绿盟堡垒机云服务

技术白皮书

目录

一. IT 安全运维管理变革

随着云计算技术的发展，IT 系统不断发展，网络规模迅速扩大、设备数量激增，建设重点逐步从平台建设，转向以深化应用、提升效益为特征的运行维护阶段， IT 系统运维与安全管理正逐渐走向融合。信息系统的安全运行直接关系企业效益，构建一个强健的 IT 运维安全管理体系对企业信息化的发展至关重要，对运维的安全性提出了更高要求。

目前，面对日趋复杂的 IT 系统，不同背景的运维人员已给企业信息系统安全运行带来较大潜在风险，主要表现在：

1.1 账号管理无序，暗藏巨大风险

- **多个用户混用同一个账号**

这种情况主要出现在同一工作组中，由于工作需要，同时系统管理账号唯一，因此只能多用户共享同一账号。不仅在发生安全事故时难以界定账号的实际使用者和责任人，而且无法对账号的使用范围进行有效控制，存在较大安全隐患。

- **一个用户使用多个账号**

目前，一个维护人员使用多个账号是较为普遍的情况，用户需要记忆多套口令同时在多套主机系统、网络设备之间切换。如果设备数量达到几十甚至上百台时，维护人员进行一项简单的配置需要分别逐一登录相关设备，其工作量和复杂度成倍增加，直接导致的后果是工作效率低下、管理繁琐甚至出现误操作，影响系统正常运行。

1.2 粗放式权限管理，安全性难以保证

大多数单位的 IT 运维均采用操作系统自身的授权系统，授权功能分散在各系统中。管理人员的权限大多是粗放式管理，由于缺少统一的运维操作授权策略，授权粒度粗，无法基于最小权限分配原则管理用户权限，难以与业务管理要求相协调。因此，出现运维人员权限过大、内部操作权限滥用等诸多问题，如果不及时解决，信息系统的安全性难以保证。

1.3 设备自身日志粒度粗，难以有效定位安全事件

在运维工作中，大多是通过各系统日志进行监控审计，但是由于各系统自身审计日志分散、内容深浅不一，且无法根据业务要求制定统一审计策略；因此，难以通过系统自身审计及时发现违规操作行为和追查取证。

1.4 第三方代维人员带来安全隐患

目前，越来越多的企业选择将非核心业务外包给第三方，在享受便利的同时，由于代维人员流动性大、对操作行为缺少监控带来的风险日益凸显。因此，需要通过严格的权限控制和操作行为审计，加强对代维人员的行为管理，从而达到消隐患、避风险的目的。

1.5 公有云提供的审计能力无法满足运维审计和管理的要求

- **公有云的审计功能一般侧重在排错场景下**

客户将业务系统放在公有云提供的 IaaS、PaaS 之上后，传统基于网络、系统的一些排查问题的方法不一定适合，所以这种情况下就要求公有云提供足够多的错误记录功能，从而能够利用这些功能知道系统的故障点。

- **无法审计运维加密协议、远程桌面内容**

为了加强信息系统风险管理，一些企业已经采用公有云的审计服务，希望达到对运维人员操作行为监控的目的。由于技术实现方式和系统架构，只能审计一些常规的操作行为；无法对维护人员经常使用的 SSH、RDP 等加密协议、远程桌面等进行内容审计， 无法有效解决对运维人员操作行为的监管问题。

- **基于 IP 的审计，难以准确定位责任人**

难以将 IP 地址与具体人员身份准确关联，导致发生安全事故后，追查责任人成为新的难题。

1.6 面临法规遵从的压力

传统 IT 场景下，有《信息系统等级保护》、《商业银行信息科技风险管理指引》等国家标准、行业要求；同时，随着云计算的广泛应用，云上的租户安全也已经被逐步纳入到法规遵从的范围之内，以《信息安全技术 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求》为例，明确定义了云租户侧的等级保护对象也应作为单独的定级对象定级。

二. 解决之道

2.1 目标

绿盟堡垒机云服务（简称虚拟堡垒机或 vOSMS）提供一套先进的运维安全管控与审计解决方案，目标是帮助企业转变传统 IT 安全运维被动响应的模式，建立面向用户的集中、主动的运维安全管控模式，降低人为安全风险，满足合规要求，保障企业效益。

绿盟堡垒机云服务通过逻辑上将人与目标设备分离，建立“人->主账号（堡垒机用户账号）->授权->从账号（目标设备账号）->目标设备”的管理模式；在此模式下，通过基于唯一身份标识的集中账号与访问控制策略 ，与各虚拟机、安全设备、数据库服务器等无缝连接，实现集中精细化运维操作管控与审计。

