ICS 35.240
CCS L 67

团 体 标 准

T/BSIA XXXX—XXXX

混合云自动化运维系统基本要求

Basic requirements for hybrid cloud automated maintenance systems

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

北京软件和信息服务业协会　　发 布

目 次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 1
5 系统概述 2
6 功能要求 2
6.1 资源管理 2
6.2 事件管理 2
6.3 自动巡检 3
6.4 流程自动化 4
7 自动化运维场景 4
7.1 启动停止 4
7.2 备份恢复 5
7.3 发布回退 5
7.4 故障处置 5
7.5 灾备切换 5
7.6 日常变更 6
8 安全要求 6
8.1 概述 6
8.2 权限管理 6
8.3 网络安全 6
8.4 数据安全 6
9 运维管理 6
9.1 概述 7
9.2 风险评估 7
9.3 应急响应 7
参考文献 8

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由北京软件和信息服务业协会提出。

本文件由北京软件和信息服务业协会归口。

本文件起草单位：北京神州光大科技有限公司、北京神行云服科技有限公司、北京软件和信息服务业协会、郑州迪维勒普科技有限公司、北京梦天门科技股份有限公司、神州数码融信云技术服务有限公司、北京金山顶尖科技股份有限公司、无明智囊（北京）科技有限公司、北京广通优云科技股份有限公司。

本文件主要起草人：闻军、沈昊、周峰、王建文、龙飞、张磊、刘崇、赵鑫恒、程晨、刘亚兵、周瑜、王彬、刘东海、刘玉环。

引　言

本文件的发布机构提请注意，声明符合本文件时，可能涉及到《一种混合云运维管理方法及系统》（CN113676354A）、《通过云平台对IT系统维保服务信息进行处理方法及系统》（CN114819762A）等专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构承诺，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：北京神州光大科技有限公司

地址：北京市大兴区北京经济技术开发区荣华南路2号院1号楼18层1804

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

混合云自动化运维系统基本要求

1 范围

本文件规定了混合云自动化运维系统的功能要求、自动化运维场景、安全要求及运维管理内容。

本文件适用于混合云自动化运维系统的应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估方法

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 24363 信息安全技术 信息安全应急响应计划规范

GB/Z 24364 信息安全技术 信息安全风险管理指南

GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求

GB/T 32400 信息技术 云计算 概览与词汇

GB/T 37973 信息安全技术 大数据安全管理指南

GB/Z 38649 信息安全技术 智慧城市建设信息安全保障指南

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

YD/T 4059—2022 混合云平台安全能力要求

3 术语和定义

GB/T 32400界定的以及下列术语和定义适用于本文件。

3.1

混合云 hybrid cloud

至少包含两种不同云部署模型的云部署模型。

[来源：GB/T 32400—2015，3.2.23]

注：本文件中指公有云和私有云混合的云部署模型。

3.2

混合云自动化运维系统 hybrid cloud automated maintenance systems

集成多个云平台、多个区域、多种云服务，通过自动化操作、自动化监控、自动化分析等方式提升系统运维效率和稳定性。

3.3

机器人流程自动化 robotic process automation（RPA）

是一种应用程序，模拟人类的操作方式，实现对计算机应用程序、网站、ERP系统等的自动化操作。

注：IEEE（电气与电子工程师协会）将RPA定义为：RPA是通过软件技术来预定业务规则以及活动编排过程，利用一个和多个互不相连的软件系统协作来完成一组流程活动、交易和任务，同时需要人工对异常情况进行一些管理来保证最后的交付结果和服务。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

