**安徽省自然资源厅**

**“护网2019”监测报告表**



**安徽三实信息技术服务有限公司**

**修改记录：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **时间** | **版本** | **编写/修改人员** | **审核人员** | **备注** |
| 2019.07.31 | V1.0 | 韩无贤 | 蔡飞 | 创建该文档 |
|  |  |  |  |  |
|  |  |  |  |  |

**受控范围：**

|  |  |  |
| --- | --- | --- |
| **查阅对象** | **权限** | **备注** |
| 用户 | 读取、归档 |  |
| 公司员工 | 读取 |  |
| 韩无贤 | 读取、修改 |  |
| 公司其他主管 | 读取、审核 |  |
| 三实文档管理员 | 读取、归档 | 三实公司归档 |

# 监测规范

**汇报负责人：**张伟

**汇报对象：**国土厅安全服务群(QQ群)、潘柳

**监测对象：**参看执行表

**监测时间：**2019年7月30日-8月31日(非工作日也持续) 8:00-17:30；

**监测格式：**认真填写监测执行表，做好截图存证工作，**保证网站可用性截图中包含当前系统时间；**

**汇报形式及频度：**

* 无问题时每日12:00，17:30计两次在QQ群中汇报；每日汇报邮件内容写清安全监测汇总并附上当日监测执行表；每周汇总在项目周报中体现；
* 发现严重问题时第一时间电话联系厅安全负责人和业务开发方进行跟进处置，并在处置完成后做专门汇报；

**汇报内容：**可用性检查结果、安全监测执行结果汇总、有无监测项的异常波动及其他有必要汇报的情况；

**汇报格式示例：**

* 无异常情况汇报示例1：经监测，xx月xx号，上午8:00-17:00，未发现安全预警；网站可用性正常，相关服务器和安全设备流量、硬件性能正常，安全监测指标未发现明显波动（若安全事件有则需写明重要内容），云防护拦截攻击次数XXXX次。
* 无异常情况汇报示例2：经监测，：xx月xx号，网站可用性于09:00-09:15出现异常，相关服务器和安全设备流量、硬件性能正常，安全监测指标未发现明显波动（若安全事件有则需写明重要内容），云waf拦截攻击次数XXXX次。**(于此处附加网站可用性异常处置详细说明)**

# 网站可用性及预警监测

**监测频率：**30分钟执行一次

## 检测时间：08:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 1 |
| 内网厅网站-2 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 1 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 | 1 |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 | 1 |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 | 1 |

## 检测时间：08:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 2 |
| 内网厅网站-2 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 2 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 | 2 |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 | 2 |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 | 2 |

## 检测时间：09:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 3 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 3 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：09:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 4 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 4 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：10:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 5 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 5 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：10:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 6 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 6 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：11:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 7 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 7 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：11:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 8 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 8 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：12:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 9 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 | 9 |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：12:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 10 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：13:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 11 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：13:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 12 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：14:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 13 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：14:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 14 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：15:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 15 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：15:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 16 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：16:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 17 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：16:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 18 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：17:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 19 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

## 检测时间：17:30

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 内网厅网站-1 | 网址 | http://192.168.253.2 | 可用性 | 浏览器打开页面正常 | 网站-1可用性正常 | 20 |
| 内网厅网站-2 | 网址 | http://192.168.253.31 | 可用性 | 浏览器打开页面正常 | 网站-2可用性正常 |  |
| 厅网站域名 | 网址 | http://zrzyt.ah.gov.cn | 可用性 | 浏览器打开页面正常 | 厅网站域名-可用性正常 |  |
| 征地平台域名 | 网址 | http://zrzyt.ah.gov.cn/zd/pqxxgk/index.jsp | 可用性 | 浏览器打开页面正常 | 征地平台域名-可用性正常 |  |
| 厅网站IP | 网址 | http://112.122.8.2 | 可用性 | 浏览器打开页面正常 | 厅网站ip-可用性正常 |  |

