海颐安全
HAIYI SECURITY

海颐特权账号安全管理系统

云解决方案白皮书

为您的云安全保驾护航

海颐特权账号安全管理系统-云解决方案白皮书
广州海颐信息安全技术有限公司
support@haiyisec.com

文 档 版 本

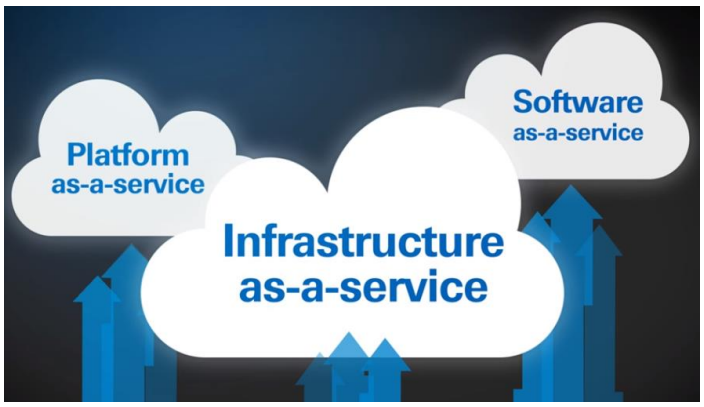
版本编号	日期	修订人	更新章节	简要说明
V1.0	2017.08.29	杨达盛	无	创建初稿，格式修订

目 录

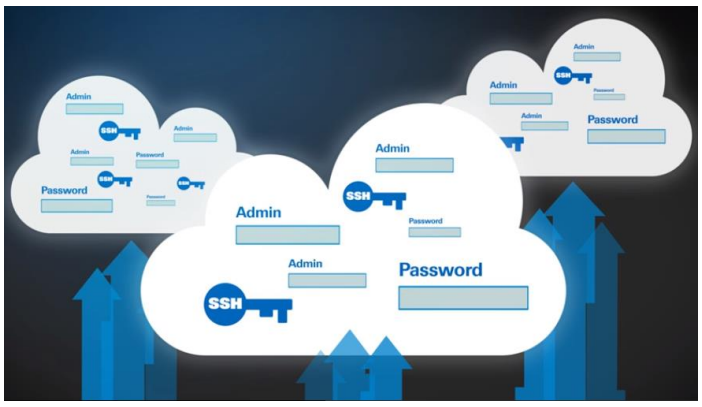
云安全的挑战

云计算的特权凭证问题

云计算带来的技术红利，让云成为当前不可逆的潮流之一。拥抱云计算是众多企业为了降低成本、提高 IT 效率、加快业务上线运行的有效途径。

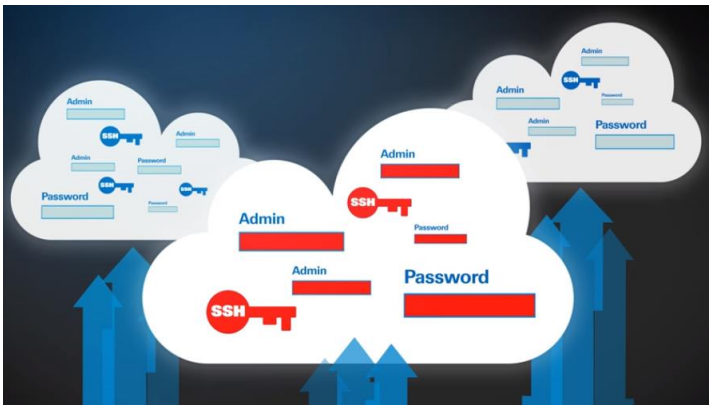


然而，随着越来越多的企业把业务部署在云端，云端的特权账号安全管理问题也越来越受到重视。而在云端的特权凭证管理不妥，可以为攻击者带来更大的便利。



在云环境里，一般会有数量庞大的实例和服务运行着。而他们的特权凭证的产生/发放/配置工作，全部都可以由一个能力强大的控制台管理账号来执行。

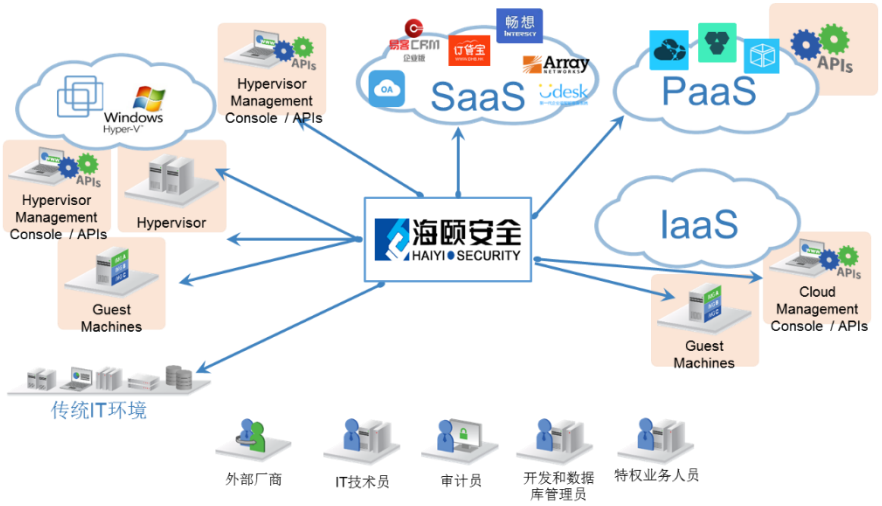
在云上，一般会由自动化编排工具、手工操作图形化控制台、或含云 API 的运维脚本来执行生成创建若干实例。而这些操作的前提，正是前面所提及的控制台管理账号。



另一方面，当云上的众多底层实例或云端管理控制台在运行与操作期间，他们上面也可能随时被随意创建本地特权凭证。这些特权凭证可能是真正需要的账号，可能是测试账号，也可能是攻击者特意留下的跳板账号。时间越久，其越容易变成幽灵账号。而人手运维查找，已经变得不太现实。唯有依靠有效的管理制度和技术，才能可以保证提高云端特权凭证管理的高覆盖率。

HaiyiPAS 为云特权凭证保驾护航

现在，只需部署一套**海颐安全特权账号安全管理平台**（下面简称“**HaiyiPAS**”），即可同时管理企业 IT 环境下的所有特权凭证，无论它们是本地机房、本地虚拟化、本地私有云，还是公有云和混合云。



而同时，HaiyiPAS 自身提供丰富的 API/SDK，甚至第三方平台兼容的 HaiyiPAS 插件，都可以无缝内嵌至用户的云管工具及自动化工具之中。例如 TerraForm、Ansible 和 Puppet 等等。

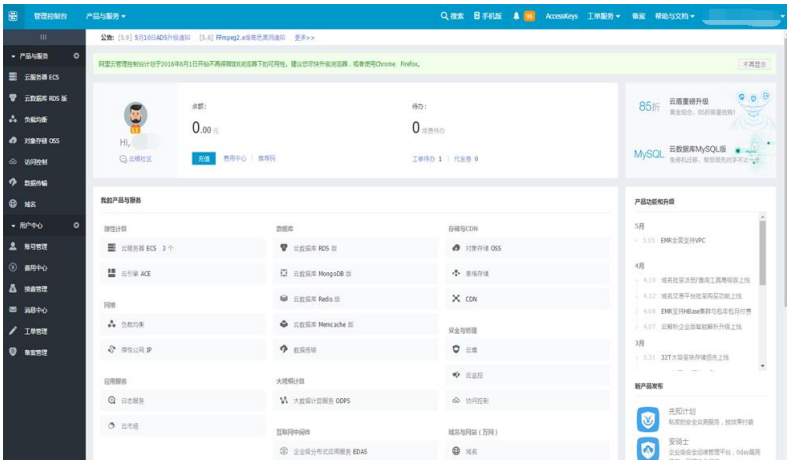
当进行云端业务操作和自动化运维时，所需要的特权凭证，以及所被产生的特权凭证，均可以与 HaiyiPAS 进行无缝协作，保证在不暴露凭证的同时，依然满足自动化运维的需求。

云中账号管理问题

云中的账号都在哪里

传统 IT 环境中，我们都“非常清楚”自己的环境有哪些特权账号和凭证。而当拥抱云计算技术后，特权凭证的数量和管理边界，变得庞大和模糊了。

众多云平台都拥有图形化管理控制台（常称“WebConsole”）。而 IT 管理员一般可以都通过该 WebConsole 进行云资产的配置管理。下图是国内阿里云的 WebConsole 样例：