CPU：中央处理器（Central Processing Unit）

CLI：命令行界面（Command-Line Interface）

RPA：机器人流程自动化（Robotic process automation）

5 系统概述

不同厂商针对混合云部署场景开发了不同的运维工具，本文件旨在针对混合云自动化运维系统提出详细要求及参考模型（如图1所示）。

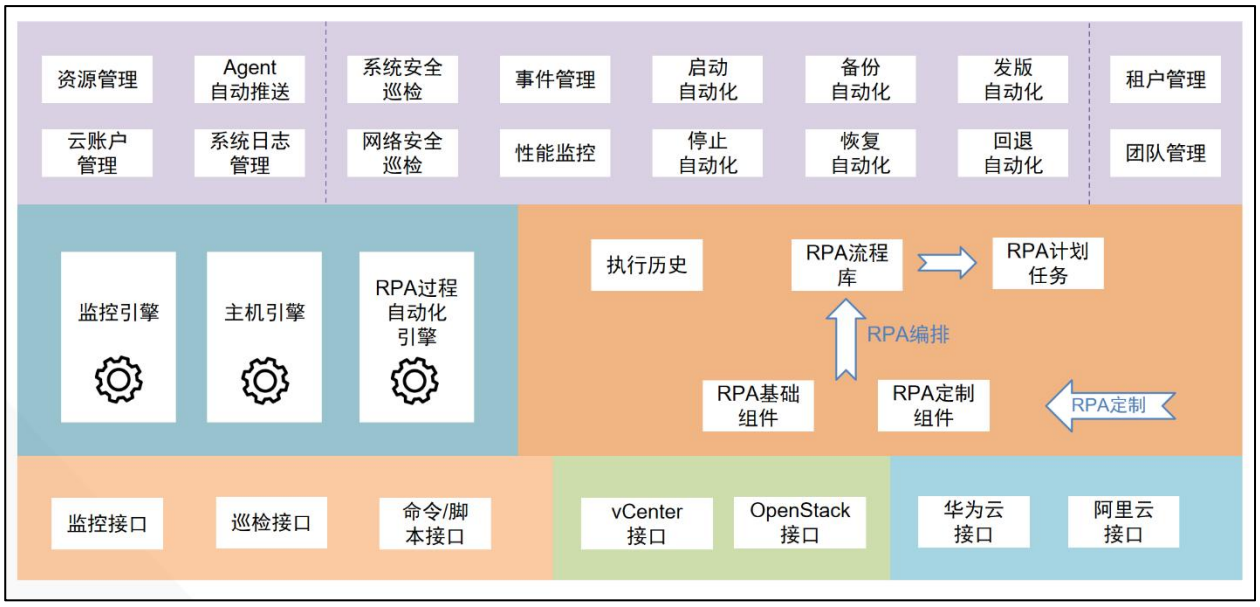

图 1 混合云自动化运维系统参考模型

6 功能要求

6.1 资源管理

6.1.1 资源导入

混合云自动化运维系统应支持导入一个云服务客户组织在不同云服务提供商的设备信息，且支持客户自定义导入区域。

6.1.2 设备监管

混合云自动化运维系统设备监管应具备以下功能：

a) 设备信息展示；
b) 设备性能监控；
c) 设备状态巡检；
d) 设备操作记录；
e) 设备控制。

6.2 事件管理

6.2.1 事件统计

系统应针对平台事项监控发出的告警数量进行实时统计，宜通过以下3种方式进行事件统计：

a) 按事件状态划分进行统计，事件状态一般分为已处理、未处理 2 种；
b) 按事件类型划分进行统计，事件类型包括但不限于 CPU、内存、磁盘、文件系统、网络接口、系统日志、应用、数据库等；
c) 按事件严重等级划分进行统计，事件严重等级一般分为严重、中等、一般 3 个等级。

6.2.2 事件列表

系统告警事件应以列表形式进行展现，支持用户进行事件搜索、查看、分类、处理等操作；事件列表宜以事件发生时间倒序进行排列。

6.3 自动巡检

6.3.1 巡检指标

6.3.1.1 系统安全

6.3.1.1.1 Windows 系统安全巡检

Windows系统的系统安全巡检项目宜包括但不限于以下内容：

a) 密码安全配置检查：密码失效时间、是否定期修改密码、密码复杂度等；
b) 匿名账户访问控制检查：是否开启匿名账户访问限制功能；
c) 安全审计检查：是否启用安全审计功能、审计是否覆盖到每个用户、是否对重要的用户行为和重要安全事件进行审计；
d) 未登录强制关机检查：是否启用未登录强制关机功能，Windows 登录屏幕上的“关机”命令是否可用；
e) 空闲会话断开检查：是否设置空闲会话自动断开功能；
f) 账户锁定策略检查：是否设置账户锁定策略、连续数次登录失败后账户是否自动锁定。