# 服务器及安全设备监测

**监测频率：**3小时执行一次

## 监测时间：08:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 厅门户网站服务器-1（地调中心） | 服务器 | 192.168.253.2 | 图形界面 | 正常登录，无卡顿 | 端口状态正常 |  |
|  |  |  | CPU使用率 | 基线值为：20%。 | 最大值为5.49%，属于正常值。 |  |
|  |  |  | 内存使用率 | 基线值为：25%。 | 最大值为13.9%，属于正常值。 |  |
| 厅门户网站服务器-2 | 服务器 | 192.168.253.31 | 图形界面 | 正常登录，无卡顿 | 端口状态正常。 |  |
|  |  |  | CPU使用率 | 基线值为：35% | 最大值为18.18%，属于正常值 |  |
|  |  |  | 内存使用率 | 基线值为：75%。 | 最大值为72.91%，属于正常值 |  |
| 厅网站数据库服务器 | 服务器 | 192.168.253.11 | 图形界面 | 数据库服务端口是否正常 | 端口状态正常 |  |
|  |  |  | CPU使用率 | 基线值为：2.0% | 最大值为：0.95%，属于正常值。 |  |
|  |  |  | 内存使用率 | 基线值为：12% | 最大值为：8.93%，属于正常值。 |  |
| 厅网站备份服务器 | 服务器 | 192.168.253.43 | 图形界面 | 正常登录，无卡顿 | 服务器远程登陆正常 |  |
|  |  |  | CPU使用率 | 基线值为：15% | 最大值为：7.14%，属于正常值。 |  |
|  |  |  | 内存使用率 | 基线值为：20% | 最大值为：9.13%，属于正常值。 |  |
| 征地平台服务器 | 服务器 | 192.168.253.17 | 图形界面 | 正常登录，无卡顿 | 端口状态正常 |  |
|  |  |  | CPU使用率 | 基线值为：40% | 最大值为：34.85%，属于正常值。 |  |
|  |  |  | 内存使用率 | 基线值为：55% | 最大值为：31.84%，属于正常值。 |  |
| 安恒云防护 | 安全设备 | http://www.websaas.cn | 三小时内攻击峰值 | <=200 | 攻击峰值为：35 |  |
|  |  |  | 攻击区域分布TOP3 | 无合肥区域，若有可填结论需关注 | 存在合肥地区地址（第一个攻击源ip地址，由于存在dns没有参考价值）。 |  |
|  |  |  | 攻击源IP排行TOP3 | "无合肥IP，若有需确认是否为厅内源: | 不是厅内的地址，地址为厅外地址：60.166.9.98 |  |
| 网防G01 | 安全设备 | http://www.gov110.cn/gov/login | 应用防护攻击次数 | 非厅内可能是攻防开始，需通告注意" | 2次 | 与业务厂家沟通是由于业务厂家的操作导致的误报。 |
|  |  |  | 系统防护异常信息 | <=200 | 156 | 由于专家库自身服务器安装软件问题导致的报错。 |
| 深信服出口防火墙 | 安全设备 | https://192.168.252.1/framework.php# | 并发会话数 | <=15000 | 在09:26-09:50时间段内30000左右属于非正常状态，其他时间属于正常状态。 |  |
|  |  |  | 新建连接数 | <=3000 | 在09:26-09:50时间段内5000左右属于非正常状态，其他时间属于正常状态。 |  |
| 绿盟WAF | 安全设备 | https://192.168.1.3 | CPU使用率 | <=65% | 在10%与55%之间，属于正常状态。 |  |
|  |  |  | 内存使用率 | <=70% | 数值在58%之间波动。 |  |
|  |  |  | 连接会话数 | 引擎并发连接数：<=75% | 会话数在：14-45之间。 |  |
| 启明星辰IPS | 安全设备 | https://192.168.1.18 | CPU使用率 | <=10% | 在6%-8%之间 |  |
|  |  |  | 内存使用率 | <=25% | 在19%-21%之间波动属于正常情况。 |  |
|  |  |  | 连接会话数 | <=2500 | 当前连接数为：1830，属于正常情况。 |  |
| 深信服负载均衡AD | 安全设备 | https://192.168.253.32 | 总连接数(系统并发连接数） | <=110 | 总连接数为：10之内属于正常情况。 |  |
|  |  |  | 流量（网络吞吐量） | <=15Mbps | 流量在：2000Mbps之间徘徊。 |  |
|  |  |  | 新建连接数(系统新建连接数） | <=40 |  |  |
|  |  |  | 门户网站总链接数（服务端并发连接数） | <=300 |  |  |
|  |  |  | 门户网站HTTP请求数 | <=25 |  |  |
|  |  |  | 门户网站新建连接数(服务端新建连接数） | <=18 |  |  |

