安骑士运维指南

中建三局信息科技有限公司

2024 年 5 月

法律声明

天工云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过天工云网站或天工云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为天工云的保密信息，您应当严格遵守保密义务；未经天工云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经天工云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。天工云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在天工云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过天工云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用天工云产品及服务的参考性指引，天工云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。天工云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但天工云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，天工云不承担任何法律责任。在任何情况下，天工云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使天工云已被告知该等损失的可能性）。

5. 天工云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由天工云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经天工云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表天工云网站、产品程序或内容。此外，未经天工云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制天工云的名称（包括但不限于单独为或以组合形式包含“天工云”、“TianGongYun”等天工云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别天工云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与天工云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

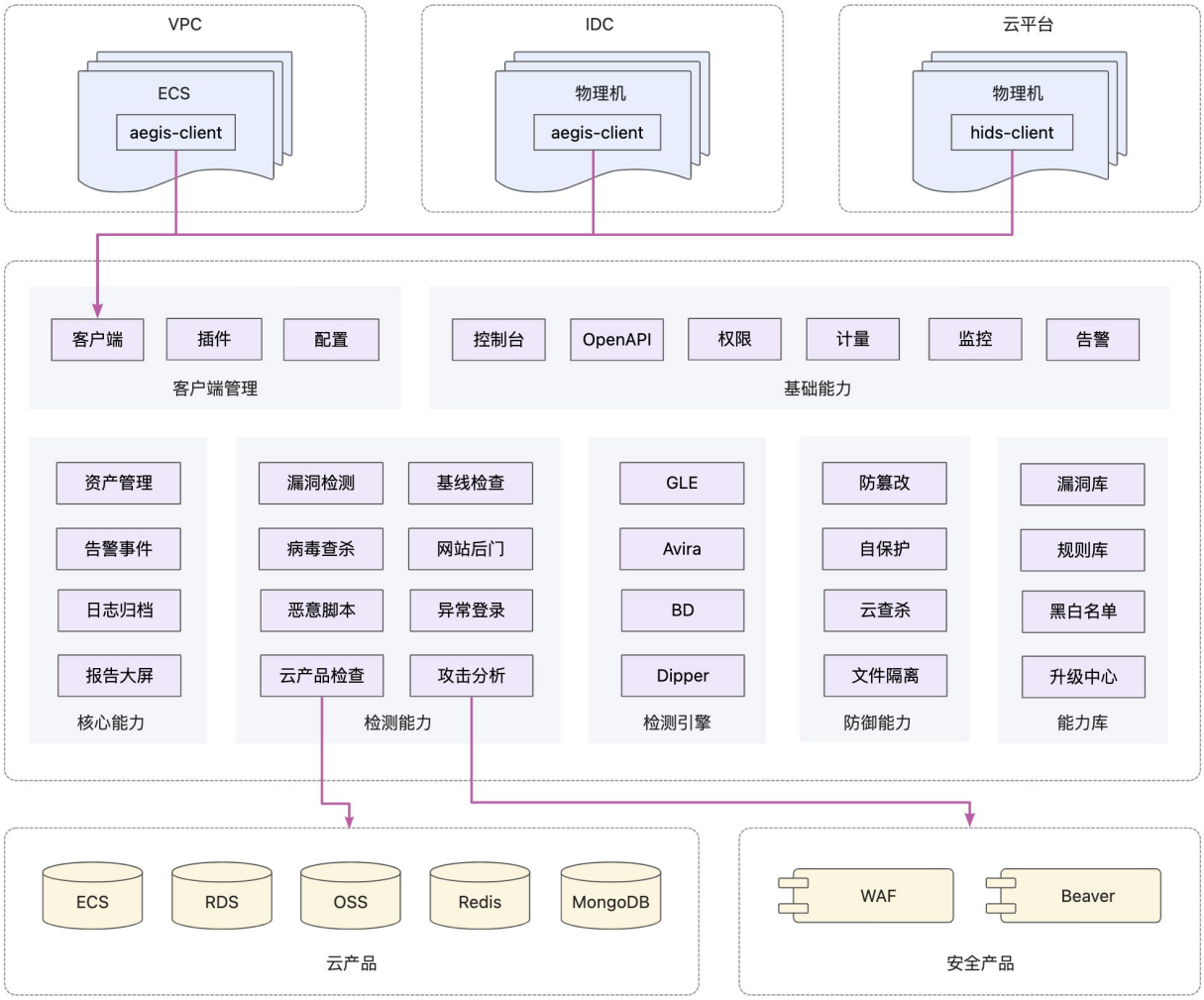
1.安骑士运维手册

1.1. 产品介绍

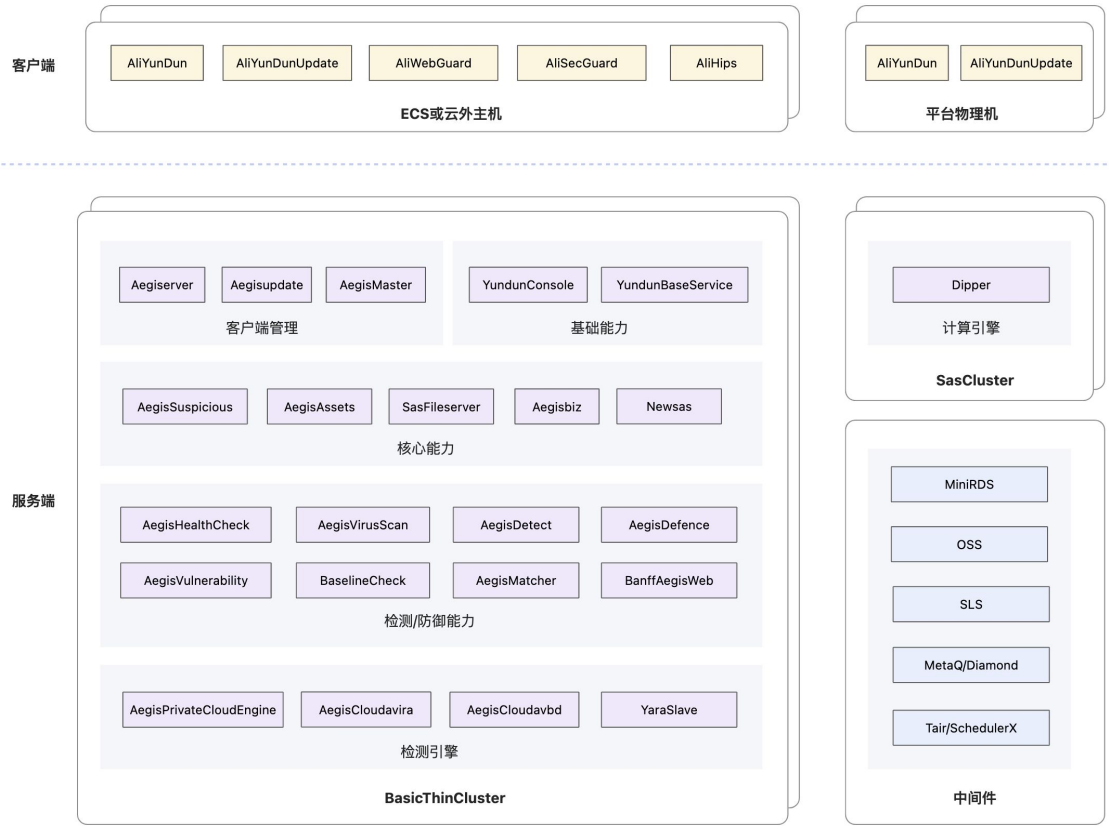
安骑士（主机安全+态势感知）是一款集持续监测、深度防御、全面分析、快速响应能力于一体的云上安全管理平台。

安骑士基于云原生架构优势，提供云上资产管理、配置核查、主动防御、安全加固、云产品配置评估和安全可视化等能力，可有效发现和阻止病毒传播、黑客攻击、勒索加密、漏洞利用等风险事件，实现一体化、自动化的安全运营闭环，保护云内云外的主机、容器、虚拟机等工作负载安全性，同时满足监管合规要求。

- 安骑士在服务器系统内核层面通过Agent插件实现云上文件和进程行为的全局监控和实时分析，对海量病毒样本持久化攻击方式的自动化分析，有效绕过顽固木马和恶意程序的反查杀能力；还可以基于程序行为分析，挖掘出黑名单未能辨识的恶意威胁，实现主动拦截；其云端病毒库实时更新，集成了国内外主流杀毒引擎、天工云自研沙箱和机器学习引擎等前沿技术，可以避免因病毒库更新不及时而造成的损失，
- 防护策略和数据源自于多年的积累，是天工云上多达百万级的用户，每天面临多达几十万次的各种攻击。天工云安全团队充分利用了这些安全攻防的数据积累，每天对公共云上10多TB的安全数据进行分析，形成恶意IP库、恶意行为库、恶意样本库、安全漏洞库等基础安全能力，并及时应用到态势感知的各个防护模块中，提升防护能力，为用户带来更好的安全保障。



1.2. 部署架构



安骑士是典型的C/S架构，包括服务端和客户端。服务端负责资产、检测、防御等核心能力，客户端负责实时监测主机状态、执行检测脚本、实时防御等。

服务端

服务端主要分成以下几个模块：

- 基础能力：云盾通用能力，提供控制台和OpenAPI。
- 客户端管理：负责管理客户端连接、配置、规则、补丁包等。
- 核心能力：包括资产、告警、日志、文件采集、安全报告等。
- 检测防御：包括漏洞、基线、文件、网络、进程的检测防御能力。
- 检测引擎：包括商业病毒检测引擎、病毒检测引擎、大数据计算引擎。

服务端每个应用的具体职责：

模块	职责
YundunConsole	安骑士控制台，为安全管理员提供了统一的管理界面。
YundunBaseService	安骑士API网关，将主机安全能力开放给三方开发者。

Aegiserver	客户端连接管理、配置下发、消息转发等。
Aegisupdate	客户单升级、规则/脚本/补丁等文件拉取。
AegisMaster	客户端配置、插件管理。
AegisSuspicious	入侵告警事件、应用白名单。
AegisAssets	资产指纹、日志归档
Aegisbiz	负责API转发到各个模块
NewSas	安全报告。
SasFileserver	文件采集。
AegisHealthCheck	主机基线检查。
AegisVirusScan	文件检测。
AegisDetect	旧版文件检测，当前仅保留文件白名单管理，其他流程全部迁移到AegisVirusScan。
AegisDefence	防篡改。
AegisVulnerability	漏洞检测。
BaselineCheck	云产品配置检查。
AegisMatcher	云查杀。
BanffAegisWeb	命令下发通道。
AegisPrivateCloudEngine	GLE引擎，病毒检测引擎。
YaraSlave	Yara二进制检测引擎，商业病毒检测引擎。

AegisCloudavira	小红伞二进制引擎，商业病毒检测引擎。
AegisCloudavbd	BD二进制检测引擎，商业病毒检测引擎。
Dipper	大数据计算引擎，入侵检测。

客户端

客户端包括以下模块，每个模块对应一个主机进程。

名称	说明
AliYunDun	核心进程，用于与云安全中心服务器建立连接。
AliYunDunUpdate	核心进程，用于定期检测云安全中心Agent是否需要升级。
AliWebGuard	网页防篡改进程。
AliSecGuard	客户端自保护进程。
AliHips	病毒木马防护进程。

> 说明
>
> 参考文档：*客户端支持的操作系统*

1.3. 核心模块

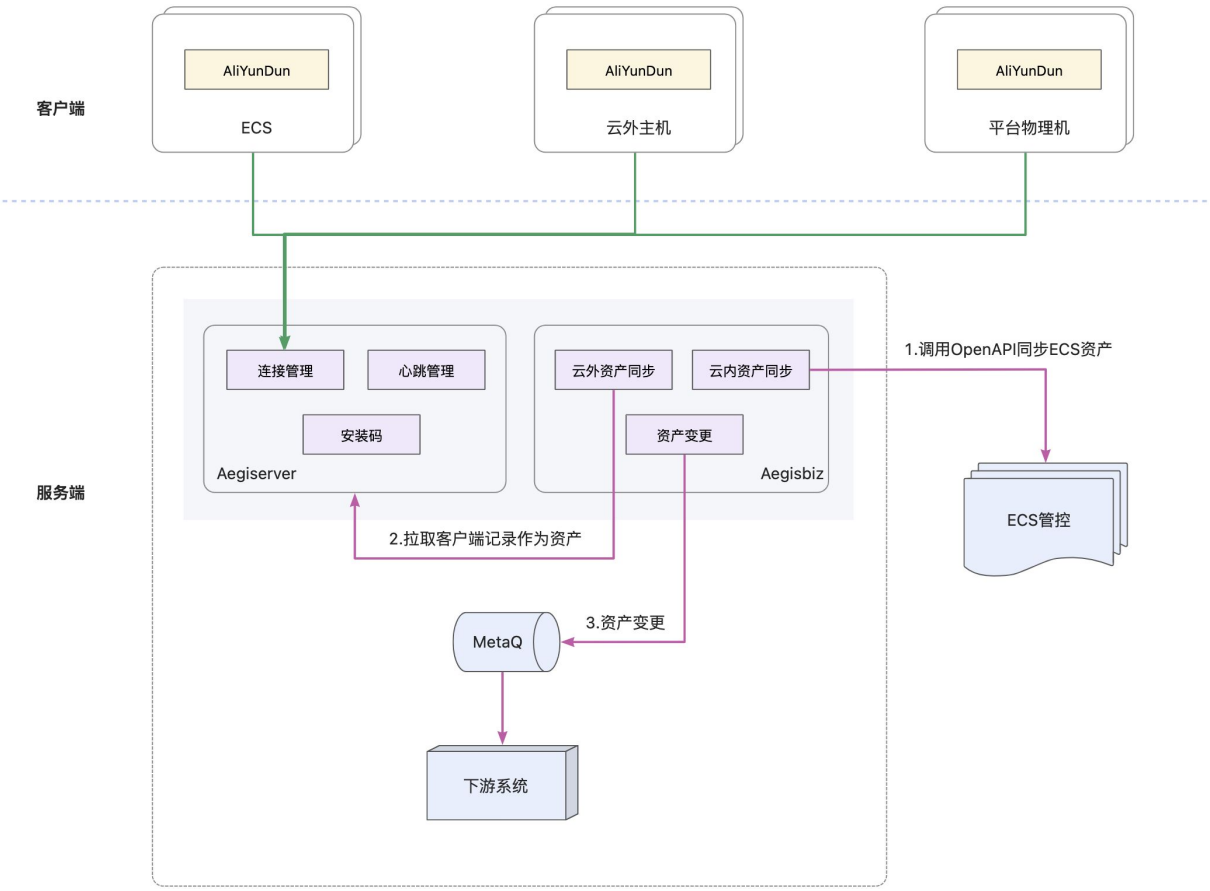
资产同步

通过资产中心的总览页面全面了解云安全中心已防护的资产的安全状态和统计信息。

资产数据来源包括：ECS、平台物理机、云外主机

- ECS资产同步：通过OpenAPI同步ECS资产，OpenAPI返回的是全量ECS列表。
- 平台物理机：当前是将连接到Aegiserver的平台侧物理机作为平台物理机资产，有一部分未安装客户端的平台物理机无法识别到，后续版本会通过Tianji Api获取到全量的物理机列表。
- 云外主机：云外主机资产同步与平台物理机类似，也是将连接到Aegiserver的云外主机作为资产，此外云外主机还需通过安装码识别到租户归属关系。

