SIEMENS

SIMATIC

SoftwareCIM

操作说明

01/2024

法律资讯

警告提示系统

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

⚠危险
表示如果不采取相应的小心措施，**将会**导致死亡或者严重的人身伤害。

⚠警告
表示如果不采取相应的小心措施，**可能**导致死亡或者严重的人身伤害。

⚠小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意
表示如果不采取相应的小心措施，可能导致财产损失。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。

合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。 由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

按规定使用 Siemens 产品

请注意下列说明：

⚠警告
Siemens 产品只允许用于目录和相关技术文件中规定的使用情况。如果要使用其他公司的产品和组件，必须得到 Siemens 推荐和允许。正确的运输、储存、组装、装配、安装、调试、操作和维护是产品安全、正常运行的前提。必须保证允许的环境条件。必须注意相关文件中的提示。

商标

所有带有标记符号 ® 的都是 Siemens Aktiengesellschaft 的注册商标。本印刷品中的其他符号可能是一些其他商标。若第三方出于自身目的使用这些商标，将侵害其所有者的权利。

责任免除

我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
德国

目录

安全 1

1.1 网络安全信息

西门子的产品及解决方案中包含工业网络安全功能，可确保工厂、系统、机器和网络的安全运行。

为了保护工厂、系统、机器和网络防止受到网络攻击，需要实施并持续维护先进的全方位工业网络安全保护措施。Siemens 的产品和解决方案构成此类概念的其中一个要素。

客户负责防止其工厂、系统、机器和网络受到未经授权的访问。只有在有必要连接时并仅在采取适当安全措施（例如，防火墙和/或网络分段）的情况下，才能将该等系统、机器和组件连接到企业网络或 Internet。

有关实施保护性工业网络安全措施的更多信息，请访问此处 (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html)。

Siemens 不断对产品和解决方案进行开发和完善以提高安全性。Siemens 强烈建议您及时更新产品并始终使用最新产品版本。如果使用的产品版本不再受支持，或者未能应用最新的更新程序，客户遭受网络攻击的风险会增加。

要随时了解有关产品更新的信息，请订阅 Siemens Industrial Cybersecurity RSS Feed：网址 (https://new.siemens.com/global/en/products/services/cert.html)。

1.2 数据保护

西门子遵守数据保护准则，尤其是有关数据最小化（通过设计保护隐私）的要求。对于该产品，这表示：本产品不会处理/保存任何个人信息，仅处理或保存技术功能数据（如时间戳）。如果用户将此数据链接到其它数据（例如轮班计划），或者如果用户将个人信息保存在同一介质（例如硬盘）并因此在处理过程中创建人称指称，则用户必须确保符合数据保护准则。

1.3 安全说明

说明

有关保护管理员帐户的说明

具有管理员权限的用户具有大量的系统访问和操作权限。
因此，请确保采取充分的防护措施来保护管理员帐户，以防止未经授权的更改。为此，请使用安全密码和标准用户帐户进行正常操作。应根据需要采取其它措施，例如使用安全策略。

说明

为防止 SoftwareCIM 在用户 PC 遭遇网络恶意攻击时被意外篡改，西门子强烈建议在 PC 上安装白名单工具。使用此工具管理 PC 上安装的软件。

请遵循以下安全建议，防止未经授权的系统访问。

密码

- 定期更新密码，提高系统安全性
- 仅使用强密码
- 妥善保管所有密码，防止未经授权的人员访问
- 针对各个用户和系统使用独立的密码

协议

- 仅启用系统所需的协议

简介

2

2.1 功能

SoftwareCIM 具有强大的网络连接能力，可以提供更好的网络连接解决方案。

基本功能

SoftwareCIM 支持以下功能：

- 通用数据模型 (UDM)

  UDM 可以作为 SoftwareCIM 的数据中心，借助支持的协议进行数据通信。

- 安全全球局域网 (SGLAN)

  同一 SGLAN 中的设备可以互相通信。

- SoftwareCIM 配置

  可以使用以下配置：

  - 配置 SoftwareCIM 的 LAN、WAN 或 SGLAN
  - 配置变量和数据绑定
  - 修改和监视变量
  - 配置支持的协议
  - 配置安全功能，例如证书管理
  - 维护功能，例如系统重启或恢复出厂设置

- 协议网关

  SGLAN 中的所有设备都可以通过 S7/Modbus 协议与基于通用数据模型 (UDM) 的 SoftwareCIM 通信。

  应用程序可以通过 RESTful API 访问基于 UDM 的 SoftwareCIM 上的数据。

- 数据管理

  触发所配置的事件时，SoftwareCIM 将执行相应操作。例如，UDM 更改。

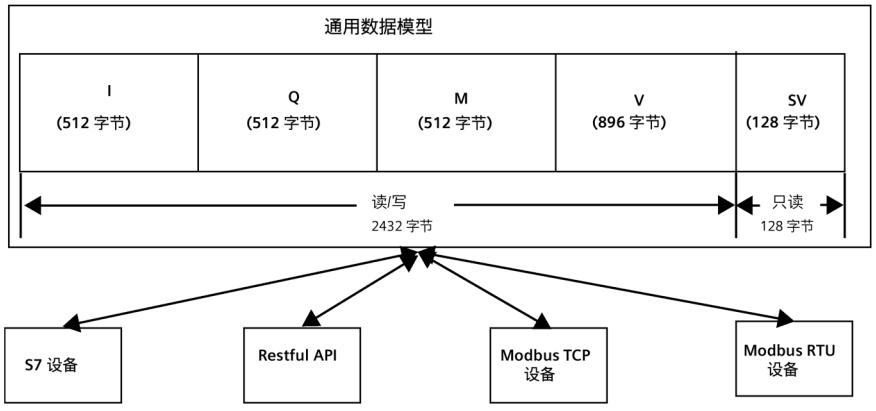
- 时间服务器
  - SoftwareCIM 可以作为 NTP 服务器向 NTP 客户端提供时间。
  - SoftwareCIM 可以启用/禁用 UDM 的时间映射。不支持 NTP 的 SGLAN 客户端可以通过多协议或 RESTful API 获取时间。
- 证书管理
  - 自带证书：生成并选择用于设置安全 Web 服务器和 SGLAN 服务器的证书；SoftwareCIM 还支持上传自定义的可信证书来构建用户的安全策略。
  - 受信任的证书：选择用于设置 SGLAN 客户端的证书。

2.2 通用数据模型

通过"通用数据模型 (UDM)"，通信协议各不相同的兼容 PLC 设备可以将过程数据映射到 UDM 中。UDM 作为 SoftwareCIM 的数据中心，支持多种通信协议。

