<资产-主机组优化>  
Functional and Design Specification

< One-line description of the purpose of the document and/or feature>

Reviewers（文档审批人）

|  |  |  |
| --- | --- | --- |
| Department（部门） | Name（姓名） | Approval Date（批准日期） |
| Software（软件） | 吴永健 |  |
| Software（软件） |  |  |
| Software（软件） |  |  |
| QA（测试） |  |  |
| QA（测试） |  |  |
| DB |  |  |
| ARC |  |  |
| PLM |  |  |
| Documentation（文档） |  | 邮件评审即可 |

Modification History（修改历史）

|  |  |  |  |
| --- | --- | --- | --- |
| Revision（版本） | Date  （日期） | Author  （作者） | Comments  （修改说明） |
| 1 | 9/11/2022 | 吴永健 | Init Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[<Feature Name> Functional and Design Specification 1](#_Toc113972777)

[Reviewers（文档审批人） 1](#_Toc113972778)

[Modification History（修改历史） 2](#_Toc113972779)

[1 问题定义和用户需求 5](#_Toc113972780)

[1.1 软件功能需求列表 6](#_Toc113972781)

[1.2 软件功能规格列表 6](#_Toc113972782)

[2 相关FRs 6](#_Toc113972783)

[3 软件支持平台 6](#_Toc113972784)

[3.1 支持的OS/CPU 6](#_Toc113972785)

[4 软件架构和总体框图 7](#_Toc113972786)

[5 模块详解 7](#_Toc113972787)

[6 系统资源和性能影响 7](#_Toc113972788)

[7 安全考虑 7](#_Toc113972789)

[8 健壮性及容错 7](#_Toc113972790)

[9 功能详述 8](#_Toc113972791)

[9.1 时间表资源的增删改查 8](#_Toc113972792)

[9.1.1 Api\_server对象设计 8](#_Toc113972793)

[9.1.2 实现方法 9](#_Toc113972794)

[9.1.3 Debug 10](#_Toc113972795)

[9.1.4 SYSLog 10](#_Toc113972796)

[9.1.5 白盒测试 10](#_Toc113972797)

[9.2 Policy资源和 TimeTable资源的匹配 10](#_Toc113972798)

[9.2.1 Policy结构体添加字段 10](#_Toc113972799)

[9.2.2 实现方法 11](#_Toc113972800)

[9.3 Policy在匹配的TimeTable的时间段内不生效 11](#_Toc113972801)

[9.3.1 实现方法 11](#_Toc113972802)

[10 功能限制 11](#_Toc113972803)

[11 典型用户配置 11](#_Toc113972804)

[12 测试考虑 12](#_Toc113972805)

[13 References（参考资料） 12](#_Toc113972806)

[14 Glossary（术语表） 12](#_Toc113972807)

[15 Attachment（附件） 12](#_Toc113972808)

[15.1 Review Action Items（评审纪要） 12](#_Toc113972809)

# 问题定义和用户需求

在某一些情况下， 用户部署agent的时候不能确定这台主机的业务归属信息。或者用户对于工作节点的使用比较灵活， 主机的业务所属关系会发生变化。

因此需要Agent部署时可以不提供该主机所属的主机组和集群，将此类主机归类到未分类资产。 并且允许将主机移动到当前集群的已有主机组中，策略自动跟随生效。

# 功能列表

## 软件功能需求列表

|  |  |
| --- | --- |
| Requirements | Engineering Comments |
| 允许主机agent上线时不指定集群和主机组。 | 这部分主机显示在未分类资产下。 |
| 修改主机所属的主机组。 | 1. 修改config\_channel中sysmonitor资源和node资源的主机组信息 2. 修改agent缓存的主机组信息 3. 修改mongo中node表存储的hostGroup信息。 |
| 透视镜统计模块更新。 | 1. 修改mongo中透视镜显示方案表insightfilter和insightmyfilter |
| 转移后日志信息修改，转移前日志信息不做修改。 | 1. 修改agent和controller在打印日志的时候获取集群和主机组的信息的方式。 |