6.3.1.1.2 Linux 系统安全巡检

Linux系统的系统安全巡检项目宜包括但不限于以下内容：

a) Id 为 0 的非 root 账户：是否存在 Id 为 0 的非 root 帐户；
b) 空密码账户：是否存在空密码账户；
c) 异常登录检查：是否存在异常登录；

注：24小时内连续3次登录失败，将被归为异常登录。

d) SSH 密钥登录检查：是否使用 SSH 密钥登录并关闭密码登录；
e) 密码安全配置检查：密码失效时间、是否定期修改密码、密码复杂度；
f) 匿名访问服务检查：是否开启远程登陆服务和 ftp 匿名访问功能；
g) Web Server 权限检查：是否以 root 身份运行 apache/tomcat/nginx；
h) 临时目录权限检查：是否存在远程下载恶意程序到/tmp;/var/tmp;/dev/shm 等临时目录。

6.3.1.2 网络安全

网络安全检查主要对主机的网络安全配置进行检查，包括防火墙检查和危险端口开放检查，具体如下：

a) 防火墙检查：是否开启防火墙，防火墙关闭后将导致主机被暴露在网络上，易遭受网络攻击；
b) 危险端口开放检查：是否关闭非必要的端口服务，有效降低网络风险。

6.3.1.3 性能负载

性能负载检查主要应针对主机的CPU、内存资源的负载情况进行监控和分析。

6.3.2 巡检自定义

6.3.2.1 自定义检查

混合云自动化运维系统应支持用户自定义检查项，被忽略的检查项，在之后的巡检中将不会被检查，直到取消忽略。

6.3.2.2 白名单设置

混合云自动化运维系统应支持用户将巡检结果中的异常记录加入标记为正常情况，并加入白名单中。

6.3.3 巡检统计

6.3.3.1 巡检主机

以主机的巡检状态为统计维度，统计最近一次巡检中各种状态主机的数量。主机的巡检状态包括问题主机、正常主机和待检主机三种，具体如下：

a) 问题主机：指巡检结果中存在一个或多个问题的主机；
b) 正常主机：指巡检结果中不存在任何问题的主机；
c) 待检主机：指未进行过巡检的主机，一般是因为未安装代理程序，并且 CLI 登录不了主机。

6.3.3.2 巡检结果

以巡检结果中问题的严重程度为统计维度，统计最近一次巡检中各种严重程度问题的数量。问题的严重等级包括一般问题、严重问题和可优化问题三种，具体如下：

a) 一般问题：对系统影响较小，不会导致系统崩溃或性能严重下降；
b) 严重问题：对系统影响较大，可能导致系统崩溃、性能严重下降或者安全风险；
c) 可优化问题：对系统运行影响较小，但仍有改进空间的问题。

6.3.4 即时巡检

混合云自动化运维系统应支持用户即时发起巡检，便于用户主机配置或检查项做了相应的修改时，及时查看巡检结果。

6.3.5 服务报告

6.3.5.1 宜根据巡检结果，从资源概览、性能指标、故障告警、变更记录、运维活动、优化建议等方面的内容，形成服务报告。

6.3.5.2 服务报告应支持按照预设的周期（如每周、每月）自动生成，并通过多种方式（如邮件、文件共享等）发送给运维团队和相关人员。

6.4 流程自动化

6.4.1 流程管理

RPA流程管理功能宜支持以下操作：

a) 创建流程：用户根据不同业务场景需求，创建对应的流程，业务场景包括但不限于：启动、停止、发布、回退、备份和恢复、其他；
b) 删除流程：对已创建的流程进行删除操作；
c) 修改流程：对已创建的流程进行修改；
d) 查找流程：对目标流程进行检索，可查看流程的基本信息、执行记录及关联任务等内容；
e) 执行流程：选定已创建的特定流程自主发起执行，宜可查阅相关流程执行日志。

