



明御®数据库审计与风险控制系统

V4.0.69

软件安装指南

文档版本：01

发布日期：2022-11-19



本文中出现的任何文字描述、文字格式、插图、照片、方法等内容，除另有特别注明，版权均属杭州安恒信息技术股份有限公司（简称“安恒信息”）所有，受到有关产权及版权法保护。任何个人、机构未经安恒信息的书面授权许可，不得以任何方式复制或引用本文的任何片段。

经授权使用本文中内容的单位或个人，应在授权范围内使用，并注明“来源：安恒信息”。违反上述声明者，安恒信息保留追究其法律责任的权利。

除杭州安恒信息技术股份有限公司的商标外，本手册中出现的其他商标、产品标识及商品名称，由各自权利人拥有。

This file is restricted to the personal use of 134****1101 time: 2022-11-25
source: bbs.dbappsecurity.com.cn

文档说明

产品名称		明御®数据库审计与风险控制系统（软件版）	
适用平台/版本		V4.0.69	
拟制人	AH8505（AiLPHA-数据库审计）	评审组	AH6861（远程技术支持-标准文档）
发布人	AH5888（远程技术支持-标准文档）	备注	受控文档

修订记录

日期	修订版本	修改记录	修改人
2022-11-19	01	初次发布	AH5888（远程技术支持-标准文档）

目 录

前言	1
1 安装简介	1
1.1 部署模式	1
1.1.1 单机部署	1
1.1.2 分布式部署	2
1.2 安装方案	2
2 安装前准备	4
2.1 检查安装环境	4
2.2 获取软件安装包	4
2.3 安装工具	4
2.4 合同信息准备	5
2.5 数据规划	5
2.5.1 IP 地址规划	5
2.5.2 端口资源规划	5
3 创建 CentOS 系统虚拟机	7
3.1 虚拟机配置要求	7
3.2 为虚拟机设置 IP 地址的注意事项	7

3.3 操作步骤	7
4 在虚拟机上安装云 DAS-DBAuditor	20
4.1 安装步骤	20
4.2 安装后验证	21
5 基本配置	23
5.1 申请并导入许可证文件	23
5.2 安装 Agent	24
5.3 分布式部署配置	28

前言

概述

感谢您选择安恒信息的网络安全产品。本手册详细介绍了明御®数据库审计与风险控制系统软件版（简称“云 DAS-DBAuditor”）的安装方法。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异——说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于安装云 DAS-DBAuditor 的读者，包括运维工程师、网络管理员等。本文假设读者对以下领域的知识有一定了解：





- ◆ TCP/IP 基础网络通讯协议
- ◆ Linux 系统基本操作
- ◆ 虚拟机原理

格式约定

本手册内容格式约定如下。

内容	说明
粗体字	Web 界面中的各类控件名称以及内容。例如：“在菜单栏选择‘ 系统状态 ’进入 系统状态 页面，选择 接口状态 页签”。
<>	Web 界面中的按钮。例如：“微信认证失败，点击< 我要上网 >不弹出微信认证界面”。
➤	介绍 Web 界面的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等）。例如：“在菜单栏选择‘ 策略配置 ➤ 认证管理 ➤ 认证策略 ’查看是否开启了认证策略”。
<i>斜体字</i>	可变参数，必须使用实际值进行替代。例如：“在浏览器地址栏输入‘http:// <i>管理 IP</i> ’，回车后进入系统 Web 管理平台登录页面”。

本手册图标格式约定如下。

图标	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或者数据丢失。
	警告，该图标后的内容需引起格外重视，否则可能导致人身伤害。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 <https://bbs.dbappsecurity.com.cn> 获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310051

电话：0571-88380999

传真：0571-28863666

官网：<http://www.dbappsecurity.com.cn>

邮箱：400-doc@dbappsecurity.com.cn

1 安装简介

1.1 部署模式

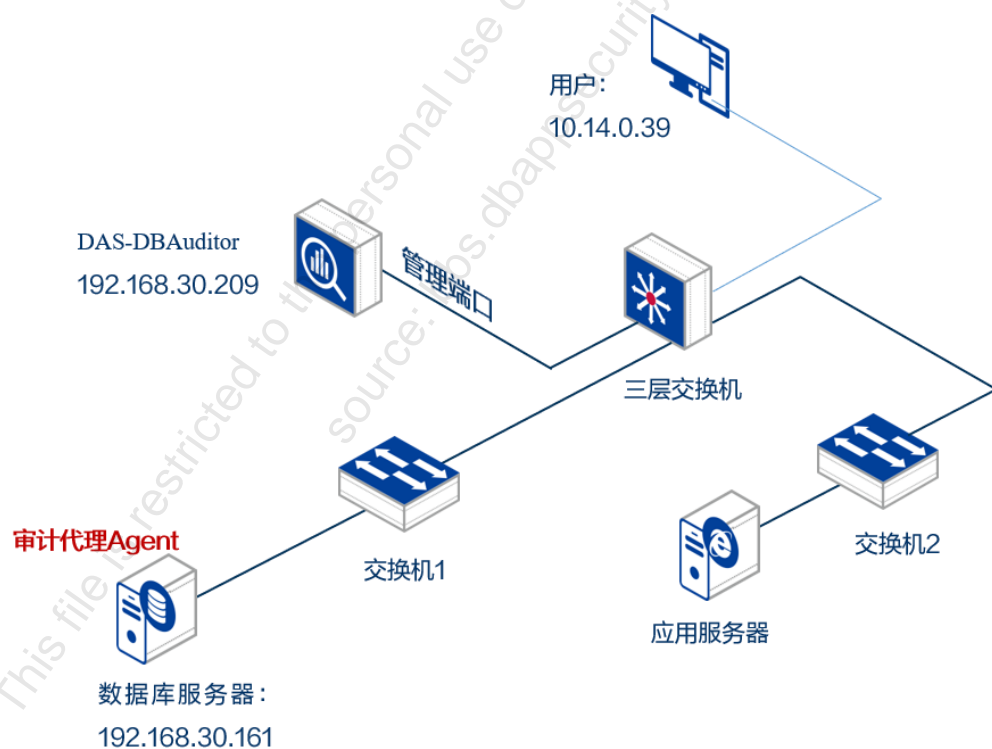
云 DAS-DBAuditor 主要分为两种部署模式：单机部署与分布式部署，并且由许可证书控制部署的模式。

1.1.1 单机部署

适用场景：用户数据库流量未超过单机处理性能，对可靠性要求一般。

云 DAS-DBAuditor 支持以下两种方式采集数据库流量信息：

- ◆ 流量代理方式：在宿主机上安装 Agent，Agent 将数据库流量信息发送至云 DAS-DBAuditor。宿主机可以是数据库系统所在主机，也可能是访问数据库系统的应用系统所在主机，或是运维数据库的运维终端。流量代理根据 DAS-DBAuditor 上配置的资产信息，通过在安装审计代理插件的服务器上的网卡抓取数据库请求和响应报文，并将报文发送到 DAS-DBAuditor 上。流量代理方式的网络拓扑如下图所示。

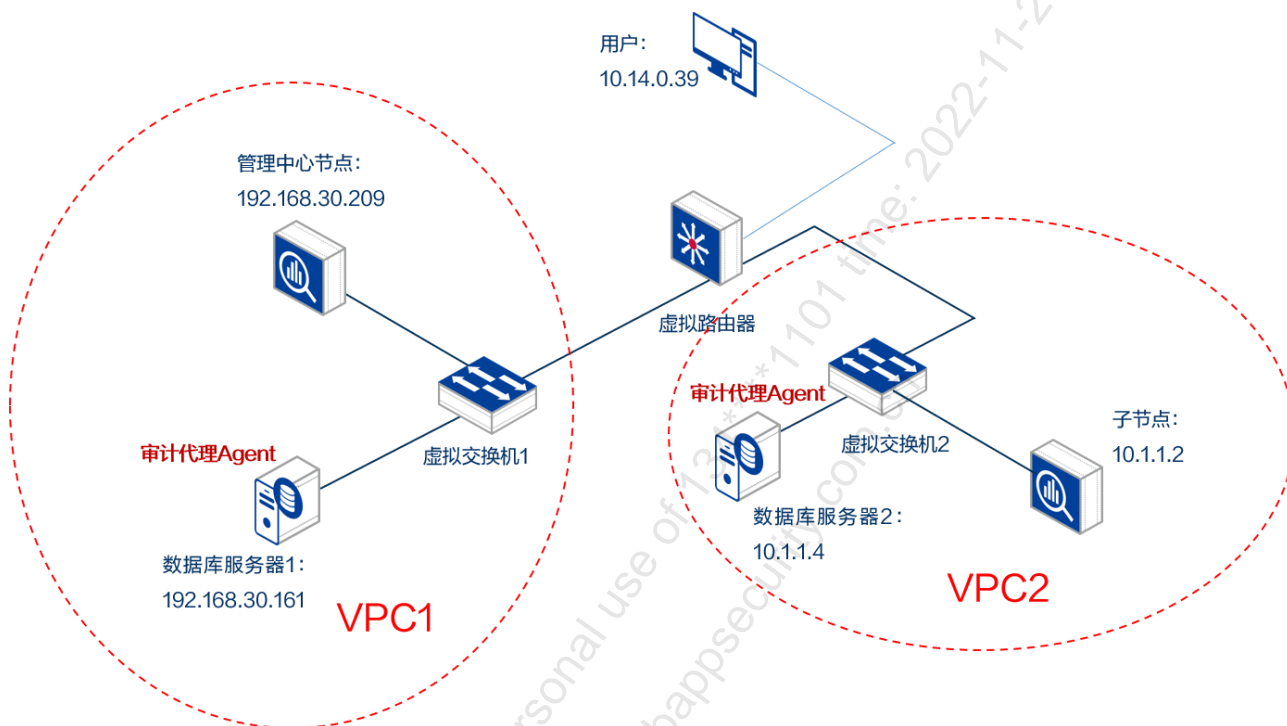


- ◆ 端口镜像方式：在虚拟交换机上配置端口镜像，将数据库流量镜像至云 DAS-DBAuditor。通过云控制台进行端口镜像的方式，将访问数据库系统的流量通过端口镜像的方式镜像到 DAS-DBAuditor 的网口上。

