 SSH 的安全要求。

Example — 检索密钥对信息

您可以通过检索密钥对的信息来验证密钥对是否已成功创建。

```
$ aws lightsail get-key-pair --key-pair-name cli-tutorial-keys
{
    "keyPair": {
        "name": "cli-tutorial-keys",
        "arn": "arn:aws:lightsail:us-east-2:123456789012:KeyPair/e00xmpl-6a6a-434a-
bff1-87f2bb815e21",
        "supportCode": "123456789012/cli-tutorial-keys",
        "createdAt": 1673596800.000,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-east-2"
        },
        "resourceType": "KeyPair",
        "tags": [],
        "fingerprint": "d0:0d:30:db:5a:24:df:f6:17:f0:e2:15:45:77:3d:bb:d0:6d:fc:81"
    }
}
```

输出显示有关您的密钥对的详细信息，包括其名称、ARN、创建时间、区域和指纹。连接到实例时，此指纹可用于验证密钥的真实性。

创建和管理实例

Lightsail 实例是运行应用程序或网站的虚拟专用服务器。在本节中，您将创建一个 WordPress 实例并检索其详细信息。

Example — 创建实 WordPress 例

以下命令使用nano_3_0捆绑包（最小的 Lightsail 实例大小）创建一个新 WordPress 实例，并将其与您的密钥对相关联。该命令使用AWS_REGION环境变量在您配置的区域的可用区中创建实例。

```
$ aws lightsail create-instances --instance-names cli-tutorial \
        --availability-zone ${AWS_REGION}a --blueprint-id wordpress \
        --bundle-id nano_3_0 --key-pair-name cli-tutorial-keys
{
    "operations": [
        {
            "id": "f30xmpl-3727-492a-9d42-5c94ad3ef9a8",
            "resourceName": "cli-tutorial",
            "resourceType": "Instance",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "isTerminal": false,
            "operationType": "CreateInstance",
            "status": "Started",
            "statusChangedAt": 1673596800.000
        }
    ]
}
```

响应表示实例创建操作已开始。您的实例可能需要几分钟才能变为可用。

Example — 获取实例详情

创建实例后，您可以使用以下命令检索其详细信息。

```
$ aws lightsail get-instance --instance-name cli-tutorial
{
```

```
    "instance": {
        "name": "cli-tutorial",
        "arn": "arn:aws:lightsail:us-east-2:123456789012:Instance/7d3xmpl-ae2e-44d5-
bbd9-22f9ec2abe1f",
        "supportCode": "123456789012/i-099cxmpl5dad5923c",
        "createdAt": 1673596800.000,
        "location": {
            "availabilityZone": "us-east-2a",
            "regionName": "us-east-2"
        },
        "resourceType": "Instance",
        "tags": [],
        "blueprintId": "wordpress",
        "blueprintName": "WordPress",
        "bundleId": "nano_3_0",
        "isStaticIp": false,
        "privateIpAddress": "172.26.6.136",
        "publicIpAddress": "203.0.113.75",
        "ipv6Addresses": [
            "2600:1f14:ab4:3800:ceef:89e2:f57:f25"
        ],
        "ipAddressType": "dualstack",
        "hardware": {
            "cpuCount": 2,
            "disks": [
                {
                    "createdAt": 1673596800.000,
                    "sizeInGb": 20,
                    "isSystemDisk": true,
                    "iops": 100,
                    "path": "/dev/xvda",
                    "attachedTo": "cli-tutorial",
                    "attachmentState": "attached"
                }
            ],
            "ramSizeInGb": 0.5
        },
        "networking": {
            "monthlyTransfer": {
                "gbPerMonthAllocated": 1024
            },
            "ports": [
                {
                    "fromPort": 80,
```

```
                    "toPort": 80,
                    "protocol": "tcp",
                    "accessFrom": "Anywhere (0.0.0.0/0 and ::/0)",
                    "accessType": "public",
                    "commonName": "",
                    "accessDirection": "inbound",
                    "cidrs": [
                        "0.0.0.0/0"
                    ],
                    "ipv6Cidrs": [
                        "::/0"
                    ],
                    "cidrListAliases": []
                },
                {
                    "fromPort": 22,
                    "toPort": 22,
                    "protocol": "tcp",
                    "accessFrom": "Anywhere (0.0.0.0/0 and ::/0)",
                    "accessType": "public",
                    "commonName": "",
                    "accessDirection": "inbound",
                    "cidrs": [
                        "0.0.0.0/0"
                    ],
                    "ipv6Cidrs": [
                        "::/0"
                    ],
                    "cidrListAliases": []
                },
                {
                    "fromPort": 443,
                    "toPort": 443,
                    "protocol": "tcp",
                    "accessFrom": "Anywhere (0.0.0.0/0 and ::/0)",
                    "accessType": "public",
                    "commonName": "",
                    "accessDirection": "inbound",
                    "cidrs": [
                        "0.0.0.0/0"
                    ],
                    "ipv6Cidrs": [
                        "::/0"
                    ],
```

```
                    "cidrListAliases": []
                }
            ]
        },
        "state": {
            "code": 16,
            "name": "running"
        },
        "username": "bitnami",
        "sshKeyName": "cli-tutorial-keys",
        "metadataOptions": {
            "state": "applied",
            "httpTokens": "optional",
            "httpEndpoint": "enabled",
            "httpPutResponseHopLimit": 1,
            "httpProtocolIpv6": "disabled"
        }
    }
}
```

输出提供了有关您的实例的全面信息，包括其 IP 地址、硬件规格、网络配置和状态。记下公有 IP 地址和用户名，因为您需要这些地址和用户名才能连接到您的实例。

连接到您的实例

创建实例后，您可以使用之前创建的密钥 pair 使用 SSH 连接到该实例。本节介绍如何建立 SSH 连接和管理安全设置。

Example — SSH 进入你的实例

使用以下命令通过 SSH 连接到您的实例，将 IP 地址替换为实例的公有 IP。

```
$ ssh -i ~/.ssh/cli-tutorial-keys.pem bitnami@203.0.113.75
Linux ip-172-26-6-136 6.1.0-32-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1
 (2025-03-06) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
       ___ _ _                   _
```

```
      | _ |_) |_ _ _  __ _ _ __ (_)
      | _ \ |  _| ' \/ _` | '  \| |
      |___/_|\__|_|_|\__,_|_|_|_|_|

  *** Welcome to the Bitnami package for WordPress 6.7.2           ***
  *** Documentation:  https://docs.bitnami.com/aws/apps/wordpress/ ***
  ***                 https://docs.bitnami.com/aws/                ***
  *** Bitnami Forums: https://github.com/bitnami/vms/              ***

bitnami@ip-172-26-6-136:~$ df
Filesystem      1K-blocks    Used Available Use% Mounted on
udev               217920       0    217920   0% /dev
tmpfs               45860     480     45380   2% /run
/dev/nvme0n1p1   20403592 3328832  16142256  18% /
tmpfs              229292       0    229292   0% /dev/shm
tmpfs                5120       0      5120   0% /run/lock
/dev/nvme0n1p15    126678   11840    114838  10% /boot/efi
tmpfs               45856       0     45856   0% /run/user/1000
```

连接后，您可以管理 WordPress 安装、配置服务器或安装其他软件。上面的示例使用df命令显示了实例的磁盘使用情况。

Example — 关闭公共端口

当您不使用 SSH 时，可以关闭实例上的公共端口。这有助于保护您的实例免受未经授权的访问尝试。

```
$ aws lightsail close-instance-public-ports --instance-name cli-tutorial \
        --port-info fromPort=22,protocol=TCP,toPort=22
{
    "operation": {
        "id": "6cdxmpl-9f39-4357-a66d-230096140b4f",
        "resourceName": "cli-tutorial",
        "resourceType": "Instance",
        "createdAt": 1673596800.000,
        "location": {
            "availabilityZone": "us-east-2a",
            "regionName": "us-east-2"
        },
        "isTerminal": true,
        "operationDetails": "22/tcp",
        "operationType": "CloseInstancePublicPorts",
        "status": "Succeeded",
        "statusChangedAt": 1673596800.000
```

```
    }
}
```

> **Note**
>
> 关闭端口 22 会阻止所有 SSH 连接，包括从 Lightsail 控制台启动的连接。有关更多信息，请参阅以下主题。
>
> - 管理 SSH 密钥对并连接到你的 Lightsail 实例
> - 在 Lightsail 中使用防火墙控制实例流量

响应确认端口 22 已成功关闭。当你需要通过 SSH 重新连接时，你可以使用`open-instance-public-ports`命令重新打开端口。

向您的实例添加存储空间

随着应用程序的增长，您可能需要额外的存储空间。Lightsail 允许您创建其他磁盘并将其连接到您的实例。本节演示如何添加额外的存储空间。

Example — 创建磁盘

以下命令创建一个新的 32GB 磁盘。

```
$ aws lightsail create-disk --disk-name cli-tutorial-disk \
        --availability-zone ${AWS_REGION}a --size-in-gb 32
{
    "operations": [
        {
            "id": "070xmpl-3364-4aa2-bff2-3c589de832fc",
            "resourceName": "cli-tutorial-disk",
            "resourceType": "Disk",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "isTerminal": false,
            "operationType": "CreateDisk",
            "status": "Started",
            "statusChangedAt": 1673596800.000
```

```
        }
    ]
}
```

响应表示磁盘创建操作已开始。磁盘可能需要一段时间才能变为可用。

Example — 将磁盘连接到您的实例

创建磁盘后，您可以使用以下命令将其连接到您的实例。

```
$ aws lightsail attach-disk --disk-name cli-tutorial-disk \
        --disk-path /dev/xvdf --instance-name cli-tutorial
{
    "operations": [
        {
            "id": "d17xmpl-2bdb-4292-ac63-ba5537522cea",
            "resourceName": "cli-tutorial-disk",
            "resourceType": "Disk",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "isTerminal": false,
            "operationDetails": "cli-tutorial",
            "operationType": "AttachDisk",
            "status": "Started",
            "statusChangedAt": 1673596800.000
        },
        {
            "id": "01exmpl-c04e-42d4-aa6b-45ce50562a54",
            "resourceName": "cli-tutorial",
            "resourceType": "Instance",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "isTerminal": false,
            "operationDetails": "cli-tutorial-disk",
            "operationType": "AttachDisk",
            "status": "Started",
            "statusChangedAt": 1673596800.000
        }
```

```
    ]
}
```

磁盘路径参数指定磁盘在 Linux 文件系统中的连接位置。挂载磁盘后，您需要将其格式化并从实例中挂载。

Example — 验证磁盘附件

您可以通过检索磁盘的详细信息来确认磁盘是否已正确连接。

```
$ aws lightsail get-disk --disk-name cli-tutorial-disk
{
    "disk": {
        "name": "cli-tutorial-disk",
        "arn": "arn:aws:lightsail:us-east-2:123456789012:Disk/1a9xmpl-8a34-46a4-
b87e-19184f0cca9c",
        "supportCode": "123456789012/vol-0dacxmplc1c3108e2",
        "createdAt": 1673596800.000,
        "location": {
            "availabilityZone": "us-east-2a",
            "regionName": "us-east-2"
        },
        "resourceType": "Disk",
        "tags": [],
        "sizeInGb": 32,
        "isSystemDisk": false,
        "iops": 100,
        "path": "/dev/xvdf",
        "state": "in-use",
        "attachedTo": "cli-tutorial",
        "isAttached": true,
        "attachmentState": "attached"
    }
}
```

输出确认磁盘已连接到您的实例。“状态” 字段显示 “正在使用”，“isAttacted” 设置为 true，表示连接成功。

创建和使用快照

快照提供了一种备份实例并利用备份创建新实例的方法。这对于灾难恢复、测试或创建重复环境非常有用。

Example — 创建实例快照

以下命令创建您的实例的快照。

```
$ aws lightsail create-instance-snapshot --instance-name cli-tutorial \
        --instance-snapshot-name cli-tutorial-snapshot
{
    "operations": [
        {
            "id": "41bxmpl-7824-4591-bfcc-1b1c341613a4",
            "resourceName": "cli-tutorial-snapshot",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            },
            "isTerminal": false,
            "operationDetails": "cli-tutorial",
            "operationType": "CreateInstanceSnapshot",
            "status": "Started",
            "statusChangedAt": 1673596800.000
        },
        {
            "id": "725xmpl-158e-46f6-bd49-27b0e6805aa2",
            "resourceName": "cli-tutorial",
            "resourceType": "Instance",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "isTerminal": false,
            "operationDetails": "cli-tutorial-snapshot",
            "operationType": "CreateInstanceSnapshot",
            "status": "Started",
            "statusChangedAt": 1673596800.000
        }
    ]
}
```

响应表示快照过程已启动。获取快照的实例有一个异步操作，一个用于正在创建的快照的异步操作。快照包括连接到该实例的所有磁盘。

Example — 从快照创建新实例

快照完成后，您可以使用它来创建新实例。

```
$ aws lightsail create-instances-from-snapshot --availability-zone ${AWS_REGION}b \
        --instance-snapshot-name cli-tutorial-snapshot --instance-name cli-tutorial-bup
 --bundle-id small_3_0
{
    "operations": [
        {
            "id": "a35xmpl-efa1-4d6c-958e-9d58fd258f5f",
            "resourceName": "cli-tutorial-bup",
            "resourceType": "Instance",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "us-east-2b",
                "regionName": "us-east-2"
            },
            "isTerminal": false,
            "operationType": "CreateInstancesFromSnapshot",
            "status": "Started",
            "statusChangedAt": 1673596800.000
        }
    ]
}
```

此命令us-east-2b使用small_3_0捆绑包大小cli-tutorial-bup在可用区中创建一个名为的新实例。请注意，您可以为新实例选择不同的捆绑包大小，这对于向上或向下扩展非常有用。

清理资源

使用 Lightsail 资源后，应将其删除，以免产生额外费用。本节向您展示如何清理本教程中创建的所有资源。

Example — 删除实例快照

要删除不再需要的快照，请使用以下命令。

```
$ aws lightsail delete-instance-snapshot --instance-snapshot-name cli-tutorial-snapshot
{
    "operations": [
        {
```

```
            "id": "cf8xmpl-0ec7-43ec-9cbc-6dedd9d8eda8",
            "resourceName": "cli-tutorial-snapshot",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            },
            "isTerminal": true,
            "operationDetails": "",
            "operationType": "DeleteInstanceSnapshot",
            "status": "Succeeded",
            "statusChangedAt": 1673596800.000
        }
    ]
}
```

响应确认快照删除操作已成功。

Example — 删除实例

要删除实例，请使用以下命令。

```
$ aws lightsail delete-instance --instance-name cli-tutorial
{
    "operations": [
        {
            "id": "f4bxmpl-2df1-4740-90d7-e30adaf7e3a1",
            "resourceName": "cli-tutorial",
            "resourceType": "Instance",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "isTerminal": true,
            "operationDetails": "",
            "operationType": "DeleteInstance",
            "status": "Succeeded",
            "statusChangedAt": 1673596800.000
        }
    ]
}
```

记得删除您创建的所有实例，包括通过快照创建的所有实例。

Example — 删除磁盘

要删除不再需要的磁盘，请使用以下命令。

```
$ aws lightsail delete-disk --disk-name cli-tutorial-disk
{
    "operations": [
        {
            "id": "aacxmpl-8626-4edd-8b3b-bf108d6b279c",
            "resourceName": "cli-tutorial-disk",
            "resourceType": "Disk",
            "createdAt": 1673596800.000,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "isTerminal": true,
            "operationDetails": "",
            "operationType": "DeleteDisk",
            "status": "Succeeded",
            "statusChangedAt": 1673596800.000
        }
    ]
}
```

如果磁盘已连接到实例，则需要先使用detach-disk命令将其分离。

Example — 删除密钥对

最后，删除您在本教程开头创建的密钥对。

```
$ aws lightsail delete-key-pair --key-pair-name cli-tutorial-keys
{
    "operation": {
        "id": "dbfxmpl-c954-4a45-93a4-ab3e627d2c23",
        "resourceName": "cli-tutorial-keys",
        "resourceType": "KeyPair",
        "createdAt": 1673596800.000,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-east-2"
```

```
        },
        "isTerminal": true,
        "operationDetails": "",
        "operationType": "DeleteKeyPair",
        "status": "Succeeded",
        "statusChangedAt": 1673596800.000
    }
}
```

此命令仅从中删除 key pair AWS。现在，您也可以删除本地副本。

```
$ rm ~/.ssh/cli-tutorial-keys.pem
```

后续步骤

既然你已经学习了使用管理 Lightsail 资源的基础知识，那就 AWS CLI来探索其他 Lightsail 功能吧。

1. 域名-为您的应用程序分配域名。
2. 负载均衡器-将流量路由到多个实例，以提高容量和弹性。
3. 自动快照-自动备份您的应用程序数据。
4. 指标-监控资源的运行状况，获取通知并设置警报。
5. 数据库-将您的应用程序连接到关系数据库。

有关可用 AWS CLI 命令的更多信息，请参阅 Lightsa AWS CLI il 的命令参考。

Lightsail 经销商

您可以成为亚马逊 Lightsail 的注册经销商，向自己的客户提供 Lightsail 产品。作为 Lightsail 经销商，可以为 Lightsail 实例提供更高的默认配额，并且能够使用注册经销商专有的控制台内反馈表。

主题

- 转售 Lightsail 的好处
- Lightsail 经销商权益和增加的默认配额如何适用于您的账户
- 如何成为 Lightsail 经销商
- 成为 Lightsail 经销商
- 申请增加经销商账户的服务配额
- 以经销商身份联系 Lightsail

转售 Lightsail 的好处

成为 Lightsail 经销商可为 Lightsail 资源在扩展、预算和获得帮助方面带来各种好处。

在 Lightsail 上扩展您的业务

作为经销商，您可以在Lightsail的全球云基础架构上更快地扩展业务。借助经销商权益，默认情况下，您将在 AWS 区域 每个注册账户中为 Lightsail 实例提供更高的服务配额。

简化您的预算

Lightsail具有可预测的定价模式，即内存、vCPU和固态硬盘 (SSD) 存储作为捆绑计划提供。该模型使您可以轻松预测随着业务增长的成本，并利用Lightsail的大规模资源管理业务。

可靠性

借助诸如数据自动快照、针对违反配置阈值的资源发出警报和通知以及 IPv6网络支持等功能，提高资源的运营效率和可靠性。

Lightsail 经销商权益和增加的默认配额如何适用于您的账户

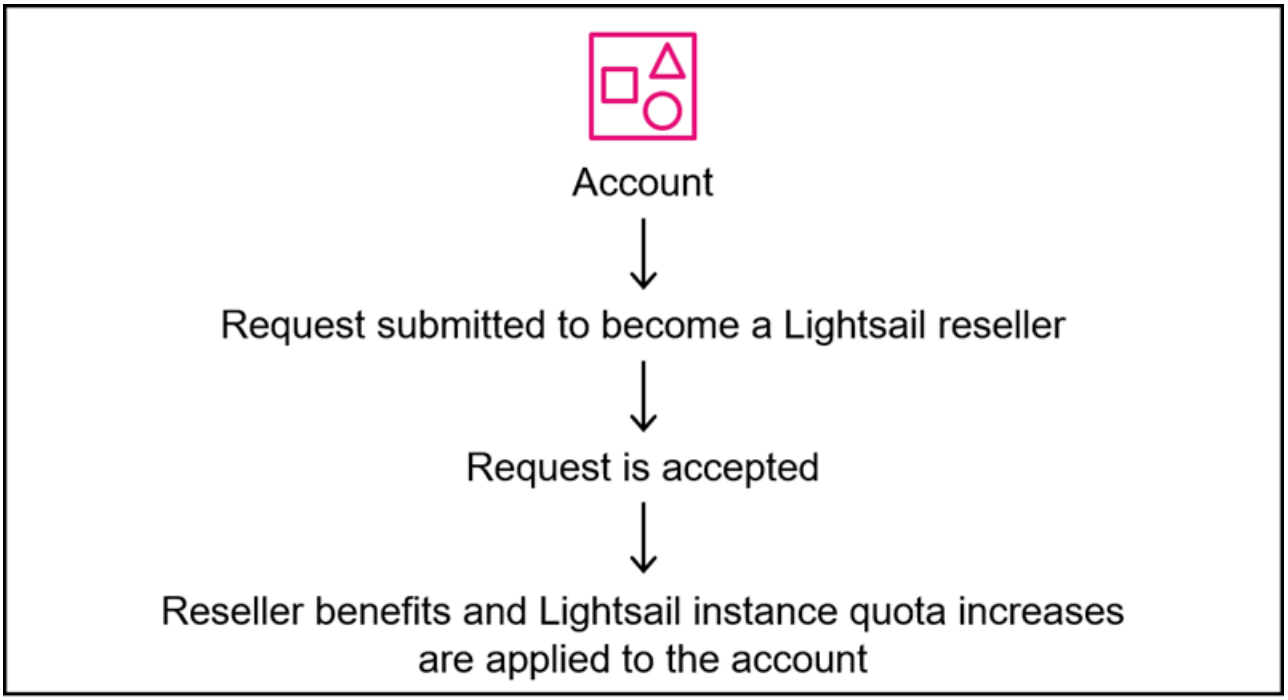
经销商权益适用于 AWS 账户 您提交请求的人。如果您的请求获得批准，则可以请求添加更多 AWS 账户 以增加默认 Lightsail 实例配额。如果您使用 AWS Organizations，则经销商权益和增加的默认 Lightsail 实例配额适用于您的管理账户。对于成员账户，Lightsail 实例的默认配额将增加。有关

Organizations 的更多信息，请参阅什么是 AWS Organizations？ 在《AWS Organizations 用户指南》中。

下图说明了 Lightsail 经销商的好处和增加的默认 Lightsail 实例配额是如何适用的。 AWS 账户

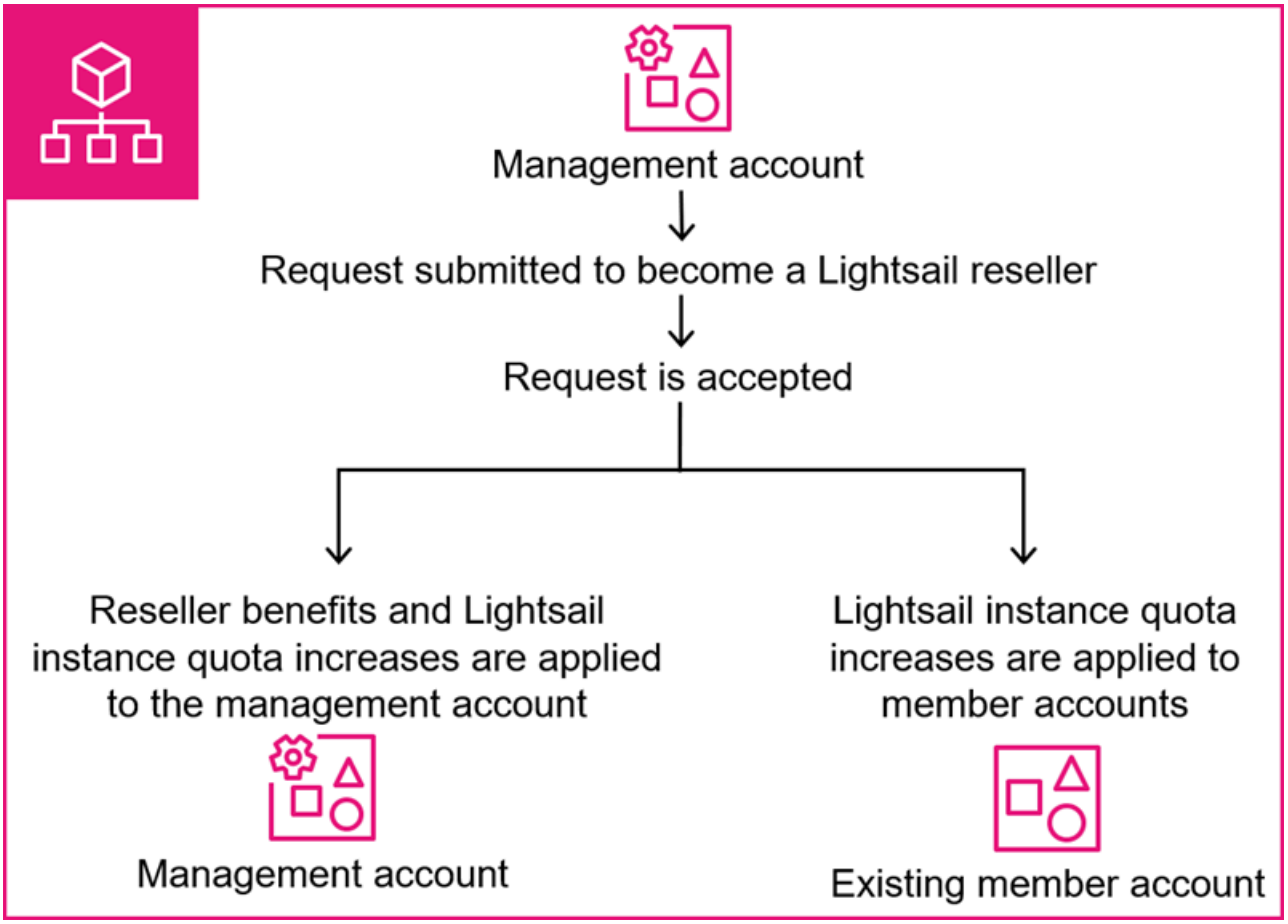
单曲 AWS 账户

下图详细说明了外部的单个账户 AWS Organizations 成为 Lightsail 经销商时会发生的情况。



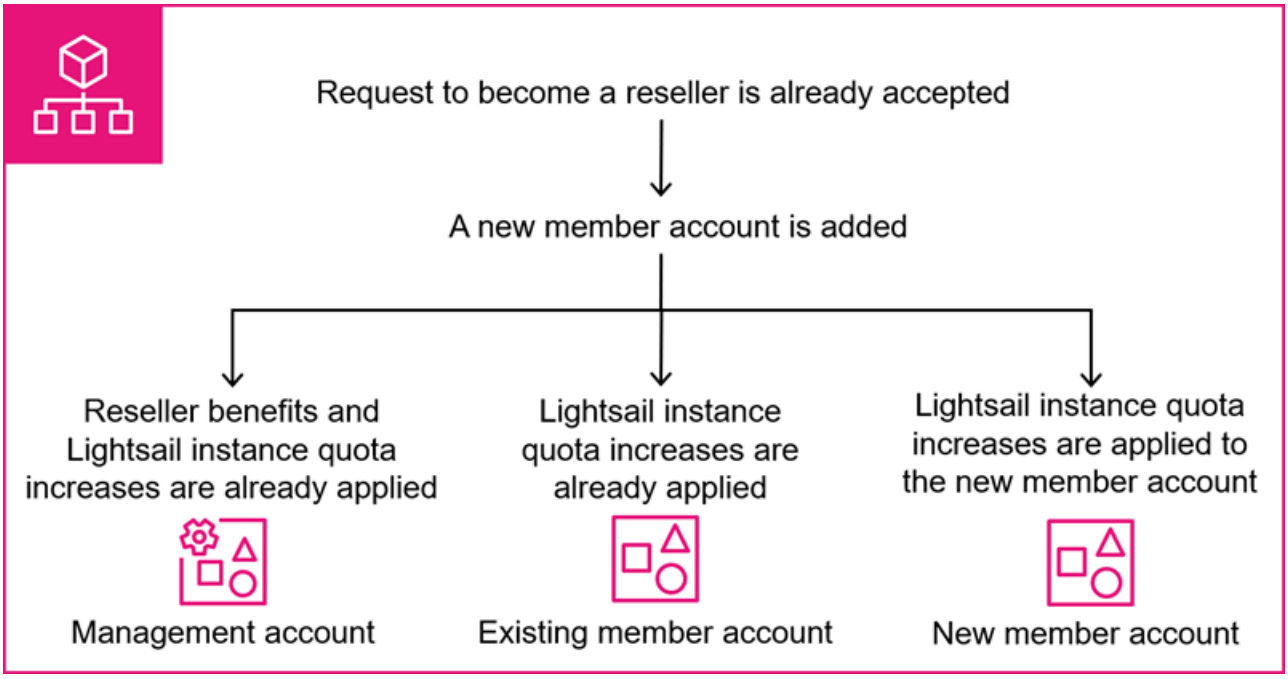
AWS 账户 在组织中

下图详细说明了中的管理账户 AWS Organizations 成为 Lightsail 经销商时会发生的情况。



AWS 账户 在成为经销商后添加的 Organizations

下图详细说明了向您的组织添加新成员帐户时会发生的情况，而该组织的管理帐户已注册为 Lightsail 经销商。



如何成为 Lightsail 经销商

要继续，您需要提交一份表格，详细说明成为Lightsail经销商的业务需求。有关更多信息，请参阅 成为 Lightsail 经销商。

成为 Lightsail 经销商

您必须提交一份表格，才能考虑成为 Amazon Lightsail 经销商。申请将使用您在填写表单时登录时所用的提交。 AWS 账户 如果您使用 AWS Organizations 帮助集中管理您的 AWS 账户，则应在使用管理账户成为经销商的同时提交申请。通过使用您的管理账户，您可以增加组织中各个成员账户的默认 Lightsail 实例配额。有关 Lightsail 经销商权益如何影响您的 AWS 账户更多信息，请参阅。Lightsail 经销商权益和增加的默认配额如何适用于您的账户

如果您的请求获得批准，并且您有多个组织，则可以再提交一份请求以添加每个组织的管理账户的 AWS 账户 ID，以便将增加的默认 Lightsail 实例配额也扩展到这些组织的成员账户。有关 Organizations 的更多信息，请参阅什么是 AWS Organizations？ 在《AWS Organizations 用户指南》中。

主题

- 成为 Lightsail 经销商所需的信息
- 申请成为 Lightsail 经销商
- 申请其他账户成为 Lightsail 经销商

成为 Lightsail 经销商所需的信息

我们将需要一些有关您的计划使用情况和用例的信息，以便考虑您申请成为 Amazon Lightsail 经销商。Lightsail 控制台上有一份表格可供您填写并提交以供考虑。除了有关您的业务的详细信息外，您还应提供以下信息来填写表格：

- 您计划使用的 Lightsail 资源的实例捆绑包的大小和数量。有关可用捆绑包的更多信息，请参阅亚马逊 Light sail 定价。
- AWS 账户 IDs 你想注册的。如果您正在使用 AWS Organizations，则只应在请求中指定您的管理账户。这也会在组织中注册相应的成员帐户。有关更多信息，请参阅《AWS Organizations 用户指南》AWS Organizations中的术语和概念。

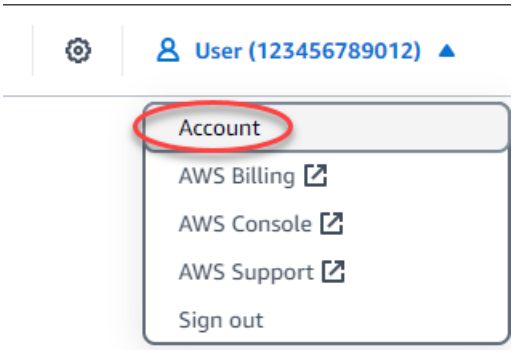
申请成为 Lightsail 经销商

以下步骤将提交成为经销商的申请。您通过身份验证的 AWS 账户 ID 将用作您想要获得经销商权益的账户。如果您的申请获得批准，则可以申请添加其他账户。

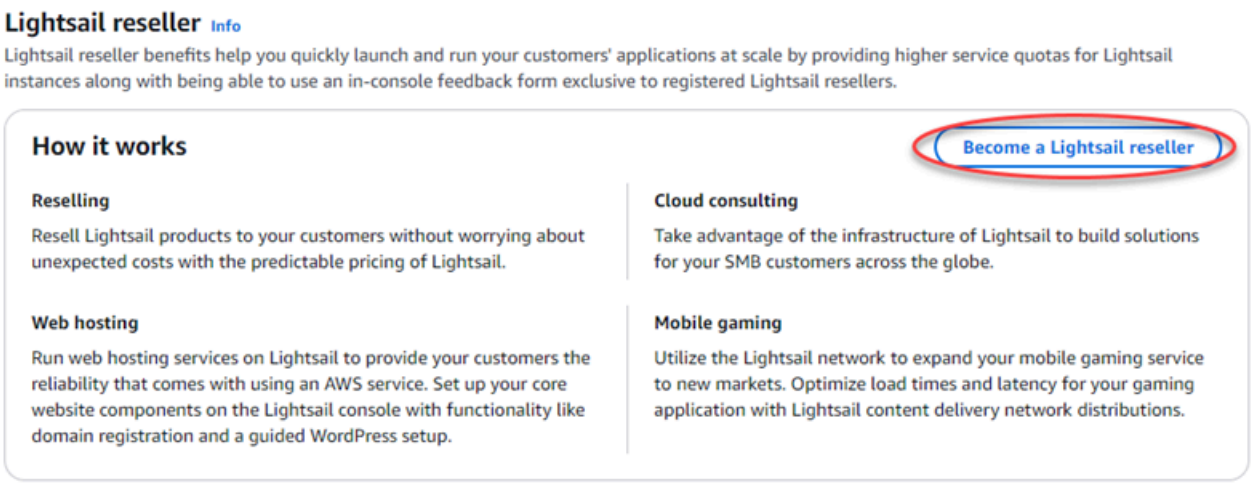
> **Tip**
>
> 如果您正在使用 AWS Organizations，则应以组织管理账户的身份执行此过程，这样您的成员账户还能获得更高的默认 Lightsail 实例配额。

申请成为经销商

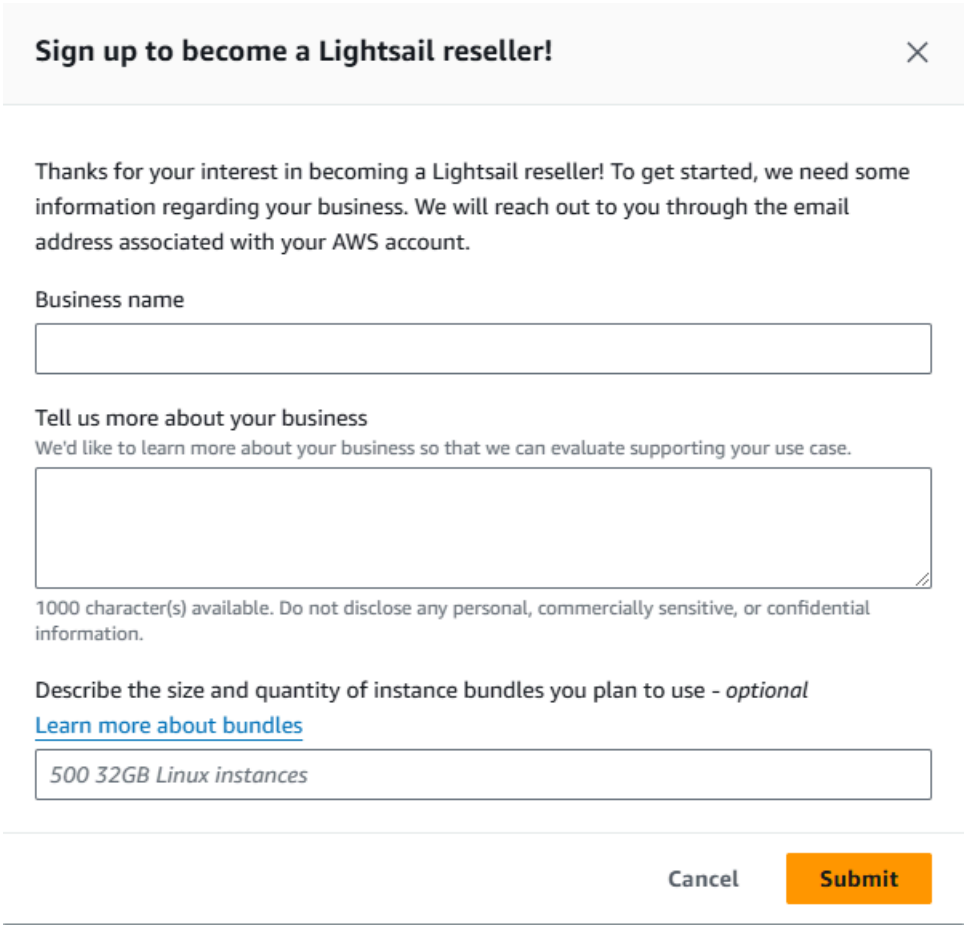
1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 在 “个人资料” 选项卡上的 Lightsail 经销商部分下，选择 “成为 Light sail 经销商”。

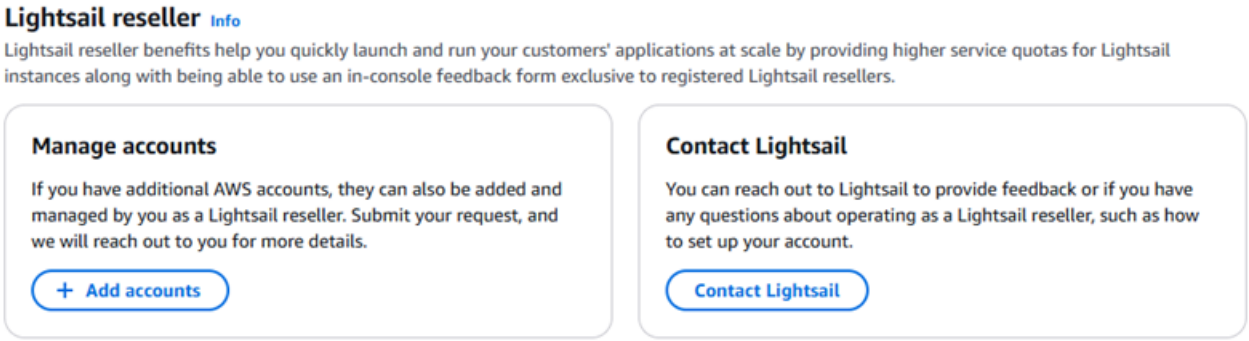


5. 在注册表上，在字段中输入您的信息，然后选择提交。



您将在账户的电子邮件中收到一封确认信，确认您有兴趣成为经销商。如果您的申请获得批准，Lightsail 控制台中的 “帐户” 页面将有一个经过修改的 Lightsail 经销商部分，其中包含管理您的经销商账户以及以 Lightsa il 经销商身份联系 Lightsail 团队以获取反馈或查询的选项。只有提交申请成为

Lightsail 经销商的账户才能看到此部分。您还将获得更高的 Lightsail 实例服务配额，并且可以申请增加额外的 AWS 账户 服务配额以成为 Lightsail 经销商。



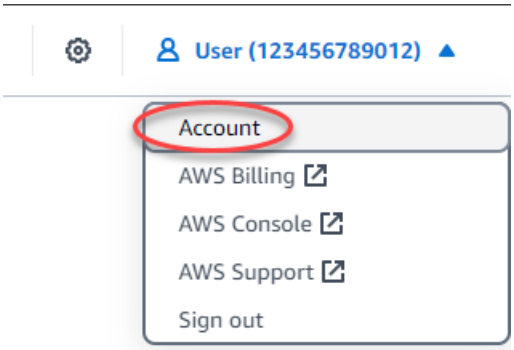
申请其他账户成为 Lightsail 经销商

以下步骤将提交其他人成为经销商 AWS 账户 的申请。

> **Tip**
>
> 如果您正在使用 AWS Organizations，则应将管理账户指定为 AWS 账户 要添加的。这种方法可以将增加的默认 Lightsail 实例配额扩展到管理账户组织中的所有成员账户。

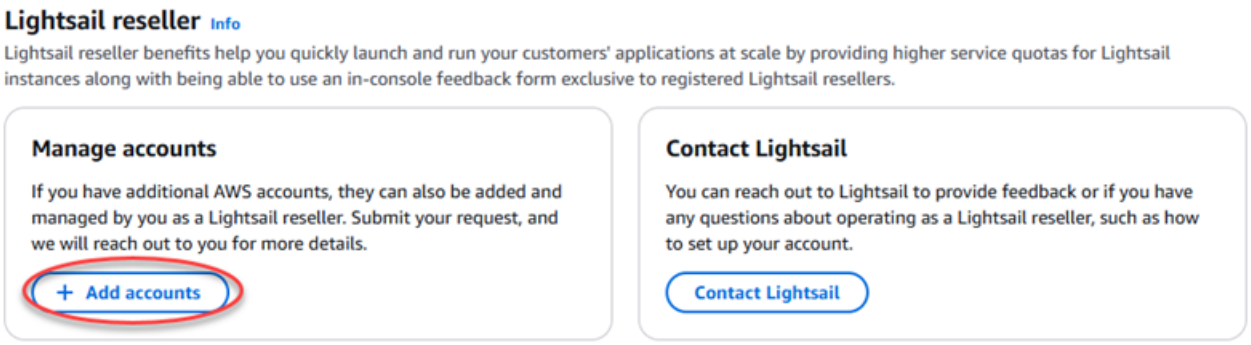
申请其他账户成为 Lightsail 经销商

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



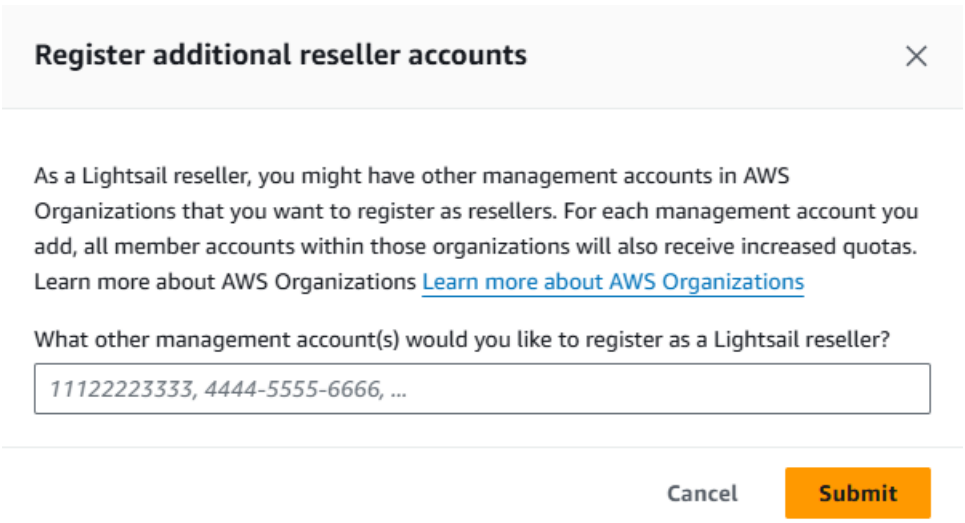
4. 在 “个人资料” 选项卡上的 Lightsail 经销商部分中，选择 “添加账户”。

> **Important**
>
> “添加账户” 操作仅适用于申请成为 Lightsail 经销商并已被接受的账户。



5. 在注册表中，输入您要注册的组织的任何其他帐户 AWS 账户 IDs 或管理帐户。

> **Note**
>
> 如果您使用的是 Organizations，则无需申请您的成员帐户。



6. 选择提交。

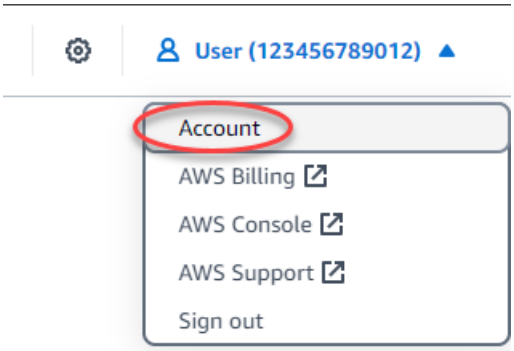
申请增加经销商账户的服务配额

一旦您成为 Amazon Lightsail 经销商，您的组织中当前账户和任何成员账户的 Lightsail 实例的默认服务配额将增加。如果您想进一步提高成员账户的限额，则应使用以下流程申请增加配额。您可以从 Lightsail 控制台查看当前配额并申请增加配额。

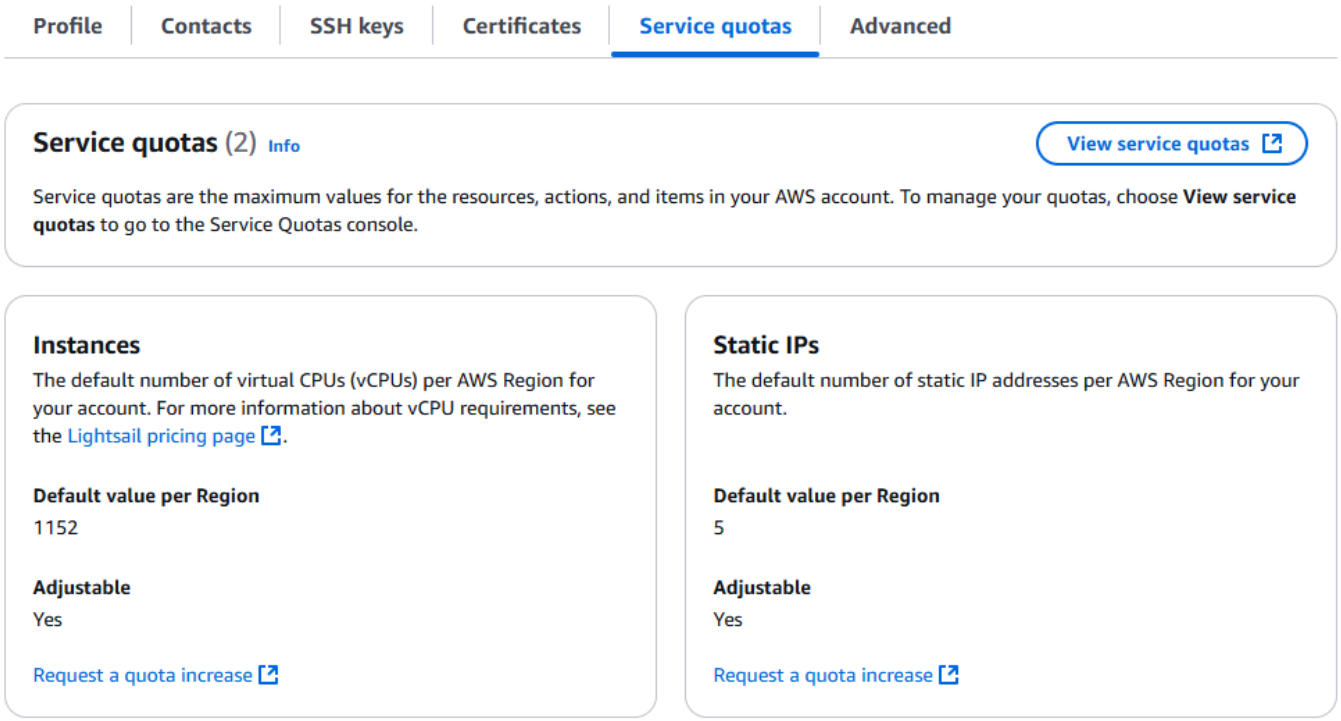
> **Note**
>
> 对于关联到 Lightsail 经销商账户的多个成员账户，您应使用经销商反馈表申请增加服务配额。有关更多信息，请参阅 以经销商身份联系 Lightsail。

申请增加经销商账户的服务配额

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 选择 “服务配额” 选项卡。
5. 对于要增加的配额，请选择申请增加配额。



6. 在 Service Quotas 控制台上，选择在账户级别申请增加配额。
7. 对于增加配额值，请输入数量。
8. 要提交您的请求，请选择请求。

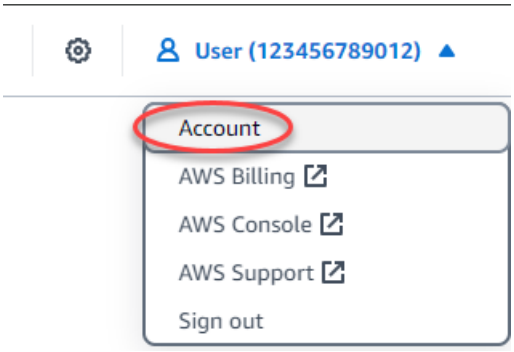
提交配额增加请求后，您可能会生成一个 支持 案例，您可以监控其是否有更新。如果增加获得批准，它将适用于您每个地区的所有经销商账户。有关未列出的配额增加情况，请参阅以经销商身份联系 Lightsail。

以经销商身份联系 Lightsail

作为亚马逊 Lightsail 经销商，您可以直接从 Lightsail 控制台联系 Lightsail 团队，询问有关您作为经销商所做努力的问题或反馈。您也可以通过这种方式请求在组织中的成员账户中增加 Lightsail 的服务配额。

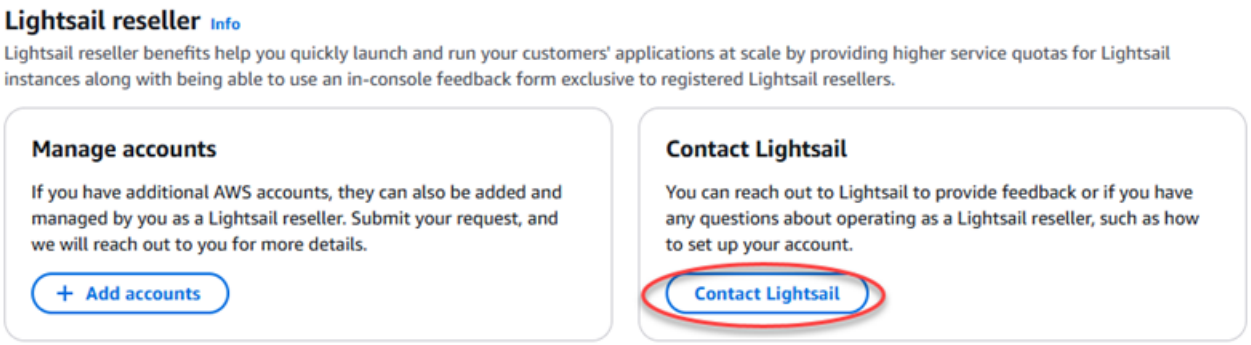
联系 Lightsail 团队

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。

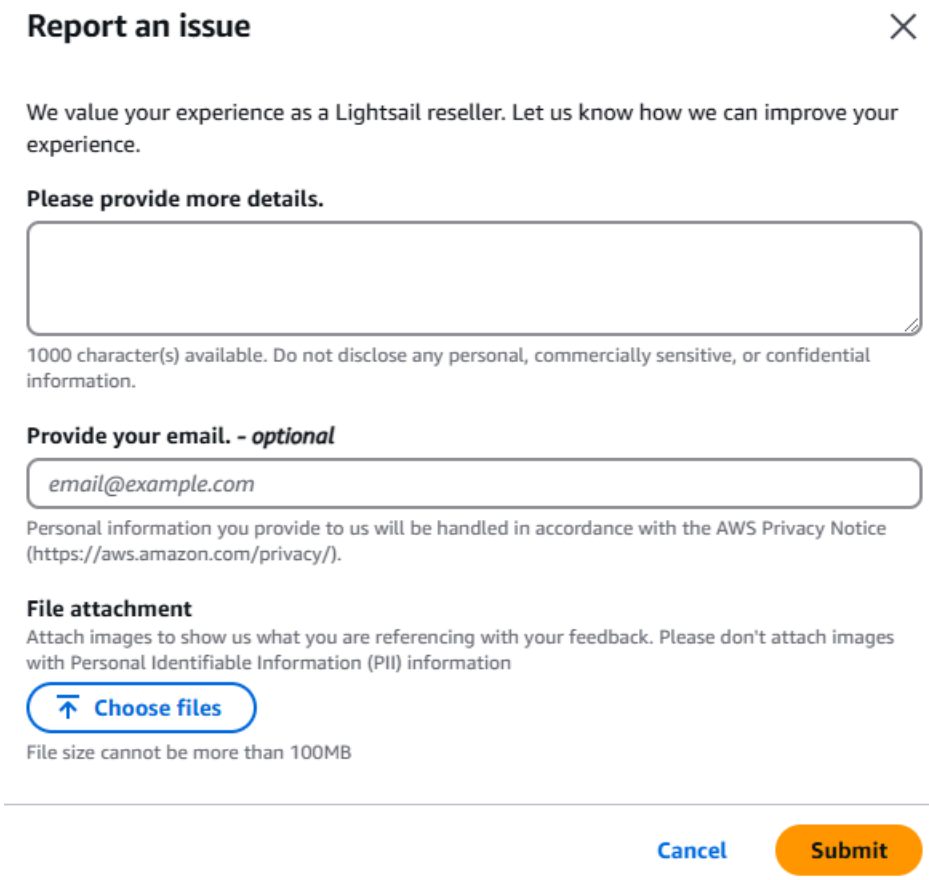


4. 在 “个人资料” 选项卡上的 Lightsail 经销商部分中，选择 “联系 Light sail”。

> **Important**
>
> Con tact Lightsail 操作仅适用于申请成为 Lightsail 经销商并已被接受的账户。有关更多信息，请参阅 成为 Lightsail 经销商。



5. 填写您的请求的必填字段。如果您请求增加 Lightsail 的服务配额，则可以指定多个成员账户。



6. 选择提交。

如果您提供电子邮件地址，我们可能会就您的反馈与您联系。

Lightsail 中的虚拟专用服务器实例

您的 Lightsail 实例是一个虚拟专用服务器（也称为虚拟机）。在创建您的实例时，选择包含操作系统 (OS) 的映像。您也可以选择包含应用程序或开发堆栈 (包括基础 OS) 的实例映像。

有关操作系统、应用程序和开发框架的完整列表，请参阅选择 Lightsail 实例镜像。

有关实例的更多信息，请参阅以下主题：

主题

- 创建 Lightsail 实例
- 查看 Lightsail 实例蓝图产品
- 在 Lightsail 中使用防火墙控制实例流量
- 检测 Lightsail 实例爆发以获得最佳性能
- 连接并管理你的 Lightsail 实例
- 删除 Lightsail 实例
- 管理 SSH 密钥对并连接到你的 Lightsail 实例
- 在 Lightsail 中访问实例元数据服务 (IMDS) 和用户数据

创建 Lightsail 实例

本节涵盖以下与在 Amazon Lightsail 中创建实例相关的主题：

主题

- 在 Lightsail 上使用应用程序创建 Linux/Unix 实例
- 在 Lightsail 中创建 Windows 服务器实例

在 Lightsail 上使用应用程序创建 Linux/Unix 实例

创建一个基于 Linux/UNIX 的 Amazon Lightsail 实例（虚拟私有服务器），运行类似的 WordPress 应用程序或像 LAMP 这样的开发堆栈。在您的实例开始运行后，您无需离开 Lightsail 即可通过 SSH 连接到该实例。方法如下。

要创建基于 Windows 的实例，请参阅 Amazon Lightsail 中基于 Windows 的实例入门。

创建基于 Linux 的实例

1. 在主页上，选择 Create instance（创建实例）。
2. 为您的实例选择一个位置（ AWS 区域 和可用区）。

   选择变更 AWS 区域 和可用区在其他位置创建您的实例。
3. （可选）您可以更改可用区。

   选择更改您的可用区。
4. 选择 Linux 平台。
5. 选取一个应用程序（Apps + OS（应用 + 操作系统））或操作系统（OS Only（仅限操作系统））。

   要了解有关 Lightsail 实例镜像的更多信息，请参阅选择亚马逊 Lightsail 实例镜像。
6. 选择实例计划。

   选择您的实例是使用双堆栈（IPv4 和 IPv6）还是 IPv6仅使用双堆栈（和）网络。有些 Lightsail 蓝图目前不支持 IPv6仅限联网。要查看哪些蓝图支持 IPv6仅限网络连接，请参阅。查看 Lightsail 实例蓝图产品

   你可以免费试用 5 美元的 Lightsail 套餐一个月（最长 750 小时）。我们将向您的账户免费提供一个月的积分。查看我们的 Lightsail 定价页面以了解更多信息。

   > **Note**
   >
   > 作为 AWS 免费套餐的一部分，您可以免费开始使用特定实例捆绑包的 Amazon Lightsail。有关更多信息，请参阅亚马逊 Lightsail 定价页面上的AWS 免费套餐。
7. 输入实例的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
8. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

a. 对于密钥，输入标签密钥。



b. （可选）在“值”中，输入标签值。



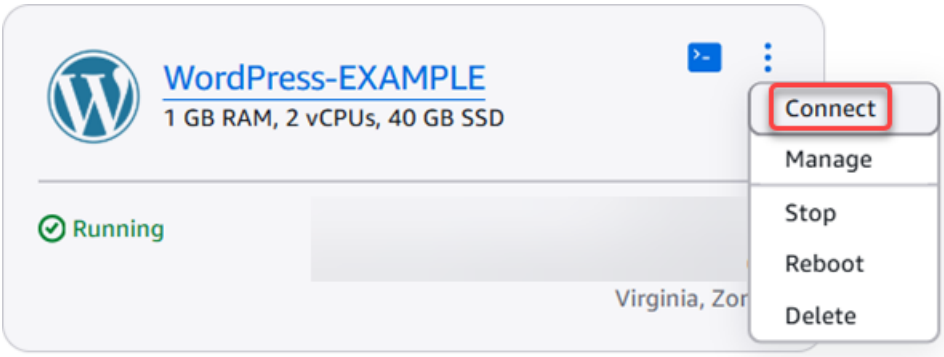
9. 选择创建实例。

有关高级创建选项，请参阅使用启动脚本在 Amazon Lightsail 实例启动时对其进行配置或为基于 Linux/UNIX 的 Lightsail 实例设置 SSH。

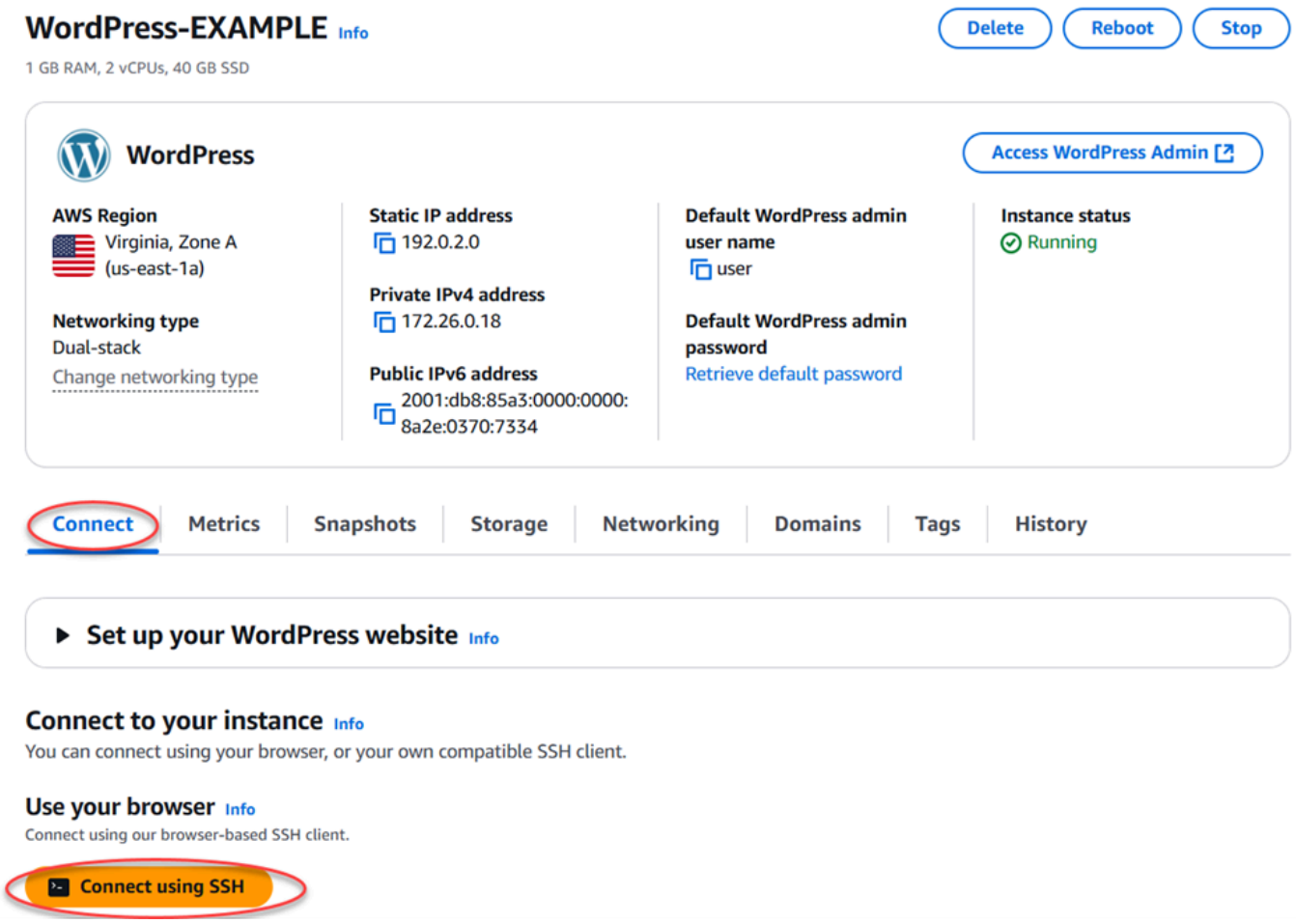
几分钟之内，你的 Lightsail 实例就准备好了，你可以通过 SSH 连接到它，而无需离开 Lightsail！

连接到您的实例

1. 在 Lightsail 主页上，选择实例名称右侧的菜单，然后选择 Connect。

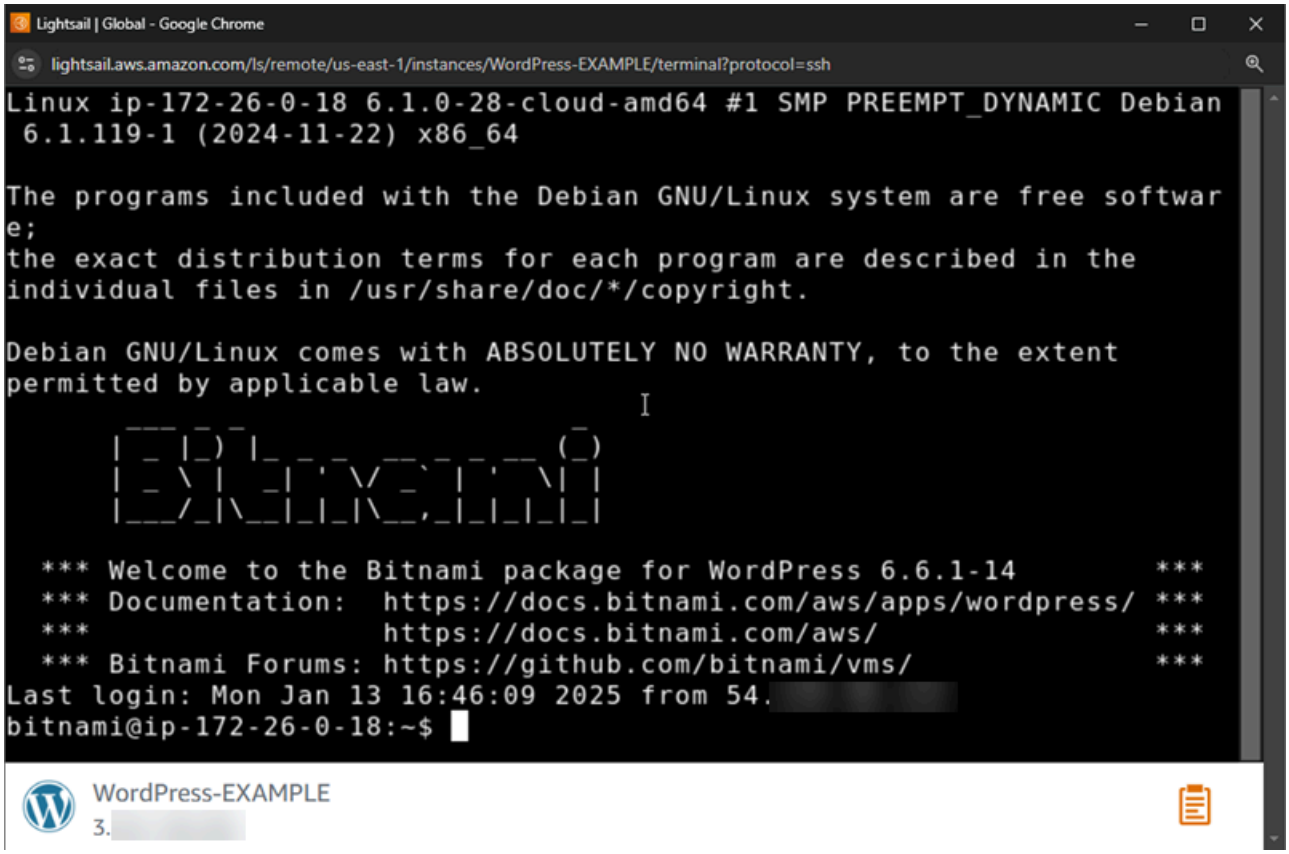


或者，您可以打开您的实例管理页面，选择 Connect 选项卡，然后选择使用 SSH 连接。



> **Note**
>
> 要使用 PuTTY 等 SSH 客户端连接到您的实例，您可以按照以下步骤操作：设置 PuTTY 以连接到您的 Light sail 实例。

2. 现在，您无需设置 SSH 客户端即可在终端中键入命令并管理 Lightsail 实例。



后续步骤

现在，您可以连接到您的实例，而您的下一步操作取决于您计划如何使用它。例如：

- 如果您正在创建博客，则使用 the section called “WordPress”。
- 为您的实例@@ 创建一个静态 IP 地址，以便每次重启 Lightsail 实例时都保持相同的 IP 地址。
- 创建实例的快照作为备份。

在 Lightsail 中创建 Windows 服务器实例

创建运行 Windows 服务器操作系统 (OS) 的 Lightsail 实例。我们提供了三个操作系统蓝图：Windows Server 2022、Windows Server 2019 和 Windows Server 2016。此外，我们还提供预配置了 SQL Server 2022、2019 和 2016 Express 的蓝图。

本主题提供了有关选择软件、创建基于 Windows Server 的实例以及连接到该实例的信息。

了解有关亚马逊云科技上的 Windows Server 的更多信息

选择基于 Windows Server 的实例

在 Lightsail 中创建基于 Windows 服务器的实例有三个选项。

Windows Server 2022

运行 Windows Server 的 Lightsail 是一个使用微软 Web 平台部署应用程序的快速而可靠的环境。借助 Lightsail，你可以在高性能、可靠、经济实惠的计算平台上运行任何兼容的基于 Windows 的解决方案。 AWS Cloud 常见的 Windows 应用场景包括基于 Windows 的企业应用程序托管、网站和 Web 服务托管、数据处理、分布式测试、ASP.NET 应用程序托管以及任何其他需要 Windows 软件的应用程序。

了解有关 Windows Server 2022 镜像的更多信息

Windows Server 2019

除非您由于某种原因需要运行 Windows Server 2016 或 Windows Server 2019，否则，我们建议您使用最新版本的 Windows Server 2022。

运行 Windows Server 的 Lightsail 是一个使用微软 Web 平台部署应用程序的快速而可靠的环境。Lightsail 使您能够在 AWS“高性能、可靠、经济实惠的云计算平台” 上运行任何兼容的基于 Windows 的解决方案。常见的 Windows 使用案例包括基于 Windows 的企业应用程序托管、网站和 Web 服务托管、数据处理、分布式测试、ASP.NET 应用程序托管以及任何其他需要 Windows 软件的应用程序。

了解有关 Windows Server 2019 镜像的更多信息

Windows Server 2016

除非您由于某种原因需要运行 Windows Server 2016 或 Windows Server 2019，否则，我们建议您使用最新版本的 Windows Server 2022。

运行 Windows Server 的 Lightsail 是一个使用微软 Web 平台部署应用程序的快速而可靠的环境。Lightsail 使您能够在 AWS 的高性能、可靠、经济实惠的云计算平台上运行任何兼容的基于 Windows 的解决方案。常见的 Windows 使用案例包括基于 Windows 的企业应用程序托管、网站和 Web 服务托管、数据处理、分布式测试、ASP.NET 应用程序托管以及任何其他需要 Windows 软件的应用程序。

了解有关 Windows Server 2016 镜像的更多信息

SQL Server Express 2022

SQL Server Express 是一个可免费下载、分发和使用的关系数据库管理系统。它包含专门针对嵌入式和小型应用程序的数据库。这张 Lightsail 镜像在 Windows Server 2022 的基础操作系统上运行。

了解有关 SQL Server Express 2022 映像的更多信息

SQL Server Express 2019

SQL Server Express 是一个可免费下载、分发和使用的关系数据库管理系统。它包含专门针对嵌入式和小型应用程序的数据库。这张 Lightsail 镜像在 Windows Server 2022 的基础操作系统上运行。

了解有关 SQL Server Express 2019 映像的更多信息

SQL Server Express 2016

SQL Server Express 是一个可免费下载、分发和使用的关系数据库管理系统。它包含专门针对嵌入式和小型应用程序的数据库。这张 Lightsail 镜像在 Windows Server 2016 的基本操作系统上运行。

了解有关 SQL Server Express 镜像的更多信息

创建基于 Windows Server 的实例

你可以使用 Lightsail 控制台或使用 () 创建基于 Windows 服务器的实例 AWS Command Line Interface 。AWS CLI

使用控制台创建实例

1. 登录 Lightsail，然后进入主页。
2. 选择创建实例。
3. 选择要 AWS 区域 在哪里创建基于 Windows 服务器的 Lightsail 实例。

   例如，`Ohio (us-east-2)`。
4. 选择 Microsoft Windows 平台。
5. 要选择 Windows Server 2022、Windows Server 2019、Windows Server 2016 蓝图，请选择仅限操作系统。

要选择 SQL Server Express 蓝图，请选择 Apps + OS（应用 + 操作系统）。

6. 选择实例计划。

   选择您的实例是使用双堆栈（IPv4 和 IPv6）还是 IPv6仅使用双堆栈（和）网络。有些 Lightsail 蓝图目前不支持 IPv6仅限联网。要查看哪些蓝图支持 IPv6仅限网络连接，请参阅。查看 Lightsail 实例蓝图产品

   计划还包括较低的可预测成本和计算机配置（RAM、SSD、vCPU）以及数据传输。

   > **Note**
   >
   > 有些实例计划不适用于某些蓝图。例如，SQL Server Express 蓝图要求您使用至少具有 4 GB 内存和 80 GB 固态硬盘存储空间的计划。

7. 输入实例的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

8. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

   a. 对于密钥，输入标签密钥。

   b. （可选）在“值”中，输入标签值。

9. 选择创建实例。

要使用创建实例 AWS CLI

1. 如果尚未安装并配置 AWS CLI，请执行该操作。

   有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface
2. 打开命令提示符或终端窗口。
3. 如果您尚未执行此操作，请配置 AWS CLI 使用`aws configure`并选择要创建 Lightsail 资源 AWS 区域 的位置。
4. 键入以下 AWS CLI 命令创建在俄亥俄州地区运行的每月价值 44 美元的 Windows Server 2022 实例：

   ```
   aws lightsail create-instances --instance-names InstanceName --availability-zone
    us-east-2a --blueprint-id windows_server_2022 --bundle-id medium_win_3_0
   ```

   在命令中，*InstanceName*用新实例的名称替换。

   如果成功，将会看到 AWS CLI的以下输出。

   ```
   {
       "operations": [
           {
               "status": "Started",
               "resourceType": "Instance",
               "isTerminal": false,
               "statusChangedAt": 1508086226.4,
               "location": {
                   "availabilityZone": "us-east-2a",
                   "regionName": "us-east-2"
               },
               "operationType": "CreateInstance",
               "resourceName": "my-windows-instance",
               "id": "344acdc8-f9c4-4eda-8232-12345EXAMPLE",
               "createdAt": 1508086225.467
           }
       ]
   }
   ```

> **Note**
>
> 要获取可用的蓝图列表，请使用 get-blueprints 命令。要获取可用的包列表，请使用 get-bundles 命令。详细了解如何使用get-instance-access-details命令获取实例的密码。

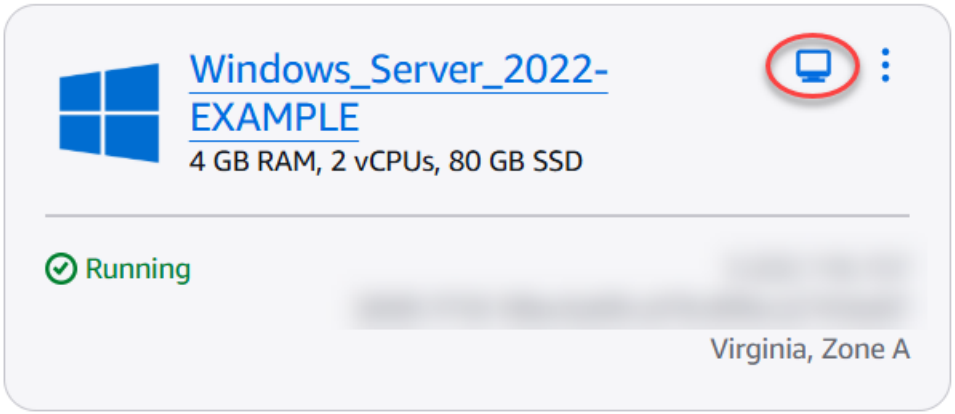
连接到您的实例

创建基于 Windows 服务器的 Lightsail 实例后，您可以使用基于浏览器的 RDP 客户端或您选择的远程桌面客户端连接到该实例。

> **Note**
>
> 在创建您的实例后，您可能最多需要等待 15 分钟的时间，然后才能连接到该实例。

使用基于 Lightsail 浏览器的 RDP 客户端进行连接

1. 在主页上，选择您的实例旁边的 Connect using RDP（使用 RDP 连接）图标。

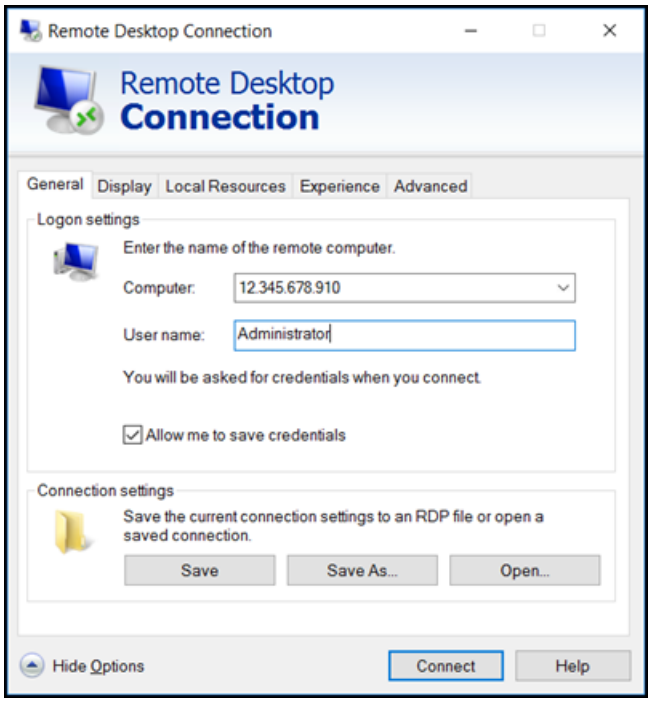


2. 或者，您也可以从快捷菜单或实例管理页面中连接到您的实例。

使用您自己的 RDP 客户端进行连接

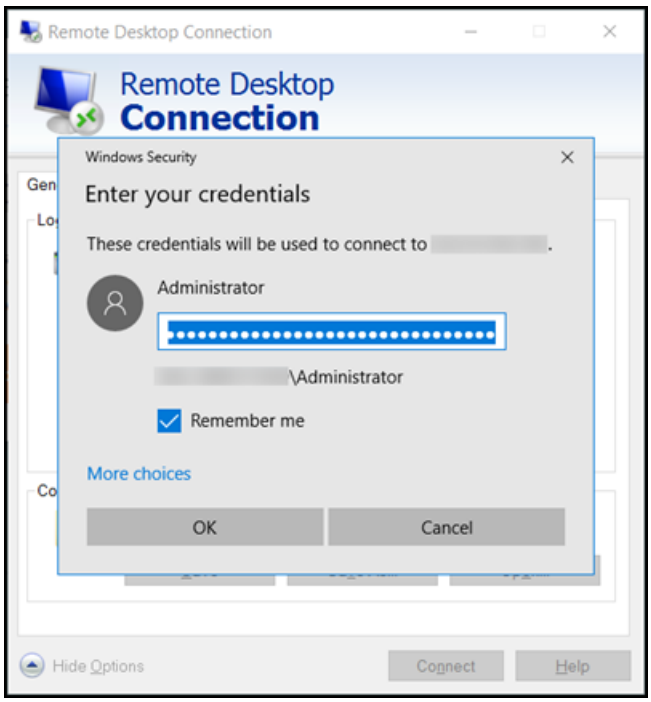
1. 要获取你的 IP 地址，请前往 Lightsail 主页。
2. 将 IP 地址复制到剪贴板。
3. 在 Windows 中打开一个 RDP 客户端，如远程桌面连接。
4. 将 IP 地址粘贴到 Computer（计算机）字段中。

5. 选择 Show Options（显示选项），然后键入 `Administrator` 作为 User name（用户名）。



6. 选择连接。
7. 要获取密码，请前往 Lightsail 中的实例管理页面。

   在 Lightsail 主页上选择实例名称（或从快捷菜单中选择 “管理”），即可进入实例管理页面。
8. 选择 Show default password（显示默认密码）。
9. 将默认密码复制到剪贴板中。
10. 将您的密码粘贴到 Remote Desktop Connection（远程桌面连接）中，然后选择 Remember me（记住我），使系统以后不再显示该对话框。



11. 选择 OK（确定）。
12. 选择 Don't ask me again for connections to this computer（不再询问我是否连接到此计算机），然后选择 Yes（是）。

按照 step-by-step说明创建运行 Linux 和 Unix 发行版（例如亚马逊 Linux、Ubuntu、Debian 或 Windows Server 2022、2019 和 2016 年等 Windows Server 操作系统）的实例。

对于 Linux 和 Unix 实例，您可以从各种应用程序蓝图（例如 LAMP WordPress、LEMP）中进行选择，也可以仅选择操作系统。对于 Windows Server 实例，您可以从 Windows Server 蓝图或 SQL Server Express 蓝图中进行选择。

该指南包括选择 AWS 区域 和可用区、选择包含所需计算和存储资源的实例计划（捆绑包）、配置网络选项（如 IPv4 和）IPv6、命名实例以及添加标签。创建实例后，您可以使用基于 Lightsail 浏览器的 SSH 或 RDP 客户端连接到该实例，也可以使用自己的 SSH 或 RDP 客户端与提供的连接详细信息进行连接。通过遵循本指南，您可以在 Lightsail 中快速启动和访问 Linux 和 Unix 或 Windows 服务器实例，这些实例是根据您的特定要求量身定制的。

查看 Lightsail 实例蓝图产品

Lightsail 为您提供了多种创建虚拟专用服务器的选项。本主题帮助您确定哪些操作系统 (OS)、应用程序或开发堆栈适合您的项目。我们按功能领域（如 CMS 和电子商务）组织了应用程序。

操作系统

Lightsail 有几个基于 Linux/UNIX 或基于 Windows 的操作系统可供选择。

Windows Server 2022

运行 Windows Server 的 Lightsail 是一个使用微软 Web 平台部署应用程序的快速而可靠的环境。借助 Lightsail，你可以在高性能、可靠、经济实惠的计算平台上运行任何兼容的基于 Windows 的解决方案。 AWS Cloud 常见的 Windows 应用场景包括基于 Windows 的企业应用程序托管、网站和 Web 服务托管、数据处理、分布式测试、ASP.NET 应用程序托管以及任何其他需要 Windows 软件的应用程序。有关支持终止信息，请参阅 Microsoft 网站。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 Windows Server 2022 的更多信息。

Windows Server 2019

运行 Windows Server 的 Lightsail 是一个使用微软 Web 平台部署应用程序的快速而可靠的环境。Lightsail 使您能够在高性能、可靠、经济实惠的 AWS 云计算平台上运行任何兼容的基于 Windows 的解决方案。常见的 Windows 应用场景包括基于 Windows 的企业应用程序托管、网站和 Web 服务托管、数据处理、分布式测试、ASP.NET 应用程序托管以及任何其他需要 Windows 软件的应用程序。有关支持终止信息，请参阅 Microsoft 网站。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 Windows Server 2019 的更多信息。

Windows Server 2016

运行 Windows Server 的 Lightsail 是一个使用微软 Web 平台部署应用程序的快速而可靠的环境。Lightsail 使您能够在高性能、可靠、经济实惠的 AWS 云计算平台上运行任何兼容的基于 Windows 的解决方案。常见的 Windows 应用场景包括基于 Windows 的企业应用程序托管、网站和 Web 服务托管、数据处理、分布式测试、ASP.NET 应用程序托管以及任何其他需要 Windows 软件的应用程序。有关支持终止信息，请参阅 Microsoft 网站。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 Windows Server 2016 的更多信息。

Amazon Linux 2023

亚马逊 Linux 2023 (AL2023) 是下一代亚马逊 Linux，非常适合通用工作负 AWS载。 AL2023 正式上市后将在五年内获得支持。 AL2023 锁定到特定版本的 Amazon Linux 软件包存储库，让您可以

控制吸收更新的方式和时间。 AL2023 还提供获取频繁更新的功能，并附带可帮助您满足合规需求的功能。

默认情况下，从 AL2 023 启动的 Lightsail 实例将强制使用实例元数据服务版本 2 (IMDSv2)。有关更多信息，请参阅 实例元数据服务版本 2 的工作原理。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 Amazon Linux 2023 的更多信息。

Amazon Linux 2

Amazon Linux 2 是上一代 Amazon Linux，是由 AWS推出的 Linux 服务器操作系统。它旨在为开发和运行云和企业应用程序提供安全稳定和高性能的执行环境。使用 Amazon Linux 2，您可以拥有一个提供长期支持的应用程序环境，并可访问 Linux 中的最新创新。Amazon Linux 2 无需额外付费。有关终止支持的信息，请参阅亚马逊 Linux 2 FAQs。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 Amazon Linux 2 的更多信息。

AlmaLinux 操作系统 9

AlmaLinux OS 9 是一款开源、社区所有和管理、永远免费的企业 Linux 发行版，专注于长期稳定性，提供强大的生产级平台。 AlmaLinux 与 RHEL® 和直播前的 CentOS 兼容。有关终止支持的信息，请访问AlmaLinux 操作系统基金会网站。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 AlmaLinux OS 9 的更多信息。

CentOS Stream 9

CentOS Stream 9 是 CentOS Stream 发行版的下一个主要版本。CentOS Stream 9 是一个持续交付的发行版，紧随 Red Hat Enterprise Linux（RHEL）开发之前，它定位于 Fedora Linux 和 RHEL 之间的中游。其旨在与 RHEL 功能兼容，提供稳定、可预测、可管理和可重现的 Linux 环境。有关支持终止信息，请参阅 CentOS 网站。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

在 CentOS Stream 网站中了解更多信息。

Debian 11 和 12

Debian 是免费的操作系统，由来自世界各地的数千名志愿者通过互联网协作开发而成。Debian 项目的主要优势在于其庞大的志愿者基础、对 Debian 社会契约和免费软件的奉献精神以及提供尽可

能完善操作系统的承诺。此新版本是朝着这一承诺迈出的又一个坚实脚步。有关支持终止信息，请参阅 Debian 网站。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

在 Debian 网站中了解更多信息。

FreeBSD 13 和 14

FreeBSD 是一种用于为服务器、台式机和嵌入式系统供电的操作系统。源自加州大学伯克利分校开发的 UNIX 版本 BSD，FreeBSD 由一个大型社区持续开发了30多年。FreeBSD的网络、安全、存储和监控功能，包括 pf 防火墙、Capsicum 和 Cloudabi 功能框架、ZFS 文件系统和动态跟踪框架，使 DTrace FreeBSD 它是许多最繁忙的网站和最普遍的嵌入式网络和存储系统的首选平台。有关终止支持的信息，请参阅 FreeBSD网站。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

要了解更多信息，请访问 FreeBSD网站。

openSUSE 15

这些区域有：openSUSE 发行版是一个稳定、易于使用且完整的多用途 Linux 发行版。它面向从事桌面或服务器方面的工作的用户和开发人员。它非常适合初学者、经验丰富的用户以及超级极客等，总之，它是所有人的理想之选！有关终止支持的信息，请参阅 openSUSE网站。

默认情况下，此操作系统的密码身份验证处于禁用状态。这意味着，即使您根据启用了密码身份验证的实例的快照创建实例，新实例也将禁用密码身份验证。有关 SUSE Linux 中密码身份验证的更多信息，请参阅 SUSE 文档中的文档 3404214。

要在禁用密码身份验证的情况下登录您的实例，您可以使用 Lightsail 控制台上基于浏览器的 SSH 客户端或密钥对。有关登录的更多信息，请参阅在 L ightsail 上连接到 Linux 或 Unix 实例或使用 SSH 命令连接到 Lightsail Linux 或 Unix 实例。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

要了解更多信息，请访问 openSUSE网站。

Ubuntu 20、22 和 24

> **Important**
>
> Ubuntu 20.04 将于 2025 年 4 月 2 日结束标准支持。在 2025 年 4 月 2 日当天或之后，您将无法使用此蓝图创建新的 Lightsail 实例。有关更多信息，请参阅 Ubuntu 网站。

Ubuntu Server 是用于虚拟服务器的基于 Debian 的 Linux 操作系统。Ubuntu 的默认安装包含各种各样的软件，包括 Firefox LibreOffice、Thunderbird 和 Transmission。您可以使用基于 APT 的软件包管理工具 (`apt-get`) 来安装很多其他软件包，如 Evolution、GIMP、Pidgin 和 Synaptic。有关支持终止信息，请参阅 Ubuntu 网站。

默认情况下，使用 Ubuntu 24 蓝图创建的 Lightsail 实例将强制使用实例元数据服务版本 2 (IMDSv2)。有关更多信息，请参阅 实例元数据服务版本 2 的工作原理。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

在 Ubuntu 网站中了解更多信息。

数据库应用程序

Lightsail 中提供了以下数据库应用程序：

SQL Server 2022 Express

SQL Server Express 是一个可免费下载、分发和使用的关系数据库管理系统。它包含专门针对嵌入式和小型应用程序的数据库。这张 Lightsail 镜像在 Windows Server 2022 的基础操作系统上运行。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 SQL Server 2022 Express 的更多信息。

SQL Server 2019 Express

SQL Server Express 是一个可免费下载、分发和使用的关系数据库管理系统。它包含专门针对嵌入式和小型应用程序的数据库。这张 Lightsail 镜像在 Windows Server 2022 的基础操作系统上运行。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 SQL Server 2019 Express 的更多信息。

SQL Server 2016 Express

SQL Server Express 是一个可免费下载、分发和使用的关系数据库管理系统。它包含专门针对嵌入式和小型应用程序的数据库。这张 Lightsail 镜像在 Windows Server 2016 的基本操作系统上运行。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

了解有关 SQL Server 2016 Express 的更多信息。

CMS 应用程序

Lightsail 中提供了以下内容管理系统 (CMS) 应用程序：

WordPress 由 Bitnami 认证

Bitnami WordPress 是一个预配置的 ready-to-use镜像，用于在 Lightsail 上运行。 WordPress WordPress 是一个流行的网络发布平台，用于构建博客和网站。您可以使用各种主题、扩展、插件和小部件来自定义它。

WordPress 具有完整的主题系统，只需单击几下即可更改网站的外观和风格。您也可以使用现有的免费或商业 WordPress 主题。 WordPress 完全符合万维网联盟 (W3C) 的标准。

在 Lightsa WordPress il 上启动和配置

要了解更多信息 WordPress，请访问 Bitnami 网站。

WordPress 通过 Bitnami 认证的多站点

WordPress Multisite 使管理员能够通过同一个 WordPress 实例托管和管理多个网站。这些网站都可以具有唯一域名，并可由其所有者自定义，同时共享由服务器管理员提供的主题和插件等资产。您可以一次推送对所有站点的更新，确保它们始终安全。

WordPress Multisite 非常适合大学、公司和机构等组织，这些组织需要让许多人能够托管自己的网站，同时将总体控制权交给中央管理员。

在 Lightsail 上设置 WordPress多站点

要了解有关 WordPress Multisite 的更多信息，请访问 Bitnami 网站。

cPanel & WebHost Manager (WHM)

cPanel 和 WHM 是一套专为 Linux 操作系统构建的工具，让您能够通过使用简单的图形用户界面实现 Web 托管任务自动执行。它旨在降低您管理服务器以及您的客户管理网站的难度。

在 Lightsail 上使用 cPanel 和 WHM 托管网站、电子邮件和服务

在 cPanel 网站中了解有关 cPanel 和 WHM 的更多信息。

PrestaShop 由 Bitnami 打包

PrestaShop 是世界上最多产的电子商务解决方案之一。它是一款免费的开源软件，拥有一个活跃成员多达 100 万的社群。它旨在让您的在线商店快速启动并运行，并具有预配置的主题，因此您几乎

可以立即开始销售，并使用实时配置器轻松自定义网站的外观。 PrestaShop 提供多店支持、可定制 URLs、多种支付网关选项（包括 PayPal 和 Stripe），以及与亚马逊、eBay、Facebook 等的市场集成。

在 Lightsa PrestaShop il 上建立一个网站

要了解更多信息 PrestaShop，请PrestaShop访问网站。

Bitnami 打包的 Ghost

Ghost 是一个发布平台，适用于从个人博客到主要新闻网站的所有内容。基于 Node.js 构建，其现代技术堆栈使其变得具有多功能和灵活性，适合寻求与其他应用程序和工具集成的开发人员，同时为内容创作者保持易用性。

在 Lightsail 上部署 Ghost 网站

在 Bitnami 网站中了解有关 Bitnami Ghost 的更多信息。

Bitnami 打包的 Joomla!

Bitnami Joomla！ 是用于运行 Joomla 的预配置 ready-to-use镜像！ 在 Lightsail 上。Joomla! 是一种可用于构建各种网站或门户的 CMS。这包括个人、公司、小型企业、非营利性机构和其他组织网站。

Joomla! 还包含供用户配置个人选项的注册系统。身份验证是用户管理的重要组成部分，而 Joomla! 支持多种协议，包括 LDAP、OpenID 等。Joomla! 支持很多不同的语言，并提供了有关将这些语言用于网站和管理面板的指南。此外，Banner Manager 可让您轻松设置和管理网站上的横幅。您可以跟踪指标，包括设置展示次数 URLs、特殊展示次数等。

开始使用 Joomla 吧！ 在 Lightsail 上

在 Bitnami 网站中了解有关 Joomla! 的更多信息。

由 Bitnami 打包的 Drupal

Bitnami Drupal 是一张预先配置的 ready-to-use镜像，用于在 Lightsail 上运行 Drupal。Drupal 是一个内容管理平台，可帮助用户轻松发布、管理和组织内容。它用于社群 Web 门户、讨论站点、企业网站等。您可以通过插入模块来轻松扩展 Drupal。Drupal 专为实现高性能而打造，可扩展到很多服务器，并且可与 REST、JSON、SOAP 和其他格式轻松集成。

有数千个适用于 Drupal 的附加模块和设计。Drupal 还提供有多个语言版本。

在 Lightsail 上设置和自定义你的 Drupal 网站

在 Bitnami 网站中了解有关 Drupal 的更多信息。

应用程序堆栈和服务器

Lightsail 有五个应用程序堆栈和服务器，适用于各种开发项目。每个镜像均使用 Linux/Unix (Ubuntu) 作为基本操作系统。

由 Bitnami 打包的 LAMP 堆栈（PHP 8）

Bitnami LAMP 堆栈简化了 PHP 应用程序的开发和部署。它包括 ready-to-run Apache、MySQL phpMyAdmin、PHP 和，以及运行每个组件所需的其他软件。Bitnami LAMP 堆栈已完全集成和配置，因此在 Lightsail 中创建实例后，您就可以开始开发应用程序了。Bitnami LAMP 堆栈会定期更新，旨在确保您始终有权访问每个捆绑组件的最新稳定版本。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

在 Lightsail 上设置 LAMP 堆栈

在 Bitnami 网站中了解有关 Bitnami LAMP 堆栈的更多信息。

由 Bitnami 打包的 Django

Django 是一个高级 Python Web 框架，旨在促进快速开发和整洁、务实的设计。Python 是一种面向对象的动态编程语言，可用于进行多种软件开发。Bitnami Django Stack 极大地简化了 Django 的部署及其运行时依赖项，包括 Python、Django、MySQL 和 Apache ready-to-run 的版本。

在 Bitnami 网站中了解有关 Bitnami Django 堆栈的更多信息。

由 Bitnami 打包的 Node.js

Bitnami Node.js 是一张预配置的 ready-to-use镜像，用于在 Lightsail 上运行 Node.js。Node.js 是一个基于 Chrome JavaScript 运行时构建的平台，用于轻松创建快速、可扩展的网络应用程序。它使用事件驱动的非阻塞 I/O 模型，从而更轻量、高效。Node.js 非常适用于数据密集型实时应用程序。

开始在 Lightsail 上使用 Node.js

在 Bitnami 网站中了解有关 Node.js 堆栈的更多信息。

由 Bitnami 打包的 MEAN 堆栈

Bitnami MEAN 堆栈提供了一个只需单击一下即可部署的适用于 MongoDB 和 Node.js 的完整开发环境。它包括最新稳定版本的 MongoDB、Express、Angular、Node.js、Git、PHP 和。RockMongo

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

在 Bitnami 网站中了解有关 MEAN 堆栈的更多信息。

GitLab 由 Bitnami 打包的 CE

Bitnami GitLab 社区版 (CE) 是一个预先配置的 ready-to-use镜像，用于在 Lightsail 上 GitLab 运行。 GitLab 是一款基于 Ruby on Rails 的自托管的 Git 管理软件，它快速、安全。 GitLab CI（也包括在内）是一款与 Git 紧密集成的开源持续集成 (CI) 服务器 GitLab。

使用 GitLab，您可以在自己的服务器上保护代码的安全，管理存储库、用户和访问权限。它是独立的，因此您可以轻松地将安装复制或移动到不同的服务器。

在 Lightsail 上设置和配置 GitLab CE 实例

要了解有关GitLab堆栈的更多信息，请访问 Bitnami 网站。

由 Bitnami 打包的 Nginx (LEMP 堆栈)

Bitnami NGINX 堆栈提供了一个只需单击一次即可启动的完整的 PHP、MySQL 和 NGINX 开发环境。它还捆绑了 phpMyAdmin、、 SQLite、fastCGI ImageMagick、Memcache、GD、CURL、PEAR、PECL 和其他组件。

NGINX 是一种异步服务器，其主要优势在于可扩展性。NGINX 堆栈又称为 LEMP（Linux、Nginx、MySQL 和 PHP）。

在 Lightsail 上部署和管理 Nginx 网络服务器

在 Bitnami 网站中了解有关 Nginx 堆栈的更多信息。

Ubuntu 上的 Plesk 托管堆栈，Ubuntu 上的 Plesk 托管堆栈 (BYOL)

> **Important**
>
> 2024 年 8 月 1 日，Plesk 过渡到付费许可模式。以下许可行为适用于运行 Plesk 的 Lightsail 实例：
>
> - 从 2025 年 2 月 1 日起，在 Ubuntu 蓝图上使用较旧的 Plesk Hosting Stack 的任何实例都需要付费许可。
> - 使用 Ubuntu 上的 Plesk 托管堆栈 (BYOL) 蓝图启动的实例有 30 天的试用许可证。30 天后，您必须从 Plesk 购买许可证才能继续使用 Plesk 应用程序。
>
> 有关更多信息，请参阅购买 Plesk 许可证。

使用 Plesk 支持的托管堆栈在 Lightsail 和 AWS 上构建、保护和运行网站和应用程序。这包括所有基于 Web 的服务器管理和安全工具，以及图形用户界面中的 WordPress 自动化。它减轻了 Web 专业人员的工作，并提供客户所需的可扩展性、安全性和性能。

设置和配置 Plesk。

在 Plesk 网站中了解有关 Plesk 堆栈的更多信息。

电子商务应用程序

Lightsail 目前有一张电子商务应用程序图片：Magento。此 Magento 镜像使用 Linux/Unix (Ubuntu) 作为基本操作系统。

由 Bitnami 打包的 Magento

Bitnami Magento 是一张预先配置的镜像，用于在 Lightsail 上运行 M ready-to-use agento。您可以使用 Magento 构建吸引眼球、响应迅速且安全的网站。Magento 是一个功能丰富且灵活的电子商务解决方案，其包含交易选项、multistore 功能、忠诚度计划、产品分类、顾客筛选、促销规则等。

您可以使用 Magento 创建可反映您的品牌的高度自定义的电子商务网站。Magento 与您的业务运营集成，因此您可以根据业务需求管理您的电子商务网站。

在 Lightsail 上设置和配置 Magento

在 Bitnami 网站中了解有关 Magento 堆栈的更多信息。

项目管理应用程序

Lightsail 目前有一个项目管理应用程序镜像，即 Redmine。此镜像使用 Linux/Unix (Ubuntu) 作为基本操作系统。

由 Bitnami 打包的 Redmine

Bitnami Redmine 是一张预先配置的 ready-to-use镜像，用于在 Lightsail 上运行 Redmine。Redmine 是一种灵活的项目管理 Web 应用程序。它包含对以下内容的支持：多个项目；基于角色的访问控制；甘特图和日历；新闻、文档和文件的管理；每个项目的 Wiki 和论坛；SCM 集成等。

此蓝图与 IPv6仅限 Lightsail 的实例计划兼容。

[在 Lightsail 上配置和保护 Redmine 实例]

在 Bitnami 网站中了解有关 Redmine 堆栈的更多信息。

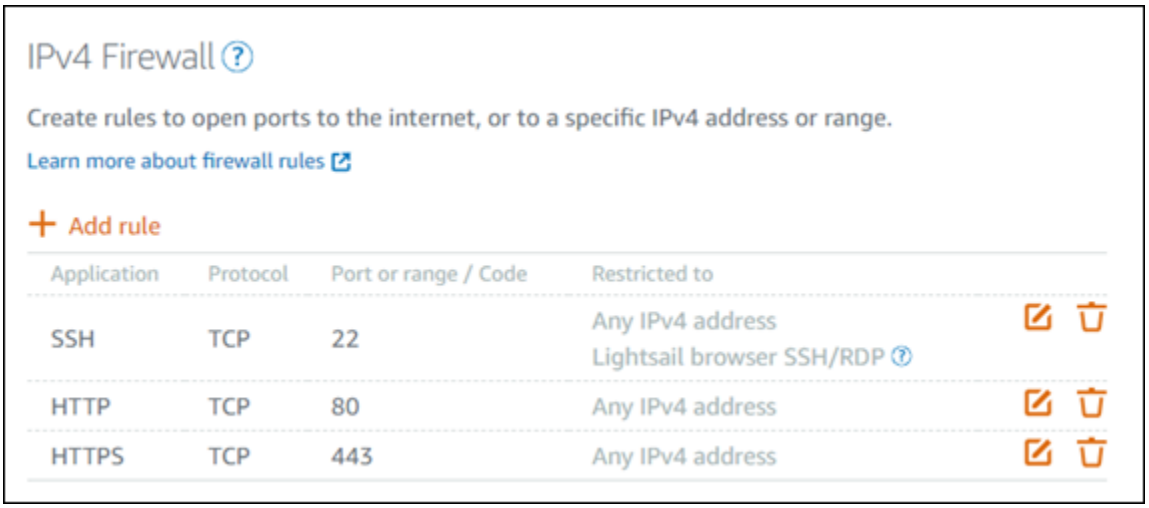
在 Lightsail 中使用防火墙控制实例流量

Amazon Lightsail 控制台中的防火墙充当虚拟防火墙，用于控制允许通过其公有 IP 地址连接到您的实例的流量。您在 Lightsail 中创建的每个实例都有两个防火墙；一个用于 IPv4 地址，另一个用于地址。IPv6每个防火墙均包含一组规则来过滤进入实例的流量。两个防火墙彼此独立；必须为 IPv4 和 IPv6分别配置防火墙规则。可以通过添加和删除允许或限制流量的规则，来随时编辑实例的防火墙。

Lightsail 防火墙

每个 Lightsail 实例都有两个防火墙；一个用于 IPv4 地址，另一个用于地址。 IPv6所有进出您的 Lightsail 实例的互联网流量都要通过其防火墙。实例的防火墙控制允许流入实例的 Internet 流量。但是，防火墙不控制流出实例的流量，而是允许所有出站流量。可以通过添加和删除允许或限制传入流量的规则，来随时编辑实例的防火墙。请注意，两个防火墙彼此独立；必须为 IPv4 和 IPv6分别配置防火墙规则。

防火墙规则始终是允许型的；您无法创建拒绝访问的规则。可以向实例的防火墙添加规则以允许流量到达实例。向实例的防火墙添加规则时，您可以指定要使用的协议、要打开的端口以及允许连接到您的实例的 IPv4 和 IPv6 地址，如以下示例（对于 IPv4）所示。您还可以指定应用层协议类型，这是一种预设，根据您计划在自己实例上使用的服务来为你指定协议和端口范围。



> **Important**
>
> 防火墙规则仅影响通过实例的公有 IP 地址传入的流量。它不会影响通过实例私有 IP 地址流入的流量，该地址可以来自您账户中的 Lightsail 资源，也可以来自 AWS 区域同一个对等虚拟私有云 (VPC) 中的资源。 AWS 区域

本指南接下来的几个部分将说明防火墙规则及其可配置的参数。

创建防火墙规则

您可以创建防火墙规则，以使客户端能够与您的实例或其上运行的应用程序建立连接。例如，要使所有 Web 浏览器都能连接到您的实例上的 WordPress 应用程序，您需要配置一条防火墙规则，允许从任意 IP 地址通过端口 80 使用传输控制协议 (TCP)。如果您的实例的防火墙上已经配置了此规则，则可以将其删除以阻止 Web 浏览器连接到您的实例上的 WordPress 应用程序。

> **Important**
>
> 您可以使用 Lightsail 控制台一次最多添加 30 个源 IP 地址。要一次最多添加 60 个 IP 地址，请使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或 SD AWS K。对于 IPv4 规则和 IPv6 规则，此配额是单独实施的。例如，防火墙可以有 60 条入站 IPv4 流量规则和 60 条入站 IPv6 流量规则。建议您将单个 IP 地址整合到 CIDR 范围内。有关更多信息，请参阅本指南的指定源 IP 地址部分。

您还可以允许 SSH 客户端连接到实例并在服务器上执行管理任务，方法是配置一个防火墙规则，该规则仅从需要建立连接的计算机的 IP 地址，通过端口 22 上启用 TCP。在这一使用情形中，您应该不希望任意 IP 地址都与您的实例建立 SSH 连接；因为这可能会给实例带来安全风险。

> **Note**
>
> 此部分中描述的防火墙规则示例可能默认存在于您实例的防火墙中。有关更多信息，请参阅本指南后面的默认防火墙规则。

如果特定端口有多条规则，我们会使用最宽松的规则。例如，如果添加一个允许从 IP 地址 192.0.2.1 访问 TCP 端口 22 (SSH) 的规则。然后，添加另一个允许每个人访问 TCP 端口 22 的规则。结果就是每个人都能访问 TCP 端口 22。

指定协议

协议是在两台计算机之间传输数据的格式。Lightsail 允许您在防火墙规则中指定以下协议：

- 传输控制协议（TCP）主要用于建立和维持客户端与实例上运行的应用程序之间的连接，直到数据交换完成。它是一种广泛使用的协议，您可能经常在防火墙规则中指定该协议。TCP 可保证不会丢失任何已传输的数据，并且已发送的数据都将发送给预期的接收者。它最适用于需要高可靠性且传输时间相对不太重要的网络应用程序，例如 Web浏览、金融交易和文本消息传递。这些使用情形中，如果部分数据丢失，将造成重大价值损失。
- 用户数据报协议 (UDP) 主要用于在客户端和实例上运行的应用程序之间建立低延迟的容损连接。它最适用于所感知的延迟至关重要的网络应用程序，例如游戏、语音和视频通信。这些使用情形可承受某种程度的数据丢失，而不会对所感知的质量产生负面影响。
- Internet 控制消息协议（ICMP）主要用于诊断网络通信问题，例如，确定数据是否及时到达预期目的地。它最适用于 Ping 实用程序，可以使用该实用程序来测试本地计算机和实例之间的连接速度。它会报告数据到达实例并返回到本地计算机所花费的时间。

  > **Note**
  >
  > 当您使用 Lightsail 控制台向实例的 IPv6 防火墙添加 ICMP 规则时，该规则会自动配置为使用。 ICMPv6有关更多信息，请参阅维基百科 IPv6上的互联网控制消息协议。

- 所有用于允许所有协议流量流入实例。当不确定要指定哪个协议时，请指定此协议。这包括所有 Internet 协议；而不仅仅是上面指定的协议。有关更多信息，请参阅互联网编号分配机构网站上的协议编号。

指定端口

与计算机上的物理端口（允许计算机与键盘和鼠标等外围设备进行通信）类似，网络端口将充当实例的 Internet 通信终端节点。当计算机寻求与您的实例连接时，它会公开一个端口来建立通信。

可在防火墙规则中指定的端口范围是 0 到 65535。在创建防火墙规则以允许客户端与实例建立连接时，可以指定将使用的协议（本指南前面已介绍）以及可用于建立连接的端口号。还可以指定允许使用协议和端口建立连接的 IP 地址；本指南的下一部分将介绍这一点。

以下是一些常用端口以及使用它们的服务：

- 通过文件传输协议 (FTP) 进行的数据传输操作使用端口 20。
- FTP 命令控制使用端口 21。

- Secure Shell（SSH）使用端口 22。
- Telnet 远程登录服务，以及未加密的文本消息使用端口 23。
- 简单邮件传输协议 (SMTP) 电子邮件路由使用端口 25。

> **Important**
>
> 要在实例上启用 SMTP，您还必须为实例配置反向 DNS。否则，您的电子邮件可能会受到 TCP 端口 25 的限制。有关更多信息，请参阅在 Amazon Lightsail 实例上为电子邮件服务器配置反向 DNS。

- 域名系统 (DNS) 服务使用端口 53。
- Web 浏览器用来连接到网站的超文本传输协议 (HTTP) 使用端口 80。
- 电子邮件客户端用来从服务器检索电子邮件的邮局协议 (POP3) 使用端口 110。
- 网络新闻传输协议 (NNTP) 使用端口 119。
- 网络时间协议 (NTP) 使用端口 123。
- 用于管理数字邮件的 Internet 消息访问协议 (IMAP) 使用端口 143。
- 简单网络管理协议 (SNMP) 使用端口 161。
- Web 浏览器用来建立与网站的加密连接的 HTTP Secure (HTTPS) 或 HTTP over TLS/SSL 使用端口 443。

有关更多信息，请参阅互联网编号分配机构网站上的服务名称和传输协议端口号注册表。

指定应用层协议类型

可以在创建防火墙规则时指定应用层协议类型，它是一种预设，用于根据要在实例上启用的服务为您指定规则的协议和端口范围。这样一来，您便无需搜索要用于像 SSH、RDP、HTTP 这样的服务以及其他服务的通用协议和端口。您只需选择这些应用层协议类型即可为您指定协议和端口。如果您想指定自己的协议和端口，则可以选择自定义规则应用层协议类型，这样您便能控制这些参数。

> **Note**
>
> 您只能使用 Lightsail 控制台来指定应用层协议类型。您无法使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或指定应用层协议类型。 SDKs

Lightsail 控制台中提供了以下应用层协议类型：

- 自定义 - 选择此选项可指定您自己的协议和端口。
- 所有协议 - 选择此选项可指定所有协议，并指定您自己的端口。
- 所有 TCP - 选择此选项可使用 TCP 协议，但不指定要开放哪个端口。这将在所有端口 (0-65535) 上启用 TCP。
- 所有 UDP - 选择此选项可使用 UDP 协议，但您不指定要开放哪个端口。这将在所有端口 (0-65535) 上启用 UDP。
- 所有 ICMP - 选择此选项可指定所有 ICMP 类型和代码。
- 自定义 ICMP - 选择此选项可使用 ICMP 协议并定义 ICMP 类型和代码。有关 ICMP 类型和代码的更多信息，请参阅 Wikipedia 上的控制消息。
- DNS - 如果要在实例上启用 DNS，请选择此选项。这将在端口 53 上启用 TCP 和 UDP。
- HTTP - 如果要使 Web 浏览器能够连接到实例上托管的网站，请选择此选项。这将在端口 80 上启用 TCP。
- HTTPS - 如果您要使 Web 浏览器能够与实例上托管的网站建立加密连接，请选择此选项。这将在端口 443 上启用 TCP。
- MySQL/aurora - 选择此选项可使客户端连接到实例上托管的 MySQL 或 Aurora 数据库。这将在端口 3306 上启用 TCP。
- Oracle-RDS - 选择此选项可使客户端连接到实例上托管的 Oracle 或 RDS 数据库。这将在端口 1521 上启用 TCP。
- Ping (ICMP) - 选择此选项可使您的实例响应使用 Ping 实用程序发出的请求。在 IPv4 防火墙上，这将启用 ICMP 类型 8（回声）和代码 -1（所有代码）。在 IPv6 防火墙上，这将启用 ICMP 类型 129（回声回复）和代码 0。
- RDP - 选择此选项可使 RDP 客户端连接到您的实例。这将在端口 3389 上启用 TCP。
- SSH - 选择此选项可使 SSH 客户端连接到您的实例。这将在端口 22 上启用 TCP。

指定源 IP 地址

默认情况下，防火墙规则允许所有 IP 地址通过指定的协议和端口连接到实例。这最适用于像通过 HTTP 和 HTTPS 传输的 Web 浏览器流量等情形。但是，这会给 SSH 和 RDP 等流量带来安全风险，因为您不希望允许所有 IP 地址使用这些应用程序连接到您的实例。因此，您可以选择将防火墙规则限制为 IPv4 或 IPv6地址或 IP 地址范围。

- 对于 IPv4 防火墙-您可以指定单个 IPv4地址（例如，203.0.113.1）或地址范围。 IPv4 在 Lightsail 控制台中，可以使用破折号（例如 192.0.2.0-192.0.2.255）或 CIDR 块表示法（例如 192.0.2.0/24）来指定范围。有关 CIDR 块表示法的更多信息，请参阅 Wikipedia 上的无类域间路由。

- 对于 IPv6 防火墙-您可以指定单个 IPv6地址（例如，2001:0 db 8:85 a 3:0000:00:8 a2e:0370:7334）或地址范围。 IPv6在 Lightsail 控制台中，只能使用 CIDR 区块表示法来指定 IPv6 范围（例如，2001:db8:: /32）。有关 IPv6 CIDR 区块表示法的更多信息，请参阅维基百科上的 IPv6CIDR 块。

Lightsail 的默认防火墙规则

创建新实例时，其 IPv4 和 IPv6 防火墙会预先配置以下一组默认规则，允许对您的实例进行基本访问。默认规则因您创建的实例的类型而异。这些规则将以应用程序、协议、端口和源 IP 地址的方式列出（例如，应用程序 - 协议 - 端口 - 源 IP 地址）。

AlmaLinux，亚马逊 Linux 2，亚马逊 Linux 2023，CentOS, Debian, FreeBSD, openSUSE，以及 Ubuntu （基础操作系统）

SSH - TCP - 22 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

WordPress，幽灵，Joomla！ PrestaShop、和 Drupal（内容管理系统应用程序）

SSH - TCP - 22 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

HTTPS - TCP - 443 - 所有 IP 地址

cPanel 和 WHM（CMS 应用程序）

SSH - TCP - 22 - 所有 IP 地址

DNS (UDP) - UDP - 53 - 所有 IP 地址

DNS (TCP) - TCP - 53 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

HTTPS - TCP - 443 - 所有 IP 地址

自定义 - TCP - 2078 - 所有 IP 地址

自定义 - TCP - 2083 - 所有 IP 地址

自定义 - TCP - 2087 - 所有 IP 地址

自定义 - TCP - 2089 - 所有 IP 地址

LAMP、Django、Node.js、MEAN GitLab 和 Nginx（开发堆栈）

SSH - TCP - 22 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

HTTPS - TCP - 443 - 所有 IP 地址

Magento（电子商务应用程序）

SSH - TCP - 22 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

HTTPS - TCP - 443 - 所有 IP 地址

Redmine（项目管理应用程序）

SSH - TCP - 22 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

HTTPS - TCP - 443 - 所有 IP 地址

Plesk（托管堆栈）

SSH - TCP - 22 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

HTTPS - TCP - 443 - 所有 IP 地址

自定义 - TCP - 53 - 所有 IP 地址

自定义 - UDP - 53 - 所有 IP 地址

自定义 - TCP - 8443 - 所有 IP 地址

自定义 - TCP - 8447 - 所有 IP 地址

Windows Server 2022、Windows Server 2019 和 Windows Server 2016

SSH - TCP - 22 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

RDP - TCP - 3389 - 所有 IP 地址

SQL Server Express 2022、SQL Server Express 2019 和 SQL Server Express 2016

SSH - TCP - 22 - 所有 IP 地址

HTTP - TCP - 80 - 所有 IP 地址

RDP - TCP - 3389 - 所有 IP 地址

向 Lightsail 实例添加防火墙规则

您可以在 Amazon Lightsail 实例的 IPv4 和 IPv6 防火墙中添加规则，以控制允许连接到该实例的流量。添加防火墙规则时，您可以指定应用层协议类型、协议、端口以及允许连接到您的实例的一个 IPv4 或 IPv6 多个源地址。有关防火墙的更多信息，请参阅防火墙和端口。

添加和编辑实例防火墙规则

完成以下步骤，在 Lightsail 控制台中添加或编辑防火墙规则。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择要为其添加或编辑防火墙规则的实例的名称。
4. 选择实例的管理页面上的 Networking (联网) 选项卡。

   网络选项卡显示您的实例的公有和私有 IP 地址，以及您的实例的已配置 IPv4 或 IPv6 防火墙。

   > **Note**
   >
   > 只有在您为实例启用 IPv6 IPv6 防火墙后，才会显示防火墙。有关更多信息，请参阅启用或禁用 IPv6。

5. 根据规则的源 IP 是否为 IPv4 或 IPv6 地址，完成以下步骤之一：

   - 要添加 IPv4 防火墙规则，请向下滚动到页面的IPv4防火墙部分，然后选择添加规则。
   - 要添加 IPv6 防火墙规则，请向下滚动到页面的IPv6防火墙部分，然后选择添加规则。

   也可以在要编辑的防火墙的现有规则旁边，选择 Edit (编辑) (铅笔图标) 来编辑它。

6. 在 Application (应用程序) 下拉菜单中选择应用层协议类型。

在选择应用层协议类型时，系统会为您指定一组协议和端口预设。示例值包括 Custom (自定义)、All TCP (所有 TCP)、All UDP (所有 UDP)、Custom ICMP (自定义 ICMP)、SSH 和 RDP。

您可以根据选择的应用程序层协议类型配置以下可选设置：

- （可选）如果选择 Custom (自定义) 选项，则可以在 Protocol (协议) 下拉菜单中选择一个值。可用的协议值包括 TCP 和 UDP。

  您还可以在 Port (端口) 字段中输入单个端口号或端口号范围（例如 7000-8000）。

- （可选）如果选择 Custom ICMP (自定义 ICMP) 选项，则可以在 Type (类型) 字段中指定 ICMP 类型，并在 Code (代码) 字段中指定 ICMP 代码。有关 ICMP 类型和代码的更多信息，请参阅 Wikipedia 上的控制消息。

  > **Note**
  >
  > 当您使用 Lightsail 控制台向实例的 IPv6 防火墙添加 ICMP 规则时，该规则会自动配置为使用。 ICMPv6有关更多信息，请参阅维基百科 IPv6上的互联网控制消息协议。

- （可选）选择 Restrict to IP address (限制为 IP 地址) 可将指定协议和端口的访问限制为某个特定的 IP 地址或 IP 地址范围。将此选项保持未选中状态可为指定协议和端口允许所有 IP 地址。

  您可以输入单个 IPv4 地址（例如，`203.0.113.1`）或 IPv4 地址范围。可以使用短划线（例如，`192.0.2.0-192.0.2.255`）或 CIDR 块表示法（例如，`192.0.2.0/24`）来指定范围。有关 CIDR 块表示法的更多信息，请参阅 Wikipedia 上的无类域间路由。

- （可选）如果您选择 SSH 或 RDP 应用层协议类型，然后选择限制为 IP 地址，则可以选择允许 Lightsail 浏览器 SSH/RDP，以允许使用 Lightsail 控制台中提供的基于浏览器的 SSH 和 RDP 客户端连接到您的实例。将此选项保持未选中状态可阻止通过这些基于浏览器的客户端进行的访问。

7. 选择 Create (创建) 将规则添加到防火墙。

   等待一段时间后，防火墙规则就添加好了。

删除防火墙规则

除了添加和编辑防火墙规则外，您可能还需要删除 Amazon Lightsail 实例的现有规则。如果您不再要求允许某些入站流量进入您的实例，则可能需要移除防火墙规则。删除 IPv4 和 IPv6 防火墙规则的过

程非常简单，可以直接通过 Lightsail 控制台完成。完成以下步骤，在 Lightsail 控制台中删除实例防火墙规则。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择要为其删除防火墙规则的实例的名称。
4. 选择实例的管理页面上的 Networking (联网) 选项卡。
5. 根据规则的源 IP 是否为 IPv4 或 IPv6 地址，完成以下步骤之一：

   - 要删除 IPv4 防火墙规则，请向下滚动到页面的 “IPv4防火墙” 部分，然后选择现有规则旁边的删除（垃圾图标）将其删除。
   - 要删除 IPv6 防火墙规则，请向下滚动到页面的 “IPv6防火墙” 部分，然后选择现有规则旁边的删除（垃圾图标）将其删除。

   > **Important**
   >
   > 防火墙规则仅影响通过实例的公有 IP 地址传入的流量。它不会影响通过实例私有 IP 地址流入的流量，该地址可以来自您账户中的 Lightsail 资源，也可以来自 AWS 区域同一个对等虚拟私有云 (VPC) 中的资源。 AWS 区域例如，如果您从实例防火墙中删除 SSH 规则（TCP 端口 22），则同一 Lightsail 账户中的其他实例可以通过指定该实例的私有 IP 地址继续使用 SSH 连接到该规则。 AWS 区域

   等待一段时间后，防火墙规则就删除了。

Lightsail 实例的防火墙规则参考

您可以向 Amazon Lightsail 实例的防火墙添加反映该实例角色的规则。例如，配置作为 Web 服务器的实例需要允许入站 HTTP 和 HTTPS 访问的防火墙规则。数据库实例需要允许数据库类型访问的规则，例如，对 MySQL 允许通过端口 3306 进行访问。有关防火墙的更多信息，请参阅 Lightsail 中的实例防火墙。

本指南提供了各种防火墙规则示例，您可以将这些规则添加到实例防火墙以进行特定类型的访问。除非另行说明，否则这些规则将以应用程序、协议、端口和源 IP 地址的方式列出（例如，应用程序 - 协议 - 端口 - 源 IP 地址）。

内容

- Web 服务器规则
- 用于从计算机连接到实例的规则
- 数据库服务器规则
- DNS 服务器规则
- SMTP 电子邮件

Web 服务器规则

以下入站规则允许 HTTP 和 HTTPS 访问。

> **Note**
>
> 某些 Lightsail 实例默认配置了以下防火墙规则。有关更多信息，请参阅防火墙和端口。

HTTP

HTTP - TCP - 80 - 所有 IP 地址

HTTPS

HTTPS - TCP - 443 - 所有 IP 地址

用于从计算机连接到实例的规则

要连接到您的实例，请添加允许 SSH 访问（适用于 Linux 实例）或 RDP 访问（适用于 Windows 实例）的规则。

> **Note**
>
> 默认情况下，所有 Lightsail 实例都配置了以下任一防火墙规则。有关更多信息，请参阅防火墙和端口。

SSH

SSH - TCP - 22 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

RDP

RDP - TCP - 3389 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

数据库服务器规则

以下入站规则是您可以为数据库访问添加的规则示例，具体取决于您的实例上运行的数据库类型。

SQL Server

自定义 - TCP - 1433 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

MySQL/Aurora

MySQL/Aurora - TCP - 3306 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

PostgreSQL

PostgreSQL - TCP - 5432 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

Oracle-RDS

Oracle-RDS - TCP - 1521 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

Amazon Redshift

自定义 - TCP - 5439 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

DNS 服务器规则

如果您已将实例设置为 DNS 服务器，则必须确保 TCP 和 UDP 流量可通过端口 53 到达您的 DNS 服务器。

DNS (TCP)

DNS (TCP) - TCP - 53 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

DNS (UDP)

DNS (UDP) - UDP - 53 - 计算机的公有 IP 地址或本地网络中的 IP 地址范围（采用 CIDR 块表示法）

SMTP 电子邮件

要在您的实例上启用 SMTP，您必须配置以下防火墙规则。

> **Important**
>
> 配置以下规则后，您还必须为实例配置反向 DNS。否则，您的电子邮件可能会受到 TCP 端口 25 的限制。有关更多信息，请参阅为电子邮件服务器配置反向 DNS。

SMTP

自定义 - TCP - 25 - 与实例进行通信的主机的 IP 地址

检测 Lightsail 实例爆发以获得最佳性能

Amazon Lightsail 实例提供基准的 CPU 性能，但也能够根据需要临时提供高于基准的额外 CPU 性能。这被称为突增。基准性能和突增能力由以下实例指标控制：

- CPU 利用率 - 当前正在实例上使用的已分配计算单位的百分比。此指标可确定用于在实例上运行应用程序的处理能力。
- CPU 容量爆增百分比 - 您的实例可用的 CPU 性能百分比。
- CPU 突增容量分钟数 - 实例以 100% CPU 利用率进行突增的可用时间。

通过以下主题，您将学习如何监控这些指标以最大限度地提高实例可用性。

主题

- 了解 Lightsail 实例的基准 CPU 性能和突发容量累积
- 查看 Lightsail 实例的 CPU 突发容量累积
- 确定你的 Lightsail 实例何时爆发
- 监控 Lightsail 实例的 CPU 突发容量
- 查看 Lightsail 实例的 CPU 利用率和突发容量
- 解决您的 Lightsail 实例的 CPU 使用率过高的问题

了解 Lightsail 实例的基准 CPU 性能和突发容量累积

Lightsail 实例每小时（以毫秒级分辨率）持续获得设定的 CPU 突发容量，当您的实例的 CPU 利用率大于 0% 时，也会消耗该容量。累积或消耗突增容量的核算过程也以毫秒级精度为单位，因此，您无需担心过度消耗 CPU 突增容量，短时间突增 CPU 使用少量突增容量。

如果您的实例使用的 CPU 资源少于基准性能所需的数量（例如，当它处于空闲状态时），则会以 CPU 容量爆增百分比和分钟数的形式累积未使用的 CPU 容量爆增。如果您的实例需要突增至基准性能水平以上，它将花费累积的 CPU 突增容量。实例累积的 CPU 突增容量越多，在需要更高性能时，它突增到基线以上的时间就越长。

基准 CPU 性能

下表概述了 Lightsail 中双栈实例计划的性能基准。虽然 IPv6仅限套餐的价格不同，但性能基准是相同的。

实例计划	v CPUs	内存	存储	性能基准
Linux 或 Unix 5 USD 和 Windows 9.50 USD	2	512MB	20GB	5%
Linux 或 Unix 7 USD 和 Windows 14 USD	2	1 GB	40GB	10%
Linux 或 Unix 12 USD 和 Windows 22 USD	2	2 GB	60GB	20%
Linux 或 Unix 24 USD 和 Windows 44 USD	2	4 GB	80 GB	20%
Linux 或 Unix 44 USD 和 Windows 74 USD	2	8 GB	160GB	30%
Linux 或 Unix 84 USD 和 Windows 124 USD	4	16 GB	320GB	40%
Linux 或 Unix 164 USD 和 Windows 244 USD	8	32 GB	640GB	40%

实例计划	v CPUs	内存	存储	性能基准
* Linux 或 Unix 384 USD 和 Windows 574 USD	16	64 GB	1,280GB	40%

* Linux 或 Unix 384 USD 和 Windows 574 USD 实例计划不会累积 CPU 容量爆增。它们将根据需要自动爆增。

这些性能基准是按每个 vCPU 计算的。Lightsail 控制台中的 CPU 利用率指标图平均了具有多个 vCPU 的实例的 CPU 利用率和基准。例如，基于 Linux 或 Unix 的每月 44 美元的实例有两个 vCPUs ，CPU 平均利用率基准为 30%。因此，如果：

- 一个 vCPU 利用率为 50%，另一个为 0%，图形上会显示 25% 的平均 CPU 利用率。这使实例的 CPU 利用率低于 30% 的基线，因此处于可持续区域。
- 一个 vCPU 利用率为 30%，另一个为 20%，图形上会显示 25% 的平均 CPU 利用率。这使实例的 CPU 利用率低于 30% 的基线，因此处于可持续区域。
- 一个 vCPU 利用率为 35%，另一个为 25%，图形上会显示 30% 的平均 CPU 利用率。这使实例的 CPU 利用率等于 30% 的基线。
- 一个 vCPU 利用率为 100%，另一个为 90%，图形上会显示 95% 的平均 CPU 利用率。这使实例的 CPU 利用率高于 30% 的基线，因此处于可突增区域。

有关可持续区域和可暴增区域的更多信息，请参阅本指南下文的确定您的实例何时暴增。

上一代 CPU 性能

下表概述了在 2023 年 6 月 29 日之前创建的 Lightsail 实例的性能基准。这些性能基准是按每个 vCPU 计算的。

实例计划	v CPUs	内存	存储	性能基准
Linux 或 Unix 5 USD 和 Windows 9.50 USD	1	512MB	20GB	5%
Linux 或 Unix 7 USD 和 Windows 14 USD	1	1 GB	40GB	10%

实例计划	v CPUs	内存	存储	性能基准
Linux 或 Unix 12 USD 和 Windows 22 USD	1	2 GB	60GB	20%
Linux 或 Unix 24 USD 和 Windows 44 USD	2	4 GB	80 GB	20%
Linux 或 Unix 44 USD 和 Windows 74 USD	2	8 GB	160GB	30%
Linux 或 Unix 84 USD 和 Windows 124 USD	4	16 GB	320GB	22.5%
Linux 或 Unix 164 USD 和 Windows 244 USD	8	32 GB	640GB	17%

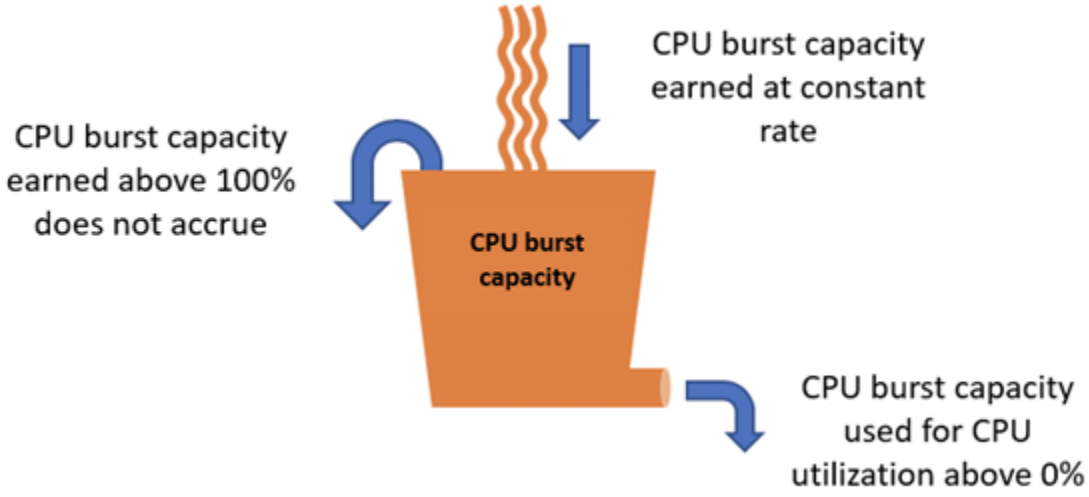
查看 Lightsail 实例的 CPU 突发容量累积

Amazon Lightsail实例计划，除了 384美元的Linux或Unix和574美元的 Windows 计划外，每小时累积的CPU突发容量为4.17%。可累积的最大 CPU 容量爆增等于 24 小时内可获得的 CPU 容量爆增百分比。当您的实例 CPU 容量爆增百分比达到 100% 时，将停止累积。

Important

累积的 CPU 容量突增

- Linux 或 Unix 384 USD 和 Windows 574 USD 实例计划 – 这些计划不会累积 CPU 容量爆增。它们将根据需要自动爆增。
- 2023 年 6 月 29 日之前创建的实例 – 如果您的实例停止，CPU 容量爆增不会持久。如果您停止实例，它将失去所有累积的容量突增。
- 在 2023 年 6 月 29 日当天或之后创建的实例 – CPU 容量爆增在实例停止和启动之间持久存在七天。
- 正在运行的实例的累积 CPU 突增容量不会过期。

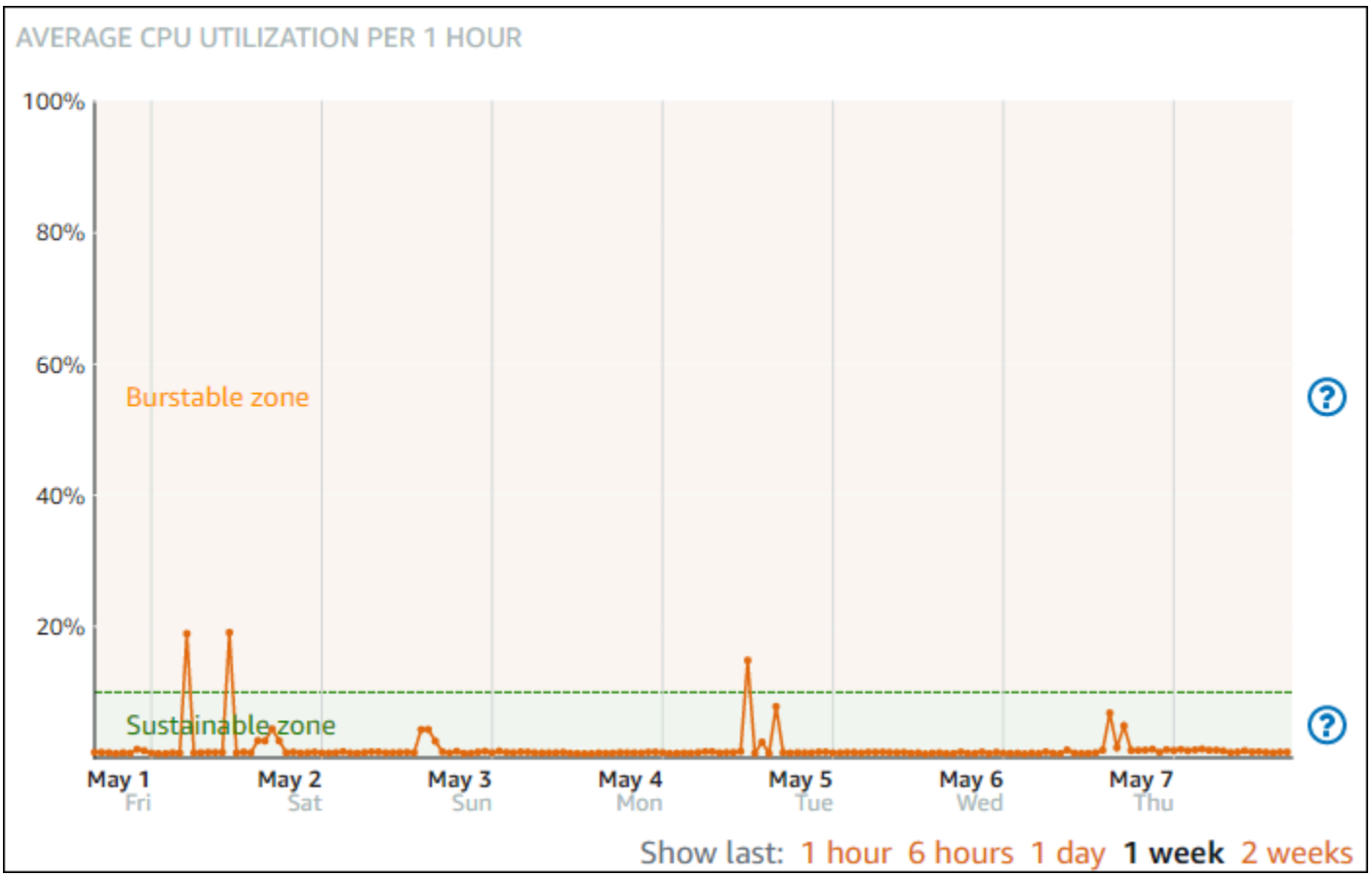


Lightsail 实例在启动时会获得额外的 CPU 突发容量，这称为启动 CPU 突发容量。启动 CPU 突增容量允许实例在启动后立即突增，然后再累积额外的突增容量。启动 CPU 突增容量不计入突增容量限制。如果您的实例尚未消耗其启动 CPU 突增容量，并且在 24 小时内处于空闲状态，同时累积更多突增容量，则其 CPU 突增容量（百分比）指标图表将显示为超过 100%。

此外，一些 Lightsail 实例以启动模式启动，这会暂时消除突发性能实例上通常存在的一些性能限制。使用启动模式时，您可以在启动时运行资源密集型脚本，而不会影响实例的整体性能。

确定你的 Lightsail 实例何时爆发

在实例的 CPU 利用率指标图表上，您将看到一个可持续区域和一个可突增区域。在以下 CPU 利用率指标图表示例中，性能基线为 10%，因为实例使用基于 Linux 或 Unix 的 7 USD/月实例计划。

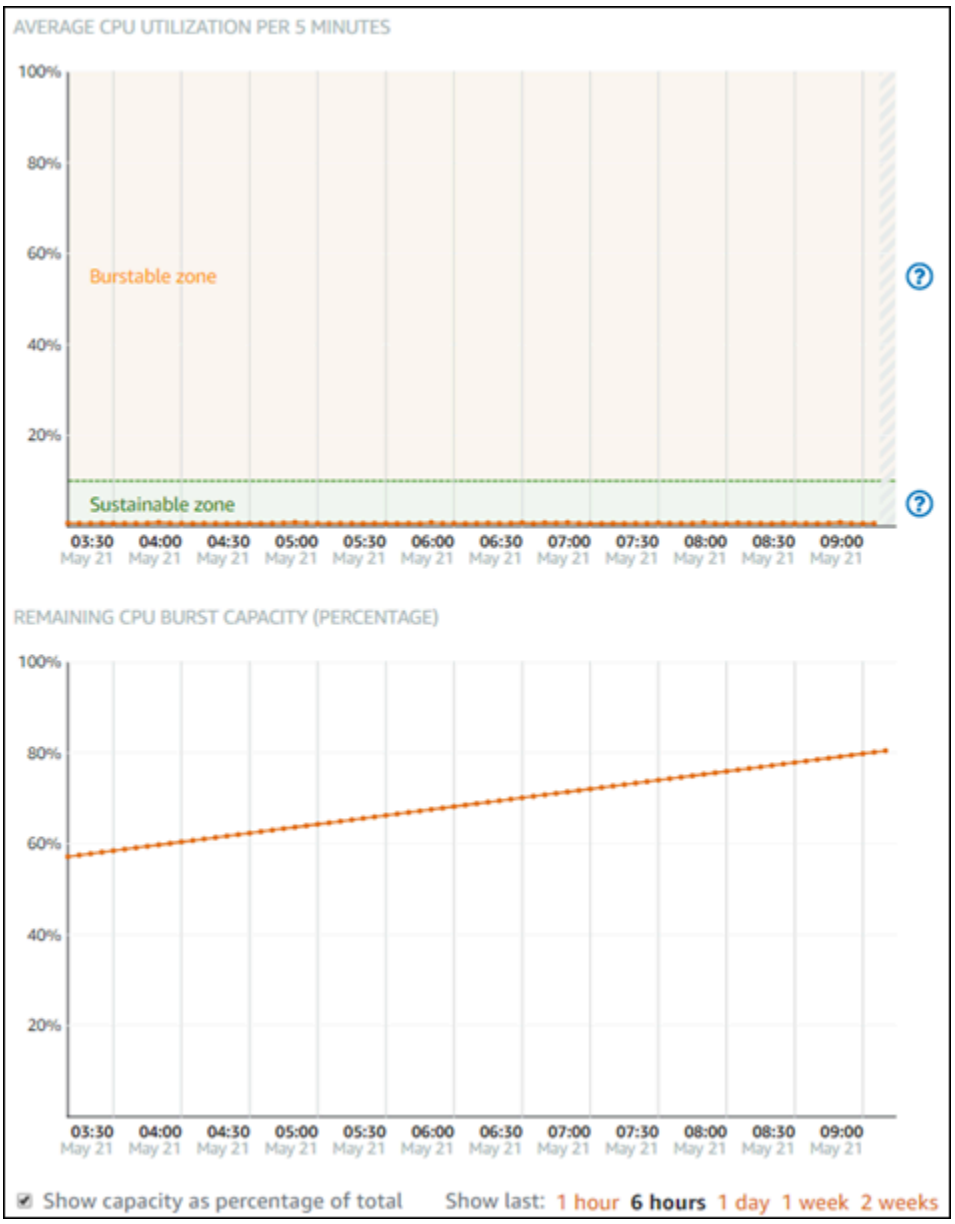


您的 Lightsail 实例可以在可持续区域中无限期地运行，而不会影响系统的运行。您的实例可能会在负载较重的情况下在可突增区域中开始运行，例如编译代码、安装新软件、运行批处理作业或满足峰值负载请求时。在可突增区域内运行时，您的实例会消耗更多的 CPU 周期。因此，它只能在此区域内运行一段有限的时间。

您的实例可以在可突增区域内运行的时段取决于它在可突增区域内的深度。与在可突增区域的较高端运行的实例相比，在可突增区域的较低端运行的实例的突增时段可能会更长。但是，已在可突增区域内的任何位置持续一段时间的实例最终将耗尽所有 CPU 容量，直到它再次在可持续区域内运行。因此，还必须监控剩余的 CPU 突增容量，本指南以下部分将介绍这一内容。

监控 Lightsail 实例的 CPU 突发容量

Lightsail 控制台中的 CPU 概述页面显示您的实例的 CPU 利用率与其可用 CPU 突发容量的比较。在以下 CPU 概览示例中，CPU 容量爆增百分比有所增加，因为实例在可持续区域中一直低于基线运行。



剩余 CPU 容量爆增图表视图可在 CPU 容量爆增百分比和分钟数之间切换。在突增区域中运行时，您的实例会消耗更多 CPU 突增容量。CPU 突增容量分钟数指标是您的实例以 100% CPU 利用率突发的可用时间。在可突增区域中运行时，实例的消耗速度与实例当前 CPU 利用率百分比相同。例如，基于 Linux 或 Unix 的 7 USD/月实例的 CPU 利用率基准为 10%，每小时累积 6 分钟的 CPU 突增容量分钟数。因此，如果实例在以下情况下运行：

- 在可突增区域中以 100% CPU 利用率运行 60 分钟，那么会在该期间以 100% 的速率消耗 CPU 突增容量分钟数。实例消耗 60 分钟的 CPU 突增容量，累积 6 分钟，净消耗 54 分钟。
- 在可突增区域中以 50% CPU 利用率运行 60 分钟，那么会在该期间以 50% 的速率消耗 CPU 突增容量分钟数。实例消耗 30 分钟的 CPU 突增容量，累积 6 分钟，净消耗 24 分钟。

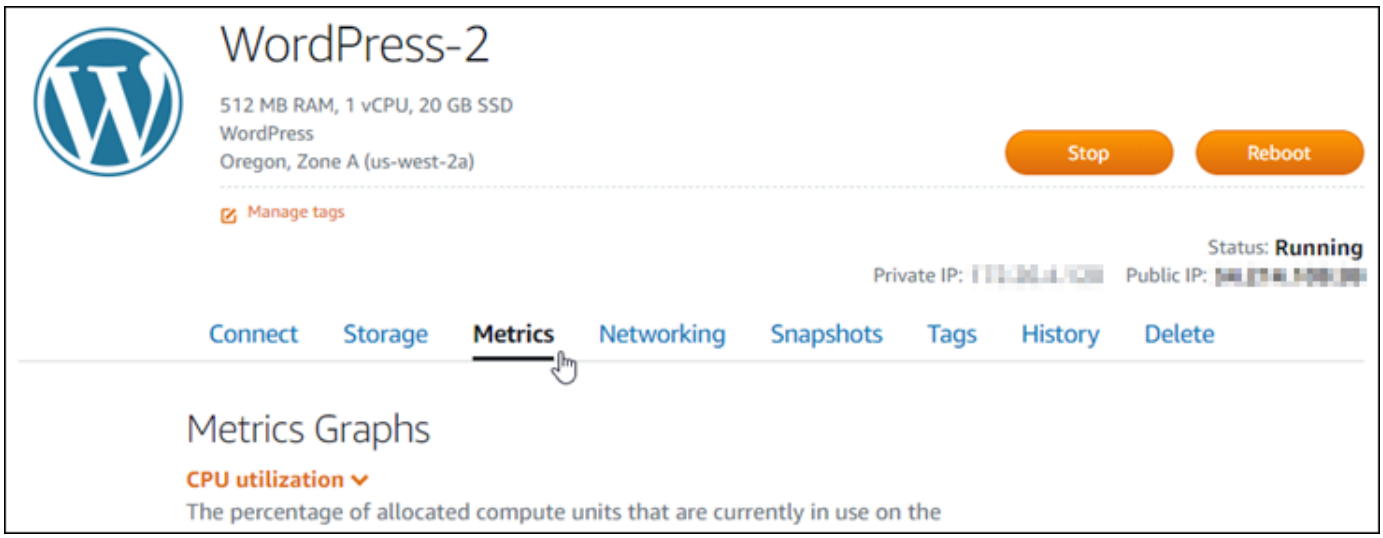
- 在实例的基准以 10% CPU 利用率运行 60 分钟，那么会在该期间以 10% 的速率消耗 CPU 突增容量分钟数。实例消耗 6 分钟的 CPU 突增容量，累积 6 分钟。当实例以其基准运行时，CPU 突增容量分钟数不会增加或减少。
- 在可持续区域中以 5% CPU 利用率运行 60 分钟，那么会在该期间以 5% 的速率消耗 CPU 突增容量分钟数。实例消耗 3 分钟的 CPU 突增容量，累积 6 分钟，净累积 3 分钟。

或者，如果实例累积了 60 分钟的 CPU 突增容量，那么它能够以 100% CPU 利用率运行 60 分钟内，以 50% CPU 利用率运行 120 分钟，或者以 25% CPU 利用率运行 150 分钟。

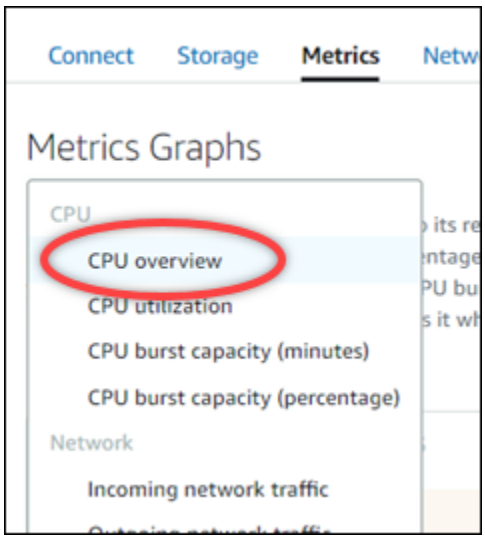
查看 Lightsail 实例的 CPU 利用率和突发容量

完成以下步骤以访问 CPU 概览页面，并查看实例的 CPU 利用率和剩余 CPU 突增容量。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，选择要查看其 CPU 利用率和突发容量的实例的名称。
3. 选择实例管理页面上的 Metrics（指标）选项卡。



4. 在 Metrics graphs（指标图表）标题下的下拉菜单中选择 CPU overview（CPU 概览）。



该页显示 Average CPU utilization per 5 minutes（每 5 分钟的平均 CPU 利用率）和 Remaining CPU burst capacity（剩余 CPU 突增容量）图表。

> **Note**
>
> 您创建实例后，Remaining CPU burst capacity（剩余 CPU 突增容量）图表可能会在短期内显示 Launch mode（启动模式）区域。某些 Lightsail 实例以启动模式启动，这会暂时消除突发性能实例上通常存在的一些性能限制。使用启动模式时，您可以在启动时运行资源密集型脚本，而不会影响实例的整体性能。



5. 您可以对指标图表执行以下操作：

   - 对于突增容量图表，选择 Show capacity as percentage of total（将容量显示为总容量百分比），以将视图从可用突增容量分钟数更改为可用突增容量百分比。
   - 更改图表的视图以显示 1 小时、6 小时、1 天、1 周和 2 周的数据。
   - 将光标停在一个数据点上可查看有关该数据点的详细信息。
   - 添加告警，以便在 CPU 利用率和突增容量超过您指定的阈值时收到通知。无法在 CPU 概览页面中添加告警。您必须在单个 CPU 利用率、CPU 容量爆增百分比和 CPU 容量爆增分钟数指标图表页中添加告警。有关更多信息，请参阅警报和创建实例指标警报。

解决您的 Lightsail 实例的 CPU 使用率过高的问题

如果您的实例频繁在突增区域运行或长时间运行，将使用其所有突增容量。这可能表示您的实例预置不足。也可能是服务运行频率过高，或者您的实例正在运行不必要的软件。

使用 Linux/Unix 实例上的工具和 Windows Server 实例上的任务管理器，调查导致您的实例突增的原因。这些工具可向您显示哪些服务在消耗实例上的资源。确定哪些服务消耗的资源最多，并确定是否可以在不影响实例工作负载的情况下禁用这些服务。通过禁用服务或卸载软件，您应该可以降低实例的突增，并避免增加实例的大小。

如果您的实例确实没有充分预置，并且您无法降低其 CPU 利用率，可以通过添加更多的处理能力来减少突增容量消耗。为此，您可以创建实例的快照，然后使用更大的 Lightsail 实例计划从快照中创建一个新实例。例如，对您的新实例使用基于 Linux 或 Unix 的 24 USD/月计划，而不是使用上一个实例使用的基于 Linux 或 Unix 的 12 USD/月计划。当您的新实例启动并运行时，根据需要对工作负载的 DNS 进行更改，以便将旧实例与新实例交换。在流量开始路由到新实例后，删除未充分预置的旧实例。有关更多信息，请参阅快照。

连接并管理你的 Lightsail 实例

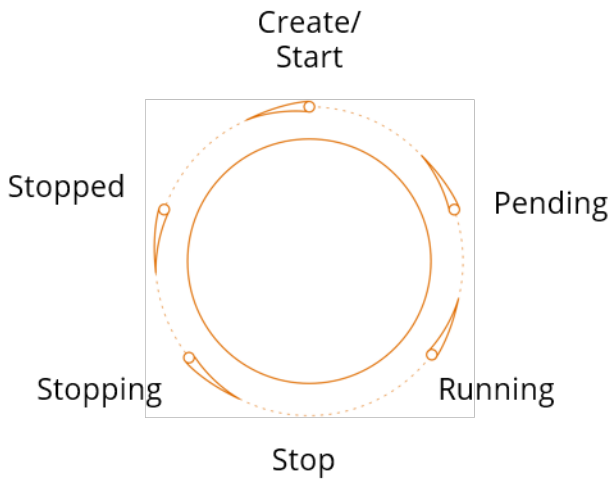
本指南涵盖以下与管理和连接您的 Amazon Lightsail 实例相关的主题：

主题

- 启动、停止或重启你的 Lightsail 实例
- 强制停止卡住的 Lightsail 实例
- 为 Amazon EC2 实例启用增强联网
- 在 Lightsail 中扩展 Windows 服务器实例的文件系统
- 在 Lightsail 中使用启动脚本配置 Linux/Unix 实例
- 使用批处理 PowerShell 脚本配置 Windows Lightsail 实例
- 在 Lightsail 上保护 Windows 服务器实例

启动、停止或重启你的 Lightsail 实例

当 Amazon Lightsail 创建您的实例时，您的计算机在开始运行之前会进入待处理状态。在您的实例运行后，您可以将其重启或停止，然后再启动它。周期如下所示：

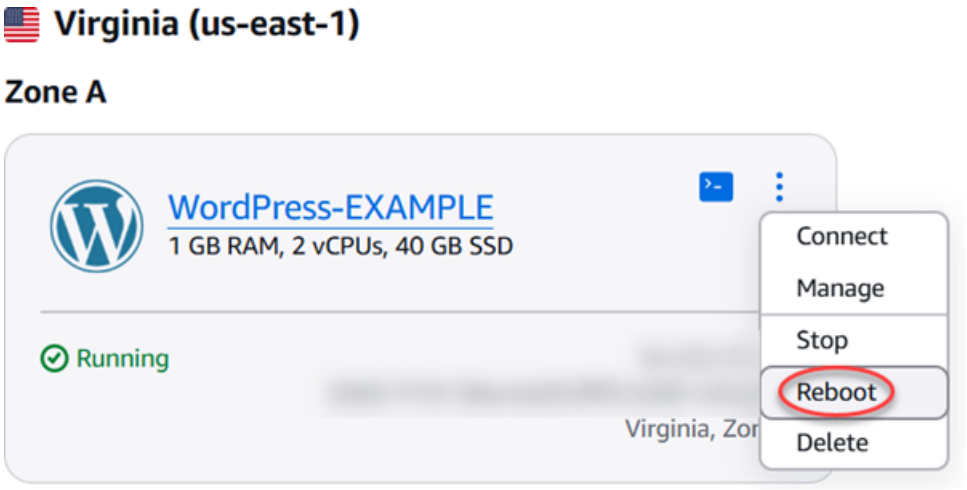


当您在主页上管理或查看实例时，可以看到实例状态。

> **Important**
>
> 当您停止和启动实例时，在创建实例时分配给您的实例的默认公有 IPv4 地址将发生变化。您可以选择创建静态 IPv4 地址并将其附加到您的实例。静态 IPv4 地址取代了实例的默认公有 IPv4地址，当您停止和启动实例时，静态地址将保持不变。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

在实例运行时重启实例

- 在主页上，选择要重启的实例，或者从管理实例菜单中选择重启。

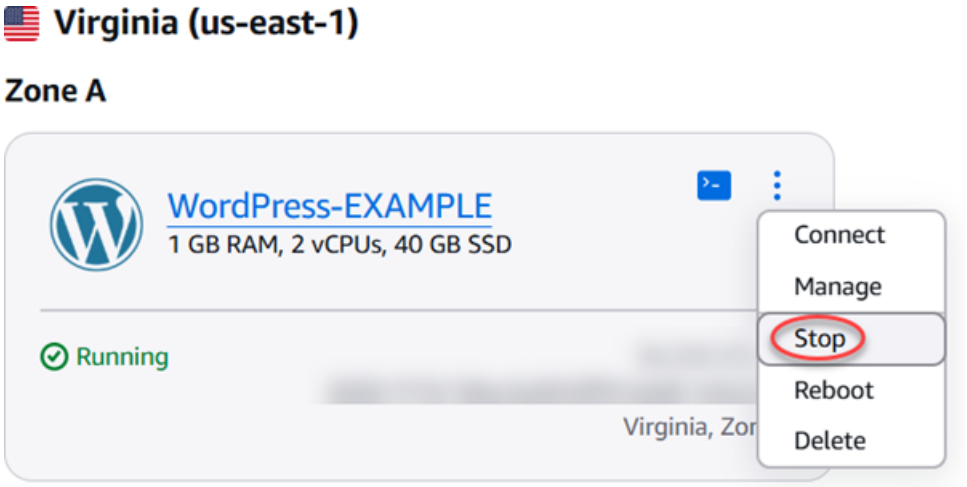


  如果您从实例管理页面查看实例，请选择重启，然后在出现提示时选择确认。

> **Note**
>
> 要重启您的实例，它必须处于运行状态。

停止正在运行的实例

- 在主页上，选择要停止的实例，或从管理实例菜单中选择 Stop（停止）。

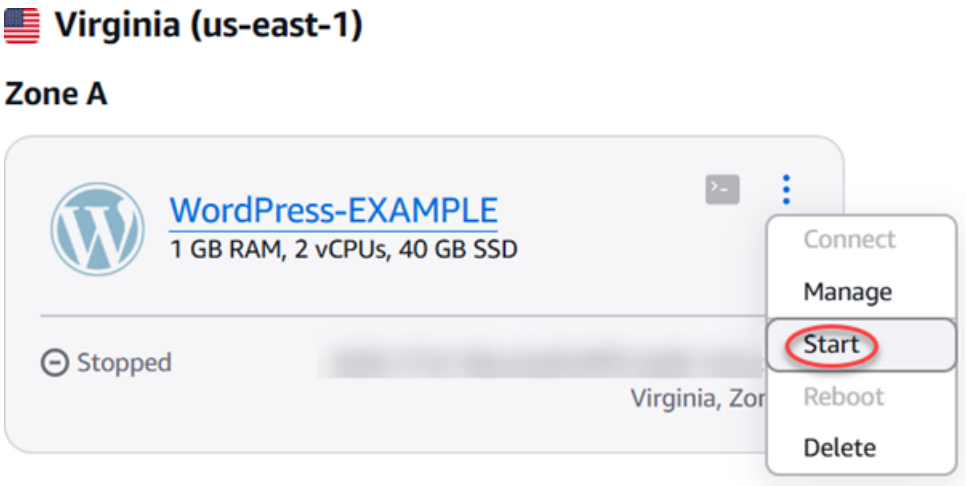


如果您正在从实例管理页面查看您的实例，请选择 Stop（停止），然后在系统提示时选择 Confirm（确认）。

> **Note**
>
> 要停止您的实例，实例必须处于 Running（正在运行）状态。

在实例停止后启动它

- 在主页上，选择要启动的实例，或从管理实例菜单中选择 Start（启动）。



如果您正在从实例管理页面查看您的实例，请选择 Start（启动）。

> **Note**
>
> 要启动您的实例，实例必须处于 Stopped（已停止）状态。

强制停止卡住的 Lightsail 实例

在极少数情况下，实例会卡在 `Stopping` 状态。如果发生这种情况，则托管您的 Amazon Lightsail 实例的底层硬件可能会出现问题。在本指南中，您将学习如何强制停止卡在 `stopping` 状态的实例。有关实例状态的更多信息，请参阅启动、停止或重启您的 Lightsail 实例。

如何强制停止实例

您可以使用 Lightsail 控制台强制停止您的实例，但只能在实例处于状态时使用。`stopping`另外，在实例处于除 `shutting-down` 和 `terminated` 以外的任何状态时，您可以使用 AWS Command Line Interface（AWS CLI）强制停止实例。强制停止操作可能需要几分钟才能完成。如果该实例在 10 分钟后仍未停止，请再次执行强制停止。

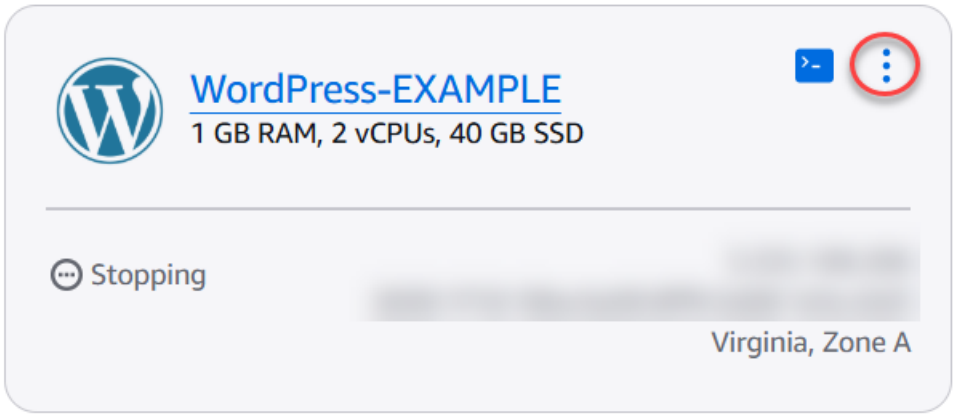
被强制停止的实例无法刷新文件系统缓存或文件系统元数据。强制停止实例后，您应执行文件系统检查和修复程序。

以下过程说明了强制停止 Lightsail 实例的不同方法。

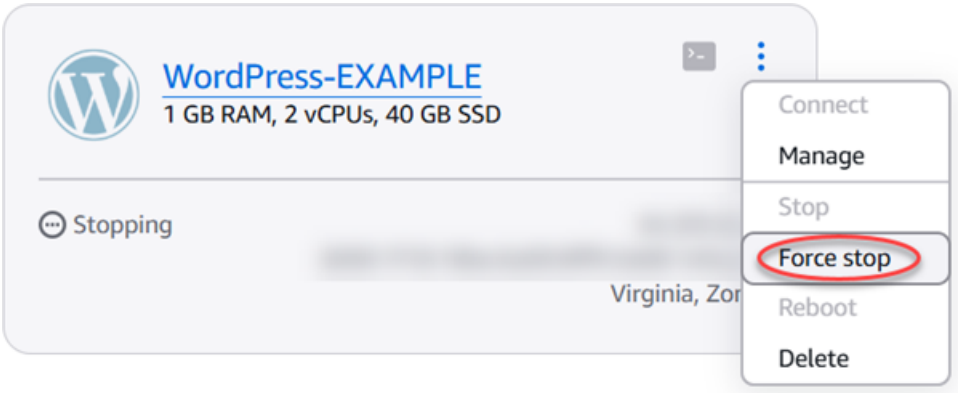
在 Lightsail 控制台中强制停止实例

1. 登录 Lightsail 控制台。

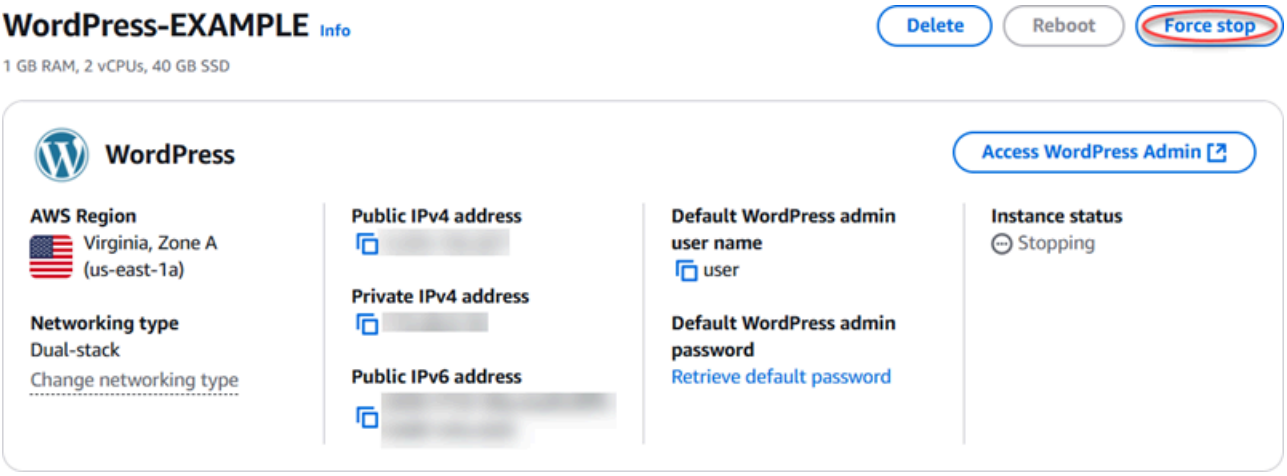
2. 选择 Instances 选项卡。
3. 找到卡在 `Stopping` 状态的实例。然后，选择实例名称旁边显示的操作菜单图标（⋮）。



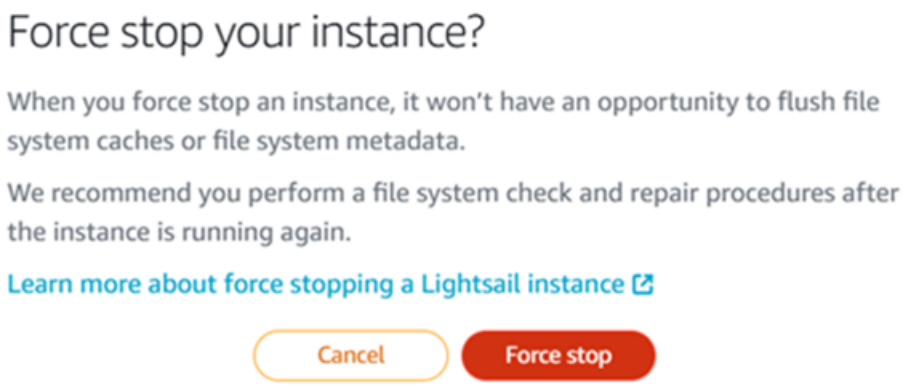
4. 在显示的下拉列表中，选择强制停止。



或者，您也可以选择实例名称来访问实例管理页面。然后，选择强制停止按钮。



5. 查看此操作的注意事项。要继续，请选择强制停止。



使用强制停止实例 AWS CLI

1. 在开始之前，您需要安 AWS CLI。要了解更多信息，请参阅安装 AWS Command Line Interface。安装后，请务必配置 AWS CLI。
2. 使用 stop-instance 命令和 `--force` 参数，如下所示：

```
aws lightsail stop-instance --instance-name Wordpress-1 --force
```

为 Amazon EC2 实例启用增强联网

某些 Lightsail 实例与当前一代的 EC2 实例类型（T3、M5、C5 或 R5）不兼容，因为它们未启用增强联网功能。如果您的源 Lightsail 实例不兼容，则在根据导出的快照创建实例时，您需要选择上一代实例类型（T2、M4、C4 或 R4）。 EC2 在使用 Lightsail 控制台中的 “创建亚马逊 EC2 实例” 页面创建 EC2 实例时，会向您显示这些实例类型选项。

> **Note**
>
> 有关增强联网的更多信息，请参阅 Amazon EC2 文档中的 Linux 上的增强联网或 Windows 上的增强联网。

要在源 Lightsail 实例不兼容时使用最新一代 EC2 的实例类型，您需要使用上一代 EC2 实例类型（T2、M4、C4 或 R4）创建新实例，更新实例上的网络驱动程序，然后将该实例升级到所需的当前一代实例类型。

先决条件

您必须使用导出的 Lightsail 快照创建亚马逊 EC2 实例。如果您的 Lightsail 实例不兼容，您将在创建亚马逊实例时选择上一代实例类型（T2、M4、C4 或 R4）。 EC2 要了解更多信息，请参阅在 Lightsail 中使用导出的快照创建亚马逊 EC2实例。

新 EC2 实例启动并运行后，请继续阅读本指南的使用弹性网络适配器启用增强联网部分，了解如何启用增强联网。

启用 Elastic Network Adapter 增强联网

新实例启动并运行后，请参阅 Amazon EC2 文档中的以下指南之一，使用弹性网络适配器 (ENA) 启用增强联网：

- 在 Linux 实例上启用 ENA 增强联网
- 在 Windows 实例上启用 ENA 增强联网

升级实例类型

启用增强联网后，您可以按照以下任一指南中的说明升级实例类型：

- 对于 Windows Server 实例 – 迁移到最新一代实例类型
- 对于 Linux 或 Unix 实例 – 更改实例类型

在 Lightsail 中扩展 Windows 服务器实例的文件系统

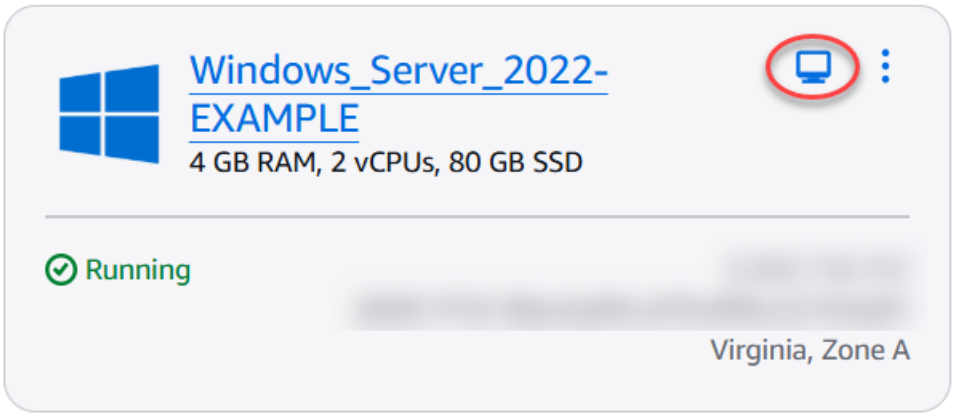
您使用快照创建新的具有更大计划的 Windows Server 实例后，可能会看到可用的存储空间小于计划指定的存储空间。这通常是因为更大计划提供的额外存储空间尚未被分配；因此，活动卷未使用它。本主题中的步骤将向您演示如何扩展 Windows Server 实例的文件系统以使用尽可能大的存储空间。

> **Note**
>
> 仅当您使用在运行 System Preparation (Sysprep) 实用程序之前创建的快照来创建 Windows Server 实例时，才会出现此情形。有关更多信息，请参阅创建 Windows Server 实例的快照。

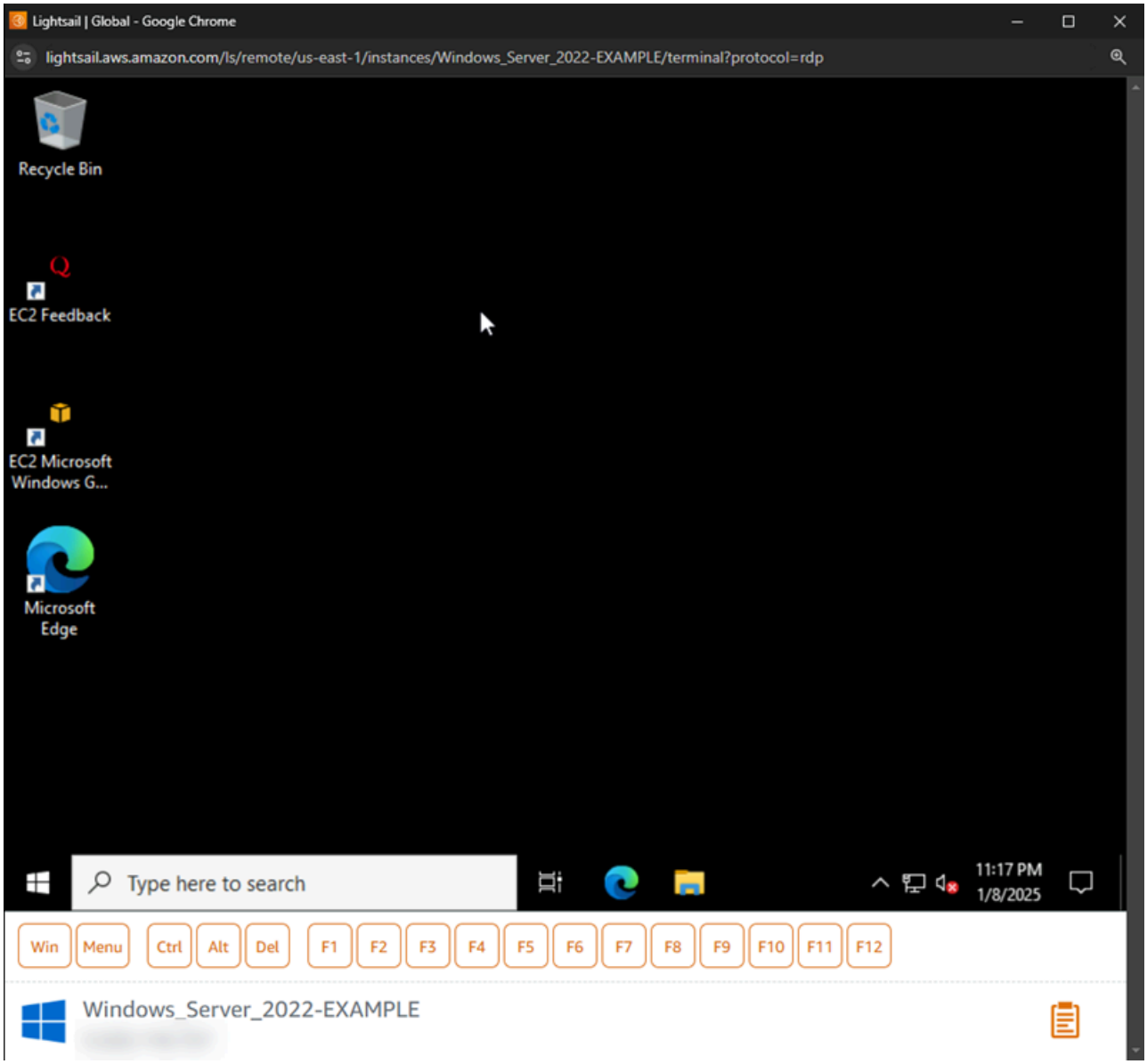
要扩展 Windows Server 实例的文件系统

1. 登录 Lightsail 控制台。

2. 在 Lightsail 主页上，选择要连接的实例的 RDP 客户端图标。



此时系统会打开基于浏览器的 RDP 客户端窗口，如下例所示：

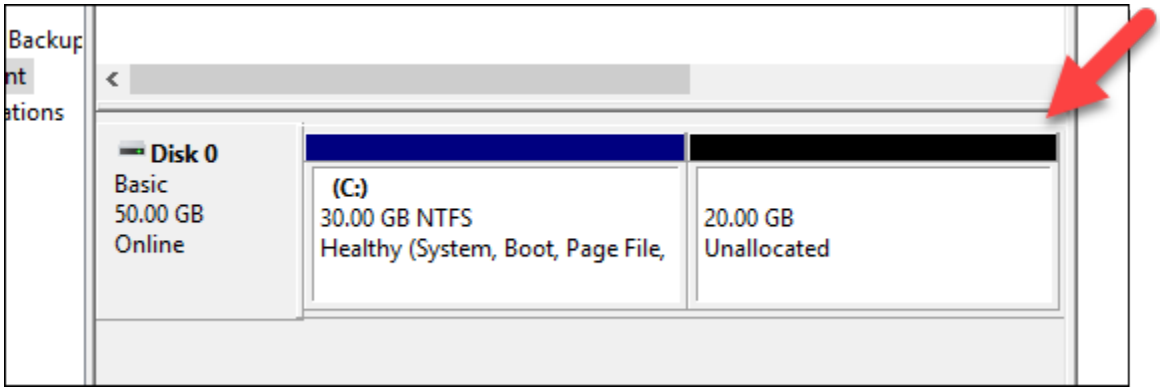


3. 在任务栏中，选择 Windows 图标，然后选择以下选项之一：

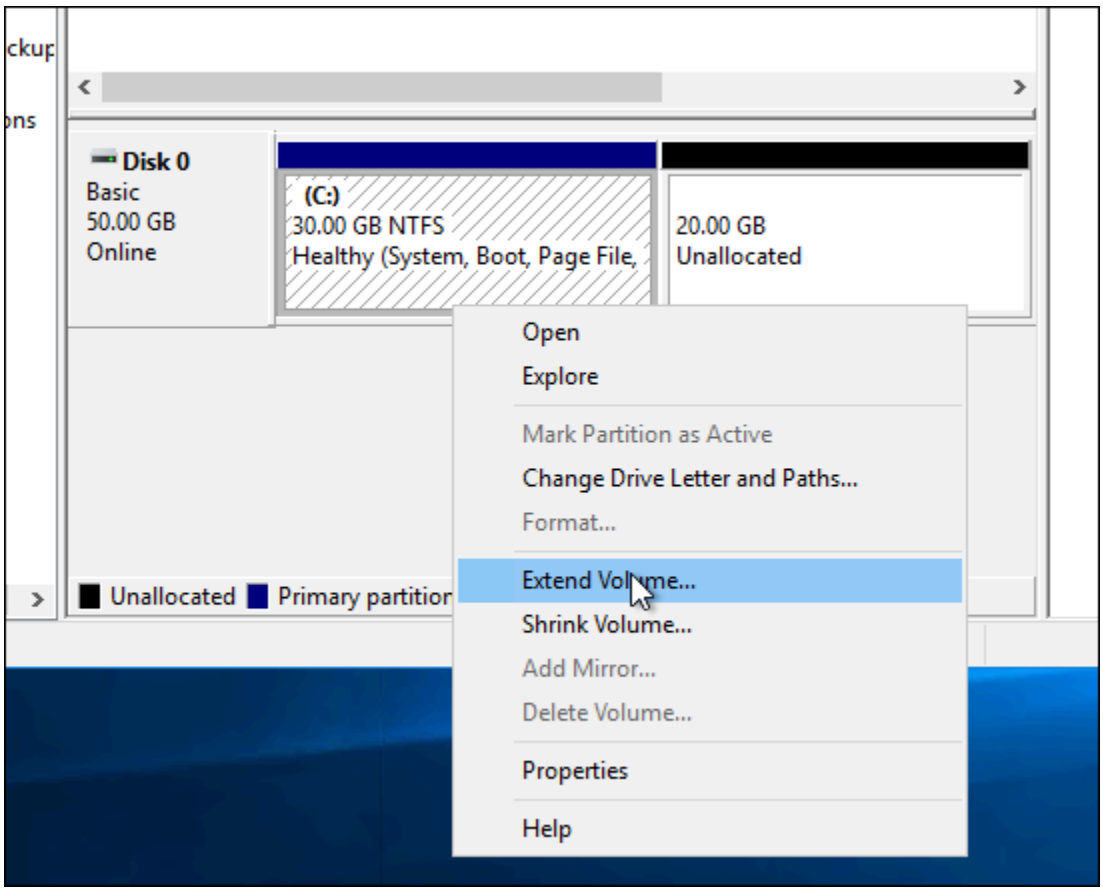
   - 在 Windows Server 2022、Windows Server 2019 和 Windows Server 2016 实例上，选择开始，然后选择 Windows 管理工具。

4. 选择 Computer Management（计算机管理）。
5. 在 Computer Management（计算机管理）控制台的左侧窗格中，选择 Disk Management（磁盘管理）。
6. 在 Actions（操作）菜单上，选择 Rescan Disks（重新扫描磁盘）。

   您可能会看到与磁盘关联的未分配空间。扩展磁盘上的活动卷以使用未分配的空间。

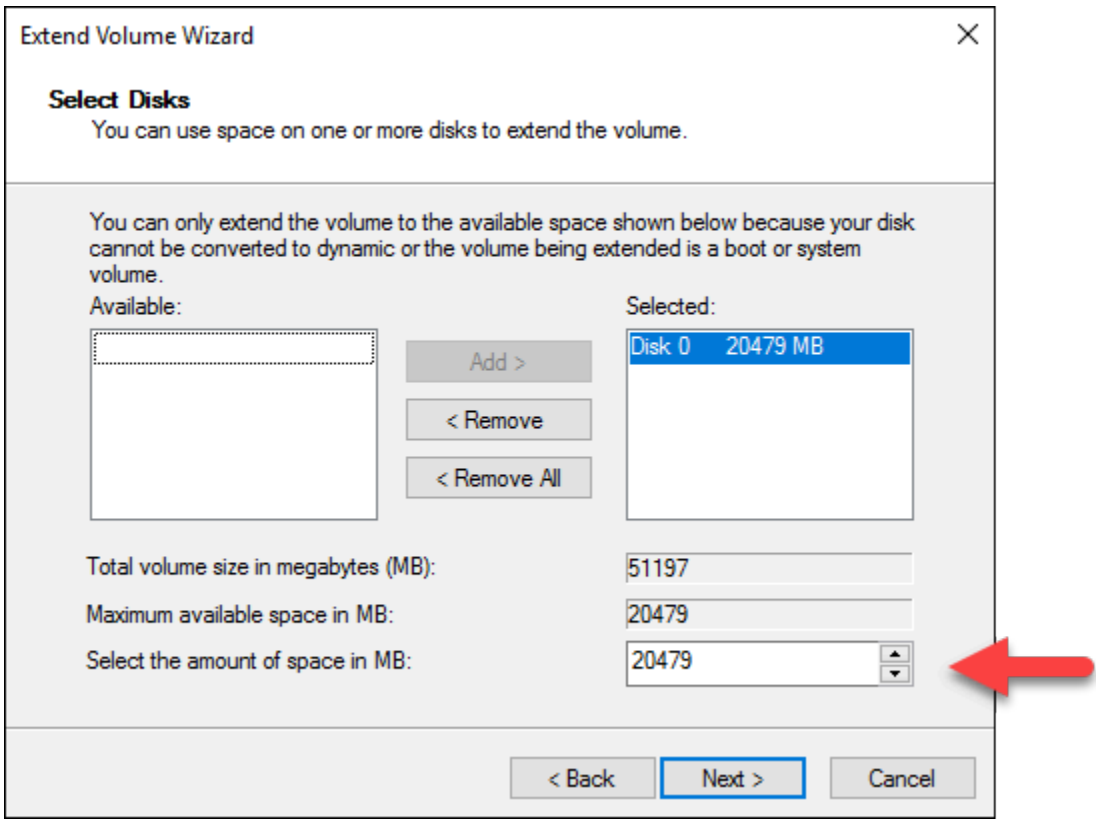


7. 右键单击未分配空间所在磁盘上的活动卷，然后选择 Extend Volume（扩展卷）。



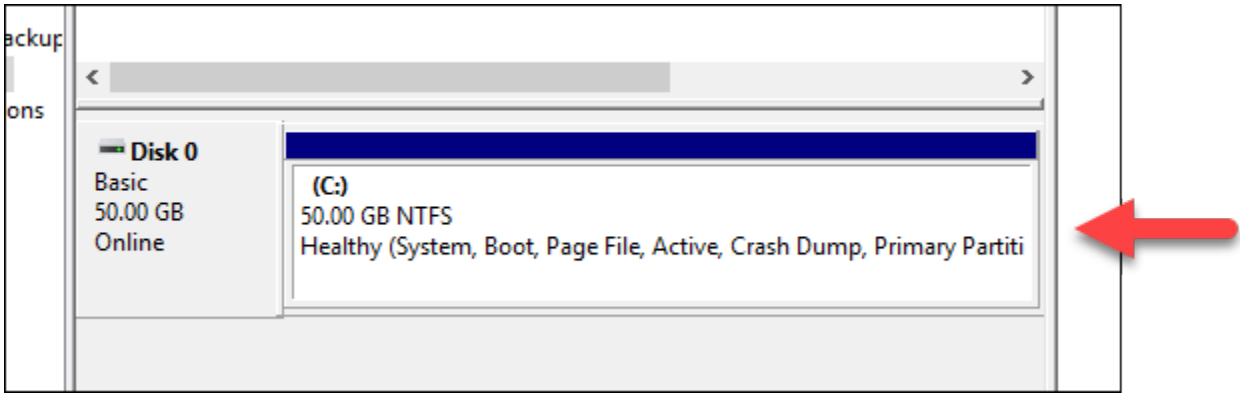
8. 扩展卷向导打开时，选择 Next（下一步）。

9. 在 Select the amount of space in MB（选择空间大小（以 MB 为单位））字段中，输入将卷扩展多少兆字节。通常，您可以将此设置为最大未分配空间。您输入的值是您要添加的空间大小，而不是卷的最终大小。



10. 完成扩展卷向导。

    扩展活动卷以使用指定的未分配空间。以下示例显示了所有已选择的未分配空间。



在 Lightsail 中使用启动脚本配置 Linux/Unix 实例

在创建基于 Linux 或 Unix 的实例时，您可以添加启动脚本以添加或更新软件，或以某种其他方式配置实例。要使用其他数据配置基于 Windows 的实例，请参阅使用 Windows 配置您的新 Lightsail 实例。PowerShell

> **Note**
>
> 根据您选择的系统映像，用于使软件在实例上运行的命令会有所不同。亚马逊 Linux 使用`yum`，而 Debian 和 Ubuntu 都使用。`apt-get` WordPress 而其他应用程序映像`apt-get`之所以使用，是因为它们将 Debian 作为操作系统运行。FreeBSD 以及 openSUSE 需要额外的用户配置才能使用自定义工具，例如`freebsd-update`或 `zypper` (openSUSE).

示例：配置 Ubuntu 服务器以安装 Node.js

以下示例更新程序包列表，然后通过 `apt-get` 命令安装 Node.js。

1. 在创建实例页面上，选择仅限操作系统选项卡上的 Ubuntu。
2. 向下滚动并选择 Add launch script (添加启动脚本)。
3. 键入以下内容：

```
# update package list
apt-get update -y
# install some of my favorite tools
apt-get install nodejs -y
```

> **Note**
>
> 您发送的用于配置服务器的命令作为根运行，因此，您无需在命令前包含 `sudo`。

4. 选择创建实例。

示例：将 WordPress服务器配置为下载和安装插件

以下示例更新了软件包列表，然后下载并安装了的BuddyPress 插件 WordPress。

1. 在创建实例页面上，选择WordPress。
2. 选择 Add launch script（添加启动脚本）。
3. 键入以下内容：

```
# update package list
apt-get update
# download wordpress plugin
```

```
wget "https://downloads.wordpress.org/plugin/buddypress.14.0.0.zip"
apt-get install unzip
# unzip into wordpress plugin directory
unzip buddypress.14.0.0.zip -d /bitnami/wordpress/wp-content/plugins
```

4. 选择创建实例。

使用批处理 PowerShell 脚本配置 Windows Lightsail 实例

创建基于 Windows 的实例时，可以使用 Windows PowerShell 脚本或任何其他批处理脚本对其进行配置。这是在您的实例启动后立即运行的一次性脚本。本主题介绍了这些脚本的语法，并提供一个示例以说明如何使用这些脚本。我们还介绍了如何测试您的脚本以确定其是否成功运行。

创建启动并运行 PowerShell 脚本的实例

以下过程会在新实例上安装一个名为 chocolatey 的工具，它在实例启动后立即运行。

1. 在左侧导航窗格中，选择创建实例。
2. 选择要在其中创建实例的 AWS 区域 和可用区。
3. 在 Select a platform（选择平台）下，选择 Microsoft Windows。
4. 选择仅限操作系统，然后选择 Windows Server 2022、Windows Server 2019、Windows Server 2016。
5. 选择 Add launch script（添加启动脚本）。
6. 键入以下内容：

```
<powershell>
iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/
install.ps1'))
</powershell>
```

> **Note**
>
> 必须始终将 PowerShell 脚本封装在<powershell></powershell>标签中。您可以使用<script></script>标签输入非PowerShell命令或批处理脚本，也可以不使用任何标签。

7. 输入实例的名称。

资源名称：

- 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
- 必须包含 2 到 255 个字符。
- 必须以字母数字字符或数字作为开头和结尾。
- 可以包括字母数字字符、数字、句点、连字符和下划线。

8. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

   a. 对于密钥，输入标签密钥。

   b. （可选）在“值”中，输入标签值。

9. 选择 Create instance（创建实例）。

验证您的脚本是否成功运行

您可以登录到您的实例以验证该脚本是否成功运行。基于 Windows 的实例最多可能需要 15 分钟的时间，才能准备好接受 RDP 连接。在准备就绪后，请使用基于浏览器的 RDP 客户端登录或配置您自己的 RDP 客户端。有关更多信息，请参阅连接到基于 Windows 的实例。

1. 连接到 Lightsail 实例后，打开命令提示符（或打开 Windows 资源管理器）。
2. 键入以下命令以转到 Log 目录：

```
cd C:\ProgramData\Amazon\EC2-Windows\Launch\Log
```

3. 在文本编辑器中打开 `UserdataExecution.log`，或者键入以下命令：`type UserdataExecution.log`。

   将会在日志文件中看到以下内容。

```
2017/10/11 20:32:12Z: <powershell> tag was provided.. running powershell content
2017/10/11 20:32:13Z: Message: The output from user scripts: iex ((New-Object
 System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))

2017/10/11 20:32:13Z: Userdata execution done
```

在 Lightsail 上保护 Windows 服务器实例

在本文中，我们提供了一些提示和技巧，以帮助您在使用运行 Windows Server 的 Lightsail 实例时避免安全风险。

关于 Lightsail 密码

当你创建基于 Windows 服务器的实例时，Lightsail 会随机生成一个难以猜测的长密码。请仅在新实例上使用该密码。您可以使用默认密码通过远程桌面 (RDP) 快速连接到您的实例。您始终以管理员身份登录您的 Lightsail 实例。

管理密码

您可以在基于 Windows Server 的实例上更改密码。如果您想使用远程桌面客户端来访问您的 Lightsail 实例，这可能会很有用。Lightsail 从不存储你生成的密码。

> **Note**
>
> 您可以在 Lightsail 中使用基于浏览器的 RDP 客户端，也可以使用 LightSail 生成的密码或自己的自定义密码。如果使用自定义密码，每次登录时，将会提示您输入密码。如果您想快速访问您的实例，则在基于浏览器的 RDP 客户端上使用 LightSail 生成的默认密码会更容易。

可以使用 Windows Server 密码管理器安全地更改您的密码。请按 `Ctrl + Alt + Del`，然后选择 Change a password (更改密码)。请务必记录您的密码，因为 Lightsail 不会存储您的密码。如果您需要找回密码，请参阅以下内容：更改基于 Windows 的实例的管理员密码。

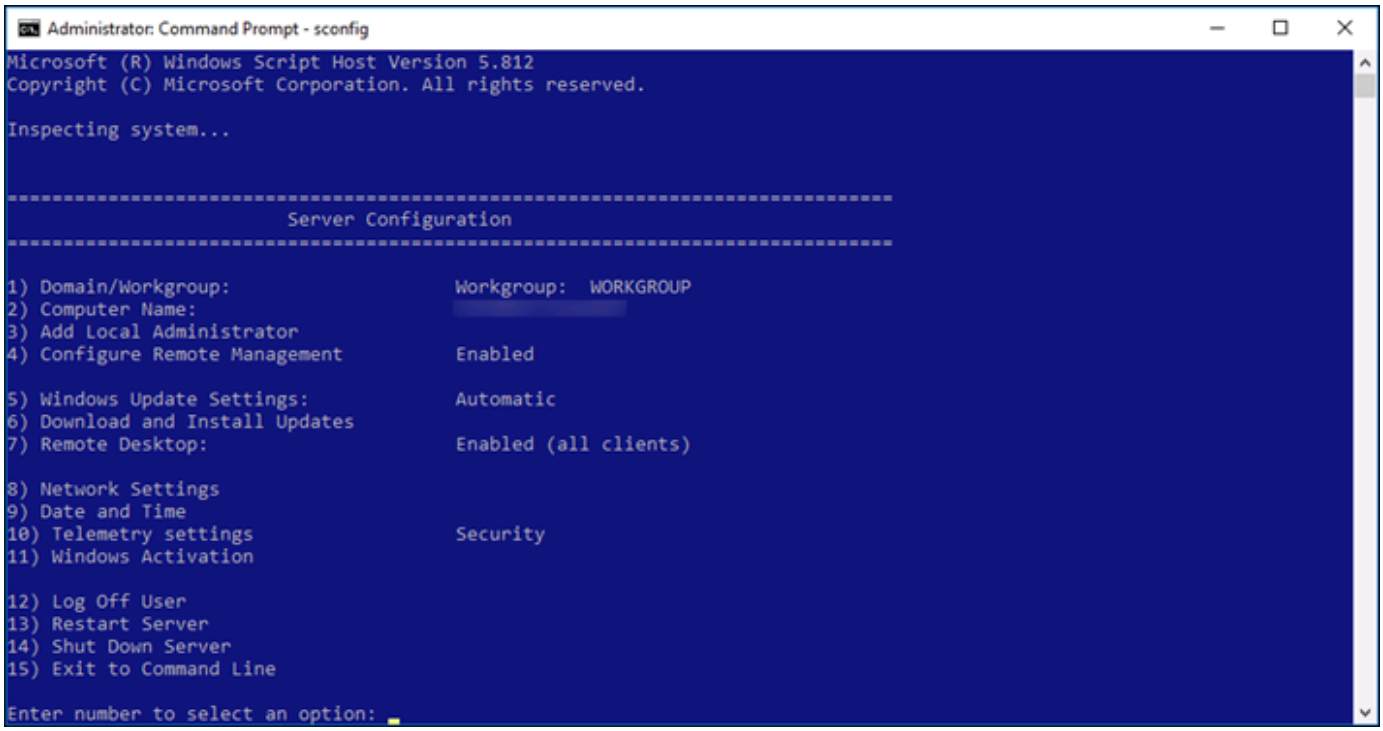
如果将密码更改为非默认唯一密码，请务必使用增强密码。应避免使用基于名称或词典单词的密码，或者避免使用具有重复字符序列的密码。

安全修补

我们建议使用最新的安全补丁更新基于 Windows 服务器的 Lightsail 实例。请确保配置您的服务器以下载并安装更新。以下过程告诉你如何直接在运行 Windows Server 的 Lightsail 实例上执行此操作。

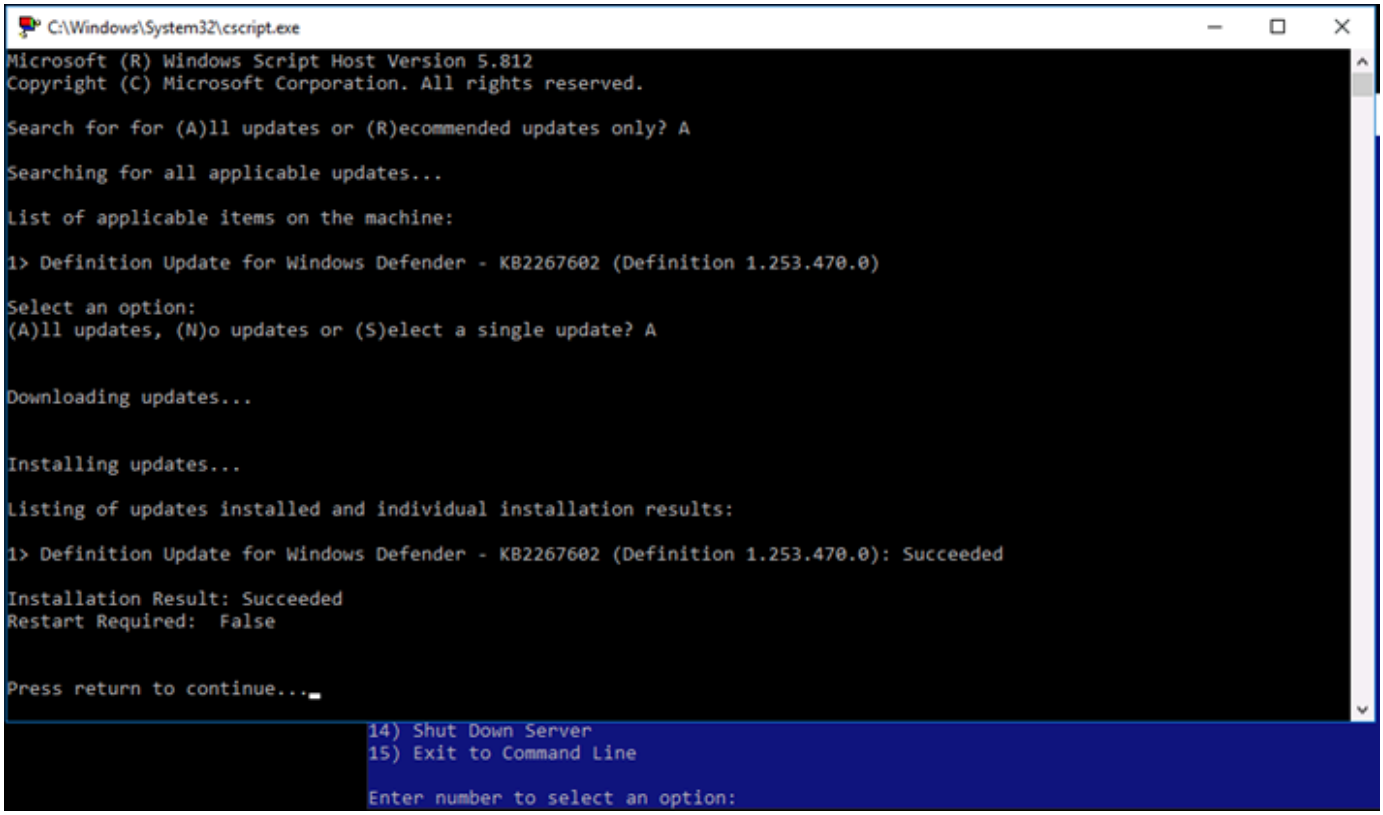
1. 在基于 Windows Server 的实例上，打开命令提示符。
2. 键入 `sconfig`，然后按 `Enter`。

   默认情况下，Windows Update 设置 (编号 5) 为 `Automatic`。



3. 要下载并安装新的更新，请键入 `6`，然后按 `Enter`。
4. 键入 `A` 以在新命令窗口中搜索 (A)ll updates (所有更新)，然后按 `Enter`。
5. 再次键入 `A` 以安装所有更新，然后按 `Enter`。

   在完成后，将显示一条消息，其中包含安装结果和更多说明 (如果适用)。



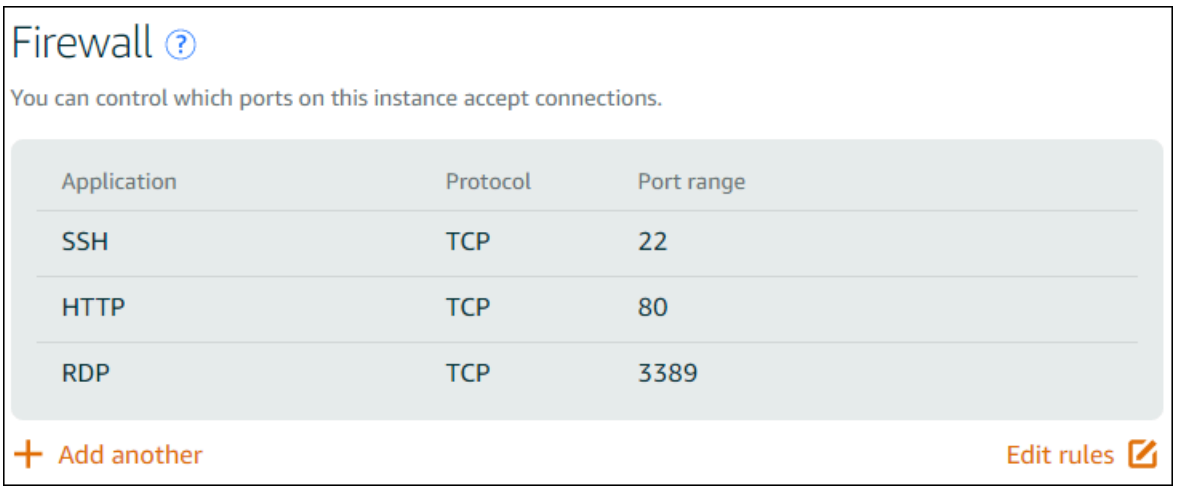
在 Windows Server 中启用账户锁定策略

您可以配置 Windows Server，以便在达到一定数量的失败登录尝试时临时或无限期地禁用账户。例如，您可以锁定尝试使用三个失败密码登录到实例的用户。

有关更多信息，请参阅 Windows Server 文档 中的账户锁定策略。

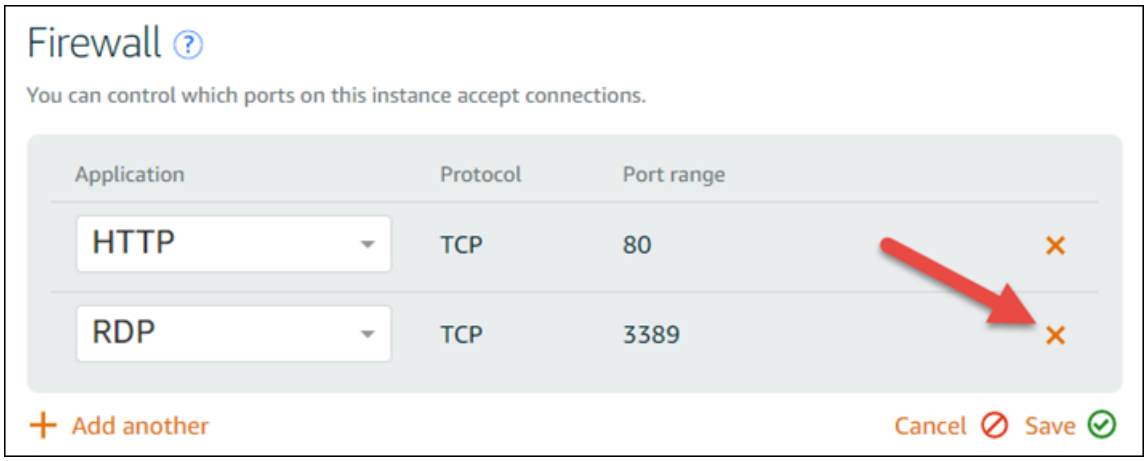
端口和防火墙设置

默认情况下，我们在基于 Windows Server 的实例上打开以下端口。



您启用的端口将向外部环境公开，而无法按源 IP 进行限制。要限制访问您的实例，您可以禁用这些端口，而仅在需要访问您的实例时启用这些端口。方法如下：

1. 在 Lightsail 中找到你要管理的实例，然后选择管理。
2. 选择联网。
3. 在您实例的联网页面中，选择编辑规则。
4. 选择 RDP/TCP/3389 规则旁边的橙色“x”以删除该规则。



5. 选择保存。

按照 step-by-step说明学习如何控制实例的状态、强制停止卡住的实例、更新实例以增强联网、扩展 Windows Server 实例的文件系统、使用脚本在启动时配置实例，以及如何保护您的 Windows Server 实例。

该指南涵盖 Linux 或 Unix 和 Windows Server 实例，针对安装软件、更新配置、管理密码、启用安全补丁和配置防火墙设置等任务提供提示和最佳实践。通过遵循本指南，您可以有效地管理和保护 Lightsail 实例，确保针对您的特定用例实现最佳性能、安全性和自定义。

删除 Lightsail 实例

如果您不再需要某个实例，则可以使用 Amazon Lightsail 控制台或 AWS Command Line Interface ()AWS CLI将其删除。一旦删除该实例，它将不再产生费用。然而，附加到已删除实例的资源会继续产生费用，直至您将其删除。有关这些资源以及如何在删除实例后将其删除的更多信息，请参阅 后续步骤。

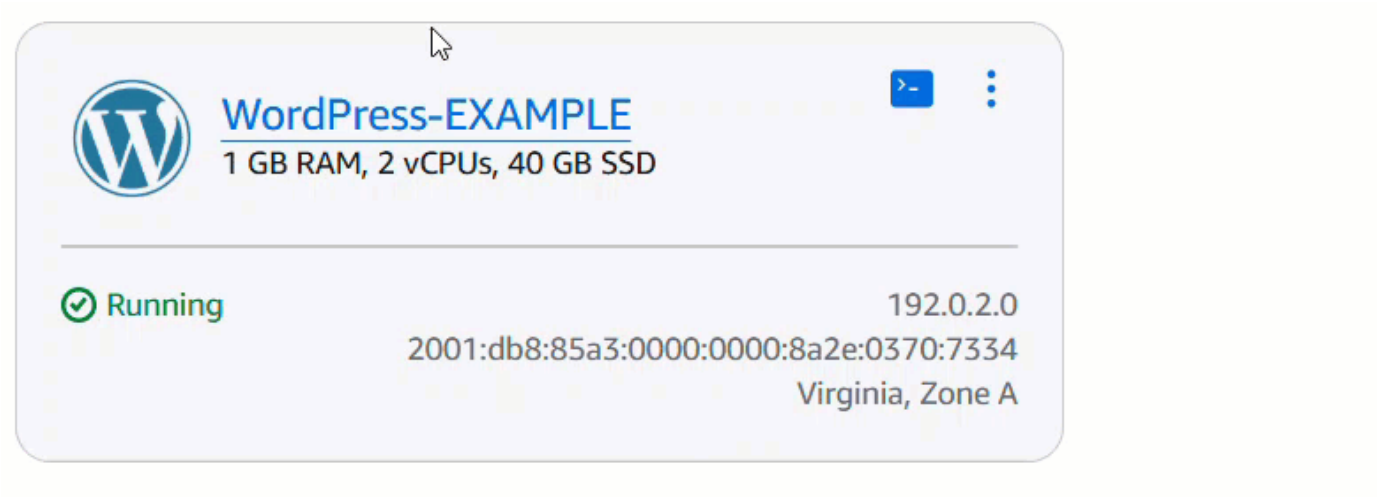
Warning

当您删除实例时，该实例将无法恢复。作为此操作的一部分，该实例的所有自动快照也将被删除。如果您想保留数据以备日后使用，则必须先创建实例的快照或选择保留现有的自动快照。有关更多信息，请参阅以下文档：

- 防止自动快照在 Lightsail 中被替换
- 使用快照备份 Linux/Unix Lightsail 实例
- 创建你的 Lightsail Windows Server 实例的快照

从 Lightsail 控制台主页中删除实例

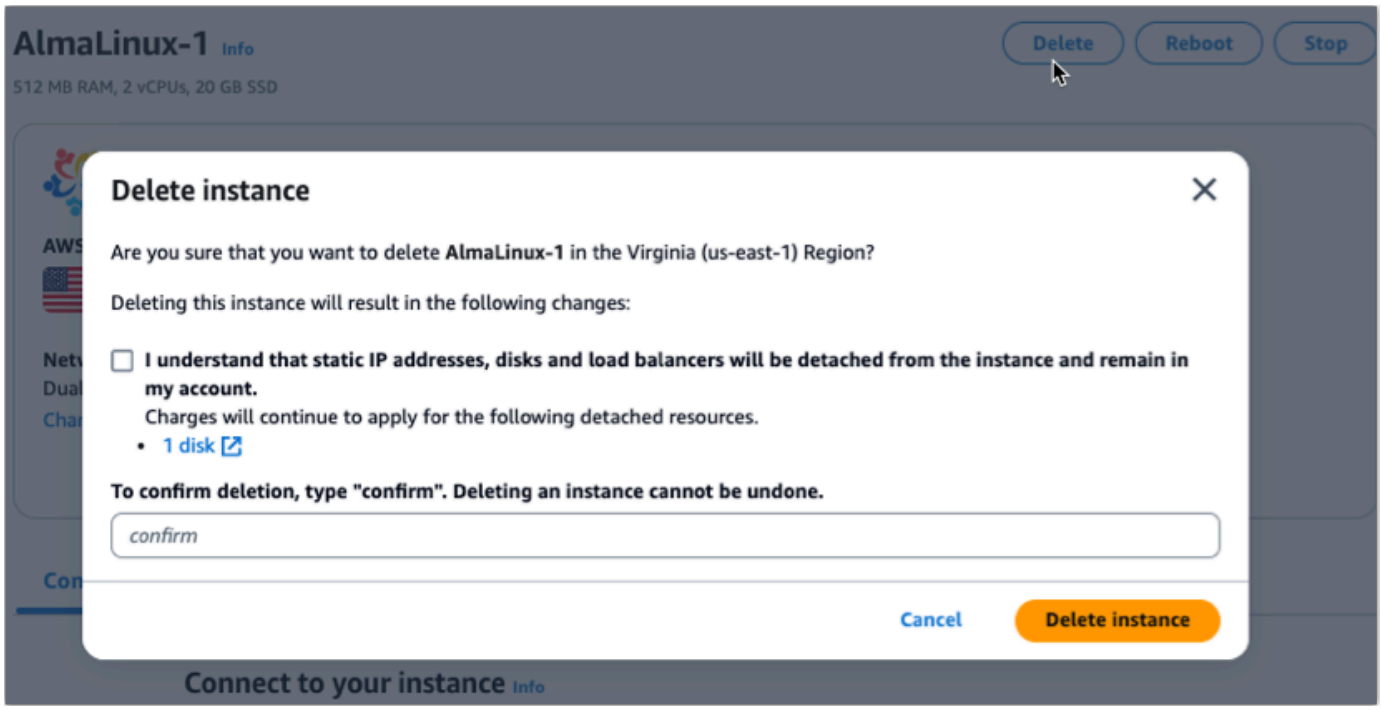
1. 登录 Lightsail 控制台。
2. 针对要删除的实例，选择操作菜单图标 (⋮)，然后选择 Delete (删除)。



3. 选择是，删除以确认删除。

从 Lightsail 控制台的实例管理页面中删除实例

1. 在主页上的 Lightsail 控制台中，选择要删除的实例。
2. 选择删除按钮，然后选择删除实例。



3. 选中该复选框，然后在输入字段中输入 Confirm 以确认您要删除该实例。
4. 选择删除实例以确认删除。

使用删除实例 AWS CLI

1. 满足以下先决条件（如果尚未满足）。
   a. 安装 AWS CLI。有关更多信息，请参阅安装 AWS CLI。
   b. 配置 AWS CLI。有关更多信息，请参阅配置 AWS CLI。
   c. （可选）使用 AWS CloudShell。有关更多信息，请参阅 ???。
2. 打开终端、命令提示符或 CloudShell 窗口，然后键入以下命令以获取要删除的实例的名称：

```
aws lightsail get-instances
```

您应该会看到类似于如下所示的结果：



3. 选择并复制要删除的实例的名称，以便在下一步中使用。

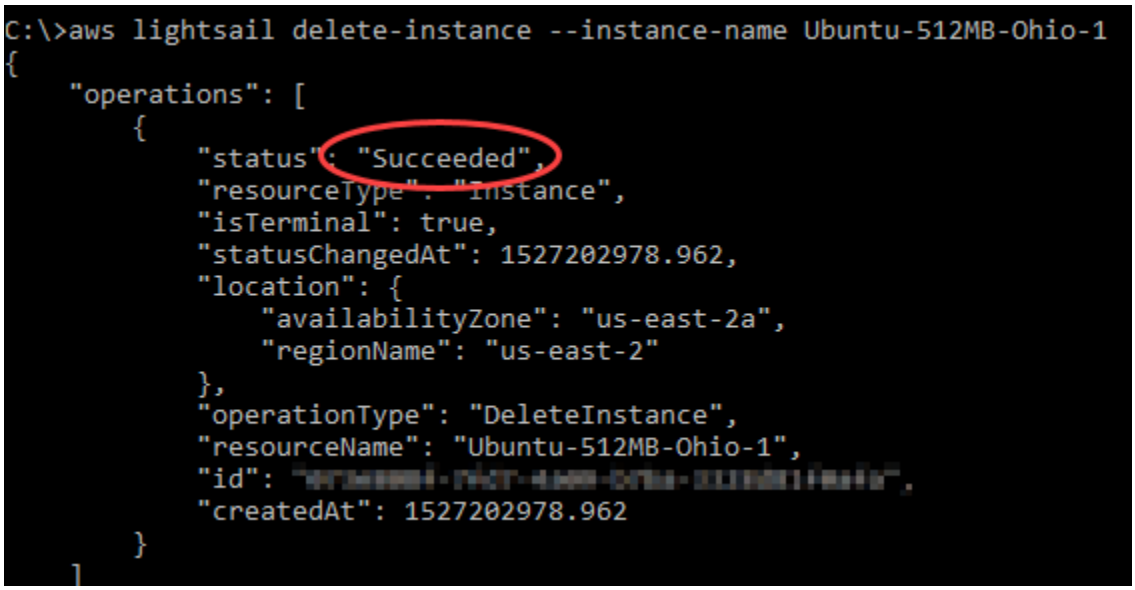
> **Note**
>
> 如果您要删除的实例未出现，请确认您的 AWS CLI 实例已针对该实例 AWS 区域 所在的位置进行了配置。有关更多信息，请参阅配置 AWS CLI。

4. 键入以下命令可删除实例。

```
aws lightsail delete-instance --instance-name InstanceName
```

在命令中，*InstanceName*替换为实例的名称。

如果成功删除，则您应该会看到类似于以下示例的确认信息：



> **Note**
>
> 如果未成功删除，则您应该会看到一条错误消息。确认您已复制并粘贴确切的实例名称，然后重试。

后续步骤

删除实例后，与实例关联的静态 IP、快照、块存储磁盘和负载均衡器将保留在 Lightsail 中，并且会产生额外费用。有关如何删除这些资源的更多信息，请参阅以下文章：

- 删除静态 IP
- 删除快照
- 断开连接并删除数据块存储磁盘
- 删除负载均衡器

管理 SSH 密钥对并连接到你的 Lightsail 实例

密钥对是一组安全证书，您在连接到 Amazon Lightsail 实例时使用这些证书来证明自己的身份。密钥对包含公有密钥和私有密钥。Lightsail 将公钥存储在您的实例上，然后由您存储私钥。

密钥对文件包含以下文本：

Public key example:

```
ssh-rsa
EXAMPLEzaC1yc2EAAAADAQABAAABAQCoYFOS10yNQ2AoRuvt2uM2LpuZXLGpNoHFxCAmXZjNIZ6t6s
sHCAWgiqzbp5fzRSZnPXjeuxQo2KsGkZCD6f81YHfEIBTSPWoiA6HPWAlAOR6K7E4ZGBkpYhOJKDK1
BYzCKUTgyRUvemmNmGme/c5O4ts50se0A/8m26YNt8TYgKqLV7mjl+Q1uMix0qS3wOim4x
+Iq5eV3cdTa0v0iuQJd01aXoCdJ1cdMW6qEDxZ5ILEMtle8FoLvvMe67JLqjCTxy8i/6x
+SiBWVITOgBKfeePPHsq2PceOQN/XfajeLd+CMAXYyRrvUo4HIiR443BJG1zevIvKYA7+yEXAMPLE
```

Private key example:

```
-----BEGIN RSA PRIVATE KEY-----
EXAMPLEBAAKCAQEAqGBTktdMjUNgKEbr7drjNi6bmVyxqTaBxcQgJl2YzSGererL
BwgFoIqs26eX80UmZz143rsUKNirBpGQg+n/JWB3xCAU0j1qIgOhz1gJQDkeiuxO
GRgZKWITiSgypQWMwilE4MkVL3ppjZhpnv3OTuLbOdLHtAP/JtumDbfE2ICqi1e5
o5fkNbjIsdKkt8DopuMfiKuXld3HU2tL9IrkCXdNWl6AnSdXHTFuqhA8WeSCxDLZ
XvBaC77zHuuyS6owk8cvIv+sfkogVlSEzoASn3njzx7Ktj3HjkDf132o3i3fgjAF
2Mka71KOByIkeONwSRtc3ryLymAO/smHHNQRzwIDAQABAoIBAGoipiu2uVOGd/OL
mSaKxpSd1olaq8atTCo8kcN9Vldf7OVWTnp1LQ7gu0uOnjLDkQyc7DcCGBgTU+NF
GKJ+es21vGkNi/JmsiMUxQetR8+K8dzCTgx1a07xurzHcP0ivXKajwde2ZLfB/Aw
dcu50zVYvLX7TtUDe++jn02gXF3X3q98lqWmSPV+dtlZPctQqcmemjQg3onUdpZo
4yrAKUKJdrchIMHhBD0jisom86Zl3jEPXRY7iuOfa1bB76cmErja18rijUhMH5Pn
mjAsbvZ0CTxU7QGx5yHnFtSK73oLN4LoYKek0TA7JARc4lp0MELtkOTn9mj2IeEw
h2yygPECgYEA37mi3uGVBBAVLEU3Z2sAS/thF0+L2y6qcuBxjY/HeyPnwvuXied0
xJhb9wPpODRTShDkKLfHPiVYD7H6bXZLetZfNLjIu/IKvseL85zCX8fWz6cJ6IeS
3QKRYu2VdpQW2prs+58QyKD1DqQ0hfE3dHZvSayLmm/9/sBZ24+G/WcCgYEAwKqb
yYkDOZtXIHZyTt1UUHvKFzo9LFuuMwlHQdNpvy2QbNNw4iE706DzVjy9FNuMXzIs
Skhhn7m+wredBP+r8udX3+gA1vY329wJ/+c7W8IPN21RiWIT4VtawmoHgMeJHOv4
4mdxqMo6L44Nkny/4KLtGAuZCUrJzoLr+d+Fn1kCgYEAyA7MIdo+0r8+77OFc6kv
PsKvc5TiT0FPkiI56IilrOvSl307aUncFODZe+23Y1cHE7g/DloohN4H/SD9+1xI
6rM/t3l1pvstuKPf9hw7hELDSDTqm1CAd7mQIJKrkLmkJh9bwzXeYEngC1Oz1AJ7
wF0X7x2oSJXU3zVKJRgXcgkCgYEAn504DxC5YUI2Piiirn9iWIMVe4S+JT+W46Uu
KXSSSNXgrqfE/zH1NHBE6A7NvrfcZQlV8/xfFEp3pS0kon2F4GiUPmUgPPYidLyo
dB8G6A+vN4YTZLOiMLLUT/gzWxbzmshLmpWEbgeLiNYwnE1JVTrlHWSOVkp1Qfbo
tEvfkZECgYAayAwDXa2gbZBmqInwCTNJyqu8XW/Kc4JBT6mugXzQqxMr6ZnXM70h
Fq0EAT7kAHt4wKfZyPkcgrrmj0Mej6VoL2GlJejPykNa20nxrPIi8ecJDYhjiaIp
zoO5rFDVcZhMctewa70OL3c1q+nDGf7Sd9pqw0q31K6MiJwEXAMPLE==
-----END RSA PRIVATE KEY-----
```

在 Linux 和 Unix 实例上，私有密钥用来建立到实例的安全 SSH 连接。在 Windows 实例上，私有密钥会解密在建立到实例的安全 RDP 连接时所用的默认管理员密码。

任何人只要拥有您的私有密钥都可以连接到您的实例，因此您必须将您的私有密钥存储在安全的位置。

内容

- 选择密钥对选项
- 连接到实例
- 管理存储在实例上的密钥

选择密钥对选项

创建 Lightsail 实例时，您可以选择以下密钥对选项之一。Windows 实例始终使用默认密钥；因此，在创建 Windows 实例时，您无法创建密钥对或上传密钥。

- 默认 SSH 密钥 — Lightsail 会在您创建实例的每个 AWS 区域 位置自动创建一个默认密钥对。当您在实例中使用默认密钥对时，Lightsail 会将公钥存储在您的实例上。您可以随时从 Lightsail 控制台的“帐户”页面下载默认密钥对的私钥。每个密钥对中最多可以有一个默认 key pair AWS 区域。
- 创建自定义密钥（Linux 和 Unix 实例）— 您可以使用 Lightsail 控制台创建新的自定义密钥对以用于您的实例。创建自定义密钥对时，您需要为其指定一个唯一的名称，然后 Lightsail 会将公钥存储在您的实例上。您只能在第一次创建自定义密钥对时下载它的私有密钥。
- 上传密钥（Linux 和 Unix 实例）— 要使用自己的现有密钥对，您可以将公钥上传到 Lightsail。当您上传用于实例的公钥时，您会为其指定一个唯一的名称，然后 Lightsail 会将其存储在您的实例上。您负责保管和存储密钥对的私有密钥。

如果您在多个实例上配置了同一个公有密钥，则可以使用该密钥对的相同私有密钥连接到这些实例。有关管理密钥对的更多信息，请参阅在 Amazon Lightsail 中管理密钥对。

连接到您的实例

您可以使用以下选项之一连接到您的 Lightsail 实例。

基于 Lightsail 浏览器的 SSH 和 RDP 客户端

在 Lightsail 控制台中，您可以使用基于浏览器的 SSH 客户端即时连接到您的 Linux 和 Unix 实例，并使用基于浏览器的 RDP 客户端连接到您的 Windows 实例。使用基于浏览器的客户端连接到实例时，无需在电脑上安装 SSH 客户端、配置密钥对或指定管理员密码。这是最快捷的实例连接方式。有关更多信息，请参阅连接到 Amazon Lightsail 中的 Linux 或 Unix 实例和连接到 Amazon Lightsail 中的 Windows 实例。

基于浏览器的客户端使用的密钥对不同于您在创建实例时配置的密钥对（例如默认密钥或您创建或上传的密钥）。因此，即使删除或丢失了最初配置的任何一个密钥，您仍然可以继续使用基于浏览器的客户端连接到实例。

第三方 SSH 和 RDP 客户端

您可以使用第三方 SSH 客户端连接到 Linux 和 Unix 实例，以及使用第三方 RDP 客户端连接到 Windows 实例。使用 SSH 客户端时，您必须将其配置为使用您在实例上配置的密钥对的私有密钥。使用 RDP 客户端时，必须指定 Windows 实例的管理员密码。

如果您在本地使用 Windows 计算机，则可以使用以下客户端连接您的 Lightsail 实例。

- PuTTY – 使用 PuTTY 通过 SSH 连接到 Linux 或 Unix 实例。有关更多信息，请参阅设置 PuTTY 以连接到实例。

- 远程桌面连接 – 使用远程桌面连接客户端以通过 RDP 连接到 Windows 实例。有关更多信息，请参阅在 Windows 电脑上使用远程桌面连接客户端连接到 Windows 实例。

如果您在本地使用 Mac 电脑，请使用以下客户端连接您的 Lightsail 实例。

- 终端中的本机 SSH 客户端 – 使用终端中的本机 SSH 客户端连接到 Linux 和 Unix 实例。有关更多信息，请参阅在终端中使用 SSH 连接到 Linux 或 Unix 实例。
- Microsoft 远程桌面 – 使用适用于 macOS 的 Microsoft 远程桌面客户端通过 RDP 连接到 Windows 实例。有关更多信息，请参阅在 Mac 电脑上使用 Microsoft 远程桌面客户端连接到 Windows 实例。

管理存储在实例上的密钥

实例启动并运行后，您可以向实例添加新密钥，或替换您最初分配给实例的密钥。例如，假设组织中有用户需要使用单独的密钥访问实例，您可以将该密钥添加到实例。再如有人离开组织并且他们拥有私有密钥文件（.PEM）的副本时。您可以通过用新密钥替换旧密钥或将旧密钥完全删除来阻止他们连接到您的实例。有关更多信息，请参阅在 Amazon Lightsail 中管理存储在实例上的密钥。

主题

- 为 Lightsail 设置 SSH 密钥
- 使用 Lightsail SSH 密钥控制安全的实例连接
- 管理 Lightsail Linux 实例上的 SSH 密钥
- 在 Lightsail 上连接到 Linux 或 Unix 实例
- 使用 RDP 连接到你的 Lightsail Windows 实例

为 Lightsail 设置 SSH 密钥

安全 SHell (SSH) 是一种用于安全连接到虚拟专用服务器（或 Lightsail 实例）的协议。SSH 工作时会创建公有密钥和私有密钥，以将远程服务器与授权用户匹配。使用该密钥对，您可以使用基于浏览器的 SSH 终端连接到您的 Lightsail 实例。

有关 SSH 的更多信息，请参阅了解 SSH。

当你创建 Lightsail 实例时，默认选项是让 Lightsail 为你管理你的 SSH 密钥。Lightsail 提供了基于浏览器的 SSH 客户端，用于安全地连接到基于 Linux 的实例。它是一个功能完备的终端，您可以在其中输入命令和更改实例。

基于 Windows 的实例使用远程桌面 (RDP) 协议，而不是 SSH。有关 Lightsail 中基于 Windows 的实例的更多信息，请参阅 Lightsail 中基于 Windows 的实例入门。

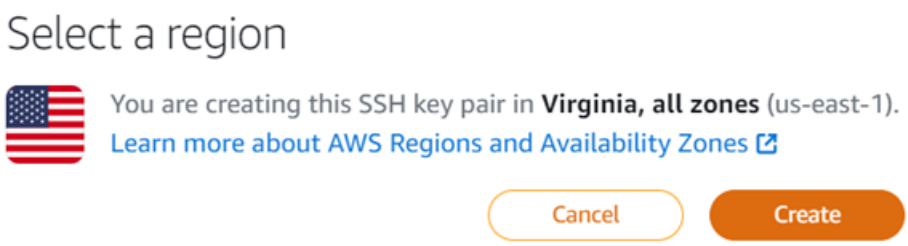
> **Important**
>
> SSH 密钥管理是区域性的。在新建实例中创建实例时 AWS 区域，您可以选择使用该区域的默认密钥对。您也可以在该区域中使用自定义密钥。请记住，如果您上传自己的密钥，则必须为每个拥有 Lightsail 实例的区域执行此操作。

如果您使用默认密钥，则仍可以下载私有密钥以实现保护目的。可在创建您的实例时或之后下载私有密钥。如果您选择在创建实例之后下载密钥，可在 Account（账户）页上的 SSH keys（SSH 密钥）下执行此操作。

创建新密钥

如果您不选择使用默认密钥，则可以在创建 Lightsail 实例时创建新的密钥对。

1. 如果您尚未创建密钥对，请选择 Create instance（创建实例）。
2. 在创建实例页面上，选择创建自定义密钥。
3. Lightsail 会显示我们正在创建新密钥的区域。



选择 Create（创建）。

4. 为您的密钥对输入名称。

资源名称：

- 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
- 必须包含 2 到 255 个字符。
- 必须以字母数字字符或数字作为开头和结尾。
- 可以包括字母数字字符、数字、句点、连字符和下划线。

5. 选择 Generate key pair（生成密钥对）。

> **Important**
>
> 将您的密钥保存在方便找到的某个位置。此外，最好是确保设置权限以便他人无法读取。

6. 继续创建您的实例。

上传现有密钥

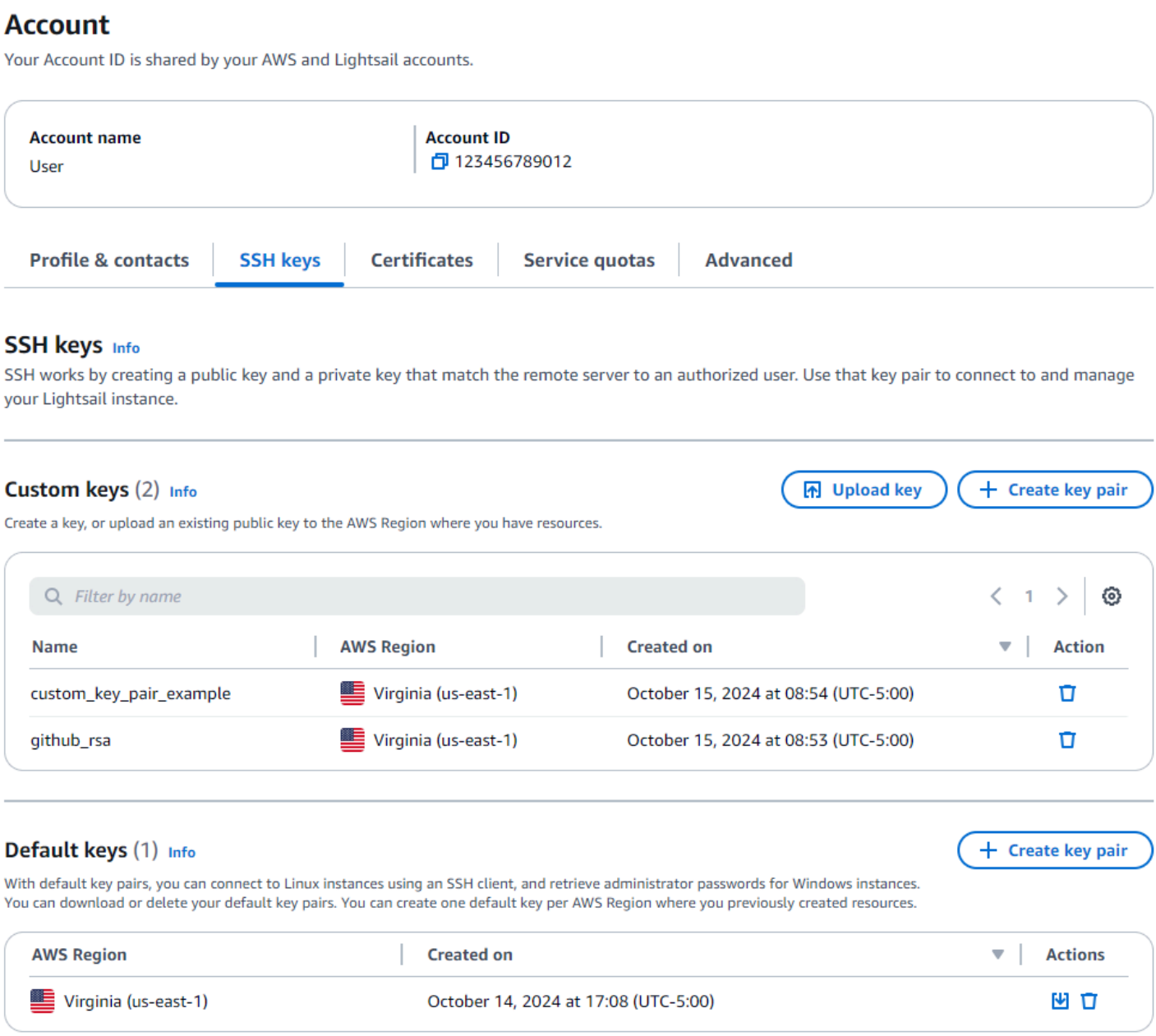
您也可以选择在创建 Lightsail 实例时上传现有密钥。

1. 如果您尚未创建密钥对，请选择 Create instance（创建实例）。
2. 在创建实例页面上，选择上传密钥。
3. 选择上传。
4. Lightsail 会显示你要上传新密钥的区域。
5. 选择“选择文件”，在本地计算机上查找密钥。

   请务必上传公有密钥（而不是私有密钥）。例如，`github_rsa.pub`。
6. 选择 Upload key（上传密钥）。
7. 继续创建您的实例。

管理您的密钥

您可在 Account（账户）页的 SSH keys（SSH 密钥）选项卡上管理您的密钥。您将看到每个区域中使用的每个密钥对。



在此页面上，您可以创建新密钥、删除现有密钥、上传现有密钥或下载私有密钥。您可能想使用 SSH 客户端（如 PuTTY）进行连接，这需要您具有密钥的私有密钥部分。您可以在 Account（账户）页面上下载密钥。了解有关设置 PuTTY 以连接到 Lightsail 实例的更多信息。

使用 Lightsail SSH 密钥控制安全的实例连接

您可以使用密钥对与您的 Amazon Lightsail 实例建立安全连接。首次创建 Amazon Lightsail 实例时，您可以选择使用 Lightsail 为您创建的密钥对（Lightsail 默认密钥对），也可以选择使用您创建的自定义密钥对。有关更多信息，请参阅 Amazon Lightsail 中的密钥对和连接实例。

在 Linux 和 Unix 实例上，私有密钥用来建立到实例的安全 SSH 连接。在 Windows 实例上，私有密钥会解密在建立到实例的安全 RDP 连接时所用的默认管理员密码。

在本指南中，我们将向您展示如何管理可用于 Lightsail 实例的密钥。您可以查看密钥、删除现有的密钥以及创建或上传新密钥。

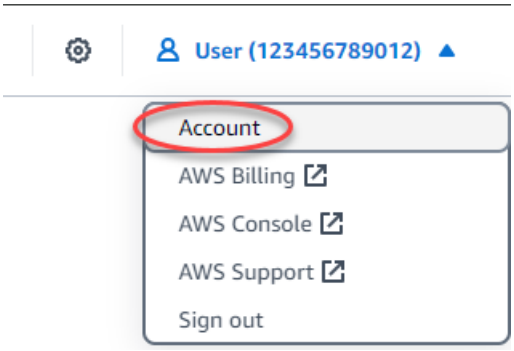
内容

- 查看默认密钥和自定义密钥
- 从 Lightsail 控制台下载默认密钥的私钥
- 在 Lightsail 控制台中删除自定义密钥
- 在 Lightsail 控制台中删除默认密钥并创建一个新密钥
- 使用 Lightsail 控制台创建自定义密钥
- 使用 ssh-keygen 创建自定义密钥并上传到 Lightsail

查看默认密钥和自定义密钥

完成以下步骤，从 Lightsail 控制台查看您的默认密钥和自定义密钥。

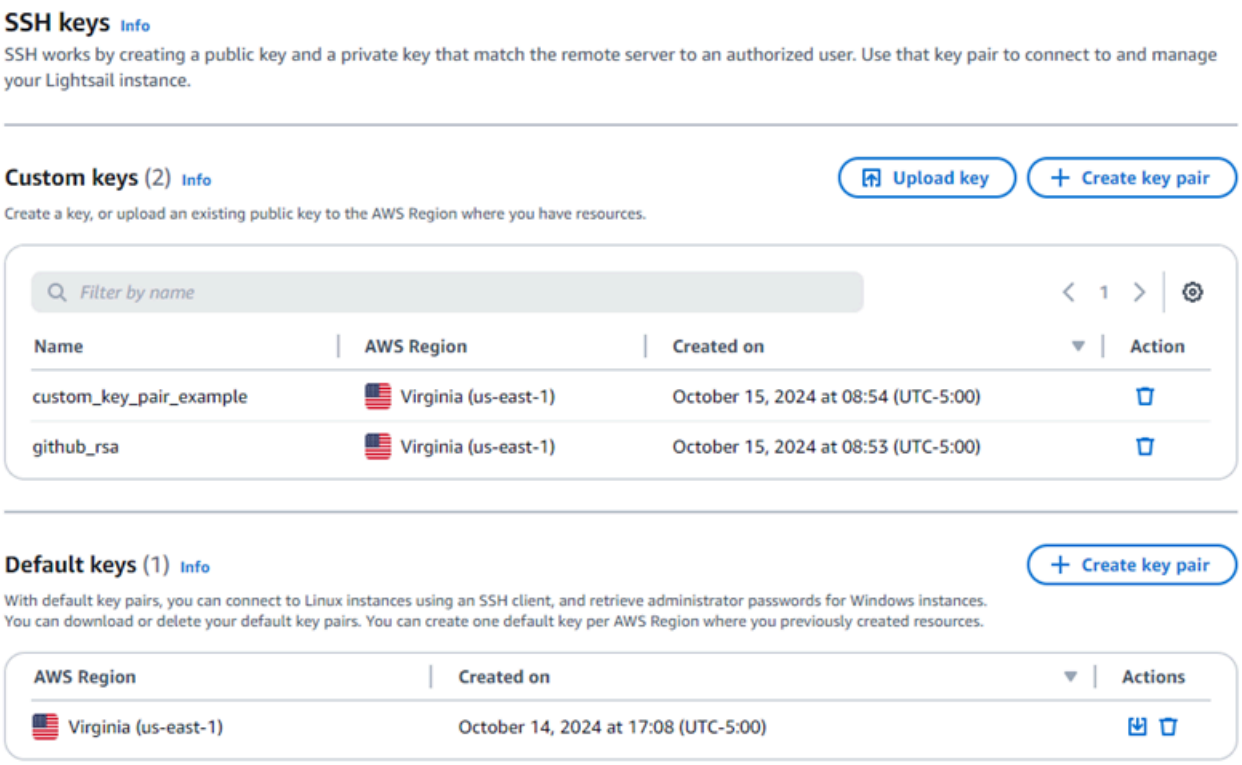
1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 选择 SSH 密钥选项卡。

   SSH keys（SSH 密钥）页面将会列出：

   - 自定义密钥 — 这些密钥是您使用 Lightsail 控制台或第三方工具（例如 ssh-keygen）创建的密钥。每个密钥中可以有许多自定义密钥 AWS 区域。
   - 默认密钥 — 这些是 Lightsail 为您创建的密钥。每个 AWS 区域只能有一个默认密钥。



自定义密钥和默认密钥都是区域性的。例如，美国西部（俄勒冈州）AWS 区域 中的密钥只能在该区域中创建的实例上配置。有关密钥的更多信息，请参阅 Amazon Lightsail 中的密钥对和连接到实例。

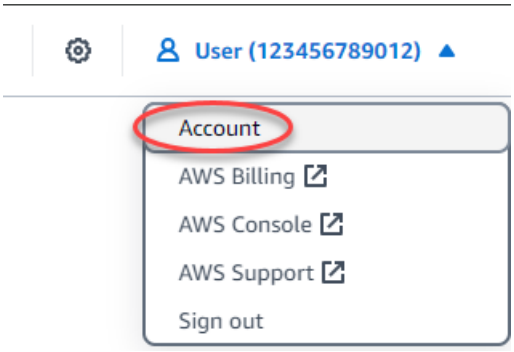
在 SSH 密钥页面上，您可以创建密钥对、上传密钥、删除密钥以及下载 Lightsail 默认密钥对的私钥。

> **Note**
>
> 您无法下载自定义密钥对的私钥，因为 Lightsail 不会为您存储该密钥。如果您丢失了自定义密钥对的私有密钥，则应创建一个新密钥，然后在实例上进行配置。然后删除已经丢失的密钥。有关更多信息，请参阅本指南后面的使用 Lightsail 控制台创建自定义密钥或使用 ssh -keygen 创建自定义密钥并上传到 Lightsail。

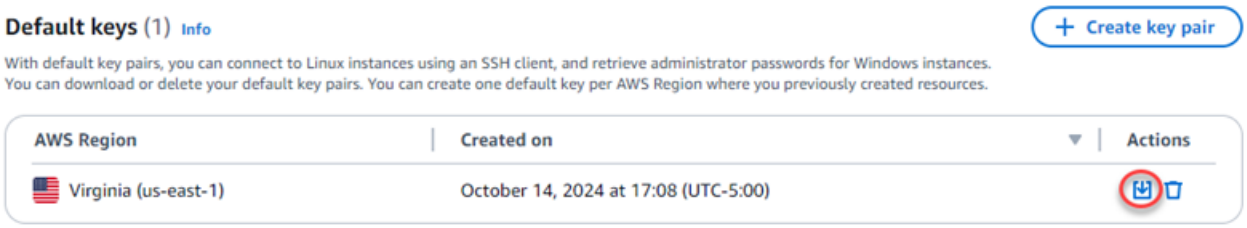
从 Lightsail 控制台下载默认密钥的私钥

完成以下步骤，从 Lightsail 控制台下载默认密钥对的私钥。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 选择 SSH 密钥选项卡。
5. 在此页的 Default keys（默认密钥）部分，选择要下载的密钥的下载图标。



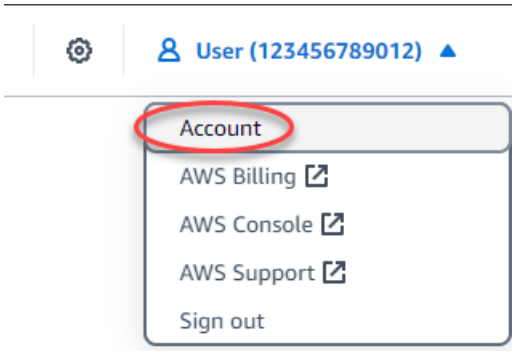
> **Important**
>
> 将私有密钥存储在安全的位置。不要公开分享此密钥，因为它可以用来连接到您的实例。

您可以配置 SSH 客户端以使用私有密钥连接到您的实例。有关更多信息，请参阅连接到实例。

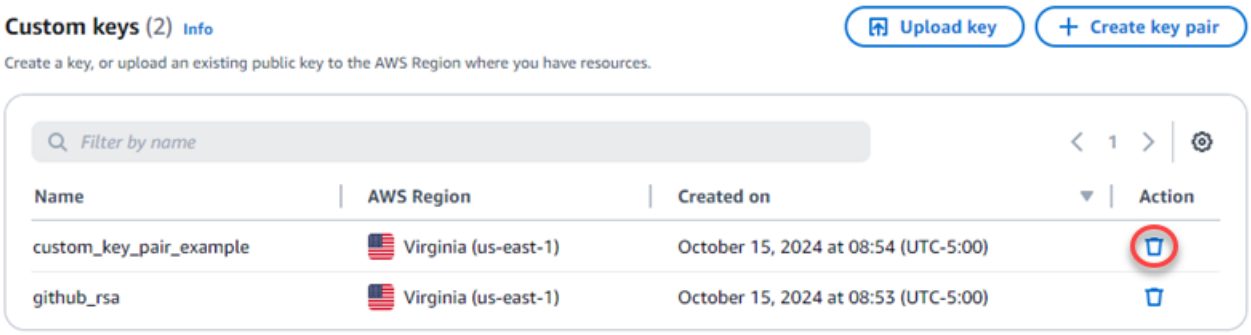
在 Lightsail 控制台中删除自定义密钥

完成以下步骤，在 Lightsail 控制台中删除自定义密钥。这样可以防止在您在 Lightsail 中创建的新实例上配置自定义密钥。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 选择 SSH 密钥选项卡。
5. 在此页的 Custom keys（自定义密钥）部分，选择要删除的密钥的删除图标。

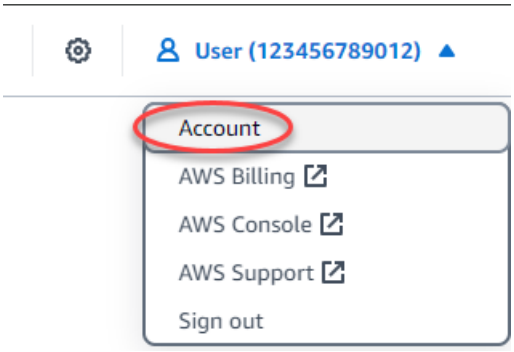


这不会从先前创建并且当前正在运行的实例中删除自定义密钥对的公有密钥。要移除存储在正在运行的实例上的先前配置的公钥，请参阅在 Amazon Lightsail 中管理存储在实例上的密钥。

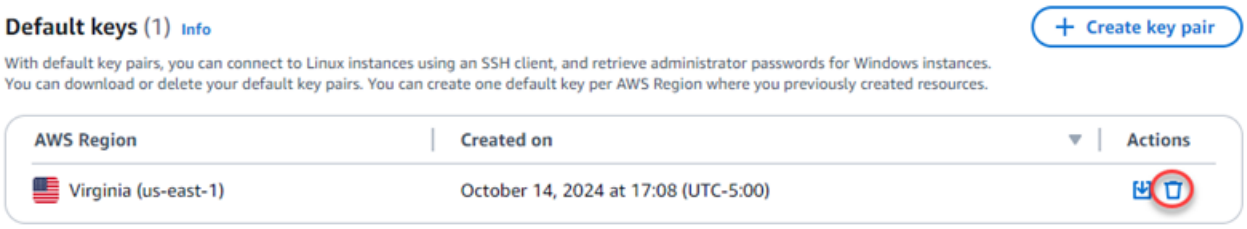
在 Lightsail 控制台中删除默认密钥并创建一个新密钥

完成以下步骤以删除 Lightsail 控制台中的默认密钥。这样可以防止在您在 Lightsail 中创建的新实例上配置该默认密钥。然后，您可以创建一个新的默认密钥来替换已删除的密钥。您将能够在您在 Lightsail 中创建的新实例上配置新的默认密钥。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。

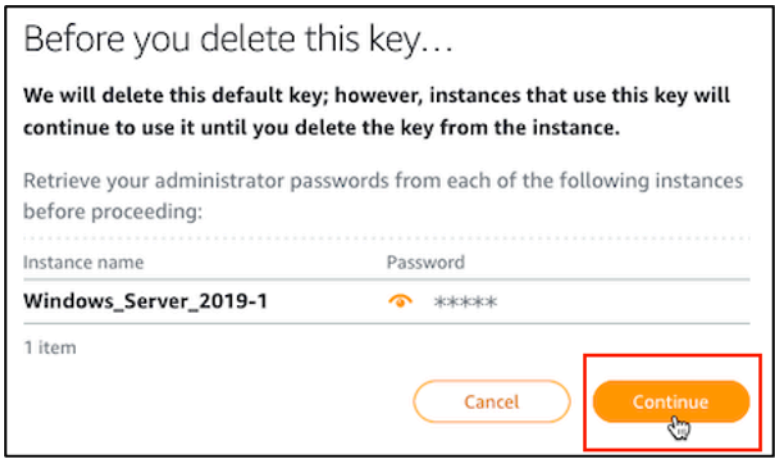


4. 选择 SSH 密钥选项卡。
5. 在此页的 Default keys（默认密钥）部分，选择要删除的默认密钥的删除图标。

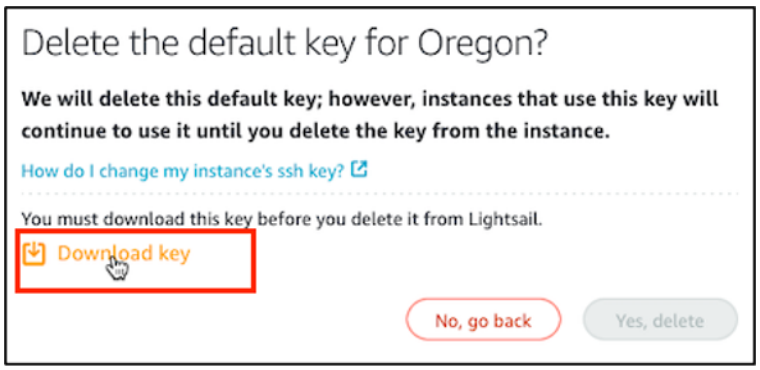


> **Important**
>
> 删除默认密钥不会从先前创建并且当前正在运行的实例中删除自定义密钥对的公有密钥。有关更多信息，请参阅在 Amazon Lightsail 中管理存储在实例上的密钥。

6. 默认密钥用于生成 Windows 实例的管理员密码。在删除默认密钥之前，对于使用要删除的默认密钥的任何 Windows 实例，您应检索并保存其管理员密码。
7. 选择 Continue（继续）以删除默认密钥。



8. 您必须首先下载默认密钥，然后才能将其删除。在下载默认密钥后，您可以选择 Yes, delete（是的，请删除）以永久删除默认密钥。



9. 默认密钥已被删除。选择 Okay (确定)。

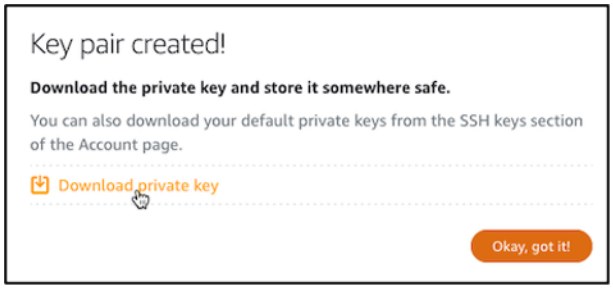


以下步骤是可选的，仅应在需要替换已删除的默认密钥对时使用。

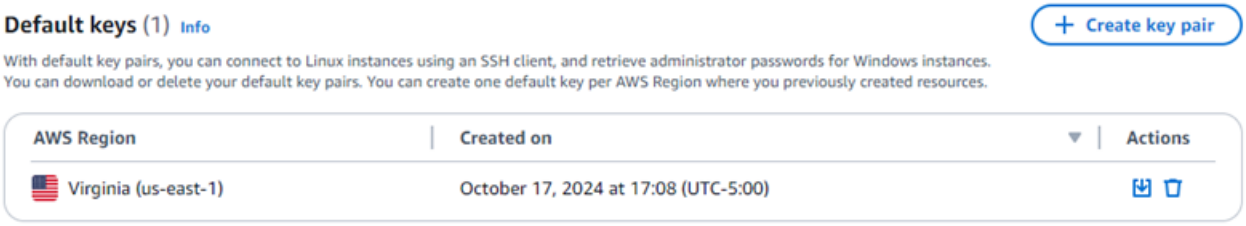
10. 在此页的 Default keys（默认密钥）部分，选择 Create key pair（创建密钥对）。
11. 在出现的 “选择区域” 提示中，选择要 AWS 区域 在其中创建新默认密钥的。您将能够在您在同一 AWS 区域中创建的新实例上配置新的默认密钥。

> **Note**
>
> 使用这些步骤，您只能在已创建 Light AWS 区域 sail 资源的地方创建默认密钥对。要在新区域中创建默认密钥对，必须在该区域创建 Lightsail 资源。创建资源还会创建默认密钥对。

12. 下载私有密钥并将其存储在安全的位置。
13. 选择 Ok, got it!（好，明白了！）以继续。



14. 在 Lightsail 控制台 SSH 密钥页面上确认新的默认密钥。

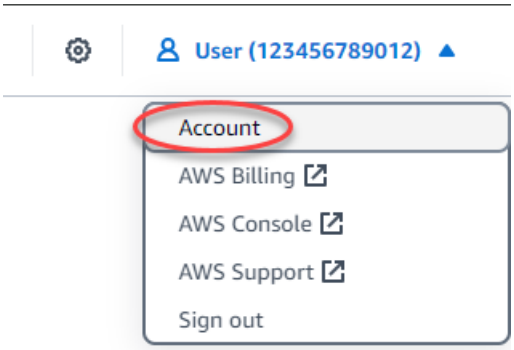


您可以在 Lightsail 中创建的新实例上配置新的默认密钥。要在之前创建且当前正在运行的实例上配置新的默认密钥，请参阅在 Amazon Lightsail 中管理存储在实例上的密钥。

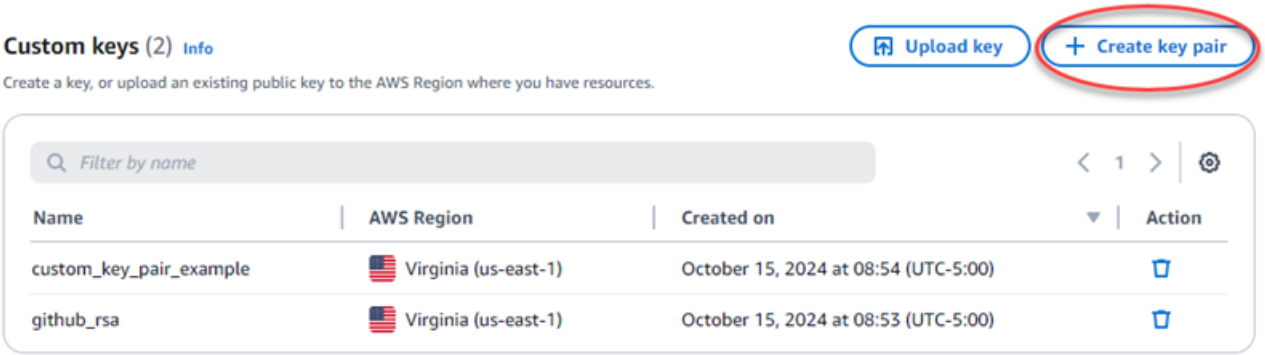
使用 Lightsail 控制台创建自定义密钥

完成以下过程，使用 Lightsail 控制台创建自定义密钥对。您将能够在您在 Lightsail 中创建的新实例上配置新的自定义密钥。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



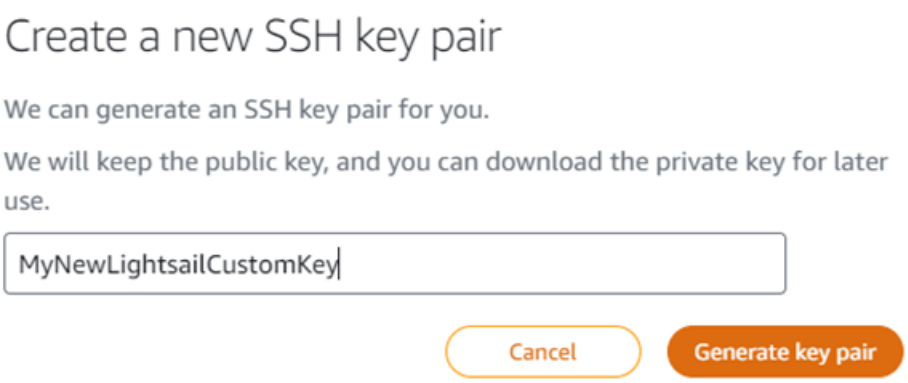
4. 选择 SSH 密钥选项卡。
5. 在此页的 Custom keys（自定义密钥）部分下选择 Create key pair（创建密钥对）。



6. 在显示的 Select a region（选择一个区域）提示框中，选择您要在其中创建新的自定义密钥的 AWS 区域 。您将能够在您在同一 AWS 区域中创建的新实例上配置新的自定义密钥。

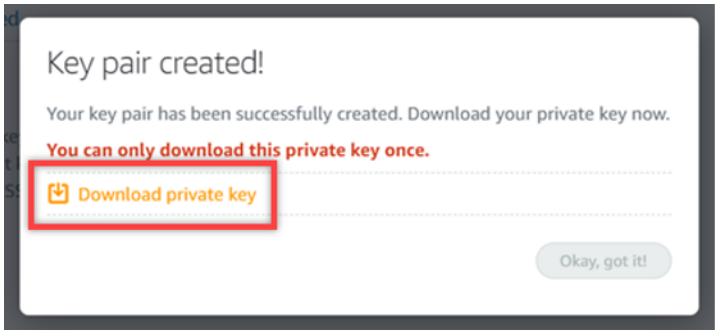


7. 在显示的 Create a new SSH key pair（创建新的 SSH 密钥对）提示框中，提供自定义密钥的名称，然后选择 Generate key pair（生成密钥对）。

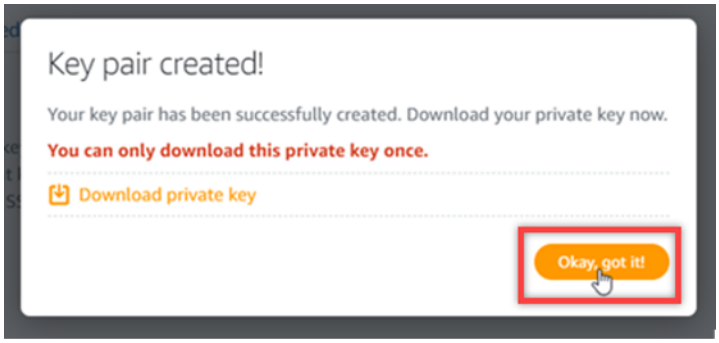


8. 在显示的 Key pair created!（已创建密钥对！）提示框中，选择 Download private key（下载私有密钥）以将私有密钥保存到本地电脑。

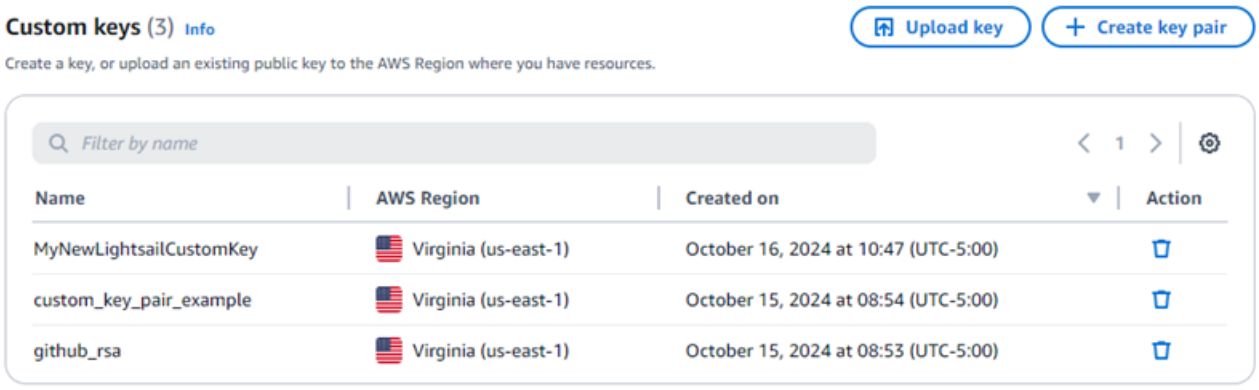
> **Important**
>
> 将私有密钥存储在安全的位置。不要公开分享此密钥，因为它可以用来连接到您的实例。这是您可以下载自定义密钥对的私有密钥的唯一机会。Lightsail 不存储自定义密钥对的私钥。在您关闭此提示框后，您将无法再次下载它。



9. 选择 Ok, got it!（好，明白了！）以关闭提示框。



10. 您的新自定义密钥将在此页的自定义密钥部分列出。



您可以在 Lightsail 中创建的新实例上配置新的自定义密钥。要在之前创建且当前正在运行的实例上配置新的自定义密钥，请参阅在 Amazon Lightsail 中管理存储在实例上的密钥。

使用 ssh-keygen 创建自定义密钥并上传到 Lightsail

完成以下过程以使用第三方工具（例如 ssh-keygen）在本地电脑上创建自定义密钥对。创建密钥后，您可以将其上传到 Lightsail 控制台。您将能够在您在 Lightsail 中创建的新实例上配置新的自定义密钥。

1. 在本地电脑上打开命令提示符或终端。
2. 输入以下命令以创建密钥对。

```
ssh-keygen -t rsa
```

3. 在电脑上指定用于保存密钥对的目录位置。

   例如，您可以指定以下目录中的一个：

   a. 在 Windows 上：C:\Users*<UserName>*\.ssh*<KeyPairName>*

   b. Linux、macOS 或 Unix：/home/*<UserName>*/.ssh/*<KeyPairName>*

   将 *<UserName>* 替换为您当前登录的用户名称，并将 *<KeyPairName>* 替换为新密钥对的名称。

   在以下示例中，我们指定了 Windows 电脑上的 C:\Keys 目录，并将新密钥命名为 MyNewLightsailCustomKey。

```
C:\Users\[redacted]>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\[redacted]/.ssh/id_rsa): C:\Keys\MyNewLightsailCustomKey
```

4. 输入密钥的密码短语然后按 Enter 键。输入密码短语时您不会看到它。

   稍后在 SSH 客户端上配置密钥对的私有密钥以连接到已配置密钥对的公有密钥的实例时，您将需要此密码短语。

```
Enter passphrase (empty for no passphrase):
```

5. 再次输入密码短语以进行确认，然后按下 Enter 键。输入密码短语时您不会看到它。

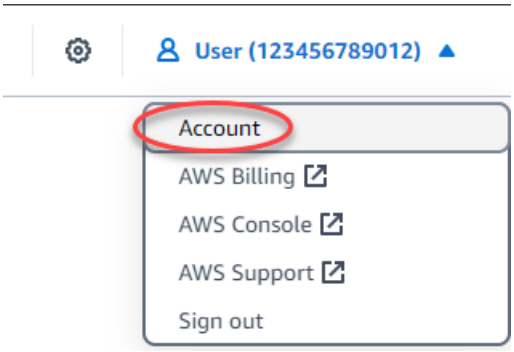
```
Enter same passphrase again:
```

6. 提示消息将会确认您的私有密钥和公有密钥已保存到指定目录中。

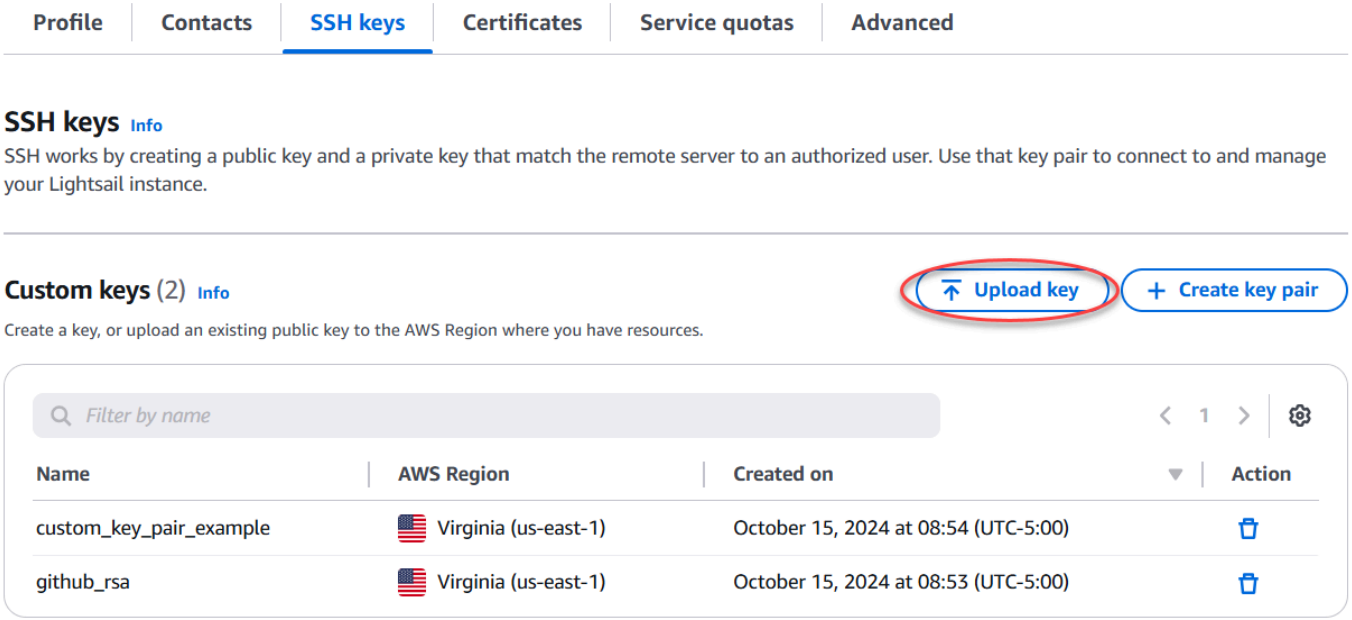
```
Your identification has been saved in C:\Keys\MyNewLightsailCustomKey.
Your public key has been saved in C:\Keys\MyNewLightsailCustomKey.pub.
```

   接下来，您将密钥对的公钥上传到 Lightsail 控制台。

7. 登录 Lightsail 控制台。
8. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
9. 在下拉菜单中选择账户。



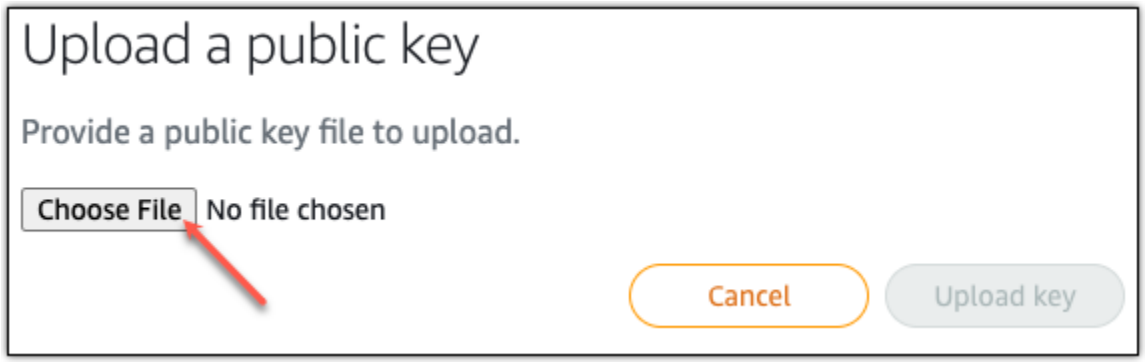
10. 选择 SSH 密钥选项卡。
11. 在此页的 Custom keys（自定义密钥）部分下选择 Upload key（上传密钥）。



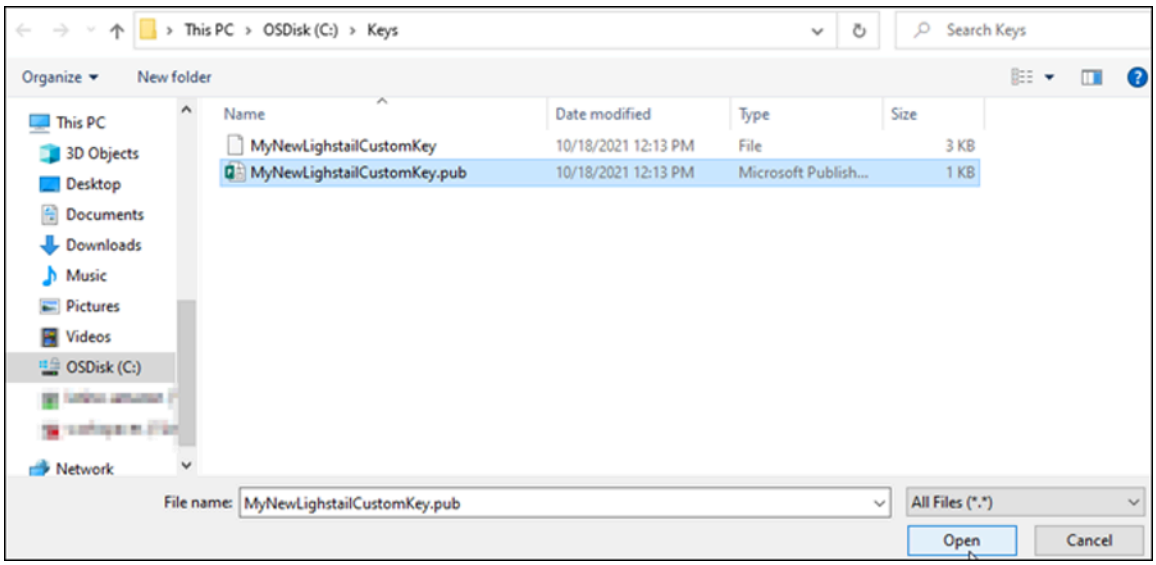
12. 在出现的 “选择区域” 提示 AWS 区域 中，选择要在其中上传新的自定义密钥。您将能够在您在同一 AWS 区域中创建的新实例上配置新的自定义密钥。



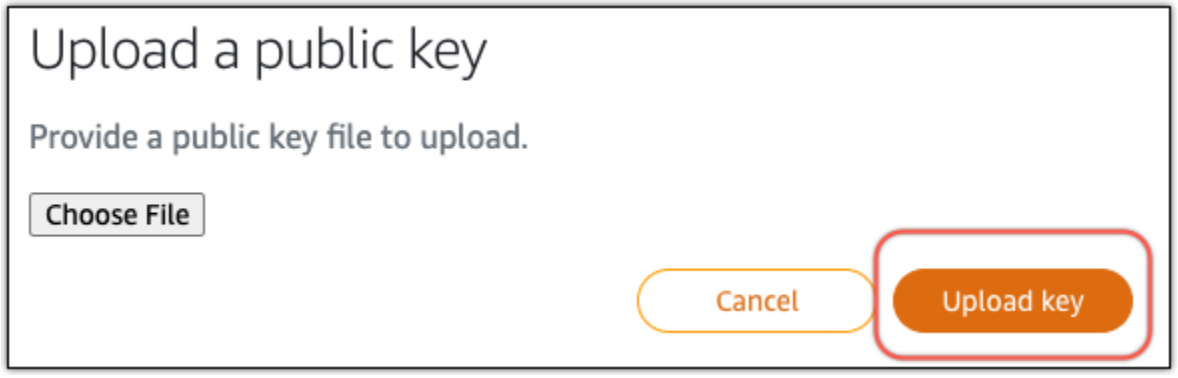
13. 选择上传。
14. 在显示的 Upload a public key（上传公有密钥）提示框中单击 Choose File（选择文件）。



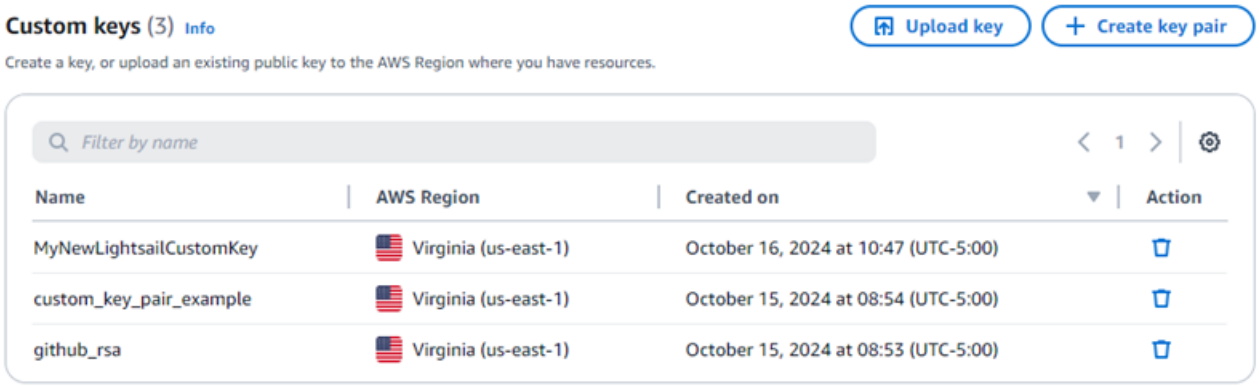
15. 在本地电脑上查找您在此过程之前创建的密钥对的公有密钥，然后选择 Open（打开）。密钥对的公有密钥是使用 .PUB 文件扩展名的文件。



16. 选择 Upload key（上传密钥）。



17. 您的新自定义密钥将在此页的 Custom keys（自定义密钥）部分列出。



在您上传了密钥的亚马逊云科技区域，您可以在您创建的新实例上配置新的自定义密钥。要在之前创建且当前正在运行的实例上配置新的自定义密钥，请参阅在 Amazon Lightsail 中管理存储在实例上的密钥。

管理 Lightsail Linux 实例上的 SSH 密钥

您可以使用密钥对与您的 Amazon Lightsail 实例建立安全连接。当你首次创建密钥对时，Lightsail 会在你的 Linux 或 Unix 实例上配置密钥对的公钥。密钥对的私有密钥用于在建立 SSH 连接时对实例进行身份验证。有关密钥的更多信息，请参阅密钥对以及连接到实例。

在实例启动并运行后，您可以通过在实例上添加新的公有密钥，或者替换实例上的公有密钥（删除现有公有密钥并添加新的公有密钥），从而更改用于连接到实例的密钥对。您可能出于以下原因来执行该操作：

- 如果组织中有用户需要使用单独的密钥对访问实例，您可以将此公有密钥添加到实例。
- 如果您需要保护从使用已泄露密钥的实例的快照创建的新实例。
- 如果有人拥有私有密钥的副本，而您想要防止他们连接到实例（例如他们已离开组织时），您可以删除实例上的公有密钥，并将其替换为新的公有密钥。

要添加或替换实例上的密钥，您必须能够连接到实例。如果您现有的私有密钥丢失，则可以使用基于 Lightsail 浏览器的 SSH 客户端连接到实例。有关更多信息，请参阅连接到 Linux 或 Unix 实例。

内容

- 步骤 1：了解流程
- 第 2 步：创建密钥对
- 第 3 步：将公有密钥添加到实例
- 第 4 步：使用新密钥对连接到实例
- 第 5 步：从实例中删除现有的公有密钥

步骤 1：了解流程

以下是在实例上添加和删除密钥的一般步骤。如果您想从实例中删除密钥但不添加新密钥，请参阅本指南后面的第 5 步：从实例中删除现有的公有密钥。

1. 创建密钥对 – 要向您的实例添加新密钥，则必须首先创建新的密钥对。您可以使用 Lightsail 控制台创建自定义或默认密钥对，也可以在本地计算机上使用第三方工具（例如 ssh-keygen）创建自定义或默认密钥对。这两种方法都会生成一个由公有密钥和私有密钥组成的新密钥对。有关更多信息，请参阅本指南后面的第 2 步：创建密钥对。
2. 将公有密钥添加到实例 – 创建密钥对后，您可以使用 SSH 连接到实例并将密钥对的公有密钥添加到实例。有关更多信息，请参阅本指南后面的第 3 步：将公有密钥添加到实例。

3. 测试能否使用新的密钥对连接到实例 – 在实例上保存密钥对的公有密钥后，需要测试是否可以使用密钥对的私有密钥通过 SSH 连接到实例。有关更多信息，请参阅本指南后面的第 4 步：使用新密钥对连接到实例。
4. 从实例中删除旧公有密钥 – 使用新密钥成功连接到实例后，您可以从实例中删除旧公有密钥。完成此步骤以防止用户使用旧密钥对连接到实例。有关更多信息，请本指南后面的第 5 步：从实例中删除现有的公有密钥。

第 2 步：创建密钥对

完成以下步骤以使用 ssh-keygen 在本地电脑上创建一个密钥对。

1. 在本地电脑上打开命令提示符或终端。
2. 输入以下命令以创建密钥对。

```
ssh-keygen -t rsa
```

3. 在电脑上指定用于保存密钥对的目录位置。

   例如：

   - 在 Windows 上：C:\Users*<UserName>*\.ssh*<KeyPairName>*
   - Linux、macOS 或 Unix：/home/*<UserName>*/.ssh/*<KeyPairName>*

   将 *<UserName>* 替换为您当前登录的用户名称，并将 *<KeyPairName>* 替换为新密钥对的名称。

   在以下示例中，我们指定了 Windows 电脑上的 C:\Keys 目录，并将新密钥命名为 MyNewLightsailCustomKey。

```
C:\Users\[redacted]>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\[redacted]/.ssh/id_rsa): C:\Keys\MyNewLighstailCustomKey
```

4. 输入密钥的密码短语然后按 Enter 键。输入密码短语时您不会看到它。

   稍后在 SSH 客户端上配置私有密钥以连接到已配置公有密钥的实例时，您将需要此密码短语。

```
Enter passphrase (empty for no passphrase):
```

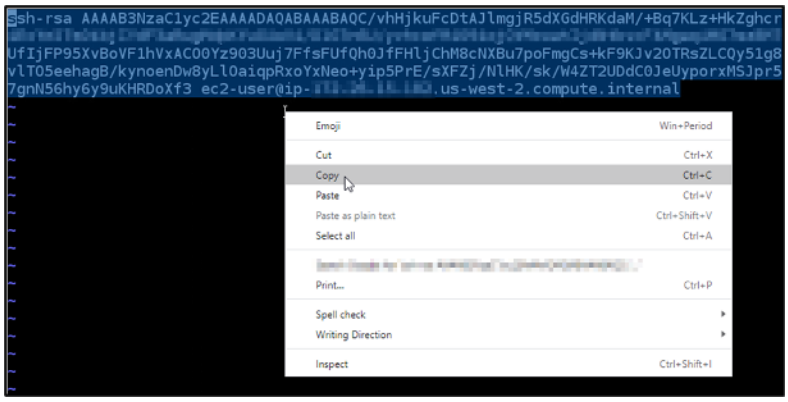
5. 再次输入密码短语以进行确认，然后按下 Enter 键。输入密码短语时您不会看到它。

```
Enter same passphrase again:
```

6. 提示消息将会确认您的私有密钥和公有密钥已保存到指定目录中。

```
Your identification has been saved in C:\Keys\MyNewLighstailCustomKey.
Your public key has been saved in C:\Keys\MyNewLighstailCustomKey.pub.
```

7. 打开公有密钥（.PUB）文件，然后复制文件中的文本。

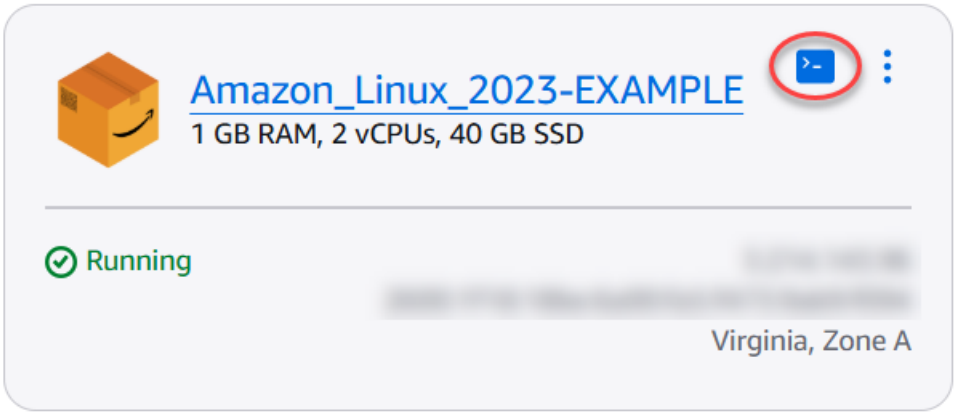


继续阅读本指南的下一部分，将您的新公钥添加到 Lightsail 实例。

第 3 步：将公有密钥添加到实例

完成以下过程以将公有密钥添加到您的实例中。公有密钥内容保存在 Linux 和 Unix 实例上的 `~/.ssh/authorized_keys` 文件中。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上选择 “实例” 部分。
3. 选择适用于要连接的实例的基于浏览器的 SSH 客户端图标。



4. 连接成功后，输入以下命令，以使用您选择的文本编辑器编辑 authorized_keys 文件。以下步骤将使用 Vim 进行演示。

```
sudo vim ~/.ssh/authorized_keys
```

您应看到类似于以下示例的结果，其中显示了在实例上配置的当前公有密钥。在本例中，在 AWS 区域 中创建实例的 Lightsail 默认密钥是在该实例上配置的唯一公钥。



5. 在 Vim 编辑器中按 I 键以进入插入模式。
6. 在文件中的最后一个公有密钥之后输入换行符。
7. 粘贴您之前在本指南中复制的公有密钥文本（创建新密钥对之后）。您会看到类似于以下示例的结果：



8. 按 ESC 键。然后键入 `:wq!` 并按 Enter 键以保存编辑内容，然后退出 Vim 编辑器。

新的公有密钥现已添加到您的实例。继续按照本指南的下一部分操作，以使用新的公有密钥连接到实例。

第 4 步：使用新密钥对连接到实例

要测试新密钥对，请断开与实例的连接，然后使用您之前在本指南中创建的私有密钥重新连接。有关更多信息，请参阅 Amazon Lightsail 中的密钥对和连接实例。使用新密钥成功连接到实例后，您可以从实例中删除旧密钥。继续下一步骤以了解如何从实例中删除公有密钥。

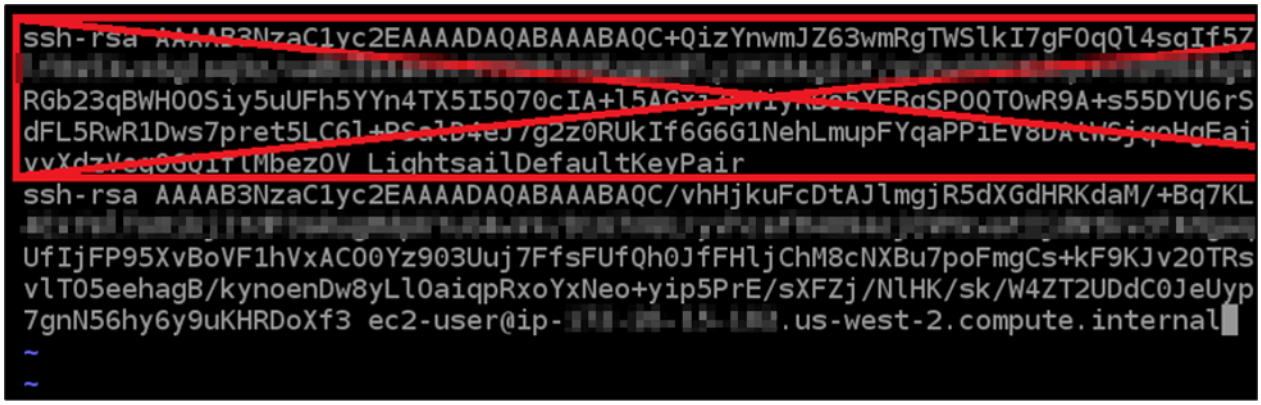
第 5 步：从实例中删除现有的公有密钥

完成以下过程以从实例中删除公有密钥。这可以防止用户使用旧密钥对连接到实例。使用新密钥对成功连接到实例后，请执行此操作。

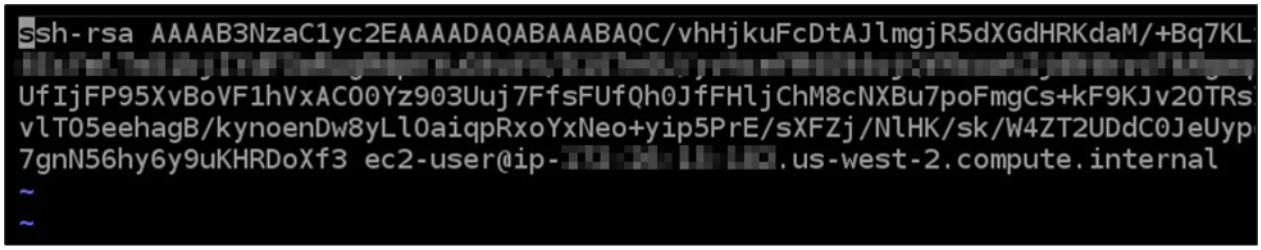
1. 使用 SSH 连接到实例。
2. 输入以下命令，以使用您选择的文本编辑器编辑 authorized_keys 文件。以下步骤将使用 Vim 进行演示。

```
sudo vim ~/.ssh/authorized_keys
```

3. 在 Vim 编辑器中按字母 I 键以进入插入模式。
4. 删除包含要从实例中删除的公有密钥的文本行。



结果应与以下示例类似，仅显示新的公有密钥。



5. 按 ESC 键。然后键入 :wq! 并按 Enter 键以保存编辑内容，然后退出 Vim 编辑器。

删除的密钥随即从您的实例中删除。您的实例将拒绝使用该密钥对的私有密钥进行连接。

在 Lightsail 上连接到 Linux 或 Unix 实例

Amazon Lightsail 为您提供基于浏览器的 SSH 客户端，这是连接您的 Linux 或 Unix 实例的最快方式。您也可以使用自己的 SSH 客户端连接到实例。有关更多信息，请参阅下载并设置 PuTTY。

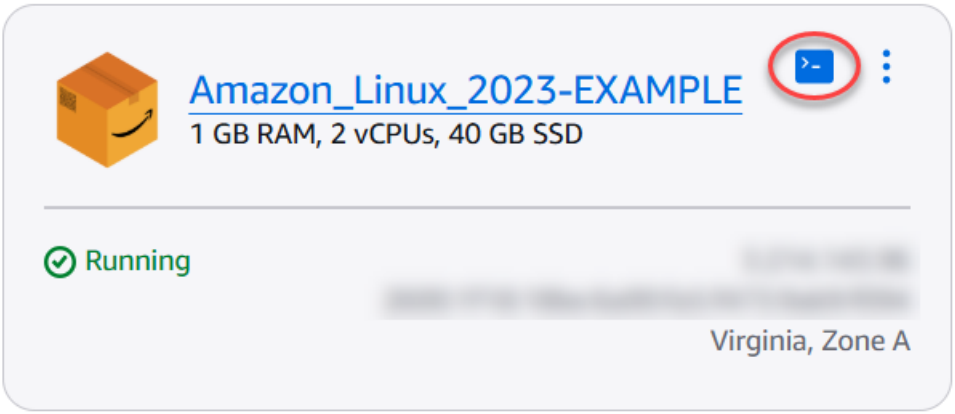
通过 SSH 连接到实例后可在服务器上执行管理任务，例如安装软件包或配置 Web 应用程序。使用基于浏览器的 SSH 客户端时不需要安装任何软件，并且几乎在您创建实例后就可立即使用它。

要连接到 Lightsail 中的 Windows 服务器实例，请参阅连接到基于 Windows 的实例。

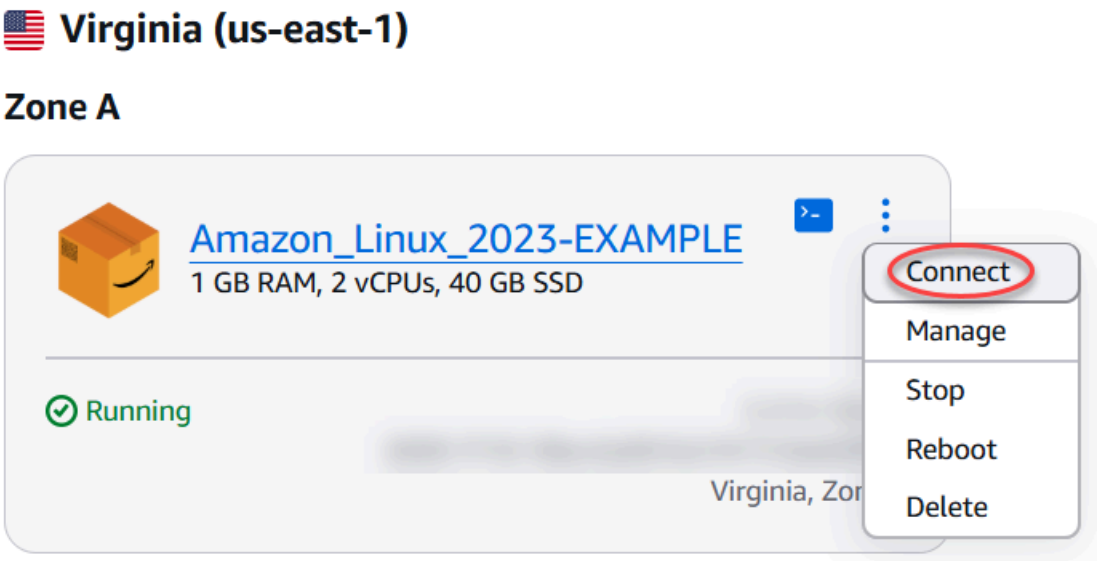
连接到 Linux 或 Unix 实例

1. 登录 Lightsail 控制台。
2. 通过以下方法之一访问要连接到的实例的基于浏览器的 SSH 客户端：

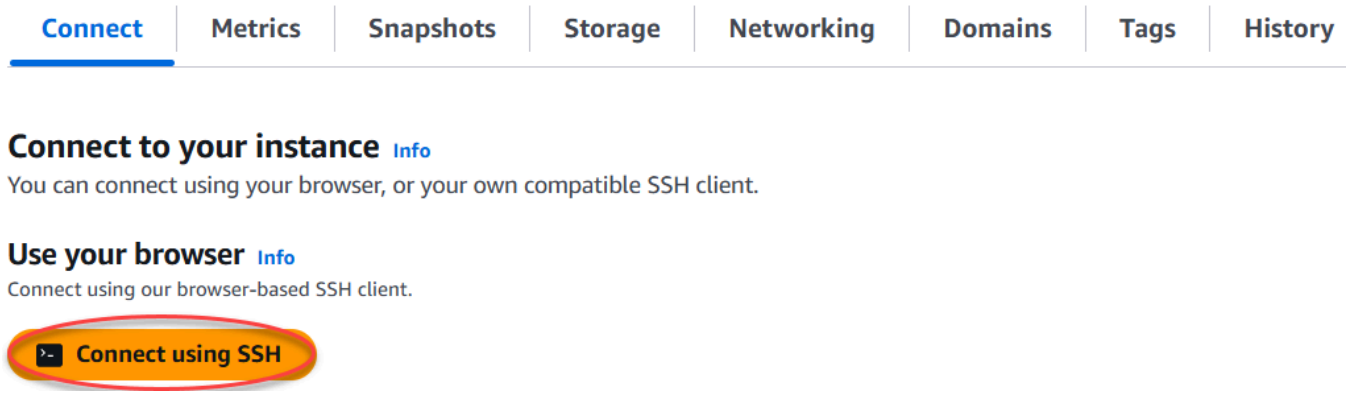
   - 选择快速连接图标，如以下示例所示。



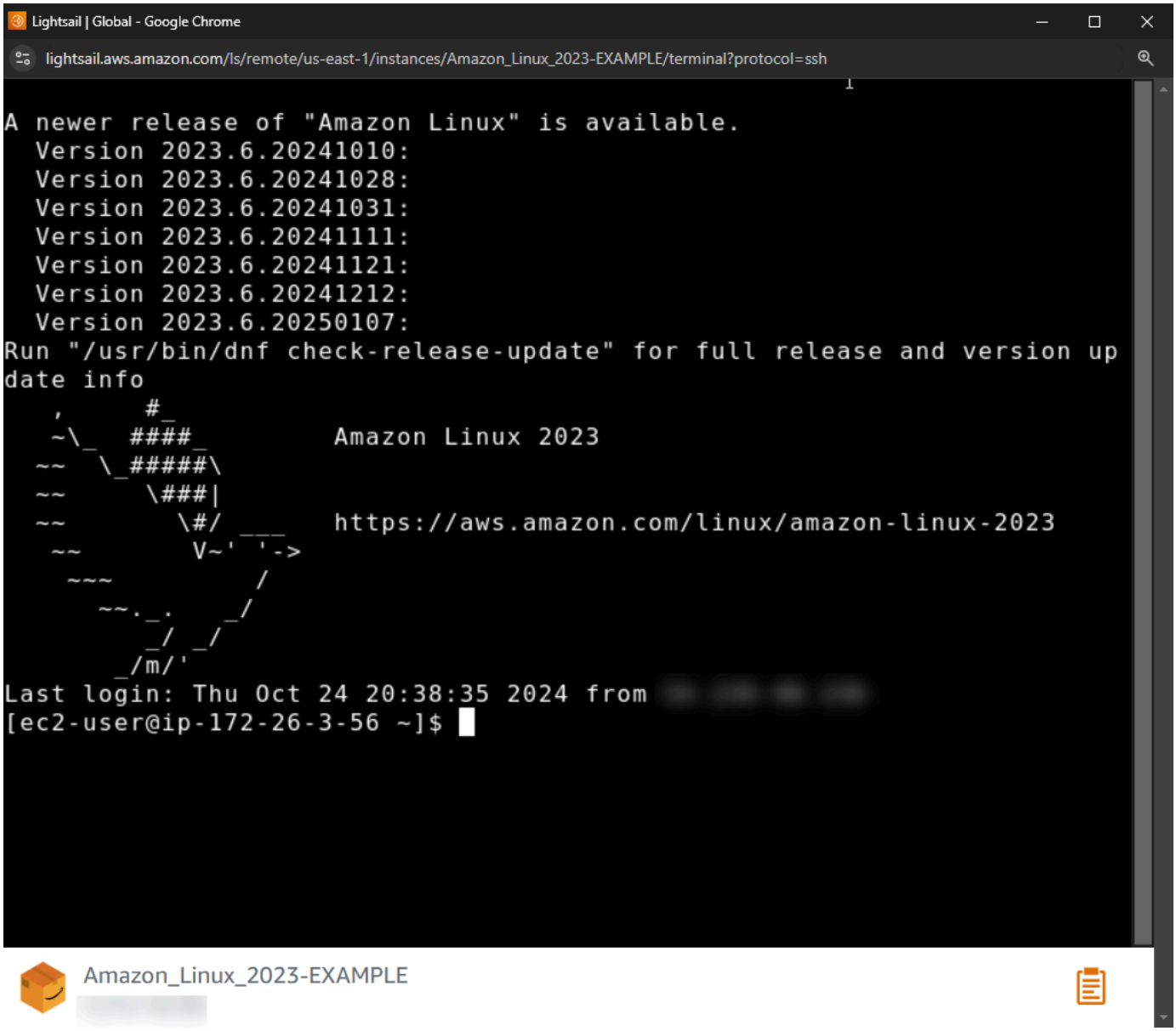
   - 选择操作菜单图标 (⋮)，然后选择 Connect (连接)。



   - 选择实例的名称，在 Connect（连接）选项卡上，选择 Connect using SSH（使用 SSH 连接）。



您可以在基于浏览器的 SSH 客户端打开后开始与实例交互，此时会显示一个终端屏幕，如以下示例所示：



> **Note**
>
> Connect（连接）选项卡还提供了使用您自己的 SSH 客户端进行连接所需的信息。有关更多信息，请参阅下载并设置 PuTTY

使用基于浏览器的 SSH 客户端与 Linux 或 Unix 实例交互

键入 Linux 或 Unix 命令直接进入终端屏幕，将文本粘贴到终端屏幕，或从基于浏览器的 SSH 客户端的终端屏幕上复制文本。以下部分演示了如何利用 SSH 中的剪贴板复制并粘贴文本。

将文本粘贴到基于浏览器的 SSH 客户端中

1. 选中本地桌面中的文本，然后按 Ctrl+C 或 Cmd+C 以将其复制到本地剪贴板中。
2. 在基于浏览器的 SSH 客户端的右下角，选择剪贴板图标。此时系统将显示基于浏览器的 SSH 客户端剪贴板文本框。
3. 单击该文本框，然后按 Ctrl+V 或 Cmd+V 组合键，将内容从本地剪贴板粘贴到基于浏览器的 SSH 客户端的剪贴板。
4. 右键单击 SSH 终端屏幕上的任意区域，将文本从基于浏览器的 SSH 客户端剪贴板粘贴到终端屏幕。



从基于浏览器的 SSH 客户端中复制文本

1. 在终端屏幕上选中要复制的文本。
2. 在基于浏览器的 SSH 客户端的右下角，选择剪贴板图标。此时系统将显示基于浏览器的 SSH 客户端剪贴板文本框。
3. 选中要复制的文本，然后按 Ctrl+C 或 Cmd+C，以将其复制到本地剪贴板中。您现在可以将复制的文本粘贴到本地桌面上的任何位置。



使用 SSH 命令连接到 Lightsail Linux 或 Unix 实例

如果你的本地计算机使用 Linux 或 Unix 操作系统，包括 macOS，那么你可以使用 SSH 客户端通过终端窗口连接到 Amazon Lightsail 中的 Linux 或 Unix 实例。

本指南中介绍的连接实例的方法是众多方法之一。有关其他方法的更多信息，请参阅 SSH 密钥对。

在 Lightsail 中连接你的 Linux 或 Unix 实例的最简单方法是使用 Lightsail 控制台中提供的基于浏览器的 SSH 客户端。有关更多信息，请参阅连接到 Linux 或 Unix 实例。

内容

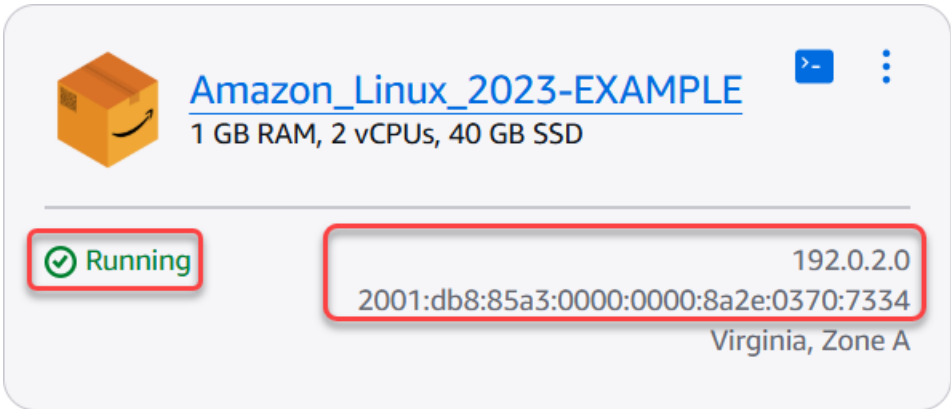
- 步骤 1：确认实例正在运行并获取公有 IP 地址
- 步骤 2：确认实例正在使用 SSH 密钥对
- 步骤 3：更改私有密钥的权限并使用 SSH 连接到实例

步骤 1：确认实例正在运行并获取公有 IP 地址

在以下步骤中，您登录 Lightsail 控制台以确认您的实例处于运行状态并获取您的实例的公有 IP 地址。实例必须处于运行状态才能建立 SSH 连接，并且在本指南之后的部分需要实例的公有 IP 地址才能进行连接。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的 “实例” 部分，找到您要连接的实例。
3. 确认实例处于正在运行状态，并记下实例的公有 IP 地址。

   实例的状态及其公有 IP 地址在实例名称的旁边列出，如以下示例所示。

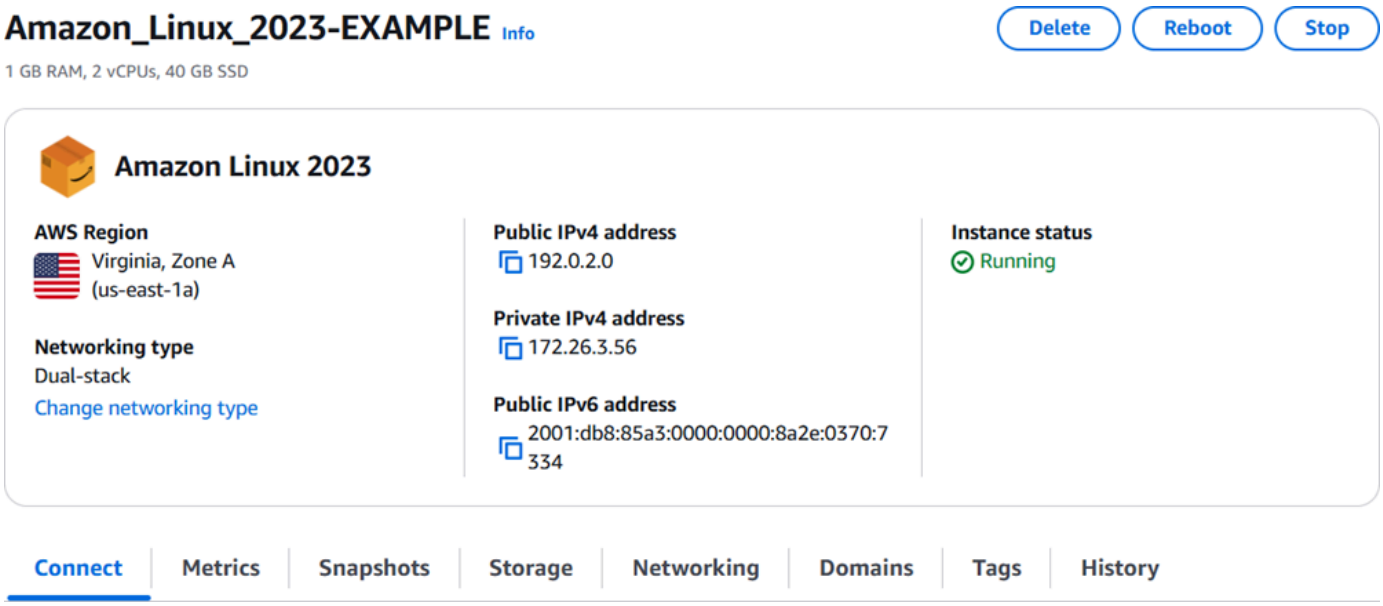


步骤 2：确认实例正在使用 SSH 密钥对

在以下过程中，您将确认实例正在使用 SSH 密钥对。您需要密钥对的私有密钥才能对实例进行身份验证并建立 SSH 连接。

1. 在 Lightsail 主页的 “实例” 部分，选择要连接的实例的名称。

   实例管理页面随即显示，其中包含用于管理实例的各种选项卡选项。

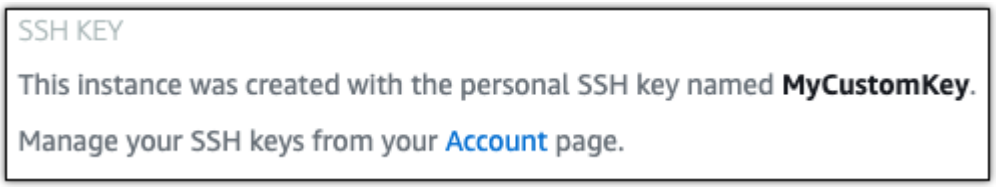


2. 在连接选项卡中，向下滚动以查看实例正在使用密钥对。有两种可能的情况：

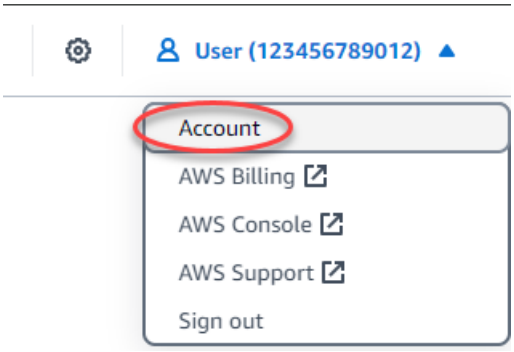
   1. 以下示例显示的实例使用您在其中创建实例的亚马逊云科技区域的默认密钥对。如果实例使用默认密钥对，则可以继续执行此过程的步骤 3 以下载密钥对的私有密钥。Lightsail 仅存储每个 AWS 区域的默认密钥对的私钥。

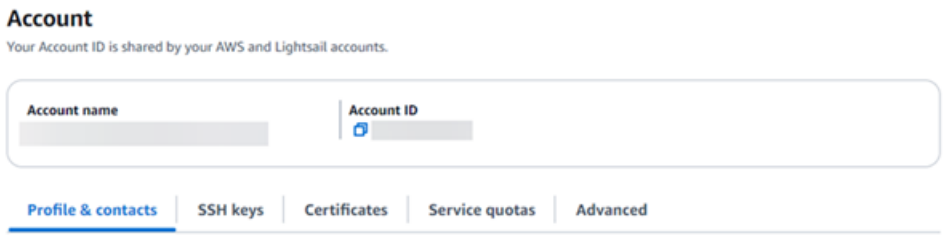
   2. 以下示例显示的实例使用您上传或创建的自定义密钥对。如果实例使用的是自定义密钥对，则需要找到存储密钥的自定义密钥对的私有密钥。如果您丢失了自定义密钥对的私有密钥，则无法使用您自己的客户端与实例建立 SSH 连接。但是，您可以继续使用 Lightsail 控制台中提供的基于浏览器的 SSH 客户端。继续本指南的下一个部分步骤 3：更改私有密钥的权限并使用 SSH 连接到实例部分，然后找到自定义密钥对的私有密钥。

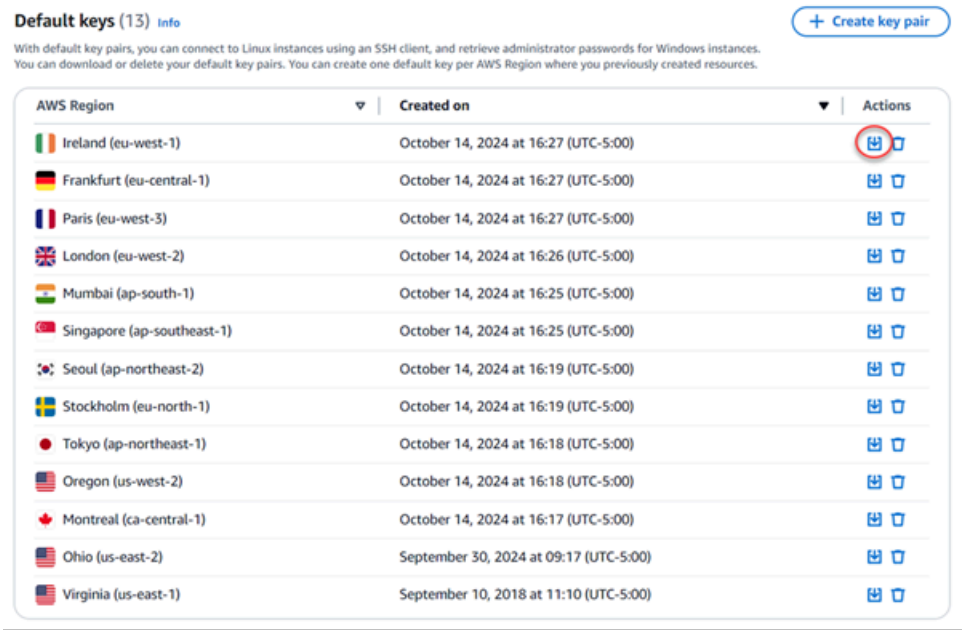
3. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
4. 在下拉菜单中选择账户。



账户管理页面随即显示，其中包含用于管理账户设置的各种选项卡选项。



5. 选择 SSH 密钥选项卡。
6. 向下滚动，然后选择要连接的实例 AWS 区域 的默认密钥旁边的下载图标。



私有密钥将下载到本地机器中。您可能希望将下载的密钥移动到存储所有 SSH 密钥的目录，例如用户主目录中的“Keys”文件夹。您将需要引用在本指南下一部分保存私有密钥的目录。如果私有密钥尝试使用 .pem 以外的格式保存，则应在保存之前手动将格式更改为 .pem。

> **Note**
>
> Lightsail 不提供用于操作.pem文件或其他证书格式的实用工具。如果您需要转换私有密钥文件的格式，可以随时使用免费的开源工具（如 OpenSSL）。

继续本指南的下一个部分步骤 3：更改私有密钥的权限并使用 SSH 连接到实例，以使用刚才下载的私有密钥并建立实例的 SSH 连接。

步骤 3：更改私有密钥的权限并使用 SSH 连接到实例

在以下过程中，您将更改私有密钥文件的权限，以便只有您可以读取和写入该文件。然后，您可以在本地计算机上打开终端窗口，并运行 SSH 命令在 Lightsail 中与您的实例建立连接。

1. 在本地机器上打开终端窗口。
2. 输入以下命令，使密钥对的私有密钥只能由您读写。这是某些操作系统所需的最佳安全实践。

```
sudo chmod 400 /path/to/private-key.pem
```

在该命令中，将 */path/to/private-key.pem* 替换为保存实例所用密钥对的私有密钥的目录路径。

示例：

```
sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
```

3. 输入以下命令，使用 SSH 连接到 Lightsail 中的实例：

```
ssh -i /path/to/private-key.pem username@public-ip-address
```

在该命令中，将：

- */path/to/private-key.pem*其中包含您保存实例正在使用的密钥对的私钥的目录路径。
- *username*使用您的实例的用户名。根据实例使用的蓝图，您可以指定以下用户名之一：
  - AlmaLinux OS 9，亚马逊 Linux 2，亚马逊 Linux 2023，CentOS Stream 9,FreeBSD，以及 openSUSE 实例：`ec2-user`
  - Debian 实例：`admin`

- Ubuntu 实例：`ubuntu`
- Bitnami 实例：`bitnami`
- Plesk 实例：`ubuntu`
- cPanel 和 WHM 实例：`centos`

- *`public-ip-address`*替换为你在本指南前面的 Lightsail 控制台中记下的实例的公有 IP 地址。

具有绝对路径的示例：

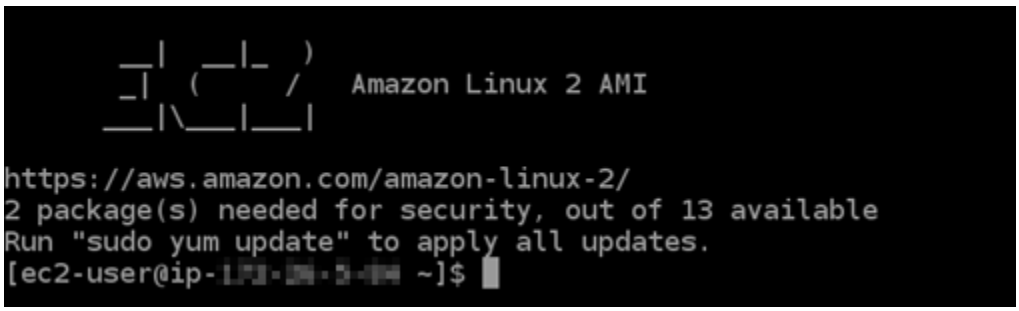
```
ssh -i /Users/user/Keys/LightsailDefaultKey-us-west-2.pem ec2-user@192.0.2.0
```

具有相对路径的示例：

请注意 `.pem` 文件的 `./` 前缀。将不能忽略 `./` 而只是写入 `LightsailDefaultKey-us-west-2.pem`。

```
ssh -i ./LightsailDefaultKey-us-west-2.pem ec2-user@192.0.2.0
```

如果您看到实例的欢迎消息，则您已成功连接到实例。以下示例显示了 Amazon Linux 2 实例的欢迎消息；其他实例蓝图具有类似的欢迎消息。连接后，您可以在 Lightsail 中对您的实例执行命令。要断开连接，请输入 `exit` 并按 Enter。



使用 Putty 连接到 Linux/Unix Lightsail 实例

除了 Lightsail 中基于浏览器的 SSH 终端外，你还可以使用 Putty 等 SSH 客户端连接到基于 Linux 的实例。要了解如何设置 PuTTY，请参阅在 Lightsail 中下载并设置 PuTTY 以使用 SSH 进行连接。

> **Note**
>
> 要使用 RDP 连接到基于 Windows 的实例，请参阅连接到基于 Windows 的 Lightsail 实例。

您可以使用 Lightsail 提供的默认私钥、来自 Lightsail 的新私钥或用于其他服务的其他私钥。

1. 启动 PuTTY（例如，从 Start（开始）菜单中，选择 All Programs（所有程序）、PuTTY、PuTTY）。
2. 选择 Load（加载），然后查找已保存的会话。

   如果您没有保存的会话，请参阅步骤 4：使用私有密钥和实例信息完成对 PuTTY 的配置。
3. 根据您的实例操作系统，使用以下默认用户名称之一登录：

   - AlmaLinux，亚马逊 Linux 2，亚马逊 Linux 2023，CentOS Stream 9,FreeBSD，以及 openSUSE 实例：`ec2-user`
   - Debian 实例：`admin`
   - Ubuntu 实例：`ubuntu`
   - Bitnami 实例：`bitnami`
   - Plesk 实例：`ubuntu`
   - cPanel 和 WHM 实例：`centos`

   有关实例操作系统的更多信息，请参阅在 Lightsail 中选择镜像。

要了解有关 SSH 的更多信息，请参阅 SSH 和连接到您的 Amazon Lightsail 实例。

使用 Putty 连接到你的 Lightsail Linux 实例

你可以使用像 Putty 这样的 SSH 客户端连接到你的 Amazon Lightsail 实例。PuTTY 需要您的私有 SSH 密钥的副本。你可能已经有了密钥，或者你可能想使用 Lightsail 创建的密钥对。无论怎样，我们都能满足您的需求。有关 SSH 的更多信息，请参阅 SSH 密钥对。本主题将引导您完成下载密钥对并将 PuTTY 设置为连接到您的实例的步骤。

本指南中介绍的连接实例的方法是众多方法之一。有关其他方法的更多信息，请参阅 SSH 密钥对。

在 Lightsail 中连接你的 Linux 或 Unix 实例的最简单方法是使用 Lightsail 控制台中提供的基于浏览器的 SSH 客户端。有关更多信息，请参阅在 Amazon Lightsail 中连接您的 Linux 或 Unix 实例。

先决条件

- 你需要在 Lightsail 中运行一个正在运行的实例。有关更多信息，请参阅在 Amazon Lightsail 中创建实例。
- 建议您创建一个静态 IP 地址并将其附加到实例，这样，如果您的公有 IP 地址稍后发生更改，您就不必重新配置 PuTTY。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

步骤 1：下载并安装 PuTTY

PuTTY 是适用于 Windows 的 SSH 的免费实现形式。在 PuTTY 网站上详细了解 PuTTY，包括与不允许加密的国家/地区相关的限制。如果您已经有 PuTTY，则可跳至步骤 2。

1. 通过以下链接下载 PuTTY 安装程序或可执行文件：下载 PuTTY。

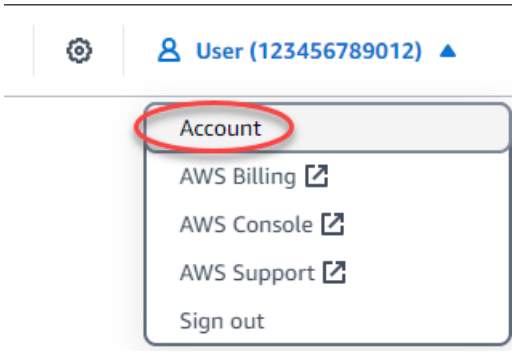
   如果您在决定要选择的下载内容方面需要帮助，请参阅 PuTTY 文档。建议使用最新版本。

2. 在配置 PuTTY 之前，请转到步骤 2 以获取您的私有密钥。

步骤 2：准备好您的私有密钥

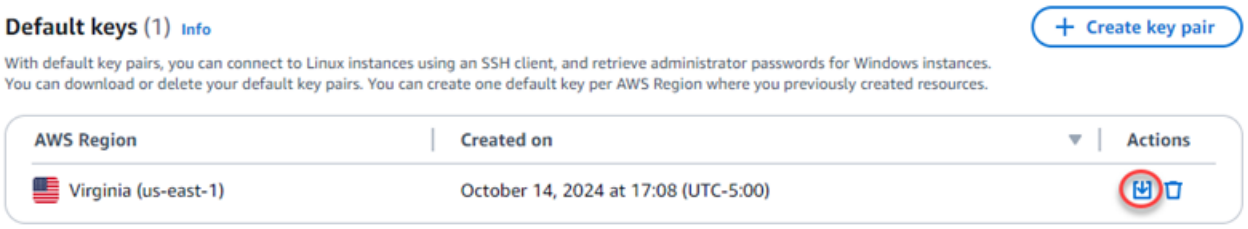
您有多个用于获取私有密钥的选项。你可能想使用 Lightsail 生成的默认私钥，你可能想让 Lightsail 为你创建一个新的私钥，或者你可能已经有来自其他服务的私钥。每个选项的步骤如以下过程中所述：

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 选择 SSH Keys（SSH 密钥）选项卡。
5. 根据您想要使用的私有密钥，选择以下选项之一：

- 要使用 Lightsail 生成的默认私钥，请在页面的默认密钥部分，选择您的实例 AWS 区域 所在位置的默认私钥旁边的下载图标。



- 要在 Lightsail 中创建新的密钥对，请在页面的自定义密钥部分，选择创建密钥对。选择您的实例 AWS 区域 所在的位置，然后选择创建。输入名称，然后选择 Generate key pair（生成密钥对）。您可以选择下载私有密钥。

> **Important**
>
> 您只能下载一次私有密钥。请将其保存在安全位置。

- 要使用您自己的密钥对，请选择 Upload New（上传新项）。选择您的实例 AWS 区域 所在的位置，然后选择上传。选择 Upload key（上传文件），然后在本地驱动器中找到该文件。当您准备好将公钥文件上传到 Lightsail 时，请选择上传密钥。

6. 如果您下载了私钥，或者在 Lightsail 中创建了新的私钥，请确保将`.pem`密钥文件保存在可以轻松找到的地方。

   我们还建议您为该文件设置权限以使他人无法读取。

第 3 步：TTYgen 使用你的 Lightsail 私钥配置 Pu

现在你已经有了`.pem`密钥文件的副本，你可以使用 PuTTY 密钥生成器 (Pu) 来设置 PuTTY。TTYgen

1. 启动 PuTTYgen （例如，从 “开始” 菜单中选择 “所有程序”、“P utty”、“Pu TTYgen”）。
2. 选择 Load（加载）。

   默认情况下，Pu 仅TTYgen 显示`.ppk`扩展名为的文件。要找到您的 `.pem` 文件，请选择显示所有类型的文件的选项。
3. 选择 `lightsailDefaultKey.pem`，然后按 Open（打开）。

   Pu TTYgen 确认您已成功导入密钥，然后您可以选择 “确定”。
4. 选择 Save private key（保存私有密钥），然后确认您不想使用密码保存它。

如果您选择创建密码来作为一项额外的安全措施，请记住，您每次使用 PuTTY 连接到您的实例时都需要输入密码。

5. 指定名称和用于保存私有密钥的位置，然后选择 Save（保存）。
6. 近距离观察TTYgen。

步骤 4：使用您的私有密钥和实例信息完成配置 PuTTY

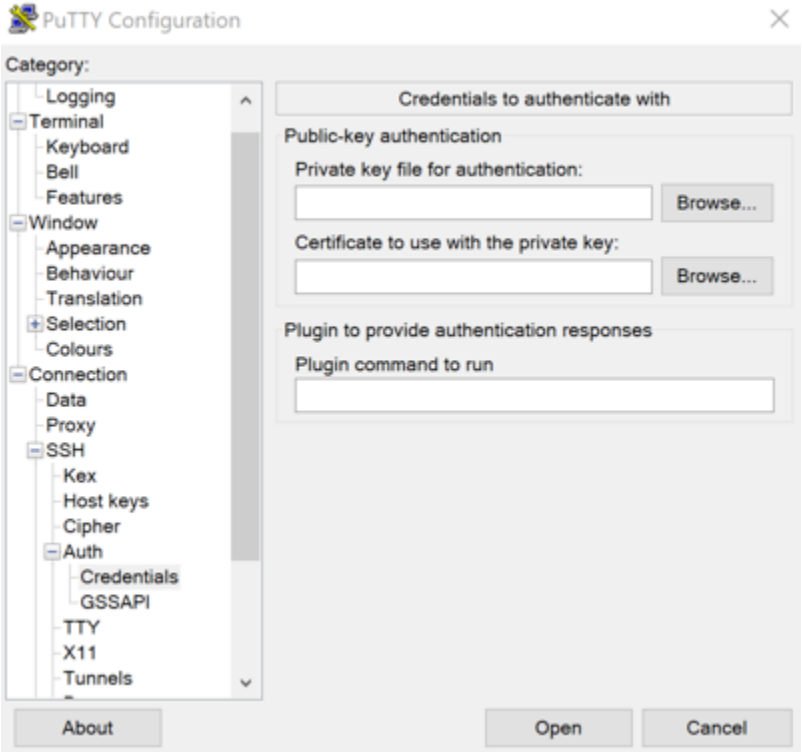
您就要成功了！坚持一下，我们将进行最后一个更改。

1. 打开 PuTTY。
2. 从 Lightsail 中，从实例管理页面获取公有 IP 地址（希望你使用的是静态 IP 地址）。

   您可以从 Lightsail 主页获取公有 IP 地址，也可以选择您的实例以查看有关它的更多详细信息。
3. 将公有 IP 地址键入（或粘贴）到 Host Name（主机名称）（或 IP address（IP 地址））字段。

> **Note**
>
> 您的 Lightsail 实例上的端口 22 已开放给 SSH，因此请接受默认端口。

4. 在连接下，展开 SSH 和身份验证，然后选择凭证。



5. 选择 Browse（浏览）以导航到您在上一步中创建的 .ppk 文件，然后选择 Open（打开）。
6. 再次选择打开，然后选择接受以在将来信任此连接。
7. 根据您的实例操作系统，使用以下默认用户名称之一登录：

   - AlmaLinux，亚马逊 Linux 2，亚马逊 Linux 2023，CentOS Stream 9,FreeBSD，以及 openSUSE 实例：`ec2-user`
   - Debian 实例：`admin`
   - Ubuntu 实例：`ubuntu`
   - Bitnami 实例：`bitnami`
   - Plesk 实例：`ubuntu`
   - cPanel 和 WHM 实例：`centos`

   有关实例操作系统的更多信息，请参阅选择映像。
8. 请务必保存您的连接以供将来使用。

后续步骤

如果您需要再次连接，请参阅使用 PuTTY 连接到您基于 Linux/Unix 的实例。

使用 SFTP 将文件安全地传输到 Lightsail Linux 实例

您可以使用 SFTP（SSH 文件传输协议）连接到您的实例，从而在本地计算机与 Amazon Lightsail 中的 Linux 或 Unix 实例之间传输文件。要执行此操作，您必须获取实例的私有密钥，然后使用它来配置 FTP 客户端。本教程向您展示如何配置 FileZilla FTP 客户端以连接到您的实例。这些步骤可能也适用于其他 FTP 客户端。

内容

- 前提条件
- 获取实例的 SSH 密钥
- 配置 FileZilla 并连接到您的实例

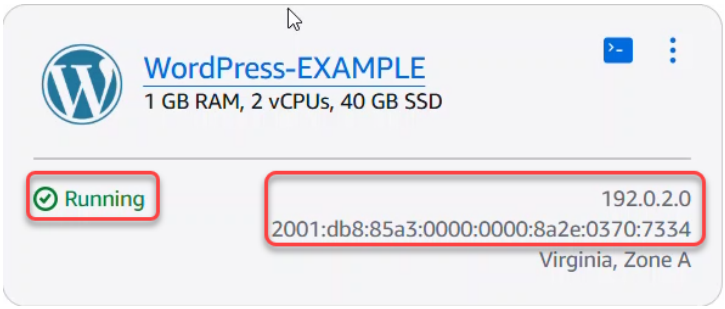
前提条件

满足以下先决条件（如果尚未满足）：

- 下载并安装到您的本地计算机 FileZilla 上。有关更多信息，请参阅以下下载选项：

- 下载适用于 Windows 的 FileZilla 客户端
- 下载适用于 Mac OS X 的 FileZilla 客户端
- 下载 Linux 版 FileZilla 客户端

- 获取实例的公有 IP 地址。登录 Lightsail 控制台，然后复制显示在您的实例旁边的公有 IP 地址，如以下示例所示：

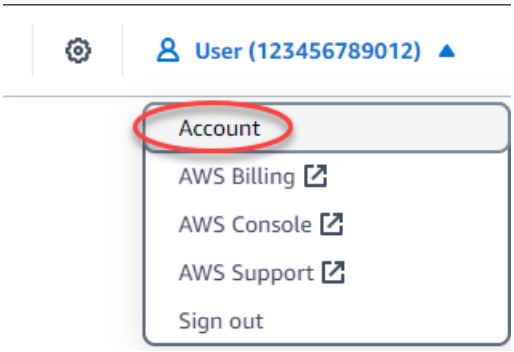


获取实例的 SSH 密钥

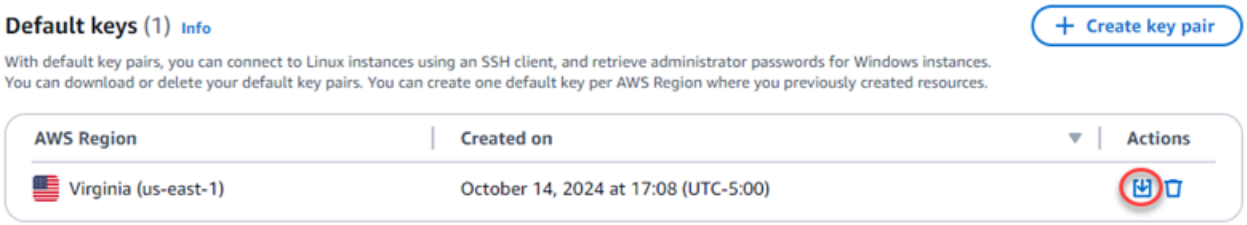
完成以下步骤以获取您的实例 AWS 区域的默认私有密钥，这是使用连接到您的实例所必需的 FileZilla。

> **Note**
>
> 如果您使用的是自己的密钥对，或者使用 Lightsail 控制台创建了密钥对，请找到自己的私钥并使用它来连接您的实例。当你上传自己的密钥或使用 Lightsail 控制台创建密钥对时，Lightsail 不会存储你的私钥。没有您的私有密钥，无法使用 SFTP 连接到您的实例。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 选择 SSH Keys（SSH 密钥）选项卡。
5. 向下滚动到页面的 Default keys（默认密钥）部分。
6. 选择实例所在区域的默认私有密钥旁边的 Download (下载)。

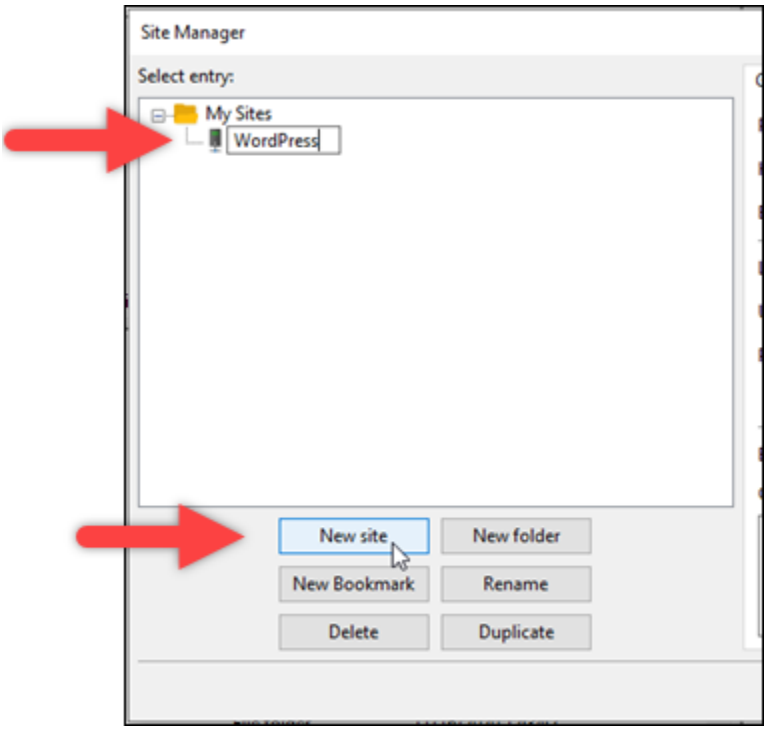


7. 将私有密钥保存在您的本地驱动器上的安全位置。

配置 FileZilla 并连接到您的实例

完成以下步骤进行配置 FileZilla 以连接到您的实例。

1. 打开 FileZilla。
2. 依次选择文件、站点管理器。
3. 选择新站点，然后为您的网站指定一个名称。



4. 在协议下拉列表中，选择 SFTP – SSH 文件传输协议。
5. 在主机文本框中，输入或粘贴您实例的公有 IP 地址。

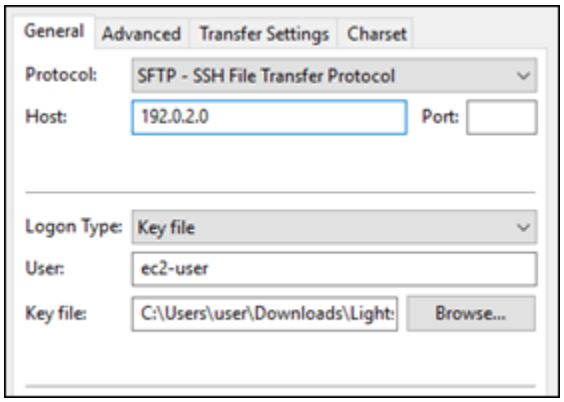
6. 在登录类型下拉列表中，选择密钥文件。
7. 在用户文本框中，根据您的实例操作系统，输入以下默认用户名之一：

   - AlmaLinux，亚马逊 Linux 2，亚马逊 Linux 2023，CentOS Stream 9,FreeBSD，以及 openSUSE 实例：`ec2-user`
   - Debian 实例：`admin`
   - Ubuntu 实例：`ubuntu`
   - Bitnami 实例：`bitnami`
   - Plesk 实例：`ubuntu`
   - cPanel 和 WHM 实例：`centos`

   Important

   如果您使用的用户名与此处列出的默认用户名不同，则可能需要授予实例的用户写入权限。

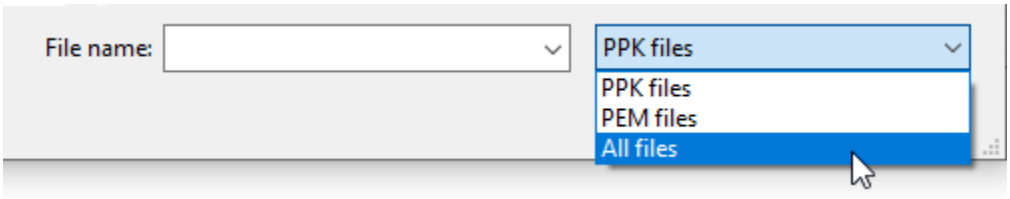
8. 在密钥文件文本框旁边，选择浏览。



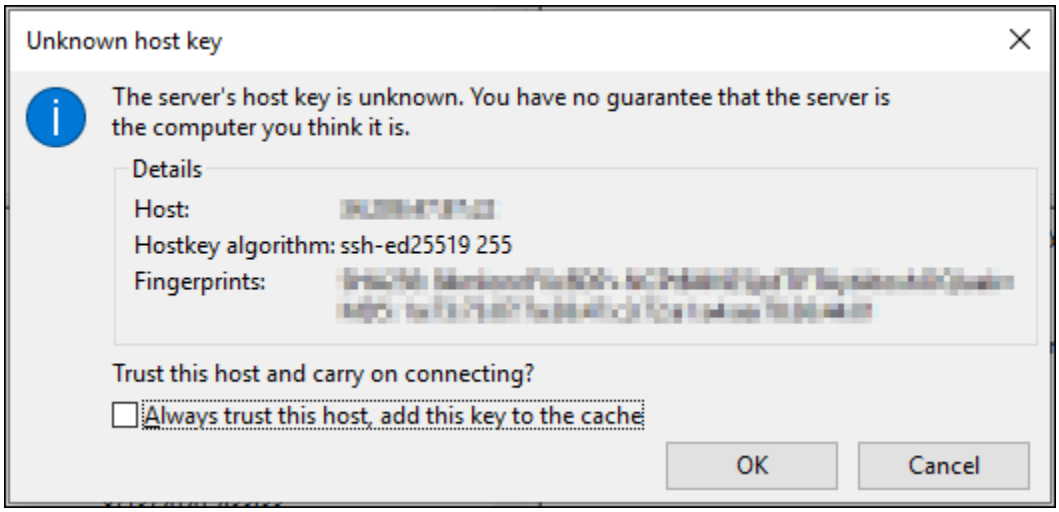
9. 找到您之前在本步骤中从 Lightsail 控制台下载的私钥文件，然后选择 “打开”。

   Note

   如果您使用的是 Windows，在搜索 pem 文件时将默认文件类型更改为所有文件。



10. 选择连接。
11. 您可能会看到类似于以下示例的提示，指示主机密钥未知。选择确定确认提示，然后连接到您的实例。



如果您看到类似于以下示例的状态消息，则说明已成功连接：

```
Status:     Connecting to 192.0.2.0..
Status:     Connected to 192.0.2.0
Status:     Retrieving directory listing...
Status:     Listing directory /home/ec2-user
Status:     Directory listing of "/home/ec2-user" successful
```

有关使用的更多信息 FileZilla，包括如何在本地计算机和实例之间传输文件，请参阅 FileZilla Wiki 页面。

使用 RDP 连接到你的 Lightsail Windows 实例

你可以使用 Lightsail 控制台中提供的基于浏览器的 RDP 客户端在 Amazon Lightsail 中连接你的 Windows 服务器实例。基于浏览器的 RDP 客户端不需要安装软件，您可以在创建 Windows Server 实例后立即连接到该实例，而该实例随即就会变为可用状态。连接到实例后可在服务器上执行管理任务，例如安装软件或配置 Web 应用程序。

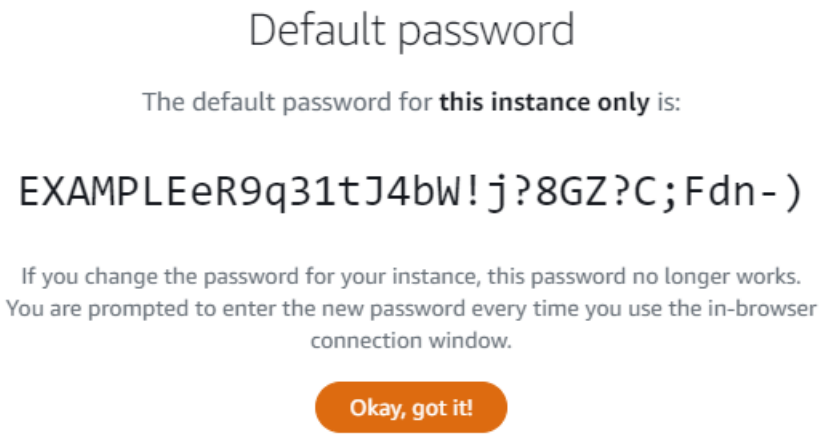
您还可以使用您自己的 RDP 客户端连接到您的实例，例如 Windows 附带的远程桌面连接。有关配置您自己的 RDP 客户端的更多信息，请参阅使用远程桌面连接客户端连接到 Windows 实例。要在 Lightsail 中连接到 Linux 或 Unix 实例，请参阅连接到你的 Linux 或 Unix 实例。

Windows Server 实例的默认管理员密码

随机生成的默认管理员密码会在创建 Windows Server 实例时分配给这些实例。Lightsail 控制台中基于浏览器的 RDP 客户端使用默认管理员密码登录您的实例。如果您更改了实例的管理员密码，则在您每次尝试使用基于浏览器的 RDP 客户端连接到该实例时，系统都会提示您手动输入该新密码。Lightsail 不会存储您的新管理员密码，也无法从您的实例中检索该密码。

> **Important**
>
> 如果您丢失了管理员密码，您将无法登录您的实例，也无法重置密码。将您的新管理员密码存储在安全的地方，以便在丢失密码时稍后可以找回，例如 S AWS ecrets Manager。有关更多信息，请参阅AWS Secrets Manager 用户指南。

您也可以将管理员密码改回原始默认管理员密码，以避免每次使用基于浏览器的 RDP 客户端访问实例时都会被提示输入密码。您可以通过在 Lightsail 主页上选择 “实例” 选项卡来找到原始的默认管理员密码。选择您的 Windows Server 实例的名称，选择 Connect（连接）选项卡，然后选择 Show default password（显示默认密码），即可查看原始默认管理员密码，如以下示例所示。



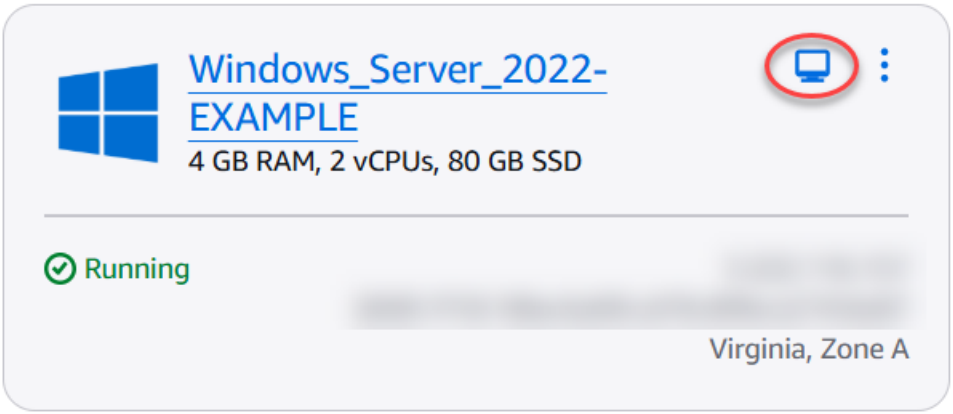
使用基于浏览器的 RDP 客户端连接到您的 Windows Server 实例

使用以下步骤在 Lightsail 控制台中使用基于浏览器的 RDP 客户端连接到你的 Windows 服务器实例。

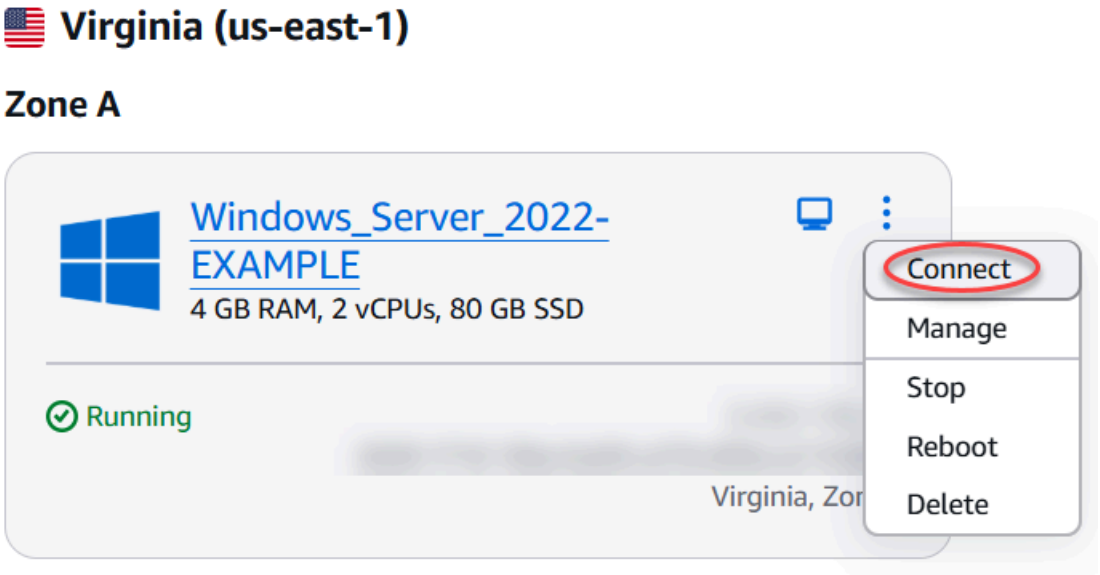
1. 登录 Lightsail 控制台。

2. 通过以下步骤之一访问您要连接的实例所对应的基于浏览器的 RDP 客户端：

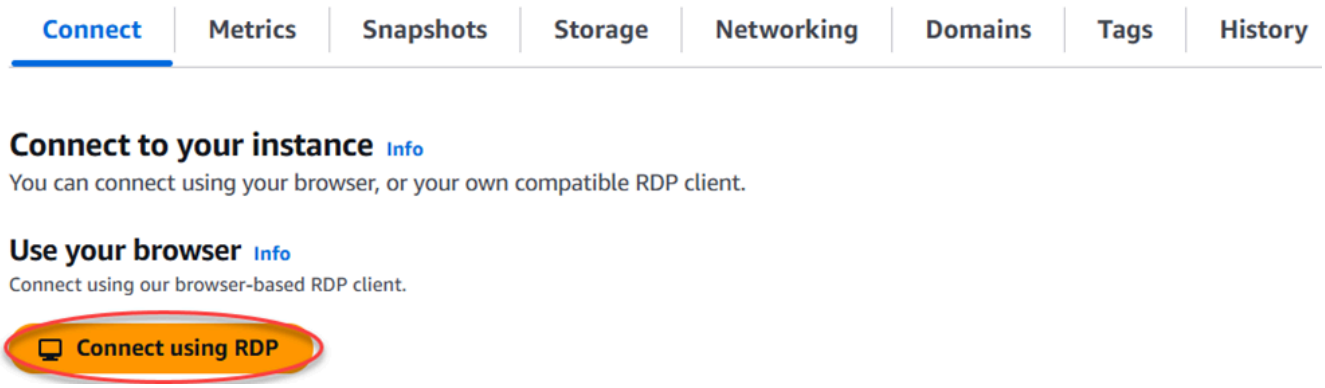
   - 选择基于浏览器的 RDP 客户端的图标，如以下示例所示。



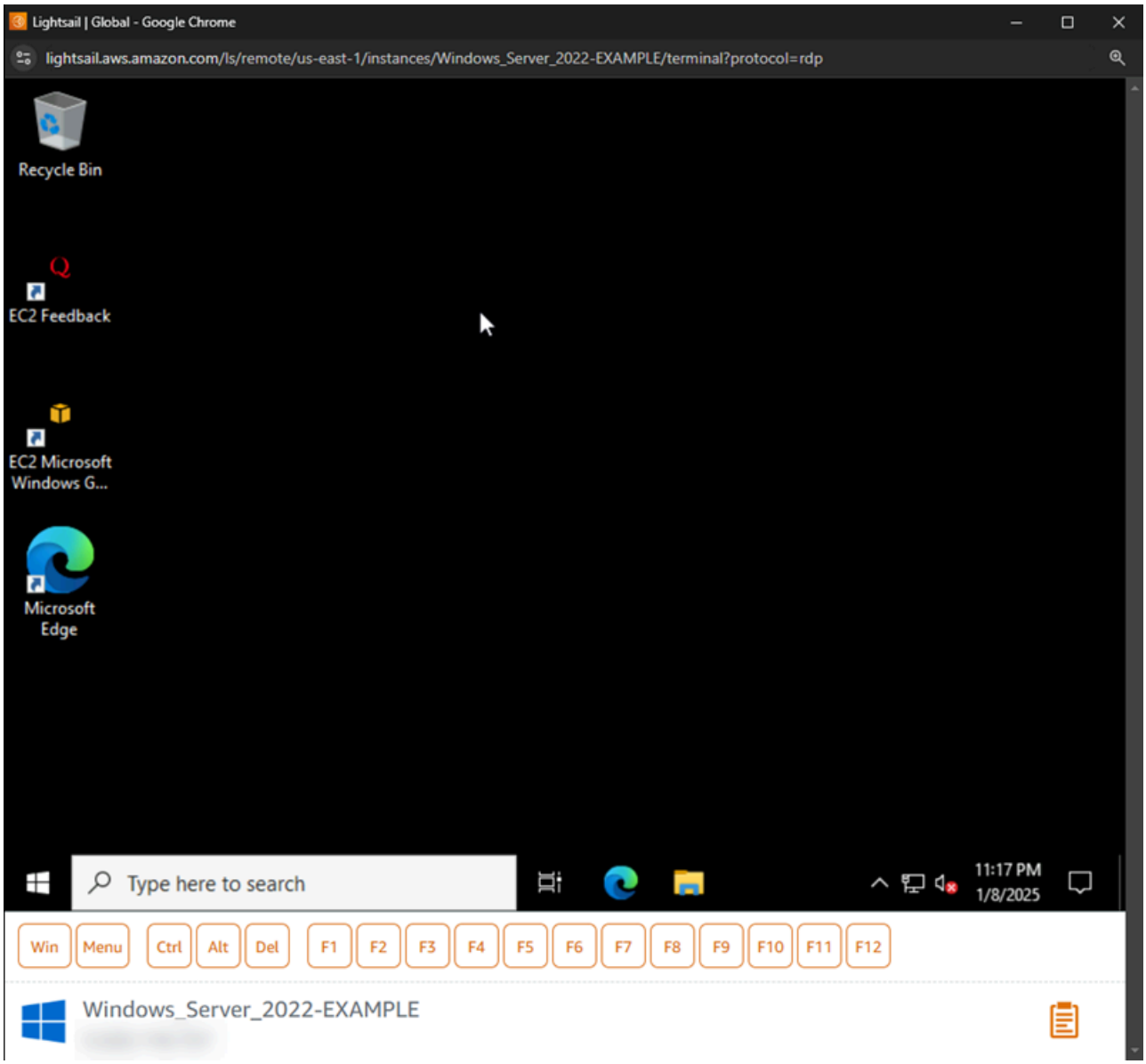
   - 选择操作菜单图标（⋮），然后选择连接，如以下示例所示。



   - 选择实例的名称，在 Connect（连接）选项卡上，选择 Connect using RDP（使用 RDP 连接）。



基于浏览器的 RDP 客户端打开后，您就可开始与实例进行交互，此时会显示一个 Windows 桌面，如以下示例所示。



> **Note**
>
> Connect（连接）选项卡还提供了使用您自己的 RDP 客户端进行连接所需的信息，如您的 Windows 实例的默认用户名和密码。有关配置自己的 RDP 客户端的更多信息，请参阅使用远程桌面连接客户端在 Amazon Lightsail 中连接您的 Windows 实例。

使用基于浏览器的 RDP 客户端与 Windows 实例交互

像使用您自己的本地 Windows 桌面那样使用基于浏览器的 RDP 客户端。RDP 包含专用于 Windows 的功能键和其他键，可帮助您与实例进行交互。以下部分演示了如何利用 RDP 中的剪贴板复制并粘贴文本。

将文本粘贴到基于浏览器的 RDP 客户端中

1. 选中本地桌面中的文本，然后按 Ctrl+C 或 Cmd+C 以将其复制到本地剪贴板中。
2. 在基于浏览器的 RDP 客户端的右下角，选择剪贴板图标。此时将显示基于浏览器的 RDP 客户端剪贴板文本框。
3. 单击该文本框，然后按 Ctrl+V 或 Cmd+V，以将内容从本地剪贴板粘贴到基于浏览器的 RDP 客户端的剪贴板。
4. 右键单击远程桌面屏幕上的任一区域，以将文本从基于浏览器的 RDP 客户端剪贴板粘贴到远程桌面屏幕。



从基于浏览器的 RDP 客户端中复制文本

1. 在远程桌面屏幕上选中要复制的文本。

2. 在基于浏览器的 RDP 客户端的右下角，选择剪贴板图标。此时将显示基于浏览器的 RDP 客户端剪贴板文本框。
3. 选中要复制的文本，然后按 Ctrl+C 或 Cmd+C，以将其复制到本地剪贴板中。您现在可以将复制的文本粘贴到本地桌面上的任何位置。



更改 Lightsail Windows 实例的管理员密码

当你创建基于 Windows 服务器的 Lightsail 实例时，我们会使用创建实例 AWS 区域 的默认密码。这样，就可以使用基于浏览器的远程桌面 (RDP) 客户端以及远程桌面连接等客户端轻松进行连接。

> **Important**
>
> 我们强烈建议您让 Lightsail 为您的实例生成密码。由于我们不存储您的自定义密码，因此如果您更改管理员密码，您可能会面临无法访问您的 Lightsail 实例的风险。

使用 Windows Server 更改管理员密码

您可以使用 Windows Server Change Password（更改密码）工具更改管理员密码。在基于 Windows 服务器的 Lightsail 实例Del上键入 Ctrl Alt + +，然后选择 “更改密码”。

使用获取 Lightsail 密钥对的密文 AWS CLI

如果您在基于 Windows 服务器的 Lightsail 实例上更改 AWS Command Line Interface 了密码，则可以使用AWS CLI() 获取有助于解密密码的信息。

> **Note**
>
> Lightsail 不提供用于操作.pem 文件的实用工具。如果您需要转换私有密钥文件的格式，可以随时使用免费的开源工具（如 OpenSSL for Linux 和 base64 for Windows）。

获取加密文字

1. 如果尚未安装并配置 AWS CLI，请执行该操作。

   有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface
2. 打开命令提示符或终端。
3. 键入以下命令。

   ```
   aws lightsail get-instance-access-details --instance-name my-instance
   ```

   您要获取相关信息的实例的名称在哪里*my-instance*。

   将会看到类似下面的输出。

   ```
   {
       "accessDetails": {
           "username": "Administrator",
           "protocol": "rdp",
           "ipAddress": "12.345.678.910",
           "passwordData": {
               "ciphertext": "cipher",
               "keyPairName": "my-ohio-key"
           },
           "password": "",
           "instanceName": "2016-ohio-windows"
   ```

```
    }
}
```

4. 您可以将密文与任何可用的应用程序一起使用以解密您的密码。

使用远程桌面从 Windows 连接到 Lightsail Windows 实例

你可以使用 Windows 操作系统附带的远程桌面连接 (RDC) 客户端在 Amazon Lightsail 中连接你的 Windows 实例。RDC 要求您使用 Windows 实例的管理员用户名和密码，可以是创建实例时分配给该实例的默认密码，如果您更改了默认密码，则可以是您自己的密码。

本主题将引导您完成从 Lightsail 控制台获取默认管理员密码以及配置 RDC 以连接到您的 Windows 实例的步骤。您也可以使用浏览器从 Lightsail 控制台中连接到您的实例。有关更多信息，请参阅使用基于 Web 的 RDP 客户端连接到 Windows 实例。

为您的 Windows 实例获取默认管理员密码

完成以下步骤，为您的 Windows 实例获取默认管理员密码，这是使用 RDC 连接到实例所必需的。

> **Note**
>
> 如果您更改了默认管理员密码，则在 Lightsail 控制台中显示的您的实例的密码将不起作用。您需要记住自己的密码。没有管理员密码，您便无法使用 RDC 连接到实例。

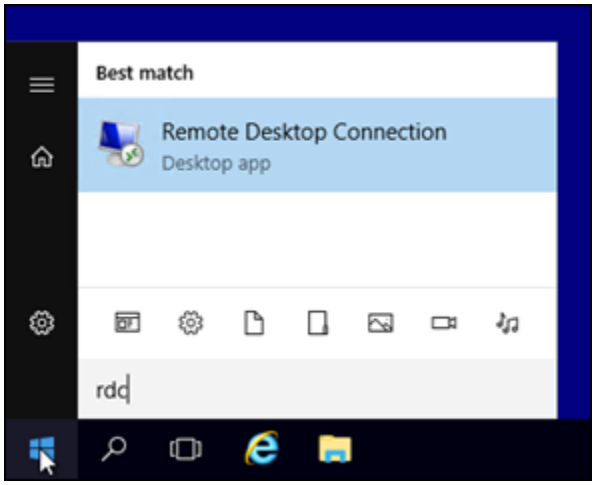
1. 登录 Lightsail 控制台。
2. 选择要连接的 Windows 实例。
3. 在实例管理页面的 Connect (连接) 选项卡中，选择 Show default password (显示默认密码)。
4. 突出显示所显示的默认密码，然后按下 Ctrl+C 或 Cmd+C 复制。现在密码将已复制到剪贴板中。

   继续阅读本指南的下一部分，以配置 RDC，并将密码粘贴到客户端中。

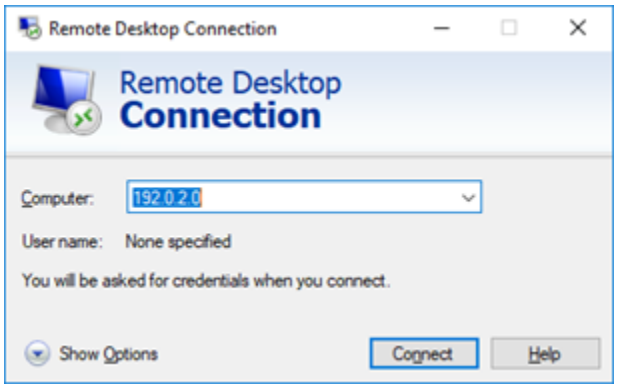
配置 RDC 并连接到您的 Windows 实例

完成以下步骤来配置 RDC 并连接到您的 Windows 实例。

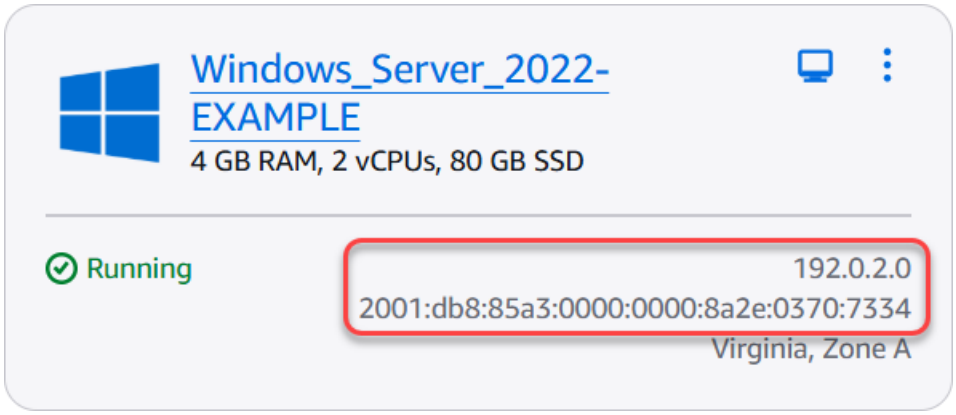
1. 打开 Windows 菜单，然后搜索 `Remote Desktop Connection` 或 RDC。
2. 在搜索结果中选择 Remote Desktop Connection (远程桌面连接)。



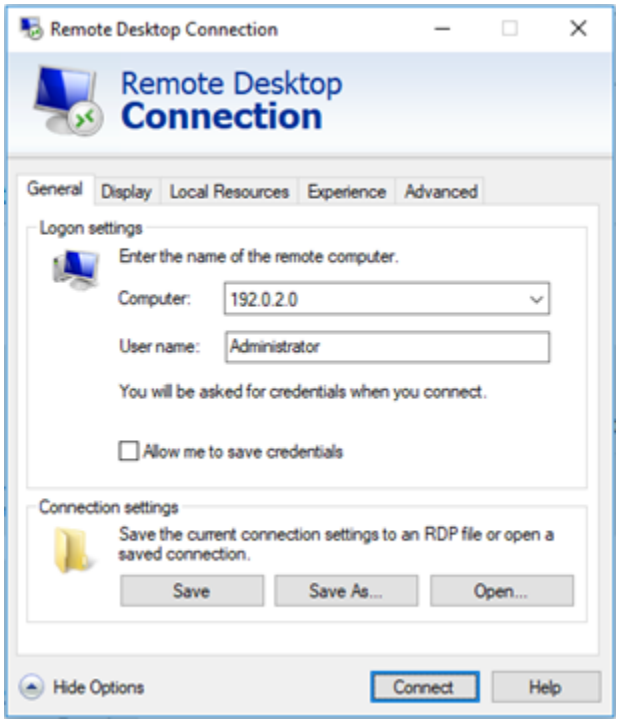
3. 在 Computer（电脑）文本框中，输入您的 Windows 实例的公有 IP 地址。



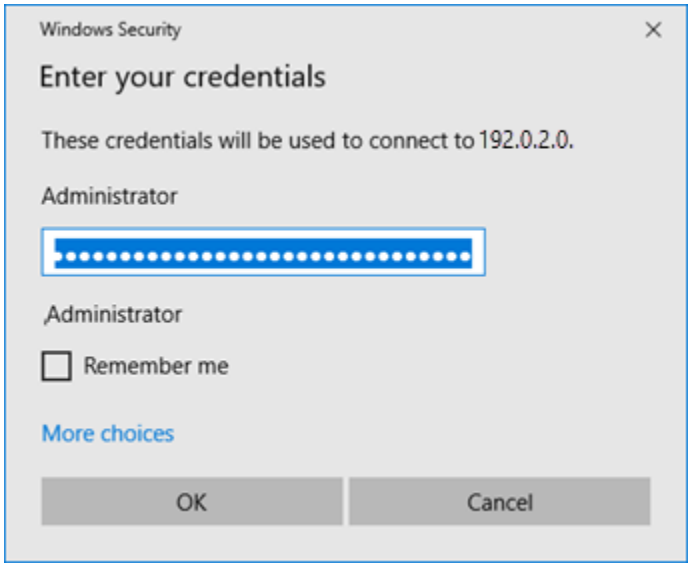
在 Lightsail 控制台中，公有 IP 显示在您的实例旁边，如以下示例所示：



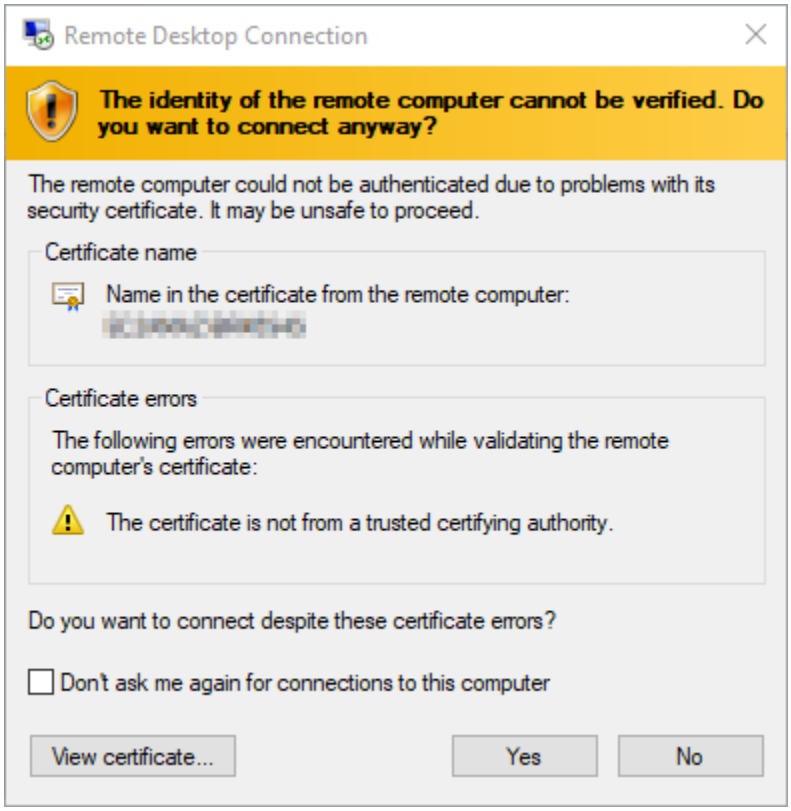
4. 选择 Show Options (显示选项) 以查看更多连接选项。
5. 在用户名文本框中输入`Administrator`，这是 Lightsail 中所有 Windows 实例的默认用户名。



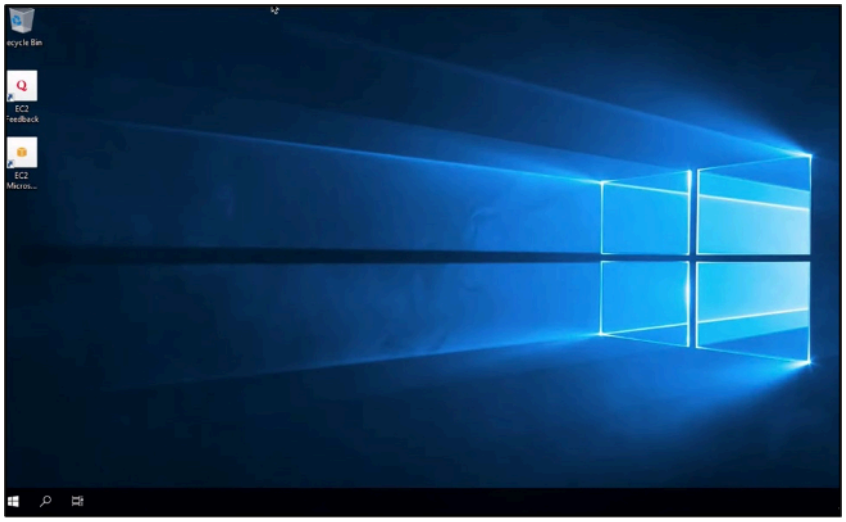
6. 选择连接。
7. 在出现的提示中，输入或粘贴您在本过程之前从 Lightsail 控制台复制的默认管理员密码，然后选择 “确定”。