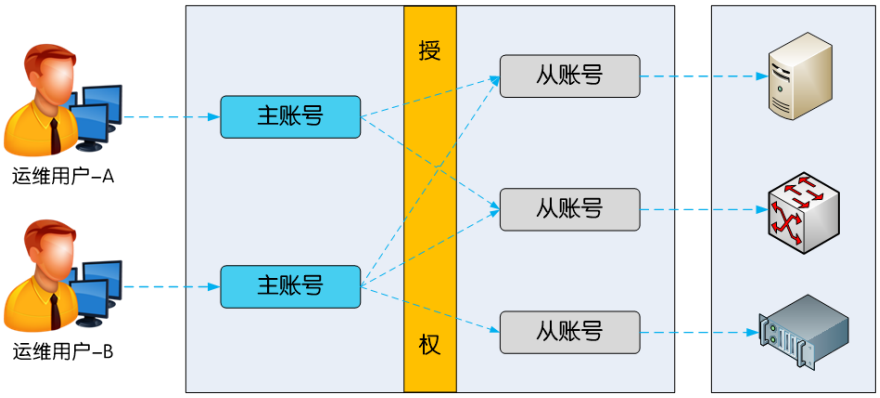

图 2.1 核心思路

2.2 应用场景

- 堡垒机云服务主要应用于以下场景：

IT 运维/共享帐号的责任认定；

第三方审计机构对运维的审计；

数据库敏感数据防范；

- 管理对象

用户对象：管理员、运维人员、第三方代维人员等。

设备对象：服务器(Windows/Linux/UNIX)、安全设备、数据库等。

- 管理范围

集中监控各种运维操作行为。

- 协议类型

SSH、Telnet、RDP、VNC、FTP、SFTP、HTTP、HTTPS、X11、KVM 等。

- 应用类型

各类数据库客户端、浏览器、专有客户端工具等。

- 部署方式

堡垒机采用“虚拟旁路，逻辑串联”的部署思路，主要通过两步实现：

1) 一般可以通过配置目标设备的安全组策略，只允许堡垒机的 IP 访问目标设备的运维、管理服务。

2) 将堡垒机部署在 VPC 中，运维人员从公网直接访问或 VPN 接入方式访问堡垒机。

- 达成效果

✓ 建立集中的运维操作监控平台，建立基于唯一身份标识的实名制管理，统一账号管理策略，实现跨平台管理，消灭管理孤岛。

✓ 通过集中访问控制与授权，实现单点登录(SSO)和细粒度的命令级访问授权。

✓ 基于用户的审计，审计到人，实现从登录到退出的全程操作行为审计，满足合规管理和审计要求。

下面分别从堡垒机的管理员和普通用户的角度，介绍实现流程与效果：

2.2.1 管理员制定运维管理策略

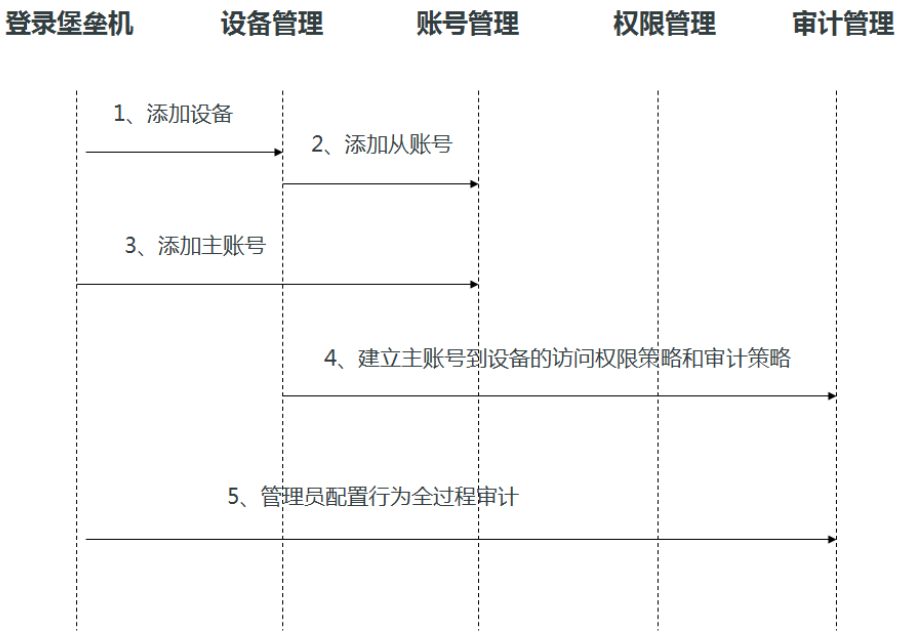

图 2.2 管理员制定策略

1. 添加设备（资源）

管理员添加需要管理的设备。设备包括虚拟机、安全设备、前置机、数据库服务器等维护对象，支持编辑相关设备信息包括设备类型、所属部门、设备名称、IP 地址、协议类型、应用程序等。