1.1.2 分布式部署

适用场景：用户数据库流量较大，超过单机处理性能，且数据库服务器分散于不同地区的机房。

该场景下需要部署多台云 DAS-DBAuditor，部署后需要登录管理中心节点进行分布式配置。典型组网如下图所示。

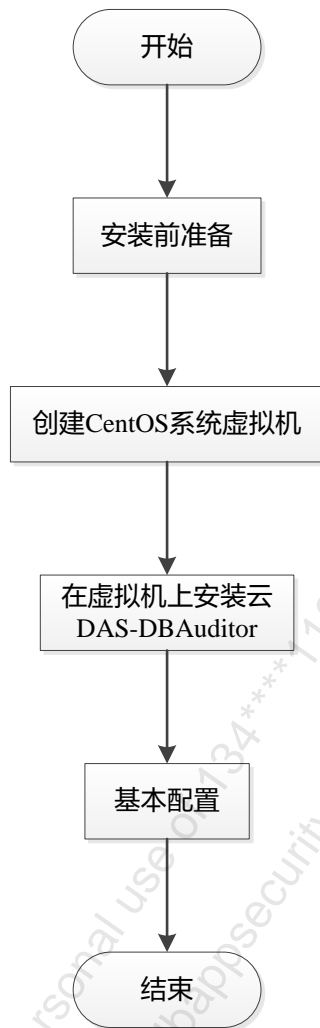


1.2 安装方案

云 DAS-DBAuditor 支持部署在主流云平台，包括采用 KVM 和 ESXi 等主流虚拟化技术的云平台。

用户只需要在云平台上创建一台 CentOS 系统虚拟机（分布式部署时需要创建多台 CentOS 系统虚拟机），然后在虚拟机上安装云 DAS-DBAuditor 软件，导入许可文件后即可完成云 DAS-DBAuditor 的安装。

安装流程如下图所示。



- 步骤1. [安装前准备](#)，主要包括安装环境检查、安装文件准备以及数据规划等。
- 步骤2. [创建 CentOS 系统虚拟机](#)。
- 步骤3. [在虚拟机上安装云 DAS-DBAuditor](#)。
- 步骤4. [基本配置](#)。

2 安装前准备

2.1 检查安装环境

检查客户的云平台是否支持安装云 DAS-DBAuditor。支持安装云 DAS-DBAuditor 的云平台如下表所示。

虚拟化技术	云平台	备注
KVM	<ul style="list-style-type: none"> ◆ OpenStack ◆ 阿里云、AWS 等常见公有云 	大部分私有云平台基于 KVM 技术。
ESXi	VMware vSphere Server	支持 VMware Workstation 平台，仅供测试评估。

2.2 获取软件安装包

安装前，请获取以下软件安装包。

项目	名称	获取路径	备注
CentOS 安装镜像包	CentOS-7.6-x86_64-DVD-1810.iso	各大公有云网站下载或者 CentOS 官方网站下载。	必须是 CentOS-7.6-x86_64-DVD-1810.iso 镜像文件。
云 DAS-DBAuditor 软件安装包	dbaudit-4.0.69.221103.2013-install.zip	登录安恒社区，在菜单栏选择“产品中心>网络安全基础产品>安全防护产品>明御数据库审计与风险控制系统”，选择软件下载页签，点击“软件版本>V4.0.68 版本”，找到对应的软件安装包并且下载。	请校验软件安装包的 MD5 码（3daaa93ac40c8b9e58dc1334224e5888），用于验证软件安装包的完整性。

2.3 安装工具

安装前，请准备好以下安装工具。

项目	名称	获取路径
终端连接工具	XShell 或 SecureCRT 等	推荐工具官网下载并安装。
FTP 工具	Xftp 等	推荐工具官网下载并安装。
浏览器	Chrome 浏览器	推荐工具官网下载并安装。

2.4 合同信息准备

云 DAS-DBAuditor 安装完成后，需要查看设备序列号，然后致电安恒信息客服热线 400-6059-110 申请许可。申请许可需要用到用户的商务合同信息，包括客户名称、合同类型、合同编号、产品类型等。建议提前做好。

2.5 数据规划

2.5.1 IP 地址规划

为适配用户网络环境，需提前进行 IP 地址规划。下表仅为示例，具体请以实际为准。

数据类型	参数	样例
设备信息（管理中心节点）	管理平面 IP 地址	192.168.1.4
	管理平面子网掩码	255.255.255.0
	管理平面网关	192.168.1.1
设备信息（子节点 1）	管理平面 IP 地址	192.168.1.10
	管理平面子网掩码	255.255.255.0
	管理平面网关	192.168.1.1
设备信息（子节点 2）	管理平面 IP 地址	192.168.1.11
	管理平面子网掩码	255.255.255.0
	管理平面网关	192.168.1.1

2.5.2 端口资源规划

为保证云 DAS-DBAuditor 能访问第三方系统或被第三方系统访问，需开放以下端口。

- ◆ 单机部署且采用镜像流量方式时。

源设备	源端口	目的设备	目的端口	协议	使用场景
客户端 PC	随机分配	DAS-DBAuditor	443	TCP	用于客户端 PC 访问 DAS-DBAuditor 的 Web 管理平台。
			22	TCP	客户端通过 SSH 方式访问 DAS-DBAuditor。
			3306	TCP	客户端 PC 访问 DAS-DBAuditor 的后台数据库。
网管系统	随机分配	DAS-DBAuditor	161	UDP	网管系统通过 SNMP 协议管理 DAS-DBAuditor。
DAS-DBAuditor	随机分配	NTP 服务器	123	UDP	DAS-DBAuditor 从 NTP 服务器同步时间。
		邮件服务器	25	TCP	DAS-DBAuditor 发送告警信息至邮件服务器。
		FTP 服务器	21	TCP	DAS-DBAuditor 发送配置备份数据至 FTP 服务器。或通过 FTP 服务器进行配置恢复。
		Syslog 服务器	514	UDP	DAS-DBAuditor 发送日志信息至 Syslog 服务器。

◆ 单机部署且采用 Agent 方式获取审计流量时，相对于镜像流量部署，需要增加开放以下端口。

源设备	源端口	目的设备	目的端口	协议	使用场景
数据库服务器	随机分配	DAS-DBAuditor	13001	TCP	DAS-DBAuditor 下发配置信息至 Agent。
			13002	TCP	DAS-DBAuditor 接收 Agent 发送的数据。

◆ 分布式部署时，相对于单机部署，需要增加开放以下端口。

协议	端口	使用场景	需开放此端口的设备
TCP	8443	用于管理中心节点与探测器节点通讯。	需要管理中心节点和探测器节点均开放此端口。
TCP	9300	审计数据查询用端口。	需要管理中心节点和探测器节点均开放此端口。

3 创建 CentOS 系统虚拟机

3.1 虚拟机配置要求

安装云 DAS-DBAuditor 对虚拟机软硬件配置有要求。如果虚拟机配置过低，可能会导致云 DAS-DBAuditor 无法安装或者无法正常运行。用户流量增大，最低配置要求也要变高，对于大流量客户，必须使用超过最低配置的服务器。



- ◆ 由于没有采用推荐虚拟机配置要求的服务器导致数据丢失或者其他运行问题，安恒信息无法承诺提供售后服务支持。
- ◆ 虚拟机最低配置要求如下表所示，实际应用中请尽量使用更高配置的虚拟机资源。

项目 \ 型号	DAS-1500-C1	DAS-1500-C2	DAS-1500-C3	DAS-1500-C4	DAS-1500-C5	DAS-1500-C6
操作系统	CentOS 7.6 (1810) 版本，内核版本：3.10.0-957.21.3.el7.x86_64					
CPU	2 核	2 核	4 核	8 核	16 核	32 核
内存	8GB	8GB	16GB	32GB	32GB	64GB
数据盘（必选）	1TB	1TB	2TB	4TB	4TB	10TB
网卡	至少一张网卡，推荐虚拟网卡类型为 Intel E1000 或 Virtio，其它网卡类型可能缺少驱动。					

3.2 为虚拟机设置 IP 地址的注意事项

虚拟机获取 IP 地址的方式有两种：自动分配地址和手工静态分配地址。

- ◆ **自动分配：**CentOS 安装后通过 DHCP 方式自动分配 IP，无需手工创建 IP。
- ◆ **手工静态分配：**CentOS 安装后没有配置 IP，需要手工修改接口配置文件（/etc/sysconfig/network-scripts/ifcfg-*，其中“*”表示网卡名称），手动添加 IP 地址（具体数据请参见 [IP 地址规划](#)）等。

3.3 操作步骤

步骤1. 登录云控制台，参考[虚拟机配置要求](#)，创建虚拟机。



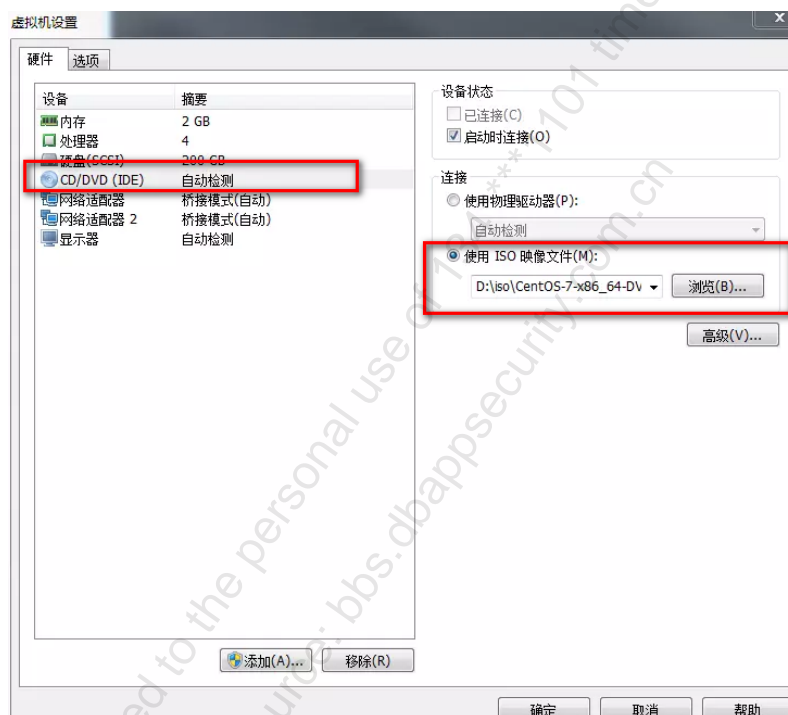
- ◆ 创建虚拟机一般由云平台管理员完成。
- ◆ 某些虚拟机平台例如 VMware，在创建虚拟机的时候，CD/DVD 驱动器可以直接选择使用本地的 CentOS7.6 (1810) 操作系统镜像文件。虚拟机创建完成后，启动虚拟机即可直接安装 CentOS 操作系统。

