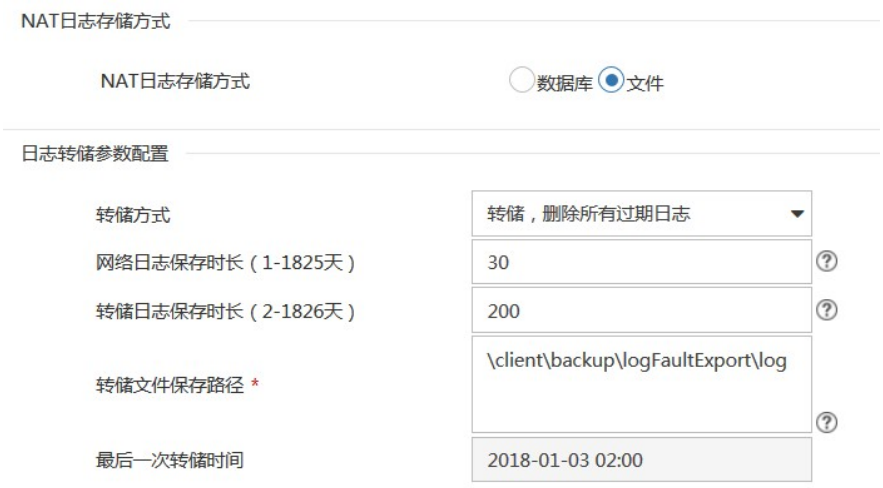
某局点SSM功能组件监视防火墙日志量过大

李大维 2018-01-03 发表

某局点使用IMC和SSM功能组件，目前对两台M9000防火墙进行监控。按照他们要求需要对防火墙日志会话存储，但是由于使用带宽比较高，导致日志存储比较大，生成的日志量大致为每分钟1.4GB大小。由于后期还需要上线更多防火墙，客户希望能实行日志文件自动压缩功能，减少磁盘存储日志压力。

建议对数据进行转储，转储的方式有多种，其目的一致都是要对空间进行转储，最佳的问题就是要对磁盘进行扩容。然而一般客户对于磁盘的扩容需要备份及考虑成本的情况，不愿意主动进行更改操作，因此可以考虑对于日志进行转储的操作，然而SSM组件的转储功能需要理解几点：

首先对于SSM组件转储日志的配置方式是在业务页签下，安全业务管理---全局参数配置：



其中NAT日志存储方式是指接收和查询NAT日志的方式，包括数据库或者文件两种方式，默认情况下，NAT日志存放在文件中，不进行转储。

在转储时有两个时间需要特殊关注：

网络日志保存时长，是指日志在文件或者数据库中保留的时间，以天为单位，在这个时间段内日志不会进行转储，因此需要操作人员对于磁盘空间进行预留。转储日志保存时长是指转储后的日志文件保存的时间，以天为单位，日志在转储后的文件内保存的时长。

如果磁盘空间压力过大，可以将网络日志保存时长时间调小，及时备份转储后的文件。