2. 添加从账号

管理员添加与设备对应的从账号（即设备的系统账号、数据库账号或 WEB 登录账号），包括账号名、口令等；其中口令可由堡垒机定期自动更新。

3. 添加主账号

管理员添加主账号（即普通用户账号）。主账号是登录堡垒机，获取目标设备访问权的唯一账号，与实际用户身份一一对应，每个用户一个主账号，每个主账号只属于一个用户。

4. 建立主账号到设备的访问控制与审计策略

基于访问权限策略，管理员建立基于“时间+主账号+目标设备+从账号+权限+审计”等要素的关联管理策略。

5. 管理员配置行为全程审计

堡垒机自动记录管理员的设备管理、账号管理和权限管理等所有行为日志，以便审计员监控。

2.2.2 普通用户访问目标设备

普通用户登录堡垒机后，可以实现下述功能：

- 可修改堡垒机登录密码；
- 可集中访问各类已授权设备；
- 用户点击设备名称，无须再次输入密码，即可实现对各种设备的登录。

具体实现流程如下：

图 2.3 普通用户访问目标设备

1. 登录请求

用户在终端通过 HTTPS 或第三方客户端工具登录堡垒机，输入主账号和口令，发起访问请求。

2. 登录认证

堡垒机的认证模块对用户的认证请求进行鉴别。

3. 检查主账号访问权限

认证成功之后，堡垒机的权限管理模块通过分析主账号属性（包括可访问的目标设备、访问权限、从账号、协议类型、应用程序等），确定主账号可访问的所有设备。

4. 显示可访问设备

直观地呈现出主账号可访问的所有目标设备。

5. 访问目标设备

用户选择需要访问的目标设备，进行操作维护。如果有违反访问控制策略的行为，堡垒机基于策略将自动记录、阻断及电邮通知管理员。

6. 返回访问结果

堡垒机将用户访问目标设备的所有操作执行结果，返回到用户终端。

7. 用户访问行为全程审计

堡垒机全程审计用户“登录堡垒机->目标设备访问操作->退出系统”的所有行为。

2.3 客户价值

绿盟堡垒机云服务为企业带来的价值主要体现在：

- 管理效益

所有运维账号在一个平台上进行管理，账号管理更加简单有序；

通过建立用户与账号的唯一对应关系，确保用户拥有的权限是完成任务所需的最小权限；

可视化运维行为监控，及时预警发现违规操作。

- 用户效益

运维人员只需记忆一个账号和口令，一次登录，便可实现对其所维护的多台设备的访问，提高工作效率，降低工作复杂度。

- 企业效益

降低人为安全风险，避免安全损失，满足合规要求，保障企业效益。

三. 系统介绍

3.1 系统功能

绿盟堡垒机云服务主要有三大功能：

- **集中账号管理**

建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略，实现与各虚拟机、安全设备、数据库服务器等无缝连接。