步骤2. 上传 CentOS 安装镜像包到虚拟机本地磁盘。

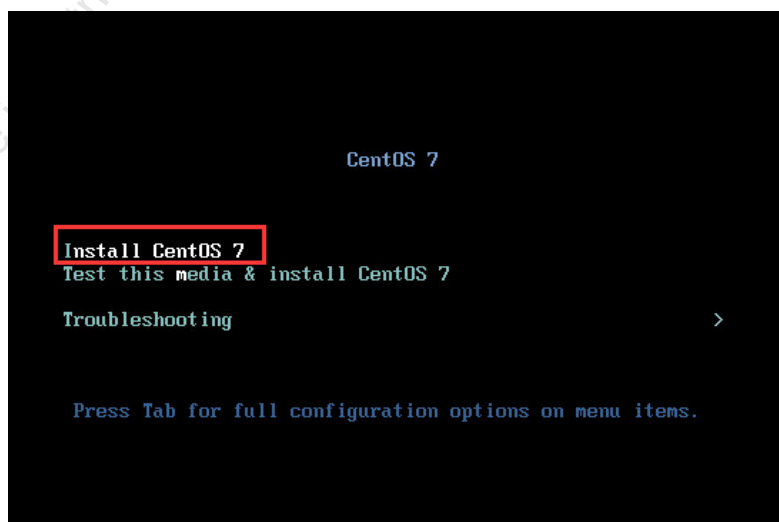
步骤3. 在创建好的虚拟机上安装 CentOS7.6 (1810) 版本。

1) 导入镜像安装包。

在虚拟机设置页面选择 CD/DVD (IDE)，选择使用 ISO 镜像文件，导入 CentOS 镜像安装文件。



2) 界面提示开始安装 CentOS，选择 **Install CentOS 7**，然后回车。



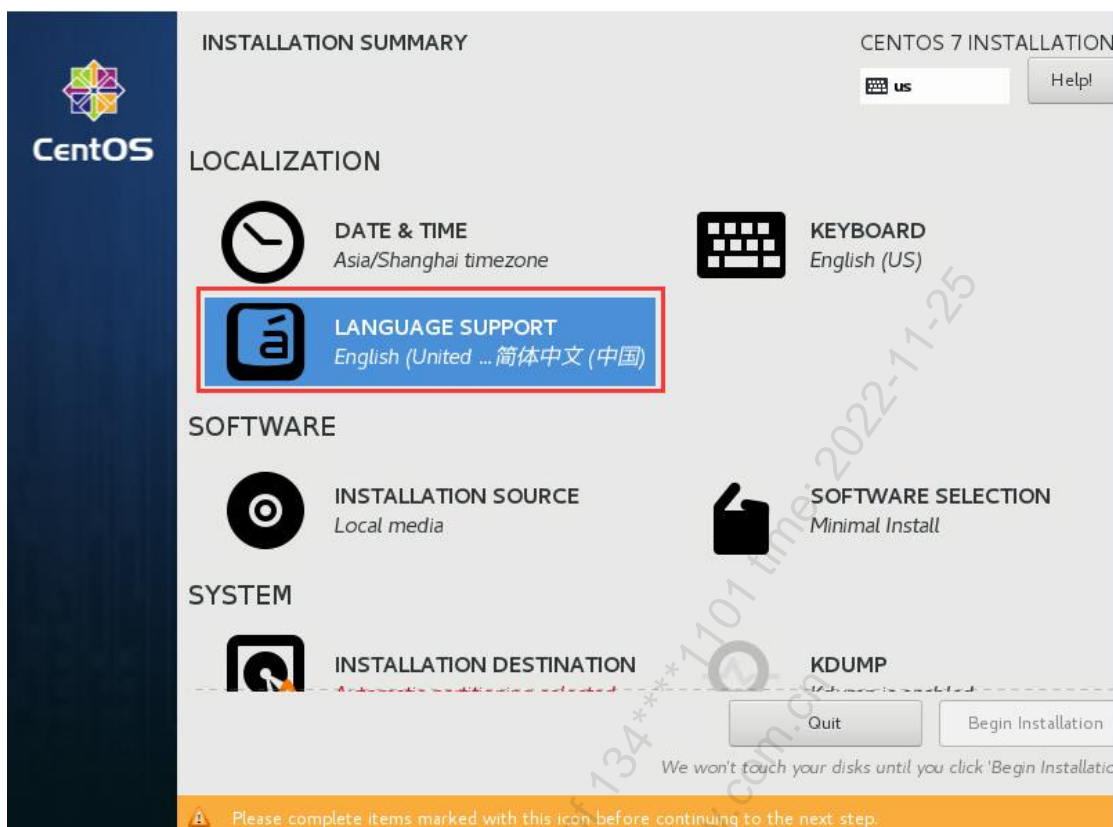
- 3) 进入系统安装界面，点击<DATE & TIME>。



- 4) 设置时区为“Asia/Shanghai”，并设置系统时间和日期，点击<Done>。



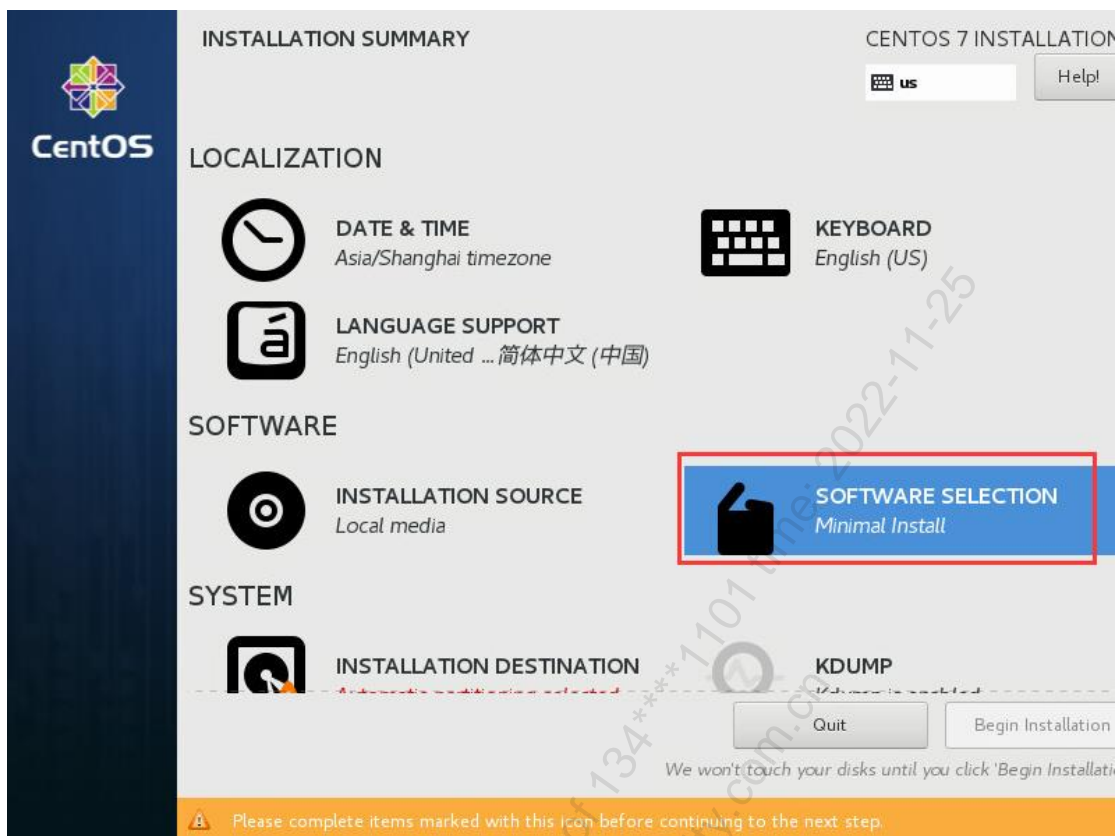
- 5) 点击<LANGUAGE SUPPORT>，配置系统支持的语言。



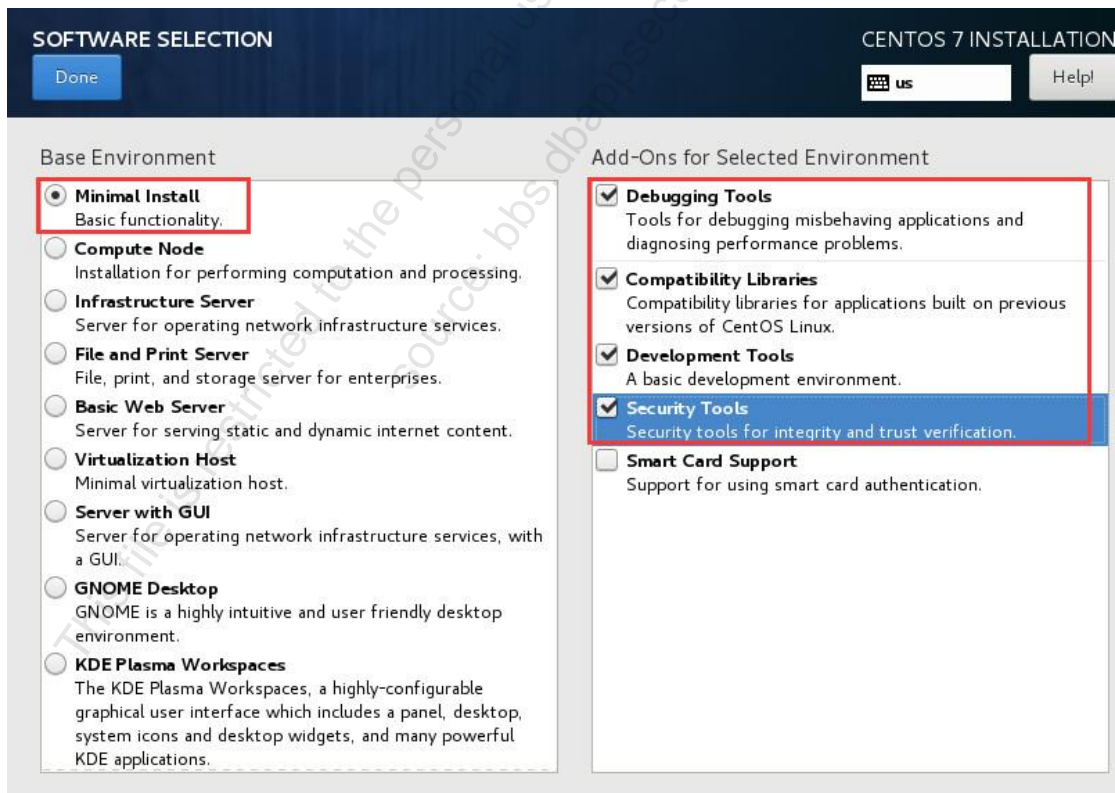
6) 选择 English 和 English(united states), 然后点击<Continue>。