资产同步后，会将资产变更消息发给MetaQ，下游系统会订阅该消息进行相应的逻辑处理。



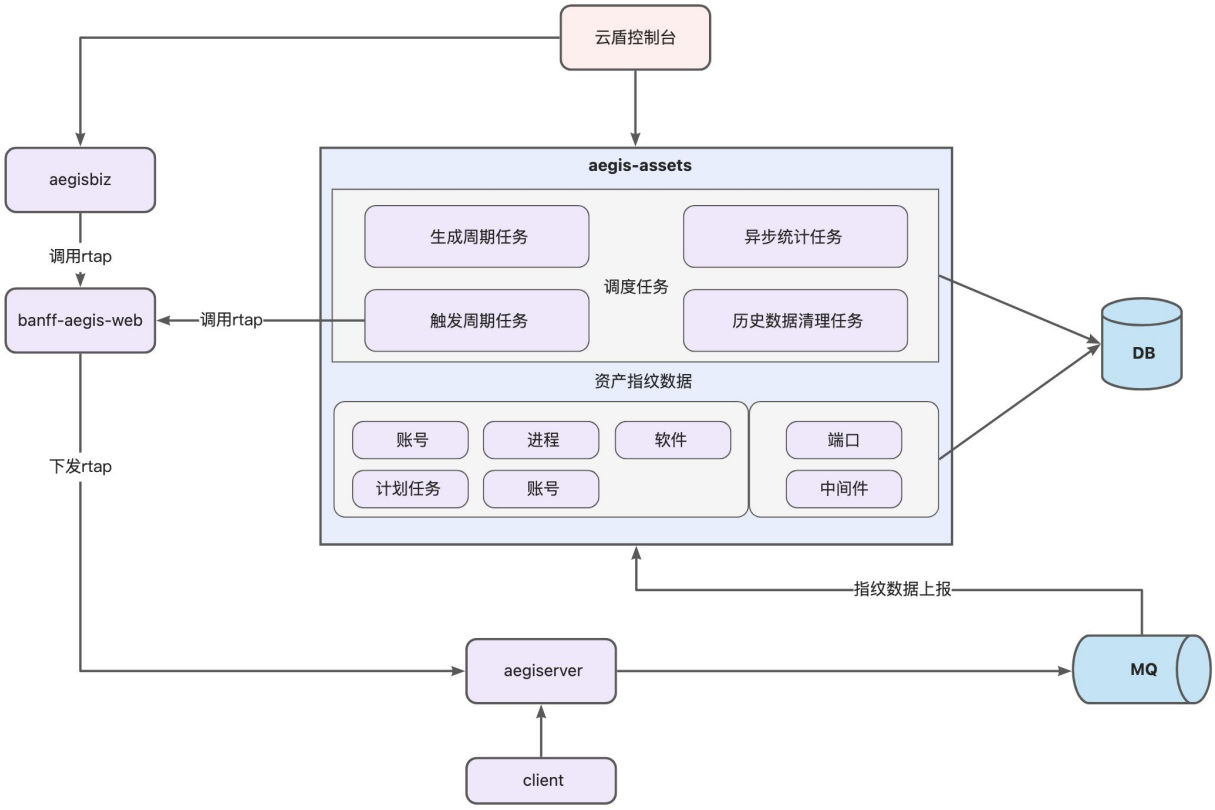
主机指纹

资产指纹周期性采集服务器的账号、端口、进程、中间件、软件、计划任务、启动项等数据。

采集方式：

- **周期性自动采集**
- **采集单个或多个资产最新指纹数据**

> **说明**
>
> 周期采集取决于页面上的周期扫描配置，关闭后则无法采集，其中如果需要使用云外暴露检查功能，则必须开启中间件采集。
>
> **周期性自动采集时间：**不是在同一时间点采集全部资产的指纹数据，如：扫描周期为一天，则实际会把采集任务打散到这一天的各个时间段。



云外暴露检查

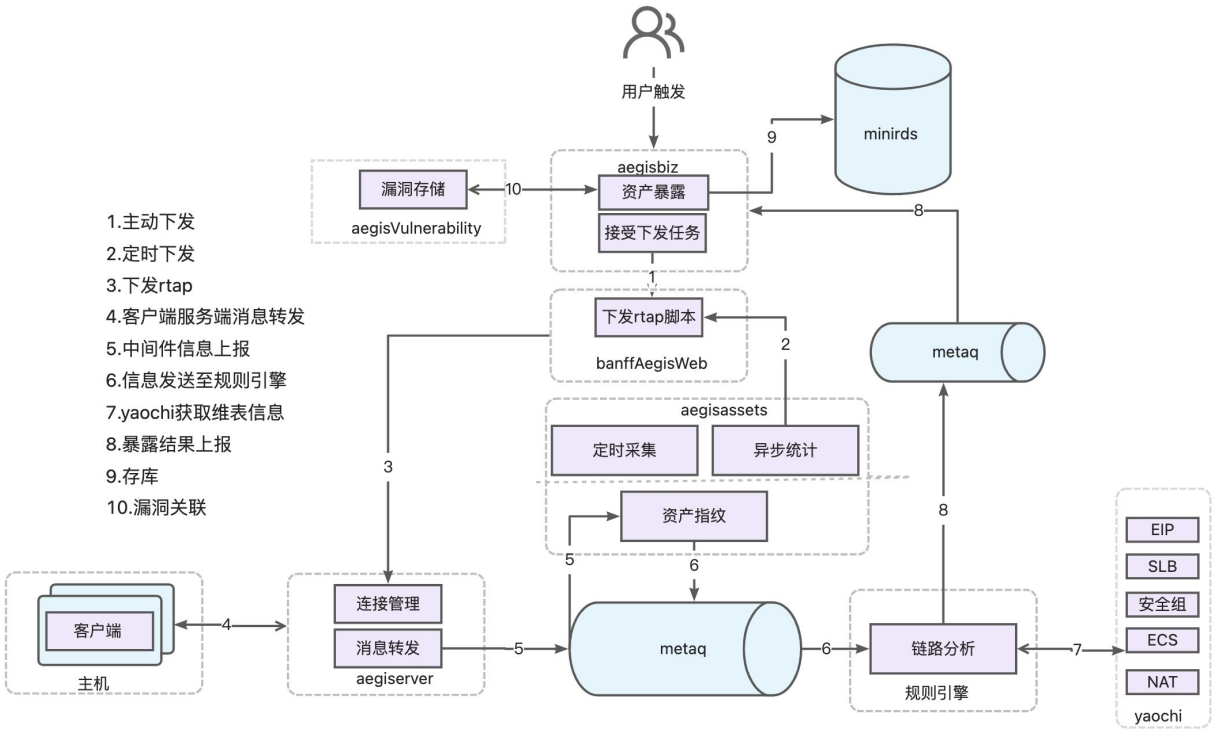
云外暴露检查功能依赖于资产指纹的调查中采集的中间件信息

云外暴露检查支持自动分析您的ECS服务器在互联网上的暴露情况，可视化呈现ECS与互联网的通信链路，并集中展示您暴露在公网的ECS的漏洞信息，帮助您快速定位您资产在互联网上的异常暴露情况并提供相应漏洞的修复建议。

统计数据说明：

统计项名称	说明
暴露资产/公网IP数	暴露在互联网上的服务器总数量和IP地址总数量。
网关资产	暴露在互联网上的网关资产（负载均衡、NAT网关）总数量。单击相应数值打开网关资产面板，可查看网关资产的列表。在网关资产面板，单击网关资产名称可跳转至对应资产详情页面。
暴露端口	暴露在互联网上的端口总数量。单击相应数值打开暴露端口面板，可查看暴露端口的列表。在暴露端口面板，单击暴露端口名称查看存在该暴露端口的资产列表。
暴露组件	暴露在互联网上的您服务器的系统组件（例如OpenSSL、OpenSSH）总数量。单击相应数值打开暴露组件面板，可查看暴露组件的列表。在暴露组件面板，单击暴露组件名称查看存在该暴露组件的资产列表。

可被利用漏洞	暴露在互联网上可被黑客利用的漏洞总数量及高危、中危、低危漏洞数量。单击表示高危、中危、低危漏洞数量的数字可跳转至漏洞修复页面。不同类型的漏洞使用不同颜色表示： • 高危：红色。此类漏洞会对您的资产安全较大的威胁，建议您重点关注并及时修复。 • 中危：橙色。此类漏洞对您的资产会产生一定的危害，建议您及时修复。 • 低危：灰色。此类漏洞对您的资产安全危害较小，您可以延后修复。



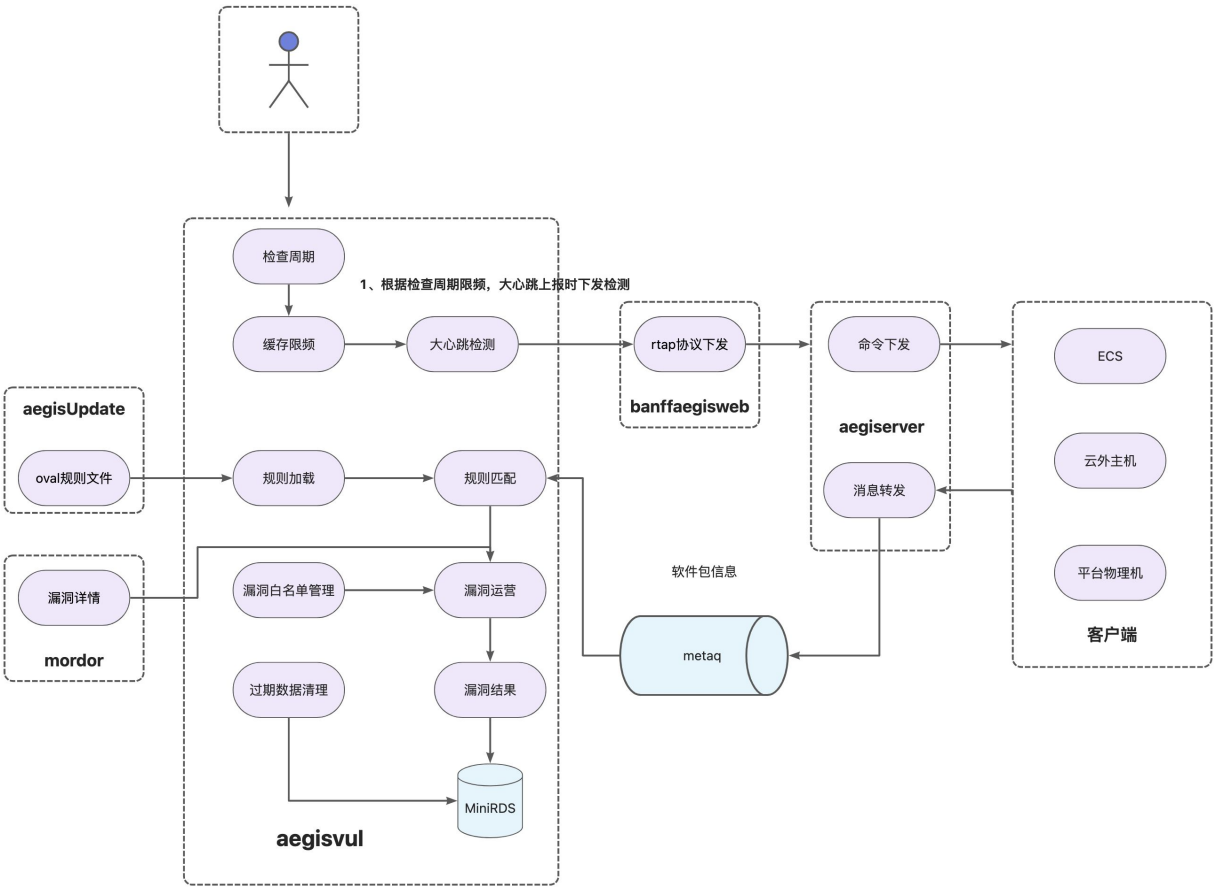
漏洞管理

安骑士支持对常见漏洞类型进行检测和修复，包括Linux漏洞、Windows漏洞、CMS漏洞、应用漏洞、应急漏洞。

Linux漏洞检测流程

1、客户端段上报心跳时根据扫描周期定时下发扫描。

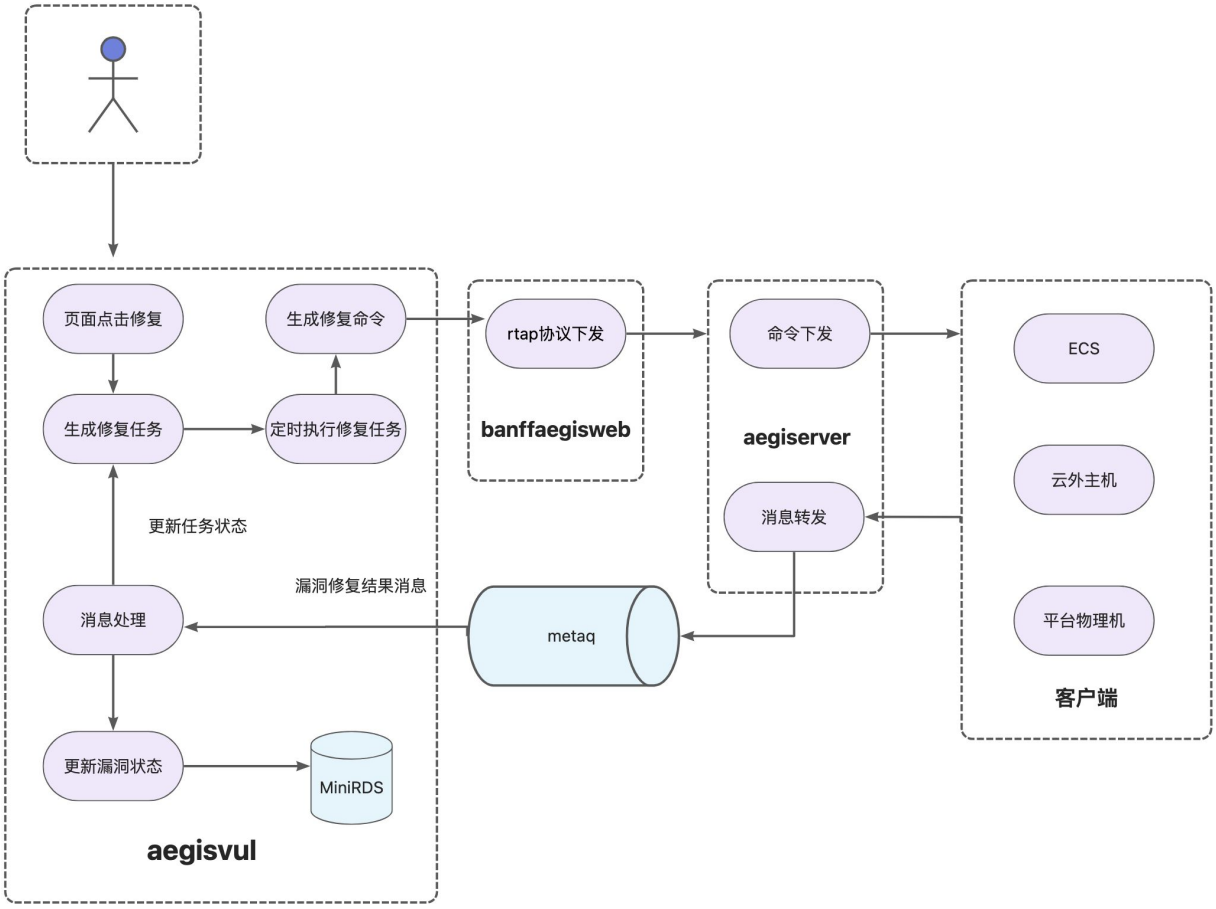
2、客户端上报软件包信息后，根据oval规则匹配漏洞，补充漏洞详情，经历漏洞白名单，漏洞运营过滤后入库。