6.4.2 执行过程管理

RPA执行历史管理功能宜支持以下操作：

a) 搜索：在 RPA 主页内可进行搜索内容展示相应的数据；
b) 暂停执行：正在执行中的流程可在 RPA 执行历史页面进行暂停操作；
c) 恢复执行：已被暂停的流程可在 RPA 执行历史页面进行恢复操作；
d) 取消执行：RPA 执行历史页面可取消正在执行或已暂停的流程。

6.4.3 定制管理

RPA 具备定制功能，为用户提供提交定制流程开发需求的功能。

7 自动化运维场景

7.1 启动停止

混合云自动化运维系统启动停止应满足以下要求：

a) 能自动识别所有混合云环境中的云资源并进行统一管理，包括虚拟机、数据库、存储、负载均衡器等；

b) 提供一个按钮或者命令，实现一键启停目标云资源的操作，需手动去配置或者管理目标云资源；
c) 提供批量启停功能，支持对单个或多个资源进行启停操作，并提供附加选项，例如强制关闭、关机前保存数据、自动重启等；
d) 在执行启动停止之前，系统应自动检查目标云资源的运行状态，并给出反馈；
e) 当启动或者关闭云资源过程中发生异常，系统应能够自动捕获异常并进行处理；
f) 支持定时任务，可以设置定时启动或停止特定资源；
g) 针对不同云平台的特性和限制，提供相应的启停策略，并能够根据场景自动选择合适的启动策略。

7.2 备份恢复

混合云自动化运维系统备份恢复应满足以下要求：
a) 支持对云环境中的应用进行自动化备份，保证数据的安全性和可靠性；
b) 支持应用级别的备份，即可对应用程序、配置文件、数据文件等不同层次的应用数据进行备份；
c) 支持增量备份能力，对应用在每次备份的过程中，只备份增加的部分，以提高备份效率和减少备份成本；
d) 具备容错机制，能检测备份中可能存在的错误，例如数据损坏、备份完整性等，以避免影响备份恢复操作；
e) 支持热备份和冷备份，以覆盖多种应用场景下的备份需求；
f) 支持多种恢复策略，如全量恢复、增量恢复、点到点恢复等，以提高恢复效率和减少恢复成本；
g) 支持远程备份能力，可进行跨地域或多数据中心之间的备份，以实现数据资产管理的高可用性和灾备性。

7.3 发布回退

混合云自动化运维系统发布回退应满足以下要求：
a) 支持自动化的应用程序发布，包括上传、校验、部署、启动等自动化操作；
b) 支持应用程序的版本控制，能够对多个版本的程序进行管理，便于发布回退操作时的版本选择；
c) 支持快速回退操作，当一次发布出现问题时，能够快速回退到前一个版本，避免损失和影响；
d) 支持回退验证操作，即在进行回退操作之前，能够对回退涉及的资源、配置、数据进行验证，以确保回退的安全性和正确性；
e) 支持多环境的发布操作，包括测试环境、预发布环境、生产环境等，以适配不同阶段的部署需求；
f) 支持自动化测试，能够对发布的程序进行自动化测试，比如功能测试、性能测试、稳定性测试等操作，保证发布效果的正确性和稳定性。

7.4 故障处置

混合云自动化运维系统故障处置应满足以下要求：
a) 故障诊断：能够对多种故障类型进行检测，包括软件、硬件、网络等故障类型，用户可通过系统提供的一键排查按钮对故障进行快速定位并排查故障；
b) 自动化故障处置：能够识别并自动进行故障处置，包括故障隔离、自动修复、自动故障转移等；
c) 故障告警：当系统检测到无法自动化处置的异常或故障时，通过多种通知方式（如邮件、短信、手机推送等）及时通知运维团队进行处理；
d) 人工干预：能够远程对故障设备进行管理和操作，快速解决故障；
e) 故障记录：记录各种故障的发生情况、故障处置情况，便于故障原因分析和问题追溯。

