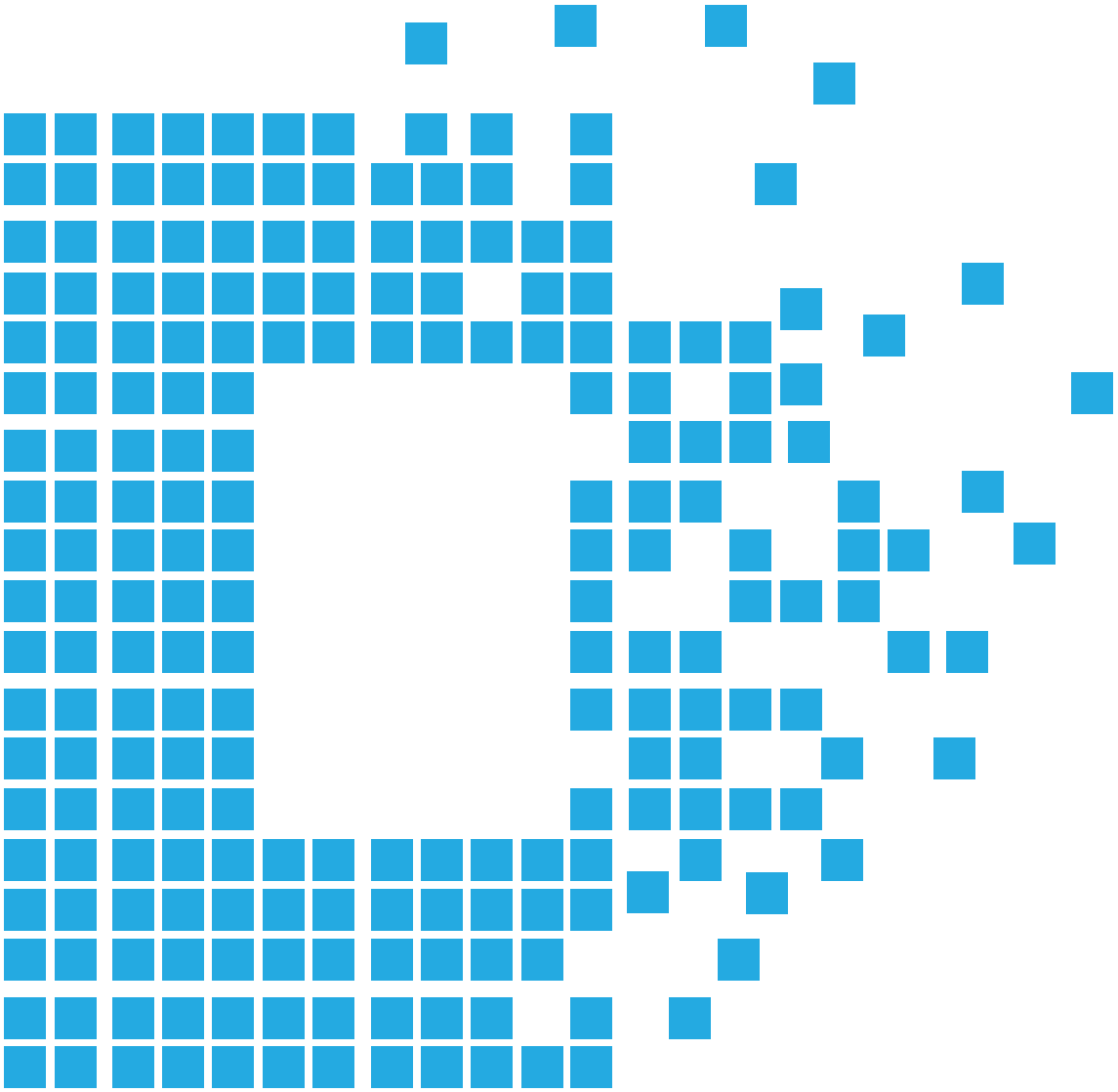


DCLive

特权访问管理

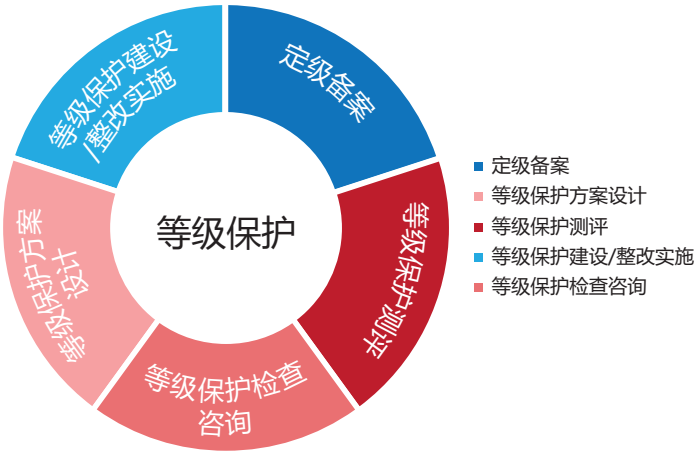
Privileged Access Management

Datcent

德 讯 科 技

一、特权访问与合规

随着信息化与业务内容及模式日渐紧密的融合，IT 合规成为企业合规与内控中不可或缺的重要一环。特权访问管理归属于 IT 合规 / 身份管理领域中的一个特定场景，即对能给企业 IT 架构安全造成重大风险的高权限账号使用的管控。特权账号一旦被盗取或被恶意使用极可能给业务连续运行和核心信息安全带来重大甚至不可挽回的损失。因此，《信息系统等级保护基本要求》将特权访问管理作为评级为等保第三级及以上信息系统的必要安保技术措施之一。



设备、系统、应用中设定有管理员账号，可对系统进行部署、配置变更、重启、删除等高危操作。且系统都设计有默认特权账号，例如 root、administrator、admin 等。在运维实践中，特权账号，特别是默认特权账号，通常由多个运维人员共同掌握。且运维人员为方便记忆，习惯在多个不同系统中创建相同的特权账号。这些运维实践不能满足《等保基本要求》中的身份标识唯一性、以单个用户为颗粒度的授权控制、和安全审计等要求，也增加了特权账号被盗用的风险。构建特权访问管理（Privileged Access Management，PAM）解决方案，或称堡垒机，成为企业建设信息安全时的必要措施。