Linux漏洞修复流程

1、手动修复会生成修复任务，定时执行下发

2、系统内核内漏洞不支持修复

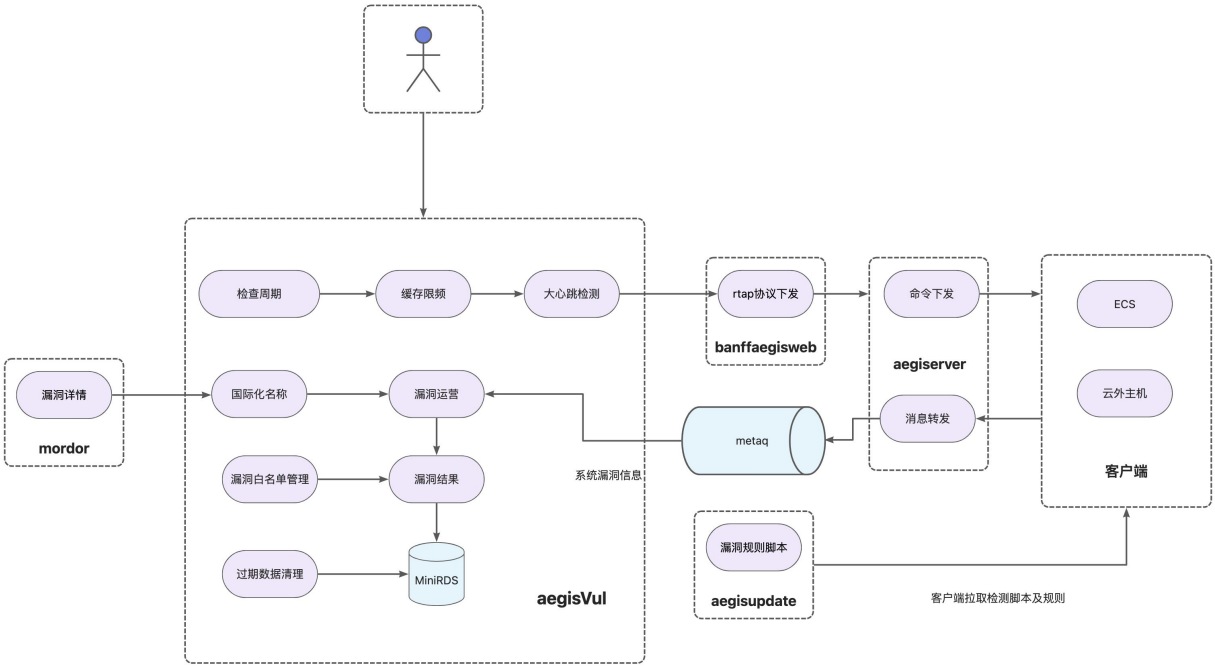


Windows漏洞检测流程

1、每48小时会在大心跳上报时下发漏洞检测命令

2、客户端接收命令后，从aegisupdate中更新检测脚本及规则后执行检测，将执行结果上报

3、服务端接收后，会根据漏洞详情获取漏洞名称，经漏洞运营，漏洞白名单后入库。

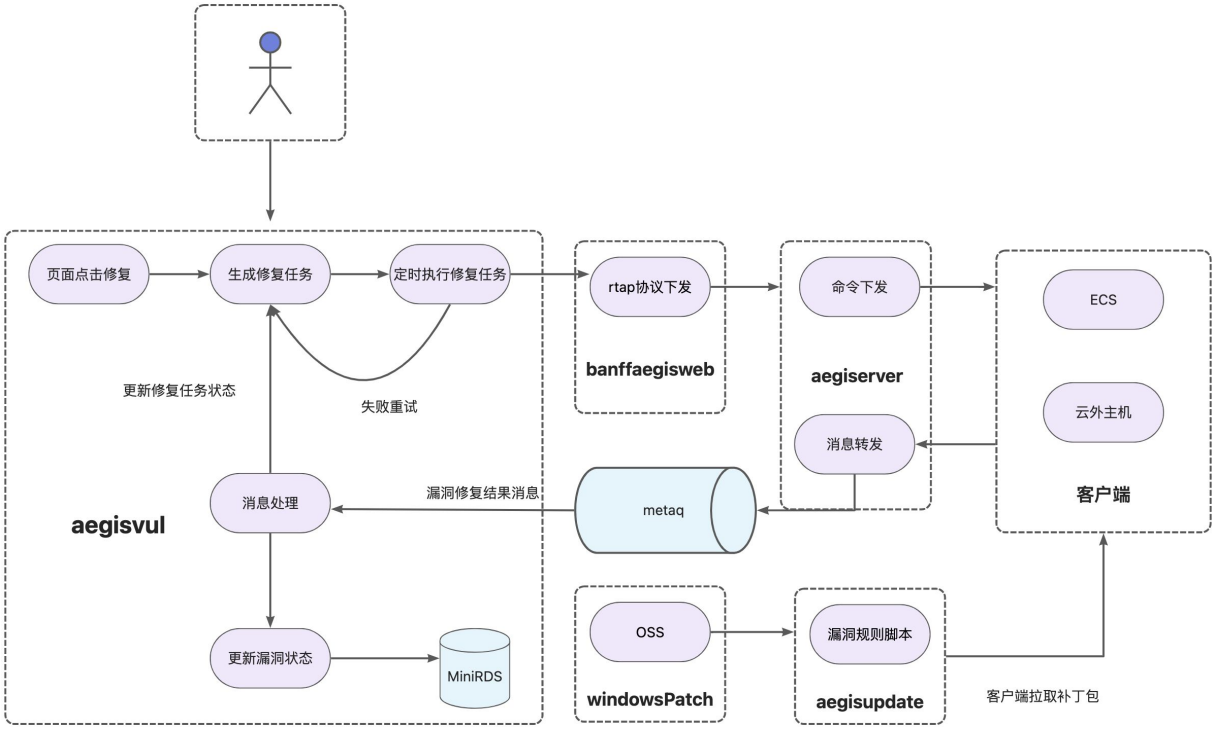


Windows漏洞修复流程

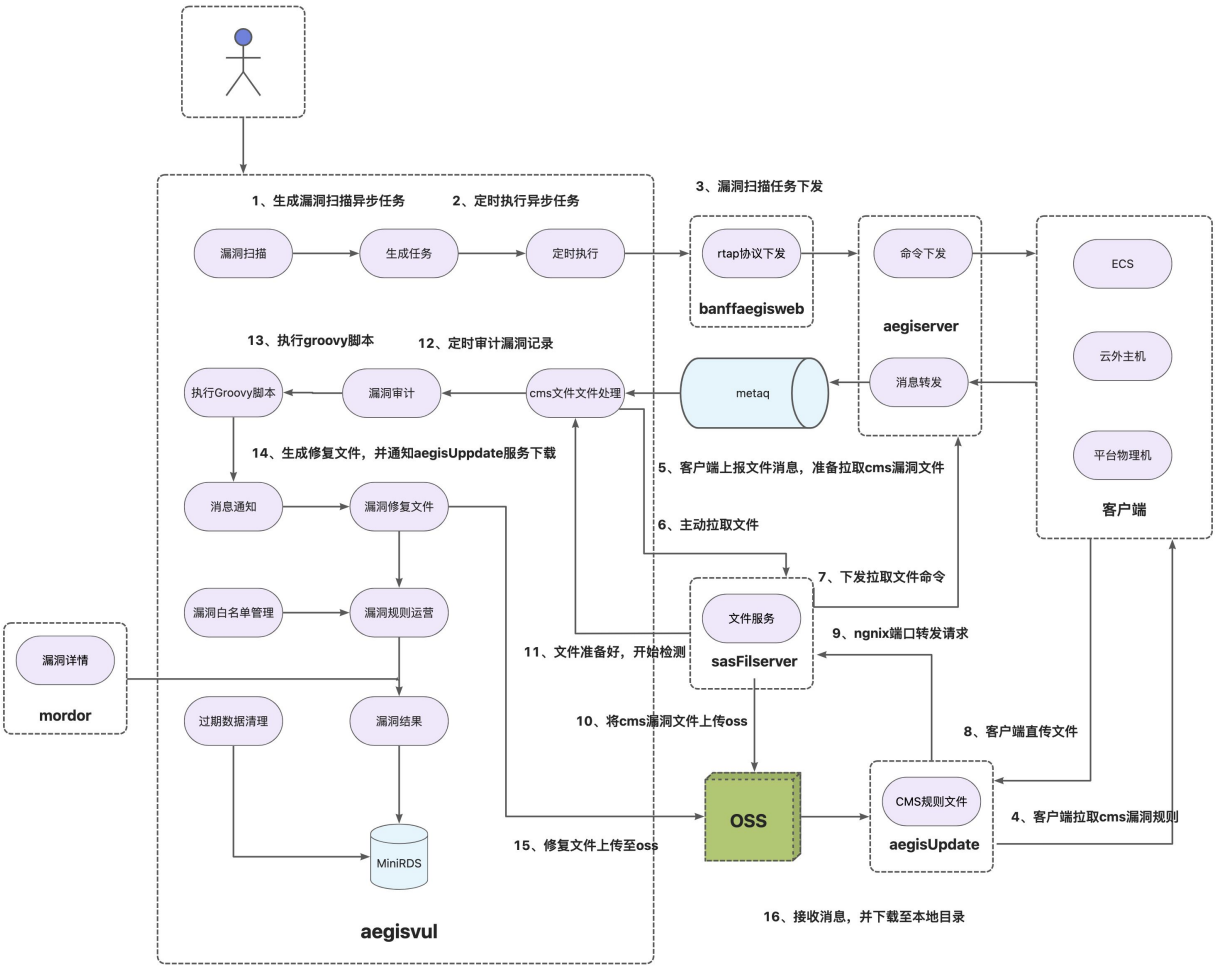
1、点击修复会生成修复任务，通过定时任务下发修复命令

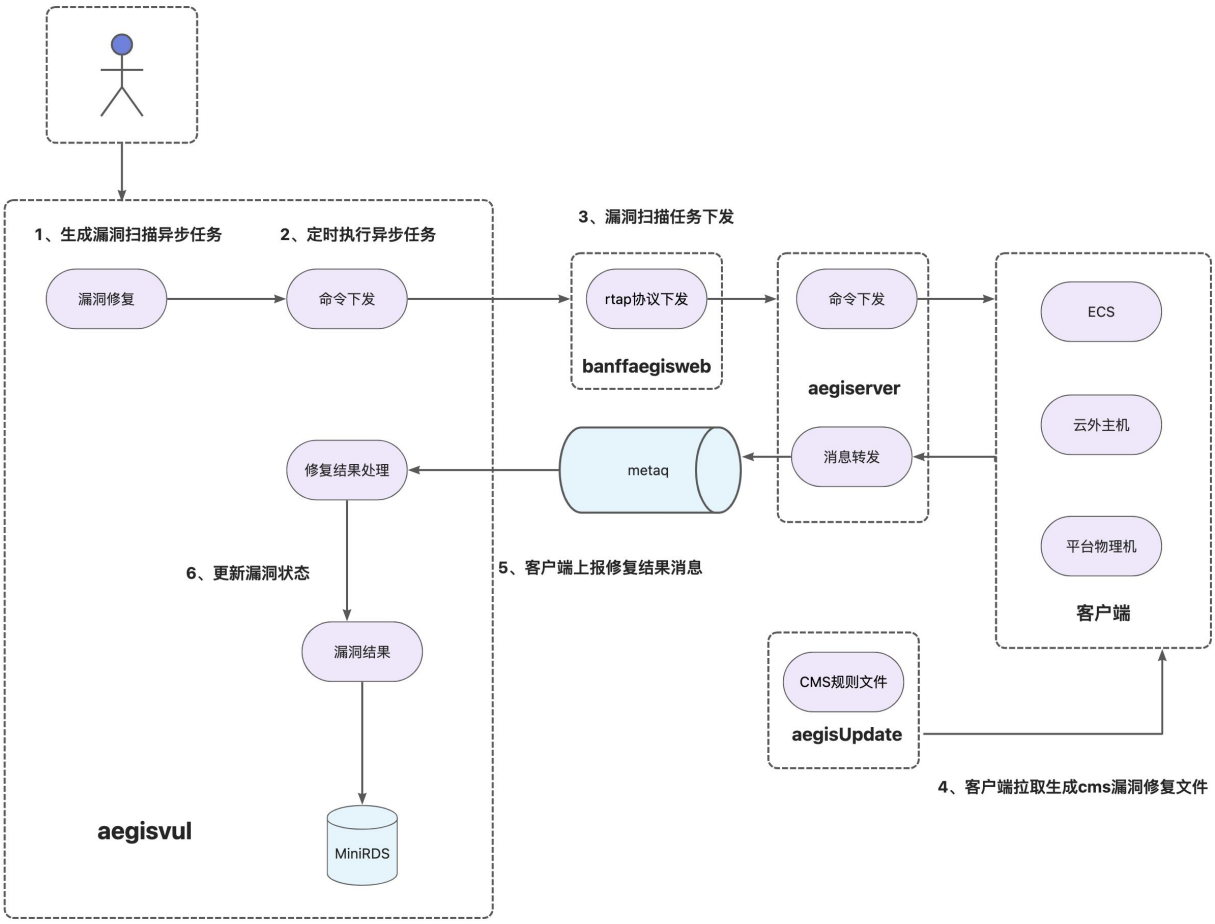
2、当修复失败后，会定时检测修复结果，当修复失败时，默认会失败重试修复2次。

3、aegisUpdate服务启动时从windowsPath服务的OSS中获取系统补丁包文件，客户端从aegisUpdate容器中下载补丁并修复。



CMS漏洞检测及修复流程


1、生成漏洞扫描异步任务
2、定时执行异步任务
漏洞扫描
生成任务
定时执行
3、漏洞扫描任务下发
rtap协议下发
banffaegisweb
命令下发
aegiserver
ECS
云外主机
平台物理机
客户端
13、执行groovy脚本
12、定时审计漏洞记录
执行Groovy脚本
漏洞审计
cms文件文件处理
metaq
消息转发
14、生成修复文件，并通知aegisUppdate服务下载
5、客户端上报文件消息，准备拉取cms漏洞文件
消息通知
漏洞修复文件
6、主动拉取文件
7、下发拉取文件命令
漏洞白名单管理
漏洞规则运营
文件服务
sasFilserver
9、ngnix端口转发请求
11、文件准备好，开始检测
漏洞详情
mordor
过期数据清理
漏洞结果
10、将cms漏洞文件上传oss
8、客户端直传文件
OSS
CMS规则文件
aegisUpdate
4、客户端拉取cms漏洞规则
15、修复文件上传至oss
MiniRDS
aegisvul
16、接收消息，并下载至本地目录



