睿石云 WAF

犀盾产品快速配置手册

睿石网云（北京）科技有限公司

2017 年 08 月 29 日

声明

- 本手册所含内容若有任何改动，恕不另行通知。
- 在法律法规的最大允许范围内，**睿石网云（北京）科技有限公司**除就本手册和产品应负的瑕疵担保责任外，无论明示或默示，不作其它任何担保，包括（但不限于）本手册中推荐使用产品的适用性和安全性、产品的适销性和适合某特定用途的担保。
- 在法律法规的最大允许范围内，**睿石网云（北京）科技有限公司**对于您的使用或不能使用本产品而发生的任何损坏（包括，但不限于直接或间接的个人损害、商业利润的损失、业务中断、商业信息的遗失或任何其它损失），不负任何赔偿责任。
- 本手册含受版权保护的信息，未经**睿石网云（北京）科技有限公司**书面允许不得对本手册的任何部分进行影印、复制或翻译。

睿石网云(北京)科技有限公司

章节目录

1. 云 WAF 介绍

1.1. 云 WAF 组成

云 WAF 系统由三部分组成：集中管理 **RManager、态势分析 RSight、WAF 节点 RNode**

1) **集中管理 RManager：**对 WAF 节点进行管理配置，包括站点管理、防护策略配置等；
2) **态势分析 RSight：**接收所有 WAF 节点的日志，对网站的访问和攻击情况进行态势分析；
3) **WAF 节点 RNode：**具备 WAF 功能，根据 RManger 下发的策略针对性防护。

1.2. 云 WAF 管理

1) RManager 和 Rsight 可以通过浏览器进行管理和配置；
2) RManager 和 Rsight 默认 WEB 登录用户名 **admin** 密码 **admin123**；
3) RManager 超级 WEB 登录用户名 **RSCloudWAF** 密码 **admin123**；
4) RManager、Rsight、RNode 系统后台登录用户名 **root** 密码 **111111**；
5) 建议使用的客户端浏览器类型是：**谷歌 Chrome；**

2. 配置思路

(一) 正确配置集中管理 RManager、态势分析 RSight、WAF 节点 RNode 的管理 IP 地址，并能互通；

(二) 登录集中管理 RManager 依次配置租户、证书、安全策略、站点管理、WAF 节点管理；

(三) 在集中管理 RManager 中，对添加的 WAF 节点进行授权、host 数量授权；

(四) 在集中管理 RManager 中，系统—高级选项—Rsight 访问和节点配置中，配置数据中心地址为态势分析 Rsight 的地址；

(五) 在集中管理 RManager 中，WAF 节点模块点击配置下发，将已经配置好的站点和安全策略下发给 RNode；

(六) 上述配置完成后，RNode 工作在反向代理模式下，更改对应网站的 DNS 解析到 RNode 的 IP 上面，此时访问域名或者 RNode 的 IP 地址就能访问到网站；