- **集中访问控制**

通过集中访问控制和细粒度的命令级授权策略，基于最小权限原则，实现集中有序的运维操作管理，让正确的人做正确的事。

- **集中安全审计**

基于唯一身份标识，通过对用户从登录到退出的全程操作行为进行审计，监控用户对目标设备的所有敏感操作，聚焦关键事件，实现对安全事件的实时发现与预警。

3.2 系统架构

绿盟堡垒机云服务由平台管理模块、功能管理模块和平台接口构成。总体架构如下图所示：

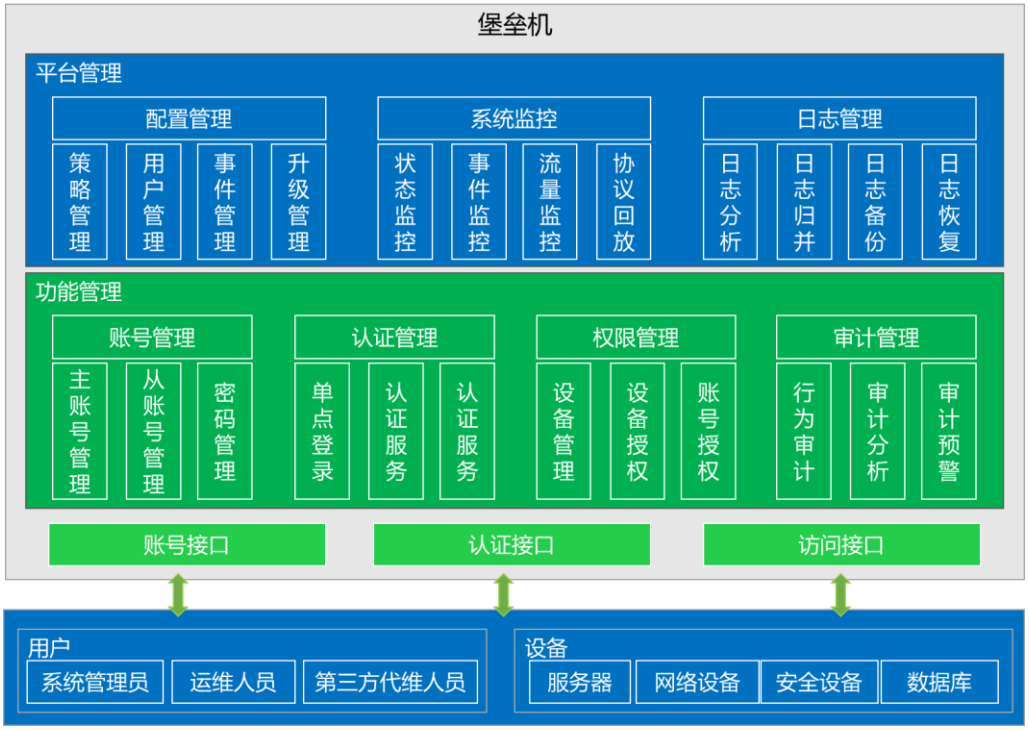

图 3.1 系统架构

1. 功能管理模块

提供账号管理功能、认证管理功能、权限管理功能和审计管理功能。

- 账号管理：提供账号生命周期管理，包括账号创建、账号修改、状态调整、账号删除、账号查询等功能。
- 认证管理：支持多种认证方式，包括本地认证、短信认证、LDAP/RADIUS 认证。
- 权限管理：提供基于时间、用户/用户组、设备/设备组、设备账号、命令关键字、危险级别等组合策略，授权用户可访问的目标设备及可使用的命令。
- 审计管理：提供对用户通过堡垒机对目标设备的所有操作行为审计、事件查询分析和报表管理。

2. 平台管理

提供对堡垒机平台自身的管理，包括系统配置管理、系统监控及审计日志管理。

3. 平台接口

提供对用户（包括管理员、运维人员、代维人员等）、设备(包括虚拟机、安全设备、数据库服务器等)的各种管理接口，包括设备导入接口、账号的同步和导入接口、认证接口、访问接口等。

四. 产品特性

4.1 多维度、细粒度的认证与授权体系

- 灵活的认证方式

绿盟堡垒机云服务对主账号的认证，支持本地认证、短信认证、LDAP 认证、RADIUS 认证、USBkey 认证等多种方式，能够根据用户实际需求，设置混合认证方式，即不同主账号采取不同的认证方式，实现按需设置认证方式。

- 多维度、细粒度的访问控制

绿盟堡垒机云服务支持基于角色的访问控制（RBAC ,Role-Based Access Control）。管理员可按照时间、部门、职责和安全策略等维度，设置细粒度权限策略，让正确的人做正确的事，简化授权管理。

通过集中统一的访问控制和细粒度的命令级授权策略，确保用户拥有的权限是完成任务所需的最小权限。系统支持创建基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、危险级别（分为高、中、低）等元素的组合条件，授权用户可访问的目标设备、定义高危操作监控策略。当用户越权执行特定命令的时候，实时进行告警、阻断，确保信息系统安全运行。

- 金库（双认证）模式授权

绿盟堡垒机支持金库（即双认证）模式，运维人员登录关键服务器或执行高危命令时，须有两人均认证通过方可执行，最大化地降低运维风险。

✓ 登录双认证授权

运维人员试图登录重要、关键服务器进行运维时，首选输入正确的认证口令来发起登录请求，管理员收到登录请求后，如果同意此次登录请求，则同样需要输入正确的认证口令，运维人员方可成功登录服务器。

✓ 高危命令双认证授权

运维人员在运维过程中，试图执行一些高危命令（如关闭服务器、重启服务器等命令）时，同样需要额外的授权。针对不同的角色，可设置允许、授权、警告或拒绝其执行高危命

令，即允许其执行、管理员专门授权后方可执行、警告过后方可执行、拒绝执行，以加强、细化对高危命令的管控。

4.2 一站式管理

绿盟堡垒机云服务界面展示方式丰富而多样，智能关联相关信息，充分体现了人性化用户界面设计的原则和思路。

- 门户式管理

绿盟堡垒机智能关联设备、主账号、访问控制策略和审计信息。

在【首页-访问设备】中以设备为基准，可直接查询、编辑与该设备相关的访问控制策略，查询有权限访问该设备的主账号以及该设备的审计信息。

图 4.1 设备关联信息查询

在【首页-主帐号】中以主账号为基准，直接查询、编辑与该主账号相关的访问控制策略，查询该主账号有权访问的设备以及该主账号的审计信息。

图 4.2 主帐号关联查询

门户式管理极大地简化了管理员对设备、主帐号、策略等的维护操作，优化管理员体验、提高管理员工作效率。

- 灵活的设备分组展示

绿盟堡垒机云服务支持按照部门、设备类型、业务类型等不同的分组方式展示目标设备；不同的用户完全可以根据管理要求及使用习惯，选择不同的展示方式。

4.3 自身安全性保障

- 绿盟堡垒机云服务采用专门设计的安全、可靠、高效的系统平台。定制的系统内核大大提升处理能力；
- 操作系统经过优化和安全性处理，保证系统的安全性；
- 绿盟堡垒机云服务支持 HA 模式，具有更强的高可用性；
- 绿盟堡垒机云服务采用强加密的 SSL 传输控制命令，避免可能存在的嗅探行为，确保数据传输安全。