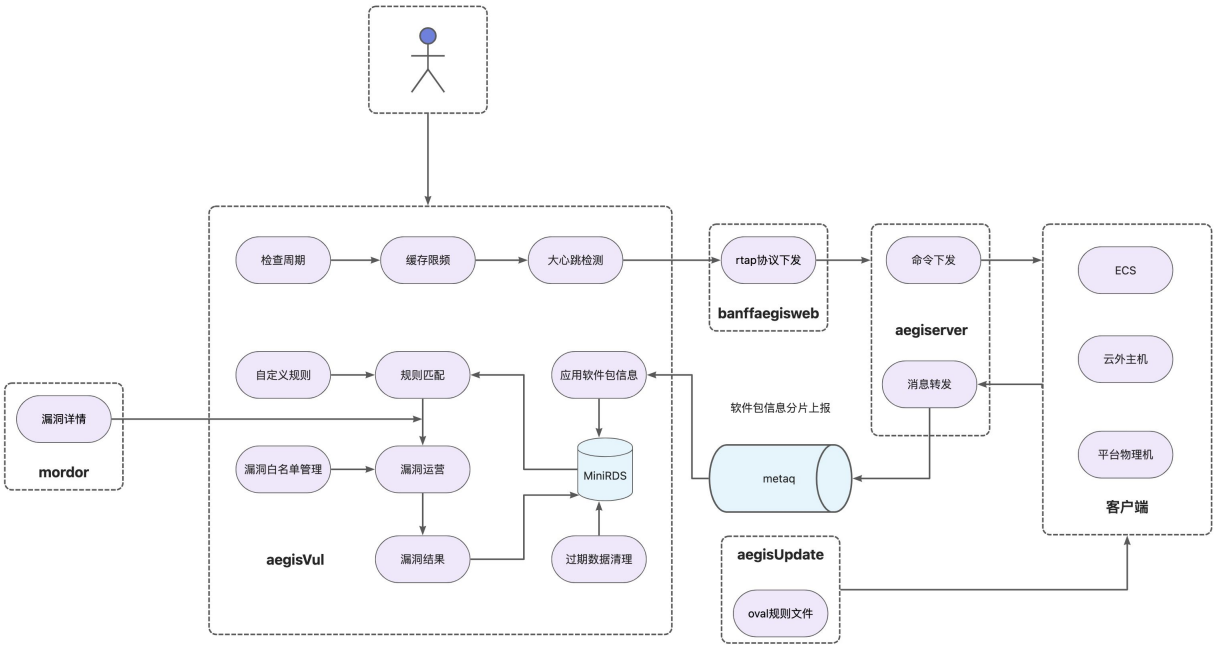
应用漏洞检测流程

1、每48小时会在大心跳上报时下发漏洞检测命令

2、客户端从aegisUpdate中拉取脚本并执行

3、客户端分片上报运行时软件包信息

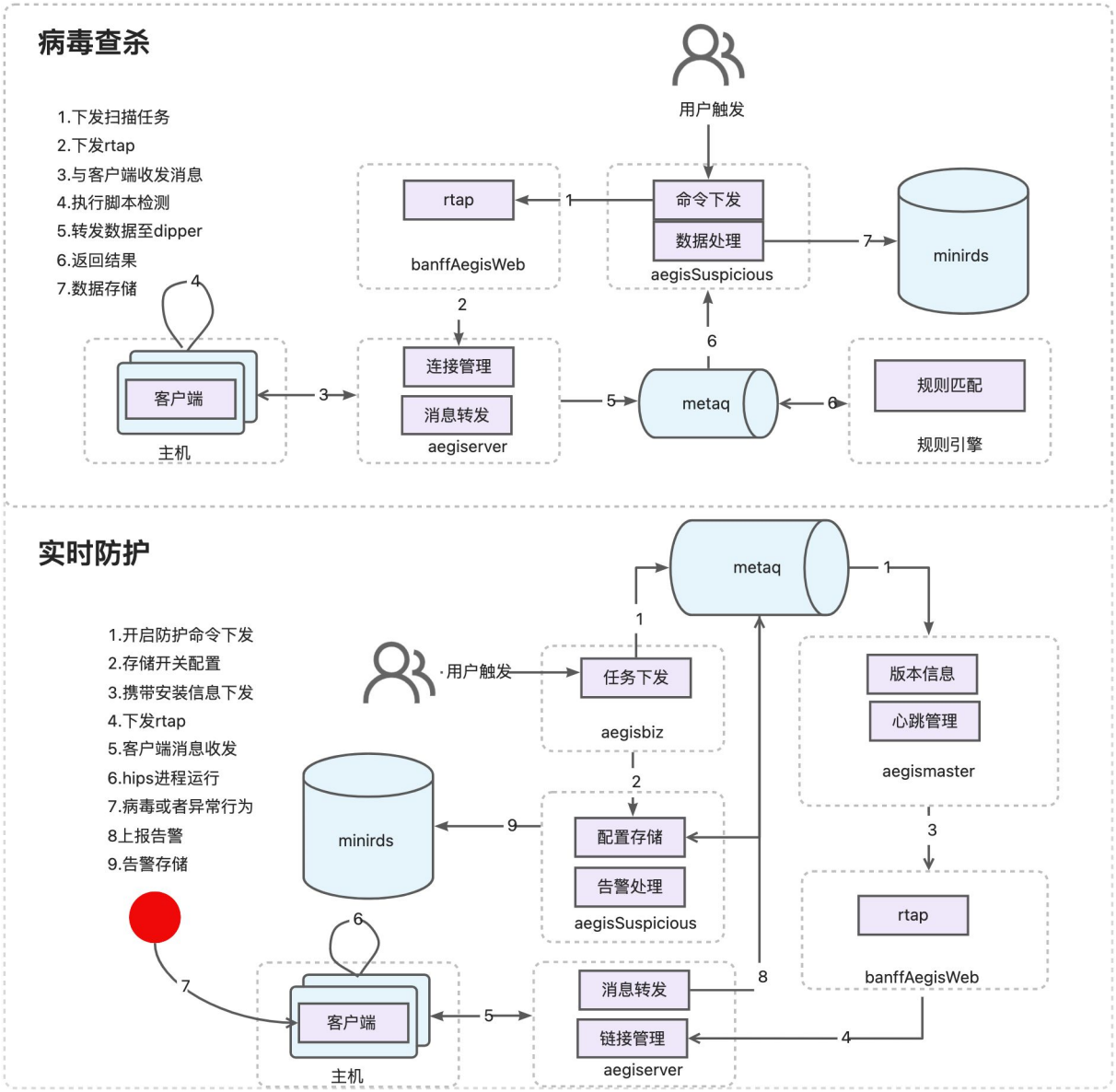
4、软件包信息上报完成后，统一进行规则匹配（自定义规则），并修改历史漏洞状态



病毒查杀

勒索病毒、挖矿程序等持久化、顽固型病毒已经成为网络安全最大的威胁。病毒防御功能针对此类病毒提供扫描、告警、深度查杀的能力，可有效预防此类病毒入侵您的服务器。

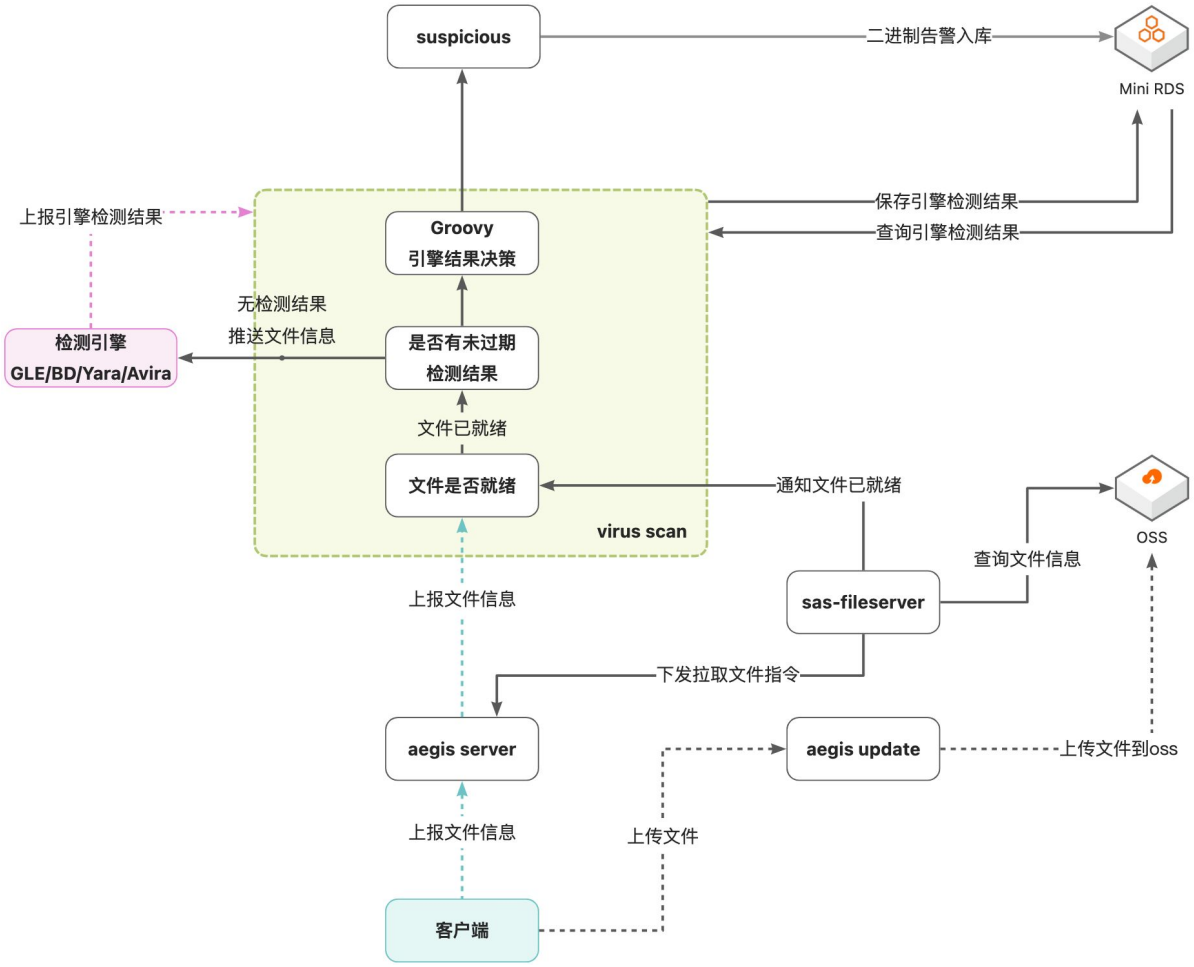
病毒防御功能针对勒索病毒、挖矿程序等顽固性病毒，对安骑士所有服务器提供深度扫描服务。安骑士支持立即扫描和周期性扫描病毒。