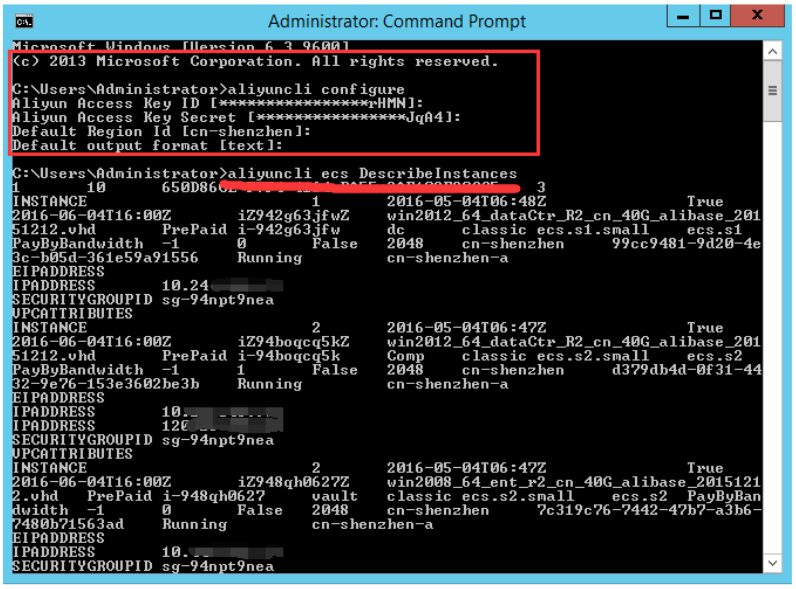


与之对应的，每个云控制台的账号，都可以使用云平台开放出来的 API/SDK。而调用 API/SDK 时所用的凭证，通常称为 AccessKeyID/AccessKeySecret，由云平台成对产生和发放下载。

下图，是阿里云新建控制台子账号时，按需创建的对应的 AccessKeyID 和 AccessKeySecret 样例：

获得 AccessKeyID/AccessKeySecret 后，只要权限策略允许，即可调用阿里云

API/SDK 实现图形化控制台相同的功能。一般可以被内嵌至运维脚本、自动化工具等里面。下面，是阿里云 CLI Tools 的运行样例：



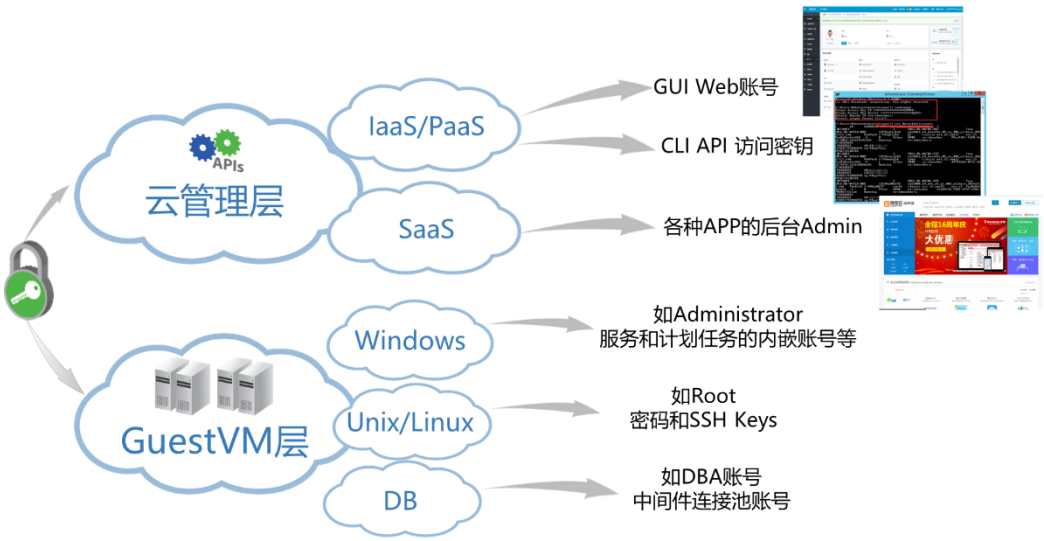
云计算的红利远不止“计算”，还有“高效”和“便利”。目前，众多大型云平台，都提供云市场服务（或称“软件市场”），用户只需在云市场中，一键购买下单，即可自动或半自动地，获得并运行众多商业/开源软件系统。下图，为各大云平台的云市场样例：

阿里云

腾讯云

亚马逊

而这里，“一键购买”的便利性，让企业的云端特权凭证管理变得更加不可预知。管理者无法预知以后会有什么样的应用的特权账号需要被纳管，所以就要求传统的管理方案具备灵活插件开发能力，适配 SaaS 服务中的各种新型应用特权账号。例如，云市场中购买的 HR 系统/VPN 系统/ERP 系统等等，其后台系统的 admin/root 也属于企业的特权凭证之一。



以上，都需要企业 IT 管理部门拥有一套完善、灵活的特权凭证管理平台来实现全面管理。

同时，从成本环节考虑，企业本地已有的特权凭证管理系统如果无法有效、无缝地实现本地/云端账号统一管理的话，也会为企业带来不必要的额外的管理成本、技术成本和财务成本。毕竟，没有企业会主观地愿意购买多套平台，适配本地机房和云端环境，而且还得考虑企业特权账号管理策略的可延续性。这些无疑都是一堆棘手的问题。

云中的账号有何特别

传统方案难以被融合

首先，云中特权账号会被企业的自动化运维工具、运维脚本、甚至应用所内嵌。换句话说，使用云端特权凭证的身份，不再只是自然人，工具/脚本/应用也是身份，也需要使用这些云端特权凭证。

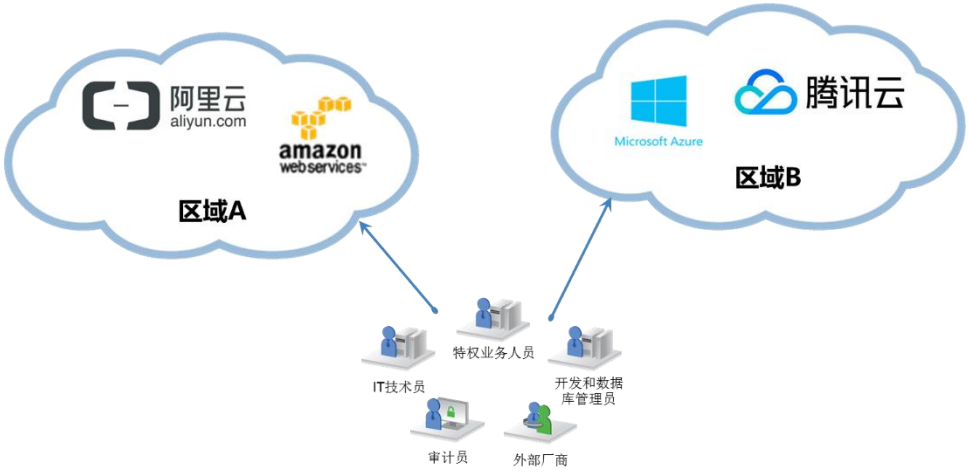
当企业需要利用传统运维管理方案，去管理这些云中特权账号时，会显得尤为尴尬。例如，运维脚本或自动化工具中，经常会碰见如下截图的引用，其引用 AccessKeyID 和 KeySecret，然后连接云端，实现后续的管理运维逻辑：

```
$AccessKeyID = “A2T4cfB35gL9gb”
$AccessKeySecret = “s5X02y5locJVd234FRxPjpl”
aliyuncli configure set --AccessKeyId $AccessKeyId /
--AccessKeySecret $AccessKeySecret
```

假如，我们轮换了这些云端凭证后，但传统方案并没有提供相关 API/SDK 让已有的运维脚本、自动化运维工具去调取的他们话，企业的已有自动化运维流程将被割裂。或者传统的管理方案只能放弃这些云端凭证的部分，不去管理。这不是企业管理者希望的。

多云让 IT 边界无限延伸

较大型的企业，经常会采用多家虚拟化或云平台技术，并且部署在全国/全球的不同区域节点处。然后，由总部统一管理或分部下放管理等。
这样大规模分布式的架构，就要求我们的特权账号管理平台，必须具备灵活的分布式部署结构，来跟随企业的 IT 环境进行纵向或横向扩展。



云特权凭证使用的审计难题

正如前文一直强调的，云管理控制台的高权限账号、AccessKeyID/KeySecret 都具备超高权限和超广覆盖范围的能力，它们的整个使用过程极其容易被造成滥用。**这里，容易发生特权凭证滥用的，除了自然人之外，还有我们的自动化工具、运维脚本甚至业务应用。这些凭证的滥用，往往是因为传统方案情况下的审计缺失。**
例如之前提供过的一个调用 AccessKeyID/KeySecret 的脚本截选：

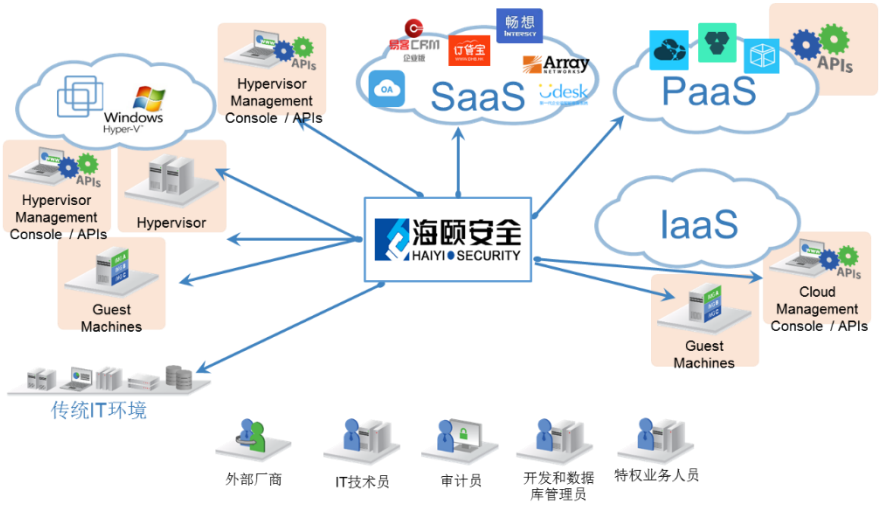
```
$AccessKeyID = “A2T4cfB35gL9gb”
$AccessKeySecret = “s5X02y5IocJVd234FRxPjpl”
aliyuncli configure set --AccessKeyId $AccessKeyId /
--AccessKeySecret $AccessKeySecret
```

