阿里云
云安全中心（态势感知）

接入云安全中心

文档版本：20190919

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 Agent说明

工作原理

云安全中心Agent每隔五个小时会主动向云安全中心服务器端上报一次在线数据信息。

如果云安全中心Agent没有按时上报在线信息，云安全中心服务器端则在12小时后判定该服务器不在线，并在云安全中心控制台中将对应服务器的保护状态变更为未受保护。

相关进程

云安全中心Agent包含以下两个主要进程：

说明:
云安全中心Agent的进程在Linux系统的服务器上以root账号运行，在Windows系统的服务器上以system账号运行。

- AliYunDun

  此进程用于与云安全中心服务器建立连接。

  进程文件所在路径如下：

  - Windows 32位系统：`C:\Program Files\Alibaba\aegis\aegis_client`
  - Windows 64位系统：`C:\Program Files (x86)\Alibaba\aegis\aegis_client`
  - Linux系统：`/usr/local/aegis/aegis_client`

- AliYunDunUpdate

  此进程用于定期检测云安全中心Agent是否需要升级。

  进程文件所在路径如下：

  - Windows 32 位系统：`C:\Program Files\Alibaba\aegis\aegis_update`
  - Windows 64 位系统：`C:\Program Files (x86)\Alibaba\aegis\aegis_update`
  - Linux系统：`/usr/local/aegis/aegis_update`

2 安装Agent

云安全中心Agent是云安全中心提供的本地插件，您必须在服务器操作系统上安装云安全中心Agent插件才能使用云安全中心提供的安全防护服务。

背景信息

未安装Agent插件的服务器将不受云安全中心保护，控制台页面也不会显示该资产的任何漏洞、告警、基线漏洞和资产指纹等数据。

如何查看哪些资产需要安装Agent插件?

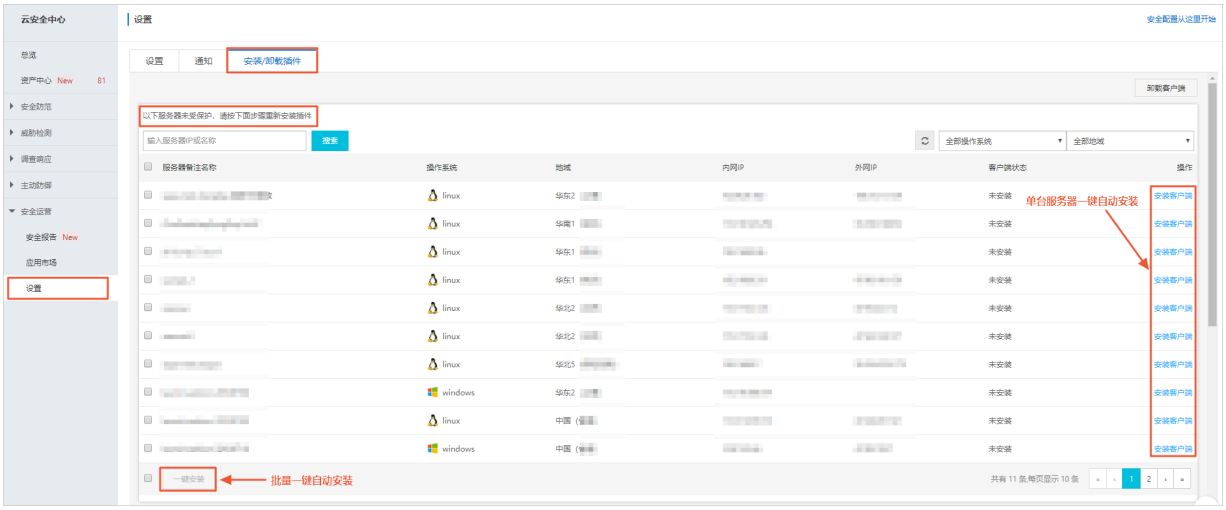
每台资产都需安装Agent插件，您可以在云安全中心控制台总览页面资产保护模块，查看未安装Agent插件（即未防护服务器）的服务器数量。单击安装Agent跳转到设置 > 安装/卸载插件页面。

说明:

您也可以在资产中心页面确认服务器Agent安装状态。

- 保护状态为开启：表示Agent已安装且处于正常运行状态。
- 保护状态为关闭：表示Agent未安装或处于离线状态。

安装/卸载插件页面会展示出您所有未安装Agent插件（包含已关机的服务器）的服务器列表。您可在该页面对未安装Agent的服务器执行一键自动安装或手动下载、执行命令安装。一键安装功能无需您单独下载插件。



该页面下方还会展示出对于不支持一键安装功能的服务器，您需手动安装Agent插件的操作指引。

注意事项

非阿里云服务器必须通过安装程序（Windows）或脚本命令（Linux）安装云安全中心Agent。

如果您的非阿里云服务器通过以下方式安装了Agent，则您需要删除云安全中心Agent目录后，按照下述手动安装步骤重新安装Agent。

- 通过已安装云安全中心Agent的镜像批量安装服务器。
- 从已安装云安全中心Agent的服务器上，直接复制云安全中心Agent文件。

云安全中心Agent文件目录

- Windows：`C:\Program Files (x86)\Alibaba\Aegis`
- Linux：`/usr/local/aegis`

一键自动安装Agent

执行一键安装前，需确定您的服务器已满足以下条件：

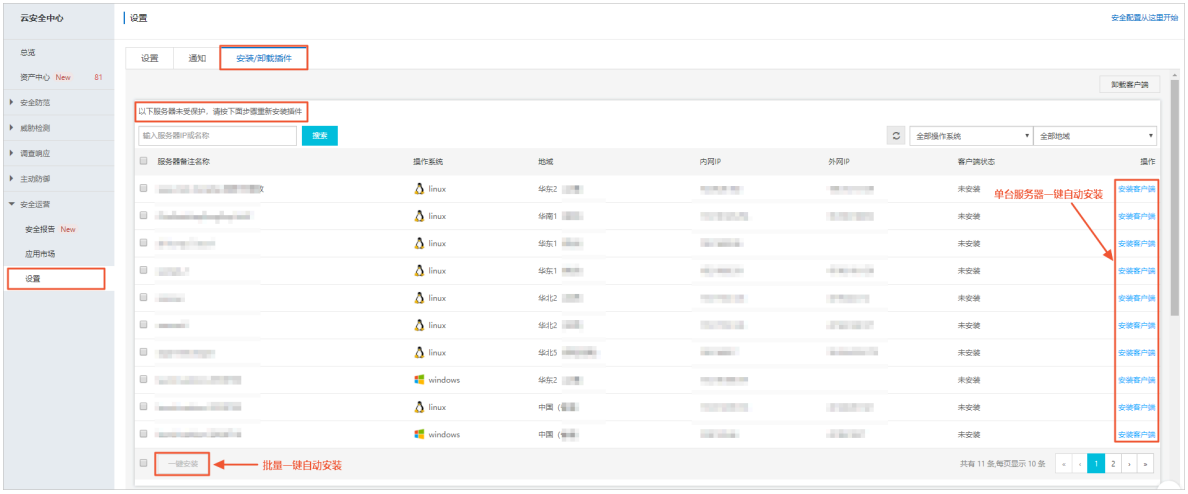
- 服务器为阿里云服务器，非阿里云服务器需进行手动安装
- ECS在支持一键安装功能支持的地域内
- 服务器已在运行中
- 网络已正常连接
- 该服务器已安装云助手

> 说明:
> 云助手安装相关内容参见文档云助手。

- 如果您已在服务器上安装了安全软件（如安全狗、云锁等），可能会导致Agent插件无法正常安装。建议您在安装Agent插件前确认您的服务器上是否存在这类安全软件。如果存在，建议您先关闭或卸载该安全软件之后再安装Agent插件。

操作步骤

1. 登录云安全中心管理控制台。
2. 单击安全运营 > 设置 > 安装/卸载插件。
3. 单击操作栏的安装客户端，勾选单个服务器安装Agent，或单击左下角一键安装对多台服务器执行批量安装Agent。