4.4 跨平台无缝管理

绿盟堡垒机云服务具有跨平台的运维行为管控能力，可覆盖多种主流主机操作系统、数据库和运维协议。

- 协议类型：SSH、RDP、VNC、SFTP、Telnet、FTP、HTTP、HTTPS、X11 等；
- 数据库类型：Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、PostgreSQL 等；
- 操作系统类型：FreeBSD、Solaris、RedHat Linux、Windows 等；

4.5 强大的应用扩展能力

绿盟堡垒机云服务能够审计基于 Windows 平台下所有应用程序的运维操作。基于在 VPC 中部署前置机的架构，当需要支持一款新的专有运维客户端程序时，只需管理员在前置机上安装、发布该客户端程序，而无须任何定制开发，堡垒机即可对通过该应用程序的运维操作进行审计。用户的投入产出比实现最大化，在零附加成本的基础之上，轻松支持所有通用及专有的运维客户端程序。

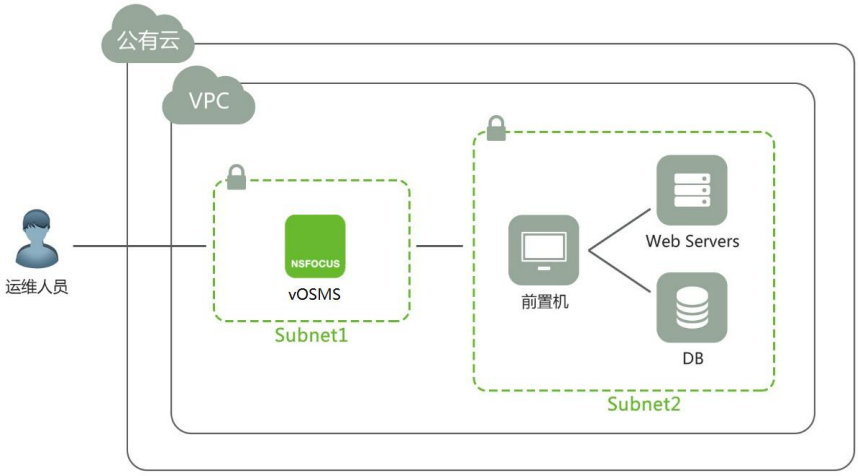

图 4.3 前置机架构示意图

运维设备时，运维人员只需登录堡垒机、选择目标设备以及应用程序，堡垒机将根据管理员事先配置好的参数自动启动前置机上相应的应用程序，并连接目标设备，前置机对运维人员完全透明。

4.6 灵活多样的登录方式

绿盟堡垒机支持以多种方式登录堡垒机及目标设备，灵活适应各种需求下的使用场景。

- 登录堡垒机

绿盟堡垒机云服务支持运维人员通过浏览器或第三方客户端工具登录堡垒机，最大程度上保证运维人员的操作习惯不被改变。第三方客户端工具支持 RDP、Telnet、SSH、SFTP、VNC、HTTP/HTTPS 等协议的客户端工具软件，如 SecurCRT、Mstsc 等。

- 登录目标设备

绿盟堡垒机云服务支持运维人员以三种方式登录需要运维的目标设备：

✓ **自动登录**：管理员事先将设备账号及其密码保存在堡垒机，运维人员登录堡垒机并经过认证授权后就可以直接访问目标设备，无须再次手工输入设备账号和密码信息，无须记忆多个设备账号和密码，实现真正意义上的单点登录（SSO），提高运维人员工作效率、改善用户体验；

✓ **半自动登录**：运维人员首次登录目标设备，输入账号和密码信息时，选择“记忆登录信息”，在后续登录该目标设备时，就无须再输入账号和密码信息，在降低由于管理员集中管理、维护设备帐号而带来的安全风险的同时，极大简化运维人员的登录操作，在安全性与便利性之间达到最优平衡点；

- ✓ **手动登录**：设备帐号及密码信息只由相关的运维人员掌握，无需管理员参与。运维人员通过堡垒机访问目标设备时，每次都手工输入设备账号和密码，认证成功后方可登录设备，设备帐号及密码信息的安全性得到最大保障。
- ✓ **密钥登录**：用户可以上传自己的私钥文件，在登录目标设备时，堡垒机将该私钥和同行短语发送到目标服务器上进行认证，如果认证成功，则用户可以进行运维。客户可以保持运维习惯不改变，通过私钥认证的形式也保证了登录安全。

4.7 基于唯一身份标识的审计

绿盟堡垒机云服务主账号是获取目标设备访问权利的唯一账号，通过本地认证、短信认证、LDAP 认证、RADIUS 认证、USBkey 认证等多种认证方式，将主帐号与实际用户身份一一对应，确保不同设备、系统间行为审计的一致性，从而准确定为事故责任人，弥补传统网络安全审计产品无法准确定位用户身份的缺陷。

4.8 工单系统

对运维人员的授权可通过工单系统完成审批，运维人员需要审批前可提前创建工单，审批人员可极大自由度完成授权审批，解决了审批人必须时刻守在电脑前，时刻与运维人员一起等待审批请求的问题。工单系统既提高运维人员的运维效率，同时也解放审批人员，不再担心出差或请假不在电脑前无法审批导致无法运维的情况。