8. 在出现的提示中，选择 Yes (是) 以连接到 Windows 实例（尽管出现证书错误）。



连接到该实例后，您应该能看到类似以下示例的屏幕：



使用远程桌面从 macOS 连接到 Lightsail Windows 实例

您可以使用 Microsoft 远程桌面客户端从 macOS 电脑连接到您的 Windows 实例。微软远程桌面要求你使用你的 Lightsail Windows 实例的管理员用户名和密码。这可以是创建实例时分配给该实例的默认密码，也可以是您自己的密码（如果您更改了默认密码）。

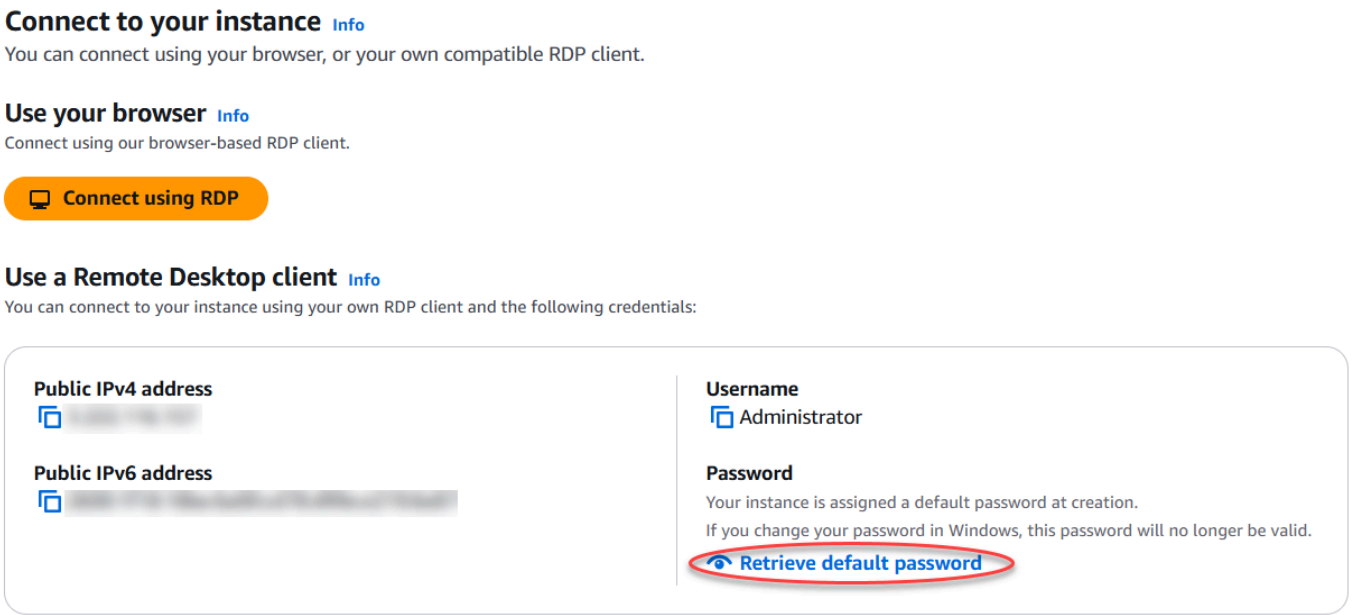
本主题将引导你完成从 Lightsail 控制台获取默认管理员密码以及配置 Microsoft 远程桌面以连接到你的 Windows 实例的步骤。您也可以使用浏览器从 Lightsail 控制台中连接到您的实例。有关更多信息，请参阅使用 Microsoft 远程桌面客户端连接到 Windows 实例。

获取 Windows 实例需要的连接信息

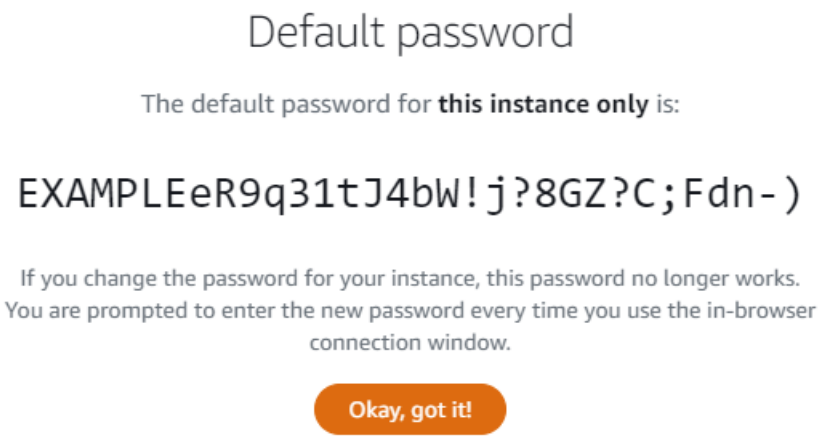
您需要 Windows 实例的公有 IP 地址、用户名和管理员密码才能使用 Microsoft 远程桌面客户端连接到该实例。

完成以下过程以获取所需的信息。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上选择 “实例” 部分。
3. 记下要连接到的实例的公有 IP 地址。
4. 选择您要连接的实例的名称。
5. 选择 Connect（连接）选项卡。
6. 选择 Show default password（显示默认密码）以获取实例的 Windows 管理员密码。



提示框将显示您的 Windows 实例的默认管理员密码。

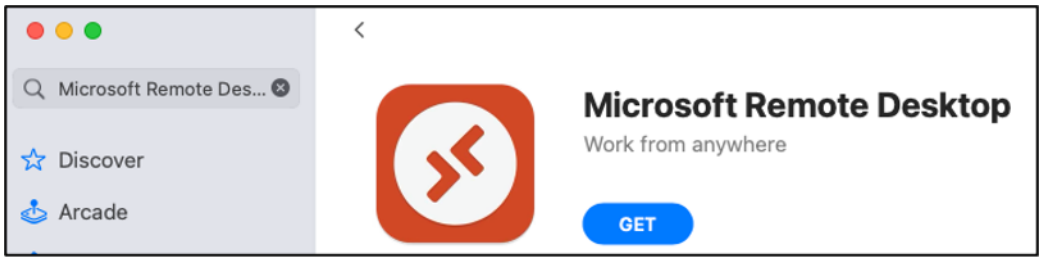


7. 复制该管理员密码。在本指南后面部分，您将使用它通过 Microsoft 远程桌面客户端登录实例。

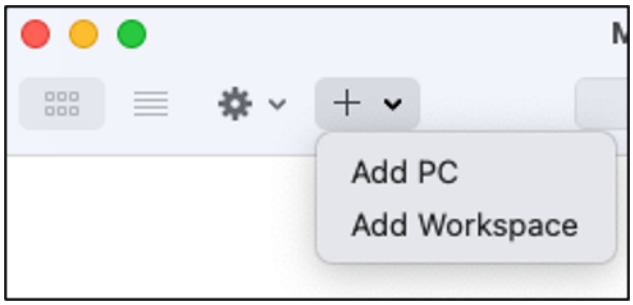
配置 Microsoft 远程桌面并连接到实例

完成以下过程以在 Mac 电脑上安装 Microsoft 远程桌面客户端，然后对其配置以连接到实例。

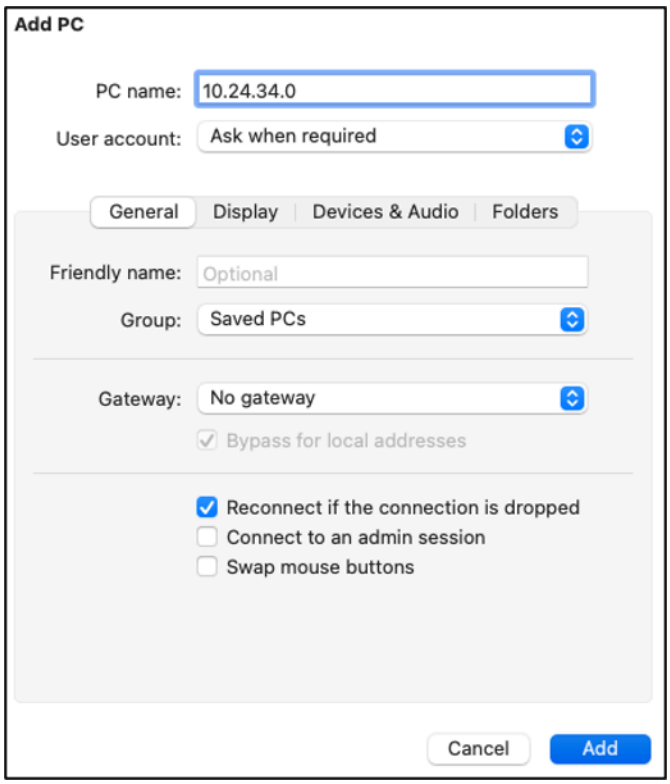
1. 在 Mac 电脑上打开 App Store，然后搜索 Microsoft Remote Desktop（Microsoft 远程桌面）。
2. 在搜索结果中查找 Microsoft Remote Desktop（Microsoft 远程桌面）应用程序，然后选择 GET（获取）以安装该应用程序。



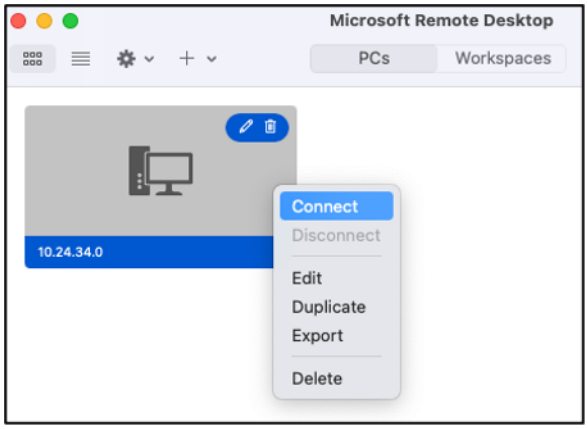
3. 完成安装后打开 Microsoft Remote Desktop（Microsoft 远程桌面）。
4. 选择顶部的加号（+）图标，然后选择添加 PC。



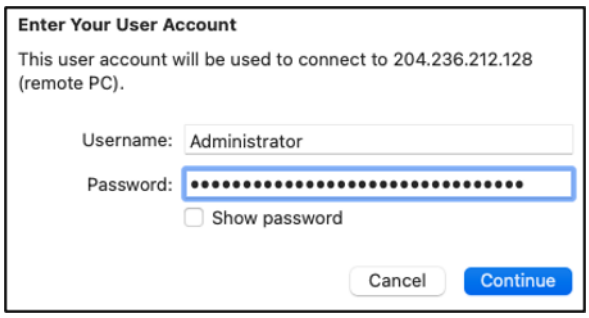
5. 在 PC name（PC 名称）文本框中，粘贴实例的公有 IP 地址。
6. 选择 添加。



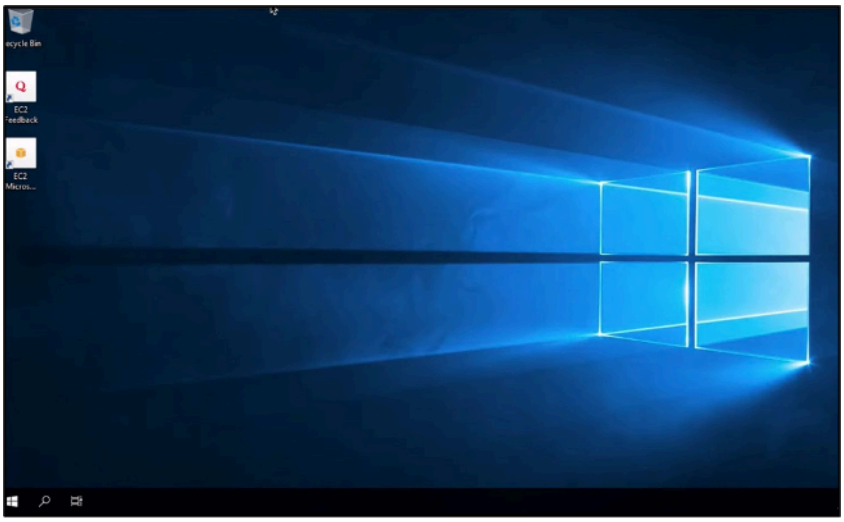
7. 右键单击实例的图标，然后选择 Connect（连接）。



8. 在用户名文本框中输入 Administrator，然后在密码文本框中输入您在本指南的前面获得的默认管理员密码。
9. 选择 Continue（继续）以连接到实例。



你现在已连接到 Lightsail Windows 实例。



在 Lightsail 中访问实例元数据服务 (IMDS) 和用户数据

实例元数据 是有关您的实例的数据，可以用来配置或管理正在运行的实例。实例元数据分为几类，例如，主机名、事件和安全组。您也可以使用实例元数据访问您启动实例时指定的用户数据。例如，您可以指定参数以配置实例，或者包含简单的脚本。实例还可包括动态数据，例如启动实例时生成的实例身份文档。

> **Important**
>
> 虽然您只能从实例本身中访问实例元数据和用户数据，但并未使用身份验证或加密方法对数据进行保护。任何可以直接访问实例的人以及可能在实例上运行的任何软件都可以查看其元数据。因此，您不应将敏感数据（例如密码或长期保存的加密密钥）存储为用户数据。

使用实例元数据服务

您可以使用以下方法之一从 Lightsail 中正在运行的实例访问实例元数据：

- 实例元数据服务版本 1 (IMDSv1)-一种请求/响应方法
- 实例元数据服务版本 2 (IMDSv2)-一种面向会话的方法

> **Important**
>
> 不是 Light IMDSv2 sail 中的所有实例蓝图都支持。使用`MetadataNoToken`实例指标来跟踪正在使用的对实例元数据服务的调用次数 IMDSv1。有关更多信息，请参阅查看实例指标。

有关使用 IMDS 的更多信息，请参阅配置实例元数据服务（IMDS）。

其他 IMDS 文档

以下 IMDS 文档在《Amazon Elastic Compute Cloud 用户指南（适用于 Linux 实例）》和《Amazon Elastic Compute Cloud 用户指南（适用于 Windows 实例）》中提供：

> **Note**
>
> 在亚马逊中 EC2，实例蓝图被称为亚马逊机器映像 (AMIs)。

- 对于 Linux 实例：
  - 配置实例元数据选项
  - 检索实例元数据
  - 处理实例用户数据
  - 检索动态数据
  - 实例元数据类别
  - 示例：AMI 启动索引值
  - 实例身份文档
- 对于 Windows 实例：
  - 配置实例元数据选项
  - 检索实例元数据

- 处理实例用户数据
- 检索动态数据
- 实例元数据类别
- 示例：AMI 启动索引值
- 实例身份文档

在 Lightsail 上访问和配置实例元数据服务 (IMDS)

您可以使用以下其中一种方法，从正在运行的实例中访问实例元数据：

- 实例元数据服务版本 1 (IMDSv1)-一种请求/响应方法
- 实例元数据服务版本 2 (IMDSv2)-一种面向会话的方法

> **Important**
>
> 不是 Light IMDSv2 sail 中的所有实例蓝图都支持。使用`MetadataNoToken`实例指标来跟踪正在使用的对实例元数据服务的调用次数 IMDSv1。有关更多信息，请参阅查看实例指标。

默认情况下，您可以使用 IMDSv1 或 IMDSv2，或两者兼而有之。实例元数据服务根据任何给定 IMDSv2 请求中是否存在唯一的`PUT`或`GET`标头来 IMDSv2区分 IMDSv1 和请求。有关更多信息，请参阅通过增强实例元数据服务，进一步增强针对开放防火墙、反向代理和 SSRF 漏洞的防御。 EC2

您可以在每个实例上配置实例元数据服务，以便本地代码或用户必须使用 IMDSv2。当您指定 IMDSv2 必须使用时，将 IMDSv1 不再起作用。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南（适用于 Linux 实例）》中的配置实例元数据选项。

要检索实例元数据，请参阅《Amazon Elastic Compute Cloud 用户指南（适用于 Linux 实例）》中的检索实例元数据。

> **Note**
>
> 本节中的示例使用实例元数据服务 IPv4 的地址:`169.254.169.254`. 如果您要通过 IPv6 地址检索实例的实例元数据，请务必启用并改用该 IPv6 地址：`fd00:ec2::254`。实例元数据服务 IPv6 的地址与 IMDSv2命令兼容。

实例元数据服务版本 2 的工作原理

IMDSv2 使用面向会话的请求。对于面向会话的请求，您创建一个会话令牌以定义会话持续时间，该时间最少为 1 秒，最多为 6 小时。在指定的持续时间内，您可以将相同的会话令牌用于后续请求。在指定的持续时间到期后，您必须创建新的会话令牌以用于将来的请求。

> **Important**
>
> 默认情况下，从亚马逊 Linux 2023 和 Ubuntu 24 蓝图启动的 Lightsail 实例将进行配置。IMDSv2

以下示例使用 Linux 和 PowerShell shell 脚本 IMDSv2 来检索顶级实例元数据项。这些示例执行以下操作：

- 使用 PUT 请求创建持续 6 小时（21600 秒）的会话令牌
- 将会话令牌标头存储在名为 `TOKEN`（在 Linux 上）或 `token`（在 Windows 上）的变量中
- 使用令牌请求顶级元数据项

通过运行以下命令开始：

- 在 Linux 上：
  - 首先，使用以下命令生成令牌。

    ```
    [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
    ```

  - 然后，通过令牌使用以下命令生成顶级元数据项。

    ```
    [ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
    ```

- 在 Windows 上：
  - 首先，使用以下命令生成令牌。

    ```
    PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
    ```

  - 然后，通过令牌使用以下命令生成顶级元数据项。

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
```

创建令牌后，您可以重复使用令牌，直到令牌过期。在以下示例中，每个命令都会获取用于启动实例的蓝图（亚马逊云机器镜像（AMI））的 ID。上一个示例中的令牌可以重复使用。该令牌存储在 $TOKEN（在 Linux 上）或 $token（在 Windows 上）中。

- 在 Linux 上：

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/ami-id
```

- 在 Windows 上：

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
-Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

当您使用 IMDSv2 请求实例元数据时，请求必须包含以下内容：

- **PUT** 请求 – 使用 PUT 请求可启动到实例元数据服务的会话。PUT 请求返回一个令牌，该令牌必须包含在对实例元数据服务的后续 GET 请求中。使用时需要使用令牌才能访问元数据 IMDSv2。
- 令牌 – 将该令牌包含在对实例元数据服务的所有 GET 请求中。如果将令牌使用设置为 `required`，没有有效令牌或令牌过期的请求将显示 `401 - Unauthorized` HTTP 错误代码。有关更改令牌使用要求的信息，请参阅《AWS CLI 命令参考》update-instance-metadata-options中的。
  - 令牌是实例特定的密钥。令牌在其他实例上无效，如果尝试在生成令牌的实例外部使用，令牌将会被拒绝。
  - PUT 请求必须包含一个标头，它以秒为单位指定令牌的生存时间（TTL）。TTL 最多可以指定为 6 小时（21600 秒）。令牌表示一个逻辑会话。TTL 指定令牌的有效时间长度，因而指定会话的持续时间。
  - 在令牌过期后，要继续访问实例元数据，您必须使用另一个 PUT 请求创建新会话。
  - 您可以选择在每个请求中重复使用令牌或创建新的令牌。对于少量请求，在每次需要访问实例元数据服务时生成并立即使用令牌可能更方便。但为了提高效率，您可以为令牌指定更长的持续时间并重复使用令牌，而不是在每次需要请求实例元数据时都编写 PUT 请求。并发令牌的数量没有实际限制，每个令牌代表自己的会话。 IMDSv2 但是，仍受普通实例元数据服务连接和限制的限

制。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南（适用于 Linux 实例）》中的查询限制。

允许在 IMDSv2 实例元数据请求中使用 HTTP GET 和 HEAD 方法。如果 PUT 请求包含 X-Forwarded-For 标头，则会被拒绝。

默认情况下，PUT 请求的响应在 IP 协议级别的响应跃点数限制（生存时间）为 1。如果需要更大的跃点数限制，您可以使用 update-instance-metadata-options 命令进行调整。例如，您可能需要使用更大的跃点数限制，以便与实例上运行的容器服务保持向后兼容。有关更多信息，请参阅 AWS CLI 命令参考 中的 update-instance-metadata-options。

转换为使用 实例元数据服务版本 2

使用实例元数据服务版本 2 (IMDSv2) 是可选的。将继续无限期地支持实例元数据服务版本 1 (IMDSv1)。如果您选择迁移到使用 IMDSv2，我们建议您使用以下工具和过渡路径。

帮助转换为 IMDSv2 的工具

如果您的软件使用 IMDSv1，请使用以下工具来帮助重新配置要使用的 IMDSv2软件。

- AWS 软件： AWS SDKs 和 AWS CLI 支持的最新版本 IMDSv2。要使用 IMDSv2，请确保您的实例具有 AWS SDKs 和的最新版本 AWS CLI。有关更新的信息 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS CLI中的安装、更新和卸载。所有亚马逊 Linux 2 软件包都支持 IMDSv2。
- 实例指标： IMDSv2 使用令牌支持的会话，但 IMDSv1 不使用。MetadataNoToken实例指标跟踪正在使用的对实例元数据服务的调用次数 IMDSv1。通过查看该指标是否为零，您可以确定是否以及何时将所有软件升级为使用 IMDSv2。有关更多信息，请参阅在 Amazon Lightsail 中查看实例指标。
- 对 Lightsail API 操作和 AWS CLI 命令的更新：对于现有实例，您可以使用update-instance-metadata-options AWS CLI 命令（或 UpdateInstanceMetadataOptionsAPI 操作）来要求使用。IMDSv2以下命令是一个示例。请务必*InstanceName*替换为实例的名称，并*RegionName*替换为实例 AWS 区域 所在的名称。

```
aws lightsail update-instance-metadata-options --region RegionName --instance-
name InstanceName --http-tokens required
```

要求 IMDSv2 访问的建议途径

在使用上述工具时，我们建议您按照以下途径转换为 IMDSv2：

步骤 1：在开始时

将 AWS SDKs您的实例上使用角色凭证的 AWS CLI、和您的软件更新为 IMDSv2兼容版本。有关更新的信息 AWS CLI，请参阅AWS Command Line Interface 用户指南 AWS CLI中的升级到最新版本的。

然后，使用 IMDSv2 请求更改直接访问实例元数据（换句话说，不使用 S AWS DK）的软件。

步骤 2：在转换期间

使用实例指标 `MetadataNoToken` 跟踪您的转换进度。该指标显示您的实例上使用的对实例元数据服务的调用 IMDSv1 次数。有关更多信息，请参阅查看实例指标。

步骤 3：在所有实例上一切准备就绪时

当实例指标`MetadataNoToken`记录的 IMDSv1 使用率为零时，所有实例都已准备就绪。在此阶段，您可以通过update-instance-metadata-options命令要求 IMDSv2 使用。您可以在正在运行的实例上进行这些更改，而无需重新启动实例。

更新现有实例的实例元数据选项只能通过 Lightsail API 或。 AWS CLI它目前在 Lightsail 控制台中不可用。有关更多信息，请参阅 update-instance-metadata-options。

其他 IMDS 文档

以下 IMDS 文档在《Amazon Elastic Compute Cloud 用户指南（适用于 Linux 实例）》和《Amazon Elastic Compute Cloud 用户指南（适用于 Windows 实例）》中提供：

> **Note**
>
> 在亚马逊中 EC2，实例蓝图被称为亚马逊机器映像 (AMIs)。

- 对于 Linux 实例：
  - 配置实例元数据选项
  - 检索实例元数据
  - 处理实例用户数据
  - 检索动态数据
  - 实例元数据类别
  - 示例：AMI 启动索引值
  - 实例身份文档

- 对于 Windows 实例：
  - 配置实例元数据选项
  - 检索实例元数据
  - 处理实例用户数据
  - 检索动态数据
  - 实例元数据类别
  - 示例：AMI 启动索引值
  - 实例身份文档

使用 Lightsail 块存储磁盘扩展存储空间和性能

系统磁盘提供运行您的工作负载所需的一致的低延迟性能。借助 Lightsail 磁盘，您可以在几分钟内扩大或缩小使用量，并且只需为预配置的内容支付低廉的价格。

您可以在基于 Linux/Unix 或 Windows Server 的实例上选择最多 80 GB 系统磁盘。请参阅 L ightsail 中基于 Linux 的实例入门或开始使用基于 Windows 服务器的实例。

您还可以创建额外的数据块存储磁盘，以便在虚拟私有服务器中添加更多存储。请参阅 Create and attach block storage disks to your Linux-based instance，或 Create and attach block storage disks to your Windows Server instance。

数据块存储磁盘

数据块存储是将数据作为“块”进行管理的存储架构。每个存储块（在 Lightsail 中称为 “磁盘”）就像一个单独的硬盘，您可以将其连接到服务器。通常，您可以将额外的数据块存储用于必须将特定数据与其核心服务分开的应用程序或软件，以及保护应用程序数据以防止实例和启动存储磁盘发生故障或出现其他问题。

Lightsail 提供用于块存储的固态硬盘 (SSD)。这种类型的数据块存储兼具合理的价格和良好的性能。它旨在支持在 Lightsail 上运行的绝大多数工作负载。Lightsail 额外的块存储磁盘可提供稳定的性能和频繁访问存储数据的应用程序或软件所需的低延迟。

> **Note**
>
> 对于需要持续 IOPS 性能或每个磁盘高吞吐量的应用程序的客户，或者运行大型数据库（如 MongoDB、Cassandra 等）的客户，我们建议将 EC2 亚马逊 GP2 与预配置 IOPS 固态硬盘存储一起使用或预配置 IOPS 固态硬盘存储来代替 Lightsail。

您可以在亚马逊 EC2 用户指南中了解有关 Amazon EBS 卷的更多信息。

磁盘配额

- 每个区域 20,000 GB。
- 每个磁盘最大 16 TB，或每个磁盘最小 8 GB。
- 每个实例可以有最多 15 个附加磁盘和 1 个启动卷磁盘。

创建 Lightsail 块存储磁盘并将其连接到 Linux 实例

您可以为您的 Amazon Lightsail 实例创建和附加额外的块存储磁盘。创建其他磁盘后，您需要连接到基于 Linux/UNIX 的 Lightsail 实例，然后格式化并装载该磁盘。

本主题向您展示如何使用 Lightsail 创建新磁盘并连接该磁盘。它还介绍了如何使用 SSH 连接到基于 Linux/Unix 的实例，以便格式化并装载连接的磁盘。

如果您拥有基于 Windows Server 的实例，请改为参阅以下主题：创建数据块存储磁盘并将其附加到 Windows Server 实例。

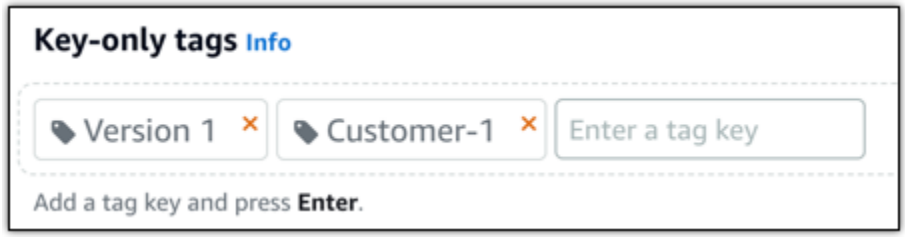
步骤 1：创建新磁盘并将其连接到您的实例

1. 在左侧导航窗格中，选择存储。
2. 选择创建磁盘。
3. 选择您的 Lightsail 实例所在的 AWS 区域 和可用区。
4. 选择一种大小。
5. 输入磁盘的名称。

   资源名称：

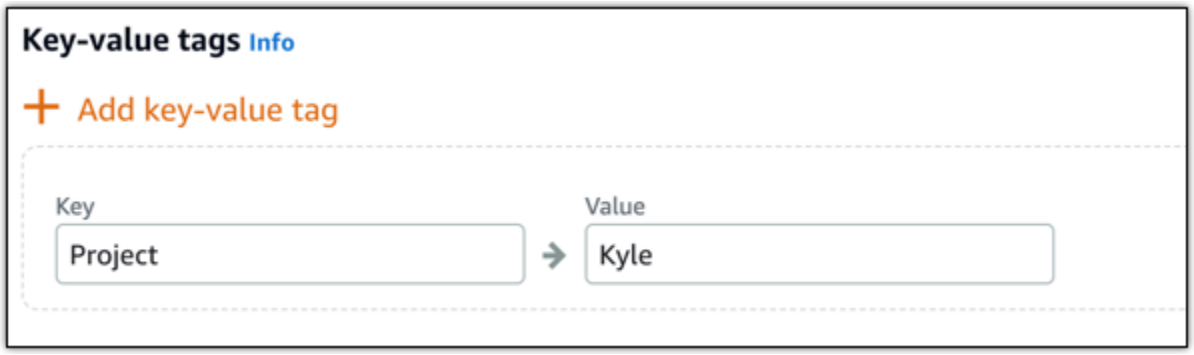
   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
6. 选择以下选项之一以将标签添加到磁盘：

   - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

   - 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。



> **Note**
>
> 有关“仅键”标签和键值标签的更多信息，请参阅标签。

7. 选择 Create disk（创建磁盘）。

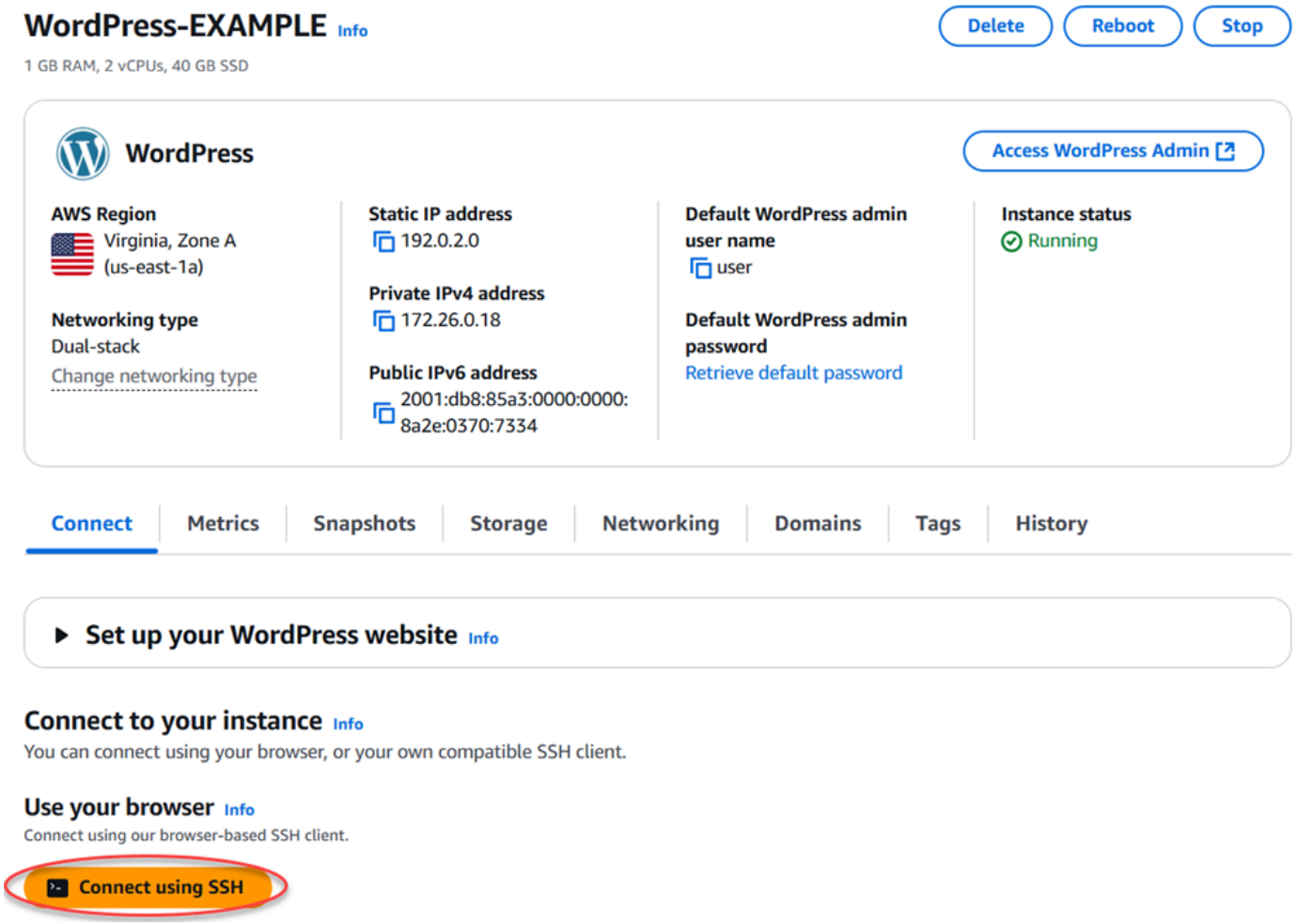
   在几秒钟后，将创建您的磁盘，并显示新的磁盘管理页面。

8. 从列表中选择您的实例，然后选择 Attach（连接）以将新磁盘连接到您的实例。

步骤 2：连接到您的实例以格式化并装载磁盘

1. 创建并连接磁盘后，返回 Lightsail 中的实例管理页面。

   默认情况下，将显示 Connect（连接）选项卡。



2. 选择 Connect using SSH（使用 SSH 连接）以连接到您的实例。
3. 在终端窗口中输入以下命令：

```
lsblk
```

`lsblk` 的输出从磁盘路径中忽略 `/dev/` 前缀。

> **Note**
>
> 2023 年 6 月 29 日，我们更新了 Lightsail 实例的基础硬件。在以下示例中，上一代实例的设备名称显示为 `/dev/xvda`。在此日期之后创建的实例的设备名称显示为 `/dev/nvme0n1`。

Current generation instances

在以下示例输出中，根卷（nvme0n1）有两个分区（nvme0n1p1 和 nvme0n1p128），而额外的卷（nvme1n1）没有分区。

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0   8G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Previous generation instances

在以下示例输出中，根卷（xvda）有一个分区（xvda1），而额外的卷（xvdf）没有分区。

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0   8G  0 part /
xvdf    202:80   0  24G  0 disk
```

4. 确定是否在磁盘上创建文件系统。新磁盘为原始块存储设备，您必须在这些设备上创建文件系统，然后才能装载并使用这些设备。在通过快照还原的磁盘上可能已具有文件系统。如果在现有的文件系统上创建新的文件系统，该操作将覆盖您的数据。

   使用以下方法来确定您的磁盘是否有文件系统。如果您的磁盘没有文件系统，请继续执行步骤 2.5。如果您的磁盘确实有文件系统，请跳至步骤 2.6。

   Current generation instances

   ```
   sudo file -s /dev/nvme1n1
   ```

   将会在全新的磁盘上看到以下输出。

   ```
   /dev/nvme1n1: data
   ```

   如果看到类似下面的输出，这意味着您的磁盘已具有文件系统。

```
/dev/nvme1n1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

Previous generation instances

```
sudo file -s /dev/xvdf
```

将会在全新的磁盘上看到以下输出。

```
/dev/xvdf: data
```

如果看到类似下面的输出，这意味着您的磁盘已具有文件系统。

```
/dev/xvda1: Linux rev 1.0 ext4 filesystem data, UUID=1701d228-e1bd-4094-
a14c-12345EXAMPLE (needs journal recovery) (extents) (large files) (huge files)
```

5. 可以使用以下命令在磁盘上创建新的文件系统。用设备名称（例如/dev/nvme1n1）代替*device_name*。根据应用程序要求或操作系统限制，您可以选择不同的文件系统类型，如 ext3 或 ext4。

> **Important**
>
> 该步骤假定您装载的是空磁盘。如果在要装载的磁盘上已具有数据（例如，通过快照还原的磁盘），请在装载该磁盘之前不要使用 mkfs。而是跳到步骤 2.6 并创建一个挂载点。否则，将会格式化磁盘并删除现有的数据。

Current generation instances

```
sudo mkfs -t xfs device_name
```

将会看到类似下面的输出。

```
meta-data=/dev/nvme1n1           isize=512    agcount=16, agsize=1048576 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=1 inobtcount=1
data     =                       bsize=4096   blocks=16777216, imaxpct=25
         =                       sunit=1      swidth=1 blks
```

```
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=16384, version=2
         =                       sectsz=512   sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Previous generation instances

```
sudo mkfs -t ext4 device_name
```

您应看到类似下面的输出。

```
mke2fs 1.42.9 (4-Feb-2014)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
4194304 inodes, 16777216 blocks
838860 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
512 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
4096000, 7962624, 11239424

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

6. 可以使用以下命令创建磁盘的装载点目录。装载点是磁盘在文件系统树中的位置，以及在装载磁盘后读写文件的位置。将位置替换为未使用的空间，例如/data。*mount_point*

```
sudo mkdir mount_point
```

7. 您可以输入以下命令，以验证在磁盘上现在是否具有文件系统。

Current generation instances

```
sudo file -s /dev/nvme1n1
```

将会看到类似下面的输出，而不是 /dev/nvme1n1: data。

```
/dev/nvme1n1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

Previous generation instances

```
sudo file -s /dev/xvdf
```

将会看到类似下面的输出，而不是 /dev/xvdf: data。

```
/dev/xvdf: Linux rev 1.0 ext4 filesystem data, UUID=0ee83fdf-e370-442e-
ae38-12345EXAMPLE (extents) (large files) (huge files)
```

8. 最后，键入以下命令以挂载磁盘。

```
sudo mount device_name mount_point
```

检查新磁盘装载的文件权限，以确保您的用户和应用程序可以在该磁盘中写入数据。有关文件权限的更多信息，请参阅《亚马逊 EC2 用户指南》中的 “让 Amazon EBS 卷可供使用”。

步骤 3：每次重启您的实例时装载磁盘

每次重启 Lightsail 实例时，你可能都想挂载这张磁盘。如果不希望这样做，则该步骤是可选的。

1. 要在每次系统重启时装载该磁盘，请在 /etc/fstab 文件中为该设备添加一个条目。

   创建 /etc/fstab 文件的备份，以便在编辑时误损坏或删除该文件时使用。

   ```
   sudo cp /etc/fstab /etc/fstab.orig
   ```

2. 使用任何文本编辑器（如 vim）打开 /etc/fstab 文件。

   您必须在打开该文件之前输入 sudo，以便保存更改。

3. 在该文件末尾，使用以下格式为磁盘添加一个新行。

```
device_name  mount_point  file_system_type  fs_mntops  fs_freq  fs_passno
```

例如，新行可能如下所示。

Current generation instances

```
/dev/nvme1n1 /data xfs defaults,nofail 0 2
```

Previous generation instances

```
/dev/xvdf /data ext4 defaults,nofail 0 2
```

4. 保存文件并退出文本编辑器。

创建 Lightsail 块存储磁盘并将其连接到 Windows 服务器实例

如果您需要额外的存储空间，可以在 Amazon Lightsail 中创建块存储磁盘并将其连接到您的 Windows 服务器实例。有关数据块存储磁盘的更多信息，请参阅数据块存储磁盘。

本指南向您展示如何使用 Lightsail 控制台创建新的块存储磁盘并将其连接到您的 Windows Server 实例。它还介绍了如何使用 RDP 连接到 Windows Server 实例以便将磁盘联机和初始化。

> **Note**
>
> 如果您拥有 Linux 或 Unix 实例，请参阅创建磁盘并将其附加到 Linux 或 Unix 实例。

步骤 1：创建新的数据块存储磁盘并将其连接到您的实例

使用 Amazon Lightsail 控制台创建新的块存储磁盘并将其连接到您的实例。

创建新的数据块存储磁盘并将其连接到您的实例

1. 登录 Lightsail 控制台。
2. 选择 Storage（存储）选项卡，然后选择 Create disk（创建磁盘）。
3. 选择您的 Lightsail 实例所在的 AWS 区域 和可用区。
4. 选择磁盘大小。

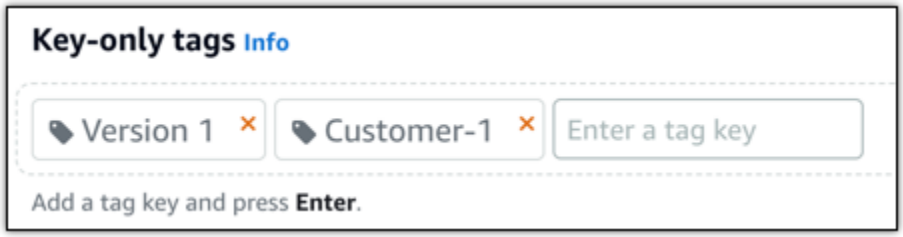
5. 为存储磁盘输入名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

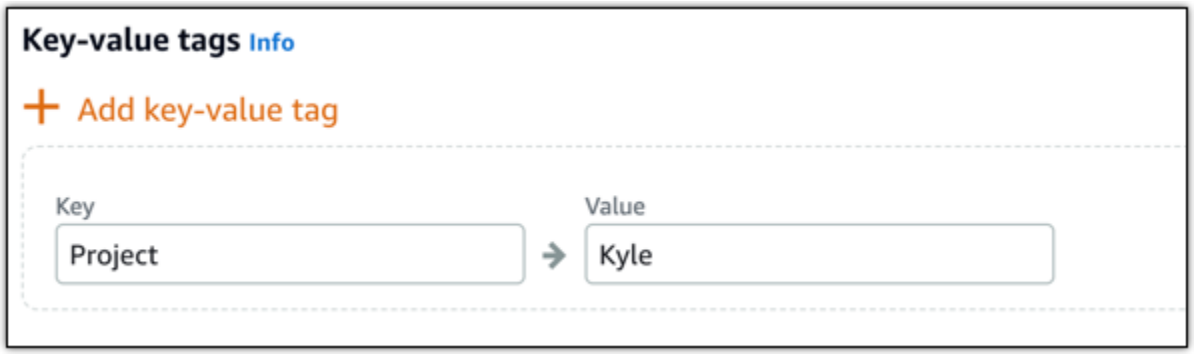
6. 选择以下选项之一以将标签添加到磁盘：

   - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

   - 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

     一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。

   > **Note**
   >
   > 有关“仅键”标签和键值标签的更多信息，请参阅标签。

7. 选择 Create disk（创建磁盘）。

在几秒钟后，将创建磁盘，并且您可以在磁盘管理页面中查看有关磁盘的信息。

8. 从列表中选择您的实例，然后选择 Attach（连接）以将新磁盘连接到您的实例。



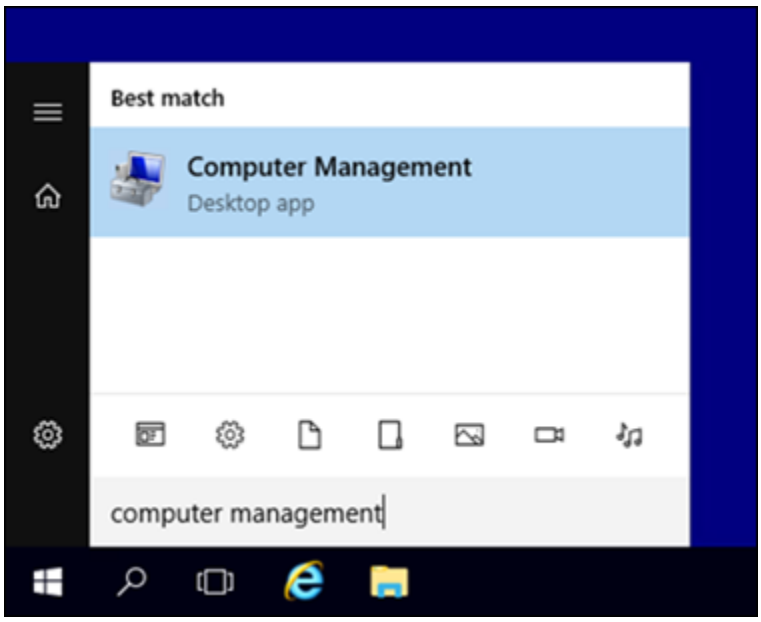
继续执行本指南的步骤 2：连接到您的实例并将数据块存储磁盘联机部分，使数据块存储磁盘联机。

步骤 2：连接到您的实例并将数据块存储磁盘联机

连接到 Windows Server 实例并使用磁盘管理实用工具将最近连接的数据块存储磁盘联机。

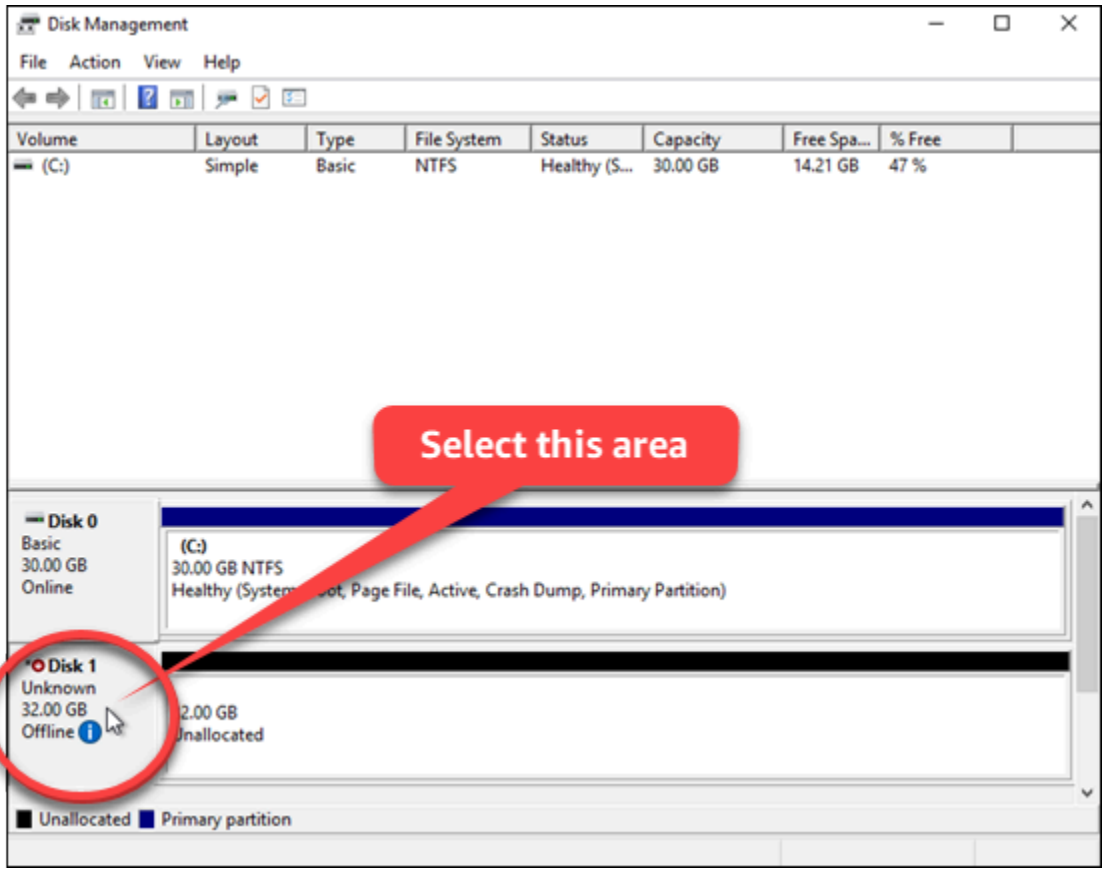
连接到您的实例并将数据块存储磁盘联机

1. 导航到 Lightsail 主机主页。
2. 选择要将本指南中前面提到的额外存储磁盘连接到的实例的名称。
3. 在 Connect（连接）选项卡下，选择 Connect using RDP（使用 RDP 连接）。
4. 在 Windows 的开始菜单中，搜索 Computer Management（计算机管理），然后在搜索结果中选择 Computer Management（计算机管理）。

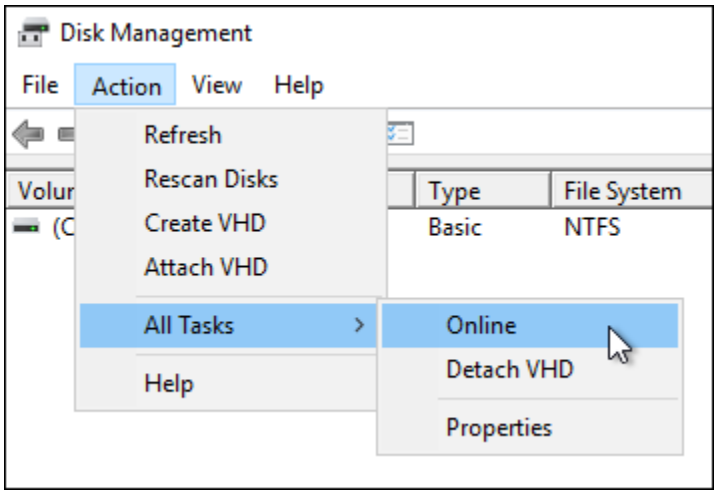


5. 在 Computer Management（计算机管理）的左侧窗格中，选择 Disk Management（磁盘管理）。

6. 在磁盘管理实用工具的底部窗格中，选择标为 Unknown / Offline（未知/脱机）的磁盘。它就是连接到本指南中前面提到的实例的数据块存储磁盘。



7. 选择相应磁盘后，在 Action（操作）菜单上，选择 All Tasks（所有任务），然后选择 Online（联机）。



您会看到相应数据块存储磁盘的状态已更新为 Not Initialized（未初始化）。数据块存储磁盘尚未联机。继续执行本指南的步骤 3：初始化数据块存储磁盘部分，以初始化数据块存储磁盘。

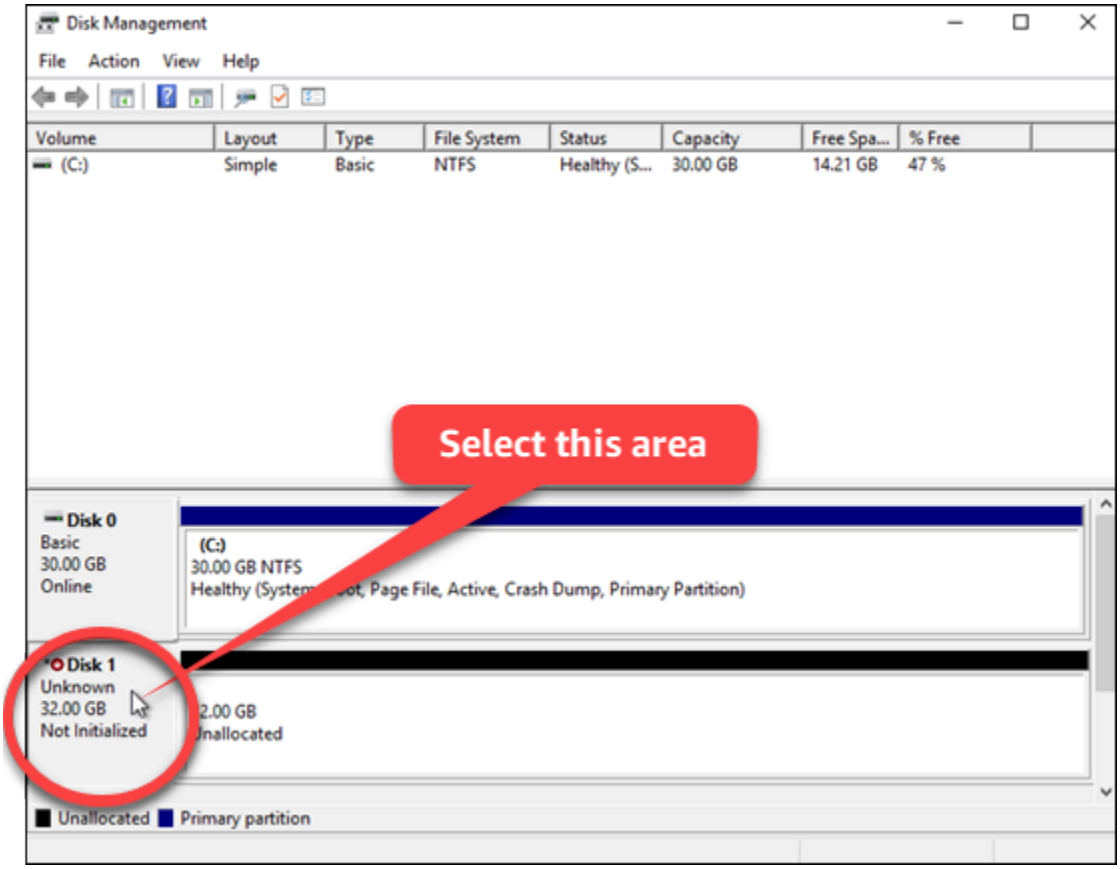
步骤 3：初始化数据块存储磁盘

初始化数据块存储磁盘，以便可将其格式化。

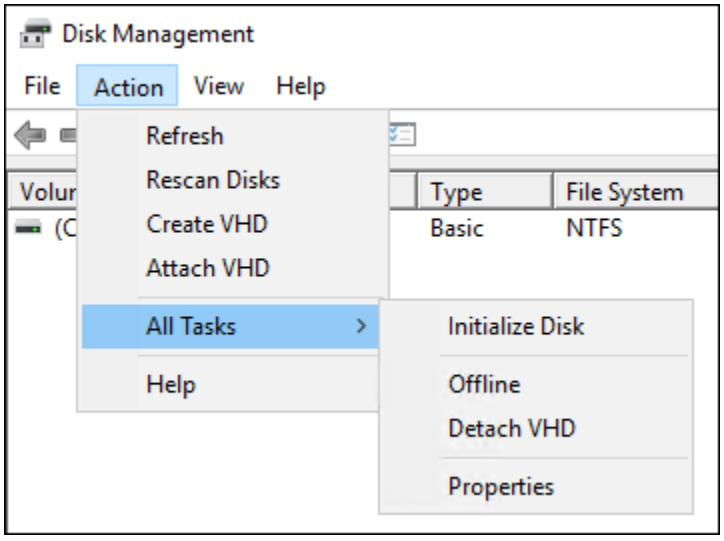
> **Important**
>
> 如果您装载的磁盘已包含数据（例如，从快照创建的磁盘），请确保不要重新格式化该磁盘并删除现有的数据。

初始化数据块存储磁盘

1. 在磁盘管理实用工具的底部窗格中，选择标为 Unknown / Not initialized（未知/未初始化）的磁盘。



2. 选择相应磁盘后，在 Action（操作）菜单上，选择 All Tasks（所有任务），然后选择 Initialize Disk（初始化磁盘）。



3. 为新磁盘选择分区格式，然后选择 OK（确定）。

> **Note**
>
> 有关分区格式的更多信息，请参阅 Microsoft 文章：关于分区格式 – GPT 和 MBR。

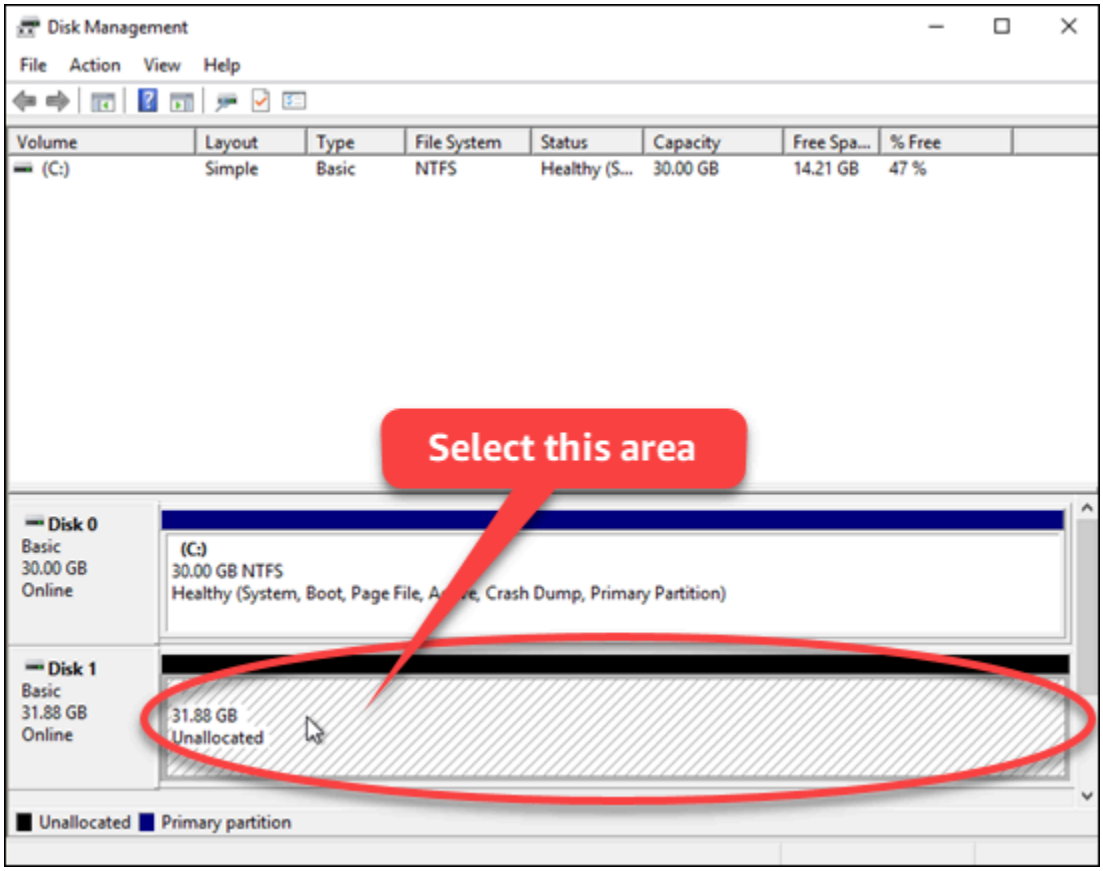
您会看到数据块存储磁盘的状态已更新为 Online（联机）。继续执行本指南的步骤 4：通过文件系统格式化磁盘部分，通过文件系统格式化数据块存储磁盘。

步骤 4：通过系统文件格式化磁盘

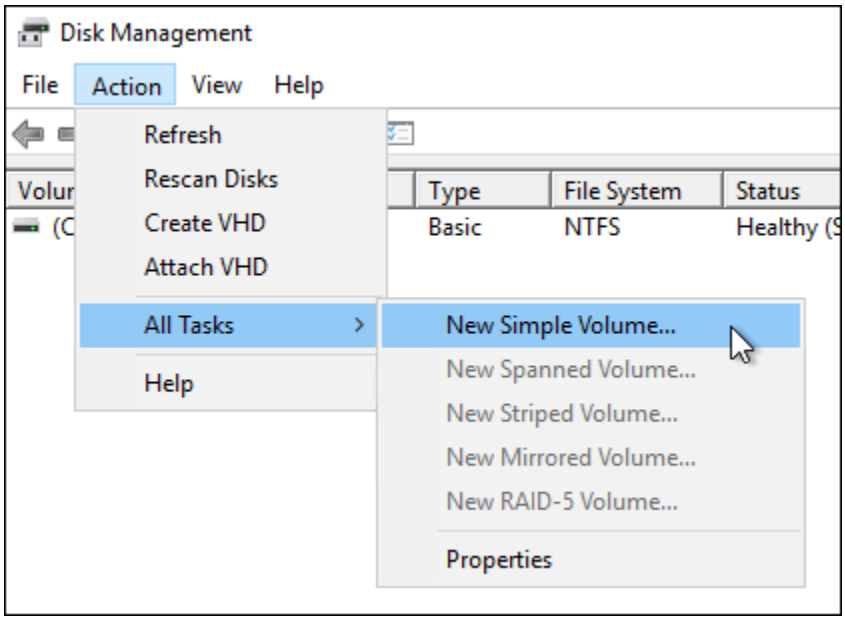
使用 Windows Server 中的 New Simple Volume（新建简单卷）向导分配驱动器号并通过文件系统格式化磁盘。

通过系统文件格式化磁盘

1. 在“磁盘管理”实用工具的底部窗格中，选择数据块存储磁盘上标为 Unallocated（未分配）的分区。



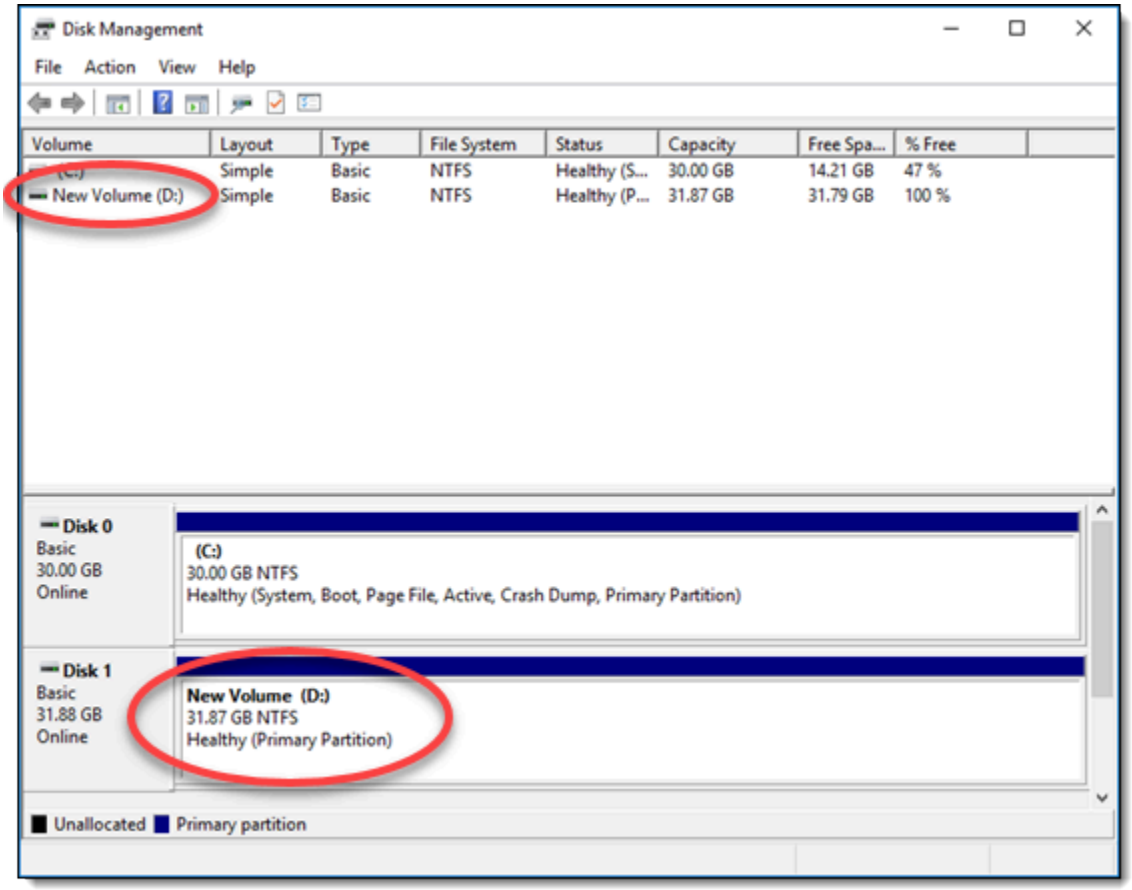
2. 选择相应分区后，在 Action（操作）菜单上，选择 All Tasks（所有任务），然后选择 New Simple Volume（新建简单卷）。



3. 按照 “新建简单卷” 向导中的说明选择 NTFS FAT32、或 reFS 文件系统类型并格式化磁盘。

> **Note**
>
> 有关这些文件系统的更多信息，请参阅 Micro soft 的 NTFS 概述、弹性文件系统 (RefS) 概述和文件系统描述文章。 FAT32

完成后，您会在磁盘管理实用工具中看到驱动器号及以下消息。



分离并删除 Lightsail 块存储磁盘

如果您不再需要块存储磁盘，可以将其与已停止的 Amazon Lightsail 实例分离，然后将其删除。本主题介绍了如何备份您的数据并安全地删除磁盘。

先决条件

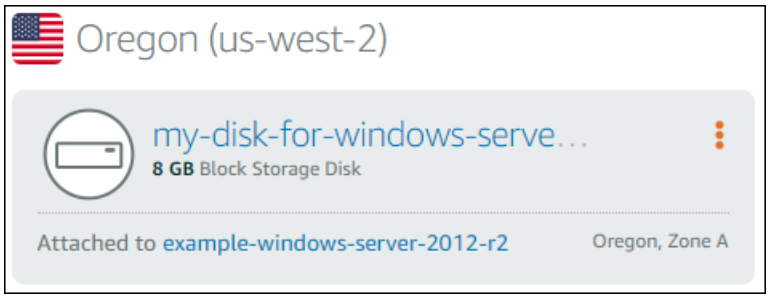
- 停止运行您的实例。您必须执行该操作，然后才能断开连接并删除您的磁盘。了解如何停止实例
- (可选) 我们建议您创建磁盘的快照。这样，您就具有一个备份，以防止您以后改变主意。有关更多信息，请参阅创建数据库的快照。

断开连接并删除您的磁盘

停止 Lightsail 实例后，您可以安全地分离和删除磁盘。

1. 在主页上，选择 Storage (存储)。

2. 选择连接的磁盘名称以对其进行管理。



3. 在磁盘管理页面上，选择 Detach (断开连接)。

   在几秒钟后，将断开连接该磁盘，可以将其删除或重新连接。

4. 选择删除选项卡。
5. 选择 Delete disk (删除磁盘)，然后选择 Yes, delete (是，删除)以进行确认。

> **Important**
>
> 这是一个永久性操作，无法撤消。在删除磁盘时，磁盘上的所有数据将会丢失。

亚马逊 Lightsail 中的快照

您可以在 Amazon Lightsail 中创建实例、数据库和块存储磁盘的 point-in-time快照，并将其用作创建新资源或进行数据备份的基准。快照包含恢复您的资源所需的所有数据（从拍摄快照的那一刻开始）。当您通过从快照中创建资源来进行恢复时，新资源作为创建快照所用原始资源的准确副本开始。无论是手动快照、自动快照、复制的快照还是系统盘快照，您都需要为自己的 Lightsail 账户中的快照支付快照存储费。如果您遇到数据损坏或磁盘故障，则可以根据拍摄的快照创建磁盘并替换旧磁盘。您还可以使用快照来配置新磁盘并在新实例启动期间连接它们。

内容

- 手动快照
- 自动快照
- 系统磁盘快照
- 根据快照创建新资源
- 复制快照
- 将快照导出到亚马逊 EC2
- 删除快照

手动快照

可以随时创建实例、托管数据库和块存储磁盘的手动快照。手动快照将无限期存储，直到删除它们为止。

有关创建手动快照的更多信息，请参阅以下指南：

- 创建 Linux 或 Unix 实例的快照
- 创建 Windows Server 实例的快照
- 创建数据库的快照
- 创建数据块存储磁盘的快照

自动快照

如果您在 Lightsail 实例或块存储磁盘上托管关键信息，则应通过创建手动快照来经常对其进行备份。但是，找到时间来执行频繁的管理任务并不总是那么容易。如果是这样，请使用自动快照让 Lightsail

代表您创建实例或块存储磁盘的每日备份，无需手动交互。将存储每日最新的七个自动快照，然后将最旧的一个替换为最新的一个。

有关自动快照的更多信息，请参阅以下指南：

- 启用或禁用自动实例快照
- 更改实例或磁盘的自动快照时间
- 删除自动快照

> **Important**
>
> 当您删除源资源时，将会删除与该资源相关联的所有自动快照。此行为与手动快照不同，手动快照即使在您删除源资源后，手动快照仍保留在您的 Lightsail 帐户中。要在删除源资源时保留自动快照，请参阅保留自动快照。

系统磁盘快照

如果您的实例无响应，并且您需要访问系统磁盘上的文件，则可以通过创建系统磁盘快照来备份实例根卷。然后，您可以通过从快照创建新块存储磁盘并将其连接到另一个实例，访问系统磁盘中的文件。有关更多信息，请参阅创建实例根卷的快照。

根据快照创建新资源

使用快照创建新的 Lightsail 资源，使用与原始资源相同的套餐或更大的套餐。使用较小的 Lightsail 套餐时，不能使用快照来创建新资源。当您基于快照创建资源时，新资源将开始作为用于创建快照的原始资源的副本。

有关更多信息，请参阅以下指南：

- 从快照创建实例
- 根据快照创建数据库
- 根据快照创建数据块存储磁盘
- 根据快照创建更大的实例、数据块存储磁盘或数据库

复制快照

实例和块存储磁盘快照可以在同一 Lightsail 账户中从一个 Amazon Web Services (AWS) 区域复制到另一个区域。数据库快照不能在区域之间复制。有关更多信息，请参阅将快照从一个复制 AWS 区域到另一个快照。

将快照导出到亚马逊 EC2

Lightsail 是最简单的入门方法。 AWS但是，Lightsail存在亚马逊 EC2 或其他 AWS 服务中不存在的限制。将您的 Lightsail 实例和块存储磁盘快照导出 EC2 到 Amazon，以利用更广泛的可用实例类型，并使用中的全方位服务。 AWS有关更多信息，请参阅将快照导出到 Amazon EC2。

> **Note**
>
> cPanel 和 WHM (CentOS 7) 实例的快照无法导出到亚马逊。 EC2

删除快照

在不再需要 Lightsail 快照时将其删除，以免产生月度快照存储费。有关更多信息，请参阅删除快照。

为 Lightsail 实例和磁盘配置自动快照

当您启用实例或块存储磁盘的自动快照功能时，Amazon Lightsail 会在默认自动快照时间或您指定的时间内为您的资源创建每日快照。就像手动快照一样，您可以使用自动快照作为基准来创建新资源或进行数据备份。

创建自动快照时，您需要为存储在您的 Lightsail 帐户中的自动快照支付快照存储费。

内容

- 自动快照限制
- 自动快照保留
- 使用 Lightsail 控制台启用或禁用自动实例快照
- 使用 AWS CLI为实例或数据块存储磁盘启用或禁用自动快照

自动快照限制

以下限制适用于自动快照：

- 无法使用 Lightsail 控制台为块存储磁盘启用或禁用自动快照。要启用或禁用块存储磁盘的自动快照，必须使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或。 SDKs有关更多信息，请参阅使用 AWS CLI启用或禁用自动快照。
- Windows 实例或托管数据库当前不支持自动快照。相反，您必须为 Windows 实例或托管数据库创建手动快照以备份它们。有关更多信息，请参阅创建 Windows Server 实例的快照和创建数据库快照。默认情况下，托管数据库还启用了 point-in-time备份功能，您可以使用该功能将数据恢复到新数据库。有关更多信息，请参阅使用 point-in-time备份创建数据库。
- 自动快照不保留来自源资源的标签。要在从自动快照创建的新资源上保留来自源资源的标签，您必须在从自动快照创建新资源时，手动添加标签。有关更多信息，请参阅向资源添加标签。

自动快照保留

将存储最新的七个每日自动快照，然后用最新的快照替换最旧的快照。此外，当您删除源资源时，将会删除与资源关联的所有自动快照。此行为与手动快照不同，手动快照即使在您删除源资源后，手动快照仍保留在您的 Lightsail 帐户中。要防止替换自动快照，或者防止在删除源资源时删除自动快照，可以将自动快照复制为手动快照。

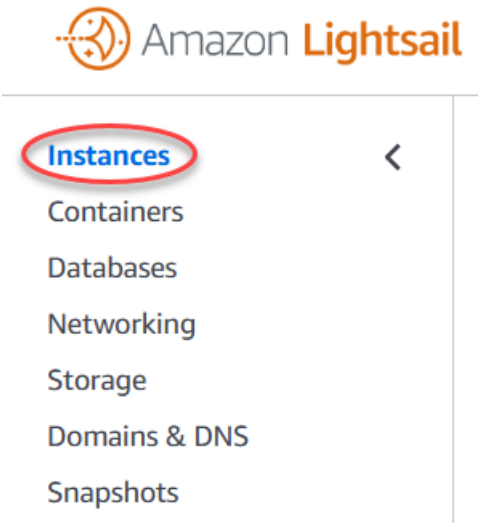
禁用资源的自动快照功能后，将与源资源一起保留资源的现有自动快照，直到您执行以下操作之一：

- 重新启用自动快照，现有的自动快照将替换为更新的快照。
- 手动删除现有的自动快照。
- 删除源资源，这将删除关联的自动快照。

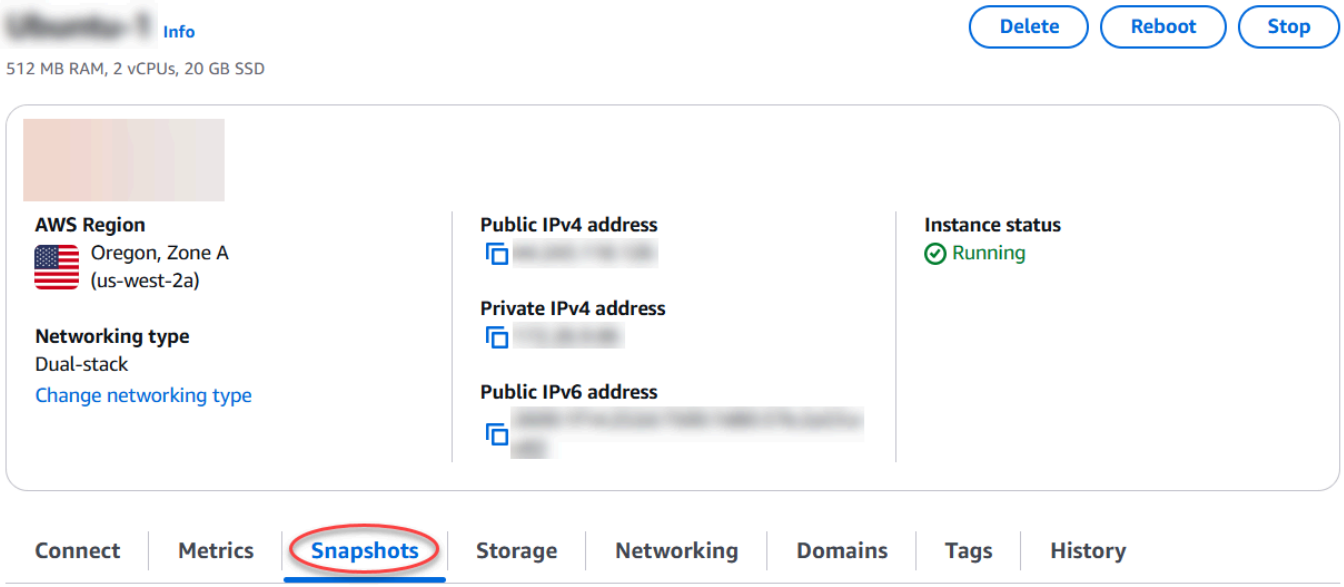
使用 Lightsail 控制台启用或禁用自动实例快照

完成以下步骤，使用 Lightsail 控制台启用或禁用实例的自动快照。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。



3. 选择要为其启用或禁用自动快照的实例的名称。
4. 在实例管理页面中，选择 Snapshots (快照) 选项卡。



5. 在 Automatic snapshots (自动快照) 部分下，选择开关可启用它。同样，如果它处于启用状态，则选择开关可禁用它。
6. 在出现提示时，选择 Yes, enable (是，启用) 可启用自动快照，而选择 Yes, disable (是，禁用) 可禁用该功能。

   稍后，将启用或禁用自动快照。

   - 如果您启用了 自动快照功能，则可能还需要更改自动快照时间。有关更多信息，请参阅更改实例或数据块存储磁盘的自动快照时间。

- 如果您禁用了 自动快照功能，将保留该资源的现有自动快照，直到您重新启用该功能并且系统将其替换为新快照，或者直到您删除自动快照。对于存储在您的 Lightsail 帐户中的自动快照，您需要支付快照存储费。有关删除自动快照的更多信息，请参阅删除自动实例快照。

使用启用或禁用实例或块存储磁盘的自动快照 AWS CLI

完成以下步骤，以使用 AWS CLI启用或禁用实例或块存储磁盘的自动快照。

1. 打开终端或命令提示符窗口。

   如果你还没有，请安装 AWS CLI 并将其配置为与 Lightsail 配合使用。

2. 根据您要启用还是禁用自动快照，输入此步骤中所述命令之一：

> **Note**
>
> autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00} 参数在这些命令中是可选的。如果您在启用自动快照时未指定每日自动快照时间，Lightsail 会为您的资源分配默认快照时间。有关更多信息，请参阅更改实例或数据块存储磁盘的自动快照时间。

- 输入以下命令，为现有资源启用自动快照：

```
aws lightsail enable-add-on --region Region --resource-name ResourceName --add-on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

在该命令中，将：

- *Region*与资源 AWS 区域 所在的。
- *ResourceName*加上资源的名称。
- *HH:00*每日自动快照时间以小时为增量，以协调世界时 (UTC) 为单位。

示例：

```
aws lightsail enable-add-on --region us-west-2 --resource-name WordPress-1 --add-on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:00}
```

- 输入以下命令以在创建新实例时启用自动快照：

```
aws lightsail create-instances --region Region --availability-
zone AvailabilityZone --blueprint-id BlueprintID --
bundle-id BundleID --instance-name InstanceName --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

在该命令中，将：

- *Region*使用应 AWS 区域 在其中创建实例。
- *AvailabilityZone*以及应在其中创建实例的可用区。
- *BlueprintID*并附上要用于实例的蓝图 ID。
- *BundleID*附上要用于实例的捆绑包 ID。
- *InstanceName*并附上要用于实例的名称。
- *HH:00*每日自动快照时间以小时为增量，以协调世界时 (UTC) 为单位。

示例：

```
aws lightsail create-instances --region us-west-2 --availability-
zone us-west-2a --blueprint-id wordpress_5_1_1_2 --bundle-
id medium_2_0 --instance-name WordPressInstance --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=20:00}
```

- 输入以下命令以在创建新磁盘时启用自动快照：

```
aws lightsail create-disk --region Region --availability-
zone AvailabilityZone --size-in-gb Size --disk-name DiskName --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

在该命令中，将：

- *Region*使用应 AWS 区域 在其中创建磁盘。
- *AvailabilityZone*以及应在其中创建磁盘的可用区。
- *Size*所需磁盘大小（以 GB 为单位）。
- *DiskName*并附上要用于磁盘的名称。
- *HH:00*每日自动快照时间以小时为增量，以协调世界时 (UTC) 为单位。

示例：

```
aws lightsail create-disk --region us-west-2 --availability-
zone us-west-2a --size-in-gb 32 --disk-name Disk01 --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:59}
```

- 输入以下命令，为资源禁用自动快照：

```
aws lightsail disable-add-on --region Region --resource-name ResourceName --add-
on-type AutoSnapshot
```

在该命令中，将：

- *Region*与资源 AWS 区域 所在的。
- *ResourceName*加上资源的名称。

示例：

```
aws lightsail disable-add-on --region us-west-1 --resource-
name MyFirstWordPressWebsite01 --add-on-type AutoSnapshot
```

您会看到类似于以下示例的结果：



稍后，将启用或禁用自动快照。

- 如果您启用了 自动快照，则可能还需要更改自动快照时间。有关更多信息，请参阅更改实例或数据块存储磁盘的自动快照时间。
- 如果您禁用了 自动快照，将保留现有自动快照，直到您重新启用该功能并且系统将其替换为新快照，或者直到您删除自动快照。对于存储在您的 Lightsail 帐户中的自动快照，您需要支付快照存储费。有关删除自动快照的更多信息，请参阅删除自动实例快照。

> **Note**
>
> 有关这些命令中 EnableAddOn 和 DisableAddOn API 操作的更多信息，请参阅 Lightsail API 文档DisableAddOn中的EnableAddOn和。

调整 Lightsail 实例和磁盘的自动快照计划

当您为实例或块存储磁盘启用自动快照功能时，Lightsail 会在默认自动快照时间或您指定的时间内创建资源的每日快照。请按照本指南中的步骤操作，更改资源的自动快照时间。

内容

- 自动快照时间限制
- 的默认自动快照时间 AWS 区域
- 使用 Lightsail 控制台更改自动快照时间
- 使用更改自动快照时间和块存储磁盘 AWS CLI

自动快照时间限制

以下限制适用于自动快照时间：

- 无法使用 Lightsail 控制台更改块存储磁盘的自动快照时间。要更改块存储磁盘的自动快照时间，必须使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或。 SDKs有关更多信息，请参阅使用 AWS CLI更改自动快照时间。
- 只能以小时为增量指定自动快照时间。它还必须超过当前时间 30 分钟以上。Lightsail 会在您指定的时间和之后最多 45 分钟之间创建自动快照。

> **Important**
>
> 创建自动快照时，您无法创建手动快照。

- 当您更改资源的自动快照时间时，该时间通常会立即生效，以下情况例外：
  - 如果已为当天创建了自动快照，并且将快照时间更改为一天中的较晚时间，则新的快照时间将在第二天生效。这样可以确保当天不会创建两个快照。
  - 如果还没有为当天创建自动快照，并且将快照时间更改为一天中的较早时间，则新的快照时间将在第二天生效。此外，还会在当天预先设置的时间自动创建快照。这样可以确保当天创建一个快照。
  - 如果还没有为当天创建自动快照，而您将快照时间更改当前时间 30 分钟以内的时间，则新的快照时间将在第二天生效。此外，还会在当天预先设置的时间自动创建快照。这样可以确保为当天创建快照，因为在当前时间和指定的新快照时间之间需要 30 分钟。
  - 如果计划在当前时间后的 30 分钟内创建自动快照，并且您更改了快照时间，则新快照时间将在第二天生效。此外，还会在当天预先设置的时间自动创建快照。这样可以确保为当天创建快照，因为在当前时间和指定的新快照时间之间需要 30 分钟。

  当这些条件满足任一条件时，Lightsail 控制台中将显示一条消息，通知您新的快照时间最长可能需要 24 小时才能生效。

AWS 区域的默认自动快照时间

如果您在启用自动快照时未指定自动快照时间，则 Lightsail 会分配以下默认自动快照时间之一。时间取决于您的实例或块存储磁盘所在的位置： AWS 区域

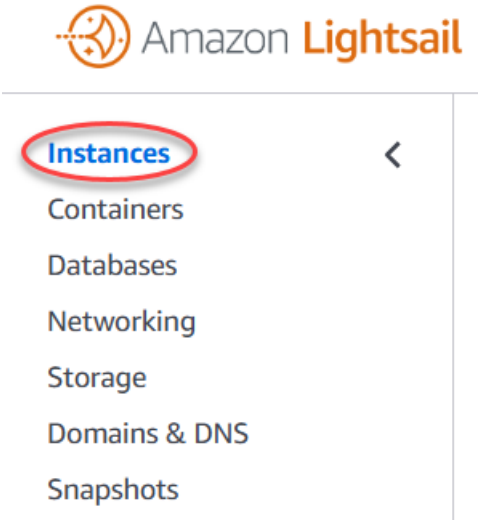
- 美国东部（俄亥俄）(us-east-2)：03:00 UTC
- 美国东部（弗吉尼亚北部）(us-east-1)：06:00 UTC
- 美国西部（俄勒冈）(us-west-2)：06:00 UTC
- 亚太地区（孟买）(ap-south-1)：17:00 UTC
- 亚太地区（首尔）(ap-northeast-2)：13:00 UTC
- 亚太地区（新加坡）(ap-southeast-1)：14:00 UTC
- 亚太地区（悉尼）(ap-southeast-2)：12:00 UTC
- 亚太地区（东京） (ap-northeast-1)：13:00 UTC
- 加拿大（中部）(ca-central-1)：06:00 UTC
- 欧洲（法兰克福）(eu-central-1)：20:00 UTC

- 欧洲（爱尔兰）(eu-west-1)：22:00 UTC
- 欧洲（伦敦）(eu-west-2)：06:00 UTC
- 欧洲（巴黎）(eu-west-3)：07:00 UTC
- 欧洲（斯德哥尔摩）(eu-north-1)：08:00 UTC

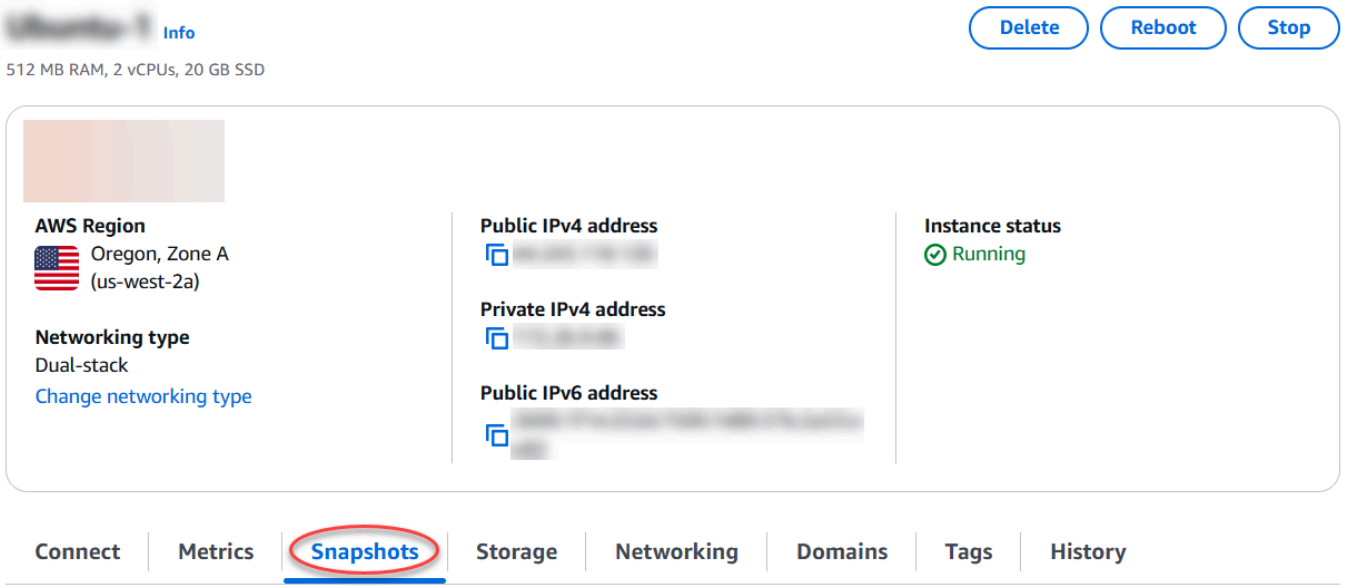
使用 Lightsail 控制台更改自动快照时间

完成以下步骤，使用 Lightsail 控制台更改实例的自动快照时间。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。



3. 选择要为其更改自动快照时间的实例的名称。
4. 在实例管理页面中，选择 Snapshots (快照) 选项卡。



5. 在 Automatic snapshots (自动快照) 部分下，选择 Change snapshot time (更改快照时间)。
6. 选择一天中你希望 Lightsail 创建自动快照的时间。您选择的时间必须采用协调世界时 (UTC) 格式。
7. 选择 Change (更改) 以保存新的快照时间。

   自动快照时间稍后更新。新自动快照时间的生效日期可能会有限制。有关更多信息，请参阅自动快照时间限制。

使用更改实例和块存储磁盘的自动快照时间 AWS CLI

完成以下步骤，以使用 AWS CLI更改实例或块存储磁盘的自动快照时间。

1. 打开终端或命令提示符窗口。

   如果你还没有，请安装 AWS CLI 并将其配置为与 Lightsail 配合使用。
2. 输入以下命令来更改资源的自动快照时间：

   ```
   aws lightsail enable-add-on --region Region --resource-name ResourceName --add-on-request addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
   ```

   在该命令中，将：

   - *Region*与资源 AWS 区域 所在的。
   - *ResourceName*加上资源的名称。

- *HH:00*每日自动快照时间以小时为增量，以协调世界时 (UTC) 为单位。

示例：

```
aws lightsail enable-add-on --region us-west-1 --resource-
name MyFirstWordPressWebsite01 --add-on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=12:00}
```

您会看到类似于以下示例的结果：



自动快照时间稍后更新。新自动快照时间的生效日期可能会有限制。有关更多信息，请参阅自动快照时间限制。

> **Note**
>
> 有关此命令中 EnableAddOn API 操作的更多信息，请参阅 Lightsail API 文档EnableAddOn中的。

删除未使用的 Lightsail 实例和磁盘快照

您可以随时删除 Amazon Lightsail 中实例或块存储磁盘的自动快照；无论该功能是否已启用，还是在启用后是否禁用。对于存储在您的 Lightsail 账户中的自动快照，您需要支付快照存储费。如果不再需要自动快照，请按照本指南中的步骤删除它们。例如，如果您已将自动快照复制到手动快照，而不再需要原始快照，或者如果您已经为资源禁用了自动快照功能，并且不需要已保留的现有自动快照。

内容

- 删除自动快照限制
- 使用 Lightsail 控制台删除实例的自动快照
- 使用删除实例或块存储磁盘的自动快照 AWS CLI

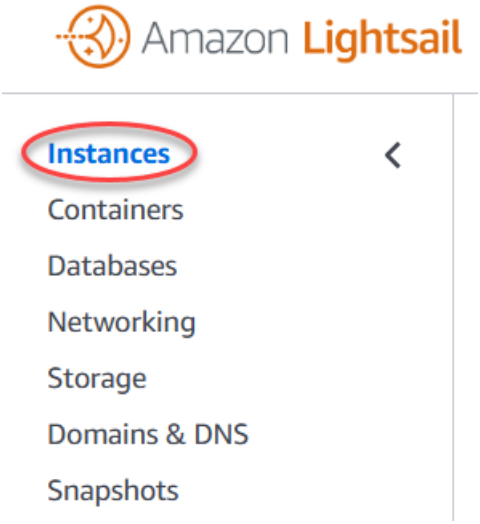
删除自动快照限制

无法使用 Lightsail 控制台删除块存储磁盘的自动快照。要删除块存储磁盘的自动快照，必须使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或。 SDKs有关更多信息，请参阅使用 AWS CLI删除实例或数据块存储磁盘的自动快照。

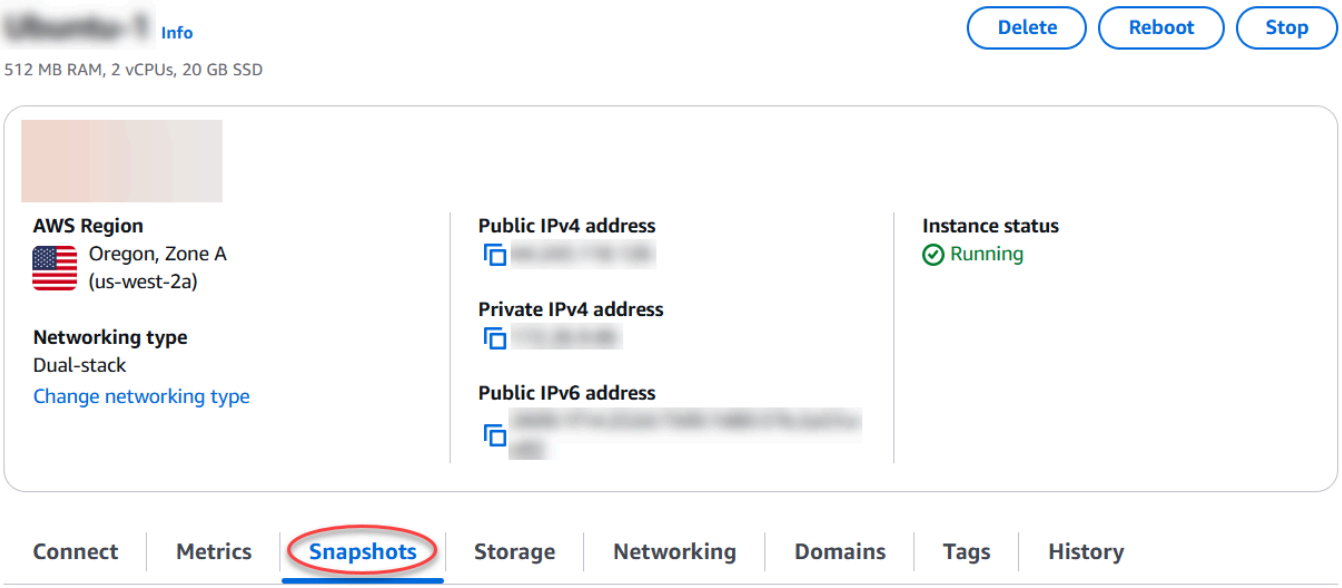
使用 Lightsail 控制台删除实例的自动快照

完成以下步骤，使用 Lightsail 控制台删除实例的自动快照。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。



3. 选择要为其删除自动快照的实例的名称。
4. 在实例管理页面中，选择 Snapshots (快照) 选项卡。



5. 在 Automatic snapshots (自动快照) 部分下，选择要删除的自动快照旁边的省略号图标，然后选择 Delete snapshot (删除快照)。
6. 在提示符下，选择 Yes (是) 以确认您要删除该快照。

   稍等一会后，系统会删除自动快照。

使用删除实例或块存储磁盘的自动快照 AWS CLI

完成以下步骤，以使用 AWS CLI删除实例或块存储磁盘的自动快照。

1. 打开终端或命令提示符窗口。

   如果你还没有，请安装 AWS CLI 并将其配置为与 Lightsail 配合使用。
2. 输入以下命令以获取特定资源的可用自动快照的日期。您需要将自动快照的日期指定为后续命令中的 `date` 参数。

   ```
   aws lightsail --region Region get-auto-snapshots --resource-name ResourceName
   ```

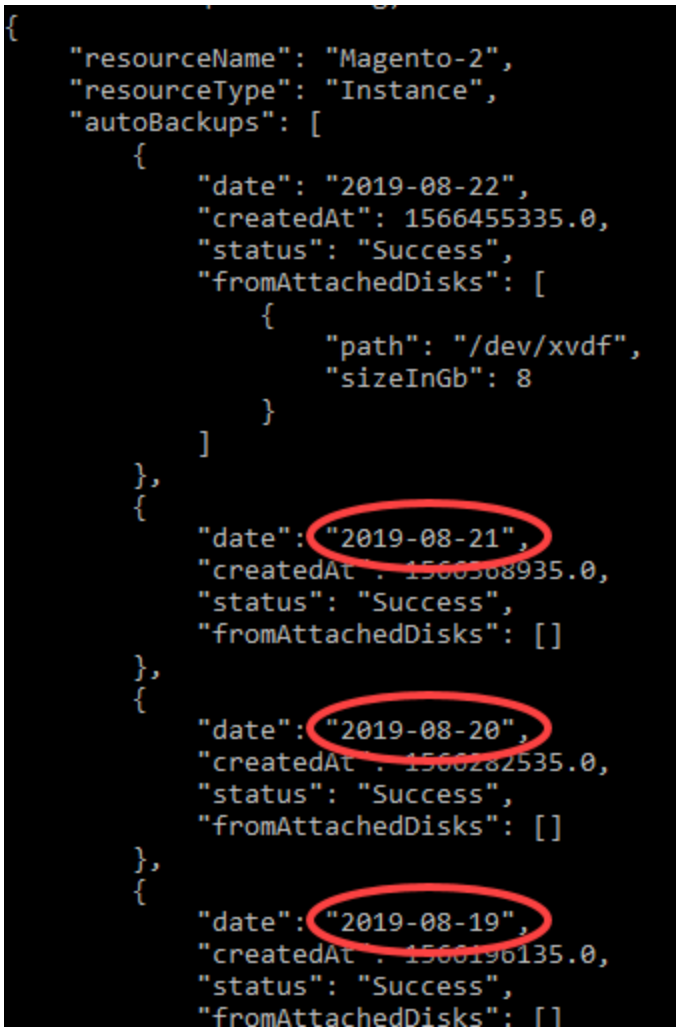
   在该命令中，将：

   - *Region*与资源 AWS 区域 所在的。
   - *ResourceName*加上资源的名称。

   示例：

```
aws lightsail --region us-west-2 get-auto-snapshots --resource-
name MyFirstWordPressWebsite01
```

您应该看到类似下面的结果，其中列出了可用的自动快照：



3. 输入以下命令可删除自动快照：

```
aws lightsail --region Region delete-auto-snapshot --resource-name ResourceName --
date YYYY-MM-DD
```

在该命令中，将：

- *Region*与资源 AWS 区域 所在的。
- *ResourceName*加上资源的名称。
- *YYYY-MM-DD*以及您使用上述命令获得的可用自动快照的日期。

示例：

```
aws lightsail --region us-west-2 delete-auto-snapshot --resource-
name MyFirstWordPressWebsite01 --date 2019-09-16
```

您会看到类似于以下示例的结果：


```
{
    "operation": {
        "id": "8f253c00-c34f-4073-9b0e-e5507ce264d9",
        "resourceName": "Magento-2",
        "resourceType": "Instance",
        "createdAt": 1566507472.323,
        "location": {
            "availabilityZone": "us-west-2",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationDetails": "DeleteAutoBackup-2019-08-16",
        "operationType": "DeleteAutoBackup",
        "status": "Succeeded"
    }
}
```


稍等一会后，系统会删除自动快照。

> **Note**
>
> 有关这些命令中 GetAutoSnapshots 和 DeleteAutoSnapshot API 操作的更多信息，请参阅 Lightsail API 文档DeleteAutoSnapshot中的GetAutoSnapshots和。

防止自动快照在 Lightsail 中被替换

当您在 Amazon Lightsail 中为实例或块存储磁盘启用自动快照功能时，仅存储该资源的最新七张每日自动快照。之后将使用最新的快照替换最早的快照。此外，当您删除源资源时，将会删除与资源关联的所有自动快照。

如果要防止替换特定的自动快照，或者防止在删除源资源时删除特定的自动快照，可以将其复制为手动快照。手动快照将一直保留，直到您手动删除它们为止。

按照本指南中的步骤操作，通过将其复制为手动快照来保留自动快照。对于存储在您的 Lightsail 帐户中的自动快照，您需要支付快照存储费。

> **Note**
>
> 如果您禁用资源的自动快照功能，将保留该资源的现有自动快照，直到您重新启用该功能并且系统将其替换为较新的快照，或者直到您删除自动快照。

内容

- 保留自动快照限制
- 使用 Lightsail 控制台保存实例的自动快照
- 使用保存实例和块存储磁盘的自动快照 AWS CLI

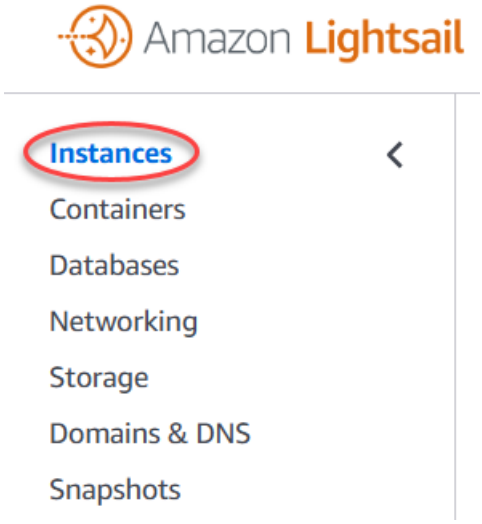
保留自动快照限制

无法使用 Lightsail 控制台将块存储磁盘的自动快照复制到手动快照中。要复制块存储磁盘的自动快照，必须使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或。 SDKs有关更多信息，请参阅使用 AWS CLI保留实例和数据数据块存储磁盘的自动快照。

使用 Lightsail 控制台保存实例的自动快照

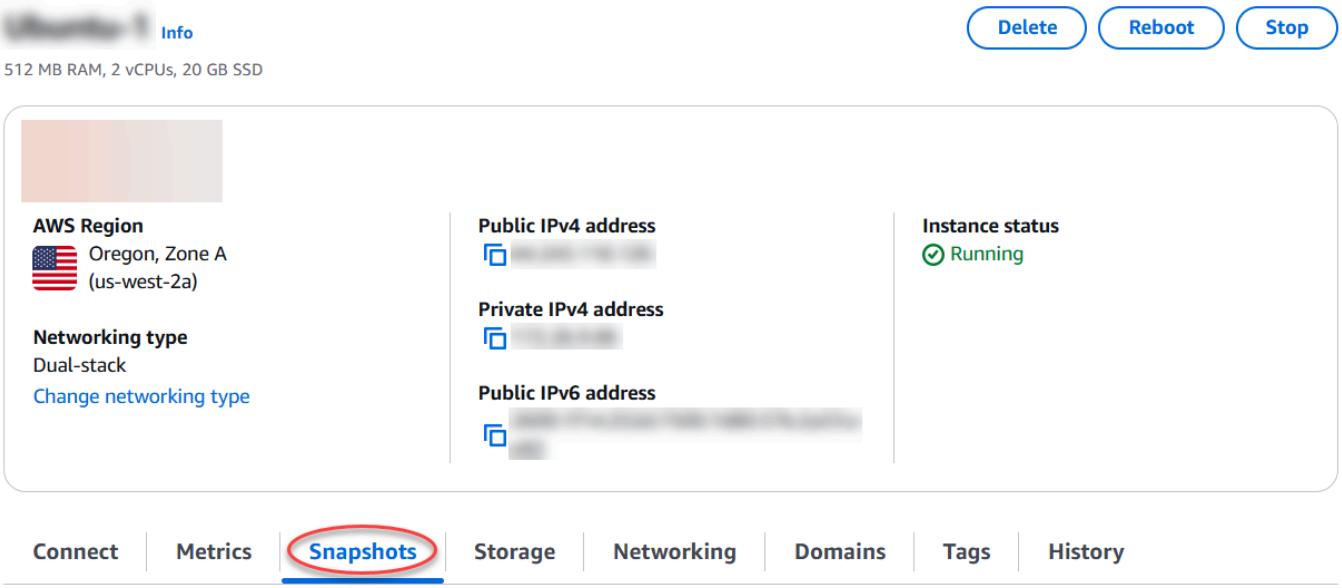
完成以下步骤，使用 Lightsail 控制台保存实例的自动快照。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。



3. 选择要为其保留自动快照的实例的名称。

4. 在实例管理页面中，选择 Snapshots (快照) 选项卡。



5. 在 Automatic snapshots (自动快照) 部分下，选择要保留的自动快照旁边的省略号图标，然后选择 Keep snapshot (保留快照)。
6. 在提示符下，选择 Yes, save (是，保存) 以确认您要保留自动快照。

   稍等一会，自动快照将被复制为手动快照。手动快照将一直保留，直到您删除它们为止。

> **Important**
>
> 如果您不再需要自动快照，建议您删除它。否则，您需要为存储在您的 Lightsail 帐户中的自动快照和重复的手动快照支付快照存储费。有关更多信息，请参阅删除自动实例快照。

使用保存实例和块存储磁盘的自动快照 AWS CLI

完成以下步骤，以使用 AWS CLI保留实例或块存储磁盘的自动快照。

1. 打开终端或命令提示符窗口。

   如果你还没有，请安装 AWS CLI 并将其配置为与 Lightsail 配合使用。
2. 输入以下命令以获取特定资源的可用自动快照的日期。您需要将自动快照的日期指定为后续命令中的 `restore date` 参数。

```
aws lightsail get-auto-snapshots --region Region --resource-name ResourceName
```

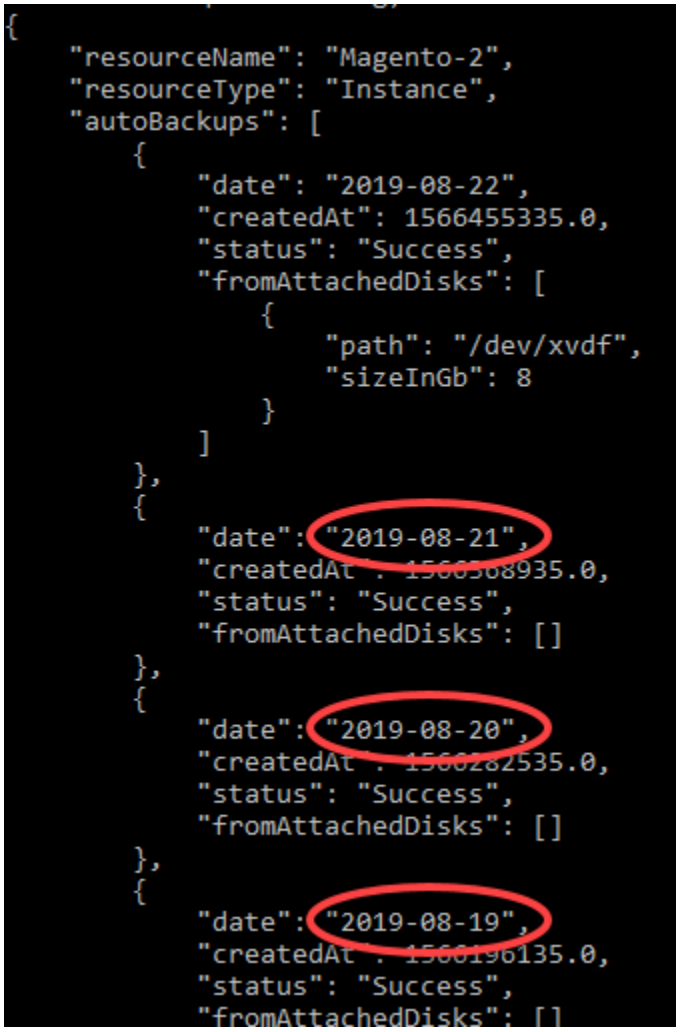
在该命令中，将：

- *Region*与资源 AWS 区域 所在的。
- *ResourceName*加上资源的名称。

示例：

```
aws lightsail get-auto-snapshots --region us-west-2 --resource-
name MyFirstWordPressWebsite01
```

您应该看到类似下面的结果，其中列出了可用的自动快照：



3. 输入以下命令来保留特定资源的自动快照：

```
aws lightsail copy-snapshot --region TargetRegion --source-resource-
name ResourceName --restore-date YYYY-MM-DD --source-region SourceRegion --target-
snapshot-name SnapshotName
```

在该命令中，将：

- *TargetRegion*使用要将快照复制到的。 AWS 区域
- *ResourceName*加上资源的名称。
- *YYYY-MM-DD*以及您使用上述命令获得的可用自动快照的日期。
- *SourceRegion*使用当前 AWS 区域 自动快照所在的。
- *SnapshotName*使用要创建的新快照的名称。

示例：

```
aws lightsail copy-snapshot --region us-west-2 --source-resource-
name MyFirstWordPressWebsite01 --restore-date 2019-09-16 --source-region us-west-2
 --target-snapshot-name Snapshot-Copied-From-Auto-Snapshot
```

您会看到类似于以下示例的结果：


```
{
    "operations": [
        {
            "id": "6f2607ca-c3d3-4e92-9795-8d7c8d72b038",
            "resourceName": "Snapshot-Copied-From-Auto-Backup",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1566504306.107,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "us-west-2:Magento-2",
            "operationType": "CopySnapshot",
            "status": "Started",
            "statusChangedAt": 1566504306.107
        }
    ]
}
```


稍等一会，自动快照将被复制为手动快照。手动快照将一直保留，直到您删除它们为止。

> **Important**
>
> 如果您不再需要自动快照，建议您删除它。否则，您需要为存储在您的 Lightsail 帐户中的自动快照和重复的手动快照支付快照存储费。有关更多信息，请参阅删除自动实例快照。

> **Note**
>
> 有关这些命令中 GetAutoSnapshots 和 CopySnapshot API 操作的更多信息，请参阅 Lightsail API 文档CopySnapshot中的GetAutoSnapshots和。

使用快照备份 Linux/Unix Lightsail 实例

你可以为基于 Linux/UNIX 的 Amazon Lightsail 实例创建快照。实例快照是系统磁盘的副本，并与原始计算机配置（内存、CPU、磁盘大小和数据传输速率）匹配。如果您已将块存储磁盘挂载到您的实例，Lightsail 会将这些额外的磁盘作为快照的一部分进行复制。有关更多信息，请参阅快照。

> **Note**
>
> 创建基于 Windows 服务器的 Lightsail 实例快照的步骤有所不同。有关更多信息，请参阅创建 Windows Server 实例的快照。

你必须已经在 Lightsail 中有一个实例才能创建它的快照。拥有实例后，请按照以下步骤创建快照：

1. 在 Lightsail 主页上，选择要为其创建快照的实例的名称。
2. 选择 Snapshots（快照）选项卡。
3. 在页面的 Manual snapshots（手动快照）部分中，选择 Create snapshot（创建快照），然后输入您快照的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。

- 可以包括字母数字字符、数字、句点、连字符和下划线。

4. 选择 Create（创建）。

   您可以看到刚创建的快照的状态为 Snapshotting...（正在创建快照...）。

   当快照完成后，您可以从该快照创建另一个实例。例如，您可能希望选择一个比之前拥有的更大的包。

> **Important**
>
> 当您使用快照创建新实例时，Lightsail 允许您创建大小相同或更大的实例包。我们目前不支持从快照创建更小的实例大小。在从快照创建新实例时，较小的选项将显示为灰色。

要使用快照创建更大的实例大小，您可以使用 Lightsail 控制台、CL create-instances-from-snapshotl 命令或 API 操作。CreateInstancesFromSnapshot有关更多信息，请参阅从快照创建实例。有关 Lightsail 捆绑包的更多信息，请参阅 Lightsail 定价。

创建你的 Lightsail Windows Server 实例的快照

快照是系统磁盘和实例初始配置的副本。快照包含内存、CPU、磁盘大小和数据传输速率等信息。有关更多信息，请参阅快照。

要在 Lightsail 中创建 Windows 服务器实例的快照，请先创建备份快照。接下来，使用称为 System Preparation (Sysprep) 的特殊实用工具再创建一个快照。Sysprep 使 Windows Server 安装实现了一般化，以便实例能够作为快照备份。然后，当您使用该快照创建实例时，您会 out-of-box体验到第一次运行该 Windows 实例的体验。

要创建 Linux 或 Unix 实例的快照，请参阅创建 Linux 或 Unix 实例的快照。

内容

- 步骤 1：在运行 Sysprep 之前创建备份快照
- 步骤 2：连接到您的实例并使用 Sysprep 将其关闭
- 步骤 3：运行 Sysprep 之后创建快照

步骤 1：在运行 Sysprep 之前创建备份快照

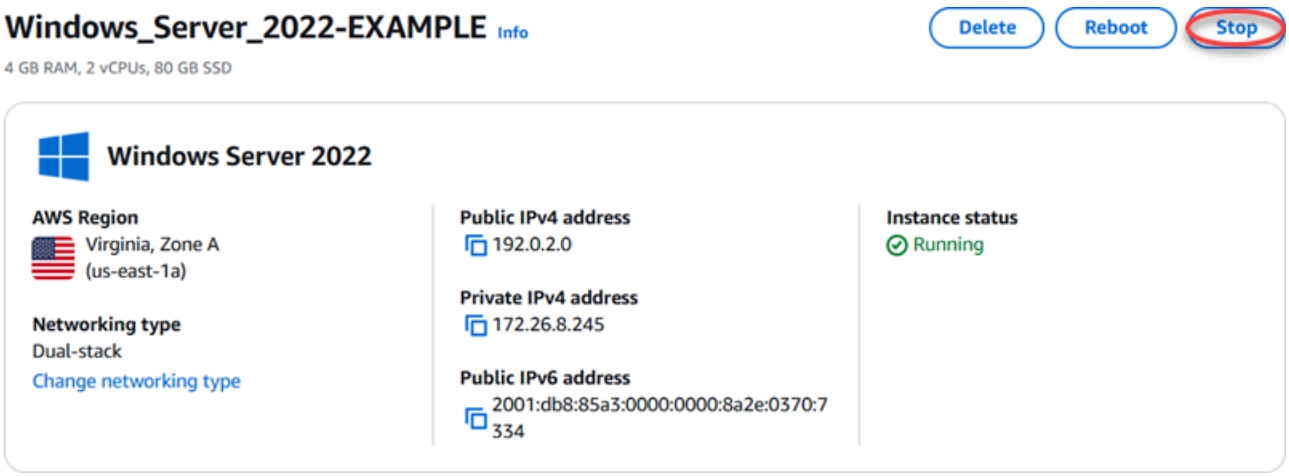
在您运行 Sysprep 以创建快照时，系统特定的信息会从实例中移除。这可能会对在该实例上运行的应用程序造成意外后果。因此，在运行 Sysprep 之前，您应先创建备份快照，以确保出现错误时有备用快照。

在运行 Sysprep 之前创建快照时，您使用备份快照创建的实例与原始实例具有相同的管理员密码。您无法在 Lightsail 控制台中使用基于浏览器的 RDP 客户端连接到这些实例。但是，您可以使用您自己的 RDP 客户端和与原始实例相同的管理员密码进行连接。有关更多信息，请参阅在 Windows 电脑上使用远程桌面连接客户端连接到 Amazon Lightsail 中的 Windows 实例。

> **Important**
>
> 保存原始 Windows 实例的管理员密码，并将其存储在安全的位置。如果出现问题，您稍后将需要该管理员密码，并从运行 Sysprep 之前创建的快照创建一个实例。

在运行 Sysprep 之前创建备份快照

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，选择要为其创建快照的 Windows 服务器实例的名称。
3. 选择实例管理页面顶部的 Stop（停止）以停止您的实例。



> **Note**
>
> 停止实例会导致其上的所有网站或服务不可用，直到再次启动该实例才可用。

4. 选择 Snapshots（快照）选项卡。

5. 在页面的 Manual snapshots（手动快照）部分中，选择 Create snapshot（创建快照），然后输入您快照的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
6. 选择 Create（创建）。
7. 在出现提示时，再次选择 Create snapshot（创建快照）以确认。

   快照创建过程需要几分钟才能完成。
8. 创建快照后，选择实例管理页面顶部的 Start（启动）再次启动实例。

步骤 2：连接到您的实例并使用 Sysprep 将其关闭

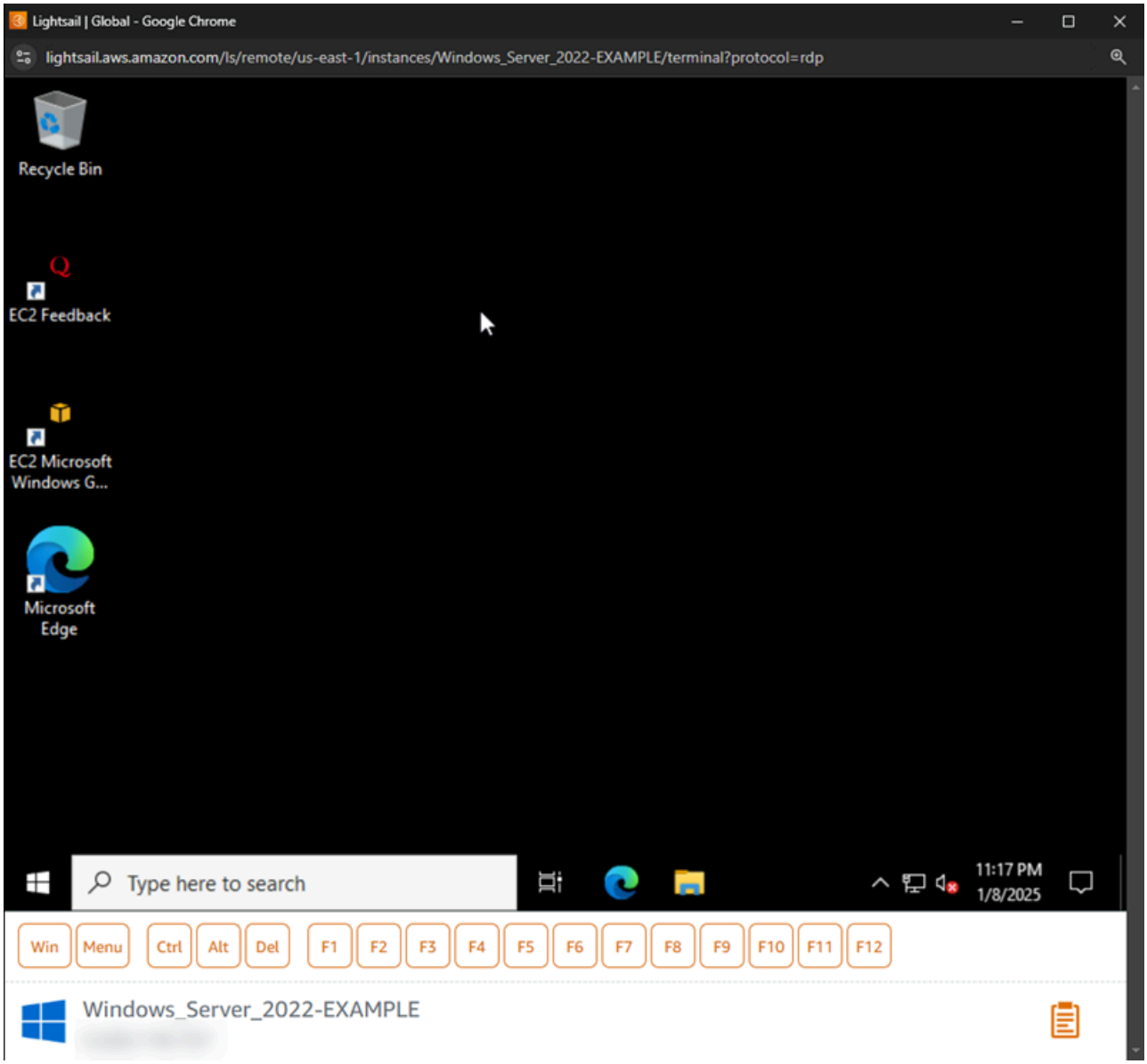
现在您已拥有备份快照，便可以在 Windows Server 实例上运行 Sysprep。这会导致实例关闭，以便您可以拍摄快照。有关 Sysprep 的更多信息，请参阅 Microsoft 文档中的 Sysprep 概览。

在此步骤中，连接到您的实例并通过一个预安装的应用程序运行 Sysprep。该应用程序EC2LaunchSettings在 Windows Server 2019 和 Windows Server 2016 实例上调用，在 Windows Server 2012 实例上调用 Ec 2 ConfigService 设置。

连接到您的实例并运行 Sysprep

1. 在实例管理页面上，选择 Connect（连接）选项卡，然后选择 Connect using RDP（使用 RDP 连接）。

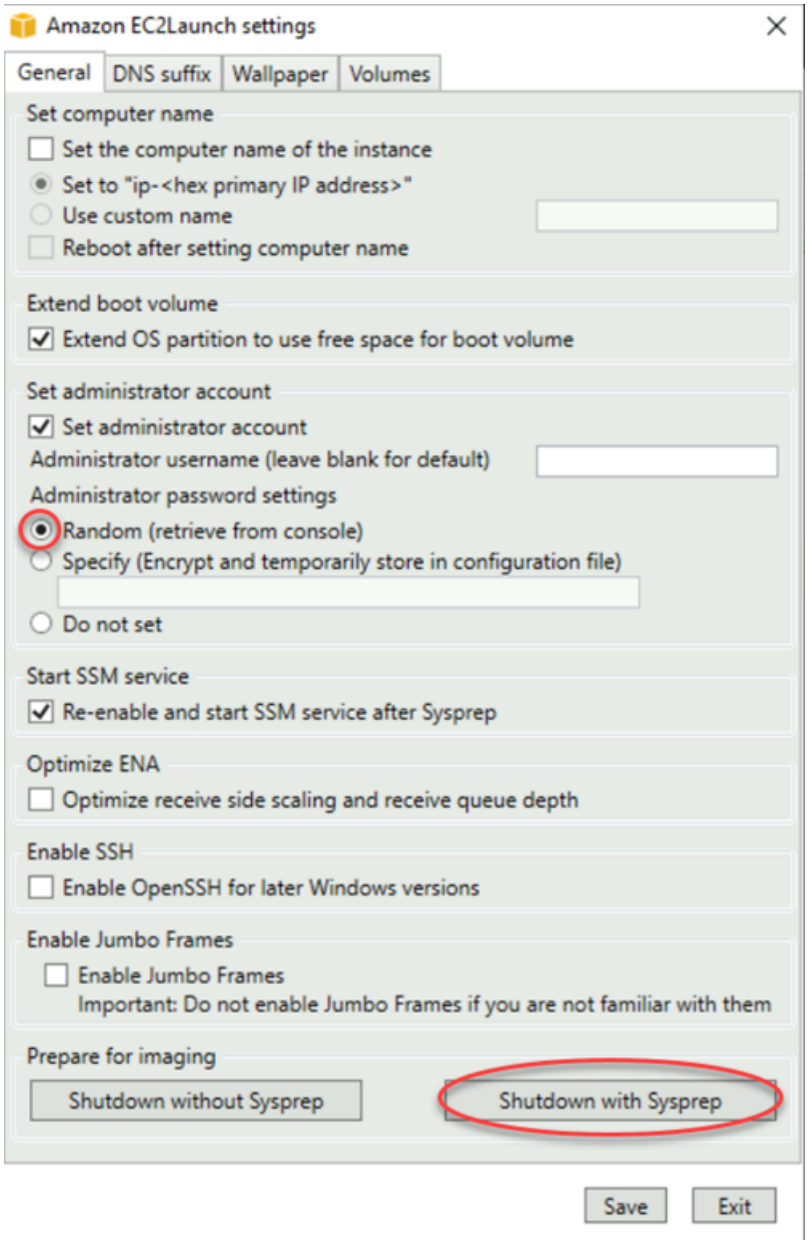
   此时基于浏览器的 RDP 窗口会打开，如以下示例所示：



2. 在任务栏上，选择 Windows 图标，或者选择 Win打开 “开始” 菜单。
3. 选择以下选项之一：

   - 在 Windows Server 2022、Windows Server 2019 和 Windows Server 2016 实例上，选择 “开始”，然后选择 E c2 LaunchSettings。

4. 在 Administrator Password（管理员密码）部分中，选择 Random (Retrieve from console)（随机（从控制台中检索）），然后选择 Shutdown with Sysprep（关闭 Sysprep）。



5. 选择 Yes（是），确认您要运行 Sysprep 并关闭实例。

   您的实例开始运行 Sysprep，您的 RDP 连接关闭，您的 Lightsail 实例将在几分钟后停止运行。

步骤 3：运行 Sysprep 之后创建快照

在您的实例处于停止状态后，在 Lightsail 控制台中创建快照。在运行 Sysprep 之后创建 Windows Server 实例的快照时，您基于该快照创建的所有实例具有唯一的管理员密码。您可以在 Lightsail 控制台中使用基于浏览器的 RDP 客户端连接到这些实例。

在 Lightsail 控制台中创建快照

1. 切换回 Lightsail 控制台。
2. 在 Windows Server 实例的实例管理页面中，选择 Snapshots（快照）选项卡
3. 在页面的 Manual snapshots（手动快照）部分中，选择 Create snapshot（创建快照），然后输入您快照的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
4. 选择 Create（创建）。
5. 在出现提示时，选择 Create snapshot（创建快照）以确认您准备了用于快照的实例。

   快照创建过程需要几分钟才能完成。
6. 创建快照后，选择实例管理页面顶部的 Start（启动）再次启动实例。

   此时，您应该有两个 Windows Server 实例的快照，如以下示例所示：



   使用 Sysprep 快照创建新实例。仅在运行 Sysprep 后原始实例未按期运行时使用备份快照。

后续步骤

现在您已拥有 Sysprep 和备份快照，您应该完成以下后续步骤：

- 连接到您的原始实例，并确认运行 Sysprep 后，该实例上的应用程序能够按预期运行。有关更多信息，请参阅使用 Amazon Lightsail 连接到 Windows Server 实例。
- 使用 Sysprep 快照创建新实例，连接到该实例，并确认新实例上的应用程序能够按预期运行。有关更多信息，请参阅从快照创建实例。
- 在运行 Sysprep 并确认原始实例按预期运行后，删除备份快照。有关更多信息，请参阅删除快照。
- 如果在运行 Sysprep 后您的实例未按预期运行，请按照从快照创建实例中的步骤从备份快照创建一个新实例。

创建 Lightsail 块存储磁盘快照以进行备份或基准

您可以在 Amazon Lightsail 中创建磁盘快照作为额外块存储磁盘的备份。

您可以将磁盘快照作为新磁盘或数据备份的基准。如果定期拍摄磁盘快照，则这些快照为增量快照。仅在新快照中保存在上一快照之后更改的设备块。尽管快照是以增量方式保存的，但快照删除过程仅要求保留最新的快照以还原整个磁盘。

有关更多信息，请参阅快照。

1. 在左侧导航窗格中，选择存储。
2. 选择要为其创建快照的数据数据块存储磁盘的名称。
3. 选择 Snapshots（快照）选项卡。
4. 在页面的 Manual snapshots（手动快照）部分中，选择 Create snapshot（创建快照），然后输入您快照的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
5. 选择 Create（创建）。

   您可以看到刚创建的快照的状态为 Snapshotting...（正在创建快照...）。

   当快照完成后，您可以从该快照创建另一个磁盘。

在 Lightsail 中根据快照创建块存储磁盘

您可以通过磁盘快照创建新的数据块存储磁盘。如果要创建全新的磁盘，请参阅以下主题之一：创建额外的数据块存储磁盘（Linux/Unix）或创建数据块存储磁盘并将其附加到 Windows Server 实例。

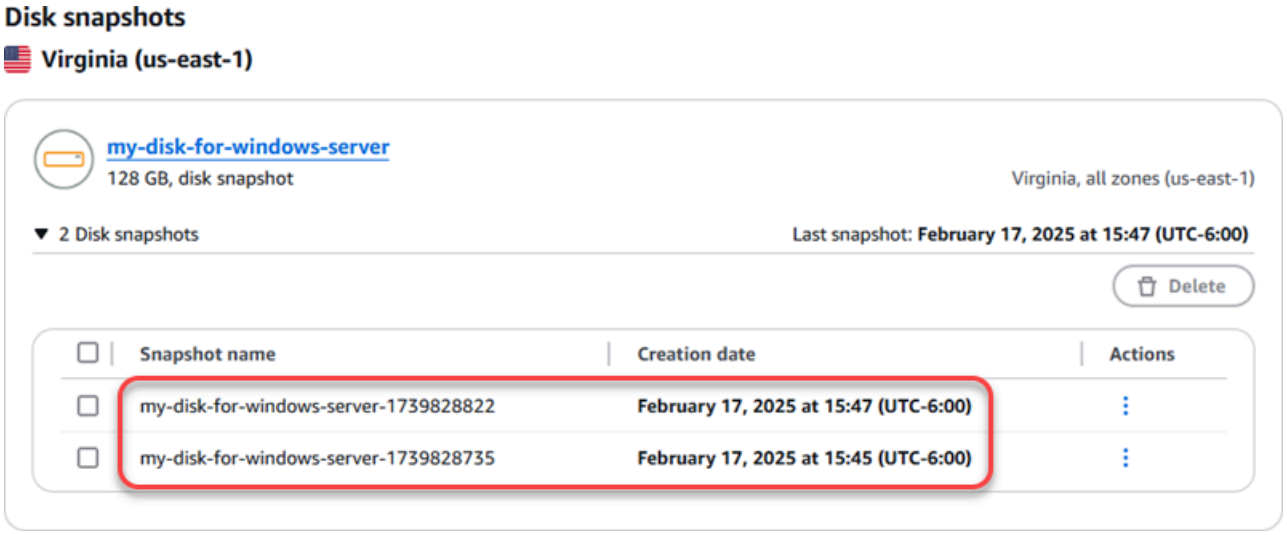
您可以将数据块存储磁盘快照作为新磁盘或数据备份的基准。如果定期拍摄磁盘快照，则这些快照为增量快照。仅在新快照中保存在上一快照之后更改的磁盘数据块。尽管快照是以增量方式保存的，但快照删除过程仅要求保留最新的快照以还原整个磁盘。要创建数据块存储磁盘的快照，请参阅创建数据块存储磁盘快照。

步骤 1：查找您的磁盘快照并选择创建新磁盘

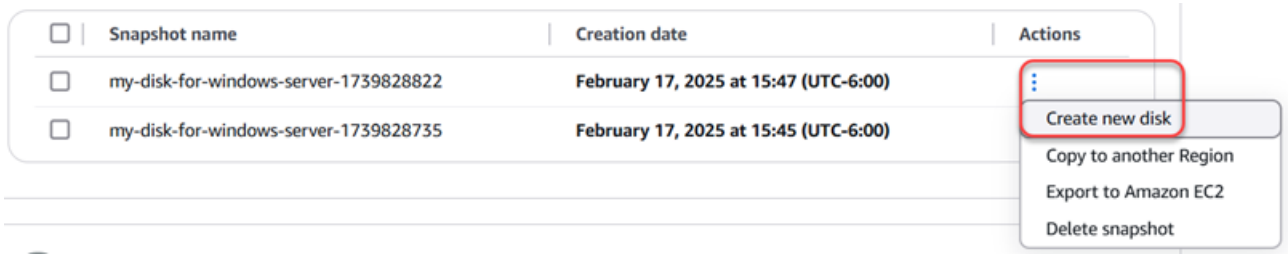
您可以在 Lightsail 的两个位置之一根据磁盘快照创建新实例：在 Lightsail 主页的 “快照” 选项卡上，或者在磁盘管理页面的 “快照” 选项卡上。

来自 Lightsail 主页

1. 在左侧导航窗格中、左侧导航栏上，选择快照。
2. 查找磁盘的名称，然后展开其下的节点以查看该磁盘的所有可用快照。

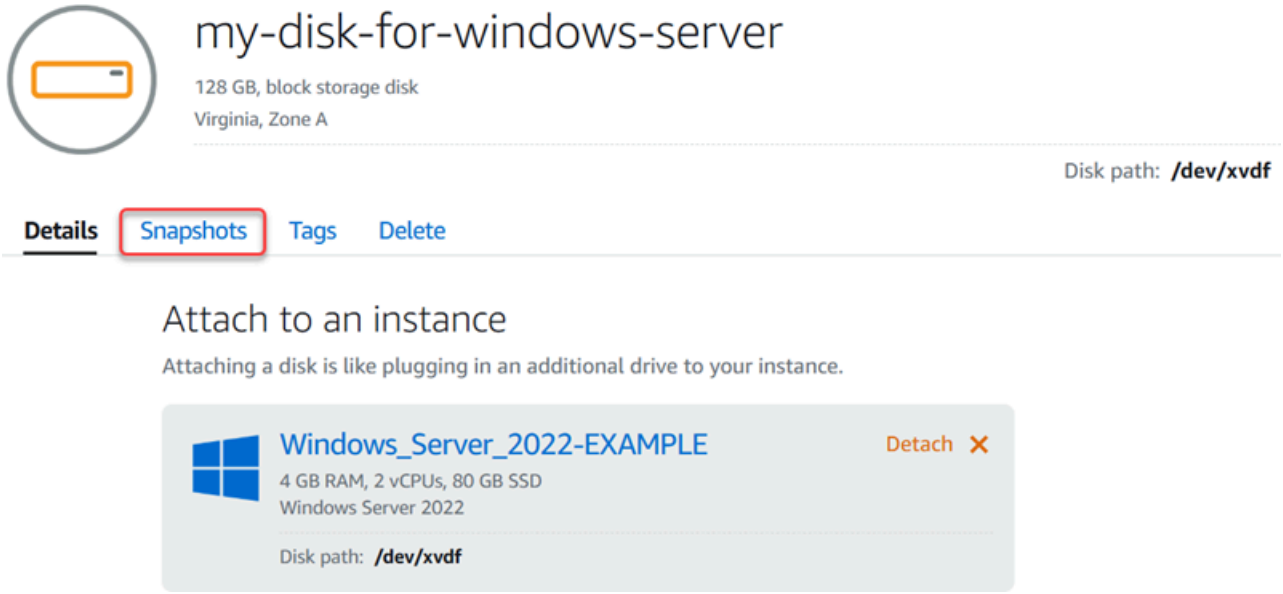


3. 选择用于创建新磁盘的快照旁边的操作菜单图标 (⋮)，然后选择 Create new disk (创建新磁盘)。

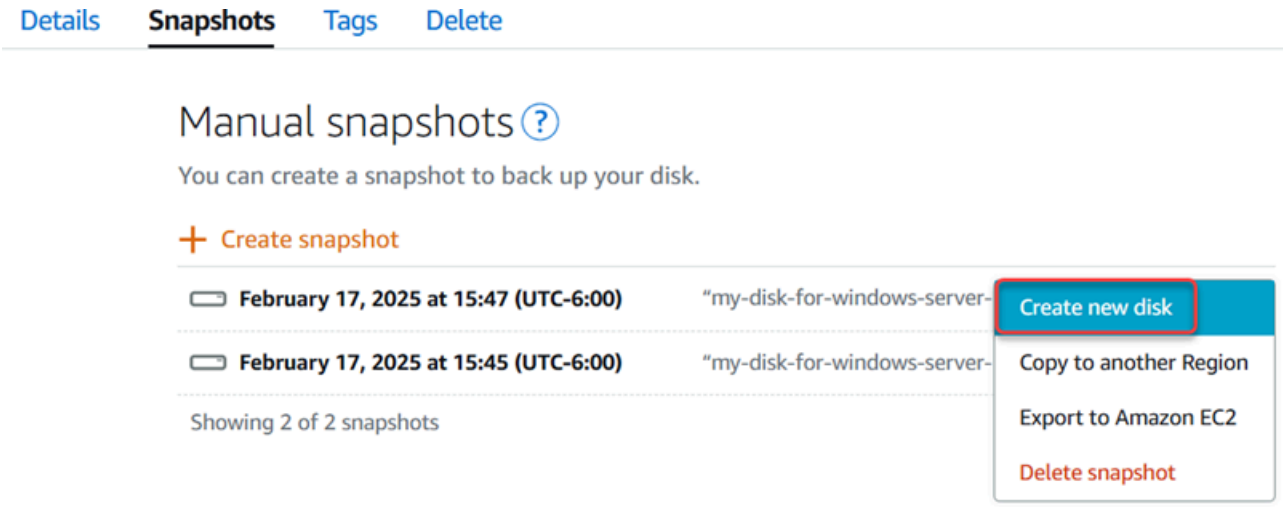


来自 Lightsail 中的磁盘管理页面

1. 在左侧导航窗格中、左侧导航栏上，选择存储选项卡。
2. 选择要查看其快照的磁盘的名称。
3. 选择 Snapshots（快照）选项卡。



4. 在页面的 Manual snapshots (手动快照) 部分中，选择要从中创建新磁盘的快照旁边的操作菜单图标 (⋮)，然后选择 Create new disk (创建新磁盘)。



步骤 2：通过磁盘快照创建新磁盘

1. 为新磁盘选择一个可用区，或者接受默认值（`us-east-2a`）。

   您必须在与源磁盘 AWS 区域 相同的位置创建新磁盘。

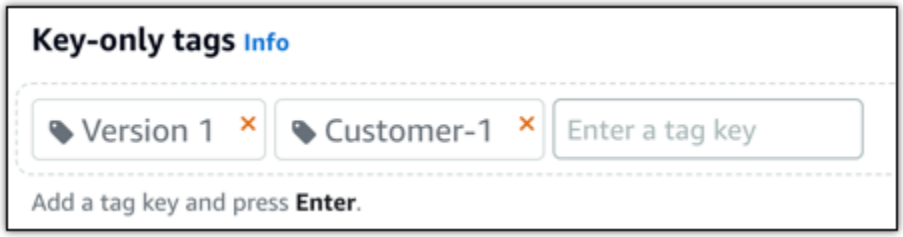
2. 为新磁盘选择大于或等于源快照的大小。
3. 输入磁盘的名称。

   资源名称：

- 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
- 必须包含 2 到 255 个字符。
- 必须以字母数字字符或数字作为开头和结尾。
- 可以包括字母数字字符、数字、句点、连字符和下划线。

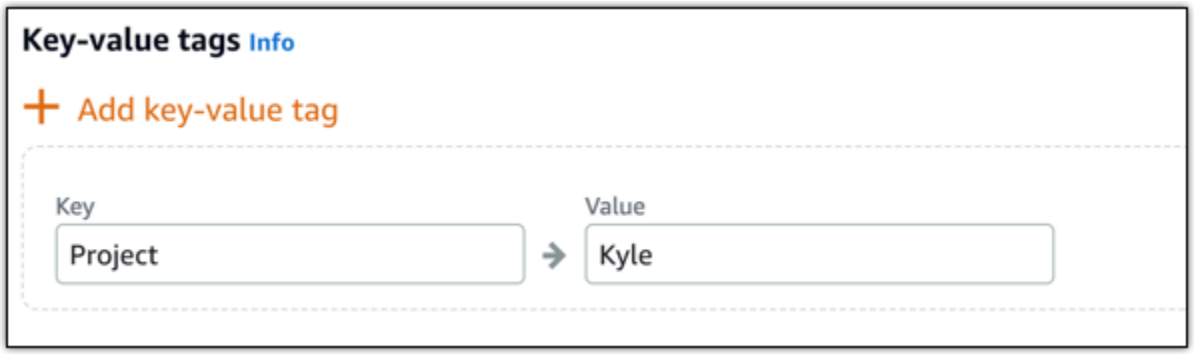
4. 选择以下选项之一以将标签添加到磁盘：

   - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

   - 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

     一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。

   > **Note**
   >
   > 有关“仅键”标签和键值标签的更多信息，请参阅标签。

5. 选择 Create disk（创建磁盘）。

为 Lightsail 实例创建根卷的快照

通过创建系统磁盘的快照，备份 Amazon Lightsail 中的实例根卷。然后，通过从快照创建新数据块存储磁盘并将其连接到另一个实例，访问备份中的文件。如果您具有以下需求，请执行此操作：

- 恢复出现问题的实例的根卷中的数据。
- 创建实例的根卷的备份，就像对待数据块存储磁盘一样。

您可以使用 AWS Command Line Interface (AWS CLI) 或创建实例根卷快照 AWS CloudShell。创建快照后，使用 Lightsail 控制台根据快照创建块存储磁盘。然后，将它连接到正在运行的实例，并从该实例访问它。

内容

- 步骤 1：完成先决条件
- 步骤 2：创建实例根卷快照
- 步骤 3：从快照创建数据块存储磁盘并将其连接到实例
- 步骤 4：从实例访问数据块存储磁盘

步骤 1：完成先决条件

使用 AWS Command Line Interface (AWS CLI) 或 AWS CloudShell 创建实例根卷快照。 CloudShell 是一款基于浏览器的预先认证外壳，您可以直接从 Lightsail 控制台启动它。有关更多信息，请参阅为 Lightsai AWS CLI l 操作设置和配置 和使用管理 Lightsail 资源 AWS CloudShell。

步骤 2：创建实例根卷快照

打开终端 CloudShell 或命令提示符窗口，然后键入以下命令来创建实例根卷快照。

```
aws lightsail create-disk-snapshot --region AWSRegion --instance-name InstanceName --
disk-snapshot-name DiskSnapshotName
```

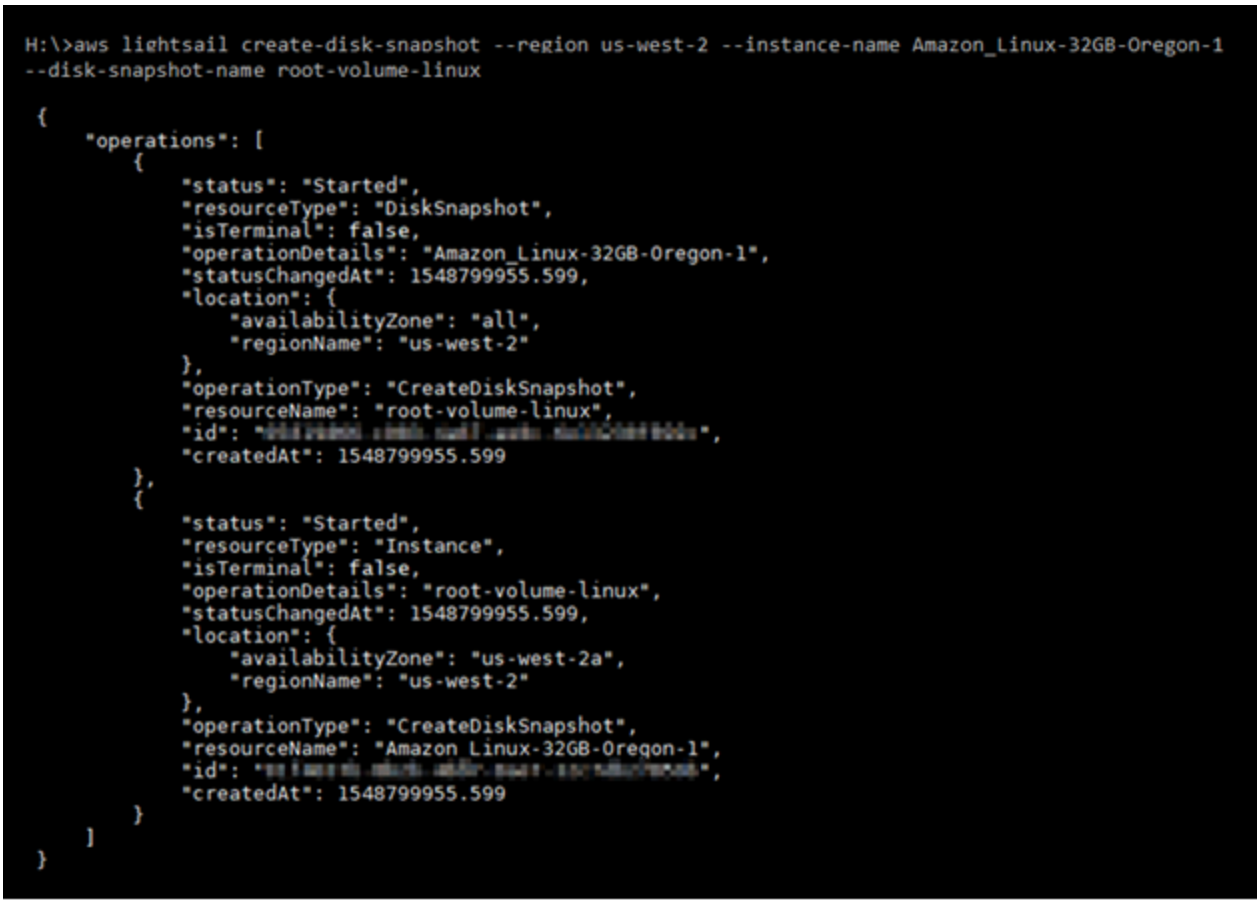
在该命令中，将：

- *AWSRegion*使用实例 AWS 区域 的。
- *InstanceName*使用您要备份其根卷的实例的名称。
- *DiskSnapshotName*使用要创建的新磁盘快照的名称。

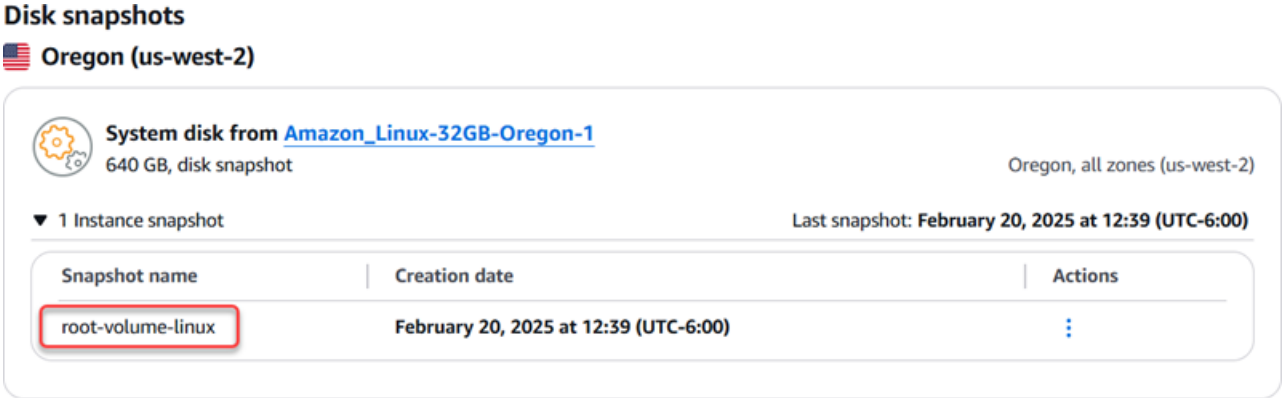
示例：

```
aws lightsail create-disk-snapshot --region us-west-2 --instance-
name Amazon_Linux-32GB-Oregon-1 --disk-snapshot-name root-volume-linux
```

如果成功，您将看到与以下内容类似的结果：



等待几分钟来创建快照。创建完成后，您可以在 Lightsail 主页中查看它，方法是在左侧导航窗格中选择 “快照”，然后向下滚动到 “磁盘快照” 部分，如下例所示。



步骤 3：从快照创建数据块存储磁盘并将其连接到实例

如果您必须访问快照内容，请从实例根卷快照创建新数据块存储磁盘并将其连接到另一个实例。如果您需要恢复出现问题的实例的根卷中的数据，请执行此操作。

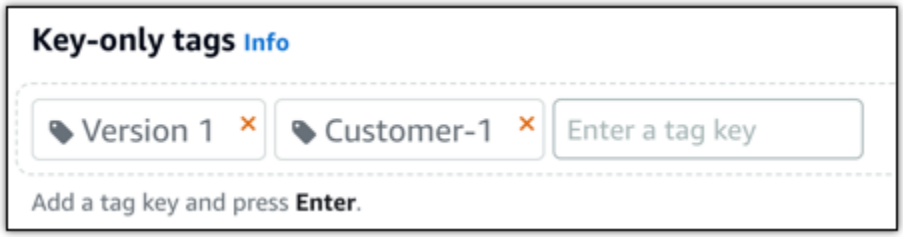
> **Note**
>
> 新的块存储磁盘的创建方式与源快照 AWS 区域 相同。要在其他区域中创建数据块存储磁盘，请将快照复制到所需区域，然后从复制的快照创建新磁盘。有关更多信息，请参阅将快照从一个复制 AWS 区域 到另一个快照。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择快照。
3. 选择要使用的根卷磁盘快照旁边显示的操作菜单图标 (:)，然后选择 Create new disk (创建新磁盘)。
4. 为磁盘选择可用区，或者接受默认值。
5. 为磁盘选择大于或等于源磁盘的大小。
6. 输入磁盘的名称。

   资源名称：

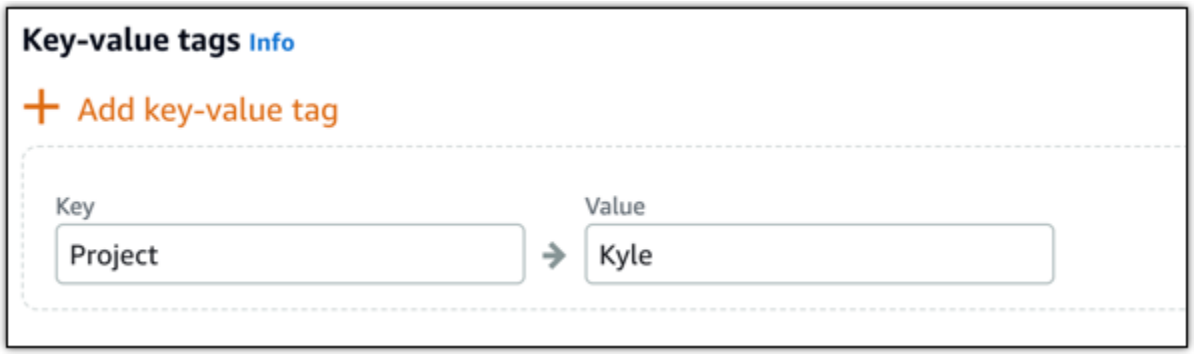
   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
7. 选择以下选项之一以将标签添加到磁盘：

   - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

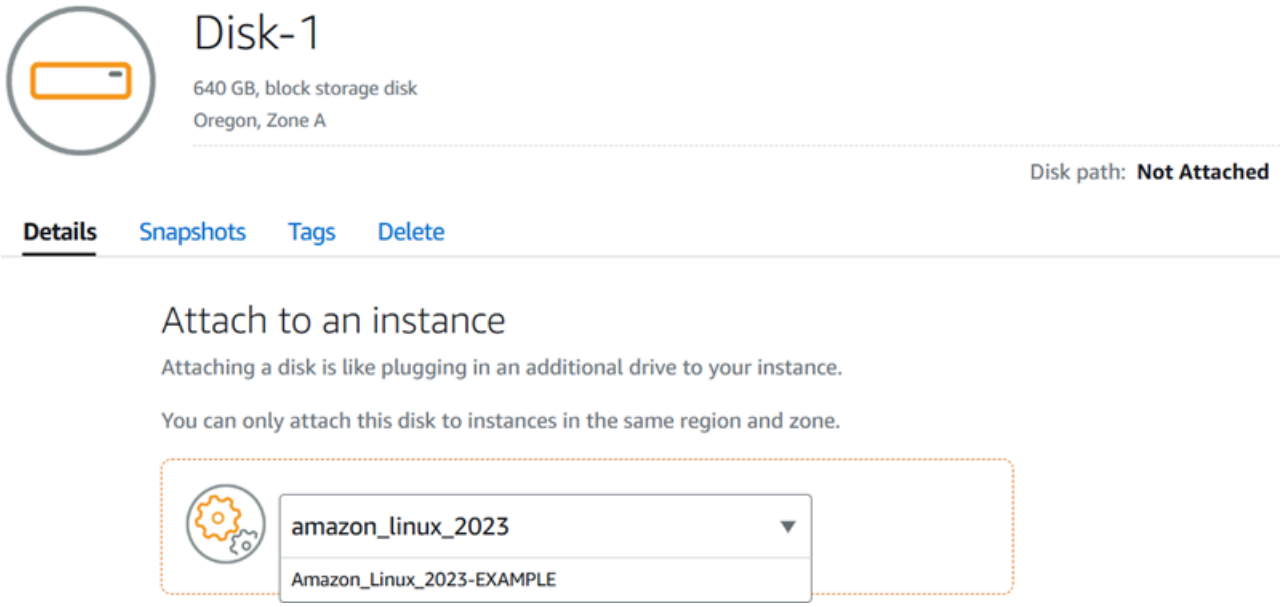
- 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

  一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。



> **Note**
>
> 有关“仅键”标签和键值标签的更多信息，请参阅标签。

8. 选择创建磁盘。
9. 在创建磁盘后，在 Select an instance (选择实例) 下拉菜单中选择要将磁盘连接到的实例。如以下示例所示。



10. 选择 Attach (连接) 以将磁盘连接到所选的实例。

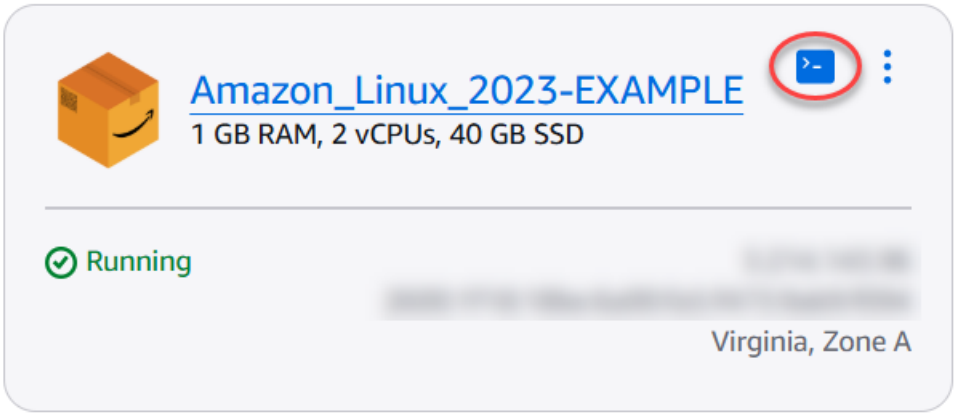
    磁盘现已连接到该实例。接下来，在 Linux 上装载它或在 Windows 上在线引入它，以使适用的操作系统可访问它。有关更多信息，请参阅本指南后面的从实例访问数据块存储部分。

步骤 4：从实例访问数据块存储磁盘

要在将数据块存储磁盘连接到实例后访问该磁盘，您必须在 Linux 或 Unix 上装载它，或在 Windows 上在线引入它。

在 Linux 或 Unix 实例上装载并访问数据块存储磁盘

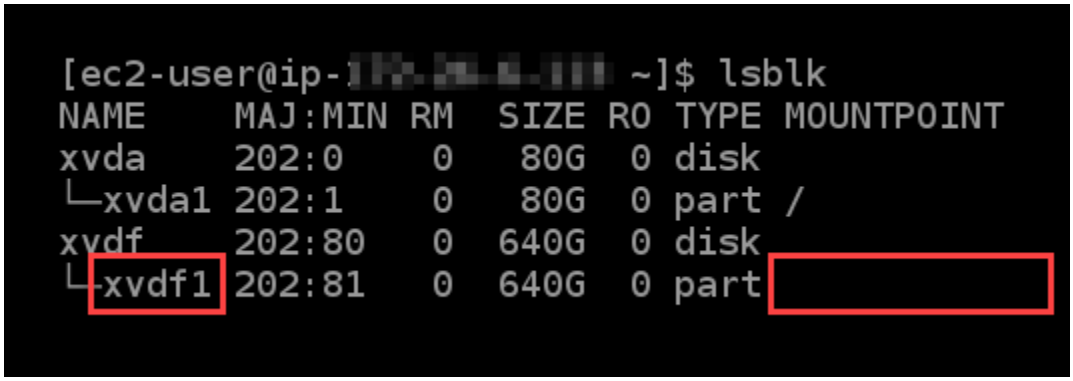
1. 在 Lightsail 主页上，为挂载块存储磁盘的 Linux 或 Unix 实例选择基于浏览器的 SSH 客户端图标。



2. 在连接基于浏览器的 SSH 客户端后，输入以下命令，以查看连接到实例的数据块存储磁盘设备：

```
lsblk
```

您应看到类似于以下示例的结果。在此示例中，xvdf1 是连接到实例的数据块存储磁盘，由于没有装载点而尚未装载。此外，结果省略了设备名称中的 /dev/，因此设备名称实际上为 /dev/xvdf1。



3. 输入以下命令来为数据块存储磁盘创建装载点。

```
sudo mkdir MountPoint
```

在命令中，*MountPoint*替换为将装载和访问块存储磁盘的目录的名称。

示例：

```
sudo mkdir xvdf
```

4. 输入以下命令来将数据块存储磁盘装载到您在上一步中创建的装载点。

```
sudo mount /dev/DeviceName MountPoint
```

在该命令中，将：

- *DeviceName*使用块存储磁盘设备的名称。
- *MountPoint*使用您在上一步中创建的挂载点目录。

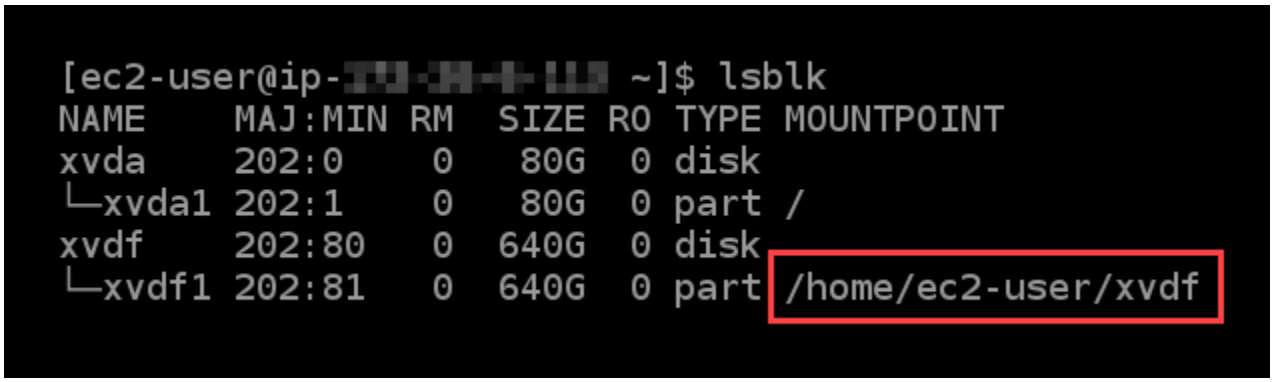
示例：

```
sudo mount /dev/xvdf1 xvdf
```

5. 输入以下命令，以查看连接到实例的数据块存储磁盘设备：

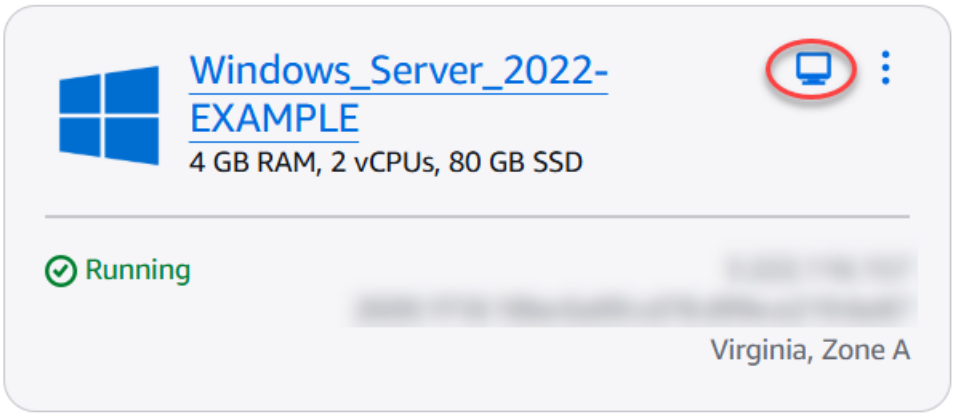
```
lsblk
```

您应看到类似于以下示例的结果。在此示例中，*xvdf1*设备现已安装并可在*/home/ec2-user/xvdf*目录中访问。现在，通过转至装载点目录，可以访问数据块存储磁盘及其内容。

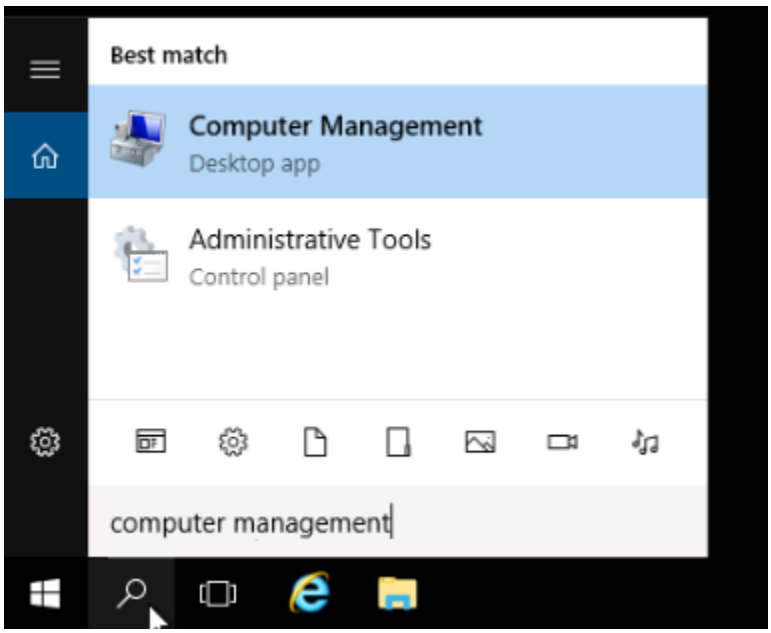


在 Windows 实例上在线引入数据块存储磁盘并访问它

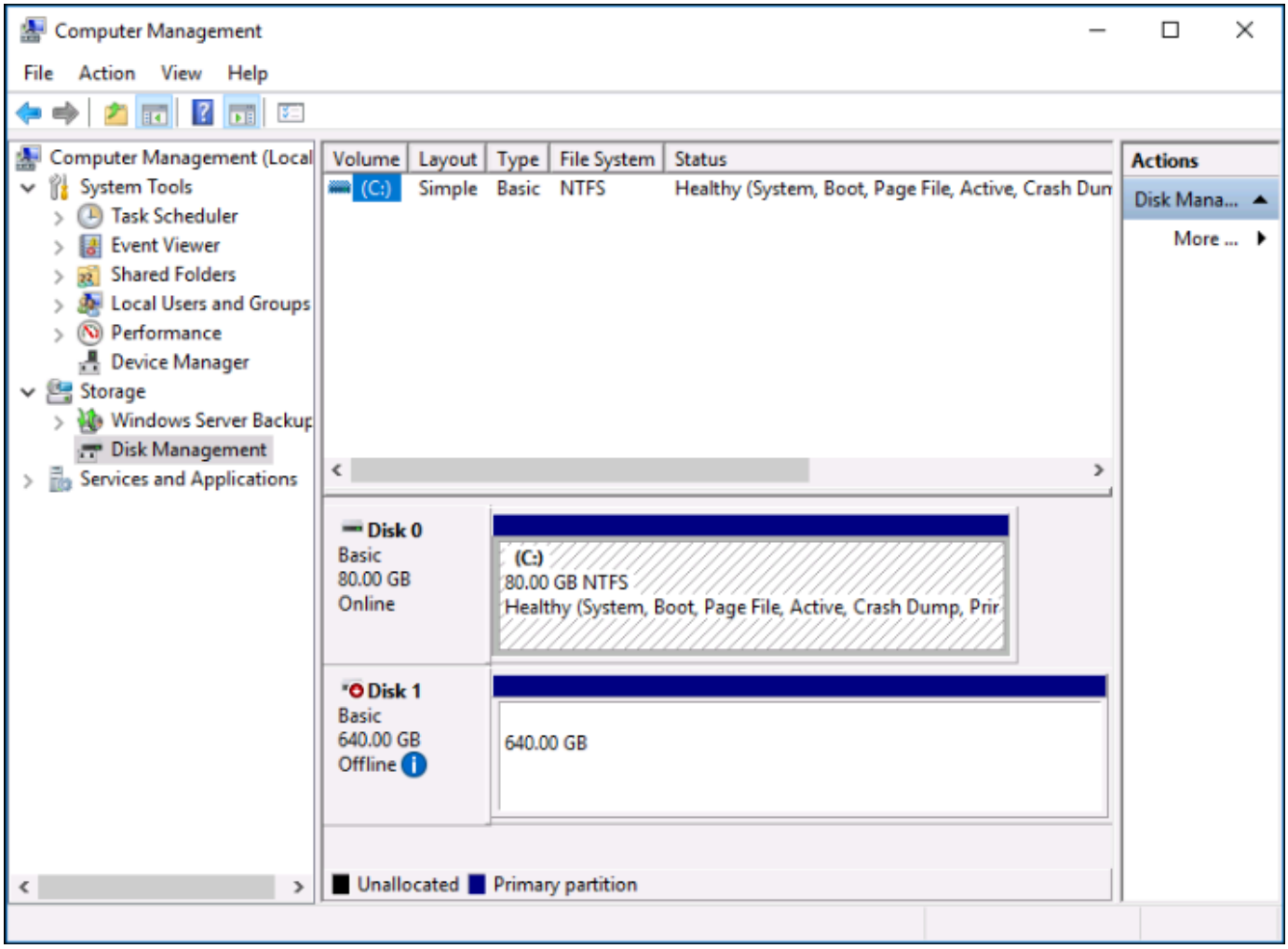
1. 在 Lightsail 主页上，为挂载块存储磁盘的 Windows 实例选择基于浏览器的 RDP 客户端图标。



2. 在连接基于浏览器的 SSH 客户端后，在 Windows 任务栏中搜索计算机管理，然后从结果中选择计算机管理。

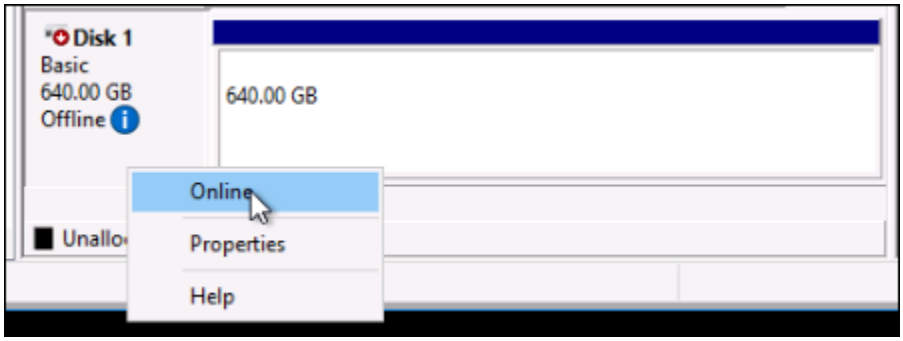


3. 在计算机管理控制台的左侧导航菜单中，选择磁盘管理，如以下示例所示。

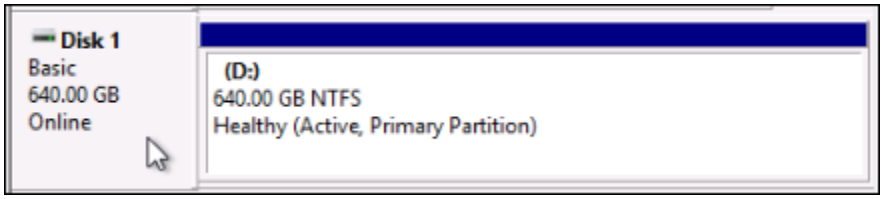


4. 找到最近连接到实例的磁盘。它应标记为“离线”。

5. 右键单击离线标签，然后选择在线。



磁盘现在应该标记为在线，并且驱动器号应与之关联。现在，您可以打开文件资源管理器并浏览到指定的驱动器号来访问数据块存储磁盘及其内容。

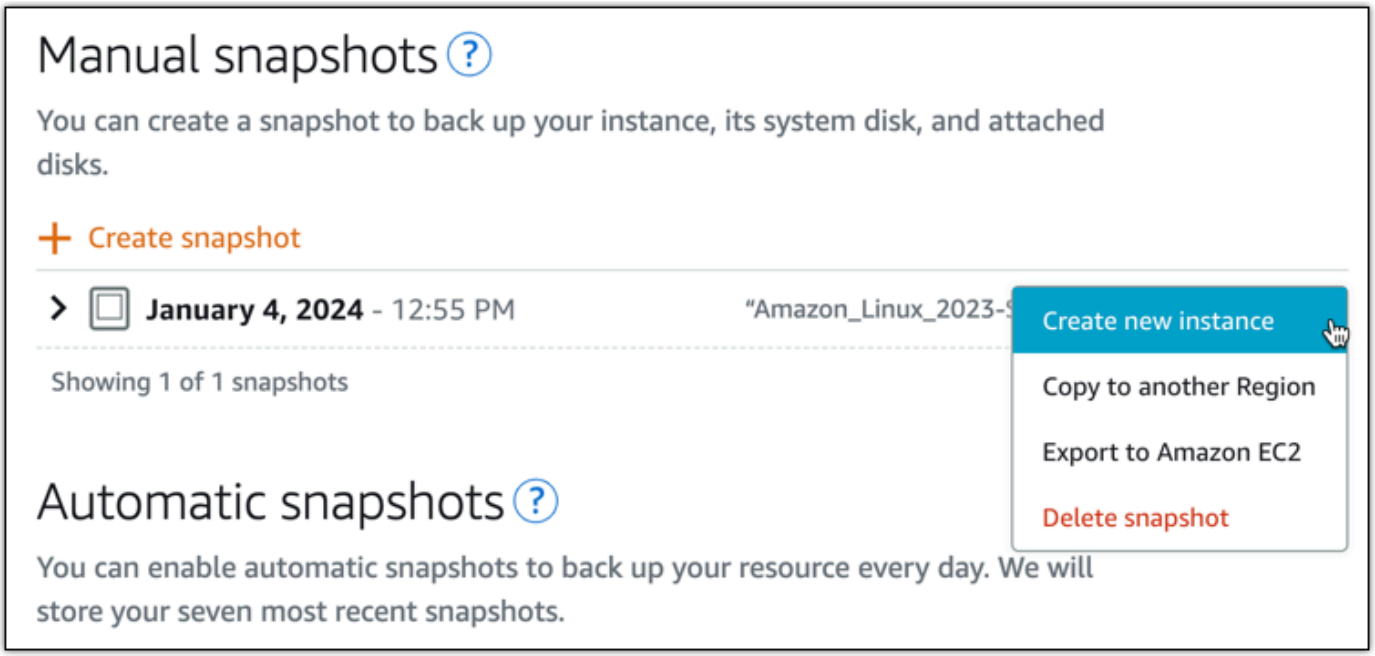


从快照创建 Lightsail 实例

在 Lightsail 中创建快照后，您可以根据该快照创建新实例。您可以更改新实例的属性，例如实例大小和网络类型（双堆栈或 IPv6仅限）。新实例将包含系统磁盘以及添加的任何附加块存储磁盘。

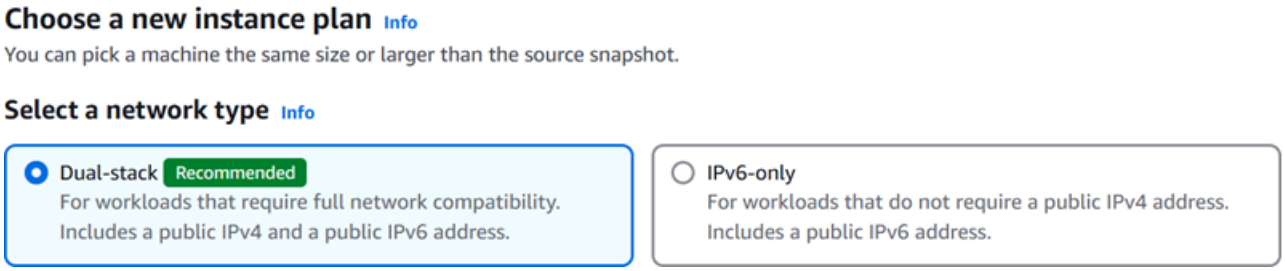
您必须拥有实例的快照，然后才能从该快照再创建一个实例。有关更多信息，请参阅 使用快照备份 Linux/Unix Lightsail 实例或 创建你的 Lightsail Windows Server 实例的快照。

1. 在 Lightsail 控制台上，选择要创建新实例快照的实例。
2. 选择 Snapshots（快照）选项卡。
3. 在手动快照部分中，选择快照旁边的操作菜单图标（⋮），然后选择创建新实例。



4. 从快照创建实例页面打开。选择要使用的可选设置。例如，您可以更改可用区、添加启动脚本或更改连接到实例的方式。
5. 为新实例选择计划（或捆绑包）。您可以选择创建使用双堆栈（IPv4 和 IPv6）实例计划或 IPv6 仅限计划的实例。您还可以选择比原始实例更大的捆绑包大小。有关 IPv6仅限实例计划的更多信息，请参阅为 IPv6 Lightsail 实例配置仅限网络连接。

> **Note**
>
> 您无法创建使用小于原始实例的捆绑包大小的实例。



6. 输入实例的名称。

   资源名称：

   - 在你的每个 Lightsail 账户 AWS 区域 中必须是唯一的。
   - 必须包含 2–255 个字符。
   - 必须以字母数字字符作为开头和结尾。
   - 可以包括字母数字字符、句点、连字符和下划线。

7. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

   a. 对于密钥，输入标签密钥。

   b. （可选）在“值”中，输入标签值。

8. 选择创建实例。

   Lightsail 会打开管理页面，您可以在其中管理您的新实例。

> **Important**
>
> 原始实例中的自定义防火墙规则不会复制到您通过快照创建的新实例。只有默认规则会复制到新实例。有关更多信息，请参阅默认实例防火墙规则。

通过快照扩大 Lightsail 实例、存储空间或数据库的大小

发生了此情况。您的云项目不断增长，您现在需要更多计算能力！我们可以帮助您做到这一点。要扩大 Lightsail 实例、块存储磁盘或数据库的大小，请创建资源快照，然后使用该快照创建该资源的更大新版本。

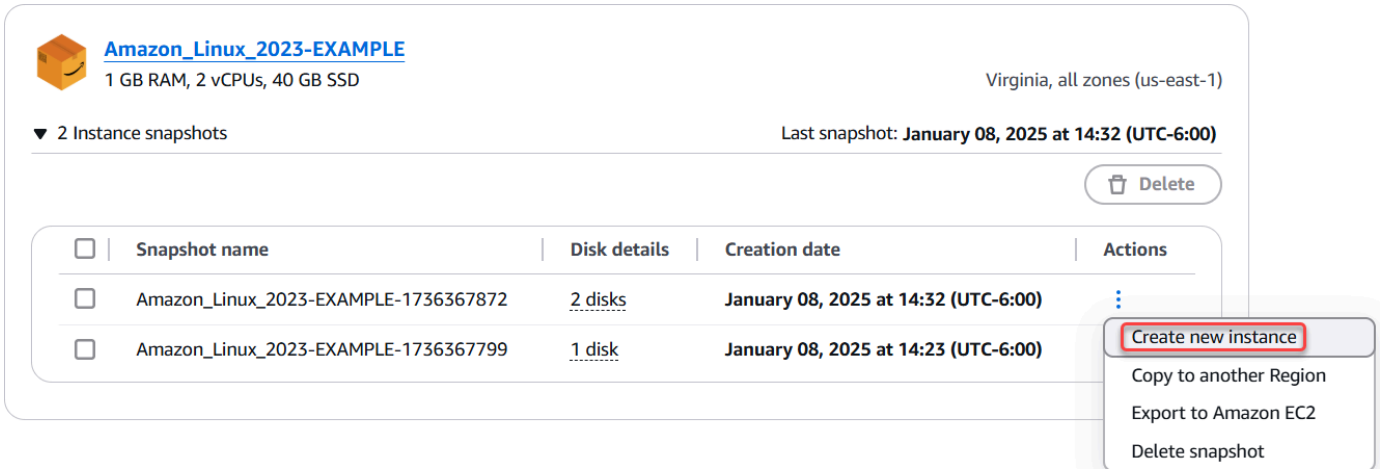
> **Note**
>
> 您无法使用比原始资源更小的计划大小从快照创建资源。例如，您无法从 8 GB 实例创建 2 GB 实例。
>
> 当您停止和启动实例时，在创建实例时分配给您的实例的默认公有 IPv4 地址将发生变化。您可以选择创建静态 IPv4 地址并将其附加到您的实例。使用静态 IP 地址，您可以快速将地址重新映射到您的账户中的另一个实例，从而屏蔽实例或软件故障。或者，您可以在域的 DNS 记录中指定静态 IP 地址，以使域指向您的实例。有关更多信息，请参阅 IP 地址。

先决条件

你需要一张 Lightsail 实例、块存储磁盘或数据库的快照。有关更多信息，请参阅快照。

创建您的资源

1. 登录 Lightsail 控制台。
2. 选择 Snapshots（快照）选项卡。
3. 找到要使用其快照创建更大的新资源的 Lightsail 资源，然后选择右箭头展开快照列表。
4. 选择要使用的快照旁边的省略号图标，然后选择创建新实例。



5. Create（创建）页面有多种可选择的可选设置。例如，您可以更改可用区。对于实例，您可以添加一个启动脚本，或者更改用于连接该实例的 SSH 密钥。

   您可以接受所有默认值，然后转到下一步。

6. 为新资源选择计划（或包）。目前，您可以根据需要，选择大于原始资源的捆绑大小。

   > **Note**
   >
   > 您不能使用小于原始资源的计划大小创建资源。小于原始资源的包选项将不可用。

7. 输入实例的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

8. 选择创建。

   Lightsail 会将您带到新资源的管理页面，然后您就可以开始管理它了。

使用 Lightsail 快照创建更大的实例、块存储磁盘或数据库 AWS CLI

发生了此情况。您的云项目不断增长，您现在需要更多计算能力！我们可以帮助您做到这一点。你可以在 Lightsail 控制台中执行所有操作，也可以使用 AWS Command Line Interface (AWS CLI) 来完成。

我们将向您展示如何拍摄当前 Lightsail 实例的快照，并根据该快照创建具有所需计算能力的新的、更大的实例。

> **Note**
>
> 目前，我们不支持通过快照创建小型实例（或包）。您只能创建相同大小的实例或更大的实例。

先决条件

1. 首先，如果您还没有，则需要安装 AWS CLI。要了解更多信息，请参阅安装 AWS Command Line Interface。务必配置 AWS CLI。
2. 您还需要使用在其中工作的实例的快照。要了解更多信息，请参阅创建 Linux 或 Unix 实例的快照。

步骤 1：获取您的快照名称

这看似显而易见，但您需要先获取您的快照名称，然后再执行此 AWS CLI 命令以创建大型实例。好消息是可轻松获取快照名称。

1. 在中 AWS CLI，键入以下内容。

```
aws lightsail get-instance-snapshots
```

您应该可以看到类似于如下所示的输出内容。

```
{
    "instanceSnapshots": [
        {
            "fromInstanceName": "WordPress-512MB-EXAMPLE",
            "name": "WordPress-512MB-EXAMPLE-system-1234567891011",
            "sizeInGb": 20,
            "resourceType": "InstanceSnapshot",
            "fromInstanceArn":
            "arn:aws:lightsail:us-
east-1:123456789101:Instance/86f49ee4-26cc-4802-9b0d-12345EXAMPLE",
            "state": "available",
```

```
            "arn": "arn:aws:lightsail:us-east-1:123456789101:InstanceSnapshot/
c87acb5f-851e-4fbc-94f1-12345EXAMPLE",
            "fromBundleId": "nano_1_0",
            "fromBlueprintId": "wordpress_4_6_1",
            "createdAt": 1480898073.653,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        }
    ]
}
```

2. 将名称值复制到您可在稍后获取该值的某个位置。这是您将在 AWS CLI 命令中使用的 `--instance-snapshot-name` 值。

步骤 2：选择套装

包实际上只是您的实例的定价计划和配置。例如，基于 Linux 的中型包的每月费用为 24 USD，并拥有 4.0GB RAM、80GB SSD 存储等。

如果您开始时使用的是较小的包，并且需要更多计算能力，则您可能需要升级到较大的包。有关更多信息，请参阅从快照创建更大的实例、数据块存储磁盘或数据库。

> **Important**
>
> 您无法从快照调整为小型包。如果您要创建小型包，则必须重新开始。

1. 键入以下 AWS CLI 命令。

```
aws lightsail get-bundles
```

您的输出应类似于以下内容。

```
{
    "bundles": [
        {
            "price": 5.0,
            "cpuCount": 2,
            "diskSizeInGb": 20,
```

```
            "bundleId": "nano_3_0",
            "instanceType": "nano",
            "isActive": true,
            "name": "Nano",
            "power": 298,
            "ramSizeInGb": 0.5,
            "transferPerMonthInGb": 1024,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ],
            },
        {
            "price": 7.0,
            "cpuCount": 2,
            "diskSizeInGb": 40,
            "bundleId": "micro_3_0",
            "instanceType": "micro",
            "isActive": true,
            "name": "Micro",
            "power": 500,
            "ramSizeInGb": 1.0,
            "transferPerMonthInGb": 2048,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ],
            },
        {
            "price": 12.0,
            "cpuCount": 2,
            "diskSizeInGb": 60,
            "bundleId": "small_3_0",
            "instanceType": "small",
            "isActive": true,
            "name": "Small",
            "power": 1000,
            "ramSizeInGb": 2.0,
            "transferPerMonthInGb": 3072,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ],
            },
        {
            "price": 24.0,
            "cpuCount": 2,
```

```
            "diskSizeInGb": 80,
            "bundleId": "medium_3_0",
            "instanceType": "medium",
            "isActive": true,
            "name": "Medium",
            "power": 2000,
            "ramSizeInGb": 4.0,
            "transferPerMonthInGb": 4096,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ],
            },
        {
            "price": 44.0,
            "cpuCount": 2,
            "diskSizeInGb": 160,
            "bundleId": "large_3_0",
            "instanceType": "large",
            "isActive": true,
            "name": "Large",
            "power": 3000,
            "ramSizeInGb": 8.0,
            "transferPerMonthInGb": 5120,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ],
            },
    ]
}
```

2. 找到所需包的 bundleId 值。有关更多信息，请参阅 Lightsail 定价。

第 3 步：编写 AWS CLI 命令并创建新实例

现在，您已有参数值，已准备好编写和执行您的命令来创建实例！

1. 键入以下内容。

```
aws lightsail create-instances-from-snapshot --instance-names
 MyNewInstanceFromSnapshot --availability-zone us-east-1a --instance-snapshot-name
 WordPress-512MB-EXAMPLE-system-1234567891011 --bundle-id medium_1_0
```

您的输出应类似于以下内容。

```
{
    "operations": [
        {
            "status": "Started",
            "resourceType": "Instance",
            "isTerminal": false,
            "statusChangedAt": 1486863990.961,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "operationType": "CreateInstance",
            "resourceName": "MyNewInstanceFromSnapshot",
            "id": "30fec45e-e7d7-4e18-96c8-12345EXAMPLE",
            "createdAt": 1486863989.784
        }
    ]
}
```

> **Note**
>
> 您也可以使用返回区域和可用区的列表 AWS CLI。只需键入 `aws lightsail get-regions --include-availability-zones` 以利用您的 `get-regions` 请求返回可用区的列表。

2. 现在，在 Lightsail 控制台中打开您的新实例并开始对其进行修改。

后续步骤

通过快照创建新实例后，以下是您接下来可执行的一些操作：

- 如果您不再使用旧实例，则可能需要将其删除。您可以使用 Lightsail 控制台或删除实例 CLI 命令来执行此操作。
- 如果您不需要旧快照，则可能需要将其删除。你可以使用 Lightsail 控制台或 CL delete-instance-snapshot l 命令来执行此操作。
- 如果您已将一个静态 IP 地址附加到旧实例，则可能需要保留该地址并将其附加到新实例。可使用控制台执行此操作。请参阅创建静态 IP 并将其附加到实例。

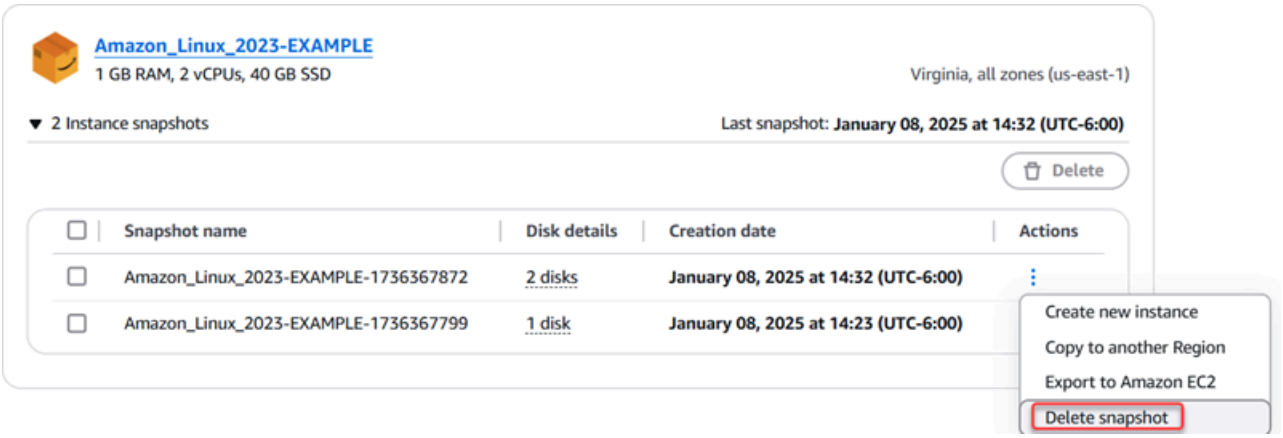
删除未使用的 Lightsail 快照以避免按月收费

如果您不再需要实例、数据库和磁盘快照，请删除 Amazon Lightsail 中的实例、数据库和磁盘快照，以免产生月度费用。

删除单个快照

> **Important**
>
> 这是一个永久性操作，无法撤消。在删除快照时，快照上的所有数据将会丢失。

1. 在 Lightsail 控制台上，选择 “快照” 选项卡。
2. 找到要删除其快照的 Lightsail 资源，然后选择右箭头展开该资源的可用快照列表。
3. 选择要删除的快照旁的操作菜单图标 (⋮)，然后选择 Delete snapshot (删除快照)。

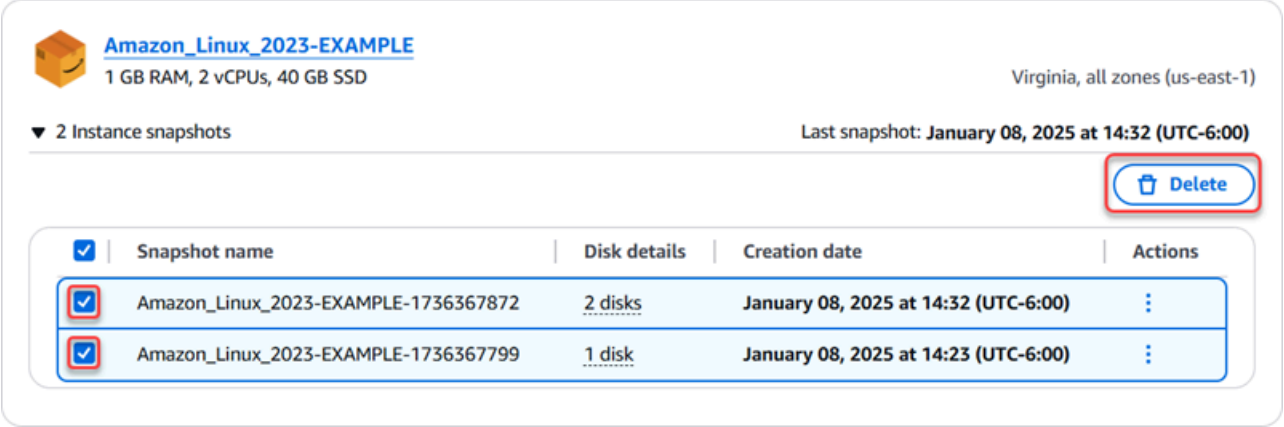


4. 选择 Yes (是) 以确认您要删除该快照。

删除多个快照

> **Important**
>
> 这是一个永久性操作，无法撤消。在删除快照时，快照上的所有数据将会丢失。

1. 在 Lightsail 主页上，选择 “快照”。
2. 找到要删除其快照的 Lightsail 资源，然后展开该资源的快照部分。
3. 选择要删除的资源的快照，然后选择删除。



4. 选择 Yes (是) 以确认您要删除这些快照。

将 Lightsail 快照复制到各处 AWS 区域

在 Amazon Lightsail 中，您可以将实例快照和块存储磁盘快照从一个复制 AWS 区域 到另一个区域，或者复制到同一区域。例如，如果您在一个区域中创建和配置了资源，但随后决定使用其他区域更合适，则可以在区域之间复制快照。您可能还会决定跨多个区域复制您的资源。

先决条件

创建要复制的 Lightsail 实例或块存储磁盘的快照。有关更多信息，请参阅下列指南之一：

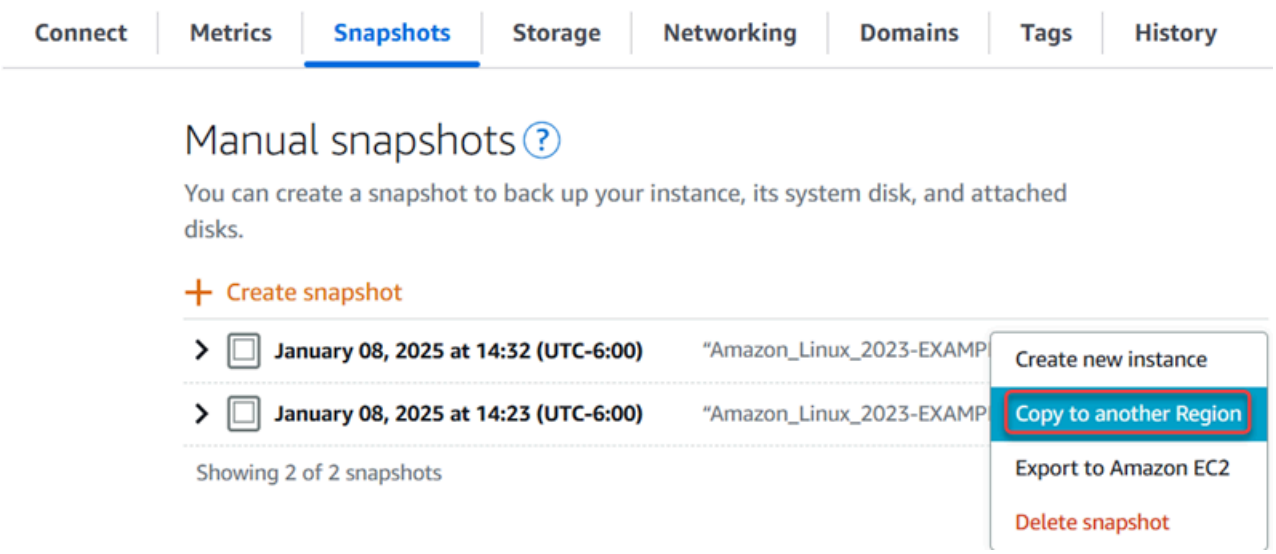
- 创建 Linux 或 Unix 实例的快照
- 创建 Windows Server 实例的快照
- 创建数据块存储磁盘的快照

复制快照

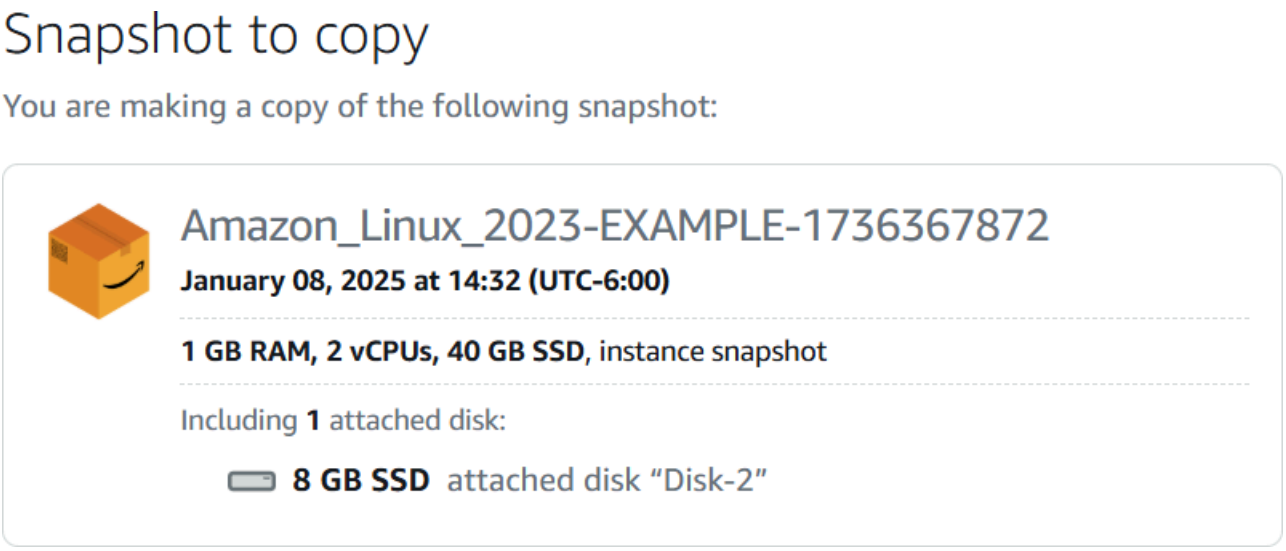
您可以将 Lightsail 实例快照和块存储磁盘快照从一个复制 AWS 区域 到另一个或在同一区域内复制。

复制 Lightsail 快照

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，选择 “快照” 选项卡。
3. 找到要复制的实例或数据数据块存储磁盘，然后展开节点以查看该资源的可用快照。
4. 针对所需快照选择菜单图标 (⋮)，然后选择复制到其他区域。



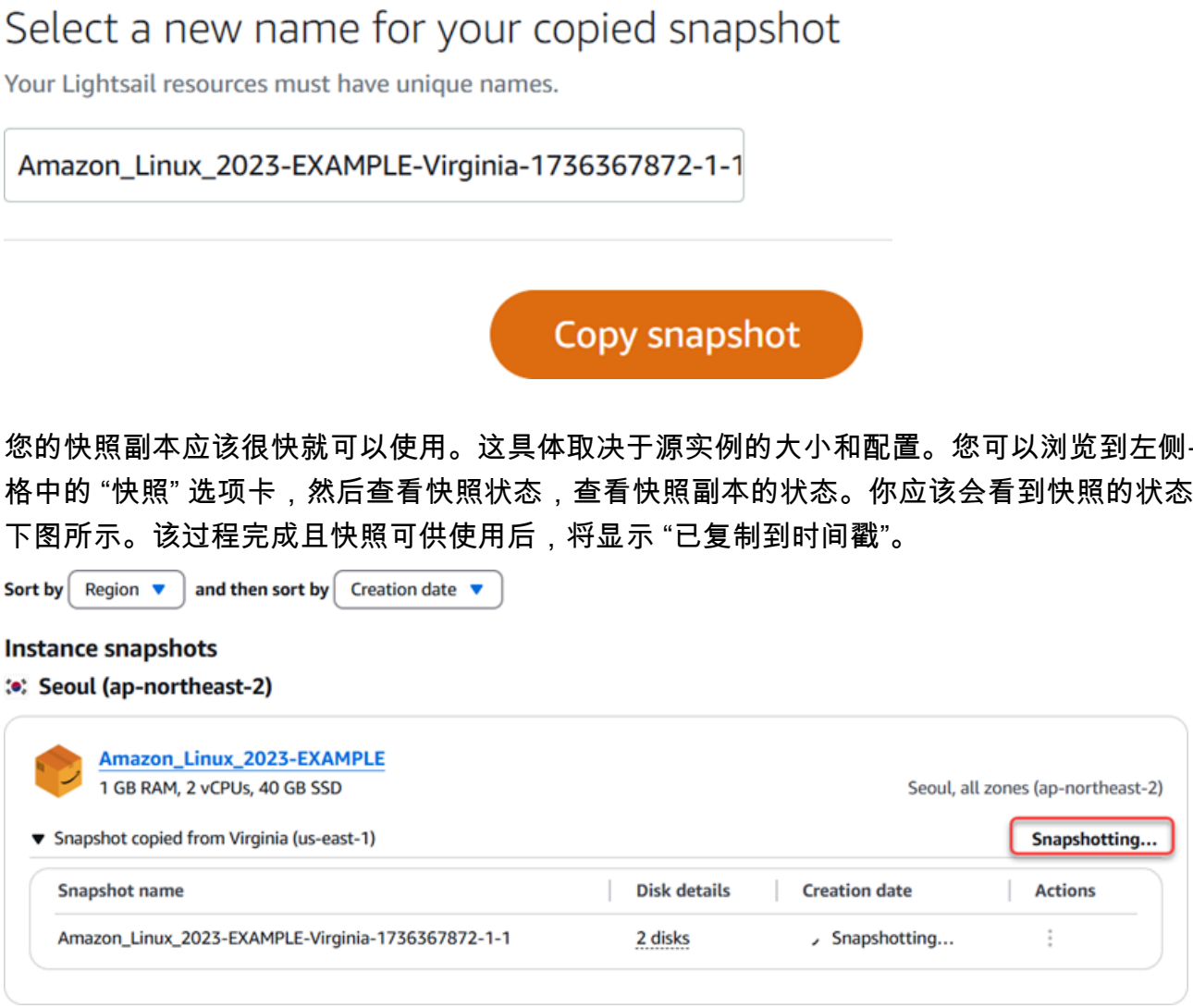
5. 在 Copy a snapshot (复制快照) 页面的 Snapshot to copy (要复制的快照) 部分中，确认显示的快照详细信息与源实例或数据数据块存储磁盘的规格相匹配。



6. 在页面的选择区域部分中，为快照副本选择区域。
7. 输入快照副本的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
8. 选择复制快照。



您的快照副本应该很快就可以使用。这具体取决于源实例的大小和配置。您可以浏览到左侧导航窗格中的 “快照” 选项卡，然后查看快照状态，查看快照副本的状态。你应该会看到快照的状态... 如下图所示。该过程完成且快照可供使用后，将显示 “已复制到时间戳”。

后续步骤

在 Lightsail 中将快照复制到另一个区域后，您可以执行以下几个额外步骤：

- 在复制的快照可用之后，即可从其中创建新实例。有关更多信息，请参阅从快照创建实例。
- 如果不再需要源快照，则可以将其删除。否则，您将需要为存储快照付费。

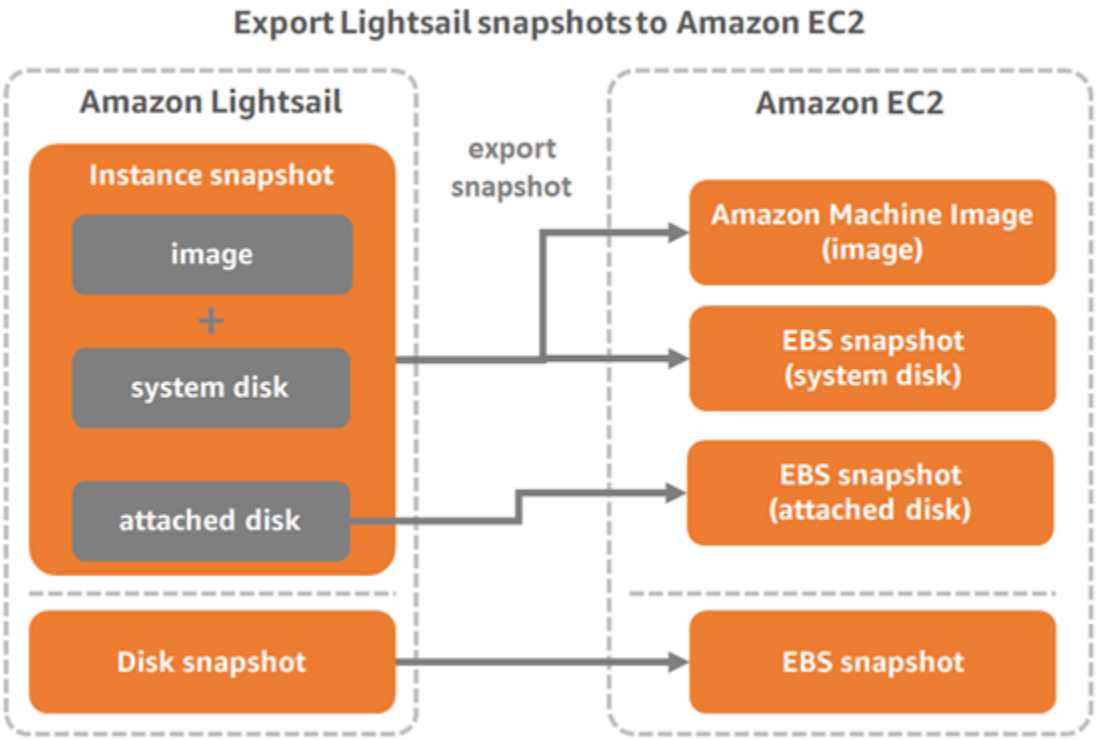
了解如何将 Lightsail 快照导出到亚马逊 EC2

您可以将 Lightsail 快照导出到亚马逊 EC2，利用导出的快照创建 EC2 资源，选择兼容的 EC2 实例类型，连接实例，以及保护从 Lightsail 快照创建的 EC2实例。 EC2 可以使用以下方法之一将 Amazon Lightsail 实例和块存储磁盘快照导出到亚马逊弹性计算云 EC2 (Amazon)：

- Lightsail 控制台。有关更多信息，请参阅将快照导出到 Amazon EC2。
- Lightsail API、 AWS Command Line Interface (AWS CLI) 或。 SDKs有关更多信息，请参阅 Lightsail API 文档中的ExportSnapshot 操作或文档中的导出快照命令。 AWS CLI

您可以导出实例快照和数据块存储磁盘快照。但是，cPanel 和 WHM（CentOS 7）实例的快照无法导出到亚马逊。 EC2快照将 AWS 区域 从 Lightsail 导出到亚马逊。 EC2要将快照导出到其他区域，请先将快照复制到 Lightsail 中的其他区域，然后执行导出。有关更多信息，请参阅将快照从一个复制 AWS 区域 到另一个快照。

导出 Lightsail 实例快照会导致亚马逊系统映像 (AMI) 和亚马逊弹性区块存储 (Amazon EBS) 快照在亚马逊中创建。 EC2这是因为 Lightsail 实例由镜像和系统磁盘组成，为了提高管理效率，它们在 Lightsail 控制台中作为单个实例实体组合在一起。如果在创建快照时，源 Lightsail 实例附有一个或多个块存储磁盘，则将在 Amazon 中为每个连接的磁盘创建额外的 EBS 快照。 EC2导出 Lightsail 块存储磁盘快照会导致在亚马逊中创建单个 EBS 快照。 EC2亚马逊上所有导出的资源 EC2 都有自己独特的唯一标识符，这些标识符与 Lightsail 对应的资源不同。



> **Note**
>
> Lightsail 使用 AWS Identity and Access Management (IAM) 服务相关角色 (SLR) 将快照导出到亚马逊。 EC2有关更多信息 SLRs，请参阅服务关联角色。

导出过程可能需要一段时间。这取决于源实例或数据块存储磁盘的大小和配置。使用 Lightsail 控制台中的 “导出” 部分来跟踪您的导出状态。有关更多信息，请参阅 在 Lightsail 中跟踪快照导出状态。

根据导出的 Lightsail 快照创建亚马逊 EC2 资源

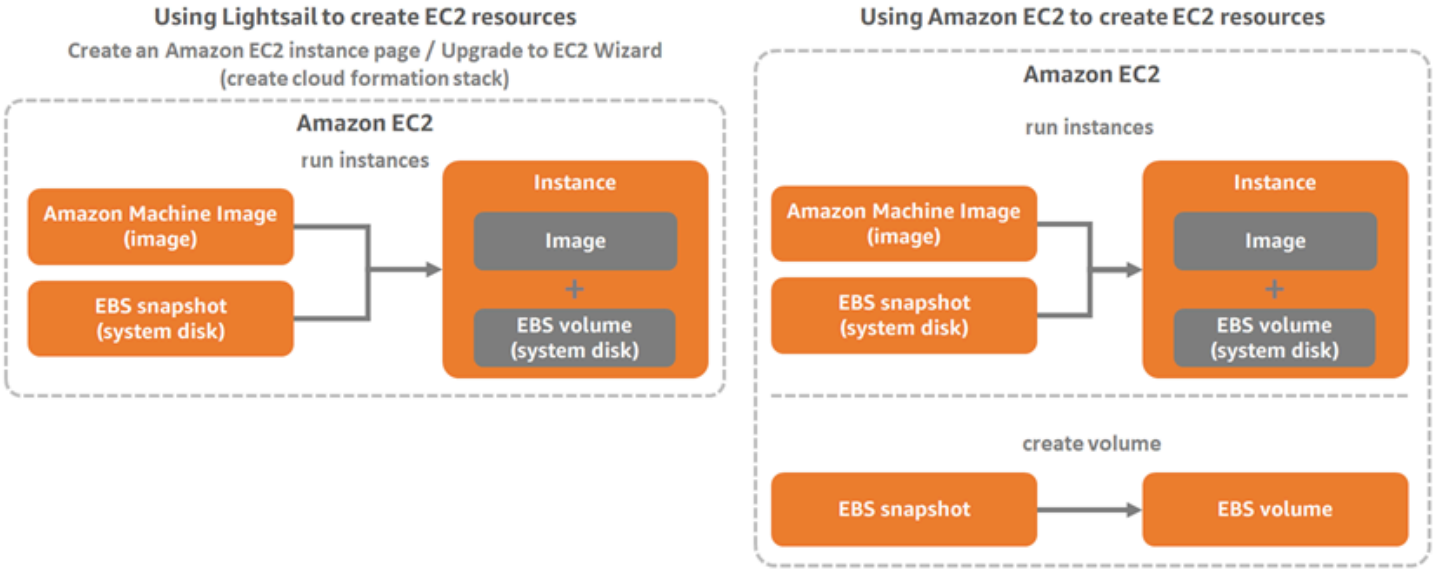
导出 Lightsail 快照并在亚马逊上线 EC2（作为 AMI、EBS 快照或两者兼而有之）后，您可以使用以下方法之一从该快照创建亚马逊 EC2 资源：

- Light sail 控制台中的 “创建亚马逊 EC2 实例” 页面，也称为 “升级到亚马逊 EC2 向导”。有关更多信息，请参阅使用导出的快照创建 Amazon EC2 实例。
- Lightsail API AWS CLI，或。 SDKs有关更多信息，请参阅 Lightsail API 文档中的CreateCloudFormationStack 操作或文档中的create-cloud-formation-stack AWS CLI 命令。

> **Note**
>
> Lightsail 可用于根据导出的 EC2 实例快照创建 Amazon 实例，但不能用于根据导出的块存储磁盘快照创建 EBS 卷。为此，您必须使用亚马逊 EC2 控制台、API 或 AWS CLI。有关更多信息，请参阅从导出的磁盘快照创建 Amazon EBS 卷。

- 亚马逊 EC2 控制台、亚马逊 EC2 API 或 SDKs。 AWS CLI有关更多信息，请参阅 Amazon EC2 文档中的使用启动实例向导启动实例或从快照恢复 Amazon EBS 卷。

从导出的 EC2 实例快照（AMI 和 EBS 快照）创建 Amazon EC2 实例会导致启动单个实例。通过导出 Lightsail 实例快照生成的 AMI 和 EBS 快照会自动链接在一起形成 EC2实例。导出的 Lightsail 块存储磁盘快照（EBS 快照）可用于在亚马逊创建 EBS 卷。 EC2



> **Note**
>
> Lightsail 使用 CloudFormation 堆栈在中创建实例及其相关资源。 EC2有关更多信息，请参阅 Lights ail 的AWS CloudFormation 堆栈。

从导出的快照创建 Amazon EC2 资源的过程可能需要一段时间。这具体取决于源实例的大小和配置。使用 Lightsail 控制台中的 “导出” 部分来跟踪您的导出状态。有关更多信息，请参阅在 Lightsail 中跟踪快照导出状态。

选择 Amazon EC2 实例类型

与 Lightsail 相比，亚马逊 EC2 提供的实例选项范围更广。在 Amazon 中 EC2，您可以选择针对计算 (C5)、内存 (R5) 或两者兼而有之（T3 和 M5）进行了优化的实例类型。Lightsail 在 “创建亚马逊 EC2 实例” 页面中提供了这些选项；但是，如果您使用 Ama EC2 zon 从导出的快照创建新实例，则可以使用更多实例类型选项。有关 EC2实例类型的更多信息，请参阅 Amazon EC2 文档中的实例类型。

在根据导出的快照创建 EC2 实例之前，请务必了解 Lightsail 和 Amazon 之间的实例价格差异。 EC2有关实例定价的更多信息，请参阅 Lightsail 定价和亚马逊定 EC2价页面。

Lightsail 和 Amazon EC2 实例类型兼容性

某些 Lightsail 实例与当前一代的 EC2 实例类型（T3、M5、C5 或 R5）不兼容，因为它们未启用增强联网功能。如果您的源 Lightsail 实例不兼容，则在根据导出的快照创建实例时，您需要选择上一代实例类型（T2、M4、C4 或 R4）。 EC2 在使用 Lightsail 控制台中的 “创建亚马逊 EC2 实 EC2例” 页面创建实例时，会向您显示这些选项。

要在源 Lightsail 实例不兼容时使用最新一代 EC2 的实例类型，您需要使用上一代 EC2 实例类型（T2、M4、C4 或 R4）创建新实例，更新网络驱动程序，然后将该实例升级到所需的当前一代实例类型。有关更多信息，请参阅 Amazon EC2 实例的增强联网。

Connect 到亚马逊 EC2 实例

您可以像连接到 Lightsail EC2 实例一样连接到亚马逊实例。这意味着，对 Linux 和 Unix 实例使用 SSH，对 Windows Server 实例则使用 RDP。但是，基于浏览器的SSH/RDP client that you might have used in the Lightsail console might not be available in Amazon EC2 depending on the browser version that you're using, so you may need to configure your own SSH/RDP客户端可以连接到您的 EC2 实例。有关更多信息，请参阅以下指南：

- 连接到根据 Lightsail 快照创建的亚马逊 EC2 Linux 或 Unix 实例
- 连接到根据 Lightsail 快照创建的亚马逊 EC2 Windows 服务器实例

保护 Amazon EC2 实例

根据导出的 Lightsail 快照创建 EC2 实例后，您可能需要执行一些操作来提高新实例的安全性。根据您的 EC2 实例的操作系统，操作会有所不同。

保护亚马逊中的 Linux 和 Unix 实例 EC2

如果您使用 EC2 （ EC2 控制台、 EC2 API、for 或 for EC2 ） EC2 从导出的快照在亚马逊中创建 Linux 或 SDKs Unix 实例 EC2，则新 EC2 实例可能包含来自 Lightsail 服务的剩余 SSH 密钥。 AWS CLI 我们建议您删除这些密钥，以更好地保护新实例。

有关更多信息，请参阅保护从 Lightsail 快照创建的 Amazon EC2 Linux 或 Unix 实例。

保护亚马逊中的 Windows 服务器实例 EC2

通过导出的快照在亚马逊 EC2 中创建 Windows Server 实例后，您 AWS 账户中任何有权访问 Lightsail 的用户都 EC2 将能够检索首先分配给源实例的默认管理员密码，该密码也是新 EC2 实例的密码。为了提高安全性，我们建议您更改 Amazon EC2 实例的默认管理员密码（如果您尚未这样做）。

有关更多信息，请参阅保护根据 Lightsail 快照创建的亚马逊 EC2 Windows 服务器实例。

将 Lightsail 快照导出到亚马逊 EC2

您可以将 Amazon Lightsail 实例和块存储磁盘快照导出到亚马逊弹性计算云 (亚马 EC2逊)。导出 Lightsail 实例快照会导致亚马逊系统映像 (AMI) 和亚马逊弹性区块存储 (Amazon EBS) 快照在亚马逊中创建。 EC2这是因为 Lightsail 实例由镜像和系统磁盘组成，为了提高管理效率，它们在 Lightsail 控制台中作为单个实例实体组合在一起。如果在创建快照时，源 Lightsail 实例附有一个或多个块存储磁盘，则会在 Amazon 中为每个连接的磁盘创建额外的 EBS 快照。 EC2

导出 Lightsail 块存储磁盘快照会导致在亚马逊中创建单个 EBS 快照。 EC2亚马逊上所有导出的资源 EC2 都有自己独特的唯一标识符，这些标识符与 Lightsail 对应的资源不同。

本指南介绍如何导出 Lightsail 快照、跟踪导出状态，以及导出的快照在亚马逊上线后的后续步骤 EC2（作为 AMI、EBS 快照或两者兼而有之）。

> **Important**
>
> 我们建议在完成本指南中的步骤之前，先熟悉 Lightsail 的导出流程。有关更多信息，请参阅将快照导出到 Amazon EC2。

内容

- 服务相关角色和导出 Lightsail 快照所需的 IAM 权限
- 先决条件
- 将 Lightsail 快照导出到亚马逊 EC2
- 跟踪导出状态

服务相关角色和导出 Lightsail 快照所需的 IAM 权限

Lightsail 使用 AWS Identity and Access Management (IAM) 服务相关角色 (SLR) 将快照导出到亚马逊。 EC2有关更多信息 SLRs，请参阅服务关联角色。

您可能还需要在 IAM 中配置以下额外的权限，具体取决于执行快照导出操作的用户：

- 如果 Amazon 账户根用户来执行导出操作，则继续执行本指南中的“先决条件”部分。账户根用户已具有执行快照导出操作所需的权限。
- 如果 IAM 用户将执行导出，则 AWS 账户管理员必须向该用户添加以下策略。有关如何更改用户权限的更多信息，请参阅 IAM 文档中的更改 IAM 用户的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
lightsail.amazonaws.com/AWSServiceRoleForLightsail*",
            "Condition": {"StringLike": {"iam:AWSServiceName":
 "lightsail.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/
lightsail.amazonaws.com/AWSServiceRoleForLightsail*"
        }
    ]
}
```

先决条件

创建要导出到亚马逊的 Lightsail 实例或块存储磁盘的快照。 EC2有关更多信息，请参阅下列指南之一：

- 创建 Linux 或 Unix 实例的快照
- 创建 Windows Server 实例的快照
- 创建数据块存储磁盘的快照

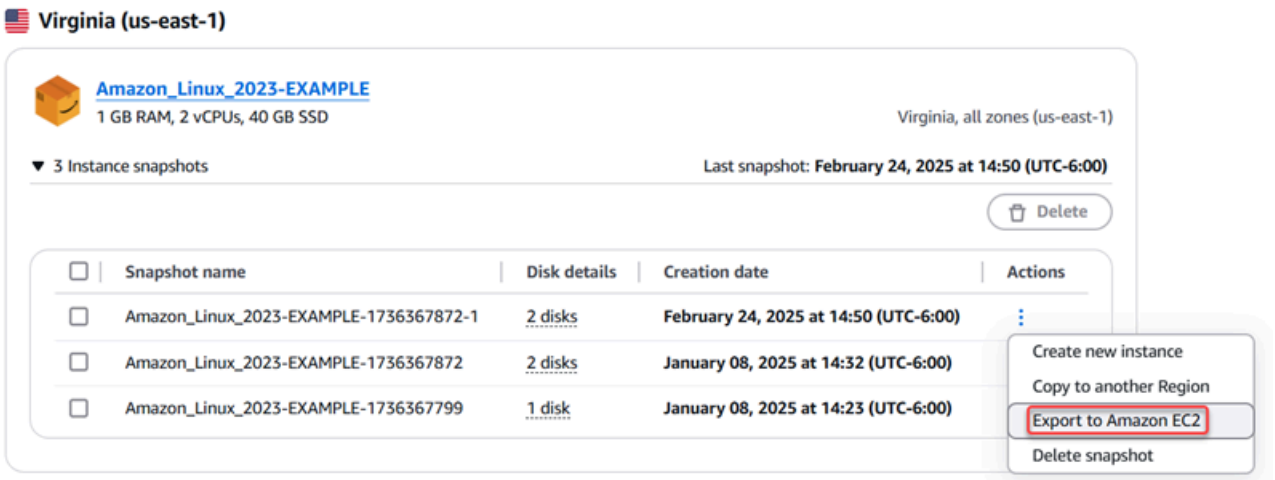
将 Lightsail 快照导出到亚马逊 EC2

将快照导出到亚马逊的最有效方法 EC2 是使用 Lightsail 控制台。你也可以使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或导出快照。 SDKs有关更多信息，请参阅 Lightsail API 文档中的ExportSnapshot 操作或文档中的导出快照命令。 AWS CLI

> **Note**
>
> 快照将 AWS 区域 从 Lightsail 导出到亚马逊。 EC2要将快照导出到其他区域，请先将快照复制到 Lightsail 中的其他区域，然后执行导出。有关更多信息，请参阅将快照从一个复制 AWS 区域 到另一个快照。

将 Lightsail 快照导出到亚马逊 EC2

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择快照。
3. 找到要导出的实例或数据块存储磁盘，然后展开节点以查看该资源的可用快照。
4. 选择所需快照的 “操作” 菜单，然后选择 “导出到亚马逊” EC2。



> **Note**
>
> cPanel 和 WHM (CentOS 7) 实例的快照无法导出到亚马逊。 EC2

5. 查看提示符下显示的重要详细信息。
6. 如果您同意向亚马逊出口 EC2，请选择 “是”，继续开始流程。

   导出过程可能需要一段时间。这取决于源实例或数据块存储磁盘的大小和配置。使用 Lightsail 控制台中的 “导出” 部分来跟踪您的导出状态。有关更多信息，请参阅 在 Lightsail 中跟踪快照导出状态。

跟踪导出状态

在 Lightsail 控制台的 “导出” 部分中跟踪您的导出状态。可以从 Lightsail 控制台所有页面的左侧导航窗格对其进行访问。有关更多信息，请参阅 在 Lightsail 中跟踪快照导出状态。

在导出中显示以下信息：

- 快照名称-源 Lightsail 快照的名称。
- 状态 — 导出的状态。这可以是 `In progress`、`Successful` 或 `Failed`。
- Export started (导出开始时间) – 开始导出快照的日期和时间。
- 来源详情-源 Lightsail 实例的规格，例如内存、处理和存储。
- 源实例名称 — 快照的源实例的名称。
- 快照类型 – Lightsail 快照的类型。类型可能是实例快照或磁盘快照。
- 创建快照 — 源 Lightsail 快照的创建日期和时间。

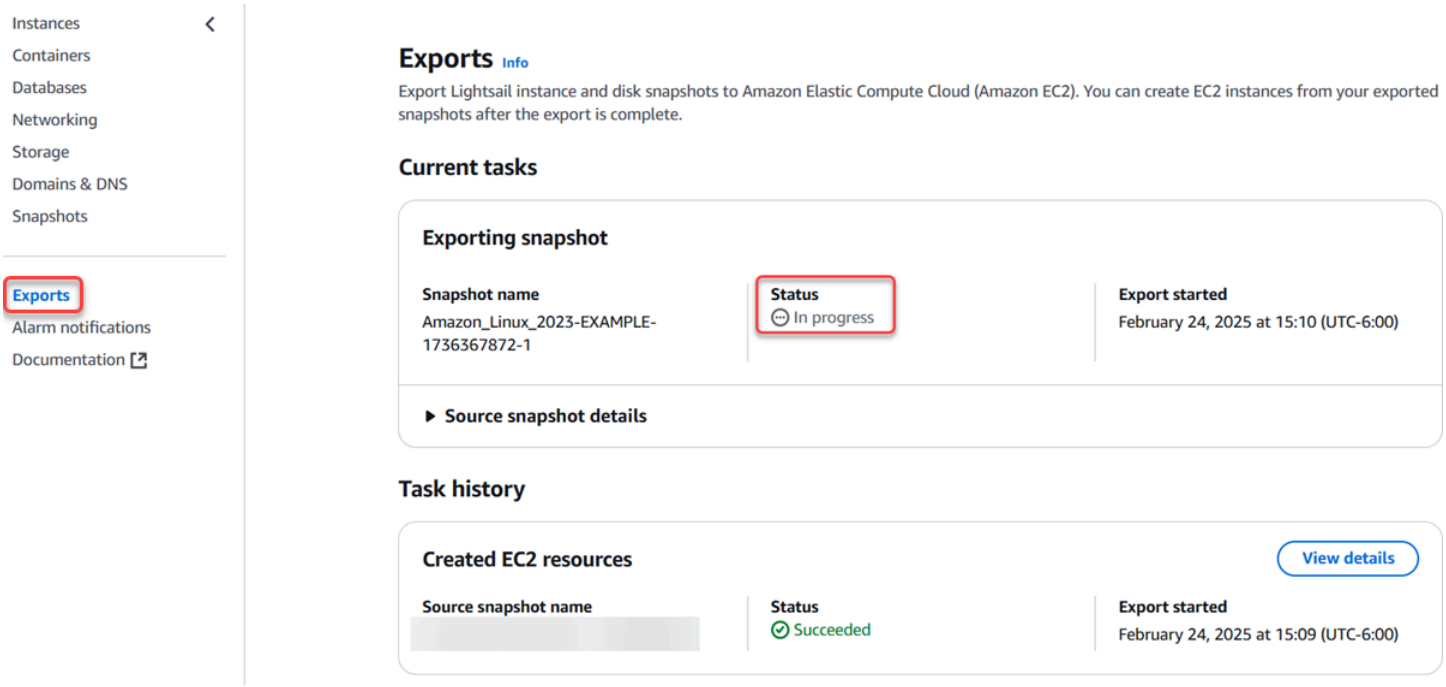
已完成导出的任务历史记录部分中将显示以下信息：

- 在中创建实例 EC2 — 选择此选项可 EC2 使用 Lightsail 控制台在亚马逊中创建新实例。有关更多信息，请参阅使用导出的快照创建 Amazon EC2 实例。
- 打开 EC2 — 选择此选项可使用 Amazon EC2 控制台从导出的快照创建新 EC2 资源。如果您导出了 Lightsail 块存储磁盘快照，则必须使用亚马逊 EC2 根据该快照（EBS 快照）创建 EBS 卷。有关更多信息，请参阅亚马逊 EC2 文档中的使用启动实例向导启动实例或从快照恢复 Amazon EBS 卷。

> **Note**
>
> 如果您不再需要源 Lightsail 快照，请将其删除。否则，您将需要为其付存储费。

在 Lightsail 中跟踪快照导出状态

在 Amazon Lightsail 控制台的“导出”部分，您可以跟踪将 Lightsail 快照导出到亚马逊的状态 EC2，或者使用导出的 EC2 实例快照创建新实例的状态。导出任务可能需要一段时间，具体取决于源实例或数据块存储磁盘的大小和配置。可以从 Lightsail 控制台所有页面的左侧导航窗格访问导@@ 出内容。



有关将 Lightsail 快照导出到亚马逊 EC2或使用导出的快照创建 EC2实例的更多信息，请参阅以下指南：

- 将快照导出到亚马逊 EC2

- 根据导出的快照创建 Amazon EC2 实例

根据导出的 Lightsail 快照创建亚马逊 EC2实例

导出 Lightsail 实例快照并在亚马逊上线 EC2 （作为 AMI 和 EBS 快照）后，您可以使用亚马 EC2 逊 Lightsail 控制台（也称为升级到亚马逊向导）中的创建亚马逊 EC2 实例页面，从快照创建亚马逊实例。 EC2 它会指导您完成 EC2 实例配置选项，例如选择符合您要求的 EC2 实例类型、配置安全组端口、添加启动脚本等。Lightsail 控制台中的向导简化了创建新 EC2 实例及其相关资源的过程。

> **Note**
>
> 要从导出的数据数据块存储磁盘快照创建 Amazon Elastic Block Store (Amazon EBS) 卷，请参阅从导出的磁盘快照创建 Amazon EBS 卷。

您也可以使用 Lightsail API 创建新 EC2 实例 AWS CLI、或。 SDKs有关更多信息，请参阅 Lightsail API 文档中的CreateCloudFormationStack 操作或文档中的create-cloud-formation-stack AWS CLI 命令。或者，如果您对亚马逊感到满意 EC2，则可以使用 EC2 控制台、亚马逊 EC2 API 或 SDKs。AWS CLI有关更多信息，请参阅亚马逊 EC2 文档中的使用启动实例向导启动实例或从快照恢复 Amazon EBS 卷。

> **Important**
>
> 我们建议在完成本指南中的步骤之前，先熟悉 Lightsail 的导出流程。有关更多信息，请参阅将快照导出到 Amazon EC2。

内容

- AWS CloudFormation Lightsail 的堆栈
- 先决条件
- 在 Lightsail EC2 控制台中访问 “创建亚马逊实例” 页面
- 创建一个 Amazon EC2 实例
- 跟踪您的新 Amazon EC2 实例的状态

AWS CloudFormation Lightsail 的堆栈

Lightsail 使用 AWS CloudFormation 堆栈来创建 EC2 实例及其相关资源。有关 Lightsail CloudFormation 堆栈的更多信息，AWS CloudFormation 请参阅 Lightsail 的堆栈。

可能需要在 IAM 中配置以下额外权限，具体取决于使用创建 A mazon EC2 实例页面创建 EC2 实例的用户：

- 如果 Amazon 账户根用户将创建 EC2 实例，请继续阅读本指南的先决条件部分。根用户已经拥有使用 Lightsail 创建 EC2 实例所需的权限。
- 如果 IAM 用户将创建 EC2 实例，则 AWS 账户管理员必须向该用户添加以下权限。有关如何更改用户权限的更多信息，请参阅 IAM 文档中的更改 IAM 用户的权限。
  - 用户需要以下权限才能使用 Lightsail 创建亚马逊 EC2 实例：

    > **Note**
    >
    > 这些权限允许创建 CloudFormation 堆栈。但是，如果创建失败，则回滚过程可能需要更多权限。缺乏权限可能会导致剩余资源无法在 Amazon 中回滚 EC2。如果发生这种情况，您可以前往 AWS CloudFormation 控制台手动删除 EC2 资源。有关更多信息，请参阅 Lightsail 的AWS CloudFormation 堆栈

    - ec2: DescribeAvailabilityZones
    - ec2: DescribeSubnets
    - ec2: DescribeRouteTables
    - ec2: DescribeInternetGateways
    - ec2: DescribeVpcs
    - 云层形成：CreateStack
    - 云层形成：ValidateTemplate
    - 我是：CreateServiceLinkedRole
    - 我是：PutRolePolicy
  - 如果用户要在安全组中为 EC2 实例配置端口，则需要以下权限：
    - ec2: DescribeSecurityGroups
    - ec2: CreateSecurityGroup
    - ec2: AuthorizeSecurityGroupIngress

- 如果用户在亚马逊创建 Windows 服务器实例，则需要以下权限 EC2：
  - ec2: DescribeKeyPairs
  - ec2: ImportKeyPair
- 如果用户是首次创建 Amazon EC2 实例，或者当虚拟私有云 (VPC) 无法完全配置时，则需要以下权限：
  - ec2: AssociateRouteTable
  - ec2: AttachInternetGateway
  - ec2: CreateInternetGateway
  - ec2: CreateRoute
  - ec2: CreateRouteTable
  - ec2: CreateSubnet
  - ec2: CreateVpc
  - ec2: ModifySubnetAttribute
  - ec2: ModifyVpcAttribute

先决条件

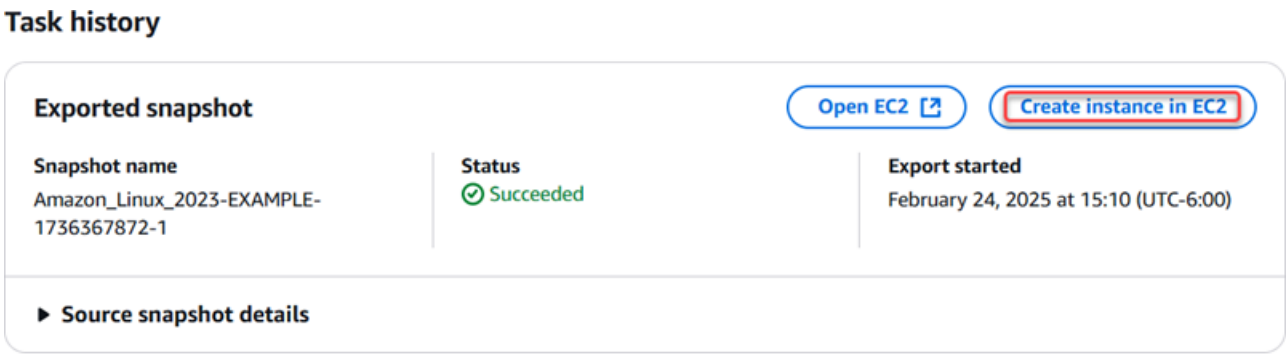
将 Lightsail 实例快照导出到亚马逊。 EC2有关更多信息，请参阅将快照导出到 Amazon EC2。

在 Lightsail EC2 控制台中访问 “创建亚马逊实例” 页面

只有成功将 EC2 实例快照导出到之后，才能从任务监视器访问 Lightsail 控制台中的 “创建亚马逊实例” 页面。 EC2

在 Lightsail 控制 EC2 台中访问 “创建亚马逊实例” 页面

1. 登录 Lightsail 控制台。
2. 从顶部导航窗格中选择 Task monitor（任务监控）图标。
3. 在任务历史记录部分找到已完成的实例快照导出，然后在中选择创建实例 EC2。



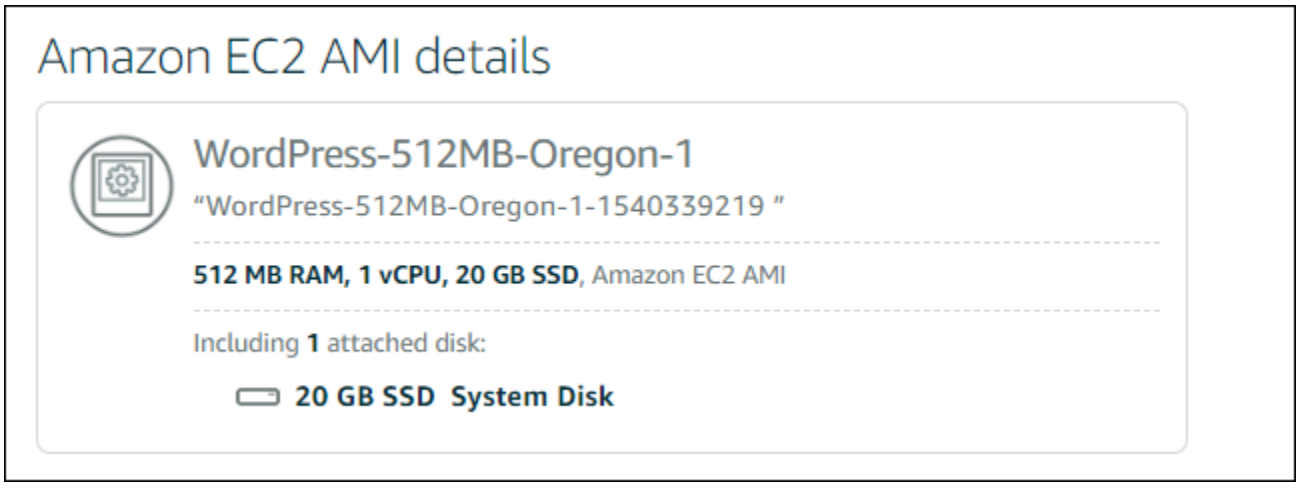
此时将出现 “创建 Amazon EC2 实例” 页面。继续阅读本指南的以下 “创建 Amazon EC2 实例” 部分，了解如何使用此页面配置和创建 EC2实例。

创建一个 Amazon EC2 实例

使用创建 Amazon EC2 实例页面创建 EC2 实例。要从导出的 Lightsail 快照创建多个 EC2 实例，请多次重复以下步骤，但要等到每个实例创建完毕后再创建下一个实例。

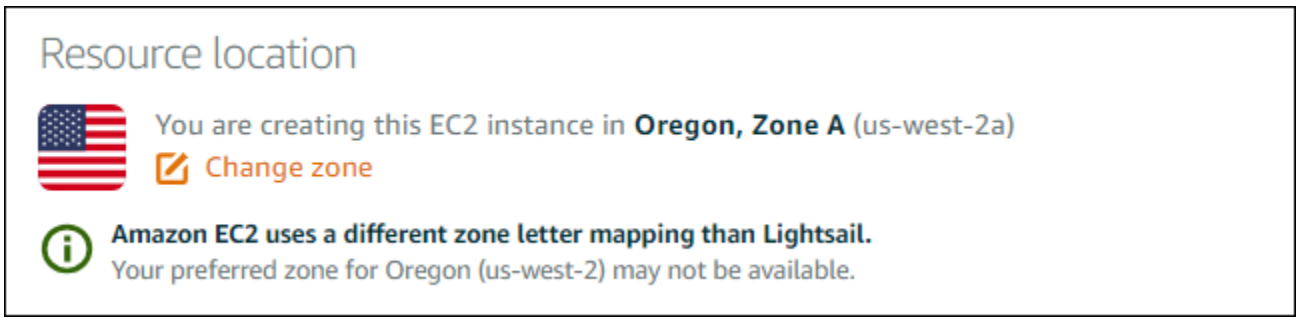
创建 Amazon EC2 实例

1. 在页面的亚马逊 EC2 AMI 详情部分，确认显示的亚马逊系统映像 (AMI) 详细信息与源 Lightsail 实例的规格相符。

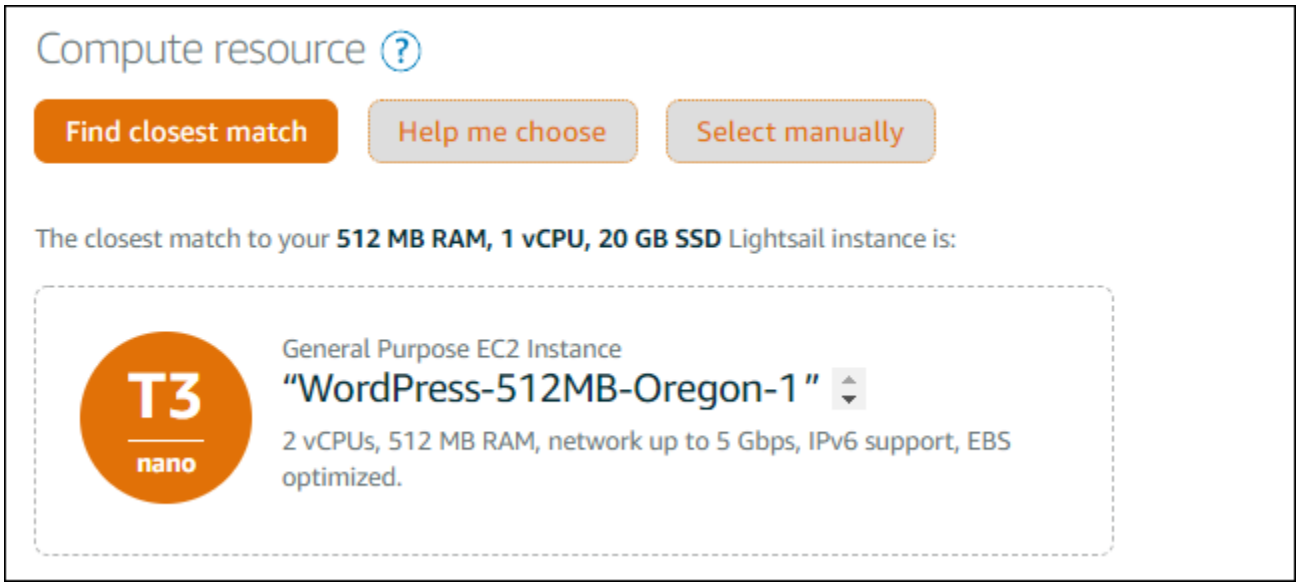


2. 在该页面的 Resource location（资源位置）部分，更改实例的可用区（如有必要）。亚马逊 EC2 资源的创建方式与源 Lightsail 快照 AWS 区域 相同。

> **Note**
>
> 并非所有可用区对所有用户都可用。选择不可用的可用区将导致创建 EC2 实例时出错。



3. 在该页面的 Compute resource（计算资源）部分，选择以下选项之一：



a. 查找最接近的匹配项以自动选择与源 Lightsail EC2 实例规格密切匹配的亚马逊实例类型。

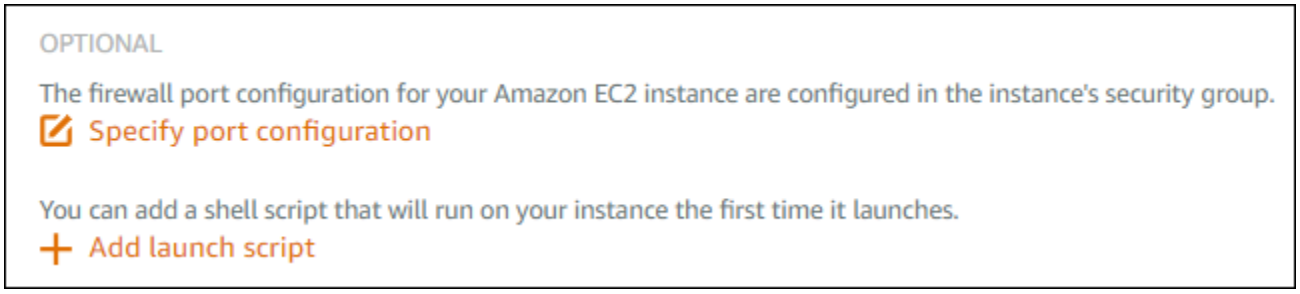
b. 帮我选择回答一份关于您的新 Amazon EC2 实例规格的简短问卷。您可以从计算优化或内存优化的实例类型中进行选择，也可以选择这两者的平衡类型。

c. 手动选择可通过创建 Amazon 实例页面查看可用 EC2 实例类型列表。

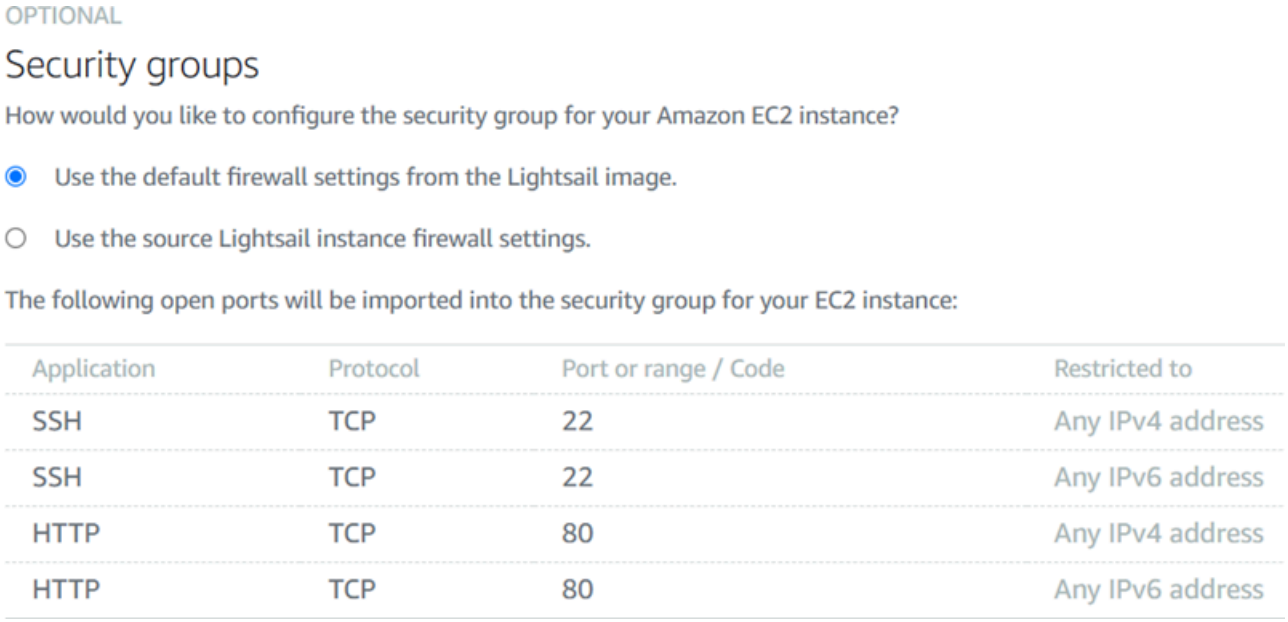
> **Note**
>
> 某些 Lightsail 实例与当前一代的 EC2实例类型（T3、M5、C5 或 R5）不兼容，因为它们未启用增强联网功能。如果您的源 Lightsail 实例不兼容，则在根据导出的快照创建实例时，您需要选择上一代实例类型（T2、M4、C4 或 R4）。 EC2这些实例类型选项显示在 Lightsa il 控制台的 "创建亚马逊 EC2 实例" 页面上。
> 要在源 Lightsail 实例不兼容时使用最新一代 EC2 的实例类型，您需要使用上一代 EC2 实例类型（T2、M4、C4 或 R4）创建新实例，更新网络驱动程序，然后将该实

例升级到所需的当前一代实例类型。有关更多信息，请参阅更新 Amazon EC2 实例以增强联网。

4. 在该页面的可选部分：



a. 选择指定端口配置以选择您的 Amazon EC2 实例的防火墙设置，然后选择以下选项之一：



i. 使用 Lightsail 镜像中的默认防火墙设置，在新实例上配置源 Lightsail 蓝图中的默认端口。 EC2 有关 Lightsail 蓝图默认端口的更多信息，请参阅防火墙和端口。

ii. 使用源 Lightsail 实例防火墙设置在新实例上配置来自源 Lightsail 实例的端口。 EC2只有当源 Lightsail 实例仍在运行时，此选项才可用。

b. 如果您想添加在实例启动时配置 EC2 实例的脚本，请在该页面的启动脚本部分，选择添加启动脚本。

5. 在页面的 “连接安全” 部分，确定您如何连接到源 Lightsail 实例。这样可以确保您获得正确的 SSH 密钥来连接到您的新 EC2 实例。您可以使用以下方法之一连接到源 Lightsail 实例：

a. 使用源实例区域的默认 Lightsail 密钥对 — 下载并使用该密钥的唯一默认 Lightsail 密钥 AWS 区域 来连接到您的实例。 EC2

> **Note**
>
> 默认的 Lightsail 密钥对始终用于 Lightsail 中的 Windows 服务器实例。

b. 使用您自己的密钥对 — 找到私钥并使用它来连接您的 EC2 实例。

> **Note**
>
> Lightsail 不会存储您的个人私钥。因此，未提供下载私有密钥的选项。如果您找不到私钥，则将无法连接到您的 EC2 实例。

6. 在该页面的存储资源部分，确认正在创建的 EBS 卷与源 Lightsail 实例的系统磁盘和所有附加的块存储磁盘相匹配。



7. 查看有关在 Lightsail 之外创建资源的重要细节。
8. 如果您同意在 Amazon 中创建实例 EC2，请选择在中创建资源 EC2。

Lightsail 确认您的实例正在创建中，并显示有关 AWS CloudFormation 堆栈的信息。Lightsail 使用 CloudFormation 堆栈来创建 EC2实例及其相关资源。有关更多信息，请参阅 Lights ail 的AWS CloudFormation 堆栈。

继续阅读本指南的 “跟踪您的新 Amazon EC2 实例的状态” 部分，以跟踪您的新 EC2实例的状态。

> **Important**
>
> 等到您的新 EC2 实例创建完毕后，才能使用相同的导出快照创建另一个 EC2 实例。

跟踪您的新 Amazon EC2 实例的状态

使用 Lightsail 控制台中的 “导出” 部分来跟踪您的 EC2 实例的状态。有关更多信息，请参阅 在 Lightsail 中跟踪快照导出状态。

对于正在创建的 EC2 实例，将显示以下信息：

- 源名称-源 Lightsail 快照的名称。
- 开始时间 - 创建请求的开始日期和时间。

对于已创建的 EC2 实例，任务监视器中会显示以下信息：

- 如果成功@@ 创建 Amazon EC2 资源，则会显示已创建。
- 如果创建 EC2 实例时出现问题，则会显示 “失败”。

根据导出的 Lightsail 磁盘快照创建亚马逊弹性区块存储卷

导出 Lightsail 块存储磁盘快照并在亚马逊上线 EC2 （作为 EBS 快照）后，您可以使用亚马逊控制台从该快照创建 EBS 卷。 EC2

> **Note**
>
> 要使用导出的 EC2 实例快照创建实例，请参阅在 Lightsail 中使用导出的快照创建亚马逊 EC2 实例。

您也可以使用 Amazon EC2 API 创建新的 EBS 卷 AWS CLI、或 SDKs。有关更多信息，请参阅亚马逊 EC2 文档中的使用启动实例向导启动实例或从快照恢复 Amazon EBS 卷。

> **Important**
>
> 我们建议在完成本指南中的步骤之前，先熟悉 Lightsail 的导出流程。有关更多信息，请参阅将快照导出到 Amazon EC2。

先决条件

将 Lightsail 块存储磁盘快照导出到亚马逊。 EC2有关更多信息，请参阅将快照导出到 Amazon EC2。

根据导出的 Lightsail 块存储磁盘快照创建 EBS 卷

使用亚马逊 EC2 控制台根据导出的 Lightsail 块存储磁盘快照创建新的 EBS 卷。

> **Note**
>
> 这些步骤也在 Amazon EC2 文档中。要了解更多信息，请参阅亚马逊 EC2文档中的从快照恢复 Amazon EBS 卷。

使用导出的 Lightsail 块存储磁盘快照创建 EBS 卷

1. 登录 Amazon EC2 控制台。
2. 在导航栏中，选择快照所处的区域。
3. 在左导航窗格中的 Elastic Block Store (弹性数据块存储) 下，选择 Snapshots (快照)。
4. 找到并选择导出的 Lightsail 块存储磁盘快照。

   导出的磁盘快照可以通过 EBS 快照的 “从 Amazon Lightsail 导出的磁盘快照” 描述来识别，如以下屏幕截图所示：



5. 选择操作，然后选择创建卷。
6. 从卷类型下拉菜单中选择卷类型。有关更多信息，请参阅亚马逊 EC2 文档中的 Amazon EBS 卷类型。

7. 对于 Size (GiB)，键入卷的大小，或验证快照的默认大小是否足够。
8. 对于带有预配置 IOPS SSD 卷的 IOPS，键入该卷应该支持的每秒输入/输出操作 (IOPS) 的最大数量。
9. 对于 Availability Zone，选择要在其中创建卷的可用区。EBS 卷只能连接到同一可用区中的 EC2 实例。
10. (可选) 选择 Create additional tags 以将标签添加到卷。对于每个标签，提供标签键和标签值。
11. 选择 Create Volume。创建您的卷后，它将列在亚马逊 EC2控制台的 Elastic Block Store > Volumes 部分。

连接到通过 Lightsail 快照创建的 Linux 亚马逊 EC2 实例

通过亚马逊 Lightsail 快照在亚马逊弹性计算云 (亚马逊 EC2) 中创建 Linux 或 Unix 实例后，您可以通过 SSH 连接到该实例，类似于连接到源 Lightsail 实例的方式。要对您的实例进行身份验证，请使用源实例的默认 Lightsail 密钥对或您自己的密钥对。 AWS 区域本指南向你展示了如何 EC2 使用 Putty 连接你的 Linux 或 Unix 实例。

> **Note**
>
> 有关连接到 Windows 服务器实例的更多信息，请参阅连接到通过 Lightsail 快照创建的亚马逊 EC2 Windows 服务器实例。

内容

- 获取实例的密钥
- 获取实例的公有 DNS 地址
- 下载并安装 PuTTY
- 使用 Pu 配置密钥 TTYgen
- 配置 PuTTY 以连接到实例
- 后续步骤

获取实例的密钥

获取连接到您的新 Amazon EC2 实例所需的正确密钥。你需要的密钥取决于你连接到源 Lightsail 实例的方式。您可以使用以下方法之一连接到源 Lightsail 实例：

- 使用源实例区域的默认 Lightsail 密钥对 — 从 L ig htsail 账户页面的 SSH 密钥选项卡下载默认私钥。有关默认 Lightsail 密钥的更多信息，请参阅 SSH 密钥对。

> **Note**
>
> 在您连接到您的 EC2 实例后，我们建议从实例中移除默认 Lightsail 密钥，并将其替换为您自己的密钥对。有关更多信息，请参阅保护通过 Lightsail 快照在亚马逊中 EC2 创建的 Linux 或 Unix 实例。

- 使用您自己的密钥对 — 找到您的私钥并使用它来连接您的 Amazon EC2 实例。当你使用自己的密钥对时，Lightsail 不会存储你的私钥。如果您丢失了私钥，则无法连接到您的 Amazon EC2 实例。

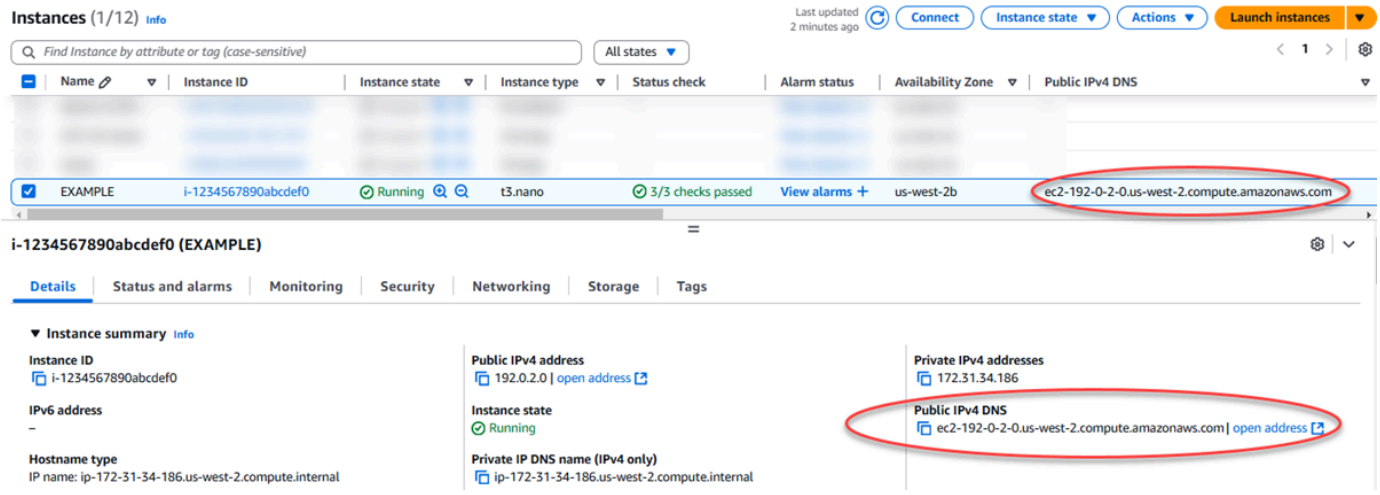
获取实例的公有 DNS 地址

获取您的 Amazon EC2 实例的公有 DNS 地址，这样您就可以在配置 SSH 客户端（例如 PuTTY）连接到您的实例时使用该地址。

获取实例的公有 DNS 地址

1. 登录 Amazon EC2 控制台。
2. 从左侧导航窗格中选择实例。
3. 选择要连接的正在运行的 Linux 或 Unix 实例。
4. 在下方窗格中，找到实例的公有 DNS 地址。

   这是配置 SSH 客户端来连接实例时需要使用的地址。继续阅读本指南的下载并安装 PuTTY 部分，以了解如何下载并安装 PuTTY SSH 客户端。



下载并安装 PuTTY

PuTTY 是适用于 Windows 的免费 SSH 客户端。有关 PuTTY 的更多信息，请参阅 PuTTY：一个免费的 SSH 和 Telnet 客户端。本网站还介绍了不允许加密的国家/地区的限制。如果您已经有 PuTTY，则可以跳至本指南的以下使用 Pu 配置密钥TTYgen部分。

下载 PuTTY 安装程序或可执行文件。建议使用最新版本。不过，如需了解有关选择哪种下载的信息，请参阅 PuTTY 文档。

继续阅读本指南的 “使用 Pu 配置密钥 TTYgen” 部分，使用 Pu 配置密钥TTYgen。

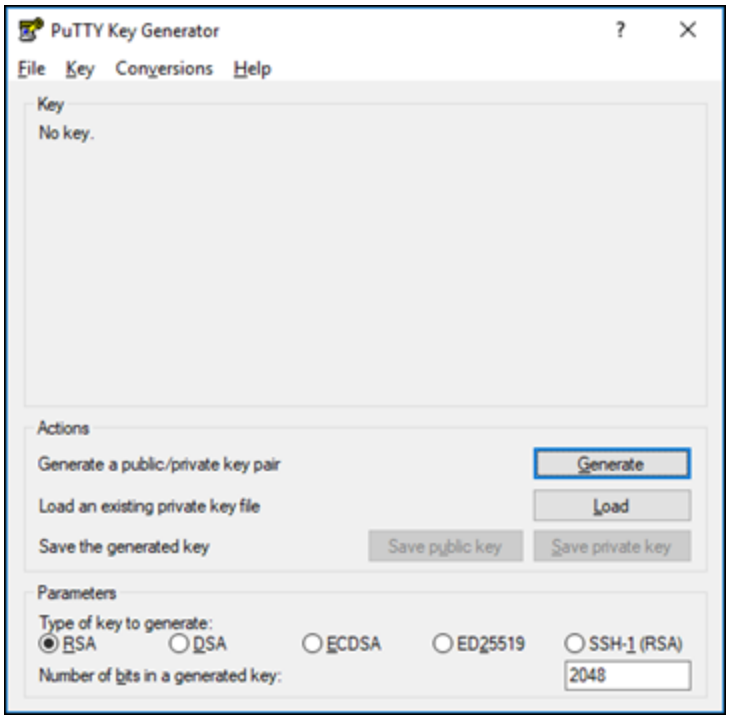
使用 Pu 配置密钥 TTYgen

Pu TTYgen 生成成对的公钥和私钥以与 PuTTY 一起使用。要使用 PuTTY 接受的密钥文件类型 (.PPK)，则需要进行此步骤。

使用 Pu 配置密钥 TTYgen

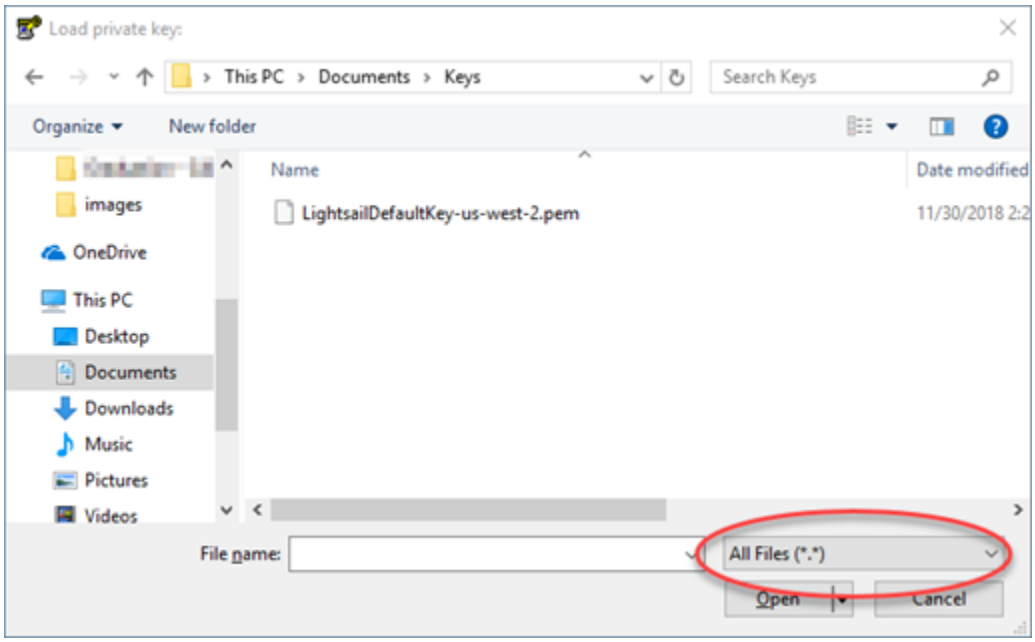
1. 启动 Pu TTYgen。

   例如，选择 Windows 的 “开始” 菜单，选择 “所有程序”，选择 “Putty”，然后选择 Pu。TTYgen

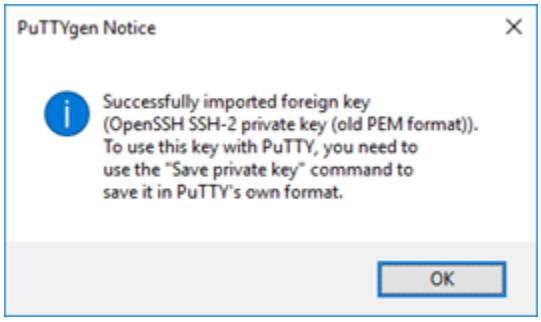


2. 选择 Load (打开)。

默认情况下，Pu 仅TTYgen 显示扩展名为.PPK 的文件。要找到您的 .PEM 文件，请选择相应选项以显示所有类型的文件。

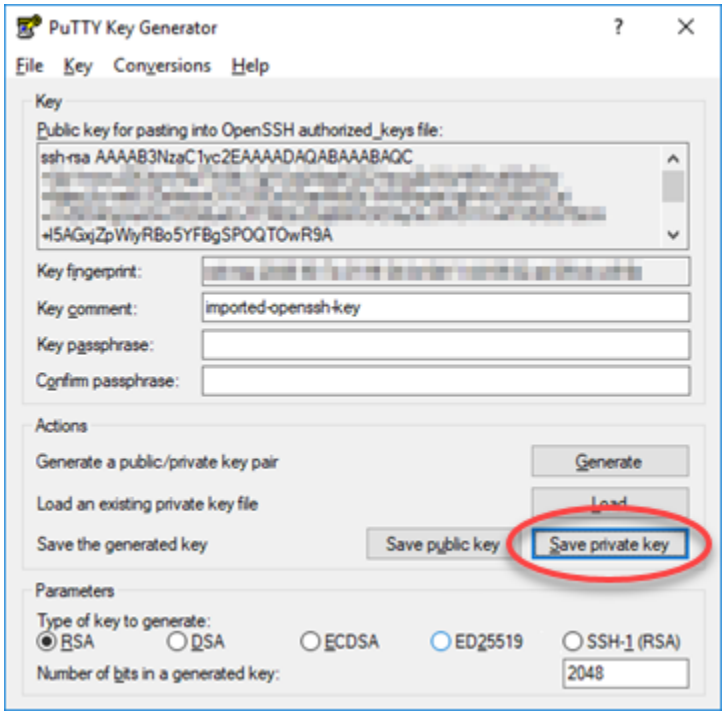


3. 选择您在本指南前面部分下载的默认 Lightsail 密钥文件 (.PEM)，然后选择 “打开”。
4. Pu TTYgen 确认成功导入密钥后，选择 OK。



5. 选择 Save private key (保存私有密钥)，然后确认您不想使用密码保存它。

   如果您创建一个密码作为一项额外安全措施，那么您每次使用 PuTTY 连接到实例时都需要输入该密码。



6. 指定名称和用于保存私有密钥的位置，然后选择 Save（保存）。

   Pu TTYgen 将您的新密钥文件保存为.PPK 文件类型。

7. 近距离观察TTYgen。

   继续阅读本指南的配置 PuTTY 以连接到您的实例部分，使用您生成的新的.PPK 文件来配置 PuTTY 并连接到亚马逊上的 Linux 或 Unix 实例。 EC2

配置 PuTTY 以连接到实例

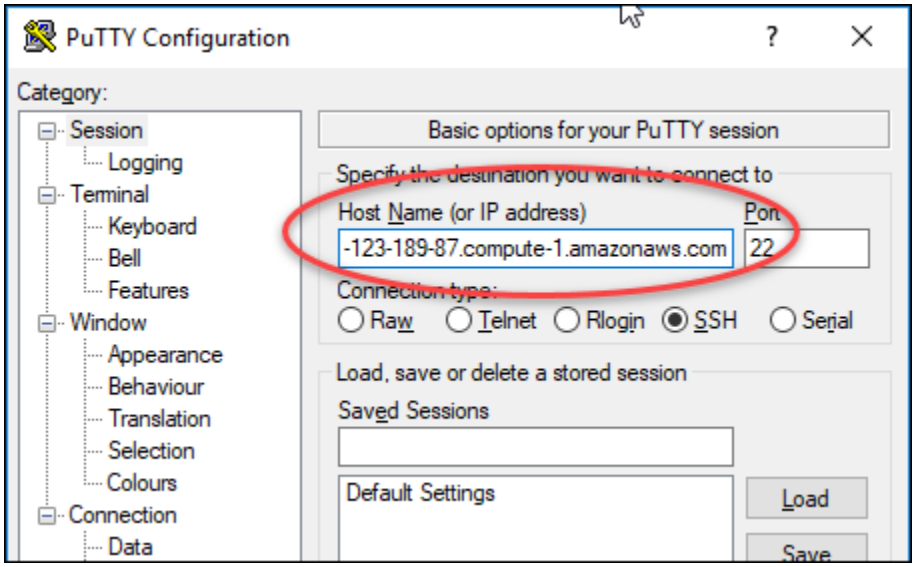
配置 PuTTY，然后您就满足使用 SSH 连接到 Linux 或 Unix 实例的所有要求了。

配置 PuTTY 以连接到 Linux 或 Unix 实例

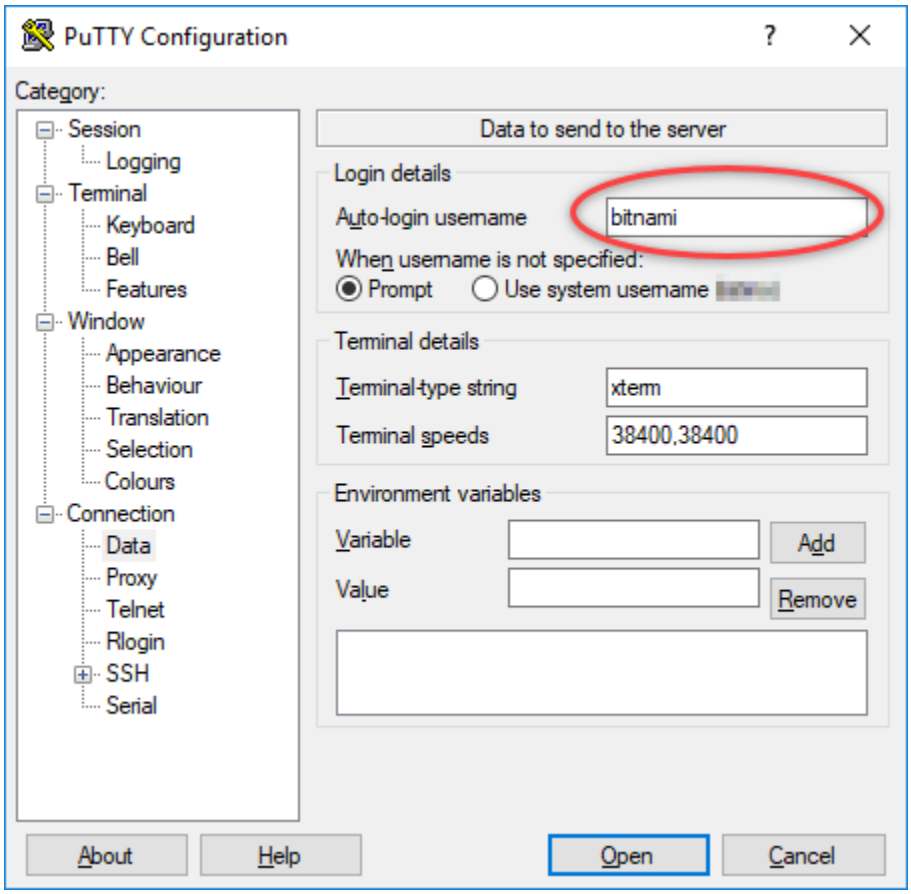
1. 打开 PuTTY。

   例如，依次选择 Windows 开始菜单、所有程序、PuTTY 和 PuTTY。

2. 在主机名文本框中，输入本指南前面部分从 Amazon EC2 控制台获取的实例的公有 DNS 地址。



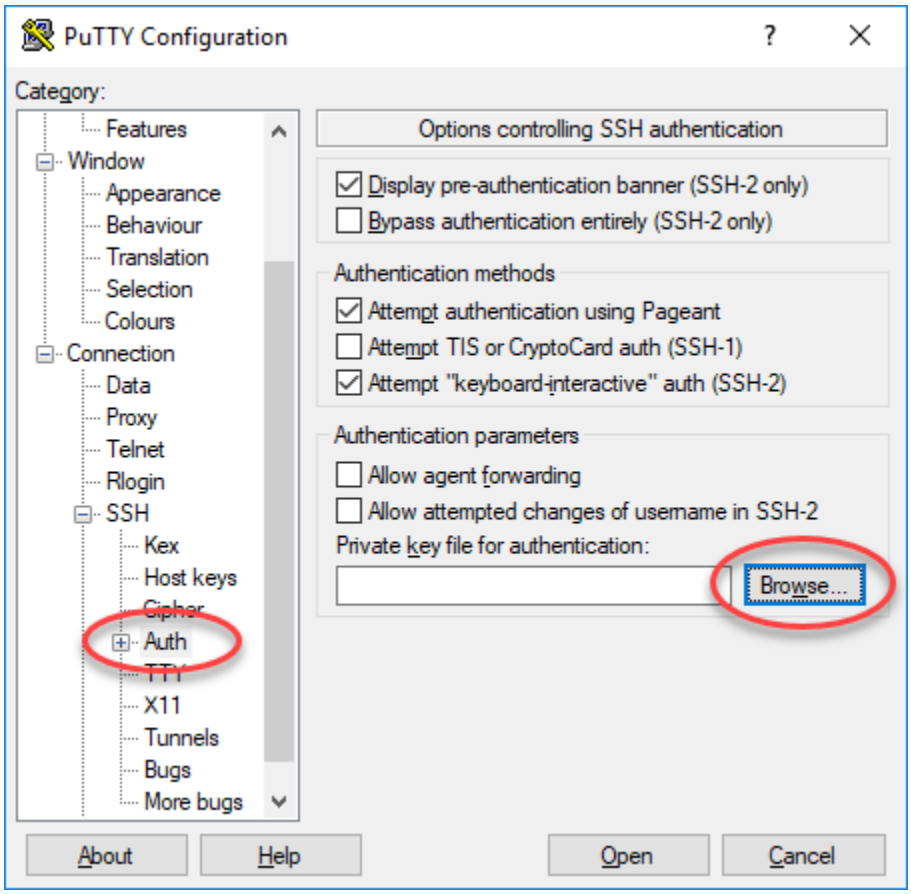
3. 在左侧导航窗格中的 Connection (连接) 部分下，选择 Data (数据)。
4. 在 Auto-login username (自动登录用户名) 文本框中，输入登录实例时使用的用户名。



根据源 Lightsail 实例的蓝图，输入以下默认用户名之一：

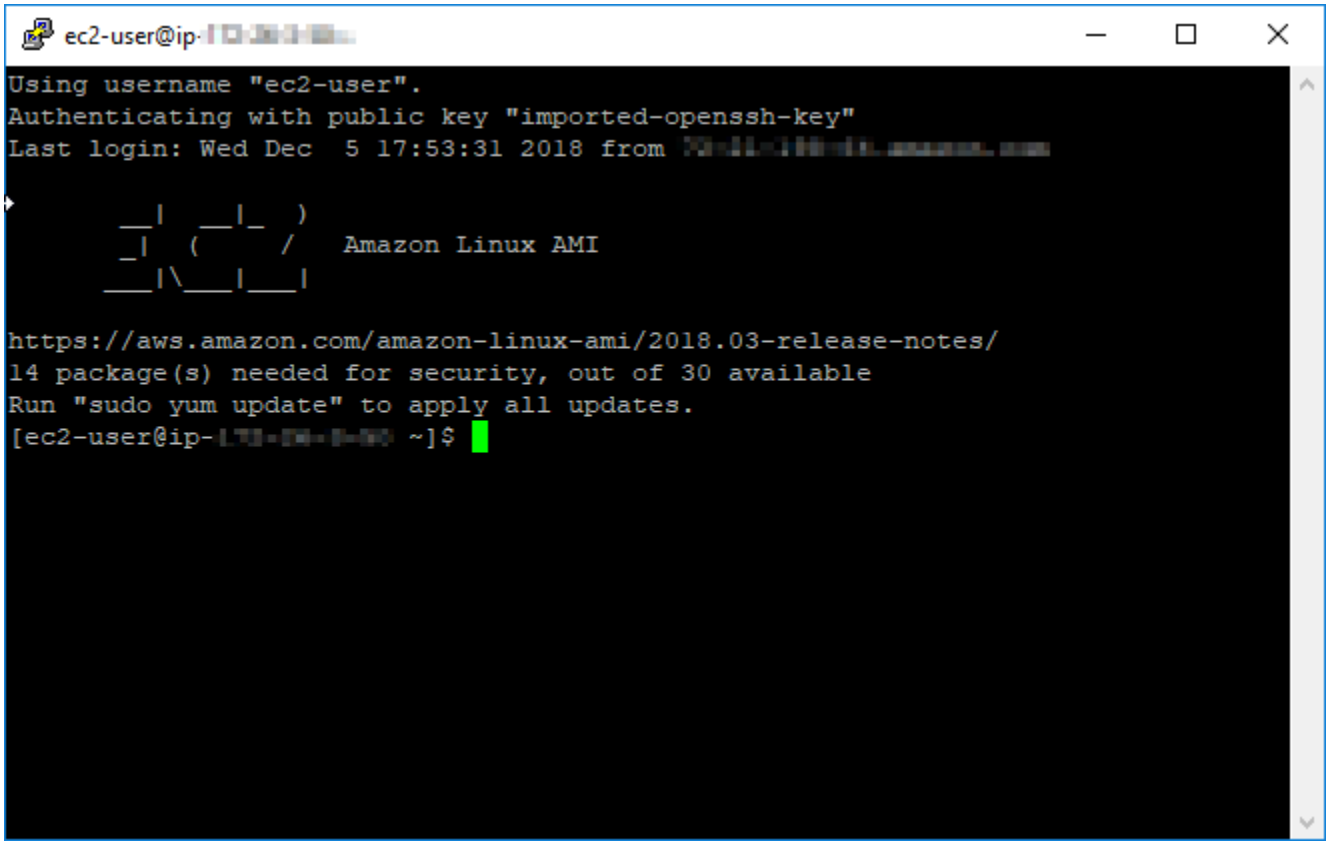
- AlmaLinux，亚马逊 Linux 2，亚马逊 Linux 2023，CentOS Stream 9,FreeBSD，以及 openSUSE 实例：`ec2-user`
- Debian 实例：`admin`
- Ubuntu 实例：`ubuntu`
- Bitnami 实例：`bitnami`
- Plesk 实例：`ubuntu`
- cPanel 和 WHM 实例：`centos`

5. 在左侧导航窗格中的 Connection (连接) 部分下，展开 SSH，然后选择 Auth (身份验证)。
6. 选择 Browse (浏览)，导航到您在本指南的上一部分创建的 .PPK 文件，然后选择 Open (打开)。



7. 再次选择 Open (打开) 以连接到实例，然后选择 Yes (是) 以在将来信任此连接。

   如果您已成功连接到实例，应该会看到与以下屏幕相似的屏幕：



后续步骤

如果您使用亚马逊根据导出的快照创建新实例，那么您在亚马逊中的新 Linux 或 Unix 实例 EC2 包含 EC2 来自 Lightsail 服务的剩余密钥。我们建议移除这些密钥，以增强新 Amazon EC2 实例的安全性。有关更多信息，请参阅保护通过 Lightsail 快照在亚马逊中 EC2 创建的 Linux 或 Unix 实例。

从 Lightsail 快照启动的亚马逊安全 EC2实例

亚马逊 Lightsail 和亚马逊弹性计算云 EC2（亚马逊）使用公钥加密来加密和解密登录信息。公有密钥密码术使用公有密钥加密某个数据 (如一个密码)，然后收件人可以使用私有密钥解密数据。公有和私有密钥被称为密钥对。

当你将 Linux 或 Unix Lightsail 实例导出到时 EC2，新 EC2 实例将包含来自 Lightsail 服务的剩余密钥。作为最佳安全实践，您应删除实例中未使用的密钥。

为了提高从 Lightsail 快照创建 EC2 的 Linux 或 Unix 实例的安全性，我们建议您在创建实例后执行以下操作：

- 如果你使用 Lightsail 默认密钥连接到 Lightsail 中的源实例，请移除并替换该密钥。如果您使用自己的密钥连接到您的 EC2 实例，或者您在 Lightsail 控制台中为实例创建了密钥，那么您的亚马逊实例中不存在 Lightsail 默认密钥。
- 移除 Lightsail 系统密钥，也称为密钥。`lightsail_instance_ca.pub`Linux 和 Unix 实例上的此密钥允许基于 Lightsail 浏览器的 SSH 客户端进行连接。使用 Lightsail 控制台中的 “创建亚马逊 EC2 实例” 页面或 Lightsail API 创建 EC2 实例时，该`lightsail_instance_ca.pub`密钥会自动删除。

内容

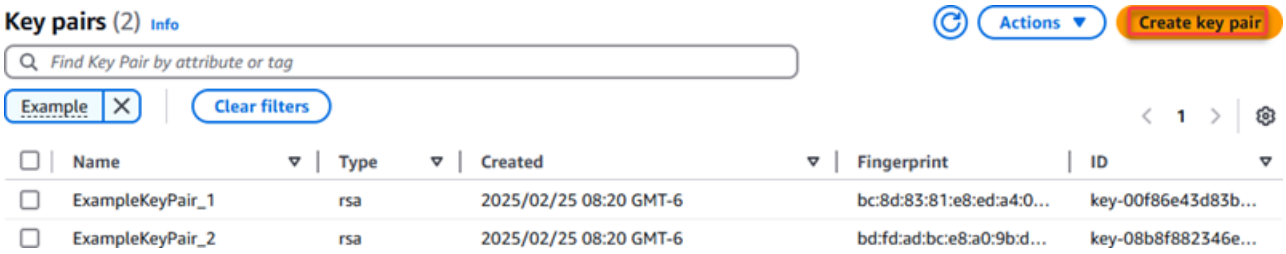
- 使用 Amazon 创建私钥 EC2
- 使用 Pu 创建公钥 TTYgen
- 在亚马逊上连接到你的 Linux 或 Unix 实例 EC2
- 将公有密钥添加到您的实例并测试连接
- 移除 Lightsail 的默认密钥
- 移除 Lightsail 系统密钥

使用 Amazon 创建私钥 EC2

使用亚马逊 EC2 控制台创建新的密钥对，您可以使用它来替换 Lightsail 的默认密钥对。

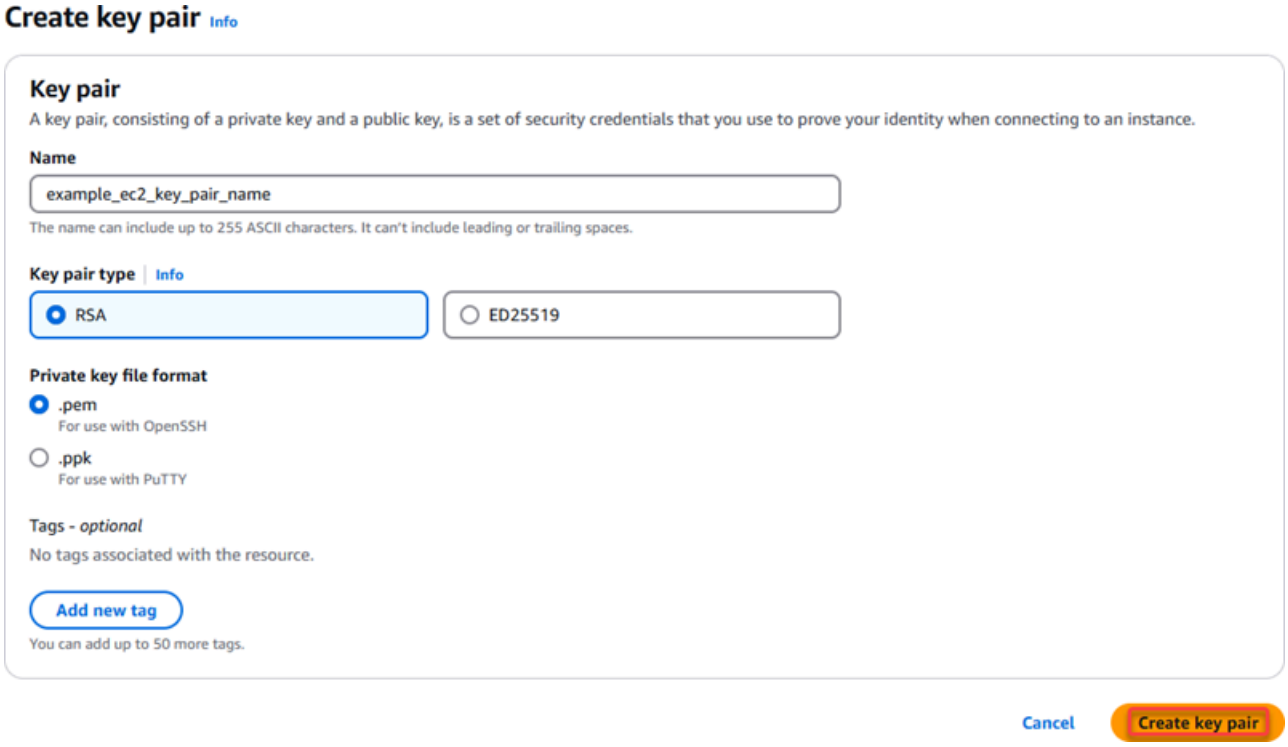
使用 Amazon 创建私钥 EC2

1. 登录 Amazon EC2 控制台。
2. 在左侧导航窗格中，选择 Key Pairs (密钥对)。
3. 选择 Create key pair (创建密钥对)。



4. 在密钥对名称文本框中输入密钥的名称，然后选择创建密钥对。有关在亚马逊中创建密钥对的更多信息 EC2，请参阅亚马逊弹性计算云用户指南中的为您的亚马逊 EC2实例创建密钥对。

此时会自动下载新的私有密钥。记下该私有密钥的保存位置。您需要在本指南的以下使用 Pu 创建公钥TTYgen部分中使用它来创建公钥。



使用 Pu 创建公钥 TTYgen

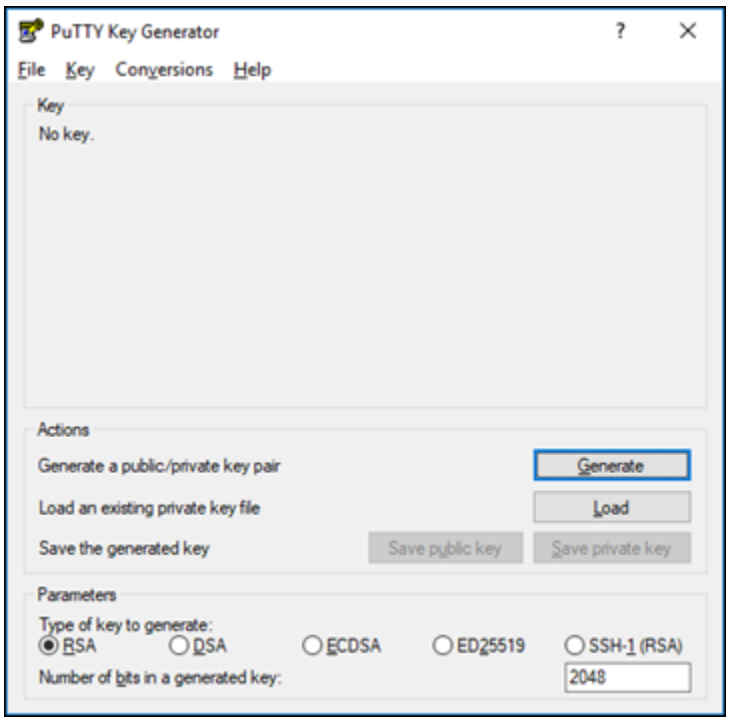
Pu TTYgen 是 Putty 中包含的工具。使用 Pu TTYgen 生成公钥文本，您将在本指南的后面部分将其添加到您的实例中。

> **Note**
>
> 有关如何配置 PuTTY 以连接到你的 Linux 或 Unix 实例的更多信息，请参阅连接到通过 Lightsail 快照创建的亚马逊 EC2 Linux 或 Unix 实例。

使用 Pu 创建公钥 TTYgen

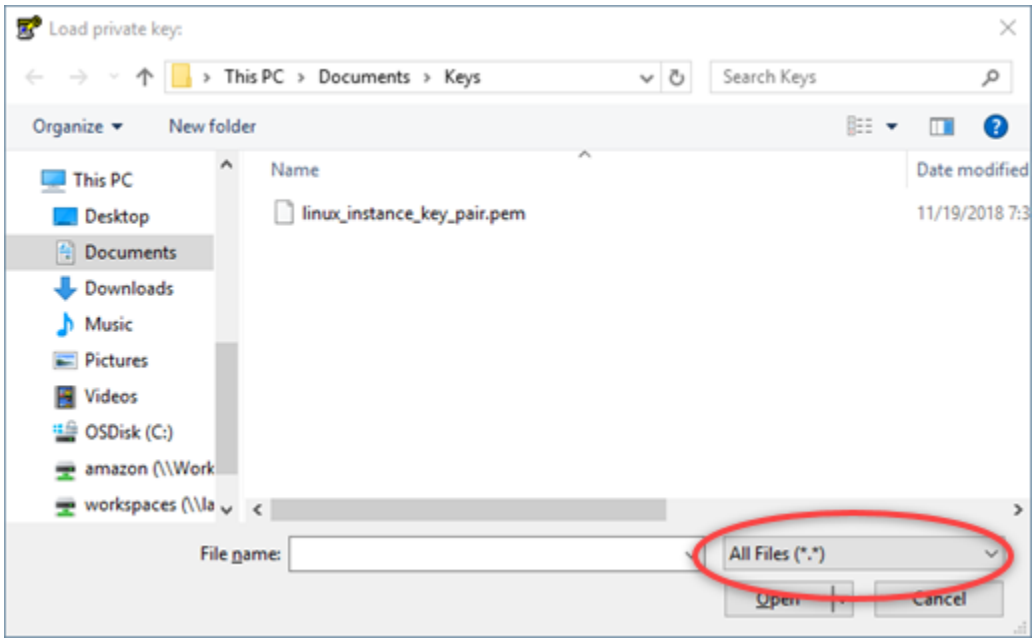
1. 启动 Pu TTYgen。

   例如，选择 Windows 的 “开始” 菜单，选择 “所有程序”，选择 “Putty”，然后选择 Pu。TTYgen



2. 选择 Load (打开)。

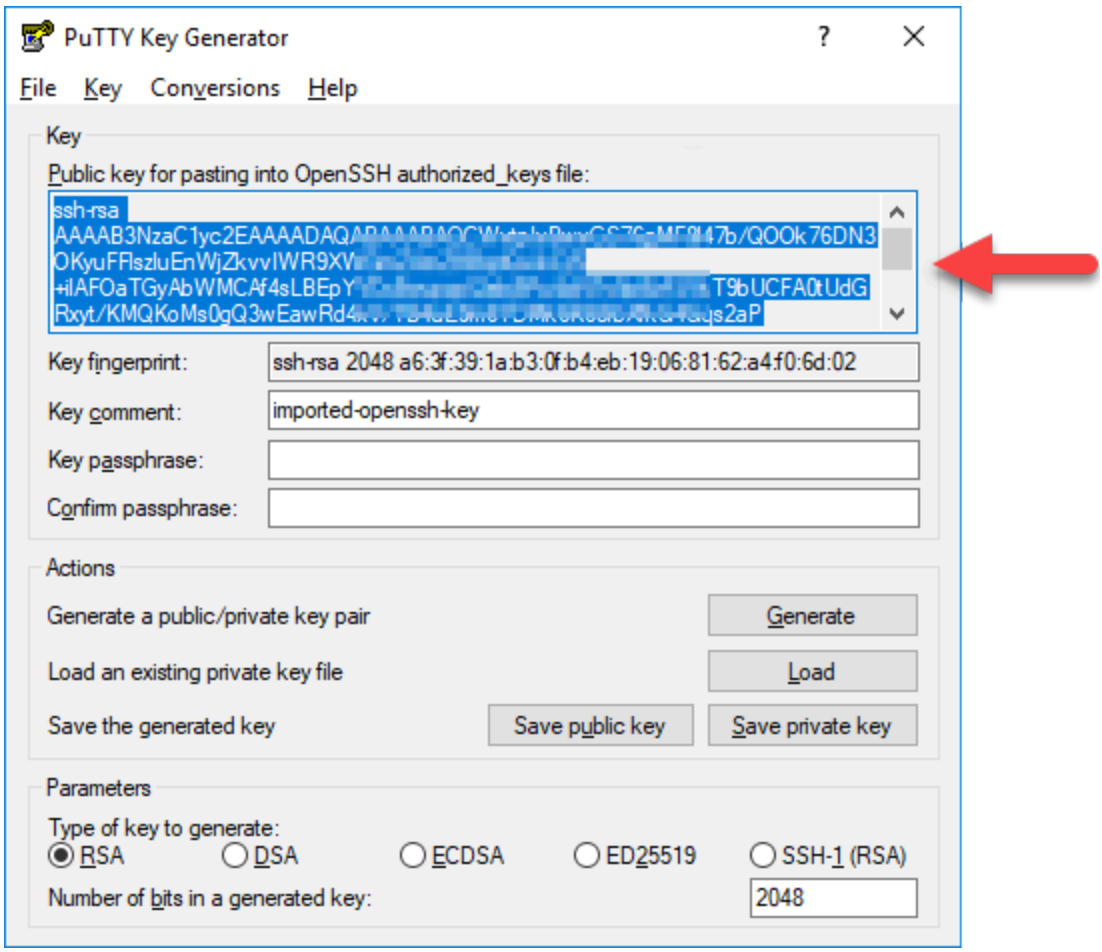
   默认情况下，Pu 仅TTYgen 显示扩展名为.PPK 的文件。要找到您的 .PEM 文件，请选择相应选项以显示所有类型的文件。



3. 导航到本指南中之前创建的私有密钥的位置。选择私有密钥，然后选择 Open (打开)。
4. Pu TTYgen 确认成功导入密钥后，选择 OK。

5. 突出显示 Public key (公有密钥) 文本框的内容，然后按 Ctrl+C (如果您使用的是 Windows) 或按 Cmd+C (如果您使用的是 macOS)，将其复制到剪贴板。

   打开文本编辑器，例如记事本或，如果你使用的是 Windows TextEdit，请按 Ctrl+V 将公钥文本粘贴到其中，如果你使用的是 macOS，则按 Cmd+V。保存这个含有您的公有密钥文本的文件；稍后您需要在本指南中使用它。



6. 继续阅读本指南的 “在 Amazon 中连接您的 Linux 或 Uni x 实例 EC2” 部分，连接到您的 EC2 实例并添加公钥。

在亚马逊上连接到你的 Linux 或 Unix 实例 EC2

EC2 使用 SSH 连接到亚马逊中的 Linux 或 Unix 实例，删除 Lightsail 的默认密钥和系统密钥。有关更多信息，请参阅连接到根据亚马逊 Lightsail 快照 EC2 创建的亚马逊中的 Linux 或 Unix 实例。

在 Amazon 中连接到您的实例后，继续阅读本指南的向您的实例添加公钥并测试连接部分 EC2。

将公有密钥添加到您的实例并测试连接

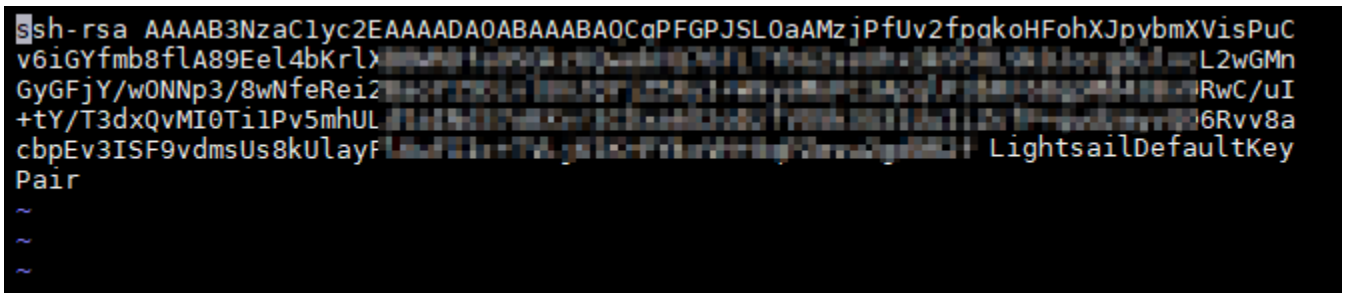
公有密钥内容保存在 Linux 和 Unix 实例上的 ~/.ssh/authorized_keys 文件中。编辑文件以从亚马逊的 Linux 或 Unix 实例中删除和替换 Lightsail 默认密钥。 EC2

将公有密钥添加到您的实例并测试连接

1. 建立与实例的 SSH 连接后，请输入以下命令以在 Vim 文本编辑器中编辑 authorized_keys。

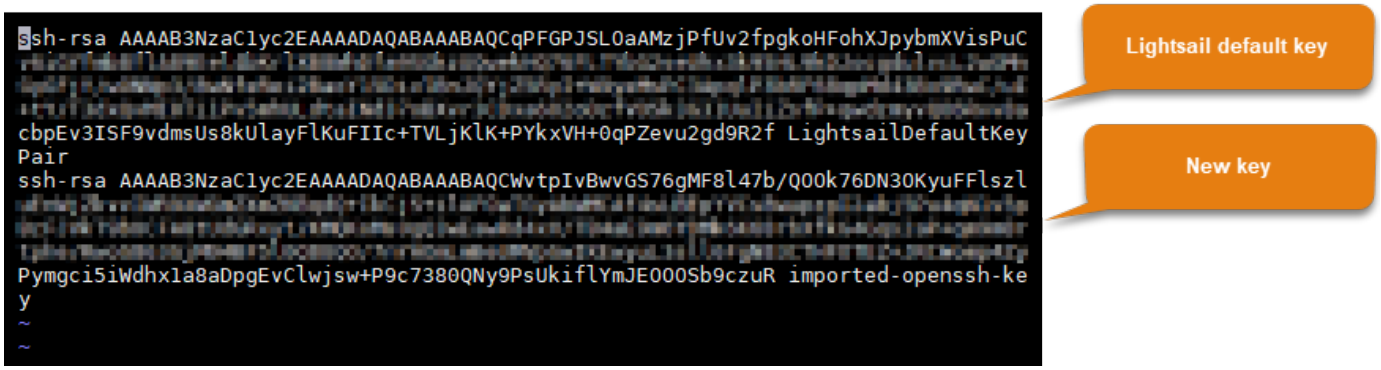
```
sudo vim ~/.ssh/authorized_keys
```

> **Note**
>
> 本指南将使用 Vim 演示这些步骤。但是，您可以使用任何文本编辑器执行这些步骤。



2. 按 I 键以进入 Vim 编辑器的插入模式。
3. 在 Lightsail 默认密钥之后再输入一行。
4. 复制并粘贴您之前在本指南中保存的公有密钥文本。

   结果应该类似以下内容：



5. 按 ESC 键，然后输入 :wq! 以保存您的编辑内容并退出 Vim。

6. 输入以下命令以重新启动 Open SSH 服务器：

```
sudo /etc/init.d/sshd restart
```

您应该会看到类似以下内容的结果：

```
[ec2-user@ip-172-26-11-173 ~]$ sudo /etc/init.d/sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[ec2-user@ip-172-26-11-173 ~]$
```

新的公有密钥现已添加到您的实例。要测试新的密钥对，请断开与您的实例的连接。将 PuTTY 配置为使用你的新私钥而不是 Lightsail 的默认密钥。如果您能够使用新的密钥对成功连接到您的实例，请继续阅读本指南的移除 Lightsail 默认密钥部分，移除 Lig htsail 默认密钥。

移除 Lightsail 的默认密钥

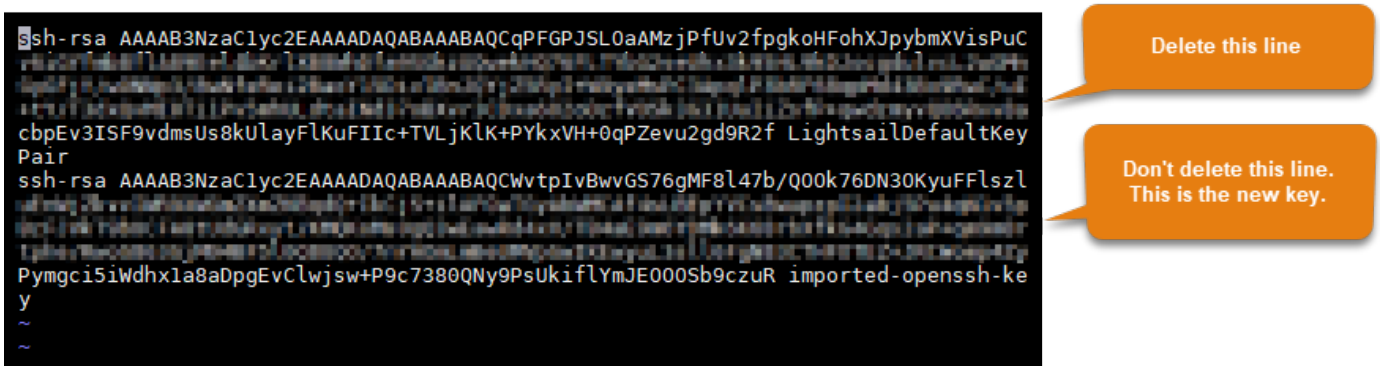
在向实例添加新的公钥并使用新的密钥对成功连接到实例后，请移除 Lightsail 默认密钥。

移除 Lightsail 的默认密钥

1. 建立与实例的 SSH 连接后，请输入以下命令以在 Vim 文本编辑器中编辑 `authorized_keys file`。

```
sudo vim ~/.ssh/authorized_keys
```

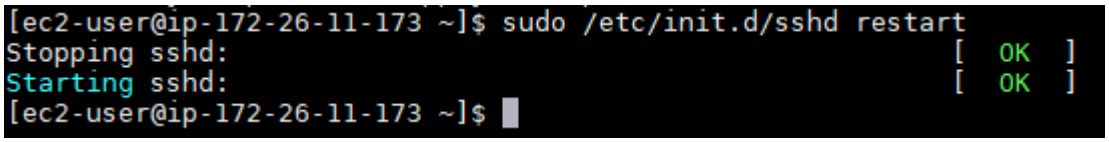
2. 按 I 键以进入 Vim 编辑器的插入模式。
3. 删除以 `LightsailDefaultKeyPair` 结尾的行。这是 Lightsail 的默认密钥。



4. 按 ESC 键，然后输入 `:wq!` 以保存您的编辑内容并退出 Vim。
5. 输入以下命令以重新启动 Open SSH 服务器：