Agent插件安装完成约五分钟后，您即可在资产中心中查看您服务器的在线情况：阿里云服务器将会从关闭变成开启。

> 说明:
> 一键安装后如果客户端状态显示为安装失败并提示未安装云助手，请先安装云助手。云助手安装相关内容参见文档云助手。

手动安装Agent

以下情况不支持一键自动安装、必须执行手动安装Agent：

- 您的服务器为非阿里云服务器
- 网络类型为经典网络
- ECS不在支持的区域内
- 服务器操作系统为Windows 2019、Windows 2016、Windows 2012、Windows 2008、Windows 2003
- 未安装云助手
- 通过专线连接、内网通信的非阿里云服务器，需要修改服务器的DNS配置，指定以下任意一个云安全中心服务端DNS解析地址：

```
106.11.248.209/106.11.248.51 jsrv.aegis.aliyun.com
```

```
106.11.248.90/106.11.250.224 update.aegis.aliyun.com
```

说明:

手动安装Agent前，请确认该服务器已正常运行，并且网络已连通。

操作步骤

1. 登录云安全中心控制台。
2. 单击安全运营 > 设置 > 安装/卸载插件。

3. 根据您的服务器操作系统选择安装步骤，获取最新版本Agent插件。

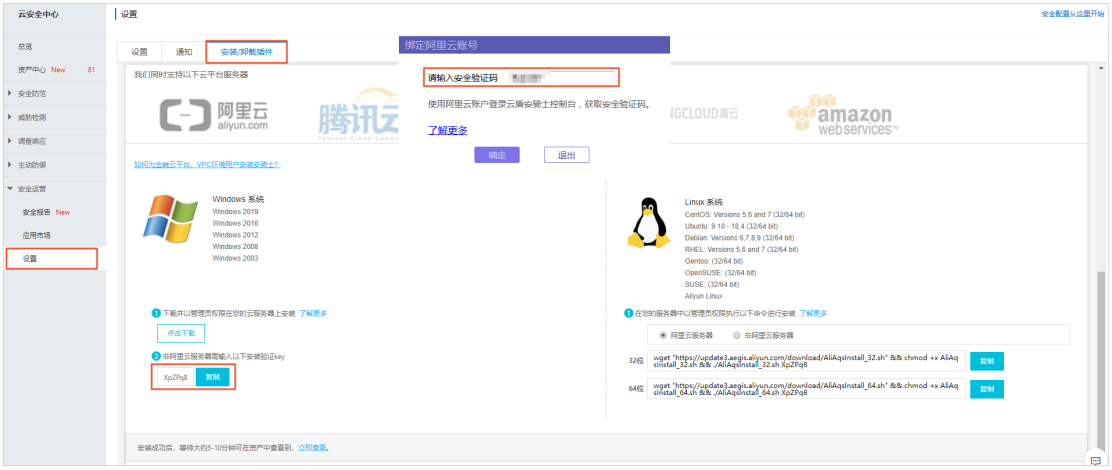
- Windows系统

  a. 在安装Agent页面，单击点击下载下载最新版本Agent安装文件到本地计算机。

  b. 将安装文件上传至您的Windows服务器，例如通过FTP工具将安装文件上传到服务器。

  c. 在您的Windows服务器上以管理员权限运行Agent插件安装程序。

  d. 非阿里云服务器输入安装验证Key关联您的阿里云账号。您可在Agent安装页面找到您的安装验证Key。



说明:

每个安装验证KEY有效期为1小时，超过该时间将无法正确安装Agent插件。安装插件前请及时刷新安装验证KEY。

- Linux 系统

  a. 根据您的实际情况，在安装Agent页面选择阿里云服务器或非阿里云服务器。

  b. 以管理员身份登录您的Linux服务器。

  c. 根据您的服务器，选择32位或64位的安装命令并复制至您的Linux服务器上。

  d. 执行安装命令即可完成Agent插件的下载及安装。

  说明:
  该安装命令包含从阿里云站点下载最新的Agent插件，如您使用的是非阿里云服务器请确认您的服务器已连接公网。

Agent插件安装完成约五分钟后，您即可在云安全中心管理控制台中查看您服务器的在线情况：

- 阿里云服务器会从关闭变成开启。
- 非阿里云服务器将会被添加至您的服务器列表中。

说明:
请不要对无需保护的机器（例如：线下测试机器、您自己的工作电脑等）安装Agent。

后续步骤

安装Agent后，建议您参照以下步骤进行验证Agent是否已成功安装：

1. 检查您服务器上云安全中心Agent的*AliYunDun*和*AliYunDunUpdate*进程是否正常运行。关于云安全中心Agent进程说明，请参考Agent说明。
2. 在您的服务器上执行以下telnet命令，检查您的服务器是否能正常连通云安全中心服务器：

