

集成安全平台 XSEC

用户手册



深信服智安全
SANGFOR SECURITY

深信服科技有限公司

目录

1. 声明	3
2. 前言	3
3. XSEC 控制台登录方式	4
4. XSEC 初始化操作	4
5. XSEC 授权激活	9
6. XSEC 部署配置	10
6.1 创建业务物理出口	10
6.2 创建安全应用	12
6.3 自定义网络拓扑	12
6.4 模板	14
6.5 单点登录	19
7. XSEC 日常管理功能使用	20
7.1 首页	20
7.2 运营中心	21
7.3 集中管控	23
7.4 应用市场	23
7.5 资源池	24
7.5.1 应用管理	24
7.5.2 网络管理	26
7.5.3 主机扩容	27
7.5.4 磁盘扩容	28
7.5.5 模板管理	28
7.6 系统	29
7.6.1 平台升级	29
7.6.2 管理员账号	29
7.6.3 时间和日期	31
7.6.4 操作日志	31
7.6.5 告警信息	32
7.6.6 平台授权	32
7.6.7 恢复默认配置	33
7.6.8 高可用	33
7.6.9 其他设置	34

1. 声明

Copyright © 2018 深信服科技股份有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

为深信服科技股份有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系深信服科技股份有限公司技术服务部。

深信服科技股份有限公司（以下简称为深信服科技、）。

2. 前言



本手册以深信服 XSECxsec5.0.0 版本为例进行配置说明。

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

3. XSEC 控制台登录方式

XSEC 默认 IP 地址是 10.251.251.251，将笔记本电脑配置一个 10.251.251.0/24 的 IP，并与安装完成的主机 eth0 口直连。

在浏览器中输入 https://10.251.251.251，并使用默认账号密码：admin/admin 登录安全服务平台。



提示：admin 默认密码为 admin，初次登录会被系统要求强制修改密码。

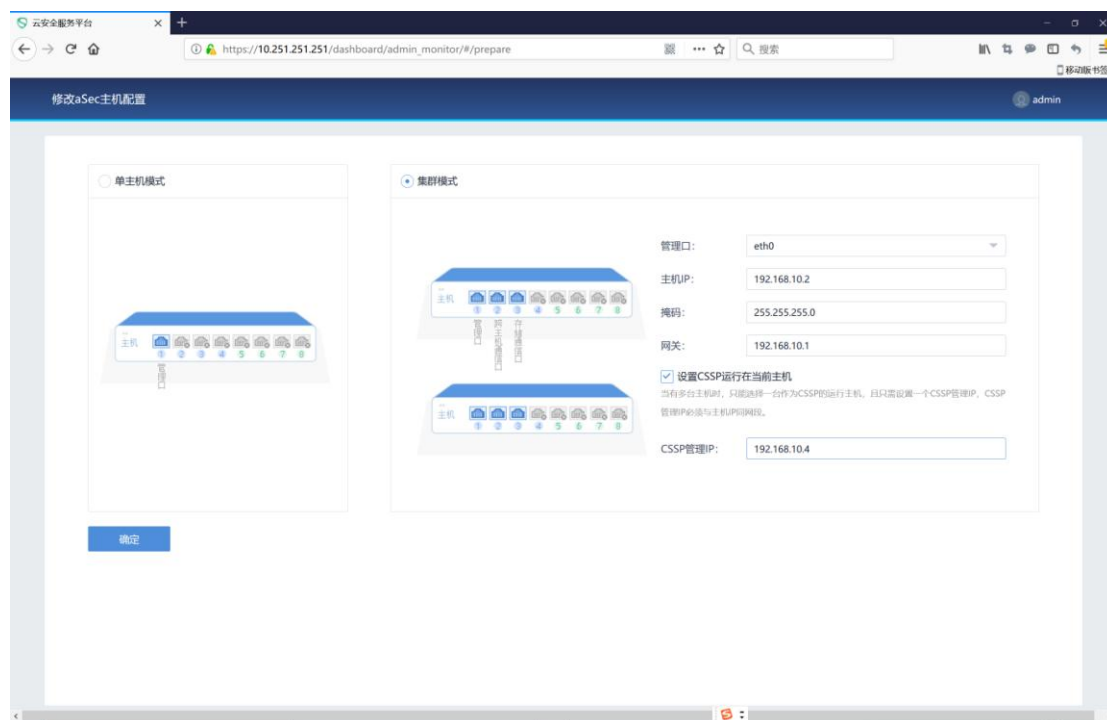


提示：推荐使用 Chrome 浏览器登录 XSEC 控制台页面。

4. XSEC 初始化操作

首次登录 XSEC，系统会进入初始化操作页面，系统初始化之后，后续再登录 XSEC 就不会出现初始化页面。

首先需要 XSEC 的数量选择[单机模式]还是[集群模式]，如果是单台部署，则选择[单主机模式]，如果是多台部署，则选择[集群模式]。



如果选择[单主机模式]，进入欢迎页面后，配置主机 IP、CSSP 管理 IP 后，完成初始化流程。

如果选择[集群模式]，除了需要配置主机 IP、CSSP 管理 IP，还需要选择其中一台主机作为主机，在该主机的此页面里勾选设置【CSSP 运行在当前主机】，其他主机不需要勾选。

将所有主机配置完毕后，按照标准的接线方式，将所有主机连接到交换机上。

添加主机：自动跳转到云安全服务平台欢迎页面，点击下一步，选择需要添加的主机，并配置好集群管理 IP，点击下一步



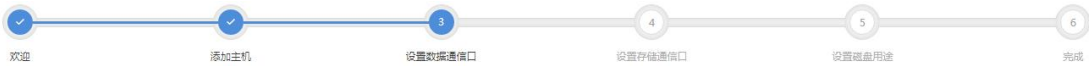
刷新 + 添加

199.201.88.39	199.201.88.55	199.201.88.102	199.201.88.122	199.201.88.123	199.201.88.150	199.201.88.151	199.201.88.152
199.201.88.202	199.201.88.205	199.201.88.239	199.201.90.33	199.201.90.34	199.201.90.130	199.201.91.30	199.201.91.51
199.201.91.157	199.201.91.204						

集群管理IP
用于多主机之间的集群通信, 也可以访问该IP进行主机运维。

上一步 下一步

配置数据通信口。每台主机选择网口, 作为数据通信口, 可以使用网口聚合



提示:
1. 请务必将数据通信口相连的交换机的MTU值设置为1600, 否则会导致网络不通。
[我知道了](#)

刷新 数据通信IP池 聚合网口

主机名称	数据通信口	IP	掩码
199.201.88.150	150ag1	197.231.201.1	255.255.255.0
199.201.88.151	151ag1	197.231.201.2	255.255.255.0
199.201.88.152	152ag1	197.231.201.3	255.255.255.0
199.201.90.34	34ag1	197.231.201.4	255.255.255.0

上一步 下一步

配置存储通信口。每台主机选择网口, 作为存储通信口



提示：

1. 平台初始化完成后，存储通信部署方式不能再修改，也不能再设置其他网口为存储通信口；
2. 存储通信IP池已内置IP网段，可点击“设置存储通信IP池”进行查看和修改，平台初始化完成后可以追加地址；

