API

计划任务

获取计划任务列表

```
GET /jobs
```

```
{
  "jobs": [{
    "jobkey": String,
    "cron": String,
    "count": Number,
    "start_at": Number(epoch_millis)
  }, ...]
}
```

获取指定的计划任务

```
GET /jobs/:jobkey
```

```
{
  "job": {
    "jobkey": String,
    "cron": String,
    "count": Number,
    "start_at": Number(epoch_millis)
  }
}
```

系统配置

获取系统配置

```
GET /config
```

```
{
  "config": {
    # 主机发现的目标网络，nmap的target语法
    "hs:network": String,
    # 执行时间，使用cron描述
    "hs:hostDetection:cron": String,
    # 自动探测操作系统
    "hs:osDetection:auto": Boolean,
    # 探测操作系统的并行数量
    "hs:osDetection:parallel": Number,
    # 探测操作系统的结果缓存时间
    "hs:osDetection:cache:ttl": Boolean,
    # 自动探测端口服务版本
    "hs:versionDetection:auto": Boolean,
    # 探测端口服务版本的并行数量
    "hs:versionDetection:parallel": Number,
    # 探测端口服务版本的结果缓存时间
    "hs:versionDetection:cache:ttl": Boolean,

    "ids:vars:address-groups": {
      "HOME_NET": "
[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]",
      "EXTERNAL_NET": "!$HOME_NET",
      "HTTP_SERVERS": "$HOME_NET",
      "SMTP_SERVERS": "$HOME_NET",
      "SQL_SERVERS": "$HOME_NET",
      "DNS_SERVERS": "$HOME_NET",
```

```
        # 变量可任意添加
        # "TELNET_SERVERS": "$HOME_NET",
        # "AIM_SERVERS": "$EXTERNAL_NET",
        # "DNP3_SERVER": "$HOME_NET",
        # "DNP3_CLIENT": "$HOME_NET",
        # "MODBUS_CLIENT": "$HOME_NET",
        # "MODBUS_SERVER": "$HOME_NET",
        # "ENIP_CLIENT": "$HOME_NET",
        # "ENIP_SERVER": "$HOME_NET"
      },

      "ids:vars:port-groups": {
        # 变量可任意添加
        "HTTP_PORTS": "80",
        "SHELLCODE_PORTS": "!80",
        "ORACLE_PORTS": 1521,
        "SSH_PORTS": 22,
        "DNP3_PORTS": 20000,
        "MODBUS_PORTS": 502
      },
      "ids:enable-rule": [
        "botcc.rules",
        "ciarmy.rules",
        "compromised.rules",
        "drop.rules",
        "emerging-sql.rules",
        "emerging-user_agents.rules"
      ]
    }
  }
```

更新系统配置

```
PUT /config
PATCH /config
```

```
{
  "config": {
    # 主机发现的目标网络，nmap的target语法
    "hs:network": String,
    # 执行时间，使用cron描述
    "hs:hostDetection:cron": String,
    # 自动探测操作系统
    "hs:osDetection:auto": Boolean,
    # 探测操作系统的并行数量
    "hs:osDetection:parallel": Number,
    # 探测操作系统的结果缓存时间
    "hs:osDetection:cache:ttl": Boolean,
    # 自动探测端口服务版本
    "hs:versionDetection:auto": Boolean,
    # 探测端口服务版本的并行数量
    "hs:versionDetection:parallel": Number,
    # 探测端口服务版本的结果缓存时间
    "hs:versionDetection:cache:ttl": Boolean,

    "ids:vars:address-groups": {
      "HOME_NET": "
[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]",
      "EXTERNAL_NET": "!$HOME_NET",
      "HTTP_SERVERS": "$HOME_NET",
      "SMTP_SERVERS": "$HOME_NET",
      "SQL_SERVERS": "$HOME_NET",
      "DNS_SERVERS": "$HOME_NET",
      # 变量可任意添加
      # "TELNET_SERVERS": "$HOME_NET",
      # "AIM_SERVERS": "$EXTERNAL_NET",
      # "DNP3_SERVER": "$HOME_NET",
      # "DNP3_CLIENT": "$HOME_NET",
      # "MODBUS_CLIENT": "$HOME_NET",
      # "MODBUS_SERVER": "$HOME_NET",
      # "ENIP_CLIENT": "$HOME_NET",
      # "ENIP_SERVER": "$HOME_NET"
    },
```

```
    "ids:vars:port-groups": {
      # 变量可任意添加
      "HTTP_PORTS": "80",
      "SHELLCODE_PORTS": "!80",
      "ORACLE_PORTS": 1521,
      "SSH_PORTS": 22,
      "DNP3_PORTS": 20000,
      "MODBUS_PORTS": 502
    },
    "ids:enable-rule": [
      "botcc.rules",
      "ciarmy.rules",
      "compromised.rules",
      "drop.rules",
      "emerging-sql.rules",
      "emerging-user_agents.rules"
    ]
  }
}
```

服务节点信息（包括agent和node）

获取所有服务节点信息

```
# 获取所有服务节点
GET /bismuth
# 仅获取agent
GET /bismuth?type=agent
# 仅获取node
GET /bismuth?type=node
```

```
{
  "bismuths": [{
    "id": String
```

```
    # 可以是`hs`, `ids` `node`的组合
    "mode": ["hs", "ids", "node"],
    "ipaddr": String,
    "last_online": Number(epoch_millis)
  }, ...]
}
```

获取指定的服务节点信息

```
GET /bismuth/:id
```

```
{
  "bismuths": {
    "id": String
    # 可以是`hs`, `ids` `node`的组合
    "mode": ["hs", "ids", "node"],
    "ipaddr": String,
    "last_online": Number(epoch_millis)
  }
}
```

内网扫描代理的运行状态

获取内网扫描代理的运行状态（仅在运行模式包含hs时有效）

```
GET /hs_status
```

```
{
  "hs_status": {
    # 操作系统探测队列中的缓存数量
```

```
    "os_detectoin_queue": Number,
    # 已缓存的主机
    "os_cache": [
      <host_ip>,
      ...
    ],
    # 端口及服务版本探测队列中的缓存数量
    "version_detectoin_queue": Number,
    "version_cache": [
      <host_ip>,
      ...
    ]
  }
}
```