运维工程师拿到该特权凭证，完全可以放在其他脚本、工具、业务环境中执行，甚至是恶意行为。这类型问题，在讲究“一键式”、“傻瓜式”高效操作的云运维环境中，是经常出现的。毕竟，云的一大特点就是高度自动化。

所以，当管理者希望查看该 AccessKey 的使用记录和使用地方时，就不得不依赖云平台自身有的审计功能，但并不一定所有云平台（或者特权凭证产生平台）都具备非常完善的审计记录机制。

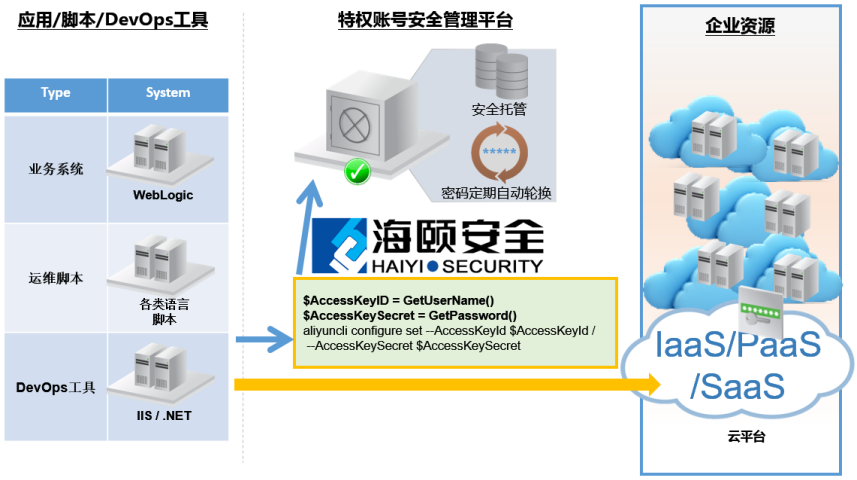
云中的账号要怎样管

您需要只用一套平台，即可管理本地与多云环境



您需要所有云端特权凭证的使用与发放，均被审计录像

您需要所有云端特权凭证在不被暴露的情况下嵌入自动化运维



您需要平台具备灵活插件开发性来适配多变的 SaaS 应用账号

HaiyiPAS 平台方案架构

核心与功能组件简介

密码保险库（Vault）-- 安全存取密码的保险库

这是一个为企业特权账号密码提供安全的集中存储、保护和管理访问的仓库。

Vault 构建于坚固的加密技术，提供多层次的安全机制，保证最高的安全要求。Vault 的部署可以为 HA，其也具备同城/异地/多级的灾备 DR Vault 部署能力。

集中策略管理器（CPM）-- 高效灵活可定制的改密能手

Central Policy Manager，简称“CPM”，可以为多种目标系统的特权账号密码提供密码更新、验证以及重置等功能。

CPM 可以改密的目标包括各种路由器、数据库、服务器、目录服务和内嵌于应用程序/脚本/配置文件/自动化工具中的密码。目标包括但不局限于 Z/OS、OS390、AS400、Windows Server、AIX、HP-UX、Solaris、SuSE Linux、Redhat Linux、Unix、SQL Server、Oracle、Sybase ASE、Sybase IQ、DB2、Informix、MySQL、AWS、MS Azure、Alicloud、HUAWEI FusionManager、RedHat Virtualization、Vmware、Cisco、Juniper、HUAWEI 等等。
利用 CPM 强大的定制开发的能力，我们以及用户有一定动手能力的工程师，都可以开发出更多改密对象插件包，然后简单导入和修改配置，即可让企业的特殊系统/新系统的特权凭证也能被纳入管理之中。
所以，CPM 的改密支持列表是无限扩展的，毕竟企业的业务系统总是日新月异。

密码保险库 Web 门户（PVWA） – 简介易用的 WebUI 界面

Password Vault Web Access，简称“PVWA”，基于 Web 的操作界面。

利用 PVWA，可以允许 IT 人员能够快速地使用/获取目标系统的特权账号密码。审计员利用该 Web 门户，更可随时查看导出特权凭证的相关使用记录、视频等信息。
HaiyiPAS 平台管理员，更可利用本 Web 门户，配置修改各种密码管理策略。

特权会话管理器（PSM） – 实现特权凭证 SSO 会话隔离审计

Privileged Session Manager，简称“PSM”。当我们在 Web 门户上点击使用某个特权凭证之后，实际上，用户正通过 PSM 进行 SSO 单点登录连接至目标系统。同时，其所有操作过程均被 PSM 录像审计。这就是我们强调的特权会话审计记录。

例如，当我们点击连接某个云平台 WebConsole 密码后，我们将被重定向至连接 PSM，然后 PSM 会为我们实现 SSO 单点登陆到该 WebConsole。用户本地无法接触密码，也无需安装对应 BS/CS 工具。
假如，企业有自开发的 CRM 系统，有专用的客户端，那么我们也能利用 PSM 为其定制发布该专用客户端。CRM 系统的 Admin 账号被 HaiyiPAS 平台托管后，用户无法知道密码，也无需安装客户端，但依然能通过 Web 门户和 PSM 实现连接效果。
这里，如果配套前面的改密能手 CPM，实现定期改密（如 60 天周期或一次一密）的话，则 WebConsole 平台、CRM 系统的特权凭证安全系数将会大大提高。

应用身份管理（AIM） – 解决内嵌账号的安全问题

Application Identity Management，简称“AIM”方案。其目的是为了解决在应用程序代码、配置文件、脚本、自动化工具中的密码存储、审计和管理难题。

当所有密码均集中和安全地存放在 HaiyiPAS 的密码保险库 Vault 中时，企业的应用程序、配置文件、脚本、自动化工具等通过 AIM 的 API/SDK 向 Vault 获取密码后，依然能正常高效运行，而且已经无需暴露明文内嵌的硬编码—即密码。利用这种独特的技术，企业能够轻松符合内审和外审的合规性要求。
在技术上，企业可以轻松地做到密码定期更换，而无需对业务系统/自动化运维

流程进行排查修改。

并且，通过我们的 API/SDK 向 Vault 获取密码的话，通通被记录审计在案。而在一些高规格场景下，甚至可以对密码提取申请者——我们的应用/脚本/自动化工具进行身份指纹验证，如代码哈希、路径审核、OS 执行用户、源 IP 等组合，验证通过了才发放密码。

AIM 方案有缓存级和轻量级两种选择：

- *缓存级 - 在需要获取密码的操作系统上，部署 AIM 代理，Credential Provider，简称“CP”。通过代理 CP，即可调用向 Vault 获取密码的各种 SDK，如 Java、C、.Net、COM、CLI 等等各类语言。同时，CP 还会在本地划分多级加密缓存，使得哪怕 CP 与密码保险库 Vault 失去网络通讯，也依然能从本地多级加密缓存里拿出密码提供给应用、脚本和自动化工具。*
- *轻量级 – 顾名思义，即无代理形式。利用 AIM 的另一组件，Central CP，简称“CCP”，即可并对外发布 Https Restful/SoapWebService 的取密接口。只要在我们的应用、脚本、自动化工具上按规范调用这些取密接口即可。在通过了应用身份验证（轻量级别的指纹验证）后，即可安全返回密码。*