7) 点击<SOFTWARE SELECTION>, 配置需要安装的组件。



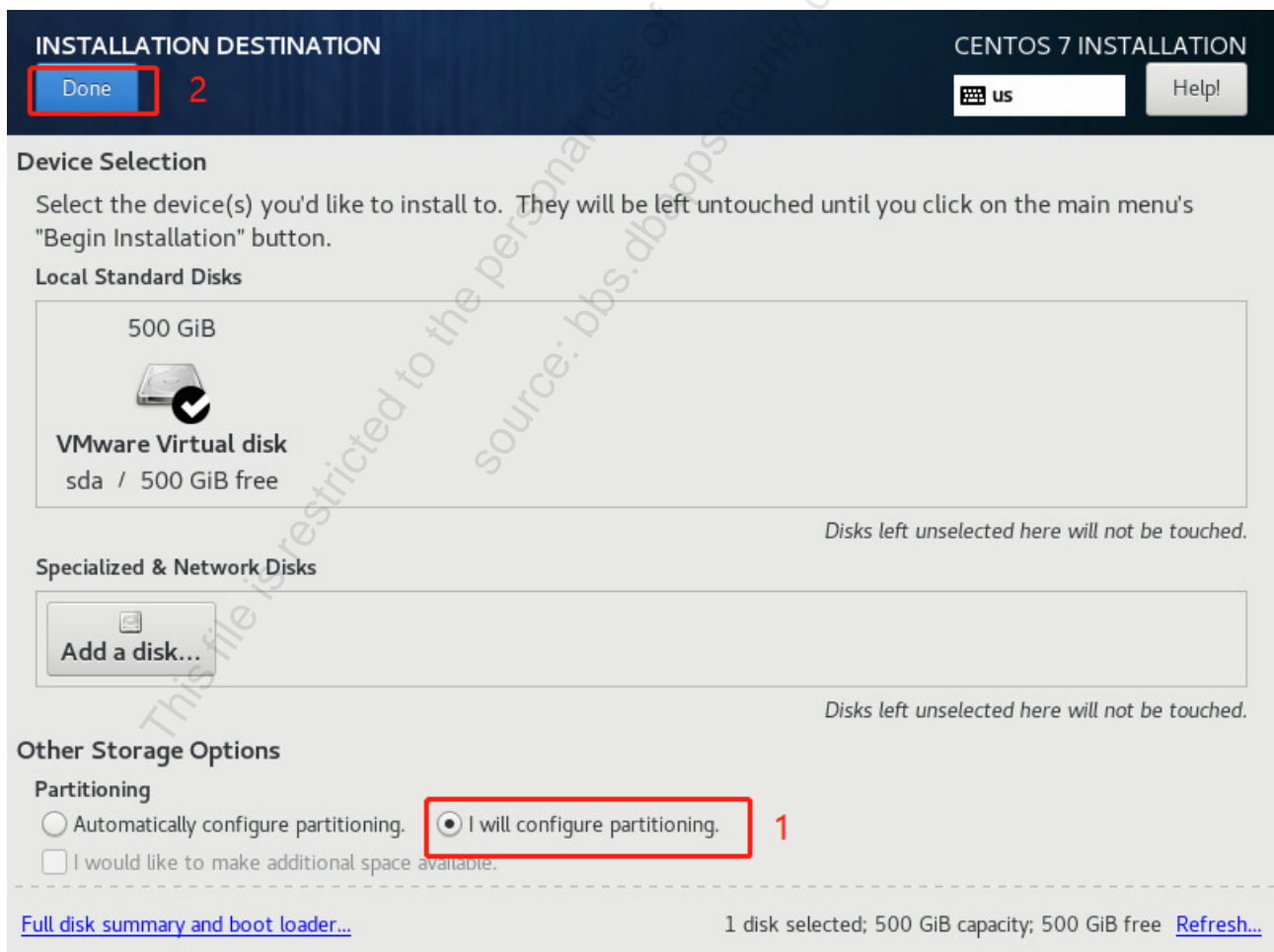
8) 选择 Minimal Install 和 Add-Ons 安装包，然后点击<Done>。



9) 点击<INSTALLATION DESTINATION>, 进行分区设置。

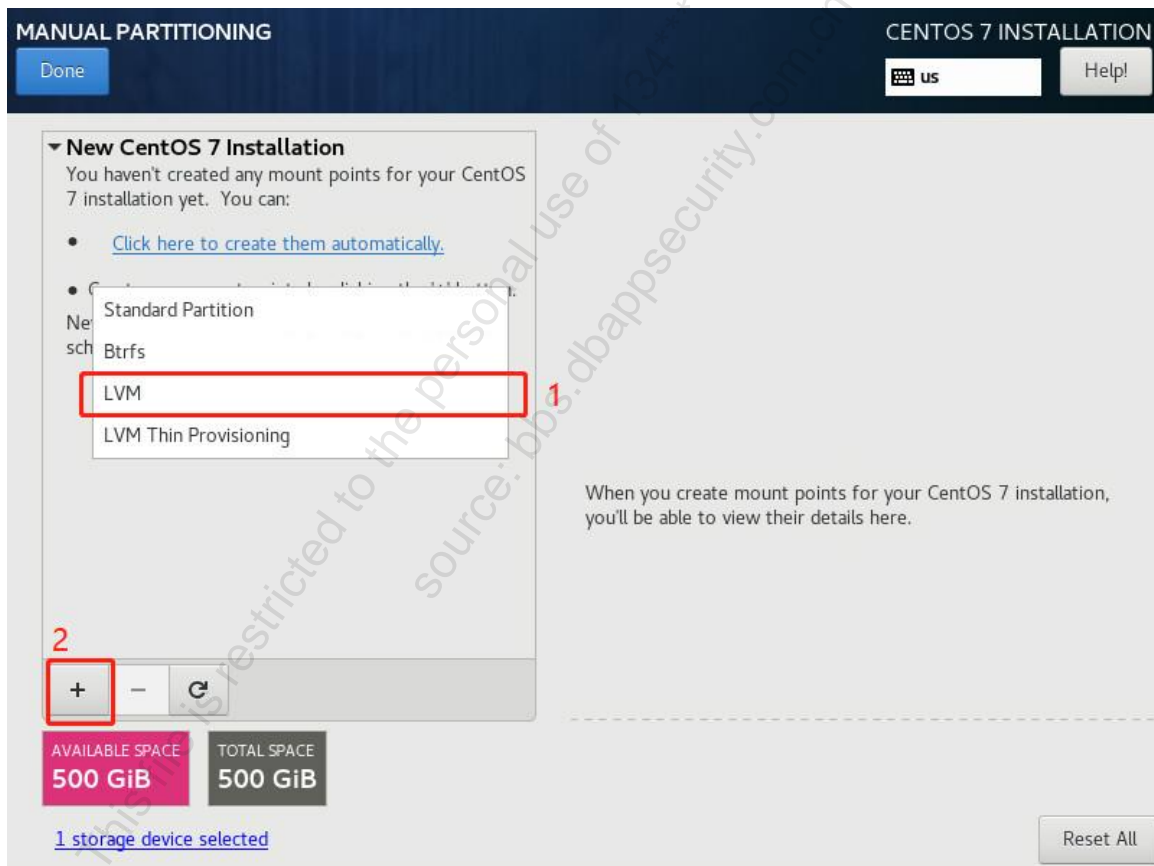


10) 选择 I will configure partitioning, 然后点击<Done>。



11) 选择 LVM，再点击 **+** 图标，创建分区。弹出 **ADD A NEW MOUNT POINT** 对话框，按照以下格式创建磁盘分区。填写完成后，点击 **<Add mount point>**。

- “Monut Point” 选择 /， “Desired Capacity” 填写为 50GiB， “Device Type” 选择 Standard Partition， “File System” 选择 xfs。
- “Monut Point” 选择 /boot， “Desired Capacity” 填写为 1024MiB， “Device Type” 选择 Standard Partition， “File System” 选择 xfs。
- “Monut Point” 选择 swap， “Desired Capacity” 填写为 32GiB， “Device Type” 选择 Standard Partition， “File System” 选择 swap。
- “Monut Point” 选择 /dbfw， “Desired Capacity” 填写为 50GiB， “Device Type” 选择 Standard Partition， “File System” 选择 xfs。
- “Monut Point” 选择 /data， “Desired Capacity” 填写为 剩余空间， “Device Type” 选择 LVM， “File System” 选择 xfs。



MANUAL PARTITIONING

CENTOS 7 INSTALLATION

Done

us

Help!

▼ New CentOS 7 Installation

SYSTEM

/

centos-root

50 GiB

>

centos-root

Mount Point:

/

Desired Capacity:

50 GiB

Device Type:

Standard ...

File System:

xfs

Device(s):

VMware Virtual disk (sda)

Modify...

