<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

[<资产-主机组优化> Functional and Design Specification 1](#_Toc119940907)

[Reviewers（文档审批人） 1](#_Toc119940908)

[Modification History（修改历史） 2](#_Toc119940909)

[1 问题定义和用户需求 5](#_Toc119940910)

[2 功能列表 6](#_Toc119940911)

[2.1 软件功能需求列表 6](#_Toc119940912)

[2.2 软件功能规格列表 6](#_Toc119940913)

[3 相关FRs 6](#_Toc119940914)

[4 软件支持平台 6](#_Toc119940915)

[4.1 支持的OS/CPU 6](#_Toc119940916)

[5 软件架构和总体框图 7](#_Toc119940917)

[6 模块详解 8](#_Toc119940918)

[7 系统资源和性能影响 N/A 9](#_Toc119940919)

[8 安全考虑 N/A 9](#_Toc119940920)

[9 健壮性及容错 N/A 9](#_Toc119940921)

[9.1 异常容错N/A 9](#_Toc119940922)

[10 功能详述 9](#_Toc119940923)

[10.1 修改主机所属主机组 9](#_Toc119940924)

[10.1.1 实现方法 9](#_Toc119940925)

[10.2 策略配置自动跟随 10](#_Toc119940926)

[10.2.1 实现方法 10](#_Toc119940927)

[10.3 透视镜和其他统计模块更新 11](#_Toc119940928)

[10.3.1 实现方法 11](#_Toc119940929)

[10.4 日志信息更新 11](#_Toc119940930)

[10.4.1 Agent输出日志包含集群和主机组代码统计 11](#_Toc119940931)

[10.5 WebUI 12](#_Toc119940932)

[10.5.2 Debug 14](#_Toc119940933)

[10.5.3 SYSLog 14](#_Toc119940934)

[10.5.4 黑盒测试 14](#_Toc119940935)

[10.5.5 白盒测试 14](#_Toc119940936)

[11 功能限制N/A 14](#_Toc119940937)

[12 典型用户配置N/A 14](#_Toc119940938)

[13 测试考虑 14](#_Toc119940939)

[14 References（参考资料） N/A 15](#_Toc119940940)

[15 Glossary（术语表）N/A 15](#_Toc119940941)

[16 Attachment（附件） 15](#_Toc119940942)

[16.1 Review Action Items（评审纪要） 15](#_Toc119940943)

# 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 |
| 系统中主机对主机组的归属信息的修改 | 1. 校验主机移动请求的合法性。 2. 修改config\_channel中sysmonitor资源和node资源的主机组信息 3. 修改agent缓存的主机组信息 4. 修改mongo中node表存储的hostGroup信息。 |
| 策略等配置自动跟随。 | 1. 更新合规漏扫查杀配置 2. 更新微隔离 行为规则 入侵防御 配置 |
| 透视镜和统计模块更新。 | 1. 修改mongo中透视镜显示方案表insightfilter和insightmyfilter。 |
| 日志信息跟更新 | 1. 所有转移前的日志信息不做修改， 转移后的日志信息按新的主机组归属产生。 2. 入侵防御 微隔离 行为安全事件转移前的日志不做修改， 转移后按新的主机组产生。 |