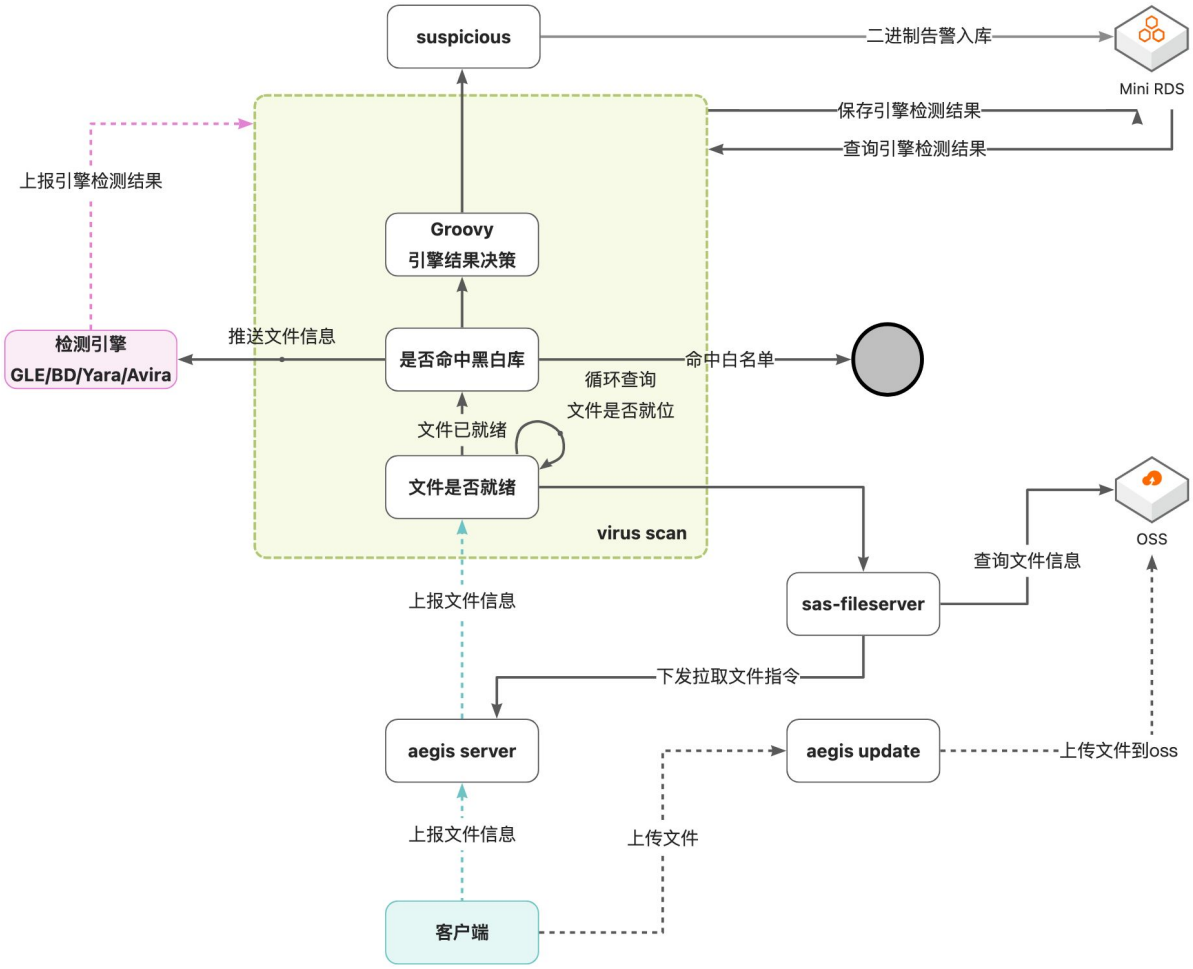
文件检测防御

二进制文件检测防御

业务流程图

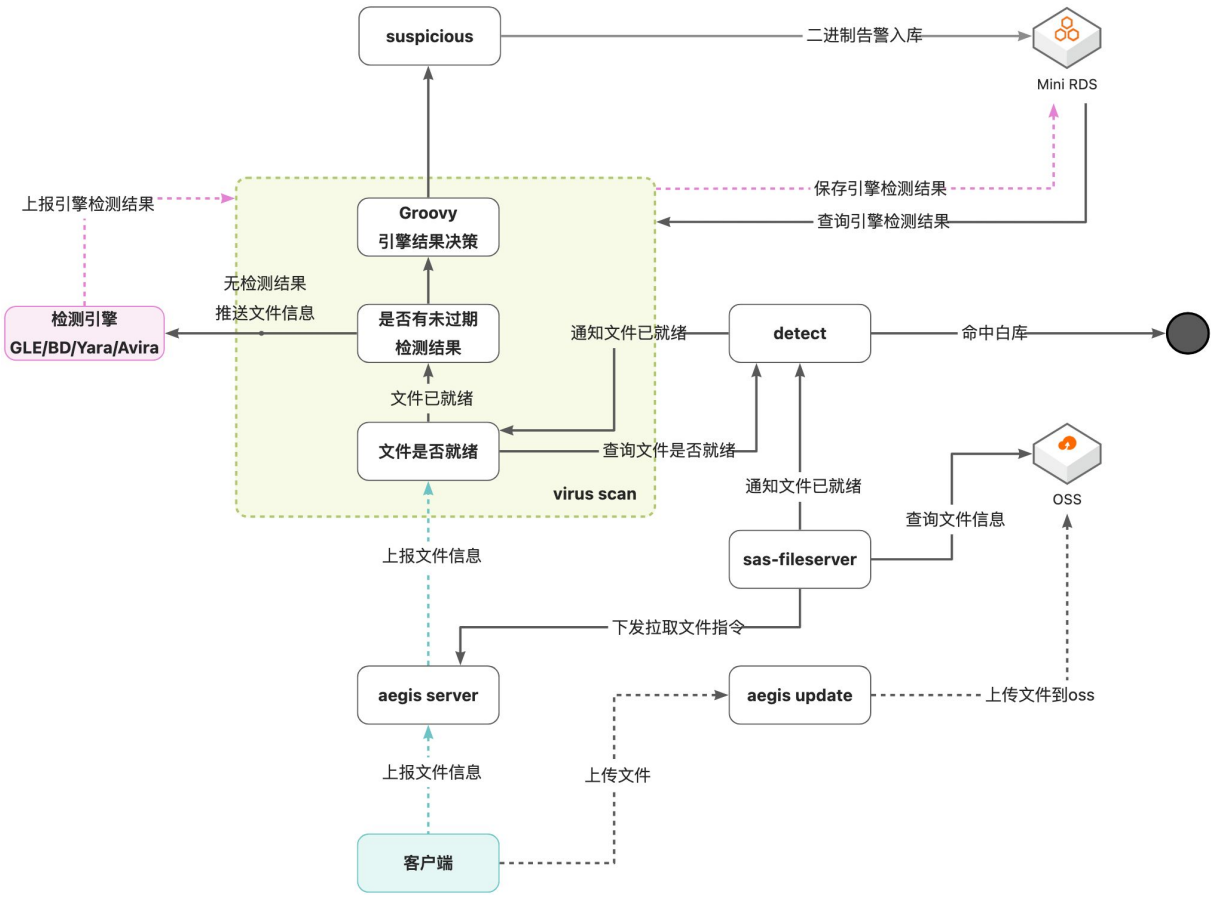

suspicious
二进制告警入库
Mini RDS
上报引擎检测结果
Groovy
引擎结果决策
保存引擎检测结果
查询引擎检测结果
无检测结果
推送文件信息
检测引擎
GLE/BD/Yara/Avira
是否有未过期
检测结果
文件已就绪
文件是否就绪
通知文件已就绪
virus scan
OSS
查询文件信息
上报文件信息
sas-fileserver
下发拉取文件指令
aegis server
aegis update
上传文件到oss
上报文件信息
上传文件
客户端

恶意脚本检测防御

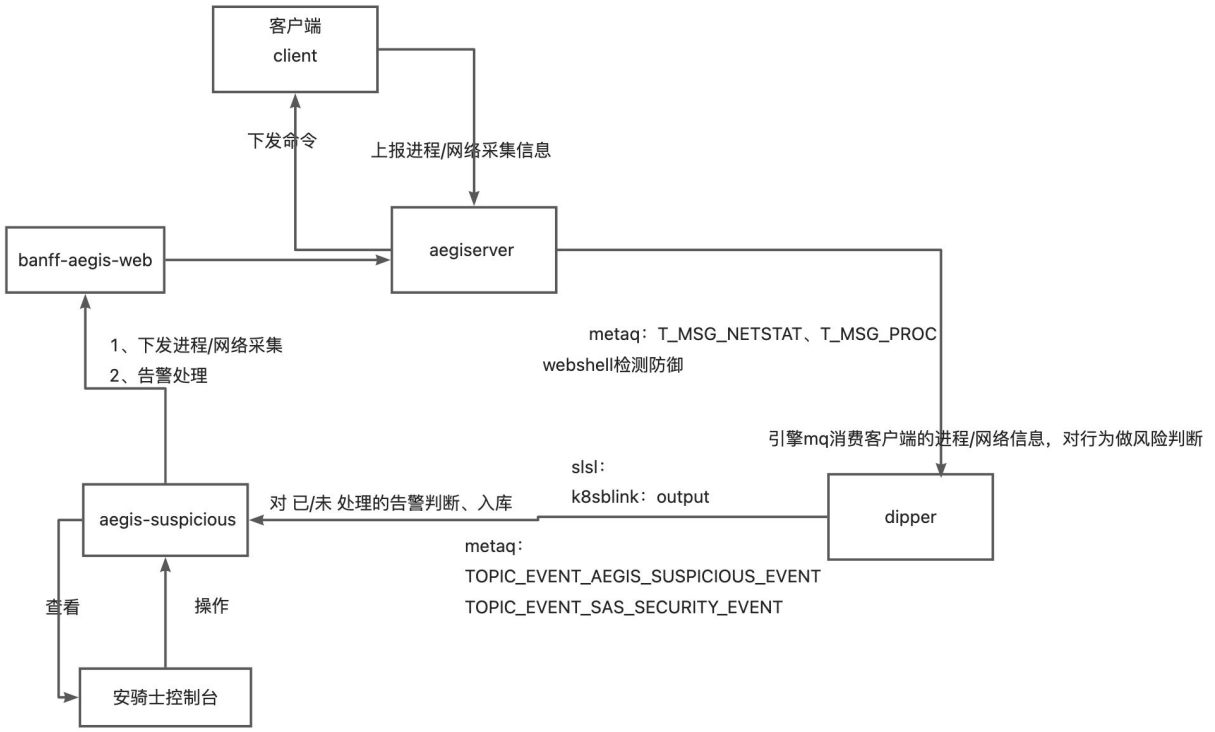


webshell检测防御

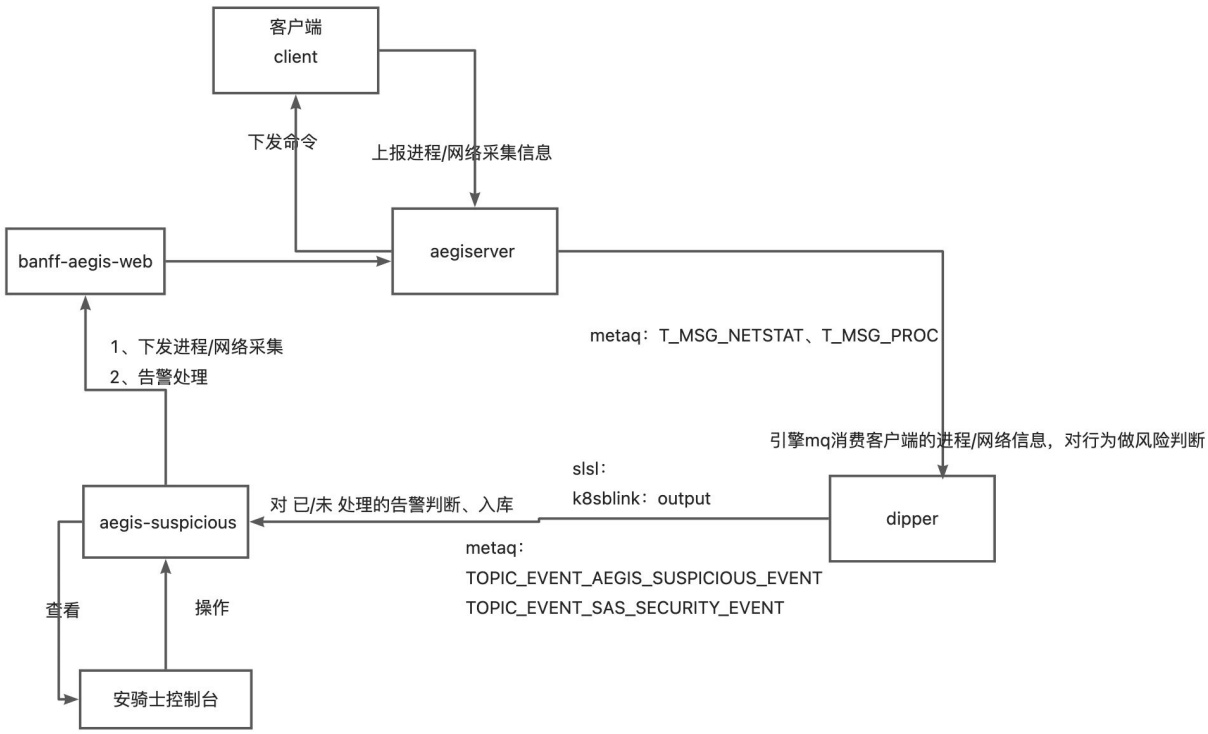
业务流程图



进程检测防御

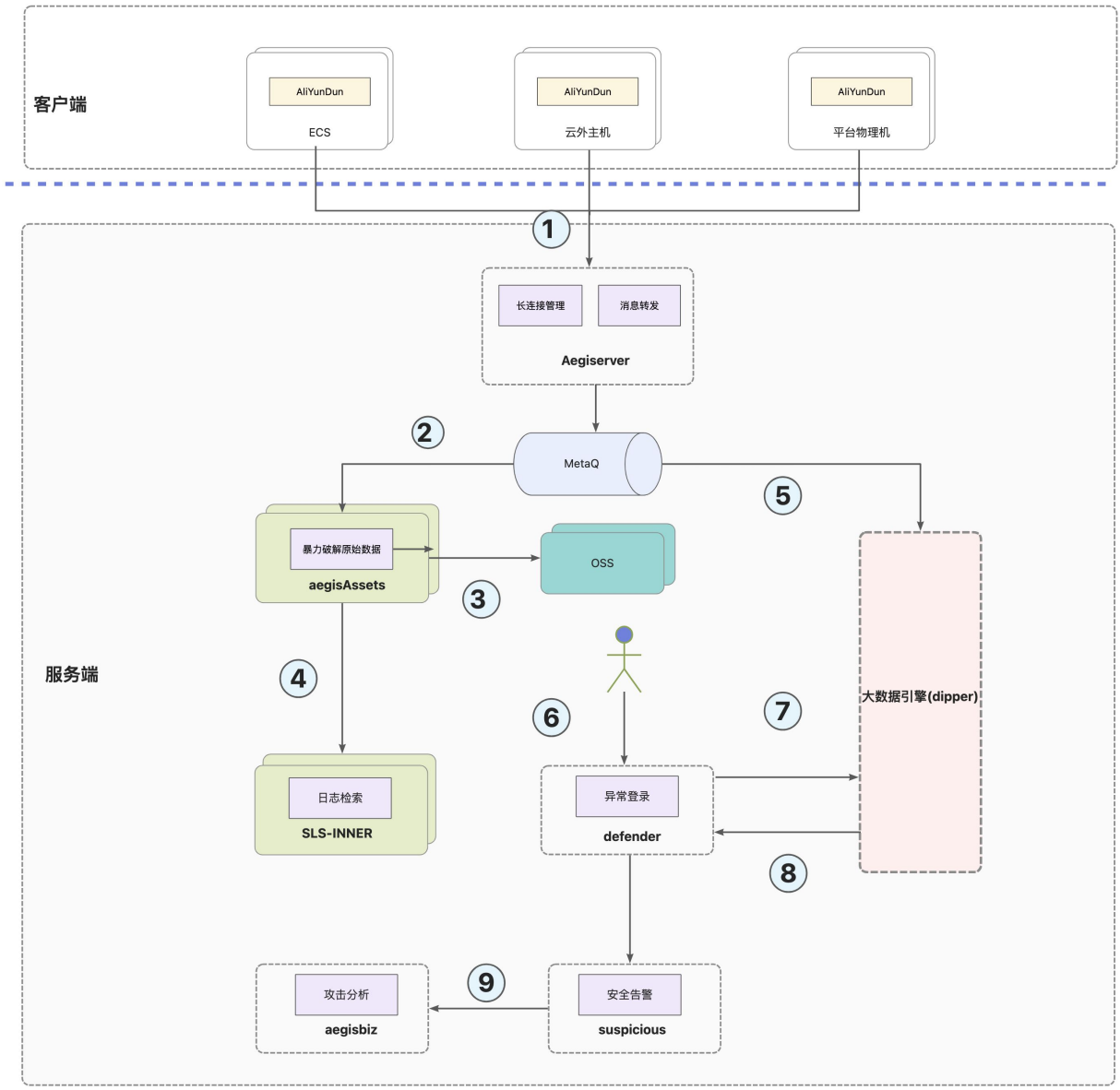


网络检测防御



暴力破解

安骑士支持配置自定义暴力破解防御规则。配置防暴力破解规则后，登录服务器时，在某个时间范围内登录服务器的失败次数超过限定次数将被禁止登录一段时间。防暴力破解功能，可有效防止您服务器账号的密码被暴力破解。



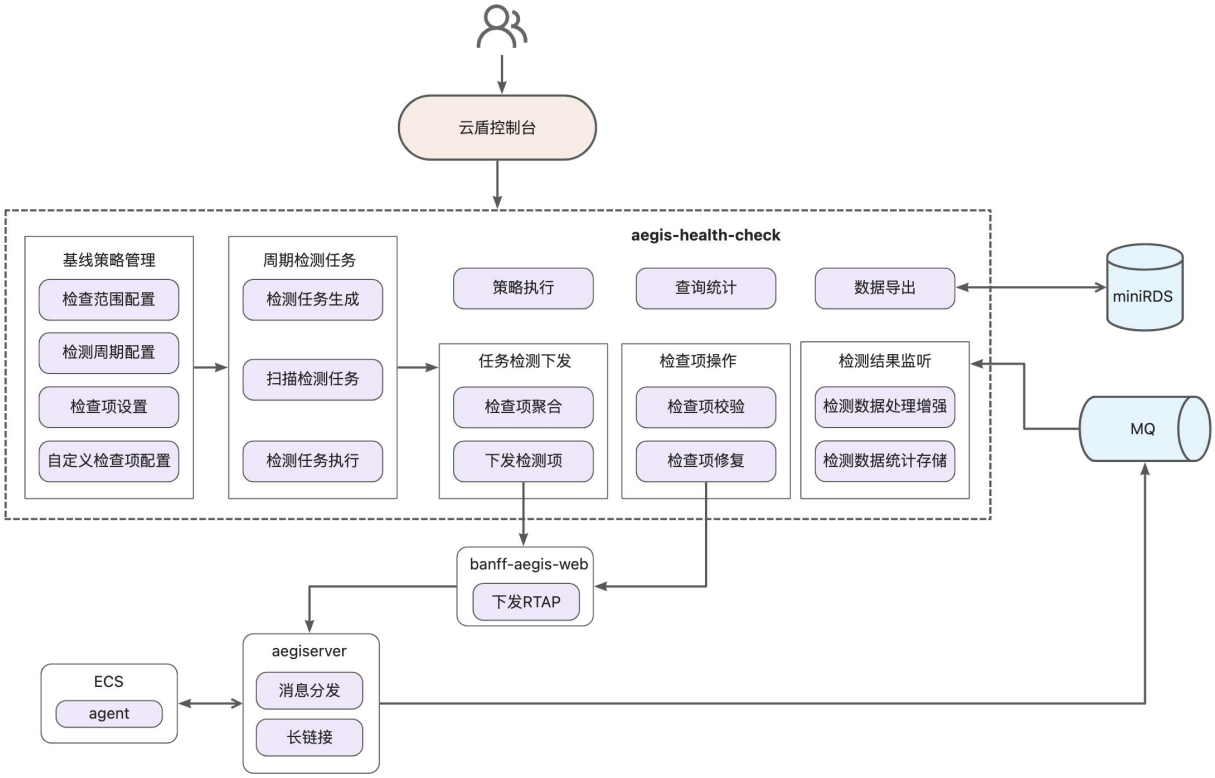
说明

1. 客户端上报原始主机登录日志
2. aegisAssets消费原始主机登录日志消息
3. 主机登录日志归档至OSS,满足等保要求（185天）
4. 主机登录日志接入sls-inner，提供日志检索能力
5. 大数据引擎消费主机登录日志
6. 客户在控制台设置暴力破解相关规则
7. 大数据引擎定去获取客户设置的暴力破解规则（每小时获取一次）
8. 大数据引擎根据规则，消费主机登录日志后，产出暴力破解数据结果（只发送未加白的告警数据）
9. suspicious服务消费告警数据后，发送主机暴力破解数据至攻击分析模块（告警已加白直接发送，告警未加白，消费入库后再发送攻击分析）。