Encrypt

Reformat

Label:

Name:

+

-

↺

AVAILABLE SPACE

450 GiB

TOTAL SPACE

500 GiB

[1 storage device selected](#)

Reset All

MANUAL PARTITIONING

CENTOS 7 INSTALLATION

Done

us

Help!

▼ New CentOS 7 Installation

SYSTEM

/boot

sda1

1024 MiB

>

/

sda2

50 GiB

sda1

Mount Point:

/boot

Desired Capacity:

1024 MiB

Device Type:

Standard ...

File System:

xfs

Device(s):

VMware Virtual disk (sda)

Modify...

Encrypt

Reformat

Label:

Name:

sda1

+

-

↺

AVAILABLE SPACE

449 GiB

TOTAL SPACE

500 GiB

[1 storage device selected](#)

Reset All

MANUAL PARTITIONING CENTOS 7 INSTALLATION

[Done](#) US [Help!](#)

▼ New CentOS 7 Installation

SYSTEM	Size
/boot sda1	1024 MiB
/ sda2	50 GiB
swap centos-swap	32 GiB >

AVAILABLE SPACE: **417 GiB** TOTAL SPACE: **500 GiB**

[1 storage device selected](#)

centos-swap

Mount Point:

Desired Capacity: [Modify...](#)

Device Type: ☐ Encrypt

File System: ☒ Reformat

Label:

Name:

[Reset All](#)

MANUAL PARTITIONING CENTOS 7 INSTALLATION

[Done](#) US [Help!](#)

▼ New CentOS 7 Installation

DATA	Size
/dbfw centos-dbfw	50 GiB >

SYSTEM	Size
/boot sda1	1024 MiB
/ sda2	50 GiB
swap sda3	32 GiB

AVAILABLE SPACE: **367 GiB** TOTAL SPACE: **500 GiB**

[1 storage device selected](#)

centos-dbfw

Mount Point:

Desired Capacity: [Modify...](#)

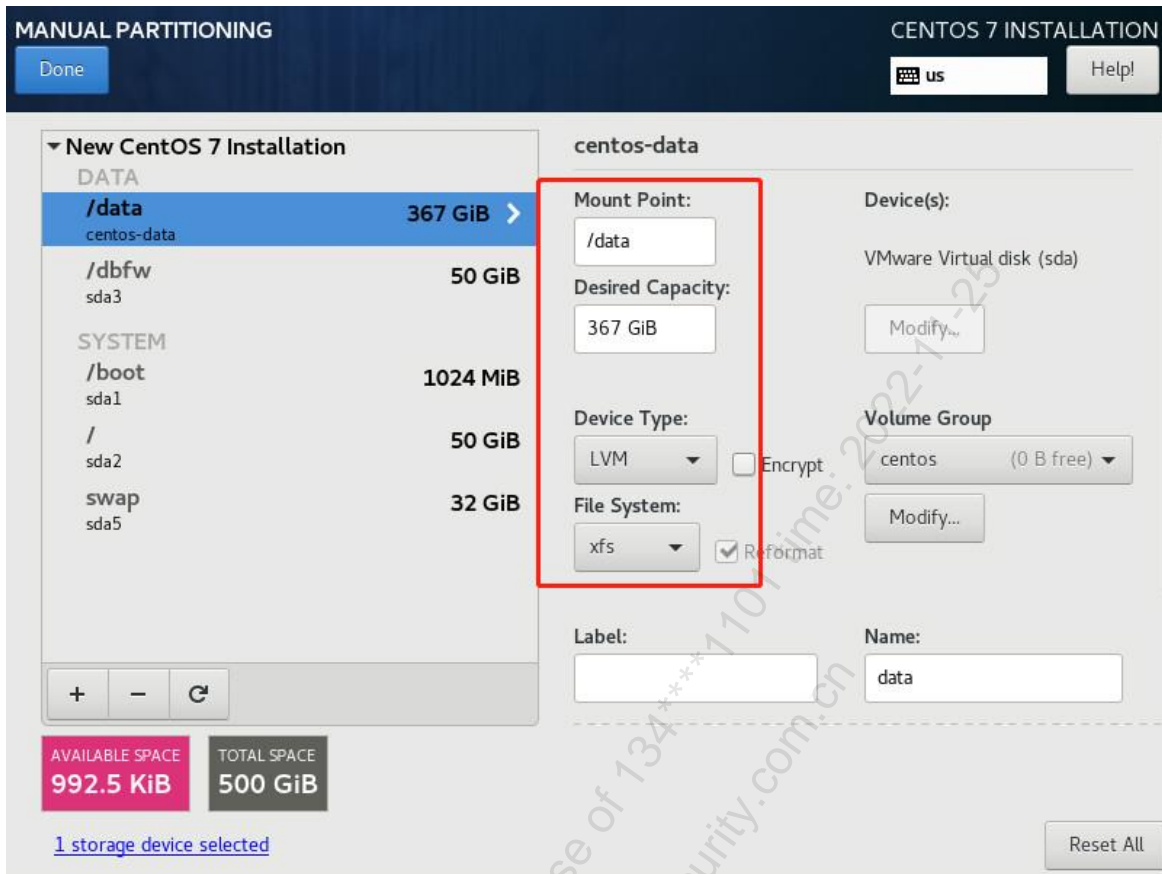
Device Type: ☐ Encrypt

File System: ☒ Reformat

Label:

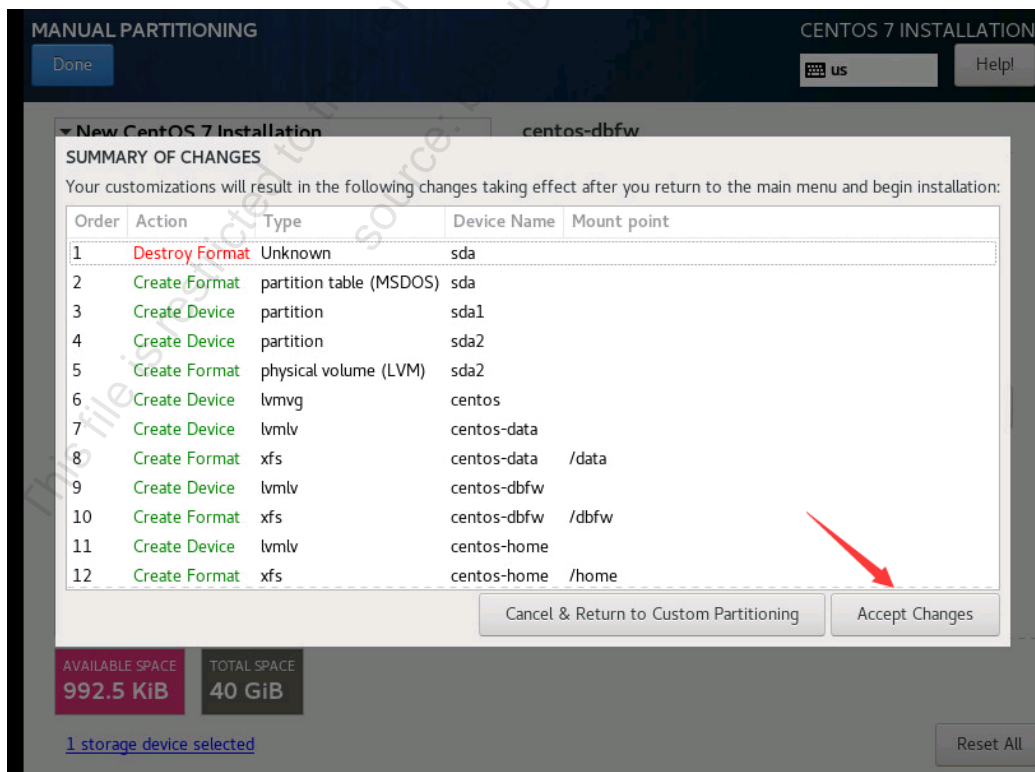
Name:

[Reset All](#)