[我知道了](#)

刷新 存储通信IP池 存储通信部署方式： 无链路聚合

主机名称	存储通信口	IP	掩码
199.201.88.150	eth2	197.157.244.1	255.255.255.0
199.201.88.151	eth2	197.157.244.2	255.255.255.0
199.201.88.152	eth2	197.157.244.3	255.255.255.0
199.201.90.34	eth2	197.157.244.4	255.255.255.0

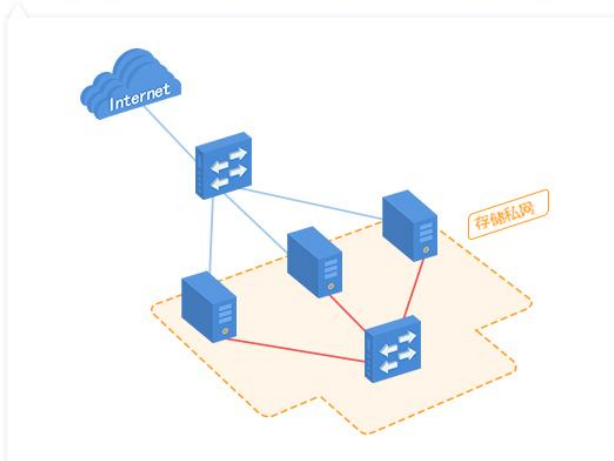
[上一步](#)

[下一步](#)

在该步，可以配置存储通信的配置方式：无链路聚合、单交换机链路聚合、双交换机链路聚合

存储通信部署方式

- 无链路聚合
 单交换机链路聚合 (推荐)
 双交换机链路聚合



无链路聚合

- 优点**
将存储数据通信的网络独立出来，能提升虚拟存储的稳定性。
- 不足**
当某条链路出现故障，会直接导致连接主机上的存储无法使用。
- 注意事项**
存储私网专用于存储节点交换数据，请按示意图连接网线。使用普通的二层交换机即可，不需要在交换机上作任何配置。
如果集群只有两个主机，可用网线直连私网网口，无需额外交换机。

[确定](#)

[取消](#)

设置磁盘用途。服务平台会列出所有主机的所有磁盘信息，客户在无特殊情况下，选择推荐的磁盘用途即可



931.51GB
可利用存储空间

931.51GB **0B**
1个数据盘 0个缓存盘

磁盘名称	类型	大小	用途
199.201.152.94			
/dev/sdb	机械硬盘	931.51GB	数据盘



上一步

开始初始化

初始化。点击初始化按钮，平台进入初始化步骤，大概半小时后，即可完成初始化步骤。并自动跳转到网络配置页面，方便客户进行业务网口配置



✔ 恭喜您，初始化配置成功！

删除主机本地vma完成
已花费时间 34分钟

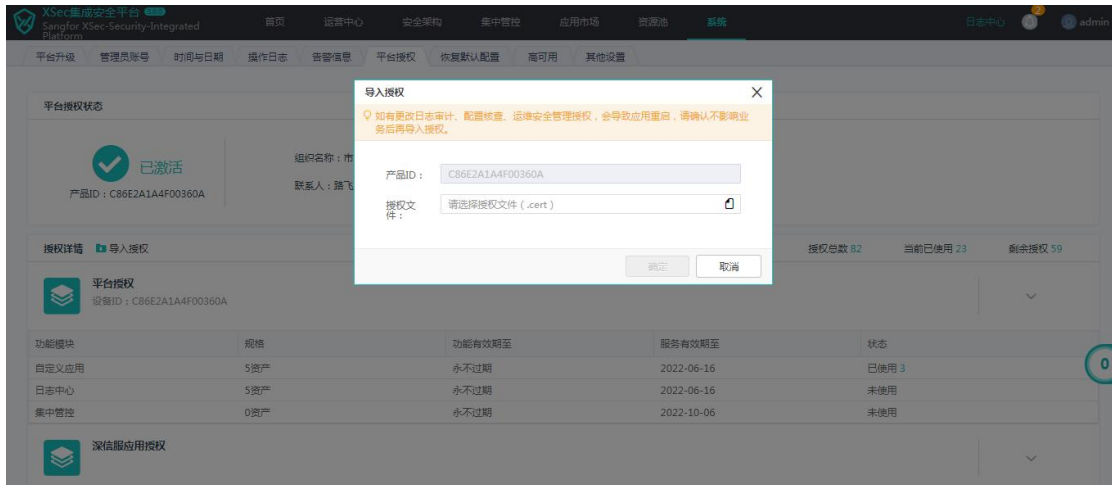
完成



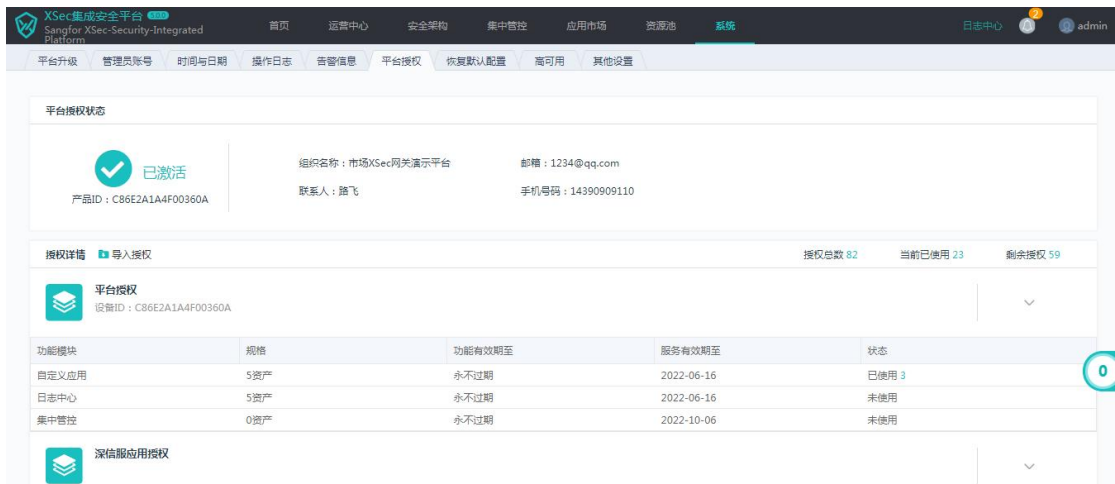
5. XSEC 授权激活

首次使用 XSEC，需要对 XSEC 进行授权激活。如果是服务器（SdSec-1000-A600、SdSec-1000-A602、SdSec-1000-B606 等），授权激活首先需要有一个授权 KEY，将 KEY 插在其中一台主机上，然后点击立即激活。如果是工控机（SdSec-1000-H440M、SdSec-1000-I444M、SdSec-1000-J444M 等），授权激活不需要授权 KEY，直接点击[立即激活](#)。