```
sudo /etc/init.d/sshd restart
```

您应该会看到类似以下内容的结果：



Lightsail 默认密钥现已从您的实例中移除。现在，您的实例将拒绝使用 Lightsail 默认密钥的连接。继续阅读本指南的移除 Lightsail 系统密钥部分，移除 Lightsail 系统密钥。

移除 Lightsail 系统密钥

Linux 和 Unix 实例上的 Lightsail 系统`lightsail_instance_ca.pub`密钥（也称为密钥）允许基于 Lightsail 浏览器的 SSH 客户端进行连接。执行以下步骤从亚马逊的 Linux 或 Unix 实例中删除`lightsail_instance_ca.pub`密钥 EC2，然后编辑该`/etc/ssh/sshd_config`文件。该 `/etc/ssh/sshd_config` 文件定义了用于与您的实例建立 SSH 连接的参数。

移除 Lightsail 系统密钥

1. 在连接到实例的 SSH 终端窗口中，输入以下命令以删除 `lightsail_instance_ca.pub` 密钥：

   ```
   sudo rm -r /etc/ssh/lightsail_instance_ca.pub
   ```

2. 输入以下命令，以使用 Vim 文本编辑器编辑 `sshd_config` 文件。

   ```
   sudo vim /etc/ssh/sshd_config
   ```

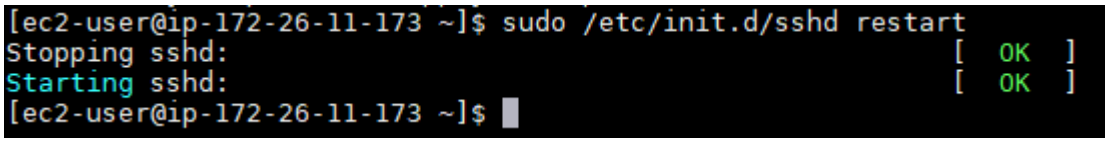
3. 按 I 键以进入 Vim 编辑器的插入模式。
4. 如果该文件中出现以下文本，请将其删除：

   ```
   TrustedUserCAKeys /etc/ssh/lightsail_instance_ca.pub
   ```

5. 按 ESC 键，然后输入 `:wq!` 以保存您的编辑内容并退出 Vim。
6. 输入以下命令以重新启动 Open SSH 服务器：

   ```
   sudo /etc/init.d/sshd restart
   ```

您应该会看到类似以下内容的结果：



`lightsail_instance_ca.pub` 密钥现已从您的实例中删除。相关联的 `sshd_config` 文件已更新，以排除该密钥。

连接到通过 Lightsail 快照创建的 Windows 服务器亚马逊 EC2 实例

在亚马逊弹性计算云 (Amazon EC2) 中创建新的 Windows Server 实例后，您可以使用远程桌面协议 (RDP) 连接到该实例。这与您连接到源 Amazon Lightsail 实例的方式类似。使用源 EC2 实例的默认 Lightsail 密钥对连接到您的实例。 AWS 区域本指南向您介绍如何使用 Microsoft 远程桌面连接功能连接到您的 Windows Server 实例。

> **Note**
>
> 有关连接到 Linux 或 Unix 实例的更多信息，请参阅连接亚马逊中通过 Lightsail 快照 EC2 创建的 Linux 或 Unix 实例。

内容

- 获取实例的密钥
- 获取实例的公有 DNS 地址
- 获取 Windows Server 实例的密码
- 配置远程桌面连接以连接到 Windows Server 实例
- 后续步骤

获取实例的密钥

您在亚马逊的 Windows 服务器实例 EC2 使用源实例所在区域的默认 Lightsail 密钥对来检索默认管理员密码。

从 Lightsail 账户页面的 SSH 密钥选项卡下载默认私钥。有关默认 Lightsail SSH 密钥的更多信息，请参阅 SSH 密钥对。

> **Note**
>
> 在您连接到您的 EC2 实例后，我们建议您在 Amazon 中更改您的 Windows 服务器实例的管理员密码 EC2。它会移除默认 Lightsail 密钥对与你在亚马逊中的 Windows 服务器实例之间的关联。 EC2有关更多信息，请参阅保护根据 Lightsail 快照创建的亚马逊 EC2 Windows 服务器实例。

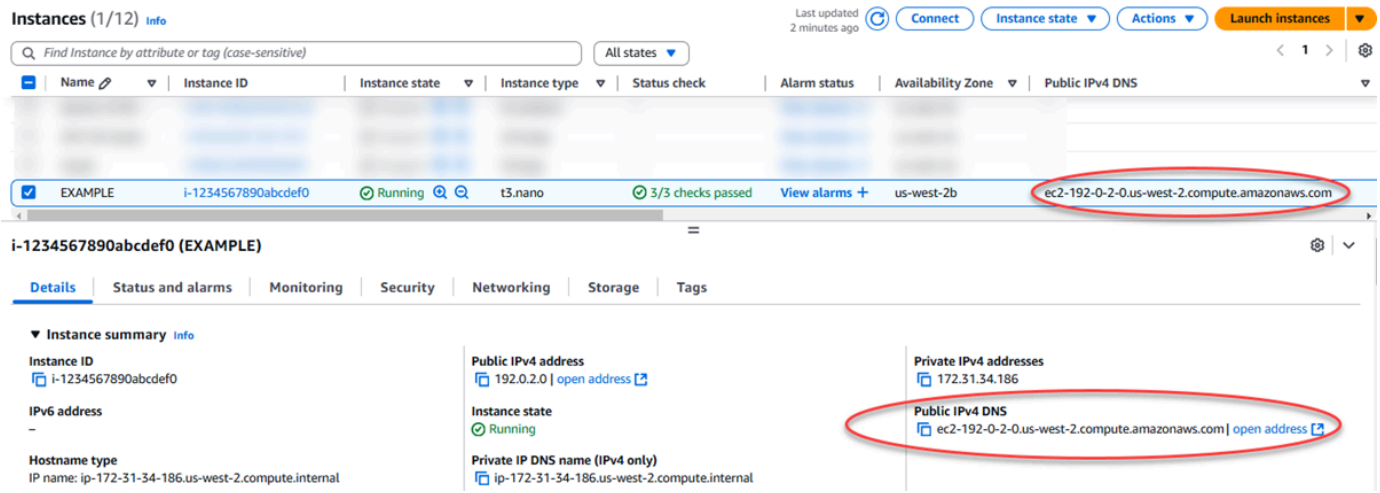
获取实例的公有 DNS 地址

获取您的 Amazon EC2 实例的公有 DNS 地址，以便在配置 RDP 客户端（例如 Microsoft 远程桌面连接）以连接到您的实例时使用该地址。

获取实例的公有 DNS 地址

1. 登录 Amazon EC2 控制台。
2. 从左侧导航窗格中选择实例。
3. 选择要连接的正在运行的 Windows Server 实例。
4. 在下方窗格中，找到实例的公有 DNS 地址。

   这是在配置 RDP 客户端来连接实例时需要使用的地址。继续阅读本指南的 “获取 Windows 服务器实例的密码” 部分，了解如何在亚马逊上获取 Windows 服务器实例的默认管理员密码 EC2。

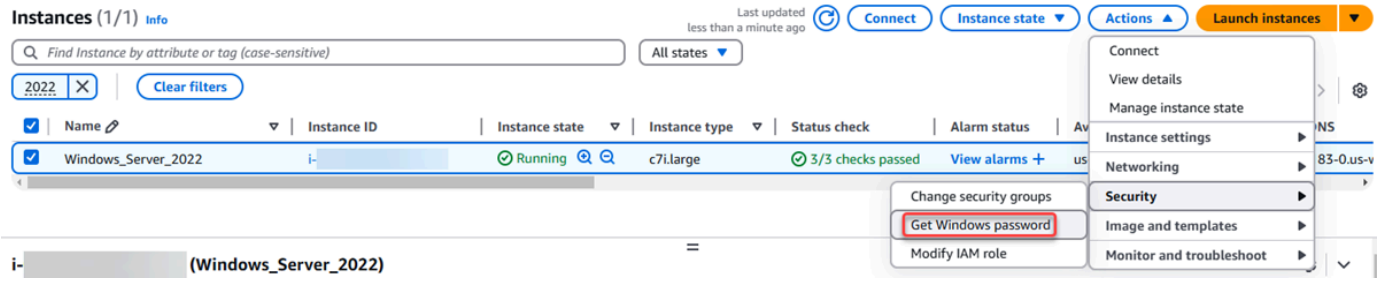


获取 Windows Server 实例的密码

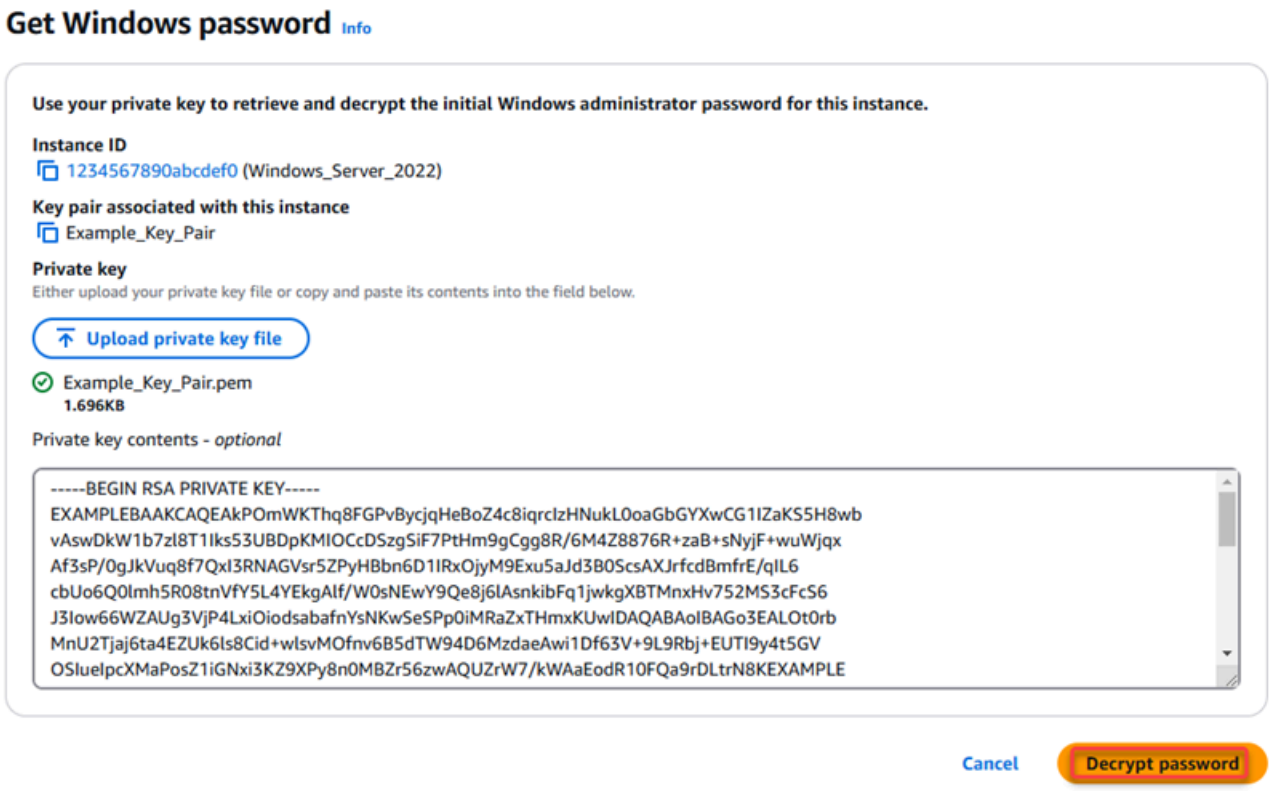
从亚马逊 EC2 控制台获取您的 Windows 服务器实例的密码。通过 RDP 连接到 Windows Server 实例时，您需要此密码来登录该实例。

获取 Windows Server 实例的密码

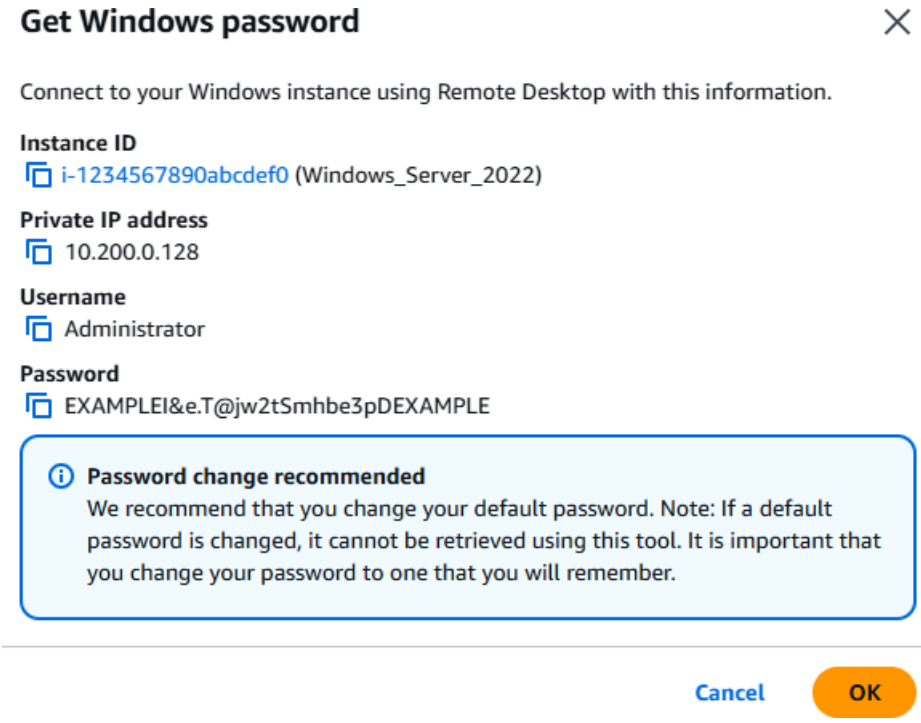
1. 登录 Amazon EC2 控制台。
2. 从左侧导航窗格中选择实例。
3. 选择要连接的 Windows Server 实例。
4. 在 “操作” 中，选择 “安全”、“获取 Windows 密码”。



5. 出现提示时，选择 “浏览”，然后打开本指南前面部分从 Lightsail 下载的默认私钥文件。
6. 选择 Decrypt Password。



将显示密码、用户名和私有 IP 地址。将密码复制到剪贴板，以便在本指南接下来的配置远程桌面连接以连接到 Windows Server 实例部分使用。请突出显示该密码，如果您使用 Windows，请按 Ctrl+C；如果您使用 macOS，请按 Cmd+C。



继续阅读本指南的配置远程桌面连接以连接您的 Windows Server 实例部分，了解如何配置远程桌面连接以连接到您的 Amazon 中的 Windows Server 实例 EC2。

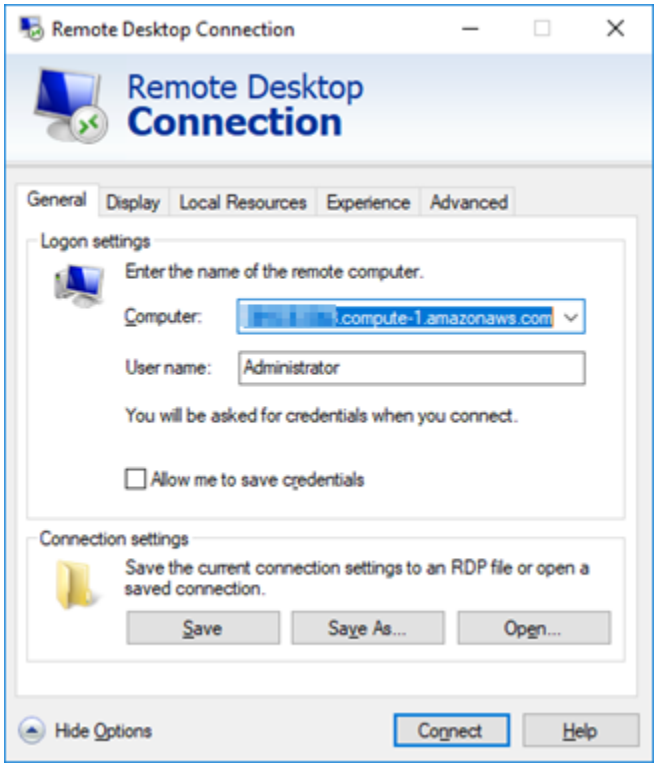
配置远程桌面连接以连接到 Windows Server 实例

远程桌面连接是在大多数 Windows 操作系统中预装的 RDP 客户端。使用它以图形方式连接到您在亚马逊中的 Windows 服务器实例 EC2。

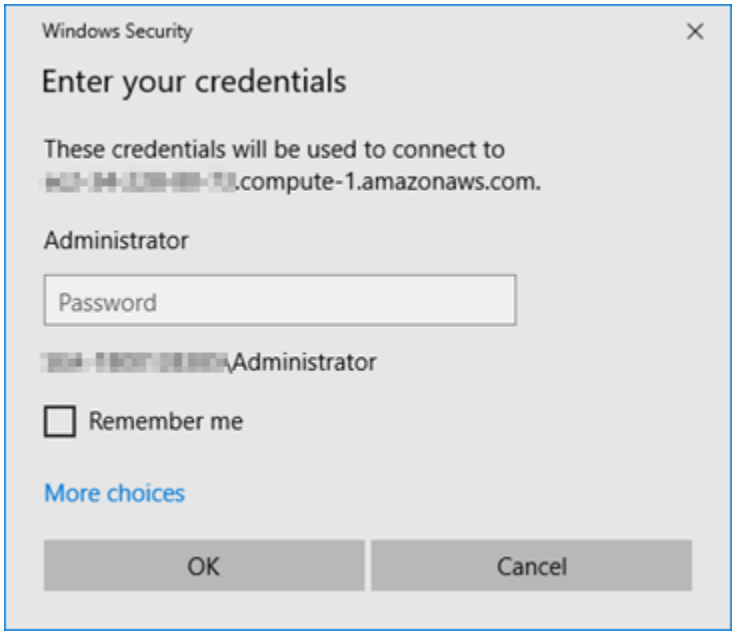
配置远程桌面连接以连接到 Windows Server 实例

1. 打开远程桌面连接。

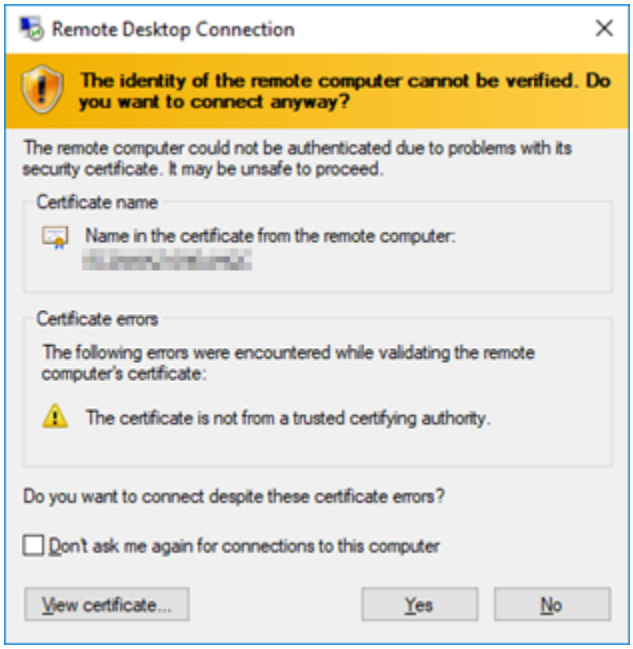
   例如，选择 Windows 开始菜单，然后搜索远程桌面连接。
2. 在“计算机”文本框中，输入本指南前面部分 EC2 获取的亚马逊 Windows 服务器实例的公有 DNS 地址。
3. 选择显示选项以查看更多选项。
4. 在用户名文本框中输入 `Administrator`。



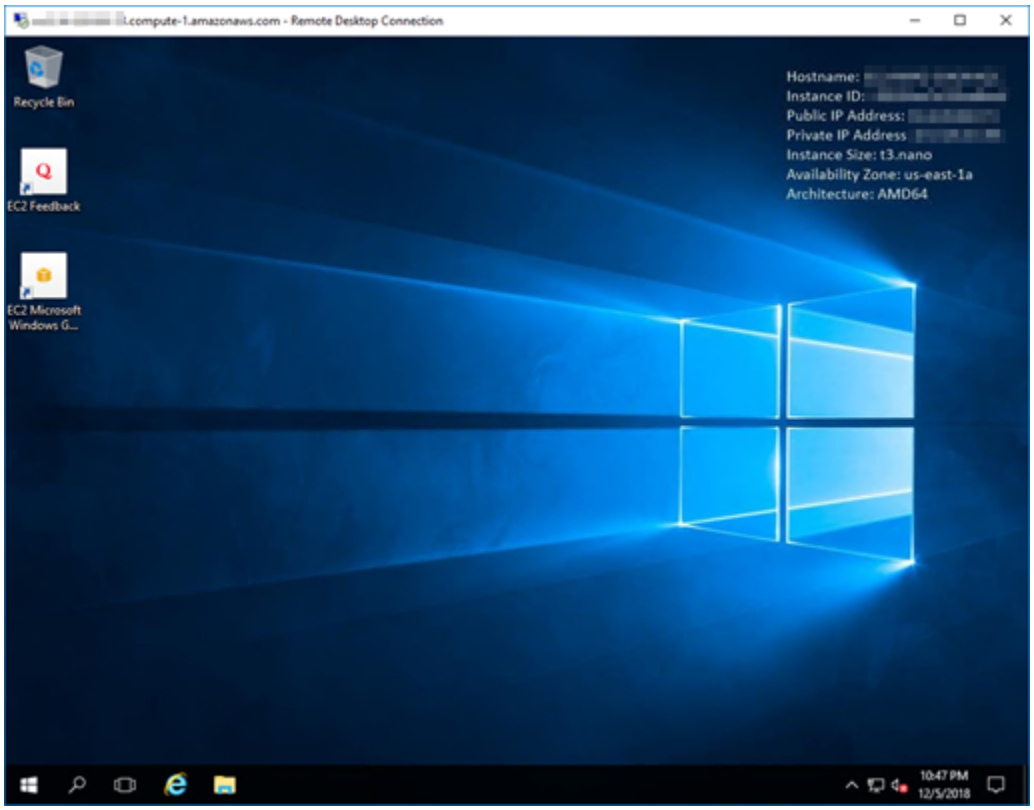
5. 选择连接以连接到您的 Windows Server 实例。
6. 根据 Windows 安全提示，将 Windows Server 实例的密码输入密码文本框，然后选择确定。



7. 根据远程桌面连接提示，选择是以进行连接。



如果您已成功连接到实例，应该会看到与以下屏幕相似的屏幕：



后续步骤

我们建议您在 Amazon 中更改您的 Windows 服务器实例的管理员密码 EC2。它会移除默认 Lightsail 密钥对与你在亚马逊中的 Windows 服务器实例之间的关联。 EC2有关更多信息，请参阅保护通过 Lightsail 快照在亚马逊中 EC2 创建的 Windows 服务器实例。

从 Lightsail 快照启动的安全 Windows 服务器亚马逊 EC2 实例

为了提高亚马逊弹性计算云（亚马逊 EC2）中根据亚马逊 Lightsail 快照创建的 Windows 服务器实例的安全性，我们建议您更改默认管理员密码。这将移除你的 Lightsail 密钥对与亚马逊中的新 Windows Server 实例之间的关联。 EC2

> **Note**
>
> 如果您通过 Lightsail 快照在亚马逊 EC2 创建了 Linux 或 Unix 实例，则应执行几个步骤来保护这些实例。有关更多信息，请参阅保护从 Lightsail 快照创建的 Amazon EC2 Linux 或 Unix 实例。

内容

- 在亚马逊上连接到你的 Windows 服务器实例 EC2
- 在亚马逊中更改您的 Windows 服务器实例的默认管理员密码 EC2

在亚马逊上连接到你的 Windows 服务器实例 EC2

要更改您的 Windows 服务器管理员密码，请 EC2 使用远程桌面协议 (RDP) 连接到您在亚马逊的 Windows 服务实例。要了解如何连接到您的实例，请参阅连接亚马逊中通过 Lightsail 快照 EC2 创建的 Windows 服务器实例。

在亚马逊上连接到您的实例后，继续阅读本指南的在亚马逊中更改您的 Windows Server 实例的默认管理员密码 EC2部分 EC2。

在亚马逊中更改您的 Windows 服务器实例的默认管理员密码 EC2

更改 Windows 服务器实例上的默认密码，以移除 Lightsail 密钥对与亚马逊中的新 Windows 服务器实例之间的关联。 EC2

在亚马逊中更改您的 Windows 服务器实例的默认管理员密码 EC2

1. 与实例建立 RDP 连接后，请打开命令提示符并输入以下命令。

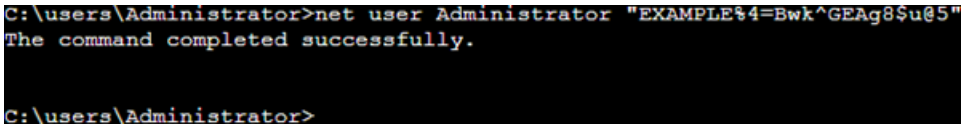
   ```
   net user Administrator "Password"
   ```

   在命令中，*Password*用您的新密码替换。

   示例：

   ```
   net user Administrator "EXAMPLE%4=Bwk^GEAg8$u@5"
   ```

   您应该会看到类似以下内容的结果：

2. 将新密码保存在安全位置。您无法使用 Amazon EC2 控制台找回新密码。控制台只能检索默认密码。如果您尝试在更改默认密码后使用该密码连接到实例，则会出现一条错误消息，指明您的凭证无效。

   如果您丢失了密码或密码过期，则可以生成新密码。有关密码重置程序，请参阅 Amazon EC2 文档中的重置丢失或过期的 Windows 管理员密码。

查看 AWS CloudFormation Lightsail 实例的堆栈

Amazon Lightsail 使用 AWS CloudFormation 导出的快照创建亚马逊弹性计算云 EC2 (亚马逊) 实例。当您使用 Lightsail 控制台或 Lightsail API 请求创建亚马逊 EC2 实例时，就会创建 CloudFormation 堆栈。堆栈在您的 Amazon Web Services (AWS) 账户中执行一系列操作，为该实例创建所有相关资源，例如来自亚马逊系统映像 (AMI) 的亚马逊 EC2实例、EBS 快照中的弹性块存储 (EBS) Elastic Block Store 系统卷以及该实例的安全组。要了解有关 AWS CloudFormation 堆栈的更多信息，请参阅文档中的使用堆栈。 AWS CloudFormation

你可以通过 Lightsail 控制台或在控制台中 AWS CloudFormation 访问 AWS CloudFormation 堆栈。本指南向您介绍如何通过这两种方式进行访问。

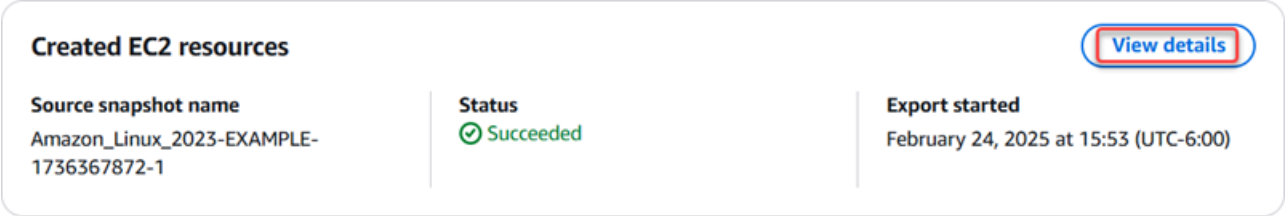
> **Note**
>
> 用于创建您的亚马逊 EC2 资源的 AWS CloudFormation 堆栈与您的亚马逊 EC2资源永久关联。如果您删除该堆栈，所有相关资源将会自动删除。因此，您不应删除 Lightsail 创建的任何 AWS CloudFormation 堆栈，而应使用 EC2 控制台删除您的 EC2 亚马逊资源。

通过 Lightsail 控制台访问 AWS CloudFormation 堆栈

在你选择 EC2 使用 Lightsail 控制台或 Lightsail API 在亚马逊创建实例后，系统会创建一个 AWS CloudFormation 堆栈，并在 Lightsail 控制台的 “导出” 部分跟踪其状态。要了解有关导出的更多信息，请参阅 在 Lightsail 中跟踪快照导出状态。

在 Lightsail 控制台中查看你的 AWS CloudFormation 堆栈

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中选择导出。
3. 要访问先前创建的 Amazon EC2 实例的 CloudFormation 堆栈，请为标有 “已创建的 EC2 资源” 的任务选择查看详情。

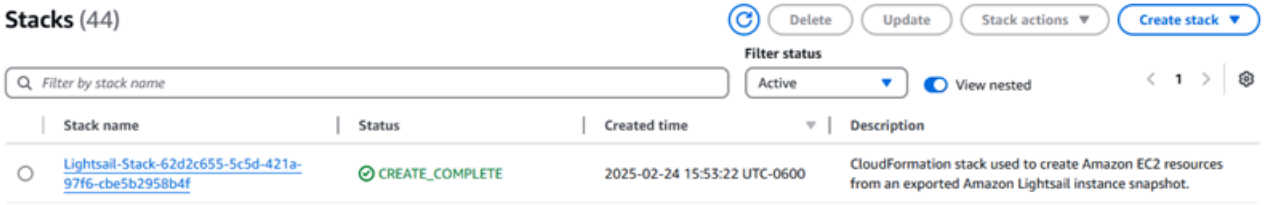


4. 出现的确认页面列出了该任务的 CloudFormation 堆栈。选择堆栈名称以在 AWS CloudFormation 控制台中打开堆栈详细信息。

在控制台中访问堆栈 AWS CloudFormation

您也可以通过 AWS CloudFormation 控制台访问堆栈详细信息。Lightsail 创建的堆栈以 “LightSail-Stack” 开头，描述了 “用于创建 EC2 亚马逊资源的CloudFormation 堆栈”，如以下屏幕截图所示。

状态为 CREATE_IN_PROGRESS 的堆栈正在根据导出的 Lightsail 快照创建亚马逊 EC2 资源。状态为 CREATE_COMPLETE D 的堆栈已完成创建亚马逊资源的过程。 EC2要查看由堆栈创建的资源，请选中堆栈名称旁边的复选框，然后选择 Resources (资源) 选项卡。


Stacks (44)
Delete
Update
Stack actions
Create stack
Filter status
Filter by stack name
Active
View nested
1
Stack name
Status
Created time
Description
Lightsail-Stack-62d2c655-5c5d-421a-97f6-cbe5b2958b4f
CREATE_COMPLETE
2025-02-24 15:53:22 UTC-0600
CloudFormation stack used to create Amazon EC2 resources from an exported Amazon Lightsail instance snapshot.

在 Lightsail 中为您的网站注册和管理域名

您的网站需要一个名称，如 `example.com`。使用 Amazon Lightsail，您可以为您的网站注册一个名称，即域名。要访问您的网站，用户需要在其 Web 浏览器中键入您的域名。

使用 Amazon Lightsail 控制台中的 “域名和 DNS” 选项卡注册和管理域名。Lightsail 使用 Amazon Route 53（一项高度可用且可扩展的域名系统 (DNS) 网络服务）为您注册域名。注册域名后，您可以将其分配给您的 Lightsail 资源或管理其的 DNS 记录。有关 DNS 的一般信息，请参阅 DNS。

有关在 Amazon Lightsail 中注册域名的更多信息，请继续阅读。

内容

- 域注册的工作原理
- 你可以在 Lightsail 中注册的域名
- 域注册定价

域注册的工作原理

以下概述显示了如何在 Amazon Lightsail 中注册域名：

1. 确认您想要的域名可以在互联网上使用。如果您想要的域名不可用，则您可以尝试其他名称，或仅将顶级域（例如 .com）更改为其他顶级域（如 .org 或 .net）。有关 Lightsail 支持的顶级域名 (TLDs) 的列表，请参阅您可以在 Amazon Lightsail 中注册的域名。
2. 在 Lightsail 上注册域名。注册域时，您可以提供域所有者和其他联系人的姓名和联系信息。

在注册过程结束时，我们会将您提供的信息发送给域注册商。域名注册商是一家经互联网名称与数字地址分配机构 (ICANN) 认可处理特定 TLDs域名注册的公司。域注册商为 Amazon Registrar 或我们的注册商合作者 Gandi。

Amazon Registrar 和 Gandi 默认隐藏不同的信息。Amazon Registrar, Inc. 会隐藏所有联系人信息，而 Gandi 会隐藏除组织名称以外的所有联系人信息。

- 要了解您的域名的注册商是谁，请参阅您可以在 Amazon Lightsail 中注册的域名。
- 该注册商会将您的信息发送给域的注册机构。注册机构是销售一个或多个顶级域（如 .com）的域注册的公司。

- 注册机构将有关您的域的信息存储在其自己的数据库中，并将一些信息存储在公共 WHOIS 数据库中。

有关如何注册域名的更多信息，请参阅注册新域。

使用 Lightsail 注册域名后，Route 53 会通过为你的域名分配一组域名服务器来使自己成为你的域名的 DNS 服务。名称服务器是帮助将域名转换为 IP 地址的服务器。

Lightsail 会自动执行以下操作以使自己成为该域的 DNS 服务：

- 创建与您的域名同名的 Lightsail DNS 区域。
- 将一组四个域名服务器分配给 Lightsail DNS 区域。
- 用你的 Lightsail DNS 区域中的域名服务器替换域名的 Route 53 域名服务器。

如果您已经向另一个注册商注册了域名，则可以选择将该域 DNS 的管理转移到 Lightsail。使用其他 Lightsail 功能则不需要执行此操作。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

你可以在 Lightsail 中注册的域名

Lightsail 使用的通用顶级域名 (TLDs) 与 Route 53 相同。有关可用于在 Lightsail 中注册域名的通用 TLDs 域名列表，请参阅《亚马逊 Route 53 开发者指南》中的可在亚马逊 Route 53 注册的域名。

如果 TLD 未包含在列表中，或者您想注册地理域，我们建议您使用 Route 53 控制台。使用 Route 53 注册后，您的地理域名将在 Lightsail 控制台中可用。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的地理顶级域。

域注册定价

Lightsail 使用 Route 53 进行域名注册。因此，53号公路的定价也适用于Lightsail的注册。

有关注册域费用的信息，请参阅《Amazon Route 53 开发人员指南》中的可在 Amazon Route 53 中注册的域。

有关域的其他信息

以下文章可以帮助你在 Lightsail 中管理域名：

- DNS

- 设置域名格式
- 管理 Amazon Route 53 中的 Lightsail 域名
- 创建 DNS 区域以管理域的 DNS 记录
- 域注册续订
- 编辑或删除 DNS 区域
- 将域指向负载均衡器
- 将域指向分配
- 将域指向实例
- 将域的流量路由到容器服务

了解 Lightsail 中的 DNS

人们可以通过浏览您的实例的公共互联网协议 (IP) 地址（可能是 IPv4 或 IPv6 地址）来访问您的 Lightsail 实例上的 Web 应用程序。不过，对用户来说，IP 地址往往复杂且难以记忆。因此，你应该让人们浏览到 easy-to-remember域名`example.com`，比如访问你的实例上的 Web 应用程序。域名系统 (DNS) 即可实现这一点，该系统充当将注册的域名映射到 IP 地址的目录。

要将域名的流量路由到您的 Lightsail 实例，您可以添加一条将您的域名指向您的实例静态 IPv4 地址的地址 (A) 记录，或者添加一条指向您的实例 IPv6 地址的 AAAA 记录。如果您使用 Lightsail 注册了域名，则可以管理注册域名时创建的 DNS 区域中的 DNS 记录。如果您的域名是通过其他注册商注册的，则可以在注册商处管理 DNS 记录，也可以将域名 DNS 的管理权转移到 Lightsail。

为了更轻松地将您的域名映射到 Lightsail 实例，我们建议您通过创建 DNS 区域将域名 DNS 记录的管理权转移到 Lightsail。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。你最多可以在 Lightsail 中创建六个 DNS 区域。如果需要六个以上的 DNS 区域，我们建议使用 Route 53 管理所有域的 DNS。你可以使用 Route 53 将你的域名指向你的 Lightsail 实例。有关使用 Route 53 管理 DNS 的更多信息，请参阅使用 Amazon Route 53 将域指向实例。

DNS 术语

为了管理域的 DNS，您应该先熟悉一些术语。

顶级域/根域

> 顶级域（也称为根域）是不包含子域部分的域。例如，`example.com` 就是一个顶级域。`www.example.com` 和 `blog.example.com` 则为子域。这些都是子域，因为它们分别包含 `www` 和 `blog` 子域部分。

域名系统（DNS）

DNS 将 easy-to-remember域名（例如`example.com`）路由到 Web 服务器的 IP 地址。

有关更多信息，请参阅 Wikipedia 上的域名系统。

DNS 记录

DNS 记录是一种映射参数，它将域（或子域）所关联的 IP 地址或主机名告知 DNS 服务器。

有关更多信息，请参阅 Wikipedia 上的 DNS 记录类型列表。

DNS 区域

DNS 区域是一种容器，用于存储有关如何路由特定域（如 `example.com`）及其子域（如 `blog.example.com`）上的 Internet 流量的信息。

有关更多信息，请参阅 Wikipedia 上的 DNS 区域。

域名注册商

域名注册商（也称为域名提供商）是管理域名分配的公司或组织。您可以使用 Lightsail、Amazon Route 53 或任何其他域名注册商购买域名或管理现有域名。

有关更多信息，请参阅 Wikipedia 上的域名注册商。

名称服务器

名称服务器将流量路由至您的域。在 Lightsail 中，域名服务器是一个运行网络服务以帮助将 easy-to-remember域名转换为 IP 地址的 AWS 实例。Lightsail 提供了多个 AWS 域名服务器选项（例如`ns-NN.awsdns-NN.com`），用于将流量路由到您的域名。使用域名注册商更改域 AWS 名时，您可以从这些域名服务器中进行选择。

有关更多信息，请参阅 Wikipedia 上的名称服务器。

子域

子域是域层次结构（而不是根域）中的属于大型域的任何内容。例如，`blog` 是 `blog.example.com` 子域的子域部分。

有关更多信息，请参阅 Wikipedia 上的子域。

生存时间 (TTL)

TTL 表示本地解析名称服务器上 DNS 记录的生命周期，TTL 越短，则更改生效所需的时间越短。无法在 Lightsail DNS 区域中配置 TTL。相反，所有 Lightsail DNS 记录的 TTL 默认为 60 秒。

有关更多信息，请参阅 Wikipedia 上的存活时间。

通配符 DNS 记录

通配符 DNS 记录用于匹配对不存在的域名的请求。通配符 DNS 记录是通过在域名最左侧使用星号 (*) 指定的，例如 `*.example.com` 或 `*example.com`。

> **Note**
>
> Lightsail DNS 区域支持域名服务器 (NS`*awsdns.com`) 记录中定义的域名服务器域 () 的通配符记录。

Lightsail DNS 区域支持的 DNS 记录类型

地址 (A) 记录

A 记录将域（如 `example.com`）或子域（如 `blog.example.com`）映射到 Web 服务器的 IP 地址。

例如，在 Lightsail DNS 区域中，您想将`example.com`（域的顶点）的网络流量定向到您的实例。您会创建一个 A 记录，在 Subdomain（子域）文本框中输入 @ 符号，然后将 Web 服务器的 IP 地址输入到 Resolves to address（解析为地址）文本框。

有关 A 记录的更多信息，请参阅 Wikipedia 上的 DNS 记录类型列表。

AAAA 记录

AAAA 记录将域名（例如`example.com`）或子域名（例如`blog.example.com`）映射到 Web 服务器的地 IPv6 址。

例如，在 Lightsail DNS 区域中，您想通过协议将`example.com`（域的顶点）的网络流量引导到您的实例。 IPv6您会创建一个 AAAA 记录，在 Subdomain（子域）文本框中输入 @ 符号，然后将 Web 服务器的 IP 地址输入 Resolves to address（解析为地址）文本框。

有关 AAAA 记录的更多信息，请参阅维基百科 IPv6上的域名系统。

> **Note**
>
> Lightsail 不支持静态地址 IPv6 。如果您删除了 Lightsail 资源并创建了新资源，或者在同一资源 IPv6 上禁用并重新启用，则可能需要更新 AAAA 记录以反映该资源的最新 IPv6 地址。

别名记录 (CNAME)

别名记录可将别名或子域（如 blog.example.com）映射到另一个域或子域。

例如，在 Lightsail DNS 区域中，你想将网络流量定www.example.com向到。example.com您可以为 www 创建一条别名记录，其中“解析为”地址为 example.com。

有关更多信息，请参阅 Wikipedia 上的别名记录。

邮件交换器 (MX) 记录

当定义了多个服务器时，MX 记录会将子域（如 mail.example.com）映射到带有优先级值的电子邮件服务器地址。

例如，在 Lightsail DNS 区域中，你想将邮件直接发送mail.example.com到10 inbound-smtp.us-west-2.amazonaws.com亚马逊 WorkMail 服务器。您可以创建一条 MX 记录，其中子域为 example.com，优先级为 10，“解析为”地址为 inbound-smtp.us-west-2.amazonaws.com。

有关更多信息，请参阅 Wikipedia 上的 MX 记录。

名称服务器 (NS) 记录

NS 记录将子域（如 test.example.com）委派给名称服务器（如 ns-NN.awsdns-NN.com）。

有关更多信息，请参阅 Wikipedia 上的名称服务器。

服务定位器 (SRV) 记录

SRV 记录可将子域（如 service.example.com）映射到具有优先级值、权重和端口号的服务地址。通话或即时消息收发是通常与 SRV 记录相关联的两项服务。

例如，在 Lightsail DNS 区域中，你想将流量引导至。service.example.com 1 10 5269 xmpp-server.example.com您可以创建一条 SRV 记录，其中优先级为 1，权重为 10，端口号为 5269，“映射到”地址为 xmpp-server.example.com。

有关更多信息，请参阅 Wikipedia 上的 SRV 记录。

文本 (TXT) 记录

TXT 记录将子域映射到纯文本。您可以创建 TXT 记录以向服务提供商确认您的域的所有权。

例如，在 Lightsail DNS 区域中，您希望在查询_amazonchime.example.com主机名23223a30-7f1d-4sx7-84fb-31bdes7csdbb时使用进行响应。您

可以创建一条 TXT 记录，其中子域值为 `_amazonchime`，“响应内容”值为 `23223a30-7f1d-4sx7-84fb-31bdes7csdbb`。

有关更多信息，请参阅 Wikipedia 上的 TXT 记录。

创建 DNS 区域来管理 Lightsail 实例的域名记录

要将域名（例如）的流量路由到 Amazon Lightsail 实例，您需要向域名的域名系统 (DNS) 添加一条记录。`example.com`您可以使用注册域名的注册商管理域名的 DNS 记录，也可以使用 Lightsail 管理这些记录。

我们建议您将域名 DNS 记录的管理权移交给 Lightsail。这使您能够在一个地方（LightSail）高效地管理您的域和计算资源。你可以通过创建 Lightsail DNS 区域来使用 Lightsail 管理你的域名的 DNS 记录。你最多可以创建六个 Lightsail DNS 区域。如果由于您需要管理六个以上的域名而需要六个以上的 DNS 区域，我们建议您使用 Amazon Route 53 管理所有域的 DNS。你可以使用 Route 53 将你的域名的流量路由到你的 Lightsail 资源。有关使用 Route 53 管理 DNS 的更多信息，请参阅使用 Amazon Route 53 将域指向实例。

本指南向您展示如何为您的域名创建 Lightsail DNS 区域，以及如何将域名 DNS 记录的管理权转移到 Lightsail。将域名 DNS 记录的管理权移交给 Lightsail 后，您将继续在域名注册商处管理域名的续订和账单。

> **Important**
>
> 您对域的 DNS 所做的任何更改都可能需要几个小时才能在 Internet 的 DNS 内传播。因此，在向Lightsail转移管理权时，您应该将域名的 DNS 记录保存在域名的当前 DNS 托管服务提供商处。这可确保域流量在转移期间继续不间断地路由到您的资源。

步骤 1：完成先决条件

请完成以下先决条件（如果尚未完成）：

1. 注册一个域名。然后，确认您有编辑域的名称服务器的管理访问权限。

   如果您需要注册域名，则可以使用 Lightsail 注册域名。有关更多信息，请参阅域注册。
2. 确认 Lightsail DNS 区域是否支持您的域所必需的 DNS 记录类型。Lightsail DNS 区域目前支持地址（A 和 AAAA）、规范名称（CNAME）、邮件交换器 (MX)、域名服务器 (NS)、服务定位器 (SRV) 和文本 (TXT) 记录类型。对于 NS 记录，您可以使用通配符 DNS 记录条目。

如果 Lightsail DNS 区域不支持您的域名所需的 DNS 记录类型，则您可能需要使用 Route 53 作为域名的 DNS 托管提供商，因为它支持更多的记录类型。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的支持的 DNS 记录类型和将 Amazon Route 53 作为现有域的 DNS 服务。

3. 创建一个 Lightsail 实例，你要将你的域指向该实例。有关更多信息，请参阅创建实例。
4. 创建静态 IP 并将其附加到您的 Lightsail 实例。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

第 2 步：在 Lightsail 控制台中创建 DNS 区域

完成以下步骤，在 Lightsail 中创建 DNS 区域。当您创建 DNS 区域时，您必须指定该 DNS 区域将应用于的域名。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择域和 DNS。然后，选择创建 DNS 区域。
3. 请选择以下选项之一：
   - 使用向 Amazon Route 53 注册的域，指定向 Amazon Route 53 注册的域
   - 使用其他注册商的域，指定使用其他注册商的域
4. 选择或输入注册的域名，例如 `example.com`。

   输入域名时，不必包含 `www`。您可以在执行本指南后面的步骤 3：向 DNS 区域添加记录部分时，使用地址 (A) 记录添加 `www`。

   > **Note**
   >
   > Lightsail DNS 区域是在弗吉尼亚州创建的 () `us-east-1`。 AWS 区域如果您在该区域中将资源命名为与要创建的 Lightsail DNS 区域 () 相同，则会收到资源名称冲突错误（“某些名称已在使用中”`example.com`）。
   > 要纠正该错误，请创建资源的快照。从快照创建新的资源并为其指定一个新的、唯一名称。然后，删除已命名为要为其创建 LightSail DNS 区的域相同的原始资源。

5. 选择 Create DNS zone（创建 DNS 区域）。

   您将重定向到 DNS 区域的 Assignments（分配）页面，并可在此管理域资源分配。使用分配将域指向您的 Lightsail 资源，例如负载均衡器和实例。

步骤 3：向 DNS 区域添加记录

完成以下步骤以将记录添加到您所在域的 DNS 区域。DNS 记录指定如何为域路由 Internet 流量。例如，您可以将顶级域（如 example.com）的流量路由到一个实例，同时将子域（如 blog.example.com）的流量路由到另一个实例。

1. 从 DNS 区域分配页面，选择 DNS records（DNS 记录）选项卡。

   你的 DNS 区域列在 Lightsail 控制台的 “域名和 DNS” 选项卡中。

   > **Note**
   >
   > 在 DNS 区域的 Assignments（分配）页面上，您可以添加、移除或更改域指向的 Lightsail 资源。您可以将域指向 Lightsail 实例、分配、容器服务、负载均衡器、静态 IP 地址等资源。您可以在 DNS records（DNS 记录）页面上添加、编辑或删除域的 DNS 记录。

2. 选择以下记录类型之一：

   地址 (A) 记录

   A 记录将域名（例如example.com）或子域名（例如）映射到 Web 服务器或实例的地 IPv4 址，例如192.0.2.255。blog.example.com

   1. 在 Record name（记录名称）文本框中，输入该记录的目标子域，或输入一个 @ 符号以定义顶级域名。
   2. 在 Resolves to（解析为）文本框中，输入该记录的目标 IP 地址，然后选择您正在运行的实例或配置的负载均衡器。选择正在运行的实例后，该实例的公有 IP 地址将会自动添加。
   3. 选择 “是 AWS 资源别名”，将流量路由到您的 Lightsail 和 AWS 资源，例如分发或容器服务。它们还允许您将流量从 DNS 区域中的一个记录路由到另一个记录。

      > **Note**
      >
      > 我们建议您将静态 IP 附加到 Lightsail 实例，然后选择静态 IP 作为记录解析到的值。有关更多信息，请参阅创建静态 IP。

   AAAA 记录

   AAAA 记录将域名（例如example.com）或子域名（例如）映射到 Web 服务器或实例的地 IPv6 址，例如。blog.example.com 2001:0db8:85a3:0000:0000:8a2e:0370:7334

> **Note**
>
> Lightsail 不支持静态地址 IPv6 。如果您删除了 Lightsail 资源并创建了新资源，或者在同一资源 IPv6 上禁用并重新启用，则可能需要更新 AAAA 记录以反映该资源的最新 IPv6 地址。

1. 在 Record name（记录名称）文本框中，输入该记录的目标子域，或输入一个 @ 符号以定义顶级域名。
2. 在 Resolves to 文本框中，输入记录的目标 IPv6地址，选择正在运行的实例或配置的负载均衡器。当您选择正在运行的实例时，会自动添加该实例的公共 IPv6 地址。
3. 选择 “是 AWS 资源别名”，将流量路由到您的 Lightsail 和 AWS 资源，例如分发或容器服务。它们还允许您将流量从 DNS 区域中的一个记录路由到另一个记录。

别名记录 (CNAME)

别名记录将别名或子域（如 `www.example.com`）映射到另一个域（如 `example.com`）或另一个子域（如 `blog.example.com`）。

1. 在 Record name（记录名称）文本框中，输入该记录的子域。
2. 在 Route traffic to（将流量路由到）文本框中，输入该记录的目标域或子域。

邮件交换器 (MX) 记录

当定义了多个服务器时，MX 记录会将子域（如 `mail.example.com`）映射到带有优先级值的电子邮件服务器地址。

1. 在 Record name（记录名称）文本框中，输入该记录的子域。
2. 在 Priority（优先级）文本框中，输入该记录的优先级。在为多个服务器添加记录时，这点非常重要。
3. 在 Route traffic to（将流量路由到）文本框中，输入该记录的目标域或子域。

服务定位器 (SRV) 记录

SRV 记录可将子域（如 `service.example.com`）映射到具有优先级值、权重和端口号的服务地址。通话或即时消息收发是通常与 SRV 记录相关联的两项服务。

1. 在 Record name（记录名称）文本框中，输入该记录的子域。
2. 在 Priority（优先级）文本框中，输入该记录的优先级。
3. 在 Weight（权重）文本框中，输入具有相同优先级的 SRV 记录的相对权重。

4. 在 Route traffic to（将流量路由到）文本框中，输入该记录的目标域或子域。
5. 在 Port（端口）文本框中，输入可在其中建立到服务的连接的端口号。

文本 (TXT) 记录

TXT 记录可将子域映射到纯文本。您可以创建 TXT 记录以向服务提供商确认您的域的所有权。

1. 在 Record name（记录名称）文本框中，输入该记录的子域。
2. 在 Responds with（响应内容）文本框中，输入查询子域时给出的文本响应。

> **Note**
>
> 输入文本不需要用引号括起来。

3. 添加完记录后，请选择 Save（保存）图标，以保存您的更改。

记录已添加到 DNS 区域。重复上述步骤，以将多个记录添加到您所在域的 DNS 区域。

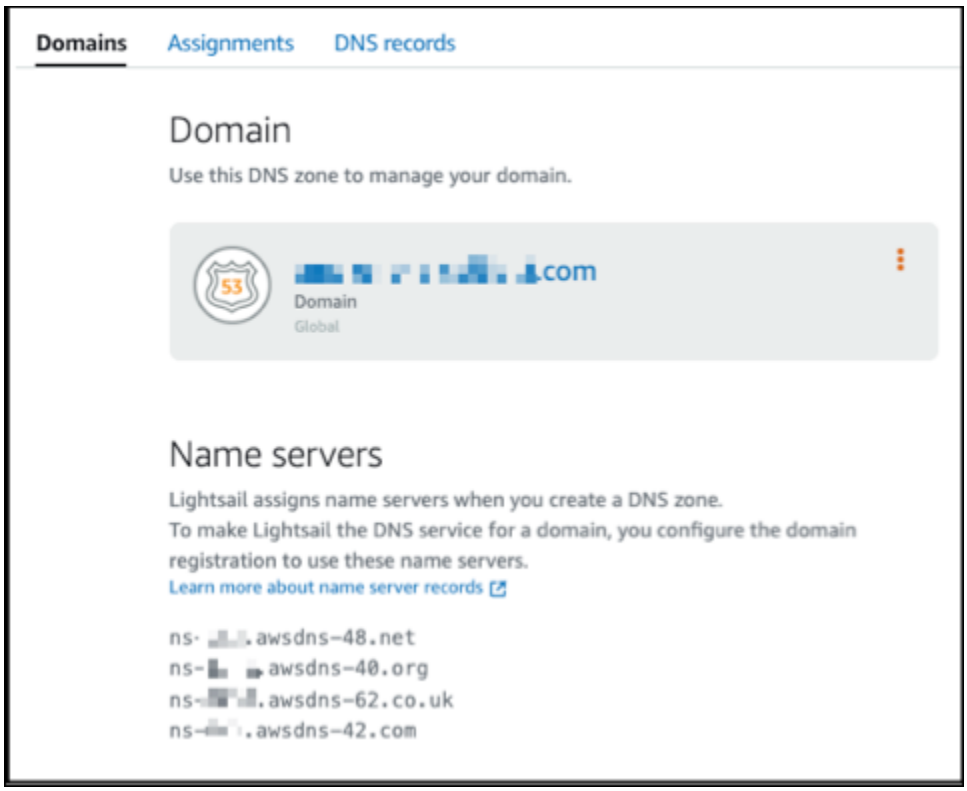
> **Note**
>
> 无法在 Lightsail DNS 区域中配置 DNS 记录的生存时间 (TTL)。相反，所有 Lightsail DNS 记录的 TTL 默认为 60 秒。有关更多信息，请参阅 Wikipedia 上的存活时间。

步骤 4：通过您所在域的当前 DNS 托管提供商更改名称服务器

完成以下步骤，将您的域名 DNS 记录的管理权转移到 Lightsail。为此，您需要登录域名的当前 DNS 托管服务提供商的网站，并将域名的名称服务器更改为 Lightsail 域名服务器。

> **Important**
>
> 如果当前正在将网络流量路由到您的域名，请确保所有现有 DNS 记录都存在于 Lightsail DNS 区域中，然后再更改域名的当前 DNS 托管提供商的域名服务器。这样，流量可以在传输到 Lightsail DNS 区域后持续不间断地流动。

1. 写下你域名的 DNS 区域管理页面上列出的 Lightsail 域名服务器。域名服务器位于 Lightsail DNS 区域的 “域名” 选项卡上。



2. 登录到您的域的当前 DNS 托管提供商的网站。
3. 找到可从中编辑域的名称服务器的页面。

   有关找到此页面的更多信息，请参阅您的域的当前 DNS 托管提供商提供的文档。
4. 输入 Lightsail 域名服务器，然后移除列出的其他域名服务器。
5. 保存您的更改。

   请等待一段时间，以便名称服务器更改在 Internet 的 DNS 内进行传播，这可能需要几个小时。完成后，您所在域的 Internet 流量路由应开始在 Lightsail DNS 区内路由。

后续步骤

- 编辑 DNS 区域
- 创建负载均衡器并向其附加实例

编辑 Lightsail DNS 区域

在域的 DNS 区域中编辑 DNS 记录。如果您想将域名 DNS 记录的管理权转移给其他 DNS 托管服务提供商或移交给您注册域名的注册商，也可以在 Amazon Lightsail 中删除您域名的 DNS 区域。有关更多信息，请参阅 ???

> **Note**
>
> 在使用 Lightsail 控制台中的 DNS 编辑器编辑记录之前，必须将域名 DNS 记录的管理权转移到 Lightsail。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

编辑 DNS 记录

您可以随时使用 Lightsail 控制台编辑您域名的 DNS 区域的 DNS 记录。

编辑 DNS 区域

1. 登录 Lightsail 控制台。
2. 在 Lightsail 控制台主页上，在左侧导航窗格中，选择 “域名和 D NS”。
3. 选择要编辑的 DNS 区域的名称。
4. 在 DNS 区域 DNS 记录页面上，选择要删除的记录旁边的删除图标。
5. 完成操作后，选择保存图标以保存您的更改。

> **Note**
>
> 给 DNS 记录一些时间在 Internet 的 DNS 内进行传播，这可能需要几个小时。

在 Lightsail 中删除 DNS 区域

在某些情况下，您可能需要完全删除您在 Amazon Lightsail 中为管理域名的 DNS 记录而设置的 DNS 区域。也许您想将 DNS 管理转移给其他提供者，或者将其转移回您的域注册商。删除 DNS 区域是一个简单的过程，但重点是要提前做好计划，以确保您的域流量继续正确路由。让我们来看看在 Lightsail 中删除 DNS 区域的步骤。

> **Important**
>
> 如果您计划继续通过您的域名路由流量，请在删除 Lightsail 中域名的 DNS 区域之前，先准备好其他的 DNS 托管提供商。否则，当您删除 Lightsail DNS 区域时，您的网站的所有流量都会停止。

删除 DNS 区域

1. 在 Lightsail 控制台主页上，在左侧导航窗格中，选择 “域名和 D NS”。
2. 选择要删除的 DNS 区域的名称。
3. 选择垂直省略号菜单（⋮）。然后，选择 Delete（删除）选项。
4. 选择 Delete DNS zone（删除 DNS 区域）以确认删除。

   DNS 区域已从 Lightsail 中删除。

在 Lightsail 中了解互联网流量是如何路由到你的网站的

互联网上的所有计算机，包括智能手机、笔记本电脑和网站服务器，都使用唯一的字符串相互通信。称为 IP 地址的这些字符串采用以下格式之一：

- 互联网协议版本 4 (IPv4) 格式，例如 192.0.2.44
- 互联网协议版本 6 (IPv6) 格式，例如 2001:DB8: /32

当您打开浏览器访问某个网站时，您不需要记住并输入像这么长的一串字符。相反，您可以输入像 example.com 这样的域名，仍然可访问预期的网站。域名系统 (DNS) 即可实现这一点，该系统充当将注册的域名映射到 IP 地址的目录。

内容

- 概述如何配置 Lightsail 以路由域名的互联网流量
- 如何为您的域路由流量
- 后续步骤

概述如何配置 Lightsail 以路由域名的互联网流量

本概述介绍了如何使用 Lightsail 注册和配置将互联网流量路由到您的网站或 Web 应用程序的域。

1. 注册域名。有关概述，请参阅域注册。
2. 注册域名后，Lightsail 会自动创建一个与该域名同名的 DNS 区域。
3. Lightsail 控制台允许您轻松地将域分配给 Lightsail 资源，例如实例或负载均衡器。您还可以在您的 DNS 区域中创建 DNS 记录，以将流量路由到您的资源。每个记录都包含有关如何要为您的域路由流量的信息，比如：

   名称

   记录的名称对应于域名（example.com）或子域名（www.example.com、retail.example.com）。DNS 区域中每个记录的名称必须以 DNS 区域的名称结尾。例如，如果 DNS 区域的名称为 example.com，则所有记录名称均必须以 example.com 结尾。

   类型

   记录类型通常取决于您希望流量路由到的资源的类型。例如，要将流量路由到电子邮件服务器，请将 Type（类型）指定为 MX。要将域名的流量路由到 Lightsail 实例，您可以添加一条将您的域名指向实例静态 IPv4 地址的 A 记录，或者添加一条指向您的实例 IPv6地址的 AAAA 记录。
4. 目标

   目标就是您想要将流量路由到的位置。您可以创建别名记录，将流量路由到 Lightsail 实例、Lightsail 容器服务和其他 Lightsail 资源。有关更多信息，请参阅 DNS。

如何为您的域路由流量

在将 Lightsail 配置为将互联网流量路由到您的资源（例如实例、负载均衡器、分布或容器服务）之后，当有人请求 www.example.com 的内容时会发生以下情况。

1. 用户打开 Web 浏览器并在地址栏中输入 www.example.com，然后按 Enter。
2. 对 www.example.com 的请求会被路由到 DNS 解析器，该解析器通常由用户的互联网服务提供商 (ISP) 管理。 ISPs可以是有线互联网提供商、DSL 宽带提供商或公司网络。
3. ISP 的 DNS 解析程序将对 www.example.com 的请求转发到 DNS 根名称服务器。
4. DNS 解析程序将再次转发对 www.example.com 的请求，而这次会转发到 .com 域的其中一个 TLD 名称服务器。.com 域的名称服务器使用与 example.com 域关联的四个名称服务器的名称来响应该请求。

   DNS 解析程序会缓存（存储）四个名称服务器。下次有人浏览到 example.com 时，解析程序将跳过步骤 3 和 4，因为它已缓存了 example.com 的名称服务器。名称服务器通常缓存时长为两天。

5. DNS 解析程序选择一个名称服务器，并将对 www.example.com 的请求转发到该名称服务器。
6. 名称服务器在 xample.com DNS 区域中查找 www.example.com 记录、获取关联值（比如 Web 服务器的 IP 地址 192.0.2.44）。然后，名称服务器将该 IP 地址返回到 DNS 解析程序。
7. DNS 解析程序最终将获得用户所需的 IP 地址。解析程序将该值返回给 Web 浏览器。
8. Web 浏览器将对 www.example.com 的请求发送到它从 DNS 解析程序那里获得的 IP 地址。例如，您的内容是在 Lightsail 实例上运行的 Web 服务器或配置为网站终端节点的容器服务。
9. 192.0.2.44 上的 Web 服务器或其他资源将 www.example.com 的网页返回到 Web 浏览器，而 Web 浏览器会显示该页面。

后续步骤

- DNS
- 将域指向实例
- 将域指向负载均衡器
- 将域指向分配

将域流量路由到 Lightsail 实例

您可以使用 Amazon Lightsail 中的 DNS 区域将注册域名（例如 example.com）指向在 Lightsail 实例（也称为虚拟专用服务器 (VPS)）上运行的网站。你可以在你的 Lightsail 账户中创建最多六个 DNS 区域。并非所有 DNS 记录类型均受支持。有关 Lightsail DNS 区域的更多信息，请参阅 DNS。

如果您希望创建六个以上的 DNS 区域或使用 Lightsail 不支持的 DNS 记录类型，我们建议您使用亚马逊 Route 53 托管区域。使用 Route 53，您可以管理多达 500 个域的 DNS。它还支持更多种类的 DNS 记录类型。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用托管区域。

本指南向您展示如何编辑在 Lightsail 中管理的域的 DNS 记录，使其指向您的 Lightsail 实例。给 DNS 区域更改留出最多 48 小时时间在互联网的 DNS 内进行传播。

先决条件

请完成以下先决条件（如果尚未完成）：

- 使用 Lightsail 注册域名。有关更多信息，请参阅注册新域。
- 如果您已经注册了域名，但没有使用 Lightsail 来管理其记录，则必须将域名的 DNS 记录的管理转移给 Lightsail。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

- 每次停止和重启实例时，连接到 Lightsail 实例的默认动态公有 IP 地址都会发生变化。创建一个静态 IP 并将其附加到您的实例，以防止公有 IP 地址发生变化。在本指南中，您将在域的 DNS 区域中创建解析为静态 IP 地址的 DNS 记录，这样您就不必在每次停止和重新启动实例时更新域的 DNS 记录。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

  可选-您可以将 Lightsail 实例保持 IPv6 启用状态。当您停止和启动实例时，该 IPV6 地址仍然存在。有关更多信息，请参阅启用和禁用 IPv6。

为 Lightsail 实例分配域名

使用以下方法之一为 Lightsail 中的实例分配域：

- Instance domains tab（实例域选项卡）
- Static IP domains tab（静态 IP 域选项卡）
- DNS zone assignments tab（DNS 区域分配选项卡）

实例域选项卡

在 Lightsail 控制台的 “域名和 DNS” 部分完成以下过程，将您的域分配给 Lightsail 实例。

使用实例 Domains（域）选项卡分配域

1. 登录 Lightsail 控制台。
2. 选择要为其分配域的实例名称。
3. 在 Domains（域）选项卡中选择 Assign domain（分配域）。
4. 选择要分配给 Lightsail 实例的域。
5. 验证路由信息是否正确，然后选择 Assign（分配）。

可选

要从实例中编辑或删除域分配，请选择域名旁边的编辑图标或垃圾箱图标。

静态 IP 域选项卡

完成以下过程，在 Lightsail 控制台的静态 IP 域和 DNS 选项卡中将您的域分配给 Lightsail 实例。

使用静态 IP Domains（域）选项卡分配域

1. 登录 Lightsail 控制台。

2. 选择 Networking（联网）选项卡。
3. 选择要将域分配到的静态 IP。
4. 在 Domains（域）选项卡中选择 Assign domain（分配域）。
5. 选择要分配给静态 IP 的域。
6. 验证路由信息是否正确，然后选择 Assign（分配）。

可选

要从静态 IP 中编辑或删除域分配，请选择域名旁边的编辑图标或垃圾箱图标。

DNS 区域分配选项卡

完成以下过程，在 DNS 区域的 “分配” 选项卡中将您的域分配给 Lightsail 实例。

使用 Assignments（分配）选项卡分配域

1. 登录 Lightsail 控制台。
2. 选择 Domains & DNS（域和 DNS）选项卡。
3. 选择要使用的域名的 DNS 区域。
4. 在 Assignments（分配）选项卡中，选择 Add assignment（添加分配）。
5. 选择要分配给 Lightsail 实例的域名。如果静态 IP 尚未附加到实例，则系统会提示您附加一个。
6. 验证路由信息是否正确，然后选择 Assign（分配）。

可选

要从资源中编辑或删除域分配，请选择域名旁边的编辑图标或垃圾箱图标。

将您的域名指向 Lightsail 负载均衡器

在您确认自己控制了要使用加密 (HTTPS) 流量的域名后，您需要向域名的 DNS 托管提供商添加地址 (A) 记录，该记录将您的域指向 Lightsail 负载均衡器。在本指南中，我们将向您展示如何将 A 记录添加到 Lightsail DNS 区域和亚马逊 Route 53 托管区域。

使用 DNS 区域 - 分配页面添加 A 记录

1. 在左侧导航窗格中，选择 域和 DNS。
2. 选择要管理的 DNS 区域。

3. 选择 Assignments（分配）选项卡。
4. 选择 Add assignment（添加分配）。
5. 在 Select a domain name（选择域名）字段中，选择是使用域名还是域的子域。
6. 在 Select a resource（选择资源）下拉列表中，选择要为其分配该域的负载均衡器。
7. 选择 Assign (分配)。

请等待一段时间，以便这些更改在 Internet 的 DNS 内进行传播。该过程可能需要几分钟到几小时的时间。

使用 DNS 区域 - DNS 记录页面添加 A 记录

1. 在左侧导航窗格中，选择 域和 DNS。
2. 选择要管理的 DNS 区域。
3. 选择 DNS records（DNS 记录）选项卡。
4. 根据 DNS 区域的当前状态，完成以下其中一个步骤：
   - 如果您尚未添加 A 记录，请选择添加记录。
   - 如果您之前添加了 A 记录，请选择页面上列出的现有 A 记录旁边的编辑图标，然后跳到此过程的步骤 5。
5. 在记录类型下拉菜单中，选择 A 记录。
6. 在 Record name（记录名称）文本框中，输入以下选项之一：
   - 输入 @ 将到顶级域（例如 `example.com`）的流量路由到负载均衡器。
   - 输入 `www` 将 www 子域（例如 `www.example.com`）的流量路由到负载均衡器。
7. 在 “解析为” 文本框中，选择 Lightsail 负载均衡器的名称。
8. 选择保存图标。

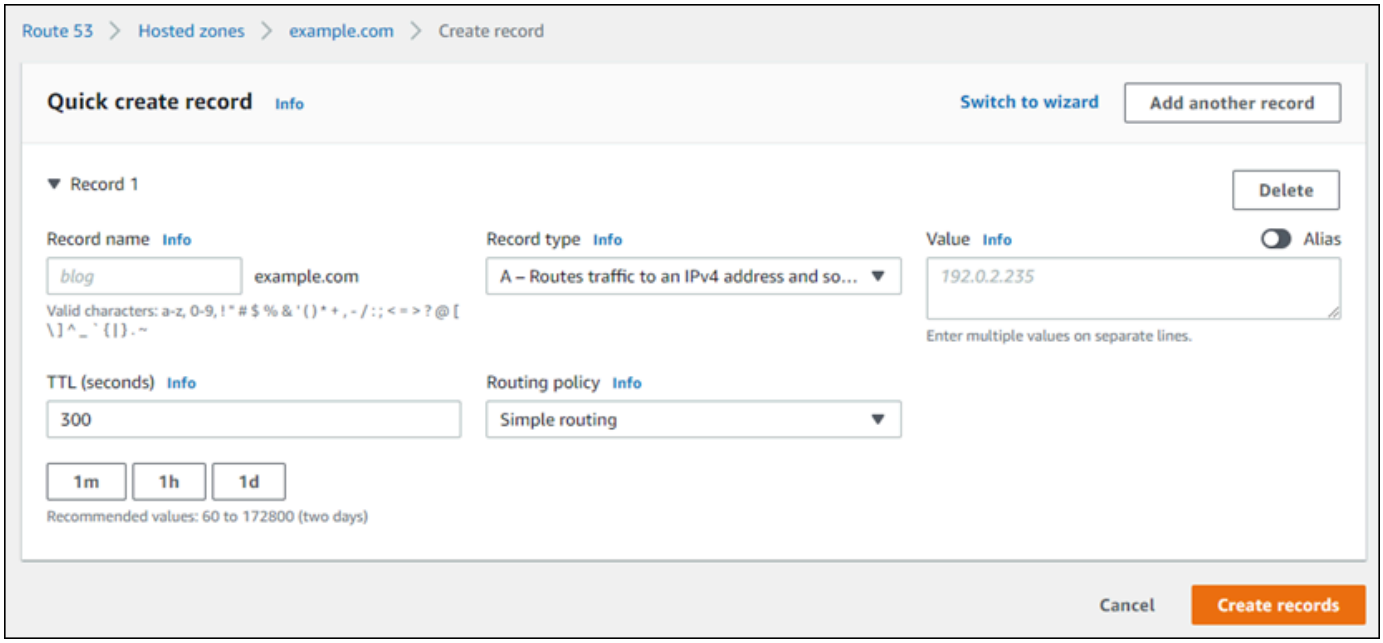
请等待一段时间，以便这些更改在 Internet 的 DNS 内进行传播。该过程可能需要几分钟到几小时的时间。

在 Route 53 中添加 A 记录

1. 登录 Route 53 控制台。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 为要用于将流量路由到负载均衡器的域名选择托管区域。

4. 选择创建记录。

   快速创建记录页面显示。



> **Note**
>
> 如果您看到选择路由策略页面，则选择切换到快速创建以切换到快速创建向导，然后继续执行以下步骤。

5. 对于记录名称，键入www（如果您计划使用 www 子域（即 www.example.com）），或将其留空（如果您计划使用顶级域（即example.com））。
6. 对于记录类型，选择 A-将流量路由到一个 IPv4地址和一些 AWS 资源。
7. 选择别名以启用别名记录。
8. 对于将流量路由到选择以下选项：

   a. 对于选择端点中，选择应用程序和经典负载均衡器的别名。

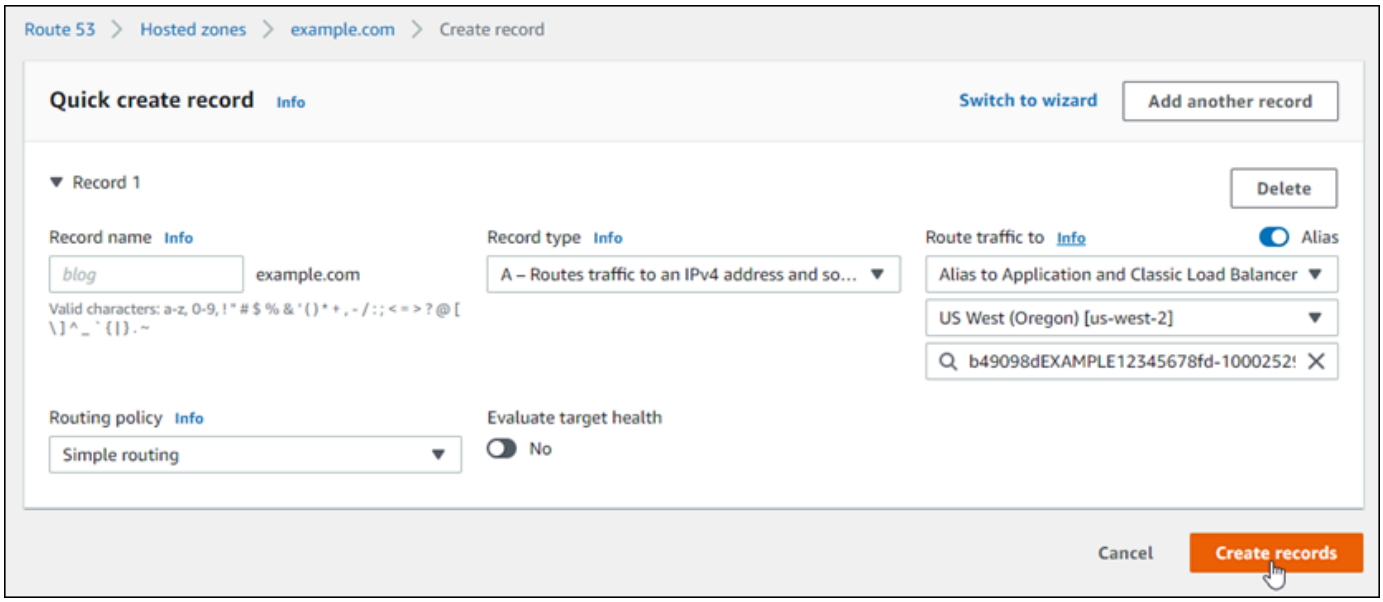
   b. 在选择区域中，选择您在其中创建 Lightsail 负载均衡器的 AWS 区域。

   c. 在 “选择负载均衡器” 中，输入或粘贴 Lightsail 负载均衡器的终端节点 URL（即 DNS 名称）。

9. 对于路由策略，选择简单路由，并禁用 Evaluate Target Health 切换。

   Lightsail 已经对您的负载均衡器执行运行状况检查。有关更多信息，请参阅对负载均衡器进行运行状况检查。

您的记录应类似于以下示例：



10. 选择Create records (创建记录)以将记录添加到托管区域。

> **Note**
>
> 请等待一段时间，以便这些更改在 Internet 的 DNS 内进行传播。该过程可能需要几分钟到几小时的时间。

转移你的 Lightsail 域名的 DNS 管理权限

您可以使用 Amazon Lightsail DNS 区域来管理使用 Lightsail 注册的域名的 DNS 记录。或者，如果您希望，您可以将域的 DNS 记录管理转移到其他 DNS 托管提供商。在本指南中，我们将向您展示如何将您在Lightsail注册的域名的 DNS 记录管理转移到其他 DNS 托管提供商。

> **Important**
>
> 您对域的 DNS 所做的任何更改都可能需要几个小时才能在互联网的 DNS 内传播。因此，您应将域的 DNS 记录保存在当前的 DNS 托管提供商处，直到完成管理转移。这可确保域流量在转移期间继续不间断地路由到您的资源。

内容

- 完成先决条件
- 向 DNS 区域添加记录

完成 先决条件

请完成以下先决条件（如果尚未完成）：

1. 注册一个域名。你可以使用 Lightsail 注册域名。有关更多信息，请参阅注册新域。
2. 使用 DNS 服务提供的过程获取域的名称服务器。

向 DNS 区域添加记录

完成以下步骤，将另一个 DNS 托管提供商的域名服务器添加到您在 Lightsail 中的注册域中。

1. 登录 Lightsail 控制台。
2. 选择 Domains & DNS（域和 DNS）选项卡。
3. 选择您要配置为使用其他 DNS 服务的域的名称。
4. 选择 Edit Name Servers（编辑名称服务器）。
5. 将名称服务器的名称更改为您完成先决条件后从 DNS 服务获取的名称服务器。
6. 选择保存。

使用亚马逊 Route 53 将域名指向你的 Lightsail 实例

Amazon Lightsail 中的 DNS 区域可以轻松地将注册域名（比如`example.com`）指向在 Lightsail 实例上运行的网站。您最多可以创建六个 Lightsail DNS 区域，但并非所有的 DNS 记录类型都受支持。有关 Lightsail DNS 区域的更多信息，请参阅 DNS。

如果 Lightsail DNS 区域对你来说太有限了，那么我们建议你使用亚马逊 Route 53 托管区域来管理你的域名的 DNS 记录。使用 Route 53 时，您可管理多达 500 个域的 DNS，并且支持各种 DNS 记录类型。或者，您可能已在使用 Route 53 管理您所在域的 DNS 记录，并希望继续使用。本指南向您展示如何编辑在 Route 53 中管理的域的 DNS 记录以指向您的 Lightsail 实例。

先决条件

请完成以下先决条件（如果尚未完成）：

- 使用 Route 53 注册域名。有关更多信息，请参阅 Route 53 文档中的注册新域。
- 如果您已注册一个域，但未使用 Route 53 来管理其记录，则必须将对您所在域的 DNS 记录的管理工作转移给 Route 53。有关更多信息，请参阅 Route 53 文档中的将 Amazon Route 53 作为现有域的 DNS 服务。
- 在 Route 53 中为您所在域创建一个公有托管区。有关更多信息，请参阅 Route 53 文档中的创建公有托管区。
- 创建静态 IP 并将其附加到您的 Lightsail 实例。在本指南中，您将在您所在域的 Route 53 托管区中创建 DNS 记录，该记录解析为实例的静态 IP 地址（公有 IP 地址）。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

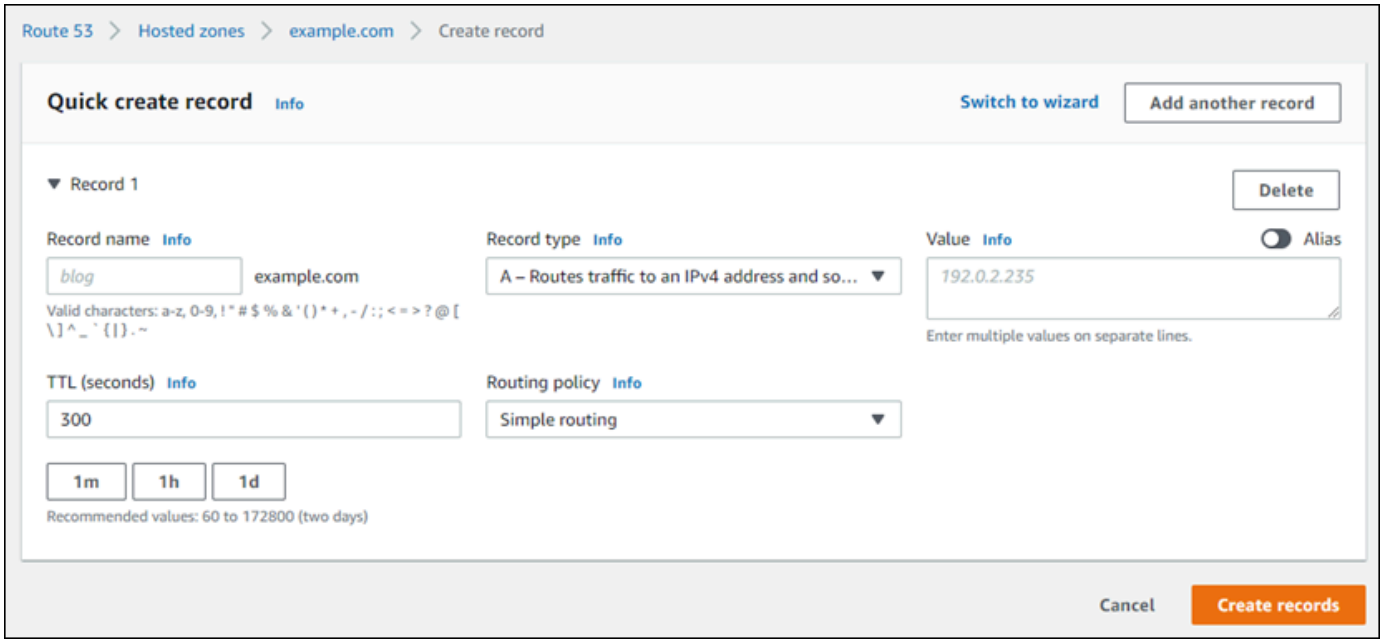
使用 Route 53 将域名指向 Lightsail 实例

完成以下步骤，在 Route 53 中配置两个最常见的 DNS 记录（地址和规范名称），以将您的域指向 Lightsail 实例。

> **Note**
>
> 《Route 53 开发人员指南》中也记录了此过程。有关更多信息，请参阅 Route 53 文档中的使用 Amazon Route 53 控制台创建记录。

1. 登录 Route 53 控制台。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 为要用于将流量路由到负载均衡器的域名选择托管区域。
4. 选择创建记录。

   快速创建记录页面显示。



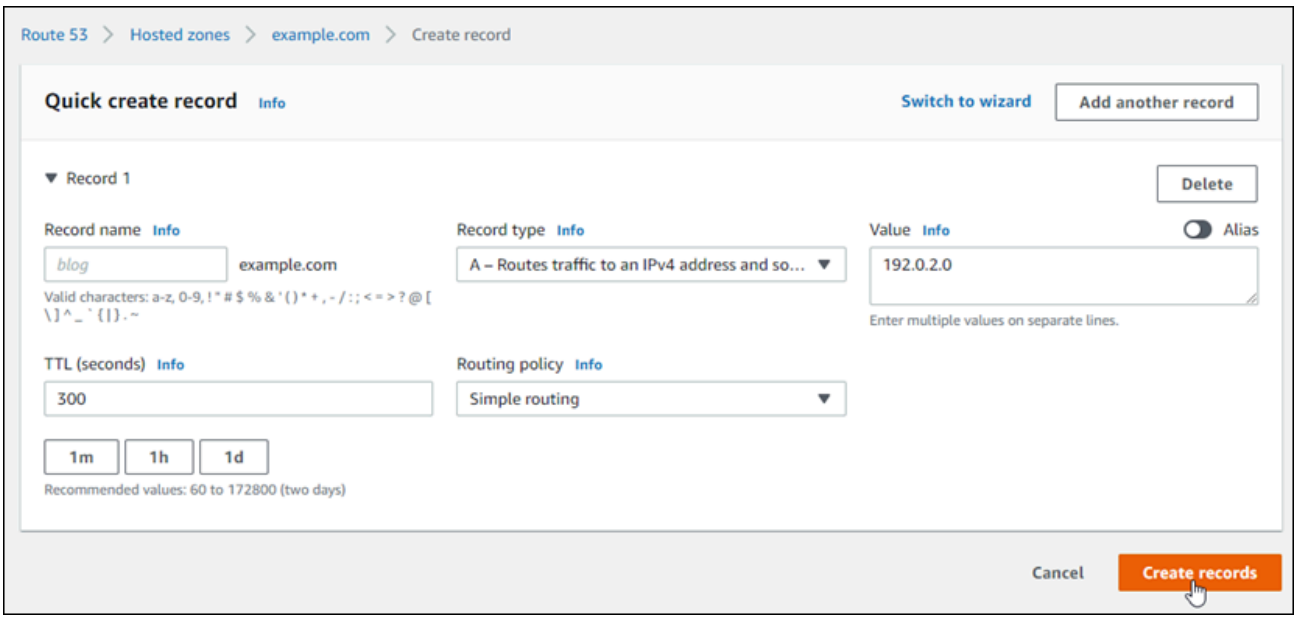
> **Note**
>
> 如果您看到选择路由策略页面，则选择切换到快速创建以切换到快速创建向导，再继续执行以下步骤。

5. 对于 Record type (记录类型)，选择以下选项之一：

A-将流量路由到某个 IPv4 地址和一些 AWS 资源

地址 (A) 记录将域（如 `example.com`）或子域（如 `blog.example.com`）映射到 Web 服务器的 IP 地址（如 `192.0.2.255`）。

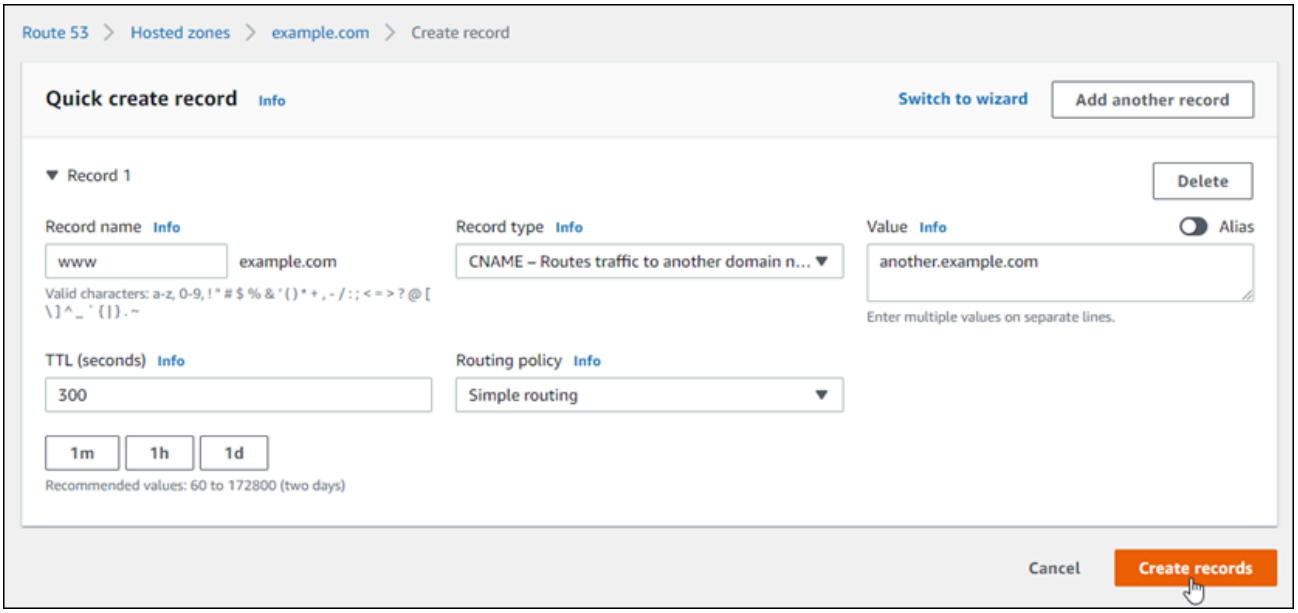
1. 将 Record name (记录名称) 文本框保留为空以将顶级域（如 `example.com`）指向 IP 地址，或者输入子域。
2. 在记录类型下拉菜单中选择 A-将流量路由到 IPv4 地址和一些 AWS 资源。
3. 在值文本框中输入您的 Lightsail 实例的静态 IP 地址（公有 IP 地址）。
4. 将 TTL 保持为 300，路由策略保持为简单路由。



别名记录 - 将流量路由到另一个域名和某些亚马逊云科技资源

规范名称记录（别名记录）将别名或子域（如 `www.example.com`）映射到域（如 `example.com`）或子域（如 `www2.example.com`）。别名记录将一个域重新导向到另一个域。

1. 在 Name (名称) 文本框中输入子域。
2. 在 Record type (记录类型) 下拉菜单中，选择 CNAME - Routes traffic to another domain name and to some Amazon Web Services resources (别名记录 - 将流量路由到另一个域名和某些亚马逊云科技资源)。
3. 在 Value (值) 文本框中输入域（即 `example.com`）或子域（即 `another.example.com`）。
4. 将 TTL 保持为 300，路由策略保持为简单路由。



6. 选择Create records (创建记录)以将记录添加到托管区域。

> **Note**
>
> 请等待一段时间，以便这些更改在 Internet 的 DNS 内进行传播。该过程可能需要几分钟到几小时的时间。

要编辑 Route 53 托管区中的现有记录集，请选择要编辑的记录，输入您的更改，然后选择保存。

在 Lightsail 中注册域名

您可以使用 Amazon Lightsail 注册新域名。Lightsail 域名通过 Amazon Route 53 注册，这是一项高度可用且可扩展的 DNS 网络服务。如果您有在其他提供商处注册的域名，则可以将这些域名的 DNS 管理转移到 Lightsail。你也可以将这些域名指向你的 Lightsail 资源。

选择以下步骤之一向 Lightsail 注册新域名：

- 要注册新域名，请参阅使用 Lightsail 注册新域名。
- 对于现有域，请参阅创建 DNS 区域以管理域的 DNS 记录。
- 要将域名移至其他注册商，请参阅在 Amazon Route 53 中管理 Lightsail 域名。

开始之前，请注意以下域注册注意事项：

域注册定价

有关注册域的费用的信息，请参阅 Amazon Route 53 定价指南。

域服务限额

您可以注册的域数量有限制。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的服务限额。如果要提高限制，请联系 Route 53。

支持的域

Lightsail 支持注册所有通用顶级域名 () TLDs。有关支持的域名列表 TLDs，请参阅《亚马逊 Route 53 开发者指南》中的可在亚马逊 Route 53 注册的域名。

您必须使用 Route 53 注册地理顶级域。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的地理顶级域。

注册后域名不能更改

如果您意外地注册了错误的域名，将无法进行更改。而是必须注册新的域名并指定正确的名称。意外注册的域名不予退款。

DNS 区域的费用

当您向 Lightsail 注册域名时，我们会自动为该域名创建 DNS 区域。Lightsail 不收取 DNS 区域的费用。

使用 Lightsail 注册一个新域名

主题

- 注册新域名的先决条件
- 注册新域
- 验证域联系人信息

注册新域名的先决条件

确认 Lightsail DNS 区域是否支持您的域所必需的 DNS 记录类型。Lightsail DNS 区域目前支持地址 (A)、规范名称 (CNAME)、邮件交换器 (MX)、域名服务器 (NS)、服务定位器 (SRV) 和文本 (TXT) 记录类型。对于 NS 记录，您可以使用通配符 DNS 记录条目。

如果 Lightsail DNS 区域不支持您的域名所需的 DNS 记录类型，则您可能需要使用 Route 53 作为域名的 DNS 托管提供商。Route 53 支持更多的记录类型。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的支持的 DNS 记录类型和将 Amazon Route 53 作为现有域的 DNS 服务。

注册新域

注册新域

1. 登录 Lightsail 控制台。
2. 选择 Domains & DNS（域和 DNS）选项卡。
3. 选择 Register domain（注册域），并指定要注册的域。
   a. 输入要注册的域名，选择 Check availability（检查可用性）来了解该域名是否可用。如果域可用，请继续 Automatic domain renewal（自动续订域）。
   b. 如果域名不可用，您将看到希望注册的其他域的列表，以代替首选域，或者在首选域之外注册其他域。为您想要注册的域选择 Select（选择）。
4. 选择是否在到期日期前自动续订您的域注册。注册一个域名后，您默认拥有该域名一年。如果您不更新您的域名注册，则将会过期，而其他人可以注册该域名。为确保保留您的域名，您可以选择每年自动续订，也可以选择更长的期限。
5. 在 Domain contact information（域联系人信息）部分中，输入域注册人、管理员和技术联系人的联系信息。有关更多信息，请参阅 Values that you specify when you register or transfer a domain（您在注册或转移域时指定的值）。

   请注意以下注意事项：

   名字和姓氏

   对于 First name（名字）和 Last Name（姓氏），我们建议您指定官方 ID 上的姓名。对于域设置的某些更改，有些域注册机构要求您提供身份证明。您的 ID 的姓名必须与该域的注册联系人的姓名匹配。

   不同联系人

   默认情况下，我们对全部三个联系人使用相同信息。如果要为一个或多个联系人输入不同的信息，请取消选中 Same as registrant（与注册人相同）复选框，然后输入新的联系人信息。
6. 在 Privacy protection（隐私保护）部分中，选择是否要在 WHOIS 查询中隐藏您的联系信息。

   有关更多信息，请参阅以下主题：

   - Privacy protection（隐私保护）
   - 可向 Amazon Route 53 注册的域

7. 选择 Register domain（注册域）以继续。DNS zones（DNS 区域）和 Summary（摘要）部分显示有关域的 DNS 区域、定价和续订计划的信息。
8. 您必须接受 Amazon Route 53 域名注册协议才能注册域。

验证域联系人信息

注册域后，必须验证注册人联系人的电子邮件地址是否有效。

我们将从以下电子邮件地址之一自动发送验证电子邮件：

- noreply@registrar.amazon — 适用于以亚马逊注册商为注册商的域名。
- noreply@domainnameverification.net — 适用于由我们的注册商助理 Gandi 作为注册商的域名。要确定您的 TLD 的注册商是谁，请参阅《Amazon Route 53 开发人员指南》中的可向 Amazon Route 53 注册的域。

使用以下过程完成域验证流程。

完成域验证

1. 当您收到验证电子邮件时，请选择电子邮件中用于确认电子邮件地址是否有效的链接。如果您没有立即收到该电子邮件，请检查垃圾电子邮件文件夹。
2. 返回 Lightsail 控制台。如果状态没有自动更新为 Verified（已验证），请选择 Refresh status（刷新状态）。

> **Important**
>
> 注册联系人必须按照电子邮件中的说明来验证已收到电子邮件，否则我们将按照 ICANN 的要求暂停该域。域被暂停后，将无法在 Internet 上访问该域。

3. 域名注册完成后，选择是使用 Lightsail 作为您的 DNS 服务，还是使用其他 DNS 服务。
   - Lightsail

     在 Lightsail 在你注册域名时创建的 DNS 区域中，创建记录以告诉 Lightsail 你想如何路由该域和子域的流量。

     例如，当有人在浏览器中输入您的域名并将该查询转发给 Lightsail 时，您希望 Lightsail 使用网络服务器的 IP 地址还是使用负载均衡器的名称来响应查询？ 有关更多信息，请参阅编辑或删除 DNS 区域。

- 使用其他 DNS 服务

  将您的新域配置为将 DNS 查询路由到 Lightsail 以外的 DNS 服务。有关更多信息，请参阅 Update the name servers for your domain when you want to use another DNS service（在您要使用其他 DNS 服务时更新域的名称服务器）。

查看向 Amazon Registrar 注册的域的注册详细信息

您可以查看有关使用亚马逊 Lightsail 和 Amazon Route 53 注册的.com、.net 和.org 域名的信息，亚马逊注册商是这些域名的注册商。此信息包括一些详细信息，例如域最初注册的时间以及域所有者以及技术和管理联系人的联系信息。

请注意以下几点：

在激活隐私保护的情况下向域联系人发送电子邮件

如果为域激活隐私保护，则注册人、技术和管理联系人的联系信息将替换为 Amazon Registrar 隐私服务的联系信息。例如，如果 example.com 域已在 Amazon Registrar 注册，并且激活了隐私保护，则对 WHOIS 查询的响应中的 Registrant Email（注册人电子邮件）的值将类似于 `owner1234@example.com.whoisprivacyservice.org`。

要在激活隐私保护的情况下联系一个或多个域联系人，请向相应的电子邮件地址发送电子邮件。我们会自动将您的电子邮件转发给相应的联系人。

举报滥用行为

要举报任何非法活动或违反可接受使用政策的行为，包括不当内容、网络钓鱼、恶意软件或垃圾邮件，请发送电子邮件至 trustandsafety@support.aws.com。

查看有关在 Amazon Registrar 中注册的域的信息

1. 在 Web 浏览器中，转到以下某个网站。两个网站都显示相同的信息。但是，它们使用不同的协议并以不同的格式显示信息：
   - WHOIS: https://registrar.amazon.com /whois
   - RDAP: https://registrar.amazon.com /rdap
2. 输入要查看其信息的域的名称，然后选择搜索。如果您搜索的域名不是使用 Amazon Lightsail 或 Route 53 注册的，那么您将看到一条消息，说明该域不在注册商数据库中。

在 Lightsail 中格式化域名

为了帮助人们访问网站或应用程序，请选择一个容易记住的域名。域名（以及 DNS 区域和记录的名称）由一系列以点号（.）分隔的标签组成。命名要求取决于您是注册域名还是指定 DNS 区域或记录的名称。

根据以下准则设置域名格式。

内容

- 为域名注册设置域名格式
- 为 DNS 区域和记录设置域名格式
- 在 DNS 区域和记录的名称中使用星号（*）
- 后续步骤

为域名注册设置域名格式

对于域名注册，您的域名必须包含 1-255 个字符。域名的有效字符包括（a-z）、（A-Z）、（0-9）、连字符（-）和句点（.）。

您不能在域名的开头或结尾处使用空格或连字符。Lightsail 支持任何有效的通用顶级域名 (TLD) 名称。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的通用顶级域。

为 DNS 区域和记录设置域名格式

对于 DNS 区域和记录，域名必须具有 1-255 个字符。域名的有效字符包括（a-z）、（A-Z）、（0-9）、连字符（-）和句点（.）。不能使用空格。

Lightsail 将字母字符存储为小写字母 (a-z)，即使您将其指定为大写字母 (A-Z) 也是如此。

Lightsail 支持通用和地理区域的 DNS 区域。 TLDs有关地理位置的更多示例 TLDs，请参阅 Amazon Route 53 开发者指南中的地理顶级域名。

在 DNS 区域和记录的名称中使用星号（*）

DNS 会将星号（*）字符作为通配符处理，具体视星号出现在名称中的位置而定。通配符 DNS 记录是应答您尚未定义的任何子域的 DNS 请求的记录。在 Lightsail 中，您可以创建名称中包含星号 (*) 的 DNS 区域和记录，条件如下：

DNS 区域

- 域名最左侧的标签中不能包含星号（*）。例如，你不能使用 *.ex ample.com。
- 如果在其他位置包含星号（*），DNS 会将其视为 ASCII 42 字符，而不是通配符。有关 ASCII 字符的更多信息，请参阅 Wikipedia 中的 ASCII。

DNS 记录

请注意有关在 DNS 记录名称中使用星号（*）作为通配符的以下限制：

- 作为通配符，星号必须替换域名中最左侧的标签，例如 *.example.com 或 *.acme.example.com。如果在任何其他位置包含星号（例如 prod.*.example.com），DNS 会将其视为 ASCII 42 字符，而不是通配符。
- 星号必须替换整个标签。例如，您不能指定 *prod.example.com 或 prod*.example.com。
- 具体的域名优先。例如，如果您为 *.example.com 和 acme.example.com 创建记录，则使用 acme.example.com 记录中的值响应对 acme.example.com 的 DNS 查询。
- 星号应用到针对包含星号的子域级别的 DNS 查询，以及该子域的所有子域。例如，如果您创建名为 *.example.com 的记录，则 *.example.com 的 DNS 查询将响应以下内容：

  zenith.example.com

  acme.zenith.example.com

  pinnacle.acme.zenith.example.com（如果该 DNS 区域没有任何类型的记录）

如果你创建了一条名为 *.example.com的记录但没有 example.com 记录，Light sail 会使用（不存在的域）来响应 example .com 的 DNS 查询。 `NXDOMAIN`

您可以将 Lightsail 配置为对同一级别的所有子域名以及该域名的 DNS 查询返回相同的响应。例如，你可以使用 example.com 记录将 Lightsail 配置为响应 acme.example.com 和 zenith.example.com 等 DNS 查询。执行以下步骤将子域的流量路由到 example.com 顶级域：

1. 为域创建记录，如 example.com。
2. 为子域创建别名记录，如 *.example.com。将您在上一步中创建的记录指定作为别名记录的目标。

后续步骤

有关更多信息，请参阅以下主题：

- 创建 DNS 区域以管理域的 DNS 记录
- DNS

使用 Route 53 的高级功能管理 Lightsail 域名

Amazon Lightsail 通过 Amazon Route 53 注册域名，这是一项高度可用且可扩展的 DNS 网络服务。当你使用 Lightsail 注册域名时，你可以在 Lightsail 和 Route 53 中同时管理该域名。

诸如注册域名以及将域的流量路由到 Lightsail 资源之类的任务都在 Lightsail 控制台中完成。有关更多信息，请参阅亚马逊 Lightsail 中的域名注册。

转移域和删除注册等高级任务必须在 Amazon Route 53 控制台中完成。

本指南提供有关您可以使用 Route 53 控制台完成的一些高级管理任务的信息。有关 Route 53 的完整概述，请参阅《Amazon Route 53 开发人员指南》中的什么是 Amazon Route 53？。

内容

- 查看域注册的状态
- 锁定域以防止未经授权转移到另一个注册商
- 恢复已到期或已删除的域
- 转移域
- 删除域名注册

查看域注册的状态

域名具有也称为可扩展预置协议（EPP）状态代码的状态。维护域名中央数据库的组织 ICANN 开发了 EPP 状态代码。EPP 状态码告诉您各种操作的状态。例如，注册域名、续订域名注册等。所有注册商都使用这组状态代码。要查看域的状态代码，请参阅《Amazon Route 53 开发人员指南》中的查看域注册的状态。

锁定域以防止未经授权转移到另一个注册商

所有通用顶级域名的域名注册机构 (TLDs) 允许您锁定域名，以防止有人在未经您许可的情况下将域名转让给其他注册商。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的锁定域以防止未经授权转移到另一个注册商。

恢复已到期或已删除的域

如果您在延迟续期结束之前没有续订域名，或者您不小心删除了该域名，则某些顶级域名注册机构 (TLDs) 允许您在域名可供其他人注册之前将其恢复。使用链接的过程尝试恢复您的域注册。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的恢复已到期或已删除的域。

转移域注册

您可以将域注册从另一个注册商转移到 Route 53，从一个 AWS 账户转移到另一个账户，或从 Route 53 转移到另一个注册商。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的转移域。

删除域名注册

对于大多数顶级域名 (TLDs)，如果您不再需要注册，则可以将其删除。如果注册机构允许您删除注册，请执行本主题中的过程。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的删除域名注册。

在 Lightsail 中注册或转移域名时提供域名信息

当您使用 Amazon Lightsail 注册域名时，您需要提供域名信息，例如注册期限（期限）和域名联系信息。您还可以配置自动域续订和隐私保护。

您还可以更改当前已在 Lightsail 注册的域名的信息。

> **Note**
>
> - 如果您更改域的联系人信息，我们会向注册联系人发送有关这一更改的电子邮件通知。这封电子邮件来自 noreply@registrar.amazon。对于大多数更改，注册联系人不需要响应。
> - 如果联系人信息更改还构成所有权更改，我们将向注册联系人另外发送一封电子邮件。维护域名中央数据库的组织 ICANN 要求注册人联系人确认收到电子邮件。有关更多信息，请参阅本节后面的 First name, last name（名字、姓氏）和 Organization（组织）。

有关更改现有域联系人信息的更多信息，请参阅更新域的联系人信息。

您提供的域信息

- 租期
- 自动域续订

- 注册人、管理、技术和账单联系人
- Contact type（联系人类型）
- 名字、姓氏
- 组织
- 电子邮件
- 电话
- Address 1（地址 1）
- Address 2（地址 2）
- 国家/地区
- 州/省
- 城市
- 邮政编码
- Privacy protection（隐私保护）

租期

域的注册期。该期限通常为一年，但您可以在注册域时将期限延长至十年。

自动域续订

当您向 Lightsail 注册域名时，我们会将该域名配置为自动续订。自动续订期通常为一年。选择是否让 Lightsail 在域名到期之前自动续订该域名。注册费将从您的 AWS 账户中扣除。有关更多信息，请参阅域注册续订。

> **Important**
>
> 如果您停用自动域续订，则到期日期过后将不续订域注册。因此，您可能会失去对域名的控制。

注册人、管理、技术和账单联系人

注册域名时需要以下联系人：

- 注册人-域名的所有者。

- 管理员- point-of-contact 负责管理域的人。
- 技术人员 — point-of-contact 负责对域名进行技术更改。
- 账单 — point-of-contact 负责查询有关域名的账单。

> **Note**
>
> 默认情况下，我们会使用您为注册人指定的相同信息，并将其应用于其他联系人。要为联系人输入不同的信息，请清除 “与注册人相同” 选项。

Contact type（联系人类型）

此联系人的类别。

> **Note**
>
> - 如果选择 Company（公司）或 Association（关联）选项，则必须输入组织名称。
> - 对于某些顶级域名 (TLDs)，隐私保护的可用性取决于您为联系人类型选择的值。有关您 TLD 的隐私保护设置，请参阅可向 Amazon Route 53 注册的域

名字、姓氏

联系人的名字和姓氏。对于 First name（名字）和 Last name（姓氏），我们建议您使用官方 ID 上的姓名。对于域设置的某些更改，您必须提供身份证明。在这些情况下，您的 ID 的姓名必须与该域的注册联系人的姓名匹配。

如果您更改注册联系人的电子邮件地址，我们会同时向新旧电子邮件地址发送此电子邮件。

组织

与联系人关联的组织 (如果有)。对于注册和管理联系人，此组织通常为注册该域的组织。对于技术联系人，此组织可以是管理该域的组织。

当联系人类型为 Person（个人）之外的任意值并且您更改了注册联系人的 Organization（组织）字段时，便会更改域所有者。ICANN 要求我们向注册联系人发送电子邮件以获得批准。电子邮件来自以下电子邮件地址之一：

- noreply@registrar.amazon — 适用于以亚马逊注册商为注册商的域名。
- noreply@domainnameverification.net — 适用于由我们的注册商助理 Gandi 作为注册商的域名。

要确定您 TLD 的注册商是谁，请参阅可向 Amazon Route 53 注册的域。

如果您更改注册联系人的电子邮件地址，我们会同时向新旧电子邮件地址发送此电子邮件。

电子邮件

联系人的电子邮件地址。

> **Note**
>
> 如果您更改注册联系人的电子邮件地址，我们会同时向新旧电子邮件地址发送通知电子邮件。这封电子邮件来自 noreply@registrar.amazon。

电话

联系人的电话号码：

- 如果您输入美国或加拿大境内位置的电话号码，请输入 1，然后输入 10 位带区号的电话号码。
- 如果要输入其他任何位置的电话号码，请输入国家/地区代码，后跟电话号码的其余部分。有关国家/地区呼叫代码的列表，请参阅 Wikipedia 上的 List of country calling codes（国家/地区呼叫代码列表）。

Address 1（地址 1）

联系人的街道地址或邮政信箱。

Address 2（地址 2）

联系人的其他地址信息，如公寓、套房、单元、大楼、楼层或邮寄地址。

国家/地区

联系人的国家/地区。

州/省

联系人的州或省 (如果有)。

城市

联系人的城市。

邮政编码

联系人的邮政编码。

Privacy protection（隐私保护）

选择是否向 WHOIS 查询隐藏您的联系人信息。如果您为域的联系人信息激活隐私保护，则 WHOIS（“谁是”）查询将返回域注册商的联系人信息，而不是您的个人信息。域注册商是管理域名注册的公司。

> **Note**
>
> 相同的隐私设置适用于管理、注册人和技术联系人。

如果停用域联系人信息的隐私保护，则您将在指定的电子邮件地址收到更多垃圾邮件。

任何人都可以发送针对某个域的 WHOIS 查询并获取该域的所有联系人信息。WHOIS 命令在许多操作系统中都可用，并且在许多网站中还可作为 Web 应用程序提供。

> **Important**
>
> 尽管有域联系人信息的合法用户，但最常见的用户是垃圾邮件发送者，他们的目标是向域联系人发送不需要的电子邮件和伪造优惠。一般来说，我们建议为 Contact information（联系人信息）激活 Privacy protection（隐私保护）。

有关隐私保护的更多信息，请参阅以下主题：

- 管理域的隐私保护

- 可向 Amazon Route 53 注册的域

在 Lightsail 中续订或停用域名注册

当您在 Amazon Lightsail 注册域名时，我们会将该域名配置为默认自动续订。默认的自动续订期限为一年，但某些顶级域名的注册机构 (TLDs) 的续订期限更长。所有通用域名都 TLDs 允许您将域名注册延长更长的期限，通常以一年为增量延长至十年。

> **Note**
>
> 如果您打算关闭自动续订，请务必停用自动续订。 AWS 账户否则，即使您关闭帐户，您的域注册也将续订。

内容

- Automatic renewal（自动续订）
- Configure automatic renewal for a domain during domain registration（在域注册期间为域配置自动续订）
- Configure automatic renewal for a domain that is already registered（为已注册的域配置自动续订）

Automatic renewal（自动续订）

以下时间线显示了自动续订激活时发生的情况：

到期前 45 天

我们会向注册人联系人发送一封电子邮件，告知您自动续费已激活。该电子邮件还包含有关如何停用自动续订的说明。使注册人联系人电子邮件地址保持最新，以免错过电子邮件。

到期前 35 天或 30 天

对于除 .com.ar、.com.br 和 .jp 域之外的所有域，我们会在到期日期前 35 天更新域注册。这样，我们就有时间在域名到期前解决任何续订问题。

.com.ar、.com.br 和 .jp 域的注册机构要求在域到期之前的 30 天内续订域。我们的联合注册商 Gandi 将在到期前 30 天发送续订电子邮件。如果自动续订已激活，则此电子邮件将在我们续订域的同一天发送。

如果自动续订未激活，则以下时间线显示域名到期日期临近时发生的情况：

到期前 45 天

我们会发送一封电子邮件通知注册人联系人自动续订当前未激活。该电子邮件还包含有关如何激活自动续订的说明。使注册人联系人电子邮件地址保持最新，以免错过电子邮件。

到期前 35 天和 7 天

如果域自动续订未激活，则域注册管理机构 ICANN 要求注册商向注册人联系人发送一封电子邮件。电子邮件来自以下电子邮件地址之一：

noreply@registrar.amazon — 适用于以亚马逊注册商为注册商的域名。

noreply@domainnameverification.net — 适用于由我们的注册商助理 Gandi 作为注册商的域名。

如果您在到期前 30 天内激活自动续订，则我们将在 24 小时内续订域注册。

有关续订时间段的更多信息，请参阅《Amazon Route 53 开发人员指南》的可向 Amazon Route 53 注册的域中有关您的 TLD 的“续订和恢复域的截止日期”部分。

到期日期之后

对于大多数域，注册商都会在域到期之后的短时间内予以保留，这样您便可以在到期日期之后续订已到期域，但如果您要保留域，我们强烈建议使自动续订功能保持活动状态。有关在到期日期之后尝试续订域的信息，请参阅《Amazon Route 53 开发人员指南》的恢复已到期或已删除的域。

如果您的域过期，但允许延迟续订，您可以按标准续订价格续订域。要确定某个域是否仍在延期续订期内，请执行《Amazon Route 53 开发人员指南》的延长域的注册期中的过程。如果仍列出了该域，则说明它仍在延期续订期内。

在域注册期间为域配置自动续订

当您向 Lightsail 注册新域名时，我们会将该域名配置为自动续订。您可以在域注册期间选择停用自动域续订。

1. 登录 Lightsail 控制台。
2. 选择 Domains & DNS（域和 DNS）选项卡。
3. 选择 Register domain（注册域）按钮。
4. 指定要向 Lightsail 注册的域名，然后选择 Check availability（检查可用性）。

5. 如果域名可用，则您将看到域注册页面。在 Automatic domain renewal（自动续订域）部分中，打开或关闭切换开关以激活或停用自动域续订。

为已注册的域配置自动续订

如果您想更改 Lightsail 是否在域名到期日前不久自动续订域名，或者想要查看当前的自动续订设置，请执行以下步骤。

1. 登录 Lightsail 控制台。
2. 选择 Domains & DNS（域和 DNS）选项卡。
3. 选择要查看或更新的域。
4. 选择 Contact info（联系人信息）选项卡
5. 5. 在 Automatic domain renewal（自动续订域）部分中，打开或关闭切换开关以激活或停用域注册期间的自动续订。

在 Lightsail 中管理域名联系人的隐私保护

当你在 Amazon Lightsail 上注册域名时，默认情况下，我们会为所有域名联系人激活隐私保护。这通常会在 WHOIS (即“Who is”) 查询中隐藏大多数联系信息，并减少收到的垃圾邮件数量。您的联系信息将被替换为注册商的联系信息或“REDACTED FOR PRIVACY”（掩蔽以保护隐私）短语。使用隐私保护不收取任何费用。

如果您选择停用隐私保护，任何人都可以发送该域名的 WHOIS 查询，对于大多数顶级域名 (TLDs)，他们可能能够获得您在注册域名时提供的所有联系信息。此信息包括姓名、地址、电话号码和电子邮件地址。WHOIS 命令可广泛使用。许多操作系统中都包含该命令，并且还以 Web 应用程序的形式存在于许多网站上。

要管理使用 Lightsail 注册的域名的隐私保护，请执行以下步骤。

内容

- 完成先决条件
- 管理域的隐私保护

完成 先决条件

在 Lightsail 上注册一个域名。有关更多信息，请参阅注册新域。

管理域的隐私保护

1. 登录 Lightsail 控制台。
2. 选择 Domains & DNS（域和 DNS）选项卡。
3. 选择希望为其更改隐私保护的域的名称。
4. 选择 Contact info（联系人信息）。
5. 您可以通过打开或关闭 Privacy protection（隐私保护）切换开关来管理联系人信息的隐私保护。

在 Lightsail 中更新域名联系信息

在 Amazon Lightsail 注册域名时，必须指定域名的联系信息。域联系人信息用于验证您的域的所有权，并让您随时了解与域名相关的任何最新信息。有关域名注册期间所需信息的更多信息，请参阅在 Lightsail 中注册或转移域名时提供域名信息。

主题

- Who is the owner of a domain?（域的所有者是谁？）
- 更新域的联系信息

Who is the owner of a domain?（域的所有者是谁？）

当联系人类型为 Person 时，如果您更改注册联系人的 First Name 或 Last Name 字段，就等于更改了域的所有者。

当联系人类型为 Person 以外的任何值时，如果您更改 Organization，就等于更改了域的所有者。

当您更改当前已在 Lightsail 注册的域名的联系信息时，会发生以下操作：

- 如果您更改域的联系人信息，我们会向注册联系人发送有关这一更改的电子邮件通知。这封电子邮件来自 noreply@registrar.amazon。对于大多数更改，注册联系人不需要响应。
- 如果联系人信息更改还构成所有权更改，我们将向注册联系人另外发送一封电子邮件。维护域名中央数据库的组织 ICANN 要求注册人联系人确认收到电子邮件。

更新域的联系信息

要更新域的联系信息，请执行以下过程。

1. 登录 Lightsail 控制台。
2. 选择 Domains & DNS（域和 DNS）选项卡。
3. 选择要更新的域的名称。
4. 选择 Contact info（联系人信息）选项卡。然后，选择 Edit contact（编辑联系人）。
5. 更新适用的值。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的您在注册或转移域时指定的值。
6. 选择保存。

在 Lightsail 中创建和管理关系数据库

只需几个步骤，您就可以在 Amazon Lightsail 中创建 MySQL 或 PostgreSQL 托管数据库。Lightsail 通过管理您的常见维护和安全任务，提高了数据库管理的效率。使用 Lightsail 控制台，你可以：

- 将数据库备份至快照。
- 从快照创建一个较大型的新数据库。
- 解决基于浏览器的日志和指标的常见问题。
- 使用 point-in-time备份和还原操作恢复数据。

您可以在 Lightsail 实例上构建您的应用程序，然后将其连接到 Lightsail 托管的数据库。您还可以创建一个独立的数据库，并为公司连接分析或查询工具。从每月收取固定费用的标准或高可用性数据库计划中进行选择，包括预配置的数据库、基于 SSD 的存储和数据传输分配。你也可以使用 AWS Command Line Interface (AWS CLI)、API 或 SDK 管理 Lightsail 数据库。

为您的项目选择正确的 Lightsail 数据库

Amazon Lightsail 提供 MySQL 和 PostgreSQL 数据库的最新主要版本。本指南可帮助您确定适合您项目的数据库。

Lightsail 还提供带有 SQL Server 的 Windows Server 2022 实例。有关更多信息，请参阅选择 Amazon Lightsail 实例镜像。

比较 Lightsail 中的托管数据库

MySQL

MySQL 5.7 和 8.0 在 Lightsail 中可用。MySQL 是应用最广泛的开源关系数据库。它用作许多常用网站、应用程序和商业产品的主关系数据存储。MySQL 是一种可靠、稳定且安全的基于 SQL 的数据库管理系统，拥有 20 多年的社区开发和支持历史。MySQL 数据库适用于各种使用案例，包括任务关键型应用程序和动态网站。它还用作软件、硬件和设备的嵌入式数据库。

> **Important**
>
> 从 2024 年 6 月 30 日起，Lightsail 将不再支持 MySQL 5.7，您将无法使用此蓝图创建新数据库。要了解如何升级数据库实例的主要版本，请参阅升级 Lightsail 数据库的主要版本。

有关更多信息，请参阅以下 MySQL 文档：

- MySQL 5.7 文档
- MySQL 8.0 文档

PostgreSQL

PostgreSQL Lightsail 中有 12、13、14、15 和 16 可供选择。PostgreSQL 是一个功能强大的开源对象关系数据库系统，经过30多年的积极开发，在可靠性、功能稳健性和性能方面赢得了良好的声誉。

可以找到大量描述如何安装和使用的信息 PostgreSQL 通过官方文档。这些区域有：PostgreSQL 社区提供了许多有用的场所，让您可以熟悉这项技术，了解其工作原理，并寻找职业机会。

> **Important**
>
> - 从 2024 年 6 月 30 日起，Lightsail 将不再支持 PostgreSQL 11，而且您将无法使用此蓝图创建新数据库。要了解如何升级数据库实例的主要版本，请参阅升级 Lightsail 数据库的主要版本。
> - 这些区域有：PostgreSQL 社区计划弃用 PostgreSQL 2024 年 11 月 14 日为 12，从该蓝图启动的 Lightsail 实例在此日期之后将不会收到安全补丁。因此，亚马逊 Lightsail 将终止对的标准支持 PostgreSQL 2025 年 2 月 28 日为 12。您将无法使用创建新的 Lightsail 数据库 PostgreSQL 2025 年 2 月 28 日当天或之后有 12 个。有关更多信息，请参阅 。PostgreSQL 网站。

有关更多信息，请参阅以下内容 PostgreSQL 文档：

- PostgreSQL 11 文档
- PostgreSQL 12 文档
- PostgreSQL 13 文档
- PostgreSQL 14 文档
- PostgreSQL 15 文档
- PostgreSQL 16 文档

优化数据导入

Lightsail 中提供了多种数据库计划，每种计划都有特定的内存、vCPU、存储空间和数据传输限额规格。由于每个数据库计划都有这些规范，因此为要导入新 Lightsail 数据库的数据量选择大小合适的数据库计划非常重要。如果您选择的计划低于大小要求，数据导入速度可能会减慢。使用以下准则，针对您的数据导入要求选择合适的数据库计划：

- 微型 15 USD/月数据库计划 – 如果传输的数据超过 10GB，则数据导入速度可能会减慢。
- 小型 30 USD/月数据库计划 – 如果传输的数据超过 20GB，则数据导入速度可能会减慢。
- 中型 60 USD/月数据库计划 – 如果传输的数据超过 85GB，则数据导入速度可能会减慢。
- 大型 115 USD/月数据库计划 – 如果传输的数据超过 156GB，则数据导入速度可能会减慢。

> **Note**
>
> 有关将数据导入数据库的更多信息，请参阅将数据导入 MySQL 数据库或将数据导入 PostgreSQL 数据库。

Lightsail 中的高可用性数据库

Lightsail 高可用性托管数据库提供故障转移支持，主数据库位于一个可用区，辅助备用数据库位于另一个可用区。如果生产工作负载存在大量使用问题并需要数据冗余，我们建议您使用高可用性数据库。如果是用于开发和测试，您可以使用不具有高可用性的标准数据库。

要创建高可用性数据库，请在创建托管数据库时选择 Lightsail 中提供的高可用性数据库计划之一。有关更多信息，请参阅创建数据库。您还可以将标准数据库更改为高可用性数据库。首先创建标准数据库的快照，再从该快照创建新数据库，然后选择高可用性计划。有关更多信息，请参阅从快照创建数据库。

创建具有高可用性的 Lightsail 数据库

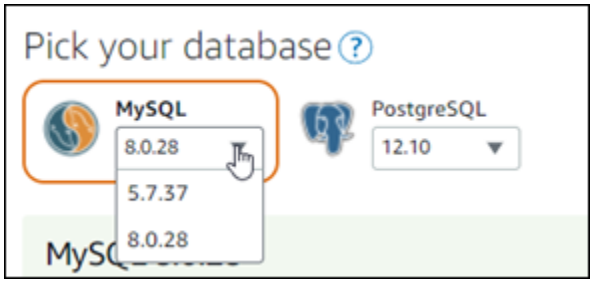
只需几分钟，即可在 Amazon Lightsail 中创建托管数据库。您可以在 MySQL 或 PostgreSQL 的最新主要版本之间进行选择，并使用标准或高可用性计划配置数据库。

> **Note**
>
> 有关 Lightsail 中托管数据库的更多信息，请参阅选择数据库。

创建数据库

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择创建数据库。
4. 为您的数据库选择 AWS 区域 和可用区。

   1. 选择更改 AWS 区域 和可用区，然后选择一个区域。
   2. 选择更改可用区，然后选择一个可用区。
5. 选择数据库类型。在其中一个可用的数据库引擎选项下，选择下拉菜单，然后选择 Lightsail 支持的最新主要数据库版本之一。



6. 如有必要，请选择以下选项之一：

   - Specify login credentials (指定登录凭证) – 指定自己的数据库用户名和密码。否则，Lightsail 会指定用户名，并为您创建一个强密码。
     - 要指定自己的用户名，请选择 Specify login credentials (指定登录凭证)，然后在文本框中输入您的用户名。根据您选择的数据库引擎，将具有以下约束条件：

       MySQL

       - MySQL 所需条件。
       - 必须为 1 到 16 个字母或数字。
       - 第一个字符必须是字母。
       - 不能是所选数据库引擎的保留字。有关 MySQL 中保留字的更多信息，请参阅 MySQL 5.6、MySQL 5.7 或 MySQL 8.0 的关键字和保留字文章。

       PostgreSQL

       - PostgreSQL 所需条件。
       - 必须为 1 到 63 个字母或数字。
       - 第一个字符必须是字母。

- 不能是所选数据库引擎的保留字。有关 PostgreSQL 中保留字的更多信息，请参阅 PostgreSQL 9.6、PostgreSQL 10、PostgreSQL 11 或 PostgreSQL 12 的 SQL 关键字文章。

- 要指定自己的密码，请清除 Create a strong password for me (为我创建强密码) 复选框，然后在文本框中输入您的密码。密码可以包含除“/”、“”“或“@”之外的任意可打印 ASCII 字符。对于 MySQL 数据库，密码可包含 8 到 41 个字符。对于 PostgreSQL 数据库，密码可包含 8 到 128 个字符。

- 指定主数据库名称-指定您自己的主数据库名称，或者 Lightsail 为您指定名称。要指定您自己的主数据库名称，请选择 Specify the master database name (指定主数据库名称)，然后在文本框中输入名称。根据您选择的数据库引擎，将具有以下约束条件：

  MySQL

  - 必须包含 1 到 64 个字母或数字。
  - 必须以字母开头。后续字符可以是字母、下划线或数字（0-9）。
  - 不能是所选数据库引擎的保留字。有关 MySQL 中保留字的更多信息，请参阅 MySQL 5.6、MySQL 5.7 或 MySQL 8.0 的关键字和保留字文章。

  PostgreSQL

  - 必须包含 1 到 63 个字母、数字或下划线。
  - 必须以字母开头。后续字符可以是字母、下划线或数字（0-9）。
  - 不能是所选数据库引擎的保留字。有关 PostgreSQL 中保留字的更多信息，请参阅 PostgreSQL 9.6、PostgreSQL 10、PostgreSQL 11 或 PostgreSQL 12 的 SQL 关键字文章。

7. 选择高可用性或标准数据库计划。

   利用高可用性计划创建的数据库在另一个可用区中具有主数据库和辅助备用数据库，以支持故障转移。有关更多信息，请参阅高可用性数据库。我们提供了定价不同的数据库服务包选项，每个选项都有不同级别的内存、处理能力、存储空间和传输速率。

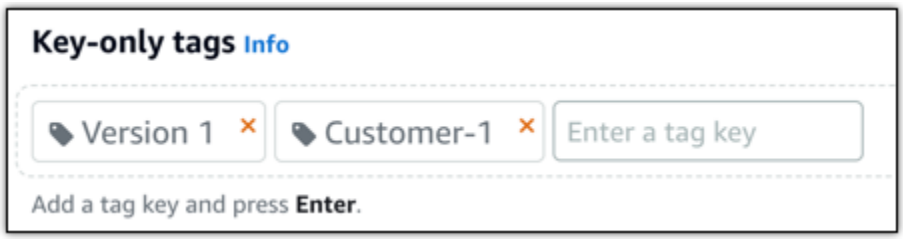
8. 输入数据库的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

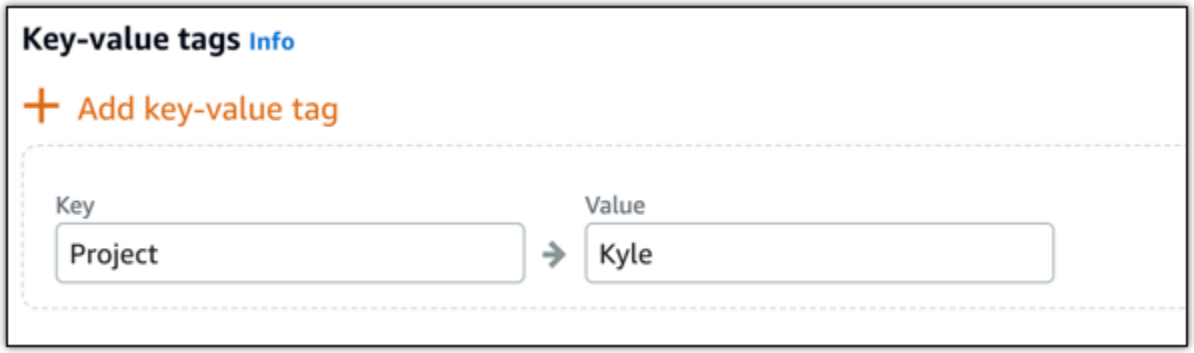
9. 选择以下选项之一，以将标签添加到数据库：

   - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

   - 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

     一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。

   > **Note**
   >
   > 有关“仅键”标签和键值标签的更多信息，请参阅标签。

10. 选择创建数据库。

    几分钟之内，你的 Lightsail 数据库就准备好了。您可以开始配置数据库以便执行数据导入，或者使用数据库客户端连接该数据库。

后续步骤

以下是一些指南，可帮助你在 Lightsail 启动并运行后在 Lightsail 中管理新数据库：

- 为您的数据库配置数据导入模式

- 在 Amazon Lightsail 中为您的数据库配置公共模式
- 管理数据库密码
- 连接到 MySQL 数据库
- 连接到 PostgreSQL 数据库
- 将数据导入 MySQL 数据库
- 将数据导入 PostgreSQL 数据库
- 创建数据库的快照

从客户端应用程序连接到你的 Lightsail MySQL 数据库

在 Amazon Lightsail 中创建 MySQL 托管数据库后，您可以使用任何标准的 MySQL 客户端应用程序或实用程序与之连接。您必须从 Lightsail 控制台的数据库管理页面获取数据库端点、端口、用户名和密码。您将在客户端或 Web 应用程序中配置数据库连接时指定这些值。

本指南向您介绍如何获取所需的连接信息，以及如何将 MySQL Workbench 配置为连接到托管式数据库。

> **Note**
>
> 有关连接到 PostgreSQL 数据库的更多信息，请参阅连接到 PostgreSQL 数据库。

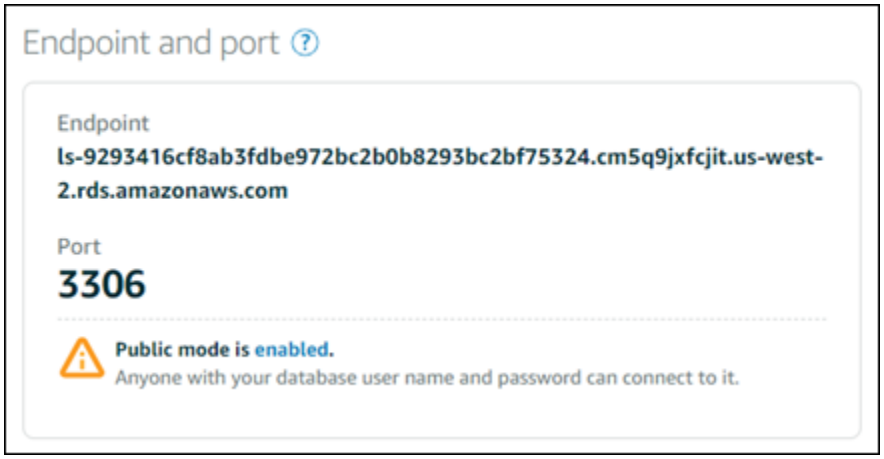
步骤 1：获取 MySQL 数据库连接详细信息

从 Lightsail 控制台获取您的数据库端点和端口信息。稍后在将客户端配置为连接到数据库时，您会用到这些信息。

获取数据库连接详细信息

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择要连接到的数据库的名称。
4. 在 Connect (连接) 选项卡的 Endpoint and port (终端节点和端口) 部分下，记下终端节点和端口信息。

我们建议您将终端节点复制到剪贴板，以避免输入错误的信息。要执行此操作，请突出显示该终端节点，然后按 Ctrl+C（如果使用的是 Windows）或 Cmd+C（如果使用的是 macOS），将其复制到剪贴板。然后，相应地按 Ctrl+V 或 Cmd+V 对其进行粘贴。



5. 在 Connect (连接) 选项卡的 User name and passwords (用户名和密码) 部分下方，记下用户名，然后选择 Password (密码) 部分下方的 Show (显示) 以查看当前的数据库密码。

   由于托管密码很复杂，我们还建议您复制并粘贴此密码，以避免输入错误的密码。突出显示该托管密码，然后按 Ctrl+C（如果使用的是 Windows）或 Cmd+C（如果使用的是 macOS），将其复制到剪贴板。然后，相应地按 Ctrl+V 或 Cmd+V 对其进行粘贴。

步骤 2：配置 MySQL 数据库的公有可用性

您必须启用公共模式，这样您的数据库才能从外部连接到该数据库，或者从与您的数据库 AWS 区域不同的 Lightsail 实例进行连接。启用公有模式后，拥有数据库用户名和密码的任何人都可以连接到数据库。要配置数据库的公有可用性，请按照为您的数据库配置公有模式指南中的步骤操作。

> **Note**
>
> 如果您计划从与您的数据库位于同一区域的其中一个 Lightsail 实例连接到数据库，请跳至步骤 3。

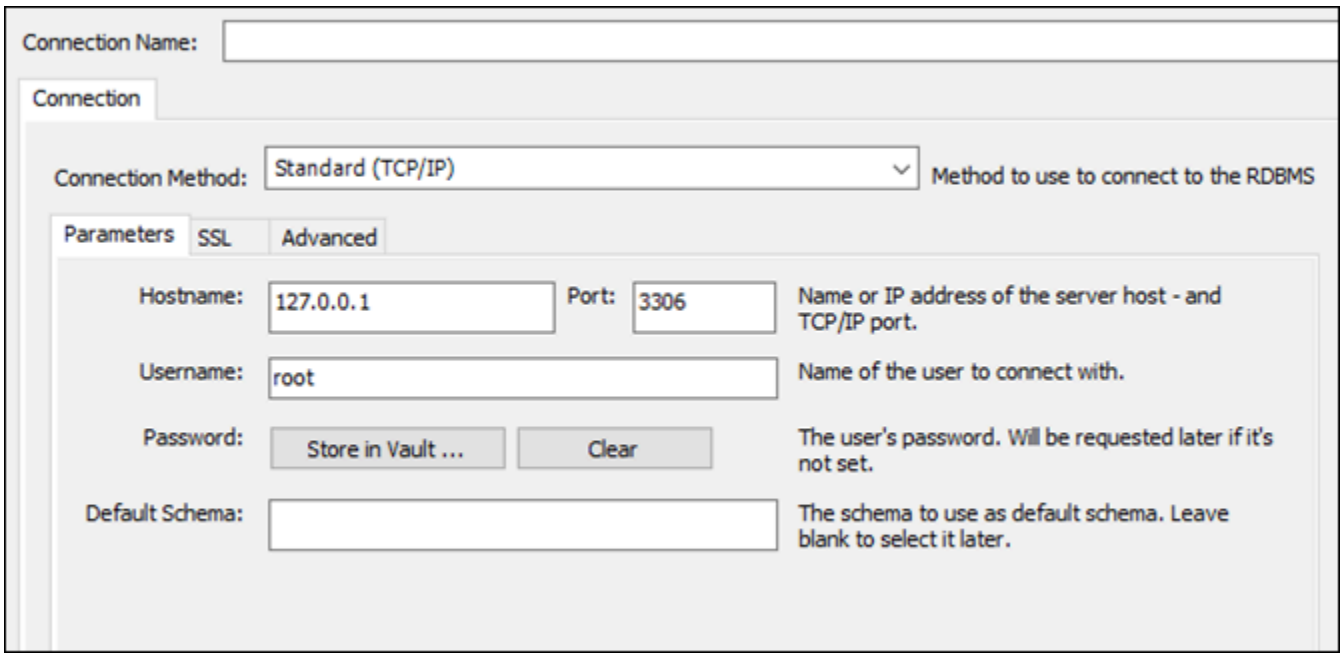
步骤 3：将数据库客户端配置为连接到 MySQL 数据库

要连接到 MySQL 数据库，可将数据库客户端配置为使用您先前获取的终端节点和端口。以下步骤向您演示如何配置 MySQL Workbench，但这些步骤可能与其他客户端的步骤类似。

> **Note**
>
> 有关如何使用 MySQL Workbench 的更多信息，请参阅 MySQL Workbench 手册。

将 MySQL Workbench 配置为连接到数据库

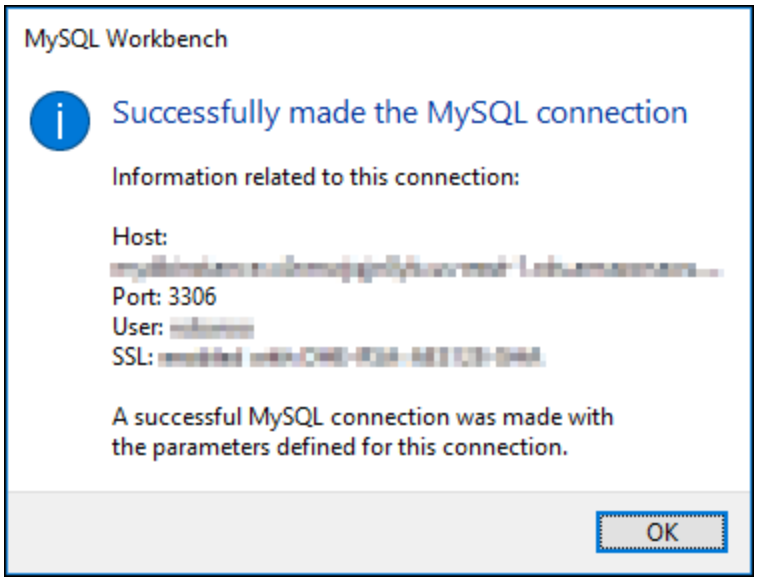
1. 打开 MySQL Workbench。
2. 选择 Database (数据库) 菜单，然后选择 Manage connections (管理连接)。
3. 将以下信息输入到显示的表格中：



- Connection Name – 我们建议您对连接使用与数据库类似的名称。这有助于您在以后识别它。
- Connection Method – 选择 Standard (TCP/IP)。
- Port – 输入先前获取的数据库的端口。MySQL 的默认端口是 3306。
- Hostname – 输入先前获取的数据库终端节点。如果你从 Lightsail 控制台复制了数据库端点，但它仍在剪贴板中，如果你使用的是 Windows，请按 Ctrl+V 进行粘贴，如果你使用的是 macOS，则按 Cmd+V 将其粘贴。
- Username – 输入先前获取的数据库用户名。
- Password – 选择 Store in Vault。在显示的窗口中，输入先前获取的数据库密码。如果你从 Lightsail 控制台复制了密码，但密码仍在剪贴板中，如果你使用的是 Windows，请按 Ctrl+V 进行粘贴，如果你使用的是 macOS，则按 Cmd+V 进行粘贴。选择 OK 以保存密码。
- Default Schema – 保留此文本框为空。

4. 选择 Test connection 以确定客户端是否可以与数据库建立连接。

   如果连接成功，系统会显示类似于以下示例的提示。读取此信息后，选择 OK 将其关闭。

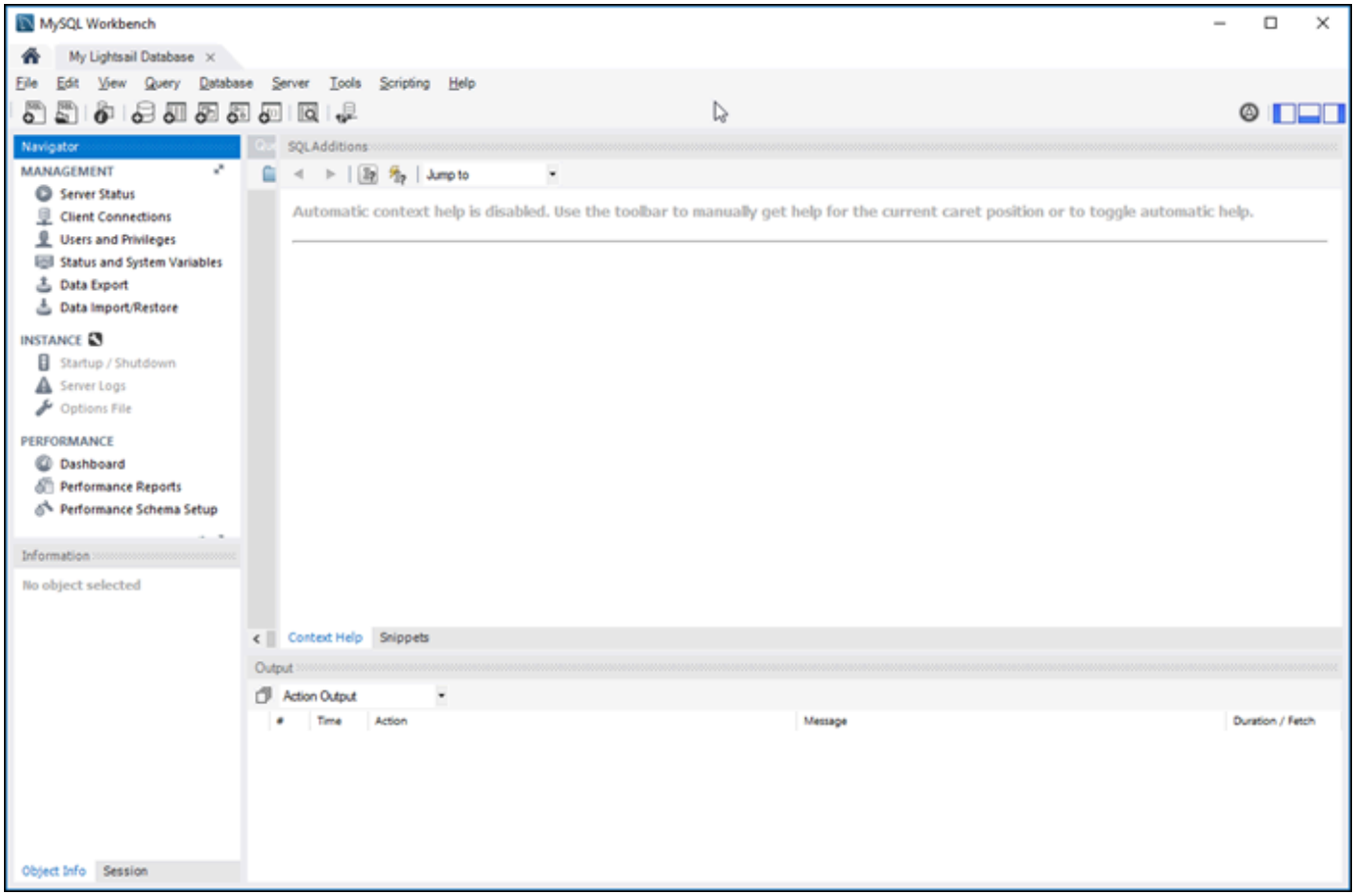


5. 选择 New 以保存新的连接详细信息，然后选择 Close 以关闭连接管理窗口。

   新数据库连接会显示在 MySQL Workbench 应用程序主页的“MySQL Connections”部分下方。

6. 要连接到数据库，请选择新数据库连接。

   如果连接成功，系统将显示类似于以下示例的窗口。



后续步骤

以下是帮助您在 Lightsail 中将数据导入数据库的指南：

- 将数据导入 MySQL 数据库

使用 SSL/TLS 安全地连接到 Lightsail MySQL 数据库

Amazon Lightsail 会创建 SSL 证书，并在预配置后将其安装在你的 MySQL 托管数据库上。证书由证书颁发机构 (CA) 签名，并且包括数据库终端节点作为 SSL 证书的公用名 (CN)，以防止欺骗攻击。

Lightsail 创建的 SSL 证书是可信的根实体，在大多数情况下应该可以使用，但如果您的应用程序不接受证书链，则可能会失败。如果您的应用程序不接受证书链，则您可能需要使用中间证书才能连接到您的 AWS 区域。

有关托管数据库的 CA 证书、受支持的 AWS 区域以及如何能够为应用程序下载中间证书的详细信息，请参阅为托管式数据库下载 SSL 证书。

支持的连接

MySQL 在以下版本中使用 yaSSL 进行安全连接：

- MySQL 5.7.19 和更早的 5.7 版本
- MySQL 5.6.37 和更早的 5.6 版本
- MySQL 5.5.57 和更早的 5.5 版本

MySQL 在以下版本中使用 OpenSSL 进行安全连接：

- MySQL 8.0 版
- MySQL 5.7.21 和更高的 5.7 版本
- MySQL 5.6.39 和更高的 5.6 版本
- MySQL 5.5.59 和更高的 5.5 版本

MySQL 托管数据库支持传输层安全性 (TLS) 版本 1.0、1.1 和 1.2。以下列表显示了各个 MySQL 版本的 TLS 支持情况：

- MySQL 8.0— TLS1 .0、TLS 1.1 和 TLS 1.2
- MySQL 5.7 — TLS1 .0 和 TLS 1.1。只有 MySQL 5.7.21 及更高版本支持 TLS 1.2。
- MySQL 5.6 — TLS1 .0
- MySQL 5.5— TLS1 .0

先决条件

- 将 MySQL 服务器安装到用于连接数据库的计算机上。有关详细信息，请参阅 MySQL 网站中的 MySQL 社群服务器下载。
- 为您的数据库下载相应的证书。有关信息，请参阅为托管式数据库下载 SSL 证书。

使用 SSL 连接到 MySQL 数据库

要使用 SSL 连接到 MySQL 数据库，请完成以下步骤。

1. 打开终端或命令提示符窗口。

2. 输入以下命令之一，具体取决于 MySQL 数据库的版本：

   - 输入以下命令以连接到 MySQL 5.7 或更高版本的数据库。

     ```
     mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY -u UserName -p
     ```

     在该命令中，将：

     - *DatabaseEndpoint*使用数据库的终端节点。
     - */path/to/certificate/rds-combined-ca-bundle.pem*使用您下载和保存数据库证书的本地路径。
     - *UserName*使用数据库的用户名。

     示例：

     ```
     mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY -u dbmasteruser -p
     ```

   - 输入以下命令以连接到 MySQL 6.7 或更早版本的数据库。

     ```
     mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-bundle.pem --ssl-verify-server-cert -u UserName -p
     ```

     在该命令中，将：

     - *DatabaseEndpoint*使用数据库的终端节点。
     - */path/to/certificate/rds-combined-ca-bundle.pem*使用您下载和保存数据库证书的本地路径。
     - *UserName*使用数据库的用户名。

     示例：

     ```
     mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem --ssl-verify-server-cert -u dbmasteruser -p
     ```

3. 出现提示时，键入您在上一个命令中指定的数据库用户的密码，然后按 Enter。

   您会看到类似于以下示例的结果：

```
[ec2-user@ip-172-26-5-44 ~]$ mysql -h ls-1c51a[redacted]829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws
.com --ssl-ca=/home/ec2-user/rds-ca-2015-root.pem --ssl-verify-server-cert -u dbmasteruser -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2727
Server version: 8.0.16 Source distribution

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

4. 键入 **`status`**，然后按 Enter 以查看您的连接状态。

   如果您看到 SSL 旁边的值为“正在使用的密码是”，则表示您的连接已加密。

```
mysql> status
--------------
mysql  Ver 14.14 Distrib 5.5.62, for Linux (x86_64) using readline 5.1

Connection id:          2727
Current database:
Current user:           dbmasteruser@172.26.5.44
SSL:                    Cipher in use is DHE-RSA-AES256-SHA
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server version:         8.0.16 Source distribution
Protocol version:       10
Connection:             ls-1c51a7beedc70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws.com via TCP/I
P
Server characterset:    utf8mb4
Db     characterset:    utf8mb4
Client characterset:    utf8
Conn.  characterset:    utf8
TCP port:               3306
Uptime:                 9 days 16 hours 24 min 33 sec

Threads: 3  Questions: 557480  Slow queries: 0  Opens: 242  Flush tables: 3  Open tables: 146  Queries per second avg:
 0.666
--------------
```

连接到你的 Lightsail PostgreSQL 数据库实例

在 Amazon Lightsail 中创建 PostgreSQL 托管数据库后，您可以使用任何标准的 PostgreSQL 客户端应用程序或实用程序与之连接。您必须从 Lightsail 控制台的数据库管理页面获取数据库端点、端口、用户名和密码。您将在客户端或 Web 应用程序中配置数据库连接时指定这些值。

本指南向您介绍如何获取所需的连接信息，以及如何将 pgAdmin 客户端配置为连接到托管式数据库。

> **Note**
>
> 有关连接到 MySQL 数据库的更多信息，请参阅连接到 MySQL 数据库。

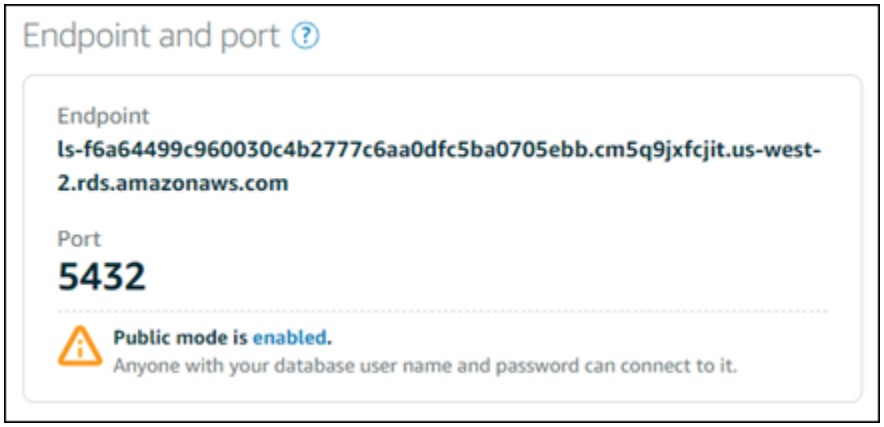
步骤 1：获取 PostgreSQL 数据库连接详细信息

从 Lightsail 控制台获取您的数据库端点和端口信息。稍后在将客户端配置为连接到数据库时，您会用到这些信息。

获取数据库连接详细信息

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择要连接到的数据库的名称。
4. 在 Connect (连接) 选项卡的 Endpoint and port (终端节点和端口) 部分下，记下终端节点和端口信息。

   我们建议您将终端节点复制到剪贴板，以避免输入错误的信息。要执行此操作，请突出显示该终端节点，然后按 Ctrl+C（如果使用的是 Windows）或 Cmd+C（如果使用的是 macOS），将其复制到剪贴板。然后，相应地按 Ctrl+V 或 Cmd+V 对其进行粘贴。

5. 在 Connect (连接) 选项卡的 User name and passwords (用户名和密码) 部分下方，记下用户名，然后选择 Password (密码) 部分下方的 Show (显示) 以查看当前的数据库密码。

   由于托管密码很复杂，我们还建议您复制并粘贴此密码，以避免输入错误的密码。突出显示该托管密码，然后按 Ctrl+C（如果使用的是 Windows）或 Cmd+C（如果使用的是 macOS），将其复制到剪贴板。然后，相应地按 Ctrl+V 或 Cmd+V 对其进行粘贴。

步骤 2：配置 PostgreSQL 数据库的公有可用性

您必须为数据库启用公共模式才能从外部连接到该数据库，或者从与数据库不同区域的 Lightsail 实例进行连接。启用公有模式后，拥有数据库用户名和密码的任何人都可以连接到数据库。要配置数据库的公有可用性，请按照为您的数据库配置公有模式指南中的步骤操作。

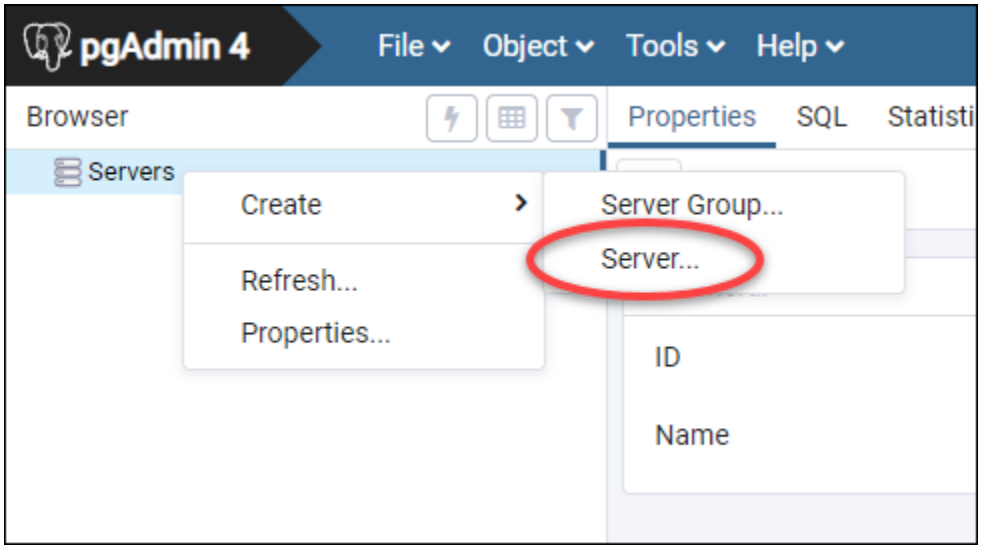
> **Note**
>
> 如果您计划从与数据库位于同一区域的 Lightsail 实例连接到数据库，请跳至步骤 3。

步骤 3：将数据库客户端配置为连接到 PostgreSQL 数据库

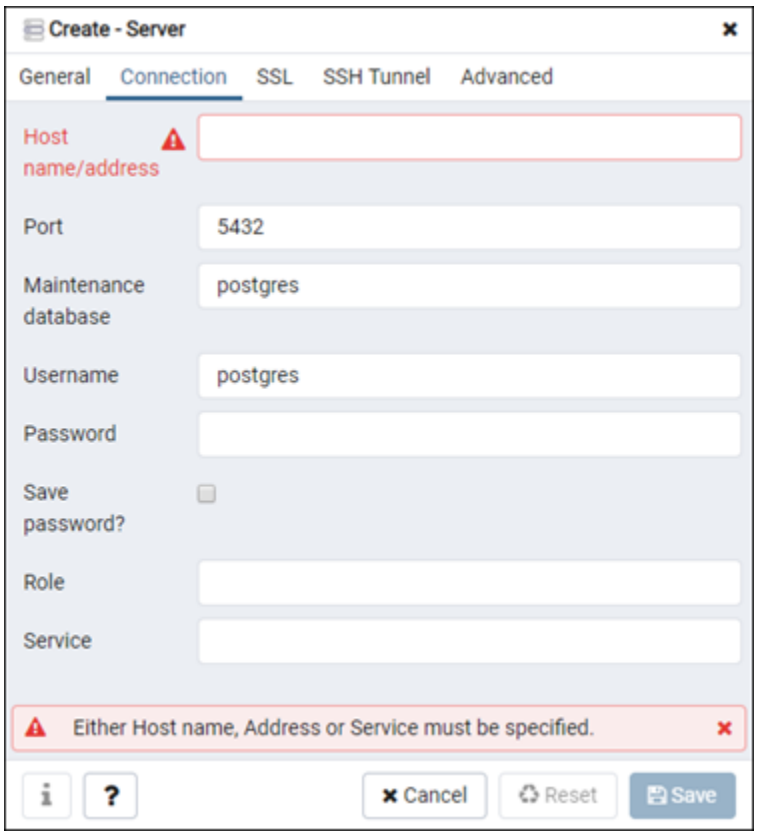
要连接到 PostgreSQL 数据库，可将数据库客户端配置为使用您先前获取的终端节点和端口。以下步骤向您演示如何配置 pgAdmin，但这些步骤可能与其他客户端的步骤类似。

> **Note**
>
> 有关使用 pgAdmin 的更多信息，请参阅 pgAdmin 文档。

将 pgAdmin 配置为连接到数据库

1. 打开 pgAdmin。
2. 从左侧导航菜单中，右键单击 Servers。
3. 选择 Create，然后选择 Server。
4. 

5. 在 Create - Server 表单中，输入服务器的名称。我们建议您对连接使用与数据库类似的名称。这有助于您在以后识别它。
6. 选择 Connection 选项卡，然后将以下信息输入到显示的表单中：



- Host name/address – 输入先前获取的数据库终端节点。如果你从 Lightsail 控制台复制了数据库端点，但它仍在剪贴板中，如果你使用的是 Windows，请按 Ctrl+V 进行粘贴，如果你使用的是 macOS，则按 Cmd+V 将其粘贴。
- Port – 输入先前获取的数据库的端口。PostgreSQL 的默认端口为 5432。
- Maintenance database – 指定客户端将连接到的初始数据库的名称。这是你在 Lightsail 中创建 PostgreSQL 数据库时指定的主数据库名称。

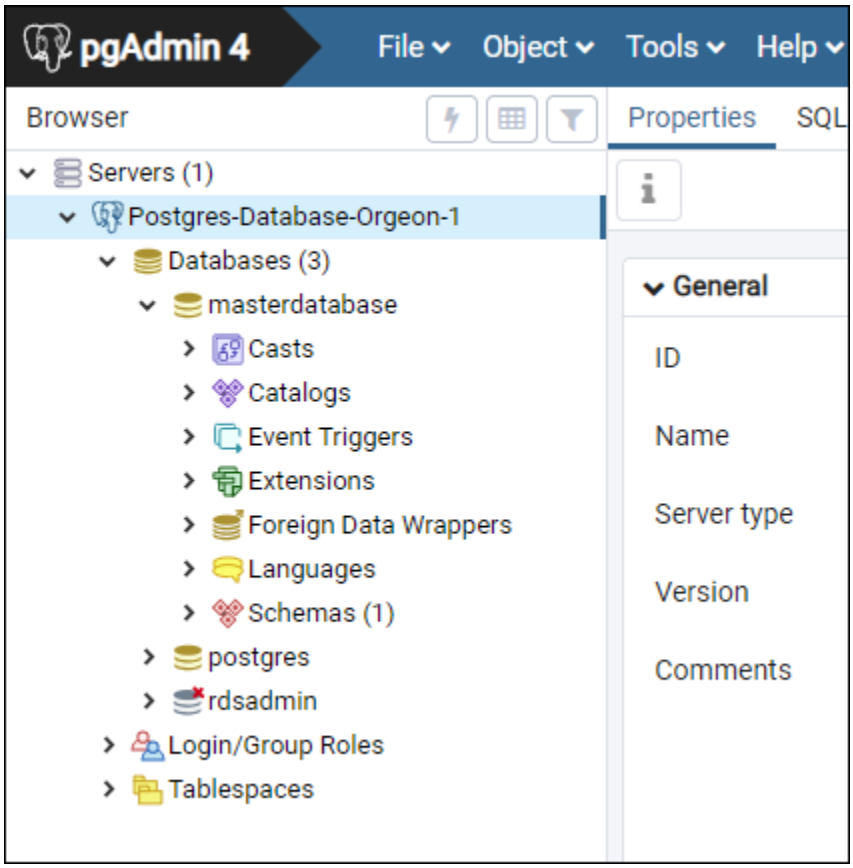
  如果您忘记了主数据库的名称，可输入 `postgres`。每个 PostgreSQL 托管数据库都有一个您可连接到的 `postgres` 数据库，之后，您将能够访问 PostgreSQL 托管数据库上的所有其他数据库。
- Username – 输入先前获取的数据库用户名。
- Password – 输入先前获取的数据库密码。如果你从 Lightsail 控制台复制了密码，但密码仍在剪贴板中，如果你使用的是 Windows，请按 Ctrl+V 进行粘贴，如果你使用的是 macOS，则按 Cmd+V 进行粘贴。选择 Save password 以保存您的密码。
- Role 和 Service – 将这些字段留空。

7. 选择 Save 以保存新服务器详细信息。

   您的新数据库连接将显示在 pgAdmin 应用程序的左侧导航菜单上的“Servers”部分下。

8. 要连接到您的数据库，请双击您的新数据库连接。

   如果连接成功，您将看到该数据库的可用资源列表。



后续步骤

以下是帮助您在 Lightsail 中将数据导入数据库的指南：

- 将数据导入 PostgreSQL 数据库

使用 SSL 安全地连接到 Lightsail PostgreSQL 数据库

Amazon Lightsail 会创建 SSL 证书，并在配置后将其安装到你的 PostgreSQL (Postgres) 托管数据库上。证书由证书颁发机构 (CA) 签名，并且包括数据库终端节点作为 SSL 证书的公用名 (CN)，以防止欺骗攻击。

由 Lightsail 创建的 SSL 证书是可信的根实体，在大多数情况下应该可以使用，但是如果您的应用程序不接受证书链，则可能会失败。如果您的应用程序不接受证书链，则您可能需要使用中间证书才能连接到您的 AWS 区域。

有关托管数据库的 CA 证书、受支持的 AWS 区域以及如何能够为应用程序下载中间证书的详细信息，请参阅为托管式数据库下载 SSL 证书。

先决条件

- 将 PostgreSQL 服务器安装到用于连接数据库的计算机上。有关详细信息，请参阅 Postgres 网站中的 PostgreSQL 下载
- 为您的数据库下载相应的证书。有关信息，请参阅为托管式数据库下载 SSL 证书。

使用 SSL 连接到您的 Postgres 数据库

要使用 SSL 连接到 Postgres 数据库，请完成以下步骤。

1. 打开终端或命令提示符窗口。
2. 输入以下命令以连接到 PostgreSQL 数据库。

```
psql -h DatabaseEndpoint -p 5432 "dbname=DatabaseName user=UserName sslrootcert=/
path/to/certificate/rds-combined-ca-bundle.pem sslmode=verify-full"
```

在该命令中，将：

- *DatabaseEndpoint*使用数据库的终端节点。
- *DatabaseName*使用您要连接的数据库的名称。
- *UserName*使用数据库的用户名。
- */path/to/certificate/rds-combined-ca-bundle.pem*使用您下载和保存数据库证书的本地路径。

示例：

```
psql -h ls-8e81e07f8b821917b11e1c6a0e26cb73c203.czowadgeezqi.us-
west-2.rds.amazonaws.com -p 5432 "dbname=dbmaster user=dbmasteruser sslrootcert=/
home/ec2-user/rds-combined-ca-bundle.pem sslmode=verify-full"
```

3. 出现提示时，键入您在上一个命令中指定的数据库用户的密码，然后按 Enter。

您应看到类似于以下示例的结果。如果您看到“SSL 连接”值，则表示您的连接已加密。



删除 Lightsail 数据库并创建最终快照

如果您不再需要 Amazon Lightsail 中的托管数据库，请将其删除。数据库在删除后将停止产生费用。

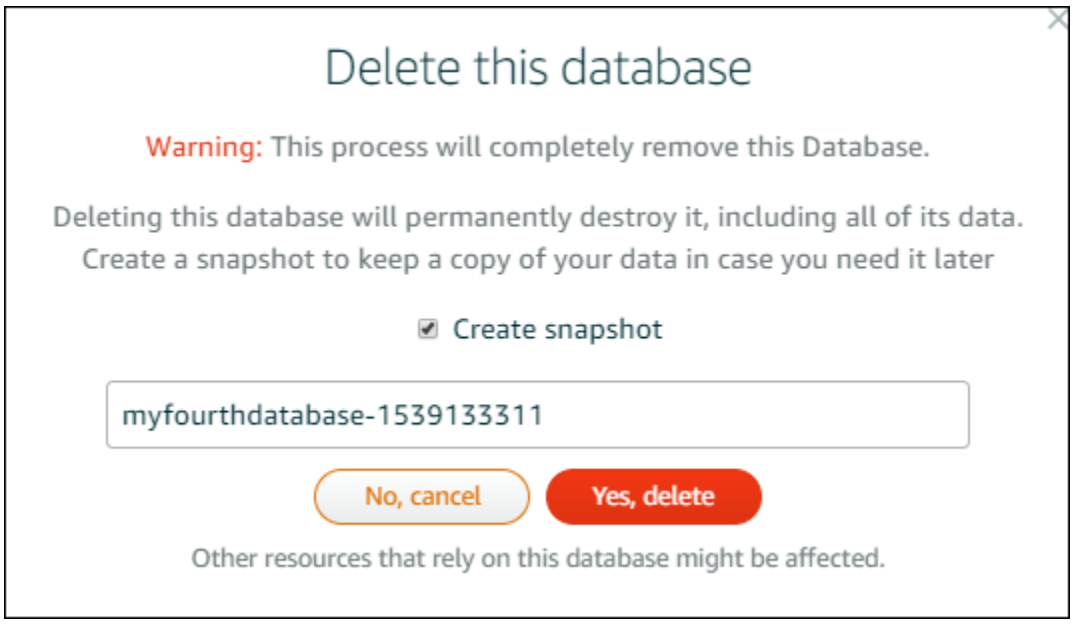
> **Note**
>
> 无法恢复已删除的数据库。您可以将创建数据库的最终快照作为本指南中介绍的步骤的一部分，也可以在删除过程之外单独创建快照。有关更多信息，请参阅创建数据库的快照。

删除数据库

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择要删除的数据库的名称。
4. 选择删除选项卡。
5. 在删除前创建快照旁边添加一个复选标记，以在删除数据库之前创建最终快照。然后，输入快照的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
6. 选择删除数据库。
7. 选择是，删除以确认删除。



如果您选择在删除之前创建快照，则可以在 Lightsail 主页的 “快照” 部分进行查看。

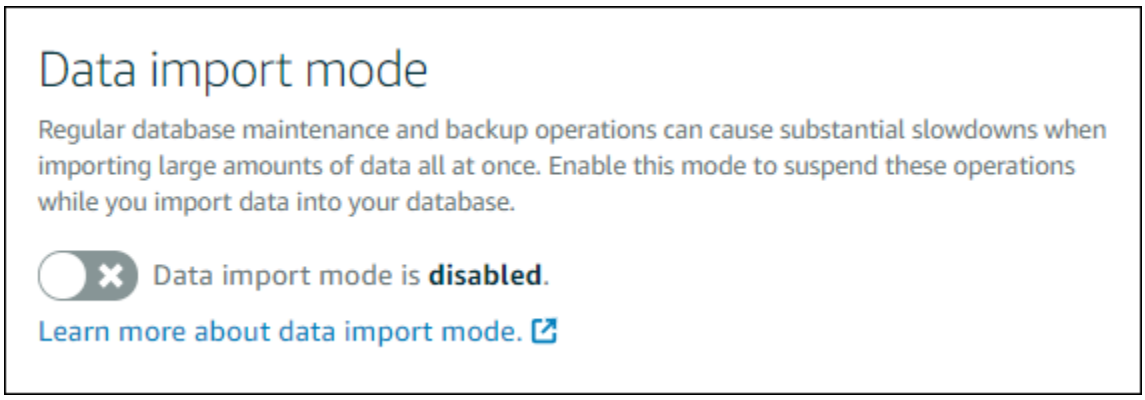
毫不延迟地将大型数据集导入您的 Lightsail 数据库

当一次性导入大量数据时，数据库常规备份操作可能会导致严重的延迟或运行速度大幅降低。启用您的 Amazon Lightsail 托管数据库的数据导入模式，以便在您导入大量数据时暂停这些操作。

> **Important**
>
> 启用数据导入模式后，会删除所有紧急还原备份。如果您希望在启用数据导入模式之前具有备份，可以创建数据库的快照。有关更多信息，请参阅创建数据库的快照。

为您的数据库配置数据导入模式

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择您要为其配置数据导入模式的数据库的名称。
4. 在连接选项卡中的数据导入模式部分下，使用切换按钮来启用数据导入模式。在导入完成后，同样使用切换按钮来关闭该模式。



现在，数据导入模式已启用，而数据库备份操作已暂停。我们建议您暂时启用数据导入模式。仅在您需要将大量数据导入到数据库时才使用该模式。导入完成后，禁用数据导入模式以恢复备份操作。

> **Note**
>
> 您的导入速度可能会降低，具体取决于要导入的数据量。有关更多信息，请参阅优化数据导入。

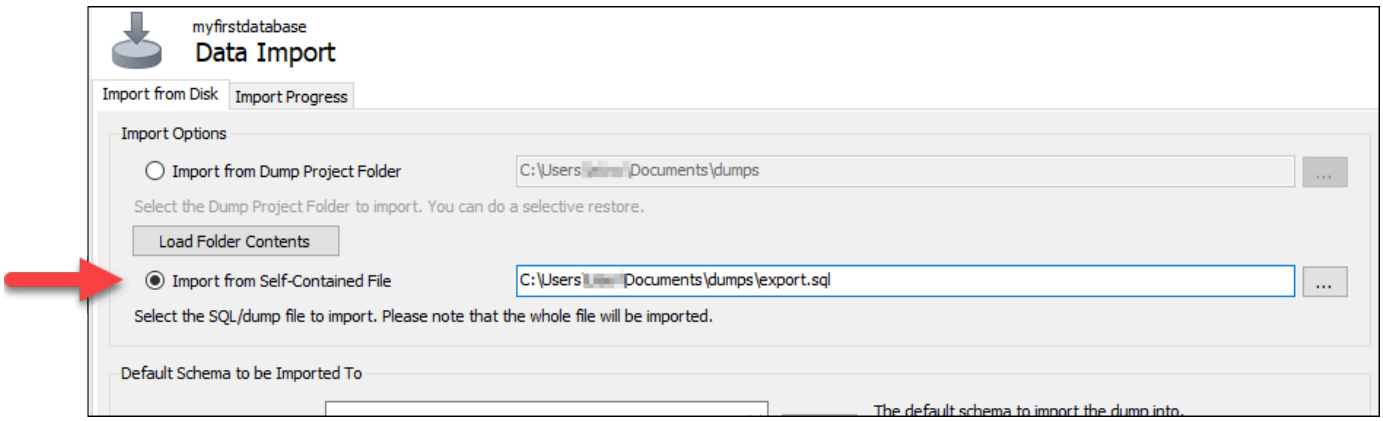
将 SQL 数据导入 Lightsail MySQL 数据库

你可以使用 MySQL Workbench 将 SQL 文件 (.SQL) 导入 Amazon Lightsail 中的 MySQL 托管数据库。

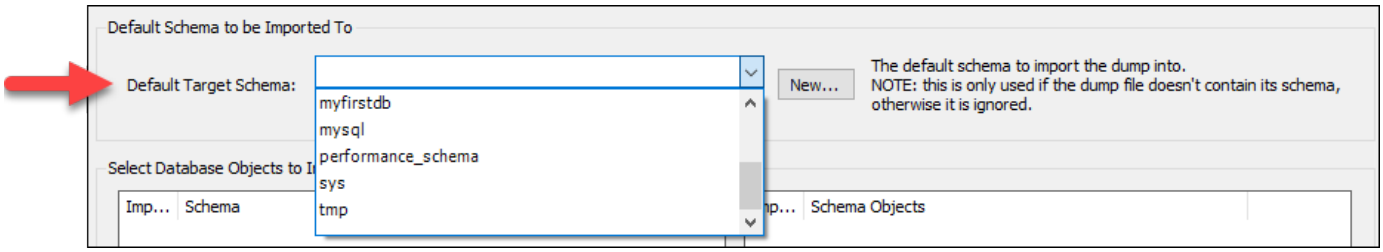
> **Note**
>
> 要了解如何将 MySQL Workbench 连接到您的数据库，请参阅连接到 MySQL 数据库。

将数据导入数据库

1. 打开 MySQL Workbench。
2. 在 MySQL 连接列表中，选择您的 MySQL 托管数据库。
3. 从左侧导航菜单中选择 Data Import/Restore。
4. 在“数据导入”窗格中，选择导入选项部分下方的从自包含文件导入。

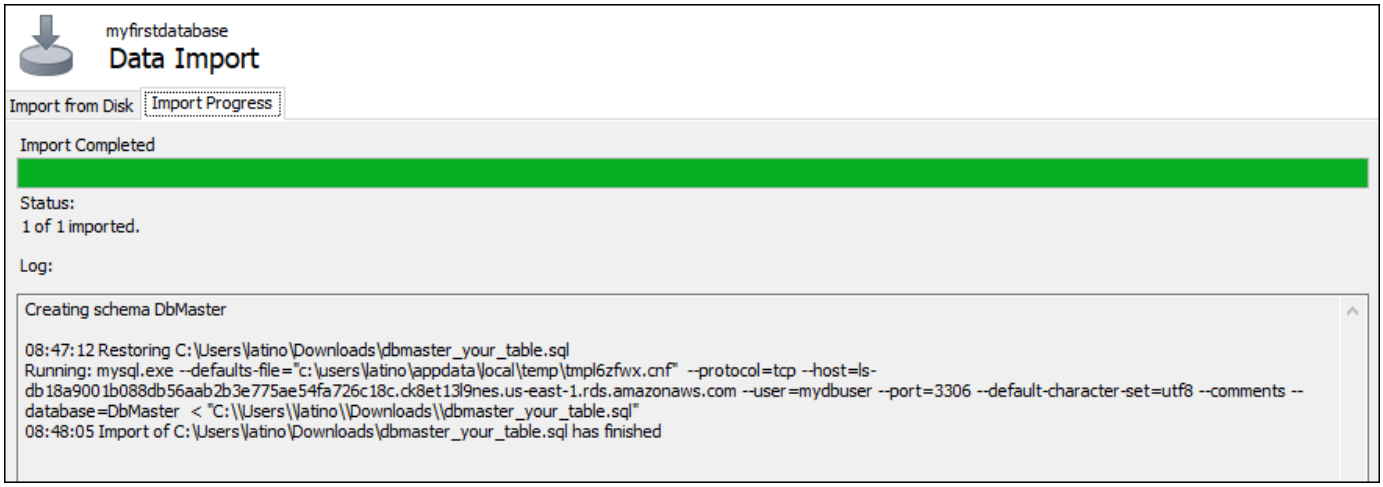


5. 选择省略号按钮，以在本地驱动器查找要导入的 .SQL 文件。
6. 选择要导入的 .SQL 文件，然后选择 Open。
7. 选择 Default Target Schema 下拉菜单，然后选择要向其导入文件的现有数据库。您还可以通过选择 New 来创建新数据库。



8. 选择 Start Import 以开始导入。

   导入过程可能需要几分钟或更长时间，具体取决于 .SQL 文件的大小。导入完成后，您应该会看到一条类似于以下内容的消息：



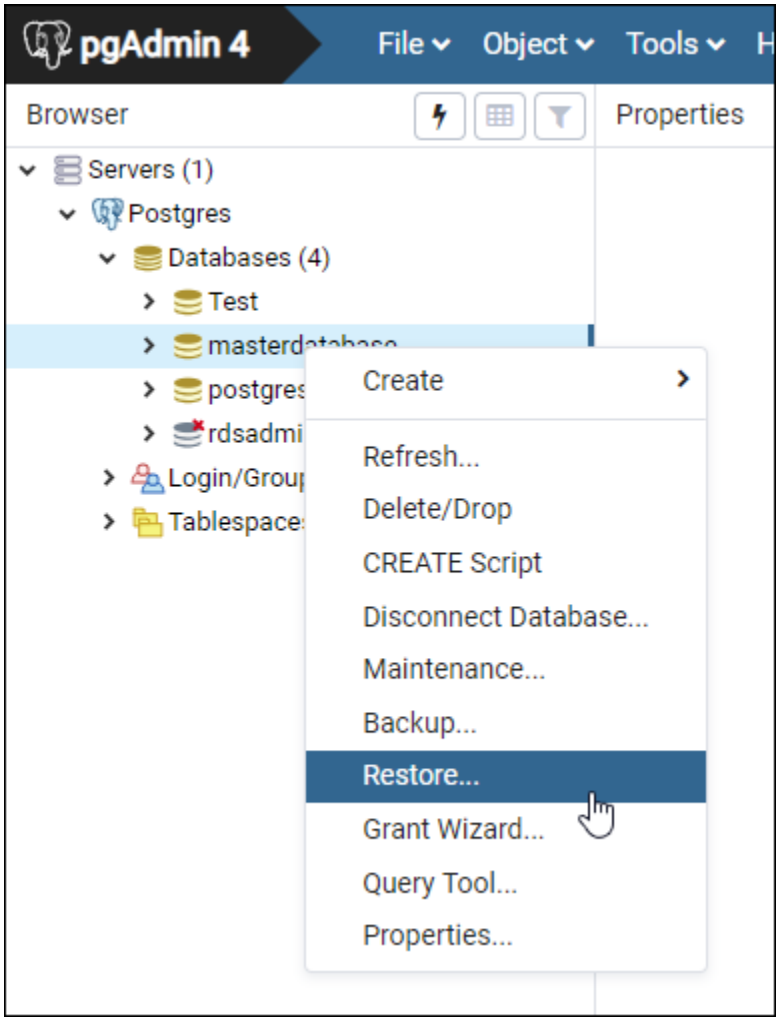
将 PostgreSQL 数据库备份导入 Lightsail 托管的数据库

你可以使用 pgadmin 将数据库备份文件导入到 Amazon Lightsail 中的 PostgreSQL 托管数据库中。

> **Note**
>
> 要了解如何将 pgAdmin 连接到您的数据库，请参阅连接到 PostgreSQL 数据库。有关创建可导入另一个数据库的 PostgreSQL 数据库备份的更多信息，请参阅 pgAdmin 文档中的备份对话框。

将备份文件导入数据库

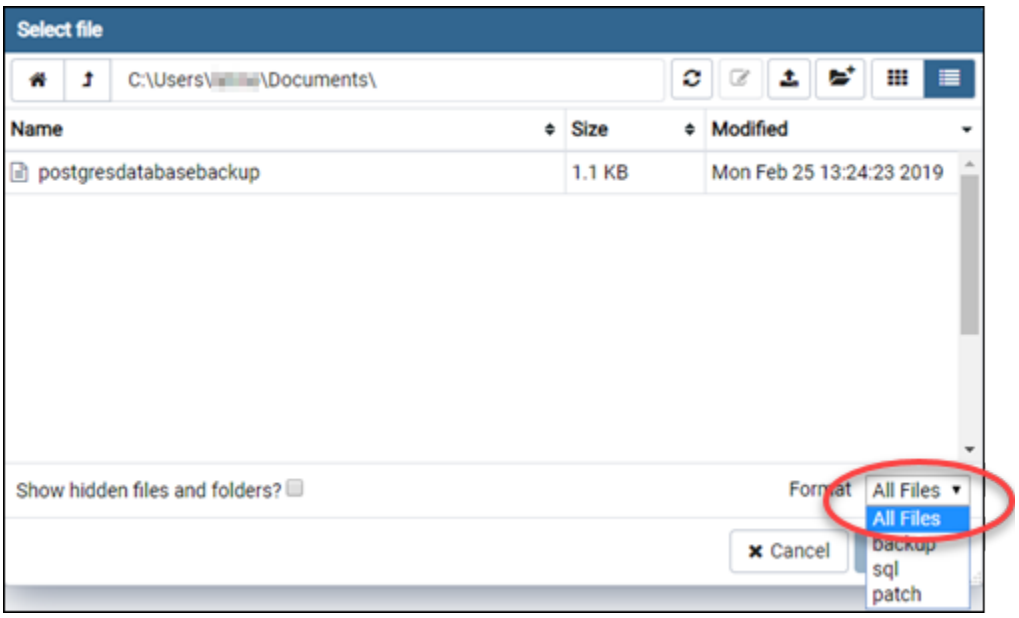
1. 打开 pgAdmin。
2. 在服务器连接列表中，双击 Amazon Lightsail 中你的 PostgreSQL 托管数据库进行连接。
3. 展开 Databases 节点
4. 右键单击要在其中导入数据库备份文件中的数据的数据库，然后选择 Restore。



5. 在 Restore 表单中，填写以下字段：

   - Format – 选择您的备份文件的格式。
   - Filename – 选择省略号图标，然后找到并选择本地驱动器上的数据库备份文件。突出显示该文件后，选择 Select 以返回到 Restore 提示。

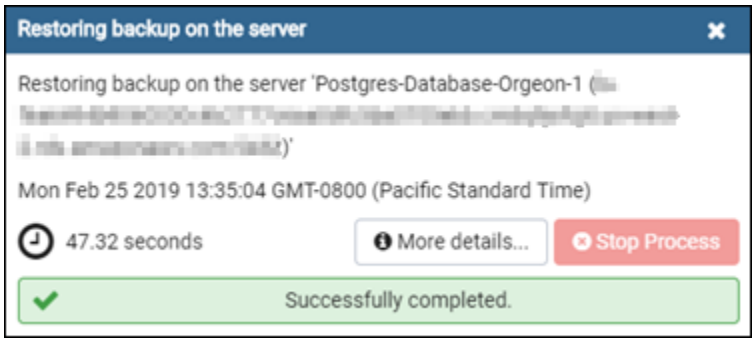
   > **Note**
   >
   > 选择 Format 下拉菜单，然后选择 All files 以查看本地驱动器上的所有文件格式。您的备份文件可能保存为与默认选择的文件类型 (sql) 不同的文件类型。



- Number of jobs 和 Role name – 将这些字段留空。

6. 选择 Restore 以启动导入。

   导入过程可能需要几分钟或更长时间，具体取决于数据库备份文件的大小。导入完成后，您应该会看到一条类似于以下内容的消息：



查看你的 Lightsail 数据库日志和历史记录

在 Amazon Lightsail 控制台中查看您的数据库日志和更改历史记录。数据库日志可提供有用的信息，有助于您诊断数据库存在的问题。同样，数据库历史记录将显示您对数据库所做的更改，使您可以将问题与最新的更改关联起来。

查看数据库日志

1. 登录 Lightsail 控制台。

2. 在左侧导航窗格中，选择数据库。
3. 选择要查看其日志的数据库的名称。
4. 选择 Logs and history (日志和历史记录) 选项卡。

   页面将显示数据库日志及数据库更改历史记录。
5. 选择一个数据库日志。有以下几种数据库日志可用：

   MySQL 数据库名称

   - 错误日志 – 对 mysqld 启动和关闭次数的记录。它还包含诊断消息，例如在服务器启动和关闭期间以及服务器运行期间发生的错误、警告和注释。有关更多信息，请参阅 MySQL 5.6、MySQL 5.7 或 MySQL 8.0 文档中有关错误日志的文章。
   - 常规日志 – 对 mysqld 所执行的操作的常规记录。当客户端连接或断开连接时，服务器会将信息写入此日志，并记录从客户端收到的每个 SQL 语句。有关更多信息，请参阅 MySQL 5.6、MySQL 5.7 或 MySQL 8.0 文档中有关常规查询日志的文章。
   - 慢速查询日志 – 对运行时间超过 long_query_time 秒且需要至少检查 min_examined_row_limit 行的 SQL 语句的记录。有关更多信息，请参阅 MySQL 5.6、MySQL 5.7 或 MySQL 8.0 文档中有关慢速查询日志的文章。

   > **Note**
   >
   > 默认情况下，对于 MySQL 数据库禁用一般日志和慢速查询日志。您可以通过更新几个数据库参数来启用这些日志并开始收集数据。有关更多信息，请参阅在 Amazon Lightsail 中启用 MySQL 数据库一般日志和慢速查询日志。

   PostgreSQL 数据库日志

   - Postgres 日志 – 对数据库启动和关闭次数的记录。它还可以包含数据库启动、关闭和运行期间发生的诊断，如错误、警告、通知和调试消息。有关更多信息，请参阅 PostgreSQL 9.6、PostgreSQL 10、PostgreSQL 11 或 PostgreSQL 12 文档中的错误报告和日志记录文章。

主题

- 使用 Lightsail 中的常规查询日志和慢速查询日志监控 MySQL 查询性能

使用 Lightsail 中的常规查询日志和慢速查询日志监控 MySQL 查询性能

默认情况下，Amazon Lightsail 中的 MySQL 数据库的常规和慢速查询日志处于禁用状态。您可以通过更新几个数据库参数来启用这些日志并开始收集数据。使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或更新数据库参数。 SDKs在本指南中，我们将向您展示如何使用更新数据库参数以及启用常规和慢速查询日志。 AWS CLI 此外，我们还提供了其他选项，用于控制一般查询日志和慢速查询日志以及如何处理日志数据保留。

先决条件

如果尚未安装并配置 AWS CLI，请执行该操作。有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface

在 Lightsail 控制台中启用常规和慢速查询日志

要在 Lightsail 控制台中启用常规查询日志和慢速查询日志，必须将`general_log`和`slow_query_log`数据库参数更新为的值`1`，将`log_output`参数更新为的值。`FILE`

在 Lightsail 控制台中启用常规和慢速查询日志

1. 打开终端或命令提示符窗口。
2. 输入以下命令以将 `general_log` 参数更新为值 `1`，即 true 或启用。

   ```
   aws lightsail update-relational-database-parameters --
   region Region --relational-database-name DatabaseName --parameters
    "parameterName=general_log,parameterValue=1,applyMethod=pending-reboot"
   ```

   在该命令中，将：

   - *DatabaseName*用你的数据库的名字。
   - *Region*用 AWS 区域 你的数据库的。
3. 输入以下命令以将 `slow_query_log` 参数更新为值 `1`，即 true 或启用。

   ```
   aws lightsail update-relational-database-parameters --
   region Region --relational-database-name DatabaseName --parameters
    "parameterName=slow_query_log,parameterValue=1,applyMethod=pending-reboot"
   ```

   在该命令中，将：

- *DatabaseName*用你的数据库的名字。
- *Region*用 AWS 区域 你的数据库的。

4. 输入以下命令将log_output参数更新为的值FILE，这会将日志数据写入系统文件并使其显示在 Lightsail 控制台中。

```
aws lightsail update-relational-database-parameters --
region Region --relational-database-name DatabaseName --parameters
 "parameterName=log_output,parameterValue=FILE,applyMethod=pending-reboot"
```

在该命令中，将：

- *DatabaseName*用你的数据库的名字。
- *Region*用 AWS 区域 你的数据库的。

5. 输入以下命令以重新引导数据库并使更改生效。

```
aws lightsail reboot-relational-database --region Region --relational-database-
name DatabaseName
```

在该命令中，将：

- *DatabaseName*用你的数据库的名字。
- *Region*用 AWS 区域 你的数据库的。

此时，您的数据库重启并变得不可用。等待几分钟，然后登录 Lightsail 控制台，查看数据库的常规和慢速查询日志。有关更多信息，请参阅在 Amazon Lightsail 中查看您的数据库日志和历史记录。

> **Note**
>
> 有关更新数据库参数的更多信息，请参阅在 Amazon Lightsail 中更新数据库参数。

控制其他数据库日志选项

要控制 MySQL 一般查询日志和慢速查询日志的其他选项，请更新以下参数：

- log_output — 将该参数设置为 TABLE。这会将一般查询写入 mysql.general_log 表，将慢速查询写入 mysql.slow_log 表。还可以将 log_output 参数设置为 NONE 以禁用日志记录。

  > **Note**
  >
  > 将log_output参数设置为TABLE会禁用常规和慢速查询日志数据在 Lightsail 控制台中显示。而是必须参考数据库上的 mysql.general_log 和 mysql.slow_log 以查看日志数据。

- long_query_time — 要防止在慢速查询日志中记录快速运行的查询，请指定需要记录的最短查询执行时间值，以秒为单位。默认值为 10 秒，最小值为 0。如果 log_output 参数设置为 FILE，则可以指定精确到微秒的浮点值。如果 log_output 参数设置为 TABLE，则必须指定精确到秒的整数值。系统只记录执行时间超过 long_query_time 参数值的查询。例如，将 long_query_time 设置为 0.1 可防止记录任何运行时间少于 100 毫秒的查询。
- log_queries_not_using_indexes — 要将所有不使用索引的查询记录到慢速查询日志，请设置为 1。默认值是 0。将记录不使用索引的查询，即使它们的执行时间小于 long_query_time 参数的值。

日志数据保留

启用了日志记录时，会定期轮换表日志或删除日志文件。这是一种预防措施，用于降低大型日志文件阻止数据库使用或影响性能的可能性。当 log_output 参数设置为 FILE 或 TABLE 时，按如下所示处理日志记录：

- 启用了 FILE 日志记录时，会每小时检查日志文件并删除 24 小时之前的日志文件。在一些情况下，删除之后的剩余日志文件的总体大小可能超过了数据库的分配空间的 2% 阈值。在这些情况下，将删除最大的日志文件，直到日志文件大小不再超过此阈值。
- 启用了 TABLE 日志记录时，在某些情况下，日志表每 24 小时轮换一次。

  如果表日志使用的空间大于分配存储空间的 20% 或所有日志的总体大小超过 10GB，则会执行此轮换。

  如果用于数据库的空间量大于数据库的分配存储空间的 90%，则减小日志轮换的阈值。

  随后，如果表日志使用的空间大于分配存储空间的 10% 或是所有日志的总体大小超过 5 GB，则轮换日志表。

  您可以订阅 low_free_storage 事件，在轮换日志表以释放空间时，会发送相关通知。

- 轮换日志表时，会将当前日志表复制到备份日志表，随后删除当前日志表中的条目。如果备份日志表已存在，则先将其删除，然后将当前日志表复制到备份。您可以查询备份日志表。mysql.general_log 表的备份日志表名为 mysql.general_log_backup。mysql.slow_log 表的备份日志表名为 mysql.slow_log_backup。
- 您可以通过调用 mysql.rds_rotate_general_logprocedure 来轮换 mysql.general_log 表。您可以通过调用 mysql.rds_rotate_slow_logprocedure 来轮换 mysql.slow_log 表。
- 表日志在数据库版本升级期间会进行轮换。

禁用 Lightsail 数据库的 point-in-time备份

使用以下步骤禁用 Lightsail 托管数据库的 point-in-time备份。

> **Important**
>
> 通过 point-in-time备份，如果数据库出现故障，您可以轻松恢复数据。我们建议您为 Lightsail 托管数据库启用时间点备份。

先决条件

使用 AWS Command Line Interface (AWS CLI) 或启用或 AWS CloudShell 禁用 Lightsail 数据库的 point-in-time备份。 CloudShell 是一款基于浏览器的预先认证外壳，您可以直接从 Lightsail 控制台启动它。有关更多信息，请参阅为 Lightsai AWS CLI I 操作设置和配置 和使用管理 Lightsail 资源 AWS CloudShell。

禁用数据库 point-in-time备份

要在 Lightsail 中禁用托管数据库的 point-in-time备份，必须使用的 Lightsail 命令update-relational-database更新数据库。 AWS CLI有关更多信息，请参阅 AWS CLI 命令参考update-relational-database中的。

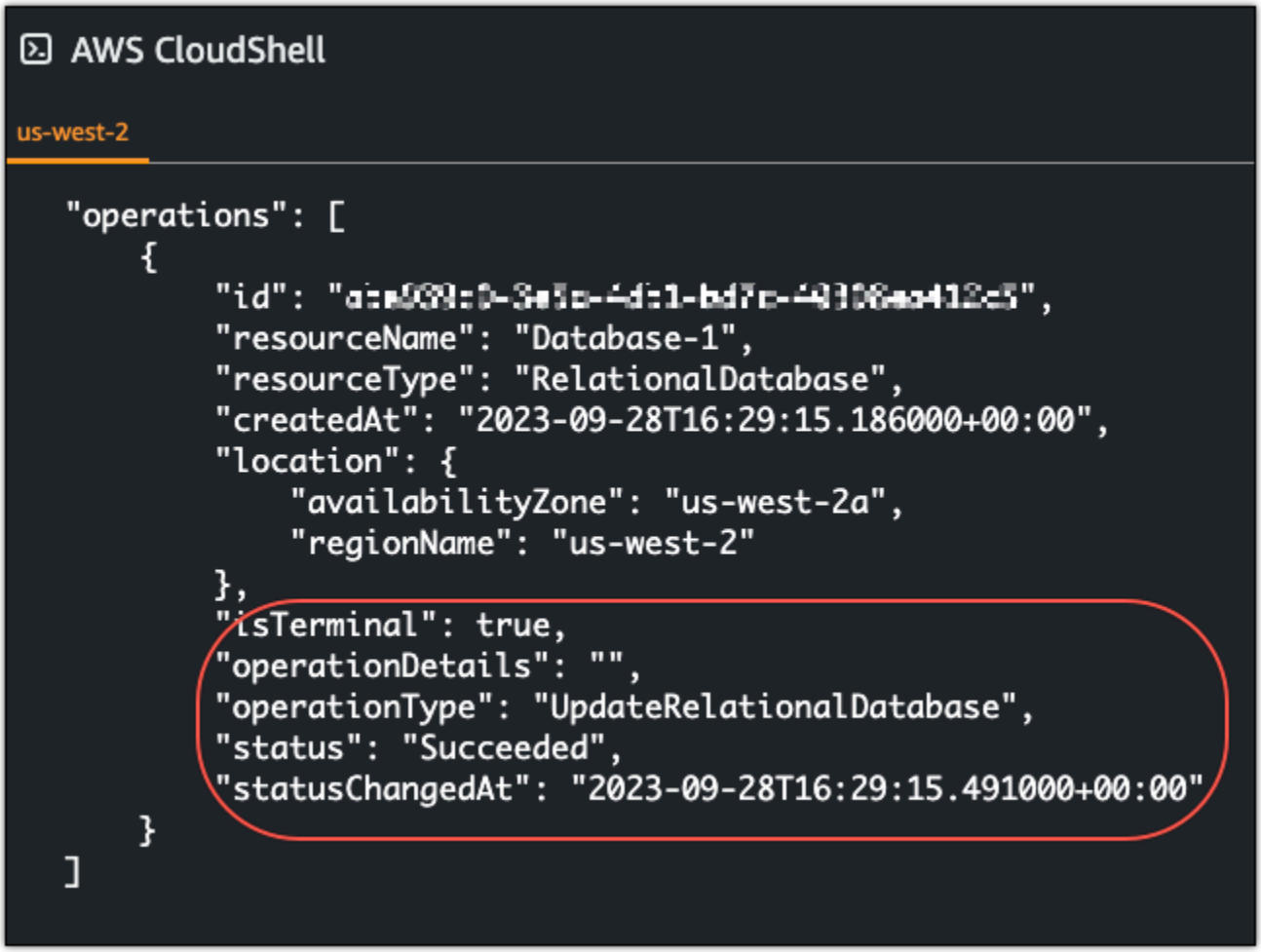
- 在终端、命令提示符或 CloudShell窗口中输入以下命令：

```
aws lightsail update-relational-database --region Region --relational-database-
name DatabaseName --disable-backup-retention --apply-immediately
```

命令中的`--disable-backup-retention`值会关闭指定数据库的 point-in-time备份。在该命令中，将：

- *DatabaseName*用你的数据库的名字。
- *Region*用 AWS 区域 你的数据库的。

您应该会看到状态为 Succeeded 的操作响应。更新期间，数据库的状态将在短时间内更改为正在修改。当数据库的状态变回“可用”时， point-in-time还原选项将被禁用，如以下示例所示。



> **Note**
>
> 要启用 point-in-time备份，请运行前面列出的相同命令，但改为使用`--enable-backup-retention`参数。

使用快照备份你的 Lightsail 数据库

您可以在 Amazon Lightsail 中创建托管数据库的快照。快照是数据库的副本，如果出现错误，您可以使用它来还原数据库。您还可以使用快照来创建使用不同计划（例如，高可用性或标准计划）的新数据库。

当您创建标准数据库的快照时，数据库将在几秒到几分钟内变得不可用，具体取决于数据库的大小。高可用性数据库不受快照操作的影响，因为快照是使用备用数据库创建的。

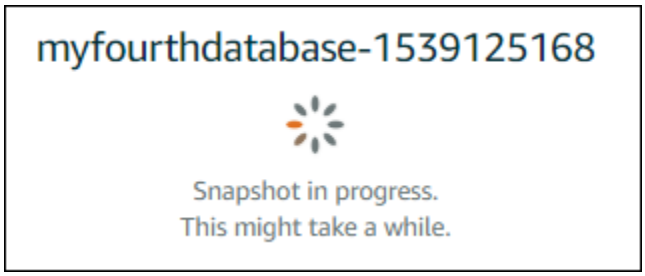
创建数据库的快照

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择要为其创建快照的数据库的名称。
4. 选择 Snapshots & restore（快照和还原）选项卡。
5. 在页面的 Manual snapshots（手动快照）部分中，选择 Create snapshot（创建快照），然后输入您快照的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
6. 选择 Create（创建）。

   快照创建过程开始，此时会显示一个 Snapshot in progress（快照拍摄正在进行中）状态。



   快照创建过程完成后，新快照将在 Recent snapshots（近期快照）部分下列出。您也可以在 Lightsail 主页的 “快照” 选项卡下查看您账户的所有快照。



后续步骤

快照准备就绪后，您可以从该快照创建一个新数据库，新数据库是原始数据库的副本。有关更多信息，请参阅根据快照创建数据库。

主题

- 在 Lightsail 中从 point-in-time备份中恢复数据库
- 在 Lightsail 中使用快照创建托管数据库

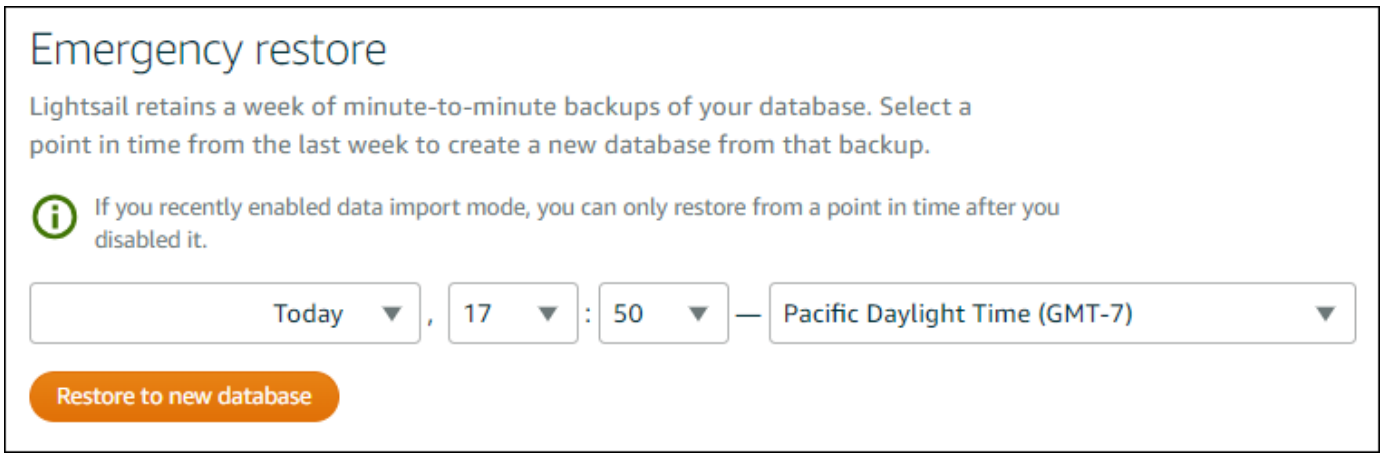
在 Lightsail 中从 point-in-time备份中恢复数据库

您可以在 Amazon Lightsail 中使用 point-in-time备份来创建新的托管数据库。 Point-in-time数据库的备份以 5 分钟为增量提供，并且是针对前 7 天的备份。这样，您能够将出现故障的数据库还原到过去一周中的特定日期和时间。

您还可以从快照创建新数据库。有关更多信息，请参阅在 Amazon Lightsail 中根据快照创建数据库。

使用 point-in-time备份创建数据库

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择要为其更改计划的数据库的名称。
4. 选择 Snapshots & restore (快照和还原) 选项卡。
5. 在 Emergency restore (紧急还原) 部分下方，选择要用于新数据库的备份的日期和时间。



6. 选择 Restore to new database (还原到新数据库)。
7. 在 Create a new database (创建新数据库) 页面上，选择 Change zone (更改可用区) 以选择不同的可用区。然后，系统会在与您先前所选快照相同的亚马逊云科技区域中创建新数据库。
8. 选择新数据库计划。

   选择高可用性或标准数据库计划。利用高可用性计划创建的数据库在另一个可用区中具有主数据库和辅助备用数据库，以支持故障转移。有关更多信息，请参阅高可用性数据库。

   > **Note**
   >
   > 您无法选择比原始数据库计划小的数据库计划。

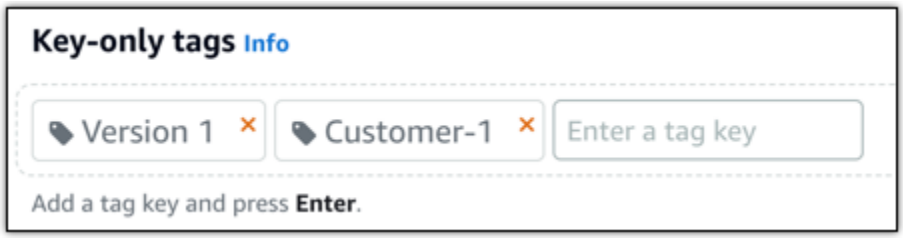
9. 输入数据库的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

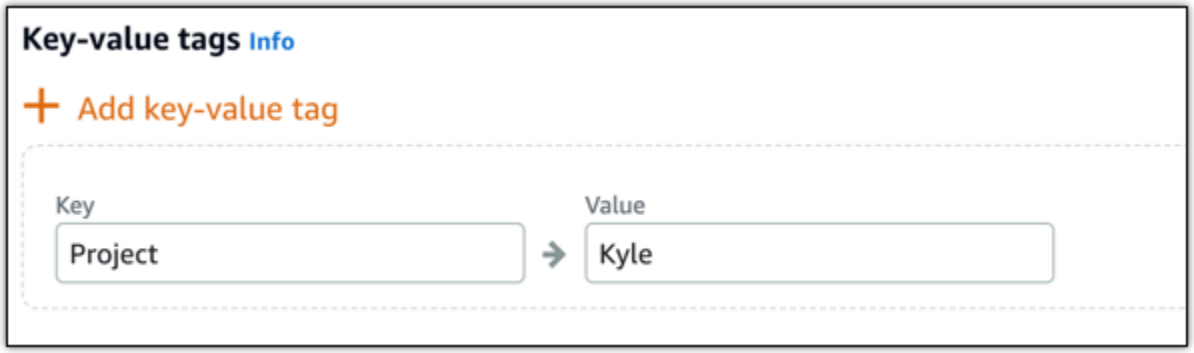
10. 选择以下选项之一，以将标签添加到数据库：

    - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。



- 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

  一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。



> **Note**
>
> 有关“仅键”标签和键值标签的更多信息，请参阅标签。

11. 选择创建数据库。

    几分钟之内，您的新 Lightsail 数据库就可以使用新的数据库计划或捆绑包了。

后续步骤

在新数据库已启用且运行正常后，完成以下操作：

- 如果不再需要原始数据库，则将其删除。有关更多信息，请参阅删除您的数据库。
- 通过 point-in-time备份创建的数据库配置为使用由 Lightsail 创建的强密码。有关更多信息，请参阅管理数据库密码。

在 Lightsail 中使用快照创建托管数据库

如果您的原始数据库出现问题，则可以从 Amazon Lightsail 中的快照创建新的托管数据库。您还可以将数据库更改为不同的计划，例如，高可用性或标准计划。您也可以使用原始数据库的 point-in-time备份创建新数据库。有关更多信息，请参阅在 Amazon Lightsai point-in-time l 中使用备份创建数据库。

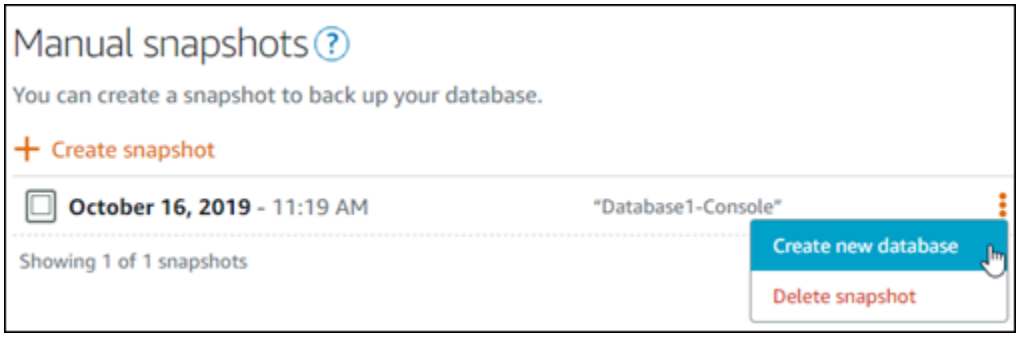
创建重复的数据库时，可以选择与原始数据库不同或更大的计划。但是，您不能选择比原始数据库小的计划。

> **Note**
>
> 利用高可用性计划创建的数据库在另一个可用区中具有主数据库和辅助备用数据库，以支持故障转移。有关更多信息，请参阅高可用性数据库。

从快照创建数据库

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 通过从快照创建新数据库，选择要复制的数据库的名称。
4. 选择 Snapshots & restore（快照和还原）选项卡。
5. 在页面的 Manual snapshots (手动快照) 部分中，选择要从中创建新数据库的快照旁边的操作菜单图标 (⋮)，然后选择 Create new database (创建新数据库)。

> **Note**
>
> 您需要一个要从中进行操作的数据库快照。如果尚未创建快照，请参阅创建数据库的快照。



6. 选择 Create new database (创建新数据库)。
7. 在 Create a new database (创建新数据库) 页面上，选择 Change zone (更改可用区) 以选择不同的可用区。此时，系统会在与您先前所选快照相同的亚马逊云科技区域中创建新数据库。
8. 选择新数据库计划。

   选择高可用性或标准数据库计划。利用高可用性计划创建的数据库在另一个可用区中具有主数据库和辅助备用数据库，以支持故障转移。有关更多信息，请参阅高可用性数据库。

   > **Note**
   >
   > 您无法选择比原始数据库（用于创建快照）计划小的数据库计划。

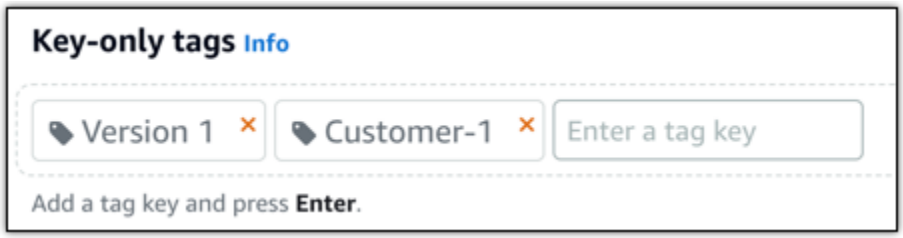
9. 输入数据库的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

10. 选择以下选项之一，以将标签添加到数据库：

    - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

    - 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

      一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。



> **Note**
>
> 有关“仅键”标签和键值标签的更多信息，请参阅标签。

11. 选择创建数据库。

    几分钟之内，您的新 Lightsail 数据库就可以使用新的数据库计划或捆绑包了。

后续步骤

在新数据库已启用且运行正常后，完成以下操作：

- 如果要通过创建新数据库来替换现有数据库，并且有应用程序依赖于此现有数据库，请务必将应用程序依赖关系更新到新数据库。
- 如果不再需要原始数据库，则将其删除。有关更多信息，请参阅删除您的数据库。
- 根据快照创建的数据库配置为使用由 Lightsail 创建的强密码。有关更多信息，请参阅管理数据库密码。

下载 SSL/TLS 证书，确保应用程序与 Lightsail 数据库的安全连接

您可以使用应用程序中的安全套接字层 (SSL) 或传输层安全 (TLS) 来加密与运行 MySQL 或 PostgreSQL 的 Amazon Lightsail 中托管数据库的连接。每个数据库引擎都有自己的用于实施 SSL/TLS 的过程。有关更多信息，请参阅使用 SSL 连接到 MySQL 数据库，或使用 SSL 连接到 PostgreSQL 数据库。

> **Note**
>
> 可供下载的证书标有亚马逊关系数据库服务（Amazon RDS）的标签，但也适用于Lightsail中的托管数据库。

所有 AWS 区域 s 的证书捆绑包

要获取包含所有 AWS 区域中间证书和根证书的证书包，或者如果您的应用程序在 Microsoft Windows 上并且需要 PKCS7 文件，请查看 Amazon Relational Database AWS 区域 Service 用户指南中的所有证书捆绑包。

此根证书是受信任的根实体，并且应适用于大多数情况。但是，如果您的应用程序不接受证书链，则其可能失败。如果您的应用程序不接受证书链，请继续本文档的下一部分。

特定 AWS 区域的证书捆绑包

要获取包含特定证书的中间证书和根证书的证书包，请参阅 Amazon Relational Database AWS 区域 Service 用户指南中针对特定证书的证书捆绑包。 AWS 区域

更新 Lightsail 数据库的 CA 证书版本

Amazon Lightsail 发布了新的证书颁发机构 (CA) 证书，用于使用 SSL/TLS 连接到您的托管数据库。本指南描述如何升级到新的 CA 证书。您只能使用以下方法升级证书 update-relational-databaseAPI 操作。新证书称为 `rds-ca-rsa2048-g1`、`rds-ca-rsa4096-g1` 和 `rds-ca-ecc384-g1`。旧证书称为 `rds-ca-2019`。我们提供 CA 证书作为 AWS 安全最佳实践。有关托管数据库的 CA 证书和受支持的 AWS 区域的信息，请参阅为托管数据库下载 SSL 证书。

旧的 CA 证书（`rds-ca-2019`）将于 2024 年 8 月 22 日到期。因此，我们强烈建议您尽快完成本指南中的步骤，修改您的托管式数据库以使用新证书。如果您的应用程序在 2024 年 8 月 22 日SSL/TLS, no action is required. If these steps are not completed, your applications will fail to connect to your managed database using SSL/TLS之后未使用连接到 Lightsail 托管数据库。

默认情况下，在 2024 年 1 月 26 日之后创建的新托管数据库将使用 `rds-ca-rsa2048-g1` 证书。如果您希望临时修改新的托管数据库以使用旧证书（`rds-ca-2019`），可以使用 AWS Command Line Interface（AWS CLI）进行修改。在 2024 年 1 月 26 日之前创建的任何托管数据库都会使用这些 `rds-ca-2019` 证书，直到您将它们更新为 `rds-ca-rsa2048-g1`、`rds-ca-rsa4096-g1` 和 `rds-ca-ecc384-g1` 证书。

> **Note**
>
> 在生产环境中使用本指南中的步骤之前，请先在开发或测试环境中进行测试。

先决条件

- 更新数据库客户端应用程序以使用新的 SSL/TLS 证书，再完成此过程中的步骤。

  更新应用程序以获取新SSL/TLS certificates depend on your specific applications. Work with your application developers to update the SSL/TLS certificates for your applications. To learn more about updating applications for new SSL/TLS证书的方法，请参阅 Amazon Relati onal Database Service 用户指南中的更新应用程序以使用新的 SSL/TLS 证书连接到 MySQL 数据库实例或更新应用程序以使用新 SSL/TLS 证书连接到 PostgreSQL 数据库实例。
- 在本指南中，您将使用 AWS CloudShell 来执行升级。 CloudShell 是一款基于浏览器的预先认证外壳，您可以直接从 Lightsail 控制台启动它。使用 CloudShell，您可以使用首选外壳运行 AWS Command Line Interface (AWS CLI) 命令，例如 Bash PowerShell、或 Z shell。您无需下载或安装命令行工具，即可完成此操作。有关如何设置和使用的 CloudShell更多信息，请参阅 Lightsai AWS CloudShell l 中的。

识别托管数据库的有效 CA 证书

完成以下步骤以识别您的 Lightsail 数据库实例的有效 CA 证书。

1. 打开终端、AWS CloudShell 或命令提示符窗口。
2. 输入以下命令以识别托管数据库的有效 CA 证书。

   ```
   aws lightsail get-relational-database --relational-database-name DatabaseName --
   region DatabaseRegion | grep "caCertificateIdentifier"
   ```

   在命令中，*DatabaseName*替换为要修改的数据库的*DatabaseRegion*名称以及数据库实例所在 AWS 区域 的名称。

   示例

   ```
   aws lightsail get-relational-database --relational-database-name Database-1 --
   region us-east-1 | grep "caCertificateIdentifier"
   ```

该命令将返回您数据库的有效 CA 证书的 ID。

示例

```
"caCertificateIdentifier": "rds-ca-rsa2048-g1"
```

修改托管式数据库以使用新 CA 证书

完成以下步骤，在 Lightsail 中修改您的托管数据库，使其使用其中一个新的 CA 证书（`rds-ca-rsa2048-g1`、`rds-ca-rsa4096-g1`和`rds-ca-ecc384-g1`）。

> **Important**
>
> 在更新数据库上的 CA 证书之前，请先更新使用 CA 证书的所有客户端应用程序。

1. 打开终端、AWS CloudShell 或命令提示符窗口。
2. 输入以下命令以在托管数据库上使用新证书。

```
aws lightsail update-relational-database --relational-database-name DatabaseName --region DatabaseRegion --ca-certificate-identifier rds-ca-rsa2048-g1
```

在命令中，*DatabaseName*替换为要修改的数据库的*DatabaseRegion*名称以及数据库实例所在 AWS 区域 的名称。

示例

```
aws lightsail update-relational-database --relational-database-name Database-1 --region us-east-1 --ca-certificate-identifier rds-ca-rsa2048-g1
```

托管数据库使用的 CA 证书将在数据库的下一个维护时段内更新，或者如果您在命令末尾添加 `--apply-immediately` 参数，则会立即更新。

修改托管式数据库以使用旧 CA 证书

完成以下步骤，在 Lightsail 中修改您的托管数据库，使其使用旧的 CA 证书 () `rds-ca-2019`。仅在使用新证书（`rds-ca-rsa2048-g1`、`rds-ca-rsa4096-g1` 和 `rds-ca-ecc384-g1`）时遇到严重问题并需要暂时恢复旧证书时执行此操作。

> **Important**
>
> 在更新数据库上的 CA 证书之前，请先更新使用 CA 证书的所有客户端应用程序。

1. 打开终端、AWS CloudShell 或命令提示符窗口。
2. 输入以下命令以在托管式数据库上使用 `rds-ca-2019`。

```
aws lightsail update-relational-database --relational-database-name DatabaseName --
region DatabaseRegion --ca-certificate-identifier rds-ca-2019
```

在命令中，*DatabaseName*替换为要修改的数据库的*DatabaseRegion*名称以及数据库实例所在 AWS 区域 的名称。

示例

```
aws lightsail update-relational-database --relational-database-name Database-1 --
region us-east-1 --ca-certificate-identifier rds-ca-2019
```

托管数据库使用的 CA 证书将在数据库的下一个维护时段内更新，或者如果您在命令末尾添加 `--apply-immediately` 参数，则会立即更新。

为 Lightsail 数据库安排维护和备份

当 Amazon Lightsail 支持新版本的数据库时，您现有的托管数据库可以升级到该版本。有两种升级方式：次要版本升级和主要版本升级。目前，Lightsail 仅支持次要版本升级。

次要版本升级以及其他数据库维护任务会在您数据库的首选维护时段内自动执行。首选维护时段是从 8 小时的时间段中随机选择 30 分钟的时段。 AWS 区域它可以是一周中的任意一天。数据库备份在首选备份时段内执行。首选的备份窗口是从 8 小时的时间段中随机选择 30 分钟的窗口。 AWS 区域它也可以是一周中的任意一天。

> **Note**
>
> 有关每个区域的首选维护时段的更多信息，请参阅 Amazon Relational Database Service (Amazon RDS) 文档中的维护数据库实例指南。有关每个区域的首选备份时段的更多信息，请参阅 Amazon RDS 文档中的使用备份指南。

本指南介绍如何更改首选维护和备份时段，以便数据库处于最低负载时执行这些操作。

先决条件

必须使用 AWS Command Line Interface (AWS CLI) 来更改数据库的首选维护和备份窗口。

完成以下先决任务：

- 安装 AWS CLI — 有关更多信息，请参阅安装 AWS CLI I。
- 配置 AWS CLI-有关更多信息，请参阅配置 AWS CLI。

更改数据库维护时段

在执行维护或备份操作期间，您的数据库可能会不可用。因此，您可能需要将首选维护或备份时段更改为数据库负载处于最低状态的时间。

更改数据库维护时段

1. 打开终端或命令提示符窗口。
2. 输入以下命令以获取您要更改其维护时段的数据库的名称。

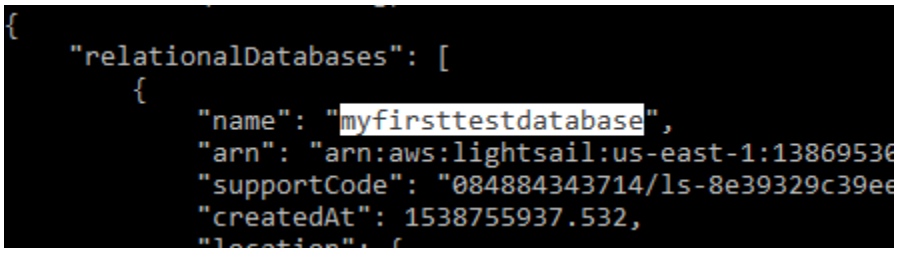
   ```
   aws lightsail get-relational-databases
   ```

   您会看到类似于以下示例的结果：



> **Note**
>
> 如果未列出要修改的数据库，请确认您的 AWS CLI 数据库已针对该数据库 AWS 区域 所在的位置进行了配置。有关更多信息，请参阅配置 AWS CLI。

3. 选中要修改的数据库的名称，然后按 Ctrl+C（如果使用 Windows）或 Cmd+C（如果使用 macOS）将其复制到剪贴板，以便在下一步中使用。



4. 根据您要更改的首选时段，输入以下命令之一。

   - 输入以下命令，以更改数据库维护时段。

```
aws lightsail update-relational-database --relational-database-name DatabaseName
 --preferred-maintenance-window MaintenanceWindow
```

在该命令中，将：

- *DatabaseName*使用数据库的名称。
- *MaintenanceWindow*随着新的维护窗口期限。

  以 ddd:hh24:mi-ddd:hh24:mi 格式定义首选维护时段的时间。它还必须采用通用协调时间 (UTC) 格式，并定义为至少 30 分钟的时段。首选维护时段不能与首选备份时段重叠。

示例：

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-maintenance-window Tue:16:00-Tue:16:30
```

- 输入以下命令，以更改数据库备份时段。

```
aws lightsail update-relational-database --relational-database-name DatabaseName
 --preferred-backup-window BackupWindow
```

在该命令中，将：

- *DatabaseName*使用数据库的名称。
- *BackupWindow*使用新的备份窗口期限。

  以 hh24:mi-hh24:mi 格式定义首选备份时段的时间。它还必须采用通用协调时间 (UTC) 格式，并定义为至少 30 分钟的时段。首选备份时段不能与首选维护时段重叠。

示例：

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-backup-window 14:00-14:30
```

您会看到类似于以下示例的结果：



后续步骤

以下指南可帮助您管理数据库：

- 为您的数据库配置数据导入模式
- 为您的数据库配置公有模式
- 管理数据库密码
- 连接到 MySQL 数据库
- 连接到 PostgreSQL 数据库
- 将数据导入 MySQL 数据库
- 将数据导入 PostgreSQL 数据库
- 创建数据库的快照

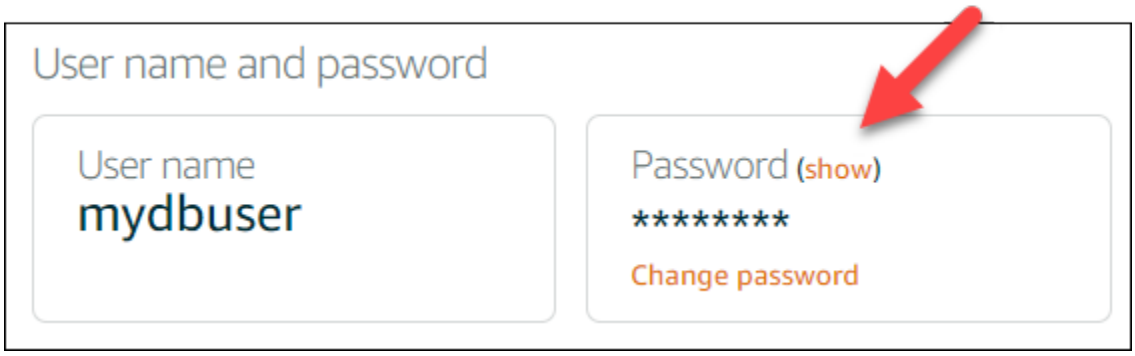
更改你的 Lightsail 数据库密码

当你在 Amazon Lightsail 中创建新数据库时，你可以让 Lightsail 为你创建一个强密码或指定你自己的密码。您可以随时在 Lightsail 控制台中查看或更改当前的数据库密码。

管理数据库密码

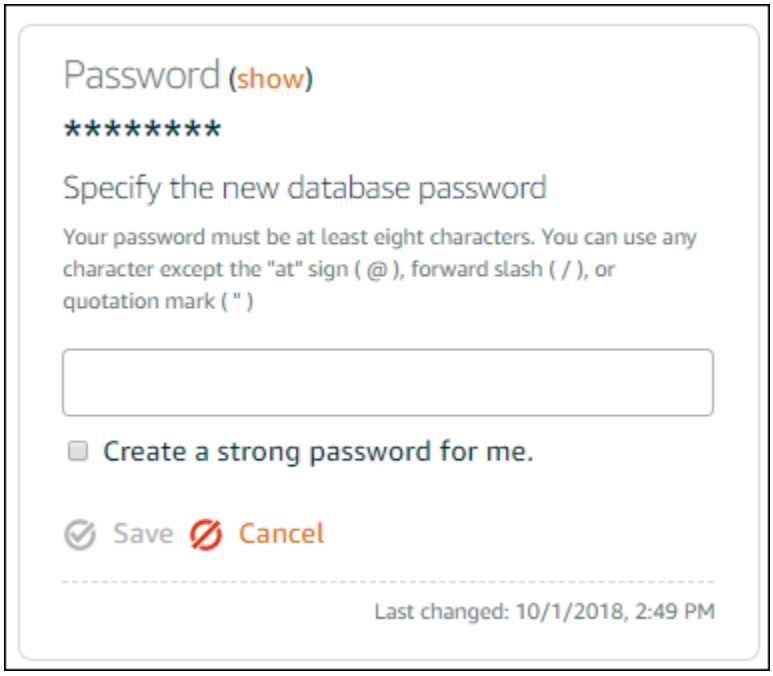
1. 登录 Lightsail 控制台。

2. 在左侧导航窗格中，选择数据库。
3. 选择要管理其密码的数据库的名称。
4. 在 Connect (连接) 选项卡的 User name and passwords (用户名和密码) 部分下方，选择显示以查看当前数据库密码。



5. 要更改数据库密码，请选择 Change password (更改密码)。

   您可以选择让 Lightsail 为您创建强密码，也可以在文本框中输入自己的密码。密码可以包含除“/”、“””或“@”之外的任意可打印 ASCII 字符。对于 MySQL 数据库，密码必须包含 8 到 41 个字符。对于 PostgreSQL，密码必须包含 8 到 128 个字符。



6. 完成此操作后，选择保存。

   系统将立即应用更改后的数据库密码。如果您输入了自己的密码，系统会立即保存该密码。如果 Lightsail 为您创建了密码，则密码将在几秒钟内生成。选择显示以查看新密码。

后续步骤

以下是一些指南，可帮助您在 Lightsail 中管理数据库：

- 连接到 MySQL 数据库
- 连接到 PostgreSQL 数据库
- 创建数据库的快照

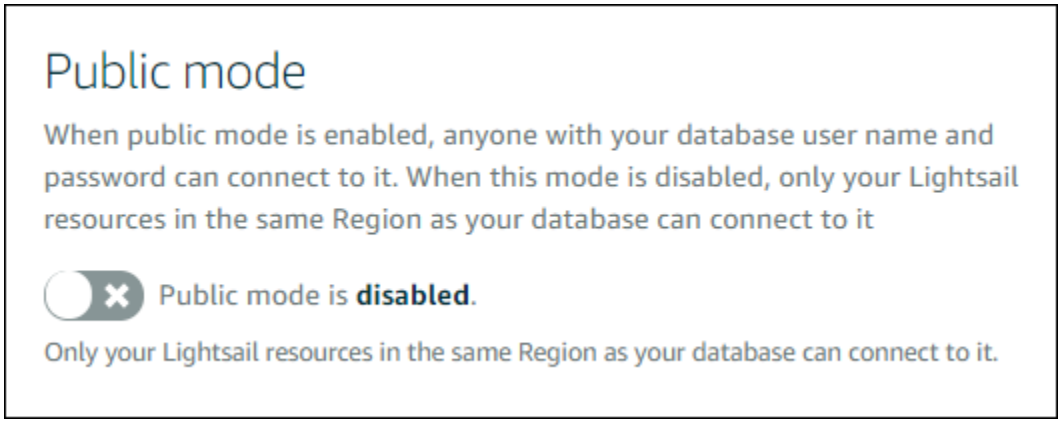
为您的 Lightsail 数据库配置公共访问权限

只有同一 Lightsail 账户中的 Lightsail 资源（实例、负载均衡器等）才能访问您在 Amazon Lightsail 中的托管数据库。一种常见的场景是创建包含面向公众的 Web 应用程序的 Lightsail 实例和不可公开访问的 Lightsail 数据库，然后将两者连接起来。

启用公有模式功能以使您的数据库可公开访问。这样，拥有数据库终端节点、端口、用户名和密码的任何人都可以连接到您的数据库。有关更多信息，请参阅连接到 MySQL 数据库或连接到 PostgreSQL 数据库。

为您的数据库配置公有模式

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择您要为其配置公有模式的数据库的名称。
4. 选择 Networking（联网）选项卡。
5. 在公有模式部分下，使用切换按钮将其打开。同样，使用切换按钮将其关闭。



公开可访问性设置立即开始应用，但可能需要几分钟才能完成。在此期间，您的数据库的状态会更改为正在修改。应用公开可访问性设置后，数据库的状态会更改为可用。

后续步骤

以下指南可帮助您管理数据库：

- 为您的数据库配置数据导入模式
- 管理数据库密码
- 连接到 MySQL 数据库
- 连接到 PostgreSQL 数据库
- 将数据导入 MySQL 数据库
- 将数据导入 PostgreSQL 数据库
- 创建数据库的快照

通过参数更新优化 Lightsail 数据库性能

数据库参数，也称为数据库系统变量，用于定义 Amazon Lightsail 中托管数据库的基本属性。例如，您可以定义某个数据库参数以限制数据库连接数，或者定义另一个参数以限制数据库缓冲池的大小。本指南向您介绍如何获取托管数据库的参数列表，以及如何使用 AWS Command Line Interface (AWS CLI) 更新这些参数。

> **Note**
>
> 有关 MySQL 系统变量的更多信息，请参阅 MySQL 5.6、MySQL 5.7 或 MySQL 8.0 文档。有关 PostgreSQL 系统变量的更多信息，请参阅 PostgreSQL 9.6、PostgreSQL 10、PostgreSQL 11 或 PostgreSQL 12 文档。

先决条件

- 如果尚未安装并配置 AWS CLI，请执行该操作。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

获取可用数据库参数的列表

数据库参数因数据库引擎而异，因此，您应获取可用于托管式数据库的参数列表。这样您就可以判断哪些参数需要修改，以及参数的生效方式。

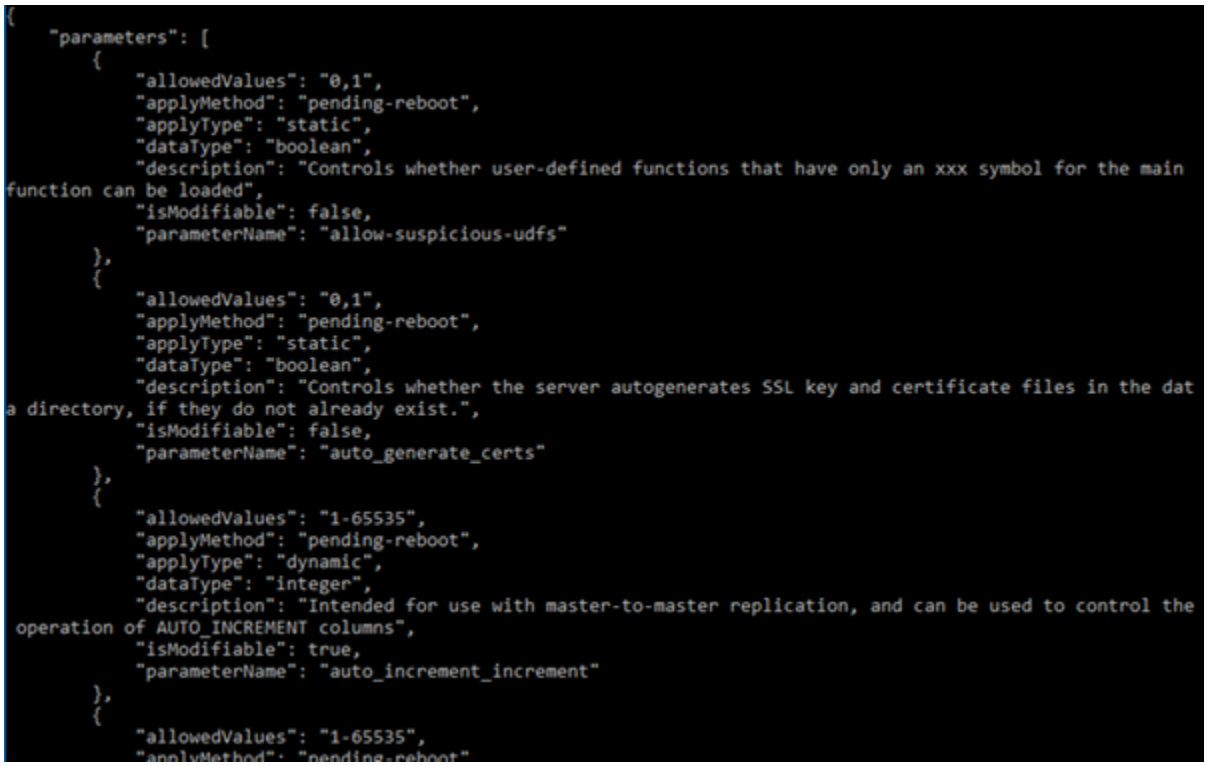
获取可用数据库参数的列表

1. 打开终端或命令提示符窗口。
2. 输入以下命令以获取您数据库参数的列表。

```
aws lightsail get-relational-database-parameters --relational-database-
name DatabaseName
```

在命令中，*DatabaseName*替换为数据库的名称。

您会看到类似于以下示例的结果：



> **Note**
>
> 如果参数结果分页显示，系统会列出下一页标记 ID。请记下下一页标记 ID 并在下一步中使用该 ID，以查看下一页参数结果。

3. 如果结果分页显示，请使用以下命令查看其他参数集。否则，请跳到下一步。

```
aws lightsail get-relational-database-parameters --relational-database-
name DatabaseName --page-token NextPageTokenID
```

在该命令中，将：

- *DatabaseName*用你的数据库的名字。
- *NextPageTokenID*使用下一页的令牌 ID。

结果将显示每个数据库参数的以下信息：

- 允许的值 – 指定参数值的有效范围。
- Apply method (应用方法) – 指定何时应用参数更改。允许的选项为 `immediate` 或 `pending-reboot`。有关如何定义应用方法的更多信息，请参阅下面的“Apply type (应用类型)”。
- Apply type (应用类型) – 指定特定于引擎的提交类型。如果为 `dynamic`，则说明可以使用 `immediate` 应用方法应用该参数，且数据库将立即开始使用新参数值。如果为 `static`，则说明只能使用 `pending-reboot` 应用方法应用该参数，且数据库将仅在重启后开始使用新参数。
- Data type (数据类型) – 指定参数的有效数据类型。
- Description (描述) – 对参数的描述。
- Is modifiable (可修改) – 一个布尔值，用于指示参数是否可修改。如果为 `true`，则说明可修改参数。
- 参数名称 – 指定参数的名称。此值应与 `update relational database` 操作及 `parameter name` 参数结合使用。

4. 找到您要更改的参数，并记下参数名称、允许的值及应用方法。我们建议您将参数名称复制到剪贴板，以避免输入错误的信息。要执行此操作，请突出显示该参数名称，然后按 Ctrl+C（如果使用的是 Windows）或 Cmd+C（如果使用的是 macOS），将其复制到剪贴板。然后，相应地按 Ctrl+V 或 Cmd+V 对其进行粘贴。

   找到要修改的参数的名称后，继续执行本指南的下一部分，将参数更改为所需的值。

更新数据库参数

获得要更改的参数名称后，请执行以下步骤在 Lightsail 中修改托管数据库的参数：

更新数据库参数

- 在终端窗口或命令提示符窗口中输入以下命令以更新托管式数据库的参数。

```
aws lightsail update-relational-database-parameters
 --relational-database-name DatabaseName --parameters
 "parameterName=ParameterName,parameterValue=NewParameterValue,applyMethod=ApplyMethod"
```

在该命令中，将：

- *DatabaseName*用你的数据库的名字。
- *ParameterName*使用您要修改的参数的名称。
- *NewParameterValue*使用参数的新值。
- *ApplyMethod*使用参数的 apply 方法。

  如果参数的应用类型为 dynamic，则可以使用 immediate 应用方法应用该参数，且数据库将立即开始使用新参数值。但是，如果参数的应用类型为 static，则只能使用 pending-reboot 应用方法应用该参数，且数据库将仅在重启后开始使用新参数。

您会看到类似于以下示例的结果：


```
{
    "operations": [
        {
            "id": "2c650987-11e8-463f-94d5-0c15aacaf12b",
            "resourceName": "myfirsttestdatabase",
            "resourceType": "RelationalDatabase",
            "createdAt": 1539204831.214,
            "location": {
                "availabilityZone": "us-east-1a",
                "regionName": "us-east-1"
            },
            "isTerminal": true,
            "operationType": "UpdateRelationalDatabaseParameters",
            "status": "Succeeded",
            "statusChangedAt": 1539204831.214
        }
    ]
}
```


数据库参数的更新取决于所用的应用方法。

升级 Lightsail 数据库的主要版本

当 Amazon Lightsail 支持新版本的数据库引擎时，您可以将数据库升级到新版本。Lightsail 提供了两个数据库蓝图，MySQL 和 PostgreSQL。本指南介绍如何升级 MySQL 或 PostgreSQL 数据库实例的主要版本。您只能使用以下方法升级数据库的主要版本 update-relational-databaseAPI 操作。

我们将使用 AWS CloudShell 来执行升级。 CloudShell 是一款基于浏览器的预先认证外壳，您可以直接从 Lightsail 控制台启动它。使用 CloudShell，您可以使用首选外壳运行 AWS Command Line Interface (AWS CLI) 命令，例如 Bash PowerShell、或 Z shell。您无需下载或安装命令行工具，即可完成此操作。有关如何设置和使用的 CloudShell更多信息，请参阅 Lightsai AWS CloudShell I 中的。

了解更改

主要版本升级可能会引入与先前版本的许多不兼容之处。在升级期间，这些不兼容性会引起问题。为成功执行升级，可能需要准备数据库。有关升级数据库主要版本的信息，请参阅 MySQL 和 PostgreSQL 网站上的以下主题。

- 准备安装以进行升级
- MySQL 升级检查器实用程序
- 升级 PostgreSQL 集群

先决条件

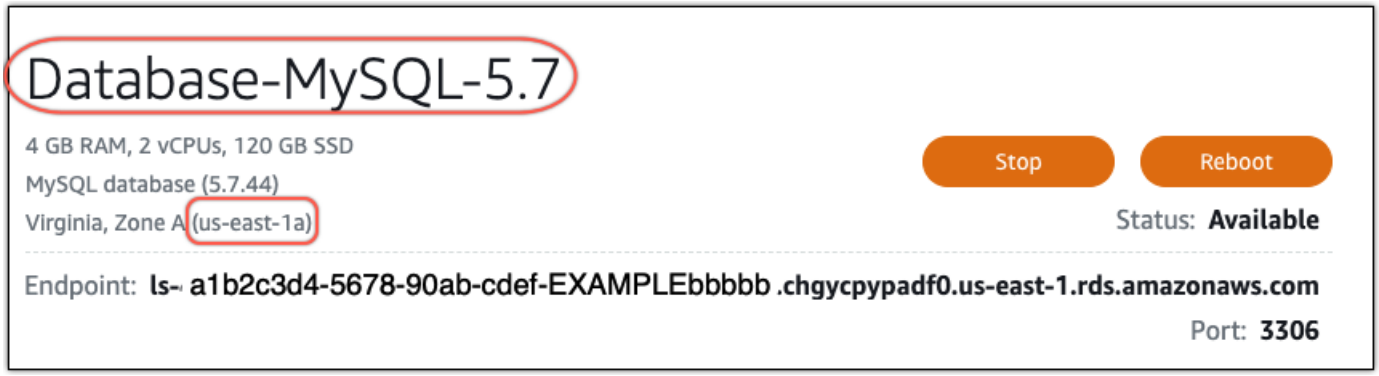
1. 确认您的应用程序支持数据库的两个主要版本。
2. 建议您在进行任何更改之前创建数据库实例的快照。有关更多信息，请参阅创建 Lightsail 数据库的快照。
3. （可选）根据刚创建的快照创建新的数据库实例。由于数据库更新需要停机时间，因此您可以在升级当前处于活动状态的数据库之前，在新数据库上测试升级情况。有关创建数据库副本的更多信息，请参阅创建 Lightsail 数据库的快照。

更新数据库主要版本

Lightsail 支持 MySQL 和 PostgreSQL 数据库实例的主要版本升级。以下过程以 MySQL 数据库为例。但是，PostgreSQL 数据库的过程和命令是相同的。

完成以下过程以升级 Lightsail 数据库的数据库主版本。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 记下要升级 AWS 区域 的数据库实例的名称和名称。



4. 在 Lightsail 控制台的左下角，选择。CloudShell CloudShell 终端将在同一个浏览器选项卡中打开。当系统显示命令提示符时，表示 shell 已经准备就绪，可以进行交互。
5. 在 CloudShell 提示符下输入以下命令以获取可用数据库蓝图 IDs 的列表。

```
aws lightsail get-relational-database-blueprints
```

6. 记下您要升级的主要版本的蓝图 ID。例如，`mysql_8_0`。



7. 输入以下命令以升级数据库的主要版本。升级将在数据库的下一个维护时段内进行。在命令中，*DatabaseName*替换为数据库的名称、*blueprintId*要升级到的主要版本的蓝图 ID 以及数据库所在版本*DatabaseRegion* AWS 区域 的蓝图 ID。

```
aws lightsail update-relational-database \
 --relational-database-name DatabaseName \
 --relational-database-blueprint-id blueprintId \
 --region DatabaseRegion
```

（可选）要立即应用升级，请在命令中包含 `--apply-immediately` 参数。您将看到与以下示例类似的响应，并且在应用升级时数据库将不可用。有关更多信息，请参阅 update-relational-database在 Lightsail API 参考中。

```
% aws lightsail update-relational-database \
--relational-database-name "Database-Mysql-5.7" \
--relational-database-blueprint-id "mysql_8_0" \
--apply-immediately \
[--region us-east-1
{
    "operations": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
            "resourceName": "Database-Mysql-5.7",
            "resourceType": "RelationalDatabase",
            "createdAt": 2024-01-01T00:00:00.00000+00:00",
            "location": {
                "availabilityZone": "us-east-1a",
                "regionName": "us-east-1"
            },
            "isTerminal": true,
            "operationDetails": "",
            "operationType": "UpdateRelationalDatabase",
            "status": "Succeeded",
            "statusChangedAt": 2024-01-01T00:00:00.00000+00:00",
        }
```

8. 输入以下命令以验证是否已计划在下一个数据库维护时段进行主要版本升级。在命令中，*DatabaseName*替换为数据库的*DatabaseRegion*名称和数据库所在 AWS 区域 的名称。

```
aws lightsail get-relational-database \
 --relational-database-name DatabaseName \
 --region DatabaseRegion
```

在get-relational-database响应中，数据库 state将在下一个维护时段通知您即将进行主要版本升级。您可以在中找到下一个维护时段的日期和时间 preferredMaintenanceWindow回复的部分。

数据库实例状态

```
"state": "upgrading",
  "backupRetentionEnabled": true,
  "pendingModifiedValues": {
  "engineVersion": "8.0.36"
```

维护窗口

```
"preferredMaintenanceWindow": "wed: 09:22-wed: 09:52"
```

后续步骤

如果您创建测试数据库，则可以在确认应用程序可以与升级数据库结合使用后将其删除。保留您为先前数据库创建的快照，以备不时之需。您还应该为升级后的数据库创建快照，以便拥有该数据库的新point-in-time副本。

在 Lightsail 中将数据从 MySQL 5.6 数据库迁移到更新的版本

在本教程中，我们将介绍如何在 Amazon Lightsail 中将数据从 MySQL 5.6 数据库迁移到新的 MySQL 5.7 数据库。要执行迁移，请连接到 MySQL 5.6 数据库并导出现有数据。然后连接到 MySQL 5.7 数据库并导入数据。在新数据库获得所需数据后，您可以重新配置应用程序以连接到新数据库。

内容

- 步骤 1：了解更改
- 步骤 2：完成先决条件
- 步骤 3：连接到 MySQL 5.6 数据库并导出数据
- 步骤 4：连接到 MySQL 5.7 数据库并导入数据

- 步骤 5：测试您的应用程序并完成迁移

步骤 1：了解更改

从 MySQL 5.6 数据库到 MySQL 5.7 数据库是一次重大的版本升级。主要的版本升级可能包含未与现有应用程序向后兼容的数据库更改。建议您在将任何升级应用于生产实例前全面测试这些升级。有关更多信息，请参阅 MySQL 文档中的 MySQL 5.7 中的更改。

我们建议您首先将数据从现有的 MySQL 5.6 数据库迁移到新的 MySQL 5.7 数据库。然后在预生产实例上使用新的 MySQL 5.7 数据库测试您的应用程序。如果应用程序的运行与预期一致，则将更改应用于生产实例中的应用程序。为了更进一步，您可以将数据从现有的 MySQL 5.7 数据库迁移到新的 MySQL 8.0 数据库，再次在预生产中测试应用程序，并将更改应用于生产中的应用程序。

步骤 2：完成先决条件

您必须完成以下先决条件才能继续本教程的后续部分：

- 在本地计算机上安装 MySQL Workbench，您将使用该计算机连接到数据库以导出和导入数据。 有关更多信息，请参阅 MySQL网站上的 MySQL Workbench 下载。
- 在 Lightsail 中创建 MySQL 5.7 数据库。有关更多信息，请参阅在 Amazon Lightsail 中创建数据库。
- 启用数据库的公有模式。这将允许您使用 MySQL Workbench 来连接它们。导出和导入数据后，可以禁用数据库的公有模式。有关更多信息，请参阅配置数据库的公有模式。
- 配置 MySQL Workbench 以连接数据库 有关更多信息，请参阅连接到您的 MySQL 数据库。

步骤 3：连接到 MySQL 5.6 数据库并导出数据

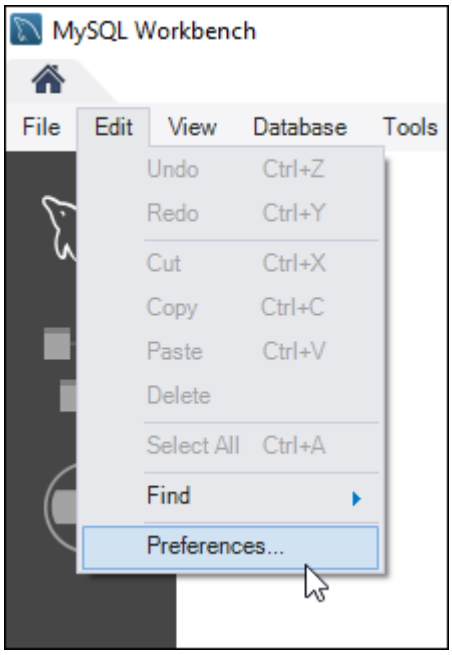
在这部分教程中，您将连接到 MySQL 5.6 数据库，并使用 MySQL Workbench 从中导出数据。有关使用 MySQL Workbench 导出数据的更多信息，请参阅 MySQL Workbench 手册中的 SQL 数据导出和导入向导。

1. 使用 MySQL Workbench 连接您的 MySQL 5.6 数据库。

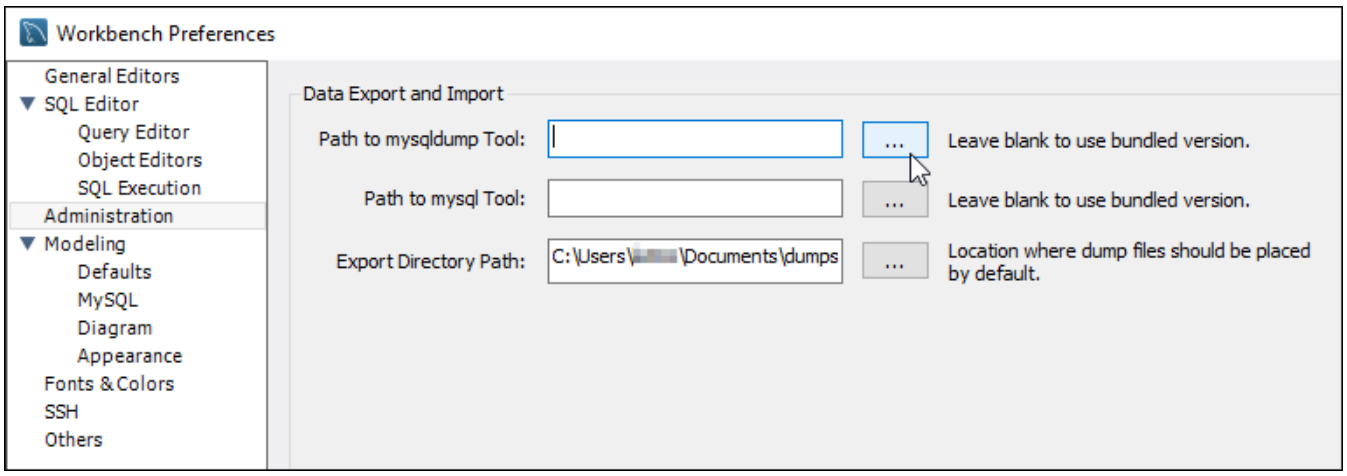
   MySQL Workbench 使用 mysqldump 来导出数据。MySQL Workbench 使用的 mysqldump 版本必须与您将从中导出数据的 MySQL 数据库版本相同（或版本更高）。例如，如果您要从 MySQL 5.6.51 数据库中导出数据，则必须使用 mysqldump 版本 5.6.51 或更高版本。您可能需要在本地计算机上下载并安装适当版本的 MySQL 服务器，以确保您使用的是正确版本的 mysqldump。要下载特定版本的 MySQL 服务器，请参阅 MySQL 网站上的 MySQL 社群版本下载。Windows MSI 的 MySQL 安装程序提供了下载任何版本 MySQL 服务器的选项。

请完成以下步骤，选择要在 MySQL Workbench 中使用的正确版本的 mysqldump：

1. 在 MySQL Workbench 中，选择编辑，然后选择首选项。

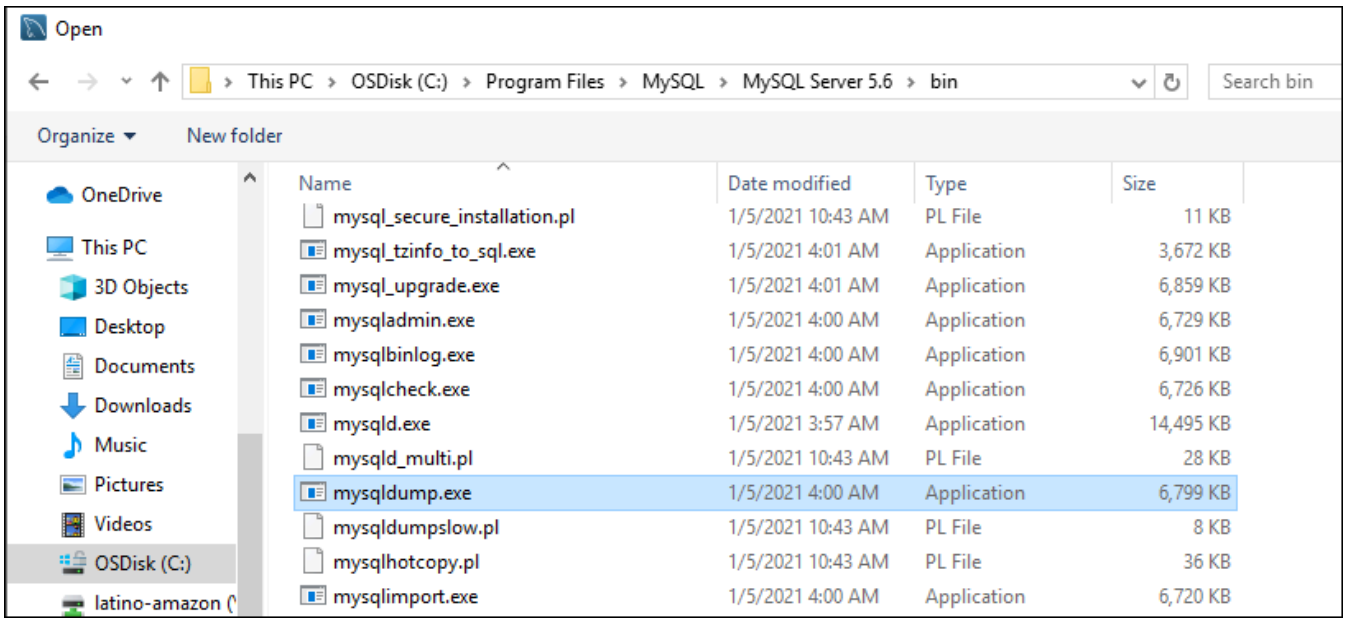


2. 在导航窗格中选择管理。
3. 在 Workbench 首选项窗口中，选择 Myqldump 工具的路径文本框。

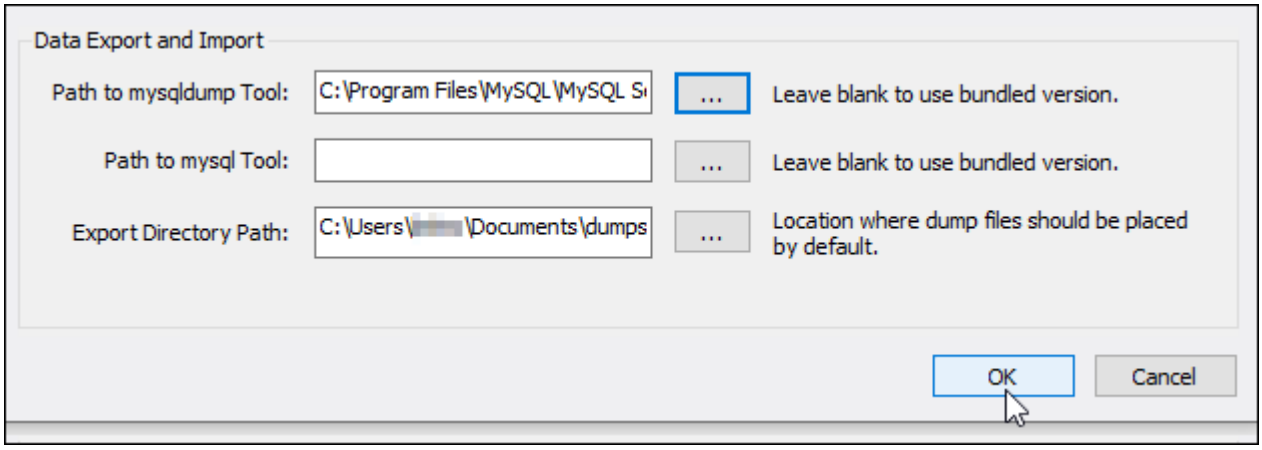


4. 浏览到相应的 mysqldump 可执行文件所在的位置，然后双击它。

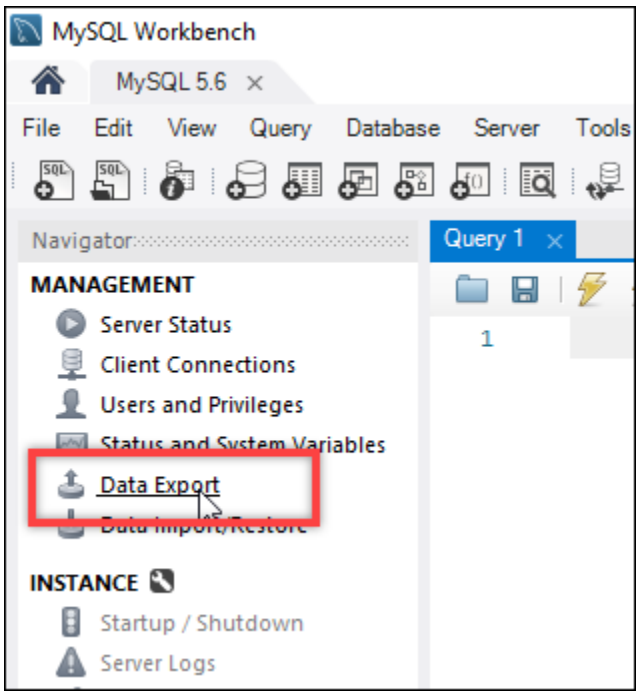
   在 Windows 中，mysqldump.exe 文件通常位于 C:\Program Files\MySQL\MySQL Server 5.6\bin 目录。对于 Linux，在终端中输入 which mysqldump 以查看 mysqldump 文件的位置。



5. 在 Workbench 首选项窗口中选择确定。

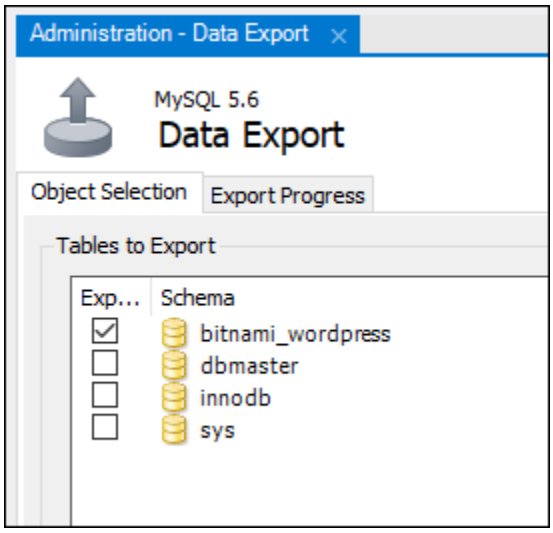


2. 在导航窗格中选择数据导出

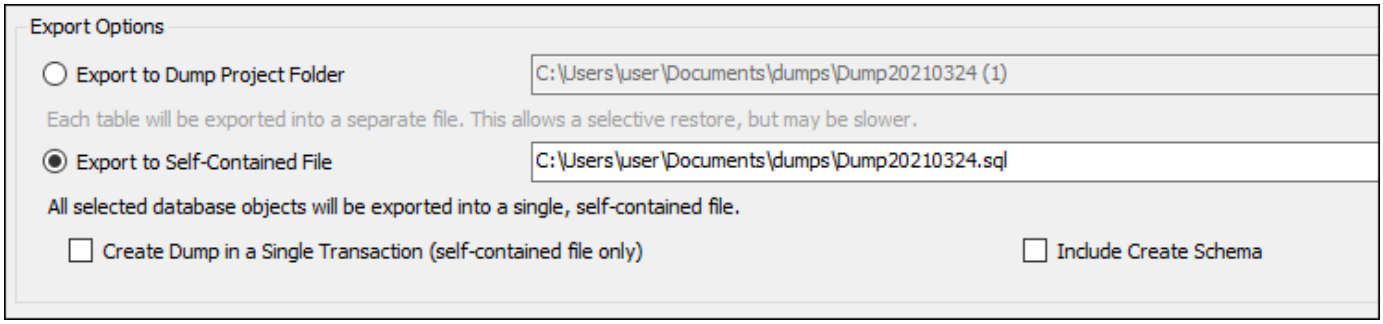


3. 在显示的数据导出选项卡上，在要导出的表旁边添加复选标记。

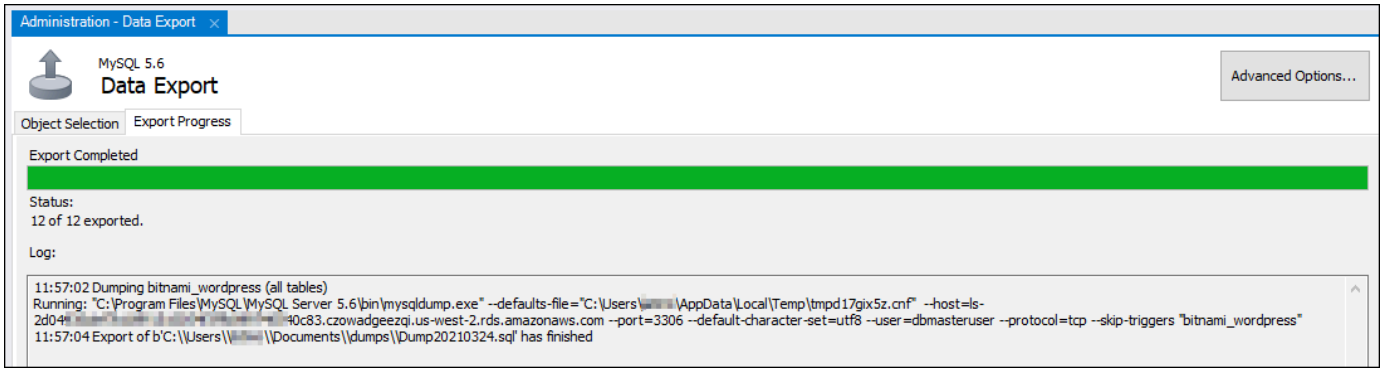
> **Note**
>
> 在此示例中，我们选择了包含 “Bitnami 认证” WordPress 实例上的 WordPress 网站数据的`bitnami_wordpress`表。



4. 在导出选项部分，选择导出到自包含文件，然后记下保存导出文件的目录。



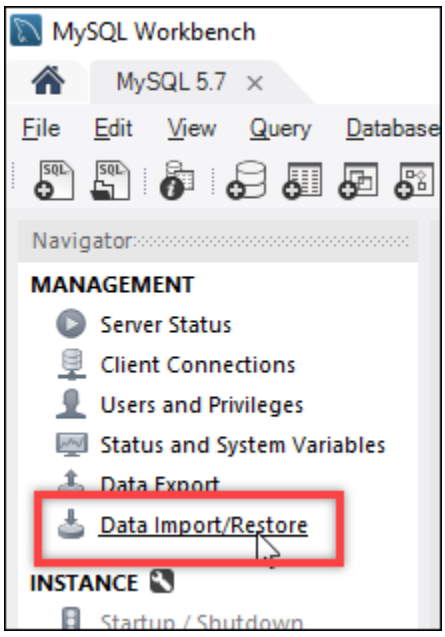
5. 选择 Start Export (开始导出)。
6. 等待导出完成，然后再继续执行本教程的下一部分。



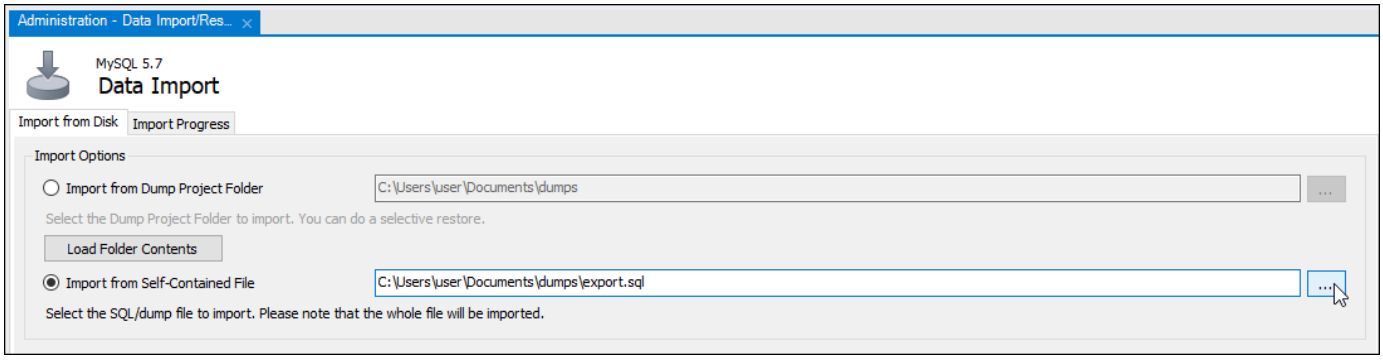
步骤 4：连接到 MySQL 5.7 数据库并导入数据

在这部分教程中，您将连接到 MySQL 5.7 数据库，并使用 MySQL Workbench 导入数据。

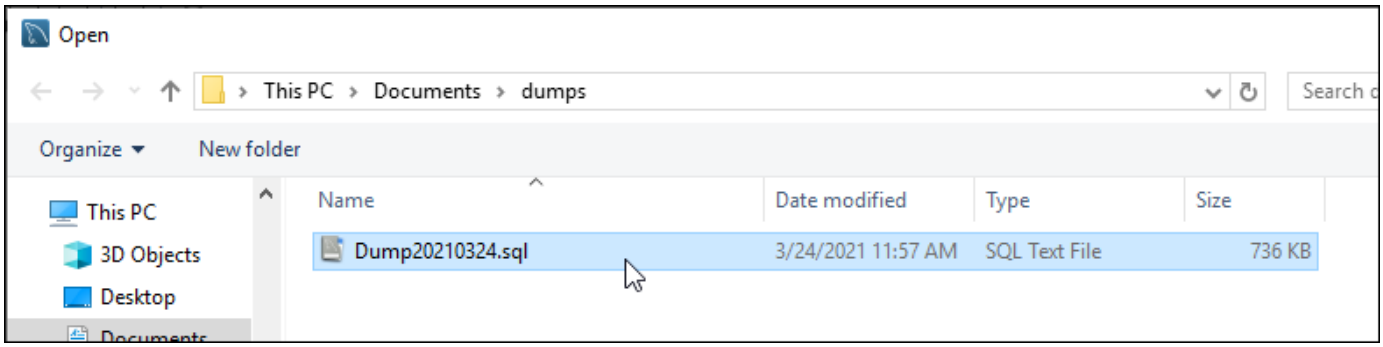
1. 在本地计算机上使用 MySQL Workbench 连接您的 MySQL 5.7 数据库。
2. 在导航窗格中选择数据导入/恢复。



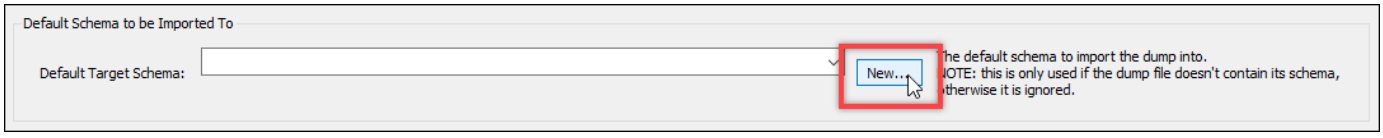
3. 在显示的数据导入选项卡中，选择从自包含文件导入，然后选择文本框旁边的省略号按钮。



4. 浏览到导出文件的保存位置，然后双击它。

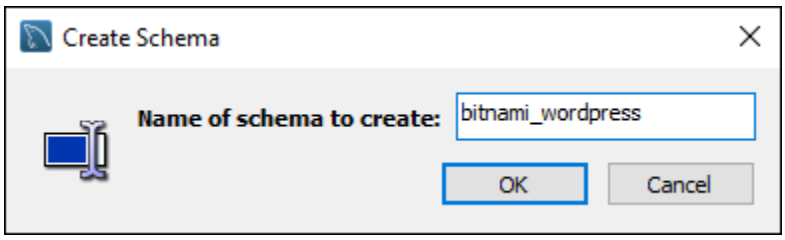


5. 在要导入到的默认架构部分中选择新建。

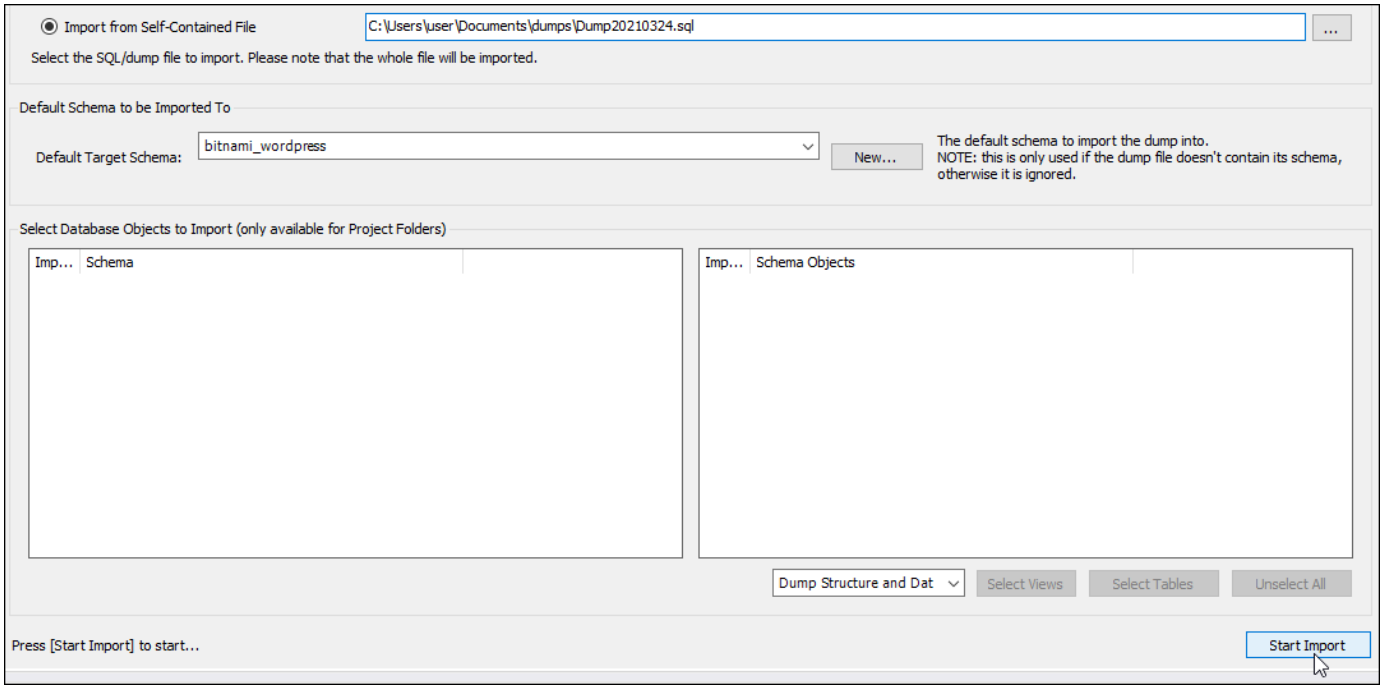


6. 在显示的创建架构窗口中输入架构的名称。

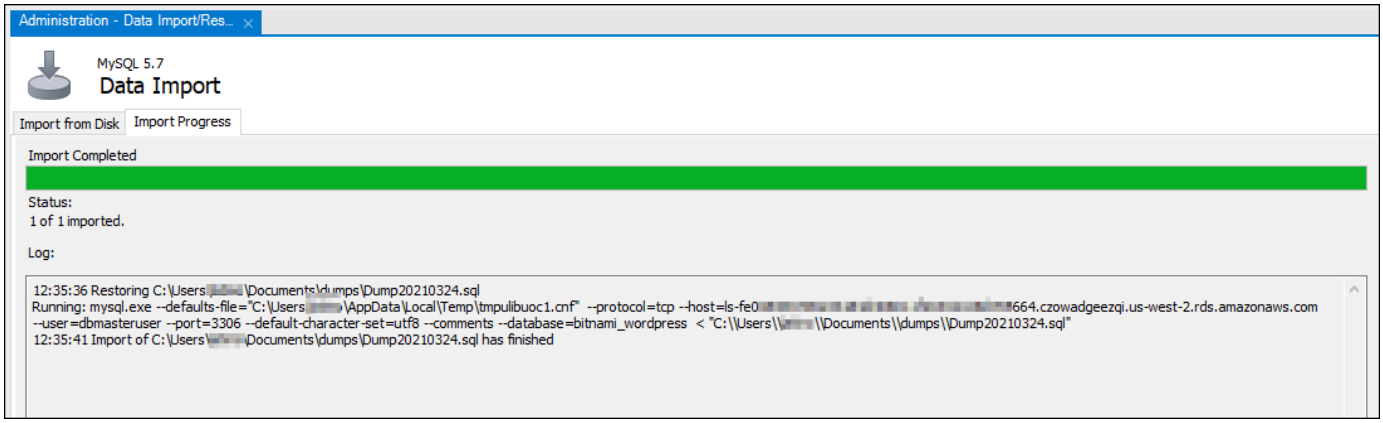
> **Note**
>
> 在此示例中，我们输入 `bitnami_wordpress`，因为它是我们导出的数据库表的名称。



7. 选择 Start Import (开始导入)。



8. 等待导入完成，然后再继续本教程的下一部分。



步骤 5：测试您的应用程序并完成迁移

至此，您的数据已经位于您的新 MySQL 5.7 数据库中。在预生产环境中配置应用程序，并测试应用程序与新 MySQL 5.7 数据库之间的连接。如果应用程序的运行与预期一致，则将更改应用于生产环境中的应用程序。

完成迁移后，应禁用数据库的公有模式。当您确定您不再需要 MySQL 5.6 数据库时，可将其删除。但是，您应该先创建 MySQL 5.6 数据库的快照，然后再删除它。使用时，您还应该创建新 MySQL 5.7 数据库的快照。有关更多信息，请参阅创建数据库快照。

使用 Lightsail 负载均衡器分配网络流量

Lightsail 负载均衡器在多个可用区的多个 Lightsail 实例之间分配传入的网络流量。负载平衡可提高应用程序在实例上的可用性和容错能力。您可以根据需求的变化在 Lightsail 负载均衡器中添加和删除实例，而不会中断应用程序的整体请求流。

借助 Lightsail 负载平衡，我们可以创建 DNS 主机名，并将发送到该主机名的所有请求路由到目标 Lightsail 实例池。您可以根据需要向负载均衡器添加任意数量的目标实例，前提是您的实例总数保持在 Lightsail 账户配额之内。

负载均衡器功能

Lightsail 负载均衡器提供以下功能：

- HTTPS 加密 — 默认情况下，Lightsail 负载均衡器通过端口 80 处理未加密 (HTTP) 的流量请求。通过将经过验证的 Lightsail SSL/TLS 证书附加到您的负载均衡器来激活 HTTPS 加密。这使负载均衡器能够通过端口 443 处理加密的 (HTTPS) 流量请求。有关更多信息，请参阅 SSL/TLS 证书。

  在负载均衡器上激活 HTTPS 加密后，可以使用以下功能：

  - HTTP 到 HTTPS 重新导向 – 激活 HTTP 到 HTTPS 重新导向以自动将 HTTP 请求重新导向到 HTTPS 加密连接。有关更多信息，请参阅为负载均衡器配置 HTTP 到 HTTPS 重新导向。
  - TLS 安全策略 – 在负载均衡器上配置 TLS 安全策略。有关更多信息，请参阅在 Amazon Lightsail 负载均衡器上配置 TLS 安全策略。
- 运行状况检查 – 默认情况下，将在所连接实例上运行的 Web 应用程序的根目录下对这些实例执行运行状况检查。运行状况检查可监控实例的运行状况，以便负载均衡器仅将请求发送到正常运行的实例。有关更多信息，请参阅 Lightsail 负载均衡器的运行状况检查。
- 会话持久性 – 如果在网站访问者的浏览器本地存储会话信息，请配置会话持久性。例如，您可能正在运行一个 Magento 电子商务应用程序，在负载均衡的 Lightsail 实例上有一个购物车。如果配置了会话持久性，而您的网站访问者在购物车中添加商品，然后结束会话，那么当他们返回时，仍会找到购物车商品。有关更多信息，请参阅为负载均衡器启用会话持久性。

何时使用负载均衡器

在很多访客同时使用时，如果您的网站偶尔会出现流量高峰，或者提供的内容可能在实例上产生大量负载，您应该使用负载均衡器。例如，如果网站上的图像较多，您可以将图像请求与其他页面请求进行负载均衡。这样，就会提高页面加载速度和用户满意度。

您可以使用负载均衡器创建高可用性的网站。高可用性是指您的网站或应用程序在给定时间段内保持启动状态的时间。如果您曾经遇到网站故障，则负载均衡器可以帮助您增加正常运行时间。您可以使用 Lightsail 负载均衡器通过添加分布在多个可用区的目标实例来提高应用程序的高可用性。

容错能力是一个相关的概念。如果您的网站在某个实例或数据库发生故障后仍能继续正常工作，则将其视为具有容错能力。负载均衡器可以帮助您创建容错的应用程序或网站。

建议进行负载均衡的应用程序

并非所有 Lightsail 应用程序都需要负载均衡器。如果您决定创建负载均衡的应用程序，必须先配置您的应用程序。例如，要准备 LAMP 堆栈应用程序以进行负载均衡，应先创建集中的专用数据库，以使所有目标实例在其中读取/写入数据。您也可以考虑创建集中式媒体存储，例如 Lightsail 对象存储桶。有关更多信息，请参阅配置实例进行负载均衡。

开始使用负载均衡器

你可以使用 Lights ail 控制台、 AWS Command Line Interface (AWS CLI) 或 Lightsail API 创建负载均衡器。您还必须配置实例以进行负载均衡。

在创建负载均衡器并连接配置的实例后，您可以使用以下主题启用 HTTPS。有关更多信息，请参阅为负载均衡器创建 SSL/TLS 证书。

使用 Lightsail 负载均衡器分配网络流量

您可以创建负载均衡器以在应用程序中添加冗余，或者处理更多 Web 流量。创建负载均衡器后，您可以连接要平衡的 Lightsail 实例。要了解更多信息，请参阅负载均衡器

先决条件

在开始之前，请确保您已为 Lightsail 实例做好负载平衡的准备。有关更多信息，请参阅配置实例进行负载均衡。

创建负载均衡器

1. 登录 Lightsail 控制台。
2. 选择 Networking（联网）选项卡。
3. 选择创建负载均衡器。
4. 确认将在 AWS 区域 哪里创建负载均衡器，或者选择更改区域以选择其他区域。

> **Note**
>
> 默认情况下，将会创建负载均衡器并打开端口 80 以接受 HTTP 请求。在创建负载均衡器后，您可以创建 SSL/TLS 证书并配置 HTTPS。有关更多信息，请参阅为负载均衡器创建 SSL/TLS 证书

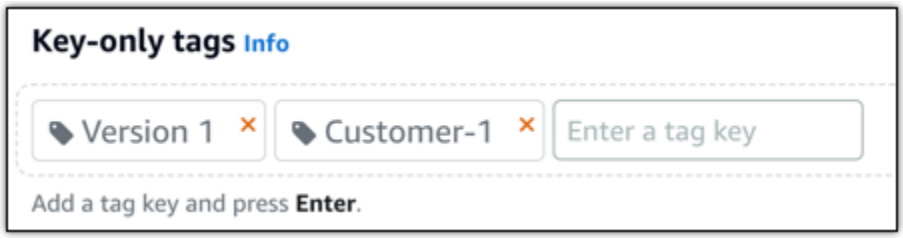
5. 输入负载均衡器的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

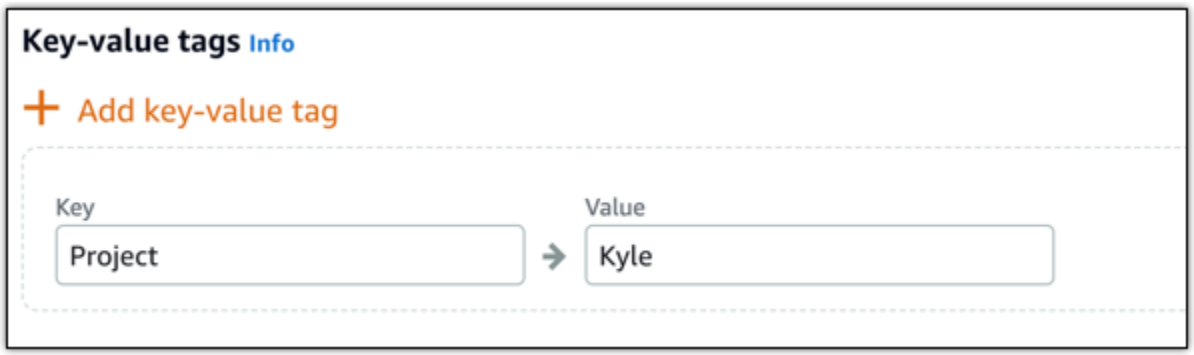
6. 选择以下选项之一，以将标签添加到负载均衡器：

   - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

   - 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

     一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。

> **Note**
>
> 有关“仅键”标签和键值标签的更多信息，请参阅标签。

7. 选择创建负载均衡器。

将实例附加到您的负载均衡器

创建负载均衡器后，Lightsail 会将您带到负载均衡器管理页面。如果您需要再次找到该页面，请在 Lightsail 主页上选择 “网络” 选项卡，然后选择 Lightsail 负载均衡器的名称进行管理。

> **Note**
>
> 您的 Lightsail 实例必须处于运行状态，然后才能成功将其连接到您的负载均衡器。

1. 在负载均衡器管理页面上，选择 Target instances（目标实例）。
2. 在 Target instances（目标实例）下拉菜单中选择实例。
3. 选择 Attach（连接）。连接可能需要几分钟的时间。

   通过选择 Attach another（连接另一个），然后重复上述步骤，将另一个实例连接到负载均衡器。

后续步骤

创建负载均衡器并连接您的实例后，请完成以下后续步骤，以配置负载均衡器：

- 为负载均衡器创建 SSL/TLS 证书
- 自定义负载均衡器的运行状况检查

如果在使用负载均衡器时遇到问题，请参阅对负载均衡器进行故障排除

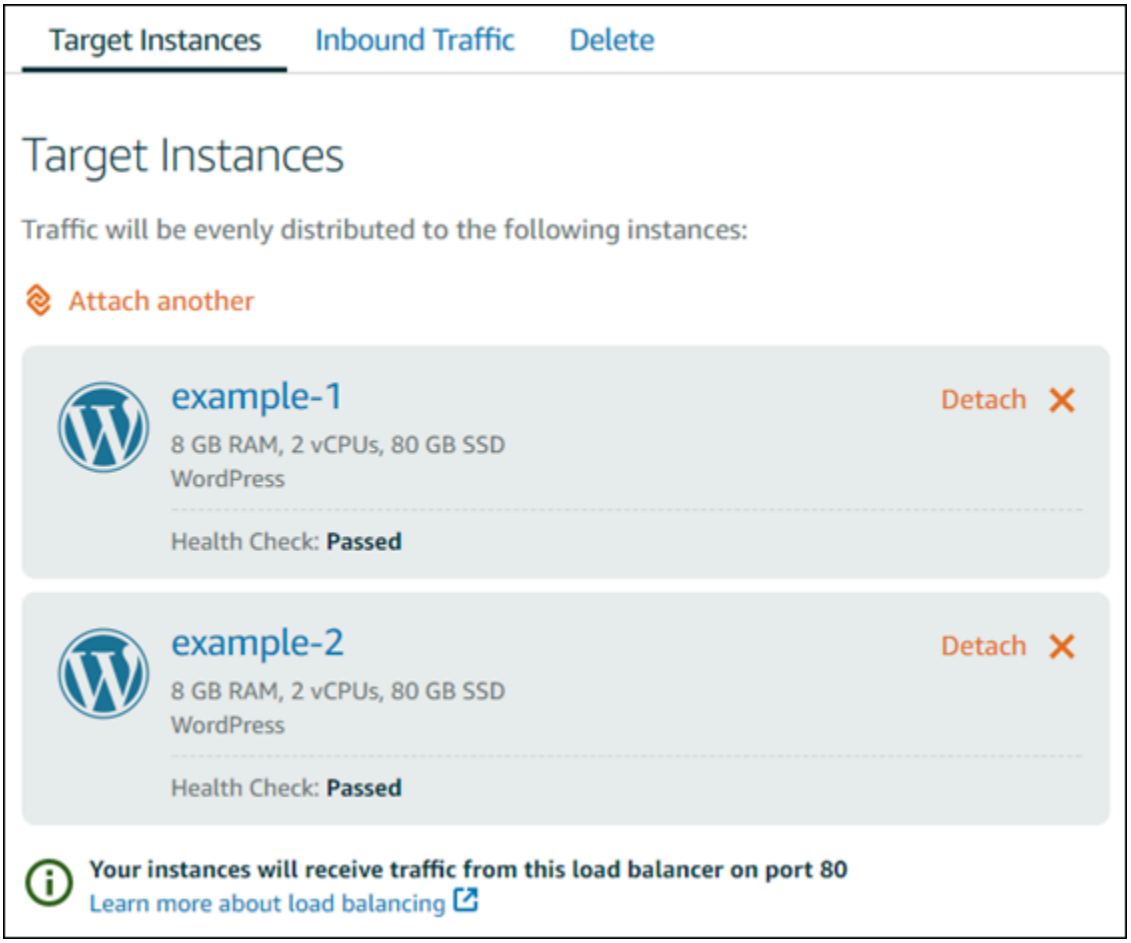
自定义 Lightsail 负载均衡器运行状况检查和 HTTPS 设置

创建 Lightsail 负载均衡器时，需要选择 AWS 区域 和名称。本主题指导您如何更新负载均衡器以启用更多选项。

如果您尚未执行此操作，则需要创建一个负载均衡器。创建负载均衡器

运行状况检查

您要做的第一件事是配置一个实例以进行负载均衡。在完成后，您可以将实例连接到负载均衡器。在连接实例时，将启动运行状况检查过程，并在负载均衡器管理页面上显示通过或失败消息。



您还可以自定义运行状况检查路径。例如，如果您的主页加载缓慢或上面有很多图片，则可以将 Lightsail 配置为查看加载速度更快的其他页面。自定义负载均衡器运行状况检查路径

加密的流量 (HTTPS)

您可以设置 HTTPS，以便为网站用户提供更安全的体验。这是一个包含三个步骤的过程，用于在设置负载均衡器后创建和验证 SSL/TLS 证书。

了解有关 HTTPS 的更多信息

会话持久性

如果在用户的浏览器本地存储会话信息，会话持久性是非常有用的。例如，您可能在 Lightsail 上运行具有购物车的 Magento 电子商务应用程序。如果启用会话持久性，您的用户可以在购物车中添加商品，然后结束会话，在他们返回时，仍会在购物车中找到这些商品。

您还可以调整持久性会话的 Cookie 持续时间。如果要设置特别长或特别短的持续时间，这是非常有用的。有关更多信息，请参阅为负载均衡器启用会话持久性。

配置 Lightsail 实例以实现负载平衡

在将实例附加到 Amazon Lightsail 负载均衡器之前，您需要评估应用程序的配置。例如，在数据层与应用程序的其余部分分开时，负载均衡器通常具有更好的性能。本主题向您介绍每个 Lightsail 实例，并就是否进行负载平衡（或水平扩展）以及如何最好地配置应用程序提出了建议。

一般准则：使用数据库的应用程序

对于使用数据库的 Lightsail 应用程序，我们建议您将数据库实例与应用程序的其余部分分开，这样您就只有一个数据库实例。主要原因是，您希望避免将数据写入到多个数据库中。如果未创建单个数据库实例，数据将写入到用户访问的相应实例上的数据库中。

WordPress

横向扩展？ 是的，适用于 WordPress 博客或网站。

使用 Lightsail 负载均衡器之前的配置建议

- 将您的数据库分开，以便在负载均衡器后面运行的每个 WordPress 实例都能从同一个位置存储和检索信息。如果您需要从数据库中获得更高的性能，您可以独立于 Web 服务器复制或更改处理能力或内存。
- 将您的文件和静态内容卸载到 Lightsail 存储桶。为此，你必须在你的 WordPress 网站上安装 WP Offload Media Lite 插件，并将其配置为连接到你的 Lightsail 存储桶。有关更多信息，请参阅教程：将 WordPress实例连接到存储桶。

Node.js

横向扩展？ 是，但需要注意一些事项。

使用 Lightsail 负载均衡器之前的配置建议

- 在 Lightsail 中，Bitnami 打包的 Node.js 堆栈包含 Node.js、Apache、Redis（内存数据库）和 Python。根据部署的应用程序，您可以在几个服务器之间进行负载均衡。不过，您需要配置负载均衡器以在所有 Web 服务器之间均衡流量，并将 Redis 移到另一个服务器。
- 将 Redis 服务器拆分到另一个服务器，以便与所有实例进行通信。如有必要，请添加一个数据库服务器。
- Redis 的一个主要使用案例是在本地缓存数据，因此，您不必持续访问中央数据库。建议您启用会话持久性以利用 Redis 中提升的性能。有关更多信息，请参阅为负载均衡器启用会话持久性。
- 您还可能具有共享的 Redis 节点，因此，您也可以共享一个节点，或者通过会话持久性使用每个计算机上的本地缓存。
- 如果要使用 Apache 部署负载均衡器，请考虑在 Apache 服务器中包含 `mod_proxy_balancer`。

有关更多信息，请参阅扩展 Node.js 应用程序。

Magento

横向扩展？ 是。

使用 Lightsail 负载均衡器之前的配置建议

- 你可以使用使用其他组件的 Magento AWS 参考部署，例如亚马逊 RDS 数据库：Terraform Magento Adobe Commer ce 开启。 AWS
- 请务必启用会话持久性。Magento 使用购物车；对于在多个会话中进行多次访问的客户，这有助于确保客户在使用新会话返回时在购物车中保留商品。有关更多信息，请参阅为负载均衡器启用会话持久性。

GitLab

横向扩展？ 是，但需要注意一些事项。

使用 Lightsail 负载均衡器之前的配置建议

您必须具备以下各项：

- Redis 节点正在运行并且可以使用
- 共享的网络存储服务器 (NFS)
- 应用程序的集中数据库（MySQL 或 PostgreSQL）。请参阅上面的数据库一般准则。

有关更多信息，请参阅GitLab网站上的高可用性。

> **Note**
>
> 上面提到的共享网络存储服务器 (NFS) 目前在 GitLab 蓝图中不可用。

Drupal

横向扩展？ 是。Drupal 提供了正式文档以说明如何横向扩展应用程序：服务器扩展。

使用 Lightsail 负载均衡器之前的配置建议

您必须设置一个 Drupal 模块以在不同实例之间同步文件。Drupal 网站提供了一些模块，但它们可能更适用于原型而不是生产使用。

使用允许在 Amazon S3 中存储文件的模块。这会提供一个集中位置以存储您的文件，而不是在每个目标实例上保留单独的副本。这样，如果您编辑文件，则会从集中的存储中获取更新并且用户看到相同的文件，而无论他们访问哪个实例。

- Amazon S3 文件系统
- 内容同步

有关更多信息，请参阅 横向扩展以及在云中扩展 Drupal。

LAMP 堆栈

横向扩展？ 是。

使用 Lightsail 负载均衡器之前的配置建议

- 您应该在单独的实例上创建一个数据库。负载均衡器后面的所有实例应指向该单独数据库实例，因此，它们在相同的位置中存储和检索信息。
- 根据您要部署的应用程序，考虑如何共享文件系统（NFS、Lightsail 块存储磁盘或 Amazon S3 存储）。

MEAN 堆栈

横向扩展？ 是。

使用 Lightsail 负载均衡器之前的配置建议

将 MongoDB 移至另一台计算机并配置一种机制以在 Lightsail 实例之间共享根文档。

Redmine

横向扩展？ 是。

使用 Lightsail 负载均衡器之前的配置建议

- 获取 Redmine_S3 插件以在 Amazon S3 上存储附件，而不是在本地文件系统中存储。
- 将数据库拆分到不同的实例中。

Nginx

横向扩展？ 是。

你可以让一个或多个 Lightsail 实例运行 Nginx 并连接到 Lightsail 负载均衡器。有关更多信息，请参阅使用 NGINX 扩展 Web 应用程序，第 1 部分：负载均衡。

Joomla!

横向扩展？ 是，但需要注意一些事项。

使用 Lightsail 负载均衡器之前的配置建议

尽管在 Joomla 网站上没有提供正式的文档，但在社群论坛中具有一些讨论内容。某些用户已成功横向扩展 Joomla 实例，这些实例具有使用以下配置的集群：

- 配置为启用会话持久性的 Lightsail 负载均衡器。有关更多信息，请参阅为负载均衡器启用会话持久性。
- 几个运行 Joomla 的 Lightsail 实例连接到负载均衡器，文档根目录为 Joomla！ 已同步。您可以使用诸如 Rsync 之类的工具来实现此目的，也可以使用 NFS 服务器来同步所有 Lightsail 实例之间的内容，或者使用共享文件。 AWS
- 为一些数据库服务器配置了复制集群。
- 在每个 Lightsail 实例中配置的缓存系统相同。有一些有用的扩展，例如JotCache。

为您的 Lightsail 负载均衡器配置 TLS 安全策略

在 Amazon Lightsail 负载均衡器上启用 HTTPS 后，您可以为加密连接配置 TLS 安全策略。本指南提供有关您可以在 Lightsail 负载均衡器上配置的安全策略以及更新负载均衡器安全策略的过程的信息。有关负载均衡器的更多信息，请参阅负载均衡器。

安全策略概述

Lightsail 负载平衡使用安全套接字层 (SSL) 协商配置（称为安全策略）来协商客户端和负载均衡器之间的 SSL 连接。安全策略是协议和密码的组合。协议在客户端与服务器之间建立安全连接，确保在客户端与负载均衡器之间传递的所有数据都是私密数据。密码是使用加密密钥创建编码消息的加密算法。协议使用多种密码对 Internet 上的数据进行加密。在 连接协商过程中，客户端和负载均衡器会按首选项顺序提供各自支持的密码和协议的列表。默认情况下，会为安全连接选择服务器列表中与任何一个客户端的密码匹配的第一个密码。Lightsail 负载均衡器不支持客户端或目标连接的 SSL 重新协商。

当您在 Lightsail 负载均衡器上启用 HTTPS 时，系统会默认配置`TLS-2016-08`安全策略。如本指南后面所述，您可以根据需要配置不同的安全策略。您可以选择仅用于前端连接的安全策略。`TLS-2016-08` 安全策略始终用于后端连接。Lightsail 负载均衡器不支持自定义安全策略。

支持的安全策略和协议

Lightsail 负载均衡器可以使用以下安全策略和协议进行配置：

Security policies	TLS-2016-08 (default)	TLS-FS-1-2-Res-2019-08
TLS Protocols		
Protocol-TLSv1	✓	
Protocol-TLSv1.1	✓	
Protocol-TLSv1.2	✓	✓
TLS Ciphers		
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓
ECDHE-ECDSA-AES128-SHA	✓	
ECDHE-RSA-AES128-SHA	✓	
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓
ECDHE-RSA-AES256-SHA	✓	
ECDHE-ECDSA-AES256-SHA	✓	
AES128-GCM-SHA256	✓	
AES128-SHA256	✓	
AES128-SHA	✓	

完成先决条件

满足以下先决条件（如果尚未满足）：

- 创建负载均衡器并向其附加实例。有关更多信息，请参阅创建负载均衡器并向其附加实例。
- 创建 SSL/TLS 证书，然后将它连接到您的负载均衡器以启用 HTTPS。有关更多信息，请参阅为 Lightsail 负载均衡器创建 SSL/TLS 证书。有关证书的更多信息，请参阅 SSL/TLS 证书。

使用 Lightsail 控制台配置安全策略

完成以下过程，使用 Lightsail 控制台配置安全策略。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其配置 TLS 安全策略的负载均衡器的名称。
4. 选择 Inbound traffic（入站流量）选项卡。
5. 在页面的 TLS 安全协议部分下选择更改协议。
6. 在支持的协议下拉菜单中选择以下选项之一：
   - TLS 1.2 版：此选项最为安全，但较旧的浏览器可能无法连接。
   - TLS 1.0、1.1 和 1.2 版：此选项提供与浏览器的最大兼容性。
7. 选择保存将所选协议应用于您的负载均衡器。

   您的更改需要一些时间才能生效。

使用配置安全策略 AWS CLI

使用 AWS Command Line Interface（AWS CLI）完成以下过程以配置安全策略。使用 `update-load-balancer-attribute` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》update-load-balancer-attribute中的。

> **Note**
>
> 在继续执行此过程之前，必须为 Lightsail 安装 AWS CLI 并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以更改负载均衡器的 TLS 安全策略。

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name TlsPolicyName --attribute-value AttributeValue
```

在该命令中，将以下示例文本替换为自己的文本：

- *LoadBalancerName*使用您要为其更改 TLS 安全策略的负载均衡器的名称。
- *AttributeValue*使用TLS-2016-08或TLS-FS-1-2-Res-2019-08安全策略。

> **Note**
>
> 命令中的 TlsPolicyName 属性指定您希望编辑在负载均衡器上配置的 TLS 安全策略。

示例：

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer --
attribute-name TlsPolicyName --attribute-value TLS-2016-08
```

您的更改需要一些时间才能生效。

Lightsail 负载均衡器的 HTTP 重定向到 HTTPS

在 Amazon Lightsail 负载均衡器上配置 HTTPS 后，您可以配置 HTTP 到 HTTPS 的重定向，以便使用 HTTP 连接浏览您的网站或网络应用程序的用户自动重定向到加密的 HTTPS 连接。有关负载均衡器的更多信息，请参阅负载均衡器。

完成先决条件

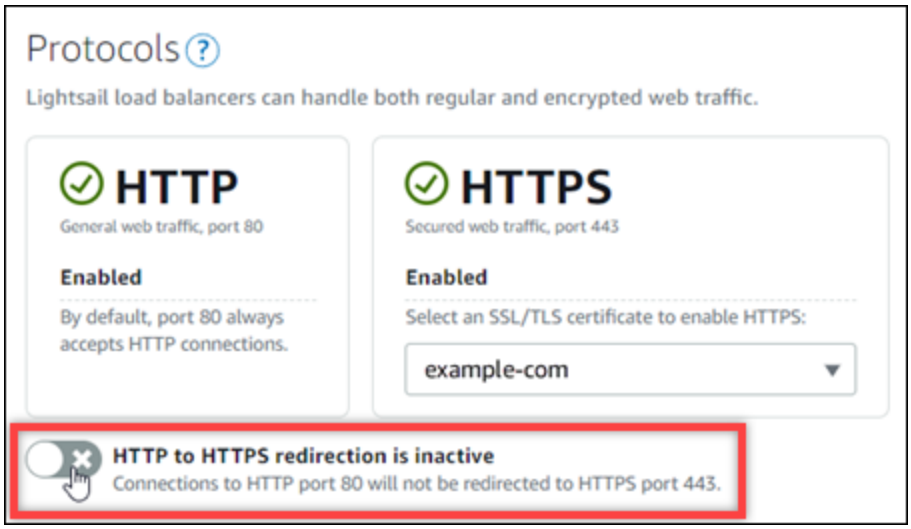
满足以下先决条件（如果尚未满足）：

- 创建负载均衡器并向其附加实例。有关更多信息，请参阅创建负载均衡器并向其附加实例。
- 创建 SSL/TLS 证书，然后将它连接到您的负载均衡器以启用 HTTPS。有关更多信息，请参阅为 Lightsail 负载均衡器创建 SSL/TLS 证书。有关证书的更多信息，请参阅 SSL/TLS 证书。

使用 Lightsail 控制台在您的负载均衡器上配置 HTTPS 重定向

完成以下过程，使用 Lightsail 控制台在您的负载均衡器上配置 HTTPS 重定向。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其配置 HTTPS 重新导向的负载均衡器的名称。
4. 选择 Inbound traffic（入站流量）选项卡。
5. 在页面的协议部分，您可以执行以下操作之一：



   - 将方向选项切换为激活以启用 HTTP 到 HTTPS 重新导向。
   - 将方向选项切换为停用以禁用 HTTP 到 HTTPS 重新导向。

   您的更改需要一些时间才能生效。

使用以下命令为负载均衡器配置 HTTP 到 HTTPS 重定向 AWS CLI

完成以下过程，使用 AWS Command Line Interface (AWS CLI) 在您的负载均衡器上配置 HTTPS 重定向。使用 `update-load-balancer-attribute` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》update-load-balancer-attribute中的。

> **Note**
>
> 在继续执行此过程之前，必须为 Lightsail 安装 AWS CLI 并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以在负载均衡器上配置 HTTPS 重新导向。

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name HttpsRedirectionEnabled --attribute-value AttributeValue
```

在该命令中，将以下示例文本替换为自己的文本：

- *LoadBalancerName*使用您要为其激活或停用 HTTP 到 HTTPS 重定向的负载均衡器的名称。
- *AttributeValue*使用`true`来激活重定向，或者停用重`false`定向。

> **Note**
>
> 命令中的 HttpsRedirectionEnabled 属性指定您希望编辑是否为指定的负载均衡器启用或禁用 HTTPS 重新导向。

示例：

- 要在负载均衡器上激活 HTTP 到 HTTPS 重新导向：

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
 --attribute-name HttpsRedirectionEnabled --attribute-value true
```

- 要在负载均衡器上停用 HTTP 到 HTTPS 重新导向：

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
 --attribute-name HttpsRedirectionEnabled --attribute-value false
```

您的更改需要一些时间才能生效。

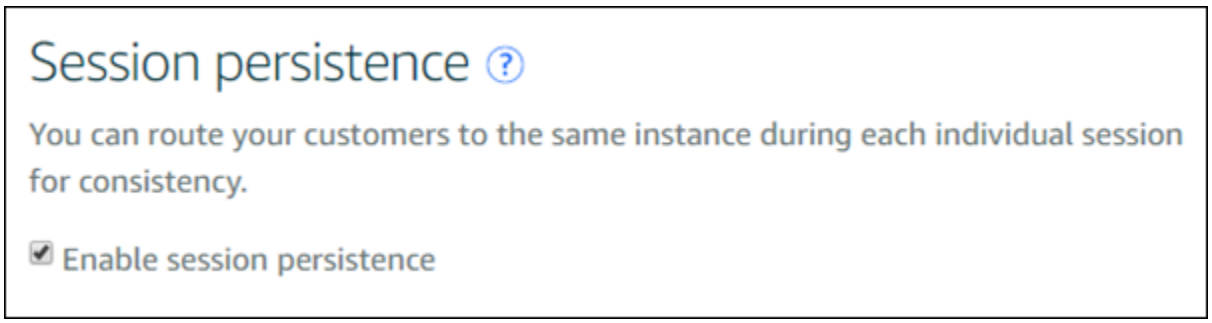
为 Lightsail 负载均衡器启用会话保持

您可以为用户启用会话持久性。如果在用户的浏览器本地存储会话信息，这是非常有用的。例如，您可能正在亚马逊 Lightsail 上运行带有购物车的 Magento 电子商务应用程序。如果启用会话持久性，您的用户可以在购物车中添加商品，然后离开该网站，在他们返回时，仍会在购物车中找到这些商品。

你也可以使用 AWS Command Line Interface (AWS CLI) 或 Lightsail API 来调整 cookie 的持续时间。

启用会话持久性

1. 在左侧导航窗格中，选择联网。
2. 选择您的负载均衡器以对其进行管理。
3. 选择 Inbound traffic（入站流量）选项卡。
4. 选择 Enable session persistence（启用会话持久性）。



调整 Cookie 持续时间

您还可以调整持久性会话的 Cookie 持续时间。如果要设置特别长或特别短的持续时间，这是非常有用的。例如，对于很多电子商务网站，持续时间是相当长的。这样，在客户离开并返回时，购物车中的商品不会丢失。

如果您还没有这样做，请对其进行设置 AWS CLI 和配置。

配置为与 Amazon Lightsail 配合使用 AWS Command Line Interface

1. 打开命令提示符或终端窗口。
2. 键入以下 AWS CLI 命令将 Cookie 持续时间增加到三天（259,200 秒）。

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name SessionStickiness_LB_CookieDurationSeconds --attribute-value
 259200
```

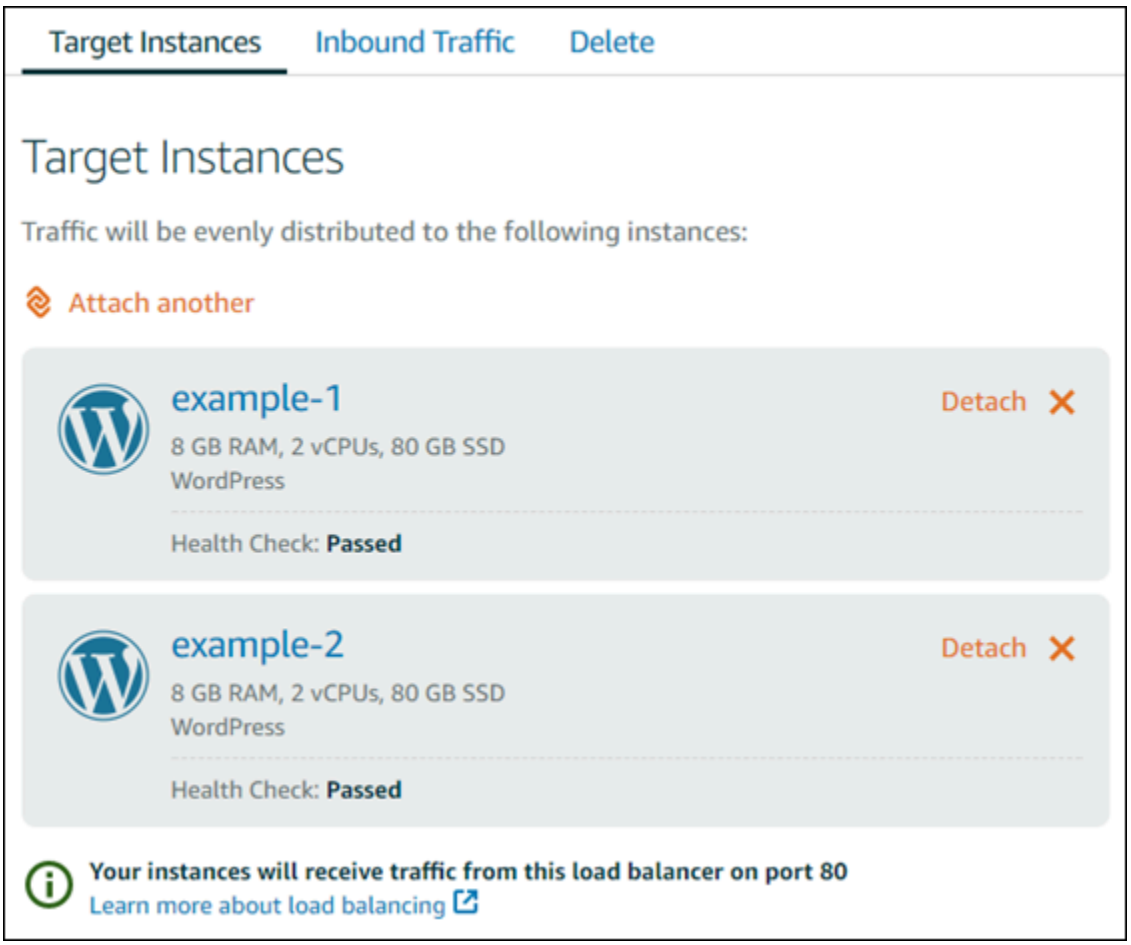
在命令中，*LoadBalancerName*替换为负载均衡器的名称。

如果成功，将会看到以下响应。

```
{
    "operations": [
        {
            "status": "Succeeded",
            "resourceType": "LoadBalancer",
            "isTerminal": true,
            "operationDetails": "SessionStickiness_LB_CookieDurationSeconds",
            "statusChangedAt": 1511758936.174,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "operationType": "UpdateLoadBalancerAttribute",
            "resourceName": "example-load-balancer",
            "id": "681c2bd9-9a51-402b-8ad2-12345EXAMPLE",
            "createdAt": 1511758936.174
        }
    ]
}
```

为 Lightsail 负载均衡器配置运行状况检查设置

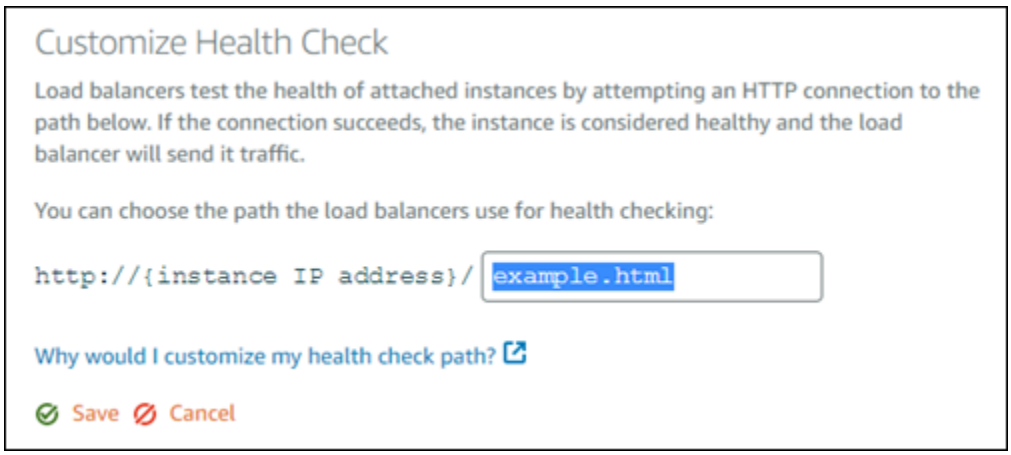
健康检查将在您的 Lightsail 实例连接到负载均衡器后立即开始，此后每 30 秒进行一次。您可以在负载均衡器管理页面上查看运行状况检查状态。



自定义运行状况检查路径

您可能希望自定义您的运行状况检查路径。例如，如果您的主页加载缓慢或上面有很多图片，则可以将 Lightsail 配置为查看加载速度更快的其他页面。

1. 在左侧导航窗格中，选择联网。
2. 选择您的负载均衡器以对其进行管理。
3. 在 Target instances（目标实例）选项卡上，选择 Customize health checking（自定义运行状况检查）。
4. 键入有效的运行状况检查路径，然后选择 Save（保存）。



运行状况检查指标

以下指标可以帮助您诊断运行状况检查问题。使用 AWS Command Line Interface 或 Lightsail API 返回有关特定运行状况检查指标的信息。

- **ClientTLSNegotiationErrorCount** - 由未与负载均衡器建立会话的客户端启动的 TLS 连接数。可能的原因包括密码或协议不匹配。

  Statistics：最有用的统计工具是 Sum。
- **HealthyHostCount** - 被视为正常运行的目标实例数。

  Statistics：最有用的统计数据是 Average、Minimum 和 Maximum。
- **UnhealthyHostCount** - 被视为未正常运行的目标实例数。

  Statistics：最有用的统计数据是 Average、Minimum 和 Maximum。
- **HTTPCode_LB_4XX_Count** - 源自负载均衡器的 HTTP 4XX 客户端错误代码数。如果请求格式错误或不完整，则会生成客户端错误。目标实例尚未收到这些请求。该计数不包含目标实例生成的任何响应代码。

  Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均返回 1。
- **HTTPCode_LB_5XX_Count** - 源自负载均衡器的 HTTP 5XX 服务器错误代码数。该计数不包含目标实例生成的任何响应代码。

  Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均返回 1。请注意，Minimum、Maximum 和 Average 均返回 1。

- **HTTPCode_Instance_2XX_Count** - 由目标实例生成的 HTTP 响应代码数。它不包括负载均衡器生成的任何响应代码。

  Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均返回 1。
- **HTTPCode_Instance_3XX_Count** - 由目标实例生成的 HTTP 响应代码数。它不包括负载均衡器生成的任何响应代码。

  Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均返回 1。
- **HTTPCode_Instance_4XX_Count** - 由目标实例生成的 HTTP 响应代码数。它不包括负载均衡器生成的任何响应代码。

  Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均返回 1。
- **HTTPCode_Instance_5XX_Count** - 由目标实例生成的 HTTP 响应代码数。它不包括负载均衡器生成的任何响应代码。

  Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均返回 1。
- **InstanceResponseTime** - 从请求离开负载均衡器到从目标实例收到响应之间所用的时间（以秒为单位）。

  Statistics：最有用的统计工具是 Average。
- **RejectedConnectionCount** - 由于负载均衡器已达到最大连接数而拒绝的连接数。

  Statistics：最有用的统计工具是 Sum。
- **RequestCount**-已处理的请求数 IPv4。该计数仅包含具有负载均衡器的目标实例生成的响应的请求。

  Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均返回 1。

主题

- 配置 Lightsail 负载均衡器运行状况检查

配置 Lightsail 负载均衡器运行状况检查

默认情况下，Lightsail 会在您的 Web 应用程序根目录 ("/") 中对您的实例执行运行状况检查。运行状况检查用于监控注册的实例的运行状况，以便负载均衡器仅将请求发送到正常运行的实例。在将实例连接到您的负载均衡器时，将会立即启动运行状况检查。

将返回以下状态之一。

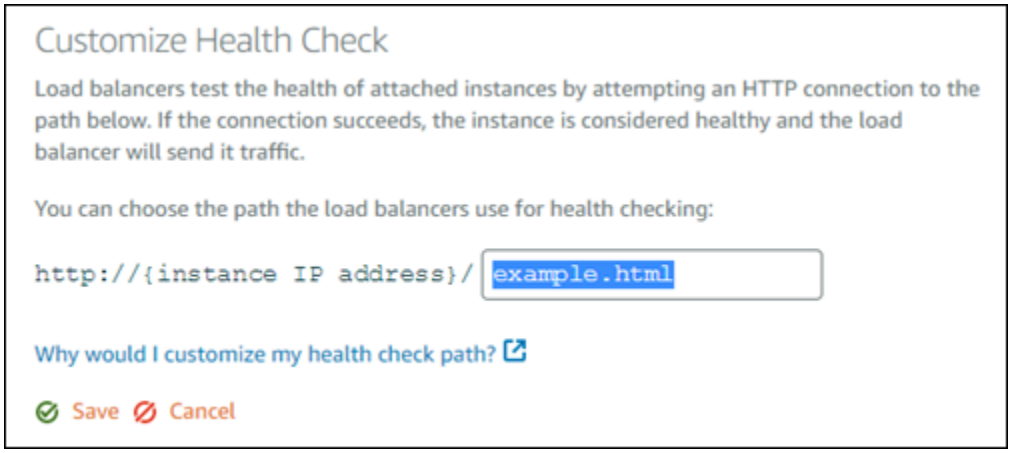
- 通过
- 失败

如果你的运行状况检查失败，你可以尝试使用 AWS Command Line Interface 或 Lightsail API 来找出问题所在。请参阅我们的故障排除指南以了解更多信息。

自定义运行状况检查路径

您可能希望自定义您的运行状况检查路径。例如，如果您的主页加载缓慢或上面有很多图片，则可以将 Lightsail 配置为查看加载速度更快的其他页面。

1. 在左侧导航窗格中，选择联网。
2. 选择您的负载均衡器以对其进行管理。
3. 在 Target instances（目标实例）选项卡上，选择 Customize health checking（自定义运行状况检查）。
4. 键入有效的运行状况检查路径，然后选择 Save（保存）。



将实例与 Lightsail 负载均衡器分离

如果您不想再将实例连接到您的 Amazon Lightsail 负载均衡器，则可以将其分离。当您将 Lightsail 实例与负载均衡器断开连接时，我们会等到不再需要指定的实例后再进行分离。

1. 在左侧导航窗格中，选择联网。
2. 选择要管理的负载均衡器。

3. 在 Target instances (目标实例) 选项卡上，选择要与之断开连接的负载均衡器旁边的 Detach (断开连接)。

删除 Lightsail 负载均衡器

如果您不再需要 Lightsail 负载均衡器，则可以将其删除。删除负载均衡器还会分离与其连接的任何 Lightsail 实例，但不会删除 Lightsail 实例。如果您使用与负载均衡器关联的SSL/TLS certificate, deleting the load balancer will also permanently delete any SSL/TLS证书启用了加密 (HTTPS) 流量。

> **Important**
>
> 删除 Lightsail 负载均衡器及其关联证书是最终决定，无法撤消。

1. 在左侧导航窗格中，选择联网。
2. 选择要删除的负载均衡器。
3. 选择删除。
4. 选择 Delete load balancer (删除负载均衡器)。
5. 选择是，删除。

使用 Lightsail 内容交付分发版在全球范围内提供网络内容

Lightsail 发行版使用全球分布的服务器网络（也称为边缘站点）来更快地向用户交付内容。要使用发行版，您需要先在 Lightsail 实例或容器服务，或者在 Lightsail 负载均衡器上创建和托管您的网站或 Web 应用程序，或者在 Lightsail 负载均衡器上创建和托管您的静态内容，或者将您的静态内容存储在 Lightsail 存储桶上。然后，您可以创建并配置 Lightsail 发行版，以从您的实例、容器服务、负载均衡器或存储桶中提取、缓存和提供内容。您的实例、容器服务、负载均衡器或存储桶（也称为分配的源），是您内容的确定来源。

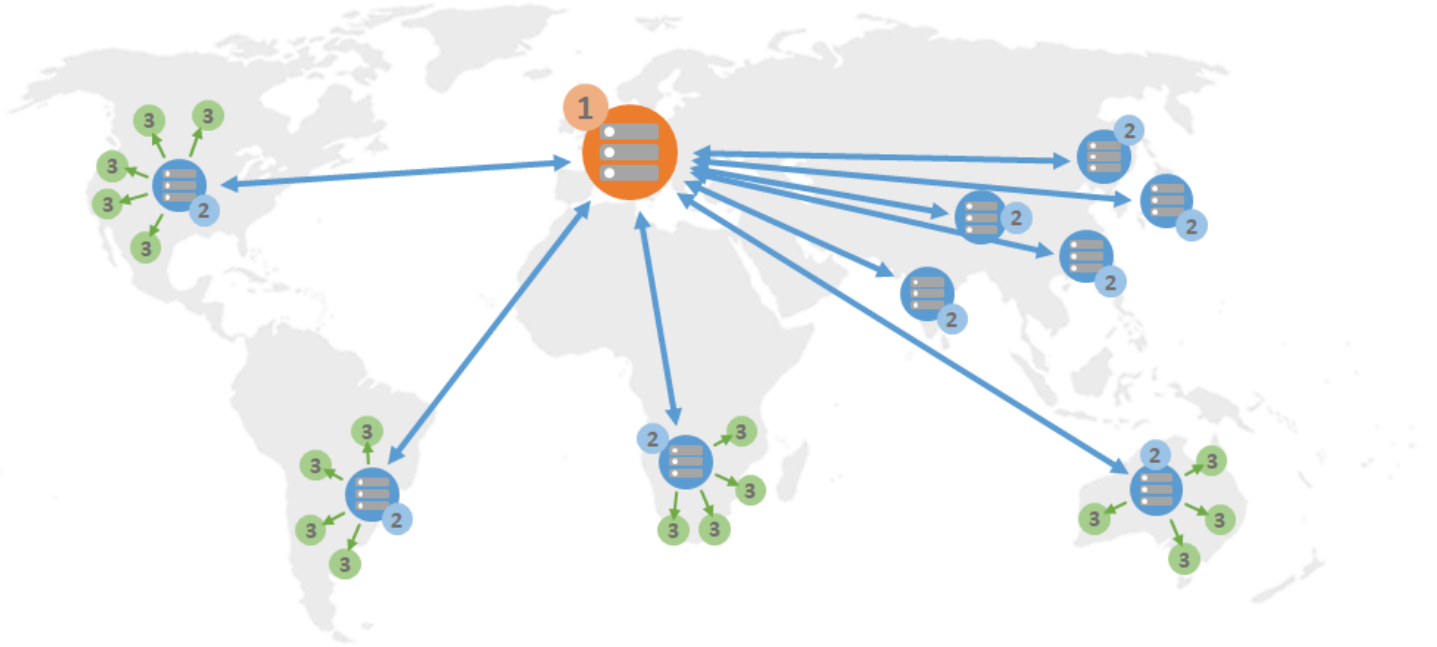
当您的用户通过访问网站请求内容（通过分配提供内容）时，考虑到延迟，会将请求路由到最近的站点。然后您的分配将执行以下操作之一：

- 如果内容已经在边缘站点中缓存，则分配将立即将其提供给您的用户。
- 如果内容尚未缓存在该边缘站点中，则分配将从指定的源检索并缓存内容，然后将其提供给您的用户。

您的内容会在您为分配指定的缓存寿命（存活时间）内缓存在边缘站点中，以便立即满足同一站点的其他请求。当缓存内容达到缓存寿命时，将从边缘站点中将其清除。下次将内容请求路由到边缘站点时，分配会检索、缓存和提供内容。

在下图中：

- 1 表示您的分发来源，例如托管您的网站的 Lightsail 实例或容器服务、附有实例的负载均衡器或托管静态内容的存储桶。
- 2 表示从源提取、缓存和提供内容的分配或边缘站点。
- 3 表示从边缘站点获得内容的用户。

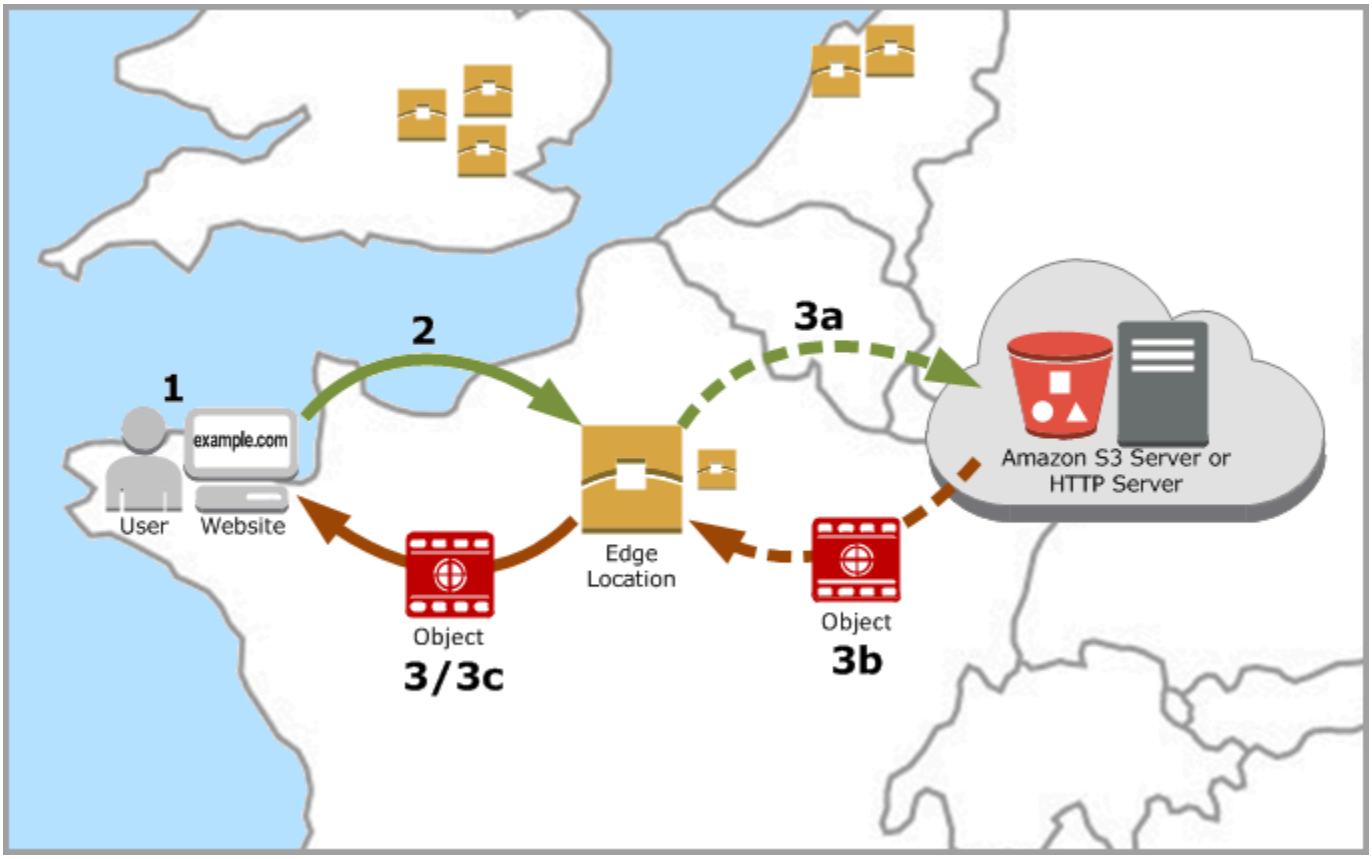


> **Note**
>
> 此图仅用于说明目的，不显示实际的边缘站点。有关边缘站点的更多信息，请参阅本指南下文中的边缘站点和 IP 地址范围。

例如，如果您的网站托管在法国，而来自法国其他地区的人想要查看您的内容，则页面将在几毫秒内加载。

当您的访客不在附近时，事情会变得有点困难。

如果来自澳大利亚的人想要查看您的内容，则浏览器必须从位于法国的服务器上获取内容，然后将其展示给数千英里以外的用户。如果来自不同国家/地区的用户同时请求相同的内容，则服务器会被请求堵塞，并且加载和提供内容需要的时间较长。这会影响最终用户的内容加载速度。



CDN 通过在边缘站点缓存您的网站内容来解决这种情况。与从一个中心资源提供内容的传统方法相比，这种提供内容的方法更快、更高效。当查看者在您的网站上或通过您的应用程序发出请求时，DNS 会将请求路由到最能满足用户请求的位置。用户从附近的站点访问您的内容，而不是所有用户都访问可能很远的同一个中心资源。

使用案例

提供快速、安全的网站

Lightsail 分发可加快向全球观众交付内容（例如网站页面、图片 JavaScript、样式表等）的速度。通过使用分配，您可以充分利用 AWS 骨干网络和边缘服务器，以便在查看器访问您的网站时为其提供快速、安全且可靠的体验。

提高您网站的安全性

利用 TLS 终止来增强您的网站并提高其性能，这样可将加密处理分载到您的分配，从而减少源的负载。您可以将注册的域名与 Lightsail SSL/TLS 证书一起使用，为您的分发启用安全超文本传输协议 (HTTPS)。您的用户将建立与分配的加密 HTTPS 连接，同时您的分配使用 HTTP 从源提取内容。

应用程序优化

针对各种应用程序（包括 WordPress 静态网站）轻松优化您的发行版。使用分配缓存和提供您的内容也会减少源的负载，因为大多数请求都由您的分配提供，而不是由您的实例、容器服务、负载均衡器或存储桶提供。

配置您的分配

以下是使用 Lightsail 实例和发行版为您的网站或 Web 应用程序提供服务时需要遵循的一般步骤。

1. 根据您是在分配中使用实例、容器服务还是存储桶，完成以下其中一项操作。
   - 创建一个 Lightsail 实例来托管你的内容。实例将用作分配的源。源存储内容的原始最终版本。有关更多信息，请参阅创建实例。

     将 Lightsail 静态 IP 附加到您的实例。如果您停止并启动实例，则实例的默认公有 IP 地址会发生变化，这将中断您的分配与源实例之间的连接。如果您停止和启动实例，静态 IP 不会更改。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

     将您的内容和文件上传到实例。您的文件也称为对象，通常包括网页、图像和媒体文件，但可以是可通过 HTTP 提供的任何内容。
   - 创建 Lightsail 容器服务来托管您的网站或 Web 应用程序。容器服务将用作分配的源。源存储内容的原始最终版本。有关更多信息，请参阅创建 Amazon Lightsail 容器服务。
   - 创建一个 Lightsail 存储桶来存储你的静态内容。存储桶将用作分配的源。源存储内容的原始最终版本。有关更多信息，请参阅创建存储桶。

     使用 Lightsail 控制台 AWS Command Line Interface（AWS CLI）和，将文件上传到您的存储桶。 AWS APIs有关上传文件的更多信息，请参阅将文件上传到存储桶。
2. （可选）如果您的网站托管在实例上需要容错，请创建 Lightsail 负载均衡器。将实例的多个副本附加到负载均衡器。您可以将负载均衡器（附加了一个或多个实例）配置为分配的源，而不是将实例配置为源。有关更多信息，请参阅创建负载均衡器并向其附加实例。
3. 创建 Lightsail 发行版，并将您的实例、容器服务、负载均衡器或存储桶配置为源。同时，您可以指定详细信息，例如内容的缓存寿命和缓存网站或 Web 应用程序的哪些元素。有关更多信息，请参阅创建分配。
4. （可选）如果您的分配源是 WordPress 实例，则必须编辑实例中的 WordPress 配置文件以使您的 WordPress 网站与您的分配配合使用。有关更多信息，请参阅配置您的 WordPress实例以与您的分配配合使用。

5. （可选）在 Lightsail 控制台中创建 Lightsail DNS 区域来管理你的域名的 DNS。这使您可以轻松地将您的域名映射到您的 Lightsail 资源。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。或者，您也可以继续在当前托管的位置托管域的 DNS。
6. 为您的域名创建 Lightsail SSL/TLS 证书，以便将其用于您的发行版。Lightsail 发行版需要 HTTPS，因此您必须先为您的域名申请 SSL/TLS 证书，然后才能将其用于您的发行版。有关更多信息，请参阅创建分配的 SSL/TLS 证书。
7. 为您的分配启用自定义域，以便将注册的域名用于您的分配。启用自定义域名需要您指定为域名创建的 Lightsail SSL/TLS 证书。这会将您的域添加到分配中并启用 HTTPS。有关更多信息，请参阅启用分配的自定义域。
8. 将别名记录添加到域的 DNS 以开始将域的流量路由到您的分配。添加别名记录后，将通过您的分配对访问域的用户进行路由。有关更多信息，请参阅将域指向分配。
9. 测试您的分配是否在缓存内容。有关更多信息，请参阅测试分配。

边缘站点和 IP 地址范围

Lightsail 发行版使用与亚马逊相同的边缘服务器和 IP 地址范围。 CloudFront有关 CloudFront 边缘服务器位置的列表，请参阅 Amazon CloudFront 产品详情页面。有关 CloudFront IP 范围的列表，请参阅CloudFront 全局 IP 列表。

创建 Lightsail 内容分发网络发行版

在本指南中，我们将向您展示如何使用 Lightsail 控制台创建 Amazon Lightsail 发行版，并描述了您可以配置的分发设置。有关分配的更多信息，请参阅内容分发网络分配。

内容

- 先决条件
- 源资源
- 源协议策略
- 缓存行为和缓存预设
- 最适合 WordPress 缓存预设
- 默认行为
- 目录和文件覆盖
- 高级缓存设置
- 分配计划

- 创建分配
- 后续步骤

先决条件

在开始创建分配之前，请满足以下先决条件：

1. 根据您是在分配中使用实例、容器服务还是存储桶，完成以下其中一项操作。
   - 创建一个 Lightsail 实例来托管你的内容。实例将用作分配的源。源存储内容的原始最终版本。有关更多信息，请参阅创建实例。

     将 Lightsail 静态 IP 附加到您的实例。如果您停止并启动实例，则实例的默认公有 IP 地址会发生变化，这将中断您的分配与源实例之间的连接。如果您停止和启动实例，静态 IP 不会更改。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

     将您的内容和文件上传到实例。您的文件也称为对象，通常包括网页、图像和媒体文件，但可以是可通过 HTTP 提供的任何内容。
   - 创建 Lightsail 容器服务来托管您的网站或 Web 应用程序。容器服务将用作分配的源。源存储内容的原始最终版本。有关更多信息，请参阅创建 Amazon Lightsail 容器服务。
   - 创建一个 Lightsail 存储桶来存储你的静态内容。存储桶将用作分配的源。源存储内容的原始最终版本。有关更多信息，请参阅创建存储桶。

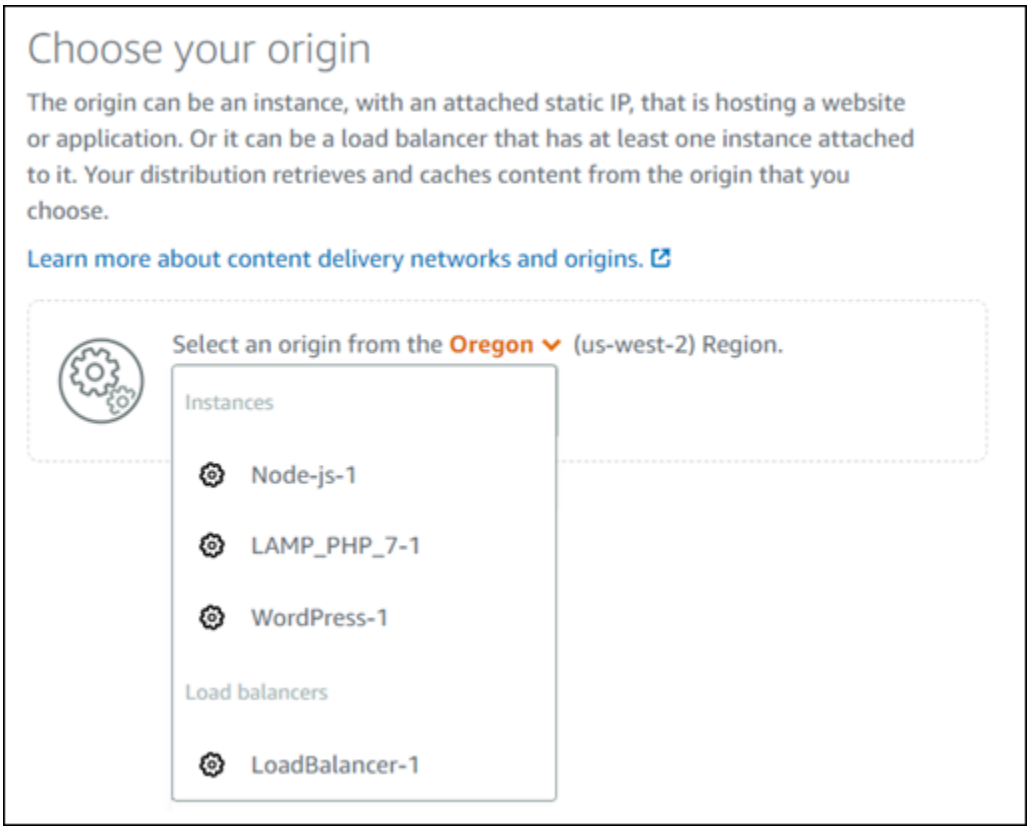
     使用 Lightsail 控制台 AWS Command Line Interface （AWS CLI）和，将文件上传到您的存储桶。 AWS APIs有关上传文件的更多信息，请参阅将文件上传到存储桶。
2. （可选）如果您的网站需要容错，请创建 Lightsail 负载均衡器。将实例的多个副本附加到负载均衡器。您可以将负载均衡器（附加了一个或多个实例）配置为分配的源，而不是将实例配置为源。有关更多信息，请参阅创建负载均衡器并向其附加实例。

源资源

源是分配内容的确定来源。创建分配时，您可以选择托管您的网站或 Web 应用程序内容的 Lightsail 实例、容器服务、存储桶或负载均衡器（附加了一个或多个实例）。

> **Note**
>
> IPv6目前无法将仅限于-的实例配置为 Lightsail 内容分发网络 (CDN) 分发的来源。

每个分配只能选择一个源。您可以在创建分配后随时更改源。有关更多信息，请参阅更改分配的源。



源协议策略

源协议策略是在从源中提取内容时分配使用的协议策略。选择分配的源之后，您应确定在从源中提取内容时分配是使用超文本传输协议 (HTTP) 还是安全超文本传输协议 (HTTPS)。如果源没有进行 HTTPS 配置，则必须使用 HTTP。

您可以为分配选择以下源协议策略之一：

- 仅 HTTP - 分配仅使用 HTTP 访问源。这是默认设置。
- 仅 HTTPS - 分配仅使用 HTTPS 访问源。

编辑源协议策略的步骤包含在本指南的以下更改分配的源部分。

> **Note**
>
> 当您选择 Lightsail 存储桶作为分配的来源时，Ori gin 协议策略默认为仅 HTTPS。当存储桶是分配的源时，您无法更改源协议策略。

缓存行为和缓存预设

缓存预设为在源上托管的内容类型自动配置分配设置。例如，选择最适合静态内容预设会自动将分配配置为最适合静态网站的设置。如果您的网站托管在 WordPress 实例上，请选择 “最适合 WordPress预设”，将您的发行版自动配置为与您的 WordPress 网站配合使用。

> **Note**
>
> 当您选择 Lightsail 存储分区作为分发源时，缓存预设选项不可用。我们会自动应用最适合存储桶中存储的静态内容的分配设置。

您可以为分配选择以下缓存预设之一：

- 最适合静态内容 - 此预设将分配配置为缓存所有内容。如果您在源上托管静态内容（例如静态 HTML 页面），或者对于每个访问网站的用户来说内容不会更改，则非常适合使用此预设。选择此预设后，将缓存分配的所有内容。
- 最适合动态内容 - 此预设将分配配置为除了在创建分配页面的目录和文件覆盖部分指定为缓存的文件，将不缓存任何内容。有关更多信息，请参阅本指南下文中的目录和文件覆盖。如果您在源上托管动态内容，或者每个访问网站或 Web 应用程序的用户可以更改内容，则非常适合使用此预设。
- 最适 WordPress合-此预设将您的发行版配置为只缓存 WordPress实例`wp-includes/`和`wp-content/`目录中的文件。如果您的来源是使用 Certified by Bitnami 和 Automattic 蓝图（不包括多站点蓝图）的实例，则此预设非常理想。WordPress 有关此预设的更多信息，请参阅最适合 WordPress 缓存预设。

  > **Note**
  >
  > 无法选择自定义设置预设。如果您选择了预设，但随后手动修改分配的设置，则系统会自动为您选择该预设。

只能在 Lightsail 控制台中指定缓存预设。无法使用 Lightsail API 和进行指定。 AWS CLI SDKs

最适合 WordPress 缓存预设

当你选择一个使用 Certified by Bitnami 和 Automattic 蓝图作为发行版来源的实例时，Lightsail 会询问你是否要将最适合 WordPress缓存的预设应用于你的分发。WordPress 如果您应用现在，则您的发行版将自动配置为最适合您的 WordPress 网站。没有其他需要应用的分配设置。最适合 WordPress 预设

为除了 WordPress网站`wp-includes/`和`wp-content/`目录中的文件之外什么都不缓存。它还会将您的分配配置为每天清除缓存（缓存寿命为 1 天）、允许所有的 HTTP 方法、仅转发 `Host` 标头、不转发 Cookie 以及转发所有查询字符串。

> **Important**
>
> 您必须编辑实例中的 WordPress 配置文件才能使您的 WordPress网站与您的发行版配合使用。有关更多信息，请参阅配置您的 WordPress实例以与您的分配配合使用。

默认行为

默认行为指定分配如何处理内容缓存。系统会根据您选择的缓存预设，自动为您指定分配的默认行为。如果选择不同的默认行为，缓存预设会自动更改为自定义设置。

> **Note**
>
> 当您选择 Lightsail 存储分区作为分发来源时，默认行为选项不可用。我们会自动应用最适合存储桶中存储的静态内容的分配设置。

您可以为分配选择以下默认行为之一：

- 缓存所有内容 - 此行为将您的分配配置为缓存并将您的整个网站作为静态内容提供服务。如果源托管的内容不会因查看者而变化，或者您的网站没有使用 Cookie、标头或查询字符串来个性化内容，则非常适合使用此选项。
- 不缓存任何内容 - 此行为将您的分配配置为仅缓存源文件和您指定的文件夹路径。如果您的网站或 Web 应用程序使用 Cookie、标题和查询字符串为单个用户个性化内容，则非常适合使用此选项。如果选择此选项，您必须指定要缓存的目录和文件路径覆盖。

目录和文件覆盖

目录和文件覆盖可用于覆盖您选择的默认行为或添加例外。例如，如果您选择缓存所有内容，可通过覆盖指定分配不应缓存的目录、文件或文件类型。或者，如果您选择不缓存任何内容，可通过覆盖指定分配应缓存的目录、文件或文件类型。

在页面的目录和文件覆盖部分，您可以指定要缓存或不缓存的目录或文件的路径。使用星号可指定通配符目录 (`path/to/assets/*`) 和文件类型（`*.html`、`*jpg`、`*js`）。目录和文件路径区分大小写。

> **Note**
>
> 当您选择 Lightsail 存储桶作为分发源时，目录和文件覆盖选项不可用。将缓存存储在选定存储桶中的所有内容。

这些只是如何指定目录和文件覆盖的几个示例：

- 指定以下内容以缓存在 Lightsail 实例上运行的 Apache Web 服务器的文档根目录中的所有文件。

```
var/www/html/
```

- 指定以下设置以仅缓存 Apache Web 服务器文档根目录中的索引页面。

```
var/www/html/index.html
```

- 指定以下设置以仅缓存 Apache Web 服务器文档根目录中的 .html 文件。

```
var/www/html/*.html
```

- 指定以下设置以仅缓存 Apache Web 服务器文档根目录的镜像子目录中的 .jpg、.png 和 .gif 文件。

```
var/www/html/images/*.jpg
```

```
var/www/html/images/*.png
```

```
var/www/html/images/*.gif
```

  指定以下设置以缓存 Apache Web 服务器文档根目录的镜像子目录中的所有文件。

```
var/www/html/images/
```

高级缓存设置

高级设置可用于指定分配中内容的缓存寿命、允许的 HTTP 方法、HTTP 标头转发、Cookie 转发和查询字符串转发。指定的高级设置仅应用于分发缓存的目录和文件，包括指定为缓存的目录和文件覆盖。

> **Note**
>
> 当您选择 Lightsail 存储分区作为分配来源时，创建分发页面上的高级缓存设置不可用。我们会自动应用最适合存储桶中存储的静态内容的分配设置。但是，创建分配后您可以在分配管理页面中修改高级缓存设置。

您可以配置以下高级设置：

缓存寿命 (TTL)

控制在分配将另一个请求转发到源以确定内容是否已更新之前，内容在分配缓存中保留的时间。默认值为一天。减少此持续时间可以更好地提供动态内容。增加此持续时间意味着您的用户将获得更好的性能，因为更有可能从边缘站点直接提供文件。增加此持续时间还会降低源的负载，因为分配提取内容的频率更低。

> **Note**
>
> 仅当来源没有向内容添加 HTTP 标头（如 `Cache-Control max-age`、`Cache-Control s-maxage` 和 `Expires`）时才应用指定的缓存寿命值。

允许的 HTTP 方法

控制您的分配处理和转发到源的 HTTP 方法。HTTP 方法指示需要在源上执行的操作。例如，GET 方法从源检索数据，PUT 方法请求将所包含的实体存储在源上。

您可以为分配选择以下 HTTP 方法选项之一：

- 允许 GET、HEAD、OPTIONS、PUT、POST、PATCH 和 DELETE 方法
- 允许 GET、HEAD 和 OPTIONS 方法
- 允许 GET 和 HEAD 方法

分配会始终缓存对 GET 和 HEAD 请求的响应。如果您选择允许这些请求，则您的分配还会缓存对 OPTIONS 请求的响应。分配不会缓存对任何其他 HTTP 方法的响应。有关更多信息，请参阅 HTTPS 方法。

> **Important**
>
> 如果您将分配配置为允许支持的所有 HTTP 方法，则必须将源实例配置为处理所有方法。例如，如果由于要使用 POST 而将分配配置为允许这些方法，则必须配置源服务器以相应地处理 DELETE 请求，以便查看器无法删除您不希望删除的资源。有关更多信息，请搜索网站或 Web 应用程序的文档。

HTTP 标头转发

控制分配是否根据指定的标头值缓存内容，如果是，则要缓存哪些内容。HTTP 标头包含有关客户端浏览器、请求的页面、源等方面的信息。例如，Accept-Language 标头发送客户端的语言（例如 en-US 为英语），以便源可以用客户端语言响应内容（如果可用）。

您可以为分配选择以下 HTTP 标头选项之一：

- 不转发任何标头
- 仅转发我指定的标头

如果您选择不转发任何标头，则分配不会根据标头值缓存您的内容。无论您选择哪个选项，分配都会将特定标头转发到您的源并根据您转发的标头执行特定操作。有关分配如何处理标头转发的更多信息，请参阅 HTTP 请求标头和分配行为。

Cookie 转发

控制您的分配是否将 Cookie 转发到源，如果是，则要转发哪些 Cookie。Cookie 包含发送到源的一小部分数据，例如访问者在源的 Web 页面上的操作信息，以及访问者提供的任何信息（例如他们的姓名和兴趣）。

您可以为分配选择以下 Cookie 转发选项之一：

- 不转发 Cookie
- 转发所有 Cookie
- 转发我指定的 Cookie

如果您选择转发所有 Cookie，不管您的应用程序使用多少 Cookie， 分配都会转发所有 Cookie。如果您选择转发我指定的 Cookie，则在显示的文本框中输入您希望分配转发的 Cookie 的名称。指定 Cookie 名称时可以使用以下通配符：

- * 匹配 Cookie 名称中的 0 个或多个字符
- ? 与 Cookie 名称中的 1 个字符完全匹配

例如，假设对象的查看器请求包含一个名为 `userid_member-number` 的 Cookie。其中，您的每个用户对于 `member-number` 均有一个唯一的值（`userid_123`、`userid_124`、`userid_125` 等）。您希望分配为每个成员缓存内容的单独版本。您可以通过将所有 Cookie 转发到源来完成该操作，但查看器请求包含一些您希望分配不要缓存的 Cookie。您可以指定以下值以作为 Cookie 名称，这会导致您的分配将所有以 `userid_` 开头的 Cookie 转发到源：`userid_*`

查询字符串转发

控制您的分配是否将查询字符串转发到源，如果是，则要转发哪些查询字符串。查询字符串是为将值分配给指定参数的一部分 URL。例如，`https://example.com/over/there?name=ferret` URL 包含 `name=ferret` 查询字符串。当服务器收到此类页面的请求时，它可能会运行一个程序，将 `name=ferret` 查询字符串原封不动地传递给程序。问号将用作分隔符，而不是查询字符串的一部分。

您可以选择让您的分配不转发任何查询字符串，或者选择仅转发指定的查询字符串。如果源返回相同版本的内容，则无论查询字符串参数的值为何，请选择不转发查询字符串。这增加了分配可从缓存处理请求的可能性，将提高性能并降低源的负载。如果您的源服务器根据一个或多个查询字符串参数返回不同版本的内容，请选择此选项，以仅转发您指定的查询字符串。

分配计划

分配计划指定每月数据传输配额和分配成本。如果分配传输的数据超过计划的每月数据传输配额，则会向您收取超额费用。有关更多信息，请参阅 Lightsail 定价页。

为避免超额费用，请将分配的当前计划更改为不同的计划，以在分配超出每月配额之前提供更大的每月数据传输量。在每个 AWS 计费周期内，您只能更改一次分配的计划。有关在创建分配套餐后更改分配套餐的更多信息，请参阅更改分配套餐。

创建分配

完成以下过程以创建分配。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择创建分配。
4. 在页面的选择您的源部分，选择您在其中创建了源资源的 AWS 区域 。

分配是全局资源。他们可以在任何来源中引用来源 AWS 区域，并在全球范围内分发其内容。

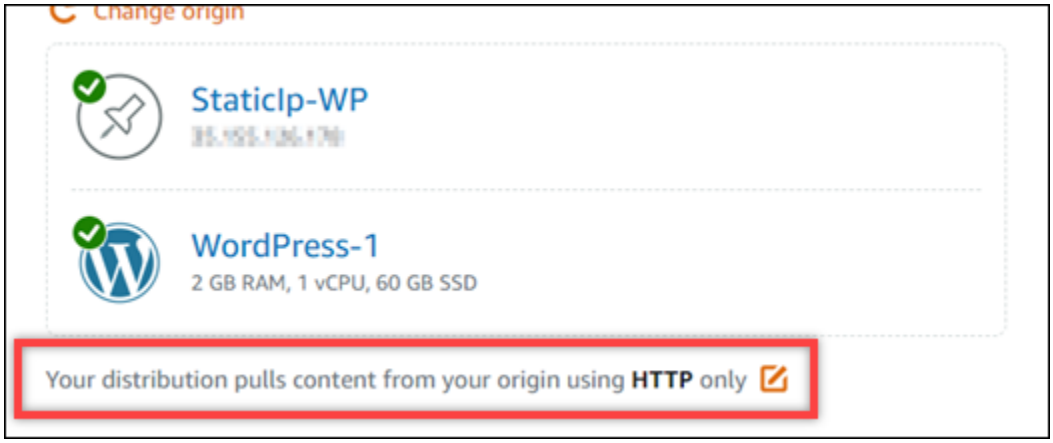
5. 选择您的源。源可以是 Lightsail 实例、容器服务、存储桶或负载均衡器（附加了一个或多个实例）。有关更多信息，请参阅源资源。

> **Important**
>
> 如果您选择 Lightsail 容器服务作为分发的来源，Lightsail 会自动将分配的默认域名添加为容器服务上的自定义域。这使流量能够在您的分配和容器服务之间进行路由。但是，在某些情况下，您可能需要手动将分配的原定设置域名添加到容器服务中。有关更多信息，请参阅将分配的原定设置域添加到容器服务。

6. （可选）要更改源协议策略，请选择在分配使用的当前源协议策略旁边显示的铅笔图标。有关更多信息，请参阅源协议策略。

   此选项列在页面的选择源部分，在您为分配选择的源资源下面。

> **Note**
>
> 当您选择 Lightsail 存储桶作为分配的来源时，Ori gin 协议策略默认为仅 HTTPS。当存储桶是分配的源时，您无法更改源协议策略。



7. 选择分配的缓存行为（也称为缓存预设）。有关更多信息，请参阅缓存行为和缓存预设。

> **Note**
>
> 当您选择 Lightsail 存储分区作为分发源时，缓存预设选项不可用。我们会自动应用最适合存储桶中存储的静态内容的分配设置。

8. （可选）选择显示所有设置以查看分配的其他缓存行为设置。

> **Note**
>
> 当您选择 Lightsail 存储分区作为分发源时，缓存行为设置不可用。我们会自动应用最适合存储桶中存储的静态内容的分配设置。

9. （可选）选择分配的默认行为。有关更多信息，请参阅默认行为。

> **Note**
>
> 当您选择 Lightsail 存储分区作为分发来源时，默认行为选项不可用。我们会自动应用最适合存储桶中存储的静态内容的分配设置。

10. （可选）选择添加路径以将目录和文件覆盖添加到分配的缓存行为中。有关更多信息，请参阅目录和文件覆盖。

> **Note**
>
> 当您选择 Lightsail 存储桶作为分发源时，目录和文件覆盖选项不可用。我们会自动应用最适合存储桶中存储的静态内容的分配设置。

11. （可选）选择要为分配编辑的高级设置旁边显示的铅笔图标。有关更多信息，请参阅高级缓存设置。

> **Note**
>
> 当您选择 Lightsail 存储分区作为分配来源时，创建分发页面上的高级缓存设置不可用。我们会自动应用最适合存储桶中存储的静态内容的分配设置。但是，创建分配后您可以在分配管理页面中修改高级缓存设置。

12. 选择您的分配计划。有关更多信息，请参阅分配计划。
13. 为分配输入名称。

资源名称：

- 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
- 必须包含 2 到 255 个字符。
- 必须以字母数字字符或数字作为开头和结尾。
- 可以包括字母数字字符、数字、句点、连字符和下划线。

14. 查看分配的成本。
15. 选择创建分配。

    将在片刻后创建您的分配。

后续步骤

在分配启动并运行后，我们建议您完成以下后续步骤。

1. 如果您的分配源是一个 WordPress 实例，则必须编辑实例中的 WordPress配置文件以使您的 WordPress 网站与您的分配配合使用。有关更多信息，请参阅配置您的 WordPress实例以与您的分配配合使用。
2. （可选）在 Lightsail 控制台中创建 Lightsail DNS 区域来管理你的域名的 DNS。这使您可以轻松地将您的域名映射到您的 Lightsail 资源。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。或者，您也可以继续在当前托管的位置托管域的 DNS。
3. 先为您的域创建 Lightsail SSL/TLS certificate for your domain to use it with your distribution. Lightsail distributions require HTTPS, so you must request an SSL/TLS 证书，然后才能将其用于发行版。有关更多信息，请参阅创建分配的 SSL/TLS 证书。
4. 为您的分配启用自定义域，以便将域用于您的分配。启用自定义域名需要您指定为域名创建的 Lightsail SSL/TLS 证书。这会将您的域添加到分配中并启用 HTTPS。有关更多信息，请参阅启用分配的自定义域。
5. 将别名记录添加到域的 DNS 以开始将域的流量路由到您的分配。添加别名记录后，将通过您的分配对访问域的用户进行路由。有关更多信息，请参阅将域指向分配。
6. 测试您的分配是否在缓存内容。有关更多信息，请参阅测试分配。

删除 Lightsail 发行版

如果您不再使用您的 Amazon Lightsail 发行版，则可以随时将其删除。

删除分配

完成以下过程以删除分配。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要删除的分配的名称。
4. 在分配的管理页面上选择删除选项卡。
5. 选择删除分配以删除分配。
6. 选择是，删除以确认删除。

为 Lightsail 发行版配置缓存

缓存行为允许您配置 Amazon Lightsail 发行版从您的来源缓存或未缓存的内容。例如，您可以指定缓存源中的各个目录、文件或文件类型。您还可以指定已转发到源的 HTML 方法和标头。在本指南中，我们将介绍如何更改分配的行为。有关分配的更多信息，请参阅内容分发网络分配。

内容

- 缓存预设
- 最适合 WordPress 缓存预设
- 默认行为
- 目录和文件覆盖
- 高级缓存设置
- 更改分配的缓存行为

缓存预设

缓存预设为在源上托管的内容类型自动配置分配设置。例如，选择最适合静态内容预设会自动将分配配置为最适合静态网站的设置。如果您的网站托管在 WordPress 实例上，请选择 “最适合 WordPress预设”，将您的发行版自动配置为与您的 WordPress 网站配合使用。

您可以为分配选择以下缓存预设之一：

- 最适合静态内容 - 此预设将分配配置为缓存所有内容。如果您在源上托管静态内容（例如静态 HTML 页面），或者对于每个访问网站的用户来说内容不会更改，则非常适合使用此预设。选择此预设后，将缓存分配的所有内容。
- 最适合动态内容 - 此预设将分配配置为除了在创建分配页面的目录和文件覆盖部分指定为缓存的文件，将不缓存任何内容。有关更多信息，请参阅本指南下文中的目录和文件覆盖。如果您在源上托管动态内容，或者每个访问网站或 Web 应用程序的用户可以更改内容，则非常适合使用此预设。
- 最适 WordPress合-此预设将您的发行版配置为只缓存 WordPress实例`wp-includes/`和`wp-content/`目录中的文件。如果您的来源是使用 Certified by Bitnami 和 Automattic 蓝图（不包括多站点蓝图）的实例，则此预设非常理想。WordPress 有关此预设的更多信息，请参阅最适合 WordPress缓存预设。

> **Note**
>
> 无法选择自定义设置预设。如果您选择了预设，但随后手动修改分配的设置，则系统会自动为您选择该预设。

只能在 Lightsail 控制台中指定缓存预设。无法使用 Lightsail API 和进行指定。 AWS CLI SDKs

最适合 WordPress缓存预设

当你选择一个使用 Certified by Bitnami 和 Automattic 蓝图作为发行版来源的实例时，Lightsail 会询问你是否要将最适合 WordPress缓存的预设应用于你的分发。WordPress 如果您应用现在，则您的发行版将自动配置为最适合您的 WordPress 网站。没有其他需要应用的分配设置。最适合 WordPress 预设为除了 WordPress网站`wp-includes/`和`wp-content/`目录中的文件之外什么都不缓存。它还会将您的分配配置为每天清除缓存（缓存寿命为 1 天）、允许所有的 HTTP 方法、仅转发 `Host` 标头、不转发 Cookie 以及转发所有查询字符串。

> **Important**
>
> 您必须编辑实例中的 WordPress 配置文件才能使您的 WordPress网站与您的发行版配合使用。有关更多信息，请参阅配置您的 WordPress实例以与您的分配配合使用。

默认行为

默认行为指定分配如何处理内容缓存。系统会根据您选择的缓存预设，自动为您指定分配的默认行为。如果选择不同的默认行为，缓存预设会自动更改为自定义设置。

您可以为分配选择以下默认行为之一：

- 缓存所有内容 - 此行为将您的分配配置为缓存并将您的整个网站作为静态内容提供服务。如果源托管的内容不会因查看者而变化，或者您的网站没有使用 Cookie、标头或查询字符串来个性化内容，则非常适合使用此选项。
- 不缓存任何内容 - 此行为将您的分配配置为仅缓存源文件和您指定的文件夹路径。如果您的网站或 Web 应用程序使用 Cookie、标题和查询字符串为单个用户个性化内容，则非常适合使用此选项。如果选择此选项，您必须指定要缓存的目录和文件路径覆盖。

目录和文件覆盖

目录和文件覆盖可用于覆盖您选择的默认行为或添加例外。例如，如果您选择缓存所有内容，可通过覆盖指定分配不应缓存的目录、文件或文件类型。或者，如果您选择不缓存任何内容，可通过覆盖指定分配应缓存的目录、文件或文件类型。

在页面的目录和文件覆盖部分，您可以指定要缓存或不缓存的目录或文件的路径。使用星号可指定通配符目录 (`path/to/assets/*`) 和文件类型 (`*.html`、`*jpg`、`*js`)。目录和文件路径区分大小写。

以下是如何指定目录和文件覆盖的几个示例：

- 指定以下内容以缓存在 Lightsail 实例上运行的 Apache Web 服务器的文档根目录中的所有文件。

```
var/www/html/
```

- 指定以下设置以仅缓存 Apache Web 服务器文档根目录中的索引页面。

```
var/www/html/index.html
```

- 指定以下设置以仅缓存 Apache Web 服务器文档根目录中的 .html 文件。

```
var/www/html/*.html
```

- 指定以下设置以仅缓存 Apache Web 服务器文档根目录的镜像子目录中的 .jpg、.png 和 .gif 文件。

```
var/www/html/images/*.jpg
```

```
var/www/html/images/*.png
```

```
var/www/html/images/*.gif
```

指定以下设置以缓存 Apache Web 服务器文档根目录的镜像子目录中的所有文件。

```
var/www/html/images/
```

高级缓存设置

高级设置可用于指定分配中内容的缓存寿命、允许的 HTTP 方法、HTTP 标头转发、Cookie 转发和查询字符串转发。指定的高级设置仅应用于分配缓存的目录和文件，包括指定为缓存的目录和文件覆盖。

您可以配置以下高级设置：

缓存寿命 (TTL)

控制在分配将另一个请求转发到源以确定内容是否已更新之前，内容在分配缓存中保留的时间。默认值为一天。减少此持续时间可以更好地提供动态内容。增加此持续时间意味着您的用户将获得更好的性能，因为更有可能从边缘站点直接提供文件。增加此持续时间还会降低源的负载，因为分配提取内容的频率更低。

> **Note**
>
> 仅当来源没有向内容添加 HTTP 标头（如 `Cache-Control max-age`、`Cache-Control s-maxage` 和 `Expires`）时才应用指定的缓存寿命值。

允许的 HTTP 方法

控制您的分配处理和转发到源的 HTTP 方法。HTTP 方法指示需要在源上执行的操作。例如，GET 方法从源检索数据，PUT 方法请求将所包含的实体存储在源上。

您可以为分配选择以下 HTTP 方法选项之一：

- 允许 GET、HEAD、OPTIONS、PUT、POST、PATCH 和 DELETE 方法
- 允许 GET、HEAD 和 OPTIONS 方法
- 允许 GET 和 HEAD 方法

分配会始终缓存对 GET 和 HEAD 请求的响应。如果您选择允许这些请求，则您的分配还会缓存对 OPTIONS 请求的响应。分配不会缓存对任何其他 HTTP 方法的响应。

> **Important**
>
> 如果您将分配配置为允许支持的所有 HTTP 方法，则必须将源实例配置为处理所有方法。例如，如果由于要使用 POST 而将分配配置为允许这些方法，则必须配置源服务器以相应地处理 DELETE 请求，以便查看器无法删除您不希望删除的资源。有关更多信息，请搜索网站或 Web 应用程序的文档。

HTTP 标头转发

控制分配是否根据指定的标头值缓存内容，如果是，则要缓存哪些内容。HTTP 标头包含有关客户端浏览器、请求的页面、源等方面的信息。例如，Accept-Language 标头发送客户端的语言（例如 en-US 为英语），以便源可以用客户端语言响应内容（如果可用）。

您可以为分配选择以下 HTTP 标头选项之一：

- 不转发任何标头
- 仅转发我指定的标头

如果您选择不转发任何标头，则分配不会根据标头值缓存您的内容。无论您选择哪个选项，分配都会将特定标头转发到您的源并根据您转发的标头执行特定操作。

Cookie 转发

控制您的分配是否将 Cookie 转发到源，如果是，则要转发哪些 Cookie。Cookie 包含发送到源的一小部分数据，例如访问者在源的 Web 页面上的操作信息，以及访问者提供的任何信息（例如他们的姓名和兴趣）。

您可以为分配选择以下 Cookie 转发选项之一：

- 不转发 Cookie
- 转发所有 Cookie
- 转发我指定的 Cookie

如果您选择转发所有 Cookie，不管您的应用程序使用多少 Cookie， 分配都会转发所有 Cookie。如果您选择转发我指定的 Cookie，则在显示的文本框中输入您希望分配转发的 Cookie 的名称。指定 Cookie 名称时可以指定以下通配符：

- * 匹配 Cookie 名称中的 0 个或多个字符
- ? 与 Cookie 名称中的 1 个字符完全匹配

例如，假设对象的查看器请求包含一个名为 `userid_member-number` 的 Cookie。其中，您的每个用户对于 `member-number` 均有一个唯一的值（`userid_123`、`userid_124`、`userid_125` 等）。您希望分配为每个成员缓存内容的单独版本。您可以通过将所有 Cookie 转发到源来完成该操作，但查看器请求包含一些您希望分配不要缓存的 Cookie。您可以指定以下值以作为 Cookie 名称，这会导致您的分配将所有以 `userid_` 开头的 Cookie 转发到源：`userid_*`

查询字符串转发

控制您的分配是否将查询字符串转发到源，如果是，则要转发哪些查询字符串。查询字符串是为将值分配给指定参数的一部分 URL。例如，`https://example.com/over/there?name=ferret` URL 包含 `name=ferret` 查询字符串。当服务器收到此类页面的请求时，它可能会运行一个程序，将 `name=ferret` 查询字符串原封不动地传递给程序。问号将用作分隔符，而不是查询字符串的一部分。

您可以选择让您的分配不转发任何查询字符串，或者选择仅转发指定的查询字符串。如果源返回相同版本的内容，则无论查询字符串参数的值为何，请选择不转发查询字符串。这增加了分配可从缓存处理请求的可能性，将提高性能并降低源的负载。如果源服务器根据一个或多个查询字符串参数返回不同版本的内容，则选择仅转发您指定的查询字符串。

更改分配的缓存行为

完成以下过程以更改分配的缓存行为。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其更改默认缓存行为的分配名称。
4. 在分配的管理页面上选择缓存选项卡。
5. 在页面的配置缓存部分，为您的分配选择缓存预设。有关更多信息，请参阅缓存预设。
6. 选择更改默认缓存行为以更改分配的默认行为。然后，为您的分配选择默认行为。有关更多信息，请参阅默认行为。

7. 选择添加路径以将目录和文件覆盖添加到分配的缓存行为中。有关更多信息，请参阅目录和文件覆盖。
8. 选择要为分配编辑的高级设置旁边显示的铅笔图标。有关更多信息，请参阅高级缓存设置。

当您将更改保存到您的分配配置中时，分配会开始将更改传播到所有边缘站点。在您的配置在边缘站点中经更新前，您的分配将继续根据先前的配置从该站点提供内容。在您的配置在边缘站点已更新后，您的分配将立即根据新的配置从该站点提供内容。

您的更改不会立即传播到每个边缘站点。传播完成后，分配的状态将从InProgress变为 “已启用”。当分配传播您的更改时，我们无法确定一个指定边缘站点是根据先前配置还是新配置提供内容。

主题

- 重置 Lightsail 发行版的缓存

重置 Lightsail 发行版的缓存

缓存寿命（生存时间）设置控制您的内容在 Amazon Lightsail 发行版缓存中的停留时间。如果您需要在缓存生命周期间隔之前清除缓存，也可以手动重置分配的缓存。清除缓存后，当用户下次请求内容时，您的分配会从源中提取最新版本的内容并对其进行缓存。在本指南中，我们将介绍如何手动重置分配的缓存。有关分配的更多信息，请参阅内容分发网络分配。

重置分配的缓存

完成以下过程以重置分配的缓存。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其重置缓存的分配名称。
4. 在分配的管理页面上选择缓存选项卡。
5. 滚动到页面的重置缓存部分，然后选择重置缓存。
6. 对于确认提示，选择是，重置以确认您要重置分配的缓存。或者选择否，取消而不重置分配的缓存。

更改 Lightsail 发行版的内容来源

在本指南中，我们将向您展示如何在创建 Amazon Lightsail 发行版后更改其来源。源是分配内容的确定来源。在创建发行版时，您可以选择托管您的网站或 Web 应用程序内容的 Lightsail 实例、Lightsail 存储桶或 Lightsail 负载均衡器（附加了一个或多个实例）。有关更多信息，请参阅内容分发网络分配。

您可以在创建分配后随时更改源。在更改源时，分配会立即开始将更改复制到 边缘站点。分配将继续将请求转发到指定边缘站点中的先前源，直至分配更新为该边缘站点中的新源。

更改源并不要求分配用新源的内容重新填充边缘缓存。只要网站或 Web 应用程序中的用户请求未更改，分配就会继续提供边缘缓存中已有的内容，直至内容的缓存寿命过期。

源协议策略

源协议策略是在从源中提取内容时分配使用的协议策略。选择分配的源之后，您应确定在从源中提取内容时分配是使用超文本传输协议 (HTTP) 还是安全超文本传输协议 (HTTPS)。如果源没有进行 HTTPS 配置，则必须使用 HTTP。

您可以为分配选择以下源协议策略之一：

- 仅 HTTP - 分配仅使用 HTTP 访问源。这是默认设置。
- 仅 HTTPS - 分配仅使用 HTTPS 访问源。

编辑源协议策略的步骤包含在本指南的以下更改分配的源部分。

更改分配的源

完成以下过程以更改分配的源。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其更改源的分配名称。
4. 在分配管理页面上选择详细信息选项卡，然后滚动到页面的选择源部分。

   页面的选择源部分显示分配的当前源。
5. 选择更改源。

6. 选择在其中创建了源资源的亚马逊云科技区域。

   分配是全局资源。其可以引用任何亚马逊云科技区域中的源，并在全局范围内分发其内容。

7. 选择您的源。源可以是实例、存储桶或负载均衡器（附加了一个或多个实例）。

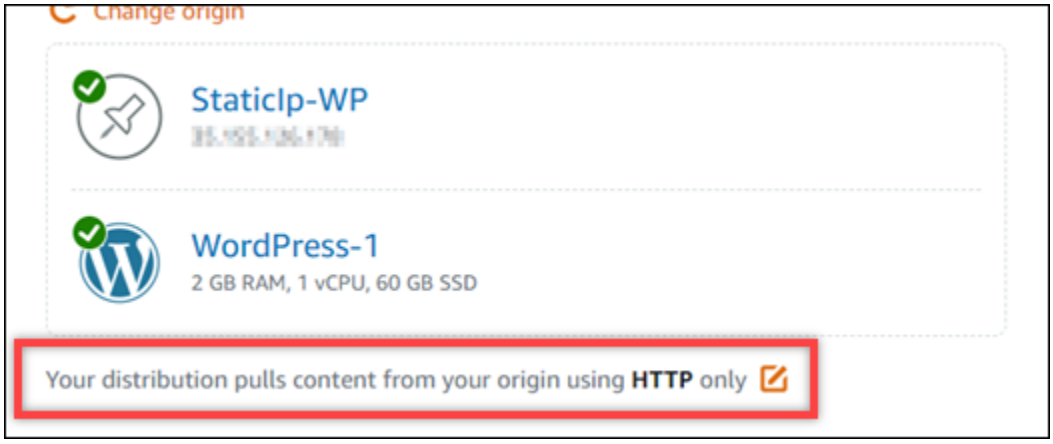
8. 选择保存以使用新源更新分配。

   选择分配的源之后，您应确定在从源中提取内容时分配是使用超文本传输协议 (HTTP) 还是安全超文本传输协议 (HTTPS)。

9. （可选）要更改源协议策略，请选择在分配使用的当前源协议策略旁边显示的铅笔图标。有关更多信息，请参阅源协议策略。

   此选项列在页面的选择源部分，在您为分配选择的源资源下面。

   > **Note**
   >
   > 当您选择 Lightsail 存储桶作为分配的来源时，Ori gin 协议策略默认为仅 HTTPS。当存储桶是分配的源时，您无法更改源协议策略。



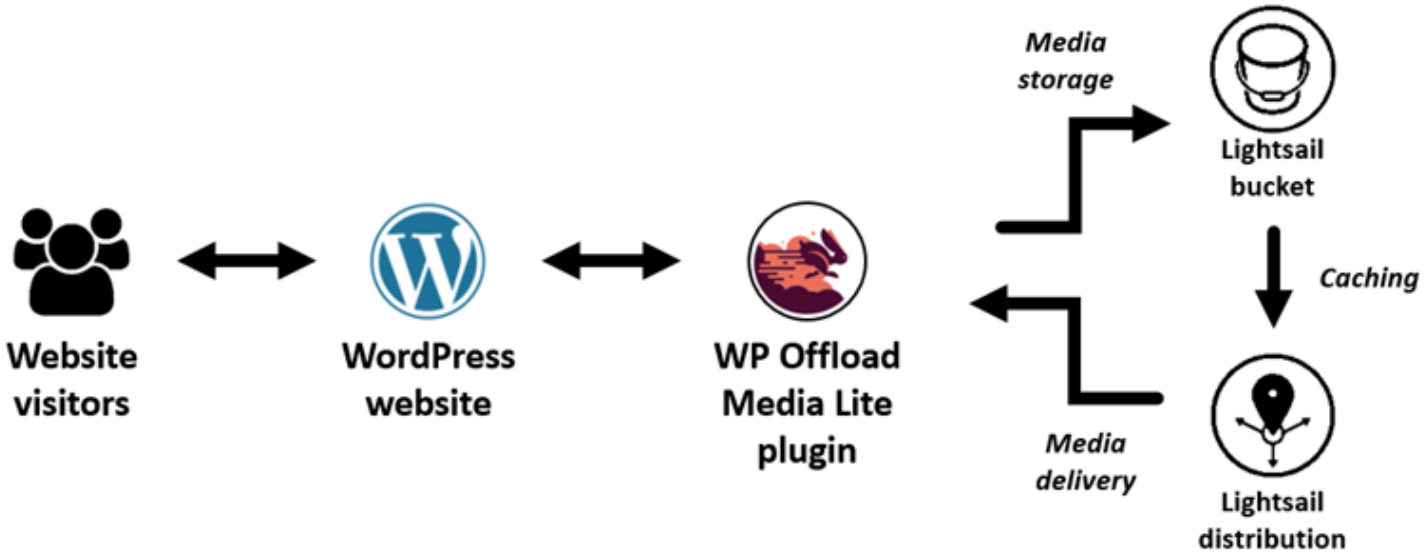
10. 选择仅 HTTP或仅 HTTPS，然后选择保存以保存源协议策略。

当您将更改保存到您的分配配置中时，分配会开始将更改传播到所有边缘站点。在您的配置在边缘站点中经更新前，您的分配将继续根据先前的配置从该站点提供内容。在您的配置在边缘站点已更新后，您的分配将立即根据新的配置从该站点提供内容。

您的更改不会立即传播到每个边缘站点。传播完成后，分配的状态将从InProgress变为“已启用”。当分配传播您的更改时，我们无法确定一个指定边缘站点是根据先前配置还是新配置提供内容。

使用 Lightsail 存储桶和 CDN 发行版高效地提供媒体文件

本教程介绍了将您的亚马逊 Lightsail 存储桶配置为 Lightsail 内容分发网络 (CDN) 分发的来源所需的步骤。它还描述了如何将您的 WordPress 网站配置为在存储桶中上传和存储媒体（例如图像和电影文件），以及如何从您的发行版中传送媒体。执行此操作的一个示例是使用 WP Offload Media Lite 插件。下面的示意图对此配置进行说明。



将网站媒体存储在 Lightsail 存储桶中可以减轻您的实例存储和提供这些文件的负担。缓存和提供来自 Lightsail 发行版的媒体可以加快向网站访问者交付这些文件的速度，还可以提高网站的整体性能。有关分配的更多信息，请参阅内容分发网络分配。有关存储桶的更多信息，请参阅对象存储。

内容

- 步骤 1：完成先决条件
- 步骤 2：修改存储桶权限
- 步骤 3：创建使用存储桶作为源的分配
- 步骤 4：启用分配的自定义子域
- 第 5 步：在你的 WordPress 网站上安装 WP Offload Media Lite 插件
- 第 6 步：测试你的 WordPress 网站与 Lightsail 存储桶和发行版之间的连接

步骤 1：完成先决条件

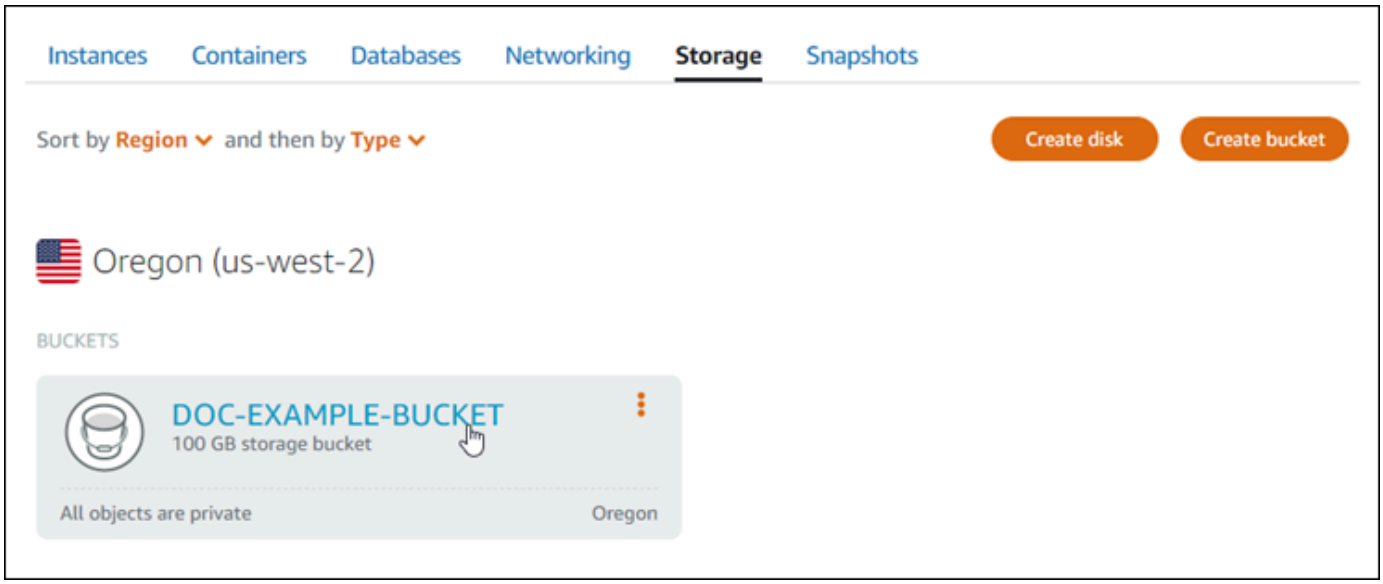
满足以下先决条件（如果尚未满足）：

- 在 Lightsail 中创建和配置 WordPress 实例，然后获取登录管理仪表板的密码。有关更多信息，请参阅教程：在 Amazon Lightsai WordPress l 中启动和配置实例。
- 在 Lightsail 对象存储服务中创建存储桶。有关更多信息，请参阅在 Lights ail 中创建存储桶。

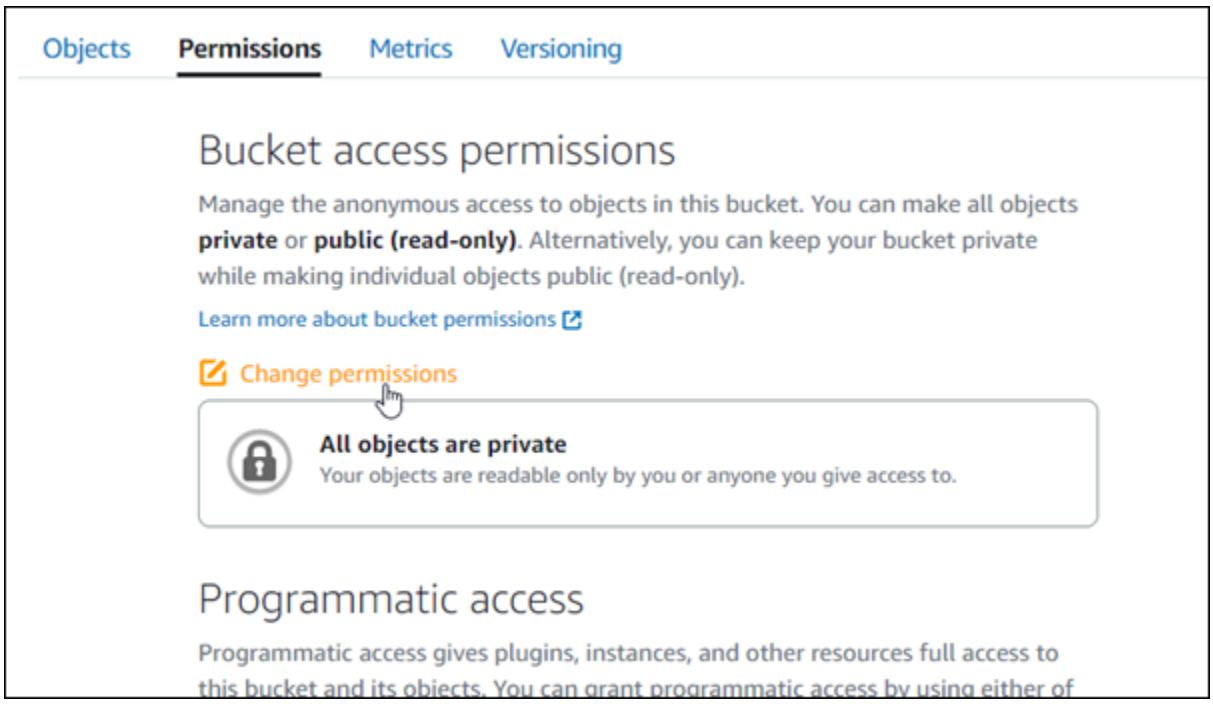
步骤 2：修改存储桶权限

完成以下步骤以授予您的 WordPress 实例和 WP Offload Media Lite 插件访问存储桶的权限。存储桶的权限必须设置为个别对象可设为公有（只读）。您还必须将您的 WordPress 实例附加到您的存储桶。有关存储桶权限的更多信息，请参阅存储桶权限。

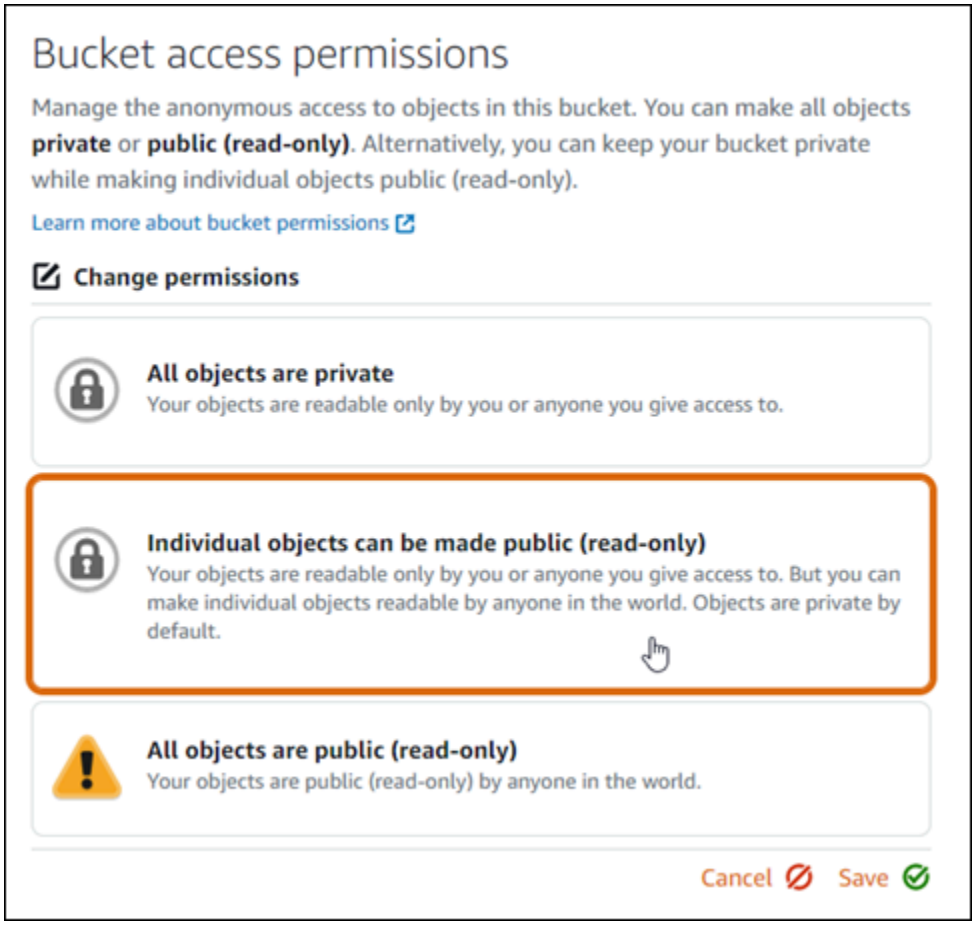
1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择您要用于 WordPress 网站的存储桶的名称。



4. 在存储桶管理页面上选择权限选项卡。
5. 在页面的存储桶访问权限部分下面选择更改权限。

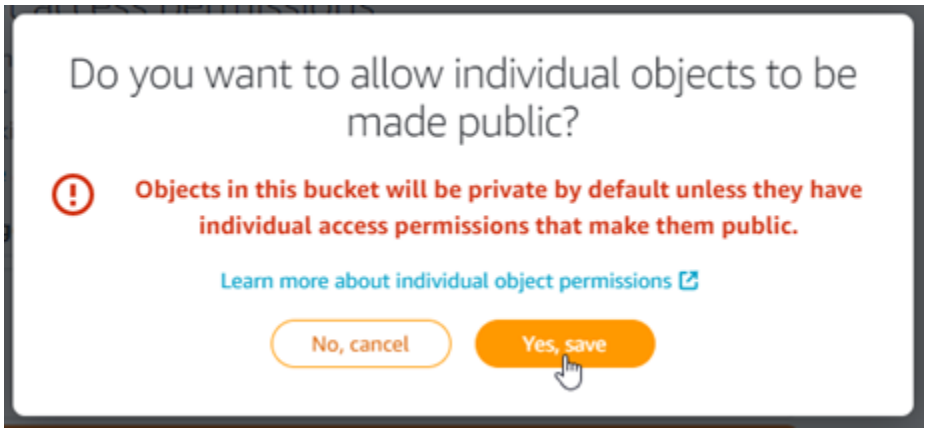


6. 选择个别对象可设为公有（只读）。



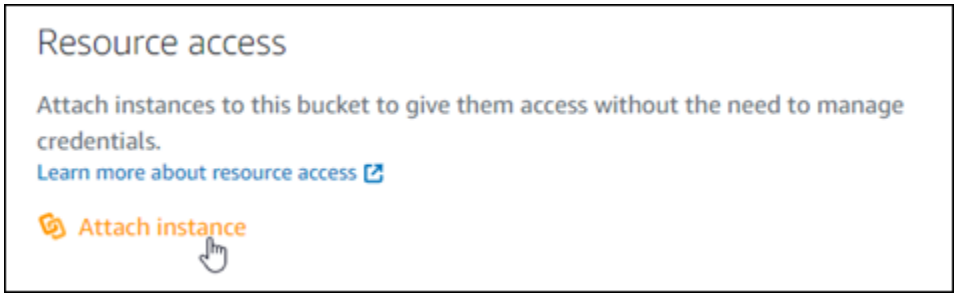
7. 选择保存。

8. 在显示的确认提示中选择是，保存。

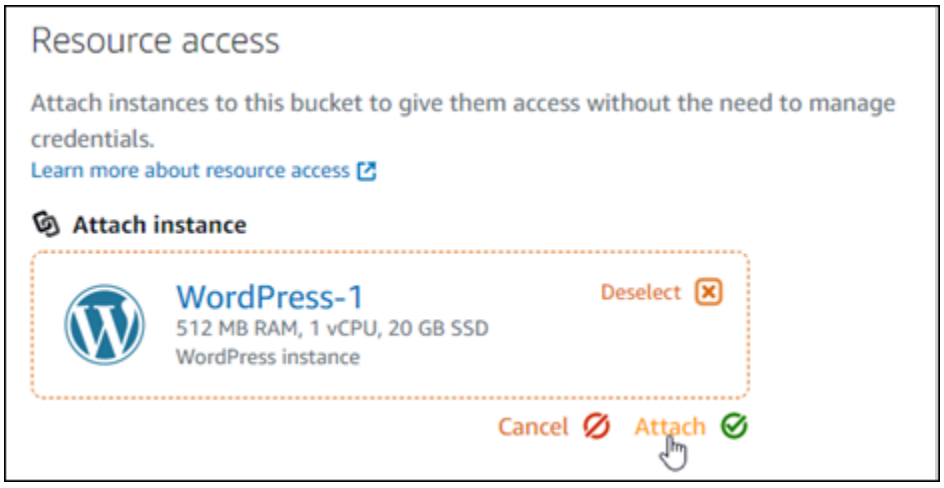


稍等片刻，存储桶将被配置为允许个别对象访问。这样可以确保客户可以读取使用 Offload Media Lite 插件从您的 WordPress 网站上传到您的存储桶的对象。

9. 滚动到页面的资源访问权限部分，然后选择附加实例。



10. 在出现的下拉列表中选择您的 WordPress 实例名称，然后选择附加。



片刻之后，您的 WordPress 实例将连接到您的存储桶。这使您的 WordPress 实例能够管理您的存储桶及其对象。

步骤 3：创建使用存储桶作为源的分配

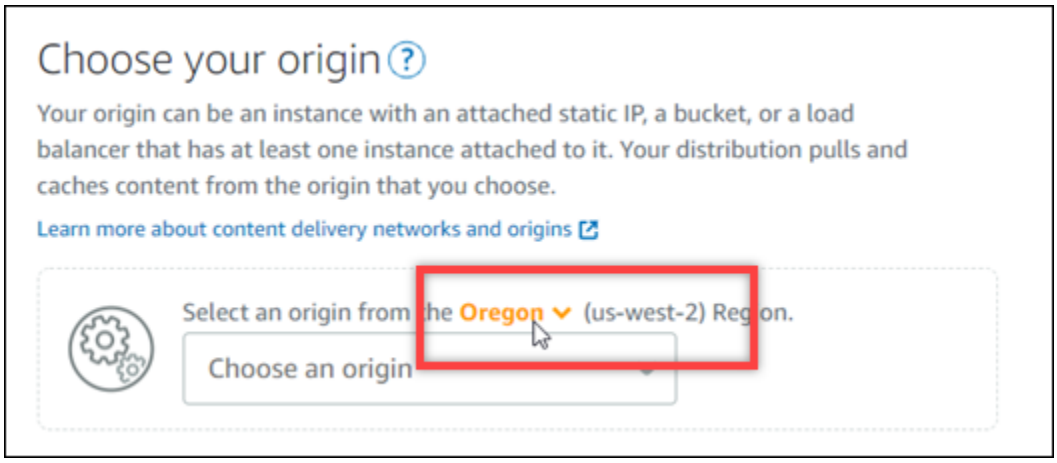
完成以下步骤创建 Lightsail 发行版并选择你的 Lightsail 存储桶作为来源。

1. 在 Lightsail 控制台的顶部导航菜单上选择 “主页”。
2. 在左侧导航窗格中，选择联网。
3. 选择创建分配。

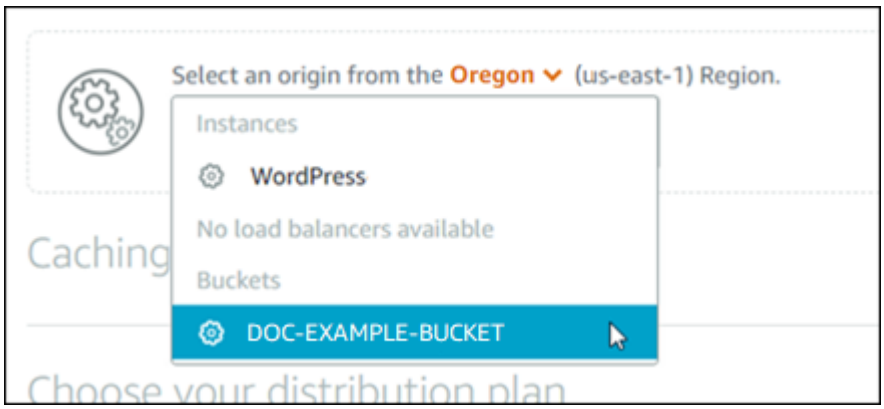


4. 在页面的选择您的源部分，选择您在其中创建了存储桶的 AWS 区域 。

   分配是全局资源。他们可以在任何存储桶中引用存储桶 AWS 区域，并在全球范围内分发其内容。

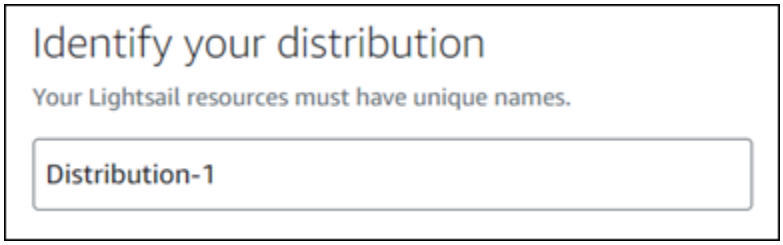


5. 选择存储桶作为源。



> **Note**
>
> 存储桶的权限必须设置为个别对象可设为公有（只读）。只有公开的单个对象才会被缓存并由分配提供。当您选择存储桶作为分配的源时，用于指定源协议策略、缓存行为、默认行为以及目录和文件覆盖的选项将变为不可用，且无法编辑。对于存储桶，源协议策略默认为仅 HTTP，并且缓存行为默认为缓存所有内容。您可以在创建分配后更改分配的高级缓存设置。

6. 选择您的分配计划。
7. 为分配输入名称。



分配名称：

- 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
- 必须包含 2–255 个字符。
- 必须以字母数字字符或数字作为开头和结尾。
- 可以包括字母数字字符、数字、句点、连字符和下划线。

8. 选择创建分配。



将在片刻后创建您的分配。当您的新分配达到 Enabled (已启用)状态时，便准备就绪可以提供和缓存存储桶中的对象。

步骤 4：启用分配的自定义子域

创建分配时，配置的默认域类似于 `123abc.cloudfront.net`。配置 WP Offload Media Lite 插件时，可以指定默认域作为媒体文件的源。但是，我们强烈建议您为分配启用自定义域。您为分发启用的自定义域名应该是您在 WordPress网站中使用的域名的子域名。例如，如果您在 WordPress网站中`mycustomdomain.com`使用，则可以选择在发行版中使用自定义域名`media.mycustomdomain.com`。在您的 WordPress网站和发行版之间使用相同的域名和子域名组合有助于提高网站的搜索引擎优化得分。

完成以下步骤为分配配置自定义域：

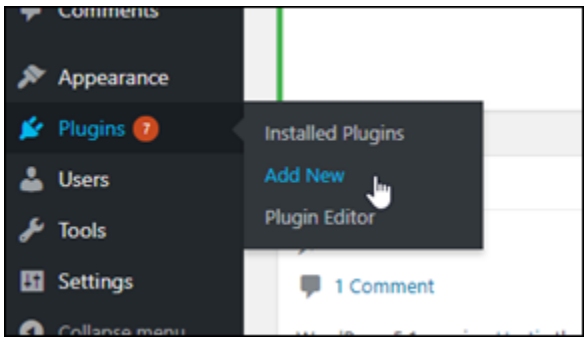
1. 先为您的域创建 Lightsail SSL/TLS certificate for your domain to use it with your distribution. Lightsail distributions require HTTPS, so you must request an SSL/TLS 证书，然后才能将其用于发行版。有关更多信息，请参阅创建分配的 SSL/TLS 证书。
2. 为您的分配启用自定义域，以便将域用于您的分配。启用自定义域名需要您指定为域名创建的 Lightsail SSL/TLS 证书。这会将您的域添加到分配中并启用 HTTPS。有关更多信息，请参阅启用分配的自定义域。
3. 将记录添加到域的 DNS 添加别名记录后，将通过您的分配对访问域的用户进行路由。有关更多信息，请参阅将域指向分配。

第 5 步：在你的 WordPress 网站上安装 WP Offload Media Lite 插件

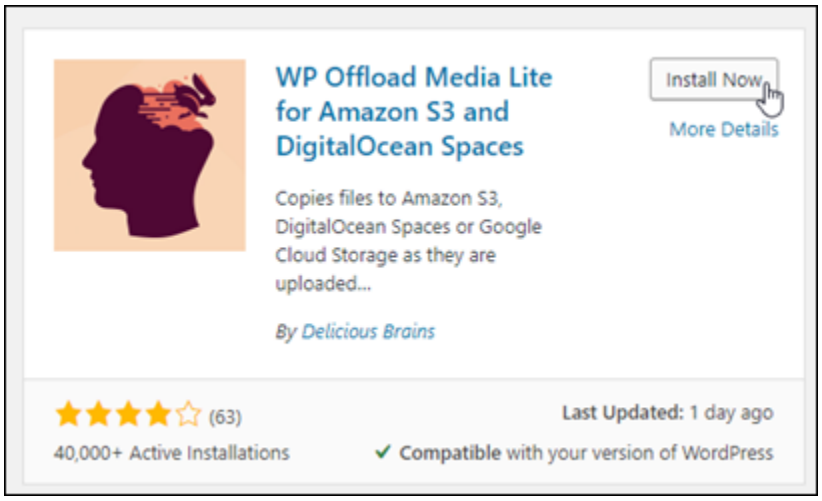
完成以下步骤，在您的 WordPress 网站上安装 WP Offload Media Lite 插件。此插件会自动将通过 WordPress “媒体上传器” 添加的图像、视频、文档和任何其他媒体复制到您的 Lightsail 存储桶中。也可以将其配置为通过 Lightsail 发行版提供存储桶中的媒体。有关更多信息，请参阅WordPress 网站中的 WP Offload Media Lite。

1. 以管理员身份登录到您 WordPress 网站的控制面板。

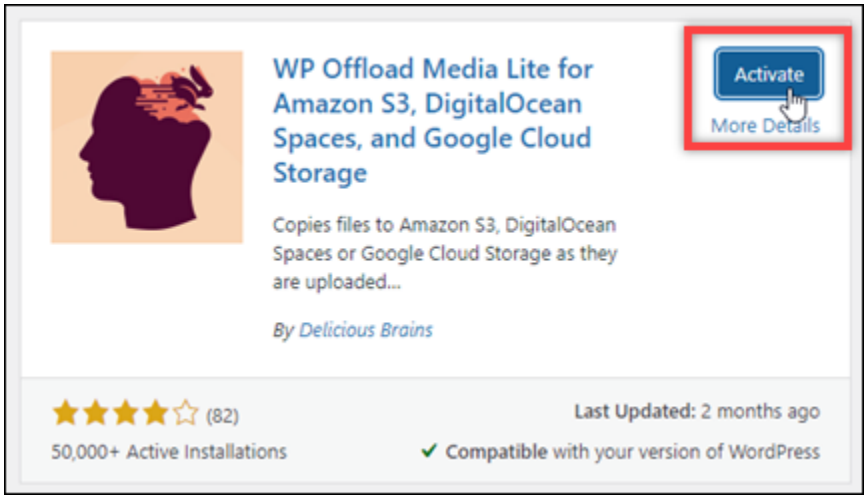
   有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。
2. 在左侧导航菜单中暂停插件，然后选择新增。



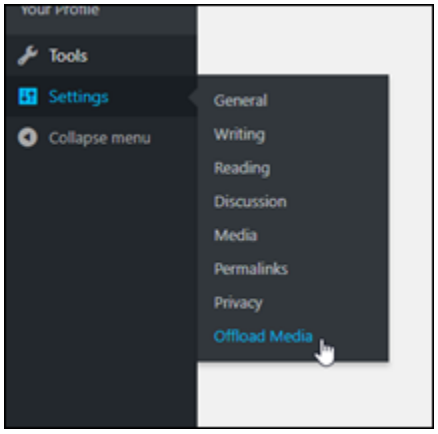
3. 搜索 WP Offload Media Lite。
4. 在搜索结果中，选择 WP Offload Media 插件旁边的立即安装。



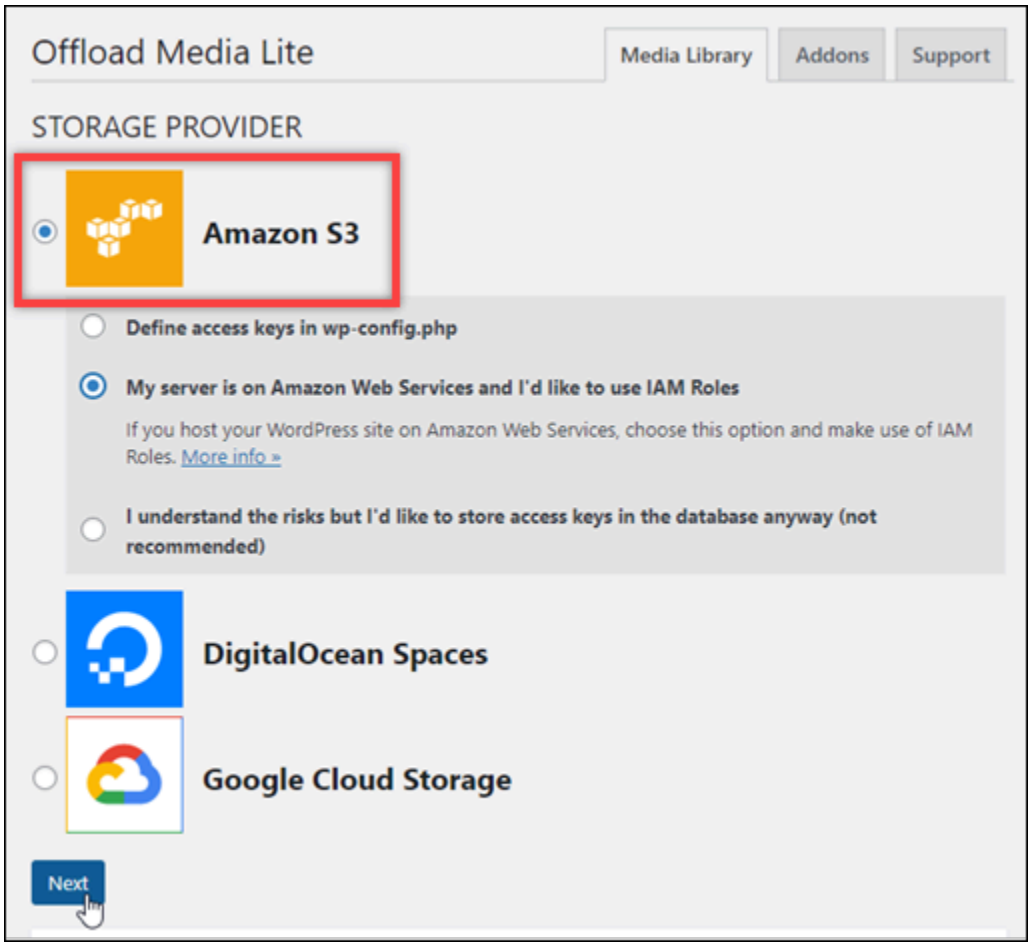
5. 完成插件安装后，选择 Activate (激活)。



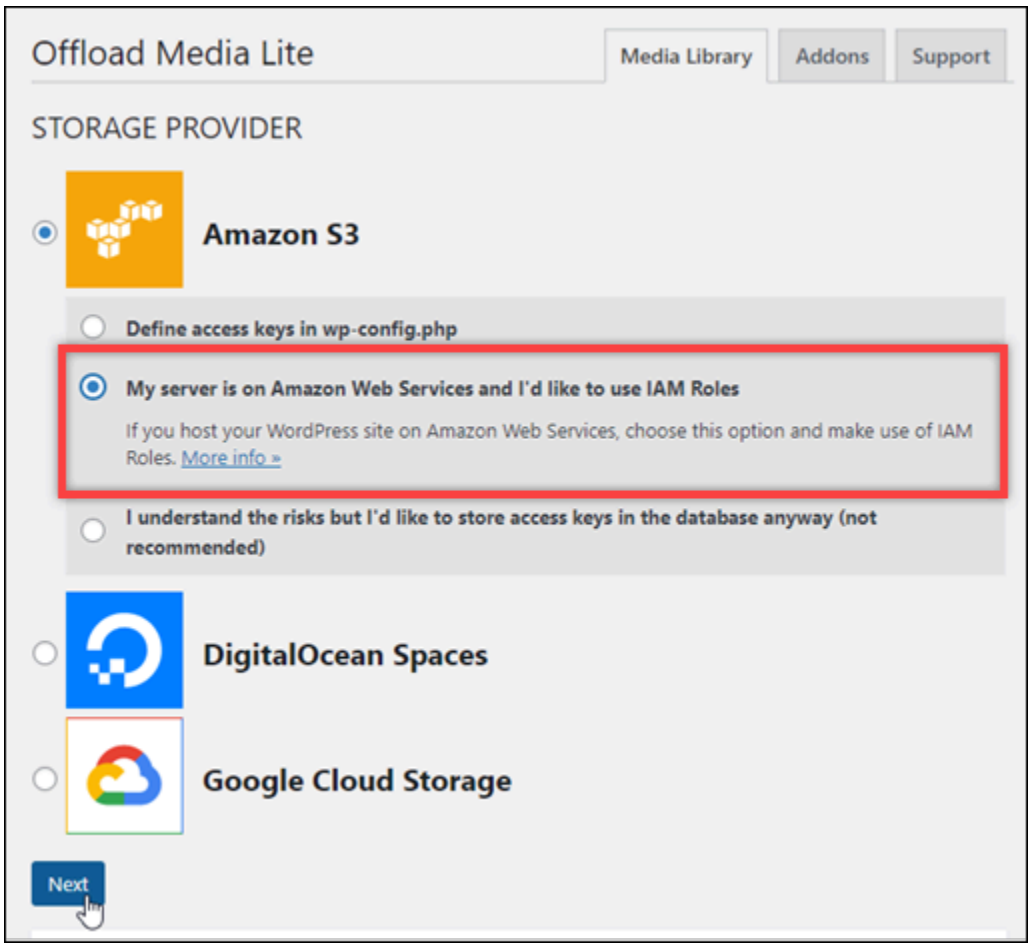
6. 在左侧导航菜单中，选择 Settings (设置)，然后选择 Offload Media。



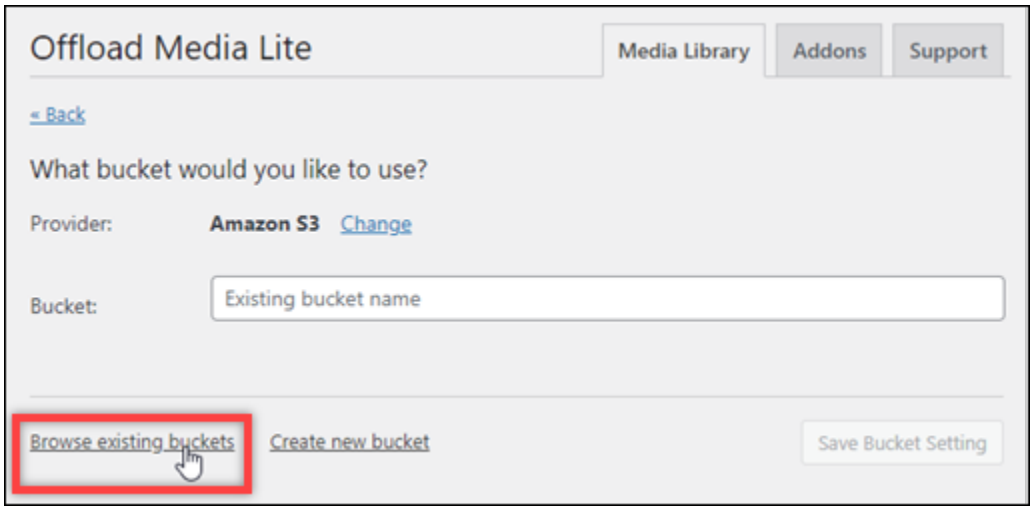
7. 在 Offload Media Lite 页面上，选择 Amazon S3 作为存储提供程序。



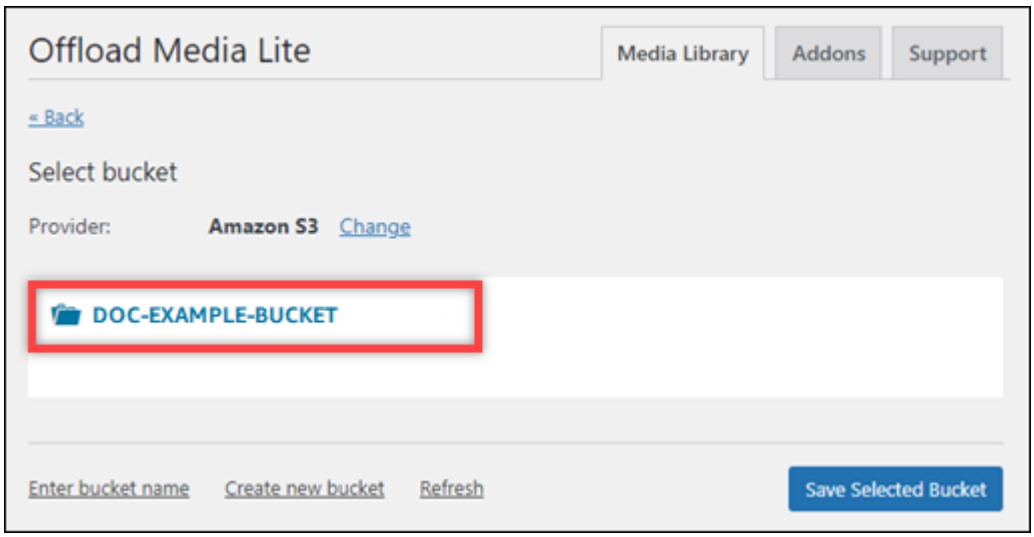
8. 选择我的服务器位于亚马逊云科技上，我想使用 IAM 角色。



9. 选择下一步。
10. 在显示的您想要使用什么存储桶？页面中选择浏览现有存储桶。



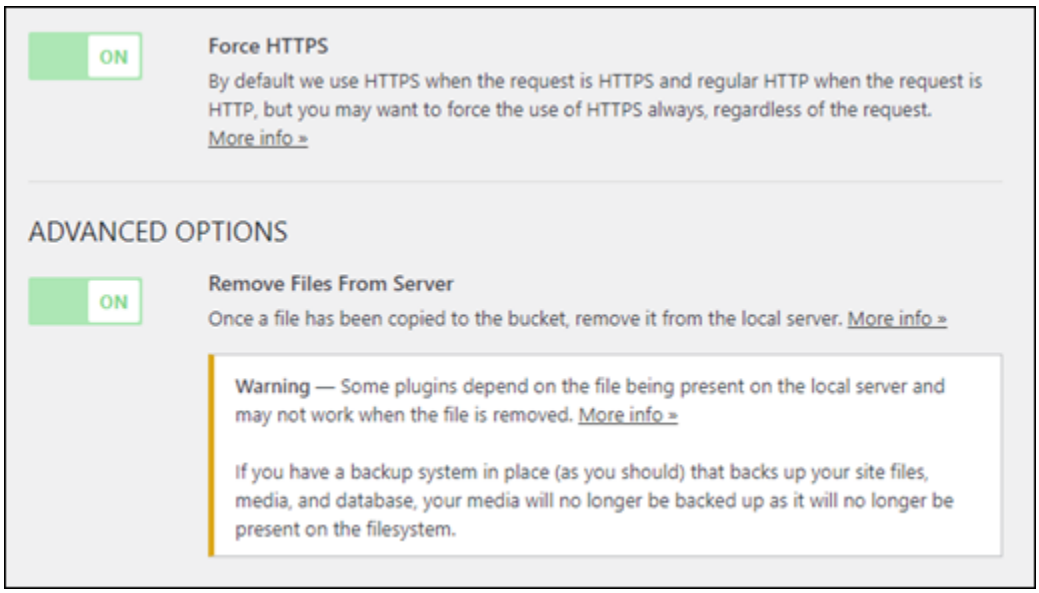
11. 选择您创建的用于 WordPress实例的存储桶的名称。



12. 在显示的 Offload Media Lite 设置页面中，打开强制执行 HTTPS 和从服务器中删除文件。

    - 必须开启强制 HTTPS 设置，因为 Lightsail 存储桶默认使用 HTTPS 来提供媒体文件。如果您不开启此功能，则从您的 WordPress 网站上传到您的 Lightsail 存储桶的媒体文件将无法正确提供给您的网站访问者。

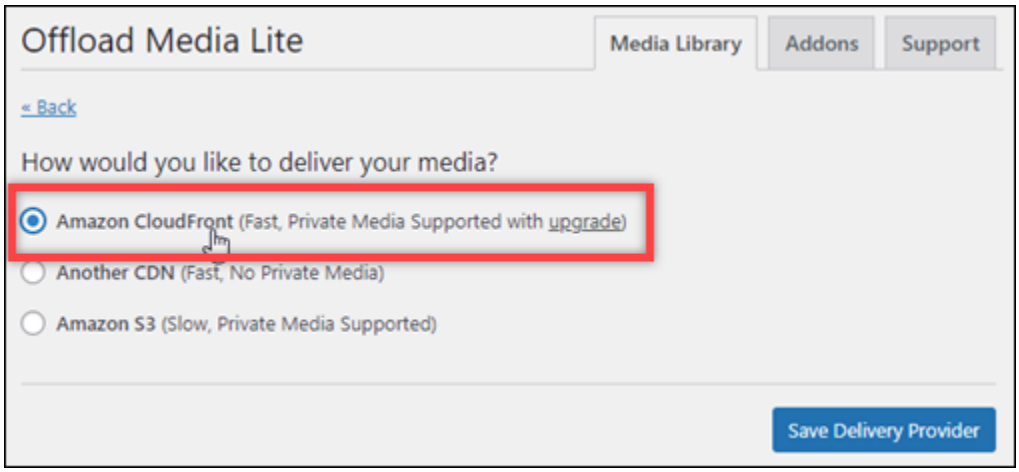
      “从服务器移除文件” 设置可确保上传到 Lightsail 存储桶的媒体不会也存储在实例的磁盘上。如果您不开启此功能，则上传到您的 Lightsail 存储桶的媒体文件也会存储在实例的本地存储中。WordPress



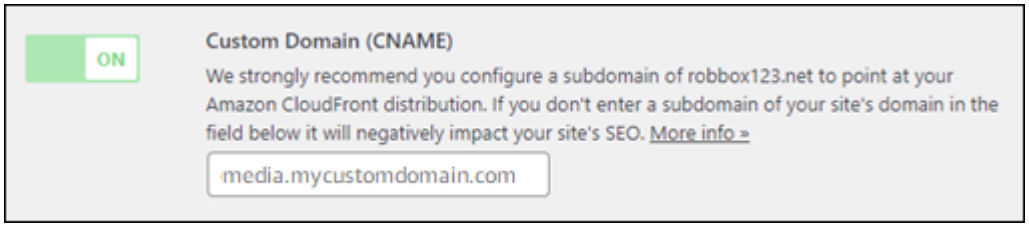
13. 在页面的传送部分，选择 Amazon S3 标签旁边的更改。



14. 在 “你想如何投放媒体？ 出现的页面，选择 Amazon CloudFront。



15. 选择保存分发提供商。
16. 在显示的 Offload Media Lite 设置页面中，打开自定义域（别名记录）。然后，在文本框中输入你的 Lightsail 发行版的域名。这可能是分配的默认域（例如，`123abc.cloudfront.net`），或者在启用了自定义域的情况下为分配的自定义域（例如，`media.mycustomdomain.com`）。



17. 选择 Save Changes（保存更改）。

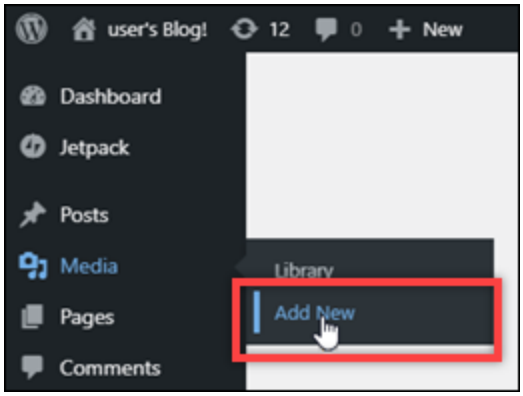
> **Note**
>
> 之后若要返回 Offload Media Lite 设置页面，请在左侧导航菜单中暂停设置，然后在选择 Offload Media。

您的 WordPress 网站现已配置为使用 Media Lite 插件。下次您通过上传媒体文件时 WordPress，该文件会自动上传到您的 Lightsail 存储桶，并由发行版提供。要测试配置，请继续执行本教程的下一部分。

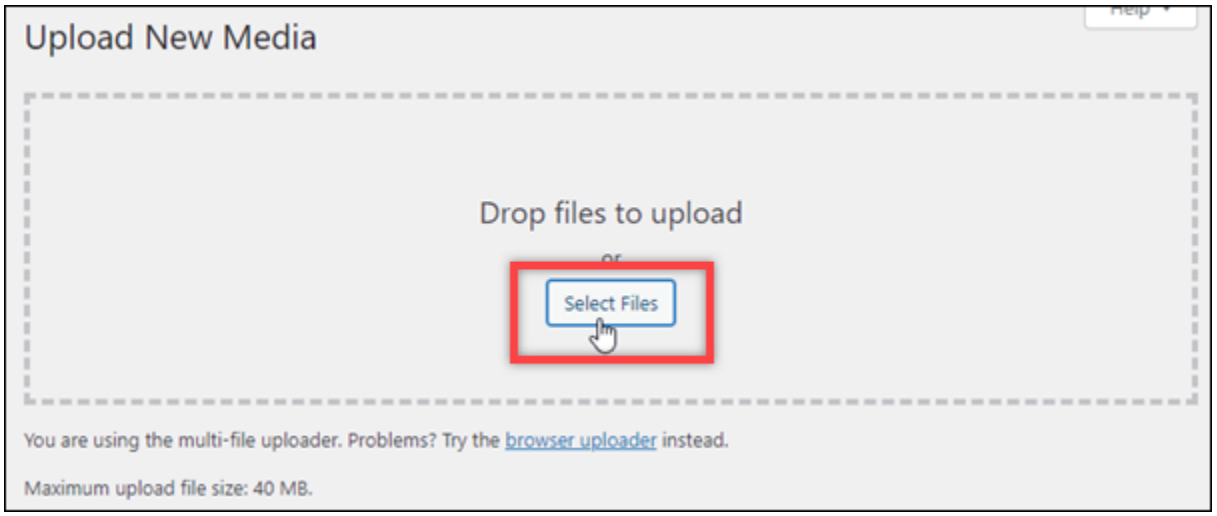
第 6 步：测试你的 WordPress 网站与 Lightsail 存储桶和发行版之间的连接