其余组件

HaiyiPAS 功能组件家族庞大，但又高度松耦合，可以根据需要和预算，灵活按需部署。分别是：

PSMP— 特权会话 SSH 代理器

SKM—SSHKey 管理器

OPM—按需特权管理器

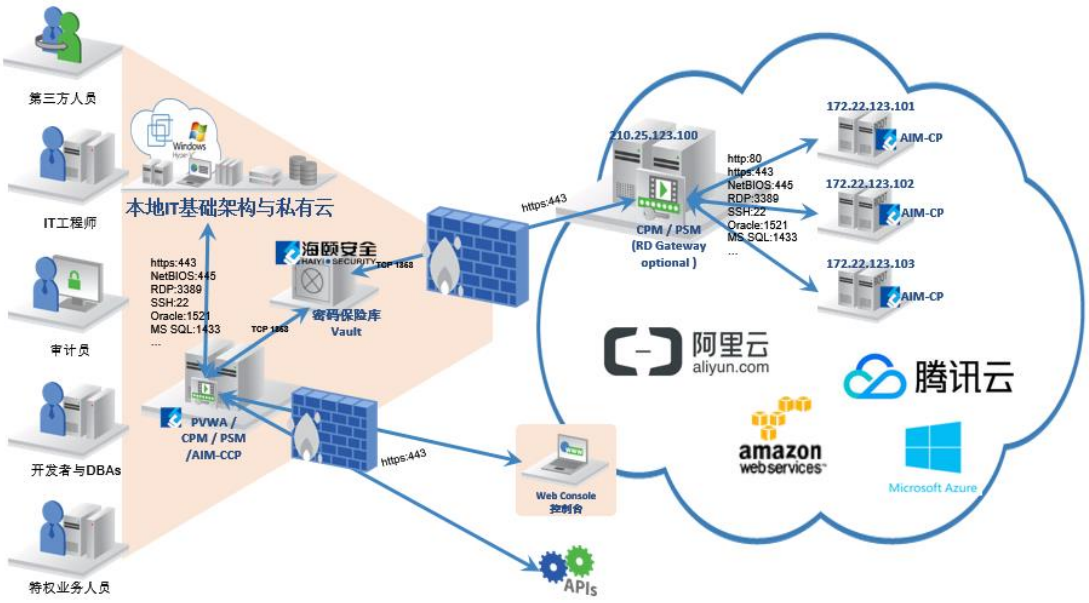
DDM—动态数据脱敏器

PTA—特权威胁分析等等

在本文则不一一介绍。如希望进一步了解，请咨询我们技术团队。

灵活的云部署架构

一套平台打通本地与云端示例



本地机房部分：

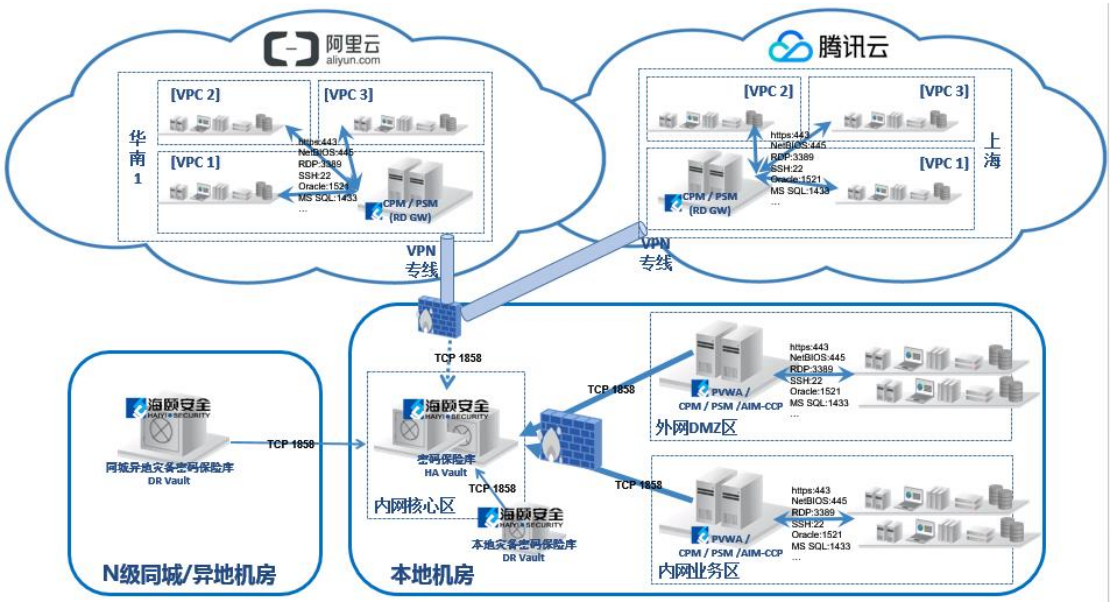
部署重要的密码保险库 Vault（并且考虑 HA、灾备等模式）

部署若干 Web 门户 PVWA、改密组件 CPM、会话管理组件 PSM，负责本地特权凭证对象的管理。

云端部分：

只需部署若干改密组件 CPM、会话管理组件 PSM，即可负责云端的特权凭证对象的管理和连接。

多云架构基本部署示例



密码保险库 Vault 部分：

密码保险库 Vault 是整套 HaiyiPAS 的核心。如有本地机房，建议部署在本地机房，并配套 HA Vault 或者 DR Vault 等高可用模式。（当然，Vault 也可以部署在云端）

功能组件 CPM/PVWA/PSM 部分：

无论是本地托管对象，还是云端的托管对象，只要在对应位置部署我们的改密能手 CPM、连接管理器 PSM 后，即可对他们进行密码生命周期管理。

云端通讯说明

- *在云端对应的 VPC 中部署至少一套 CPM/PSM 时，只需开通对应安全组/ACL/路由策略，让它们能网络可达目标对象即可。云端的 VPC 之间，只要保证相互间路由可达，即可最大化地节省功能组件的节点数量。一个区域最少 1 套 CPM/PSM 就可以。*
- *如采用 VPN 打通云端的 VPC，并保证本地路由可达云端，那么直接采用本地的 CPM/PSM 管理云端对象也可以*
- *而 Web 门户 PVWA，则可根据情况选择部署，可以只在本地，也可以让云端也具备相关节点，其无需与目标网络可达。*
- *而 PVWA/CPM/PSM 功能组件，只需能到达本地机房的密码保险库 Vault 的 TCP 1858 端口（甚至可改成 443 或其他端口）。*
- *本地与云端的联通，只要他们所在 VPC 可以利用云端提供的专线、VPN 甚至是弹性公网等方式对接本地即可满足。*

松耦合的优势：

从架构可看到，所有功能组件直接面对被管理目标对象，他们负责联通目标的协议和端口即可。

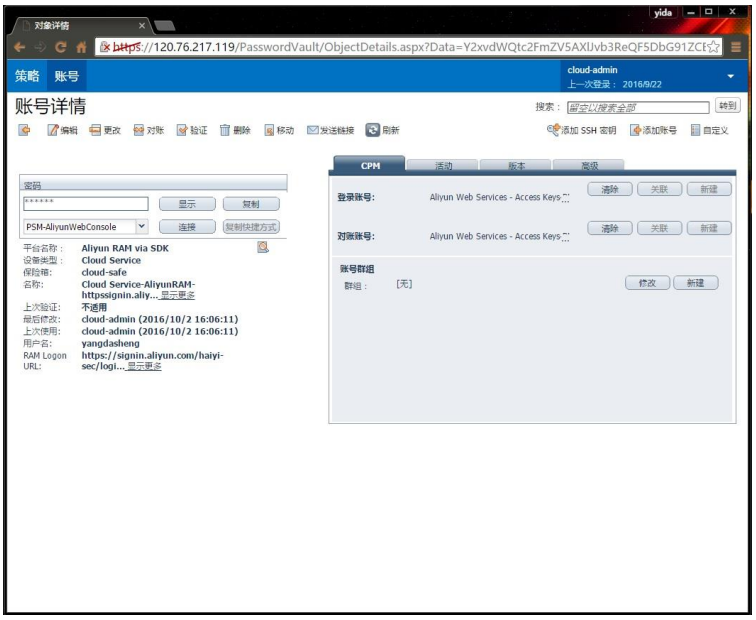
然后，功能组件到密码保险库（本地机房）只需开通 TCP1858 端口。本地 PC 无需开通网络到达目标系统。本地 PC 只需要能到达功能组件的 443、3389 等端口即可。