7.5 灾备切换

混合云自动化运维系统灾备切换应满足以下要求：

a) 自动化灾备切换：能够及时备份数据并存储在安全的地方，当主系统出现故障时，自动切换到备用系统，数据可通过备用系统立即恢复，防止业务中断；
b) 灾备演练：测试灾难恢复计划的可行性和可靠性；
c) 远程控制：用户不在当前位置时，可以随时通过系统远程控制备用系统，并保留所有的数据和应用程序。

7.6 日常变更

混合云自动化运维系统日常变更应满足以下要求：

a) 具有对多种设备、多种操作系统、多种应用程序、多种存储设备自动化执行各种日常变更操作：
   1) 跨网络变更：支持自动化配置 IP 地址、网关等参数的变更操作；
   2) 跨系统变更：支持各种操作系统的变更，包括 Windows、Linux、Unix 等操作系统，可以自动执行系统软件的升级、配置修改、应用程序安装等操作；
   3) 跨应用变更：支持应用程序及常见应用软件的部署、配置变更、软件升级、数据迁移等操作。

注：常见应用软件包括：Web服务器、应用服务器、数据库等。

   4) 跨存储变更：支持存储设备的升级、扩容、配置修改、数据备份等操作。

注：常见的存储设备包括：硬盘阵列、网络存储等。

b) 支持用户向系统提交变更请求，包括变更类型、影响范围、变更内容等信息；
c) 支持自动化执行变更操作，并提供变更执行结果的记录和监控；
d) 支持在变更执行出现异常情况时，快速回退到变更前的状态，保证业务不受影响；
e) 具备变更日志的记录、查询、统计等功能，以便跟踪变更历史和排查问题；
f) 具备变更操作的通知和协作功能，确保所有相关人员能够及时获得变更相关信息。

8 安全要求

8.1 概述

8.1.1 混合云自动化运维系统应满足 YD/T 4059—2022 中第 5 章、第 6 章的要求。

8.1.2 混合云自动化运维系统数据安全应满足 GB/T 37973、GB/T 39477、GB/Z 38649 的要求。

8.2 权限管理

混合云自动化运维系统权限管理应满足以下要求：

a) 支持用户类型的设置，如管理人员、运维人员等；
b) 支持根据用户类型设置不同的权限，如浏览信息的范围、操作的范围等；
c) 支持对混合云自动化运维系统的用户进行身份鉴别、证书鉴别等。

8.3 网络安全

网络安全管理应符合GB/T 22239中的规定，且满足以下要求：

a) 不同用户虚拟网络之间进行隔离；
b) 建立安全防护机制，对网络进行 24 小时监控，能检测到对客户发起的网络攻击行为，及时封禁攻击来源和记录攻击的类型、时间、流量并进行告警。

8.4 数据安全

混合云自动化运维系统数据安全应满足以下要求：

a) 支持信息完整性校验机制确保数据传输的完整性；
b) 支持密码技术对于鉴别信息、重要数据等敏感信息进行加密，确保数据传输保密性；
c) 采用时间戳机制等技术保证数据传输的可用性。

9 运维管理

9.1 概述

混合云自动化运维系统运维管理应满足GB/T 28827.1的要求。

9.2 风险评估

安全风险评估应满足GB/T 20984和GB/Z 24364的要求。

9.3 应急响应

应急响应应满足以下要求：

a) 建立网络与信息安全事件信息接收机制；
b) 在统一的应急预案框架下制定不同安全事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
c) 应急预案符合 GB/T 24363 的要求；
d) 制定事件报告和处置管理制度，明确事件类型，规定事件的现场处理、事件报告和后期恢复的管理职责；
e) 在事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。

参 考 文 献

[1] GB/T 42136—2022　智能制造　远程运维系统通用要求
[2] 柴娟伟，RPA（流程自动化机器人）入门，电子工业出版社，2021.