12) 配置完成后，点击<Done>。

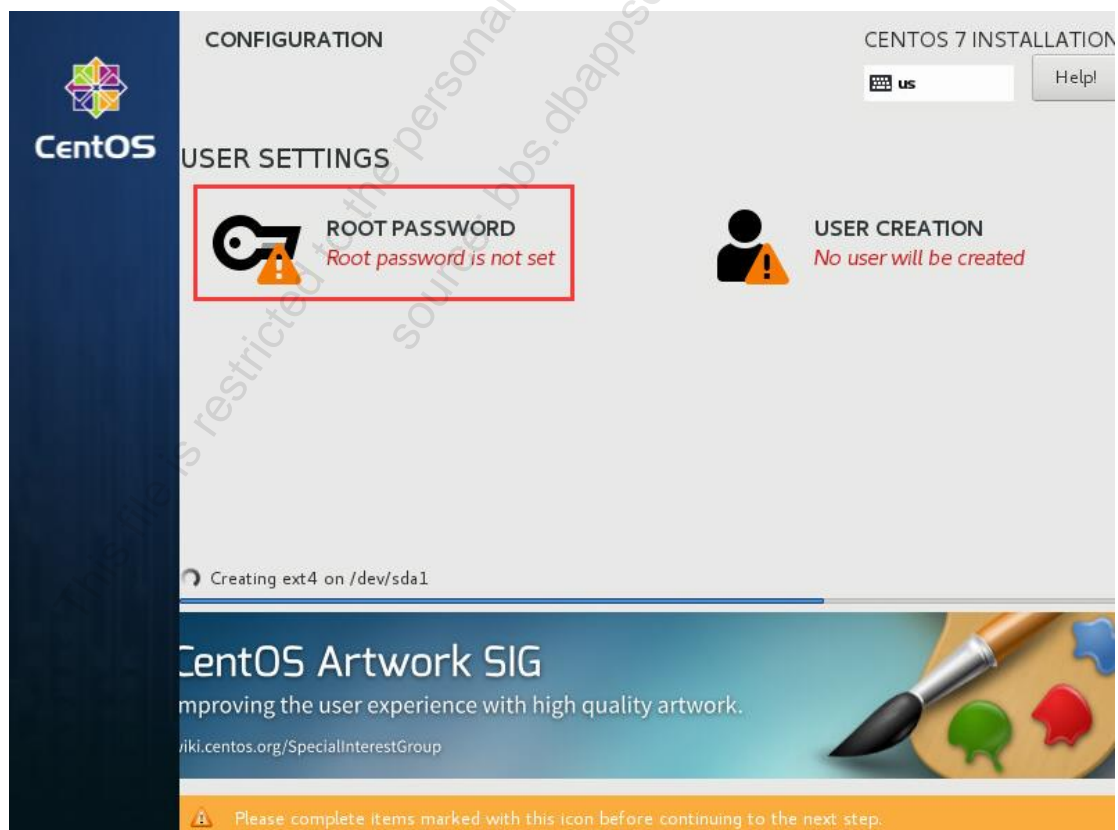
13) 点击<Accept Changes>。



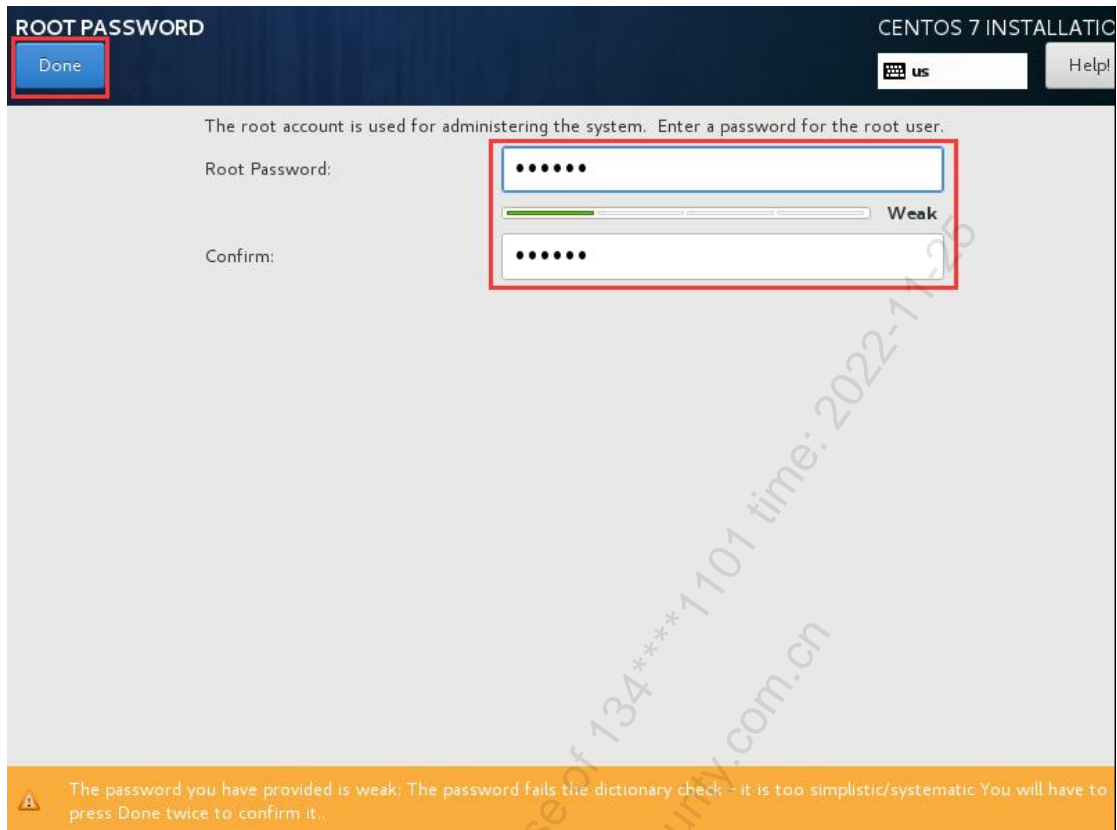
14) 点击<Begin Installation>, 开始安装。



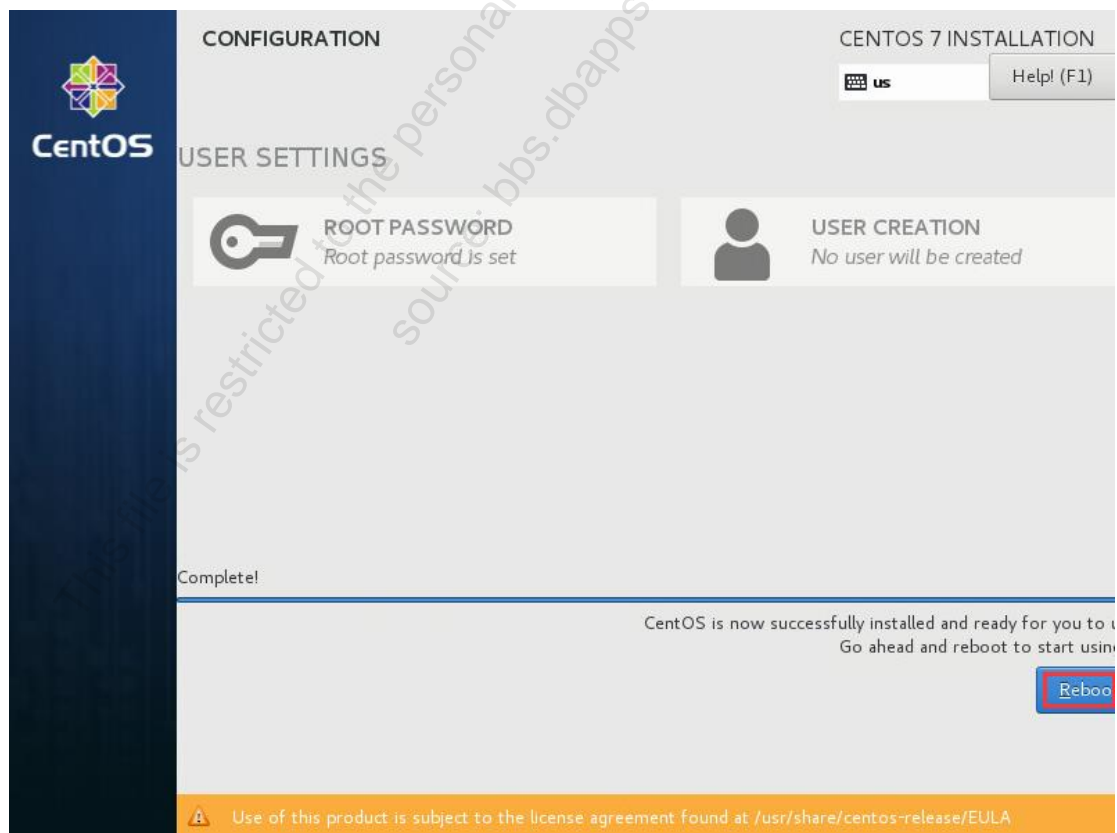
15) 点击<ROOT PASSWORD>, 配置 root 用户密码。



16) 设置密码并确认密码，点击<Done>。



17) 点击<reboot>，重启系统。



- 18) 重启完成后，可使用 root 用户登录系统。

```
CentOS Linux 7 (Core)  
Kernel 3.10.0-693.el7.x86_64 on an x86_64  
  
localhost login:
```

This file is restricted to the personal use of 134****1101 time: 2022-
source: bbs.dbappsecurity.com.cn

4 在虚拟机上安装云 DAS-DBAuditor

4.1 安装步骤

- 步骤1. 使用 Xftp 工具将安装包（dbaudit-4.0.69.221103.2013-install.zip）上传至虚拟机的/root 目录下。
- 步骤2. 使用 root 用户登录虚拟机操作系统，进入/root 目录，检验文件的 MD5 值，如 MD5 值正确，则解压安装包（解压密码为 yltest）。

```
[root@localhost ~]# cd /root

[root@localhost root]# md5sum dbaudit-4.0.69.221103.2013-install.zip

[root@localhost root]# unzip -P yltest /root/dbaudit-4.0.69.221103.2013-install.zip
```

```
[root@administrator ~]# ll
total 1029592
-rw-r--r-- 1 root root 1054298017 Nov  3 21:01 dbaudit-4.0.69.221103.2013-install.zip
[root@administrator ~]# unzip -P yltest /root/dbaudit-4.0.69.221103.2013-install.zip
Archive:  /root/dbaudit-4.0.69.221103.2013-install.zip
  creating: dbaudit-4.0.69.221103.2013/
  creating: dbaudit-4.0.69.221103.2013/service/
  inflating: dbaudit-4.0.69.221103.2013/service/load_resource
  inflating: dbaudit-4.0.69.221103.2013/service/dbaudit_upgrade
  inflating: dbaudit-4.0.69.221103.2013/service/mariadb
  inflating: dbaudit-4.0.69.221103.2013/service/javakafka
  inflating: dbaudit-4.0.69.221103.2013/service/java_audit_core
  inflating: dbaudit-4.0.69.221103.2013/service/sensor
  inflating: dbaudit-4.0.69.221103.2013/service/nginx
  inflating: dbaudit-4.0.69.221103.2013/service/java_audit_dsc
  inflating: dbaudit-4.0.69.221103.2013/service/dbfw
```

- 步骤3. 进入解压后的文件目录，执行 sh install.sh 命令进行安装。

```
[root@localhost ~]# cd /root/dbaudit-4.0.69.221103.2013

[root@localhost dbaudit-4.0.68.220621.0900]# sh install.sh
```

- 步骤4. 等待安装完成。如安装过程中有明显的 error 或者 warning 信息，请联系安恒信息客服热线 400-6059-110 获取帮助。



安装完成后 root 密码会自动修改。更改后的 root 密码需访问 DAS-DBAuditor Web 管理平台，在菜单栏选择“系统管理>系统维护>设备管理”进入设备管理页面，获取 SSH 登录 KEY 并联系安恒信息客服热线 400-6059-110 获取 root 密码。

- 步骤5. 如果安装后使用域名访问或公网地址访问数据库审计，页面会提示疑似 CSRF 问题。

输入默认用户名 [admin](#)，密码 [Dbapp@2013](#)，如果公网 IP 访问域名位置填写 [https://公网 IP](#)，域名访问域名位置填写 [https://域名](#)。