说明

UDM 使用 Little Endian 存储多字节型数据。



I、Q、M、V 构建了一个数据模型，在 PLC 中仿真过程映像。

UDM 地址的命名规则：地址类型 + 短数据类型 + 起始地址。无需字节对齐。如，VW3 表示该字由区域 V 中的字节 3 和字节 4 组成。

UDM 地址不区分大小写。

数据类型（短数据类型）	**长度**	**值范围**	I（512 字节）	Q（512 字节）	M（512 字节）	V（W：896 字节 R：1024 字节）	
布尔型 (x)	1 位	0 ~ 1	0.0-511.7	0.0-511.7	0.0-511.7	0.0-895.7	0.0-1023.7
字节 (b)	8 位	0 ~ FF	0-511	0-511	0-511	0-895	0-1023
字 (w)	16 位	0 ~ FFFF	0-510	0-510	0-510	0-894	0-1022
双字 (dw)	32 位	0 ~ FFFFFFFF	0-508	0-508	0-508	0-892	0-1020
长字 (lw)	64 位	0 ~ FFFFFFFFFFFFFFFF	0-504	0-504	0-504	0-888	0-1016
短整型 (si)	8 位	-128 ~127	0-511	0-511	0-511	0-895	0-1023
整型 (i)	16 位	-32768 ~ 32767	0-510	0-510	0-510	0-894	0-1022
双整型 (di)	32 位	-2147483648 ~ 2147483647	0-508	0-508	0-508	0-892	0-1020
长整型 (li)	64 位	-9223372036854775808 至 9223372036854775807	0-504	0-504	0-504	0-888	0-1016
实数 (r)	32 位	-3.4E38 ~ +3.4E38	0-508	0-508	0-508	0-892	0-1020
长实数 (lr)	64 位	-1.797E308 ~ +1.797E308	0-504	0-504	0-504	0-888	0-1016
无符号短整型 (su)	8 位	0 ~ 255	0-511	0-511	0-511	0-895	0-1023
无符号 (u)	16 位	0 ~ 65535	0-510	0-510	0-510	0-894	0-1022
无符号双精度 (du)	32 位	0 ~ 4294967295	0-508	0-508	0-508	0-892	0-1020
无符号长整型 (lu)	64 位	0 ~ 18446744073709551615	0-504	0-504	0-504	0-888	0-1016

系统变量

SV（系统变量）用于保存系统数据，如时间信息等。

条目	类型	大小	地址	范围	单位	备注	Restful 接口样例
时间							
有效标志	布尔型	1 位	896.0	0 或 1		时间值的有效标志	/pi/rest/vx896.0
UNIX 时间戳	无符号双精度	4 个字节	897	0 至 4294967295	秒	当前时间，从 1970-1-1 00:00:00 开始计数的秒数 单位：秒	/pi/rest/vdu897
年	无符号	2 个字节	901	1970 至 2106	年	当前数据，年份	/pi/rest/vu901
月	无符号短整型	1 个字节	903	1 至 12	月	当前数据，月	/pi/rest/vsu903
日	无符号短整型	1 个字节	904	1 至 31	日	当前数据，月 日	/pi/rest/vsu904
小时	无符号短整型	1 个字节	905	0 至 23	小时	当前时间，小时	/pi/rest/vsu905
分钟	无符号短整型	1 个字节	906	0 至 59	分钟	当前时间，分钟	/pi/rest/vsu906
秒	无符号短整型	1 个字节	907	0 至 59	秒	当前时间，秒	/pi/rest/vsu907

2.3 SGLAN

SGLAN（安全全球局域网）可通过 SoftwareCIM 创建私有网络。SGLAN 是私有网络的基本构成模块。SGLAN 网络中的设备可相互安全通信。

SGLAN 中的角色

SGLAN 中有两种角色：

- **SGLAN 服务器**：SGLAN 服务器是数据交换中心。SGLAN 服务器负责传输数据、授权连接请求、处理登录和注销请求。

  说明

  只有 CIM 设备或 SoftwareCIM 可用作 SGLAN 服务器。将 SoftwareCIM 部署到 AWS 或 Alibaba 云后，作为 SGLAN 服务器的 SoftwareCIM 最多可连接 500 个 SGLAN 客户端。

- **SGLAN 客户端**：SGLAN 中的所有设备，包括 SGLAN 客户端以及 SGLAN 客户端所在 LAN 中的其它设备可以相互通信。SGLAN 客户端可以是 CIM 设备或 SoftwareCIM。

有关 SGLAN 的配置方法，请参见“SGLAN 设置 (页 36)”。

2.4 兼容性

支持以下操作系统：

- Windows 10（64 位）（21H2、22H2）
- Windows 11 (22H2)

安装 SoftwareCIM

3

3.1 在本地 PC 上安装 SoftwareCIM

要在本地 PC 上安装 SoftwareCIM，请按以下步骤操作：

1. 双击安装程序“SoftwareCIMInstaller.exe”。
2. 查看许可条款并单击“接受”(Accept) 继续。
3. 选择“安装到这台 PC”(Install to This PC) 并单击“下一步”(Next)。

4. 选择安装路径并单击“下一步”(Next)。
5. 上传证书文件和私钥文件。单击“安装”(Install)。此外，也可单击“跳过”(Skip)，使用默认的西门子证书。
6. 安装完成。

3.2 将 SoftwareCIM 部署到云

成功部署到云后，系统将 SoftwareCIM 默认配置为 SGLAN 服务器。SGLAN 服务器最多可以连接 500 个 SGLAN 客户端。如果要将部署后的 SoftwareCIM 配置为 SGLAN 客户端，则可更改 SoftwareCIM 配置页面上的设置。

以下云支持部署 SoftwareCIM：

- 部署到 AWS (页 13)
- 部署到 Alibaba (页 21)