4.9 全程运维行为审计

绿盟堡垒机云服务可完整审计运维人员通过账号“在什么时间登录什么设备、做什么操作、返回什么结果、什么时间登出”等行为，全面记录“运维人员从登录到退出”的整个过程，帮助管理人员及时发现权限滥用、违规操作，准确定位身份，以便追查取证。

- 字符会话审计

系统支持审计通过 SSH、Telnet 等协议的操作行为，审计内容包括访问起始和终止时间、用户名、用户 IP、设备名称、设备 IP、协议类型、危险等级、操作命令等。可提供操作内容倍速回放、定位播放等功能。

- 图形操作审计

系统支持审计通过 RDP、VNC 等远程桌面以及 HTTP/HTTPS 协议的图形操作行为，审计内容包括访问起始和终止时间、用户名、用户 IP、设备名称、设备 IP、协议类型、危险等级、操作内容等。支持通过视频录像方式记录操作内容，可提供倍速回放、定位播放等功能。

- 数据库运维审计

系统支持审计 Oracle、MS SQL Server、IBM DB2、PostgreSQL 等各主流数据库的操作行为。支持通过视频录像方式记录操作内容，可提供倍速回放、进度拖拉等功能。

- 文件传输审计

系统支持审计通过 SFTP、FTP 等协议的操作行为，审计内容包括访问起始和终止时间、用户名、用户 IP、设备名称、目标设备 IP、协议类型、文件名称、危险等级、操作命令等。可提供操作内容倍速回放功能。

- 合规审计

对上述各类运维审计日志，审计员能够单独或批量进行合规审计，方便地审核每一次运维行为及操作是否符合规章制度的要求，并填写具体的审核批注，最后统一输出合规审计结果。

4.10 审计信息“零管理”

绿盟堡垒机云服务支持“日志零管理”技术

- 日志自动维护：根据日志自动维护计划的设置，系统在指定时间自动进行相应的日志数据备份。
- 日志查询：系统提供多种审计日志查询条件，包括时间、IP 地址、用户名、设备名、关键字、危险等级（高、中、低）等；
- 审计报表：系统提供详细的多种类别的报表模板，可提供基于操作时长、高危操作、阻断操作等类别的用户操作 TOP10。系统支持生成：日、周、月、年度综合报表，报表支持 Word、Excel 等格式导出，降低维护费用与管理员的工作强度。
- 自动报表：客户需要周期（比如每周、每月）进行运维审计，同时审计报表的范围都一致。此时客户可以自定义时间点和报表模板，堡垒机就可以周期生成统计报表，自动发送到客户邮箱中。

4.11 配置向导功能

提供对堡垒机管理配置向导、设备管理员策略配置向导、数据库运维配置向导；通过将配置操作分解成逻辑性更强的操作，在多个页面上进行向导，达到引导用户完成复杂配置的目的，极大提高产品易用性。

