

# 服务安全与监控

**NSD SECURITY**

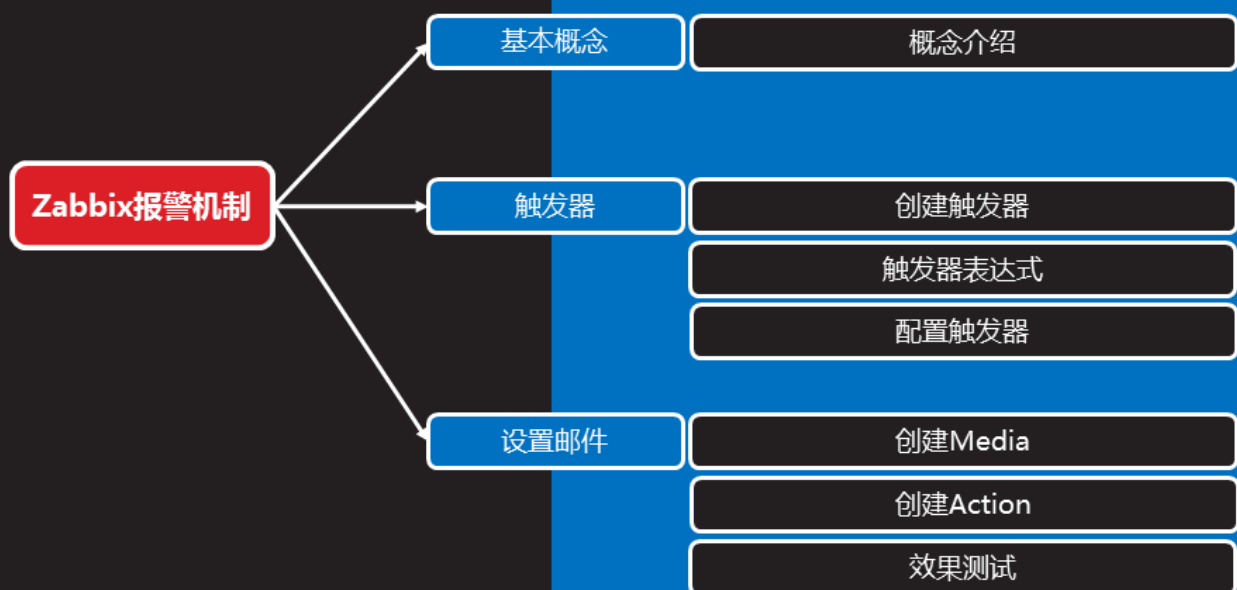
**DAY06**

# 内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	Zabbix报警机制
	10:30 ~ 11:20	
	11:30 ~ 12:00	Zabbix进阶操作
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	监控案例
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑



## Zabbix报警机制



# 基本概念

## 概念介绍

- 自定义的监控项默认不会自动报警
- 首页也不会提示错误
- 需要配置触发器与报警动作才可以自定义报警

知识讲解

Problems							
Time ▼	Recovery time	Status	Info	Host	Problem • Severity	Duration	
02/14/2018 09:20:07 PM		PROBLEM		<u>zabbix_client_web</u>	HTTP service is down on <u>zabbix_client_web</u>	2d 14h 51m	



## 概念介绍（续1）

知识讲解

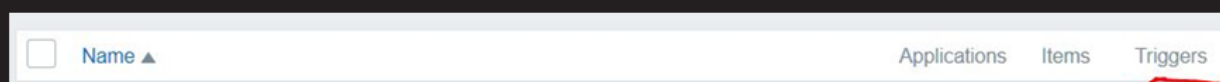
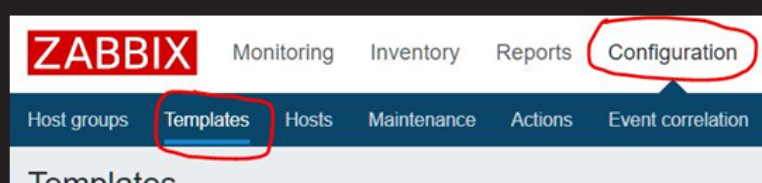
- 触发器（trigger）
  - 表达式，如内存不足300M，用户超过30个等
  - 当出发条件发生后，会导致一个触发事件
  - 触发事件会执行某个动作
- 动作（action）
  - 触发器的条件被触发后的行为
  - 可以是发送邮件、也可以是重启某个服务等