菜单简介

单击 图标，打开导航菜单。导航菜单中包括"起始页面"入口、"云登录页面"入口、安装程序版本信息、帮助文档和 OSS 自述文件。

单击 图标，打开显示语言菜单。

3.2.1 部署到 AWS

要求

AWS 云帐户必须满足以下最低权限要求：

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
           "Sid":"Statement1",
           "Effect":"Allow",
           "Action": [
              "ec2:DescribeInstanceTypes",
              "ec2:DescribeInstanceTypeOfferings",
              "ec2:DescribeRegions",
              "pricing:GetProducts",
               "ec2:DescribeVpcs",
              "ec2:CreateDefaultVpc",
              "ec2:DescribeSubnets",
              "ec2:CreateDefaultSubnet",
              "ec2:CreateSecurityGroup",
              "ec2:AuthorizeSecurityGroupIngress",
               "ec2:RunInstances",
              "ec2:DescribeInstanceStatus",
              "ec2:AllocateAddress",
              "ec2:AssociateAddress",
              "ec2:DescribeInstances",
              "ec2:DescribeSecurityGroups",
              "ec2:DescribeSecurityGroupRules",
              "ec2:RevokeSecurityGroupIngress",
              "ec2:DescribeAddresses",
               "ec2:DescribeImages",
    "ec2:DescribeAvailabilityZones",
               "ec2:CreateTags",
               "ec2:DescribeTags"
           ],
           "Resource": [
               "*"
           ]
       }
   ]
}
```

有关 AWS 云帐户权限的详细信息，请参见“这里 (https://docs.aws.amazon.com/zh_cn/AWSEC2/latest/UserGuide/dlm-access-control.html)”。

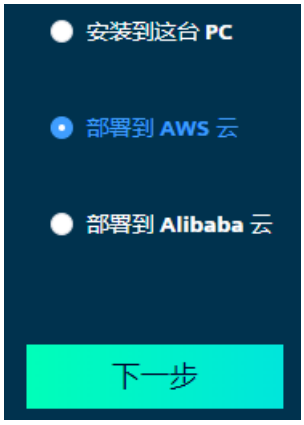
要更改 AWS 云帐户的权限，请参见“这里 (https://docs.aws.amazon.com/zh_cn/IAM/latest/UserGuide/id_users_change-permissions.html)”。

要创建 AWS 帐户，请参见“这里 (https://docs.aws.amazon.com/zh_cn/organizations/latest/userguide/orgs_manage_accounts_create.html)”。

操作步骤

要将 SoftwareCIM 部署到 AWS 云，请执行以下步骤：

1. 双击安装程序“SoftwareCIMInstaller.exe”。
2. 查看许可条款，然后单击“接受”(Accept)。如果单击“取消”(Cancel)，程序将退出。
3. 选择“部署到 AWS 云”(Deploy to AWS Cloud)，然后单击“下一步”(Next)。



4. 登录云。
   - 输入“访问密钥 ID”(Access Key ID)。
   - 输入“秘密访问密钥”(Secret Access Key)。
   - 如果使用 AWS 临时凭据帐户 (TVM) 登录，请输入“会话令牌”(Session Token)。

单击"下一步"(Next) 按钮以继续。

5. 选择实例的"区域"(Region)。
   - 如果选择"创建新实例"(Create a new instance)，请单击"下一步"(Next) 按钮继续执行步骤 6。
   - 如果选择"选择现有实例"(Choose an existing instance)，则表格会显示所选区域中所有运行的实例。如果所选实例没有显示链接，请单击"下一步"(Next) 按钮继续执行步骤 7。
   - 如果所选实例显示链接，可以取消部署并通过此链接访问 SoftwareCIM。

6. 创建实例。
   - 输入“实例名称”(Instance Name)，或者使用默认名称。
   - 还可以输入“描述”(Description)。

     说明

     实例名称和描述的输入限制

     将鼠标悬停在问号图标上方，可显示“实例名称”(Instance Name) 和“描述”(Description) 的具体输入限制。

   - 选择“虚拟机映像”(Machine Image)。
   - 选择“安全组规则”(Security Group Rule)。

     说明

     安全组规则选择

     - SSH/22：访问云上的虚拟 PC。
     - SGLAN/8444：作为 SGLAN 服务器部署的 SoftwareCIM 连接到 SGLAN 客户端。
     - RDP/3389：启用远程桌面连接功能。
     - HTTPS/443：通过支持的 Web 浏览器访问已部署的 SoftwareCIM 配置页面。

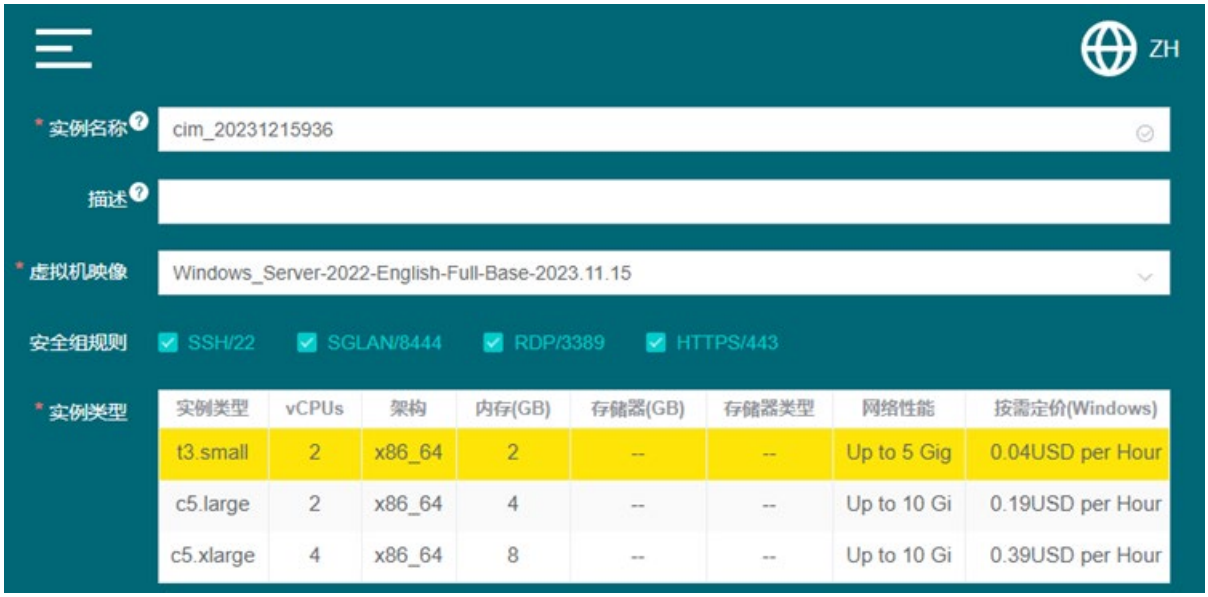
     默认选择所有安全组规则。如果取消选中某一规则，则会显示一条消息提醒用户将禁用相应的功能。

     SSH/22 和 SGLAN/8444 是必选规则。如果取消选中其中一个规则或同时取消选中这两个规则，则无法继续执行后续的配置步骤。

     还可以在 AWS 控制台中配置这些规则。

   - 选择“实例类型”(Instance Type)。

单击“下一步”(Next) 按钮以继续。



7. 上传证书和私钥文件。单击“下一步”(Next) 按钮以继续。

如果单击“跳过”(Skip)，系统将提示用户将使用默认的 Siemens 证书。

说明

出于安全原因，西门子强烈建议用户创建自定义证书来构建专属的信任区域。

8. 设置以下帐户的密码：
   - Windows 帐户：登录云上的虚拟 PC。
   - SoftwareCIM 帐户：登录 SoftwareCIM。稍后可在 SoftwareCIM 配置页面中更改密码。
   - SGLAN 帐户：授权 SGLAN 客户端连接到 SGLAN 服务器。

   如果在步骤 5 中选择创建新实例，则需要为上述所有帐户设置相应的密码。

如果在步骤 5 中选择使用现有实例，则需要输入正确的 Windows 帐户密码才能登录云上的虚拟 PC。然后需要设置 SoftwareCIM 帐户和 SGLAN 帐户的密码。

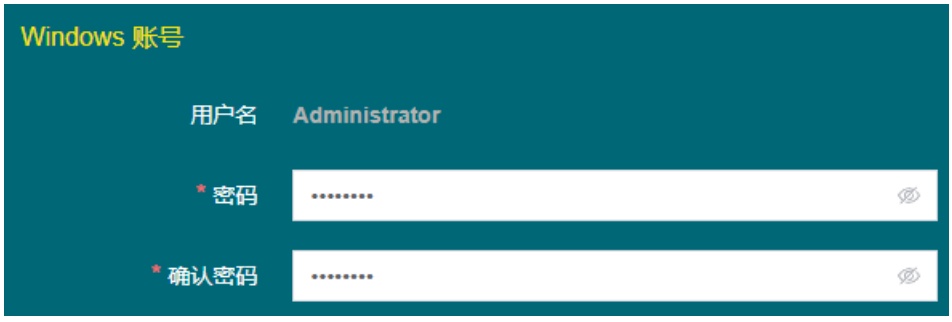
说明

SGLAN 帐户的默认密码是 sglan。
Windows 帐户的默认密码是 Cim@1234。
SoftwareCIM 帐户的默认密码是 cim。

说明

密码输入限制

将鼠标悬停在问号图标上方，可显示所有密码的具体输入限制。



9. 单击"部署"(Deploy) 按钮。

   此过程通常需要 10 分钟左右，具体取决于所选区域。此过程完成后，如果在步骤 6 中选择了 HTTPS/443 安全组规则，窗口将显示二维码和链接。可通过该二维码或链接访问 SoftwareCIM 配置页面。如果未选择 HTTPS/443 安全组规则，部署完成后，窗口将仅显示 SoftwareCIM 的公共 IP。

3.2.2 部署到 Alibaba

要求

Alibaba 云帐户必须满足以下最低权限要求：