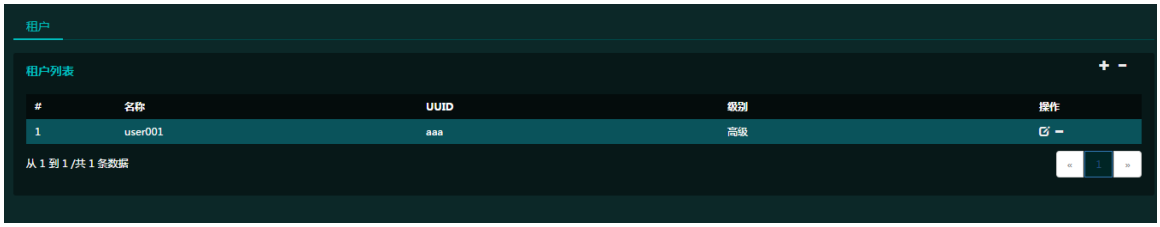
(七) 网站能正常访问后，登录态势分析 Rsight 可以看到相应的访问日志；

3. 配置步骤

3.1. 租户

新建租户，（*在实际云环境中该 UUID 是云平台租户的唯一标示，由云平台下发，故实际云环境下此租户信息由云平台下发不用配置*）：

- 新建租户，操作路径：点击“R>>租户”，界面如下：



点击  按钮添加租户，添加界面如下：

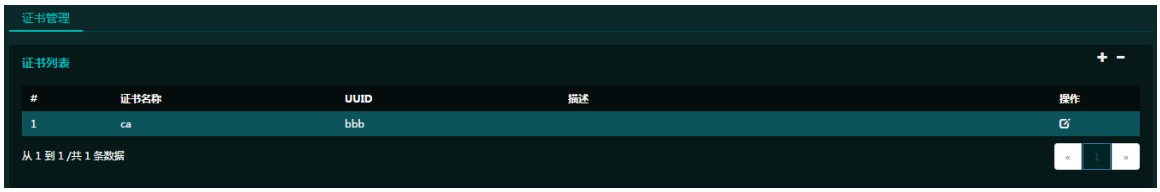
注意：

租户配置中的 UUID 必须唯一，且在其他功能配置中如果有涉及 UUID，说明该功能允许租户配置，并且每个租户输入自己的 UUID 后，只能看到自己定义的内容，其他租户的看不到，所以此 UUID 涉及后续相关功能调用，必须配置准确。

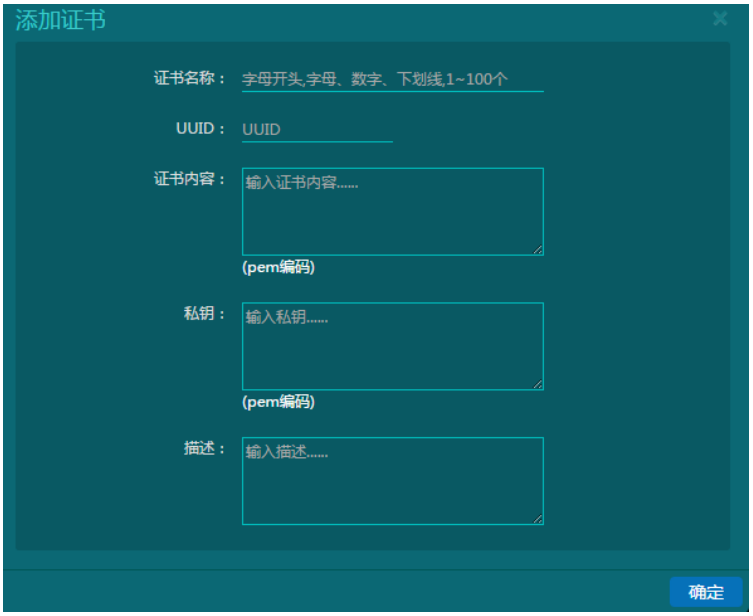
3.2. 证书

新建证书，非 HTTPS 网站可忽略此步骤：

- 操作路径：点击“R>>证书”，界面如下：



点击  按钮添加证书，界面如下：



3.3. 规则集

新建安全规则，防护规则的配置：

- 操作路径：点击“R>>规则”，该模块下创建的规则被‘规则集’调用安全策略集默认提供 3 种防护规则：高级防护、中级防护和基本防护，默认防护规则无法编辑删除。

点击  按钮添加规则集，当没有创建自定义规则时，可引用默认规则。

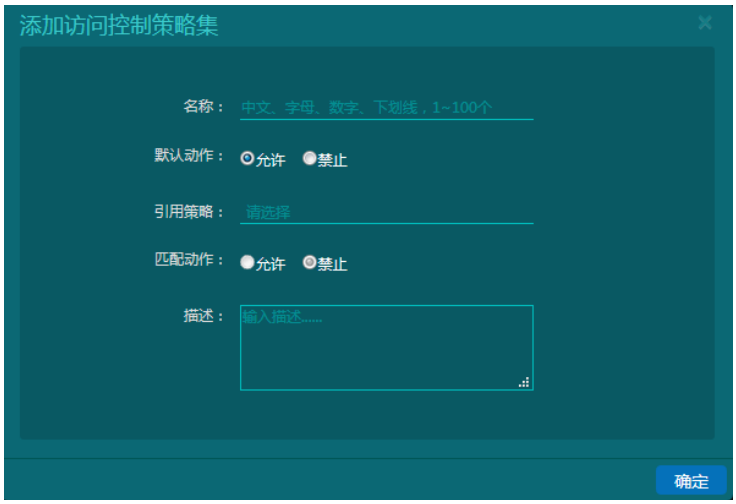
3.4. 访问控制

新建访问控制策略集及访问控制策略：

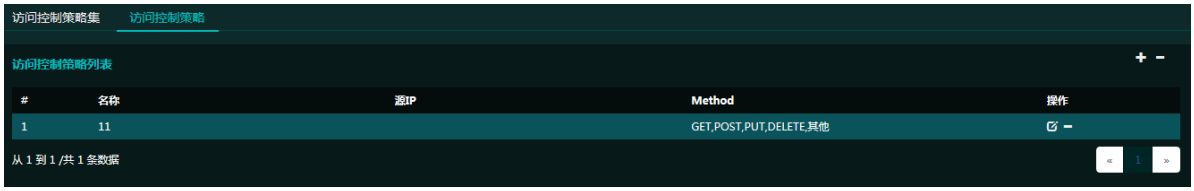
- 操作路径：点击“R>>访问控制”，界面如下：

该模块下‘访问控制策略’创建的规则被‘访问控制策略集’调用，如图：

点击  按钮添加访问控制策略集，添加界面如下：



其中‘引用策略’在‘访问控制策略’一栏中创建，如下：



点击  按钮添加‘访问控制策略’