## 软件功能规格列表

# 相关FRs

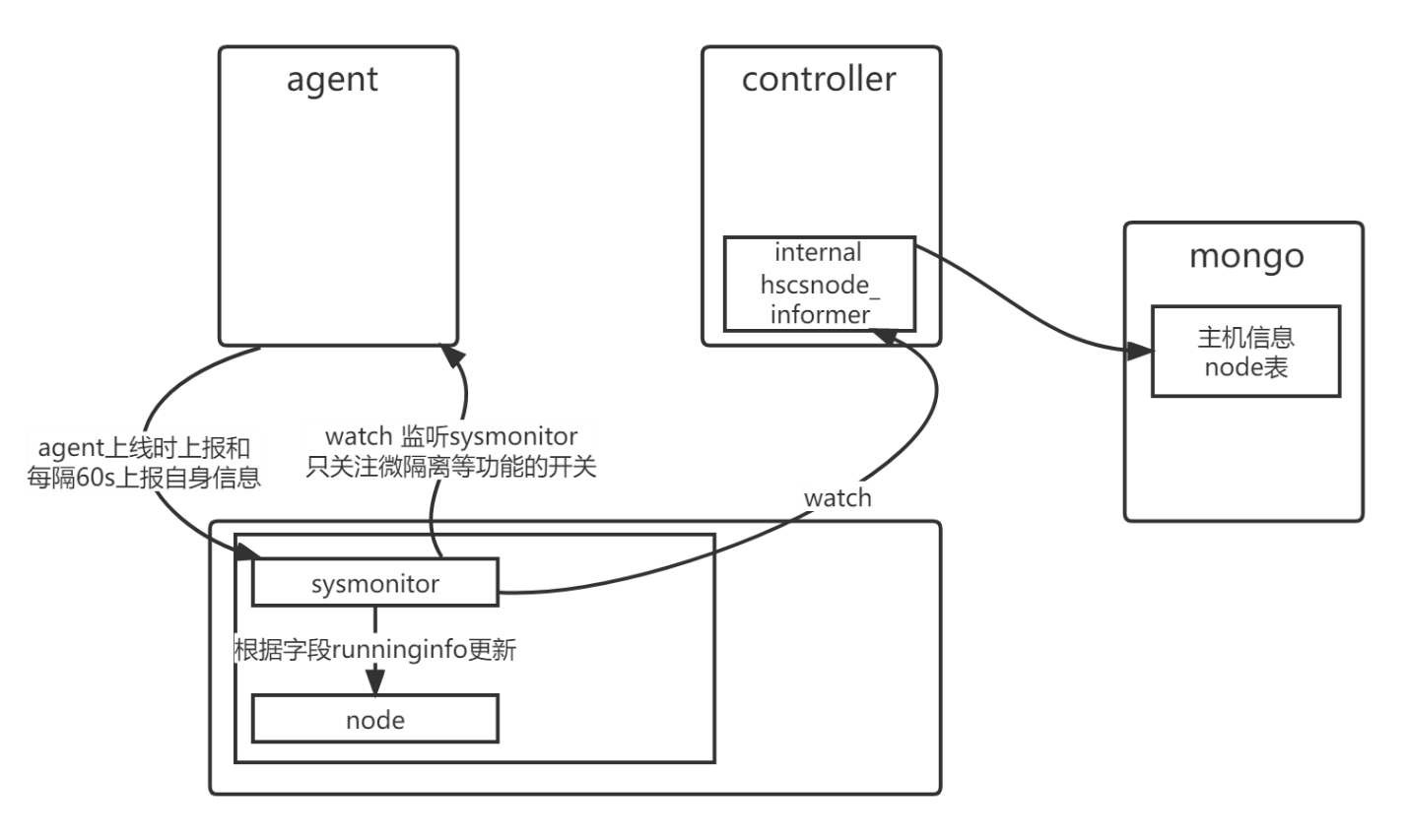
# 软件支持平台

## 支持的OS/CPU

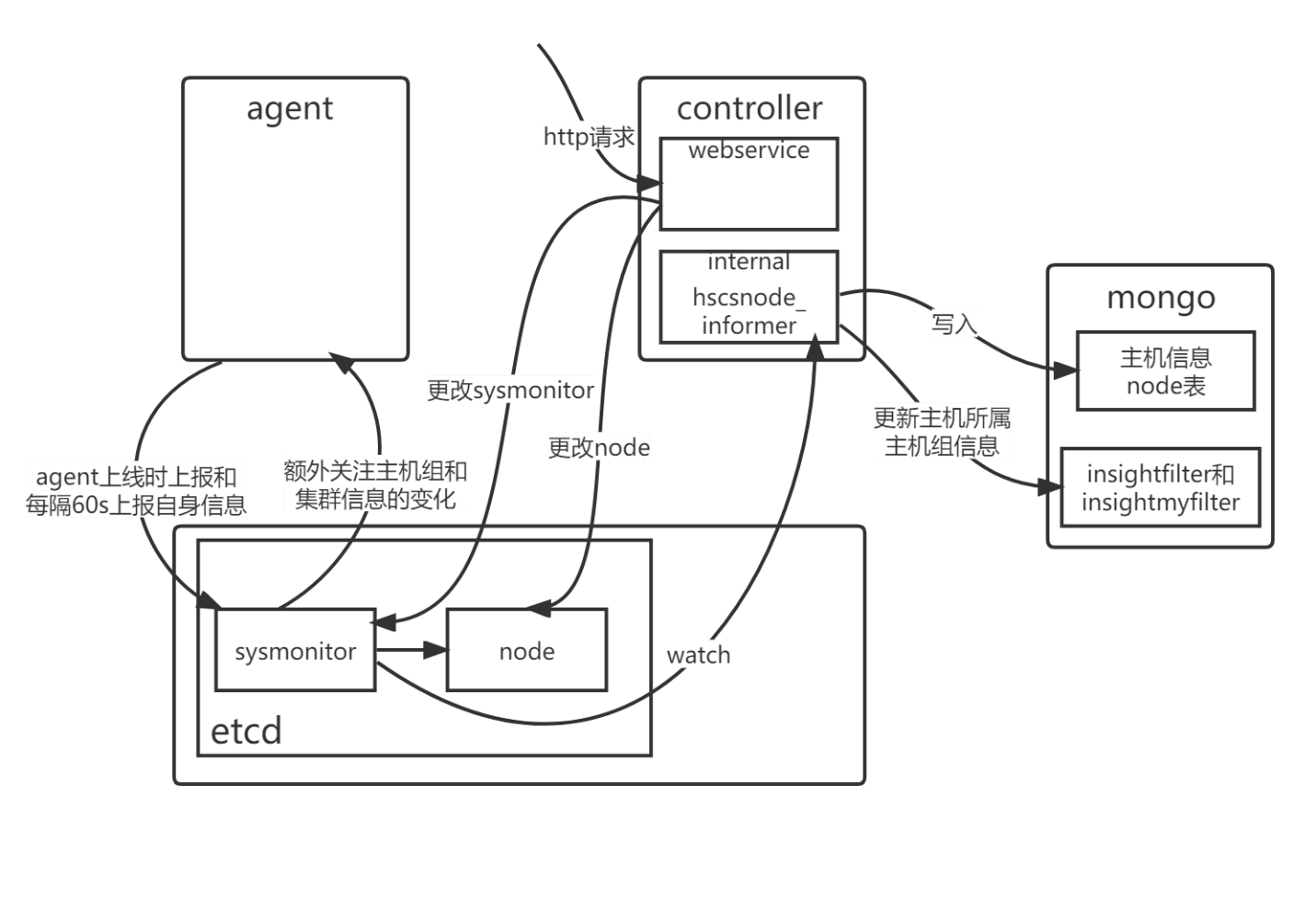
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OS | CPU Arch | Kernel Version | Release | Supported（Yes/No） |
| Linux | X86-64 | > 4.10 | Ubuntu 14.04/16.04/18.04  Centos XXX  Suse XXX | Yes |
| Linux | ARM64 |  | 麒麟 Linux V10服务器版本 | No |
| Windows Server | AMD64 | N/A | 2012/2016/2019 | Yes |

# 软件架构和总体框图

更改前 主机信息流转图



更改后的主机信息 流转图



# 模块详解

系统内主机组信息更新流程：

1. 更新node和sysmonitor资源， 只要这两个资源更新成功，api返回的结果就是success。
2. 其他模块中缓存的主机信息修改同步进行， 如果发生错误，不会影响api返回的结果， 通过log反馈。
3. Agent通过监听sysmonitor资源的变化来感知集群和主机组信息的变化。
4. Agent信息上报时，只有create 一个sysmonitor资源的时候才会带上自己的clusterName和hostGroup信息。 Update sysmonitor资源的时候不会覆盖原有的cluster和hostgroup信息。