这些极简的配置要求对于企业安全规划来说，可以大大降低网络规划复杂度，而且还提高网络安全性。

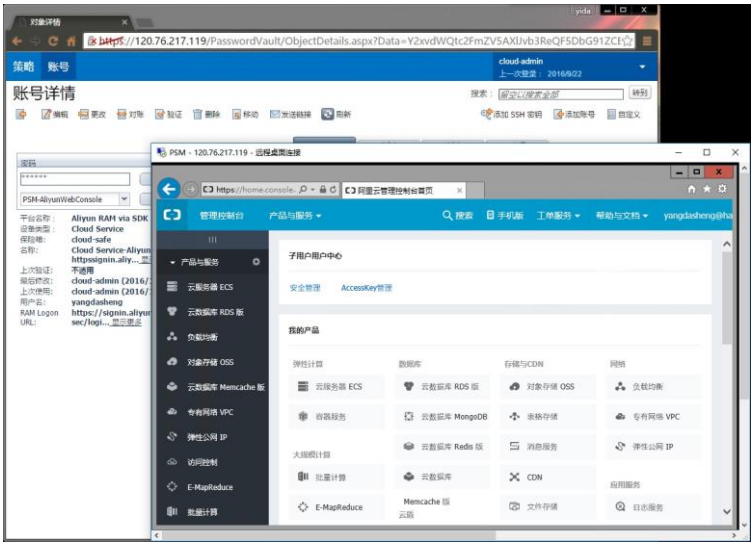
云端特权凭证生命周期管理样例

阿里云 RAM 子账号 WebConsole 密码托管

如下图，我们已经对阿里云 RAM 子账号进行托管：



点击连接后，即可 SSO 单点登陆至该 RAM 子账号的控制台界面：

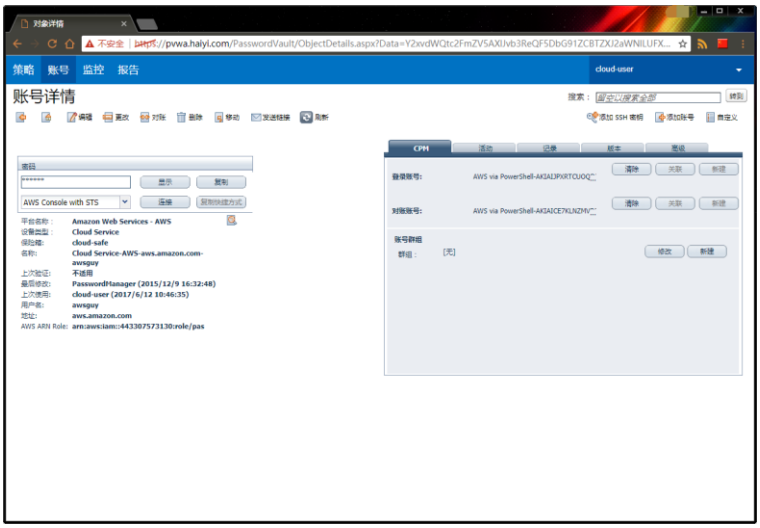


子账号的控制台密码校验、轮换、重置和 SSO 单点连接--视频演示地址：

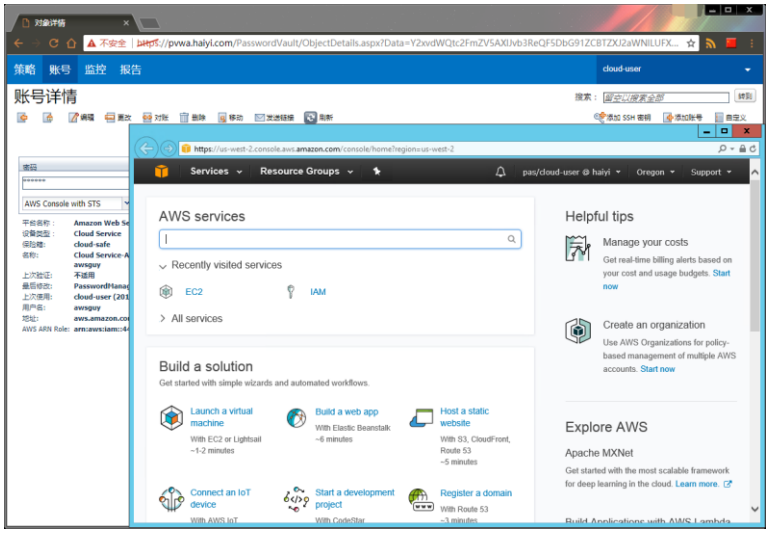
https://v.qq.com/x/page/k0186sdkkl7.html

AWS IAM 子账号 WebConsole 密码托管

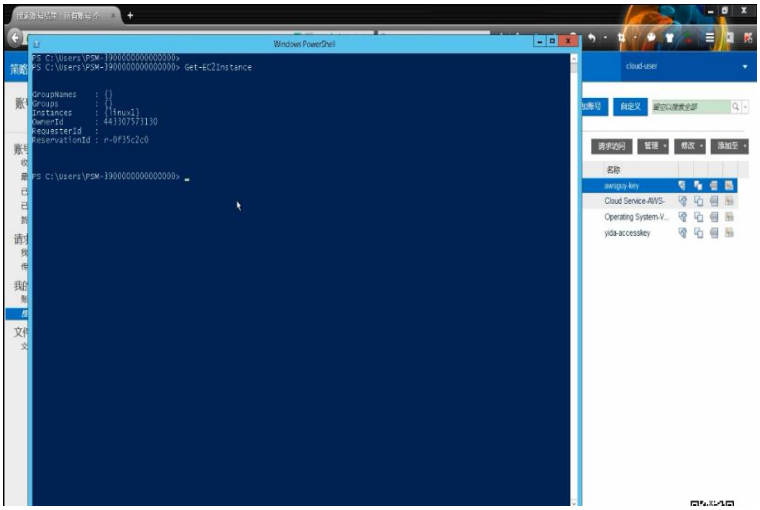
如下图，我们已经对某 AWS IAM 子账号进行托管：



点击连接后，即可 SSO 单点登陆至该 IAM 子账号的控制台界面：



甚至，我们可以根据用户要求，定制发布 AccessKeyID/KeySecret 的 AWS 命令行使用工具，如 Powershell Tool，同样地实现 SSO 单点登陆：



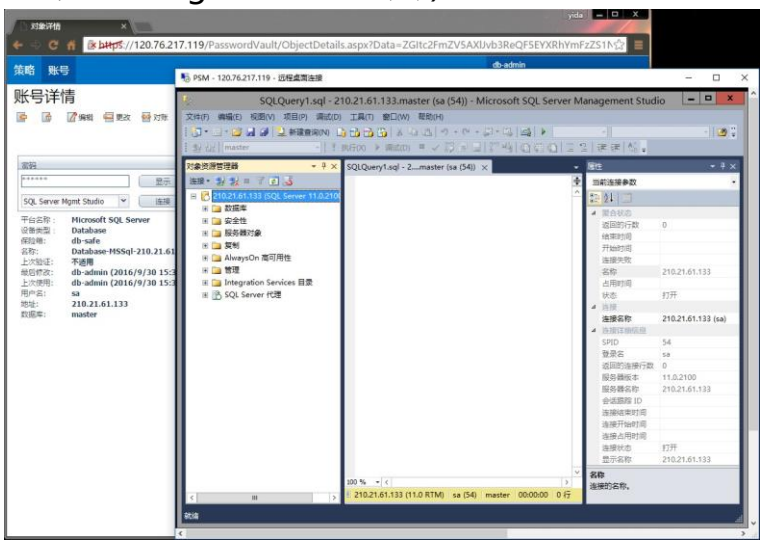
子账号的控制台密码校验、轮换、重置和 SSO 单点连接--视频演示地址：

https://v.qq.com/x/page/m01745sojti.html

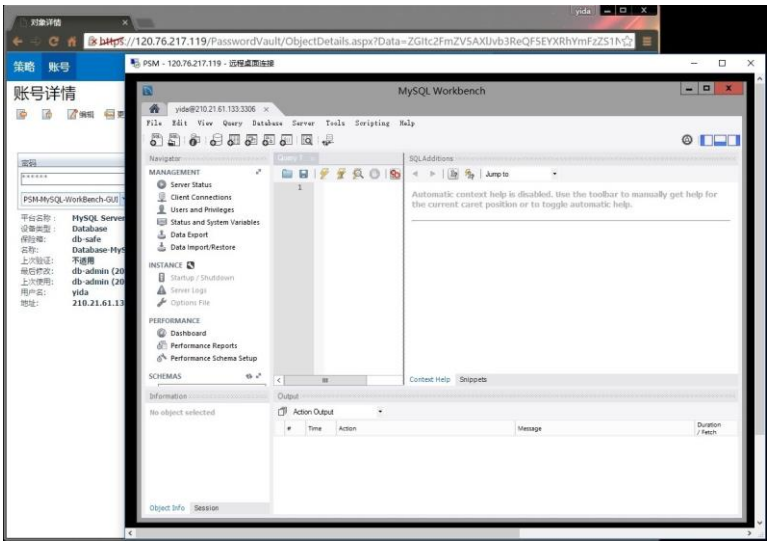
AccessKeyID/Secret 工具 PowershellTool 发布--视频演示地址：
https://v.qq.com/x/page/t0174l5uujf.html

数据库账号密码托管

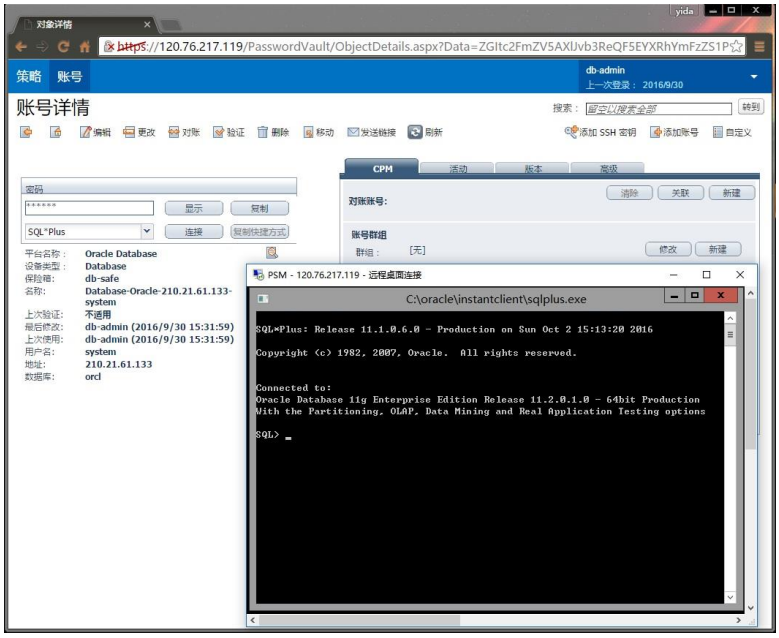
如下，是对 MSSQL 数据库账号托管并进行单点登陆（我们可以为用户发布对应工具，如图配置发布了 MgmtStudio 工具）：