导入离线授权文件即可完成激活，其中产品 ID 为 KEY ID 或者硬件特征码。



完成激活后，在管理->平台授权页面，可以查看该平台当前的授权详情，包括平台的激活状态以及应用授权的详情。



6. XSEC 部署配置

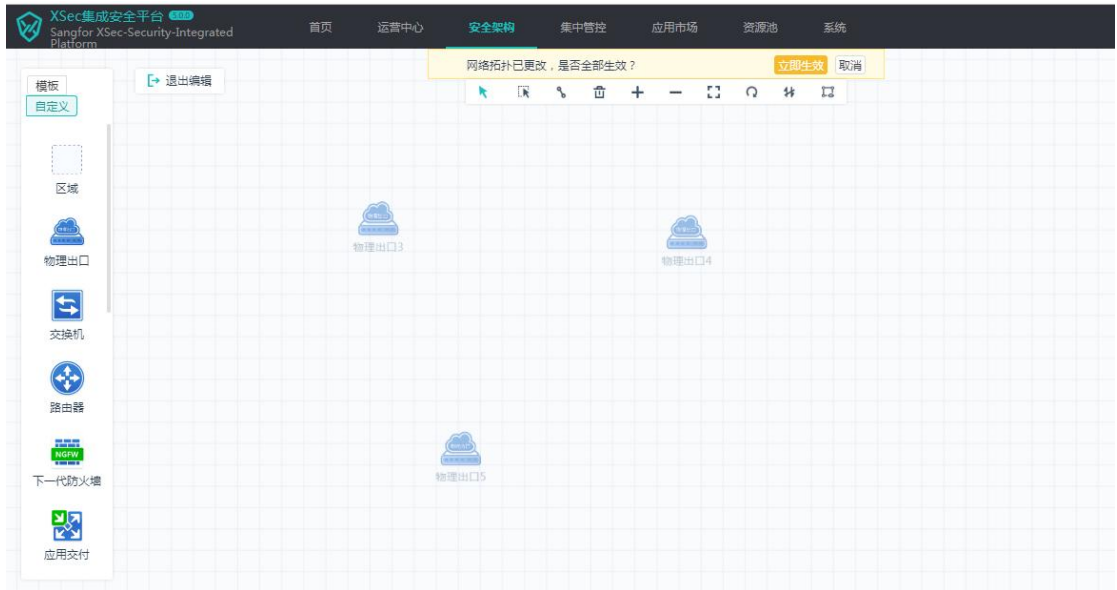
管理员可以根据规划的部署模式在【安全架构】完成部署配置，包括以下内容：

- 创建业务物理出口；
- 创建安全应用；
- 自定义网络拓扑；
- 快速进入各个安全应用；

6.1 创建业务物理出口

物理出口：物理出口用来连通虚拟网络和物理网络，对用户呈现为服务器物理网口。“物理出口”对内可以通过端口组连接虚拟路由器、虚拟网络设备或虚拟机，对外通过主机的物理网口连接连接交换机与外部网络互通。

管理员根据 XSEC 规划的部署模式，创建相应数量的业务物理出口。比如 XSEC 规划的是路由模式做网关，外网有两个互联网链路，内网有两个交换机做堆叠，那就需要创建 3 个业务物理出口，2 个外网业务物理出口，以及 1 个内网业务物理出口；比如 XSEC 规划的是单臂部署在核心交换机上，那就需要创建 1 个业务物理出口；



如果 XSEC 是集群部署，那创建物理出口的时候需要将所有主机的物理网口都添加上，否则发生主机故障，或者安全组件故障迁移的时候，网络会出现不通的故障。

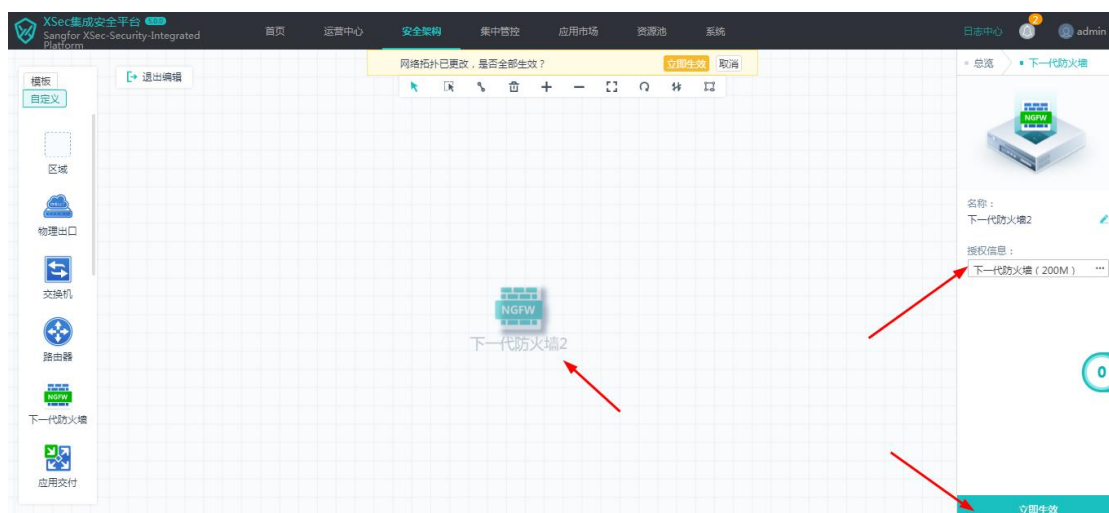


另外，如果 XSEC 需要镜像部署，那就可以创建 1 个物理出口并开启镜像模式。



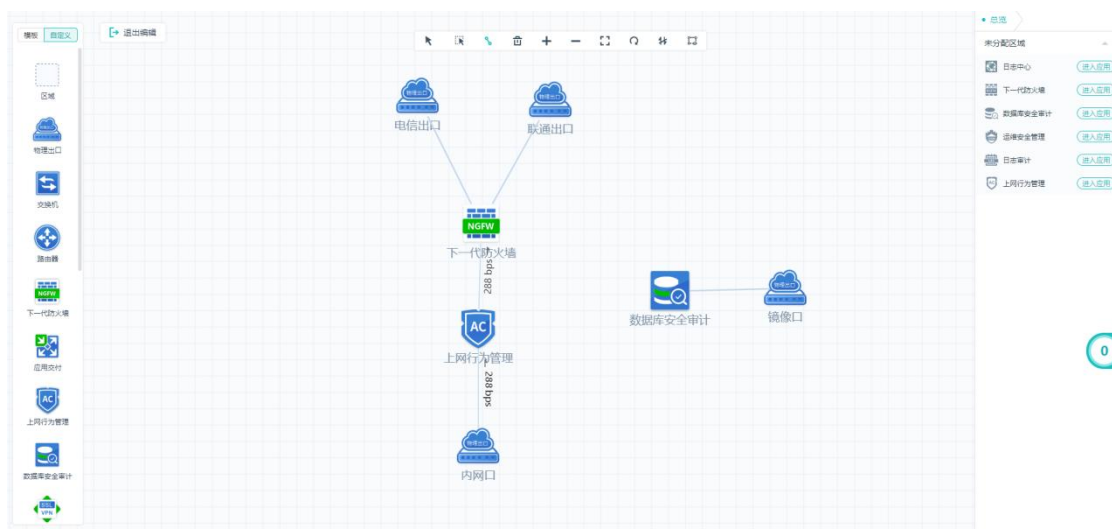
6.2 创建安全应用

管理员可以根据需求创建所需的安全应用组件，比如 vAF、vAC、vAD、SSL、OSM、LAS、BVT、EDR、DAS 其中一种或几种。管理员可以从【安全架构】左边列表将安全应用组件拖拽到中间，并选择相应的授权，然后点【立即生效】就可以创建好安全应用组件了。