```
{
 "Version":"1",
 "Statement": [
   {
     "Effect":"Allow",
     "Action": [
       "ecs:DescribeInstances",
       "ecs:DescribeSecurityGroups",
      "ecs:DescribeSecurityGroupAttribute",
       "ecs:CreateSecurityGroup",
       "ecs:AuthorizeSecurityGroup",
       "ecs:CreateInstance",
       "ecs:DescribeInstanceStatus",
       "ecs:StartInstance",
       "ecs:RevokeSecurityGroup",
       "ecs:DescribeImages",
      "ecs:DescribeAvailableResource",
      "ecs:DescribeImageSupportInstanceTypes",
       "ecs:DescribeResourceByTags",
       "ecs:DescribeTagKeys",
       "ecs:DescribeTags",
       "ecs:ListTagResources",
       "ecs:AddTags",
       "ecs:RemoveTags",
       "ecs:TagResources",
       "ecs:UntagResources",
       "ecs:DescribePrice"
     ],
     "Resource": "*"
   },
   {
     "Effect":"Allow",
     "Action": [
       "vpc:DescribeVpcs",
       "vpc:CreateDefaultVpc",
       "vpc:DescribeVpcAttribute",
       "vpc:CreateDefaultVSwitch",
      "vpc:DescribeVSwitchAttributes",
       "vpc:DescribeVSwitches"
     ],
     "Resource": "*"
   },
   {
     "Effect":"Allow",
     "Action": [
       "vpc:AllocateEipAddress",
```