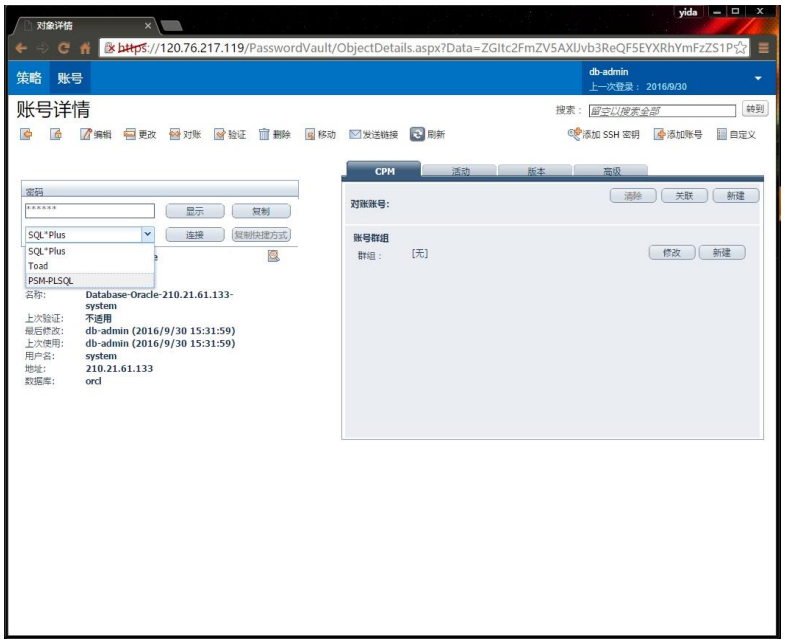
如下，是对 MySQL 数据库账号托管并进行单点登陆（我们配置发布了 Workbench GUI 工具）：



如下，是对 Oracle 数据库账号托管并进行单点登陆（我们配置发布了 SQLPlus 工具）：



当然也可以额外发布其他商业工具，如 PLSQL、Toad 等：



中间件连接池的内嵌数据库账号改密解决方案

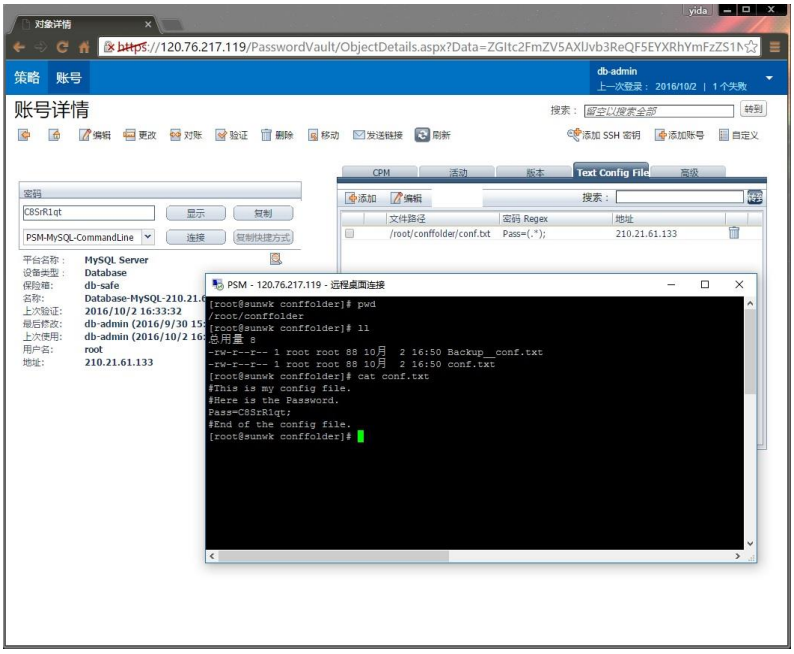
经过一定配置，利用 AIM 的特性，我们可以对中间件连接池里的内嵌数据库账号进行安全优化，最终效果可以让数据库改密，业务无需重启。

下面是以 Weblogic+Oracle 为例--视频演示地址：

https://v.qq.com/x/page/a0196fextg1.html

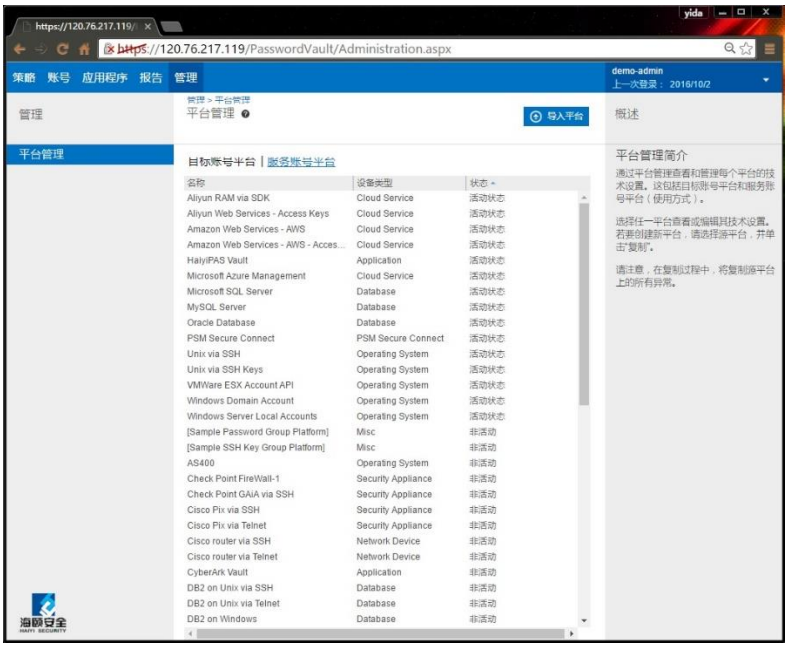
配置文件中的密码同步修改

例如，有个 Root 密码，被写在另一台机器的 conf.txt 上。那么对 Root 改密时，能连同另一机器的 conf.txt 的密码字段一同修改：



强大的插件式定制开发支持

HaiyiPAS 平台支持用户或工程师自开发改密插件（即下图中的平台列表）。开发完毕后，最终只需把 Zip 压缩包通过下图的“导入平台”按钮上传插件和简单配置，即可让您的 HaiyiPAS 快速支持企业自开发的业务系统：



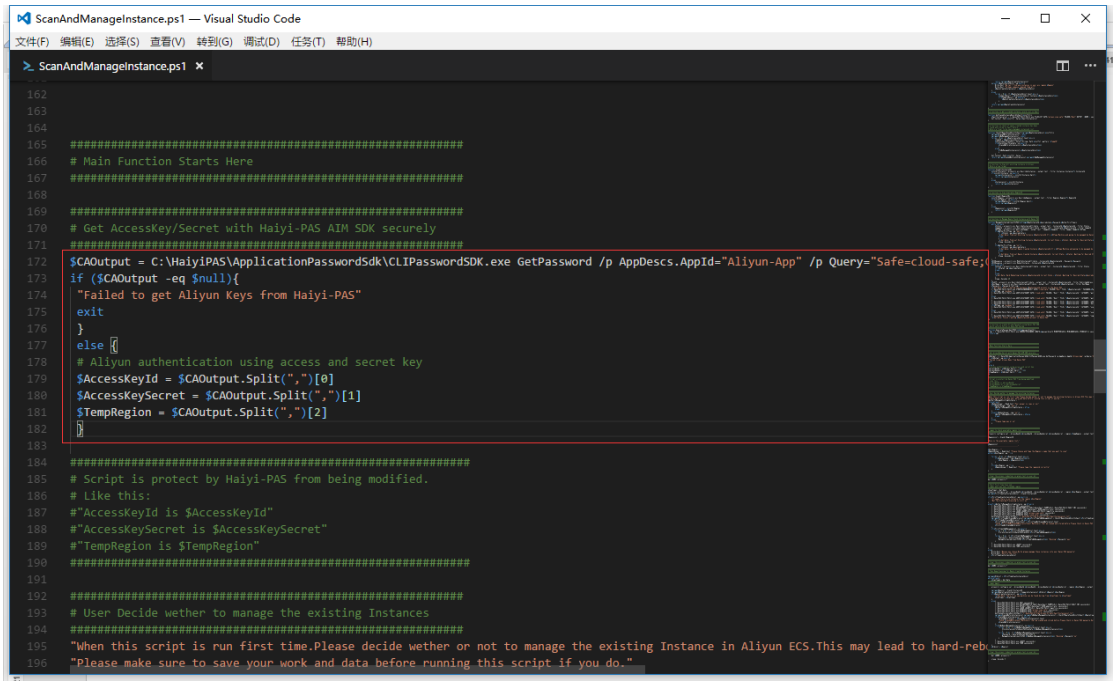
其他特色云端特权凭证管理

如前面提及，我们支持众多（甚至可自开发支持）管理目标。例如微软 Azure 云账号 WebConsole。下面是其演示视频地址：
https://v.qq.com/x/page/q0176et2yf4.html
除了前面提及的，我们还已经可以对 vCenter SSO 账号、RedHat Virtualization 账号、HUAWEI FusionManager 私有云账号等等进行托管。如希望进一步了解，请咨询我们技术团队。

AIM 加强自动化运维的特权凭证管理

阿里云实例扫描脚本示例

云端运维离不开自动化。众多云平台都会对外提供各种 API/SDK 供运维、开发调用。但这些 API/SDK 都需要特权凭证登陆。
而利用 AIM 方案提供的 SDK，例如 CLI、JAVA、Net 等，可以让我们的脚本、工具无需明文内嵌这些特权凭证。例如，下面是我们的一个演示脚本。其目的是利用阿里云的 API(CLI Tool)进行云端实例扫描。脚本的登陆阶段，调用了 AIM 的 CLI SDK，向 HaiyiPAS 平台获取对应特权凭证 AccessKeyID/Secret，而再也无需明文写上这些凭证了：