6.3 自定义网络拓扑

创建好物理出口以及安全应用后，管理员就可以根据规划部署方案来自定义网络拓扑了。比如用户希望在 XSEC 里部署 vAF、vAC、vDAS，然后将 XSEC 的 vAF 作为网关接电信和联通两个外网出口，vAC 网桥接在 vAF 和内网口物理出口之间与物理交换机互联，同时还将数据库审计桥接到镜像物理出口上。如下图：



以下是常见的几种自定义部署案例：

1) 日志审计类组件部署方案



2) 镜像类组件部署方案



3) 透明部署方案



6.4 模板

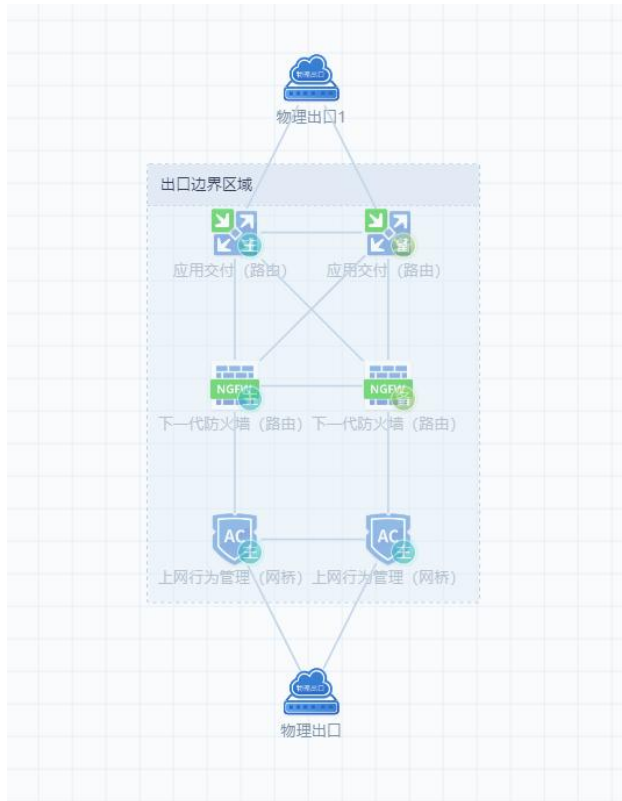
除了自定义网络拓扑以外，系统还内置了4个常用的模板，包括出口边界模板、等保合规模板（单臂）、等保合规模板（路由）和安全管理中心模板。这些模板已经预设好物理出口、区域、虚拟组件、虚拟路由器、虚拟交换机等元素，并且已经连好线。用户只需根据需求选择虚拟组件及配置物理出口，配置生效后就可以创建好相应的虚拟网络。

出口边界模板

出口边界模板包括应用交付、下一代防火墙和上网行为管理这3种虚拟组件，还包括2个物理出口。其中，应用交付是路由模式做网关，下一代防火墙是路由模式，上网行为管理是网桥模式。

该模板适用于将XSEC做为安全网关部署在出口，该方案可以替代传统硬件网关方案。考虑到网关的高可用性，出口边界模板里的虚拟组件都支持高可用部署，用户可以通过配置来启用高可用。

启用高可用后，应用交付和下一代防火墙为主备模式部署，上网行为管理为主主模式部署。【备注】高可用只能在集群两台以上部署时才能启用；



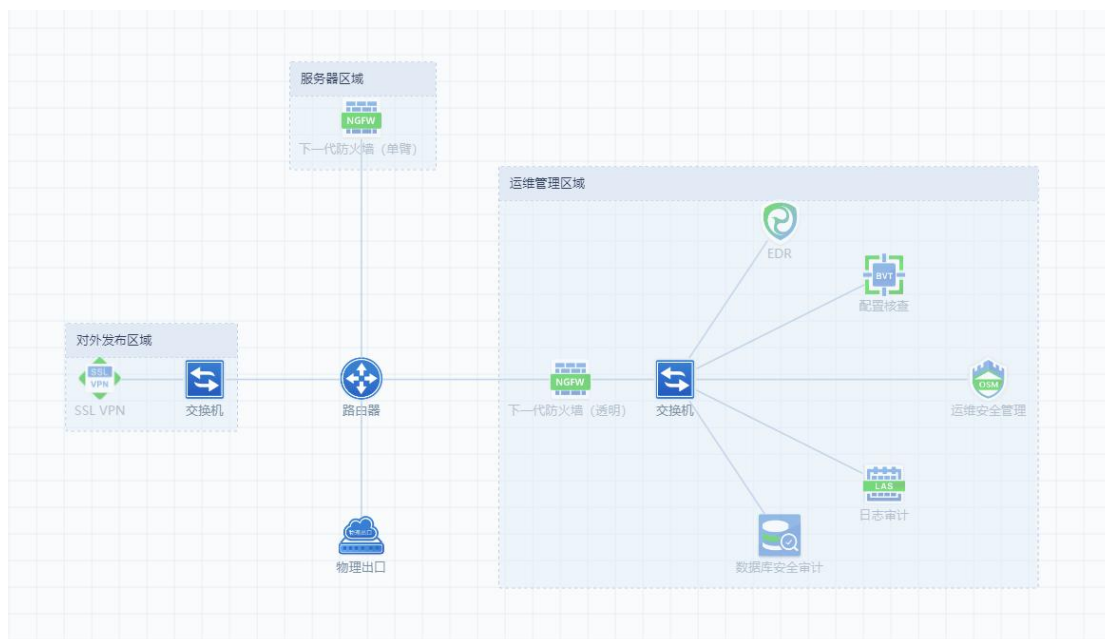
以下是出口边界模板双机集群部署的配置步骤：

- 1) 将出口边界模板拖到安全架构内；
- 2) 开启高可用；
- 3) 勾选 vAD、vAF、vAC，以及选择相应的授权；
- 4) 配置上行物理出口及下行物理出口；
- 5) 配置主 vAD 的上联运营商地址，以及下联与 vAF 对接的交换网口地址，上联接口建议配置链路健康检查，然后配置路由、NAT 以及链路负载和应用负载策略；配置主 vAD 双机配置里的网口同步列表和故障切换；
- 6) 配置主 vAF 高可用性的配置同步角色为主控，然后配置主 vAF 的上联与 vAD 对接的 VLAN 接口地址，以及下联与 vAC 对接的 LAN 口地址，下联接口建议配置链路故障检测，然后配置路由和安全防护策略；
- 7) 配置 vAC 的功能策略；