基线检查

基线检查功能针对服务器操作系统、数据库、软件和容器的配置进行安全检测，并提供检测结果说明和加固建议。

基线指操作系统、数据库及中间件的安全实践及合规检查的配置红线，包括弱口令、账号权限、身份鉴别、密码策略、访问控制、安全审计和入侵防范等安全配置检查。云安全中心的安全基线支持弱口令、未授权访问、历史漏洞和配置红线的立体巡检，合规基线支持等保合规和CIS标准。安全基线与合规基线均已覆盖常用的30多个系统版本和10多个数据库及中间件，可以满足企业多种合规需求。



攻击分析

攻击分析对资产受到的攻击行为进行分析，并展示攻击相关的数据。

攻击分析的数据来源：

- 安骑士：主机层攻击数据，主要包括暴力破解数据，客户端上报登录日志给Aegiserver，Dipper分析登录日志产出暴力破解数据，Aegisbiz消费暴力破解数据，按资产、类型、小时维度归类后存储到MiniRDS。
- WAF：应用层攻击数据，Aegisbiz消费暴力破解数据，按资产、类型、小时维度归类后存储到MiniRDS。
- NDR：网络层攻击数据，Aegisbiz消费暴力破解数据，按资产、类型、小时维度归类后存储到MiniRDS。

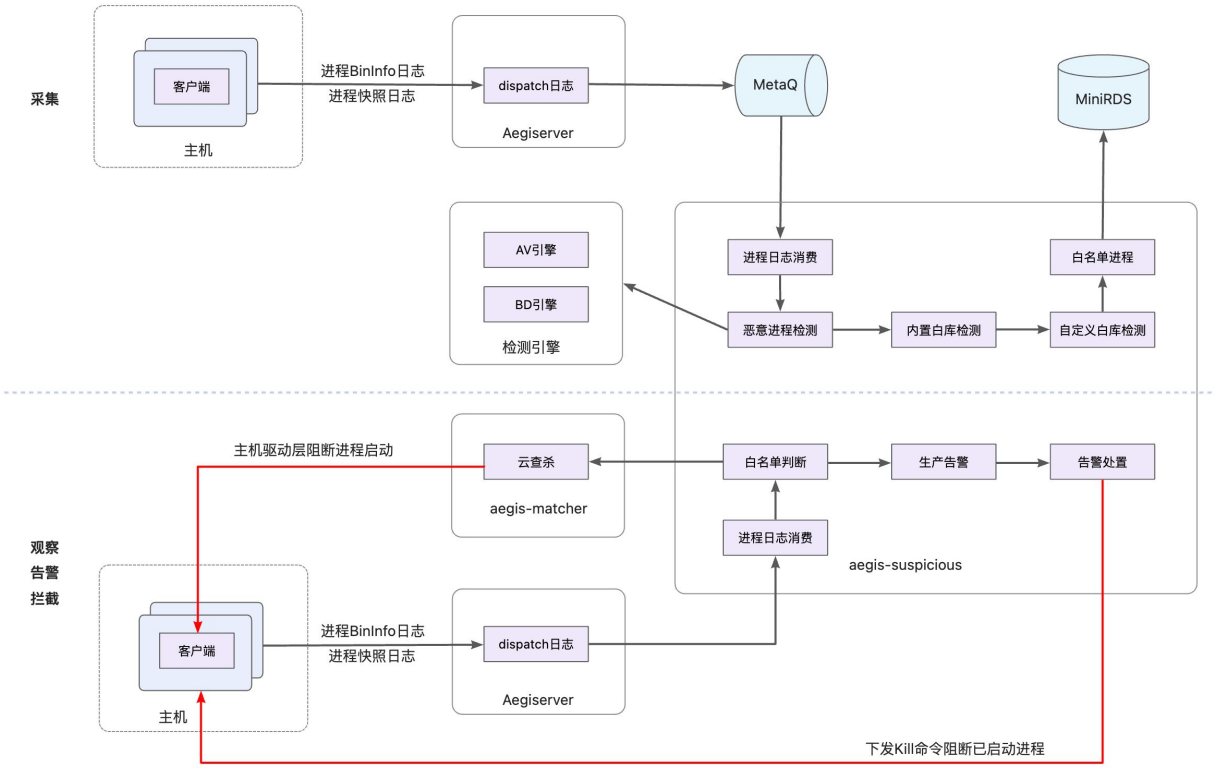
应用白名单

应用白名单功能支持将需要重点防御的服务器加入到白名单中，通过检测白名单中指定的应用程序区分可信、可疑和恶意程序，防止未经白名单授权的程序运行。

应用白名单功能主要包括采集、告警、拦截三个流程，其中拦截模式只针对特定局点开启。

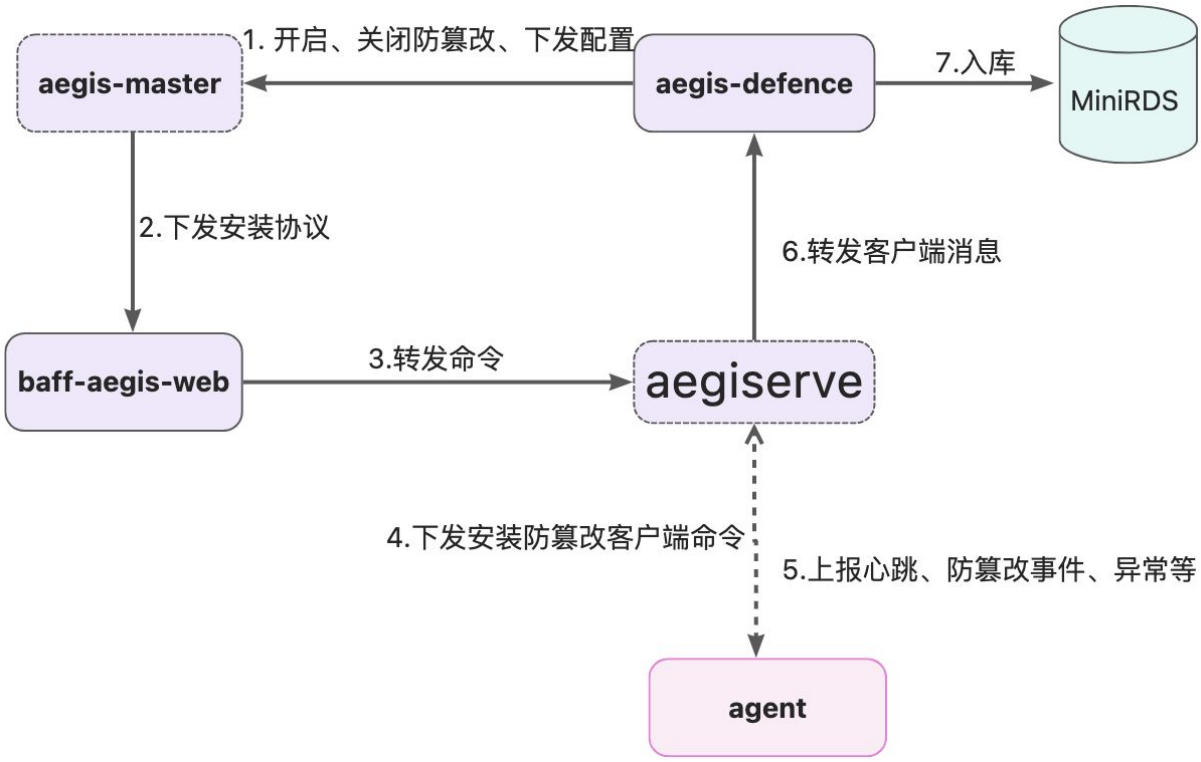
- 采集流程：客户端上报进程BinInfo或快照日志，aegis-suspicious消费后通过引擎、内置白库、自定义白库三类检测后，确定是否是白名单进程并入库。

- 告警流程：客户端上报进程BinInfo或快照日志，aegis-suspicious通过采集的白名单进程判断是否是可信进程，如果是不可信进程，则生成告警。
- 拦截流程：如果开启了拦截模式，aegis-suspicious会通知aegis-matcher更新云查杀库，云查杀模块会通过客户端HIPS进程阻断主机上的进程启动，同时还会主动下发kill进程命令用于阻断已启动的进程。



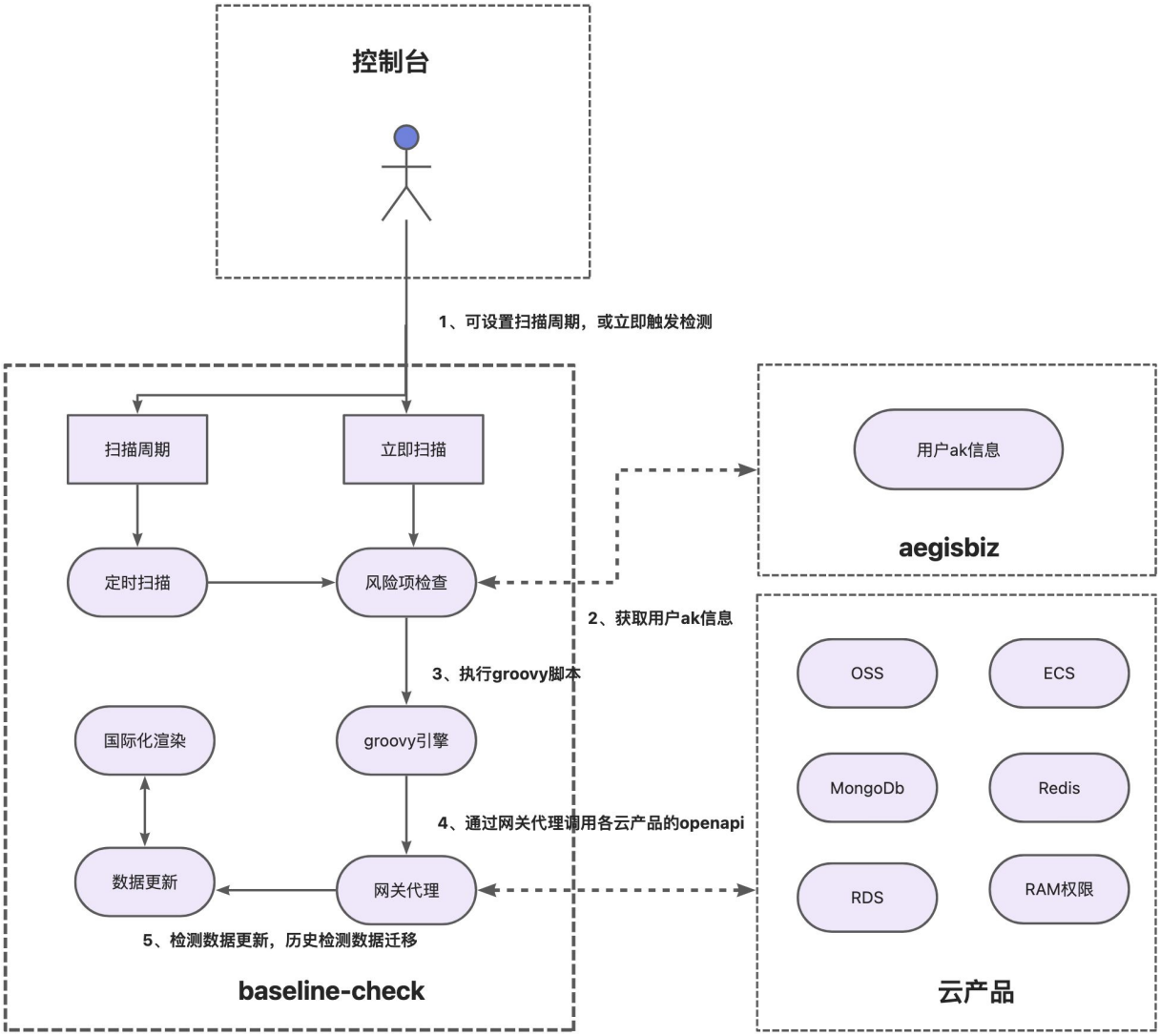
网页防篡改

网页防篡改实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入等入侵。



云产品检查

云平台配置检查功能，可帮助您检查您云产品的安全配置是否存在安全隐患，主要可检查的云产品涉及（oss,sls,rds，ecs，MongoDb,redis等）



1、用户可设置扫描周期或立即扫描触发云产品检查

2、当开始扫描时，先从aegisbi获取ak信息

3、通过groovy脚本中使用网关代理调用各个云产品的openapi，获取检查结果

1.4. 高可靠性

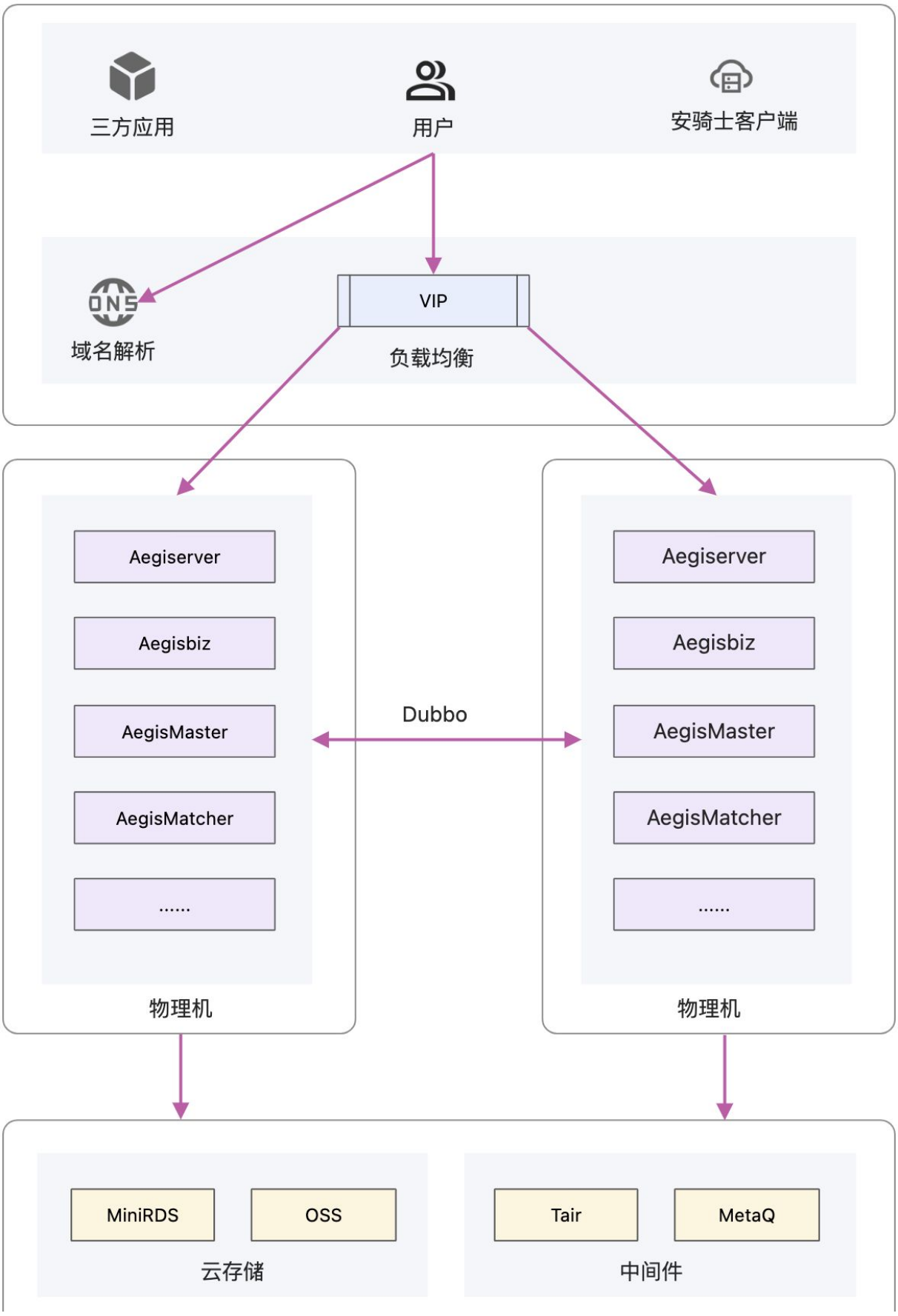
服务端高可用

> 说明
>
> 服务端整体设计原则：无状态应用

安骑士服务端全部是无状态应用，通过VIP+Dubbo实现负载均衡保证服务可用性。

- 服务端本身是无状态的，部署在至少两台物理机上，只要有一台物理机正常运行即可保证可用性。
- 数据存储在在MiniRDS、SLS、OSS、Tair、Diamond、MetaQ等中间件或云服务上，存储高可用性由中间件或云服务保证。
- 对外提供HTTPS协议的OpenAPI，通过DNS+VIP实现负载均衡保证可用性。