另外，AIM 可以对该脚本进行“应用身份指纹”验证，例如哈希值等。如上述脚本被篡改一个字符，其就无法利用 AIM SDK 获取到凭证了。这样可以防止恶意打印密码等行为。

下面是该脚本演示的视频地址：

https://v.qq.com/x/page/y0186alakg5.html

Cloud 自动化与 DevOps 安全

HaiyiPAS 各组件都有各自丰富的 API/SDK。如 Vault 能提供命令行管理能力、PVWA 门户网站提供 RestFul 运维 API、AIM 提供 SDK/Soap/RestFul Get 等取密能力。

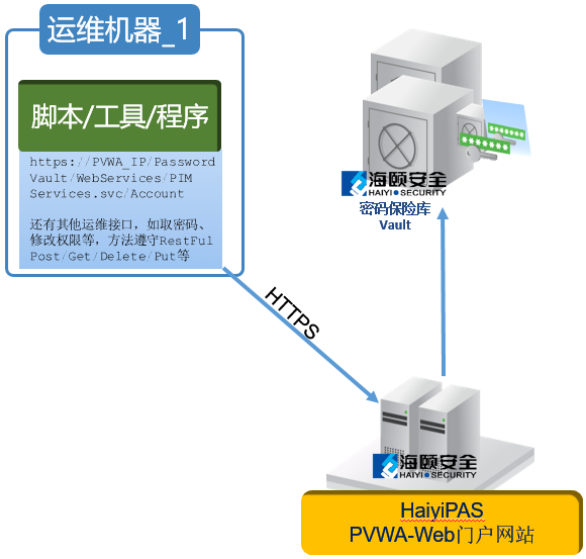
企业只需要把 HaiyiPAS 的接口能力，加入到自身的 Cloud AutoMation 和 DevOps 生命链条中，即可解决特权凭证明文内嵌密码的“老大难”问题。

接口简要

PVWA RestFul API

HaiyiPAS 的 Web 门户自带免费的 RestFul API，调用者的程序/脚本或工具只需使用 HaiyiPAS 平台的用户账号密码成功登陆后，即可进行 API 层面的 PAS 平台操作。

下面，我们有一台运维机器_1，其上跑 Powershell 脚本。脚本中利用 PVWA RestFul 接口添加一个新密码至 HaiyiPAS 平台。逻辑流程如下：



添加密码接口的部分代码样例（需要先登录获取会话 Token）：

```
#adding pass
$targetaddress = "10.0.10.20"
$currentpass      = "Passw0rD"
$targetusername= "Root"
$accountdetail = @{account = @{
            safe= 'os-safe'
            platformID= 'UnixSSH'
```

```
            address= $targetaddress
            accountName = $null
            password = $currentpass
            username = $targetusername
            disableAutoMgmt = 'false'
            }
      }
$addpassbody = (ConvertTo-Json $accountdetail)
$tokenhdrs = @{}
$tokenhdrs.Add("Authorization",$pastoken)
$addkeyurl = "https://PVWA_IP/PasswordVault/WebServices/PIMServices.svc/Account"
      Invoke-RestMethod -Uri $addkeyurl -Method Post -Body $addpassbody -ContentType
'application/json' -Headers $tokenhdrs
```

本接口最终将添加一个 10.0.10.20 地址的 root 密码至 HaiyiPAS 实现托管。

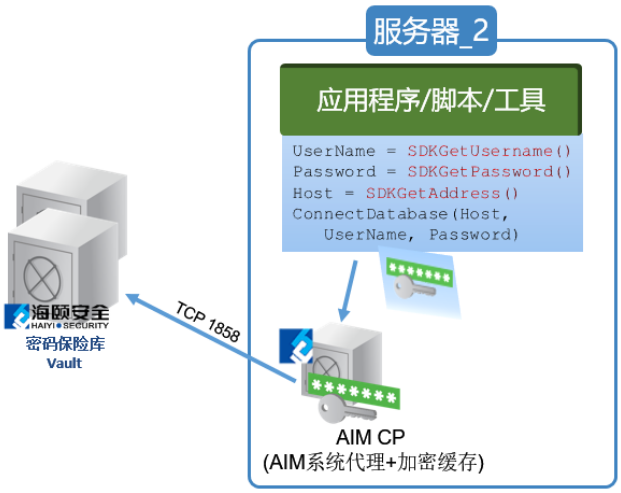
除了添加密码外，PVWA RestFul API 还有多达 50 多个运维接口供调用。

AIM 高性能缓存级 SDK

HaiyiPAS 的 AIM 方案中，提供一个可选的高效加密缓存级别的系统代理。当部署了该代理后，系统上的程序/脚本或工具只需要替换原来内嵌密码的部分，变成我们的 GetPassword()等 SDK 函数即可。

下面，我们有一台服务器_2，其上有一段代码程序。程序中利用 AIM CP 提供的接口，向 HaiyiPAS 平台的密码保险库 Vault 获取特权凭证。

具体逻辑流程如下：



其中，AIM CP 能提供的 SDK 有 CLI、JAVA、C/C++、.Net、COM 等等语言。

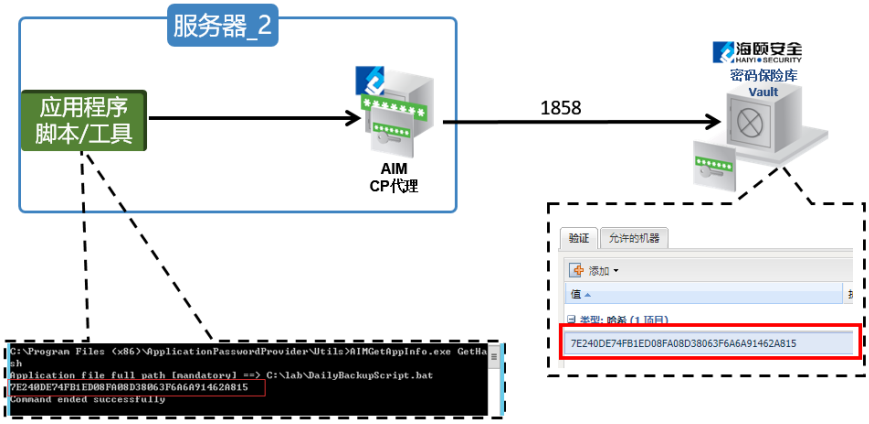
当应用程序/脚本/工具等调用 AIM CP 的 SDK 后，将会向系统代理 AIM CP 索要密码，然后系统代理 CP 则向密码保险库 Vault 索要并返回。同时，代理还会在本地分级加密缓存这些凭证。所以，即使网络断开，也可以依然从本地缓存中为应用程序/脚本/工具提供密码。

同时，我们还能利用代理，对应用/脚本/工具的身份进行指纹验证。例如：

- *代码/脚本哈希值*

- *源 IP*
- *运行身份*
- *证书*
- *执行路径*

下图，是为运维脚本配置了哈希校验并向密码保险库 Vault 获取密码。哈希值一致才能获得密码。

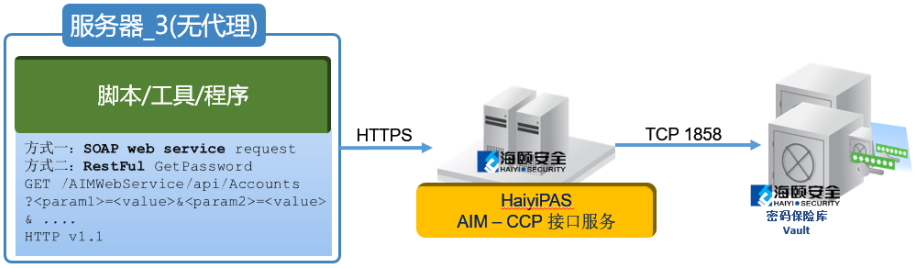


所以，只要开发逻辑得当，哪怕攻击者改动一个源码字符，也无法通过我们的应用身份指纹验证，也就无法获取密码。

AIM 轻量级无代理安全取密 API

HaiyiPAS 的 AIM 另一方案中，可以提供一个集中式的应用身份请求取密接口服务，即 CCP（Central CP）。程序/脚本或工具只需要替换原来内嵌密码的部分，变成取密的 SoapWebService 请求，或者 RestFul Get 请求即可。

下面，我们有一台服务器_3，其上有一段代码程序需要获取凭证。



程序中，有两种选择：既可以利用 SOAP WebService 方式，向 CCP 接口服务组件进行取密；也可以利用 RestFul 的 Get 方式，向 CCP 接口服务组件进行取密。两种方式都会由 CCP 接口组件代为向密码保险库 Vault 索取所指定的密码凭证。操作系统本地无需安装代理。