   说明:
   确保您的服务器能够连通至少一个jsrv和一个update服务域名。

   - `telnet jsrv.aegis.aliyun.com 80`
   - `telnet jsrv2.aegis.aliyun.com 80`
   - `telnet jsrv3.aegis.aliyun.com 80`
   - `telnet update.aegis.aliyun.com 80`
   - `telnet update2.aegis.aliyun.com 80`
   - `telnet update3.aegis.aliyun.com 80`

如果云安全中心Agent安装验证失败，请参考Agent离线排查。

一键安装功能支持的地域

支持的地域	地域名称
亚太	华东 1（杭州）
	华东 2（上海）
	华东 2 金融云
	华北 1（青岛）
	华北 2（北京）
	华北 3（张家口）
	华北 5（呼和浩特）
	华南 1（深圳）
	香港
	新加坡
	澳大利亚（悉尼）
	马来西亚（吉隆坡）
	印度尼西亚（雅加达）
	日本（东京）
欧洲与美洲	德国（法兰克福）
	英国（伦敦）
	美国（硅谷）
	美国（弗吉尼亚）
中东与印度	印度（孟买）
	阿联酋（迪拜）

相关文档

#unique_10/unique_10_Connect_42_section_ymh_u9c_vbp

3 金融云和VPC用户安装Agent

针对无法直接连通公网的云服务器（如：阿里金融云上的服务器或使用专有网络VPC的云服务器），您可以参照本文介绍的方法为其安装云安全中心Agent。

操作步骤

参照以下步骤，为金融云或VPC环境下的服务器安装云安全中心Agent：

> **说明：**
> 如果您的服务器上安装了安全软件（如安全狗、云锁等），则云安全中心Agent可能无法正常安装。在安装云安全中心Agent前，请确认您的服务器上是否存在这类安全软件。如果存在，建议您关闭或卸载该安全软件后，再安装云安全中心Agent。

1. 登录云安全中心控制台。
2. 单击安全运营 > 设置 > 安装/卸载插件。

3. 根据服务器操作系统类型，选择安装步骤，获取并安装最新版本的云安全中心Agent。
   - Windows 系统
     a. 在安装/卸载插件页面，单击点击下载，下载最新版本云安全中心Agent安装文件到本地计算机。
     b. 将安装文件上传到Windows服务器。例如，通过FTP工具将安装文件上传到服务器。
     c. 在Windows服务器上，以管理员权限运行云安全中心Agent安装程序，按照向导完成安装。

     > **说明：**

云安全中心Agent安装过程中可能会提示您输入安装验证Key。该安装验证Key用于关联您的阿里云账号，您可在安装/卸载插件页面找到您的安装验证 Key。

- Linux系统

a. 根据服务器的Linux系统版本，单击以下链接将云安全中心Agent安装程序下载至本地计算机。

- Linux 32位系统：云安全中心Agent安装程序
- Linux 64位系统：云安全中心Agent安装程序

b. 将云安全中心Agent安装程序上传至Linux服务器。例如，通过FTP工具将安装文件上传到服务器。

c. 以管理员身份登录Linux服务器。

d. 定位到已上传的云安全中心Agent安装程序所在目录，根据服务器的Linux系统版本，执行以下命令安装云安全中心Agent。

- Linux 32位系统：`chmod +x AliAqsInstall_32.sh && ./AliAqsInstall_32.sh xxxxxx`
- Linux 64位系统：`chmod +x AliAqsInstall_64.sh && ./AliAqsInstall_64.sh xxxxxx`

说明：

此安装命令末尾处的`xxxxxx`为安装验证Key，执行安装命令时请使用安装/卸载插件页面中显示的六位安装验证Key替换`xxxxxx`部分。该安装验证Key与Windows系统安装步骤中的安装验证Key一致，用于关联您的阿里云账号。

4. 云安全中心Agent安装完成约五分钟后，您可在云盾云安全中心控制台资产管理页面查看服务器的保护状态。服务器保护状态将从未受保护变为保护中。

验证Agent安装

成功安装云安全中心Agent后，建议您参考以下步骤进行验证：

1. 检查服务器上云安全中心Agent的*AliYunDun*和*AliYunDunUpdate*进程是否正常运行。关于云安全中心Agent进程的说明，请参考Agent说明。