# 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

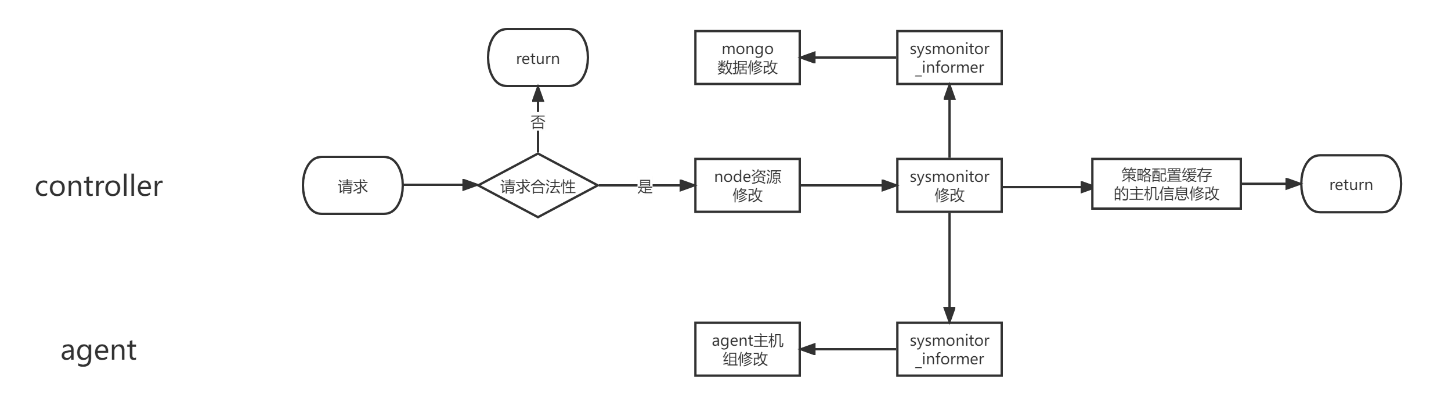
1. Config\_channel端主机组信息修改完成， agent修改失败的情况：

Agent上线的时候， 查看自身agentID对应的sysmonitor资源， 如果sysmonitor资源的主机组集群和agent端信息不一样， 修改agent自身缓存的信息。

# 功能详述

## 主机组归属信息修改

### 实现方法



#### 主机移动请求校验

设计IsMoveHostAvailable(agentID, hostGroup, clusterName string)函数 校验移动主机的请求是否合法， 包括一下几个内容：

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， 判断当前project下是否存在对应agentID的node资源， 判断该agent所在集群下是否存在对应hostGroup的baseHostGroup资源。
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. 上述校验合法后同步修改node资源和sysmonitor资源（先修改node资源后修改sysmonitor资源）。

#### 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。设计IsAgentTaskRuning（agentid string）函数判断该agent是否有任务运行。

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hostvulnscannodeinfo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。

#### 修改Agent端缓存的集群和主机组信息

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。

新增UpdateAgentCache(cluster string, hostgroup string)函数修改agent端保存的信息。

* 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。
  3. 修改/agent/go/internal/hcnf/internal/hcnf/init.go 中定义的MyCluster和MyHostGroup缓存信息。
  4. Ues那边是不是需要修改？
  5. 或则只修改product.yaml文件， 让curator进程重启一次。

1. Agent向config\_channel上报自身信息的时候，只有create 一个sysmonitor资源的时候才会带上自己的clusterName和hostGroup信息。 Update sysmonitor资源的时候不会覆盖原有的cluster和hostgroup信息。