3.5. 站点

新建站点，涉及网站 IP 端口及域名的关联配置：

- 操作路径：点击“R>>站点管理”，界面如下：

站点管理模块下有‘站点’、‘HOST’、‘物理服务器&集群’3 个子模块，‘站点’引用‘HOST’和‘物理服务器&集群’中的数据，具体配置步骤如下：

1) 配置物理服务器&集群，添加网站的 IP 地址和端口，如果有多台进行负载均衡，那么以集群方式添加；

2) 配置 HOST，该 HOST 是指网站域名，如果网站有多个域名可以添加到 HOST 组；

3) 配置站点，新建站点，把对应的 HOST、安全策略、物理服务器、租户进行关联；

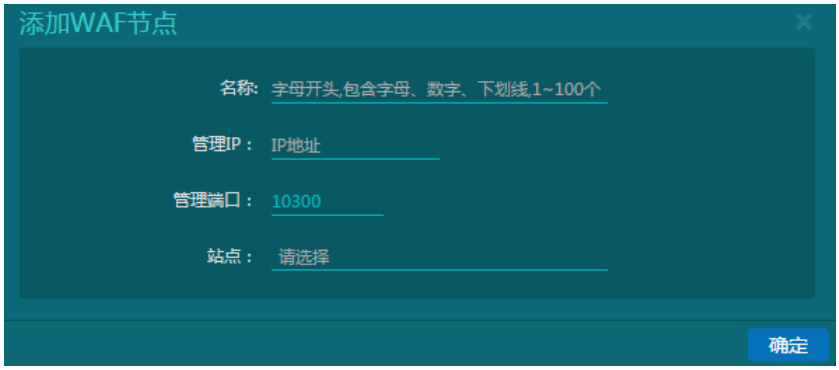
4) 注意 HOST 的 UUID 要和对应租户的 UUID 是一致的；

3.6. WAF 节点

新建 WAF 节点，添加 RNode WAF 节点，并关联对应的站点策略：

➢ 操作路径：点击“R>>WAF 节点”，界面如下：

点击  按钮添加 WAF 节点，添加界面如下



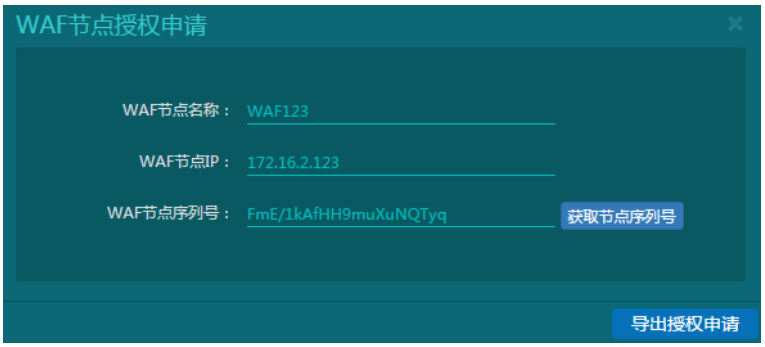
- **管理 IP：**添加 RNode 的 IP；

- **站点：**选择文档中 3.5.2 中创建的站点。

3.7. WAF 节点授权

节点新建完成后，WAF 节点属于未授权状态，无法下发，如图：

需授权后才能下发，点击  按钮出现弹窗，界面如图：



点击 

按钮，会自动生成申请文件并下载，**将申请文件发送给睿石公司制作授权文件**，点击  按钮出现弹窗，将授权文件导入，界面如图：

授权成功后，授权状态会由  变为  ，点击  下发配置到 RNode

下发成功状态为  ，下发失败状态为由  。

3.8 HA 设置

添加 HA 策略，需关联 RNode WAF 节点，HA 策略的部署模式通常为主备模式，需建立两条 HA 策略，关联

两个 waf 节点

➢ 操作路径：点击“R>>HA 设置”，界面如下：

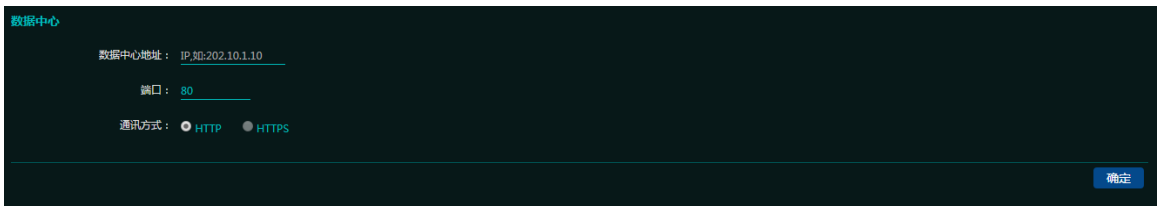
点击  按钮添加 HA 策略，添加界面如下

WAF 节点：选择关联的 node 节点
心跳口：选择 node 节点上任一的接口
组 ID：为 HA 策略的组 ID