- 服务内部调用依赖Dubbo框架，由Dubbo的软负载保证可用性。



底座资源

客户端高可用

客户端高可用是为了保证客户端进程不会被操作系统或恶意程序kill，导致主机脱离安全管理。

客户端高可用有两个措施保证：

1、AliYunDun和AliYunDunUpdate互为守护进程，当其中一个被kill后，另一个进程会实时拉起对方。

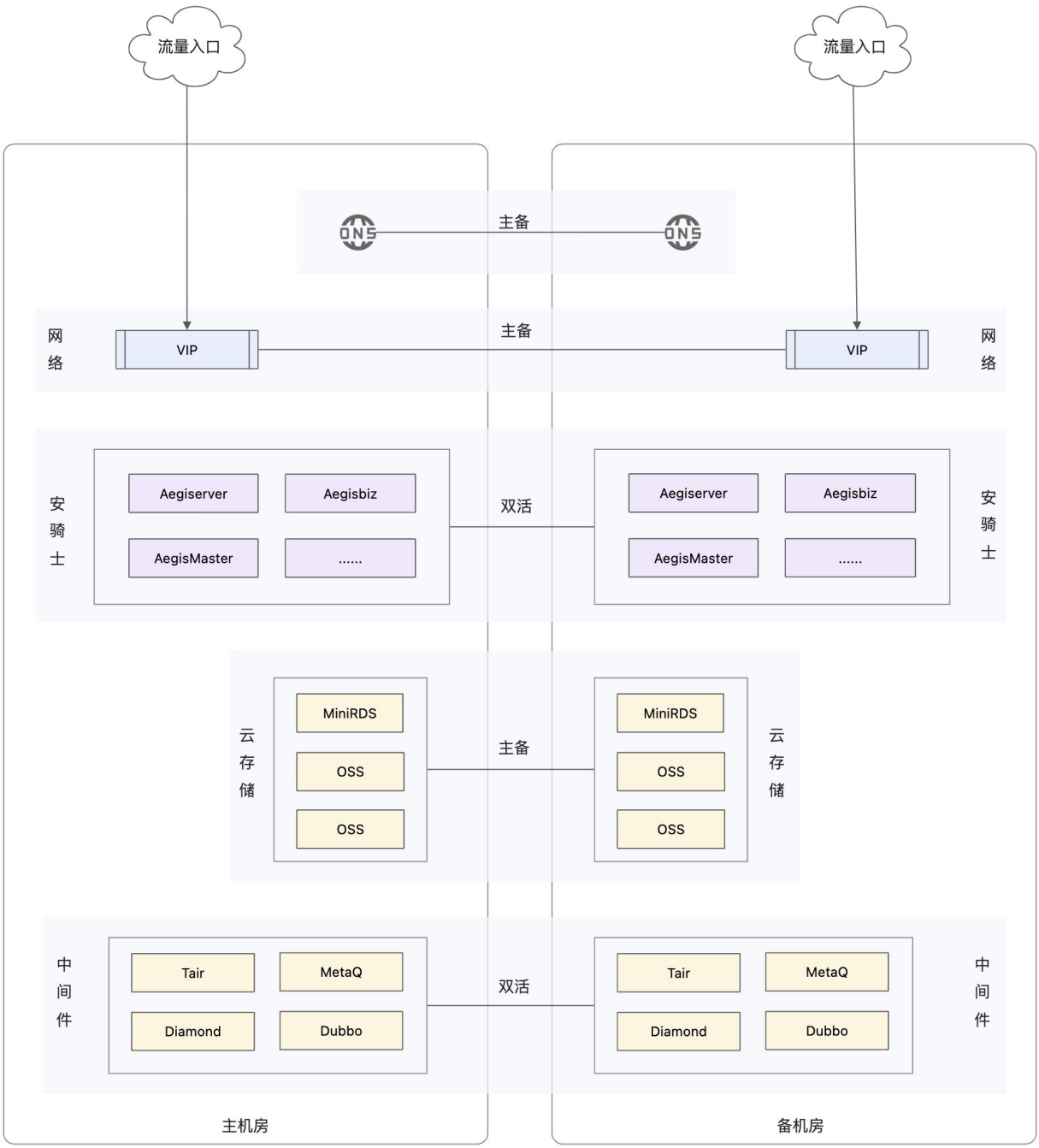
2、当启用自保护（AliSecGuard）时，AliSecGuard会在驱动层保证客户端无法被Killed。

1.5. 容灾备份

同城容灾

> 说明
>
> 设计原则：业务双活

安骑士同城容灾架构遵循双活原则，数据由云存储或中间件自身保证容灾。



各组件同城容灾实现方案介绍：

组件	方案
安骑士	双活部署，依赖中间件及云存储保证数据一致。
DNS	通过Anycast VIP实现主备机房流量隔离。
VIP	通过BGP路由实现主备切换。

MiniRDS	主从库binlog复制。
SLS	基于OSS备份实现数据同步。
OSS	主备机房数据同步。
中间件	双活部署，依赖MiniRDS保证数据一致。

异地灾备

> 说明
>
> 设计原则：Region间相互独立

安骑士多Region架构遵循独立原则，单元Region对中心Region无任何依赖，数据及服务保证完全隔离。

1.6. 容量规划

安骑士基于可用区内的NC数量ExpectedNcCountOfLocalZone（当前机房的机器预期数量）计算出规格。

每增加500台NC，BasicThinCluster和SasCluster都需增加2台物理机（NC和ECS的比例按照1:6，500台NC对应3000台ECS）。

> 重要
>
> 安骑士最大规格只能支持到8000台NC，如超过上限需联系安骑士研发介入。

资源规格定义

安骑士规格	BasicThinCluster	SasCluster	计算公式（整朵云的机器预期数量）
small	2	2	ExpectedNcCountOfLocalZone < 500
standard	2~4	2~4	ExpectedNcCountOfLocalZone < 1000
large	4~8	4~8	ExpectedNcCountOfLocalZone < 2000
xlarge	8~16	8~16	ExpectedNcCountOfLocalZone < 4000
2xlarge	16~32	16~32	ExpectedNcCountOfLocalZone < 8000

MiniRDS资源规格定义

x86数据库规格

容量规格	small		standard		large		xlarge		2xlarge	
数据库实例名称	数据库规格	磁盘（单位:G）	数据库规格	磁盘（单位:G）	数据库规格	磁盘（单位:G）	数据库规格	磁盘（单位:G）	数据库规格	磁盘（单位:G）
aegis erver	rds.mys2.standard	50	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.xlarge	200	rds.mys2.2xlarge	500
healthcheck	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.xlarge	200	rds.mys2.2xlarge	500	rds.mys2.2xlarge	500
defender	rds.mys2.standard	50	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.xlarge	200	rds.mys2.xlarge	200
aegis vul	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.xlarge	200	rds.mys2.2xlarge	500	rds.mys2.2xlarge	500
mordor	rds.mys2.standard	50	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.xlarge	200	rds.mys2.xlarge	200
aegis biz	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.large	100	rds.mys2.xlarge	200	rds.mys2.2xlarge	500
aegis assets	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.xlarge	200	rds.mys2.2xlarge	500	rds.mys2.2xlarge	500

aegis detect	rds.mys2.standard	50	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.large	100	rds.mys2.xlarge	200
aegis master	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.xlarge	200	rds.mys2.2xlarge	500	rds.mys2.2xlarge	500
suspicious	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.xlarge	200	rds.mys2.2xlarge	500	rds.mys2.2xlarge	500
banffweb	rds.mys2.standard	50	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.large	100	rds.mys2.xlarge	200
aegisvirusscan	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.xlarge	200	rds.mys2.2xlarge	500	rds.mys2.2xlarge	500
sasfileserver	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.xlarge	200
aegismetadata	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.large	100	rds.mys2.xlarge	200	rds.mys2.2xlarge	500
baseline	rds.mys2.standard	50	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.xlarge	200	rds.mys2.2xlarge	500
newsas	rds.mys2.standard	50	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.large	100	rds.mys2.xlarge	200

aegis matcher	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.large	50	rds.mys2.xlarge	200	rds.mys2.xlarge	200
aegis defence	rds.mys2.standard	50	rds.mys2.standard	50	rds.mys2.large	100	rds.mys2.xlarge	200	rds.mys2.xlarge	200
magpiebridgedb	rds.mys2.standard	-	rds.mys2.standard	-	rds.mys2.standard	-	rds.mys2.large	-	rds.mys2.large	-
yundunapi	rds.mys2.standard	-	rds.mys2.standard	-	rds.mys2.standard	-	rds.mys2.large	-	rds.mys2.large	-
yundunluban	rds.mys2.standard	-	rds.mys2.standard	-	rds.mys2.standard	-	rds.mys2.large	-	rds.mys2.large	-
datasync	rds.mys2.standard	-	rds.mys2.standard	-	rds.mys2.standard	-	rds.mys2.large	-	rds.mys2.large	-

arm/sw数据库规格

数据库实例名称	small	standard	large	xlarge	2xlarge
aegiserver	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large
healthcheck	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large	rds.mysql.c1.large
defender	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.s3.large

aegisvul	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large	rds.mysql.c1.large
mordor	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.s3.large
aegisbiz	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large
aegisassets	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large	rds.mysql.c1.large
aegisdetect	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large	rds.mysql.s3.large
aegismaster	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large	rds.mysql.c1.large
suspicious	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large	rds.mysql.c1.large
banffweb	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large	rds.mysql.s3.large
aegisvirusscan	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large	rds.mysql.c1.large
sasfileserver	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large	rds.mysql.s3.large
aegismetadata	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large
baseline	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.c1.large
newsas	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large	rds.mysql.s3.large
aegismatcher	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.s3.large

aegisdefence	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s3.large	rds.mysql.s3.large
magpiebridgedb	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large
yundunapi	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large
yundunluban	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large
datasync	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s1.small	rds.mysql.s2.large	rds.mysql.s2.large

Oss 、Sls-inner资源容量规划

规格	机器总数（物理机+ECS机器）	OSS容量(GB)	sls-Inner盘古磁盘总用（GB）
	计算公式：	2GB/单台机器	0.1GB/单台机器
small	500+3000	7000	350
standard	1000+6000	14000	700
large	2000+12000	28000	1400
xlarge	4000+24000	56000	2800
2xlarge	8000+48000	112000	5600

Tair资源容量规划

规格	机器总数 （物理机+ECS机器）	tair 各namespace所需分配配额（MB）

	namespace	92	381	499	663	106	690	478	692	总计(MB)
small	500+3000	512	512	512	256	256	256	256	256	2816
standard	1000+6000	512	512	512	256	256	256	256	256	2816
large	2000+12000	512	512	512	256	256	256	256	256	2816
xlarge	4000+24000	1024	1024	1024	512	512	512	512	512	5632
2xlarge	8000+48000	联系研发确认								

MetaQ资源容量规划

规格	机器总数（物理机+ECS机器）	metaq容量规划 (单位:万条)						
		进程消息	网络消息	文件消息	进程写文件消息	插件心跳消息	其他	总计(单位:万条)
	计算公式:（消息数/小时/机器）	240	20	5	15	60	140	0.058
small	500+3000	84	7	1.75	5.25	21	49	203
standard	1000+6000	168	14	3.5	10.5	42	98	406
large	2000+12000	336	28	7	21	84	196	812

xlarge	4000+24000	672	56	14	42	168	392	1624
2xlarge	8000+48000	1344	112	28	84	336	784	3248

1.7. 信创支持

企业版与国产化能力差异

企业版与国产化能力差异主要是平台差异导致，

- x86企业版与x86海光能力100%一致。
- arm飞腾、arm鲲鹏与企业版能力差异在30%以内，未来有计划对齐。
- sw申威与x86企业版能力差异50%以内，未来暂无计划对齐。

主机安全能力差异

功能	x86	arm	sw	描述
总览	100%	100%	100%	展示需要重点关注的资产，漏洞，异常，配置缺陷，事件等信息总览
主机资产	100%	100%	100%	提供服务器安全状态相关信息，例如服务器的防护状态、分组、专有网络VPC等统计信息，统计区分所有服务器、存在风险的服务器、未受保护的服务器、未启动的服务器和新增服务器的资产数量，单击目标服务器名称可查看详细信息，包括漏洞信息、安全告警处理、基线检查、资产指纹调查等。
主机指纹	100%	100%	100%	周期性采集服务器的账号、端口、进程、中间件、软件、计划任务、启动项等数据。 端口：清点主机端口监听信息，包括监听端口、网络协议、对应的进程、ip地址最新采集时间等信息。 软件：清点主机软件安装的资产信息，包括具体软件资产名称、软件版本、软件安装目录、最新采集时间等信息。 进程：清点主机进程信息，包括进程名、进程路径、启动参数、启动时间、运行用户、运行权限、pid、父进程、最新采集时间等信息。 账户：清点主机账户信息，包括账户名、登录权限、root权限、用户组、到期时间、上次登陆时间、最新采集时间等信息。 计划任务：清点主机的计划任务，包括任务路径、执行命令、任务周期、账户名称，最新采集时间等信息。

