在Linux服务器安装配置Redis

1.描述

介绍如何在Linux服务器安装Redis。

2.在Linux服务器安装Redis

基于Debian（操作系统为Ubuntu）

操作步骤

1. 安装Redis。

   ①通过SSH终端执行以下命令，更新apt软件包列表。

   ```
   sudo apt update
   ```

   ②执行以下命令，安装Redis。

   ```
   sudo apt install redis-server
   ```

   ③安装完成后，Redis服务将自动启动。执行以下命令，检查服务的状态。

   ```
   sudo systemctl status redis-server
   ```

   输出类似如下的内容，表示您已在服务器上安装并运行Redis。

   ```
   redis-server.service - Advanced key-value store
     Loaded: loaded (/lib/systemd/system/redis-server.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2018-10-28 05:10:45 PDT; 2h ago
       Docs: http://redis.io/documentation,
             man:redis-server(1)
   Process: 2197 ExecStop=/bin/kill -s TERM $MAINPID (code=exited, status=0/SUCCESS)
   Process: 2201 ExecStart=/usr/bin/redis-server /etc/redis/redis.conf (code=exited, status=0/SUCCESS)
   Main PID: 2226 (redis-server)
      Tasks: 4 (limit: 2319)
     CGroup: /system.slice/redis-server.service
             `-2226 /usr/bin/redis-server 0.0.0.0:6379
   ```

   如果您的服务器上禁用了IPv6，则Redis服务将无法启动。

2. 配置Redis远程访问。

   默认情况下，Redis不允许远程连接。您只能从运行Redis的计算机127.0.0.1（localhost）连接到Redis服务器。

   仅当您要从远程主机连接到Redis服务器时，才执行以下步骤。如果使用单个服务器设置，并且应用程序和Redis在同一台计算机上运行，则不需要启用远程访问。

   ①要将Redis配置为接受远程连接，请使用文本编辑器打开Redis配置文件。执行以下命令：

   ```
   sudo vi /etc/redis/redis.conf
   ```

   在这个文件中，找到以“bind 127.0.0.1 ::1 ”开头的行，并替换“127.0.0.1”为“0.0.0.0”。

```
# IF YOU ARE SURE YOU WANT YOUR INSTANCE TO LISTEN TO ALL THE INTERFACES
# JUST COMMENT THE FOLLOWING LINE.
#
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
bind 0.0.0.0 ::1
```

编辑完之后，保存并关闭。

②执行以下命令，重启Redis服务使之生效。

```
sudo systemctl restart redis-server
```

③执行以下命令来验证redis正在侦听端口6379上的所有接口。

```
ss -an | grep 6379
```

输出类似如下内容，“0.0.0.0”表示该机器上的所有IPv4地址。

```
tcp  LISTEN 0   128   0.0.0.0:6379   0.0.0.0:*
tcp  LISTEN 0   128      [::]:6379      [::]:*
```

④添加防火墙规则，以启用来自远程计算机上TCP端口6379。

假设您正在使用UFW管理防火墙，并且要允许从192.168.121.0/24子网进行访问，则可以执行以下命令：

```
sudo ufw allow proto tcp from 192.168.121.0/24 to any port 6379
```

此时，Redis服务器将接受TCP端口6379上的远程连接。您需要确保将防火墙配置为仅接受来自受信任IP范围的连接。

要验证所有设置是否正确，您可以尝试使用redis-cli实用程序从远程计算机ping Redis服务器。执行以下命令：

```
redis-cli -h <REDIS_IP_ADDRESS> ping
```

该命令应返回PONG的响应：

```
PONG
```

结束

基于RPM（操作系统为CentOS、RedHat 7.6、中标麒麟）

操作步骤

1. 安装Redis。

   在安装Redis之前，我们必须首先将Enterprise Linux的额外软件包（EPEL）存储库添加到服务器的软件包列表中。
   EPEL是一个软件包存储库，其中包含许多开源附加软件包，其中大多数由Fedora Project维护。