```
        "vpc:AllocateEipAddressPro",
        "vpc:DescribeEipAddresses",
        "vpc:AssociateEipAddress"
      ],
      "Resource": "*"
    },
    {
      "Effect":"Allow",
      "Action": "bssapi:GetSubscriptionPrice",
      "Resource": "*"
    }
  ]
}
```

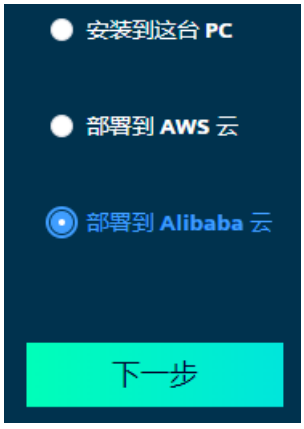
要更改 Alibaba 云帐户的权限，请参见“这里 (https://www.alibabacloud.com/help/zh/ram/user-guide/grant-permissions-to-a-ram-role)”。

要创建 Alibaba 云帐户，请参见“这里 (https://www.alibabacloud.com/help/zh/analyticdb-for-mysql/getting-started/create-an-alibaba-cloud-account-2)”。

操作步骤

要将 SoftwareCIM 部署到 Alibaba 云，请执行以下步骤：

1. 双击安装程序“SoftwareCIMInstaller.exe”。
2. 查看许可条款，然后单击“接受”(Accept)。如果单击“取消”(Cancel)，程序将退出。
3. 选择“部署到 Alibaba 云”(Deploy to Alibaba Cloud)，然后单击“下一步”(Next)。

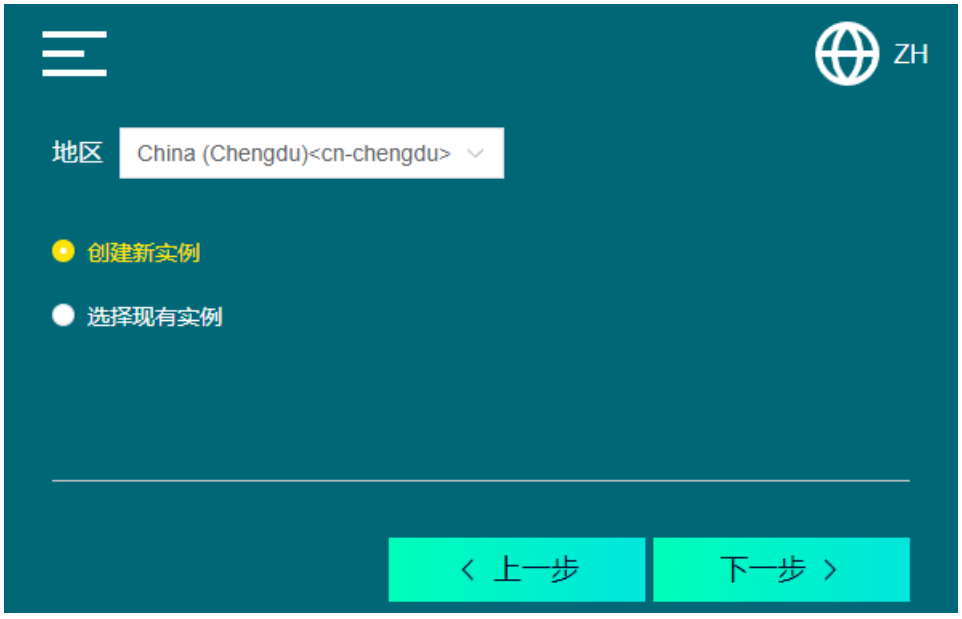


4. 登录云。
   - 输入“访问密钥 ID”(Access Key ID)。
   - 输入“秘密访问密钥”(Secret Access Key)。
   - 如果使用 Alibaba 临时凭据帐户 (TVM) 登录，请输入“会话令牌”(Session Token)。

   单击“下一步”(Next) 按钮以继续。

5. 选择实例的“区域”(Region)。
   - 如果选择“创建新实例”(Create a new instance)，请单击“下一步”(Next) 按钮继续执行步骤 6。
   - 如果选择“选择现有实例”(Choose an existing instance)，则表格会显示所选区域中所有运行的实例。如果所选实例没有显示链接，请单击“下一步”(Next) 按钮继续执行步骤 7。

– 如果所选实例显示链接，可以取消部署并通过此链接访问 SoftwareCIM。



6. 创建实例。
   – 输入“实例名称”(Instance Name)，或者使用默认名称。
   – 还可以输入“描述”(Description)。

   说明

   实例名称和描述的输入限制

   将鼠标悬停在问号图标上方，可显示“实例名称”(Instance Name) 和“描述”(Description) 的具体输入限制。

   – 选择“虚拟机映像”(Machine Image)。

– 选择“安全组规则”(Security Group Rule)。

说明

安全组规则选择

- SSH/22：访问云上的虚拟 PC。
- SGLAN/8444：作为 SGLAN 服务器部署的 SoftwareCIM 连接到 SGLAN 客户端。
- RDP/3389：启用远程桌面连接功能。
- HTTPS/443：通过支持的 Web 浏览器访问已部署的 SoftwareCIM 配置页面。

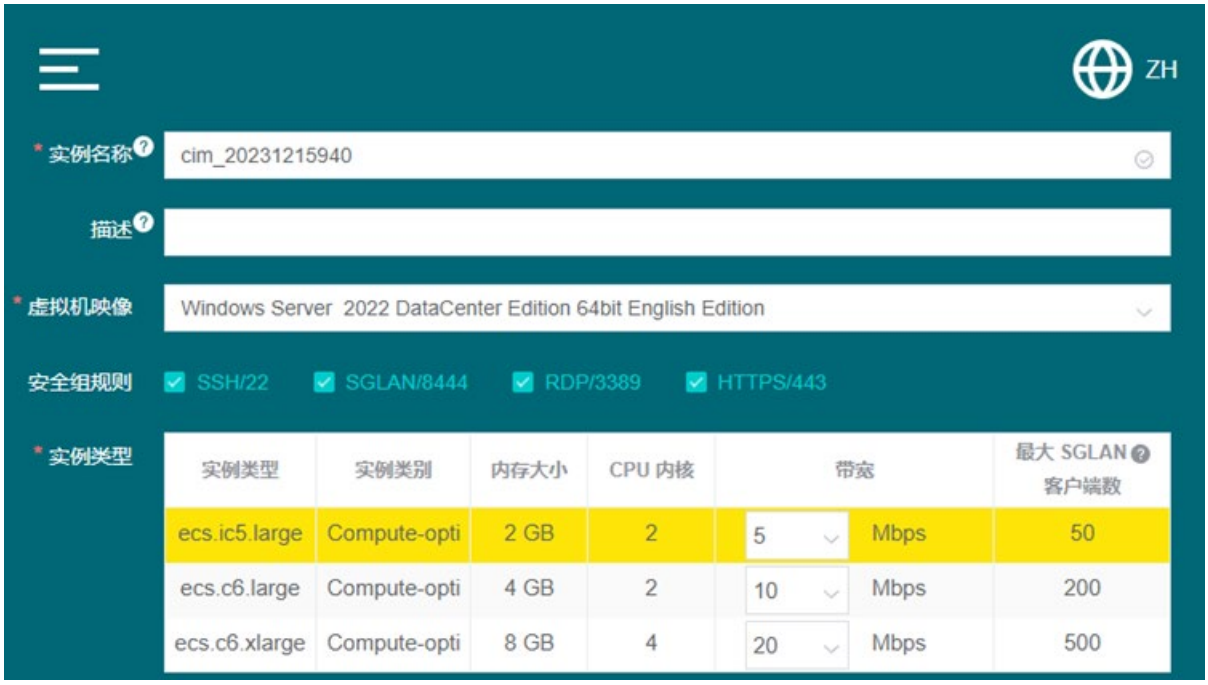
默认选择所有安全组规则。如果取消选中某一规则，则会显示一条消息提醒用户将禁用相应的功能。

SSH/22 和 SGLAN/8444 是必选规则。如果取消选中其中一个规则或同时取消选中这两个规则，则无法继续执行后续的配置步骤。

还可以在 Alibaba 控制台中配置这些规则。

– 选择“实例类型”(Instance Type)。

单击“下一步”(Next) 按钮以继续。



7. 上传证书和私钥文件。单击“下一步”(Next) 按钮以继续。

如果单击“跳过”(Skip)，系统将提示用户将使用默认的 Siemens 证书。

说明

出于安全原因，西门子强烈建议用户创建自定义证书来构建专属的信任区域。

8. 设置以下帐户的密码：
   - Windows 帐户：登录云上的虚拟 PC。
   - SoftwareCIM 帐户：登录 SoftwareCIM。稍后可在 SoftwareCIM 配置页面中更改密码。
   - SGLAN 帐户：授权 SGLAN 客户端连接到 SGLAN 服务器。

   如果在步骤 5 中选择创建新实例，则需要为上述所有帐户设置相应的密码。