监控网口：为 node 节点的监控网口
选择开启：则开启 HA 策略

3.9 日志接收配置

在 RManager 中配置 RSight 数据接收中心地址：

➢ 操作路径：点击“R>>系统>>高级选项>>RSight 访问”，界面如下：

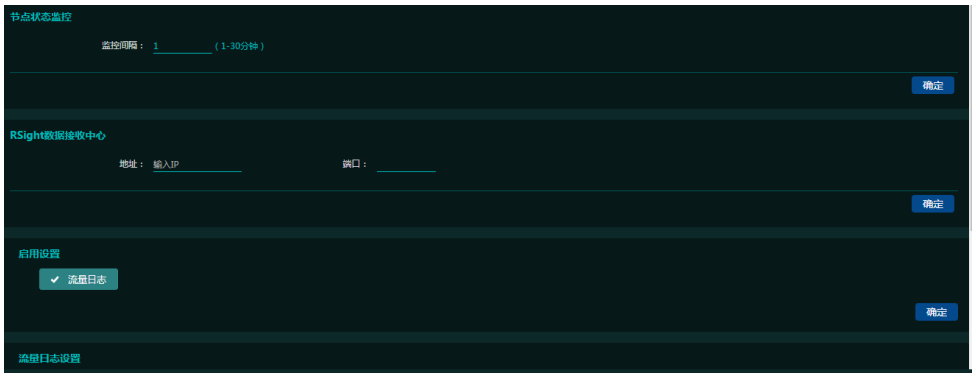


- **数据中心地址：**添加 RSight 的 IP 地址；

- **端口：**默认 80 端口；
- **请求方式：**默认 HTTP。

配置完成够点击‘确定’按钮。

➢ 操作路径：点击“R>>系统>>高级选项>>节点配置”，界面如下：



- **地址：**填写 RSight 的 IP 地址；
- **端口：**填写 RSight 数据接收端口，默认 514 端口。

配置完成够点击‘确定’按钮。

4. 关于 RStone 睿石

睿石网云（北京）科技有限公司（简称“RStone 睿石”）是一家以应用监控管理和 WEB 应用安全技术为核心，专注于云安全和企业级 APM 应用性能监控的创新型高科技企业，核心成员均来自全球一流安全厂商，在云安全、网络和应用性能监控、大数据等领域，具有深厚技术积淀和丰富应用经验。

公司聚焦于网络性能监控和诊断（NPMD）、应用性能监控（APM）产品和 WEB 安全产品，面向当前云计算、虚拟化、大数据、移动互联网络、智慧城市、物联网等方面应用的迅猛发展，提供富有技术前瞻性的云安全、APM & NPM、智能运维解决方案，全面适用政府、金融、能源、医疗、运营商、教育、军工、大中型企业等行业市场。

目前，公司拥有 50 多项知识产权和重要资质，包括：国家高新技术企业认证、公安部安全专用产品销售许可证、国家保密局涉密信息系统证书、软件著作权项、发明技术专利等，以国内领先的技术架构，高效能的研发体系和完备的精益管理工具，持续驱动产品技术的迭代发展。

“睿达卓见，心如磐石”，RStone 睿石将立足全球视野，倾力打造属于中国云时代的卓越产品。

总部地址：北京市海淀区上地三街九号嘉华大厦 A1202

公司官网：www.rstonenet.com

服务热线：400-060-1565 **总机电话：（010）6297 9676**

销售邮箱：sales@rstonenet.com **技术支持邮箱：support@rstonenet.com**