二、PAM 面临的挑战

企业在构建特权访问管理（Privileged Access Management，PAM）解决方案过程中须应对以下几个挑战。

- 特权账号使用权限的控制

首先需要将运维人员身份识别与特权账号使用分离开来。PAM 通过用户名 + 口令、双因素、生物信息识别等认证技术对运维人员身份进行唯一性识别。PAM 集中管理特权账号的用户名 + 口令或登录秘钥等登录信息，并细颗粒度地定义和控制运维人员使用特权账号登录目标系统的权限。例如，对运维人员使用特权账号的场景做细致的分析，从操作位置、操作时间、人员身份、目标对象等四个角度来控制特权账号的使用。

- 特权账号的保护

特权账号保护需解决三个层面的挑战。第一层，PAM 需要管理所有设备、系统、业务应用中存在的所有特权账号。第二层，PAM 需对特权账号的口令或秘钥定期更新。第三层，PAM 中的特权账号存储须安全且高可用。

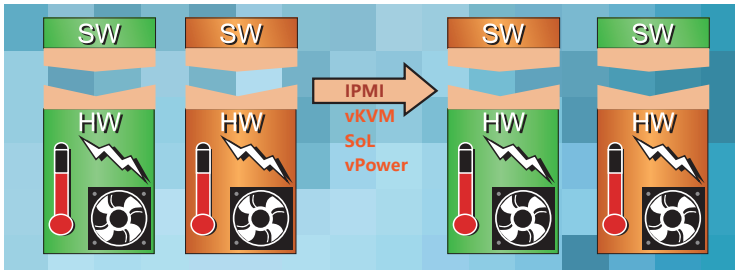
在第一层面上面临的挑战是如何做到无遗漏地归集所有设备、系统、业务应用中的特权账号，并能够定期清理或归集目标系统上新增的特权账号。若手工完成此项工作则将耗费大量的人力与时间，且不能难免遗漏。自动化或部分自动化将是应对此挑战的关键。

在第二层面上面临的挑战是特权账号口令定期更新过程的完整性管理。PAM 须定期对所有被管理的特权账号进行自动更新，并在更新后对新口令的有效性进行验证，若出现异常则能自动修复。