## 创建触发器

知识讲解

- 通过Configuration→Templates
- 选择模板点击后面的Triggers→Create trigger
  - 强烈建议使用英文创建（中文翻译不敢恭维）



# 触发器表达式

## 配置触发器（续1）



- 选择触发器报警级别
- Add创建该触发器

# 创建Media

- 设置邮件服务器
  - Administration→Media Type→选择Email邮件
  - 设置邮件服务器信息

知识讲解



<input type="checkbox"/>	名称 ▲	类型
<input type="checkbox"/>	Email	电子邮件
<input type="checkbox"/>	Jabber	Jabber
<input type="checkbox"/>	SMS	短信

The image shows the configuration form for the 'Email' media type. The form includes the following fields and options:

- 名称 (Name): Email
- 类型 (Type): 电子邮件 (Email)
- SMTP服务器 (SMTP Server): localhost
- SMTP服务器端口 (SMTP Server Port): 25
- SMTP HELO: company.com
- SMTP电邮 (SMTP Email): root@localhost
- 安全链接 (Security Link): 无 (None) / STARTTLS(纯文本通信协议扩展)
- 认证 (Authentication): 无 (None) / Username and password
- 已启用 (Enabled): ☒

Buttons at the bottom: 更新 (Update), 克隆 (Clone), 删除 (Delete), 取消 (Cancel).

# 效果测试

- 在被监控主机创建账户
- 登录监控端Web页面，在仪表盘中查看问题

知识讲解



问题						
时间 ▼	恢复时间	状态	信息	主机	问题 • 严重性	持续时间
23:13:39		问题		zabbix_client_web	passwd_line_gt_26	57s





# 概述

## 知识讲解

- 自动发现 ( Discovery )
  - 当Zabbix需要监控的设备越来越多，手动添加监控设备越来越有挑战，此时，可以考虑使用自动发现功能
  - 需要批量一次性添加一组监控主机，也可以使用自动发现功能
- 自动发现可以实现：
  - 自动发现、添加主机，自动添加主机到组
  - 自动连接模板到主机，自动创建监控项目与图形等





# 主被动监控



# 修改监控项模式

知识讲解

- 将模板中的所有监控项目全部修改为主动监控模式
  - Configuration→Templates
  - 选择新克隆的模板，点击后面的Items（监控项）
  - 点击全选，选择所有监控项目，点击批量更新
  - 将类型修改为：Zabbix Agent（Active主动模式）

<input checked="" type="checkbox"/>	Wizard	名称	触发器	键值
<input checked="" type="checkbox"/>	...	Template App Zabbix Agent: Version of zabbix_agent(d) running	触发器 1	agent.version
<input checked="" type="checkbox"/>	...	Template App Zabbix Agent: Host name of zabbix_agentd running	触发器 1	agent.hostname
<input checked="" type="checkbox"/>	...	Template App Zabbix Agent: Agent ping	触发器 1	agent.ping
<input checked="" type="checkbox"/>	...	Maximum number of processes	触发器 1	kernel.maxproc
<input checked="" type="checkbox"/>	...	Maximum number of opened files	触发器 1	kernel.maxfiles
<input checked="" type="checkbox"/>	...	Number of processes	触发器 1	proc.num[]
<input checked="" type="checkbox"/>	...	Number of running processes	触发器 1	proc.num[,run]
<input checked="" type="checkbox"/>	...	CPU iowait time	触发器 1	system.cpu.util[,iowait]

☒ 类型 ☐ Zabbix 客户端  
☐ JMX endpoint ☐ Zabbix 客户端  
☐ SNMP community ☒ Zabbix客户端(主动式)  
☐ 上下文名称 ☐ 简单检查  
☐ SNMPv1 客户端  
☐ SNMPv2 客户端