2. 在服务器上执行以下telnet命令，检查服务器是否能正常连通态云安全中心服务器。

> **说明:**
> 确保以下两个服务器都能连通。
>
> - `telnet jsrv3.aegis.aliyun.com 80`
> - `telnet update3.aegis.aliyun.com 80`

如果云安全中心Agent安装验证失败，请参考Agent离线排查。

4 卸载Agent

如果您决定不再使用云盾云安全中心服务的安全防护功能，您可以选择自动或手动卸载云安全中心Agent。卸载云安全中心Agent后，请耐心等待六个小时，然后该服务器在云安全中心控制台上的保护状态就会由保护中变更为未受保护。

背景信息

卸载云安全中心Agent前您需了解以下信息：

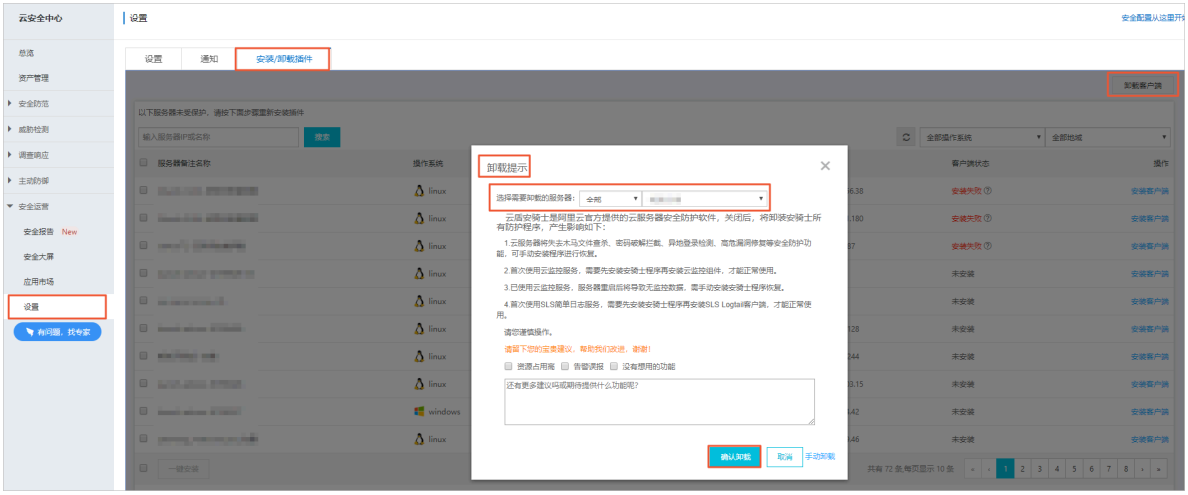
- 卸载Agent后再次安装Agent时，历史的告警数据、隔离文件无法关联您的资产，请谨慎卸载。
- Agent卸载后，控制台中该主机资产的保护状态将变更为离线状态，您可以使用解绑功能删除处于离线状态的主机资产的记录。
- 通过本文档步骤来卸载指定主机Agent，请务必确保当前机器云安全中心处于在线状态，否则无法接收到卸载指令。如果卸载后重新安装云安全中心Agent，请手工进行安装，忽略期间的报错，重复操作3次以上（Agent卸载会有一段保护期24小时或重复执行3次以上安装命令）。

控制台卸载Agent

您可以参考以下步骤从云安全中心控制台卸载Agent插件。

1. 登录云安全中心控制台 。
2. 单击安全运营 > 设置 > 安装/卸载插件。
3. 单击页面右上角的卸载客户端按钮。
4. 在弹出的卸载提示对话框中，选择您决定卸载Agent 的服务器，并单击确认卸载。

   系统将自动卸载您选择的服务器上的云安全中心Agent。



手动卸载Agent操作步骤

请提交工单获取Agent手动卸载的命令和方法。

5 Agent离线排查

如果您已按照#unique_14为服务器成功安装云安全中心Agent，但在云安全中心控制台上仍看到该服务器的保护状态为未受保护，则说明Agent处于离线状态，请参照本文进行排查。