   如果在步骤 5 中选择使用现有实例，则需要输入正确的 Windows 帐户密码才能登录云上的虚拟 PC。然后设置 SoftwareCIM 帐户和 SGLAN 帐户的密码。

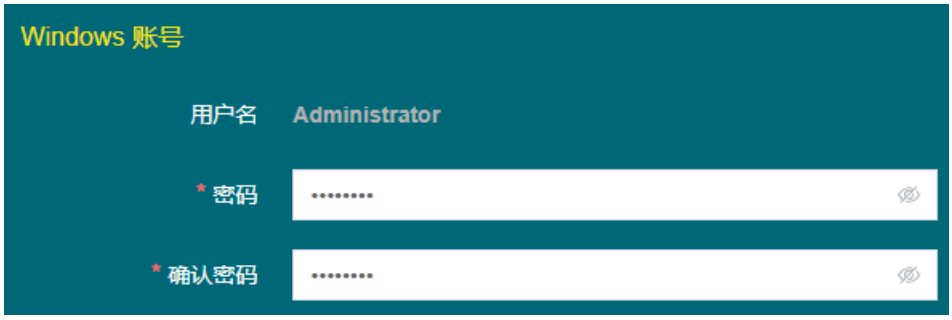
说明

SGLAN 帐户的默认密码是 sglan。
Windows 帐户的默认密码是 Cim@1234。
SoftwareCIM 帐户的默认密码是 cim。

说明

密码输入限制

将鼠标悬停在问号图标上方，可显示所有密码的具体输入限制。



9. 单击“部署”(Deploy) 按钮。

   此过程通常需要 10 分钟左右，具体取决于所选区域。此过程完成后，如果在步骤 6 中选择了 HTTPS/443 安全组规则，窗口将显示二维码和链接。可通过该二维码或链接访问 SoftwareCIM 配置页面。如果未选择 HTTPS/443 安全组规则，部署完成后，窗口将仅显示 SoftwareCIM 的公共 IP。

3.2.3 SoftwareCIM cloud deployment 故障排除

本章介绍了确定故障位置和排除故障等信息。

诊断	可能的原因	可采取的补救措施
未知错误	未知错误。	退出后重新运行“SoftwareCIMInstaller.exe”。
登录失败	云凭据错误。	检查云访问密钥 ID 和秘密访问密钥。
网络错误	网络不稳定或网络连接中断。	检查网络配置。
许可被拒	云帐户不符合权限要求。	检查并更改云帐户权限。
证书校验失败	• 证书文件大小超出限制 • 证书不在有效期内	续订证书。
EIP 分配失败	弹性 IP 数量超出限制。	从云控制台删除未使用的弹性 IP。
SSH 服务连接错误	连接实例的 SSH 服务失败	检查下列各项： • 实例是否初始化 • 云帐户是否锁定 • 实例的 SSH 服务是否正常运行 • 网络连接是否稳定

配置 SoftwareCIM

4

4.1 用户界面概述

登录页面

登录页面显示如下：

① 根据需要选择合适的显示语言。

② 查看 OSS 自述文件。

③ 输入密码。

④ 启用“保持登录”(Keep me logged in) 功能。下次登录时无需输入密码。

⑤ 登录 SoftwareCIM。

说明

默认登录密码为 cim。

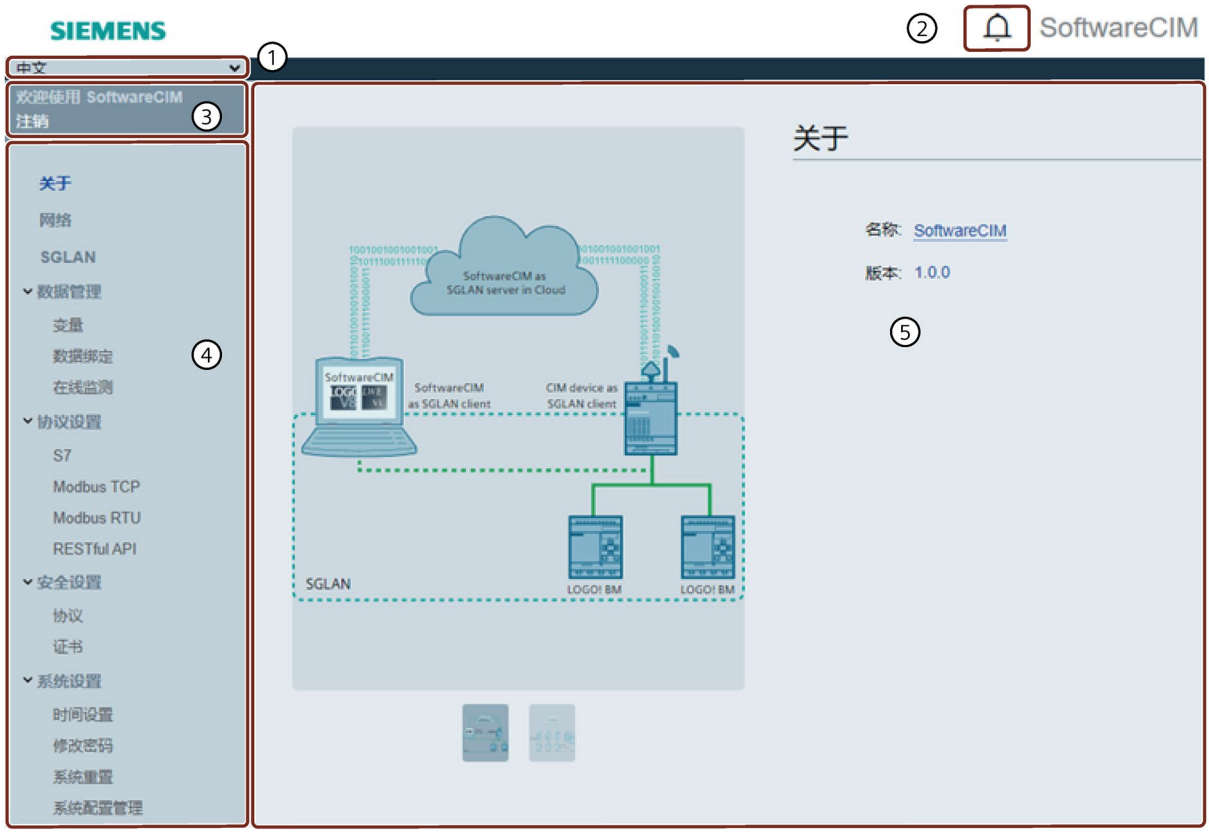
出于安全考虑，西门子建议首次成功登录后将默认登录密码更改为强密码。

说明

默认情况下“保持登录”(Keep me logged in) 为禁用状态。如果启用此功能，此配置将在 30 天后过期。

配置页面

登录后，配置页面显示如下：



① 显示语言选择菜单

② SoftwareCIM 系统状态表

③ 登录/注销

④ 配置页面导航器

⑤ 特定 Web 页面的详细信息。

SoftwareCIM 包括以下配置页面：

配置页面	描述
关于 (页 34)	显示 SoftwareCIM 的常规信息
网络 (页 35)	配置 LAN 或 WAN
SGLAN (页 36)	设置 SGLAN 服务器或客户端
数据管理 (页 41)	编辑变量和绑定
协议设置 (页 46)	设置通信协议
安全设置 (页 62)	配置安全策略
系统设置 (页 68)	配置系统设置

SoftwareCIM 系统状态

单击 🔔，显示 SoftwareCIM 系统状态表。可查看所有 SoftwareCIM 功能模块的状态。当功能模块发生错误时，系统状态表中会显示错误信息。要了解错误原因及解决方法，请参见“SoftwareCIM 系统状态故障排除表 (页 75)”。

功能	状态	上次更新时间	诊断信息
S7 服务器	已禁用	2023-12-05 10:16:11	
S7 客户端	已禁用	2023-12-05 10:16:11	
NTP 服务器	已禁用	2023-12-05 10:16:11	
Modbus TCP 服务端	已禁用	2023-12-05 10:16:11	
Modbus TCP 客户端	已禁用	2023-12-05 10:16:11	
Modbus RTU	已禁用	2023-12-05 10:16:11	
SGLAN	已禁用	2023-12-05 10:16:10	

导航/操作员控制和显示元素概述

配置页面包含以下元素：

图标	功能
	编辑项目
	删除项目
	帮助信息

配置页面包含以下按钮：

图标	功能
	添加一个新行
	保存当前页面上的更改。
	放弃当前页面上的更改。

SoftwareCIM 系统托盘图标菜单

SoftwareCIM 运行时，系统托盘中显示一个应用程序图标。右键单击该图标，将显示如下菜单：

菜单项	功能
打开 SoftwareCIM	显示 SoftwareCIM 窗口。
语言	选择系统托盘图标菜单、“更新和配置更新”窗口的显示语言
更新 (页 72)	检查 SoftwareCIM 是否推出新版本
配置更新 (页 72)	配置 SoftwareCIM 更新
停止/启动 SoftwareCIM 服务	停止或启动正在运行的 SoftwareCIM 服务。
