Linux虚拟机的安全加固

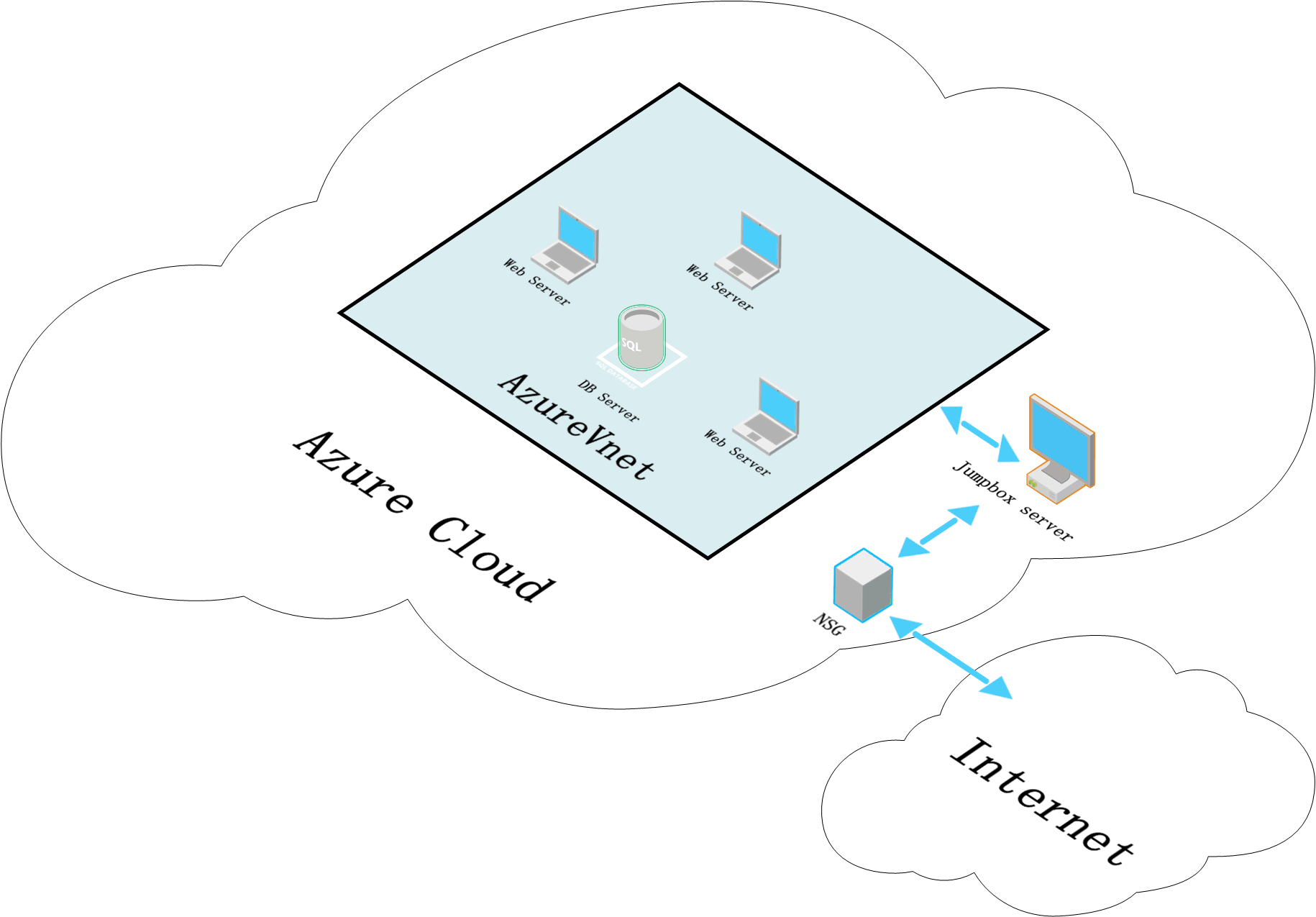
* 背景介绍

在云时代，各种层出不穷的安全问题越来越困扰着用户，数据被恶意删除，加密进行勒索。无差别的恶意攻击致使网络瘫痪。各种流氓软件极大地降低用户体验。基于Azure平台，我们已经通过各种安全手段来保护用户的资源和数据（相关介绍，请参考[这里](https://docs.azure.cn/zh-cn/security/security-virtual-machines-overview)）。对于IaaS的用户，我们还需要在虚拟机内部进行安全加固来提升资源和数据的安全性。以下内容介绍了如何在Linux虚拟机内部通过一些“小手段”来辅助提升Linux系统的安全性。

Important：以下范例基于Azure平台部署的CentOS7.3，如果您使用的是其他版本的Linux操作系统，请注意其中的差异性。

* 方案介绍

**Azure IaaS 安全架构**

****

对于IaaS的虚拟机资源，除了业务需求对外访问的端口开放之外，所有的访问都通过跳板机（Jumpbox）进行内部访问，特别是数据库，重要的业务服务器，一定要启用防火墙进行安全加固。

**Linux虚拟机的安全加固建议**

* + **修改用户的密码口令策略：**

[root@centos-73-1 chpaadmin]# cat /etc/login.defs |grep -i pass

# passwd command) should therefore be configured elsewhere. Refer to

# Password aging controls:

# PASS\_MAX\_DAYS Maximum number of days a password may be used.

# PASS\_MIN\_DAYS Minimum number of days allowed between password changes.

# PASS\_MIN\_LEN Minimum acceptable password length.

# PASS\_WARN\_AGE Number of days warning given before a password expires.

PASS\_MAX\_DAYS 99999 🡪修改密码有效期

PASS\_MIN\_DAYS 0

PASS\_MIN\_LEN 5 🡪修改密码长度

PASS\_WARN\_AGE 7