背景信息

如果您的云安全中心Agent处于离线状态，请按照以下步骤进行排查：

操作步骤

1. 登录您的服务器，查看云安全中心Agent相关进程（`AliYunDun`和`AliYunDunUpdate`）是否正常运行。

   如果云安全中心Agent相关进程无法运行，建议您重启服务器，或者参考安装Agent重新安装云安全中心Agent。

   - Windows系统

     在任务管理器中，查看相关进程是否正常运行。

   - Linux系统

     执行`top`命令，查看相关进程是否正常运行。

2. 对于首次安装云安全中心Agent的服务器，如果在安装Agent后，保护状态仍然为未受保护，请参考以下方法，重新启动云安全中心Agent：

   - Linux 系统：执行`killall AliYunDun && killall AliYunDunUpdate && /usr/local/aegis/aegis_client/aegis_10_xx/AliYunDun`命令。

     > 说明：
     > 您必须将命令中的`xx`替换为该目录下的最大的数字。

   - Windows 系统：在服务项中重新启动以下两个服务项，选中对应服务，右键选择重新启动即可。

3. 检查您的服务器网络连接是否正常。
   - 服务器有公网IP（如经典网络、EIP、云外机器）
     - Windows 系统：在命令行中执行`ping jsrv.aegis.aliyun.com -l 1000`命令。
     - Linux 系统：执行`ping jsrv.aegis.aliyun.com -s 1000`命令。
   - 服务器无公网IP（如金融云、VPC专有网络）
     - Windows 系统：在命令行中执行`ping jsrv3.aegis.aliyun.com -l 1000`命令。
     - Linux 系统：执行`ping jsrv3.aegis.aliyun.com -s 1000`命令。
4. 如果解析不通，请使用以下方法，检查您的服务器网络连接状况：
   a. 确认您的服务器的DNS服务正常运行。如果DNS服务无法运行，重启您的服务器，或者检查服务器DNS服务是否有故障。
   b. 检查服务器是否设置了防火墙ACL规则或阿里云安全组规则。如果有，请确认已将云安全中心的服务端IP加入防火墙白名单（出、入方向均需添加）以允许网络访问。

   说明:
   请将下列IP段的80端口添加至白名单，最后一个IP段需要同时添加80和443端口至白名单。
   - 140.205.140.0/24 80
   - 106.11.68.0/24 80
   - 110.173.196.0/24 80
   - 106.11.68.0/24 80

- 100.100.25.0/24 80 443

c. 检查您的服务器公网带宽是否为零。如果您的服务器公网带宽为零，请参考以下步骤进行处理：

A. 在您服务器的hosts文件添加以下域名解析记录：

- 国内经典网络：`100.100.110.61 jsrv.aegis.aliyun.com`、`100.100.45.131 jsrv.aegis.aliyun.com`、`100.100.110.62 update.aegis.aliyun.com`和`100.100.45.29 update.aegis.aliyun.com`
- 国外经典网络：`100.100.103.52 jsrv.aegis.aliyun.com`、`100.100.30.54 jsrv.aegis.aliyun.com`、`100.100.30.55 update.aegis.aliyun.com`和`100.100.103.54 update.aegis.aliyun.com`

B. 修改hosts文件后，执行`ping jsrv.aegis.aliyun.com`命令。

说明：

如果返回的结果不是`100.100.25.3`，请您重启服务器或检查服务器DNS服务是否有故障。

C. 如果仍然无法解析到正确的IP，您可以尝试修改云安全中心Agent安装目录下*conf*目录中的`network_config`配置文件，将`t_srv_domain`、`h_srv_domain`对应的值分别修改为`100.100.25.3`及`100.100.25.4`。修改完成后，重启云安全中心Agent进程。

说明：

修改前请务必备份`network_config`配置文件。

此方法只适用于公网带宽为零，且保护状态为未受保护的服务器。

d. 如果Ping命令执行解析成功，再次尝试通过Telnet命令连接解析出的域名IP的80端口（例如，执行`telnet 140.205.140.205 80`命令），查看是否连通。如果无法连通，请确认防火墙是否存在相关限制。

5. 检查您的服务器CPU、内存是否长期维持较高占用率（如 95%、100%），此情况可能导致云安全中心Agent进程无法正常工作。
6. 检查服务器是否已安装第三方的防病毒产品（如安全狗、云锁等）。部分第三方防病毒软件可能会禁止云安全中心Agent插件访问网络。

   如果有，请暂时关闭该产品，并重新安装云安全中心Agent。