在第三层面上面临的挑战是口令的安全与可用性管理。特权账号的口令须加密存储，入侵者无法获得明文口令。口令的存储空间需有完整性设计，能验证是否曾遭受侵入。特权账号口令高可用性需通过冗余的在线存储空间叠加离线的存储空间的方式来实现。

▶ 访问接口的管理

访问接口管理的挑战在于，设备、系统、和业务应用的多样性造成了接口类型与数据格式的多样性。PAM 需要能够支持企业 IT 基础架构上所有存在的特权访问接口。可以将特权访问接口分为带内、带外两大类。带内接口是指由操作系统或业务应用提供的管理接口，例如 RDP、VNC、X11、SSH、Telnet、Rlogin、HTTP/HTTPS 等。带外接口是指由 IT 硬件设备提供的管理接口，例如 KVM、RS232 console、IPMI、vKVM、SoL、vPower 等。带外接口虽由硬件设备提供，但通过操作系统提供的 API 可再进入操作系统，乃至操控设备上安装的业务应用。

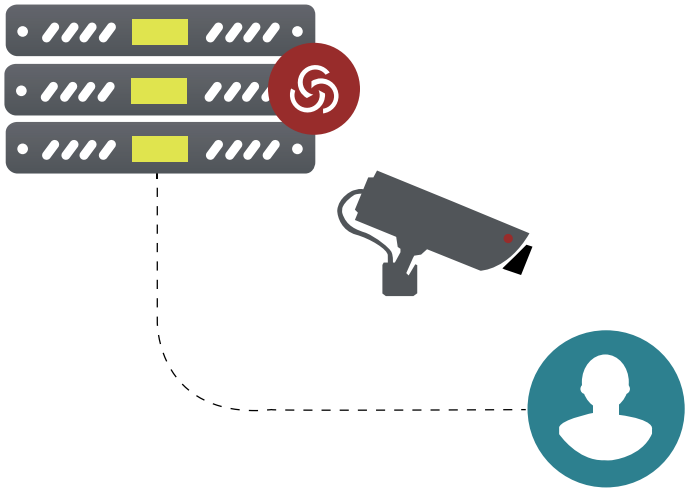


X86 服务器已成为企业业务运算的标准计算平台，IPMI、vKVM、SoL、vPower 作为 x86 服务器的标准带外接口必须被纳入 PAM 的管理范围。IPMI 接口提供服务器硬件健康监测和 BIOS 参数设定；vKVM 提供图形管理界面，可接入操作系统并操控业务应用；SoL 提供字符管理界面，亦可接入操作系统并操控业务应用；vPower 可对服务器电源进行开、关、重启操作。遗漏上述带外接口的管理，则不能建立一个完整的 PAM 系统。

▶ 访问过程的风险控制和操作审计

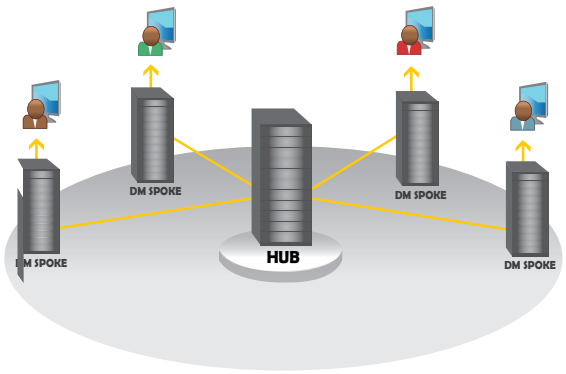
访问过程需要被记录并建立索引，操作指令的风险需要实时分析，对恶意操作能够被阻拦，事后形成统计报表等。不同的特权访问接口有不同的操作界面与数据格式，因此 PAM 相应的记录手段与方式也各异。挑战在于 PAM 需要在异构的 IT 基础架构上建立一致的审计方式和风险控制手段来满足企业风险控制与安全审计的规程与要求。无论操作是通过带外或是带内特权访问接口进行，无论操作方式是图形化或是命令行，无论特权访问接口协议是开放或是私有，操作全程都需要被记录。

操作记录建立索引是基本需求。索引可以建立在操作人员身份、操作发起地址、操作目标系统、操作时间（起始、终止、时间片段）等之上。操作指令的自动识别是高级需求。风险识别与风险防范建立在操作指令自动识别基础之上。



