FortiMail HA 原理及配置

版本	1.0
时间	2012 年 1 月
作者	胡丹丹(ddhu@fortinet.com)
支持的版本	FortiMail v4.2.3
状态	草稿

目录

1.目的 3

2.环境介绍 4

3.心跳与同步 4

3.1 不被同步的设定 5

3.2 Failover 后 MTA 队列目录的同步 6

4. HA 的配置 7

4.1 主设备配置 7

4.2 从设备配置 9

5.参考 12

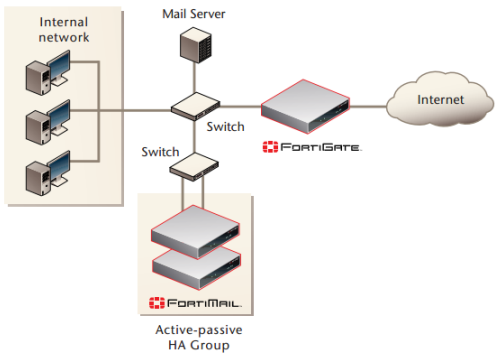
1.目的

FortiMail HA 用于增强处理能力及提高高可靠性。

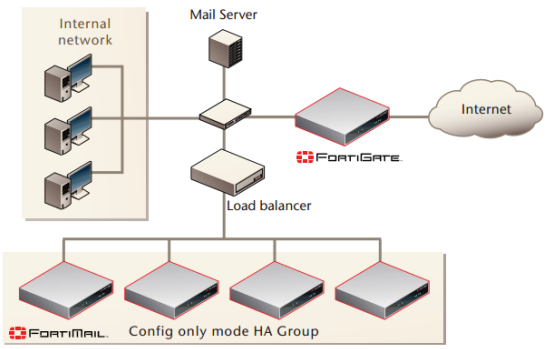
FortiMail 可以操作于 2 种模式，主动-被动，Config-only 模式。以下为两种模式的特性比较。

主动-被动模式	Config-only 模式
2 台 FortiMail 工作于同一 HA 组	2-25 台 FortiMail 工作于同一 HA 组
典型部署在交换机之后	典型部署在负载均衡器之后
配置和数据均同步	仅同步配置
仅有主设备处理邮件	所有 HA 成员均处理邮件
硬件失效后数据不丢失	硬件失效丢失数据
故障恢复保护，不增加邮件处理能力	邮件处理能力增强，但无故障恢复能力

主动-被动模式



Config-only 模式

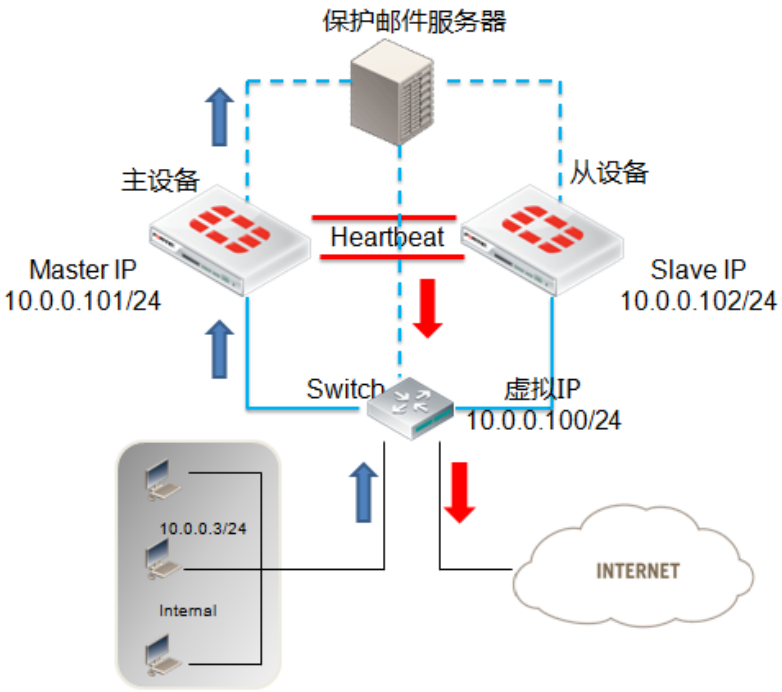


FortiMail 支持不同型号的设备组建 HA ,但所有的 FortiMail 必须有相同的软件版本。当使用混合型号组建 HA，HA 的处理能力将被最低端型号的处理能力所限制。

本文就 FortiMail 常用的主动-被动模式进行说明。

2.环境介绍

本文使用 2 台 FortiMail 100 进行说明,本文使用的系统版本为 FortiMail v4.0MR2 Patch2。



3.心跳与同步

心跳与同步流量使用 TCP 数据包在 FortiMail 成员之间通过心跳接口传递。心跳与同步流量有三个主要功能:

- 监控 HA 其他成员是否响应；

- 主设备配置发生变化同步至其他从设备；
- 同步邮件数据从主设备至其他从设备(邮件数据包含 FortiMail 系统邮件目录，用户目录以及邮件队列)。

当主设备配置发生改变，立即通过心跳接口同步至其他从设备，一旦同步失败，则可以通过手动同步将配置同步至从设备。同样在命令行下可以使用 diagnose system ha sync 进行同步。

一旦发生故障切换，从设备将成为新的主设备，在切换的同时，所有正在进行处理的邮件将会中断，那么这类邮件需要重新发送，大部分邮件客户端及服务器能够很好的处理此类情况。

3.1 不被同步的设定

不同步项目	描述
操作模式	**在每个 HA 成员组建 HA 之前定义操作模式**
主机名	**用于区分 HA 成员**
接口配置(server 及网关模式)	**HA 成员为连接目的配置不同的网络接口**
管理 IP(透明模式)	**HA 成员管理地址**
SNMP 系统信息	**HA 成员拥有的诸如 snmp 描述，地点，联系人信息**

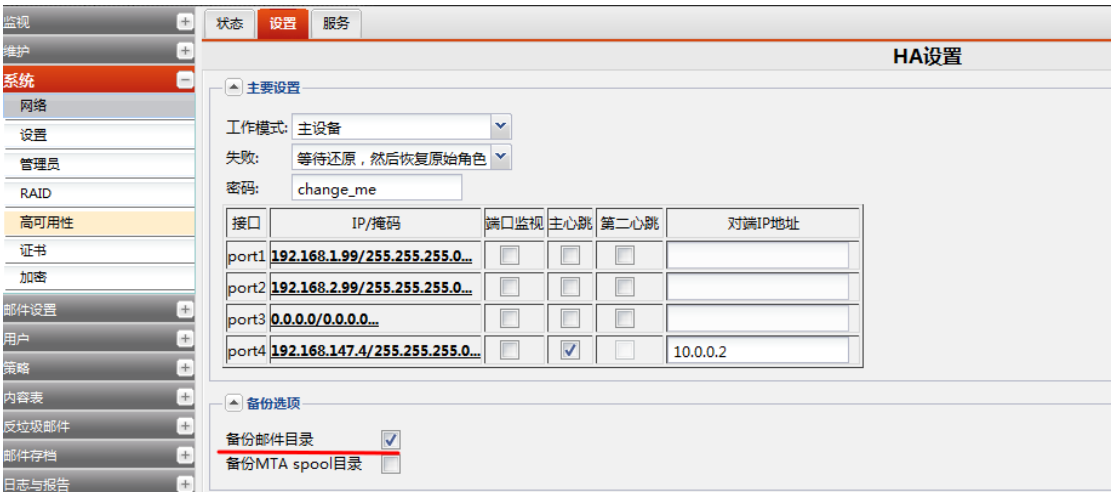
Raid 配置	**Raid 设定为硬件独立配置，无需存储于系统配置中，因此 HA 不同步 raid 配置**
HA 关键配置	**如 HA 成员工作角色，作为主设备还是从设备**
HA 相关设定	**备份邮件选项，备份邮件队列选项**
HA 服务监控配置	**在主动-被动模式中，HA 的服务监控配置不被同步，远程服务监控配置于从设备用于监控主设备**

3.2 Failover 后 MTA 队列目录的同步

正常操作中，email 工作于以下三种状态之一:

- 由主设备接收并发送;
- 处于邮件队列中等待发送；
- 存储于主设备邮件数据目录中(如邮件隔离 ,邮件归档 ,服务器模式的收件箱)。

当正常运行的系统出现故障时，邮件发送及接受受中断，发送者 fortimail 通常将重新发送邮件，但是保存的邮件位于主设备的邮件数据目录。所以建议在配置 Fortimail HA 时开启邮件数据队列的同步防止邮件数据的丢失。