漏洞管理	100%	100%	100%	支持检测包括Linux、Windows、Web-CMS、应用漏洞以及应急漏洞五种漏洞类型，针对检测出来的漏洞提供修复方案、验证等操作，提供具体漏洞详情，提供一键扫描功能。 注意：部分国产化操作系统不在支持范围，需通过规则包适配。
基线检测	100%	100%	100%	自动检测服务器上的系统、账号、数据库、弱密码、合规性配置中存在的风险点，并提供加固建议，支持的资产类型包括常见数据库、系统、中间件等。 注意：部分国产化操作系统不在支持范围，需通过规则包适配。
云外暴露检查	100%	100%	100%	云外暴露检查支持自动分析您的ECS服务器在互联网上的暴露情况，可视化呈现ECS与互联网的通信链路，并集中展示您暴露在公网的ECS的漏洞信息，帮助您快速定位您资产在互联网上的异常暴露情况并提供相应漏洞的修复建议。
病毒防御	100%	60%	60%	提供病毒查杀和网站后门查杀功能，检测出主流木马病毒、勒索软件、挖矿病毒、DDoS木马后自动隔离查杀。 能力差异：arm/sw不支持主动防御、诱捕勒索功能呢
防篡改	100%	60%	60%	网页防篡改实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入等入侵。 防篡改支持驱动版和rsync版，驱动版支持全部功能，rsync版不支持进程白名单、告警模式、NFS 路径防御，能力是驱动版的60%左右。能力差异说明 能力差异：x86支持驱动版和rsync版本，arm/sw仅支持rsync。
入侵事件告警	100%	80%	50%	集中展示受影响主机资产的告警信息，包括存在告警服务器的数量、待处理告警总数、需要紧急处理的告警等，其中告警类型覆盖进程异常行为、网站后门、异常登录、恶意进程（云查杀）、敏感文件篡改、异常网络连接、持久化后门、web应用威胁检测等多种入侵告警类型。 能力差异：arm不支持AV/BD检测引擎，仅支持GLE。sw均不支持。
日志检索	100%	100%	100%	提供登录流水、暴力破解、进程快照、网络连接、端口监听快照、账号快照、进程启动的日志查询
客户端安装	100%	100%	100%	支持查看离线的服务器，选择重新安装，提供安装教程，可选择指定服务器卸载安骑士插件。
防护模式	100%	50%	0%	提供业务优先和防护优先两种模式，供不同的业务场景使用。 能力差异：arm版本不支持自保护功能，sw版本不支持防护模式设置。

态势感知能力差异

功能	x86	arm	sw	描述
总览	100%	100%	100%	提供整体安全威胁概览信息，包括总体安全评分、防护资产状态、待处理风险告警、已处理风险等态势信息。
安全大屏	100%	100%	100%	提供基于态势感知的大屏展示，将安全攻防数据转化并呈现到安全大屏上，展示包括资产、漏洞、基线、攻击来源、攻击分布等网络安全态势信息。
安全告警	100%	80%	50%	提供如下类型告警：进程异常行为，网站后门，异常登录，敏感文件篡改，恶意进程（云查杀），异常网络连接，web应用威胁检测，按照紧急，可疑，提醒三种程度告警，展示受影响资产，最新告警时间。 能力差异：arm检测引擎不支持AV/BD，仅支持GLE。sw均不支持。
攻击分析	100%	100%	100%	展示最近7天/30天攻击趋势和攻击类型分布 包括：SSH暴力破解、RDP暴力破解、SQLSERVER暴力破解、MYSQL暴力破解、FTP暴力破解、远程文件包含、路径遍历、越权访问、CSRF、SQL注入，XSS攻击，反弹shell，代码执行等攻击行为。提供展示包括攻击时间，攻击来源，被攻击资产，攻击次数，风险等级，攻击类型等具体信息。
云产品检查	100%	100%	100%	从网络访问控制、数据安全两个维度提供云产品安全配置检查，涉及的云产品检查项包括RDS-白名单，MongoDB-白名单，redis白名单，OSS-bucke权限设置，RDS-数据库安全策略，ECS自动快照，ECS安全组策略等，并根据检查结果定义低、中、高风险等级，支持手工启动检查以及周期性自动检查，并对检查结果进行验证或者加白操作。
应用白名单	100%	90%	0%	通过采集将需要重点防御的服务器加入到白名单中，通过检测白名单中指定的应用程序区分可信、可疑和恶意程序，防止未经白名单授权的程序运行。 能力差异：arm不支持拦截模式。sw均不支持。
资产中心	100%	100%	100%	提供服务器安全状态相关信息，例如服务器的防护状态、分组、专有网络VPC等统计信息，统计区分所有服务器、存在风险的服务器、未受保护的服务器、未启动的服务器和新增服务器的资产数量。 提供云产品安全状态相关信息，支持负载均衡、NAT网关。
安全报告	100%	80%	80%	提供报表查询功能，可根据报表名称检索历史报表 可按日，周，月自定义报表任务，发送到指定邮箱 报表内容可选：安全评分、资产风险分布、安全告警趋势、主动防御趋势、防篡改趋势、漏洞趋势、基线问题趋势、攻击数量趋势 能力差异：arm/sw不支持报告导出。

当前各模块适配情况

模块	x86（企业版、海光）	arm（飞腾、鲲鹏）	sw（申威）
客户端	100%	50% （不支持AliHips、AliSecGuard、AliNet）	50% （不支持AliHips、AliSecGuard、AliNet）
服务端	100%	99% （不支持报告导出）	80% （不支持报告导出，版本落后于x86和arm）
前端	100%	100%	100%
计算引擎	100%	100%	100%
检测引擎	100%	50% （不支持AV、BD引擎）	0% （所有检测引擎都不支持）

一云多芯支持情况

一云多芯的主要包括异构同城容灾（主备机房机房级硬件异构）以及异构多Region（中心/单元机房级硬件异构）2大横向场景。

安骑士对一云多芯的支持情况如下：

场景	支持情况
异构同城容灾（x86+arm） 主备机房机房级硬件异构	支持 （部分能力在arm机房不生效，如主动防御、自保护）
异构多Region（x86+arm） 中心/单元机房级硬件异构	支持

1.8. 热升级

安骑士默认支持热升级，无需额外运维操作。

2.安骑士运维操作

2.1. 登录飞天基础运维平台

本文介绍如何登录飞天基础运维平台。

前提条件

- 已从部署人员或管理员处获取Apsara Uni-manager运维控制台的访问地址、用户名和密码。

  Apsara Uni-manager运维控制台访问地址格式为*ops*.asconsole.*intranet-domain-id*.com。
- 推荐使用Chrome浏览器。

操作步骤

1. 打开浏览器。
2. 在地址栏中，输入Apsara Uni-manager运维控制台的访问地址*ops*.asconsole.*intranet-domain-id*.com，按回车键。

> **说明** 您可以单击页面右上角的下拉按钮来进行语言切换。

3. 输入正确的用户名及密码。

> **说明** 登录Apsara Uni-manager运维控制台的用户名和密码请从部署人员或管理员处获取。

首次登录Apsara Uni-manager运维控制台时，需要修改登录用户名的密码，请按照提示完成密码修改。

为提高安全性，密码必须满足以下要求：

- 英文大小写字母
- 阿拉伯数字（0~9）
- 特殊符号，包括感叹号（！）、at（@）、井号（#）、美元符号（$）、百分号（%）等
- 密码长度10~20个字符

4. 单击登录。
5. 在Apsara Uni-manager运维控制台的顶部菜单栏，选择**产品运维 > 云平台运维 > 飞天基础运维平台**。

2.2. 客户端状态检查

检查安骑士客户端以下状态信息，确定安骑士客户端正常运行。

客户端日志

客户端日志存放在进程文件所在目录层级data目录下，
如/usr/local/aegis/aegis_client/aegis_xx_xx/data。

客户端日志按照日期存储：data.1-data.7

客户端在线状态

执行以下命令，查看客户端在线状态。

```
ps -aux | grep AliYunDun
```

网络连接状态

执行以下命令，查看客户端是否与服务器端正常建立TCP连接。

```
netstat -tunpe |grep AliYunDun
```

客户端UUID

打开客户端日志文件data.x，查看 `Currentuid Ret` 后续字符串，即为当前的UUID。

客户端进程

客户端共有两个常运行进程（选择了自动病毒阻断时，会启动 `AliHips` ）： `AliYunDun` 、 `AliYunDunUpdate` 。

正常工作时上述两个进程都正常运行。

> 说明 在Windows系统客户端中， `AliYunDun` 、 `AliYunDunUpdate` 进程均以服务形式存在，服务名分别为 `Alibaba Security Aegis Detect Service` 和 `Alibaba Security Aegis Update Service` 。

2.3. 检查服务器端（Aegiserver）状态

背景信息

参考以下操作步骤，进行安骑士服务器端运行状态检查：

操作步骤

1. 执行 `ssh 宿主机IP` 命令，登录安骑士服务器端（Aegiserver）所在的宿主机。
2. 执行以下命令，查找安骑士服务器所对应的imageId。

   ```
   docker ps -a |grep aegiserver
   ```

   系统显示如下信息：

   ```
   b9e59994df41
   reg.docker.alibaba-inc.com/aqs/aegiserverlite@sha256:f9d292f54c58646b672a8533a0d78fba534d
   26d376a194034e8840c70d9aa0b3 "/bin/bash /startApp." 2 hours ago Up 2 hours 80/tcp, 7001/tcp,
   8005/tcp, 8009/tcp yundun-aegis.Aegiserverlite__.aegiserverlite.1484712802
   ```

3. 执行以下命令，进入Docker内部。

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. 执行以下命令，查看相关Java进程是否正常运行。

   ```
   ps aux |grep aegiserver
   ```

   正常情况下，系统显示如下信息：

   ```
   root 153 0.6 25.8 2983812 1084588 ? Sl 12:13 1:01 /opt/taobao/java/bin/java -Djava.util.logging.co
   nfig.file=/home/admin/aegiserverlite/.default/conf/logging.properties -Djava.util.logging.manager
   =org.apache.juli.ClassLoaderLogManager -server -Xms2g -Xmx2g -XX:PermSize=96m -XX:MaxPermSi
   ze=384m -Xmn1g -XX:+UseConcMarkSweepGC -XX:+UseCMSCompactAtFullCollection -XX:CMSMaxAb
   ortablePrecleanTime=5000 -XX:+CMSClassUnloadingEnabled -XX:+UseCMSInitiatingOccupancyOnly -
   XX:CMSInitiatingOccupancyFraction=80 -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/
   home/admin/logs/java.hprof -verbose:gc -Xloggc:/home/admin/logs/gc.log -XX:+PrintGCDetails -XX
   :+PrintGCDateStamps -Djava.awt.headless=true -Dsun.net.client.defaultConnectTimeout=10000 -Ds
   un.net.client.defaultReadTimeout=30000 -XX:+DisableExplicitGC -Dfile.encoding=UTF-8 -Ddruid.filter
   s=mergeStat -Ddruid.useGloalDataSourceStat=true -Dproject.name=aegiserverlite -Dcatalina.vendo
   r=alibaba -Djava.security.egd=file:/dev/./urandom -Dlog4j.defaultInitOverride=true -Dorg.apache.to
   mcat.util.http.ServerCookie.ALLOW_EQUALS_IN_VALUE=true -Dorg.apache.tomcat.util.http.ServerCoo
   kie.ALLOW_HTTP_SEPARATORS_IN_V0=true -Djava.endorsed.dirs=/opt/taobao/tomcat/endorsed -cla
   sspath /opt/taobao/tomcat/bin/bootstrap.jar:/opt/taobao/tomcat/bin/tomcat-juli.jar -Dcatalina.lo
   gs=/home/admin/aegiserverlite/.default/logs -Dcatalina.base=/home/admin/aegiserverlite/.defaul
   t -Dcatalina.home=/opt/taobao/tomcat -Djava.io.tmpdir=/home/admin/aegiserverlite/.default/tempo
   org.apache.catalina.startup.Bootstrap -Djboss.server.home.dir=/home/admin/aegiserverlite/.defaul
   t -Djboss.server.home.url=file:/home/admin/aegiserverlite/.default start
   ```

5. 执行以下命令，进行健康检查。

   ```
   curl 127.0.0.1:7001/checkpreload.htm
   ```

   如果返回success，表示服务正常。

6. 查看日志。
   - **协议日志**：/home/admin/aegiserver/logs/AEGIS_MESSAGE.log，查看与客户端上下行协议日志。
   - **运行日志**：/home/admin/aegiserver/logs/aegis-default.log，查看运行过程中异常的堆栈信息。
   - **离线日志**：/home/admin/aegiserver/logs/AEGIS_OFFLINE_MESSAGE.log，查看客户端超时掉线日志。

2.4. 检查更新服务（Aegisupdate）状态

背景信息

参考以下操作步骤，进行安骑士更新服务状态检查：

操作步骤

1. 执行 `ssh 宿主机IP` 命令，登录安骑士服务器端所在的宿主机。
2. 执行以下命令，查找安骑士服务器所对应的imageId。

   ```
   docker ps -a |grep aegiserver
   ```

3. 执行以下命令，进入Docker内部。

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. 执行以下命令，查看相关Java进程是否正常运行。

   ```
   ps aux |grep aegisupdate
   ```

5. 执行以下命令，进行健康检查。

   ```
   curl 127.0.0.1:7001/checkpreload.htm
   ```

   如果返回success，表示服务正常。

2.5. 检查Defender模块状态

背景信息

参考以下操作步骤，进行安骑士Defender模块状态检查：

操作步骤

1. 执行 `ssh 宿主机IP` 命令，登录安骑士Defender模块所在的宿主机。
2. 执行以下命令，查找安骑士Defender模块对应的imageId。

   ```
   docker ps -a |grep defender
   ```

3. 执行以下命令，进入Docker内部。

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. 执行以下命令，查看相关Java进程是否正常运行。

   ```
   ps aux |grep defender
   ```

5. 执行如下命令，进行健康检查。

   ```
   curl 127.0.0.1:7001/checkpreload.htm
   ```

   如果返回success，表示服务正常运行。

2.6. 重启安骑士服务

背景信息

在安骑士模块出现故障时，可参考以下操作步骤，尝试重启相关服务。

操作步骤

1. 执行 `ssh 宿主机IP` 命令，登录到安骑士功能模块所在的宿主机。
2. 执行以下命令，查找安骑士功能模块所对应的imageId。

   ```
   docker ps -a |grep 应用名称
   ```

3. 执行以下命令，进入Docker内部。

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. 重启安骑士相关服务。
   - 重启安骑士客户端服务：
     - Windows系统主机：进入服务管理器，找到服务Alibaba Security Aegis Detect Service，重启该服务。
     - Linux系统主机，可以使用以下两种方法：
       - 执行 `service aegis restart` 命令，重启服务。
       - 以root权限执行 `killall AliYunDun` 命令关闭当前进程后，重新启动/usr/local/aegis/aegis_client/aegis_xx_xx/AliYunDun进程。
   - 重启安骑士服务器端服务：
     a. 执行以下命令，查看相关Java进程的进程id。

     ```
     ps aux |grep aegiserver
     ```

     b. 执行以下命令，关闭当前进程。

     ```
     kill -9 进程
     ```

     c. 执行以下命令，重启进程。

     ```
     sudo -u admin /home/admin/aegiserever/bin/jbossctl restart
     ```

     d. 执行以下命令，检查进程是否重启成功。

     ```
     curl 127.0.0.1:7001/checkpreload.htm
     ```

   - 重启安骑士更新服务（Aegisupdate）：
     a. 执行如下命令，查找java的进程id。

     ```
     ps aux |grep aegisupdate
     ```

     b. 执行如下命令，关闭当前进程。

     ```
     kill -9 进程
     ```

     c. 执行如下命令，重启进程。

     ```
     sudo -u admin /home/admin/aegisupdate/bin/jbossctl restart
     ```

d. 执行如下命令，查看进程是否重启成功。

```
curl 127.0.0.1:7001/checkpreload.htm
```

- 重启安骑士Defender服务：

a. 执行以下命令，查找相关Java进程的进程id。

```
ps aux |grep secure-service
```

b. 执行以下命令，关闭当前进程。

```
kill -9 进程
```

c. 执行以下命令，重启进程。

```
sudo -u admin /home/admin/secure-service/bin/jbossctl restart
```

d. 执行以下命令，查看进程是否重启成功。

```
curl 127.0.0.1:7001/checkpreload.htm
```