PAM 系统可用性管理

PAM 作为 IT 基础架构运维操作的汇聚点，PAM 的可用性直接影响到 IT 基础架构运维 SLA（服务等级合约）中的 MTTR（平均修复时间）等关键指标。PAM 的可用性管理需从两个方面入手，PAM 系统健壮性和网络可达性。主备双机配置的 PAM 虽然防止了单点故障提升了系统健壮性，但无法应对局部网络故障可能造成的 PAM 不可达。经典的“Hub+Spoke”分布式架构则可以很好地同时应对系统健壮性与网络可达性这两方面的要求。



“Hub+Spoke”架构对 PAM 的构架设计提出了挑战。从 PAM 的使用用户角度出发，“Hub+Spoke”架构表现为一个分布式多节点系统，任一节点提供的服务内容与质量完全相同，用户根据节点负载和网络路径选择最优节点登录访问。从组成 PAM 系统的各节点出发，则分为 Hub 节点、Backup 节点、Spoke 节点，各节点承担的系统角色不同又互为备份。因此，经典的“Hub+Spoke”提供了 PAM 系统的高可用性。

三、DCLive 特权访问管理

DCLive 是德讯科技继 ICS 堡垒机之后发布的新一代 PAM 系统。DCLive 核心功能如下：

人员身份与访问管理

DCLive 采用集中账号管理，基于角色控制访问操作权限，对运维人员身份账号进行细粒度、全生命周期的管理。

（1）身份识别

实名制创建用户，账户与人员身份一一对应，身份唯一。

用户访问目标设备，需先登录 DCLive 进行身份识别认证，支持用户名 + 口令、生物信息识别、动态双因素（Radius、RSA SecureID 认证、LDAP/AD 域等）等认证方式。

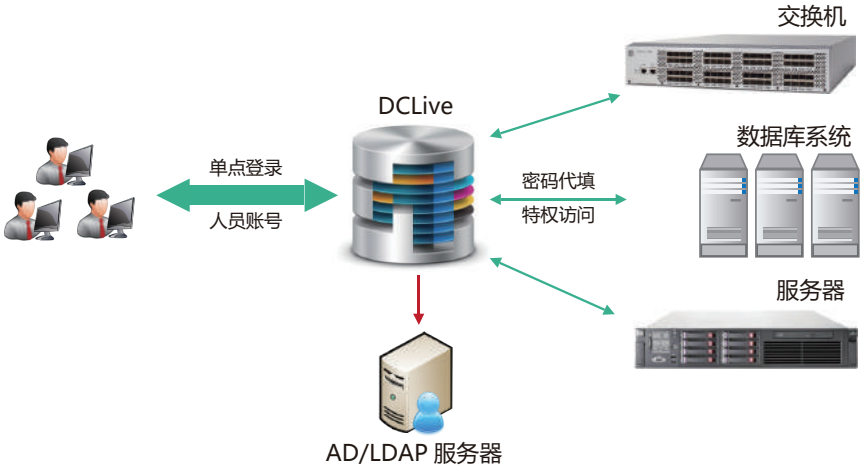
登录过程中若连续输错密码，系统会自动锁定被登陆的该用户账号，保护账户安全。

（2）角色定义

系统定义五种身份角色：系统管理员、设备管理员、运维管理员、审计管理员和普通用户，并规范了角色对应的访问权限。

（3）IT 设备资源管理

通过 DCLive，可根据 IT 设备的类型、应用类别、归属部门等条件划分设备组，并提供视图管理。同时，可按照部门、职位、角色等条件划分用户组，并统一配置用户组的访问权限，实现了人员、设备等资源的统一管理，权限的统一分配。



（4）访问控制

DCLive 从操作位置、操作时间、人员身份、目标对象等四个角度来控制特权账号的使用，采用多纬度细粒度控制手段，实现访问权限最小化，操作行为安全化。

可通过黑白名单形式预先授权用户可执行的访问指令，确保正确的用户执行正确的动作，保障访问的合规性。

根据关键业务设备的重要程度灵活设置采取双人授权访问机制，需要双人口令认证通过后才能访问，两者相互制约，增设一层安全访问保护屏障

（5）单点登录

DCLive 提供单点登录、密码代填的功能，用户只需完成一次登录认证，即可直接访问所有权限内的目标设备，无需多次输入目标设备的特权帐号及密码，既简化了访问过程，又降低了泄密风险。