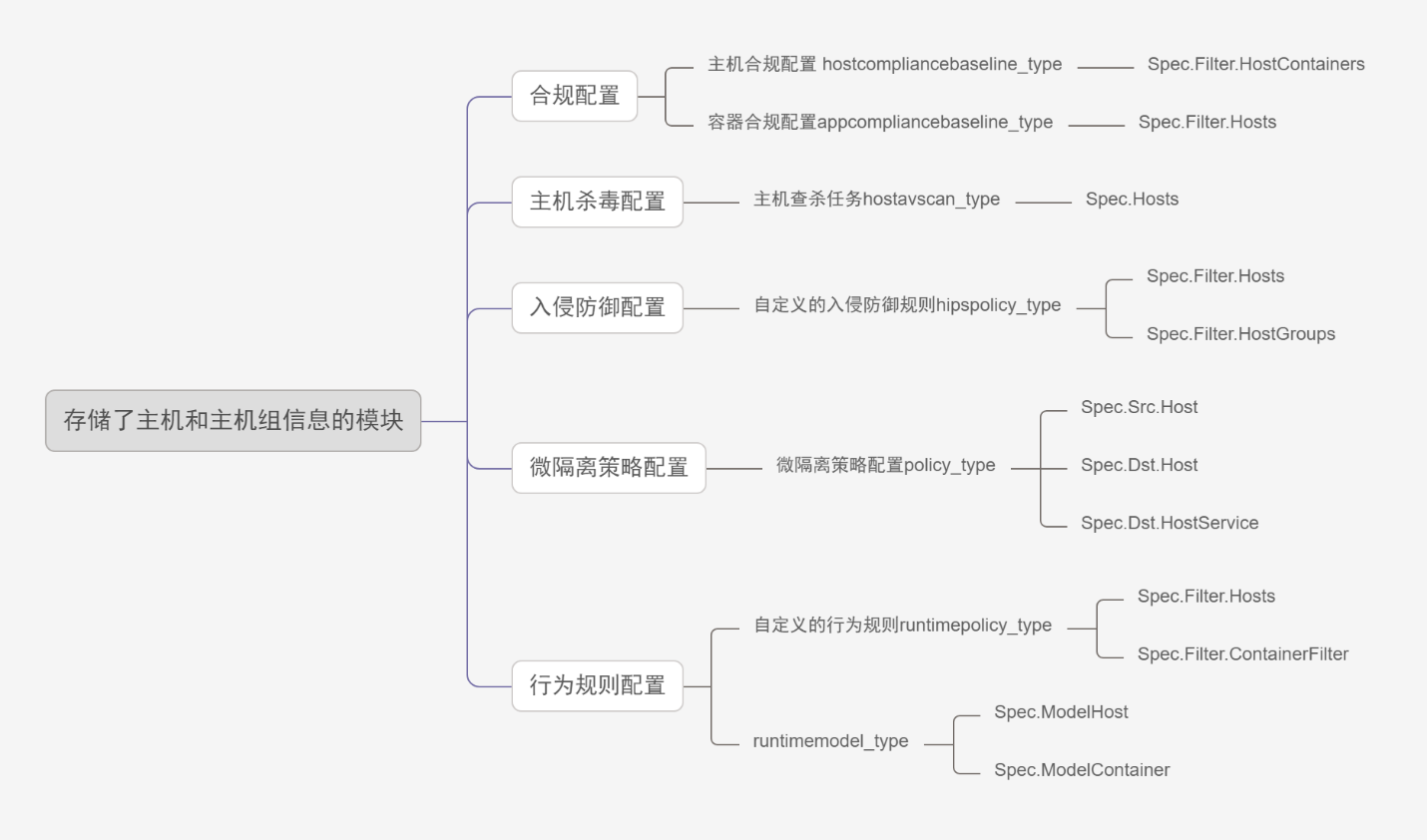
#### mongo中主机信息node表更新

现在controller会watch sysmonitor资源， 会更根据变化的sysmonitor资源和node资源来更新mongo里的node表。

#### 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。

## 策略配置自动跟随



### 实现方法

设计UpdateOtherMoudleHostCache()函数 修改其他模块中缓存的主机信息， 对不同模块的不同资源进行更新可以异步展开。

这部分内容的更新如果出现错误失败不会影响返回结果， 通过debug或log系统反馈哪一部分的信息更新失败了。

#### 主机组转移后合规 杀毒配置立即更新

1. 合规配置中主机合规和容器合规涉及到了主机组信息的存储
   1. 主机的主机组被修改后， 查找主机合规配置HostComplianceBaseline资源中是否存储了和该主机有关的信息HostFilter 并修改
   2. 查找容器合规配置AppComplianceBaseline资源的spec.Filter.HostContainers字段。
2. clientset.ComplianceV1().HostComlianceBaseline(project).List(meta1.ListOptions{FileldSelector: string})获取缓存了对应agentID主机信息的资源列表。 遍历修改缓存的信息。

#### 入侵防御 微隔离 行为规则配置立即更新

1. 入侵防御策略资源/config\_channel/pkg/apis/atp/v1/hipspolicy中存储的主机信息和主机容器信息。
2. 微隔离策略资源/config\_channel/pkg/apis/cnnf/v1/policy\_types.go中存储的源和目的的过滤器。
   1. 源PlcSrc过滤器中的Host
   2. 目的PlcDst过滤器中的Host HostService
3. 行为规则配置资源
   1. /config\_channel/pkg/apis/runtimesec/v1/runtimepolicy\_type.go中存储的主机过滤器HostFilter和主机容器过滤器ContainerFilter
   2. /config\_channel/pkg/apis/runtimesec/v1/runtimemodel\_type.go 中存储的 ModelContainer ModelHost