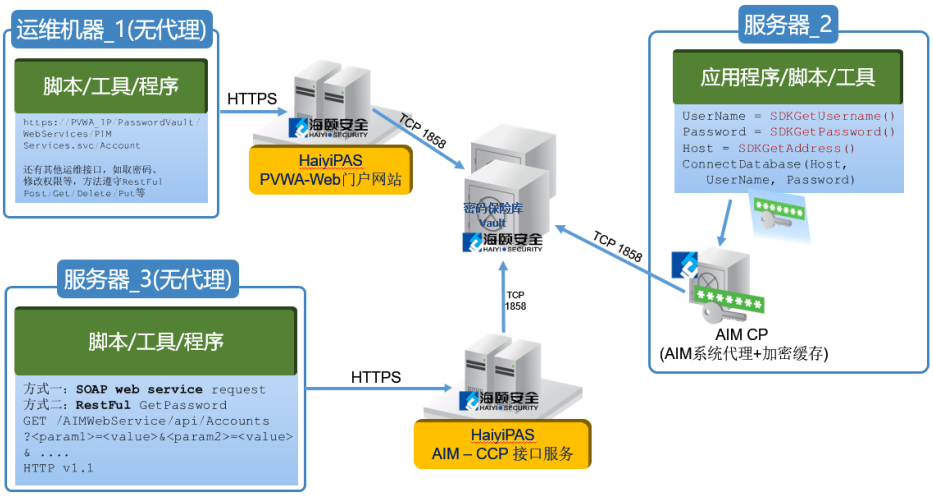
同时，CCP 可以对应用/脚本/工具的身份进行指纹验证。例如：

- *源 IP*

- *运行身份*
- *证书*

接口灵活按需使用

上述所有接口，都可以混合按需封装组合起来，为我们的自动化运维与应用提供可靠安全的凭证获取服务：

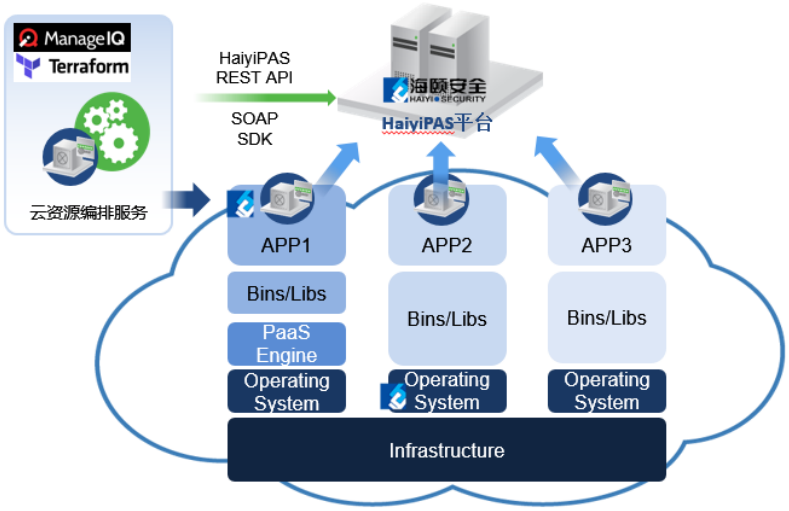


加强资源编排服务过程中的凭证安全管理

例子一：云管平台与第三方资源编排类工具对接

较大型企业会拥有多云多虚拟化数据中心的 IT 架构，因而都采用一些综合能力较强的云管理平台或编排工具，例如 ManageIQ、CloudForm、TerraForm 或者 Packer 等。

举个例子 ,如企业已利用 Terraform 的编排模板 ,实现一键部署某云平台的 EC2、VPC、安全组、负载均衡、路由等，方便快速上架业务应用。那么在原有的” Terraform Play” 动作执行逻辑前后，根据业务情况，利用 HaiyiPAS 的各种 API/SDK 把批量部署生成的实例、数据库账号、业务账号托管至 HaiyiPAS 平台里即可。如下图：

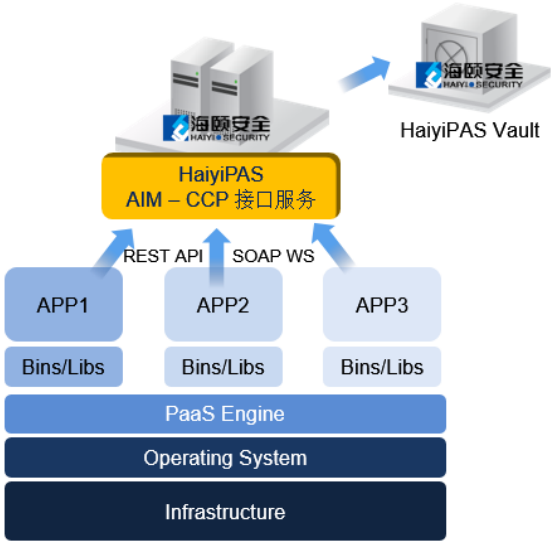


而 HaiyiPAS 平台自身支持“一托管，即改密”的配置，让批量生成的实例、数据库、业务账号都能马上被安全托管。

例子二：Docker Container/VM 等调用 CCP 取密

越来越多企业青睐 Docker 的轻量级、敏捷快速部署应用的解决方案，都把业务/微服务等放在 Docker 集群上运行。

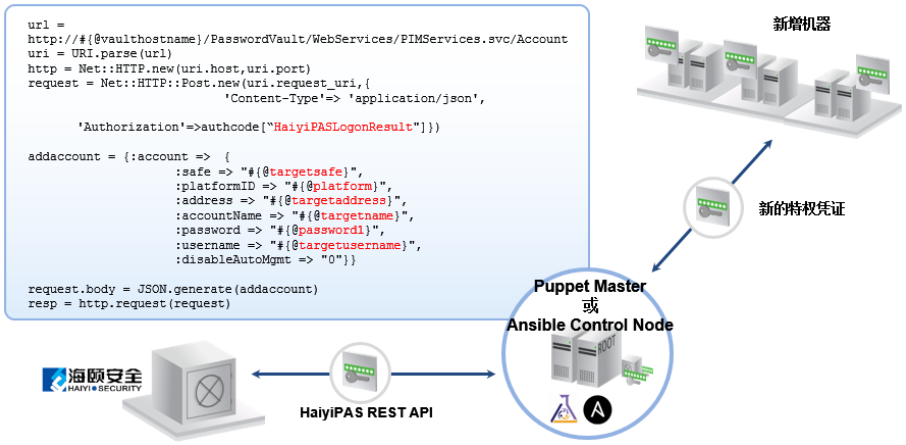
举个例子，下面，是 Docker 上每个容器 Container 里利用 SOAP WebService 或 Rest API 实现取密后，运行对应业务逻辑。



例子三：Ansible/Puppet 等自动工具集成

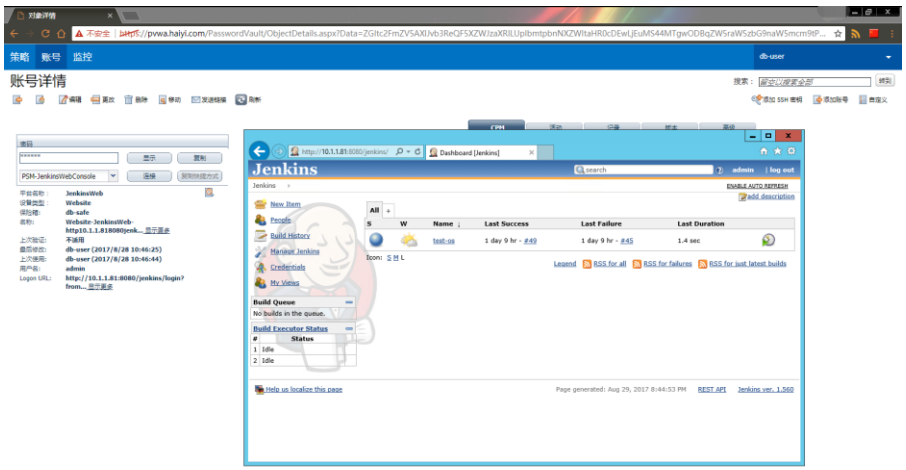
很多企业已经在使用 DevOps 概念实现业务的快速开发测试部署运维闭环。但

其中，所用的 CI/CD 工具，常见如 Jenkins、Ansible、Puppet 等，在使用过程中都面临凭证传递、创建和安全保管等问题。那么可以考虑利用 HaiyiPAS 的 Rest API 等，对过程中所用的特权凭证保护起来。



例子四：CI/CD 工具的 WebConsole 账号托管

不止云平台有 WebConsole，其他绝大多数的 DevOps 工具，都会有自己的 WebConsole 的 admin 账号。这些特权账号都可以被 HaiyiPAS 所安全托管。下图，是 Jenkins 工具 WebConsole 的 admin 账号被安全托管和实现 SSO 登陆：



方案优势总结

当企业部署了 HaiyiPAS 平台后，可以为企业带来如下好处：

保护云环境的核心安全

- 控制台账号安全托管
- 特权账号的使用会话都有全程审计记录

实现云自动化运维安全

- 自动化部署可以马上托管新增的特权凭证
- 应用/工具/脚本可以安全地使用或获取特权凭证

集中式与分布式部署兼顾

- 组件化/模块化设计可以高度兼容各种云平台的部署与对接

平台可灵活按需地平稳升级

- 完美适配和跟随企业的物理环境-本地虚拟化-私有云-混合云架构进化

平台高可靠设计和架构

- 核心组件可提供 HA 与多级灾备部署
- 功能组件可以横向扩展部署成集群等
- 支持配套负载均衡进行 HTTP 访问分发

改密插件式开发灵活应对 SaaS 挑战

- 改密插件的自开发或定制开发使得企业灵活应对未知的 SaaS 应用特权账号管理难题
- 无需重复购置新平台，提高投资回报