▶ 特权账号管理

（1）自动采集

DCLive 内置采集账号脚本，通过 SSH 和 TELNET 协议，可自动采集设备、系统、业务应用的所有帐号，并定期进行安全性检测。管理员通过 DCLive 提供的账号列表无遗漏的进行管理，节省了大量的人力，提高了管理效率。

支持对服务器、网络设备的特权帐号定期进行安全性检测，提供人工或自动定期采集，按指定密码强度定期批量修改，提高密码管理高效性；

提供人工设定或随机生成密码机制，按密码强度规则随机生成密码。

（2）保存与防护

DCLive 对特权账号的口令均采用密文管理，帐号采集及密码的校验 / 更新均以密文形式通过邮件发送给指定的特权帐号管理人员，保证了账号口令的安全性。

同时，管理员可定期将特权账号导出备份，通过专用的帐号阅读器，结合加密密钥进行查看与管理，实现在线存储和离线存储的备份机制，保证账号口令的高可用性。

（3）定期变更口令

管理员可设置DCLive定期更改账号口令并变更周期、密码强度、重复校验等手段来保证口令的安全。同时，为保证账号口令的正确性和完整性，DCLive 会在口令自动更新后实时校验，若出现异常会及时自动修复。

（4）密码代填

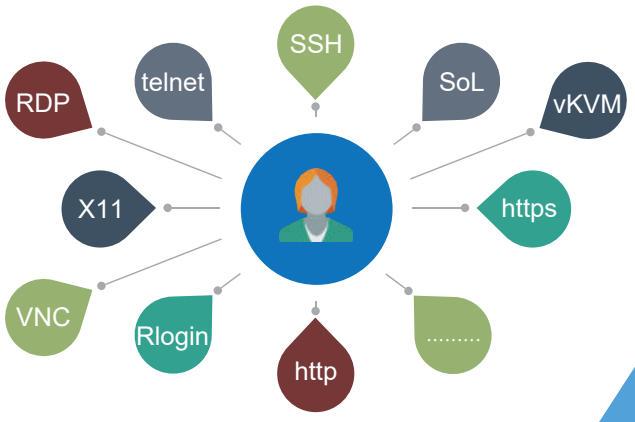
通过 DCLive，管理员可预先填写账户的密码口令，使用者只需登录 DCLive 账号即可发起对目标设备的访问，既简化了访问过程，又降低了泄密风险。

▶ 带内接口管理

带内接口是指由操作系统、虚拟化层、数据库系统、应用系统发布的访问接口。DCLive 为带内接口提供访问控制、账号代填、操作审计。DCLive 以自有插件的方式提供带内接口的访问客户端程序。

DCLive 支持的带内接口如下：

- 字符型访问接口，如 Telnet、SSH、RLogin 等
- 图形化访问接口，如 RDP、Xwindows、VNC、VDP 等
- 文件传输接口，如 SCP、SFTP、FTP 等
- Web 访问接口，如 HTTP、HTTPS 等
- 数据库访问接口，如 Oracle、MS-SQL、DB2、Informix、Sybase、MySQL 等
- 第三方访问工具，如 Radmin、AS400、PC Anywhere、VMWare、XManager 访问等



IPMI 接口管理

IPMI 是 x86 服务器上 BMC(主板控制芯片)提供的带外管理接口。DCLive 支持标准 IPMI1.5/2.0 接口，同时支持各服务器厂商的扩展接口，例如 HP iLO、DELL DRAC、华为 iMana、联想 IMM 等等。DCLive 为 IPMI 接口提供访问控制、账号代填、操作审计。DCLive 使用通道技术向操作者提供 IPMI 原生 Java 控件客户端。