等保合规模板（单臂）

等保合规模板（单臂）包括下一代防火墙、SSLVPN、EDR、基线核查、运维安全管理、日志审计、数据库安全审计这 7 种虚拟组件，还包括 1 个物理出口。

该模板适合希望通过 XSEC 过等保同时又不能改变物理网络拓扑的用户，此时可以将 XSEC 单臂部署在物理交换机上，同时在物理交换机上做策略路由将指定业务流量引流到 XSEC 进行流量清洗。



以下是等保合规模板（单臂）部署的配置步骤：

1) 虚拟路由器

- 需要给虚拟路由器的接口配置 IP 地址与物理网络互联；
- 需要给虚拟路由器的接口配置 IP 地址与各安全组件互联；
- 配置指向物理交换机的默认路由；
- 配置两条策略路由，将业务系统进出的流量都引流至 AF；

2) 安全组件

- 需要在所有组件上配置接口 IP 地址
- 需要配置默认路由指向虚拟路由器；
- 需要配置相关的功能策略；

3) 物理交换机

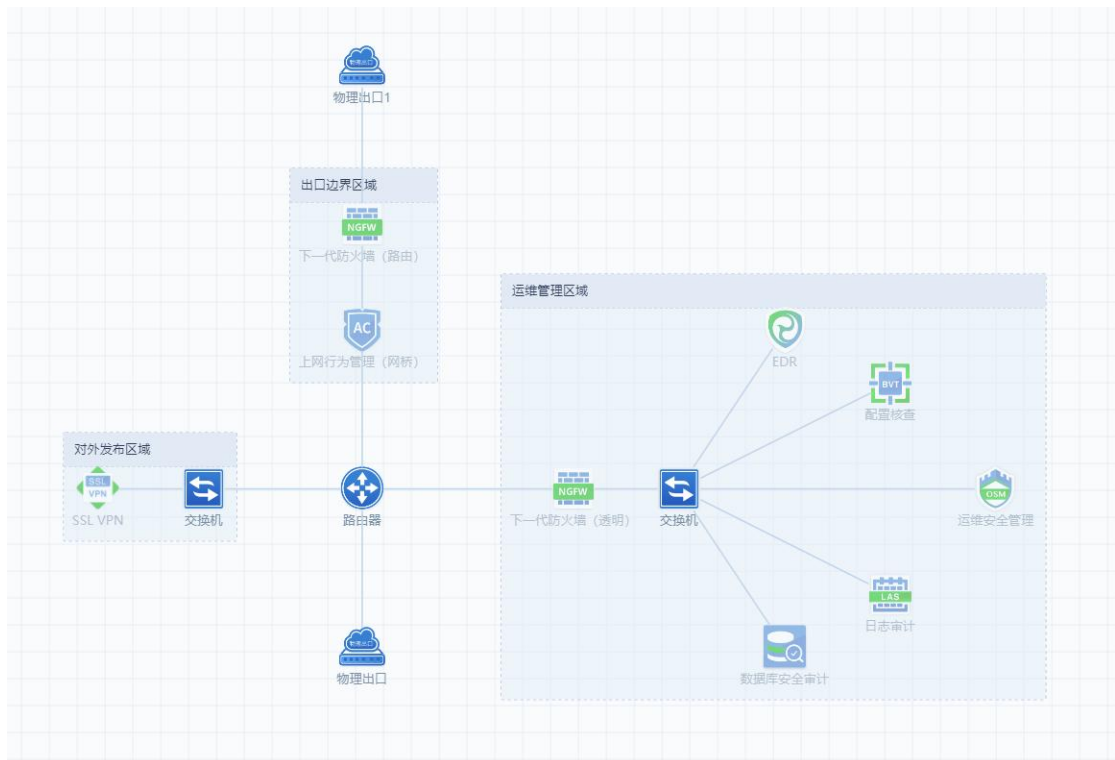
- 配置目的为安全组件 IP 地址段的路由指向虚拟路由器的互联 IP；

- 如果有购买服务器区域的 AF，则需要配置两条策略路由，将业务系统进出的流量都引流至虚拟路由器的互联 IP；

等保合规模板（路由）

等保合规模板（路由）包括下一代防火墙、上网行为管理、SSLVPN、EDR、基线核查、运维安全管理、日志审计、数据库安全审计这 8 种虚拟组件，还包括 2 个物理出口。

该模板适用于将 XSEC 作为网关部署。



以下是等保合规模板（路由）部署的配置步骤：

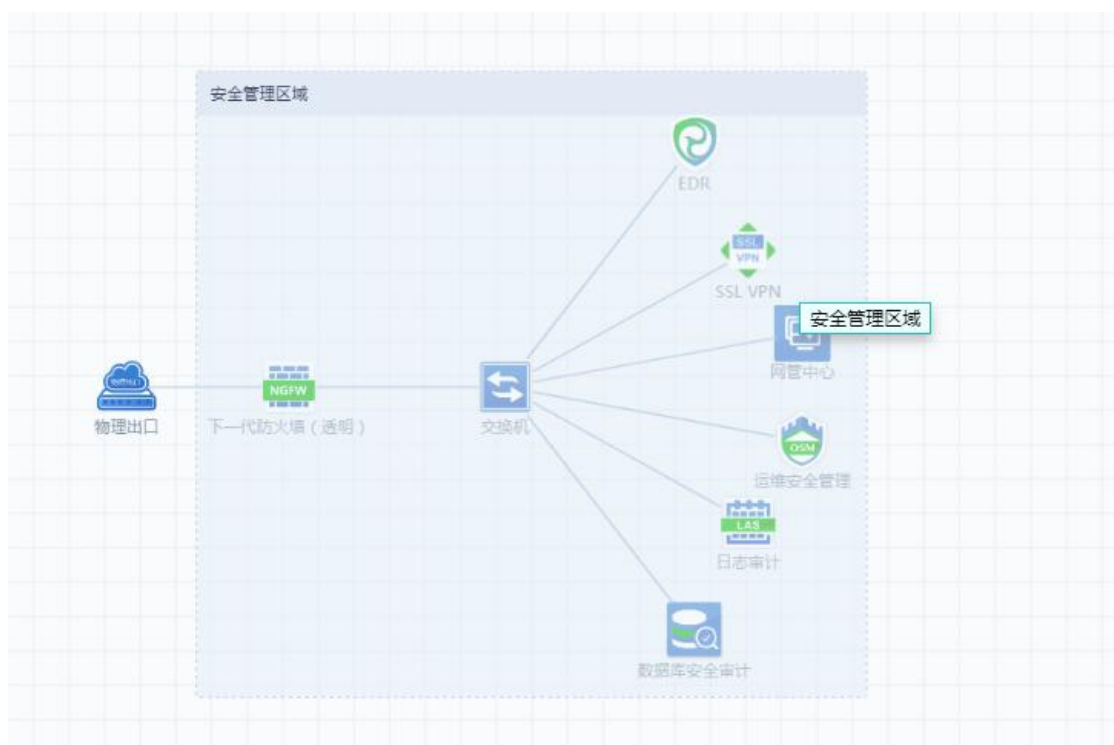
- 1) 虚拟路由器
 - 需要给虚拟路由器的接口配置 IP 地址与物理网络互联；
 - 需要给虚拟路由器的接口配置 IP 地址与各安全组件互联；
 - 需要配置指向出口 vAF 的默认路由；
 - 需要配置目的地址为内网网段的回包路由指向下联交换机；
- 2) 安全组件
 - 需要在所有组件上配置接口 IP 地址、默认路由；