## 软件功能规格列表

# 相关FRs

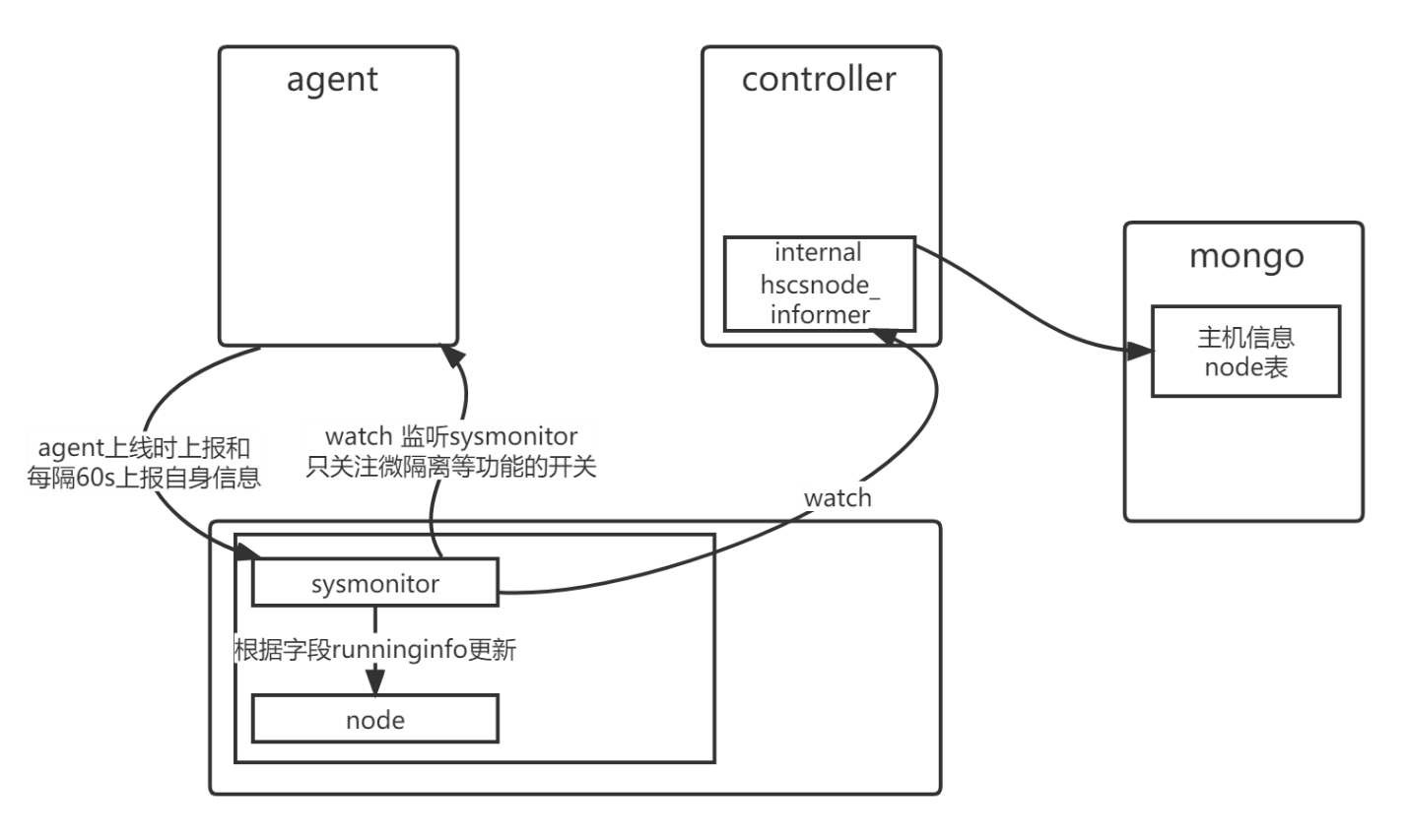
# 软件支持平台

## 支持的OS/CPU

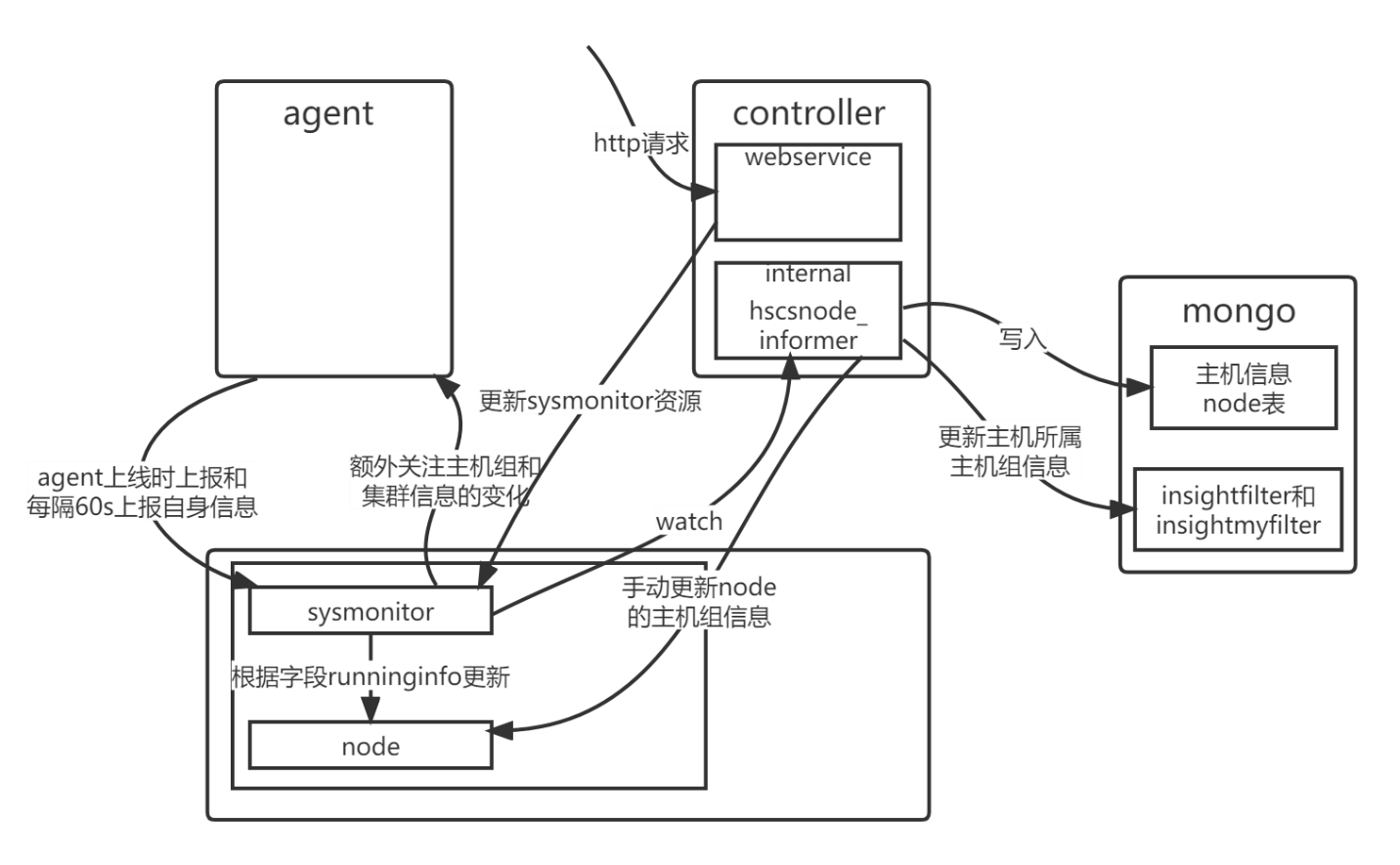
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OS | CPU Arch | Kernel Version | Release | Supported（Yes/No） |
| Linux | X86-64 | > 4.10 | Ubuntu 14.04/16.04/18.04  Centos XXX  Suse XXX | Yes |
| Linux | ARM64 |  | 麒麟 Linux V10服务器版本 | No |
| Windows Server | AMD64 | N/A | 2012/2016/2019 | Yes |