DCLive 在 IPMI 接口上提供的功能如下：

（1）提供服务器硬件健康监测，如 CPU、内存、RAID、机箱温度、风扇转速等；

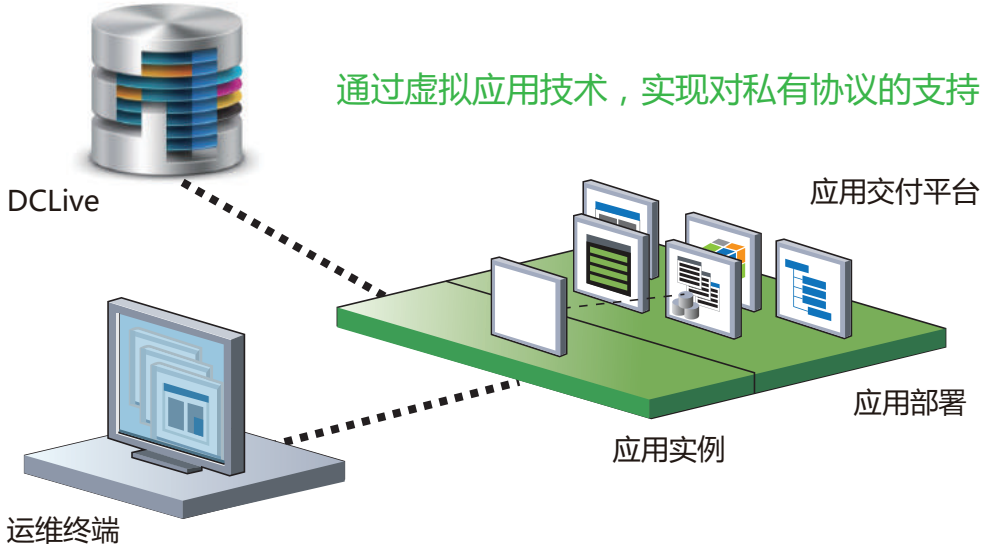
（2）vKVM 接口，获得操作系统与业务应用的图形操作界面；

（3）SoL 接口，获得操作系统与业务应用的字符操作界面；

（4）vPower，对服务器电源进行开、关、重启操作。

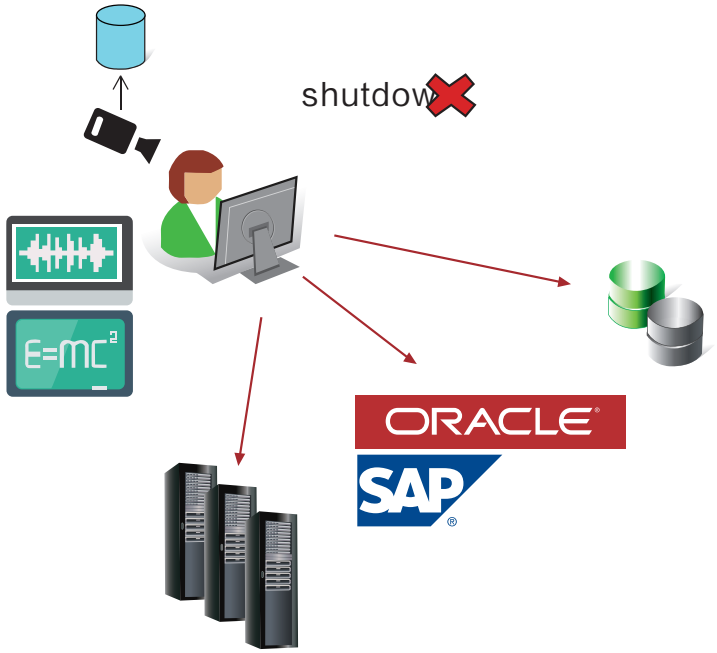
私有接口管理

对于封闭的应用系统，DCLive 内嵌的应用交付平台通过虚拟应用发布技术，将应用系统的客户端操作界面推送到操作者的桌面。DCLive 在完成使用者的身份识别与确认使用者的访问权限后，在同一界面中向使用者提供封闭应用系统的访问与操作。