- 需要在 vAF 上配置到内网网段的回包路由指向虚拟路由器；
 - 需要配置对应的功能策略；
- 3) 物理交换机
- 配置指向虚拟路由器的默认路由；

安全管理中心模板

等保合规模板（路由）包括下一代防火墙、SSLVPN、EDR、运维安全管理、日志审计、数据库安全审计和网管中心这 7 种虚拟组件，还包括 1 个物理出口。

该模板针对等保 2.0 安全管理中心技术指标所做，适合希望通过 XSEC 过等保同时又不能改变物理网络拓扑的用户。



以下是安全管理中心模板部署的配置步骤：

- i. 安全组件
 - 需要在所有组件上配置接口 IP 地址
 - 需要配置默认路由指向物理交换机；

- 需要配置相关的功能策略;
- ii. 物理交换机
- 配置与物理出口相连的互联 IP;

6.5 单点登录

管理员可以在【安全架构】页面中，选中某个应用，通过点击『进入应用』就能够单点登录跳转到应用界面，进行策略配置；或者通过点击『进入控制台』就能跳转到后台维护界面，进行后台命令行排障等。



A: 在【安全架构】里点击 BVT 的【配置应用】，进入到 BVT 的硬件管理平台。



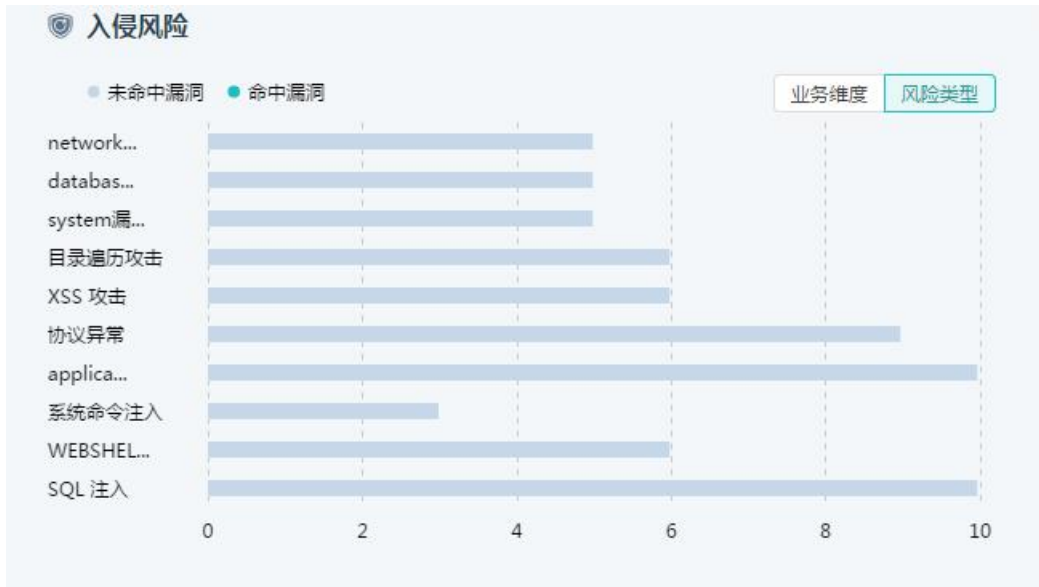
7. XSEC 日常管理功能使用

7.1 首页

1、在云安全服务平台的首页，能够清晰地看到应用状态、主机状态、磁盘状态、网络风险、网络状态和 CSSP 双机状态



2、入侵风险：展示客户被攻击的主机，可切换攻击的类型。



2、僵尸主机：展示客户环境中的僵尸主机信息。

3、外发流量异常：展示客户环境被攻击的信息。

4、在首页可切换不同的防火墙信息。

5、在平台右上角的告警页面中，能够看到对于平台网口通信故障告警、应用（即将）过期告警。



5、在【系统】->【告警信息】页面中，能够展示所有的历史告警信息。



7.2 运营中心

1、资产中心：实现以业务、用户组为维度的风险评估



2、业务风险：



3、用户风险:



4、 大屏中心:





7.3 集中管控

支持设备的统一纳管、规则库与补丁包的统一升级、策略的统一配置、客户端补丁包统一升级。



7.4 应用市场

应用市场上列出了 XSEC 支持的安全应用, 管理员可以在该页面了解各安全应用的功能详情, 也可以免费试用安全应用, 试用期 3 个月。



免费试用



EDR

终端检测响应平台 (EDR) 是深信服公司提供的一套终端安...

规格: (终端)

时长:

剩余试用次数: 6

确定

取消

7.5 资源池

『资源池』页面包括『应用』、『网络』、『主机』、『存储』和『模板』。



7.5.1 应用管理

在用户侧的【资源池】->【应用】界面，能够清晰看到用户所有的正式购买、免费试用的应用信息。



应用磁盘空间扩容

用户可以在【资源池】->【应用】页面中，对运维安全管理和聚铭日志审计应用进行磁盘扩容。



注：支持运维安全管理和日志审计的磁盘扩容

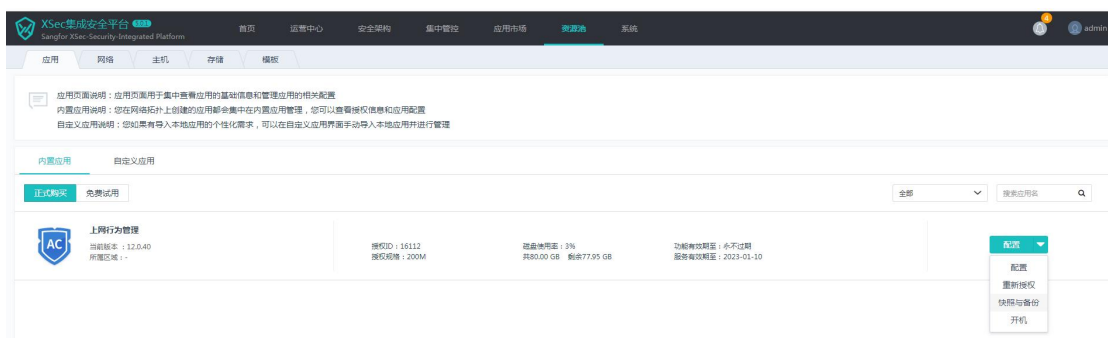
修改应用的规格

在用户侧的【资源池】->【应用】界面，能够对应用更改规格



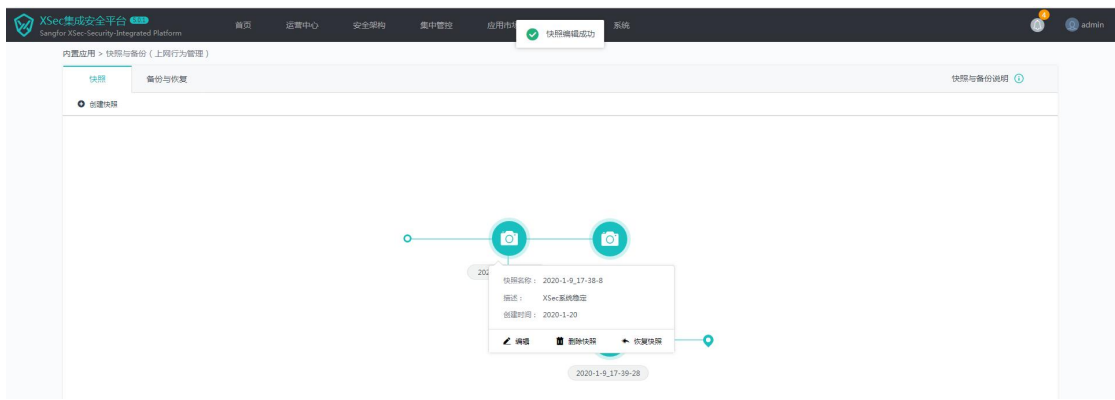
应用快照

用户可以在【资源池】-【应用】页面进入应用的快照与备份页面。



快照是数据存储某一时刻的状态记录，数据恢复速度较快。但在原数据损坏时，无法通过快照恢复数据，主要用于临时回滚操作。

系统不会永久保存快照，默认 5 天后自动清理。



应用备份

用户可以在【资源池】-【应用】页面进入应用的快照与备份页面。



备份是数据存储的某一个时刻的副本，灾备可靠性更高，原数据存储损坏可备份恢复，适应于生产环境。

备份支持全量备份和增量备份，新存储首次为全量备份耗时长，后续为增量备份耗时长短。

恢复备份后，原应用将被关机并删除，30天内可以联系技术支持还原，超期将被自动清理，且不会改变应用的硬件信息，应用操作系统或者软件不需要重新进行授权。应用恢复备份后，网络会与原来保持一致。



7.5.2 网络管理

网络管理页面可以查看主机网口用途及 IP 地址、修改管理地址、设置聚合网口等。

运维管理设置 聚合网口设置						
名称	用途	IP	掩码	网关	网口速率	
199.200.5.119						
eth0	管理口	199.200.5.119	255.255.255.0	199.200.5.1	自动协商 (1000M / 全双工)	
eth1	扩容保留网口	197.231.200.1	255.255.255.0	-	自动协商不成功	
eth2	审计专网	-	-	-	自动协商不成功	
eth3	物理出口	-	-	-	自动协商不成功	
eth4	-	-	-	-	自动协商不成功	
eth5	物理出口1	-	-	-	自动协商不成功	
eth6	物理出口3	-	-	-	10000M / 全双工	
eth7	物理出口2	-	-	-	10000M / 全双工	
eth8	-	-	-	-	10000M / 全双工	
eth9	-	-	-	-	10000M / 全双工	

运维管理设置 ×

CSSP管理IP :

通过https://199.200.5.118 访问并管理该平台

主机IP :

子网掩码 :

网关 :

新增聚合网口 ×

主机 :

聚合网口 :

描述 :

聚合方式 :

网口名称 :

> 高级设置

7.5.3 主机扩容

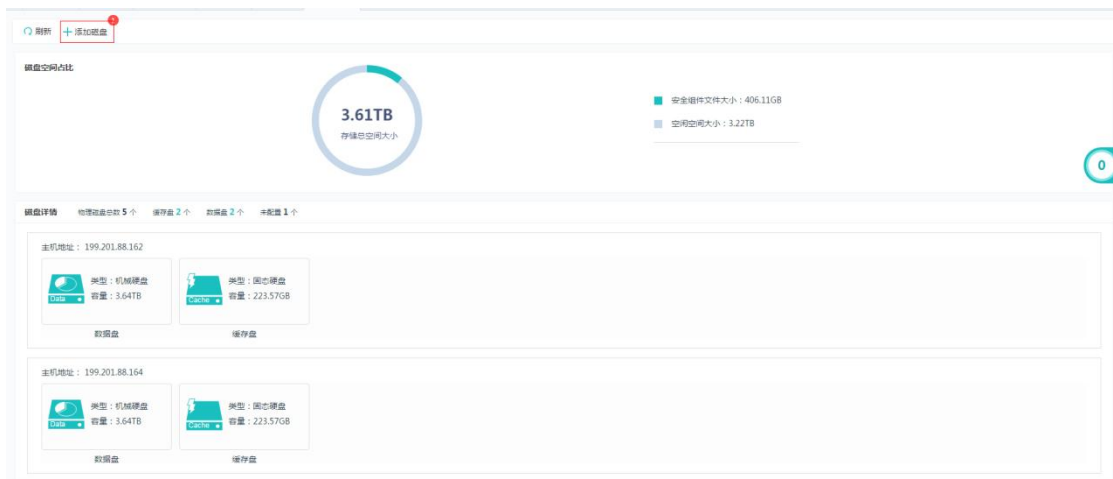
随着业务的发展，安全服务平台会存在资源不够的情况。进入【资源池】->【主机】页面，通过添加主机的方式，增加主机资源。



添加主机的过程，详见 2.3 配置安全服务平台。

7.5.4 磁盘扩容

用户可以在【资源池】->【存储】页面中，添加磁盘



注：只支持集群环境下，主机磁盘扩容

7.5.5 模板管理

进入资源池，点击模板，可查看组件的模板信息，并上传模板。

模板名称	当前版本	版本发布时间	操作	
应用交付	AF7.3.61R2 20181219	7.3R2	2018-12-19 10:00:10	删除
上网行为管理	AF8.0.8 20190530	8.0.8	2019-05-30 18:26:30	删除
数据库安全审计	AF8.0.8 20190709	8.0.8	2019-07-09 11:17:01	删除

7.6 系统

7.6.1 平台升级

平台升级

当前版本 5.0.0 (182 Build20190929)

请选择升级文件

7.6.2 管理员账号

XSEC 管理员支持三权分立配置，以及设置密码安全策略、登录失败策略。

+ 新增 × 删除 密码安

新增管理员

三权分立 安全管理员

审计员

系统管理员

新增管理员账号 ×

用户名:

描述:

登录安全设置 页面权限设置

全部可编辑 全部只允许查看

模块	编辑权限	查看权限
首页	<input type="checkbox"/>	<input checked="" type="checkbox"/>
安全架构	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
应用市场	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
资源池	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
系统	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

密码安全策略 ×

安全密码格式必须为：

- 1、密码不包含用户名
- 2、密码长度大于等于8位
- 3、必须同时包含字母、数字和特殊字符中的两者

下次登录必须修改密码

密码最长使用天数:

最大并发管理数： ↑

单用户的多重并发： 允许 禁止

登录失败重试： 次

登录超时： 分钟

允许访问的源IP： ⓘ

确定

取消

7.6.3 时间和日期

用于设置系统时间与日期，配置 NTP 服务器。

平台升级 管理员账号 时间与日期 操作日志 告警信息 平台授权 其他设置


17:34:59
2019年03月27日 星期三
(UTC+08:00)北京、上海、香港
[更改时间](#)