完成以下步骤将媒体文件上传到您的 WordPress 实例，并确认该文件已上传到您的 Lightsail 存储桶并由您的分发提供。

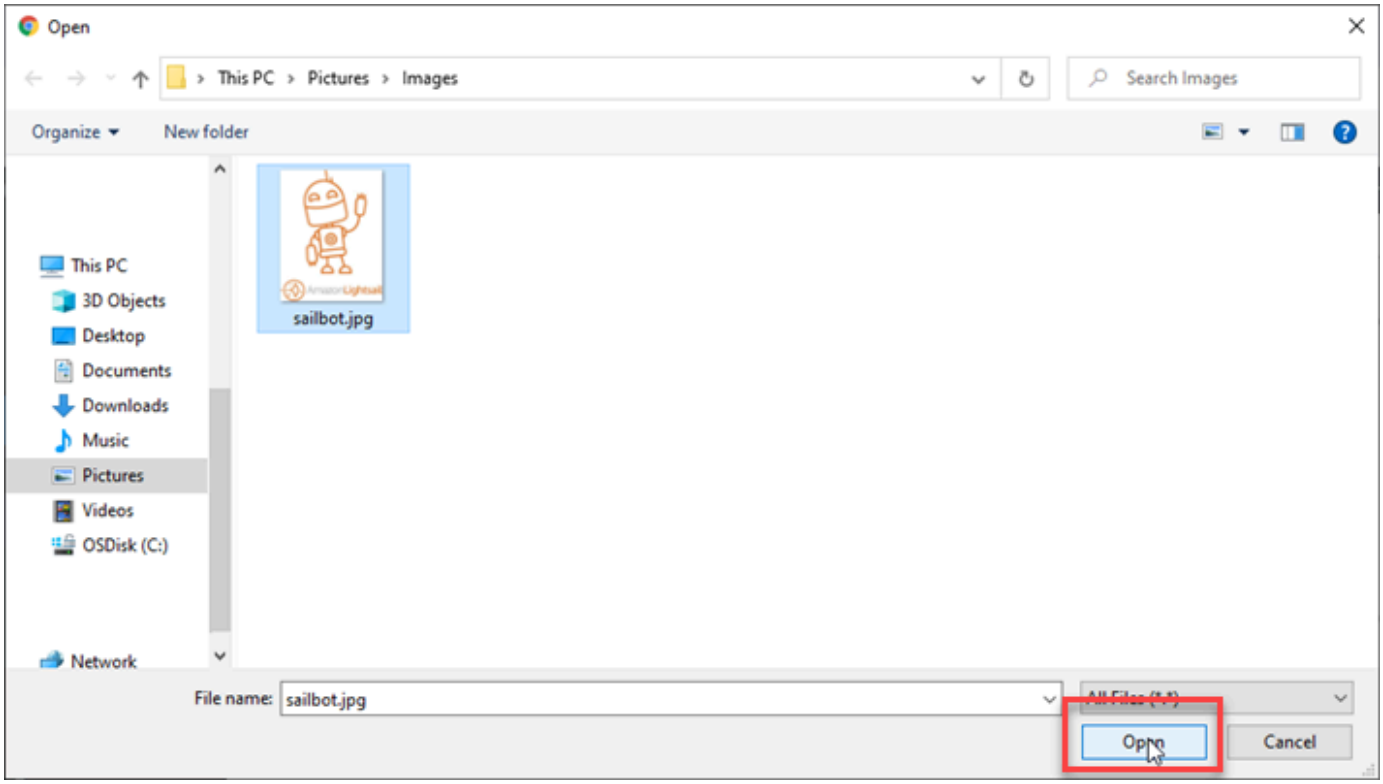
1. 在 WordPress仪表板左侧导航菜单中暂停在 “媒体” 上，然后选择 “新增”。



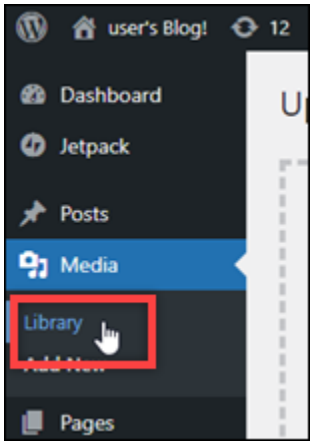
2. 在显示的上传新媒体页面上选择选择文件。



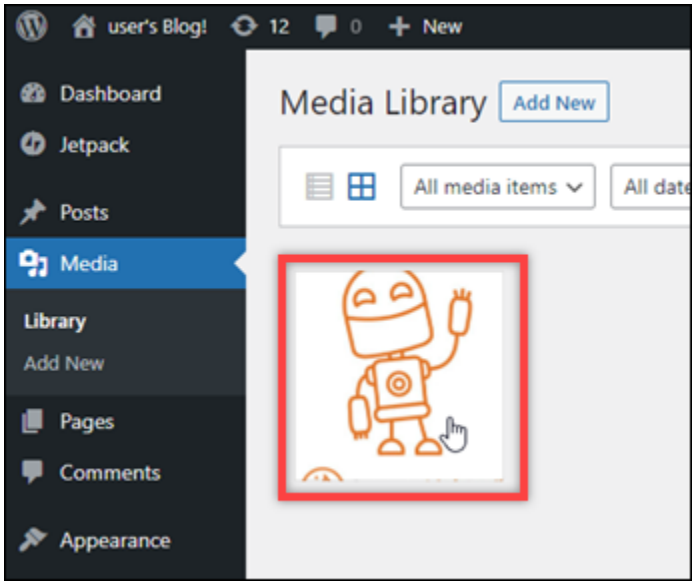
3. 选择要从本地计算机上传的媒体文件，然后选择打开。



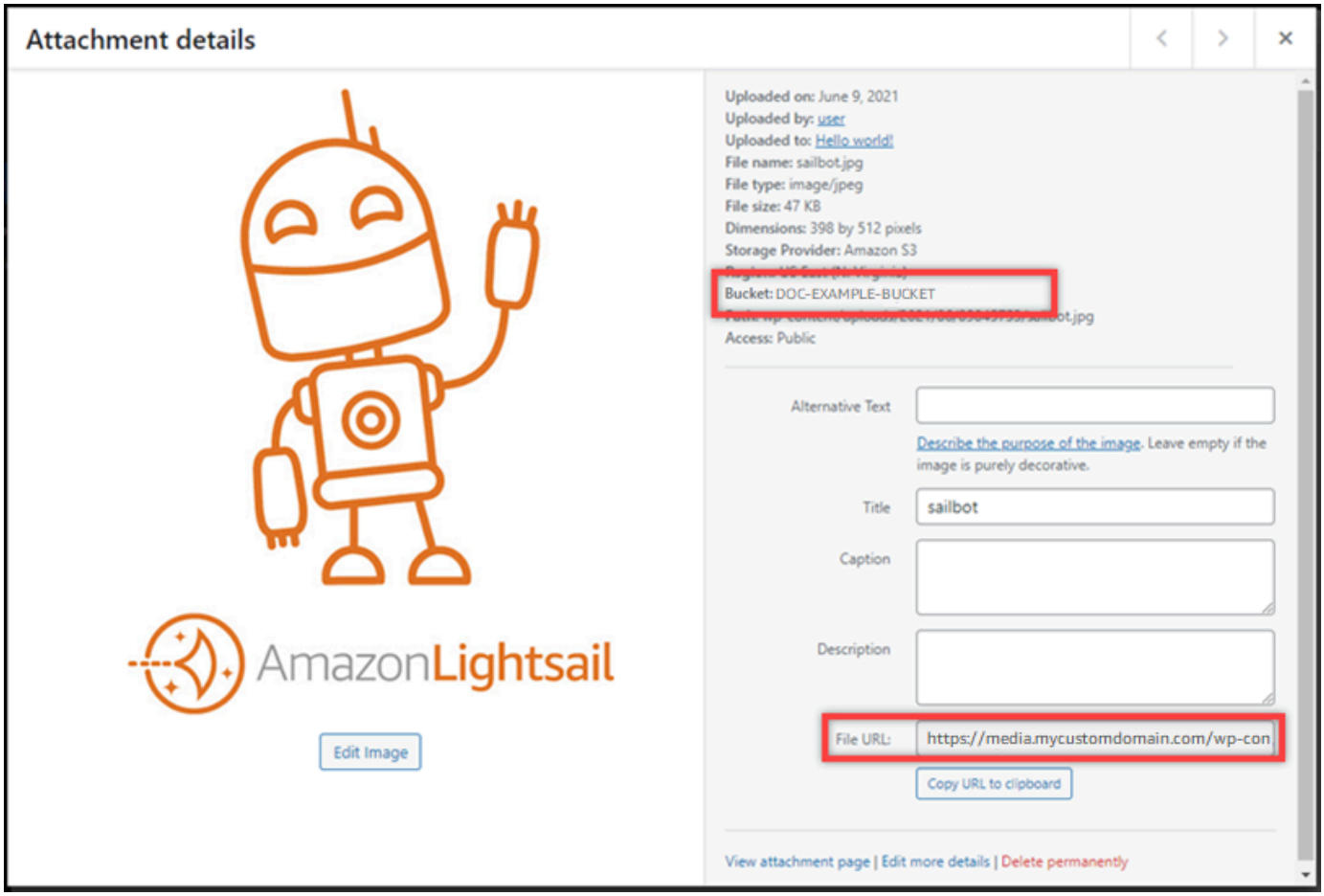
4. 文件完成上传后，在左侧导航菜单的媒体下方选择库。



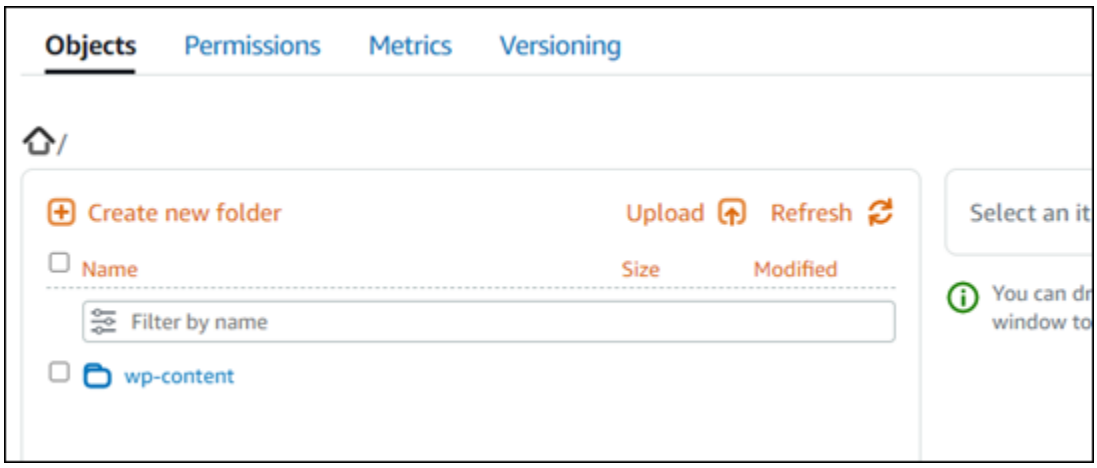
5. 选择您最近上传的文件。



6. 在文件的详细信息面板中，存储桶的名称会显示在存储桶字段中。分配的 URL 将显示在文件URL字段中。



7. 如果你前往 Lightsail 存储分区管理页面的 “对象” 选项卡，你应该会看到一个 w p-content 文件夹。此文件夹由 Offload Media Lite 插件创建，用于存储您上传的媒体文件。



管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 在 Amazon Lightsail 中封锁存储桶的公开访问权限
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。

- 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
- Amazon Lightsail 对象存储服务中存储桶的访问日志格式
- 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
- 使用 Amazon Lightsail 中存储段的访问日志来识别请求

6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象
9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

调整 Lightsail 发行版的数据传输配额

创建 Amazon Lightsail 分配时，您需要选择一个指定每月数据传输配额和分配费用的分配计划。如果分配传输的数据超过计划的每月数据传输配额，则会向您收取超额费用。有关超额定价的更多信息，请参阅 Lightsail 定价页面。

为避免超额费用，请将分配的当前计划更改为不同的计划，以在分配超出每月配额之前提供更大的每月数据传输量。在每个 AWS 计费周期内，您只能更改一次分配的计划。在本指南中，我们将介绍如何更改分配的计划。

有关分配的更多信息，请参阅内容分发网络分配。

更改分配计划

完成以下过程以更改分配的计划。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要查看其当前每月数据传输信息的分配的名称。
4. 在分配的管理页面上选择详细信息选项卡。
5. 在页面的数据传输部分，选择更改分配计划。
6. 对于确认提示，选择是，重置以确认您要更改分配的计划。
7. 在下一个提示中，为分配选择新计划，然后选择选择计划。
8. 在下一个提示中，选择是，应用以确认您要将新计划应用于分配。或者选择否，返回而不将新计划应用于分配。

使用自定义域名为你的 Lightsail 发行版提供内容

为您的 Amazon Lightsail 分发启用自定义域名，以便在分配中使用您的注册域名。
在启用自定义域之前，您的分配仅接受在您首次创建分配时与之关联的默认域（例如，`123456abcdef.cloudfront.net`）的流量。启用自定义域名时，必须选择为要用于分发的域名创建的 Lightsail SSL/TLS 证书。启用自定义域后，您的分配将接受与所选证书关联的所有域的流量。

> **Important**
>
> 每个分配一次只能使用一个证书。如果您在分配中禁用自定义域，则您的分配将无法再处理已注册域的 HTTPS 流量，直至您重新启用自定义域。
> 所有 Amazon Web Services (AWS) 账户中的其他分配（包括亚马逊服务上的分配）都不能使用与 SSL/TLS 证书关联的域名。 CloudFront您可以为域创建证书，但您将无法将其用于您的分配。

有关分配的更多信息，请参阅内容分发网络分配。

先决条件

在开始之前，你需要创建一个 Lightsail 发行版。有关更多信息，请参阅创建分配。

您还应为分配创建并验证 SSL/TLS 证书。有关更多信息，请参阅创建分配的 SSL/TLS 证书和验证分配的 SSL/TLS 证书。

启用分配的自定义域

完成以下过程以启用分配的自定义域。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其启用自定义域的分配名称。
4. 在分配的管理页面上选择自定义域选项卡。
5. 选择附加证书。

   如果您没有证书，则必须首先创建和验证域的 SSL/TLS 证书，然后才能将证书附加到您的分配。有关更多信息，请参阅创建分配的 SSL/TLS 证书。
6. 在显示的下拉菜单中，为要用于分配的域选择有效证书。
7. 验证证书信息是否正确，然后选择 Attach（附加）。
8. 分配的 Status（状态）将更改为 Updating（正在更新）。在状态变为 Enabled（已启用）后，证书的域将在 Custom domains（自定义域）部分中显示。
9. 选择 Add domain assignment（添加域分配）将域指向您的分配。
10. 验证证书和 DNS 信息是否正确，然后选择 Add assignment（添加分配）。稍等片刻，您选择的域的流量将开始被分配接受。

主题

- 将自定义域名指向 Lightsail 发行版
- 更新 Lightsail 发行版的 SSL/TLS 证书域
- 禁用 Lightsail 发行版的自定义域名
- 将分配的默认域添加到 Lightsail 容器服务

将自定义域名指向 Lightsail 发行版

在为分配启用自定义域名后，您必须将注册的域名指向您的 Amazon Lightsail 分配。您可以通过将别名记录添加到用于分配的证书上指定的每个域的 DNS 区域中，来执行此操作。您添加的所有记录都应该指向分配的默认域（例如 `123456abcdef.cloudfront.net`）。

在本指南中，我们为您提供了使用 Lightsail DNS 区域将您的域名指向您的发行版的程序。使用其他 DNS 托管服务提供商（例如 Domain.com 或 GoDaddy）将您的域名指向您的分发的程序可能类似。有关 Lightsail DNS 区域的更多信息，请参阅 DNS。

有关分配的更多信息，请参阅创建分配。

内容

- 步骤 1：完成先决条件
- 步骤 2：获取分配的默认域
- 步骤 3：将记录添加到域的 DNS 记录

步骤 1：完成先决条件

在开始之前，您应该为 Lightsail 发行版启用自定义域名。有关更多信息，请参阅启用分配的自定义域。

步骤 2 ：获取分配的默认域

完成以下过程以获取分配的默认域名，您可以在将别名记录添加到域的 DNS 中时指定该域名。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要获取默认域名的分配名称。

4. 在分配管理页面的标题部分，记下分配的默认域名。分配的默认域名类似于 `123456abcdef.cloudfront.net`。

   您必须将此值添加为域的 DNS 中的别名记录的一部分。我们建议您将此值复制并粘贴到文本文件中，以供之后参考。继续本教程中接下来的步骤 3：将记录添加到域的 DNS 区域部分。

步骤 3：将记录添加到域的 DNS 记录

完成以下步骤以将记录添加到您所在域的 DNS 区域。

1. 在左侧导航窗格中，选择域和 DNS。
2. 在页面的 DNS 区域部分下方，选择要添加记录的域名，以将域的流量引导到您的分配。
3. 选择 DNS records（DNS 记录）选项卡。然后，选择 Add record（添加记录）。
4. 根据您要指向分配的域类型，完成以下步骤之一：

   - 选择一个地址 (A) 记录以将顶级域（例如 `example.com`）指向您的分配。

     如果顶级域的 A 记录已存在于您的 DNS 区域中，则您需要编辑该现有记录，而不是添加另一个 A 记录。

   - 选择一个规范名称（CNAME）以将子域（例如 `website.example.com`）指向您的分配。

5. 如果要添加 A 记录，则在解析到文本框中选择分配的名称。如果要添加别名记录，则在映射到文本框中输入分配的默认域名。

   > **Note**
   >
   > 当您将 A 记录添加到 DNS 区域并选择分配的名称时，实际上是在添加别名记录，该记录与地址记录不同。Lightsail 使您可以轻松添加别名记录，而无需执行其他 DNS 托管提供商通常需要的额外步骤。

6. 选择保存图标以将记录保存到 DNS 区域。

   重复这些步骤，为您用于分配的证书上的域添加其他 DNS 记录。留出时间以便更改通过 Internet 的 DNS 传播。几分钟后，您应能够查看您的域是否指向您的分配。您还应该测试您的分配。有关更多信息，请参阅下面的测试分配。

更新 Lightsail 发行版的 SSL/TLS 证书域

您可以将您的 Amazon Lightsail 分配使用的自定义域名更改为另一个域名或一组域名。为此，您必须首先为要用于分配的域创建新的 SSL/TLS 证书。有关更多信息，请参阅创建分配的 SSL/TLS 证书。验证新证书后，将旧证书交换为新证书，从而更改分配的自定义域。

有关分配的更多信息，请参阅创建分配。

更改分配的自定义域

完成以下过程以更改分配的自定义域。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其更改默认自定义域的分配名称。
4. 在分配的管理页面上选择自定义域选项卡。
5. 分离当前附加到分配的 SSL/TLS 证书。

   分配的状态将更改为 In progress（正在进行）。
6. 分配的状态变回 Enabled（已启用）后，选择 Attach certificate（附加证书）。
7. 在显示的下拉菜单中，为要用于分配的域选择有效证书。
8. 验证证书信息是否正确，然后选择 Attach（附加）。
9. 向域的 DNS 添加域分配，以将域指向分配。

   分配的 Status（状态）将更改为 Updating（正在更新）。将状态更改为 Ready（就绪）后，证书的域将在 Custom domains（自定义域）部分中显示。选择 Add domain assignment（添加域分配）将域指向您的分配。
10. 选择 Add assignment（添加分配）。稍等片刻，您选择的域的流量将开始被分配接受。
11. 选择保存。

禁用 Lightsail 发行版的自定义域名

禁用您的 Amazon Lightsail 分发的自定义域名，以停止在分配中使用您的注册域名。禁用自定义域后，您的分配将仅接受在您首次创建分配时与之关联的默认域（例如，`123456abcdef.cloudfront.net`）的流量，对于之前关联的自定义域的流量，将显示 403 错误。

有关分配的更多信息，请参阅内容分发网络分配。

禁用分配的自定义域

完成以下过程以禁用分配的自定义域。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要禁用自定义域的分配名称。
4. 在分配的管理页面上选择自定义域选项卡。

   Custom domains（自定义域）页面显示当前附加到分配的 SSL/TLS 证书（如果有）。
5. 请选择以下选项之一：

   1. 选择 Configure distribution domains（配置分配域）取消选择之前选定的域，或选择更多与分配关联的域。
   2. 选择分离将证书从分配中分离，再删除其所有关联的域。
6. 将提交禁用自定义域的请求，并且分配的状态将更改为正在进行。过段时间以后，分配状态将更改为已启用。

禁用自定义域后，您的分配将仅接受在您首次创建分配时与之关联的默认域（例如，`123456abcdef.cloudfront.net`）的流量，对于之前关联的自定义域的流量，将显示 403 错误。您应更新域的 DNS 记录，以便将这些域的流量引导到另一个资源。

将分配的默认域添加到 Lightsail 容器服务

您可以选择 Amazon Lightsail 容器服务作为内容分发网络 (CDN) 分发的来源。然后，该分配会缓存并提供您的容器服务上托管的网站或 Web 应用程序。如果你在 Lightsail 容器服务中使用 Lightsail 发行版，Lightsail 会自动将你的分配的默认域名作为自定义域添加到你的容器服务上。这使流量能够在您的分配和容器服务之间进行路由。但是，您必须在以下情况下，执行本指南中概述的步骤，将分配的原定设置域名手动添加到容器服务中：

- 如果出现问题且您分配的原定设置域名不会自动添加到容器服务中。
- 如果您在容器服务中使用了 Lightsail 发行版以外的发行版。

您只能使用 AWS Command Line Interface (AWS CLI) 将分配的默认域名手动添加到容器服务。有关容器服务的更多信息，请参阅容器服务。有关分配的更多信息，请参阅对象存储。

将分配的原定设置域添加到容器服务

完成以下过程，使用 AWS Command Line Interface ()AWS CLI将分配的默认域添加到 Lightsail 中的容器服务。使用 `update-container-service` 命令完成此操作。有关更多信息，请参阅 AWS CLI 命令参考 中的 update-container-service。

> **Note**
>
> 在继续执行此过程之前，必须为 Lightsail 安装 AWS CLI 并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令之一以将分配的原定设置域添加到容器服务。

   > **Note**
   >
   > 如果您将自定义域添加到容器服务中，则需要同时指定自定义域和分配的原定设置域。

   容器服务上没有配置自定义域：

   ```
   aws lightsail update-container-service --service-name ContainerServiceName --
   public-domain-names '{"_": ["DistributionDefaultDomain"]}'
   ```

   容器服务上没有配置一个或多个自定义域：

   ```
   aws lightsail update-container-service --service-name ContainerServiceName
    --public-domain-names '{"CertificateName": ["ExistingCustomDomain"],"_":
    ["DistributionDefaultDomain"]}'
   ```

   在该命令中，将以下示例文本替换为自己的文本：

   - *ContainerServiceName*-指定为发行版来源的 Lightsail 容器服务的名称。
   - *DistributionDefaultDomain*-使用容器服务作为来源的分配的默认域。例如，`example123.cloudfront.net`。
   - *CertificateName*“-当前附加到容器服务的自定义域名的 Lightsail 证书的名称（如果有）。如果没有附加到容器服务的自定义域，则使用标记为容器服务上未配置自定义域的命令。

- *DistributionDefaultDomain*-当前附加到容器服务的自定义域。

示例：

- 容器服务上没有配置自定义域：

```
aws lightsail update-container-service --service-name ContainerServiceName --
public-domain-names '{"_": ["example123.cloudfront.net"]}'
```

- 容器服务上没有配置一个或多个自定义域：

```
aws lightsail update-container-service --service-name ContainerServiceName
 --public-domain-names '{"example-com": ["example.com"],"_":
 ["example123.cloudfront.net"]}'
```

管理 Lightsail 发行版的请求和响应行为

在本指南中，我们描述了您的 Amazon Lightsail 配送在处理请求并将其转发到您的来源以及处理来自您的来源的响应时的行为方式。有关分配的更多信息，请参阅内容分发网络分配。

主题

- 分配如何处理请求并将请求转发到源
- 分配如何处理来自源的响应

分配如何处理请求并将请求转发到源

本部分包含有关分配如何处理查看器请求并将请求转发到源的信息。

内容

- 身份验证
- 缓存持续时间
- 客户端 IP 地址
- 客户端 SSL 身份验证
- 压缩
- 有条件请求

- Cookie
- 跨源资源共享 (CORS)
- 加密
- 包含正文的 GET 请求
- HTTP 方法
- HTTP 请求标头和分配行为
- HTTP 版本
- 请求的最大长度与 URL 的最大长度
- OCSP Stapling
- 持久性连接
- 协议
- 查询字符串
- 源连接超时和尝试次数
- 源响应超时
- 同一对象的并行请求 (流量高峰)
- User-agent 标头

身份验证

对于 DELETE、GET、HEAD、PATCH、POST 和 PUT 请求，如果配置分配以将 Authorization 标头转发到源，您可以将源服务器配置为请求客户端身份验证。

对于 OPTIONS 请求，您可以将源服务器配置为仅在使用以下分配设置时请求客户端身份验证：

- 配置分配以将 Authorization 标头转发到源。
- 配置分配以不缓存对 OPTIONS 请求的响应。

您可以配置分配以使用 HTTP 或 HTTPS 将请求转发到源。

缓存持续时间

要控制对象在分配缓存中保留多长时间后分配将另一请求转发到源，您可以：

- 配置您的源，以将 Cache-Control 或 Expires 标题字段添加到每个对象。

- 对缓存寿命 (TL) 使用默认值 1 天。

有关更多信息，请参阅分配高级设置。

客户端 IP 地址

如果查看器将请求发送到您的分配并且不包含 X-Forwarded-For 请求标头，您的分配将通过 TCP 连接获取查看器的 IP 地址，添加包含该 IP 地址的 X-Forwarded-For 标头，并将请求转发到源。例如，如果您的分配通过 TCP 连接获取 IP 地址 192.0.2.2，则它将以下标头转发到源：

```
X-Forwarded-For: 192.0.2.2
```

如果查看器将请求发送到您的分配并且包含 X-Forwarded-For 请求标头，分配将通过 TCP 连接获取查看器的 IP 地址，将该 IP 地址附加到 X-Forwarded-For 标头的末尾，并将请求转发到源。例如，如果查看器请求包含 X-Forwarded-For: 192.0.2.4,192.0.2.3，并且您的分配通过 TCP 连接获取 IP 地址 192.0.2.2，则它将以下标头转发到源：

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

一些应用程序（例如，负载均衡器、Web 应用程序防火墙、反向代理、入侵防御系统以及 API Gateway）会将转发请求的分配边缘服务器的 IP 地址附加到 X-Forwarded-For 标头的末尾。例如，如果您的分配在它转发到 ELB 的请求中包含 X-Forwarded-For: 192.0.2.2，并且分配边缘服务器的 IP 地址为 192.0.2.199，则您的实例收到的请求会包含以下标头：

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

> **Note**
>
> X-Forwarded-For标头包含 IPv4 地址（例如 192.0.2.44）和 IPv6 地址（例如 2001:0 db 8:85 a 3:0000:00:8 a2e：0370:7334）。

客户端 SSL 身份验证

Lightsail 发行版不支持使用客户端 SSL 证书进行客户端身份验证。如果源请求客户端证书，则您的分配将删除请求。

压缩

Lightsail 分发会转发具有Accept-Encoding字段值"identity"和的请求。"gzip"

有条件请求

在您的分配从边缘缓存中收到已过期的对象的请求时，它将请求转发到源以获取对象的最新版本，或者从源中获得分配边缘缓存已具有最新版本的确认。通常，在源最后将对象发送到您的分配时，它在响应中包含 ETag 值和/或 LastModified 值。在您的分配转发到源的新请求中，您的分发将添加以下一项或两项：

- If-Match 或 If-None-Match 标头，其中包括对象过期版本的 ETag 值。
- If-Modified-Since 标头，其中包含对象过期版本的 LastModified 值。

源使用该信息来确定对象是否已更新，以及是否将整个对象返回到您的分配或只返回 HTTP 304 状态代码 (Not Modified)。

Cookie

您可以配置您的分配以将 Cookie 转发到源。有关更多信息，请参阅分配高级设置。

跨源资源共享 (CORS)

如果您希望您的分配采用跨源资源共享设置，请配置源以将 Origin 标头转发到源。

加密

您可以要求查看器使用 HTTPS 连接到您的分配，并要求您的分配使用 HTTP 或 HTTPS 将请求转发到源。

您的分配使用 SSLv3、 TLSv1 .0、. TLSv1 1 和. TLSv1 2 协议将 HTTPS 请求转发到您的源。不支持其他版本的 SSL 和 TLS。

包含正文的 GET 请求

如果查看器 GET 请求包含正文，则您的分配会将 HTTP 状态代码 403 (Forbidden) 返回到查看器。

HTTP 方法

如果您将您的分配配置为允许其支持的所有 HTTP 方法，则分配会接受来自查看器的以下请求，并将这些请求转发到您的源：

- DELETE

- GET
- HEAD
- OPTIONS
- PATCH
- POST
- PUT

分配会始终缓存对 GET 和 HEAD 请求的响应。您也可以将分配配置为缓存对 OPTIONS 请求的响应。分配不缓存对使用其他方法的请求的响应。

有关如何配置是否让源处理这些方法的信息，请参阅该源的文档。

> **Important**
>
> 如果将分配配置为接受其支持的所有 HTTP 方法并将这些方法转发到源，请配置源服务器以处理所有方法。例如，如果因为您想使用 POST 而将分配配置为接受并转发这些方法，则必须将您的源服务器配置为适当处理 DELETE 请求，以便查看器无法删除您不希望其删除的资源。有关更多信息，请参阅您的 HTTP 服务器的文档。

HTTP 请求标头和分配行为

下表列出了 HTTP 请求标头，您可以将其转发到源 (有例外情况需要注意)。对于每个标头，该列表会包含有关以下内容的信息：

- 支持 - 您是否能将分配配置为根据标头的标头值缓存对象。

  您可以将分配配置为根据 Date 和 User-Agent 标头中的值缓存对象，但我们建议您不要这样做。这些标头具有许多可能的值，并且基于其值的缓存操作会导致分配将更多请求转发到源。
- 未配置时的行为 - 未配置分配以将标头转发到源（这会导致分配根据标头值缓存您的对象）时的分配行为。

- 标头 - 其他定义的标头

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Accept

  支持 - 是

  未配置时的行为 - 分配将删除标头。

- 标头 - Accept-Charset

  支持 - 是

  未配置时的行为 - 分配将删除标头。

- 标头 - Accept-Encoding

  支持 - 是

  未配置时的行为 - 如果值包含 gzip，分配会将 Accept-Encoding: gzip 转发到源。如果值不包含 gzip，在将请求转发到源之前， 分配会删除 Accept-Encoding 标头字段。

- 标头 - Accept-Language

  支持 - 是

  未配置时的行为 - 分配将删除标头。

- 标头 - Authorization

  支持 - 是

  未配置时的行为：

  - GET 和 HEAD 请求 – 在将请求转发到源之前，分配将删除 Authorization 标头字段。
  - OPTIONS 请求 – 如果您将分配配置为缓存对 OPTIONS 请求的响应，则在将请求转发到源之前，分配将删除 Authorization 标头字段。

    如果未将分配配置为缓存 OPTIONS 请求的响应，则分配将 Authorization 标头字段转发到源。

  - DELETE、PATCH、POST 和 PUT 请求 – 在将请求转发到源之前，分配不会删除标头字段。

- 标头 - Cache-Control

  支持 - 否

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - CloudFront-Forwarded-Proto

支持 - 是

未配置时的行为 - 在将请求转发到源之前，分配不会添加标头。

- 标头 - CloudFront-Is-Desktop-Viewer

  支持 - 是

  未配置时的行为 - 在将请求转发到源之前，分配不会添加标头。

- 标头 - CloudFront-Is-Mobile-Viewer

  支持 - 是

  未配置时的行为 - 在将请求转发到源之前，分配不会添加标头。

- 标头 - CloudFront-Is-Tablet-Viewer

  支持 - 是

  未配置时的行为 - 在将请求转发到源之前，分配不会添加标头。

- 标头 - CloudFront-Viewer-Country

  支持 - 是

  未配置时的行为 - 在将请求转发到源之前，分配不会添加标头。

- 标头 - Connection

  支持 - 否

  未配置时的行为 - 在将请求转发到源之前，分配不会将此标头替换为 Connection: Keep-Alive。

- 标头 - Content-Length

  支持 - 否

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Content-MD5

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Content-Type

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Cookie

  支持 - 否

  未配置时的行为 - 如果将分配配置为转发 Cookie，则它会将 Cookie 标头字段转发到源。如果没有进行此配置，则分配会删除 Cookie 标头字段。

- 标头 - Date

  支持 - 是，但建议不要这样做

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Expect

  支持 - 是

  未配置时的行为 - 分配将删除标头。

- 标头 - From

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Host

  支持 - 是

  未配置时的行为 - 分配将值设置为与请求的对象关联的源的域名。

- 标头 - If-Match

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - If-Modified-Since

  支持 - 是

未配置时的行为 - 分配会将标头转发到源。

- 标头 - If-None-Match

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - If-Range

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - If-Unmodified-Since

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Max-Forwards

  支持 - 否

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Origin

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Pragma

  支持 - 否

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Proxy-Authenticate

  支持 - 否

  未配置时的行为 - 分配将删除标头。

- 标头 - Proxy-Authorization

  支持 - 否

未配置时的行为 - 分配将删除标头。

- 标头 - Proxy-Connection

  支持 - 否

  未配置时的行为 - 分配将删除标头。

- 标头 - Range

  支持 - 是（默认值）

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Referer

  支持 - 是

  未配置时的行为 - 分配将删除标头。

- 标头 - Request-Range

  支持 - 否

  未配置时的行为-> 分配会将标头转发到源。

- 标头 - TE

  支持 - 否

  未配置时的行为 - 分配将删除标头。

- 标头 - Trailer

  支持 - 否

  未配置时的行为 - 分配将删除标头。

- 标头 - Transfer-Encoding

  支持 - 否

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Upgrade

  支持-否（ WebSocket连接除外）

行为（如果未配置）-除非您已建立 WebSocket 连接，否则您的分发会删除标题。

- 标头 - User-Agent

  支持 - 是，但建议不要这样做

  未配置时的行为 - 分配会将此标头字段的值替换为 Amazon CloudFront。

- 标头 - Via

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - Warning

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - X-Amz-Cf-Id

  支持 - 否

  未配置时的行为 - 在将请求转发到源之前，分配会将标头添加到查看器请求。标头值包含一个用于唯一标识请求的加密字符串。

- 标头 - X-Edge-*

  支持 - 否

  未配置时的行为 - 分配将删除所有 X-Edge-* 标头。

- 标头 - X-Forwarded-For

  支持 - 是

  未配置时的行为 - 分配会将标头转发到源。

- 标头 - X-Forwarded-Proto

  支持 - 否

  未配置时的行为 - 分配将删除标头。

- 标头 - X-Real-IP

支持 - 否

未配置时的行为 - 分配将删除标头。

HTTP 版本

分配使用 HTTP/1.1 将请求转发到自定义源。

请求的最大长度与 URL 的最大长度

请求的最大长度，包括路径、查询字符串（如果有）以及标头，是 20480 个字节。

分配将根据请求来构造 URL。此 URL 的最大长度是 8192 个字节。

如果请求或 URL 超出这些最大值，则分配将 HTTP 状态代码 413（请求实体过大）返回到查看器，然后终止与查看器的 TCP 连接。

OCSP Stapling

当查看器提交对象的 HTTPS 请求时，分配或查看器必须与证书颁发机构 (CA) 确认尚未吊销域的 SSL 证书。OCSP Stapling 允许分配验证证书并缓存来自 CA 的响应，这将使客户端无需直接向 CA 验证证书，从而加快证书验证速度。

当分配收到对同一域中对象的大量 HTTPS 请求时，OCSP Stapling 的性能改进会更明显。分配边缘站点中的每个服务器必须提交一个单独的验证请求。在分配收到同一域的大量 HTTPS 请求时，边缘站点中的每个服务器很快将收到来自 CA 的响应，指出它可以在 SSL 握手中“固定”到一个数据包；在查看器认为证书有效时，分配可以提供请求的对象。如果您的分配未在分配边缘站点中产生大量流量，则新请求更有可能定向到尚未向 CA 验证证书的服务器。在这种情况下，查看器将单独执行验证步骤，并且分配服务器将提供对象。该分配服务器还会向 CA 提交验证请求，因此，在它下次收到包含同一域名的请求时，便已获得来自 CA 的验证响应。

持久性连接

当分配收到来自源的响应时，它会尝试将连接保持几秒钟，以防在此时段内有另一个请求到达。保持持久性连接可节省重新建立 TCP 连接以及针对后续请求再次进行 TLS 握手所需的时间。

协议

您的发行版根据 Lightsail 控制台中的 Origin 协议策略字段的值将 HTTP 或 HTTPS 请求转发到源服务器。在 Lightsail 控制台中，选项仅限 HTTP，仅限 HTT P S。

如果您指定仅 HTTP 或仅 HTTPS，则分配仅使用指定的协议将请求转发到源，而不考虑查看器请求中的协议。

> **Important**
>
> 如果分配使用 HTTPS 协议将请求转发到源，并且源服务器返回无效的证书或自签名证书，分配将中断 TCP 连接。

查询字符串

您可配置分配是否将查询字符串参数转发到源。

源连接超时和尝试次数

默认情况下，分配在将错误响应返回给查看器之前等待长达 30 秒（3 次尝试，每次 10 秒）。

源响应超时

源响应超时（也称为源读取超时 或源请求超时）同时适用于以下两种情况：

- 分配在将请求转发到源后等待响应的时间长度（以秒为单位）。
- 分配从收到来自源的响应的一个数据包到收到下一个数据包之间等待的时间长度（以秒为单位）。

分配的行为取决于查看器请求的 HTTP 方法：

- GET 和 HEAD 请求 – 如果源在响应超时的持续时间内没有响应或停止响应，则分配会中断连接。如果指定的源连接尝试次数超过 1 次，分配将再次尝试获取完整响应。分配最多尝试 3 次，具体取决于源连接尝试次数 设置的值。如果源在最终尝试期间未响应，则在收到对同一个源上的内容的其他请求之前，分配都不会重试。
- DELETE、OPTIONS、PATCH、PUT 和 POST 请求 – 如果源在 30 秒内未做出响应，分配将中断连接并且不会再次尝试联系源。如有必要，客户端可以重新提交请求。

同一对象的并行请求 (流量高峰)

如果分配边缘站点收到对象的请求，并且对象当前没有位于缓存中或对象已过期，则分配会立即将请求发送到源。如果遇到流量高峰（即，在源响应第一个请求之前，针对同一对象的其他请求到达边缘站

点），分配先短暂中止，然后再将对象的其他请求转发到源。通常，对第一个请求的响应会在对后续请求的响应之前到达分配边缘站点。此短暂中止有助于减少源服务器上的不必要负载。如果其他请求不完全相同（例如，由于将分配配置为根据请求标头或 Cookie 进行缓存），则分配会将所有唯一请求转发到源。

User-agent 标头

如果您希望分配基于用户用来查看内容的设备缓存不同版本的对象，建议您将分配配置为将一个或多个以下标头转发到源：

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

根据 `User-Agent` 标头的值，在将请求转发到源之前，分配会将这些标头的值设置为 `true` 或 `false`。如果某个设备归入多个类别中，则多个值可能为 `true`。例如，对于一些平板电脑设备，分配可能将 `CloudFront-Is-Mobile-Viewer` 和 `CloudFront-Is-Tablet-Viewer` 设置为 `true`。

您可以将分配配置为根据 `User-Agent` 标头中的值缓存对象，但我们建议您不要这样做。`User-Agent` 标头具有许多可能的值，并且根据这些值的缓存操作会导致分配将更多请求转发到源。

如果未将分配配置为根据 `User-Agent` 标头中的值缓存对象，在将请求转发到源之前，分配将添加具有以下值的 `User-Agent` 标头：

```
User-Agent = Amazon CloudFront
```

无论来自查看器的请求是否包含 `User-Agent` 标头，分配都会添加该标头。如果来自查看器的请求包含 `User-Agent` 标头，分配将删除该标头。

分配如何处理来自源的响应

本部分包含分配如何处理来自源的响应的相关信息。

内容

- 100-Continue 响应
- 缓存

- 已取消的请求
- 内容协商
- Cookie
- 中断的 TCP 连接
- 分配删除或替换的 HTTP 响应标头
- 最大文件大小
- 源不可用
- 重新导向
- 传输编码

100-Continue 响应

源不能向分配发送多个 100-Continue 响应。在第一个 100-Continue 响应之后，分配需要 HTTP 200 OK 响应。如果源在第一个 100-Continue 响应之后又发送了该响应，分配将返回错误。

缓存

- 确保源为 `Date` 和 `Last-Modified` 标头字段设置有效、准确的值。
- 如果来自查看器的请求包含 `If-Match` 或 `If-None-Match` 请求标头字段，请设置 `ETag` 响应标头字段。如果未指定 `ETag` 值，分配将忽略随后的 `If-Match` 或 `If-None-Match` 标头。
- 分配通常采用来自源的响应中的 `Cache-Control: no-cache` 标头。有关例外的信心，请参阅同一对象的并行请求（流量高峰）。

已取消的请求

如果对象没有位于边缘缓存中，或者在分配从源中获取对象后，查看器便终止了会话（例如，关闭浏览器）而没来得及传送请求的对象，则分配不会将该对象缓存在边缘站点中。

内容协商

如果您的源在响应中返回 `Vary:*`，并且相应缓存行为的最小 TTL 的值为 0，则分配将缓存对象，但仍会将对象的每个后续请求转发到源以确认缓存包含最新版本的对象。分配不包含任何条件标头，例如 `If-None-Match` 或 `If-Modified-Since`。因此，源会将对象返回到分配以响应每个请求。

如果您的来源在响应`Vary:*`中返回，并且相应缓存行为的最小 TTL 值为任何其他值，则会按照分配删除或替换的 HTTP 响应标`Vary`头中所述 CloudFront 处理标头。

Cookie

如果您为缓存行为启用了 Cookie，并且如果源返回带对象的 Cookie， 则分配将缓存对象和 Cookie。请注意，这降低了对象的缓存能力。

中断的 TCP 连接

在源将对象返回到分配时，如果分配和源之间的 TCP 连接中断， 分配行为将取决于源是否在响应中包含 `Content-Length` 标头：

- Content-Length 标头 – 分配在从源中获取对象时，会将对象返回到查看器。但是，如果 `Content-Length` 标头值与对象大小不匹配，则分配不会缓存对象。
- Transfer-Encoding: Chunked – 分配在从源中获取对象时，会将对象返回到查看器。但是，如果分块响应未完成，则分配不会对该对象进行缓存。
- 无 Content-Length 标头 – 分配将对象返回到查看器并进行缓存，但该对象可能不完整。在无 `Content-Length` 标头的情况下，分配无法确定 TCP 连接是偶然中断还是有意中断。

我们建议您配置您的 HTTP 服务器，以添加 `Content-Length` 标头，防止分配缓存部分对象。

分配删除或替换的 HTTP 响应标头

在将来自源的响应转发到查看器之前，分配将删除或更新以下标头字段：

- `Set-Cookie` – 如果将分配配置为转发 Cookie，则会将 `Set-Cookie` 标头字段转发到客户端。
- `Trailer`
- `Transfer-Encoding` – 如果源返回该标头字段，在将响应返回到查看器之前，分配会将值设置为 `chunked`。
- `Upgrade`
- `Vary` – 请注意以下几点：
  - 如果您将分配配置为将任何设备特定的标头转发到您的源 (`CloudFront-Is-Desktop-Viewer`、`CloudFront-Is-Mobile-Viewer`、`CloudFront-Is-SmartTV-Viewer`、`CloudFront-Is-Tablet-Viewer`)，并且您将源配置为将 `Vary:User-Agent` 返回给分配，则分配会将 `Vary:User-Agent` 返回给查看器。
  - 如果配置源以将 `Accept-Encoding` 或 `Cookie` 包含在 `Vary` 标头中，则分配会将这些值包含在对查看器的响应中。

  - 如果配置分配以将标头的允许列表转发到源，并且配置源以将标头名返回到 Vary:Accept-Charset,Accept-Language 标头（如 Vary）中的分配，则分配会将具有这些值的 Vary 标头返回到查看器。
  - 有关分配如何处理 Vary 标头中的 * 值的信息，请参阅内容协商。
  - 如果配置源以将任何其他值包含在 Vary 标头中，在将响应返回到查看器之前，分配将删除这些值。
- Via – 在对查看器的响应中，分配会将值设置为以下内容：

  Via: *http-version alphanumeric-string*.cloudfront.net (CloudFront)

  例如，如果客户端通过 HTTP/1.1 发出请求，该值类似于如下所示：

  Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)

最大文件大小

分配将返回到查看器的响应正文最大为 20 GB 大小。这包括未指定 Content-Length 标头值的分块传输响应。

源不可用

如果源服务器不可用，并且分配收到位于边缘缓存中但已过期的对象的请求（例如，由于在 Cache-Control max-age 指令中指定的期限已过），分配将提供该对象的已过期版本或提供自定义错误页面。

某些情况下，将逐出很少被请求的对象且不再在边缘缓存中提供。分配不能提供已被逐出的对象。

重新导向

如果更改对象在源服务器上的位置，您可以配置 Web 服务器以重新导向请求到新位置。在您配置重新导向后，查看器第一次提交对象请求时， 分配会将请求发送到源，源则响应重新导向（例如 302 Moved Temporarily）。分配缓存重新导向并将其返回给查看器。您的分配不会遵照重新导向。

您可以配置 Web 服务器以将请求重新导向到以下位置之一：

- 对象在源服务器上的新 URL。在查看器进行重新导向以访问新的 URL 时，查看器将绕过分配，直接到达源。因此，我们建议您不要将请求重新导向到对象在源上的新 URL。

- 对象新的分配 URL。当查看器提交包含新分配 URL 的请求时，分配将从源上的新位置获取对象，并将其缓存在边缘站点中，然后将该对象返回到查看器。对象随后的请求将由边缘站点提供。这避免了查看器从源请求对象相关的延迟和负载。但是，对象的每个新请求将产生两个分配请求的费用。

传输编码

Lightsail 发行版仅支持标chunked题的Transfer-Encoding值。如果源返回 Transfer-Encoding: chunked，则分配在边缘站点中收到对象后将该对象返回到客户端，然后以分块格式缓存该对象以提供给后续请求。

如果查看器发出 Range GET 请求，并且源返回Transfer-Encoding: chunked ，则分配会将整个对象返回到查看器，而不是请求的范围。

如果无法预先确定响应的内容长度，建议您使用分块编码。有关更多信息，请参阅中断的 TCP 连接。

验证 Lightsail 发行版的内容缓存

在本指南中，您将学习如何测试您的 Amazon Lightsail 发行版是否正在缓存和提供来自您的来源的内容。在您将注册的域名添加到您的分配之后，您应该执行此测试。有关分配的更多信息，请参阅内容分发网络分配。

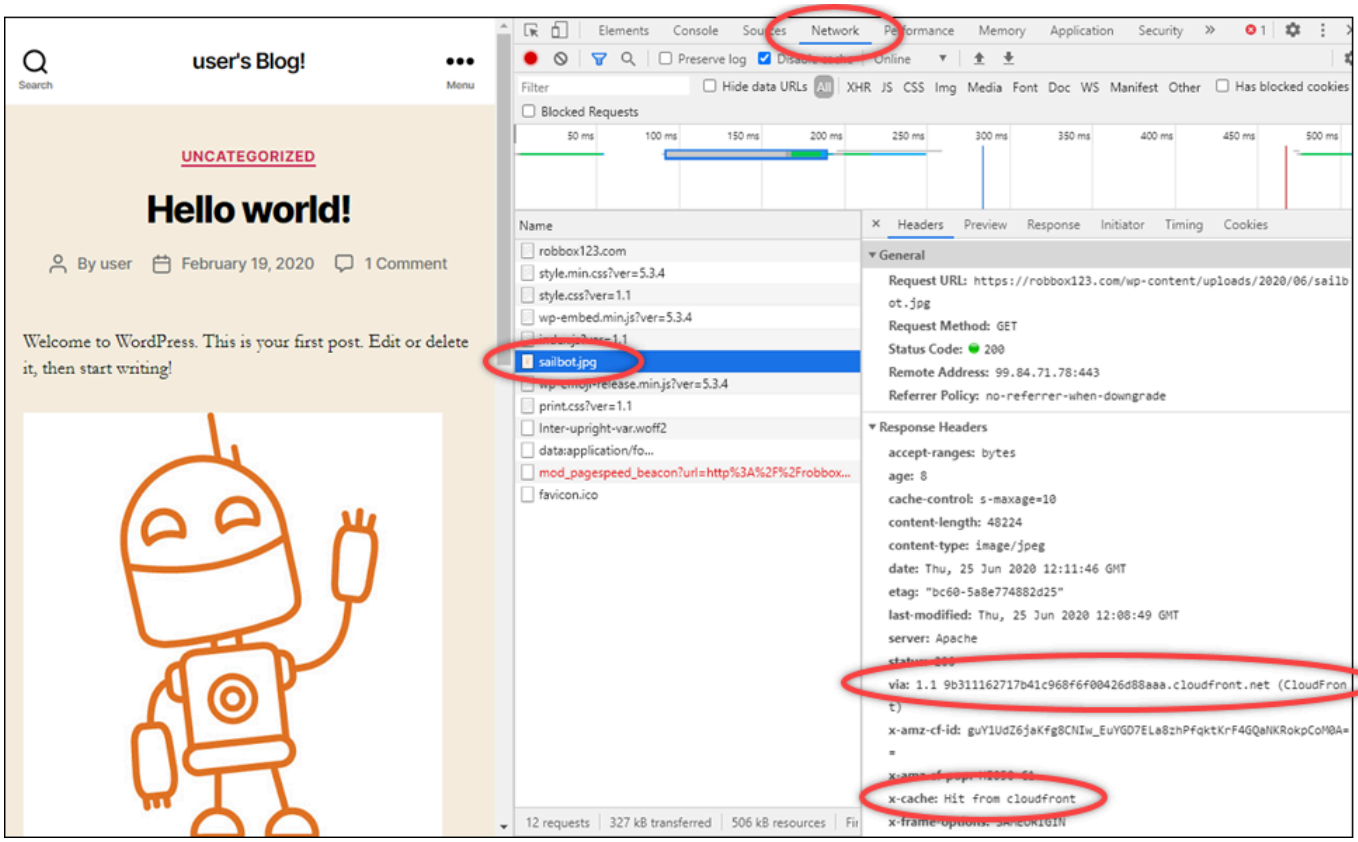
测试您的分配。

完成以下过程以测试您的分配。我们在此过程中使用 Chrome Web 浏览器；其他浏览器可能使用类似的步骤。

1. 打开 Chrome Web 浏览器。
2. 打开浏览器窗口一 upper-right-hand角的 Chrome 菜单，然后选择 “更多工具” > “开发者工具”。

   您也可以使用快捷方式选项 + ⌘ + J（在 macOS 上）或 Shift + CTRL + J（在 Windows /Linux 上）。
3. 在开发人员工具窗格中，选择网络选项卡。
4. 浏览到分配的域（例如 https://www.example.com)。

   在 Chrome 开发人员工具的网络选项卡中，应会填充您网站中的对象列表。
5. 选择静态对象，如图像文件（.jpg、.png、.gif）。
6. 在显示的标头面板中，您应该看到 via 和 x-cache 标头文件都提到 CloudFront。这就确认您的分配正在从源缓存和提供内容。


user's Blog!
Search
Menu
UNCATEGORIZED
Hello world!
By user
February 19, 2020
1 Comment
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!
Elements
Console
Network
Performance
Memory
Application
Security
Name
robbox123.com
style.min.css?ver=5.3.4
style.css?ver=1.1
wp-embed.min.js?ver=5.3.4
sailbot.jpg
print.css?ver=1.1
Inter-upright-var.woff2
favicon.ico
Headers
Preview
Response
Initiator
Timing
Cookies
General
Request URL: https://robbox123.com/wp-content/uploads/2020/06/sailbot.jpg
Request Method: GET
Status Code: 200
Remote Address: 99.84.71.78:443
Referrer Policy: no-referrer-when-downgrade
Response Headers
accept-ranges: bytes
age: 8
cache-control: s-maxage=10
content-length: 48224
content-type: image/jpeg
date: Thu, 25 Jun 2020 12:11:46 GMT
etag: "bc60-5a8e774882d25"
last-modified: Thu, 25 Jun 2020 12:08:49 GMT
server: Apache
via: 1.1 9b311162717b41c968f6f00426d88aaa.cloudfront.net (CloudFront)
x-amz-cf-id: guY1UdZ6jaKfg8CNIw_EuYGD7ELa8zhPfqktKrF4GQaNKRokpCoM0A==
x-cache: Hit from cloudfront
12 requests
327 kB transferred
506 kB resources

亚马逊 Lightsail 中的社交资源

Lightsail 网络资源改善了用户和外部服务连接到你的 Lightsail 实例的方式。

负载均衡器

您可以创建负载均衡器以添加冗余或处理更多流量。有关更多信息，请参阅负载均衡器。

静态 IPs

您可以创建静态 IP 地址，以便在每次重启实例时保留相同的 IP 地址。有关更多信息，请参阅静态 IP 地址。

查看和管理 Lightsail 资源的 IP 地址

你可以使用你的 Lightsail 实例和其他 Lightsail 资源的 IP 地址与它们通信。例如，通过使用实例的公有 IP 地址，您可以查看实例的网络状态（使用 PING），与实例建立 SSH 连接，并将流量从自定义域名路由到实例。使用 Lightsail 资源的 IP 地址，你可以做更多的事情。

Lightsail 实例、容器服务和负载均衡器同时支持 IPv4 和 IPv6寻址协议。默认情况下，这些资源使用 IPv4 寻址协议；您无法禁用此行为。您可以选择 IPv6 为实例、容器服务和负载均衡器启用。

在本指南中，我们将介绍您需要了解的有关 Lightsail 中的 IP 地址的信息。

内容

- 实例的私有 IPv4 地址和公有地址
- 实例的静态 IP 地址
- IPv6 用于实例、容器服务、CDN 分发和负载均衡器

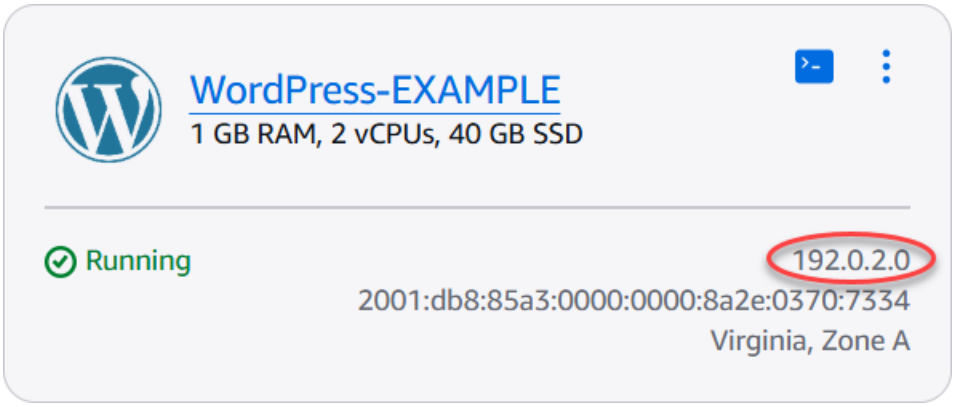
实例的私有 IPv4 地址和公有地址

当您创建 Lightsail 实例时，系统会为其分配一个公用地址和一个私 IPv4有地址。公有 IP 地址可供互联网访问，而私有 IP 地址只能由同一 Lightsail 账户中的资源访问。 AWS 区域

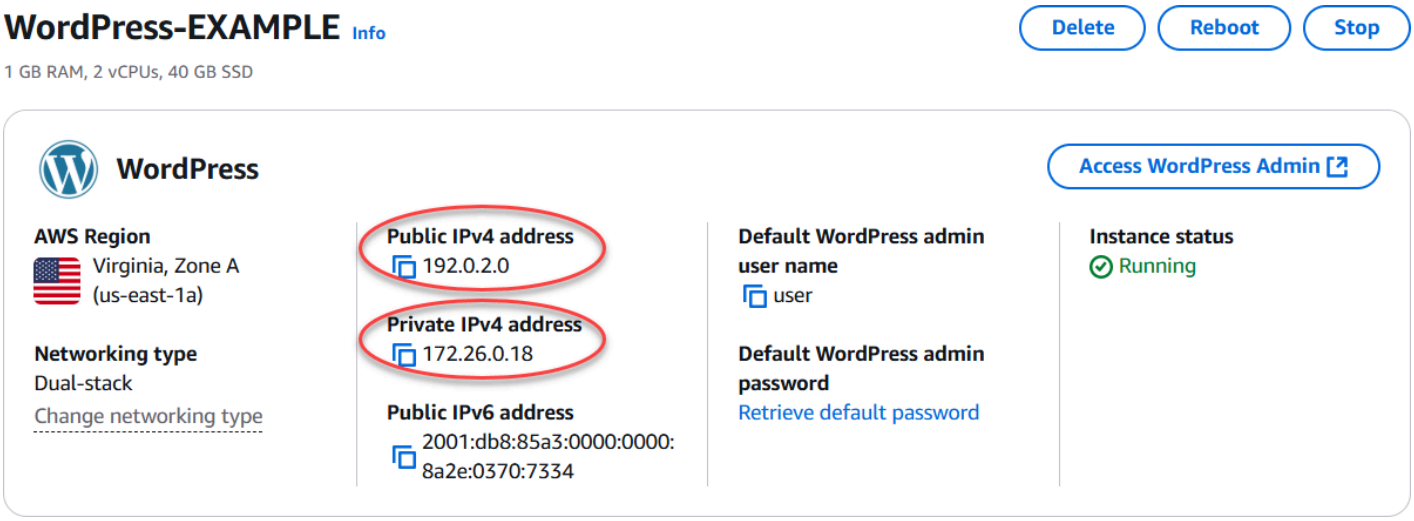
> **Note**
>
> 如果您启用 VPC 对等互连，则位于同一 AWS 区域的其他 AWS 资源可以访问您的实例的私有 IP 地址，但可以在您的 Lightsail 账户之外访问。有关更多信息，请参阅设置亚马逊 VPC 对等互连以使用 Lightsail 之外的 AWS 资源。

您的实例的 IP 地址显示在 Lightsail 控制台的以下区域中：

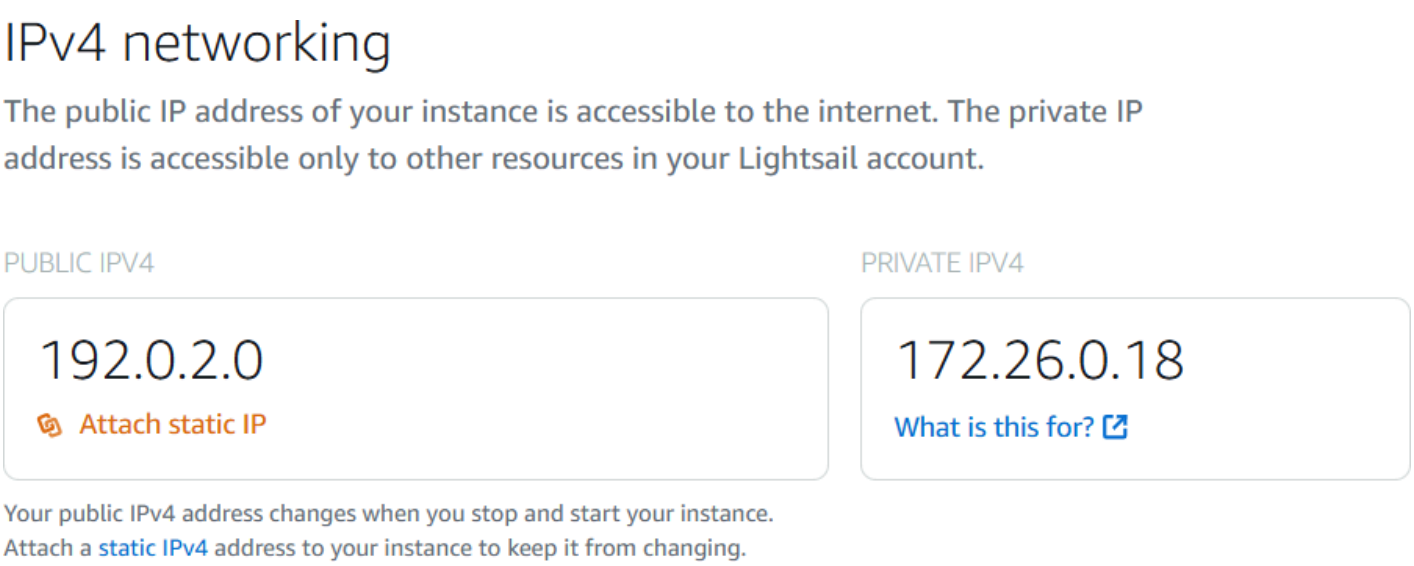
- 以下示例显示了 Lightsail 主页上实例的公有 IPv4 地址。



- 以下示例显示了实例管理页面标题区域中实例的公用 IPv4 地址和私有地址。



- 以下示例在实例管理页面的网络选项卡上显示了实例的公有 IPv4 地址和私有地址。



使用您的实例 IPv4 地址时，请记住以下几点：

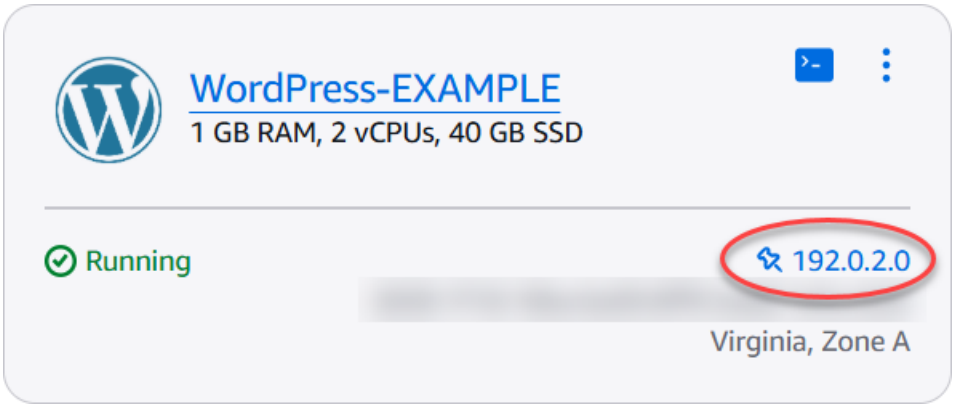
- 实例的公有 IP 地址可能会发生变化。通过将静态 IP 附加到实例，可为此实例提供一个始终不变的 IP 地址。有关更多信息，请参阅本指南的实例的静态 IP 地址部分。
- Lightsail 默认使用 IPv4 地址。但是，您可以选择 IPv6为在 2021 年 1 月 12 日之前创建的某些 Lightsail 资源启用。2021 年 1 月 12 日当天或之后创建的资源默认 IPv6 处于启用状态。有关更多信息，请参阅本指南IPv6 的实例、容器服务、CDN 分配和负载均衡器部分。
- 向实例防火墙添加规则，以控制允许连接到该实例的流量。有关更多信息，请参阅实例防火墙。

实例的静态 IPv4 地址

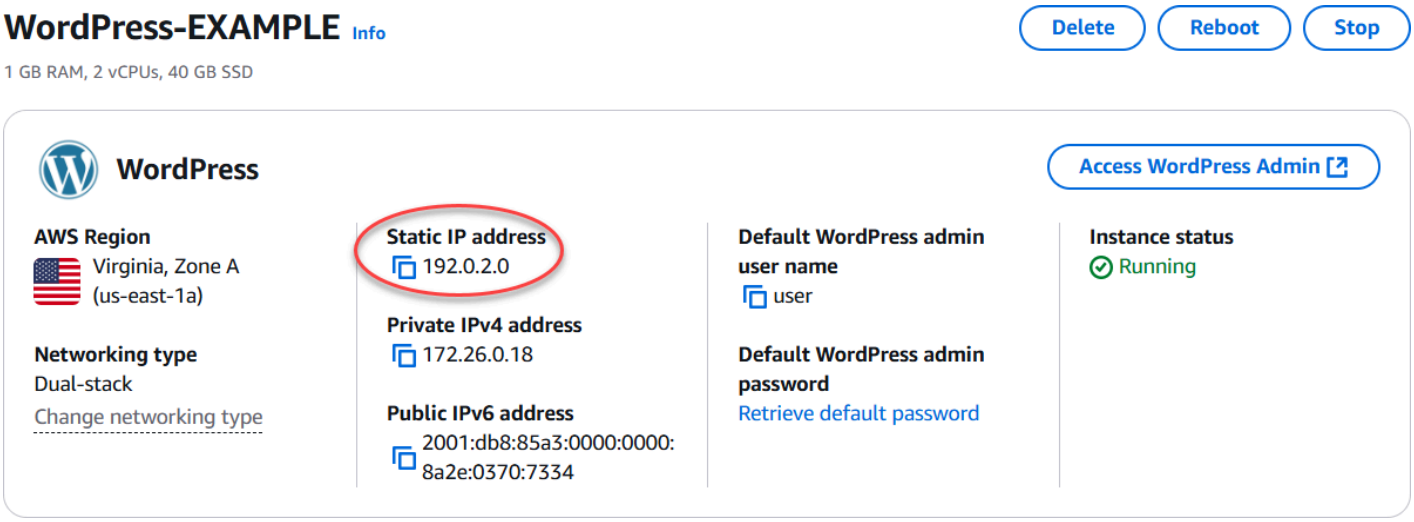
当您停止和启动实例时，在创建实例时分配给您的实例的默认公有 IPv4 地址将发生变化。您可以选择创建静态 IPv4 地址并将其附加到您的实例。静态 IPv4 地址取代了实例的默认公有 IPv4地址，当您停止和启动实例时，静态地址将保持不变。您可以将静态 IP 附加到实例。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

在您创建静态 IP 并将其附加到您的实例后，它会显示在 Lightsail 控制台的以下区域：

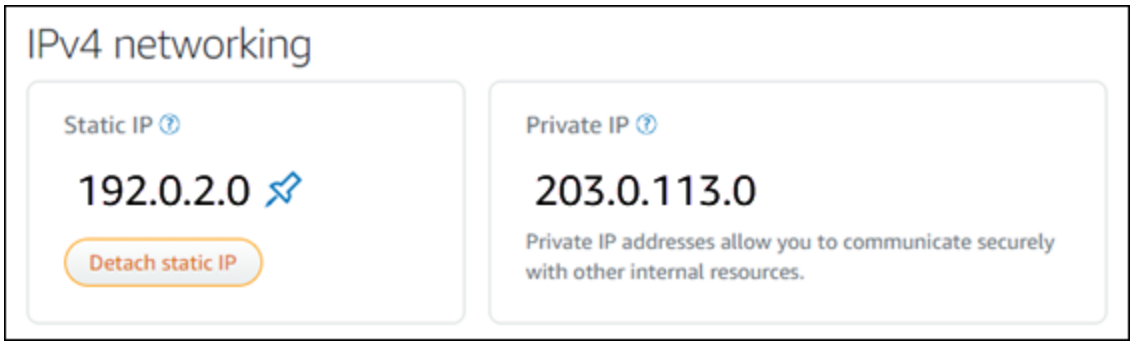
- 以下示例显示了 Lightsail 主页上实例的静态 IP 地址。图钉图标表示公有 IP 地址是静态的。



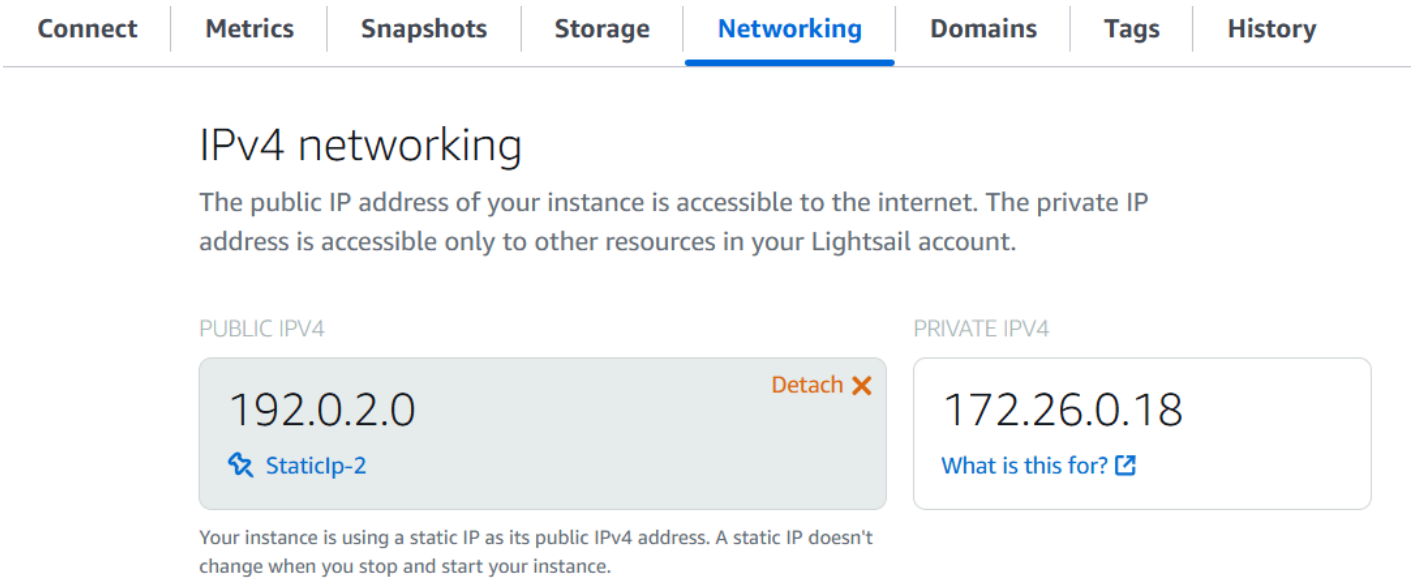
- 实例管理页面的标头区域显示的实例静态 IP 地址如下例所示。图钉图标表示公有 IP 地址是静态的。



- 实例管理页面的 Networking（联网）选项卡上显示的实例静态 IP 地址如下例所示。默认的公有 IP 地址不再列出，它已被静态 IP 地址替换。图钉图标表示公有 IP 地址是静态的。



- 您可以通过转 IPs 到 Lightsail 主页的 “网络” 选项卡来查看您创建的所有静态内容，如以下示例所示。



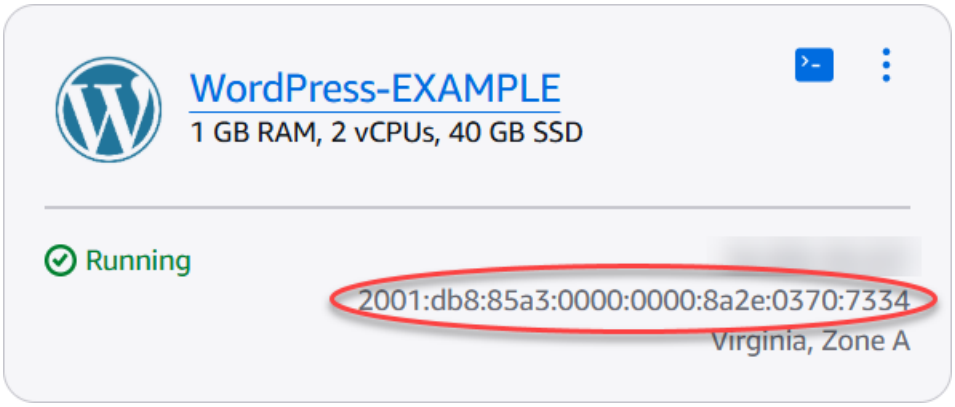
IPv6 用于实例、容器服务、CDN 分发和负载均衡器

IPv6 在 2021 年 1 月 12 日当天或之后创建的 Lightsail 实例、容器服务、CDN 分配和负载均衡器默认处于启用状态。您可以选择 IPv6 为那些在 2021 年 1 月 12 日之前创建的资源启用。当您 IPv6 为特定资源启用时，Lightsail 会自动为该资源分配 IPv6 地址；您无法自己选择或指定地址。 IPv6 有关更多信息，请参阅启用或禁用 IPv6。

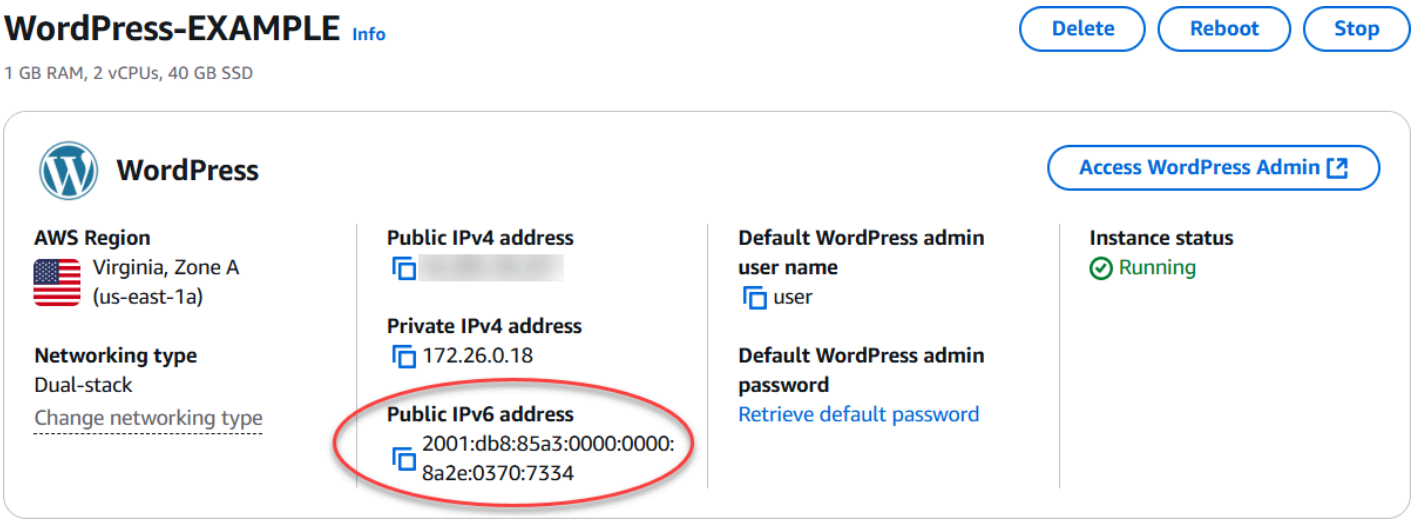
您也可以创建 IPv6仅限实例的实例。 IPv6仅限实例 IPv6 只能通过公开通信，并且没有公共 IPv4 地址。有关更多信息，请参阅 为 IPv6 Lightsail 实例配置仅限网络连接

您的实例 IPv6 地址显示在 Lightsail 控制台的以下区域中：

- 以下示例显示了 Lightsail 主页上某个实例 IPv6 的地址。



- 以下示例显示了资源管理页面标题区域中资源的地 IPv6 址。



- 以下示例显示了资源管理页面的 “网络” 选项卡上的资源 IPv6 地址。



在启用和使用 IPv6 资源时，请记住以下几点：

- 当您为资源启用时，您的资源可以通过 IPv4 和 IPv6 （在双栈模式下）进行通信，也可以 IPv4 仅通过和 IPv6 进行通信。
- 启用资源后，Lightsail 会自动 IPv6 为该资源分配 IPv6 地址；您无法自己选择或指定地址。 IPv6 当您 IPv6 为某个资源启用时，它会开始通过 IPv6 协议接受网络流量。

- 当您停止和启动实例时，实例 IPv6 的地址仍然存在。只有在您删除实例或禁用 IPv6 实例时，它才会被释放。执行上述任一操作后，您都无法找回 IPv6 地址。
- 分配给您的实例的所有 IPv6 地址都是公开的，可通过互联网访问。没有向您的实例分配私有 IPv6 地址。
- IPv4 和实例 IPv6 的地址相互独立；必须为 IPv4 和分别配置实例防火墙规则 IPv6。有关更多信息，请参阅实例防火墙。
- 并非所有在 Lightsail 中可用的实例蓝图都是在启用 IPv6 时自动配置 IPv6 的。使用以下蓝图的实例在启用 IPv6 后需要额外的配置步骤：
  - cPanel — 有关更多信息，请参阅配置 IPv6 cPanel 实例。
  - GitLab— 有关更多信息，IPv6 请参阅配置 GitLab实例。
  - Nginx — 有关更多信息，请参阅为 Nginx 实例 IPv6 进行配置。
  - Plesk — 有关更多信息，请参阅配置 IPv6 Plesk 实例。

> **Note**
>
> PrestaShop 目前不支持 IPv6 地址。您可以 IPv6 为该实例启用，但该 PrestaShop 软件不会响应通过 IPv6网络发送的请求。

Lightsail 中的静态 IP 地址

静态 IP 是一个固定的公有 IP 地址，可将其分配和重新分配给实例或其他资源。如果您尚未设置静态 IP 地址，则每次停止或重启实例时，Lightsail 都会分配一个新的公有 IP 地址。

当静态 IP 地址连接到 Lightsail 实例时，不会产生任何相关费用。但是，如果静态 IP 地址未连接到实例，则会产生费用。有关更多信息，请参阅 Lightsail 静态 IPv4地址的费用是多少？。

> **Important**
>
> 如果您停止或重新启动实例，而未先创建静态 IP 地址并将其挂载到实例，则您在实例重新启动时将丢失 IP 地址。应创建静态 IP 地址并将其挂载到实例，以确保实例始终具有相同的公有 IP 地址。有关更多信息，请参阅创建静态 IP 地址。

内容

- 创建静态 IP 并将其附加到你的 Lightsail 实例

- 在 Lightsail 中删除静态 IP 地址

创建静态 IP 并将其附加到你的 Lightsail 实例

每次停止和重启实例时，附加到您的 Amazon Lightsail 实例的默认动态公有 IP 地址都会发生变化。创建一个静态 IP 地址并将其附加到您的实例，以防止公有 IP 地址发生变化。当您稍后将注册域名指向实例时，无需在每次停止和重启实例时都更新域的 DNS 记录。您可以将静态 IP 附加到实例。有关更多信息，请参阅静态 IP 地址。

先决条件

你至少需要一个在 Lightsail 中运行的双栈实例。要创建实例，请参阅创建实例。

创建一个静态 IP 地址并将其分配给某个实例

按照以下步骤创建新的静态 IP 地址并将其附加到 Lightsail 中的实例。

1. 登录 Lightsail 控制台，网址为https://lightsail.aws.amazon.com/。
2. 在左侧导航窗格中，选择联网。
3. 选择 Create static IP（创建静态 IP）。
4. 选择要创建静态 IP AWS 区域 的位置。

   > **Note**
   >
   > 静态 IP 地址只能附加到同一区域中的实例。

5. 选择要将静态 IP 附加到的 Lightsail 资源。
6. 输入静态 IP 的名称。

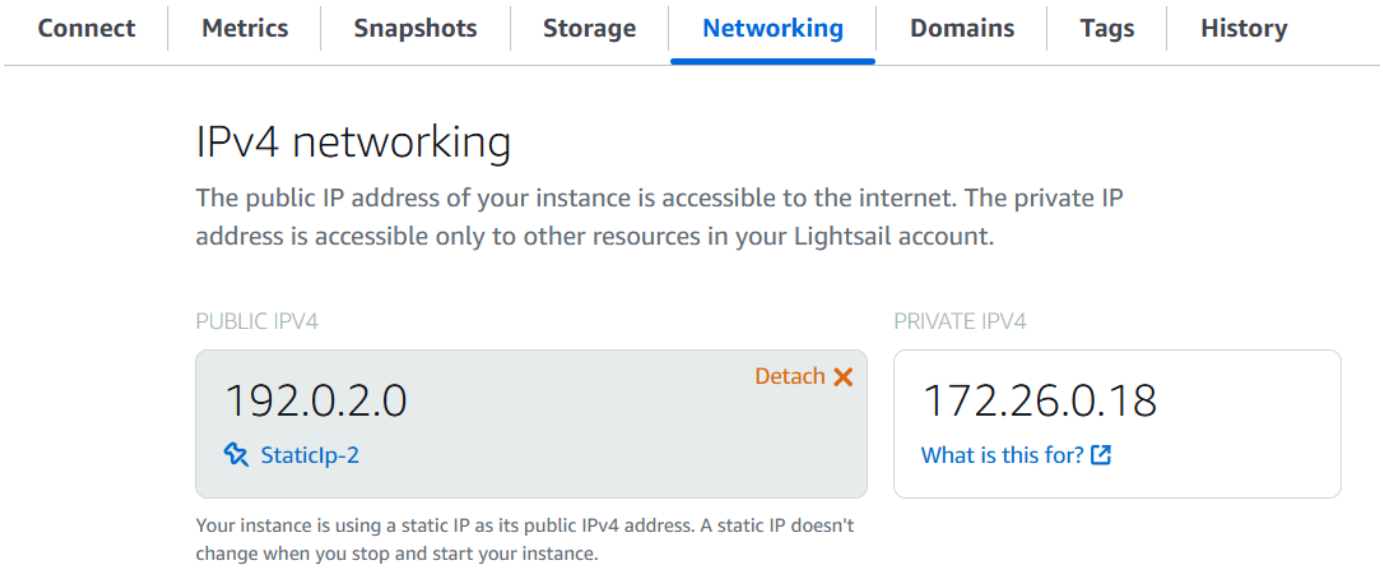
   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
7. 选择 Create（创建）。

   现在，如果您转到主页，就会看到一个静态 IP 地址，您可以管理该地址。



在您实例管理页面的 Networking（联网）选项卡上，您还会看到公有 IP 地址旁边有一颗蓝色图钉。这表明该 IP 地址现在是静态的。



有关更多信息，请参阅公有和私有 IP 地址。

在 Lightsail 中删除静态 IP 地址

AWS 区域 在您的亚马逊 Lightsail 账户中，您最多可以 IPs 为每个账户创建五个静态数据。如果您删除了挂载静态 IP 地址的实例，则该静态 IP 地址仍留在您的账户中。如果您不再需要静态 IP 地址，则可以使用 Lightsail 控制台或 AWS Command Line Interface ()AWS CLI将其删除。在本指南中，我们将向您展示如何从您的 Lightsail 账户中删除静态 IP 地址。有关静态的更多信息 IPs，请参阅 IP 地址。

> **Important**
>
> 删除静态 IP 会将该静态 IP 从你的 Lightsail 账户中完全删除。使用该静态 IP 的资源（例如实例）将受到影响。删除静态 IP 后将无法取回。

使用 Lightsail 控制台删除静态 IP

完成以下步骤，使用 Lightsail 控制台删除静态 IP。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 在联网页面上，选择要删除的静态 IP 地址旁边的垂直省略号图标，然后选择删除。



使用删除静态 IP AWS CLI

完成以下过程，以使用 AWS CLI删除静态 IP。从你的 Lightsail 账户中删除静态 IP 的命令是。release-static-ip当您创建静态 IP 时，实际上是分配 静态 IP。因此，您实际上不是删除了静态 IP，而是释放了静态 IP。

先决条件

首先，如果您还没有，则需要安装 AWS CLI。要了解更多信息，请参阅安装 AWS Command Line Interface。务必配置 AWS CLI。

您将需要静态 IP 的名称才能将其释放。你可以使用`get-static-ips` AWS CLI 命令来获得。

1. 键入以下命令：

```
aws lightsail get-static-ips
```

您应该可以看到类似于如下所示的输出内容。

```
{
    "staticIps": [
        {
            "name": "Example-StaticIP",
            "resourceType": "StaticIp",
            "attachedTo": "MyInstance",
            "arn": "arn:aws:lightsail:us-east-2:123456789101:StaticIp/5282f35e-
c720-4e5a-1234-12345EXAMPLE",
            "isAttached": true,
            "ipAddress": "192.0.2.0",
            "createdAt": 1489750629.026,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        },
        {
            "name": "my-other-static-ip",
            "resourceType": "StaticIp",
            "arn": "arn:aws:lightsail:us-east-2:123456789101:StaticIp/
f5885e14-8984-49e5-1234-12345EXAMPLE",
            "isAttached": false,
            "ipAddress": "192.0.2.2",
            "createdAt": 1483653597.815,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        }
    ]
}
```

2. 选择要释放的静态 IP 的名称值并记下它，以便在下一步中使用。

   例如，您可以将此值复制到剪贴板。

3. 键入以下命令。

```
aws lightsail release-static-ip --static-ip-name StaticIpName
```

在命令中，*StaticIpName*替换为静态 IP 的名称。

如果成功，您应看到与以下内容类似的输出。

```
{
    "operations": [
        {
            "status": "Succeeded",
            "resourceType": "StaticIp",
            "isTerminal": true,
            "statusChangedAt": 1489860944.19,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            },
            "operationType": "ReleaseStaticIp",
            "resourceName": "Example-StaticIP",
            "id": "92a2f0d2-eef2-4e6f-1234-12345EXAMPLE",
            "createdAt": 1489860944.19
        }
    ]
}
```

为 Lightsail 资源启用或禁用双栈联网

IPv6 在 2021 年 1 月 12 日当天或之后创建的 Lightsail 双栈实例、容器服务和负载均衡器默认处于启用状态。您可以选择 IPv6 为那些在 2021 年 1 月 12 日之前创建的资源启用。在本指南中，我们将向您展示如何为双栈实例启用或禁用 IPv6 联网。有关的更多信息 IPv6，请参阅 IP 地址。

双堆栈注意事项

IPv6 已于 2021 年 1 月 12 日在 Lightsail 中推出；因此，您可能需要根据以下指南手动启用或禁用 IPv6 某些资源：

- 在您启用之前，在 1 月 12 日之前创建的实例和负载均衡器已 IPv6禁用。但是，1 月 12 日之后创建的实例和负载均衡器在创建时已 IPv6 启用。
- 在 1 月 12 日之前或之后创建的容器服务已 IPv6 启用。
- IPv6 可以随时手动启用或禁用实例和负载均衡器。无法对容器服务禁用 IPv6。

启用和使用时，请记住以下几点 IPv6：

- 当您为资源启用时，您的资源 IPv4 只能通过 IPv4 和 IPv6 （在双栈模式下） IPv6 进行通信。
- 当您 IPv6 为某个实例启用时，Lightsail 会自动为该实例分配 IPv6地址；您无法自己选择或指定地址。 IPv6 当您启用 IPv6 容器服务或负载均衡器时，该资源将开始接受互联网流量 IPv6。
- 当您停止和启动实例时，实例 IPv6 的地址仍然存在。只有在您删除实例或禁用 IPv6 实例时，它才会被释放。执行上述任一操作后，您都无法找回 IPv6 地址。
- 分配给您的实例的所有 IPv6 地址均为公有地址，可通过互联网访问。没有向您的实例分配私有 IPv6 地址。
- IPv4 和实例 IPv6 的地址相互独立；必须为 IPv4 和分别配置实例防火墙规则 IPv6。有关更多信息，请参阅实例防火墙。
- 并非所有在 Lightsail 中可用的实例蓝图都是在启用 IPv6 时自动配置 IPv6 的。使用以下蓝图的实例在启用 IPv6 后需要额外的配置步骤：
  - cPanel — 有关更多信息，请参阅配置 IPv6 cPanel 实例。
  - GitLab— 有关更多信息， IPv6 请参阅配置 GitLab实例。
  - Nginx — 有关更多信息，请参阅为 Nginx 实例 IPv6 进行配置。
  - Plesk — 有关更多信息，请参阅配置 IPv6 Plesk 实例。

主题

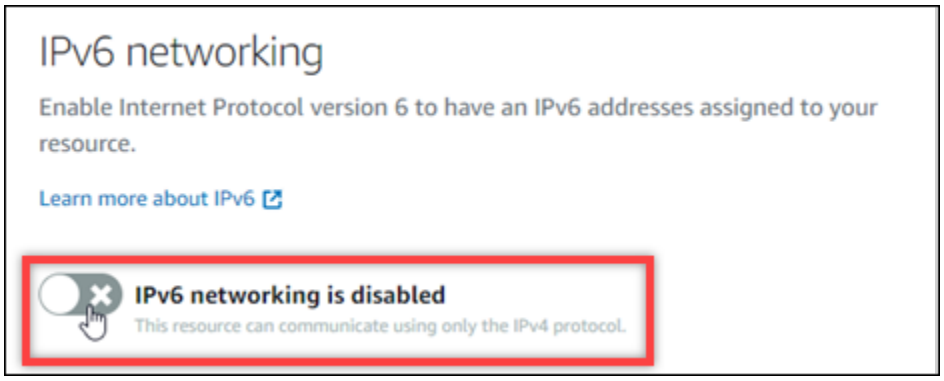
- 为 Lightsail 资源启用 IPv6 联网
- 禁用 Lightsail 资源的 IPv6 联网功能

为 Lightsail 资源启用 IPv6 联网

完成以下步骤， IPv6 为实例、CDN 分配和负载均衡器启用。

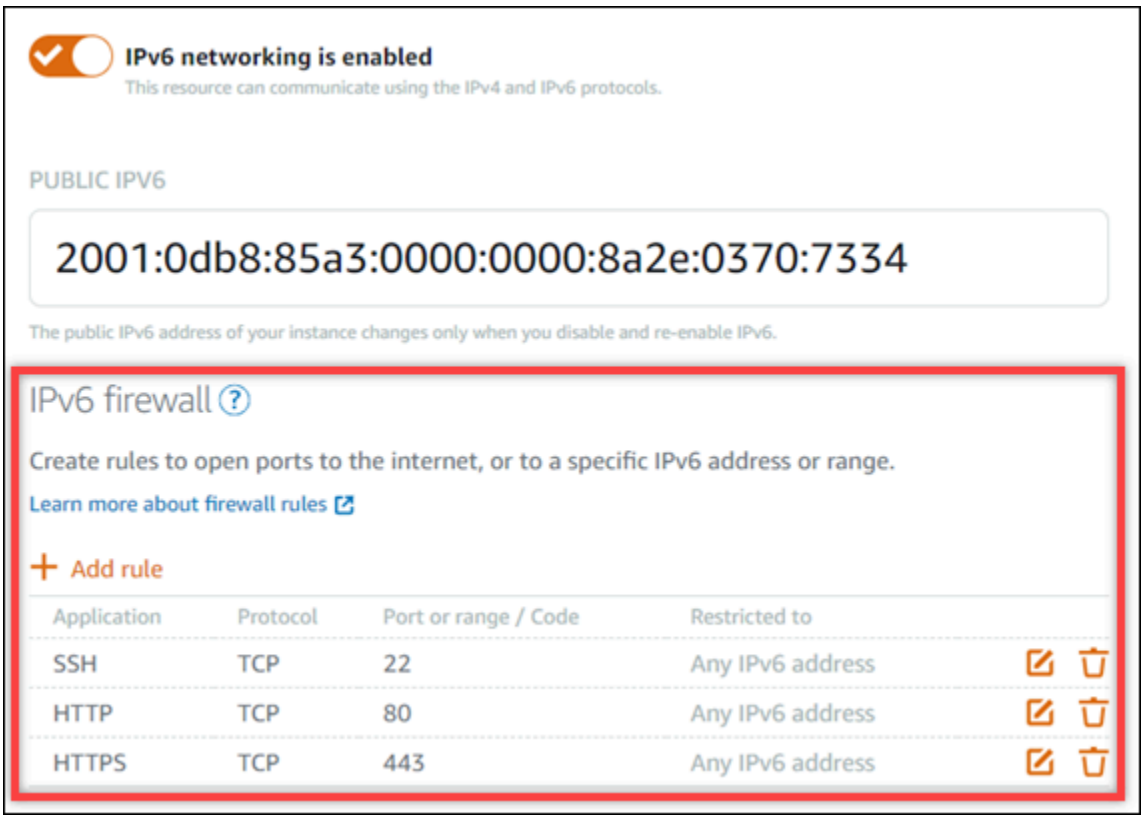
1. 登录 Lightsail 控制台。
2. 根据要启用的资源，完成以下步骤之一 IPv6：
   - 要 IPv6 为实例启用，请在 Lightsail 主页上选择 “实例” 选项卡，然后选择要为其启用的实例的名称。 IPv6
   - 要启 IPv6 用 CDN 分配或负载均衡器，请在左侧导航窗格中选择网络选项卡，然后选择要为其启用的 CDN 分配或负载均衡器的名称。 IPv6
3. 在资源的管理页面中选择联网选项卡。

4. 在页面的 “IPv6 网络” 部分，选择要 IPv6 为资源启用的开关。



启用 IPv6 资源后，请注意以下事项：

- 如果您启 IPv6 用 CDN 分发或负载均衡器，则该资源将开始接受 IPv6 流量。如果您 IPv6 为某个实例启用，则会为其分配一个 IPv6地址，并且 IPv6 防火墙变为可用，如以下示例所示。



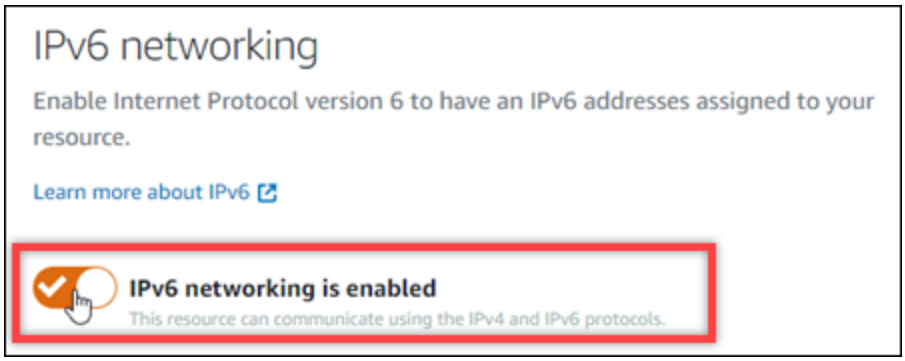
- 使用以下蓝图的实例在启用后需要额外的步骤， IPv6 以确保实例知道其新 IPv6 地址：
  - cPanel — 有关更多信息，请参阅配置 IPv6 cPanel 实例。
  - GitLab— 有关更多信息， IPv6 请参阅配置 GitLab实例。
  - Nginx — 有关更多信息，请参阅为 Nginx 实例 IPv6 进行配置。
  - Plesk — 有关更多信息，请参阅配置 IPv6 Plesk 实例。

- 如果您已注册域名将流量引导至您的实例、容器服务、CDN 分发或负载均衡器，请务必在域名的 DNS 中创建 IPv6 地址记录 (AAAA)，以便将 IPv6 流量路由到您的资源。

禁用 Lightsail 资源的 IPv6 联网功能

完成以下步骤以禁 IPv6 用实例、CDN 分配和负载均衡器。

1. 登录 Lightsail 控制台。
2. 根据要禁用的资源，完成以下步骤之一 IPv6：
   - 要禁 IPv6 用某个实例，请在 Lightsail 主页上选择 “实例” 选项卡，然后选择要禁用的实例的名称。 IPv6
   - 要禁 IPv6 用 CDN 分配或负载均衡器，请在左侧导航窗格中选择 “网络” 选项卡，然后选择要禁用的 CDN 分配或负载均衡器的名称。 IPv6
3. 在资源的管理页面中选择联网选项卡。
4. 在页面的 “IPv6 网络” 部分，选择要禁 IPv6 用该资源的开关。



为 IPv6 Lightsail 实例配置仅限网络连接

Lightsail 实例支持两种类型的联网：双栈联网（IPv4 和 IPv6）和IPv6仅限联网。使用双栈网络时，您的实例会被分配一个公有地址 IPv4 和一个公有 IPv6 地址。对于采用双堆栈网络的实例，您可以根据需要启用或禁 IPv6 用。

使用 IPv6仅限联网时，您的实例会被分配一个公共 IPv6 地址，并且不支持公共 IPv4 流量。并非所有 Lightsail 蓝图都兼容。 IPv6要了解哪些蓝图 IPv6仅支持-，请参阅。IPv6 兼容的蓝图此外，不能将具有 IPv6仅限网络的实例配置为 Lightsail 内容分发网络 (CDN) 分发的原始资源。有关 Lightsail 发行版的更多信息，请参阅。使用 Lightsail 内容交付分发版在全球范围内提供网络内容

如果您不需要公共 IPv4 地址，请使用 IPv6仅限网络连接。但首先，请确保您的本地网络、计算机、设备和最终用户可以使用 IPv6进行通信。有关更多信息，请参阅中的 IPv6 可接通性。验证 Lig IPv6 htsail 实例的可访问性

对于蓝图支持的现有实例，您可以在双栈联网和 IPv6仅限网络之间更改网络类型。要查看 IPv6仅限联网的注意事项并对现有实例进行更改，请参阅在 Lightsail 中将实例网络类型切换为 IPv6 或双堆栈。

主题

- 在 Lightsail 中将实例网络类型切换为 IPv6 或双堆栈
- IPv6 兼容的蓝图

在 Lightsail 中将实例网络类型切换为 IPv6 或双堆栈

实例的联网类型决定了它使用哪种协议通过 Internet 进行通信。创建实例时，您可以在双堆栈网络或IPv6仅限网络之间进行选择。您也可以将现有实例的网络类型从双堆栈更改为 IPv6仅限，反之亦然。使用向导、 step-by-step工作流程或完成各个步骤来更改网络类型。

使用引导式工作流程，在配置新的联网类型时，您的实例将继续运行。使用此选项可让您的实例在更改发生时保持可通过 Internet 访问的状态。但首先，请确保您的本地网络、计算机、设备和最终用户可以使用 IPv6进行通信。有关更多信息，请参阅 验证 Lig IPv6 htsail 实例的可访问性。

通过完成各个步骤，您将建立实例的快照，然后根据快照创建一个新实例。在创建新实例时，您可以选择不同的联网类型。在更改其他实例的配置之前，使用此选项验证 IPv6 兼容性。在开始之前，我们建议您首先查看 IPv6-仅考虑因素。

IPv6-仅考虑因素

请查看以下注意事项：

- 每当实例的联网类型更改时，实例计划就会相应变化。有关更多信息，请参阅计算博客上的 Amazon Lightsail 上宣布 IPv6 实例捆绑包和定价更新AWS。
- 您的实例将通过公开通信 IPv6。它将不支持传入或传出的公共 IPv4 流量。它将收到一个私有 IPv4地址，用于与您的 Lightsail 账户中的其他资源进行通信。有关更多信息，请参阅 查看和管理 Lightsail 资源的 IP 地址。
- IPv6只能将仅限实例配置为 Lightsail 内容分发网络 (CDN) 分发的来源。
- 您可以向 Light IPv6 sail 负载均衡器添加仅限运行的实例。
- 更改联网类型时，您的实例的数据传输计划限额将延续。此限额不会重置。

- 验证您的本地设备、网络和互联网服务提供商 (ISP) 是否 IPv6兼容。有关更多信息，请参阅 验证 Lig IPv6 htsail 实例的可访问性。

选项：引导式工作流程

要使用向导配置您的实例联网类型

1. 在实例管理页面的信息面板上，选择更改联网类型。
2. 在 “选择网络类型” 中，选择 “双堆栈” 或 IPv6 “仅限”。查看所选选项下方突出显示的信息，然后选择下一步。
3. 对于查看资源，请查看将对当前与实例关联的资源执行的更改。资源可以是静态 IP 地址，也可以是 Lightsail 负载均衡器。如果您的实例上没有附加任何资源，则不会进行任何更改。仅在完成下一步的工作流程后，才会进行资源更改。选择下一步以继续。
4. 对于确认更改，请查看新的实例联网类型、定价和资源更改，然后选择确认更改。我们开始配置你的 Lightsail 资源。
5. （可选）在工作流程完成后更新您的实例配置。例如，将静态 IP 附加到您的实例，或者更新的 DNS A 记录和 AAAA 记录。 IPv4 IPv6有关后续步骤，请参阅本指南中的 the section called “后续步骤” 部分。

选项：各个步骤

要通过完成各个步骤来配置您的实例联网类型

1. 在实例管理页面中的快照选项卡上，选择创建快照。有关更多信息，请参阅下列主题之一：
   - 使用快照备份 Linux/Unix Lightsail 实例
   - 创建你的 Lightsail Windows Server 实例的快照
2. 为快照命名，然后选择创建。
3. 从快照操作菜单（⋮）中选择创建新实例。有关更多信息，请参阅 从快照创建 Lightsail 实例。
4. 从 “选择网络类型” 部分，选择双栈或IPv6仅限。
5. 查看其余选项，然后选择创建实例。您的新实例即会创建。
6. （可选）在工作流程完成后更新您的实例配置。例如，将静态 IP 附加到您的实例，或者更新的 DNS A 记录和 AAAA 记录。 IPv4 IPv6有关后续步骤，请参阅本指南中的 the section called “后续步骤” 部分。

后续步骤

更改实例的联网类型后，有其他几项可执行的任务：

- （IPv6仅限）确保您的应用程序和用户能够通过 IPv6通信。有关更多信息，请参阅 验证 Lig IPv6 htsail 实例的可访问性。
- （双堆栈）将静态 IP 地址附加到实例。有关更多信息，请参阅将静态 IP 附加到实例。
- （双栈）将您的实例配置为 Lightsail 发行版的来源。有关更多信息，请参阅 Lightsail 中的 CDN 发行版。
- （两者）为您的实例添加或更新防火墙设置。有关更多信息，请参阅 Lightsai l 中的实例防火墙。
- （两者）添加或更新的 DNS A 记录和 AAAA 记录。 IPv4 IPv6有关更多信息，请参阅将域指向实例。
- （两者）将您的实例添加到 Lightsail 负载均衡器。有关更多信息，请参阅 Lightsail 中的负载均衡器。

IPv6 兼容的蓝图

以下 Lightsail 蓝图与仅限实例 IPv6的计划兼容

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Amazon Linux 2023
- Amazon Linux 2
- AlmaLinux OS 9
- CentOS Stream 9
- Debian 11, and 12
- FreeBSD 13, and 14
- Ubuntu 20, 22, and 24
- SQL Server 2022 Express
- SQL Server 2019 Express
- SQL Server 2016 Express

- LAMP stack (PHP 8) packaged by Bitnami
- MEAN stack packaged by Bitnami
- Redmine packaged by Bitnami

有关 Lightsail 蓝图的更多信息，请参阅。the section called “蓝图”

Lightsail 的区域和可用区

在 Amazon Lightsail 中创建资源时 AWS 区域 ，请在最接近用户的地方创建资源。例如，如果您的博客流量主要来自瑞士，请选择 Frankfurt（法兰克福）或 Paris（巴黎）。

> **Note**
>
> DNS 区域是全球性资源。仅在美国东部（弗吉尼亚州北部）(us-east-1) 区域中创建，但其可以引用任何 AWS 区域中的任何实例。

Lightsail 有以下几种可供选择： AWS 区域

- 美国东部（俄亥俄州）(us-east-2)
- 美国东部（弗吉尼亚北部）(us-east-1)
- 美国西部（俄勒冈州）(us-west-2)
- 亚太地区（孟买）(ap-south-1)
- 亚太地区（首尔）(ap-northeast-2)
- 亚太地区（新加坡）(ap-southeast-1)
- 亚太地区（悉尼）(ap-southeast-2)
- 亚太地区（东京）(ap-northeast-1)
- 加拿大（中部）(ca-central-1)
- 欧洲（法兰克福）(eu-central-1)
- 欧洲（爱尔兰）(eu-west-1)
- 欧洲（伦敦）(eu-west-2)
- 欧洲（巴黎）(eu-west-3)
- 欧洲（斯德哥尔摩）(eu-north-1)



SSH 密钥和 Lightsail 区域

在 Lightsail 中，只要您在中创建实例 AWS 区域，我们就会在该区域创建默认 SSH 密钥。此默认密钥仅可用于连接到在该特定区域中的实例。要在您具有实例的所有区域中使用相同密钥，请创建您自己的密钥对并将其上传到所有这些区域。或者，在这些区域中上传现有密钥对。

有关更多信息，请参阅 SSH 密钥对。

使用 Lightsail 区域的技巧

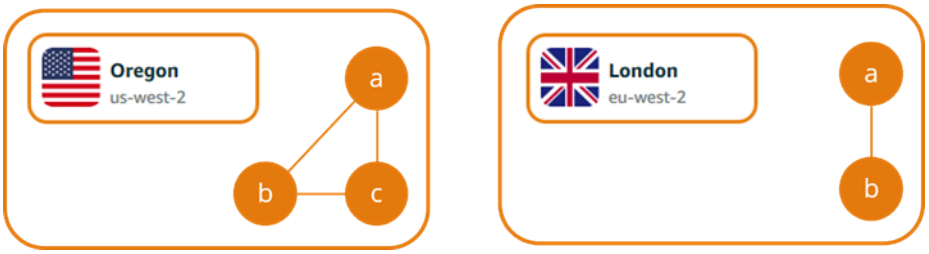
每一个 AWS 区域 都被设计成与其他完全隔离 AWS 区域。这可实现最大程度的容错能力和稳定性。

区域之间的所有通信都通过公共 Internet 进行。因此，您应使用合适的加密方法来保护您的数据。请注意，在区域之间传输数据需要收费。有关更多信息，请参阅 Amazon EC2 定价-数据传输。

当您使用 AWS Command Line Interface (AWS CLI) 或 API 操作使用 Lightsail 实例时，必须指定其区域终端节点。在 AWS CLI 命令中使用 `--region` 选项，并指定 `us-east-1` 以返回有关 DNS 区域和网络资源的信息。有关使用该 AWS CLI `--region`选项的更多信息，请参阅AWS CLI 参考中的常规选项。

Lightsail 可用区

可用区是在独立的、物理上显著不同的基础设施中运行的数据中心的集合。可用区设计为高度可靠。可用区之间不共用常见的故障点，如发电机和冷却设备。可用区在物理上也是相互独立的，以至于即使火灾、龙卷风或洪涝等极端灾难也只会影响发生此灾难的单个可用区。



每个可用区 AWS 区域 都有多个隔离的可用区，这些可用区由区域名称后面的字母表示 (us-east-2*a*)。您一次只能在一个可用区中创建 Lightsail 实例。在创建您的实例时，您可能看不到所有可用区。如果您根本未看到可用区列表，请确保您已在上一步中选定了一个区域。

可用区和你的 Lightsail 应用程序

通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。

要创建在多个可用区中可用的实例，请先创建实例的快照。接下来，在您通过创建的快照创建新实例时选择其他可用区。

有关更多信息，请参阅 Amazon EC2 用户指南中的AWS 区域 和可用区。

使用 VPC 对等互连将 Lightsail 资源连接到 AWS 服务

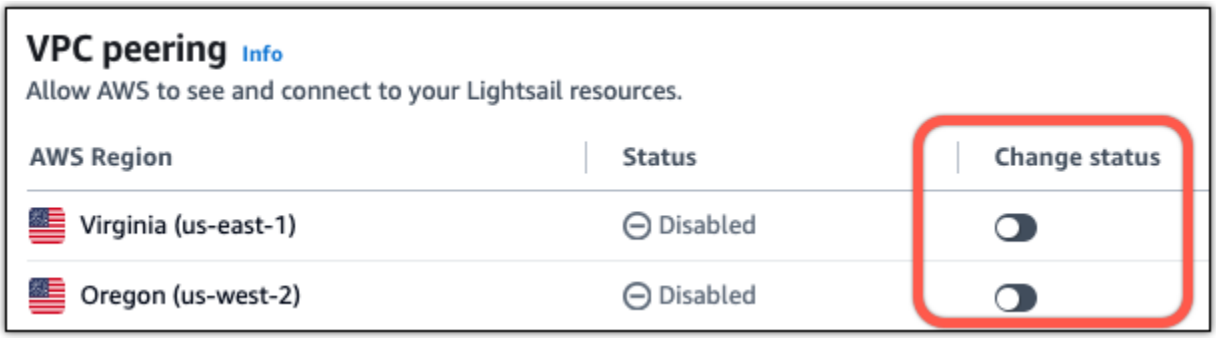
借助 Amazon Lightsail，您可以通过虚拟私有云 (VPC) 对等连接连接到 AWS 资源，例如亚马逊 RDS 数据库。VPC 是专用于您的 AWS 账户的虚拟网络。你在 Lightsail 中创建的所有内容都在 VPC 内，你可以将你的 Lightsail VPC 连接到亚马逊 VPC。

某些 AWS 资源，例如 Amazon S3、Amazon 和 Amazon DynamoDB CloudFront，不需要您启用 VPC 对等互连。

> **Note**
>
> 要在 Lightsail 中启用 VPC 对等互连，您的中必须有一个默认 VPC。 AWS 区域对等关系将建立在您在 Lightsail 中的资源与您启用 VPC 对等互连的区域的默认 VPC 中的资源之间。如果您没有默认 Amazon VPC，则可以创建一个。有关更多信息，请参阅 Amazon VPC 用户指南中的默认 VPCs和创建默认 VPC。
>
> 由于 AWS 区域 s 彼此隔离，因此 VPC 也会在您创建它的区域中隔离。你需要在每个你有 Lightsail 资源 AWS 区域 的地方启用 VPC 对等互连，你要将其他资源连接到这些资源。

拥有默认亚马逊 VPC 后，请按照以下说明将您的 Lightsail VPC 与您的亚马逊 VPC 对等。

1. 在 Lightsail 控制台中，在顶部导航菜单中选择您的用户名。
2. 从下拉列表中选择 Account（账户）。
3. 选择 Advanced（高级）选项卡。
4. 在要启用 VPC 对等互连的 AWS 区域 位置旁边切换状态。



如果对等连接失败，请再次尝试启用 VPC 对等。如果此操作不起作用，请联系 AWS 支持。

如果对等互连请求成功，则会在您的 AWS 账户中创建对等连接。转至 Amazon VPC 控制面板，然后在导航窗格中选择对等连接，以查看创建的对等连接。

有关 Amazon VPC 的更多信息，请参阅 Amazon VPC 用户指南中的 VPC 和子网。

允许与其他 AWS 服务通信

启用 VPC 对等互连后，您必须确保要连接的其他 AWS 服务中的资源能够接受来自您的 Lightsail 资源的入站流量。如果您希望其他 AWS 服务的资源连接到您的 Lightsail 实例，则可以添加防火墙规则以允许所需的入站流量。有关更多信息，请参阅向 Lightsail 实例添加防火墙规则。

您可能执行的步骤将取决于您使用的服务和流量类型。有关将 Lightsail 实例连接到 Amazon RDS 数据库可能采取的步骤的示例，请参阅 Amazon Lightsail 数据库提示和 AWS 技巧博客文章。有关您可以使用 VPC 对等连接与 Lightsail 集成的服务的更多信息，请参阅。通过 VPC 对等互连将 Lightsail 与其他 AWS 服务集成

Lightsail 中的 SSL/TLS 证书

Amazon Lightsail 使用 SSL/TLS 证书来验证可与 Lightsail 负载均衡器、内容分发网络 (CDN) 分发和容器服务配合使用的自定义（注册）域名。将经过验证的证书附加到其中一个 Lightsail 资源后，将使用安全超文本传输协议 (HTTPS) 对通过该域路由到该资源的流量进行加密。

您可以在 Amazon Lightsail 中创建传输层安全 (TLS) 证书，以便为您想要与 Lightsail 负载均衡器、内容分发、网络分发和容器服务一起使用的自定义（注册）域启用加密网络流量。TLS 是一个更安全的更新安全套接字层 (SSL) 版本。在 Lightsail 文档和控制台中，你会看到我们将其称为 SSL/TLS。

> **Important**
>
> 您可以附加到负载均衡器、CDN 分发和容器服务的 Lightsail 证书由 AWS Certificate Manager (ACM) 服务颁发。从 2022 年 10 月 11 日起，通过 Lightsail 为您的负载均衡器、CDN 分发和容器服务获取的任何公共证书都将从 ACM 管理的多个中间证书颁发机构之一 (ICAs) 或下 CAs 级证书颁发机构颁发。有关更多信息，请参阅亚马逊云科技安全博客中的 Amazon introduces dynamic intermediate certificate authorities（Amazon 引入动态中间证书颁发机构）。

为什么使用 HTTPS？

首先是安全，这也是最重要的。HTTPS 提供额外的安全层，因为它使用 TLS 移动数据。HTTPS 加密在 Web 服务器和客户端的浏览器之间是机密的，因为它们是唯一两个可解密流量的实体。HTTPS 连接也更加安全，因为其他方无法修改客户端与服务器交换的数据。

除了上面提到的安全优势以外，还有其他一些原因在 HTTP 基础上额外使用 HTTPS。例如，2014 年，Google 开始在搜索结果中为安全网站提供更高的排名。换句话说，与仅使用 HTTP 的网站相比，使用 HTTPS（所有其他条件相同）的网站的搜索结果排名更靠前。

了解有关将 HTTPS 作为排名指标的更多信息

过程概述

使用 Lightsail 证书的过程很简单。它涉及以下步骤：

1. 创建可以使用 Lightsail 证书的 Lightsail 资源，例如负载均衡器、CDN 分发或容器服务。
2. 使用 Lightsail 为您的域名创建证书。
3. 通过将规范名称（CNAME）记录添加到域的 DNS 来验证证书
4. 将经过验证的证书附加到您的 Lightsail 资源。
5. 修改您的域名的 DNS 以将流量路由到您的 Lightsail 资源。



将经过验证的证书挂载到该资源后，通过域路由到该资源的流量将使用 HTTPS 进行加密。

将 SSL/TLS 证书与分配和容器服务结合使用

Lightsail 发行版和容器服务需要使用 HTTPS。创建其中任何一个资源时，默认情况下会为资源的默认域启用 HTTPS（例如，`https://123456abcdef.cloudfront.net/` 用于分配或 `https://container-service-1.123456abcdef.us-west-2.cs.amazonlightsail.com/` 用于容器服务）。如果您想将注册的域名（例如`example.com`）用于分发或容器服务，则必须创建 Lightsail SSL/TLS 证书，使用您的域名对其进行验证，然后在资源上启用自定义域。在分配或容器服务中启用自定义域还会将域经过验证的证书挂载到资源。

通过访问以下链接，您可以开始在分配上启用自定义域和 HTTPS。

- 创建分配的 SSL/TLS 证书
- 验证分配的 SSL/TLS 证书
- 查看分配的 SSL/TLS 证书
- 启用分配的自定义域
- 将域指向分配

有关分配的更多信息，请参阅内容分发网络分配。

通过访问以下链接，您可以开始在容器服务上启用自定义域和 HTTPS。

- 创建容器服务的 SSL/TLS 证书
- 验证容器服务的 SSL/TLS 证书
- 启用和管理自定义域

有关容器服务的更多信息，请参阅容器服务。

将 SSL/TLS 证书与负载均衡器结合使用

创建 Lightsail 负载均衡器时，端口 80 默认处于打开状态，用于处理常规 HTTP 流量。要通过端口 443 启用 HTTPS 流量，您必须创建 SSL/TLS 证书，并使用域名验证该证书，并将其附加到负载均衡器。

您最多可以为每个负载均衡器创建两个 SSL/TLS 证书。每个负载均衡器一次只能使用一个证书。如果从您的负载均衡器中删除正在使用的有效证书，负载均衡器将无法再处理特定域的 HTTPS 流量，直到您挂载另一个有效的证书。

通过访问以下链接，您可以开始在负载均衡器上启用 HTTPS。

- 创建负载均衡器并向其附加实例
- 创建 SSL/TLS 证书
- 验证域所有权
- 附加已验证的证书以启用 HTTPS

有关负载均衡器的更多信息，请参阅负载均衡器。

为安全的 Lightsail 容器服务域创建 SSL/TLS 证书

您可以为您的 Lightsail 容器服务创建 Amazon Lightsail TLS/SSL 证书。创建证书时，您可以指定证书的主域名和备用域名。为容器服务启用自定义域并选择证书时，最多可以从要添加作为容器服务的自定义域的证书中选择四个域。更新域的 DNS 记录以将流量指向您的容器服务后，您的服务将接受流量并使用 HTTPS 提供内容。可以创建的证书数量存在配额。有关更多信息，请参阅 Lightsail Service Quotas。

有关 SSL/TLS 证书的更多信息，请参阅容器服务证书。

先决条件

在开始之前，您需要创建 Lightsail 容器服务。有关更多信息，请参阅创建容器服务和容器服务。

创建容器服务的 SSL/TLS 证书

完成以下过程以为您的容器服务创建 SSL/TLS 证书。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。

3. 选择所需的容器服务的名称，以为其创建证书。
4. 在容器服务管理页面上选择 Custom domains（自定义域）选项卡。
5. 向下滚动到页面的 Attached certificates（附加的证书）部分。

   您的所有证书都列在页面的 “附加证书” 部分下，包括为其他 Lightsail 资源创建的证书，以及正在使用但未使用的证书。
6. 选择创建证书。
7. 在 Certificate name（证书名称）文本框中输入唯一的名称以标识您的证书。然后，选择 Continue（继续）。
8. 在 Specify up to 10 domains or subdomains（最多指定 10 个域或子域）字段中，输入要用于证书的主域名（例如，`example.com`）。
9. （可选）在 Specify up to 10 domains or subdomains（最多指定 10 个域或子域）字段中输入其他域名（例如，www.example.com）。

   您最多可以向证书添加九个备用代域。启用自定义域并为服务选择证书后，最多可以将证书的四个域用于容器服务。
10. 选择创建证书。

    将提交您的证书请求，并且新证书的状态将更改为Attempting to validate your certificate（正在尝试验证您的证书）。在此期间，Lightsail 会尝试将证书的验证记录添加到主域名的 DNS 中。过段时间以后，状态将更改为 Valid（有效）。

    如果自动验证失败，您需要先使用您的域验证证书，然后才能将证书用于您的容器服务。有关更多信息，请参阅验证容器服务的 SSL/TLS 证书。

主题

- 验证 Lightsail 容器服务的 SSL/TLS 证书
- 查看 Lightsail 容器服务的 SSL/TLS 证书

验证 Lightsail 容器服务的 SSL/TLS 证书

Amazon Lightsail SSL/TLS 证书在创建后必须经过验证，然后才能将其与 Lightsail 容器服务一起使用。提交您的证书请求后，新证书的状态将更改为 Attempting to validate your certificate（正在尝试验证您的证书）。在此期间，Lightsail 会尝试将证书的验证记录添加到您为证书指定的域名的 DNS 中。过段时间以后，状态将更改为 Valid（有效）或 Validation timed out（验证超时）。

如果自动验证失败，则必须验证您是否控制了您在创建证书时为证书指定的所有域名。可以通过将别名记录 (CNAME) 添加到证书上指定的每个域的 DNS 区域，完成此操作。您需要添加的记录列在证书的 Validation details（验证详细信息）部分。

在本指南中，我们为您提供了使用 Lightsail DNS 区域手动验证证书的程序。使用其他 DNS 托管服务提供商（例如 Domain.com 或 GoDaddy）验证证书的过程可能类似。有关 Lightsail DNS 区域的更多信息，请参阅 DNS。

有关 SSL/TLS 证书的更多信息，请参阅 SSL/TLS 证书。

先决条件

在开始之前，您需要为容器服务创建 SSL/TLS 证书。有关更多信息，请参阅创建容器服务的 SSL/TLS 证书。

获取别名记录值以验证证书

完成以下过程，以获取要验证证书必须添加到域的别名记录。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择所需的容器服务的名称，以为其创建证书。
4. 在容器服务管理页面上选择 Custom domains（自定义域）选项卡。
5. 向下滚动到页面的 Attached certificates（附加的证书）部分。

   您的所有证书都列在页面的 “附加证书” 部分下，包括为其他 Lightsail 资源创建的证书和待验证的证书。
6. 找到要验证的证书，展开 Validation details（验证详细信息），记下必须为列出的各个域添加的 CNAME 记录的 Name（名称）和 Value（值）。

   您必须准确地添加这些列出的记录。我们建议您将这些值复制并粘贴到文本文件中，以供之后参考。有关更多信息，请参阅本指南的以下部分将别名记录添加到域的 DNS 区域。

将别名记录添加到域的 DNS 区域

完成以下过程以将别名记录添加到域的 DNS 区域。

1. 在左侧导航窗格中，选择域和 DNS。
2. 在此页面的 DNS zones（DNS 区域）部分，选择所需域名，以将别名记录添加到其中并验证证书。

3. 选择 DNS records（DNS 记录）选项卡。
4. 在 DNS 记录管理页面上，选择 Add record（添加记录）。
5. 在 Record type（记录类型）下拉菜单中，选择 CNAME。
6. 在 Record name（记录名称）文本框中，输入从证书获得的 CNAME 记录的 Name（名称）值。

   Lightsail 控制台会预先填充域的顶级域部分。例如，如果想要添加子域 `www.example.com`，您只需在文本框中输入 `www`，您保存此记录时 Lightsail 会添加 `.example.com` 部分。
7. 在 Route traffic to（将流量路由到）文本框中，输入从证书中获得的 CNAME 记录的 Value（值）部分。
8. 确认您输入的值与要验证的证书上列出的值完全一致。
9. 选择保存图标以将记录保存到 DNS 区域。

   重复这些步骤，为需要验证的证书上的域添加其他别名记录。留出时间以便更改通过 Internet 的 DNS 传播。几分钟后，您应能够查看证书的状态是否已更改为 Valid（有效）。有关更多信息，请参阅本指南的以下查看证书的状态部分。

查看证书的状态

完成以下过程以查看 SSL/TLS 证书的状态。

1. 在左侧导航窗格中，选择容器。
2. 选择所需的容器服务的名称，以查看其证书的状态。
3. 在容器服务管理页面上选择 Custom domains（自定义域）选项卡。
4. 向下滚动到页面的 Attached certificates（附加的证书）部分。

   所有证书都列在页面的 Attached certificates（附加的证书）部分下方，包括状态为 Pending validation（等待验证）和 Valid（有效）的证书。

   > **Note**
   >
   > 如果在验证证书时让 Custom domains（自定义域）页面保持了打开状态，则您可能需要刷新才能查看更新的证书状态。

   Valid（有效）状态可确认您已成功使用添加到域的别名记录验证证书。选择 Details（详细信息）以查看证书的重要日期、加密详细信息、标识和验证记录。证书自验证之日起生效，有效期为 13

个月，之后 Lightsail 会尝试自动重新验证证书。在列出的 Valid until（有效期至）日期重新验证证书时，需要使用添加到域的别名记录，因此请勿删除这些记录。

验证 SSL/TLS 证书后，应为容器服务启用自定义域，以便在服务上使用证书的域名。有关更多信息，请参阅启用和管理容器服务的自定义域。

查看 Lightsail 容器服务的 SSL/TLS 证书

您可以查看为 Lightsail 容器服务创建的 Amazon Lightsail SSL/TLS 证书。您可以通过访问 Lightsail 控制台中任何容器服务的管理页面来完成此操作。

有关 SSL/TLS 证书的更多信息，请参阅 SSL/TLS 证书。

先决条件

在开始之前，您需要创建 Lightsail 容器服务。有关更多信息，请参阅创建 Amazon Lightsail 容器服务和容器服务。

您还应为容器服务创建 SSL/TLS 证书。有关更多信息，请参阅创建容器服务的 SSL/TLS 证书。

查看容器服务 SSL/TLS 证书

完成以下过程以查看容器服务 SSL/TLS 证书。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择容器服务的名称。

   无论您选择哪种容器服务，都可以查看您的所有证书。
4. 在容器服务管理页面上选择 Custom domains（自定义域）选项卡。
5. 向下滚动到页面的 Attached certificates（附加的证书）部分。

   所有证书都列在页面的 Attached certificates（附加的证书）部分下方。选择 Details（详细信息）以查看证书的重要日期、加密详细信息、标识和域。选择 Validation details（验证详细信息）以查看证书的验证记录。证书自创建之日起生效，有效期为 13 个月，之后 Lightsail 会尝试自动重新验证证书。在列出的 Valid until（有效期至）日期重新验证证书时，需要使用添加到域的别名记录，因此请勿删除这些记录。

   有与容器服务搭配使用的有效 SSL/TLS 证书后，您应启用自定义域，以便在服务上使用证书的域名。有关更多信息，请参阅启用和管理自定义域。

使用 SSL/TLS 证书保护 Lightsail CDN 发行版

你可以为你的 Lightsail 发行版创建 Amazon Lightsail TLS/SSL 证书。创建证书时，您可以指定证书的主域名和备用域名。当您为启用分配的自定义域并选择证书时，这些域将添加成为分配的自定义域。更新域的 DNS 记录以指向您的分配后，您的分配将接受流量并使用 HTTPS 提供内容。可以创建的证书数量存在配额。有关更多信息，请参阅 Lightsail Service Quotas。

有关 SSL/TLS 证书的更多信息，请参阅 SSL/TLS 证书。

> **Important**
>
> 您在为分配创建 SSL/TLS 证书时指定的域名不能被所有亚马逊云服务 (AWS) 账户的其他分配（包括亚马逊服务上的分配）使用。 CloudFront 您可以为域创建证书，但您将无法将证书用于您的分配。

先决条件

在开始之前，你需要创建一个 Lightsail 发行版。有关更多信息，请参阅创建分配和内容分发网络分配。

为您的分配创建 SSL/TLS 证书

完成以下过程以为您的分配创建 SSL/TLS 证书。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其创建证书的分配的名称。
4. 在分配的管理页面上选择自定义域选项卡。
5. 向下滚动到页面的 Attached certificates（附加的证书）部分。

   所有的分配证书都将列在页面的 Attached certificates（附加的证书）部分下方，包括为其他分配创建的证书以及正在使用和未使用的证书。
6. 选择创建证书。
7. 在 Certificate name（证书名称）文本框中输入唯一的名称以标识您的证书。然后，选择 Continue（继续）。
8. 在 Specify up to 10 domains or subdomains（最多指定 10 个域或子域）字段中，输入要用于证书的主域名（例如，`example.com`）。

9. （可选）在剩余的 Specify up to 10 domains or subdomains（最多指定 10 个域或子域）字段中输入备用域名（例如 `www.example.com`）。

   您最多可以向证书添加九个备用代域。启用自定义域并为您的分配选择证书后，可以将证书的所有域用于您的分配。

10. 选择创建。

    将提交您的证书请求，并且新证书的状态将更改为Attempting to validate your certificate（正在尝试验证您的证书）。在此期间，Lightsail 会尝试将证书的验证记录添加到主域名的 DNS 中。过段时间以后，状态将更改为 Valid（有效）。

    如果自动验证失败，您需要先使用您的域验证证书，然后才能将证书用于您的分配。有关更多信息，请参阅验证分配的 SSL/TLS 证书。

主题

- 查看 Lightsail 发行版的 SSL/TLS 证书
- 验证 Lightsail 发行版的 SSL/TLS 证书
- 使用最低的 TLS 协议版本保护你的 Lightsail 发行版
- 从 Lightsail 发行版中删除未使用的 SSL/TLS 证书

查看 Lightsail 发行版的 SSL/TLS 证书

你可以查看你为 Lightsail 发行版创建的 Amazon Lightsail SSL/TLS 证书。为此，您可以在 Lightsail 控制台中访问任何发行版的管理页面。

有关 SSL/TLS 证书的更多信息，请参阅 SSL/TLS 证书。

先决条件

在开始之前，你需要创建一个 Lightsail 发行版。有关更多信息，请参阅创建分配和内容分发网络分配。

您还应为分配创建 SSL/TLS 证书。有关更多信息，请参阅创建分配的 SSL/TLS 证书。

查看分配 SSL/TLS 证书

完成以下过程以查看分配 SSL/TLS 证书。

1. 登录 Lightsail 控制台。

2. 在左侧导航窗格中，选择联网。
3. 选择分配的名称。

   无论您选择哪个分配，都可以查看您的所有证书。
4. 在分配的管理页面上选择 Custom domains（自定义域）选项卡。
5. 向下滚动到页面的 Attached certificates（附加的证书）部分。

   您的所有分配证书都列在此页面的 Attached certificates（附加的证书）部分下方。展开 Validation details（验证详细信息）查看证书的重要日期、加密详细信息、标识和验证记录。证书自创建之日起生效，有效期为 13 个月，之后 Lightsail 会尝试自动重新验证证书。在列出的 Valid until（有效期至）日期重新验证证书时，需要使用添加到域的别名记录，因此请勿删除这些记录。

   有与分配搭配使用的有效 SSL/TLS 证书后，您应该启用自定义域，以便可以在分配上使用证书的域名。有关更多信息，请参阅启用分配的自定义域。

验证 Lightsail 发行版的 SSL/TLS 证书

Amazon Lightsail SSL/TLS 证书在创建后必须经过验证，然后才能将其用于 Lightsail 发行版。提交您的证书请求后，新证书的状态将更改为 Attempting to validate your certificate（正在尝试验证您的证书）。在此期间，Lightsail 会尝试将证书的验证记录添加到您为证书指定的域名的 DNS 中。过段时间以后，状态将更改为 Valid（有效）或 Validation timed out（验证超时）。

如果自动验证失败，则必须验证您是否控制了您在创建证书时为证书指定的所有域名。可以通过将别名记录 (CNAME) 添加到证书上指定的每个域的 DNS 区域，完成此操作。您需要添加的记录列在证书的 Validation details（验证详细信息）部分。

在本指南中，我们为您提供了使用 Lightsail DNS 区域手动验证证书的程序。使用其他 DNS 托管服务提供商（例如 Domain.com 或 GoDaddy）验证证书的过程可能类似。有关 Lightsail DNS 区域的更多信息，请参阅 DNS。

有关 SSL/TLS 证书的更多信息，请参阅 SSL/TLS 证书。

内容

- 先决条件
- 获取别名记录值以验证您的证书
- 将别名记录添加到域的 DNS 区域
- 查看分配证书的状态

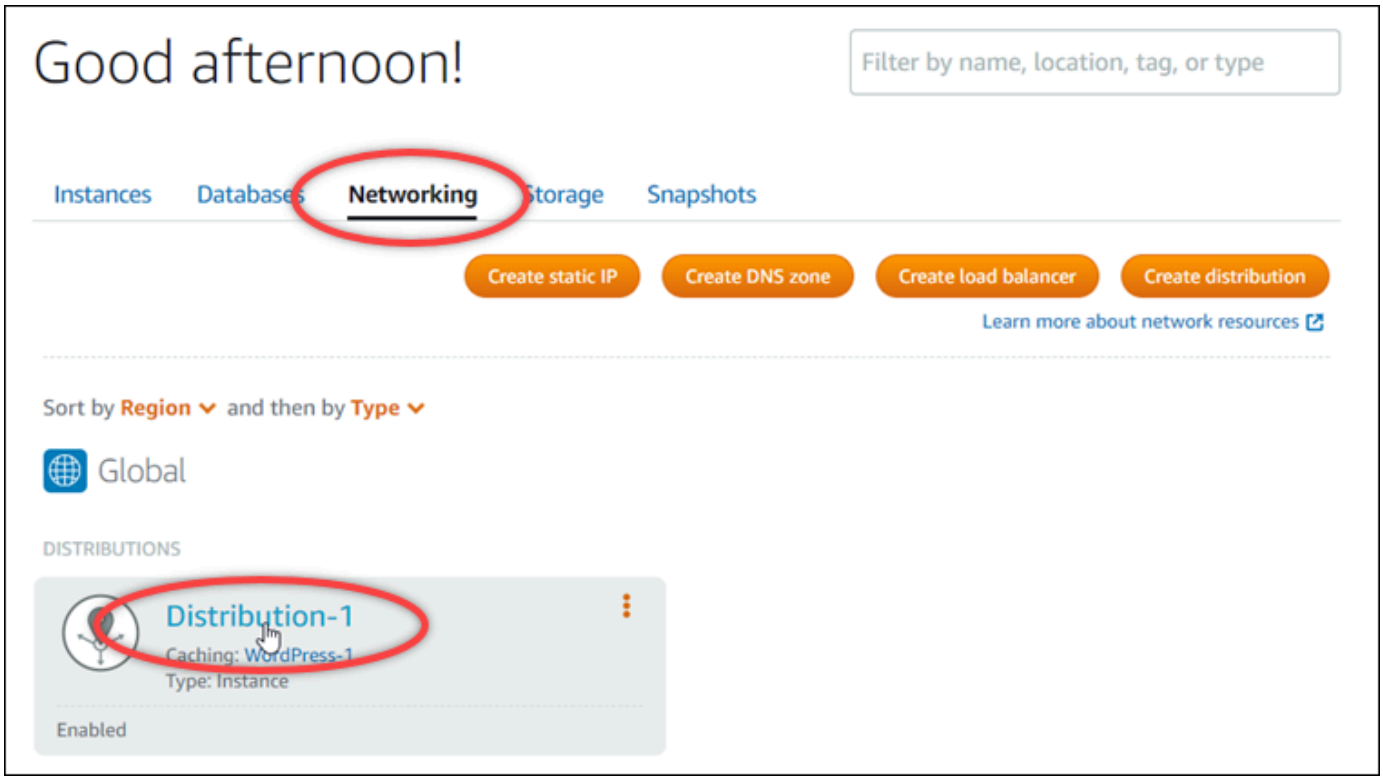
先决条件

在开始之前，您需要为分配创建 SSL/TLS 证书。有关更多信息，请参阅创建分配的 SSL/TLS 证书。

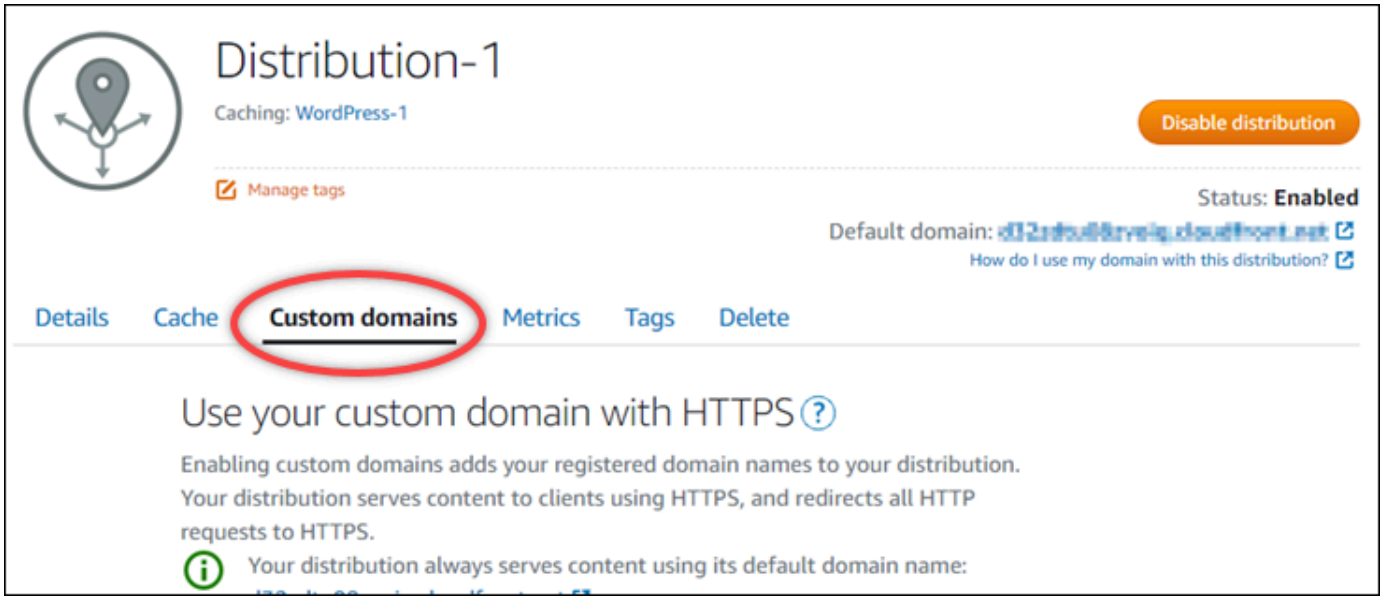
获取别名记录值以验证证书

完成以下过程，以获取要验证证书必须添加到域的别名记录。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要获取其证书别名记录值的分配的名称。



4. 在分配的管理页面上选择自定义域选项卡。



5. 向下滚动到页面的 Attached certificates（附加的证书）部分。

   您的所有分发证书都列在页面的“附加证书”部分下，包括为其他 Lightsail 资源创建的证书和待验证的证书。

6. 找到要验证的证书，展开 Validation details（验证详细信息），记下必须为列出的各个域添加的 CNAME 记录的 Name（名称）和 Value（值）。

   您必须准确地添加这些列出的记录。我们建议您将这些值复制并粘贴到文本文件中，以供之后参考。有关更多信息，请参阅本指南的以下部分将别名记录添加到域的 DNS 区域。

将别名记录添加到域的 DNS 区域

完成以下过程以将别名记录添加到域的 DNS 区域。

1. 在左侧导航窗格中，选择域和 DNS。
2. 在此页面的 DNS zones（DNS 区域）部分，选择所需域名，以将别名记录添加到其中并验证证书。
3. 选择 DNS records（DNS 记录）选项卡。
4. 在 DNS 记录管理页面上，选择 Add record（添加记录）。
5. 在 Record type（记录类型）下拉菜单中，选择 CNAME。
6. 在 Record name（记录名称）文本框中，输入从证书获得的 CNAME 记录的 Name（名称）值。

   Lightsail 控制台会预先填充域的顶级域部分。例如，如果想要添加子域 `www.example.com`，您只需在文本框中输入 `www`，您保存此记录时 Lightsail 会添加 `.example.com` 部分。

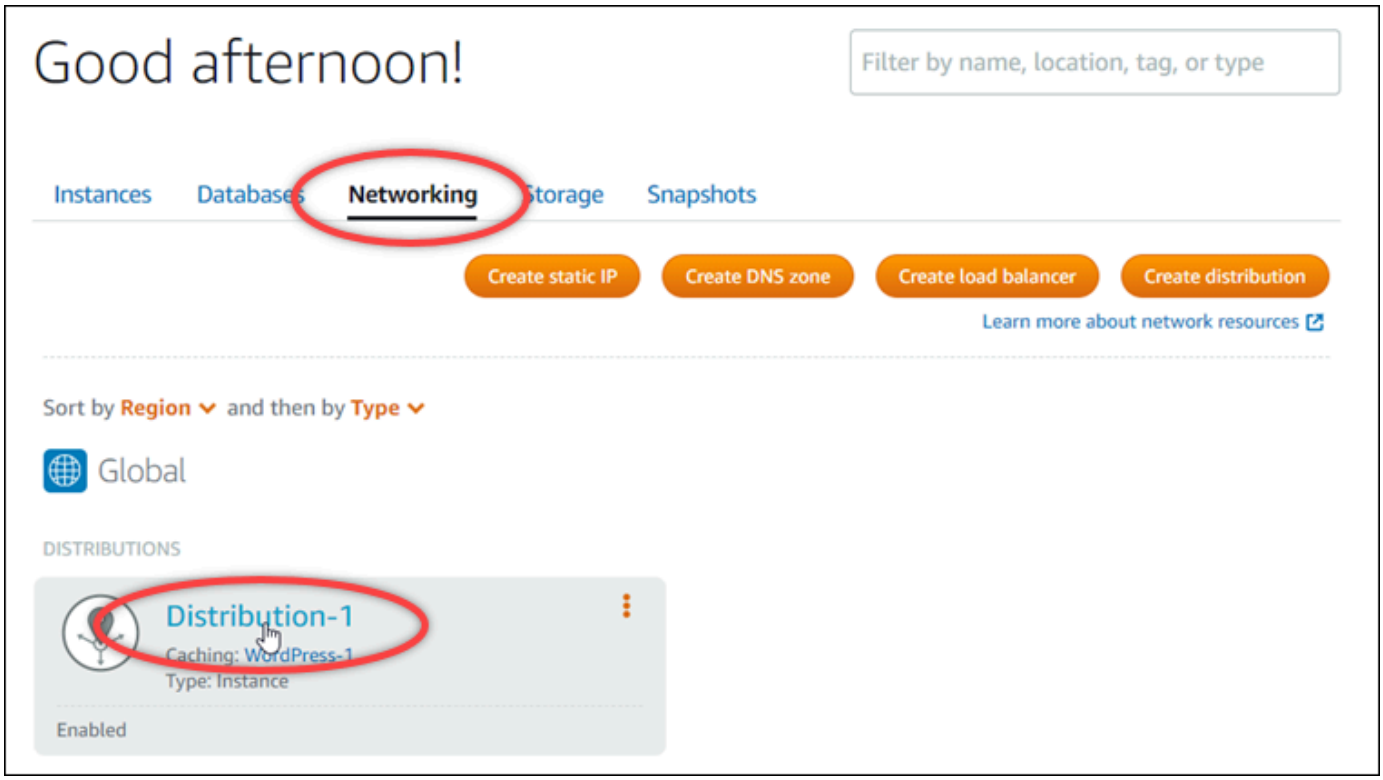
7. 在 Route traffic to（将流量路由到）文本框中，输入从证书中获得的 CNAME 记录的 Value（值）部分。
8. 确认您输入的值与要验证的证书上列出的值完全一致。
9. 选择保存图标以将记录保存到 DNS 区域。

重复这些步骤，为需要验证的证书上的域添加其他别名记录。留出时间以便更改通过 Internet 的 DNS 传播。几分钟后，您应能够看到分配证书的状态是否变为有效。有关更多信息，请参阅本指南的以下查看分配证书的状态部分。

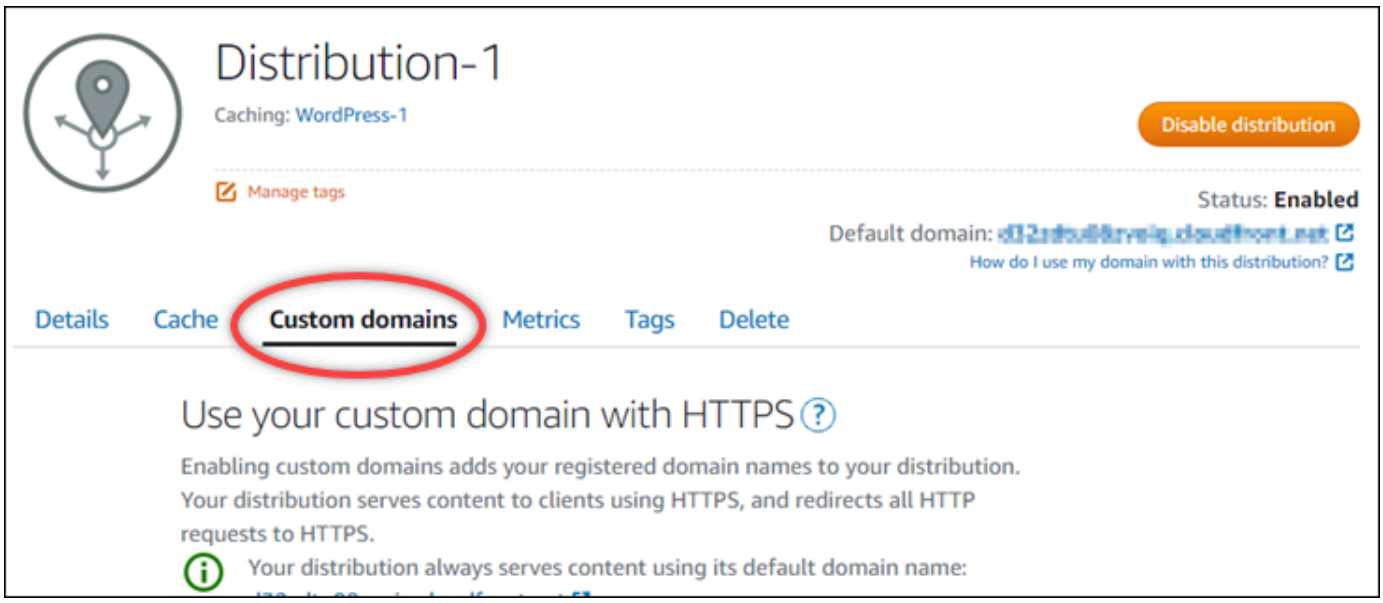
查看分配证书的状态

成以下过程以查看分配的 SSL/TLS 证书状态。

1. 在左侧导航窗格中，选择联网。
2. 选择所需分配的名称，以查看其证书状态。



3. 在分配的管理页面上选择自定义域选项卡。



4. 向下滚动到页面的 Attached certificates（附加的证书）部分。

   所有的分配证书都列在页面的 Attached certificates（附加的证书）部分下方，包括状态为 Pending validation（等待验证）和 Valid（有效）的证书。



   有效状态确认您已使用添加到域的别名记录成功验证证书。选择 Details（详细信息）以查看证书的重要日期、加密详细信息、标识和验证记录。证书自验证之日起生效，有效期为 13 个月，之后 Lightsail 会尝试自动重新验证证书。在列出的 Valid until（有效期至）日期重新验证证书时，需要使用添加到域的别名记录，因此请勿删除这些记录。

   验证 SSL/TLS 证书后，您应该启用分配的自定义域，以便可以在分配上使用证书的域名。有关更多信息，请参阅启用分配的自定义域。

使用最低的 TLS 协议版本保护你的 Lightsail 发行版

亚马逊 Lightsail 使用SSL/TLS certificates to validate custom (registered) domains that you can use with your Lightsail distribution. This guide provides information about the viewer minimum TLS protocol versions (protocol versions) that you can configure for your SSL/TLS certificate. For more information about SSL/TLS证书，请参阅 Lightsail 中的 SSL/TLS 证书。查看器是一种向与您的 Lightsail 发行版关联的边缘站点发出 HTTP 请求的应用程序。有关发行版的更多信息，请参阅 Lightsail 中的内容分发网络分发。

当您为分配启用自定义域时，默认情况下会配置 TLSv1.2_2021 协议版本。如本指南后面所述，您可以配置不同的协议版本。Lightsail 发行版不支持自定义 TLS 协议版本。

受支持的协议

Lightsail 发行版可以使用以下 TLS 协议进行配置：

- （推荐）TLSv1.2_2021
- TLSv1.2_2019
- TLSv1.2_2018
- TLSv1.1_2016

先决条件

满足以下先决条件（如果尚未满足）：

- 创建 Lightsail 内容分发网络发行版
- 创建分配的 SSL/TLS 证书
- 验证分配的 SSL/TLS 证书
- 启用分配的自定义域
- 将域指向该分配

确定您的分配的最低 TLS 协议版本

完成以下步骤以确定您的 Lightsail 发行版的最低 TLS 协议版本

> **Note**
>
> 在本指南中，您将使用 AWS CloudShell 来执行升级。 CloudShell 是一款基于浏览器的预先认证外壳，您可以直接从 Lightsail 控制台启动它。使用 CloudShell，您可以使用首选外壳运行 AWS CLI 命令，例如 Bash PowerShell、或 Z shell。您无需下载或安装命令行工具，即可完成此操作。有关如何设置和使用的更多信息 CloudShell，请参阅 Lightsai AWS CloudShell l 中的。

1. 打开终端、AWS CloudShell 或命令提示符窗口。
2. 输入以下命令以确定您的 Lightsail 发行版的最低 TLS 协议版本。

```
aws lightsail get-distributions --distribution-name DistributionName --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
```

在命令中，*DistributionName*替换为要修改的发行版的名称。

示例

```
aws lightsail get-distributions --distribution-name Distribution-1 --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
```

该命令将返回分配的最低 TLS 协议版本的 ID。

示例

```
"viewerMinimumTlsProtocolVersion": "TLSv1.2_2021"
```

使用配置最低 TLS 协议版本 AWS CLI

完成以下过程以使用 AWS Command Line Interface （ AWS CLI ）配置 TLS 协议版本。使用 `update-distribution` 命令完成此操作。有关更多信息，请参阅AWS CLI 命令参考中的 update-distribution 属性。

1. 打开终端、AWS CloudShell 或命令提示符窗口。
2. 输入以下命令以更改分配的最低 TLS 协议版本。

```
aws lightsail update-distribution --distribution-name DistributionName --viewer-
minimum-tls-protocol-version ProtocolVersion
```

在该命令中，将以下示例文本替换为自己的文本：

- *DistributionName*使用您要更新的发行版的名称。
- *ProtocolVersion*使用有效的 TLS 协议版本。例如，TLSv1.2_2021 或 TLSv1.2_2019。

示例：

```
aws lightsail update-distribution --distribution-name  MyDistribution --viewer-
minimum-tls-protocol-version TLSv1.2_2021
```

您的更改需要一些时间才能生效。

从 Lightsail 发行版中删除未使用的 SSL/TLS 证书

您可以删除不再在分配中使用的亚马逊 Lightsail SSL/TLS 证书。例如，您的证书可能已过期，并且您已附加已验证的更新证书。有关证书的更多信息，请参阅 SSL/TLS 证书。有关分配的更多信息，请参阅内容分发网络分配。

删除 SSL/TLS 证书是最终的，无法撤消。您在 365 天的期限内可以创建的证书数量有一个配额。有关更多信息，请参阅中的 Lightsail 服务配额。AWS 一般参考

删除分配的 SSL/TLS 证书

完成以下过程以为删除分配的 SSL/TLS 证书。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要删除 SSL/TLS 证书的分配的名称。如果证书当前未使用，则可以选择任何分配，因为会在每个分配中列出所有的证书。
4. 在分配的管理页面上选择自定义域选项卡。
5. 在此页面的证书部分中，选择要删除的证书的省略号图标（⋮），然后选择删除。

如果正在使用要删除的证书，则无法使用删除选项。要删除正在使用的证书，您需要先更改使用证书的分配的自定义域，或者在使用证书的分配上禁用自定义域。有关更多信息，请参阅更改分配的自定义域和启用分配的自定义域。

6. 选择是，删除以确认删除。

使用 SSL/TLS 证书为 Lightsail 负载均衡器启用 HTTPS

创建 Lightsail 负载均衡器后，您可以附加传输层安全 (TLS) 证书以启用 HTTPS。通过使用 SSL/TLS 证书，您的负载均衡器可以处理加密的 Web 流量，以便为用户提供更安全的体验。要了解更多信息，请参阅 SSL/TLS 证书。

先决条件

在开始之前，您需要满足以下条件。

- Lightsail 负载均衡器。要了解更多信息，请参阅创建负载均衡器。

创建证书请求

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其配置 SSL/TLS 证书的负载均衡器的名称。
4. 选择 Custom domains（自定义域）选项卡。
5. 选择创建证书。
6. 输入您证书的名称或接受默认值。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
7. 输入主域（`www.example.com`），以及最多 9 个备用域或子域。

   有关更多信息，请参阅将备用域和子域添加到 SSL/TLS 证书。

8. 选择创建证书。

   Lightsail 开始了验证过程。您可以在 72 小时内验证您是否拥有您的域

   在创建证书后，将会看到该证书、域名以及所有备用域和子域。您需要为每个域和子域创建一个 DNS 记录。

后续步骤

- 验证您是否拥有您的域

主题

- 将备用域名和子域名添加到您的 Lightsail SSL/TLS 证书
- 在 Lightsail 中使用别名记录验证 SSL/TLS 证书域
- 将经过验证的 SSL/TLS 证书附加到您的 Lightsail 负载均衡器
- 从 Lightsail 负载均衡器中移除 SSL/TLS 证书

将备用域名和子域名添加到您的 Lightsail SSL/TLS 证书

当您为 Lightsail 负载均衡器创建 SSL/TLS 证书时，您可以向其中添加备用域名和子域名。这些备用名称帮助确保对到您的负载均衡器的所有流量进行加密。

在指定主域时，您可以使用完全限定域名 (如 `www.example.com`) 或顶级域名 (如 `example.com`)。

总域和子域数不能超过 10 个，因此，您最多可以在您的证书中添加 9 个备用域和子域。您可能希望添加类似于以下列表的条目。

- example.com
- example.net
- blog.example.com
- myexamples.com

创建具有备用域和子域的证书

1. 如果尚未创建，请创建一个负载均衡器。
2. 在左侧导航窗格中，选择联网。

3. 选择你的 Lightsail 负载均衡器。
4. 选择 Custom domains（自定义域）选项卡。
5. 选择创建证书。
6. 输入您证书的名称或接受默认名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
7. 输入主域（`www.example.com`），以及最多 9 个备用域或子域。
8. 选择创建证书。

   在创建后，您可以在 72 小时内验证您是否拥有您的域。

后续步骤

- 使用 DNS 验证域所有权

  验证后，您可以选择经过验证的证书，将其与您的 Lightsail 负载均衡器相关联。
- 启用会话持久性

在 Lightsail 中使用别名记录验证 SSL/TLS 证书域

在 Lightsail 中创建 SSL/TLS 证书后，您需要验证自己是否控制了添加到证书中的所有域和子域名。

内容

- 第 1 步：为您的域名创建 Lightsail DNS 区域
- 步骤 2：将记录添加到域的 DNS 记录
- 下一步

第 1 步：为您的域名创建 Lightsail DNS 区域

如果你还没有这样做，请为你的域名创建 Lightsail DNS 区域。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录

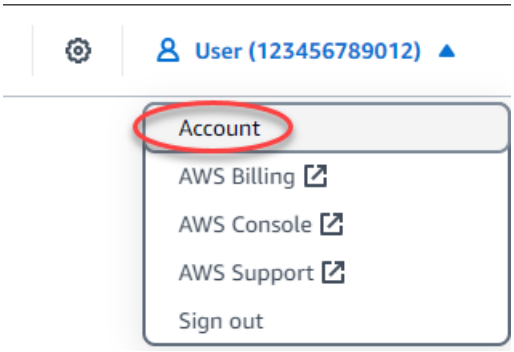
步骤 2：将记录添加到域的 DNS 记录

您创建的证书提供了一组规范名称（CNAME）记录。您可以将这些记录添加到域的 DNS 区域，以验证您拥有或控制该域。

> **Important**
>
> Lightsail 将尝试自动验证您是否控制了您在创建证书时指定的域名或子域名。选择 Create certificate（创建证书）后，CNAME 记录将添加到域的 DNS 区域。如果自动验证成功，证书的状态将从 Attempting to validate your certificate（正在尝试验证您的证书）变为 Valid, in use（有效，正在使用）。
> 如果自动验证失败，请继续执行以下步骤。

在以下步骤中，我们将向您展示如何在 Lightsail 控制台中获取别名记录并将其添加到您的域名的 DNS 区域。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 选择 Certificates (证书) 选项卡。
5. 找到要验证的证书，并记下必须为各个域添加的 CNAME 记录的 Name（名称）和 Value（值）。

   按 Ctrl+C（如果使用的是 Windows）或 Cmd+C（如果使用的是 Mac），以将其复制到剪贴板。



6. 如果你使用的是 Windows 或 TextEdit Mac，请打开文本编辑器，例如记事本。在文本文件中，按 Ctrl+V（如果您使用的是 Windows）或 Cmd+V（如果您使用的是 Mac），以将值粘贴到文本文件中。

   使此文本文件保持打开状态；在本指南的后面部分将记录添加到域的 DNS 区域时，您将需要这些别名记录值。



7. 在 Lightsail 控制台的顶部导航栏上选择 “主页”。
8. 在 Lightsail 主页上选择 “域名和 DNS”。
9. 选择将使用证书的域的 DNS 区域。
10. 在 DNS records（DNS 记录）选项卡中选择 Add record（添加记录）。
11. 为记录类型选择 CNAME（别名记录）。
12. 切换到包含证书的别名记录的文本文件。

    复制别名记录的 Name（名称）。例如，`_1bfb0b9ef15a50f9041e559d2c67b760`。
13. 切换到 DNS 记录页面并将 Name（名称）粘贴到 Record name（记录名称）字段中。

> **Important**
>
> 添加包含域名（如 `.example.com`）的别名记录将导致域名重复（如 `.example.com.example.com`）。为避免重复，请编辑该条目，以便仅添加所需的别名记录部分。这将是 `_1bfb0b9ef15a50f9041e559d2c67b760`。

14. 复制别名记录的值。例如，`_c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws.`。
15. 切换到 DNS 记录页面并将 Value（值）粘贴到 Route traffic to（将流量路由到）字段中。
16. 选择 Save（保存）以添加记录。
17. 如果具有备用子域，请选择 Add record（添加记录）以添加另一个记录。

> **Note**
>
> 要了解有关备用域名或子域名的更多信息，请参阅在 Amazon Lightsail 中将备用域名和子域名添加到您的 SSL/TLS 证书。

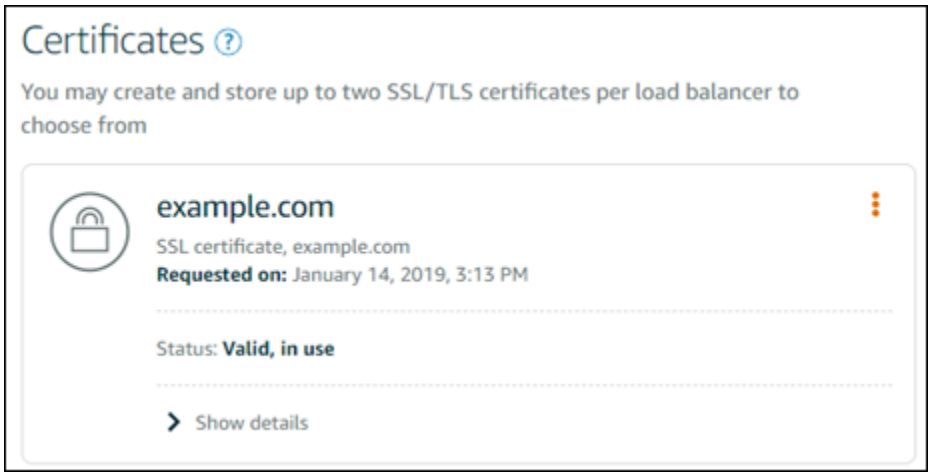
18. 重复步骤 11 - 17 以便为备用子域添加 CNAME 记录。

    在 DNS 区域管理页面上，您还可以添加别名 (A) 记录以指向您的负载均衡器或其他 Lightsail 资源。

    在完成后，您的 DNS 区域应类似于以下屏幕截图。



在经过一段时间后，您的域将被验证，并且您将在证书上看到以下消息。

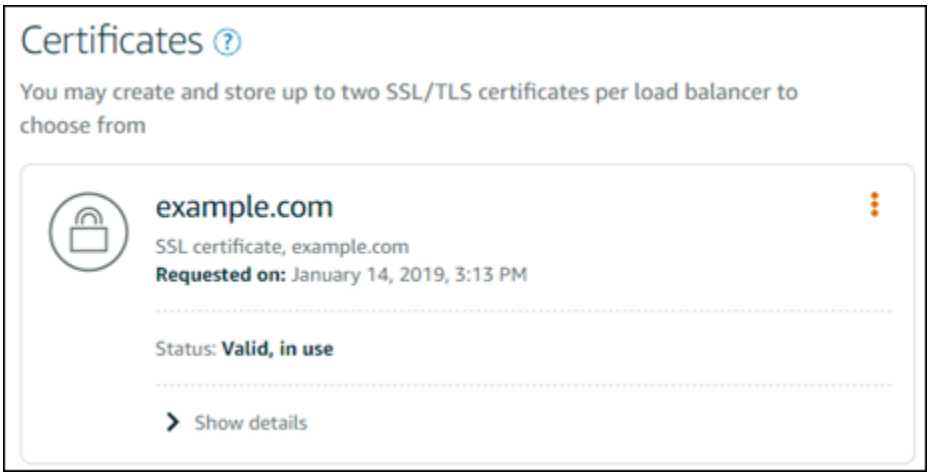


后续步骤

验证您的域后，您便可以将经验证的 SSL/TLS 证书附加到负载均衡器。

将经过验证的 SSL/TLS 证书附加到您的 Lightsail 负载均衡器

验证了您对域的控制后，证书的状态将更改为 Valid（有效）。



下一步是将证书附加到您的 Lightsail 负载均衡器。

1. 在 Lightsail 主页上，选择网络。
2. 选择负载均衡器。
3. 选择 Custom domains（自定义域）选项卡。
4. 在 Certificates（证书）部分中，选择 Attach certificate（附加证书）。

5. 从下拉列表中选择证书。
6. 选择附加以附加证书。

从 Lightsail 负载均衡器中移除 SSL/TLS 证书

您可以删除不再使用的 SSL/TLS 证书。例如，您的证书可能已过期，并且您已附加已验证的更新证书。如果要在删除您的证书之前复制该证书，您可以在下面的步骤 5 中从同一快捷菜单选择 Duplicate（复制）。

> **Important**
>
> 如果要删除的证书有效并且正在使用，您的负载均衡器将无法再处理加密的 (HTTPS) 流量。您的 Lightsail 负载均衡器仍将支持未加密 (HTTP) 流量。
> 删除 SSL/TLS 证书是最终的，无法撤消。您在 365 天的期限内可以创建的证书数量有一个配额。有关更多信息，请参阅《亚马逊云科技 Certificate Manager 用户指南》中的配额。

1. 在左侧导航窗格中，选择联网。
2. 选择将您的 SSL/TLS 证书附加到的负载均衡器。
3. 在负载均衡器的管理页面上选择 Inbound traffic（入站流量）选项卡。
4. 在此页面的证书部分中，选择要删除的证书的省略号图标（⋮），然后选择删除。

   如果要删除的证书处于使用状态，Delete（删除）选项将不可用。要删除处于使用状态的证书，您需要首先更改正在使用证书的负载均衡器的证书，或者在使用证书的负载均衡器上禁用 HTTPS。

配置反向 DNS 以防止你的 Lightsail 实例发送垃圾邮件

电子邮件服务器使用反向域名系统 (DNS) 查找来跟踪邮件的来源，并确认它不是垃圾邮件或恶意邮件。反向 DNS 查找会返回 IP 地址的域名。与之相对，正向 DNS 查找返回的是域的 IP 地址。

例如，如果 IP 地址 `192.168.1.2` 的反向 DNS 查找返回了子域 `mail.example.com`，而子域 `mail.example.com` 的正向 DNS 查找返回了 IP 地址 `192.168.1.2`，则意味着 IP 地址 `192.168.1.2` 的反向 DNS 经过正向确认。要了解更多信息，请参阅维基百科上的正向确认的反向 DNS。

您可以通过完成先决条件，然后向 AWS Support 提交删除出站消息配额的请求来为 Amazon Lightsail 实例配置反向 DNS。后文部分将介绍这些步骤。

先决条件

要配置反向 DNS，请按照所示顺序完成以下先决条件：

1. 创建一个用作电子邮件服务器的 Lightsail 实例。有关更多信息，请参阅创建实例。
2. 创建用于反向 DNS 记录的静态 IP，并将其附加到正在运行的实例上。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

   > **Important**
   >
   > 对于反向 DNS，您不能使用在首次创建实例时分配给实例的默认公有 IP。这是因为，实例的默认公有 IP 会在您停止和启动实例时发生更改。

3. 在域的 DNS 区域中，将指向子域（例如 `mail.example.com`）的别名记录（A 记录）添加到正在运行的实例的静态 IP 地址。这是在执行静态 IP 地址的反向 DNS 查询时返回的子域。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

   > **Note**
   >
   > 我们建议您将域名 DNS 记录的管理权转移给 Lightsail。这使您可以在一个地方（Lightsail 控制台）中管理包括域名在内的所有资源。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

4. 留出时间以便更改通过 Internet 的 DNS 传播。然后，您可以继续向 Amazon Web Services Support 提交请求来配置反向 DNS。

向 Amazon Web Services Support 提交请求以配置反向 DNS

出于安全考虑，Lightsail 默认限制出站邮件通过端口 25。但是，您可以请求 Amazon Web Services Support 消除您账户中的此项配额限制，并为您的静态 IP 配置反向 DNS。

向 Amazon Web Services Support 提交请求

1. 以 AWS 账户根用户身份登录 Lightsail 控制台。

> **Important**
>
> 您必须使用亚马逊云科技账户根用户身份提交请求。有关亚马逊云科技账户根用户的更多信息，请参阅亚马逊云科技账户根用户。

2. 导航到请求消除电子邮件发送限制表单，然后输入以下所需信息：

> **Note**
>
> 该表单引用了 Amazon Elastic Compute (EC2) 资源，例如弹性 IPs (EIPs) 和 EC2 实例。但是，您也可以使用该表单来获取 Lightsail 资源，例如静态实例和 Lig IPs htsail 实例。

- 电子邮件地址 – 输入可接收与请求相关的通信的电子邮件地址。该文本框中预填充了您的账户电子邮件地址。
- 使用案例描述 – 输入请求消除电子邮件配额限制的原因。
- 弹性 IP 地址 – 输入您在本指南前文部分（“先决条件”部分的第 2 步）所连接实例的静态 IP 地址。您最多可输入 2 个静态 IP 地址。
- EIP 的反向 DNS 记录 – 输入您在本指南前文部分（“先决条件”部分的第 3 步）定义的子域。这是在执行反向 DNS 查询时返回的域。

3. 完成后，选择 Submit (提交)。

Amazon Web Services Support 完成您的请求后，您的静态 IP 地址可使用反向 DNS 查找进行正向确认。

如果您以后想从您的 Lightsail 账户中删除静态 IP 地址，则必须向 AWS Support 提交删除反向 DNS 配置的请求。移除反向 DNS 配置后，你可以使用 Lightsail 控制台从 Lightsail 账户中删除静态 IP 地址。有关更多信息，请参阅删除静态 IP。

使用 Lightsail 对象存储桶存储和管理数据

使用 Amazon Lightsail 对象存储服务随时随地从互联网上的任何地方存储和检索对象。该服务旨在降低开发人员进行 Web 级计算的难度，其使用 Amazon Simple Storage Service（Amazon S3）构建。Lightsail 对象存储使您可以访问与 Amazon 用于运行自己的全球网站网络相同的高度可扩展、可靠、快速、廉价的数据存储基础设施。此服务旨在为您带来最大化的规模效益。

对象存储概念

以下概念和术语适用于 Lightsail 对象存储。

存储桶

存储桶是存储在 Lightsail 对象存储服务中的对象的容器。每个对象都包含在存储桶中，而存储桶都具有其自己的 URL。例如，如果名为 `media/sailbot.jpg` 的对象存储在美国东部（弗吉尼亚北部）区域 `us-east-1` 的 `amzn-s3-demo-bucket` 存储桶中，则可使用类似于 `https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg` 的 URL 对该对象进行寻址。

你可以在 Lightsail 可用 AWS 区域 的地方创建存储桶。有关哪个 AWS 区域 Lightsail 在哪些版本中可用的更多信息，请参阅AWS 一般参考中的区域和终端节点。

存储桶存储计划

存储计划（在 AWS API 中称为捆绑包）指定存储桶的每月费用、存储空间和数据传输配额。首次创建存储桶时，您必须选择一个存储计划。存储桶启动并运行后，您稍后可以更改其计划。

在每月 AWS 账单周期内，您只能更改一次存储桶套餐。如果存储桶始终超出其存储空间或数据传输配额，或者存储桶的使用量始终处于其存储空间或数据传输配额的较低范畴，请更改存储桶的计划。由于存储桶可能会遇到不可预测的使用量波动，我们强烈建议您仅将更改存储桶计划作为一项长期策略，而不将其作为每月削减成本的短期措施。选择的存储套餐应在未来很长一段时间内为存储桶提供充足的存储空间和数据传输限额。

对象

对象是存储桶中存储的基本实体。上传到存储桶的文件在存储期间称为对象。对象由数据和元数据组成。数据部分对于 Lightsail 对象存储服务来说是不透明的。元数据是一组描述对象的名称-值对。其中包括一些默认元数据（如最后修改日期）和标准 HTTP 元数据（如 Content-Type）。

在存储桶中，对象将由键名称和版本 ID 进行唯一地标识。

对象键名称

键名称是存储桶中对象的唯一标识符。存储桶内的每个对象都只能有一个键。存储桶、键和版本 ID 的组合唯一标识各个对象。因此，您可以将 Lightsail 对象存储视为 “存储桶 + 密钥 + 版本” 和对象本身之间的基本数据映射。Lightsail 对象存储中的每个对象都可以通过 Web 服务端点、存储桶名称、密钥以及可选的版本（可选）的组合进行唯一寻址。例如，在 URL `https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg` 中，`amzn-s3-demo-bucket` 是存储桶的名称，`media/sailbot.jpg` 是对象键名称。

对象版本控制

版本控制是在相同的存储桶中保留对象的多个变量的功能。启用版本控制，可保留、检索和还原存储桶存储的每个对象的各个版本。使用版本控制能够更加轻松地从用户意外操作和应用程序故障中恢复数据。

默认情况下，在您创建存储桶时，版本控制处于禁用状态。版本控制启用后，您存储在存储桶中的每个对象的各个版本都会保留，直到您手动删除存储的版本。例如，如果您存储 `media/sailbot.jpg` 对象，稍后您存储一个具有相同对象键名称的较大文件，则较小的初始对象将作为先前版本保留。较大的新对象将成为当前版本。如果您认为不再需要此对象的先前版本，则可删除此版本。删除对象的当前版本时，您将删除该对象的所有先前存储版本。

存储对象版本占用存储桶存储空间的方式与存储对象的当前版本方式相同。启用版本控制后，可以暂停此功能，以便停止存储对象版本。上传新对象版本时，这也会占用较少的存储桶存储空间。当版本控制暂停时，将保留存储的对象版本，但不会保留在版本控制暂停期间上传的新对象版本。

存储桶和对象访问

默认情况下，所有对象存储资源（存储桶和对象）都是私有的。这意味着只有存储桶拥有者（创建该存储桶的 Lightsail 账户）才能访问存储分区及其对象。存储桶拥有者可以选择将其访问权限授予其他人员。要实现此目的，可以将所有对象或单个对象设置为公有，这样可让全球各地的人员读取它们。您还可以通过将 Lightsail 实例附加到存储分区或为存储分区创建访问密钥来授予完全编程访问权限。最后，您可以向其他 AWS 账户授予对您的存储桶的编程只读访问权限。

AWS 区域

你可以在所有可用 Lightsail 的存储桶中创建 Lightsail 对象存储桶。 AWS 区域 您可以选择一个区域，以便优化延迟、尽可能降低成本或满足法规要求。存储在中的对象 AWS 区域 不会离开该区域，除非您明确将其转移到另一个区域。例如，在美国西部（俄勒冈州）区域存储的对象将一直保留在该区域。

管理存储桶和对象

Lightsail 对象存储是故意使用最少的功能集构建的，该功能集侧重于简单性和稳健性。以下是管理存储桶和对象的一些元素：

- 创建存储桶 – 创建存储数据的存储桶。存储桶是 Lightsail 对象存储服务中的基本容器。有关更多信息，请参阅创建存储桶。
- 存储数据-使用 Lightsail 控制台 AWS Command Line Interface （AWS CLI）和，将文件上传到您的存储桶。 AWS APIs有关上传文件的更多信息，请参阅将文件上传到存储桶。
- 下载数据 — 随时下载已存储的对象。有关更多信息，请参阅下载存储桶对象。
- 授予访问权限 — 对于要上传数据或下载存储桶中数据的其他人（如软件或个人），授予其访问权限或拒绝其访问。身份验证机制可帮助确保数据安全，以防未授权访问。有关更多信息，请参阅存储桶的权限。
- 管理版本控制 — 启用版本控制，以保留存储桶中存储的每个对象的各个版本。有关更多信息，请参阅启用和暂停存储桶中的对象版本控制。
- 监控使用情况 — 监控存储桶中存储的对象数以及正在使用的存储空间量。有关更多信息，请参阅查看存储桶指标。
- 更改存储计划 — 如果存储桶被超额使用，则提高存储桶的大小；如果存储桶未得到充分利用，则缩小存储桶的大小。有关更多信息，请参阅更改存储桶的套餐。
- 连接您的存储桶 — 将您的 Lightsail 存储桶连接到您的 WordPress 网站以存储网站图像和附件。您也可以将您的存储桶指定为 Lightsail 内容分发网络 (CDN) 分发的来源。这可以加快向世界各地用户传递存储桶中对象的速度。有关更多信息，请参阅教程：将存储桶连接到您的 WordPress 实例和教程：使用带有内容分发网络分发的存储桶。
- 删除存储桶 — 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅删除存储桶。

创建用于存储对象的 Lightsail 存储桶

准备好开始将文件上传到云端时，在 Amazon Lightsail 对象存储服务中创建存储桶。你上传到 Lightsail 对象存储服务的每个文件都存储在 Lightsail 存储桶中。有关存储桶的更多信息，请参阅对象存储。

创建存储桶

完成以下步骤以创建 Lightsail 存储桶。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择创建存储桶。
4. 选择更改 AWS 区域 以选择要在其中创建存储桶的区域。

   我们建议您在创建存储桶时使用的资源与您计划用于存储桶的资源 AWS 区域 相同。创建存储桶后无法更改其区域。
5. 为您的存储桶选择存储计划。

   存储计划指定存储桶的每月成本、存储空间配额和数据传输配额。

   在每月 AWS 账单周期内，您只能更改一次存储桶套餐。如果存储桶始终超出其存储空间或数据传输配额，或者存储桶的使用量始终处于其存储空间或数据传输配额的较低范畴，请更改存储桶的计划。有关更多信息，请参阅更改存储桶的套餐。
6. 输入存储桶的名称。

   有关存储桶名称的更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
7. 选择创建存储桶。

   将重新导向到新存储桶的管理页面。继续本指南的后续步骤部分以获取有关使用和管理存储桶的其他文档。

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

- 在 Amazon Lightsail 中封锁存储桶的公开访问权限
- 在 Amazon Lightsail 中配置存储桶访问权限
- 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
- 在 Amazon Lightsail 中为存储桶创建访问密钥
- 在 Amazon Lightsail 中为存储桶配置资源访问权限
- 在 Amazon Lightsail 中为存储桶配置跨账户访问权限

5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象
9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。

12配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。

13如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。

14.了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。

- 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
- 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶

15如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

删除 Lightsail 对象存储桶

如果您不再使用 Amazon Lightsail 对象存储服务，请将其删除。删除存储桶时，将永久删除存储桶中的所有对象（包括存储的对象版本和访问密钥）。

有关存储桶的更多信息，请参阅对象存储。

强制删除存储桶

除非您确认删除，否则无法删除具有以下条件之一的存储桶：

- 存储桶是分配的源。
- 存储桶有附加的实例。
- 存储桶包含对象。
- 存储桶具有访问密钥。

您必须确认删除操作，以确保不会中断与存储桶相关的现有工作流。例如，在存储桶上存储媒体的 WordPress 网站或在存储桶中缓存和提供对象的分发。

若要确认删除具有上述条件之一的存储桶，您必须强制删除该存储桶。在您删除存储桶之前，Lightsail 服务会提示您存储桶上存在哪些条件。如果您使用 Lightsail 控制台删除存储桶，则可以选择强制将其删除。如果使用 AWS CLI，则必须在`delete-bucket`发出请求时指定`--force-delete`标志。使用 Lightsail控制台删除存储桶和使用本指南删除存储分区 AWS CLI部分介绍了这两个过程。

使用 Lightsail 控制台删除你的存储桶

完成以下过程，使用 Lightsail 控制台删除您的存储桶。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要删除的存储桶的名称。
4. 在选项卡菜单中选择省略号 (⋮) 图标，然后选择删除。
5. 选择删除存储桶。
6. 在显示的提示中，确认您的存储桶是否符合以下任何条件：

   - 包含一个对象
   - 有访问密钥
   - 已附加到实例
   - 是分配的源

   如果存储桶符合上述任何条件，则必须选择强制删除存储桶。
7. 请选择以下选项之一：

   - 选择强制删除以删除您的存储桶，即使存储桶符合此过程的步骤 6 中列出的任何条件。
   - 选择是，删除以删除您的存储桶，如果储桶不符合此过程的步骤 6 中列出的任何条件。
   - 选择否，取消以取消删除。

使用删除您的存储桶 AWS CLI

完成以下过程，使用 AWS Command Line Interface (AWS CLI) 删除您的存储桶。使用 `delete-bucket` 命令完成此操作。有关更多信息，请参阅 AWS CLI Command Reference 中的 delete-bucket。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 在命令提示符或终端窗口中，输入以下命令之一：

   - 输入以下命令以删除不符合本指南的强制删除存储桶部分列出的条件的存储桶。

```
aws lightsail delete-bucket --bucket-name BucketName
```

- 输入以下命令以删除符合本指南的强制删除存储桶部分列出的条件的存储桶。

```
aws lightsail delete-bucket --bucket-name BucketName --force-delete
```

在命令中，*BucketName*替换为要删除的存储桶的名称。

示例：

```
aws lightsail delete-bucket --bucket-name amzn-s3-demo-bucket
```

您会看到类似于以下示例的结果：

```
C:\>aws lightsail delete-bucket --bucket-name DOC-EXAMPLE-BUCKET
{
    "operations": [
        {
            "id": "6example-4d30-4442-ae9a-examplef4f52",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-30T13:42:43.873000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "62example362/DOC-EXAMPLE-BUCKET/small_1_0",
            "operationType": "DeleteBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-30T13:42:43.873000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 禁止公开访问亚马逊 Lightsail 中的存储桶
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，允许用户在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象

- 从 Amazon Lightsail 中的存储桶下载对象
- 在 Amazon Lightsail 中筛选存储桶中的对象
- 在 Amazon Lightsail 中标记存储桶中的对象
- 在 Amazon Lightsail 中删除存储桶中的对象

9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

创建 Lightsail 对象存储桶访问密钥

您可以使用访问密钥创建一组证书，以授予对存储桶及其对象的完全访问权限。访问密钥包含一组访问密钥 ID 和秘密访问密钥。秘密访问密钥仅在您创建它时可见。当您在软件或插件上配置访问密钥时，它可以使用 AWS APIs、和对存储桶拥有完全的读写权限 AWS SDKs。您还可以在 AWS CLI上配置访问密钥。

> **Important**
>
> 尽管每个存储桶可以有两个访问密钥，但我们建议您一次只能创建一个存储桶访问密钥。我们还建议您定期轮换密钥并清点现有密钥。如果您的私有访问密钥被复制、丢失或泄露，则应删除您的访问密钥并创建一个新的访问密钥。有关轮换存储桶访问密钥的最佳实践的更多信息，请参阅轮换存储桶访问密钥。

有关权限选项的更多信息，请参阅存储桶权限。有关存储桶的更多信息，请参阅对象存储。

为存储桶创建访问密钥

完成以下过程以配置存储桶的访问权限。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要为其配置访问权限的存储桶的名称。
4. 选择 Permissions(权限) 选项卡。

   页面的访问密钥部分将显示存储桶的现有访问密钥（如果有）。
5. 要为存储桶创建新密钥，请选择创建访问密钥。
6. 在显示的提示中，选择是，创建以确认您要创建新的访问密钥。否则，选择否，取消。
7. 在显示的成功提示符中，记下访问密钥 ID。
8. 选择显示秘密访问密钥以查看秘密访问密钥，并记下该密钥。不会再显示秘密访问密钥。

   > **Important**
   >
   > 将访问密钥 ID 和秘密访问密钥存储在安全位置。如果发生泄露，您应删除它然后创建一个新的密钥。有关更多信息，请参阅 删除 Lightsail 对象存储桶的访问密钥。
9. 选择继续完成操作。

   新的访问密钥将在页面的访问密钥部分列出。如果访问密钥发生泄露或丢失，可删除访问密钥，然后创建新的访问密钥。

   > **Note**
   >
   > 每个访问密钥旁边显示的上次使用列标识上次使用密钥的时间。如果密钥尚未使用，将显示破折号。展开访问密钥节点以查看服务以及上次使用密钥 AWS 区域 的位置。

删除 Lightsail 对象存储桶的访问密钥

访问密钥是一组证书，用于授予对存储桶及其对象的完全访问权限。访问密钥包含一组访问密钥 ID 和秘密访问密钥。如果您的私有访问密钥被复制、丢失或泄露，则应删除您的访问密钥。

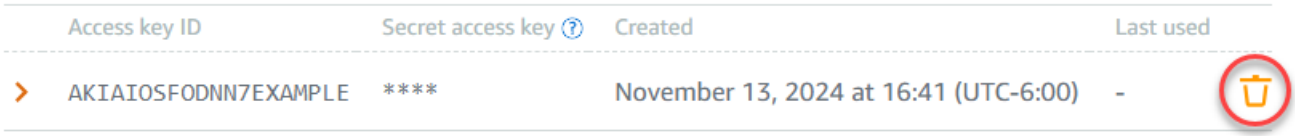
删除存储桶的访问密钥

您可以使用以下过程删除存储桶访问密钥。

> **Warning**
> 在您删除访问密钥后，该密钥将永久消失且无法恢复。您只能将其替换为新的访问密钥。

删除现有的 Lightsail 对象存储桶访问密钥

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要删除其访问密钥的存储桶的名称。
4. 选择 Permissions（权限）选项卡。
5. 在“访问密钥”下，选择要删除的访问密钥的删除图标。



6. 选择“是，删除”继续删除访问密钥。

删除现有密钥后，您可以创建新的访问密钥并针对您的软件或插件进行配置。有关更多信息，请参阅轮换存储桶访问密钥。

限制公众访问 Lightsail 存储桶和对象

Amazon Simple Storage Service（Amazon S3）是一种可让客户存储和保护数据的对象存储服务。Amazon Lightsail 对象存储服务基于亚马逊 S3 技术构建。Amazon S3 提供账户级屏蔽公共访问权限，您可以使用它来限制对 AWS 账户中所有 S3 存储桶的公共访问权限。账户级封禁公有访问权限可以将所有 S3 存储桶设为 AWS 账户 私有，无论现有的个人存储桶和对象权限如何。

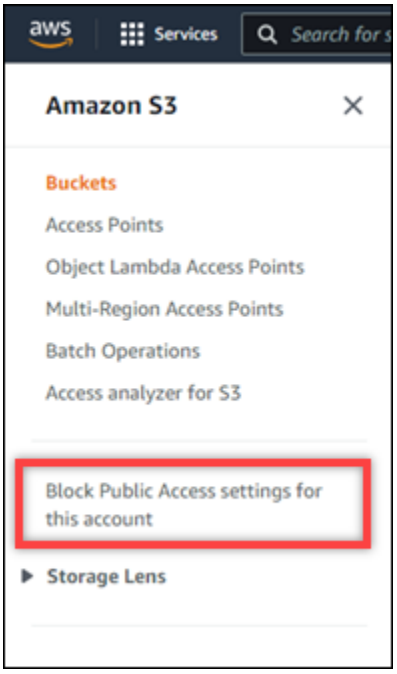
在允许或拒绝公开访问时，Lightsail 对象存储分区会考虑以下因素：

- Lightsail 存储桶访问权限。有关更多信息，请参阅存储桶的权限。
- Amazon S3 账户级别的封锁公共访问配置，它会覆盖 Lightsail 存储桶的访问权限。

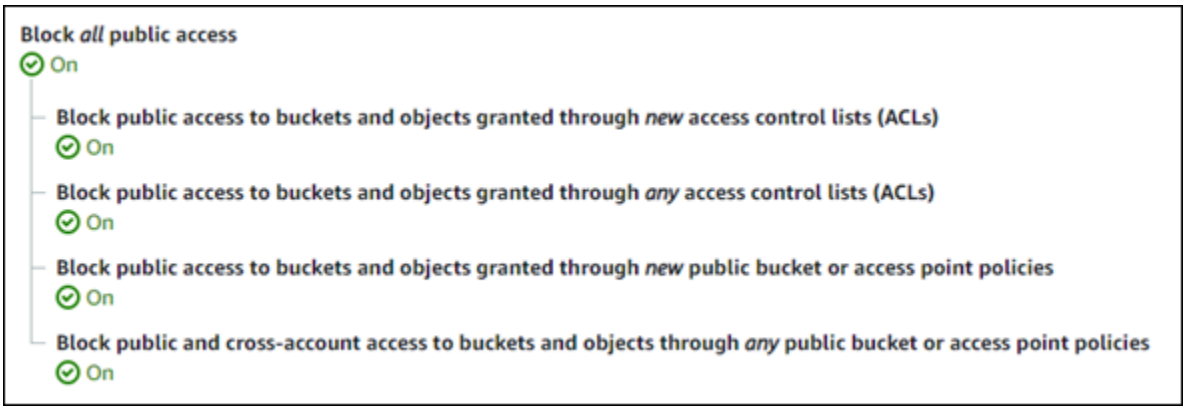
如果您在 Amazon S3 中开启账户级屏蔽所有公开访问权限，则您的公有 Lightsail 存储桶和对象将变为私有且无法再公开访问。

为您的账户配置屏蔽公共访问权限设置

您可以使用 Amazon S3 控制台、 AWS Command Line Interface (AWS CLI) 和 REST API 来配置阻止公共访问设置。 AWS SDKs您可以在 Amazon S3 控制台的导航窗格中访问账户级屏蔽公共访问权限功能，如以下示例所示。



Amazon S3 控制台提供的设置可以屏蔽所有公共访问权限，屏蔽通过新的或任何访问控制列表授予的公共访问权限，以及屏蔽通过新的或任何公有存储桶或接入点策略授予的对存储桶和对象的公共访问权限。



您可以在 Amazon S3 控制台中打开或关闭每个设置。在 API 中，相应的设置为 TRUE（打开）或 FALSE（关闭)。以下各节描述了每种设置对 S3 存储桶和 Lightsail 存储桶的影响。

> **Note**
>
> 以下各节提到了访问控制列表 (ACLs)。ACL 定义拥有或有权访问存储桶或单个对象的用户。有关更多信息，请参阅《Amazon S3 用户指南》中的访问控制列表概述。

- 阻止所有公开访问-启用此设置可阻止对您的 S3 存储桶、Lightsail 存储分区及其相应对象的所有公开访问。此设置包含以下所有设置。启用此设置后，只有您（存储桶所有者）和授权用户可以访问您的存储桶及其对象。您只能在 Amazon S3 控制台中启用此设置。它在 AWS CLI、Amazon S3 API 中不可用，或 AWS SDKs。
  - 阻止对通过新的访问控制列表授予的存储分区和对象的公开访问权限 (ACLs)-启用此设置可阻止对存储分区和对象 ACLs 进行公开访问。此设置不影响现有设置 ACLs。因此，已有公有 ACL 的对象仍然是公有的。由于存储桶访问权限设置为 All objects are public and read-only（所有对象均为公有且只读），因此此设置对公有对象也没有影响。此设置在 Amazon S3 API 中被标记为 `BlockPublicAcls`。

    > **Note**
    >
    > WordPress 启用此设置后，将媒体放入 Lightsail 存储桶中的插件（例如 Offload Media Light 插件）可能会停止工作。这是因为大多数 WordPress 插件都会在对象上配置公共读取 ACL。 WordPress 切换对象的插件也 ACLs 可能停止工作。

  - 阻止对通过任何访问控制列表授予的存储桶和对象的公开访问权限 (ACLs)-启用此设置可忽略公共存储桶 ACLs 和对象，并阻止公共访问存储桶和对象。此设置允许将公共 ACLs 存储桶和对象放在存储桶和对象上，但在授予访问权限时会忽略它们。对于 Lightsail 存储桶，将存储分区的访问权限设置为 “所有对象” 均为公开且只读，或者将单个对象的权限设置为 “公共（只读）”，等同于在两者上设置公有 ACL。此设置在 Amazon S3 API 中被标记为 `IgnorePublicAcls`。
  - 阻止通过新的公共存储分区或接入点策略授予的对存储分区和对象的公开访问权限-启用此设置可阻止在您的 Lightsail 存储分区上配置 “所有对象都是公有的” 和 “只读” 存储分区访问权限。此设置不影响已配置 All objects are public and read-only（所有对象均为公有且只读）存储桶访问权限的存储桶。此设置在 Amazon S3 API 中被标记为 `BlockPublicPolicy`。
  - 通过任何公共存储分区或接入点策略阻止对存储分区和对象的公开和跨账户访问 — 启用此设置可将您的所有 Lightsail 存储分区设为私有。这会将所有 Lightsail 存储分区设为私有，即使它们配置了 “所有对象均为公用” 和 “只读” 存储分区访问权限。此设置在 Amazon S3 API 中被标记为 `RestrictPublicBuckets`。

> **Important**
>
> 此设置还会阻止在 Lightsail 存储分区上配置的跨账户访问，该存储分区还配置了 Lightsail 中的 “所有对象都是公有的” 和 “只读” 存储分区访问权限。要继续允许跨账户访问，请务必在 Lightsail 中将 Lightsail 存储桶配置为 “所有对象均为私有存储桶” 访问权限，然后在 Amazon S3 中启用 “禁止通过任何公用存储桶或接入点策略对存储桶和对象的公开和跨账户访问权限” 设置。

有关屏蔽公共访问权限以及如何对其进行配置的更多信息，请参阅《Amazon S3 用户指南》中的以下资源：

- 阻止对 Amazon S3 存储的公有访问
- 为您的账户配置阻止公有访问设置

使用 Lightsail 控制台、 AWS CLI AWS SDKs、和 REST API 为您的 Lightsail 存储桶配置访问权限。有关更多信息，请参阅存储桶的权限。

> **Note**
>
> Lightsail 使用服务相关角色从 Amazon S3 获取当前账户级别的封禁公开访问配置，并将其应用于 Lightsail 对象存储资源。在 Amazon S3 中配置封锁公共访问后，请至少等待一小时使其在 Lightsail 中生效。有关更多信息，请参阅服务相关角色。

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。

4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 禁止公开访问亚马逊 Lightsail 中的存储桶
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象

9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

使用访问日志跟踪对象存储桶请求

访问日志记录为向 Amazon Lightsail 对象存储服务中的存储桶发出的请求提供了详细记录。这些信息可能包括请求类型、请求中指定的资源以及处理请求的时间和日期。对于许多应用程序而言，访问日志很有用。例如，访问日志信息可能在安全和访问权限审核方面很有用。此外，它还可以帮助您了解您的客户群。

内容

- 启用日志传输需要哪些操作
- 日志对象密钥格式
- 如何传输日志？
- 尽量访问日志传输
- 存储桶日志记录状态更改将逐渐生效

启用日志传输需要哪些操作？

启用日志传输之前，请考虑以下事项。有关详细信息，请参阅启用存储桶访问日志记录。

1. 确定日志的目标存储桶。您希望 Lightsail 在此存储桶中将访问日志保存为对象。源存储桶和目标存储桶必须位于同一个亚马逊云科技区域，并且由同一个账户拥有。

您可以让日志传输至您拥有的且与源存储桶位于同一区域中的任何存储桶，包括源存储桶本身。不过，为了更方便地管理日志，我们建议您将访问日志保存在不同的桶中。

当源桶和目标桶是同一桶时，将为写入该桶的日志创建额外的日志。这样做可能并不理想，因为它会导致您的存储空间使用量小幅增加。此外，有关日志的额外日志可能会导致更难以找到您所查找的日志。如果您选择将访问日志保存在源存储桶中，我们建议您为日志对象键指定前缀，以便对象名称以通用字符串开头，且日志对象更易于识别。当多个桶记录到同一目标桶时，键前缀也可用于区分源桶。

2. （可选）确定日志对象键的前缀。通过该前缀可更方便地查找日志对象。例如，如果您指定前缀值`logs/`，则 Lightsail 创建的每个日志对象都以其键中的`logs/`前缀开头。需要尾部斜杠 / 来表示前缀的末尾。以下是一个采用 `logs/` 前缀的日志对象键示例：

```
logs/2021-11-31-21-32-16-E568B2907131C0C0
```

日志对象密钥格式

Lightsail 对上传到目标存储桶中的日志对象使用以下对象密钥格式：

```
TargetPrefix/YYYY-mm-DD-HH-MM-SS-UniqueString
```

在键中，YYYY、mm、DD、HH、MM 和 SS 分别为日志文件传输时间中表示年、月、日、小时、分钟和秒的数字。这些日期和时间采用协调世界时 (UTC)。

在特定时间传输的日志文件可包含在该时间前的任何时刻编写的记录。无法知道是否已传输特定时间间隔内的所有日志记录。

键的 `UniqueString` 部分用于防止覆盖文件。它没有意义，日志处理软件应忽略它。

如何传输日志？

Lightsail 会定期收集访问日志记录，将记录整合到日志文件中，然后将日志文件作为日志对象上传到目标存储桶。如果您对传输至相同目标存储桶的多个源存储桶启用了日志记录，则此目标存储桶中将保留所有这些源存储桶的访问日志。但是，每个日志对象只会报告特定源存储桶的访问日志记录。

尽量访问日志传输

访问日志记录会以最大努力进行传输。针对已正确配置了日志记录的存储桶的大多数请求会导致传输一条日志记录。大多数日志记录将在记录后的几小时内传输，但可以更频繁地传输这些记录。

因此，不能保证访问日志记录的完整性和即时性。特殊请求的日志记录可能会在实际处理了请求之后进行传输，也可能根本不会传输。访问日志的用途在于向您提供有关存储桶流量性质方面的信息。丢失日志记录的情况十分少见，但是访问日志记录不旨在完整记录所有请求。

存储桶日志记录状态更改将逐渐生效

桶日志记录状态的更改需要一定时间才能实际影响日志文件的传输。例如，如果您为某个桶启用了日志记录，那么将记录在以下时间内发送的请求，而不会记录其他请求。如果您将日志记录的目标桶从桶 A 更改为桶 B，则在接下来的一个小时里仍可能有一些日志传输到桶 A，但其他日志则会传输到新的目标桶 B。无论如何，新的设置将最终生效，并且您无需执行任何操作。

主题

- 使用 Lightsail 存储桶日志分析对象存储访问权限
- 在 Lightsail 中启用存储桶访问日志记录
- 在 Lightsail 中使用亚马逊 Athena 分析存储桶访问日志

使用 Lightsail 存储桶日志分析对象存储访问权限

访问日志记录为向 Amazon Lightsail 对象存储服务中的存储桶发出的请求提供了详细记录。您可以使用访问日志进行安全和访问审计，或者了解客户群。本节介绍了有关访问日志文件的格式和其他详细信息。有关日志记录基本知识的更多信息，请参阅存储桶访问日志。

访问日志文件由一系列的换行分隔日志记录组成。每个日志记录表示一个请求并由空格分隔的字段组成。

以下是含有五份日志记录的示例日志。

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket?versioning HTTP/1.1" 200 - 113 - 7 -
 "-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-demo-bucket.s3.us-
west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
 REST.GET.LOGGING_STATUS - "GET /amzn-s3-demo-bucket?logging HTTP/1.1" 200 -
```

```
 242 - 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mXOcqPGzQOI5XLnCtZNPxev+Hf
+7tpT6sxDwDty4LHBUOZJG96N1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
 REST.GET.BUCKETPOLICY - "GET /amzn-s3-demo-bucket?policy HTTP/1.1" 404
 NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLeMC78iwEIWxs99CRUrbS4n11234= SigV2 ECDHE-RSA-AES128-GCM-SHA256
 AuthHeader amzn-s3-demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:01:00 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket?versioning HTTP/1.1" 200 -
 113 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuUlPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpybfEseEME/u7ME1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:01:57 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /amzn-s3-demo-bucket/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
 10S62Zv81kBW7BB6SX4XJ48o6kpcl6LPwEoizZQQxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
 ECDHE-RSA-AES128-SHA AuthHeader amzn-s3-demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

> **Note**
>
> 任何日志记录字段都可以设置为 - 以指示数据未知或不可用，或者该字段不适用于此请求。

内容

- 日志记录字段
- 复制操作的其他日志记录
- 自定义访问日志信息
- 可扩展访问日志格式的编程注意事项

日志记录字段

以下列表介绍了日志记录字段。

接入点 ARN（Amazon 资源名称）

请求访问点的 Amazon Resource Name (ARN)。如果访问点的 ARN 格式不正确或未使用，则该字段将包含“-”。如需有关访问点的更多信息，请参阅使用访问点。有关更多信息 ARNs，请参阅 AW S 一般参考中有关亚马逊资源名称 (ARN) 的主题。

示例条目

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

存储桶拥有者

源存储桶拥有者的规范用户 ID。规范用户 ID 是另一种形式的 AWS 账户 ID。有关规范用户 ID 的更多信息，请参阅 AWS 一般参考中的 AWS 账户标识符。有关如何查找您的账户的规范用户 ID 的信息，请参阅查找 AWS 账户的规范用户 ID。

示例条目

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

存储桶

请求处理的存储桶的名称。如果系统收到格式错误的请求且无法确定存储桶，则请求不会显示在任何的访问日志中。

示例条目

```
amzn-s3-demo-bucket
```

时间

收到请求的时间；这些日期和时间采用协调世界时 (UTC)。使用 *strftime()* 术语的格式如下所示：*[%d/%b/%Y:%H:%M:%S %z]*

示例条目

```
[06/Feb/2019:00:00:38 +0000]
```

远程 IP

请求者的显式 Internet 地址。中间代理和防火墙可能会隐藏发送请求的计算机的实际地址。

示例条目

```
192.0.2.3
```

请求者

请求者的规范用户 ID 或用于未经验证请求的 -。如果请求者是 IAM 用户，此字段会返回请求者的 IAM 用户名以及该 IAM 用户所属的 AWS 根账户。此标识符与用于访问控制目的的标识符是相同的。

示例条目

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

请求 ID

由 Lightsail 生成的字符串，用于唯一标识每个请求。

示例条目

```
3E57427F33A59F07
```

操作

此处列出的操作将声明为 SOAP.*operation*、REST.*HTTP_method.resource_type*、WEBSITE.*HTTP_method.resource_type* 或 BATCH.DELETE.OBJECT。

示例条目

```
REST.PUT.OBJECT
```

键

请求的“密钥”部分、已编码的 URL 或“-” (如果操作没有使用密钥参数)。

示例条目

```
/photos/2019/08/puppy.jpg
```

请求 URI

HTTP 请求消息的“请求-URI”部分。

示例条目

```
"GET /amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

HTTP 状态

响应的数字 HTTP 状态代码。

示例条目

```
200
```

错误代码

Amazon S3 错误代码或“-”（如果没有发生错误）。

示例条目

```
NoSuchBucket
```

发送的字节数

发送的响应字节数，不包括 HTTP 协议支出或“-” (如果为零)。

示例条目

```
2662992
```

对象大小

所涉及的对象的总大小。

示例条目

```
3462992
```

总时间

从存储桶传输请求的毫秒数。该值计算从收到请求到发出响应的最后一个字节的时间。由于网络延迟，从客户端计算出的时间可能会更长。

示例条目

```
70
```

周转时间

Lightsail 处理您的请求所花费的毫秒数。该值计算从收到您的请求的最后一个字节到发出响应的第一个字节的时间。

示例条目

```
10
```

引用

HTTP 引用站点标头的值（如果存在）。发送请求时，HTTP 用户代理（例如，浏览器）通常会将此标头设置为链接的 URL 或嵌入页面。

示例条目

```
"http://www.amazon.com/webservices"
```

用户代理

HTTP 用户代理标头的值。

示例条目

```
"curl/7.15.1"
```

版本 ID

请求中的版本 ID；如果操作没有使用 `versionId` 参数，则为 `-`。

示例条目

```
3HL4kqtJvjVBH40Nrjfkd
```

主机 ID

x-amz-id-2 或 Lightsail 扩展请求编号。

示例条目

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

签名版本

签名版本，用于对请求进行身份验证的 SigV2 或 SigV4，或未经身份验证的请求的 -。

示例条目

```
SigV2
```

密码套件

协商 HTTPS 请求的安全套接字层 (SSL) 密码或协商 HTTP 的 -。

示例条目

```
ECDHE-RSA-AES128-GCM-SHA256
```

身份验证类型

所使用的请求身份验证的类型，身份验证标头使用 AuthHeader，查询字符串（预签名 URL）使用 QueryString，未经身份验证的请求使用 -。

示例条目

```
AuthHeader
```

主机标头

用于连接 Lightsail 的端点。

示例条目

```
s3.us-west-2.amazonaws.com
```

TLS 版本

客户端协商的传输层安全性 (TLS) 版本。为以下值之一：TLSv1、TLSv1.1、TLSv1.2；如果不使用 TLS 则为 -。

示例条目

```
TLSv1.2
```

复制操作的其他日志记录

复制操作包括 GET 和 PUT。出于该原因，我们会在执行复制操作时记录两份记录。前面的部分描述了与操作的 PUT 部分相关的字段。以下列表描述了记录中与复制操作的 GET 部分相关的字段。

存储桶拥有者

用于存储将复制的对象的存储桶的规范用户 ID。规范用户 ID 是另一种形式的 AWS 账户 ID。有关规范用户 ID 的更多信息，请参阅 AWS 一般参考中的 AWS 账户标识符。有关如何查找您的账户的规范用户 ID 的信息，请参阅查找 AWS 账户的规范用户 ID。

示例条目

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

存储桶

用于存储被复制对象的存储桶的名称。

示例条目

```
amzn-s3-demo-bucket
```

时间

收到请求的时间；这些日期和时间采用协调世界时 (UTC)。使用 strftime() 术语的格式如下所示：[%d/%B/%Y:%H:%M:%S %z]

示例条目

```
[06/Feb/2019:00:00:38 +0000]
```

远程 IP

请求者的显式 Internet 地址。中间代理和防火墙可能会隐藏发送请求的计算机的实际地址。

示例条目

```
192.0.2.3
```

请求者

请求者的规范用户 ID 或用于未经验证请求的 -。如果请求者是 IAM 用户，此字段将返回请求者的 IAM 用户名与该 IAM 用户所属的 AWS 根账户。此标识符与用于访问控制目的的标识符是相同的。

示例条目

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

请求 ID

由 Lightsail 生成的字符串，用于唯一标识每个请求。

示例条目

```
3E57427F33A59F07
```

操作

此处列出的操作将声明为 SOAP.*operation*、REST.*HTTP_method.resource_type*、WEBSITE.*HTTP_method.resource_type* 或 BATCH.DELETE.OBJECT。

示例条目

```
REST.COPY.OBJECT_GET
```

键

被复制对象的“密钥”或“-” (如果操作没有使用密钥参数)。

示例条目

```
/photos/2019/08/puppy.jpg
```

请求 URI

HTTP 请求消息的“请求-URI”部分。

示例条目

```
"GET /amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-foo=bar"
```

HTTP 状态

复制操作的 GET 部分的数字 HTTP 状态代码。

示例条目

```
200
```

错误代码

复制操作的 GET 部分的 Amazon S3 错误代码或 - （如果没有发生任何错误）。

示例条目

```
NoSuchBucket
```

发送的字节数

发送的响应字节数，不包括 HTTP 协议支出或“-” (如果为零)。

示例条目

```
2662992
```

对象大小

所涉及的对象的总大小。

示例条目

```
3462992
```

总时间

从存储桶传输请求的毫秒数。该值计算从收到请求到发出响应的最后一个字节的时间。由于网络延迟，从客户端计算出的时间可能会更长。

示例条目

```
70
```

周转时间

Lightsail 处理您的请求所花费的毫秒数。该值计算从收到您的请求的最后一个字节到发出响应的第一个字节的时间。

示例条目

```
10
```

引用

HTTP 引用站点标头的值（如果存在）。发送请求时，HTTP 用户代理（例如，浏览器）通常会将此标头设置为链接的 URL 或嵌入页面。

示例条目

```
"http://www.amazon.com/webservices"
```

用户代理

HTTP 用户代理标头的值。

示例条目

```
"curl/7.15.1"
```

版本 ID

被复制对象的版本 ID 或 -（如果 `x-amz-copy-source` 标头没有将 `versionId` 参数指定为复制源的一部分）。

示例条目

```
3HL4kqtJvjVBH40Nrjfkd
```

主机 ID

x-amz-id-2 或 Lightsail 扩展请求编号。

示例条目

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

签名版本

签名版本，用于对请求进行身份验证的 SigV2 或 SigV4，或未经身份验证的请求的 -。

示例条目

```
SigV2
```

密码套件

协商 HTTPS 请求的安全套接字层 (SSL) 密码或协商 HTTP 的 -。

示例条目

```
ECDHE-RSA-AES128-GCM-SHA256
```

身份验证类型

所使用的请求身份验证的类型，身份验证标头使用 AuthHeader，查询字符串（预签名 URL）使用 QueryString，未经身份验证的请求使用 -。

示例条目

```
AuthHeader
```

主机标头

用于连接 Lightsail 的端点。

示例条目

```
s3.us-west-2.amazonaws.com
```

TLS 版本

客户端协商的传输层安全性 (TLS) 版本。为以下值之一：TLSv1、TLSv1.1、TLSv1.2；如果不使用 TLS 则为 -。

示例条目

```
TLSv1.2
```

自定义访问日志信息

您可以包含要存储在请求的访问日志记录中的自定义信息。为此，请将自定义查询字符串参数添加到请求的 URL 中。Lightsail 会忽略以 “x-” 开头的查询字符串参数，但会将这些参数作为日志记录Request-URI字段的一部分包含在请求的访问日志记录中。

例如，GET 的 "s3.amazonaws.com/amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-user=johndoe" 请求工作方式与 "s3.amazonaws.com/amzn-s3-demo-bucket/photos/2019/08/puppy.jpg" 的请求的相同，只是 "x-user=johndoe" 字符串包含在关联日志记录的 Request-URI 字段中。此功能仅在 REST 界面中可用。

可扩展访问日志格式的编程注意事项

有时我们可能会通过向每一行的末尾添加新字段来扩展访问日志记录格式。因此，您应该编写解析访问日志的任何代码，以处理后续可能未知的字段。

在 Lightsail 中启用存储桶访问日志记录

访问日志记录为向 Amazon Lightsail 对象存储服务中的存储桶发出的请求提供了详细记录。对于许多应用程序而言，访问日志很有用。例如，访问日志信息可能在安全和访问权限审核方面很有用。此外，它还可以帮助您了解您的客户群。

默认情况下，Lightsail 不会收集存储桶的访问日志。启用日志记录后，Lightsail 会将源存储桶的访问日志传送到您选择的目标存储桶。源存储桶和目标存储桶必须位于同一个存储桶中， AWS 区域 并且由同一个账户拥有。

访问日志记录包含有关对存储桶做出的请求的详细信息。这些信息可能包括请求类型、请求中指定的资源以及处理请求的时间和日期。在本指南中，我们将向您展示如何使用 Lightsail API、 AWS Command Line Interface AWS CLI() 或 AWS 为存储桶启用或禁用访问日志记录。 SDKs

有关日志记录基本知识的更多信息，请参阅存储桶访问日志。

内容

- 访问日志记录的成本
- 使用 AWS CLI启用访问日志记录
- 使用 AWS CLI禁用访问日志记录

访问日志记录的成本

在存储桶上启用访问日志记录不收取额外费用。但是，系统提交给存储桶的日志文件将会占用存储空间。您可以随时删除日志文件。如果日志存储桶的数据传输在配置的月度限额内，我们不会评估日志文件传输的数据传输费。

您的目标存储桶不应启用访问日志记录。您可以让日志传输至您拥有的且与源存储桶位于同一区域中的任何存储桶，包括源存储桶本身。不过，为了更方便地管理日志，我们建议您将访问日志保存在不同的存储桶中。

使用启用访问日志记录 AWS CLI

要为您的存储桶启用访问日志记录，我们建议您在每个 AWS 区域 存储桶中创建一个专用的日志存储桶。然后，将访问日志传输到该专用日志记录存储桶。

完成以下步骤，以使用 AWS CLI启用访问日志记录。

> **Note**
>
> 在继续执行此过程之前，必须为 Lightsail 安装 AWS CLI 并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 在本地计算机上打开命令提示符或终端窗口。
2. 输入以下命令以启用访问日志记录。

```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
 "{\"enabled\": true, \"destination\": \"TargetBucketName\", \"prefix\":
 \"ObjectKeyNamePrefix/\"}"
```

在该命令中，将以下示例文本替换为自己的文本：

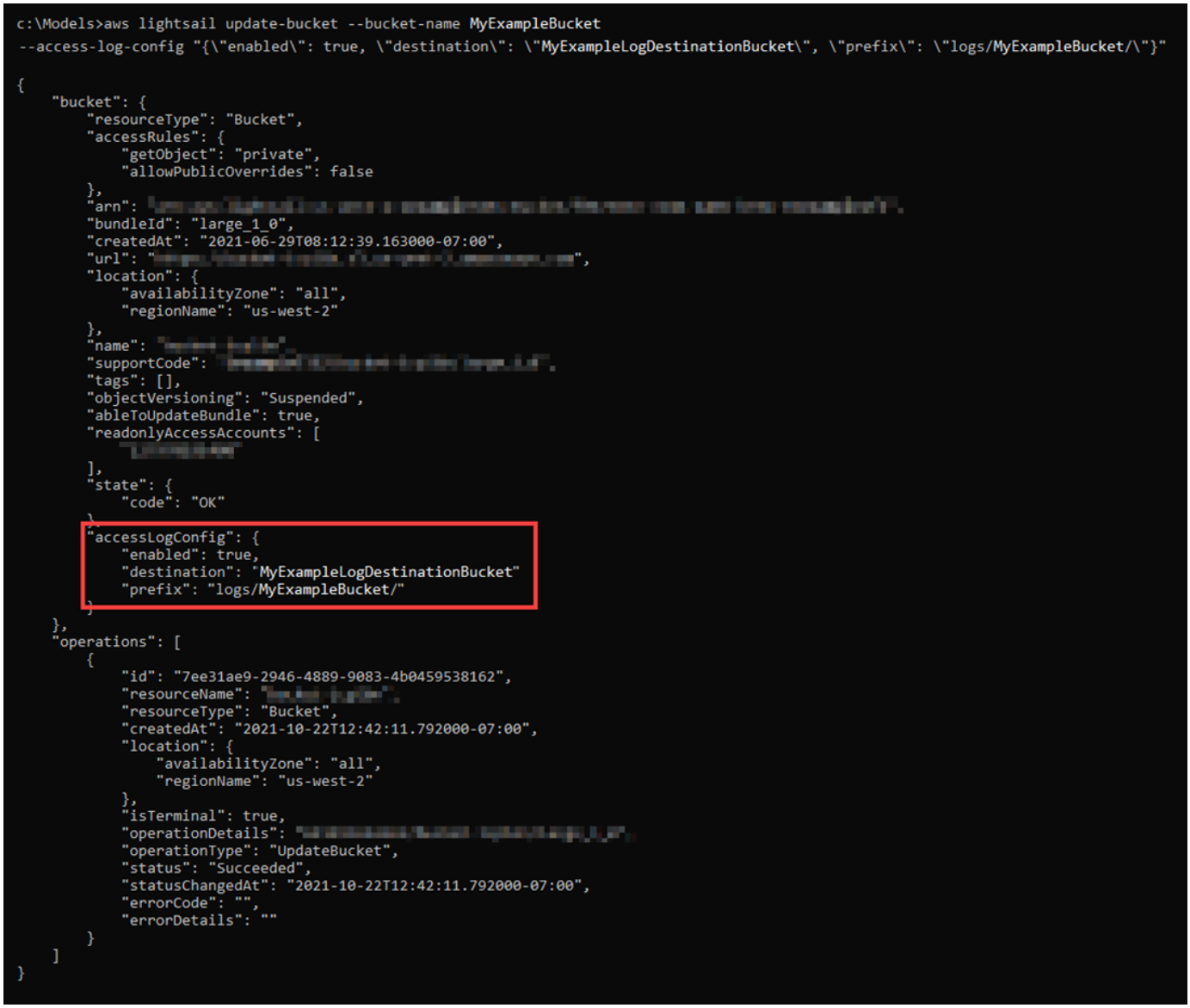
- *SourceBucketName*-将为其创建访问日志的源存储桶的名称。
- *TargetBucketName*— 将保存访问日志的目标存储桶的名称。
- *ObjectKeyNamePrefix/*-访问日志的可选对象密钥名称前缀。请注意，前缀必须以正斜杠 (/) 结尾。

示例

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket1 --access-log-config
 "{\"enabled\": true, \"destination\": \"amzn-s3-demo-bucket2\", \"prefix\":
 \"logs/amzn-s3-demo-bucket1/\"}"
```

在示例中，*amzn-s3-demo-bucket1*是要为其创建访问日志的源存储桶，*amzn-s3-demo-bucket2*是保存访问日志的目标存储桶，*logs/amzn-s3-demo-bucket1/*也是访问日志的对象密钥名称前缀。

运行命令之后，您应看到类似于以下示例的结果。源存储桶已更新，访问日志应开始生成并存储在目标存储桶中。



使用禁用访问日志记录 AWS CLI

完成以下步骤，以使用 AWS CLI禁用访问日志记录。

> **Note**
>
> 在继续执行此过程之前，必须为 Lightsail 安装 AWS CLI 并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 在本地计算机上打开命令提示符或终端窗口。
2. 输入以下命令禁用访问日志记录。

```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
 "{\"enabled\": false}"
```

在命令中，替换*SourceBucketName*为要禁用访问日志记录的源存储桶的名称。

示例

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket --access-log-config
 "{\"enabled\": false}"
```

运行命令之后，您应看到类似于以下示例的结果。

```
>aws lightsail update-bucket --bucket-name MyExampleBucket --access-log-config "{\"enabled\": false}"
{
    "bucket": {
        "resourceType": "Bucket",
        "accessRules": {
            "getObject": "private",
            "allowPublicOverrides": false
        },
        "arn": "
        "bundleId": "large_1_0",
        "createdAt": "2021-06-29T08:12:39.163000-07:00",
        "url": "
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "name": "
        "supportCode": "
        "tags": [],
        "objectVersioning": "Suspended",
        "ableToUpdateBundle": true,
        "readonlyAccessAccounts": [
            "
        ],
        "state": {
            "code": "OK"
        },
        "accessLogConfig": {
            "enabled": false
        }
    },
    "operations": [
        {
            "id": "
            "resourceName": "
            "resourceType": "Bucket",
            "createdAt": "2021-10-22T13:24:36.881000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "
            "operationType": "UpdateBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-10-22T13:24:36.881000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

在 Lightsail 中使用亚马逊 Athena 分析存储桶访问日志

在本指南中，我们向您介绍如何使用访问日志确定对存储桶所做的请求。有关更多信息，请参阅存储桶访问日志。

内容

- 使用 Amazon Athena 查询请求的访问日志
- 使用 Amazon S3 访问日志确定对象访问请求

使用 Amazon Athena 查询请求的访问日志

您可以使用 Amazon Athena 查询和确定对访问日志中的存储桶所做的请求。

Lightsail 将访问日志作为对象存储在 Lightsail 存储桶中。使用可以分析日志的工具通常会更轻松。Athena 支持分析对象，并且可用于查询访问日志。

示例

以下示例展示了如何在 Amazon Athena 中查询存储桶服务器访问日志。

> **Note**
>
> 要在 Athena 查询中指定存储桶位置，您需要格式化目标 存储桶名称和目标前缀，其中日志以 S3 URI 形式传递，如下所示：`s3://amzn-s3-demo-bucket1-logs/prefix/`

1. 从 https://console.aws.amazon.com/athena/ 打开 Athena 控制台。
2. 在查询编辑器中，运行类似如下的命令。

```
create database bucket_access_logs_db
```

> **Note**
>
> 最佳做法是在与 S3 存储桶 AWS 区域 相同的地方创建数据库。

3. 在查询编辑器中，运行类似如下的命令以便在步骤 2 中创建的数据库中创建一个表架构。STRING 和 BIGINT 数据类型值是访问日志属性。您可以在 Athena 中查询这些属性。对于 LOCATION，请输入之前记下的存储桶和前缀。

```
CREATE EXTERNAL TABLE `s3_access_logs_db.amzn-s3-demo-bucket_logs`(
  `bucketowner` STRING,
  `bucket_name` STRING,
  `requestdatetime` STRING,
  `remoteip` STRING,
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
```

```
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
  `turnaroundtime` STRING,
  `referrer` STRING,
  `useragent` STRING,
  `versionid` STRING,
  `hostid` STRING,
  `sigv` STRING,
  `ciphersuite` STRING,
  `authtype` STRING,
  `endpoint` STRING,
  `tlsversion` STRING)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://amzn-s3-demo-bucket1-logs/prefix/'
```

4. 在导航窗格中，在 Database (数据库) 下，请选择您的数据库。
5. 在 Tables (表) 下，请选择表名称旁边的 Preview table (预览表)。

   在 Results (结果) 窗格中，您应看到来自服务器访问日志中的数据，如 bucketowner、bucket、requestdatetime 等。这表示您成功创建了 Athena 表。您现在可以查询存储桶服务器访问日志。

示例 — 显示对象删除者和删除事件（时间戳、IP 地址和 IAM 用户）

```
SELECT RequestDateTime, RemoteIP, Requester, Key
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

示例 — 显示 IAM 用户执行的所有操作

```
SELECT *
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

示例 — 显示在特定时间段内对对象执行的所有操作

```
SELECT *
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE Key='prefix/images/picture.jpg'
    AND parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
    BETWEEN parse_datetime('2017-02-18:07:00:00','yyyy-MM-dd:HH:mm:ss')
    AND parse_datetime('2017-02-18:08:00:00','yyyy-MM-dd:HH:mm:ss');
```

示例 — 显示在特定时间段内特定 IP 地址传输的数据量

```
SELECT SUM(bytessent) AS uploadTotal,
      SUM(objectsize) AS downloadTotal,
      SUM(bytessent + objectsize) AS Total
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE RemoteIP='1.2.3.4'
AND parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2017-06-01','yyyy-MM-dd')
AND parse_datetime('2017-07-01','yyyy-MM-dd');
```

使用 Amazon S3 访问日志确定对象访问请求

对于诸如 GET、PUT 和 DELETE 等操作，您可以对访问日志使用查询以确定对象访问请求，并发现有关这些请求的进一步信息。

以下 Amazon Athena 查询示例说明了如何从服务器访问日志中获取存储桶的所有 PUT 对象请求。

示例 — 显示将在特定期间内发送 PUT 对象请求的所有请求者

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db
WHERE Operation='REST.PUT.OBJECT' AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

以下 Amazon Athena 查询示例说明了如何从服务器访问日志中获取 Amazon S3 的所有 GET 对象请求。

示例 — 显示将在特定期间内发送 GET 对象请求的所有请求者

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db
WHERE Operation='REST.GET.OBJECT' AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

以下 Amazon Athena 查询示例说明了如何从服务器访问日志中获取向 S3 存储桶发出的所有匿名请求。

示例 — 显示在特定时间段内向存储桶发出请求的所有匿名请求者

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE Requester IS NULL AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

> **Note**
>
> - 您可以修改日期范围，以满足您的需要。
> - 也可以使用这些查询示例进行安全监控。您可以查看意外或未经授权的 IP 地址/请求者的 `PutObject` 或 `GetObject` 调用结果，以及确定向桶发出的任何匿名请求。
> - 此查询仅从启用了日志记录的时间检索信息。

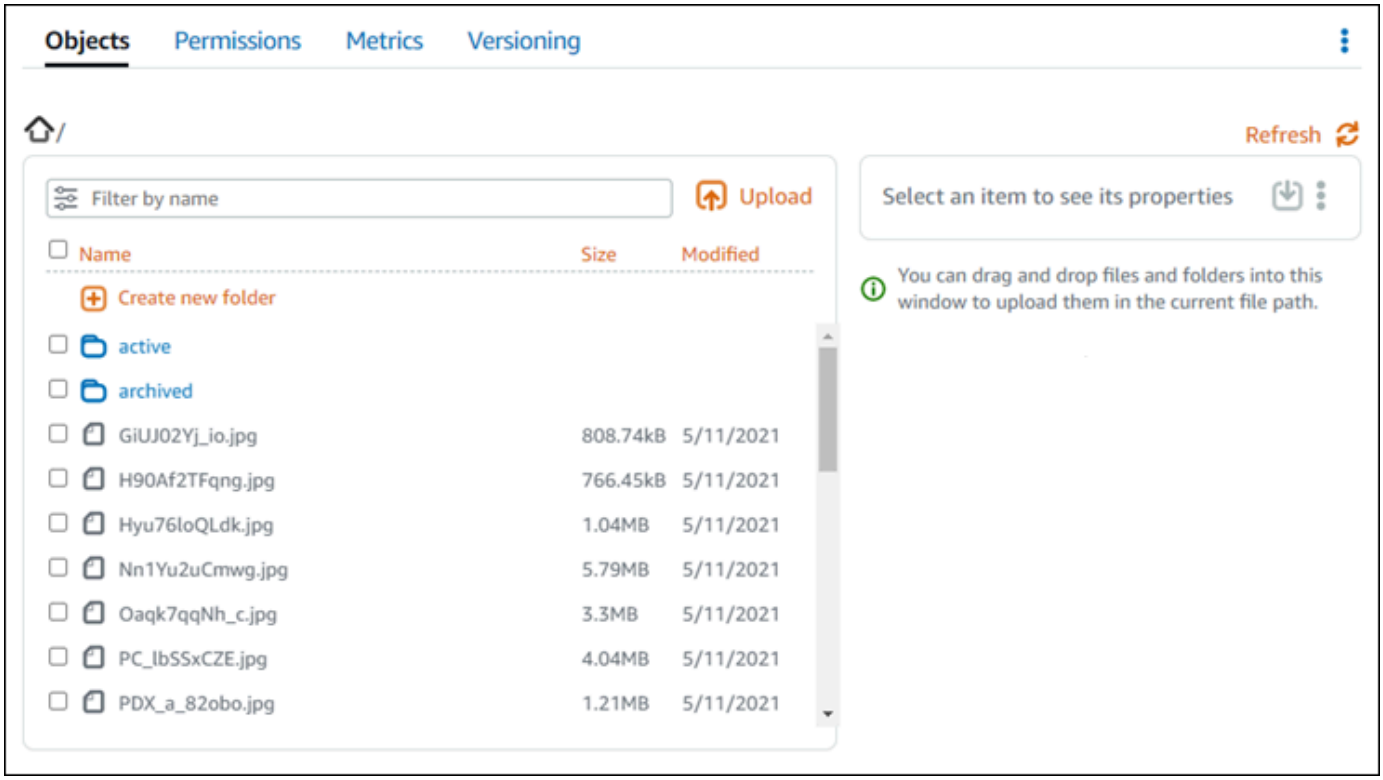
管理 Lightsail 存储桶中的文件和文件夹

您可以使用 Lightsail 控制台在 Amazon Lightsail 对象存储服务中查看存储在存储桶中的所有对象。您还可以使用 AWS Command Line Interface (AWS CLI) 和 AWS 列 SDKs 出存储桶中的对象密钥。有关存储桶的更多信息，请参阅对象存储。

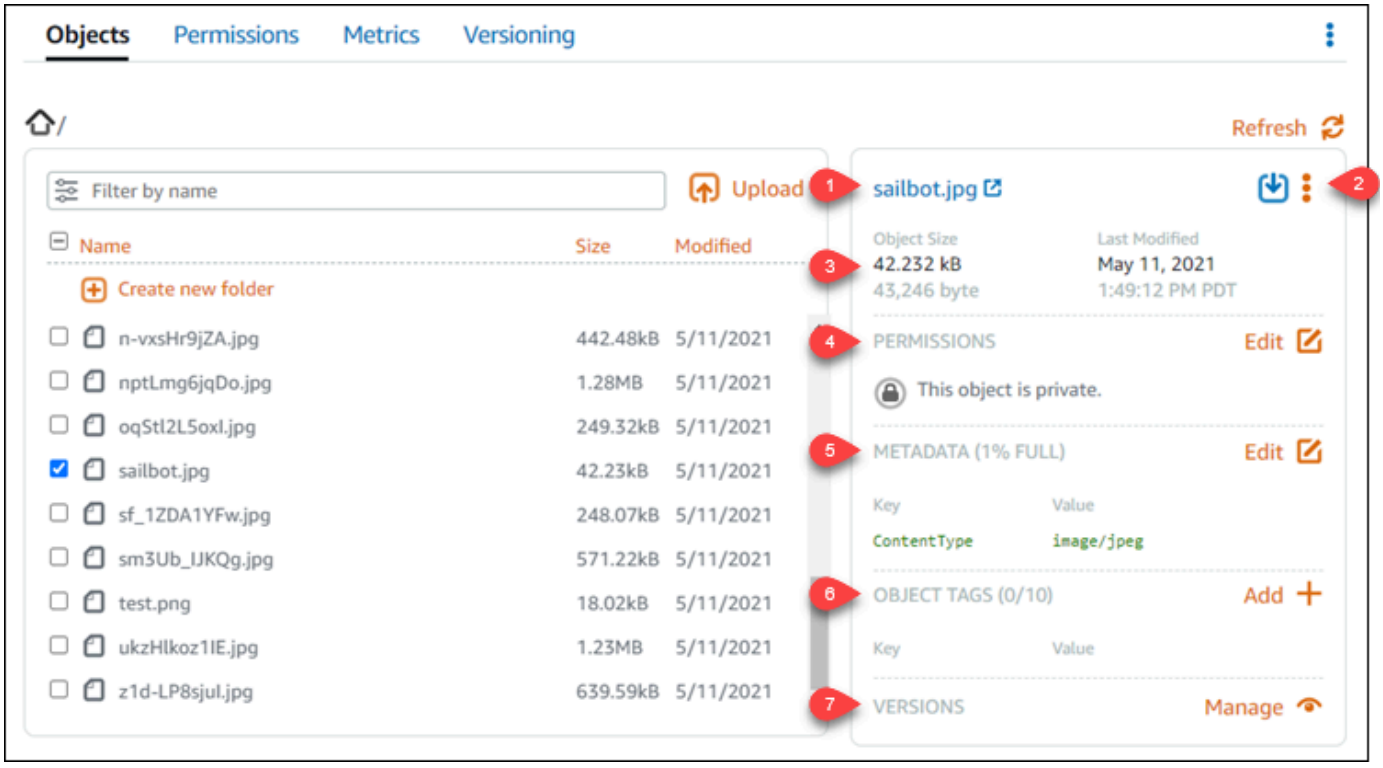
使用 Lightsail 控制台过滤对象

完成以下过程，使用 Lightsail 控制台查看存储在存储桶中的对象。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择所需存储桶的名称，以查看其中的对象。
4. 对象选项卡中的对象浏览器窗格将显示存储桶中存储的对象和文件夹。



5. 浏览到所需对象的位置，以查看其属性。
6. 在所需对象的旁边添加复选标记，以查看其属性。
7. 此页面右侧的 Object properties（对象属性）窗格将显示有关该对象的信息。



显示的信息包括：

1. 用于查看和下载对象的链接。
2. 用于复制或删除对象的操作菜单（⋮）。有关复制和删除对象的更多信息，请参阅在 Amazon Lightsail 中复制或移动存储桶中的对象和删除存储桶对象。
3. 对象大小和上次修改时间戳。
4. 单个对象的访问权限，可以是私有或公有（只读）。有关对象权限的更多信息，请参阅存储桶权限。
5. 对象的元数据。内容类型 (`ContentType`) 密钥是 Lightsail 对象存储服务目前唯一支持的元数据。
6. 对象键值标记。有关更多信息，请参阅为存储桶对象添加标签。
7. 用于管理对象的存储版本的选项。有关更多信息，请参阅启用和暂停存储桶中的对象版本控制。

> **Note**
>
> 当您选择多个对象时，Object properties（对象属性）窗格仅显示所选对象的总大小。

使用查看对象 AWS CLI

完成以下过程，以使用 AWS Command Line Interface （ AWS CLI ）列出存储桶中的对象。使用 `list-objects-v2` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》中的 list-objects-v2。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface

1. 打开命令提示符或终端窗口。
2. 输入以下命令之一。

   - 输入以下命令列出存储桶中的所有对象键。

     ```
     aws s3api list-objects-v2 --bucket BucketName --query "Contents[].{Key: Key,
      Size: Size}"
     ```

     在命令中，*BucketName*替换为要列出其所有对象的存储桶的名称。

   - 输入以下命令列出以特定对象键名称前缀开头的对象。

     ```
     aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --
     query "Contents[].{Key: Key, Size: Size}"
     ```

     在该命令中，将以下示例文本替换为自己的文本：

     - *BucketName*-您要列出其所有对象的存储桶的名称。
     - *ObjectKeyNamePrefix*-对象密钥名称前缀，用于将响应限制为以指定前缀开头的密钥。

     > **Note**
     >
     > 这些命令使用 `--query` 参数筛选对每个对象的键值和大小的 `list-objects-v2` 请求的响应。

   示例：

列出存储桶中的所有对象键

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --query "Contents[].{Key:
 Key, Size: Size}"
```

上面命令的结果应类似于下面的示例。

```
C:\>aws s3api list-objects-v2 --bucket DOC-EXAMPLE-BUCKET --query "Contents[].{Key: Key, Size: Size}"
[
    {
        "Key": "GiUJ02Yj_io.jpg",
        "Size": 828150
    },
    {
        "Key": "H90Af2TFqng.jpg",
        "Size": 784846
    },
    {
        "Key": "Hyu76loQLdk.jpg",
        "Size": 1086363
    },
    {
        "Key": "Nn1Yu2uCmwg.jpg",
        "Size": 6075006
    },
    {
        "Key": "Oaqk7qqNh_c.jpg",
        "Size": 3458557
    },
    {
        "Key": "PC_lbSSxCZE.jpg",
        "Size": 4239636
    },
    {
        "Key": "PDX_a_82obo.jpg"
```

列出以 `archived/` 对象键名称前缀开头的对象键

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --prefix archived/ --query
 "Contents[].{Key: Key, Size: Size}"
```

上面命令的结果应类似于下面的示例。

```
C:\>aws s3api list-objects-v2  --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query "Contents[].{Key: Key, Size: Size}"
[
    {
        "Key": "archived/",
        "Size": 0
    },
    {
        "Key": "archived/1_CMoFsPfso.jpg",
        "Size": 2561865
    },
    {
        "Key": "archived/3y1zF4hIPCg.jpg",
        "Size": 6404907
    },
    {
        "Key": "archived/5IHz5WhosQE.jpg",
        "Size": 2377975
    },
    {
        "Key": "archived/sailbot.jpg",
        "Size": 43246
    }
]
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 禁止公开访问亚马逊 Lightsail 中的存储桶
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限

5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象
9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

主题

- 在 Lightsail 存储桶之间复制和移动对象
- 通过删除对象来清除 Lightsail 存储桶的存储空间
- 从 Lightsail 存储桶下载对象
- 按名称前缀筛选 Lightsail 存储桶中的对象
- 在 Lightsail 中启用和暂停对象版本控制
- 在 Lightsail 存储桶中恢复以前的对象版本
- 在 Lightsail 存储桶中标记对象

在 Lightsail 存储桶之间复制和移动对象

您可以在 Amazon Lightsail 对象存储服务中复制已存储在存储桶中的对象。在本指南中，我们将向您展示如何使用 Lightsail 控制台和 AWS Command Line Interface ()AWS CLI复制对象。复制存储桶中的对象以创建对象的重复副本、重命名对象或在 Lightsail 位置之间移动对象（例如，将对象从一个位置移动 AWS 区域 到另一个位置，其中 Lightsail 可用）。只能使用 AWS APIs AWS SDKs、和 AWS Command Line Interface (AWS CLI) 跨位置复制对象。

有关存储桶的更多信息，请参阅对象存储。

复制对象的限制

您可以使用 Lightsail 控制台创建大小不超过 2 GB 的对象的副本。您可以使用 AWS Command Line Interface (AWS CLI)、和，通过单个复制对象操作来创建大小不超过 5 GB 的对象的副本 AWS SDKs。 AWS APIs要复制大小超过 5 GB 的对象，必须使用 AWS CLI AWS APIs、和 AWS SDKs的分段上传操作。有关更多信息，请参阅使用分段上传操作将文件上传到存储桶。

使用 Lightsail 控制台复制对象

完成以下过程，使用 Lightsail 控制台复制存储在存储桶中的对象。要移动存储桶中的对象，您应将其复制到新位置，然后删除原始对象。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择所需存储桶的名称，以复制其中的对象。
4. 使用对象选项卡中，使用对象浏览器窗格浏览到要复制的对象所在的位置。
5. 在要复制的对象旁边添加复选标记。

6. 在对象信息窗格中，选择操作 (:) 菜单，然后选择复制到。
7. 在选择目标窗格中，浏览到存储桶中要复制所选对象的位置。您还可以通过将文件夹名称输入到目标路径文本框中，来创建新路径。
8. 选择复制将对象复制到选定或指定的目的地。否则，选择否，取消。

   成功复制对象后，将显示复制完成消息。如果您是要移动对象，则应删除原始对象。有关更多信息，请参阅删除存储桶对象。

使用复制对象 AWS CLI

完成以下过程，使用 AWS Command Line Interface (AWS CLI) 复制存储桶中的对象。使用 `copy-object` 命令完成此操作。有关更多信息，请参阅《AWS CLI Command Reference》中的 copy-object。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令复制存储桶中的对象。

```
aws s3api copy-object --copy-source SourceBucketNameAndObjectKey --
key DestinationObjectKey --bucket DestinationBucketName --acl bucket-owner-full-
control
```

在该命令中，将以下示例文本替换为自己的文本：

- *SourceBucketNameAndObjectKey*-当前存在源对象的存储桶的名称，以及要复制的对象的完整对象密钥。例如，若要从存储桶 `amzn-s3-demo-bucket` 中复制对象 `images/sailbot.jpg`，请指定 `amzn-s3-demo-bucket/images/sailbot.jpg`。
- *DestinationObjectKey*-新对象副本的完整对象密钥。
- *DestinationBucket* - 目标桶的名称。

示例：

- 将存储桶中的对象复制到同一存储桶：

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/images/sailbot.jpg
 --key media/sailbot.jpg --bucket amzn-s3-demo-bucket --acl bucket-owner-full-
control
```

- 将对象从一个存储桶复制到另一个存储桶：

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/images/sailbot.jpg --
key images/sailbot.jpg --bucket amzn-s3-demo-bucket2 --acl bucket-owner-full-
control
```

您会看到类似于以下示例的结果：

```
C:\>aws s3api copy-object --copy-source DOC-EXAMPLE-BUCKET/images/sailbot.jpg --key images/archived/sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
    "ServerSideEncryption": "AES256",
    "CopyObjectResult": {
        "ETag": "\"694d34example91d92d64f342aa234c3\"",
        "LastModified": "2021-05-10T05:35:42+00:00"
    }
}
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 在 Amazon Lightsail 中封锁存储桶的公开访问权限

- 在 Amazon Lightsail 中配置存储桶访问权限
- 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
- 在 Amazon Lightsail 中为存储桶创建访问密钥
- 在 Amazon Lightsail 中为存储桶配置资源访问权限
- 在 Amazon Lightsail 中为存储桶配置跨账户访问权限

5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象
9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。

13.如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。

14.了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。

- 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
- 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶

15.如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

通过删除对象来清除 Lightsail 存储桶的存储空间

您可以在 Amazon Lightsail 对象存储服务中从存储桶中删除对象。要释放存储空间，请删除不再需要的对象。例如，如果您收集了日志文件，最好在不再需要这些文件时将其删除。

有关存储桶的更多信息，请参阅对象存储。

内容

- 从启用版本控制的存储桶中删除对象
- 使用 Lightsail 控制台删除对象
- 使用 Lightsail 控制台删除对象版本
- 使用删除单个对象或对象版本 AWS CLI
- 使用删除多个对象或对象版本 AWS CLI

从启用版本控制的存储桶中删除对象

如果您的存储桶已启用版本控制，则存储桶中可能存在同一对象的多个版本。您可以使用 Lightsail 控制台、 AWS CLI AWS APIs、或 AWS 软件开发工具包删除对象的任何版本。但是，您应考虑以下选项。

使用 Lightsail 控制台删除对象和对象版本

在 Lightsail 控制台的 “对象” 选项卡的 “对象” 浏览器窗格中删除对象的当前版本时，也会删除该对象的所有先前版本。要删除对象的特定版本，您必须从管理版本窗格中执行操作。如果您使用管理版本窗格删除对象的当前版本，则会将最新的先前版本还原为当前版本。有关更多信息，请参阅本指南后面的使用 Lightsail 控制台删除对象版本。

使用 Lightsail API 删除对象和对象版本，或 AWS CLI AWS SDKs

要删除单个对象及其所有存储的版本，请在删除请求中仅指定该对象的键。要删除对象的特定版本，请指定对象键以及版本 ID。有关更多信息，请参阅本指南后面的使用 AWS CLI删除单个对象或对象版本。

使用 Lightsail 控制台删除对象

完成以下过程，使用 Lightsail 控制台删除对象，包括其存储的先前版本。使用 Lightsail 控制台，您一次只能删除一个对象。使用 AWS CLI 可以同时删除多个对象。有关更多信息，请参阅本指南后面的使用 AWS CLI删除多个对象或对象版本。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择所需存储桶的名称，以删除其中的对象。
4. 使用对象选项卡中的对象浏览器窗格浏览到要删除的对象所在的位置。
5. 在要删除的对象旁边添加复选标记。
6. 在对象信息窗格中，选择操作 (:) 菜单，然后选择删除。
7. 在出现的确认窗格中，选择是，删除以确认您要永久删除对象。

   如果删除您所在的文件夹中的唯一对象，则也会删除该文件夹。发生这种情况是因为文件夹是对象键名称的一部分，当存储桶中没有其他对象共用相同的对象前缀时，删除该对象也会删除前面的文件夹。有关更多信息，请参阅对象存储桶的键名称。

使用 Lightsail 控制台删除对象版本

完成以下过程以删除存储的对象版本。这仅适用于启用版本控制的存储桶。有关更多信息，请参阅启用和暂停存储桶中的对象版本控制。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择所需存储桶的名称，以删除其中的对象。
4. 使用的对象浏览器窗格浏览到要删除的对象所在的位置。
5. 在要删除存储的先前版本的对象旁边添加复选标记。
6. 在对象信息窗格的版本部分中选择管理，然后选择“管理”。
7. 从显示的管理存储的对象版本窗格中，在要删除的对象版本旁边添加复选标记。

您也可以选择删除对象的当前版本。

8. 选择删除选定项以删除选定版本。

   如果删除：

   - 对象的当前版本 - 对象最新的先前版本将还原为当前版本。
   - 对象的唯一版本 - 将从存储桶中删除对象。如果删除的版本是当前文件夹中的唯一对象，则也会删除该文件夹。发生这种情况是因为文件夹是对象键名称的一部分，当存储桶中没有其他对象共用相同的对象键前缀时，删除该对象也会删除前面的文件夹。有关更多信息，请参阅启用和暂停存储桶中的对象版本控制。

使用删除单个对象或对象版本 AWS CLI

完成以下过程，使用 AWS Command Line Interface (AWS CLI) 删除存储桶中的单个对象或对象版本。使用 `delete-object` 命令完成此操作。有关更多信息，请参阅 AWS CLI Command Reference 中的 delete-object。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface

1. 打开命令提示符或终端窗口。
2. 输入以下命令删除存储桶中的对象或对象版本。

   删除对象：

   ```
   aws s3api delete-object --bucket BucketName --key ObjectKey
   ```

   删除对象版本：

   > **Note**
   >
   > 只有启用版本控制的存储桶才能删除对象版本。有关更多信息，请参阅启用和暂停存储桶中的对象版本控制。

```
aws s3api delete-object --bucket BucketName --key ObjectKey --version-id VersionID
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要从中删除对象的存储桶的名称。
- *ObjectKey*-要删除的对象的完整对象密钥。
- *VersionID*-要删除的对象版本的 ID。

示例：

删除对象：

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg
```

删除对象版本：

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --
version-id YF0YMBlUvexampleO07l2vJi9hRz4ujX
```

您会看到类似于以下示例的结果：

```
C:\Users\latino>aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET  --key  images/sailbot.jpg  --version-id YF0YMBlUvexampleO07l2vJi9hRz4ujX
{
    "VersionId": "YF0YMBexampleY7PO07l2vJi9hRz4ujX"
}
```

使用 AWS CLI删除多个对象或对象版本

完成以下过程，以使用 AWS Command Line Interface （AWS CLI）删除存储桶中的多个对象。使用 `delete-objects` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》中的 “删除对象”。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface

1. 打开命令提示符或终端窗口。
2. 输入以下命令删除存储桶中的多个对象或多个对象版本。

```
aws s3api delete-objects --bucket BucketName --delete file://LocalDirectory
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要从中删除多个对象或多个对象版本的存储桶的名称。
- *LocalDirectory*-计算机上指定要删除的对象或版本的.json 文档的目录路径。可使用的 .json 文档格式如下。

  要删除对象，请在.json 文件中输入以下文本，然后*ObjectKey*用要删除的对象的对象密钥替换。

```
{
  "Objects": [
    {
      "Key": "ObjectKey1"
    },
    {
      "Key": "ObjectKey2"
    }
  ],
  "Quiet": false
}
```

  要删除对象版本，请在 .json 文件中输入以下文本。将*ObjectKey*和*VersionID*替换为要删除 IDs 的对象密钥和对象版本。

> **Note**
>
> 只有启用版本控制的存储桶才能删除对象版本。有关更多信息，请参阅启用和暂停存储桶中的对象版本控制。

```
{
  "Objects": [
    {
      "Key": "ObjectKey1",
```

```
      "VersionId": "VersionID1"
    },
    {
      "Key": "ObjectKey2",
      "VersionId": "VersionID2"
    }
  ],
  "Quiet": false
}
```

示例：

- 在 Linux 或 Unix 计算机上：

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://home/user/Documents/delete-objects.json
```

- 在 Windows 计算机上：

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://C:\Users\user\Documents\delete-objects.json
```

您会看到类似于以下示例的结果：

```
C:\>aws s3api delete-objects --bucket DOC-EXAMPLE-BUCKET  --delete file://C:\Users\user\Documents\delete-objects.json
{
    "Deleted": [
        {
            "Key": "images/sailbot.jpg",
            "VersionId": "26sqexampleztRiT6TsGhMMz0FxQAEw."
        },
        {
            "Key": "images/sailbot.jpg",
            "VersionId": "QwDrexampleDJxJtZC1CrExbpNlEC5O4"
        }
    ]
}
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。

2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 禁止公开访问亚马逊 Lightsail 中的存储桶
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象

- 在 Amazon Lightsail 中筛选存储桶中的对象
- 在 Amazon Lightsail 中标记存储桶中的对象
- 在 Amazon Lightsail 中删除存储桶中的对象

9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

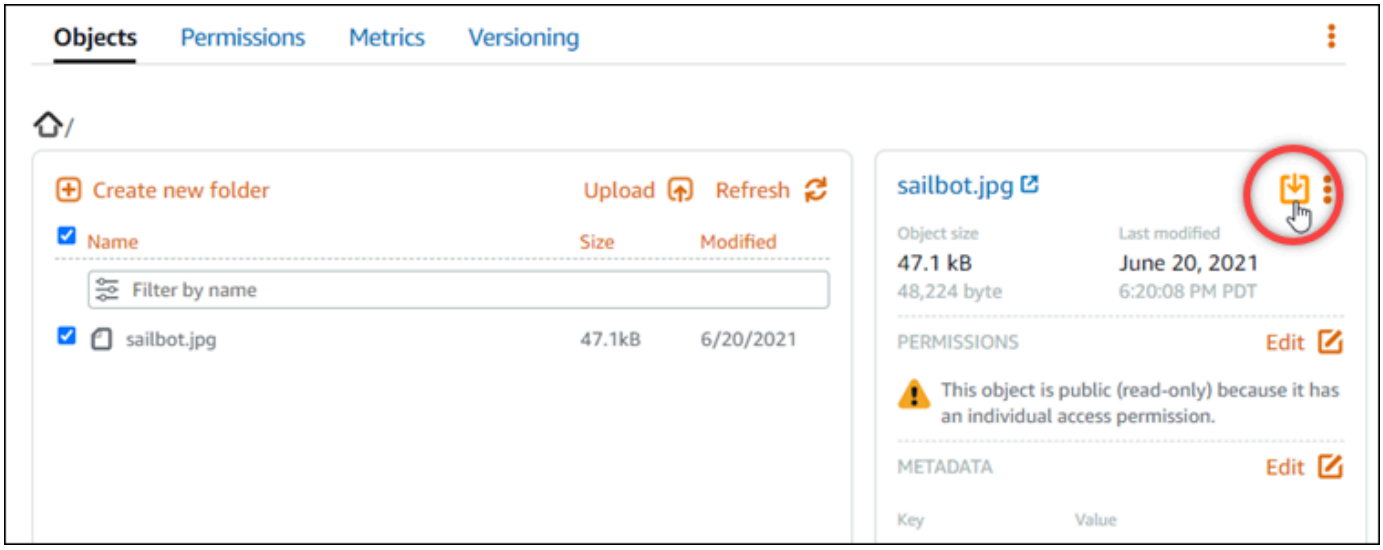
从 Lightsail 存储桶下载对象

您可以从 Amazon Lightsail 对象存储服务中您有权访问的存储桶或公有（只读）的存储桶下载对象。你可以使用 Lightsail 控制台一次下载一个对象。要在一个请求中下载多个对象，请使用 AWS Command Line Interface (AWS CLI) AWS SDKs、或 REST API。在本指南中，我们将向您展示如何使用 Lightsail 控制台下载对象，以及。 AWS CLI有关存储桶的更多信息，请参阅对象存储。

使用 Lightsail 控制台下载对象

完成以下过程，使用 Lightsail 控制台从存储桶下载对象。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要从中下载文件的存储桶的名称。
4. 使用对象选项卡中的对象浏览器窗格浏览到要下载的对象所在的位置。
5. 在要下载的对象旁边添加复选标记。
6. 在对象信息窗格中，选择下载图标。



根据浏览器的配置，您选择的文件将显示在页面上，或者下载到您的计算机中。如果文件显示在页面上，您可以右键单击该文件并选择另存为将其保存到计算机中。

使用下载对象 AWS CLI

完成以下过程，以使用 AWS Command Line Interface（AWS CLI）从存储桶中下载对象。使用 `get-object` 命令完成此操作。有关更多信息，请参阅 AWS CLI Command Reference 中的 get-object。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface

1. 打开命令提示符或终端窗口。
2. 输入以下命令从存储桶下载对象。

```
aws s3api get-object --bucket BucketName --key ObjectKey LocalFilePath
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要从中下载对象的存储桶的名称。
- *ObjectKey*-要下载的对象的完整对象密钥。
- *LocalFilePath*-计算机上要保存已下载文件的完整文件路径。

示例：

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg C:\Users
\user\Pictures\sailbot.jpg
```

您会看到类似于以下示例的结果：

```
C:\>aws s3api get-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg C:\Users\user\Pictures\sailbot.jpg
{
    "AcceptRanges": "bytes",
    "LastModified": "2021-05-10T05:09:31+00:00",
    "ContentLength": 48224,
    "ETag": "\"694d34example91d92d64f342aa234c3\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 禁止公开访问亚马逊 Lightsail 中的存储桶
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限

- 在 Amazon Lightsail 中为存储桶配置跨账户访问权限

5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象
9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶

- 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶

15如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

按名称前缀筛选 Lightsail 存储桶中的对象

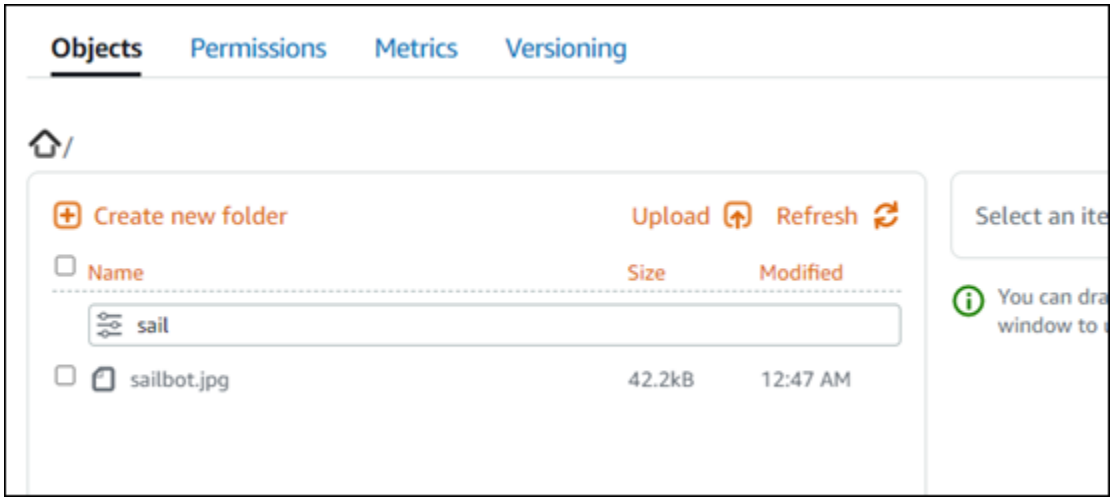
您可以使用筛选功能在 Amazon Lightsail 对象存储服务中查找存储桶中的对象。在本指南中，我们将向您展示如何使用 Lightsail 控制台和 AWS Command Line Interface ()AWS CLI过滤对象。有关存储桶的更多信息，请参阅对象存储。

使用 Lightsail 控制台过滤对象

完成以下过程，使用 Lightsail 控制台筛选存储桶中的对象。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择所需存储桶的名称，以筛选其中的对象。
4. 在对象选项卡的按名称筛选文本框中，输入对象前缀。

   将筛选当前正在查看的文件夹中的对象列表，以匹配您输入的文本。以下示例显示，如果输入 `sail`，则会筛选页面上的对象列表，仅显示以 `sail` 开头的对象。



   要筛选其他文件夹中的对象列表，请导航到该文件夹。然后，在按名称筛选文本框中输入对象前缀。

使用过滤对象 AWS CLI

完成以下过程，以使用 AWS Command Line Interface （ AWS CLI ）筛选存储桶中的对象。使用 `list-objects-v2` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》中的 list-objects-v2。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface

1. 打开命令提示符或终端窗口。
2. 输入以下命令列出以特定对象键名称前缀开头的对象。

```
aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --query
 "Contents[].{Key: Key, Size: Size}"
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要列出其所有对象的存储桶的名称。
- *ObjectKeyNamePrefix*-对象密钥名称前缀，用于将响应限制为以指定前缀开头的密钥。

> **Note**
>
> 此命令使用 `--query` 参数筛选对每个对象的键值和大小的 `list-objects-v2` 请求的响应。

示例：

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --prefix archived/ --query
 "Contents[].{Key: Key, Size: Size}"
```

您应看到类似于以下示例的结果。

```
C:\>aws s3api list-objects-v2  --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query "Contents[].{Key: Key, Size: Size}"
[
    {
        "Key": "archived/",
        "Size": 0
    },
    {
        "Key": "archived/1_CMoFsPfso.jpg",
        "Size": 2561865
    },
    {
        "Key": "archived/3y1zF4hIPCg.jpg",
        "Size": 6404907
    },
    {
        "Key": "archived/5IHz5WhosQE.jpg",
        "Size": 2377975
    },
    {
        "Key": "archived/sailbot.jpg",
        "Size": 43246
    }
]
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 在 Amazon Lightsail 中封锁存储桶的公开访问权限
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限

5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象
9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

在 Lightsail 中启用和暂停对象版本控制

Amazon Lightsail 对象存储服务中的版本控制是一种将对象的多个变体保存在同一个存储桶中的方法。对于存储桶中存储的每个对象，您可以使用版本控制功能来保留、检索和还原它们的各个版本。使用版本控制能够更加轻松地从用户意外操作和应用程序故障中恢复数据。当您为存储分区启用版本控制时，如果 Lightsail 对象存储服务同时收到同一对象的多个写入请求，则它会存储所有这些对象。默认情况下，Lightsail 对象存储服务中的存储分区处于禁用状态，因此您必须明确启用它。有关存储桶的更多信息，请参阅对象存储。

> **Important**
>
> 当您在配置了个别对象可设为公有（只读）访问权限的存储桶上启用或暂停版本控制后，权限将重置为所有对象都是私有的。如果您希望可以继续选择将个别对象设为公有，则必须手动将存储桶访问权限更改回个别对象可设为公有（只读）。有关更多信息，请参阅配置存储桶访问权限。

禁用、启用和暂停版本控制的存储桶

在 Lightsail 控制台中，存储桶版本控制可能处于以下三种状态之一：

- 已禁用（`NeverEnabled`在 API 中和 SDKs）
- 已启用（`Enabled`在 API 中和 SDKs）
- 已暂停（`Suspended`在 API 中和 SDKs）

在存储桶中启用版本控制后，它将无法返回到禁用状态。但是，您可以暂停版本控制。您可以在存储桶级别启用和暂停版本控制。

版本控制状态将应用到该存储桶中的所有 (不是某些) 对象。当您在存储桶中启用版本控制功能时，所有新对象都将受版本控制，并为其指定唯一的版本 ID。启用版本控制时已存在于存储桶中的对象将始终向前增加版本。如果在以后的请求中进行了修改，将为其提供唯一的版本 ID。

版本 IDs

如果您为存储分区启用版本控制，Lightsail 对象存储服务会自动为正在存储的对象生成唯一的版本 ID。例如，在一个存储桶中，您可以有两个密钥相同但版本不同的对象 IDs，例如`photo.gif`（版本 111111）和`photo.gif`（版本 121212）。



版本 IDs 无法编辑。它们是 Unicode、UTF-8 编码、URL 就绪、不透明的字符串，长度不超过 1,024 字节。以下版本 ID 的示例：

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

使用 Lightsail 控制台启用或暂停对象版本控制

完成以下过程，使用 Lightsail 控制台启用或暂停对象版本控制。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要启用或暂停版本控制的存储桶的名称。
4. 选择 Versioning（版本控制）选项卡。
5. 根据存储桶的当前版本控制状态，完成以下操作之一：
   - 如果版本控制当前已暂停或尚未启用，请在页面的对象版本控制部分下方启用版本控制。
   - 如果版本控制当前已启用，请在页面的对象版本控制部分下方暂停版本控制。

使用启用或暂停对象版本控制 AWS CLI

完成以下过程以使用 AWS Command Line Interface（AWS CLI）启用或暂停对象版本控制。使用 `update-bucket` 命令完成此操作。有关更多信息，请参阅《AWS CLI Command Reference》中的 update-bucket。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以启用或暂停对象版本控制。

```
aws lightsail update-bucket --bucket-name BucketName --versioning VersioningState
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要为其启用对象版本控制的存储桶的名称。
- *VersioningState* - 下列值之一：
  - Enabled- 启用对象版本控制。
  - Suspended- 暂停对象版本控制（如果之前已启用）。

示例：

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket --versioning Enabled
```

您会看到类似于以下示例的结果：

```
C:\>aws lightsail update-bucket --bucket-name DOC-EXAMPLE-BUCKET --versioning Enabled
{
    "bucket": {
        "resourceType": "Bucket",
        "accessRules": {
            "getObject": "private",
            "allowPublicOverrides": false
        },
        "arn": "arn:aws:lightsail:us-west-2:1example7491:Bucket/f067383e-ee41-4485-b934-example2e2fd",
        "bundleId": "small_1_0",
        "createdAt": "2021-06-29T08:12:39.163000-07:00",
        "url": "https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com",
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "name": "DOC-EXAMPLE-BUCKET",
        "supportCode": "621291663362/DOC-EXAMPLE-BUCKET/small_1_0",
        "tags": [],
        "objectVersioning": "Enabled",
        "ableToUpdateBundle": true
    },
    "operations": [
        {
            "id": "0d53d290-f4b2-43f0-89d2-example43448",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-29T08:29:56.241000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "6example3362/DOC-EXAMPLE-BUCKET/small_1_0",
            "operationType": "UpdateBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-29T08:29:56.241000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。

4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 在 Amazon Lightsail 中封锁存储桶的公开访问权限
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象

9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

在 Lightsail 存储桶中恢复以前的对象版本

如果您在 Amazon Lightsail 对象存储服务中的存储桶支持版本控制，则可以恢复对象的先前版本。还原先前版本的对象，从意外用户操作或应用程序故障中恢复。

您可以使用 Lightsail 控制台恢复对象的先前版本。您也可以使用 AWS Command Line Interface (AWS CLI) 并 AWS SDKs 恢复对象的先前版本。为此，请将对象的特定版本复制到同一存储桶中，并使用相同的对象键名称。这将使用先前的版本替换当前版本，使先前的版本成为当前版本。有关版本控制的更多信息，请参阅启用和暂停存储桶中的对象版本控制。有关存储桶的更多信息，请参阅对象存储。

使用 Lightsail 控制台恢复对象的先前版本

完成以下过程，使用 Lightsail 控制台恢复对象的先前版本。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要为其还原先前版本对象的存储桶的名称。
4. 使用对象选项卡中的对象浏览器窗格浏览到对象的位置。
5. 在要还原先前版本的对象旁边添加复选标记。
6. 在对象信息窗格的版本部分下方选择管理。
7. 选择 Restore (还原)。

8. 从显示的存储版本窗格，在还原对象中选择要还原的对象的版本。
9. 选择继续。
10. 在显示的确认提示中，选择是，还原以还原对象版本。否则，选择否，取消。

使用恢复对象的先前版本 AWS CLI

完成以下过程以使用 AWS Command Line Interface （ AWS CLI ）还原先前版本的对象。使用 `copy-object` 命令完成此操作。您必须使用相同的对象键，将先前版本的对象复制到同一存储桶中。有关更多信息，请参阅《AWS CLI Command Reference》中的 copy-object。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Amazon Lightsail 配合使用。 AWS Command Line Interface

1. 打开命令提示符或终端窗口。
2. 输入以下命令以还原先前版本的对象。

```
aws s3api copy-object --copy-source "BucketName/ObjectKey?versionId=VersionId" --
key ObjectKey --bucket BucketName
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要为其恢复对象的先前版本的存储桶的名称。您必须为 `--copy-source` 和 `--bucket` 参数指定相同的存储桶名称。
- *ObjectKey*-要恢复的对象的名称。您必须为 `--copy-source` 和 `--key` 参数指定相同的对象键。
- *VersionId*-要恢复到当前版本的先前对象版本的 ID。使用`list-object-versions`命令获取存储桶中对象 IDs 的版本列表。

示例：

```
aws s3api copy-object --copy-source "amzn-s3-demo-bucket/sailbot.jpg?
versionId=GQWEexample87Mdl8Q_DKdVTiVMi_VyU" -key sailbot.jpg --bucket amzn-s3-demo-
bucket
```

您会看到类似于以下示例的结果：

```
C:\>aws s3api copy-object --copy-source "DOC-EXAMPLE-BUCKET/sailbot.jpg?versionId=GQWEexample87Mdl8Q_DKdVTiVMi_VyU"
--key sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
    "CopySourceVersionId": "GQWEcouyrfexampleQ_DKdVTiVMi_VyU",
    "VersionId": "hjL8anKzI1xcXYyexampleDvvqMXSLoi",
    "ServerSideEncryption": "AES256",
    "CopyObjectResult": {
        "ETag": "\"dc5afd388fb3example20cda3fe41c54\"",
        "LastModified": "2021-05-16T06:45:35+00:00"
    }
}
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 在 Amazon Lightsail 中封锁存储桶的公开访问权限
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。

   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录

- Amazon Lightsail 对象存储服务中存储桶的访问日志格式
- 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
- 使用 Amazon Lightsail 中存储段的访问日志来识别请求

6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中为存储桶中的对象添加标签
   - 在 Amazon Lightsail 中删除存储桶中的对象
9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

在 Lightsail 存储桶中标记对象

标记存储桶中的对象，按用途、拥有者、环境或其他标准对它们进行分类。当您上传对象时或上传对象后，可以向对象添加标签。有关存储桶的更多信息，请参阅对象存储。

使用 Lightsail 控制台为对象添加和删除标签

完成以下过程，使用 Lightsail 控制台为存储桶中的对象添加或删除标签。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择所需存储桶的名称，以标记其中的对象。
4. 使用对象选项卡中的对象浏览器窗格浏览到对象的位置。
5. 在所需对象的旁边添加复选标记，以添加或删除标签。
6. 在对象信息窗格中，选择对象标签部分下的下列选项之一：

   - 添加或编辑（如已添加标签）。在键文本框中输入一个键，然后在值文本框中输入一个值。然后选择保存以添加标签。否则，选择取消。
   - 进行编辑，然后选择要删除的键值标签旁边的 X。选择保存以完成标签的删除，或选择取消而不删除。

使用 AWS CLI添加和删除对象的标签

完成以下过程，使用 AWS Command Line Interface (AWS CLI) 向对象添加标签或从对象中删除标签。使用 `put-object-tagging` 和 `delete-object-tagging` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》delete-object-tagging中的 “put-object-tagging和”。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入下列命令之一：

   - 向对象添加标签

```
aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
 "{\"TagSet\":[{ \"Key\": \"KeyTag\", \"Value\": \"ValueTag\" }]}"
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-包含您要标记的对象的存储桶的名称。
- *ObjectKey*-要标记的对象的完整对象密钥。
- *KeyTag*-标签的密钥值。
- *ValueTag*-您的标签的价值。

- 向对象添加标签

```
aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
 "{\"TagSet\":[{ \"Key\": \"KeyTag1\", \"Value\": \"ValueTag1\" }, { \"Key\":
 \"KeyTag2\", \"Value\": \"ValueTag2\" }]}"
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-包含您要标记的对象的存储桶的名称。
- *ObjectKey*-要标记的对象的完整对象密钥。
- *KeyTag1*-您的第一个标签的键值。
- *ValueTag1*-您的第一个标签的值。
- *KeyTag2*-第二个标签的密钥值。
- *ValueTag2*-你的第二个标签的值。

- 删除对象的标签：

```
aws s3api delete-object-tagging --bucket BucketName --key ObjectKey
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-包含您要删除其所有标签的对象的存储桶的名称。
- *ObjectKey*-要标记的对象的完整对象密钥。

示例：

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key nptLmg6jqDo.jpg --
tagging "{\"TagSet\":[{ \"Key\": \"Importance\", \"Value\": \"High\" }]}"
```

您会看到类似于以下示例的结果：

```
C:\>aws s3api put-object-tagging --bucket DOC-EXAMPLE-BUCKET  --key nptLmg6jqDo.jpg
--tagging "{\"TagSet\":[{ \"Key\": \"Importance\", \"Value\": \"High\" }]}"
{
    "VersionId": "9nL2d41NuZdhdk4HS3kZIwOxJeS1kCkm"
}
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 在 Amazon Lightsail 中封锁存储桶的公开访问权限
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。

   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录

- 使用 Amazon Lightsail 中存储段的访问日志来识别请求

6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象
   - 在 Amazon Lightsail 中筛选存储桶中的对象
   - 在 Amazon Lightsail 中标记存储桶中的对象
   - 在 Amazon Lightsail 中删除存储桶中的对象
9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

控制实例对 Lightsail 存储桶的访问权限

将 Amazon Lightsail 实例附加到 Lightsail 存储桶，使其能够以编程方式访问存储桶及其对象。将实例附加到存储桶时，您无需像管理访问密钥那样管理凭证。附加的实例和存储桶必须位于同一 AWS 区域中。您无法将实例附加到位于其他区域的存储桶。

如果您在实例上配置软件或插件，以便将文件直接上传到存储桶，则非常适合使用资源访问权限。例如，如果您想将 WordPress 实例配置为在存储桶上存储媒体文件。有关更多信息，请参阅教程：将存储桶连接到您的 WordPress 实例。

有关权限选项的更多信息，请参阅存储桶权限。有关安全最佳实践的更多信息，请参阅对象存储的安全最佳实践。有关存储桶的更多信息，请参阅对象存储。

配置存储桶的资源访问权限

完成以下过程以配置存储桶的资源访问权限。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择您要为其配置资源访问权限的存储桶的名称。
4. 选择 Permissions (权限) 选项卡。

   页面的资源访问权限部分显示当前附加到存储桶的实例（如果有）。
5. 选择附加实例以将实例附加到存储桶。
6. 在选择实例下拉菜单中，选择您要附加到存储桶的实例。

   > **Note**
   >
   > 您只能附加正在运行或处于已停止状态的实例。此外，您只能连接与存储桶 AWS 区域 相同的实例。
7. 选择附加以附加实例。否则，选择取消。

   附加后实例具有存储桶及其对象的完全访问权限。您可以在实例上配置软件或插件，以便以编程方式上传和访问存储桶上的文件。例如，如果您想将 WordPress 实例配置为在存储桶上存储媒体文件。有关更多信息，请参阅教程：将存储桶连接到您的 WordPress 实例。

根据使用量波动调整 Lightsail 存储空间计划

在 Amazon Lightsail 对象存储服务中，存储桶的存储计划会指定其每月成本、存储空间配额和数据传输配额。在一个月度 AWS 账单周期内，您只能更新一次存储桶的存储套餐。当您更改存储桶的存储计划时，将重置存储空间和网络传输配额。但是，您因使用之前的存储计划而可能产生的超额存储空间和数据传输费用不包括在内。

如果存储桶始终超出其存储空间或数据传输配额，或者存储桶的使用量始终处于其存储空间或数据传输配额的较低范畴，请更新存储桶的存储计划。由于存储桶可能会遇到不可预测的使用量波动，我们强烈建议您仅将更新存储桶的存储计划作为一项长期策略，而不将其作为每月削减成本的短期措施。选择的存储计划应在未来很长一段时间内为存储桶提供充足的存储空间和数据传输配额。

有关存储桶的更多信息，请参阅对象存储。

使用 Lightsail 控制台更改存储分区的存储计划

完成以下过程，使用 Lightsail 控制台更改存储分区的存储计划。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要为其更新计划的存储桶的名称。
4. 在存储桶管理页面中选择 Metrics (指标) 选项卡。
5. 选择创建存储计划。
6. 在显示的确认提示中，选择是，更改以继续更改存储桶的存储计划。否则，选择否，取消。
7. 选择要使用的计划，然后选择选择计划。
8. 在显示的确认提示中，选择是，应用以将更改应用到您的存储桶，或者选择否，返回而不应用。

使用更改存储桶的存储计划 AWS CLI

完成以下过程，使用 AWS Command Line Interface (AWS CLI) 更改存储桶的套餐。使用 `update-bucket-bundle` 命令完成此操作。请注意，存储桶的存储计划在 API 中称为存储桶捆绑。有关更多信息，请参阅 AWS CLI 命令参考 中的 update-bucket-bundle。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令，以更改存储桶的计划。

```
aws lightsail update-bucket-bundle --bucket-name BucketName --bundle-id BundleID
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要为其更新存储计划的存储桶的名称。
- *BundleID*-您要应用于存储桶的新存储桶捆绑包的 ID。使用get-bucket-bundles命令查看可用存储桶捆绑包及其 IDs列表。有关更多信息，请参阅 AWS CLI 命令参考 中的 get-bucket-bundles。

示例：

```
aws lightsail update-bucket-bundle --bucket-name amzn-s3-demo-bucket --bundle-
id medium_1_0
```

您会看到类似于以下示例的结果：

```
C:\>aws lightsail update-bucket-bundle --bucket-name DOC-EXAMPLE-BUCKET --bundle-id medium_1_0

{
    "operations": [
        {
            "id": "8example-8176-48bd-b1da-exampleb8404",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-30T12:05:57.362000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "62example362/DOC-EXAMPLE-BUCKET/medium_1_0",
            "operationType": "UpdateBucketBundle",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-30T12:05:57.362000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

管理 Lightsail 存储分区访问权限以增强安全性

使用存储桶访问权限控制存储桶中对象的公有（未经身份验证的）只读访问权限。您可以将存储桶设为私有或公有（只读）。您还可以将存储桶设为私有，同时还可以选择将个别对象设为公有（只读）。

> **Important**
>
> 当您将存储桶设为公有（只读）时，您将允许互联网上的任何人都可以通过存储桶的 URL（例如，`https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg`）读取存储桶中的所有对象。如果您不希望互联网上的任何人都能访问您的对象，则不要将存储桶设为公有（只读）。

有关权限选项的更多信息，请参阅存储桶权限。有关安全最佳实践的更多信息，请参阅对象存储的安全最佳实践。有关存储桶的更多信息，请参阅对象存储。

> **Important**
>
> 在允许或拒绝公开访问时，Lightsail 对象存储资源会同时考虑 Lightsail 存储桶访问权限和 Amazon S3 账户级别的封禁公共访问配置。有关更多信息，请参阅屏蔽对存储桶的公共访问权限。

配置存储桶访问权限

完成以下过程以配置存储桶的访问权限。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要为其配置访问权限的存储桶的名称。
4. 选择 Permissions (权限) 选项卡。

   页面的存储桶访问权限部分显示当前为存储桶配置的访问权限。
5. 选择更改权限以更改存储桶访问权限。
6. 请选择以下选项之一：

   - 所有对象都是私有的 — 只有您或您授予访问权限的人才可以读取存储桶中的所有对象。
   - 个别对象可设为公有（只读）— 存储桶中的对象只能由您或您授予访问权限的人读取，除非您将个别对象设为公有（只读）。有关个别对象访问权限的更多信息，请参阅在存储桶中配置个别对象的访问权限。

     建议您仅在有特别需求时才选择个别对象可设为公有（只读）选项，比如仅将存储桶中的某些对象设为公有，同时保持所有其他对象的私有状态。例如，某些 WordPress 插件要求您的存储桶允许公开单个对象。有关更多信息，请参阅教程：将存储桶连接到您的 WordPress 实例和教程：使用带有内容分发网络分发的存储桶。
   - 所有对象都是公有的（只读）— 互联网上的任何人都可以读取存储桶中的所有对象。

     > **Important**
     >
     > 当您将存储桶设为公有（只读）时，您将允许互联网上的任何人都可以通过存储桶的 URL（例如，`https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg`）读取存储桶中的所有对象。如果您不希望互联网上的任何人都能访问您的对象，则不要将存储桶设为公有（只读）。
7. 选择保存以保存更改。否则，选择取消。

   根据您更改的存储桶访问权限，将执行以下更改：

   - 所有对象都是私有的 - 存储桶中的所有对象都将变成私有状态，即使它们之前配置了公有（只读）的个别对象访问权限。

- 个别对象可设为公有（只读）- 之前配置的对象（公有（只读）的个别对象访问权限）将为公有状态。现在，您可以为对象配置个别对象访问权限。
- 所有对象都是公有的（只读）- 存储桶中的所有对象都将变成公有（只读）状态，即使它们之前配置了私有的个别对象访问权限。

  有关个别对象访问权限的更多信息，请参阅在存储桶中配置个别对象的访问权限。

为跨账户授予对 Lightsail 存储桶的只读访问权限 AWS

使用跨账户存取为其他 AWS 账户及其用户授予存储桶中所有对象的只读访问权限。如果您想与其他账户共享对象，则跨 AWS 账户访问是理想的选择。当您向另一个账户授予跨 AWS 账户访问权限时，该账户中的用户通过存储桶和对象（例如`https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg`）的 URL 对存储桶中的对象具有只读访问权限。您最多可以向 10 个 AWS 账户授予存储桶访问权限。

有关权限选项的更多信息，请参阅存储桶权限。有关安全最佳实践的更多信息，请参阅对象存储的安全最佳实践。有关存储桶的更多信息，请参阅对象存储。

配置存储桶的跨账户存取

完成以下过程以配置存储桶的跨账户存取。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要为其配置跨账户存取的存储桶的名称。
4. 选择 Permissions (权限) 选项卡。

   页面的跨账户访问部分显示当前配置为访问存储桶 IDs 的 AWS 账户（如果有）。
5. 选择添加跨账户访问权限以授予其他 AWS 账户对存储桶的访问权限。
6. 在 AWS 账户 ID 文本框中输入您要授予访问权限的账户的 ID。
7. 选择保存以授予访问权限。否则，选择取消。

   您添加的 AWS 账户 ID 列在页面的跨账户访问部分。要删除 AWS 账户的跨账户存取，请在要删除的 AWS 账户 ID 的旁边选择删除（垃圾桶）图标。

向公众授予对 Amazon Lightsail 中各个存储桶对象的访问权限

使用个别对象访问权限控制存储桶中个别对象的公有（未经身份验证的）只读访问权限。您可以将存储桶中的个别对象设为私有或公有（只读）。

> **Important**
>
> 仅当存储桶的访问权限设置为个别对象可设为公有（只读）时，才可以配置个别对象访问权限。有关存储桶权限选项的更多信息，请参阅存储桶权限。有关存储桶的更多信息，请参阅对象存储。

建议您仅在有特别需求时才配置个别对象访问权限，比如仅将存储桶中的某些对象设为公有，同时保持所有其他对象的私有状态。例如，某些 WordPress 插件要求您的存储桶允许公开单个对象。有关更多信息，请参阅教程：将存储桶连接到您的 WordPress 实例和教程：使用带有内容分发网络分发的存储桶。

有关权限选项的更多信息，请参阅存储桶权限。有关安全最佳实践的更多信息，请参阅对象存储的安全最佳实践。有关存储桶的更多信息，请参阅对象存储。

配置个别对象访问权限

完成以下过程以配置存储桶中个别对象的访问权限。有关授予用户在 Lightsail 中管理存储桶的权限的 IAM 策略示例，请参阅用于管理存储分区的 IAM 策略。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要为其配置个别对象访问权限的存储桶的名称。
4. 选择对象选项卡。
5. 在要为其配置访问权限的对象旁边添加复选标记。

   对象信息窗格显示对象的当前访问权限。
6. 在对象信息窗格的权限部分选择编辑，以更改对象的访问权限。

> **Note**
>
> 如果编辑选项不可用，则存储桶的访问权限不允许配置个别对象访问权限。要配置个别对象访问权限，存储桶访问权限必须设置为个别对象可设为公有（只读）。有关更多信息，请参阅配置存储桶访问权限。

7. 在选择权限下拉菜单中，选择以下选项之一：

   - 私有 — 只有您或您授予访问权限的人才可以读取对象。
   - 公有（只读）— 世界上任何人都可以读取对象。

8. 选择保存以保存更改。否则，选择取消。

   存储桶的存储桶访问权限设置对个别对象访问权限具有以下影响：

   - 如果您将存储桶访问权限更改为所有对象都是私有的，存储桶中的所有对象都将变成私有状态，即使它们之前配置了公有（只读）的个别对象访问权限。但是，会保留已配置的个别对象访问权限。例如，如果您将存储桶访问权限更改回个别对象可设为公有（只读），则可再次公开读取所有具有公有（只读）个别访问权限的对象。
   - 如果您将存储桶访问权限更改为所有对象都是公有的（只读），存储桶中的所有对象都将变成公有（只读）状态，即使它们之前配置了私有的个别对象访问权限。

     有关存储桶访问权限的更多信息，请参阅配置存储桶访问权限。

通过分段上传将文件上传到 Lightsail 存储桶

通过分段上传，可将单个文件作为一组分段上传到存储桶。每个分段都是文件数据的连续部分。您可以独立上传以及按任意顺序上传这些文件分段。如果任意分段传输失败，可以重新传输该分段且不会影响其它分段。文件的所有部分都上传完毕后，Amazon S3 会汇编这些部分，然后在 Amazon Lightsail 的存储桶中创建对象。一般而言，如果您的对象大小达到了 100 MB，您应该考虑使用分段上传，而不是在单个操作中上传对象。有关存储桶的更多信息，请参阅对象存储。

使用分段上传可提供以下优势：

- 提高吞吐量 – 您可以并行上传分段以提高吞吐量。
- 从任何网络问题中快速恢复 - 较小的分段大小可以将由于网络错误而需重启失败的上传所产生的影响降至最低。

- 逐步上传 — 您可以在一段时间内逐步上传文件分段。启动分段上传后，您可以在 24 小时内完成分段上传。
- 在您知道最终文件大小前开始上传 – 您可以在创建对象时将其上传。

我们建议您按以下方式使用分段上传：

- 如果您在稳定的高带宽网络上传大文件，通过并行上传文件分段进行多线程上传，分段上传可以充分利用您的可用带宽。
- 如果您在断点网络中上传对象，请使用分段上传以提高应对网络错误的复原能力，从而避免重新上传。在使用分段上传时，您只需重新尝试上传中断的分段即可。无需重头开始或重新上传整个文件。

内容

- 分段上传流程
- 并发分段上传操作
- 分段上传保留
- Amazon Simple Storage Service 分段上传限制
- 拆分要上传的文件
- 使用启动分段上传 AWS CLI
- 使用上传分段 AWS CLI
- 使用列出分段上传的各个部分 AWS CLI
- 创建分段上传 .json 文件
- 使用完成分段上传 AWS CLI
- 使用列出存储桶的分段上传 AWS CLI
- 使用 AWS CLI停止分段上传

分段上传流程

分段上传是一个三步过程，它使用 Amazon S3 操作将文件上传到 Lightsail 中的存储桶：

1. 您可以使用CreateMultipartUpload操作启动分段上传。
2. 您可以使用UploadPart操作上传文件片段。
3. 您可以使用CompleteMultipartUpload操作完成分段上传。

> **Note**
>
> 在启动分段上传后，您可以使用AbortMultipartUpload操作停止分段上传。

分段上传请求完成后，Amazon Simple Storage Service 将根据上传的分段构建对象。然后，您可以按照访问存储桶中任何其他对象的方式访问该对象。

您可以列出所有正在执行的分段上传，或者获取为特定分段上传操作上传的分段列表。以上每个操作都在本节中进行了说明。

分段上传开始

当您发送请求以开始分段上传时，Amazon Simple Storage Service 将返回具有上传 ID 的响应。这是分段上传的唯一标识符。无论您何时上传分段、列出分段、完成上传或停止上传，您都必须包括此上传 ID。如果您想要提供描述已上传的对象的任何元数据，必须在请求中指定元数据以开始分段上传。

分段上传

上传分段时，除了指定上传 ID，还必须指定分段编号。您可以选择 1 和 10000 之间的任意分段编号。分段编号在您正在上传的对象中唯一地识别分段及其位置。您选择的分段编号不必是连续序列（例如，它可以是 1、5 和 14）。如果您使用之前上传的分段的同一分段编号上传新分段，则之前上传的分段将被覆盖。

每当您上传分段时，Amazon Simple Storage Service 都会在其响应中返回ETag标头。对于每个分段上传，您都必须记录分段编号和 ETag 值。您必须在随后的请求中包括这些值以完成分段上传。

> **Note**
>
> 分段上传的所有上传分段都会存储在您的存储桶中。它们会占用存储桶的存储空间，直到您完成上传、停止上传或上传超时。有关更多信息，请参阅 分段上传保留本指南下文中的。

分段上传完成

完成分段上传后，Amazon Simple Storage Service 会根据分段编号按升序连接各分段，而从创建对象。如果在开始分段上传请求中提供了任何对象元数据，则 Amazon Simple Storage Service 会将该元数据与对象相关联。成功完成请求后，分段将不再存在。

您完整的分段上传请求必须包含上传 ID 以及分段编号和相应 ETag 值的列表。Amazon 简单存储服务响应包括 ETag 唯一标识组合对象数据的。这不一定 ETag 是对象数据的 MD5 哈希值。

您可以选择停止分段上传。停止分段上传后，无法再次使用该上传 ID 上传任何分段。然后，释放取消的分段上传的任何分段的所有存储空间。如果有任何分段上传正在进行，则即使在您停止后，它们仍然可能会成功或失败。要释放所有分段使用的所有存储，必须仅在完成所有分段的上传后才停止分段上传。

分段上传列表

您可以列出特定分段上传或所有正在进行的分段上传的分段。列出分段操作将返回您已为特定分段上传而上传的分段信息。对于每个列表分段请求，Amazon Simple Storage Service 将返回有关特定分段上传的分段信息，最多为 1000 个分段。如果分段上传中的分段超过 1000 个，您必须发送一系列列出分段请求以检索所有分段。请注意，返回的分段列表不包括仍在上传的分段。使用“列出分段上传”操作，您可以获得正在进行的分段上传的列表。

正在进行的分段上传是已开始但还未完成或停止的上传。每个请求将返回最多 1000 个分段上传。如果正在进行的分段上传超过 1000 个，您必须发送其他请求才能检索剩余的分段上传。仅使用返回的列表进行验证。发送“完成分段上传”请求时，请勿使用此列表的结果。相反，请保留您自己的列表，列出您在上传分段时指定的分段编号以及 Amazon Simple Storage Service 返回的相应 ETag 值。

并发分段上传操作

在分布式开发环境中，您的应用程序可以同时在同一对象上开始多个更新。您的应用程序可能会使用同一对象键开始多个分段上传。然后，对于其中的每个上传，您的应用程序可以上传分段并将完成上传的请求发送到 Amazon Simple Storage Service，以创建数据元。当存储桶启用了版本控制时，完成分段上传将始终创建一个新版本。对于未启用版本控制的存储桶，其他请求可能会优先开始，例如在开始分段上传和完成分段上传之前收到的请求。

> **Note**
>
> 可能会优先考虑其他请求，例如在开始分段上传之后和完成之前收到的请求。例如，使用键开始分段上传之后，其他操作可能会在完成分段上传之前删除该键。如果发生这种情况，则完成分段上传的响应可能表示在未看到对象的情况下成功创建了对象。

分段上传保留

分段上传的所有上传分段都会存储在您的存储桶中。它们会占用存储桶的存储空间，直到您完成上传、停止上传或上传超时。分段上传超时，分段上传将在创建后 24 小时后删除。若您停止分段上传或分段上传超时，所有上传的分段都将被删除，并释放它们在存储桶上占用的存储空间。

Amazon Simple Storage Service 分段上传限制

下表提供了分段上传的核心规范。

- 最大对象大小：5 TB
- 每次上传的最大分段数量：10000 个
- 分段编号：1-10000（含）
- 分段大小：5 MB（最小值）- 5 GB（最大值）。未对分段上传的最后一段施加大小限制。
- “列出分段”请求返回的最大分段数量：1,000
- “列出分段上传”请求返回的最大分段上传数量：1,000

拆分要上传的文件

在 Linux 或 Linux 操作系统中使用 `split` 命令可以将文件拆分为多个分段，然后将其上传到存储桶。您可以在 Windows 操作系统中使用类似的免费软件应用程序来拆分文件。将文件拆分为多个部分后，继续执行本指南的启动分段上传部分。

使用 AWS CLI启动分段上传

完成以下过程，以使用 AWS Command Line Interface（AWS CLI）启动分段上传。使用 `create-multipart-upload` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》create-multipart-upload中的。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以为存储桶创建分段上传。

```
aws s3api create-multipart-upload --bucket BucketName --key ObjectKey --acl bucket-owner-full-control
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要为其创建分段上传的存储桶的名称。
- *ObjectKey*-用于要上传的文件的对象密钥。

示例：

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket --key sailbot.mp4 --
acl bucket-owner-full-control
```

您应看到类似于以下示例的结果。响应包括一个 UploadID，您必须在随后的命令中指定，才能上传分段以及完成此对象的分段上传。

```
C:\ >aws s3api create-multipart-upload --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4
{
    "AbortDate": "2021-05-20T00:00:00+00:00",
    "AbortRuleId": "ExpireMultiPart",
    "ServerSideEncryption": "AES256",
    "Bucket": "DOC-EXAMPLE-BUCKET",
    "Key": "sailbot.mp4",
    "UploadId": "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
}
```

在拥有分段上传的 UploadID 之后，请继续执行本指南的以下使用 AWS CLI上传分段部分，然后开始上传分段。

使用上传分段 AWS CLI

完成以下过程，以使用 AWS Command Line Interface （ AWS CLI ）上传分段上传的分段。使用 upload-part 命令完成此操作。有关更多信息，请参阅《AWS CLI Command Reference》中的 upload-part。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以将分段上传到存储桶。

```
aws s3api upload-part --bucket BucketName --key ObjectKey --part-number Number --
body FilePart --upload-id "UploadID"  --acl bucket-owner-full-control
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要为其创建分段上传的存储桶的名称。
- *ObjectKey*-用于要上传的文件的对象密钥。
- *Number*-您正在上传的分段的部件号。分段编号在您正在上传的对象中唯一地识别分段及其位置。请确保每次上传分段时，以递增方式增加 `--part-number` 参数。为此，请按照完成分段上传时 Amazon Simple Storage Service 组装对象的顺序来对其进行编号。
- *FilePart*-要从您的计算机上传的零件文件。
- *UploadID*-您在本指南前面部分创建的分段上传的上传 ID。

示例：

```
aws s3api upload-part --bucket amzn-s3-demo-bucket --
key sailbot.mp4 --part-number 1 --body sailbot.mp4.001 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

您应看到类似于以下示例的结果。对每个上传的分段重复 `upload-part` 命令。每个上传分段请求的响应将包括已上传分段的 ETag 值。记录您上传的每个分段的 ETag 值。您将需要所有的 ETag 值来完成分段上传，之后这将在本指南中进行介绍。

```
C:\ >aws s3api upload-part --bucket DOC-EXAMPLE-BUCKET  --key sailbot.mp4  --part-number 1 --body sailbot.mp4.001
 --upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "ServerSideEncryption": "AES256",
    "ETag": "\"4example7530246113e837a860a38bbb\""
}
```

使用 Amazon CLI 列出分段上传的分段

完成以下过程，以使用 AWS Command Line Interface（AWS CLI）列出分段上传的分段。使用 `list-parts` 命令完成此操作。有关更多信息，请参阅《AWS CLI Command Reference》中的 list-parts。

完成此过程以获取分段上传中所有已上传分段的 ETag 值。您将需要这些值来完成分段上传，之后这将在本指南中进行介绍。但是，如果您记录了分段上传响应中的 ETag 值，则可以跳过此过程并继续执行本指南的创建分段上传 .json 文件部分。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以列出存储桶中分段上传的分段。

```
aws s3api list-parts --bucket BucketName --key ObjectKey --upload-id "UploadID"
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要列出分段上传的各个部分的存储桶的名称。
- *ObjectKey*-分段上传的对象密钥。
- *UploadID*-您在本指南前面部分创建的分段上传的上传 ID。

示例：

```
aws s3api list-parts --bucket amzn-s3-demo-bucket --key sailbot.mp4 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
```

您应看到类似于以下示例的结果。响应列出了所有分段编号和您在分段上传中上传的分段的 ETag 值。将这些值复制到剪贴板，然后继续执行本指南的创建分段上传 .json 部分。

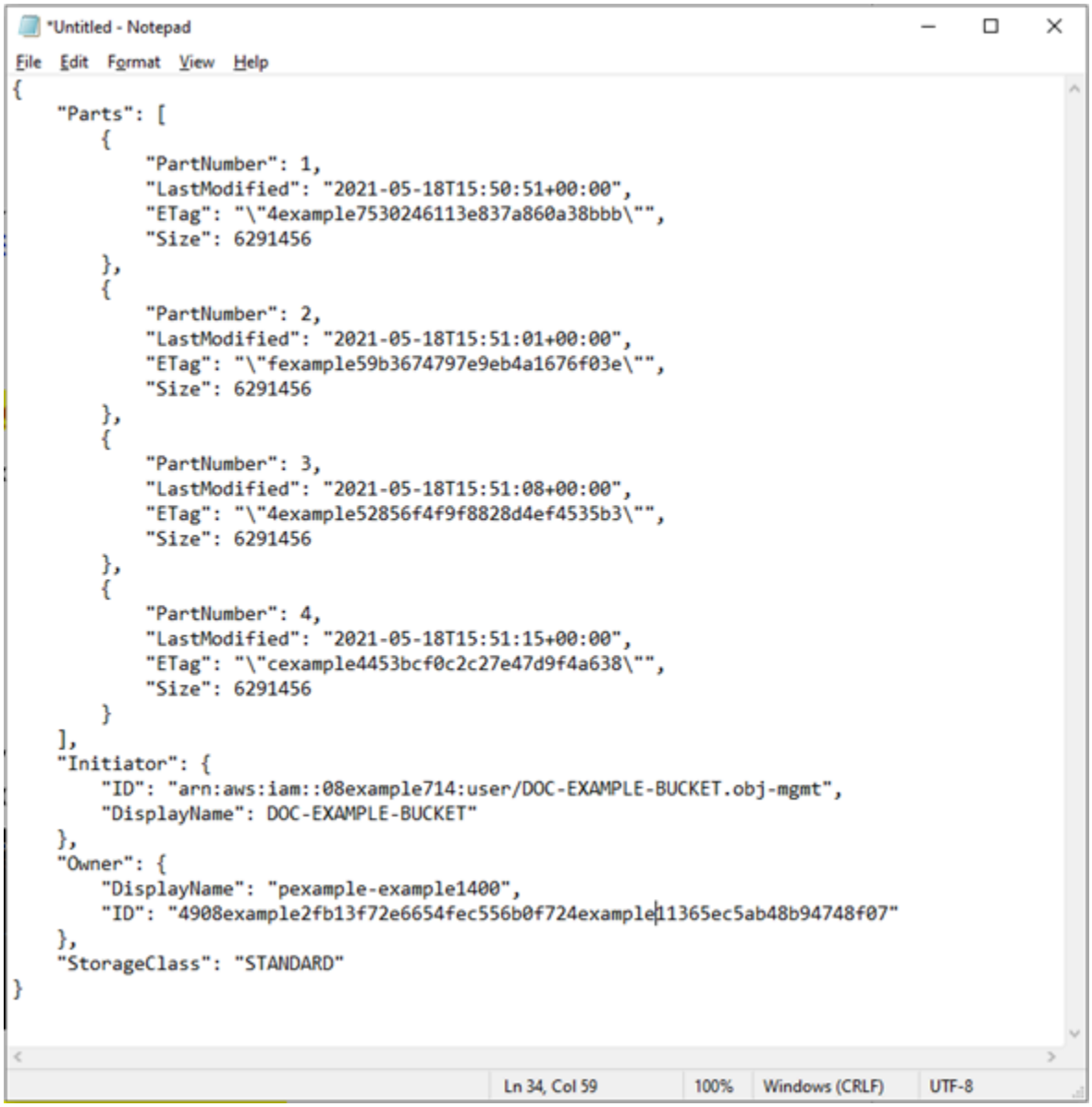
```
C:\>aws s3api list-parts --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotR
hTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "Parts": [
        {
            "PartNumber": 1,
            "LastModified": "2021-05-18T15:50:51+00:00",
            "ETag": "\"4example7530246113e837a860a38bbb\"",
            "Size": 6291456
        },
        {
            "PartNumber": 2,
            "LastModified": "2021-05-18T15:51:01+00:00",
            "ETag": "\"fexample59b3674797e9eb4a1676f03e\"",
            "Size": 6291456
        },
        {
            "PartNumber": 3,
            "LastModified": "2021-05-18T15:51:08+00:00",
            "ETag": "\"4example52856f4f9f8828d4ef4535b3\"",
            "Size": 6291456
        },
        {
            "PartNumber": 4,
            "LastModified": "2021-05-18T15:51:15+00:00",
            "ETag": "\"cexample4453bcf0c2c27e47d9f4a638\"",
            "Size": 6291456
        }
    ],
    "Initiator": {
        "ID": "arn:aws:iam::08example714:user/DOC-EXAMPLE-BUCKET.obj-mgmt",
        "DisplayName": "DOC-EXAMPLE-BUCKET"
    },
    "Owner": {
        "DisplayName": "pexample-example1400",
        "ID": "4908example2fb13f72e6654fec556b0f724example11365ec5ab48b94748f07"
    },
    "StorageClass": "STANDARD"
}
```

创建分段上传 .json 文件

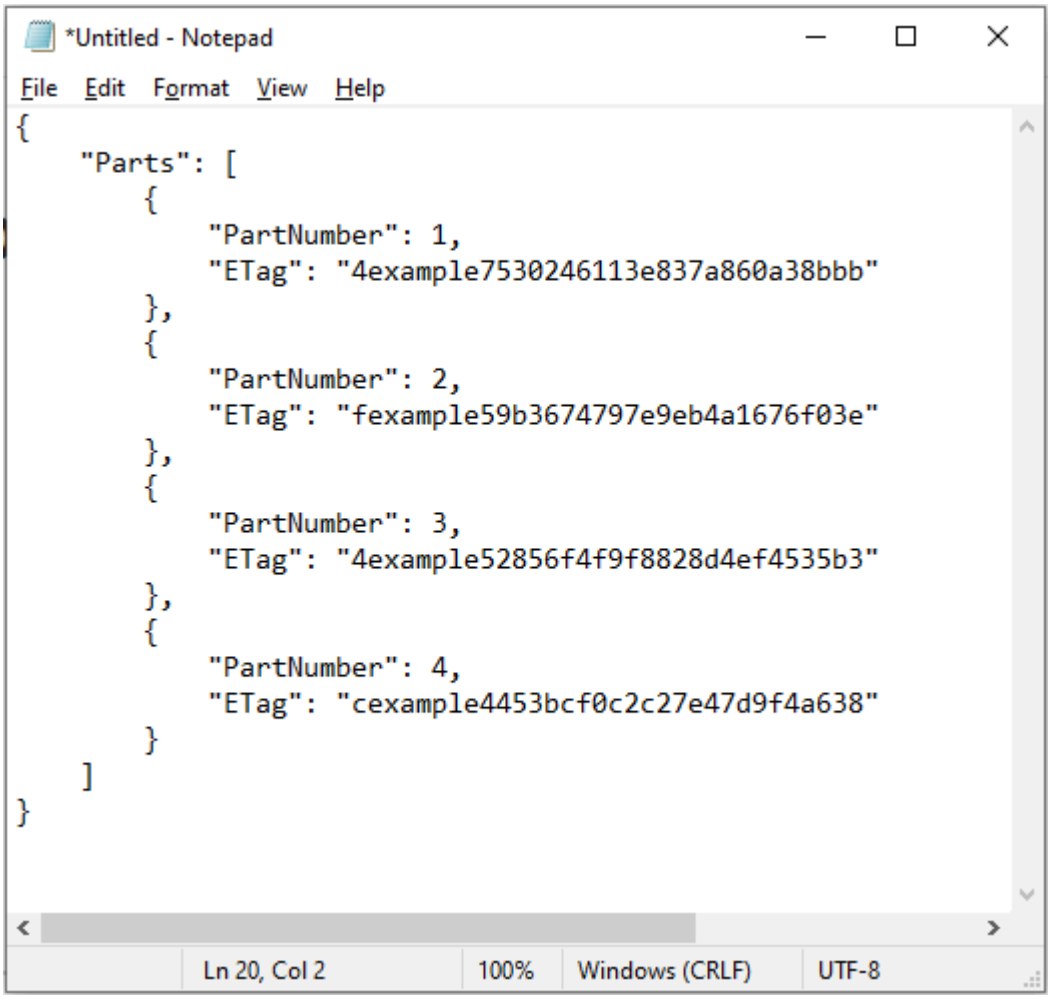
完成以下步骤以创建分段上传 .json 文件，该文件定义您上传的所有分段及其 ETag 值。之后在本指南中需要该文件才能完成分段上传。

1. 打开文本编辑器，将在本指南的上一部分中请求的 `list-parts` 命令的响应粘贴在其中。

   结果应该类似以下示例。



2. 重新格式化文本文件，如以下示例所示：



3. 将文本文件作为 `mpstructure.json` 保存到计算机，然后继续执行本指南的使用 Amazon CLI 完成分段上传部分。

使用 Amazon CLI 完成分段上传

完成以下过程，以使用 AWS Command Line Interface （AWS CLI）完成分段上传。使用 `complete-multipart-upload` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》complete-multipart-upload中的。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。

2. 输入以下命令以将分段上传到存储桶。

```
aws s3api complete-multipart-upload --multipart-upload file://JSONFileName --
bucket BucketName --key ObjectKey --upload-id "UploadID"  --acl bucket-owner-full-
control
```

在该命令中，将以下示例文本替换为自己的文本：

- *JSONFileName*-您在本指南前面部分创建的.json 文件的名称（例如，mpstructure.json）。
- *BucketName*-您要为其完成分段上传的存储桶的名称。
- *ObjectKey*-分段上传的对象密钥。
- *UploadID*-您在本指南前面部分创建的分段上传的上传 ID。

Example:

```
aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json
 --bucket amzn-s3-demo-bucket --key sailbot.mp4 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

您应看到类似于以下示例的响应。这确认分段上传已完成。现在，可在存储桶中组装并提供该对象。

```
C:\>aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json --bucket DOC-EXAMPLE-BUCKET  --key sailbot.mp4
--upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "ServerSideEncryption": "AES256",
    "VersionId": "MexampleKMdfPQb.2YZHqOvE_T.vSDtY",
    "Location": "https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com/sailbot.mp4",
    "Bucket": "DOC-EXAMPLE-BUCKET",
    "Key": "sailbot.mp4",
    "ETag": "\"1example5964e3115e5d3f3c9a731585-4\""
}
```

使用 Amazon CLI 列出存储桶分段上传

完成以下过程，以使用 AWS Command Line Interface（AWS CLI）列出存储桶所有的分段上传。使用 list-multipart-uploads 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》list-multipart-uploads中的。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以将分段上传到存储桶。

```
aws s3api list-multipart-uploads --bucket BucketName
```

在命令中，*BucketName*替换为要列出其所有分段上传的存储桶的名称。

示例：

```
aws s3api list-multipart-uploads --bucket amzn-s3-demo-bucket
```

您应看到类似于以下示例的响应。



使用 Amazon CLI 停止分段上传

使用 AWS Command Line Interface (AWS CLI) 完成以下步骤以停止分段上传。如果您已开始分段上传但不想继续上传，则可以执行此操作。使用 `abort-multipart-upload` 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》abort-multipart-upload中的。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以将分段上传到存储桶。

```
aws s3api abort-multipart-upload --bucket BucketName --key ObjectKey --upload-id
 "UploadID" --acl bucket-owner-full-control
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*-您要停止分段上传的存储桶的名称。
- *ObjectKey*-分段上传的对象密钥。
- *UploadID*-您要停止的分段上传的上传 ID。

示例：

```
aws s3api abort-multipart-upload --bucket amzn-s3-demo-bucket --key sailbot.mp4 --
upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

此命令不会返回响应。您可以运行 `list-multipart-uploads` 命令以确认分段上传已停止。

遵守 Lightsail 对象存储的存储分区命名要求

在 Amazon Lightsail 对象存储服务中创建存储桶时，必须为其命名。存储桶名称是客户在访问存储桶中存储的对象时将使用的 URL 的一部分。例如，如果您`amzn-s3-demo-bucket`在中命名存储桶 `us-east-1` AWS 区域，则您的存储桶的 URL 为`amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com`。创建存储桶后无法更改其名称。请记住，客户能够看到您指定的存储桶名称。有关 Lightsail 对象存储服务的更多信息，请参阅对象存储。有关创建存储桶的更多信息，请参阅创建存储桶。

存储桶名称必须符合 DNS 标准。因此，以下规则适用于在 Lightsail 中命名存储桶：

- 存储桶名称必须介于 3 到 56 个字符之间。
- 存储桶名称只能由小写字母、数字和连字符 (-) 组成。
- 存储桶名称必须以字母或数字开头和结尾。
- 连字符 (-) 可以分隔单词，但不能连续指定。例如，允许使用 doc-example-bucket，但不允许使用 doc--example--bucket。
- 存储桶名称必须在 aws（标准区域）分区中是唯一的，其中包括 Amazon Simple Storage Service（Amazon S3）中的存储桶。
- 存储桶名称不得以前缀 amzn-s3-demo- 开头。
- 存储桶名称不得以前缀 sthree- 开头。
- 存储桶名称不得以前缀 sthree-configurator 开头。
- 存储桶名称不得以后缀 -s3alias 结尾。

示例存储桶名称

以下示例存储桶名称是有效的，并遵循建议的命名准则：

- docexamplebucket1
- log-delivery-march-2020
- my-hosted-content

不允许使用以下示例存储桶名称：

- doc.example.bucket（包含句点）
- doc--example--bucket（包含两个连续的连字符）
- doc-example-bucket-（以连字符结尾）

Lightsail 对象存储桶的密钥名称

您上传到存储桶的文件将作为对象存储在 Amazon Lightsail 对象存储服务中。对象键（或键名称）唯一标识存储桶中存储的对象。本指南解释了密钥名称和密钥名称前缀的概念，它们构成了通过 Lightsail 控制台查看的存储桶的文件夹结构。有关存储桶的更多信息，请参阅对象存储。

键名称

Lightsail 对象存储服务数据模型使用扁平结构，而不是像在文件系统中看到的那样使用分层结构。它不包含文件夹和子文件夹层次结构。但您可以使用键名称前缀和分隔符推断逻辑层次结构。Lightsail 控制台使用密钥名称前缀以文件夹结构显示您的对象。

假设您的存储桶包含具有以下对象键的四个对象：

- `Development/Projects.xls`
- `Finance/statement1.pdf`
- `Private/taxdocument.pdf`
- `to-dos.doc`

Lightsail 控制台使用密钥名称前缀 (`Development/`、`Finance/`和`Private/`) 和分隔符 (`/`) 来呈现文件夹结构。`to-dos.doc` 键名称没有前缀，因此其对象直接在存储桶的根级别出现。如果您在 Lightsail 控制台中浏览到该`Development/`文件夹，则会看到该对象。`Projects.xls`您会在 `Finance/` 文件夹中看到 `statement1.pdf` 对象，并且会在 `Private/` 文件夹中看到 `taxdocument.pdf` 对象。

Lightsail 控制台允许通过创建以密钥名称前缀和分隔符值作为密钥名称的零字节对象来创建文件夹。这些文件夹对象不会显示在控制台中。但是，它们的行为与任何其他对象一样。您可以使用 Amazon S3 API、 AWS Command Line Interface (AWS CLI) 或来查看和操作它们 AWS SDKs。

对象键命名准则

您可以在对象键名中使用任意 UTF-8 字符。但是，在键名中使用某些字符可能导致一些应用程序和协议出现问题。以下准则可帮助您最大限度地遵守 DNS、Web 安全字符、XML 解析器等。 APIs

安全字符

以下字符集通常可安全地用于键名。

- 字母数字字符
  - 0-9
  - a-z
  - A-Z
- 特殊字符

- 正斜杠 (/)
- 感叹号 (!)
- 连字符 (-)
- 下划线 (_)
- 句点 (.)
- 星号 (*)
- 单引号 (')
- 左括号 (()
- 右括号 ())

以下是有效对象键名的示例：

- `4my-organization`
- `my.great_photos-2014/jan/myvacation.jpg`
- `videos/2014/birthday/video1.wmv`

> **Important**
>
> 如果对象密钥名称以单个句点 (.) 或两个句点 (..) 结尾，则无法使用 Lightsail 控制台下载该对象。要下载密钥名称以一两个句点结尾的对象，必须使用 Amazon S3 API AWS CLI、和 AWS SDKs。有关更多信息，请参阅下载存储桶对象。

可能需要特殊处理的字符

键名中的以下字符可能需要另外进行代码处理，并且可能需要以十六进制形式在 URL 中编码或引用。其中部分字符是不可打印的字符，浏览器可能无法处理它们，这也需要特殊处理：

- 表示和的符号 ("&")
- 美元符号 ("$")
- ASCII 字符范围 00–1F 十六进制（0–31 十进制）和 7F（127 十进制）
- "At" 符号 ("@")
- 等于号 ("=")
- 分号 (";")

- 冒号 (":")
- 加号 ("+")
- 空格 – 大量连续空格可能会在某些使用情形中丢失（特别是多个空格）
- 逗号 (",")
- 问号 ("?")