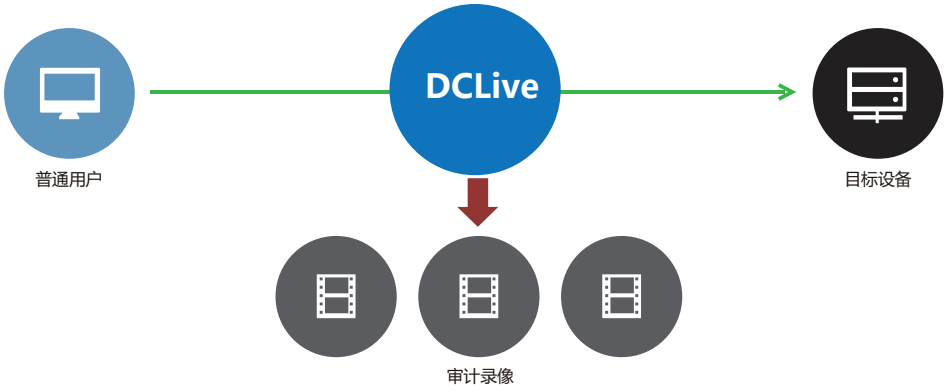
风险识别与阻断

对于字符型会话（如 TELNET、SSH），DCLive 可实时监控运维过程中的操作员发出的指令。管理员可设置操作命令黑白名单实现操作监控和报警策略制定，对于合法指令操作并审计，对于非法的指令操作，可采取“告警”、“拒绝”或“断开”等控制。



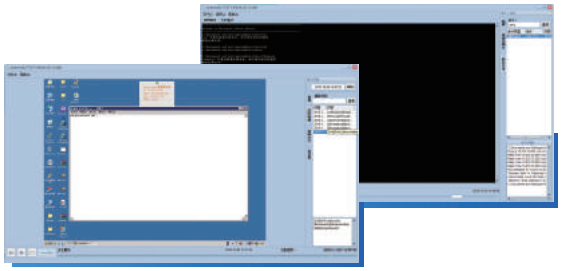
操作审计

DCLive 实现运维管理全生命周期的审计，采用流媒体形式记录运维人员登陆 DCLive 至登出 DCLive 的完整会话过程，支持对字符、图形等多种类型会话的全面审计。



管理员可查看操作日志和回看录像，全方位审计什么人，在什么时间，什么地点（IP/MAC），通过什么方式，做了哪些操作。

同时，管理员在观看审计录像时，可在检索栏中输入敏感指令，审计录像可快速定位到敏感指令的画面，实现运维操作过程的快速定位、精确跟踪以及真实重现，协助审计人员对非法运维操作节点的排查及故障责任的追溯。



矩阵式监看与操作界面

除单个独立的会话操作窗口外，DCLive 还提供整合多个会话操作窗口的矩阵式操作界面。矩阵式会话操作界面可用于日常实时监看业务系统的运行情况、远程多人协同操作等场景，例如电力行业调度监控、金融行业资金交易监管等。

通过 DCLive，监控人员选择多个业务主机，采用矩阵式窗口（如 2*2、3*3、4*4、…、8*8）呈现，各个会话窗口画面同时播放，动态、直观地了解所有业务主机的运行状态。如在监看过程中发生异常或违规操作现象，可快速由“监看”模式切换至“操作”模式，强行阻断当前会话，确保运维过程事中有效监控。