4. HA 的配置

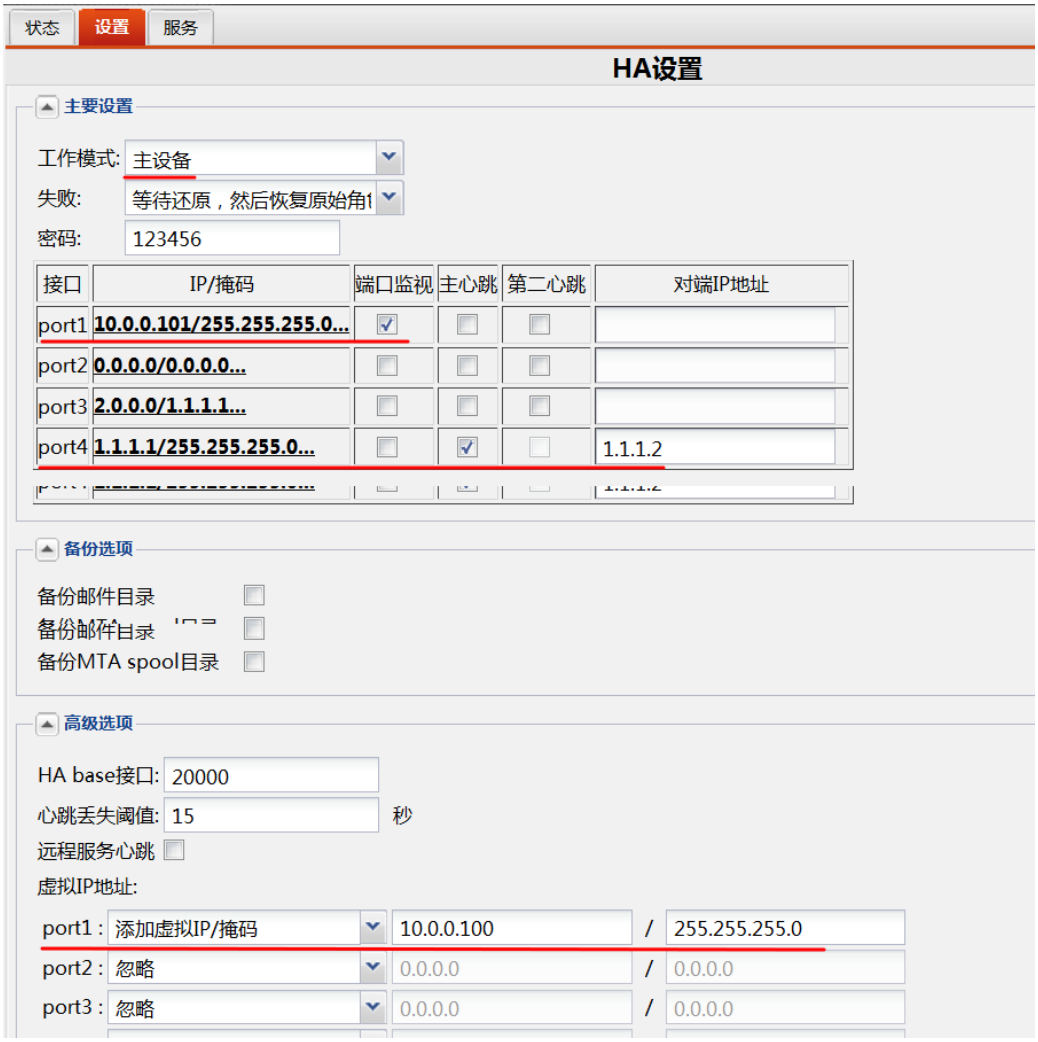
配置及启用 HA ，需要进行如下操作:

1. 如果 Fortimail HA 集群使用 ForitGuard 反病毒及反垃圾邮件服务 ,需要确定所有 HA 成员有反病毒及反垃圾邮件服务；
2. 必须配置至少一个接口用于 HA 成员之间的心跳及同步；
3. 启用 HA 模式，选择各自 Foritmail 的工作模式，以及失败后角色的重定义，心跳接口需要配置本端及对端地址用于心跳及同步通讯。

此例 port1 为业务接口，port4 为心跳接口，并为 port1 添加虚拟 ip 10.0.0.100

4.1 主设备配置

HA 设置



主设备服务,启用网络接口监控服务，当主设备接口失效，即切换至从设备工作。检查时间间隔及频率默认为每 10 秒检测一次，3 次连续检测失效后切换至从设备工作。

主设备状态查看

4.2 从设备配置

port1 为业务接口，port4 为心跳接口，并为 port1 添加虚拟 ip 10.0.0.100

从设备服务配置，配置远程服务用于监控主设备是否工作正常,监控的服务可以从 stmp，pop3，web 三项任意选择。


状态
设置
服务
HA服务监视
远程服务
(当设备工作在slave模式时，需要检查这些服务。)
服务类型 状态 主机：端口 检查间隔(分钟) 等待时间(秒) 失败频率
SMTP服务 10.0.0.101:25 1 30 3
POP服务 10.0.0.101:110 1 30 3
Web服务 10.0.0.101:80 1 30 3
本地服务
(当设备工作在主设备模式时，需要检查这些服务。)
服务类型 状态 检查间隔(秒) 失败频率
网络接口 10 3
硬盘 10 3
应用
取消

从设备的状态查看


监视
维护
系统
网络
设置
管理员
RAID
高可用性
证书
加密
邮件设置
用户
策略
内容表
反垃圾邮件
邮件存档
日志与报告
状态
设置
服务
HA状态
无
刷新
模式状态
可设置的运行模式: 从设备
生效的运行模式: 从设备
后台程序状态
监视: 下一次检查将在 Fri Nov 18 15:42:08 2011, 失败 0
设置: 上次同步时间 Fri Nov 18 15:39:30 2011
数据: 上次同步时间 Fri Nov 18 15:38:30 2011
(当前时间是 Fri Nov 18 15:42:06 2011)
动作
点击此处，开始同步设置/数据...
点击此处，切换到主设备模式...

5.参考

Administration Guide