要避免的字符

避免在键名中使用以下字符，因为这些字符需要进行大量的特殊处理，才能在所有应用程序间保持一致性。

- 反斜杠 ("\")
- 左大括号 ("{")
- 不可打印的 ASCII 字符（128–255 十进制字符）
- 插入符号 ("^")
- 右大括号 ("}")
- 百分比字符 ("%")
- 重音符/反勾号 ("`")
- 右方括号 ("]")
- 引号
- “大于”符号 (">")
- 左方括号 ("[")
- 波浪字符 ("~")
- “小于”符号 ("<")
- “井号”字符 ("#")
- 竖线 ("|")

XML 相关的对象键约束

按照 XML end-of-line 处理标准的规定，所有 XML 文本都经过标准化，因此单回车符（ASCII 代码 13）和紧接着换行符的回车符（ASCII 代码 10）被单个换行符所取代。为了确保正确解析 XML 请求中

的对象键，当将回车符和其他特殊字符插入 XML 标签时，必须使用等效的 XML 实体代码替换回车符和其他特殊字符。以下是此类特殊字符及其等效实体代码的列表：

- ' 用作 '
- ” 用作 "
- & 用作 &
- < 用作 <
- < 用作 >
- \r 用作
 或
- \n 用作
 或

以下示例说明了使用 XML 实体代码替换回车的情况。此 DeleteObjects 请求将删除带有键参数 /some/prefix/objectwith\rcarriagereturn 的对象（其中 \r 是回车）。

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
      <Object>
        <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
      </Object>
    </Delete>
```

安全 Lightsail 对象存储桶

Amazon Lightsail 对象存储提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

目录

- 预防性安全最佳实践
  - 实施最低权限访问
  - 确认您的 Lightsail 存储桶不可公开访问
  - 在 Amazon S3 中启用屏蔽公共访问权限
  - 将实例附加到存储桶，以授予完全编程访问
  - 轮换存储桶访问密钥
  - 使用跨账户访问权限向其他 AWS 账户授予对存储桶中对象的访问权限
  - 数据加密

- 启用版本控制
- 监测和审计最佳实践
  - 启用访问日志记录并定期执行安全和访问审计
  - 识别、标记和审核您的 Lightsail 存储桶
  - 使用 AWS 监控工具实施监控
  - 使用 AWS CloudTrail
  - 监控 AWS 安全公告

预防性安全最佳实践

以下最佳做法可以帮助防止 Lightsail 存储桶发生安全事件。

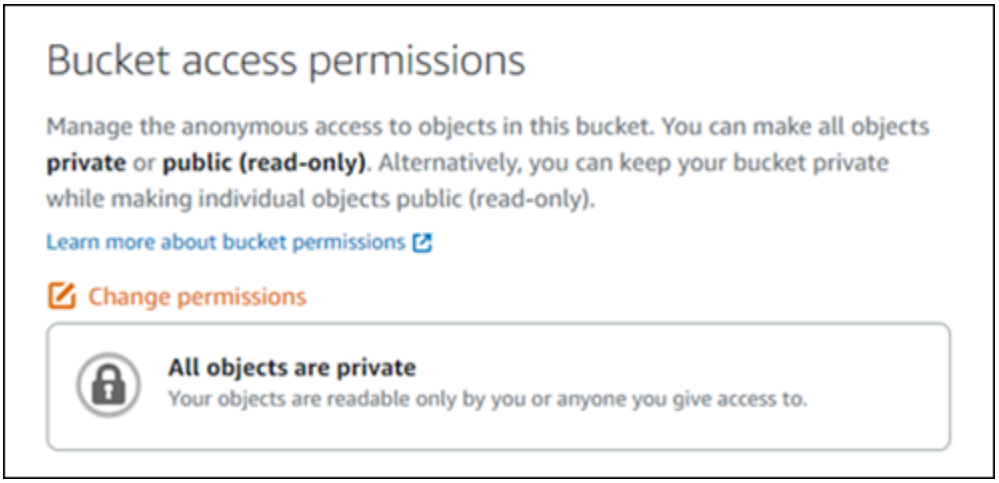
实施最低权限访问

在授予权限时，您可以决定谁将获得哪些 Lightsail 资源的权限。您可以对这些资源启用希望允许的特定操作。因此，您应仅授予执行任务所需的权限。实施最低权限访问对于减小安全风险以及可能由错误或恶意意图造成的影响至关重要。

有关创建 IAM policy 来管理存储桶的更多信息，请参阅用于管理存储桶的 IAM policy。有关 Lightsail 存储桶支持的 Amazon S3 操作的更多信息，请参阅 Ama z on Lightsail API 参考中的对象存储操作。

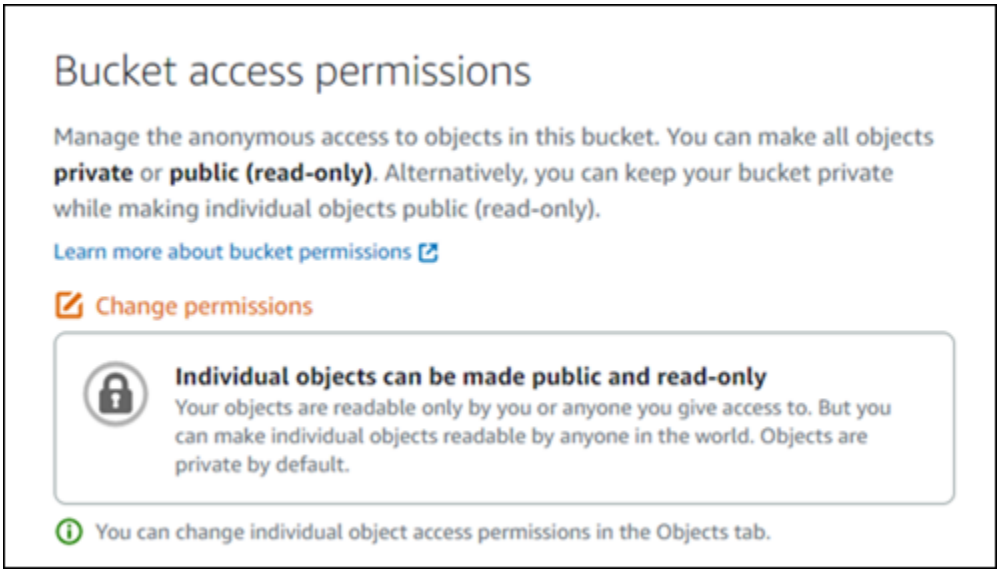
确认您的 Lightsail 存储桶不可公开访问

默认情况下，存储桶和对象都是私有的。通过将存储桶访问权限设置为 All objects are private（所有存储桶均为私有）使存储桶保持私有。对于大多数用例，您无需将存储桶或单个对象设为公有。有关更多信息，请参阅配置存储桶中个别对象的访问权限。

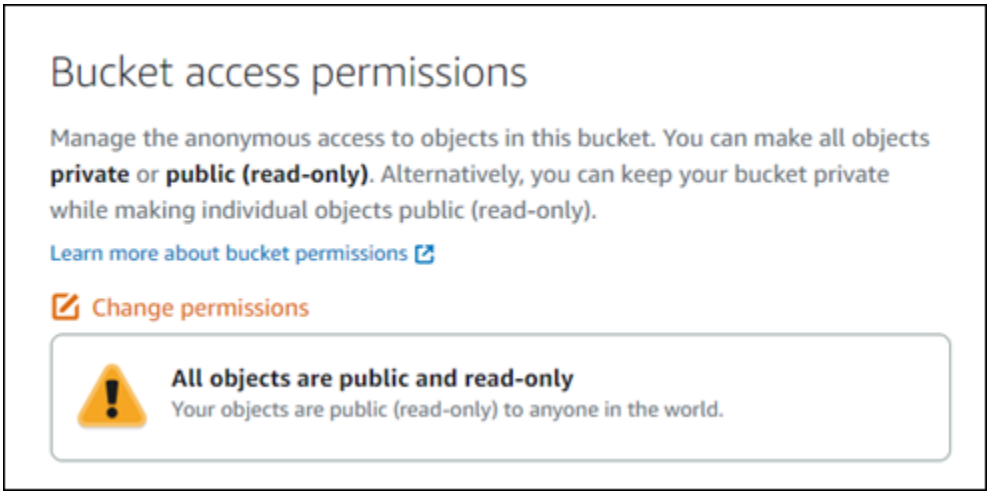


但是，如果您使用存储桶托管网站或应用程序的媒体，在某些情况下，可能需要将存储桶或单个对象设为公有。您可以配置以下选项之一，以将存储桶或单个对象设为公有：

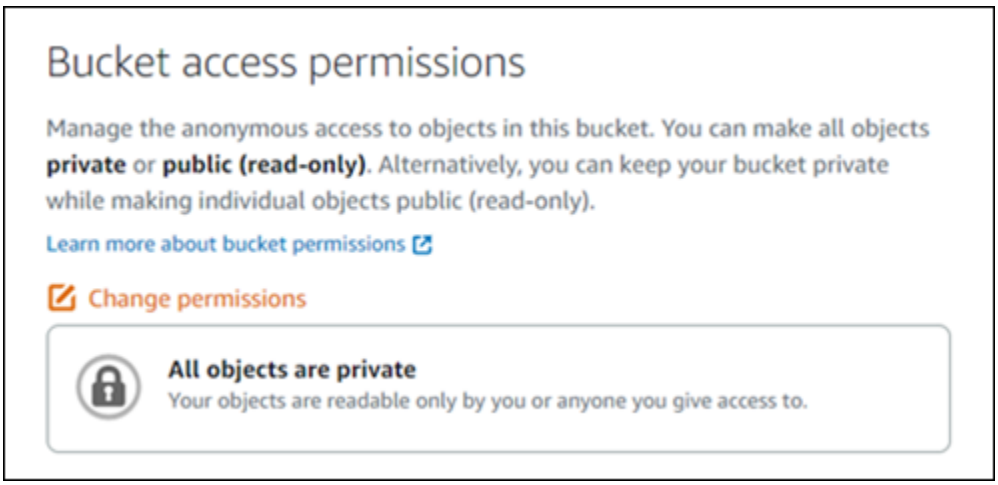
- 如果存储桶中的某些对象需要对互联网上的任何人公开（只读），请将存储桶访问权限更改为 Individual objects can be made public and read-only（单个对象可设为公有且只读），并且仅将需要设为公有的对象更改为 Public (read-only)（公有（只读））。此选项会将存储桶设为私有，但允许您选择将单个对象设为公有。如果单个对象包含您不希望可公有访问的敏感或机密信息，则不要将其设为公有。如果您将单个对象设为公有，则应定期验证各个对象的公共可访问性。



- 如果存储桶中的所有对象都需要对互联网上的任何人公开（只读），请将存储桶访问权限更改为 All objects are public and read-only（所有对象均为公有且只读）。如果存储桶中的任何对象包含敏感或机密信息，请勿使用此选项。



- 如果您之前已将存储桶更改为公有，或者将单个对象更改为公有，则可以通过将存储桶访问权限更改为 All objects are private（所有对象均为私有）来快速将存储桶及其所有对象更改为私有。

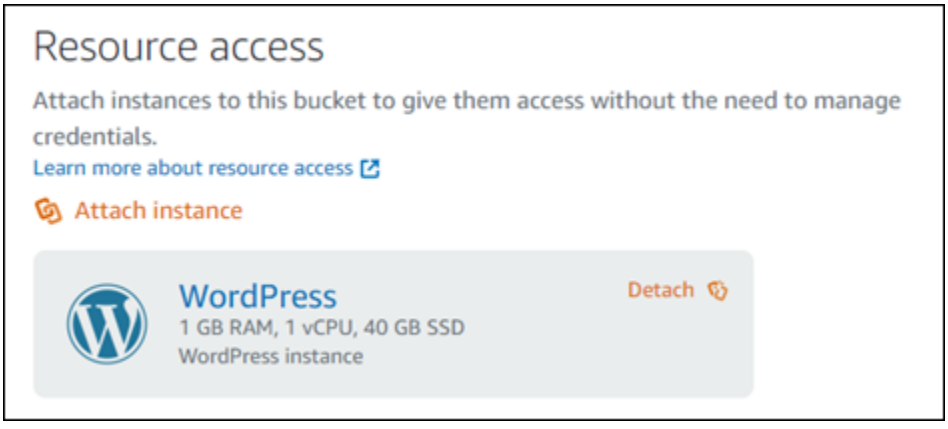


在 Amazon S3 中启用屏蔽公共访问权限

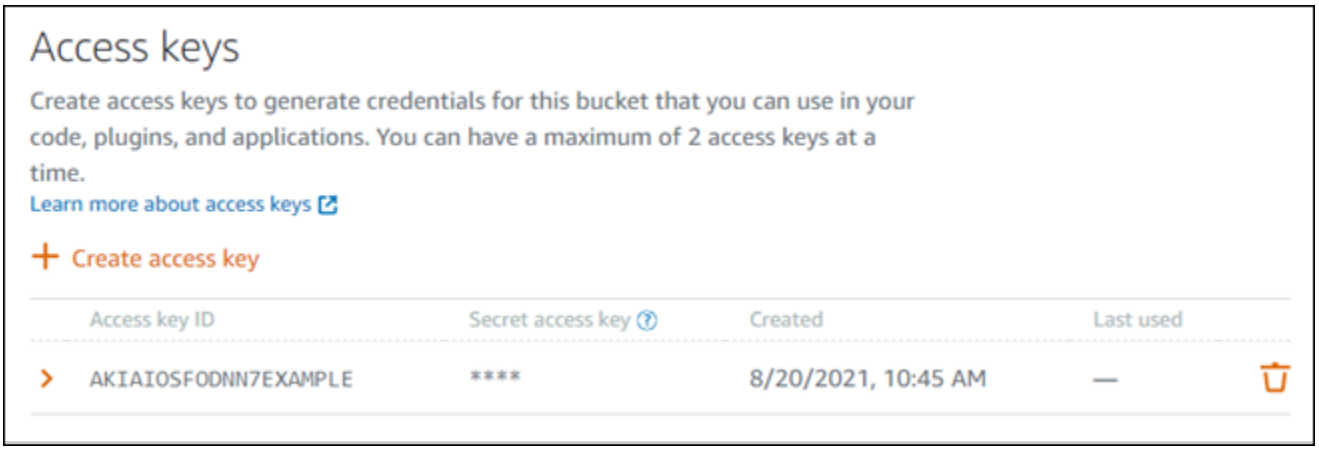
在允许或拒绝公开访问时，Lightsail 对象存储资源会同时考虑 Lightsail 存储桶访问权限和 Amazon S3 账户级别的封禁公共访问配置。借助 Amazon S3 账户级别的封禁公共访问权限，账户管理员和存储桶拥有者可以集中限制公众对其的 Amazon S3 和 Lightsail 存储桶的访问权限。封锁公有访问可以将所有 Amazon S3 和 Lightsail 存储桶设为私有，无论资源是如何创建的，也无论可能配置了哪个存储桶和对象权限。有关更多信息，请参阅屏蔽对存储桶的公共访问权限。

将实例附加到存储桶，以授予完全编程访问

将实例附加到 Lightsail 对象存储桶是提供对存储桶的访问权限的最安全的方式。资源访问功能（将实例附加到存储桶的方式）可以授予实例对存储桶的完全编程访问权限。使用此方法，您不必将存储桶凭证直接存储在实例或应用程序中，也不必定期轮换凭证。例如，某些 WordPress 插件可以访问实例有权访问的存储桶。有关更多信息，请参阅配置存储桶的资源访问权限和教程：将存储桶连接到您的 WordPress 实例。



但是，如果应用程序不在 Lightsail 实例上，则可以创建和配置存储桶访问密钥。存储桶访问密钥是长期凭证，不会自动轮换。有关更多信息，请参阅 创建 Lightsail 对象存储桶访问密钥。



轮换存储桶访问密钥

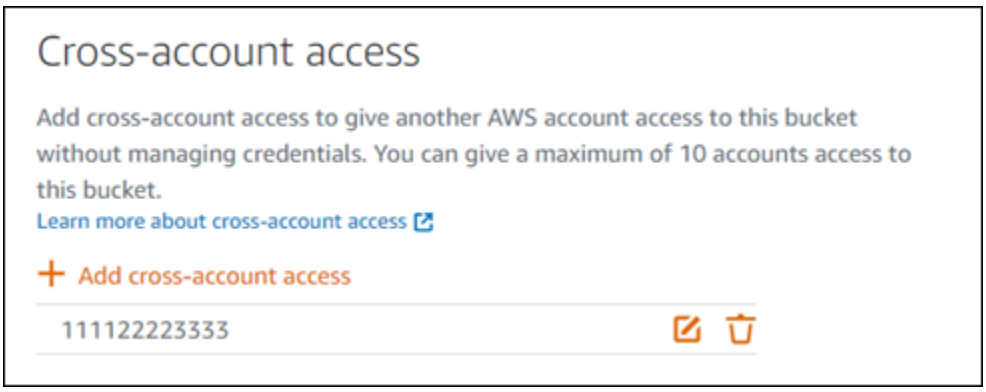
每个存储桶最多可以有两个访问密钥。尽管您可以同时拥有两个不同的访问密钥，但我们建议您在密钥轮换时间之外一次只为存储桶创建一个访问密钥。这种方法可确保您可以随时创建新的存储桶访问密钥，而不必使用该密钥。例如，如果您现有的私有访问密钥被复制、丢失或泄露，并且需要轮换现有访问密钥，则创建第二个访问密钥进行轮换会很有帮助。

如果您在存储桶中使用访问密钥，则应定期轮换密钥，并清点现有密钥。请确认上次使用访问密钥的日期以及使用访问密钥的 AWS 区域 与您对该密钥的使用方式期望相符。上次使用访问密钥的日期显示在 Lightsail 控制台的存储分区管理页面 “权限” 选项卡的 “访问密钥” 部分中。删除未使用的访问密钥。

要轮换访问密钥，您应该创建一个新的访问密钥，在软件上对其进行配置并进行测试，然后删除以前使用的访问密钥。在您删除访问密钥后，该密钥将永久消失且无法恢复。您只能将其替换为新的访问密钥。有关更多信息，请参阅创建 Lightsail 对象存储桶访问密钥 和删除 Lightsail 对象存储桶的访问密钥。

使用跨账户访问权限向其他 AWS 账户授予对存储桶中对象的访问权限

您可以使用跨账户访问权限使拥有 AWS 账户的特定个人可以访问存储桶中的对象，而无需将存储桶及其对象公开。如果您配置了跨账户访问权限，请确保 IDs 列出的账户是您想要授予对存储桶中对象的访问权限的正确账户。有关更多信息，请参阅为存储桶配置跨账户存取。



数据加密

Lightsail 使用亚马逊托管密钥执行服务器端加密，并通过强制执行 HTTPS (TLS) 对传输中的数据进行加密。服务器端加密通过单独服务中存储的密钥对数据进行加密，有助于降低数据风险。此外，对传输中的数据进行加密有助于防止潜在的攻击者使用 person-in-the-middle或类似的攻击窃听或操纵网络流量。

启用版本控制

版本控制是在相同的桶中保留对象的多个变量的方法。您可以使用版本控制来保存、检索和还原存储在 Lightsail 存储桶中的每个对象的每个版本。使用版本控制能够轻松从用户意外操作和应用程序故障中恢复数据。有关更多信息，请参阅启用和暂停存储桶对象版本控制。

监测和审计最佳实践

以下最佳做法可以帮助检测 Lightsail 存储桶的潜在安全漏洞和事件。

启用访问日志记录并定期执行安全和访问审计

访问日志记录详细地记录对存储桶做出的各种请求。这些信息可能包括请求类型（GET、PUT）、请求中指定的资源以及处理请求的时间和日期。为存储桶启用访问日志记录，并定期执行安全和访问审计，以确定正在访问存储桶的实体。默认情况下，Lightsail 不会收集存储桶的访问日志。您必须手动启用访问日志记录。有关更多信息，请参阅存储桶访问日志和启用存储桶访问日志记录。

识别、标记和审核您的 Lightsail 存储桶

确定您的 IT 资产是监管和安全性的一个至关重要的方面。您需要查看所有 Lightsail 存储桶，以评估其安全态势并对潜在的薄弱环节采取措施。

使用标签确定安全性敏感或审计敏感资源，然后在您需要搜索这些资源时使用这些标签。有关更多信息，请参阅标签。

使用 AWS 监控工具实施监控

监控是维护 Lightsail 存储桶和其他资源的可靠性、安全性、可用性和性能的重要组成部分。您可以在 Lightsail 中监控存储桶大小 (BucketSizeBytes) 和 Number of objects (NumberOfObjects) 存储桶指标并创建通知警报。例如，当存储桶的大小增加或减少到特定大小时，或者当存储桶中的对象数量上升或下降到特定数量时，您可能希望收到通知。有关更多信息，请参阅创建存储桶指标警报。

使用 AWS CloudTrail

AWS CloudTrail 提供用户、角色或 AWS 服务在 Lightsail 中执行的操作的记录。您可以使用收集的信息 CloudTrail 来确定向 Lightsail 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。例如，您可以识别影响数据访问的操作 CloudTrail条目，特别是CreateBucketAccessKeyGetBucketAccessKeys、DeleteBucketAccessKeySetResourceAcces和UpdateBucket。设置 AWS 账户时，默认 CloudTrail 处于启用状态。您可以在 CloudTrail 控制台中查看最近的事件。要为您的 Lightsail 存储桶创建持续的活动和事件记录，您可以在控制台中创建跟踪。 CloudTrail 有关更多信息，请参阅 AWS CloudTrail 用户指南中的记录数据事件以便跟踪。

监控 AWS 安全公告

主动监控注册到 AWS 账户的主电子邮件地址。 AWS 将使用此电子邮件地址就可能影响您的新出现的安全问题与您联系。

AWS 具有广泛影响的运营问题发布在 S AWS ervice Health Das hboard 上。操作性问题也会通过 Personal Health Dashboard 发布给个人账户。有关更多信息，请参阅 AWS Health 文档。

控制对 Lightsail 存储桶和对象的访问权限

默认情况下，所有 Amazon Lightsail 对象存储资源（存储桶和对象）都是私有的。这意味着只有存储桶拥有者，即创建该存储分区的 Lightsail 账户，才能访问存储分区及其对象。存储桶拥有者可以选择将其访问权限授予其他人员。您可以通过以下方式授予存储桶及其对象的访问权限：

- 只读访问权限 — 以下选项控制通过存储桶 URL（例如，https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg）对存储桶及其对象进行只读访问的权限。
  - 存储桶访问权限 — 使用存储桶访问权限向互联网上的所有人授予存储桶中所有对象的访问权限。有关更多信息，请参阅本指南下文中的存储桶访问权限。
  - 个别对象访问权限 — 使用个别对象访问权限向互联网上的所有人授予存储桶中个别对象的访问权限。有关更多信息，请参阅本指南下文中的个别对象访问权限。
  - 跨账户访问权限-使用跨账户访问权限为其他 AWS 账户授予对存储桶中所有对象的访问权限。有关更多信息，请参阅本指南下文中的跨账户存取。

- 读写访问权限 — 以下选项控制存储桶及其对象的完全读写访问权限。将这些选项与 AWS Command Line Interface (AWS CLI) AWS APIs、和 AWS SDKs。
  - 访问密钥 — 使用访问密钥授予应用程序或插件的访问权限。有关更多信息，请参阅本指南下文中的访问密钥。
  - 资源访问权限-使用资源访问权限来授予对 Lightsail 实例的访问权限。有关更多信息，请参阅本指南下文中的资源访问权限。
- 亚马逊简单存储服务阻止公开访问 — 使用亚马逊简单存储服务 (Amazon S3) 账户级封锁公开访问功能，集中限制公众对亚马逊 S3 和 Lightsail 中存储桶的访问。封锁公有访问可以将所有 Amazon S3 和 Lightsail 存储桶设为私有，无论可能配置了何种存储桶和对象权限。有关更多信息，请参阅本指南下文中的 Amazon S3 屏蔽公共访问权限。

有关存储桶的更多信息，请参阅对象存储。有关安全最佳实践的更多信息，请参阅对象存储的安全最佳实践。

存储桶访问权限

使用存储桶访问权限控制存储桶中对象的公有（未经身份验证的）只读访问权限。配置存储桶访问权限时，您可以选择以下选项之一：

- 所有对象都是私有的 — 只有您或您授予访问权限的人才可以读取存储桶中的所有对象。此选项不允许将个别对象设为公有（只读）。
- 个别对象可设为公有（只读）— 存储桶中的对象只能由您或您授予访问权限的人读取，除非您将个别对象设为公有（只读）。此选项允许将个别对象设为公有（只读）。有关更多信息，请参阅本指南下文中的个别对象访问权限。
- 所有对象都是公有的（只读）— 互联网上的任何人都可以读取存储桶中的所有对象。如果您选择此选项，则互联网上的所有人都可以通过存储桶的 URL（例如，`https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg`）来读取所有对象。

有关配置存储桶访问权限的更多信息，请参阅配置存储桶访问权限。

个别对象访问权限

使用个别对象访问权限控制存储桶中个别对象的公有（未经身份验证的）只读访问权限。仅当存储桶的存储桶访问权限允许将个别对象设为公有（只读）时，才可以配置个别对象访问权限。配置个别对象的访问权限时，您可以选择以下选项之一：

- 私有 — 只有您或您授予访问权限的人才可以读取对象。

- 公有（只读）— 互联网上的任何人都可以读取对象。通过存储桶的 URL（例如，`https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg`），互联网上的任何人都可以读取个别对象。

有关配置个别对象访问权限的更多信息，请参阅在存储桶中配置个别对象的访问权限。

跨账户访问

使用跨账户访问权限为其他 AWS 账户及其用户授予对存储桶中所有对象的经过身份验证的只读访问权限。如果您想与其他账户共享对象，则跨 AWS 账户访问是理想的选择。如果您将跨账户存取授予其他 AWS 账户，则该账户中的用户可以通过存储桶的 URL（例如 `https://amzn-s3-demo-bucket.us-east-1.amazonaws.com/media/sailbot.jpg`）以只读方式访问存储桶中的对象。您最多可以授予 10 个 AWS 账户的访问权限。

有关配置跨账户存取的更多信息，请参阅配置存储桶的跨账户存取。

访问密钥

使用访问密钥创建一组凭证，以授予存储桶及其对象的完全读写访问权限。访问密钥包含一组访问密钥 ID 和秘密访问密钥。每个存储桶最多可以有两个访问密钥。您可以在应用程序上配置访问密钥，使其可以使用 AWS APIs、和访问您的存储桶及其对象 AWS SDKs。您也可以在 AWS CLI 上配置访问密钥。

有关创建访问密钥的更多信息，请参阅创建存储桶的访问密钥。

资源访问权限

使用资源访问权限为 Lightsail 实例授予对存储桶及其对象的完全读写权限。使用资源访问权限，则您不必管理访问密钥等凭证。要授予实例的访问权限，请将实例附加到同一 AWS 区域中的存储桶。要拒绝访问，请将实例从存储桶中分离。如果您要在实例上将应用程序配置为以编程方式上传和访问存储桶上的文件，则非常适合使用资源访问权限。其中一个用例是将 WordPress 实例配置为在存储桶上存储媒体文件。有关更多信息，请参阅教程：将存储桶连接到您的 WordPress 实例和教程：使用带有内容分发网络分发的存储桶。

有关配置资源访问权限的更多信息，请参阅配置存储桶的资源访问权限。

Amazon S3 屏蔽公共访问权限

使用 Amazon S3 阻止公开访问功能集中限制公众对 Amazon S3 和 Lightsail 中的存储桶的访问。封锁公有访问可以将所有 Amazon S3 和 Lightsail 存储桶设为私有，无论可能配置了何种存储桶和对象权

限。您可以使用 Amazon S3 控制台 AWS SDKs、 AWS CLI 和 REST API 为账户中的所有存储桶（包括 Lightsail 对象存储服务中的存储桶）配置阻止公开访问设置。有关更多信息，请参阅屏蔽对存储桶的公共访问权限。

将文件上传到 Lightsail 对象存储桶

当您将文件上传到 Amazon Lightsail 对象存储服务中的存储桶时，该文件将作为对象存储。对象由文件数据和描述对象的元数据组成。一个存储桶中可以包含任意数量的对象。

您可以将任何类型的文件上传至存储桶，包括映像、备份、数据、电影等。使用 Lightsail 控制台可以上传的最大文件大小为 2 GB。要上传更大的文件，请使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 或。 AWS SDKs

Lightsail 根据您要上传的文件的大小提供以下选项：

- 使用 Lightsail 控制台上传大小不超过 2 GB 的对象 — 使用 Lightsail 控制台，你可以上传一个大小不超过 2 GB 的对象。有关更多信息，请参阅本指南后面的使用 Lightsail 控制台将文件上传到存储桶。
- 使用 AWS SDKs、REST API 通过单个操作上传大小不超过 5 GB 的对象，或者 AWS CLI— 使用单个 PUT 操作，您可以上传大小不超过 5 GB 的单个对象。有关更多信息，请参阅本指南下文中的使用 AWS CLI将文件上传到存储桶。
- 使用 AWS SDKs、REST API 分段上传对象，或者 AWS CLI — 使用分段上传 API，您可以上传一个大小为 5 MB 到 5 TB 的大型对象。分段上传 API 旨在改进大型对象的上传体验。您可以分段上传对象。这些对象分段可以按任何顺序并行独立上传。有关更多信息，请参阅使用分段上传操作将文件上传到存储桶。

有关存储桶的更多信息，请参阅对象存储。

对象键名称和版本控制

使用 Lightsail 控制台上传文件时，文件名将用作对象密钥名称。对象键（或键名称）唯一标识存储在存储桶中的对象。将文件上传到的文件夹（如果有）将用作键名称前缀。例如，如果您将名为 `sailbot.jpg` 的文件上传到存储桶中名为 `images` 的文件夹，则完整的对象键名称和前缀将是 `images/sailbot.jpg`。但是，对象会像 `sailbot.jpg` 在 `images` 文件夹中一样在控制台中显示。有关对象键名称的更多信息，请参阅对象存储桶的键名称。

使用 Lightsail 控制台上传目录时，该目录中的所有文件和子文件夹都将上传到存储桶。然后，Lightsail 会分配一个对象密钥名称，该名称由每个上传的文件名和文件夹名称组合而成。例如，如果您上传一

个名为sample1.jpg且images包含两个文件的文件夹sample2.jpg，Lightsail 会上传这些文件，然后分配相应的密钥名称和。images/sample1.jpg images/sample2.jpg控制台中的对象显示为 images 文件夹中的 sample1.jpg 和 sample2.jpg。

如果您上传的文件包含已存在的键名，并且您的存储桶没有启用版本控制，则新上传的对象将替换上一个对象。但是，如果您的存储桶启用了版本控制，Lightsail 会创建对象的新版本，而不是替换现有对象。有关更多信息，请参阅启用和暂停存储桶中的对象版本控制。

使用 Lightsail 控制台将文件上传到存储桶

完成以下过程，使用 Lightsail 控制台上传文件和目录。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要将文件夹和文件上传到的存储桶的名称。
4. 在对象选项卡中，执行以下操作之一：

   - 将文件和文件夹拖放到对象页面。
   - 选择上传，然后选择文件以上传单个文件，或者选择目录以上传文件夹及其所有内容。

   > **Note**
   >
   > 您还可以通过选择创建新文件夹来创建文件夹。然后，您可以浏览到新文件夹并将文件上传到该文件夹中。

   完成上传后，将显示上传成功消息。

使用 AWS CLI将文件上传到存储桶

完成以下过程，以使用 AWS Command Line Interface （ AWS CLI ）将文件和文件夹上传到存储桶。使用 put-object 命令完成此操作。有关更多信息，请参阅《AWS CLI Command Reference》中的 PutObject。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，您必须为 Lightsail 和 Amazon S3 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以将文件上传到存储桶。

```
aws s3api put-object --bucket BucketName --key ObjectKey --body LocalDirectory --
acl bucket-owner-full-control
```

在该命令中，将以下示例文本替换为自己的文本：

- *BucketName*使用您要将文件上传到的存储桶的名称。
- *ObjectKey*使用存储桶中对象的完整对象密钥。
- *LocalDirectoryFire*其中包含要上传的文件的计算机上的本地目录文件夹路径。

示例：

- 在 Linux 或 Unix 计算机上：

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --
body home/user/Pictures/sailbot.jpg --acl bucket-owner-full-control
```

- 在 Windows 计算机上：

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --
body "C:\Users\user\Pictures\sailbot.jpg" --acl bucket-owner-full-control
```

您会看到类似于以下示例的结果：

```
C:\>aws s3api put-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --body "C:\Users\user\Pictures\sailbot.jpg"
{
    "ETag": "\"694d34edexampled92d64f342aa234c3\""
}
```

为 IPv6仅限请求配置 AWS CLI

Amazon S3 支持通过访问存储桶 IPv6。您可以使用双堆栈终端节点通过 IPv6 Amazon S3 API 调用发出请求。本节提供了如何向双堆栈终端节点发出请求的示例。 IPv6有关更多信息，请参阅 Amazon S3 用户指南中的使用 Amazon S3 双堆栈端点。有关设置的说明 AWS CLI，请参阅配置 AWS Command Line Interface 以与 Amazon Lightsail 配合使用。

> **Important**
>
> 访问存储桶的客户端和网络必须支持使用 IPv6。有关更多信息，请参阅可接通IPv6性。

有两种方法可以从 IPv6仅限实例发出 S3 请求。您可以将配置为 AWS CLI 将所有 Amazon S3 请求定向到指定的 AWS 区域双堆栈终端节点。或者，如果您只想对指定 AWS CLI 命令（不是所有命令）使用双堆栈终端节点，则可以在每个命令中添加 S3 双堆栈终端节点。

配置 AWS CLI

`true`在您的 AWS Config 文件中的配置文件中将配置值`use_dualstack_endpoint`设置为，以将亚马逊 S3 和 s3api AWS CLI 命令发出的所有 Amazon S3 请求定向到指定区域的双栈终端节点。您可以在 AWS CLI 配置文件中指定区域，也可以使用--region 选项在命令中指定区域。

输入以下命令以配置 AWS CLI。

```
aws configure set default.s3.use_dualstack_endpoint true
```

```
aws configure set default.s3.addressing_style virtual
```

将双堆栈端点添加到特定命令中

您可以通过将任何 s3 或 s3api 命令的 `--endpoint-url` 参数设置为 `https://s3.dualstack.`*`aws-region`*`.amazonaws.com` 或 `http://s3.dualstack.`*`aws-region`*`.amazonaws.com` 来对每条命令使用双堆栈端点。在以下示例中，将*`bucketname`*和*`aws-region`*替换为存储桶的名称和您的 AWS 区域。

```
aws s3api list-objects --bucket bucketname --endpoint-url https://s3.dualstack.aws-region.amazonaws.com
```

在 Lightsail 中管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 在 Amazon Lightsail 中封锁存储桶的公开访问权限
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶

- 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
- 在 Amazon Lightsail 中查看存储桶中的对象
- 在 Amazon Lightsail 中复制或移动存储桶中的对象
- 从 Amazon Lightsail 中的存储桶下载对象
- 在 Amazon Lightsail 中筛选存储桶中的对象
- 在 Amazon Lightsail 中标记存储桶中的对象
- 在 Amazon Lightsail 中删除存储桶中的对象

9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

在 Amazon Lightsail 上部署和管理容器

Amazon Lightsail 容器服务是一种高度可扩展的计算和联网资源，您可以在其中部署、运行和管理容器。容器是将代码和依赖关系打包在一起的软件标准单位，这样应用程序就可以从一个计算环境快速可靠地转到另一个计算环境运行。

您可以将 Lightsail 容器服务视为一种计算环境，它允许您使用在本地计算机上创建并推送到服务的映像，或来自在线存储库（例如 Amazon ECR 公共画廊）的图像，在 AWS 基础设施上运行容器。

您还可以通过安装诸如 Docker 之类的软件，在本地计算机上本地运行容器。亚马逊弹性容器服务 (Amazon ECS) 和亚马逊弹性计算云 (A EC2 mazon) 是基础设施中的 AWS 其他资源，您可以在这些资源上运行容器。有关更多信息，请参阅 Amazon ECS 开发人员指南。

内容

- 容器
- Lightsail 容器服务元素
  - Lightsail 容器服务
  - 容器服务容量（规模和功率）
  - 定价
  - 部署
  - 部署版本
  - 容器镜像源
  - 容器服务 ARN
  - 公有端点和默认域
  - 自定义域和 SSL/TLS 证书
  - 容器日志
  - Metrics
- 使用 Lightsail 容器服务

容器

容器是将代码和依赖关系打包在一起的软件标准单位，这样应用程序就可以从一个计算环境快速可靠地转到另一个计算环境运行。您可以在开发环境中运行容器，将其部署到预生产环境中，然后将其部署到

生产环境中。无论您的开发环境是本地机器、预生产环境是数据中心中的物理服务器，抑或您的生产环境是云端的虚拟私有服务器，您的容器都可以可靠地运行。

容器镜像是一种轻型、独立、可执行的软件包，其中包括运行应用程序所需的一切：代码、运行时、系统工具、系统库和设置。容器镜像在运行时成为容器。通过对应用程序及其依赖关系进行容器化，您不再需要担心软件是否在部署软件的操作系统和基础设施中正确运行 — 这样就可以腾出更多的时间来关注代码本身。

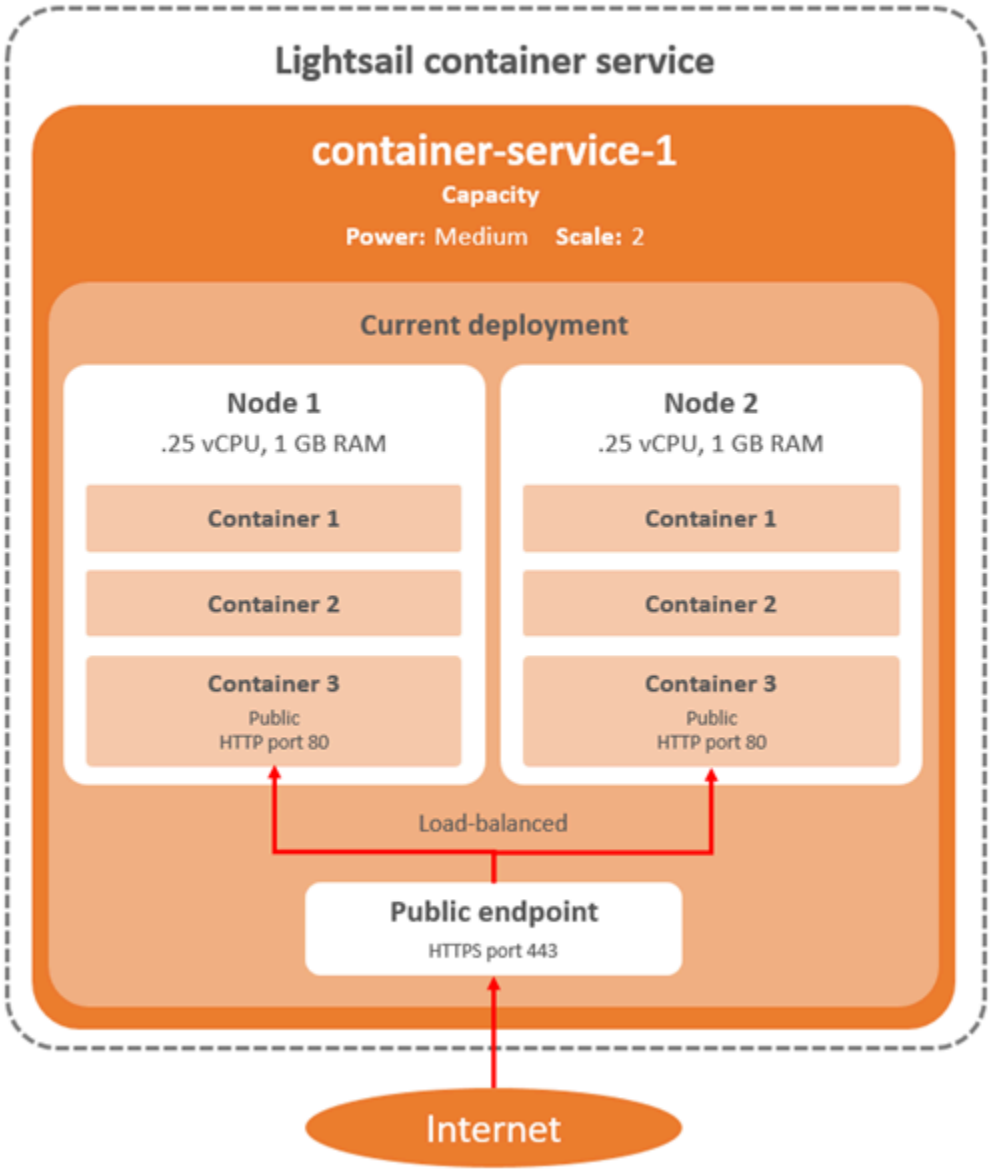
有关容器和容器镜像的更多信息，请参阅中的 Docker 文档中的什么是容器？。

Lightsail 容器服务元素

以下是您在开始使用之前应了解的 Lightsail 容器服务的关键要素。

Lightsail 容器服务

容器服务是 Lightsail 计算资源，你可以在任何可用 Lightsail AWS 区域 的环境中创建该资源。您可以随时创建和删除容器服务。有关更多信息，请参阅创建 Lightsail 容器服务和删除 Ligh tsail 容器服务。



容器服务容量（规模和功率）

首次创建容器服务时，必须选择以下容量参数：

- 规模 — 要在其中运行容器工作负载的计算节点数。您的容器工作负载会在服务的计算节点间复制。最多可以为容器服务指定 20 个计算节点。可以根据您要为服务提供支持的节点数量来选择规模，以实现更高的可用性和更高的容量。容器的流量将在所有节点之间实现负载平衡。
- Power — 容器服务中每个节点的内存和 v CPUs 。你可以选择的功率有 Nano (Na)、Micro (Mi)、Small (Sm)、Medium (Md)、Large (Lg) 和 Xlarge (Xl)，每种功率都有逐渐增加的内存量和 v CPUs。

如果将容器服务的规模指定为大于 1，则容器工作负载将在服务的多个计算节点间复制。例如，如果您的服务规模为 3，功率为 Nano，则您的容器工作负载有三个副本在三个计算资源上运行，每个副本有 512 MB 的 RAM 和 0.25 v CPUs。 传入流量在这三个资源之间进行负载平衡。您为容器服务指定的容量越大，它能够处理的流量就越多。

如果您发现容器服务配置不够，您可以随时动态增加容器服务的功率和规模，而无需任何停机时间；如果您发现容器服务过度配置，则可以减少容器服务的功率和规模。Lightsail 会自动管理容量变化以及您当前的部署。有关更多信息，请参阅更改容器服务的容量。

定价

容器服务的每月价格是通过将其功率价格乘以其计算节点的数量（您的服务规模）来计算的。例如，中功率（价格为 40 美元）且规模为 3 个计算节点的服务每月的费用将为 120 美元。无论您的容器服务是否启用，以及是否有部署，您都需要为容器服务付费。必须删除您的容器服务才能停止向您收费。

每个容器服务（无论其配置的容量是多少）都包含 500 GB 的月度数据传输配额。无论为服务选择什么功率和规模，数据传输配额都不会改变。超出配额的数据传输到互联网将产生超额费用，费用各不相同，起价为每 AWS 区域 GB 0.09美元。从互联网传入的数据超出配额不会产生超额费用。有关更多信息，请参阅 Lightsail 定价页。

部署

您可以在 Lightsail 容器服务中创建部署。部署是您要在服务上启动的容器工作负载的一组规范。

您可以为部署中的每个容器条目指定以下参数：

- 要启动的容器名称
- 用于容器的源容器镜像
- 启动容器时运行的命令
- 应用于容器的环境变量
- 要在容器上打开的网络端口
- 部署中允许通过容器服务的默认域公开访问的容器

> **Note**
>
> 对于每个容器服务，一个部署中只能有一个容器可以设为公开访问。

启动部署后，将会对部署的公有中断节点应用以下运行状况检查参数：

- 执行运行状况检查的目录路径。
- 高级运行状况检查设置，例如间隔（秒）、超时（秒）、成功代码、运行状况阈值和不正常阈值。

您的容器服务一次可以有一个活动部署，一个部署最多可以有 10 个容器条目。您可以在创建容器服务的同时创建部署，也可以在服务启动并运行后创建部署。有关更多信息，请参阅创建和管理容器服务的部署。

部署版本

您在容器服务中创建的每个部署都会保存为一个部署版本。如果修改现有部署的参数，则会将容器重新部署到您的服务中，并且修改后的部署将生成一个新的部署版本。将保存每个容器服务最近的 50 个部署版本。您可以在同一容器服务中使用 50 个部署版本中的任何一个创建新部署。有关更多信息，请参阅创建和管理容器服务的部署。

容器镜像源

创建部署时，必须为部署中的每个容器条目指定源容器镜像。创建部署后，容器服务将从指定的源中提取镜像，并使用它们来创建容器。

您指定的镜像可以来自以下源：

- 公有注册表，如 Amazon ECR Public Gallery 或其他一些公有容器映像注册表。有关 Amazon ECR Public 的更多信息，请参阅《Amazon ECR Public User Guide》中的 What Is Amazon Elastic Container Registry Public?。
- 从本地机器推送到容器服务的镜像。如果您在本地计算机上创建容器镜像，则可以将它们推送到容器服务，以便在创建部署时使用它们。有关更多信息，请参阅创建容器服务映像和推送和管理容器映像。

Lightsail 容器服务支持基于 Linux 的容器镜像。目前不支持基于 Windows 的容器镜像，但你可以在 Windows 上运行 Docker、 AWS Command Line Interface (AWS CLI) 和 Lightsail Control (lightsailctl) 插件来构建基于 Linux 的镜像并将其推送到你的 Lightsail 容器服务。

容器服务 ARN

Amazon 资源名称 (ARNs) 唯一标识 AWS 资源。当您需要在所有资源（例如在 IAM 策略和 API 调用中）中明确指定资源时 AWS，我们需要 ARN。

要获取容器服务的 ARN，请使用 Lightsa GetContainerServices il API 操作，并使用参数指定容器服务的名称。serviceName您的容器服务 ARN 将在该操作的结果中列出，如下例所示。有关更多信息，请参阅GetContainerServices《亚马逊 Lightsail API 参考》。

将会看到类似下面的输出：

```
{
    "containerServices": [
        {
            "containerServiceName": "container-service-1",
            "arn": "arn:aws:lightsail: :111122223333:ContainerService/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "createdAt": "2024-01-01T00:00:00+00:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
        },
        .....
}
```

公有端点和默认域

创建部署时，可以在部署中指定容器条目，该条目将用作容器服务的公有端点。公有端点
容器上的应用程序可通过随机生成的容器服务默认域在互联网上公开访问。默认域的格式为https://*<ServiceName>*.*<RandomGUID>*.*<AWSRegion>*.cs.amazonlightsail.com，其中*<ServiceName>*是您的容器服务的名称，*<RandomGUID>*是您的 Lightsail 账户中随机生成的容器服务的全局唯一标识符，*<AWSRegion>*也是创建容器服务的所在地。 AWS 区域 AWS 区域 Lightsail 容器服务的公共端点仅支持 HTTPS，不支持 TCP 或 UDP 流量。只有一个容器可作为服务的公有端点。因此，请确保选择托管应用程序前端的容器作为公有端点，而其余容器则可以内部访问。

您可以使用容器服务的默认域，也可以使用您自己的自定义域（已注册的域名）。有关将自定义域与容器服务结合使用的更多信息，请参阅启用和管理容器服务的自定义域。

私有域

所有容器服务还有一个私有域，其格式为*<ServiceName>*.service.local，其中*<ServiceName>*是您的容器服务的名称。使用私有域可以从与您的服务位于同一亚马逊云科技区域的另一个 Lightsail 资源访问您的容器服务。如果您没有在服务部署中指定公有端点，则私有域是访问您的容器服务的唯一方式。即使您没有指定公有端点，也会为您的容器服务生成默认域，但会在您尝试浏览它时显示 404 No Such Service 错误消息。

要使用容器服务的私有域访问特定容器，必须指定接受连接请求的容器开放端口。为此，您可以将请求的域格式化为*<ServiceName>*.service.local:*<PortNumber>*，其中*<ServiceName>*是您的容器服务的名称，*<PortNumber>*也是您要连接的容器的开放端口。例如，如果您在名为 container-service-1 的容器服务上创建一个部署，并指定具有开放端口 6379 的 Redis 容器，那么您请求的域应使用格式 *container-service-1*.service.local:*6379*。

自定义域和 SSL/TLS 证书

您最多可以在容器服务中使用 4 个自定义域，而不使用默认域。例如，您可以将自定义域（例如 example.com）的流量引导到部署中标记为公有端点的容器。

要在服务中使用自定义域名，必须先向服务申请SSL/TLS certificate for the domains that you want to use. You must then validate the SSL/TLS certificate by adding a set of CNAME records to the DNS of your domains. After the SSL/TLS certificate is validated, you enable custom domains on your container service by attaching the valid SSL/TLS证书。有关更多信息，请参阅为您的 Lightsail 容器服务创建 SSL/TLS 证书、验证 Lightsail 容器服务的 SSL/TLS 证书，以及为 Lightsail 容器服务启用和管理 Lightsail 容器服务的自定义域。

容器日志

容器服务中的每个容器都会生成一个日志，您可以访问该日志来诊断容器的操作。这些的日志信息包括在容器内运行的 stdout 和 stderr 进程流。有关更多信息，请参阅查看容器服务日志。

Metrics

监控容器服务的指标，以诊断可能由于过度使用而导致的问题。您还可以对指标进行监控，来帮助您确定服务是配置不足还是过度配置。有关更多信息，请参阅查看容器服务指标。

使用 Lightsail 容器服务

以下是管理 Lightsail 容器服务以及将映像从本地计算机推送到服务或使用公共注册表中的容器镜像的一般步骤。

管理 Lightsail 容器服务并在部署中使用容器镜像

1. 在您的 Lightsail 账户中创建容器服务。有关更多信息，请参阅创建 Lightsail 容器服务。
2. 使用以下选项之一将容器镜像与 Lightsail 容器服务配合使用：
   - 使用本地计算机上的容器镜像 — 您可以在本地计算机上安装软件来创建自己的容器镜像，然后将其推送到您的 Lightsail 容器服务。有关更多信息，请参阅以下指南：

    - 安装软件来管理您的 Lightsail 容器服务的容器镜像
    - 为您的 Lightsail 容器服务创建容器镜像
    - 在 Lightsail 容器服务上推送和管理容器镜像
  - 使用公共注册表中的容器镜像 — 您可以从 Amazon ECR 公共图库等公共注册表中查找和使用 Lightsail 容器服务的容器镜像。有关 Amazon ECR 公共库的更多信息，请参阅什么是亚马逊弹性容器注册表公开？ 在 Amazon ECR 公共用户指南中。
3. 安装软件来管理您的 Lightsail 容器服务的容器镜像。
4. 为您的 Lightsail 容器服务创建容器镜像。
5. 在 Lightsail 容器服务上推送和管理容器镜像。
6. 在配置和启动容器的容器服务中创建部署。有关更多信息，请参阅创建和管理您的 Lightsail 容器服务的部署。
7. 查看之前的容器服务部署。您可以使用之前的部署版本来创建新的部署。有关更多信息，请参阅查看和管理 Lightsail 容器服务的部署版本。
8. 查看容器服务的容器日志。有关更多信息，请参阅查看 Lightsail 容器服务的容器日志。
9. 为要与容器搭配使用的域创建 SSL/TLS 证书。有关更多信息，请参阅为您的 L ightsail 容器服务创建 SSL/TLS 证书。
10. 通过向域的 DNS 添加记录来验证 SSL/TLS 证书。有关更多信息，请参阅验证您的 Lightsail 容器服务的 SSL/TLS 证书。
11. 通过将有效的 SSL/TLS 证书附加到容器服务启用自定义域。有关更多信息，请参阅为您的 Lightsail 容器服务启用和管理自定义域。
12. 监控容器服务的利用率指标。有关更多信息，请参阅查看容器服务指标。
13. （可选）通过提高容器服务的指定功率来纵向扩展容量，以及通过提高其指定的规模来横向扩展容量。有关更多信息，请参阅更改 Lightsail 容器服务的容量。
14. 如果未在使用容器服务，请将其删除，以免每月产生费用。有关更多信息，请参阅删除 Lightsail 容器服务。

使用 Lightsail 创建高度可用的容器服务

在本指南中，我们将向您展示如何使用 Lightsail 控制台创建 Amazon Lightsail 容器服务，并描述了您可以配置的容器服务设置。

在开始之前，我们建议您熟悉 Lightsail 容器服务的元素。有关更多信息，请参阅容器服务。

容器服务容量（规模和功率）

首次创建容器服务时，必须选择容器服务的容量。容量由以下参数组合组成：

- 规模 — 要在其中运行容器工作负载的计算节点数。您的容器工作负载会在服务的计算节点间复制。最多可以为容器服务指定 20 个计算节点。可以根据您要为服务提供支持的节点数量来选择规模，以实现更高的可用性和更高的容量。容器的流量将在所有节点之间实现负载平衡。
- Power-容器服务中每个节点的内存和 v CPUs 。你可以选择的功率有 Nano (Na)、Micro (Mi)、Small (Sm)、Medium (Md)、Large (Lg) 和 Xlarge (Xl)；每种功率都有逐渐增加的内存量和 v CPUs。

传入流量在容器服务的规模（计算节点数）上实现负载均衡。例如，具有 Na 功率和规模为 3 的服务将运行 3 个容器工作负载副本。每个节点将有 512 MB 的内存和 0.25 v CPUs。 传入流量将在 3 个节点之间进行负载平衡。您为容器服务选择的容量越大，它能够处理的流量就越多。

如果您发现容器服务配置不够，您可以随时动态增加容器服务的功率和规模，而无需任何停机时间；如果您发现容器服务过度配置，则可以减少容器服务的功率和规模。Lightsail 会自动管理容量变化以及您当前的部署。有关更多信息，请参阅更改 Lightsail 容器服务的容量。

定价

容器服务的每月价格是通过将其功率的基价乘以规模（计算节点的数量）来计算的。例如，一个具有 40 美元中等功率和规模为 3 的服务，每月的费用为 120 美元。

每个容器服务（无论其配置的容量如何）都包含 500 GB 的每月数据传输配额。无论为服务选择什么功率和规模，数据传输配额都不会改变。如果传输到互联网的数据超出配额，将导致超额费用，该费用因亚马逊云科技区域而异，起始价为每 GB 0.09 美元。从互联网传入的数据超出配额不会产生超额费用。有关更多信息，请参阅 Lightsail 定价页。

无论您的容器服务是否启用，以及是否有部署，您都需要为容器服务付费。必须删除您的容器服务才能停止向您收费。有关更多信息，请参阅删除 Lightsail 容器服务。

容器服务节点

容器服务可以处于以下某种状态：

- 待处理 — 正在创建容器服务。
- 就绪 — 您的容器服务正在运行，但没有活动的容器部署。
- 正在部署 — 您的容器服务正在启动部署。

- 正在运行 — 您的容器服务正在运行，且具有活动的容器部署。
- 正在更新 — 正在更新您的容器服务容量或其自定义域。
- 正在删除 — 正在删除容器服务。您选择删除后，您的容器服务将处于此状态，并且仅处于此状态很短的时间。
- 已禁用 — 您的容器服务处于禁用状态，且已关闭其活动部署和容器（如果有）。

容器服务子状态

如果您的容器服务处于正在部署或正在更新状态，则以下附加子状态之一将显示在容器服务状态下面：

- 正在创建系统资源 - 正在创建容器服务的系统资源。
- 正在创建网络基础设施 - 正在创建容器服务的网络基础设施。
- 正在预置证书 - 正在创建容器服务的 SSL/TLS 证书。
- 正在预置服务 - 正在预置您的容器服务。
- 正在创建部署 - 正在您的容器服务中创建您的部署。
- 正在评估运行状况检查 - 正在评估部署的运行状况。
- 正在激活部署 - 正在激活您的部署。

如果您的容器服务处于待处理状态，则以下附加子状态之一将显示在容器服务状态下面：

- 超出证书限制 - 容器服务所需的 SSL/TLS 证书超出账户允许的最大证书数量。
- 未知错误 - 创建容器服务时出现错误。

创建容器服务

完成以下步骤以创建 Lightsail 容器服务。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择创建容器服务。
4. 在创建容器服务页面中，选择更改 AWS 区域，然后 AWS 区域 为您的容器服务选择一个。
5. 选择容器服务的容量。有关更多信息，请参阅本指南的容器服务容量（规模和功率）部分。
6. 请完成以下步骤以创建部署，该部署将在创建容器服务的同时启动。否则，请跳到步骤 7 以创建没有部署的容器服务。

如果您计划使用公有注册表中的容器镜像，请创建具有部署的容器服务。否则，如果您计划使用本地机器上的容器镜像，则创建没有部署的服务。在服务启动并运行后，您可以将容器镜像从本地机器推送到容器服务。然后，可以使用已注册到容器服务的已推送容器镜像创建部署。

a. 选择创建部署。

b. 请选择以下选项之一：

- 选择示例部署 — 选择此选项可使用由 Lightsail 团队精心策划的容器映像以及一组预先配置的部署参数来创建部署。此选项提供了在容器服务中启动并运行常见容器的最快、最简单的方法。
- 指定自定义部署 — 选择此选项可通过指定所选容器来创建部署。

将打开部署表单视图，您可以在其中输入新的部署参数。

c. 输入部署的参数。有关您可以指定的部署参数的更多信息，请参阅 Lightsail 容器服务创建和管理部署指南中的部署参数部分。

d. 选择添加容器条目以将多个容器条目添加到您的部署。部署中最多可拥有 10 个容器条目。

e. 在输入部署参数后，选择保存并部署以在容器服务中创建部署。

7. 输入容器服务的名称。

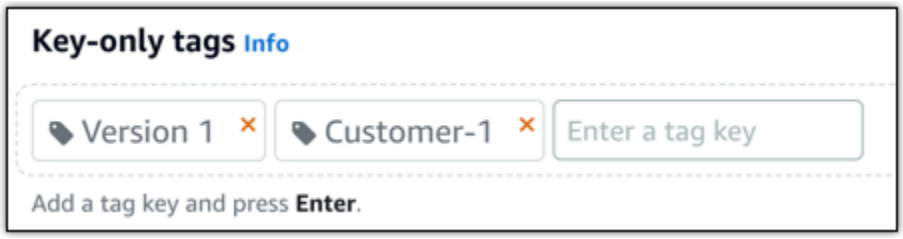
容器服务名称：

- 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
- 必须包含 2 到 63 个字符。
- 只能包含字母数字字符和连字符。
- 连字符 (-) 可以分隔字词，但不能位于名称的开头或结尾。

> **Note**
>
> 您指定的名称将成为容器服务默认域名的一部分（公众可见）。

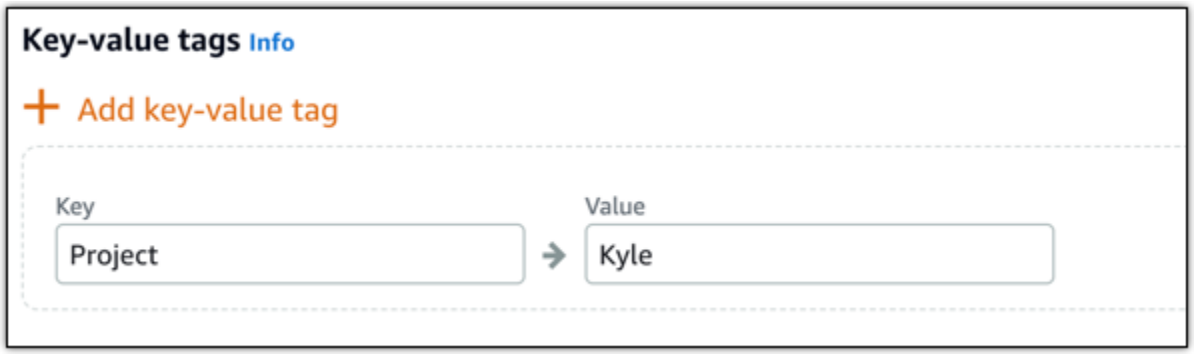
8. 选择以下选项之一，以将标签添加到容器服务：

- Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。



- 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

  一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。



> **Note**
>
> 有关“仅键”标签和键值标签的更多信息，请参阅标签。

9. 选择创建容器服务。

   将重新导向到新容器服务的管理页面。正在创建时，新容器服务的状态为待处理。稍等片刻，服务的状态将更改为就绪（如果它没有当前部署），或更改为正在运行（如果您创建了部署）。

为 Lightsail 容器服务构建和测试 Docker 镜像

通过 Docker，您可以构建、运行、测试和部署基于容器的分布式应用程序。Amazon Lightsail 容器服务使用部署中的 Docker 容器镜像来启动容器。

在本指南中，我们将介绍如何使用 Docker 文件在本地机器上创建容器镜像。创建镜像后，您可以将其推送到 Lightsail 容器服务以进行部署。

要完成本指南中的步骤，您应基本了解 Docker 是什么及其工作方式。有关 Docker 的更多信息，请参阅 Docker 是什么？和 Docker 概述。

内容

- 步骤 1：完成先决条件
- 步骤 2：创建 Docker 文件并构建容器镜像
- 步骤 3：运行新容器镜像
- （可选）步骤 4：清除本地机器上运行的容器
- 创建容器镜像后的后续步骤

步骤 1：完成先决条件

在开始之前，您必须安装创建容器所需的软件，然后将其推送到 Lightsail 容器服务。例如，您必须安装并使用 Docker 来创建和构建容器镜像，然后便可以用于您的 Lightsail 容器服务。有关更多信息，请参阅 。安装软件以管理 Amazon Lightsail 容器服务的容器镜像。

步骤 2：创建 Docker 文件并构建容器镜像

完成以下过程以创建 Docker 文件并用其构建 `mystaticwebsite` Docker 容器镜像。容器映像将用于在 Ubuntu 的 Apache Web 服务器上托管的简单静态网站。

1. 在本地机器上创建 `mystaticwebsite` 文件夹，以在其中存储 Docker 文件。
2. 在您刚创建的文件夹中创建 Docker 文件。

   Docker 文件不使用文件扩展名，例如 `.TXT`。完整文件名为 `Dockerfile`。
3. 根据您希望如何配置容器镜像，复制以下代码块之一，并将其粘贴到 Docker 文件中：

   - 如果您想创建一个包含 Hello World 消息的简单静态网站容器镜像，则复制以下代码块并将其粘贴到 Docker 文件中。此代码示例使用 Ubuntu 18.04 镜像。`RUN` 指令更新程序包缓存，并安装和配置 Apache，然后将 Hello World 消息打印到 Web 服务器的文档根目录。`EXPOSE` 指令在容器上公开端口 80，`CMD` 指令启动 Web 服务器。

     ```
     FROM ubuntu:18.04

     # Install dependencies
     RUN apt-get update && \
      apt-get -y install apache2

     # Write hello world message
     RUN echo 'Hello World!' > /var/www/html/index.html
     ```

```
# Open port 80
EXPOSE 80

# Start Apache service
CMD ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
```

- 如果您想为静态网站容器镜像使用您自己的 HTML 文件集，请在存储 Docker 文件的相同文件夹中创建 `html` 文件夹。然后把您的 HTML 文件放在该文件夹中。

  在您的 HTML 文件位于 `html` 文件夹中之后，复制以下代码块并将其粘贴到 Docker 文件中。此代码示例使用 Ubuntu 18.04 镜像。`RUN` 指令更新程序包缓存，并安装和配置 Apache。`COPY` 指令将 html 文件夹的内容复制到 Web 服务器的文档根目录。`EXPOSE` 指令在容器上公开端口 80，`CMD` 指令启动 Web 服务器。

  ```
  FROM ubuntu:18.04

  # Install dependencies
  RUN apt-get update && \
   apt-get -y install apache2

  # Copy html directory files
  COPY html /var/www/html/

  # Open port 80
  EXPOSE 80

  CMD ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
  ```

4. 打开命令提示符或终端窗口，然后将目录更改为要存储 Docker 文件的文件夹。
5. 输入以下命令以使用文件夹中的 Docker 文件构建容器镜像。此命令将构建一个名为 `mystaticwebsite` 的新 Docker 容器镜像。

   ```
   docker build -t mystaticwebsite .
   ```

   您应该看到一条确认镜像已成功构建的消息。
6. 输入以下命令以查看本地机器上的容器镜像。

   ```
   docker images --filter reference=mystaticwebsite
   ```

您应看到类似于以下示例的结果，其中显示新创建的容器镜像。

```
C:\Users\[redacted]\Documents\Docker\Dockerfiles\mystaticwebsite>docker images --filter reference=mystaticwebsite
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
mystaticwebsite     latest              8f7ffd1013e0        8 minutes ago       199MB
```

您新构建的容器镜像已准备好进行测试，可使用它在本机计算机上运行新容器。继续本指南的下一部分步骤 3：运行新容器镜像。

步骤 3：运行新容器镜像

完成以下步骤以运行您创建的新容器镜像。

1. 在命令提示符或终端窗口中，输入以下命令以运行您之前在本指南的步骤 2：创建 Docker 文件并构建容器镜像部分中构建的容器镜像。`-p 8080:80` 选项将容器上公开的端口 80 映射到本地机器上的端口 8080。`-d` 选项指定容器应在分离模式下运行。

   ```
   docker container run -d -p 8080:80 --name mystaticwebsite mystaticwebsite:latest
   ```

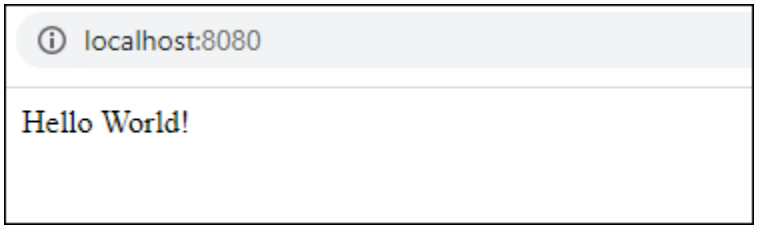
2. 输入以下命令以查看正在运行的容器。

   ```
   docker container ls -a
   ```

   您应看到类似于以下示例的结果，其中显示新运行的容器。

   ```
   C:\Users\[redacted]\Documents\Docker\Dockerfiles\mystaticwebsite>docker container ls -a
   CONTAINER ID        IMAGE                     COMMAND                  CREATED             STATUS              PORTS                    NAMES
   62382081e06b        mystaticwebsite:latest    "/bin/sh -c /root/ru…"   6 minutes ago       Up 6 minutes        0.0.0.0:8080->80/tcp     mystaticwebsite
   ```

3. 要确认容器已启动并正在运行，请打开一个新的浏览器窗口并浏览到 `http://localhost:8080`。您应看到类似于以下示例的消息。这确认您的容器已启动并在本地机器上运行。

您新构建的容器镜像已准备好被推送到您的 Lightsail 账户，以便您可以将其部署到 Lightsail 容器服务。有关更多信息，请参阅在 Amazon Lightsail 服务中推送和管理容器镜像。

（可选）步骤 4：清除本地机器上运行的容器

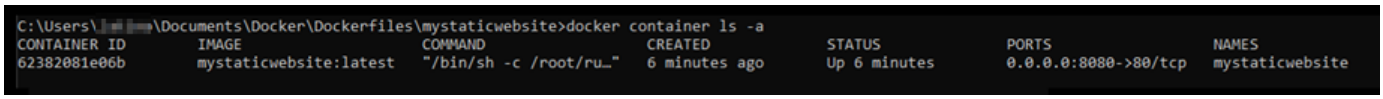
既然您已经创建了可以推送到 Lightsail 容器服务的容器镜像，按照本指南中的步骤，现在可以清除本地机器上运行的容器。

完成以下步骤以清除本地计算机上运行的容器：

1. 运行以下命令以查看本地机器上运行的容器。

   ```
   docker container ls -a
   ```

   您应该看到类似下面的结果，其中列出了本地计算机上运行的容器的名称。

2. 运行以下命令可删除之前在本指南中创建的运行中容器。这会强制停止容器，并永久删除容器。

   ```
   docker container rm <ContainerName> --force
   ```

   在命令中，将 < ContainerName > 替换为要停止的容器的名称，然后将其删除。

   示例：

   ```
   docker container rm mystaticwebsite --force
   ```

   现在可以删除据本指南创建的容器。

创建容器镜像后的后续步骤

创建容器镜像后，在准备部署容器镜像时将其推送到 Lightsail 容器服务。有关更多信息，请参阅管理 Lightsail 容器服务镜像。

主题

- 推送、查看和删除 Lightsail 容器服务的容器镜像
- 安装 Docker 和容器的 Lightsail Control 插件 AWS CLI
- 授予 Lightsail 容器服务访问亚马逊 ECR 私有存储库的权限

推送、查看和删除 Lightsail 容器服务的容器镜像

在 Amazon Lightsail 容器服务中创建部署时，必须为每个容器条目指定源容器镜像。您可以使用 Amazon ECR Public Gallery 等公有注册表中的映像，也可以使用您在本地计算机上创建的映像。在本指南中，我们将介绍如何将容器镜像从本地机器推送到 Lightsail 容器服务。有关创建容器映像的更多信息，请参阅创建容器服务映像。

内容

- 先决条件
- 将容器镜像从本地机器推送到容器服务
- 查看存储在容器服务中的容器镜像
- 查看存储在容器服务中的容器镜像

先决条件

在开始将容器镜像推送到容器服务之前，请完成以下先决条件：

- 在您的 Lightsail 账户中创建容器服务。有关更多信息，请参阅创建 Amazon Lightsail 容器服务。
- 在本地机器上安装软件，您需要创建自己的容器镜像，并将其推送到 Lightsail 容器服务。有关更多信息，请参阅安装软件以管理 Amazon Lightsail 容器服务的容器镜像。
- 在本地机器上创建镜像，您可以将其推送到 Lightsail 容器服务。有关更多信息，请参阅创建 Amazon Lightsail 容器服务的容器镜像。

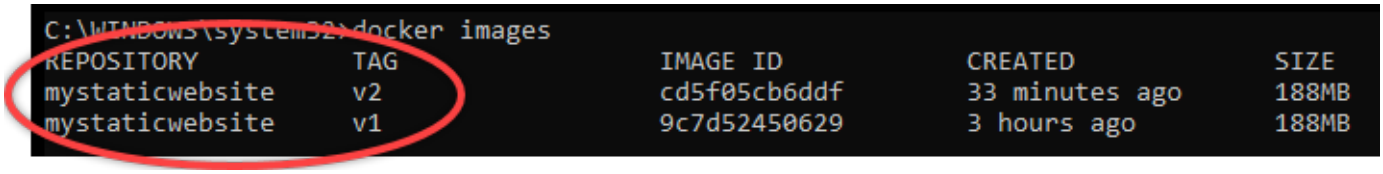
将容器镜像从本地机器推送到容器服务

完成以下过程，将容器镜像推送到容器服务。

1. 打开命令提示符或终端窗口。
2. 在命令提示符或终端窗口中，输入以下命令以查看当前位于本地机器上的 Docker 镜像。

   ```
   docker images
   ```

3. 在结果中，找到要推送到容器服务的容器镜像的名称（存储库名称）和标签。请记下这些信息，因为需要在下一步中用到。



4. 输入以下命令以将本地机器上的容器镜像推送到容器服务。

```
aws lightsail push-container-image --region <Region> --service-
name <ContainerServiceName> --label <ContainerImageLabel> --
image <LocalContainerImageName>:<ImageTag>
```

在该命令中，将：

- *<Region>*使用创建容器服务的 AWS 区域。
- *<ContainerServiceName>*使用您的容器服务的名称。
- *<ContainerImageLabel>*带有您要在容器镜像存储在容器服务上时为其提供的标签。指定描述性标签，可用于跟踪不同版本的注册容器镜像。

  标签将成为容器服务生成的容器镜像名称的一部分。例如，如果容器服务名称为 container-service-1，容器镜像标签为 mystaticsite，且这是您要推送的容器镜像的第一个版本，那么容器服务生成的图像名称将是 :container-service-1.mystaticsite.1。
- *<LocalContainerImageName>*使用您要推送到容器服务的容器镜像的名称。您在此过程的上一步中获取了容器镜像名称。
- *<ImageTag>*带有您要推送到容器服务的容器镜像的标签。您在此过程的上一步中获取了容器镜像标签。

例如：

```
aws lightsail push-container-image --region us-west-2 --service-name myservice --
label mystaticwebsite --image mystaticwebsite:v2
```

您应该看到类似于以下示例的结果，其中确认您的容器镜像已推送到容器服务。

```
C:\WINDOWS\system32>aws lightsail push-container-image --service-name myservice --label mystaticwebsite
--image mystaticwebsite:v2

[1B5a355b95: Preparing
[1B0994b087: Preparing
[1B0c904ff3: Preparing
[1B370aa736: Preparing
[1Bf192bbc8: Preparing
[1Bbc0bd923: Preparing
[7BDigest: sha256:3a585ca39bba342e390b39f2fea00bbc20f492c0cda7b923dd766abe31918f3bB/1.96kB
Image "mystaticwebsite:v2" registered.
Refer to this image as ":myservice.mystaticwebsite.2" in deployments.
```

请参阅本指南的以下部分查看存储在容器服务中的容器镜像，在 Lightsail 控制台上查看容器服务中已推送的容器镜像。

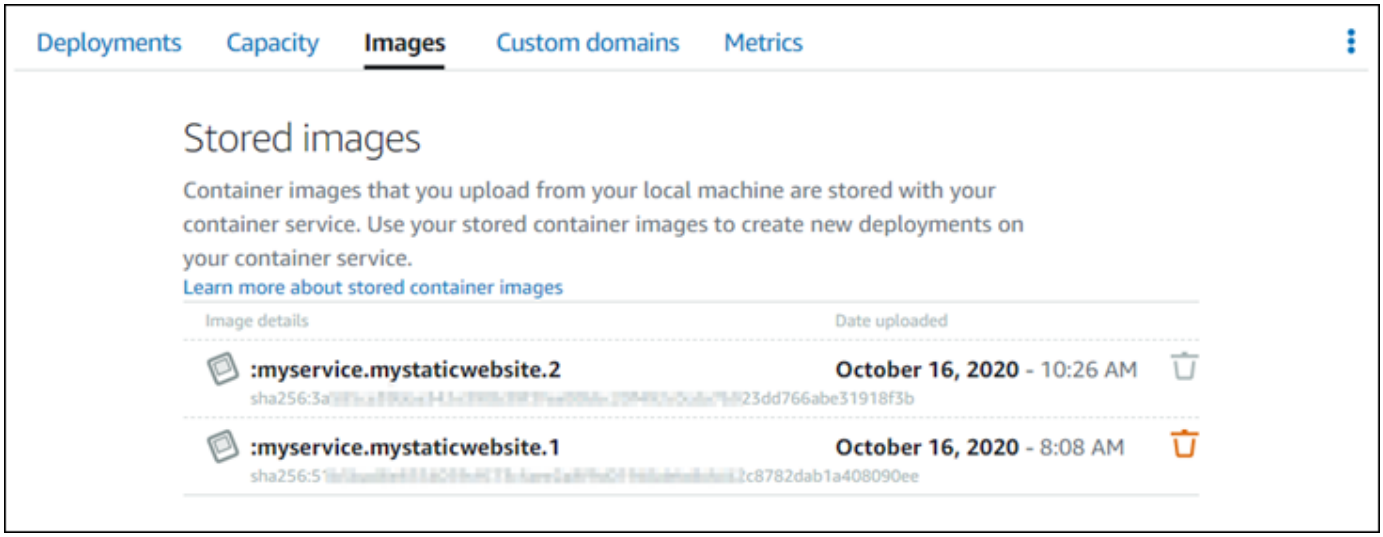
查看存储在容器服务中的容器镜像

请完成以下过程，查看容器服务中已推送和已存储的容器镜像。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择要查看其存储容器镜像的容器服务的名称。
4. 在容器服务管理页面中，选择镜像选项卡。

> **Note**
>
> 如果尚未将镜像推送到容器服务，则不会显示镜像选项卡。要显示容器服务的镜像选项卡，必须首先将容器镜像推送到服务。

镜像页面列出了已推送到容器服务且当前存储在服务中的容器镜像。无法删除当前部署中正在使用的容器镜像，其使用灰色删除图标列出。



您可以使用存储在服务中的容器镜像创建部署。有关更多信息，请参阅“创建和管理 Amazon Lightsail 容器服务的部署”。

查看存储在容器服务中的容器镜像

请完成以下过程，删除容器服务中已推送和已存储的容器镜像。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择要查看其当前部署的容器服务的名称。
4. 在容器服务管理页面中，选择镜像选项卡。

> **Note**
>
> 如果尚未将镜像推送到容器服务，则不会显示镜像选项卡。要显示容器服务的镜像选项卡，必须首先将容器镜像推送到服务。

5. 找到要删除的容器镜像，然后选择 删除图标（垃圾桶图标）。

> **Note**
>
> 无法删除当前部署中正在使用的容器镜像，其删除图标为灰色。

6. 在出现的确认提示中，选择是，请删除以确认您要永久删除存储的镜像。

您存储的容器镜像将立即从容器服务中删除。

安装 Docker 和容器的 Lightsail Control 插件 AWS CLI

您可以使用 Amazon Lightsail 控制台创建 Lightsail 容器服务，并使用来自在线公共注册表（例如 Amazon ECR 公共图库）的容器映像创建部署。要创建自己的容器镜像并将其推送到您的容器服务，则必须在您计划创建容器镜像的同一台计算机上安装以下附加软件：

- Docker — 运行、测试和创建自己的容器镜像，然后您可以将其与 Lightsail 容器服务一起使用。
- AWS Command Line Interface (AWS CLI) — 指定您创建的容器镜像的参数，然后将其推送到您的 Lightsail 容器服务。2.1.1 及更高版本将与 Lightsail Control 插件配合使用。
- Lightsail Control (lightsailctl) 插件 — AWS CLI 允许访问本地计算机上的容器镜像。

本指南的以下章节介绍了可从何处下载这些软件包以及如何进行安装。有关容器服务的更多信息，请参阅容器服务。

内容

- 安装 Docker
- 安装 AWS CLI
- 安装 Lightsail 控制插件
  - 在 Windows 上安装 lightsailctl 插件
  - 在 macOS 上安装 lightsailctl 插件
  - 在 Linux 上安装 lightsailctl 插件

安装 Docker

Docker 技术可以构建、运行、测试和部署基于 Linux 容器的分布式应用程序。如果您想创建自己的容器镜像，然后将其与 Lightsail 容器服务一起使用，则必须安装和使用 Docker 软件。有关更多信息，请参阅为您的 Lightsail 容器服务创建容器镜像。

Docker 适用于许多不同的操作系统，包括大多数现代 Linux 分发版 (如 Ubuntu) 甚至 MacOS 和 Windows。有关如何在特定的操作系统上安装 Docker 的更多信息，请参阅 Docker 安装指南。

> **Note**
>
> 务必安装最新版本的 Docker。不保证旧版本的 Docker 可以与本指南后面介绍的 Lightsail C AWS CLI ontrol (lightsailctl) 插件配合使用。

安装 AWS CLI

AWS CLI 是一款开源工具，可让您使用命令行外壳中的命令与 Lightsail 等 AWS 服务进行交互。您必须安装并使用将您在本地计算机上创建的容器映像推送 AWS CLI 到您的 Lightsail 容器服务。

AWS CLI 有以下版本可用：

- 版本 2.x – 目前最新的 AWS CLI版本。这是的最新主要版本，支持所有最新功能 AWS CLI ，包括能够将容器映像推送到 Lightsail 容器服务。2.1.1 及更高版本将与 Lightsail Control 插件配合使用。
- 版本 1.x — 以前版本可用于向后兼容。 AWS CLI 此版本不支持将您的容器镜像推送到 Lightsail 容器服务。因此，您必须改为安装 AWS CLI 版本 2。

AWS CLI 版本 2 可用于 Linux、macOS 和 Windows 操作系统。有关如何在这些操作系统 AWS CLI 上安装的说明，请参阅《AWS CLI 用户指南》中的安装 AWS CLI 版本 2。

安装 Lightsail 控制插件

Lightsail Control (lightsailctl) 插件是一款轻量级应用程序， AWS CLI 允许访问您在本地计算机上创建的容器镜像。它允许您将容器映像推送到 Lightsail 容器服务，以便可以将它们部署到您的服务中。

系统要求

- 支持 64 位的 Windows、macOS 或 Linux 操作系统。
- AWS CLI 要使用 lightsailctl 插件，必须将版本 2 安装在本地计算机上。有关更多信息，请参阅本指南前面介绍的安装 AWS CLI一节。

使用最新版本的 lightsailctl 插件

此插件会不时更新，已提供增强功能。每次使用 lightsailctl 插件时，它都会检查确认您使用的是最新版本。如果发现可用的新版本，则会提示您更新到最新版本以利用最新功能。发布更新版本时，您必须重复安装过程以获取最新版本的 lightsailctl 插件。

下表列出了 lightsailctl 插件的所有版本，以及每个版本所含的功能和增强功能。

- v1.0.0（2020 年 11 月 12 日发布）— 初始版本为 AWS CLI 版本 2 增加了将容器映像推送到 Lightsail 容器服务的功能。

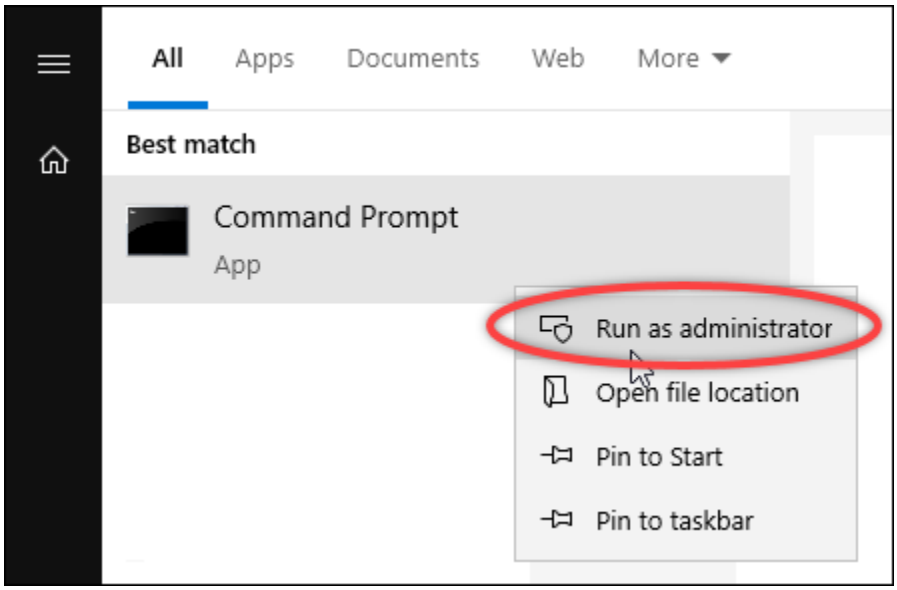
在 Windows 上安装 lightsailctl 插件

请完成以下过程以在 Windows 上安装 lightsailctl 插件。

1. 通过以下 URL 下载可执行文件，并将其保存到 `C:\Temp\lightsailctl\` 目录中。

```
https://s3.us-west-2.amazonaws.com/lightsailctl/latest/windows-amd64/
lightsailctl.exe
```

2. 选择 Windows 开始按钮，然后搜索 cmd。
3. 在搜索结果中，右键单击 Command Prompt (命令提示符) 应用程序并选择 Run as administrator (以管理员身份运行)。



> **Note**
>
> 您可能会看到一个提示，询问你是否要允许命令提示符对你的设备进行更改。您必须选择 Yes（是）以继续安装。

4. 输入以下命令以设置路径环境变量，该变量指向您保存 lightsailctl 插件的 `C:\Temp\lightsailctl\` 目录。

```
setx PATH "%PATH%;C:\Temp\lightsailctl" /M
```

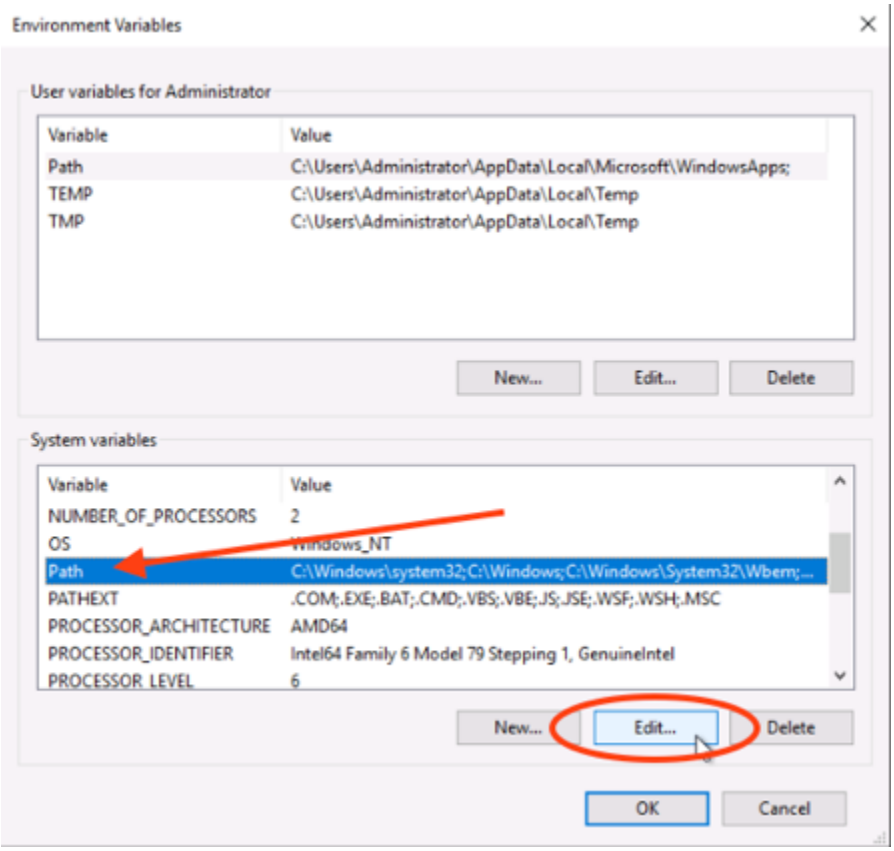
您应看到类似于以下示例的结果。

```
C:\WINDOWS\system32>setx PATH "%PATH%;C:\Temp\lightsailctl\" /M

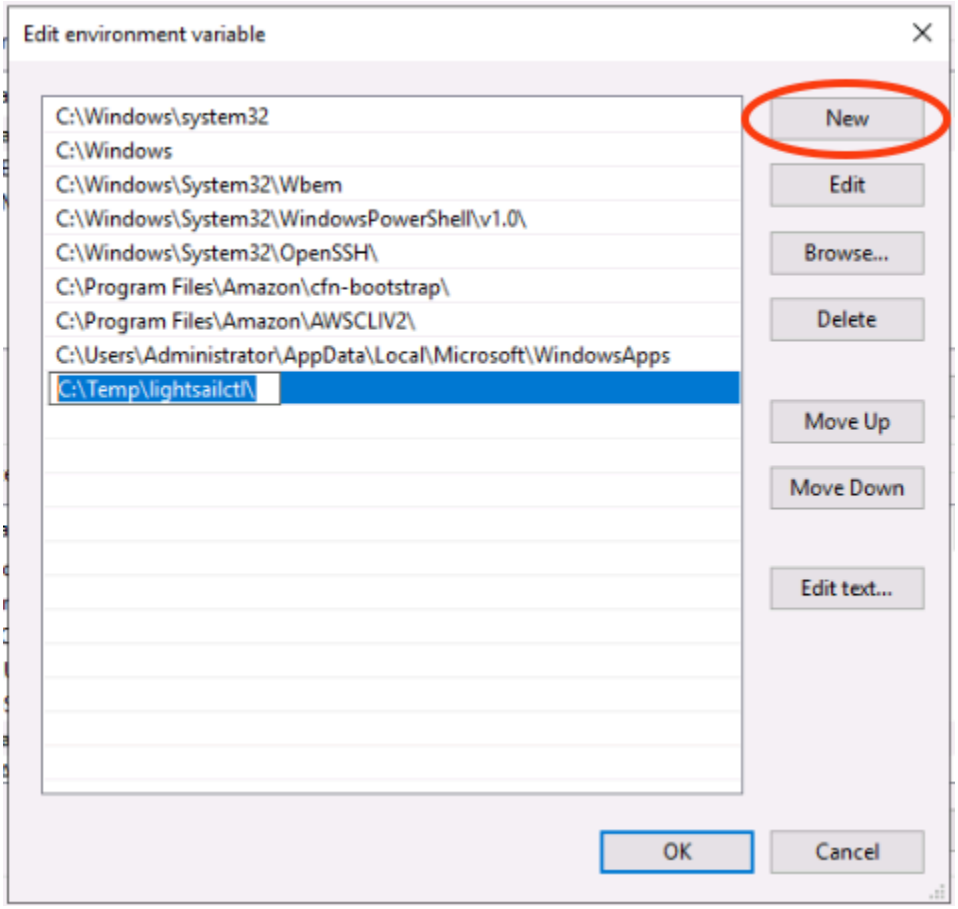
SUCCESS: Specified value was saved.
```

`setx` 命令将在超过 1024 个字符截断文本。如果您已经在 PATH 中设置了多个变量，请使用以下步骤手动设置路径环境变量。

1. 在 Start（开始）菜单上，打开 Control Panel（控制面板）。
2. 选择 System and Security（系统与安全），然后选择 System（系统）。
3. 选择高级系统设置。
4. 在 System Properties（系统属性）对话框的 Advanced（高级）选项卡中，选择 Environment Variables（环境变量）。
5. 在 Environment Variables（环境变量）对话框的 System Variables（系统变量）框中，选择 Path（路径）。
6. 选择 System Variables（系统变量）对话框下的 Edit（编辑）按钮。



7. 选择 New（新建），然后输入以下路径：C:\Temp\lightsailctl\



8. 在接下来的三个对话框中选择 OK（确定），然后关闭 System（系统）对话框。

现在，您可以使用 AWS Command Line Interface (AWS CLI) 将容器镜像推送到您的 Lightsail 容器服务了。有关更多信息，请参阅推送和管理容器映像。

在 macOS 上安装 lightsailctl 插件

请完成以下其中一个过程，在 Windows 上下载并安装 lightsailctl 插件。

Homebrew 下载和安装

1. 打开终端窗口。
2. 输入以下命令以下载并安装 lightsailctl 插件。

```
brew install aws/tap/lightsailctl
```

> **Note**
>
> 有关 Homebrew 的更多信息，请参阅 Homebrew 网站。

手动下载和安装

1. 打开终端窗口。
2. 输入以下命令以下载 lightsailctl 插件并将其复制到 bin 文件夹。

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/darwin-amd64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. 输入以下命令以构建可执行的插件。

```
chmod +x /usr/local/bin/lightsailctl
```

4. 输入以下命令以清除插件的扩展属性。

```
xattr -c /usr/local/bin/lightsailctl
```

现在，您可以使用将容器镜像推送 AWS CLI 到您的 Lightsail 容器服务了。有关更多信息，请参阅推送和管理容器映像。

在 Linux 上安装 lightsailctl 插件

完成以下过程，在 Linux 上安装 Lightsail 容器服务插件。

1. 打开终端窗口。
2. 输入以下命令以下载 lightsailctl 插件。

   - 对于 AMD 64 位架构版本的插件：

   ```
   curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-amd64/
   lightsailctl" -o "/usr/local/bin/lightsailctl"
   ```

   - 对于 ARM 64 位架构版本的插件：

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-arm64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. 输入以下命令以构建可执行的插件。

```
sudo chmod +x /usr/local/bin/lightsailctl
```

现在，您可以使用将容器镜像推送 AWS CLI 到您的 Lightsail 容器服务了。有关更多信息，请参阅推送和管理容器映像。

授予 Lightsail 容器服务访问亚马逊 ECR 私有存储库的权限

Amazon Elastic Container Registry (Amazon ECR) AWS 是一项托管容器镜像注册服务，它使用 (IAM) 支持具有基于资源的权限 AWS Identity and Access Management 的私有存储库。您可以授予您的 Amazon Lightsail 容器服务访问您的 Amazon ECR 私有存储库的权限。 AWS 区域然后，您可以将映像从私有存储库部署到容器服务。

您可以使用 Lightsail 控制台或 () 来管理 Lightsail 容器服务和 Amazon ECR 私有存储库的访问权限。AWS Command Line Interface AWS CLI但是，我们建议您使用 Lightsail 控制台，因为它可以简化流程。

有关容器服务的更多信息，请参阅容器服务。有关 Amazon ECR 的更多信息，请参阅 Amazon ECR 用户指南。

内容

- 所需权限
- 使用 Lightsail 控制台管理对私有仓库的访问权限
- 使用来管理 AWS CLI 对私有仓库的访问权限
  - 激活或停用 Amazon ECR 映像拉取器 IAM 角色
  - 确定您的 Amazon ECR 私有存储库是否有策略语句
    - 将策略添加到没有策略语句的私有存储库
    - 将策略添加到有策略语句的私有存储库

所需的权限

负责管理 Lightsail 容器服务对 Amazon ECR 私有存储库的访问权限的用户必须在 IAM 中拥有以下权限策略之一。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的添加和删除 IAM 标识权限。

授予对任何 Amazon ECR 私有存储库的访问权限

以下权限策略向用户授予配置对任何 Amazon ECR 私有存储库的访问的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:*:AwsAccountId:repository/*"
        }
    ]
}
```

在政策中，*AwsAccountId*替换为您的 AWS 账号。

授予对特定 Amazon ECR 私有存储库的访问权限

以下权限策略向用户授予在特定 AWS 区域中配置对特定 Amazon ECR 私有存储库的访问的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
```

```
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:AwsRegion:AwsAccountId:repository/RepositoryName"
        }
    ]
}
```

在该策略中，将以下示例文本替换为自己的文本：

- *AwsRegion*— 私有存储库的 AWS 区域 代码（例如us-east-1）。您的 Lightsail 容器服务必须与您要访问 AWS 区域 的私有存储库位于同一个存储库中。
- *AwsAccountId*— 您的 AWS 账号。
- *RepositoryName*— 您要管理其访问权限的私有存储库的名称。

以下是使用示例值填充的权限策略的示例。

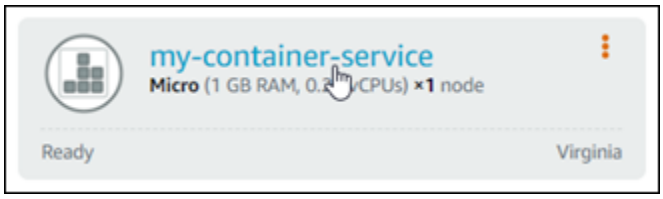
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/my-private-repo"
        }
    ]
}
```

使用 Lightsail 控制台管理对私有仓库的访问权限

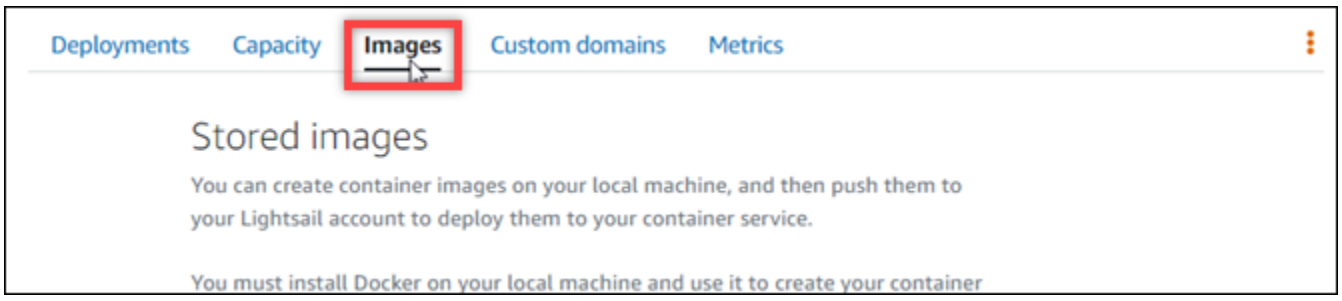
完成以下过程，使用 Lightsail 控制台管理 Lightsail 容器服务对 Amazon ECR 私有存储库的访问权限。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。

3. 选择您想要为其配置对 Amazon ECR 私有存储库的访问权限的容器服务的名称。

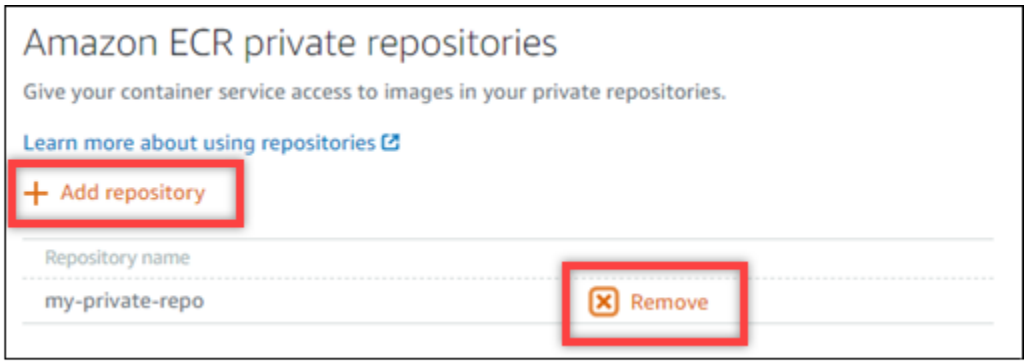


4. 选择映像选项卡。

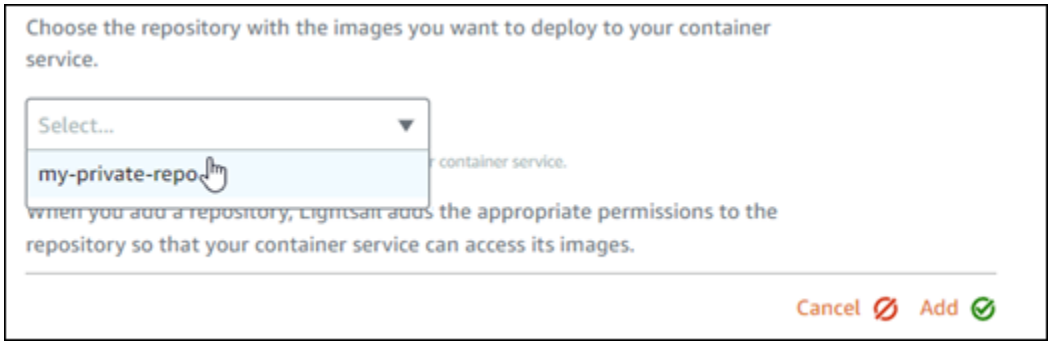


5. 选择添加存储库以授予您的容器服务访问 Amazon ECR 私有存储库的权限。

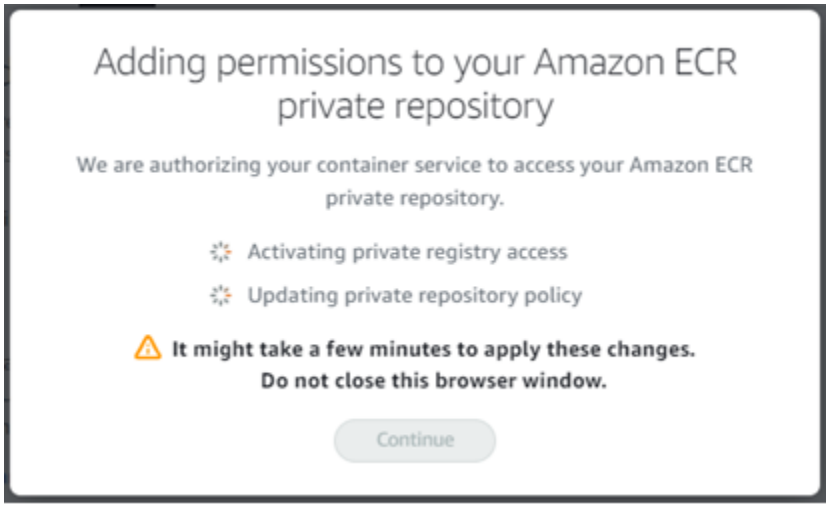
> **Note**
>
> 您可以选择删除以从先前添加的 Amazon ECR 私有存储库中删除容器服务的访问权限。



6. 在出现的下拉菜单中，选择要访问的私有存储库，然后选择 Add（添加）。

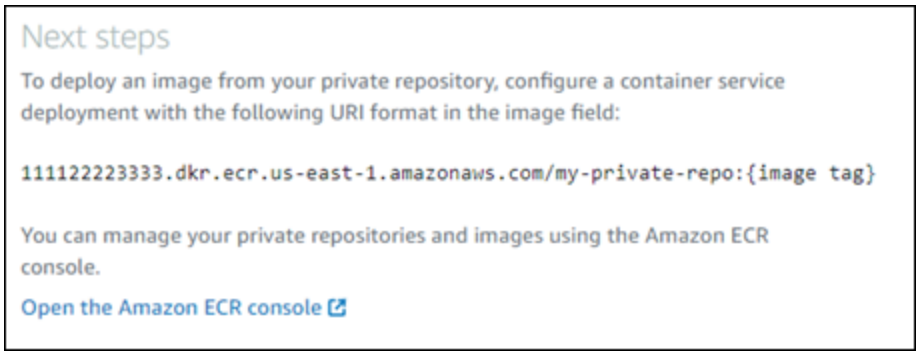


Lightsail 花点时间为您的容器服务激活 Amazon ECR 图像提取器 IAM 角色，其中包括主要的亚马逊资源名称 (ARN)。然后，Lightsail 会自动将 IAM 角色委托人 ARN 添加到您选择的 Amazon ECR 私有存储库的权限策略中。这将授予容器服务对私有存储库及其映像的访问权限。在出现的模式表明该过程已完成之前，不要关闭浏览器窗口，您可以选择 Continue（继续）。



7. 在激活完成时选择 Continue（继续）。

添加选择的 Amazon ECR 私有存储库后，它将列在页面的 Amazon ECR 私有存储库部分。该页面包含有关如何将镜像从私有存储库部署到 Lightsail 容器服务的说明。要使用私有存储库中的映像，请在创建容器服务部署时将页面上显示的 URI 格式指定为 Image（映像）值。在您指定的 URI 中，将示例*{image tag}*替换为要部署的映像的标签。有关更多信息，请参阅创建和管理容器服务的部署。



使用来管理 AWS CLI 对私有仓库的访问权限

使用 AWS Command Line Interface (AWS CLI) 管理 Lightsail 容器服务对 Amazon ECR 私有存储库的访问权限需要执行以下步骤：

> **Important**
>
> 我们建议您使用 Lightsail 控制台来管理 Lightsail 容器服务对 Amazon ECR 私有存储库的访问权限，因为它可以简化流程。有关更多信息，请参阅本指南前面的“使用 Lightsail 控制台管理私有仓库的访问权限”。

1. 激活或停用 Amazon ECR 图像提取器 IAM 角色 — 使用 Lightsail AWS CLI `update-container-service` 的命令激活或停用 Amazon ECR 图像提取器 IAM 角色。当您激活 Amazon ECR 映像拉取器 IAM 角色时，会为该角色创建一个主体 Amazon 资源名称（ARN）。有关更多信息，请参阅本指南的激活或停用 Amazon ECR 映像拉取器 IAM 角色一节。
2. 确定您的 Amazon ECR 私有存储库是否有策略语句：激活 Amazon ECR 映像拉取器 IAM 角色之后，您需要确定您想要使用容器服务访问的 Amazon ECR 私有存储库是否具有现有的策略语句。有关更多信息，请参阅本指南后面部分中的确定您的 Amazon ECR 私有存储库是否有策略语句。

   您可以使用以下方法之一将 IAM 角色主体 ARN 添加到存储库中，具体取决于存储库是否具有现有策略语句：

   a. 向没有政策声明的私有存储库添加策略 — 使用 Amazon ECR AWS CLI `set-repository-policy` 命令将您的容器服务的 Amazon ECR 图像提取器角色委托人 ARN 添加到具有现有策略的私有存储库中。有关更多信息，请参阅本指南后面部分中的将策略添加到没有策略语句的私有存储库。

   b. 向包含策略声明的私有存储库添加策略 — 使用 Amazon ECR AWS CLI `set-repository-policy` 命令将容器服务的 Amazon ECR 图像提取器角色添加到没有现有策略的私有存储库中。有关更多信息，请参阅本指南后面部分中的将策略添加到有策略语句的私有存储库。

激活或停用 Amazon ECR 映像拉取器 IAM 角色

完成以下步骤以激活或停用 Lightsail 容器服务的 Amazon ECR 图像提取器 IAM 角色。你可以使用 Lightsail 的命令激活或停用 Amazon ECR 图像提取器 IAM 角色 AWS CLI `update-container-service`。有关更多信息，请参阅 AWS CLI 命令参考 中的 update-container-service。

> **Note**
>
> 必须先为 Lightsail 安装 AWS CLI 并对其进行配置，然后才能继续执行此过程。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以更新容器服务并激活或停用 Amazon ECR 映像拉取器 IAM 角色。

```
aws lightsail update-container-service --service-name ContainerServiceName --
private-registry-access ecrImagePullerRole={isActive=RoleActivationState} --
region AwsRegionCode
```

在该命令中，将以下示例文本替换为自己的文本：

- *ContainerServiceName*— 要为其激活或停用 Amazon ECR 图像提取器 IAM 角色的容器服务的名称。
- *RoleActivationState*— Amazon ECR 图像提取器 IAM 角色的激活状态。指定 `true` 以激活角色，或指定 `false` 停用角色。
- *AwsRegionCode*— 容器服务的 AWS 区域 代码（例如，`us-east-1`）。

示例：

- 激活 Amazon ECR 映像拉取器 IAM 角色：

```
aws lightsail update-container-service --service-name my-container-service --
private-registry-access ecrImagePullerRole={isActive=true} --region us-east-1
```

- 停用 Amazon ECR 映像拉取器 IAM 角色：

```
aws lightsail update-container-service --service-name my-container-service --
private-registry-access ecrImagePullerRole={isActive=false} --region us-east-1
```

3. 如果您：

- 已激活 Amazon ECR 映像拉取器角色：在收到之前的回复后至少等待 30 秒钟。然后，继续下一步以获取您的容器服务的 Amazon ECR 映像拉取器 IAM 角色的主体 ARN。
- 已停用 Amazon ECR 映像拉取器角色：如果您之前已将 Amazon ECR 映像拉取器 IAM 角色主体 ARN 添加到您的 Amazon ECR 私有存储库的权限策略，则您应该从存储库中删除该权限策略。有关更多信息，请参阅《Amazon ECR 用户指南》中的删除私有存储库策略语句。

4. 输入以下命令以获取您的容器服务的 Amazon ECR 映像拉取器 IAM 角色的主体 ARN。

```
aws lightsail get-container-services --service-name ContainerServiceName --
region AwsRegionCode
```

在该命令中，将以下示例文本替换为自己的文本：

- *ContainerServiceName*— 要为其获取 Amazon ECR 图像提取器 IAM 角色主体 ARN 的容器服务的名称。
- *AwsRegionCode*— 容器服务的 AWS 区域 代码（例如，us-east-1）。

示例：

```
aws lightsail get-container-services --service-name my-container-service --
region us-east-1
```

在响应中寻找 ECR 映像拉取器 IAM 角色主体 ARN。如果列出了角色，请将其复制或记下来。在本指南的下一部分，您将需要它。接下来，您需要确定您想要使用容器服务访问的 Amazon ECR 私有存储库上是否有现有的策略语句。继续浏览本指南的确定 Amazon ECR 私有存储库是否具有策略语句一节。

确定您的 Amazon ECR 私有存储库是否有策略语句

使用以下程序确定您的 Amazon ECR 私有存储库是否有策略语句。您可以将 AWS CLI get-repository-policy命令用于 Amazon ECR。有关更多信息，请参阅 AWS CLI 命令参考 中的 update-container-service。

> **Note**
>
> 必须先为 Amazon ECR 安装 AWS CLI 并对其进行配置，然后才能继续执行此过程。有关更多信息，请参阅《Amazon ECR 用户指南》中的对 Amazon ECR 进行设置。

1. 打开命令提示符或终端窗口。
2. 输入以下命令以获取特定私有存储库的策略语句。

```
aws ecr get-repository-policy --repository-name RepositoryName --
region AwsRegionCode
```

在该命令中，将以下示例文本替换为自己的文本：

- *RepositoryName*— 您要为其配置 Lightsail 容器服务访问权限的私有仓库的名称。

- *AwsRegionCode*— 私有存储库的 AWS 区域 代码（例如，us-east-1）。

示例：

```
aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
```

您应看到以下响应之一：

- RepositoryPolicyNotFoundException— 您的私有仓库没有政策声明。如果您的存储库没有策略语句，请按照本指南稍后部分中的将策略添加到没有策略语句的私有存储库一节中的步骤。

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo

An error occurred (RepositoryPolicyNotFoundException) when calling the GetRepositoryPolicy operation: Repository policy
does not exist for the repository with name 'my-private-repo' in the registry with id '[redacted]'
```

- 存储库策略已找到 - 您的私有存储库具有策略语句，它在您的请求的响应中显示。如果存储库有策略语句，请复制现有策略，然后按照本指南稍后部分中的将策略添加到有策略语句的私有存储库一节中的步骤。

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo
{
    "registryId": "[redacted]",
    "repositoryName": "my-private-repo",
    "policyText": "{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" : \"AllowUserPushPull\",\n
\"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::[redacted]:user/example-user\"\n    },\
n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\", \"ecr:GetDo
wnloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\", \"ecr:UploadLayerPart\" ]\n  } ]\n}"
}
```

将策略添加到没有策略语句的私有存储库

完成以下过程以将策略添加到没有策略语句的 Amazon ECR 私有存储库。您添加的策略必须包含您的 Lightsail 容器服务的 Amazon ECR 图片提取器 IAM 角色主体 ARN。这将授予容器服务访问权限，以部署私有存储库中的映像。

> **Important**
>
> 当你使用 Lightsail 控制台配置访问权限时，Lightsail 会自动将 Amazon ECR 图像提取器角色添加到你的亚马逊 ECR 私有存储库中。在这种情况下，您不必使用本部分中的程序将 Amazon ECR 映像拉取器角色手动添加到您的私有存储库中。有关更多信息，请参阅本指南前面的“使用 Lightsail 控制台管理私有仓库的访问权限”。

您可以使用 AWS CLI向私有存储库添加策略。为此，您可以创建包含策略的 JSON 文件，然后使用 Amazon ECR 的 `set-repository-policy` 命令引用该文件。有关更多信息，请参阅 AWS CLI 命令参考 中的 set-repository-policy。

> **Note**
>
> 在继续执行此过程之前，您必须为 Amazon ECR 安装 AWS CLI 并对其进行配置。有关更多信息，请参阅《Amazon ECR 用户指南》中的对 Amazon ECR 进行设置。

1. 打开文本编辑器，然后将以下策略语句粘贴到新的文本文件中。

```
{
  "Version": "2008-10-17",
  "Statement": [
  {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

   在文本中，*IamRolePrincipalArn*用本指南前面部分的容器服务的 Amazon ECR 图像提取器 IAM 角色主体 ARN 替换。

2. 在计算机上的可访问位置将文件另存为 `ecr-policy.json`（例如，Windows 上的 `C:\Temp\ecr-policy.json` 或 macOS 或 Linux 上的 `/tmp/ecr-policy.json`）。
3. 记下所创建的 `ecr-policy.json` 文件的文件路径位置。您将在此过程后面部分的命令中指定它。
4. 打开命令提示符或终端窗口。
5. 输入以下命令，为要使用容器服务访问的私有存储库设置策略语句。

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
 file://path/to/ecr-policy.json --region AwsRegionCode
```

在该命令中，将以下示例文本替换为自己的文本：

- *RepositoryName*— 要为其添加策略的私有存储库的名称。
- *path/to/*— 在本指南前面部分创建的计算机上ecr-policy.json文件的路径。
- *AwsRegionCode*— 私有存储库的 AWS 区域 代码（例如，us-east-1）。

示例：

- 在 Windows 上：

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file://C:\Temp\ecr-policy.json --region us-east-1
```

- 在 macOS 或 Linux 上：

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file:///tmp/ecr-policy.json --region us-east-1
```

您的容器服务现在能够访问您的私有存储库及其映像。要使用存储库中的映像，请将以下 URI 指定为您的容器服务部署的 Image（映像）值。在 URI 中，将示例*tag*替换为要部署的映像的标签。有关更多信息，请参阅创建和管理容器服务的部署。

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

在 URI 中，将以下示例文本替换为自己的文本：

- *AwsAccountId*— 您的 AWS 账号。
- *AwsRegionCode*— 私有存储库的 AWS 区域 代码（例如，us-east-1）。
- *RepositoryName*— 用于部署容器映像的私有存储库的名称。
- *ImageTag*— 私有存储库中要部署在容器服务上的容器镜像的标签。

示例：

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

将策略添加到有策略语句的私有存储库

完成以下过程以将策略添加到有策略语句的 Amazon ECR 私有存储库。您添加的策略必须包括现有策略和包含您的 Lightsail 容器服务的 Amazon ECR 图像提取器 IAM 角色主体 ARN 的新策略。这将维护私有存储库上的现有权限，同时授予容器服务从私有存储库部署映像的访问权限。

> **Important**
>
> 当你使用 Lightsail 控制台配置访问权限时，Lightsail 会自动将 Amazon ECR 图像提取器角色添加到你的亚马逊 ECR 私有存储库中。在这种情况下，您不必使用本部分中的程序将 Amazon ECR 映像拉取器角色手动添加到您的私有存储库中。有关更多信息，请参阅本指南前面的 “使用 Lightsail 控制台管理私有仓库的访问权限”。

您可以使用 AWS CLI向私有存储库添加策略。您可以通过创建包含现有策略和新策略的 JSON 文件来完成此操作。然后，使用 Amazon ECR 的 `set-repository-policy` 命令引用该文件。有关更多信息，请参阅 AWS CLI 命令参考 中的 set-repository-policy。

> **Note**
>
> 必须先为 Amazon ECR 安装 AWS CLI 并对其进行配置，然后才能继续执行此过程。有关更多信息，请参阅《Amazon ECR 用户指南》中的对 Amazon ECR 进行设置。

1. 打开命令提示符或终端窗口。
2. 输入以下命令以获取特定私有存储库的策略语句。

```
aws ecr get-repository-policy --repository-name RepositoryName --
region AwsRegionCode
```

在该命令中，将以下示例文本替换为自己的文本：

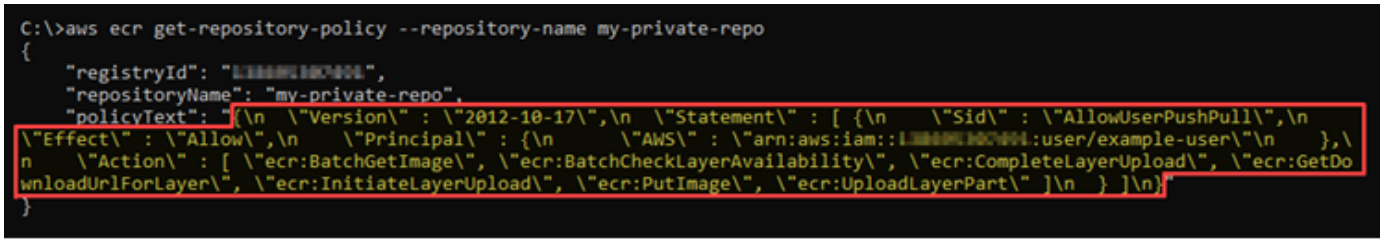
- *RepositoryName*— 您要为其配置 Lightsail 容器服务访问权限的私有仓库的名称。
- *AwsRegionCode*— 私有存储库的 AWS 区域 代码（例如，`us-east-1`）。

示例：

```
aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
```

3. 在响应中，复制现有策略并继续下一个步骤。

   您应该仅复制显示在双引号之间的 `policyText` 的内容，见下面示例中突出显示的内容。



4. 打开文本编辑器，将在上一步中复制的私有存储库的现有策略粘贴在其中。

   结果应该类似以下示例。



5. 在粘贴的文本中，将 `\n` 替换为换行符并删除剩余的 `\`。

   结果应该类似以下示例。



6. 将以下策略语句粘贴在文本文件末尾。

```
,
{
  "Version": "2008-10-17",
  "Statement": [
  {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

7. 在文本中，*IamRolePrincipalArn*用本指南前面部分的容器服务的 Amazon ECR 图像提取器 IAM 角色主体 ARN 替换。

结果应该类似以下示例。



8. 在计算机上的可访问位置将文件另存为 `ecr-policy.json`（例如，Windows 上的 `C:\Temp\ecr-policy.json` 或 macOS 或 Linux 上的 `/tmp/ecr-policy.json`）。
9. 记下 `ecr-policy.json` 文件的文件路径位置。您将在此过程后面部分的命令中指定它。
10. 打开命令提示符或终端窗口。
11. 输入以下命令，为要使用容器服务访问的私有存储库设置策略语句。

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
 file://path/to/ecr-policy.json --region AwsRegionCode
```

在该命令中，将以下示例文本替换为自己的文本：

- *RepositoryName*— 要为其添加策略的私有存储库的名称。
- *path/to/*— 在本指南前面部分创建的计算机上ecr-policy.json文件的路径。
- *AwsRegionCode*— 私有存储库的 AWS 区域 代码（例如，us-east-1）。

示例：

- 在 Windows 上：

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file://C:\Temp\ecr-policy.json --region us-east-1
```

- 在 macOS 或 Linux 上：

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file:///tmp/ecr-policy.json --region us-east-1
```

您应看到类似于以下示例的响应。

```
C:\>aws ecr set-repository-policy --repository-name my-private-repo --policy-text file://C:\Temp\ecr-policy.json --regio
n us-west-2
{
    "registryId": "[redacted]",
    "repositoryName": "my-private-repo",
    "policyText": "{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" : \"AllowLightsailPull-my-cont
ainer-service\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::[redacted]:role/a
mazon/lightsail/[redacted]/containers/my-container-service/private-repo-access/[redacted]
[redacted]\"\n    },\n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:GetDownloadUrlForLayer\" ]\n  }, {\n    \"Sid\" :
\"AllowUserPushPull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::[redacted]:
user/example-user\"\n    },\n    \"Action\" : [ \"ecr:BatchCheckLayerAvailability\", \"ecr:BatchGetImage\", \"ecr:Comple
teLayerUpload\", \"ecr:GetDownloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\", \"ecr:UploadLayerPart\"
]\n  } ]\n}"
}
```

如果您再次运行 get-repository-policy 命令，您应该会看到私有存储库上新的附加策略语句。您的容器服务现在能够访问您的私有存储库及其映像。要使用存储库中的映像，请将以下 URI 指定为您的容器服务部署的 Image（映像）值。在 URI 中，将示例*tag*替换为要部署的映像的标签。有关更多信息，请参阅创建和管理容器服务的部署。

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

在 URI 中，将以下示例文本替换为自己的文本：

- *AwsAccountId*— 您的 AWS 账号。
- *AwsRegionCode*— 私有存储库的 AWS 区域 代码（例如，us-east-1）。
- *RepositoryName*— 用于部署容器映像的私有存储库的名称。
- *ImageTag*— 私有存储库中要部署在容器服务上的容器镜像的标签。

示例：

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

在 Lightsail 中创建和管理容器服务部署

当您准备好在 Amazon Lightsail 容器服务上启动容器时，便可以创建部署。部署是您希望在服务上启动的一组容器规范。容器服务一次可以运行一个部署，一个部署最多可以有 10 个容器条目。您可以在创建容器服务的同时创建部署，也可以在服务启动并运行后创建部署。

> **Note**
>
> 如果创建新部署，则容器服务的现有利用率指标将消失，并且仅显示当前新部署的指标。

有关容器服务的更多信息，请参阅 Amazon Lightsail 中的容器服务。

内容

- 先决条件
- 部署参数
  - 容器条目参数
  - 公有终端节点参数
- 容器之间的通信
- 容器日志

- 部署版本
- 部署状态
- 部署失败
- 查看当前的容器服务部署
- 创建或修改容器服务部署

先决条件

在开始在容器服务中创建部署之前，请完成以下先决条件：

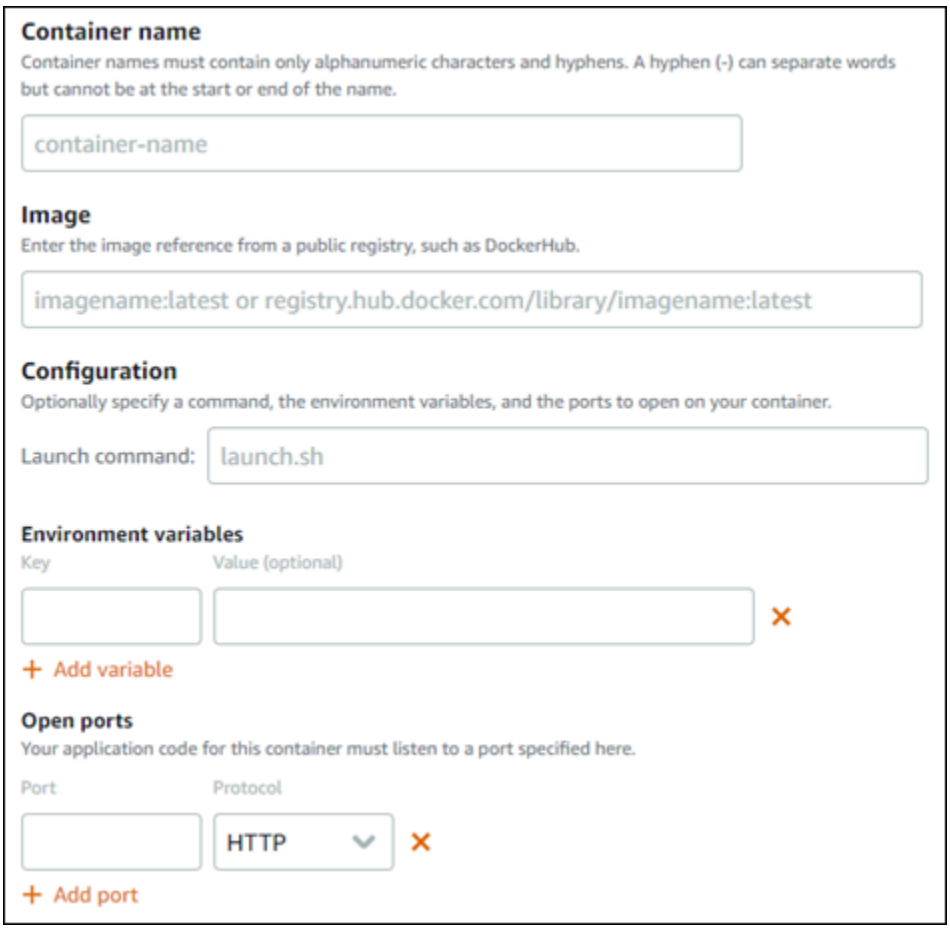
- 在您的 Lightsail 账户中创建容器服务。有关更多信息，请参阅创建 Amazon Lightsail 容器服务。
- 确定在容器服务上启动容器时要使用的容器镜像。
  - 在 Amazon ECR Public Gallery 等公有注册表中查找容器映像。有关更多信息，请参阅《Amazon ECR Public User Guide》中的 Amazon ECR Public Gallery。
  - 在本地计算机上创建容器镜像，然后将其推送到 Lightsail 容器服务。有关更多信息，请参阅以下指南：
    - 安装软件来管理您的 Amazon Lightsail 容器服务的容器镜像
    - 创建容器服务映像
    - 推送和管理容器映像

部署参数

本节介绍可以为部署的容器条目和公有终端节点指定的参数。

容器条目参数

您最多可以在部署中添加 10 个容器条目。每个容器条目都具有可供您指定的以下参数：



- 容器名称 – 输入容器的名称。部署中的所有容器都必须具有唯一的名称，并且只能包含字母数字字符和连字符。连字符可以分隔字词，但不能位于名称的开头或结尾。
- 源镜像 — 指定容器的源容器镜像。可从以下源指定容器镜像：
  - 公有注册表，如 Amazon ECR Public Gallery 或其他一些公有容器映像注册表。

    有关 Amazon ECR Public 的更多信息，请参阅《Amazon ECR Public User Guide》中的 What Is Amazon Elastic Container Registry Public?。
  - 从本地机器推送到容器服务的镜像。要指定已存储的镜像，请选择 Choose stored image（选择已存储的镜像），然后选择您要使用的镜像。

    如果在本地计算机上创建容器镜像，则可以将它们推送到容器服务，以便在创建部署时使用它们。有关更多信息，请参阅创建 Amazon Lightsail 容器服务的容器镜像和推送和管理 Amazon Lightsail 容器服务的容器镜像。
- 启动命令— 指定一个启动命令以运行创建用于配置容器 shell 脚本或 bash 脚本。启动命令可以执行下列操作：添加软件、更新软件或以其他方式配置容器。

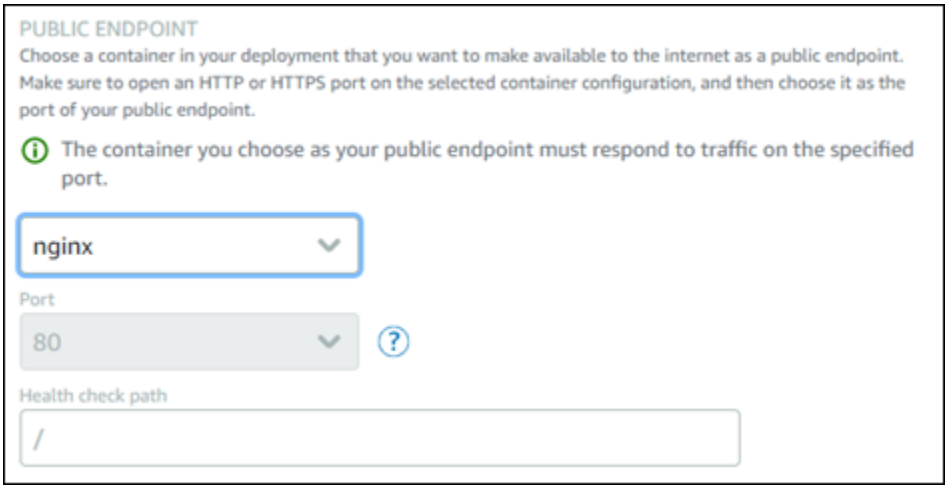
- 环境变量— 指定环境变量，这些变量是键值参数，用于提供容器运行的应用程序或脚本的动态配置。
- 打开端口— 指定要在容器上打开的端口和协议。您可以指定通过 HTTP、HTTPS、TCP 和 UDP 打开任何端口。必须为计划用作容器服务公有终端节点的容器打开 HTTP 或 HTTPS 端口。有关更多信息，请参阅本指南的以下部分。

公有终端节点参数

您可以在部署中指定将用作容器服务公有终端节点的容器条目。公有终端节点容器上的应用程序可通过随机生成的容器服务默认域在互联网上公开访问。默认域的格式为`https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`，其中`<ServiceName>`是您的容器服务的名称，`<RandomGUID>`是您的 Lightsail 账户在 AWS 区域中随机生成的容器服务的全球唯一标识符，`<AWSRegion>`也是创建容器服务的 AWS 区域。Lightsail 容器服务的公共端点仅支持 HTTPS，不支持 TCP 或 UDP 流量。只有一个容器可作为服务的公有端点。因此，请确保选择托管应用程序前端的容器作为公有端点，而其余容器则可以内部访问。

> **Note**
>
> 您可以将自己的自定义域名用于容器服务。有关更多信息，请参阅启用和管理 Amazon Lightsail 容器服务的自定义域。

部署和容器服务的公有终端节点具有以下可以指定的参数：



- 端点容器 — 在部署中选择将用作容器服务的公有终端节点的容器名称。只有在部署中打开了 HTTP 或 HTTPS 端口的容器才会在下拉菜单中列出。

- 端口 — 选择要用于公有终端节点的 HTTP 或 HTTPS 端口。下拉菜单中仅列出在所选容器上打开的 HTTP 和 HTTPS 端口。如果首次启动时所选容器没有为支持 HTTPS 连接进行配置，请选择 HTTP 端口。

  > **Note**
  >
  > 默认情况下，容器服务的默认域使用 HTTPS，即使您选择 HTTP 端口作为公有终端节点端口。这是因为默认情况下，容器服务的负载均衡器会配置为 HTTPS，但它将使用 HTTP 建立与容器的连接。
  > 容器服务的负载均衡器使用 HTTP 连接到容器，但使用 HTTPS 向用户提供内容。

- 运行状况检查路径 — 在所选的公有终端节点容器上指定一个路径，容器服务的负载均衡器将定期进行检查以确保其正常运行。
- 高级运行状况检查设置 – 您可以为选定的公有终端节点容器配置以下运行状况检查设置：
  - 运行状况检查超时（秒）- 等待响应的时长（以秒为单位）。如果在此期间内没有收到任何回复，则运行状况检查将失败。可以指定 2-60 秒。
  - 运行状况检查间隔（秒）- 容器的运行状况检查之间的大约间隔（以秒为单位）。可以指定 5-300 秒。
  - 运行状况检查成功代码 - 检查容器是否成功响应时使用的 HTTP代码。您可以指定 200 到 499 之间的值。您可以指定多个值（例如，200,202）或一系列值（例如，200–299）。
  - 运行状况检查正常阈值 - 将容器移至“正常”状态之前需要的运行状况检查连续成功次数。
  - 运行状况检查不正常阈值 - 将容器移至“不正常”状态之前需要的运行状况检查连续失败次数。

私有域

所有容器服务还有一个私有域，其格式为*<ServiceName>*.service.local，其中*<ServiceName>*是您的容器服务的名称。使用私有域可以从与您的服务位于同一亚马逊云科技区域的另一个 Lightsail 资源访问您的容器服务。如果您没有在服务部署中指定公有端点，则私有域是访问您的容器服务的唯一方式。即使您没有指定公有端点，也会为您的容器服务生成默认域，但会在您尝试浏览它时显示 `404 No Such Service` 错误消息。

要使用容器服务的私有域访问特定容器，必须指定接受连接请求的容器开放端口。为此，您可以将请求的域格式化为*<ServiceName>*.service.local:*<PortNumber>*，其中*<ServiceName>*是您的容器服务的名称，*<PortNumber>*也是您要连接的容器的开放端口。例如，如果您在名为 `container-service-1` 的容器服务上创建一个部署，并指定具有开放端口 6379 的 Redis 容器，那么您请求的域应使用格式 *container-service-1*.service.local:*6379*。

容器之间的通信

使用环境变量，您可以打开同一容器服务中的容器之间、不同容器服务中的容器之间或容器与其他资源之间（例如，容器和托管式数据库之间）之间的通信。

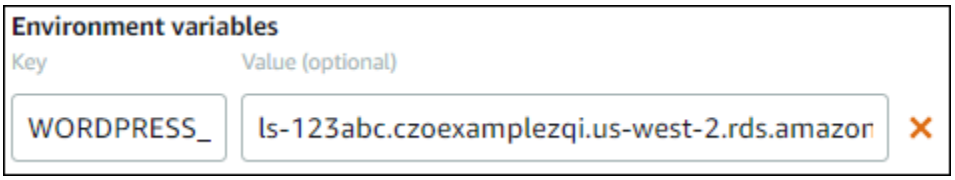
要打开同一容器服务内容器之间的通信，请为引用了 `localhost` 的容器部署添加环境变量，如以下示例所示。



要打开不同容器服务中容器之间的通信，请为引用了其他容器服务的私有域（例如 `container-service-1.service.local`）的容器部署添加环境变量，如以下示例所示。



要打开容器与其他资源之间的通信，请为引用了资源的公有端点 URL 的容器部署添加环境变量。例如，Lightsail 托管数据库的公共端点通常是。`ls-123abc.czoexamplezqi.us-west-2.rds.amazonaws.com`因此，您应该在环境变量中引用这一内容，如以下示例所示。



容器日志

部署中的每个容器都会生成日志。容器日志提供容器内运行的 stdout 和 stderr 进程流。定期访问容器的日志以诊断其运行情况。有关更多信息，请参阅查看 Amazon Lightsail 容器服务的容器日志。

部署版本

您在容器服务中创建的每个部署都会保存为一个部署版本。如果修改现有部署的参数，则会将容器重新部署到您的服务中，并且修改后的部署将生成一个新的部署版本。将保存每个容器服务最近的 50 个部署版本。您可以使用 50 个部署版本中的任何一个在同一容器服务中创建新部署。有关更多信息，请参阅查看和管理 Amazon Lightsail 容器服务的部署版本。

部署状态

在创建部署后，您的部署可能处于下列状态之一：

- 正在激活 — 正在激活部署并正在创建容器。
- 活动 — 部署已成功创建，并且它当前正在容器服务中运行。
- 非活动 — 您之前成功创建的部署已不在容器上运行。
- 失败 — 部署失败，因为部署中指定的一个或多个容器无法启动。

部署失败

如果部署中的一个或多个容器无法启动，部署将失败。如果部署失败，并且容器服务中正在运行之前的部署，则容器服务会将之前的部署保留为活动部署。如果没有之前的部署，则容器服务将保持就绪状态，且当前没有活动状态的部署。

查看失败部署的容器日志，以诊断出现的问题并进行故障排除。有关更多信息，请参阅查看 Amazon Lightsail 容器服务的容器日志。

查看当前的容器服务部署

完成以下步骤以查看 Lightsail 容器服务上的当前部署。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择要查看其当前部署的容器服务的名称。
4. 在容器服务管理页面中，选择部署选项卡。

   部署页面列出了您当前的部署和部署版本。如果您尚未在容器服务中创建部署，则页面的这两个部分将为空白。

创建或修改容器服务部署

完成以下步骤以在 Lightsail 容器服务中创建或修改部署。无论是创建新部署还是修改现有部署，容器服务都会将每个部署保存为新部署版本。有关更多信息，请参阅查看和管理 Amazon Lightsail 容器服务的部署版本。

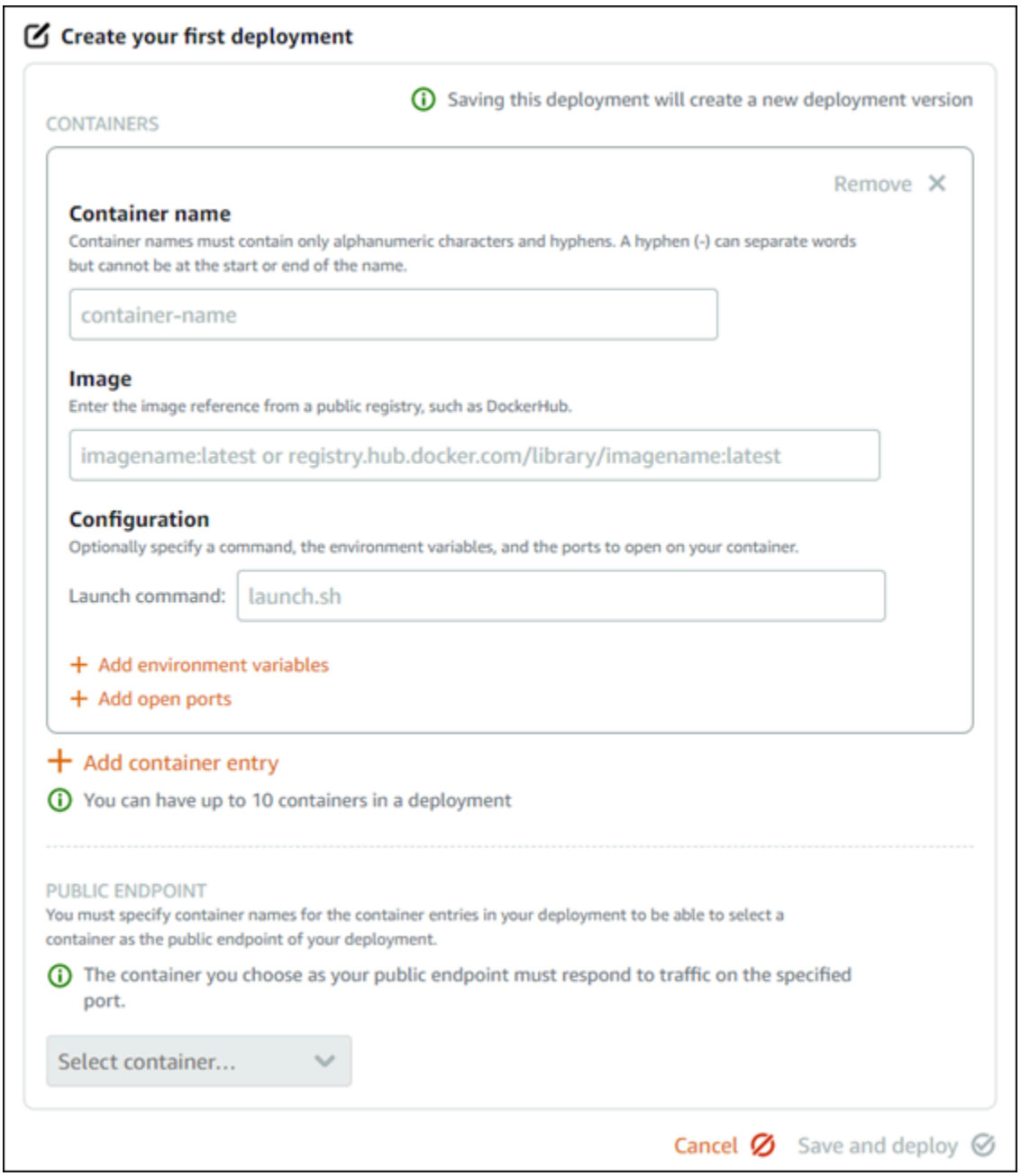
1. 登录 Lightsail 控制台。

2. 在左侧导航窗格中，选择容器。
3. 选择要为其创建或修改容器服务部署的容器服务的名称。
4. 在容器服务管理页面中，选择部署选项卡。

   部署页面列出了您当前的部署和部署版本（如有）。
5. 请选择以下选项之一：

   - 如果容器服务具有现有部署，请选择修改部署。
   - 如果容器服务还没有部署，请选择创建部署。

     此时将打开部署表单，您可以在其中编辑现有部署参数，或者输入新的部署参数。



6. 输入部署的参数。有关可指定的部署参数的更多信息，请参阅本指南中之前的部署参数部分。
7. 选择添加容器条目以将多个容器条目添加到您的部署。部署中最多可拥有 10 个容器条目。
8. 选择将用作公有终端节点容器服务的部署的容器条目。这包括指定 HTTP 或 HTTPS 端口、所选容器条目上的运行状况检查路径以及高级运行状况检查设置。有关更多信息，请参阅本指南前面的公有终端节点参数。
9. 在输入部署参数后，选择保存并部署以在容器服务中创建部署。

   创建部署时，容器服务的状态将变为正在部署。几分钟后，根据部署的状态，容器服务的状态将变为以下状态之一：

- 如果部署成功，容器服务的状态将变为正在运行，并且部署的状态将变为活动。如果您在部署中配置了公有终端节点，则可以通过容器服务的默认域选择使用公有端点的容器。
- 如果部署失败，并且容器服务中正在运行之前的部署，则容器服务的状态将变为正在运行，且容器服务会将之前的部署保留为活动部署。如果没有之前的部署，则容器服务的状态将变为就绪，且当前没有活动状态的部署。查看失败部署的容器日志，以诊断出现的问题并进行故障排除。有关更多信息，请参阅查看 Amazon Lightsail 容器服务的容器日志。

主题

- 扩展 Lightsail 容器服务的容量
- 查看和管理 Lightsail 容器服务部署版本
- 分析 Lightsail 容器服务日志

扩展 Lightsail 容器服务的容量

您的 Amazon Lightsail 容器服务的容量由其规模和功能组成。比例指定容器服务中计算节点的数量，功率指定服务中每个节点CPUs 的内存和 v。可以根据您要为服务提供支持的节点数量来选择规模，以实现更高的可用性和更高的容量。

如果您发现容器服务配置不够，您可以按照本指南中的步骤，随时动态增加容器服务的功率和规模，而无需任何停机时间；如果您发现容器服务过度配置，则可以减少容器服务的功率和规模。Lightsail 会自动管理容量变化以及您当前的部署。

> **Note**
>
> 如果创建新部署，则容器服务的现有利用率指标将消失，并且仅显示当前新部署的指标。

有关容器服务的更多信息，请参阅容器服务。

更改 容器服务的容量

完成以下步骤以更改 Lightsail 容器服务的容量。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择要为其更改容量的容器服务的名称。

4. 在容器服务管理页面中，选择容量选项卡。

   容器服务的当前功率、规模和每月价格显示在容量页面中。

5. 选择更改容量可更改功率和规模。
6. 在显示的确认提示中，选择是，继续以确认更改容器服务的容量将重新配置当前的部署。
7. 选择容器服务的新功率和规模。
8. 选择是，应用以将新容量应用于容器服务。

   容器服务的状态将更改为正在更新。几分钟后，服务的状态将变为已启用，并在新的容量下开始运行。

查看和管理 Lightsail 容器服务部署版本

您在 Amazon Lightsail 容器服务中创建的每个部署都会保存为一个部署版本。如果修改现有部署的参数，则容器将重新部署到您的服务，并且修改部署会生成新的部署版本。将保存每个容器服务最近的 50 个部署版本。您可以在同一容器服务中使用 50 个部署版本中的任何一个创建新部署。在本指南中，我们将介绍如何查看和管理容器服务的部署版本。

有关容器服务的更多信息，请参阅容器服务。

部署版本状态

创建后，各部署版本可能处于下列状态之一：

- 正在部署（正在激活）– 正在启动部署。
- 活动 — 部署已成功创建，并且它当前正在容器服务中运行。容器服务一次只能有一个处于活动状态的部署。
- 非活动 — 您之前成功创建的部署没有在容器上运行。
- 失败 — 部署失败，因为部署中指定的一个或多个容器无法启动。

先决条件

在开始之前，您需要创建 Lightsail 容器服务。有关更多信息，请参阅创建容器服务。

您还应在配置和启动容器的容器服务中创建部署。有关更多信息，请参阅创建和管理 Amazon Lightsail 容器服务的部署。

查看容器服务的部署版本

完成以下步骤以查看 Lightsail 容器服务的部署版本。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择要查看其部署版本的容器服务的名称。
4. 在容器服务管理页面中，选择部署选项卡。

   部署页面列出了您当前的部署和部署版本（如有）。
5. 容器服务的部署版本列在页面的部署版本部分下方。

   每个部署都有一个创建日期、状态和操作菜单。
6. 通过部署版本的操作菜单选择以下选项之一：

   - 创建新部署 — 选择此选项可从所选的部署版本创建新部署。有关创建部署的更多信息，请参阅创建或修改容器服务部署。

     > **Note**
     >
     > 如果您选择从具有失败状态的部署版本创建新部署，则必须在创建部署之前纠正失败的原因。否则，部署可能再次失败。

   - 查看详细信息 — 选择此选项可查看所选部署版本的容器条目和公有端点参数。在需要诊断失败的部署时，您还可以查看部署的容器日志。有关更多信息，请参阅查看容器服务日志。

分析 Lightsail 容器服务日志

Amazon Lightsail 容器服务部署中的每个容器都会生成日志。容器日志提供容器内运行的进程的 stdout 和 stderr 流。请定期访问容器的日志以诊断它们的操作。该日志将存储最近三天的日志条目，然后将最早的条目替换为最新条目。

筛选容器日志

容器日志每天可以包含数百个条目。使用筛选选项可减少日志窗口中显示的条目数量，并便于查找所需条目。您可以按开始日期和结束日期（按本地时间）以及特定术语筛选容器日志。按术语进行筛选时，可以选择包含或排除指定术语的日志条目。



包含或排除筛选术语将查找精确匹配，并且区分大小写。例如，如果您指定仅包含消息中含 HTTP 的录入事件，则将看到所有消息中含 HTTP 的录入事件，而不会看到任何一个消息中含 http 的录入事件。如果您指定排除 Error，则将看到所有消息中不含 Error 的录入事件，还会看到消息中含 ERROR 的录入事件。

先决条件

在开始使用之前，您需要创建 Lightsail 容器服务。有关更多信息，请参阅创建 Amazon Lightsail 容器服务。

您还应在配置和启动容器的容器服务中创建部署。有关更多信息，请参阅创建和管理 Amazon Lightsail 容器服务的部署。

查看容器日志

完成以下过程以查看 Lightsail 容器服务的容器日志。

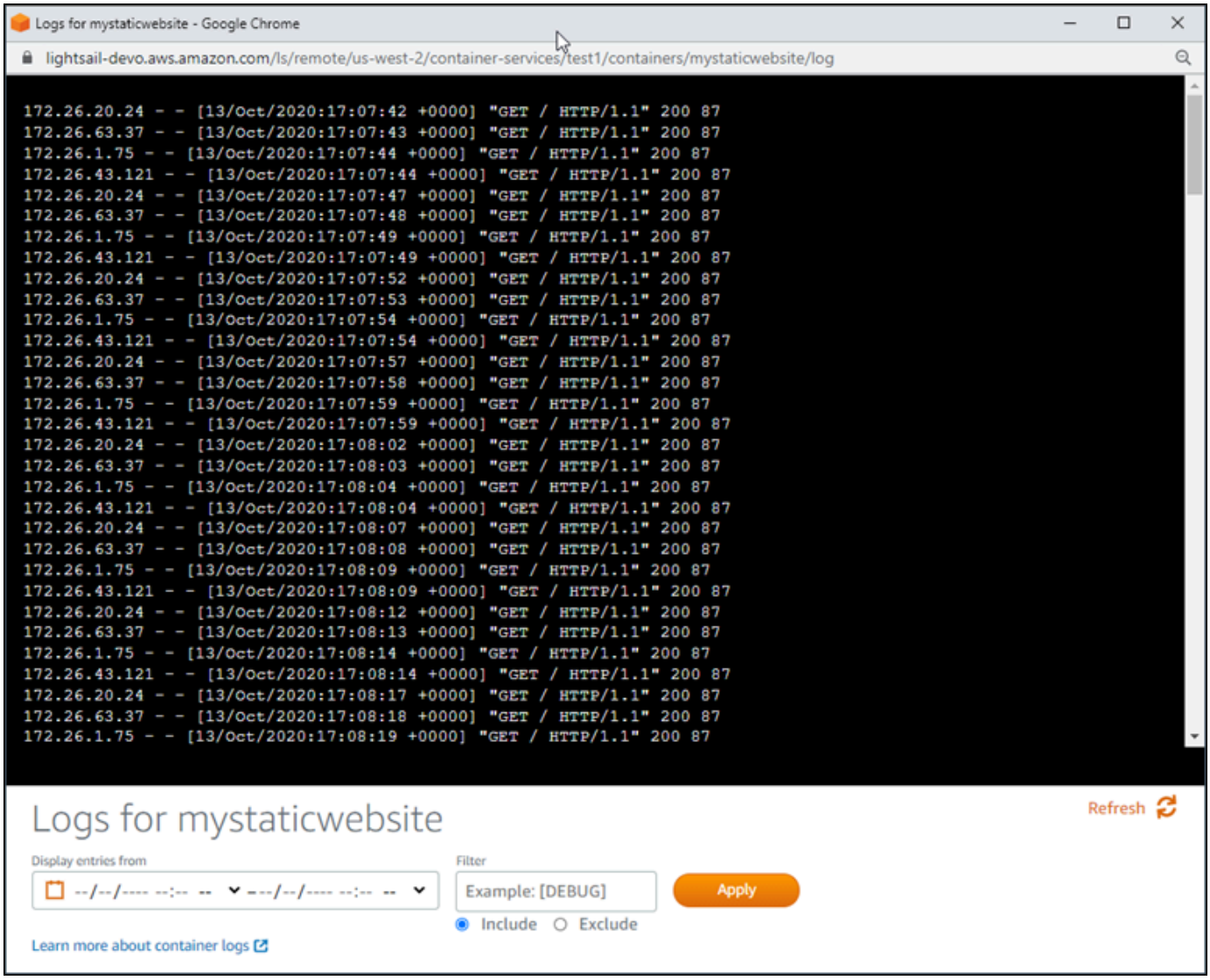
1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择所需容器服务的名称，以查看其容器日志。
4. 在容器服务管理页面上，选择 Deployments（部署）选项卡。

   Deployments（部署）页面将列出您当前的部署和各个部署版本（如果有）。
5. 选择以下选项之一来查看容器日志：

   - 要访问当前部署的容器日志，请选择此页面 Current deployment（当前部署）部分下容器条目的 Open log（打开日志）选项。
   - 要访问先前部署的容器日志，请选择此页面的 Deployment versions（部署版本）部分下先前部署的操作菜单图标（⋮），然后选择 Show details（显示详细信息）。在显示的 Version details（版本详细信息）页面上，选择列出的容器条目的 Open log（打开日志）选项。

容器日志将在新的浏览器窗口中打开。您可以向下滚动来查看更多日志条目，可以刷新页面以加载最新的条目集。筛选选项将显示在页面底部。

> **Note**
>
> 日志条目按协调世界时 (UTC)升序显示。也就是说，最早的日志条目位于顶部，您必须向下滚动才能查看较新的日志条目。



在 Lightsail 中使用自定义域名实现安全的网络访问

为您的 Amazon Lightsail 容器服务启用自定义域，以便将您注册的域名用于您的服务。在启用自定义域之前，您的容器服务仅接受在您首次创建服务时与之关联的默认域（例如，`containerservicename.123456abcdef.us-west-2.cs.amazonlightsail.com`）的流量。启用自定义域时，您可以选择为要用于容器服务的域创建的 Lightsail SSL/TLS 证书，然后从该证书中选择要使用的域。启用自定义域后，您的容器服务将接受与所选证书关联的所有域的流量。

> **Important**
>
> 如果您选择 Lightsail 容器服务作为分发的来源，Lightsail 会自动将分配的默认域名添加为容器服务上的自定义域。这使流量能够在您的分配和容器服务之间进行路由。但是，在某些情况下，您可能需要手动将分配的原定设置域名添加到容器服务中。有关更多信息，请参阅将分配的原定设置域添加到容器服务。

内容

- 容器服务自定义域限制
- 先决条件
- 查看容器服务的自定义域
- 为容器服务启用自定义域
- 禁用容器服务的自定义域

容器服务自定义域限制

容器服务自定义域适用于以下限制：

- 您可以在每个 Lightsail 容器服务中使用最多 4 个自定义域，并且不能在多个服务中使用相同的域。
- 如果您使用 Lightsail DNS 区域来管理您的域名的 DNS，则可以将顶级域（例如 `example.com`）和子域（例如 `www.example.com`）的流量路由到您的容器服务。

先决条件

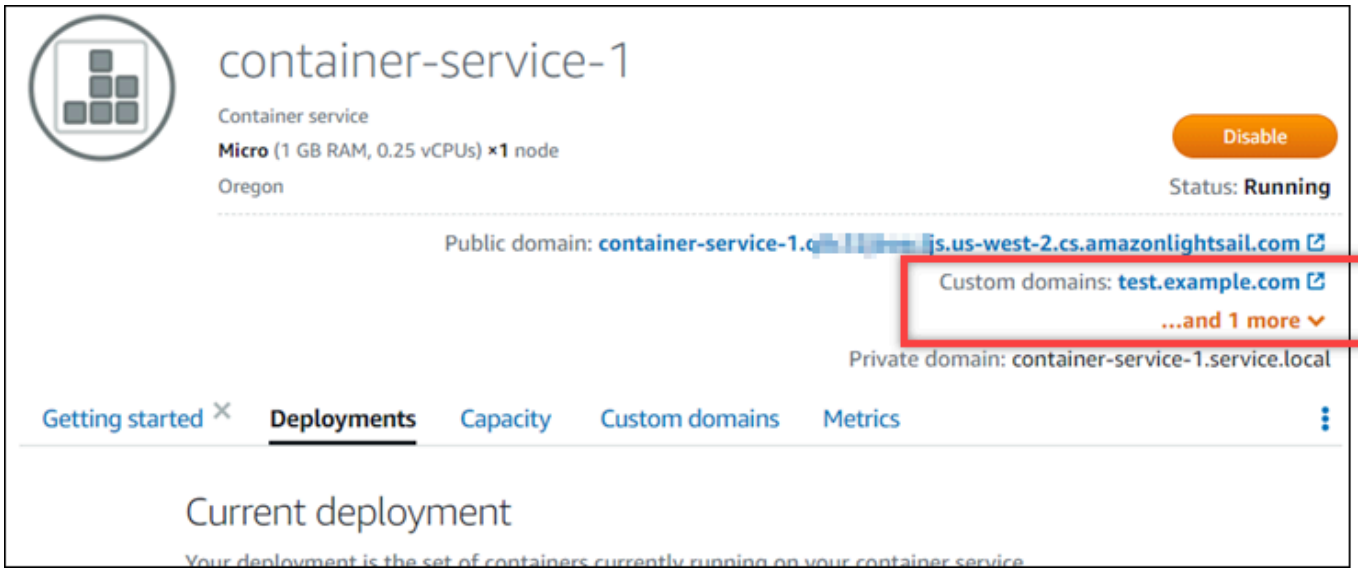
在开始使用之前，您需要创建 Lightsail 容器服务。有关更多信息，请参阅创建 Amazon Lightsail 容器服务。

您还应为容器服务创建并验证 SSL/TLS 证书。有关更多信息，请参阅创建容器服务的 SSL/TLS 证书和验证容器服务的 SSL/TLS 证书。

查看容器服务的自定义域

完成以下过程以查看当前为容器服务启用的自定义域。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择容器服务的名称以查看为其启用的自定义域。
4. 在容器服务管理页面的标题中找到自定义域值，如以下示例中所示。这些是当前为容器服务启用的自定义域。



5. 在容器服务管理页面上选择自定义域选项卡。

   每个附加证书下使用的自定义域列在页面的 Custom domain SSL/TLS certificates（自定义域 SSL/TLS 证书）部分下方。当前附加到容器服务的证书列在 Attached certificates（附加的证书）部分下方。

为容器服务启用自定义域

完成以下过程，通过将证书附加到您的服务，为 Lightsail 容器服务启用自定义域。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。

3. 选择要为其启用自定义域的容器服务名称。
4. 在容器服务管理页面上选择自定义域选项卡。

   自定义域页面显示当前附加到容器服务的 SSL/TLS 证书（如果有）。
5. 选择附加证书。

   如果您没有证书，则必须首先创建和验证域的 SSL/TLS 证书，然后才能将证书附加到容器服务。有关更多信息，请参阅创建容器服务的 SSL/TLS 证书。
6. 在显示的下拉菜单中，为要用于容器服务的域选择有效证书。
7. 验证证书信息是否正确，然后选择 Attach（附加）。
8. 容器服务的 Status（状态）将更改为 Updating（正在更新）。将状态更改为 Ready（就绪）后，证书的域将在 Custom domains（自定义域）部分中显示。
9. 选择 Add domain assignment（添加域分配）以将域指向容器服务
10. 验证证书和 DNS 信息是否正确，然后选择 Add assignment（添加分配）。稍等片刻，您选择的域的流量将开始被容器服务接受。
11. 添加域分配后，打开一个新的浏览器窗口并浏览到已为容器服务启用的自定义域。应加载在容器服务中运行的应用程序（如果有）。

禁用容器服务的自定义域

完成以下过程，通过从服务中分离证书或取消选择之前选定的域来禁用 Lightsail 容器服务的自定义域。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择要为其禁用自定义域的容器服务名称。
4. 在容器服务管理页面上选择自定义域选项卡。

   自定义域页面显示当前附加到容器服务的 SSL/TLS 证书（如果有）。
5. 请选择以下选项之一：

   1. 选择 Configure container service domains（配置容器服务域）取消选择之前选定的域，或选择更多与容器服务关联的域。
   2. 选择分离将证书从容器服务中分离，再从服务中删除其所有关联的域。

> **Important**
>
> 如果尚未执行此操作，请修改域的 DNS 记录，以便流量停止路由到容器服务，改为路由到其他资源。

主题

- 将域流量路由到 Lightsail 容器服务
- 使用 Route 53 将域流量路由到 Lightsail 容器服务

将域流量路由到 Lightsail 容器服务

在为服务启用自定义域后，您必须将注册的域名指向 Amazon Lightsail 容器服务。您可以通过将别名记录添加到与容器服务一起使用的证书上指定的每个域的 DNS 区域中。您添加的所有记录都应该指向容器服务的默认域（例如 `https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`）。

在本指南中，我们介绍了使用 Lightsail DNS 区域将您的域指向容器服务的过程。有关 Lightsail DNS 区域的更多信息，请参阅 Amazon Lightsail 中的 DNS。

有关容器服务的更多信息，请参阅容器服务。

> **Note**
>
> 如果您是使用 Route 53 来托管域的 DNS，那么您应该将别名记录添加到 Route 53 中域的托管区域。有关更多信息，请参阅将 R oute 53 中域的流量路由到 Amazon Lightsail 容器服务。

先决条件

在开始使用之前，您应为 Lightsail 容器服务启用自定义域。有关更多信息，请参阅启用和管理 Amazon Lightsail 容器服务的自定义域。

获取容器服务的默认域

完成以下过程以获取容器服务的默认域名，您可以在将别名记录添加到域的 DNS 中时指定该域名。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择要获取默认域名的容器服务的名称。
4. 在容器服务管理页面的标题部分，记下您的默认域名。您的容器服务默认域名类似于 *<ServiceName>*.*<RandomGUID>*.*<AWSRegion>*.cs.amazonlightsail.com。

   您必须将此值添加为域的 DNS 中的规范名称（别名记录）记录的一部分。我们建议您将此值复制并粘贴到文本文件中，以供之后参考。有关更多信息，请参阅本指南的以下部分将别名记录添加到域的 DNS 区域。

将记录添加到域的 DNS 区域

完成以下步骤，向域名的 DNS 区域添加地址（A 代表 IPv4 或 AAAA 表示 IPv6）记录或规范（CNAME）记录。

1. 在左侧导航窗格中，选择域和 DNS。
2. 在页面的 DNS 区域部分下方，选择要添加记录的域名，以将域的流量引导到容器服务。
3. 选择 DNS records（DNS 记录）选项卡。
4. 根据 DNS 区域的当前状态，完成以下其中一个步骤：

   - 如果您尚未添加 A、AAAA 或别名记录，请选择添加记录。
   - 如果您之前添加了 A、AAAA 或别名记录，请选择页面上列出的现有 A、AAAA 或别名记录旁边的编辑图标，然后跳到此过程的步骤 5。
5. 在 Record type（记录类型）下拉菜单中选择 A record（A 记录）、AAAA record（AAAA 记录）或 CNAME record（别名记录）。

   - 添加 A 记录以将您的域名（例如example.com）或子域名（例如）的顶点映射到网络下的 IPv4 容器服务。www.example.com
   - 添加 AAAA 记录以将您的域名（例如example.com）或子域名（例如）的顶点映射到网络下的容器服务。www.example.com IPv6
   - 添加别名记录以将子域（例如 www.example.com）映射到容器服务的公有域（默认 DNS）。
6. 在 Record name（记录名称）文本框中，输入以下选项之一：

   - 对于 A 记录或 AAAA 记录，请输入 @ 以将顶级域（例如 example.com）的流量路由到容器服务，或者输入一个子域（例如 www）以将子域（例如 www.example.com）的流量路由到您的容器服务。

- 对于别名记录，请输入一个子域（例如 www）以将子域（例如 www.example.com）的流量路由到您的容器服务。

7. 根据要添加的记录，完成以下其中一个步骤：

   - 对于 A 记录或 AAAA 记录，请在解析到文本框中选择容器服务的名称。
   - 对于别名记录，请将容器服务的默认域名输入到映射到文本框中。

8. 选择保存图标以将记录保存到 DNS 区域。

   重复这些步骤，为您用于容器服务的证书上的域添加其他 DNS 记录。留出时间以便更改通过 Internet 的 DNS 传播。几分钟后，您应能够查看您的域是否指向您的容器服务。

使用 Route 53 将域流量路由到 Lightsail 容器服务

您可以将注册域名（例如）的流量路由到在 Amazon Lightsail 容器服务上运行的应用程序。example.com为此，您可以向域的托管区域添加指向 Lightsail 容器服务的默认域的别名记录。

在本教程中，我们将向您展示如何将您的 Lightsail 容器服务的别名记录添加到 Route 53 中的托管区域。只有使用 AWS Command Line Interface (AWS CLI) 才能执行此操作。无法使用 Route 53 控制台来完成此操作。

> **Note**
>
> 如果你使用 Lightsail 来托管你的域名的 DNS，那么你应该在 Lightsail 中将别名记录添加到你的域名的 DNS 区域。有关更多信息，请参阅将 Amazon Lightsail 中域名的流量路由到 Lightsail 容器服务。

内容

- 步骤 1：完成先决条件
- 第 2 步：获取 Lightsail IDs 容器服务的托管区域
- 步骤 3：创建记录集 JSON 文件
- 步骤 4：将记录添加到 Route 53 中域的托管区域

步骤 1：完成先决条件

满足以下先决条件（如果尚未满足）：

- 在 Route 53 中注册域名，或将 Route 53 设为您注册的（现有）域名的 DNS 服务。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用 Amazon Route 53 注册域名或将 Amazon Route 53 作为现有域的 DNS 服务。
- 将您的应用程序部署到您的 Lightsail 容器服务。有关更多信息，请参阅创建和管理容器服务的部署。
- 在 Lightsail 容器服务上启用您的注册域名。有关更多信息，请参阅启用和管理自定义域。
- 使用您的账户 AWS CLI 进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

第 2 步：获取 Lightsail IDs 容器服务的托管区域

在 Route 53 中的托管区域中添加别名记录时，必须为 Lightsail 容器服务指定托管区域 ID。例如，如果您的 Lightsail 容器服务位于美国西部（俄勒冈）(us-west-2)，则在将您的 Lightsail 容器服务的别名记录`Z0959753D43BBB908BAV`添加到 Route 53 的托管区域时，您必须指定托管区域 ID。 AWS 区域

以下是每个 AWS 区域 IDs 的托管区域，您可以在其中创建 Lightsail 容器服务。

欧盟（伦敦）（eu-west-2）：Z0624918 ZXDYQZLOXA66

美国东部（弗吉尼亚北部）（us-east-1）：Z06246771KYU0 W4 IRHI74

亚太地区（新加坡）（ap-southeast-1）：Z0625921354 V0 DRJH4 EY9

欧盟（爱尔兰）（eu-west-1）：Z0624732 Y21 FELAMMKW3

亚太地区（东京）（ap-northeast-1）：Z0626125 JSKN UAU4 JWQ9

亚太地区（首尔）（ap-northeast-2）：Z06260262 B2WPLHH XZM84

亚太地区（孟买）(ap-south-1)：Z10460781IQMISS0I0VVY

亚太地区（悉尼）（ap-southeast-2）：Z09597943 E PQQZATPFE96

加拿大（中部）（ca-central-1）：Z10450993 W RIRIJJUUMA5

欧洲（法兰克福）（eu-central-1）：Z06137433FV04 L0 OY4 EC6

欧洲（斯德哥尔摩）（eu-north-1）：Z016970523 TZMUXKK TDG2

欧洲（巴黎）（eu-west-3）：Z09594631 CFG O DSW2 QUR7

美国东部（俄亥俄州）（us-east-2）：Z10362273 VJ548563 IY84

美国西部（俄勒冈州）（us-west-2）：Z0959753D43 08BAV BBB9

步骤 3：创建记录集 JSON 文件

使用将 DNS 记录添加到 Route 53 中域的托管区域时 AWS CLI，必须为该记录指定一组配置参数。最简单的方法是创建一个包含所有参数的 JSON (.json) 文件，然后在请求中引用 JSON 文件。 AWS CLI

完成以下过程以使用别名记录的记录集参数创建一个 JSON 文件：

1. 打开文本编辑器，例如 Windows 上的记事本或 Linux 上的 Nano。
2. 将以下文本复制并粘贴到文本编辑器中：

```
{
  "Comment": "Comment",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "Domain.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "LightsailContainerServiceHostedZoneID",
          "DNSName": " LightsailContainerServiceAddress.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

在您的文件中，将以下示例文本替换为自己的文本：

- *Comment*附上关于记录集的个人笔记或评论。
- *Domain*使用您想要在 Lightsail 容器服务中使用的注册域名（例如，example.com或www.example.com）。要在 Lightsail 容器服务中使用您的域的根目录，您必须在域的子域空间中指定一个@符号（例如）。@.example.com
- *LightsailContainerServiceHostedZoneID*使用您在其中创建 Lightsail 容器服务的 AWS 区域的托管区域 ID。有关更多信息，请参阅本指南前面的步骤 2：获取 Lightsail 容器服务的托管区域 IDs。
- *LightsailContainerServiceAddress*使用你的 Lightsail 容器服务的公共域名。您可以通过登录 Lightsail 控制台、浏览您的容器服务并复制容器服务管理页面标题部分中列

出的公共域名（例如）来获取此信息。container-service-1.q8cexampleljs.us-west-2.cs.amazonlightsail.com

示例：

```
{
  "Comment": "Alias record for Lightsail container service",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "@.example.com.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "Z0959753D43BBB908BAV",
          "DNSName": "container-service-1.q8cexampleljs.us-
west-2.cs.amazonlightsail.com.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

3. 将文件以 change-resource-record-sets.json 格式保存到本地目录。

步骤 4：将记录添加到 Route 53 中域的托管区域

完成以下过程以使用 AWS CLI将记录添加到 Route 53 中域的托管区域。您可以使用 change-resource-record-sets 命令完成此操作。有关更多信息，请参阅《AWS CLI 命令参考》change-resource-record-sets中的。

> **Note**
>
> 在 AWS CLI 继续执行此过程之前，必须为 Lightsail 和 Route 53 安装并对其进行配置。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

1. 打开命令提示符或终端窗口。
2. 输入以下命令以将记录添加到 Route 53 中域的托管区域。

```
aws route53 change-resource-record-sets --hosted-zone-id HostedZoneID --change-
batch PathToJsonFile
```

在该命令中，将以下示例文本替换为自己的文本：

- *HostedZoneID*其中包含您在 Route 53 中注册域的托管区域的 ID。使用list-hosted-zones命令获取 Route 53 账户中托管区域的列表。 IDs
- *PathToJsonFile*使用计算机上包含记录参数的.json 文件的本地目录文件夹路径。有关更多信息，请参阅本指南前面部分中的步骤 3：创建记录集 JSON 文件。

示例：

在 Linux 或 Unix 计算机上：

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ --
change-batch home/user/awscli/route53/change-resource-record-sets.json
```

在 Windows 计算机上：

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ --
change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

您会看到类似于以下示例的结果：

```
H:\>aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ
--change-batch file://C:\awscli\route53\change-resource-record-sets.json
{
    "ChangeInfo": {
        "Id": "/change/C05953EXAMPLEZ4V4LOAC",
        "Status": "PENDING",
        "SubmittedAt": "2021-08-11T20:58:30.960000+00:00",
        "Comment": "Alias record for Lightsail container service"
    }
}
```

请让更改在 Internet 的 DNS 内进行传播，这可能需要几个小时。完成后，您在 Route 53 中注册域的互联网流量应开始路由到您的 Lightsail 容器服务。

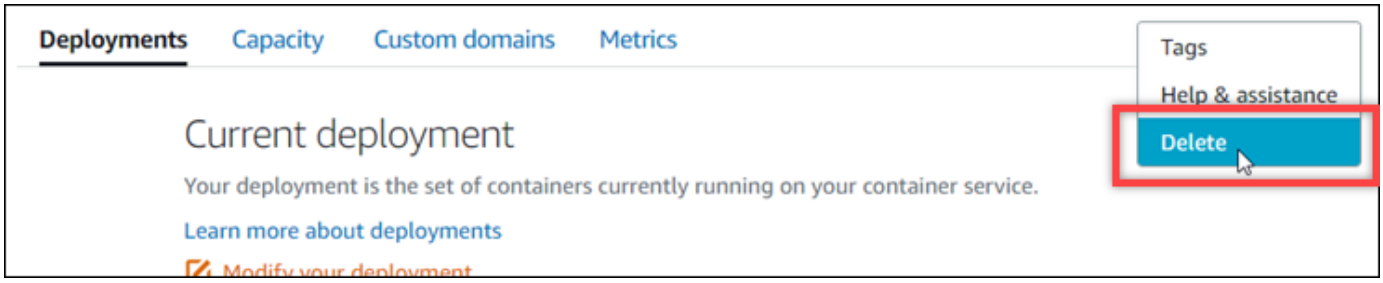
删除 Lightsail 容器服务

如果您不再使用 Amazon Lightsail 容器服务，您可以随时将其删除。删除容器服务时，将永久销毁与服务关联的所有部署和已注册的容器镜像。但是，您创建的 SSL/TLS 证书和域仍会保留在您的 Lightsail 账户中，您可以将它们用于其他资源。有关容器服务的更多信息，请参阅 Amazon Lightsail 中的容器服务。

删除容器服务

完成以下过程以删除容器服务。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择要删除的容器服务的名称。
4. 在选项卡菜单中选择省略号图标，然后选择删除。



5. 选择删除容器服务可删除您的服务。
6. 在显示的提示中，选择是，删除以确认您要永久删除存储的镜像。

   将在片刻后删除容器服务。

亚马逊 Lightsail 中的安全

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。要详细了解合规性计划以及相关合规性计划所适用的服务，请参阅合规性计划范围内的亚马逊云科技服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Amazon Lightsail 时如何应用分担责任模型。以下主题向您展示了如何配置 Amazon Lightsail 以实现您的安全和合规目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Amazon Lightsail 资源。

Amazon Lightsail 中的基础设施安全

作为一项托管服务，Amazon Lightsail 受到 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Lightsail。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

亚马逊 Lightsail 的弹性

AWS 全球基础设施是围绕 AWS 区域 s和可用区构建的。 AWS 区域 s 提供多个物理分隔和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在

可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础结构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础设施外，Amazon Lightsail 还提供多项功能来帮助支持您的数据弹性和备份需求。

- 跨区域复制实例和磁盘快照。有关更多信息，请参阅快照。
- 实例和磁盘快照自动化。有关更多信息，请参阅快照。
- 使用负载均衡器在一个或多个可用区中的多个实例之间分配传入流量 有关更多信息，请参阅负载均衡器。

亚马逊 Lightsail 的身份和访问管理

受众

你的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于你在 Amazon Lightsail 中所做的工作。

服务用户 — 如果您使用 Amazon Lightsail 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多的 Amazon Lightsail 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Amazon Lightsail 中的某项功能，请参阅身份和访问管理疑难解答 (IAM) Access Management。

服务管理员 — 如果你负责公司的亚马逊 Lightsail 资源，那么你可能拥有对亚马逊 Lightsail 的完全访问权限。您的工作是确定您的员工应该访问哪些 Amazon Lightsail 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何将 IAM 与 Amazon Lightsail 配合使用，请参阅亚马逊 Lightsa il 如何与 IA M 配合使用。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 Amazon Lightsail 的访问权限。要查看您可以在 IAM 中使用的亚马逊 Lightsail 基于身份的策略示例，请参阅亚马逊 Lightsail 基于身份的策略示例。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。有关使用登录的更多信息 AWS Management Console，请参阅 IAM 用户指南中的 IAM 控制台和登录页面。

您必须以 AWS 账户 根用户、IAM 用户身份或通过担任 IAM 角色进行身份验证（登录 AWS）。您还可以使用公司的单一登录身份验证方法，甚至使用 Google 或 Facebook 登录。在这些情况下，您的管

理员以前使用 IAM 角色设置了联合身份验证。当你 AWS 使用另一家公司的凭证进行访问时，你就是在间接担任角色。

要直接登录到AWS Management Console，请使用您的密码和根用户电子邮件地址或 IAM 用户名。您可以使用根用户或 IAM 用户访问密钥 AWS 以编程方式进行访问。 AWS 提供 SDK 和命令行工具，可使用您的凭证对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。使用签名版本 4（用于对入站 API 请求进行验证的协议）完成此操作。有关验证请求的更多信息，请参阅 AWS 一般参考 中的签名版本 4 签名流程。

无论使用何种身份验证方法，您可能还需要提供其它安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可

以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 临时 IAM 用户权限 – IAM 用户可以代入 IAM 角色，以暂时获得不同的权限以执行特定的任务。
- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅 AWS IAM Identity Center 用户指南中的权限集。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某项操作是否需要策略中的其他相关操作，请参阅《服务授权参考》中的 Amazon Lightsail 的操作、资源和条件密钥。
  - 服务角色——服务角色是服务代表您在账户中执行操作而代入的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

每个 IAM 实体（用户或角色）最初没有任何权限。换言之，预设情况下，用户什么都不能做，甚至不能更改他们自己的密码。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有预期权限的组中。当管理员为某个组授予访问权限时，该组内的全部用户都会获得这些访问权限。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南中的在托管式策略与内联策略之间进行选择。

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的使用客户管理型策略定义自定义 IAM 权限。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。

- 服务控制策略 (SCPs)- SCPs 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体的基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)- SCPs 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中实体的权限，包括每个 AWS 账户 root 用户。有关 Organizations 和的更多信息 SCPs，请参阅《AWS Organizations 用户指南》中的 SCPs 工作原理。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

主题

- AWS 亚马逊 Lightsail 的托管政策
- 亚马逊 Lightsail 如何与 IAM 合作

- 向 IAM 用户授予 Lightsail 访问权限

AWS 亚马逊 Lightsail 的托管政策

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管策略添加其他权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当推出新功能或有新操作可用时，服务最有可能更新 AWS 托管策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的AWS 托管式策略。

AWS 托管策略： LightsailExportAccess

您无法附加 LightsailExportAccess 到您的 IAM 实体。此政策附加到一个服务相关角色，该角色允许 Lightsail 代表您执行操作。有关更多信息，请参阅服务相关角色。

该策略授予的权限允许 Lightsail 将您的实例和磁盘快照导出到亚马逊弹性计算云，并从亚马逊简单存储服务 (Amazon S3) Simple Storage S3获取当前账户级别的阻止公共访问配置。

权限详细信息

该策略包含以下权限。

- `ec2` – 允许访问，以列出和复制实例映像和磁盘快照。
- `iam` – 允许访问，以删除服务相关角色并检索服务相关角色删除的状态。
- `s3`— 允许访问以检索 AWS 帐户的`PublicAccessBlock`配置。

```
{
 "Version": "2012-10-17",
```

```
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
   ],
   "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:CopySnapshot",
    "ec2:DescribeSnapshots",
    "ec2:CopyImage",
    "ec2:DescribeImages"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "s3:GetAccountPublicAccessBlock"
   ],
   "Resource": "*"
  }
 ]
}
```

Lightsail 更新了托管 AWS 策略

- 编辑到 `LightsailExportAccess` 托管式策略

  向 `LightsailExportAccess` 托管式策略添加了 `s3:GetAccountPublicAccessBlock` 操作。它允许 Lightsail 从 Amazon S3 获取当前账户级别的阻止公共访问配置。

  2022 年 1 月 14 日

- Lightsail 开始追踪更改

  Lightsail 开始跟踪其 AWS 托管策略的变更。

  2022 年 1 月 14 日

亚马逊 Lightsail 如何与 IAM 合作

在使用 IAM 管理对 Lightsail 的访问权限之前，你应该了解有哪些 IAM 功能可用于 Lightsail。要全面了解 Lightsail 和其他 AWS 服务如何与 IAM 配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的 AWS 服务。

Lightsail 基于身份的策略

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。Lightsail 支持特定的操作、资源和条件键。要了解在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》 中的 IAM JSON 策略元素参考。

操作

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

Lightsail 中的策略操作在操作前使用以下前缀:. `lightsail:` 例如，要授予某人通过 Lightsail `CreateInstances` API 操作运行 Lightsail 实例的权限，您需要将该`lightsail:CreateInstances`操作包含在他们的策略中。策略语句必须包含 `Action` 或 `NotAction` 元素。Lightsail 定义了自己的一组操作，这些操作描述了您可以使用此服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "lightsail:action1",
      "lightsail:action2"
```

您也可以使用通配符 （*) 指定多个操作。例如，要指定以单词 `Create` 开头的所有操作，包括以下操作：

```
"Action": "lightsail:Create*"
```

要查看 Lightsail 操作列表，请参阅 IAM 用户指南中的亚马逊 Lightsail 定义的操作。

资源

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

> **Important**
>
> Lightsail 不支持某些 API 操作的资源级权限。有关更多信息，请参阅对基于标签的资源级权限和授权的支持。

Lightsail 实例资源具有以下 ARN：

```
arn:${Partition}:lightsail:${Region}:${Account}:Instance/${InstanceId}
```

有关格式的更多信息 ARNs，请参阅 Amazon 资源名称 (ARNs) 和 AWS 服务命名空间。

例如，要在语句中指定 ea123456-e6b9-4f1d-b518-3ad1234567e6 实例，请使用以下 ARN：

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/ea123456-e6b9-4f1d-
b518-3ad1234567e6"
```

要指定属于特定账户的所有实例，请使用通配符 (*)：

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/*"
```

某些 Lightsail 操作（例如用于创建资源的操作）无法对特定资源执行。在这些情况下，您必须使用通配符（*)。

```
"Resource": "*"
```

许多 Lightsail API 操作都涉及多个资源。例如，将 Lightsail 块存储磁盘`AttachDisk`附加到实例，因此 IAM 用户必须有权使用该磁盘和实例。要在单个语句中指定多个资源，请 ARNs 用逗号分隔。

```
"Resource": [
      "resource1",
      "resource2"
```

要查看 Lightsail 资源类型及其类型列表 ARNs，请参阅 IAM 用户指南中的 Amazon Lightsail 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 Amazon Light sail 定义的操作。

条件键

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

Lightsail 不提供任何特定于服务的条件密钥，但它确实支持使用一些全局条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Lightsail 条件键列表，请参阅 IAM 用户指南中的亚马逊 Lightsail 条件密钥。要了解您可以使用条件键的操作和资源，请参阅 Amazon Lightsail 定义的操作。

示例

要查看 Lightsail 基于身份的策略示例，请参阅亚马逊 Lightsail 基于身份的策略示例。

Lightsail 基于资源的政策

Lightsail 不支持基于资源的策略。

访问控制列表 (ACLs)

Lightsail 不支持访问控制列表 () ACLs。

基于 Lightsail 标签的授权

你可以向 Lightsail 资源附加标签，也可以在请求中将标签传递给 Lightsail。要基于标签控制访问，您需要使用 `lightsail:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

> **Important**
>
> Lightsail 不支持根据标签对某些 API 操作进行授权。有关更多信息，请参阅对基于标签的资源级权限和授权的支持。

有关为 Lightsail 资源添加标签的更多信息，请参阅标签。

要查看基于身份的策略示例，该策略用于根据资源上的标签限制对该资源的访问，请参阅允许根据标签创建和删除 Lightsail 资源。

Lightsail IAM 角色

IAM 角色是 AWS 账户中具有特定权限的实体。

在 Lightsail 上使用临时证书

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。您可以调用 AWS STS API 操作（如AssumeRole 或 GetFederationToken ）以获取临时安全凭证。

Lightsail 支持使用临时证书。

服务相关角色

服务相关角色允许 AWS 服务访问其他服务中的资源以代表您完成操作。服务相关角色显示在 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Lightsail 支持与服务相关的角色。有关创建或管理 Lightsail 服务相关角色的详细信息，请参阅服务相关角色。

服务角色

Lightsail 不支持服务角色。

主题

- 在 Lightsail 中使用 IAM 身份策略授予最低权限权限
- 使用 IAM 策略授予对特定 Lightsail 资源的访问权限
- 为 Amazon Lightsail 使用服务相关角色
- 使用 IAM 策略管理 Lightsail 存储桶

在 Lightsail 中使用 IAM 身份策略授予最低权限权限

默认情况下，IAM 用户和角色无权创建或修改 Lightsail 资源。他们也无法使用 AWS Management Console AWS CLI、或 AWS API 执行任务。IAM 管理员必须创建 IAM 策略，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅《IAM 用户指南》中的 在 JSON 选项卡上创建策略。

策略最佳实践

基于身份的策略决定了是否有人可以在您的账户中创建、访问或删除亚马逊 Lightsail 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略或工作职能的AWS 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。

- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Lightsail 控制台

要访问亚马逊 Lightsail 控制台，您必须拥有所有 Lightsail 操作和资源的完全访问权限。这些权限必须允许您列出和查看有关您 AWS 账户中 Lightsail 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略（即，没有完整访问权限），对于附加了该策略的实体（IAM 用户或角色），控制台将无法按预期正常运行。

为确保这些实体可以使用 Lightsail 控制台，请将以下策略附加到这些实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:*"
            ],
            "Resource": "*"
        }
    ]
}
```

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允许根据标签创建和删除 Lightsail 资源

您可以使用基于身份的策略中的条件根据标签控制对 Lightsail 资源的访问权限。此示例说明如何创建限制用户创建新的 Lightsail 资源的策略，除非在创建请求中定义`true`了密钥标签`allow`和值。该策略还会限制用户删除资源，除非他们具有 `allow/true` 键值标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Create*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/allow": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Delete*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allow": "true"
                }
            }
        }
    ]
}
```

以下示例会限制用户更改其键值标签不是 allow/false 的资源的标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
```

```
}
```

您可以将这些策略附加到账户中的 IAM 用户。有关更多信息，请参阅 IAM 用户指南 中的 IAM JSON 策略元素：条件。

使用 IAM 策略授予对特定 Lightsail 资源的访问权限

资源级权限指的是能够指定允许用户对哪些资源执行操作的能力。Amazon Lightsail 支持资源级权限。这意味着，对于某些 Lightsail 操作，您可以根据必须满足的条件或允许用户使用或编辑的特定资源来控制何时允许用户使用这些操作。例如，您可以授予用户权限，以管理具有特定 Amazon Resource Name (ARN) 的实例或数据库。

> **Important**
>
> Lightsail 不支持某些 API 操作的资源级权限。有关更多信息，请参阅对基于标签的资源级权限和授权的支持。

有关由 Lightsail 操作创建或修改的资源以及您可以在 IAM 策略声明中使用的和 ARNs Lightsail 条件键的更多信息，请参阅 IAM 用户指南中的 A mazon Lightsail 操作、资源和条件密钥。

允许管理特定实例

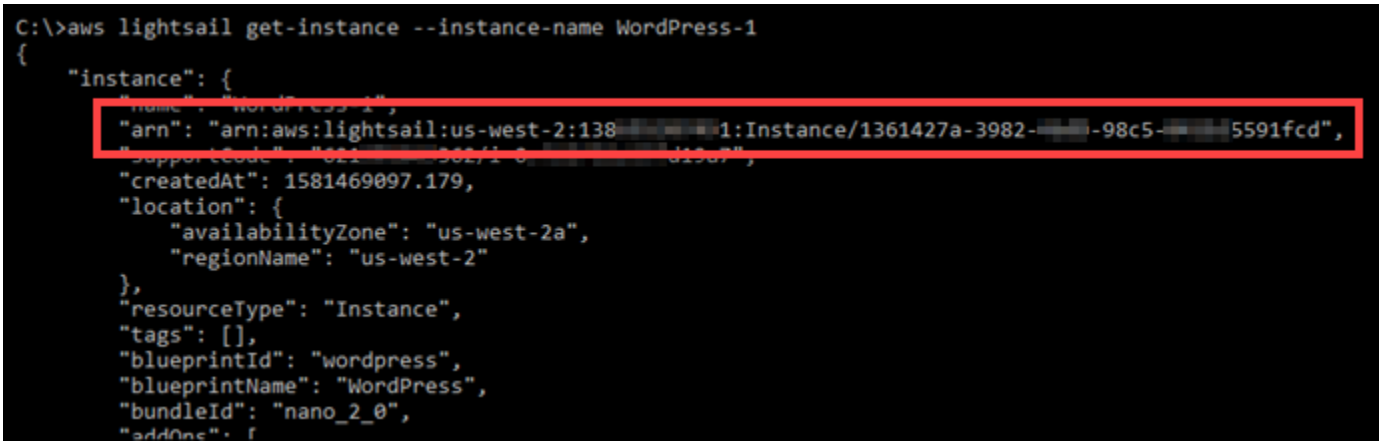
以下策略授予对reboot/start/stop实例的访问权限、管理实例端口以及为特定实例创建实例快照。它还提供对 Lightsail 账户中其他与实例相关的信息和资源的只读访问权限。在策略中，*InstanceARN*替换为您的实例的 Amazon 资源名称 (ARN)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "lightsail:GetActiveNames",
                "lightsail:GetAlarms",
                "lightsail:GetAutoSnapshots",
                "lightsail:GetBlueprints",
                "lightsail:GetBundles",
                "lightsail:GetCertificates",
                "lightsail:GetCloudFormationStackRecords",
                "lightsail:GetContactMethods",
```

```
                "lightsail:GetDisk",
                "lightsail:GetDisks",
                "lightsail:GetDiskSnapshot",
                "lightsail:GetDiskSnapshots",
                "lightsail:GetDistributionBundles",
                "lightsail:GetDistributionLatestCacheReset",
                "lightsail:GetDistributionMetricData",
                "lightsail:GetDistributions",
                "lightsail:GetDomain",
                "lightsail:GetDomains",
                "lightsail:GetExportSnapshotRecords",
                "lightsail:GetInstance",
                "lightsail:GetInstanceAccessDetails",
                "lightsail:GetInstanceMetricData",
                "lightsail:GetInstancePortStates",
                "lightsail:GetInstances",
                "lightsail:GetInstanceSnapshot",
                "lightsail:GetInstanceSnapshots",
                "lightsail:GetInstanceState",
                "lightsail:GetKeyPair",
                "lightsail:GetKeyPairs",
                "lightsail:GetLoadBalancer",
                "lightsail:GetLoadBalancerMetricData",
                "lightsail:GetLoadBalancers",
                "lightsail:GetLoadBalancerTlsCertificates",
                "lightsail:GetOperation",
                "lightsail:GetOperations",
                "lightsail:GetOperationsForResource",
                "lightsail:GetRegions",
                "lightsail:GetRelationalDatabase",
                "lightsail:GetRelationalDatabaseBlueprints",
                "lightsail:GetRelationalDatabaseBundles",
                "lightsail:GetRelationalDatabaseEvents",
                "lightsail:GetRelationalDatabaseLogEvents",
                "lightsail:GetRelationalDatabaseLogStreams",
                "lightsail:GetRelationalDatabaseMetricData",
                "lightsail:GetRelationalDatabaseParameters",
                "lightsail:GetRelationalDatabases",
                "lightsail:GetRelationalDatabaseSnapshot",
                "lightsail:GetRelationalDatabaseSnapshots",
                "lightsail:GetStaticIp",
                "lightsail:GetStaticIps",
                "lightsail:IsVpcPeered"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "lightsail:CloseInstancePublicPorts",
                "lightsail:CreateInstanceSnapshot",
                "lightsail:OpenInstancePublicPorts",
                "lightsail:PutInstancePublicPorts",
                "lightsail:RebootInstance",
                "lightsail:StartInstance",
                "lightsail:StopInstance"
            ],
            "Resource": "InstanceARN"
        }
    ]
}
```

要获取您的实例的 ARN，请使用 Lightsa GetInstance il API 操作，然后使用参数指定实例的名称。instanceName您的实例 ARN 将在该操作的结果中列出，如下例所示。有关更多信息，请参阅GetInstance《亚马逊 Lightsail API 参考》。



允许管理特定数据库

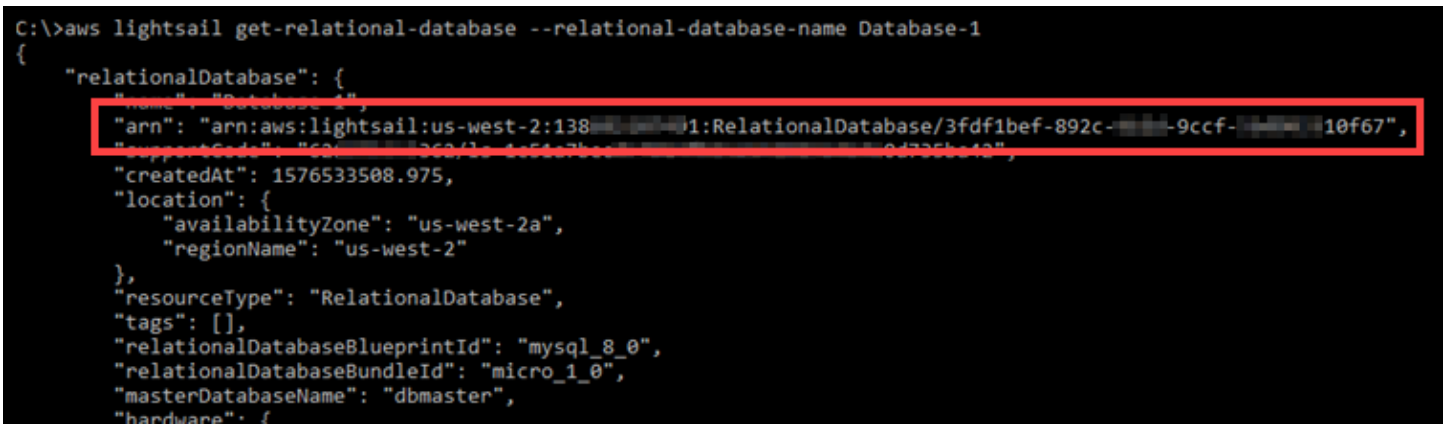
以下策略授予访问reboot/start/stop和更新特定数据库的权限。它还提供对 Lightsail 账户中其他与数据库相关的信息和资源的只读访问权限。在策略中，*DatabaseARN*替换为数据库的 Amazon 资源名称 (ARN)。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "lightsail:GetActiveNames",
                "lightsail:GetAlarms",
                "lightsail:GetAutoSnapshots",
                "lightsail:GetBlueprints",
                "lightsail:GetBundles",
                "lightsail:GetCertificates",
                "lightsail:GetCloudFormationStackRecords",
                "lightsail:GetContactMethods",
                "lightsail:GetDisk",
                "lightsail:GetDisks",
                "lightsail:GetDiskSnapshot",
                "lightsail:GetDiskSnapshots",
                "lightsail:GetDistributionBundles",
                "lightsail:GetDistributionLatestCacheReset",
                "lightsail:GetDistributionMetricData",
                "lightsail:GetDistributions",
                "lightsail:GetDomain",
                "lightsail:GetDomains",
                "lightsail:GetExportSnapshotRecords",
                "lightsail:GetInstance",
                "lightsail:GetInstanceAccessDetails",
                "lightsail:GetInstanceMetricData",
                "lightsail:GetInstancePortStates",
                "lightsail:GetInstances",
                "lightsail:GetInstanceSnapshot",
                "lightsail:GetInstanceSnapshots",
                "lightsail:GetInstanceState",
                "lightsail:GetKeyPair",
                "lightsail:GetKeyPairs",
                "lightsail:GetLoadBalancer",
                "lightsail:GetLoadBalancerMetricData",
                "lightsail:GetLoadBalancers",
                "lightsail:GetLoadBalancerTlsCertificates",
                "lightsail:GetOperation",
                "lightsail:GetOperations",
                "lightsail:GetOperationsForResource",
                "lightsail:GetRegions",
                "lightsail:GetRelationalDatabase",
                "lightsail:GetRelationalDatabaseBlueprints",
```

```
                "lightsail:GetRelationalDatabaseBundles",
                "lightsail:GetRelationalDatabaseEvents",
                "lightsail:GetRelationalDatabaseLogEvents",
                "lightsail:GetRelationalDatabaseLogStreams",
                "lightsail:GetRelationalDatabaseMetricData",
                "lightsail:GetRelationalDatabaseParameters",
                "lightsail:GetRelationalDatabases",
                "lightsail:GetRelationalDatabaseSnapshot",
                "lightsail:GetRelationalDatabaseSnapshots",
                "lightsail:GetStaticIp",
                "lightsail:GetStaticIps",
                "lightsail:IsVpcPeered"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "lightsail:RebootRelationalDatabase",
                "lightsail:StartRelationalDatabase",
                "lightsail:StopRelationalDatabase",
                "lightsail:UpdateRelationalDatabase"
            ],
            "Resource": "DatabaseARN"
        }
    ]
}
```

要获取数据库的 ARN，请使用 Lightsai GetRelationalDatabase l API 操作，然后使用参数指定数据库的名称。relationalDatabaseName您的数据库 ARN 将在该操作的结果中列出，如下例所示。有关更多信息，请参阅GetRelationalDatabase《亚马逊 Lightsail API 参考》。



为 Amazon Lightsail 使用服务相关角色

Amazon Lightsail 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接关联到 Amazon Lightsail。服务相关角色由 Amazon Lightsail 预定义，包括 Lightsail 代表您调用 AWS 其他服务所需的所有权限。

服务相关角色使设置 Amazon Lightsail 变得更加容易，因为您不必手动添加必要的权限。Amazon Lightsail 定义了其服务相关角色的权限，除非另有定义，否则只有亚马逊 Lightsail 才能担任其角色。定义的权限包括信任策略和权限策略，这些策略不能附加到任何其他 IAM 实体。

只有在首先删除相关资源后，您才能删除服务相关角色。这样可以保护您的 Amazon Lightsail 资源，因为您不会无意中删除访问这些资源的权限。

有关支持服务关联的角色的其他服务的信息，请参阅与 IAM 配合使用的亚马逊云科技服务，并查找 服务相关角色（Service-Linked Role）列设为 Yes（是）的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

亚马逊 Lightsail 的服务相关角色权限

Amazon Lightsail 使用名为 AWSServiceRoleForLightsail“角色” 的服务相关角色将 Lightsail 实例和块存储磁盘快照导出到亚马逊弹性计算云 (亚马逊 EC2)，并从亚马逊简单存储服务 (Amazon S3) 获取当前账户级别的阻止公共访问配置。

AWSServiceRoleForLightsail 服务相关角色信任以下服务来代入该角色：

- `lightsail.amazonaws.com`

角色权限策略允许 Amazon Lightsail 对指定资源完成以下操作：

- 操作：`ec2:CopySnapshot`对所有 AWS 资源采取行动。
- 操作：`ec2:DescribeSnapshots`对所有 AWS 资源采取行动。
- 操作：`ec2:CopyImage`对所有 AWS 资源采取行动。
- 操作：`ec2:DescribeImages`对所有 AWS 资源采取行动。
- 操作：`cloudformation:DescribeStacks`在所有 AWS AWS CloudFormation 堆栈上。
- 操作：`s3:GetAccountPublicAccessBlock`对所有 AWS 资源采取行动。

服务相关角色权限

您必须配置权限以允许 IAM 实体（例如，用户、组或角色）创建或编辑服务相关角色的描述。

允许 IAM 实体创建特定服务相关角色

将以下策略添加到需要创建服务相关角色的 IAM 实体中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*",
            "Condition": {"StringLike": {"iam:AWSServiceName":
 "lightsail.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
        }
    ]
}
```

允许 IAM 实体创建任何服务相关角色

将以下语句添加到 IAM 实体的权限策略，该实体需要创建服务相关角色或任何包含所需策略的服务角色。此策略会将策略附加到角色。

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

允许 IAM 实体编辑任何服务角色的描述

将以下语句添加到 IAM 实体的权限策略，该实体需要编辑服务相关角色或任何服务角色的描述。

```
{
    "Effect": "Allow",
    "Action": "iam:UpdateRoleDescription",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

允许 IAM 实体删除特定服务相关角色

将以下语句添加到需要删除服务相关角色的 IAM 实体的权限策略。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
}
```

允许 IAM 实体删除任何服务相关角色

将以下语句添加到 IAM 实体的权限策略，该实体需要删除服务相关角色或任何服务角色。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

或者，您可以使用 AWS 托管策略来提供对服务的完全访问权限。

为 Amazon Lightsail 创建服务相关角色

您无需手动创建服务相关角色。当你将 Lightsail 实例或块存储磁盘快照导出到亚马逊，或者在 EC2、或 API 中创建或更新 Lightsail 存储桶时 AWS AWS Management Console， AWS Amazon Lightsail 会为您创建服务相关角色。 AWS CLI

如果您删除了此服务相关角色然后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。当你将 Lightsail 实例或块存储磁盘快照导出到亚马逊 EC2，或者创建或更新 Lightsail 存储桶时，Amazon Lightsail 会再次为您创建服务相关角色。

> **Important**
>
> 您必须配置 IAM 权限才能允许 Amazon Lightsail 创建服务相关角色。为此，请完成以下服务相关角色权限部分中的步骤。

编辑 Amazon Lightsail 的服务相关角色

Amazon Lightsail 不允许您编辑 AWSServiceRoleForLightsail 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 Amazon Lightsail 的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，在删除 AWSServiceRoleForLightsail服务相关角色之前，您必须确认没有处于待复制状态的 Amazon Lightsail 实例或磁盘快照。有关更多信息，请参阅将快照导出到 Amazon EC2。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForLightsail 服务相关角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

亚马逊 Lightsail 服务相关角色支持的区域

Amazon Lightsail 支持在提供服务的所有地区使用服务相关角色。有关 Lightsail 在哪些地区可用的更多信息，请参阅亚马逊 Lightsail 区域。

使用 IAM 策略管理 Lightsail 存储桶

以下策略授予用户管理Amazon Lightsail对象存储服务中特定存储段的权限。此策略允许通过 Lightsail 控制台、AWS CLI() AWS 、API AWS Command Line Interface 和访问存储桶。 AWS SDKs在策略中，*<BucketName>*替换为要管理的存储桶的名称。有关 IAM policy 的更多信息，请参阅《AWS Identity and Access Management 用户指南》中的创建 IAM policy。有关创建 IAM 用户和用户组的更多信息，请参阅《AWS Identity and Access Management 用户指南》中的创建您的第一个 IAM 委派用户和用户组。

> **Important**
>
> 没有此政策的用户在 Lightsail 控制台中查看存储分区管理页面的 “对象” 选项卡时会遇到错误。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LightsailAccess",
            "Effect": "Allow",
            "Action": "lightsail:*",
            "Resource": "*"
        },
        {
            "Sid": "S3BucketAccess",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::<BucketName>/*",
                "arn:aws:s3:::<BucketName>"
            ]
        }
    ]
}
```

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。

2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 禁止公开访问亚马逊 Lightsail 中的存储桶
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶
   - 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
   - 在 Amazon Lightsail 中查看存储桶中的对象
   - 在 Amazon Lightsail 中复制或移动存储桶中的对象
   - 从 Amazon Lightsail 中的存储桶下载对象

- 在 Amazon Lightsail 中筛选存储桶中的对象
- 在 Amazon Lightsail 中标记存储桶中的对象
- 在 Amazon Lightsail 中删除存储桶中的对象

9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

向 IAM 用户授予 Lightsail 访问权限

作为AWS 账户根用户或具有管理员权限的 AWS Identity and Access Management (IAM) 用户，您可以在自己的 AWS 账户中创建一个或多个 IAM 用户，并且可以将这些用户配置为对所提供的服务的不同访问级别 AWS。

对于 Amazon Lightsail，你可能需要创建一个只能访问 Lightsail 服务的 IAM 用户。当有人加入你的团队，需要查看、创建、编辑或删除 Lightsail 资源，但不需要访问提供的其他服务时，你就会这样做。AWS要对此进行配置，您必须先创建一个授予 Lightsail 访问权限的 IAM 策略，然后创建一个 IAM 群组，并将该策略附加到该群组。然后，您可以创建 IAM 用户并使其成为该群组的成员，这样他们就可以访问 Lightsail。

当有人离开你的团队时，你可以将该用户从 Lightsail 访问组中移除，以撤消他们对 Lightsail 的访问权限，例如，如果他们离开了你的团队但仍在你的公司工作。或者，您可以从 IAM 删除该用户，例如，他们离开您的公司，无需再次访问时。

> **Warning**
>
> 此场景需要 IAM 用户具有编程访问权限和长期凭证，这会带来安全风险。为帮助减轻这种风险，我们建议仅向这些用户提供执行任务所需的权限，并在不再需要这些用户时将其移除。必要时可以更新访问密钥。有关更多信息，请参阅《IAM 用户指南》中的更新访问密钥。

内容

- 为访问 Lightsail 创建一个 IAM 策略
- 创建一个 IAM 群组以获得 Lightsail 访问权限并附上 Lightsail 访问策略
- 创建一个 IAM 用户并将该用户添加到 Lightsail 访问组

为访问 Lightsail 创建一个 IAM 策略

按照以下步骤创建用于 Lightsail 访问的 IAM 策略。有关更多信息，请参阅 IAM 文档中的创建 IAM 策略。

1. 登录 IAM 控制台。
2. 在左侧导航窗格中，选择策略。
3. 请选择创建策略。
4. 在创建策略页面中，选择 JSON 选项卡。



5. 突出显示文本框的内容，然后复制并粘贴以下策略配置文本。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:*"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

结果应该类似于以下示例：

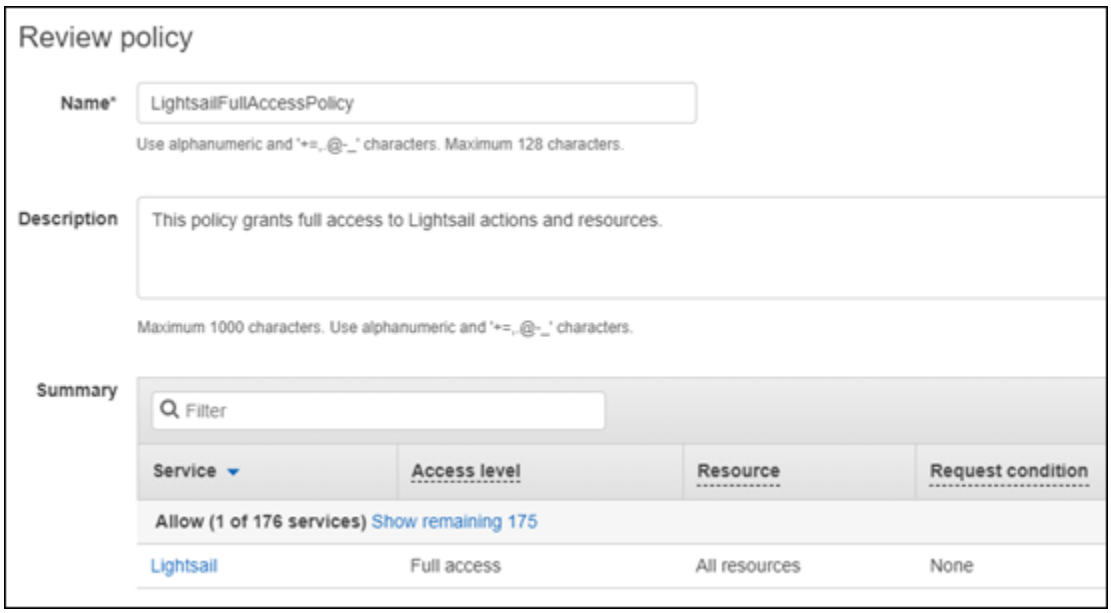


这允许访问所有 Lightsail 操作和资源。需要访问由提供的其他服务的操作（例如启用 VPC 对等互连 AWS、将 Lightsail 快照导出到 EC2亚马逊或使用 Lightsail 创建 EC2 亚马逊资源）需要本政策中未包含的额外权限。有关更多信息，请参阅以下指南：

- 设置亚马逊 VPC 对等互连以使用亚马逊 Lightsail 以外的 AWS 资源
- 将亚马逊 Lightsail 快照导出到亚马逊 EC2
- 在 Lightsail 中 EC2 使用导出的快照创建亚马逊实例

有关您可以授予的操作特定权限和资源特定权限的示例，请参阅 Amazon Lightsail 资源级权限策略示例。

6. 选择 Review Policy（查看策略）。
7. 在查看策略页面中，为策略命名。为它提供描述性名称；例如，`LightsailFullAccessPolicy`。
8. 添加描述，并查看策略设置。如果需要进行更改，请选择上一步来修改策略。



9. 在您确认策略设置正确后，选择创建策略。

   现已创建策略并可将其添加到现有 IAM 组，也可以使用本指南的以下部分中的步骤创建新 IAM 组。

创建一个 IAM 群组以获得 Lightsail 访问权限并附上 Lightsail 访问策略

按照以下步骤创建用于访问 Lightsail 的 IAM 群组，然后附加在本指南上一节中创建的 Lightsail 访问策略。有关更多信息，请参阅 IAM 文档中的创建 IAM 组和将策略附加到 IAM 组。

1. 在 IAM 控制台的左侧导航窗格中，选择组。
2. 选择 Create New Group (创建新组)。
3. 在设置组名页面中，为该组命名。为它提供描述性名称；例如，`LightsailFullAccessGroup`。
4. 在 “附加策略” 页面中，搜索您在本指南前面部分创建的 Lightsail 策略；例如。`LightsailFullAccessPolicy`
5. 在该策略旁边添加复选标记，然后选择下一步。
6. 查看组设置。如果需要进行更改，请选择上一步来修改组策略。
7. 在您确认组设置正确后，选择创建组。

   该群组现已创建，添加到该群组的用户将有权访问 Lightsail 操作和资源。您可以将现有 IAM 用户添加到该组，也可以使用本指南的以下部分中的步骤创建新 IAM 用户。

创建一个 IAM 用户并将该用户添加到 Lightsail 访问组

按照以下步骤创建 IAM 用户并将该用户添加到 Lightsail 访问组。有关更多信息，请参阅 IAM 文档中的在亚马逊云科技账户中创建 IAM 用户和在 IAM 组中添加和删除用户。

1. 在 IAM 控制台的左侧导航窗格中，选择用户。
2. 选择添加用户。
3. 在该页面的 Set user details (设置用户详细信息) 部分中，为用户命名。
4. 在页面的 “选择 AWS 访问类型” 部分下，从以下选项中进行选择：

   a. 选择 “编程访问”，为 AWS API、CLI、SDK 和其他开发工具启用访问密钥 ID 和私有访问密钥，这些工具可用于 Lightsail 操作和资源。有关更多信息，请参阅配置为与 Lightsail 配合使用。 AWS CLI

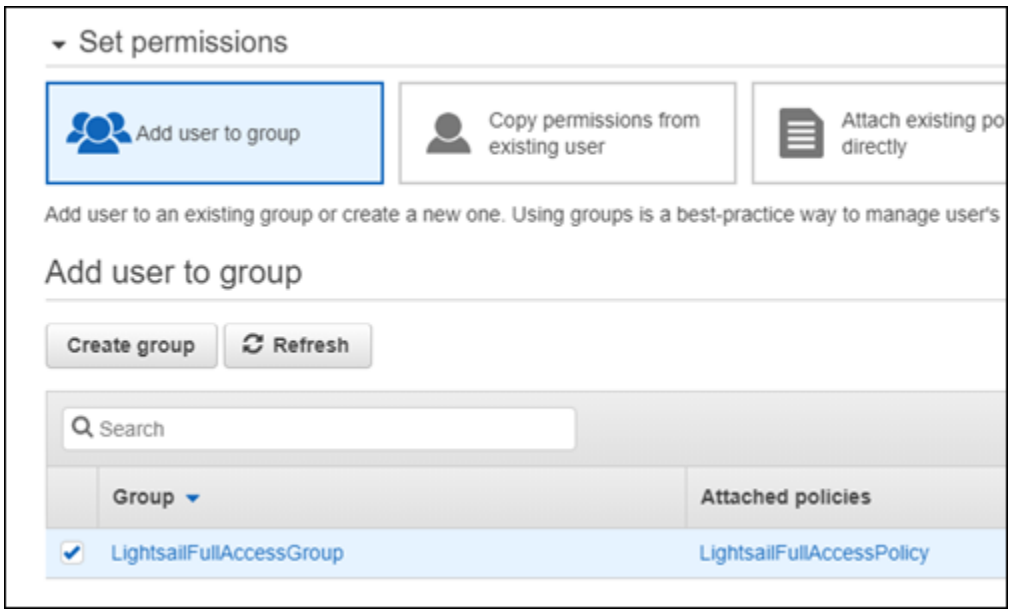
   b. 选择AWS 管理控制台访问权限以启用允许用户登录 AWS 管理控制台的密码，从而登录Lightsail控制台。在选择此选项时，会显示以下密码选项：

      i. 选择自动生成的密码可让 IAM 生成密码，或选择“自定义密码”来输入您自己的密码。

      ii. 选择 Require password reset (需要密码重置) 可让用户在下次登录时创建新密码（重置其密码）。

   > **Note**
   >
   > 如果您仅选择编程访问选项，则用户将无法登录控制台和 Lightsail AWS 控制台。

5. 选择下一步: 权限。
6. 在该页面的 “设置权限” 部分下，选择 “将用户添加到群组”，然后选择您在本指南前面部分创建的 Lightsail 访问组；例如，。`LightsailFullAccessGroup`



7. 选择下一步: 标签。
8. （可选）通过以键值对的形式附加标签来向用户添加元数据。有关在 IAM 中使用标签的更多信息，请参阅“标记 IAM 实体”。
9. 选择 下一步: 审核。
10. 查看用户设置。如果需要进行更改，请选择上一步来修改用户的组或策略。
11. 在您确认用户设置正确后，选择创建用户。

    用户已创建，用户将有权访问 Lightsail。要撤消用户的 Lightsail 访问权限，请将该用户从 Lightsail 访问组中移除。有关更多信息，请参阅 IAM 文档中的在 IAM 组中添加和删除用户。
12. 要获取用户的凭证，请选择以下选项：

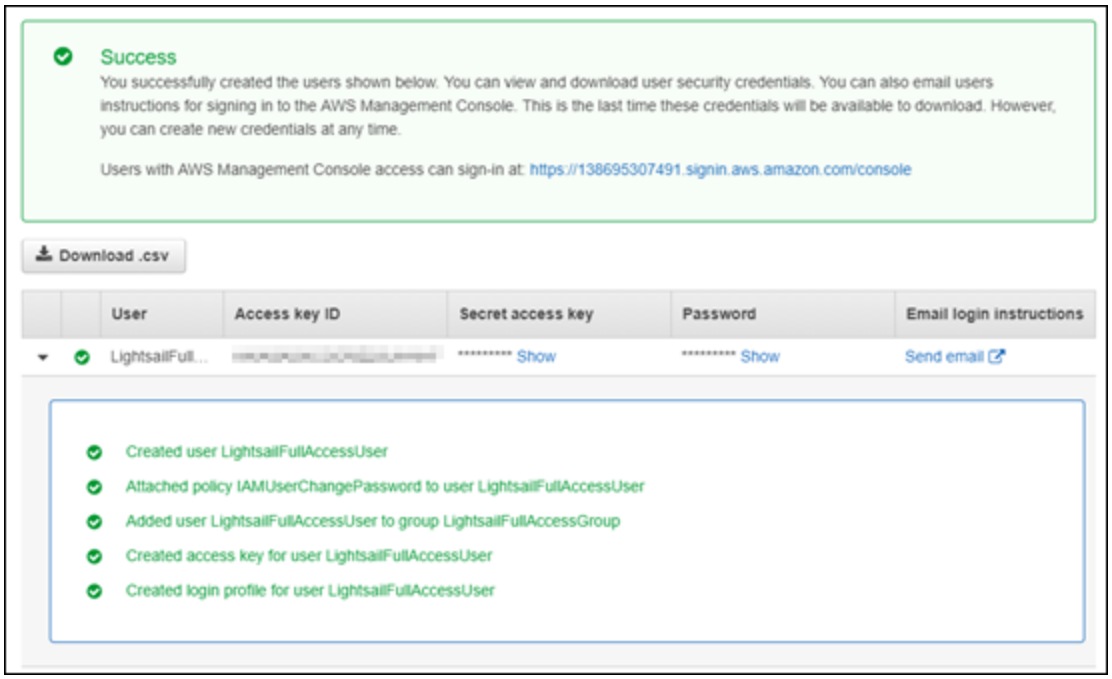
    a. 选择 D ownload .csv 下载包含您账户的用户名、密码、访问密钥 ID、私有访问密钥和 AWS 控制台登录链接的文件。

    b. 选择 “秘密访问密钥” 下方显示，查看可用于以编程方式（使用 API AWS 、CLI、SDK 和其他开发工具）访问 Lightsail 的访问密钥。

> **Important**
>
> 这是您查看或下载私有访问密钥的唯一机会，您必须先向用户提供这些信息，然后他们才能使用 AWS API。将用户的新访问密钥 ID 和秘密访问密钥保存在安全的地方。完成此步骤后，您再也无法访问这些秘密访问密钥。

c. 选择密码下的显示，可查看由 IAM 生成的用户密码。您应向用户提供密码，以便他们可以第一次登录。

d. 选择 “发送电子邮件”，向用户发送一封电子邮件，告知他们现在可以访问 Lightsail。



通过更新管理保障 Lightsail 实例和容器的安全

Amazon Web Services (AWS)、Amazon Lightsail 和第三方应用程序供应商会定期更新和修补 Lightsail 上提供的实例映像（也称为蓝图）。 AWS 而且 Lightsail 不会在您创建实例后更新或修补实例上的操作系统或应用程序。Lightsail 也不会更新或修补你在 Lightsail 容器服务上配置的操作系统和软件。因此，我们建议您定期更新、修补和保护您的 Amazon Lightsail 实例和容器服务上的操作系统和应用程序。有关更多信息，请参阅 AWS 责任共担模式。

实例蓝图软件支持

以下 Amazon Lightsail 平台和蓝图列表链接到每个供应商的支持页面。在那里，您可以查看操作指南等信息，并使操作系统和应用程序保持最新状态。您可以使用任何自动更新服务或建议的过程安装应用程序供应商提供的更新。

Windows

- Windows Server 2022、Windows Server 2019 和 Windows Server 2016
- Microsoft SQL Server

Linux 和 Unix — 仅限操作系统

- Amazon Linux 2023
- Amazon Linux 2
- Ubuntu
- Debian
- FreeBSD
- openSUSE
- CentOS

Linux 和 Unix — 操作系统和应用程序

- Ubuntu 上的 Plesk 托管堆栈
- 适用于 Linux 的 cPanel & WHM
- WordPress
- WordPress多站点
- LAMP (PHP 8)
- Node.js
- Joomla!
- Magento
- MEAN
- Drupal
- GitLab CE
- Redmine
- Nginx
- Ghost
- Django
- PrestaShop

验证 Amazon Lightsail 资源的合规性

AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在上部署以安全性和合规性为重点的基准环境的步骤。 AWS
- AWS 合规资源 — 此工作簿和指南集可能适用于您所在的行业和所在地。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 此 AWS 服务可全面了解您的安全状态 AWS ，帮助您检查是否符合安全行业标准和最佳实践。

使用接口终端节点访问 Amazon Lightsail ()AWS PrivateLink

您可以使用 AWS PrivateLink 在您的 VPC 和 Amazon Lightsail 之间创建私有连接。您可以像在您的 VPC 中一样访问 Amazon Lightsail，无需使用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。您的 VPC 中的实例不需要公有 IP 地址即可访问 Amazon Lightsail。

您可以通过创建由 AWS PrivateLink提供支持的接口端点来建立此私有连接。我们将在您为接口端点启用的每个子网中创建一个端点网络接口。这些是请求者管理的网络接口，用作发往 Amazon Lightsail 的流量的入口点。

有关更多信息，请参阅AWS PrivateLink 指南 AWS PrivateLink中的AWS 服务 直通访问。

亚马逊 Lightsail 的注意事项

在为 Amazon Lightsail 设置接口终端节点之前，必须创建虚拟私有云 (VPC)。有关更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的创建 VPC。此外，请查看AWS PrivateLink 指南中的注意事项。

Amazon Lightsail 支持通过接口终端节点调用其所有 API 操作。有关 Lightsail 可用的 API 操作的更多信息，请参阅亚马逊 Lightsail API 参考。

为 Amazon Lightsail 创建接口终端节点

您可以使用亚马逊 VPC 控制台或 AWS Command Line Interface ()AWS CLI为 Amazon Lightsail 创建接口终端节点。有关更多信息，请参阅《AWS PrivateLink 指南》中的创建接口端点。

使用以下服务名称为 Amazon Lightsail 创建接口终端节点：

```
com.amazonaws.region.lightsail
```

如果您为接口终端节点启用私有 DNS，则可以使用其默认区域 DNS 名称向 Amazon Lightsail 发出 API 请求。例如，`lightsail.us-east-1.amazonaws.com`。有关您可以使用的区域代码，请参阅Lightsail 的区域和可用区。

AWS CLI 例子

要使用接口端点访问 Lightsail，请在命令中使用`--region`和`--endpoint-url`参数。 AWS CLI 有关您可以在 Lightsail 中执行的操作列表，请参阅《亚马逊 Lightsail API 参考》中的操作。

在以下示例中，将 VPC 终端节点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 的 DNS 名称替换 AWS 区域 *us-east-1*为您自己的信息。

示例：使用终端节点 URL 列出 Lightsail 实例

以下示例列出了使用接口终端节点的实例。

```
aws lightsail get-instances --region us-east-1 --endpoint-url
 https://vpce-1a2b3c4d-5e6f.lightsail.us-east-1.vpce.amazonaws.com
```

示例：使用终端节点 URL 列出 Lightsail 磁盘

以下示例使用接口终端节点列出了您的磁盘。

```
aws lightsail get-disks --region us-east-1 --endpoint-url
 https://vpce-1a2b3c4d-5e6f.lightsail.us-east-1.vpce.amazonaws.com
```

为接口端点创建端点策略

端点策略是一种 IAM 资源，您可以将其附加到接口端点。默认终端节点策略允许通过接口终端节点对 Amazon Lightsail 进行完全访问。要控制允许从您的 VPC 访问 Amazon Lightsail 的权限，请将自定义终端节点策略附加到接口终端节点。

端点策略指定以下信息：

- 可执行操作的主体（AWS 账户、IAM 用户和 IAM 角色）。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《AWS PrivateLink 指南》中的使用端点策略控制对服务的访问权限。

示例：亚马逊 Lightsail 操作的 VPC 终端节点策略

以下是自定义端点策略的示例。当您将此策略附加到接口终端节点时，它会拒绝所有人通过终端节点删除 Lightsail 中的块存储磁盘的权限，并授予所有人执行所有其他 Lightsail 操作的权限。

```
{
  "Statement": [
    {
      "Action": "lightsail:*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    },
    {
      "Action": "lightsail:DeleteDisk",
      "Effect": "Deny",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

监控你的 Lightsail 资源指标

通过检查和收集指标数据，监控 Amazon Lightsail 中的实例、数据库、分配、负载均衡器、容器服务和存储桶的性能。建立一个时段内的基准，以便您能够配置告警，从而更轻松地检测有关资源性能的异常和问题。

Amazon Lightsail 报告实例、数据库、内容分发网络 (CDN) 分配、负载均衡器、容器服务和存储桶的指标数据。您可以在 Lightsail 控制台中查看和监控这些数据。监控是维护资源的可靠性、可用性和性能的重要环节。定期监控和收集资源中的指标数据，以便您能够更轻松地调试多点故障（如果发生）。

内容

- 有效地监控您的资源
- 指标的概念和术语
- Lightsail 中提供的指标

有效地监控您的资源

您应为环境中的正常资源性能建立基准。在不同时间和不同负载条件下测量性能。在监控您的资源时，您应记下并记录一段时间内的资源性能的历史记录。将资源的当前性能与您收集到的历史数据进行比较。这将帮助您确定一般的性能模式和性能异常，并设计方法来解决它们。

例如，您可以监控实例的 CPU 利用率、网络使用率和状态检查。如果性能低于您所建立的基准，则您可能需要重新配置或优化实例以降低 CPU 使用率或减少网络流量。如果您的实例继续运行在 CPU 使用率阈值之上，则可能需要为实例切换到更大的套餐（使用 7 美元的USD/month plan instead of the $5 USD/month套餐）。可以通过为实例创建一个新快照，然后使用更大的计划从该快照创建新的实例来切换到更大的计划。

建立基准后，您可以在 Lightsail 控制台中配置警报，以便在资源超过指定阈值时通知您。有关更多信息，请参阅通知和警报。

指标的概念和术语

以下术语和概念可帮助您更好地理解 Lightsail 中指标的用法。

Metrics

指标代表一个按时间顺序排列的数据点集。可将指标视为要监控的变量，而数据点代表该变量随时间变化的值。指标通过一个名称唯一定义。例如，Lightsail 提供的一些实例指标包括 CPU 利用率 (CPUUtilization)、传入网络流量 (NetworkIn) 和传出网络流量 (NetworkOut)。有关 Lightsail 中所有可用资源指标的更多信息，请参阅 Lightsail 中的可用指标。

指标保留

时间段为 60 秒（1 分钟解析时间）的数据点可用 15 天。时间段为 300 秒（5 分钟解析时间）的数据点可用 63 天。时间段为 3600 秒（1 小时解析时间）的数据点可用 455 天（15 个月）。

最初以较短时间段提供的数据点汇总在一起，可实现长期存储。例如，具有 1 分钟粒度的数据点在 15 天内保持可用（1 分钟解析时间）。15 天之后，此数据仍可用，但汇总在一起，只能以 5 分钟的精度检索。63 天之后，数据进一步汇总，以 1 小时的精度提供。如果您需要超过这些时间段的指标可用性，则可以使用 Lightsail API、 AWS Command Line Interface (AWS CLI) 和 SDKs 来检索用于离线存储或其他存储的数据点。

有关更多信息 GetInstanceMetricData，请参阅 Lightsail API 参考GetRelationalDatabaseMetricData中的GetBucketMetricDataGetLoadBalancerMetricDataGetDistributionMetricData、、、和。

统计信息

指标统计数据是在一段时间内聚合数据的方法。示例统计数据包括 Average、Sum 和 Maximum。例如，可以使用 Average 统计数据取实例 CPU 利用率指标数据的平均值，可以使用 Sum 统计数据添加数据库连接，可以使用 Maximum 统计数据检索最大负载均衡器响应时间，依此类推。

有关可用指标统计信息的列表，请参阅 Lightsail API 参考 GetRelationalDatabaseMetricData中的统计信息 GetLoadBalancerMetricData GetDistributionMetricData、统计信息、统计数据和统计信息。 GetInstanceMetricData GetBucketMetricData

单位

所有统计数据都有度量单位。示例单位包括 Bytes、Seconds、Count 和 Percent。有关单位的完整列表，请参阅 Lightsail API 参考 GetRelationalDatabaseMetricData中的单位 GetDistributionMetricData、单位和单位。 GetInstanceMetricData GetLoadBalancerMetricData

时间段

时间段是与特定数据点关联的时间长度，即返回的数据点的粒度。每个数据点代表在指定时间段内对收集的指标数据的聚合。时间段以秒为单位定义，时间段的有效值是 60 秒（1 分钟）和 300 秒（5 分钟）的任意倍数。

使用 Lightsail API 检索数据点时，可以指定周期、开始时间和结束时间。这些参数决定了与数据点关联的时间的总长度。Lightsail 以 1 分钟或 5 分钟为增量报告指标数据；因此，您必须以 60 秒和 300 秒的倍数指定周期。您为开始时间和结束时间指定的值决定 Lightsail 返回的周期数。如果您想要以 10 分钟为一块来聚合统计信息，请指定时间段 600。对于一个完整小时内聚合的统计数据，请指定时间段 3600，依此类推。

时段对于 Lightsail 警报也很重要。Lightsail 每 5 分钟评估一次警报的数据点，警报的每个数据点代表 5 分钟的聚合数据周期。当您创建用于监控特定指标的警报时，您是在要求 Lightsail 将该指标与您指定的阈值进行比较。你可以广泛控制 Lightsail 如何进行这种比较。您可以指定进行比较的时间段，并且可以指定用于得出结论的评估时间段的数量。有关更多信息，请参阅警报。

警报

告警将在指定时间段内监控单个指标，并在指标超过您指定的阈值时通知您。通知可以是显示在 Lightsail 控制台中的横幅、发送到您指定的电子邮件地址的电子邮件以及发送到您指定的手机号码的 SMS 短信。有关更多信息，请参阅警报。

Lightsail 中提供的指标

实例指标

提供了以下实例指标。有关更多信息，请参阅在 Amazon Lightsail 中查看实例指标。

- CPU 利用率 (**CPUUtilization**) – 是当前正在实例上使用的已分配计算单位的百分率。此指标用于确定在实例上运行应用程序的处理能力。当未为实例分配完整的处理器内核时，操作系统中的工具显示的百分比可能低于 Lightsail。

  在 Lightsail 控制台中查看实例的 CPU 利用率指标图表时，您将看到可持续和可突发区域。有关这些区域的含义的更多信息，请参阅 CPU 利用率可持续区域和可突增区域。
- 容量暴增分钟数 (**BurstCapacityTime**) 和百分比 (**BurstCapacityPercentage**) – 容量暴增分钟数表示实例以 100% CPU 利用率暴增的可用时间。容量暴增百分比是您的实例可用的 CPU 性能百分比。您的实例会持续消耗和累积突增容量。仅当您的实例以 100% CPU 利用率运行时，容量暴

增分钟数才会以全速率消耗。有关实例突增容量的更多信息，请参阅在 Amazon Lightsail 中查看实例突增容量。

- 传入网络流量 (**NetworkIn**) – 实例在所有网络接口上收到的字节数。此指标用于确定流向实例的传入网络流量。报告的数量是该期间内接收的字节数。由于此指标每 5 分钟报告一次，因此将报告的数量除以 300 来得出字节/秒。
- 传出网络流量 (**NetworkOut**) – 实例在所有网络接口上发出的字节数。此指标用于确定来自实例的传出网络流量。报告的数字是该时间段内发送的字节数。由于此指标每 5 分钟报告一次，因此将报告的数量除以 300 来得出字节/秒。
- 状态检查故障 (**StatusCheckFailed**) – 报告通过还是未通过实例状态检查和系统状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 实例状态检查故障 (**StatusCheckFailed_Instance**) – 报告实例通过还是未通过实例状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 系统状态检查故障 (**StatusCheckFailed_System**) – 报告实例通过还是未通过系统状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 没有令牌元数据请求 (**MetadataNoToken**) – 在没有令牌的情况下成功访问实例元数据服务的次数。该指标确定是否有任何进程正在使用实例元数据服务版本 1 访问实例元数据，但未使用令牌。如果所有请求都使用支持令牌的会话（如实例元数据服务版本 2），则该值为 0。有关更多信息，请参阅 Amazon Lightsail 中的实例元数据和用户数据。

数据库指标

提供了以下数据库指标。有关更多信息，请参阅在 Amazon Lightsail 中查看数据库指标。

- CPU 利用率 (**CPUUtilization**) – 数据库当前使用的 CPU 利用率的百分比。
- 数据库连接数 (**DatabaseConnections**) – 正在使用的数据库连接数。
- 磁盘队列深度 (**DiskQueueDepth**)-等待访问磁盘的未处理 IOs （读/写请求）的数量。
- 可用存储空间 (**FreeStorageSpace**) – 可用存储空间的大小。
- 网络接收吞吐量 (**NetworkReceiveThroughput**) – 数据库的传入（接收）网络流量，包括客户数据库流量和用于监控和复制的 AWS 流量。
- 网络传输吞吐量 (**NetworkTransmitThroughput**) – 数据库的传出（传输）网络流量，包括客户数据库流量和用于监控和复制的 AWS 流量。

分配指标

提供以下分配指标：有关更多信息，请参阅在 Amazon Lightsail 中查看配送指标。

- 请求数 (**Requests**) – 分配收到的查看器请求总数，针对所有 HTTP 方法以及 HTTP 和 HTTPS 请求。
- 已上传的字节数 (**BytesUploaded**) – 分配使用 POST 和 PUT 请求上传到源的字节数。
- 已下载的字节数 (**BytesDownloaded**) – 查看器针对 GET、HEAD 和 OPTIONS 请求下载的字节数。
- 错误率总计 (**TotalErrorRate**) – 响应的 HTTP 状态代码为 4xx 或 5xx 的所有查看器请求所占的百分比。
- HTTP 4xx 错误率 (**4xxErrorRate**) – 响应的 HTTP 状态代码为 4xx 的所有查看器请求所占的百分比。在这些情况下，客户端或客户端查看器可能出现了错误。例如，404（未找到）状态代码表示无法找到客户端请求的对象。
- HTTP 5xx 错误率 (**5xxErrorRate**) – 响应的 HTTP 状态代码为 5xx 的所有查看器请求所占的百分比。在这些情况下，源服务器未满足请求。例如，503（服务不可用）状态代码表示源服务器当前不可用。

负载均衡器指标

提供了以下负载均衡器指标。有关更多信息，请参阅在 Amazon Lightsail 中查看负载均衡器指标。

- 正常主机计数 (**HealthyHostCount**) – 被视为正常运行的目标实例数。
- 不正常主机计数 (**UnhealthyHostCount**) – 被视为未正常运行的目标实例数。
- 负载均衡器 HTTP 4XX (**HTTPCode_LB_4XX_Count**) – 源自负载均衡器的 HTTP 4XX 客户端错误代码的数量。如果请求格式错误或不完整，则会生成客户端错误。目标实例未收到这些请求。该计数不包含目标实例生成的响应代码。
- 负载均衡器 HTTP 5XX (**HTTPCode_LB_5XX_Count**) – 源自负载均衡器的 HTTP 5XX 服务器错误代码的数量。这不包含由目标实例生成的任何响应代码。如果没有运行正常的实例附加到负载均衡器，或者请求速率超过实例或负载均衡器的容量（溢出），则会报告该指标。
- 实例 HTTP 2XX (**HTTPCode_Instance_2XX_Count**) – 由目标实例生成的 HTTP 2XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例 HTTP 3XX (**HTTPCode_Instance_3XX_Count**) – 由目标实例生成的 HTTP 3XX 响应代码数。它不包括负载均衡器生成的任何响应代码。

- 实例 HTTP 4XX (**HTTPCode_Instance_4XX_Count**) – 由目标实例生成的 HTTP 4XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例 HTTP 5XX (**HTTPCode_Instance_5XX_Count**) – 由目标实例生成的 HTTP 5XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例响应时间 (**InstanceResponseTime**) – 从请求离开负载均衡器到从目标实例收到响应之间所用的时间（以秒为单位）。
- 客户端 TLS 协商错误计数 (**ClientTLSNegotiationErrorCount**) – 由于负载均衡器生成 TLS 错误而未与负载均衡器建立会话的客户端发起的 TLS 连接数。可能的原因包括密码或协议不匹配。
- 请求计数 (**RequestCount**)-已处理的请求数 IPv4。该计数仅包含具有负载均衡器的目标实例生成的响应的请求。
- 已被拒绝的连接计数 (**RejectedConnectionCount**) – 由于负载均衡器达到连接数上限被拒绝的连接的数量。

容器服务指标

提供以下容器服务指标：有关更多信息，请参阅查看容器服务指标。

- CPU 利用率 (**CPUUtilization**) – 容器服务的所有节点当前正在使用的计算单位的平均百分比。此指标标识在容器服务上运行容器所需的处理能力。
- 内存利用率 (**MemoryUtilization**) – 容器服务的所有节点当前正在使用的内存的平均百分比。此指标确定在容器服务上运行容器所需的内存。

存储桶指标

提供以下存储桶指标 ：有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶指标。

- 存储桶大小 (**BucketSizeBytes**) – 桶中存储的数据量。此值通过汇总存储桶中所有对象（当前对象和非当前对象）的大小计算得出，包括所有向存储桶进行分段上传而未完成的所有部分的大小。
- 对象的数量 (**NumberOfObjects**) – 桶中存储的对象总数。此值通过对存储桶中所有对象（当前对象和非当前对象）以及所有向存储桶进行分段上传而未完成的所有部分的总数进行计数而计算得出。

> **Note**
>
> 存储桶为空时，不会报告存储桶指标数据。

使用运行状况指标监控 Lightsail 资源

您可以在不同时间段内查看以下 Amazon Lightsail 资源指标。有关 Lightsail 中资源指标的更多信息，请参阅资源指标。

实例指标

提供了以下实例指标。有关更多信息，请参阅在 Amazon Lightsail 中查看实例指标。

- CPU 利用率 (**CPUUtilization**) – 是当前正在实例上使用的已分配计算单位的百分率。此指标用于确定在实例上运行应用程序的处理能力。当未为实例分配完整的处理器内核时，操作系统中的工具显示的百分比可能低于 Lightsail。

  在 Lightsail 控制台中查看实例的 CPU 利用率指标图表时，您将看到可持续和可突发区域。有关这些区域的含义的更多信息，请参阅 CPU 利用率可持续区域和可突增区域。
- 容量暴增分钟数 (**BurstCapacityTime**) 和百分比 (**BurstCapacityPercentage**) – 容量暴增分钟数表示实例以 100% CPU 利用率暴增的可用时间。容量暴增百分比是您的实例可用的 CPU 性能百分比。您的实例会持续消耗和累积突增容量。仅当您的实例以 100% CPU 利用率运行时，容量暴增分钟数才会以全速率消耗。有关实例容量暴增的更多信息，请参阅查看实例容量暴增。
- 传入网络流量 (**NetworkIn**) – 实例在所有网络接口上收到的字节数。此指标用于确定流向实例的传入网络流量。报告的数量是该期间内接收的字节数。由于此指标每 5 分钟报告一次，因此将报告的数量除以 300 来得出字节/秒。
- 传出网络流量 (**NetworkOut**) – 实例在所有网络接口上发出的字节数。此指标用于确定来自实例的传出网络流量。报告的数字是该时间段内发送的字节数。由于此指标每 5 分钟报告一次，因此将报告的数量除以 300 来得出字节/秒。
- 状态检查故障 (**StatusCheckFailed**) – 报告通过还是未通过实例状态检查和系统状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 实例状态检查故障 (**StatusCheckFailed_Instance**) – 报告实例通过还是未通过实例状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 系统状态检查故障 (**StatusCheckFailed_System**) – 报告实例通过还是未通过系统状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 系统状态检查故障 (**StatusCheckFailed_System**) – 报告实例通过还是未通过系统状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 没有令牌元数据请求 (**MetadataNoToken**) – 在没有令牌的情况下成功访问实例元数据服务的次数。该指标确定是否有任何进程正在使用实例元数据服务版本 1 访问实例元数据，但未使用令牌。如果

所有请求都使用支持令牌的会话（如实例元数据服务版本 2），则该值为 0。有关更多信息，请参阅实例元数据和用户数据。

数据库指标

提供了以下数据库指标。有关更多信息，请参阅查看数据库指标。

- CPU 利用率 (**CPUUtilization**) – 数据库当前使用的 CPU 利用率的百分比。
- 数据库连接数 (**DatabaseConnections**) – 正在使用的数据库连接数。
- 磁盘队列深度 (**DiskQueueDepth**)-等待访问磁盘的未处理 IOs （读/写请求）的数量。
- 可用存储空间 (**FreeStorageSpace**) – 可用存储空间的大小。
- 网络接收吞吐量 (**NetworkReceiveThroughput**) – 数据库的传入（接收）网络流量，包括客户数据库流量和用于监控和复制的 AWS 流量。
- 网络传输吞吐量 (**NetworkTransmitThroughput**) – 数据库的传出（传输）网络流量，包括客户数据库流量和用于监控和复制的 AWS 流量。

分配指标

提供以下分配指标：有关更多信息，请参阅在 Amazon Lightsail 中查看配送指标。

- 请求数 – 分配收到的查看器请求总数，针对所有 HTTP 方法以及 HTTP 和 HTTPS 请求。
- 已上传字节 – 分配使用 POST 和 PUT 请求上传到源的字节数。
- 已下载字节 – 查看器针对 GET、HEAD 和 OPTIONS 请求下载的字节数。
- 总错误率 – 响应的 HTTP 状态代码为 4xx 或 5xx 的所有查看器请求所占的百分比。
- HTTP 4xx 错误率 – 响应的 HTTP 状态代码为 4xx 的所有查看器请求所占的百分比。在这些情况下，客户端或客户端查看器可能出现了错误。例如，404（未找到）状态代码表示无法找到客户端请求的对象。
- HTTP 5xx 错误率 – 响应的 HTTP 状态代码为 5xx 的所有查看器请求所占的百分比。在这些情况下，源服务器未满足请求。例如，503（服务不可用）状态代码表示源服务器当前不可用。

负载均衡器指标

提供了以下负载均衡器指标。有关更多信息，请参阅查看负载均衡器指标。

- 正常主机计数 (**HealthyHostCount**) – 被视为正常运行的目标实例数。
- 不正常主机计数 (**UnhealthyHostCount**) – 被视为未正常运行的目标实例数。
- 负载均衡器 HTTP 4XX (**HTTPCode_LB_4XX_Count**) – 源自负载均衡器的 HTTP 4XX 客户端错误代码的数量。如果请求格式错误或不完整，则会生成客户端错误。目标实例未收到这些请求。该计数不包含目标实例生成的响应代码。
- 负载均衡器 HTTP 5XX (**HTTPCode_LB_5XX_Count**) – 源自负载均衡器的 HTTP 5XX 服务器错误代码的数量。这不包含由目标实例生成的任何响应代码。如果没有运行正常的实例附加到负载均衡器，或者请求速率超过实例或负载均衡器的容量（溢出），则会报告该指标。
- 实例 HTTP 2XX (**HTTPCode_Instance_2XX_Count**) – 由目标实例生成的 HTTP 2XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例 HTTP 3XX (**HTTPCode_Instance_3XX_Count**) – 由目标实例生成的 HTTP 3XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例 HTTP 4XX (**HTTPCode_Instance_4XX_Count**) – 由目标实例生成的 HTTP 4XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例 HTTP 5XX (**HTTPCode_Instance_5XX_Count**) – 由目标实例生成的 HTTP 5XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例响应时间 (**InstanceResponseTime**) – 从请求离开负载均衡器到从目标实例收到响应之间所用的时间（以秒为单位）。
- 请求计数 (**RequestCount**)-已处理的请求数 IPv4。该计数仅包含具有负载均衡器的目标实例生成的响应的请求。
- 客户端 TLS 协商错误计数 (**ClientTLSNegotiationErrorCount**) – 由于负载均衡器生成 TLS 错误而未与负载均衡器建立会话的客户端发起的 TLS 连接数。可能的原因包括密码或协议不匹配。
- 已被拒绝的连接计数 (**RejectedConnectionCount**) – 由于负载均衡器达到连接数上限被拒绝的连接的数量。

容器服务指标

提供以下容器服务指标：有关更多信息，请参阅查看容器服务指标。

- CPU 利用率 — 容器服务的所有节点当前正在使用的计算单位的平均百分比。此指标标识在容器服务上运行容器所需的处理能力。
- 内存利用率 — 容器服务的所有节点当前正在使用的内存的平均百分比。此指标确定在容器服务上运行容器所需的内存。

存储桶指标

提供以下存储桶指标 ：有关更多信息，请参阅查看存储桶指标。

- Bucket size（存储桶大小）— 存储桶中存储的数据量。此值通过汇总存储桶中所有对象（当前对象和非当前对象）的大小计算得出，包括所有向存储桶进行分段上传而未完成的所有分段的大小。
- Number of objects（对象数）— 存储桶中存储的对象总数。此值通过对存储桶中所有对象（当前对象和非当前对象）以及所有向存储桶进行分段上传而未完成的所有分段的总数进行计数而计算得出。

> **Note**
>
> 存储桶为空时，不会报告存储桶指标数据。

主题

- 为 Lightsail 资源配置指标通知
- 使用指标监控 Lightsail 实例的性能
- Lightsail 中的指标警报
- 创建 Lightsail 实例指标警报
- 删除或禁用 Lightsail 指标警报

为 Lightsail 资源配置指标通知

您可以将 Lightsail 配置为在您的某个实例、数据库、负载均衡器或内容分发网络 (CDN) 分布的指标超过指定阈值时通知您。通知的形式可以是 Lightsail 控制台中显示的横幅、发送到您指定地址的电子邮件或发送到您指定的手机号码的 SMS 短信。有关如何查看待验证的联系人是否有通知的更多信息，请参阅查看待验证的电子邮件联系人。

要获取通知，您必须配置告警来监视某个资源指标。例如，您可以配置一个告警，当实例的传出网络流量在指定时长内超过 500 KB 时通知您。有关更多信息，请参阅指标告警。

触发警报后，Lightsail 控制台中会显示一条通知横幅。要通过电子邮件和短信收到通知，您必须将您的电子邮件地址和手机号码添加为要监控资源的每个 AWS 区域 位置的通知联系人。有关更多信息，请参阅添加通知联系人。

> **Note**
>
> 并非所有可以创建 Light AWS 区域 sail 资源的系统都支持短信，并且无法向世界上某些国家和地区发送短信。有关更多信息，请参阅添加通知联系人。

如果您在预期收到通知时没有收到通知，请检查确认您的通知联系人是否正确配置。要了解更多信息，请参阅排除通知的故障。

要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除或禁用指标警报。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

使用指标监控 Lightsail 实例的性能

在 Amazon Lightsail 中启动实例后，您可以在实例管理页面的指标选项卡上查看其指标图表。监控指标是维护资源的可靠性、可用性和性能的重要环节。定期监控和收集资源中的指标数据，以便您能够更轻松地调试多点故障（如果发生）。有关指标的更多信息，请参阅 Amazon Lightsail 中的指标。

在监控资源时，应为环境中的正常资源性能建立基准。然后，您可以在 Lightsail 控制台中配置告警，以便在资源性能超出指定阈值时通知您。有关更多信息，请参阅通知和警报。

内容

- Lightsail 中提供的实例指标
- CPU 利用率可持续区域和可突增区域
- 在 Lightsail 控制台中查看实例指标
- 查看实例指标后的后续步骤

可用的实例指标

提供了以下实例指标：

- CPU 利用率 (**CPUUtilization**) – 是当前正在实例上使用的已分配计算单位的百分率。此指标用于确定在实例上运行应用程序的处理能力。当未为实例分配完整的处理器内核时，操作系统中的工具显示的百分比可能低于 Lightsail。

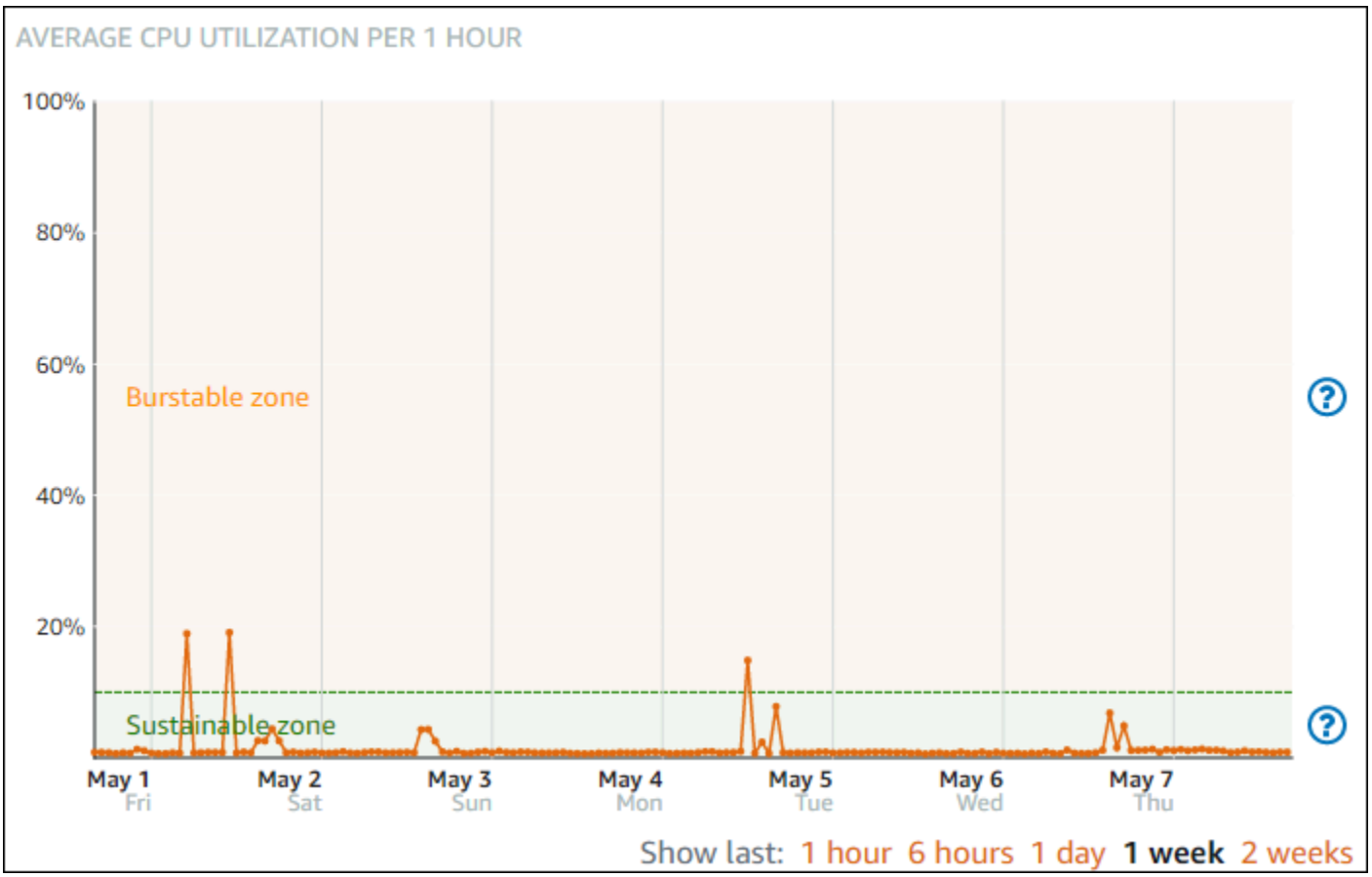
  在 Lightsail 控制台中查看实例的 CPU 利用率指标图表时，您将看到可持续和可突发区域。有关这些区域的含义的更多信息，请参阅 CPU 利用率可持续区域和可突增区域。

- 容量暴增分钟数 (**BurstCapacityTime**) 和百分比 (**BurstCapacityPercentage**) – 容量暴增分钟数表示实例以 100% CPU 利用率暴增的可用时间。容量暴增百分比是您的实例可用的 CPU 性能百分比。您的实例会持续消耗和累积突增容量。仅当您的实例以 100% CPU 利用率运行时，容量暴增分钟数才会以全速率消耗。有关实例容量暴增的更多信息，请参阅查看实例容量暴增。
- 传入网络流量 (**NetworkIn**) – 实例在所有网络接口上收到的字节数。此指标用于确定流向实例的传入网络流量。报告的数量是该期间内接收的字节数。由于此指标每 5 分钟报告一次，因此将报告的数量除以 300 来得出字节/秒。
- 传出网络流量 (**NetworkOut**) – 实例在所有网络接口上发出的字节数。此指标用于确定来自实例的传出网络流量。报告的数字是该时间段内发送的字节数。由于此指标每 5 分钟报告一次，因此将报告的数量除以 300 来得出字节/秒。
- 状态检查故障 (**StatusCheckFailed**) – 报告通过还是未通过实例状态检查和系统状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 实例状态检查故障 (**StatusCheckFailed_Instance**) – 报告实例通过还是未通过实例状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 系统状态检查故障 (**StatusCheckFailed_System**) – 报告实例通过还是未通过系统状态检查。此指标可以是 0（通过）或 1（失败）。此指标按 1 分钟一次的频率提供。
- 没有令牌元数据请求 (**MetadataNoToken**) – 在没有令牌的情况下成功访问实例元数据服务的次数。该指标确定是否有任何进程正在使用实例元数据服务版本 1 访问实例元数据，但未使用令牌。如果所有请求都使用支持令牌的会话（如实例元数据服务版本 2），则该值为 0。有关更多信息，请参阅实例元数据和用户数据。

CPU 利用率可持续区域和可突增区域

Lightsail 使用可突发实例，这些实例可提供基准 CPU 性能，但也能够根据需要临时提供高于基准的额外 CPU 性能。这被称为突增。对于可突增的实例，您不必过度预配置实例来处理偶尔的性能峰值，因此您不必为从未使用的容量付费。

在实例的 CPU 利用率指标图表上，您将看到一个可持续区域和一个可突增区域。您的 Lightsail 实例可以在可持续区域中无限期地运行，而不会影响系统的运行。



您的实例可能会在负载较重的情况下在可突增区域中开始运行，例如编译代码、安装新软件、运行批处理作业或满足峰值负载请求时。在可突增区域内运行时，您的实例会消耗更多的 CPU 周期。因此，它只能在此区域内运行一段有限的时间。

您的实例可以在可突增区域内运行的时段取决于它在可突增区域内的深度。与在可突增区域的较高端运行的实例相比，在可突增区域的较低端运行的实例的突增时段可能会更长。但是，已在可突增区域内的任何位置持续一段时间的实例最终将耗尽所有 CPU 容量，直到它再次在可持续区域内运行。

监控实例的 CPU 利用率指标，以了解其性能在可持续区域和可突增区域之间的分配方式。如果您的系统只是偶尔进入可突增区域，您应能够继续使用您正在运行的实例。但是，如果您看到您的实例在突发区域中花费了大量时间，则可能需要为您的实例切换到更大的套餐（使用 12 美元的USD/month plan instead of the $5 USD/month套餐）。可以通过为实例创建一个新快照，然后从该快照创建新的实例来切换到更大的计划。

在 Lightsail 控制台中查看实例指标

完成以下步骤，即可在 Lightsail 控制台中查看实例指标。

1. 登录 Lightsail 控制台。

2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择所需实例的名称，以查看其指标。
4. 选择实例管理页面上的 Metrics（指标）选项卡。
5. 在 Metrics graphs（指标图表）标题下的下拉菜单中，选择要查看的指标。

   该图表显示所选指标的数据点的直观表示形式。

   > **Note**
   >
   > 在 Lightsail 控制台中查看实例的 CPU 利用率指标图表时，您将看到可持续和可突发区域。有关这些区域的更多信息，请参阅 CPU 利用率可持续区域和可突增区域。

6. 您可以对指标图表执行以下操作：
   - 更改图表的视图以显示 1 小时、6 小时、1 天、1 周和 2 周的数据。
   - 将光标停在一个数据点上可查看有关该数据点的详细信息。
   - 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅警报和创建实例指标警报。

后续步骤

对于实例指标，有其他几项可执行的任务：

- 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅指标警报和创建实例指标警报。
- 触发警报后，Lightsail 控制台中会显示一条通知横幅。要通过电子邮件和短信收到通知，您必须将您的电子邮件地址和手机号码添加为要监控资源的每个 AWS 区域 位置的通知联系人。有关更多信息，请参阅添加通知联系人。
- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除或禁用指标警报。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

Lightsail 中的指标警报

您可以在 Amazon Lightsail 中创建警报，监控您的实例、数据库、负载均衡器和内容分发网络 (CDN) 分布的单个指标。可以将警报配置为根据您指定了阈值的指标值来向您发送通知。通知可以是显示在

Lightsail 控制台中的横幅、发送到您的电子邮件地址的电子邮件以及发送到您的手机号码的 SMS 短信。在本指南中，我们将介绍您可以配置的告警条件和设置。有关如何查看所有 Lightsail 资源的活动警报的更多信息，请参阅。查看警报通知以了解活动警报

内容

- 配置警报
- 告警状态
- 告警示例
- 配置警报如何处理缺失数据
- 在数据缺失时如何评估告警状态
- 图形示例中的缺失数据
- 有关告警的更多信息

配置告警

要在 Lightsail 控制台中添加警报，请浏览至您的实例、数据库、负载均衡器或 CDN 分发的 “指标” 选项卡。然后选择要监控的指标，再选择添加告警。您可以为每个指标添加两个告警。有关指标的更多信息，请参阅资源指标。

要配置告警，首先要确定一个阈值，该指标值是告警改变状态的点（例如，从 OK 状态变为 ALARM 状态，反之亦然）。有关更多信息，请参阅告警状态。然后选择一个比较运算符，该运算符将用于比较指标与阈值。可使用的运算符为大于或等于、大于、小于以及小于或等于。

然后，您可以指定警报改变状态必须超过阈值的次数与评估指标的时段。Lightsail 每 5 分钟评估一次警报的数据点，每个数据点代表一段 5 分钟的聚合数据。例如，如果您指定当阈值超过 2 次时触发的告警，则评估期必须为过去 10 分钟或更长时间（最多 24 小时）。如果您指定当阈值超过 10 次时触发的告警，则评估期必须为过去 50 分钟或更长时间（最多 24 小时）。

配置告警条件后，您可以配置进行通知的方式。当警报从状态变为OK状态时，通知横幅始终显示在 Lightsail 控制台中ALARM。您也可以选择通过电子邮件和 SMS 文本消息进行通知，但必须配置相应的联系人。有关更多信息，请参阅指标通知。如果您选择通过电子邮件和/或 SMS 文本消息进行通知，您也可以选择在告警状态从 ALARM 状态变为 OK 状态时通知，其被视为是全部清除通知。

在警报的高级设置中，您可以选择 Lightsail 如何处理缺失的指标数据。有关更多信息，请参阅配置警报如何处理缺失数据。

告警状态

告警始终处于以下状态之一：

- 警报：指标在规定的阈值范围外。

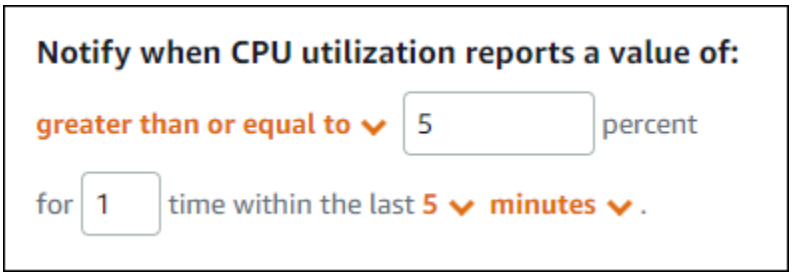
  例如，如果您选择大于比较运算符，告警将在指标大于指定阈值时为 ALARM 状态。如果您选择小于比较运算符，告警将在指标小于指定阈值时为 ALARM 状态。
- 正常：指标在规定的阙值范围内。

  例如，如果您选择大于比较运算符，告警将在指标小于指定阈值时为 OK 状态。如果您选择小于比较运算符，告警将在指标大于指定阈值时为 OK 状态。
- 数据不足：警报刚刚开始、指标不可用或没有足够的指标数据供警报来确定警报状态。

告警仅在状态改变时触发。警报不会仅仅因为其处于颗粒状态而触发，状态必须已更改。触发警报后，Lightsail 控制台中会显示一条横幅。您还可以配置告警以通过电子邮件和 SMS 文本消息进行通知。

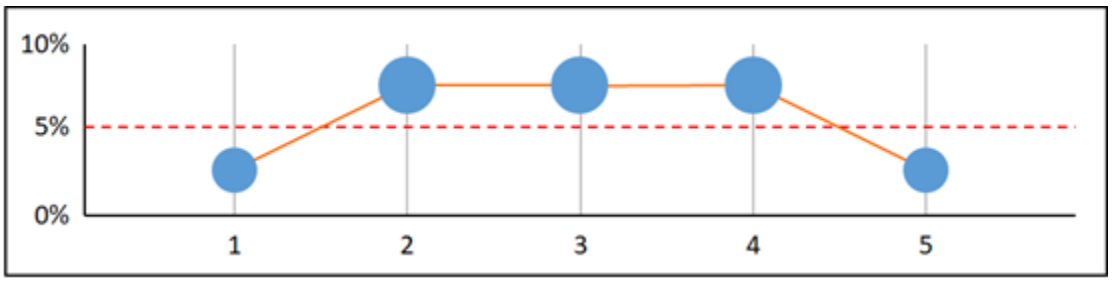
告警示例

根据之前描述的告警条件，您可以配置一个告警，当实例的 CPU 使用率在一个 5 分钟的时段内有一次大于或等于 5% 时，便进入 ALARM 状态。以下示例显示了 Lightsail 控制台中此警报的设置。



在此示例中，如果实例的 CPU 使用率指标仅报告一个数据点的使用率为 5% 或以上，则告警将从 OK 状态变为 ALARM 状态。后续数据点报告使用率为 5% 或以上会将告警保持在 ALARM 状态。在如果实例的 CPU 使用率指标仅报告一个数据点的使用率为 4.9% 或以下，则告警将从 ALARM 状态变为 OK 状态。

下图进一步说明了此告警。红色虚线表示 5% 的 CPU 使用率阈值，蓝点表示指标数据点。对于第一个数据点，告警为 OK 状态。第二个数据点将告警变为 ALARM 状态，因为该数据点大于阈值。第三个和第四个数据点保持 ALARM 状态，因为数据点继续大于阈值。第五个数据点会将告警变为 OK 状态，因为该数据点小于阈值。



配置警报如何处理缺失数据

在某些情况下，不报告带有告警的指标的某些数据点。例如，当连接丢失或服务器出现故障时，可能会发生这种情况。

Lightsail 允许您指定在配置警报时如何处理丢失的数据点。这可帮助您为要监控的数据类型配置适时进入 ALARM（告警）状态的告警。您可以避免在缺失数据没有指示问题时进行误报。

与每个告警始终处于三种状态之一类似，报告的每个特定数据点将属于以下三个类别之一：

- 未超出：数据点在阈值范围内。

  例如，如果您选择大于比较运算符，数据点将在其小于指定阈值时为 `Not breaching` 状态。如果您选择大于比较运算符，数据点将在其大于指定阈值时为 `Not breaching` 状态。
- 超出：数据点超出阈值范围。

  例如，如果您选择大于比较运算符，数据点将在其大于指定阈值时为 `Breaching` 状态。如果您选择大于比较运算符，数据点将在其小于指定阈值时为 `Breaching` 状态。
- 缺失：缺失数据点的行为由 `treat missing data` 参数指定。

对于每个警报，您可以指定 Lightsail 以将缺失的数据点视为以下任意一项：

- 未超出：将缺失数据点视为“良好”，并在阈值范围内。
- 超出：将缺失数据点视为“不良”，并超出阈值。
- 忽略：保持当前警报状态。
- 缺失：在评估是否改变状态时，警报不考虑缺失数据点。这是默认的告警行为。

最佳选择取决于指标的类型。对于诸如实例的 CPU 使用率等指标，您可能需要将缺失数据点视为超出阈值。这是因为缺失数据点可能表明有些问题。但对于仅在发生错误时生成数据点的指标 (如负载均衡器的 HTTP 500 服务器错误计数)，您可能需要将缺失数据视为未超出阈值。

为您的告警选择最佳选项可防止不必要和误导性的告警条件更改。它还可以更准确地指示系统的运行状况。

在数据缺失时如何评估告警状态

无论您为如何处理缺失数据设置了什么值，当警报评估是否更改状态时，Lightsail 都会尝试检索比评估周期指定的更多的数据点。它尝试检索的数据点的确切数量取决于告警期限长度。它尝试检索的数据点时间范围为评估范围。

Lightsail 检索到这些数据点后，会发生以下情况：

- 如果评估范围内没有丢失任何数据点，Lightsail 会根据最近收集的数据点对警报进行评估。
- 如果评估范围内的某些数据点缺失，但收集的现有数据点数量等于或大于警报的评估周期，Lightsail 会根据成功收集的最新现有数据点评估警报状态。在此情况下，您针对如何处理缺失数据而设置的值便没有必要，将被忽略。
- 如果评估范围内的某些数据点缺失，并且收集的现有数据点数量少于警报的评估周期数，Lightsail 会使用您为如何处理缺失数据而指定的结果填充缺失的数据点，然后对警报进行评估。但是，评估范围内的任何实际数据点（无论何时报告）都包含在评估中。Lightsail 仅尽可能少地使用缺失的数据点。

在所有这些情况下，评估的数据点数等于评估期的值。如果少于 Datapoints to Alarm (触发告警的数据点数) 的值超出阈值，则告警状态设置为“正常”。否则，状态设置为“告警”。

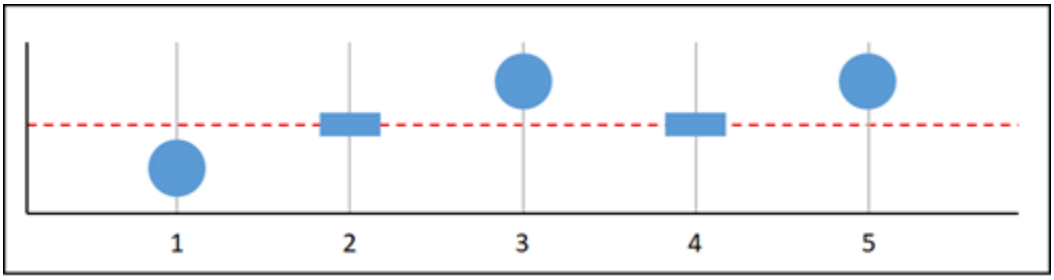
> **Note**
>
> 这种行为的一个特殊情况是，Lightsail 警报可能会在指标停止流动后的一段时间内反复重新评估最后一组数据点。如果告警在指标流即将停止之前更改了状态，这种重新评估可能会导致告警更改状态并重新执行操作。要缓解此行为，请使用较短时间段。

图形示例中的缺失数据

本部分中的以下图表阐明了告警评估行为的示例。在图 A、B、C、D 和 E 中，必须超出到警报状态的数据点和评估期数量都是 3。红色虚线表示阈值，蓝点表示有效的数据点，破折号表示缺失数据。阈值线上方的数据点为超出阈值，阈值线下方的数据未超过阈值。如果最近三个数据点中的某些数据点丢失，Lightsail 将尝试检索其他有效数据点。

> **Note**
>
> 如果在创建警报后不久缺少数据点，并且在您创建警报之前已将指标报告给 Lightsail，则在评估警报时，Lightsail 会检索警报创建之前的最新数据点。

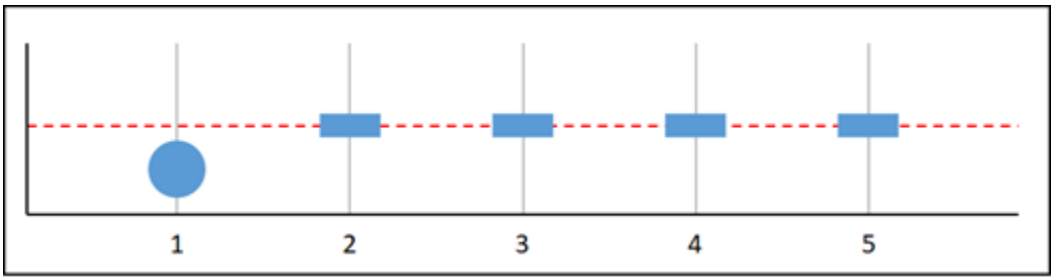
图 A



在前面的图形指标中，数据点 1 在阈值范围内，数据点 2 缺失，数据点 3 超出阈值，数据点 4 缺失，数据点 5 超出阈值。由于在评估范围内有三个有效的数据点，因此该指标具有零个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“正常”状态。
- 超出：警报将处于“正常”状态。
- 忽略：警报将处于“正常”状态。
- 缺失：警报将处于“正常”状态。

图 B



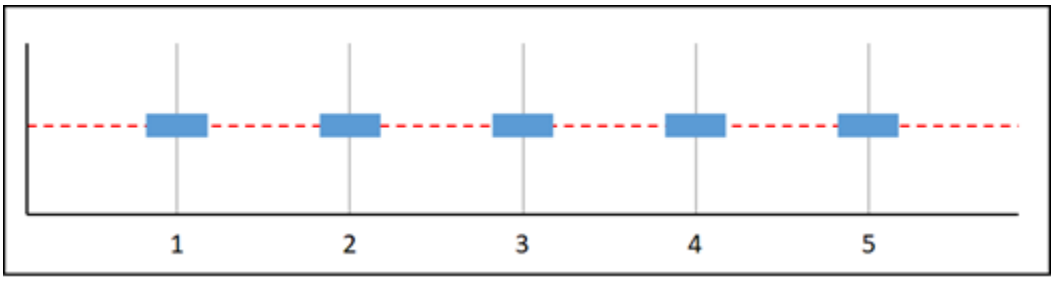
在前面的图形指标中，数据点 1 在阈值范围内，数据点 2 至 5 缺失。由于在评估范围内只有一个有效的数据点，因此该指标具有两个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“正常”状态。
- 超出：警报将处于“正常”状态。

- 忽略：警报将处于“正常”状态。
- 缺失：警报将处于“正常”状态。

在这种情况下，告警将保持在正常状态，即使缺失的数据被视为超出阈值。这是因为一个现有数据点未超出阈值，并且该数据点与两个被视为超出阈值的缺失数据点一起评估。下次评估此告警时，如果数据仍然缺失，它将进入“告警”状态。这是因为未超出阈值的数据点不再是检索的五个最近数据点当中的一个。

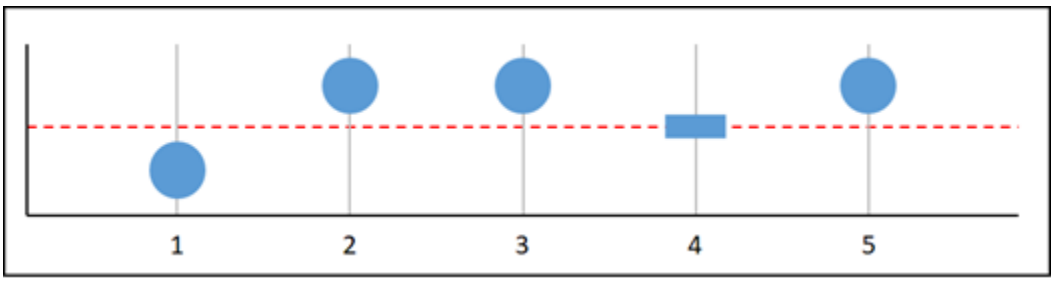
图 C



前面的图形指标中缺失所有数据点。由于评估范围内的所有数据点都缺失，因此该指标具有三个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“正常”状态。
- 超出：警报将处于“警报”状态。
- 忽略：警报将保持当前状态。
- 缺失：警报将处于“数据不足”状态。

图 D



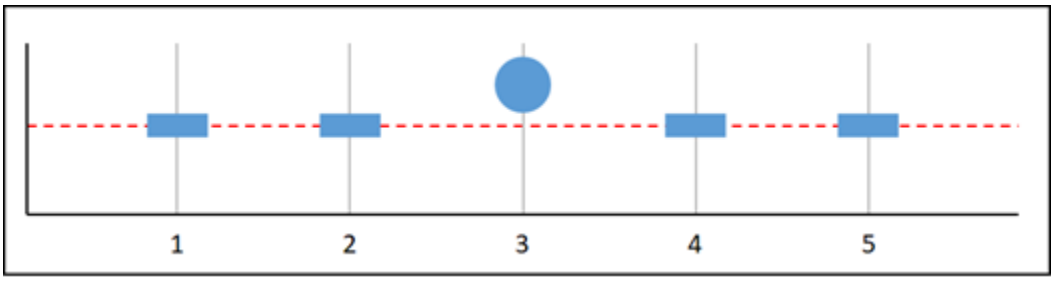
在前面的图形指标中，数据点 1 在阈值范围内，数据点 2 超出阈值，数据点 3 超出阈值，数据点 4 缺失，数据点 5 超出阈值。由于在评估范围内有四个有效的数据点，因此该指标具有零个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“警报”状态。

- 超出：警报将处于“警报”状态。
- 忽略：警报将处于“警报”状态。
- 缺失：警报将处于“警报”状态。

在这种情况下，告警将在所有情形进入“告警”状态。这是因为存在足够的实时数据点，因此不需要设置如何处理缺失数据，缺失数据将被忽略。

图 E

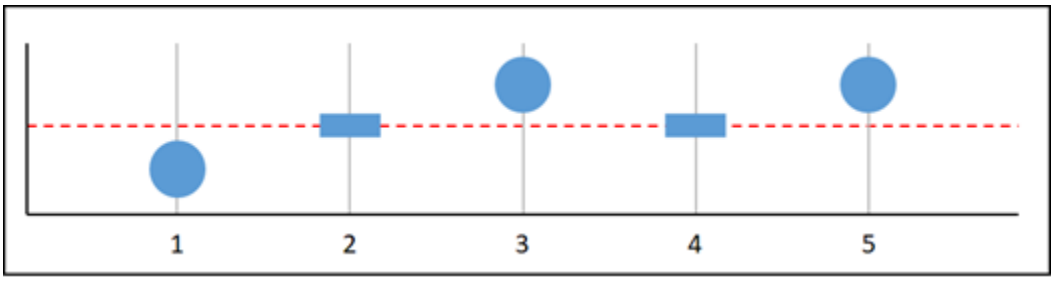


在前面的图形指标中，数据点 1 和 2 缺失，数据点 3 超出阈值，数据点 4 和 5 缺失。由于在评估范围内只有一个有效的数据点，因此该指标具有两个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“正常”状态。
- 超出：警报将处于“警报”状态。
- 忽略：警报将保持当前状态。
- 缺失：警报将处于“警报”状态。

在图 F、G、H、I 和 J 中，告警的数据点有 2 个，而评估期是 3 个。这是“N 中的 M”告警，其中 M 为 2，N 为 3。5 是告警的评估范围。

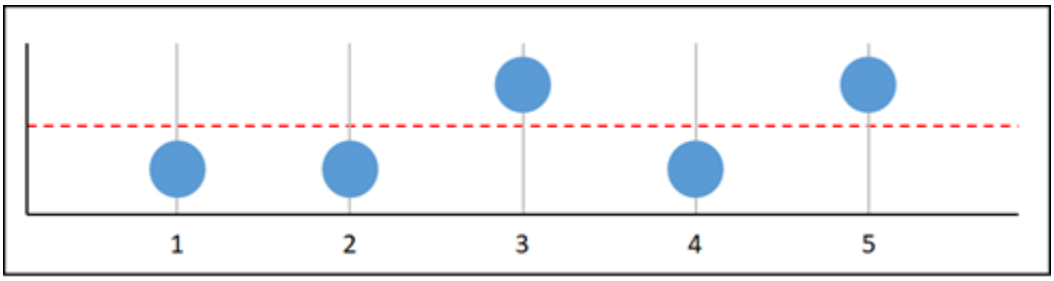
图 F



在前面的图形指标中，数据点 1 在阈值范围内，数据点 2 缺失，数据点 3 超出阈值，数据点 4 缺失，数据点 5 超出阈值。由于在评估范围内有三个数据点，因此该指标具有零个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“警报”状态。
- 超出：警报将处于“警报”状态。
- 忽略：警报将处于“警报”状态。
- 缺失：警报将处于“警报”状态。

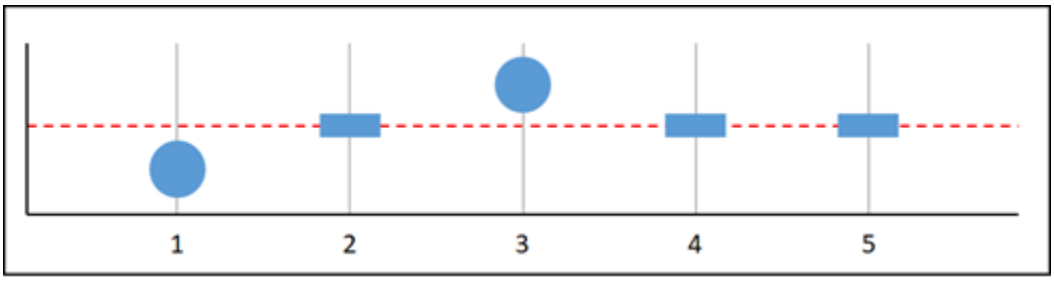
图 G



在前面的图形指标中，数据点 1 和 2 在阈值范围内，数据点 3 超出阈值，数据点 4 在阈值范围内，数据点 5 超出阈值。由于在评估范围内有五个数据点，因此该指标具有零个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“警报”状态。
- 超出：警报将处于“警报”状态。
- 忽略：警报将处于“警报”状态。
- 缺失：警报将处于“警报”状态。

图 H

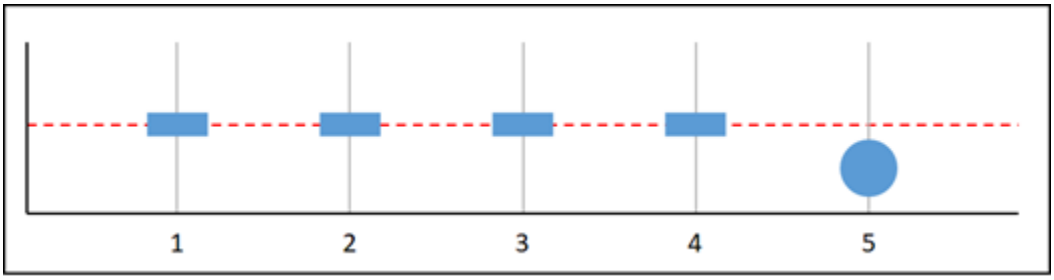


在前面的图形指标中，数据点 1 在阈值范围内，数据点 2 缺失，数据点 3 超出阈值，数据点 4 和 5 缺失。由于在评估范围内有两个数据点，因此该指标具有一个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“正常”状态。
- 超出：警报将处于“警报”状态。

- 忽略：警报将处于“正常”状态。
- 缺失：警报将处于“正常”状态。

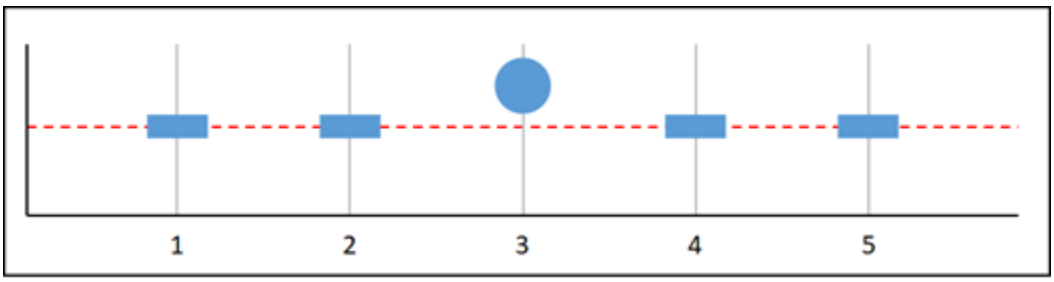
图 I



在前面的图形指标中，数据点 1 到 4 缺失，数据点 5 在阈值范围内。由于在评估范围内有一个数据点，因此该指标具有两个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“正常”状态。
- 超出：警报将处于“警报”状态。
- 忽略：警报将处于“正常”状态。
- 缺失：警报将处于“正常”状态。

图 J



在前面的图形指标中，数据点 1 和 2 缺失，数据点 3 超出阈值，数据点 4 和 5 缺失。由于在评估范围内有一个数据点，因此该指标具有两个缺失数据点。如果您配置告警并将缺失数据点视为：

- 未超出：警报将处于“正常”状态。
- 超出：警报将处于“警报”状态。
- 忽略：警报将保持当前状态。
- 缺失：警报将处于“警报”状态。

有关告警的更多信息

以下是一些可帮助您在 Lightsail 中管理警报的文章：

- 创建实例指标警报
- 创建数据库指标警报
- 创建负载均衡器指标警报
- 创建分配指标警报
- 删除或禁用指标警报

创建 Lightsail 实例指标警报

您可以创建监视单个实例指标的 Amazon Lightsail 警报。可以将告警配置为基于相对于您指定的阈值的指标值来向您发送通知。通知可以是显示在 Lightsail 控制台中的横幅、发送到您的电子邮件地址的电子邮件以及发送到您的手机号码的 SMS 短信。有关警报的更多信息，请参阅警报。

内容

- 实例告警限制
- 配置实例告警的最佳实践
- 默认告警设置
- 使用 Lightsail 控制台创建实例指标警报
- 使用 Lightsail 控制台测试实例指标警报
- 创建实例告警后的后续步骤

实例告警限制

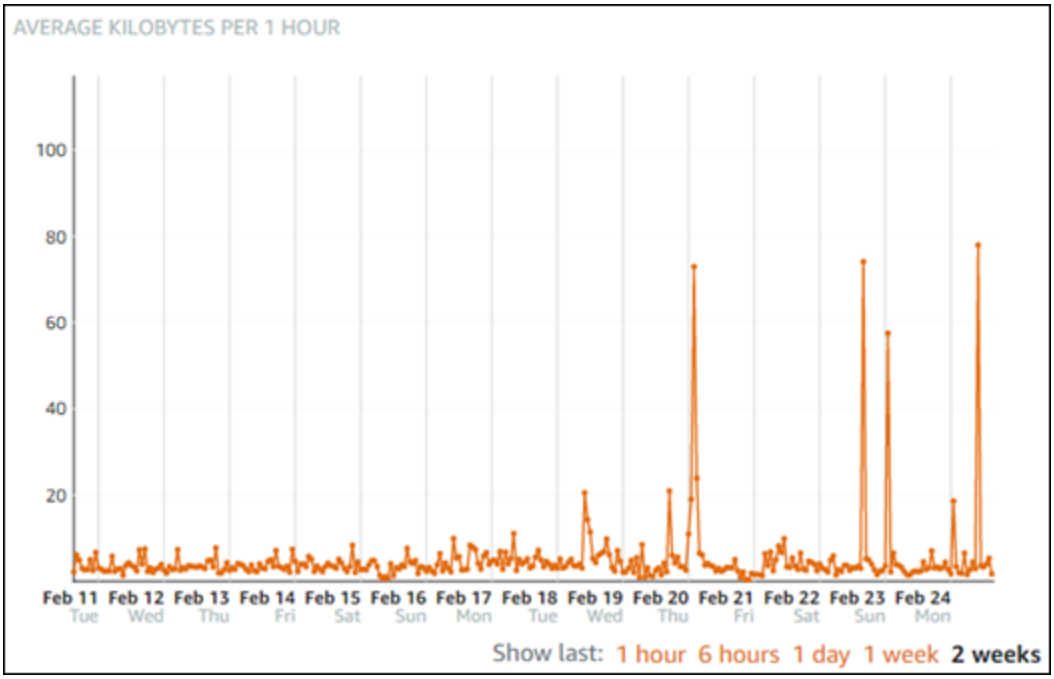
以下限制适用于告警：

- 您可以为每个指标配置两个告警。
- 每隔 5 分钟评估一次告警，告警的每个数据点代表一个 5 分钟时段的聚合指标数据。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能配置告警以在告警状态变为 OK 时通知您。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能测试 OK 告警通知。

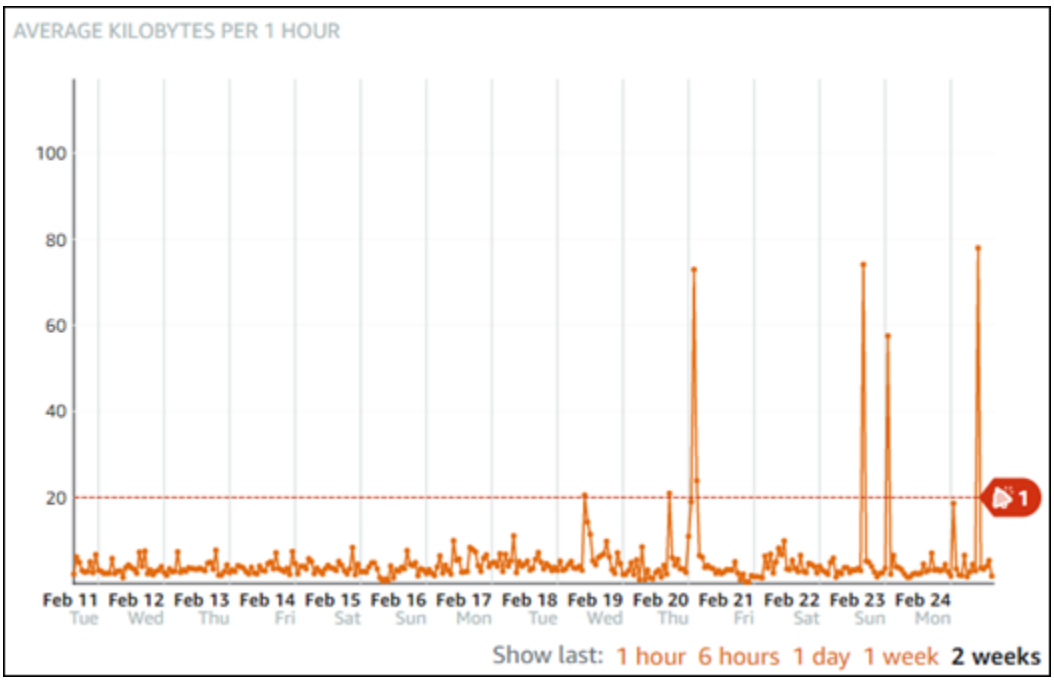
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，以及您对于缺失数据点选择 Do not evaluate the missing data (不评估缺失数据) 选项，则您只能配置告警以在告警状态变为 `INSUFFICIENT_DATA` 时通知您。
- 只有当告警处于 OK（正常）状态时，才能测试通知。

配置实例告警的最佳实践

在为实例配置指标告警之前，您应该查看该指标的历史数据。识别过去两周内低级、中级和高级的指标情况。在以下传出网络流量 (`NetworkOut`) 指标图表示例中，低级为每小时 0-10 KB，中级为每小时 10-20 KB，高级为每小时 20-80 KB。



如果将告警阈值配置为大于或等于低级范围内的某个值（例如，每小时 5 KB），那么您将收到更频繁且可能不必要的告警通知。如果将告警阈值配置为大于或等于高级范围内的某个值（例如，每小时 20 KB），那么您将很少收到通知，但可能也是更重要的需要调查的情况。当您配置并启用告警时，图表上会显示一条表示阈值的告警线，如以下示例所示。标记为 1 的告警线表示告警 1 的阈值，标记为 2 的告警线表示告警 2 的阈值。



默认告警设置

在 Lightsail 控制台中添加新警报时，系统会预先填充默认警报设置。这是所选指标的建议告警配置。您应确认默认告警配置是否适合您的资源。例如，实例传出网络流量 (`NetworkOut`) 指标的默认告警阈值为在过去 10 分钟内有 2 次小于或等于 0 个字节。但是，如果您有兴趣收到高流量事件的通知，那么您可能需要将警报阈值修改为在过去 10 分钟内有 2 次大于或等于 50KB，或者使用这些设置添加第二个警报，以便在没有流量和流量较高时收到通知。您指定的阈值应进行调整，以匹配指标的高级和低级情况，如本指南的配置实例告警的最佳实践部分所述。

使用 Lightsail 控制台创建实例指标警报

完成以下步骤，使用 Lightsail 控制台创建实例指标警报。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择要为其创建警报的实例的名称。
4. 选择实例管理页面上的 Metrics（指标）选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要创建告警的指标。有关更多信息，请参阅资源指标。
6. 在页面的 Alarms (告警) 部分选择 Alarms (添加告警)。
7. 在下拉菜单中选择比较运算符值。示例值为大于或等于、大于、小于以及等于。

8. 输入告警的阈值。
9. 输入告警的数据点。
10. 选择评估期。时段可以 5 分钟为增量指定，从 5 分钟到 24 小时。
11. 选择以下通知方法之一：

    - 电子邮件 — 当告警状态变为 ALARM（告警）时，您会收到电子邮件通知。
    - SMS 文本消息 — 当告警状态变为 ALARM（告警）时，您会收到 SMS 文本消息通知。并非所有可以创建 Lightsail 资源的 AWS 区域都支持短信，也无法向所有国家/地区发送短信。有关更多信息，请参阅 SMS 文本消息支持。

    > **Note**
    >
    > 如果您选择通过电子邮件或 SMS 进行通知，但尚未在资源的亚马逊云科技区域中配置通知联系人，则需要添加电子邮件地址或手机号码。有关更多信息，请参阅指标通知。

12. （可选）选择 Send me a notification when the alarm state change to OK（当告警状态变为正常时，向我发送通知），以在告警状态变为 OK（正常）时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
13. （可选）选择 Advanced settings（高级设置），然后选择下列选项之一：

    - 选择警报应如何处理缺失数据。以下选项可用：
      - 假设不在阈值范围内（超出阈值）— 将缺失数据点视为“不良”和超出阈值。
      - 假设在阈值范围内（未超出阈值）— 将缺失数据点视为“良好”和在阈值范围内。
      - 使用最后一个良好数据点的值（忽略并保持当前警报状态）：维持当前警报状态。
      - 不评估（将缺失的数据视为缺失）— 在评估是否更改状态时，告警不考虑缺失数据点。
    - 选择如果数据不足，则发送通知，在告警状态变为 INSUFFICIENT_DATA 时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
14. 选择 Create (创建) 以添加告警。

之后要编辑警报，选择要编辑的警报旁边的省略号图标（⋮），然后选择编辑警报。

使用 Lightsail 控制台测试实例指标警报

完成以下步骤，使用 Lightsail 控制台测试警报。您可能需要测试告警以确认已配置的通知选项是否正常工作，例如确保在触发告警时收到电子邮件或 SMS 文本消息。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择要测试告警的实例的名称。
4. 选择实例管理页面上的 Metrics（指标）选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要测试告警的指标。
6. 向下滚动到页面的警报部分，然后选择要测试的警报旁边的省略号图标（⋮）。
7. 请选择以下选项之一：

   - 测试警报通知：选择此选项可测试警报状态变为 ALARM 时的通知。
   - 测试确定通知：选择此选项可测试警报状态变为 OK 时的通知。

   > **Note**
   >
   > 如果这些选项都无法使用，您可能尚未配置告警的通知选项，或者告警当前处于 ALARM 状态。有关更多信息，请参阅实例告警限制。

   根据您选择的测试选项，告警将立即变为 ALARM 或 OK 状态，并且会根据您配置为告警通知方法的内容发送电子邮件和/或 SMS 文本消息。只有当您选择测试通知时，通知横幅才会显示在 Lightsail 控制台中。ALARM如果您选择测试 OK 通知，将不会显示通知横幅。告警通常会在几秒钟后恢复为实际状态。

后续步骤

对于实例告警，有其他几项可执行的任务：

- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除通知联系人。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

删除或禁用 Lightsail 指标警报

您可以删除 Amazon Lightsail 警报，以停止通知警报所监控的指标何时超过阈值。您还可以禁用警报以停止接收通知。有关更多信息，请参阅警报。

内容

- 使用 Lightsail 控制台删除指标警报
- 使用 Lightsail 控制台禁用和启用指标警报

使用 Lightsail 控制台删除指标警报

完成以下步骤，使用 Lightsail 控制台删除指标警报。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择实例、数据库或联网。
3. 选择要为其删除警报的资源（实例、数据库或负载均衡器）的名称。
4. 在资源管理页面上选择指标选项卡。
5. 在指标图表标题下的下拉菜单中，选择要删除警报的指标。
6. 向下滚动到页面的警报部分，然后选择要删除的警报旁边的省略号图标（⋮）。
7. 选择删除。
8. 在提示符下，选择是以确认您要删除警报。

使用 Lightsail 控制台禁用和启用指标警报

完成以下步骤，使用 Lightsail 控制台禁用指标警报。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择实例、数据库或联网。
3. 选择要禁用警报的资源（实例、数据库或负载均衡器）的名称。
4. 在资源管理页面上选择指标选项卡。
5. 在指标图表标题下的下拉菜单中，选择要禁用警报的指标。
6. 向下滚动到页面的警报部分，找到要禁用的警报，然后进行切换以将其禁用。同样，如果它处于禁用状态，则进行切换可禁用它。

监控 Lightsail 存储桶的性能和使用情况

在 Amazon Lightsail 对象存储服务中创建存储桶后，您可以在存储桶管理页面的指标选项卡上查看其指标图表。监控指标是维护存储桶可用性和性能的重要环节。请定期监控和收集存储桶的指标数据，以便能够在必要时增加或缩小存储桶的存储空间和网络传输配额。有关指标的更多信息，请参阅资源指标。

在监控资源时，应为环境中的正常资源性能建立基准。然后，您可以在 Lightsail 控制台中配置告警，以便在资源性能超出指定阈值时通知您。有关更多信息，请参阅通知和警报。

存储桶指标

提供以下存储桶指标 ：

- Bucket size（存储桶大小）— 存储桶中存储的数据量。此值通过汇总存储桶中所有对象（当前对象和非当前对象）的大小计算得出，包括所有向存储桶进行分段上传而未完成的所有部分的大小。
- Number of objects（对象数）— 存储桶中存储的对象总数。此值通过对存储桶中所有对象（当前对象和非当前对象）以及所有向存储桶进行分段上传而未完成的所有部分的总数进行计数而计算得出。

> **Note**
>
> 存储桶为空时，不会报告存储桶指标数据。

在 Lightsail 控制台中查看存储桶指标

完成以下过程，以在 Lightsail 控制台中查看存储桶指标。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择所需存储桶的名称，以查看其指标。
4. 在存储桶管理页面上选择 Metrics（指标）选项卡。
5. 在 Metrics graphs（指标图表）标题下的下拉菜单中，选择要查看的指标。

   该图表显示所选指标的数据点的直观表示形式。

   ScreenshotTBD

   您可以对指标图表执行以下操作：

   - 更改图表的视图以显示 1 小时、6 小时、1 天、1 周和 2 周的数据。
   - 将光标停在一个数据点上可查看有关该数据点的详细信息。
   - 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅警报和创建存储桶指标警报。

管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 禁止公开访问亚马逊 Lightsail 中的存储桶
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶

- 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
- 在 Amazon Lightsail 中查看存储桶中的对象
- 在 Amazon Lightsail 中复制或移动存储桶中的对象
- 从 Amazon Lightsail 中的存储桶下载对象
- 在 Amazon Lightsail 中筛选存储桶中的对象
- 在 Amazon Lightsail 中标记存储桶中的对象
- 在 Amazon Lightsail 中删除存储桶中的对象

9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。
10. 启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。
11. 监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。
12. 配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。
13. 如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。
14. 了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。
    - 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
    - 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶
15. 如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

主题

- 使用指标警报监控 Lightsail 存储桶的存储空间

使用指标警报监控 Lightsail 存储桶的存储空间

您可以创建监视单个存储桶指标的 Amazon Lightsail 警报。可以将告警配置为基于相对于您指定的阈值的指标值来向您发送通知。通知可以是显示在 Lightsail 控制台中的横幅、发送到您的电子邮件地址的电子邮件以及发送到您的手机号码的 SMS 短信。有关警报的更多信息，请参阅警报。

内容

- 存储桶告警限值

- 配置存储桶告警的最佳实践
- 默认告警设置
- 使用 Lightsail 控制台创建存储桶指标警报
- 使用 Lightsail 控制台测试存储桶指标警报
- 创建存储桶告警后的后续步骤

存储桶告警限制

以下限制适用于告警：

- 您可以为每个指标配置两个告警。
- 每隔 5 分钟评估一次告警，告警的每个数据点代表一个 5 分钟时段的聚合指标数据。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能配置告警以在告警状态变为 OK 时通知您。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能测试 OK 告警通知。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，以及您对于缺失数据点选择 Do not evaluate the missing data (不评估缺失数据) 选项，则您只能配置告警以在告警状态变为 `INSUFFICIENT_DATA` 时通知您。
- 只有当告警处于 OK（正常）状态时，才能测试通知。

配置存储桶告警的最佳实践

在为存储桶配置指标告警之前，您应确定要收到哪些通知。例如，使用存储桶大小指标时，您可能希望在存储桶几乎装满的时候收到通知。如果存储桶的当前计划包含 5 GB 的存储空间，则您可能需要配置当存储桶达到 4.5 GB 时的存储桶大小指标告警。之后您会收到通知，从而有足够的时间来升级存储桶计划。

默认告警设置

在 Lightsail 控制台中添加新警报时，系统会预先填充默认警报设置。这是所选指标的建议告警配置。您应确认默认告警配置是否适合您的资源。例如，存储桶大小字节指标的默认警报阈值为大于或等于 75GB。但是，如果您的存储桶配置为只有 5 GB 的存储空间，则该请求阈值可能太高。您可能需要将告警阈值修改为等于或大于 4.5 GB。

使用 Lightsail 控制台创建存储桶指标警报

完成以下步骤，使用 Lightsail 控制台创建存储桶指标警报。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要为其创建警报的存储桶的名称。
4. 在存储桶管理页面上选择 Metrics (指标) 选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要创建告警的指标。有关更多信息，请参阅资源指标。
6. 在页面的 Alarms (告警) 部分选择 Alarms (添加告警)。
7. 在下拉菜单中选择比较运算符值。示例值为大于或等于、大于、小于以及等于。
8. 输入告警的阈值。
9. 输入告警的数据点。
10. 选择评估期。时段可以 5 分钟为增量指定，从 5 分钟到 24 小时。
11. 选择以下通知方法之一：

    - 电子邮件 — 当告警状态变为 ALARM（告警）时，您会收到电子邮件通知。
    - SMS 文本消息 — 当告警状态变为 ALARM（告警）时，您会收到 SMS 文本消息通知。并非所有 AWS 区域都支持 SMS 消息收发，SMS 文本消息可能无法发送到所有国家/地区。有关更多信息，请参阅 SMS 文本消息收发支持。

    > **Note**
    >
    > 如果您选择通过电子邮件或 SMS 进行通知，但尚未在资源的 AWS 区域中配置通知联系人，则需要添加电子邮件地址或手机号码。有关更多信息，请参阅通知。

12. （可选）选择 Send me a notification when the alarm state change to OK（当告警状态变为正常时，向我发送通知），以在告警状态变为 OK（正常）时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
13. （可选）选择 Advanced settings（高级设置），然后选择下列选项之一：

    - 选择告警应如何处理缺失数据。以下选项可用：
        - 假设不在阈值范围内（超出阈值）— 将缺失数据点视为“不良”和超出阈值。

- 假设在阈值范围内（未超出阈值）— 将缺失数据点视为“良好”和在阈值范围内。
- 使用最后一个良好数据点的值（忽略并保持当前警报状态）：维持当前警报状态。
- 不评估（将缺失的数据视为缺失）— 在评估是否更改状态时，告警不考虑缺失数据点。

- 选择如果数据不足，则发送通知，在告警状态变为 INSUFFICIENT_DATA 时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。

14. 选择 Create (创建) 以添加告警。

之后要编辑警报，选择要编辑的警报旁边的省略号图标（⋮），然后选择编辑警报。

使用 Lightsail 控制台测试存储桶指标警报

完成以下步骤，使用 Lightsail 控制台测试警报。您可能需要测试告警以确认已配置的通知选项是否正常工作，例如确保在触发告警时收到电子邮件或 SMS 文本消息。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择要测试告警的存储桶的名称。
4. 在存储桶管理页面上选择 Metrics (指标) 选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要测试告警的指标。
6. 向下滚动到页面的警报部分，然后选择要测试的警报旁边的省略号图标（⋮）。
7. 请选择以下选项之一：

- 测试警报通知：选择此选项可测试警报状态变为 ALARM 时的通知。
- 测试确定通知：选择此选项可测试警报状态变为 OK 时的通知。

> **Note**
>
> 如果这些选项都无法使用，您可能尚未配置告警的通知选项，或者告警当前处于 ALARM 状态。有关更多信息，请参阅存储桶告警限制。

根据您选择的测试选项，告警将立即变为 ALARM 或 OK 状态，并且会根据您配置为告警通知方法的内容发送电子邮件和/或 SMS 文本消息。只有当您选择测试通知时，通知横幅才会显示在 Lightsail 控制台中。ALARM如果您选择测试 OK 通知，将不会显示通知横幅。告警通常会在几秒钟后恢复为实际状态。

创建存储桶告警后的后续步骤

对于存储桶告警，有其他几项可执行的任务：

- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除通知联系人。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

监控 Lightsail 容器服务的资源利用率

创建 Amazon Lightsail 容器服务后，可以在该服务的管理页面的 “指标” 选项卡上查看其指标图表。监控指标是维护资源的可靠性、可用性和性能的重要环节。定期监控和收集资源中的指标数据，以便您能够更轻松地调试多点故障（如果发生）。有关指标的更多信息，请参阅 Amazon Lightsail 中的指标。

在监控资源时，应为环境中的正常资源性能建立基准。

> **Note**
>
> 容器服务指标当前不支持告警和通知。

容器服务指标

提供以下容器服务指标：

- CPU 利用率 — 容器服务的所有节点当前正在使用的计算单位的平均百分比。此指标标识在容器服务上运行容器所需的处理能力。
- 内存利用率 — 容器服务的所有节点当前正在使用的内存的平均百分比。此指标标识在容器服务上运行容器所需的内存。

> **Note**
>
> 如果创建新部署，则容器服务的现有利用率指标将消失，并且仅显示当前新部署的指标。

在 Lightsail 控制台中查看容器服务指标

完成以下过程以在 Lightsail 控制台中查看容器服务指标。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择容器。
3. 选择所需容器的名称，以查看其指标。
4. 选择容器服务管理页面上的 Metrics（指标）选项卡。
5. 在 Metrics（指标）图表标题下的下拉菜单中，选择要查看的指标。

   该图表显示所选指标的数据点的直观表示形式。
6. 您可以对指标图表执行以下操作：

   - 更改图表的视图以显示 1 小时、6 小时、1 天、1 周和 2 周的数据。
   - 将光标停在一个数据点上可查看有关该数据点的详细信息。

> **Note**
>
> 容器服务指标当前不支持告警和通知。

监控 Lightsail 数据库性能指标

在 Amazon Lightsail 中启动数据库后，您可以在数据库管理页面的 “指标” 选项卡上查看其指标图表。监控指标是维护资源的可靠性、可用性和性能的重要环节。定期监控和收集资源中的指标数据，以便您能够更轻松地调试多点故障（如果发生）。有关指标的更多信息，请参阅指标。

在监控资源时，应为环境中的正常资源性能建立基准。建立基准后，您可以在 Lightsail 控制台中配置警报，以便在资源运行超出指定阈值时通知您。有关更多信息，请参阅通知和警报。

内容

- 数据库指标
- 查看数据库指标
- 查看数据库指标后的后续步骤

数据库指标

提供了以下数据库指标：

- CPU 利用率 (**`CPUUtilization`**) – 数据库当前使用的 CPU 利用率的百分比。

- 数据库连接数 (**DatabaseConnections**) – 正在使用的数据库连接数。
- 磁盘队列深度 (**DiskQueueDepth**)-等待访问磁盘的未处理 IOs （读/写请求）的数量。
- 可用存储空间 (**FreeStorageSpace**) – 可用存储空间的大小。
- 网络接收吞吐量 (**NetworkReceiveThroughput**) – 数据库的传入（接收）网络流量，包括客户数据库流量和用于监控和复制的 AWS 流量。
- 网络传输吞吐量 (**NetworkTransmitThroughput**) – 数据库的传出（传输）网络流量，包括客户数据库流量和用于监控和复制的 AWS 流量。

在 Lightsail 控制台中查看数据库指标

完成以下步骤，即可在 Lightsail 控制台中查看数据库指标。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择所需数据库的名称，以查看其指标。
4. 选择数据库管理页面上的 Metrics（指标）选项卡。
5. 在 Metrics graphs（指标图表）标题下的下拉菜单中，选择要查看的指标。

   该图表显示所选指标的数据点的直观表示形式。
6. 您可以对指标图表执行以下操作：

   - 更改图表的视图以显示 1 小时、6 小时、1 天、1 周和 2 周的数据。
   - 将光标停在一个数据点上可查看有关该数据点的详细信息。
   - 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅警报和创建数据库指标警报。

查看数据库指标后的后续步骤

对于数据库指标，有其他几项可执行的任务：

- 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅警报和创建数据库指标警报。
- 触发警报后，Lightsail 控制台中会显示一条通知横幅。要通过电子邮件和短信收到通知，您必须将您的电子邮件地址和手机号码添加为要监控资源的每个 AWS 区域 位置的通知联系人。有关更多信息，请参阅添加通知联系人。

- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除或禁用指标警报。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

主题

- 使用指标警报监控 Lightsail 数据库的运行状况

使用指标警报监控 Lightsail 数据库的运行状况

您可以创建监视单个数据库指标的 Amazon Lightsail 警报。可以将告警配置为基于相对于您指定的阈值的指标值来向您发送通知。通知可以是显示在 Lightsail 控制台中的横幅、发送到您的电子邮件地址的电子邮件以及发送到您的手机号码的 SMS 短信。有关警报的更多信息，请参阅警报。

内容

- 数据库告警限制
- 配置数据库告警的最佳实践
- 默认告警设置
- 使用 Lightsail 控制台创建数据库指标警报
- 使用 Lightsail 控制台测试数据库指标警报
- 创建数据库告警后的后续步骤

数据库告警限制

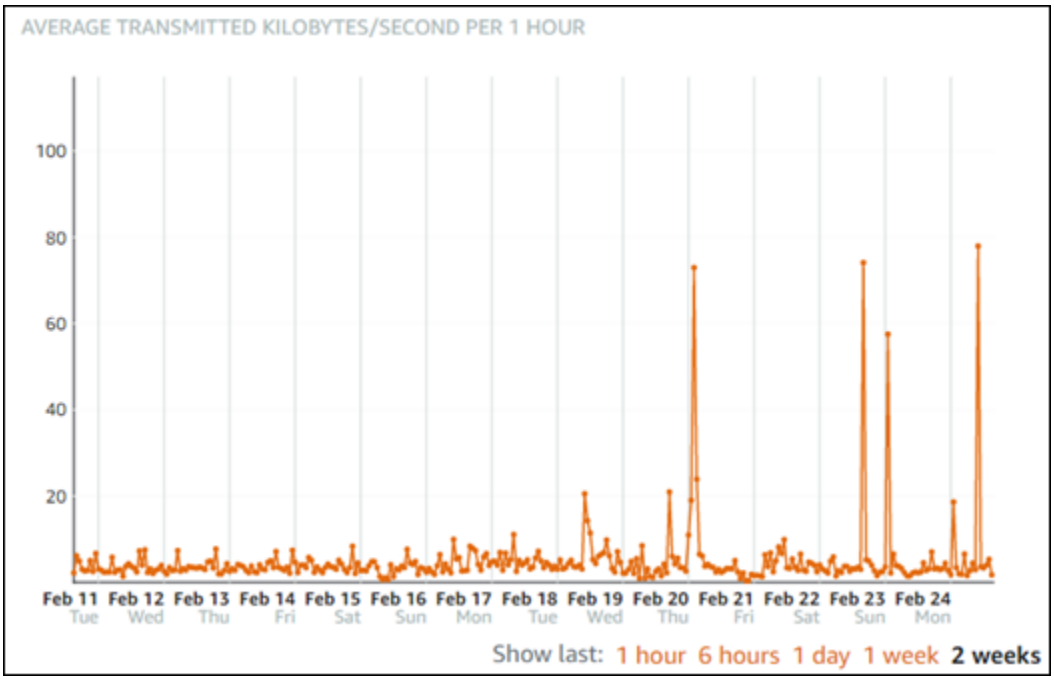
以下限制适用于告警：

- 您可以为每个指标配置两个告警。
- 每隔 5 分钟评估一次告警，告警的每个数据点代表一个 5 分钟时段的聚合指标数据。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能配置告警以在告警状态变为 OK 时通知您。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能测试 OK 告警通知。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，以及您对于缺失数据点选择 Do not evaluate the missing data (不评估缺失数据) 选项，则您只能配置告警以在告警状态变为 `INSUFFICIENT_DATA` 时通知您。

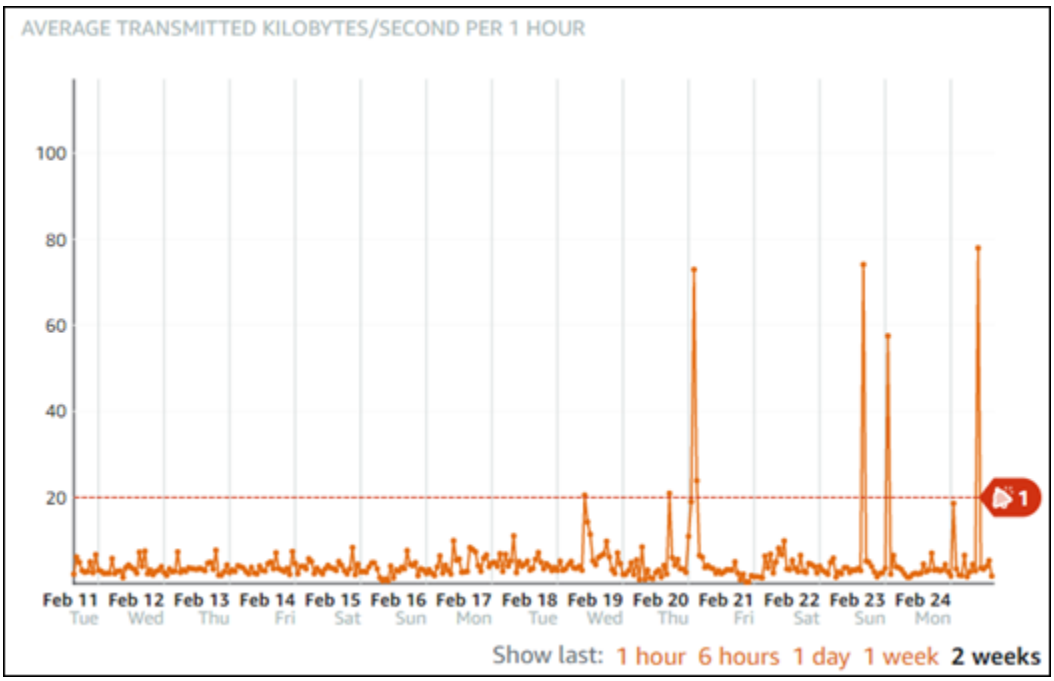
- 只有当告警处于 OK（正常）状态时，才能测试通知。

配置数据库告警的最佳实践

在为数据库配置指标告警之前，应查看指标的历史数据。识别过去两周内低级、中级和高级的指标情况。在以下网络传输吞吐量 (NetworkTransmitThroughput) 指标图示例中，低级别为KB/second per hour, the mid-levels are between 10-20 KB/second per hour, and the high-levels are between 20-80 KB/second每小时 0-10。



如果将告警阈值配置为大于或等于低级范围内的某个值（例如，每小时 5 KB/秒），那么您将收到更频繁且可能不必要的告警通知。如果将告警阈值配置为大于或等于高级范围内的某个值（例如，每小时 20 KB/秒），那么您将很少收到通知，但可能也是更重要的需要调查的情况。当您配置并启用告警时，图表上会显示一条表示阈值的告警线，如以下示例所示。标记为 1 的告警线表示告警 1 的阈值，标记为 2 的告警线表示告警 2 的阈值。



默认告警设置

在 Lightsail 控制台中添加新警报时，系统会预先填充默认警报设置。这是所选指标的建议告警配置。您应确认默认告警配置是否适合您的资源。例如，可用存储空间 (`FreeStorageSpace`) 指标的默认告警阈值为在过去 5 分钟内有 1 次小于 5 个字节。但是，可用存储空间阈值对于您的数据库来说可能太低。您可能需要将告警阈值修改为在过去 5 分钟内有 1 次小于 4 GB。

使用 Lightsail 控制台创建数据库指标警报

完成以下步骤，使用 Lightsail 控制台创建数据库指标警报。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。
3. 选择要为其创建警报的数据库的名称。
4. 在数据库管理页面上选择指标选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要创建告警的指标。有关更多信息，请参阅资源指标。
6. 在页面的 Alarms (告警) 部分选择 Alarms (添加告警)。
7. 在下拉菜单中选择比较运算符值。示例值为大于或等于、大于、小于以及等于。
8. 输入告警的阈值。
9. 输入告警的数据点。

10. 选择评估期。时段可以 5 分钟为增量指定，从 5 分钟到 24 小时。
11. 选择以下通知方法之一：

    - 电子邮件 — 当告警状态变为 ALARM（告警）时，您会收到电子邮件通知。
    - SMS 文本消息 — 当告警状态变为 ALARM（告警）时，您会收到 SMS 文本消息通知。并非所有可以创建 Lightsail 资源的 AWS 区域都支持短信，也无法向所有国家/地区发送短信。有关更多信息，请参阅 SMS 文本消息支持。

    > **Note**
    >
    > 如果您选择通过电子邮件或 SMS 进行通知，但尚未在资源的亚马逊云科技区域中配置通知联系人，则需要添加电子邮件地址或手机号码。有关更多信息，请参阅通知。

12. （可选）选择 Send me a notification when the alarm state change to OK（当告警状态变为正常时，向我发送通知），以在告警状态变为 OK（正常）时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
13. （可选）选择 Advanced settings（高级设置），然后选择下列选项之一：

    - 选择告警应如何处理缺失数据。以下选项可用：
      - 假设不在阈值范围内（超出阈值）— 将缺失数据点视为“不良”和超出阈值。
      - 假设在阈值范围内（未超出阈值）— 将缺失数据点视为“良好”和在阈值范围内。
      - 使用最后一个良好数据点的值（忽略并保持当前警报状态）：维持当前警报状态。
      - 不评估（将缺失的数据视为缺失）— 在评估是否更改状态时，告警不考虑缺失数据点。
    - 选择如果数据不足，则发送通知，在告警状态变为 INSUFFICIENT_DATA 时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
14. 选择 Create (创建) 以添加告警。

    之后要编辑警报，选择要编辑的警报旁边的省略号图标（⋮），然后选择编辑警报。

使用 Lightsail 控制台测试数据库指标警报

完成以下步骤，使用 Lightsail 控制台测试警报。您可能需要测试告警以确认已配置的通知选项是否正常工作，例如确保在触发告警时收到电子邮件或 SMS 文本消息。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择数据库。

3. 选择要测试告警的数据库的名称。
4. 在数据库管理页面上选择指标选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要测试告警的指标。
6. 向下滚动到页面的警报部分，然后选择要测试的警报旁边的省略号图标（⋮）。
7. 请选择以下选项之一：

   - 测试警报通知：选择此选项可测试警报状态变为 ALARM 时的通知。
   - 测试确定通知：选择此选项可测试警报状态变为 OK 时的通知。

   > **Note**
   >
   > 如果这些选项都无法使用，您可能尚未配置告警的通知选项，或者告警当前处于 ALARM 状态。有关更多信息，请参阅数据库告警限制。

   根据您选择的测试选项，告警将立即变为 ALARM 或 OK 状态，并且会根据您配置为告警通知方法的内容发送电子邮件和/或 SMS 文本消息。只有当您选择测试通知时，通知横幅才会显示在 Lightsail 控制台中。ALARM如果您选择测试 OK 通知，将不会显示通知横幅。告警通常会在几秒钟后恢复为实际状态。

创建数据库告警后的后续步骤

对于数据库告警，可以执行其他几项任务：

- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除通知联系人。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

监控 Lightsail 发行绩效指标

在 Amazon Lightsail 中创建分配后，您可以在分配管理页面的 “指标” 选项卡上查看其指标图表。监控指标是维护资源的可靠性、可用性和性能的重要环节。定期监控和收集资源中的指标数据，以便您能够更轻松地调试多点故障（如果发生）。有关指标的更多信息，请参阅指标。

在监控资源时，应为环境中的正常资源性能建立基准。然后，您可以在 Lightsail 控制台中配置告警，以便在资源性能超出指定阈值时通知您。有关更多信息，请参阅通知和警报。

内容

- 分配指标
- 在 Lightsail 控制台中查看分发指标
- 查看分配指标后的后续步骤

分配指标

提供以下分配指标：

- 请求数 – 分配收到的查看器请求总数，针对所有 HTTP 方法以及 HTTP 和 HTTPS 请求。
- 已上传字节 – 分配使用 POST 和 PUT 请求上传到源的字节数。
- 已下载字节 – 查看器针对 GET、HEAD 和 OPTIONS 请求下载的字节数。
- 总错误率 – 响应的 HTTP 状态代码为 4xx 或 5xx 的所有查看器请求所占的百分比。
- HTTP 4xx 错误率 – 响应的 HTTP 状态代码为 4xx 的所有查看器请求所占的百分比。在这些情况下，客户端或客户端查看器可能出现了错误。例如，404（未找到）状态代码表示无法找到客户端请求的对象。
- HTTP 5xx 错误率 – 响应的 HTTP 状态代码为 5xx 的所有查看器请求所占的百分比。在这些情况下，源服务器未满足请求。例如，503（服务不可用）状态代码表示源服务器当前不可用。

在 Lightsail 控制台中查看分发指标

完成以下步骤即可在 Lightsail 控制台中查看分发指标。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择所需分配的名称，以查看其指标。
4. 在分配管理页面上选择 Metrics（指标）选项卡。
5. 在 Metrics graphs（指标图表）标题下的下拉菜单中，选择要查看的指标。

   该图表显示所选指标的数据点的直观表示形式。
6. 您可以对指标图表执行以下操作：

   - 更改图表的视图以显示 1 小时、6 小时、1 天、1 周和 2 周的数据。

- 将光标停在一个数据点上可查看有关该数据点的详细信息。
- 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅警报和创建实例指标警报。

查看分配指标后的后续步骤

对于分配指标，有其他几项可执行的任务：

- 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅警报和创建分配指标警报。
- 触发警报后，Lightsail 控制台中会显示一条通知横幅。要通过电子邮件和短信收到通知，您必须将您的电子邮件地址和手机号码添加为要监控资源的每个 AWS 区域 位置的通知联系人。有关更多信息，请参阅添加通知联系人。
- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除或禁用指标警报。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

主题

- 使用指标警报监控 Lightsail 分发运行状况

使用指标警报监控 Lightsail 分发运行状况

您可以创建监视单个分发指标的 Amazon Lightsail 警报。可以将告警配置为基于相对于您指定的阈值的指标值来向您发送通知。通知可以是显示在 Lightsail 控制台中的横幅、发送到您的电子邮件地址的电子邮件以及发送到您的手机号码的 SMS 短信。有关警报的更多信息，请参阅警报。

内容

- 分配告警限制
- 配置分配告警的最佳实践
- 默认告警设置
- 使用 Lightsail 控制台创建分布指标警报
- 测试分配指标警报
- 创建分配告警后的后续步骤

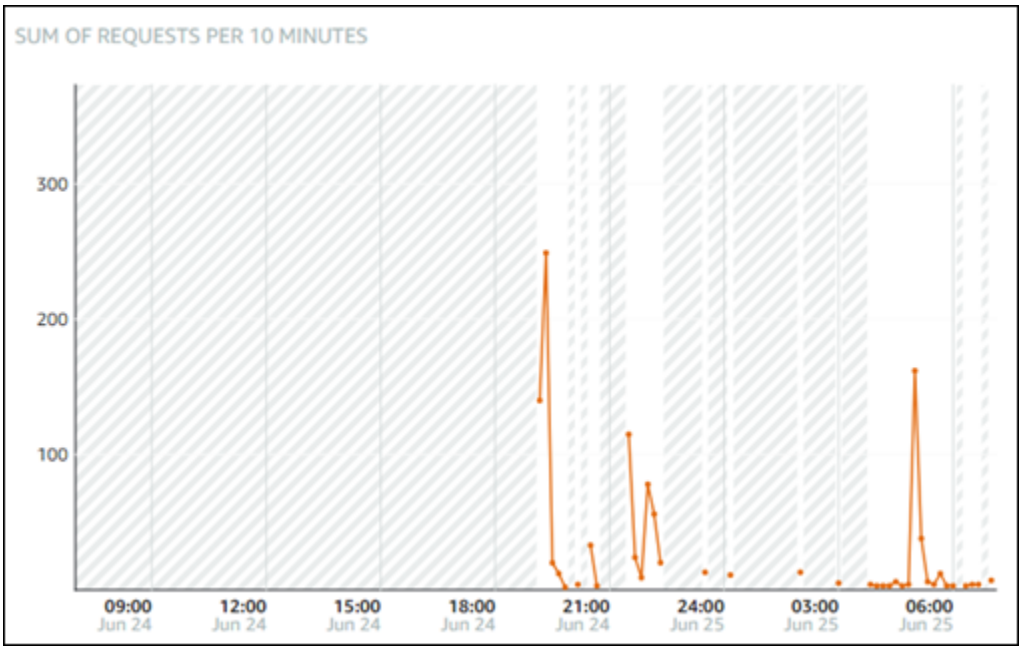
分配告警限制

以下限制适用于告警：

- 您可以为每个指标配置两个告警。
- 每隔 5 分钟评估一次告警，告警的每个数据点代表一个 5 分钟时段的聚合指标数据。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能配置告警以在告警状态变为 OK 时通知您。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能测试 OK 告警通知。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，以及您对于缺失数据点选择 Do not evaluate the missing data (不评估缺失数据) 选项，则您只能配置告警以在告警状态变为 `INSUFFICIENT_DATA` 时通知您。
- 只有当告警处于 OK（正常）状态时，才能测试通知。

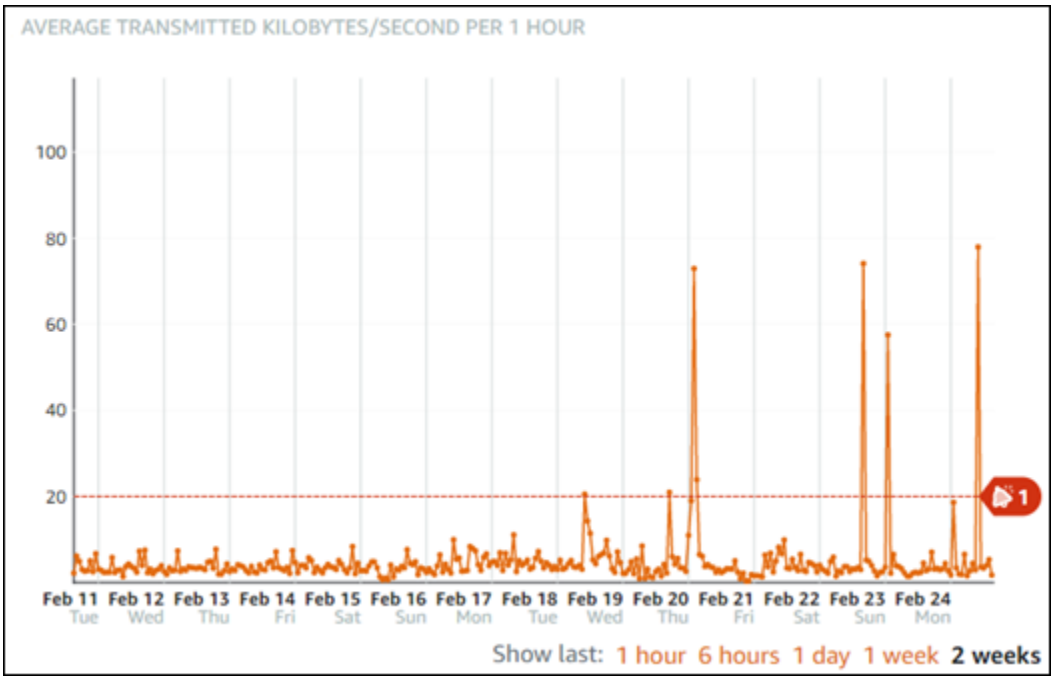
配置分配告警的最佳实践

在为分布配置指标告警之前，您应该查看该指标的历史数据。识别过去两周内低级、中级和高级的指标情况。在以下请求指标图表示例中，低级为 0-10 个请求，中级为 10-50 个，高级为 50-250 个。



如果将告警阈值配置为大于或等于低级范围内的某个值（例如，5 个请求），那么您将收到更频繁且可能不必要的告警通知。如果将告警阈值配置为大于或等于高级范围内的某个值（例如，150 个请求），那么您将很少收到通知，但可能也是更重要的需要调查的情况。当您配置并启用告警时，图表上会显示

一条表示阈值的告警线，如以下示例所示。标记为 1 的告警线表示告警 1 的阈值，标记为 2 的告警线表示告警 2 的阈值。



默认告警设置

在 Lightsail 控制台中添加新警报时，系统会预先填充默认警报设置。这是所选指标的建议告警配置。您应确认默认告警配置是否适合您的资源。例如，请求指标的默认警报阈值为在过去 15 分钟内有 3 次大于 45 个请求。但是，该请求阈值对于您的分配来说可能太低。您可能需要将告警阈值修改为在过去 15 分钟内有 3 次大于 150 个请求。

使用 Lightsail 控制台创建分布指标警报

完成以下步骤，使用 Lightsail 控制台创建分布指标警报。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其创建警报的分配的名称。
4. 在分配管理页面上选择指标选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要创建告警的指标。有关更多信息，请参阅资源指标。
6. 在页面的 Alarms (告警) 部分选择 Alarms (添加告警)。
7. 在下拉菜单中选择比较运算符值。示例值为大于或等于、大于、小于以及等于。

8. 输入告警的阈值。
9. 输入告警的数据点。
10. 选择评估期。时段可以 5 分钟为增量指定，从 5 分钟到 24 小时。
11. 选择以下通知方法之一：

    - 电子邮件 — 当告警状态变为 ALARM（告警）时，您会收到电子邮件通知。
    - SMS 文本消息 — 当告警状态变为 ALARM（告警）时，您会收到 SMS 文本消息通知。并非所有可以创建 Lightsail 资源的 AWS 区域都支持短信，也无法向所有国家/地区发送短信。有关更多信息，请参阅 SMS 文本消息收发支持。

    > **Note**
    >
    > 如果您选择通过电子邮件或 SMS 进行通知，但尚未在资源的 AWS 区域中配置通知联系人，则需要添加电子邮件地址或手机号码。有关更多信息，请参阅通知。

12. （可选）选择 Send me a notification when the alarm state change to OK（当告警状态变为正常时，向我发送通知），以在告警状态变为 OK（正常）时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
13. （可选）选择 Advanced settings（高级设置），然后选择下列选项之一：

    - 选择告警应如何处理缺失数据。以下选项可用：
      - 假设不在阈值范围内（超出阈值）— 将缺失数据点视为“不良”和超出阈值。
      - 假设在阈值范围内（未超出阈值）— 将缺失数据点视为“良好”和在阈值范围内。
      - 使用最后一个良好数据点的值（忽略并保持当前告警状态）— 维持当前告警状态。
      - 不评估（将缺失的数据视为缺失）— 在评估是否更改状态时，告警不考虑缺失数据点。
    - 选择如果数据不足，则发送通知，在告警状态变为 INSUFFICIENT_DATA 时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
14. 选择 Create (创建) 以添加告警。

之后要编辑警报，选择要编辑的警报旁边的省略号图标（⋮），然后选择编辑警报。

测试分配指标警报

完成以下步骤，使用 Lightsail 控制台测试警报。您可能需要测试告警以确认已配置的通知选项是否正常工作，例如确保在触发告警时收到电子邮件或 SMS 文本消息。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要测试告警的分配的名称。
4. 在分配管理页面上选择指标选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要测试告警的指标。
6. 向下滚动到页面的警报部分，然后选择要测试的警报旁边的省略号图标（⋮）。
7. 请选择以下选项之一：

   - 测试警报通知：选择此选项可测试警报状态变为 ALARM 时的通知。
   - 测试确定通知：选择此选项可测试警报状态变为 OK 时的通知。

   > **Note**
   >
   > 如果这些选项都无法使用，您可能尚未配置告警的通知选项，或者告警当前处于 ALARM 状态。有关更多信息，请参阅分配告警限制。

   根据您选择的测试选项，告警将立即变为 ALARM 或 OK 状态，并且会根据您配置为告警通知方法的内容发送电子邮件和/或 SMS 文本消息。只有当您选择测试通知时，通知横幅才会显示在 Lightsail 控制台中。ALARM如果您选择测试 OK 通知，将不会显示通知横幅。告警通常会在几秒钟后恢复为实际状态。

创建分配告警后的后续步骤

对于分配告警，有其他几项可执行的任务：

- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除通知联系人。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

监控 Lightsail 负载均衡器运行状况指标

在 Amazon Lightsail 中创建负载均衡器并向其附加实例后，您可以在负载均衡器管理页面的 “指标” 选项卡上查看其指标图表。监控指标是维护资源的可靠性、可用性和性能的重要环节。定期监控和收集

资源中的指标数据，以便您能够更轻松地调试多点故障（如果发生）。有关指标的更多信息，请参阅指标。

在监控资源时，应为环境中的正常资源性能建立基准。建立基准后，您可以在 Lightsail 控制台中配置警报，以便在资源运行超出指定阈值时通知您。有关更多信息，请参阅通知和警报。

内容

- 负载均衡器指标
- 查看负载均衡器指标
- 后续步骤

负载均衡器指标

提供了以下负载均衡器指标：

- 正常主机计数 (**HealthyHostCount**) – 被视为正常运行的目标实例数。
- 不正常主机计数 (**UnhealthyHostCount**) – 被视为未正常运行的目标实例数。
- 负载均衡器 HTTP 4XX (**HTTPCode_LB_4XX_Count**) – 源自负载均衡器的 HTTP 4XX 客户端错误代码的数量。如果请求格式错误或不完整，则会生成客户端错误。目标实例未收到这些请求。该计数不包含目标实例生成的响应代码。
- 负载均衡器 HTTP 5XX (**HTTPCode_LB_5XX_Count**) – 源自负载均衡器的 HTTP 5XX 服务器错误代码的数量。这不包含由目标实例生成的任何响应代码。如果没有运行正常的实例附加到负载均衡器，或者请求速率超过实例或负载均衡器的容量（溢出），则会报告该指标。
- 实例 HTTP 2XX (**HTTPCode_Instance_2XX_Count**) – 由目标实例生成的 HTTP 2XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例 HTTP 3XX (**HTTPCode_Instance_3XX_Count**) – 由目标实例生成的 HTTP 3XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例 HTTP 4XX (**HTTPCode_Instance_4XX_Count**) – 由目标实例生成的 HTTP 4XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例 HTTP 5XX (**HTTPCode_Instance_5XX_Count**) – 由目标实例生成的 HTTP 5XX 响应代码数。它不包括负载均衡器生成的任何响应代码。
- 实例响应时间 (**InstanceResponseTime**) – 从请求离开负载均衡器到从目标实例收到响应之间所用的时间（以秒为单位）。
- 客户端 TLS 协商错误计数 (**ClientTLSNegotiationErrorCount**) – 由于负载均衡器生成 TLS 错误而未与负载均衡器建立会话的客户端发起的 TLS 连接数。可能的原因包括密码或协议不匹配。

- 请求计数 (**RequestCount**)-已处理的请求数 IPv4。该计数仅包含具有负载均衡器的目标实例生成的响应的请求。
- 已被拒绝的连接计数 (**RejectedConnectionCount**) – 由于负载均衡器达到连接数上限被拒绝的连接的数量。

查看负载均衡器指标

完成以下步骤，即可在 Lightsail 控制台中查看负载均衡器指标。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择所需负载均衡器的名称，以查看其指标。
4. 选择负载均衡器管理页面上的 Metrics（指标）选项卡。
5. 在 Metrics graphs（指标图表）标题下的下拉菜单中，选择要查看的指标。

   该图表显示所选指标的数据点的直观表示形式。
6. 您可以对指标图表执行以下操作：

   - 更改图表的视图以显示 1 小时、6 小时、1 天、1 周和 2 周的数据。
   - 将光标停在一个数据点上可查看有关该数据点的详细信息。
   - 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅警报和创建负载均衡器指标警报。

后续步骤

对于负载均衡器指标，有其他几项可执行的任务：

- 为所选指标添加告警，以便在指标超过您指定的阈值时收到通知。有关更多信息，请参阅警报和创建负载均衡器指标警报。
- 触发警报后，Lightsail 控制台中会显示一条通知横幅。要通过电子邮件和短信收到通知，您必须将您的电子邮件地址和手机号码添加为要监控资源的每个 AWS 区域 位置的通知联系人。有关更多信息，请参阅添加通知联系人。
- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除或禁用指标警报。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

主题

- 使用警报监控 Lightsail 负载均衡器指标

使用警报监控 Lightsail 负载均衡器指标

您可以创建监视单个负载均衡器指标的 Amazon Lightsail 警报。可以将告警配置为基于相对于您指定的阈值的指标值来向您发送通知。通知可以是显示在 Lightsail 控制台中的横幅、发送到您的电子邮件地址的电子邮件以及发送到您的手机号码的 SMS 短信。有关警报的更多信息，请参阅警报。

内容

- 负载均衡器告警限制
- 配置负载均衡器告警的最佳实践
- 默认告警设置
- 使用 Lightsail 控制台创建负载平衡器指标警报
- 使用 Lightsail 控制台测试负载平衡器指标警报
- 后续步骤

负载均衡器告警限制

以下限制适用于告警：

- 您可以为每个指标配置两个告警。
- 每隔 5 分钟评估一次告警，告警的每个数据点代表一个 5 分钟时段的聚合指标数据。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能配置告警以在告警状态变为 OK 时通知您。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能测试 OK 告警通知。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，以及您对于缺失数据点选择 Do not evaluate the missing data (不评估缺失数据) 选项，则您只能配置告警以在告警状态变为 `INSUFFICIENT_DATA` 时通知您。
- 只有当告警处于 OK（正常）状态时，才能测试通知。

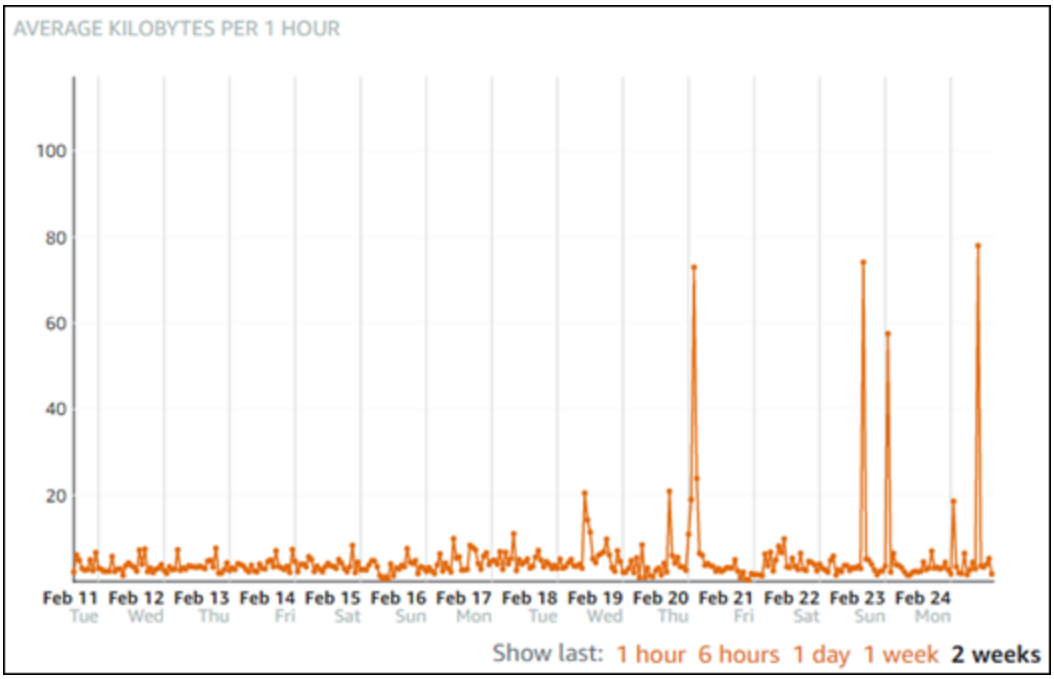
配置负载均衡器告警的最佳实践

以下限制适用于告警：

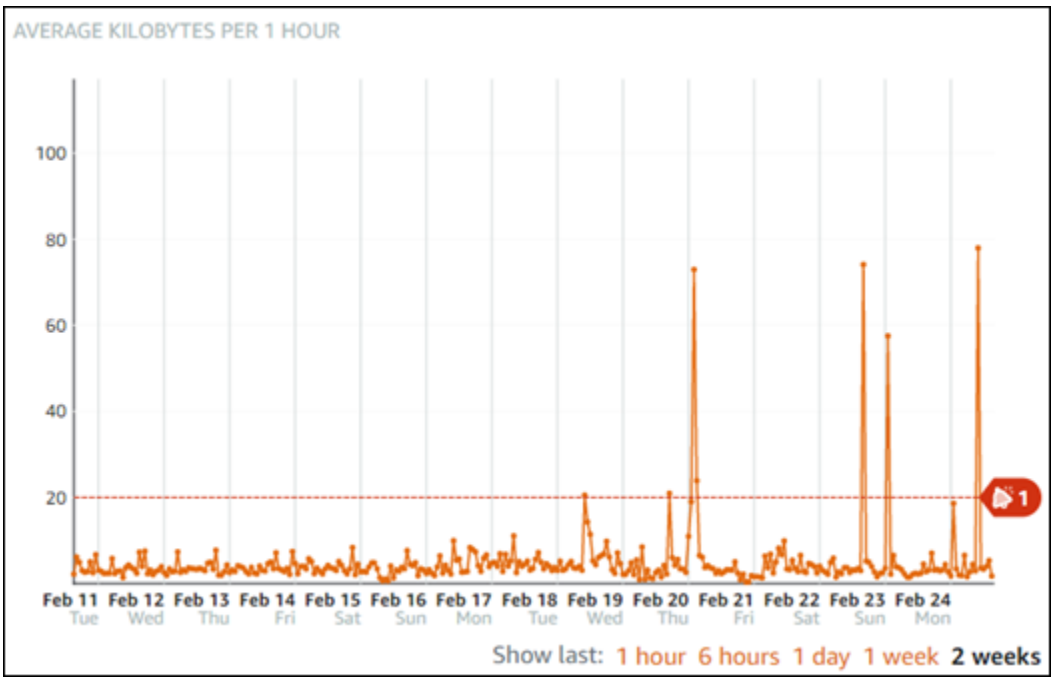
- 您可以为每个指标配置两个告警。
- 每隔 5 分钟评估一次告警，告警的每个数据点代表一个 5 分钟时段的聚合指标数据。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能配置告警以在告警状态变为 OK 时通知您。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，则您只能测试 OK 告警通知。
- 如果您将告警配置为通过电子邮件和/或 SMS 文本消息来通知您，以及您对于缺失数据点选择 Do not evaluate the missing data (不评估缺失数据) 选项，则您只能配置告警以在告警状态变为 `INSUFFICIENT_DATA` 时通知您。
- 只有当告警处于 OK（正常）状态时，才能测试通知。

默认告警设置

在配置指标告警之前，您应该查看该指标的历史数据。识别过去两周内低级、中级和高级的指标情况。在以下实例传出网络流量 (`NetworkOut`) 指标图表示例中，低级为每小时 0-10 KB，中级为每小时 10-20 KB，高级为每小时 20-80 KB。



如果将告警阈值配置为大于或等于低级范围内的某个值（例如，每小时 5 KB），那么您将收到更频繁且可能不必要的告警通知。如果将告警阈值配置为大于或等于高级范围内的某个值（例如，每小时 20 KB），那么您将很少收到通知，但可能也是更重要的需要调查的情况。当您配置并启用告警时，图表上会显示一条表示阈值的告警线，如以下示例所示。标记为 1 的告警线表示告警 1 的阈值，标记为 2 的告警线表示告警 2 的阈值。



使用 Lightsail 控制台创建负载平衡器指标警报

完成以下步骤，使用 Lightsail 控制台创建负载均衡器指标警报。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要为其创建警报的负载均衡器的名称。
4. 选择负载均衡器管理页面上的指标选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要创建告警的指标。有关更多信息，请参阅资源指标。
6. 在页面的 Alarms (告警) 部分选择 Alarms (添加告警)。
7. 在下拉菜单中选择比较运算符值。示例值为大于或等于、大于、小于以及等于。
8. 输入告警的阈值。
9. 输入告警的数据点。
10. 选择评估期。时段可以 5 分钟为增量指定，从 5 分钟到 24 小时。
11. 选择以下通知方法之一：

    - 电子邮件 — 当告警状态变为 ALARM（告警）时，您会收到电子邮件通知。

- SMS 文本消息 — 当告警状态变为 ALARM（告警）时，您会收到 SMS 文本消息通知。并非所有可以创建 Lightsail 资源的 AWS 区域都支持短信，也无法向所有国家/地区发送短信。有关更多信息，请参阅 SMS 文本消息支持。

> **Note**
>
> 如果您选择通过电子邮件或 SMS 进行通知，但尚未在资源的亚马逊云科技区域中配置通知联系人，则需要添加电子邮件地址或手机号码。有关更多信息，请参阅通知。

12. （可选）选择 Send me a notification when the alarm state change to OK（当告警状态变为正常时，向我发送通知），以在告警状态变为 OK（正常）时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
13. （可选）选择 Advanced settings（高级设置），然后选择下列选项之一：
    - 选择告警应如何处理缺失数据。以下选项可用：
      - 假设不在阈值范围内（超出阈值）— 将缺失数据点视为“不良”和超出阈值。
      - 假设在阈值范围内（未超出阈值）— 将缺失数据点视为“良好”和在阈值范围内。
      - 使用最后一个良好数据点的值（忽略并保持当前警报状态）：维持当前警报状态。
      - 不评估（将缺失的数据视为缺失）— 在评估是否更改状态时，告警不考虑缺失数据点。
    - 选择如果数据不足，则发送通知，在告警状态变为 INSUFFICIENT_DATA 时进行通知。仅当您选择通过电子邮件或 SMS 文本消息进行通知时，此选项才可用。
14. 选择 Create (创建) 以添加告警。

之后要编辑警报，选择要编辑的警报旁边的省略号图标（⋮），然后选择编辑警报。

使用 Lightsail 控制台测试负载平衡器指标警报

完成以下步骤，使用 Lightsail 控制台测试警报。您可能需要测试告警以确认已配置的通知选项是否正常工作，例如确保在触发告警时收到电子邮件或 SMS 文本消息。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择联网。
3. 选择要测试告警的负载均衡器的名称。
4. 选择负载均衡器管理页面上的指标选项卡。
5. 在 Metrics Graphs (指标图表) 标题下的下拉菜单中，选择要测试告警的指标。

6. 向下滚动到页面的警报部分，然后选择要测试的警报旁边的省略号图标（⋮）。
7. 请选择以下选项之一：
   - 测试警报通知：选择此选项可测试警报状态变为 ALARM 时的通知。
   - 测试确定通知：选择此选项可测试警报状态变为 OK 时的通知。

   > **Note**
   >
   > 如果这些选项都无法使用，您可能尚未配置告警的通知选项，或者告警当前处于 ALARM 状态。有关更多信息，请参阅负载均衡器告警限制。

   根据您选择的测试选项，告警将立即变为 ALARM 或 OK 状态，并且会根据您配置为告警通知方法的内容发送电子邮件和/或 SMS 文本消息。只有当您选择测试通知时，通知横幅才会显示在 Lightsail 控制台中。ALARM如果您选择测试 OK 通知，将不会显示通知横幅。告警通常会在几秒钟后恢复为实际状态。

创建负载均衡器告警后的后续步骤

对于负载均衡器告警，有其他几项可执行的任务：

- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除通知联系人。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

为 Lightsail 监控设置通知联系人

您可以将 Amazon Lightsail 配置为在您的某个实例、数据库、负载均衡器或内容分发网络 (CDN) 分配的指标超过指定阈值时通知您。通知的形式可以是 Lightsail 控制台中显示的横幅、发送到您指定地址的电子邮件或发送到您指定的手机号码的 SMS 短信。要通过电子邮件和短信收到通知，您必须将您的电子邮件地址和手机号码添加为要监控资源的每个 AWS 区域 位置的通知联系人。有关通知的更多信息，请参阅通知。

> **Important**
>
> 短信功能已暂时禁用，目前任何 AWS 区域 可以创建 Lightsail 资源的地方都不支持该功能。有关更多信息，请参阅 SMS 文本消息收发支持。

内容

- 区域通知联系限制
- SMS 文本消息收发支持
- 电子邮件联系人验证
- 使用 Lightsail 控制台添加通知联系人
- 使用添加通知联系人 AWS CLI
- 添加通知联系人后的后续步骤

区域通知联系人限制

每个地址中只能添加一个电子邮件地址和一个手机号码 AWS 区域。如果您在已添加电子邮件地址或手机号码的区域中添加电子邮件地址或手机号码，系统将询问您是否要用新联系人替换现有的通知联系人。

如果您需要在中包含多个电子邮件收件人 AWS 区域，则可以配置一个转发给多个收件人的通讯组列表，并将该通讯组列表的电子邮件地址添加为通知联系人。

SMS 文本消息收发支持

> **Important**
>
> 短信功能已暂时禁用，目前任何 AWS 区域 可以创建 Lightsail 资源的地方都不支持该功能。或者，您可以配置电子邮件或依赖 Lightsail 控制台中显示的通知横幅。
> 以下有关 SMS 文本消息收发支持的信息，是针对在我们禁用此功能前就已经配置了 SMS 文本消息收发的客户而发布的。

并非所有可以创建 Light AWS 区域 sail 资源的版本都支持短信。此外，SMS 文本消息可能无法发送到世界上的有些国家和地区。对于不支持 SM AWS 区域 S 消息的，您只能配置电子邮件通知联系人。

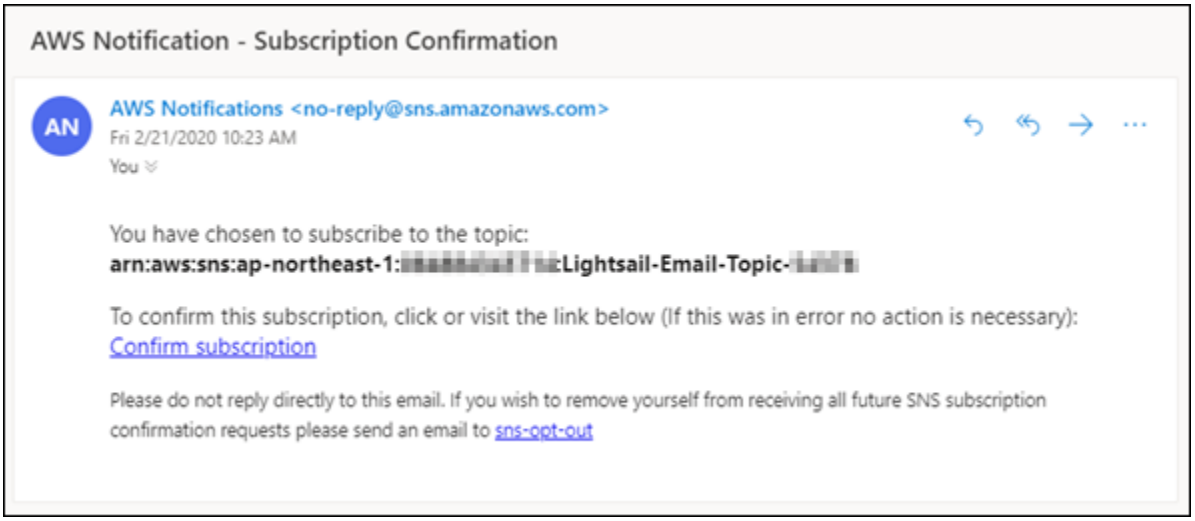
以下 AWS 区域版本支持短信。以下是亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 支持短信的地区，Lightsail 使用该服务向您发送通知：

- 美国东部（弗吉尼亚州北部）(us-east-1)
- 美国西部（俄勒冈州）(us-west-2)
- 亚太地区（新加坡）(ap-southeast-1)
- 亚太地区（悉尼）(ap-southeast-2)
- 亚太地区（东京）(ap-northeast-1)
- 欧洲地区（爱尔兰）(eu-west-1)

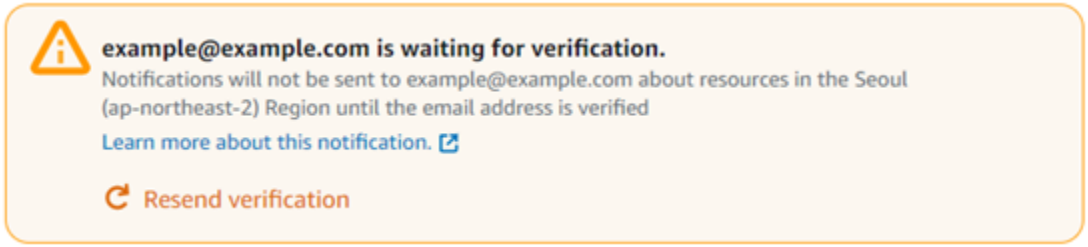
有关世界上可以发送 SM AWS 区域 S 短信的国家和地区的列表，以及最新支持短信的国家和地区，请参阅 Amazon SNS 开发者指南中的支持地区和国家。

电子邮件联系人验证

当您在 Lightsail 中添加电子邮件地址作为通知联系人时，系统会向该地址发送验证请求。验证请求电子邮件中包含一个链接，收件人必须单击该链接才能确认他们想要接收 Lightsail 通知。在验证后才会将通知发送到电子邮件地址。验证来自亚马逊云科技 通知 < no-reply@sns.amazonaws.com >，其主题是亚马逊云科技 Notification - Subscription Confirmation。SMS 消息收发不需要验证。



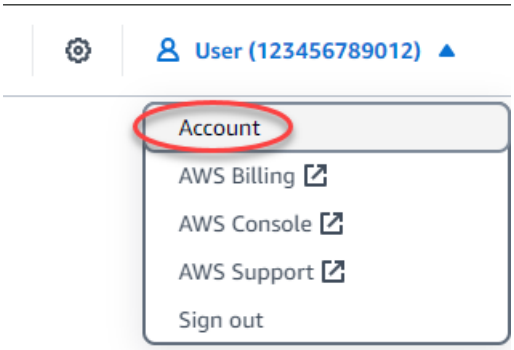
如果验证请求不在收件箱文件夹中，请检查邮箱的垃圾邮件和垃圾邮件文件夹。如果验证请求丢失或被删除，请在 Lightsail 控制台中显示的通知横幅和 “帐户” 页面中选择 “重新发送验证”。



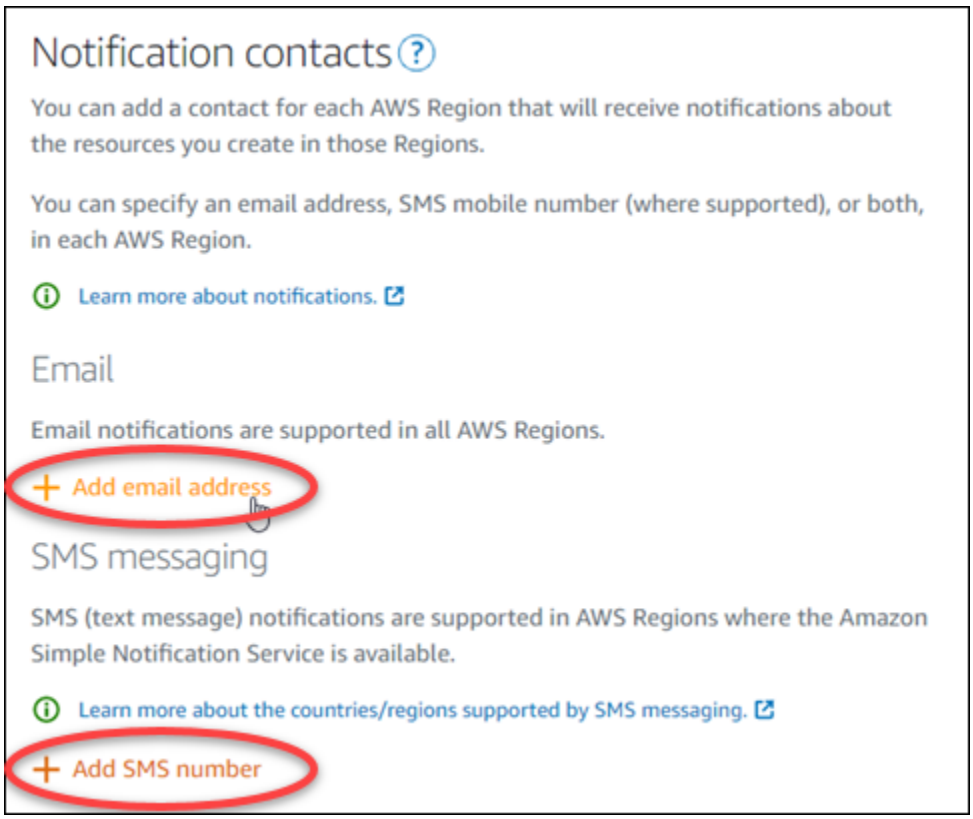
使用 Lightsail 控制台添加通知联系人

完成以下步骤，使用 Lightsail 控制台添加通知联系人。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。

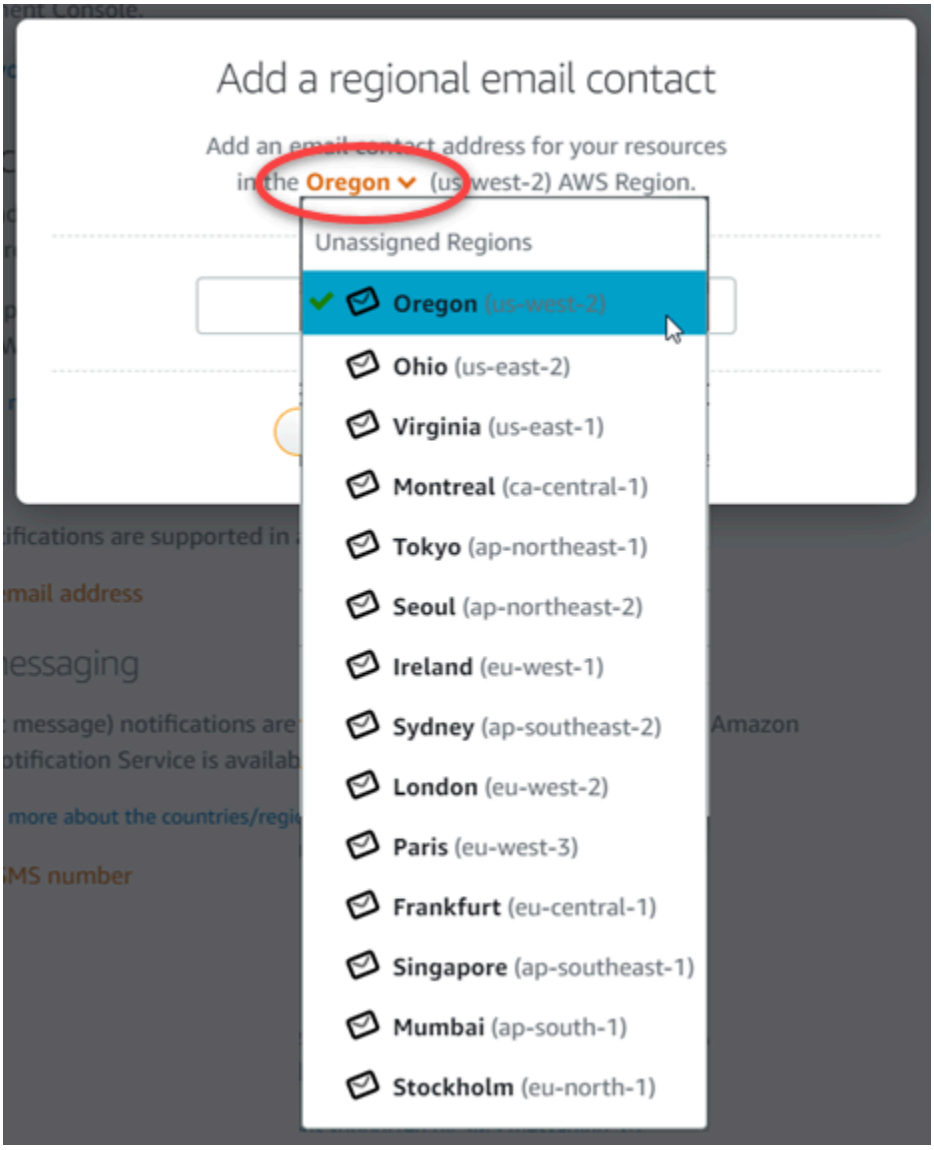


4. 在个人资料和联系人选项卡上的通知联系人部分中选择添加电子邮件地址或添加 SMS 号码。



5. 完成下列步骤之一：

   - 如果您要添加电子邮件地址，请选择要添加通知联系人的 AWS 区域 位置。在文本框中输入电子邮件地址。



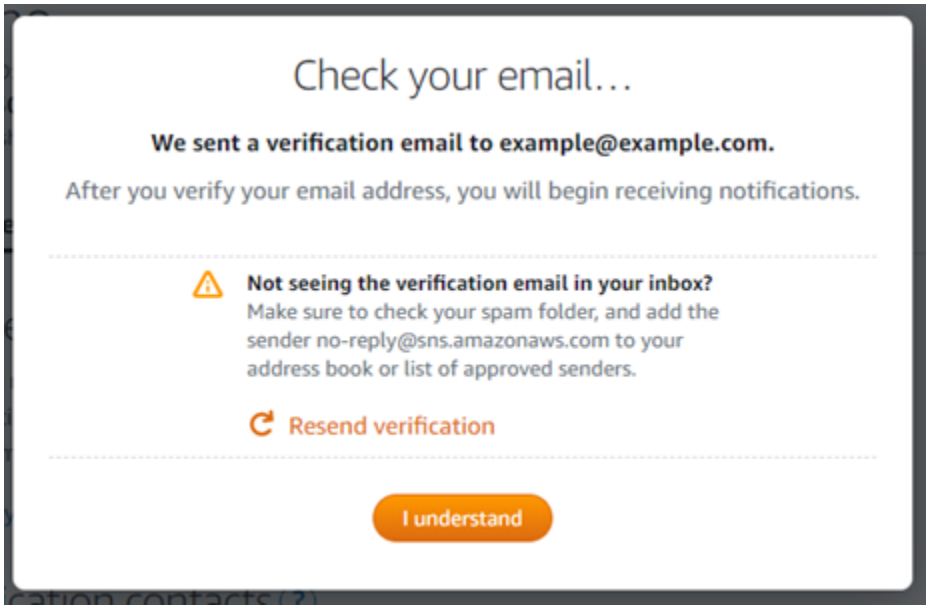
- 如果您要添加 SMS 号码，请选择要添加通知联系人的 AWS 区域 位置。选择手机号码所在的国家/地区，然后将其输入到文本框中。已为您输入国家/地区代码。

> **Important**
>
> 短信功能已暂时禁用，目前任何 AWS 区域 可以创建 Lightsail 资源的地方都不支持该功能。有关更多信息，请参阅 SMS 文本消息收发支持。



6. 选择 Add Contact (添加联系人)。

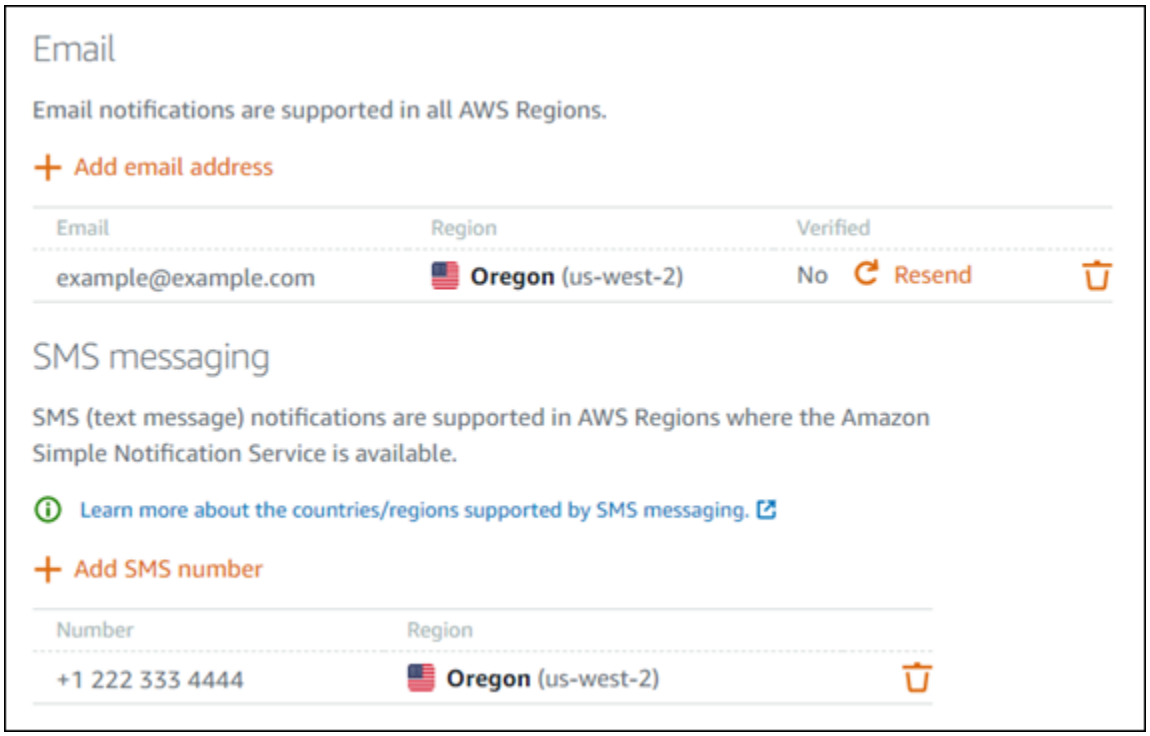
   当您添加电子邮件地址作为通知联系人时，会向该地址发送验证请求。验证请求电子邮件中包含一个链接，收件人必须单击该链接才能确认他们想要接收 Lightsail 通知。SMS 消息收发不需要验证。



7. 选择我了解。

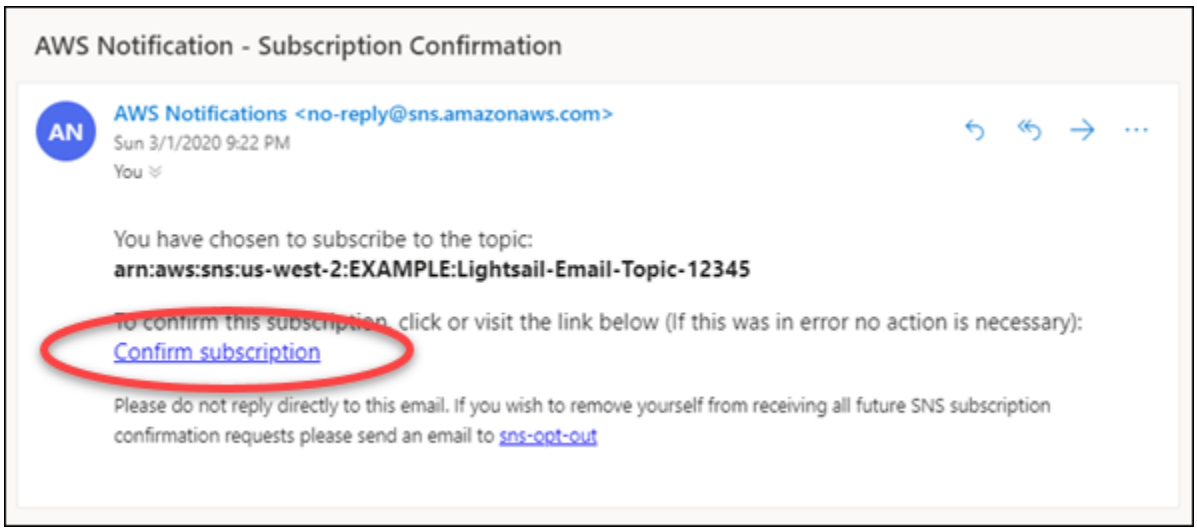
您的电子邮件地址或手机号码将添加到通知联系人部分。在您完成以下步骤中的验证过程之前，不会验证电子邮件地址。在验证后才会将通知发送到电子邮件地址。如果验证请求丢失或被删除，请在其中一个区域电子邮件地址旁边选择重新发送，以发送另一个验证请求。

> **Note**
>
> SMS 消息收发不需要验证。因此，您不需要在添加 SMS 通知联系人后完成此过程中的步骤 8 到 10。



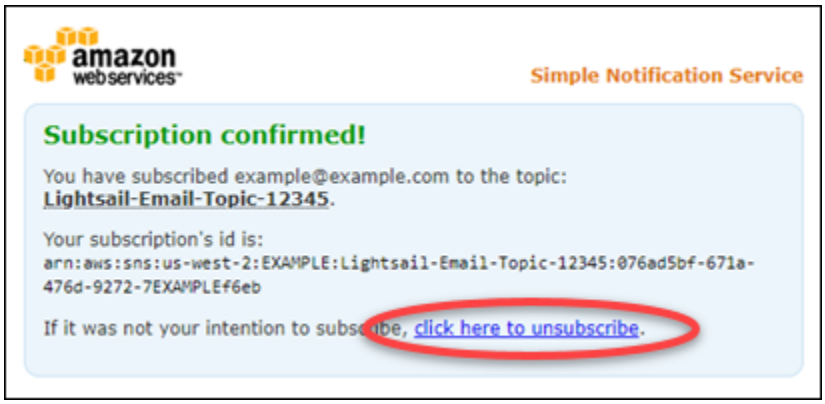
8. 打开您在 Lightsail 中添加为通知联系人的电子邮件地址的收件箱。
9. 打开来自 no-reply@sns.amazonaws.com 的 AWS 通知 – 订阅确认电子邮件。

> **Note**
>
> 如果验证请求不在收件箱文件夹中，请检查邮箱的垃圾邮件和垃圾邮件文件夹。



10. 在电子邮件中选择 “确认订阅”，以确认您要接收 Lightsail 通知。

    将打开一个浏览器窗口，显示以下确认订阅的页面。要取消订阅，请选择页面上的单击此处取消订阅。或者，如果您已关闭页面，请完成删除通知联系人的步骤。



使用 AWS CLI添加通知联系人

完成以下步骤，使用 AWS Command Line Interface ()AWS CLI为 Lightsail 添加通知联系人。

1. 打开终端或命令提示符窗口。

   如果你还没有，请安装 AWS CLI 并将其配置为与 Lightsail 配合使用。

2. 输入以下命令以添加通知联系人：

```
aws lightsail create-contact-method --region Region --notificationProtocol Protocol
 --contact-endpoint Destination
```

在该命令中，将：

- *Region*应 AWS 区域 在其中添加通知联系人。
- *Protocol*使用联系人的通知协议，应为电子邮件或短信。
- *Destination*使用您的电子邮件地址或手机号码。

> **Note**
>
> 指定手机号码时使用 E.164 格式。E.164 是用于国际电信的电话号码结构标准。采用此格式的电话号码最多可包含 15 位数字，并以加号 (+) 和国家代码作为前缀。例如，将 E.164 格式的美国电话号码指定为 +1 XXX555 0100。有关更多信息，请参阅 Wikipedia 中的 E.164。

示例：

```
aws lightsail create-contact-method --region us-west-2 --notificationProtocol Email
 --contact-endpoint example@example.com
```

```
aws lightsail create-contact-method --region us-east-1 --notificationProtocol SMS
 --contact-endpoint +14445556666
```

当您按 Enter 键时，您将看到一个操作响应，其中包含有关请求的详细信息。

验证请求将发送到您指定为通知联系人的电子邮件地址。这可以确认收件人想要订阅 Lightsail 通知。只有在完成以下步骤中的验证过程后才会验证电子邮件地址。在验证电子邮件地址后才会将通知发送到电子邮件地址。如果原始通知放错了位置，请在其中一个区域电子邮件地址的旁边选择重新发送，以发送另一个验证请求。

> **Note**
>
> SMS 消息收发不需要验证。因此，当您添加 SMS 通知联系人时，您不需要完成此过程中的步骤 8 到 10。

3. 打开您添加为通知联系人的电子邮件地址的收件箱。
4. 打开来自 no-reply@sns.amazonaws.com 的 AWS 通知 – 订阅确认电子邮件。
5. 在电子邮件中选择 “确认订阅”，以确认您要接收来自 Lightsail 的电子邮件通知。

   将打开一个浏览器窗口，显示以下确认订阅的页面。要取消订阅，请选择页面上的单击此处取消订阅。或者，如果您已关闭页面，请完成删除通知联系人的步骤。

添加通知联系人后的后续步骤

对于通知联系人，有其他几项可执行的任务：

- 在您添加通知联系人的 AWS 区域 位置添加警报。您可以选择在告警开始时通过电子邮件和 SMS 文本消息进行通知。有关更多信息，请参阅警报。
- 如果您在预期收到通知时没有收到通知，请检查确认您的通知联系人是否正确配置。要了解更多信息，请参阅排除通知的故障。
- 要停止接收通知，您可以从 Lightsail 中移除您的电子邮件和手机。有关更多信息，请参阅删除或禁用指标警报。您还可以禁用或删除告警以停止接收特定告警的通知。有关更多信息，请参阅删除或禁用指标警报。

在 Lightsail 中删除通知联系人

从 Amazon Lightsail 中删除您的电子邮件和手机号码通知联系人，以停止接收有关您的 Lightsail 资源的电子邮件和短信通知。有关通知的更多信息，请参阅通知。

您还可以禁用或删除警报以停止接收特定警报的通知。有关更多信息，请参阅删除或禁用指标警报。

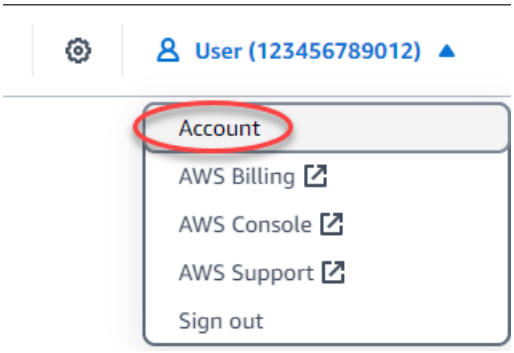
内容

- 使用 Lightsail 控制台删除通知联系人
- 使用删除通知联系人 AWS CLI
- 删除通知联系人后的后续步骤

使用 Lightsail 控制台删除通知联系人

完成以下步骤，使用 Lightsail 控制台删除通知联系人。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，在顶部导航菜单上选择您的用户或角色。
3. 在下拉菜单中选择账户。



4. 在个人资料和联系人选项卡上的通知联系人部分中，选择要删除的电子邮件地址或手机号码旁边的删除图标。
5. 选择是以确认您要删除通知联系人。

使用 AWS CLI删除通知联系人

完成以下步骤，使用 AWS Command Line Interface ()AWS CLI删除 Lightsail 的通知联系人。

1. 打开终端或命令提示符窗口。

   如果你还没有，请安装 AWS CLI 并配置它以与 Lightsail 配合使用。
2. 输入以下命令可删除通知联系人：

```
aws lightsail delete-contact-method --region Region --notificationProtocol Protocol
```

   在该命令中，将：

   - *Region*应 AWS 区域 在其中删除通知联系人。
   - *Protocol*使用您要删除的联系人的通知协议，例如电子邮件或短信。

   示例：

```
aws lightsail delete-contact-method --region us-west-2 --notificationProtocol SMS
```

   当您按 Enter 键时，您将看到一个操作响应，其中包含有关请求的详细信息。

删除通知联系人后的后续步骤

删除通知联系人后，有其他几项可执行的任务：

- 删除通知联系人会停止电子邮件和短信通知，但不会阻止通知横幅显示在 Lightsail 控制台中。要停止通知横幅以及停止电子邮件和 SMS 文本消息收发通知，请禁用或删除导致这些通知的警报。有关更多信息，请参阅删除或禁用指标警报。
- 在 Lightsail 中添加您的电子邮件地址和手机号码作为通知联系人，即可重新开始接收电子邮件和 SMS 短信通知。有关更多信息，请参阅添加通知联系人。

查看等待验证的 Lightsail 警报通知和联系人

您可以在 Lightsail 控制台的 “警报通知” 页面上查看所有亚马逊 Lightsail 资源的活动警报和通知。此页面整合了处于`In alarm`状态的警报，即已启用且当前已超过您定义的阈值的警报。您还可以查看待验证的电子邮件联系人。有关警报的更多信息，请参阅 Lightsail 中的指标警报。有关警报通知的更多信息，请参阅为 Lightsail 资源配置指标通知。

主题

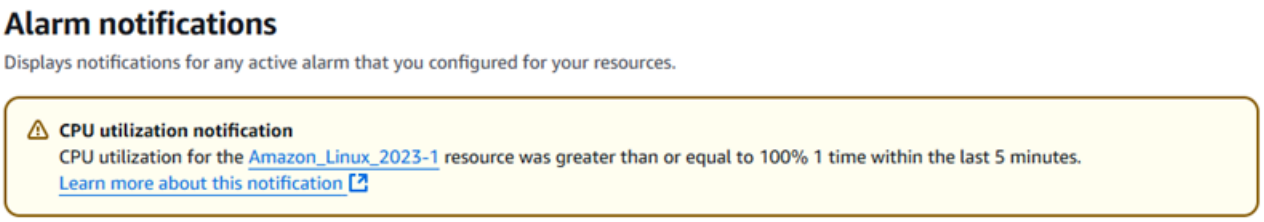
- 查看警报通知以了解活动警报
- 查看待验证的电子邮件联系人

查看警报通知以了解活动警报

你可以在 Lightsail 控制台中查看所有资源的 Lightsail 警报通知。每个条目都将包含有关警报为何处于活动状态以及警报所属资源的更多详细信息。有关如何添加警报的信息，请参阅配置告警。

查看活动警报的警报通知

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择警报通知。
3. 在 “警报通知” 下，您可以查看您的活动警报。

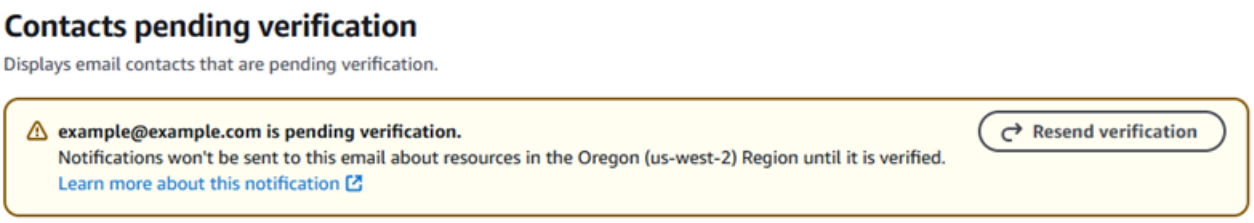


查看待验证的电子邮件联系人

您可以在 Lightsail 控制台中查看待验证的电子邮件联系人。每个条目都将包括电子邮件地址、通知用途，以及重新发送验证的功能。 AWS 区域 有关如何添加电子邮件联系人的更多信息，请参阅为 Lightsail 监控设置通知联系人。

查看正在等待验证的电子邮件联系人

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择警报通知。
3. 在 “待验证的联系人” 下，您可以查看待验证的电子邮件联系人。

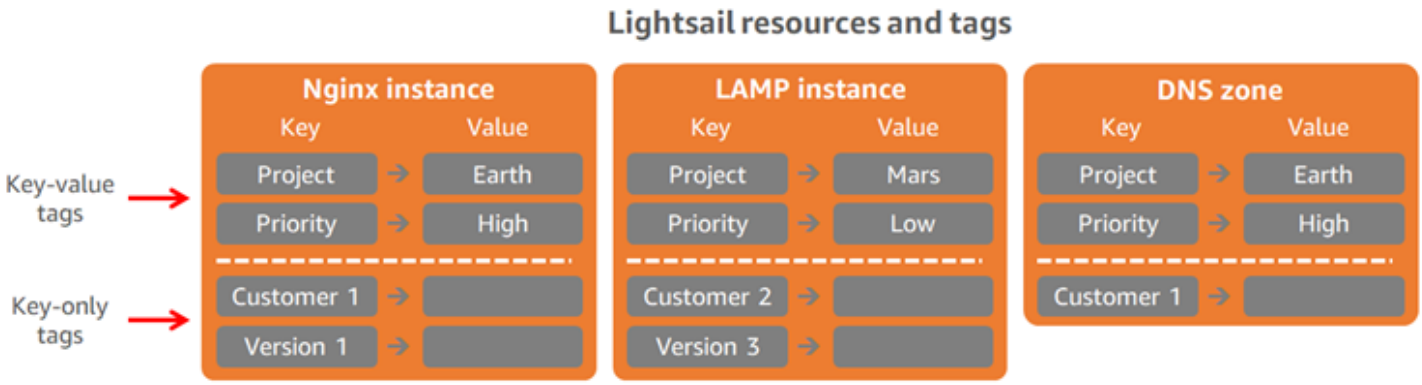


使用标签整理和筛选 Lightsail 资源

借助 Amazon Lightsail，您可以为资源分配标签作为标签。每个标签都是一个标注，包含一个密钥和一个可选值，让您能够更有效地管理、搜索和筛选资源。

借助 Amazon Lightsail，您可以为资源分配标签作为标签。每个标签都是一个标注，包含一个密钥和一个可选值，让您能够有效地管理、搜索和筛选资源。尽管没有固有的标签类型，但它们允许您按用途、所有者、环境或其他标准对 Lightsail 资源进行分类。这在您有许多相同类型的资源时会非常有用。您可以根据分配到特定资源的标签来快速识别该资源。例如，为资源定义一组标签，以帮助跟踪每个资源的项目或优先级。

在 Lightsail 中，没有值的密钥被称为纯密钥标签。具有值的键被称为“键-值”标签。下图说明了标签的工作方式。在本示例中，每个资源都有一组标签，即“键-值”标签和“仅限键”标签。“键-值”标签用于标识项目和优先级，“仅限键”标签用于标识客户和应用程序版本。



使用标签整理账单并控制访问

您还可以使用标签来组织账单、控制 Lightsail 中资源和请求的访问权限以及控制对标签密钥的访问权限。有关更多信息，请参阅下列指南之一：

- 使用标签整理资源的成本
- 使用标签控制对资源的访问权限

支持标记的 Lightsail 资源

您可以在创建大多数 Lightsail 资源时或创建后对其进行标记。如果在资源创建期间无法应用标签，Lightsail 会回退资源创建过程。这有助于确保：要么创建带有标签的资源，要么根本不创建资源，也就是说，任何时候都不会出现应该被标记的资源却未被标记的情况。

可以在 Lightsail 控制台中标记以下 Lightsail 资源：

- 实例
- 容器服务
- 内容分发网络 (CDN) 分配
- 存储桶
- 数据库
- 磁盘
- DNS 区域
- 负载均衡器

> **Important**
>
> 使用 Lightsail 控制台创建的快照会自动继承源资源的标签。根据该快照创建的 Lightsail 资源将具有创建快照时源资源上存在的相同标签。

可以使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或对以下资源进行标记： SDKs

- 数据库快照
- 数据库
- 磁盘快照
- 磁盘
- 域 (DNS 区域)
- 实例快照
- 实例
- 密钥对
- 负载均衡器 TLS 证书（使用 Lightsail 创建的 TLS 证书）
- 负载均衡器

> **Important**
>
> 使用 Lightsail API 或创建的快照 SDKs 不会自动从源资源继承标签。 AWS CLI相反，您必须使用 `tags` 参数从源资源手动指定标签。

标签限制

下面是适用于标签的基本限制：

- 每个资源的最大标签数为 50。
- 每个资源的每个标签键都必须是唯一的。每个标签键只能有一个值。
- 最大键长度 – 128 个 Unicode 字符（采用 UTF-8 格式)。
- 最大值长度 – 256 个 Unicode 字符（采用 UTF-8 格式)。
- 如果标签方案针对多个服务和资源使用，请记得其他服务可能对支持的字符有限制。通常允许使用的字符包括：字母、数字和空格，以及 + - = . _ : / @ 这几个字符
- 标签键和值区分大小写。
- 请不要使用 `aws:` 作为键或值的前缀。此前缀是专门预留下来以供亚马逊云科技使用的。

使用标签对 Lightsail 资源进行分类

使用 Amazon Lightsail 中的标签按用途、所有者、环境或其他标准对您的资源进行分类。可在资源创建过程中或创建后添加标签。请按照以下步骤，在创建资源后向其添加标签。

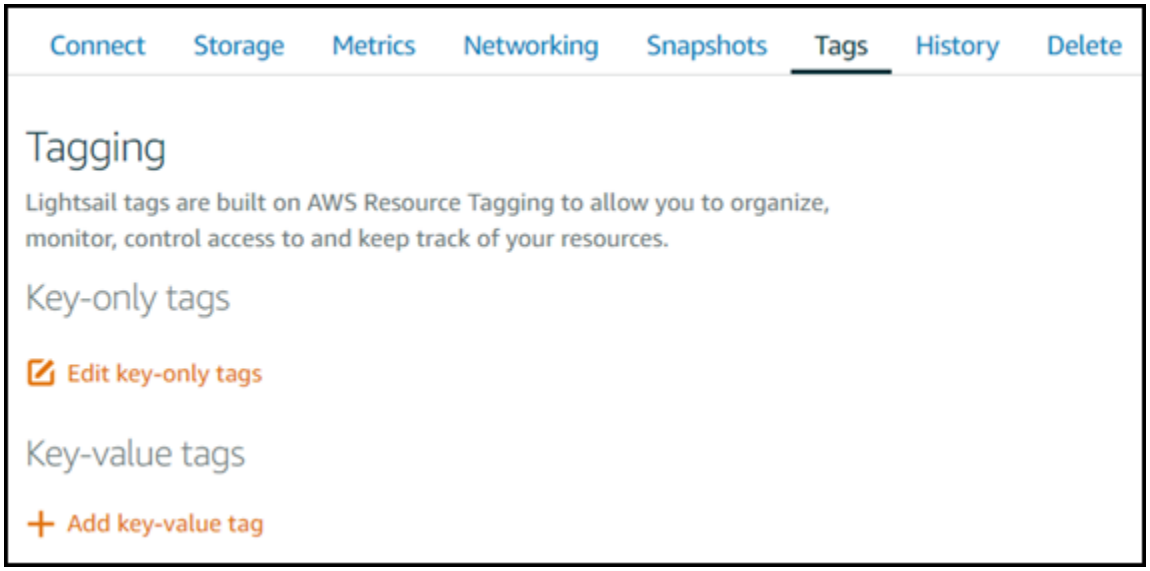
> **Note**
>
> 有关标签、可添加标签的资源以及限制的更多信息，请参阅标签。

为资源添加标签

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择要标记的资源类型的对应选项卡。例如，要向 DNS 区域添加标签，请选择 Networking (联网) 选项卡。或者，选择 Instances (实例) 选项卡以向实例添加标签。

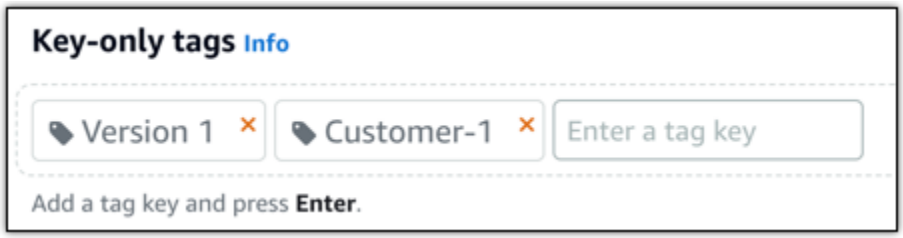
> **Note**
>
> 可以使用 Lightsail 控制台标记实例、容器服务、CDN 分发、存储桶、数据库、磁盘、DNS 区域和负载均衡器。但是，可以使用 Lightsail API 操作或 () 或，对更多 Lightsail 资源进行标记。AWS Command Line InterfaceAWS CLI SDKs有关支持标记的 Lightsail 资源的完整列表，请参阅标签。

3. 选择要添加标签的资源。
4. 在您选择的资源的管理页面中，选择 Tags (标签) 选项卡。



5. 根据您要添加的标签类型，选择以下任一选项：

   - Add key-only tags（添加仅包含键的标签）或 Edit key-only tags（编辑仅包含键的标签）（如果已添加标签）。在标签键文本框中输入新标签，然后按 Enter。在您输入标签以添加它们后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

   - 创建一个键值标签，然后在 Key（键）文本框中输入一个键，并在 Value（值）文本框中输入一个值。输入标签后，选择 Save（保存），或者选择 Cancel（取消）以取消添加。

     一次只能添加一个键值标签，然后进行保存。要添加多个键值标签，请重复前面的步骤。



后续步骤

有关向资源添加标签后可执行的任务的更多信息，请参阅以下指南：

- 使用标签整理资源
- 使用标签整理资源的成本
- 使用标签控制对资源的访问权限
- 删除标签

从 Lightsail 资源中移除标签

您可以从 Amazon Lightsail 资源中删除标签。从一个资源中删除标签不会删除所有其他资源中的相同标签。要从所有资源中完全删除某个标签，您必须分别从每个资源中删除该标签。本指南提供了从资源中删除标签的步骤。

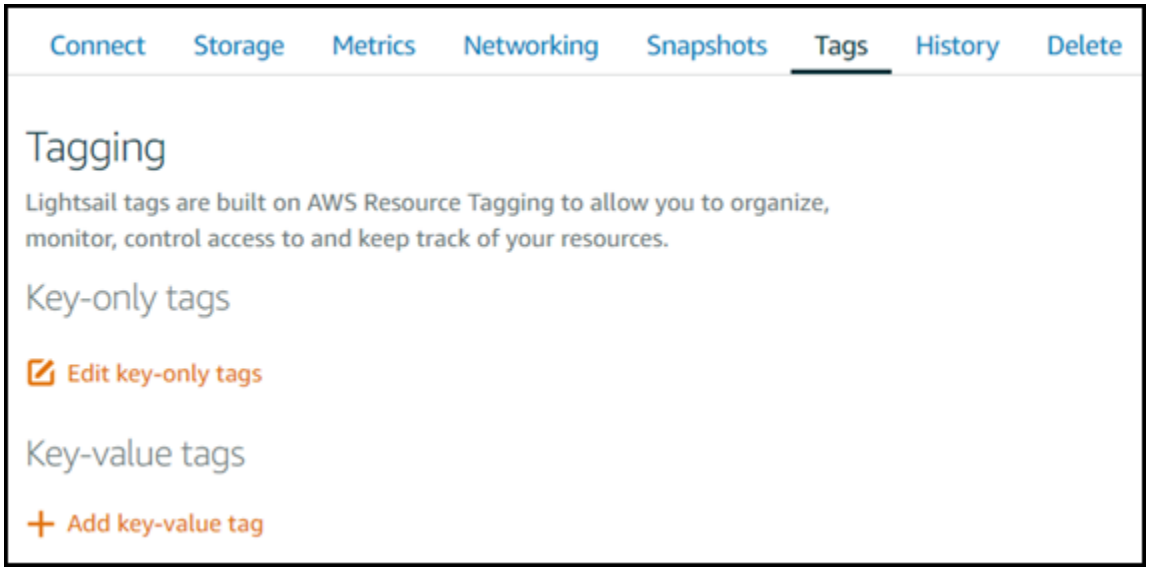
> **Note**
>
> 有关标签、可添加标签的资源以及标签限制的更多信息，请参阅标签。

从资源中删除标签

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择要从中删除标签的资源类型。例如，要从 DNS 区域删除标签，请选择联网。或者，选择实例以从实例中删除标签。

> **Note**
>
> 可以使用 Lightsail 控制台标记实例、容器服务、CDN 分发、存储桶、数据库、磁盘、DNS 区域和负载均衡器。但是，可以使用 Lightsail API 操作或AWS 命令行界面 () 或，对更多 Light sail 资源进行标记。AWS CLI SDKs有关支持标记的 Lightsail 资源的完整列表，请参阅标签。

3. 选择要从中删除标签的资源。
4. 在所选资源的管理页面中，选择 Tags (标签) 选项卡。



5. 根据要从该资源中删除的标签类型，执行以下任一操作：

   a. 选择 Edit key-only tags（编辑仅包含键的标签），然后为要从资源中删除的标签选择删除图标 (X)。删除标签后，选择保存以将其从资源中删除，或选择取消以取消删除。



   b. 要删除键值标签，请为相应的键值标签选择删除图标 (X)。在提示符处，选择是，删除以删除键值标签，或选择否，取消以取消删除。



使用资源级权限和基于标签的授权控制对 Lightsail 资源的访问权限

Lightsail 支持其某些 API 操作的资源级权限和基于标签的授权。有关更多信息，请参阅《服务授权参考》中的 Amazon Lightsail 的操作、资源和条件密钥。

使用标签控制 Lightsail 资源的访问权限

您可以在 Amazon Lightsail 中使用标签来控制对资源的访问权限、控制对请求的访问以及对标签密钥的访问权限。在本指南中，您将学习如何创建 AWS Identity and Access Management (IAM) 策略，该策略指定创建或删除 Lightsail 资源所需的键值标签，并将该策略附加到需要提出这些请求的用户或群组。

> **Note**
>
> 要详细了解 Lightsail 中的标签、可以标记哪些资源以及限制，请参阅标签。

步骤 1：创建 IAM policy

首先，在 IAM 控制台中创建以下 IAM policy。有关创建 IAM policy 的更多信息，请参阅 IAM 文档中的创建 IAM policy。

除非在创建请求中定义了密钥标签`allow`和值`true`，否则以下策略限制用户创建新的 Lightsail 资源。该策略还会限制用户删除资源，除非他们具有 `allow/true` 键值标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "lightsail:Create*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/allow": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Delete*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allow": "true"
                }
            }
        }
    ]
}
```

以下策略会限制用户更改其键值标签不是 allow/false 的资源的标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
}
```

步骤 2：将策略附加到用户或组

创建 IAM 策略后，将这些策略附加到需要使用键值对创建 Lightsail 资源的用户或组。有关将 IAM 策略附加到用户或组的更多信息，请参阅 IAM 文档中的添加和删除 IAM 策略。

使用标签整理 Lightsail 资源成本

您可以使用 Amazon Lightsail 中的标签来组织 AWS 账单，以反映您自己的成本结构。为此，请向你的 Lightsail 资源添加键值标签。然后在 AWS 账单与成本管理 控制台中激活这些标签。最后，注册以获取包含在成本分配报告中包含的标签键值的 AWS 账户账单。本指南提供了相关的设置步骤。

> **Note**
>
> 有关 Lightsail 中的标签、可以标记哪些资源以及标签限制的更多信息，请参阅标签。

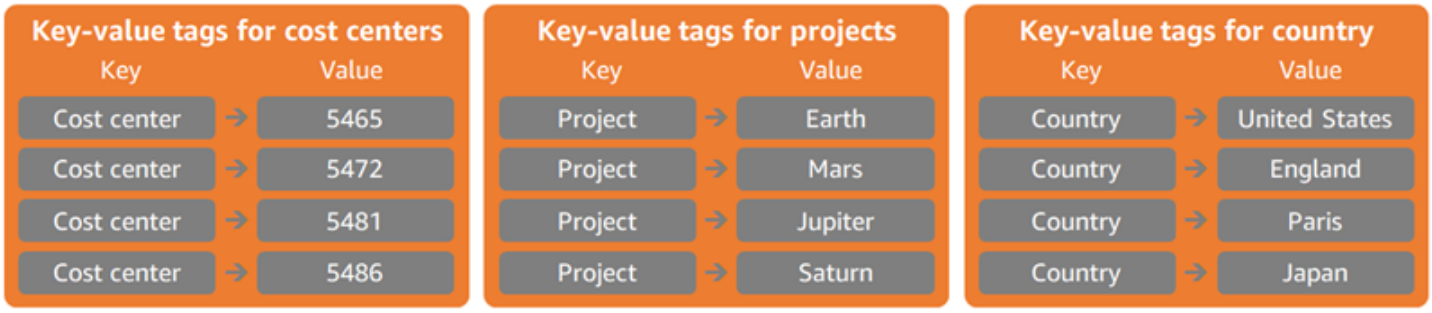
> **Important**
>
> 目前，即使在成本分配报告中添加了成本分配标签，也无法在成本分配报告中跟踪 Lightsail 数据库快照。

步骤 1：向资源添加键值标签

为要在账单控制台中整理的 Lightsail 资源添加键值标签。有关键值标签的更多信息，请参阅向资源添加标签。

设置一组能反映成本组织方式的标签键是一种好的做法。您的成本分配报告会将这些标签键作为附加列进行显示，其中包含针对每个行的适用值。因此，如果您使用的是一组具有一致性的标签键，那么成本

跟踪会更加高效。例如，您可以使用特定的成本中心标记多个 Lightsail 资源。可通过将“Cost center”键与一个数值配对来完成此操作。然后整理账单信息，以跨多个资源查看该成本中心所对应的账单。以下示例显示了可用于整理成本分配的键值标签：



步骤 2：激活用户定义的成本分配标签

向 Lightsail 资源添加必要的标签后，请在账单和成本管理控制台中激活这些标签以进行成本分配。例如，如果您创建了“Cost center”键标签，请在账单和成本管理控制台中激活该键标签，为该标签生成成本分配报告。有关更多信息，请参阅 AWS 账单与成本管理 文档中的激活用户定义的成本分配标签。

步骤 3：设置成本分配报告并进行查看

每月成本分配报告按产品类别和关联账户用户列出了您账户的 AWS 使用情况。该报告包含与您的详细账单报告相同的行项目和用于您标签键的附加列。要设置每月成本分配报告，请参阅 AWS 账单与成本管理 文档中的设置每月成本分配报告。

设置成本分配报告时，您定义了一个从中保存此报告的 Amazon Simple Storage Service（Amazon S3）存储桶。打开您定义的 Amazon S3 存储桶，并在成本分配报告可用后将其打开。有关成本分配报告内容的更多信息，请参阅 AWS 账单与成本管理 文档中的查看成本分配报告。

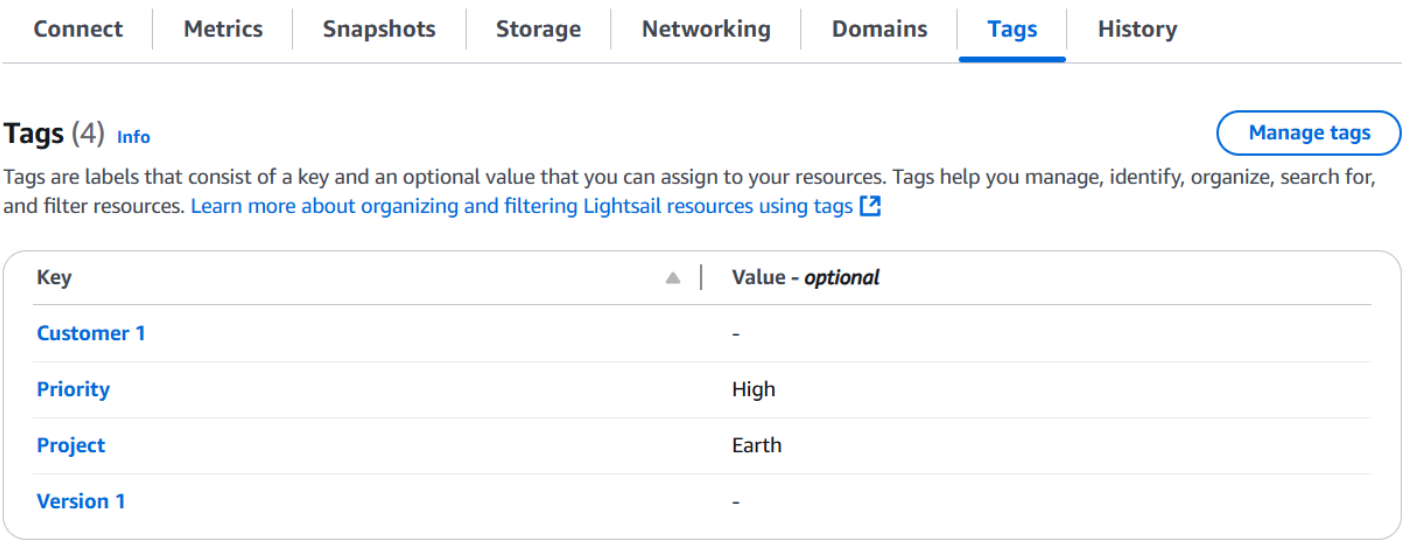
标记用于组织和筛选的 Lightsail 资源

在您为 Amazon Lightsail 资源添加标签后，您可以按已添加的标签筛选资源。您可以在 Lightsail 控制台中通过选择或搜索标签来执行此操作。本指南向您展示如何按标签查看和筛选 Lightsail 资源。

> **Note**
>
> 有关标签、可添加标签的资源以及标签限制的更多信息，请参阅标签。

查看资源的标签

可以使用 Lightsail 控制台标记实例、容器服务、CDN 分发、存储桶、数据库、磁盘、DNS 区域和负载均衡器，因此包含标签选项卡。您可通过资源的管理页面访问该选项卡，如下面的实例资源示例所示。在 Tags (标签) 选项卡上，您可以添加、编辑或删除标签。有关更多信息，请参阅向资源添加标签和删除标签。



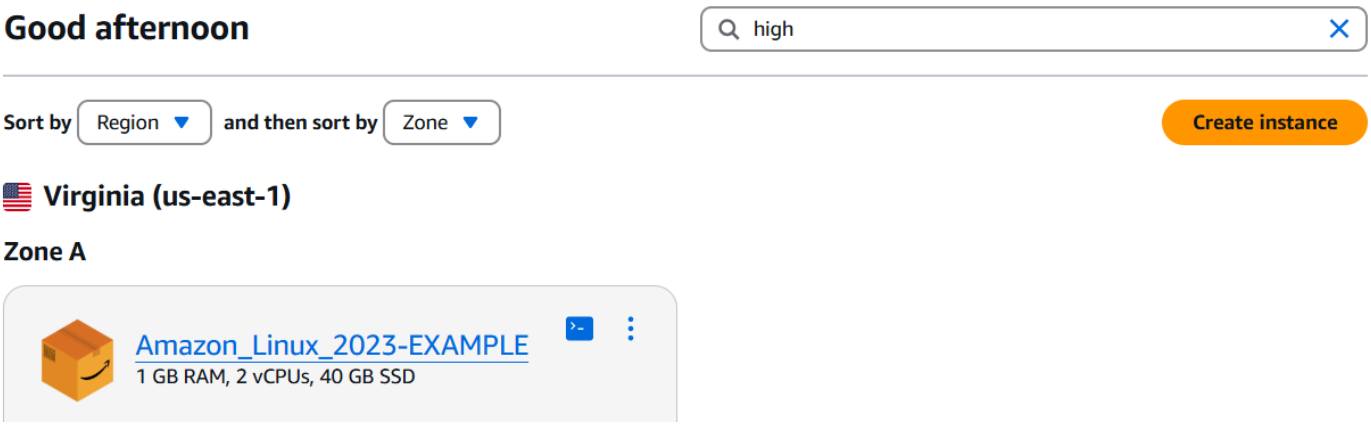
> **Note**
>
> 可以使用 Lightsail 控制台标记实例、容器服务、CDN 分发、存储桶、数据库、磁盘、DNS 区域和负载均衡器。但是，可以使用 Lightsail API 操作或 () 或，对更多 Lightsail 资源进行标记。AWS Command Line InterfaceAWS CLI SDKs有关支持标记的 Lightsail 资源的完整列表，请参阅标签。

使用标签筛选资源

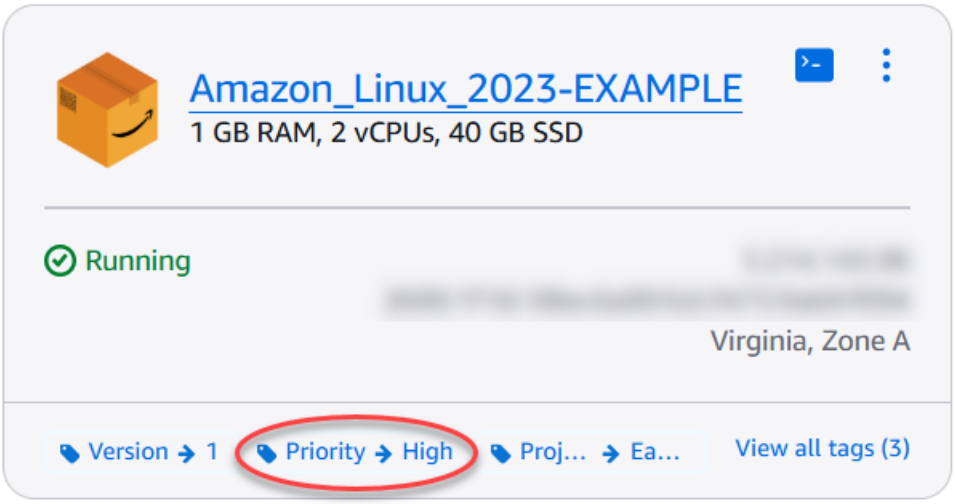
Lightsail 控制台中提供了以下选项，可使用标签筛选您的资源。所有这些选项都会刷新 Lightsail 主页，仅显示您搜索或选择的标签。

> **Note**
>
> 这些筛选选项具有持久性。如果您按标签进行筛选，然后在 Lightsail 主页的各个部分之间导航，则过滤器仍会应用。

- 在 Lightsail 主页上，在 “搜索” 文本框中输入仅限密钥的标签或要筛选的值，然后按 Enter。



- 在 Lightsail 主页上选择一个显示在资源下的标签。



解决常见的 Lightsail 资源问题

本节介绍以下 Amazon Lightsail 资源的疑难解答主题。按照 step-by-step说明和指导来诊断和解决您在使用 Lightsail 实例、数据库、网络、负载均衡器和其他资源时可能遇到的常见问题。

故障排除主题涵盖各种场景，包括 WordPress配置故障、IAM 权限问题、磁盘错误、连接问题、服务不可用、连接、实例容量限制、 IPv6 负载均衡器错误、通知传送失败以及 SSL/TLS 证书问题。通过遵循本指南，您可以有效地排除和解决与Lightsail资源相关的各种问题，从而确保应用程序和工作负载的平稳运行和最佳性能。

主题

- 解决 Lightsail 实例上的 WordPress 设置问题
- 解决 Lightsail 控制台中的 403（未经授权的）错误
- 解决 Lightsail 磁盘连接和使用问题
- 解决基于 Lightsail 浏览器的 SSH 和 RDP 客户端的连接错误
- 对 Lightsail 上的 Ghost 实例 503 服务不可用错误进行故障排除
- 对 Lightsail 中的身份和访问管理 (IAM) Management 进行故障排除
- 验证 Lig IPv6 htsail 实例的可访问性
- 解决 Lightsail 中实例容量不足的错误
- 解决 Lightsail 负载均衡器问题
- 对 Lightsail 中的通知传递进行故障排除
- 对 Lightsail 中的 SSL/TLS 证书进行故障排除

解决 Lightsail 实例上的 WordPress 设置问题

在 Amazon Lightsail 的 WordPress 设置工作流程中，可能会出现两种类型的错误消息：

常见错误

在工作流程的最后一步中选择创建证书后，会立即出现这些类型的错误。这些错误将显示在 Lightsail 控制台顶部的横幅中。它们通常是由在较旧的 WordPress 实例上运行设置工作流程或提交错误信息造成的。例如，选择未指向实例公有 IP 地址的 DNS 记录。

设置失败

这些类型的错误会在您完成工作流程最后一步之后的几分钟内出现。这些失败消息将显示在实例 Connect 选项卡的设置您的 WordPress 网站部分。如果无法在您的实例上配置 Let's Encrypt HTTPS 证书，就会发生这些错误。

使用以下主题中的信息来帮助您诊断和修复 WordPress 安装指导工作流程中可能遇到的任何错误。

主题

- 解决 Lightsail 上的 WordPress 设置错误
- 对 Lightsail 中的 WordPress 设置失败进行故障排除

有关 Amazon Lightsail 中的 WordPress 设置指导工作流程的更多信息，请参阅配置您的 WordPress实例。

解决 Lightsail 上的 WordPress 设置错误

如果在工作流程中提交的信息有问题，Lightsail 控制台的顶部将显示一条错误消息。

消息的第一行通知您设置遇到了错误：

无法*InstanceRegion*在该地区完成您的实例*InstanceName*的设置。

第二行包含设置遇到的错误：

出现错误，我们无法连接或保持与实例的连接



要开始故障排除，请将消息中出现的错误与以下错误之一进行匹配。

错误

- 未找到 DNS 记录。确认域的 DNS 记录指向实例的公有 IP 地址，并留出时间让 DNS 更改进行传播。
- DNS 记录不匹配。确认域的 DNS 记录指向实例的公有 IP 地址，并留出时间让 DNS 更改进行传播。
- 无法连接到实例。等待几分钟时间，让 SSH 连接准备就绪。然后，重新开始设置。

- 不支持的 WordPress 版本。安装程序仅支持 WordPress 版本 6 及更高版本。
- 安装程序仅支持 2023 年 1 月 1 日当天或之后创建的 WordPress 实例。
- 在设置工作流程中，实例防火墙端口 22、80 和 443 必须允许来自任何 IP 地址的 TCP 连接。您可以从“实例联网”选项卡更改这些设置。

未找到 DNS 记录。确认域的 DNS 记录指向实例的公有 IP 地址，并留出时间让 DNS 更改进行传播。

Reason

此错误是由配置错误的 DNS 记录或 DNS 记录没有足够的时间在整个 Internet 的 DNS 中传播引起的。

修复

确认 A 或 AAAA DNS 记录是否存在于 DNS 区域中，并且它们是否指向您实例的公有 IP 地址。有关更多信息，请参阅 Lightsail 中的 DNS。

当您添加或更新指向来自顶级域（`example.com`）及其 `www` 子域（`www.example.com`）的流量的 DNS 记录时，它们需要在整个 Internet 的 DNS 中传播。您可以使用诸如 nslookup 或 DNS 查找之类的工具来验证您的 DN S 更改是否已生效。MxToolbox

> **Note**
>
> 给任何 DNS 记录一些时间在 Internet 的 DNS 内进行传播，这可能需要几个小时。

DNS 记录不匹配。确认域的 DNS 记录指向实例的公有 IP 地址，并留出时间让 DNS 更改进行传播。

Reason

A 或 AAAA DNS 记录未指向实例的公有 IP 地址。

修复

确认 A 或 AAAA DNS 记录是否存在于 DNS 区域中，并且它们是否指向您实例的公有 IP 地址。有关更多信息，请参阅 Lightsail 中的 DNS。