   ①执行以下命令，使用yum安装EPEL：

   ```
   sudo yum install epel-release
   ```

   ②EPEL安装完成后，执行以下命令，使用yum安装Redis：

   ```
   sudo yum install redis -y
   ```

   ③安装完成后，执行以下命令，启动Redis服务：

   ```
   sudo systemctl start redis.service
   ```

   ④如果您希望Redis在服务器启动时自动启动，可以执行以下命令：

   ```
   sudo systemctl enable redis
   ```

   ⑤执行以下命令，查看Redis状态：

   ```
   sudo systemctl status redis.service
   ```

   输出类似如下内容，表示Redis运行正常:

```
Output redis.service - Redis persistent key-value database
  Loaded: loaded (/usr/lib/systemd/system/redis.service; disabled; vendor preset: disabled)
Drop-In: /etc/systemd/system/redis.service.d
          limit.conf
  Active: active (running) since Thu 2018-03-01 15:50:38 UTC; 7s ago
Main PID: 3962 (redis-server)
  CGroup: /system.slice/redis.service
          3962 /usr/bin/redis-server 127.0.0.1:6379
```

⑥确认Redis正在运行后，执行以下命令，测试设置：

```
redis-cli ping
```

执行命令后，应该打印PONG作为响应。
如果是这种情况，表示您现在在服务器上运行了Redis，我们可以开始对其进行配置以增强其安全性。

2

绑定Redis并使用防火墙保护。

保护Redis的有效方法是保护正在运行的服务器，即保证Redis仅绑定到localhost或私有IP地址，并且服务器有正在运行的防火墙。

如果您选择使用本教程设置Redis集群，那么您需要更新配置文件以允许从任何地方进行连接，相对于绑定到localhost或私有IP，此种方式不太安全。

①为了解决这一问题，您需要先执行以下命令，打开Redis配置文件进行编辑：

```
sudo vi /etc/redis.conf
```

②在这个文件中，找到以bind开头的行，并确保未将其注掉：

```
bind 127.0.0.1
```

如果您需要将Redis绑定到另一个IP地址（例如，要从单独的主机访问Redis），建议您将其绑定到私有IP地址。因为绑定到公共IP地址会增加Redis接口对外界的暴露。

```
bind 0.0.0.0
```

如果您已满足前提条件并在服务器上安装了防火墙，并且不打算从其他主机连接到Redis，则无需为Redis添加任何其他防火墙规则。

由于Redis服务器的默认独立安装仅在回送接口（127.0.0.1或localhost）上侦听，因此无需担心其默认端口上的传入流量。

③如果您想要从另一台主机访问Redis，则需要使用firewall-cmd命令对您的firewalld配置进行一些更改。
同样，您应该只允许主机使用其私有IP地址从其主机访问Redis服务器，以限制您的服务所使用的主机数量。

1）执行以下命令，将专用的Redis区域添加到您的防火墙策略中：

```
sudo firewall-cmd --permanent --new-zone=redis
```

2）然后，执行以下命令，指定您要打开的端口。Redis默认使用端口6379：

```
sudo firewall-cmd --permanent --zone=redis --add-port=6379/tcp
```

3）接下来，执行以下命令，指定应允许其通过防火墙并访问Redis的任何专用IP地址：

```
sudo firewall-cmd --permanent --zone=redis --add-source=client_server_private_IP
```

4）执行这些命令后，重新加载防火墙以实施新规则：

```
sudo firewall-cmd --reload
```

在这种配置下，当防火墙从您客户端的IP地址看到数据包时，它将在专用Redis区域中的规则应用于该连接。所有其他连接将由默认的公共区域处理。默认区域中的服务适用于每个连接，而不仅限于不明确匹配的服务，因此您无需向Redis区域添加其他服务（例如SSH），因为这些规则将自动应用于该连接。