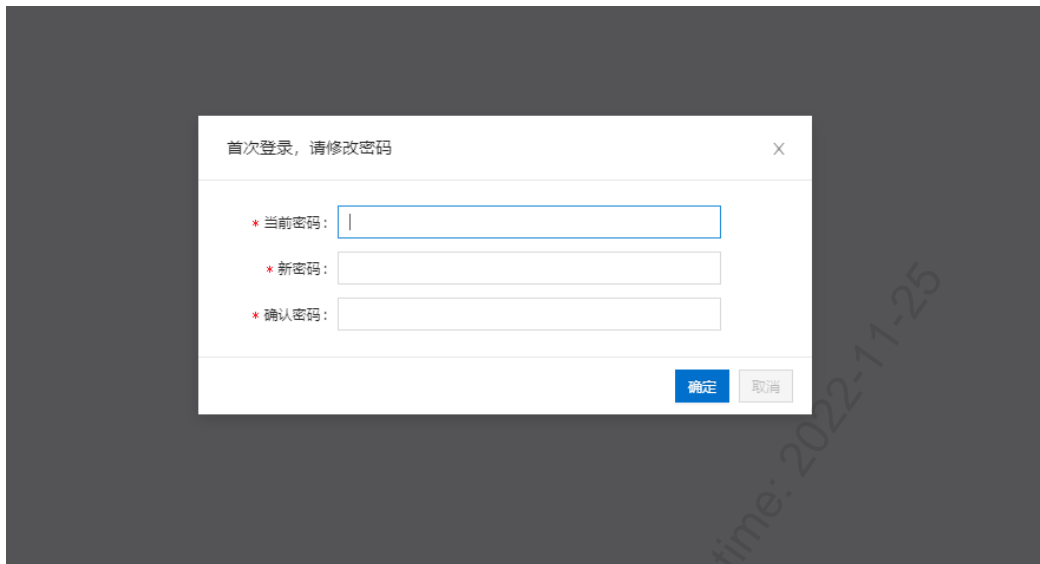


4.2 安装后验证

步骤1. 在客户端 PC（需要与云平台网络互通）浏览器地址栏中输入“[https://云 DAS-DBAuditor 的管理 IP](#)”，回车后进入系统登录界面，输入默认用户名 [admin](#)、密码 [Dbapp@2013](#)，点击<登录>。



步骤2. 首次登录系统需要修改密码。



步骤3. 登录系统后导入许可文件，验证系统功能是否可用。

5 基本配置

云 DAS-DBAuditor 安装后，需要进行一些基本配置才能使用产品的功能。主要包括申请并导入许可证文件、安装 Agent、分布式部署配置等。

5.1 申请并导入许可证文件



单机部署与分布式部署的许可类型不同，请注意区分。

DAS-DBAuditor 需要导入许可证后才能正常使用产品的功能。

步骤1. 登录系统 Web 管理平台，在菜单栏选择“系统管理>系统配置”进入系统配置页面，选择许可证页签，可查看设备序列号。



步骤2. 联系安恒信息客服热线 400-6059-110 申请许可证文件（需提供设备序列号信息）。

步骤3. 登录系统 Web 管理平台，在菜单栏选择“系统管理>系统配置”进入系统配置页面，选择许可证页签，点击<导入证书>，选择已获取的许可证文件，导入许可证。

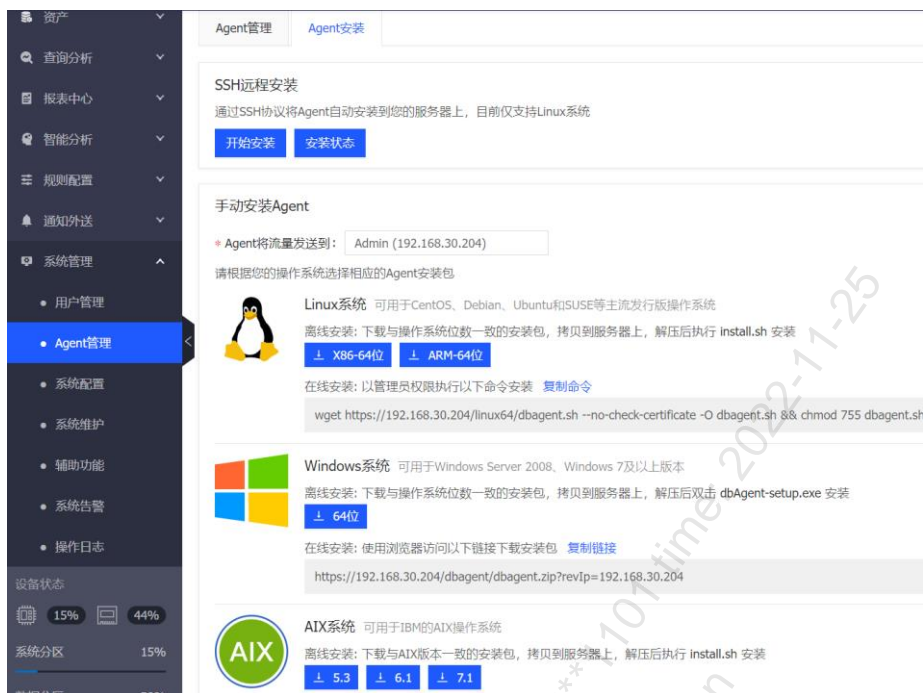


5.2 安装 Agent

如果云 DAS-DBAuditor 通过审计代理 (Agent) 采集数据库流量, 则需要在数据库服务器上安装 Agent, 本文仅以 Linux-X86 服务器举例说明。

方法一：离线安装

步骤1. 登录 DAS-DBAuditor Web 管理平台, 在菜单栏选择“系统管理>Agent 管理”进入 Agent 管理页面, 选择 Agent 安装页签, 点击<X86-64 位>下载 Linux 版 Agent 安装包。



步骤2. 安装包下载完之后，使用 Xftp 工具将 Agent 安装包上传到 Linux 服务器指定目录（如 /data/dbAuditAgent）。

```
[root@orcl11g dbAuditAgent]# ls
dbagent2.30  dbagent_linux_V2.30.tar.gz
```



- ◆ 禁止直接运行二进制文件。
- ◆ 解压目录不能出现空格。
- ◆ 每次更换运行或解压目录需重新运行安装脚本。
- ◆ Linux 环境需以 root 用户运行脚本，指定解释器 bash，或不指定解释器直接运行。

步骤3. 执行 `tar -zxvf dbAgent_V2.30.tar.gz` 命令解压 Agent 安装包。


```
[root@orc11lg dbAuditAgent]# tar -zxvf dbagent_linux_V2.30.tar.gz
dbagent2.30/
dbagent2.30/agent.ini
dbagent2.30/certificate/
dbagent2.30/certificate/client.pem
dbagent2.30/dbAgent
dbagent2.30/dbAgentHookMysql.so
dbagent2.30/dbAgentHookOracle.so
dbagent2.30/dbAgentHookPGsql.so
dbagent2.30/dbagent_start.sh
dbagent2.30/dbagent_stop.sh
dbagent2.30/dbMonitor
dbagent2.30/installHook.sh
dbagent2.30/install.sh
dbagent2.30/md5sum.txt
dbagent2.30/ReadMe
dbagent2.30/tool/
dbagent2.30/tool/agent.conf
dbagent2.30/tool/cpulimit
dbagent2.30/tool/get_io_usage.sh
dbagent2.30/tool/pcapAgent
dbagent2.30/tool/getResourceUsageInfo.sh
dbagent2.30/tool/get_network_card_name.sh
dbagent2.30/tool/getip
dbagent2.30/tool/prepare_update.sh
dbagent2.30/tool/update.sh
dbagent2.30/uninstallHook.sh
dbagent2.30/uninstall.sh
dbagent2.30/version.txt
```

步骤4. 进入安装目录，在安装目录执行“./install.sh”命令即可安装 Agent 程序。

```
cd /data/dbAuditAgent/dbagent2.30/

./install.sh
```

```
[root@orc11lg dbAuditAgent]# cd /data/dbAuditAgent/dbagent2.30/
[root@orc11lg dbagent2.30]# ./install.sh
2022年 11月 11日 星期五 10:47:08 CST
Install dbagent...
Install dbagent success
Start dbagent...
Start dbagent success
```

步骤5. 安装完成后，可以在 Agent 管理页面上查看到已经部署成功的 Agent。

<input type="checkbox"/>	Agent IP	状态	版本	操作系统	最后收包时间	转发速率	Agent的CPU、内存使用	配置信息	操作
<input type="checkbox"/>	10.50.3.110	连接正常	2.30	Linux	2022-11-11 10:47:09	0 Mbps	CPU: 3.06% 内存:0.11%	CPU亲和性:启用, CPU使用上限:100...	监控 配置 更多v

方法二：SSH 远程安装（需确保 Linux 服务器与 DAS-DBAuditor 网络互通）

步骤1. 登录 DAS-DBAuditor 系统 Web 管理平台，在菜单栏选择“系统管理>Agent 管理”进入 Agent 管理页面，选择 Agent 安装页签，点击<开始安装>。

Agent管理

Agent管理

Agent安装

通过SSH远程安装

通过SSH协议将Agent自动安装到您的服务器上，目前仅支持Linux系统

开始安装

安装状态

步骤2. 在弹出的对话框中编辑安装 Agent 服务器的 IP 和 root 账户密码，点击<安装>进行 SSH 远程安装 Agent。

通过SSH远程安装Agent

审计服务器IP:

116.62.201.14

安装Agent的服务器:

116.62.167.77

.....