> **Note**
>
> 给任何 DNS 记录一些时间在 Internet 的 DNS 内进行传播，这可能需要几个小时。

无法连接到实例。等待几分钟时间，让 SSH 连接准备就绪。然后，重新开始设置。

Reason

实例刚刚创建或重启，而 SSH 连接尚未准备就绪。

修复

等待几分钟时间，让 SSH 连接准备就绪。然后，重试引导式工作流程。有关更多信息，请参阅 Lightsail 中的 SSH 疑难解答。

不支持的 WordPress 版本。安装程序仅支持 WordPress 版本 6 及更高版本。

Reason

实例上安装 WordPress 的版本早于 WordPress 版本 6。旧 WordPress 版本包含不兼容的软件和依赖关系，会阻止 HTTPS 证书的生成。

修复

从 Lightsail 控制台创建一个新 WordPress 实例。然后，将 WordPress 网站从旧实例迁移到新实例。有关更多信息，请参阅迁移现有 WordPress 博客。

如果您要创建新实例来替换现有实例，请务必将应用程序依赖项更新为新实例。

安装程序仅支持 2023 年 1 月 1 日当天或之后创建的 WordPress 实例。

Reason

用于设置的实例可能包含过时的软件。较旧的软件会阻止生成 HTTPS 证书。

修复

从 Lightsail 控制台创建一个新 WordPress 实例。然后，将 WordPress 网站从旧实例迁移到新实例。有关更多信息，请参阅迁移现有 WordPress 博客。

如果您要创建新实例来替换现有实例，请务必将应用程序依赖项更新为新实例。

在设置工作流程中，实例防火墙端口 22、80 和 443 必须允许来自任何 IP 地址的 TCP 连接。您可以从“实例联网”选项卡更改这些设置。

Reason

在设置运行期间，实例防火墙端口 22、80 和 443 必须允许来自任何 IP 地址的 TCP 连接。当其中一个或多个端口关闭时，就会生成此错误。有关更多信息，请参阅实例防火墙。

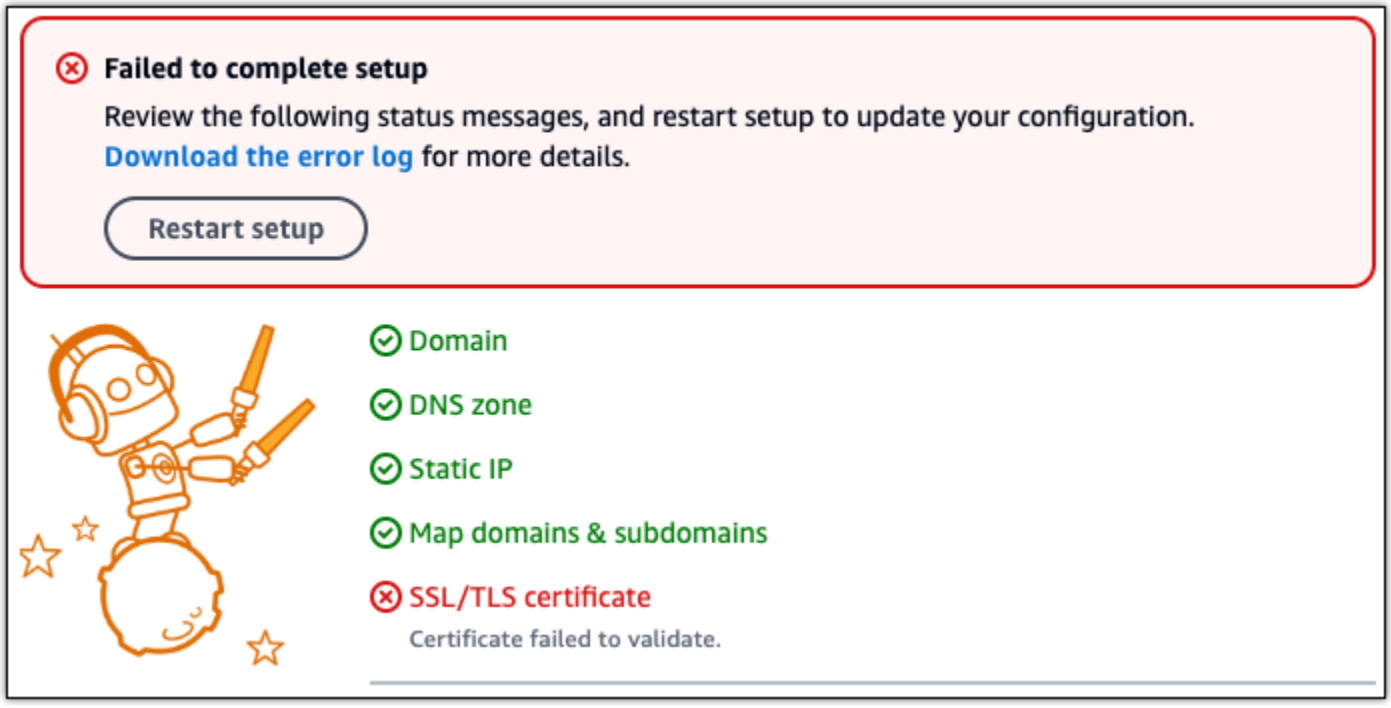
修复

添加或编辑实例 IPv4 和 IPv6 防火墙规则，以允许通过端口 22、80 和 443 进行 TCP 连接。有关更多信息，请参阅添加和编辑实例防火墙规则。

对 Lightsail 中的 WordPress 设置失败进行故障排除

以下信息可以帮助您对可能出现在实例 C onnec t 选项卡的设置您的 WordPress 网站部分的失败消息进行故障排除。设置失败可能在您完成工作流程最后一步之后的几分钟内发生。如果无法在您的实例上配置 Let's Encrypt HTTPS 证书，就会发生这些错误。

未能完成设置 – 查看以下状态消息，然后重新启动设置以更新您的配置。下载错误日志以获取更多详细信息。



从失败消息中，选择下载错误日志链接，下载并查看设置生成的错误日志。要开始故障排除，请将日志中的错误消息与以下错误之一进行匹配。

错误

- certbot.errors。 AuthorizationError: 有些挑战失败了
- Certbot 未能对某些域进行身份验证
- 存储库 http://cdn-aws.deb.debian.org/debian buster-backports 不再有发布文件
- 存储库 http://ppa.launchpad。 net/certbot/certbot/ubuntulunar Release 没有发布文件
- 在过去 168 小时内，已经为此组域颁发太多的证书（5）
- 失败的授权过多

certbot.errors。 AuthorizationError: 有些挑战失败了

Reason

此错误是由配置错误的 DNS 记录或 DNS 记录没有足够的时间在整个 Internet 中传播引起的。

修复

验证 A 或 AAAA DNS 记录是否存在于 DNS 区域中，并且它们是否指向您实例的公有 IP 地址。有关更多信息，请参阅 Lightsail 中的 DNS。

当您添加或更新指向来自顶级域（`example.com`）及其 `www` 子域（`www.example.com`）的流量的 DNS 记录时，它们需要在整个 Internet 中传播。您可以使用诸如 nslookup 或 DNS 查找之类的工具来验证您的 DN S 更改是否已生效。MxToolbox

> **Note**
>
> 给任何 DNS 记录一些时间在 Internet 的 DNS 内进行传播，这可能需要几个小时。

Certbot 未能对某些域进行身份验证

Reason

如果在实例上配置 HTTPS 证书时其他进程使用端口 80，则可能会出现此错误。

修复

重启您的 WordPress 实例。然后，再次运行引导式工作流程。如果重新启动未能解决问题，则使用以下过程终止在端口 80 上运行的实例中正在运行的所有进程。

过程

1. 使用基于 Lightsail 浏览器的 SSH 客户端或使用连接到您的实例。AWS CloudShell
2. 停止在实例上运行的 Bitnami 进程：

```
$ sudo /opt/bitnami/ctlscript.sh stop
```

   验证 Bitnami 进程是否已停止：

```
$ sudo /opt/bitnami/ctlscript.sh status
```

3. 检查是否有其他进程正在使用端口 80：

```
$ fuser -n tcp 80
```

4. 终止其他应用程序不需要的任何进程：

```
$ fuser -k -n tcp 80
```

5. 重新启动 WordPress 安装程序。

存储库 http://cdn-aws.deb.debian.org/debian buster-backports 不再有发布文件

Reason

您的实例上有一个已弃用的 Debian 存储库，并且其无法更新。

修复

使用以下过程编辑 Debian 存储库文件中列出的存储库 URL。

过程

1. 使用基于 Lightsail 浏览器的 SSH 客户端或使用连接到您的实例。AWS CloudShell
2. 导航到 `/etc/apt/sources.list.d/` 目录。

```
$ cd /etc/apt/sources.list.d/
```

3. 使用所选的文本编辑器打开 buster-backports.list 文件。如果在此目录中找不到该文件，您也可以签入 /etc/apt/sources.list。示例命令中使用了预安装的 Vim 文本编辑器。有关更多信息，请参阅 Vim 文档。

```
$ vim buster-backports.list
```

4. 找到任何包含以下文本的行：http://deb.debian.org/debian buster-backports main。

   将 deb.debian.org替换为 archive.debian.org。例如，http://**deb**.debian.org/debian buster-backports main contrib non-free 将为 http://**archive**.debian.org/debian buster-backports main contrib non-free。

5. 保存并关闭文件。
6. 重新启动 WordPress 安装程序。

存储库 http://ppa.launchpad。 net/certbot/certbot/ubuntulunar Release 没有发布文件

Reason

您的实例上有一个已弃用的 Certbot个人程序包存档（PPA）存储库，并且其无法更新。

修复

使用以下过程从实例中手动移除已弃用的 PPA 存储库。

过程

1. 使用基于 Lightsail 浏览器的 SSH 客户端或使用连接到您的实例。AWS CloudShell
2. 导航到 /etc/apt/sources.list.d/ 目录。

```
$ cd /etc/apt/sources.list.d/
```

3. 使用所选的文本编辑器打开 certbot-ubuntu-certbot-**version**.list 文件。示例命令中使用了预安装的 Vim 文本编辑器。有关更多信息，请参阅 Vim 文档。

   在命令中，将 **version** 替换为存储库不兼容的 Ubuntu 版本；这将与错误消息中显示的版本相同。例如，**lunar** 或 **mantic**。

```
$ vim certbot-ubuntu-certbot-version.list
```

4. 移除任何包含以下文本的行：`http://ppa.launchpad.net/certbot/certbot/ubuntu`。
5. 保存并关闭文件。
6. 重新启动 WordPress 安装程序。

在过去 168 小时内，已经为此组域颁发太多的证书（5）

Reason

在过去一周内，您的一个或多个域或子域已用于创建 5 个证书。有关更多信息，请参阅 Let's Encrypt 网站上的速率限制。

修复

等待一周（168 小时），然后重新启动该域的引导式工作流程。

失败的授权过多

Reason

请求中的一个或多个域或子域已超过每小时五次验证的限制。有关更多信息，请参阅 Let's Encrypt 网站上的速率限制。

修复

等待一小时，然后再次运行 WordPress 安装程序。在重新启动设置之前，请确认其他验证错误已得到修复。

解决 Lightsail 控制台中的 403（未经授权的）错误

如果你在尝试访问 Lightsail 主机时遇到 403 错误，请不要惊慌。请尝试以下步骤来解决问题：

- 如果您的 AWS 账户或 AWS Identity and Access Management (IAM) 用户是最近创建的，请等待几分钟，然后刷新浏览器。
- 如果自您上次登录以来已有一段时间，请刷新浏览器。如果系统提示你重新登录，请务必使用有权访问 Lightsail 的 IAM 用户。
- 如果您的 IAM 用户无权访问 Lightsail，请联系AWS 账户根用户或具有管理员权限的 IAM 用户请求访问 Lightsail。要了解更多信息，请参阅管理 IAM 用户对 Amazon Lightsail 的访问权限。
- 如果您在尝试上述步骤后继续收到 403 错误，请联系 AWS Support。在极少数情况下，对于 2011 年之前创建的 AWS 帐户，支持人员必须手动将您的帐户订阅 Lightsail。

解决 Lightsail 磁盘连接和使用问题

Lightsail 中的块存储磁盘可能会出现错误。本主题介绍了常见问题以及这些错误的解决方法。

常规磁盘错误

在下面选择与您的错误最相符的问题，然后访问这些链接以修复该问题。如果在列表中不包含您遇到的问题，请使用该页面底部的 Questions? 问题与意见？链接以提交反馈，或者与 Amazon Web Services Support 联系。

我无法删除磁盘，因为该磁盘仍连接到实例上。

先尝试将磁盘与您的实例断开连接，然后再尝试删除该磁盘。有关更多信息，请参阅断开连接并删除数据块存储磁盘。

实际错误消息：您无法执行此操作，因为磁盘仍连接到 Lightsail 实例：*YOUR_INSTANCE*

我的磁盘的状态为错误。

错误状态表示与您的 Lightsail 磁盘相关的底层硬件出现故障。您可以从最近的快照中恢复磁盘，否则与磁盘相关的数据将无法恢复。有关更多信息，请参阅根据快照创建数据块存储磁盘。

对于状态为错误的磁盘，您无需付费。

我无法分离磁盘，因为 Lightsail 实例仍在运行。

先尝试停止您的实例，然后再尝试断开连接该磁盘。有关更多信息，请参阅停止实例。

实际错误消息：您当前无法取消连接此磁盘。此磁盘的状态为：***DISK_STATE***

我无法指定超过 16 TB (16,384 GB) 的自定义磁盘大小。

尝试创建较小的磁盘。额外磁盘可能高达 16 TB。如果您的磁盘小于 16 TB，并且仍无法创建该磁盘，您可能遇到了列表中的下一个错误（大磁盘太多）。这是因为您的亚马逊云科技账户中的额外磁盘存储不能超过 20 TB。有关更多信息，请参阅数据块存储磁盘。

实际错误消息：块存储磁盘的大小必须在 8 - 16384 GB 之间。

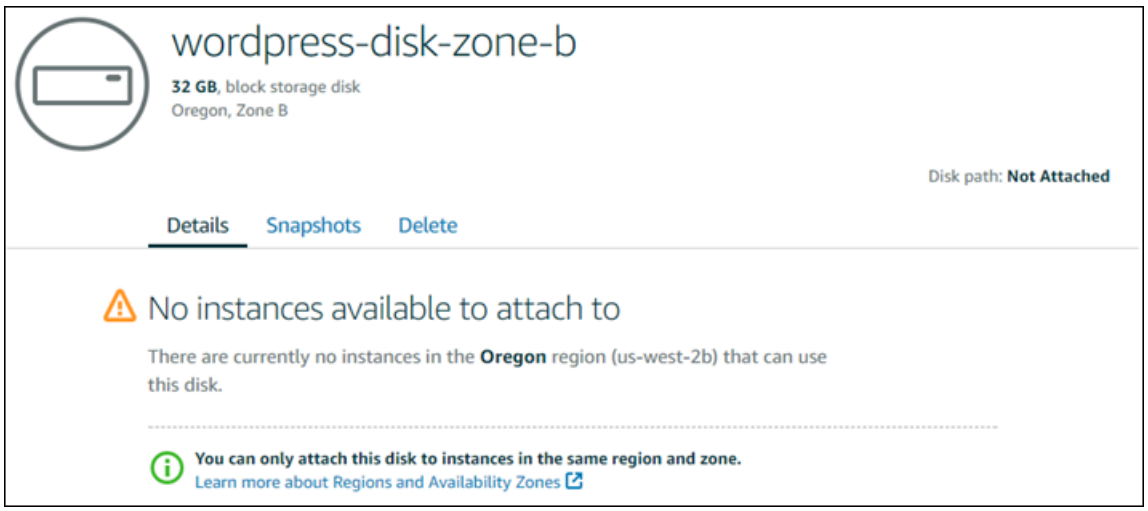
我无法再在 Lightsail 中创建任何磁盘了。

您可能已达到可创建的磁盘数配额。或者，您可能在亚马逊云科技账户中创建了太多的大磁盘（总磁盘存储大小不能超过 20 TB）。有关更多信息，请参阅数据块存储磁盘。

实际错误消息：您已达到此账户中所有磁盘的大小上限限制。或您已达到此账户中的磁盘限制。

我无法将磁盘连接到我的 Lightsail 实例

如果遇到以下错误，您需要在与打算将磁盘连接到的实例相同的亚马逊云科技区域和可用区中重新创建该磁盘。



实际错误消息：中目前没有任何实例可以使用***AWS Region***此磁盘。

解决基于 Lightsail 浏览器的 SSH 和 RDP 客户端的连接错误

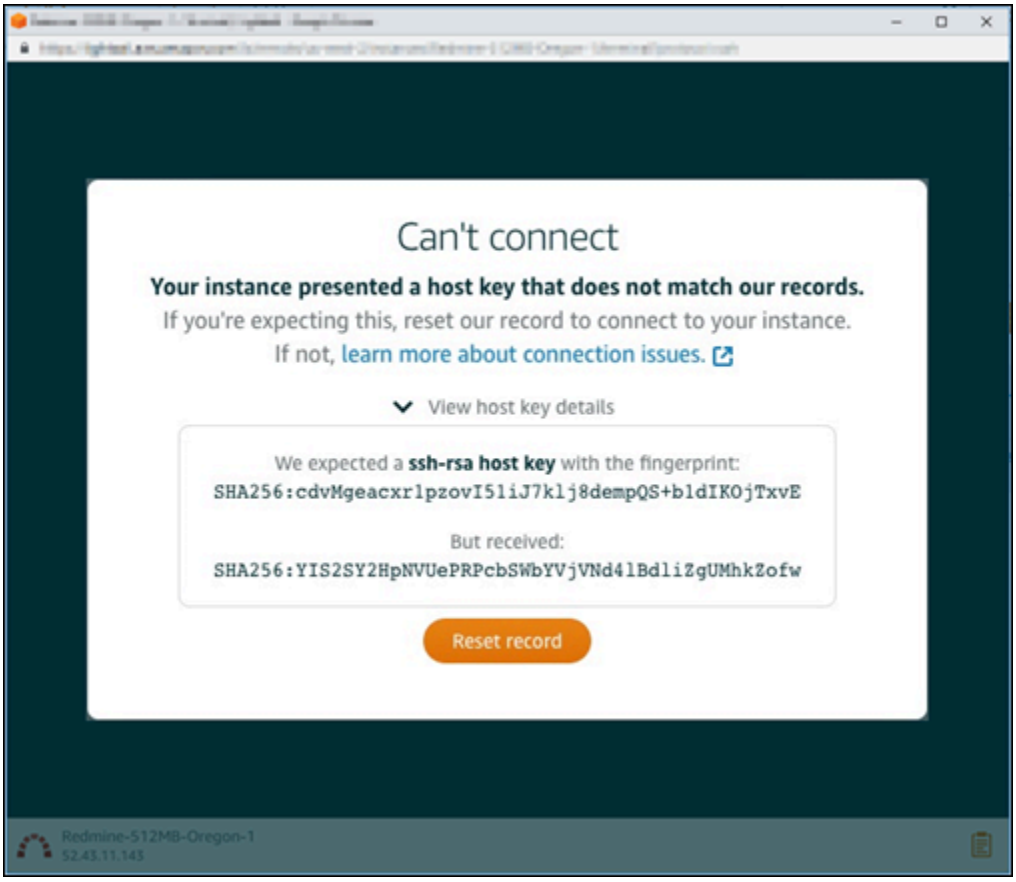
尝试使用 Amazon Lightsail 控制台中提供的基于浏览器的 SSH 或 RDP 客户端连接实例时，您可能会收到错误消息。在以下部分中讨论此错误的可能原因。

错误消息：Can’t connect (无法连接)

基于浏览器的 SSH 和 RDP 客户端在尝试连接到实例时使用主机密钥或证书验证对实例进行身份验证。如果实例提供的主机密钥或证书与 Lightsail 记录在案的主机密钥或证书不匹配，则会显示两条错误消息之一。将在此部分中显示并介绍这两条错误消息。

Can’t connect, reset record (无法连接，请重置记录)

如果主机密钥或证书不匹配，且 Lightsail 确定不匹配可能是由于最近的操作系统升级或您或其他用户故意更新主机密钥或证书所致，则会显示以下错误消息。在本例中，Lightsail 已确定主机密钥或证书不匹配不是由您的浏览器和实例之间的网络上的不良行为造成的。



如果您预料到不匹配，请选择 Reset record (重置记录)。此操作会删除 Lightsail 记录在案的主机密钥或证书，并允许基于浏览器的 SSH 或 RDP 会话连接到该实例。

您也可以使用以下 AWS Command Line Interface (AWS CLI) 命令删除 Lightsail 记录在案的主机密钥或证书。对于*InstanceName*，输入您要删除其已知主机密钥或证书的实例的名称。对于*Region*，请输入实例的 AWS 区域。

```
aws lightsail delete-known-host-keys --region Region --instance-name InstanceName
```

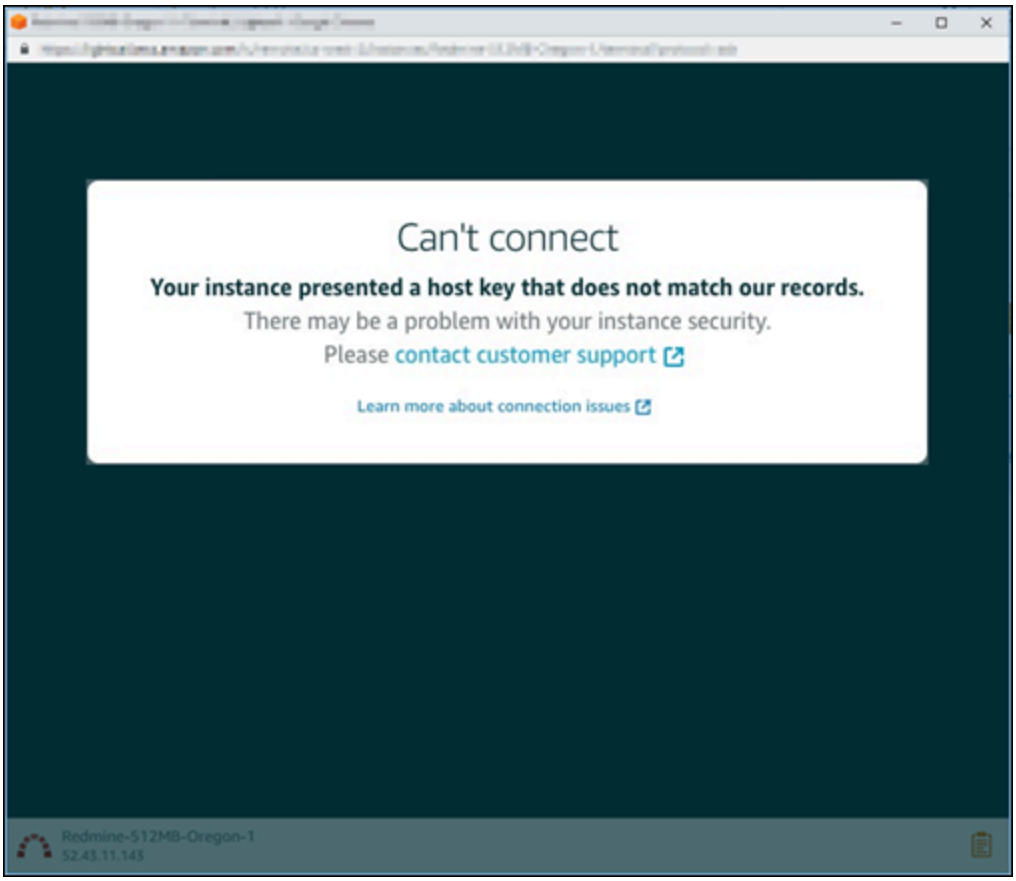
示例：

```
aws lightsail delete-known-host-keys --region us-west-2 --instance-
name WordPress-512MB-Oregon-1
```

> **Note**
>
> 有关的更多信息 AWS CLI，请参阅配置为与 Lightsail 配合使用。 AWS CLI

Can’t connect, contact customer support (无法连接，请联系客户支持)

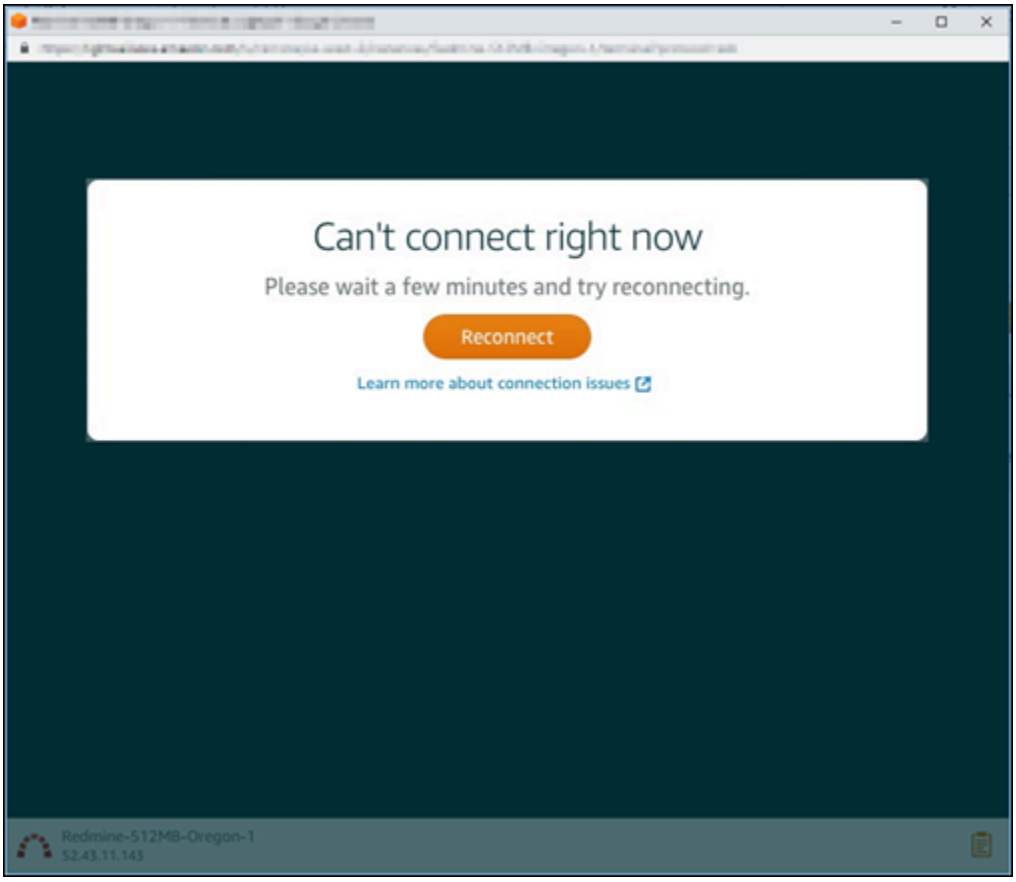
当主机密钥或证书不匹配且 Lightsail 确定存在值得进一步调查的可疑活动（例如 man-in-the-middle攻击）时，会显示以下错误消息。



此错误消息意味着您无法使用基于浏览器的 SSH 或 RDP 客户端连接到实例。请联系支持人员以获取帮助。

错误消息：Can’t connect right now (无法立即连接)

当您尝试连接到在创建或重启之后尚未启动的实例时，会显示以下错误消息。等待几分钟，然后选择 Reconnect (重新连接) 以重试。



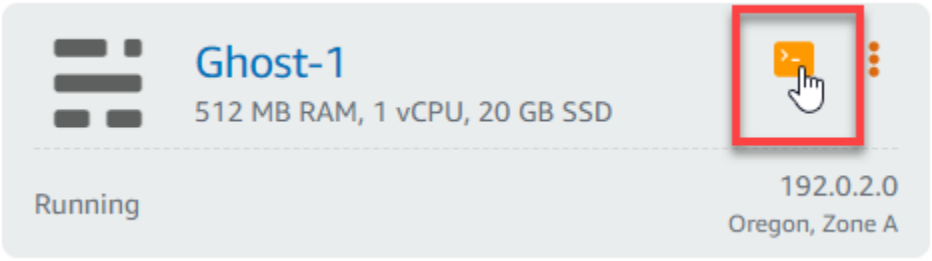
如果您仍然无法连接，请联系 Su AWS pp ort。

对 Lightsail 上的 Ghost 实例 503 服务不可用错误进行故障排除

在 Amazon Lightsail 中创建新的 Ghost 实例并尝试访问您的网站后，您可能会看到一条错误消息，指出该服务不可用 (503)。在某些情况下，创建实例后，实例上的 Ghost 服务不会自动启动。如果为实例选择 5 USD/月的包，就可能会发生这种情况。通过以下过程启动 Ghost 服务，即可解决“服务不可用”错误。

启动 Ghost 服务

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 为您的 Ghost 实例选择基于浏览器的 SSH 客户端图标。



4. 连接 SSH 客户端后，请输入以下命令以重新启动实例上的所有服务：

```
sudo /opt/bitnami/ctlscript.sh restart
```

您会看到类似于以下示例的结果：

```
bitnami@ip-172-26-11-214:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/apps/ghost/scripts/ctl.sh : ghost not running
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql  started at port 3306
- Ensuring user is not logged in as ghost user [skipped]
- Checking if logged in user is directory owner [skipped]
✔ Checking current folder permissions
✔ Validating config
✔ Checking memory availability
✔ Checking binary dependencies
✔ Starting Ghost: 127-0-0-1

------------------------------------------------------------------------

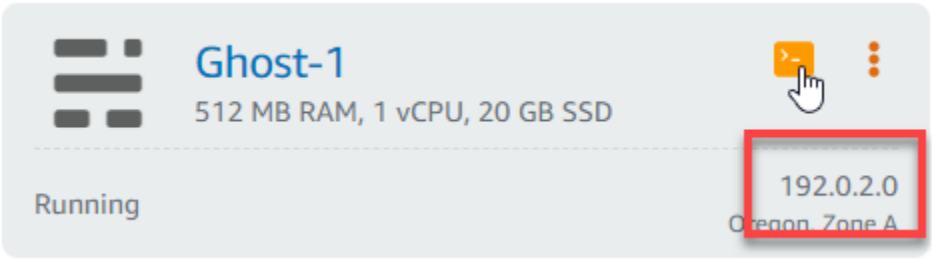
Your admin interface is located at:

    http://18.237.117.48:80/ghost/

/opt/bitnami/apps/ghost/scripts/ctl.sh : ghost started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
```

5. 浏览到实例的公有 IP 地址，确认您的 Ghost 网站已启动并正在运行。

在 Lightsail 控制台的 “实例” 部分中，您的实例的公有 IP 地址列在实例名称旁边。



当您浏览到新 Ghost 实例的公有 IP 时，您会看到默认的 Ghost 网站模板：



对 Lightsail 中的身份和访问管理 (IAM) Management 进行故障排除

使用以下信息来帮助您诊断和修复在使用 Lightsail 和 IAM 时可能遇到的常见问题。

我无权在 Lightsail 中执行任何操作

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当 `mateojackson` IAM 用户尝试访问 Lightsail 控制台但没有`lightsail:*`（完全访问权限）权限时，会出现以下示例错误。



在这种情况下，Mateo 要求管理员更新其策略，允许他使用`lightsail:*`（完全访问权限）权限访问 Lightsail 控制台。

我无权执行 iam：PassRole

如果您收到错误消息，说您无权执行该`iam:PassRole`操作，则必须更新您的政策，以允许您将角色传递给 Amazon Lightsail。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在 Amazon Lightsail 中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想要查看我的访问密钥

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 `AKIAIOSFODNN7EXAMPLE`）和秘密访问密钥（例如 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

> **Important**
>
> 请不要向第三方提供访问密钥，即便是为了帮助找到您的规范用户 ID 也不行。通过这样做，您可以授予他人永久访问您的权限 AWS 账户。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果丢失了您的秘密访问密钥，您必须为 IAM 用户添加新的访问密钥。您最多可拥有两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅 IAM 用户指南中的管理访问密钥。

我是一名管理员，想允许其他人访问 Lightsail

要允许其他人访问 Amazon Lightsail，您必须向需要访问的人员或应用程序授予权限。如果使用 AWS IAM Identity Center 管理人员和应用程序，则可以向用户或组分配权限集来定义其访问权限级别。权限集会自动创建 IAM 策略并将其分配给与人员或应用程序关联的 IAM 角色。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。

如果未使用 IAM Identity Center，则必须为需要访问的人员或应用程序创建 IAM 实体（用户或角色）。然后，您必须向该实体附加一项策略，授予他们在 Amazon Lightsail 中的正确权限。授予权限

后，向用户或应用程序开发人员提供凭证。他们将使用这些凭证访问 AWS。要了解有关创建 IAM 用户、组、策略和权限的更多信息，请参阅《IAM 用户指南》中的 IAM 身份和 IAM 中的策略和权限。

我想允许 AWS 账户之外的人访问我的 Lightsail 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon Lightsail 是否支持这些功能，请参阅。亚马逊 Lightsail 如何与 IAM 合作
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

验证 Lig IPv6 htsail 实例的可访问性

您可以使用 ping IPv6 工具验证本地计算机与 Amazon Lightsail 实例的连接。ping 是一种网络诊断实用程序，用于排查两台或多台联网设备之间的连接问题。如果 ping 成功，您应该能够通过连接您的实例。 IPv6如果网络设置或设备未配置为允许 IPv6，ping 命令将失败。有关更多信息，请参阅 IPv6-仅考虑因素

内容

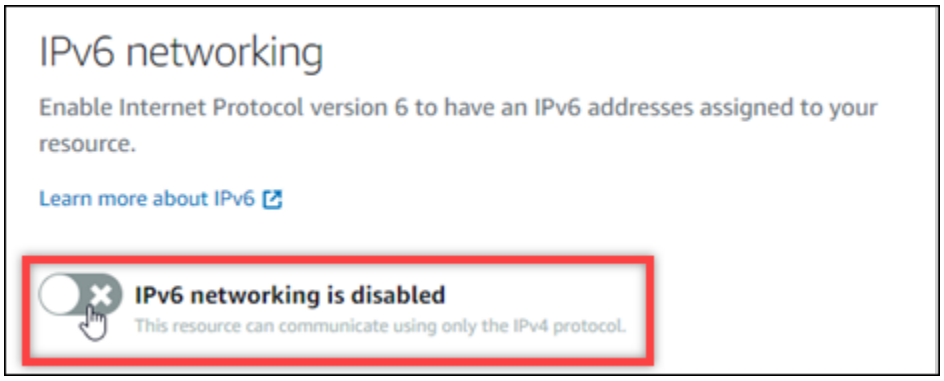
- IPv6 为双栈实例启用
- 配置实例的防火墙
- 测试您实例的可达性

IPv6 为双栈实例启用

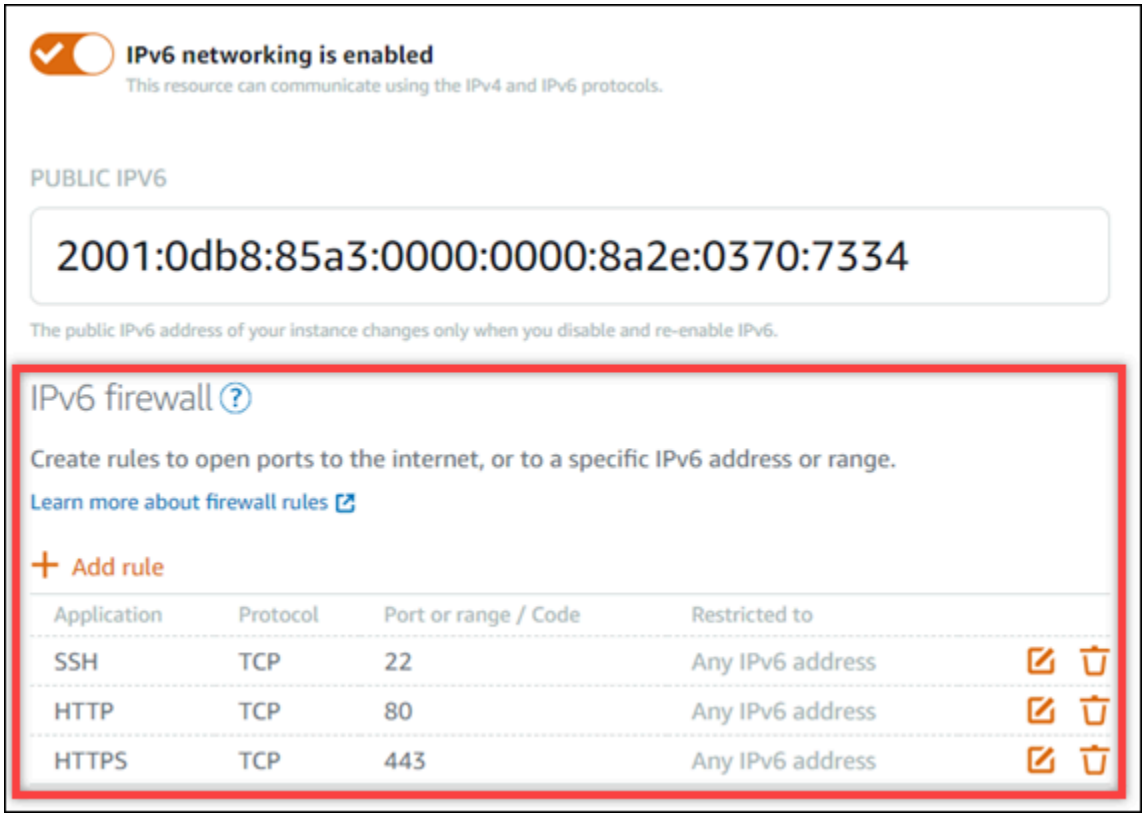
在开始测试之前，请 IPv6 为双栈实例启用。 IPv6 对于 IPv6仅限实例，始终处于开启状态。

如果双堆栈实例未启用，请完成以下步骤以在双堆栈实例 IPv6 上启用。

1. 登录 Lightsail 控制台。
2. 选择要为其启用的实例的名称 IPv6。确保您的实例正在运行。
3. 选择实例管理页面上的联网选项卡。
4. IPv6 在页面的 “IPv6 网络” 部分启用。



启用后 IPv6，将为您的实例分配一个公有 IPv6 地址，并且 IPv6 防火墙变为可用。



5. 记下页面顶部的实例的公用 IPv6地址 IPv4和公有地址。您将在以下部分用到这些地址。

配置实例的防火墙

Lightsail 控制台中的防火墙充当虚拟防火墙。这意味着它控制允许哪些流量通过其公有 IP 地址连接到您的实例。您在 Lightsail 中创建的每个双栈实例都有一个单独的地址防火墙，另一个 IPv4 IPv6 用于地址的防火墙。每个防火墙均包含一组规则来过滤进入实例的流量。两个防火墙相互独立，必须为和分别配置防火墙规则。 IPv4 IPv6 IPv6只有实例套餐的实例没有您可以配置的 IPv4 防火墙。

完成以下步骤，为 Internet 控制消息协议（ICMP）流量配置实例的防火墙。ping 实用程序使用 ICMP 协议与实例进行通信。有关更多信息，请参阅 在 Lightsail 中使用防火墙控制实例流量。

> **Important**
>
> Windows 和 Linux 包含操作系统（OS）级别的防火墙，这些防火墙可以阻止 ping 命令。在继续操作 IPv6 之前，请验证实例的操作系统防火墙是否可以接受 ICMP 流量。 IPv4 有关更多信息，请参阅以下文档：
>
> - 使用 RDP 连接到你的 Lightsail Windows 实例
> - 在 Lightsail 上连接到 Linux 或 Unix 实例

1. 登录 Lightsail 控制台。
2. 选择要为其配置防火墙规则的实例的名称。
3. 从实例管理页面选择联网选项卡，然后根据要使用的防火墙类型完成相应部分中的其余步骤。对于 IPv4，请完成 “IPv4 防火墙” 部分中的步骤。对于 IPv6，请完成 “IPv6 防火墙” 部分中的步骤。

   a. 从应用程序下拉菜单中选择 Ping（ICMP）。

   b. 选中限制到 IP 地址复选框以允许从您的本地源 IP 地址或范围进行连接，然后输入您的源 IP 地址。（可选）您可以取消选中该复选框以允许来自任何 IP 地址的连接。我们建议您仅在测试环境中使用此选项。

   c. 选择创建，将新规则应用于您的实例。

测试您实例的可达性

完成以下步骤以测试从您的本地计算机 IPv4 或网络到 Lig IPv6 htsail 实例的可访问性。您需要在中注明的实例的公共 IPv6 地址 IPv4和地址Step 5。

从 Linux、Unix 或 macOS 设备

1. 在本地设备上打开终端窗口。
2. 输入以下命令之一来 ping 你的 Lightsail 实例。*IP address*将命令中的示例替换为您的实例的公共 IPv6 地址 IPv4 或地址。

   要测试一遍 IPv4

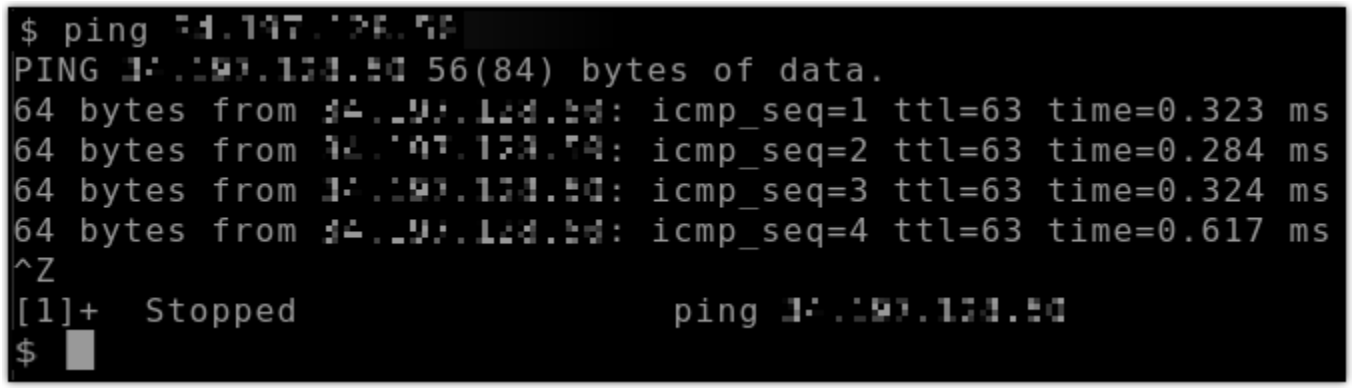
   ```
   ping 192.0.2.0
   ```

   要测试一遍 IPv6

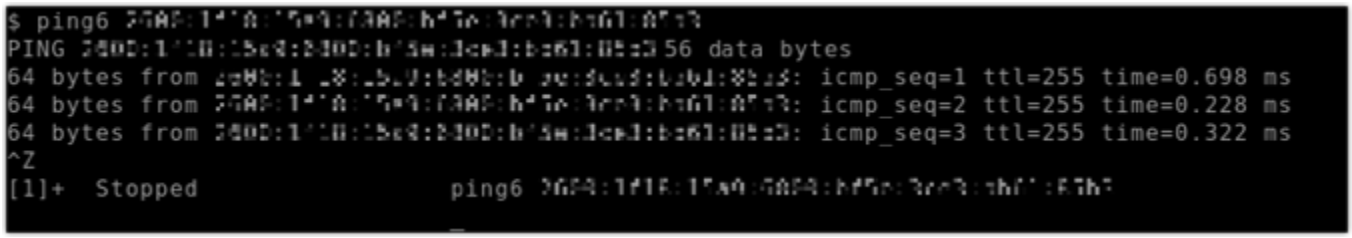
   ```
   ping6 2001:db8::
   ```

3. 命令返回几条回复后，使用设备的键盘输入 `ctrl+z` 以停止该命令。

如果成功，ping 命令会从您的实例的地 IPv4 址返回成功回复。结果应该类似以下示例。



如果成功，ping6 命令会返回来自您的实例 IPv6 地址的成功回复。结果应该类似以下示例。



如果无法访问您的实例，两个命令都会返回请求超时。

从 Windows 设备

1. 打开命令提示符。

2. 输入以下命令之一来 ping 你的 Lightsail 实例。*IP address*将命令中的示例替换为您的实例的公共 IPv6 地址 IPv4 或地址。

   要测试一遍 IPv4

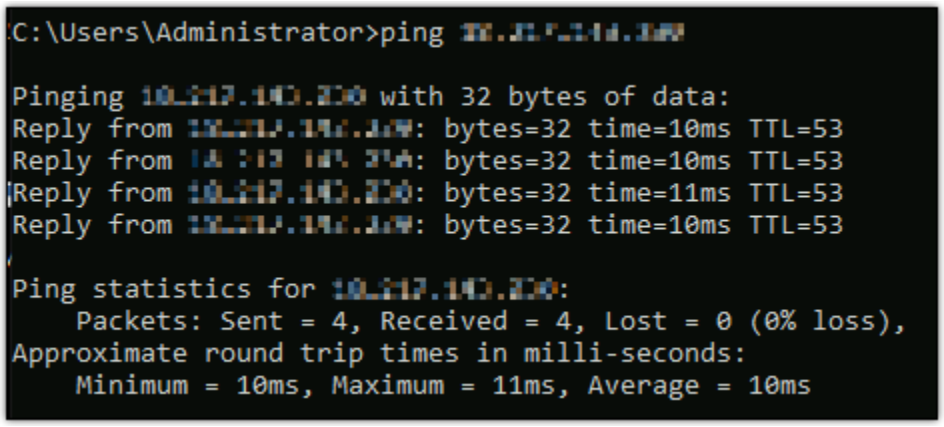
   ```
   ping 192.0.2.0
   ```

   要测试一遍 IPv6

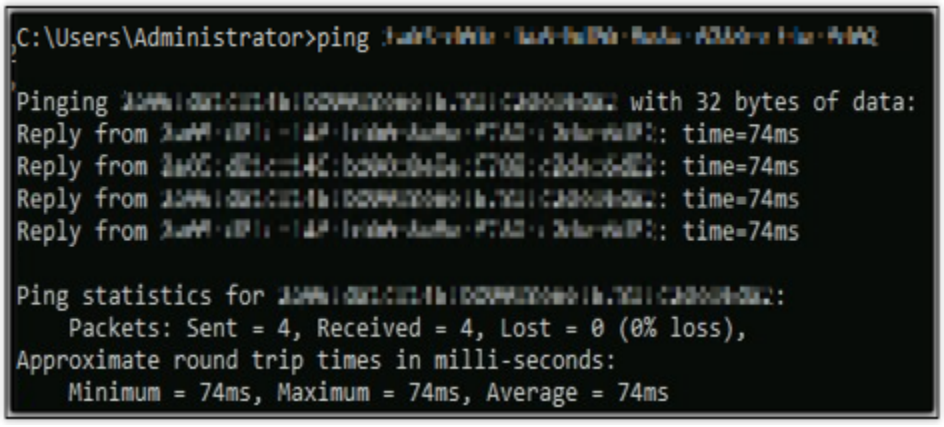
   ```
   ping 2001:db8::
   ```

3. 命令返回几条回复后，使用设备的键盘输入 `ctrl+z` 以停止该命令。

如果成功，ping 命令会从您的实例的地 IPv4 址返回成功回复。结果应该类似以下示例。



如果成功，ping 命令会从您的实例的地 IPv6 址返回成功回复。结果应该类似以下示例。



如果无法访问您的实例，两个命令都会返回请求超时。

解决 Lightsail 中实例容量不足的错误

在尝试启动新实例或重新启动已停止的实例时，您可能收到容量不足错误。这意味着 AWS 它目前没有足够的可用实例容量来满足您的请求。下面是实例容量不足错误的示例：

InsufficientInstanceCapacity：容量不足，无法满足您的实例请求。减少请求中的实例数量，或等待更多容量可用。您也可以尝试通过选择较小的 Lightsail 套餐来启动实例（您可以在稍后阶段调整其大小）。”

在本指南中，您将了解在出现实例容量不足错误时可以采取的措施。

内容

- 启动新实例时容量不足
- 启动已停止的实例时容量不足
- 相关信息

启动新实例时容量不足

如果您在启动新实例时出现实例容量不足错误，请使用以下选项。可以按顺序完成每个选项，也可以选择适合您的选项。

1. 等待几分钟，然后再次提交您的请求。实例容量可能经常转移。如果您在等待几分钟后仍无法创建实例，请继续使用选项 2。
2. 在创建实例时选择其他可用区（AZ）。每个可用区 AWS 区域 包含三个或更多 AZs，并且每个可用区保持不同的实例容量。通过选择其他可用区，您可以利用其当前的实例容量。如果您无法在其他可用区 AWS 区域 或可用区中创建实例，请继续执行选项 3。
3. 减少请求的实例数。如果您同时创建多个实例，请减少实例数量并再次提交请求。如果减少实例数量不能解决问题，请继续使用选项 4。
4. 创建实例时选择不同的实例计划。如果您无法在不同的可用区或区域创建实例，请选择其他实例计划。您可以在后期阶段调整实例的大小。有关调整实例大小的更多信息，请参阅从快照创建实例。

启动已停止的实例时容量不足

如果您在启动先前已停止的现有实例时出现实例容量不足错误，请使用以下选项。

1. 等待几分钟，然后再次提交您的请求。实例容量可能经常转移。如果您在等待几分钟后仍无法创建实例，请继续使用选项 2。
2. 从快照创建新实例 拍摄已停止实例的快照。然后，使用快照在不同于原始实例的可用区中创建新实例。例如，如果您的实例当前位于 us-east-2a（区域 A），则在创建新实例时选择 us-east-2c（区域 C）。有关更多信息，请参阅从快照创建实例。
3. 从快照创建新实例时，您也可以选择不同的实例计划。此操作是可选的。

> **Important**
>
> 在新实例运行之后，请确认您有权访问新实例且一切正常。例如，如果您的实例正在运行应用程序，请确保该应用程序按预期运行。如果一切正常，您就可以删除之前的实例。

相关信息

常见问题

Lightsail 中的韧性

解决 Lightsail 负载均衡器问题

您的 Lightsail 负载均衡器可能会遇到错误。本主题介绍了常见问题以及这些错误的解决方法。

常规负载均衡器错误

在下面选择与您的错误最相符的问题，然后访问这些链接以修复该问题。如果在列表中不包含您遇到的问题，请使用该页面底部的 Questions? Comments?（问题与意见）链接位于本页底部用以提交反馈，或者与亚马逊云科技客户支持联系。

我无法创建证书。

> 您可以在一个 AWS 账户中创建的证书数量有配额。有关更多信息，请参阅《亚马逊云科技 Certificate Manager 用户指南》中的配额。同样的配额也适用于负载均衡器的 Lightsail 证书。
>
> 实际错误消息：抱歉，您已为账户请求的证书过多。

我无法将任何其他实例连接到我的负载均衡器。

> 只要不超过每个账户总计 20 个 Lightsail 实例的配额，您就可以将任意数量的 Lightsail 实例附加到您的负载均衡器。 AWS

实际错误消息：抱歉，您已达到您可连接到此负载均衡器的实例数上限。

我无法将特定实例连接到我的负载均衡器。

首先，请检查以确保您的 Lightsail 实例正在运行。如果该实例已停止，您可以从实例管理页面中启动该实例。Lightsail 实例必须处于运行状态才能成功连接到负载均衡器。

可能是将相同实例连接到太多的负载均衡器。

实际错误消息：抱歉，您已达到可在负载均衡器中注册同一个实例的次数上限。

Lightsail 找不到我想要连接到我的负载均衡器的实例

您正在尝试连接的实例可能不再存在，或者没有位于与目标组相同的 VPC 中。

实际错误消息：抱歉，您指定的实例不存在、未与目标组位于相同的 VPC 中或它的实例类型不受支持。

对 Lightsail 中的通知传递进行故障排除

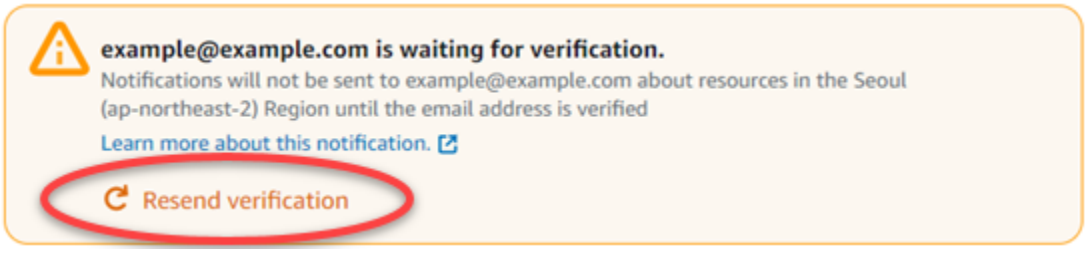
如果您在预期收到通知时没有收到通知，请检查确认您的通知联系人是否正确配置。要了解有关通知的更多信息，请参阅通知。

以下列表描述了您可能遇到的常见通知联系问题、导致这些问题的原因以及如何解决这些问题。如果在列表中不包含您遇到的问题，请使用该页面底部的 Questions? 问题与意见？链接以提交反馈，或者与 AWS 支持 中心联系。

我添加了我的电子邮件地址作为通知联系人，但我没有收到电子邮件通知

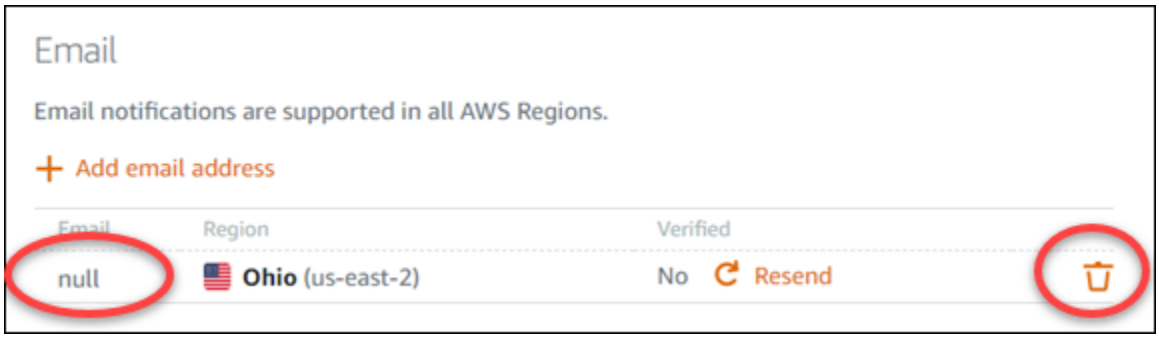
当您在 Lightsail 中添加电子邮件地址作为通知联系人时，系统会向该地址发送验证请求。验证请求电子邮件中包含一个链接，收件人必须单击该链接才能确认他们想要接收 Lightsail 通知。在验证后才会将通知发送到电子邮件地址。验证来自亚马逊云科技 通知 < no-reply@sns.amazonaws.com >，其主题是亚马逊云科技 Notification - Subscription Confirmation。SMS 消息收发不需要验证。

如果验证请求不在收件箱文件夹中，请检查邮箱的垃圾邮件和垃圾邮件文件夹。如果验证请求丢失或被删除，请在 Lightsail 控制台中显示的通知横幅和 “帐户” 页面中选择 “重新发送验证”。



我看到 null 列为我的电子邮件通知联系人。

电子邮件地址必须在添加后的 24 小时内进行验证。如果您未能在 24 小时内验证电子邮件，则该电子邮件的状态将自动变为`invalid`并从 Lightsail 中删除。这就是为什么您可能会在一个或多个电子邮件通知联系人中看到 null 值。



要修复这一问题，请删除 null 电子邮件通知联系人，然后重新添加正确的电子邮件地址。请务必在将电子邮件地址添加到 Lightsail 后立即对其进行验证。有关更多信息，请参阅通知。

我没有收到 SMS 文本消息通知，或者我最近没有再收到这些通知

您可能已选择退出而不再接收 SMS 文本消息通知。您可以通过对 SMS 文本消息通知回复 ARRET（法语）、CANCEL、END、OPT-OUT、OPTOUT、QUIT、REMOVE、STOP、TD 或 UNSUBSCRIBE 来选择退出。如果您选择停用手机号码，则必须等待 30 天才能在 Lightsail 中再次将该手机号码添加为通知联系人。

对 Lightsail 中的 SSL/TLS 证书进行故障排除

您的 Lightsail 负载均衡器可能会遇到错误。本主题介绍了常见问题以及这些错误的解决方法。

在下面选择与您的错误最相符的问题，然后访问这些链接以修复该问题。如果在列表中不包含您遇到的问题，请使用该页面底部的 Questions? Comments?（问题与意见）链接位于本页底部用以提交反馈，或者与亚马逊云科技客户支持联系。

我无法创建证书。

您可以在一个 AWS 账户中创建的证书数量有配额。有关更多信息，请参阅《亚马逊云科技 Certificate Manager 用户指南》中的配额。同样的配额也适用于负载均衡器的 Lightsail 证书。

实际错误消息： 抱歉，您已为账户请求的证书过多。

我的证书请求失败。

如果您的证书请求失败，您可以在负载均衡器管理页面的入站流量选项卡上重试。

如果仍找不到错误原因，请与亚马逊云科技客户支持联系。

我的域显示为无效。

如果在验证您是否可以控制域时遇到问题，请检查您是否有权访问 DNS 管理。如果可以访问并按照这些说明进行操作，但仍无法进行验证，请与亚马逊云科技客户支持联系。

通过教程探索 Lightsail 的功能

本节涵盖与亚马逊 Lightsail 相关的以下主题：

主题

- 使用 Lightsail 蓝图快速部署应用程序
- 在 Lightsail 上使用 Bitnami 应用程序和堆栈
- 配置和管理 Lights WordPress ail 实例
- 在 Lightsai WordPress l 上使用 Multisite 管理多个站点
- 使用 Let's Encrypt 为 Lightsail 资源启用加密通信
- 为 Lightsail 实例配置 IPv6 网络
- 为 Lightsai AWS CLI l 操作设置和配置
- 使用管理 Lightsail 资源 AWS CloudShell
- 在 Lightsail LAMP 实例上部署 PHP 应用程序
- 在 Lightsail 上启动和配置 Windows Server 2016 实例
- 使用监控 Lightsail API 活动 AWS CloudTrail
- 创建 HAR 文件来解决 Lightsail 问题
- 在 Lightsail 上使用 Prometheus 监控系统资源和应用程序
- 使用 scp 在 Lightsail 上的 Linux 实例之间传输文件
- 通过 VPC 对等互连将 Lightsail 与其他 AWS 服务集成
- 使用创建 Lightsail 资源 AWS CloudFormation
- 浏览用于应用程序部署的 Lightsail 资源

点击每个类别中提供的链接，获取有关使用 Lightsail 各个方面的 step-by-step指南、最佳实践和其他信息。

每个主题都涵盖部署应用程序、配置网络、监控和日志记录、与其他 AWS 服务集成等信息。通过浏览本节，您可以学习如何有效利用Lightsail，利用其与其他 AWS 服务的集成，并访问大量教程和资源来增强您的云计算体验。

使用 Lightsail 蓝图快速部署应用程序

使用以下快速入门指南开始使用 Lightsail 蓝图。在 Lightsail 中，蓝图是预先打包了操作系统和应用程序的虚拟映像。应用程序包括 M WordPress ult WordPress isite、cPanel 和 WHM、、Drupal、Ghos PrestaShop t、Joomla！ 、Magento、Redmine、LAMP、Nginx (LEMP) 和 Node.js

主题

- 在 Lightsail 上启动并设置一个 AlmaLinux 实例
- 在 Lightsail 上使用 cPanel 和 WHM 托管网站、电子邮件和服务
- 在 Lightsail 上设置和自定义你的 Drupal 网站
- 在 Lightsail 上部署 Ghost 网站
- 在 Lightsail 上设置和配置 GitLab CE 实例
- 开始使用 Joomla 吧！ 在 Lightsail 上
- 在 Lightsail 上设置 LAMP 堆栈
- 在 Lightsail 上设置和配置 Magento
- 在 Lightsail 上部署和管理 Nginx 网络服务器
- 开始在 Lightsail 上使用 Node.js
- 在 Lightsail 上部署 Plesk 托管堆栈
- 在 Lightsa PrestaShop il 上建立一个网站
- 在 Lightsail 上配置和保护 Redmine 实例
- 在 Lightsa WordPress il 上启动和配置
- 在 Lightsail 上设置 WordPress多站点

在 Lightsail 上启动并设置一个 AlmaLinux 实例

本快速入门指南提供了在 Amazon Lightsail 平台上创建和配置 AlmaLinux 实例的 step-by-step说明。本主题涵盖了关键步骤，包括选择您的实例位置和计划、设置网络和安全，以及从 Cen AlmaLinux tOS 过渡到。按照这些步骤操作，您可以在 Lightsail 上快速启动并运行您的 AlmaLinux 实例。

主题

- 先决条件
- 在 Lightsai AlmaLinux l 中创建一个实例

- （可选）其他设置
- 将数据从 CentOS 迁移到 Lightsail AlmaLinux 上

先决条件

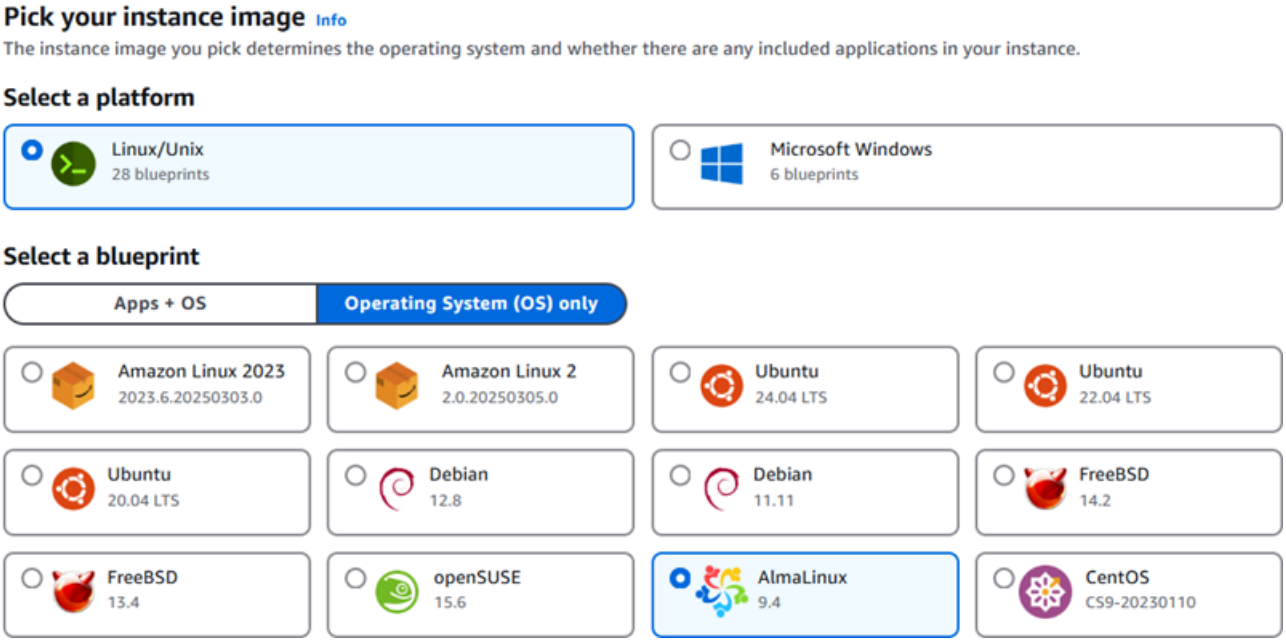
- 如果您是新 AWS 客户，请在开始使用 Amazon Lightsail 之前完成设置前提条件。有关更多信息，请参阅 为 Lightsail 设置 AWS 账户 和管理用户。
- 阅读 AlmaLinuxWiki 网站上的 AlmaLinux 文档。

在 Lightsai AlmaLinux l 中创建一个实例

完成以下过程，使用 Lightsail 控制台创建 AlmaLinux 实例。

1. 登录 Lightsail 控制台。
2. 在主页上，选择 Create instance（创建实例）。
3. 为您的实例选择一个位置（ AWS 区域 和可用区）。选择离您的实际位置最近的，以减少延迟。AWS 区域

   选择更改可用区以在另一位置创建实例。
4. 选择 Linux 平台。
5. 选择 “仅限操作系统 (OS)”，然后选择AlmaLinux蓝图。



6. （可选）您可以：

a. 通过选择添加启动脚本，添加将在您的实例首次启动时于其上运行的 shell。有关更多信息，请参阅 在 Lightsail 中使用启动脚本配置 Linux/Unix 实例。

b. 要更改您的实例的 SSH 密钥对，请从 SS H 密钥下方的下拉列表中选择一个密钥。有关更多信息，请参阅 为 Lightsail 设置 SSH 密钥。

c. 通过选择启用自动快照，为您的实例和附加的磁盘启用自动快照。有关更多信息，请参阅 为 Lightsail 实例和磁盘配置自动快照。

7. 选择实例计划。您可以选择您的实例是使用双堆栈（IPv4 和 IPv6）还是 IPv6仅使用双堆栈（和）网络。 AlmaLinux 蓝图支持双栈和 IPv6仅限双栈捆绑包。要了解有关 IPv6仅限网络的更多信息，请参阅为 IPv6 Lightsail 实例配置仅限网络连接。



8. 输入实例的名称。

资源名称：

- 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
- 必须包含 2 到 255 个字符。
- 必须以字母数字字符或数字作为开头和结尾。
- 可以包括字母数字字符、数字、句点、连字符和下划线。



9. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

   a. 对于密钥，输入标签密钥。

   b. （可选）在“值”中，输入标签值。

10. 选择创建实例。

几分钟之内，你的 Lightsail 实例就准备好了，你可以连接到它了。

（可选）其他设置

在您的 AlmaLinux 实例在 Lightsail 上启动并运行后，您应该采取以下几个步骤来开始使用：

- 将静态 IP 地址附加到实例 – 附加到实例的默认动态公有 IP 地址会在您每次停止和启动实例时发生变化。创建一个静态 IP 地址并将其附加到您的实例，以防止公有 IP 地址发生变化。稍后，当您对实例使用自己的域名时，就无需在每次停止和启动该实例时更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的“联网”选项卡下，选择创建静态 IP，然后按照页面上的说明操作。有关更多信息，请参阅 创建静态 IP 并将其附加到你的 Lightsail 实例。

- 在 Light@@ sail 中注册域名在 Lightsail 中注册并管理域名。Lightsail 使用 Amazon Route 53（一项高度可用且可扩展的域名系统 (DNS) 网络服务）为您注册域名。注册域名后，您可以将其分配给您的 Lightsail 资源或管理其的 DNS 记录。有关更多信息，请参阅 在 Lightsail 中为您的网站注册和管理域名。
- 将域名映射到实例 – 要将域名（如 `example.com`）映射到实例，您需要向域的域名系统（DNS）添加记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

  在 Lightsail 控制台主页的 “域名和 DNS” 部分，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。有关更多信息，请参阅 创建 DNS 区域来管理 Lightsail 实例的域名记录。
- 创建实例的快照 – 快照是系统磁盘和实例初始配置的副本。快照包含内存、CPU、磁盘大小和数据传输速率等信息。您可以将快照用作新实例的基准或用于数据备份。

  在实例管理页面的 Snapshot (快照) 选项卡下，输入快照名称，然后选择 Create snapshot (创建快照)。有关更多信息，请参阅 使用快照备份 Linux/Unix Lightsail 实例。

要学习如何从 CentOS 迁移到 AlmaLinux，请继续阅读下一个主题：。将数据从 CentOS 迁移到 Lightsail AlmaLinux 上

将数据从 CentOS 迁移到 Lightsail AlmaLinux 上

从 CentOS 迁移到 AlmaLinux 是一个简单的过程，通过这个过程，你可以将数据从 Lightsail 中的一个实例移动到另一个实例。本主题概述您可用于迁移数据的两个选项。

有关更多信息，请参阅 AlmaLinux Wiki 网站上的 AlmaLinux 文档。

目录

- 先决条件
- （可选）使用安全复制（scp）在实例之间传输文件
- （可选）将块存储磁盘从 CentOS 实例移至实例 AlmaLinux

先决条件

- 如果你还没有，请创建一个 AlmaLinux Lightsail 实例。有关更多信息，请参阅 在 Lightsail 上启动并设置一个 AlmaLinux 实例。
- 创建您计划移至 AlmaLinux 实例的磁盘的快照。有关更多信息，请参阅 创建 Lightsail 块存储磁盘快照以进行备份或基准。

（可选）使用安全复制（scp）在实例之间传输文件

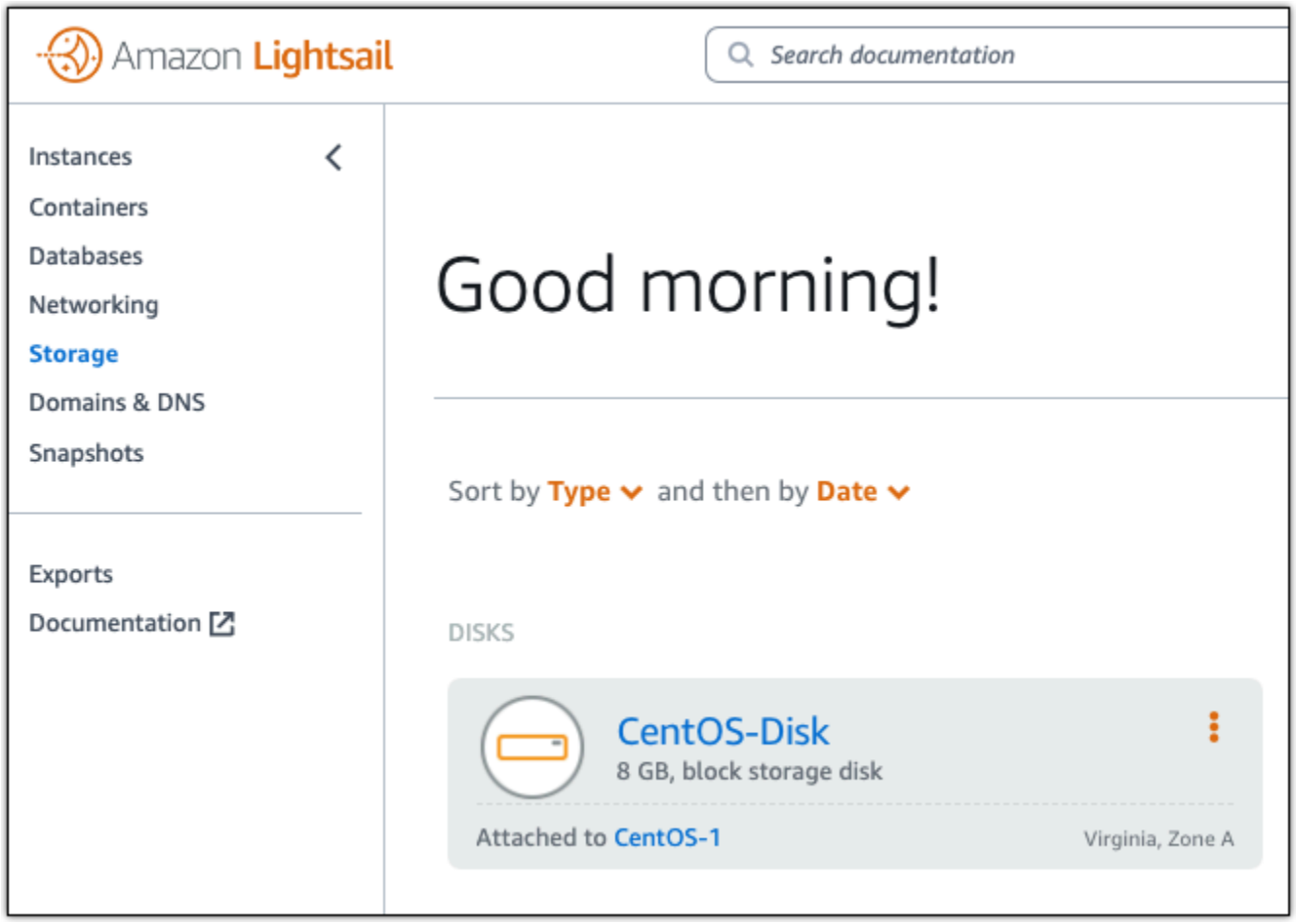
您可以在 Linux 中使用安全复制命令将文件从 CentOS AlmaLinux 实例安全地传输到新实例。有关更多信息，请参阅 使用 scp 在 Lightsail 上的 Linux 实例之间传输文件。

（可选）将块存储磁盘从 CentOS 实例移至实例 AlmaLinux

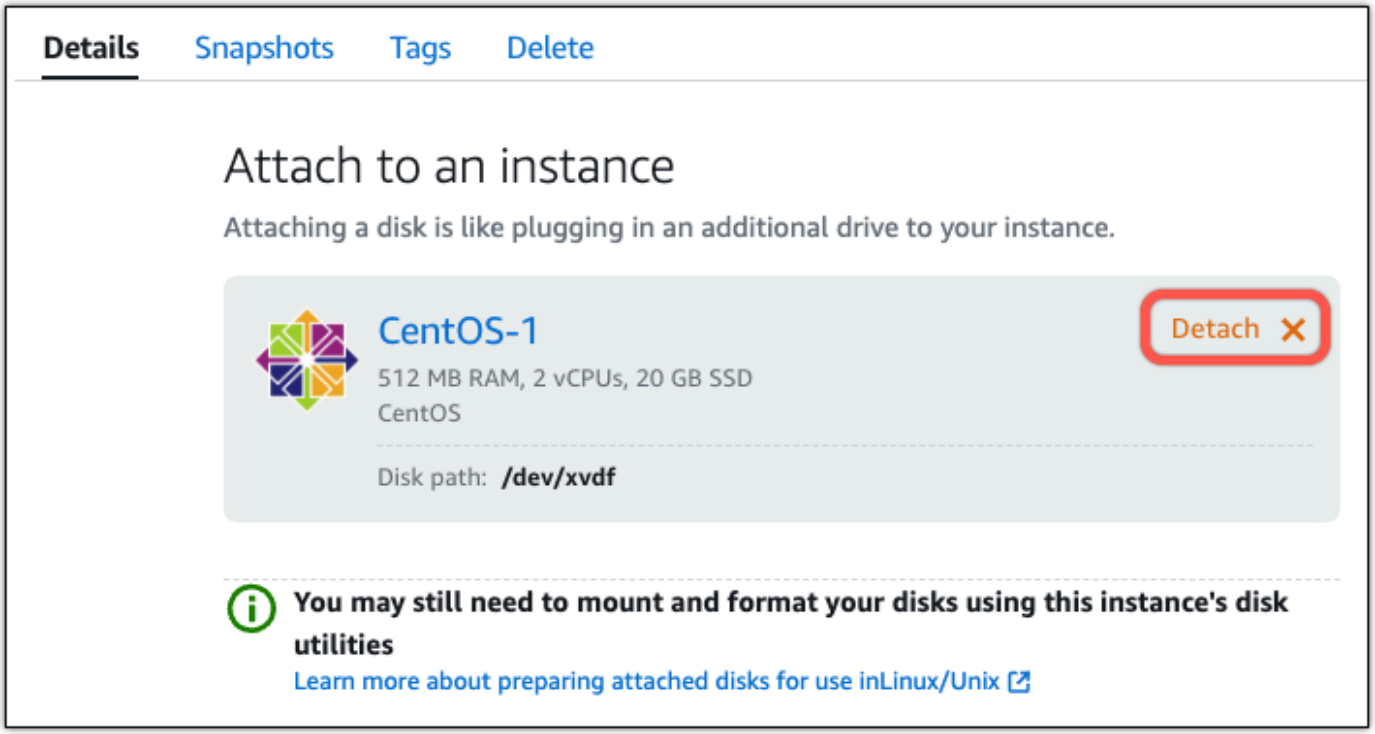
使用以下步骤将辅助块存储磁盘从 CentOS 实例捆绑包移至捆绑包。 AlmaLinux 您无法分离实例的启动卷磁盘，即包含操作系统的磁盘。将磁盘挂载到您的 AlmaLinux 实例后，您需要连接到该实例并装载该磁盘。有关更多信息，请参阅 使用 Lightsail 块存储磁盘扩展存储空间和性能。

如果您的 CentOS 实例正在运行，您需要先停止该实例，然后才能分离该磁盘。有关更多信息，请参阅停止运行的实例。

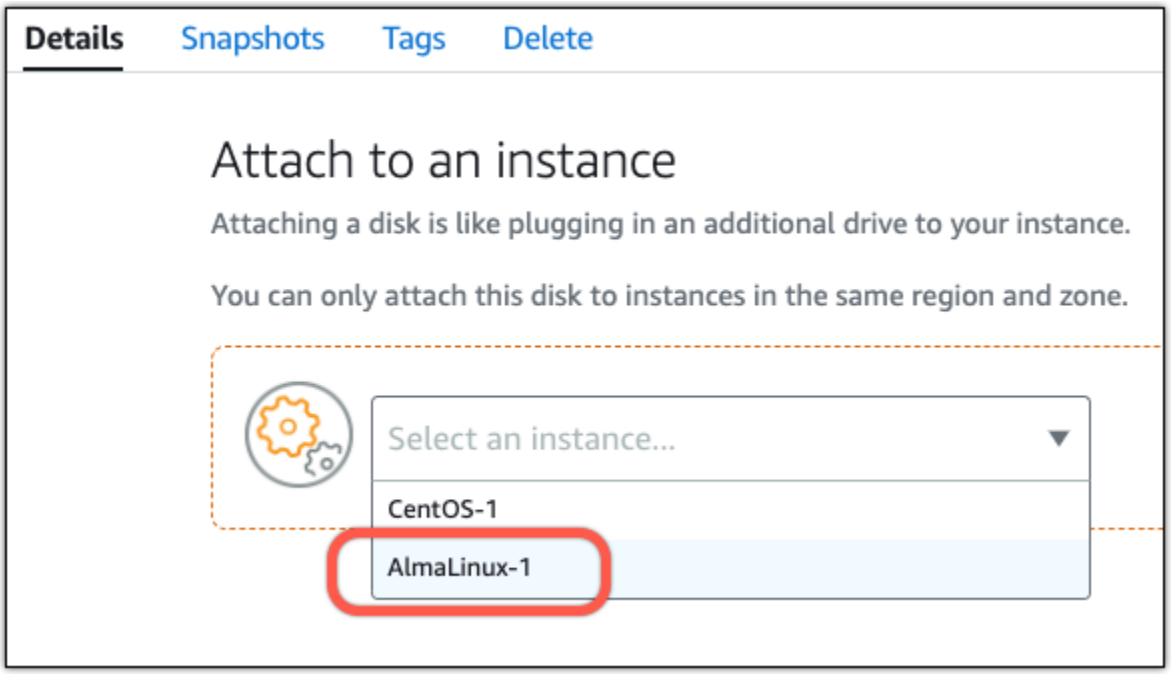
1. 从 Lightsail 控制台的 “存储” 部分，选择要与 CentOS 实例分离的磁盘。



2. 在详细信息选项卡上，选择分离。



3. 在磁盘详细信息页面中，选择附加到实例下拉菜单。然后选择您的 AlmaLinux 实例的名称。



4. 选择 附加。
5. （可选）您可能需要先连接到您的 AlmaLinux 实例并装载磁盘，然后才能访问其数据。有关更多信息，请参阅 连接到实例以格式化和挂载磁盘。

> **Warning**
>
> 上面的链接提供有关如何挂载和格式化所附加磁盘的说明。请勿格式化挂载到 AlmaLinux 实例的磁盘。对该磁盘进行格式化将永久删除存储在其上的所有信息。

在 Lightsail 上使用 cPanel 和 WHM 托管网站、电子邮件和服务

在你的 cPanel 和 WHM 实例在 Amazon Lightsail 上启动并运行之后，你应该采取以下几个步骤来开始使用。

> **Important**
>
> - 您的 cPanel 和 WHM 实例包含 15 天试用许可证。15 天后，您必须从 cPanel 购买许可证才能继续使用 cPanel 和 WHM。如果您计划购买许可证，请在购买许可证之前完成本指南的步骤 1-7。
> - 您必须选择内存至少 2 GB 的实例计划才能使用此蓝图。

内容

- 步骤 1：更改根用户密码
- 步骤 2：将静态 IP 地址附加到 cPanel 和 WHM 实例
- 步骤 3：首次登录 Web Host Manager
- 步骤 4：更改 cPanel 和 WHM 实例的主机名和 IP 地址
- 步骤 5：将域名映射到 cPanel 和 WHM 实例
- 步骤 6：编辑实例的防火墙
- 第 7 步：从你的 Lightsail 实例中移除 SMTP 限制
- 步骤 8：阅读 cPanel 和 WHM 文档并获取支持
- 步骤 9：购买 CPanel 和 WHM 的许可证
- 步骤 10：创建 CPanel 和 WHM 实例的快照

步骤 1：更改根用户密码

完成以下过程可更改 cPanel 实例上的根用户密码。您之后将使用根用户和密码登录 Web Host Manager (WHM) 控制台。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。
2. 连接后，请输入以下命令来更改根用户的密码：

```
sudo passwd
```

3. 输入强密码并通过再次输入确认密码。

> **Note**
>
> 密码不应包含词典单词，且应超过 7 个字符。如果您没有遵循这些指南，您会收到 BAD PASSWORD 警告。

请记住此密码，因为您之后会在本指南中使用它来登录 WHM 控制台。

步骤 2：将静态 IP 地址附加到 cPanel 和 WHM 实例

附加到实例的默认动态公有 IP 地址会在您每次停止和启动实例时发生变化。创建一个静态 IP 地址并将其附加到您的实例，以防止公有 IP 地址发生变化。稍后，当您对实例使用自己的域名时，就无需在每次停止和启动该实例时更新域的 DNS 记录。或者，如果您的实例出现故障，则您可以从备份恢复实例，然后将静态 IP 重新分配给新实例。您可以将静态 IP 附加到实例。

> **Important**
>
> 从 cPanel 购买许可证时，您必须指定 cPanel 和 WHM 实例的公有 IP 地址。您购买的许可证将与该 IP 地址相关联。因此，如果您计划从 cPanel 购买许可证，则必须将静态 IP 附加到 cPanel 和 WHM 实例。从 cPanel 购买许可证时请指定您的静态 IP，只要您计划在 Lightsail 实例上使用 cPanel 和 WHM 许可证，就可以保留您的静态 IP。如果您以后需要将许可证转移到另一个 IP 地址，您可以向 cPanel 提交请求。有关更多信息，请参阅 WHM 文档中的转移许可证。

在实例管理页面上的联网选项卡下，选择创建静态 IP，然后按照页面上的说明操作。

有关更多信息，请参阅创建静态 IP 并将其附加到实例。

步骤 3：首次登录 Web Host Manager

完成以下过程以首次登录 WHM 控制台。

1. 打开 Web 浏览器并导航到以下 Web 地址。*<StaticIP>*替换为您的实例的静态 IP 地址。请务必将 :2087 添加到地址末尾，即您将在其上建立与实例的连接的端口。

   ```
   https://<StaticIP>:2087
   ```

   示例：

   ```
   https://192.0.2.0:2087
   ```

   > **Important**
   >
   > 您必须在导航到实例的 IP 地址和端口时在浏览器的地址栏中包含 https://。否则，您将收到一个错误，表示无法访问该网站。

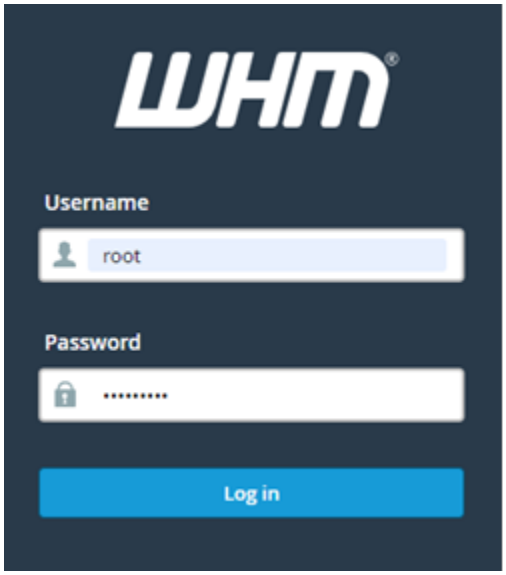
   如果您在通过端口 2087 浏览到实例的静态 IP 地址时无法建立连接，请检查您的路由器、VPN 或网络服务提供商是否允许通过端口 2087 进行 HTTP/HTTPS 连接。如果不允许，请尝试使用其他网络进行连接。

   您可能还会看到一个浏览器警告，指出您的连接不是私有的、不是安全的或存在安全风险。发生这种情况的原因是您的 cPanel 实例尚未应用 SSL/TLS 证书。在浏览器窗口中，选择高级、详细信息或更多信息以查看可用的选项。然后选择继续连接该网站，即使它不是私有或安全的。

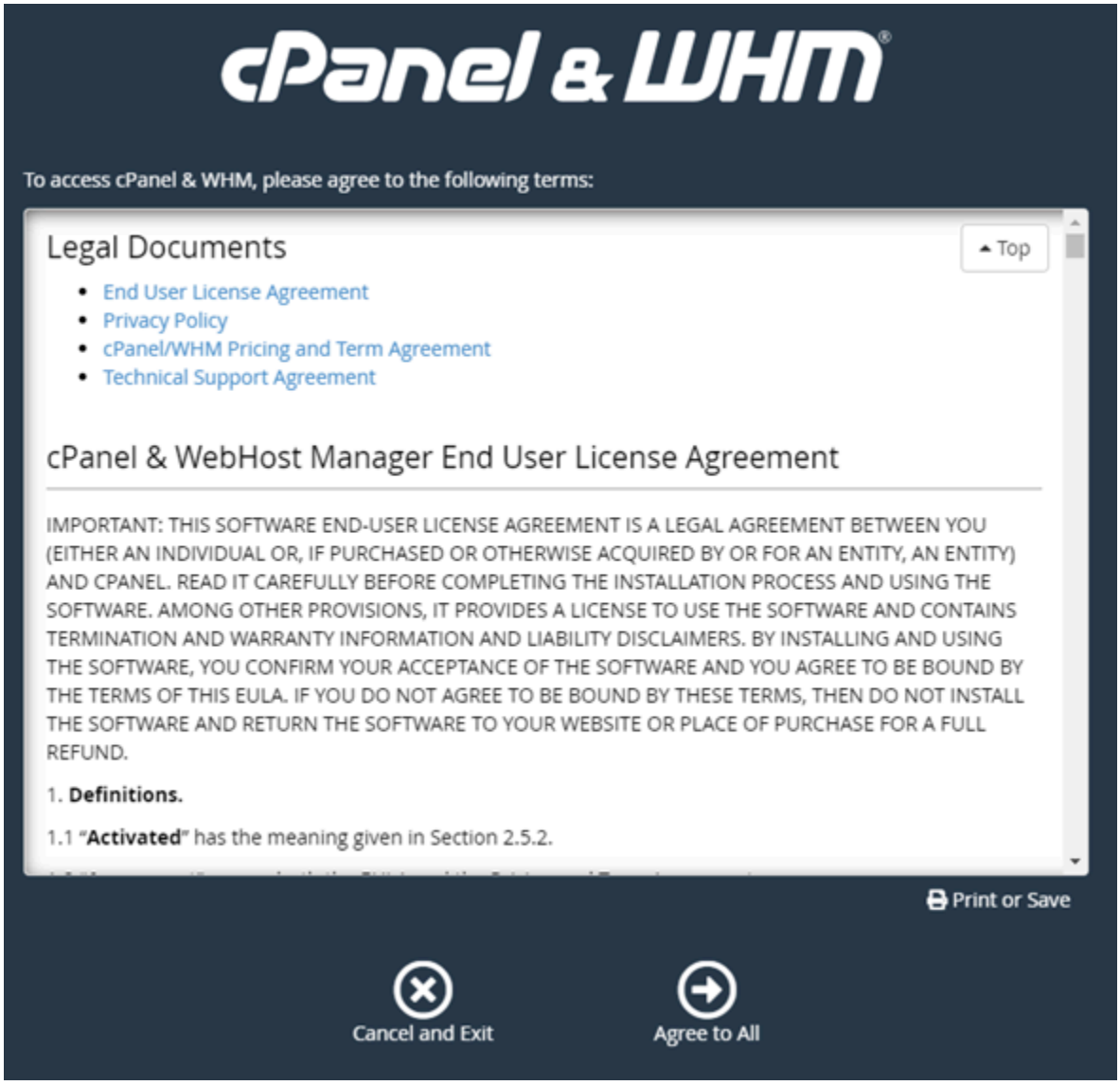
2. 在用户名文本框中输入 root。
3. 在密码文本框文本框中输入根用户密码。

   这是您之前在本指南的步骤 1：更改根用户密码部分指定的密码。

4. 选择登录。

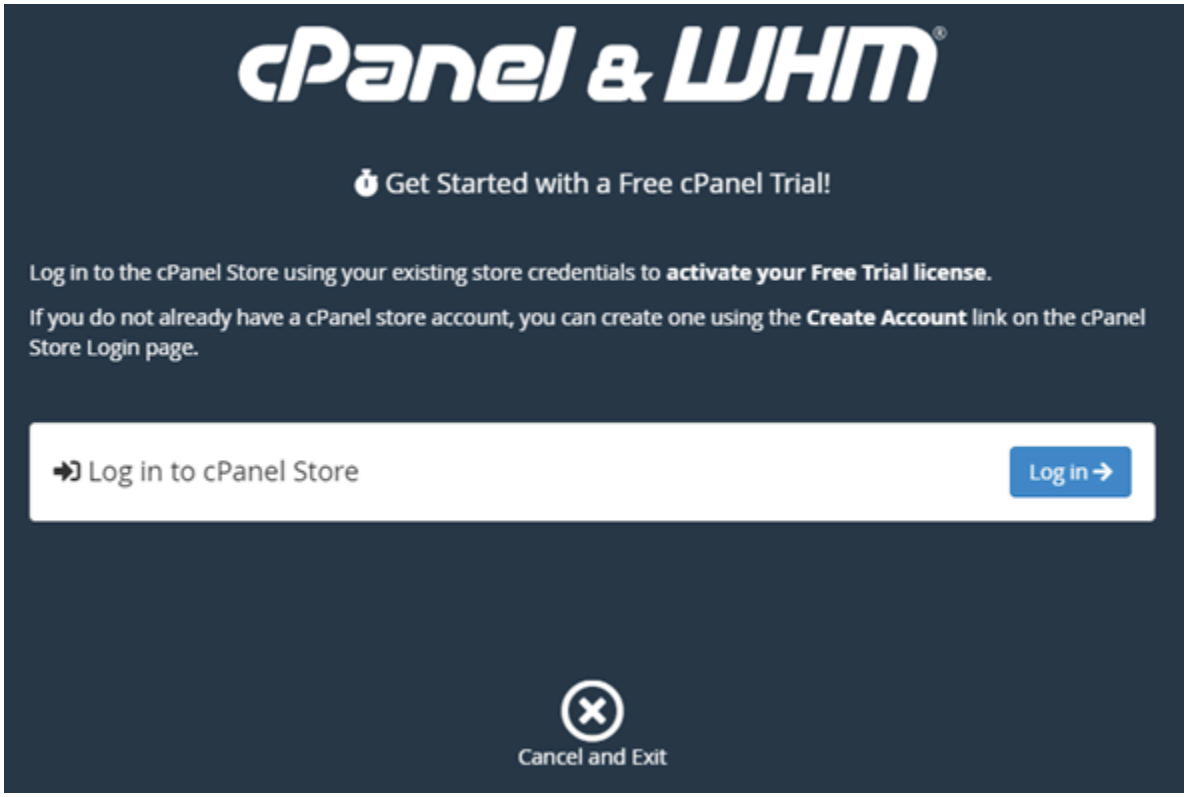


5. 阅读 cPanel 和 WHM 条款，然后选择全部同意（如果您想继续使用）。



6. 在开始使用免费的 cPanel 试用版页面上，选择登录以登录到 cPanel 商店。

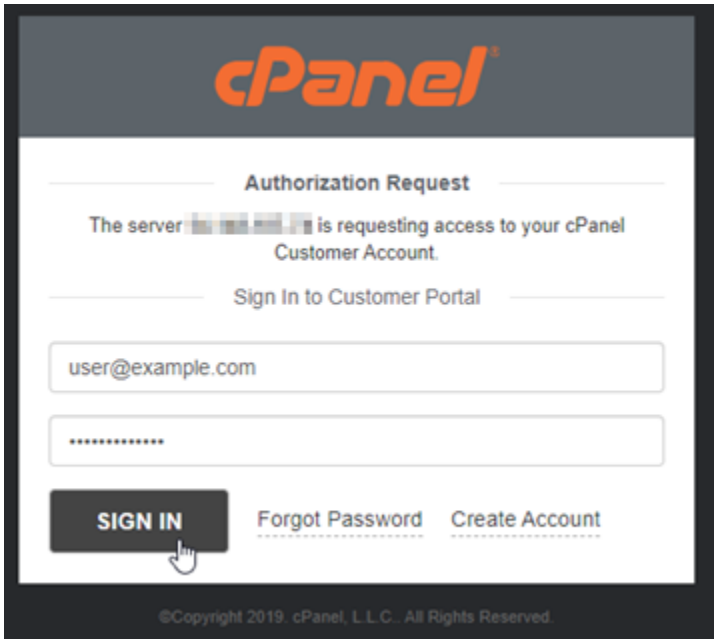
   您必须登录 cPanel 商店，才能将试用版许可证与您的账户关联。如果您没有 cPanel 商店账户，您仍应选择登录，然后您可以选择创建一个账户。



7. 在显示的授权请求页面中，输入您的电子邮件地址或用户名以及 cPanel 商店账户的密码。

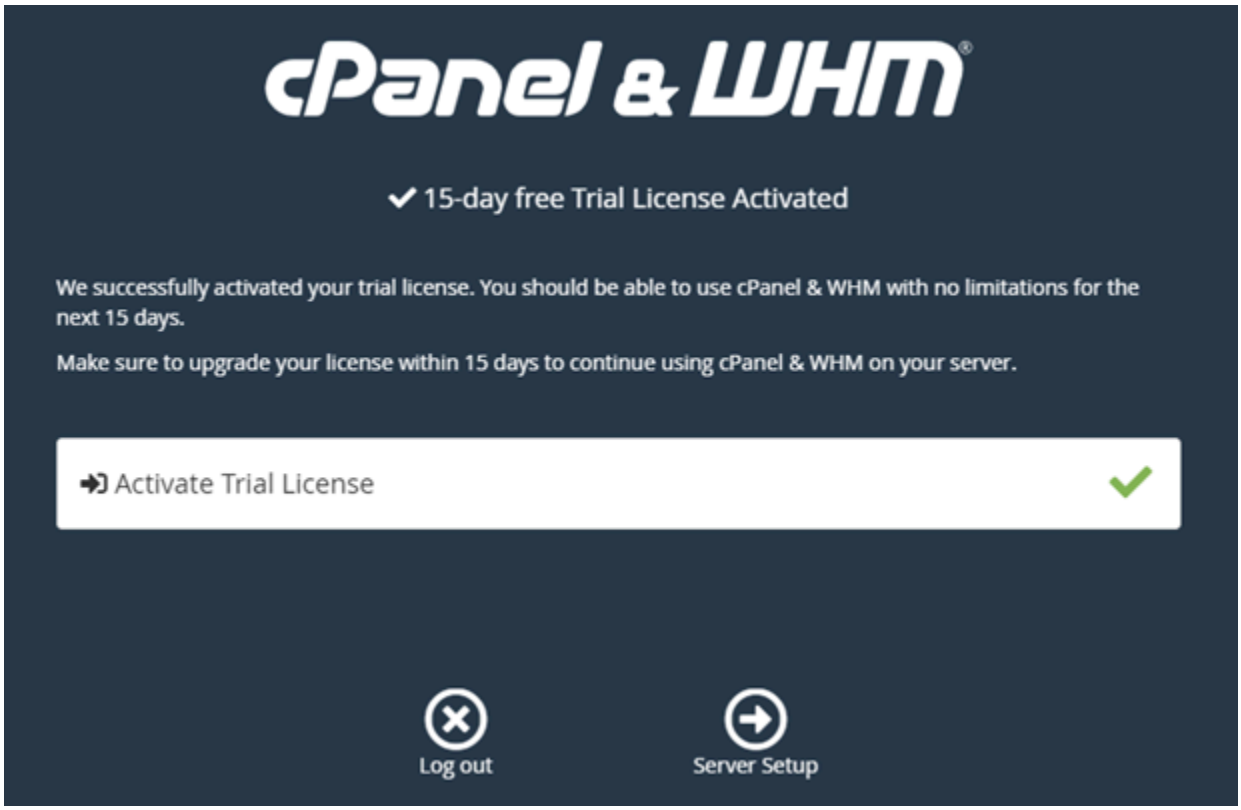
   如果您没有 cPanel 商店账户，请选择创建账户并按照提示创建新的 cPanel 商店账户。系统将要求您输入您的电子邮件地址，并向您发送一封电子邮件来设置您的 cPanel 商店账户密码。我们建议您使用新的浏览器选项卡来设置您的 cPanel 商店账户密码。设置密码后，您可以关闭该选项卡并返回到您的实例以授权您的账户，然后继续执行此过程的下一步。

8. 选择登录。

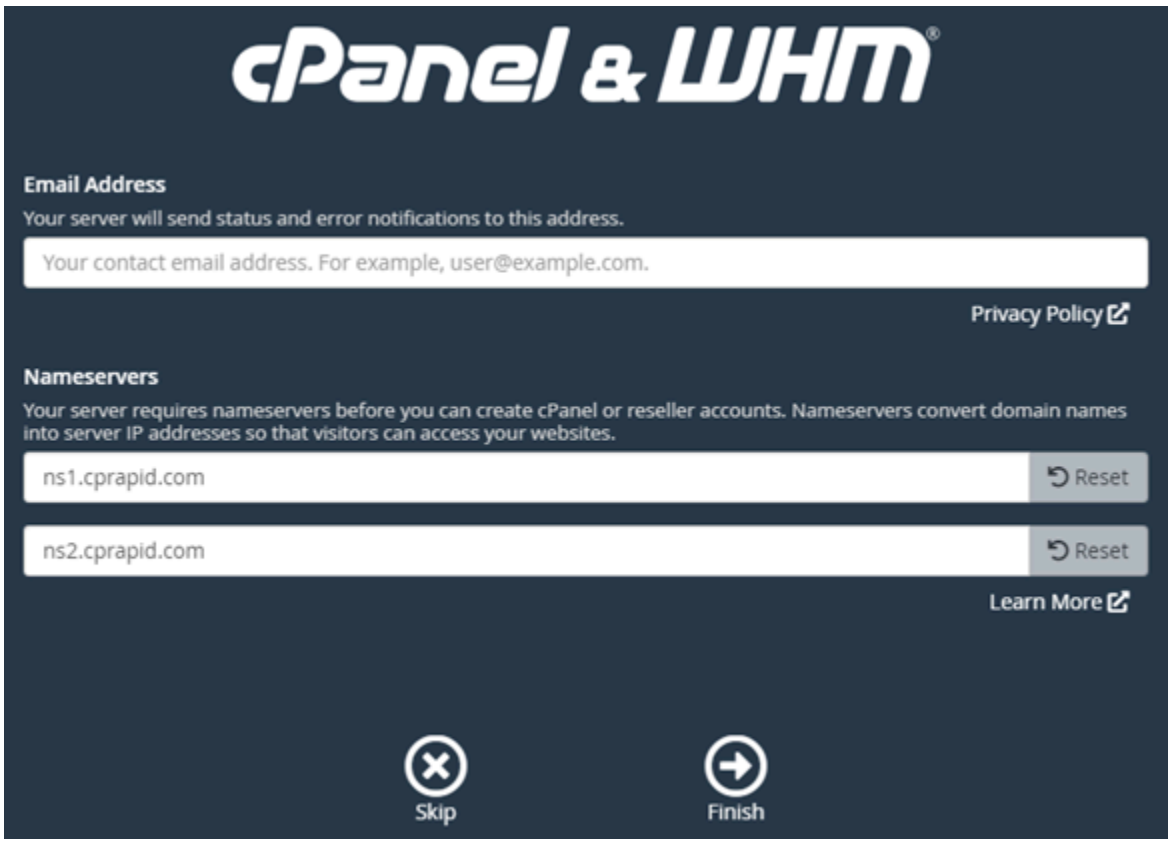


登录后，您的 cPanel 和 WHM 实例将获得与您的 cPanel 商店账户关联的 15 天试用许可证。在 cPanel 商店中转到管理许可证页面，查看已颁发的许可证，包括试用许可证。

9. 选择服务器设置以继续操作。



10. 在电子邮件地址和名称服务器页面中选择跳过。之后可以对它们进行配置。

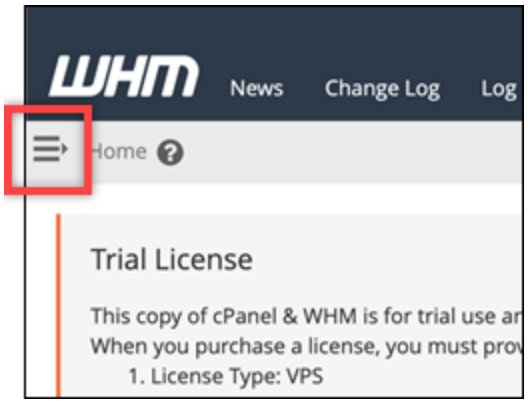


将显示 WHM 控制台，您可以在其中管理 cPanel 的设置和功能。

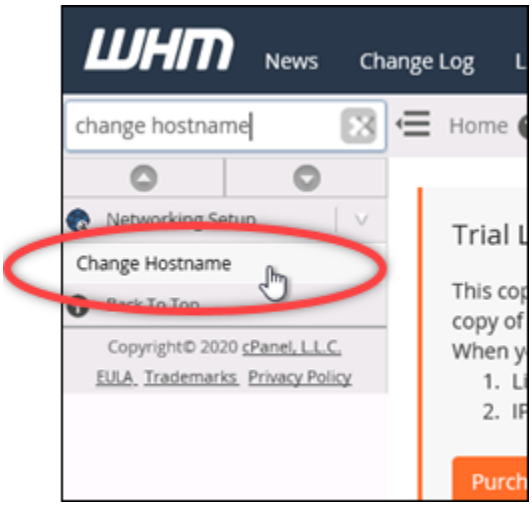
步骤 4：更改 cPanel 和 WHM 实例的主机名和 IP 地址

请完成以下步骤来更改实例的主机名，这样您就不必使用其公有 IP 地址来访问 WHM 控制台。您还应将实例的 IP 地址更改为您之前在本指南的步骤 2：将静态 IP 地址附加到 cPanel 和 WHM 实例部分附加到实例的新静态 IP 地址。

1. 选择 WHM 控制台左上角的导航菜单图标。

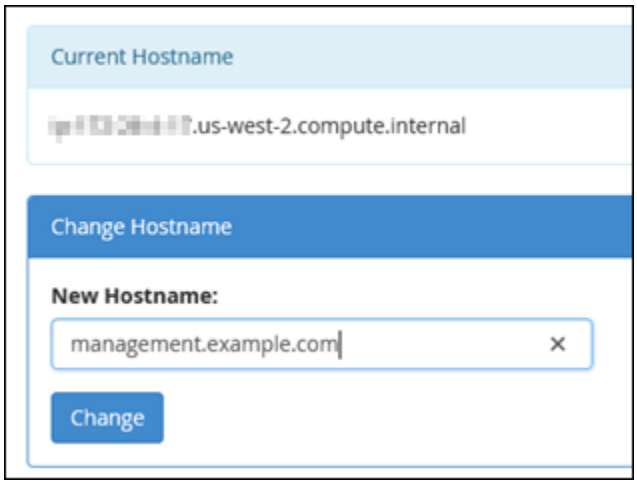


2. 在 WHM 控制台的搜索文本框中输入 Change hostname，然后选择结果中的更改主机名选项。

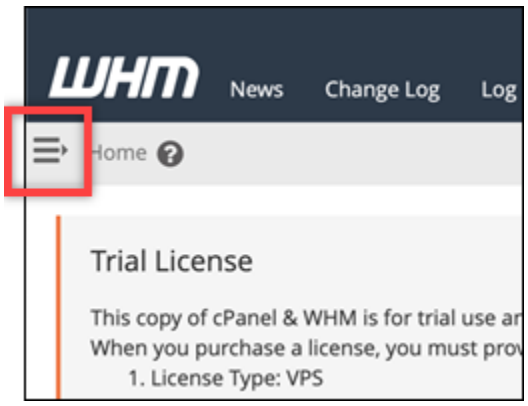


3. 在新主机名文本框中输入要用于访问 WHM 控制台的主机名。例如，输入 `management.example.com` 或 `administration.example.com`。

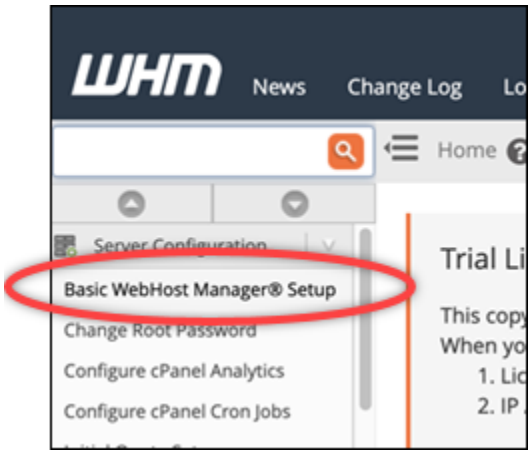
> **Note**
>
> 您只能指定子域作为主机名，不能指定 `whm` 或 `cpanel` 作为子域。



4. 选择 Change (更改)。
5. 选择 WHM 控制台左上角的导航菜单图标。

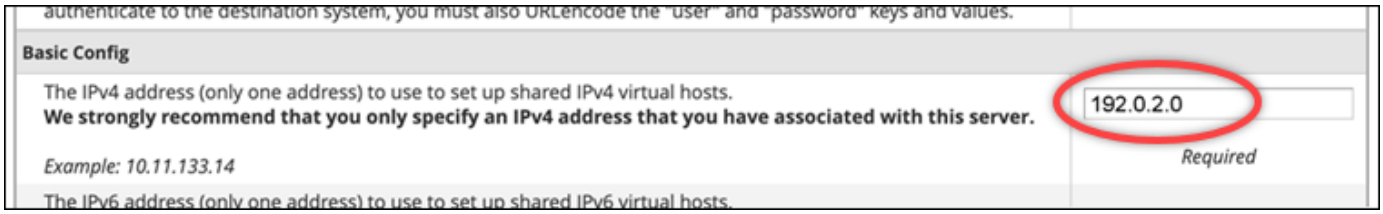


6. 选择 “基本 WebHost 管理器设置”。



7. 在全部选项卡下，向下滚动并找到页面的基本 Config部分。

8. 在 IPv4 地址文本框中，输入实例的新静态 IP 地址。有关信息 IPv6，请参阅[在 cPanel 实例 IPv6 上配置]。



9. 滚动到页面底部并选择 Save Changes (保存更改)。

> **Note**
>
> 如果您收到无效的许可证文件错误消息，请等待并在几分钟后再次尝试更改 IP 地址。

实例的主机名和 IP 地址现在已更改，但您仍然必须将您的域名映射到 cPanel 和 WHM 实例。您可以通过在您的注册域名的注册域名系统 (DNS) 中添加地址 (A) 记录来执行此操作。A 记录会将实例的主机名解析为实例的静态 IP 地址。我们将在本指南的下一部分介绍如何执行此操作。

步骤 5：将域名映射到 cPanel 和 WHM 实例

> **Note**
>
> 您可以将域映射到 cPanel 和 WHM 实例，可使用该实例来访问 WHM 控制台。您还可以在 WHM 中映射多个域，可使用这些域来管理 WHM 中的网站。本节介绍如何将域映射到 cPanel 和 WHM 实例。有关在 WHM 控制台中映射多个域（创建新账户时执行此操作）的详细信息，请参阅WHM 文档中的创建新账户。

要将域名（如 `management.example.com` 或 `administration.example.com`）映射到实例，您需要向域的域名系统 (DNS) 添加地址 (A) 记录。A 记录会将 cPanel 和 WHM 实例的主机名解析为实例的静态 IP 地址。在 A 记录中指定的子域必须与您之前在本指南的步骤 4：更改 cPanel 和 WHM 实例的主机名和 IP 地址部分指定的主机名一致。添加 A 记录后，您可以使用以下地址访问实例的 WHM 控制台，而不是使用实例的静态 IP 地址。*<InstanceHostName>*替换为您的实例的主机名。

```
https://<InstanceHostName>/whm
```

示例：

```
https//management.example.com/whm
```

DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。为此，请登录 Lightsail 控制台。在 Lightsail 控制台主页上，选择 “域名和 DNS” 选项卡，然后选择 “创建 DNS 区域”。按照页面上的说明将您的域名添加到 Lightsail。有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

步骤 6：编辑实例的防火墙

默认在您的 cPanel 和 WHM 实例上打开以下防火墙端口：

- SSH - TCP - 22
- DNS (UDP) - UDP - 53

- DNS (TCP) - TCP - 53
- HTTP - TCP - 80
- HTTPS - TCP - 443
- 自定义 - TCP - 2078
- 自定义 - TCP - 2083
- 自定义 - TCP - 2087
- 自定义 - TCP - 2089

根据计划在实例上使用的服务和应用程序，您可能需要打开其他端口。例如，为电子邮件服务打开端口 25、143、465、587、993、995、2096，以及为日历服务打开端口 2080、2091。在实例管理页面的 Networking (联网) 选项卡下，滚动到页面的“Firewall (防火墙)”部分，然后选择 Add rule (添加规则)。选择应用程序、协议以及要打开的端口或端口范围。完成后，选择 Create (创建)。

有关要打开哪些端口的更多信息，请参阅 cPanel 文档中的如何配置 cPanel 服务的防火墙。有关在 Lightsail 中编辑实例防火墙的更多信息，请参阅在 Amazon Lightsai l 中添加和编辑实例防火墙规则。

第 7 步：从你的 Lightsail 实例中移除 SMTP 限制

AWS 阻止所有 Lightsail 实例上端口 25 上的出站流量。要在端口 25 上发送出站流量，可请求移除此限制。有关更多信息，请参阅如何从我的 Lightsail 实例中移除对端口 25 的限制？ 。

> **Important**
>
> 如果您将 SMTP 配置为使用端口 25、465 或 587，则必须在 Lightsail 控制台中打开实例防火墙中的这些端口。有关更多信息，请参阅在 Amazon Lightsail 中添加和编辑实例防火墙规则。

步骤 8：阅读 cPanel 和 WHM 文档并获取支持

阅读 cPanel 和 WHM 文档，了解如何使用 cPanel 和 WHM 管理 Web 站点。有关更多信息，请参阅 cPanel 和 WHM 文档。

如果您对 cPanel 和 WHM 有疑问或需要支持，可使用以下资源联系 cPanel：

- cPanel 对您的安装进行故障排查
- cPanel Discord 通道

步骤 9：购买 CPanel 和 WHM 的许可证

您的 cPanel 和 WHM 实例包含 15 天试用许可证。15 天后，您必须从 cPanel 购买许可证才能继续使用 cPanel 和 WHM。有关更多信息，请参阅 CPanel 文档中的如何购买 cPanel 许可证。

> **Important**
>
> 从 cPanel 购买许可证时，您必须指定 cPanel 和 WHM 实例的公有 IP 地址。您购买的许可证将与该 IP 地址相关联。因此，您必须将静态 IP 附加到 cPanel 和 WHM 实例，如本指南的步骤 2：将静态 IP 地址附加到 cPanel 和 WHM 实例部分所述。从 cPanel 购买许可证时请指定您的静态 IP，只要您计划在 Lightsail 实例上使用 cPanel 和 WHM 许可证，就可以保留您的静态 IP。如果您以后需要将许可证转移到另一个 IP 地址，您可以向 cPanel 提交请求。有关更多信息，请参阅 WHM 文档中的转移许可证。

步骤 10：创建 CPanel 和 WHM 实例的快照

快照是系统磁盘和实例初始配置的副本。快照包含恢复实例所需的所有数据（从拍摄快照的那一刻开始）。您可以将快照用作新实例的基准或用于数据备份。您可以随时创建实例的手动快照，或者启用自动快照，让 Lightsail 每天为您创建快照。

> **Note**
>
> - 当前一代蓝图 cPanel 和 WHM 的实例快照 AlmaLinux可以导出到亚马逊。 EC2
> - Linux 版上一代蓝图 cPanel 和 WHM 的实例快照 EC2 目前无法导出到亚马逊。
> - 如果您从快照创建新实例，请按照步骤 3 中的说明，在登录 WHM 之前为该实例提供额外的时间来完全启动。

在实例管理页面的 Snapshot (快照) 选项卡下，输入快照名称，然后选择 Create snapshot (创建快照)。或滚动到页面的自动快照部分，然后选择开关以启用自动快照。

有关更多信息，请参阅创建 Linux 或 Unix 实例的快照和在 Amazon Lightsail 中启用或禁用实例或磁盘的自动快照。

在 Lightsail 上设置和自定义你的 Drupal 网站

在你的 Drupal 实例在 Amazon Lightsail 上启动并运行后，你应该采取以下几个步骤来开始使用：

内容

- 步骤 1：阅读 Bitnami 文档
- 步骤 2：获取默认的应用程序密码以访问 Drupal 管理控制面板
- 步骤 3：将静态 IP 地址附加到实例
- 步骤 4：登录到 Drupal 网站的管理控制面板
- 第 5 步：将注册域名的流量路由到 Drupal 网站
- 步骤 6：配置 Drupal 网站的 HTTPS
- 第 7 步：阅读 Drupal 文档并继续配置网站
- 步骤 8：创建实例的快照

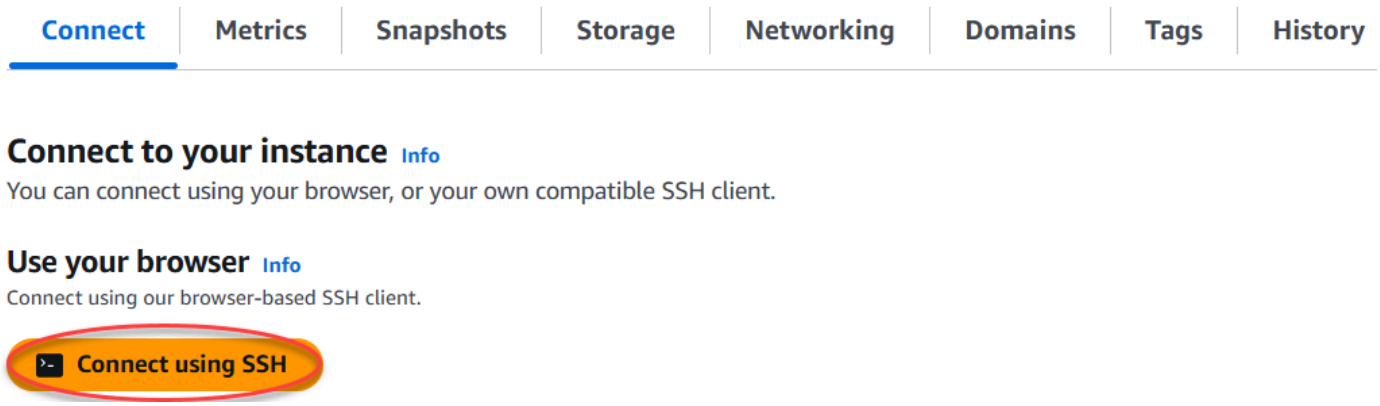
步骤 1：阅读 Bitnami 文档

阅读 Bitnami 文档以了解如何配置 Drupal 应用程序。有关更多信息，请参阅 Bitnami 为 AWS Cloud打包的 Drupal。

步骤 2：获取默认的应用程序密码以访问 Drupal 管理控制面板

完成以下程序以获取访问 Drupal 网站的管理控制面板所需的默认应用程序密码。有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

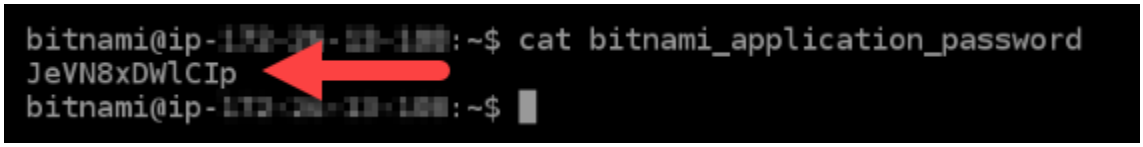
1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来获取应用程序密码：

```
cat $HOME/bitnami_application_password
```

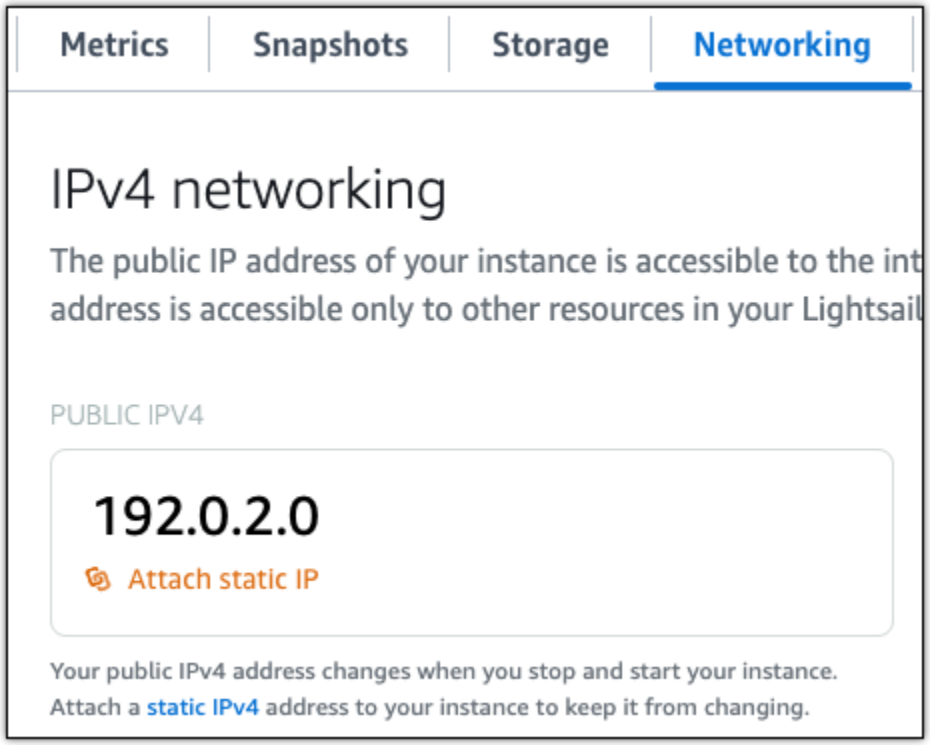
您应该会看到与以下示例类似的响应，其中包含默认应用程序密码：



步骤 3：将静态 IP 地址附加到实例

在您首次创建实例时分配给实例的公有 IP 地址会在您每次停止和启动实例时发生更改。您应为实例创建和附加静态 IP 地址，以确保其公有 IP 地址不变。之后当您将注册域名（如 `example.com`）指向实例时，无需在每次停止和重启实例时都更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择创建静态 IP或附加静态 IP（如果您之前创建了可附加到实例的静态 IP），然后按照页面上的说明操作。有关更多信息，请参阅创建静态 IP 并将其附加到实例。



步骤 4：登录到 Drupal 网站的管理控制面板

现在您已有默认用户密码，请导航到 Drupal 网站的主页，然后登录管理控制面板。登录后，您可以开始自定义网站并进行管理更改。要详细了解您可以在 Drupal 中执行的操作，请参阅本指南后面的 第 7 步：阅读 Drupal 文档并继续配置网站 部分。

1. 在实例管理页面上的 Connect（连接）选项卡下，记下实例的公有 IP 地址。公有 IP 地址也显示在实例管理页面的标题部分。



2. 浏览到实例的公有 IP 地址，例如，转到 `http://203.0.113.0`。

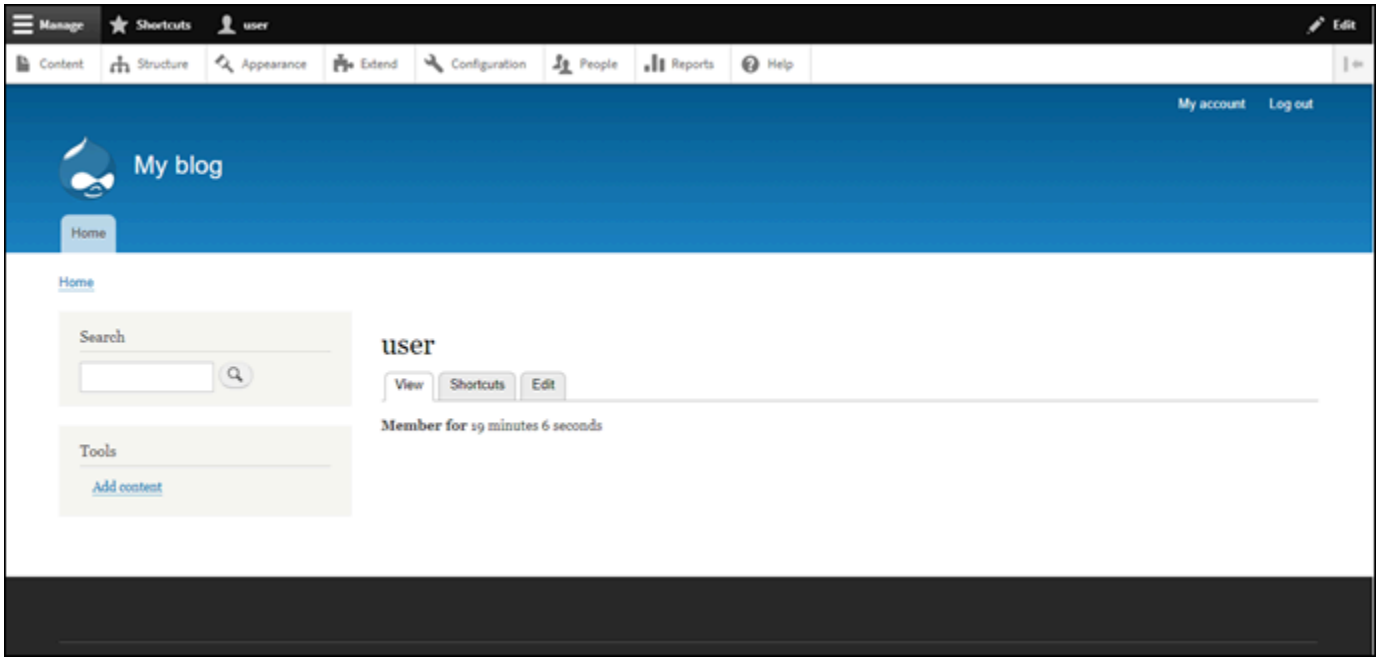
   您的 Drupal 网站的主页应该会出现。

3. 选择 Drupal 网站主页右下角的 Manage（管理）。

   如果 Manage（管理）横幅未显示，您可以通过浏览 `http://<PublicIP>/user/login` 到达登录页面。将 *<PublicIP>* 替换为实例的公有 IP 地址。

4. 使用之前在本指南中检索到的默认用户名（`user`）和默认密码登录。

   此时将显示 Drupal 管理控制面板。



步骤 5：将注册域名的流量路由到 Drupal 网站

要将注册域名（如 `example.com`）的流量路由到 Drupal 网站，您需要向域的域名系统（DNS）添加一条记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

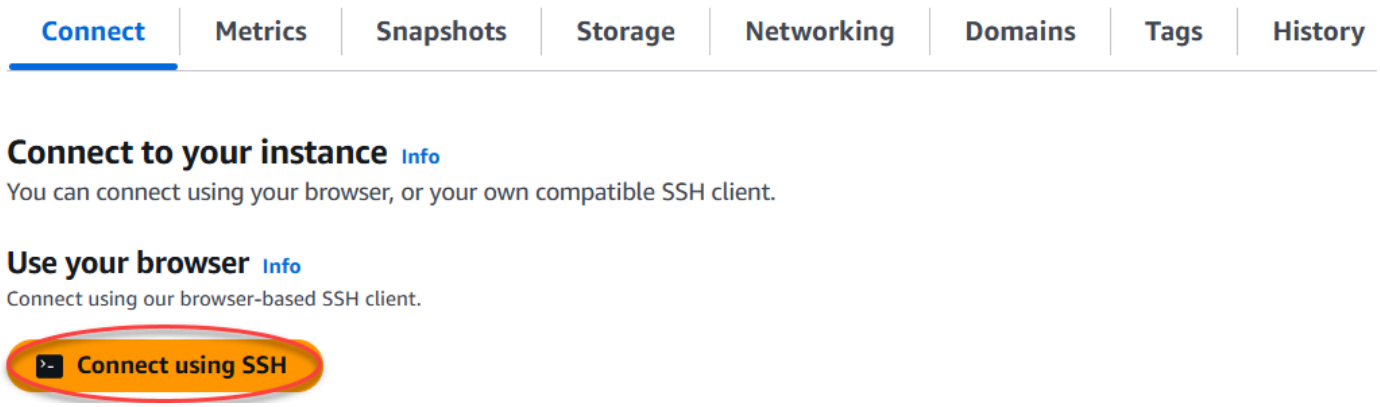
如果您浏览到为实例配置的域名，则应将您重定向到 Drupal 网站的主页。接下来，您应该生成并配置 SSL/TLS 证书，以启用 Drupal 网站的 HTTPS 连接。有关更多信息，请继续到本指南的下一节步骤 6：配置 Drupal 网站的 HTTPS。

步骤 6：配置 Drupal 网站的 HTTPS

完成以下程序以在 Drupal 网站上配置 HTTPS。这些步骤向您展示如何使用 Bitnami HTTPS 配置工具（`bncert-tool`），这是一个命令行工具，用于请求 Let's Encrypt SSL/TLS 证书。有关更多信息，请参阅 Bitnami 文档中的了解 Bitnami HTTPS 配置工具。

> **Important**
>
> 在开始此过程之前，请确保对域进行配置，以将流量路由到 Drupal 实例。否则，SSL/TLS 证书验证过程将失败。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，输入以下命令以确认 bncert 工具已安装在实例上。

```
sudo /opt/bitnami/bncert-tool
```

您应看到以下响应之一：

- 如果您在响应中看到命令未找到，则 bncert 工具未安装到实例上。继续执行此过程的后续步骤以在实例上安装 bncert 工具。
- 如果您在响应中看到欢迎使用 Bitnami HTTPS 配置工具，则 bncert 工具已安装到实例上。继续执行此过程的步骤 8。

- 如果 bncert 工具已在您的实例上安装了一段时间，那么您可能会看到一条消息，指示该工具的更新版本可供使用。选择进行下载，然后再次输入 sudo /opt/bitnami/bncert-tool 命令来运行 bncert 工具。继续执行此过程的步骤 8。

3. 输入以下命令以将 bncert 运行文件下载到您的实例中。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. 输入以下命令以在您的实例上创建 bncert 工具运行文件的目录。

```
sudo mkdir /opt/bitnami/bncert
```

5. 输入以下命令以创建可作为程序执行的 bncert 运行文件。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 输入以下命令以创建符号链接，该符号链接在您输入 sudo /opt/bitnami/bncert-tool 命令时运行 bncert 工具。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

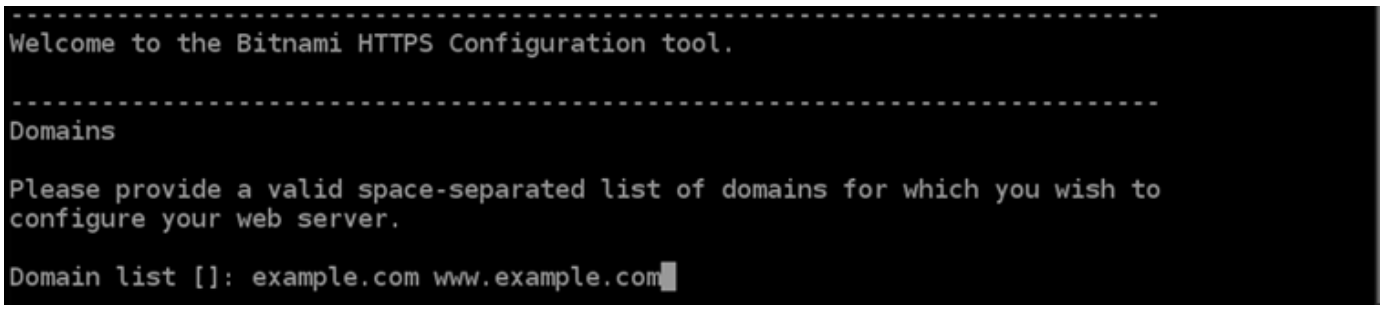
您现在已完成在实例上安装 bncert 工具的步骤。

7. 要运行 bncert 工具，请输入以下命令。

```
sudo /opt/bitnami/bncert-tool
```

8. 输入用空格分隔的主域名和备用域名，如以下示例所示。

如果您的域未配置为将流量路由到实例的公有 IP 地址，则 bncert 工具将要求您在继续之前进行该配置。您的域必须将流量路由到使用 bncert 工具以在实例上启用 HTTPS 的实例的公有 IP 地址。这将确认您拥有该域，并能用于进行证书的验证。



9. bncert 工具会询问您希望如何配置网站的重新导向。以下是可用的选项：

   - 启用 HTTP 重新导向到 HTTPS - 指定是否将浏览网站 HTTP 版本（即 http://example.com）的用户自动重新导向到 HTTPS 版本（即 https://example.com)。我们建议启用此选项，因为它会强制所有访问者使用加密连接。输入 Y 然后按 Enter 以启用它。
   - 启用非 www 重新导向到 www - 指定是否将浏览顶级域（即 https://example.com）的用户自动重新导向到域的 www 子域（即 https://www.example.com)。我们建议启用此选项。但如果您在搜索引擎工具（如 Google 站点管理员工具）中指定了顶级域作为首选网站地址，或者顶级域直接指向您的 IP 且 www 子域通过别名记录引用您的顶级域，则您可能希望禁用它并启用其他选项（启用 www 重新导向到非 www）。输入 Y 然后按 Enter 以启用它。
   - 启用 www 到非 www 重新导向 - 指定是否将浏览域的 www 子域（即 https://www.example.com）的用户自动重新导向到顶级域（即 https://example.com)。如果您启用了非 www 重新导向到 www，建议禁用此选项。输入 N 然后按 Enter 以禁用它。

   您的选择应类似于以下示例：

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.


Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

10. 将列出要进行的更改。输入 Y 然后按 Enter 以确认并继续。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. 输入要与 Let's Encrypt 证书关联的电子邮件地址，然后按 Enter（确定键）。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

12. 查看 Let's Encrypt 的加密用户协议 输入 Y 然后按 Enter 接受协议并继续。

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

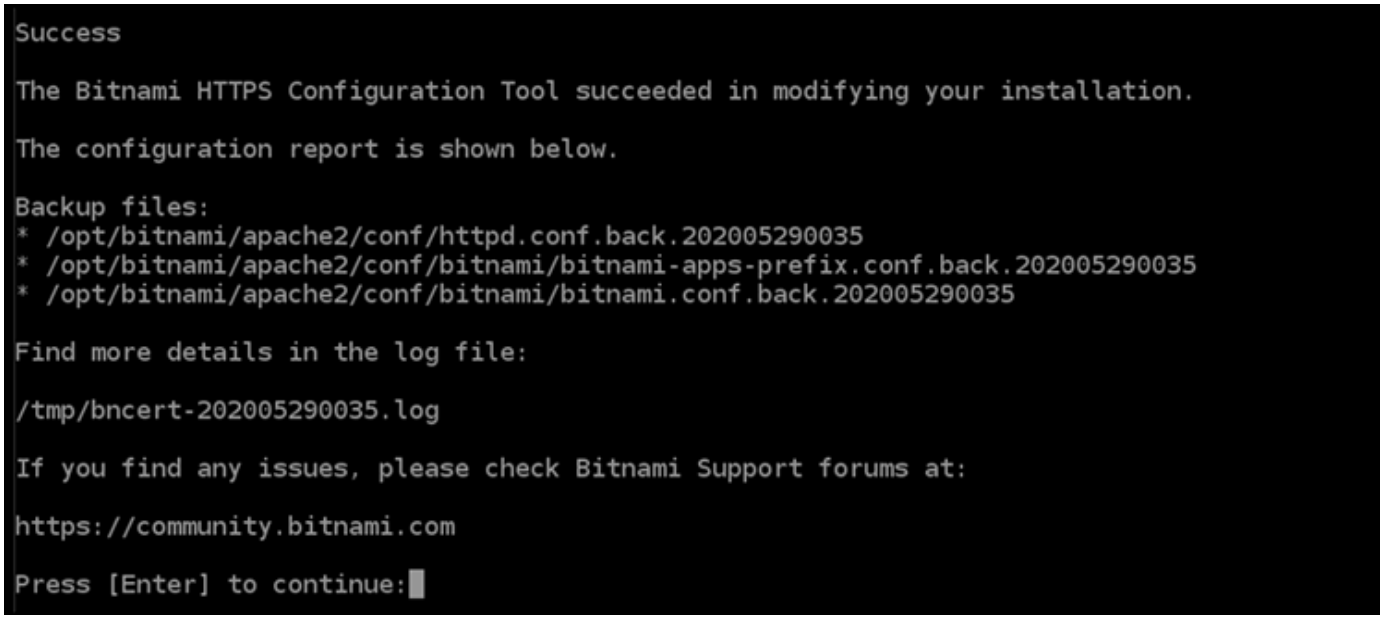
将执行这些操作以在您的实例上启用 HTTPS，包括请求证书和配置您指定的重新导向。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|
```

您的证书已成功颁发和验证，如果您看到类似于以下示例的消息，则表示在实例上成功配置了重新导向。



`bncert` 工具将在证书过期前每 80 天执行一次自动续订。如果您希望将其他域和子域用于实例，并且希望为这些域启用 HTTPS，请重复上述步骤。

您现在已完成在您的 Drupal 实例上启用 HTTPS。下次使用配置的域浏览到 Drupal 网站时，您应该会看到它重定向到 HTTPS 连接。

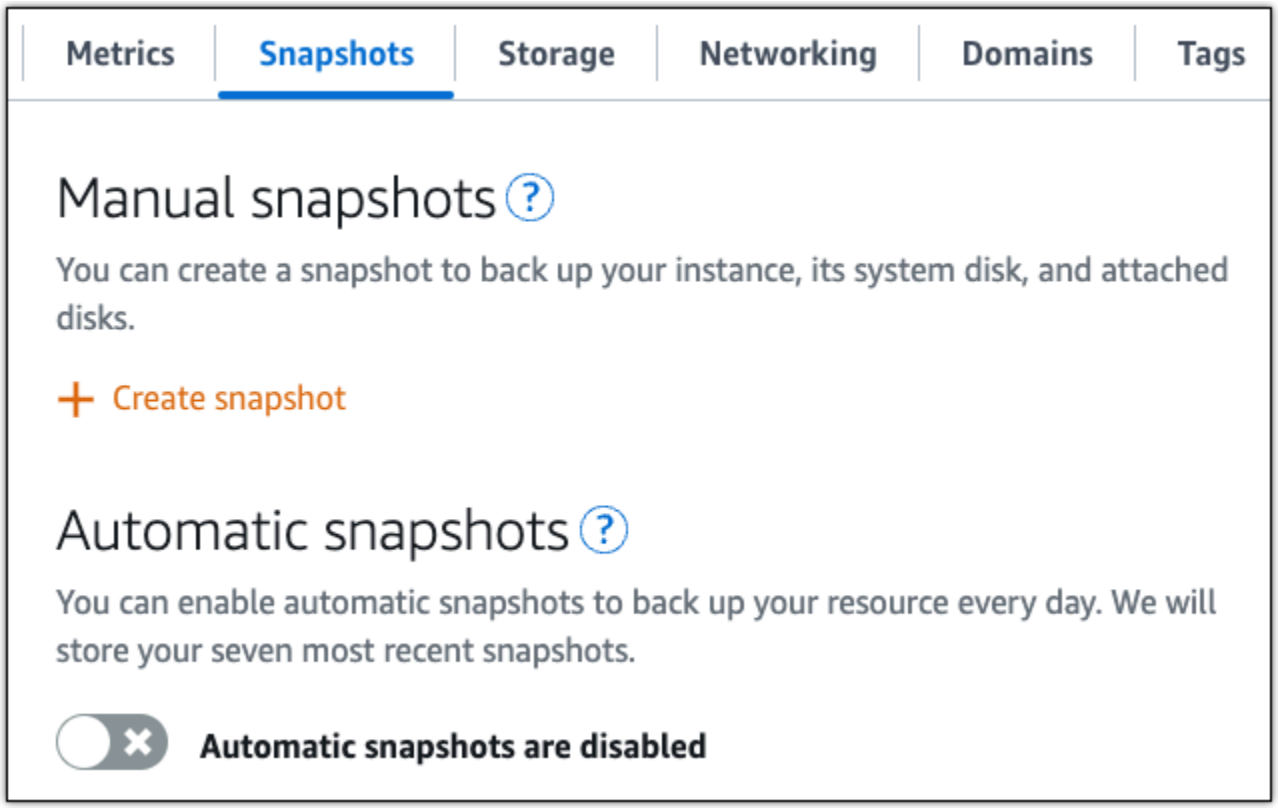
第 7 步：阅读 Drupal 文档并继续配置网站

阅读 Drupal 文档，了解如何管理和自定义网站。有关更多信息，请参阅 Drupal 文档。

步骤 8：创建实例的快照

按照您所需的方式配置 Drupal 网站后，创建实例的定期快照以进行备份。您可以手动创建快照，也可以启用自动快照，让 Lightsail 为您创建每日快照。如果实例出现错误，则可使用快照来创建新的替代实例。有关更多信息，请参阅快照。

在实例管理页面的快照选项卡下，选择创建快照或选择启用自动快照。



有关更多信息，请参阅在 Amazon Lightsail 中创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。

在 Lightsail 上部署 Ghost 网站

在你的 Ghost 实例在 Amazon Lightsail 上启动并运行之后，你应该采取以下几个步骤来开始使用：

内容

- 步骤 1：阅读 Bitnami 文档
- 步骤 2：获取默认应用程序密码以访问 Ghost 管理控制面板
- 步骤 3：将静态 IP 地址附加到实例
- 步骤 4：登录到 Ghost 网站的管理控制面板
- 步骤 5：将注册域名的流量路由到 Ghost 网站
- 步骤 6：配置 Ghost 网站的 HTTPS
- 步骤 7：阅读 Ghost 文档并继续配置网站
- 步骤 8：创建实例的快照

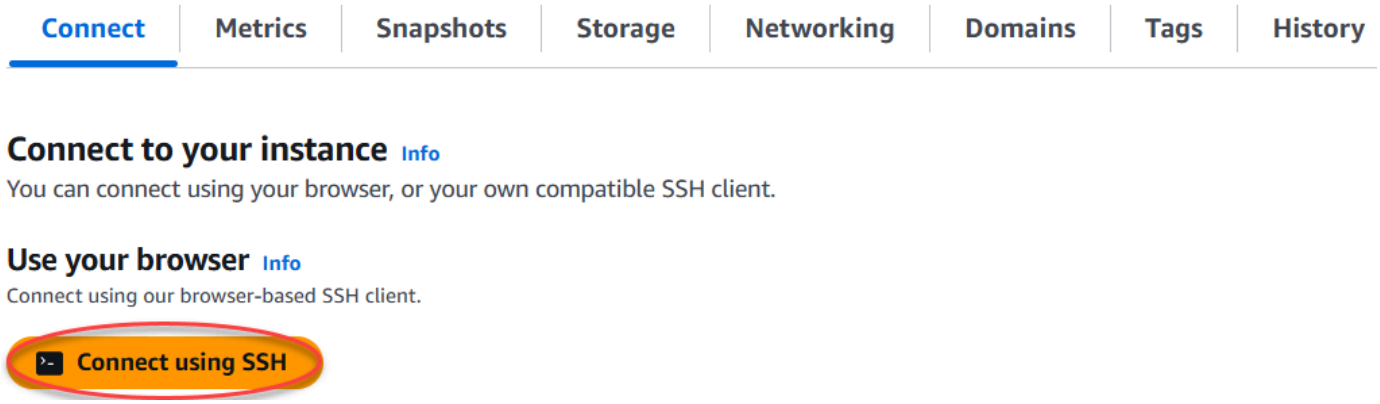
步骤 1：阅读 Bitnami 文档

阅读 Bitnami 文档以了解如何配置 Ghost 应用程序。有关更多信息，请参阅 Bitnami 为 AWS Cloud打包的 Ghost。

步骤 2：获取默认应用程序密码以访问 Ghost 管理控制面板

完成以下程序以获取访问 Ghost 网站的管理控制面板所需的默认应用程序密码。有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来获取应用程序密码：

```
$ cat $HOME/bitnami_application_password
```

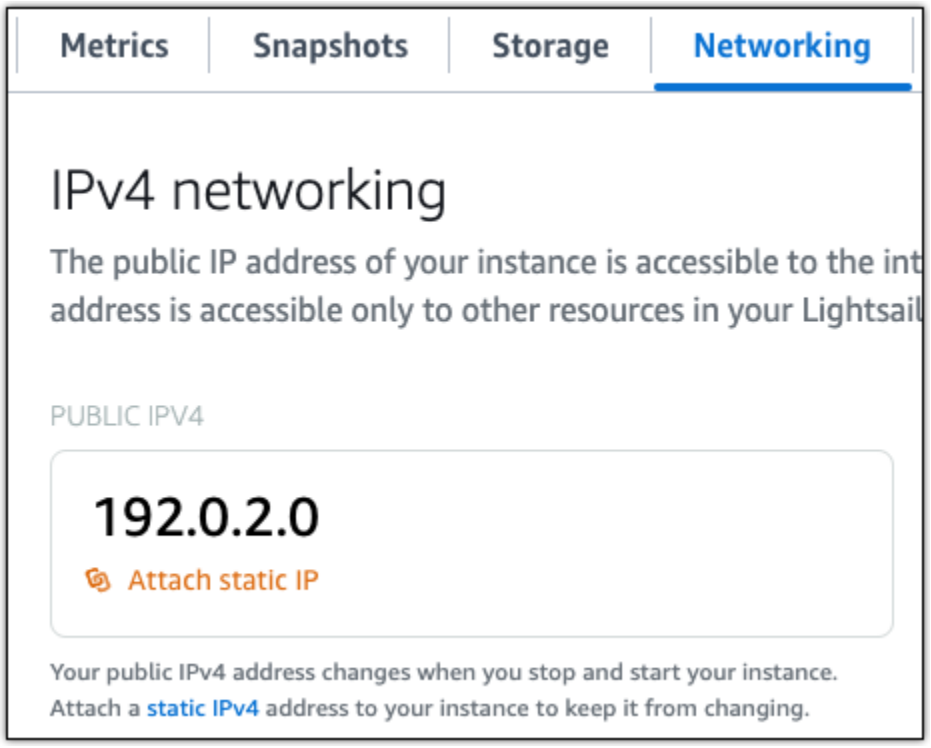
您应该会看到与以下类似的响应，其中包含默认应用程序密码：

```
bitnami@ip-192-0-2-0:~$ cat $HOME/bitnami_application_password
wB2Ex@mplEK6
```

步骤 3：将静态 IP 地址附加到实例

在您首次创建实例时分配给实例的公有 IP 地址会在您每次停止和启动实例时发生更改。您应为实例创建和附加静态 IP 地址，以确保其公有 IP 地址不变。之后当您将注册域名（如 `example.com`）指向实例时，无需在每次停止和重启实例时都更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择创建静态 IP或附加静态 IP（如果您之前创建了可附加到实例的静态 IP），然后按照页面上的说明操作。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

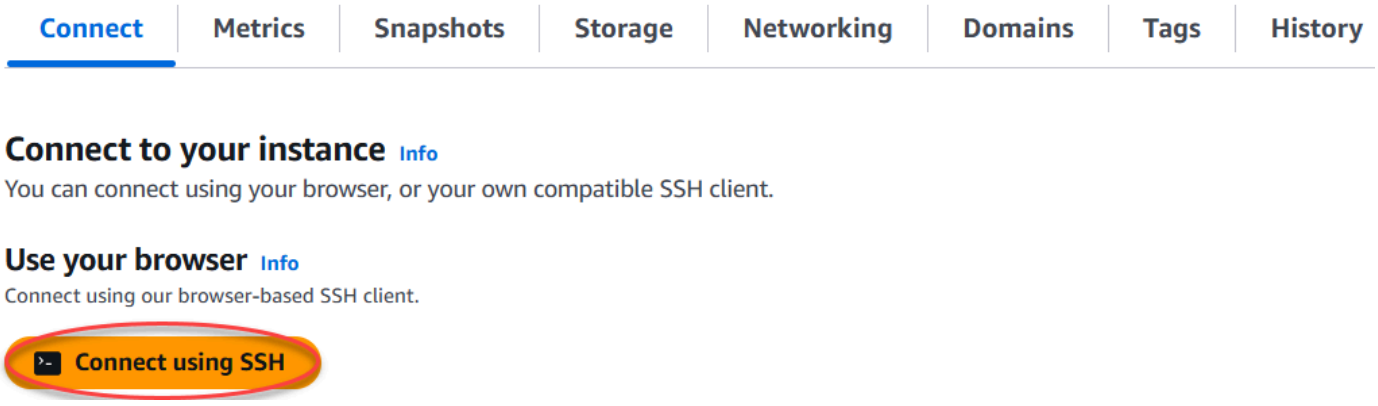


将新的静态 IP 地址附加到实例后，您必须完成以下步骤，以使应用程序知道新的静态 IP 地址。

1. 记下实例的静态 IP 地址。它列在实例管理页面的标题部分。



2. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



3. 连接后，请输入以下命令。*<StaticIP>*替换为您的实例的新静态 IP 地址。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您可以看到类似以下内容的响应。现在，实例上的应用程序应该识别到了新的静态 IP 地址。

```
bitnami@ip-203.0.113.0:~$ sudo /opt/bitnami/configure_app_domain --domain
 203.0.113.0
Configuring domain to 203.0.113.0
2024-06-06T21:43:42.393Z - info: Saving configuration info to disk
ghost 21:43:42.78 INFO  ==> Configuring Ghost URL to http://203.0.113.0
Disabling automatic domain update for IP address changes
```

步骤 4：登录到 Ghost 网站的管理控制面板

现在您已有默认应用程序密码，请完成以下程序，以导航到 Ghost 网站的主页，然后登录管理控制面板。登录后，您可以开始自定义网站并进行管理更改。有关您可以在 Ghost 中执行的操作的更多信息，请参阅本指南后面部分中的步骤 6：阅读 Ghost 文档并继续配置网站一节。

1. 在实例管理页面上的 Connect（连接）选项卡下，记下实例的公有 IP 地址。如果您之前将静态 IP 附加到您的实例，则这将是静态 IP 地址。公有 IP 地址也显示在实例管理页面的标题部分。



2. 浏览到实例的公有 IP 地址，例如，转到 `http://203.0.113.0`。

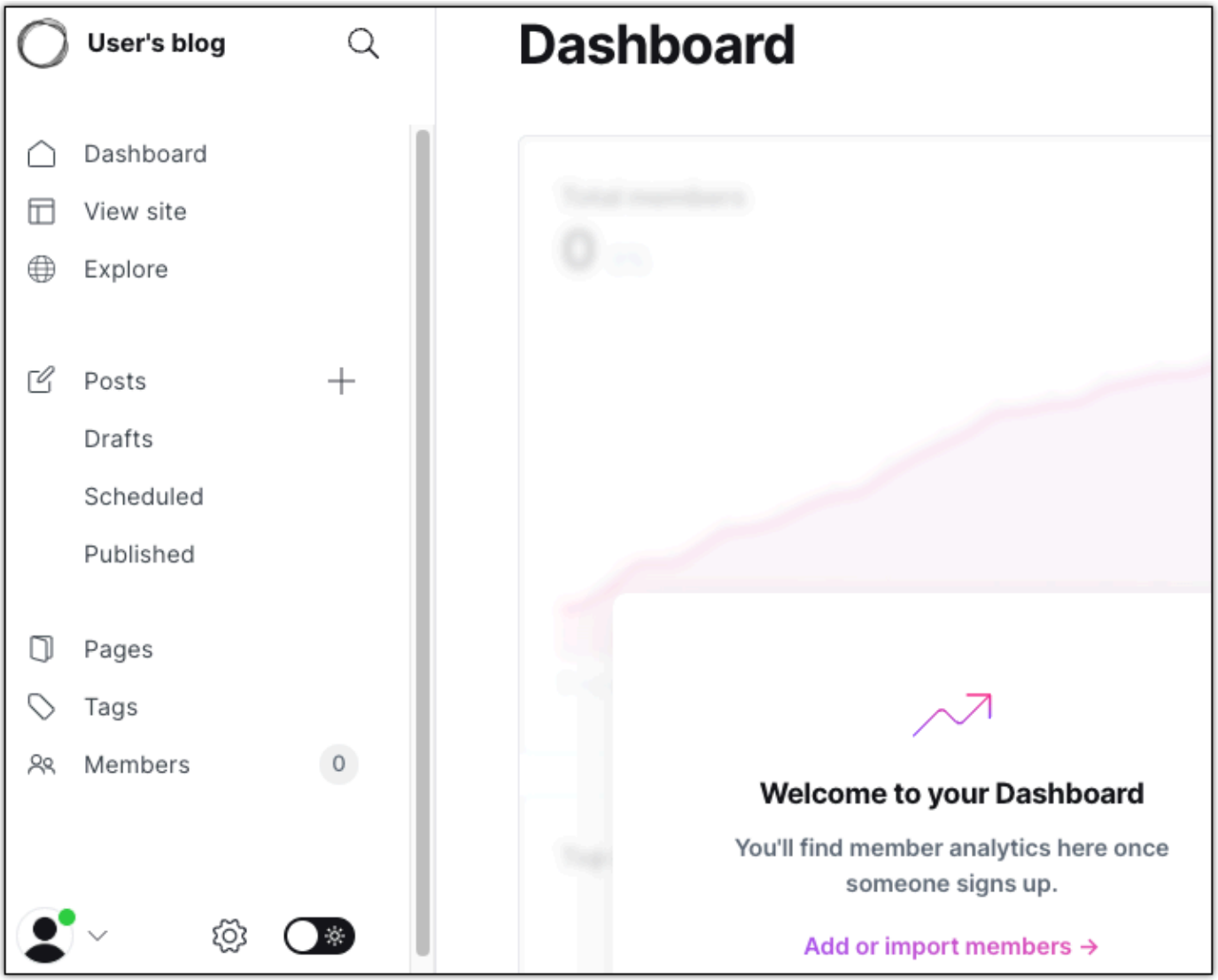
   应该会出现您的 Ghost 网站的主页。

3. 选择 Ghost 网站主页右下角的 Manage（管理）。

   如果 Manage（管理）横幅未显示，您可以通过浏览 `http://<PublicIP>/ghost` 到达登录页面。将 *<PublicIP>* 替换为实例的公有 IP 地址。

4. 使用之前在本指南中检索到的默认用户名（`user@example.com`）和默认密码登录。

将显示 Ghost 管理控制面板。



步骤 5：将注册域名的流量路由到 Ghost 网站

要将注册域名（如 `example.com`）的流量路由到 Ghost 网站，您需要向域的 DNS 添加一条记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 部分，选择创建 DNS 区域，然后按照页面上的说明进行操作。有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

在您的域名将流量路由到实例之后，您必须完成以下步骤才能让 Ghost 应用程序知道新域。

1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。

2. 连接后，请输入以下命令。*<DomainName>*替换为将流量引导到您的 Ghost 实例的域名。

```
$ sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

示例：

```
$ sudo /opt/bitnami/configure_app_domain --domain example.com
```

您应看到类似于以下示例的响应。Ghost 应用程序现在应该识别到了域。

```
bitnami@ip-203.0.113.0:~$ sudo /opt/bitnami/configure_app_domain --domain
 example.com
Configuring domain to example.com
2024-06-06T21:50:00.393Z - info: Saving configuration info to disk
ghost 21:50:25.78 INFO  ==> Configuring Ghost URL to http://example.com
Disabling automatic domain update for IP address changes
```

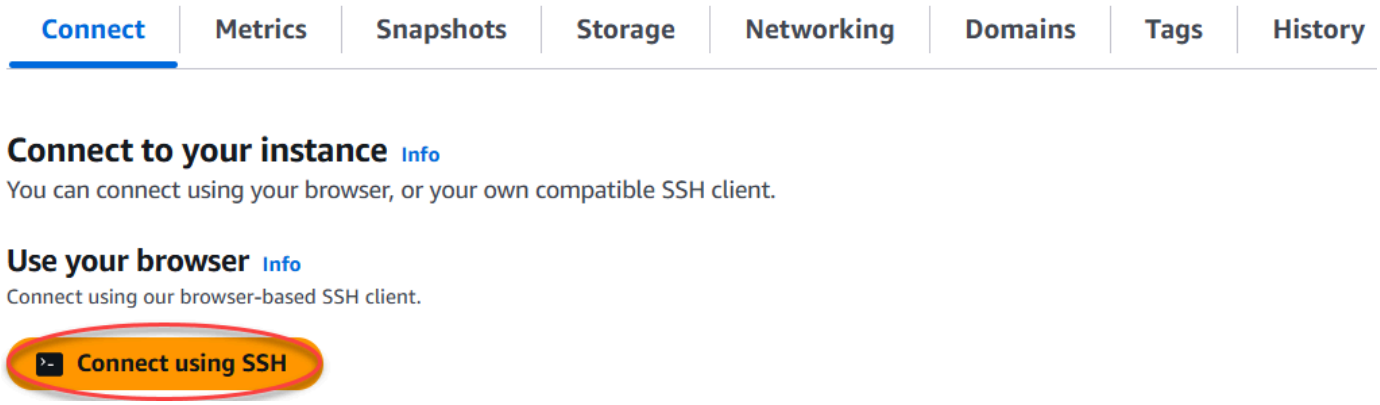
如果您浏览到为实例配置的域名，则应将您重定向到 Ghost 网站的主页。接下来，您应该生成并配置 SSL/TLS 证书，以启用 Ghost 网站的 HTTPS 连接。有关更多信息，请继续到本指南的下一节步骤 6：配置 Ghost 网站的 HTTPS。

步骤 6：配置 Ghost 网站的 HTTPS

完成以下程序以在 Ghost 网站上配置 HTTPS。这些步骤向您展示如何使用 Bitnami HTTPS 配置工具（`bncert-tool`），这是一个命令行工具，用于请求 Let's Encrypt SSL/TLS 证书。有关更多信息，请参阅 Bitnami 文档中的了解 Bitnami HTTPS 配置工具。

> **Important**
>
> 在开始此过程之前，请确保对域进行配置，以将流量路由到 Ghost 实例。否则，SSL/TLS 证书验证过程将失败。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，输入以下命令以确认 bncert 工具已安装在实例上。

```
sudo /opt/bitnami/bncert-tool
```

您应看到以下响应之一：

- 如果您在响应中看到命令未找到，则 bncert 工具未安装到实例上。继续执行此过程的后续步骤以在实例上安装 bncert 工具。
- 如果您在响应中看到欢迎使用 Bitnami HTTPS 配置工具，则 bncert 工具已安装到实例上。继续执行此过程的步骤 8。
- 如果 bncert 工具已在您的实例上安装了一段时间，那么您可能会看到一条消息，指示该工具的更新版本可供使用。选择进行下载，然后再次输入 `sudo /opt/bitnami/bncert-tool` 命令来运行 bncert 工具。继续执行此过程的步骤 8。

3. 输入以下命令以将 bncert 运行文件下载到您的实例中。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. 输入以下命令以在您的实例上创建 bncert 工具运行文件的目录。

```
sudo mkdir /opt/bitnami/bncert
```

5. 输入以下命令以创建可作为程序执行的 bncert 运行文件。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 输入以下命令以创建符号链接，该符号链接在您输入 sudo /opt/bitnami/bncert-tool 命令时运行 bncert 工具。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

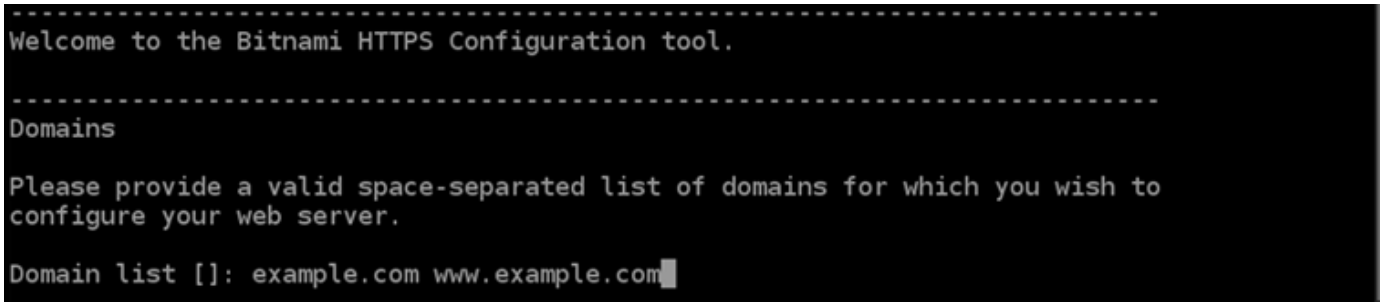
您现在已完成在实例上安装 bncert 工具的步骤。

7. 要运行 bncert 工具，请输入以下命令。

```
sudo /opt/bitnami/bncert-tool
```

8. 输入用空格分隔的主域名和备用域名，如以下示例所示。

如果您的域未配置为将流量路由到实例的公有 IP 地址，则 bncert 工具将要求您在继续之前进行该配置。您的域必须将流量路由到使用 bncert 工具以在实例上启用 HTTPS 的实例的公有 IP 地址。这将确认您拥有该域，并能用于进行证书的验证。



9. bncert 工具会询问您希望如何配置网站的重新导向。以下是可用的选项：

- 启用 HTTP 重新导向到 HTTPS - 指定是否将浏览网站 HTTP 版本（即 http://example.com）的用户自动重新导向到 HTTPS 版本（即 https://example.com)。我们建议启用此选项，因为它会强制所有访问者使用加密连接。输入 Y 然后按 Enter 以启用它。
- 启用非 www 重新导向到 www - 指定是否将浏览顶级域（即 https://example.com）的用户自动重新导向到域的 www 子域（即 https://www.example.com)。我们建议启用此选项。但如果您在搜索引擎工具（如 Google 站点管理员工具）中指定了顶级域作为首选网站地址，或者顶级域直接指向您的 IP 且 www 子域通过别名记录引用您的顶级域，则您可能希望禁用它并启用其他选项（启用 www 重新导向到非 www）。输入 Y 然后按 Enter 以启用它。
- 启用 www 到非 www 重新导向 - 指定是否将浏览域的 www 子域（即 https://www.example.com）的用户自动重新导向到顶级域（即 https://example.com)。如果您启用了非 www 重新导向到 www，建议禁用此选项。输入 N 然后按 Enter 以禁用它。

您的选择应类似于以下示例：

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

10. 将列出要进行的更改。输入 Y 然后按 Enter 以确认并继续。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. 输入要与 Let's Encrypt 证书关联的电子邮件地址，然后按 Enter（确定键）。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

12. 查看 Let's Encrypt 的加密用户协议 输入 Y 然后按 Enter 接受协议并继续。

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

将执行这些操作以在您的实例上启用 HTTPS，包括请求证书和配置您指定的重新导向。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

您的证书已成功颁发和验证，如果您看到类似于以下示例的消息，则表示在实例上成功配置了重新导向。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

bncert 工具将在证书过期前每 80 天执行一次自动续订。如果您希望将其他域和子域用于实例，并且希望为这些域启用 HTTPS，请重复上述步骤。

> **Tip**
>
> 输入以下命令以重新启动实例的服务。
>
> ```
> sudo /opt/bitnami/ctlscript.sh restart
> ```

您现在已完成在您的 Ghost 实例上启用 HTTPS。下次使用配置的域浏览到 Ghost 网站时，您应该会看到它重定向到 HTTPS 连接。

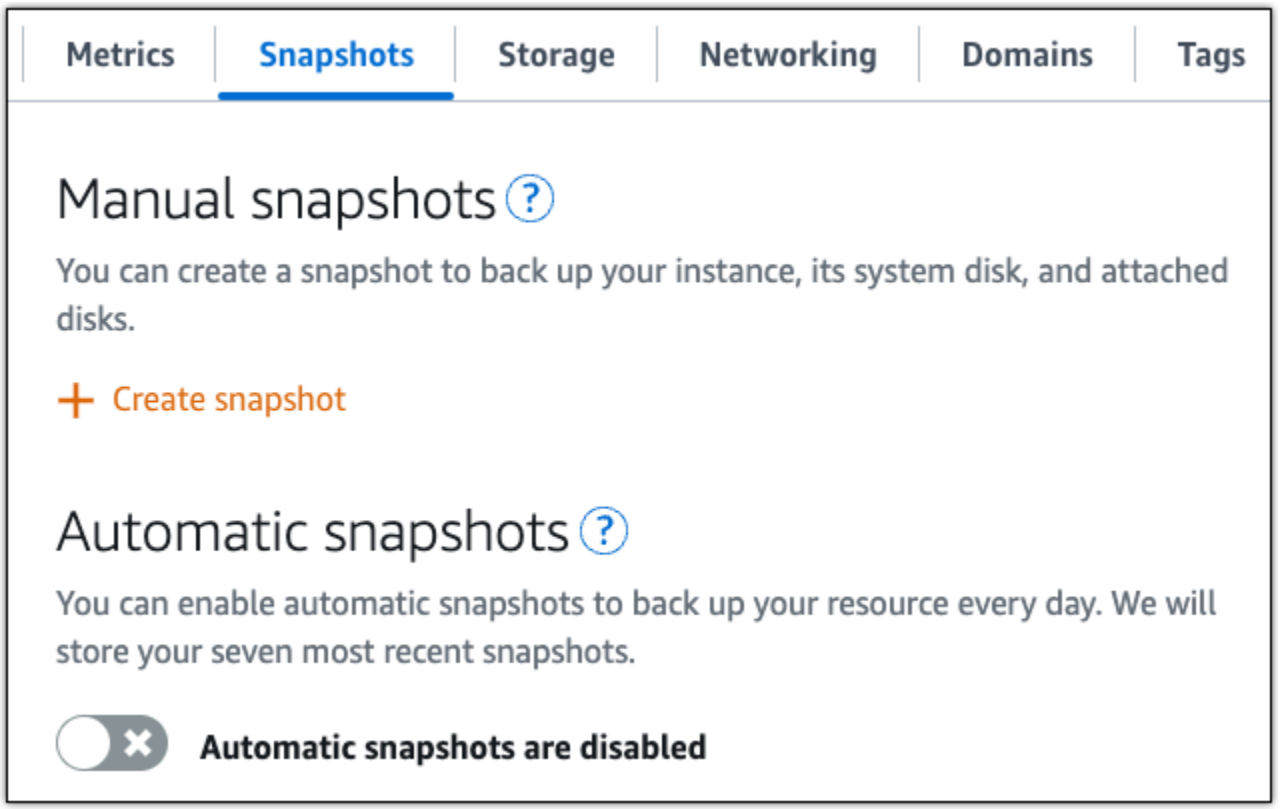
步骤 7：阅读 Ghost 文档并继续配置网站

阅读 Ghost 文档，了解如何管理和自定义网站。有关更多信息，请参阅 Ghost 文档。

步骤 8：创建实例的快照

按照您所需的方式配置 Ghost 网站后，创建实例的定期快照以进行备份。您可以手动创建快照，也可以启用自动快照，让 Lightsail 为您创建每日快照。如果实例出现错误，则可使用快照来创建新的替代实例。有关更多信息，请参阅快照。

在实例管理页面的快照选项卡下，选择创建快照或选择启用自动快照。



有关更多信息，请参阅在 Amazon Lightsail 中创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。

在 Lightsail 上设置和配置 GitLab CE 实例

在 GitLab CE 实例启动并在 Amazon Lightsail 上运行后，你应该采取以下几个步骤来开始使用：

内容

- 步骤 1：阅读 Bitnami 文档
- 步骤 2：获取访问 GitLab CE 管理区域的默认应用程序密码
- 步骤 3：将静态 IP 地址附加到实例
- 步骤 4：登录到 Gitlab CE 网站的管理区域
- 第 5 步：将您注册域名的流量路由到 GitLab CE 网站
- 第 6 步：为您的 GitLab CE 网站配置 HTTPS
- 第 7 步：阅读 GitLab CE 文档并继续配置您的网站
- 步骤 8：创建实例的快照

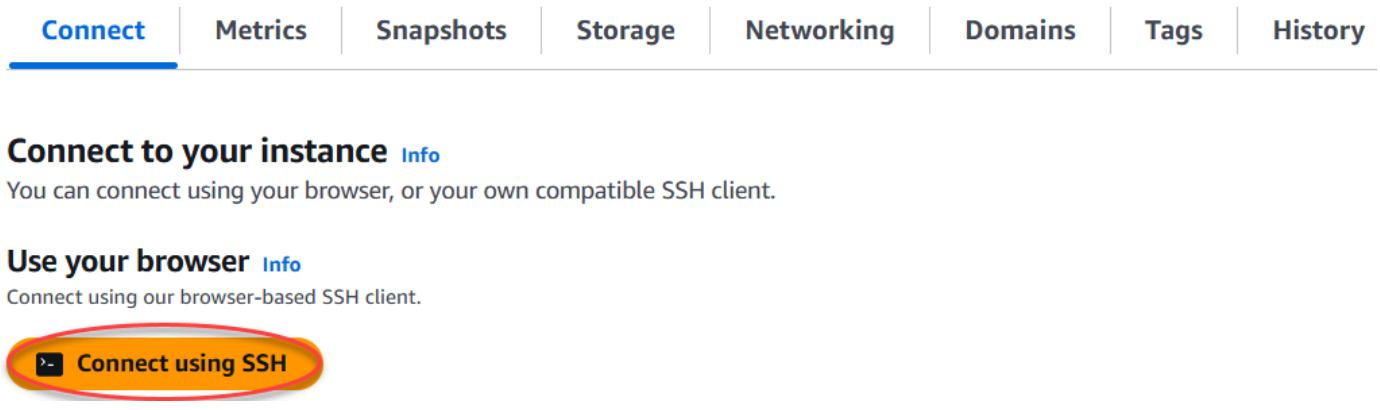
步骤 1：阅读 Bitnami 文档

阅读 Bitnami 文档，了解如何配置您的 GitLab CE 应用程序。有关更多信息，请参阅 Bitnami 打包的 GitLab CE For。 AWS Cloud

步骤 2：获取访问 GitLab CE 管理区域的默认应用程序密码

完成以下步骤以获取访问 GitLab CE 网站管理区域所需的默认应用程序密码。有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

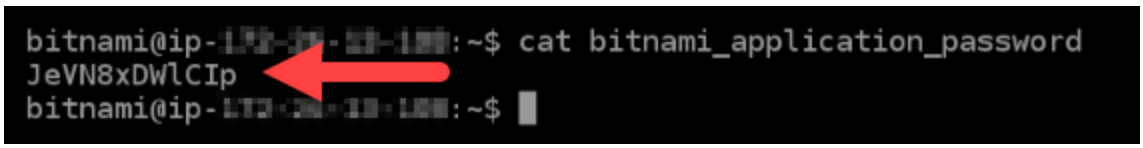
1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来获取应用程序密码：

```
cat $HOME/bitnami_application_password
```

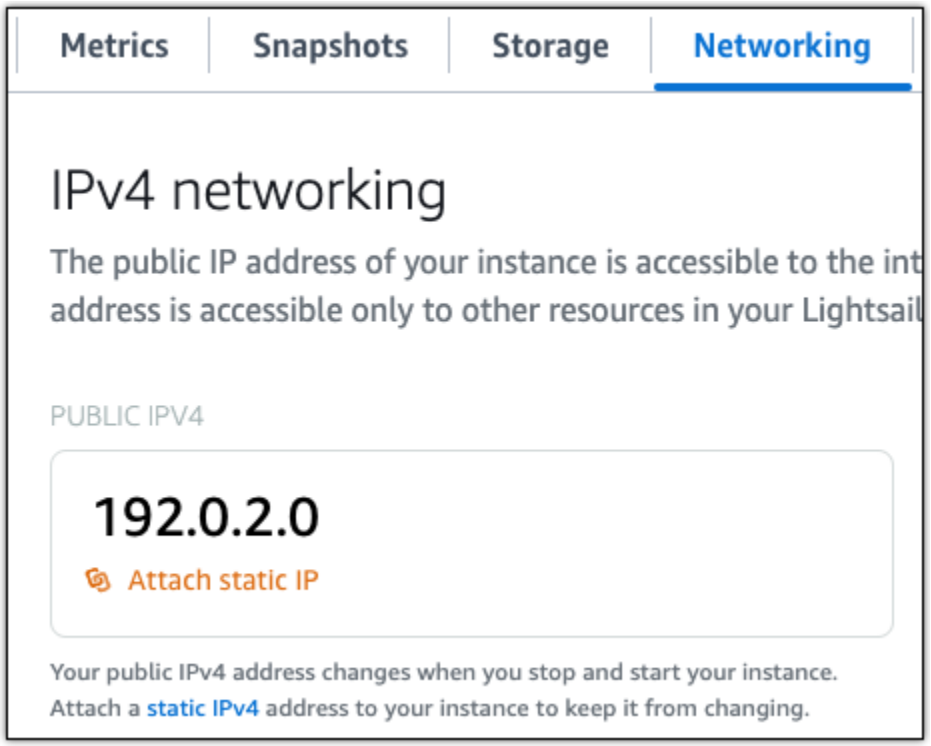
您应该会看到与以下示例类似的响应，其中包含默认应用程序密码：



步骤 3：将静态 IP 地址附加到实例

在您首次创建实例时分配给实例的公有 IP 地址会在您每次停止和启动实例时发生更改。您应为实例创建和附加静态 IP 地址，以确保其公有 IP 地址不变。之后当您将注册域名（如 `example.com`）指向实例时，无需在每次停止和重启实例时都更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择创建静态 IP或附加静态 IP（如果您之前创建了可附加到实例的静态 IP），然后按照页面上的说明操作。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

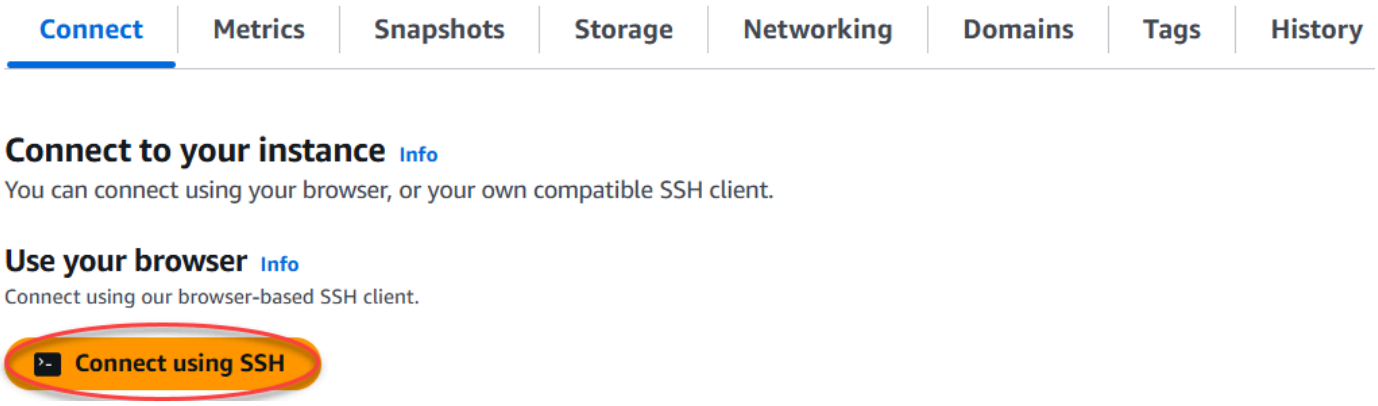


将新的静态 IP 地址附加到实例后，您必须完成以下步骤，以使应用程序知道新的静态 IP 地址。

1. 记下实例的静态 IP 地址。它列在实例管理页面的标题部分。



2. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



3. 连接后，请输入以下命令。*<StaticIP>*替换为您的实例的新静态 IP 地址。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您应看到类似于以下示例的响应。现在，实例上的应用程序应该识别到了新的静态 IP 地址。

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2022-06-09T16:47:06.737Z - info: Saving configuration info to disk
gitlab 16:47:06.86 INFO  ==> Updating external URL in GitLab configuration
gitlab 16:47:06.88 INFO  ==> Reconfiguring GitLab
gitlab 16:47:45.29 INFO  ==> Starting GitLab services
Disabling automatic domain update for IP address changes
```

步骤 4：登录到 Gitlab CE 网站的管理区域

现在您已经有了默认的用户密码，请导航到您的 GitLab CE 网站的主页并登录到管理区域。登录后，您可以开始自定义网站并进行管理更改。有关在 GitLab CE 中可以做什么的更多信息，请参阅本指南后面的 “步骤 7：阅读 GitLab CE 文档并继续配置您的网站” 部分。

1. 在实例管理页面上的 Connect（连接）选项卡下，记下实例的公有 IP 地址。公有 IP 地址也显示在实例管理页面的标题部分。

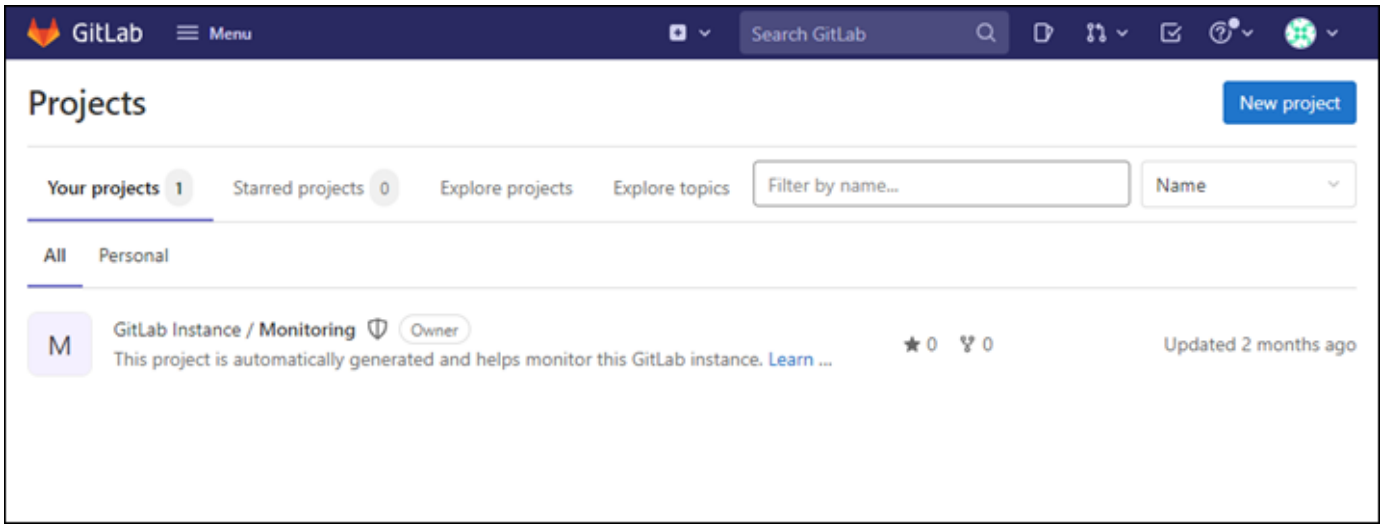


2. 浏览到实例的公有 IP 地址，例如，转到 `http://203.0.113.0`。

   应该会出现您的 Gitlab CE 网站的主页。您可能还会看到一个浏览器警告，指出您的连接不是私有的、不是安全的或存在安全风险。发生这种情况是因为您的 GitLab CE 实例尚未应用 SSL/TLS 证书。在浏览器窗口中，选择高级、详细信息或更多信息以查看可用的选项。然后选择继续连接该网站，即使它不是私有或安全的。

3. 使用之前在本指南中检索到的默认用户名（`root`）和默认密码登录。

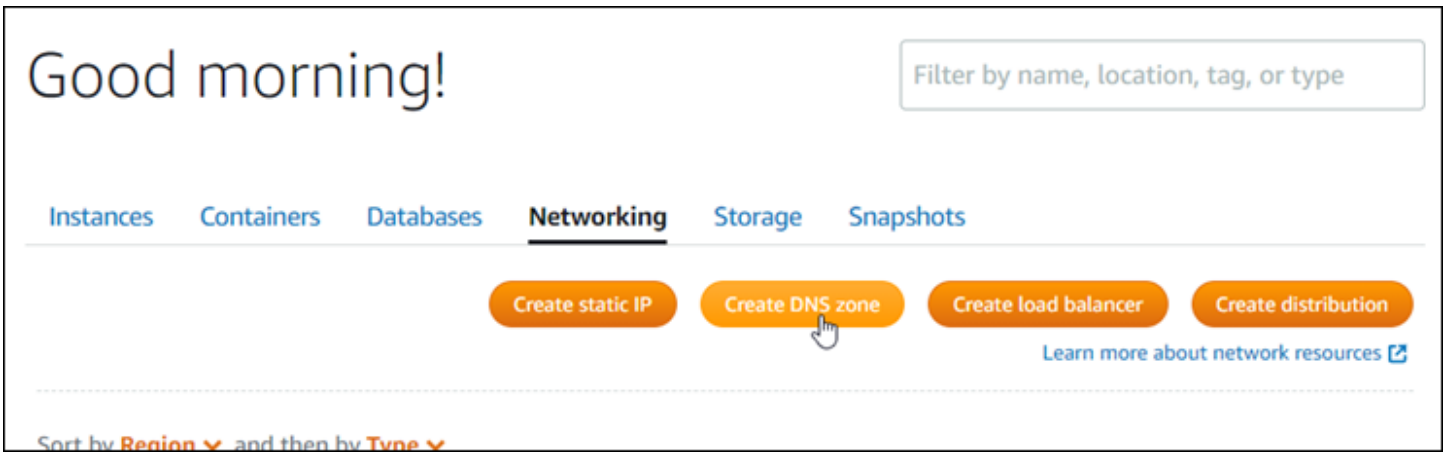
   此时将显示 Gitlab CE 管理控制面板。



第 5 步：将您注册域名的流量路由到 GitLab CE 网站

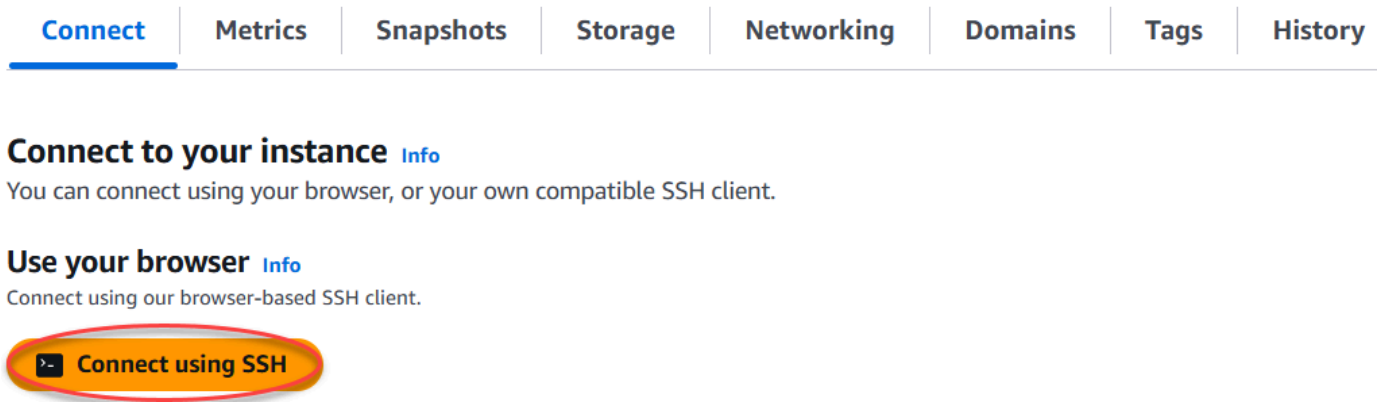
要将您的注册域名的流量（例如`example.com`路由到您的 GitLab CE 网站），您需要在域名的域名系统 (DNS) 中添加一条记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “网络” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。



在您的域名将流量路由到您的实例后，您必须完成以下步骤以让 GitLab CE 知道该域名。

1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令。*<DomainName>*替换为将流量路由到您的实例的域名。

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

您应看到类似于以下示例的响应。您的 GitLab CE 实例现在应该知道域名了。

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain example.com
Configuring domain to example.com
2022-06-09T18:44:00.235Z - info: Saving configuration info to disk
gitlab 18:44:00.36 INFO  ==> Updating external URL in GitLab configuration
gitlab 18:44:00.37 INFO  ==> Reconfiguring GitLab
gitlab 18:44:38.79 INFO  ==> Starting GitLab services
Disabling automatic domain update for IP address changes
```

如果该命令失败，则您可能使用的是旧版本的 GitLab CE 实例。尝试运行以下命令。*<DomainName>*替换为将流量路由到您的实例的域名。

```
cd /opt/bitnami/apps/gitlab
sudo ./bnconfig --machine_hostname <DomainName>
```

运行这些命令后，输入以下命令，以防止 bnconfig 工具在服务器每次重启时自动运行。

```
sudo mv bnconfig bnconfig.disabled
```

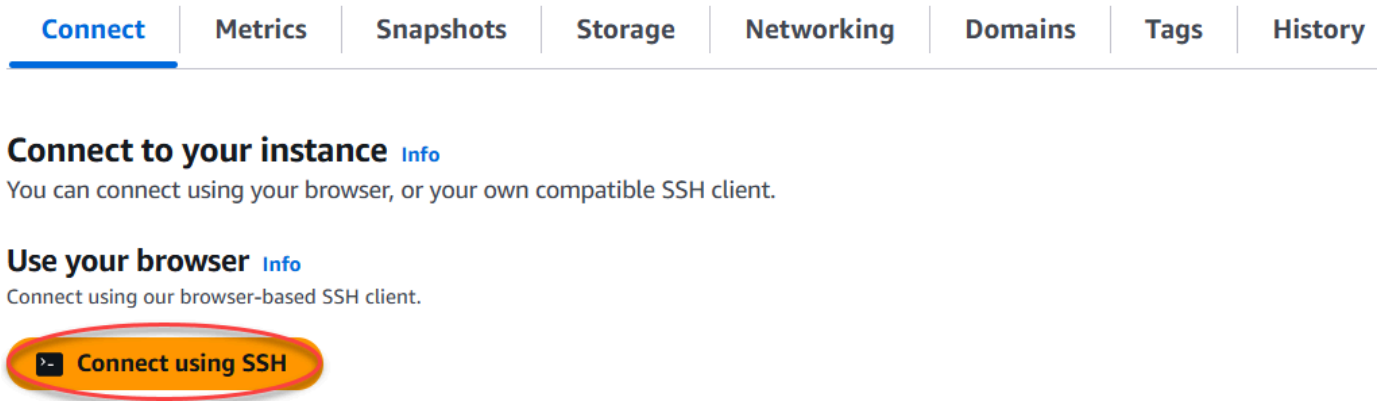
接下来，您应该生成并配置 SSL/TLS 证书，以便为 CE 网站启用 HTTPS 连接。 GitLab 有关更多信息，请继续阅读本指南的下一个步骤 6：为您的 GitLab CE 网站配置 HTTPS 部分。

第 6 步：为您的 GitLab CE 网站配置 HTTPS

完成以下步骤，在您的 GitLab CE 网站上配置 HTTPS。这些步骤向您展示如何使用 Lego 客户端，这是一个命令行工具，用于请求 Let's Encrypt SSL/TLS 证书。

> **Important**
>
> 在开始此过程之前，请确保已将域配置为将流量路由到您的 GitLab CE 实例。否则，SSL/TLS 证书验证过程将失败。要路由注册域名的流量，您需要向域的 DNS 添加一条记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。
>
> 在 Lightsail 控制台主页的 “域名和 DNS” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令以将目录更改为临时（/tmp）目录。

```
cd /tmp
```

3. 输入以下命令，下载 Lego 客户端的最新版本。此命令将下载磁带存档（tar）文件。

```
curl -Ls https://api.github.com/repos/xenolf/lego/releases/latest | grep
 browser_download_url | grep linux_amd64 | cut -d '"' -f 4 | wget -i -
```

4. 输入以下命令以从 tar 文件中提取文件。*X.Y.Z*替换为您下载的 Lego 客户端版本。

```
tar xf lego_vX.Y.Z_linux_amd64.tar.gz
```

示例：

```
tar xf lego_v4.7.0_linux_amd64.tar.gz
```

5. 输入以下命令以创建您会将 Lego 客户端文件移动到的 `/opt/bitnami/letsencrypt` 目录。

```
sudo mkdir -p /opt/bitnami/letsencrypt
```

6. 输入以下命令以将 Lego 客户端文件移动到的您创建的目录中。

```
sudo mv lego /opt/bitnami/letsencrypt/lego
```

7. 逐个输入以下命令以停止在您的实例上运行的应用程序服务。

```
sudo service bitnami stop
sudo service gitlab-runsvdir stop
```

8. 输入以下命令以使用 Lego 客户端请求 Let's Encrypt SSL/TLS 证书。

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="EmailAddress" --
domains="RootDomain" --domains="WwwSubDomain" --path="/opt/bitnami/letsencrypt" run
```

在该命令中，将以下示例值替换为自己的值：

- *EmailAddress* – 用于注册通知的电子邮件地址。
- *RootDomain*— 将流量路由到您的 GitLab CE 网站的主根域（例如，example.com）。
- *WwwSubDomain*— 将流量路由到您的 GitLab CE 网站的主根域的www子域（例如，www.example.com）。

  您可以通过在命令中指定其他 --domains 参数来为证书指定多个域。当您指定多个域时，Lego 会创建一个使用者替代名称（SAN）证书，这会导致只有一个证书对您指定的所有域有效。列表中的第一个域将添加为证书的 “CommonName”，其余域将作为 “DNSNames” 添加到证书内的 SAN 扩展中。

示例：

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="user@example.com" --
domains="example.com" --domains="www.example.com" --path="/opt/bitnami/letsencrypt"
 run
```

9. 在提示时，按下 Y 和 Enter 以接受服务条款。

   您应看到类似于以下示例的响应。

   ```
   2022/06/09 19:23:27 [INFO] [ example.com ] Server responded with a certificate.
   ```

   如果成功，一组证书将会保存到 /opt/bitnami/letsencrypt/certificates 目录。该组证书包括服务器证书文件（例如，example.com.crt）和服务器证书密钥文件（例如，example.com.key）。

10. 逐个输入以下命令以重命名实例上的现有证书。稍后，您将用新的 Let's Encrypt 证书替换这些现有证书。

    ```
    sudo mv /etc/gitlab/ssl/server.crt /etc/gitlab/ssl/server.crt.old
    sudo mv /etc/gitlab/ssl/server.key /etc/gitlab/ssl/server.key.old
    sudo mv /etc/gitlab/ssl/server.csr /etc/gitlab/ssl/server.csr.old
    ```

11. 逐一输入以下命令，在目录中为新 Let's Encript 证书创建符号链接，该`/etc/gitlab/ssl`目录是 GitLab CE 实例上的默认证书目录。

```
sudo ln -sf /opt/bitnami/letsencrypt/certificates/Domain.key /etc/gitlab/ssl/
server.key
sudo ln -sf /opt/bitnami/letsencrypt/certificates/Domain.crt /etc/gitlab/ssl/
server.crt
```

在命令中，*Domain*替换为您在申请 Let's Encrypt 证书时指定的主根域。

示例：

```
sudo ln -sf /opt/bitnami/letsencrypt/certificates/example.com.key /etc/gitlab/ssl/
server.key
sudo ln -sf /opt/bitnami/letsencrypt/certificates/example.com.crt /etc/gitlab/ssl/
server.crt
```

12. 逐个输入以下命令，以在您将其移动到的目录中更改新的 Let's Encrypt 证书的权限。

```
sudo chown root:root /etc/gitlab/ssl/server*
sudo chmod 600 /etc/gitlab/ssl/server*
```

13. 输入以下命令以在您的 GitLab CE 实例上重新启动应用程序服务。

```
sudo service bitnami start
```

下次使用您配置的域名浏览您的 GitLab CE 网站时，您应该会看到它重定向到 HTTPS 连接。请注意，GitLab CE 实例最多可能需要一个小时才能识别新证书。如果您的 GitLab CE 网站拒绝您的连接，请停止并启动实例，然后重试。

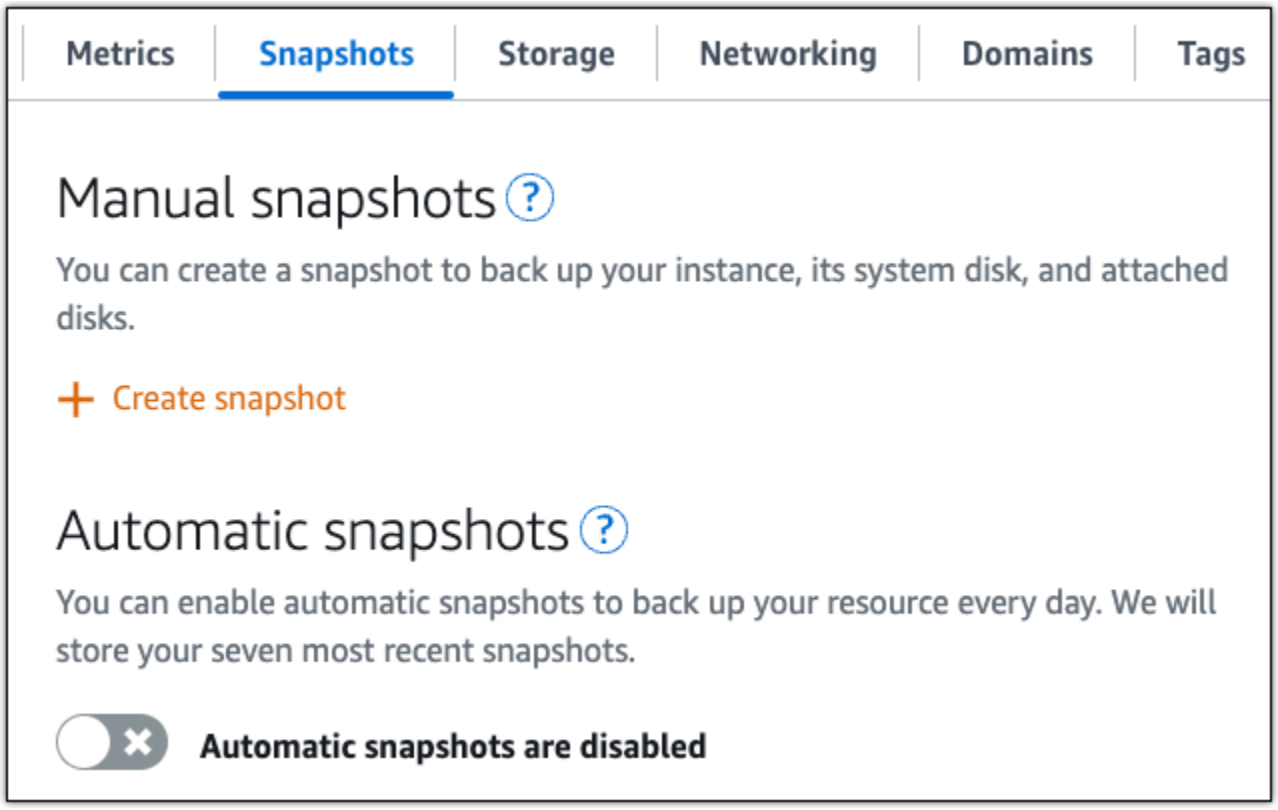
第 7 步：阅读 GitLab CE 文档并继续配置您的网站

阅读 C GitLab E 文档，了解如何管理和自定义您的网站。有关更多信息，请参阅 GitLab 文档。

步骤 8：创建实例的快照

按照您想要的方式配置 GitLab CE 网站后，创建实例的定期快照以对其进行备份。您可以手动创建快照，也可以启用自动快照，让 Lightsail 为您创建每日快照。如果实例出现错误，则可使用快照来创建新的替代实例。有关更多信息，请参阅快照。

在实例管理页面的快照选项卡下，选择创建快照或选择启用自动快照。



有关更多信息，请参阅在 Amazon Lightsail 中创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。

开始使用 Joomla 吧！ 在 Lightsail 上

在使用 Joomla 之后，你应该采取以下几个步骤来开始使用！ 实例已在 Amazon Lightsail 上启动并运行：

内容

- 步骤 1：阅读 Bitnami 文档
- 步骤 2：获取默认应用程序密码以访问 Joomla! 控制面板
- 步骤 3：将静态 IP 地址附加到实例
- 步骤 4：登录到 Joomla! 网站的控制面板
- 步骤 5：将注册域名的流量路由到 Joomla! 网站
- 步骤 6：配置 Joomla! 网站的 HTTPS
- 步骤 7：阅读 Joomla! 文档并继续配置网站
- 步骤 8：创建实例的快照

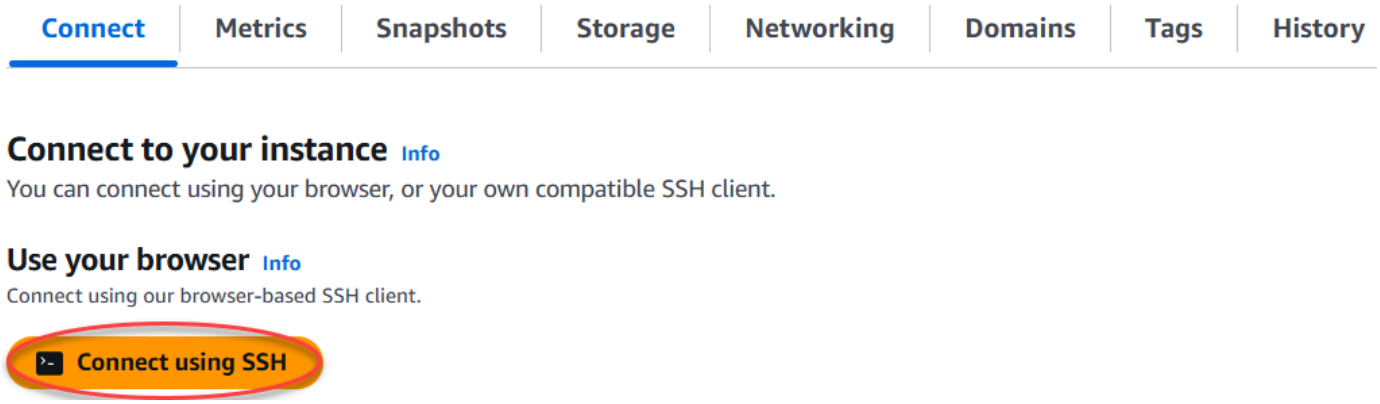
步骤 1：阅读 Bitnami 文档

阅读 Bitnami 文档以了解如何配置 Joomla! 应用程序。有关更多信息，请参阅 Joomla! 由 Bitnami 打包为。 AWS Cloud

步骤 2：获取默认应用程序密码以访问 Joomla! 控制面板

完成以下程序以获取访问 Joomla! 网站的控制面板所需的默认应用程序密码。有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

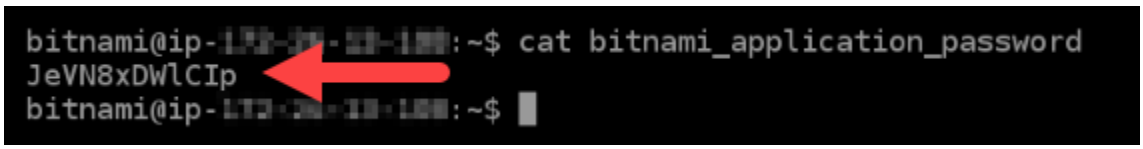
1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来获取应用程序密码：

```
cat $HOME/bitnami_application_password
```

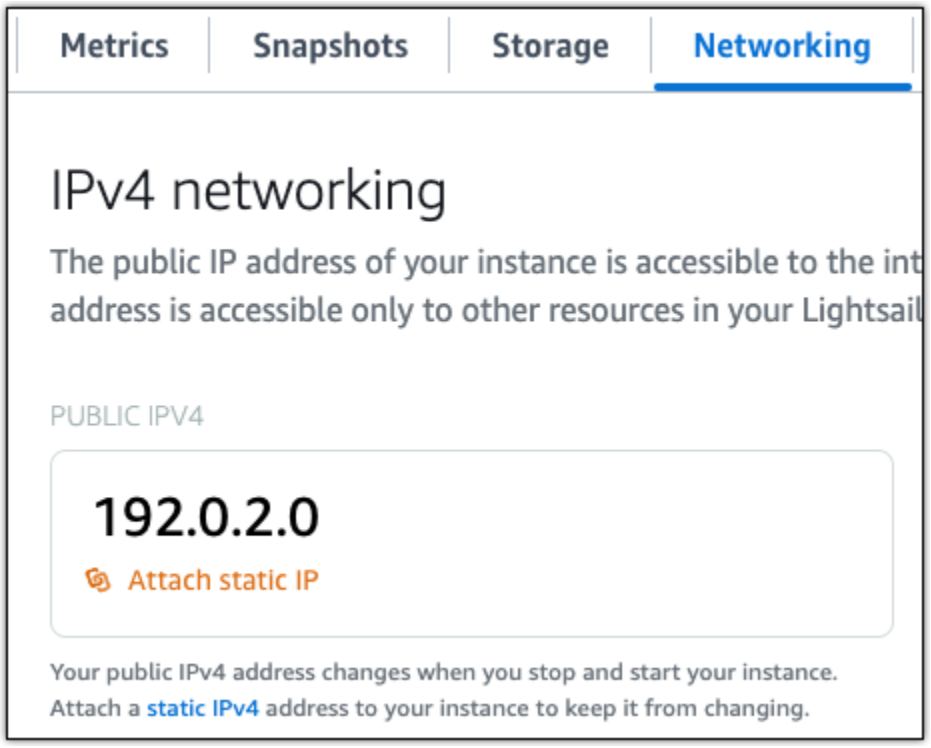
您应该会看到与以下示例类似的响应，其中包含默认应用程序密码：



步骤 3：将静态 IP 地址附加到实例

在您首次创建实例时分配给实例的公有 IP 地址会在您每次停止和启动实例时发生更改。您应为实例创建和附加静态 IP 地址，以确保其公有 IP 地址不变。之后当您将注册域名（如 `example.com`）指向实例时，无需在每次停止和重启实例时都更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择创建静态 IP或附加静态 IP（如果您之前创建了可附加到实例的静态 IP），然后按照页面上的说明操作。有关更多信息，请参阅创建静态 IP 并将其附加到实例。



步骤 4：登录到 Joomla! 网站的控制面板

现在您已有默认应用程序密码，请完成以下程序，以导航到 Joomla! 网站的主页，然后登录控制面板。登录后，您可以开始自定义网站并进行管理更改。有关您可以在 Joomla! 中执行的操作的更多信息，请参阅本指南后面部分中的步骤 7：阅读 Joomla! 文档并继续配置网站一节。

1. 在实例管理页面上的 Connect（连接）选项卡下，记下实例的公有 IP 地址。公有 IP 地址也显示在实例管理页面的标题部分。

2. 浏览到实例的公有 IP 地址，例如，转到 `http://203.0.113.0`。

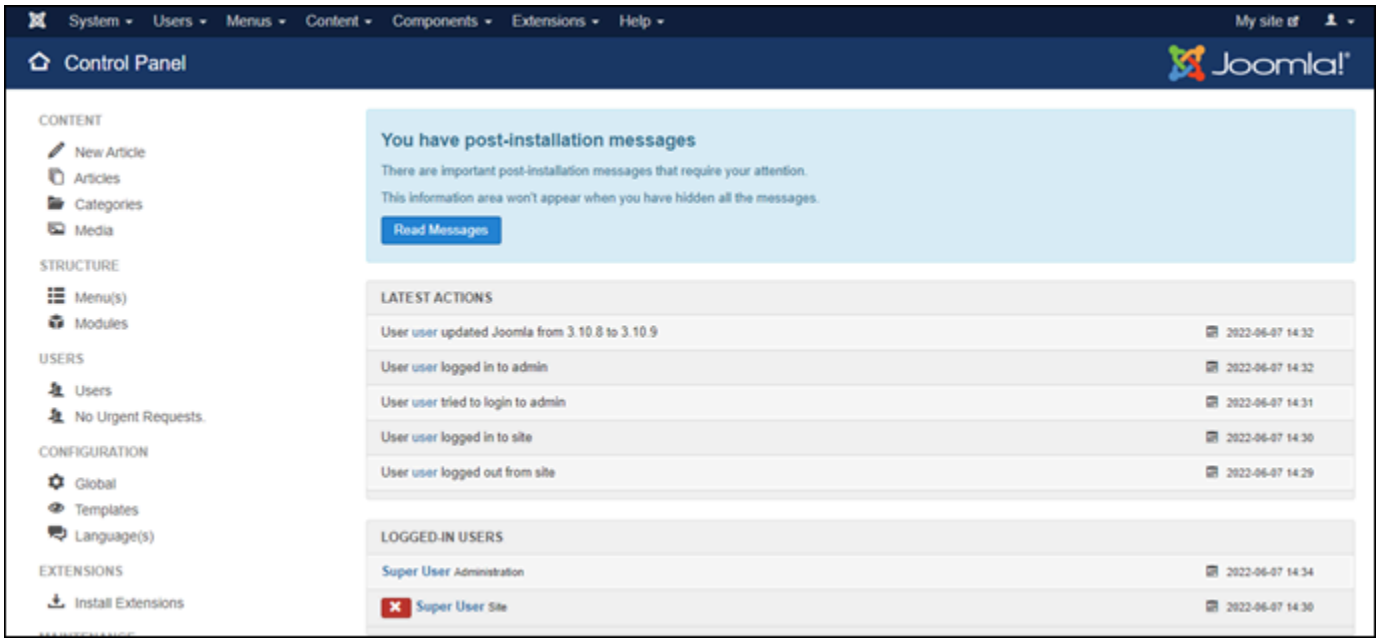
   应该会出现您的 Joomla! 网站的主页。

3. 选择 Joomla! 网站主页右下角的 Manage（管理）。

   如果 Manage（管理）横幅未显示，您可以通过浏览 `http://<PublicIP>/administrator/` 到达登录页面。将 *<PublicIP>* 替换为实例的公有 IP 地址。

4. 使用之前在本指南中检索到的默认用户名（`user`）和默认密码登录。

将显示 Joomla! 管理控制面板。



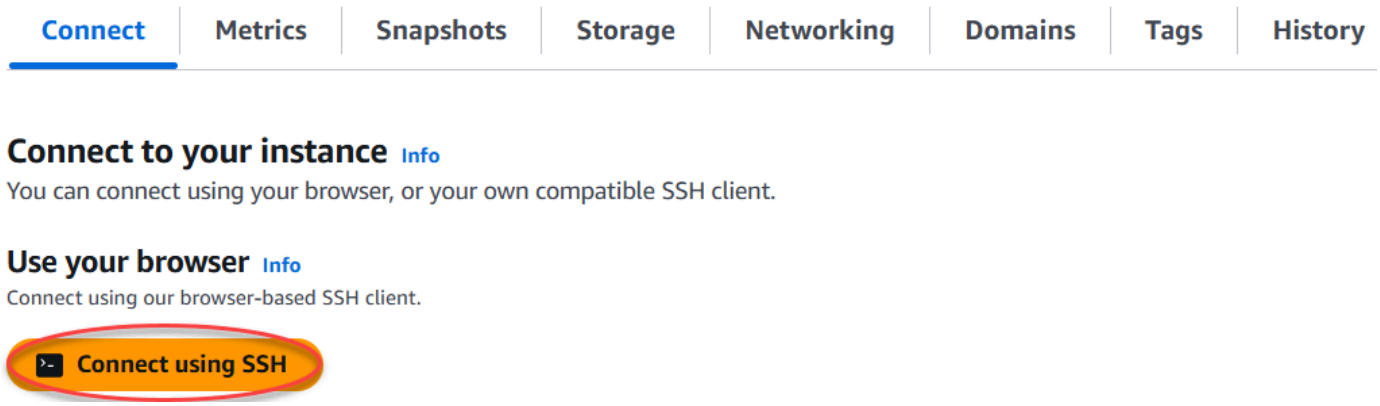
步骤 5：将注册域名的流量路由到 Joomla! 网站

要将注册域名（如 `example.com`）的流量路由到 Joomla! 网站，您需要向域的域名系统（DNS）添加一条记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

在您的域名将流量路由到实例之后，您必须完成以下步骤才能让 Joomla! 软件知道域名。

1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



2. Bitnami 正在修改许多蓝图的文件结构。本程序中的文件路径可能会发生变化，具体取决于您的 Bitnami 蓝图是使用本地 Linux 系统包（方法 A），还是自包含安装（方法 B）。要确定 Bitnami 安装类型以及要遵循的方法，请在连接后运行以下命令：

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system
 packages." || echo "Approach B: Self-contained installation."
```

3. 如果上一个命令的结果表明您应该使用方法 A，请完成以下步骤。否则，如果上一个命令的结果表明您应该使用方法 B，请继续执行步骤 4。

   1. 输入以下命令以使用 Vim 打开 Apache 虚拟主机配置文件，并为您的域名创建虚拟主机。

      ```
      sudo vim /opt/bitnami/apache2/conf/vhosts/joomla-vhost.conf
      ```

   2. 按 I 进入 Vim 的插入模式。

   3. 将域名添加到文件，如以下示例所示。在此示例中，我们使用的是 `example.com` 和 `www.example.com` 域。

      ```
      <VirtualHost 127.0.0.1:80 _default_:80>
        ServerName www.example.com
        ServerAlias example.com
        DocumentRoot /opt/bitnami/joomla
        <Directory "/opt/bitnami/joomla">
          Options -Indexes +FollowSymLinks -MultiViews
          AllowOverride None
          Require all granted
        </Directory>
        Include "/opt/bitnami/apache/conf/vhosts/htaccess/joomla-htaccess.conf"
      </VirtualHost>
      ```

   4. 按 ESC 键，然后输入 `:wq!` 以保存您的编辑（写入），然后退出 Vim。

   5. 输入以下命令以重新启动 Apache 服务器。

      ```
      sudo /opt/bitnami/ctlscript.sh restart apache
      ```

4. 如果上一个命令的结果表明您应该使用方法 B，请完成以下步骤。

   1. 输入以下命令以使用 Vim 打开 Apache 虚拟主机配置文件，并为您的域名创建虚拟主机。

      ```
      sudo vim /opt/bitnami/apps/joomla/conf/httpd-vhosts.conf
      ```

   2. 按 I 进入 Vim 的插入模式。

3. 将域名添加到文件，如以下示例所示。在此示例中，我们使用的是 example.com 和 www.example.com 域。



4. 按 ESC 键，然后输入 :wq! 以保存您的编辑（写入），然后退出 Vim。
5. 输入以下命令以确认 bitnami-apps-vhosts.conf 文件包含 Joomla! 的 httpd-vhosts.conf 文件。

```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami-apps-vhosts.conf
```

在文件中查找以下行。如果缺少，请将其添加。

```
Include "/opt/bitnami/apps/joomla/conf/httpd-vhosts.conf"
```

6. 输入以下命令以重新启动 Apache 服务器。

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

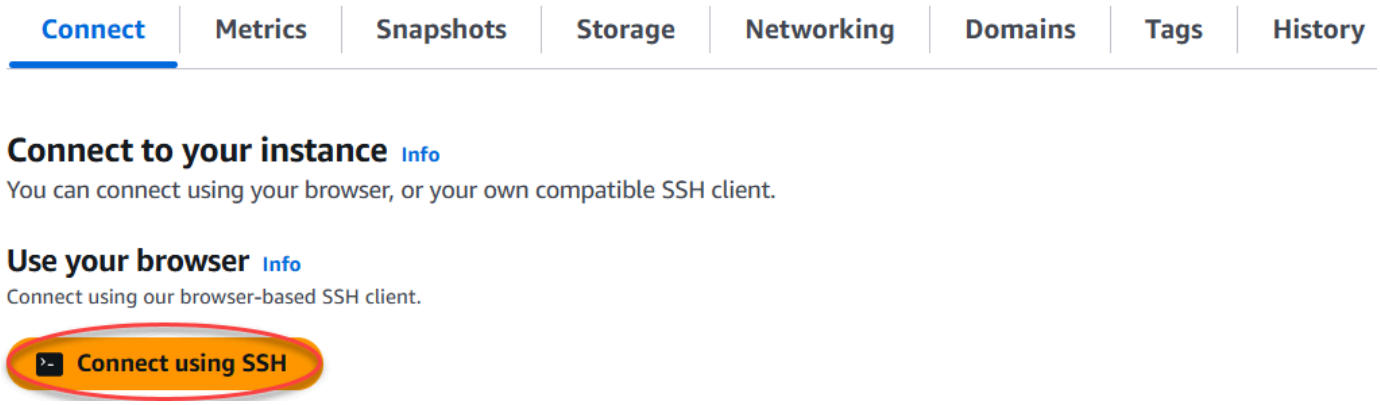
如果您浏览到为实例配置的域名，则应将您重定向到 Joomla! 网站的主页。接下来，您应该生成并配置 SSL/TLS 证书，以启用 Joomla! 网站的 HTTPS 连接。有关更多信息，请继续到本指南的下一节步骤 6：配置 Joomla! 网站的 HTTPS。

步骤 6：配置 Joomla! 网站的 HTTPS

完成以下程序以在 Joomla! 网站上配置 HTTPS。这些步骤向您展示如何使用 Bitnami HTTPS 配置工具（bncert-tool），这是一个命令行工具，用于请求 Let's Encrypt SSL/TLS 证书。有关更多信息，请参阅 Bitnami 文档中的了解 Bitnami HTTPS 配置工具。

> **Important**
>
> 在开始此过程之前，请确保对域进行配置，以将流量路由到 Joomla! 实例。否则，SSL/TLS 证书验证过程将失败。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，输入以下命令以确认 bncert 工具已安装在实例上。

```
sudo /opt/bitnami/bncert-tool
```

您应看到以下响应之一：

- 如果您在响应中看到命令未找到，则 bncert 工具未安装到实例上。继续执行此过程的后续步骤以在实例上安装 bncert 工具。
- 如果您在响应中看到欢迎使用 Bitnami HTTPS 配置工具，则 bncert 工具已安装到实例上。继续执行此过程的步骤 8。
- 如果 bncert 工具已在您的实例上安装了一段时间，那么您可能会看到一条消息，指示该工具的更新版本可供使用。选择进行下载，然后再次输入 `sudo /opt/bitnami/bncert-tool` 命令来运行 bncert 工具。继续执行此过程的步骤 8。

3. 输入以下命令以将 bncert 运行文件下载到您的实例中。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. 输入以下命令以在您的实例上创建 bncert 工具运行文件的目录。

```
sudo mkdir /opt/bitnami/bncert
```

5. 输入以下命令以创建可作为程序执行的 bncert 运行文件。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 输入以下命令以创建符号链接，该符号链接在您输入 sudo /opt/bitnami/bncert-tool 命令时运行 bncert 工具。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

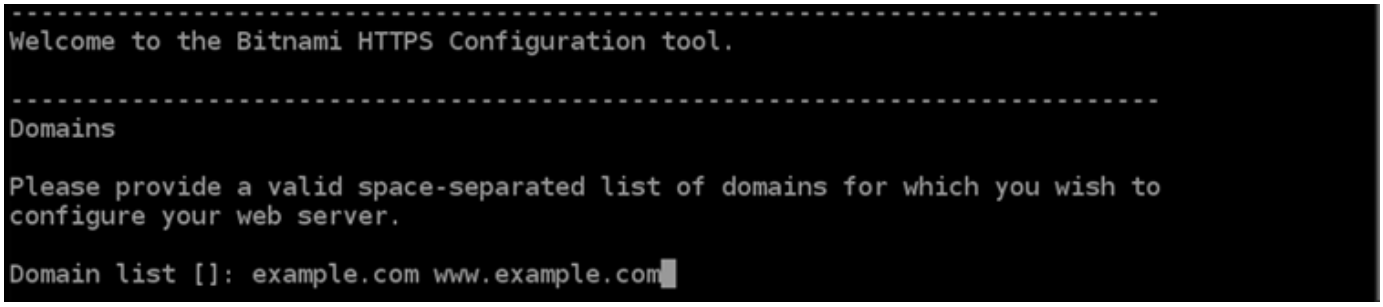
您现在已完成在实例上安装 bncert 工具的步骤。

7. 要运行 bncert 工具，请输入以下命令。

```
sudo /opt/bitnami/bncert-tool
```

8. 输入用空格分隔的主域名和备用域名，如以下示例所示。

如果您的域未配置为将流量路由到实例的公有 IP 地址，则 bncert 工具将要求您在继续之前进行该配置。您的域必须将流量路由到使用 bncert 工具以在实例上启用 HTTPS 的实例的公有 IP 地址。这将确认您拥有该域，并能用于进行证书的验证。



9. bncert 工具会询问您希望如何配置网站的重新导向。以下是可用的选项：

- 启用 HTTP 重新导向到 HTTPS - 指定是否将浏览网站 HTTP 版本（即 http://example.com）的用户自动重新导向到 HTTPS 版本（即 https://example.com)。我们建议启用此选项，因为它会强制所有访问者使用加密连接。输入 Y 然后按 Enter 以启用它。
- 启用非 www 重新导向到 www - 指定是否将浏览顶级域（即 https://example.com）的用户自动重新导向到域的 www 子域（即 https://www.example.com)。我们建议启用此选项。但如果您在搜索引擎工具（如 Google 站点管理员工具）中指定了顶级域作为首选网站地址，或者顶级域直接指向您的 IP 且 www 子域通过别名记录引用您的顶级域，则您可能希望禁用它并启用其他选项（启用 www 重新导向到非 www）。输入 Y 然后按 Enter 以启用它。
- 启用 www 到非 www 重新导向 - 指定是否将浏览域的 www 子域（即 https://www.example.com）的用户自动重新导向到顶级域（即 https://example.com)。如果您启用了非 www 重新导向到 www，建议禁用此选项。输入 N 然后按 Enter 以禁用它。

您的选择应类似于以下示例：

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

10. 将列出要进行的更改。输入 Y 然后按 Enter 以确认并继续。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. 输入要与 Let's Encrypt 证书关联的电子邮件地址，然后按 Enter（确定键）。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

12. 查看 Let's Encrypt 的加密用户协议 输入 Y 然后按 Enter 接受协议并继续。

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

将执行这些操作以在您的实例上启用 HTTPS，包括请求证书和配置您指定的重新导向。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

您的证书已成功颁发和验证，如果您看到类似于以下示例的消息，则表示在实例上成功配置了重新导向。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

`bncert` 工具将在证书过期前每 80 天执行一次自动续订。如果您希望将其他域和子域用于实例，并且希望为这些域启用 HTTPS，请重复上述步骤。

您现在已完成在您的 Joomla! 实例上启用 HTTPS。下次使用配置的域浏览到 Joomla! 网站时，您应该会看到它重定向到 HTTPS 连接。

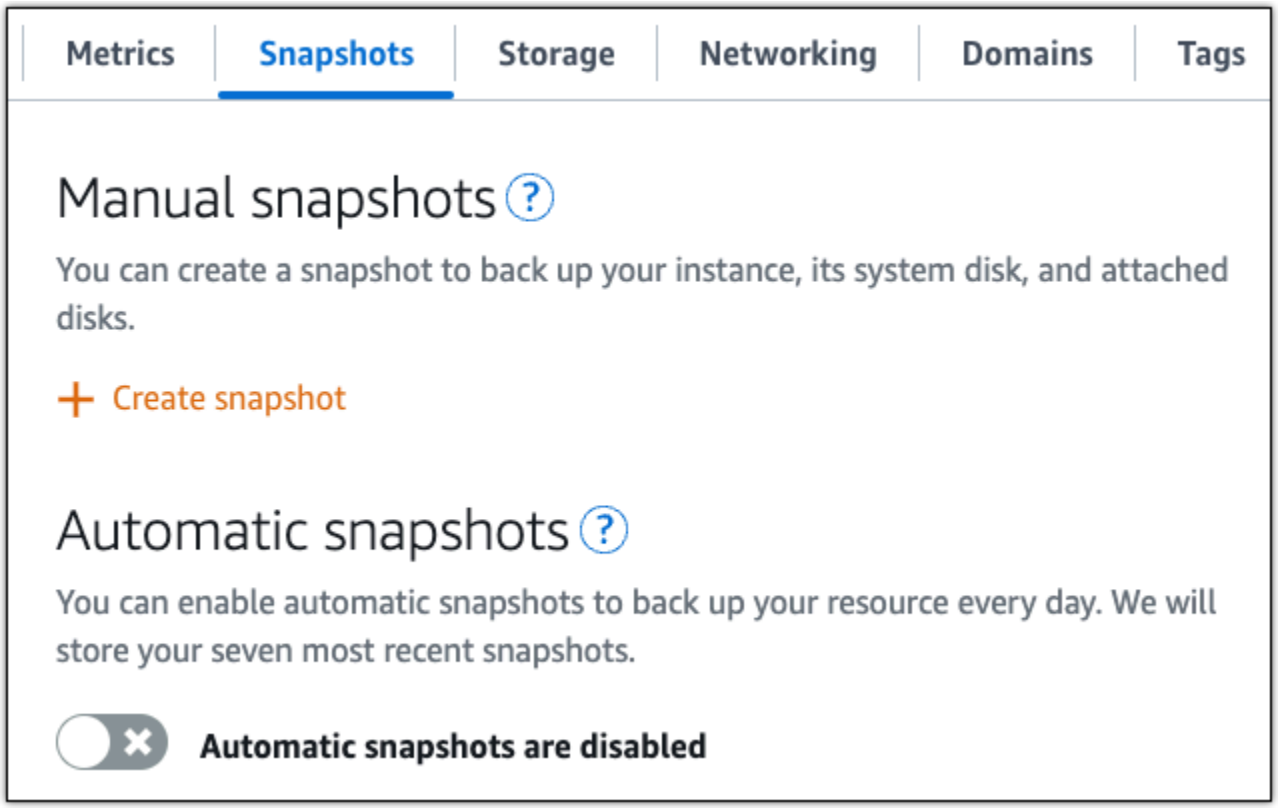
步骤 7：阅读 Joomla! 文档并继续配置网站

阅读 Joomla! 文档，了解如何管理和自定义网站。有关更多信息，请参阅 Joomla! 文档。

步骤 8：创建实例的快照

按照您所需的方式配置 Joomla! 网站后，创建实例的定期快照以进行备份。您可以手动创建快照，也可以启用自动快照，让 Lightsail 为您创建每日快照。如果实例出现错误，则可使用快照来创建新的替代实例。有关更多信息，请参阅快照。

在实例管理页面的快照选项卡下，选择创建快照或选择启用自动快照。



有关更多信息，请参阅在 Amazon Lightsail 中创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。

在 Lightsail 上设置 LAMP 堆栈

在 LAMP 实例启动并在 Amazon Lightsail 上运行后，你应该采取以下几个步骤来开始使用：

步骤 1：获取 LAMP 实例的默认应用程序密码

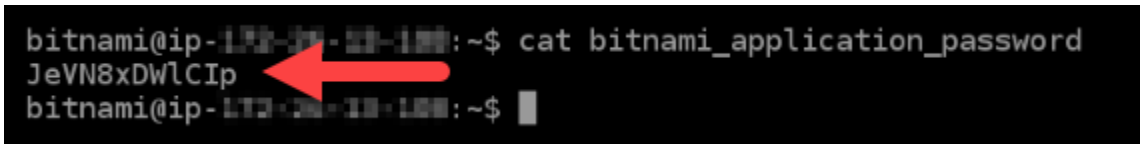
您需要使用默认应用程序密码才能访问实例上的预装应用程序或服务。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。
2. 连接后，请输入以下命令来获取应用程序密码：

```
cat bitnami_application_password
```

> **Note**
>
> 如果您所在的目录不是用户主目录，请输入 `cat $HOME/bitnami_application_password`。

您应该会看到与以下内容类似的响应，其中包含默认应用程序密码：



有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

步骤 2：将静态 IP 地址附加到 LAMP 实例

附加到实例的默认动态公有 IP 地址会在您每次停止和启动实例时发生变化。创建一个静态 IP 地址并将其附加到您的实例，以防止公有 IP 地址发生变化。稍后，当您对实例使用自己的域名时，就无需在每次停止和启动该实例时更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择创建静态 IP，然后按照页面上的说明操作。

有关更多信息，请参阅创建静态 IP 并将其附加到实例。

步骤 3：访问 LAMP 实例欢迎页面

导航到您的实例的公有 IP 地址以访问其上安装的应用程序 phpMyAdmin、访问或访问 Bitnami 文档。

1. 在实例管理页面上的 Connect (连接) 选项卡下，记下该公有 IP。
2. 浏览到该公有 IP 地址，例如，转到 `http://192.0.2.3`。

有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

步骤 4：将域名映射到 LAMP 实例

要将域名（如 `example.com`）映射到实例，您需要向域的域名系统 (DNS) 添加记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。

有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

步骤 5：阅读 Bitnami 文档

阅读 Bitnami 文档，了解如何部署应用程序、启用 SSL 证书 HTTPs支持、使用 SFTP 将文件上传到服务器等。

有关更多信息，请参阅适用于 AWS Cloud的 Bitnami LAMP。

步骤 6：创建 LAMP 实例快照

快照是系统磁盘和实例初始配置的副本。快照包含内存、CPU、磁盘大小和数据传输速率等信息。您可以将快照用作新实例的基准或用于数据备份。

在实例管理页面的 Snapshot (快照) 选项卡下，输入快照名称，然后选择 Create snapshot (创建快照)。

有关更多信息，请参阅创建 Linux 或 Unix 实例的快照。

在 Lightsail 上设置和配置 Magento

在你的 Magento 实例在 Amazon Lightsail 上启动并运行之后，你应该完成以下几个步骤才能开始使用。

内容

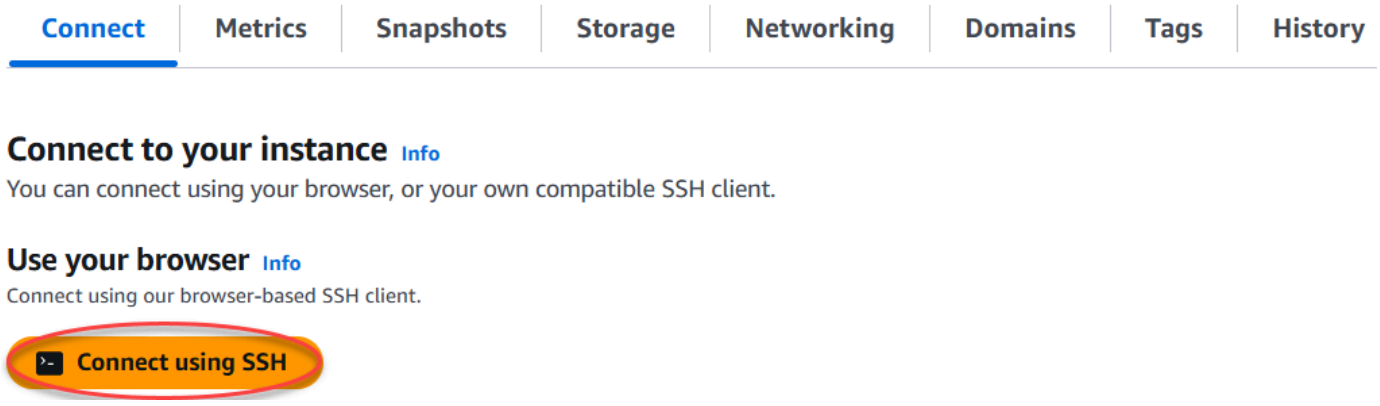
- 步骤 1：获取 Magento 网站的默认应用程序密码
- 步骤 2：将静态 IP 地址附加到 Magento 实例
- 步骤 3：登录到 Magento 网站的管理控制面板
- 步骤 4：将注册域名的流量路由到 Magento 网站
- 步骤 5：配置 Magento 网站的 HTTPS
- 步骤 6：配置电子邮件通知的 SMTP

- 步骤 7：阅读 Bitnami 和 Magento 文档
- 步骤 8：创建 Magento 实例的快照

步骤 1：获取 Magento 网站的默认应用程序密码

完成以下步骤以获取 Magento 网站的默认应用程序密码。有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

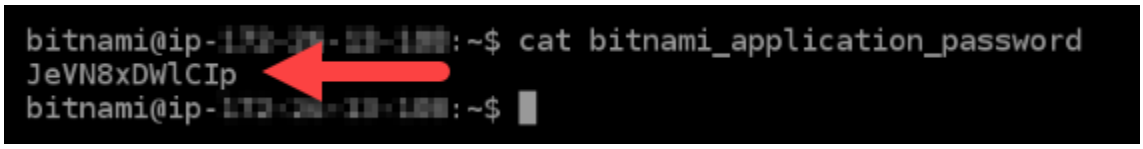
1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来获取默认应用程序密码：

```
cat $HOME/bitnami_application_password
```

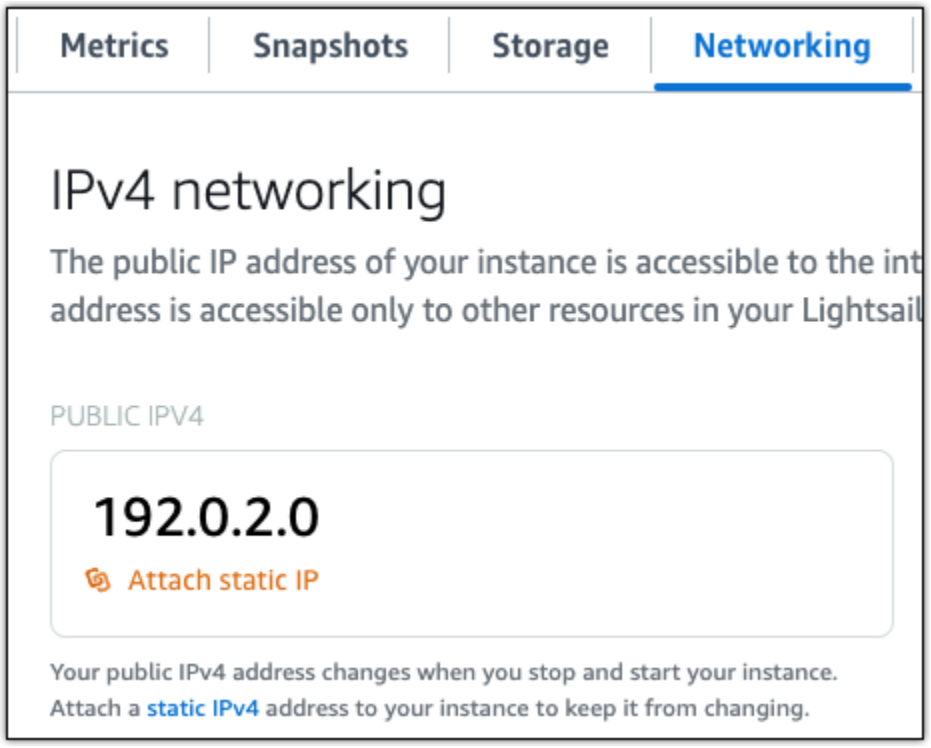
您应该会看到与以下示例类似的响应，其中包含默认应用程序密码。将此密码保存在安全位置。您将在本教程的下一部分使用它来登录 Magento 网站的管理控制面板。



步骤 2：将静态 IP 地址附加到 Magento 实例

在您首次创建实例时分配给实例的公有 IP 地址会在您每次停止和启动实例时发生更改。您应为实例创建和附加静态 IP 地址，以确保其公有 IP 地址不变。之后当您将注册域名（如 example.com）指向实例时，无需在每次停止和重启实例时都更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择创建静态 IP或附加静态 IP（如果您之前创建了可附加到实例的静态 IP），然后按照页面上的说明操作。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

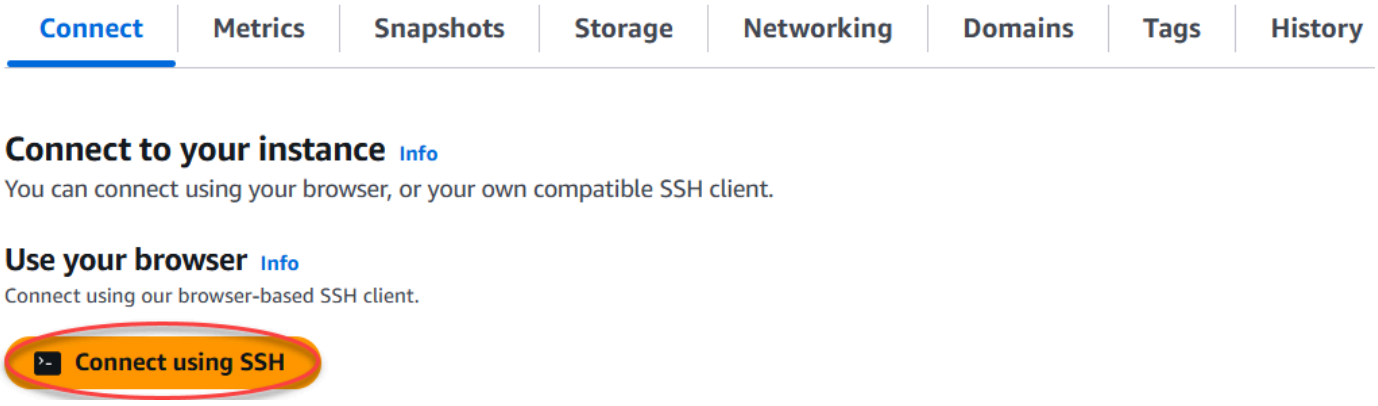


将新的静态 IP 地址附加到实例后，您必须完成以下步骤，以使 Magento 软件知道新的静态 IP 地址。

1. 记下实例的静态 IP 地址。它列在实例管理页面的标题部分。



2. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



3. 连接后，请输入以下命令。请务必*<StaticIP>*使用您的实例的新静态 IP 地址替换。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您应看到类似于以下示例的响应。Magento 软件现在应该识别到了新的静态 IP 地址。

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

> **Note**
>
> Magento 目前不支持 IPv6 地址。您可以 IPv6 为该实例启用，但是 Magento 软件不会响应通过网络发送的 IPv6 请求。

步骤 3：登录到 Magento 网站的管理控制面板

完成以下步骤以访问 Magento 网站并登录到它的管理控制面板。要进行登录，请使用默认用户名 (`user`) 和您之前在本指南中获取的默认应用程序密码。

1. 在 Lightsail 控制台中，记下实例管理页面标题区域中列出的公共或静态 IP 地址。



2. 浏览到以下地址可访问 Magento 网站管理控制面板的登录页面。请务必*<InstanceIpAddress>*替换为您的实例的公有或静态 IP 地址。

```
http://<InstanceIpAddress>/admin
```

示例：

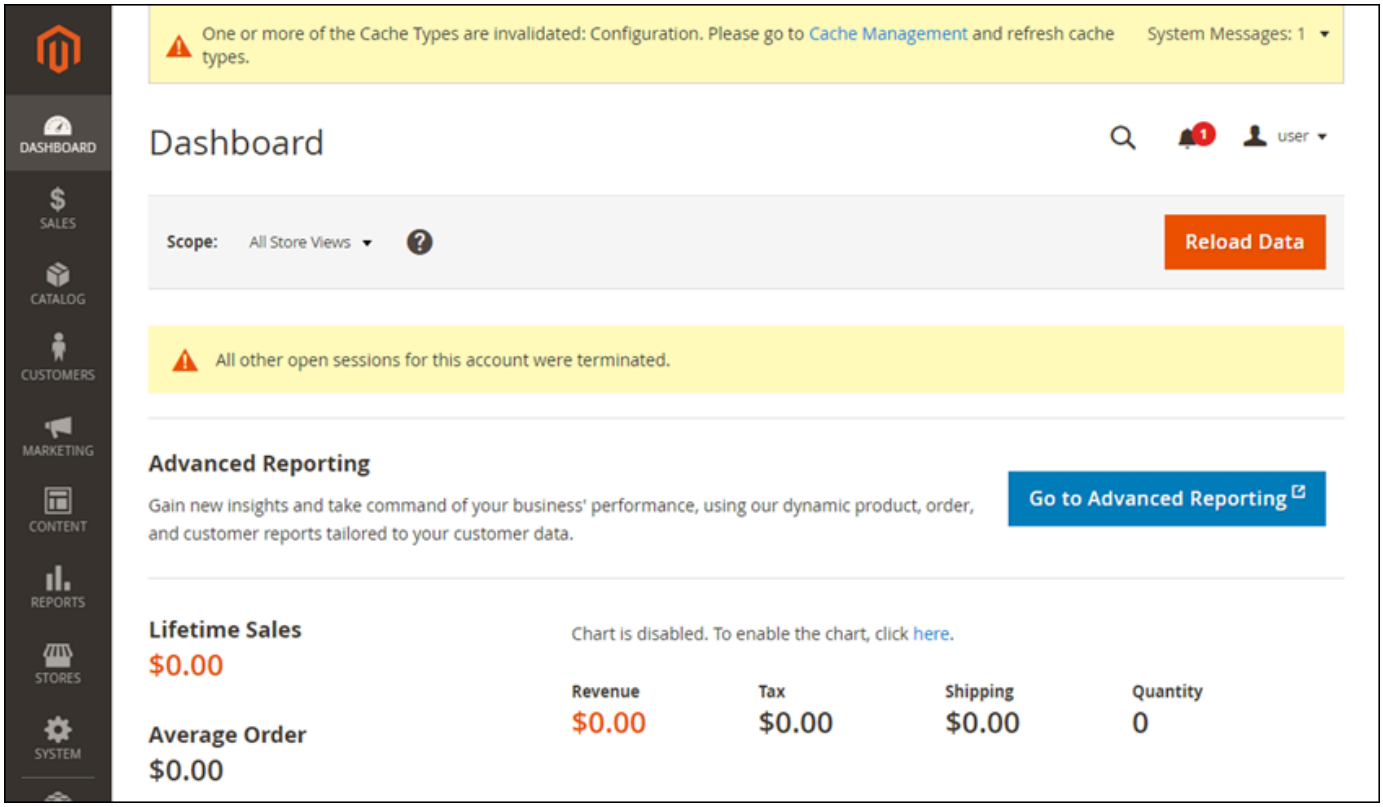
```
http://203.0.113.0/admin
```

> **Note**
>
> 如果您无法访问 Magento 管理控制面板的登录页面，则可能需要重启实例。

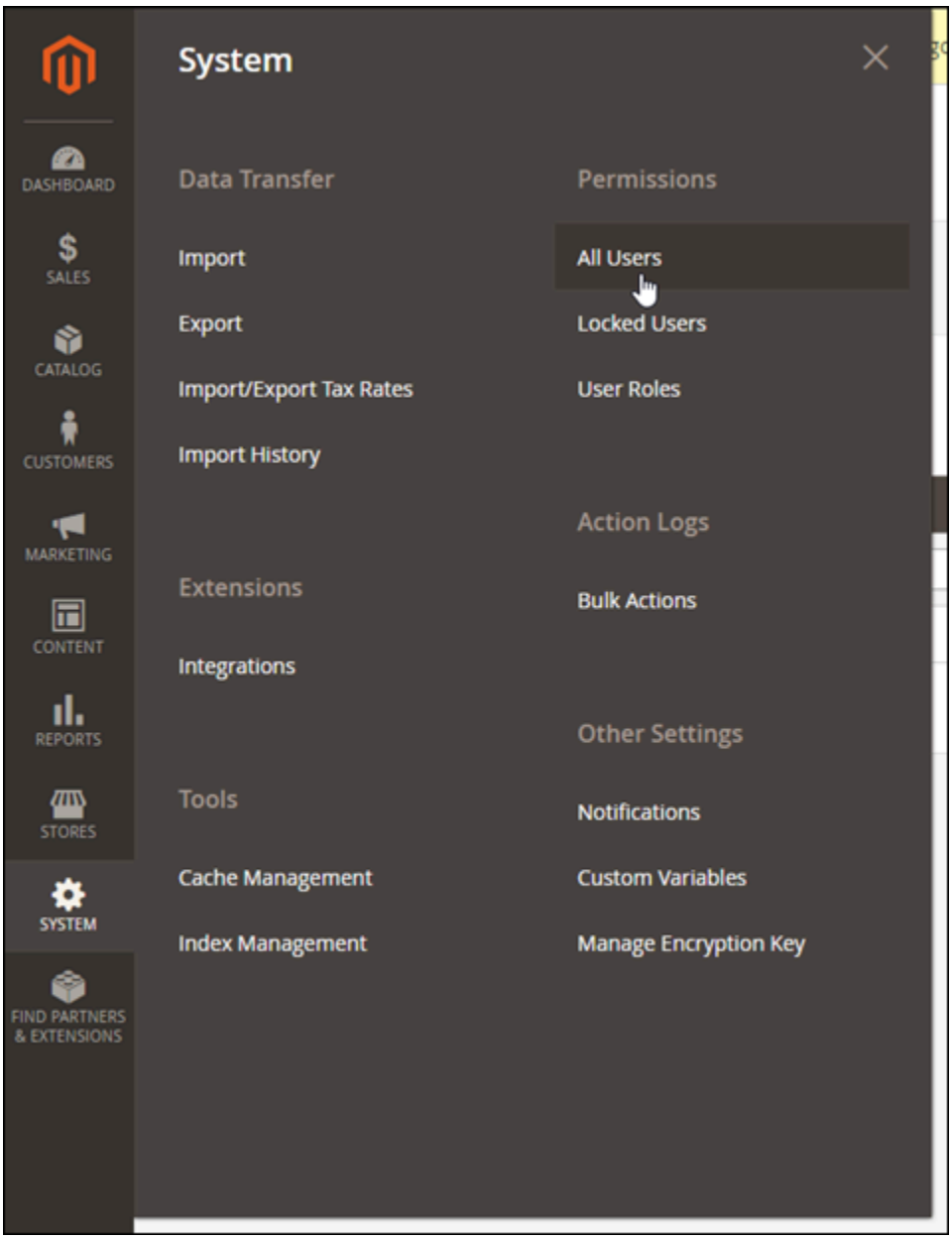
3. 输入默认用户名（`user`）和您之前在本指南中获取的默认应用程序密码，然后选择 Sign in（登录）。



将显示 Magento 管理控制面板。



要更改用于登录 Magento 网站管理控制面板的默认用户名或密码，请在导航窗格中选择 System（系统），然后选择 All Users（所有用户）。有关更多信息，请参阅 Magento 文档中的添加用户。



有关管理控制面板的更多信息，请参阅《Magento 2.4 用户指南》。

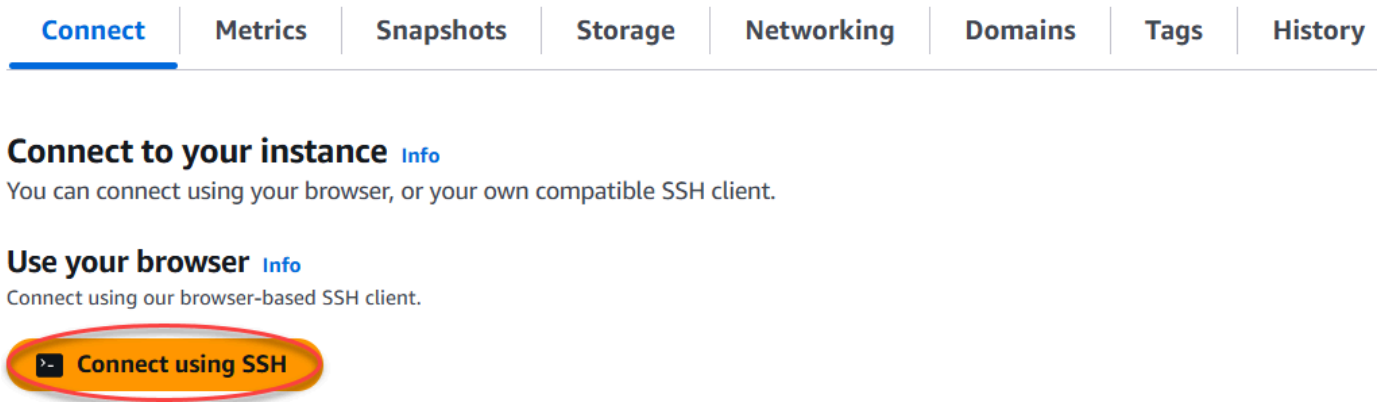
步骤 4：将注册域名的流量路由到 Magento 网站

要将注册域名（如 `example.com`）的流量路由到 Magento 网站，您需要向域的域名系统（DNS）添加记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

在您的域名将流量路由到实例之后，您必须完成以下步骤才能让 Magento 软件知道域名。

1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令。请务必*<DomainName>*替换为将流量路由到您的实例的域名。

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

您应看到类似于以下示例的响应。Magento 软件现在应该识别到了域名。

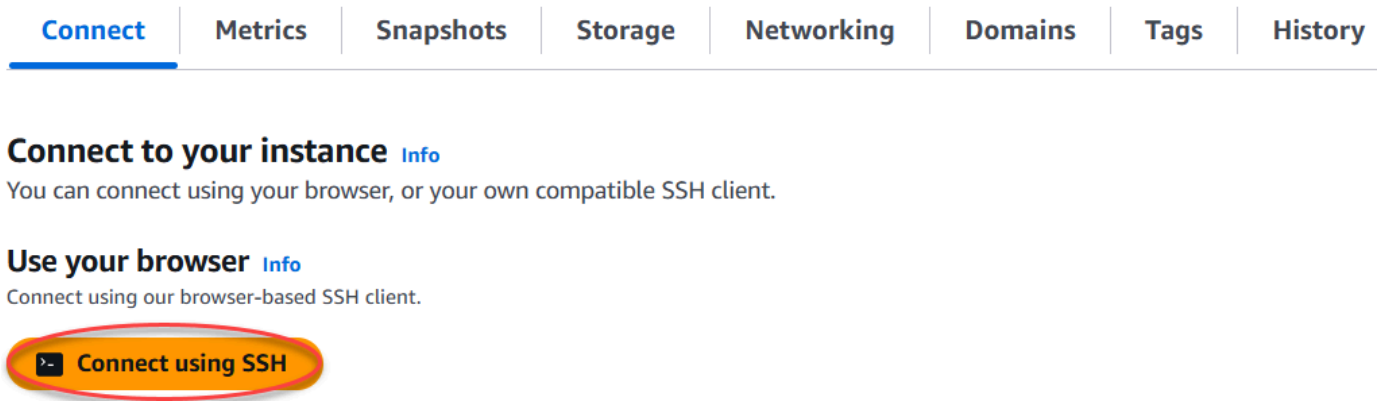
```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

步骤 5：配置 Magento 网站的 HTTPS

完成以下步骤以在 Magento 网站上配置 HTTPS。这些步骤介绍了如何使用 Bitnami HTTPS 配置工具 (bncert)，该工具是用于请求 SSL/TLS 证书、设置重新导向（例如 HTTP 到 HTTPS）和续订证书的命令行工具。

> **Important**
>
> bncert 工具将仅为当前将流量路由到 Magento 实例的公有 IP 地址的域颁发证书。在开始执行这些步骤之前，请确保您将 DNS 记录添加到要用于 Magento 网站的所有域的 DNS。

1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来启动 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

您会看到类似于以下示例的响应：

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/bncert-tool
Warning: Custom redirections are not supported in the Bitnami Magento Stack.
This tool will not be able to enable/disable redirections.
Press [Enter] to continue:
```

3. 输入用空格分隔的主域名和备用域名，如以下示例所示。

```
--------------------------------------------------------------------------------
Welcome to the Bitnami HTTPS Configuration tool.

--------------------------------------------------------------------------------
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []: example.com www.example.com
```

4. 将列出要进行的更改。输入 Y 然后按 Enter 以确认并继续。

```
------------------------------------------------------------------------------
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
 example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

5. 输入要与 Let's Encrypt 证书关联的电子邮件地址，然后按 Enter（确定键）。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

6. 查看 Let's Encrypt 的加密用户协议 输入 Y 然后按 Enter 接受协议并继续。

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

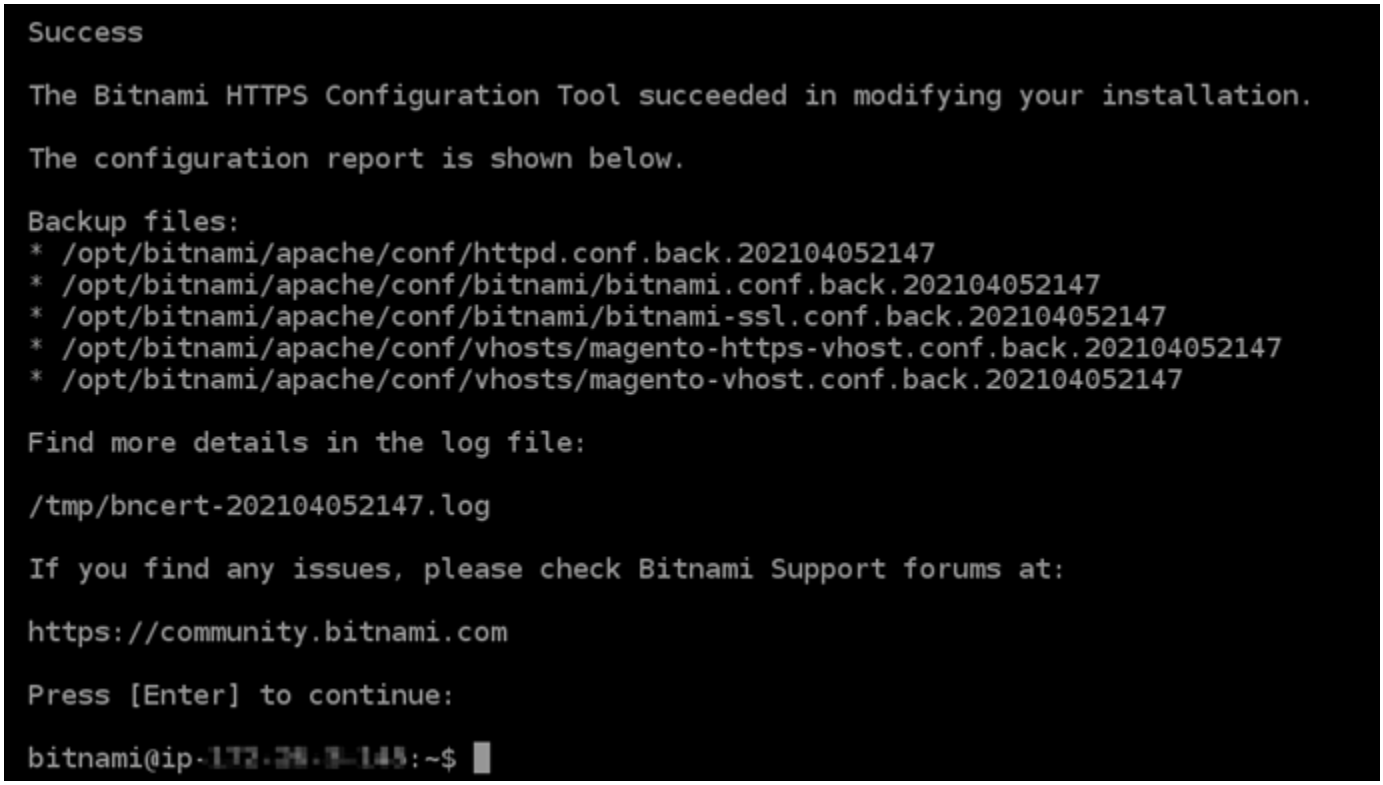
将执行这些操作以在您的实例上启用 HTTPS，包括请求证书和配置您指定的重新导向。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|
```

您的证书已成功颁发和验证，如果您看到类似于以下示例的消息，则表示在实例上成功配置了重新导向。



bncert 工具将在证书过期前每 80 天执行一次自动续订。继续执行下一组步骤，以完成在 Magento 网站上启用 HTTPS 的过程。

7. 浏览到以下地址可访问 Magento 网站管理控制面板的登录页面。请务必*<DomainName>*替换为将流量路由到您的实例的注册域名。

```
http://<DomainName>/admin
```

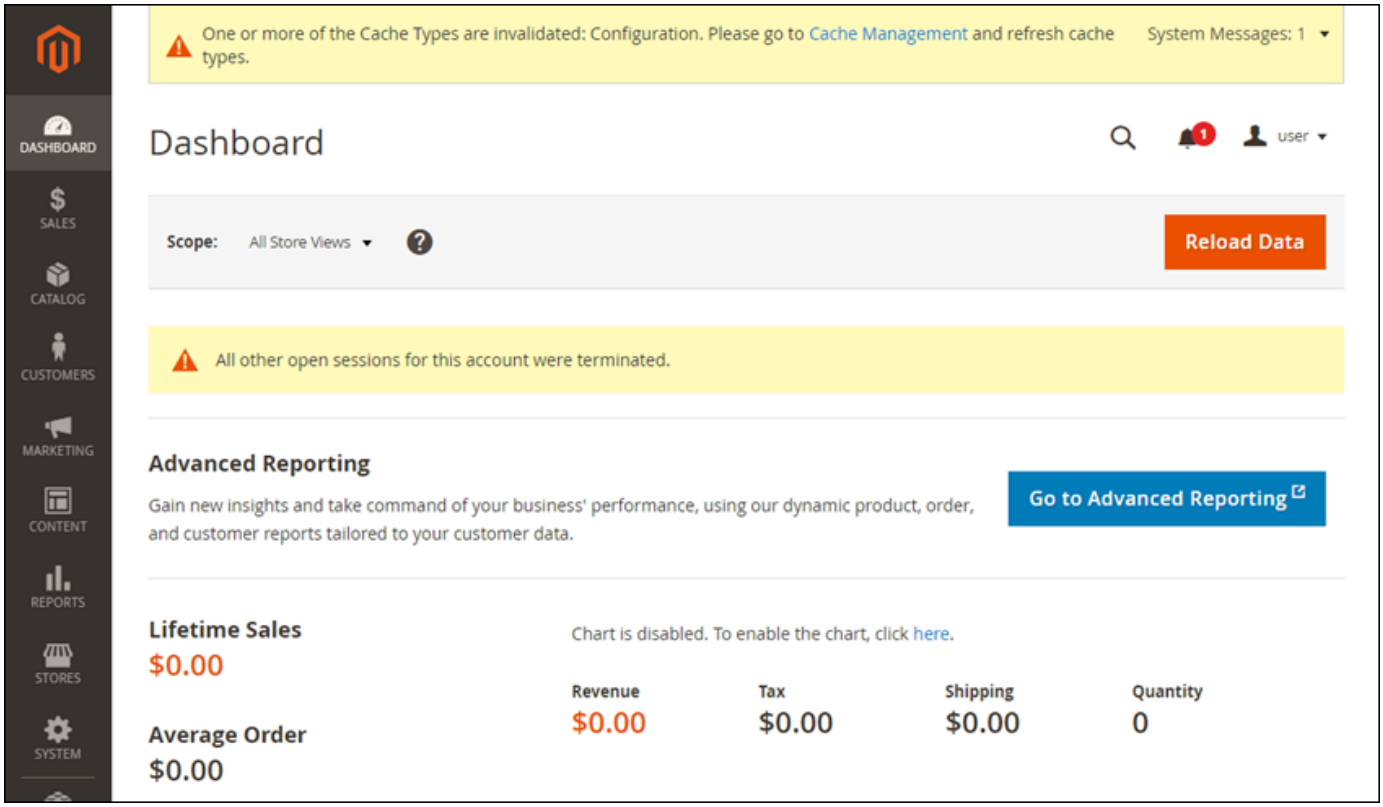
示例：

```
http://www.example.com/admin
```

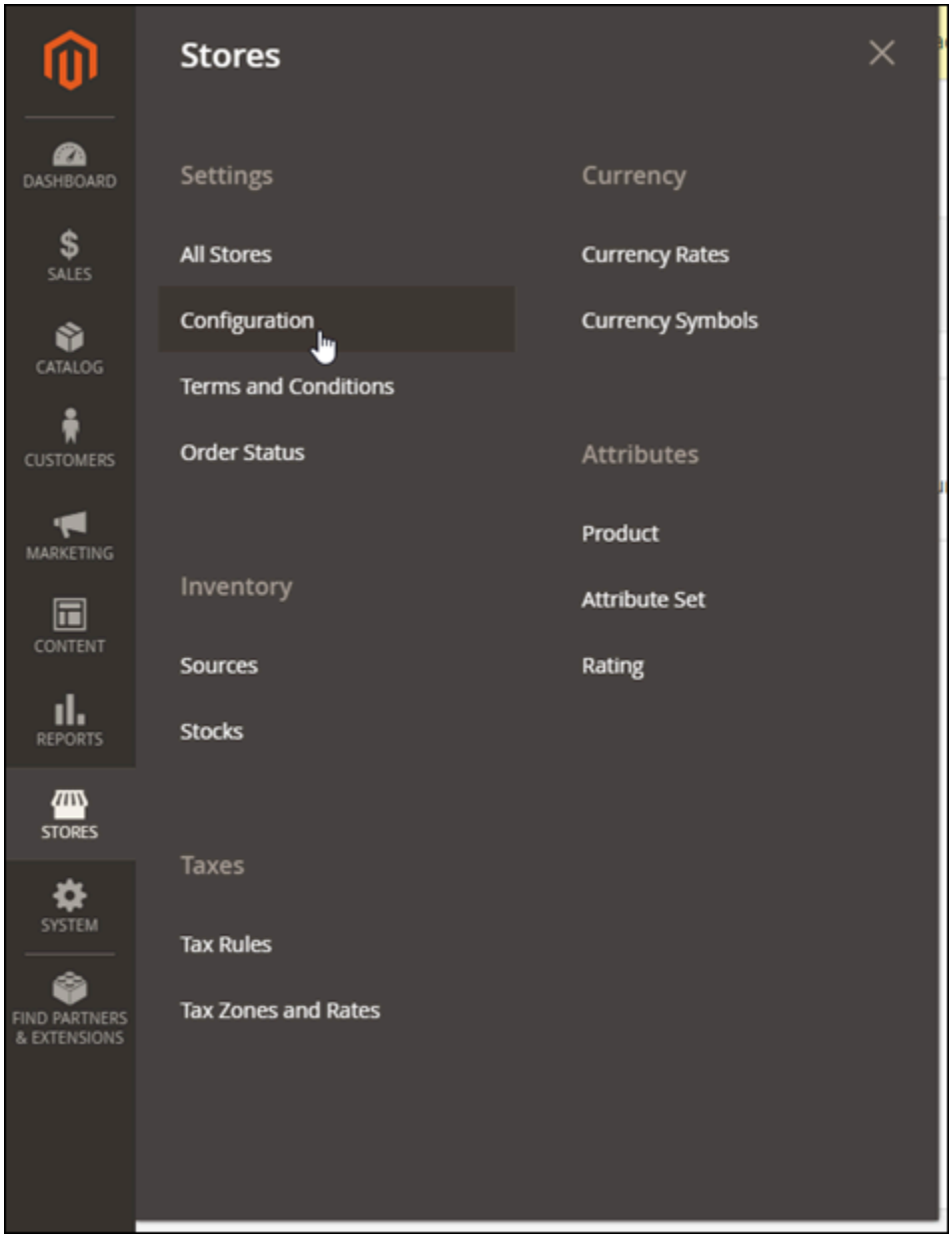
8. 输入默认用户名（user）和您之前在本指南中获取的默认应用程序密码，然后选择 Sign in（登录）。



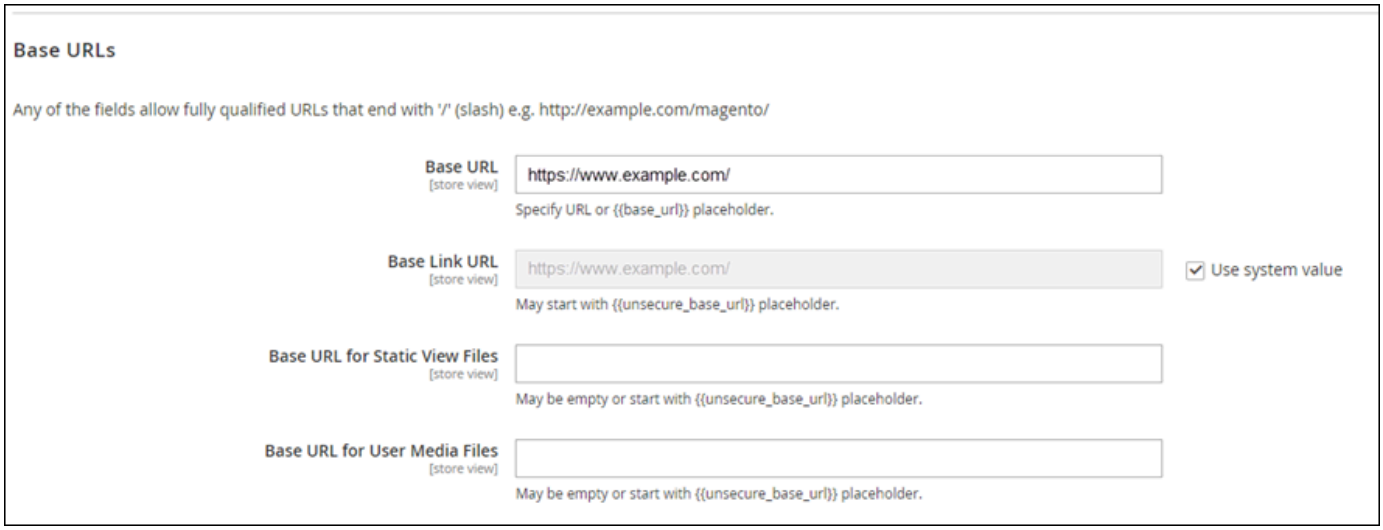
将显示 Magento 管理控制面板。



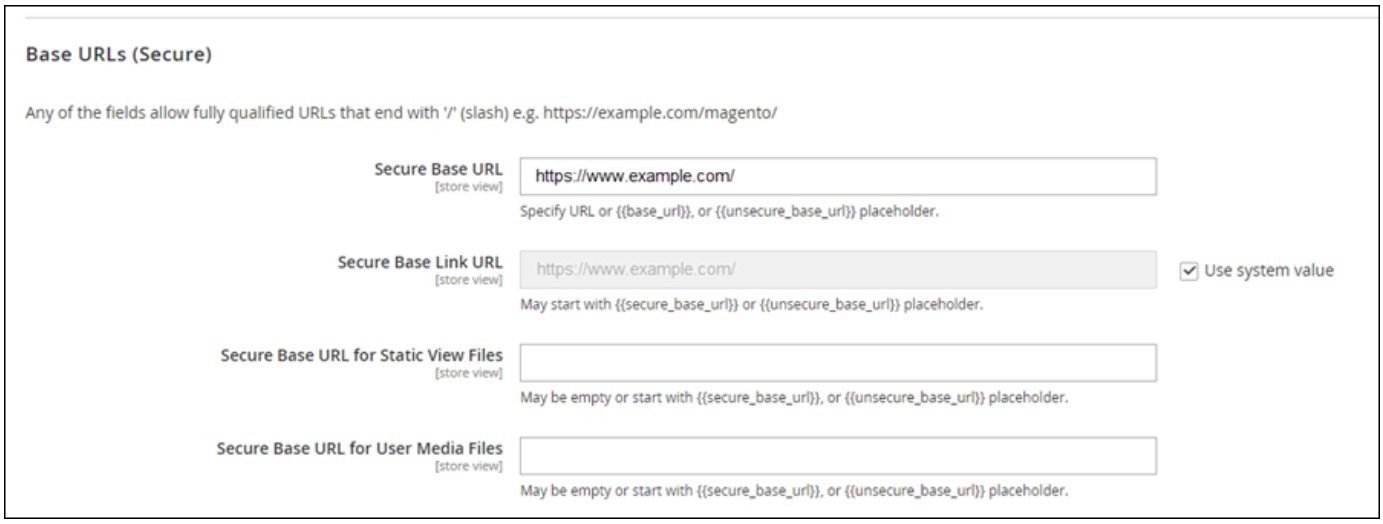
9. 在导航窗格中，选择 Stores（存储），然后选择 Configuration（配置）。



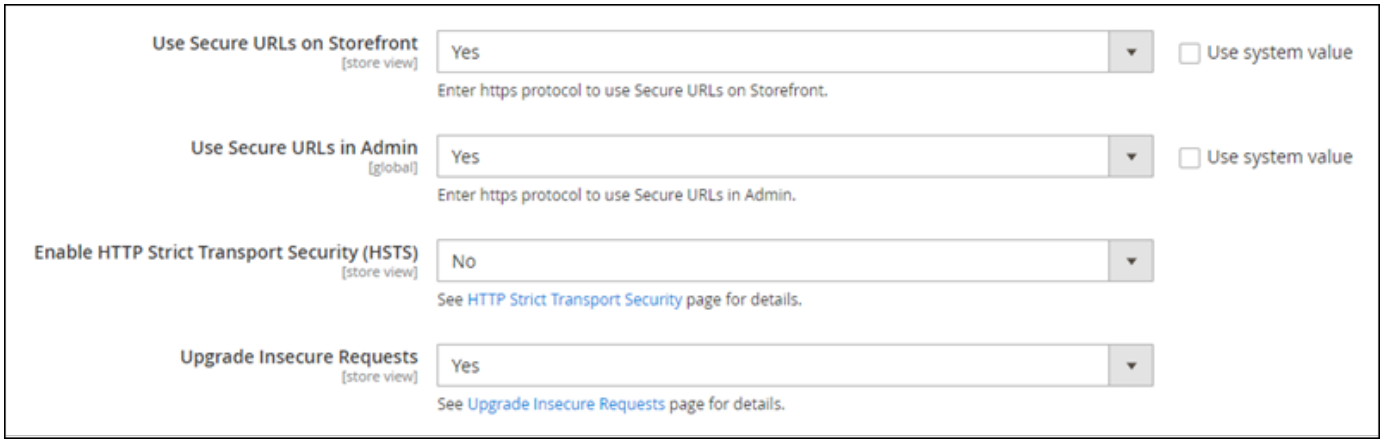
10. 选择 Web，然后展开 “基本 URLs” 节点。
11. 在 Base URL（基本 URL）文本框中，输入网站的完整 URL，例如 `https://www.example.com/`。



12. 展开 “基本 URLs （安全）” 节点。
13. 在 Secure Base URL（安全基本 URL）文本框中，输入网站的完整 URL，例如 `https://www.example.com/`。



14. 在 “ URLs 在 Storefront 上使用安全”、“ URLs 在管理中使用安全” 和 “升级不安全的请求” 选项中选择 “是”。



15. 在页面顶部，选择 Save Config（保存配置）。

    您的 Magento 网站现在已配置为 HTTPS。当客户浏览 Magento 网站的 HTTP 版本（例如 `http://www.example.com`）时，它们将被自动重新导向到 HTTPS 版本（例如 `https://www.example.com`）。

步骤 6：配置电子邮件通知的 SMTP

配置 Magento 网站的 SMTP 设置，以启用电子邮件通知。有关更多信息，请参阅 Bitnami 文档中的安装 Magento Magepal SMTP 扩展。

> **Important**
>
> 如果您将 SMTP 配置为使用端口 25、465 或 587，则必须在 Lightsail 控制台中打开实例防火墙中的这些端口。有关更多信息，请参阅在 Amazon Lightsail 中添加和编辑实例防火墙规则。如果您将 Gmail 账户配置为在 Magento 网站上发送电子邮件，那么您必须使用应用程序密码，而不是使用登录 Gmail 时使用的标准密码。有关更多信息，请参阅使用应用程序密码登录。

步骤 7：阅读 Bitnami 和 Magento 文档

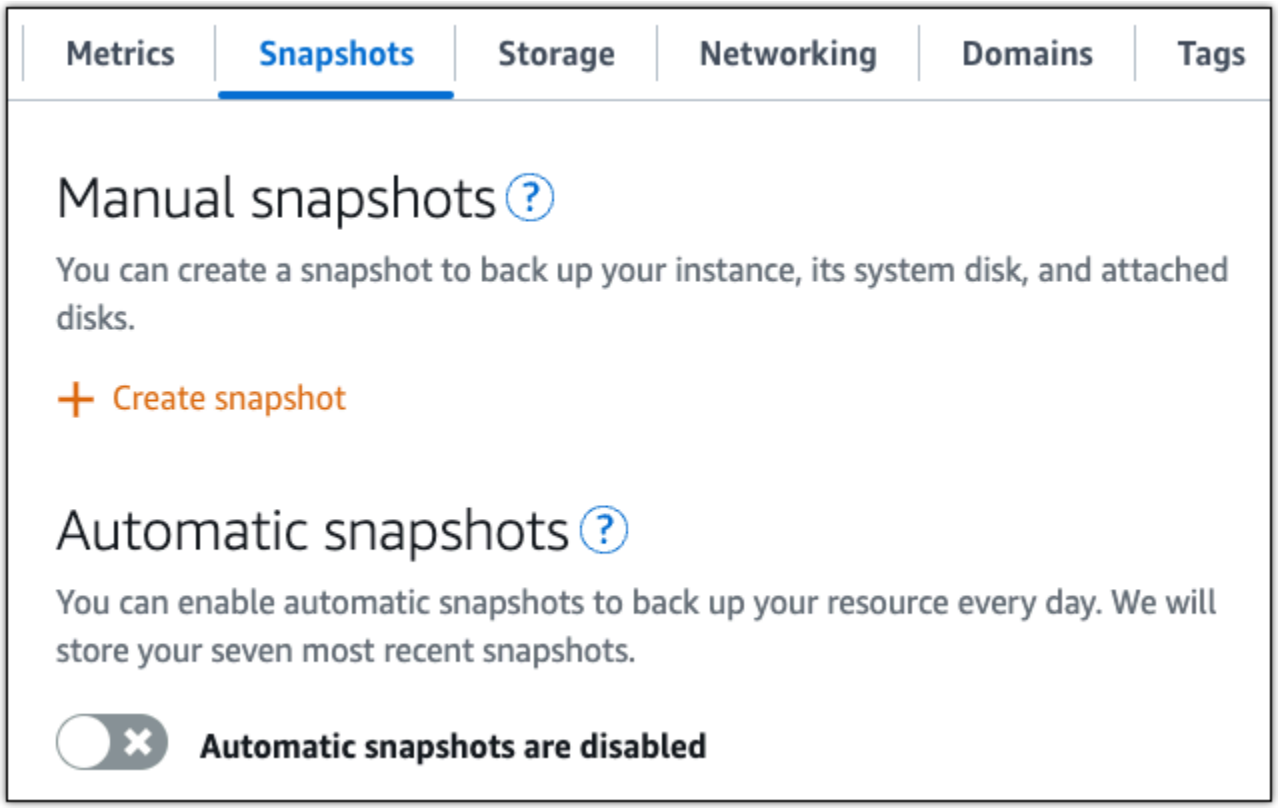
阅读 Bitnami 文档，了解如何在 Magento 实例和网站上执行管理任务，例如安装插件和自定义主题等。有关更多信息，请参阅 Bitnami 文档中的适用于亚马逊云科技云的 Bitnami Magento 堆栈。

您还应阅读 Magento 文档，以了解如何管理您的 Magento 网站。有关更多信息，请参阅《Magento 2.4 用户指南》。

步骤 8：创建 Magento 实例的快照

按照您所需的方式配置 Magento 网站后，创建实例的定期快照以进行备份。您可以手动创建快照，也可以启用自动快照，让 Lightsail 为您创建每日快照。如果实例出现错误，则可使用快照来创建新的替代实例。有关更多信息，请参阅快照。

在实例管理页面的快照选项卡下，选择创建快照或选择启用自动快照。



有关更多信息，请参阅在 Amazon Lightsail 中创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。

在 Lightsail 上部署和管理 Nginx 网络服务器

在你的 Nginx 实例在 Amazon Lightsail 上启动并运行之后，你应该采取以下几个步骤来开始使用：

步骤 1：获取 Nginx 实例的默认应用程序密码

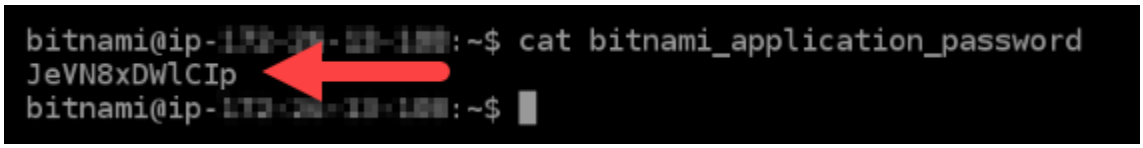
您需要使用默认应用程序密码才能访问实例上的预装应用程序或服务。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。
2. 连接后，请输入以下命令来获取默认应用程序密码：

```
cat bitnami_application_password
```

> **Note**
>
> 如果您所在的目录不是用户主目录，请输入 `cat $HOME/bitnami_application_password`。

您应该会看到与以下内容类似的响应，其中包含默认应用程序密码：



有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

步骤 2：将静态 IP 地址附加到 Nginx 实例

附加到实例的默认动态公有 IP 地址会在您每次停止和启动实例时发生变化。创建一个静态 IP 地址并将其附加到您的实例，以防止公有 IP 地址发生变化。稍后，当您对实例使用自己的域名时，就无需在每次停止和启动该实例时更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的 Domains & DNS（域和 DNS）选项卡下，选择 Create static IP（创建静态 IP），然后按照页面上的说明操作。

有关更多信息，请参阅在 Lightsail 中创建静态 IP 并将其附加到 Lightsail 中的实例。

步骤 3：访问 Nginx 实例欢迎页面

导航到您的实例的公有 IP 地址以访问其上安装的应用程序 phpMyAdmin、访问或访问 Bitnami 文档。

1. 在实例管理页面上的 Connect (连接) 选项卡下，记下该公有 IP。
2. 浏览到该公有 IP 地址，例如，转到 `http://192.0.2.3`。

有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

步骤 4：将域名映射到 Nginx 实例

要将域名（如 `example.com`）映射到实例，您需要向域的域名系统 (DNS) 添加记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “网络” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。

有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

步骤 5：阅读 Bitnami 文档

阅读 Bitnami 文档，了解如何部署 Nginx 应用程序、使用 SSL 证书启用 HTTPS 支持、使用 SFTP 将文件上传到服务器等。

有关更多信息，请参阅适用于 AWS Cloud的 Bitnami Nginx。

步骤 6：创建 Nginx 实例快照

快照是系统磁盘和实例初始配置的副本。快照包含内存、CPU、磁盘大小和数据传输速率等信息。您可以将快照用作新实例的基准或用于数据备份。

在实例管理页面的 Snapshot (快照) 选项卡下，输入快照名称，然后选择 Create snapshot (创建快照)。

有关更多信息，请参阅创建 Linux 或 Unix 实例的快照。

开始在 Lightsail 上使用 Node.js

在你的 Node.js 实例启动并在 Amazon Lightsail 上运行后，你应该采取以下几个步骤来开始使用：

步骤 1：获取 Node.js 实例的默认应用程序密码

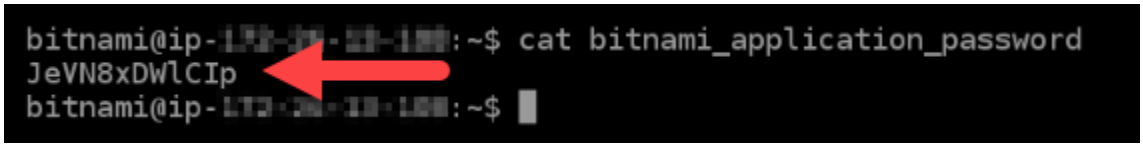
您需要使用默认应用程序密码才能访问实例上的预装应用程序或服务。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。
2. 连接后，请输入以下命令来获取默认应用程序密码：

```
cat bitnami_application_password
```

> **Note**
>
> 如果您所在的目录不是用户主目录，请输入 `cat $HOME/bitnami_application_password`。

您应该会看到与以下内容类似的响应，其中包含默认应用程序密码：



有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

步骤 2：将静态 IP 地址附加到 Node.js 实例

附加到实例的默认动态公有 IP 地址会在您每次停止和启动实例时发生变化。创建一个静态 IP 地址并将其附加到您的实例，以防止公有 IP 地址发生变化。稍后，当您对实例使用自己的域名时，就无需在每次停止和启动该实例时更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的 Domains & DNS（域和 DNS）选项卡下，选择 Create static IP（创建静态 IP），然后按照页面上的说明操作。

有关更多信息，请参阅在 Lightsail 中创建静态 IP 并将其附加到 Lightsail 中的实例。

步骤 3：访问 Node.js 实例欢迎页面

导航到您的实例的公有 IP 地址以访问其上安装的应用程序 phpMyAdmin、访问或访问 Bitnami 文档。

1. 在实例管理页面上的 Connect (连接) 选项卡下，记下该公有 IP。
2. 浏览到该公有 IP 地址，例如，转到 `http://192.0.2.3`。

有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

步骤 4：将域名映射到 Node.js 实例

要将域名（如 `example.com`）映射到实例，您需要向域的域名系统 (DNS) 添加记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “网络” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。

有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

步骤 5：阅读 Bitnami 文档

阅读 Bitnami 文档，了解如何部署 Node.js 应用程序、使用 SSL 证书启用 HTTPS 支持、使用 SFTP 将文件上传到服务器等。

有关更多信息，请参阅适用于 AWS Cloud的 Bitnami Node.js。

步骤 6：创建 Node.js 实例快照

快照是系统磁盘和实例初始配置的副本。快照包含内存、CPU、磁盘大小和数据传输速率等信息。您可以将快照用作新实例的基准或用于数据备份。

在实例管理页面的 Snapshot (快照) 选项卡下，输入快照名称，然后选择 Create snapshot (创建快照)。

有关更多信息，请参阅创建 Linux 或 Unix 实例的快照。

在 Lightsail 上部署 Plesk 托管堆栈

了解如何在 Amazon Lightsail 中创建 Plesk 实例，以及如何通过创建用户名和密码首次登录 Plesk 用户界面。您还将了解如何在 Plesk 实例启动并运行后连接和配置该实例。

> **Important**
>
> 使用 Ubuntu 上的 Plesk 托管堆栈 (BYOL) 蓝图启动的实例有 30 天的试用许可证。30 天后，您必须从 Plesk 购买许可证才能继续使用 Plesk 应用程序。

Lightsail 中的 Plesk 托管堆栈包括以下功能。

- WordPress 工具包，在图形用户界面中具有自动化功能
- 为 SSL 证书提供 Let's Encrypt 支持，并在单个实例上配置加密的 (HTTPS) 流量
- 提供 FTP 访问以在实例之间传输文件
- Docker 代理规则
- 基于 Web 的服务器管理和安全工具，包括 Plesk 防火墙、日志和 ModSecurity

步骤 1：创建 Plesk 实例

完成以下步骤在 Lightsail 上创建 Plesk 实例。

1. 登录 Lightsail 控制台，网址为https://lightsail.aws.amazon.com/。
2. 在实例主页上，选择创建实例。
3. 选择要创建实例的位置。

   选择更改 AWS 区域 和可用区以更改您的实例位置。
4. 在 “应用程序 + 操作系统” 下，选择 Plesk Hosting Stack 开启 Ubuntu (BYOL)。
5. 选择实例计划。每月5美元的Lightsail计划不支持Plesk托管堆栈。
6. 输入实例的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。
7. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

   a. 对于密钥，输入标签密钥。

   b. （可选）在 “值” 中，输入标签值。

8. 选择 Create instance（创建实例）。

   在您创建实例后，它需要几分钟的时间才能完成预置并变得可用。

如果在启动 Plesk 实例后遇到问题，请转到 Plesk 支持页面，以查看是否需要在实例上安装更新。有关更多信息，请参阅 Plesk 文档和帮助门户中的 Plesk 帮助中心和 Plesk 更新。

步骤 2：首次登录 Plesk 用户界面

使用以下过程获取一次性登录 URL。您需要使用一次性登录 URL 才能以管理员身份访问 Plesk 用户界面。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。
2. 连接后，请输入以下命令来获取一次性登录 URL。

   ```
   sudo plesk login | grep -v internal:8
   ```

   您应该看到类似于以下示例的响应，其中包含一次性登录 URL。

   ```
   https://heuristic-bassi.192-0-2-0.plesk.page/login?secret=ce-
   e3b0c44298fc1c149afbf4c8996fb92427
   ```

   > **Tip**
   >
   > 如果您最近将静态 IP 附加到 Plesk 实例，则可能会获得一个使用旧的公有 IP 地址的一次性登录 URL。重新启动实例，然后再次运行上述命令以获取使用新静态公有 IP 地址的一次性登录 URL。

3. 将一次性登录 URL 复制粘贴到 Web 浏览器中。

   > **Note**
   >
   > 您可能会看到一个浏览器警告，指出您的连接不是私有的、不是安全的或存在安全风险。发生这种情况的原因是您的 Plesk 实例尚未应用 SSL/TLS 证书。在浏览器窗口中，选择高级、详细信息或更多信息以查看可用的选项。然后选择继续连接该网站，即使它不是私有或安全的。

4. 按照页面上的说明创建您的 Plesk 登录凭证。首次登录时，您应该看到一个将域添加到 Plesk 的选项。

要稍后再次登录，请导航至 `https://PublicIPAddress:8443`。*PublicIPAddress*替换为您的实例的公有 IP 地址或静态 IP 地址。例如 `https://192.0.2.0/:8443`。然后输入您之前创建的用户名和密码来登录 Plesk 用户界面。

步骤 3：阅读 Plesk 文档

阅读 Plesk 文档，了解如何管理网站、自定义 Plesk 用户界面等。

有关更多信息，请参阅 Plesk 文档和帮助门户中的开始在 Plesk 中管理网站。

步骤 4：将静态 IP 地址附加到 Plesk 实例

附加到实例的默认动态公有 IP 地址会在您每次停止和启动实例时发生变化。创建一个静态 IP 地址并将其附加到您的实例，以防止公有 IP 地址发生变化。稍后，当您对实例使用自己的域名时，就无需在每次停止和启动该实例时更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择附加静态 IP，然后按照页面上的说明操作。

有关更多信息，请参阅创建静态 IP 并将其附加到实例。

步骤 5：将域名映射到 PLesk 实例

将域映射到 Plesk 实例，可使用该实例来访问 Plesk 用户界面。您还可以在 Plesk 用户界面中映射多个域，可使用这些域来管理网站。本节介绍如何将域映射到 Plesk 实例。有关在 Plesk 用户界面中映射多个域的更多信息，请参阅 Plesk 文档和帮助门户中的在 Plesk 中添加域。

要将域名（如 `example.com`）映射到实例，您需要向域的域名系统 (DNS) 添加记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 上，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。

有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

步骤 6：购买 Plesk 许可证

您的 Plesk 实例包含 30 天试用许可证。30 天后，您必须从 Plesk 购买许可证才能继续使用该应用程序。有关更多信息，请参阅 Plesk 网站上的定价。

从 Plesk 购买许可证后，必须安装许可证。要安装您的 Plesk 许可证，请参阅 Plesk 支持网站上的如何安装 Plesk 许可证。

步骤 7：创建 Plesk 实例快照

快照是系统磁盘和实例初始配置的副本。快照包含内存、CPU、磁盘大小和数据传输速率等信息。您可以将快照用作新实例的基准或用于数据备份。

在实例管理页面的快照选项卡下，选择创建快照。然后，按照页面上的说明操作。有关更多信息，请参阅创建 Linux 或 Unix 实例的快照。

在 Lightsa PrestaShop il 上建立一个网站

在您的 PrestaShop 实例在 Amazon Lightsail 上启动并运行后，您需要完成以下几个步骤才能开始使用。

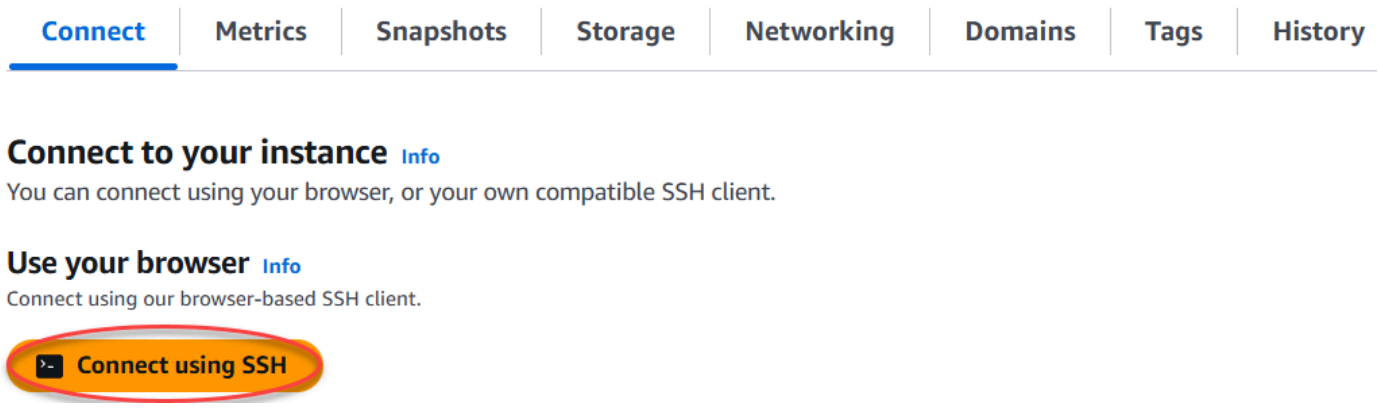
内容

- 第 1 步：获取 PrestaShop 网站的默认应用程序密码
- 步骤 2：将静态 IP 地址附加到您的 PrestaShop 实例
- 第 3 步：登录 PrestaShop 网站的管理控制面板
- 第 4 步：将您注册域名的流量路由到您的 PrestaShop网站
- 第 5 步：为您的 PrestaShop 网站配置 HTTPS
- 步骤 6：配置电子邮件通知的 SMTP
- 第 7 步：阅读 Bitnami 和文档 PrestaShop
- 步骤 8：为您的 PrestaShop 实例创建快照

第 1 步：获取 PrestaShop 网站的默认应用程序密码

完成以下步骤以获取您 PrestaShop网站的默认应用程序密码。

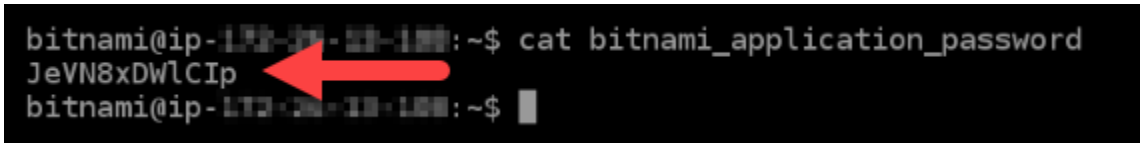
1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来获取默认应用程序密码：

```
cat $HOME/bitnami_application_password
```

您应该会看到与以下示例类似的响应，其中包含默认应用程序密码。将此密码保存在安全位置。在本教程的下一节中，您将使用它来登录 PrestaShop网站的管理控制面板。



有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

步骤 2：将静态 IP 地址附加到您的 PrestaShop 实例

在您首次创建实例时分配给实例的公有 IP 地址会在您每次停止和启动实例时发生更改。您应为实例创建和附加静态 IP 地址，以确保其公有 IP 地址不变。之后当您将注册域名（如 `example.com`）指向实例时，无需在每次停止和重启实例时都更新域的 DNS 记录。您可以将静态 IP 附加到实例。

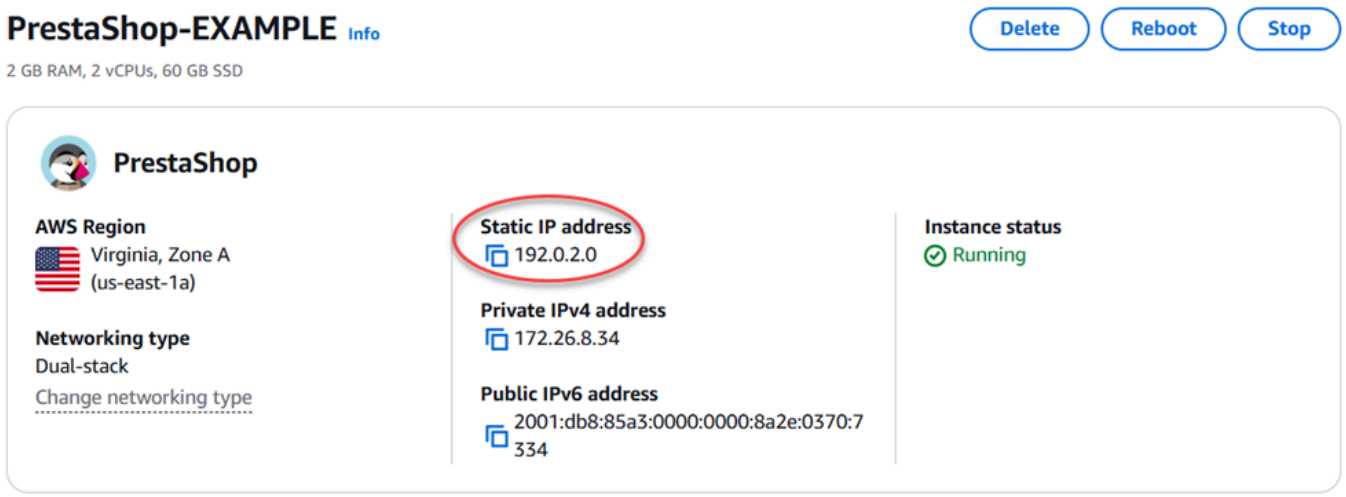
在实例管理页面上的联网选项卡下，选择创建静态 IP或附加静态 IP（如果您之前创建了可附加到实例的静态 IP），然后按照页面上的说明操作。



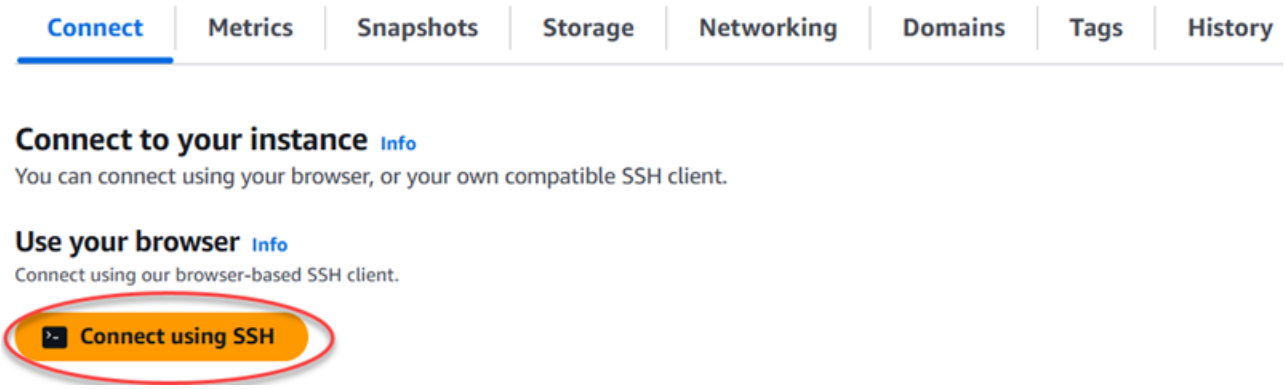
有关更多信息，请参阅创建静态 IP 并将其附加到实例。

将新的静态 IP 地址附加到您的实例后，您必须完成以下步骤才能使 PrestaShop 软件知道新的静态 IP 地址。

1. 记下实例的静态 IP 地址。它列在实例管理页面的标题部分。



2. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



3. 连接后，请输入以下命令。请务必*<StaticIP>*使用您的实例的新静态 IP 地址替换。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您应看到类似于以下示例的响应。 PrestaShop 软件现在应该知道新的静态 IP 地址了。

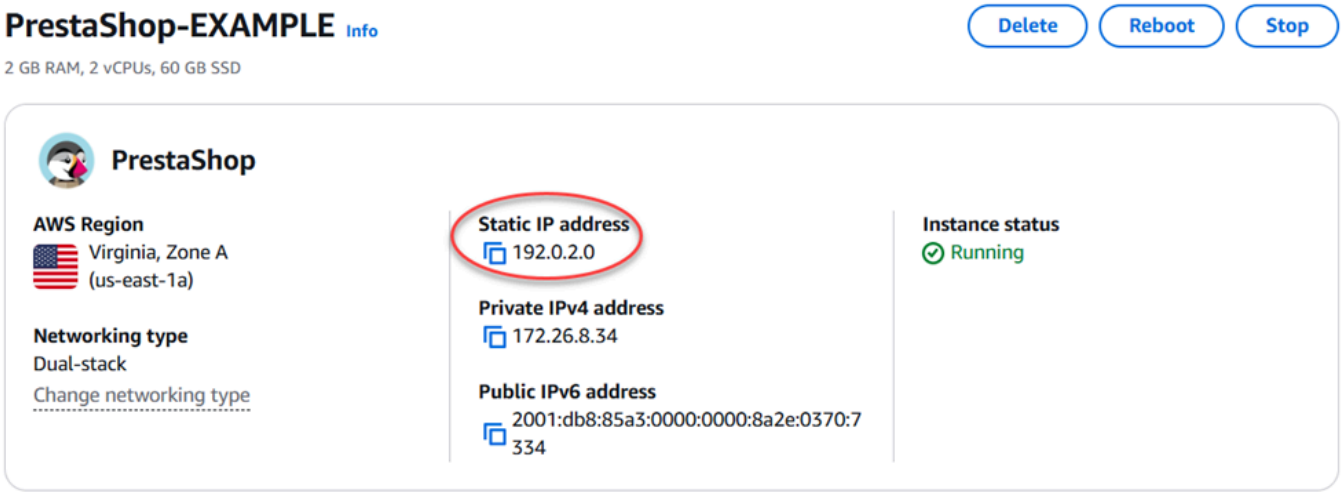
```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

> **Note**
>
> PrestaShop 目前不支持 IPv6 地址。您可以 IPv6 为该实例启用，但该 PrestaShop 软件不会响应通过 IPv6网络发送的请求。

第 3 步：登录 PrestaShop 网站的管理控制面板

完成以下步骤即可访问您的 PrestaShop 网站并登录其管理控制面板。要进行登录，请使用默认用户名 (`user@example.com`) 和您之前在本指南中获取的默认应用程序密码。

1. 在 Lightsail 控制台中，记下实例管理页面标题区域中列出的公共或静态 IP 地址。



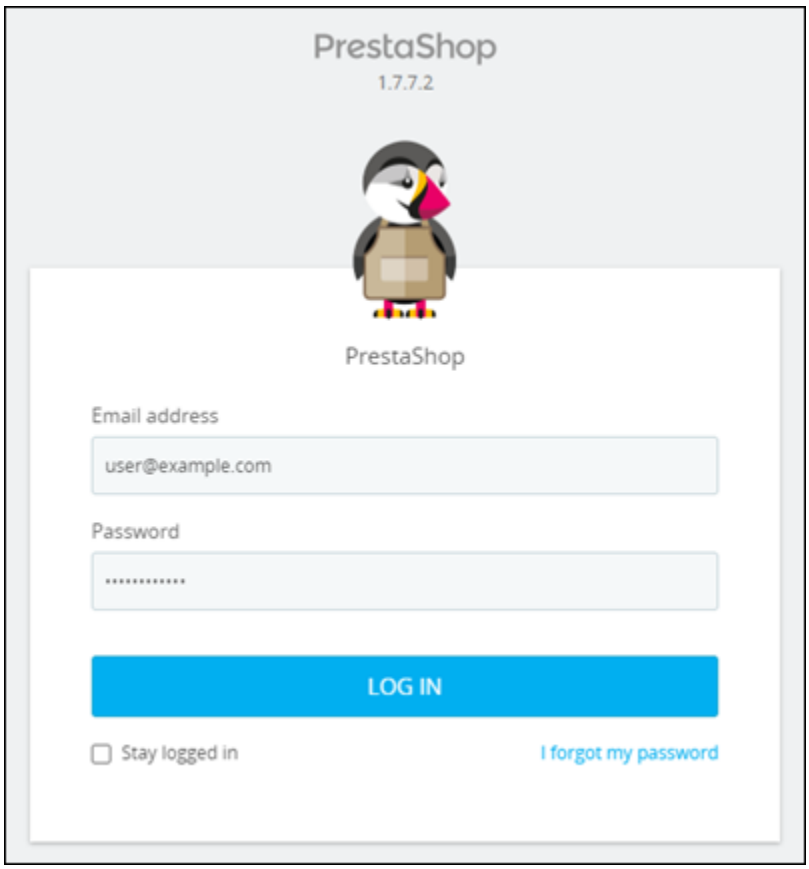
2. 浏览到以下地址以访问您 PrestaShop 网站的管理控制面板的登录页面。请务必*<InstanceIpAddress>*替换为您的实例的公有或静态 IP 地址。

```
http://<InstanceIpAddress>/administration
```

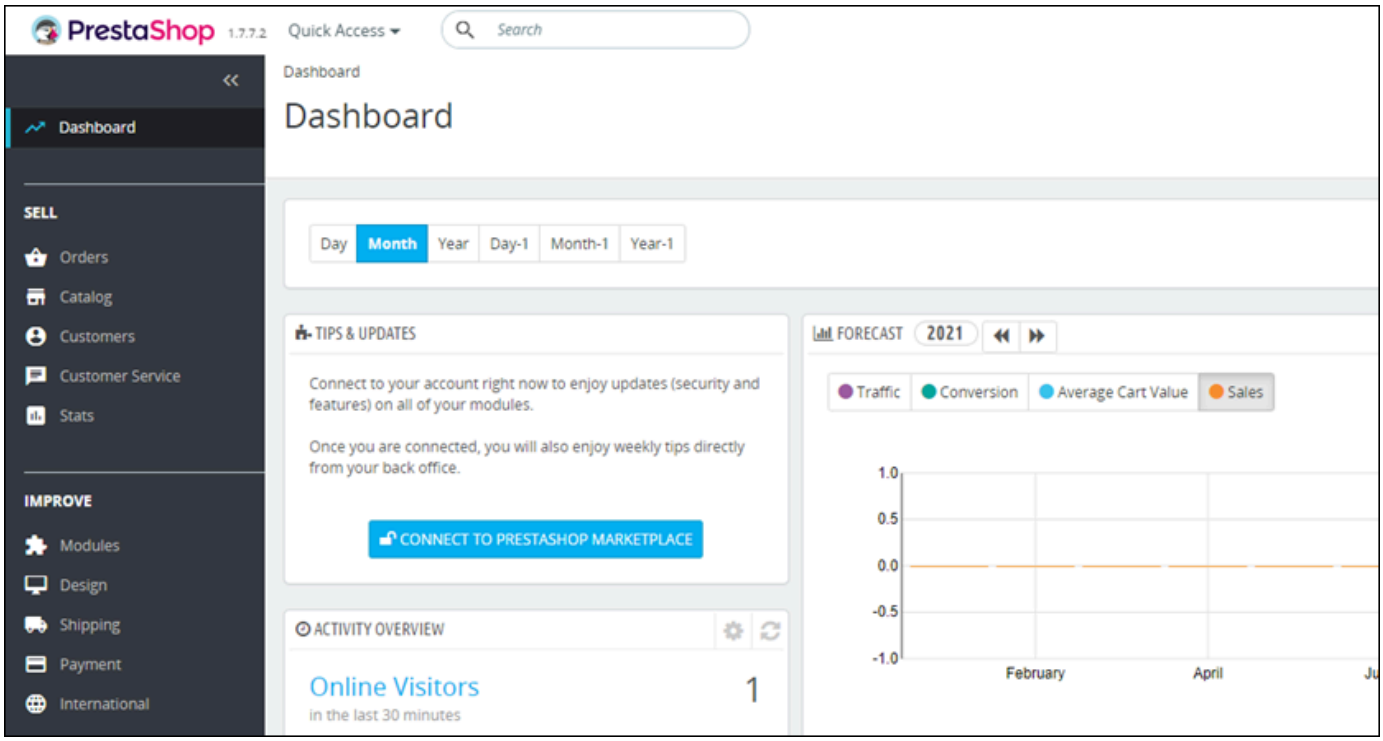
   示例：

```
http://203.0.113.0/administration
```

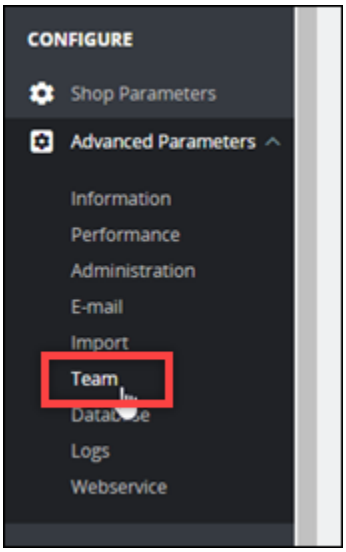
3. 输入默认用户名 (`user@example.com`) 和您之前在本指南中获取的默认应用程序密码，然后选择登录。



将出现 PrestaShop 管理控制面板。



要更改用于登录 PrestaShop 网站管理仪表板的默认用户名或密码，请在导航窗格中选择 “高级参数”，然后选择 “团队”。有关更多信息，请参阅PrestaShop 文档 PrestaShop中的用户指南。



有关管理仪表板的更多信息，请参阅PrestaShop 文档 PrestaShop中的用户指南。

第 4 步：将您注册域名的流量路由到您的 PrestaShop 网站

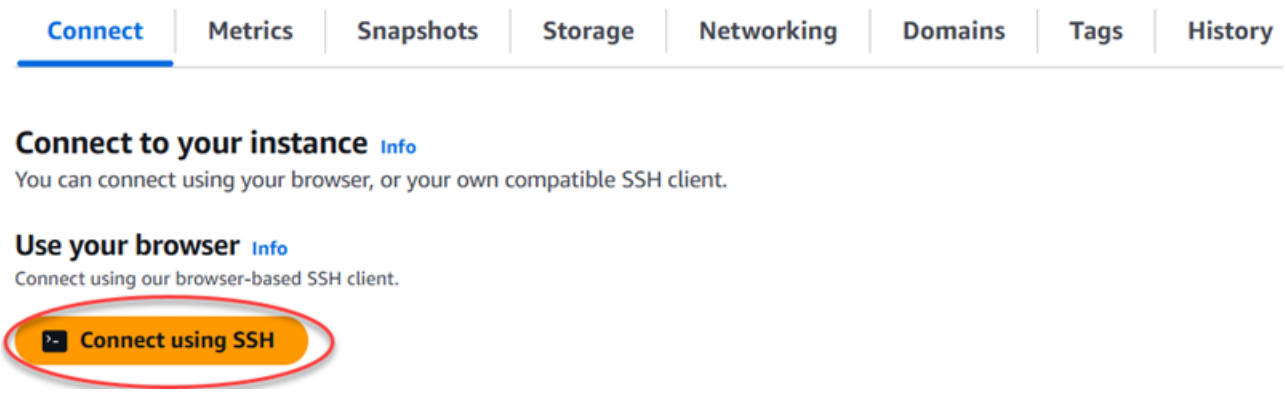
要将您的注册域名的流量（例如`example.com`您的网站）路由到您的 PrestaShop 网站，您需要在域名的域名系统 (DNS) 中添加一条记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。

有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

在您的域名将流量路由到您的实例后，您必须完成以下步骤以使 PrestaShop 软件知道该域名。

1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令。请务必*<DomainName>*替换为将流量路由到您的实例的域名。

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

您应看到类似于以下示例的响应。该 PrestaShop 软件现在应该知道域名了。

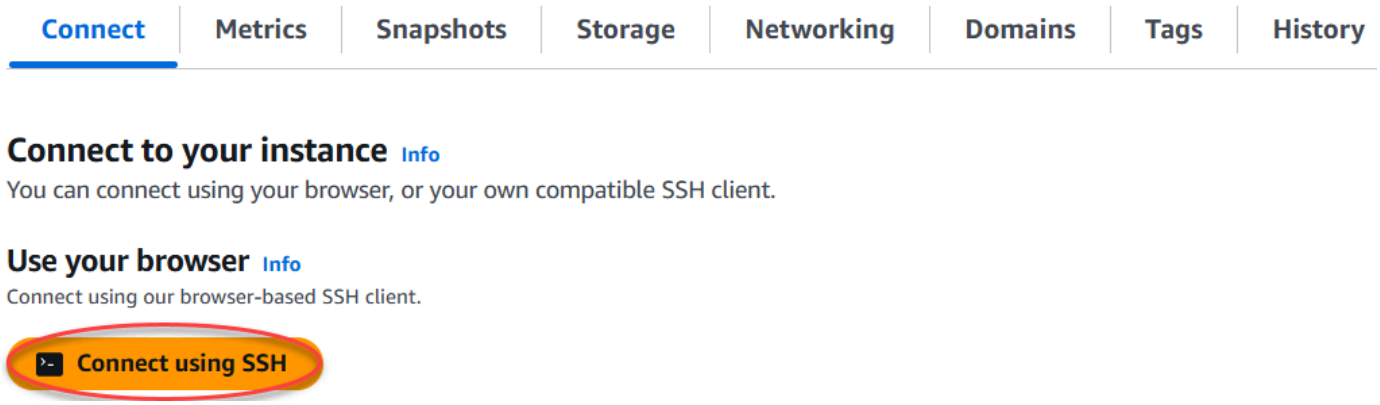
```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

第 5 步：为您的 PrestaShop 网站配置 HTTPS

完成以下步骤，在您的 PrestaShop 网站上配置 HTTPS。这些步骤介绍了如何使用 Bitnami HTTPS 配置工具 (bncert)，该工具是用于请求 SSL/TLS 证书、设置重新导向（例如 HTTP 到 HTTPS）和续订证书的命令行工具。

> **Important**
>
> bncert 工具将仅为当前将流量路由到您的 PrestaShop 实例的公有 IP 地址的域名颁发证书。在开始这些步骤之前，请确保将 DNS 记录添加到要用于 PrestaShop 网站的所有域名的 DNS 中。

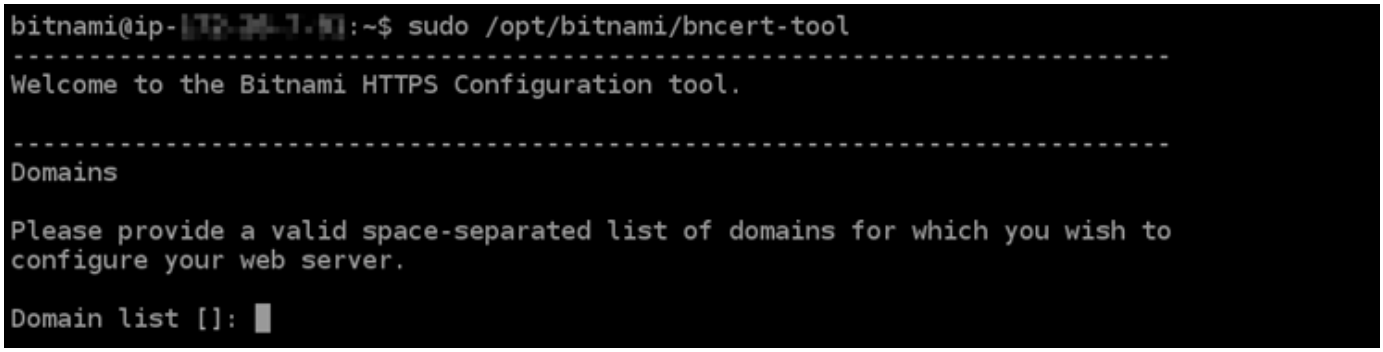
1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



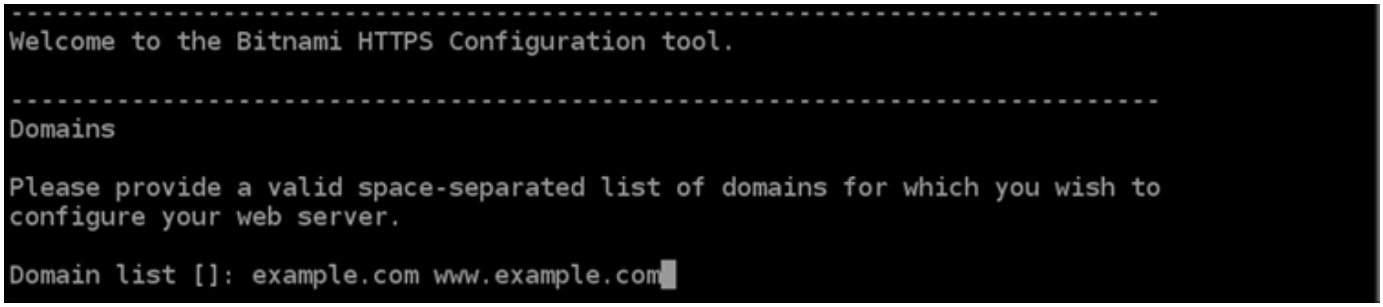
2. 连接后，请输入以下命令来启动 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

您会看到类似于以下示例的响应：



3. 输入用空格分隔的主域名和备用域名，如以下示例所示。



4. bncert 工具会询问您希望如何配置网站的重新导向。以下是可用的选项：

   - 启用 HTTP 重新导向到 HTTPS - 指定是否将浏览网站 HTTP 版本（即 `http://example.com`）的用户自动重新导向到 HTTPS 版本（即 `https://example.com`）。我们建议启用此选项，因为它会强制所有访问者使用加密连接。输入 Y 然后按 Enter 以启用它。

- 启用非 www 重新导向到 www - 指定是否将浏览顶级域（即 `https://example.com`）的用户自动重新导向到域的 www 子域（即 `https://www.example.com`)。我们建议启用此选项。但如果您在搜索引擎工具（如 Google 站点管理员工具）中指定了顶级域作为首选网站地址，或者顶级域直接指向您的 IP 且 www 子域通过别名记录引用您的顶级域，则您可能希望禁用它并启用其他选项（启用 www 重新导向到非 www）。输入 Y 然后按 Enter 以启用它。
- 启用 www 到非 www 重新导向 - 指定是否将浏览域的 www 子域（即 `https://www.example.com`）的用户自动重新导向到顶级域（即 `https://example.com`)。如果您启用了非 www 重新导向到 www，建议禁用此选项。输入 N 然后按 Enter 以禁用它。

您的选择应类似于以下示例：

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y




Enable non-www to www redirection [Y/n]: Y




Enable www to non-www redirection [y/N]: N
```

5. 将列出要进行的更改。输入 Y 然后按 Enter 以确认并继续。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

6. 输入要与 Let's Encrypt 证书关联的电子邮件地址，然后按 Enter（确定键）。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

7. 查看 Let's Encrypt 的加密用户协议 输入 Y 然后按 Enter 接受协议并继续。

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

将执行这些操作以在您的实例上启用 HTTPS，包括请求证书和配置您指定的重新导向。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

您的证书已成功颁发和验证，如果您看到类似于以下示例的消息，则表示在实例上成功配置了重新导向。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

bncert 工具将在证书过期前每 80 天执行一次自动续订。继续执行下一组步骤，完成在您的 PrestaShop 网站上启用 HTTPS。

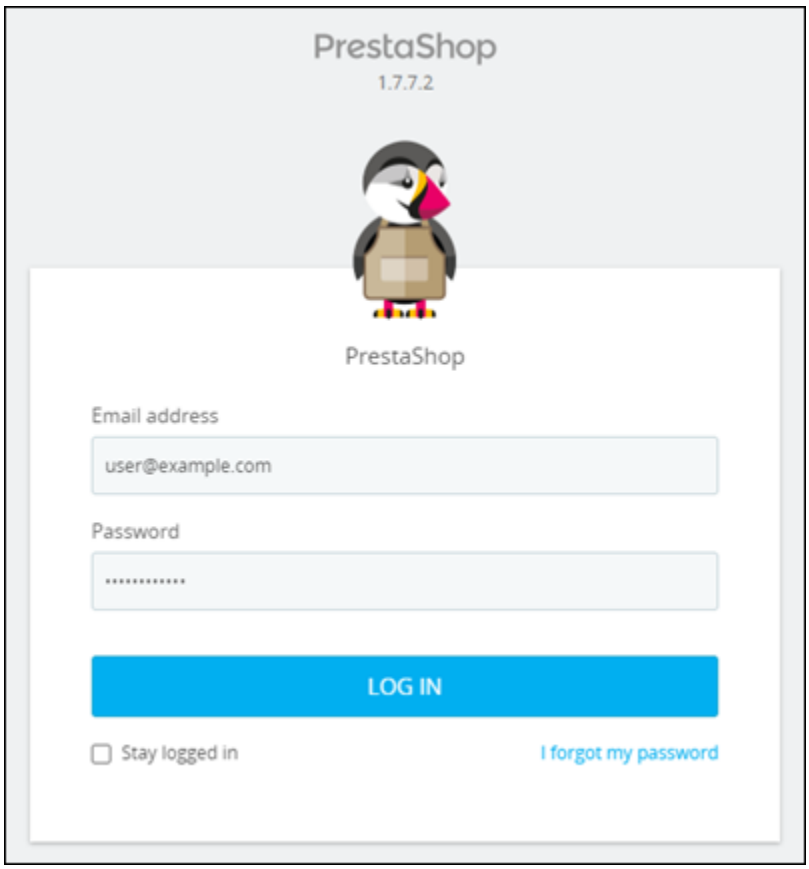
8. 浏览到以下地址以访问您 PrestaShop 网站的管理控制面板的登录页面。请务必*<DomainName>*替换为将流量路由到您的实例的注册域名。

```
http://<DomainName>/administration
```

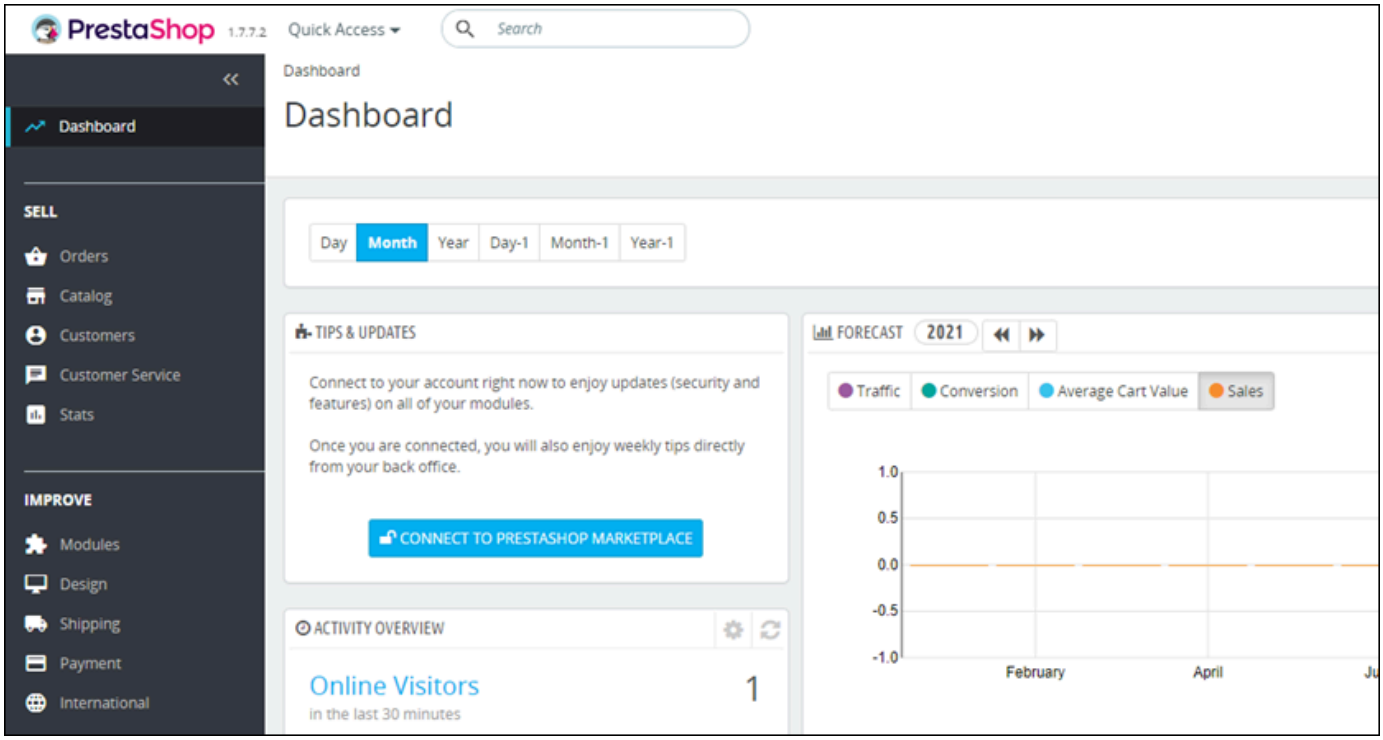
示例：

```
http://www.example.com/administration
```

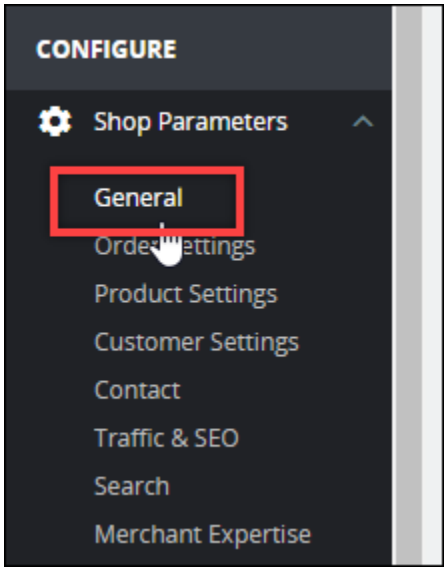
9. 输入默认用户名 (user@example.com) 和您之前在本指南中获取的默认应用程序密码，然后选择登录。



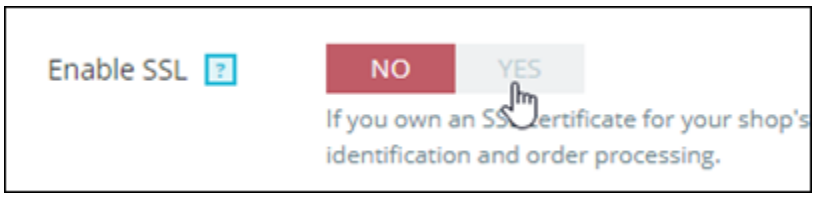
将出现 PrestaShop 管理控制面板。



10. 在导航窗格中选择 Shop 参数，然后选择常规。



11. 选择启用 SSL 旁边的是。



12. 滚动到页面底部并选择 Save (保存)。

13. 常规页面重新加载后，选择在所有页面上启用 SSL 旁边的是。

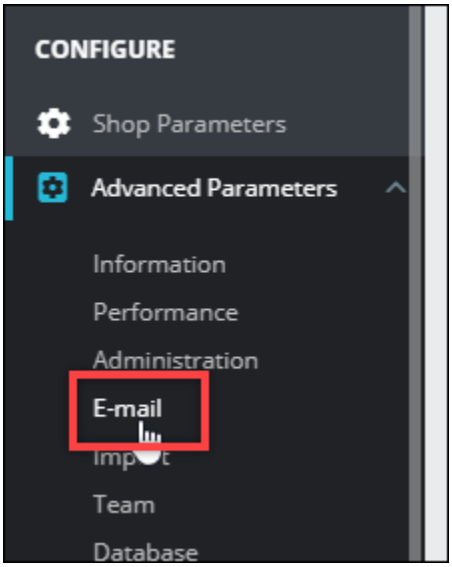


14. 滚动到页面底部并选择 Save (保存)。

    您的 PrestaShop 网站现在已经配置好了 HTTPS。当客户浏览您的 PrestaShop 网站的 HTTP 版本（例如`http://www.example.com`）时，他们将被自动重定向到 HTTPS 版本（例如`https://www.example.com`）。

步骤 6：配置电子邮件通知的 SMTP

配置 PrestaShop 网站的 SMTP 设置以为其启用电子邮件通知。为此，请登录您 PrestaShop 网站的管理控制面板。在导航窗格中选择高级参数，然后选择电子邮件。您还应相应地调整电子邮件联系人。要执行此操作，请在导航窗格中选择 Shop Parameters（Shop 参数），然后选择 Contact（联系人）。



有关更多信息，有关更多信息，请参阅文档 PrestaShop中的用户指南和 Bitnami PrestaShop 文档中的为出站电子邮件配置 SMTP。

> **Important**
>
> 如果您将 SMTP 配置为使用端口 25、465 或 587，则必须在 Lightsail 控制台中打开实例防火墙中的这些端口。有关更多信息，请参阅在 Amazon Lightsail 中添加和编辑实例防火墙规则。

如果您将 Gmail 帐户配置为在 PrestaShop 网站上发送电子邮件，则必须使用应用程序密码，而不是使用登录 Gmail 时使用的标准密码。有关更多信息，请参阅使用应用程序密码登录。

第 7 步：阅读 Bitnami 和文档 PrestaShop

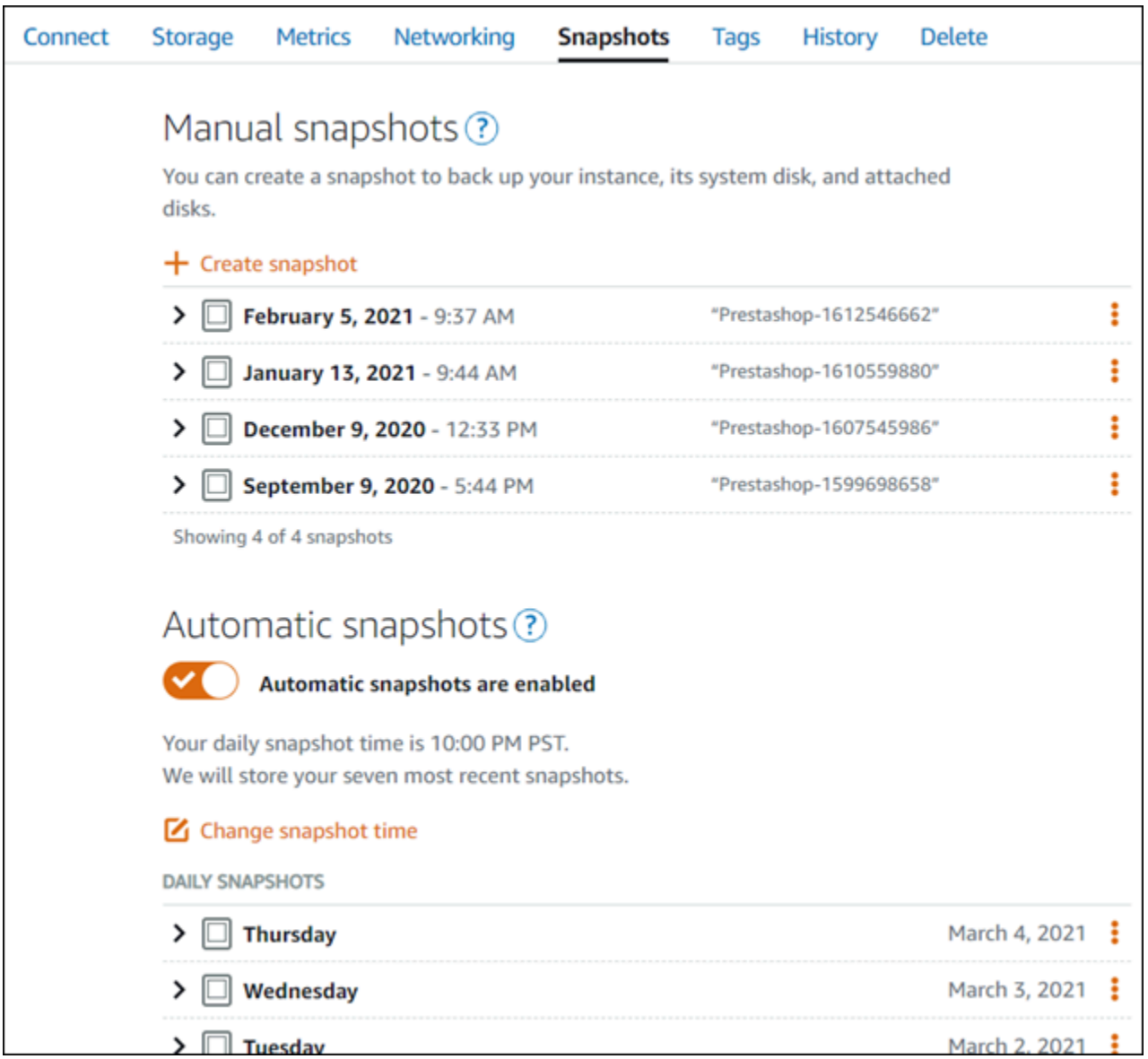
阅读 Bitnami 文档，了解如何在您的 PrestaShop 实例和网站上执行管理任务，例如安装插件和自定义主题。有关更多信息，请参阅 Bitnami 文档中的 AWS 云版 Bit nami PrestaShop 堆栈。

您还应该阅读 PrestaShop 文档，了解如何管理您的 PrestaShop 网站。有关更多信息，请参阅PrestaShop 文档 PrestaShop中的用户指南。

步骤 8：为您的 PrestaShop 实例创建快照

按照您想要的方式配置 PrestaShop 网站后，请定期创建实例快照以对其进行备份。您可以手动创建快照，也可以启用自动快照，让 Lightsail 为您创建每日快照。如果实例出现错误，则可使用快照来创建新的替代实例。有关更多信息，请参阅快照。

在实例管理页面的快照选项卡下，选择创建快照或选择启用自动快照。



有关更多信息，请参阅在 Amazon Lightsail 中创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。

在 Lightsail 上配置和保护 Redmine 实例

在你的 Redmine 实例在 Amazon Lightsail 上启动并运行之后，你应该采取以下几个步骤来开始使用：

内容

- 步骤 1：阅读 Bitnami 文档
- 步骤 2：获取默认应用程序密码以访问 Redmine 管理控制面板
- 步骤 3：将静态 IP 地址附加到实例

- 步骤 4：登录到 Redmine 网站的管理控制面板
- 步骤 5：将注册域名的流量路由到 Redmine 网站
- 步骤 6：配置 Redmine 网站的 HTTPS
- 步骤 7：阅读 Redmine 文档并继续配置网站
- 步骤 8：创建实例的快照

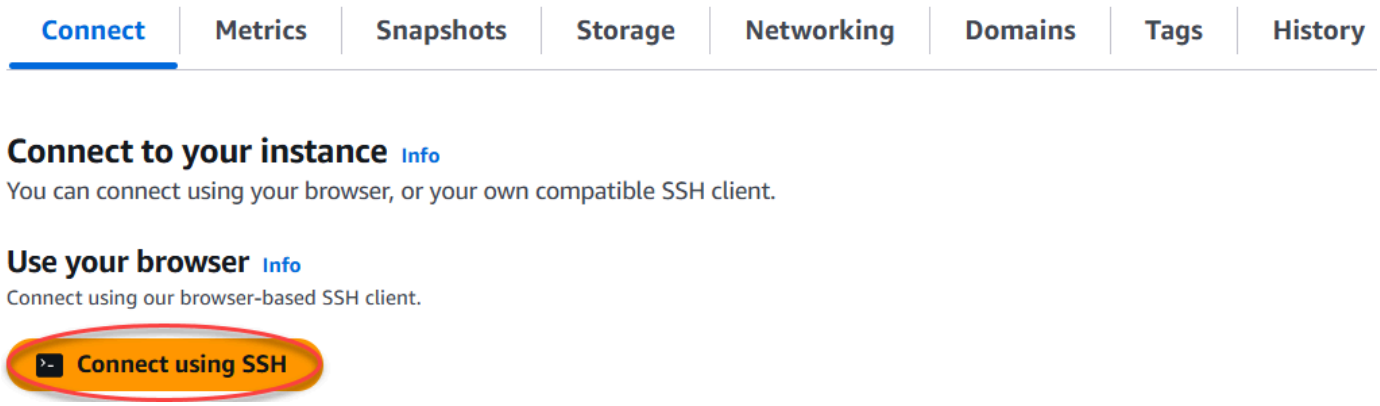
步骤 1：阅读 Bitnami 文档

阅读 Bitnami 文档以了解如何配置 Redmine 应用程序。有关更多信息，请参阅 Bitnami 为 AWS Cloud 打包的 Redmine。

步骤 2：获取默认应用程序密码以访问 Redmine 管理控制面板

完成以下程序以获取访问 Redmine 网站的管理控制面板所需的默认应用程序密码。有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

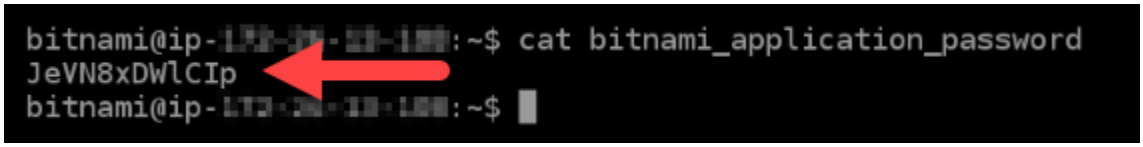
1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来获取应用程序密码：

```
cat $HOME/bitnami_application_password
```

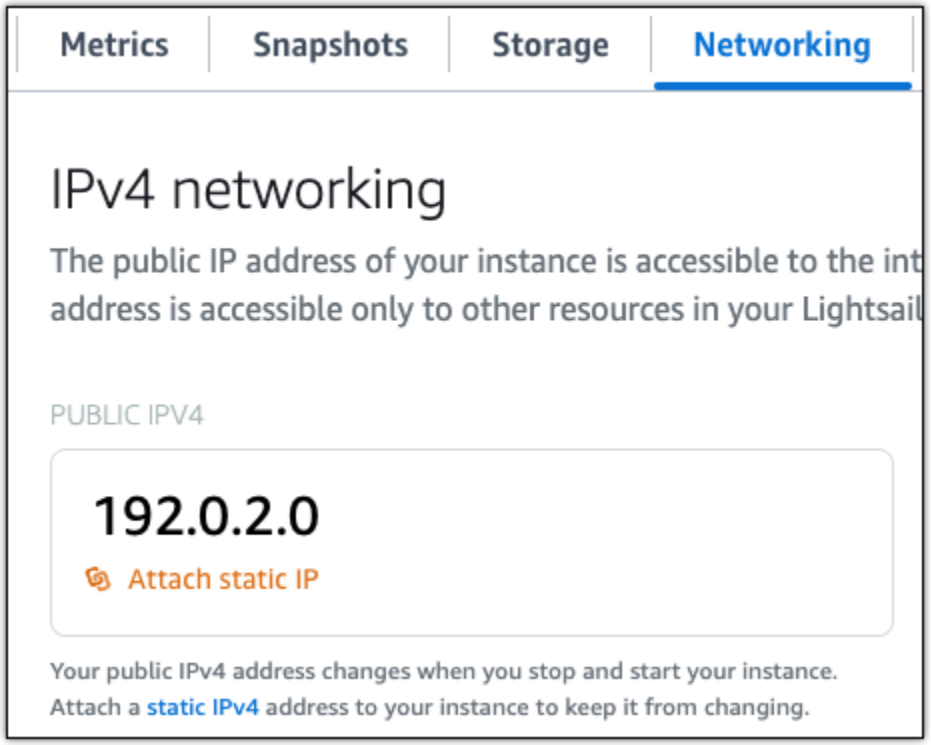
您应该会看到与以下示例类似的响应，其中包含默认应用程序密码：



步骤 3：将静态 IP 地址附加到实例

在您首次创建实例时分配给实例的公有 IP 地址会在您每次停止和启动实例时发生更改。您应为实例创建和附加静态 IP 地址，以确保其公有 IP 地址不变。之后当您将注册域名（如 `example.com`）指向实例时，无需在每次停止和重启实例时都更新域的 DNS 记录。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择创建静态 IP或附加静态 IP（如果您之前创建了可附加到实例的静态 IP），然后按照页面上的说明操作。有关更多信息，请参阅创建静态 IP 并将其附加到实例。



步骤 4：登录到 Redmine 网站的管理控制面板

现在您已有默认应用程序密码，请完成以下程序，以导航到 Redmine 网站的主页，然后登录管理控制面板。登录后，您可以开始自定义网站并进行管理更改。有关您可以在 Joomla! 中执行的操作的更多信息，请参阅本指南后面部分中的步骤 7：阅读 Redmine 文档并继续配置网站一节。

1. 在实例管理页面上的 Connect（连接）选项卡下，记下实例的公有 IP 地址。公有 IP 地址也显示在实例管理页面的标题部分。



2. 浏览到实例的公有 IP 地址，例如，转到 `http://203.0.113.0`。

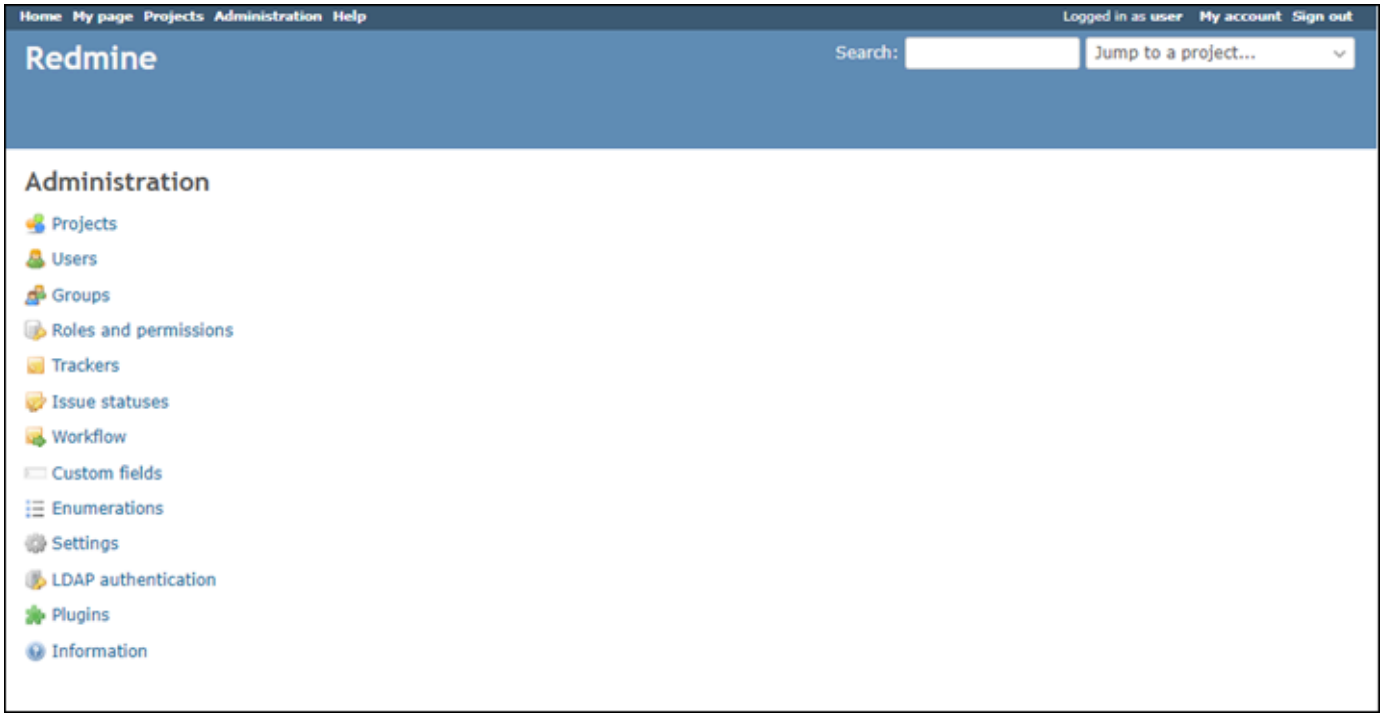
应该会出现您的 Redmine 网站的主页。

3. 选择 Redmine 网站主页右下角的 Manage（管理）。

   如果 Manage（管理）横幅未显示，您可以通过浏览 `http://<PublicIP>/admin` 到达登录页面。将 *<PublicIP>* 替换为实例的公有 IP 地址。

4. 使用之前在本指南中检索到的默认用户名（`user`）和默认密码登录。

   此时将显示 Redmine 管理控制面板。



步骤 5：将注册域名的流量路由到 Redmine 网站

要将注册域名（如 `example.com`）的流量路由到 Redmine 网站，您需要向域的 DNS 添加记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

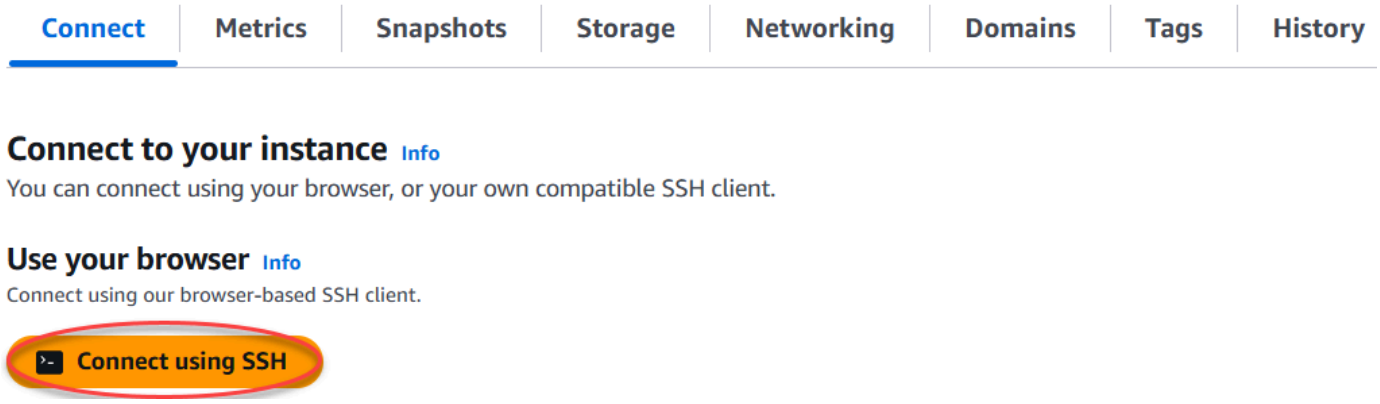
如果您浏览到为实例配置的域名，则应将您重定向到 Redmine 网站的主页。接下来，您应该生成并配置 SSL/TLS 证书，以启用 Redmine 网站的 HTTPS 连接。有关更多信息，请继续到本指南的下一节步骤 6：配置 Redmine 网站的 HTTPS。

步骤 6：配置 Redmine 网站的 HTTPS

完成以下程序以在 Redmine 网站上配置 HTTPS。这些步骤向您展示如何使用 Bitnami HTTPS 配置工具（`bncert-tool`），这是一个命令行工具，用于请求 Let's Encrypt SSL/TLS 证书。有关更多信息，请参阅 Bitnami 文档中的了解 Bitnami HTTPS 配置工具。

> **Important**
>
> 在开始此过程之前，请确保对域进行配置，以将流量路由到 Redmine 实例。否则，SSL/TLS 证书验证过程将失败。

1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，输入以下命令以确认 bncert 工具已安装在实例上。

```
sudo /opt/bitnami/bncert-tool
```

   您应看到以下响应之一：

   - 如果您在响应中看到命令未找到，则 bncert 工具未安装到实例上。继续执行此过程的后续步骤以在实例上安装 bncert 工具。
   - 如果您在响应中看到欢迎使用 Bitnami HTTPS 配置工具，则 bncert 工具已安装到实例上。继续执行此过程的步骤 8。
   - 如果 bncert 工具已在您的实例上安装了一段时间，那么您可能会看到一条消息，指示该工具的更新版本可供使用。选择进行下载，然后再次输入 `sudo /opt/bitnami/bncert-tool` 命令来运行 bncert 工具。继续执行此过程的步骤 8。

3. 输入以下命令以将 bncert 运行文件下载到您的实例中。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. 输入以下命令以在您的实例上创建 bncert 工具运行文件的目录。

```
sudo mkdir /opt/bitnami/bncert
```

5. 输入以下命令以创建可作为程序执行的 bncert 运行文件。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 输入以下命令以创建符号链接，该符号链接在您输入 sudo /opt/bitnami/bncert-tool 命令时运行 bncert 工具。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

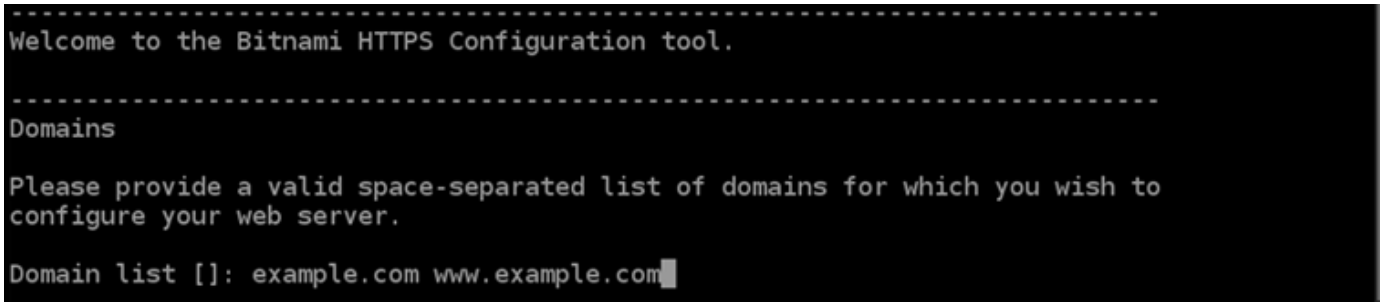
您现在已完成在实例上安装 bncert 工具的步骤。

7. 要运行 bncert 工具，请输入以下命令。

```
sudo /opt/bitnami/bncert-tool
```

8. 输入用空格分隔的主域名和备用域名，如以下示例所示。

如果您的域未配置为将流量路由到实例的公有 IP 地址，则 bncert 工具将要求您在继续之前进行该配置。您的域必须将流量路由到使用 bncert 工具以在实例上启用 HTTPS 的实例的公有 IP 地址。这将确认您拥有该域，并能用于进行证书的验证。



9. bncert 工具会询问您希望如何配置网站的重新导向。以下是可用的选项：

- 启用 HTTP 重新导向到 HTTPS - 指定是否将浏览网站 HTTP 版本（即 http:/example.com）的用户自动重新导向到 HTTPS 版本（即 https://example.com)。我们建议启用此选项，因为它会强制所有访问者使用加密连接。输入 Y 然后按 Enter 以启用它。

- 启用非 www 重新导向到 www - 指定是否将浏览顶级域（即 `https://example.com`）的用户自动重新导向到域的 www 子域（即 `https://www.example.com`)。我们建议启用此选项。但如果您在搜索引擎工具（如 Google 站点管理员工具）中指定了顶级域作为首选网站地址，或者顶级域直接指向您的 IP 且 www 子域通过别名记录引用您的顶级域，则您可能希望禁用它并启用其他选项（启用 www 重新导向到非 www）。输入 Y 然后按 Enter 以启用它。
- 启用 www 到非 www 重新导向 - 指定是否将浏览域的 www 子域（即 `https://www.example.com`）的用户自动重新导向到顶级域（即 `https://example.com`)。如果您启用了非 www 重新导向到 www，建议禁用此选项。输入 N 然后按 Enter 以禁用它。

您的选择应类似于以下示例：

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y




Enable non-www to www redirection [Y/n]: Y




Enable www to non-www redirection [y/N]: N
```

10. 将列出要进行的更改。输入 Y 然后按 Enter 以确认并继续。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. 输入要与 Let's Encrypt 证书关联的电子邮件地址，然后按 Enter（确定键）。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

12. 查看 Let's Encrypt 的加密用户协议 输入 Y 然后按 Enter 接受协议并继续。

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

将执行这些操作以在您的实例上启用 HTTPS，包括请求证书和配置您指定的重新导向。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

您的证书已成功颁发和验证，如果您看到类似于以下示例的消息，则表示在实例上成功配置了重新导向。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

`bncert` 工具将在证书过期前每 80 天执行一次自动续订。如果您希望将其他域和子域用于实例，并且希望为这些域启用 HTTPS，请重复上述步骤。

您现在已完成在您的 Redmine 实例上启用 HTTPS。下次使用配置的域浏览到 Redmine 网站时，您应该会看到它重定向到 HTTPS 连接。

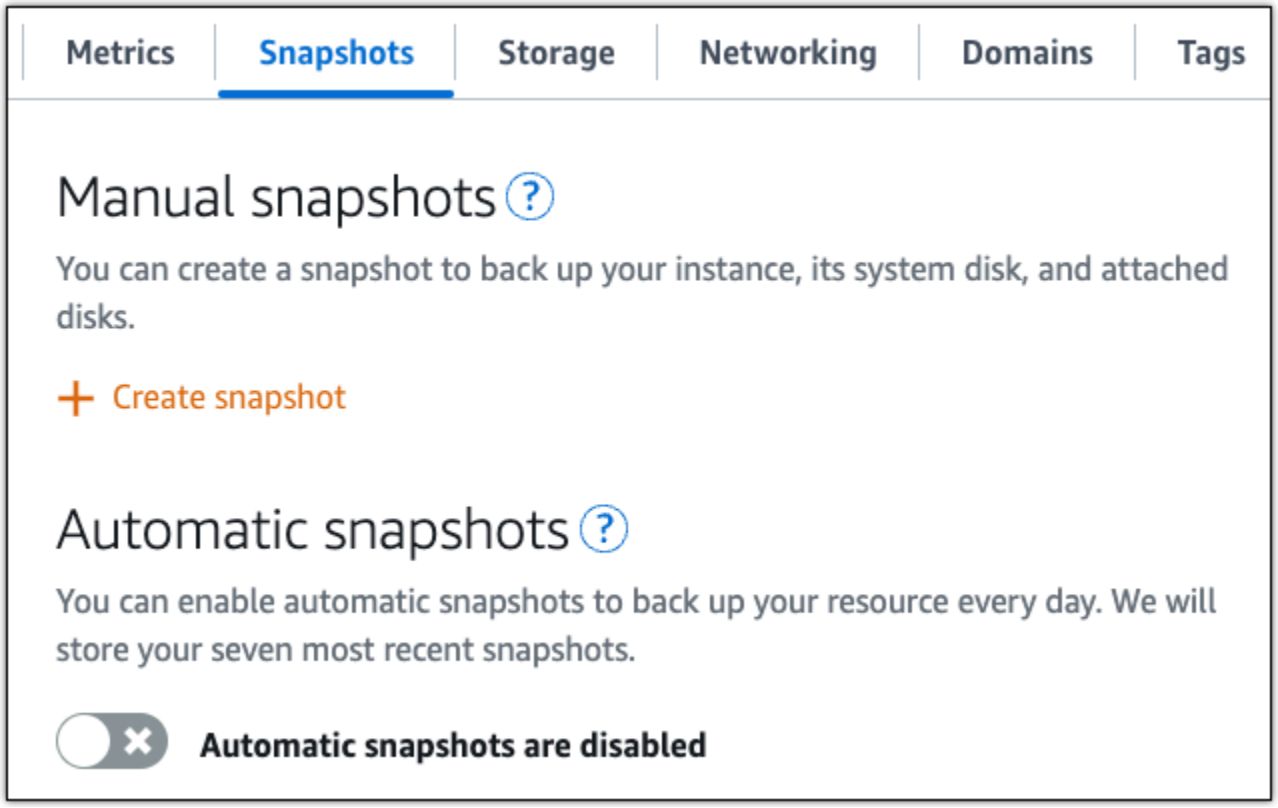
步骤 7：阅读 Redmine 文档并继续配置网站

阅读 Redmine 文档，了解如何管理和自定义网站。有关更多信息，请参阅《Redmine 指南》。

步骤 8：创建实例的快照

按照您所需的方式配置 Redmine 网站后，创建实例的定期快照以进行备份。您可以手动创建快照，也可以启用自动快照，让 Lightsail 为您创建每日快照。如果实例出现错误，则可使用快照来创建新的替代实例。有关更多信息，请参阅快照。

在实例管理页面的快照选项卡下，选择创建快照或选择启用自动快照。



有关更多信息，请参阅在 Amazon Lightsail 中创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。

在 Lightsa WordPress il 上启动和配置

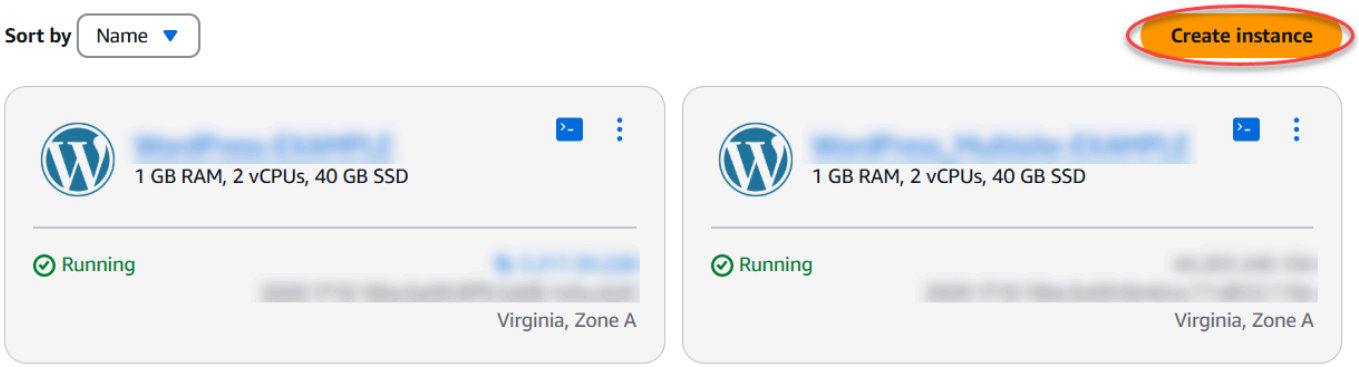
通过这份快速入门指南，您将学习如何在 Amazon Lightsail 上启动和配置 WordPress 实例。

步骤 1：创建 WordPress实例

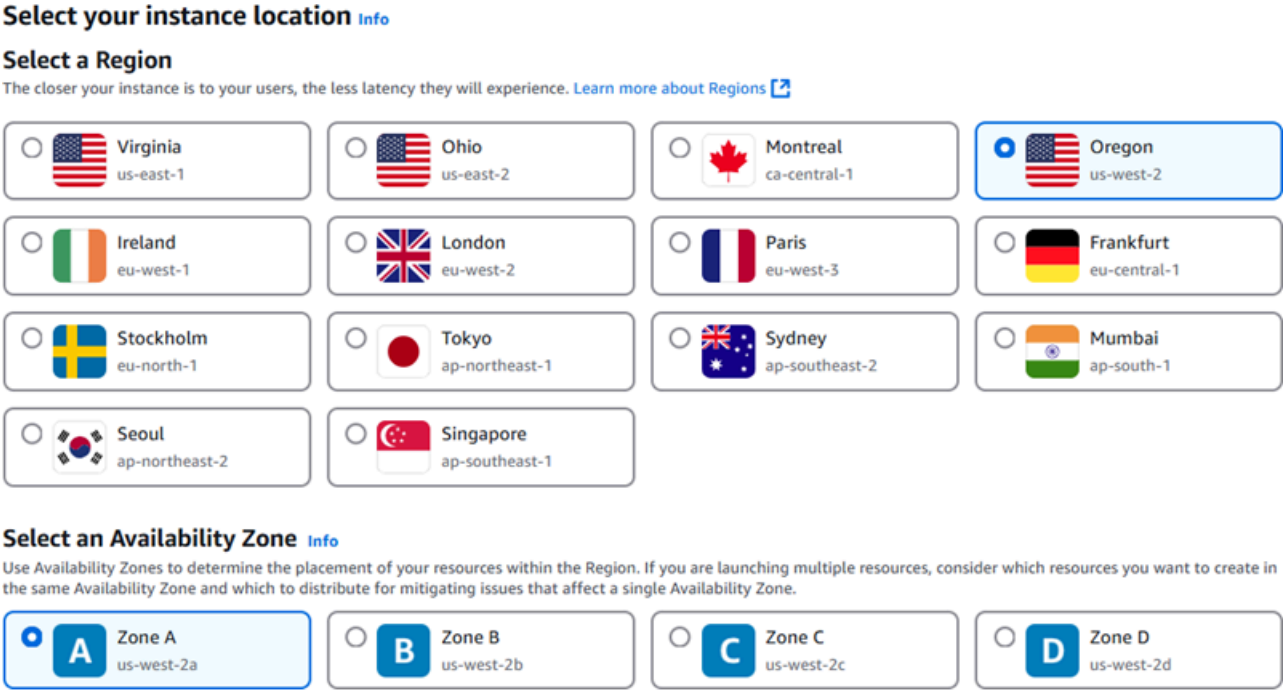
完成以下步骤以启动并运行您的 WordPress 实例。

为创建 Lightsail 实例 WordPress

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的实例部分，选择创建实例。



3. 为您的实例选择 AWS 区域 和可用区。



4. 为您的实例选择映像，如下所示：

a. 在选择平台中，选择 Linux/Unix。

b. 对于选择蓝图，选择WordPress。

5. 选择实例计划。

   计划包括采用可预测低成本的计算机配置（RAM、SSD、vCPU）以及数据传输限额。

6. 输入实例的名称。资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

7. 选择创建实例。

8. 要查看测试博客文章，请转到实例管理页面并复制页面右上角显示的公共 IPv4 地址。将该地址粘贴到已连接 Internet 的 Web 浏览器的地址栏中。浏览器显示测试博客文章。

步骤 2：配置您的 WordPress实例

您可以使用配置以下内容的指导式 step-by-step工作流程来配置您的 WordPress 实例：

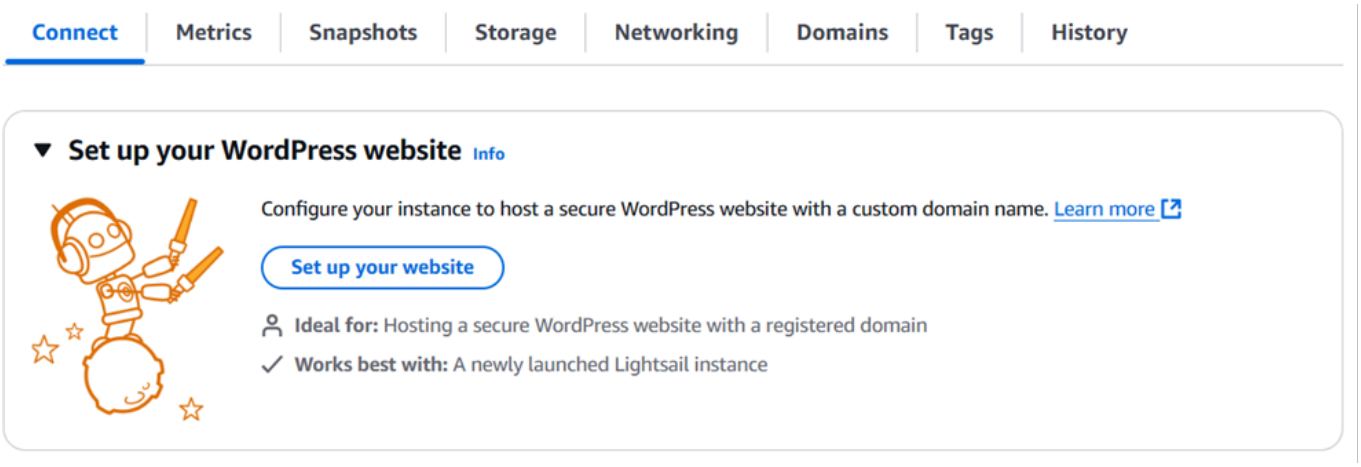
- 注册域名-您的 WordPress 网站需要一个易于记忆的域名。用户将指定此域名来访问您的 WordPress 网站。有关更多信息，请参阅 域和 DNS。
- DNS 管理 – 您必须决定如何管理域的 DNS 记录。DNS 记录将域（或子域）所关联的 IP 地址或主机名告知 DNS 服务器。DNS 区域包含域的 DNS 记录。有关更多信息，请参阅 the section called “Lightsail 中的 DNS”。
- 静态 IP 地址-如果您停止并启动实例，则 WordPress 实例的默认公有 IP 地址会发生变化。当您向实例附加静态 IP 地址时，即使您停止和启动实例，该 IP 地址也会保持不变。有关更多信息，请参阅 the section called “IP 地址”。
- SSL/TLS 证书-创建经过验证的证书并将其安装在实例上后，您可以为您的 WordPress 网站启用 HTTPS，以便使用 HTTPS 加密通过您的注册域路由到实例的流量。有关更多信息，请参阅 the section called “启用 HTTPS”。

> **Tip**
>
> 在开始之前，请查看以下提示。有关故障排除信息，请参阅故障排除 WordPress 设置。

- 安装程序支持 2023 年 1 月 1 日之后创建的 WordPress 版本 6 及更高版本的 Lightsail 实例。
- 设定期间运行的 Certbot 依赖项文件、HTTPS 重写脚本和证书续订脚本保存在您实例上的 `/opt/bitnami/lightsail/scripts/` 目录中。
- 该实例必须处于运行中状态。如果实例刚刚启动，请等待几分钟，让 SSH 连接准备就绪。
- 在设定运行期间，实例防火墙上的端口 22、80 和 443 必须允许来自任何 IP 地址的 TCP 连接。有关更多信息，请参阅实例防火墙。
- 当您添加或更新指向来自顶级域（`example.com`）及其 `www` 子域（`www.example.com`）的流量的 DNS 记录时，它们需要在整个 Internet 中传播。您可以使用诸如 nslookup 或 DNS 查找之类的工具来验证您的 DN S 更改是否已生效。MxToolbox
- 在 2023 年 1 月 1 日之前创建的 Wordpress 实例可能包含已弃用的 Certbot 个人程序包存档（PPA）存储库，这将导致网站设置失败。如果在设置过程中存在此存储库，则会将其从现有路径中移除并备份到实例上的以下位置：`~/opt/bitnami/lightsail/repo.backup`。有关已弃用的 PPA 的更多信息，请参阅 Canonical 网站上的 Certbot PPA。
- Let's Encrypt 证书将每 60 到 90 天自动续订一次。
- 在设置过程中，请勿停止或更改您的实例。配置您的实例可能最多需要 15 分钟。您可以在“实例连接”选项卡中查看每个步骤的进度。

要使用网站设置向导配置您的实例

1. 在实例管理页面的连接选项卡上，选择设置网站。



2. 对于指定域名，请使用现有的 Lightsail 托管域，向 Lightsail 注册新域名，或者使用您通过其他域名注册商注册的域名。选择使用此域进入下一步。

3. 对于配置 DNS，请执行以下操作之一：
   - 选择 Lightsail 托管域以使用 Lightsail DNS 区域。选择使用此 DNS 区域进入下一步。
   - 选择第三方域以使用管理域的 DNS 记录的托管服务。请注意，我们会在您的 Lightsail 账户中创建一个匹配的 DNS 区域，以备您以后决定使用该区域。选择使用第三方 DNS 进入下一步。
4. 在创建静态 IP 地址中，输入静态 IP 地址的名称，然后选择创建静态 IP。
5. 在管理域分配中，选择添加分配，选择域类型，然后选择添加。选择继续进入下一步。
6. 在创建 SSL/TLS 证书中，选择您的域和子域，输入电子邮件地址，选择我授权 Lightsail 在我的实例上配置 Let's Encrypt 证书，然后选择创建证书。我们开始配置 Lightsail 资源。

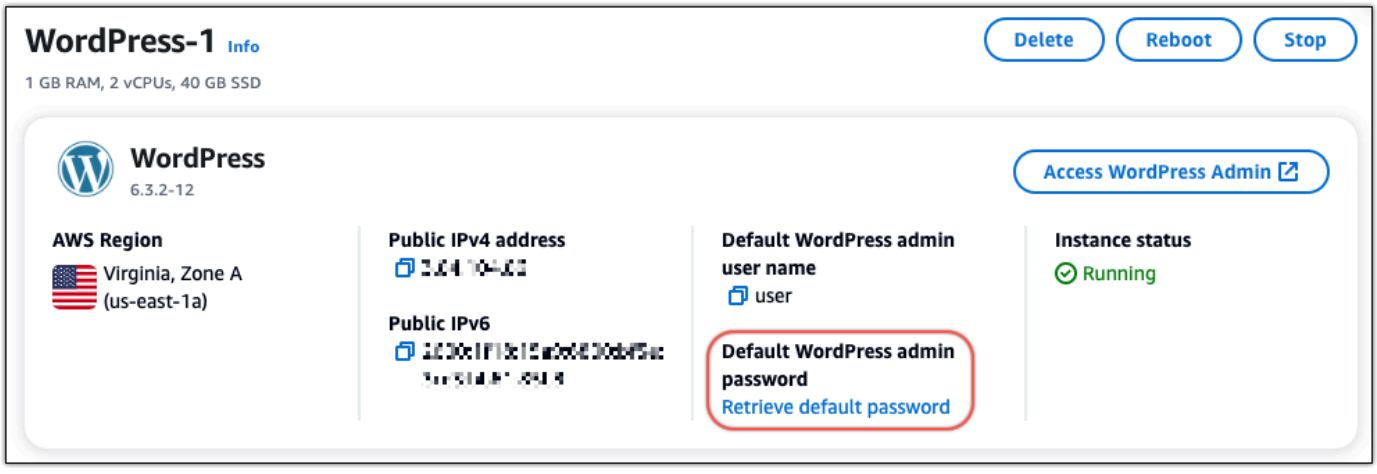
   在设置过程中，请勿停止或更改您的实例。配置您的实例可能最多需要 15 分钟。您可以在“实例连接”选项卡中查看每个步骤的进度。
7. 网站设置完成后，请 URLs 确认您在域名分配步骤中指定的已打开您的 WordPress 网站。

第 3 步：获取 WordPress 网站的默认应用程序密码

您需要使用默认的应用程序密码才能登录 WordPress 网站的管理控制面板。

获取 WordPress 管理员的默认密码

1. 打开您的实例的 WordPress 实例管理页面。
2. 在WordPress面板上，选择找回默认密码。这将在页面底部展开访问默认密码。



3. 选择启动 CloudShell。这将在页面底部打开面板。
4. 选择 “复制”，然后将内容粘贴到 CloudShell 窗口中。您可以将光标放在 CloudShell 提示符处并按 Ctrl+V，也可以右键单击打开菜单，然后选择 “粘贴”。

5. 记下 CloudShell 窗口中显示的密码。您需要使用它来登录 WordPress 网站的管理控制面板。