5）如果选择使用Iptables设置防火墙，则需要执行以下命令授予辅助主机对Redis正在使用的端口的访问权限：

```
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p tcp -s client_servers_private_IP/32 --dport 6379 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
sudo iptables -P INPUT DROP
```

确保使用发行版提供的机制保存您的Iptables防火墙规则。关于Iptables更多信息，请参见Iptables essentials guide。

需要注意的是，使用任一防火墙工具都可以。重要的是防火墙已经启动并运行，这样不明身份的人就无法访问您的服务器。下一步，我们将Redis配置为只能使用强密码访问。

3

配置Redis密码。

如果您已经为Redis配置了密码。您可以按照本节的说明设置更安全的密码。如果您尚未设置密码，本节将介绍如何设置数据库服务器密码。

配置Redis密码将启用其内置安全功能之一：auth命令。该功能要求客户端在被允许访问数据库之前进行身份验证。与绑定设置一样，密码直接在Redis的配置文件“/etc/redis.conf”中配置。

①执行以下命令，重新打开该文件：

```
sudo vi /etc/redis.conf
```

②找到“SECURITY”部分，然后查找带有注释的指令，该指令显示为：

```
# requirepass foobared
```

删除“#”取消注释，然后将“foobared”更改为您设置强密码。
您可以使用apg或pwgen之类的工具来生成一个密码，而不是自己编写一个密码。

如果您不想安装一个应用程序来生成密码，可以使用以下命令。

请注意，每次输入此命令时都会生成相同的密码。要生成不同的密码，请将引号中的单词更改为任何其他单词或短语。

```
echo "digital-ocean" | sha256sum
```

使用此命令生成的密码是一个非常强且非常长的密码，这正是Redis所需的密码类型。复制并粘贴该命令生成的密码，将其作为“requirepass”的新值，如下：

```
requirepass password_copied_from_output
```

如果您想要生成较短的密码，请改为执行以下的命令。同样，更改引号中的单词，使其不会生成与以下密码相同的密码：

```
echo "digital-ocean" | shalsum
```

③设置密码后，保存并关闭文件，然后执行以下命令，重新启动Redis：

```
sudo systemctl restart redis.service
```

④执行以下命令，测试密码是否有效：

```
redis-cli
```

⑤以下是一系列用于测试Redis密码是否有效的命令。第一个命令尝试在身份验证之前将密钥设置为某个值。

```
set key1 10
```

这个命令不会生效，因为我们还没有通过身份验证，所以Redis返回一个如下所示的错误。

```
Output(error) NOAUTH Authentication required.
```