# 软件架构和总体框图

更改前 主机信息流转图



更改后主机信息 流转图



# 模块详解

1. 主机所属主机组修改
2. 主机只能移动到同集群同项目的主机组中
3. 未分类的主机可以移动到当前用户可操作的任意的主机组中。
4. 要移入的主机组中已经存在同名主机，不允许移动。
5. 当主机上的agent正在进行合规漏扫杀毒任务时， 不允许移动该主机。（若对应任务资源的status处于init或running视为正在运行）。

# 系统资源和性能影响 N/A

# 安全考虑 N/A

# 健壮性及容错 N/A

## 异常容错N/A

# 功能详述

## 修改主机所属主机组

### 实现方法

#### 同步修改sysmonitor资源和node资源

1. Controller接收到要转移的主机的请求， 判断主机和主机组是否存在。
2. 判断主机目前所在的主机组和要转移的主机组是否在同一个集群同一个项目。
3. 判断转移进的主机组是否已经存在同名的主机。
4. 判断要移动的主机的状态， 其agent是否正在执行 合规, 漏扫, 杀毒操作。
5. 修改config\_channel存储的对应sysmonitor资源和node资源的主机组信息。

#### 修改Agent主机组信息

1. Agent监听sysmonitor资源的时候， 关注其nodegroup字段和cluster字段是否变化， 如果发生变化则立即更新agent端存储的信息。
   1. 修改 /opt/hillstone\_uhs/config/product.yaml文件中的存储的DEFENDER\_CLUSTER\_NAME字段和DEFENDER\_HOSTGROUP\_NAME字段。
   2. 修改/agent/go/pkg/common/config/config\_parse.go中定义的全局的配置信息

Conf.Env. DEFENDER\_HOSTGROUP\_NAME和

Conf.Env. DEFENDER\_CLUSTER\_NAME

* 1. 修改/agent/go/internal/assets/internal/defenderassets/hostGroup.go中定义的HostGroupCache 主机组缓存信息。
  2. 修改/agent/go/internal/assets/internal/defenderassets/cluster.go中定义的ClusterName 集群缓存信息。

1. Agent向config\_channel上报自身信息的时候， 只有第一次会上报会上报自己的集群信息和主机组信息。 后续每分钟进行的信息上报不会覆盖sysmonitor资源中存储的集群和主机组信息。

#### 主机状态检测的实现

1. 更新config\_channel中 存储的资源信息之前，先查询合规漏扫杀毒任务信息。

对于主机 镜像 容器的合规任务都检查 compliancechecknodeinfo资源。

对于主机漏扫任务可以检查hostvulnscannode资源。

对于镜像漏扫任务可以检查vulnscannodeinfo资源。

对于镜像查杀任务可以检查avscannodeinfo资源。

对于主机查杀任务可以检查virusscan资源或者查询mongo中的host\_av\_task\_status表。

1. 当对应agendID的nodeinfo资源的status字段等于running或init，则不允许移动该主机。

#### mongo中主机信息node表更新

1. 现在好像已经实现了

#### 批量修改主机所属主机组信息

1. 接收请求的一个对象数组， 每个对象代表一个主机的移动需求。
2. 首先校验对象数组中的agentID是否重复， 如果重复直接返回错误。
3. 尝试处理每个主机移动的需求， 将主机移动处理失败的agentID和失败原因记录下来并返回。