4.12 部署简单方便

绿盟堡垒机云服务采用“虚拟旁路，逻辑串联”的模式，不改变网络拓扑结构，不需要在终端安装客户端软件，不改变管理员、运维人员的操作习惯，不影响正常业务运行。

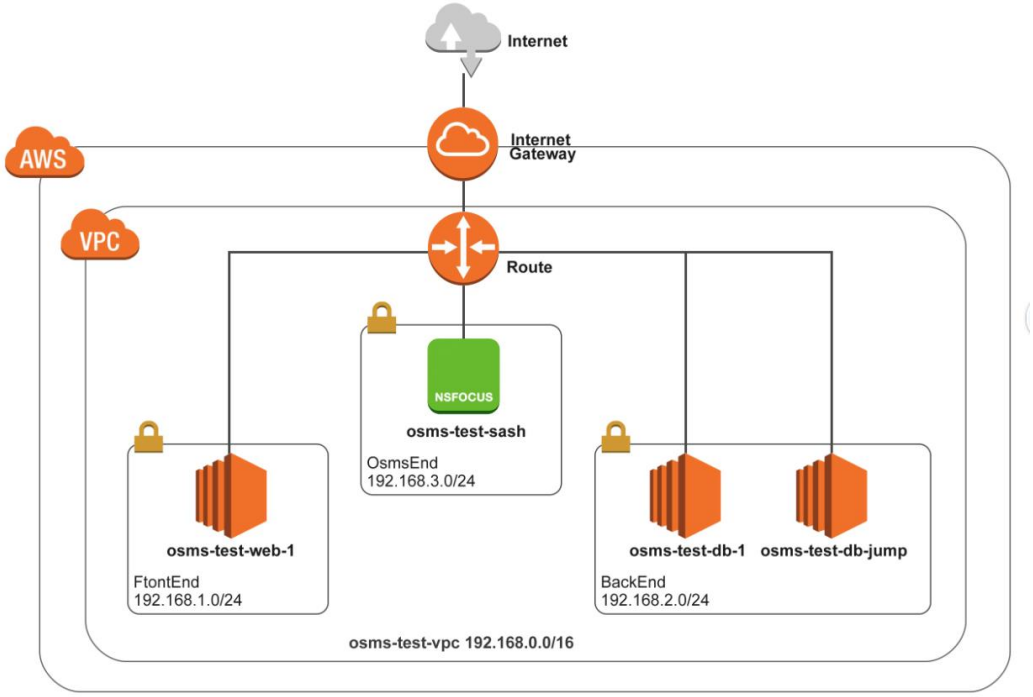

图 4.4 AWS 上的部署示例

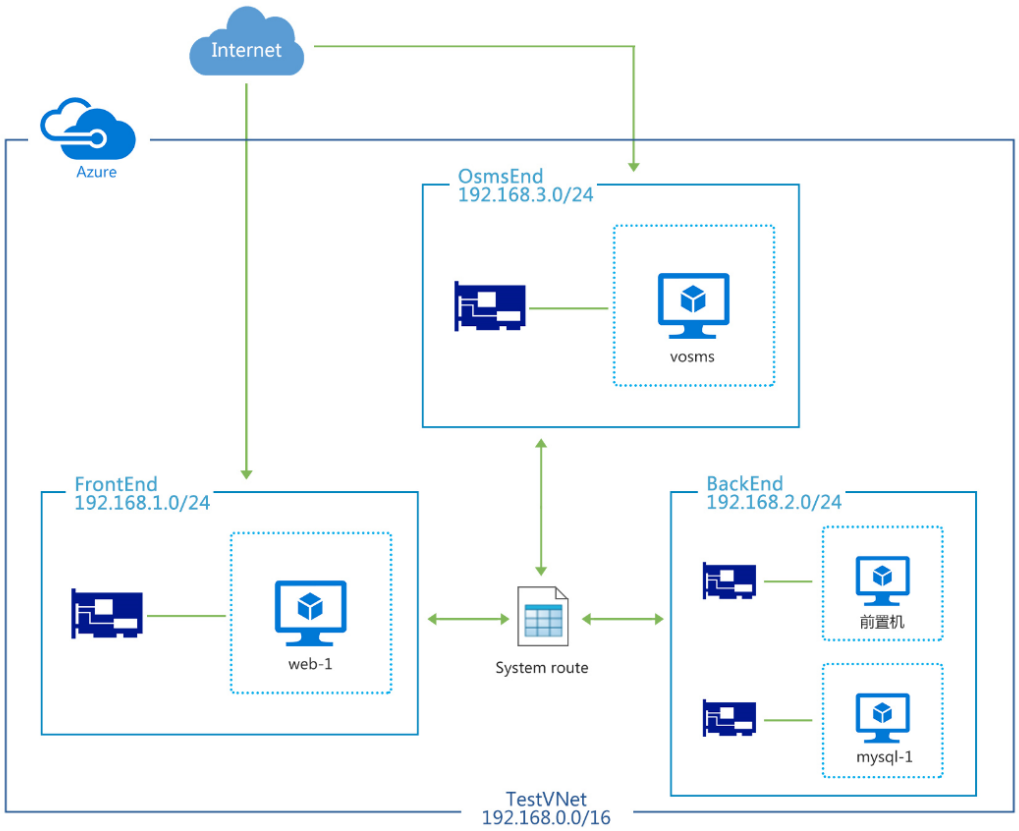

图 4.5 Azure 上的部署示例

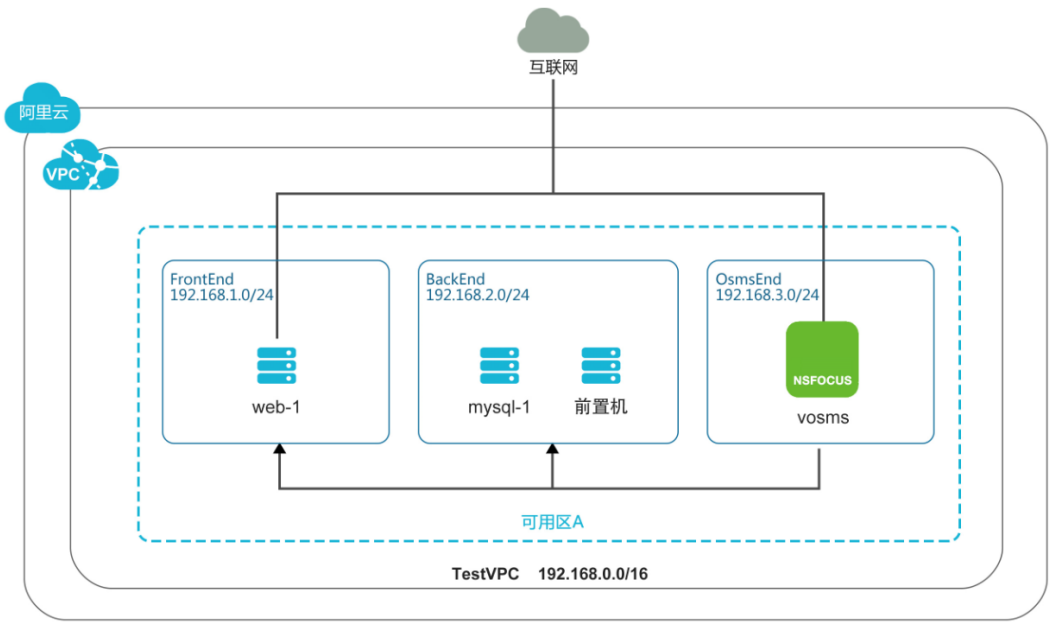

图 4.6 阿里云上的部署示例

五. 服务规格

5.1 服务规格

服务名称		绿盟堡垒机云服务（基础级）			
服务规格		标准版（30 资产）	标准版（50 资产）	标准版（100 资产）	标准版（200 资产）
功能	账号管理	√	√	√	√
	集中认证	√	√	√	√
	授权管理	√	√	√	√
	运维审计	√	√	√	√
	设备管理	√	√	√	√
	角色管理	√	√	√	√
	密码管理	√	√	√	√
	工单系统	√	√	√	√
性能	最大可管理资产数	30	50	100	200
基础服务	远程技术支持服务	√	√	√	√
	产品系统升级服务	√	√	√	√
	产品规则升级服务	√	√	√	√
专家服务	上门产品安装与培训服务	——	——	——	——
	上门技术支持服务	——	——	——	——

注：使用绿盟云短信网关，各规格默认包含 500 条/月短信。

想要了解更多规格，请与我们联系。

服务名称		绿盟堡垒机云服务（专家级）			
服务规格		增强版（30 资产）	增强版（50 资产）	增强版（100 资产）	增强版（200 资产）
功能	账号管理	√	√	√	√
	集中认证	√	√	√	√
	授权管理	√	√	√	√
	运维审计	√	√	√	√
	设备管理	√	√	√	√
	角色管理	√	√	√	√
	密码管理	√	√	√	√
	工单系统	√	√	√	√
性能	最大可管理资产数	30	50	100	200
基础服务	远程技术支持服务	√	√	√	√
	产品系统升级服务	√	√	√	√
	产品规则升级服务	√	√	√	√
专家服务	上门产品安装与培训服务	1 次	1 次	1 次	1 次
	上门技术支持服务	1 次	1 次	1 次	1 次

注：使用绿盟云短信网关，各规格默认包含 500 条/月短信。