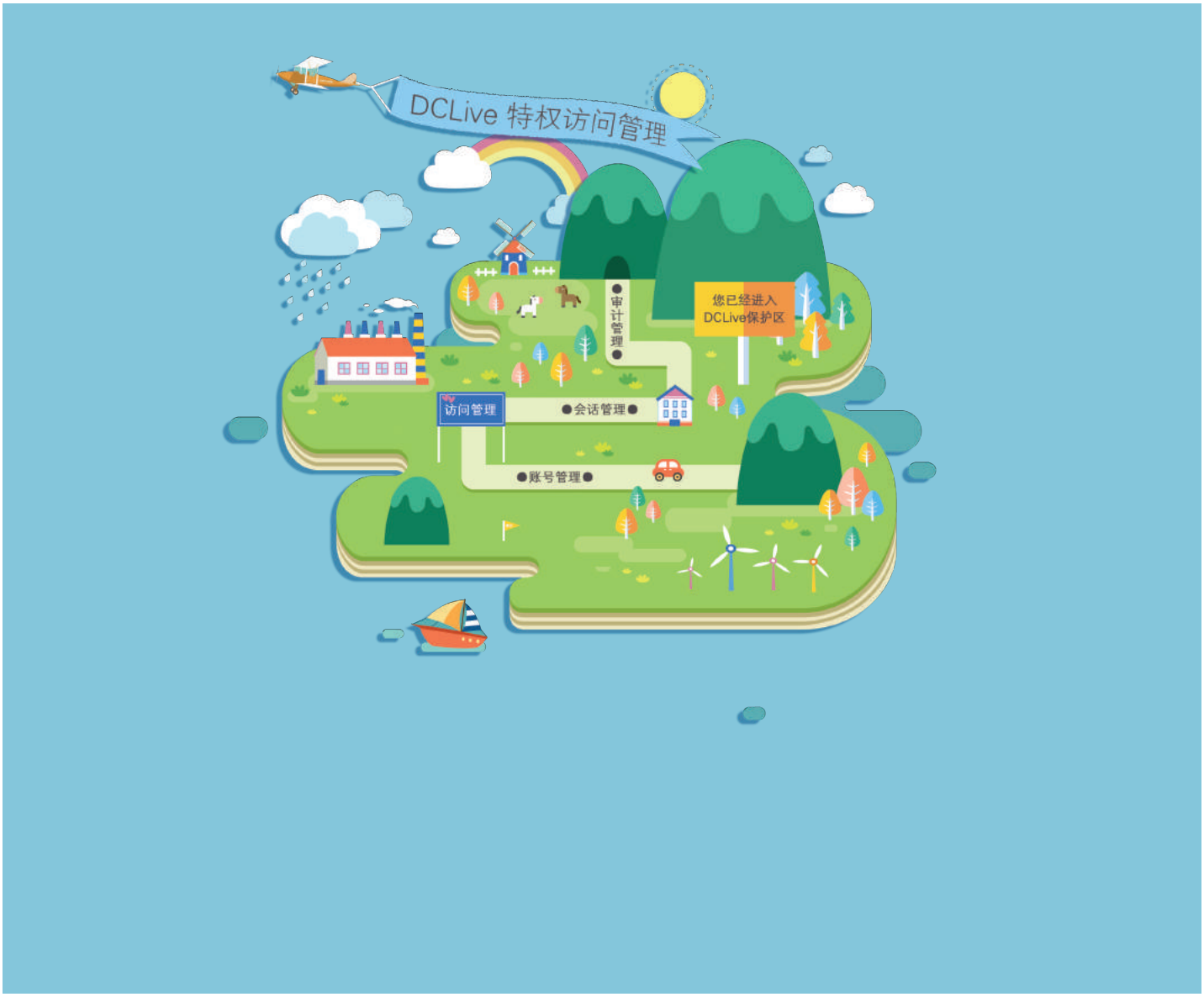
审计与报表

DCLive 基于对登录、登出、会话创建、会话释放、风险告警等运维过程数据的统计与分析，提供多元化、直观易用的报表系统。协助管理人员从多纬度了解运维安全的整体状况，对目标设备的运维历史、运维人员的操作过程、风险指令的使用安全进行有效评估，从而针对 IT 运维风险控制采取有效的优化措施。

DCLive 预设了系统会话审计与违规报警等各类报表，如会话操作、帐户管理、数据库操作审计、设备运行状态等多种报表；

DCLive 支持使用条件组合进行查询与统计，包含日报表、月报表、或年报表，提供 PDF、DOC、EXCEL、HTML 等报表格式输出；

DCLive 提供报表订阅（邮件通知）功能，支持报表格式自定义，灵活设置报表的显示内容。



WWW.DATCENT.COM 400-886-7711 SALES@DATCENT.COM

德讯 北京
北京市宣武门外10号庄胜广场中央办公楼南楼15层
邮编：100052
电话：86-10-62662755
传真：86-10-88579495

德讯 上海
上海市徐汇区虹桥路808号(淮海西路口)3幢(D栋)D331室
邮编：200051
电话：86-21-64479755
传真：86-21-64479756

德讯 南京
南京市雨花台区花神大道21号德讯科技大厦
邮编：210012
电话：86-25-82227888
传真：86-25-82227800

德讯 广州
广州市天河区中山大道西华景路1号南方通信大厦801室
邮编：510630
电话：86-20-38638387
传真：86-20-38637144

德讯 成都
成都市一环路东二段48号中电信谊商务楼601室
邮编：610000
电话：86-28-85216879
传真：86-28-84371419