时间同步设置

与NTP服务器同步

服务器:

[保存配置](#)

7.6.4 操作日志

用于查看管理员操作日志

平台升级	管理员账号	时间与日期	操作日志	告警信息	平台授权	其他设置	
刷新		搜索关键字		高级搜索			
状态	操作人	操作主机	行为	对象	开始时间	结束时间	描述
成功	admin	172.16.1.133	登录	超级管理员	2019-03-27 16:49:19	2019-03-27 16:49:19	登录成功
成功	admin	172.16.1.133	登录	超级管理员	2019-03-27 15:55:47	2019-03-27 15:55:47	登录成功
成功	admin	172.16.1.133	登录	超级管理员	2019-03-26 17:39:10	2019-03-26 17:39:10	登录成功
成功	admin	172.16.1.133	登录	超级管理员	2019-03-26 11:08:17	2019-03-26 11:08:17	登录成功
成功	admin	172.16.1.133	进入控制台	基线核查系统	2019-03-26 10:59:42	2019-03-26 10:59:42	进入控制台成功
成功	admin	172.16.1.133	进入应用	基线核查系统	2019-03-26 10:59:39	2019-03-26 10:59:39	进入应用成功
成功	admin	172.16.1.133	进入控制台	运维安全管理	2019-03-26 10:57:10	2019-03-26 10:57:10	进入控制台成功
成功	admin	172.16.1.133	进入控制台	日志审计	2019-03-26 10:57:06	2019-03-26 10:57:06	进入控制台成功
成功	admin	172.16.1.133	进入控制台	基线核查系统	2019-03-26 10:55:23	2019-03-26 10:55:23	进入控制台成功
成功	admin	172.16.1.133	登录	超级管理员	2019-03-26 10:43:51	2019-03-26 10:43:51	登录成功
成功	admin	172.16.1.133	登录	超级管理员	2019-03-13 19:26:57	2019-03-13 19:26:57	登录成功
成功	admin	172.16.1.133	登录	超级管理员	2019-03-11 14:13:39	2019-03-11 14:13:39	登录成功
失败	admin	172.16.1.133	登录	超级管理员	2019-03-11 14:13:38	2019-03-11 14:13:38	登录失败：用户名不存在或密码错误！剩余重试次数：2
失败	admin	172.16.1.133	登录	超级管理员	2019-03-11 14:13:35	2019-03-11 14:13:35	登录失败：用户名不存在或密码错误！剩余重试次数：3
失败	admin	172.16.1.133	登录	超级管理员	2019-03-11 14:13:33	2019-03-11 14:13:33	登录失败：用户名不存在或密码错误！剩余重试次数：4
成功	admin	172.16.1.133	登录	超级管理员	2019-03-11 11:23:52	2019-03-11 11:23:52	登录成功

7.6.5 告警信息

用于查看平台的告警信息


平台升级	管理员账号	时间与日期	操作日志	告警信息	平台授权	恢复默认配置	高可用	其他设置
刷新								
2020-02-20 22:11:45				<p>【平台未联网】云安全平台 云安全平台未联网，不能及时的获取最新的应用和安全资讯，请联系服务商进行处理</p>				
2019-05-06 19:45:32				<p>【平台恢复联网】云安全平台 云安全平台恢复联网，当前可能的作用：获取最新的应用和安全资讯</p>				
2019-05-03 19:23:35				<p>【网口掉线告警】主机 (199.201.91.15) 的网口 (eth4) 主机 (199.201.91.15) 的网口 (eth4) 掉线。建议：请检查该网口网线是否插好。</p>				
2019-05-03 19:23:32				<p>【网口掉线告警】主机 (199.201.91.14) 的网口 (eth4) 主机 (199.201.91.14) 的网口 (eth4) 掉线。建议：请检查该网口网线是否插好。</p>				
2019-05-03 19:23:32				<p>【网口掉线告警】主机 (199.201.91.14) 的网口 (eth6) 主机 (199.201.91.14) 的网口 (eth6) 掉线。建议：请检查该网口网线是否插好。</p>				
2019-05-03 19:23:32				<p>【网口掉线告警】主机 (199.201.91.14) 的网口 (eth7) 主机 (199.201.91.14) 的网口 (eth7) 掉线。建议：请检查该网口网线是否插好。</p>				
2019-05-03 18:52:46				<p>【网口上线提醒】主机 (199.201.91.14) 的网口 (eth2) 主机 (199.201.91.14) 的网口 (eth2) 恢复上线。</p>				

7.6.6 平台授权


用于激活及更新授权

平台升级 管理员账号 时间与日期 操作日志 告警消息 平台授权 恢复默认配置 高可用 其他设置

平台授权状态

 已激活
产品ID: ED5623271011E06

组织名称: 豫科测试 邮箱:
联系人: 手机号码:

授权详情  授权总数 130 当前已使用 6 剩余授权 124

平台授权
设备ID: ED5623271011E06

功能模块	规格	功能有效期至	服务有效期至	状态
日志中心	500M	永不过期	2020-07-16	已使用

深信服应用授权

可授权应用类型	规格	功能有效期至	服务有效期至	状态
下一代防火墙	4G	永不过期	2019-08-31	未使用
上网行为管理	200M	永不过期	2020-03-03	已使用
上网行为管理	200M	永不过期	2020-03-03	未使用
上网行为管理	200M	永不过期	2020-03-03	未使用

7.6.7 恢复默认配置

用于恢复平台默认配置，目前只支持单机恢复默认配置，集群环境不支持。



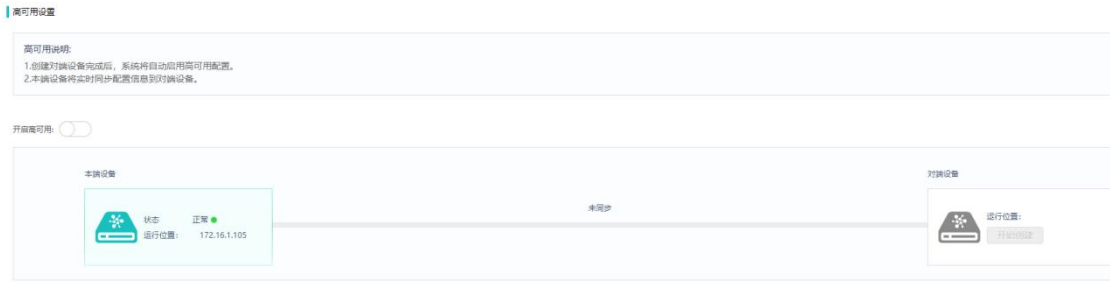
恢复默认配置说明

恢复默认配置后，平台登录密码将会恢复到初始值，同时平台配置信息和日志将会被清空，包括：已创建组件，组件连线，和相关组件日志等。平台管理IP不会更改，请牢记平台管理IP，恢复后将跳转到登录页面。

[恢复默认配置](#)

7.6.8 高可用

用于开启 CSSP 高可用，工控机集群场景建议开启。



7.6.9 其他设置

用于开启后台接入服务以及是否同意隐私政策