# the user to be removed (passed as the first argument).

# Use SHA512 to encrypt password.

* + **修改危险文件（命令）权限:**

对于一些比较危险的操作，如：rm,mv,ifconfig,cron,vi等。这类命令会直接对文件或者文件内容进行操作，那么建议上述操作只给具有root权限的管理员来执行。可以通过命令：chmod 700 <command>，来修改上述命令的权限。

* + **用户登录通知：**

目前，客户只能在发现数据或者虚拟机被恶意侵入或者用户的误操作导致了数据的丢失之后，采取善后的手段，但是并没法做到提前的预警。那么通过PAM模块，就可以实现用户登录，root权限获取时，通过邮件等方式进行通知。以实现，预先知道，预先警惕的目标，降低受影响的范围。以下是通过PAM模块实现的邮件通知用户登录的功能。

* + - 以管理员身份登录虚拟机，并切换成root用户。
    - 新建脚本/etc/ssh/login\_notifiy.sh (该脚本可以存放在任意位置，但是需要将后续的路径指定好即可),内容如下：

#!/bin/bash

[ "$PAM\_TYPE" = "open\_session" ] || exit 0

{

echo "User: $PAM\_USER"

echo "Ruser: $PAM\_RUSER"

echo "Rhost: $PAM\_RHOST"

echo "Service: $PAM\_SERVICE"

echo "TTY: $PAM\_TTY"

echo "Date: `date`"

echo "Server: `uname -a`"

} | mail -s "`hostname -s` $PAM\_SERVICE login: $PAM\_USER" [user@yourdomain.com](mailto:user@yourdomain.com)

* + - 编辑文件/etc/pam.d/sshd，在文件最后追加一行：

session optional pam\_exec.so debug /bin/bash /etc/ssh/login-notify.sh

* + - 保存并退出。
    - 至此，每一个用户登录都会发邮件通知给收件人，内容包括用户名以及登录的IP地址信息。如果遇到陌生IP，那么就要注意，该虚拟机是否正在遭受攻击。
    - 同理，你可以在把上述脚本应用到/etc/pam.d/其他模块中，比如sudo，login等，来进行监控。