执行以下命令，使用Redis配置文件中指定的密码进行身份验证。

```
auth your_redis_password
```

Redis将确认我们已通过身份验证，如下：

```
OutputOK
```

之后，再次执行前面的命令，应该会成功：

```
set key1 10
OutputOK
```

执行以下命令，向Redis查询新密钥的值。

```
get key1
Output"10"
```

执行以下命令，退出redis-cli。您也可以使用“exit”：

```
quit
```

执行完以上的命令后，未经授权的用户应该很难访问您的Redis。请注意，如果你远程连接到Redis，没有SSL或VPN的情况下，外部用户仍然可以看到未加密的密码。

接下来，我们将查看如何重命名Redis命令，以进一步保护Redis免受恶意攻击者的攻击。

4

重命名危险命令。

Redis内置的另一个安全功能允许您重命名或完全禁用某些被认为是危险的命令。由未经授权的用户运行时，此类命令可用于重新配置、销毁或以其他方式擦除您的数据。

一些已知危险的命令包括：

- FLUSHDB
- FLUSHALL
- KEYS
- PEXPIRE

- DEL
- CONFIG
- SHUTDOWN
- BGREWRITEAOF
- BGSAVE
- SAVE
- SPOP
- SREM RENAME DEBUG

根据站点的情况来决定是否禁用或重命名命令。如果您知道永远不会使用一个可能被滥用的命令，您可以将其禁用。否则，您应该将其重命名。

与身份验证密码一样，重命名或禁用命令也是在“/etc/redis.conf”文件的SECURITY 部分中配置的。

①要启用或禁用Redis命令，请执行以下命令，再次打开配置文件进行编辑：

```
sudo vi   /etc/redis.conf
```

说明：以下是示例。您应该选择禁用或重命名对您有意义的命令。您可以自己检查这些命令，并确定它们在“redis.io/Commands”中可能被误用的情况。

要禁用或终止命令，只需将其重命名为空字符串，如下所示：

```
# It is also possible to completely kill a command by renaming it into
# an empty string:
#
rename-command FLUSHDB ""
rename-command FLUSHALL ""
rename-command DEBUG ""
```

要重命名命令，请为其指定另一个名称，如下所示。

```
rename-command CONFIG ""
rename-command SHUTDOWN SHUTDOWN_MENOT
rename-command CONFIG ASC12_CONFIG
```

②保存更改并关闭文件，然后执行以下命令重新启动Redis，应用更改：

```
sudo systemctl restart redis.service
```

③执行以下命令，测试新命令：

```
redis-cli
```

④执行以下命令，使用您在前面定义的密码进行身份验证：

```
auth your_redis_password
```

```
OutputOK
```

⑤假设您已将CONFIG命令重命名为ASC12_CONFIG，则尝试使用CONFIG命令应该会失败。

```
config get requirepass
```

```
Output(error) ERR unknown command 'config'
```

调用重命名的命令应该成功(不区分大小写)：

```
asc12_config get requirepass
```

```
Output1) "requirepass"
2) "your_redis_password"
```

⑥执行以下命令，退出redis-cli：

```
exit
```

请注意，如果您已经在使用Redis命令行，然后重新启动Redis，则需要重新进行身份验证。
否则，如果您输入命令，则会出现以下错误：

```
OutputNOAUTH Authentication required.
```

5

设置数据目录所有权和文件权限。

通过更改所有权和权限来提升Redis安装的安全配置文件。这包括确保只有需要访问Redis的用户才有权读取其数据。默认情况下，该用户是redis用户。

①您可以通过grep-ing父目录的长列表中的Redis数据目录来验证这一点。该命令及其输出如下所示。

```
ls -l /var/lib | grep redis
```

```
Outputdrwxr-xr-x 2 redis    redis    4096 Aug 6 09:32 redis
```

②您可以看到，redis数据目录归redis用户所有，并授予redis组二级访问权限。此所有权设置是安全的，但文件夹的权限(设置为755)不安全。要确保只有redis用户有权访问该文件夹及其内容，请将权限设置更改为770：

```
sudo chmod 770 /var/lib/redis
```

③您需要更改的另一个权限是Redis配置文件的权限。默认情况下，文件权限为644，由root所有，根组拥有二次所有权：

```
ls -l /etc/redis.conf
```

```
Output-rw-r--r-- 1 root root 30176 Jan 14   2014 /etc/redis.conf
```

④644权限是公开的。这会带来安全问题，因为配置文件包含您在步骤4中配置的未加密密码，这意味着我们需要更改配置文件的所有权和权限。理想情况下，它应该归redis用户所有，由redis组拥有二级所有权。因此，请执行以下命令：

```
sudo chown redis:redis /etc/redis.conf
```

然后更改权限，以便只有该文件的所有者可以对其进行读取和/或写入：

```
sudo chmod 600 /etc/redis.conf
```

执行以下命令验证新的所有权和权限：

```
ls -l /etc/redis.conf
```

```
Outputtotal 40
-rw------- 1 redis redis 29716 Sep 22 18:32 /etc/redis.conf
```

⑤最后，执行以下命令，重启Redis：

```
sudo systemctl restart redis.service
```

结束

回到顶部