## 透视镜统计模块更新

1. 主机对应的主机组信息发生变化时， 查找mongo数据库insightfilter和insightmyfilter表中对应agentid的Hostinfo字段并修改。

## 日志信息更新

### Agent输出日志包含集群和主机组代码统计

#### 使用agent全局config.env的信息

## WebUI

#### UE视图



#### RESTFUL API

##### 修改主机所属主机组信息的API接口

|  |  |
| --- | --- |
| 描述 | 修改sysmoniotr资源和node资源主机组信息的接口信息 PUT |
| url | /rest/system/sysMonSvc/moveHost |
| 参数 | |  |  |  | | --- | --- | --- | | 字段 | 类型 | 描述 | | agentID | string | 具体node和sysmo  nitor资源的唯一标识。 | | newHostGroup | string | Node需要转移到的主机组。 | |
| 返回结果 | Success example   |  | | --- | | {  Total: 0,  Result: {},  } |   Fail example   |  | | --- | | {  Code: int  Msg: string  Detail: string  } | |

|  |  |  |  |
| --- | --- | --- | --- |
| 错误处理 | 错误码 | 字段 | 描述 |
| 250001 |  | 该主机组中已经存在同名主机了 |
|  | 250002 |  | 该主机组不属于当前集群 |
|  | 250003 |  | 该主机组不属于当前项目 |
|  | 250004 |  | 查询主机错误，不存在该主机 |
|  | 250005 |  | 查询主机组错误，不存在该主机组 |

##### 批量修改

|  |  |
| --- | --- |
| 描述 | 修改sysmoniotr资源和node资源主机组信息的接口信息 PUT |
| url | /rest/system/sysMonSvc/moveHosts |
| 参数 | |  |  |  | | --- | --- | --- | | 字段 | 类型 | 描述 | |  | []{agentID, newHostGroup} |  | | newHostGroup | string | Node需要转移到的主机组。 | | agentID | string | 具体node和sysmo  nitor资源的唯一标识。 | |
| 返回结果 | Success example   |  | | --- | | {  Total: int, //移动失败的数量  Result: {“failed”:[{“agentID”:{ //移动失败的agentid和原因  Code: int,  Msg: string,  Detail: string,  }},], },  } |   Fail example   |  | | --- | | {  Code: int  Msg: string  Detail: string  } | |

### Debug

### SYSLog

|  |  |  |
| --- | --- | --- |
| *Severity*  *（严重度）* | *English（英文）* | *Chinese（中文）* |
| LOG\_ERR | Create timetable “name  failed:”reason” | 创建时间表资源“资源名称”失败：“原因” |
| LOG\_INFO | Create timetable “name” succeed | 创建时间表资源“资源名称”成功 |
| LOG\_ERR | Update timetable “name  failed:”reason” | 更新时间表资源“资源名称”失败：“原因” |
| LOG\_INFO | Update timetable “name” succeed:”new” | 更新时间表资源“资源名称”成功:”更新后的资源” |
| LOG\_ERR | Delete timetable “name  Failed:”reason” | 删除时间表资源“资源名称”失败：“原因” |
| LOG\_INFO | Delete timetable “name” succeed | 删除时间表资源“资源名称”成功 |
| LOG\_ERR | Get timetable failed:reason | 查找时间表资源失败：”原因” |

### 黑盒测试

### 白盒测试

*请根据实现的设计，给出采用白盒测试的手段验证实现的准确性的考虑。包括哪些函数和过程采用白盒测试，测试的用例设计等。*

# 功能限制N/A

# 典型用户配置N/A

# 测试考虑

1. 并发的操作同一个时间表资源，微隔离策略关联时间表的同时删除时间表，是否会出现微隔离关联一个不存在的时间表资源
2. 错误的时间表配置信息，尝试添加不合规的时间信息，系统是否能够识别。

# References（参考资料） N/A

# Glossary（术语表）N/A

# Attachment（附件）

## Review Action Items（评审纪要）

End of Document