想要了解更多规格，请与我们联系。

5.2 AWS 中使用的建议虚拟机规格

服务名称	服务规格	建议规格
绿盟堡垒机云服务（基础级）	标准版（30 资产）	推荐 1：t2.medium vCPU：2；内存：4G；实例存储：100GB 推荐 2：c4.large vCPU：2；内存：3.75G；实例存储：100GB
	标准版（50 资产）	
	标准版（100 资产）	
	标准版（200 资产）	

绿盟堡垒机云服务（专家级）	增强版（30 资产）	推荐 1：t2.medium vCPU：2；内存：4G；实例存储：100GB 推荐 2：c4.large vCPU：2；内存：3.75G；实例存储：100GB
	增强版（50 资产）	
	增强版（100 资产）	
	增强版（200 资产）	

5.3 Azure 中使用的建议虚拟机规格

服务名称	服务规格	建议规格
绿盟堡垒机云服务（基础级）	标准版（30 资产）	推荐 1：Stranard_A2_V2 vCPU：2；内存：4G；实例存储：100GB 推荐 2：Stranard_A2 vCPU：2；内存：3.5G；实例存储：100GB
	标准版（50 资产）	
	标准版（100 资产）	
	标准版（200 资产）	
绿盟堡垒机云服务（专家级）	增强版（30 资产）	推荐 1：Stranard_A2_V2 vCPU：2；内存：4G；实例存储：100GB 推荐 2：Stranard_A2 vCPU：2；内存：3.5G；实例存储：100GB
	增强版（50 资产）	
	增强版（100 资产）	
	增强版（200 资产）	

5.4 阿里云中使用的建议虚拟机规格

服务名称	服务规格	建议规格
绿盟堡垒机云服务（基础级）	标准版（30 资产）	推荐 1：ecs.s2.large vCPU：2；内存：4G；实例存储：100GB 推荐 2：ecs.sn1.medium vCPU：2；内存：4G；实例存储：100GB
	标准版（50 资产）	
	标准版（100 资产）	
	标准版（200 资产）	
绿盟堡垒机云服务（专家级）	增强版（30 资产）	推荐 1：ecs.s2.large vCPU：2；内存：4G；实例存储：100GB 推荐 2：ecs.sn1.medium vCPU：2；内存：4G；实例存储：100GB
	增强版（50 资产）	
	增强版（100 资产）	
	增强版（200 资产）	