22

+ 增加

说明: 不填写密码则会使用上一次的密码

安装

取消

步骤3. 安装完成后，在 Agent 管理页面可查看到部署成功的 Agent。

<input type="checkbox"/>	Agent IP	状态	版本	操作系统	最后收包时间	转发速率	Agent的CPU、内存使用	配置信息	操作
<input type="checkbox"/>	10.50.3.110	连接正常	2.30	Linux	2022-11-11 10:47:09	0 Mbps	CPU: 3.06% 内存:0.11%	CPU亲和性:启用, CPU使用上限:100...	监控 配置 更多v

方法三：在线安装（须确保 Linux 服务器与 DAS-DBAuditor 网络互通）

步骤1. 以 root 用户登录 Linux 服务器操作系统 CLI 界面，执行在线安装命令。

wget https://192.168.30.204/linux64/dbagent.sh --no-check-certificate -O dbagent.sh && chmod 755 dbagent.sh && ./dbagent.sh 192.168.30.204

```
[root@localhost agent]# wget https://10.20.49.70/linux64/dbagent.sh --no-check-certificate -O dbagent.sh && chmod 755 dbagent.sh && ./dbagent.sh 10.20.49.70
--2021-11-29 20:34:38-- https://10.20.49.70/linux64/dbagent.sh
正在连接 10.20.49.70:443... 已连接。
警告：无法验证 10.20.49.70 的由“/C=CN/ST=Zhejiang/L=Hangzhou/O=dbone/OU=dbone/CN=www.dbone.com”颁发的证书：
出现了自己签名的证书。
警告：证书通用名“www.dbone.com”与所要求的主机名“10.20.49.70”不符。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：572 [text/plain]
正在保存至：“dbagent.sh”
100%[=====] 572 ---K/s 用
2021-11-29 20:34:38 (184 MB/s) - 已保存“dbagent.sh” [572/572])
[INFO] uninstall
2021年 11月 29日 星期一 20:34:38 CST
uninstall dbagent success
```

杭州安恒信息技术有限公司

明御®数据库审计与风险控制系統 软件安装指南

27

步骤2. Agent 程序安装完成并运行之后，登录系统 Web 管理平台，在菜单栏选择“系统管理>Agent 管理”进入 Agent 管理页面，选择 Agent 管理页签，查看 Agent 连接状态信息。

<input type="checkbox"/>	Agent IP	状态	版本	操作系统	最后收包时间	转发速率	Agent的CPU、内存使用	配置信息	操作
<input type="checkbox"/>	10.50.3.110	连接正常	2.30	Linux	2022-11-11 10:47:09	0 Mbps	CPU: 3.06% 内存:0.11%	CPU亲和性:启用, CPU使用上限:100...	监控 配置 更多

5.3 分布式部署配置

对于分布式部署模式，需要进行分布式配置，操作方法如下。

步骤1. 登录管理中心的 Web 管理平台，在菜单栏选择“系统管理>系统配置”进入系统配置页面，选择网络页签，按“Shift+S”组合键弹出闪灯校对网口位置对话框，选择已配置管理 IP 的网口，设置为“Admin”，点击<保存>即可将该网口设置为管理口。

闪灯校对网口位置

网口名称	对应位置	动作
eth3	<input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT1 GE4	闪灯
eth4	<input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT1 GE5	闪灯
eth5	<input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT1 GE6	闪灯
eth6	<input type="radio"/> Admin <input checked="" type="radio"/> HA <input type="radio"/> 业务口	闪灯
eth7	<input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT1 GE8	闪灯
eth8	<input checked="" type="radio"/> Admin <input type="radio"/> HA <input type="radio"/> 业务口	闪灯
eth9	<input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT2 GE1	闪灯

保存

取消

步骤2. 新建管理中心节点。

- 在菜单栏选择“系统管理>系统配置”进入系统配置页面，选择分布式页签，点击<转成管理节点>。

系统配置

网络
SNMP
许可证
分布式
流量接收方式

节点类型说明:
管理节点: 具有配置存储、WEB管理、协议审计等全部功能
探测器节点: 仅具有协议审计的功能, 配置由管理节点下发

节点类型
设备正处于 单机运行模式, 如需部署分布式审计集群, 请点击以下按钮转换角色

转成管理节点

- 弹出**转成管理节点**对话框, 编辑节点名称, 选择节点类型 (建议选择 S25), 点击<确定>。

转成管理节点 X

* 节点名称:
建议使用部门或位置命名, 方便管理, 如: 北京总部、研发中心

* 节点类型:

确定

取消

步骤3. 添加子节点。

- 在菜单栏选择“**系统管理>系统配置**”进入**系统配置**页面, 选择**分布式**页签, 点击<添加>。有两种添加方式: 直接添加和先安装再添加。

SNMP
许可证
分布式

节点类型说明:
管理节点: 具有配置存储、WEB管理、协议审计等全部功能
探测器节点: 仅具有协议审计的功能, 配置由管理节点下发

添加

收起查询条件

节点名称:
节点IP:
节点类型:

搜索

清空

<input type="checkbox"/>	节点名称	节点IP	节点类型	节点型号	软件版本	配置版本	审计资产	操作
<input type="checkbox"/>	杭州	10.20.49.201	管理节点	S25	4.0.68.220531.2100	973	全部资产	设置审计资产 转为单机运行
<input type="checkbox"/>	北京	10.20.49.128	探测器节点	S25	4.0.68.220531.2100	973	全部资产	设置审计资产 同步配置 更多

☐ 同步配置

共 2 条 < 1 > 20 条/页 刷新

- 直接添加适用于子节点的软件版本与管理中心的软件版本一致的场景。只需要填写子节点名称、节点 IP 和节点型号。

添加分布式节点
 ☐ 添加后不关闭，继续添加节点
 ×

添加方式:
 ☒ 直接添加②
 ☐ 先安装再添加②

* 节点名称:

建议使用部门或位置命名，方便管理；如：北京总部、研发中心

* 节点IP:

* 节点型号:

- ◆ 先安装再添加适用于以下场景：子节点的软件版本与管理中心的软件版本不一致或者子节点没有安装 DAS-DBAuditor 的主机。需要填写节点名称、节点 IP、节点型号、SSH 服务端口、用户名和密码。



- ◆ 当子节点的软件版本与管理中心的软件版本不一样时，使用先安装再添加的方式，会重装子节点的 DAS-DBAuditor 系统软件。重装会导致清空子节点的业务数据和配置数据。
- ◆ 建议先手动将子节点的软件版本升级到管理中心的软件版本，再使用直接添加的方式。

添加分布式节点
 ☐ 添加后不关闭，继续添加节点
 ×

添加方式:
 ☐ 直接添加②
 ☒ 先安装再添加②

* 节点名称:

建议使用部门或位置命名，方便管理；如：北京总部、研发中心

* 节点IP:

* 节点型号:

* SSH服务端口:

安装需要通过SSH访问节点，请填写SSH服务端口

* 用户名:

建议使用root账号

* 密码:

详细配置请参见下表。

配置项	说明
节点名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
节点 IP	节点主机的 IP，支持 IPv4 和 IPv6。
节点型号	建议设置为与管理中心一致即可。
SSH 服务端口	设置 SSH 服务所用的端口，默认为 22。
用户名	节点主机的用户名，建议设置为 root。
密码	节点主机的密码。

- 2) 点击<确定>，节点软件版本显示如果为“暂不可用”。等待一段时间后刷新页面，节点软件版本显示为与管理中心相同的版本号。同时页面上边栏的<同步配置>亮起。

系统配置

SNMP
许可证
分布式

节点类型说明:
管理节点: 具有配置存储、WEB管理、协议审计等全部功能
探测器节点: 仅具有协议审计的功能, 配置由管理节点下发

添加
节点名称
请输入查询关键字

节点名称	节点IP	节点类型	节点型号	软件版本	配置版本	审计资产	操作
杭州	10.20.49.201	管理节点	S25	4.0.68.220531.2100	977	全部资产	设置审计资产 转为单机运行
北京	10.20.49.128	探测器节点	S25	暂不可用	暂不可用	全部资产	设置审计资产 同步配置 更多

同步配置
软件升级
删除

共 2 条 < 1 > 20 条/页 跳至 页

- 3) 页面上边栏的<同步配置>亮起，并且发现新添加的节点的配置版本与管理中心不一致。

系统配置

SNMP
许可证
分布式

节点类型说明:
管理节点: 具有配置存储、WEB管理、协议审计等全部功能
探测器节点: 仅具有协议审计的功能, 配置由管理节点下发

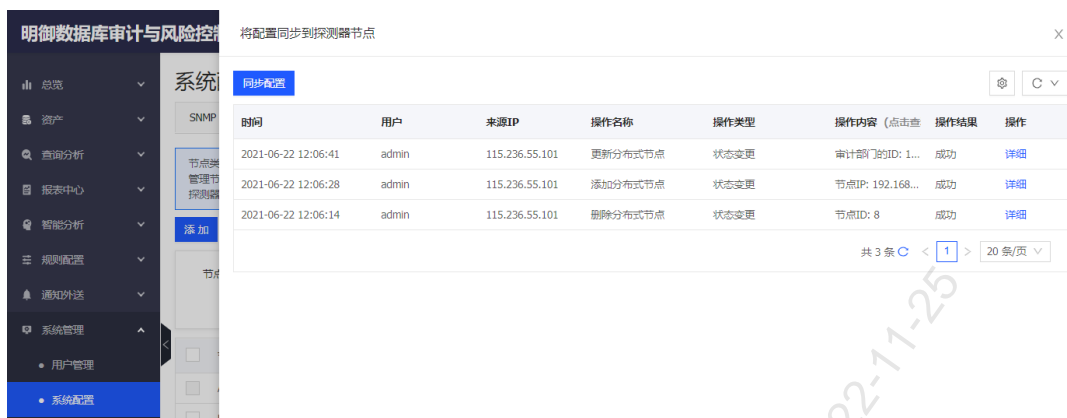
添加
节点名称
请输入查询关键字

节点名称	节点IP	节点类型	节点型号	软件版本	配置版本	审计资产	操作
杭州	10.20.49.201	管理节点	S25	4.0.68.220531.2100	977	全部资产	设置审计资产 转为单机运行
北京	10.20.49.128	探测器节点	S25	暂不可用	暂不可用	全部资产	设置审计资产 同步配置 更多

同步配置
软件升级
删除

共 2 条 < 1 > 20 条/页 跳至 页

- 4) 点击页面上边栏的<同步配置>，页面弹窗显示需要进行同步配置，点击弹窗中的<同步配置>，下发管理中心的全部配置，使节点与管理中心配置保持一致。



5) 同步配置后，节点的配置版本号与管理中心的配置版本号一致。



分布式部署配置完成后，在菜单栏选择“总览>节点信息”进入节点信息页面，可查看全部节点的当前状态。