帮助	查看帮助文档。
退出	关闭 SoftwareCIM 窗口并退出系统托盘。

4.2 关于

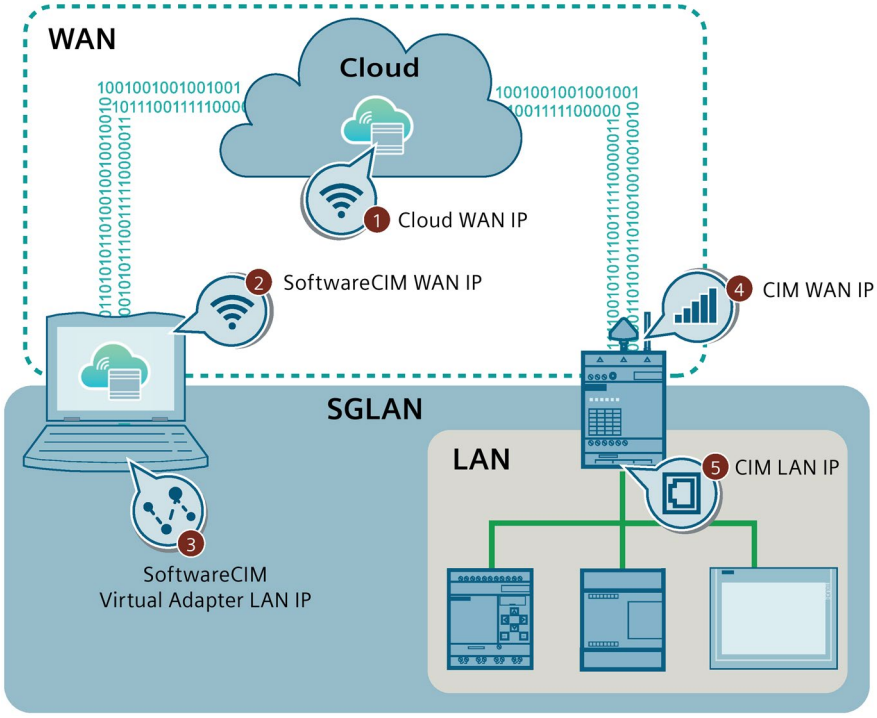
该页面显示 SoftwareCIM 的常规信息。

显示项目	简介
名称	显示 SoftwareCIM 名称。单击显示名称，可对其进行编辑。
版本	桌面应用程序的版本信息

4.3 网络设置

在网络设置中可以配置 LAN 和 WAN。

以下示意图展示了 SoftwareCIM 专用 LAN、WAN 和 SGLAN 的工作原理：



①	云 WAN IP	云上虚拟 PC 的公共 IP 地址。
②	SoftwareCIM WAN IP	安装有 SoftwareCIM 的本地 PC 的 IP 地址。该 IP 地址可用于访问 Internet。
③	SoftwareCIM 虚拟适配器 LAN IP	安装有 SoftCIM 的本地 PC 的虚拟适配器 IP 地址。该 IP 地址可用于 SGLAN 通信，并可访问 SoftwareCIM 配置页面。
④	CIM WAN IP	用于访问 Internet 的 CIM 设备的 IP 地址。
⑤	CIM LAN IP	用于 SGLAN 通信以及访问 CIM 设备配置页面的 CIM 设备的 IP 地址。

如果使用“SoftwareCIMInstaller.exe”应用程序在 AWS 或 Alibaba 云上部署 SoftwareCIM，则通过“WAN -> 高级设置”(WAN -> Advance Setting) 启用“通过 WAN 访问 SoftwareCIM”(Access SoftwareCIM via WAN) 时，系统将自动配置云上 WAN IP 地址。如果在云上手动部署 SoftwareCIM，而不使用该应用程序，则需申请一个弹性 IP，并将其与云上的虚拟 PC 绑定。随后可在“高级设置”(Advance Setting) 中配置弹性 IP。配置完成后即可使用云 WAN IP 访问云上的 SoftwareCIM。

说明

SoftwareCIM 的默认 IP 地址为 192.168.0.81。

说明

更改 SoftwareCIM WAN 接口，仅影响服务器侦听接口，而不影响客户端连接接口。客户端连接到的接口通常由操作系统确定。

4.4 SGLAN 设置

4.4.1 设置 SGLAN 服务器

在此页面中，可将 SoftwareCIM 设置为 SGLAN 服务器。

说明

为了防止泛洪攻击，西门子建议在云端的虚拟 PC 上启用并配置防火墙。

要求

- 可以通过公共 IPv4/IPv6 地址访问要安装 SoftwareCIM 的主机

设置 SGLAN 服务器

1. 启用“SoftwareCIM 作为 SGLAN 服务器”(SoftwareCIM as SGLAN Server)。
2. 选择模式。

3. 设置“访问密码”(Access password) 并在“确认访问密码”(Confirm access password) 中确认该密码。

说明

SGLAN 服务器的默认密码为 sglan。

4. 单击“保存更改”(Save changes)。

4.4.2 设置 SGLAN 客户端

在此页面中，可将 SoftwareCIM 设置为 SGLAN 客户端。

要求

- 要安装 SoftwareCIM 的 PC 可通过 IPv4/IPv6 联网

将 SGLAN 客户端连接到 SGLAN 服务器

在将 SGLAN 客户端连接到 SGLAN 服务器之前，需要获取 SGLAN 服务器的模式、IP 地址和访问密码。

1. 启用“SoftwareCIM 作为 SGLAN 客户端”(SoftwareCIM as SGLAN Client)。
2. 选择“远程主机模式”(Remote Host Mode)。
3. 在“远程主机”(Remote Host) 中输入 SGLAN 服务器 IP 地址。
4. 在“服务器密码”(Server Password) 中输入 SGLAN 服务器的访问密码。

说明

如果已启用 SGLAN 服务器而未更改密码，可使用默认密码“sglan”连接到 SGLAN 服务器。

5. 单击"保存更改"(Save changes)。

连接状态	描述
已断开连接	未连接到 SGLAN
连接	SGLAN 客户端正在连接 SGLAN 服务器并建立 SGLAN。
已连接	SGLAN 已建立，SGLAN 客户端已连接到 SGLAN 服务器。
连接错误	在 SGLAN 客户端与 SGLAN 服务器之间建立通信失败
连接超时	在 SGLAN 客户端与 SGLAN 服务器之间建立通信超时
登录失败	由于密码错误导致登录失败
登录超时	未在有效时间内登录
连接断开	由于网络通信长期失败导致 SGLAN 断开连接
证书错误	验证证书失败
常规错误	常规错误

服务器列表

可以将常用的 SGLAN 服务器添加到服务器列表中。可通过服务器列表快速连接或断开 SGLAN 服务器。