```
[cloudshell-user@ip-[redacted] ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_applic
ation_password
JKzh8wB5FAR!
```

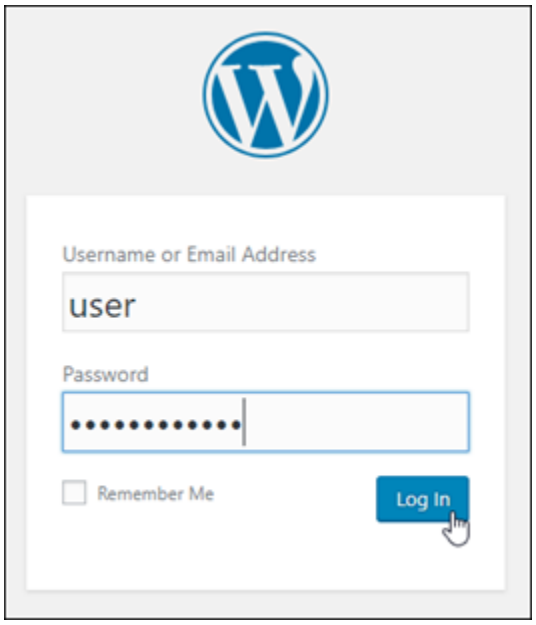
第 4 步：登录您的 WordPress网站

现在，您已经有了默认的用户密码，请导航到 WordPress 网站的主页，然后登录到管理控制面板。登录后，您可以更改默认密码。

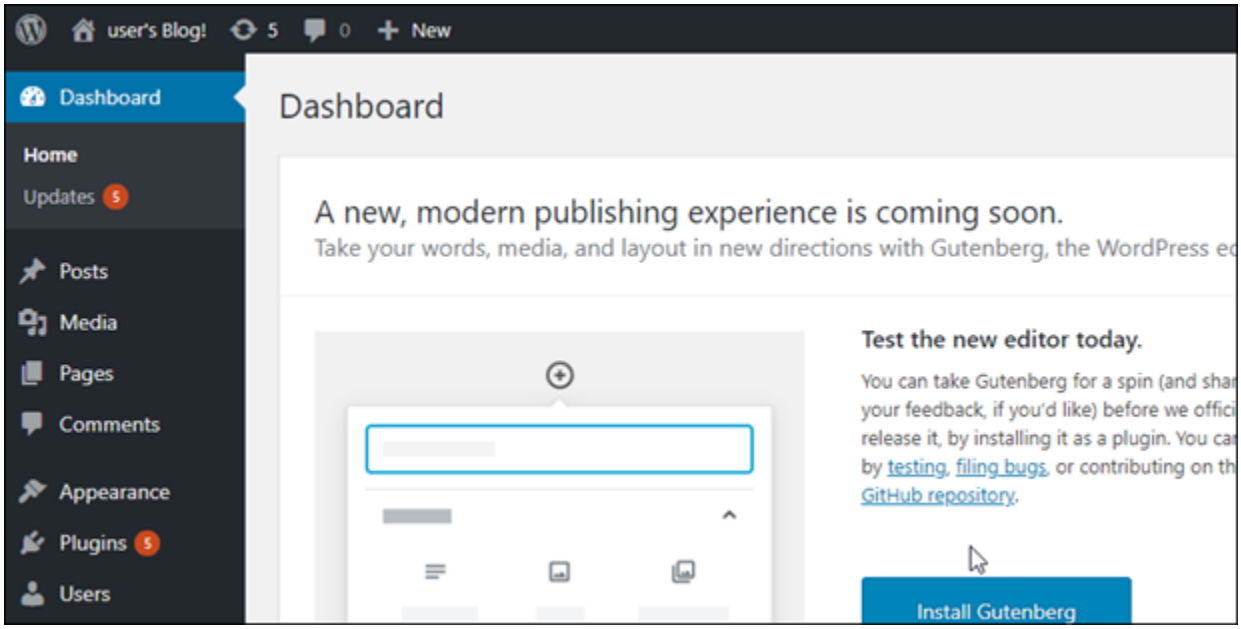
要登录管理控制面板

1. 打开您的实例的 WordPress 实例管理页面。
2. 在WordPress面板上，选择访问 WordPress 管理员。
3. 在 “访问您的 WordPress 管理员控制面板” 面板的 “使用公有 IP 地址” 下，选择以下格式的链接：

   http://*public-ipv4-address*。 /wp-admin
4. 在用户名或电子邮件地址中，输入 **user**。
5. 在密码中，输入在上一步中获得的密码。
6. 选择登录。



现在，您已登录 WordPress 网站的管理控制面板，可以在其中执行管理操作。有关管理 WordPress 网站的更多信息，请参阅 WordPress 文档中的 WordPressCodex。



步骤 5：阅读 Bitnami 文档

阅读 Bitnami 文档，了解如何在您的 WordPress 网站上执行管理任务，例如安装插件、自定义主题和升级您的版本。 WordPress

有关更多信息，请参阅 Bitnami WordPress 的。 AWS Cloud

在 Lightsail 上设置 WordPress多站点

在您的 WordPress 多站点实例启动并在 Amazon Lightsail 上运行后，您应该采取以下几个步骤来开始使用：

内容

- 步骤 1：阅读 Bitnami 文档
- 步骤 2：获取访问 WordPress管理仪表板的默认应用程序密码
- 步骤 3：将静态 IP 地址附加到实例
- 第 4 步：登录您的 WordPress 多站点网站的管理控制面板
- 第 5 步：将您注册域名的流量路由到您的 WordPress多站点网站
- 第 6 步：将博客作为域名或子域名添加到您的 WordPress 多站点网站
- 第 7 步：阅读 WordPress 多站点文档并继续配置您的网站
- 步骤 8：创建实例的快照

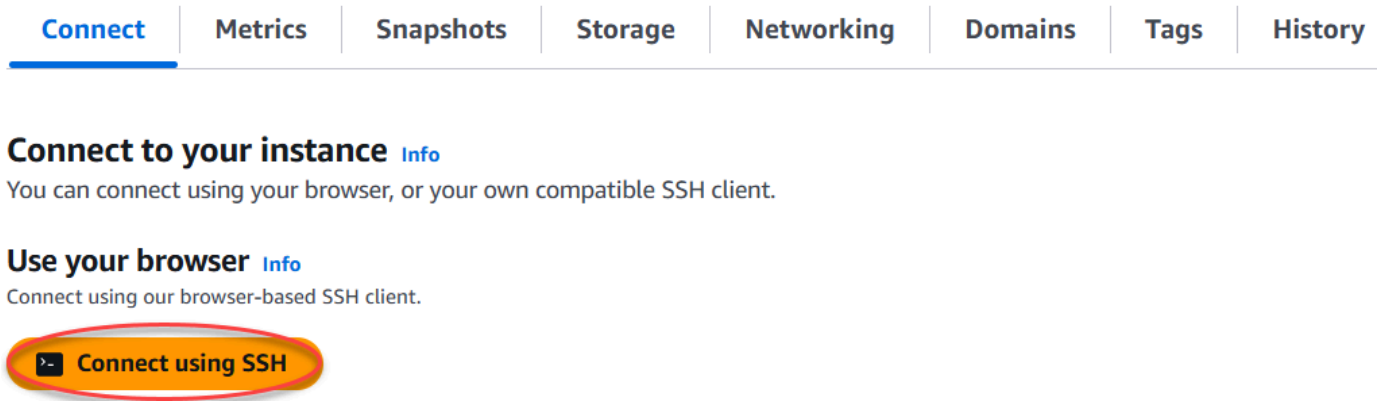
步骤 1：阅读 Bitnami 文档

阅读 Bitnami 文档，了解如何配置您的 WordPress 多站点实例。有关更多信息，请参阅 Bitnami 打包的WordPress 多站点。 AWS Cloud

步骤 2：获取访问 WordPress 管理仪表板的默认应用程序密码

完成以下步骤以获取访问 WordPress 多站点网站管理仪表板所需的默认应用程序密码。有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

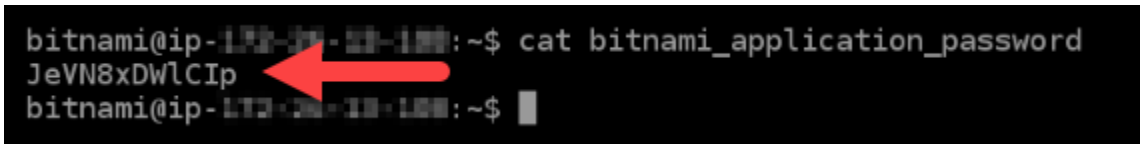
1. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令来获取默认应用程序密码：

```
cat $HOME/bitnami_application_password
```

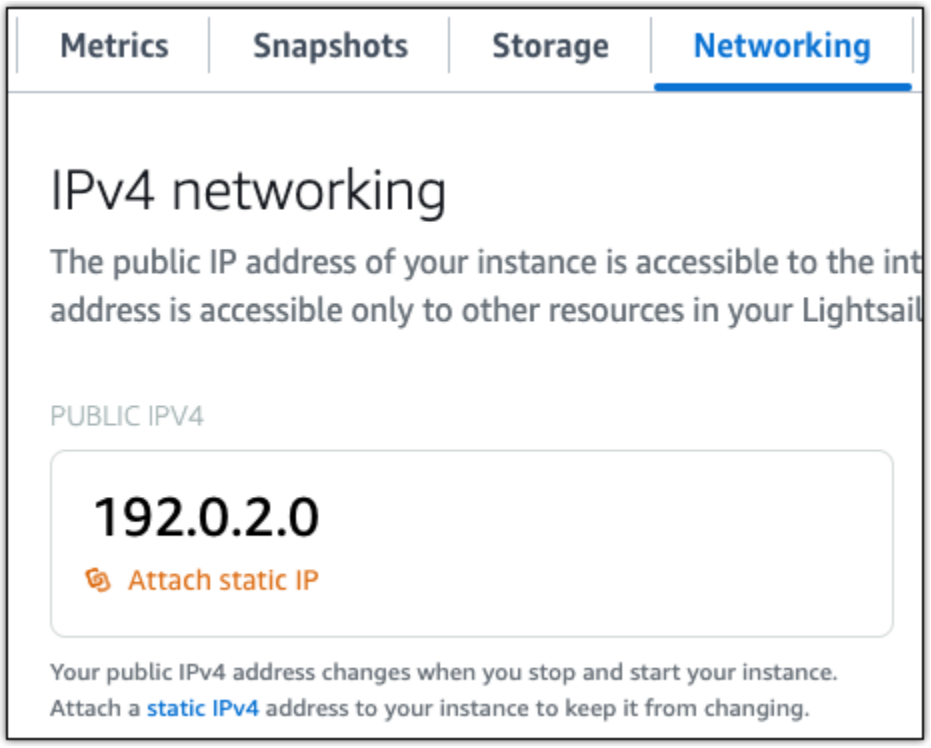
您应该会看到与以下示例类似的响应，其中包含默认应用程序密码。使用此密码登录您的 WordPress Multisite 网站的管理控制面板。



步骤 3：将静态 IP 地址附加到实例

在您首次创建实例时分配给实例的公有 IP 地址会在您每次停止和启动实例时发生更改。您应为实例创建和附加静态 IP 地址，以确保其公有 IP 地址不变。之后，当您将注册域名（如 example.com）用于实例时，无需在每次停止和重启实例时都更新域的域名系统（DNS）。您可以将静态 IP 附加到实例。

在实例管理页面上的联网选项卡下，选择创建静态 IP或附加静态 IP（如果您之前创建了可附加到实例的静态 IP），然后按照页面上的说明操作。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

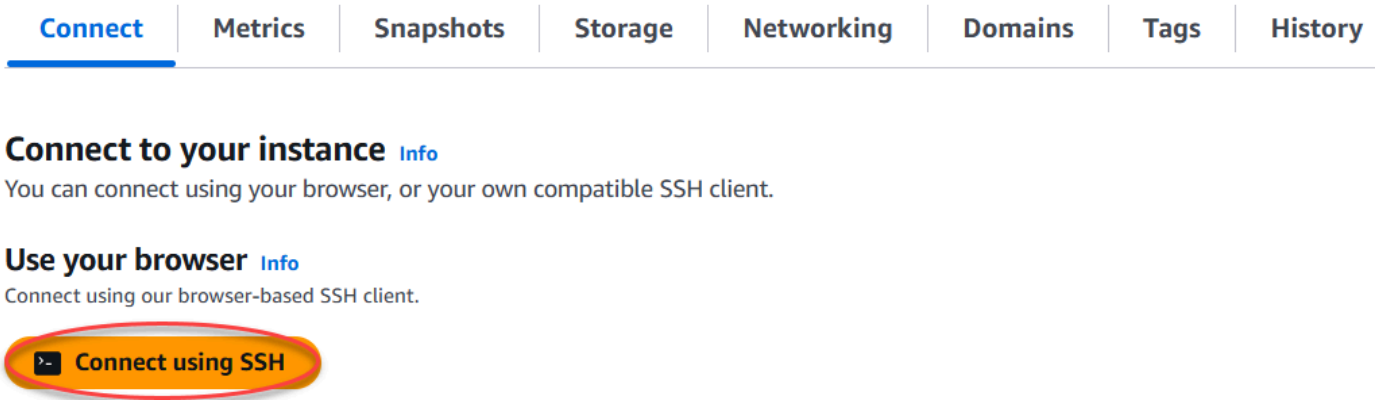


将新的静态 IP 地址附加到您的实例后，您必须完成以下步骤才能 WordPress 知道新的静态 IP 地址。

1. 记下实例的新的静态 IP 地址。它列在实例管理页面的标题部分。



2. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



3. 连接后，请输入以下命令。*<StaticIP>*替换为您的实例的新静态 IP 地址。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您应看到类似于以下示例的响应。您的实例上的 WordPress网站现在应该知道新的静态 IP 地址。

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

如果该命令失败，则您可能使用的是旧版本的 WordPress多站点实例。尝试运行以下命令。*<StaticIP>*替换为您的实例的新静态 IP 地址。

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <StaticIP>
```

运行这些命令后，输入以下命令，以防止 bnconfig 工具在服务器每次重启时自动运行。

```
sudo mv bnconfig bnconfig.disabled
```

第 4 步：登录您的 WordPress 多站点网站的管理控制面板

现在您已经有了默认的应用程序密码，请完成以下步骤以导航到您的 WordPress Multisite 网站的主页并登录到管理控制面板。登录后，您可以开始自定义网站并进行管理更改。有关可以在中执行的操作的更多信息 WordPress，请参阅本指南后面的 “步骤 7：阅读 WordPress 多站点文档并继续配置您的网站” 部分。

1. 在实例管理页面上的 Connect（连接）选项卡下，记下实例的公有 IP 地址。公有 IP 地址也显示在实例管理页面的标题部分。



2. 浏览到实例的公有 IP 地址，例如，转到 `http://203.0.113.0`。

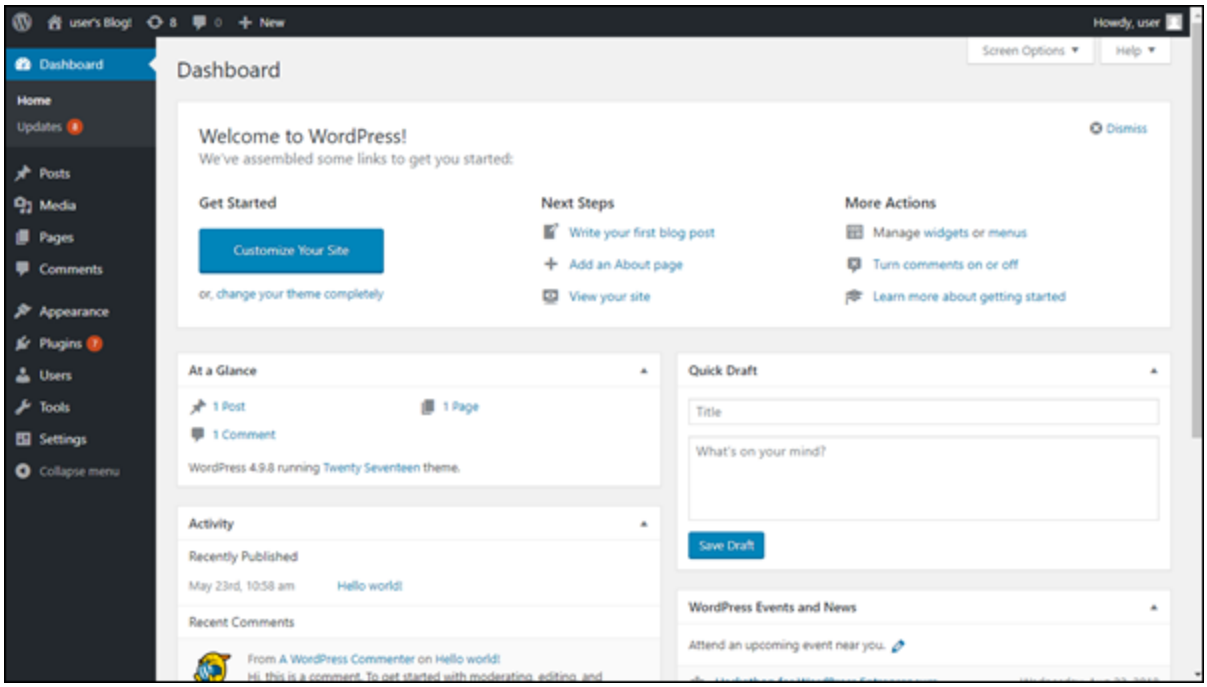
   您 WordPress 网站的主页应该会出现。

3. 选择 WordPress 网站主页右下角的管理。

   如果 Manage（管理）横幅未显示，您可以通过浏览 `http://<PublicIP>/wp-login.php` 到达登录页面。将 *<PublicIP>* 替换为实例的公有 IP 地址。

4. 使用之前在本指南中检索到的默认用户名（`user`）和默认密码登录。

   将出现 WordPress 管理控制面板。



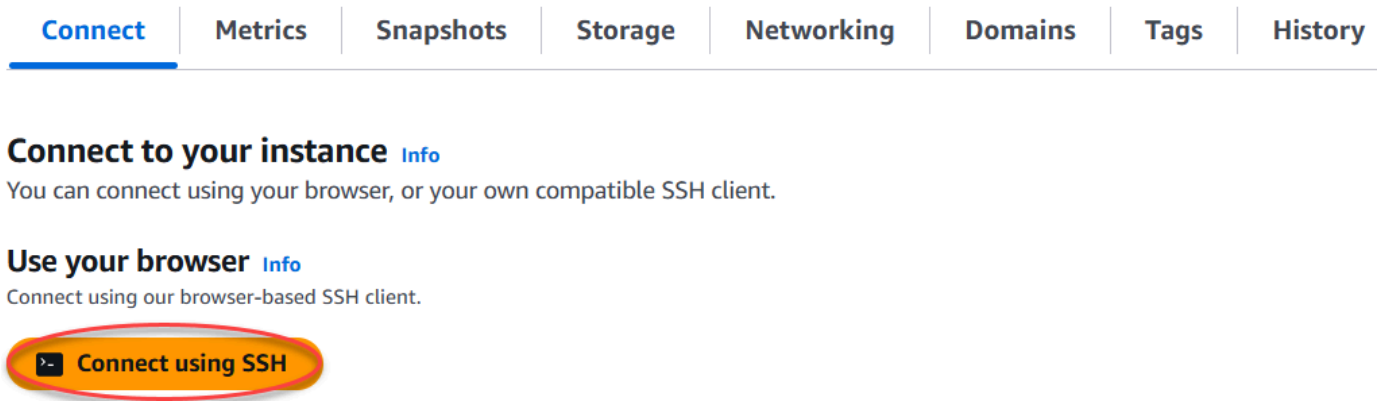
第 5 步：将您注册域名的流量路由到您的 WordPress 多站点网站

要将您的注册域名的流量（例如`example.com`路由到您的 WordPress 多站点网站），您需要在域名的 DNS 中添加一条记录。DNS 记录通常由您注册域的注册商进行托管和管理。但是，我们建议您将域名的 DNS 记录的管理权转移到 Lightsail，以便您可以使用 Lightsail 控制台对其进行管理。

在 Lightsail 控制台主页的 “域名和 DNS” 选项卡下，选择 “创建 DNS 区域”，然后按照页面上的说明进行操作。有关更多信息，请参阅在 Lightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

在您的域名将流量路由到您的实例后，您必须完成以下步骤才能 WordPress 知道该域名。

1. 在实例管理页面上的 Connect (连接) 选项卡下，选择使用 SSH 连接。



2. 连接后，请输入以下命令。*<DomainName>*替换为将流量路由到您的实例的域名。

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

您应看到类似于以下示例的响应。 WordPress多站点软件现在应该知道域名了。

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

如果该命令失败，则您可能使用的是旧版本的 WordPress多站点实例。尝试运行以下命令。*<DomainName>*替换为将流量路由到您的实例的域名。

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <DomainName>
```

运行这些命令后，输入以下命令，以防止 bnconfig 工具在服务器每次重启时自动运行。

```
sudo mv bnconfig bnconfig.disabled
```

如果您浏览到为实例配置的域名，则应被重定向到 WordPress 多站点网站的主博客。接下来，您必须决定是要将博客作为域名还是子域名添加到您的 WordPress Multisite网站。有关更多信息，请继续阅读本指南的下一个步骤 6：将博客作为域名或子域名添加到您的 WordPress 多站点网站部分。

第 6 步：将博客作为域名或子域名添加到您的 WordPress 多站点网站

WordPress Multisite旨在在一个实例上托管多个博客网站。 WordPress当你向 WordPress 多站点添加新的博客网站时，你可以将其配置为使用自己的域名或 WordPress 多站点主域名的子域名。您可以将 WordPress 多站点配置为仅使用其中一个选项。例如，如果您选择将博客站点作为域添加，则不能将博客站点添加为子域，反之亦然。要配置其中任一选项，请参阅下列指南之一：

- 要将博客网站添加为域名，例如`example1.com`和`example2.com`，请参阅在 Lightsail 中将博客作为域名添加到您的 WordPress 多站点实例。
- 要将博客网站添加为 WordPress 多站点主域名的子域名（例如`one.example.com`和`two.example.com`），请参阅在 Lightsail 中将博客作为子域名添加到您的 WordPress 多站点实例。

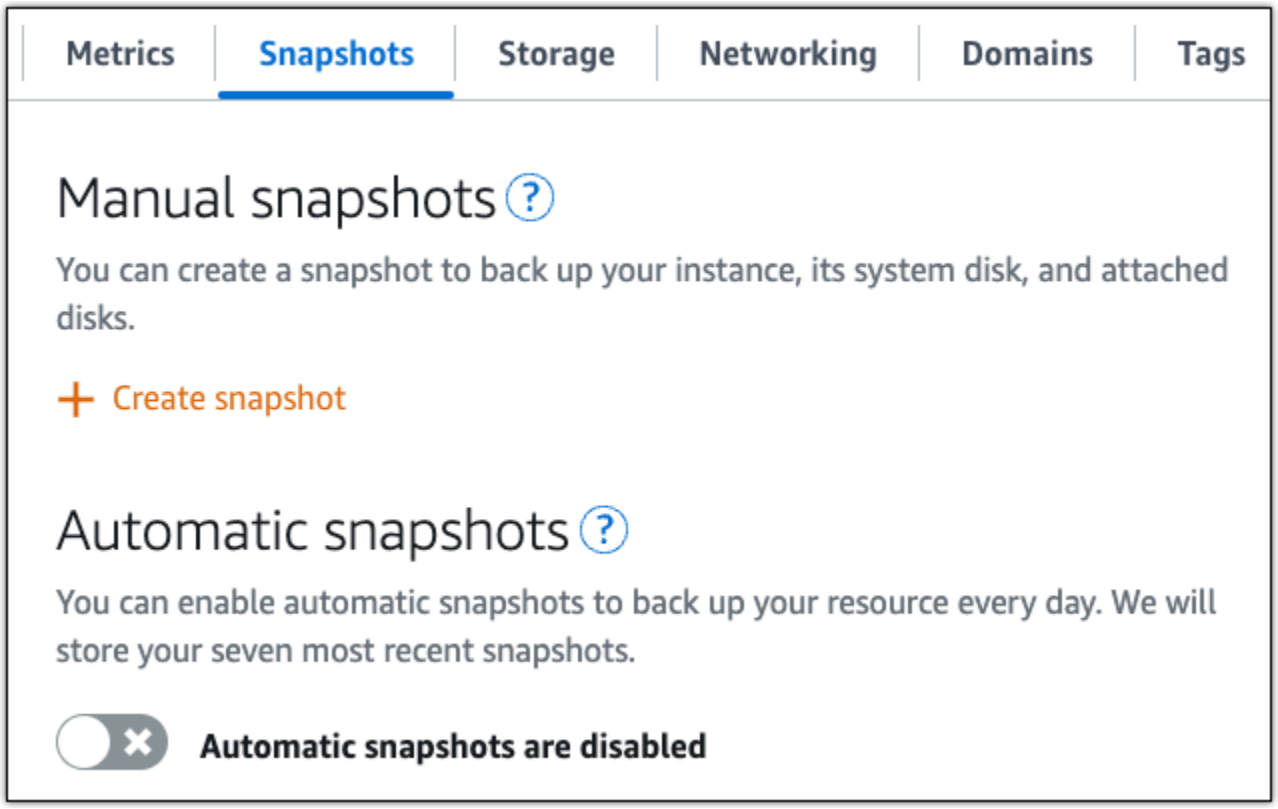
第 7 步：阅读 WordPress 多站点文档并继续配置您的网站

阅读 WordPress 多站点文档，了解如何管理和自定义您的网站。有关更多信息，请参阅WordPress 多站点网络管理文档。

步骤 8：创建实例的快照

按照您想要的方式配置 WordPress 多站点网站后，请创建实例的定期快照以对其进行备份。您可以手动创建快照，也可以启用自动快照，让 Lightsail 为您创建每日快照。如果实例出现错误，则可使用快照来创建新的替代实例。有关更多信息，请参阅快照。

在实例管理页面的快照选项卡下，选择创建快照或选择启用自动快照。



有关更多信息，请参阅在 Amazon Lightsail 中创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。

在 Lightsail 上使用 Bitnami 应用程序和堆栈

本节涵盖以下与亚马逊 Lightsail 实例上的 Bitnami 应用程序相关的主题：

主题

- 获取 Lightsail Bitnami 实例的默认应用程序用户名和密码
- 从 Lightsail 实例中移除 Bitnami 横幅

获取 Lightsail Bitnami 实例的默认应用程序用户名和密码

Bitnami 提供了许多应用程序实例映像或蓝图，您可以将其创建为 Amazon Lightsail 实例，即您的虚拟私有服务器。在 Lightsail 控制台的实例创建页面中，这些蓝图被描述为 “由 Bitnami 打包”。

在使用 Bitnami 蓝图创建实例后，您便可以登录其中并对其进行管理。要执行此操作，您必须获取在该实例上运行的应用程序和/或数据库的默认用户名称和密码。本文介绍如何获取登录和管理根据以下蓝图创建的 Lightsail 实例所需的信息：

- WordPress 博客和内容管理应用程序
- WordPress 多站点博客和内容管理应用程序，支持同一实例上的多个网站
- Django 开发堆栈
- Ghost 博客和内容管理应用程序
- LAMP 开发堆栈 (PHP 7)
- Node.js 开发堆栈
- Joomla 内容管理应用程序
- Magento 电子商务应用程序
- MEAN 开发堆栈
- Drupal 内容管理应用程序
- GitLab CE 存储库应用程序
- Redmine 项目管理应用程序
- Nginx (LEMP) 开发堆栈

获取默认的 Bitnami 应用程序和数据库用户名称

以下是使用 Bitnami 蓝图创建的 Lightsail 实例的默认应用程序和数据库用户名：

> **Note**
>
> 并非所有 Bitnami 蓝图都包含应用程序或数据库。当蓝图中不包含应用程序或数据库时，所列出的用户名称不适用 (N/A)。

- WordPress，包括 WordPress 多站点
  - 应用程序用户名：`user`
  - 数据库用户名：`root`
- PrestaShop
  - 应用程序用户名：`user@example.com`
  - 数据库用户名：`root`
- Django
  - 应用程序用户名：不适用
  - 数据库用户名：`root`

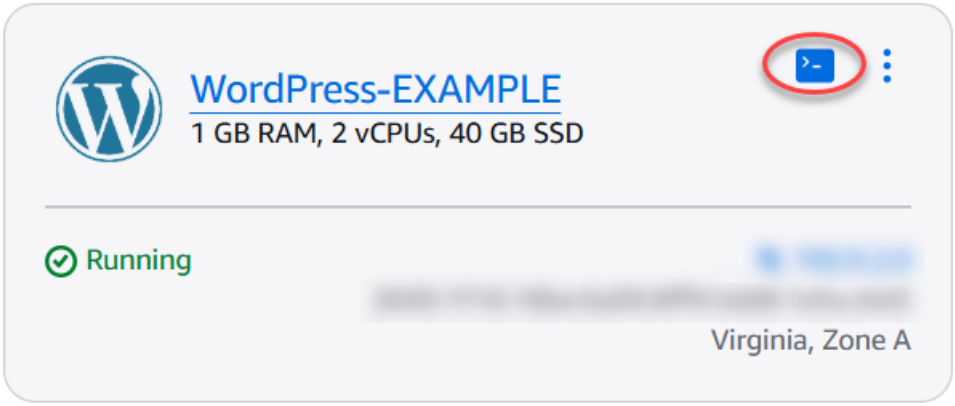
- Ghost
  - 应用程序用户名：`user@example.com`
  - 数据库用户名：`root`
- LAMP 堆栈（PHP 5 和 PHP 7）
  - 应用程序用户名：不适用
  - 数据库用户名：`root`
- Node.js
  - 应用程序用户名：不适用
  - 数据库用户名称：不适用
- Joomla
  - 应用程序用户名：`user`
  - 数据库用户名：`root`
- Magento
  - 应用程序用户名：`user`
  - 数据库用户名：`root`
- MEAN
  - 应用程序用户名：不适用
  - 数据库用户名：`root`
- Drupal
  - 应用程序用户名：`user`
  - 数据库用户名：`root`
- GitLab CE
  - 应用程序用户名：`user`
  - 数据库用户名：`postgres`
- Redmine
  - 应用程序用户名：`user`
  - 数据库用户名：`root`
- Nginx
  - 应用程序用户名：不适用
  - 数据库用户名：`root`

获取默认的 Bitnami 应用程序和数据库密码

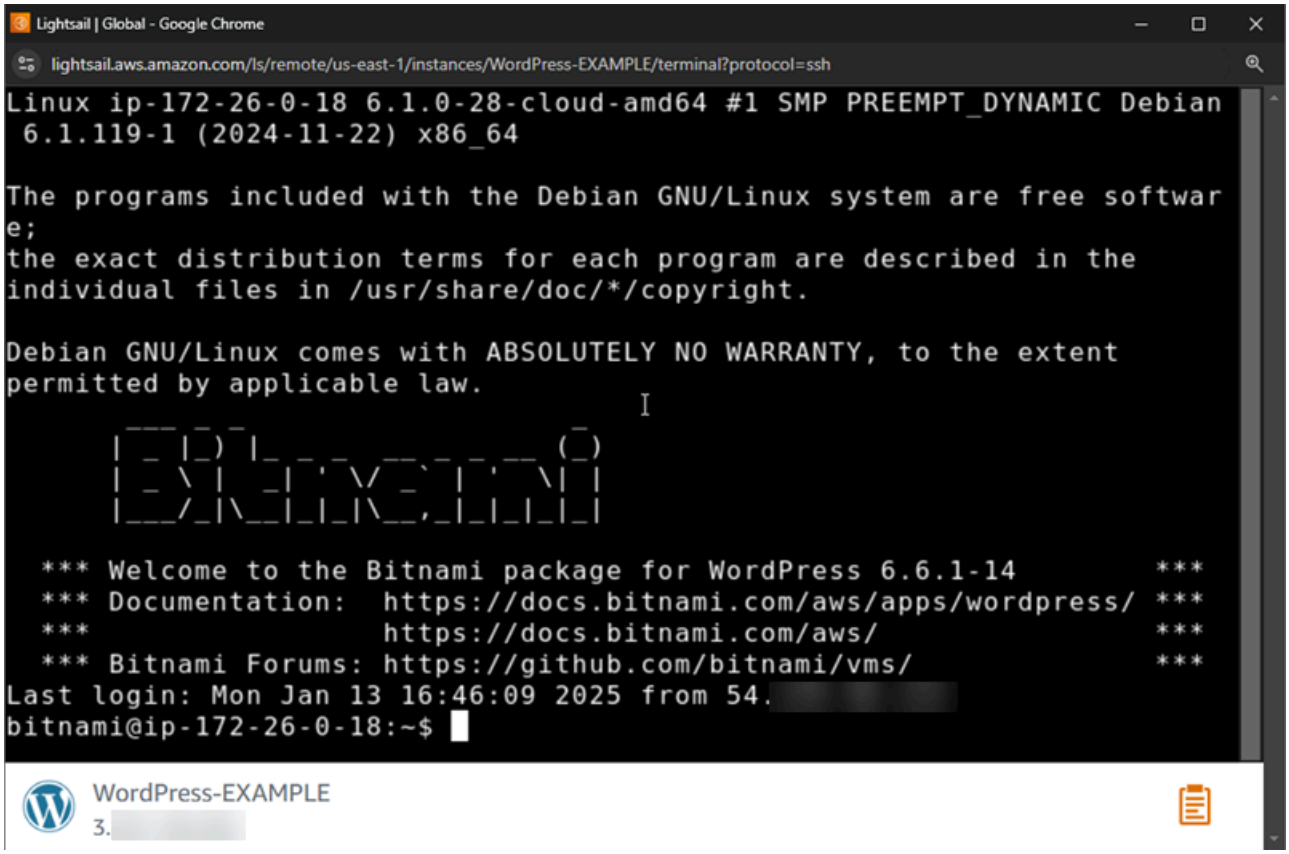
默认的应用程序和数据库密码存储在您的实例上。您可以在 Lightsail 控制台中使用基于浏览器的 SSH 终端连接到该终端并运行特殊命令来检索它。

获取默认的 Bitnami 应用程序和数据库密码

1. 登录 Lightsail 控制台。
2. 如果尚没有实例，请使用 Bitnami 蓝图创建一个实例。有关更多信息，请参阅创建 Amazon Lightsai l VPS
3. 在 Lightsail 主页上，选择要连接的实例的快速连接图标。



基于浏览器的 SSH 客户端窗口会打开，如以下示例所示。

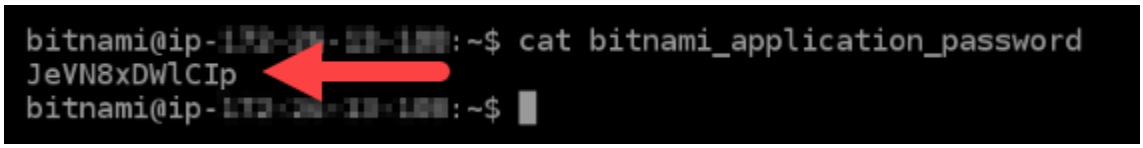


4. 键入以下命令以检索默认应用程序密码：

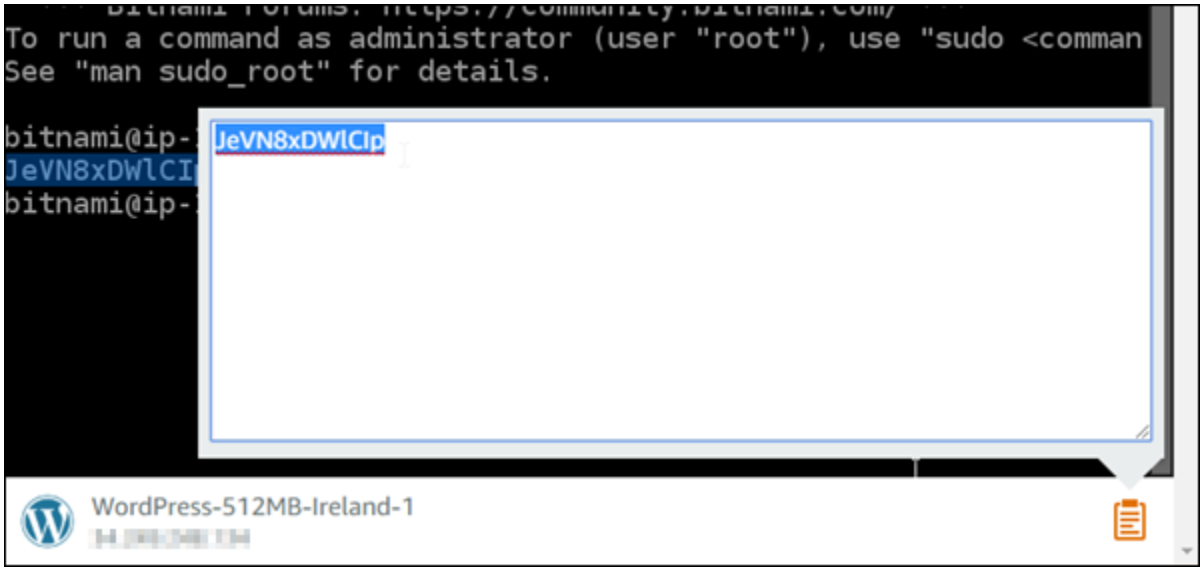
```
cat bitnami_application_password
```

> **Note**
>
> 如果您所在的目录不是用户主目录，请键入 `cat $HOME/bitnami_application_password`。

您应该会看到与以下内容类似的响应，其中包含应用程序密码：



5. 在终端屏幕中，选中该密码，然后选择基于浏览器的 SSH 客户端窗口右下角的剪贴板图标。
6. 在剪贴板文本框中，选中您想要复制的文本，然后按 Ctrl+C 或 Cmd+C，将文本复制到本地剪贴板中。



> **Important**
>
> 此时应确保将密码保存在某个位置。您可在稍后登录到实例上的 Bitnami 应用程序后进行更改。

登录到您的实例上的 Bitnami 应用程序

对于基于 Joomla WordPress、Magento、Drupal、 GitLab CE 和 Redmine 蓝图创建的实例，请浏览您的实例的公有 IP 地址登录应用程序。

登录到 Bitnami 应用程序

1. 在浏览器窗口中，导航至您的实例的公有 IP 地址。

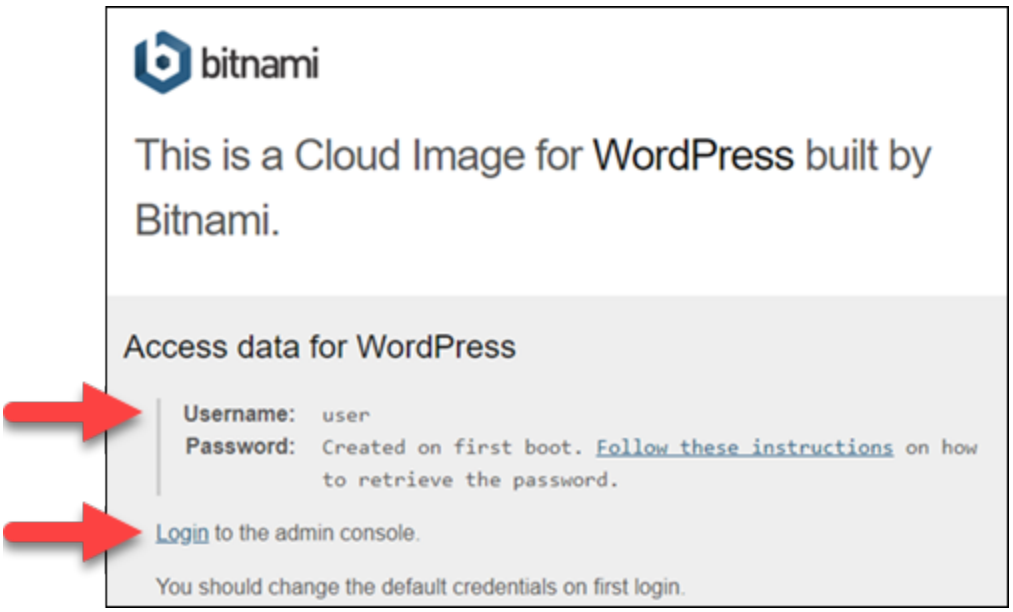
   该操作会打开 Bitnami 应用程序主页。主页会根据您为实例选择的 Bitnami 蓝图进显示相应内容。例如，这是 WordPress应用程序的主页：



2. 选择应用程序主页右下角的 Bitnami 徽标，以转至应用程序信息页面。

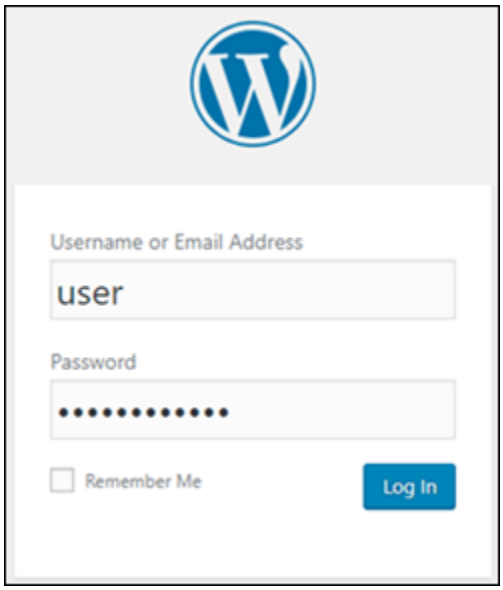
> **Note**
>
> C GitLab E 应用程序不显示 Bitnami 徽标。而是使用 GitLab CE 主页上显示的用户名和密码文本字段登录。

应用程序信息页面包含默认的用户名称和指向您实例上应用程序的登录页面的链接。



3. 选择页面上的登录链接，以转至您实例上的应用程序的登录页面。

4. 键入您刚获得的用户名称和密码，然后选择 Log In（登录）。



后续步骤

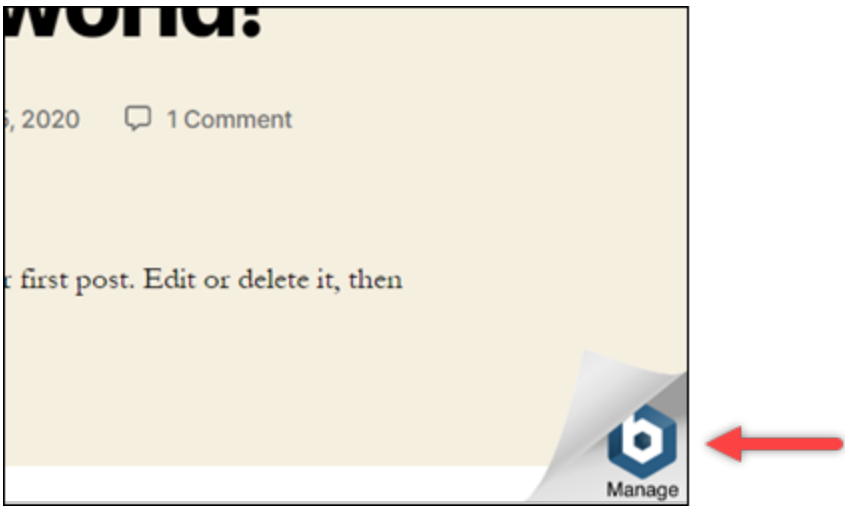
通过以下链接了解更多有关 Bitnami 蓝图的信息并查看它们的教程。例如，您可以为 WordPress 实例安装插件或使用 SSL 证书启用 HTTPS 支持。

- WordPress 适用于亚马逊 Web Services 的 Bitnami
- 适用于亚马逊云科技 的 Bitnami LAMP 堆栈
- 适用于亚马逊云科技 的 Bitnami Node.js
- 适用于亚马逊云科技 的 Bitnami Joomla
- 适用于亚马逊云科技 的 Bitnami Magento
- 适用于亚马逊云科技 的 Bitnami MEAN 堆栈
- 适用于亚马逊云科技 的 Bitnami Drupal
- GitLab 适用于亚马逊 Web Services 的 Bitnami
- 适用于亚马逊云科技 的 Bitnami Redmine
- 适用于亚马逊云科技 的 Bitnami Nginx（LEMP 堆栈）

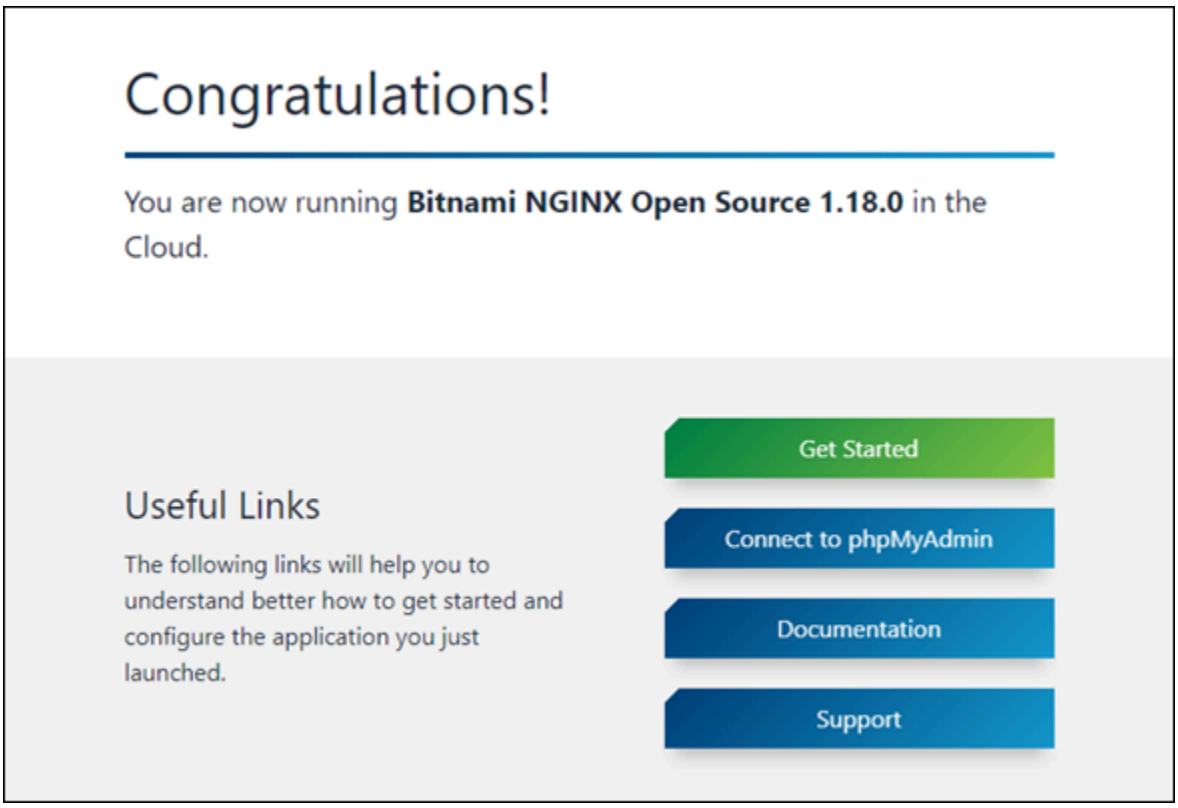
有关更多信息，请参阅使用 Amazon Lights ail 开始使用 Bitnami 应用程序或使用 Amazon Lightsail 常见问题解答。

从 Lightsail 实例中移除 Bitnami 横幅

可以为亚马逊 Lightsail 实例选择的某些 Bitnami 蓝图会在应用程序的主页上显示 Bitnami 横幅。在以下来自 “Bitnami 认证” WordPress 实例的示例中，Bitnami 横幅显示在主页的右下角。在本指南中，我们将介绍如何从实例上的应用程序主页中永久删除 Bitnami 图标。



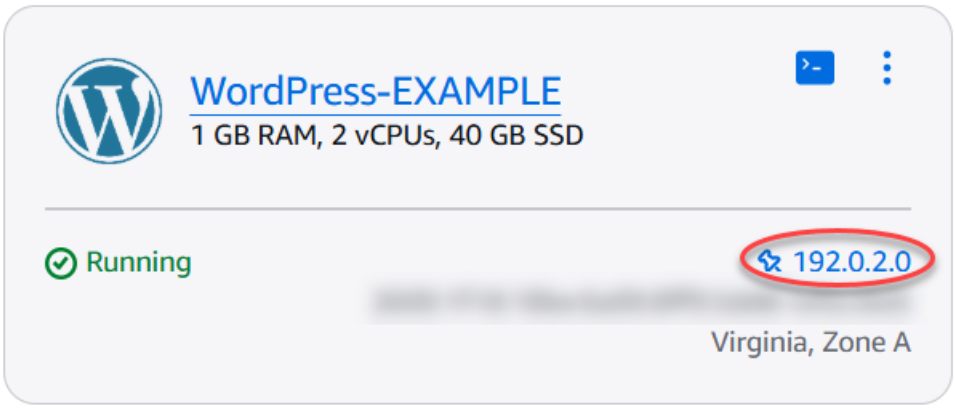
并非所有 Bitnami 蓝图应用程序都会在应用程序的主页上显示 Bitnami 横幅。访问你的 Lightsail 实例的主页，确定是否显示了 Bitnami 横幅。在“由 Bitnami 打包”Nginx 实例的以下示例中，不会显示 Bitnami 图标。而是显示一个占位符信息页面，该页面最终将由您选择部署在实例上的应用程序所替换。如果您的实例没有显示 Bitnami 横幅，则无需按照本指南中的步骤操作。



从您的实例中删除 Bitnami 横幅

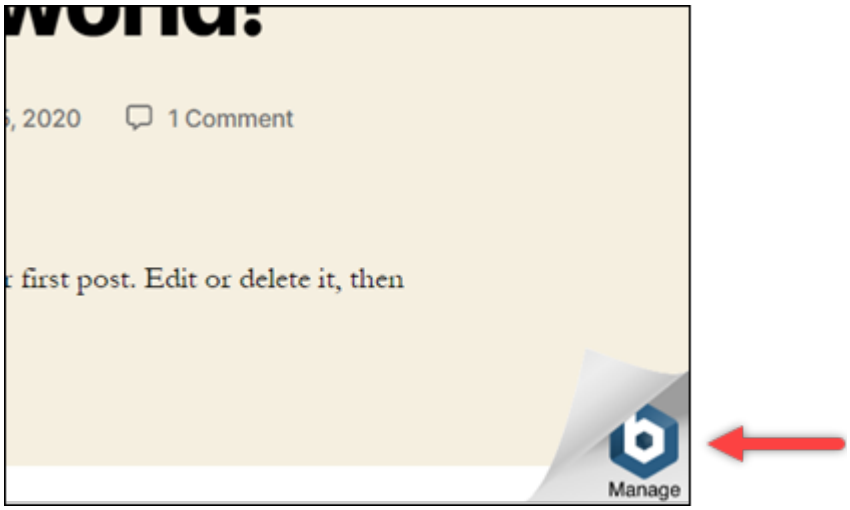
完成以下过程以确认您的实例在应用程序的主页中显示了 Bitnami 图标，并将其删除。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的 “实例” 部分，复制您要确认的实例的公有 IP 地址。



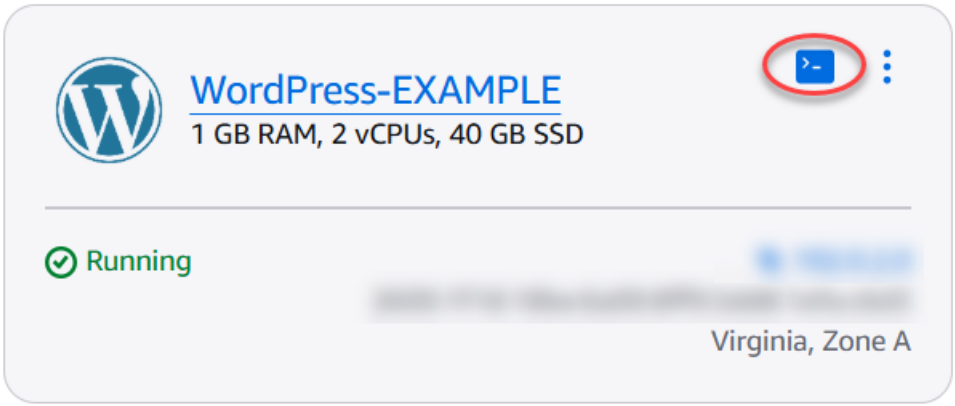
3. 打开新的浏览器选项卡，将实例的公有 IP 地址输入到地址栏中，然后按 Enter。
4. 确认以下选项之一：

1. 如果页面上未显示 Bitnami 图标，则停止执行以下步骤。您不需要从应用程序的主页中删除 Bitnami 图标。
2. 如果 Bitnami 图标显示在页面右下角（如以下示例所示），则继续执行以下步骤将其删除。



在以下步骤中，您将使用基于 Lightsail 浏览器的 SSH 客户端连接到您的实例。连接后，您将运行 Bitnami 配置工具 (bnconfig)，从应用程序的主页中删除 Bitnami 图标。bnconfig 工具是一个命令行工具，允许您在 Bitnami 蓝图实例上配置应用程序。有关更多信息，请参阅 Bitnami 文档中的了解 Bitnami 配置工具。

5. 返回 Lightsail 主页上的浏览器选项卡。
6. 选择要连接的实例名称旁边的基于浏览器的 SSH 客户端图标。



7. SSH 客户端连接到实例后，请输入以下命令之一：

1. 如果您的实例使用 Apache，则输入以下命令中的一个。如果其中一个命令失败，则尝试其他命令。此命令的第一部分将禁用 Bitnami 横幅，第二部分将重新启动 Apache 服务。

```
sudo /opt/bitnami/apps/wordpress/bnconfig --disable_banner 1 && sudo /opt/
bitnami/ctlscript.sh restart apache
```

```
sudo /opt/bitnami/wordpress/bnconfig --disable_banner 1 && sudo /opt/bitnami/
ctlscript.sh restart apache
```

您可以通过浏览实例的公有 IP 地址并确认 Bitnami 图标已消失，来确认此过程已成功完成。

按照 step-by-step说明了解如何检索 Bitnami 应用程序和数据库的默认凭据、登录应用程序的管理面板，以及如何选择从应用程序的主页上删除 Bitnami 品牌横幅。

该指南涵盖了 Lightsail 中可用的各种 Bitnami 蓝图，包括 Joomla、Drupal WordPress、Ghost、LAMP、LEMP、MEAN、Node.js 等。它提供了应用程序和数据库的默认用户名，以及用于安全获取默认密码的命令。通过遵循本指南，您可以轻松访问和管理在 Lightsail 实例上运行的 Bitnami 应用程序，根据您的要求对其进行自定义，并删除任何不需要的品牌元素。

配置和管理 Lights WordPress ail 实例

本指南涵盖了以下与 Lightsai WordPress l 中的实例相关的主题：

主题

- 在 Lightsail 上启动和配置 WordPress 实例
- 使用 WP Offload Media 将 Lightsail 上的 WordPress 网站连接到亚马逊 S3
- 将 Lightsail WordPress 实例连接到亚马逊 Aurora 数据库
- 在 Lightsail 中将 WordPress 数据传输到 MySQL 托管数据库
- 将 WordPress 实例连接到 Lightsail 存储桶以获取静态内容
- 使用 Ligh WordPress tsail 内容分发网络进行配置
- 在 Lightsail 中为 WordPress实例启用电子邮件
- 在 Lightsail 上使用 HTTPS 保护你的 WordPress 网站
- 将你的 WordPress 博客迁移到 Lightsail

在 Lightsail 上启动和配置 WordPress 实例

Amazon Lightsail 是开始使用亚马逊网络服务 ()AWS的最简单方法。Lightsail 包含快速启动项目所需的一切——实例（虚拟专用服务器）、托管数据库、基于 SSD 的存储、备份（快照）、数据传输、域 DNS 管理 IPs、静态和负载均衡器——价格低廉、可预测。

通过本教程，您将学习如何在 Lightsail 上启动和配置 WordPress 实例。它包括配置自定义域名、使用 HTTPS 保护互联网流量、使用 SSH 连接到您的实例以及登录 WordPress 网站的步骤。完成本教程后，你就具备了在 Lightsail 上启动和运行实例的基础知识。

> **Note**
>
> 作为 AWS 免费套餐的一部分，您可以免费开始使用特定实例捆绑包的 Amazon Lightsail。有关更多信息，请参阅亚马逊 Lightsail 定价页面上的AWS 免费套餐。

内容

- 第 1 步：注册 AWS
- 步骤 2：创建 WordPress 实例
- 步骤 3：配置您的 WordPress实例
- 第 4 步：获取 WordPress 网站的管理员密码
- 第 5 步：登录 WordPress 网站的管理控制面板
- 其他信息

第 1 步：注册 AWS

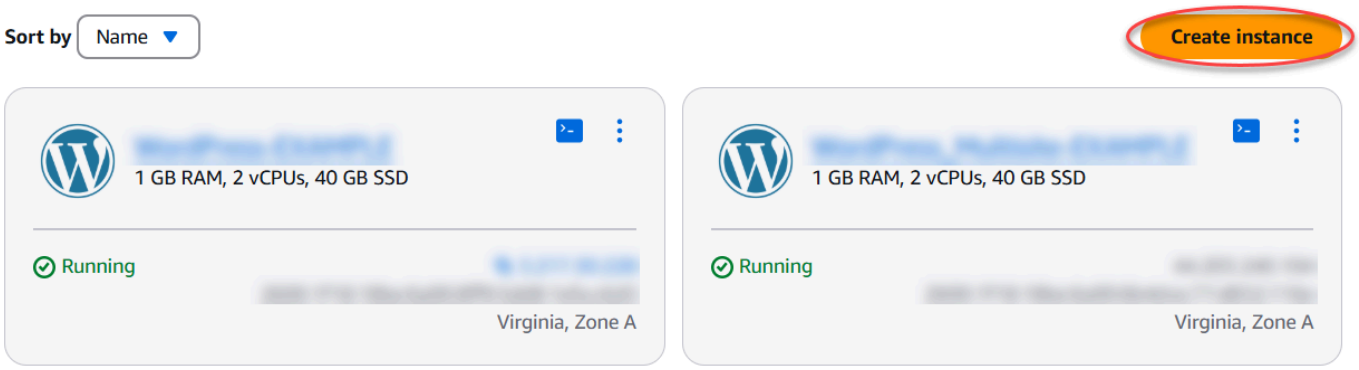
亚马逊 Lightsail 需要。 AWS 账户注册 AWS或登录（ AWS如果您已经有一个帐户）。

步骤 2：创建 WordPress 实例

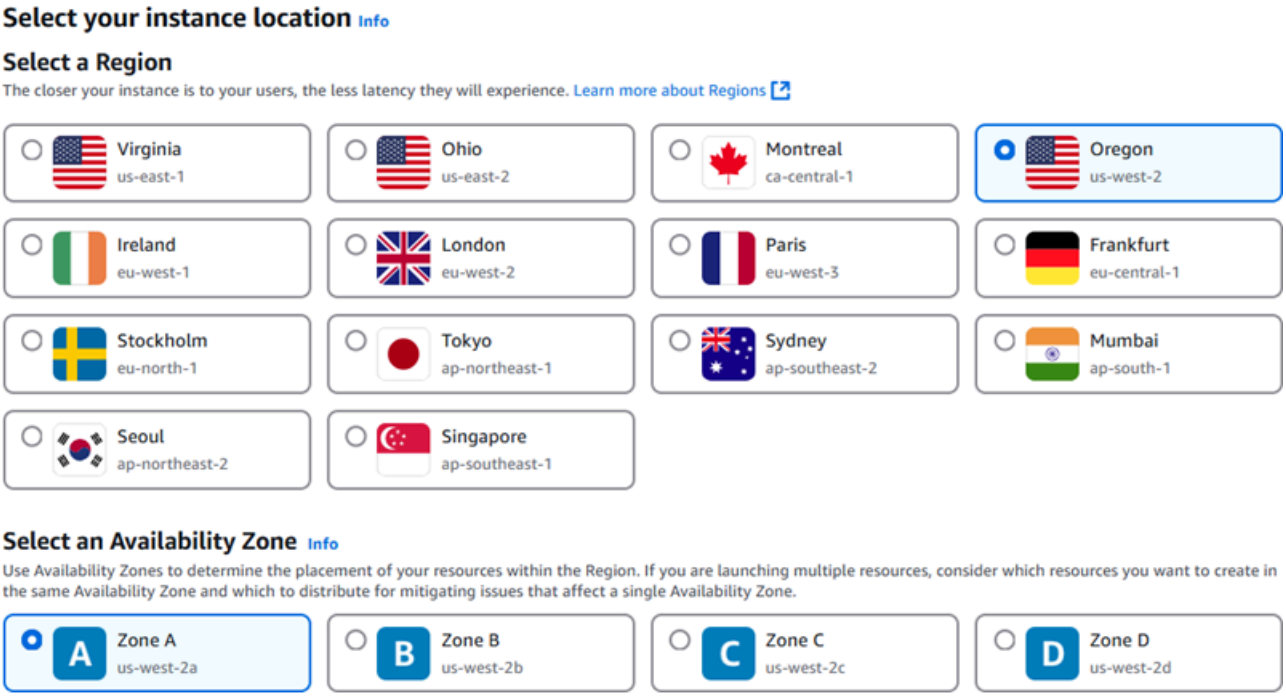
完成以下步骤以启动并运行您的 WordPress 实例。有关更多信息，请参阅 the section called “创建实例”。

为创建 Lightsail 实例 WordPress

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的 “实例” 部分，选择创建实例。



3. 为您的实例选择 AWS 区域 和可用区。



4. 为您的实例选择映像，如下所示：

   a. 在选择平台中，选择 Linux/Unix。

   b. 在 “选择蓝图” 中，选择WordPress。

5. 选择实例计划。

   计划包括采用可预测低成本的计算机配置（RAM、SSD、vCPU）以及数据传输限额。

6. 输入实例的名称。资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。

- 可以包括字母数字字符、数字、句点、连字符和下划线。

7. 选择创建实例。
8. 要查看测试博客文章，请转到实例管理页面并复制页面右上角显示的公共 IPv4 地址。将该地址粘贴到已连接 Internet 的 Web 浏览器的地址栏中。浏览器显示测试博客文章。

步骤 3：配置您的 WordPress实例

您可以使用指导式 step-by-step工作流程配置您的 WordPress 实例，也可以完成单个任务。使用任一选项，您都将配置以下内容：

- 注册域名-您的 WordPress 网站需要一个易于记忆的域名。用户将指定此域名来访问您的 WordPress 网站。有关更多信息，请参阅 域和 DNS。
- DNS 管理 – 您必须决定如何管理域的 DNS 记录。DNS 记录将域（或子域）所关联的 IP 地址或主机名告知 DNS 服务器。DNS 区域包含域的 DNS 记录。有关更多信息，请参阅 the section called “Lightsail 中的 DNS”。
- 静态 IP 地址-如果您停止并启动实例，则 WordPress 实例的默认公有 IP 地址会发生变化。当您向实例附加静态 IP 地址时，即使您停止和启动实例，该 IP 地址也会保持不变。有关更多信息，请参阅 the section called “IP 地址”。
- SSL/TLS 证书-创建经过验证的证书并将其安装在实例上后，您可以为您的 WordPress 网站启用 HTTPS，以便使用 HTTPS 加密通过您的注册域路由到实例的流量。有关更多信息，请参阅 the section called “启用 HTTPS”。

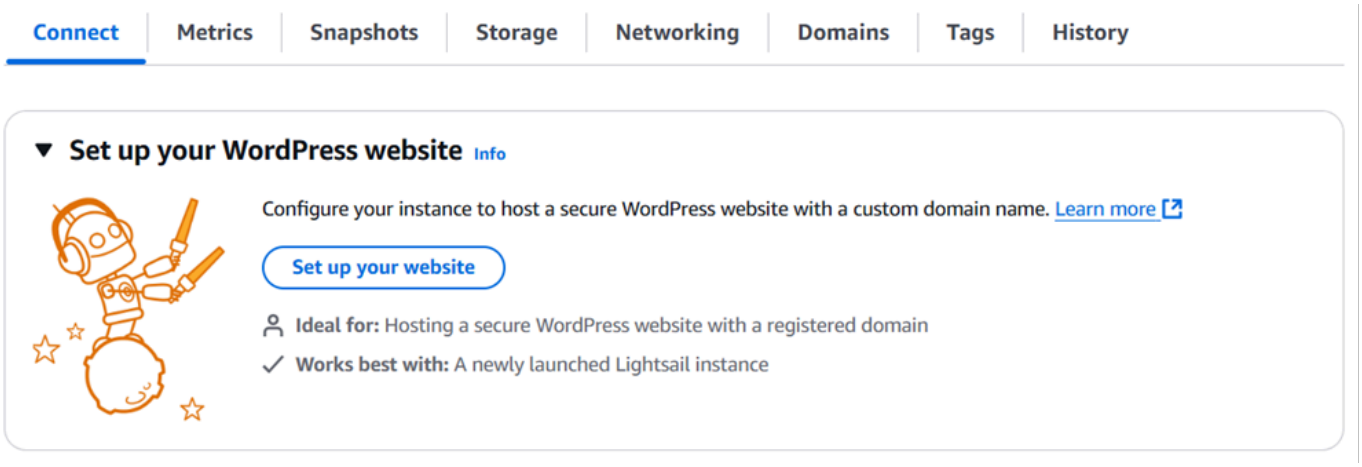
选项：引导式工作流程

> **Tip**
>
> 在开始之前，请查看以下提示。有关疑难解答信息，请参阅故障排除 WordPress 设置。
>
> - 安装程序支持 2023 年 1 月 1 日之后创建的 WordPress 版本 6 及更高版本的 Lightsail 实例。
> - 设定期间运行的 Certbot 依赖项文件、HTTPS 重写脚本和证书续订脚本保存在您实例上的 `/opt/bitnami/lightsail/scripts/` 目录中。
> - 该实例必须处于运行中状态。如果实例刚刚启动，请等待几分钟，让 SSH 连接准备就绪。
> - 在设定运行期间，实例防火墙上的端口 22、80 和 443 必须允许来自任何 IP 地址的 TCP 连接。有关更多信息，请参阅实例防火墙。

- 当您添加或更新指向来自顶级域（example.com）及其 www 子域（www.example.com）的流量的 DNS 记录时，它们需要在整个 Internet 中传播。您可以使用诸如 nslookup 或 DNS 查找之类的工具来验证您的 DN S 更改是否已生效。MxToolbox
- 在 2023 年 1 月 1 日之前创建的 Wordpress 实例可能包含已弃用的 Certbot 个人程序包存档（PPA）存储库，这将导致网站设置失败。如果在设置过程中存在此存储库，则会将其从现有路径中移除并备份到实例上的以下位置：~/opt/bitnami/lightsail/repo.backup。有关已弃用的 PPA 的更多信息，请参阅 Canonical 网站上的 Certbot PPA。
- Let's Encrypt 证书将每 60 到 90 天自动续订一次。
- 在设置过程中，请勿停止或更改您的实例。配置您的实例可能最多需要 15 分钟。您可以在“实例连接”选项卡中查看每个步骤的进度。

要使用网站设置向导配置您的实例

1. 在实例管理页面的连接选项卡上，选择设置网站。



2. 对于指定域名，请使用现有的 Lightsail 托管域，向 Lightsail 注册一个新域名，或者使用您通过其他域名注册商注册的域名。选择使用此域进入下一步。
3. 对于配置 DNS，请执行以下操作之一：
   - 选择 Lightsail 托管域以使用 Lightsail DNS 区域。选择使用此 DNS 区域进入下一步。
   - 选择第三方域以使用管理域的 DNS 记录的托管服务。请注意，我们会在您的 Lightsail 账户中创建一个匹配的 DNS 区域，以备您以后决定使用该区域时使用。选择使用第三方 DNS 进入下一步。
4. 在创建静态 IP 地址中，输入静态 IP 地址的名称，然后选择创建静态 IP。
5. 在管理域分配中，选择添加分配，选择域类型，然后选择添加。选择继续进入下一步。

6. 在创建 SSL/TLS 证书中，选择您的域名和子域名，输入电子邮件地址，选择我授权 Lightsail 在我的实例上配置 Let's Encrypt 证书，然后选择创建证书。我们开始配置 Lightsail 资源。

   在设置过程中，请勿停止或更改您的实例。配置您的实例可能最多需要 15 分钟。您可以在“实例连接”选项卡中查看每个步骤的进度。

7. 网站设置完成后，请 URLs 确认您在域名分配步骤中指定的已打开您的 WordPress 网站。

选项：各项任务

要通过完成各项任务来配置您的实例

1. 创建静态 IP 地址

   在实例管理页面上的联网选项卡中，选择创建静态 IP。系统自动选择静态 IP 位置和实例。为您的静态 IP 地址指定一个名称，然后选择创建并附加。

2. 创建一个 DNS 区域

   在导航窗格中，选择域和 DNS。选择创建 DNS 区域，输入您的域，然后选择创建 DNS 区域。如果当前正在将网络流量路由到您的域名，请确保所有现有 DNS 记录都存在于 Lightsail DNS 区域中，然后再更改域名的当前 DNS 托管提供商的域名服务器。这样，流量可以在传输到 Lightsail DNS 区域后持续不间断地流动

3. 管理域分配

   在该 DNS 区域页面上的分配选项卡中，选择添加分配。选择域或子域，选择您的实例，附加静态 IP 地址，然后选择分配。

   > **Tip**
   >
   > 在您的域名开始将流量路由到您的 WordPress 实例之前，请留出时间让这些更改传播到互联网。

4. 创建和安装 SSL/TLS 证书

   有关 step-by-step指示，请参阅the section called “启用 HTTPS”。

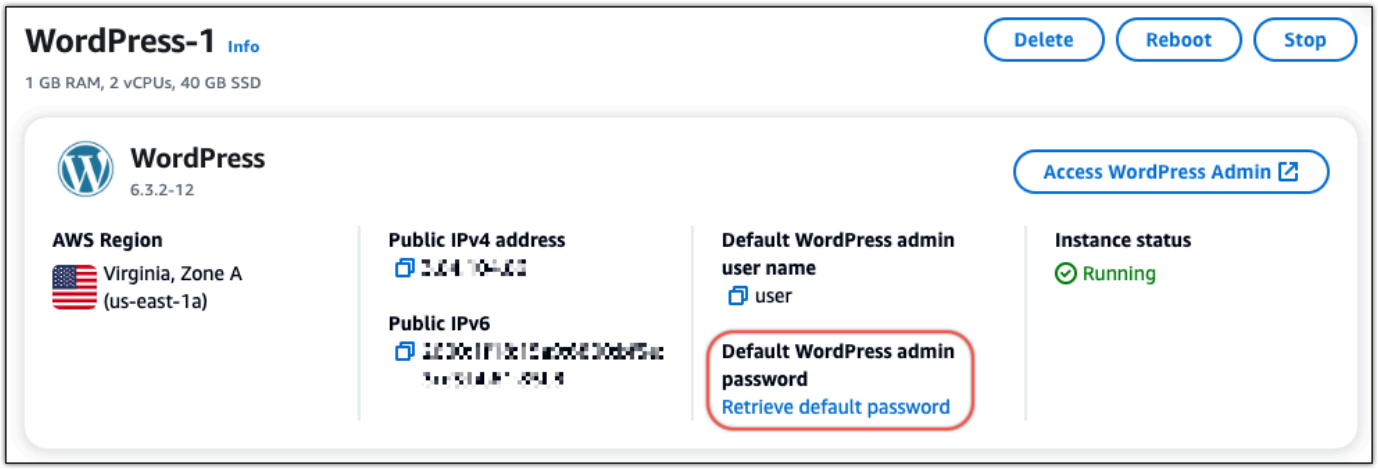
5. 验证您在域名分配步骤中指定的是否打开了您的 WordPress 网站。 URLs

第 4 步：获取 WordPress 网站的管理员密码

登录 WordPress 网站管理仪表板的默认密码存储在实例上。完成以下步骤以获取密码。

获取 WordPress 管理员的默认密码

1. 打开您的实例的 WordPress 实例管理页面。
2. 在WordPress面板上，选择 “找回默认密码”。这将在页面底部展开访问默认密码。



3. 选择启动 CloudShell。这将在页面底部打开面板。
4. 选择 “复制”，然后将内容粘贴到 CloudShell 窗口中。您可以将光标放在 CloudShell 提示符处并按 Ctrl+V，也可以右键单击打开菜单，然后选择 “粘贴”。
5. 记下 CloudShell 窗口中显示的密码。您需要使用它来登录 WordPress 网站的管理控制面板。



第 5 步：登录 WordPress 网站的管理控制面板

现在您已经有了 WordPress 网站管理仪表板的密码，就可以登录了。在管理控制面板中，您可以更改用户密码、安装插件、更改网站的主题等等。

完成以下步骤登录到您 WordPress网站的管理控制面板。

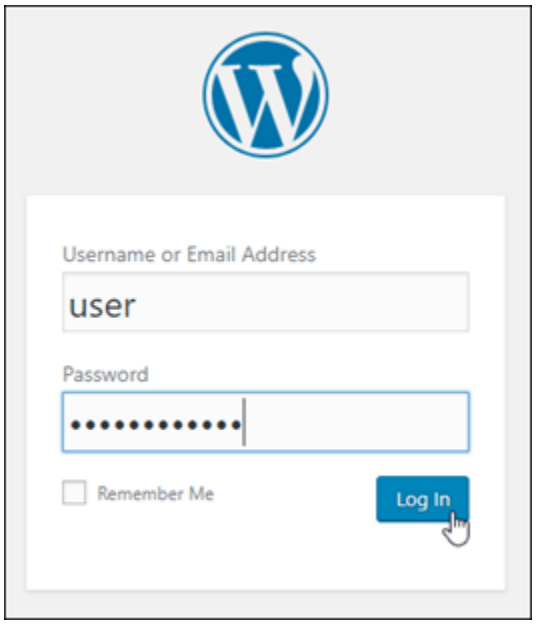
要登录管理控制面板

1. 打开您的实例的 WordPress 实例管理页面。
2. 在WordPress面板上，选择访问 WordPress 管理员。

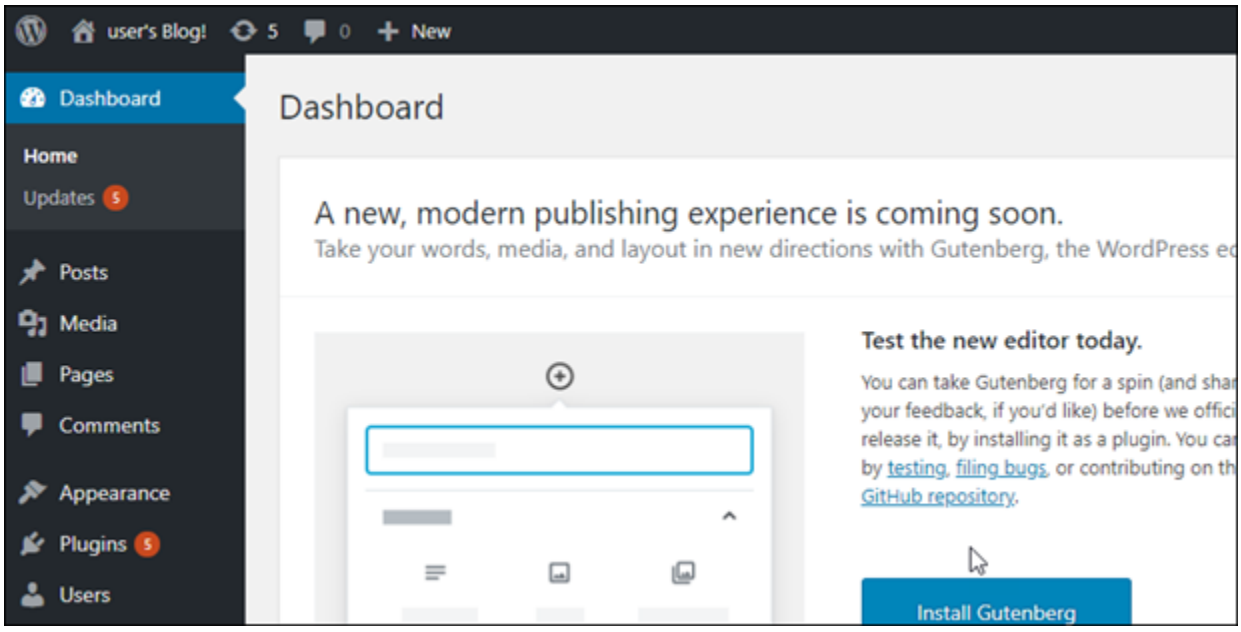
3. 在“访问您的 WordPress 管理员控制面板”面板的“使用公有 IP 地址”下，选择以下格式的链接：

   http://*public-ipv4-address*。 /wp-admin

4. 在用户名或电子邮件地址中，输入 **user**。
5. 在密码中，输入在上一步中获得的密码。
6. 选择登录。



现在，您已登录 WordPress 网站的管理控制面板，可以在其中执行管理操作。有关管理 WordPress 网站的更多信息，请参阅 WordPress 文档中的 WordPressCodex。



其他信息

以下是在 Amazon Lightsail 中启动 WordPress 实例后可以执行的一些其他步骤：

- the section called “配置 CDN”
- 创建 Linux 或 Unix 实例的快照
- 启用或禁用实例或磁盘的自动快照
- 创建额外的数据块存储磁盘并将其附加到基于 Linux 的实例

使用 WP Offload Media 将 Lightsail 上的 WordPress 网站连接到亚马逊 S3

本教程介绍了将在 Amazon Lightsail 实例上运行的 WordPress 网站连接到用于存储网站图像和附件的亚马逊简单存储服务 (Amazon S3) 存储桶所需的步骤。为此，您需要为 WordPress 插件配置一组 Amazon Web Services (AWS) 账户证书。然后，该插件会为您创建 Amazon S3 存储桶，并将您的网站配置为使用存储桶而不是实例的磁盘来存储网站图像和附件。

主题

- 步骤 1：完成先决条件
- 第 2 步：在您的 WordPress 网站上安装 WP Offload Media 插件
- 步骤 3：创建 IAM 策略
- 步骤 4：创建 IAM 用户
- 步骤 5：为您的 IAM 用户创建访问密钥
- 步骤 6：编辑 WordPress配置文件
- 第 7 步：使用 WP Offload Media 插件创建 Amazon S3 存储桶
- 步骤 8：后续步骤

步骤 1：完成先决条件

在开始之前，请在 Lightsail 中创建一个 WordPress 实例，并确保其处于运行状态。有关更多信息，请参阅教程：启动和配置实 WordPress 例。

第 2 步：在您的 WordPress 网站上安装 WP Offload Media 插件

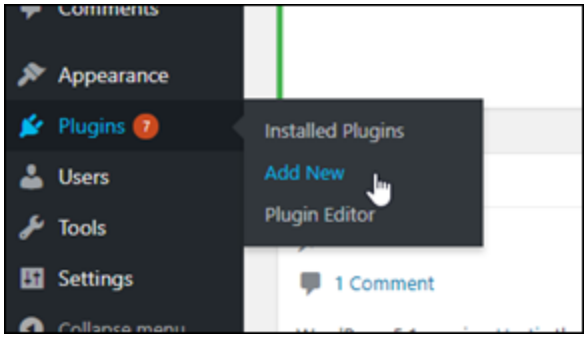
您必须使用插件来配置您的网站，以使用 Amazon S3 存储桶。许多插件可用于配置此功能；比如 WP Offload Media Lite。

在您的 WordPress网站上安装 WP Offload Media 插件

1. 以管理员身份登录 WordPress 控制面板。

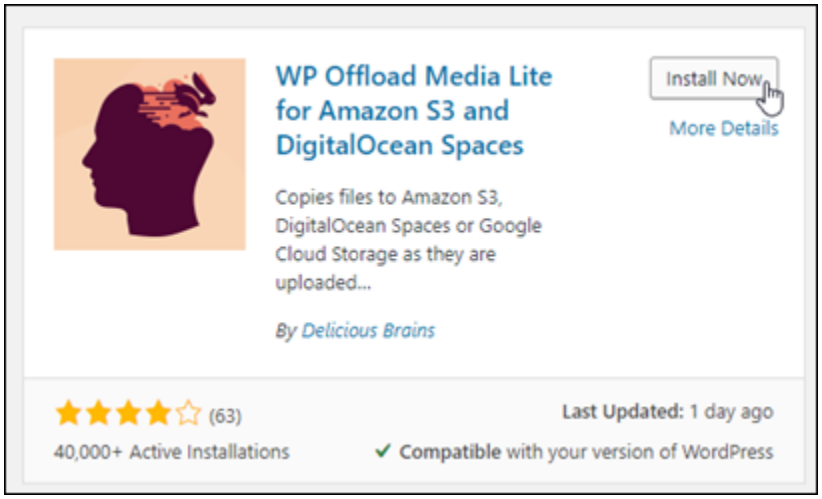
   有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

2. 将鼠标指针悬停在左侧导航菜单的 Plugins (插件) 上，然后选择 Add New (新增)。



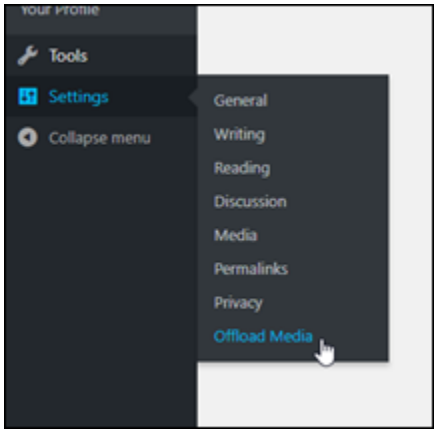
3. 搜索 WP Offload Media Lite。

4. 在搜索结果中，选择 WP Offload Media 插件旁边的立即安装。



5. 完成插件安装后，选择 Activate (激活)。

6. 在左侧导航菜单中，选择 Settings (设置)，然后选择 Offload Media。



7. 在 Offload Media 页面上，选择 Amazon S3 作为存储提供程序，然后选择在 wp-config.php 中定义访问密钥。

   使用此选项，您必须将您的 AWS 账户证书添加到实例`wp-config.php`上。本教程的后续部分中涵盖了这些步骤。



   保持 Offload Media 页面打开；在本教程的后续部分中要返回使用它。继续阅读本教程的步骤 3：创建 IAM 策略章节。

步骤 3：创建 IAM 策略

> **Warning**
>
> 此场景需要 IAM 用户具有编程访问权限和长期凭证，这会带来安全风险。为帮助减轻这种风险，我们建议仅向这些用户提供执行任务所需的权限，并在不再需要这些用户时将其移除。必要时可以更新访问密钥。有关更多信息，请参阅《IAM 用户指南》中的更新访问密钥。

WP Offload Media 插件需要访问您的 AWS 账户才能创建 Amazon S3 存储桶，以及上传您的网站图像和附件。

为 WP Offload Media 插件创建新 AWS Identity and Access Management (IAM) 策略

1. 打开一个新的浏览器选项卡，然后登录到 IAM 控制台。
2. 在左侧导航菜单的访问管理下，选择策略。
3. 选择创建策略。
4. 在创建策略页面上，选择 JSON，然后删除策略编辑器中的所有内容。
5. 在策略编辑器中指定以下内容，将的示例存储桶名称替换为您自己的存储桶名称：*amzn-s3-demo-bucket*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*",
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        }
    ]
}
```

6. 选择下一步。
7. 对于 Policy name（策略名称），输入此策略的名称。

> **Tip**
>
> 指定描述性名称，例如**wp_s3_user_policy**或**wp_offload_media_plugin_user_policy**，以便将来在执行维护时可以轻松识别该名称。

8. 选择创建策略。

   保持 IAM 控制台处于打开状态，以供下一步使用。

步骤 4：创建 IAM 用户

创建新的 IAM 用户并附加之前创建的策略，以授予使用 WP Offload Media 插件所需的权限。

为 WP Offload Media 插件创建新 AWS Identity and Access Management (IAM) 用户

1. 如有必要，请打开 IAM 控制台。
2. 在左侧导航菜单的访问管理下，选择用户。
3. 选择创建用户。
4. 在 “用户名” 中，输入新用户的名称，然后选择 “下一步”。

> **Tip**
>
> 指定描述性名称，例如**wp_s3_user**或**wp_offload_media_plugin_user**，以便将来在执行维护时可以轻松识别该名称。

5. 直接选择附加策略。
6. 在 “权限策略” 下，在搜索栏中输入您之前创建的策略的名称。
7. 选择策略，然后选择下一步。
8. 选择创建用户。

   保持 IAM 控制台处于打开状态，以供下一步使用。

步骤 5：为您的 IAM 用户创建访问密钥

为 IAM 用户创建将由 WP Offload Media 插件使用的访问密钥。

为 WP Offload Media 插件创建新 AWS Identity and Access Management (IAM) 用户

1. 如有必要，请打开 IAM 控制台。
2. 在左侧导航菜单的访问管理下，选择用户。
3. 选择用户名称转到用户详细信息页面。
4. 在 Security credentials（安全凭证）选项卡的 Access keys（访问密钥）部分中，选择 Create access key（创建访问密钥）。
5. 选择 “其他”，然后选择 “下一步”。
6. 选择创建访问密钥。
7. 记下 IAM 用户的访问密钥 ID 和私有访问密钥。您也可以选择 “下载.csv”，将这些值的副本保存到本地驱动器中。在接下来的几个步骤中，在 WordPress 实例上编辑`wp-config.php`文件时，您将需要这些内容。

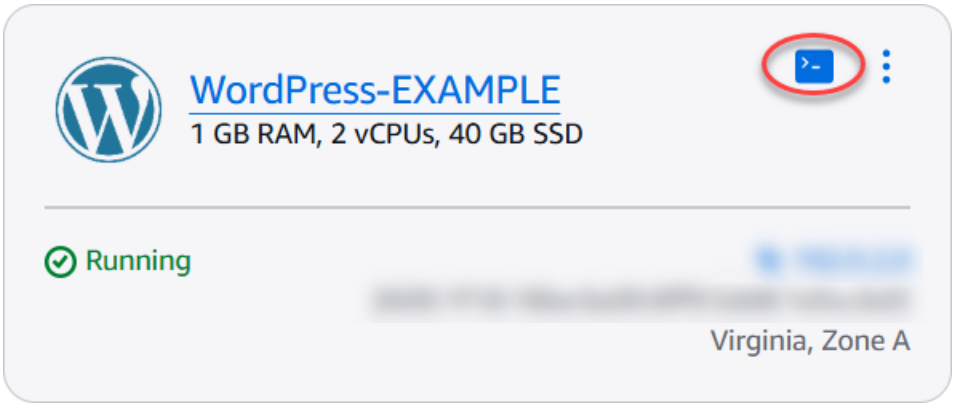
   现在，您可以关闭 IAM 控制台，然后在 Lightsail 控制台上继续执行下一步操作。

步骤 6：编辑 WordPress配置文件

该 `wp-config.php` 文件包含您网站的基础配置详细信息，如数据库连接信息。

编辑您的 WordPress 实例中的**`wp-config.php`**文件

1. 登录 Lightsail 控制台。
2. 为实例选择基于浏览器的 SSH 客户端图标。 WordPress



> **Note**
>
> 您也可以使用自己的 SSH 客户端连接到实例。有关更多信息，请参阅在 Lightsail 中下载并设置 PuTTY 以使用 SSH 进行连接。

3. 在显示的 SSH 客户端窗口中，输入以下命令来创建 wp-config.php 文件的备份，以防出现问题：

```
sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-
config.php.backup
```

4. 输入以下命令以使用文本编辑器 nano 打开 wp-config.php 文件：

```
nano /opt/bitnami/wordpress/wp-config.php
```

5. 输入 /* That's all, stop editing! Happy blogging. */ 文本上方的以下文本。

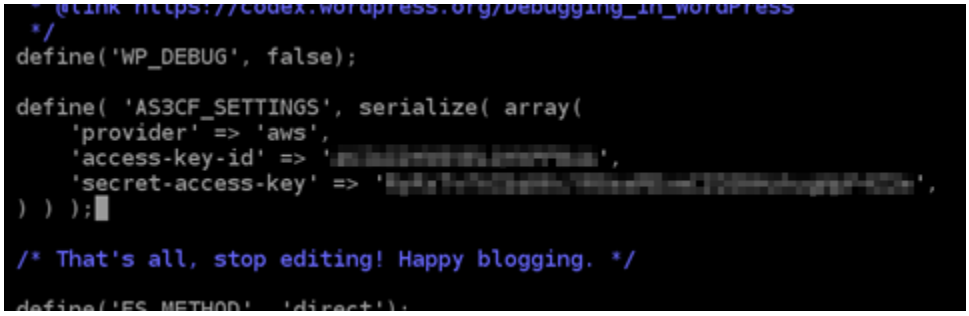
   请务必*AccessKeyID*替换为您在这些步骤之前创建的 IAM 用户的访问密钥 ID 和*SecretAccessKey*私有访问密钥。

```
define( 'AS3CF_SETTINGS', serialize( array(
    'provider' => 'aws',
    'access-key-id' => 'AccessKeyID',
    'secret-access-key' => 'SecretAccessKey',
) ) );
```

   示例：

```
define( 'AS3CF_SETTINGS', serialize( array(
    'provider' => 'aws',
    'access-key-id' => 'AKIAIOSFODNN7EXAMPLE',
    'secret-access-key' => 'wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY',
) ) );
```

   结果应该类似于以下示例：



6. 按 **Ctrl+X** 以退出 Nano，然后按下 **Y** 和 **Enter**，将您的编辑保存到 wp-config.php 文件。
7. 输入以下命令以重新启动实例上的服务：

```
sudo /opt/bitnami/ctlscript.sh restart
```

服务已重新启动时，您将看到与以下内容类似的结果：



关闭 SSH 窗口并切换回本教程前期打开的 Offload Media 页面。现在，您已准备就绪，可使用 WP Offload Media 插件创建 Amazon S3 存储桶。

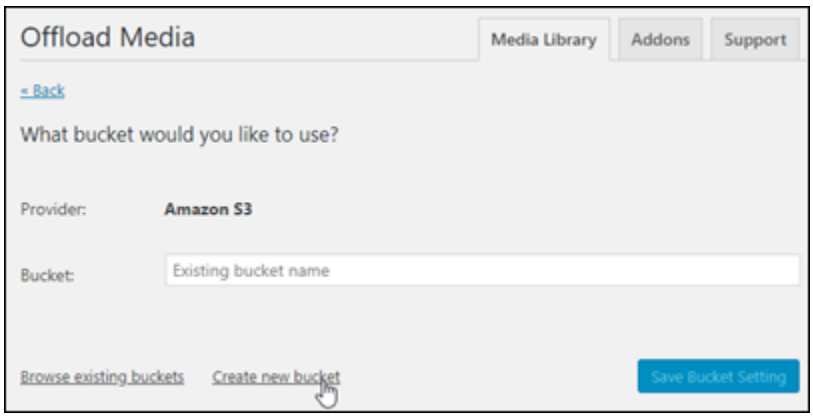
第 7 步：使用 WP Offload Media 插件创建 Amazon S3 存储桶

现在，wp-config.php 文件已使用亚马逊云科技凭证完成了配置，您可以返回 Offload Media 页面完成此流程。

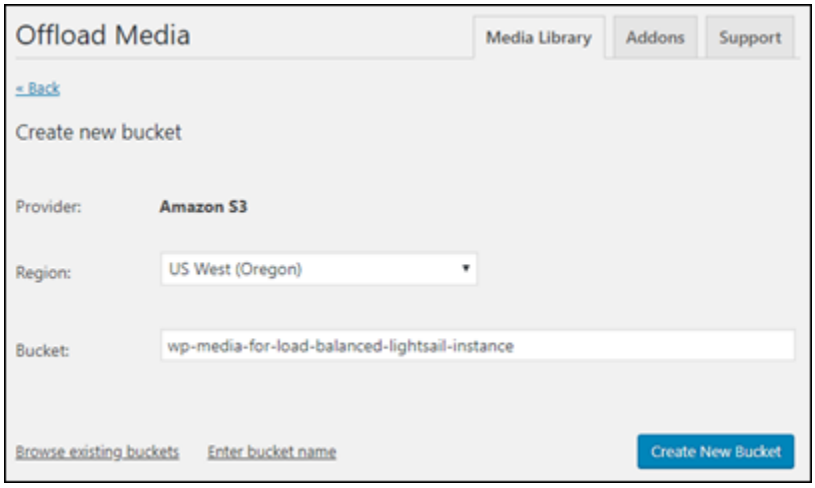
使用 WP Offload Media 插件创建 Amazon S3 存储桶

1. 刷新 Offload Media 页面，或选择 Next (下一步)。

   现在，您应该看到 Amazon S3 提供程序已配置。
2. 选择 Create new bucket (创建新的存储桶)。

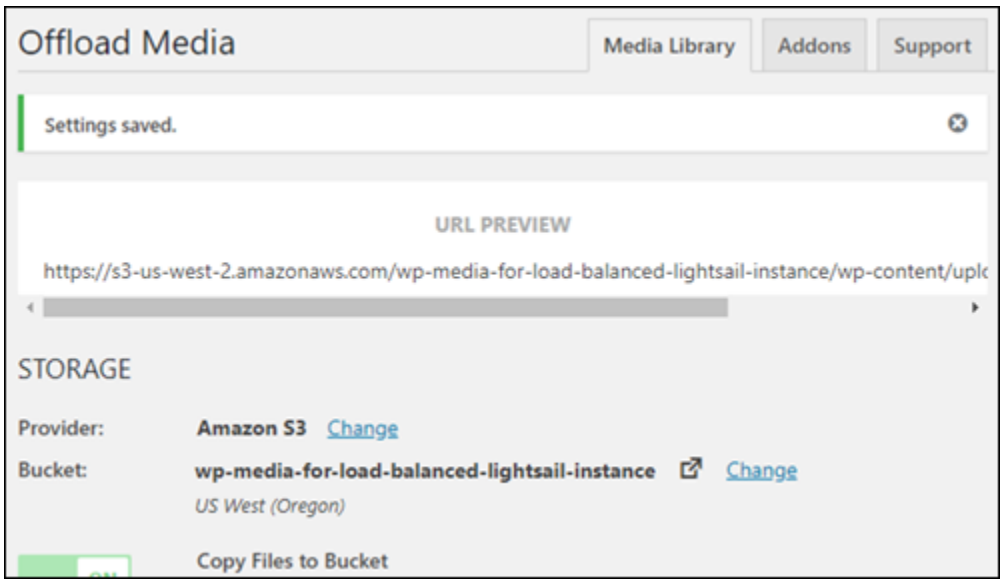


3. 在 Region (区域) 下拉菜单中，选择所需的亚马逊云科技区域。我们建议您选择 WordPress 实例所在的相同区域。
4. 在 Bucket (存储桶) 文本框中，输入新 S3 存储桶的名称。



5. 选择 Create New Bucket (创建新的存储桶)。

   此页面将刷新，以确认新存储桶已创建。查看显示的设置，并根据您希望 WordPress 网站的表现进行相应调整。



从现在开始，已添加到博客文章的图像和附件将自动上传到您已创建的 Amazon S3 存储桶中。

步骤 8：后续步骤

将 WordPress 网站连接到 Amazon S3 存储桶后，应创建 WordPress 实例快照以备份所做的更改。有关更多信息，请参阅创建 Linux 或 Unix 实例的快照。

将 Lightsail WordPress 实例连接到亚马逊 Aurora 数据库

帖子、页面和用户的网站数据存储在您的 Amazon Lightsail WordPress 实例上运行的数据库中。如果实例出现故障，您的数据可能会变得无法恢复。要避免这种情况，您应将网站数据转移到 Amazon Relational Database Service（Amazon RDS）中的 Amazon Aurora 数据库中。

Amazon Aurora 是一种专为云构建的 MySQL 和 PostgreSQL 兼容关系数据库。它既具有传统企业数据库的性能和可用性，又具有开源数据库的简单性和成本效益。Aurora 作为 Amazon RDS 的一部分提供。Amazon RDS 是一项托管式数据库服务，让用户能够在云中更轻松地设置、操作和扩展关系数据库。有关更多信息，请参阅 Amazon Relational Database Service 用户指南和适用于 Aurora 的 Amazon Aurora 用户指南。

在本教程中，我们将向您展示如何将您的网站数据库从 Lightsail 中的 WordPress 实例连接到 Amazon RDS 中的 Aurora 托管数据库。

内容

- 步骤 1：完成先决条件

- 步骤 2：为您的 Aurora 数据库配置安全组
- 第 3 步：从 Lightsail 实例连接到你的 Aurora 数据库
- 步骤 4：将 MySQL 数据库从您的 WordPress 实例转移到您的 Aurora 数据库
- 步骤 5：进行配置 WordPress 以连接您的 Aurora 托管数据库

步骤 1：完成先决条件

在开始之前，您需要首先满足以下先决条件：

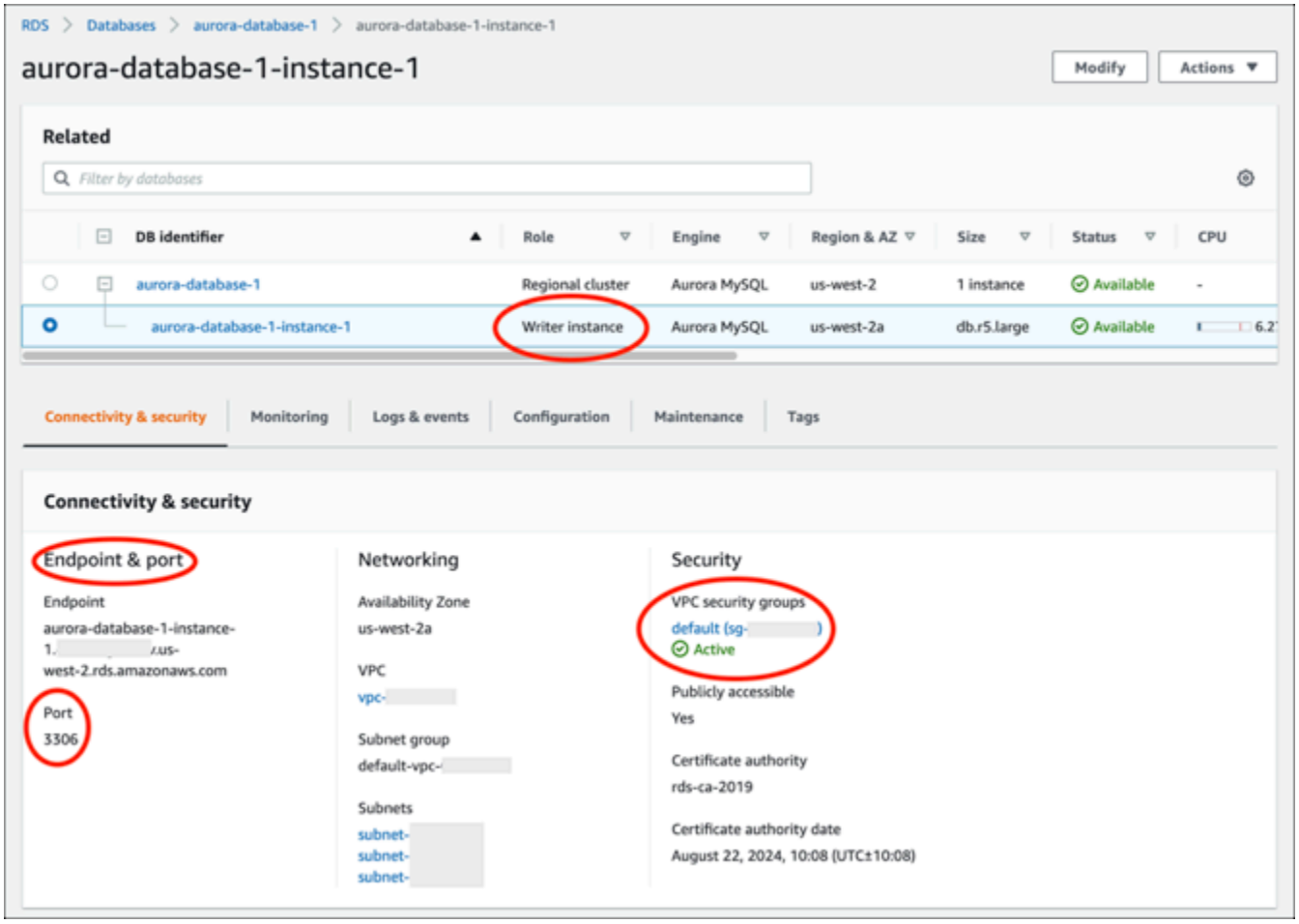
1. 在 Lightsail 中创建一个 WordPress 实例，并在其上配置您的应用程序。该实例的状态应处于正在运行后才能继续操作。有关更多信息，请参阅教程：在 Amazon Lightsai WordPress l 中启动和配置实例。
2. 在你的 Lightsail 账户中开启 VPC 对等互连。有关更多信息，请参阅设置对等互连以使用 Lightsail 之外的 AWS 资源。
3. 在 Amazon RDS 中创建 Aurora 托管式数据库。数据库必须与您的 WordPress 实例位于 AWS 区域 同一位置。其状态应处于正在运行后才能继续操作。有关更多信息，请参阅《Amazon Aurora 用户指南》中的 Amazon Aurora 入门。

步骤 2：为您的 Aurora 数据库配置安全组

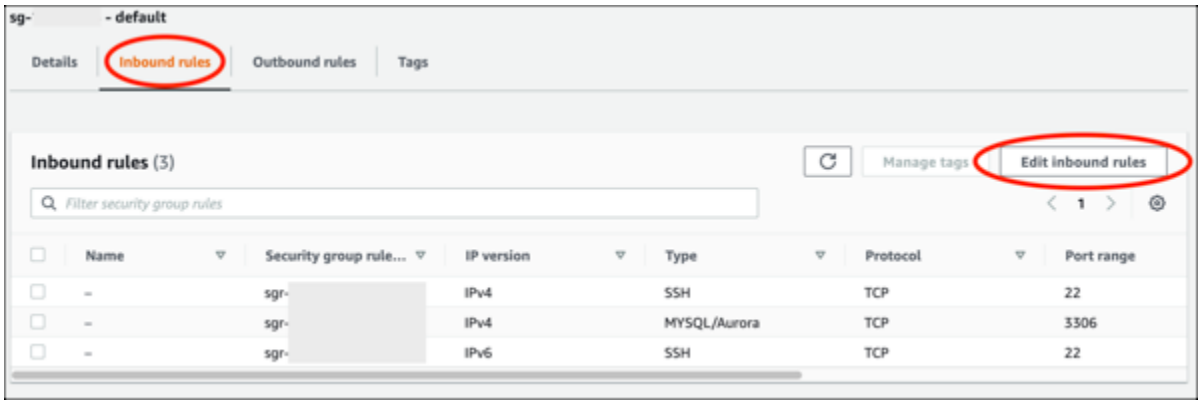
AWS 安全组充当 AWS 资源的虚拟防火墙。它会控制可以连接到 Amazon RDS 中的 Aurora 数据库的传入和传出流量。有关安全组的更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的使用安全组控制指向资源的流量。

完成以下过程以配置安全组，以便您的 WordPress实例可以与您的 Aurora 数据库建立连接。

1. 登录 Amazon RDS 控制台。
2. 在导航窗格中选择 Databases (数据库)。
3. 选择您的实例将要连接的 Aurora 数据库的 Writer WordPress 实例。
4. 选择连接和安全性选项卡。
5. 在 Endpoint & port（终端节点和端口），记下 Writer instance（写入器实例）的 Endpoint name（终端节点名称）和 Port（端口）。稍后在配置 Lightsail 实例以连接到数据库时，您将需要这些信息。
6. 在 Security（安全性）部分，选择活动 VPC 安全组的链接。您将会重新导向到数据库的安全组。



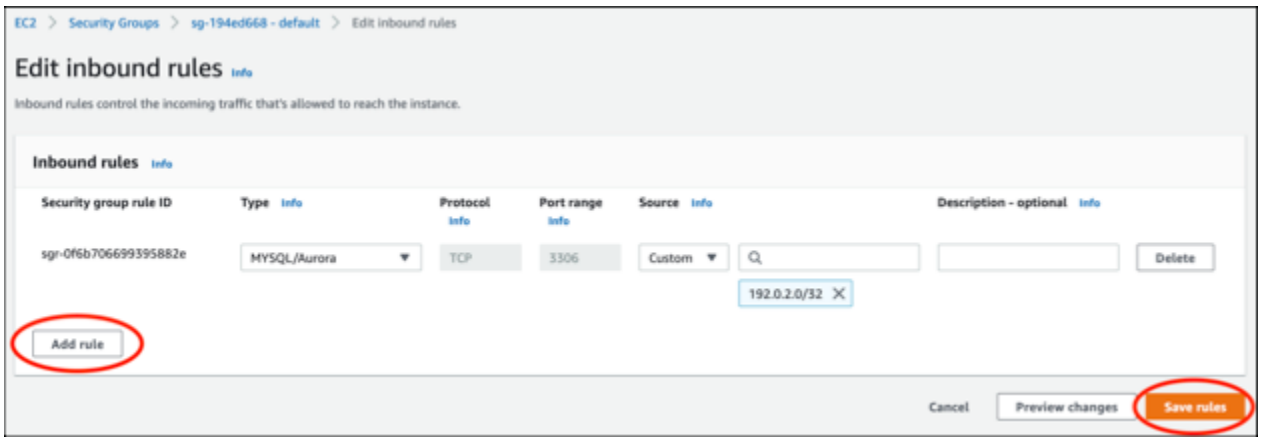
7. 确保已经选中您的 Aurora 数据库的安全组。
8. 选择入站规则选项卡。
9. 选择 Edit inbound rules（编辑入站规则）。



10. 在 Edit inbound rules（编辑入站规则）页面中，选择 Add rule（添加规则）。
11. 完成下列步骤之一：

- 如果您使用的是原定设置 MySQL 端口 3306，请在 Type（类型）下拉菜单中选择 MySQL/Aurora。
- 如果您使用的数据库的自定义端口，则在 Type（类型）下拉菜单中选择 Custom TCP（自定义 TCP），然后在 Port Range（端口范围）文本框中输入端口号。

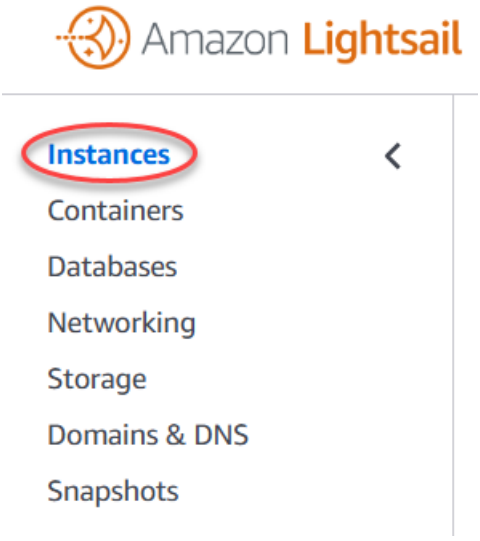
12. 在来源文本框中，添加您的 WordPress 实例的私有 IP 地址。您必须以 CIDR 表示法输入 IP 地址，这意味着必须在地址后附加 /32。例如，要允许 192.0.2.0，请输入 192.0.2.0/32。
13. 选择保存规则。



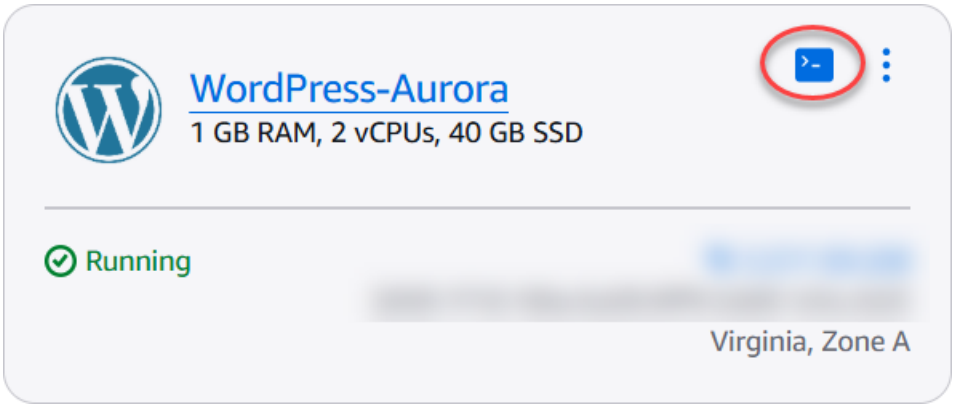
第 3 步：从 Lightsail 实例连接到你的 Aurora 数据库

完成以下过程以确认您可以从 Lightsail 实例连接到 Aurora 数据库。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。



3. 为您的实例选择基于浏览器的 SSH 客户端图标，以便使用 SSH 连接到该 WordPress 实例。



4. 连接到实例后，请输入以下命令以连接到您的 Aurora 数据库。在命令中，*DatabaseEndpoint*替换为 Aurora 数据库的终端节点地址，*Port*替换为数据库的端口。*MyUserName*替换为您在创建数据库时输入的用户名。

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

您应该会看到与以下示例类似的响应，其中确认您的实例可以访问并连接到您的 Aurora 数据库。

```
bitnami@ip-            $ mysql -h database.cluster-            .us-west-2.rds.amazonaws.
com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 215
Server version: 5.6.10 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

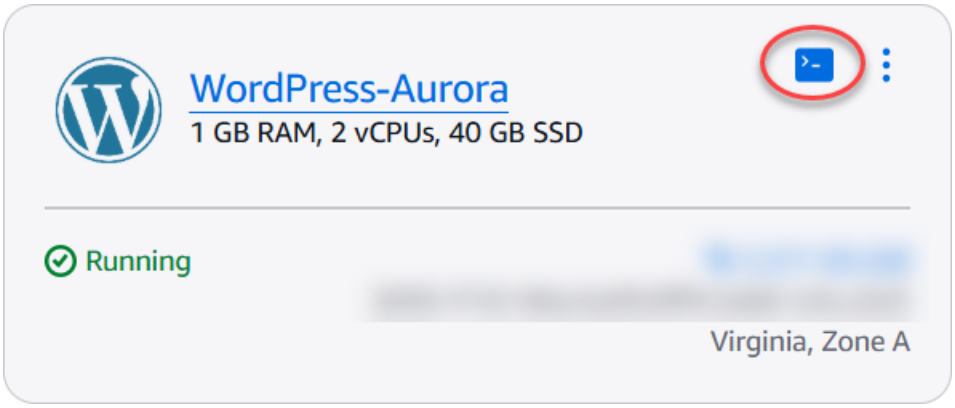
MySQL [(none)]>
```

如果您没有看到此响应，或者收到错误消息，则可能需要将 Aurora 数据库的安全组配置为允许您的 Lightsail 实例的私有 IP 地址连接到该数据库。有关更多信息，请参阅此指南中的为您的 Aurora 数据库配置安全组部分。

步骤 4：将数据库从您的 WordPress 实例传输到 Aurora 数据库

既然您已确认可以从您的实例连接到数据库，那么您应该将 WordPress 网站数据传输到 Aurora 数据库。

1. 登录 Lightsail 控制台。
2. 在实例选项卡中，为您的实例选择基于浏览器的 SSH 客户端。 WordPress



3. 在基于浏览器的 SSH 客户端连接到您的 WordPress 实例后，输入以下命令。该命令会将数据从实例上的 `bitnami_wordpress` 数据库传输并转移到您的 Aurora 数据库中。在命令中，*DatabaseUserName*使用您在创建 Aurora 数据库时输入的主用户名替换。*DatabaseEndpoint*替换为您的 Aurora 数据库的终端节点地址。

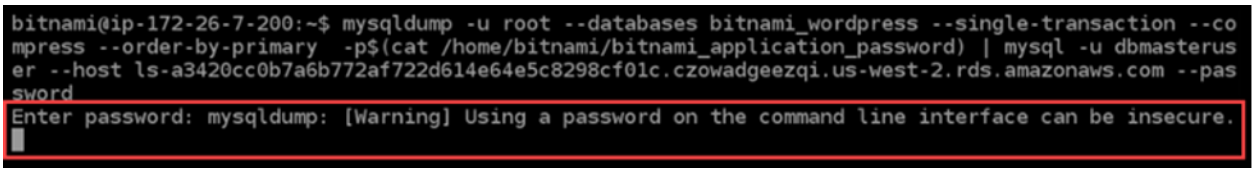
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) |
 sudo mysql -u DatabaseUserName --host  DatabaseEndpoint --password
```

示例

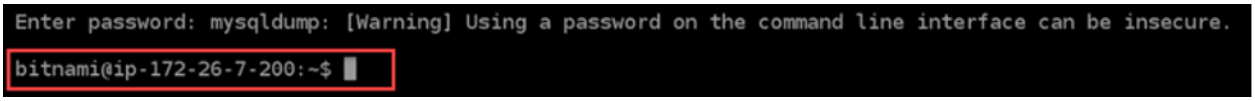
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password)
 | sudo mysql -u DBuser --host  abc123exampleE67890.czowadgeezqi.us-
west-2.rds.amazonaws.com --password
```

4. 在出现 `Enter password` 提示时，输入 Aurora 数据库的密码，然后按 Enter。

键入密码时，您将无法看到密码。



数据传输成功后，系统将会显示与以下示例类似的响应。



如果您遇到错误，请确认您使用的数据库用户名、密码和终端节点是否正确，然后重试。

步骤 5：进行配置 WordPress 以连接您的 Aurora 数据库

将应用程序数据传输到 Aurora 数据库后，应进行配置 WordPress 以连接到该数据库。完成以下过程编辑 WordPress配置文件 (wp-config.php)，以便您的网站连接到 Aurora 数据库。

1. 在连接到您的 WordPress 实例的基于浏览器的 SSH 客户端中，输入以下命令以创建文件备份：wp-config.php

```
cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
```

2. 输入以下命令以将 wp-config.php 文件设置为可写：

```
sudo chmod 664 /opt/bitnami/wordpress/wp-config.php
```

3. 请将 config 文件中的数据库用户名编辑为您在创建 Aurora 数据库时输入的主用户的名称。

```
sudo wp config set DB_USER DatabaseUserName
```

4. 使用 Aurora 数据库的端点地址和端口号编辑 config 文件中的数据库主机。例如，abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306。

```
sudo wp config set DB_HOST DatabaseEndpoint:Port
```

5. 使用 Aurora 数据库的密码编辑 config 文件中的数据库密码。

```
sudo wp config set DB_PASSWORD DatabasePassword
```

6. 输入 wp config list 命令验证您在 wp-config.php 文件中输入的信息是否正确。

```
sudo wp config list
```

结果将与以下示例类似，其中显示您的配置详细信息：

```
bitnami@ip-1          :~$ sudo wp config list
+--------------------+-----------------------------------------------------+----------+
| name               | value                                               | type     |
+--------------------+-----------------------------------------------------+----------+
| table_prefix       | wp_                                                 | variable |
| DB_NAME            | bitnami_wordpress                                   | constant |
| DB_USER            | admin                                               | constant |
| DB_PASSWORD        | Password1                                           | constant |
| DB_HOST            | database.cluster-           .us-west-2.rds.amazonaws | constant |
|                    | .com:3306                                           |          |
```

7. 输入以下命令以重新启动实例上的 Web 服务。

```
sudo /opt/bitnami/ctlscript.sh restart
```

在服务重新启动时，系统将会显示与以下示例类似的结果：



恭喜您！您的 WordPress 站点现已配置为使用您的 Aurora 数据库。

> **Note**
>
> 如果您需要还原原始 `wp-config.php` 文件，请输入以下命令，以使用您在本教程的之前部分创建的备份将其还原。
>
> ```
> cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
> ```

在 Lightsail 中将 WordPress 数据传输到 MySQL 托管数据库

帖子、页面和用户的关键 WordPress 网站数据存储在您的 Amazon Lightsail 实例上运行的 MySQL 数据库中。如果实例出现故障，您的数据可能会变得无法恢复。要避免这种情况，您应将网站数据传输到 MySQL 托管数据库。

在本教程中，我们将向您展示如何在 Lightsail 中将您的 WordPress 网站数据传输到 MySQL 托管数据库。我们还将向您展示如何编辑实例上的 WordPress 配置 (`wp-config.php`) 文件，以便您的网站连接到托管数据库，并停止连接到实例上运行的数据库。

内容

- 步骤 1：完成先决条件
- 步骤 2：将 WordPress 数据库传输到您的 MySQL 托管数据库
- 步骤 3：进行配置 WordPress 以连接您的 MySQL 托管数据库
- 步骤 4：完成后续步骤

步骤 1：完成先决条件

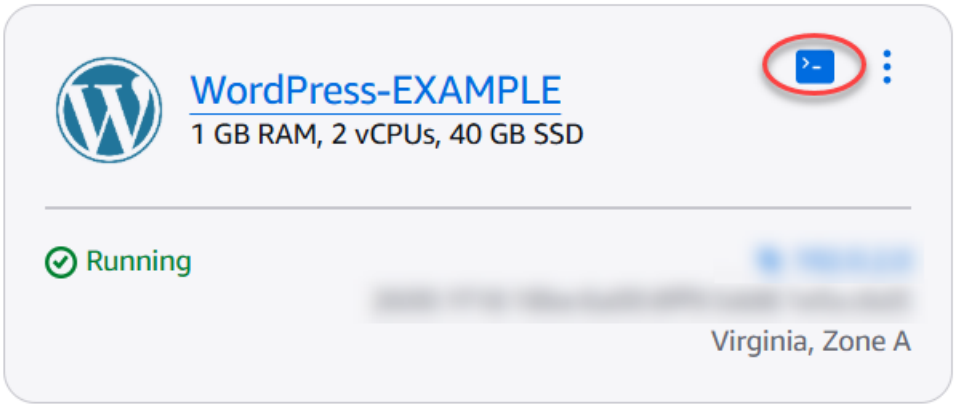
在开始之前，请满足以下先决条件：

- 在 Lightsail 中创建一个 WordPress 实例，并确保其处于运行状态。有关更多信息，请参阅教程：在 Amazon Lightsai WordPress l 中启动和配置实例。
- 在 Lightsail 中创建一个 MySQL 托管数据库，该数据库与您的 WordPress 实例位于相同的 AWS 区域，并确保其处于运行状态。 WordPress 适用于 Lightsail 中所有可用的 MySQL 数据库选项。有关更多信息，请参阅在 Amazon Lightsail 中创建数据库。
- 为 MySQL 托管数据库启用公有模式和数据导入模式。在完成本教程中的步骤后，可以禁用这些模式。有关更多信息，请参阅为您的数据库配置公有模式和为您的数据库配置数据导入模式。

步骤 2：将 WordPress 数据库传输到您的 MySQL 托管数据库

完成以下步骤，将您的 WordPress 网站数据传输到 Lightsail 中的 MySQL 托管数据库。

1. 登录 Lightsail 控制台。
2. 在实例选项卡中，为您的实例选择基于浏览器的 SSH 客户端图标。 WordPress



3. 在基于浏览器的 SSH 客户端连接到您的 WordPress 实例后，输入以下命令将您的实例上的`bitnami_wordpress`数据库中的数据传输到 MySQL 托管数据库。请务必*`DbUserName`*替换为托管数据库的用户名，并*`DbEndpoint`*替换为托管数据库的终端节点地址。

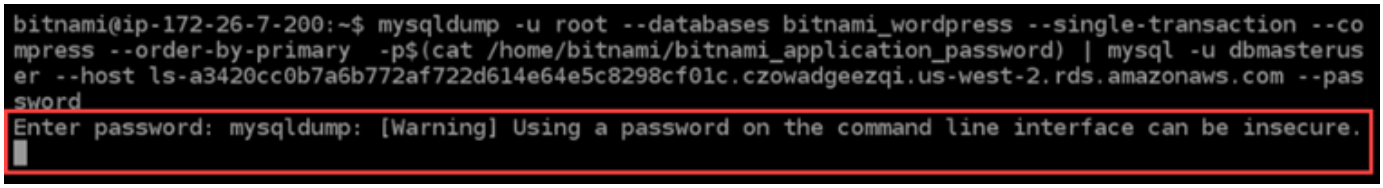
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary  -p$(cat /home/bitnami/bitnami_application_password) |
 sudo mysql -u DbUserName --host DbEndpoint --password
```

示例

```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password)
 | sudo mysql -u dbmasteruser --host ls-abc123exampleE67890.czowadgeezqi.us-
west-2.rds.amazonaws.com --password
```

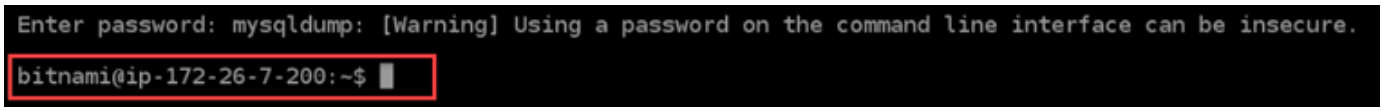
4. 在出现提示时，输入您的 MySQL 托管数据库的密码，然后按 Enter。

   在键入密码时，您将无法看到密码。



5. 如果已成功传输数据，则会显示与以下示例类似的结果。

   如果您收到错误，请确认您使用的是正确的数据库用户名、密码或端点，然后重试。



步骤 3：进行配置 WordPress 以连接您的 MySQL 托管数据库

完成以下步骤编辑 WordPress 配置文件 (wp-config.php)，以便您的网站连接到 MySQL 托管数据库。

1. 在连接到您的 WordPress 实例的基于浏览器的 SSH 客户端中，输入以下命令以创建wp-config.php文件备份，以防出现问题。

```
cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
```

2. 输入以下命令以使用 Nano 文本编辑器打开 wp-config.php 文件。

```
nano /opt/bitnami/wordpress/wp-config.php
```

3. 向下滚动直至您找到 DB_USER、DB_PASSWORD 和 DB_HOST 的值，如以下示例所示。

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'bitnami_wordpress');

/** MySQL database username */
define('DB_USER', 'bn_wordpress');

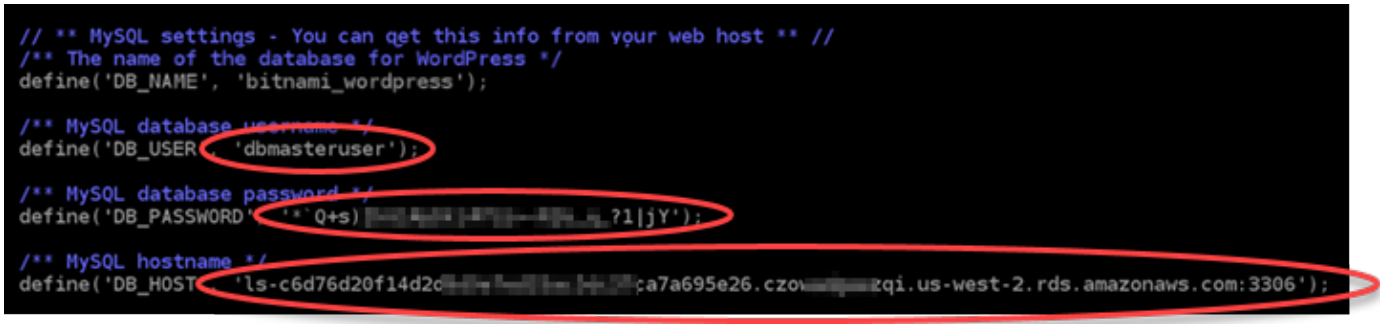
/** MySQL database password */
define('DB_PASSWORD', 'd6ab501583');

/** MySQL hostname */
define('DB_HOST', 'localhost:3306');
```

4. 修改以下值：

   - DB_USER – 编辑此值以匹配 MySQL 托管数据库的用户名。Lightsail 托管数据库的默认主用户名为。`dbmasteruser`
   - DB_PASSWORD – 编辑此值以匹配 MySQL 托管数据库的强密码。有关更多信息，请参阅管理数据库密码。
   - DB_HOST – 编辑此值以匹配 MySQL 托管数据库的端点。请务必在主机地址末尾添加 `:3306` 端口号。例如 `ls-abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306`。

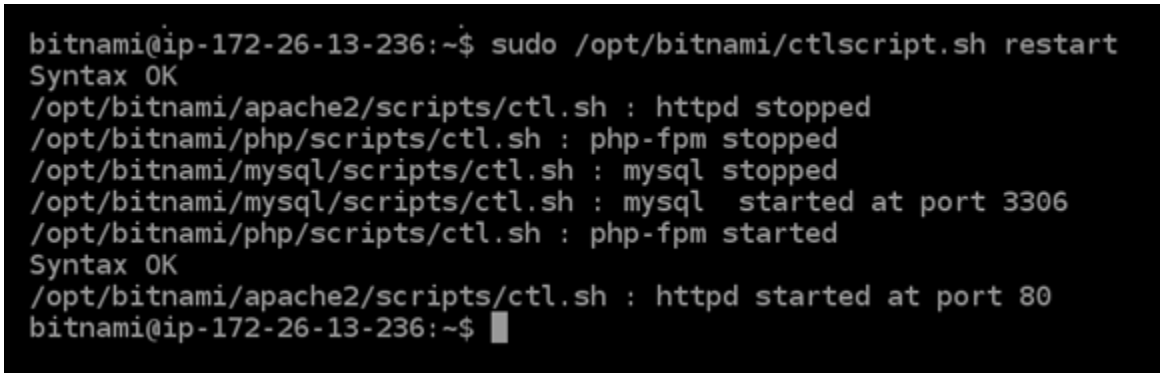
   结果应该类似以下示例。



5. 按 Ctrl+X 以退出 Nano，然后按 Y 和 Enter 以保存您的编辑。
6. 输入以下命令以重新启动实例的 Web 服务。

```
sudo /opt/bitnami/ctlscript.sh restart
```

   在服务已重新启动时，将显示与以下示例类似的结果。



恭喜您！您的 WordPress 站点现已配置为使用 MySQL 托管数据库。

> **Note**
>
> 如果出于任何原因您需要还原原始 `wp-config.php` 文件，请输入以下命令，以使用您在本教程的前面创建的备份还原它。
>
> ```
> cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
> ```

步骤 4：完成后续步骤

将 WordPress网站连接到 MySQL 托管数据库后，应完成以下额外步骤：

- 创建您的 WordPress 实例的快照。有关更多信息，请参阅创建 Linux 或 Unix 实例的快照。
- 创建 MySQL 托管数据库的快照。有关更多信息，请参阅创建数据库的快照。
- 禁用 MySQL 托管数据库的公有模式和数据导入模式。有关更多信息，请参阅为您的数据库配置公有模式和为您的数据库配置数据导入模式。

将 WordPress 实例连接到 Lightsail 存储桶以获取静态内容

本教程介绍了将在 Amazon Lightsail 实例上运行的 WordPress 网站连接到 Lightsail 存储桶所需的步骤。您可以使用存储桶托管静态内容，如图像和附件。为此，你必须在你的 WordPress 网站上安装 WP Offload Media Lite 插件，并将其配置为连接到你的 Lightsail 存储桶。配置插件后，您上传到 WordPress 网站的所有媒体都会自动添加到您的存储桶中，而不是实例的磁盘。

内容

- 步骤 1：完成先决条件
- 步骤 2：修改存储桶权限
- 第 3 步：在你的 WordPress网站上安装 WP Offload Media Lite 插件
- 第 4 步：测试你的 WordPress 网站与 Lightsail 存储桶之间的连接

步骤 1：完成先决条件

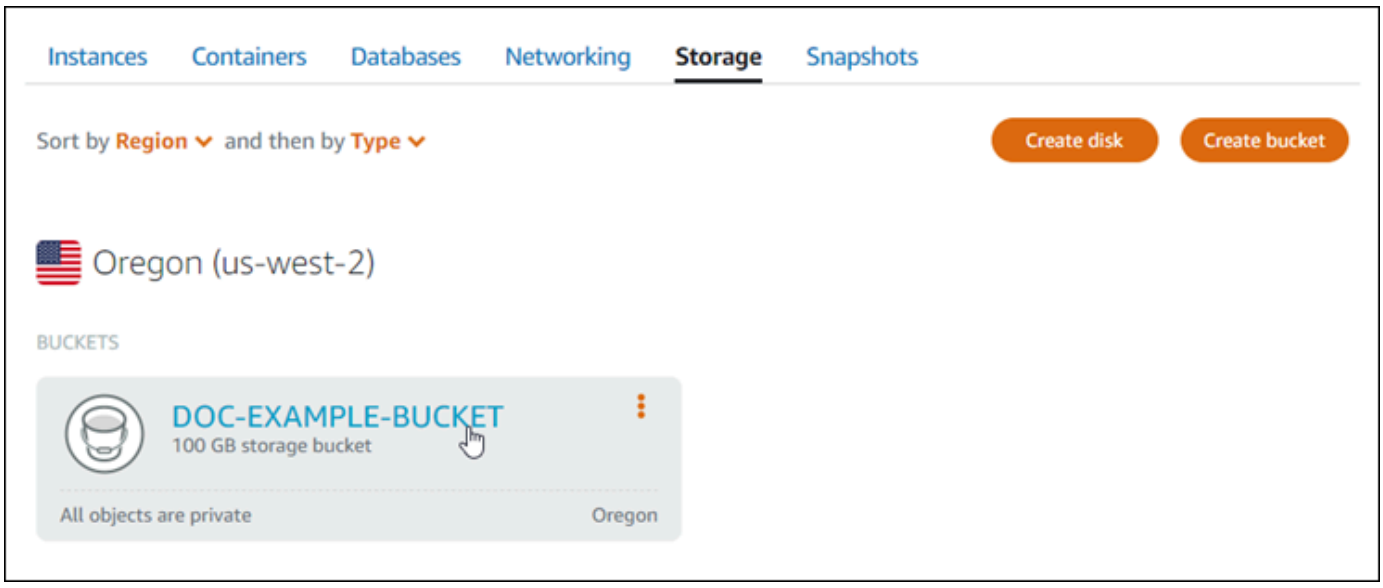
满足以下先决条件（如果尚未满足）：

- 在 Lightsail 中创建一个 WordPress 实例。有关更多信息，请参阅教程：在 Amazon Lightsai WordPress I 中启动和配置实例。
- 在 Lightsail 对象存储服务中创建存储桶。有关更多信息，请参阅创建存储桶。

步骤 2：修改存储桶权限

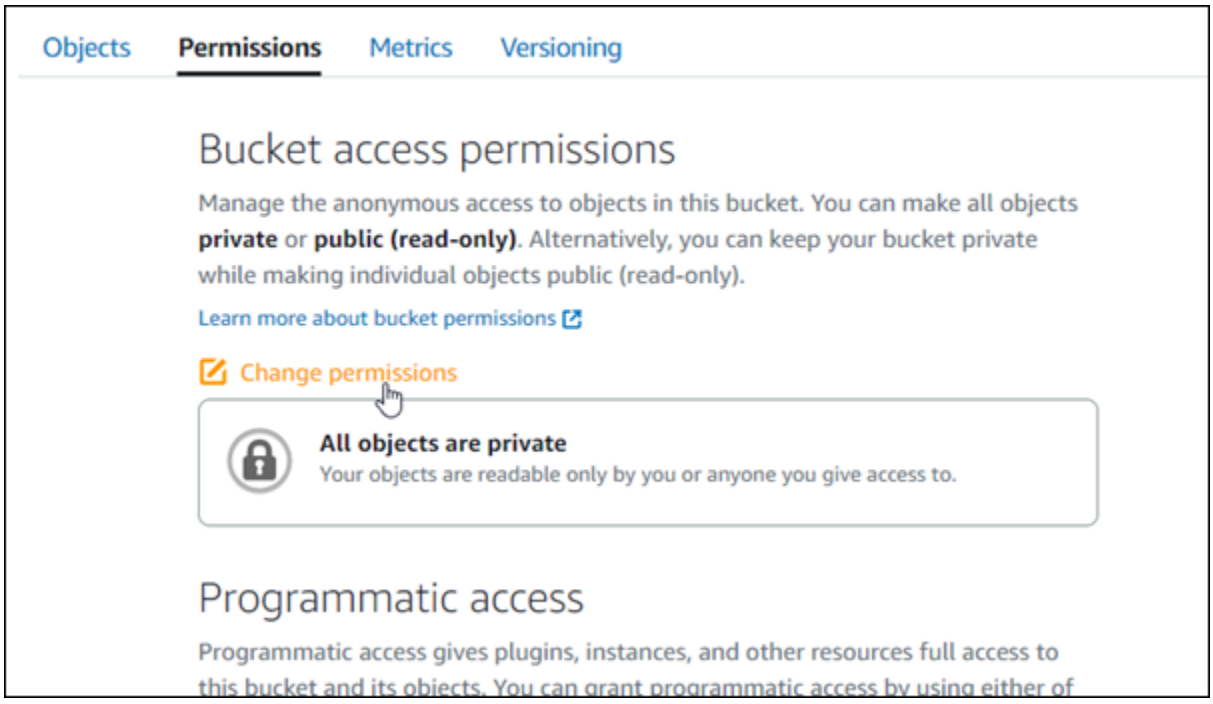
完成以下步骤以更改存储桶的权限，以允许访问您的 WordPress 实例和 Offload Media Lite 插件。存储桶的访问权限必须设置为个别对象可设为公有（只读）。您还必须将 WordPress 实例附加到存储桶的访问角色。有关存储桶权限的更多信息，请参阅存储桶权限。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择存储。
3. 选择您要用于 WordPress 网站的存储桶的名称。

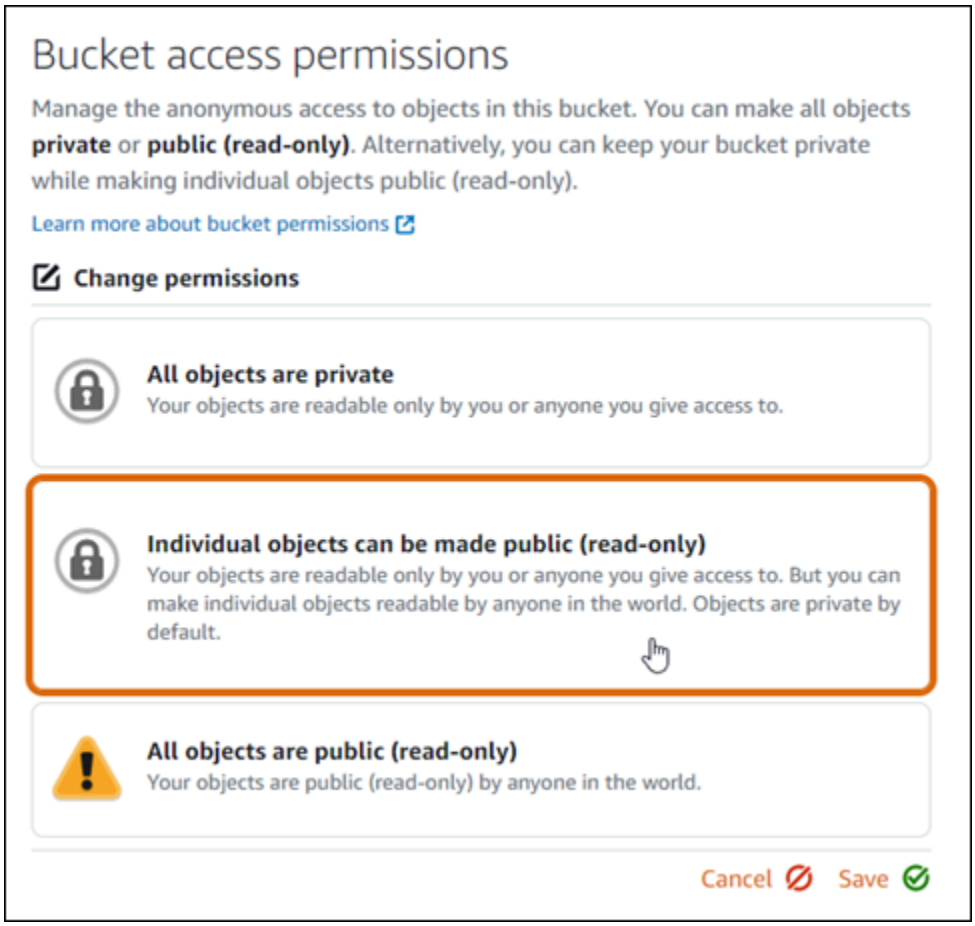


4. 在存储桶管理页面上选择权限选项卡。

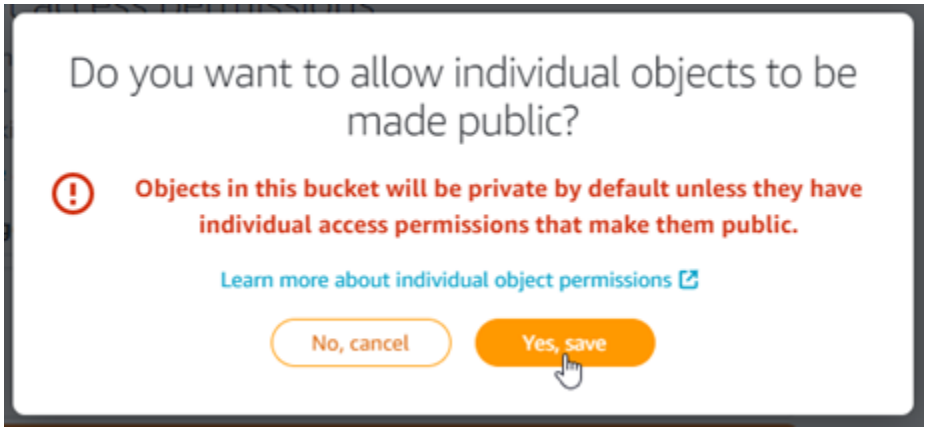
5. 在页面的存储桶访问权限部分下面选择更改权限。



6. 选择个别对象可设为公有（只读）。

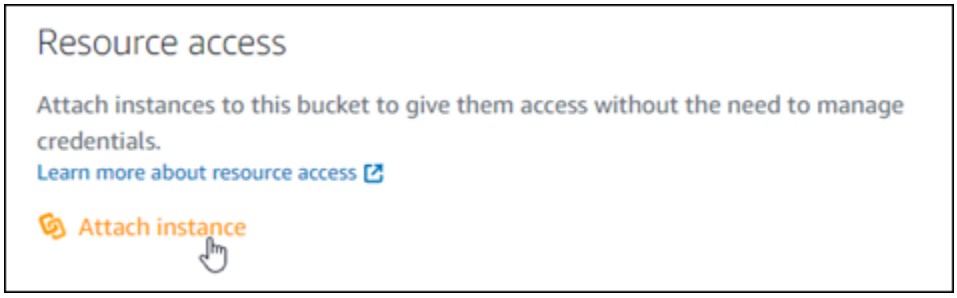


7. 选择保存。
8. 在显示的确认提示中选择是，保存。

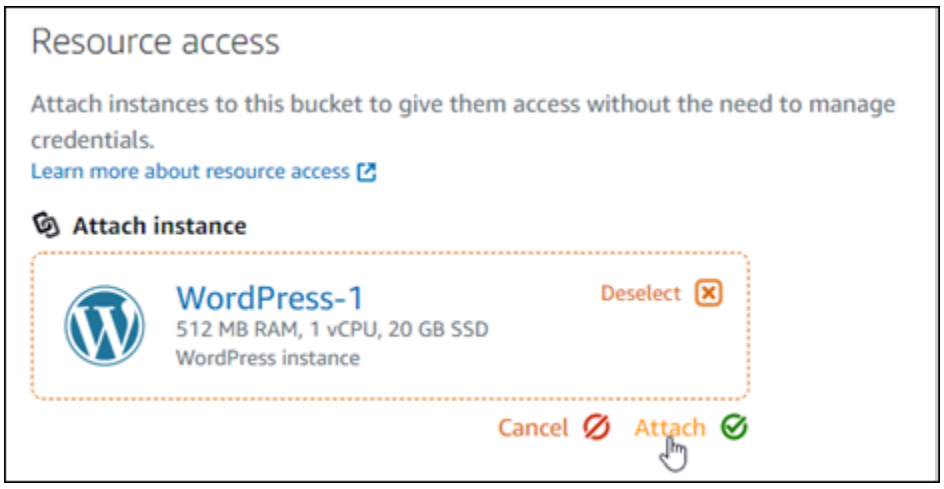


稍等片刻，存储桶将被配置为允许个别对象访问。这样可以确保客户可以读取使用 Offload Media Lite 插件从您的 WordPress 网站上传到您的存储桶的对象。

9. 滚动到页面的资源访问权限部分，然后选择附加实例。



10. 在出现的下拉列表中选择您的 WordPress 实例名称，然后选择附加。



片刻之后，您的 WordPress 实例将连接到您的存储桶。这使您的 WordPress 实例能够管理您的存储桶及其对象。

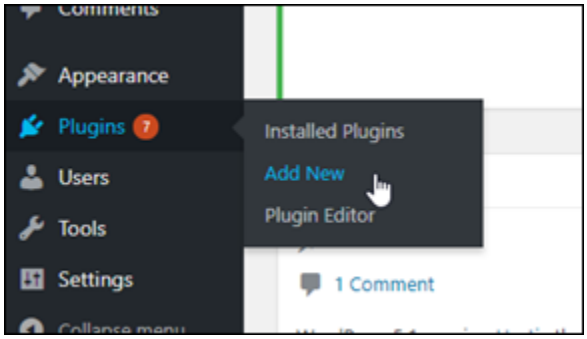
第 3 步：在你的 WordPress 网站上安装 WP Offload Media Lite 插件

完成以下步骤，在您的 WordPress 网站上安装 WP Offload Media Lite 插件。此插件会自动将通过媒体上传器添加的图像、视频、文档和任何其他媒体复制到您的 Lightsail 存储桶中。 WordPress 有关更多信息，请参阅WordPress 网站中的 WP Offload Media Lite。

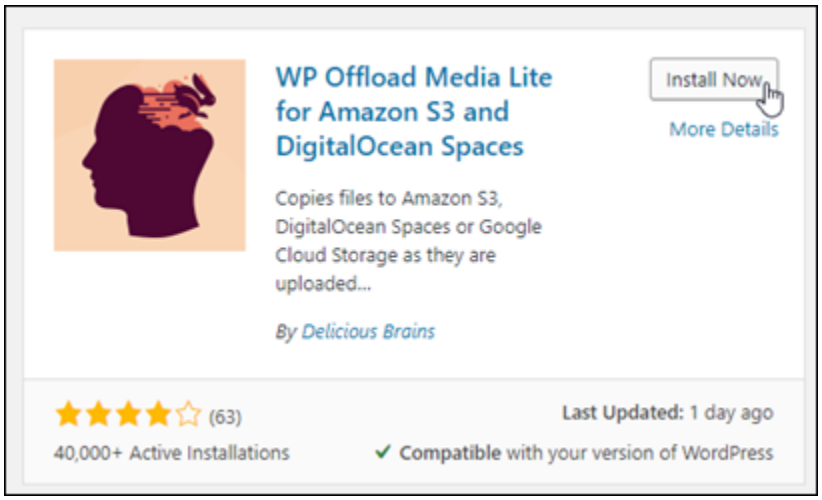
1. 以管理员身份登录 WordPress 网站的控制面板。

   有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

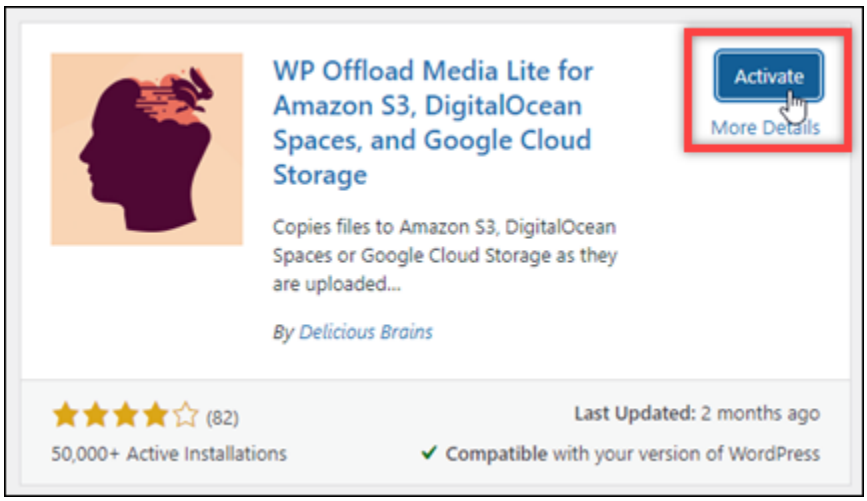
2. 在左侧导航菜单中暂停插件，然后选择新增。



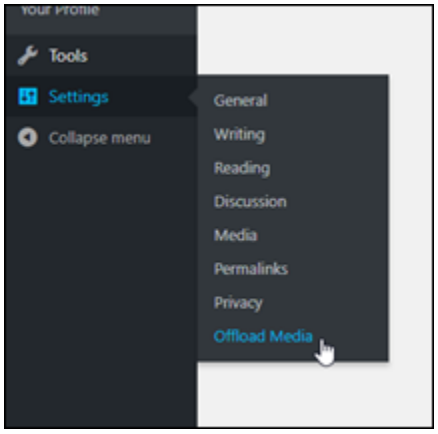
3. 搜索 WP Offload Media Lite。
4. 在搜索结果中，选择 WP Offload Media 插件旁边的立即安装。



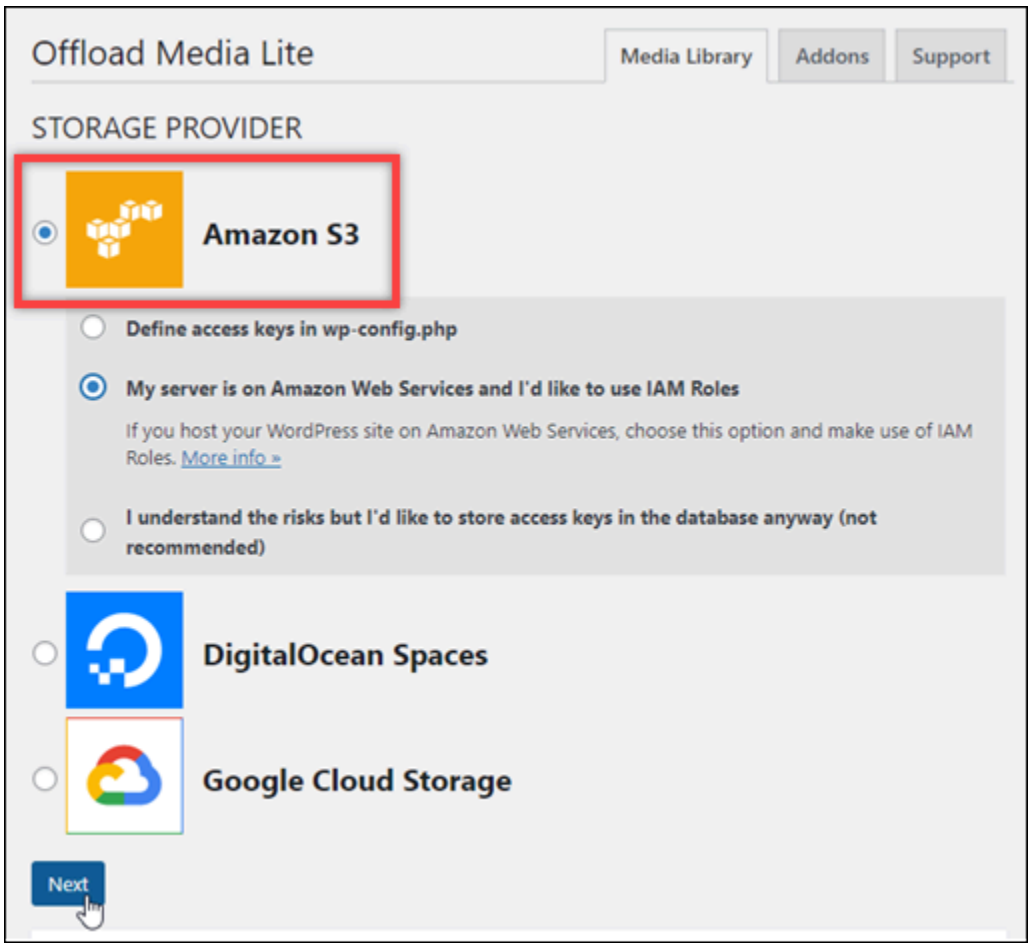
5. 完成插件安装后，选择 Activate (激活)。



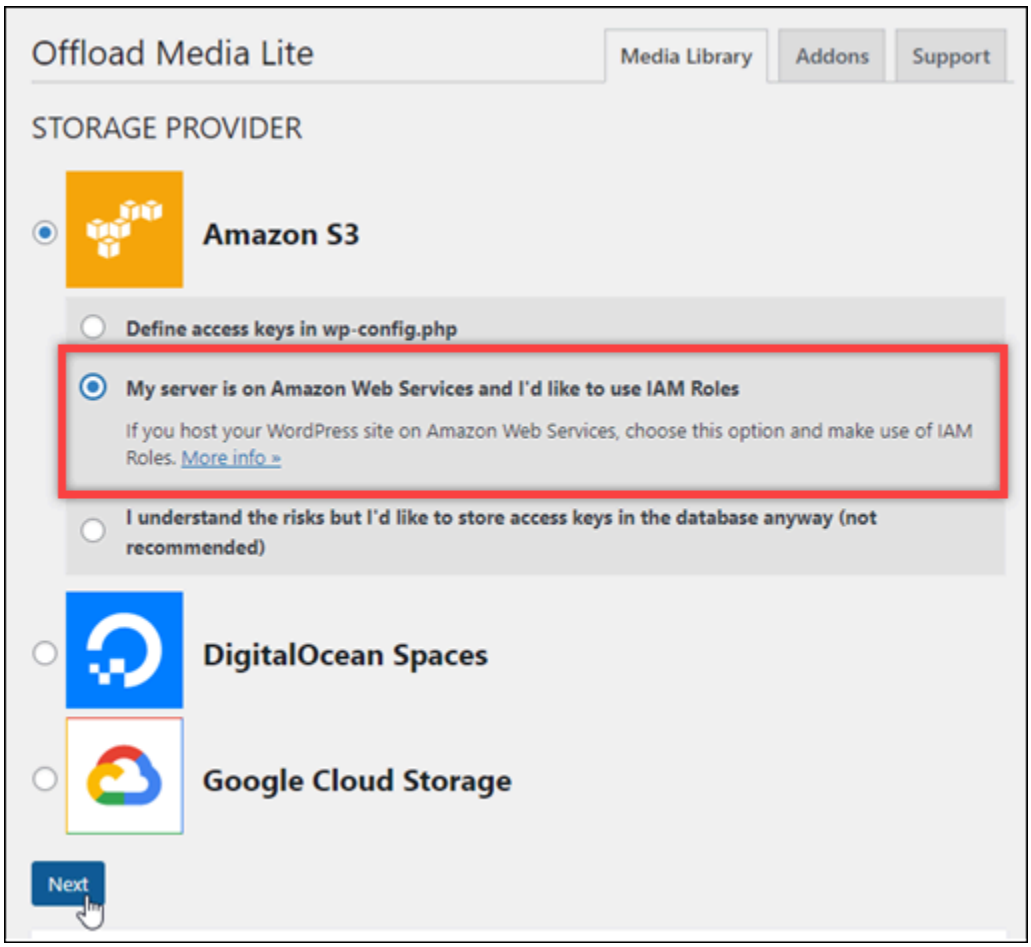
6. 在左侧导航菜单中，选择 Settings (设置)，然后选择 Offload Media。



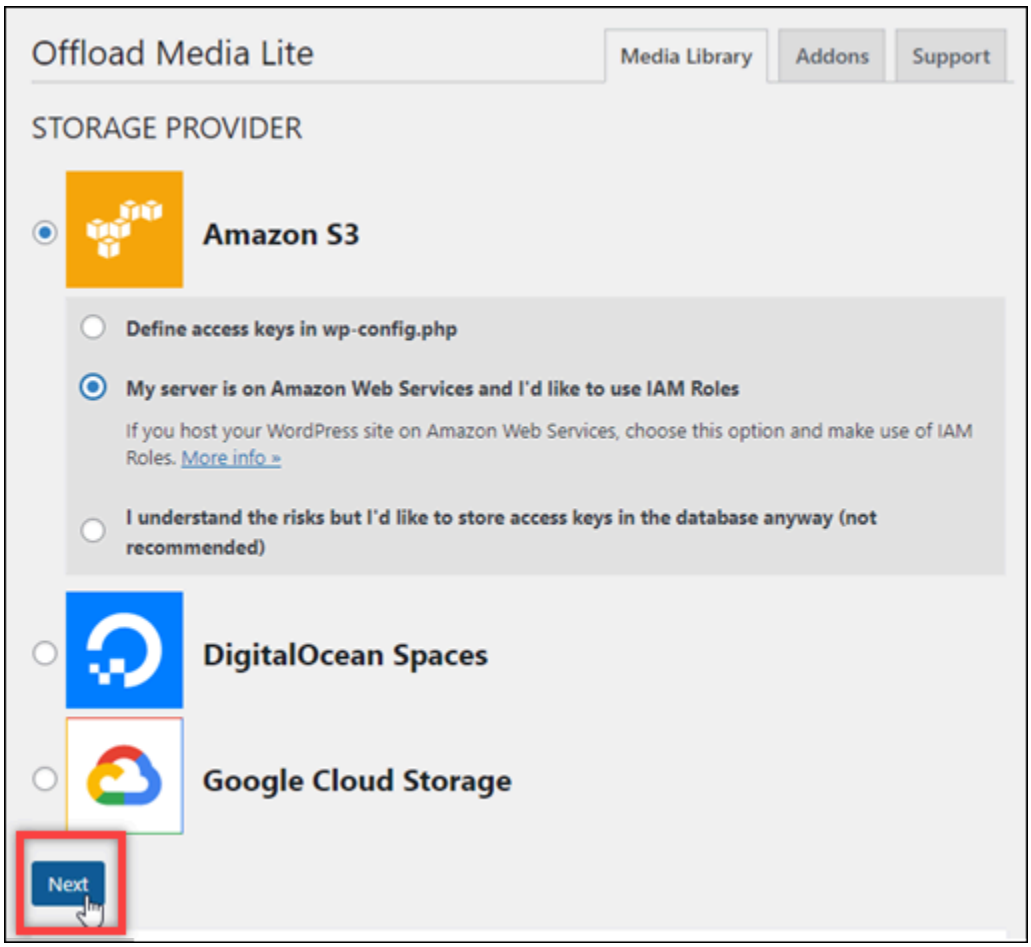
7. 在 Offload Media 页面上，选择Amazon S3作为存储提供程序。



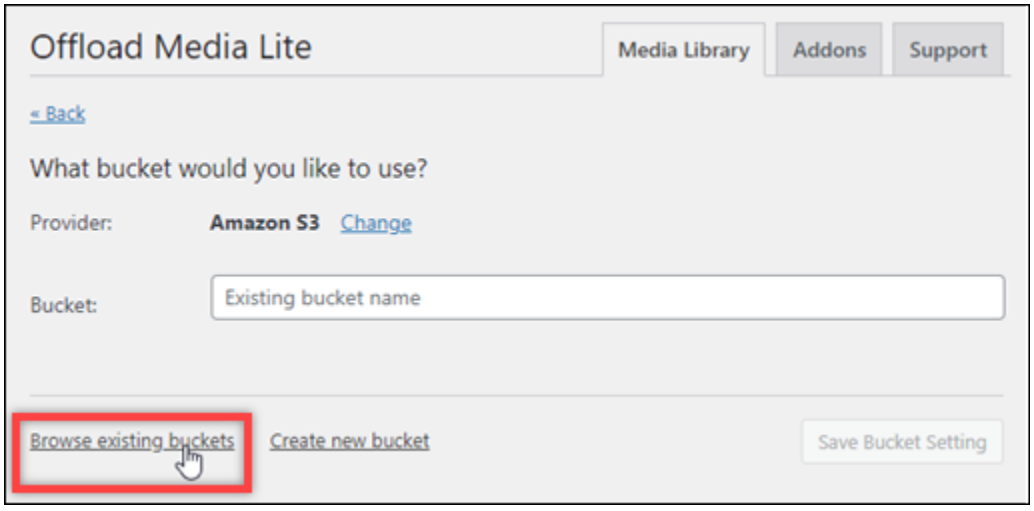
8. 选择我的服务器位于亚马逊云科技上，我想使用 IAM 角色。


Offload Media Lite
Media Library
Addons
Support
STORAGE PROVIDER
Amazon S3
Define access keys in wp-config.php
My server is on Amazon Web Services and I'd like to use IAM Roles
If you host your WordPress site on Amazon Web Services, choose this option and make use of IAM Roles. More info »
I understand the risks but I'd like to store access keys in the database anyway (not recommended)
DigitalOcean Spaces
Google Cloud Storage
Next

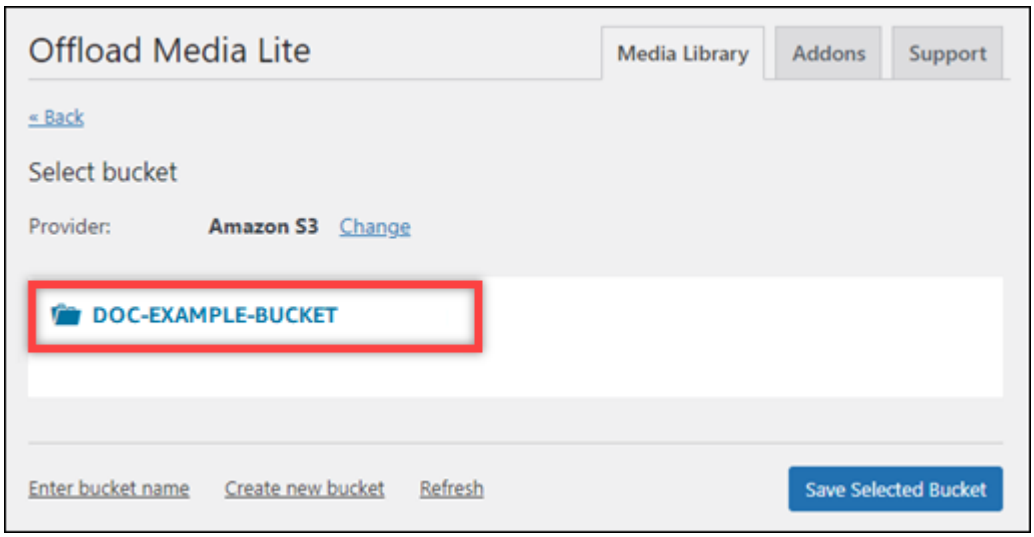
9. 选择下一步。



10. 在显示的您想要使用什么存储桶？页面中选择浏览现有存储桶。

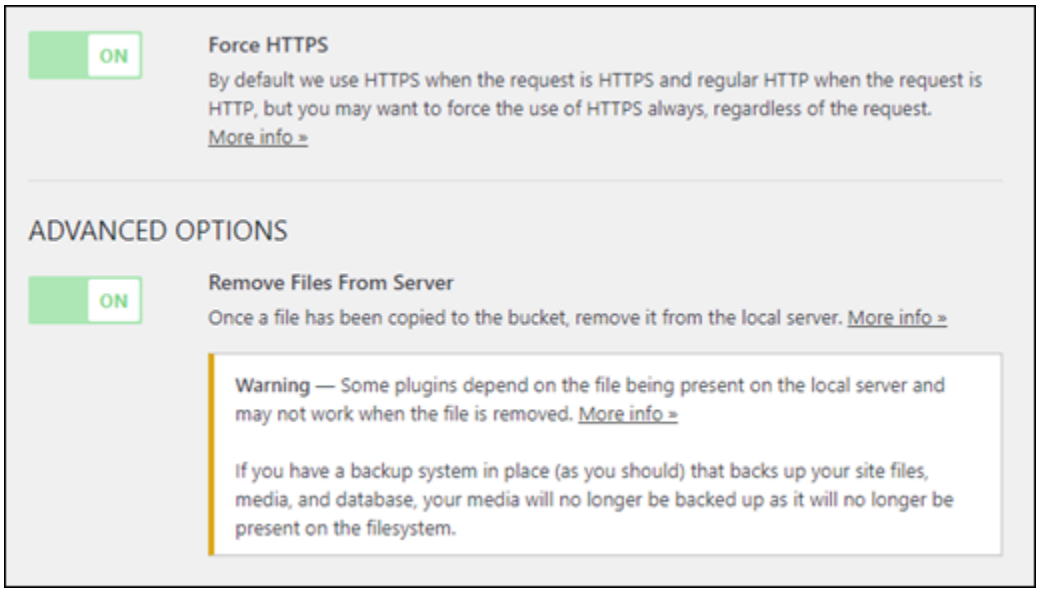


11. 选择要用于 WordPress实例的存储桶的名称。



12. 在显示的 Offload Media Lite 设置页面中，确保打开强制执行 HTTPS 和从服务器中删除文件。

    - 必须开启强制 HTTPS 设置，因为 Lightsail 存储桶默认使用 HTTPS 来提供媒体文件。如果您不开启此功能，则从您的 WordPress 网站上传到您的 Lightsail 存储桶的媒体文件将无法正确提供给您的网站访问者。
    - “从服务器移除文件” 设置可确保上传到 Lightsail 存储桶的媒体不会也存储在实例的磁盘上。如果您不开启此功能，则上传到您的 Lightsail 存储桶的媒体文件也会存储在实例的本地存储中。WordPress



13. 选择 Save Changes（保存更改）。

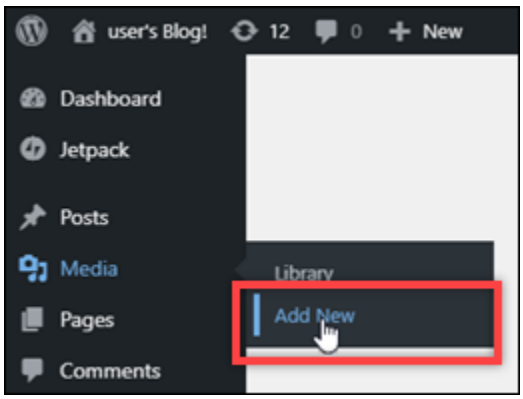
> **Note**
>
> 之后若要返回 Offload Media Lite 设置页面，请在左侧导航菜单中暂停设置，然后在选择 Offload Media Lite。

您的 WordPress 网站现已配置为使用 Media Lite 插件。下次您通过上传媒体文件时 WordPress，该文件会自动上传到您的 Lightsail 存储分区，并由存储桶提供。要测试配置，请继续执行本教程的下一部分。

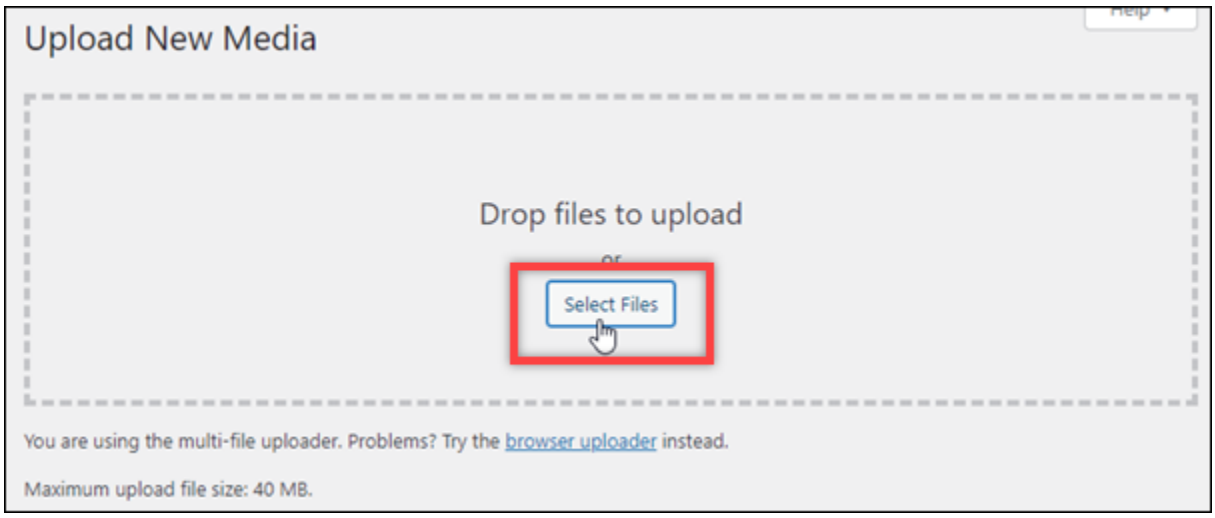
第 4 步：测试你的 WordPress 网站与 Lightsail 存储桶之间的连接

完成以下步骤将媒体文件上传到您的 WordPress 实例，并确认该文件已上传到您的 Lightsail 存储桶，并已从您的 Lightsail 存储桶中提供。

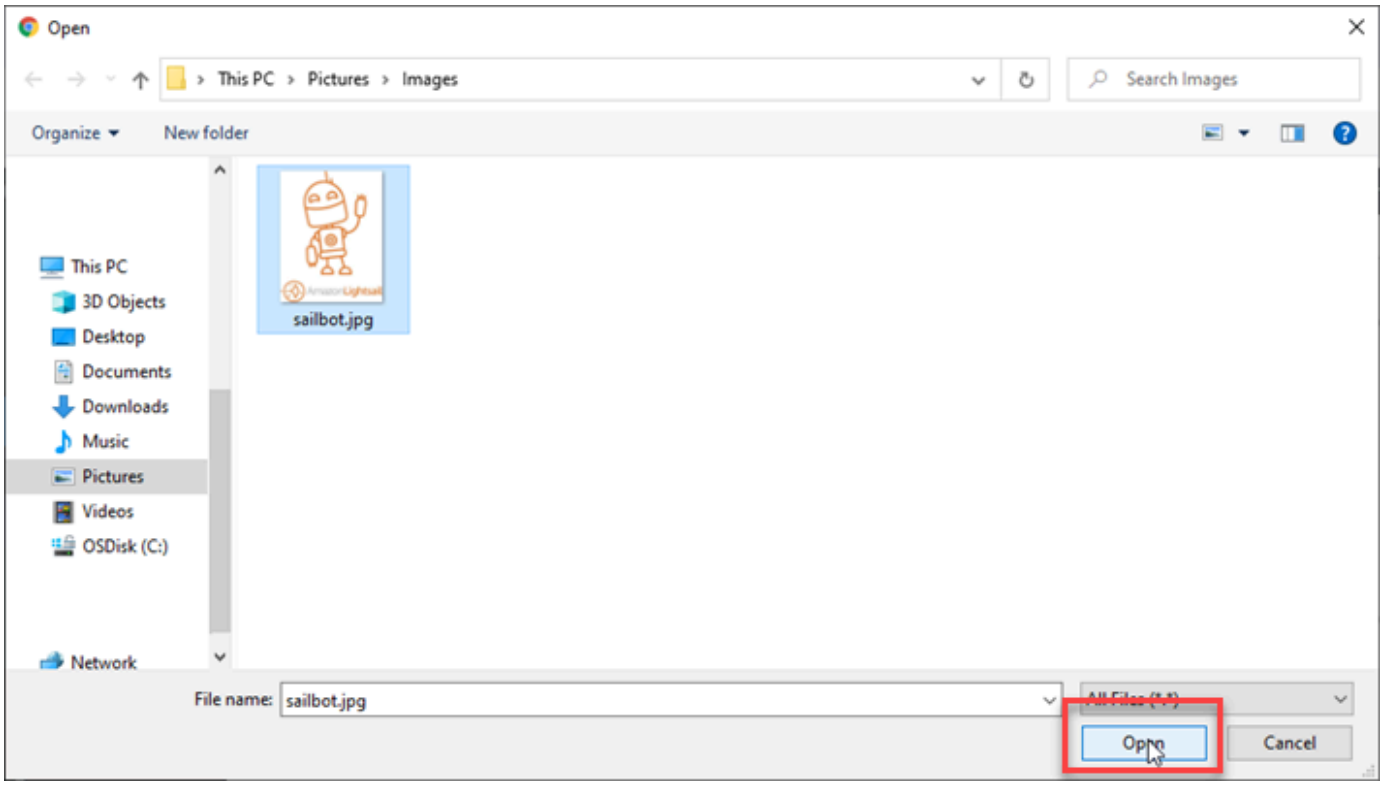
1. 在 WordPress仪表板左侧导航菜单中暂停在 “媒体” 上，然后选择 “新增”。



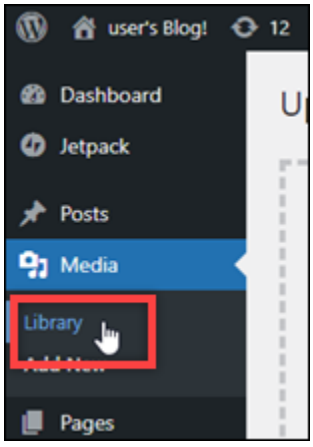
2. 在显示的“上传新媒体”页面上选择选择文件。



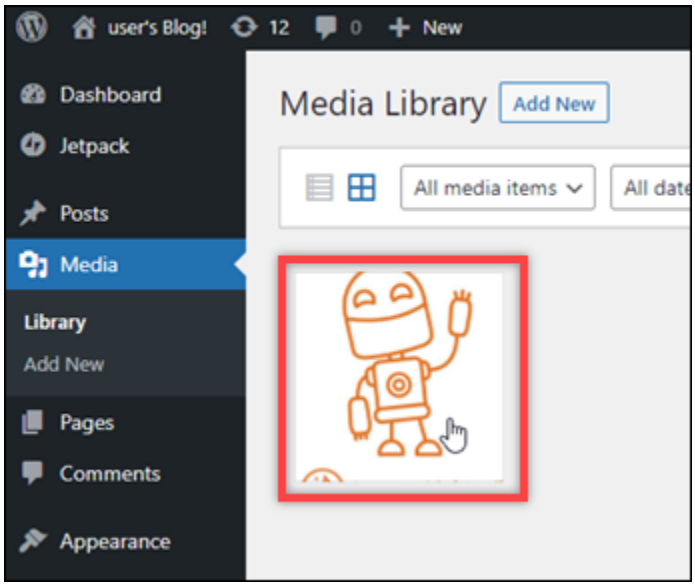
3. 选择要从本地计算机上传的媒体文件，然后选择打开。



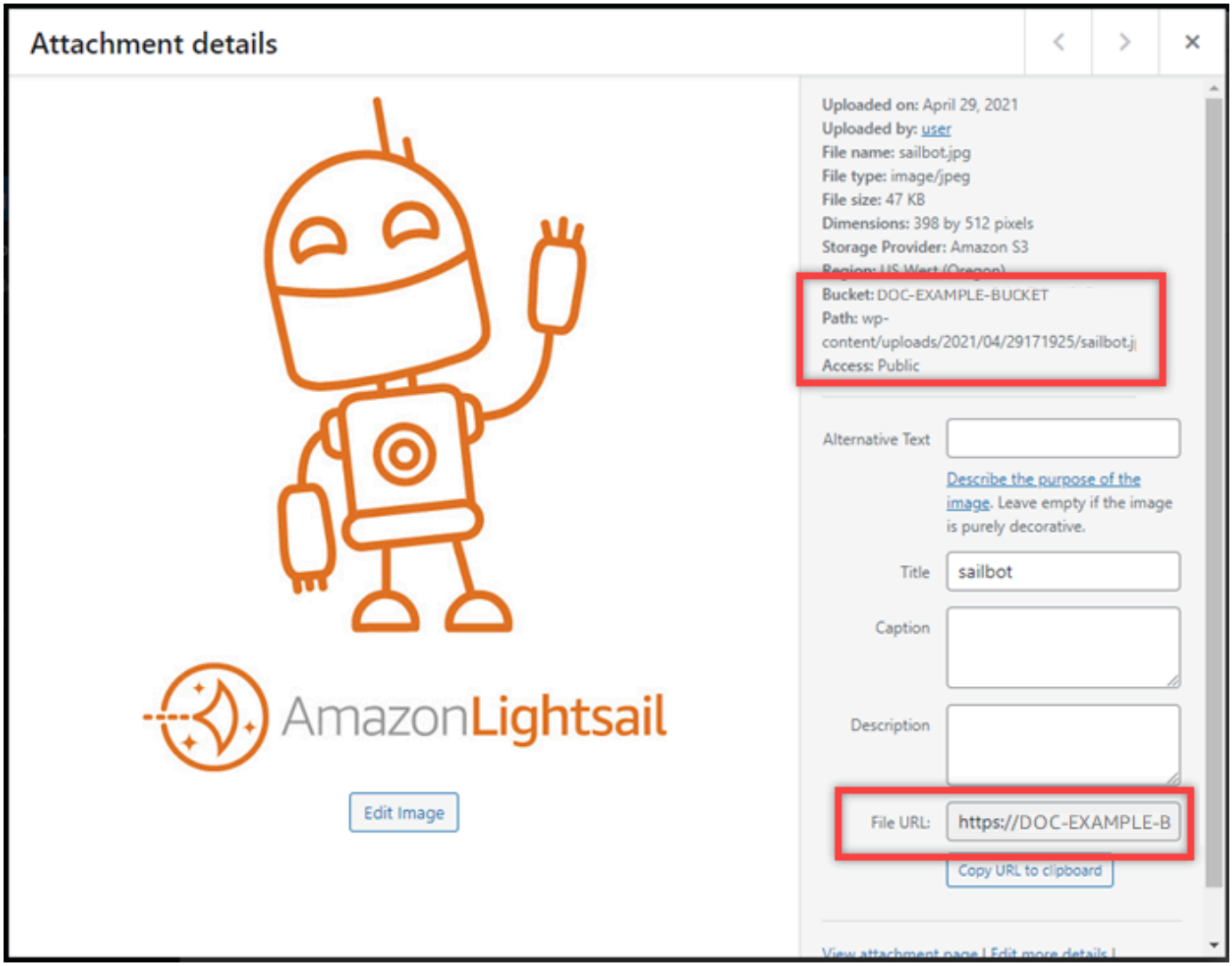
4. 文件完成上传后，在左侧导航菜单的媒体下方选择库。



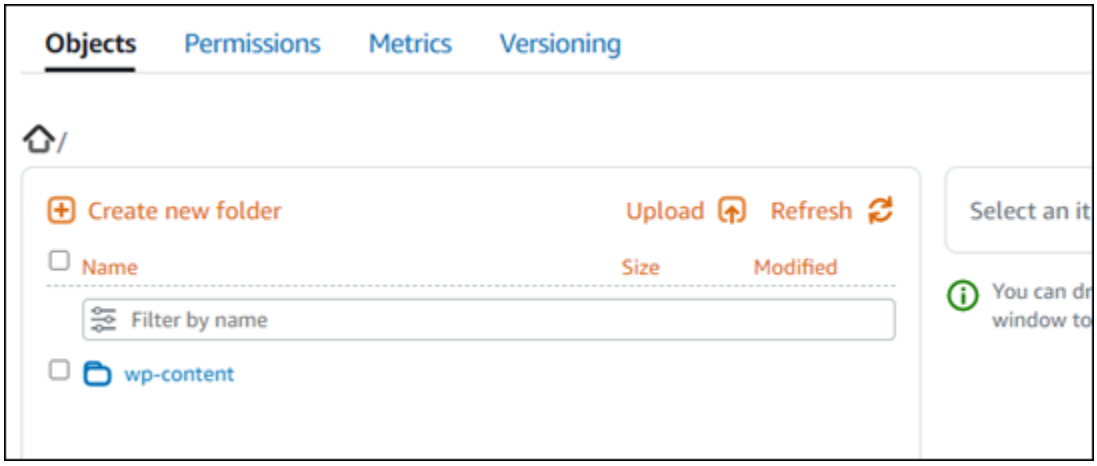
5. 选择您最近上传的文件。



6. 在文件的详细信息面板中，您应该在存储桶和文件 URL 字段中看到存储桶的名称。



7. 当你前往 Lightsail 存储分区管理页面的 “对象” 选项卡时，你应该会看到一个 w p-content 文件夹。此文件夹由 Offload Media Lite 插件创建，用于存储您上传的媒体文件。



管理存储桶和对象

以下是管理 Lightsail 对象存储桶的一般步骤：

1. 了解 Amazon Lightsail 对象存储服务中的对象和存储桶。有关更多信息，请参阅 Amazon Lightsail 中的对象存储。
2. 了解您可以在 Amazon Lightsail 中为存储桶命名的名称。有关更多信息，请参阅 Amazon Lightsail 中的存储桶命名规则。
3. 通过创建存储分区开始使用 Lightsail 对象存储服务。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶。
4. 了解存储桶的安全最佳实践以及您可以为存储桶配置的访问权限。您可以将存储桶中的所有对象设为公开或私有，也可以选择将单个对象设为公开。通过创建访问密钥、将实例附加到存储桶，以及向其他亚马逊云科技账户授予访问权限，还可以授予对存储桶的访问权限。有关更多信息，请参阅 Amazon Lights ail 对象存储的安全最佳实践和了解 Amazon Lights ail 中的存储桶权限。

   了解存储桶访问权限后，请参阅以下指南，授予对存储桶的访问权限：

   - 禁止公开访问亚马逊 Lightsail 中的存储桶
   - 在 Amazon Lightsail 中配置存储桶访问权限
   - 在 Amazon Lightsail 中为存储段中的单个对象配置访问权限
   - 在 Amazon Lightsail 中为存储桶创建访问密钥
   - 在 Amazon Lightsail 中为存储桶配置资源访问权限
   - 在 Amazon Lightsail 中为存储桶配置跨账户访问权限
5. 了解如何为存储桶启用访问日志记录，以及如何使用访问日志来审计存储桶的安全性。有关更多信息，请参阅以下指南。
   - 访问 Amazon Lightsail 对象存储服务中存储桶的日志记录
   - Amazon Lightsail 对象存储服务中存储桶的访问日志格式
   - 在 Amazon Lightsail 对象存储服务中为存储段启用访问日志记录
   - 使用 Amazon Lightsail 中存储段的访问日志来识别请求
6. 创建一个 IAM 策略，让用户能够在 Lightsail 中管理存储桶。有关更多信息，请参阅在 A mazon Lightsail 中管理存储桶的 IAM 政策。
7. 了解存储桶中对象的标记和识别方式。有关更多信息，请参阅了解 Amazon Lightsail 中的对象密钥名称。
8. 了解如何上传文件和管理存储桶中的对象。有关更多信息，请参阅以下指南。
   - 将文件上传到 Amazon Lightsail 中的存储桶

- 使用分段上传将文件上传到 Amazon Lightsail 中的存储桶
- 在 Amazon Lightsail 中查看存储桶中的对象
- 在 Amazon Lightsail 中复制或移动存储桶中的对象
- 从 Amazon Lightsail 中的存储桶下载对象
- 在 Amazon Lightsail 中筛选存储桶中的对象
- 在 Amazon Lightsail 中标记存储桶中的对象
- 在 Amazon Lightsail 中删除存储桶中的对象

9. 启用对象版本控制，可保留、检索和还原存储桶中存储的每个对象的各个版本。有关更多信息，请参阅 Amazon Lightsai l 中的存储桶中启用和暂停对象版本控制。

10启用对象版本控制后，您可以还原存储桶中对象的先前版本。有关更多信息，请参阅在 Amazon Lightsail 中恢复存储桶中对象的先前版本。

11监控存储桶的利用率。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标。

12配置存储桶指标的警报，以便在存储桶的利用率超过阈值时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建存储桶指标警报。

13如果存储桶的存储和网络传输不足，请更改存储桶的存储套餐。有关更多信息，请参阅在 Amazon Lightsail 中更改存储桶的计划。

14.了解如何将您的存储桶连接到其他资源。有关更多信息，请参阅以下教程。

- 教程：将 WordPress 实例连接到 Amazon Lightsail 存储桶
- 教程：使用带有 Lightsail 内容分发网络分发的 Amazon Lightsail 存储桶

15如果您不再使用存储桶，则将其删除。有关更多信息，请参阅在 Amazon Lightsail 中删除存储桶。

使用 Ligh WordPress tsail 内容分发网络进行配置

在本指南中，我们将向您展示如何配置您的 WordPress 实例以与 Amazon Lightsail 发行版配合使用。

默认情况下，所有 Lightsail 发行版都为其默认域启用了 HTTPS（例如）。`123456abcdef.cloudfront.net`分配的配置决定了分配与实例之间的连接是否已加密。

- 您的 WordPress 网站仅使用 HTTP — 如果您的网站仅使用 HTTP 作为分发来源，并且未配置为使用 HTTPS，则可以将分配配置为终止 SSL/TLS，并使用未加密的连接将所有内容请求转发到您的实例。
- 您的 WordPress 网站使用 HTTPS — 如果您的网站使用 HTTPS 作为分配的来源，则可以将分配配置为使用加密连接将所有内容请求转发到您的实例。此配置称为 end-to-end加密。

创建分配

完成以下步骤，为您的 WordPress实例配置 Lightsail 发行版。有关更多信息，请参阅 the section called “创建分配”。

先决条件

按照中所述创建和配置 WordPress 实例the section called “WordPress”。

为您的 WordPress 实例创建分配

1. 在左侧导航窗格中，选择联网。
2. 选择创建分配。
3. 在 “选择您的来源” 中，选择您运行 WordPress 实例的区域，然后选择您的 WordPress 实例。我们会自动使用您附加到实例的静态 IP 地址。
4. 对于 “缓存行为”，选择 “最适合” WordPress。
5. （可选）要配置 end-to-end加密，请将源协议策略更改为仅限 HTTPS。有关更多信息，请参阅 the section called “源协议策略”。
6. 配置剩余选项，然后选择创建分配。
7. 在自定义域选项卡上，选择创建证书。输入证书的唯一名称，输入您的域和子域的名称，然后选择创建证书。
8. 选择附加证书。
9. 对于更新 DNS 记录，选择我了解。

更新 DNS 记录

完成以下步骤以更新你的 Lightsail DNS 区域的 DNS 记录。

要更新分配的 DNS 记录

1. 在左侧导航窗格中，选择 域和 DNS。
2. 选择您的 DNS 区域，然后选择 DNS 记录选项卡。
3. 删除您在证书中指定的域的 A 和 AAAA 记录。
4. 选择添加记录并创建 CNAME 记录，该记录将您的域解析为分配的域（例如 d2vbec9EXAMPLE.cloudfront.net）。
5. 选择保存。

允许分配缓存静态内容

完成以下步骤编辑您的 WordPress 实例中的`wp-config.php`文件，使其适用于您的发行版。

> **Note**
>
> 我们建议您在开始使用此过程之前创建 WordPress 实例的快照。快照可用作备份，如果出现问题，您便可以从中创建另一个实例。有关更多信息，请参阅创建 Linux 或 Unix 实例的快照。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择显示在您的 WordPress 实例旁边的基于浏览器的 SSH 客户端图标。
3. 连接到实例后，请输入以下命令来创建 `wp-config.php` 文件的备份。如果出现问题，您可以使用备份还原文件。

   ```
   sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php.backup
   ```

4. 输入以下命令以使用 Vim 打开 `wp-config.php` 文件。

   ```
   sudo vim /opt/bitnami/wordpress/wp-config.php
   ```

5. 按 I 进入 Vim 的插入模式。
6. 删除文件中的以下代码行。

   ```
   define('WP_SITEURL', 'http://' . $_SERVER['HTTP_HOST'] . '/');
   define('WP_HOME', 'http://' . $_SERVER['HTTP_HOST'] . '/');
   ```

7. 根据您使用的版本向文件中添加以下代码行之一： WordPress

   - 如果您使用 3.3 或更低版本，请在之前删除代码的位置添加如下代码行。

     ```
     define('WP_SITEURL', 'https://' . $_SERVER['HTTP_HOST'] . '/');
     define('WP_HOME', 'https://' . $_SERVER['HTTP_HOST'] . '/');
     if (isset($_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'])
     && $_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'] === 'https') {
     $_SERVER['HTTPS'] = 'on';
     }
     ```

   - 如果您使用 3.3.1-5 或更高版本，请在之前删除代码的位置添加如下代码行。

```
define('WP_SITEURL', 'http://DOMAIN/');
define('WP_HOME', 'http://DOMAIN/');
if (isset($_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'])
&& $_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'] === 'https') {
$_SERVER['HTTPS'] = 'on';
}
```

8. 按 ESC 键退出 Vim 的插入模式，然后输入 `:wq!` 并按 Enter 以保存您的编辑内容（写入），再退出 Vim。
9. 输入以下命令以重新启动实例的 Apache 服务。

   ```
   sudo /opt/bitnami/ctlscript.sh restart apache
   ```

10. 稍等片刻，让 Apache 服务重新启动，然后测试您的分配是否正在缓存内容。有关更多信息，请参阅测试您的亚马逊 Lightsail 发行版。
11. 如果出现问题，请使用基于浏览器的 SSH 客户端重新连接到您的实例。运行以下命令以使用您之前在本指南中创建的备份来还原 `wp-config.php` 文件。

    ```
    sudo cp /opt/bitnami/wordpress/wp-config.php.backup /opt/bitnami/wordpress/wp-config.php
    ```

    还原文件后，请输入以下命令以重新启动 Apache 服务：

    ```
    sudo /opt/bitnami/ctlscript.sh restart apache
    ```

有关分配的其他信息

以下是一些可以帮助你在 Lightsail 中管理发行版的文章：

- 内容分发网络分配
- 创建分配
- 了解分配的请求和响应行为
- 测试分配
- 更改分配的源
- 更改分配的缓存行为
- 重置分配的缓存

- 更改分配的套餐
- 启用分配的自定义域
- 将域指向分配
- 更改分配的自定义域
- 禁用分配的自定义域
- 查看分配指标
- 删除分配

在 Lightsail 中为 WordPress实例启用电子邮件

您可以在 Amazon Lightsail 中为您的 WordPress 实例启用电子邮件。在 Amazon Simple Email Service（Amazon SES）中配置 SMTP 服务。然后，在您的实例上激活并配置 WP Mail SMTP 插件。启用电子邮件后，您的 WordPress 管理员可以请求重置其用户个人资料的密码，并会收到有关博客文章、网站更新和其他插件消息的电子邮件通知。本指南向您展示如何使用 Amazon SES 在 Amazon Lightsail 中的 WordPress 实例上启用电子邮件。

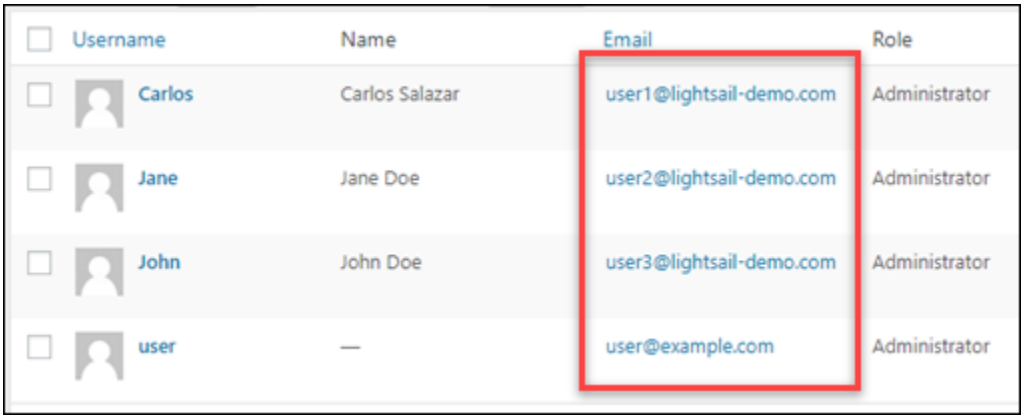
内容

- 步骤 1：查看限制
- 步骤 2：完成先决条件
- 步骤 3：在 Amazon SES 中创建 SMTP 凭证
- 步骤 4：在 Amazon SES 中验证域
- 步骤 5：在 Amazon SES 中验证电子邮件地址
- 第 6 步：在您的 WordPress 实例上配置 WP 邮件 SMTP 插件

有关更多信息，请参阅 Amazon SES 文档中的使用 Amazon SES SMTP 接口发送电子邮件。

步骤 1：查看限制

Amazon SES 沙盒中的新亚马逊云科技（AWS）账户只能向已验证地址和域发送电子邮件。如果您的账户属于这种情况，那么我们建议您验证网站的域名，并验证 WordPress管理员的电子邮件地址。要获取他们的电子邮件地址，请登录您 WordPress 网站的控制面板，然后在左侧导航菜单中选择 “用户”。您将看到列在 Email 列中的管理员电子邮件地址，如以下示例所示：



> **Note**
>
> 默认 `user` 配置文件配置了 `user@example.com` 电子邮件地址。您应将其更改为有效的电子邮件地址。有关更多信息，请参阅 WordPress 文档中的用户配置文件屏幕。

要向任何地址和域发送电子邮件，您必须请求让您的账户脱离 Amazon SES 沙盒。有关更多信息，请参阅 Amazon SES 文档中的脱离 Amazon SES 沙盒。

步骤 2：完成先决条件

在 WordPress实例上启用电子邮件之前，您必须完成以下任务：

- 在 Lightsail 中创建一个 WordPress 实例。有关更多信息，请参阅教程：在 Amazon Lightsai WordPress I 中启动和配置实例。
- 使用 Lightsail DNS 区域将您的注册域名指向您的 WordPress 实例。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。
- 注册 Amazon SES 并了解有关该服务的更多信息。有关注册 Amazon SES 的更多信息，请参阅 Amazon SES 文档中的 Amazon SES 快速入门。有关 Amazon SES 的更多信息，请参阅 Amazon SES 文档中的以下指南：
  - Amazon SES 开发人员指南
  - Amazon SES FAQs
  - Amazon SES 定价
  - Amazon SES 服务限额

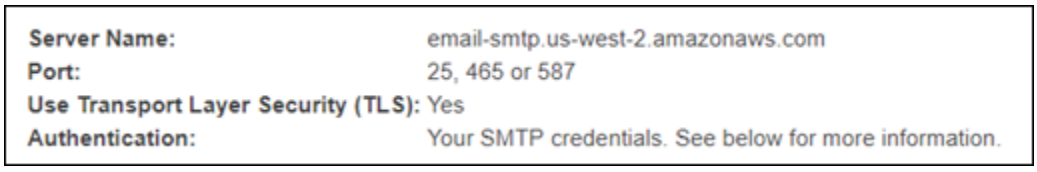
步骤 3：在 Amazon SES 中创建 SMTP 凭证

必须在您的 Amazon SES 账户中创建 SMTP 凭证，才能配置要在本指南后面配置的 WP Mail SMTP 插件。有关更多信息，请参阅 Amazon SES 文档中的获取 Amazon SES SMTP 凭证。

在 Amazon SES 中创建 SMTP 凭证

1. 登录 Amazon SES 控制台。
2. 在左侧导航菜单中，选择 SMTP settings (SMTP 设置)。

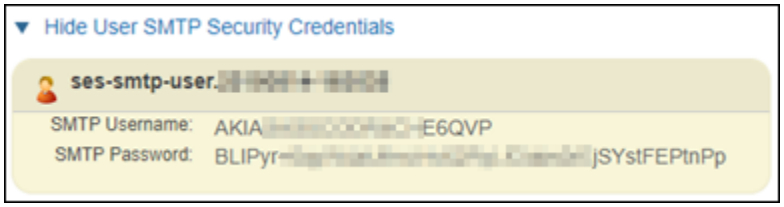
   SMTP settings (SMTP 设置) 页面会显示您的 SMTP 服务器名称、端口和 TLS 设置。请注意这些值，因为在本指南的稍后部分中，在 WordPress 实例上配置 WP Mail SMTP 插件时，您需要使用这些值。



3. 选择创建 SMTP 凭证。
4. 在 IAM 用户名文本框中，保留默认用户名，然后选择创建。



5. 选择 Show User SMTP Security Credentials (显示用户 SMTP 安全凭证) 以查看 SMTP 用户名和密码，或选择 Download Credentials (下载凭证) 以下载包含相同信息的 CSV 文件。稍后在您的 WordPress 实例上配置 WP Mail SMTP 插件时，您需要这些凭据。



> **Note**
>
> 在 Amazon SES 控制台中创建的凭证会自动添加到您账户的 AWS Identity and Access Management （IAM）。

步骤 4：在 Amazon SES 中验证域

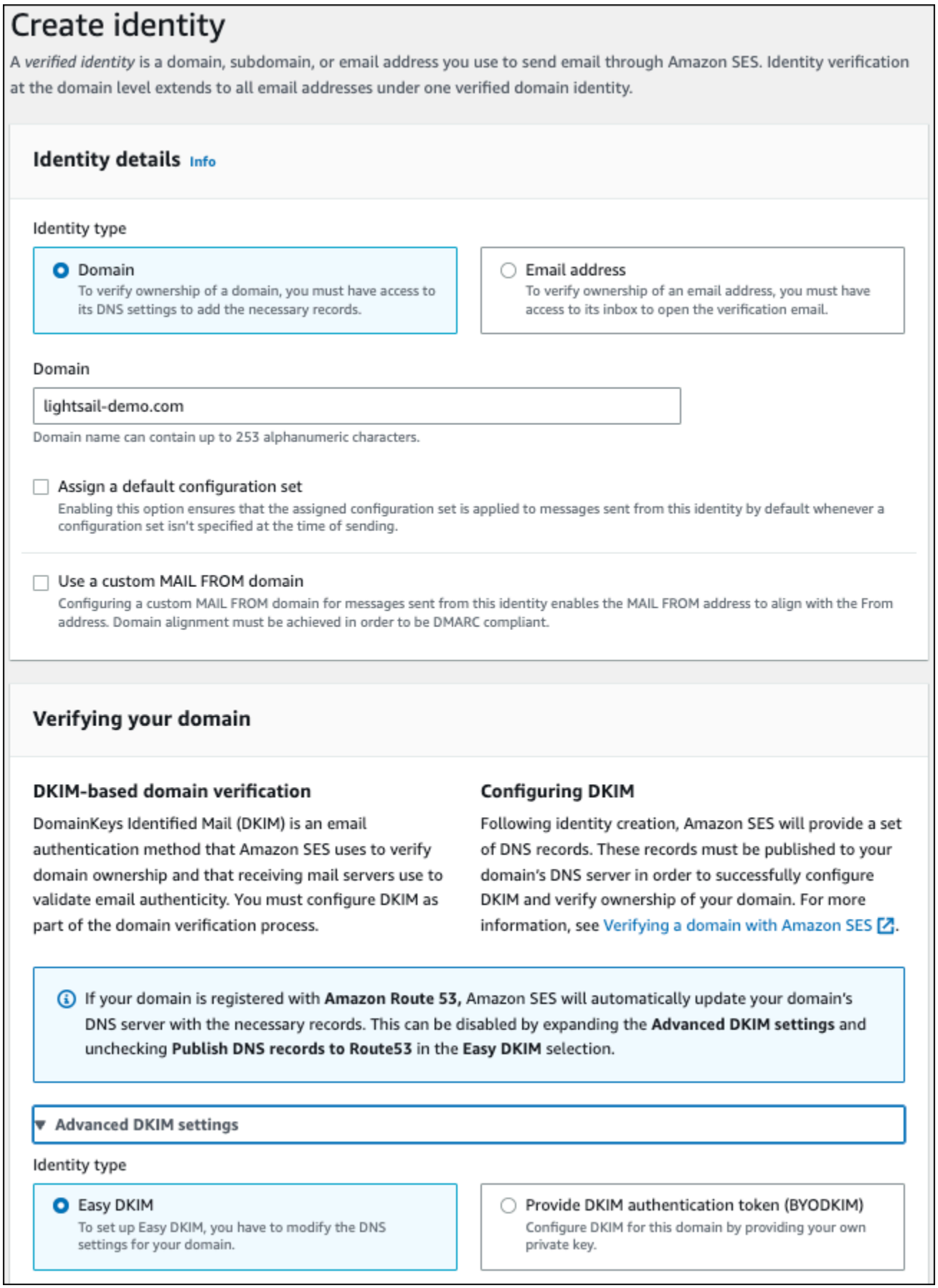
Amazon SES 要求您验证域，以确认您拥有该域并防止他人盗用。在验证域时，您将验证该域中的所有电子邮件地址，这样一来，您便无需逐个验证该域中的电子邮件地址。例如，如果您验证域 `example.com`，则可以从 `user1@example.com`、`user2@example.com` 或 `example.com` 中的任何其他用户发送电子邮件。有关更多信息，请参阅 Amazon SES 文档中的在 Amazon SES 中验证域。

在 Amazon SES 中验证域

1. 在 Amazon SES 控制台中，从左侧导航菜单中选择已验证的身份。
2. 选择创建身份。
3. 输入要验证的域，然后选择创建身份。

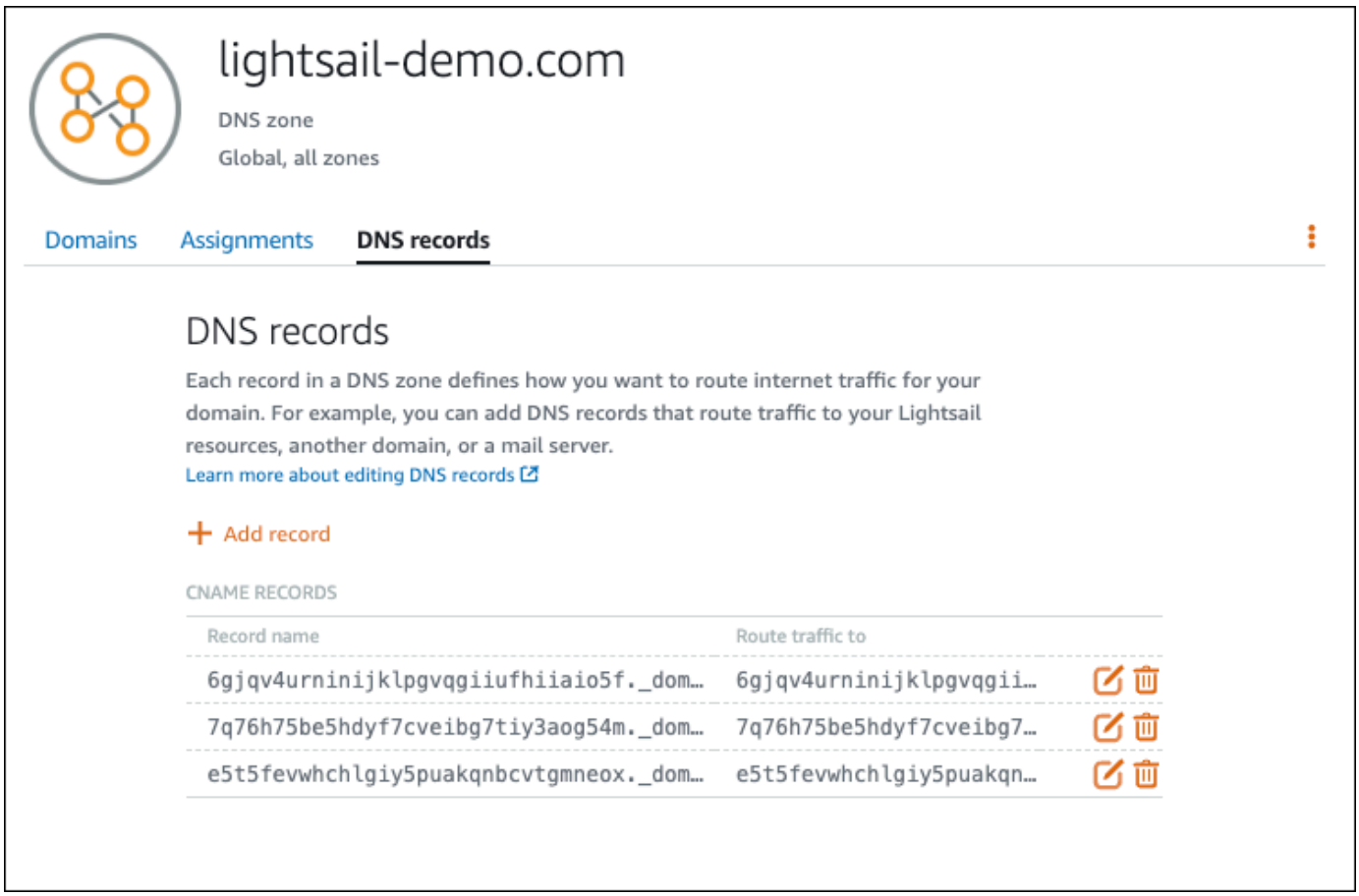
   您验证的域名应与您在 Lightsail 中的 WordPress 实例中使用的域名相同。

> **Important**
>
> 传统 TXT 记录
> Amazon SES 中的域名验证现在基于 DomainKeys 识别邮件 (DKIM)，这是一种电子邮件身份验证标准，接收邮件的服务器使用它来验证电子邮件的真实性。在域的 DNS 设置中配置 DKIM 可向 SES 确认您是身份所有者，从而无需输入 TXT 记录。使用 TXT 记录验证的域身份无需重新验证；但是，我们仍然建议启用 DKIM 签名，以提高您邮件在符合 DKIM 标准的电子邮件提供商处的送达率。


Create identity
A verified identity is a domain, subdomain, or email address you use to send email through Amazon SES. Identity verification at the domain level extends to all email addresses under one verified domain identity.
Identity details Info
Identity type
Domain
To verify ownership of a domain, you must have access to its DNS settings to add the necessary records.
Email address
To verify ownership of an email address, you must have access to its inbox to open the verification email.
Domain
lightsail-demo.com
Domain name can contain up to 253 alphanumeric characters.
Assign a default configuration set
Enabling this option ensures that the assigned configuration set is applied to messages sent from this identity by default whenever a configuration set isn't specified at the time of sending.
Use a custom MAIL FROM domain
Configuring a custom MAIL FROM domain for messages sent from this identity enables the MAIL FROM address to align with the From address. Domain alignment must be achieved in order to be DMARC compliant.
Verifying your domain
DKIM-based domain verification
DomainKeys Identified Mail (DKIM) is an email authentication method that Amazon SES uses to verify domain ownership and that receiving mail servers use to validate email authenticity. You must configure DKIM as part of the domain verification process.
Configuring DKIM
Following identity creation, Amazon SES will provide a set of DNS records. These records must be published to your domain's DNS server in order to successfully configure DKIM and verify ownership of your domain. For more information, see Verifying a domain with Amazon SES.
If your domain is registered with Amazon Route 53, Amazon SES will automatically update your domain's DNS server with the necessary records. This can be disabled by expanding the Advanced DKIM settings and unchecking Publish DNS records to Route53 in the Easy DKIM selection.
Advanced DKIM settings
Identity type
Easy DKIM
To set up Easy DKIM, you have to modify the DNS settings for your domain.
Provide DKIM authentication token (BYODKIM)
Configure DKIM for this domain by providing your own private key.

4. 在使用 Easy DKIM 创建域身份以后，您必须通过复制以下生成的 CNAME 记录并将其发布到域的 DNS 提供商来完成 DKIM 身份验证过程。这些记录的检测最长可能需要 72 小时。有关更多信息，请参阅使用 DKIM 验证域身份和 Easy DKIM
5. 打开一个新的浏览器选项卡，然后导航到 Lightsail 控制台。
6. 在左侧导航窗格 中，选择域和 DNS，然后选择您域的 DNS 区域。
7. 从 Amazon SES 控制台添加 DNS 记录。有关在 Lightsail 中编辑 DNS 区域的更多信息，请参阅亚马逊 Lightsai l 中的编辑 DNS 区域。

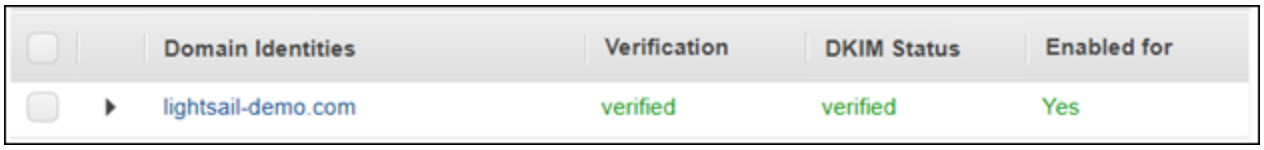
   结果应该类似以下示例。



> **Note**
>
> 在子域文本框中输入 @ 符号以将顶级域用于 MX 记录。此外，Amazon SES 提供的 MX 记录值为 `10 inbound-smtp.us-west-2.amazonaws.com`。输入 `10` 作为 Priority (优先级)，并输入 `inbound-smtp.us-west-2.amazonaws.com` 作为 Maps to (映射到)域。

8. 在 Amazon SES 控制台中，关闭验证新域页面。

   在数分钟后，Amazon SES 控制台中列出的域将标记为已验证并支持发送，如以下示例所示：



   Amazon SES 中的 SMTP 服务现在可从您的域发送电子邮件。

步骤 5：在 Amazon SES 中验证电子邮件地址

作为 Amazon SES 新客户，您必须验证要向其发送电子邮件的电子邮件地址。在 Amazon SES 控制台中添加电子邮件地址即可执行此操作。有关更多信息，请参阅 Amazon SES 文档中的在 Amazon SES 中验证电子邮件地址。

我们建议您添加 WordPress 网站管理员的电子邮件地址。这让他们可以为其用户配置文件请求密码重置，并会收到有关博客帖子、网站更新和其他插件消息的电子邮件通知。

> **Note**
>
> 如果您要将电子邮件发送至任何地址而无需验证，则必须请求让 Amazon SES 账户脱离沙盒。有关更多信息，请参阅 Amazon SES 文档中的脱离 Amazon SES 沙盒。

创建电子邮件地址身份

1. 在 Amazon SES 控制台中，从左侧导航菜单中选择已验证的身份。
2. 选择创建身份。
3. 选择电子邮件地址。再输入您要验证的电子邮件地址。
4. 选择创建身份。

为要验证的每个电子邮件地址重复执行步骤 1 至 4。验证电子邮件将发送到您输入的电子邮件地址。该地址将添加到已验证电子邮件身份列表中，其状态为“pending verification (等待验证)”。当用户打开电子邮件并完成验证过程后，它将标记为“verified (已验证)”。

验证电子邮件地址身份

1. 查看用于创建身份的电子邮件地址的收件箱并查找来自 no-reply-aws@amazon .com 的电子邮件。
2. 打开电子邮件并单击链接即可完成电子邮件地址的验证过程。完成后，身份状态将更新为已验证。

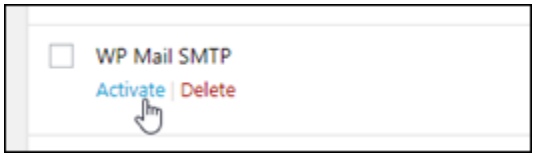


第 6 步：在您的 WordPress 实例上配置 WP 邮件 SMTP 插件

最后一步是在您的 WordPress 实例上配置 WP Mail SMTP 插件。使用您在本指南的前面在 Amazon SES 控制台中创建的 SMTP 凭证。

在您的 WordPress 实例上配置 WP 邮件 SMTP 插件

1. 以管理员身份登录您 WordPress 网站的控制面板。
2. 在左侧导航菜单中，选择 Plugins，然后选择 Installed Plugins。
3. 向下滚动到 WP Mail SMTP 插件，然后选择 Activate。如果有新版本的插件，请确保先对其进行更新，然后再继续下一步。

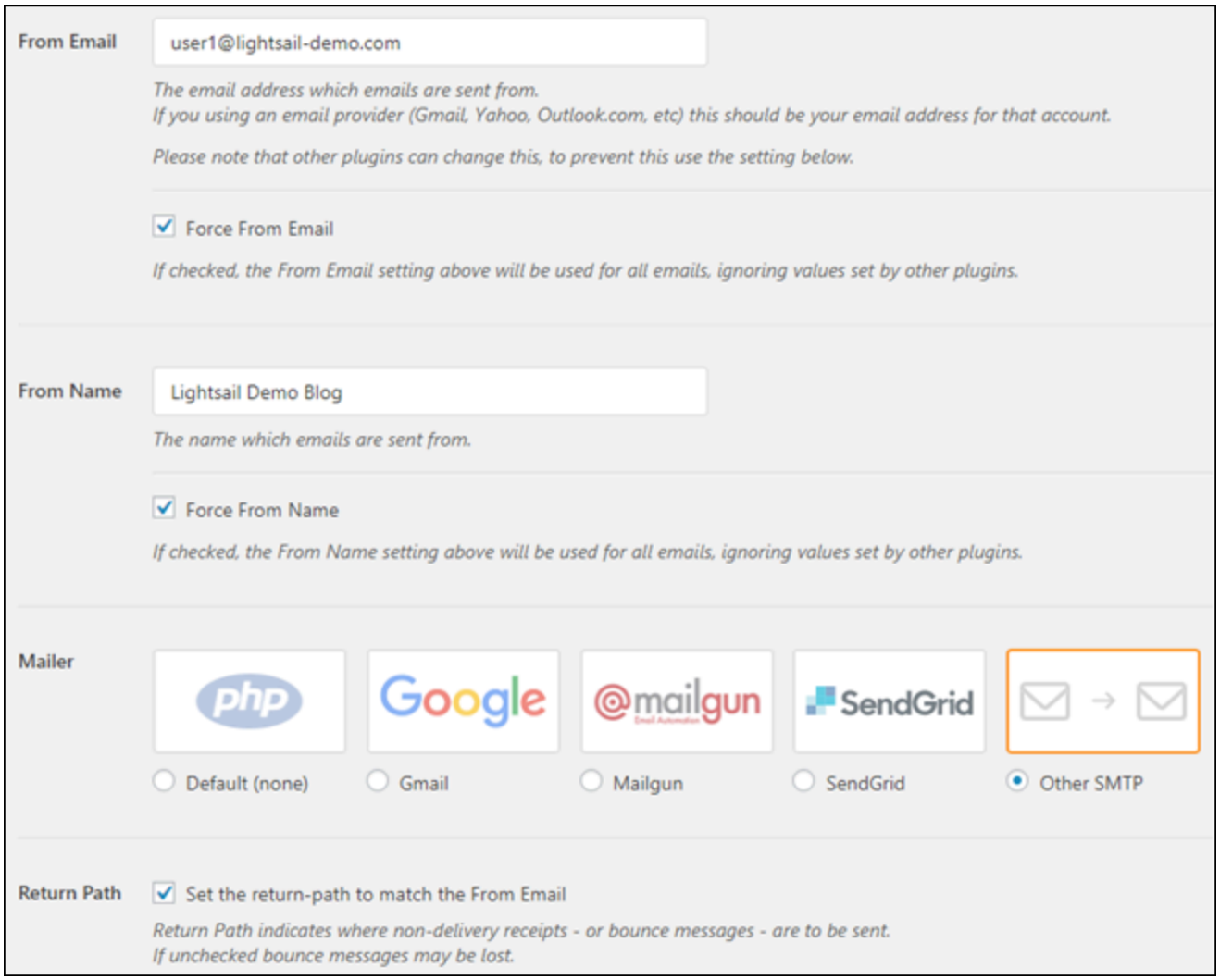


4. 激活 WP Mail SMTP 插件后，选择 Settings。您可能需要向下滚动才能找到该插件。

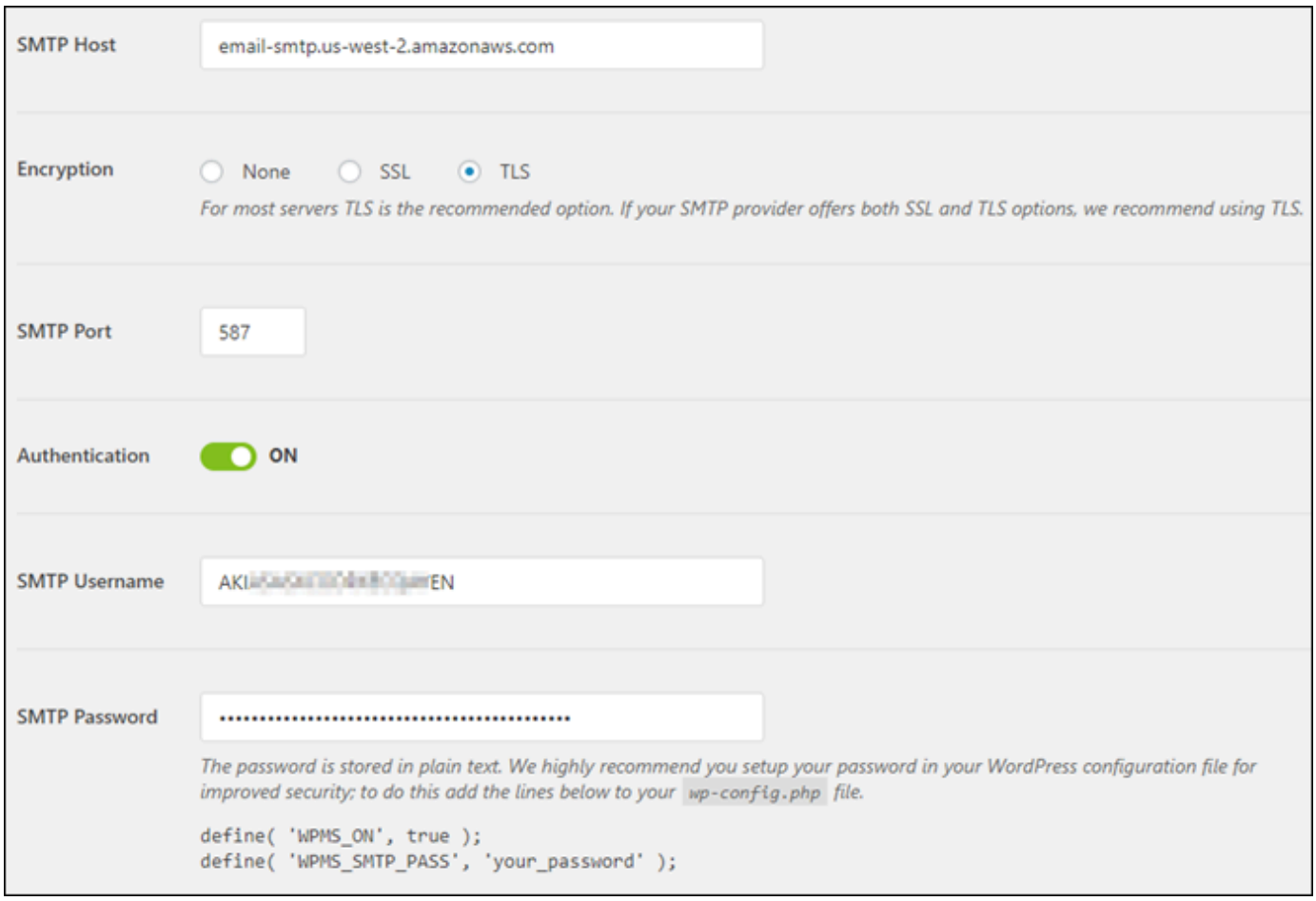


5. 在 From Email Address 文本框中，输入您希望电子邮件来自的电子邮件地址。您输入的电子邮件地址必须已使用本指南前面的步骤在 Amazon SES 中进行了确认。
6. 选择 Force From Email 以强制使用您在 From Email Address 文本框中输入的电子邮件地址，并忽略其他插件设置的“from email address”值。

7. 在“发件人姓名”文本框中，输入您想要发送电子邮件的名称，或者保留原样使用 WordPress 博客的名称。
8. 选择 Force From Name 以强制使用您在 From Name 文本框中输入的名称。选择此选项会忽略其他插件设置的“from name”值，并强制 WordPress 使用您在“From Name”文本框中输入的名称。
9. 在该页面的邮件程序部分中，选择 Other SMTP。
10. 选择 Set the return-path to match the From Email 以让未送达收据发送到您在 From Email Address 文本框中输入的电子邮件地址。



11. 在 SMTP 主机文本框中，输入您之前在本指南中从 Amazon SES 控制台的 SMTP 设置页面中获取的 SMTP 服务器名称。
12. 在页面的加密部分中选择 TLS，以指定 Amazon SES 中的 SMTP 服务使用 TLS 加密。
13. 在 SMTP Port 文本框中，保留默认值 587。
14. 将身份验证开关切换为打开，然后输入您在本指南的前面从 Amazon SES 控制台获得的 SMTP 用户名和密码。

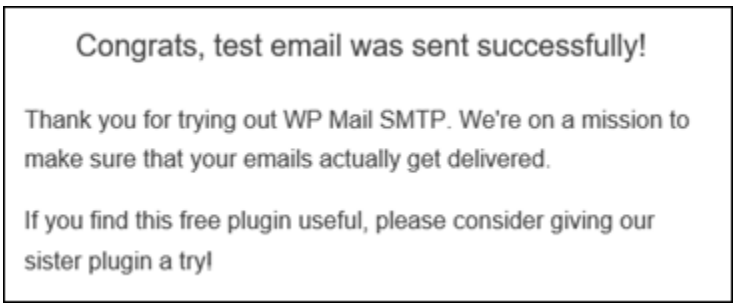


15. 选择 Save Settings。这时会出现提示，确认设置已成功保存。
16. 选择 Email Test 选项卡。

    在下一个步骤中，您将发送测试电子邮件以确认电子邮件服务正常运行。
17. 在 Send To 文本框中输入电子邮件地址，然后选择 Send Email。您输入的电子邮件地址必须已使用本指南前面的步骤在 Amazon SES 中进行了确认。

    您应该看到两种可能的结果。

    - 如果您看到成功确认消息，则说明您的 WordPress 网站已启用电子邮件功能。确认以下测试电子邮件到达指定的邮箱：



您现在可以选择 “忘记密码？” 在您 WordPress 网站控制面板的登录页面上。如果在 Amazon SES 中确认了您的 WordPress 用户个人资料中的电子邮件地址，则会通过电子邮件向您发送一个新密码。

- 如果看到失败通知，请确认您输入到 WP Mail SMTP 插件中的 SMTP 设置，与您 Amazon SES 账户中的 SMTP 服务的设置匹配。此外，确认您使用的是已在 Amazon SES 中验证的电子邮件地址。

在 Lightsail 上使用 HTTPS 保护你的 WordPress 网站

为您的 WordPress 网站启用安全超文本传输协议 (HTTPS) 可确保访问者相信您的网站是安全的；它正在发送和接收加密数据。非安全网站的地址以 `http` 开头（如 `http://example.com`），而安全网站的地址以 `https` 开头（如 `https://example.com`）。即使您的网站主要是提供参考信心，仍建议您启用 HTTPS。这是因为如未启用 HTTPS，大多数 Web 浏览器会通知网站访问者您的网站是不安全的，并且您的网站将在搜索引擎结果中排名较低。

> **Tip**
>
> Lightsail 提供指导式工作流程，可在您的实例上自动安装和配置 SSL/TLS 让我们加密证书。WordPress 我们强烈建议使用该工作流程，而不是按照本教程中的手动步骤操作。有关更多信息，请参阅启动和配置实 WordPress 例。

本指南向您展示如何使用 Bitnami HTTPS 配置工具 (`bncert`) 在 WordPress Amazon Lightsail 上的 Bitnami 认证实例上启用 HTTPS。它允许您仅为进行请求时指定的域和子域请求证书。或者，也可以使用 Certbot 工具，为域请求证书和为子域请求通配符证书。通配符证书适用于任何子域，如果您不知道将使用哪个子域将流量引导到您的实例，这样做可以带来好处。但是，Certbot 不会像 `bncert` 工具那样自动续订证书。如果您使用 Certbot，则必须每 90 天手动续订一次证书。有关使用 Certbot 启用 HTTPS 的更多信息，请参阅教程：在您的 WordPress 实例中使用让我们加密 SSL 证书。

内容

- 步骤 1：了解流程
- 步骤 2：完成先决条件
- 步骤 3：连接到您的实例
- 步骤 4：确认已在实例上安装了 bncert 工具
- 步骤 5：在您的 WordPress 实例上启用 HTTPS
- 步骤 6：测试您的网站是否使用 HTTPS

步骤 1：了解流程

> **Note**
>
> 在本部分中，您可了解此过程的简要概述。执行此过程的具体步骤包含在本指南的后续步骤中。

要为您的 WordPress 网站启用 HTTPS，请使用 SSH 连接到您的 Lightsail 实例，然后使用该bncert工具向 Let's Encryp t 证书颁发机构申请 SSL/TLS 证书。当您请求证书时，您可以指定网站的主域（example.com) 和备用域（www.example.com、blog.example.com 等），如果有的话。Let's Encrypt 通过要求您在域的 DNS 中创建 TXT 记录，或验证这些域是否已将流量引导到您发出请求的实例的公有 IP 地址，来验证您是否拥有这些域。

证书通过验证后，您可以将 WordPress 网站配置为自动将访客从 HTTP 重定向到 HTTPS（http://example.com重定向到https://example.com），这样访客就被迫使用加密连接。您还可以将您的网站配置为从 www 子域名自动重新导向到顶级域（https://www.example.com 重新导向到 https://example.com），反之亦然（https://example.com 重新导向到 https://www.example.com）。也可以使用 bncert 工具执行这些重新导向操作。

Let's Encrypt 要求您每隔 90 天续订一次证书，以便在您的网站上维持 HTTPS。bncert工具会自动为您续订证书，这样您就可以花更多时间关注您的网站。

管理工具的限制

bncert 工具有以下限制：

- 并非所有 Certified by Bitnami WordPress 实例在创建时都已预先安装在这些实例上。 WordPress 不久前在 Lightsail 上创建的实例需要您手动安装该工具。bncert本指南的步骤 4 向您介绍如何确认该工具已安装在您的实例上，以及在没有安装的情况下如何安装。

- 您可以仅为进行请求时指定的域和子域请求证书。这与 Certbot 工具不同，它可以为域请求证书和为子域请求通配符证书。通配符证书适用于任何子域，如果您不知道将使用哪个子域将流量引导到您的实例，这样做可以带来好处。但是，Certbot 不会像 `bncert` 工具那样自动续订证书。如果您使用 Certbot，则必须每 90 天手动续订一次证书。有关使用 Certbot 启用 HTTPS 的更多信息，请参阅教程：在 Amazon Lightsail 中的 WordPress 实例中使用让我们对 SSL 证书进行加密。

步骤 2：完成先决条件

请完成以下先决条件（如果尚未完成）：

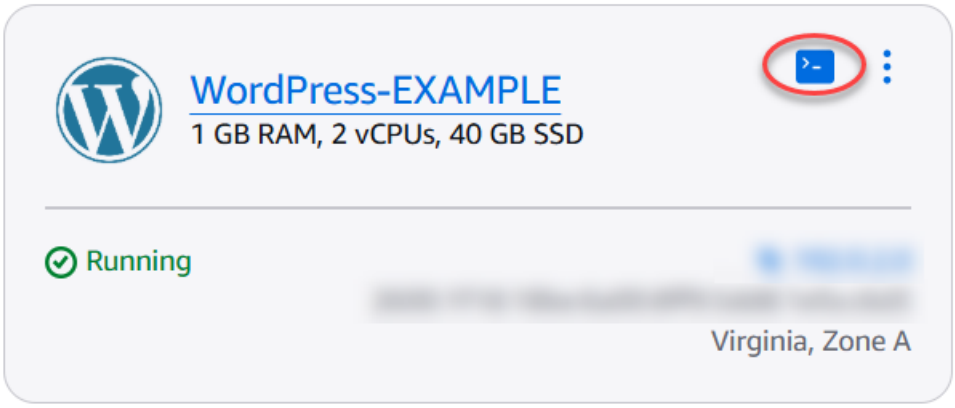
- 在 Lightsail 中创建实例，并在您的 WordPress 实例上配置您的网站。有关更多信息，请参阅 Amazon Light sail 中基于 Linux/UNIX 的实例入门。
- 将静态 IP 附加到实例。如果您停止和启动实例，则实例的公有 IP 地址会出现更改。如果您停止和启动实例，静态 IP 不会更改。有关更多信息，请参阅创建静态 IP 并将其附加到 Amazon Lightsail 中的实例。
- 配置完 WordPress 实例后，为其创建快照，或者启用自动快照。快照可用作备份，如果原始实例出现问题，您便可以从中创建另一个实例。有关更多信息，请参阅创建 Linux 或 Unix 实例的快照或在 Amazon Lightsail 中为实例或磁盘启用或禁用自动快照。
- 将 DNS 记录添加到您的域名的 DNS 中，从而将您的域名顶点 () 及其`www`子域名 (`example.com`) 的流量引导到您在 Lightsail 中 WordPress 实例的公有 IP 地址。`www.example.com`您可以在域的当前 DNS 托管提供商处完成这些操作。或者，如果您将域名 DNS 的管理权转移到 Lightsail，则可以使用 Lightsail 中的 DNS 区域来完成这些操作。要了解更多信息，请参阅 DNS。

> **Important**
>
> 将 DNS 记录添加到您要用于 WordPress网站的所有域名的 DNS 中。所有这些域名都应将流量路由到您 WordPress 网站的公共 IP 地址。该`bncert`工具将仅为当前将流量定向到您的 WordPress实例的公有 IP 地址的域名颁发证书。

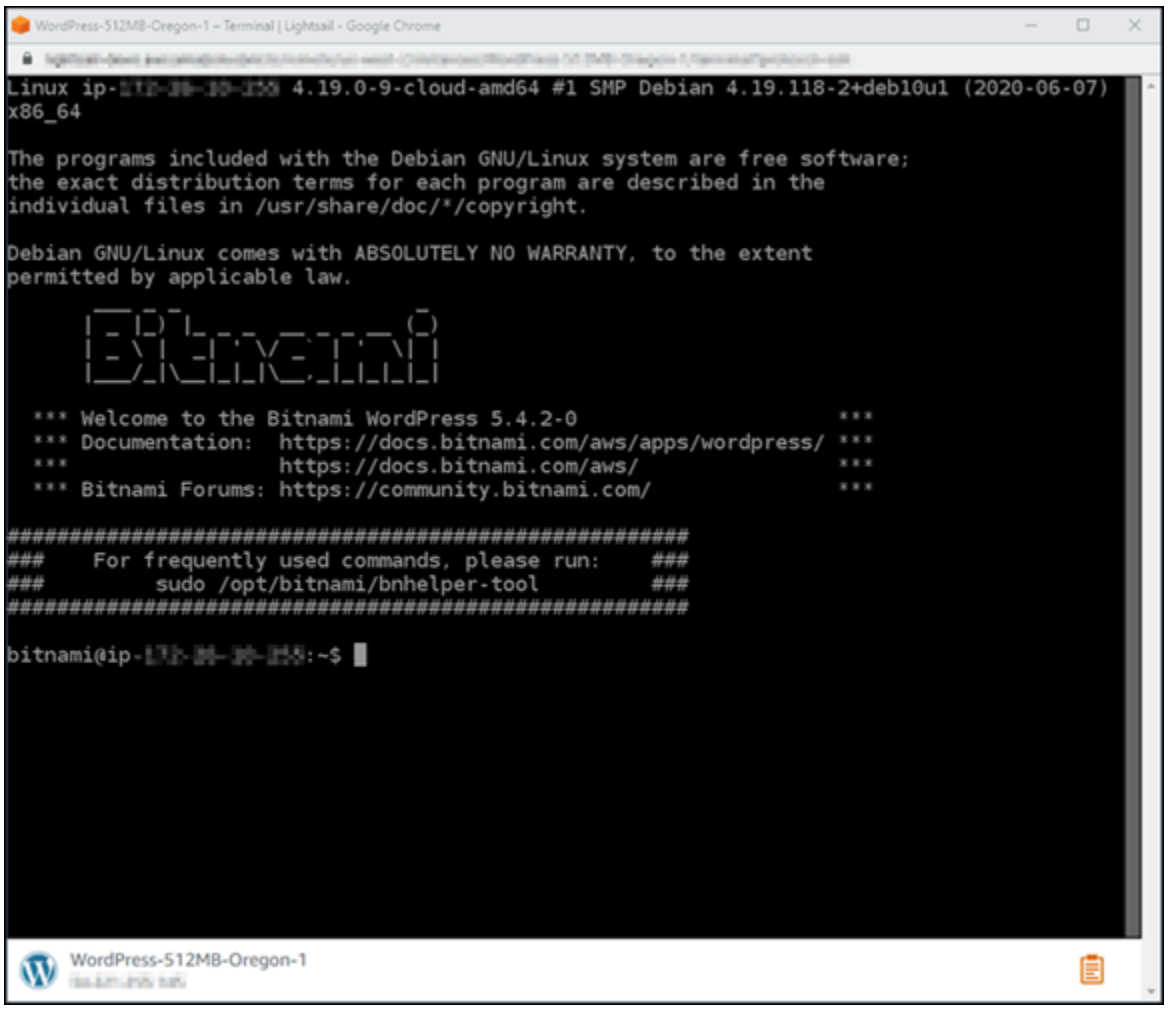
步骤 3：连接到您的实例

完成以下步骤，在 Lightsail 控制台中使用基于浏览器的 SSH 客户端连接到您的实例。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，为您的 WordPress实例选择 SSH 快速连接图标。



将打开基于浏览器的 SSH 客户端终端窗口。如果您看到 Bitnami 徽标（如以下示例所示），则您通过 SSH 成功连接到您的实例。



步骤 4：确认已在实例上安装了 bncert 工具

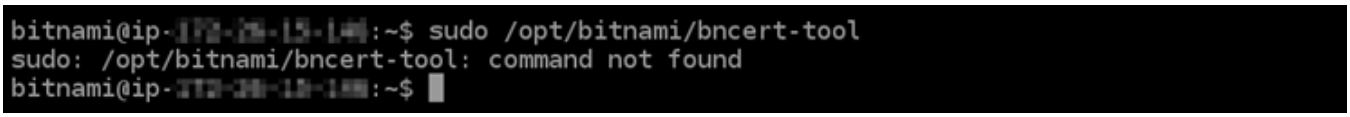
完成以下步骤以确保 Bitnami HTTPS 配置工具 (bncert) 已安装到实例上。并非所有 Certified by Bitnami WordPress 实例在创建时都已预先安装在这些实例上。 WordPress 不久前在 Lightsail 上创建的实例需要您手动安装该工具。bncert此过程包括在未安装工具时安装该工具的步骤。

1. 要运行 bncert 工具，请输入以下命令。

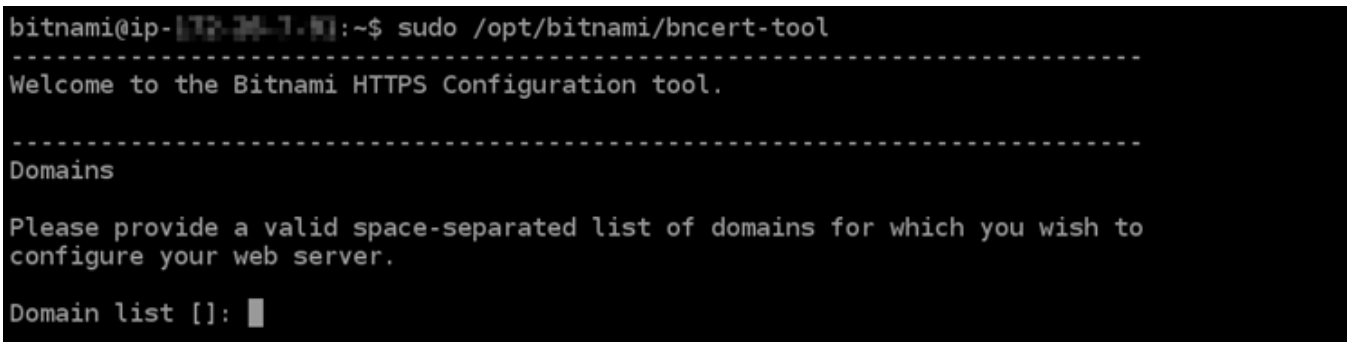
```
sudo /opt/bitnami/bncert-tool
```

- 如果您在响应中看到 command not found（如以下示例所示），则 bncert 工具未安装到实例上。继续执行此过程的后续步骤以在实例上安装 bncert 工具。

> **Important**
>
> 该bncert工具只能用于通过 Bitnami 认证的 WordPress 实例。或者，您可以使用 Certbot 工具在您的实例上启用 HTTPS。 WordPress 有关更多信息，请参阅教程：对您的 WordPress实例使用 “让我们加密 SSL 证书”。



- 如果您在响应中看到 Welcome to the Bitnami HTTPS configuration tool（如以下示例所示），则 bncert 工具已安装到实例上。继续本指南的步骤 5：在您的 WordPress 实例上启用 HTTPS 部分。



2. 输入以下命令以将 bncert 运行文件下载到您的实例中。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

3. 输入以下命令以在您的实例上创建 bncert 运行文件的目录。

```
sudo mkdir /opt/bitnami/bncert
```

4. 输入以下命令以将下载的 bncert 运行文件移动到您创建的新目录。

```
sudo mv bncert-linux-x64.run /opt/bitnami/bncert/
```

5. 输入以下命令以创建可作为程序执行的 bncert 运行文件。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 输入以下命令以创建当您输入 sudo /opt/bitnami/bncert-tool 命令时运行 bncert 工具的符号链接。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

您现在已完成在实例上安装 bncert 工具的步骤。继续本指南的步骤 5：在您的 WordPress 实例上启用 HTTPS 部分。

步骤 5：在您的 WordPress实例上启用 HTTPS

确认您的 WordPress 实例上安装了 HTTPS 后，请完成以下步骤以在bncert您的实例上启用 HTTPS。

1. 要运行 bncert 工具，请输入以下命令。

```
sudo /opt/bitnami/bncert-tool
```

您应看到类似于以下示例的消息。

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/bncert-tool
--------------------------------------------------------------------------------
Welcome to the Bitnami HTTPS Configuration tool.

--------------------------------------------------------------------------------
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []:
```

如果 bncert 工具已在您的实例上安装了一段时间，那么您可能会看到一条消息，指示该工具的更新版本可供使用。按以下示例中所示选择下载它，然后再次输入 sudo /opt/bitnami/bncert-tool 命令来运行 bncert 工具。

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/bncert-tool
An updated version is available. Would you like to download it? You would need to run it
manually later. [Y/n]: Y
```

2. 输入用空格分隔的主域名和备用域名，如以下示例所示。

   如果您的域未配置为将流量路由到实例的公有 IP 地址，则 bncert 工具将要求您在继续之前进行该配置。您的域必须将流量路由到使用 bncert 工具以在实例上启用 HTTPS 的实例的公有 IP 地址。这将确认您拥有该域，并能用于进行证书的验证。

```
--------------------------------------------------------------------------------
Welcome to the Bitnami HTTPS Configuration tool.

--------------------------------------------------------------------------------
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []: example.com www.example.com
```

3. bncert 工具会询问您希望如何配置网站的重新导向。以下是可用的选项：

   - 启用 HTTP 重新导向到 HTTPS - 指定是否将浏览网站 HTTP 版本（即 http:/example.com）的用户自动重新导向到 HTTPS 版本（即 https://example.com)。我们建议启用此选项，因为它会强制所有访问者使用加密连接。输入 Y 然后按 Enter 以启用它。
   - 启用非 www 重新导向到 www - 指定是否将浏览顶级域（即 https://example.com）的用户自动重新导向到域的 www 子域（即 https://www.example.com)。我们建议启用此选项。但如果您在搜索引擎工具（如 Google 站点管理员工具）中指定了顶级域作为首选网站地址，或者顶级域直接指向您的 IP 且 www 子域通过别名记录引用您的顶级域，则您可能希望禁用它并启用其他选项（启用 www 重新导向到非 www）。输入 Y 然后按 Enter 以启用它。

- 启用 www 到非 www 重新导向 - 指定是否将浏览域的 www 子域（即 `https://www.example.com`）的用户自动重新导向到顶级域（即 `https://example.com`)。如果您启用了非 www 重新导向到 www，建议禁用此选项。输入 N 然后按 Enter 以禁用它。

您的选择应类似于以下示例：

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.


Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

4. 将列出要进行的更改。输入 Y 然后按 Enter 以确认并继续。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

5. 输入要与 Let's Encrypt 证书关联的电子邮件地址，然后按 Enter（确定键）。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

6. 查看 Let's Encrypt 的加密用户协议 输入 Y 然后按 Enter 接受协议并继续。

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

将执行这些操作以在您的实例上启用 HTTPS，包括请求证书和配置您指定的重新导向。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|
```

您的证书已成功颁发和验证，如果您看到类似于以下示例的消息，则表示在实例上成功配置了重新导向。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

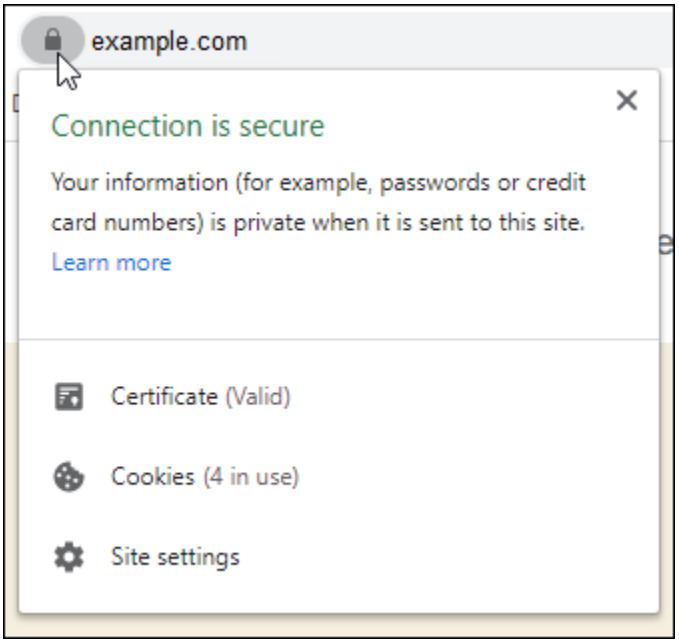
bncert 工具将在证书过期前每 80 天执行一次自动续订。如果您希望将其他域和子域用于实例，并且希望为这些域启用 HTTPS，请重复上述步骤。

现在，您已完成在您的 WordPress 实例上启用 HTTPS。继续执行本指南的步骤 6：测试您的网站是否使用 HTTPS 部分。

步骤 6：测试您的网站是否使用 HTTPS

在您的 WordPress 实例上启用 HTTPS 后，您应通过浏览您在使用该bncert工具时指定的所有域来确认您的网站正在使用 HTTPS。当您访问每个域时，您应该看到它们在使用安全连接，如以下示例所示。

> **Note**
>
> 您可能需要刷新并清除浏览器的缓存才能看到更改。



您可能还会发现非 www 地址重新导向到域的 www 子域，反之亦然，具体取决于您在运行 bncert 工具时选择的选项。

将你的 WordPress 博客迁移到 Lightsail

想要更换您的 WordPress 托管服务提供商？ Amazon Lightsail 是运行 WordPress 网站的最简单方法。 AWS

您可以选择我们的定价计划之一（起价为每月 5 美元），并完全控制您的 WordPress 安装，包括插件、主题等。

创建 Lightsail WordPress 实例只需要几分钟。按照本教程备份现有 WordPress 博客并将其导入在 Lightsail 中运行的新实例。

以下是此过程的简要概述：



继续阅读以开始使用。

先决条件

在开始之前，您需要：

1. 你需要一个 AWS 账户。注册 AWS或登录（ AWS如果您已经有一个帐户）。
2. 确保您的账户已设置为使用 Lightsail。如果自创建账户以来已经有一段时间了，或者您尚未提供信用卡，则可能需要先登录 AWS Management Console 并更新您的账户。

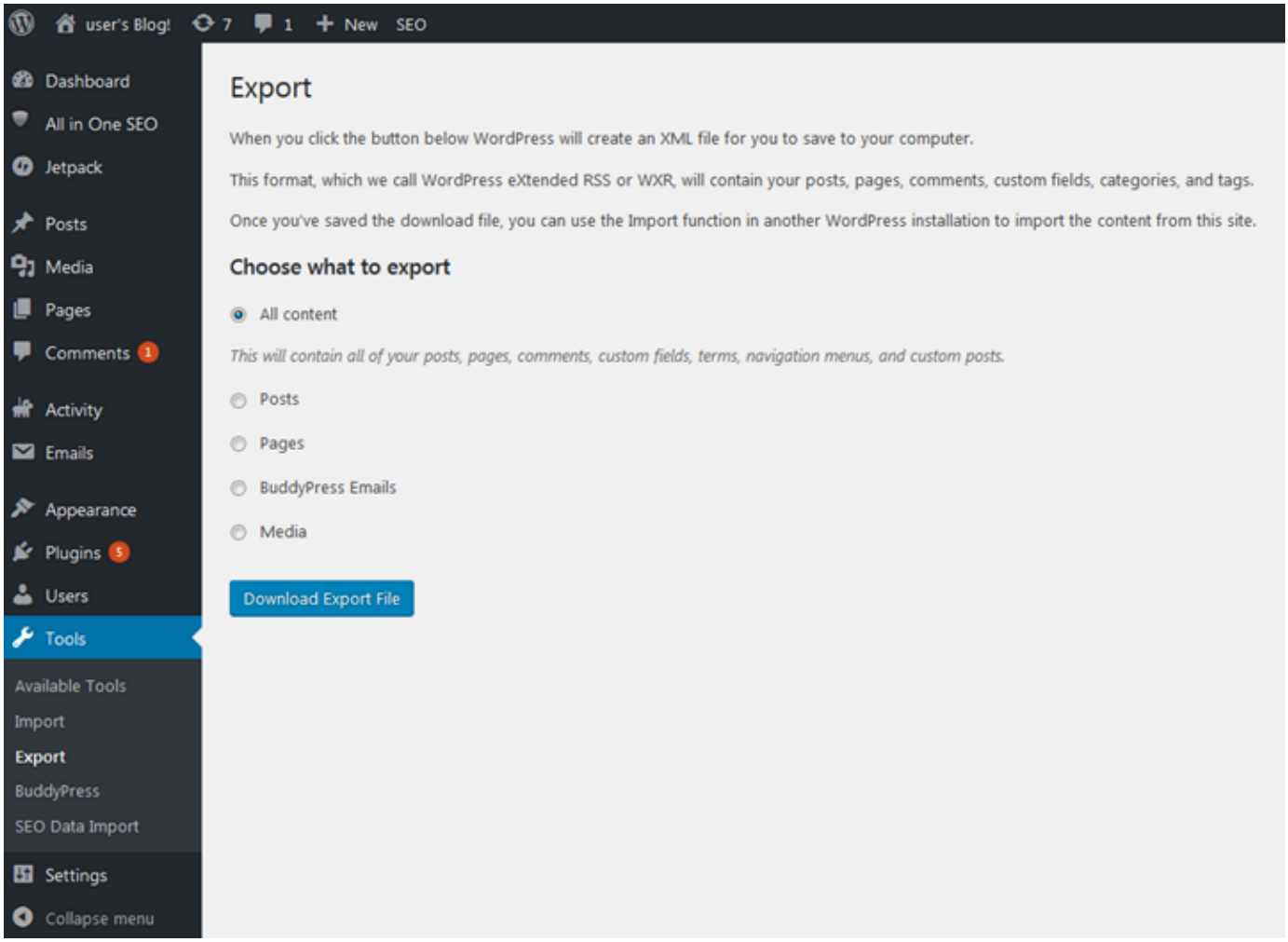
第 1 步：备份现有 WordPress 博客

您可以使用备份 WordPress 现有博客。您只需要能够登录 WordPress 管理员控制台并管理您的博客即可。

1. 导航到您的博客，然后选择 Manage（管理）。

如果 Manage（管理）横幅未显示，您可以通过浏览 `http://<PublicIP>/wp-login.php` 到达登录页面。将 *<PublicIP>* 替换为实例的公有 IP 地址。

2. 输入您的用户名和密码以登录 WordPress 管理员控制台。
3. 在 “ WordPress 控制面板” 上，选择 “工具”，然后选择 “导出”。
4. 在 Export（导出）页面上，选择 All content（所有内容）以将所有内容导出为 XML 文件。



5. 选择 Download export file（下载导出文件）以将旧博客下载为 XML 文件。

   将此 XML 文件保存便于查找的位置。您在步骤 4 中将需要此文件。

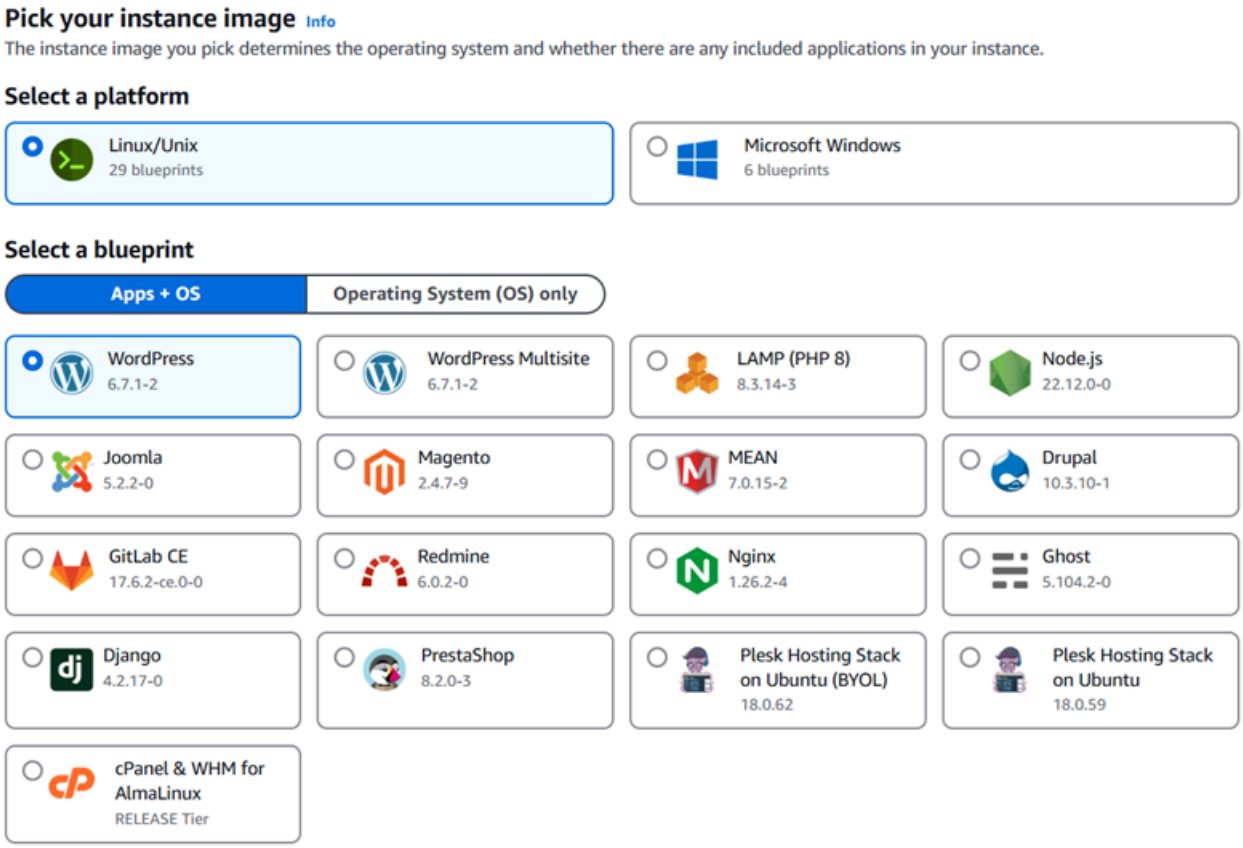
第 2 步：在 Lightsail 中创建一个新 WordPress 实例

你可以在短短几分钟内在 Lightsail 中创建一个新 WordPress 实例。方法如下：

1. 前往 Lightsail 主页并登录。

2. 选择创建实例。
3. 选择您要在 AWS 区域 哪里创建博客。

   您可以选择默认可用区，也可以在选择 AWS 区域区域后进行更改。
4. 选择 WordPress。



5. 选择实例计划（或包）。

   如果需要，您可以稍后升级您的 Lightsail 套餐。有关更多信息，请参阅在 Lightsail 中使用快照创建实例。
6. 输入实例的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2–255 个字符。
   - 必须以字母数字字符作为开头和结尾。
   - 可以包括字母数字字符、句点、连字符和下划线。

7. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

   a. 对于密钥，输入标签密钥。



   b. （可选）在“值”中，输入标签值。



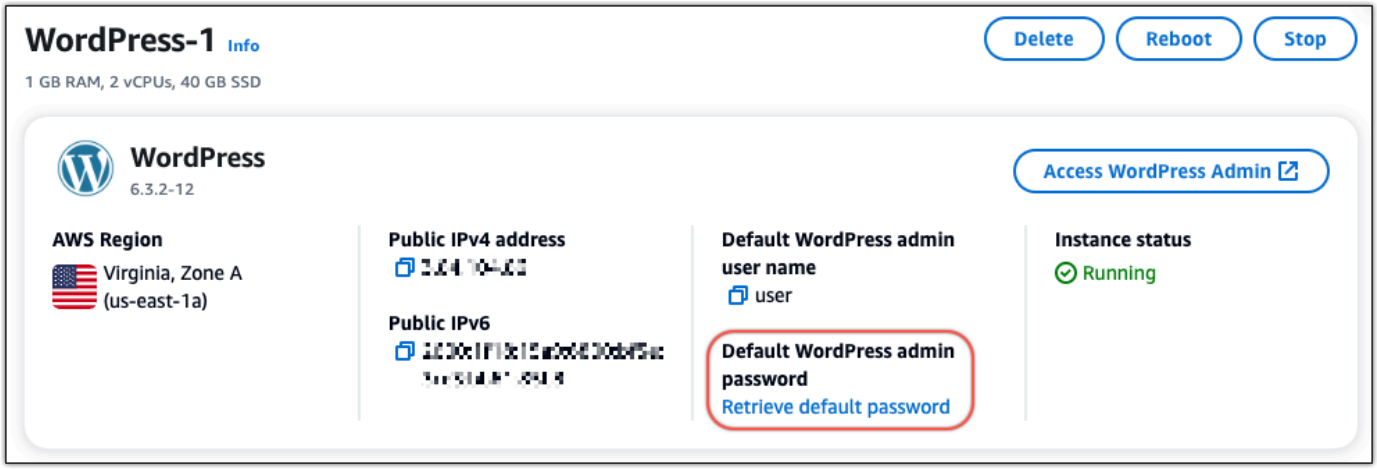
8. 选择创建实例。

第 3 步：登录你的新 Lights WordPress ail 博客

既然你在 Lightsail 中有一个新博客，你需要访问 WordPress 控制面板才能导入旧的博客数据。登录 WordPress 网站管理仪表板的默认密码存储在实例上。完成以下步骤以获取密码。

获取 WordPress 管理员的默认密码

1. 打开您的实例的 WordPress 实例管理页面。
2. 在WordPress面板上，选择“找回默认密码”。这将在页面底部展开访问默认密码。



3. 选择启动 CloudShell。这将在页面底部打开面板。
4. 选择“复制”，然后将内容粘贴到 CloudShell 窗口中。您可以将光标放在 CloudShell 提示符处并按 Ctrl+V，也可以右键单击打开菜单，然后选择“粘贴”。

5. 记下 CloudShell 窗口中显示的密码。您需要使用它来登录 WordPress 网站的管理控制面板。

```
[cloudshell-user@ip-[redacted] ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_applic
ation_password
JKzh8wB5FAR!
```

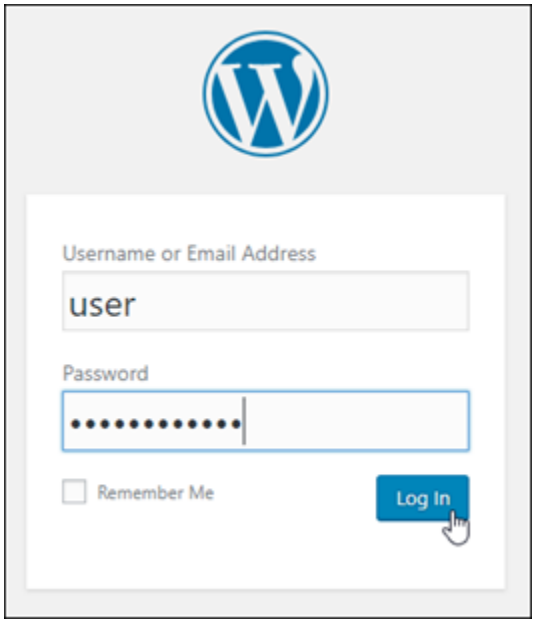
现在您已经有了 WordPress 网站管理仪表板的密码，就可以登录了。在管理控制面板中，您可以更改用户密码、安装插件、更改网站的主题等等。

完成以下步骤登录到您 WordPress网站的管理控制面板。

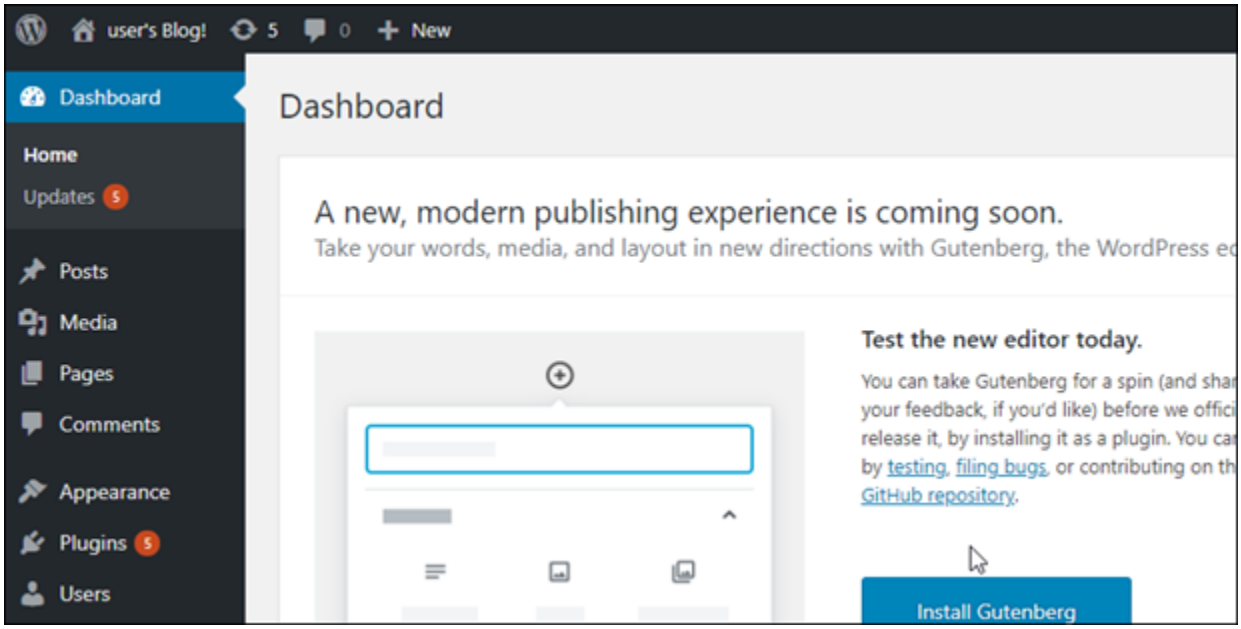
要登录管理控制面板

1. 打开您的实例的 WordPress 实例管理页面。
2. 在WordPress面板上，选择访问 WordPress 管理员。
3. 在 “访问您的 WordPress 管理员控制面板” 面板的 “使用公有 IP 地址” 下，选择以下格式的链接：

   http://*public-ipv4-address*。 /wp-admin
4. 在用户名或电子邮件地址中，输入 **user**。
5. 在密码中，输入在上一步中获得的密码。
6. 选择登录。



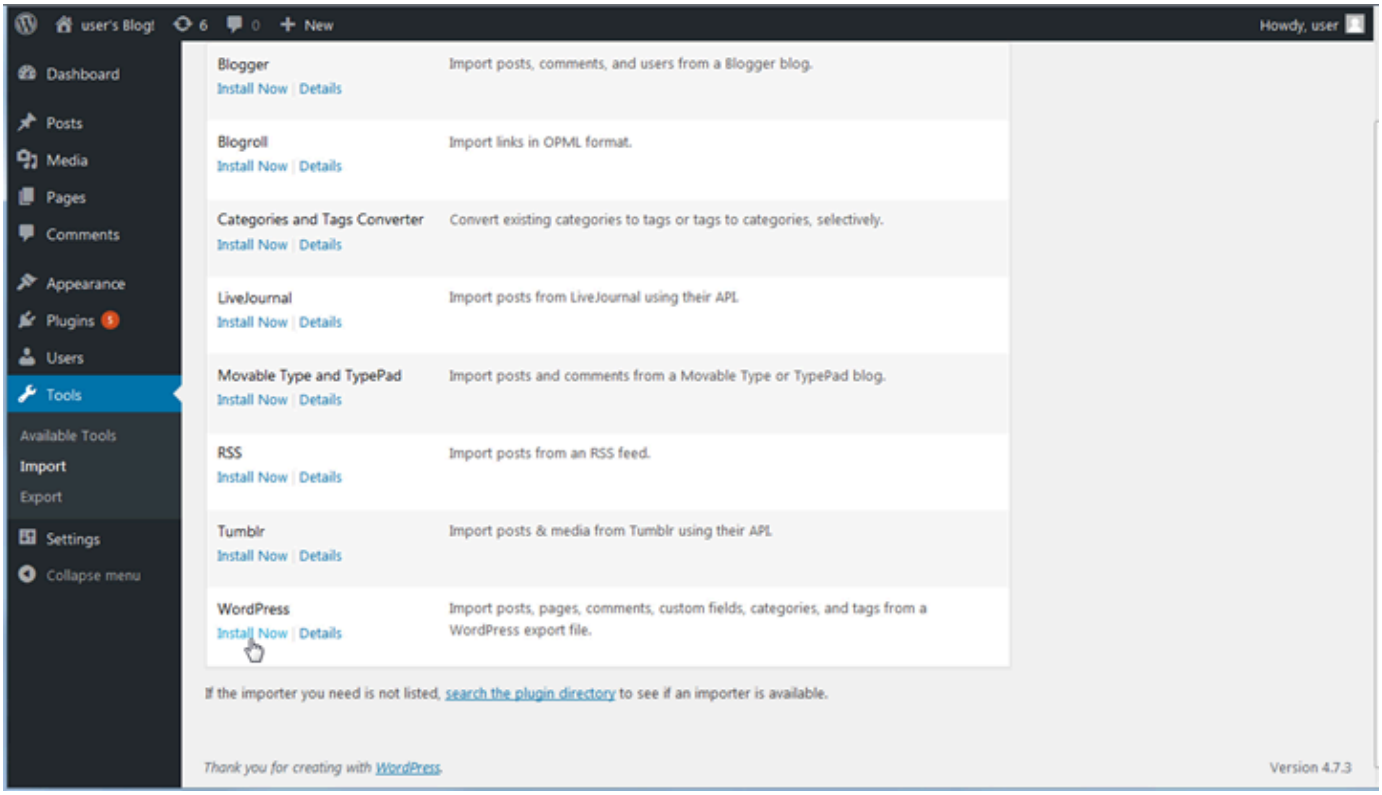
现在，您已登录 WordPress 网站的管理控制面板，可以在其中执行管理操作。有关管理 WordPress 网站的更多信息，请参阅 WordPress 文档中的 WordPressCodex。



第 4 步：将你的 XML 文件导入你的新 Lightsail 博客中

在新的 Lightsail 实例上成功登录 WordPress 控制面板后，请按照以下步骤将 XML 文件导入到新的 Lightsail 博客中。

1. 在新 Lightsail 实例的 WordPress 控制面板中，选择工具。
2. 选择 “导入”，然后选择 “立即安装” 以安装 WordPress 导入工具。



3. 安装完此工具后，选择 Run Importer（运行导入工具）以运行导入工具。
4. 在 “导入 WordPress” 页面上，选择 “浏览”。
5. 找到您在步骤 1：备份现有 WordPress博客中保存的 XML 文件，然后选择 “打开”。
6. 选择 Upload file and import（上传文件并导入）。

   接受其余默认值，然后选择 Submit（提交）。

后续步骤

您可以通过选择博客（“主页” 图标旁边），然后从 WordPress 控制面板中选择 “访问网站” 来验证一切是否正常。您也可以在浏览器中键入 IP 地址并查看博客。

下面是一些后续步骤：

- 迁移您的 DNS，以便您的域名服务器指向新版博客。
- 自定义新博客的外观和/或安装一些 WordPress 插件。
- 使用 SSL 证书启用 HTTPS 支持

按照 step-by-step说明启动和配置实例，使用 HTTPS 保护 WordPress 实例，将其连接到外部数据库或存储服务，并将现有博客迁移到 Lightsail。这些教程涵盖了基本任务，例如获取 WordPress 管理员证书、安装插件、配置 DNS 和域设置，以及与 Amazon S3、Amazon Aurora 和 Amazon SES AWS 服务 等其他内容集成。按照本指南，您可以在 Lightsail 平台上轻松设置和管理安全、可扩展且高性能的 WordPress 网站。

在 Lightsai WordPress l 上使用 Multisite 管理多个站点

本节涵盖以下与在 Amazon Lightsail 中管理 WordPress多站点实例上的博客相关的主题：

主题

- 在 Lightsail 上将博客作为域名添加到你的 WordPress 多站点
- 在 Lightsail 上将博客作为子域名添加到你的 WordPress 多站点
- 在 Lightsail 上为你的 WordPress 多站点实例定义主域名

在 Lightsail 上将博客作为域名添加到你的 WordPress 多站点

Amazon Lightsail 中的 WordPress 多站点实例旨在为您在该实例中创建的每个博客网站使用多个域名或子域名。在本指南中，我们将向您展示如何在 WordPress 多站点实例上使用与主博客主域不同的域名来添加博客网站。例如，如果您主博客的主域为 `example.com`，则可以在同一实例上创建使用 `another-example.com` 和 `third-example.com` 域的新博客站点。

> **Note**
>
> 您也可以使用子域名将网站添加到您的 WordPress 多站点实例。有关更多信息，请参阅将博客作为子域名添加到您的 WordPress 多站点实例。

先决条件

请按照显示的顺序完成以下先决条件：

1. 在 Lightsail 中创建一个 WordPress 多站点实例。有关更多信息，请参阅创建实例。
2. 在 Lightsail 中创建静态 IP 并将其附加到您的 WordPress 多站点实例。有关更多信息，请参阅创建静态 IP 并将其附加到实例。
3. 通过创建 DNS 区域将您的域添加到 Lightsail，然后将其指向您连接到 WordPress 多站点实例的静态 IP。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

4. 为您的 WordPress 多站点实例定义主域。有关更多信息，请参阅为您的 WordPress 多站点实例定义主域。

将博客作为域名添加到您的 WordPress 多站点实例

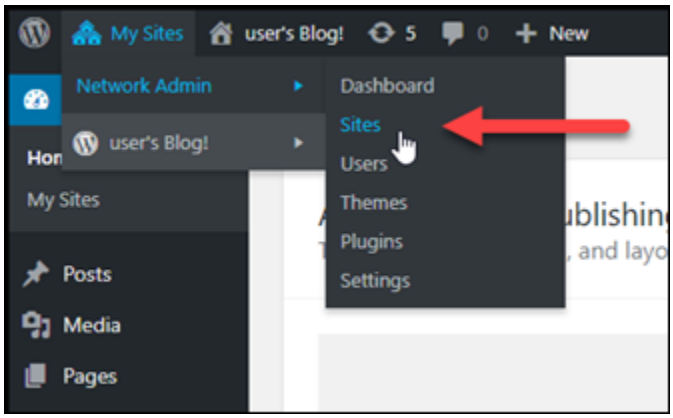
完成以下步骤，在您的 WordPress Multisite 实例上创建一个博客网站，该网站使用的域名与主博客的主域名不同。

> **Important**
>
> 在执行这些步骤之前，您必须完成本指南的先决条件部分中列出的步骤 4。

1. 登录您的 WordPress 多站点实例的管理控制面板。

   > **Note**
   >
   > 有关更多信息，请参阅获取 Bitnami 实例的应用程序用户名和密码。

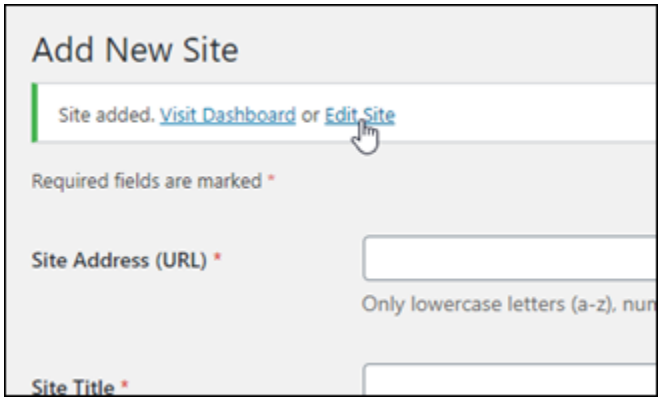
2. 在顶部导航窗格中依次选择 My Sites (我的站点)、Network Admin (网络管理) 和 Sites (站点)。



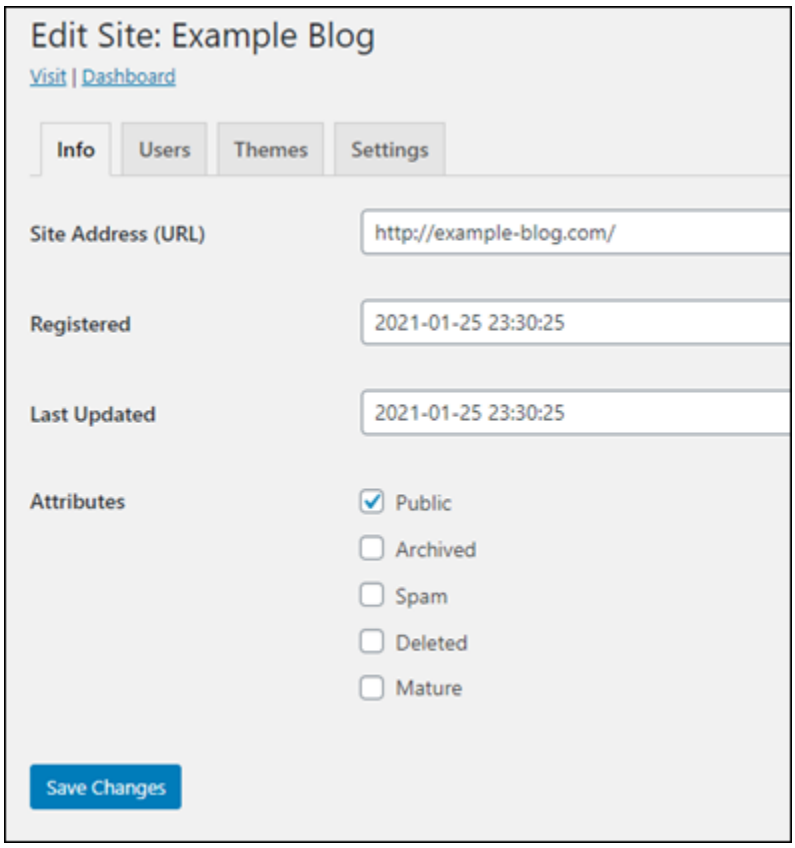
3. 选择 Add New (新增) 以添加新博客站点。
4. 在 Site Address (URL) (站点地址 [URL]) 文本框中输入站点地址。此域将用于新博客站点。例如，如果您的新博客站点将 `example-blog.com` 用作域，则在 Site Address (URL) (站点地址 [URL]) 文本框中输入 `example-blog`。忽略页面上显示的主域后缀。



5. 输入站点标题，选择站点语言，然后输入管理员电子邮件地址。
6. 选择 Add Site (添加站点)。
7. 在页面上显示的确认横幅中选择 Edit Site (编辑站点)。这将重新导向以编辑您最近创建的站点的详细信息。

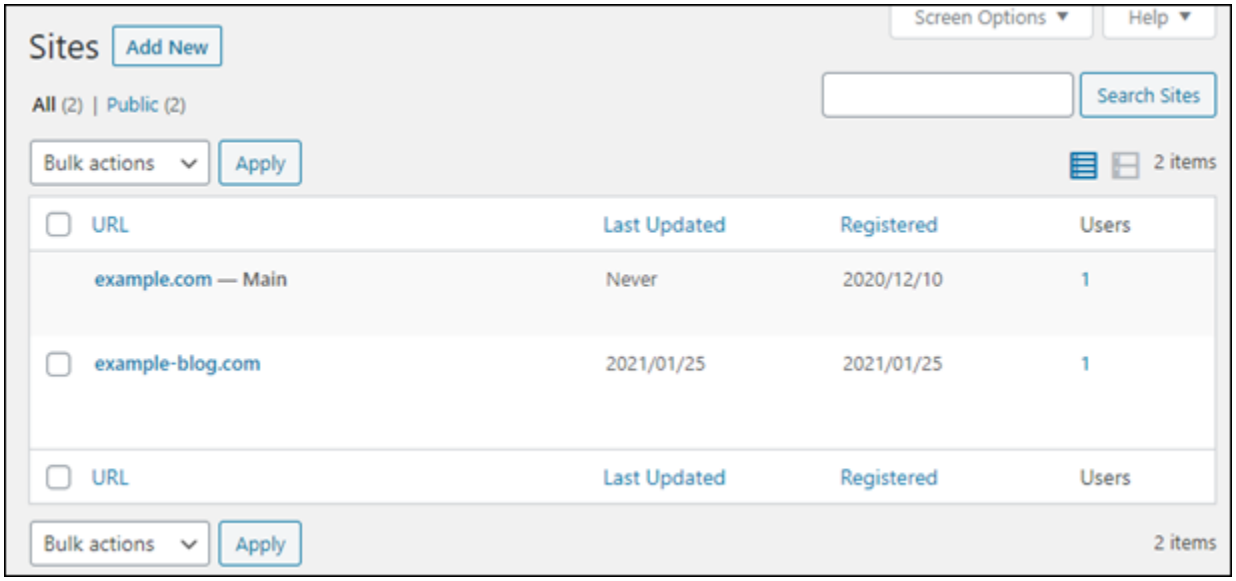


8. 在 Edit Site (编辑站点) 页面上，将 Site Address (URL) (站点地址 [URL]) 文本框中列出的子域更改为要使用的顶级域。在此示例中，我们指定了 `http://example-blog.com`。



9. 选择 Save Changes（保存更改）。

   此时，新的博客网站已在您的 WordPress 多站点实例中创建，但是该域尚未配置为路由到新的博客网站。继续执行下一步，以将地址记录（A 记录）添加到域的 DNS 区域。



将地址记录（A 记录）添加到域的 DNS 区域中

完成以下步骤，将您的新博客网站的域名指向您的 WordPress多站点实例。您必须对在 M WordPress ultisite 实例上创建的每个博客网站执行这些步骤。

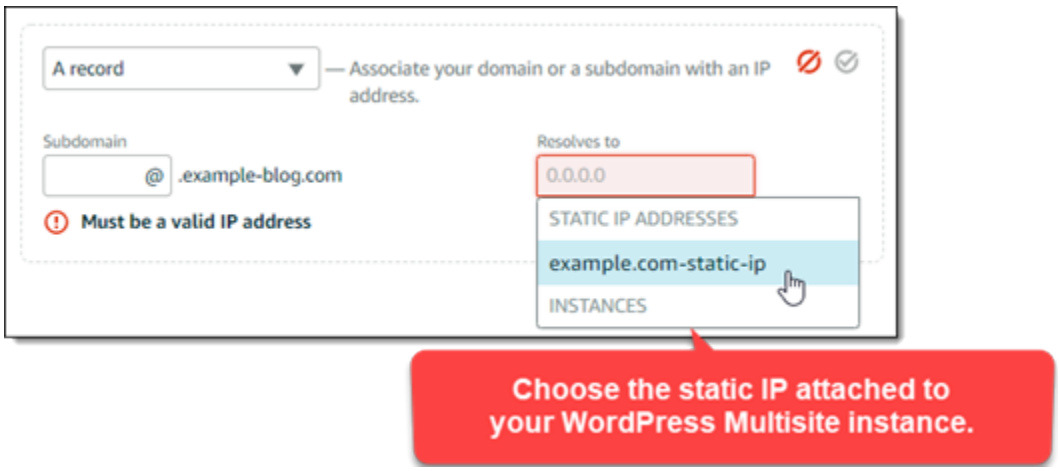
出于演示目的，我们将使用 Lightsail DNS 区域。不过，通常由域注册商托管的其他 DNS 区域的操作步骤与之类似。

> **Important**
>
> 在 Lightsail 控制台中，您最多可以创建六个 DNS 区域。如果您需要三个以上的 DNS 区域，建议您使用 Amazon Route 53 管理域的 DNS 记录。有关更多信息，请参阅将 Amazon Route 53 作为现有域的 DNS 服务。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 域和 DNS。
3. 在页面的 DNS 区域部分，为新博客站点的域选择 DNS 区域。
4. 在 DNS 区域编辑器中，选择 DNS records（DNS 记录）选项卡。然后，选择 Add record（添加记录）。



5. 在记录类型下拉菜单中，选择 A 记录。
6. 在 Record name（记录名称）文本框中，输入 @ 符号以为域的根创建记录。
7. 在解析到文本框中，选择连接到您的 WordPress 多站点实例的静态 IP 地址。



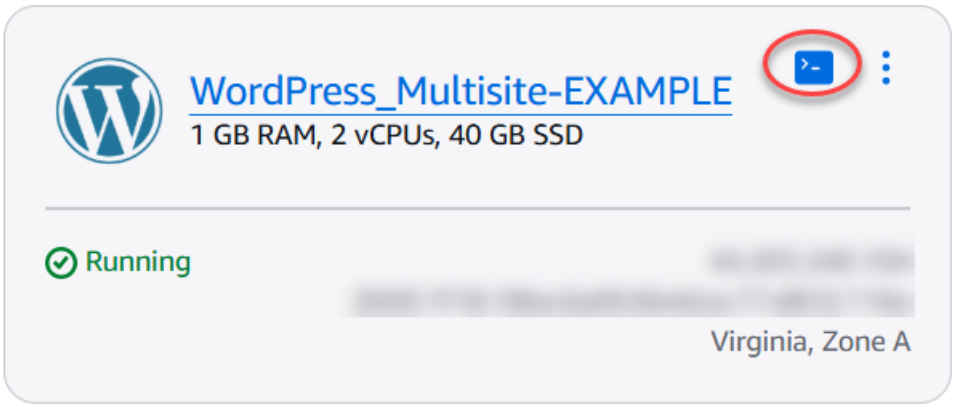
8. 选择保存图标。

   更改通过互联网的 DNS 传播后，该域会将流量路由到您的 WordPress Multisite 实例上的新博客网站。

启用 Cookie 支持以允许登录博客站点

当您将博客网站作为域名添加到 WordPress 多站点实例时，您还必须更新实例上的 WordPress 配置 (`wp-config`) 文件以启用 Cookie 支持。如果您不启用 Cookie 支持，则用户在尝试登录其博客网站的 WordPress管理仪表板时可能会遇到 “错误：Cookie 被阻止或不支持” 错误。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页上，为您的 WordPress多站点实例选择 SSH 快速连接图标。



3. 连接基于 Lightsail 浏览器的 SSH 会话后，输入以下命令以使用 Vim 打开和编辑您的`wp-config.php`实例的文件：

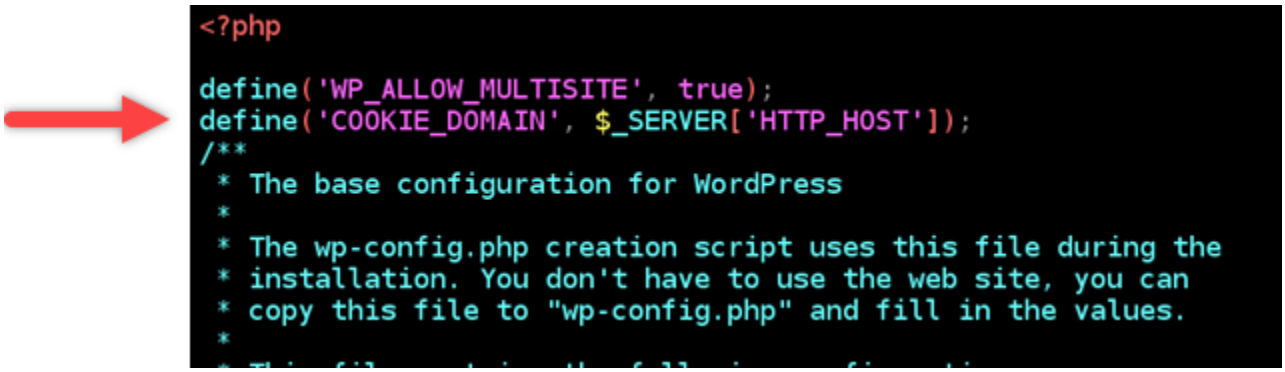
```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

> **Note**
>
> 如果此命令失败，则您可能使用的是旧版本的 WordPress多站点实例。尝试运行以下命令。
>
> ```
> sudo vim /opt/bitnami/wordpress/wp-config.php
> ```

4. 按 I 进入 Vim 的插入模式。
5. 将以下文本行添加到 `define('WP_ALLOW_MULTISITE', true);` 文本行的下面。

   ```
   define('COOKIE_DOMAIN', $_SERVER['HTTP_HOST']);
   ```

   完成后，文件将与以下内容类似：

6. 按 ESC 键退出 Vim 的插入模式，然后输入 `:wq!` 并按 Enter 以保存您的编辑内容（写入），再退出 Vim。
7. 输入以下命令以重启 WordPress实例的底层服务。

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   现在应该在您的 WordPress 多站点实例上启用 Cookie，尝试登录其博客网站的用户不会遇到 “错误：Cookie 被屏蔽或不支持” 错误。

后续步骤

将博客作为域名添加到 WordPress 多站点实例后，我们建议您熟悉 WordPress 多站点管理。有关更多信息，请参阅 WordPress 文档中的多站点网络管理。

在 Lightsail 上将博客作为子域名添加到你的 WordPress 多站点

Amazon Lightsail 中的 WordPress 多站点实例旨在为您在该实例中创建的每个博客网站使用多个域名或子域名。在本指南中，我们将向您展示如何将博客网站添加为 WordPress 多站点实例的子域。例如，如果您的主博客的主域为 `example.com`，则可以在同一实例上使用 `earth.example.com` 和 `moon.example.com` 子域创建新的博客站点。

> **Note**
>
> 您也可以使用域名将网站添加到您的 WordPress 多站点实例。有关更多信息，请参阅将博客作为域名添加到您的 WordPress 多站点实例。

先决条件

请按照显示的顺序完成以下先决条件：

1. 创建 WordPress 多站点实例。有关更多信息，请参阅创建实例。
2. 创建静态 IP 并将其附加到您的 WordPress 多站点实例。有关更多信息，请参阅创建静态 IP 并将其附加到实例。
3. 通过创建 DNS 区域将您的域添加到 Lightsail，然后将其指向您连接到 WordPress 多站点实例的静态 IP。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。
4. 为您的 WordPress 多站点实例定义主域。有关更多信息，请参阅为您的 WordPress 多站点实例定义主域。

将博客作为子域添加到您的 WordPress多站点实例

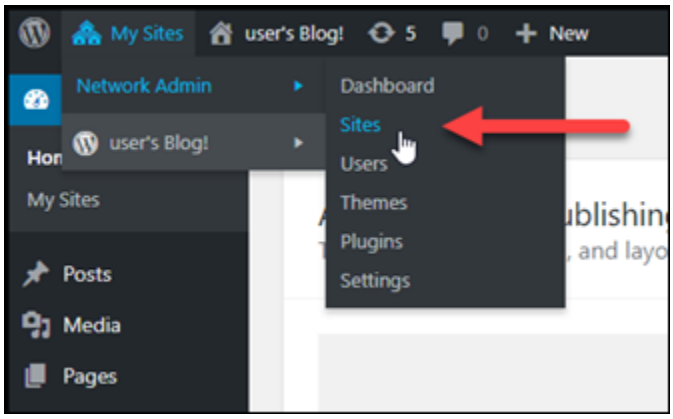
完成以下步骤，在您的 WordPress 多站点实例上创建使用主博客主域名子域的新博客。

> **Important**
>
> 在执行这些步骤之前，您必须完成本指南的先决条件部分中列出的步骤 4。

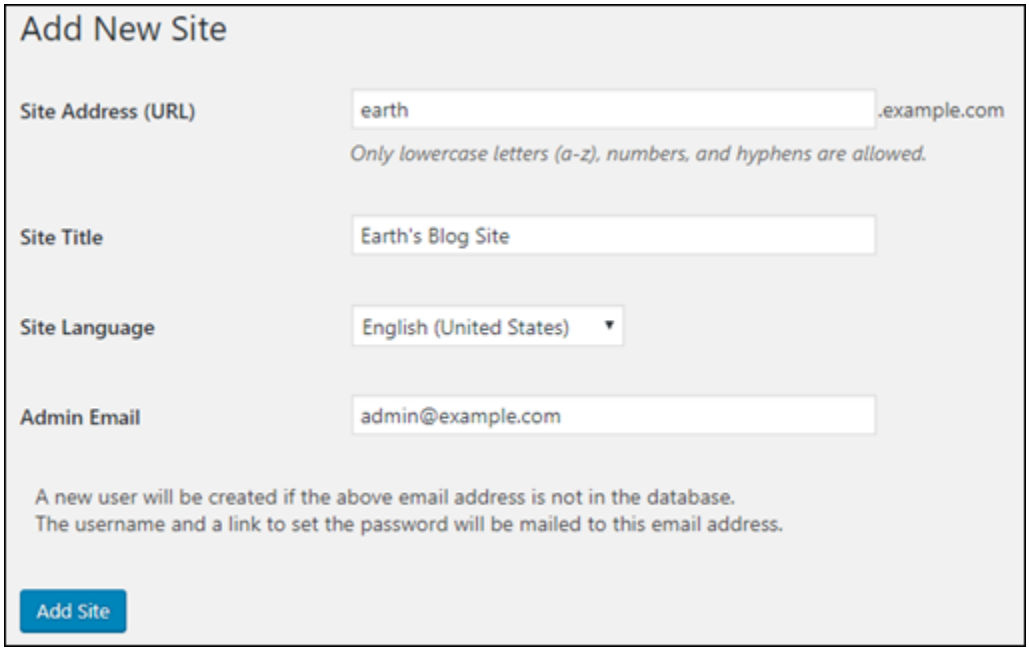
1. 登录您的 WordPress 多站点实例的管理控制面板。

> **Note**
>
> 有关更多信息，请参阅获取 Bitnami 实例的应用程序用户名和密码。

2. 在顶部导航窗格中依次选择 My Sites (我的站点)、Network Admin (网络管理) 和 Sites (站点)。

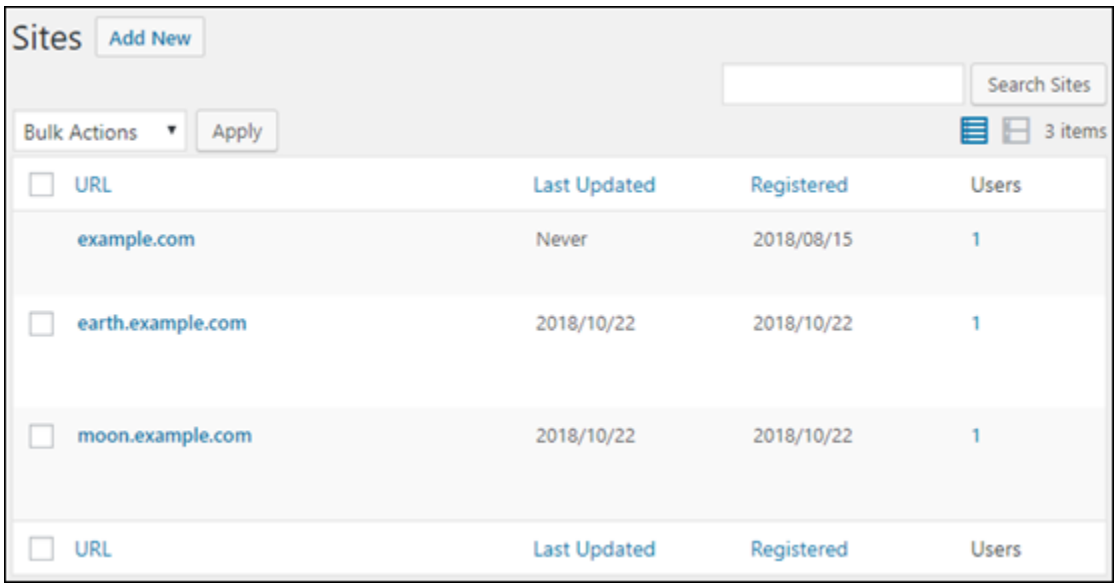


3. 选择 Add New (新增) 以添加新博客站点。
4. 输入一个站点地址，该地址是将用于新博客站点的子域。



5. 输入站点标题，选择站点语言，然后输入管理员电子邮件地址。
6. 选择 Add Site (添加站点)。

此时，新的博客网站已在您的 WordPress Multisite 实例中创建，但子域尚未配置为路由到新的博客网站。继续执行下一步，以将地址记录（A 记录）添加到域的 DNS 区域。



将地址记录（A 记录）添加到域的 DNS 区域中

完成以下步骤，将您的新博客网站的子域名指向您的 WordPress多站点实例。您必须对在 M WordPress ultisite 实例上创建的每个博客网站执行这些步骤。

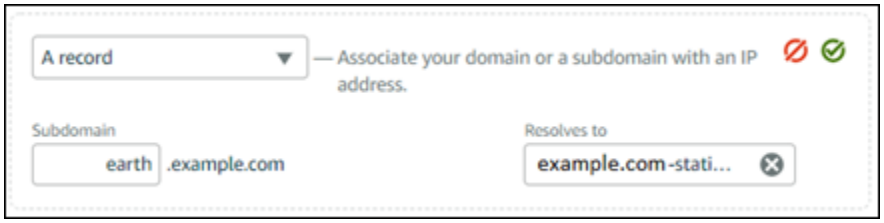
出于演示目的，我们将使用 Lightsail DNS 区域。不过，通常由域注册商托管的其他 DNS 区域的操作步骤与之类似。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择域和 DNS。
3. 在该页面的 DNS 区域部分下，选择您定义为 WordPress 多站点实例主域名的域名的 DNS 区域。
4. 在 DNS 区域编辑器中，选择 DNS records（DNS 记录）选项卡。然后，选择 Add record（添加记录）。



5. 在记录类型下拉菜单中，选择 A 记录。

6. 在记录名称文本框中，输入在 WordPress 多站点实例上创建新博客网站时指定为网站地址的子域。
7. 在“解析为”文本框中，选择连接到您的 WordPress 多站点实例的静态 IP 地址。



8. 选择保存图标。

   这是您需要执行的所有操作。更改通过互联网的 DNS 传播后，该域名将重定向到您的 WordPress 多站点实例上的新博客网站。

后续步骤

将博客作为子域添加到 WordPress 多站点实例后，我们建议您熟悉 WordPress 多站点管理。有关更多信息，请参阅 WordPress 文档中的多站点网络管理。

在 Lightsail 上为你的 WordPress 多站点实例定义主域名

Amazon Lightsail 中的 WordPress 多站点实例旨在为您在该实例中创建的每个博客网站使用多个域名或子域名。因此，您必须定义用于 WordPress 多站点实例主博客的主域名。

先决条件

请按照显示的顺序完成以下先决条件：

1. 在 Lightsail 中创建一个 WordPress 多站点实例。有关更多信息，请参阅创建实例。
2. 在 Lightsail 中创建静态 IP 并将其附加到您的 WordPress 多站点实例。有关更多信息，请参阅创建静态 IP 并将其附加到实例。

   > **Important**
   >
   > 在为 WordPress 多站点实例附加静态 IP 后，必须重启该实例。这将允许实例识别与其关联的新静态 IP。

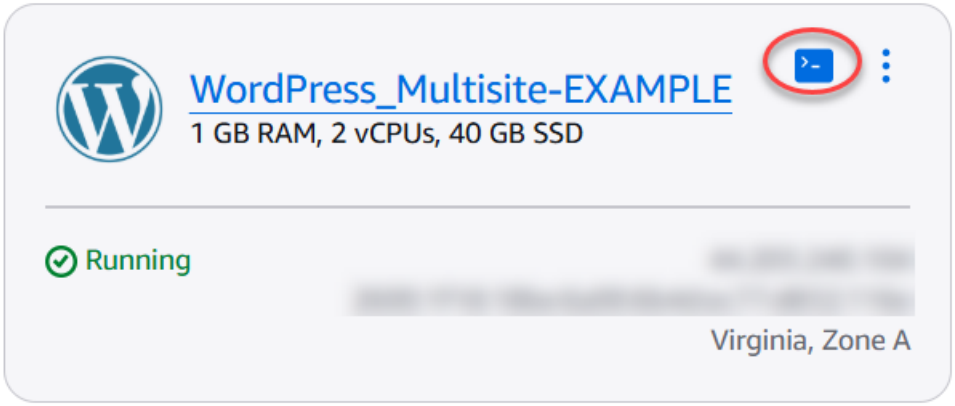
3. 通过创建 DNS 区域将您的域添加到 Lightsail，然后将其指向您连接到 WordPress 多站点实例的静态 IP。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

4. 给 DNS 更改一些时间在 Internet 的 DNS 内进行传播。然后，您可以继续阅读本指南的 “为 WordPress 多站点实例定义主域>” 部分。

为您的 WordPress 多站点实例定义主域

完成这些步骤以确保您的域名（例如`example.com`）重定向到 WordPress 多站点实例的主博客。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，为您的 WordPress多站点实例选择 SSH 快速连接图标。



3. 输入以下命令为您的 WordPress多站点实例定义主域名。请务必*<domain>*替换为适用于您的 WordPress 多站点的正确域名。

```
sudo /opt/bitnami/configure_app_domain --domain <domain>
```

示例：

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

> **Note**
>
> 如果此命令失败，则您可能使用的是旧版本的 WordPress多站点实例。改为尝试运行以下命令，并确保替换*<domain>*为适用于您的 WordPress Multisite 的正确域名。
>
> ```
> cd /opt/bitnami/apps/wordpress
> sudo ./bnconfig --machine_hostname <domain>
> ```
>
> 运行该命令后，输入以下命令，以防止 bnconfig 工具在服务器每次重启时自动运行。

```
sudo mv bnconfig bnconfig.disabled
```

此时，浏览到您定义的域名应该会将您重定向到 WordPress Multisite 实例的主博客。

后续步骤

为 WordPress多站点实例定义主域名后，请完成以下步骤：

- 将博客作为子域添加到您的 WordPress 多站点实例
- 将博客作为域名添加到您的 WordPress 多站点实例

按照 step-by-step说明学习如何使用单独的域名或子域名添加新的博客网站，以及如何在 WordPress Multisite 实例上为主博客定义主域名。

该指南涵盖了创建 WordPress 多站点实例、连接静态 IP、创建 DNS 区域和配置主域等先决条件。然后，它提供了将博客添加为域或子域、更新 DNS 记录、启用 cookie 支持以及执行其他必要配置的详细步骤。通过遵循本指南，您可以灵活地为每个博客网站使用单独的域名或子域名，从而在WordPress多站点实例中有效地管理和组织多个博客。

使用 Let's Encrypt 为 Lightsail 资源启用加密通信

本指南涵盖了以下与 “让我们在 Amazon Lightsail 中进行加密” 相关的主题。在开始之前，请确保您已满足以下先决条件：

先决条件

- 创建一个运行 LAMP、Nginx 或 WordPress
- 注册一个域，并且有权编辑其 DNS 记录
- 使用基于 Lightsail 浏览器的 SSH 终端或你自己的 SSH 客户端。

主题

- 使用 “让我们加密 SSL 证书” 保护你的 Lightsail LAMP 实例
- 使用 Let's Encrypt SSL/TLS 保护你的 Lightsail Nginx 网站
- 使用免费的 “让我们加密 SSL” 证书保护你的 Lightsail WordPress 实例

使用 “让我们加密 SSL 证书” 保护你的 Lightsail LAMP 实例

Amazon Lightsail 可以使用 Lightsail 负载均衡器使用 SSL/TLS 轻松保护您的网站和应用程序。但是，使用 Lightsail 负载均衡器通常可能不是正确的选择。您的站点可能不需要负载均衡器提供的可扩展性或容错能力，或者您可能针对成本进行了优化。

在后一种情况下，您可能会考虑使用 Let's Encrypt 获取免费 SSL 证书。如果是这样，一切都没有问题。您可以将这些证书与 Lightsail 实例集成。本教程演示了如何使用 Certbot 请求 Let's Encrypt 通配符证书，以及如何将该证书与 LAMP 实例集成。

Important

- 2020 年 7 月，Bitnami 实例使用的 Linux 发行版从 Ubuntu 更改为 Debian。由于此更改，本教程中的某些步骤将因实例的 Linux 发行版而异。在更改后创建的所有 Bitnami 蓝图实例都将使用 Debian Linux 发行版。在更改之前创建的实例将继续使用 Ubuntu Linux 发行版。要检查实例的发行版，请运行 `uname -a` 命令。响应会将 Ubuntu 或 Debian 显示为实例的 Linux 发行版。
- Bitnami 正在修改许多堆栈的文件结构。本教程中的文件路径可能会发生变化，具体取决于您的 Bitnami 堆栈是使用本地 Linux 系统包（方法 A），还是自包含安装（方法 B）。要确定 Bitnami 安装类型以及要遵循的方法，请运行以下命令：

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach
  A: Using system packages." || echo "Approach B: Self-contained
  installation."
  ```

内容

- 步骤 1：完成先决条件
- 步骤 2：在实例上安装 Certbot
- 步骤 3：请求 Let's Encrypt SSL 通配符证书
- 步骤 4：将 TXT 记录添加到域的 DNS 区域
- 步骤 5：确认 TXT 记录已传播
- 步骤 6：完成 Let's Encrypt SSL 证书请求
- 步骤 7：创建指向 Apache 服务器目录中的 Let's Encrypt 证书文件的链接
- 步骤 8：为 Web 应用程序配置 HTTP 到 HTTPS 重新导向

- 步骤 9：每 90 天续订一次 Let's Encrypt 证书

步骤 1：完成先决条件

请完成以下先决条件（如果尚未完成）：

- 在 Lightsail 中创建一个 LAMP 实例。要了解更多信息，请参阅创建实例。
- 注册一个域名，并获取管理访问权限以编辑其 DNS 记录。要了解更多信息，请参阅 Amazon Lightsail DNS。

> **Note**
>
> 我们建议您使用 Lightsail DNS 区域来管理域名的 DNS 记录。要了解更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

- 在 Lightsail 控制台中使用基于浏览器的 SSH 终端来执行本教程中的步骤。但是，您也可以使用自己的 SSH 客户端（如 PuTTY）。要了解有关配置 PuTTY 的更多信息，请参阅下载并设置 PuTTY 以使用 SSH 进行连接。

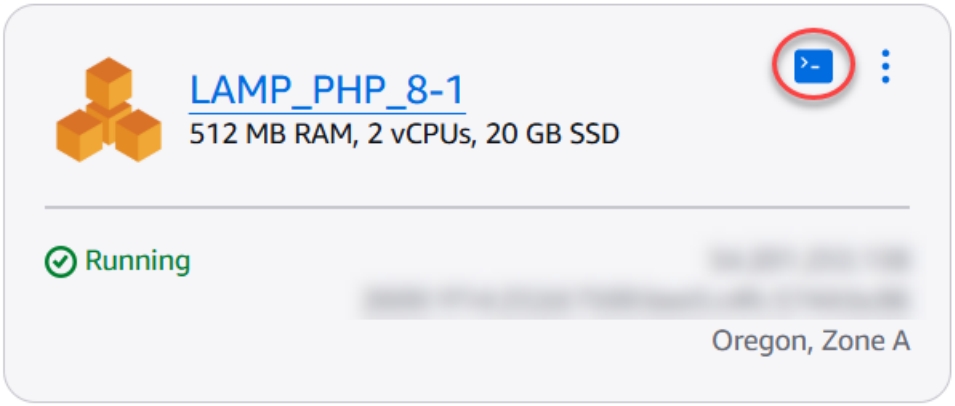
完成先决条件后，请继续执行本教程的下一部分。

步骤 2：在实例上安装 Certbot

Certbot 是用于从 Let's Encrypt 请求证书并将其部署到 Web 服务器的客户端。Let's Encrypt 使用 ACME 协议颁发证书，而 Certbot 是与 Let's Encrypt 交互且启用 ACME 的客户端。

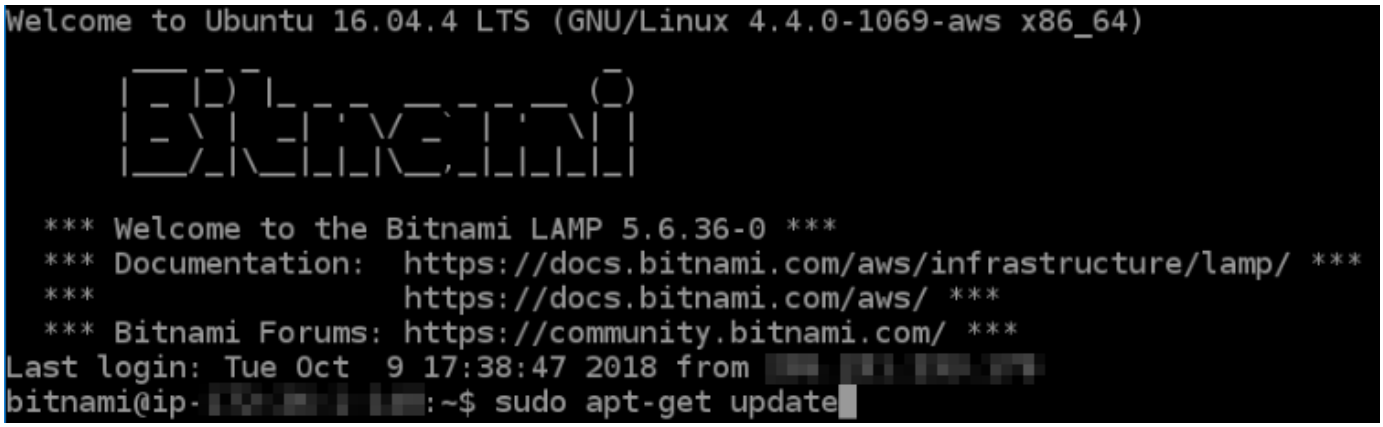
在你的 Lightsail 实例上安装 Certbot

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格，选择您想连接的实例的 SSH 快速连接图标。



3. 连接基于 Lightsail 浏览器的 SSH 会话后，输入以下命令以更新实例上的软件包：

```
sudo apt-get update
```



4. 输入以下命令以安装软件属性包。Certbot 的开发人员使用个人程序包存档 (PPA) 分配 Certbot。软件属性包使其使用起来更加高效 PPAs。

```
sudo apt-get install software-properties-common
```

> **Note**
>
> 如果您在运行 `sudo apt-get install` 命令时遇到 `Could not get lock` 错误，请等待大约 15 分钟，然后重试。此错误可能是由 cron 作业导致的，该作业使用 Apt 包管理工具来安装无人参与升级。

5. 输入以下命令以将 Certbot 添加到本地 apt 存储库：

> **Note**
>
> 步骤 5 仅适用于使用 Ubuntu Linux 发行版的实例。如果您的实例使用 Debian Linux 发行版，请跳过此步骤。

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. 输入以下命令来更新 apt，以包含新的存储库：

```
sudo apt-get update -y
```

7. 输入以下命令以安装 Certbot：

```
sudo apt-get install certbot -y
```

Certbot 现已安装在你的 Lightsail 实例上。

8. 使基于浏览器的 SSH 终端窗口保持打开状态 - 您将在本教程的稍后部分返回到该窗口。继续执行本教程的下一部分。

步骤 3：请求 Let's Encrypt SSL 通配符证书

开始从 Let's Encrypt 请求证书的流程。使用 Certbot 请求通配符证书，您可以将单个证书同时用于某个域及其子域。例如，一个通配符证书可适用于 `example.com` 顶级域、`blog.example.com` 以及 `stuff.example.com` 子域。

请求 Let's Encrypt SSL 通配符证书

1. 在本教程的步骤 2 中使用的同一个基于浏览器的 SSH 终端窗口中，输入以下命令为您的域设置环境变量。现在，您可以更高效地复制和粘贴命令以获取证书。

```
DOMAIN=Domain
```

```
WILDCARD=*.$DOMAIN
```

在命令中，*Domain*用您的注册域名替换。

示例：

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. 输入以下命令以确认变量返回正确的值：

```
echo $DOMAIN && echo $WILDCARD
```

您应该会看到类似以下内容的结果：

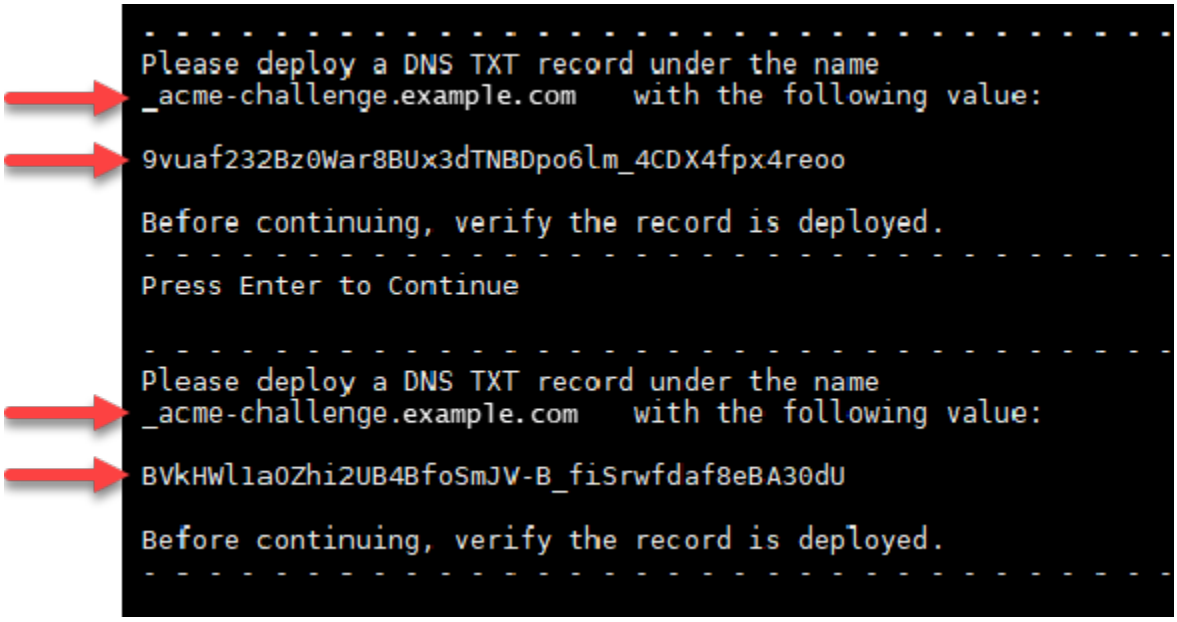


3. 输入以下命令以交互模式启动 Certbot。此命令指示 Certbot 使用具有 DNS 质询的手动授权方法验证域所有权。它可以为您的顶级域及其子域请求通配符证书。

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. 在系统提示时输入您的电子邮件地址，用于接收续订和安全通知。
5. 阅读 Let's Encrypt 服务条款。阅读完后，如果您同意该服务条款，请按 A。如果不同意，则无法获取 Let's Encrypt 证书。
6. 针对共享您电子邮件地址的提示以及有关您的 IP 地址已被记录的警告相应地做出响应。
7. Let's Encrypt 现在会提示您确认您拥有指定域。您可以通过将 TXT 记录添加到域的 DNS 记录执行此操作。系统会提供一组 TXT 记录值，如以下示例所示：

> **Note**
>
> Let's Encrypt 可以提供您必须用于验证的单个或多个 TXT 记录。在本示例中，向我们提供了两个 TXT 记录用于验证。



8. 保持基于 Lightsail 浏览器的 SSH 会话处于打开状态，本教程稍后将返回该会话。继续执行本教程的下一部分。

步骤 4：将 TXT 记录添加到域的 DNS 区域

将 TXT 记录添加到您的域的 DNS 区域中会验证您拥有该域。出于演示目的，我们使用 Lightsail DNS 区域。但是，该步骤可能类似于通常由域注册商托管的其他 DNS 区域。

> **Note**
>
> 要详细了解如何为您的域名创建 Lightsail DNS 区域，请参阅在 L ightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

在 Lightsail 中向你的域名的 DNS 区域添加 TXT 记录

1. 在左侧导航窗格中，选择域和 DNS。
2. 在页面的 DNS 区域部分下，选择您在 Certbot 证书请求中指定的域的 DNS 区域。
3. 在 DNS 区域编辑器中，选择 DNS records（DNS 记录）。
4. 选择添加记录。
5. 在 Record type（记录类型）下拉菜单中，选择 TXT record（TXT 记录）。

6. 将 Let's Encrypt 证书请求指定的值输入到 Record name（记录名称）和 Responds with（响应内容）字段中。

   > **Note**
   >
   > Lightsail 控制台会预先填充域的顶级域部分。例如，如果想要添加子域 *_acme-challenge.example.com*，您只需在文本框中输入 *_acme-challenge*，您保存此记录时 Lightsail 会添加 `.example.com` 部分。

7. 选择保存。
8. 重复执行第 4 至 7 步，以添加 Let's Encrypt 证书请求指定的另一组 TXT 记录。
9. 保持 Lightsail 控制台浏览器窗口处于打开状态，本教程稍后将返回该窗口。继续执行本教程的下一部分。

步骤 5：确认 TXT 记录已传播

使用该 MxToolbox 实用程序确认 TXT 记录已传播到互联网的 DNS。DNS 记录传播可能需要一段时间，具体取决于您的 DNS 托管提供商以及已为 DNS 记录配置的生存时间 (TTL)。请务必完成此步骤，并确认您的 TXT 记录已传播，然后再继续执行 Certbot 证书请求。否则，您的证书请求将失败。

确认 TXT 记录已传播到 Internet 的 DNS

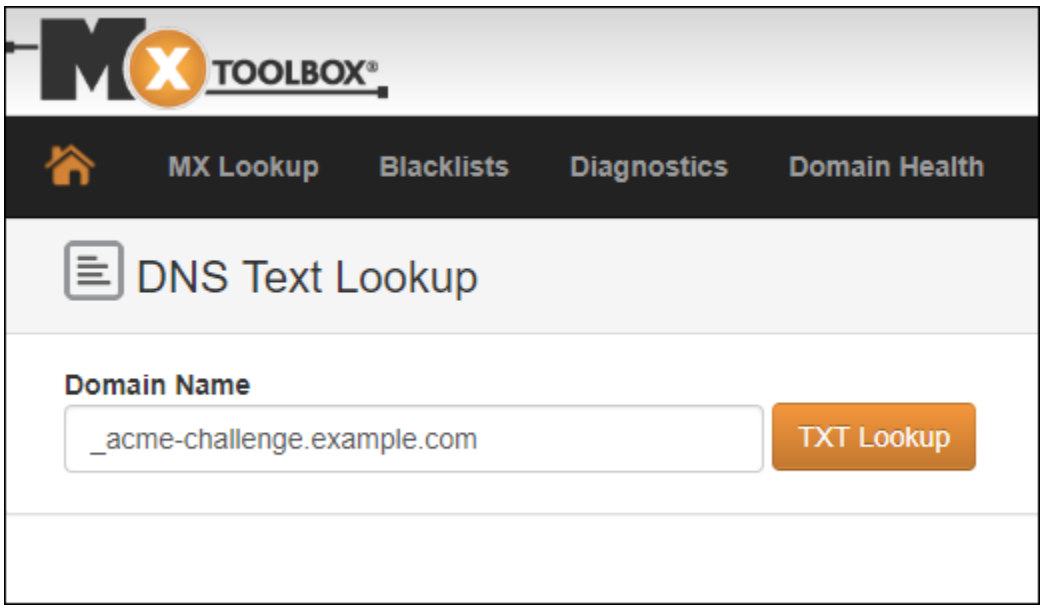
1. 打开一个新的浏览器窗口，然后转到 https://mxtoolbox.com/TXTLookup.aspx。
2. 在文本框中输入以下文本。

   ```
   _acme-challenge.Domain
   ```

   *Domain*替换为您注册的域名。

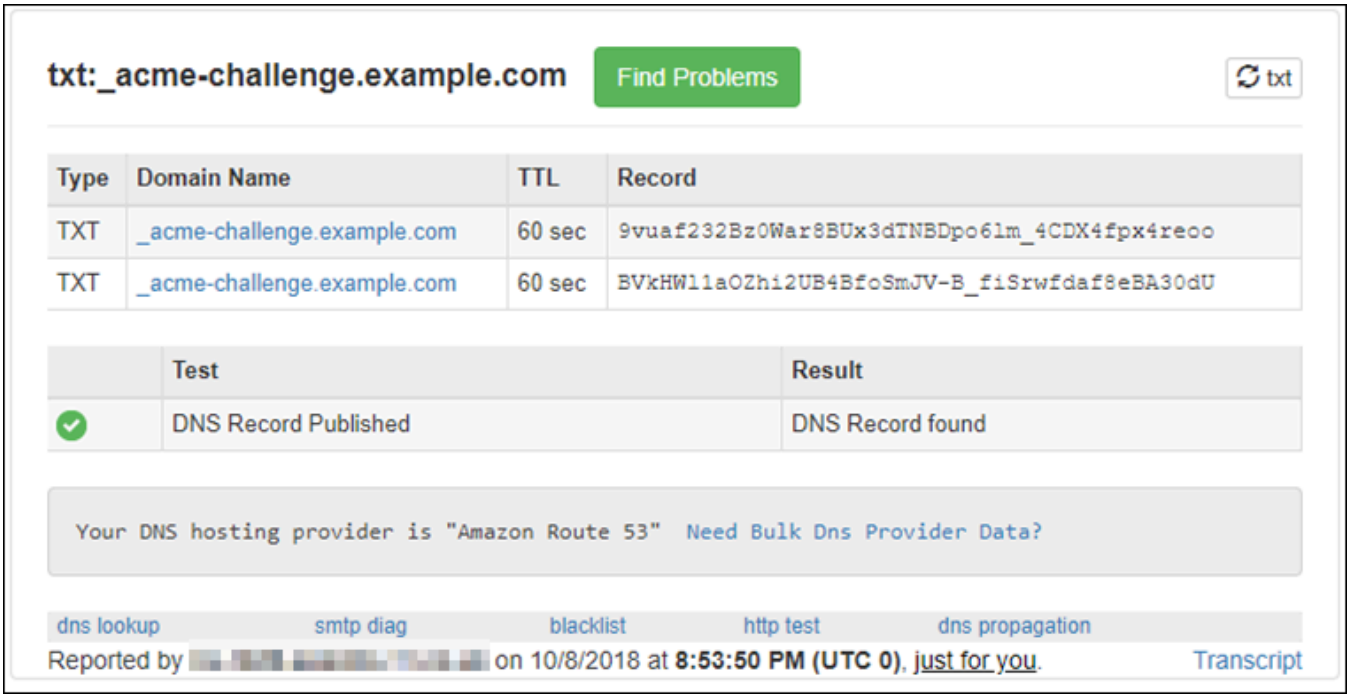
   示例：

   ```
   _acme-challenge.example.com
   ```



3. 选择 TXT Lookup (TXT 查找) 以运行检查。
4. 此时将出现以下任一响应：

   - 如果您的 TXT 记录已传播到 Internet 的 DNS，您将看到类似于以下屏幕截图中所示的响应。关闭浏览器窗口，然后继续执行本教程的下一部分。



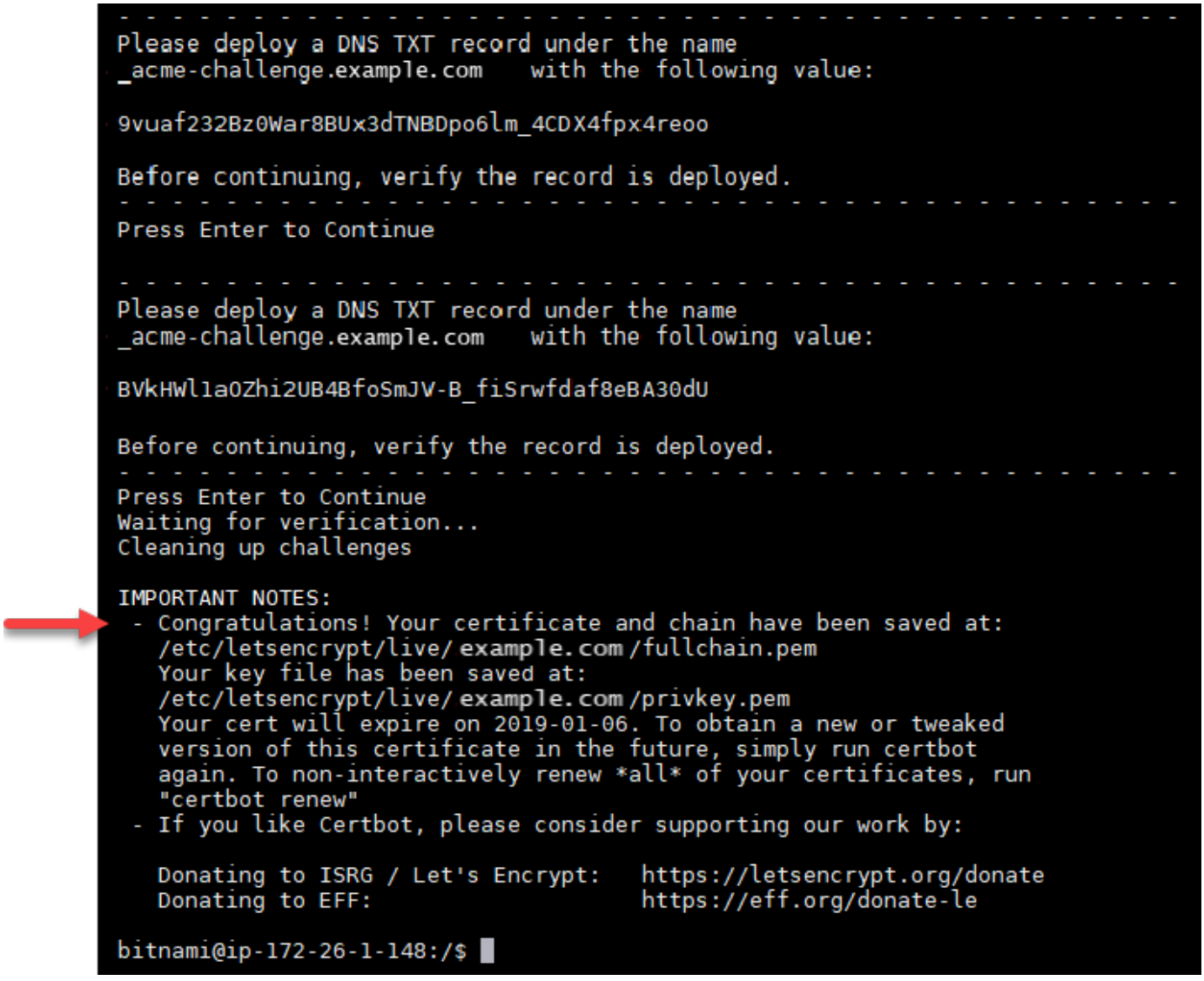
   - 如果您的 TXT 记录尚未传播到 Internet 的 DNS，您会看到 DNS Record not found (未找到 DNS 记录) 响应。确认您已将正确的 DNS 记录添加到域的 DNS 区域。如果您已添加正确的记录，请等待一段时间，让域的 DNS 记录传播，然后再次运行 TXT 查找。

步骤 6：完成 Let's Encrypt SSL 证书请求

返回您的 LAMP 实例的基于 Limtsail 浏览器的 SSH 会话，然后完成 Let's Encrypt 证书申请。Certbot 会将您的 SSL 证书、证书链和密钥文件保存在 LAMP 实例上的特定目录中。

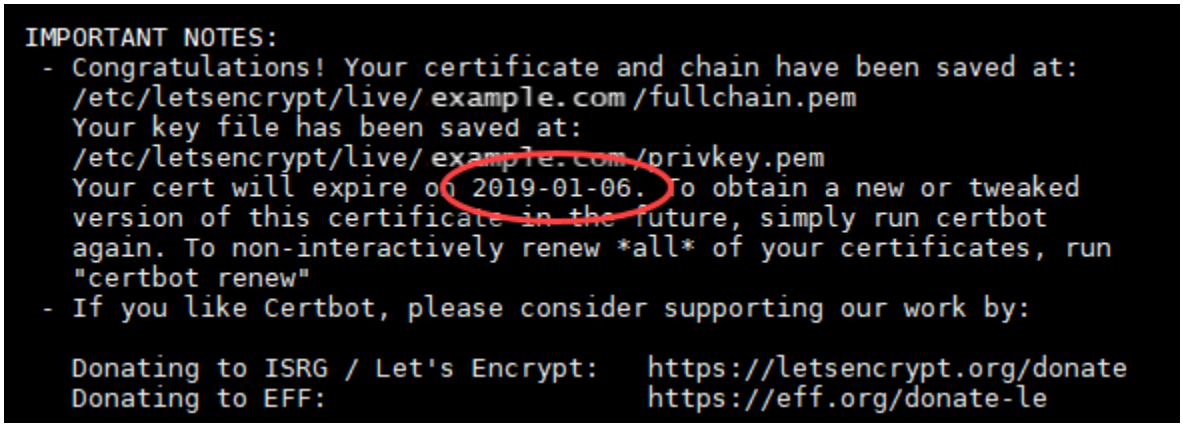
完成 Let's Encrypt SSL 证书请求

1. 在您的 LAMP 实例的基于 Lightsail 浏览器的 SSH 会话中，按 Enter 继续您的 Let's Encrypt SSL 证书申请。如果成功，系统将显示类似于以下屏幕截图中的响应：



   该消息确认您的证书、证书链和密钥文件已存储在/etc/letsencrypt/live/*Domain*/目录中。*Domain*将是您的注册域名，例如/etc/letsencrypt/live/*example.com*/。

2. 记录消息中指定的到期日期。您可以在该日期之前续订证书。



3. 您现在已拥有 Let's Encrypt SSL 证书，请继续执行本教程的下一部分。

步骤 7：创建指向 Apache 服务器目录中的 Let's Encrypt 证书文件的链接

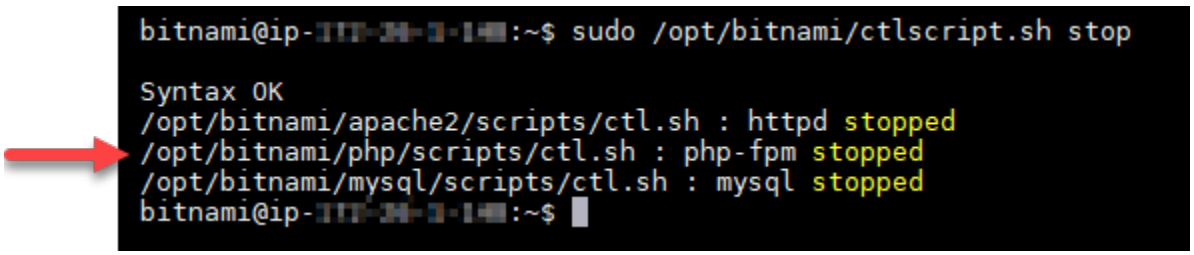
创建指向 LAMP 实例上 Apache 服务器目录中的 Let's Encrypt SSL 证书文件的链接。此外，请备份现有证书，以便之后需要。

创建指向 Apache 服务器目录中的 Let's Encrypt 证书文件的链接

1. 在您的 LAMP 实例的基于 Lightsail 浏览器的 SSH 会话中，输入以下命令以停止底层 LAMP 堆栈服务：

```
sudo /opt/bitnami/ctlscript.sh stop
```

您可以看到类似以下内容的响应：



2. 输入以下命令，为您所在域设置环境变量。

```
DOMAIN=Domain
```

在命令中，*Domain*用您的注册域名替换。

示例：

```
DOMAIN=example.com
```

3. 输入以下命令以确认变量返回正确的值：

```
echo $DOMAIN
```

您应该会看到类似以下内容的结果：



4. 分别输入以下命令，以重命名您的现有证书文件作为备份。请参阅本教程开头的重要提示，了解有关不同发行版和文件结构的信息。

   - 对于 Debian Linux发行版

     方法 A（使用系统包安装 Bitnami）：

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.crt /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.key /opt/bitnami/apache2/
     conf/bitnami/certs/server.key.old
     ```

     方法 B（自包含 Bitnami 安装）：

     ```
     sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/
     server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/
     server.key.old
     ```

   - 对于使用 Ubuntu Linux 发行版的较旧实例：

     ```
     sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.crt /opt/bitnami/apache/
     conf/bitnami/certs/server.crt.old
     ```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.key /opt/bitnami/apache/
conf/bitnami/certs/server.key.old
```

5. 分别输入以下命令，以创建指向 apache2 服务器目录中的 Let's Encrypt 证书文件的链接。请参阅本教程开头的重要提示，了解有关不同发行版和文件结构的信息。

   - 对于 Debian Linux发行版

     方法 A（使用系统包安装 Bitnami）：

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt
     ```

     方法 B（自包含 Bitnami 安装）：

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/server.crt
     ```

   - 对于使用 Ubuntu Linux 发行版的较旧实例：

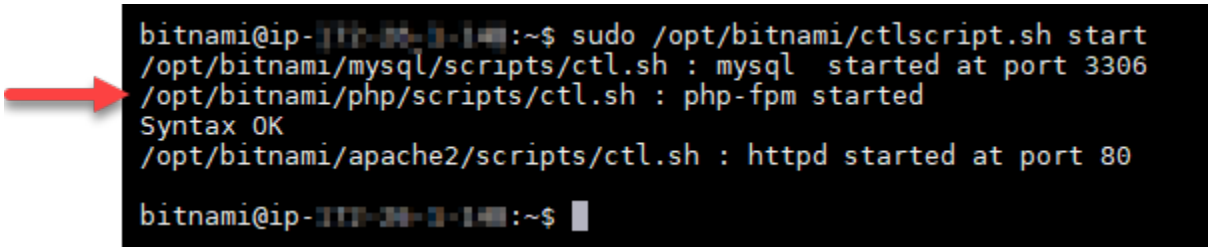
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.crt
     ```

6. 输入以下命令以启动之前停止运行的基础 LAMP 堆栈服务：

   ```
   sudo /opt/bitnami/ctlscript.sh start
   ```

   您应该会看到类似以下内容的结果：



您的 LAMP 实例现已配置为使用 SSL 加密。但是，流量不会自动从 HTTP 重新导向到 HTTPS。

7. 继续执行本教程的下一部分。

步骤 8：为 Web 应用程序配置 HTTP 到 HTTPS 重新导向

您可以为 LAMP 实例配置 HTTP 到 HTTPS 重新导向。自动从 HTTP 重新导向到 HTTPS 将使您的站点只能由使用 SSL 的客户访问，即使他们使用 HTTP 进行连接也是如此。

为 Web 应用程序配置 HTTP 到 HTTPS 重新导向

1. 在基于 LAMP 实例的 Lightsail 浏览器的 SSH 会话中，输入以下命令，使用 Vim 文本编辑器编辑 Apache Web 服务器配置文件：

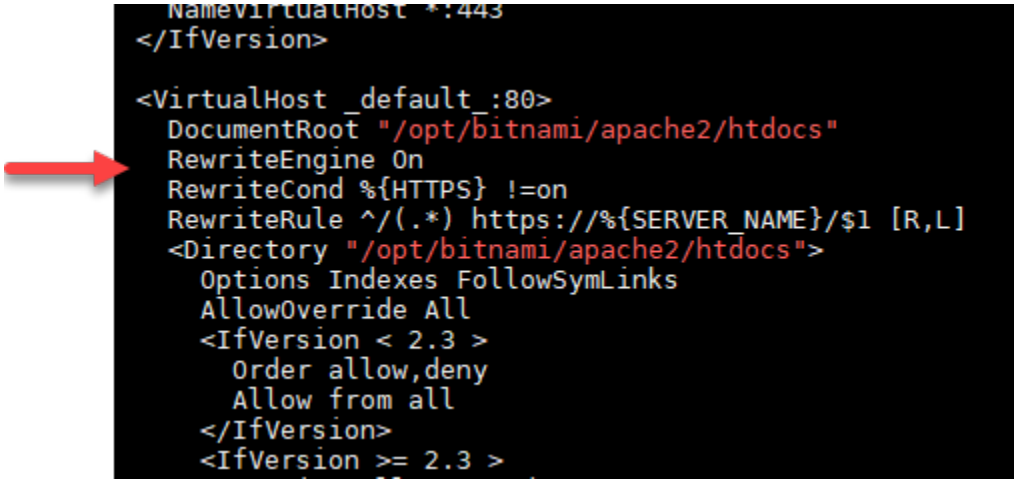
```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami.conf
```

> **Note**
>
> 本教程使用 Vim 来进行演示；但是，您可以针对此步骤使用您选择的任何文本编辑器。

2. 按 `i` 键进入 Vim 编辑器的插入模式。
3. 在文件中，在 `DocumentRoot "/opt/bitnami/apache2/htdocs"` 和 `<Directory "/opt/bitnami/apache2/htdocs">` 之间输入以下文本：

```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [R,L]
```

结果应该类似以下内容：



4. 按 ESC 键，然后输入 `:wq` 以写入（保存）您的编辑内容，然后退出 Vim。
5. 输入以下命令重新启动基础 LAMP 堆栈服务，以使编辑内容生效：

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   您的 LAMP 实例现已配置为自动将连接从 HTTP 重新导向到 HTTPS。当访问者访问 `http://www.example.com` 时，系统会自动将其重新导向至已加密的 `https://www.example.com` 地址。

步骤 9：每 90 天续订一次 Let's Encrypt 证书

Let's Encrypt 证书的有效期为 90 天。证书可以在到期前 30 天续订。要续订 Let's Encrypt 证书，请运行用于获取它们的原始命令。重复本教程的请求 Let's Encrypt SSL 通配符证书部分中的步骤。

使用 Let's Encrypt SSL/TLS 保护你的 Lightsail Nginx 网站

Amazon Lightsail 可以使用 Lightsail 负载均衡器使用 SSL/TLS 轻松保护您的网站和应用程序。但是，使用 Lightsail 负载均衡器通常可能不是正确的选择。您的站点可能不需要负载均衡器提供的可扩展性或容错能力，或者您可能针对成本进行了优化。

在后一种情况下，您可能会考虑使用 Let's Encrypt 获取免费 SSL 证书。如果是这样，一切都没有问题。您可以将这些证书与 Lightsail 实例集成。本教程演示了如何使用 Certbot 请求 Let's Encrypt 通配符证书，以及如何将该证书与您的 Nginx 实例集成。

Important

- 2020 年 7 月，Bitnami 实例使用的 Linux 发行版从 Ubuntu 更改为 Debian。由于此更改，本教程中的某些步骤将因实例的 Linux 发行版而异。在更改后创建的所有 Bitnami 蓝图实例都将使用 Debian Linux 发行版。在更改之前创建的实例将继续使用 Ubuntu Linux 发行版。要检查实例的发行版，请运行 `uname -a` 命令。响应会将 Ubuntu 或 Debian 显示为实例的 Linux 发行版。
- Bitnami 正在修改许多堆栈的文件结构。本教程中的文件路径可能会发生变化，具体取决于您的 Bitnami 堆栈是使用本地 Linux 系统包（方法 A），还是自包含安装（方法 B）。要确定 Bitnami 安装类型以及要遵循的方法，请运行以下命令：

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach
  A: Using system packages." || echo "Approach B: Self-contained
  installation."
  ```

内容

- 步骤 1：完成先决条件
- 第 2 步：在你的 Lightsail 实例上安装 Certbot
- 步骤 3：请求 Let's Encrypt SSL 通配符证书
- 步骤 4：将 TXT 记录添加到域的 DNS 区域
- 步骤 5：确认 TXT 记录已传播
- 步骤 6：完成 Let's Encrypt SSL 证书请求
- 步骤 7：创建指向 Nginx 服务器目录中的 Let's Encrypt 证书文件的链接
- 步骤 8：为 Web 应用程序配置 HTTP 到 HTTPS 重新导向
- 步骤 9：每 90 天续订一次 Let's Encrypt 证书

步骤 1：完成先决条件

请完成以下先决条件（如果尚未完成）：

- 在 Lightsail 中创建一个 Nginx 实例。要了解更多信息，请参阅创建实例。
- 注册一个域名，并获取管理访问权限以编辑其 DNS 记录。要了解更多信息，请参阅 DNS。

> **Note**
>
> 我们建议您使用 Lightsail DNS 区域管理域名的 DNS 记录。要了解更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

- 在 Lightsail 控制台中使用基于浏览器的 SSH 终端来执行本教程中的步骤。但是，您也可以使用自己的 SSH 客户端（如 PuTTY）。要了解有关配置 PuTTY 的更多信息，请参阅在 Amazon Lightsail 中下载并设置 PuTTY 以使用 SSH 进行连接。

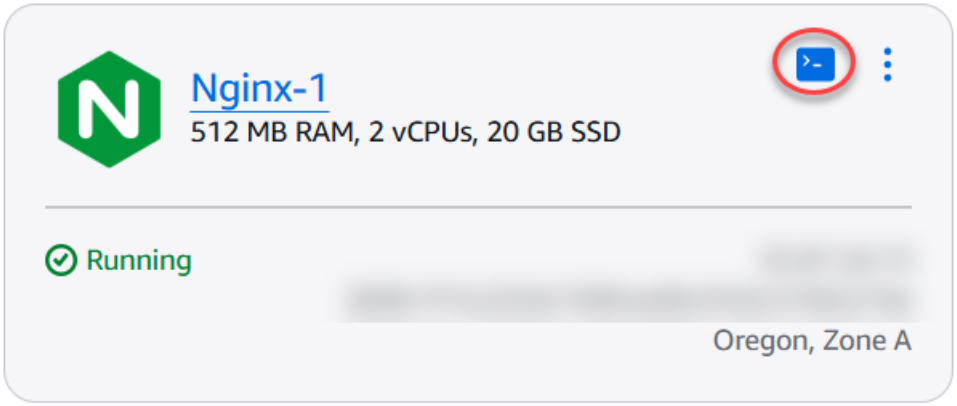
完成先决条件后，请继续执行本教程的下一部分。

第 2 步：在你的 Lightsail 实例上安装 Certbot

Certbot 是用于从 Let's Encrypt 请求证书并将其部署到 Web 服务器的客户端。Let's Encrypt 使用 ACME 协议颁发证书，而 Certbot 是与 Let's Encrypt 交互且启用 ACME 的客户端。

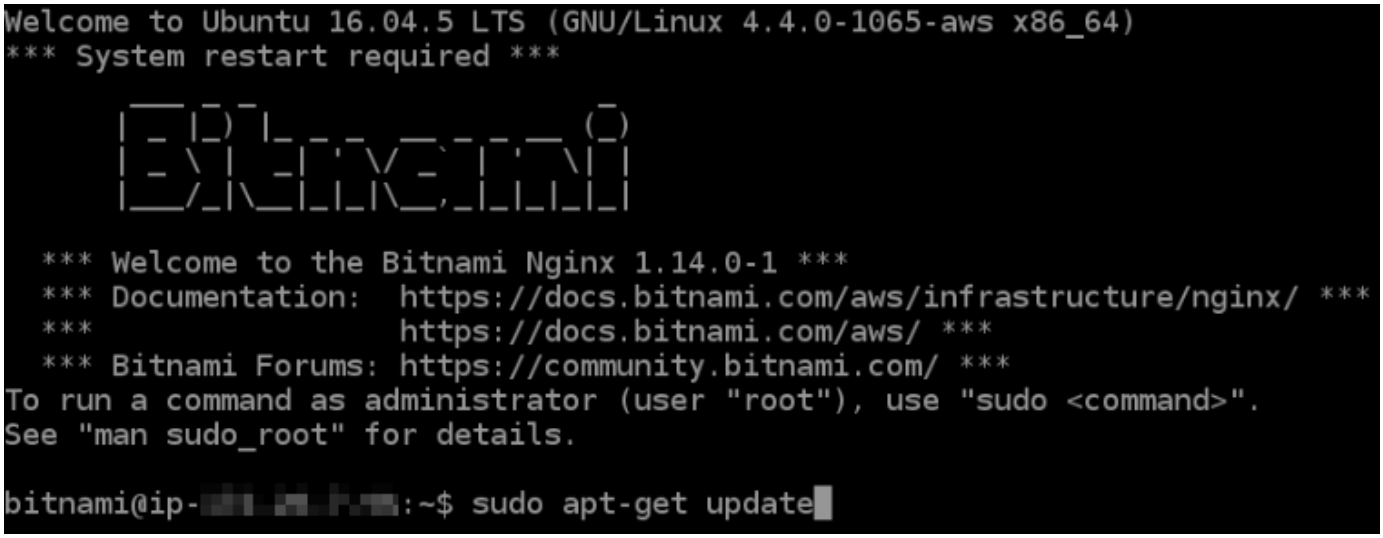
在你的 Lightsail 实例上安装 Certbot

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格，选择您想连接的实例的 SSH 快速连接图标。



3. 连接基于 Lightsail 浏览器的 SSH 会话后，输入以下命令以更新实例上的软件包：

```
sudo apt-get update
```



4. 输入以下命令以安装软件属性包。Certbot 的开发人员使用个人程序包存档 (PPA) 分配 Certbot。软件属性包提高了使用效率 PPAs。

```
sudo apt-get install software-properties-common
```

> **Note**
>
> 如果您在运行 `sudo apt-get install` 命令时遇到 `Could not get lock` 错误，请等待大约 15 分钟，然后重试。此错误可能是由 cron 作业导致的，该作业使用 Apt 包管理工具来安装无人参与升级。

5. 输入以下命令以将 Certbot 添加到本地 apt 存储库：

> **Note**
>
> 步骤 5 仅适用于使用 Ubuntu Linux 发行版的实例。如果您的实例使用 Debian Linux 发行版，请跳过此步骤。

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. 输入以下命令来更新 apt，以包含新的存储库：

```
sudo apt-get update -y
```

7. 输入以下命令以安装 Certbot：

```
sudo apt-get install certbot -y
```

Certbot 现已安装在你的 Lightsail 实例上。

8. 使基于浏览器的 SSH 终端窗口保持打开状态 - 您将在本教程的稍后部分返回到该窗口。继续执行本教程的下一部分。

步骤 3：请求 Let's Encrypt SSL 通配符证书

开始从 Let's Encrypt 请求证书的流程。使用 Certbot 请求通配符证书，您可以将单个证书同时用于某个域及其子域。例如，一个通配符证书可适用于 `example.com` 顶级域、`blog.example.com` 以及 `stuff.example.com` 子域。

请求 Let's Encrypt SSL 通配符证书

1. 在本教程的步骤 2 中使用的同一个基于浏览器的 SSH 终端窗口中，输入以下命令为您的域设置环境变量。现在，您可以更高效地复制和粘贴命令以获取证书。请务必将 *domain* 替换为您注册的域名。

```
DOMAIN=domain
```

```
WILDCARD=*.$DOMAIN
```

示例：

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. 输入以下命令以确认变量返回正确的值：

```
echo $DOMAIN && echo $WILDCARD
```

您应该会看到类似以下内容的结果：

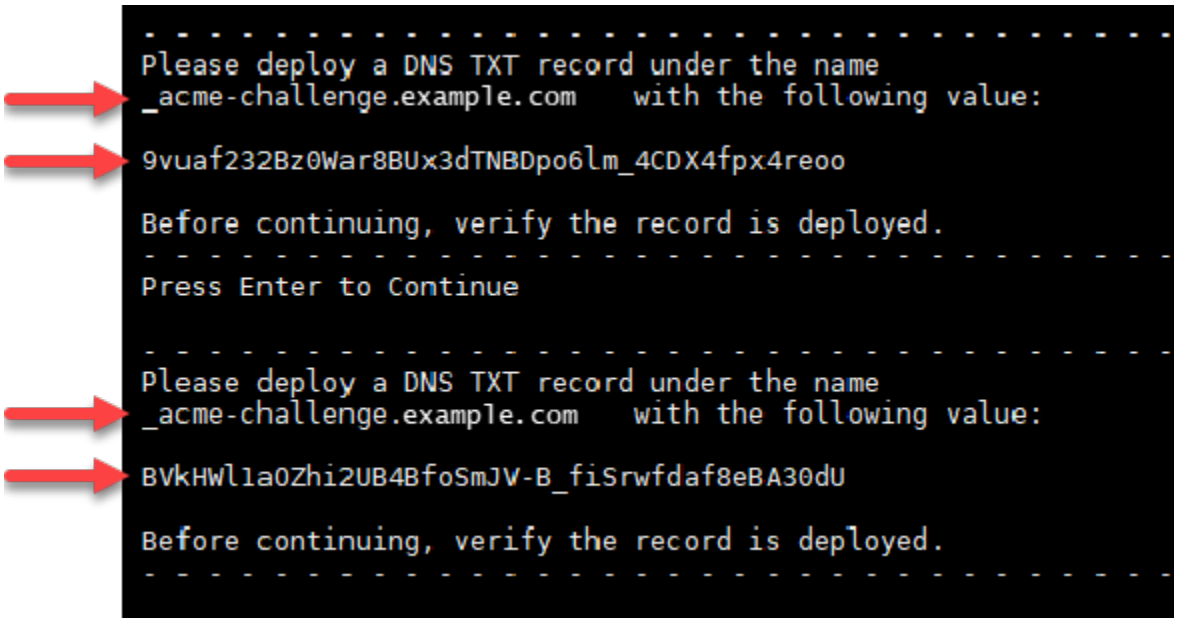


3. 输入以下命令以交互模式启动 Certbot。此命令指示 Certbot 使用具有 DNS 质询的手动授权方法验证域所有权。它可以为您的顶级域及其子域请求通配符证书。

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. 在系统提示时输入您的电子邮件地址，用于接收续订和安全通知。
5. 阅读 Let's Encrypt 服务条款。阅读完后，如果您同意该服务条款，请按 A。如果不同意，则无法获取 Let's Encrypt 证书。
6. 针对共享您电子邮件地址的提示以及有关您的 IP 地址已被记录的警告相应地做出响应。
7. Let's Encrypt 现在会提示您确认您拥有指定域。您可以通过将 TXT 记录添加到域的 DNS 记录执行此操作。系统会提供一组 TXT 记录值，如以下示例所示：

> **Note**
>
> Let's Encrypt 可以提供您必须用于验证的单个或多个 TXT 记录。在本示例中，向我们提供了两个 TXT 记录用于验证。



8. 保持基于 Lightsail 浏览器的 SSH 会话处于打开状态，本教程稍后将返回该会话。继续执行本教程的下一部分。

步骤 4：将 TXT 记录添加到域的 DNS 区域

将 TXT 记录添加到您的域的 DNS 区域中会验证您拥有该域。出于演示目的，我们使用 Lightsail DNS 区域。但是，该步骤可能类似于通常由域注册商托管的其他 DNS 区域。

> **Note**
>
> 要详细了解如何为您的域名创建 Lightsail DNS 区域，请参阅在 L ightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

在 Lightsail 中向你的域名的 DNS 区域添加 TXT 记录

1. 在左侧导航窗格中，选择域和 DNS。
2. 在页面的 DNS 区域部分下，选择您在 Certbot 证书请求中指定的域的 DNS 区域。
3. 在 DNS 区域编辑器中，选择 DNS records（DNS 记录）。
4. 选择添加记录。
5. 在 Record type（记录类型）下拉菜单中，选择 TXT record（TXT 记录）。
6. 将 Let's Encrypt 证书请求指定的值输入到 Record name（记录名称）和 Responds with（响应内容）字段中。

   > **Note**
   >
   > Lightsail 控制台会预先填充域的顶级域部分。例如，如果想要添加子域 *_acme-challenge.example.com*，您只需在文本框中输入 *_acme-challenge*，您保存此记录时 Lightsail 会添加 `.example.com` 部分。

7. 选择保存。
8. 重复执行第 4 至 7 步，以添加 Let's Encrypt 证书请求指定的另一组 TXT 记录。
9. 保持 Lightsail 控制台浏览器窗口处于打开状态，本教程稍后将返回该窗口。继续执行本教程的下一部分。

步骤 5：确认 TXT 记录已传播

使用该 MxToolbox 实用程序确认 TXT 记录已传播到互联网的 DNS。DNS 记录传播可能需要一段时间，具体取决于您的 DNS 托管提供商以及已为 DNS 记录配置的生存时间 (TTL)。请务必完成此步骤，并确认您的 TXT 记录已传播，然后再继续执行 Certbot 证书请求。否则，您的证书请求将失败。

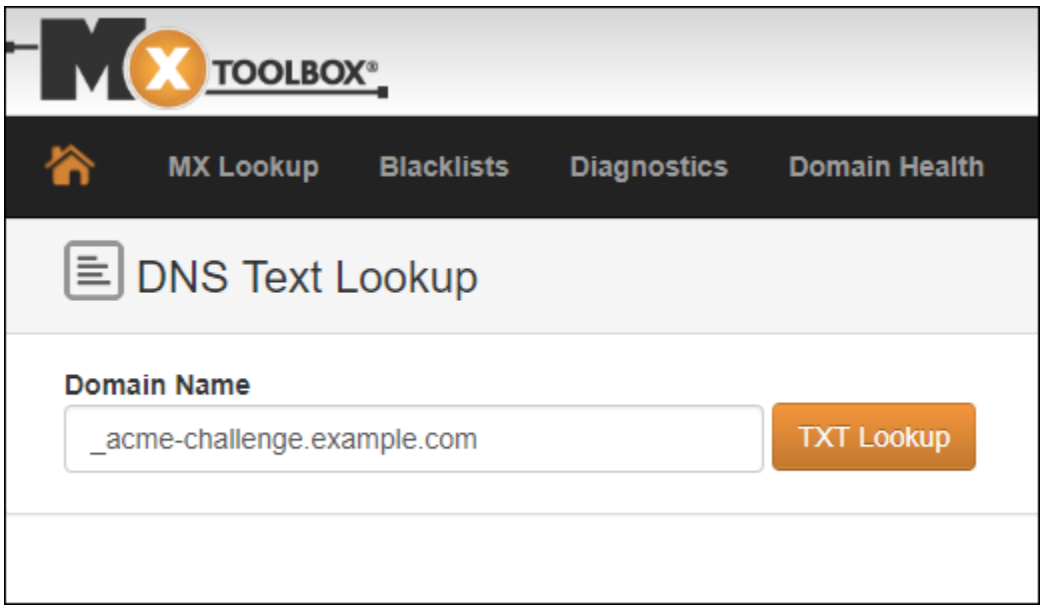
确认 TXT 记录已传播到 Internet 的 DNS

1. 打开一个新的浏览器窗口，然后转到 https://mxtoolbox.com/TXTLookup.aspx。
2. 在文本框中输入以下文本。请务必将 *domain* 替换为您的域。

   ```
   _acme-challenge.domain
   ```

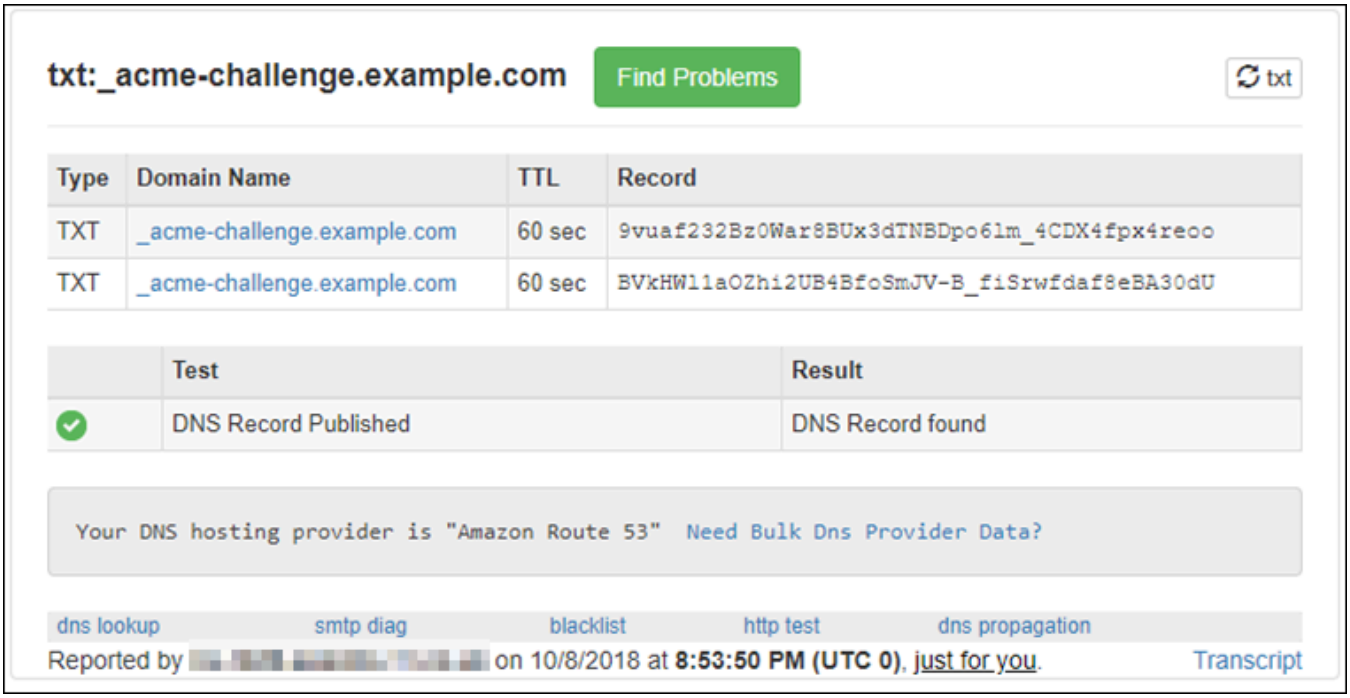
   示例：

   ```
   _acme-challenge.example.com
   ```

3. 选择 TXT Lookup (TXT 查找) 以运行检查。
4. 此时将出现以下任一响应：

   - 如果您的 TXT 记录已传播到 Internet 的 DNS，您将看到类似于以下屏幕截图中所示的响应。关闭浏览器窗口，然后继续执行本教程的下一部分。



- 如果您的 TXT 记录尚未传播到 Internet 的 DNS，您会看到 DNS Record not found (未找到 DNS 记录) 响应。确认您已将正确的 DNS 记录添加到域的 DNS 区域。如果您已添加正确的记录，请等待一段时间，让域的 DNS 记录传播，然后再次运行 TXT 查找。

步骤 6：完成 Let's Encrypt SSL 证书请求

返回 Nginx 实例的基于 Lightsail 浏览器的 SSH 会话，然后完成 Let's Encrypt 证书申请。Certbot 会将您的 SSL 证书、证书链和密钥文件保存在 Nginx 实例上的特定目录中。

完成 Let's Encrypt SSL 证书请求

1. 在你的 Nginx 实例的基于 Lightsail 浏览器的 SSH 会话中，按 Enter 继续你的 Let's Encrypt SSL 证书申请。如果成功，系统将显示类似于以下屏幕截图中的响应：

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.example.com   with the following value:

9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo

Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.example.com   with the following value:

BVkHWl1aOZhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU

Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/example.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/example.com/privkey.pem
   Your cert will expire on 2019-01-06. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le

bitnami@ip-172-26-1-148:/$
```