## 监测时间：11:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 厅门户网站服务器-1（地调中心） | 服务器 | 192.168.253.2 | 图形界面 | 正常登录，无卡顿 | 内网厅网站-1服务器  登陆情况。 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) | 最大值为5.49%，属于正常值。 |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) | 最大值为13.9%，属于正常值。 |  |
| 厅门户网站服务器-2 | 服务器 | 192.168.253.31 | 图形界面 | 正常登录，无卡顿 | 端口状态正常 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) | 最大值为18.18%，属于正常值 |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) | 最大值为72.91%，属于正常值 |  |
| 厅网站数据库服务器 | 服务器 | 192.168.253.11 | 图形界面 | 数据库服务端口是否正常 | 端口状态正常 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) | 最大值为：0.95%，属于正常值。 |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) | 最大值为：8.93%，属于正常值。 |  |
| 厅网站备份服务器 | 服务器 | 192.168.253.43 | 图形界面 | 正常登录，无卡顿 | 服务器远程登陆正常 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) | 最大值为：7.14%，属于正常值。 |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) | 最大值为：9.13%，属于正常值。 |  |
| 征地平台服务器 | 服务器 | 192.168.253.17 | 图形界面 | 正常登录，无卡顿 | 征地平台服务器在09:38-09:50时间段内出现无法登陆情况。 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) | 最大值为：34.85%，属于正常值。 |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) | 最大值为：31.84%，属于正常值。 |  |
| 安恒云防护 | 安全设备 | http://www.websaas.cn | 三小时内攻击峰值 | <=200 |  |  |
|  |  |  | 三小时内攻击次数 | <=1000 |  |  |
|  |  |  | 攻击区域分布TOP3 | 无合肥区域，若有可填结论需关注 |  |  |
|  |  |  | 攻击源IP排行TOP3 | "无合肥IP，若有需确认是否为厅内源: |  |  |
| 网防G01 | 安全设备 | http://www.gov110.cn/gov/login | 应用防护攻击次数 | 非厅内可能是攻防开始，需通告注意" |  |  |
|  |  |  | 系统防护异常信息 | <=100 |  |  |
| 深信服出口防火墙 | 安全设备 | https://192.168.252.1/framework.php# | 并发会话数 | <=50 |  |  |
|  |  |  | 新建连接数 | <=15000 |  |  |
| 绿盟WAF | 安全设备 | https://192.168.1.3 | CPU使用率 | <=3000 |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 连接会话数 | (观察均值或联系开发确认基线) |  |  |
| 启明星辰IPS | 安全设备 | https://192.168.1.18 | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 连接会话数 | (观察均值或联系开发确认基线) |  |  |
| 深信服负载均衡AD | 安全设备 | https://192.168.253.32 | CPU使用率(业务核) | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率(业务) | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 总链接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 流量 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | HTTP请求数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 新建连接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站总链接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站流量 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站HTTP请求数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站新建连接数 | (观察均值或联系开发确认基线) |  |  |