## 透视镜和其他统计模块更新

### 实现方法

#### 微隔离透视镜显示方案修改

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。
2. Mongo查数据改数据的大致代码实现。

#### 合规 漏扫 杀毒结果下次扫描更新

Mongo中的旧数据不做修改。

## 日志信息更新

### 实现方法

#### 入侵防御 微隔离 行为规则安全事件日志

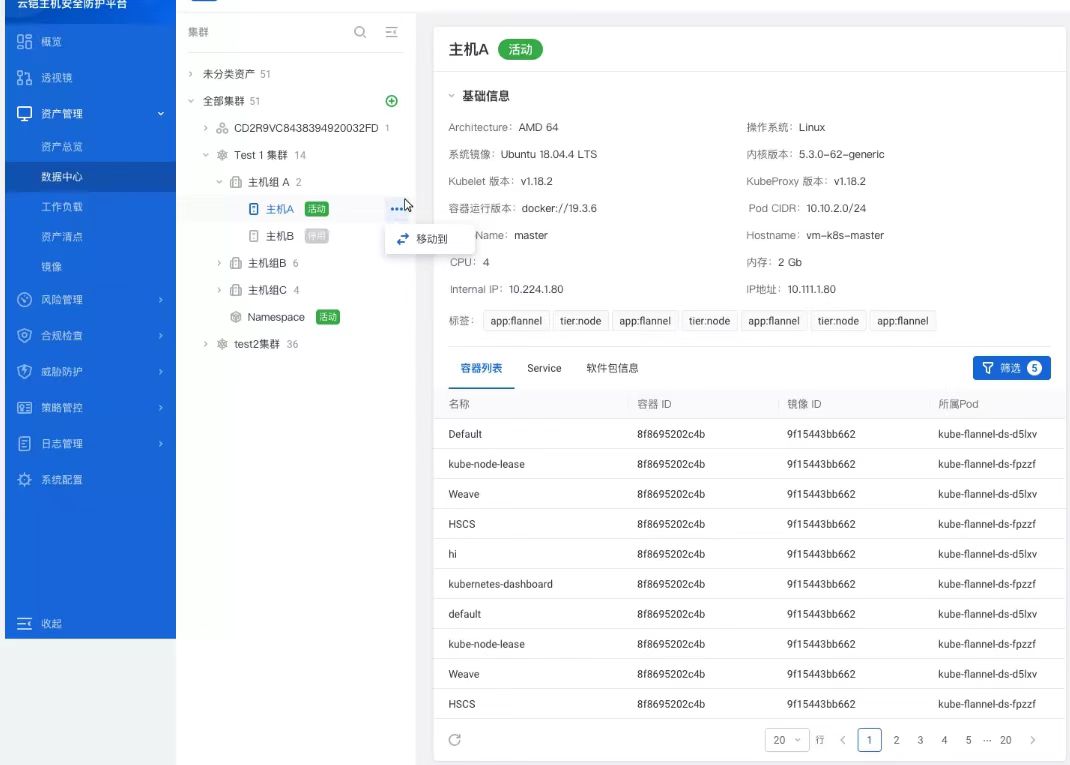
1. 微隔离安全事件中集群和主机组信息的来源是/agent/pkg/common/config/config\_parse.go的全部配置信息。 在watch sysmonitor资源的时候更新过了。
2. 入侵防御 行为规则安全事件中的集群主机组信息来源是runtimemodel资源中存储的clustername和hostgroup。

