检测项	检测内容	加固方法
身份鉴别	应启用 influxdb 的身份验证，防止未授权访问	1、创建一个管理员用户：首先进入 CLI “ influx ”，再输入命令创建用户“ CREATE USER “ <username> ” WITH PASSWORD '<password>' WITH ALL PRIVILEGES ”； 2、打开 influxdb 的配置文件：“ vi /etc/influxdb/influxdb.conf ”； 3、找到 [http] 下的字段：“ auth-enabled = false ”，将“ auth-enabled ”的值改为“ true ” 4、重启 influxdb ：“ service influxdb restart ”
默认端口	应修改 influxdb 管理控制台的的默认端口，防止攻击者扫描到默认端口直接利用	1、打开 influxdb 的配置文件：“ vi /etc/influxdb/influxdb.conf ”； 2、找到 [admin] 下的字段：“ bind-address = ":8083" ”； 3、将 8083 更改为其他端口； 4、重启 influxdb ：“ service influxdb restart ”
访问控制	如无业务需求，建议关闭 web 管理界面	1、打开 influxdb 的配置文件：“ vi /etc/influxdb/influxdb.conf ”； 2、找到 [admin] 下的字段：“ enabled = true ”；将“ enabled ”的值改为“ false ”； 3、重启 influxdb ：“ service influxdb restart ”
	使用 iptables 限制 influxdb 的访问 IP	1、例如只允许 192.168.0.105 访问： “ iptables -I INPUT -p tcp -s 192.168.0.105 --dport 8084 -j ACCEPT ” “ iptables -I INPUT -p tcp -s 192.168.0.105 --dport 8086 -j ACCEPT ”；

		2、保存新增的配置：“ service iptables save ”； 3、重启 iptables ：“ service iptables restart ”。
权限控制	应根据角色创建相应的用户来管理数据库，做到权限分离	1、创建一个非管理员用户：首先进入 CLI “ influx ”，再输入命令创建用户“ CREATE USER “ <username> ” WITH PASSWORD '<password>' ”； 2、给新创建的用户授予相应的权限： “ GRANT [READ,WRITE,ALL] ON “ <database_name> ” TO “ <username> ” ”；
数据备份	应定期对数据库进行备份，并做好备份恢复测试	1、备份：在 linux 终端输入“ influxd backup -database _internal -since 2016-10-12T00:00:00Z /tmp/backup ”对 _internal 数据库进行备份； 2、恢复：在 linux 终端输入：“ influxd restore -database _internal -datadir /var/lib/influxdb/data /tmp/backup ”