此消息可确认您的证书、证书链和密钥文件都存储在 /etc/letsencrypt/live/*domain*/ 目录中。请务必将 *domain* 替换为您的域，如 /etc/letsencrypt/live/*example.com*/。

2. 记录消息中指定的到期日期。您可以在该日期之前续订证书。

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/example.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/example.com/privkey.pem
   Your cert will expire on 2019-01-06. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

3. 您现在已拥有 Let's Encrypt SSL 证书，请继续执行本教程的下一部分。

步骤 7：创建指向 Nginx 服务器目录中的 Let's Encrypt 证书文件的链接

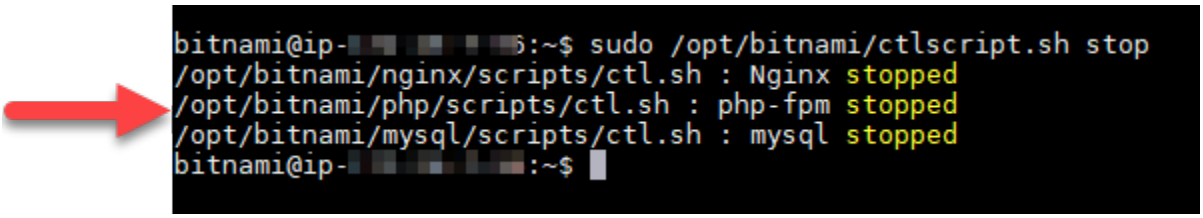
创建指向 Nginx 实例上 Nginx 服务器中的 Let's Encrypt SSL 证书文件的链接。此外，请备份现有证书，以便之后需要。

创建指向 Nginx 服务器目录中的 Let's Encrypt 证书文件的链接

1. 在 Nginx 实例的基于 Lightsail 浏览器的 SSH 会话中，输入以下命令以停止底层服务：

```
sudo /opt/bitnami/ctlscript.sh stop
```

您可以看到类似以下内容的响应：



2. 输入以下命令，为您所在域设置环境变量。您可以更高效地复制和粘贴命令来链接证书文件。请务必将 *domain* 替换为您注册的域名。

```
DOMAIN=domain
```

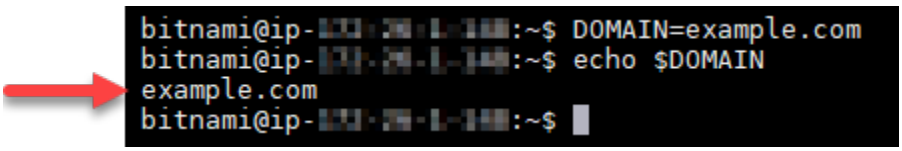
示例：

```
DOMAIN=example.com
```

3. 输入以下命令以确认变量返回正确的值：

```
echo $DOMAIN
```

您应该会看到类似以下内容的结果：



4. 分别输入以下命令，以重命名您的现有证书文件作为备份。请参阅本教程开头的重要提示，了解有关不同发行版和文件结构的信息。

   - 对于 Debian Linux发行版

     方法 A（使用系统包安装 Bitnami）：

     ```
     sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.crt /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.key /opt/bitnami/nginx/conf/
     bitnami/certs/server.key.old
     ```

     方法 B（自包含 Bitnami 安装）：

     ```
     sudo mv /opt/bitnami/nginx/conf/server.crt /opt/bitnami/nginx/conf/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/nginx/conf/server.key /opt/bitnami/nginx/conf/server.key.old
     ```

   - 对于使用 Ubuntu Linux 发行版的较旧实例：

     ```
     sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.crt /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.key /opt/bitnami/nginx/conf/
     bitnami/certs/server.key.old
     ```

5. 分别输入以下命令，以创建指向 Nginx 服务器目录中的 Let's Encrypt 证书文件的链接。请参阅本教程开头的重要提示，了解有关不同发行版和文件结构的信息。

   - 对于 Debian Linux发行版

     方法 A（使用系统包安装 Bitnami）：

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.key
     ```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
bitnami/certs/server.crt
```

方法 B（自包含 Bitnami 安装）：

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
server.crt
```

- 对于使用 Ubuntu Linux 发行版的较旧实例：

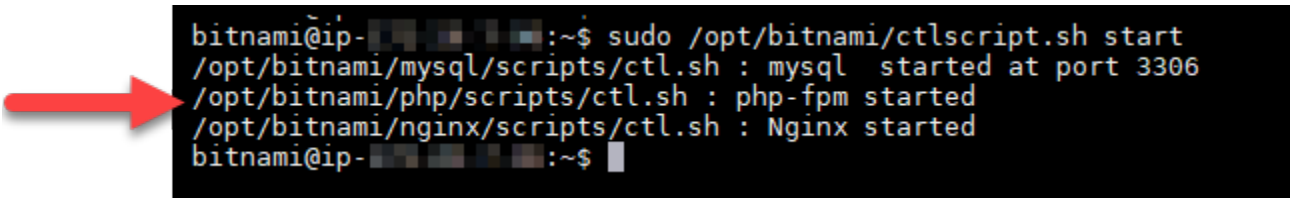
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
bitnami/certs/server.key
```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
bitnami/certs/server.crt
```

6. 输入以下命令，以启动先前停止运行的基础服务：

```
sudo /opt/bitnami/ctlscript.sh start
```

您应该会看到类似以下内容的结果：



您的 Nginx 实例现已配置为使用 SSL 加密。但是，流量不会自动从 HTTP 重新导向到 HTTPS。

7. 继续执行本教程的下一部分。

步骤 8：为 Web 应用程序配置 HTTP 到 HTTPS 重新导向

您可以为 Nginx 实例配置 HTTP 到 HTTPS 重新导向。自动从 HTTP 重新导向到 HTTPS 将使您的站点只能由使用 SSL 的客户访问，即使他们使用 HTTP 进行连接也是如此。请参阅本教程开头的重要提示，了解有关不同发行版和文件结构的信息。

本教程使用 Vim 来进行演示；但是，您可以使用您选择的任何文本编辑器。

对于 Debian Linux 发行版，为 Web 应用程序配置 HTTP 到 HTTPS 的重定向

1. 在 Nginx 实例的基于 Lightsail 浏览器的 SSH 会话中，输入以下命令来修改服务器块配置文件。将 <ApplicationName> 替换为您的应用程序的名称。

   ```
   sudo vim /opt/bitnami/nginx/conf/server_blocks/<ApplicationName>-server-block.conf
   ```

2. 按 i 键进入 Vim 编辑器的插入模式。
3. 使用以下示例中的信息编辑该文件：

   ```
   server {
       listen 80 default_server;
       root /opt/bitnami/APPNAME;
       return 301 https://$host$request_uri;
   }
   ```

4. 按 ESC 键，然后输入 :wq 以写入（保存）您的编辑内容，然后退出 Vim。
5. 输入以下命令，修改 Nginx 配置文件的服务器部分：

   ```
   sudo vim /opt/bitnami/nginx/conf/nginx.conf
   ```

6. 按 i 键进入 Vim 编辑器的插入模式。
7. 使用以下示例中的信息编辑该文件：

   ```
   server {
         listen 80;
         server_name localhost;
         return 301 https://$host$request_uri;
     }
   ```

8. 按 ESC 键，然后输入 :wq 以写入（保存）您的编辑内容，然后退出 Vim。
9. 输入以下命令重新启动基础服务，以使编辑内容生效：

```
sudo /opt/bitnami/ctlscript.sh restart
```

方法 B（自包含 Bitnami 安装）：

1. 在 Nginx 实例的基于 Lightsail 浏览器的 SSH 会话中，输入以下命令以修改 Nginx 配置文件的服务器部分：

   ```
   sudo vim /opt/bitnami/nginx/conf/nginx.conf
   ```

2. 按 `i` 键进入 Vim 编辑器的插入模式。
3. 使用以下示例中的信息编辑该文件：

   ```
   server {
         listen 80;
         server_name localhost;
         return 301 https://$host$request_uri;
     }
   ```

4. 按 ESC 键，然后输入 `:wq` 以写入（保存）您的编辑内容，然后退出 Vim。
5. 输入以下命令重新启动基础服务，以使编辑内容生效：

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

对于使用 Ubuntu Linux 发行版的较旧实例，为 Web 应用程序配置 HTTP 到 HTTPS 的重定向

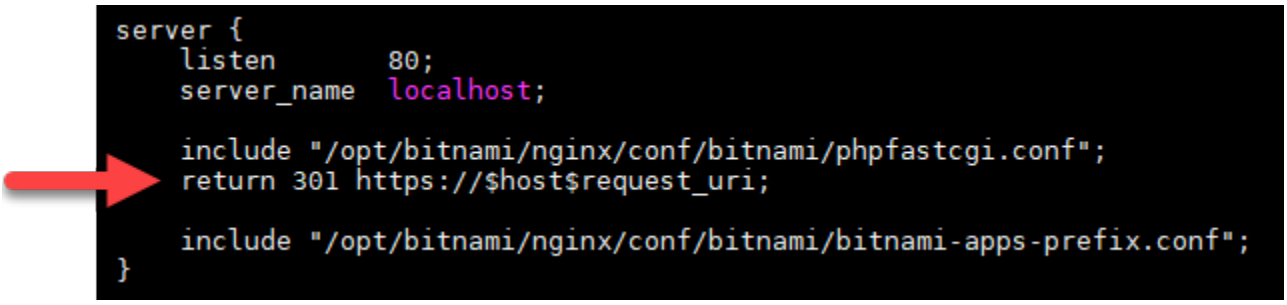
1. 在 Nginx 实例的基于 Lightsail 浏览器的 SSH 会话中，输入以下命令，使用 Vim 文本编辑器编辑 Nginx Web 服务器配置文件：

   ```
   sudo vim /opt/bitnami/nginx/conf/bitnami/bitnami.conf
   ```

2. 按 `i` 键进入 Vim 编辑器的插入模式。
3. 在文件中，在 `server_name localhost;` 和 `include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";` 之间输入以下文本：

   ```
   return 301 https://$host$request_uri;
   ```

结果应该类似以下内容：



4. 按 ESC 键，然后输入 :wq 以写入（保存）您的编辑内容，然后退出 Vim。
5. 输入以下命令重新启动基础服务，以使编辑内容生效：

```
sudo /opt/bitnami/ctlscript.sh restart
```

您的 Nginx 实例现已配置为自动将连接从 HTTP 重新导向到 HTTPS。当访问者访问 `http://www.example.com` 时，系统会自动将其重新导向至已加密的 `https://www.example.com` 地址。

步骤 9：每 90 天续订一次 Let's Encrypt 证书

Let's Encrypt 证书的有效期为 90 天。证书可以在到期前 30 天续订。要续订 Let's Encrypt 证书，请运行用于获取它们的原始命令。重复本教程的请求 Let's Encrypt SSL 通配符证书部分中的步骤。

使用免费的 “让我们加密 SSL” 证书保护你的 Lightsail WordPress 实例

> **Tip**
>
> Amazon Lightsail 提供了一个指导式工作流程，可在您的实例上自动安装和配置 Let's Encrypt 证书。 WordPress 我们强烈建议使用该工作流程，而不是按照本教程中的手动步骤操作。有关更多信息，请参阅启动和配置实 WordPress 例。

Lightsail 可以使用 Lightsail 负载均衡器轻松使用 SSL/TLS 保护你的网站和应用程序。但是，使用 Lightsail 负载均衡器通常可能不是正确的选择。您的站点可能不需要负载均衡器提供的可扩展性或容错能力，或者您可能针对成本进行了优化。在后一种情况下，您可能会考虑使用 Let's Encrypt 获取免费 SSL 证书。如果是这样，一切都没有问题。您可以将这些证书与 Lightsail 实例集成。

通过本指南，您将学习如何使用 Certbot 申请 Let's Encrypt 通配符证书，并使用 Really Simple SSL 插件将其与您的 WordPress 实例集成。

- 2020 年 7 月，Bitnami 实例使用的 Linux 发行版从 Ubuntu 更改为 Debian。由于此更改，本教程中的某些步骤将因实例的 Linux 发行版而异。在更改后创建的所有 Bitnami 蓝图实例都将使用 Debian Linux 发行版。在更改之前创建的实例将继续使用 Ubuntu Linux 发行版。要检查实例的发行版，请运行 `uname -a` 命令。响应会将 Ubuntu 或 Debian 显示为实例的 Linux 发行版。
- Bitnami 已修改许多堆栈的文件结构。本教程中的文件路径可能会发生变化，具体取决于您的 Bitnami 堆栈是使用本地 Linux 系统包（方法 A），还是自包含安装（方法 B）。要确定 Bitnami 安装类型以及要遵循的方法，请运行以下命令：

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
  ```

内容

- 开始使用之前
- 步骤 1：完成先决条件
- 第 2 步：在你的 Lightsail 实例上安装 Certbot
- 步骤 3：请求 Let's Encrypt SSL 通配符证书
- 步骤 4：将 TXT 记录添加到域的 DNS 区域
- 步骤 5：确认 TXT 记录已传播
- 步骤 6：完成 Let's Encrypt SSL 证书请求
- 步骤 7：创建指向 Apache 服务器目录中的 Let's Encrypt 证书文件的链接
- 第 8 步：使用非常简单的 SSL 插件将 SSL 证书与您的 WordPress 网站集成
- 步骤 9：每 90 天续订一次 Let's Encrypt 证书

开始使用之前

在开始使用本教程之前，您应该注意以下事项：

改为使用 Bitnami HTTPS 配置（**`bncert`**）工具

本教程中概述的步骤演示了如何使用手动过程实施 SSL/TLS 证书。但是，Bitnami 提供了一个更加自动化的流程，它使用 Bitnami HTTPS 配置 (`bncert`) 工具，该工具通常预先安装在 Lightsail 的实例上。 WordPress我们强烈建议使用该工具，而不是按照本教程中的手动步骤操作。本教程是在

bncert 工具推出之前编写的。有关使用该bncert工具的更多信息，请参阅在 Amazon Lightsail 中为您的 WordPress实例启用 HTTPS。

确定您的 WordPress实例的 Linux 发行版

2020 年 7 月，Bitnami 实例使用的 Linux 发行版从 Ubuntu 更改为 Debian。在更改后创建的所有 Bitnami 蓝图实例都将使用 Debian Linux 发行版。在更改之前创建的实例将继续使用 Ubuntu Linux 发行版。由于此更改，本教程中的某些步骤将因实例的 Linux 发行版而异。您必须确定实例的 Linux 发行版，以便了解要使用本教程中的哪些步骤。要检查实例使用的 Linux 发行版，请运行 `uname -a` 命令。响应会将 Ubuntu 或 Debian 显示为实例的 Linux 发行版。

确定适合实例的教程方法

Bitnami 正在修改许多堆栈的文件结构。本教程中的文件路径可能会发生变化，具体取决于您的 Bitnami 堆栈是使用本地 Linux 系统包（方法 A），还是自包含安装（方法 B）。要确定 Bitnami 安装类型以及要遵循的方法，请运行以下命令：

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
```

步骤 1：完成先决条件

请完成以下先决条件（如果尚未完成）：

- 在 Lightsail 中创建一个 WordPress 实例。要了解更多信息，请参阅创建实例。
- 注册一个域名，并获取管理访问权限以编辑其 DNS 记录。要了解更多信息，请参阅 DNS。

  我们建议您使用 Lightsail DNS 区域来管理域名的 DNS 记录。要了解更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。
- 在 Lightsail 控制台中使用基于浏览器的 SSH 终端来执行本教程中的步骤。但是，您也可以使用自己的 SSH 客户端（如 PuTTY）。要了解有关配置 PuTTY 的更多信息，请参阅在 Amazon Lightsail 中下载并设置 PuTTY 以使用 SSH 进行连接。

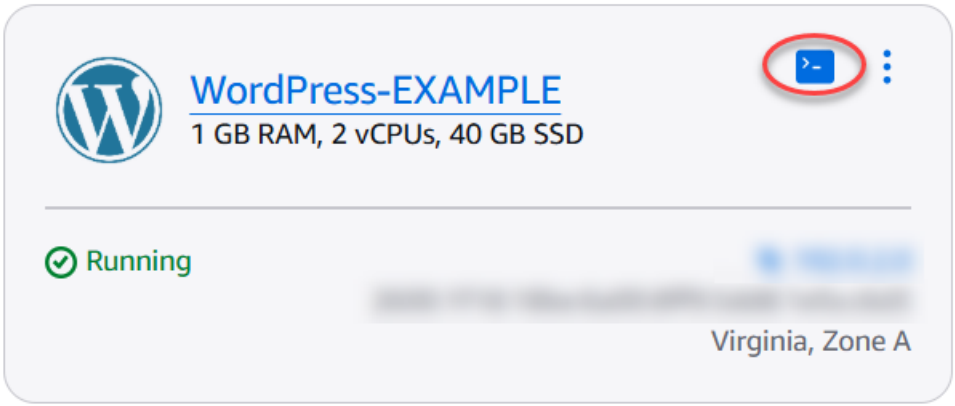
完成先决条件后，请继续执行本教程的下一部分。

第 2 步：在你的 Lightsail 实例上安装 Certbot

Certbot 是用于从 Let's Encrypt 请求证书并将其部署到 Web 服务器的客户端。Let's Encrypt 使用 ACME 协议颁发证书，而 Certbot 是与 Let's Encrypt 交互且启用 ACME 的客户端。

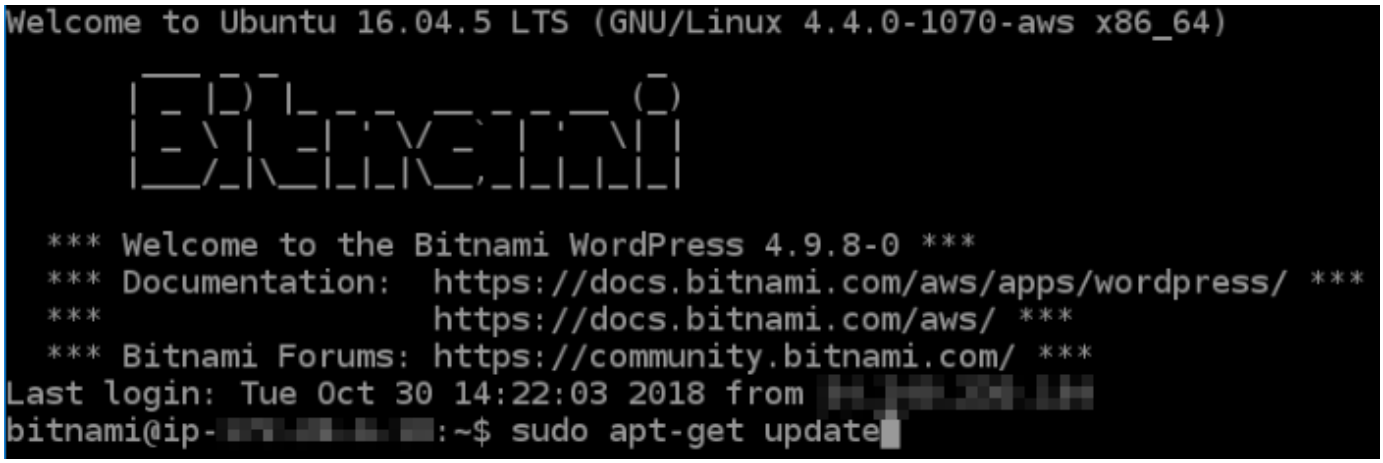
在你的 Lightsail 实例上安装 Certbot

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格，选择您想连接的实例的 SSH 快速连接图标。



3. 连接基于 Lightsail 浏览器的 SSH 会话后，输入以下命令以更新实例上的软件包：

```
sudo apt-get update
```



4. 输入以下命令以安装软件属性包。Certbot 的开发人员使用个人程序包存档 (PPA) 分配 Certbot。软件属性包使其使用起来更加高效 PPAs。

```
sudo apt-get install software-properties-common
```

> **Note**
>
> 如果您在运行 `sudo apt-get install` 命令时遇到 `Could not get lock` 错误，请等待大约 15 分钟，然后重试。此错误可能是由 cron 作业导致的，该作业使用 Apt 包管理工具来安装无人参与升级。

5. 输入以下命令以安装 GPG 软件包，然后将 Certbot 添加到本地 apt 存储库：

> **Note**
>
> 步骤 5 仅适用于使用 Ubuntu Linux 发行版的实例。如果您的实例使用 Debian Linux 发行版，请跳过此步骤。

```
sudo apt-get install gpg -y
```

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. 输入以下命令来更新 apt，以包含新的存储库：

```
sudo apt-get update -y
```

7. 输入以下命令以安装 Certbot：

```
sudo apt-get install certbot -y
```

Certbot 现已安装在你的 Lightsail 实例上。

8. 使基于浏览器的 SSH 终端窗口保持打开状态 - 您将在本教程的稍后部分返回到该窗口。继续执行本教程的下一部分。

步骤 3：请求 Let's Encrypt SSL 通配符证书

开始从 Let's Encrypt 请求证书的流程。使用 Certbot 请求通配符证书，您可以将单个证书同时用于某个域及其子域。例如，一个通配符证书可适用于 `example.com` 顶级域、`blog.example.com` 以及 `stuff.example.com` 子域。

请求 Let's Encrypt SSL 通配符证书

1. 在本教程的步骤 2 中使用的同一个基于浏览器的 SSH 终端窗口中，输入以下命令为您的域设置环境变量。现在，您可以更高效地复制和粘贴命令以获取证书。请务必将 *domain* 替换为您注册的域名。

```
DOMAIN=domain
```

```
WILDCARD=*.$DOMAIN
```

示例：

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. 输入以下命令以确认变量返回正确的值：

```
echo $DOMAIN && echo $WILDCARD
```

您应该会看到类似以下内容的结果：



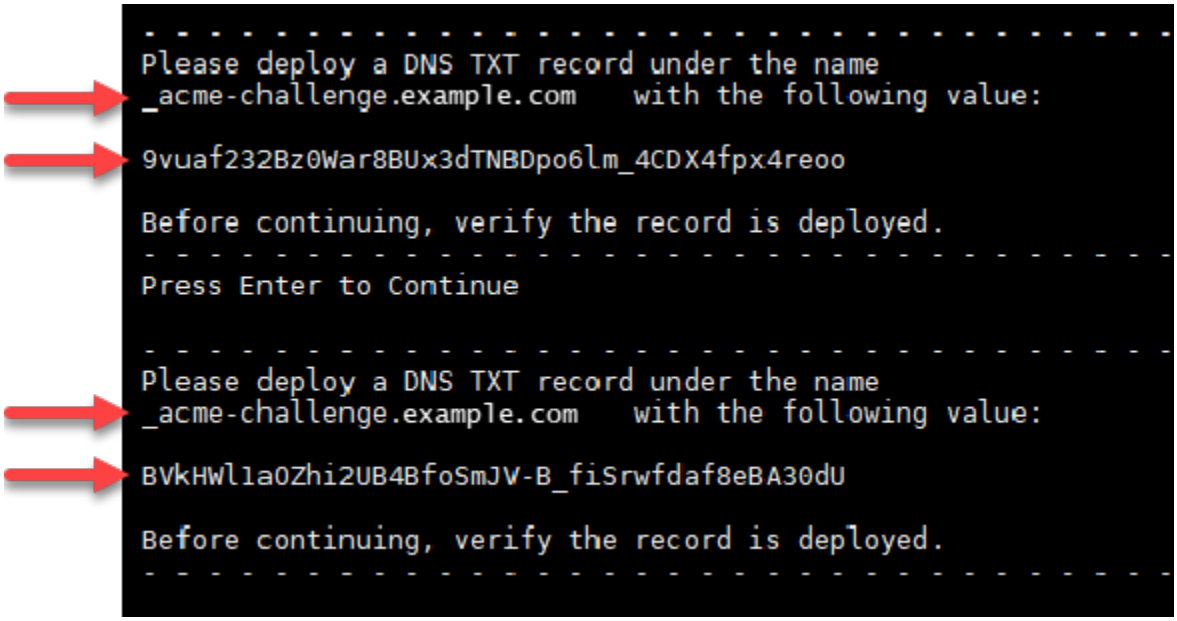
3. 输入以下命令以交互模式启动 Certbot。此命令指示 Certbot 使用具有 DNS 质询的手动授权方法验证域所有权。它可以为您的顶级域及其子域请求通配符证书。

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. 在系统提示时输入您的电子邮件地址，用于接收续订和安全通知。
5. 阅读 Let's Encrypt 服务条款。阅读完后，如果您同意该服务条款，请按 A。如果不同意，则无法获取 Let's Encrypt 证书。
6. 针对共享您电子邮件地址的提示以及有关您的 IP 地址已被记录的警告相应地做出响应。

7. Let's Encrypt 现在会提示您确认您拥有指定域。您可以通过将 TXT 记录添加到域的 DNS 记录执行此操作。系统会提供一组 TXT 记录值，如以下示例所示：

> **Note**
>
> Let's Encrypt 可以提供您必须用于验证的单个或多个 TXT 记录。在本示例中，向我们提供了两个 TXT 记录用于验证。



8. 保持基于 Lightsail 浏览器的 SSH 会话处于打开状态，本教程稍后将返回该会话。继续执行本教程的下一部分。

步骤 4：将 TXT 记录添加到域的 DNS 区域

将 TXT 记录添加到您的域的 DNS 区域中会验证您拥有该域。出于演示目的，我们使用 Lightsail DNS 区域。但是，该步骤可能类似于通常由域注册商托管的其他 DNS 区域。

> **Note**
>
> 要详细了解如何为您的域名创建 Lightsail DNS 区域，请参阅在 L ightsail 中创建 DNS 区域来管理您的域名的 DNS 记录。

在 Lightsail 中向你的域名的 DNS 区域添加 TXT 记录

1. 在左侧导航窗格中，选择域和 DNS。
2. 在页面的 DNS 区域部分下，选择您在 Certbot 证书请求中指定的域的 DNS 区域。
3. 在 DNS 区域编辑器中，选择 DNS records（DNS 记录）。
4. 选择添加记录。
5. 在 Record type（记录类型）下拉菜单中，选择 TXT record（TXT 记录）。
6. 将 Let's Encrypt 证书请求指定的值输入到 Record name（记录名称）和 Responds with（响应内容）字段中。

   > **Note**
   >
   > Lightsail 控制台会预先填充域的顶级域部分。例如，如果想要添加子域 *_acme-challenge.example.com*，您只需在文本框中输入 *_acme-challenge*，您保存此记录时 Lightsail 会添加 `.example.com` 部分。

7. 选择保存。
8. 重复执行第 4 至 7 步，以添加 Let's Encrypt 证书请求指定的另一组 TXT 记录。
9. 保持 Lightsail 控制台浏览器窗口处于打开状态，本教程稍后将返回该窗口。继续执行本教程的下一部分。

步骤 5：确认 TXT 记录已传播

使用该 MxToolbox 实用程序确认 TXT 记录已传播到互联网的 DNS。DNS 记录传播可能需要一段时间，具体取决于您的 DNS 托管提供商以及已为 DNS 记录配置的生存时间 (TTL)。请务必完成此步骤，并确认您的 TXT 记录已传播，然后再继续执行 Certbot 证书请求。否则，您的证书请求将失败。

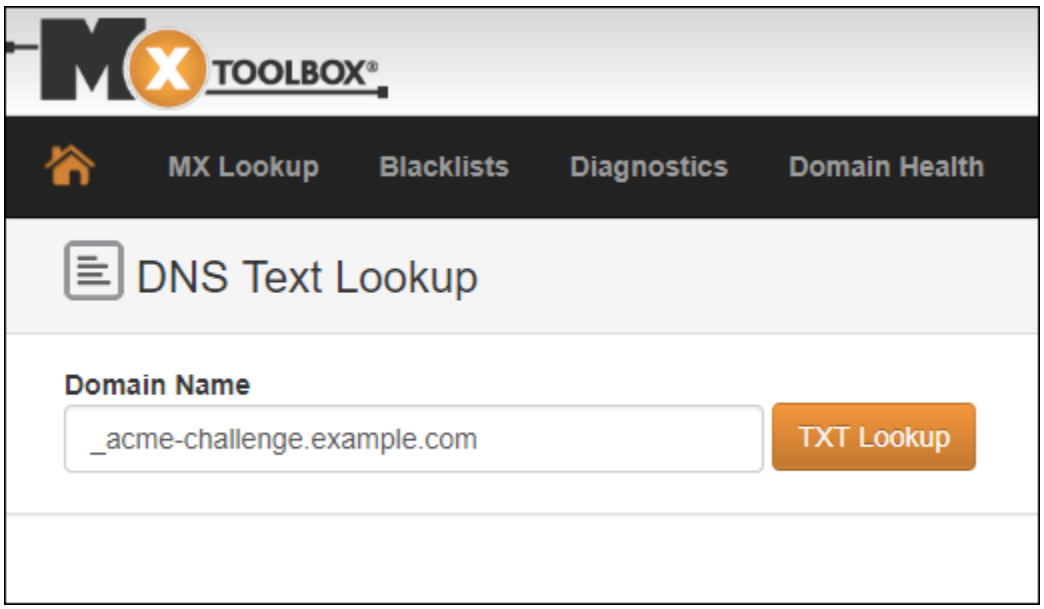
确认 TXT 记录已传播到 Internet 的 DNS

1. 打开一个新的浏览器窗口，然后转到 https://mxtoolbox.com/TXTLookup.aspx。
2. 在文本框中输入以下文本。请务必将 *domain* 替换为您的域。

   ```
   _acme-challenge.domain
   ```

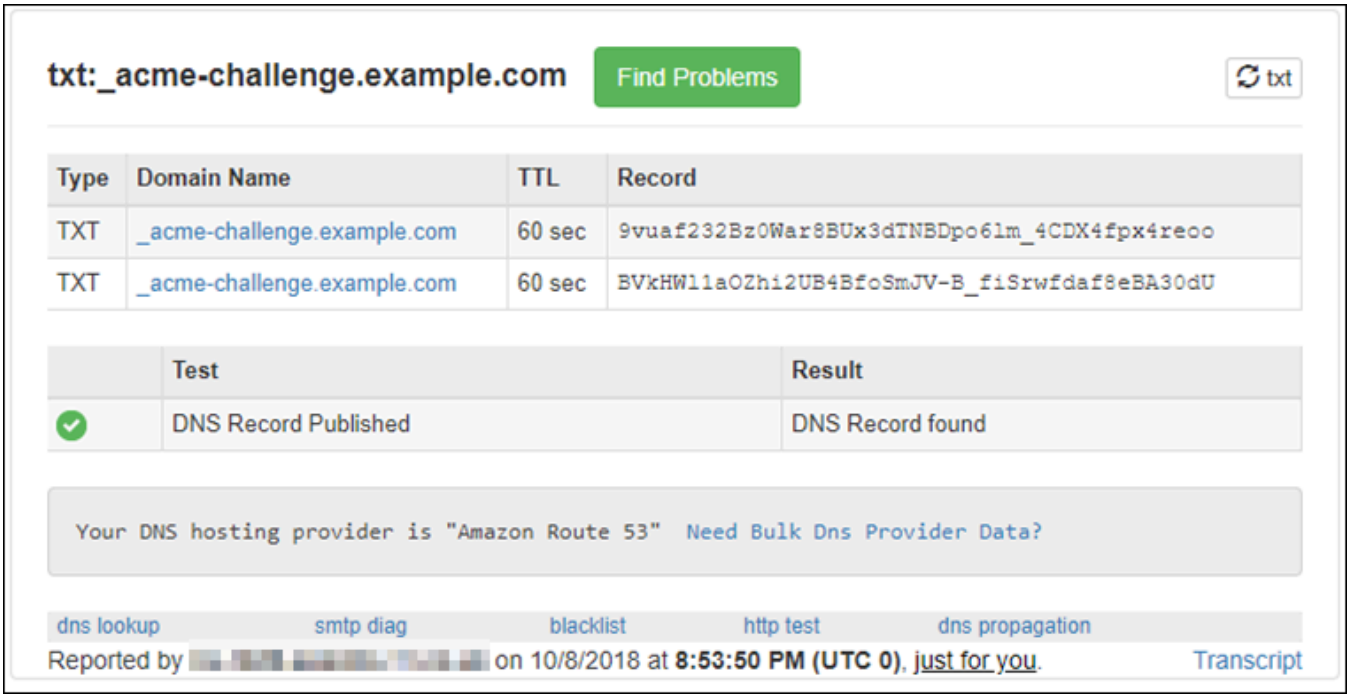
   示例：

```
_acme-challenge.example.com
```



3. 选择 TXT Lookup (TXT 查找) 以运行检查。
4. 此时将出现以下任一响应：

   - 如果您的 TXT 记录已传播到 Internet 的 DNS，您将看到类似于以下屏幕截图中所示的响应。关闭浏览器窗口，然后继续执行本教程的下一部分。



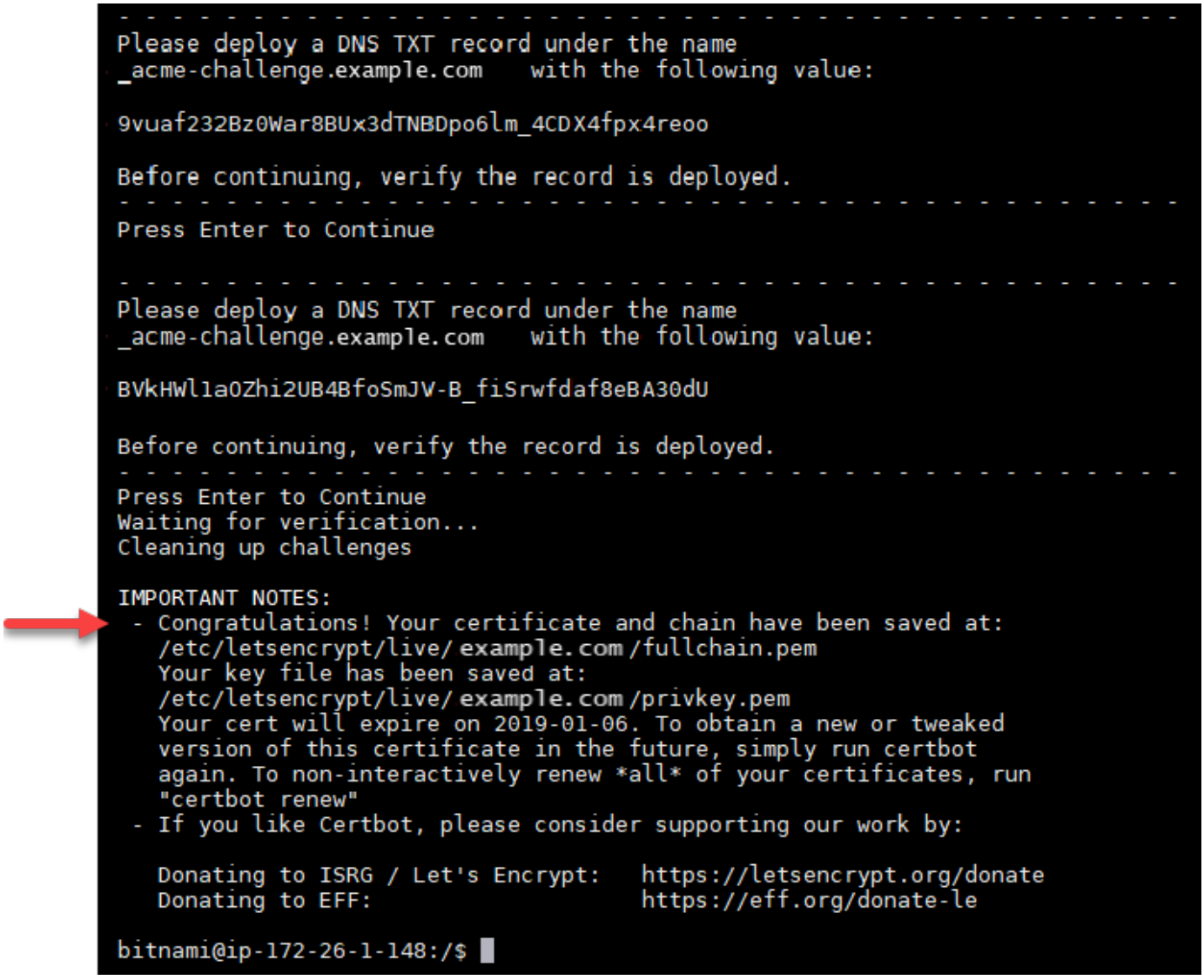
- 如果您的 TXT 记录尚未传播到 Internet 的 DNS，您会看到 DNS Record not found (未找到 DNS 记录) 响应。确认您已将正确的 DNS 记录添加到域的 DNS 区域。如果您已添加正确的记录，请等待一段时间，让域的 DNS 记录传播，然后再次运行 TXT 查找。

步骤 6：完成 Let's Encrypt SSL 证书请求

返回您的 WordPress 实例的基于 Lightsail 浏览器的 SSH 会话，然后完成 Let's Encrypt 证书申请。Certbot 会将您的 SSL 证书、链和密钥文件保存到实例上的特定目录中。 WordPress

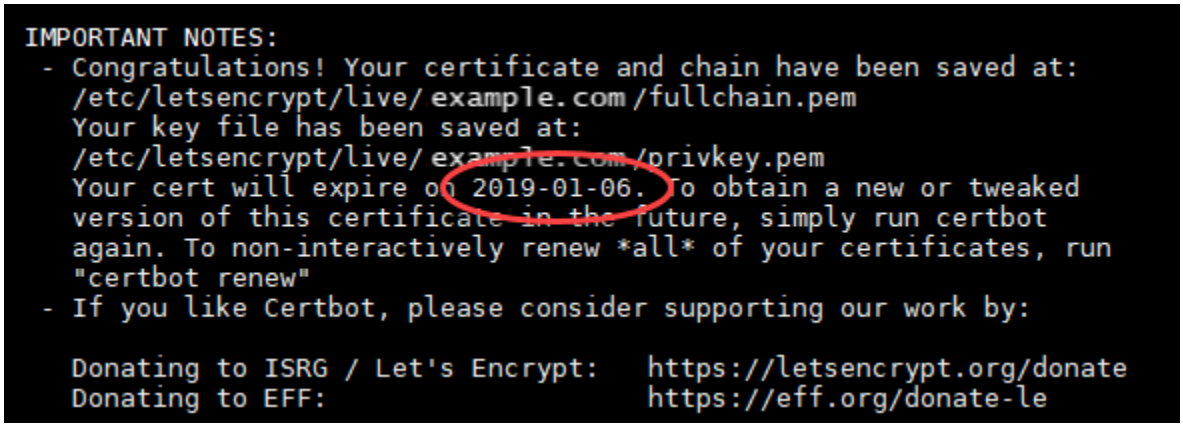
完成 Let's Encrypt SSL 证书请求

1. 在您的 WordPress 实例的基于 Lightsail 浏览器的 SSH 会话中，按 Enter 继续您的 Let's Encrypt SSL 证书申请。如果成功，系统将显示类似于以下屏幕截图中的响应：



此消息可确认您的证书、证书链和密钥文件都存储在 /etc/letsencrypt/live/*domain*/ 目录中。请务必将 *domain* 替换为您的域，如 /etc/letsencrypt/live/*example.com*/。

2. 记录消息中指定的到期日期。您可以在该日期之前续订证书。



3. 您现在已拥有 Let's Encrypt SSL 证书，请继续执行本教程的下一部分。

步骤 7：创建指向 Apache 服务器目录中的 Let's Encrypt 证书文件的链接

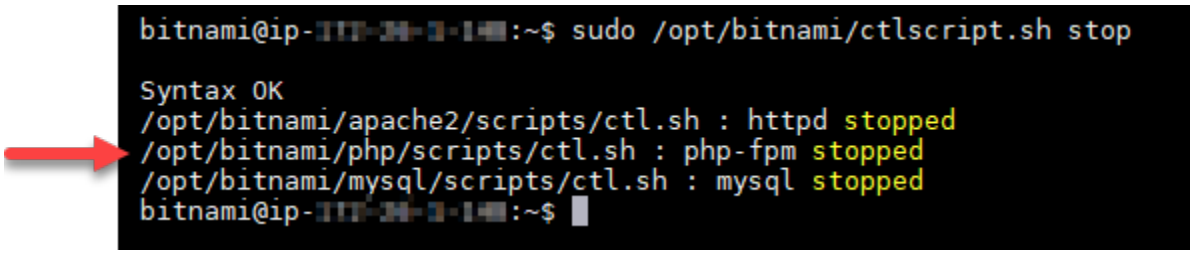
在您的 WordPress 实例上的 Apache 服务器目录中创建指向让我们加密 SSL 证书文件的链接。此外，请备份现有证书，以便之后需要。

创建指向 Apache 服务器目录中的 Let's Encrypt 证书文件的链接

1. 在您的 WordPress 实例的基于 Lightsail 浏览器的 SSH 会话中，输入以下命令以停止底层服务：

```
sudo /opt/bitnami/ctlscript.sh stop
```

您可以看到类似以下内容的响应：



2. 输入以下命令，为您所在域设置环境变量。您可以更高效地复制和粘贴命令来链接证书文件。请务必将 *domain* 替换为您注册的域名。

```
DOMAIN=domain
```

示例：

```
DOMAIN=example.com
```

3. 输入以下命令以确认变量返回正确的值：

```
echo $DOMAIN
```

您应该会看到类似以下内容的结果：



4. 分别输入以下命令，以重命名您的现有证书文件作为备份。请参阅本教程开头的重要提示，了解有关不同发行版和文件结构的信息。

   - 对于 Debian Linux发行版

     方法 A（使用系统包安装 Bitnami）：

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.crt /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.key /opt/bitnami/apache2/
     conf/bitnami/certs/server.key.old
     ```

     方法 B（自包含 Bitnami 安装）：

     ```
     sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/
     server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/
     server.key.old
     ```

   - 对于使用 Ubuntu Linux 发行版的较旧实例：

     ```
     sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.crt /opt/bitnami/apache/
     conf/bitnami/certs/server.crt.old
     ```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.key /opt/bitnami/apache/
conf/bitnami/certs/server.key.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.csr /opt/bitnami/apache/
conf/bitnami/certs/server.csr.old
```

5. 分别输入以下命令，以创建指向 Apache 目录中的 Let's Encrypt 证书文件的链接。请参阅本教程开头的重要提示，了解有关不同发行版和文件结构的信息。

   - 对于 Debian Linux发行版

     方法 A（使用系统包安装 Bitnami）：

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt
     ```

     方法 B（自包含 Bitnami 安装）：

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/server.crt
     ```

   - 对于使用 Ubuntu Linux 发行版的较旧实例：

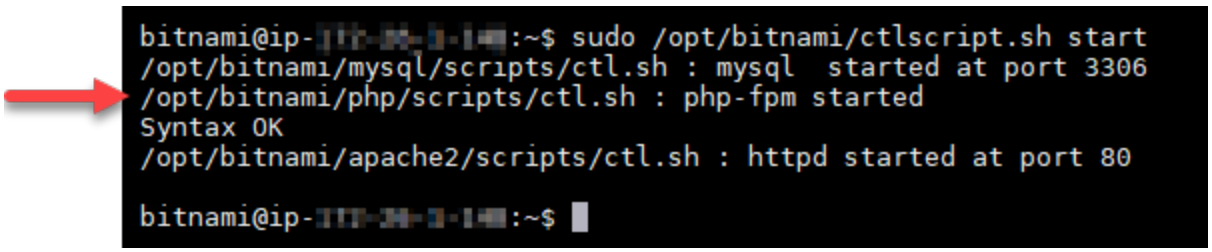
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.crt
     ```

6. 输入以下命令以启动之前停止运行的基础服务：

```
sudo /opt/bitnami/ctlscript.sh start
```

您应该会看到类似以下内容的结果：



您的 WordPress 实例的 SSL 证书文件现在位于正确的目录中。

7. 继续执行本教程的下一部分。

第 8 步：使用非常简单的 SSL 插件将 SSL 证书与您的 WordPress 网站集成

将 Really Simple SSL 插件安装到您的 WordPress 站点，然后使用它来集成 SSL 证书。Really Simple SSL 还会配置 HTTP 到 HTTPS 重新导向，从而确保访问您站点的用户始终使用 HTTPS 连接。

使用 “非常简单 SSL 插件” 将 SSL 证书与您的 WordPress 网站集成

1. 在您的 WordPress 实例的基于 Lightsail 浏览器的 SSH 会话中，输入以下命令将`wp-config.php`和`htaccess.conf`文件设置为可写入。Really Simple SSL 插件将写入 wp-config.php 文件以配置您的证书。

   - 对于使用 Debian Linux 发行版的较新实例：

     ```
     sudo chmod 666 /opt/bitnami/wordpress/wp-config.php && sudo chmod 666 /opt/
     bitnami/apache/conf/vhosts/htaccess/wordpress-htaccess.conf
     ```

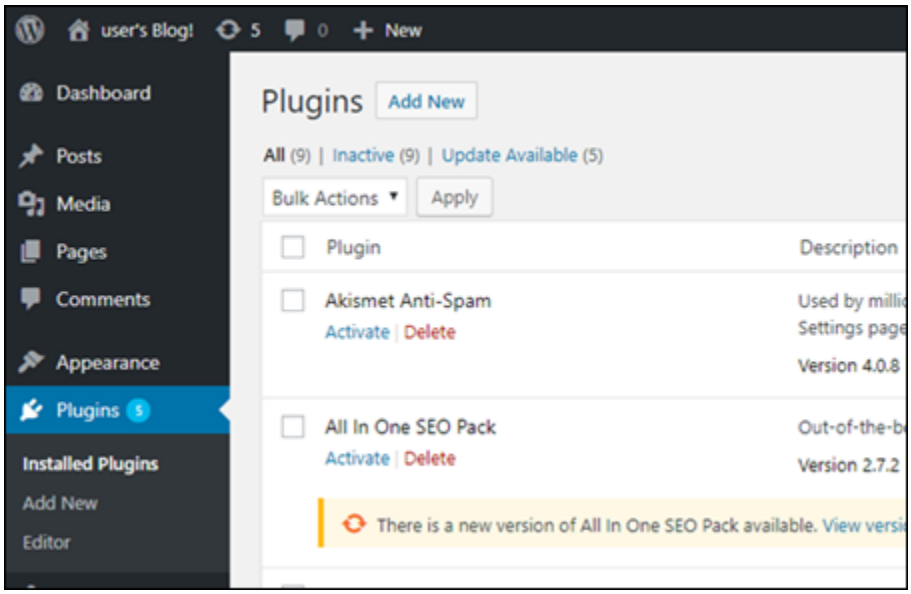
   - 对于使用 Ubuntu Linux 发行版的较旧实例：

     ```
     sudo chmod 666 /opt/bitnami/apps/wordpress/htdocs/wp-config.php && sudo chmod
      666 /opt/bitnami/apps/wordpress/conf/htaccess.conf
     ```

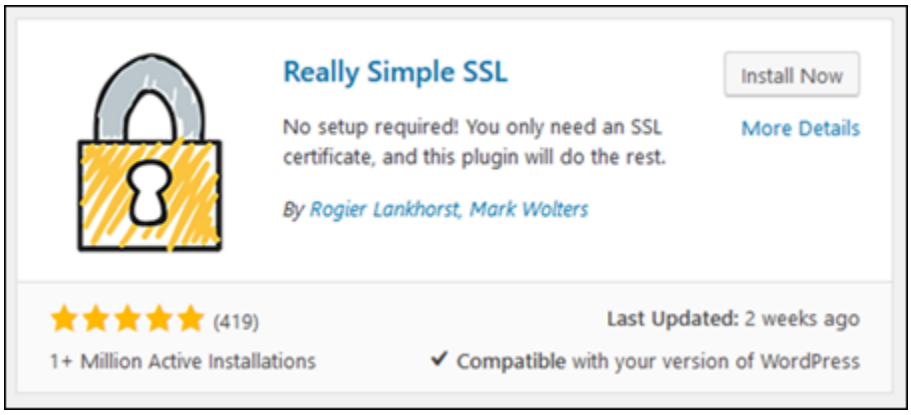
2. 打开新的浏览器窗口并登录您的 WordPress 实例的管理控制面板。

> **Note**
>
> 有关更多信息，请参阅[在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码]。

3. 从左侧导航窗格中选择 Plugins (插件)。
4. 选择“Plugins (插件)”页面顶部的 Add New (添加新插件)。



5. 搜索 Really Simple SSL。
6. 选择搜索结果中 Really Simple SSL 插件旁边的 Install Now (立即安装)。



7. 安装完成后，选择 Activate (激活)。
8. 在弹出的提示消息中选择 Go ahead, activate SSL! (继续，激活 SSL！) 您可能会被重定向到您的 WordPress实例管理控制面板的登录页面。

您的 WordPress 实例现已配置为使用 SSL 加密。此外，您的 WordPress 实例现在已配置为自动将连接从 HTTP 重定向到 HTTPS。当访问者访问 `http://example.com` 时，系统会自动将其重新导向至已加密的 HTTPS 连接（即 `https://example.com`）。

步骤 9：每 90 天续订一次 Let's Encrypt 证书

Let's Encrypt 证书的有效期为 90 天。证书可以在到期前 30 天续订。要续订 Let's Encrypt 证书，请运行用于获取它们的原始命令。重复本教程的请求 Let's Encrypt SSL 通配符证书部分中的步骤。

按照您的特定实例类型的 step-by-step说明进行操作。每个主题都提供了针对您实例的 Linux 发行版（Ubuntu 或 Debian）和 Bitnami 安装类型（系统包或独立包）量身定制的详细命令和配置步骤。通过遵循本主题，您可以使用 Let's Encrypt 提供的免费 SSL/TLS 证书保护您的 Lightsail 网站和应用程序，从而确保加密通信并提高访问者的安全性。

为 Lightsail 实例配置 IPv6 网络

本节涵盖以下与在 Lightsail 实例 IPv6 蓝图上进行配置相关的主题：

主题

- 在 Lightsail 中为 cPanel 实例配置 IPv6 连接
- 在 Lightsai GitLab l 中为实例配置 IPv6 连接
- 在 Lightsail 中为 Nginx 实例配置 IPv6 连接
- 在 Lightsail 中为 Plesk 实例配置 IPv6 连接

在 Lightsail 中为 cPanel 实例配置 IPv6 连接

默认情况下，Amazon Lightsail 中的所有实例都为其分配了公有 IPv4 地址和私有地址。您可以选择 IPv6 为您的实例启用为其分配公有 IPv6 地址。有关更多信息，请参阅 Amazon Lightsail IP 地址和启用或禁用。 IPv6

IPv6 为使用 cPanel 和 WHM 蓝图的实例启用后，您必须执行一组额外的步骤以使该实例知道其 IPv6 地址。在本指南中，我们将介绍必须对 cPanel 和 WHM 实例执行的附加步骤。

先决条件

满足以下先决条件（如果尚未满足）：

- 在 Lightsail 中创建一个 cPanel 和 WHM 实例。有关更多信息，请参阅创建实例。
- 配置 cPanel 和 WHM 实例。有关更多信息，请参阅 Amazon Lightsai l 上的快速入门指南：cPanel 和 WHM。

> **Important**
>
> 在继续执行本指南中的步骤之前，请确保已执行所有软件更新和必要的系统重启。

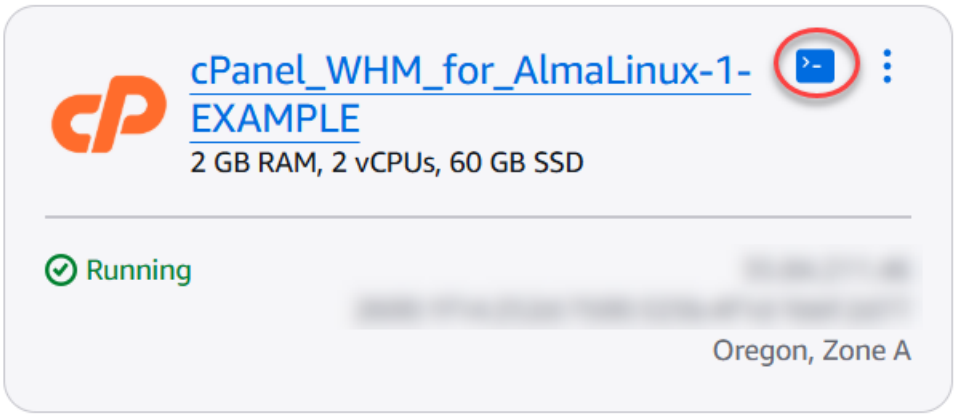
- IPv6 为你的 cPanel 和 WHM 实例启用。有关更多信息，请参阅启用或禁用 IPv6。

> **Note**
>
> 2021 年 1 月 12 日当天或之后创建的新 cPanel 和 WHM 实例在 Lightsail 控制台中创建时默认 IPv6处于启用状态。即使在创建实例时已默认启用，您也必须完成本指南中的以下步骤才能 IPv6 在实例 IPv6 上进行配置。

在 cPanel 和 WHM 实例 IPv6 上进行配置

完成以下步骤，在 Lightsail 中的 cPanel 和 WHM 实例 IPv6 上进行配置。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的 “实例” 部分，找到您要配置的 cPanel 和 WHM 实例，然后选择基于浏览器的 SSH 客户端图标以使用 SSH 连接到该实例。



3. 连接到实例后，请输入以下命令，使用 Nano 打开 `ifcfg-eth0` 网络接口配置文件。

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

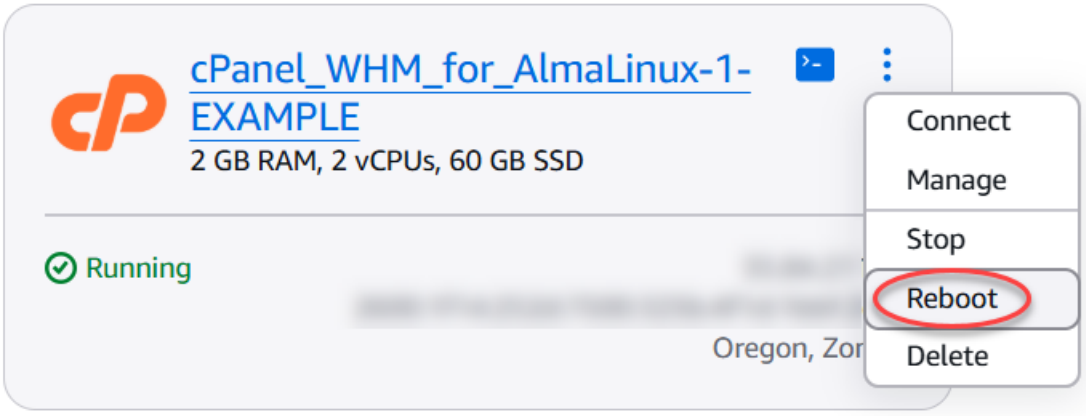
4. 将以下文本行添加到文件中（如果这些文本尚未存在）。

```
IPV6INIT=yes
IPV6_AUTOCONF=yes
DHCPV6C=yes
```

结果应该类似以下示例。

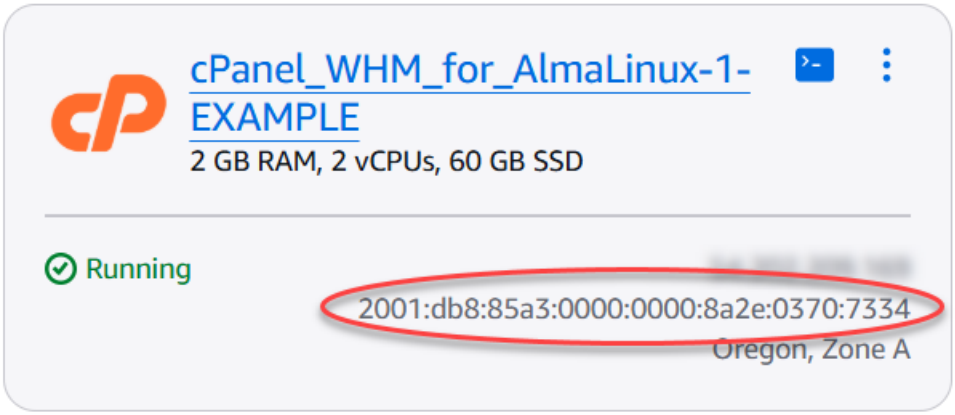
```
# Automatically generated by the vm import process
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=eth0
DEVICE=eth0
ONBOOT=yes
IPV6INIT=yes
IPV6_FAILURE_FATAL=no
DHCPV6C=yes
IPV6_AUTOCONF=yes
```

5. 按键盘上 CTRL+C 退出该文件。
6. 当系统提示保存修改后的缓冲区时，按 Y，然后按 Enter 键以保存到现有文件。这将保存您对 `ifcfg-eth0` 网络接口配置文件所做的编辑。
7. 关闭基于浏览器的 SSH 窗口并切换回 Lightsail 控制台。
8. 在 Lightsail 主页的 “实例” 部分，选择 cPanel 和 WHM 实例的操作菜单 (‹)，然后选择重启。

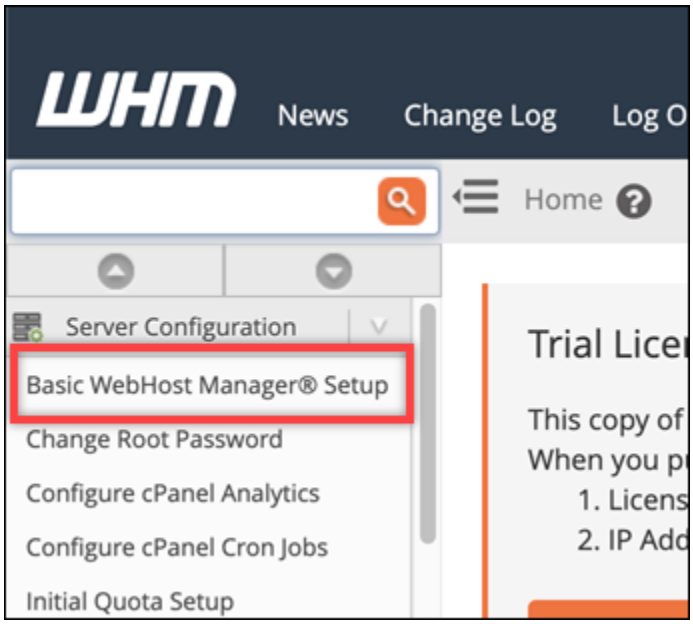


等待几分钟以完成实例的重启，然后继续执行下一步。

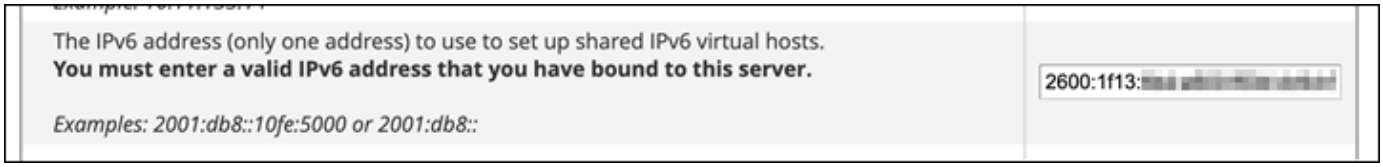
9. 在 Lightsail 主页的 “实例” 部分，记下分配给你的 cPanel 和 WHM 实例 IPv6 的地址。



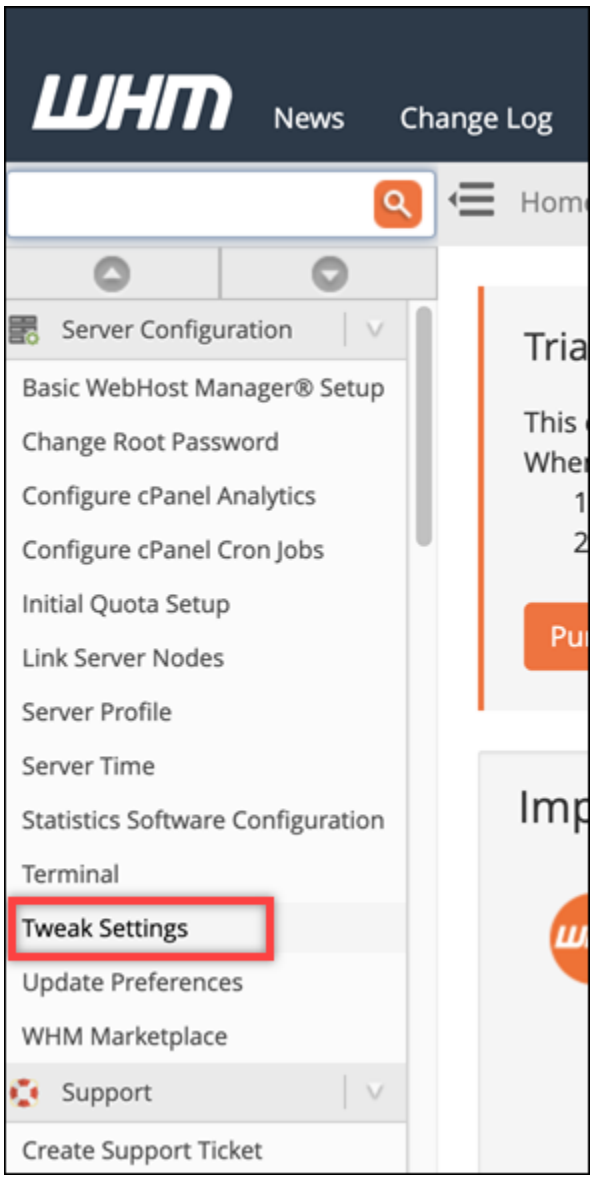
10. 打开一个新的浏览器选项卡，然后登录到 cPanel 和 WHM 实例的 Web Host Manager (WHM)。
11. 在 WHM 控制台的左侧导航窗格中，选择基本 WebHost 管理器设置。



12. 在 “全部” 选项卡中，找到要使用IPv6 的地址文本，然后输入分配给您的实例 IPv6 的地址。您应该记下本过程步骤 9 中分配给您的实例 IPv6 的地址。



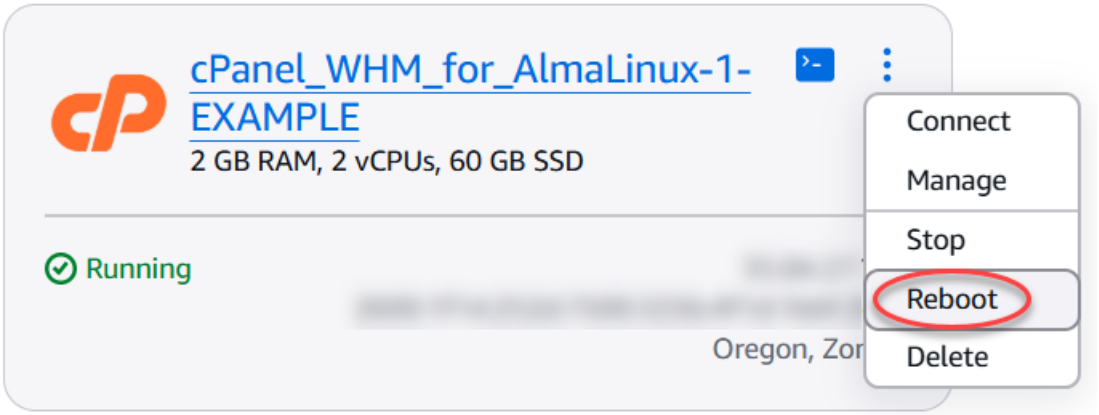
13. 滚动到页面底部并选择 Save Changes (保存更改)。
14. 在 WHM 控制台的左侧导航窗格中，选择 Tweak Settings (调整设置)。



15. 在 “全部” 选项卡中，向下滚动找到 “监听 IPv6地址” 设置，并将其设置为 “开”。

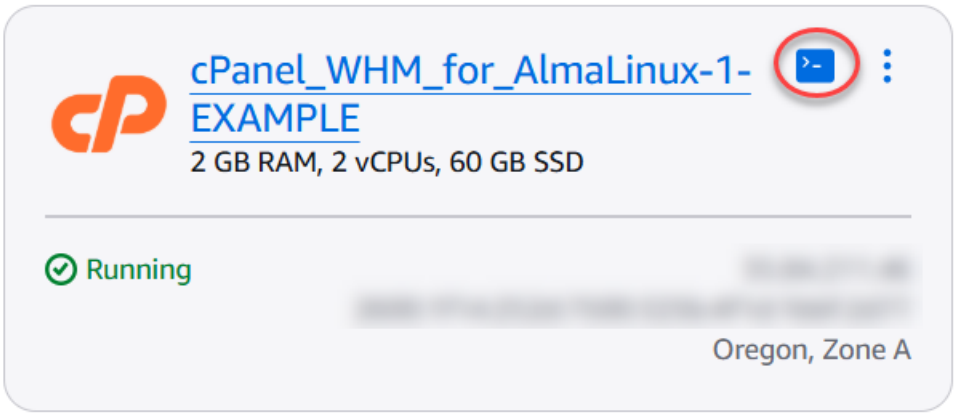


16. 滚动到页面底部并选择 Save (保存)。
17. 切换回 Lightsail 控制台。
18. 在 Lightsail 主页的 “实例” 部分，选择 cPanel 和 WHM 实例的操作菜单 (‹)，然后选择重启。



等待几分钟以完成实例的重启，然后继续执行下一步。

19. 选择 CPanel 和 WHM 实例的基于浏览器的 SSH 客户端图标，以使用 SSH 连接。



20. 连接到您的实例后，输入以下命令以查看您的实例上配置的 IP 地址，并确认它现在可以识别其分配 IPv6 的地址。

```
ip addr
```

您看到的响应与以下示例类似。如果您的实例确实识别了其 IPv6 地址，那么您将在响应中看到它列出并带有范围为全局的标签，如本示例所示。

```
[centos@ ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 02:9b:51:92:50:45 brd ff:ff:ff:ff:ff:ff
    inet /20 brd  scope global dynamic eth0
    inet6 2600:1f13:  :6d59:4ac0/128 scope global dynamic
    inet6 fe80:  :5045/64 scope link
       valid_lft forever preferred_lft forever
```

21. 输入以下命令以确认您的实例能够 ping IPv6 地址。

```
ping6 ipv6.google.com -c 6
```

结果应类似于以下示例，它确认您的实例能够 ping IPv6 地址。

```
[centos@ ~]$ ping6 ipv6.google.com
PING ipv6.google.com(sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e)) 56 data bytes
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=1 ttl=103 tim
e=7.66 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=2 ttl=103 tim
e=7.70 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=3 ttl=103 tim
e=7.68 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=4 ttl=103 tim
e=7.69 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=5 ttl=103 tim
e=7.70 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=6 ttl=103 tim
e=7.68 ms
^C
--- ipv6.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 7.667/7.690/7.702/0.052 ms
```

在 Lightsai GitLab l 中为实例配置 IPv6 连接

默认情况下，Amazon Lightsail 中的所有实例都为其分配了公有 IPv4 地址和私有地址。您可以选择 IPv6 为您的实例启用为其分配公有 IPv6 地址。有关更多信息，请参阅 Amazon Lightsail IP 地址和启用或禁用。 IPv6

IPv6 为使用该 GitLab 蓝图的实例启用后，您必须执行一组额外的步骤以使该实例知道其 IPv6 地址。在本指南中，我们将向您展示您必须为 GitLab 实例执行的其他步骤。

先决条件

满足以下先决条件（如果尚未满足）：

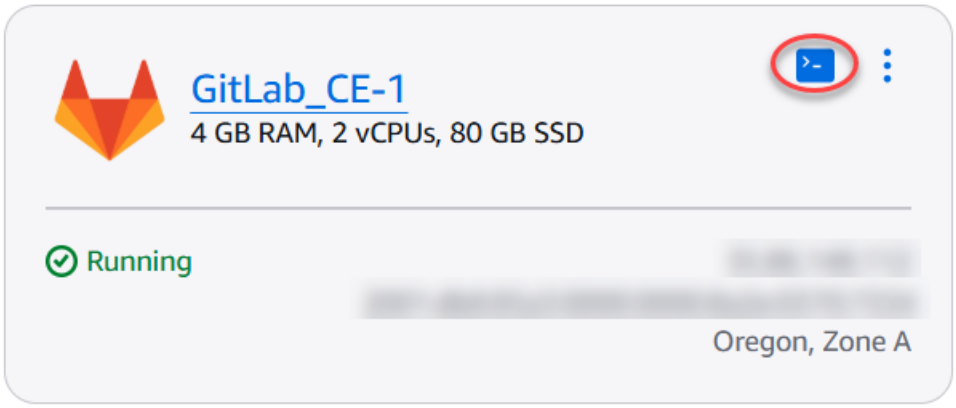
- 在 Lightsail 中创建一个 GitLab 实例。有关更多信息，请参阅创建实例。
- IPv6 为您的 GitLab 实例启用。有关更多信息，请参阅启用或禁用 IPv6。

> **Note**
>
> 2021 年 1 月 12 日当天或之后创建的新 GitLab 实例在 Lightsail 控制台中创建时默认 IPv6 处于启用状态。即使在创建实例时已默认启用，您也必须完成本指南中的以下步骤才能 IPv6 在实例 IPv6 上进行配置。

在 GitLab 实例 IPv6 上配置

完成以下步骤，在 Lightsail 中的 GitLab 实例 IPv6 上进行配置。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的 “实例” 部分，找到您要配置的 GitLab 实例，然后选择基于浏览器的 SSH 客户端图标以使用 SSH 连接到该实例。



3. 连接到实例后，输入以下命令以查看在实例上配置的 IP 地址。

```
ip addr
```

您看到的响应与以下示例类似：

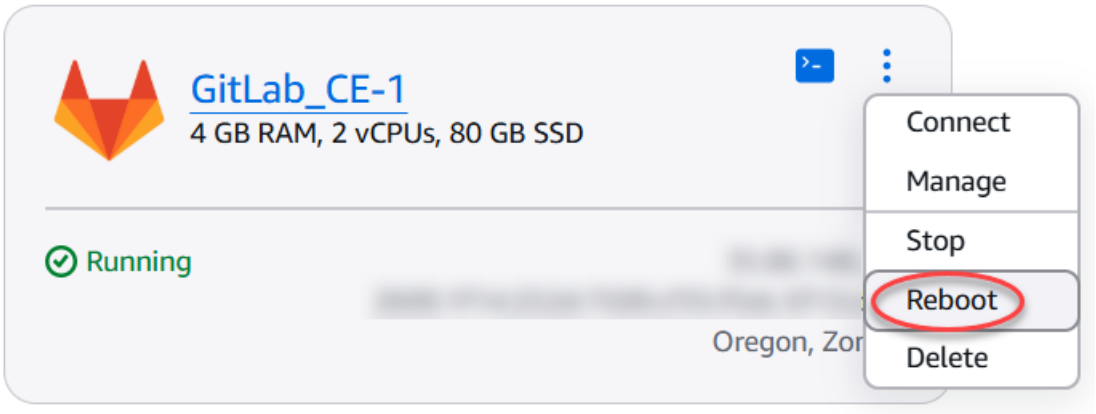
- 如果您的实例无法识别其 IPv6 地址，那么您将不会在响应中看到该地址。您应继续完成此过程的步骤 4 到 9。

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

- 如果您的实例确实识别了其 IPv6 地址，那么您将在响应中看到该地址列出，并带有此示例所`scope global`示。您应该到此为止；您无需完成此过程的第 4 步到第 9 步，因为您的实例已配置为可以识别其 IPv6 地址。

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:f383:3212/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

4. 切换回 Lightsail 控制台。
5. 在 Lightsail 主页的 “实例” 部分，选择 GitLab 实例的操作菜单 (‹)，然后选择重启。

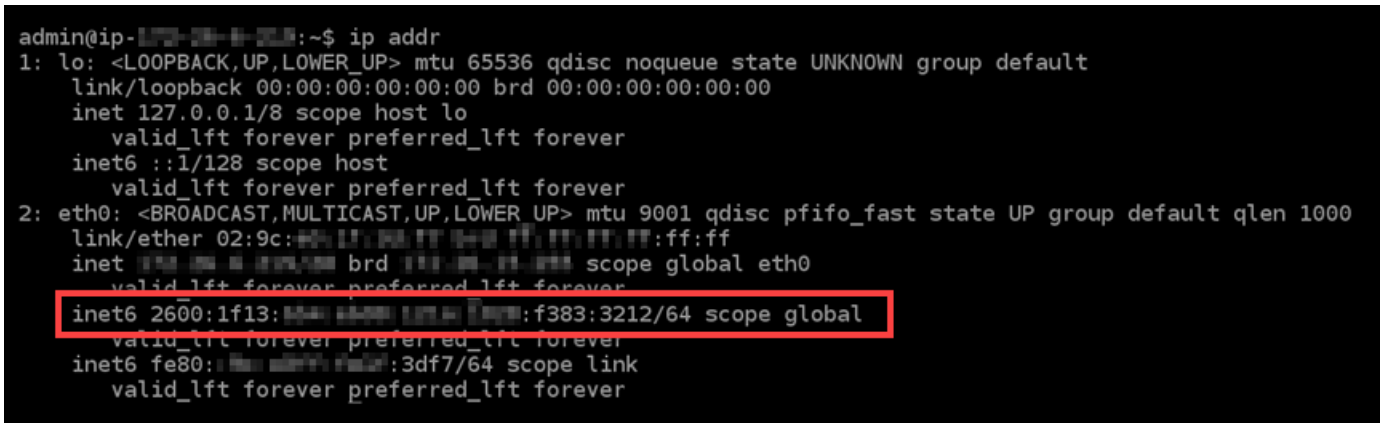


等待几分钟以完成实例的重启，然后继续执行下一步。

6. 切换回您的 GitLab 实例的 SSH 会话。
7. 输入以下命令查看您的实例上配置的 IP 地址，并确认它现在可以识别其分配 IPv6 的地址。

```
ip addr
```

您看到的响应与以下示例类似。如果您的实例确实识别了其 IPv6 地址，那么您将在响应中看到该地址的列出，标签为，`scope global`如本示例所示。



在 Lightsail 中为 Nginx 实例配置 IPv6 连接

默认情况下，Amazon Lightsail 中的所有实例都为其分配了公有 IPv4 地址和私有地址。您可以选择 IPv6 为您的实例启用为其分配公有 IPv6 地址。有关更多信息，请参阅 Amazon Lightsail IP 地址和启用或禁用。 IPv6

IPv6 为使用 Nginx 蓝图的实例启用后，您必须执行一组额外的步骤以使该实例知道其 IPv6 地址。在本指南中，我们将介绍必须对 Nginx 实例执行的附加步骤。

先决条件

满足以下先决条件（如果尚未满足）：

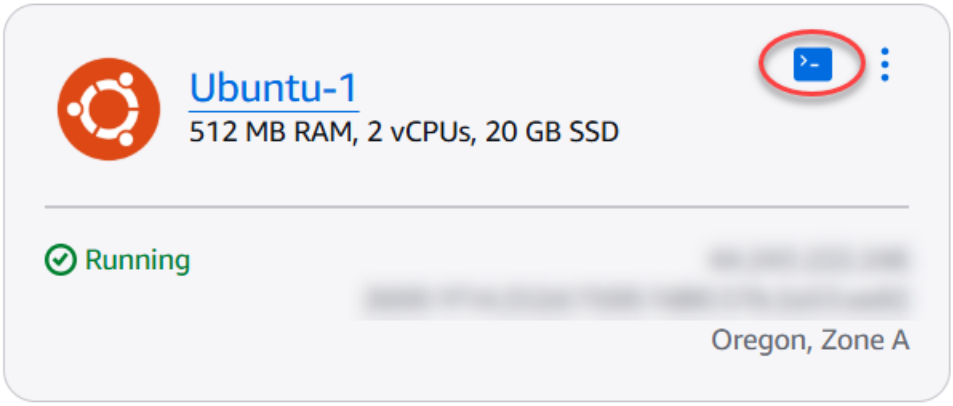
- 在 Lightsail 中创建一个 Nginx 实例。有关更多信息，请参阅创建实例。
- IPv6 为你的 Nginx 实例启用。有关更多信息，请参阅启用或禁用 IPv6。

> **Note**
>
> 2021 年 1 月 12 日当天或之后创建的新 Nginx 实例在 Lightsail 控制台中创建时默认 IPv6 处于启用状态。即使在创建实例时已默认启用，您也必须完成本指南中的以下步骤才能 IPv6 在实例 IPv6 上进行配置。

在 Nginx 实例 IPv6 上进行配置

完成以下步骤，在 Lightsai IPv6 l 中的 Nginx 实例上进行配置。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的 “实例” 部分，找到您要配置的 Ubuntu 实例，然后选择基于浏览器的 SSH 客户端图标以使用 SSH 连接到该实例。



3. 连接到实例后，输入以下命令以确定您的实例是否正在监听通过端口 80 的 IPv6 请求。请务必*<IPv6Address>*替换为分配给您的实例 IPv6 的地址。

```
curl -g -6 'http://[<IPv6Address>]'
```

示例：

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

您看到的响应与以下示例类似：

- 如果您的实例未通过端口 80 监听 IPv6 请求，则您将看到一条带有连接失败错误消息的响应。您应继续完成此过程的步骤 4 到 9。

```
bitnami@ip-[redacted]:~$ curl -g -6 'http://[2600:1f13:[redacted]:985b:25d9]:80'
curl: (7) Failed to connect to 2600:1f13:[redacted]:985b:25d9 port 80: Connection refused
```

- 如果您的实例正在监听通过端口 80 的 IPv6 请求，则您将看到包含您的实例主页的 HTML 代码的响应，如以下示例所示。您应该到此为止；您无需完成此过程的第 4 步到第 9 步，因为您的实例已配置为 IPv6。

```
bitnami@ip-[redacted]:~$ curl -g -6 'http://[2600:[redacted]:985b:25d9]:80'
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Bitnami NGINX Open Source</title>
    <meta name="description" content="Bitnami: Open Source. Simplified.">
    <meta name="author" content="Bitnami">
    <link rel="stylesheet" media="screen" href="//unpkg.com/@bitnami/hex/dist/hex.min.css">
  </head>
  <body>
    <main class="margin-t-huge">
      <section aria-labelledby="installation-title" aria-describedby="installation-desc" class="container container-tiny margin-b-gi
        <h1 id="installation-title">Congratulations!</h1>
        <div aria-hidden="true" style="height: 4px; width: 100%;" class="gradient-135-brand"></div>
        <p id="installation-desc" class="type-big">You are now running <strong>Bitnami NGINX Open Source 1.18.0</strong> in the Clou
      </section>
      <section aria-labelledby="links-title" aria-describedby="links-desc" class="bg-light padding-v-bigger margin-v-enormous">
        <div class="container container-tiny">
          <div class="row row-collapse-b-tablet align-center ">
            <div class="col-6">
              <h3 id="links-title" class="margin-t-reset">Useful Links</h3>
              <p id="links-desc" class="margin-b-reset">The following links will help you to understand better how to get started an
unched.</p>
```

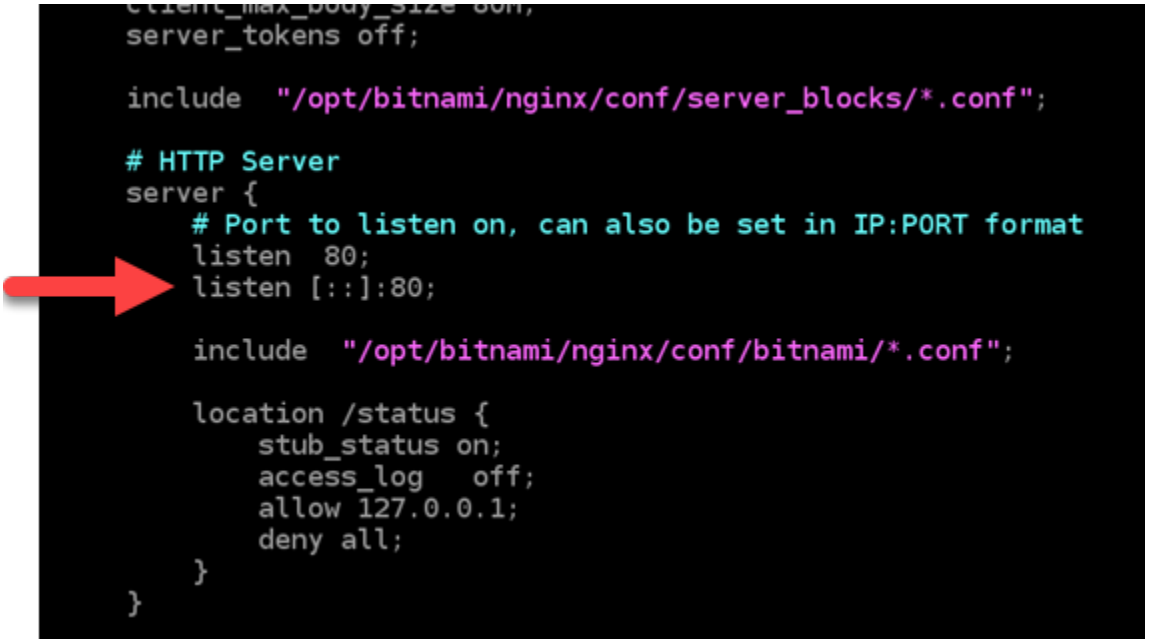
4. 输入以下命令以使用 Vim 打开 nginx.conf 配置文件。

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

5. 按 I 进入 Vim 的插入模式。
6. 在文件中已有的 `listen 80;` 文本下面，添加以下文本。您可能需要在 Vim 中向下滚动才能看到需要添加文本的部分。

```
listen [::]:80;
```

完成后，文件将与以下内容类似：



7. 按 ESC 键退出 Vim 的插入模式，然后输入 :wq! 并按 Enter 以保存您的编辑内容（写入），再退出 Vim。
8. 输入以下命令以重新启动实例的服务。

```
sudo /opt/bitnami/ctlscript.sh restart
```

9. 输入以下命令以确定您的实例是否在监听通过端口 80 的 IPv6请求。请务必*<IPv6Address>*替换为分配给您的实例 IPv6 的地址。

```
curl -g -6 'http://[<IPv6Address>]'
```

示例：

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

您看到的响应与以下示例类似。如果您的实例正在监听通过端口 80 的 IPv6 请求，则您将看到包含您的实例主页的 HTML 代码的响应。



在 Lightsail 中为 Plesk 实例配置 IPv6 连接

您必须执行一组额外的步骤才能使使用 Plesk 蓝图的实例知道其 IPv6 地址。在本指南中，我们将介绍必须对 Plesk 实例执行的附加步骤。

先决条件

满足以下先决条件（如果尚未满足）：

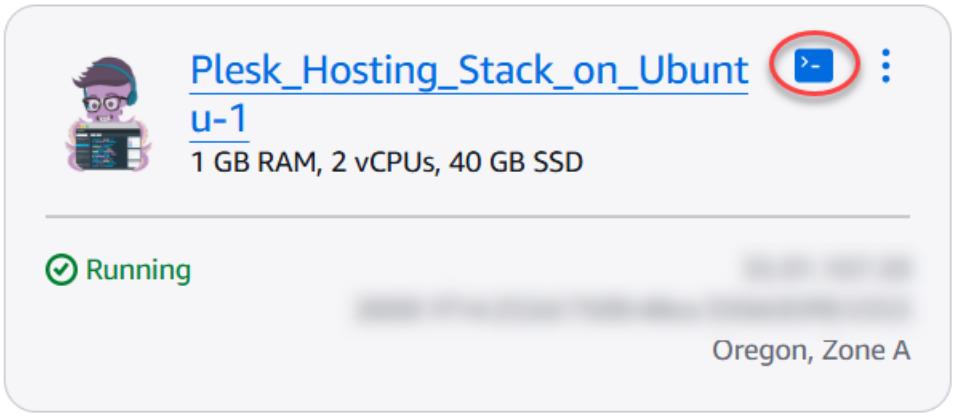
- 在 Lightsail 中创建一个 Plesk 实例。有关更多信息，请参阅创建实例。
- IPv6 为您的 Plesk 实例启用。有关更多信息，请参阅启用或禁用 IPv6。

> **Note**
>
> 2021 年 1 月 12 日当天或之后创建的 Lightsail Plesk 实例默认 IPv6 处于启用状态。即使在创建实例时已默认启用，您也必须完成本指南中的以下步骤才能 IPv6 在实例 IPv6 上进行配置。

在 Plesk 实例 IPv6 上进行配置

完成以下步骤，在 Lightsail 中的 Plesk 实例 IPv6 上进行配置。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的 “实例” 部分，找到您要配置的 Plesk 实例，然后选择基于浏览器的 SSH 客户端图标以使用 SSH 连接到该实例。

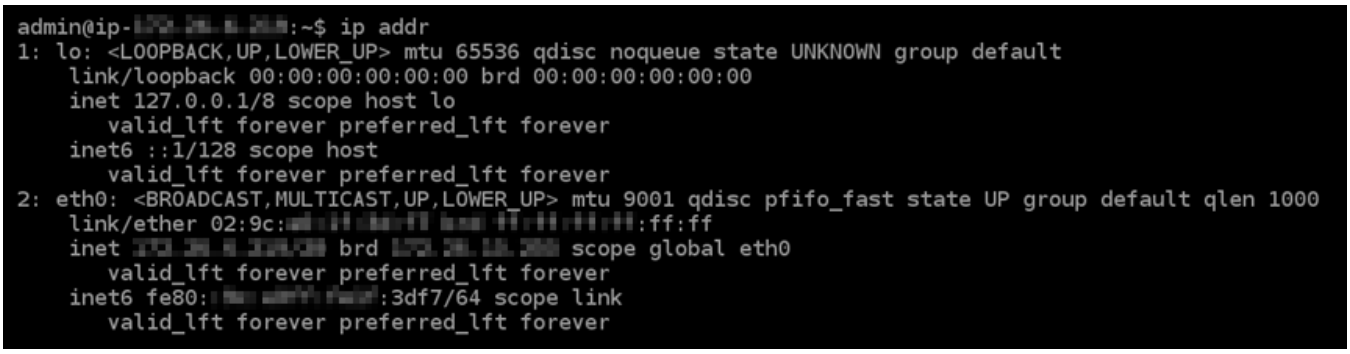


3. 连接到实例后，输入以下命令以查看在实例上配置的 IP 地址。

```
ip addr
```

您看到的响应与以下示例类似：

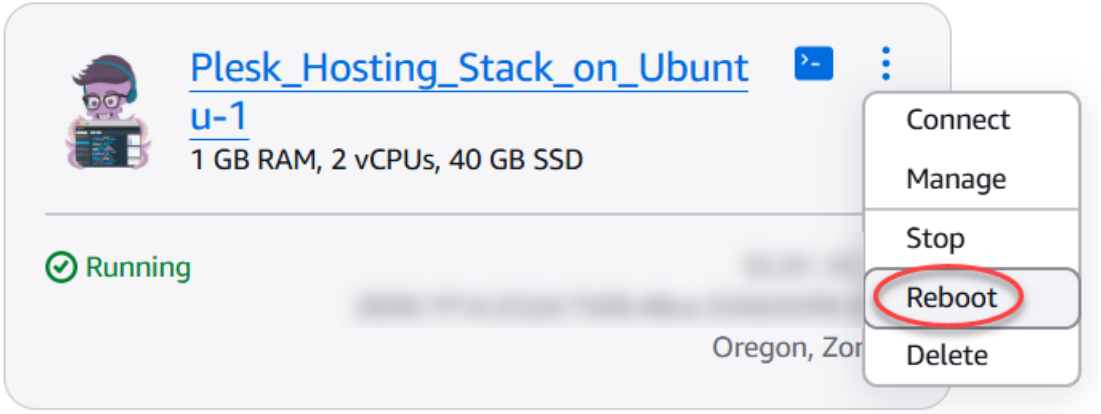
- 如果您的实例无法识别其 IPv6 地址，那么您将不会在响应中看到该地址。您应继续完成此过程的步骤 4 到 7。



- 如果您的实例确实识别了其 IPv6 地址，那么您将在响应中看到该地址列出，并带有此示例所`scope global`示。您应该到此为止；您无需完成此过程的第 4 步到第 7 步，因为您的实例已配置为可以识别其 IPv6 地址。

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:f383:3212/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

4. 切换回 Lightsail 控制台。
5. 在 Lightsail 主页的 “实例” 部分，选择 Plesk 实例的操作菜单 (‹)，然后选择重启。

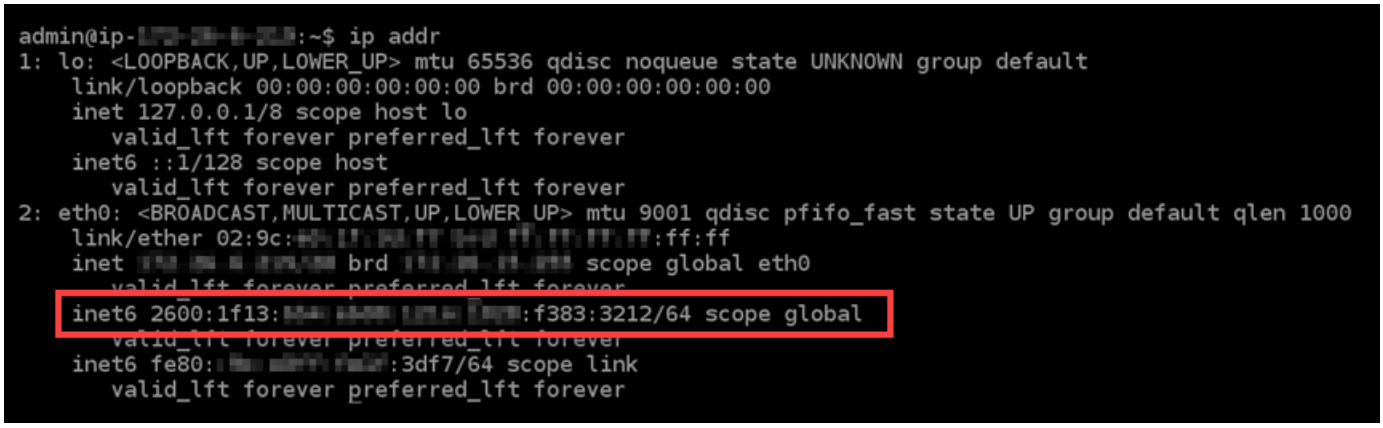


等待几分钟以完成实例的重启，然后继续执行下一步。

6. 切换回 Plesk 实例的 SSH 会话。
7. 输入以下命令查看您的实例上配置的 IP 地址，并确认它现在可以识别其分配 IPv6 的地址。

```
ip addr
```

您看到的响应与以下示例类似。如果您的实例确实识别了其 IPv6 地址，那么您将在响应中看到该地址的列出，标签为，`scope global`如本示例所示。



按照 step-by-step说明学习如何在 Lightsail 实例蓝图 IPv6 上进行配置。

该指南涵盖了各种实例蓝图，包括 cPanel、 GitLab、Nginx 和 Plesk。这些过程包括通过 SSH 连接到您的实例、修改网络配置文件、重新启动服务以及验证实例是否识别其分配 IPv6 的地址。通过遵循本指南，您可以确保正确配置您的 Lightsail 实例以同时使用 IPv4 和 IPv6 地址，从而实现更好的连接并为未来的互联网做好准备。

为 Lightsai AWS CLI I 操作设置和配置

AWS Command Line Interface (AWS CLI) 是一种工具，允许高级用户和开发人员通过在终端（在 Linux 和 Unix 上）或命令提示符（在 Windows 上）中键入命令来控制 Amazon Lightsail 服务。你还可以使用 Lightsail 控制台、图形用户界面和 Lightsail 应用程序程序接口 (API) 控制 Lightsail。

> **Tip**
>
> 您还可以使用运行 AWS CLI 命令 AWS CloudShell 来管理 Lightsail 资源，而无需下载或安装命令行工具。 CloudShell 是一款基于浏览器的预先认证外壳，您可以直接从 Lightsail 控制台启动它。有关更多信息，请参阅 使用管理 Lightsail 资源 AWS CloudShell。

主题

- 步骤 1：安装 AWS CLI
- 步骤 2：创建新的访问密钥
- 步骤 3：配置 AWS CLI
- 后续步骤

步骤 1：安装 AWS CLI

您可以将其安装在本地桌面 AWS CLI 上，也可以将其安装在您的 Lightsail 实例上。有关更多信息 AWS CLI，请参阅《AWS Command Line Interface 用户指南》。

- 要在本地桌面 AWS CLI 上安装，请参阅 AWS Command Line Interface 文档 AWS CLI中的安装。
- 要在基于 Ubuntu 的 Lightsail 实例 AWS CLI 上安装，请连接到您的实例，然后键入。`sudo apt-get -y install awscli`

> **Note**
>
> AWS CLI 应该已经安装在亚马逊 Linux Lightsail 实例上。如果您需要重新安装它，请连接到您的实例，然后键入 `sudo yum install aws-cli`。

安装后 AWS CLI，您需要生成访问密钥，然后配置为使用 AWS CLI 访问密钥。

步骤 2：创建新的访问密钥

要使用 Lightsail API 或 AWS Command Line Interface (AWS CLI)，你需要创建一个新的访问密钥。访问密钥包含访问密钥 ID 和秘密访问密钥。使用以下步骤创建密钥。

1. 登录 IAM 控制台。
2. 选择所需用户的名称，以为其创建访问密钥。您选择的用户应具有对 Lightsail 操作的完全访问权限或特定访问权限。
3. 选择 Security credentials（安全凭据）选项卡。
4. 在页面的 Access keys（访问密钥）部分下选择 Create access key（创建访问密钥）。

   > **Note**
   >
   > 针对每个用户，您一次最多可拥有两个访问密钥（活动密钥或不活动密钥）。如果您已有两个访问密钥，则必须删除其中的一个，然后才能创建新的密钥。在删除访问密钥前，请确保它未处于活动状态。

5. 记下列出的 Access key ID（访问密钥 ID）和 Secret access key（秘密访问密钥）。在 Secret access key（秘密访问密钥）列下选择 Show（显示），以查看 Secret access key（秘密访问密钥）。

您可以从此屏幕复制它们，也可以选择 “下载密钥文件” 来下载包含访问密钥 ID 和私有访问密钥的.csv文件。

> **Important**
>
> 将您的访问密钥保存在安全位置。您应按照 MyLightsailKeys.csv 的格式命名此文件，以便您稍后可轻松找到它。如果您已从 IAM 控制台下载了 CSV 文件，则应在完成下一步之后将其删除。稍后您可以根据需要创建新的访问密钥。

步骤 3：配置 AWS CLI

您需要将配置 AWS CLI 为使用您的访问密钥，这样您才能使用它。

1. 打开终端窗口或命令提示符。
2. 键入 aws configure。
3. 粘贴您在上一步中创建.csv的文件中的AWS 访问密钥 ID。
4. 在系统提示时粘贴您的 AWS 秘密访问密钥。
5. 输入 AWS 区域 您的资源所在的位置。例如，如果您的资源主要位于俄亥俄州，请在系统提示时，选择 us-east-2 作为 Default region name（默认区域名称）。

   有关使用该 AWS CLI --region选项的更多信息，请参阅AWS CLI 参考中的常规选项。
6. 选择 Default output format（默认输出格式）（如 json）。

现在，你可以使用，以编程方式与 Lightsail 进行交互。 AWS CLI你可以在《命令参考》中找到 Amazon Lightsail 命令。AWS CLI

后续步骤

以下资源可以帮助您开始安装特定语言 AWS SDKs 并熟悉 Lightsail API。

- 安装特定语言的安装 AWS SDKs
- 查看 Lightsail API 参考

使用管理 Lightsail 资源 AWS CloudShell

AWS CloudShell 是一款基于浏览器、经过预先身份验证的外壳，您可以直接从 Amazon Lightsail 控制台启动它。您可以使用 CloudShell 通过命令行界面管理您的 Lightsail 资源。你可以使用你喜欢的外壳来运行 AWS Command Line Interface (AWS CLI) 命令，比如 Bash PowerShell、或 Z shell。您无需下载或安装命令行工具，即可完成此操作。有关更多信息，请参阅什么是 AWS CloudShell。

启动时 CloudShell，将创建一个基于 Amazon Linux 2 的计算环境。在此环境中，您可以访问大量预安装的开发工具，例如 AWS CLI。有关预安装工具的完整列表，请参阅《CloudShell 用户指南》中的预安装软件。

持久性存储

使用 AWS CloudShell，您可以免费使用每种 AWS 区域 存储空间中最多 1 GB 的永久存储空间。持久性存储位于您的主目录 (`$HOME`) 中，对您而言是私有的。与每个 Shell 会话结束后删除的临时环境资源不同的是，主目录中的数据会在不同会话之间保留。

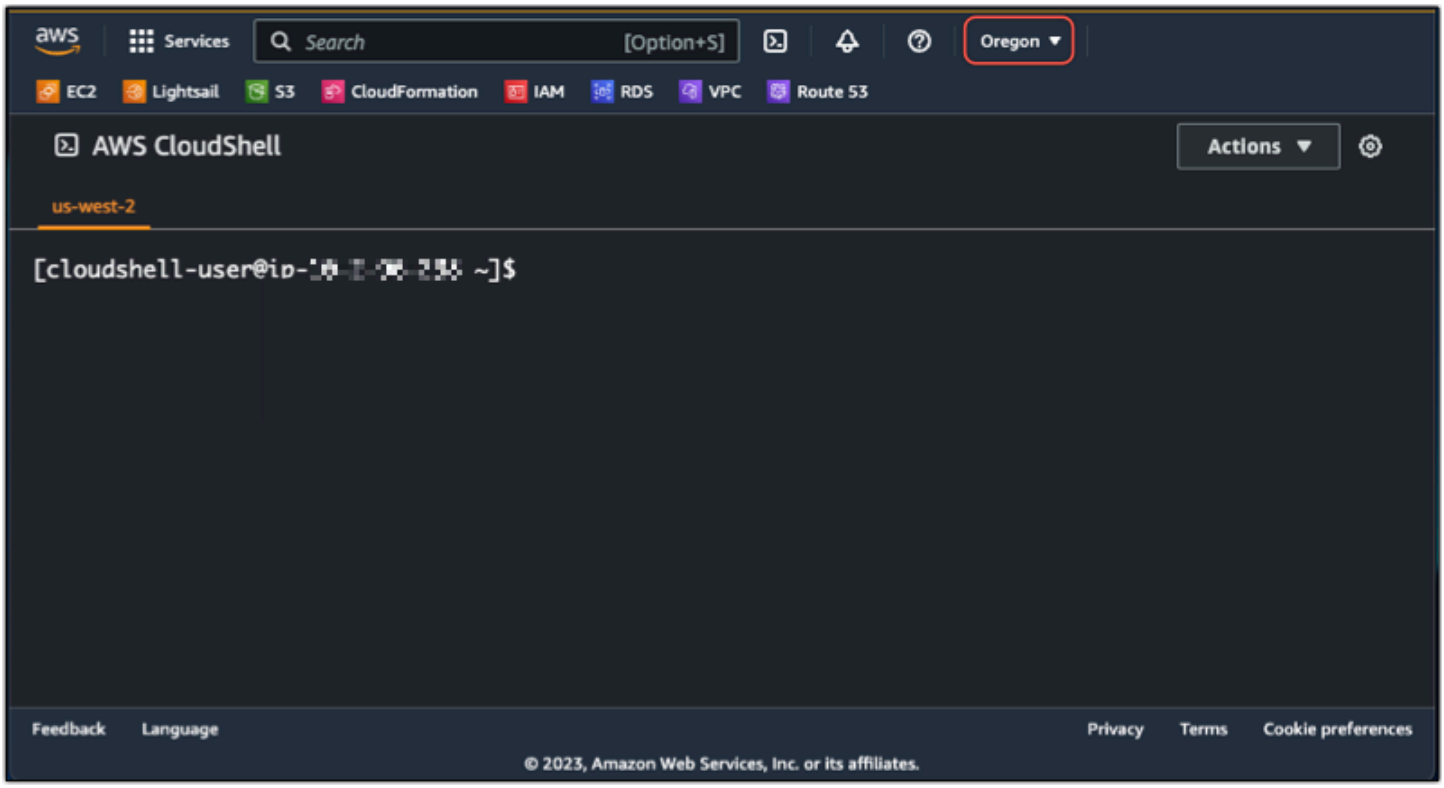
如果您停止 AWS CloudShell 在中使用 AWS 区域，则在上次会话结束后，数据将在该区域的永久存储中保留 120 天。120 天后，除非您采取措施，否则您的数据将自动从该地区的持久性存储中删除。您可以通过在 AWS 区域中再次启动 AWS CloudShell 来阻止删除。有关在永久存储中保留数据的更多信息，请参阅《CloudShell 用户指南》中的永久存储。

AWS 区域

在 Lightsail 中，将在中打开一个会 CloudShell 话 AWS 区域 ，为你的实际位置提供最少的延迟。这意味着这 AWS 区域 可能会在会话之间发生变化。记下你的 CloudShell 会话所在的 AWS 区域-->，这样你就可以使用 1 GB 的永久存储空间了。要更改会话的 AWS 区域，请选择在新浏览器选项卡中打开图标。这提供了在新的浏览器窗口中访问您的 CloudShell 会话的选项。



在新浏览器选项卡的导航栏中，选择当前显示的 AWS 区域 的名称。然后选择 AWS 区域 要切换到的。



有关的更多信息 CloudShell，请参阅《CloudShell 用户指南》。

启动和使用 AWS CloudShell

了解如何在 Lightsail 中启动和使用 AWS CloudShell 会话。如果您没有运行权限 CloudShell，则必须将`arn:aws:iam::aws:policy/AWSCloudShellFullAccess`策略添加到您正在使用的 AWS

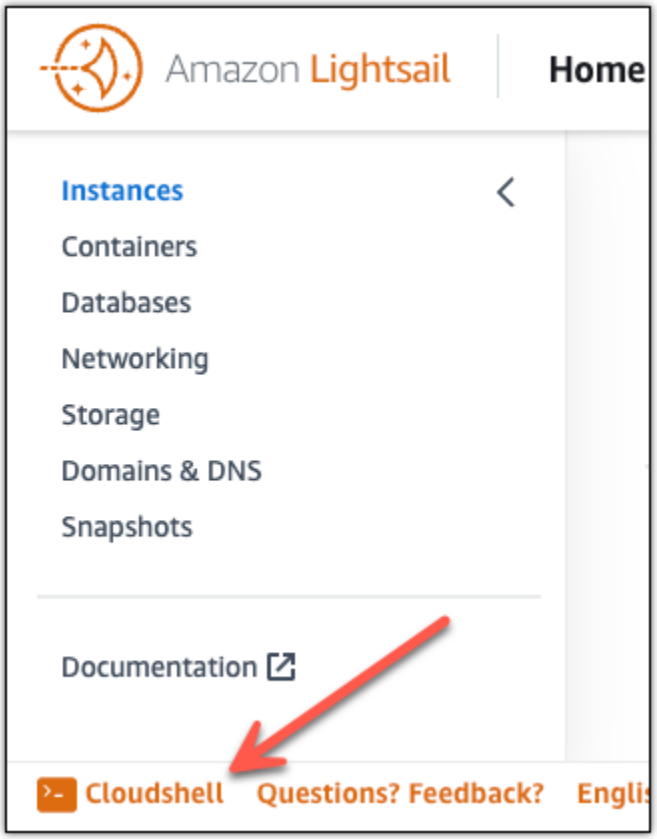
Identity and Access Management (IAM) 身份。如果您已经附加了该`arn:aws:iam::aws:policy/AdministratorAccess`策略，则应该可以访问 CloudShell。有关更多信息，请参阅 ???。

启动 AWS CloudShell

你可以 CloudShell 从 Amazon Lightsail 控制台启动。会话开始后，您可以切换到首选的 Shell，例如 `Bash`、`PowerShell` 或 `Z shell`。

完成以下步骤即可在 Lightsail 中启动新 AWS CloudShell 会话：

1. 登录 Lightsail 控制台，网址为https://lightsail.aws.amazon.com/。
2. 在控制台工具栏CloudShell上进行选择，位于控制台的左下角。当系统显示命令提示符时，表示 shell 已经准备就绪，可以进行交互。



3. （可选）要选择要使用的预安装 Shell，请在命令行提示栏中输入以下程序名称之一：

   Bash：**`bash`**

   如果切换到 Bash，则命令提示符处的符号将更新为 $。Bash 是中的默认外壳。 AWS CloudShell

PowerShell: **`pwsh`**

如果切换到 PowerShell，则命令提示符处的符号将更新为PS>。

Z shell：**`zsh`**

如果切换到 Z shell，则命令提示符处的符号将更新为 %。

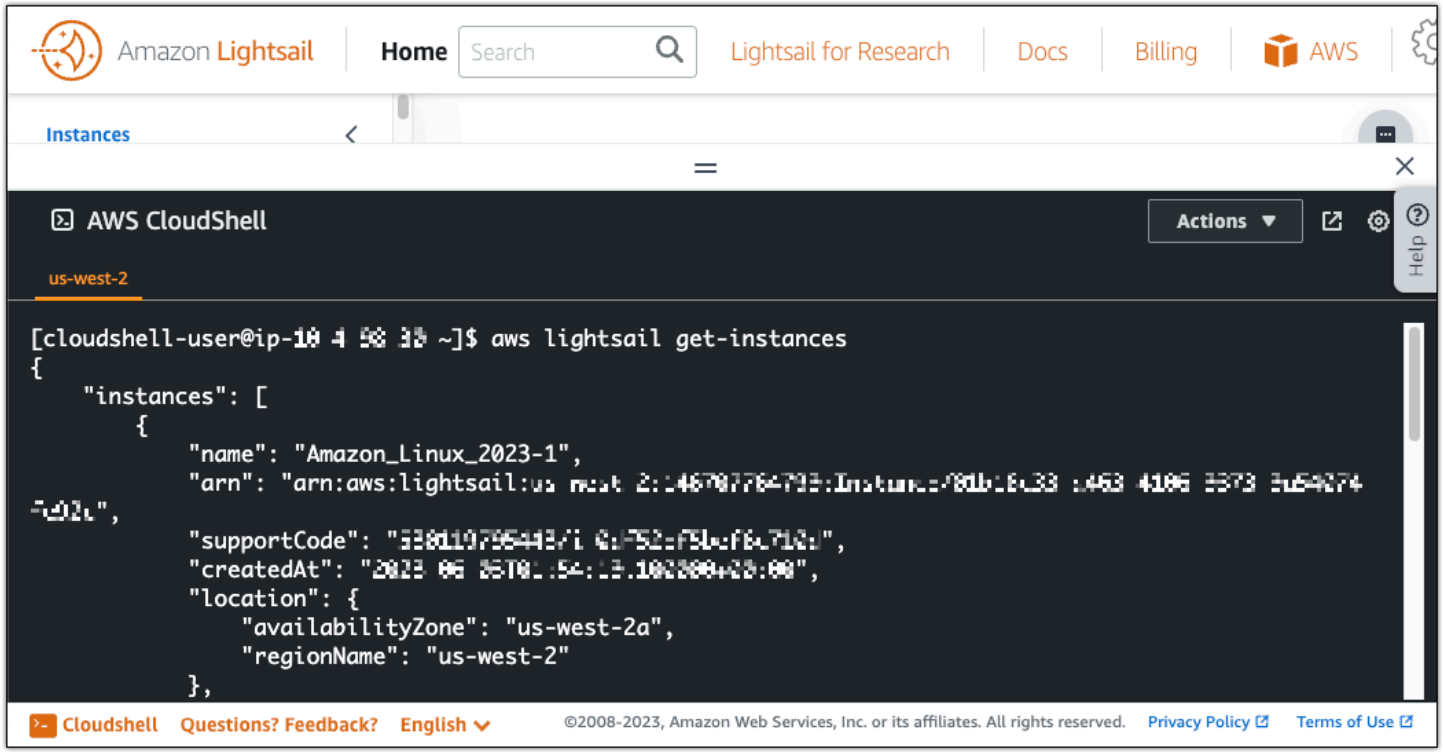
Example 中的 Lightsail API 命令示例 AWS CloudShell

会 CloudShell话中预先安装了多个命令行工具供您使用。在此示例中，您将使用 Lightsail `GetInstances` API 操作来查看您的 Lightsail 账户中的实例。要了解有关 `GetInstances` API 操作的更多信息，请参阅GetInstances《亚马逊 Lightsail API 参考》。

1. 登录 Lightsail 控制台，网址为https://lightsail.aws.amazon.com/。
2. 在控制台工具栏CloudShell上进行选择，位于控制台的左下角。
3. 在 AWS CloudShell 提示符后输入以下命令：

```
aws lightsail get-instances
```

现在，您应该会看到您的 Lightsail 账户中的实例的完整列表。



其他信息

有关以下内容的更多信息，请参阅以下文档 AWS CloudShell：

- 亚马逊 Lightsail API 参考
- 中的常见问题解答 AWS CloudShell
- 中支持的浏览器 AWS CloudShell
- 中的疑难解答 AWS CloudShell
- AWS 服务 在 in 中使用 AWS CloudShell

在 Lightsail LAMP 实例上部署 PHP 应用程序

如果你只需要虚拟专用服务器，Amazon Lightsail 是开始使用亚马逊网络服务 (AWS) 的最简单方法。Lightsail 以低廉且可预测的价格提供快速启动项目所需的一切，包括虚拟机、基于 SSD 的存储、数据传输、DNS 管理和静态 IP。

本教程向你展示了如何在 Lightsail 上启动和配置 LAMP 实例。具体步骤包括：通过 SSH 连接到您的实例，获取该实例的应用程序密码，创建静态 IP 并将其连接到该实例上，以及创建 DNS 区域并将您的域映射到该实例。完成本教程后，你就具备了在 Lightsail 上启动和运行实例的基础知识。

内容

- 步骤 1：注册亚马逊云科技
- 步骤 2：创建 LAMP 实例
- 步骤 3：通过 SSH 连接到您的实例并获取 LAMP 实例的应用程序密码
- 步骤 4：在您的 LAMP 实例上安装应用程序
- 步骤 5：创建静态 IP 地址并将其附加到 LAMP 实例
- 步骤 6：创建 DNS 区域并将域映射到 LAMP 实例
- 后续步骤

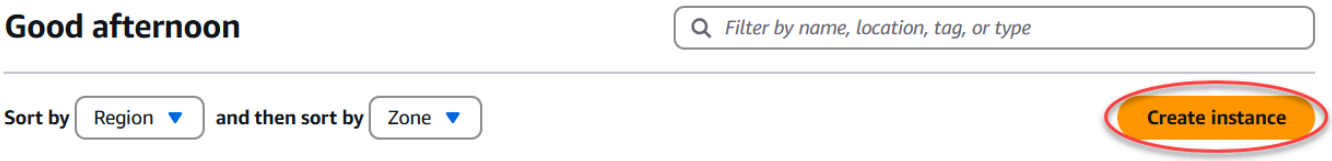
步骤 1：注册亚马逊云科技

本教程需要一个 AWS 帐户。注册 AWS或登录（ AWS如果您已经有一个帐户）。

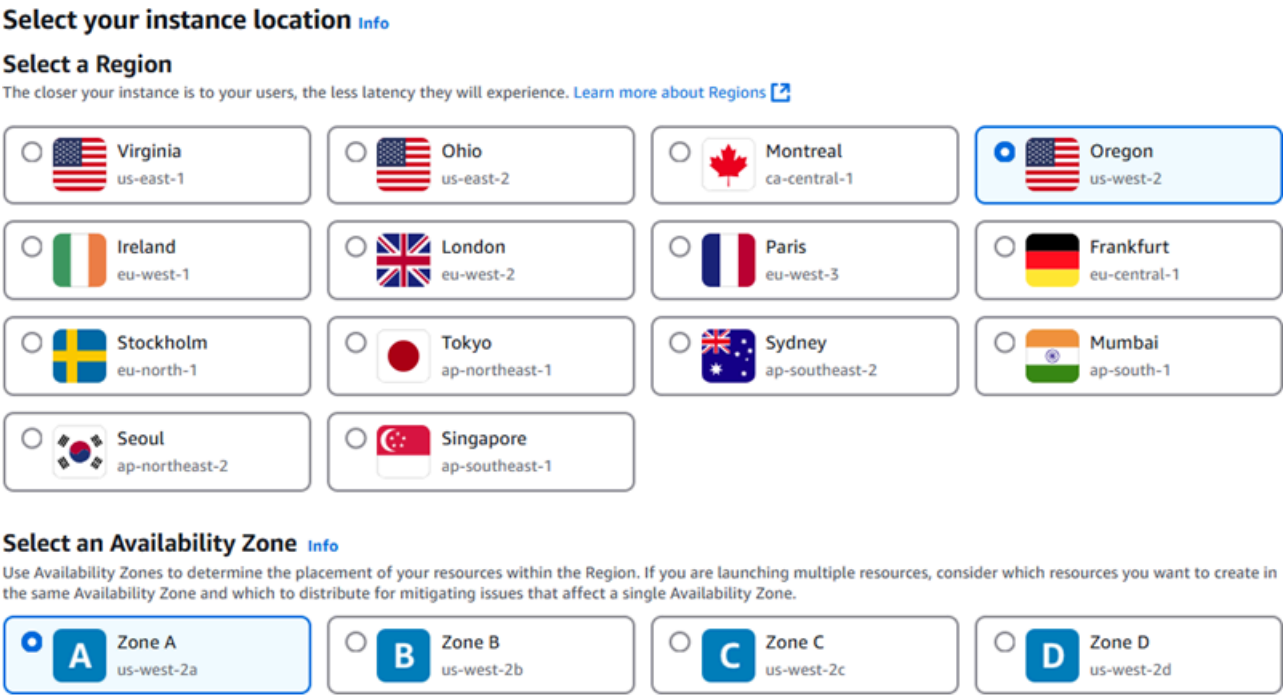
步骤 2：创建 LAMP 实例

在 Lightsail 中启动并运行你的 LAMP 实例。有关在 Lightsail 中创建实例的更多信息，请参阅 Lightsail 文档中的创建亚马逊 Lightsail 实例。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的 “实例” 部分，选择创建实例。



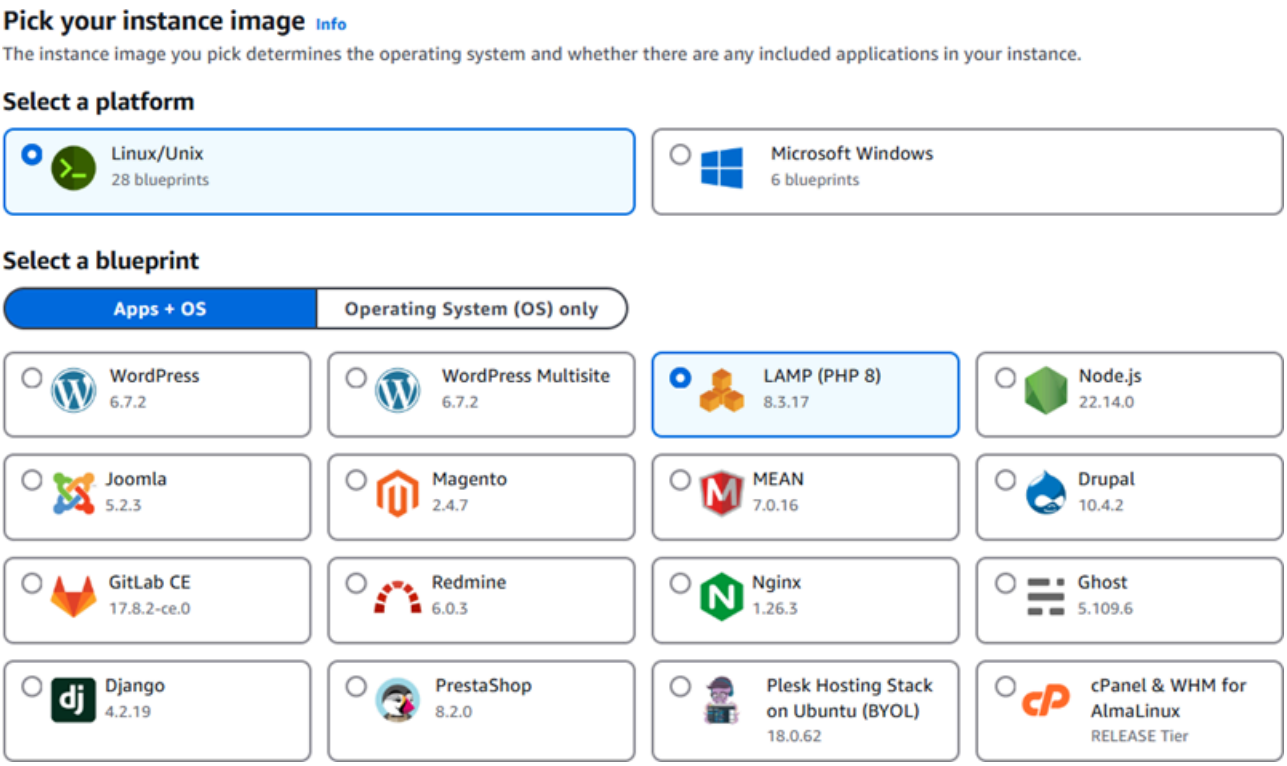
3. 为您的实例选择 AWS 区域 和可用区。



4. 选择您的实例映像。

   a. 选择 Linux/Unix 作为平台。

   b. 选择 LAMP（PHP 8）作为蓝图。



5. 选择实例计划。

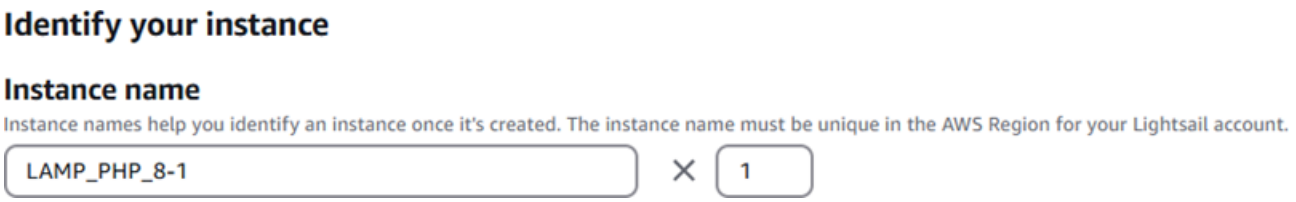
   计划包括可预测的低成本、计算机配置 (RAM、SSD、vCPU) 以及数据传输限额。你可以免费试用 5 美元的 Lightsail 套餐一个月（最长 750 小时）。 AWS 将一个月的免费积分存入您的账户。

   > **Note**
   >
   > 作为 AWS 免费套餐的一部分，您可以免费开始使用特定实例捆绑包的 Amazon Lightsail。有关更多信息，请参阅亚马逊 Lightsail 定价页面上的AWS 免费套餐。

6. 输入实例的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

7. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

   a. 对于密钥，输入标签密钥。

   b. （可选）在“值”中，输入标签值。

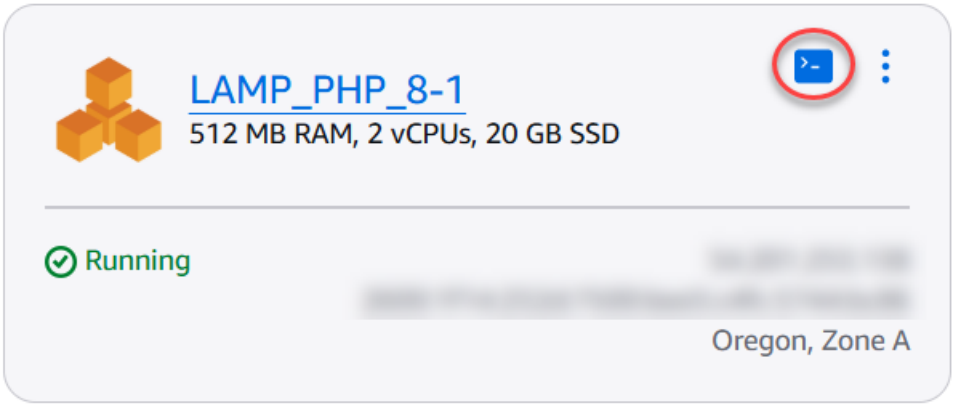
   

8. 选择创建实例。

步骤 3：通过 SSH 连接到您的实例并获取 LAMP 实例的应用程序密码

用于登录 LAMP 中数据库的默认密码存储在您的实例中。通过在 Lightsail 控制台中使用基于浏览器的 SSH 终端连接到您的实例并运行特殊命令来检索它。有关更多信息，请参阅在 Amazon Lightsail 中获取 Bitnami 实例的应用程序用户名和密码。

1. 在 Lightsail 主页的 “实例” 部分，选择 LAMP 实例的 SSH 快速连接图标。



2. 打开基于浏览器的 SSH 客户端窗口后，输入以下命令以检索默认应用程序密码：

```
cat bitnami_application_password
```

> **Note**
>
> 如果您所在的目录不是用户主目录，请输入 `cat $HOME/bitnami_application_password`。

3. 记下屏幕上显示的密码。您随后可以使用此密码在实例上安装 Bitnami 应用程序，或使用此密码结合用户名 `root` 来访问 MySQL 数据库。



步骤 4：在您的 LAMP 实例上安装应用程序

在您的 LAMP 实例上部署 PHP 应用程序或安装 Bitnami 应用程序。用于部署您的 PHP 应用程序的主目录是 `/opt/bitnami/apache2/htdocs`。将您的 PHP 应用程序文件复制到该目录并通过浏览实例的公有 IP 地址访问该应用程序。

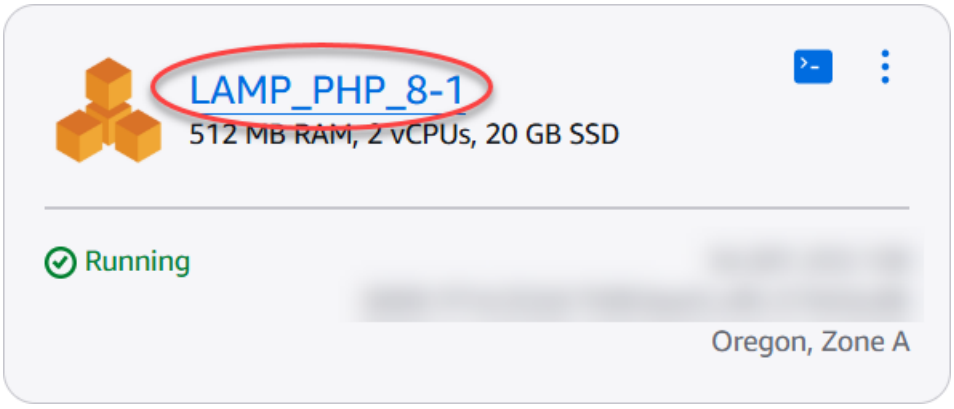
您也可以使用模块安装程序来安装 Bitnami 应用程序。从 Bitnami 网站下载 WordPress Drupal、Magento、Moodle 等应用程序，然后扩展服务器的功能。有关安装 Bitnami 应用程序的更多信息，请参阅 Bitnami 文档中的入门。

步骤 5：创建静态 IP 地址并将其附加到 LAMP 实例

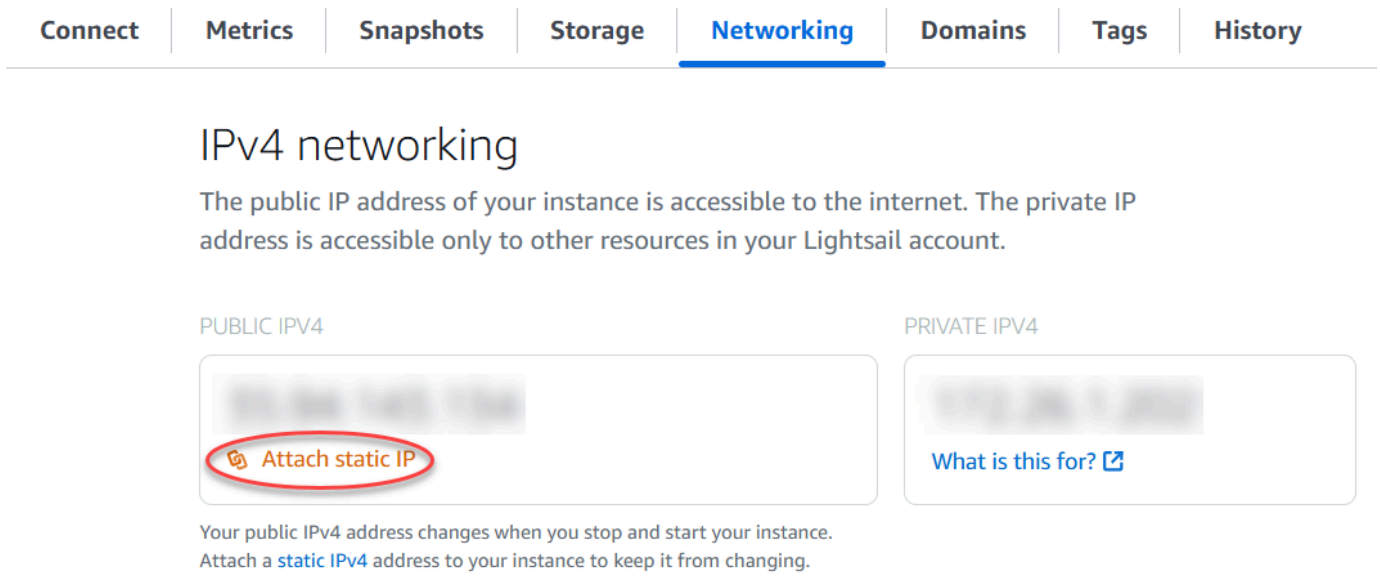
如果您停止和启动您的 LAMP 实例，则该实例的默认公有 IP 会改变。即使您停止和启动您的实例，连接到该实例的静态 IP 地址也会保持不变。

创建静态 IP 地址并将其连接到您的 LAMP 实例上。有关更多信息，请参阅 Light sail 文档中的创建静态 IP 并将其附加到实例。

1. 在 Lightsail 主页的 “实例” 部分，选择正在运行的 LAMP 实例。



2. 选择联网选项卡，然后选择附加静态 IP。



3. 为您的静态 IP 命名，然后选择创建并附加。

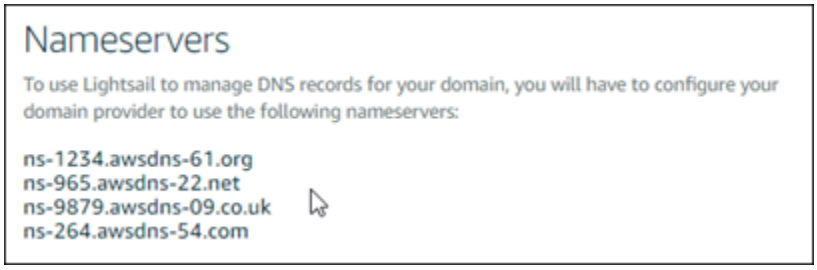


步骤 6：创建 DNS 区域并将域映射到 LAMP 实例

将您的域名 DNS 记录的管理权移交给 Lightsail。这使您可以更轻松地将域映射到您的 LAMP 实例，并使用 Lightsail 控制台管理网站的所有资源。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

1. 在 Lightsail 主页的域名和 DNS 部分，选择创建 DNS 区域。
2. 输入您的域，然后选择 Create DNS zone (创建 DNS 区域)。
3. 记下页面上列出的名称服务器地址。

   您将这些域名服务器地址添加到域名的注册商，将域名 DNS 记录的管理权转移到 Lightsail。



4. 将您的域名的 DNS 记录的管理转移到 Lightsail 后，添加一条 A 记录，将您的域名的顶点指向您的 LAMP 实例，如下所示：

   a. 在该 DNS 区域的 Assignments（分配）选项卡中，选择 Add assignment（添加分配）。

   b. 在 Select a domain（选择域）字段中，选择该域或子域。

c. 在 Select a resource（选择资源）下拉列表中，选择您在本教程前面创建的 LAMP 实例。

d. 选择 Assign（分配）。

在您的域开始将流量路由到 LAMP 实例之前，留出时间使更改传播到 Internet 的整个 DNS 中。

后续步骤

以下是在 Amazon Lightsail 中启动 LAMP 实例后可以执行的其他几个步骤：

- 创建 Linux 或 Unix 实例的快照
- 创建额外的数据块存储磁盘并将其附加到基于 Linux 的实例

将 Lightsail LAMP 实例连接到 Aurora 数据库

帖子、页面和用户的应用程序数据存储在您的 Amazon Lightsail 的 LAMP 实例上运行的 MariaDB 数据库中。如果实例出现故障，您的数据可能会变得无法恢复。要避免这种情况，您应将应用程序数据转移到一个 MySQL 托管式数据库中。

Amazon Aurora 是一种专为云构建的 MySQL 和 PostgreSQL 兼容关系数据库。它既具有传统企业数据库的性能和可用性，又具有开源数据库的简单性和成本效益。Aurora 作为 Amazon Relational Database Service（Amazon RDS）的一部分提供。Amazon RDS 是一项托管式数据库服务，让用户能够在云中更轻松地设置、操作和扩展关系数据库。有关更多信息，请参阅 Amazon Relational Database Service 用户指南和适用于 Aurora 的 Amazon Aurora 用户指南。

在本教程中，我们将向您展示如何将您的应用程序数据库从 Lightsail 中的 LAMP 实例连接到 Amazon RDS 中的 Aurora 托管数据库。

内容

- 步骤 1：完成先决条件
- 步骤 2：为您的 Aurora 数据库配置安全组
- 第 3 步：从 Lightsail 实例连接到你的 Aurora 数据库
- 步骤 4：将 MariaDB 数据库从 LAMP 实例转移到 Aurora 数据库
- 步骤 5：配置应用程序以连接到 Aurora 托管式数据库

步骤 1：完成先决条件

在开始之前，您需要首先满足以下先决条件：

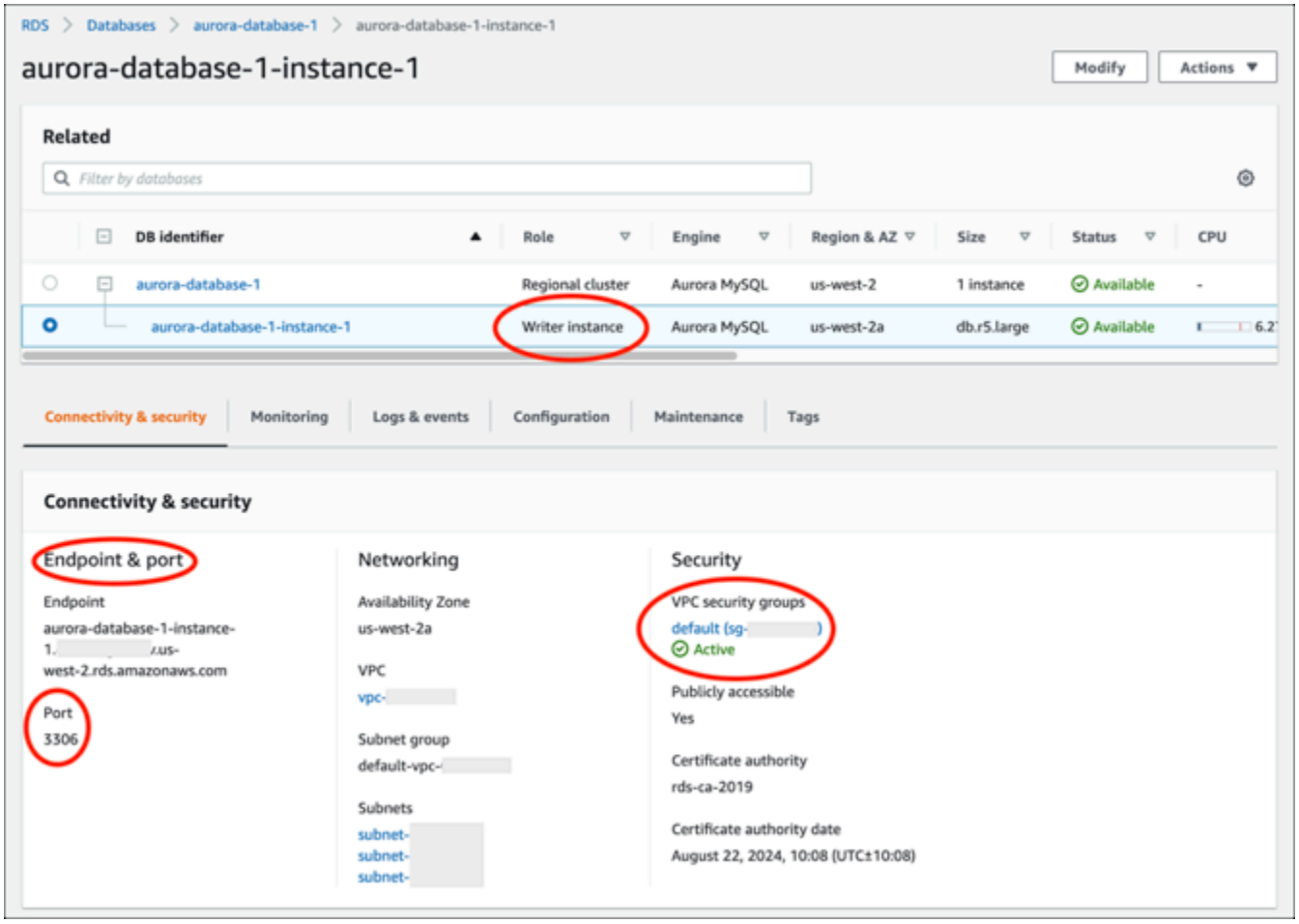
1. 在 Lightsail 中创建一个 LAMP 实例，并在其上配置您的应用程序。该实例的状态应处于正在运行后才能继续操作。有关更多信息，请参阅教程：在 Lightsail 中启动和配置 LAMP 实例。
2. 在你的 Lightsail 账户中开启 VPC 对等互连。有关更多信息，请参阅设置 Amazon VPC 对等互连以使用 Lightsail 之外的 AWS 资源。
3. 在 Amazon RDS 中创建 Aurora 托管式数据库。该数据库应位于与您的 LAMP 实例相同的 AWS 区域 中。其状态应处于正在运行后才能继续操作。有关更多信息，请参阅《适用于 Aurora 的 Amazon Aurora 用户指南》中的 Amazon Aurora 入门。

步骤 2：为您的 Aurora 数据库配置安全组

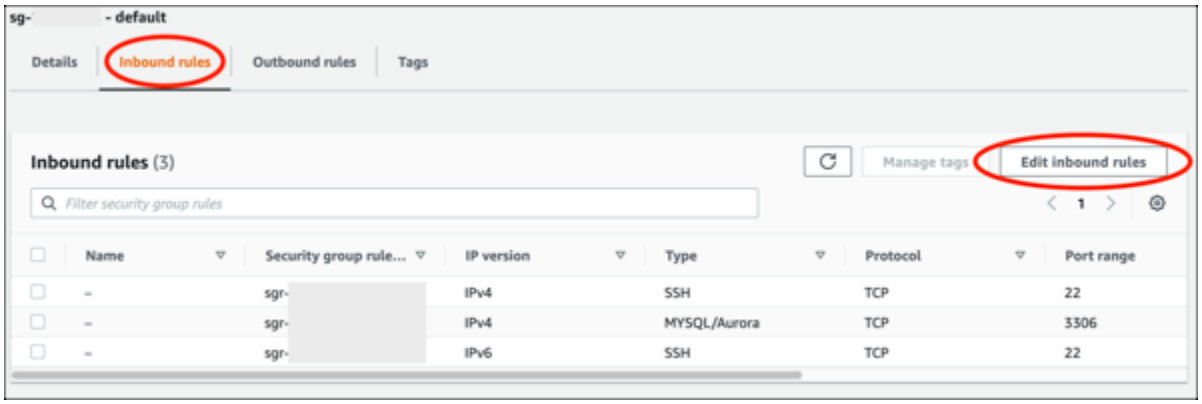
AWS 安全组充当 AWS 资源的虚拟防火墙。它会控制可以连接到 Amazon RDS 中的 Aurora 数据库的传入和传出流量。有关安全组的更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的使用安全组控制指向资源的流量。

按照以下过程完成安全组配置，以便您的 LAMP 实例可以建立到您的 Aurora 数据库的连接。

1. 登录 Amazon RDS 控制台。
2. 在导航窗格中选择 Databases (数据库)。
3. 选择您的 LAMP 实例将连接到的 Aurora 数据库的写入器实例。
4. 选择连接和安全性选项卡。
5. 在 Endpoint & port（终端节点和端口），记下 Writer instance（写入器实例）的 Endpoint name（终端节点名称）和 Port（端口）。稍后在配置 Lightsail 实例以连接到数据库时，您将需要这些信息。
6. 在 Security（安全性）部分，选择活动 VPC 安全组的链接。您将会重新导向到数据库的安全组。



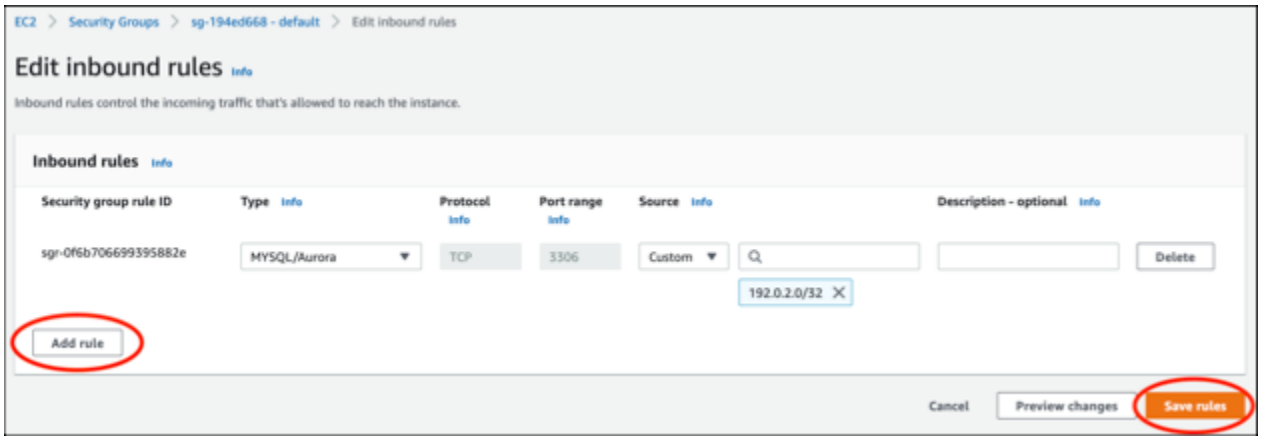
7. 确保已经选中您的 Aurora 数据库的安全组。
8. 选择入站规则选项卡。
9. 选择 Edit inbound rules（编辑入站规则）。



10. 在 Edit inbound rules（编辑入站规则）页面中，选择 Add rule（添加规则）。
11. 完成下列步骤之一：

- 如果您使用的是原定设置 MySQL 端口 3306，请在 Type（类型）下拉菜单中选择 MySQL/Aurora。
- 如果您使用的数据库的自定义端口，则在 Type（类型）下拉菜单中选择 Custom TCP（自定义 TCP），然后在 Port Range（端口范围）文本框中输入端口号。

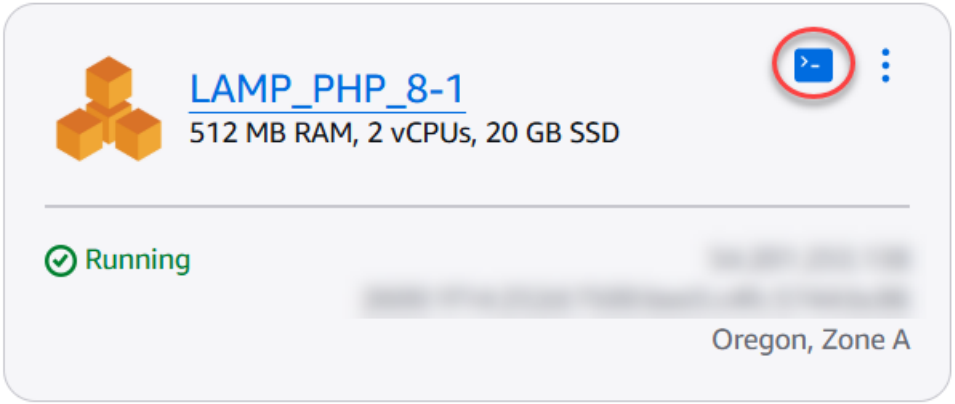
12. 在 Source（源）文本框中，添加 LAMP 实例的私有 IP 地址。您必须以 CIDR 表示法输入 IP 地址，这意味着必须在地址后附加 `/32`。例如，要允许 `192.0.2.0`，请输入 `192.0.2.0/32`。
13. 选择保存规则。



第 3 步：从 Lightsail 实例连接到你的 Aurora 数据库

完成以下过程以确认您可以从 Lightsail 实例连接到 Aurora 数据库。

1. 登录 Lightsail 控制台。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择 LAMP 实例的基于浏览器的 SSH 客户端图标，以使用 SSH 连接到数据库。



4. 连接到实例后，请输入以下命令以连接到您的 Aurora 数据库。在命令中，*DatabaseEndpoint*替换为 Aurora 数据库的终端节点地址，然后*Port*替换为数据库的端口。*MyUserName*替换为您在创建数据库时输入的用户名。

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

您应该会看到与以下示例类似的响应，其中确认您的实例可以访问并连接到您的 Aurora 数据库。

```
bitnami@ip-            $ mysql -h database.cluster-            .us-west-2.rds.amazonaws.
com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 215
Server version: 5.6.10 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

如果您没有看到此响应，或者收到错误消息，则可能需要将数据库的安全组配置为允许 Lightsail 实例的私有 IP 地址连接到该安全组。有关更多信息，请参阅此指南中的为您的 Aurora 数据库配置安全组部分。

步骤 4：将 MariaDB 数据库从 LAMP 实例转移到 Aurora 数据库

前面您确认了可以从实例连接到数据库，下面您需要将数据从 LAMP 实例数据库迁移到 Aurora 数据库。有关更多信息，请参阅《适用于 Aurora 的 Amazon Aurora 用户指南》中的将数据迁移到 Amazon Aurora MySQL 数据库集群。

步骤 5：配置应用程序以连接到 Aurora 托管式数据库

将应用程序数据转移到 Aurora 数据库中后，您需要配置在 LAMP 实例上运行的应用程序以连接到您的 Aurora 数据库。使用 SSH 连接到您的 LAMP 实例，然后访问该应用程序的数据库配置文件。在该配置文件中，定义 Aurora 数据库的端点地址、数据库用户名和密码。下面是一个配置文件示例：

```
bitnami@ip-            :~/htdocs$ cat connectvalues.php
<?php
$host           = 'database.cluster-            .us-west-2.rds.amazonaws.com';
$username       = 'admin';
$password       = 'Password1';
```

在 Lightsail 上启动和配置 Windows Server 2016 实例

如果你只需要虚拟专用服务器，Amazon Lightsail 是开始使用亚马逊网络服务 (AWS) 的最简单方法。Lightsail 以低廉且可预测的价格提供快速启动项目所需的一切，包括虚拟机、基于 SSD 的存储、数据传输、DNS 管理和静态 IP。

本教程向你展示了如何在 Lightsail 上启动和配置 Windows Server 2016 实例。其步骤包括通过 RDP 连接到您的实例，创建静态 IP 并将其附加到实例上，以及创建 DNS 区域并映射域。完成本教程后，你就具备了在 Lightsail 上启动和运行实例的基础知识。

内容

- 步骤 1：注册亚马逊云科技
- 步骤 2：创建 Windows Server 2016 实例
- 步骤 3：通过 RDP 连接到 Windows Server 2016 实例
- 步骤 4：创建静态 IP 地址并将其附加到 Windows Server 2016 实例
- 步骤 5：创建 DNS 区域并将域映射到 Windows Server 2016 实例
- 后续步骤

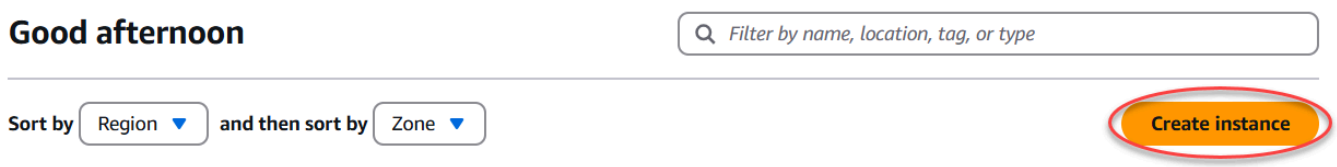
步骤 1：注册亚马逊云科技

本教程需要一个 AWS 帐户。注册 AWS或登录（ AWS如果您已经有一个帐户）。

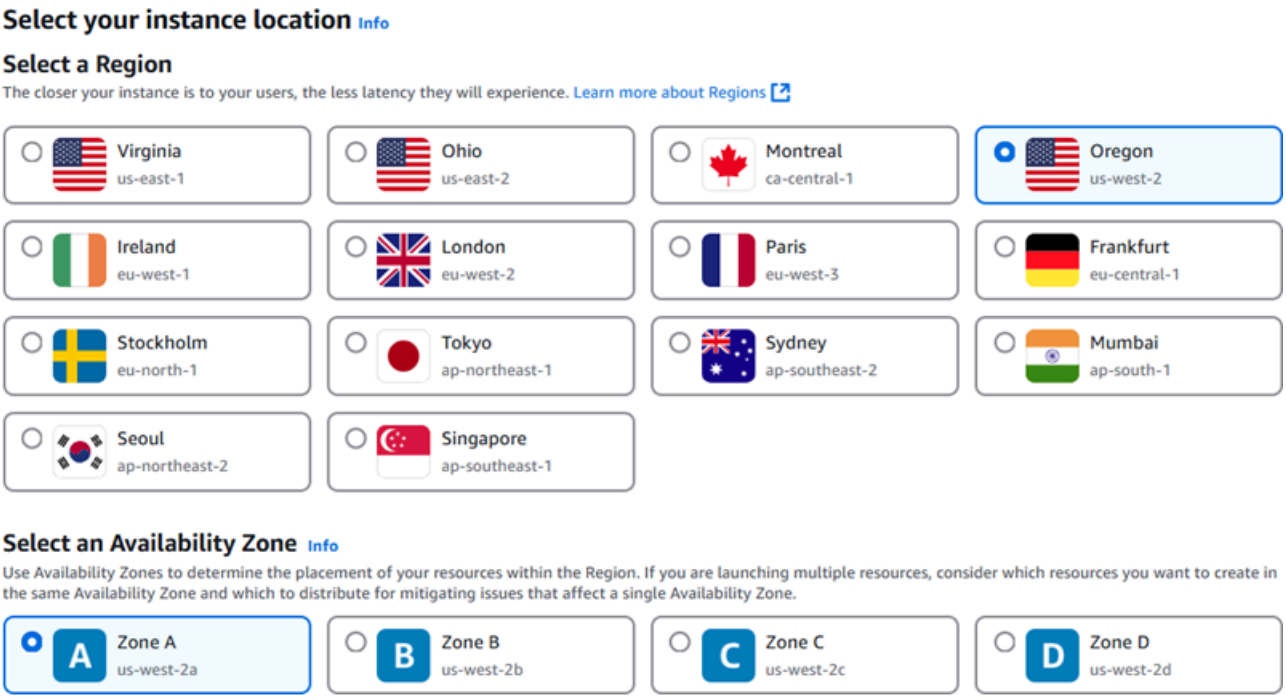
第 2 步：在 Lightsail 中创建 Windows Server 2016 实例

在 Lightsail 中启动并运行你的 Windows Server 2016 实例。有关更多信息，请参阅基于 Windows Server 的实例入门。

1. 登录 Lightsail 控制台。
2. 在 Lightsail 主页的实例部分，选择创建实例。



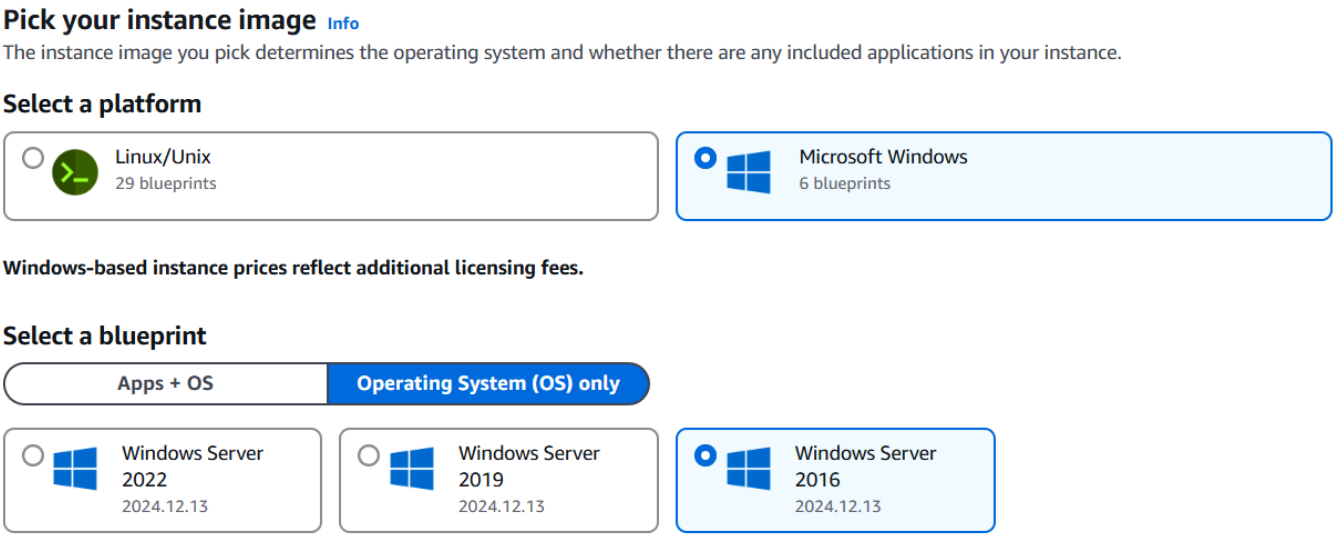
3. 为您的实例选择 AWS 区域 和可用区。



4. 选择您的实例映像。

   a. 将 Microsoft Windows 选作为平台。

   b. 选择仅限操作系统，然后将 Windows Server 2016 选作为蓝图。



5. 选择实例计划。

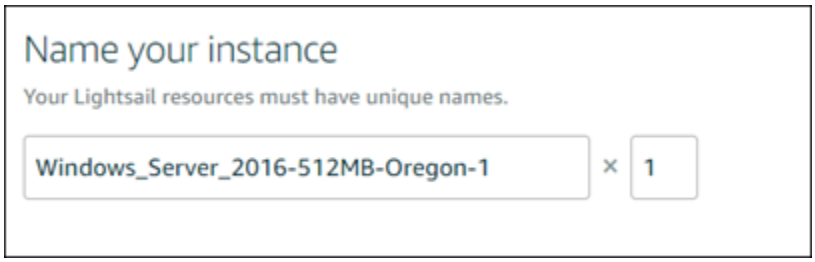
计划包括可预测的低成本、计算机配置 (RAM、SSD、vCPU) 以及数据传输限额。你可以免费试用 9.50 美元的 Lightsail 套餐一个月（最长 750 小时）。 AWS 将一个月的免费积分存入您的账户。

> **Note**
>
> 作为 AWS 免费套餐的一部分，您可以免费开始使用特定实例捆绑包的 Amazon Lightsail。有关更多信息，请参阅亚马逊 Lightsail 定价页面上的AWS 免费套餐。

6. 输入实例的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。



7. （可选）选择添加新标签以向您的实例添加标签。根据需要重复此步骤以添加其他标签。有关标签使用的更多信息，请参阅标签。

   a. 对于密钥，输入标签密钥。



   b. （可选）在“值”中，输入标签值。

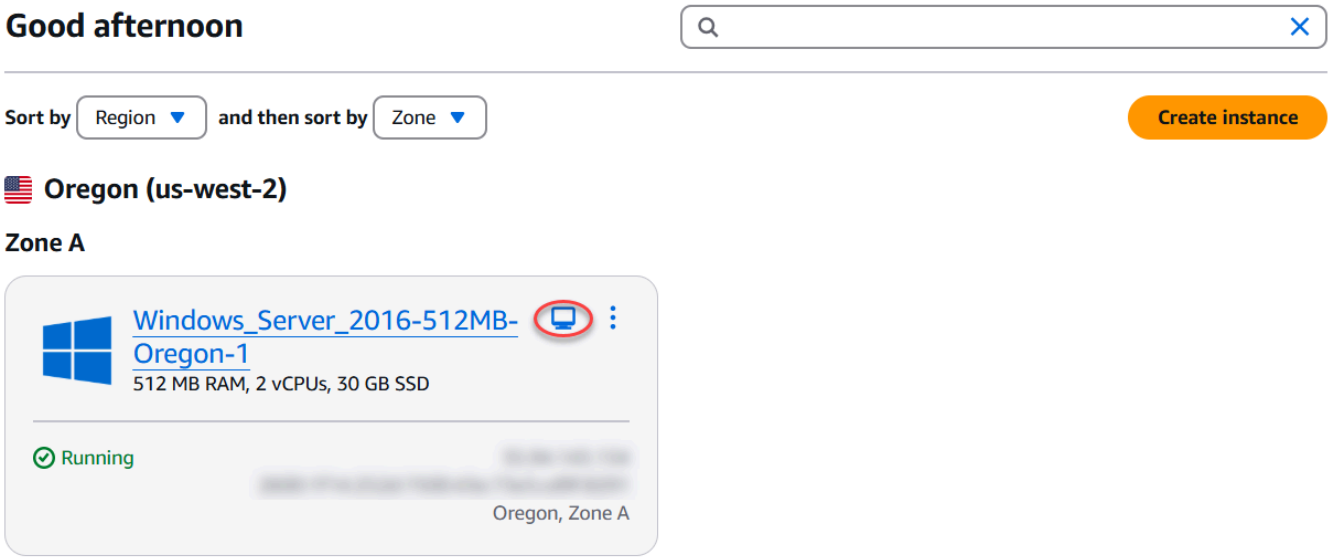


8. 选择创建实例。

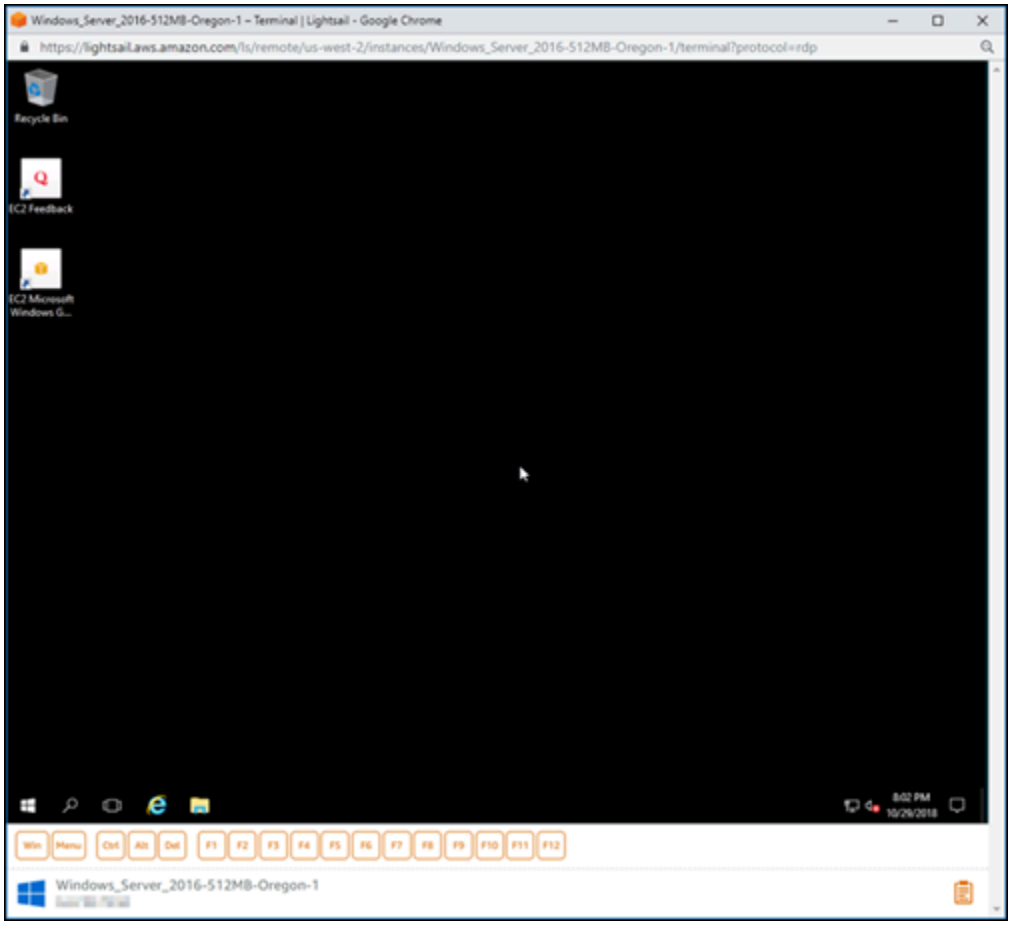
步骤 3：通过 RDP 连接到 Windows Server 2016 实例

在 Lightsail 控制台中使用基于浏览器的 RDP 客户端连接到你的 Windows Server 2016 实例。有关更多信息，请参阅连接到 Windows 实例。

1. 在 Lightsail 主页的 “实例” 部分，选择 Windows Server 2016 实例的 RDP 快速连接图标。



2. 系统打开基于浏览器的 RDP 客户端窗口后，您便可以开始配置 Windows Server 2016 实例：

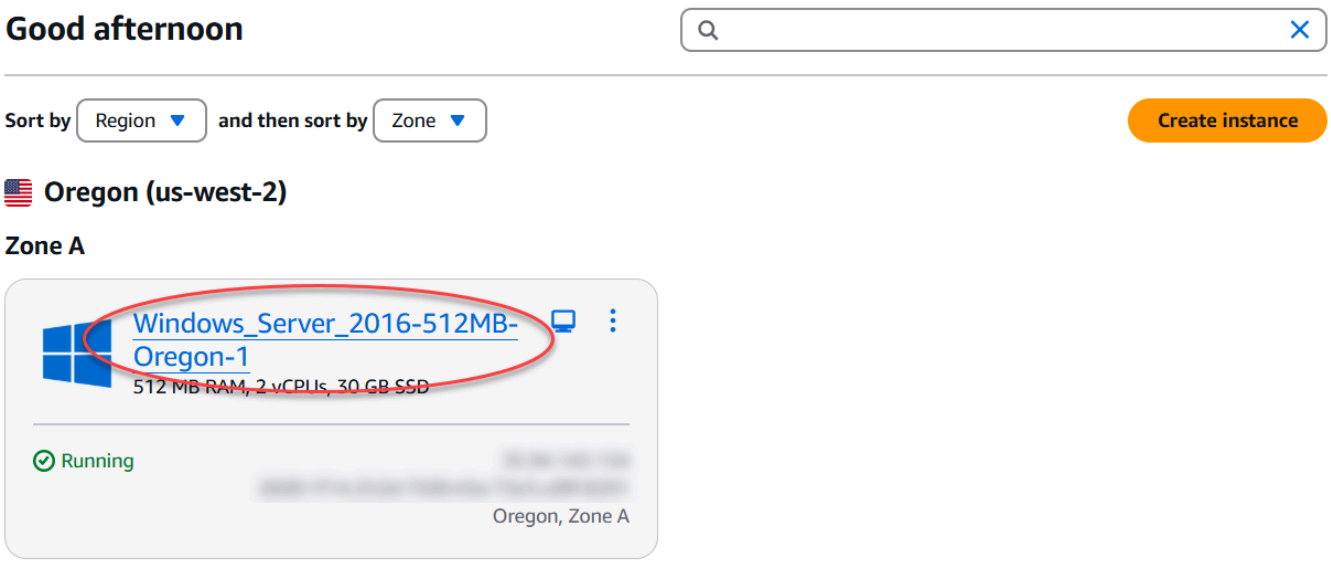


步骤 4：创建静态 IP 地址并将其附加到 Windows Server 2016 实例

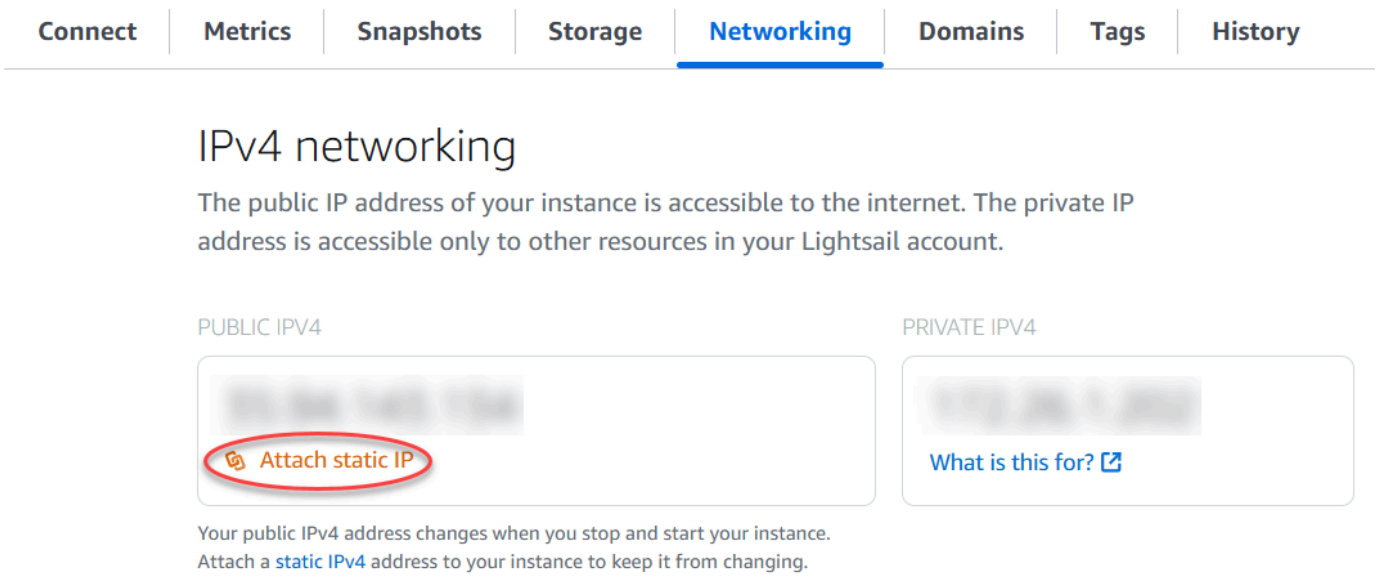
如果您停止并启动 Windows Server 2016 实例，则该实例的默认公有 IP 会发生变化。即使您停止和启动您的实例，连接到该实例的静态 IP 地址也会保持不变。

创建静态 IP 地址并将其附加到您的 Windows Server 2016 实例上。有关更多信息，请参阅 Light sail 文档中的创建静态 IP 并将其附加到实例。

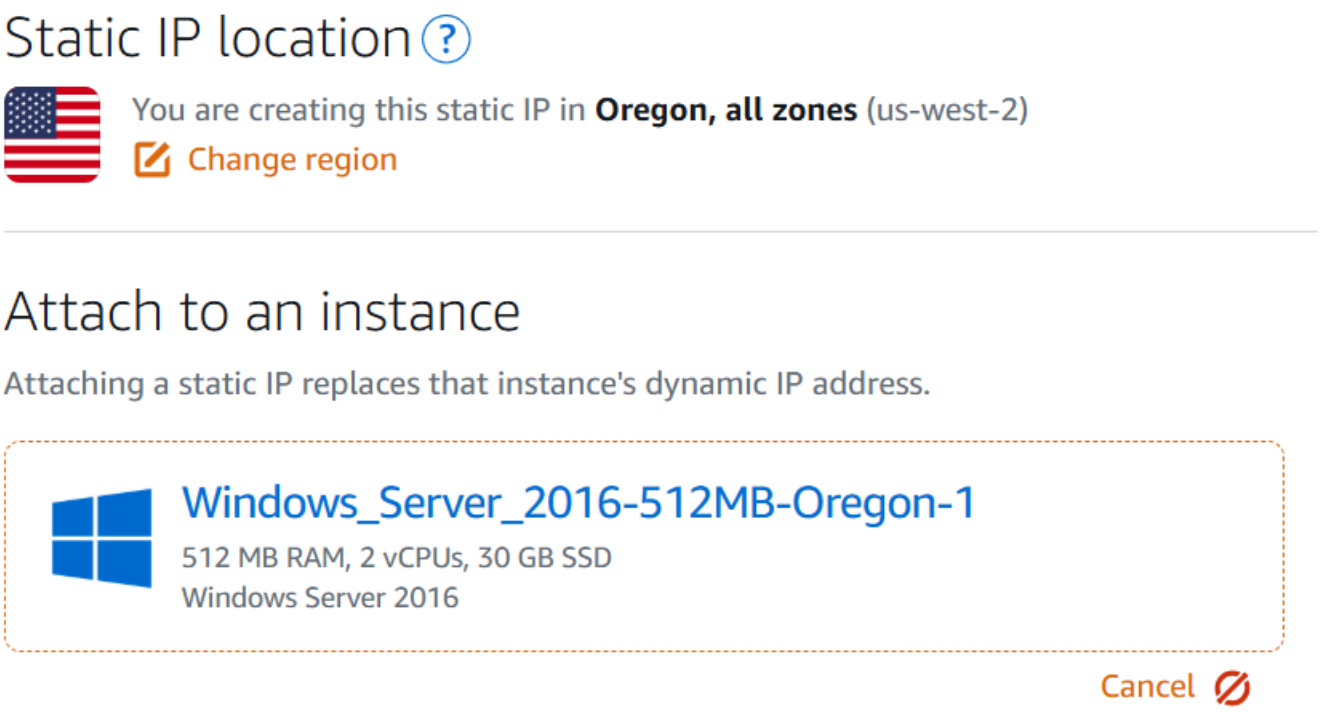
1. 在 Lightsail 主页的 “实例” 部分，选择你正在运行的 Windows Server 2016 实例。



2. 选择 Networking (联网) 选项卡，然后选择 Create static IP (创建静态 IP)。



3. 静态 IP 位置以及连接到的实例是根据您在本教程中前面部分选择的实例预先选择的。



4. 输入静态 IP 的名称。

   资源名称：

   - 在你的 Lightsail 账户 AWS 区域 中，每个账户中必须是唯一的。
   - 必须包含 2 到 255 个字符。
   - 必须以字母数字字符或数字作为开头和结尾。
   - 可以包括字母数字字符、数字、句点、连字符和下划线。

5. 选择 Create（创建）。

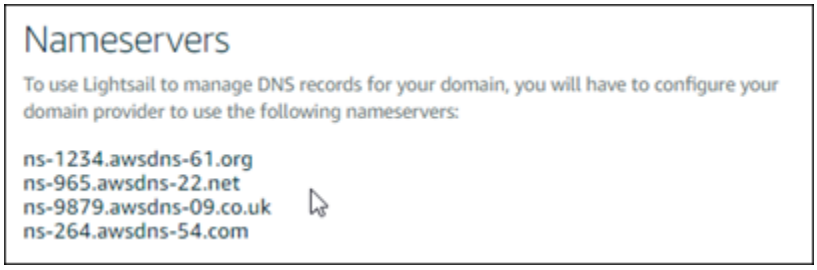


步骤 5：创建 DNS 区域并将域映射到 Windows Server 2016 实例

将您的域名 DNS 记录的管理权移交给 Lightsail。这使您可以更轻松地将域映射到 Windows Server 2016 实例，并使用 Lightsail 控制台管理网站的所有资源。有关更多信息，请参阅 Light sail 文档中的创建 DNS 区域来管理您的域名的 DNS 记录。

1. 在 Lightsail 主页的域名和 DNS 部分，选择创建 DNS 区域。
2. 输入您的域，然后选择 Create DNS zone (创建 DNS 区域)。
3. 记下页面上列出的名称服务器地址。

   您将这些域名服务器地址添加到域名的注册商，将域名 DNS 记录的管理权转移到 Lightsail。



4. 将您的域名的 DNS 记录的管理转移到 Lightsail 后，添加一条 A 记录，将您的域名的顶点指向您的 LAMP 实例，如下所示：

   a. 在该 DNS 区域的 Assignments（分配）选项卡中，选择 Add assignment（添加分配）。

   b. 在 Select a domain（选择域）字段中，选择该域或子域。

c. 在 Select a resource（选择资源）下拉列表中，选择您在本教程前面创建的 LAMP 实例。

d. 选择 Assign（分配）。

在您的域开始将流量路由到 LAMP 实例之前，留出时间使更改传播到 Internet 的整个 DNS 中。

后续步骤

以下是在 Amazon Lightsail 中启动 Windows Server 2016 实例后可以执行的其他几个步骤：

- 创建 Windows Server 实例的快照
- 保护基于 Windows 服务器的 Lightsail 实例的最佳实践
- 创建数据块存储磁盘并将其附加到 Windows Server 实例
- 扩展 Windows Server 实例的存储空间

使用监控 Lightsail API 活动 AWS CloudTrail

Amazon Lightsail 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 Lightsail 中采取的操作的记录。 CloudTrail 将 Lightsail 的所有 API 调用捕获为事件。捕获的调用包括来自 Lightsail 控制台的调用和对 Lightsail API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Lightsail 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 Lightsail 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

Lightsail 中的信息 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 Lightsail 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户中的事件，包括 Lightsail 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

所有 Lightsail 操作均由《亚马逊 Lightsail API 参考》记录 CloudTrail 并记录在案。例如，调用GetInstance、AttachStaticIp和RebootInstance节会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Lightsail 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

创建 HAR 文件来解决 Lightsail 问题

如果您在使用 Amazon Lightsail 控制台或 Lightsail 虚拟专用服务器 (VPS) 时遇到困难， 支持 可能会要求您通过网络浏览器提交 HAR 文件。HAR 文件包含可帮助解决常见且难以诊断的问题的关键信息。HAR 文件还 支持 允许调查或复制这些问题。

> **Important**
>
> HAR 文件可以捕获敏感信息，例如用户名、密码和密钥。在共享之前，请务必从 HAR 文件中删除任何敏感信息。

在本指南中，您将了解如何从 Web 浏览器创建 HAR 文件。HTTP 存档（HAR）文件是一个 JSON 文件，它包含浏览器记录的最新网络活动。按照以下 step-by-step步骤创建 HAR 文件。

内容

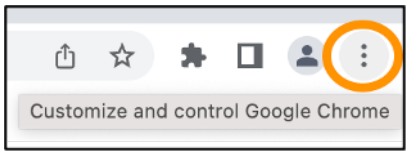
- Step 1: Create a HAR file in your browser（步骤 1：在浏览器中创建 HAR 文件）
- Step 2: Edit the HAR file to remove sensitive information（步骤 2：编辑 HAR 文件以删除敏感信息）
- Step 3: Submit the HAR file for review（步骤 3：提交 HAR 文件以供审核）

步骤 1：在浏览器中创建 HAR 文件

> **Note**
>
> 这些说明的最新测试是在 Google Chrome 版本 101.0.4951.64、Microsoft Edge（Chromium）版本 101.0.1210.47 和 Mozilla Firefox 版本 91.9 上进行的。由于这些浏览器是第三方产品，因此这些说明可能与最新版本或您所使用版本中的体验不符。在其他浏览器中，例如旧版 Microsoft Edge（EdgeHTML）或 Apple Safari for macOS，生成 HAR 文件的过程可能类似，但步骤会有所不同。

Google Chrome

1. 在浏览器的右上角，选择 Customize and control Google Chrome（自定义和控制 Google Chrome）。

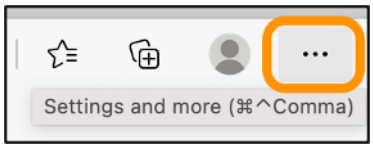


2. 在 More tools（更多工具）上暂停，然后选择 Developer tools（开发人员工具）。
3. 在浏览器中 DevTools 打开后，选择 “网络” 面板。
4. 选中 Preserve log（保留日志）复选框。
5. 选择 Clear（清除）以清除所有当前的网络请求。
6. 重现您面临的问题
7. 在中 DevTools，打开任何网络请求的上下文（右键单击）菜单。
8. 选择 Save all as HAR with content（将所有内容保存为 HAR），然后保存该文件。

如需了解更多信息，请参阅 Google 开发者网站上的打开 Chrome DevTools 和将所有网络请求保存到 HAR 文件。

Microsoft Edge (Chromium)

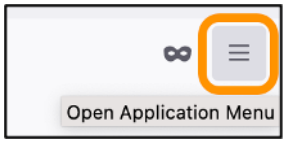
1. 在浏览器的右上角，选择 Settings and more（设置和更多）。



2. 在 More tools（更多工具）上暂停，然后选择 Developer tools（开发人员工具）。
3. 在浏览器中 DevTools 打开后，选择 “网络” 面板。
4. 选中 Preserve log（保留日志）复选框。
5. 选择 Clear（清除）以清除所有当前的网络请求。
6. 重现您面临的问题
7. 在中 DevTools，打开任何网络请求的上下文（右键单击）菜单。
8. 选择 Save all as HAR with content（将所有内容保存为 HAR），然后保存该文件。

Mozilla Firefox

1. 在浏览器的右上角，选择 Open Application Menu（打开应用程序菜单）。



2. 选择 More tools（更多工具），然后选择 Web Developer tools（Web 开发人员工具）。
3. 在 Web Developer（Web 开发人员）菜单中，选择 Network（网络）。（在某些版本的 Firefox 中，Web Developer（Web 开发人员）菜单位于 Tools（工具）菜单。）
4. 选择齿轮图标，然后选择 Persist Logs（永久性日志）。
5. 选择垃圾桶图标（Clear（清除））以清除所有当前的网络请求。
6. 重现您面临的问题。
7. 在网络监视器中，打开请求列表中任何网络请求的上下文菜单（右键单击）。
8. 选择 Save All As HAR（全部另存为 HAR），然后保存该文件。

步骤 2：编辑 HAR 文件以删除敏感信息

1. 在文本编辑器应用程序中打开 HAR 文件。
2. 使用文本编辑器的查找和替换工具来识别和替换 HAR 文件中捕获的所有敏感信息。这包括您在创建文件时在浏览器中输入的任何用户名、密码和密钥。
3. 保存已删除的敏感信息的编辑后 HAR 文件。

步骤 3：提交 HAR 文件以供审核

1. 在 AWS Support Center Console 的提交支持案例下，选择您的支持案例。
2. 在您的支持案例中，选择首选联系人选项，附加编辑后的 HAR 文件，然后提交。

在 Lightsail 上使用 Prometheus 监控系统资源和应用程序

Prometheus 是一款开源时间序列监控工具，用于管理各种系统资源和应用程序。它通过 Grafana 提供了多维数据模型、查询所收集数据的能力以及详细的报告和数据可视化。

默认情况下，Prometheus 可以在安装它的服务器上收集指标。在节点导出器的帮助下，可以从 Web 服务器、容器、数据库、自定义应用程序和其他第三方系统等其他资源收集指标。在本教程中，我们将向你展示如何在 Lightsail 实例上安装和配置带有节点导出器的 Prometheus。有关可用导出器的完整列表，请参阅 Prometheus 文档中的 Exporters and integrations（导出器和集成）。

内容

- 步骤 1：完成先决条件
- 步骤 2：将用户和本地系统目录添加到 Lightsail 实例
- 步骤 3：下载 Prometheus 二进制包
- 步骤 4：配置 Prometheus
- 步骤 5：启动 Prometheus
- 步骤 6：启动 Node Exporter
- 步骤 7：使用 Node Exporter 数据收集器配置 Prometheus

步骤 1：完成先决条件

在亚马逊 Lightsail 实例上安装 Prometheus 之前，您必须执行以下操作：

- 在 Lightsail 中创建一个实例。我们建议为实例使用 Ubuntu 20.04 LTS 蓝图。有关更多信息，请参阅在 Amazon Lightsail 中创建实例。
- 创建静态 IP 地址并将其挂载到新实例。有关更多信息，请参阅在 Amazon Lightsail 中创建静态 IP 地址。
- 在新实例的防火墙上打开端口 9090 和 9100。Prometheus 要求打开端口 9090 和 9100。有关更多信息，请参阅在 Amazon Lightsail 中添加和编辑实例防火墙规则。

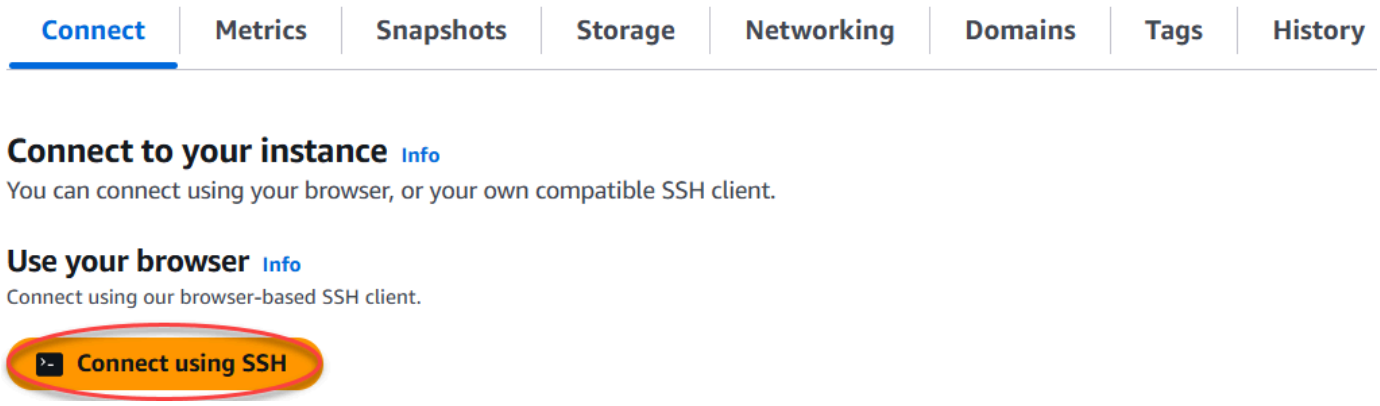
步骤 2：将用户和本地系统目录添加到 Lightsail 实例

完成以下步骤，使用 SSH 连接到您的 Lightsail 实例，并添加用户和系统目录。此过程创建以下 Linux 用户账户：

- `prometheus` – 此账户用于安装和配置服务器环境。
- `exporter` – 此账户用于配置 `node_exporter` 扩展。

创建这些用户账户仅用于管理目的，因此不需要超出此设置范围的其他用户服务或权限。在此过程中，您还将创建目录，用于存储和管理 Prometheus 用于监控资源的文件、服务设置和数据。

1. 登录 Lightsail 控制台。
2. 在实例管理页面上的 Connect（连接）选项卡下，选择使用 SSH 连接。



3. 连接后，逐个输入以下命令以创建两个 Linux 用户账户：`prometheus` 和 `exporter`。

```
sudo useradd --no-create-home --shell /bin/false prometheus
```

```
sudo useradd --no-create-home --shell /bin/false exporter
```

4. 逐个输入以下命令以创建本地系统目录。

```
sudo mkdir /etc/prometheus /var/lib/prometheus
```

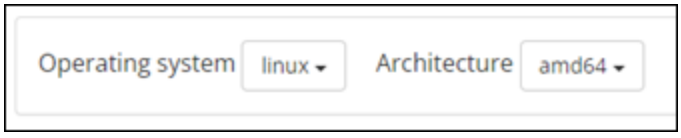
```
sudo chown prometheus:prometheus /etc/prometheus
```

```
sudo chown prometheus:prometheus /var/lib/prometheus
```

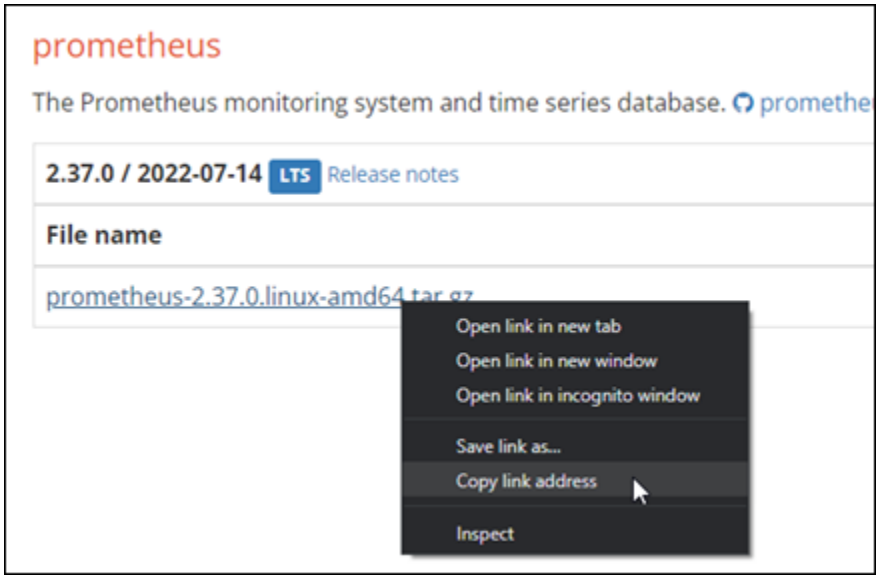
步骤 3：下载 Prometheus 二进制包

完成以下过程，将 Prometheus 二进制包下载到你的 Lightsail 实例。

1. 在本地计算机上打开 Web 浏览器，然后浏览到 Prometheus 下载页面。
2. 对于页面顶部的 Operating system（操作系统）下拉列表，选择 linux。对于 Architecture（架构），选择 amd64。



3. 选择或右键单击出现的 Prometheus 下载链接，然后将链接地址复制到计算机上的文本文件中。对出现的 node_exporter 下载链接执行相同操作。您将在此过程后面的部分使用这两个复制的地址。



4. 使用 SSH 连接到你的 Lightsail 实例。
5. 输入以下命令以将目录更改为您的主目录。

```
cd ~
```

6. 输入以下命令以将 Prometheus 二进制包下载到您的实例。

```
curl -LO prometheus-download-address
```

*prometheus-download-address*替换为您在本过程中之前复制的地址。添加该地址后，命令应类似于以下示例。

```
curl -LO https://github.com/prometheus/prometheus/releases/download/v2.37.0/
prometheus-2.37.0.linux-amd64.tar.gz
```

7. 输入以下命令以将 node_exporter 二进制包下载到您的实例。

```
curl -LO node_exporter-download-address
```

*node_exporter-download-address*替换为您在此过程的上一步中复制的地址。添加该地址后，命令应类似于以下示例。

```
curl -LO https://github.com/prometheus/node_exporter/releases/download/v1.3.1/
node_exporter-1.3.1.linux-amd64.tar.gz
```

8. 逐个运行以下命令以解压缩下载的 Prometheus 和 Node Exporter 文件的内容。

```
tar -xvf prometheus-2.37.0.linux-amd64.tar.gz
```

```
tar -xvf node_exporter-1.3.1.linux-amd64.tar.gz
```

解压缩已下载文件的内容后，会创建多个子目录。

9. 逐个输入以下命令，将 prometheus 和 promtool 解压缩文件复制到 /usr/local/bin 程序目录。

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus /usr/local/bin
```

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/promtool /usr/local/bin
```

10. 输入以下命令，将 prometheus 和 promtool 文件的所有权更改为您在本教程前面部分创建的 prometheus 用户。

```
sudo chown prometheus:prometheus /usr/local/bin/prom*
```

11. 逐个输入以下命令以将 consoles 和 console_libraries 子目录复制到 /etc/prometheus。-r 选项对层次结构中的所有目录执行递归复制。

```
sudo cp -r ./prometheus-2.37.0.linux-amd64/consoles /etc/prometheus
```

```
sudo cp -r ./prometheus-2.37.0.linux-amd64/console_libraries /etc/prometheus
```

12. 逐个输入以下命令，将所复制文件的所有权更改为您在本教程前面部分创建的 prometheus 用户。-R 选项对层次结构中的所有文件和目录执行递归所有权更改。

```
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
```

```
sudo chown -R prometheus:prometheus /etc/prometheus/console_libraries
```

13. 逐个输入以下命令，将配置文件 prometheus.yml 复制到 /etc/prometheus 目录，然后将所复制文件的所有权更改为您在本教程前面部分创建的 prometheus 用户。

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus.yml /etc/prometheus
```

```
sudo chown prometheus:prometheus /etc/prometheus/prometheus.yml
```

14. 输入以下命令，将 node_exporter 文件从 ./node_exporter* 子目录复制到 /usr/local/bin 程序目录。

```
sudo cp -p ./node_exporter-1.3.1.linux-amd64/node_exporter /usr/local/bin
```

15. 输入以下命令，将文件的所有权更改为您在本教程前面部分创建的 exporter 用户。

```
sudo chown exporter:exporter /usr/local/bin/node_exporter
```

步骤 4：配置 Prometheus

完成以下过程来配置 Prometheus。在此过程中，您将打开并编辑 prometheus.yml 文件，其中包含 Prometheus 工具的各种设置。Prometheus 根据您在文件中配置的设置建立监控环境。

1. 使用 SSH 连接到你的 Lightsail 实例。
2. 输入以下命令，在打开和编辑该文件之前创建 prometheus.yml 文件的备份副本。

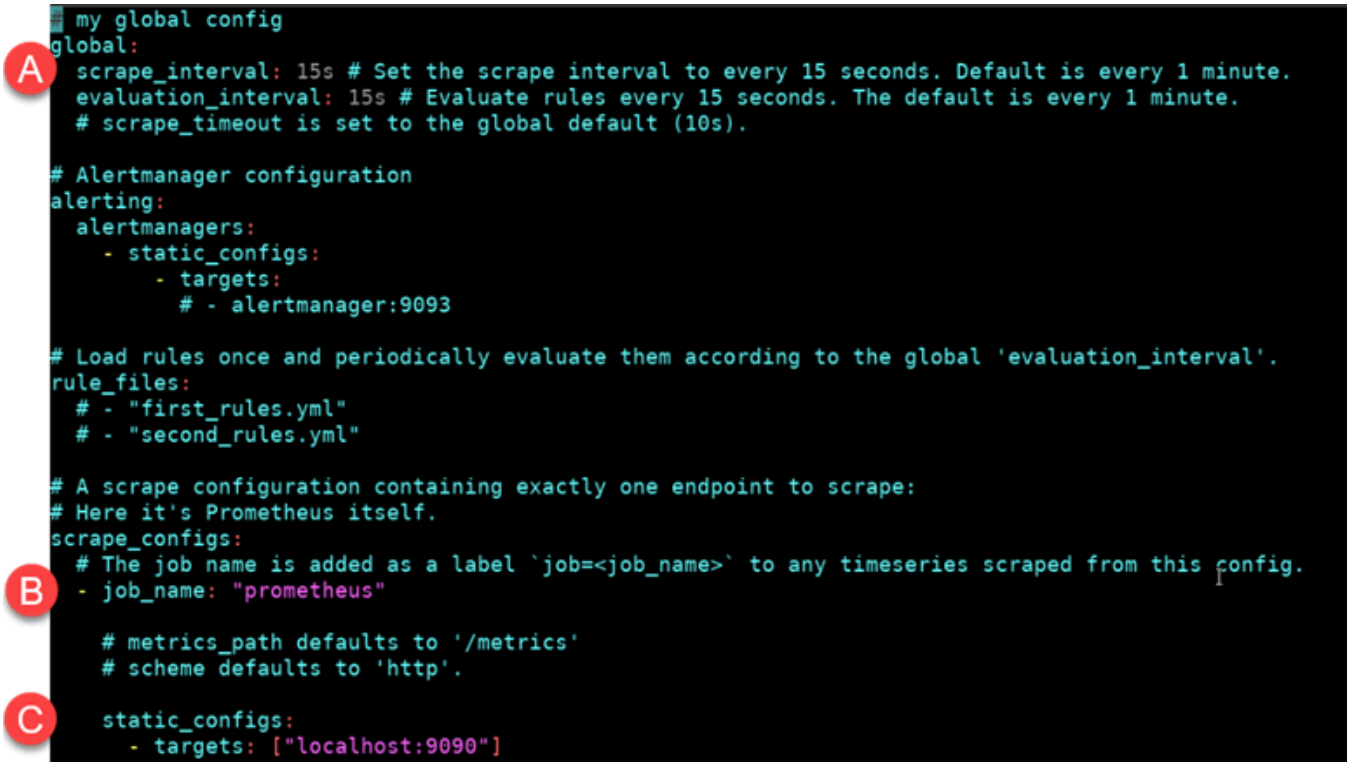
```
sudo cp /etc/prometheus/prometheus.yml /etc/prometheus/prometheus.yml.backup
```

3. 输入以下命令以使用 Vim 打开 prometheus.yml 文件。

```
sudo vim /etc/prometheus/prometheus.yml
```

以下是您可能希望在 prometheus.yml 文件中配置的一些重要参数：

- scrape_interval – 此参数位于 global 标头下，定义 Prometheus 收集或抓取给定目标指标数据频率的时间间隔（单位为秒）。如 global 标签所指示，此设置对 Prometheus 监控的所有资源通用。除非单个导出器提供覆盖全局值的不同值，否则此设置也适用于导出器。您可以将此参数设置为其当前值 15 秒。
- job_name – 此参数位于 scrape_configs 标头下，是标识数据查询或可视化显示结果集中导出器的标签。您可以指定作业名称的值，以最好地反映环境中正在监控的资源。例如，您可以将管理网站的作业标记为 business-web-app，也可以将数据库标记为 mysql-db-1。在此初始设置中，您仅监控 Prometheus 服务器，因此可以保留当前 prometheus 值。
- targets – targets 设置位于 static_configs 标头下，使用 ip_addr:port 键值对标识给定导出器运行的位置。您将在此过程的步骤 4-7 中更改默认设置。



> **Note**
>
> 对于此初始设置，不需要配置 `alerting` 和 `rule_files` 参数。

4. 在 Vim 中已打开的 `prometheus.yml` 文件中，按 I 键进入 Vim 的插入模式。
5. 滚动并找到位于 `static_configs` 标头下的 `targets` 参数。
6. 将默认设置更改为 *<ip_addr>*:9090。将 *<ip_addr>* 替换为实例的静态 IP 地址。修改后的参数应类似于以下示例。

```
static_configs:
  - targets: ["192.0.2.0:9090"]
```

7. 按 ESC 键退出插入模式，然后键入 :wq! 保存更改并退出 Vim。
8. （可选）如果出现问题，请输入以下命令，以将 `prometheus.yml` 文件替换为在此过程前面部分创建的备份。

```
sudo cp /etc/prometheus/prometheus.yml.backup /etc/prometheus/prometheus.yml
```

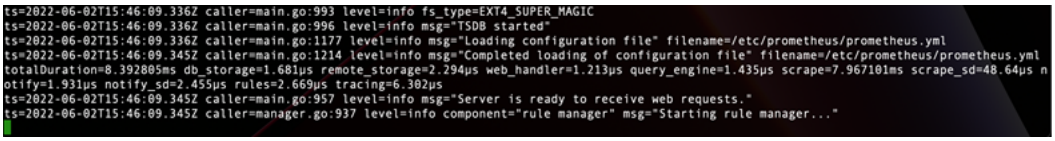
步骤 5：启动 Prometheus

完成以下过程以在实例上启动 Prometheus 服务。

1. 使用 SSH 连接到你的 Lightsail 实例。
2. 输入以下命令以启动 Prometheus 服务。

```
sudo -u prometheus /usr/local/bin/prometheus --config.file /etc/prometheus/
prometheus.yml --storage.tsdb.path /var/lib/prometheus --web.console.templates=/
etc/prometheus/consoles --web.console.libraries=/etc/prometheus/console_libraries
```

命令行输出有关启动过程和其他服务的详细信息。它还应表明该服务正在监听端口 9090。



如果服务未启动，请参阅本教程的步骤 1：完成先决条件部分，了解有关创建实例防火墙规则以允许此端口上流量的信息。对于其他错误，请查看 `prometheus.yml` 文件以确认没有语法错误。

3. 验证正在运行的服务后，按 Ctrl+C 停止该服务。
4. 输入以下命令以在 Vim 中打开 `systemd` 配置文件。此文件用于启动 Prometheus。

```
sudo vim /etc/systemd/system/prometheus.service
```

5. 将以下行插入到该文件中。

```
[Unit]
Description=PromServer
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
--config.file /etc/prometheus/prometheus.yml \
--storage.tsdb.path /var/lib/prometheus/ \
--web.console.templates=/etc/prometheus/consoles \
--web.console.libraries=/etc/prometheus/console_libraries
```

```
[Install]
WantedBy=multi-user.target
```

Linux systemd 服务管理器使用前面的指令在服务器上启动 Prometheus。调用时，Prometheus 以 prometheus 用户身份运行并引用 prometheus.yml 文件以加载配置设置并将时间序列数据存储在 /var/lib/prometheus 目录中。您可以从命令行运行 man systemd，以查看关于该服务的更多信息。

6. 按 ESC 键退出插入模式，然后键入 :wq! 保存更改并退出 Vim。
7. 输入以下命令以将信息加载到 systemd 服务管理器。

```
sudo systemctl daemon-reload
```

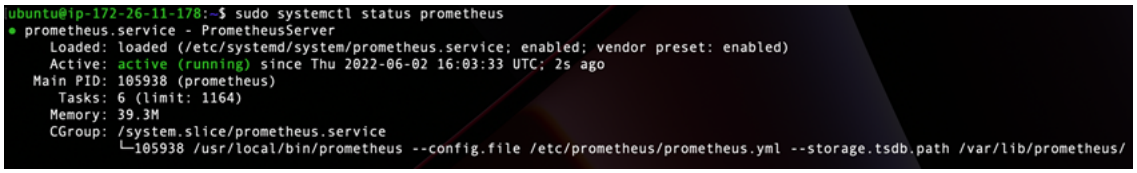
8. 输入以下命令以重新启动 Prometheus。

```
sudo systemctl start prometheus
```

9. 输入以下命令以查看 Prometheus 服务的状态。

```
sudo systemctl status prometheus
```

如果服务正常启动，您将收到类似于以下示例的输出。



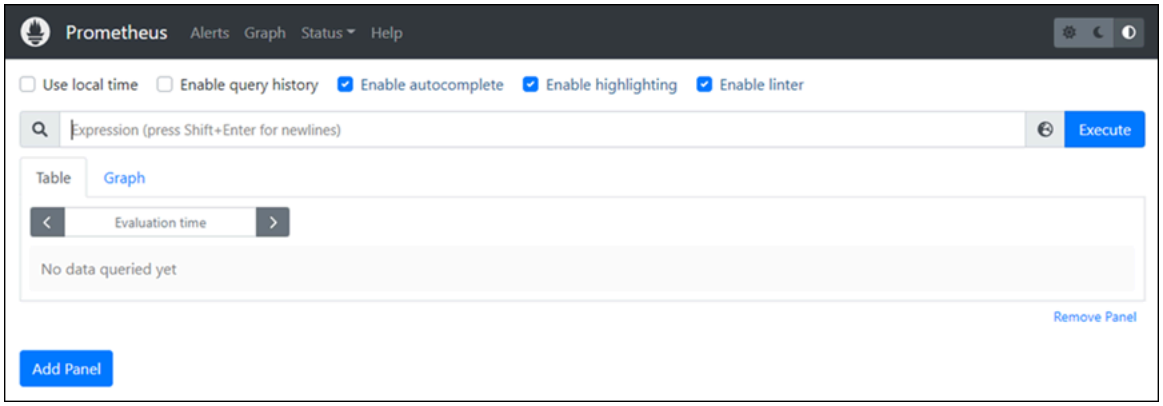
10. 按 Q 退出状态命令。
11. 输入以下命令，使 Prometheus 能够在实例启动时启动。

```
sudo systemctl enable prometheus
```

12. 在本地计算机上打开 Web 浏览器，然后转到以下网址查看 Prometheus 管理界面。

```
http:<ip_addr>:9090
```

*<ip_addr>*替换为您的 Lightsail 实例的静态 IP 地址。您应看到类似于以下示例的控制面板。



步骤 6：启动 Node Exporter

完成以下过程以启动 Node Exporter 服务。

1. 使用 SSH 连接到你的 Lightsail 实例。
2. 输入以下命令，使用 Vim 为 `node_exporter` 创建 `systemd` 服务文件。

```
sudo vim /etc/systemd/system/node_exporter.service
```

3. 在 Vim 中按 I 键以进入插入模式。
4. 将以下几行文本添加到文件中。这将为 `node_exporter` 配置 CPU 负载、文件系统使用和内存资源的监控收集器。

```
[Unit]
Description=NodeExporter
Wants=network-online.target
After=network-online.target

[Service]
User=exporter
Group=exporter
Type=simple
ExecStart=/usr/local/bin/node_exporter --collector.disable-defaults \
--collector.meminfo \
--collector.loadavg \
--collector.filesystem

[Install]
WantedBy=multi-user.target
```

> **Note**
>
> 这些说明禁用 Node Exporter 的默认机器指标。有关 Ubuntu 可用指标的完整列表，请参阅 Ubuntu 文档中的 Prometheus node_exporter 手册页。

5. 按 ESC 键退出插入模式，然后键入 :wq! 保存更改并退出 Vim。
6. 输入以下命令以重新加载 `systemd` 进程。

```
sudo systemctl daemon-reload
```

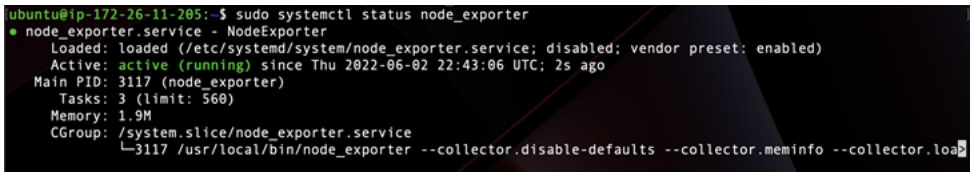
7. 输入以下命令以启动 `node_exporter` 服务。

```
sudo systemctl start node_exporter
```

8. 输入以下命令以查看 `node_exporter` 服务的状态。

```
sudo systemctl status node_exporter
```

如果服务成功启动，您将收到类似于以下示例的输出。



9. 按 Q 退出状态命令。
10. 输入以下命令，使 Node Exporter 能够在实例启动时启动。

```
sudo systemctl enable node_exporter
```

步骤 7：使用 Node Exporter 数据收集器配置 Prometheus

完成以下过程，为 Prometheus 配置 Node Exporter 数据收集器。为此，可在 `prometheus.yml` 文件中为 `node_exporter` 添加新的 `job_name` 参数。

1. 使用 SSH 连接到你的 Lightsail 实例。
2. 输入以下命令以使用 Vim 打开 `prometheus.yml` 文件。

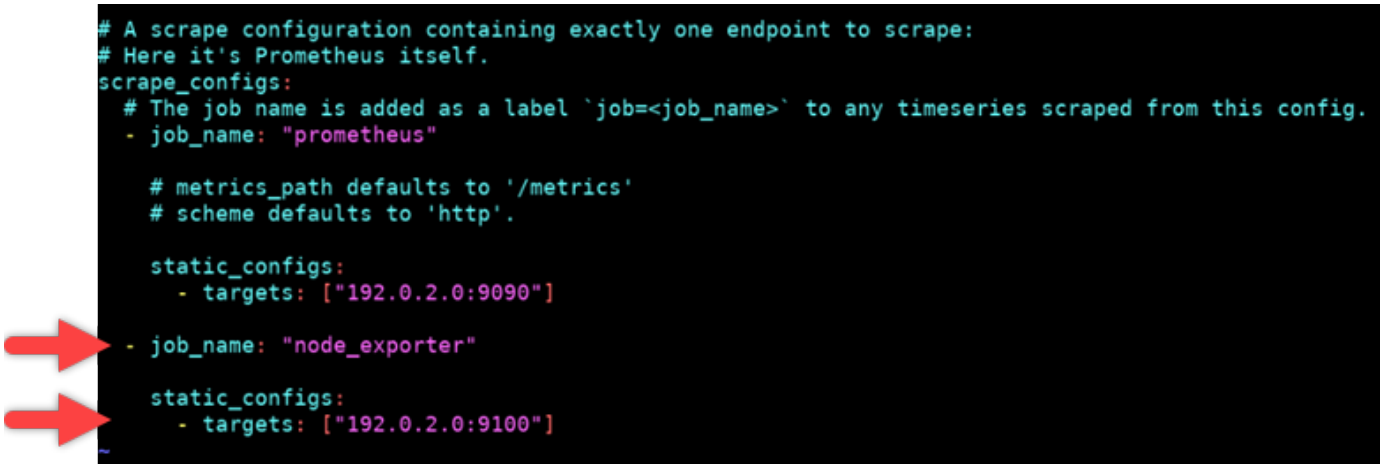
```
sudo vim /etc/prometheus/prometheus.yml
```

3. 在 Vim 中按 I 键以进入插入模式。
4. 将以下几行文本添加到文件中，位于现有 `- targets: ["<ip_addr>:9090"]` 参数下方。

```
- job_name: "node_exporter"

static_configs:
- targets: ["<ip_addr>:9100"]
```

`prometheus.yml` 文件中修改后的参数应类似于以下示例。



请注意以下几点：

- Node Exporter 监听端口 9100，以供 `prometheus` 服务器抓取数据。确认您已按照本教程的步骤 1：完成先决条件部分中概述的步骤创建实例防火墙规则。
- 与的配置一样 `prometheusjob_name`，请替换*<ip_addr>*为连接到 Lightsail 实例的静态 IP 地址。

5. 按 ESC 键退出插入模式，然后键入 :wq! 保存更改并退出 Vim。
6. 输入以下命令重新启动 Prometheus 服务，以使对配置文件所做的更改生效。

```
sudo systemctl restart prometheus
```

7. 输入以下命令以查看 Prometheus 服务的状态。

```
sudo systemctl status prometheus
```

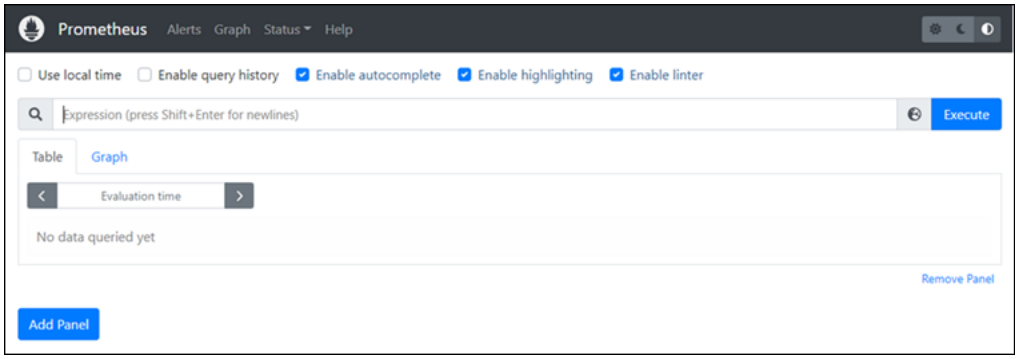
如果服务正常重新启动，您将收到类似于以下内容的输出。

```
ubuntu@ip-172-26-11-178:~$ sudo systemctl status prometheus
● prometheus.service - PrometheusServer
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2022-06-02 16:03:33 UTC; 2s ago
   Main PID: 105938 (prometheus)
      Tasks: 6 (limit: 1164)
     Memory: 39.3M
     CGroup: /system.slice/prometheus.service
             └─105938 /usr/local/bin/prometheus --config.file /etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
```

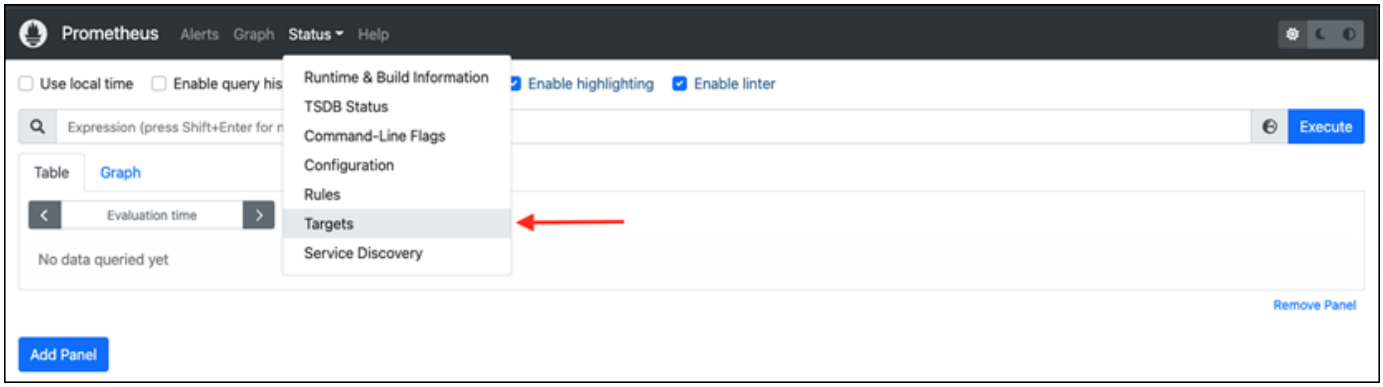
8. 按 Q 退出状态命令。
9. 在本地计算机上打开 Web 浏览器，然后转到以下网址查看 Prometheus 管理界面。

```
http:<ip_addr>:9090
```

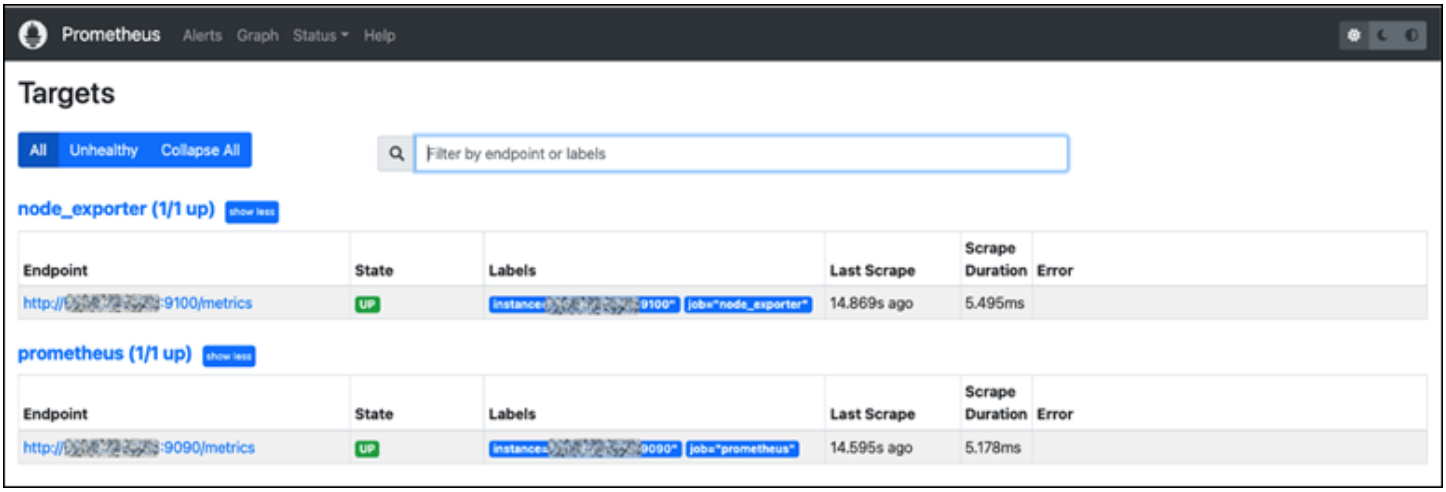
*<ip_addr>*替换为您的 Lightsail 实例的静态 IP 地址。您应看到类似于以下示例的控制面板。



10. 在主菜单中，选择 Status（状态）下拉列表，然后选择 Targets.（目标）。



在下一个屏幕上，您应该看到两个目标。第一个目标用于 node_exporter 指标收集器作业，而第二个目标用于 prometheus 作业。



现在，环境已正确设置，可收集指标和监控服务器。

使用 scp 在 Lightsail 上的 Linux 实例之间传输文件

在 Linux 中使用安全复制 (scp) 命令将文件从本地计算机传输到 Linux 或 Unix 实例，以及在 Amazon Lightsail 中从一个实例传输到另一个实例。要了解有关 scp 命令的更多信息，请参阅 man7 网站上的 scp(1) — Linux 手册页面。

本教程将引导您完成将文件从一个 Lightsail 实例复制到另一个 Lightsail 实例的步骤。

内容

- 前提条件
- 步骤 1：将私有密钥（.pem）文件保存到本地计算机
- 步骤 2：更改私有密钥的权限
- 步骤 3：将私有密钥传输到您的实例
- 第 4 步：在 Lightsail Linux 和 Unix 实例之间安全地传输文件

前提条件

- 你有两个 Lightsail 实例在运行，两个实例都有公有 IP 地址。要获取实例的公有 IP 地址。登录 Lightsail 控制台，然后复制显示在您的实例旁边的公有 IP 地址。
- 您可以使用 SSH 密钥对访问这两个实例。有关更多信息，请参阅 连接到 Linux 实例。

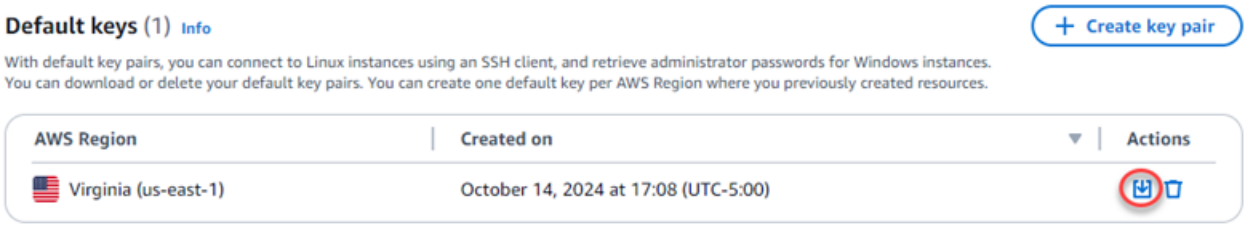
步骤 1：将私有密钥（.pem）文件保存到本地计算机

完成以下步骤，将私有密钥（.pem）文件保存到本地计算机。目标实例的私有密钥文件用于将文件从一个实例安全地传输到另一个实例。要在同一个 AWS 区域之间复制文件，您将使用该区域的默认密钥。要在不同区域的实例之间复制文件，您需要使用目标实例所在区域的默认密钥。要了解有关密钥对的更多信息，请参阅 SSH 和连接到您的实例。

> **Note**
>
> 如果您使用的是自己的密钥对，或者使用 Lightsail 控制台创建了密钥对，请找到自己的私钥并使用它来连接您的实例。当你上传自己的密钥或使用 Lightsail 控制台创建密钥对时，Lightsail 不会存储你的私钥。没有您的私有密钥，无法使用 scp 将文件传输到您的实例。

要将私有密钥（.pem）保存到本地计算机

1. 登录 Lightsail 控制台。
2. 在顶部导航栏上选择用户名，然后从下拉菜单中选择账户。
3. 选择 SSH Keys（SSH 密钥）选项卡。
4. 向下滚动到页面的 Default keys（默认密钥）部分。
5. 对于要将文件传输到其中的实例所在的 AWS 区域 ，选择默认私有密钥旁边的下载。



6. 将私有密钥保存在您的本地驱动器上的安全位置。

   您可能希望将下载的密钥移动到存储所有 SSH 密钥的目录，例如用户主目录中的“Keys”文件夹。您将需要引用在本指南下一部分保存私有密钥的目录。如果私有密钥尝试使用 `.pem` 以外的格式保存，则应在保存之前手动将格式更改为 `.pem`。

步骤 2：更改私有密钥的权限

在以下过程中，您将更改私有密钥文件的权限，以便只有您可以读取和写入该文件。

要更改私有密钥文件的权限

1. 在本地机器上打开终端窗口。
2. 输入以下命令，使密钥对的私有密钥只能由您读写。这是某些操作系统所需的最佳安全实践。

```
sudo chmod 400 /path/to/private-key.pem
```

在该命令中，将 */path/to/private-key* 替换为保存实例所用密钥对的私有密钥的目录路径。

示例：

```
sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
```

步骤 3：将私有密钥传输到您的实例

在以下步骤中，您将通过在本地计算机上运行 scp 命令将私有密钥传输到您的源实例。

要使用 scp 将私有密钥从您的计算机传输到源实例

1. 确定私有密钥文件在计算机上的位置以及在实例上的目标路径。在以下示例中，私钥文件的名称是*private-key.pem*，源实例的用户名是*ec2-user*，源实例 IPv4 的地址是*public-ipv4-address*，源实例 IPv6 的地址是*public-ipv6-address*。*destination-path/*是源实例上您要将私钥转移到的位置。

> **Note**
>
> 根据实例使用的蓝图，您可以指定以下用户名之一：
>
> - AlmaLinux OS 9、亚马逊 Linux 2、亚马逊 Linux 2023、CentOS Stream 9,FreeBSD，以及 openSUSE 实例：`ec2-user`
> - Debian 实例：`admin`
> - Ubuntu 实例：`ubuntu`
> - Bitnami 实例：`bitnami`
> - Plesk 实例：`ubuntu`
> - cPanel 和 WHM 实例：`centos`

- (IPv4) 要将私钥文件传输到实例，请在您的计算机上输入以下命令。

```
scp -i /path/private-key.pem /path/private-key.pem ec2-user@public-ipv4-address:path/
```

- (IPv6) 要在实例只有 IPv6 地址的情况下将私钥文件传输到该实例，请在您的计算机上输入以下命令。 IPv6 地址必须用方括号 ([ ]) 括起来，方括号必须转义 (\)。

```
scp -i /path/private-key.pem /path/private-key.pem ec2-user@\[public-ipv6-address\]:path/
```

2. 如果您尚未使用 SSH 连接到实例，则会看到如下响应：

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

输入 **yes**。

3. 如果传输成功，则响应的形式与下方类似：

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
private-key.pem                                100%   480     24.4KB/s   00:00
```

现在，您已将私有密钥传输到源实例，接下来可以安全地连接到目标实例并将文件传输到其中。继续执行下一步，以了解如何操作。

第 4 步：在 Lightsail Linux 和 Unix 实例之间安全地传输文件

在以下过程中，您将从一个实例（源实例）运行 scp 命令，以将文件传输到另一个实例（目标实例）。

要使用 scp 在实例之间传输文件

1. 使用 SSH 连接到源实例。您可以使用本地计算机上的终端程序进行连接，也可以使用 Lightsail 中基于浏览器的 SSH 客户端进行连接。有关更多信息，请参阅 连接到 Linux 实例。

2. 确定源文件在源实例上的位置以及在目标实例上的目标路径。在以下示例中，私钥文件的名称为*private-key.pem*，实例的用户名为*ec2-user*，实例 IPv4 的地址为*public-ipv4-address*，实例 IPv6 的地址为*public-ipv6-address*。*destination-path/*是目标实例上您要将文件传输到的位置。

   - (IPv4) 要将文件从源实例传输到目标实例，请从源实例输入以下命令。

     ```
     scp -i /path/private-key.pem /path/my-file.txt ec2-user@public-ipv4-address:destination-path/
     ```

   - (IPv6) 要将文件从源实例传输到目标实例，请从源实例输入以下命令。 IPv6 地址必须用方括号 ([ ]) 括起来，方括号必须转义 (\)。

     ```
     scp -i /path/private-key.pem /path/my-file.txt ec2-user@\[public-ipv6-address\]:destination-path/
     ```

3. 如果您尚未使用 SSH 连接到目标实例，则会看到如下响应：

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)' can't be established.
   RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
   Are you sure you want to continue connecting (yes/no)?
   ```

   输入 **yes**。

4. 如果传输成功，则响应的形式与下方类似：

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA) to the list of known hosts.
   my-file.txt                                   100%   480     24.4KB/s   00:00
   ```

通过 VPC 对等互连将 Lightsail 与其他 AWS 服务集成

Amazon Lightsail 使用亚马逊 EC2 等一系列有针对性的 AWS 服务 AWS Identity and Access Management ，以便更轻松地入门。但这并不意味着您只能使用这些服务！

您可以通过 VPC 对等互连将 Lightsail 资源与其他 AWS 服务集成。启用 VPC 对等互连后，必须确保要通过对等连接连接的资源接受所需的入站流量。有关更多信息，请参阅使用 VPC 对等连接将 Lightsail 资源连接到 AWS 服务。

某些 AWS 资源，例如亚马逊简单存储服务、亚马逊和亚马逊 DynamoDB CloudFront，不需要您启用 VPC 对等互连。点击以下链接，了解有关其他 AWS 服务的更多信息。

虚拟机（虚拟私有服务器）

Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) 是一项网络服务，可在云中提供可调整大小的计算容量。该服务旨在降低开发人员进行网络规模级云计算的难度。

借助 Amazon， EC2 您可以以最小的摩擦获得和配置容量。该服务使您可以完全控制您的计算资源，并允许您在 Amazon 经过验证的计算环境中运行。Amazon EC2 将获取和启动新服务器实例所需的时间缩短至几分钟，因此您可以根据计算需求的变化快速向上和向下扩展容量。Amazon 允许您仅为实际使用的容量付费，从而 EC2 改变了计算的经济性。Amazon EC2 为开发人员提供了工具，用于构建具有故障恢复能力的应用程序，并将自己与常见故障场景隔离开来。

了解有关亚马逊的更多信息 EC2。

Amazon VPC

Amazon Virtual Private Cloud（Amazon VPC）允许您预置 AWS Cloud 的逻辑隔离部分，您可以在其中启动您定义的虚拟网络中的亚马逊云科技资源。您可以完全掌控您的虚拟联网环境，包括选择自有的 IP 地址范围、创建子网，以及配置路由表和网络网关。

您可以轻松自定义 Amazon VPC 的网络配置。例如，您可以为可访问 Internet 的 Web 服务器创建公有子网，而将数据库或应用程序服务器等后端系统放在不能访问 Internet 的私有子网中。您可以利用多层安全措施（包括安全组和网络访问控制列表）来帮助控制对每个子网中的 Amazon EC2 实例的访问。

此外，您也可以在公司数据中心和 VPC 之间创建硬件虚拟专用网络 (VPN) 连接，将亚马逊云科技云用作公司数据中心的扩展。

了解有关 Amazon VPC 的更多信息。

无服务器计算

AWS Lambda

AWS Lambda 允许您在不预置或管理服务器的情况下运行代码。您只需按消耗的计算时间付费 - 代码未运行时不产生费用。借助 Lambda，您几乎可以为任何类型的应用程序或后端服务运行代码，并且不必进行任何管理。只需上传您的代码，Lambda 就会处理以高可用性运行和扩展您的代码所

需的一切。您可以将您的代码设置为自动从其他亚马逊云科技服务触发，或者直接从任何 Web 或移动应用程序调用。

进一步了解 AWS Lambda。

Amazon API Gateway

Amazon API Gateway 是一项完全托管的服务，让开发人员可以轻松地以任何规模创建、发布、维护、监控和保护 APIs 。只需在 AWS Management Console中单击几次，即可创建 API 来充当应用程序用来从后端服务访问数据、业务逻辑或功能的“前门”。其中包括在 Amazon 上运行的工作负载 EC2、在 Lambda 上运行的代码或任何 Web 应用程序。Amazon API Gateway 负责处理接受和处理多达数十万个并发 API 调用所涉及的所有任务。其中包括流量管理、授权和访问控制、监控以及 API 版本管理。Amazon API Gateway 没有最低费用或启动成本。您只需为收到的 API 调用和传出的数据量付费。

了解有关 Amazon API Gateway 的更多信息。

数据库

Amazon DynamoDB

Amazon DynamoDB 是一项快速而灵活的 NoSQL 数据库服务，适用于任何规模需要一致的个位数毫秒延迟的所有应用程序。它是完全托管的云数据库，支持文档和键值存储模型。此服务具有灵活的数据模型和可靠的性能，因此非常适合移动、Web、游戏、广告技术、IoT 和很多其他应用。

了解有关 DynamoDB 的更多信息。

Amazon RDS

Amazon Relational Database Service（Amazon RDS）让您可以轻松地在云中设置、操作和扩展关系数据库。该服务提供经济高效且可调整大小的容量，同时管理耗时的数据库管理任务，使您能够专注于应用程序和业务。Amazon RDS 提供 6 个常见数据库引擎供您选择，包括 Amazon Aurora、PostgreSQL、MySQL、MariaDB、Oracle 和 Microsoft SQL Server。

了解有关 Amazon RDS 的更多信息。

Amazon Aurora

Amazon Aurora 是一种与 MySQL 兼容的关系数据库引擎，将高端商业数据库的速度和可用性与开源数据库的简单性和成本效益结合在一起。Aurora 的性能最高可达到 MySQL 的五倍，并且能以十分之一的成本提供商用数据库的安全性、可用性和可靠性。

了解有关 Amazon Aurora 的更多信息。

负载均衡器

Elastic Load Balancing

Elastic Load Balancing 会自动将传入的应用程序流量分配到多个亚马逊 EC2实例。它可以让您实现应用程序容错能力，从而无缝提供路由应用程序流量所需的负载均衡容量。

Elastic Load Balancing 提供两种类型的负载均衡器。二者具有高可用性、自动扩展和可靠的安全性。其中包括基于应用程序或网络级信息路由流量的经典负载均衡器，以及基于包括请求内容的高级应用程序级信息路由流量的应用程序负载均衡器。Classic Load Balancer 非常适合在多个 Amazon EC2 实例之间对流量进行简单负载平衡。应用程序负载均衡器非常适合需要高级路由功能、微服务和基于容器的架构的应用程序。Application Load Balancer 能够将流量路由到多个服务，或者在同一 Amazon EC2 实例上的多个端口之间进行负载均衡。

了解有关 Elastic Load Balancing 的更多信息。

应用程序负载均衡器

Application Load Balancing 是 Elastic Load Balancing 服务的负载平衡选项，该服务在应用程序层运行，允许您根据在一个或多个 Amazon EC2 实例上运行的多个服务或容器之间的内容定义路由规则。

了解有关应用程序负载均衡器的更多信息。

大数据

Amazon Kinesis 服务

Amazon Kinesis 服务让您可以轻松处理亚马逊云科技云中的实时流数据。Amazon Kinesis 服务包括以下内容：Amazon Data Firehose 轻松将大量流数据加载到亚马逊云科技、适用于 Apache Flink 的亚马逊托管服务使用标准 SQL 和 Amazon Kinesis Data Streams 分析流数据，构建您自己的自定义应用程序来处理或分析流数据。

了解有关 Amazon Kinesis 服务的更多信息。

Amazon EMR

Amazon EMR 提供了一个托管 Hadoop 框架，可以轻松、快速且经济实惠地跨可动态扩展的 Amazon 实例处理大量数据。 EC2您还可以在亚马逊 EMR 中运行其他流行的分布式框架，例如 Apache Spark HBase、Presto 和 Flink，并与其他 AWS 数据存储（例如亚马逊 S3 和 DynamoDB）中的数据进行交互。

Amazon EMR 安全可靠地处理广泛的大数据用例，包括日志分析、Web 索引、数据转换（ETL）、机器学习、财务分析、科学模拟和生物信息学。

了解有关 Amazon EMR 的更多信息。

Amazon Redshift

Amazon Redshift 是一种快速、完全托管的 PB 级数据仓库，可让您使用现有的商业智能工具轻松且经济高效地分析所有数据。

了解有关 Amazon Redshift 的更多信息。

存储

Amazon Simple Storage Service（Amazon S3）

Amazon S3 为开发人员和 IT 团队提供安全、持久、高度可扩展的云存储。Amazon S3 是一种 easy-to-use对象存储，具有简单的 Web 服务接口，可从网络上的任何位置存储和检索任意数量的数据。使用 Amazon S3，您只需为实际使用的存储付费。没有最低费用，也没有设置成本。

Amazon S3 提供了一系列专为不同用例设计的存储类别，包括用于频繁访问数据的通用存储的 Amazon S3 Standard、用于长期访问但访问频率较低的数据的 Amazon S3 Standard – Infrequent Access（标准 – IA）以及 S3 Glacier 用于长期存档。Amazon S3 还提供可配置的生命周期策略，用于在整个生命周期中管理数据。设置策略后，无需更改您的应用程序，数据就会自动迁移到最合适的存储类。

Amazon S3 可以单独使用，也可以与其他 AWS 服务（例如 Amazon EC2 和 IAM）一起使用，也可以与云数据迁移服务和网关一起使用，用于初始或持续的数据摄取。Amazon S3 为各种用例提供经济高效的对象存储，包括备份和恢复、近线存档、大数据分析、灾难恢复、云应用程序和内容分发。

了解有关 Amazon S3 的更多信息。

Amazon Elastic Block Store（Amazon EBS）

Amazon EBS 提供永久性块存储卷，用于 AWS 云中的亚马逊 EC2 实例。每个 Amazon EBS 卷都会在其可用区内自动复制，以保护您免受组件故障的影响，从而提供高可用性和耐用性。Amazon EBS 卷提供运行工作负载所需的一致且低延迟的性能。借助 Amazon EBS，您可以在几分钟内扩大或缩小您的使用量，同时只需为您预配置的内容支付较低的价格。

了解有关 Amazon EBS 的更多信息。

监控和警报

Amazon CloudWatch

Amazon CloudWatch 是一项监控 AWS 云资源和您在 AWS 上运行的应用程序的服务。您可以使用 CloudWatch 来收集和跟踪指标、收集和监控日志文件、设置警报以及自动响应 AWS 资源的变化。 CloudWatch 可以监控 AWS 资源，例如 Amazon EC2 实例、Amazon DynamoDB 表和 Amazon RDS 数据库实例，以及您的应用程序和服务生成的自定义指标以及您的应用程序生成的任何日志文件。您可以使用获得 CloudWatch 对资源利用率、应用程序性能和运行状况的全系统可见性。使用这些分析结果，您可以及时做出反应，保证应用程序顺畅运行。

了解有关亚马逊的更多信息 CloudWatch。

应用程序部署

AWS Elastic Beanstalk

AWS Elastic Beanstalk 是一项 easy-to-use服务，用于在 Apache、Nginx、Passenger 和 IIS 等熟悉的服务器上部署和扩展使用 Java、.NET、Php、Node.js、Python、Ruby、Go 和 Docker 开发的 Web 应用程序和服务。

您只需上传代码，Elastic Beanstalk 就会自动处理部署，从容量配置、负载平衡、自动扩展到应用程序运行状况监控。同时，您能够完全控制为应用程序提供支持的亚马逊云科技资源，并可以随时访问底层资源。

了解有关 Elastic Beanstalk 的更多信息。

应用程序容器

Amazon Elastic Container Service (Amazon ECS)

Amazon ECS 是一项高度可扩展、高性能的容器管理服务，它支持 Docker 容器，使您能够在托管的 Amazon EC2 实例集群上轻松运行应用程序。Amazon ECS 使您无需安装、操作和扩展自己的集群管理基础设施。通过简单的 API 调用，您可以启动和停止支持 Docker 的应用程序、查询集群的完整状态以及访问许多熟悉的功能，例如安全组、Elastic Load Balancing、Amazon EBS 卷和 IAM 角色。您可以使用 Amazon ECS 根据您的资源需求和可用性要求来安排容器在集群中的放置。您还可以集成自己的计划程序或第三方计划程序，以满足特定于业务或应用的需求。

了解有关 Amazon ECS 的更多信息。

安全性和用户登录

AWS Identity and Access Management (IAM)

IAM 可让您安全地控制用户对亚马逊云科技服务和资源的访问。使用 IAM，您可以创建和管理亚马逊云科技用户和组，并使用权限来允许和拒绝他们访问亚马逊云科技资源。

了解有关 IAM 的更多信息。

Amazon Cognito User Pools

Amazon Cognito 可让您轻松将用户注册和登录添加到您的移动和 Web 应用程序。借助 Amazon Cognito，您还可以选择通过 Facebook、Twitter 或 Amazon 等社交身份提供商、使用 SAML 身份解决方案或使用您自己的身份系统对用户进行身份验证。此外，Amazon Cognito 使您能够将数据本地保存在用户设备上，从而使您的应用程序即使在设备离线时也能运行。然后，您可以在用户的多个设备间同步数据，这样，不论用户使用什么设备，都能获得一致的应用程序体验。

借助 Amazon Cognito，您可以专注于创建出色的应用程序体验，而不必担心构建、保护和扩展解决方案来处理用户管理、身份验证和跨设备同步。

了解有关 Amazon Cognito 的更多信息。

源代码控制和应用程序生命周期管理

AWS CodeCommit

AWS CodeCommit 是一项完全托管的源代码控制服务，可让公司轻松托管安全且高度可扩展的私有 Git 存储库。 AWS CodeCommit 无需操作自己的源代码控制系统或担心扩展其基础架构。您可以使用 AWS CodeCommit 安全地存储从源代码到二进制文件的所有内容，并且它可以与现有 Git 工具无缝协作。

了解 AWS CodeCommit的更多信息。

队列和消息收发

Amazon SQS

Amazon Simple Queue Service（Amazon SQS）是一种快速、可靠、可扩展且完全托管的消息队列服务。Amazon SQS 使云应用程序组件的解耦变得简单且经济高效。您可以使用 Amazon SQS 来传输任何规模的数据，而不会丢失消息，也不要求其他服务始终可用。Amazon SQS 包括具有高

吞吐量和 at-least-once处理能力的标准队列，以及提供 FIFO（先进先出）交付和精确一次处理的 FIFO 队列。

借助 Amazon SQS，您可以减轻操作和扩展高度可用的消息集群的管理负担，同时只需为您使用的内容支付较低的价格。

了解有关 Amazon SQS 的更多信息。

Amazon SNS

Amazon Simple Notification Service（Amazon SNS）是一项快速、灵活、完全托管的推送通知服务，可让您发送单独的消息或将消息群发给大量收件人。Amazon SNS 使向移动设备用户或电子邮件收件人发送推送通知，甚至向其他分布式服务发送消息变得简单且经济高效。

借助 Amazon SNS，您可以将通知发送到 Apple 推送通知服务（APNS）、Google Cloud Messaging（GCM）、Fire OS 和 Windows 设备，以及通过百度云推送发送到中国的 Android 设备。您可以使用 Amazon SNS 向全球移动设备用户发送 SMS 消息。

除了这些端点之外，Amazon SNS 还可以将消息传送到 Amazon SQS、 AWS Lambda 函数或任何 HTTP 端点。

了解有关 Amazon SNS 的更多信息。

Amazon SES

Amazon Simple Email Service（Amazon SES）是一项经济高效的电子邮件服务，建立在 Amazon.com 为服务其自身客户群而开发的可靠且可扩展的基础设施之上。借助 Amazon SES，您可以发送和接收电子邮件，无需最低承诺。您可以随用随付，且只需为所用的资源付费。

了解有关 Amazon SES 的更多信息。

工作流

Amazon Simple Workflow Service (Amazon SWF)

Amazon SWF 帮助开发人员构建、运行和扩展具有并行或顺序步骤的后台作业。您可以将 Amazon SWF 视为云中完全托管的状态跟踪器和任务协调器。

如果应用的步骤需要 500 多毫秒才能完成，则需要跟踪处理状态，并且在任务失败时需要恢复或重试。Amazon SWF 可以帮助您。

了解有关 Amazon SWF 的更多信息。

流式处理应用程序

Amazon AppStream

亚马逊 AppStream 允许您将您的 Windows 应用程序交付到任何设备。

Amazon AppStream 使您无需修改代码即可从云端流式传输现有 Windows 应用程序，在更多设备上覆盖更多用户。借助 Amazon AppStream，您的应用程序将在 AWS 基础设施上部署和呈现，并将输出流式传输到大众市场的设备，例如个人电脑、平板电脑和手机。由于您的应用程序正在云中运行，因此无论您的客户使用什么设备，都可以扩展以满足大量的计算和存储需求。Amazon AppStream 提供了一个软件开发工具包，用于将您的应用程序从云端流式传输。您可以将自己的自定义客户端、订阅、身份和存储解决方案与 Amazon 集成， AppStream 以构建满足您业务需求的自定义流媒体解决方案。

了解有关亚马逊的更多信息 AppStream。

使用创建 Lightsail 资源 AWS CloudFormation

Amazon Lightsail 与 AWS CloudFormation一项服务集成，可帮助您对 AWS 资源进行建模和设置，从而减少创建和管理资源和基础设施所花费的时间。您可以创建一个描述所需的所有 AWS 资源（例如实例和磁盘）的模板，并为您 AWS CloudFormation 预置和配置这些资源。

使用时 AWS CloudFormation，您可以重复使用模板来一致且重复地设置 Lightsail 资源。只需描述一次您的资源，然后在多个 AWS 账户 区域中一遍又一遍地配置相同的资源。

Lightsail 和模板 AWS CloudFormation

要为 Lightsail 和相关服务配置和配置资源，您必须了解AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述了您要在 AWS CloudFormation 堆栈中配置的资源。如果你不熟悉 JSON 或 YAML，可以使用 D AWS CloudFormation esigner 来帮助你开始使用 AWS CloudFormation 模板。有关更多信息，请参阅什么是 AWS CloudFormation 设计器？ 在《AWS CloudFormation 用户指南》中。

Lightsail 支持在 AWS 中创建实例和磁盘。 AWS CloudFormation有关更多信息，请参阅《AWS CloudFormation 用户指南》中的 Lightsail 资源类型参考。

了解更多关于 AWS CloudFormation

要了解更多信息 AWS CloudFormation，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API 引用
- AWS CloudFormation 命令行界面用户指南

浏览用于应用程序部署的 Lightsail 资源

以下列表包含指向未在 Lightsail 用户指南中发布的亚马逊 Lightsail 其他信息的链接。

内容

- 博客
- 教程
- 视频

博客

- 使用 Datadog 监控 Amazon Lightsail 实例的运行状况

  2022 年 3 月 30 日 — 探索使用 Datadog 监控 Lightsail 工作负载如何帮助您确保应用程序性能和控制成本。
- 如何设置 Galaxy 以研究 AWS 使用亚马逊 Lightsail

  2022 年 1 月 13 日 — 在 Lightsail 上部署 Galaxy，这是一个科学工作流程、数据集成和数字保存平台。
- 当您在浏览器中键入 URL 时会发生什么

  2021 年 8 月 26 日 – 当您在浏览器中键入 URL 并按 Enter 键时会发生什么？
- 监控 Amazon Lightsail 实例中的内存使用情况

  2021 年 6 月 14 日 — 配置 Lightsail 实例，将内存使用情况发送给亚马逊， CloudWatch 用于监控、警报和通知。
- 使用 Amazon Lightsail 顺畅托管容器化 ASP.NET 网络应用程序

  2021 年 6 月 10 日 — 如何使用连接到 PostgreSQL 数据库的容器化 ASP.NET 网络应用程序并将其部署到 Lightsail。

- 使用 Amazon Lightsail 容器启动 WordPress 网站

  2021 年 4 月 5 日 — 使用 Lightsail 容器和 Lightsail 数据库启动一个 WordPress 网站。

- Lightsail 容器：一种在云端运行容器的简便方法

  2020 年 11 月 13 日 — 在 Lightsail 上部署基于容器的工作负载。

- 将网络服务从亚马逊 Lightsail 迁移到亚马逊 EC2

  2020 年 10 月 16 日 — 在亚马逊设置生产环境，EC2 并将网络服务从 Lightsail 迁移到该环境中。

- 构建 Graylog 服务器以在 Amazon Lightsail 实例上运行

  2020 年 7 月 28 日 — 如何在 Lightsail 上构建 Graylog 服务器。

- 利用 Lightsail 内容交付网络提高网站性能

  2020 年 7 月 23 日 — 将 Lightsail 发行版配置为与标准 Web 服务器一起使用。 WordPress

- 主动监控 Amazon Lightsail 实例上的系统性能

  2020 年 6 月 4 日 – 配置突发容量警报，以便在系统性能问题影响用户之前阻止它们。

- 利用全新 Lightsail 防火墙功能增强网站安全

  2020 年 5 月 7 日 – 将使用 SSH 的远程访问限制为单个源 IP 地址。

- 使用 CodeDeploy 和 CodePipeline 将应用程序部署到 Amazon Lightsail

  2020 年 4 月 23 日 — 将 Lightsail 配置 CodePipeline 为在每次推送更改时使用 CodeDeploy和自动部署（或更新）应用程序。 GitHub

- 在 Amazon Lightsail 上使用负载均衡器

  2020 年 4 月 21 日 — 如何使用亚马逊 Lightsail 负载均衡器对简单的 Node.js 网络应用程序进行负载平衡。

- 用 Ghost 在亚马逊 Lightsail 上写照片日记

  2020 年 3 月 23 日 — 在 Lightsail 上使用 Ghost 开始写照片日记。

- 亚马逊 Lightsail 数据库提示和技巧

  2020 年 3 月 23 日 – 使用在 Amazon Relational Database Service（Amazon RDS）中发现的高级功能。

- 配置和使用监控和通知

2020 年 2 月 27 日 – 创建通知联系人、创建新警报，并通过资源监控测试通知。

- 在 Amazon Lightsail 上部署高度可用的 WordPress 网站，第 1 部分：使用以下命令实现高度可用的 Lightsail 数据库 WordPress

2019 年 10 月 22 日 — 在 Lightsail WordPress 上建立一个高度可用的网站，第 1 部分。

- 在 Amazon Lightsail 上部署高度可用的 WordPress 网站，第 2 部分：使用 Amazon S3 安全地传送媒体文件 WordPress

2019 年 10 月 31 日 — 在 Lightsail WordPress 上建立一个高度可用的网站，第 2 部分。

- 在 Amazon Lightsail 上部署高度可用的 WordPress 网站，第 3 部分：使用亚马逊提高安全性和性能 CloudFront

2019 年 11 月 7 日 — 在 Lightsail WordPress 上建立一个高度可用的网站，第 3 部分。

- 在 Amazon Lightsail 上部署高可用性 WordPress 网站，第 4 部分：使用 Lightsail 负载均衡器提高性能和可扩展性

2019 年 11 月 14 日 — 在 Lightsail WordPress 上建立一个高度可用的网站，第 4 部分。

- 使用 Amazon Lightsail 构建袖珍平台即服务

2019 年 10 月 8 日 — 在 Lightsail 上组装一个袖珍平台。

- 使用 Amazon Lightsail 部署基于 Nginx 的 HTTP/HTTPS 负载均衡器

2019 年 7 月 8 日 — 在 Lightsail 实例中设置基于 Nginx 的负载均衡器。

- 新手 AWS Cloud？ 亚马逊 Lightsail 可以提供帮助

2019 年 3 月 27 日 — 亚马逊 Lightsail 入门。

- 新增 — 亚马逊 Lightsail 的托管数据库

2018 年 10 月 16 日 – 只需点击几下即可创建托管式数据库。

- Amazon Lightsail 更新：更多实例大小和降价

2018 年 8 月 23 日 — Lightsail 实例概述。

- Amazon Lightsail：VPS 的力量 AWS、简单性

2016 年 11 月 30 日 — Lightsail 发布公告。

教程

前 5 个实践教程：

1. 创建负载平衡 WordPress 网站

   2021 年 9 月 8 日 — 使用 Lightsail 推出一个高度可用的 WordPress网站。

2. 使用 Amazon Lightsail 迁移和管理 WordPress 网站

   2021 年 2 月 22 日 — 使用 Seahorse 软件在 Lightsail 上启动你的 WordPress网站的克隆版。

3. 启动 Linux 虚拟机

   2020 年 9 月 11 日 — 使用 Lightsail 启动、配置和连接 Linux 实例。

4. 启动 Windows 虚拟机

   2020 年 9 月 11 日 — 使用 Lightsail 启动、配置和连接 Windows 实例。

5. 在亚马逊 Lightsail 上启动 cPanel 和 WHM 实例

   2020 年 7 月 27 日 — 本教程介绍了 cPanel 和 WHM 实例在 Lightsail 上启动并运行后可以采取的几个步骤。

- 如何在亚马逊 Lightsail 上设置和配置 Magento

  2021 年 8 月 11 日 – 启动并运行电子商务网站。

- 如何将您的 WordPress 网站连接到对象存储桶

  2021 年 7 月 14 日 — 在 Lightsail 上设置你的 WordPress 网站并将网站连接到 Lightsail 存储桶。

- 创建对象存储桶

  2021 年 7 月 14 日 — 在亚马逊 Lightsail 中创建对象存储桶。

- 将 WordPress 网站连接到 Amazon Lightsail 存储桶和分发

  2021 年 7 月 14 日 — 将你的 Lightsail 存储桶配置为 Lightsail 内容分发网络 (CDN) 分发的来源。

- 如何设置和配置 Plesk

  2021 年 4 月 22 日 — 在 Lightsail 上启动并运行 Plesk 托管堆栈。

- 如何设置 Prestashop 电子商务网站

2021 年 4 月 1 日 — 使用 Bitnami PrestaShop 认证蓝图启动和配置 Lightsail 实例。

- 如何在亚马逊 Lightsail 上使用亚马逊 EFS

  2021 年 3 月 15 日 — 使用 VPC 对等互连从 Lightsail 实例创建并连接到亚马逊 EFS 文件系统。

- 如何设置 Nginx 反向代理

  2021 年 2 月 10 日 — 使用 Lightsail 容器设置 Nginx 反向代理。

- 如何为 Flask 应用程序提供服务

  2021 年 2 月 3 日 — 学习如何使用 Lightsail 容器为 Flask 应用程序提供服务。

- 使用 Amazon Lightsail 创建、推送和部署容器镜像

  2020 年 11 月 11 日 – 使用 Dockerfile 在本地计算机上创建容器映像。

- 构建 Drupal 网站

  2020 年 9 月 11 日 — 在 Lightsail 上部署并托管一个可用于生产的 Drupal 网站。

- 构建 LAMP 堆栈 Web 应用程序

  2020 年 9 月 9 日 — 在 Lightsail 上启动并运行高度可用的 PHP 网络应用程序。

- 配置您的 WordPress 实例以与您的分配配合使用

  2020 年 7 月 16 日 — 将您的 WordPress 实例配置为与您的 Lightsail 发行版配合使用。

- 启动 WordPress 网站

  2020 年 3 月 23 日 — 启动并运行 WordPress 安装在 Lightsail 虚拟机上的网站。

- 托管 .NET 应用程序

  2020 年 3 月 20 日 — 使用 Lightsail 构建和部署.NET 应用程序。

- 将你在亚马逊 Route 53 上的域名映射到你的 Lightsail 资源

  将你的域名（例如 example.com）的流量路由到你的 Lightsail 资源。

视频

- 亚马逊 Lightsail 教程：部署 Django 应用程序

  2021 年 7 月 14 日 – 在本教程中，您将创建 Django 应用程序。

- 亚马逊 Lightsail 教程：部署 Flask 应用程序

  2021 年 7 月 14 日 – 在本教程中，您将创建 Flask 应用程序。

- 亚马逊 Lightsail 教程：部署 NGINX 反向代理

  2021 年 7 月 14 日 — 创建 Flask 应用程序，构建 Docker 容器，在 Lightsail 上创建容器服务，然后部署该应用程序。

- 亚马逊 Lightsail 教程：部署电子商务网站

  2021 年 7 月 14 日 — 使用 Bitnami PrestaShop 认证蓝图启动 Lightsail 实例，并对其进行配置。

- 在 Amazon Lightsail 上部署容器化应用程序

  2020 年 12 月 29 日 — 了解如何在 Lightsail 中部署容器化应用程序。

- 亚马逊 Lightsail 教程：建一个 Drupal 网站

  2020 年 8 月 31 日 – 启动并配置 Drupal 实例。

- 亚马逊 Lightsail 教程：部署 LAMP Stack 应用程序

  2020 年 8 月 31 日 — 将 LAMP（Linux Apache MySQL PHP）堆栈应用程序部署到单个 Lightsail 实例上。

- 亚马逊 Lightsail 教程：启动 Linux 实例

  2020 年 8 月 31 日 – 了解如何启动 Linux 实例。

- 亚马逊 Lightsail 教程：启动 Windows 实例

  2020 年 8 月 31 日 – 了解如何启动 Windows 实例。

- 亚马逊 Lightsail 教程：运行你自己的 Minecraft 服务器

  2020 年 8 月 31 日 – 了解如何设置专用的 Minecraft 服务器。

- 亚马逊 Lightsail 教程简介

  2020 年 8 月 31 日 — 立即使用 Lightsail 开始你的云之旅。

- 亚马逊 Lightsail：最简单的入门方法 AWS

  2020 年 3 月 20 日 — Lightsail 是最简单的入门方式。 AWS它提供虚拟服务器、存储、数据库和联网，以及经济高效的月度套餐。

- 在 Amazon Lightsail 中配置 Plesk 实例

2019 年 3 月 27 日 — 学习如何在 Lightsail 中配置 Plesk 实例。

- 在 Amazon Lightsail 中配置 WordPress多站点

  2019 年 1 月 15 日 — 了解如何在 Ligh WordPress tsail 中配置多站点实例。

- 管理 Lightsail

  2018 年 10 月 9 日 — 快速浏览一下 Lightsail 的主要功能。

- 在亚马逊 Lightsail 上部署 MEAN 堆栈应用程序

  2018 年 6 月 5 日 — 使用 Lightsail 的 MEAN 蓝图将自定义应用程序部署到云端。

- 在 Amazon Lightsail 上部署 WordPress 实例

  2018 年 6 月 5 日 — 在 Lightsai WordPress l 上部署实例。

查看 Lightsail 的详细账单和使用情况

亚马逊 Lightsail 的账单通过亚马逊网络服务 (AWS) 账单处理。要查看你的 Lightsail 账单，请前往AWS 账单与成本管理 控制面板，或者在 Lightsail 控制台顶部导航栏上选择账单。有关定价的更多信息，请参阅 Lightsail 定价页面。

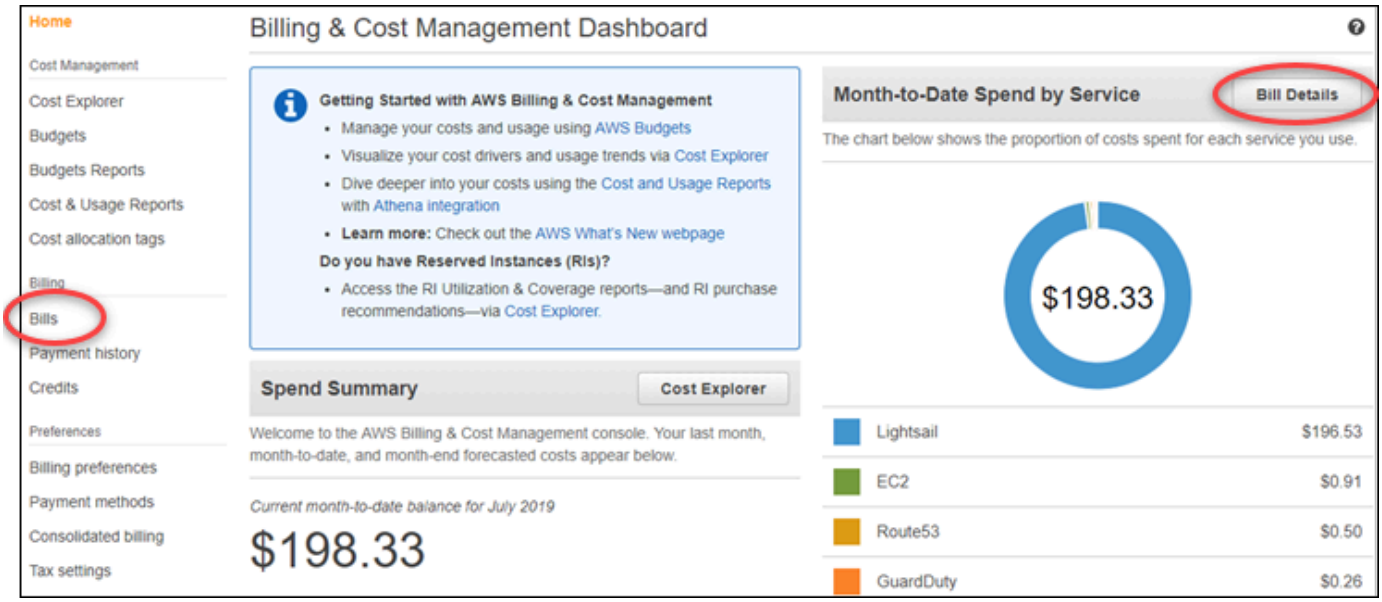
查看你的详细的 Lightsail 账单

要查看您的每月 Lightsail 账单的详细明细，请执行以下操作：

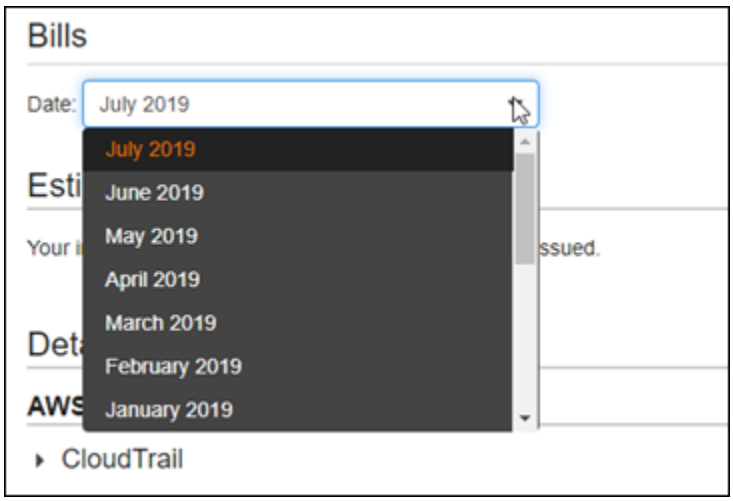
1. 登录到 AWS 账单与成本管理 控制面板。

   账单控制面板主页会显示您的账单的高级 month-to-date明细。

2. 在控制面板主页上选择 Bill Details（账单详细信息），或在左侧导航窗格选择 Bills（账单），查看月度账单的详细信息。



3. 选择 Date（日期）下拉菜单，选择除当月以外的一个月份。



4. 向下滚动 “账单” 页面，展开 Lightsail 行项目以查看每个区域的详细使用情况。



账单使用类型

以下列表描述了您的 Lightsail 账单和使用情况报告中显示的使用类型。这些使用类型有助于确定 Lightsail 资源的月度账单上的费用。

> **Note**
>
> 有关指定区域代码的以下使用类型，请参阅本指南账单中的区域代码部分，以确定相应的 AWS 区域。

- Amazon Lightsail Bundle: sizeGB：使用的 Linux 或 Unix 实例计划（以小时为单位）。Size 定义了所用实例计划的内存规范。例如，如果指定了 4 GB 内存，则会显示 24 USD/月 Linux 或 Unix 实例计划的计费小时数。

- Amazon Lightsail Bundle: sizeGB (Windows)：使用的 Windows 实例计划（以小时为单位）。Size 定义了所用实例计划的内存规范。例如，如果指定了 4 GB 内存，则会显示 44 USD/月 Windows 实例计划的计费小时数。
- 亚马逊 LightSail: sizeGB RelationalDatabase：使用的标准数据库计划（以小时为单位）。Size 定义了所用数据库计划的内存规范。例如，如果指定了 4 GB 内存，则会显示 60 美元/月标准数据库计划的计费小时数。
- Amazon LightSail: sizeGB RelationalDatabase（高可用性）：使用的高可用性数据库计划（以小时为单位）。Size 定义了所用数据库计划的内存规范。例如，如果指定了 4 GB 内存，则会显示 120 美元/月高可用性数据库计划的计费小时数。
- Amazon Lightsail 区域-DiskUsage：使用的块存储磁盘量（以每月千兆字节为单位）。
- Amazon Lightsail DNS-queries：当月的 DNS 查询数量（数量）。
- Amazon Lightsail 负载均衡器：使用的负载均衡器数量（以小时为单位）。
- Amazon Lightsail 区域-SnapshotUsage：存储的快照数据量（以每月千兆字节为单位）。
- 亚马逊 Lightsail Region-UnusedStatic IP：未连接的静态数据量 IPs （以小时为单位）。
- Amazon Lightsail Region-TotalDataXfer-In-Bytes：传输的数据总量（以千兆字节为单位）。
- Amazon Lightsail Region-TotalDataXfer-Out-Bytes：传出的数据总量（以千兆字节为单位）。
- Amazon Lightsail Region-DataXfer-Out-Overage-Bytes：传输到互联网或公众的数据量 IPs ，超过所用实例或数据库计划的允许量（以千兆字节为单位）。

账单中的区域代码

Lightsail 账单和使用情况报告使用代码和缩写。例如，针对使用类型，region 将被替换为以下缩写之一：

- APN1: 亚太地区（东京）（ap-northeast-1）
- APN2: 亚太地区（首尔）（ap-northeast-2）
- APS1: 亚太地区（新加坡）（ap-southeast-1）
- APS2: 亚太地区（悉尼）（ap-southeast-2）
- APS3: 亚太地区（孟买）（ap-south-1）
- CAN1: 加拿大（中部）（ca-central-1）
- EU：欧洲（爱尔兰）(eu-west-1)
- EUC1: 欧盟（法兰克福）（eu-central-1）
- EUW2: 欧盟（伦敦）（eu-west-2）

- EUW3: 欧盟（巴黎）（eu-west-3）
- EUN1: 欧盟（斯德哥尔摩）（eu-north-1）
- USE1: 美国东部（弗吉尼亚北部）(us-east-1)
- USE2: 美国东部（俄亥俄州）（us-east-2）
- USW2: 美国西部（俄勒冈）（us-west-2）

在 Lightsail 中获取常见问题的答案

本节涵盖了与 Lightsail 相关的常见问题和答案，分为以下几类。

主题

- 了解 Lightsail 及其全球上市情况
- 账单和账户管理
- 在 Lightsail 中传输数据
- 数据块存储（磁盘）
- 证书
- 联系人和监控通知
- 容器服务
- 内容分发网络分配
- 数据库
- 域
- 将 Lightsail 资源导出到亚马逊弹性计算云 (亚马逊) EC2
- 实例
- 负载均衡器
- 手动和自动快照
- 资源运行状况指标和警报
- 网络连接
- 对象存储和存储桶
- Lightsail 中的标签

点击每个类别中提供的链接，查找有关 Lightsail 的常见问题的详细答案。

了解 Lightsail 及其全球上市情况

什么是 Amazon Lightsail？

AWS 对于需要解决方案在云端构建和托管网站和 Web 应用程序的开发人员、小型企业、学生和其他用户来说，Amazon Lightsail 是最简单的入门方法。Lightsail 为开发人员提供计算、存储和网络容

量。Lightsail 包含快速启动项目所需的一切，包括虚拟机、容器、数据库、CDN、负载均衡器、DNS 管理等，每月价格低廉、可预测。

我能用 Lightsail 做什么？

您可以创建包含所有内容的预配置虚拟专用服务器（实例），以便轻松部署和管理您的应用程序，或者创建由 Lightsail 管理底层基础设施和操作系统的安全和运行状况的数据库。Lightsail 最适合需要几十个或更少实例的项目，以及喜欢简单管理界面的开发者。Lightsail 的常见用例包括运行网站、Web 应用程序、商业软件、博客、电子商务网站等。随着项目的发展，您可以将负载均衡器和附加的块存储与实例一起使用，以增加冗余和正常运行时间，并访问其他数十种 AWS 服务以添加新功能。

Lightsail 是否提供 API？

是。你在 Lightsail 控制台中所做的一切都由公开 API 提供支持。了解如何安装和使用 Lightsail CLI 和 API。

如何注册 Lightsail？

要开始使用 Lightsail，请选择 “入门” 并登录。你使用自己的亚马逊 Web Services 账户访问 Lightsail；如果你还没有 Lightsail，系统会提示你创建一个账户。

Light AWS 区域 sail 在哪个版本中可用？

Lightsail 目前有以下版本可供选择： AWS 区域

AWS 区域

- 美国东部（俄亥俄州）(us-east-2)
- 美国东部（弗吉尼亚北部）(us-east-1)
- 美国西部（俄勒冈州）(us-west-2)
- 亚太地区（孟买）(ap-south-1)
- 亚太地区（首尔）(ap-northeast-2)
- 亚太地区（新加坡）(ap-southeast-1)
- 亚太地区（悉尼）(ap-southeast-2)
- 亚太地区（东京）(ap-northeast-1)
- 加拿大（中部）(ca-central-1)
- 欧洲（法兰克福）(eu-central-1)
- 欧洲（爱尔兰）(eu-west-1)

- 欧洲（伦敦）(eu-west-2)
- 欧洲（巴黎）(eu-west-3)
- 欧洲（斯德哥尔摩）(eu-north-1)

有关更多信息，请参阅 AWS 区域 Lightsail 中的可用区。

什么是可用区？

可用区是一系列数据中心，这些数据中心在独立的、物理上显著不同的基础设施上运行并且被设计得高度可靠。可用区之间不共用常见的故障点，如发电机和冷却设备。此外，可用区在物理上也是相互独立的，这使得即使火灾、龙卷风或洪涝等极为罕见的灾难也只会影响单个可用区。

Lightsail 的服务配额是多少？

有关最新的 Lightsail 服务配额（包括可以增加哪些配额），请参阅中的 Lightsai l 服务配额。AWS 一般参考要增加服务配额，请使用 支持 提交案例。

我如何获得更多帮助？

Lightsail 中的上下文相关帮助面板提供了有关您在控制台中操作的即时有用提示。要打开帮助面板，请选择 Lightsail 主机右上角的帮助面板图标 ⓘ。在 Lightsail 控制台中，您还可以访问包含入门指南、概述和操作方法主题的库。而且，如果你想使用 Lightsail API，或者， AWS CLI Lightsail 提供了所有支持的编程语言的完整 API 参考。你也可以使用 Lightsail 支持资源。

如果您有账户或账单方面的问题，请在线联系 支持。使用您的 Lightsail 账户，您可以获得全天候免费访问权限。

有关如何使用 Lightsail 的一般问题，请搜索 Lightsail 文档和支持论坛。

此外，还 支持 提供一系列付费计划，以满足您的个人需求。

账单和账户管理

Lightsail 计划的费用是多少？

Lightsail 套餐按按需小时费率计费，因此您只需为实际用量付费。对于您使用的每个 Lightsail 套餐，我们都会向您收取固定的小时价格，最高不超过每月套餐的最高费用。最便宜的Lightsail套餐起价为 0. USD/hour ($5 USD/month). Lightsail plans that include a Windows Server license start at $0.0127 USD/hour ($9.50 USD/month 0067美元）。

计划在什么情况下计费？

Lightsail 实例和托管数据库在被删除之前会产生费用。即使这些资源处于停止状态，也会产生费用。如果您在月底之前删除您的 Lightsail 实例或托管数据库，我们只会根据您在当月使用 Lightsail 实例或托管数据库的总时数向您收取按比例计算的费用。例如，如果您在一个月内使用最便宜的 Lightsail 实例套餐 100 小时，则需要支付 46 美分 (100*0.0046) 的费用。

我可以免费试用 Lightsail 实例吗？

是。无论您是现有 AWS 客户还是新客户，您都可以免费使用价值 5 美元的 Lightsail 套餐 750 小时。你也可以使用 9.50 美元的 Windows 套餐免费试用包含 Windows Server 许可证的 Lightsail 套餐。您可对所需数量的实例使用这 750 小时的用量。例如，你可以运行一个 Lightsail 实例整整一个月，或者运行 10 个 Lightsail 实例持续 75 小时。免费试用优惠仅适用于自您注册使用 Lightsail 之日起的第一个日历月内的使用。如果您的账户关联到某个组织（在 AWS Organizations 下），则该组织内只有一个账户可以从这些 AWS Free Tier 优惠中受益。

实例计划包括数据传输限额。传入和传出您的实例的数据都计入您的数据传输限额。当您超出数据传输限额时，实例（包括免费试用期内的实例）将仅对传输的多余数据收取费用。有关数据传输费用的更多信息，请参阅数据传输如何收费？。

> **Note**
>
> 作为 AWS 免费套餐的一部分，您可以免费开始使用特定实例捆绑包的 Amazon Lightsail。有关更多信息，请参阅亚马逊 Lightsail 定价页面上的AWS 免费套餐。

Lightsail 免费试用什么时候开始？

Lightsail 免费试用权益从第一个符合免费试用条件的资源启动时开始。

延长的 90 天实例和数据库免费试用期仅适用于特定计划（捆绑包）。该优惠适用于在 2021 年 7 月 8 日当天或之后开始使用 Lightsail 的新 AWS 账户或现有账户。有关更多信息，请参阅 Lightsail 定价页。

Lightsail 托管数据库的成本是多少？

Lightsail 托管数据库有 4 种套餐规模，对于具有 40 GB 固态硬盘存储空间和 100 GB 数据传输限额的 1GB RAM 数据库实例，起价为每月 15 美元。高可用性计划的价格是标准计划的两倍，因为它们在另一个可用区中运行额外的数据库实例和存储磁盘，以实现冗余。

我可以免费试用 Lightsail 托管数据库吗？

可以！Lightsail 的新客户可免费获得 15 美元的 Lightsail 计划中的 1 个月。

Lightsail 区块存储的成本是多少？

Lightsail 区块存储的费用为每月每 GB 0.10 美元。

Lightsail 负载均衡器的费用是多少？

Lightsail 负载均衡器每月花费 18 美元。

证书管理如何收费？

使用 Lightsail 负载均衡器即可免费获得 Lightsail 证书和证书管理。

Lightsail 静态 IPv4地址的费用是多少？

当静态 IP 地址连接到 Lightsail 实例时，不会产生任何相关费用。静态 IPs 不能附加到 IPv6仅限实例的实例。 IPv4 地址是一种稀缺资源，Lightsail 致力于帮助有效使用它们，因此，对于 IPs 未连接到实例超过 1 小时的静态数据，我们会收取 0.005 美元/小时的小额费用。

数据传输如何收费？

您的实例、数据库和内容分发网络 (CDN) 分配计划包含数据传输限额。

对于 Lightsail 实例，传入和传出实例的数据均计入您的数据传输限额。如果您超过了数据传输限额，则只需要支付从 Lightsail 实例向互联网或使用该实例的公有 IP 地址向 AWS 资源传输的超额数据费用。您无需为传入您的 Lightsail 实例的多余数据支付费用。在您的数据传输限额之外，在使用 Lightsail 实例的私有 IP 地址时，传入到 Lightsail 实例的数据以及从 Lightsail 实例传出的数据都是免费的。

对于 Lightsail 托管的数据库，只有传出的数据才计入您的限额。如果您超过了数据传输限额，则只需要支付从 Lightsail 托管数据库向互联网传输数据的费用。

对于 Lightsail CDN 发行版，从您的分配中传输的所有数据都计入您的限额。如果超出分配数据传输限额，则会对从分配中传出的所有数据进行收费。

我针对实例的数据传输限额如何运作？

每个 Lightsail 实例计划都包含数据传输限额。传入和传出您的实例的数据传输都将计入您的数据传输限额。如果您超过了数据传输限额，则只需要支付从 Lightsail 实例向互联网或使用该实例的公有 IP 地

址向 AWS 资源传输的超额数据费用。对于处于免费试用期内的资源，也需要为超出限额的数据传输支付这笔额外费用。您的数据传输限额每月都会重置，您的实例可在当月内随时使用。

您无需为传入 Lightsail 实例的多余数据支付费用（参见示例 1）。针对某个区域中同一捆绑包（bundleId）的实例汇总数据传输限额（参见示例 2 和示例 3）。对于 IPv4 大小相同的 IPv6 实例，也会汇总数据传输限额（参见示例 4）。删除实例并创建新实例不会重置数据传输限额（参见示例 5）。创建新实例不会抵消现有的数据传输超量（参见示例 6）。有关 Lightsail 捆绑包的更多信息，请参阅亚马逊 Lightsail API 参考中的捆绑包。

- 示例 1 — 您有一个每月 5 USD 的实例捆绑包（bundleId `nano_3_0`），其中每月为 1 TB 的数据传输限额。如果您向 Internet 发送 500 GB 的数据（数据传出），向实例发送 400 GB 的数据（数据传入），则您将消耗 1 TB 限额中的 900 GB。如果您再向 Internet 发送 200 GB 的数据，则将超出您的限额 100 GB，并需支付 100 GB 的数据传输超额费用。如果您接下来向实例发送 200 GB 的数据，则无需支付超额费用。
- 示例 2 — 如果您在某个区域有两个每月 5 USD 的实例捆绑包（bundleId `nano_3_0`），为期整整一个月，且每个捆绑包都有每月 1 TB 的数据传输限额，则总共可获得 2 TB 的数据传输限额。如果您使用第一个实例向 Internet 发送 1.5 TB 的数据，使用第二个实例向 Internet 发送 100 GB 的数据，则仍将低于 2 TB 的总限额 400 GB，并且不会向您收取任何数据传输超额费用。
- 示例 3 — 您创建了两组实例捆绑包：组 A 包含两个每月 5 USD 的实例捆绑包（bundleId `nano_3_0`），组 B 包含三个每月 7 USD 的实例捆绑包（bundleId `micro_3_0`），均位于美国西部（俄勒冈）区域。总的来说，这为您提供了组 A 的 2 TB 数据传输限额，以及组 B 的 6 TB 数据传输限额。如果您通过组 A 实例将 3 TB 的数据传输到 Internet，通过组 B 实例将 4 TB 的数据传输到 Internet，则将超过组 A 实例的数据传输限额，并将支付 1 TB 的数据传输超额费用。对于组 B 实例，您仍有 2 TB 的限额。
- 示例 4 — 在账单月份的前 20 天内，您已经为每月 3.50 美元的 IPv6 实例捆绑包 (BundleIDnano_ipv6_3_0) 消耗了 1 TB 数据传输限额中的 600 GB。您决定在第 21 天将实例的网络类型切换为双堆栈（bundleId `nano_3_0` 按每月 5 USD 的价格收费）。您当月的数据传输利用率不会重置，将保持在 600 GB，还剩 400 GB 的限额。在该账单月份的剩余时间内，如果您向 Internet 发送 500 GB 的数据，则将累计 100 GB 的数据传输超额费用。
- 示例 5 — 您有三个每月价值 5 USD 的实例捆绑包（bundleId `nano_3_0`)），每个捆绑包都有每月 1 TB 的数据传输限额。假设您在账单月份内使用了总计 3 TB 数据传输限额中的 1 TB，剩余的数据传输限额为 2 TB。如果您删除所有实例，并在同一个账单月份内于同一区域创建了三个相同捆绑包（bundleId `nano_3_0`）的新实例，则您的数据传输利用率仍为 1 TB，剩余的数据传输限额仍为 2 TB。在开始累积任何数据传出超额费用之前，您可以在同一个月内通过实例再传输 2 TB 的数据。
- 示例 6 — 在账单月份的前 20 天使用每月 5 美元的实例捆绑包 (BundleIDnano_3_0) 的每月 1 TB 数据传输限额后，您又向互联网发送了 100 GB 的数据。对于这 100 GB，您将产生数据传输超额费

用。如果您现在为同一个捆绑包 (bundleIDnano_3_0) 创建另一个新实例，则仍需支付先前累积的数据传出超额费用。通过这些实例进一步向外传输数据将继续产生数据传出超额费用。

如何在我的负载均衡器中使用数据传输限额？

负载均衡器不占用您的数据传输限额。负载均衡器与目标实例或分配之间的流量按流量计量并计入您的实例或分配的数据传输限额，就像进出互联网的流量计入不在负载均衡器后面的 Lightsail 实例的数据传输限额一样。传入负载均衡器以及从中传出到 Internet 的流量不计入您的实例的数据传输限额。

如果我超出我的数据传输计划限额该怎么办？

我们已将我们的数据传输计划设计得使绝大多数客户的限额完全够用，不会产生任何额外费用。如果您的实例超出其计划数据传输限额，则将按照数据传输（仅指数据传输中以 Internet 为目的地的传出部分）所使用的 GB 数向您收取超额费用。

即使您的实例超出其计划数据传输限额，许多类型的数据传输也是免费的。向 Lightsail 实例和数据库传输数据始终是免费的。如果使用私有 IP 地址，数据从 Lightsail 实例传输到另一个 Lightsail 实例、在 Lightsail 实例和 Lightsail 托管数据库之间，或者传输到同一区域中的 AWS 资源也是免费的。

我需要为哪些类型的数据传输付费？

当您超出实例计划的每月免费数据传输限额时，在使用公有 IP 地址时，您将需要支付从 Lightsail 实例传输到互联网或其他实例 AWS 区域 或同一区域的 AWS 资源的数据传输费用。这些类型的数据传输在超出免费限额时的计费方式如下所示。

- 美国东部（俄亥俄）(us-east-2)：0.09 USD/GB
- 美国东部（弗吉尼亚北部）(us-east-1)：0.09 USD/GB
- 美国西部（俄勒冈）(us-west-2)：0.09 USD/GB
- 亚太地区（孟买）(ap-south-1)：0.13 USD/GB
- 亚太地区（首尔）(ap-northeast-2)：0.13 USD/GB
- 亚太地区（新加坡）(ap-southeast-1)：0.12 USD/GB
- 亚太地区（悉尼）(ap-southeast-2)：0.17 USD/GB
- 亚太地区（东京）(ap-northeast-1)：0.14 USD/GB
- 加拿大（中部）(ca-central-1)：0.09 USD/GB
- 欧洲（法兰克福）(eu-central-1)：0.09 USD/GB

- • 欧洲（爱尔兰）(eu-west-1)：0.09 USD/GB
- 欧洲（伦敦）(eu-west-2)：0.09 USD/GB
- 欧洲（巴黎）(eu-west-3)：0.09 USD/GB
- 欧洲（斯德哥尔摩）(eu-north-1)：0.09 USD/GB

在不同的可用区内创建的实例可以免费、私下地在各个区域之间通信，同时受损的可能性小得多。利用可用区，您可以构建高度可用的应用程序和网站，而不会增加数据传输成本或损害您的应用程序的安全性。

当您超过 Lightsail CDN 分配计划的数据传输限额时，您需要支付所有传出的数据费用。超出分配限额的数据传输费用与 Lightsail 实例不同，如下所示。

- 亚太地区：0.13 USD/GB
- 加拿大：0.09 USD/GB
- 欧洲：0.09 USD/GB
- 印度：0.13 USD/GB
- 日本：0.14 USD/GB
- 中东：0.11 USD/GB
- 南非：0.11 USD/GB
- 南美洲：0.11 USD/GB
- 美国：0.09 USD/GB

各 AWS 区域的实例数据传输限额有何差异？

Lightsail 实例的区域数据传输限额可在亚马逊 Lightsail 定价中找到。除亚太地区（孟买和悉尼）地区外 AWS 区域，所有地区的补贴均相同。孟买和悉尼区域的计划包括其他区域一半的数据传输限额。

Lightsail 托管数据库的数据传输限额完全相同。 AWS 区域

Lightsail 域名的费用是多少？

链接的 .pdf 文件中列出的价格适用于截至 2021 年 12 月 22 日的新域名注册和现有域名注册的续订。所有价格均包含 DNS 区域和隐私保护。有关域注册成本的信息，请参阅 Amazon Route 53 域注册定价和域注册。

Lightsail DNS 的管理费用是多少？

在 Lightsail 中，DNS 管理是免费的。您可以创建多达 6 个 DNS 区域并为每个 DNS 区域创建所需数量的记录。您的区域还将获得 300 万个 DNS 查询的月度限额。如果您在一个月的查询量超过 300 万个，则超出的部分将按照每 100 万个 DNS 查询 0.40 USD 的价格收费。

Lightsail 快照的费用是多少？

Lightsail 快照（手动和自动）的存储费用为每月0.05美元/GB。这意味着，如果您创建的一个实例快照使用 28 GB 空间，并保留一个月，则您需要为该月支付 $1.40 USD。

当您连续拍摄同一实例的多个快照时，Lightsail 会自动对您的快照进行成本优化。对于拍摄的每个新快照，您只需为更改的数据部分付费。在上述示例中，如果您的实例数据只有 2GB 的内容更改，则第二个实例快照的费用仅为每月 0.10 USD。

如何管理我的 AWS 账户？

Lightsail 是一项 AWS 服务，在 AWS 值得信赖且久经考验的云基础架构上运行。您使用相同的 AWS 帐户和凭据登录 Lightsail 和. AWS Management Console

您可以通过 Billin AWS g and Cost Management 控制台管理您的 AWS 账户，包括更改账户密码、用户名、联系信息或AWS 账单信息。

Lightsail 的法律使用条款是什么？

Lightsail 是一项亚马逊网络服务，因此要使用 Lightsail，您首先要同意《AWS 客户协议》和《服务条款》。创建 Lightsail 实例时，您还同意，您对软件的使用也受卖方的最终用户许可协议的约束，该协议可在创建实例页面上查看。

我怎样才能支付我的 Lightsail 账单？

您可以通过 Billing and Billing and Cost Management 控制台支付和管理 AWS 账单。 AWS 接受大多数主要的信用卡。在此处了解有关管理您的支付方式的更多信息。

在 Lightsail 中传输数据

如果我超过了实例的数据传输计划限额怎么办？

我们已将我们的数据传输计划设计得使绝大多数客户的限额完全够用，不会产生任何额外费用。如果您的实例超出其计划数据传输限额，则将按照数据传输（仅指数据传输中以 Internet 为目的地的传出部分）所使用的 GB 数向您收取超额费用。

即使您的实例超出其计划数据传输限额，许多类型的数据传输也是免费的。向 Lightsail 实例和数据库传输数据始终是免费的。如果使用私有 IP 地址，数据从 Lightsail 实例传输到另一个 Lightsail 实例、在 Lightsail 实例和 Lightsail 托管数据库之间，或者传输到同一区域中的 AWS 资源也是免费的。

对于哪些类型的数据传输，我需要为实例付费？

当您超出实例计划的每月免费数据传输限额时，在使用公有 IP 地址时，您将需要支付从 Lightsail 实例传输到互联网或其他实例 AWS 区域 或同一区域的 AWS 资源的数据传输费用。这些类型的数据传输在超出免费限额时的计费方式如下所示。

- 美国东部（俄亥俄）(us-east-2)：0.09 USD/GB
- 美国东部（弗吉尼亚北部）(us-east-1)：0.09 USD/GB
- 美国西部（俄勒冈）(us-west-2)：0.09 USD/GB
- 亚太地区（孟买）(ap-south-1)：0.13 USD/GB
- 亚太地区（首尔）(ap-northeast-2)：0.13 USD/GB
- 亚太地区（新加坡）(ap-southeast-1)：0.12 USD/GB
- 亚太地区（悉尼）(ap-southeast-2)：0.17 USD/GB
- 亚太地区（东京）(ap-northeast-1)：0.14 USD/GB
- 加拿大（中部）(ca-central-1)：0.09 USD/GB
- 欧洲（法兰克福）(eu-central-1)：0.09 USD/GB
- • 欧洲（爱尔兰）(eu-west-1)：0.09 USD/GB
- 欧洲（伦敦）(eu-west-2)：0.09 USD/GB
- 欧洲（巴黎）(eu-west-3)：0.09 USD/GB
- 欧洲（斯德哥尔摩）(eu-north-1)：0.09 USD/GB

在不同的可用区内创建的实例可以免费、私下地在各个区域之间通信，同时受损的可能性小得多。利用可用区，您可以构建高度可用的应用程序和网站，而不会增加数据传输成本或损害您的应用程序的安全性。

我针对实例的数据传输限额如何运作？

每个 Lightsail 实例计划都包含数据传输限额。传入和传出您的实例的数据传输都将计入您的数据传输限额。如果您超过了数据传输限额，则只需要支付从 Lightsail 实例向互联网或使用该实例的公有 IP 地址向 AWS 资源传输的超额数据费用。对于处于免费试用期内的资源，也需要为超出限额的数据传输支付这笔额外费用。您的数据传输限额每月都会重置，您的实例可在当月内随时使用。

您无需为传入 Lightsail 实例的多余数据支付费用（参见示例 1）。针对某个区域中同一捆绑包（bundleId）的实例汇总数据传输限额（参见示例 2 和示例 3）。对于 IPv4 大小相同的 IPv6 实例，也会汇总数据传输限额（参见示例 4）。删除实例并创建新实例不会重置数据传输限额（参见示例 5）。创建新实例不会抵消现有的数据传输超量（参见示例 6）。有关 Lightsail 捆绑包的更多信息，请参阅亚马逊 Lightsail API 参考中的捆绑包。

- 示例 1 — 您有一个每月 5 USD 的实例捆绑包（bundleId `nano_3_0`），其中每月为 1 TB 的数据传输限额。如果您向 Internet 发送 500 GB 的数据（数据传出），向实例发送 400 GB 的数据（数据传入），则您将消耗 1 TB 限额中的 900 GB。如果您再向 Internet 发送 200 GB 的数据，则将超出您的限额 100 GB，并需支付 100 GB 的数据传输超额费用。如果您接下来向实例发送 200 GB 的数据，则无需支付超额费用。
- 示例 2 — 如果您在某个区域有两个每月 5 USD 的实例捆绑包（bundleId `nano_3_0`），为期整整一个月，且每个捆绑包都有每月 1 TB 的数据传输限额，则总共可获得 2 TB 的数据传输限额。如果您使用第一个实例向 Internet 发送 1.5 TB 的数据，使用第二个实例向 Internet 发送 100 GB 的数据，则仍将低于 2 TB 的总限额 400 GB，并且不会向您收取任何数据传输超额费用。
- 示例 3 — 您创建了两组实例捆绑包：组 A 包含两个每月 5 USD 的实例捆绑包（bundleId `nano_3_0`），组 B 包含三个每月 7 USD 的实例捆绑包（bundleId `micro_3_0`），均位于美国西部（俄勒冈）区域。总的来说，这为您提供了组 A 的 2 TB 数据传输限额，以及组 B 的 6 TB 数据传输限额。如果您通过组 A 实例将 3 TB 的数据传输到 Internet，通过组 B 实例将 4 TB 的数据传输到 Internet，则将超过组 A 实例的数据传输限额，并将支付 1 TB 的数据传输超额费用。对于组 B 实例，您仍有 2 TB 的限额。
- 示例 4 — 在账单月份的前 20 天内，您已经为每月 3.50 美元的 IPv6 实例捆绑包 (BundleIDnano_ipv6_3_0) 消耗了 1 TB 数据传输限额中的 600 GB。您决定在第 21 天将实例的网络类型切换为双堆栈（bundleId `nano_3_0` 按每月 5 USD 的价格收费）。您当月的数据传输利用率不会重置，将保持在 600 GB，还剩 400 GB 的限额。在该账单月份的剩余时间内，如果您向 Internet 发送 500 GB 的数据，则将累计 100 GB 的数据传输超额费用。

- 示例 5 — 您有三个每月价值 5 USD 的实例捆绑包（bundleId nano_3_0）），每个捆绑包都有每月 1 TB 的数据传输限额。假设您在账单月份内使用了总计 3 TB 数据传输限额中的 1 TB，剩余的数据传输限额为 2 TB。如果您删除所有实例，并在同一个账单月份内于同一区域创建了三个相同捆绑包（bundleId nano_3_0）的新实例，则您的数据传输利用率仍为 1 TB，剩余的数据传输限额仍为 2 TB。在开始累积任何数据传出超额费用之前，您可以在同一个月内通过实例再传输 2 TB 的数据。
- 示例 6 — 在账单月份的前 20 天使用每月 5 美元的实例捆绑包 (BundleIDnano_3_0) 的每月 1 TB 数据传输限额后，您又向互联网发送了 100 GB 的数据。对于这 100 GB，您将产生数据传输超额费用。如果您现在为同一个捆绑包 (bundleIDnano_3_0) 创建另一个新实例，则仍需支付先前累积的数据传出超额费用。通过这些实例进一步向外传输数据将继续产生数据传出超额费用。

我的实例数据传输限额有何不同 AWS 区域？

Lightsail 实例的区域数据传输限额可在亚马逊 Lightsail 定价中找到。除亚太地区（孟买和悉尼）地区外 AWS 区域，所有地区的补贴均相同。孟买和悉尼区域的计划包括其他区域一半的数据传输限额。

Lightsail 托管数据库的数据传输限额完全相同。 AWS 区域

数据传输如何收费？

您的实例、数据库和内容分发网络 (CDN) 分配计划包含数据传输限额。

对于 Lightsail 实例，传入和传出实例的数据均计入您的数据传输限额。如果您超过了数据传输限额，则只需要支付从 Lightsail 实例向互联网或使用该实例的公有 IP 地址向 AWS 资源传输的超额数据费用。您无需为传入 Lightsail 实例的多余数据支付费用。在您的数据传输限额之外，在使用 Lightsail 实例的私有 IP 地址时，传入到 Lightsail 实例的数据以及从 Lightsail 实例传出的数据都是免费的。

对于 Lightsail 托管的数据库，只有传出的数据才计入您的限额。如果您超过了数据传输限额，则只需要支付从 Lightsail 托管数据库向互联网传输数据的费用。

对于 Lightsail CDN 发行版，从您的分配中传输的所有数据都计入您的限额。如果超出分配数据传输限额，则会对从分配中传出的所有数据进行收费。

如何在我的负载均衡器中使用数据传输限额？

负载均衡器不占用您的数据传输限额。负载均衡器与目标实例或分配之间的流量按流量计量并计入您的实例或分配的数据传输限额，就像进出互联网的流量计入不在负载均衡器后面的 Lightsail 实例的数据传输限额一样。传入负载均衡器以及从中传出到 Internet 的流量不计入您的实例的数据传输限额。

对象存储如何使用我的数据传输限额？

您可以通过将数据传入和传出 Lightsail 对象存储来消耗数据传输限额，但以下情况除外。

- 数据从互联网传输到 Lightsail 对象存储器
- Lightsail 对象存储资源之间的数据传输
- 数据从 Lightsail 对象存储器传输到同一个 Lightsail 资源中的另一个 Lightsail 资源 AWS 区域（包括转移到不同 AWS 账户中的资源，但使用相同账户） AWS 区域
- 数据从 Lightsail 对象存储传输到 Lightsail CDN 发行版

我需要为哪些类型的数据传输收取分发费用？

当您超过 Lightsail CDN 分配计划的数据传输限额时，您需要支付所有传出的数据费用。超出分配限额的数据传输费用如下。

- 亚太地区：0.13 USD/GB
- 加拿大：0.09 USD/GB
- 欧洲：0.09 USD/GB
- 印度：0.13 USD/GB
- 日本：0.14 USD/GB
- 中东：0.11 USD/GB
- 南非：0.11 USD/GB
- 南美洲：0.11 USD/GB
- 美国：0.09 USD/GB

Lightsail 的实例数据传输配额和分布式数据传输配额有什么区别？

超出分配限额的数据传输费用与 Lightsail 实例不同。虽然传入和传出的数据计入您的实例的数据传输配额，但只有传出到您的源站和查看者的数据才计入您的分配配额。此外，所有超出分配配额的数据传输都将收取超额费用，而某些类型的数据传出则是免费的。最后，Lightsail发行版使用不同的区域超额模型，尽管大多数费率与收取的费率相同，例如超额费用。

我需要为进出容器服务的数据传输付费吗？

每个容器服务都有一个数据传输配额（每月 500 GB）。这计入和传出您的服务的数据。当你超过配额时，使用公有 IP 地址时，你将需要支付从 Lightsail 容器服务传输到互联网或其他容器服务 AWS 区域或同一区域内 AWS 资源的费用。这些类型的数据传输在超出免费限额时的计费方式如下所示。

- 美国东部（俄亥俄）(us-east-2)：0.09 USD/GB
- 美国东部（弗吉尼亚北部）(us-east-1)：0.09 USD/GB
- 美国西部（俄勒冈）(us-west-2)：0.09 USD/GB
- 亚太地区（孟买）(ap-south-1)：0.13 USD/GB
- 亚太地区（首尔）(ap-northeast-2)：0.13 USD/GB
- 亚太地区（新加坡）(ap-southeast-1)：0.12 USD/GB
- 亚太地区（悉尼）(ap-southeast-2)：0.17 USD/GB
- 亚太地区（东京）(ap-northeast-1)：0.14 USD/GB
- 加拿大（中部）(ca-central-1)：0.09 USD/GB
- 欧洲（法兰克福）(eu-central-1)：0.09 USD/GB
- • 欧洲（爱尔兰）(eu-west-1)：0.09 USD/GB
- 欧洲（伦敦）(eu-west-2)：0.09 USD/GB
- 欧洲（巴黎）(eu-west-3)：0.09 USD/GB
- 欧洲（斯德哥尔摩）(eu-north-1)：0.09 USD/GB

数据块存储（磁盘）

我能用 Lightsail 区块存储做什么？

Lightsail 块存储提供了额外的存储卷（在 Lightsail 中称为 “附加磁盘”），您可以将其连接到 Lightsail 实例，类似于单个硬盘。连接的磁盘适用于需要将特定数据与其核心服务分开的应用程序或软件，以及保护应用程序数据以防止实例和系统磁盘发生故障或出现其他问题。连接的磁盘为经常访问存储的数据的应用程序或软件提供了所需的一致性能和较低的延迟。

Lightsail 块存储磁盘使用固态硬盘 (SSD)。这种类型的块存储在低廉的价格和良好的性能之间取得了平衡，旨在支持在 Lightsail 上运行的绝大多数工作负载。对于应用程序需要持续 IOPS 性能、每个磁盘的高吞吐量或运行大型数据库（如 MongoDB、Cassandra 等）的客户，我们建议使用 GP2 带有预配置 IOPS 固态硬盘存储或预配置 IOPS 固态硬盘存储的客户，而不是 Lightsail。 EC2

连接的磁盘与我的 Lightsail 套餐中包含的存储空间有何不同？

Lightsail 套餐中包含的系统磁盘是您的实例的根设备。如果终止您的实例，则还会删除系统磁盘。如果实例发生故障，则可能会影响系统磁盘。您也无法断开连接系统磁盘或将其与您的实例单独进行备份。在连接的磁盘上存储的数据将与实例单独进行保存。可以分离连接的磁盘并将其在实例之间移动。通过创建磁盘的手动快照，可以从实例独立备份它们。为了保护您的数据，我们建议您仅将 Lightsail 实例的系统磁盘用于存储临时数据。对于需要更高级别的持久性的数据，我们建议使用连接的磁盘，并使用磁盘或实例快照定期备份您的磁盘。

我可以连接多大的磁盘？

每个连接的磁盘最多可达 16 TB，Lightsail 账户中附加的块存储空间总量不得超过 20 TB。

每个 Lightsail 实例可以连接多少个磁盘？

您最多可以将 15 个磁盘连接到 Lightsail 实例。

我是否可以将一个磁盘连接到多个实例？

不能，每次只能将磁盘连接到一个实例。

是否需要将我的磁盘连接到实例上？

不需要，您可以选择不将磁盘连接到实例上。磁盘将在您的账户中处于未连接状态。如果您的磁盘未连接到实例，则价格不会发生变化。

我是否可以增加连接的磁盘大小？

可以，您可以拍摄磁盘快照并通过该快照创建新的更大磁盘以增加磁盘大小。

Lightsail 区块存储是否提供加密？

是的，为了确保您的数据安全，默认情况下，所有 Lightsail 连接的磁盘和磁盘快照都使用 Lightsail 代表您管理的密钥进行静态加密。Lightsail 还为在 Lightsail 实例和连接的磁盘之间移动的数据提供加密。

我可以期待 Lightsail 区块存储提供什么可用性？

Lightsail 区块存储旨在实现高可用性和可靠性。将在可用区中自动复制每个连接的磁盘以防止发生组件故障。Lightsail 块存储磁盘的设计可用性为 99.99%。Lightsail 还支持磁盘快照，允许定期备份您的数据。

我如何备份连接的磁盘？

您可以通过创建磁盘的手动快照备份磁盘。您还可以通过创建实例的手动快照，或者通过为连接了磁盘的实例启用自动快照，来备份整个实例和连接的所有磁盘。连接到实例的磁盘包含在实例手动快照和自动快照中。

证书

如何使用 LightSail 提供的证书？

SSL/TLS certificates are used to establish the identity of your website or application and secure connections between browsers and your website. Lightsail provides a signed certificate to use with your load balancer, and the load balancer provides SSL/TLS在通过安全 AWS 网络将经过验证的流量路由到目标实例之前终止。Lightsail 证书只能用于 Lightsail 负载均衡器，不能用于单个 Lightsail 实例。

如何验证我的证书？

Lightsail 证书经过域名验证，这意味着在证书颁发机构配置证书之前，您需要通过验证自己拥有或有权访问网站域来提供身份证明。当您申请新证书时，Lightsail 将尝试自动验证证书。如果无法自动验证证书，Lightsail 将提示您向正在验证的一个或多个域名的 DNS 区域中添加别名记录记录。无论您当前在何处管理 DNS 区域（Lightsail DNS 管理还是外部 DNS 托管提供商），您都有 72 小时的时间来添加别名记录记录。

如果无法验证我的域，会发生什么情况？

为了安全起见，您必须能够验证您是否拥有一个域。这意味着，如果您或您的组织中的某人出于任何原因无法添加 DNS 记录来验证您的证书，则您将无法在 Lightsail 中使用支持 HTTPS 的负载均衡器。

可以将多少个域和子域添加到我的证书中？

您最多可以在每个证书中添加 10 个域或子域。Lightsail 目前不支持通配符域名。

如何更改与我的证书关联的域？

要更改与您的证书关联的域 (添加/删除)，您需要重新提交该证书，然后重新验证您是否拥有这些域。请按照证书管理屏幕中的步骤重新生成证书，然后在出现提示时添加或删除域。

如何续订我的证书？

Lightsail 为您的 SSL/TLS 证书提供托管续订。这意味着 Lightsail 会尝试在证书到期之前自动续订证书，无需您采取任何操作。您的 Lightsail 证书必须主动与负载均衡器关联，然后才能自动续订。

在删除负载均衡器时，我的证书会发生什么情况？

如果删除负载均衡器，则还会删除您的证书。如果将来需要将证书用于相同的域，您需要申请并验证新证书。

我能否下载 Lightsail 提供的证书？

不是，Lightsail 证书绑定到你的 Lightsail 账户，不能在 Lightsail 之外删除和使用。

联系人和监控通知

什么是通知？

您可以在 Lightsail 中配置警报，以便在您的某个实例、数据库或负载均衡器的指标超过指定阈值时通知您。通知的形式可以是 Lightsail 控制台中显示的横幅、发送到您指定地址的电子邮件或发送到您指定的手机号码的 SMS 短信。要通过电子邮件和短信收到通知，您必须将您的电子邮件地址和手机号码添加为要监控资源的每个 AWS 区域 位置的通知联系人。有关通知的更多信息，请参阅通知。

我可以添加多少个联系人？

您可以在每个要监控资源 AWS 区域 的地方添加一个电子邮件地址和一个手机号码。并非所有可以创建 Light AWS 区域 sail 资源的系统都支持短信，并且无法向世界上某些国家和地区发送短信。有关通知的更多信息，请参阅通知。

容器服务

我可以用 Lightsail 容器服务做什么？

Lightsail 容器服务提供了一种在云中运行容器化应用程序的简便方法。您可以在容器服务中运行各种应用程序（从简单的 Web 应用程序到多层微服务）。您只需指定容器服务所需的容器映像、功率（CPU、RAM）和规模（节点数）。Lightsail 负责运行容器服务，而无需您管理任何底层基础架构。Lightsail 将为您提供负载平衡的 TLS 端点，用于访问在容器服务上运行的应用程序。

Lightsail 容器服务能否运行 Docker 容器？

是。Lightsail 支持基于 Linux 的 Docker 容器。目前不支持 Windows 容器。

如何在 Lightsail 容器服务中使用我的公共容器镜像？

您可以使用在线公共注册表（例如 Amazon ECR 公共注册表）中的容器映像，也可以使用以下简单步骤构建自己的自定义映像并将其推送到 Lightsail。 AWS CLI有关更多信息，请参阅推送和管理容器映像。

我可以从私有容器注册表中提取容器镜像吗？

目前，Lightsail 容器服务仅支持公共容器注册表。或者，您可以将自定义容器镜像从本地计算机推送到 Lightsail，以保持其私密性。

我可以根据需求更改服务的功率和规模吗？

可以，即使在创建服务后，也能随时更改容器服务的功率和规模。

我能否自定义 Lightsail 容器服务创建的 HTTPS 终端节点的名称？

Lightsail 以该格式为每个容器服务提供一个 HTTPS 端点。*<service-name>*.*<random-guid>*.*<aws-region-name>*.cs.amazonlightsail.com只能自定义服务名称。或者，您可以使用自定义域名。有关更多信息，请参阅启用和管理自定义域。

我能否将自定义域名用作 Lightsail 容器服务的 HTTPS 终端节点？

是。您可以在 Lightsail 中创建带有自定义域名的 SSL/TLS 证书并将其附加到您的容器服务。证书必须经过域验证。如果您的域名的 DNS 使用 Lightsail DNS 区域，则可以将您的域名顶点 (example.com) 或子域名 () 的流量路由到您的容www.example.com器服务。或者，您可以使用支持添加 ALIAS 记录的 DNS 托管提供商将您的域的顶点 (example.com) 映射到 Lightsail 容器服务的默认域（公有 DNS）。有关更多信息，请参阅启用和管理自定义域。

Lightsail 集装箱服务的费用是多少？

Lightsail 容器服务按需小时费率计费，因此您只需为实际用量付费。对于您使用的每个 Lightsail 容器服务，我们都会向您收取固定的小时价格，最高不超过每月最高服务价格。最高月度服务价格可通过将服务功率的基价乘以服务的规模来计算。例如，对于 Micro 功率和规模为 2 的服务，其费用最高为 10

美元 *2 = 20 美元/月。最便宜的Lightsail容器服务起价为0. USD/hour ($7 USD/month 0094美元）。每个服务的使用量如果超过 500 GB 的免费配额，可能会收取额外的数据传输费用。

如果我只是运行了几天的容器服务，会向我收取整个月的费用吗？

您的 Lightsail 容器服务只有在处于运行或禁用状态时才会收费。如果您在月底之前删除了 Lightsail 容器服务，我们会根据您使用 Lightsail 容器服务的总时长按比例向您收取费用。例如，如果您使用 Lightsail 容器服务，其功率为 Micro，一个月内缩放比例为 1，持续 100 小时，则将支付 1.34 美元（0.0134*100 美元）的费用

我需要为进出容器服务的数据传输付费吗？

每个容器服务都有一个数据传输配额（每月 500 GB）。传入和传出服务的数据都将计算在内。当你超过配额时，使用公有 IP 地址时，你将需要支付从 Lightsail 容器服务传输到互联网或其他容器服务 AWS 区域 或同一区域内 AWS 资源的费用。这些类型的数据传输在超出免费限额时的计费方式如下所示。

超过每月数据传输配额的费用

- 美国东部（俄亥俄）(us-east-2)：0.09 USD/GB
- 美国东部（弗吉尼亚北部）(us-east-1)：0.09 USD/GB
- 美国西部（俄勒冈）(us-west-2)：0.09 USD/GB
- 亚太地区（孟买）(ap-south-1)：0.13 USD/GB
- 亚太地区（首尔）(ap-northeast-2)：0.13 USD/GB
- 亚太地区（新加坡）(ap-southeast-1)：0.12 USD/GB
- 亚太地区（悉尼）(ap-southeast-2)：0.17 USD/GB
- 亚太地区（东京）(ap-northeast-1)：0.14 USD/GB
- 加拿大（中部）(ca-central-1)：0.09 USD/GB
- 欧洲（法兰克福）(eu-central-1)：0.09 USD/GB
- • 欧洲（爱尔兰）(eu-west-1)：0.09 USD/GB
- 欧洲（伦敦）(eu-west-2)：0.09 USD/GB
- 欧洲（巴黎）(eu-west-3)：0.09 USD/GB
- 欧洲（斯德哥尔摩）(eu-north-1)：0.09 USD/GB

停止和删除容器服务之间有何区别？

禁用容器服务时，容器节点处于禁用状态，服务的公有端点将返回 HTTP 状态代码“503”。启用服务会将其还原为上一个活动部署。功率和规模配置也会保留。重新启用后，公有端点名称不会更改。将保留部署历史记录和容器镜像。

当您删除容器服务时，您执行的是破坏性操作。将永久删除服务的所有容器节点。HTTPS 公有端点地址、容器镜像、部署历史记录和与服务关联的日志也将被永久删除。您将无法恢复端点地址。

如果我的容器服务处于禁用状态，会向我收取费用吗？

是的，即使容器服务处于禁用状态，也会根据容器服务的功率和规模配置收费。

我能否使用容器服务作为我的 Lightsail 内容分发网络 (CDN) 发行版的来源？

目前，不支持容器服务作为 Lightsail CDN 发行版的来源。

我能否使用容器服务作为 Lightsail 负载均衡器的目标？

不是。 容器服务目前无法用作 Lightsail 负载均衡器的目标。但是，容器服务的公有端点内置了负载均衡。

是否可以将容器服务的公有端点配置为将 HTTP 请求重新导向到 HTTPS？

Lightsail 容器服务公共端点会自动将所有 HTTP 请求重定向到 HTTPS，以确保您的内容得到安全提供。

容器服务是否支持监控和提醒？

容器服务对于跨服务节点的 CPU 使用率和内存利用率提供相关的指标。目前不支持基于这些指标的提醒。

Lightsail 容器服务支持吗？ IPv6

Lightsail 容器服务 HTTPS 端点同时支持和 IPv4 。 IPv6无法在容器服务中禁用 IPv6。

内容分发网络分配

我能用 Lightsail CDN 发行版做什么？

Lightsail 内容分发网络 (CDN) 发行版通过在由亚马逊提供支持的亚马逊全球交付网络上存储和提供内容，可以轻松加快托管在 Lightsail 资源上的内容的交付。 CloudFront分配还通过提供简单的 SSL 证书创建和托管功能，帮助您的网站支持 HTTPS 流量。最后，发行版可以帮助减少您的 Lightsail 资源的负载，并帮助您的网站应对大量流量高峰。与Lightsail的所有功能一样，只需点击几下即可完成设置，而且您只需支付简单的月费。

我可以使用哪些类型的资源作为分配的源？

Lightsail 发行版允许你使用你的 Lightsail 实例和负载均衡器作为来源。目前不支持 Lightsail 容器作为起源。不支持 Lightsail 之外的资源，例如 S3 存储桶。

我是否需要将静态 IPv4地址附加到我的 Lightsail 实例才能将其用作 Lightsail 发行版的来源？

是的，必须将静态 IPv4 地址附加到指定为来源的实例。Lightsail 发行版目前不支持。 IPv6

如何在我的 WordPress 网站上设置 Lightsail 发行版？

创建您的分配，选择您的 WordPress 实例作为来源，选择您的计划，一切就完成了。Lightsail 发行版会自动配置您的分发设置，以优化大多数 WordPress 配置的性能。

我可以附加多个源吗？

尽管您无法将多个源连接到 Lightsail 分发，但您可以将多个实例附加到 Lightsail 负载均衡器并将其指定为分配的来源。

Lightsail 发行版是否支持证书创建？

是。Lightsail 发行版可以直接从发行版的管理页面轻松创建、验证和附加证书。

是否需要证书？

仅当您希望将自定义域名用于分配时需要证书。所有 Lightsail 发行版均使用支持 HTTPS 的 CloudFront 唯一亚马逊域名创建。但是，如果您希望将自定义域用于分配，则需要将自定义域的证书附加到您的分配。

可以创建的证书数量有限制吗？

是的，有关更多信息，请参阅 Lightsail 服务配额。

如何配置我的分配以将 HTTP 请求重新导向到 HTTPS？

Lightsail 发行版会自动将所有 HTTP 请求重定向到 HTTPS，以确保您的内容得到安全传送。

如何将我的顶点域名配置为指向我的 Lightsail 发行版？

为了将顶端域指向 CDN 分配，您必须在域的域名系统 (DNS) 中创建一个别名记录，以将顶级域映射到分配的默认域。如果您的 DNS 托管服务提供商不支持 ALIAS 记录，则可以使用 Lightsail DNS 区域轻松配置您的顶点域以指向您的分配的域。

Lightsail 的实例数据传输配额和分布式数据传输配额有什么区别？

虽然数据传入和传出都会计入实例的数据传输配额，但只有传出到您的源和查看器的数据才会计入分配的配额。此外，所有超出分配配额的数据传出都需支付超额费用，但某些类型的数据传出对于实例是免费的。最后，Lightsail发行版使用不同的区域超额模型，尽管大多数费率与收取的费率相同，例如超额费用。

我可以更改与分配关联的计划吗？

是的，您可以每月更改分配计划一次。如果您希望再次更改计划，则必须等到下个月初才能更改。

如何知道我的分配是否正常工作？

Lightsail 发行版为您提供了多种跟踪分发效果的指标，包括您的分发已收到的请求总数、您的分发发送给客户和来源的数据量，以及导致错误的请求的百分比。此外，您还可以创建关联到分配指标的提示。

我能否删除 Lightsail 发行版中的缓存内容？

您可以删除所有缓存内容，但特定的文件或文件夹除外。

与亚马逊 CloudFront 发行版相比，我什么时候应该使用 Lightsail 发行版？

Lightsail 发行版专为在 Lightsail 资源（例如实例和负载均衡器）上托管网站或 Web 应用程序的用户而设计。如果您在中使用其他服务 AWS 来托管您的网站或应用程序，有复杂的配置需求，或者您的工作负载涉及每秒大量请求或大量视频流，我们建议您使用 Amazon CloudFront。

我能否将我的 Lightsail 内容分发网络 (CDN) 分发转移到亚马逊？ CloudFront

是的，您可以通过在亚马逊中创建配置相似的分配来移动 Lightsail 分发。 CloudFront在 Lightsail 发行版中可以配置的所有设置也可以在发行版中进行 CloudFront 配置。完成以下步骤，将您的发行版移至 CloudFront。

如何将你的 Lightsail 发行版移至 CloudFront

- 拍摄配置为发行版来源的 Lightsail 实例的快照。将快照导出到 Amazon EC2，然后在 Amazon 中使用该快照创建一个新实例 EC2。有关更多信息，请参阅将快照导出到 Amazon EC2。

  > **Note**
  >
  > 如果您需要均衡网站或 Web 应用程序的负载，请在 Elastic Load Balancing 中创建 Application Load Balancer。有关更多信息，请参阅 Elastic Load Balancing 用户指南。

- 禁用 Lightsail 发行版的自定义域名以分离您可能已附加到该发行版的证书。有关更多信息，请参阅为您的 Amazon Lightsail 发行版禁用自定义域名。
- 使用 AWS Command Line Interface (AWS CLI) 运行 get-distributions 命令以获取 Lightsail 发行版的设置列表。有关更多信息，请参阅《AWS CLI 参考》中的 get-distributions。
- 登录CloudFront控制台并使用与 Lightsail 发行版相同的配置设置创建发行版。有关更多信息，请参阅《Amazon CloudFront 开发者指南》中的创建分配。
- 在 AWS Certificate Manager c (ACM) 中创建要附加到 CloudFront发行版的证书。有关更多信息，请参阅《ACM 用户指南》中的请求公有证书。
- 更新您的 CloudFront 发行版以使用您创建的 ACM 证书。有关更多信息，请参阅《CloudFront 用户指南》中的 “更新您的 CloudFront 发行版”。

Lightsail CDN 打算如何使用？

Lightsail CDN 发行版是使用固定价格的数据传输捆绑包创建的，以使使用该服务的成本变得简单且可预测。分配套餐旨在覆盖一个月的使用费用。以避免产生超额费用的方式使用分配套餐（包括但不限于频繁升级或降级套餐，或单个源使用过大数量的分配）超出了预期的使用范围，将予以禁止。此外，不允许涉及每秒大量请求或大量视频流的工作负载。这些行为可能会导致您的数据服务或账户受到限制或被暂停。

Lightsail CDN 发行版是否支持？ IPv6

默认情况下，所有 Lightsail CDN 发行版均已 IPv6 启用。分发主机名同时解析为 IPv4 和 IPv6 地址。IPv6 可以使用 CDN 管理页面的 “网络” 选项卡上的切换开关来禁用。

是否需要 IPv6 启用源代码才能与 Lightsail CDN 发行版配合使用？

不是。 CDN 分发同时接受 IPv6 和 IPv4 流量，并在后端与源站通信 IPv4 时将其无缝转换为流量。因此，发行版背后的来源可以是双栈的，也可以是 IPv4 唯一的。

数据库

什么是 Lightsail 托管数据库？

Lightsail 托管数据库是专用于运行数据库的实例，而不是 Web 服务器、邮件服务器等其他工作负载。一个托管数据库可以包含多个由用户创建的数据库，并且可以使用与处理独立数据库时所用的相同工具和应用程序来访问这个数据库。Lightsail 可维护数据库底层基础设施和操作系统的安全性和健康性，因此您无需深厚的基础设施管理专业知识即可运行数据库。

与普通的 Lightsail 实例一样，Lightsail 托管数据库的计划中包含固定数量的内存、计算能力和基于 SSD 的存储，您可以随着时间的推移进行扩展。Lightsail 将在创建数据库时自动为你安装和配置你选择的数据库。

我可以用 Lightsail 托管的数据库做什么？

Lightsail 托管数据库提供了一种简单、维护成本低的方式，可将数据存储在云中。您可以将托管数据库作为新数据库运行，也可以从现有的本地或托管数据库迁移到 Lightsail。

通过将数据库分离到一个专用实例中，它们还允许您扩展应用程序以接受更大的流量和更密集的负载。Lightsail 托管数据库对于有状态的应用程序（例如 WordPress 最常见 CMSs 的应用程序）特别有用，这些应用程序需要在扩展到单个实例之外时保持数据同步。托管数据库可以与 Lightsail 负载均衡器和两个或更多 Lightsail 实例配对，以创建功能强大、可扩展的应用程序。通过使用 Lightsail 高可用性托管数据库计划，您还可以为数据库添加冗余，从而帮助确保应用程序的高正常运行时间。

Lightsail 能为我管理什么？

Lightsail 为您的托管数据库及其底层基础设施管理一系列维护活动和安全。Lightsail 会自动备份您的数据库，并允许使用数据库还原工具恢复过去 7 天的时间点，以帮助防止数据丢失或组件故障。Lightsail 还会自动加密您的静态和动态数据，以提高安全性，并存储您的数据库密码，以便轻松安全地连接到数

据库。在维护方面，Lightsail 会在您设定的维护时段内对您的数据库进行维护。该维护操作包括自动升级到最新的次要数据库版本以及对底层基础设施和操作系统执行所有管理操作。

Lightsail 支持哪些类型的数据库以及这些数据库的哪些版本？

Lightsail 托管数据库支持 MySQL 和 PostgreSQL 的最新主要版本。目前，这些版本为 MySQL 5.7、MySQL 8.0、PostgreSQL 9、PostgreSQL 10、PostgreSQL 11 和 PostgreSQL 12。Lightsail 仅为每个主要版本选项提供最新的次要版本。

Lightsail 提供哪些托管数据库计划？

Lightsail 在标准和高可用性计划中提供 4 种大小的托管数据库。每个计划都附带固定数量的存储和每月数据传输限额。您还可以随着时间的推移按需纵向扩展至更大的计划，并在标准和高可用性计划之间切换。高可用性计划包括与标准计划相同的资源，另外还包括一个在独立于您的主数据库的单独可用区中运行的备用数据库来实现冗余。

什么是高可用性计划？

Lightsail 托管数据库有标准版和高可用性套餐可供选择。标准和高可用性计划具有相同的计划资源，其中包括内存、存储和数据传输限额。高可用性计划通过在与主数据库不同的可用区中自动创建备用数据库，将数据同步复制到备用数据库，并在基础设施出现故障和维护期间提供到备用数据库的故障转移，从而确保即使数据库由 Lightsail 自动升级/维护，也能确保正常运行时间。当需要较长的正常运行时间时，应使用高可用性计划运行生产应用程序或软件。

如何扩大或缩小我的 Lightsail 托管数据库？

您可以扩展 Lightsail 托管数据库，方法是为其拍摄快照并根据快照创建新的更大的数据库计划，或者使用紧急还原功能创建更大的新数据库。您还可以使用任一方法从标准计划切换到高可用性计划，或反之。您无法缩减您的数据库。有关更多信息，请参阅 Lightsail 中根据快照创建数据库。

如何备份我的 Lightsail 托管数据库？

Lightsail 会自动备份您的数据，并允许将这些数据从特定时间点恢复到新数据库。自动备份是一项免费的数据库服务，但仅保存过去 7 天内的数据。如果您删除数据库，则会删除所有自动备份记录，并且无法再进行 point-in-time恢复。要在删除数据库后保留数据备份或保留过去 7 天以上数据的备份，请使用手动快照。

您可以从数据库管理页面手动拍摄 Lightsail 托管数据库的快照。手动快照包含您的数据库中的所有数据，并且可用作您想要永久存储的数据的备份。您还可以使用手动快照创建一个更大的新数据库或在标

准和高可用性计划之间进行切换。除非您删除手动快照，否则它们将一直存储在系统中，并按照每月 0.05 USD/GB 的价格收费。

如果我删除我的 Lightsail 托管数据库，我的数据会怎样？

如果您删除 Lightsail 托管数据库，则您的数据库本身和所有自动备份都将被删除。除非您在删除您的数据库之前拍摄手动快照，否则将无法恢复此数据。在删除数据库期间，如果需要，Lightsail 提供了一键式手动拍摄快照的选项，以帮助防止数据意外丢失。删除前是否拍摄手动快照是可选的，但强烈建议您这样做。您可以在未来不再需要存储的数据时删除手动快照。

我能否将我的实例连接到在不同 AWS 区域 或不同可用区中运行的 Lightsail 托管数据库？

您不能将 Lightsail 托管数据库与在不同实例中运行的数据库一起使用。 AWS 区域不过，您可以跨实例中的不同可用区使用数据库。

如何将数据加载到我的 Lightsail 托管数据库中？

要将数据加载到 Lightsail 托管数据库中，应先启用数据导入模式。启用数据导入模式后，您便可以使用您的首选数据库客户端继续手动上传数据。加载完数据后，切记要关闭数据导入模式，以便恢复数据库的自动备份和日志记录。有关更多信息，请参阅将数据导入 MySQL 数据库和将数据导入 PostgreSQL 数据库。

如何访问我的 Lightsail 托管数据库中的数据？

您可以使用任何标准的 SQL 客户端应用程序连接到您的数据库并查询数据。我们建议使用 MySQL Workbench 执行基于 GUI 的管理和查询。您可以在您的数据库的数据库管理屏幕中查找连接数据，其中包括端点 URL 和 DNS 名称。有关更多信息，请参阅连接你的 MySQL 数据库或在 Amazon Lightsail 中连接你的 PostgreSQL 数据库。

Lightsail 托管数据库如何与我的 Lightsail 实例配合使用？

创建 Lightsail 托管数据库后，您可以立即开始将其用于您的应用程序，将 Lightsail 实例用作 Web 服务器或应用程序的其他专用工作负载。要将 Lightsail 实例连接到数据库，请使用您的数据库终端节点并引用安全存储的密码，将数据库配置为应用程序代码中的数据存储。您可以在数据库管理屏幕中查找连接数据。数据库配置文件的文件名和位置因应用程序而异。请注意，您可以使用相同的表或不同的表将多个实例连接到一个数据库。

如何将 Lightsail 托管数据库连接到我的 AWS 账户中运行的 EC2 实例？

您可以通过公共互联网连接，将 Lightsail 托管的数据库连接到 EC2 实例。请注意，连接到所有 AWS 服务将消耗您的数据库数据传输限额，而通过公共互联网将数据发送到超过您的数据传输限额的 AWS 服务将产生超额费用。您不能在 Lightsail 托管的数据库 EC2 和实例之间使用 VPC 对等互连。

我的 Lightsail 托管数据库的公共模式和私有模式有什么区别？

默认情况下，您的 Lightsail 托管数据库是在私有模式下创建的，该模式通过仅允许 Lightsail 实例访问来保护该数据库。如果您需要通过公共 Internet 连接到软件或服务，可以将数据库设为公有模式。为确保数据的安全性，我们不建议您长期启用公有模式。您可以随时从您的数据库管理屏幕中切换公有和私有模式。

我能否管理我的 Lightsail 托管数据库使用的端口？

不，出于安全考虑，Lightsail 会自动管理你的端口，在公共模式下为所有 Lightsail 托管的数据库打开 MySQL 端口 3306。如果您的数据库处于私有模式，则您的数据库仅对通过内部网络在您的 Lightsail 账户中运行的资源开放。

Lightsail 托管数据库服务是否支持？ IPv6

Lightsail 托管数据库不支持。 IPv6

域

我能用 Lightsail 域名做什么？

Lightsail 域名允许您注册和管理您的网站或应用程序的域名。如果您有在其他提供商处注册的域名，则可以将这些域名的管理权移交给 Lightsail。你也可以将这些域名指向你的 Lightsail 资源。

我可以使用哪些顶级域名 (TLDs)？

Lightsail 使用的通用 TLDs 名称与亚马逊 Route 53 相同。如果您想注册地理域，我们建议您使用 Route 53 控制台。使用 Route 53 注册后，您的地理域名将在 Lightsail 控制台中可用。有关 Lightsail 支持的更多信息 TLDs ，请参阅《亚马逊 Route 53 开发者指南》中的可以在亚马逊 Route 53 注册的域名。

我能否将 Lightsail 作为我现有域名的 DNS 服务？

您可以将使用其他 DNS 服务提供商注册的域名的 DNS 管理转移到 Lightsail。有关更多信息，请参阅创建 DNS 区域以管理域的 DNS 记录。

如何开始在 Lightsail 中注册域名？

登录 Lightsail 后，你可以使用 Lightsai l 控制台来创建和管理域名。有关更多信息，请参阅域注册。

与 Route 53 相比，我什么时候应该在 Lightsail 中注册域名？

诸如注册域、创建 DNS 区域以及将域的流量路由到 Lightsail 资源之类的任务都在 Lightsail 中完成。我们建议将 Route 53 用于高级任务，例如扩展域注册、转移域（包括流量策略）和创建私有托管区。

我可以将我的域名转移到 Lightsail 吗？

您可以将域转移到 Route 53。域名转移完成后，您的域名将在 Lightsail 控制台中可用。有关更多信息，请参阅在亚马逊 Route 53 中管理 Lightsail 域名。

我可以将哪些 Lightsail 资源用于域？

在 Lightsail 中注册域名后，您可以将您的域指向 Lightsail 实例、容器、负载均衡器、静态 IP 或内容分发网络 (CDN)。

将 Lightsail 资源导出到亚马逊弹性计算云 (亚马逊) EC2

什么是向亚马逊出口 EC2？

导出到亚马逊 EC2 是一项功能，允许您在亚马逊中创建 Lightsail 实例的副本。 EC2当您导出到 Amazon 时 EC2，您可以从 Amazon EC2 提供的各种实例类型、配置和定价模型中进行选择，并对您的网络、存储和计算环境进行更精细的控制。

我为什么要出口到 Amazon EC2？

Lightsail 为您提供了一种以捆绑式、可预测且低廉的价格运行和扩展各种基于云的应用程序的简便方法。Lightsail 还会自动设置您的云环境配置，例如网络和访问管理。

导出到 Amazon EC2 允许您在更广泛的实例类型上运行应用程序，从具有更高 CPU 能力、内存和联网功能的虚拟机，到带有 FPGAs 和的专用或加速实例 GPUs。此外，Amazon EC2 执行的自动管理和设置较少，这使您可以更好地控制云环境（例如 VPC）的配置方式。

出口到亚马逊是如何 EC2 运作的？

首先，您需要导出 Lightsail 实例或块存储磁盘的手动快照。然后，熟悉亚马逊 EC2 的客户可以使用亚马逊 EC2 创建向导或 API 来创建新的亚马逊 EC2 实例或亚马逊 EBS 卷，就像使用现有 EC2 AMI 或 EBS 卷一样。或者，Lightsail 还提供引导式 Lightsail 控制台体验，以帮助您轻松创建新实例。 EC2

> **Note**
>
> cPanel 和 WHM (CentOS 7) 实例的快照无法导出到亚马逊。 EC2

如何计费？

使用 “导出到 Amazon EC2 ” 功能是免费的。将手动快照导出到亚马逊后 EC2，除了您的 Lightsail 手动快照之外，您还需要单独支付亚马逊 EC2 图片的费用。您启动的任何新亚马逊 EC2 实例也将由亚马逊收费 EC2，包括其亚马逊 EBS 存储量和数据传输。有关您的新实例和资源的 EC2 定价详情，请参阅 Amazon 定价页面。继续在你的 Lightsail 账户中运行的 Lightsail 资源将继续按正常费率计费，直到它们被删除。

我是否可导出托管数据库或磁盘快照？

导出功能允许您手动导出 Lightsail 磁盘快照，但目前不支持托管数据库的手动快照。磁盘快照可以从亚马逊 EC2 控制台或 API 恢复为 Amazon EBS 卷。

我可以导出哪些 Lightsail 资源？

Lightsail 导出到亚马逊 EC2 功能旨在支持将 Linux 和 Windows 实例快照导出到亚马逊。 EC2该功能还支持将数据块存储磁盘快照导出到 Amazon EBS。它目前不支持数据库、容器服务、内容分发网络 (CDN) 分发、负载均衡器 IPs、静态记录和 DNS 记录的导出。此外，Django、Ghost 和 cPanel & WHM 实例的快照 EC2 目前无法导出到亚马逊。

实例

什么是 Lightsail 实例？

Lightsail 实例是一种虚拟专用服务器 (VPS)，它位于中。 AWS Cloud使用 Lightsail 实例存储数据、运行代码以及构建基于 Web 的应用程序或网站。您的实例可以相互连接，并可以通过公用网络 (Internet)

和专用网络 (VPC) 连接到其他 AWS 资源。您可以直接从 Lightsail 控制台轻松创建、管理和连接实例。

什么是 Lightsail 计划？

Lightsail 计划也称为捆绑包，包括具有固定内存 (RAM) 和计算 (vCPUs) 量的虚拟服务器、基于 SSD 的存储（磁盘）以及免费数据传输限额。Lightsail 计划还提供静态 IPv4 地址和 DNS 管理。Lightsail 套餐按小时按需收费，因此您只需在使用套餐时才支付费用。

我可以在我的实例上运行什么软件？

Lightsail 提供了一系列操作系统和应用程序模板，这些模板会在您创建新的 Lightsail 实例时自动安装。应用程序模板包括 M WordPress ultisite WordPress、cPanel 和 WHM、、Django、Drupal PrestaShop、Ghost、Joomla！、Magento、Redmine、LAMP、Nginx (LEMP)、MEAN 和 Node.js。

您可以通过使用浏览器内 SSH 或您自己的 SSH 客户端在您的实例上安装其他软件。

我可以在 Lightsail 上使用哪些操作系统？

Lightsail 目前支持 7 个 Linux 或类似 Unix 的发行版：AlmaLinux OS 9，亚马逊 Linux 2，亚马逊 Linux 2023，CentOS, Debian, FreeBSD, OpenSUSE，以及 Ubuntu，以及三个 Windows Server 版本：2016 年、2019 年和 2022 年。

我需要自带许可证才能使用 Lightsail 实例吗？

Lightsail 上可用的所有实例蓝图都包含许可证，cPanel 和 WHM 蓝图除外。该蓝图包括 15 天的试用许可证。有关更多信息，请参阅 Amazon Lightsai l 上的快速入门指南：cPanel 和 WHM。对于所有其他实例蓝图，您无需自带许可 (BYOL)。

如何创建 Lightsail 实例？

登录 Lightsail 后，你可以使用 Lightsail 控制台、命令行界面 (CLI) 或 API 来创建和管理实例。

首次登录该控制台时，请选择“创建实例”。在“创建实例”页面中，您可以为您的实例选择软件、位置和名称。选择“创建”后，您的新实例将在几分钟内自动运行。

Lightsail 实例的性能如何？

Lightsail 实例是专门 AWS 为 Web 服务器、开发者环境和小型数据库用例设计的。此类工作负载不会经常或持续使用全部 CPU，但偶尔需要性能突增。Lightsail 使用可突发性能实例，这些实例可提供

CPU 性能的基准水平，并具有突破基准的额外能力。利用此设计，您可以在有需要时获得所需的性能，同时还能避免在其他环境中超额订阅时通常会遇到的性能可变或其他常见副作用。

如果您需要高度可配置的环境和具有持续高 CPU 性能的实例，用于视频编码或 HPC 应用程序等应用程序，我们建议您使用 Amazon EC2。

如何知道我的实例何时突增？

在实例的 CPU 使用率指标图表上，您将看到一个可持续区域和一个可突增区域。您的 Lightsail 实例可以在可持续区域中无限期地运行，而不会影响系统的运行。在高负载下，您的实例可能会开始在可突增区域内运行。在可突增区域内运行时，您的实例会消耗更多的 CPU 周期。因此，它只能在此区域内运行一段有限的时间。有关更多信息，请参阅在 Amazon Lightsail 中查看实例指标。

添加指标警报，以便在实例的 CPU 使用率从可持续区域跨越到突增区域时收到通知。有关更多信息，请参阅在 Amazon Lightsail 中创建实例指标警报。

如何连接到 Lightsail 实例？

Lightsail 提供直接从浏览器到实例终端的一键式安全连接，基于 Linux/UNIX 的实例支持 SSH 访问，基于 Windows 的实例支持 RDP 访问。要使用一键式连接，请启动实例管理屏幕，选择 Connect using SSH (使用 SSH 连接) 或 Connect using RDP (使用 RDP 连接)，此时将打开新的浏览器窗口并自动连接到您的实例。

如果您更喜欢使用自己的客户端连接到基于 Linux/UNIX 的实例，Lightsail 将为您完成 SSH 密钥存储和管理工作，并为您提供在 SSH 客户端中使用的安全密钥。

如何备份我的实例？

如果您想备份数据，可以使用 Lightsail 控制台或 API 来创建实例的手动快照，或者启用自动快照让 Lightsail 为您创建每日快照。如果出现故障或代码部署有误，您可以稍后使用您的实例快照创建全新的实例。有关更多信息，请参阅快照。

我能否升级我的计划？

是。您可以使用实例的快照创建一个更大的新实例。有关更多信息，请参阅快照。

如何将 Lightsail 实例连接到我 AWS 账户中的其他资源？

您可以使用 VPC 对等互连将您的 Lightsail 实例私下连接到 AWS 账户中的 Amazon VPC 资源。只需在你的 Lightsail 账户页面上选择 “启用 VPC 对等”，Lightsail 就会为你完成工作。启用 VPC 对等互连后，您可以使用私 IPs有 AWS 资源访问默认 Amazon VPC 中的其他资源。在此处查找说明。

> **Note**
>
> 请注意，您需要在 AWS 账户中设置默认 Amazon VPC，才能与 Lightsail 的 VPC 对等互通。AWS 2013 年 12 月之前创建的账户没有默认 VPC，您需要进行设置。在此处查找有关设置默认 VPC 的更多信息。

停止实例和删除实例有何区别？

当您停止实例时，它将会断电并保持在当前状态，您可以随时再次启动它。停止您的实例将释放其公有 IPv4地址，因此建议您为在停止和启动后必须保留相同 IP 的实例使用静态 IPv4 地址。请注意，即使实例已停止和启动，附加到实例的公有 IPv6 地址也不会改变。

当您删除实例时，您执行的是破坏性操作。除非您已创建实例快照，否则所有实例数据都将丢失并且无法再恢复。除非您通过将自动快照复制为手动快照来保留它们，否则它们也会随实例一起删除。还将释放实例的公有和私有 IP 地址。如果您在该实例上使用静态 IPv4 地址，则静态 IPv4地址会被分离，但仍保留在您的账户中。

负载均衡器

我可以用 Lightsail 负载均衡器做什么？

Lightsail 负载均衡器允许您构建高度可用的网站和应用程序。Lightsail 负载均衡器通过在不同可用区的实例之间分配流量并将流量仅指向健康的目标实例，从而降低了应用程序因实例问题或数据中心中断而停机的风险。借助 Lightsail 负载均衡器和多个目标实例，您的网站或应用程序还可以适应网络流量的增长，并在加载高峰时段为访客保持良好的性能。

此外，您还可以使用 Lightsail 负载均衡器来帮助您构建安全的应用程序并接受 HTTPS 流量。Lightsail 消除了请求、配置和维护 SSL/TLS 证书的复杂性。内置的证书管理功能代表您申请和续订证书，并将证书自动添加到负载均衡器中。

我能否将负载均衡器用于不同 AWS 区域 或不同可用区的实例？

您不能将负载均衡器用于在不同 AWS 区域中运行的实例。不过，您可以将负载均衡器用于不同可用区中的目标实例。实际上，我们建议您在不同可用区中分配目标实例以最大限度提高应用程序可用性。

我的 Lightsail 负载均衡器如何应对流量峰值？

Lightsail 负载均衡器会自动扩展以应对应用程序的流量峰值，而无需您手动调整它们。如果您的应用程序出现短暂的流量峰值，您的 Lightsail 负载均衡器将自动扩展并继续高效地将流量引导到您的 Lightsail 实例。虽然您的 Lightsail 负载均衡器专为轻松管理流量峰值而设计，但流量持续非常高的应用程序可能会遇到性能下降或受限的情况。如果您希望您的应用程序能够持续管理超过 5 GB/小时的数据或持续拥有大量连接（每小时新连接数超过 400 万，活跃并发连接数超过 15k），我们建议改用带有应用程序负载平衡功能的 Amazon。 EC2

Lightsail 负载均衡器如何将流量路由到我的目标实例？

Lightsail 负载均衡器根据轮询算法将流量引导到您的健康目标实例。

Lightsail 如何知道我的目标实例是否运行正常？

在您创建负载均衡器并连接实例后，Lightsail 会向您的 Web 应用程序的根目录发送运行状况检查请求。您可以通过指定 Lightsail ping 的路径（常用文件或网页 URL）来自定义位置。如果使用此路径可以到达目标实例，那么 Lightsail 会将流量路由到那里。如果您的一个目标实例没有响应，则运行状况检查将失败，并且 Lightsail 不会将流量路由到该实例。了解运行状况检查的更多信息

我可以将多少个实例连接到负载均衡器？

您可以根据需要向负载均衡器添加任意数量的目标实例，最多不超过您的 Lightsail 账户实例配额。

我是否可以将一个实例分配给多个负载均衡器？

是的，如果需要，Lightsail 支持将实例添加为多个负载均衡器的目标实例。

在删除负载均衡器时，我的目标实例会发生什么情况？

如果您删除负载均衡器，则附加的目标实例将继续正常运行，并将作为常规 Lightsail 实例显示在 Lightsail 控制台中。请注意，在删除负载均衡器后，您可能需要更新 DNS 记录以将流量传送到以前的某个目标实例。

什么是会话持久性？

通过使用会话持久性，负载均衡器可以将访客的会话绑定到特定目标实例。这可确保在会话期间将来自用户的所有请求发送到相同的目标实例。Lightsail 支持要求访问者访问相同目标实例以保持数据一致性

的应用程序。例如，需要用户身份验证的很多应用程序可以从使用会话持久性中受益。在创建后，您可以从负载均衡器管理屏幕中为特定负载均衡器启用会话持久性。有关更多信息，请参阅为负载均衡器启用会话持久性。

Lightsail 负载均衡器支持哪种连接？

Lightsail 负载均衡器支持 HTTP 和 HTTPS 连接。

Lightsail 负载均衡器是否支持？ IPv6

2021 年 1 月 12 日之后创建的 Lightsail 负载均衡器默认在双栈模式下运行（即，它们接受通过和 IPv4 协议传输的客户端流量）。 IPv6 IPv6 可以通过在负载均衡器管理页面的 “网络” 选项卡上切换，在此日期之前创建的负载均衡器上启用。 IPv6 也可以使用此开关在任何负载均衡器上禁用。

是否需要启用负载均衡器后面的实例才能使用 IPv6 已启用的负载均 IPv6 衡器？

不是。 负载均衡器同时接受 IPv4 和 IPv6 流量，并在与后端实例通信 IPv4时将其无缝转换为。因此，负载均衡器背后的实例可以是双堆栈的，也可以是 IPv4 只有双栈的。

手动和自动快照

什么是快照

快照是实例、数据库或块存储磁盘的 point-in-time备份。您可以随时为资源创建快照，也可以在实例和磁盘上启用自动快照，让 Lightsail 为您创建快照。您可以将快照用作基准，以创建新资源或备份您的数据。快照包含恢复您的资源所需的所有数据（从拍摄快照的那一刻开始）。当您通过从快照中创建资源来进行恢复时，新资源作为创建快照所用原始资源的准确副本开始。

您可以手动拍摄 Lightsail 实例、磁盘和数据库的快照，也可以使用自动快照指示 Lightsail 自动拍摄实例和磁盘的每日快照。有关更多信息，请参阅快照。

什么是自动快照？

自动快照是一种在 Amazon Lightsail 中安排 Linux/Unix 实例每日快照的方法。您可以选择一天中的某个时间，Lightsail 每天都会在您选择的时间自动为您拍摄快照，并始终保留最新的七张自动快照。启用快照是免费的，您只需为您的快照使用的实际存储付费。

手动快照与自动快照之间有什么区别？

自动快照不能被标记或直接导出到 Amazon EC2。但自动快照可以复制并转换为手动快照。要将自动快照复制为手动快照，从自动快照的上下文菜单中选择 Keep (保留) 以将其复制为手动快照。

哪些资源支持快照？

可以为实例、数据库和磁盘创建手动快照。

可以使用 Lightsail 控制台、Lightsail API 或，为 Linux 或 Unix 实例启用自动快照，也可以仅使用 Lightsail API 为磁盘启用自动快照 AWS CLI，或者。 AWS CLI Windows 实例或托管数据库当前不支持自动快照。

我可以存储快照多长时间？

手动快照将会存储到您选择删除它们为止。有关更多信息，请参阅在 Amazon Lightsail 中删除快照。

自动快照会一直保存下去，直到被更新的自动快照所取代。Lightsail 存储最新的七张自动快照，然后删除最旧的快照并将其替换为最新的快照。但是，您可以通过将特定的自动快照复制为手动快照来保留它。有关更多信息，请参阅在 Amazon Lightsail 中保存实例或磁盘的自动快照。对于您的账户中存储的自动快照，将向您收取快照存储费。

如何启用自动快照？

可以使用 Lightsail 控制台、Lightsail API 启用自动快照，也可以在创建 Linux 或 Unix 实例 AWS CLI 时启用，或者稍后在实例运行后启用自动快照。

也可以在创建磁盘时或创建磁盘之后为其启用自动快照；但是，只能使用 Lightsail API 或。 AWS CLI

有关更多信息，请参阅在 Amazon Lightsail 中启用或禁用实例或磁盘的自动快照。

何时创建自动快照？

启用自动快照后，将根据资源所在的 AWS 区域 设置默认时间。您可以将自动快照更改为一天中您的首选时间，以小时为单位。有关更多信息，请参阅在 Amazon Lightsail 中更改实例或磁盘的自动快照时间。

我可以存储多少个快照？

您可以存储任意数量的手动快照。但是，仅存储最新的 7 个自动快照，然后将最旧的一个替换为最新的一个。

快照如何计费？

您只需为存储在您的 Lightsail 账户中的快照付费。Lightsail 快照（手动和自动）的存储费用为每月 0.05美元/GB。

如果禁用自动快照，是否会丢失快照？

不是。 如果您禁用自动快照，Lightsail 将停止创建每日快照，并保留您现有的自动快照。重新启用自动快照后，Lightsail 将恢复拍摄每日快照，删除最旧的快照并将其替换为最新的快照。

如果我不想替换自动快照该怎么办？

您可以通过将特定的自动快照复制为手动快照来保留它。有关更多信息，请参阅在 Amazon Lightsail 中保存实例或磁盘的自动快照。

我是否可以删除自动快照？

您可以随时通过从自动快照的上下文菜单中选择 Delete (删除) 来删除自动快照。有关更多信息，请参阅删除自动实例快照。

如何使用快照？

如果原始资源有问题，则可以将快照用作基准或者创建新资源。有关更多信息，请参阅快照。

也可以将快照导出到 Amazon EC2 ，以便在该服务中创建新资源。有关更多信息，请参阅将快照导出到 Amazon EC2。

资源运行状况指标和警报

什么是指标？

Lightsail 报告实例、数据库和负载均衡器的指标数据。某些指标包括实例的 CPU 使用率百分比、入站和出站网络流量、系统和实例错误计数、数据库磁盘队列深度、数据库可用存储空间、负载均衡器错误计数、负载均衡器响应时间等。通过指标可以监控和维护资源的可靠性、可用性和性能。定期监控和收集资源中的指标数据，以便您能够更轻松地调试多点故障（如果发生）。有关更多信息，请参阅资源指标。

什么是警报？

您可以在 Lightsail 中创建警报，用于监视您的实例、数据库和负载均衡器的指标。可以将警报配置为根据您指定了阈值的指标值来向您发送通知。有关更多信息，请参阅警报。

通知可以是显示在 Lightsail 控制台中的横幅、发送到您的电子邮件地址的电子邮件以及发送到您的手机号码的 SMS 短信。有关通知的更多信息，请参阅通知。

我可以添加多少个警报？

对于实例、数据库和负载均衡器可用的每个指标，您可以配置两个警报。有关更多信息，请参阅警报。

网络连接

如何在 Lightsail 中使用 IP 地址？

每个 Lightsail 实例都会自动获得一个私有 IPv4 IPv4地址、一个公共地址或一个公共 IPv6 地址（IPv6 必须为 2021 年 1 月 12 日之前创建的实例手动启用）。您可以免费使用私有 IP 在 Lightsail 实例和 AWS 资源之间私下传输数据。您可以使用公有 IP 从互联网连接到您的实例，例如，通过已注册域名或通过本地计算机的 SSH 或 RDP 连接，等等。您也可以将静态 IPv4 地址附加到实例，该 IPv4 地址将替换为即使实例停止和启动也不会更改 IPv4 的地址。 IPv6 分配给该实例的地址保持不变，直到实例被删除或通过在实例 IPv6 上禁用来手动释放 IPv6 地址。

Lightsail 是否支持仅限实 IPv6例？

是的，Lightsail 实例支持双堆栈（IPv4 和 IPv6）和 IPv6仅限双栈配置。

什么是静态 IP？

静态 IP 是一个固定的公共 IP 地址，专用于你的 Lightsail 账户。您可以为实例分配静态 IPv4 地址，取代其公共地址 IPv4。如果您决定将您的实例替换为另一个实例，则可以将该静态 IP 重新分配给新实例。这样，您就不必在每次要替换实例时重新配置任何外部系统（如 DNS 记录）以指向新的 IP 地址。Lightsail 目前仅支持静态 IPs 模式。 IPv4 静态 IPv6 地址不可用。但是， IPv6 在删除实例或通过在实例 IPv6 上禁用手动释放 IPv6 地址之前，分配给该实例的地址保持不变。

我 IPs 可以将多少静态实例附加到一个实例？

您一次只能将一个静态 IP 附加到实例。

什么是 DNS 记录？

DNS 是一项全球分布式服务，它将用户可读名称（如 www.example.com）转换为字母数字 IP 地址（如 192.0.2.1），供计算机用来互相连接。使用 Lightsail，您可以轻松地将注册的域名映射photos.example.com到您的 Lightsail IPs 实例的公众。这样，当用户像在浏览器中一样键example.com入人类可读的名称时，Lightsail 会自动将该地址转换为您要引导用户访问的实例的 IP。这些转换都称为 DNS 查询。

重要的是要知道，要在 Lightsail 中使用域名，必须先对其进行注册。您可以使用 Lightsail 或您的首选 DNS 注册商注册域名。

我能否管理我的实例的防火墙设置？

是。您可以使用 Lightsail 防火墙控制实例的数据流量。在 Lightsail 控制台中，您可以设置规则，规定不同类型的流量可以公开访问您的实例的哪些端口。

对象存储和存储桶

我可以使用 Lightsail 对象存储执行哪些操作？

您可以在 Lightsail 对象存储服务中将静态内容（如图像、视频和 HTML 文件）存储到存储桶中。您可以将存储在存储桶中的对象用于您的网站和应用程序。Lightsail 对象存储可以关联到您的 Lightsail CDN 分配，只需点击几下，便可以快速轻松地将内容交付给全球受众。它还可以用作低成本、安全的备份解决方案。有关更多信息，请参阅对象存储。

Lightsail 对象存储如何收费？

在所有可用 Lightsail 的版本中，Lights AWS 区域 ail 对象存储都有三种不同的固定价格捆绑包。第一个套餐的价格为每月 1 美元，前 12 个月免费。此套餐包含 5 GB 存储容量和 25 GB 的数据传输。第二个套餐的价格为每月 3 美元，包含 100 GB 存储容量和 250 GB 的数据传输。最后，第三个套餐的价格为每月 5 美元，包含 250 GB 存储容量和 500 GB 的数据传输。Lightsail 对象存储可以无限制地将数据传输到您的存储桶，因为套餐的数据传输限额仅针对从存储桶传出的数据。

Lightsail 对象存储是否有超额费用？

如果对于单个存储桶，您超出所选存储计划的月度存储容量或数据传输限额，您将需要为超出的使用量付费。有关更多信息，请参阅 Lightsail 定价页。

对象存储如何使用我的数据传输限额？

您可以通过将数据传入和传出 Lightsail 对象存储来消耗数据传输限额，但以下情况除外。

- 数据从互联网传输到 Lightsail 对象存储器
- Lightsail 对象存储资源之间的数据传输
- 数据从 Lightsail 对象存储器传输到同一个 Lightsail 资源中的另一个 Lightsail 资源 AWS 区域（包括转移到不同 AWS 账户中的资源，但使用相同账户）AWS 区域
- 数据从 Lightsail 对象存储传输到 Lightsail CDN 发行版

我可以更改与我的 Lightsail 存储桶关联的计划吗？

是的，您可以在每月 AWS 账单周期内更改单个 Lightsail 存储分区的存储套餐一次。

是否可以将对象从 Lightsail 对象存储复制到 Amazon S3？

是的，支持从 Lightsail 对象存储复制到 Amazon S3。有关更多信息，请参阅 AWS Premium Support 知识中心中的如何将所有对象从一个 Amazon S3 存储桶复制到另一个存储桶？。

如何开始使用 Lightsail 对象存储？

要使用 Lightsail 对象存储，您必须首先创建用于存储数据的存储桶。有关更多信息，请参阅创建存储桶。在存储桶启动并运行后，您可以通过使用 Lightsail 控制台上传文件或配置应用程序以将日志或其他应用程序数据等内容放入存储桶中，开始向存储桶添加对象。或者，你也可以通过使用 AWS Command Line Interface ()AWS CLI开始使用 Lightsail 对象存储。

如何将对象上传到我的存储桶？

要将对象（如图像或其他静态文件）上传到您的存储桶，请从对象”顶部导航选项卡中选择“上传”，然后从计算机中选择正确的文件或目录。或者，将文件和目录从桌面拖放到 Lightsail 对象存储控制台中的标记区域。

可以阻止对存储桶的公有访问吗？

Lightsail 存储桶和对象默认设置为私有，这意味着只有具有相应权限的用户才能访问存储桶和对象。用户可以更改此默认设置，将私有存储桶中将个别对象设为公有和只读，或者选择将整个存储桶设为公有

和只读。当用户将存储桶或对象设为公有时，世界上的任何人都可以读取其内容。有关更多信息，请参阅存储桶的权限。

如何提供存储桶的编程访问权限？

您可以使用访问密钥或角色来提供存储桶的编程访问权限。首先，在 Lightsail 控制台中选择要以编程方式连接的存储桶。其次，在 “权限” 选项卡下，创建访问密钥或为 Lightsail 实例分配角色，然后配置您的网站或应用程序代码以使用您的存储桶。根据您计划的网站或应用程序使用对象存储的方式，此操作可能有所不同。有关更多信息，请参阅存储桶的权限。

如何与其他 AWS 账户共享存储桶？

Lightsail 允许您使用您在存储分区管理页面的跨账户访问部分中指定的 AWS 账户 ID 共享存储分区的访问权限，从而简化跨账户共享。指定账户 ID 后，该 AWS 账户将拥有对存储桶的只读访问权限。有关更多信息，请参阅存储桶的权限。

什么是版本控制？

版本控制功能可以保留、检索和还原存储桶中每个对象存储的各个版本，为防止意外覆盖和删除提供了额外保护。有关更多信息，请参阅启用和暂停存储桶中的对象版本控制。

如何将我的 Lightsail 存储桶关联到我的 Lightsail CDN 分配？

Lightsail 对象存储可以关联到 Lightsail CDN 分配，只需点击几下，便可以快速轻松地将内容交付给全球受众。为此，请创建一个 Lightsail CDN 分配，然后只需选择 Lightsail 存储桶作为 Lightsail CDN 分配的源。有关更多信息，请参阅使用 Amazon Lightsail 存储桶与 Lightsail 内容分发网络分配。

Lightsail 对象存储服务有什么限制？

每个账户最多可以在 Lightsail 对象存储服务中创建 20 个存储桶。对存储桶中可存储的项目数没有限制。您可以在单个存储桶中存储所有对象，也可以在多个存储桶中组织它们。

Lightsail 对象存储是否支持监控和提醒？

利用 Lightsail 对象存储，客户可以轻松查看存储桶内已用空间总量以及存储桶内对象数量的指标。还支持基于这些指标的提醒。有关更多信息，请参阅在 Amazon Lightsail 中查看存储桶的指标和创建存储桶指标警报。

Lightsail 中的标签

标签是什么？

标签是您分配给 Lightsail 资源的标签。每个标签都由键 和值组成，这两个参数都由您定义。标签值是可选的，因此您可以选择创建 “仅密钥” 标签，用于在 Lightsail 控制台中筛选资源。

如何在 Lightsail 中使用标签？

借助标签，您可以在 Lightsail 控制台和 API 中对资源进行分组和筛选，跟踪和整理账单中的费用，并通过访问管理规则规定谁可以查看或修改您的资源。通过标记您的资源，您可以：

- 整理 — 使用 Lightsail 控制台和 API 筛选器根据您为其分配的标签来查看和管理资源。这在您拥有许多同类型资源时很有用 - 您可以根据分配给资源的标签快速识别特定资源。
- 成本分配 – 通过在账单控制台中标记资源并创建“成本分配标签”，跨不同项目或用户跟踪和分配成本。例如，您可以拆分您的账单，并按项目或客户端了解您的成本。
- 管理访问权限-使用策略控制有权访问您 AWS 账户的用户如何编辑、创建和删除 Lightsail 资源。AWS Identity and Access Management 这使您可以更轻松地与其他人协作，而无需授予他们对您的 Lightsail 资源的完全访问权限。

有关在 Lightsail 中使用标签的更多信息，请参阅标签。

什么资源可以标记？

Lightsail 目前支持为以下资源添加标签：

- 实例 (Linux 和 Windows)
- 容器服务
- 数据块存储磁盘
- 负载均衡器
- 数据库
- DNS 区域
- 实例、磁盘和数据库的手动快照

手动快照支持标签；但是，您必须使用 Lightsail API 或 AWS CLI 来标记快照。如果您使用 Lightsail 控制台创建带标签的实例、磁盘或数据库的手动快照，则会自动为手动快照指定与源资源相同的标签。当您使用 Lightsail 控制台从带标签的手动快照创建新资源时，您可以编辑这些标签。

无法标记自动快照。

如何标记我的 Lightsail 快照？

Lightsail 控制台会自动使用与其源资源相同的标签来标记手动快照。如果您使用 Lightsail API 或 AWS CLI 创建快照，则可以自己为快照选择标签。

> **Important**
>
> 数据库手动快照的标签目前没有包含在账单报告（成本分配标签）中。

键-值和仅键标签之间有什么差别？

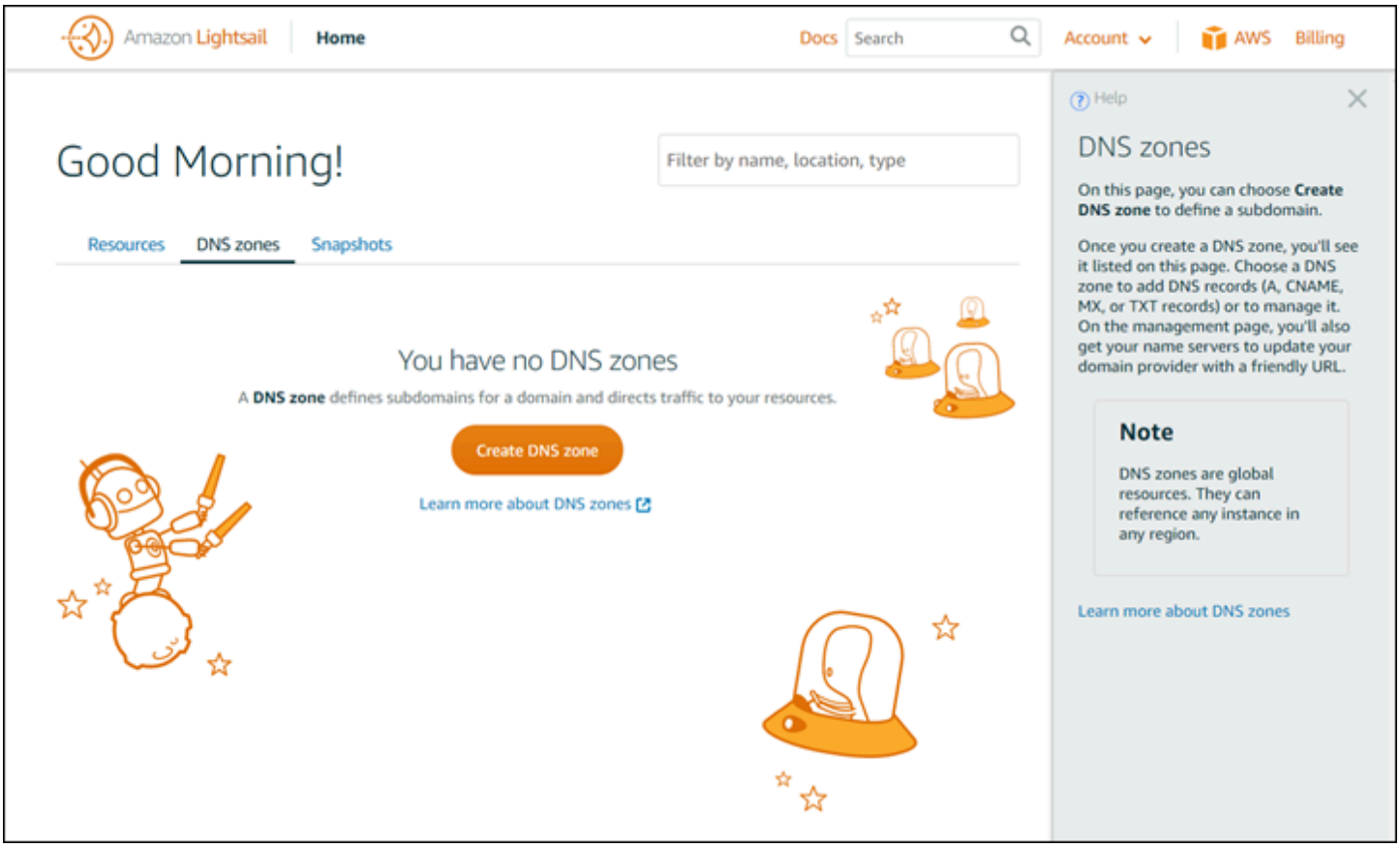
Lightsail 标签是键值对，允许你组织不同类别的资源，例如实例（例如 Project: Blog、Project: Game、Project: Game、Project: Game、Project: Test）。这使您能够对所有使用案例 (例如资源组织、账单报告和访问管理) 进行全面控制。Lightsail 控制台还允许您使用仅限密钥的标签来标记资源，以便在控制台中进行快速筛选。

查找 Lightsail 的有用资源

在 Amazon Lightsail 中，你可以通过多种方式寻求帮助。

上下文相关的帮助面板

Lightsail 在控制台的每个页面上都有一个上下文相关的 “帮助” 面板，其中包含特定于你所在页面的其他提示和信息。当您对页面上的某些内容有疑问时，可打开此帮助面板，然后在您准备好后将其关闭。您可以通过在任何页面上选择 Help（帮助）或通过选择用户界面中的任何小型问号来打开此帮助面板。



关于本用户指南

亚马逊 Lightsail 用户指南包含操作主题和概念概述，可帮助您使用 Lightsail。例如，您可以创建实例、连接到实例，或管理域。

使用搜索

您可以使用每页顶部的搜索框从 Lightsail 中的任何页面搜索文档主题。要优化您的搜索，可以从文档搜索页面再次搜索。

找不到所查找的内容？ 向我们发送反馈，我们将着手处理。在 Lightsail 的每个页面上，您可以选择“提供反馈并提交反馈” 以提出建议。

使用 Lightsail CLI 和 API

你可以使用 AWS Command Line Interface (AWS CLI) 或 Lightsail REST API 来创建、读取、更新和删除 Lightsail 资源。除了 REST API 之外，我们还有多种语言的 SDK，包括 Java、Ruby、JavaScript (Node.js)、Go、PHP、PHP、Python、.NET (C#) 和 C++。有关 Lightsail API 的更多信息，请参阅 Lightsail API 参考。

> **Note**
>
> 您需要生成访问密钥才能使用 Lightsail API。详细了解如何设置访问密钥以使用 Lightsail API。

当你使用 Light AWS CLI sail 资源时，这会很有帮助。在 AWS 中 AWS CLI，只需键入`aws lightsail help`即可了解可用的命令。有关特定 CLI 命令的帮助，请键入该命令名称，后跟`help`，以了解其参数和例外的更多信息。有关更多信息，请参阅 Lightsail CLI 参考文档。

AWS 论坛和其他社区资源

您也可以在我们的 AWS 讨论论坛中发布您的问题：AWS 论坛。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。