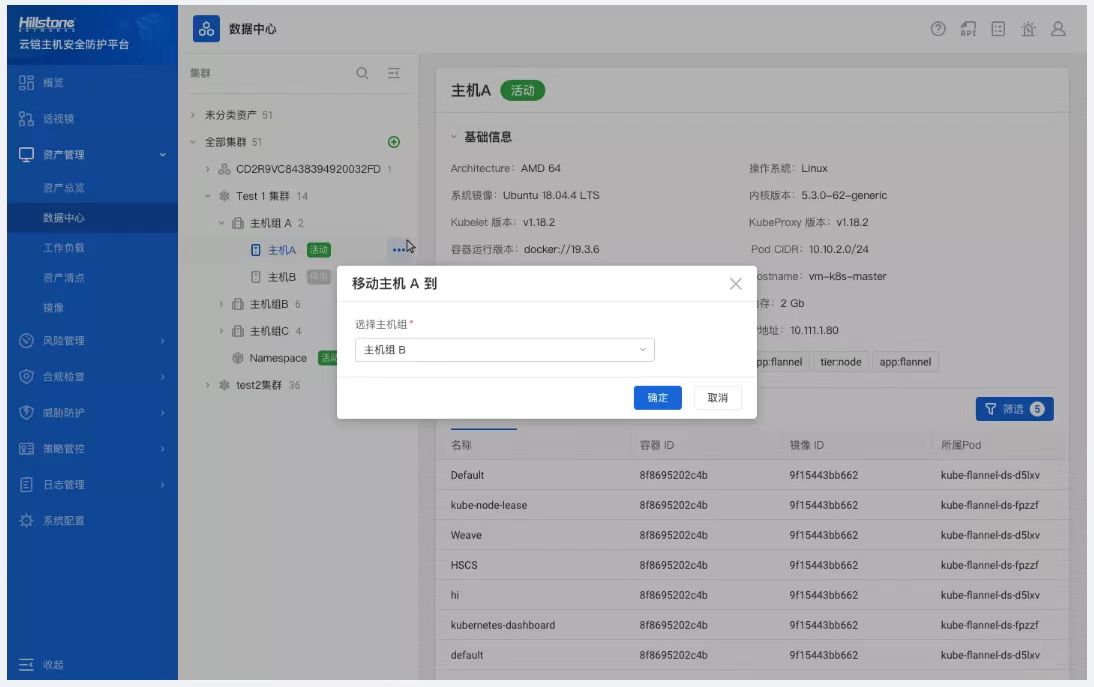
#### 其他日志

1. Agent端在打印日志时获取集群和主机组信息的方式有：
   1. 获取/agent/go/internal/assets/internal/defenderassets/xxx.go 缓存的信息
   2. 获取/agent/pkg/common/config/config\_parse.go 定义的全局配置信息变量\*ConfigRoot。

## 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/hostSvc |
| 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 | 主机需要转移到的主机组。 | | clusterName | string | 未分类主机需要转移进的集群。只有未分类主机会看这个字段。 | |
| 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 | | 批量修改sysmoniotr资源和node资源主机组信息的接口信息 PUT | | | |
| url | | /rest/system/hostSvc | | | |
| 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。 | | ClusterName | string | 未分类主机需要转移进的集群。只有未分类主机会看这个字段。 | | | | |
| 返回结果 | | Success example   |  | | --- | | {  Total: 1, //移动失败的数量  Result: [ “001” ], //移动失败的agentid  } |   Fail example   |  | | --- | | {  Code: int  Msg: string  Detail: string  } | | | | |
| 错误处理 | | 错误码 | 字段 | 描述 | |
| 250011 |  | 传入的数组中agentID有重复 | |
|  | |  |  |  | |
|  | |  |  |  | |
|  | |  |  |  | |
|  | |  |  |  | |

### Debug

### SYSLog

|  |  |  |
| --- | --- | --- |
| *Severity*  *（严重度）* | *English（英文）* | *Chinese（中文）* |
| LOG\_INFO | Move Host:  “clusterName\_GroupName\_hostname”  To  “clusterName\_NewGroupName\_hostname”  success | 移动主机：  “clusterName\_GroupName\_hostname”  到  “clusterName\_NewGroupName\_hostname”  成功 |
| LOG\_ERR | Move Host:  “clusterName\_GroupName\_hostname”  To  “clusterName\_NewGroupName\_hostname”  Fial | 移动主机：  “clusterName\_GroupName\_hostname”  到  “clusterName\_NewGroupName\_hostname”  失败 |

### 黑盒测试考虑

1. 转移主机到不合法的主机组， 验证是否拒绝此请求
2. 转移主机后， 检查资产数据中心显示是否更新， 检查微隔离等策略是否自动跟随， 检查后续产生的日志和事件结果是否按照新的主机组归属产生
3. 在agent非在线状态进行转移请求， agent上线后能否更新。

### 白盒测试

1. 测试IsAgentTaskRunning()函数能否检测agent的任务工作状态
2. 测试IsMoveHostAvailable()函数能否检测主机移动是否合法。
3. 测试修改 product.yaml文件的函数

# 功能限制

对集群和主机组信息进行缓存的模块很多，对主机的主机组信息进行修改， 会修改很多资源。 如果修改某一个资源的时候失败了， 可能会出现一部分资源的主机组信息更新了，另一部分没有更新。

将更新资源失败的情况通过debug或log信息反馈给用户。

# 典型用户配置N/A

# 测试考虑

# 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