## 监测时间：14:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 厅门户网站服务器-1（地调中心） | 服务器 | 192.168.253.2 | 图形界面 | 正常登录，无卡顿 | 内网厅网站-1 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) | 内网厅网站-2 |  |
| 厅门户网站服务器-2 | 服务器 | 192.168.253.31 | 图形界面 | 正常登录，无卡顿 |  |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 厅网站数据库服务器 | 服务器 | 192.168.253.11 | 图形界面 | 正常登录，无卡顿 |  |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 厅网站备份服务器 | 服务器 | 192.168.253.43 | 图形界面 | 正常登录，无卡顿 |  |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 征地平台服务器 | 服务器 | 192.168.253.17 | 图形界面 | 正常登录，无卡顿 |  |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 安恒云防护 | 安全设备 | http://www.websaas.cn | 三小时内攻击峰值 | <=200 |  |  |
|  |  |  | 三小时内攻击次数 | <=1000 |  |  |
|  |  |  | 攻击区域分布TOP3 | 无合肥区域，若有可填结论需关注 |  |  |
|  |  |  | 攻击源IP排行TOP3 | "无合肥IP，若有需确认是否为厅内源: |  |  |
| 网防G01 | 安全设备 | http://www.gov110.cn/gov/login | 应用防护攻击次数 | 非厅内可能是攻防开始，需通告注意" |  |  |
|  |  |  | 系统防护异常信息 | <=100 |  |  |
| 深信服出口防火墙 | 安全设备 | https://192.168.252.1/framework.php# | 并发会话数 | <=50 |  |  |
|  |  |  | 新建连接数 | <=15000 |  |  |
| 绿盟WAF | 安全设备 | https://192.168.1.3 | CPU使用率 | <=3000 |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 连接会话数 | (观察均值或联系开发确认基线) |  |  |
| 启明星辰IPS | 安全设备 | https://192.168.1.18 | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 连接会话数 | (观察均值或联系开发确认基线) |  |  |
| 深信服负载均衡AD | 安全设备 | https://192.168.253.32 | CPU使用率(业务核) | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率(业务) | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 总链接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 流量 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | HTTP请求数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 新建连接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站总链接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站流量 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站HTTP请求数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站新建连接数 | (观察均值或联系开发确认基线) |  |  |

## 监测时间：17:00

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **监测对象** | **类型** | **访问方式** | **监测项** | **参考指标** | **检查结论** | **截图存证(图片放入后手动调小)** |
| 厅门户网站服务器-1（地调中心） | 服务器 | 192.168.253.2 | 图形界面 | 正常登录，无卡顿 | 端口状态正常 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 厅门户网站服务器-2 | 服务器 | 192.168.253.31 | 图形界面 | 正常登录，无卡顿 |  |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 厅网站数据库服务器 | 服务器 | 192.168.253.11 | 图形界面 | 正常登录，无卡顿 | 端口状态正常 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 厅网站备份服务器 | 服务器 | 192.168.253.43 | 图形界面 | 正常登录，无卡顿 | 端口状态正常 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 征地平台服务器 | 服务器 | 192.168.253.17 | 图形界面 | 正常登录，无卡顿 | 端口状态正常 |  |
|  |  |  | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
| 安恒云防护 | 安全设备 | http://www.websaas.cn | 三小时内攻击峰值 | <=200 |  |  |
|  |  |  | 三小时内攻击次数 | <=1000 |  |  |
|  |  |  | 攻击区域分布TOP3 | 无合肥区域，若有可填结论需关注 |  |  |
|  |  |  | 攻击源IP排行TOP3 | "无合肥IP，若有需确认是否为厅内源: |  |  |
| 网防G01 | 安全设备 | http://www.gov110.cn/gov/login | 应用防护攻击次数 | 非厅内可能是攻防开始，需通告注意" |  |  |
|  |  |  | 系统防护异常信息 | <=100 |  |  |
| 深信服出口防火墙 | 安全设备 | https://192.168.252.1/framework.php# | 并发会话数 | <=50 |  |  |
|  |  |  | 新建连接数 | <=15000 |  |  |
| 绿盟WAF | 安全设备 | https://192.168.1.3 | CPU使用率 | <=3000 |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 连接会话数 | (观察均值或联系开发确认基线) |  |  |
| 启明星辰IPS | 安全设备 | https://192.168.1.18 | CPU使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 连接会话数 | (观察均值或联系开发确认基线) |  |  |
| 深信服负载均衡AD | 安全设备 | https://192.168.253.32 | CPU使用率(业务核) | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率(业务) | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 内存使用率 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 总链接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 流量 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | HTTP请求数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 新建连接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站总链接数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站流量 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站HTTP请求数 | (观察均值或联系开发确认基线) |  |  |
|  |  |  | 门户网站新建连接数 | (观察均值或联系开发确认基线) |  |  |