创建服务器项

1. 单击“**添加行**”(Add Row) 按钮。
2. 输入服务器信息。最多可添加 64 个服务器项。

   说明：SGLAN 服务器说明

   远程主机模式：SGLAN 服务器的远程主机模式

   远程主机：SGLAN 服务器的 IP 地址

   服务器密码：SGLAN 服务器的访问密码
3. 单击“保存”(Save) 确认服务器信息，或单击“取消”(Cancel) 放弃配置。
4. 重复步骤 1-3，添加所需的所有服务器项。

连接设备

单击 连接 SGLAN 服务器。

编辑服务器项

单击 ，然后在要更改的服务器项的相应字段中输入新值。

删除服务器项

单击待删除服务器项旁的 删除按钮。

4.5 数据管理

数据管理用于管理变量和数据绑定，并用于监视在线变量。变量和数据绑定的名称必须唯一。

4.5.1 变量

变量由变量名、数据类型、地址类型和地址定义。本章介绍如何创建和编辑用于在 SoftwareCIM 中存储值的变量。所有支持的 UDM 数据类型均可创建变量。

添加变量

1. 单击“添加行”(Add Row) 按钮。最多可以添加 16 行数据。
2. 输入变量的参数。

   名称：变量名中可包含字母、数字和特殊字符

   数据类型：变量的数据类型

   地址类型：变量的地址类型

   地址：SoftwareCIM 中的地址
3. 重复步骤 1-2，添加所需的所有变量。
4. 可监视或修改变量的值。

   值：参数的值

   修改值 (modValue)：修改后的参数值

   修改：单击复选标记可修改参数的值

   修改所有值： 单击“修改所有值”(Modify all values) 以修改作为 modValue 的参数的值

说明

如果变量由事件或动作引用，则该变量不能更改或删除。

更改变量

单击 ，然后在要更改的变量的相应字段中输入新值。

删除变量

单击 删除按钮可删除变量。

4.5.2 数据绑定

此页面用于将事件绑定到操作。更多信息，请参见“通用数据模型 (页 8)”。

用户可配置变量更改事件，并设置绑定事件发生时 SoftwareCIM 将执行的操作。

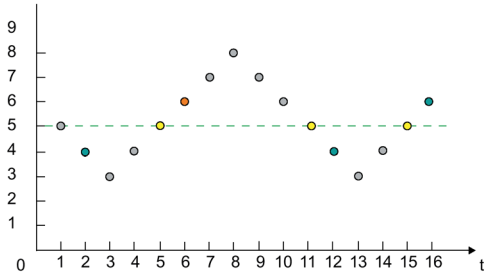
绑定数据

1. 单击"添加行"(Add Row) 添加一个新行。
2. 单击"事件类型"(Event Type) 下拉列表以选择事件。

	事件	事件源	源限制
1	1 变为 0	变量	支持的数据类型：布尔型
2	0 变为 1		
3	值更改		支持的数据类型：除布尔型之外 UDM 支持的所有数据类型
4	大于		支持的数据类型：除布尔型之外 UDM 支持的所有数据类型 **注**：引用值的类型和范围应与事件源变量相同。
5	等于		
6	小于		

说明

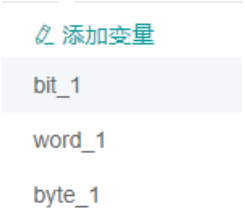
"大于"事件在上升沿触发；"小于"事件在下降沿触发。



- 没有触发事件。
- 触发事件"大于 5"。
- 触发事件"等于 5"。
- 触发事件"小于 5"。

3. 配置事件。单击“变量”(Variable) 下拉列表，选择一个变量 (页 41)。

   如果该列表中没有满足要求的变量，则可单击添加新的变量。



4. 设置操作类型

	操作	操作源	目标限制	备注
1	设定新值	变量	支持的数据类型：所有 UDM 允许的数据类型。	
2	从事件中拷贝变量值		操作的变量类型必须与其复制的源事件的变量类型相同。	
3	按指定值递增		支持的数据类型：除布尔型外所有 UDM 允许的数据类型。	• 增加或减少值只能为正值。 • 如果变量达到范围的最大值或最小值，则该变量不再增加或减少。
4	按指定递减			

5. 配置操作。用户需要从变量列表中选择一个变量，并填写新值。
6. 启用绑定。

说明

如果尚未设置任何变量，则可选择的事件和操作将无法完全显示。

更改数据绑定

对于待更改的数据绑定，单击 更改配置。

删除数据绑定

对于待删除的数据绑定，单击 。

4.5.3 在线监视

通过在线 UDM 数据表，可以监视 UDM 数据。

添加一个在线变量

1. 单击“添加行”(Add Row) 按钮。最多可以添加 64 行数据。
2. 输入变量的参数。

   范围：变量的 UDM 地址类型

   类型：变量的数据类型

   地址：SoftwareCIM 中的地址

   值：所选地址中的变量值

   ModValue：所选地址中修改后的变量值

   修改多行 ModValue 字段中的值后，可单击“修改所有值”(Modify All values) 确认所有更改。

   修改：单击复选标记可修改所选地址中的值
3. 重复步骤 1-2，添加所需的所有变量。

删除变量

单击 删除按钮可删除变量。

4.6 协议设置

在此页面中，可配置以下协议：S7、Modbus TCP、Modbus RTU、RESTful API。

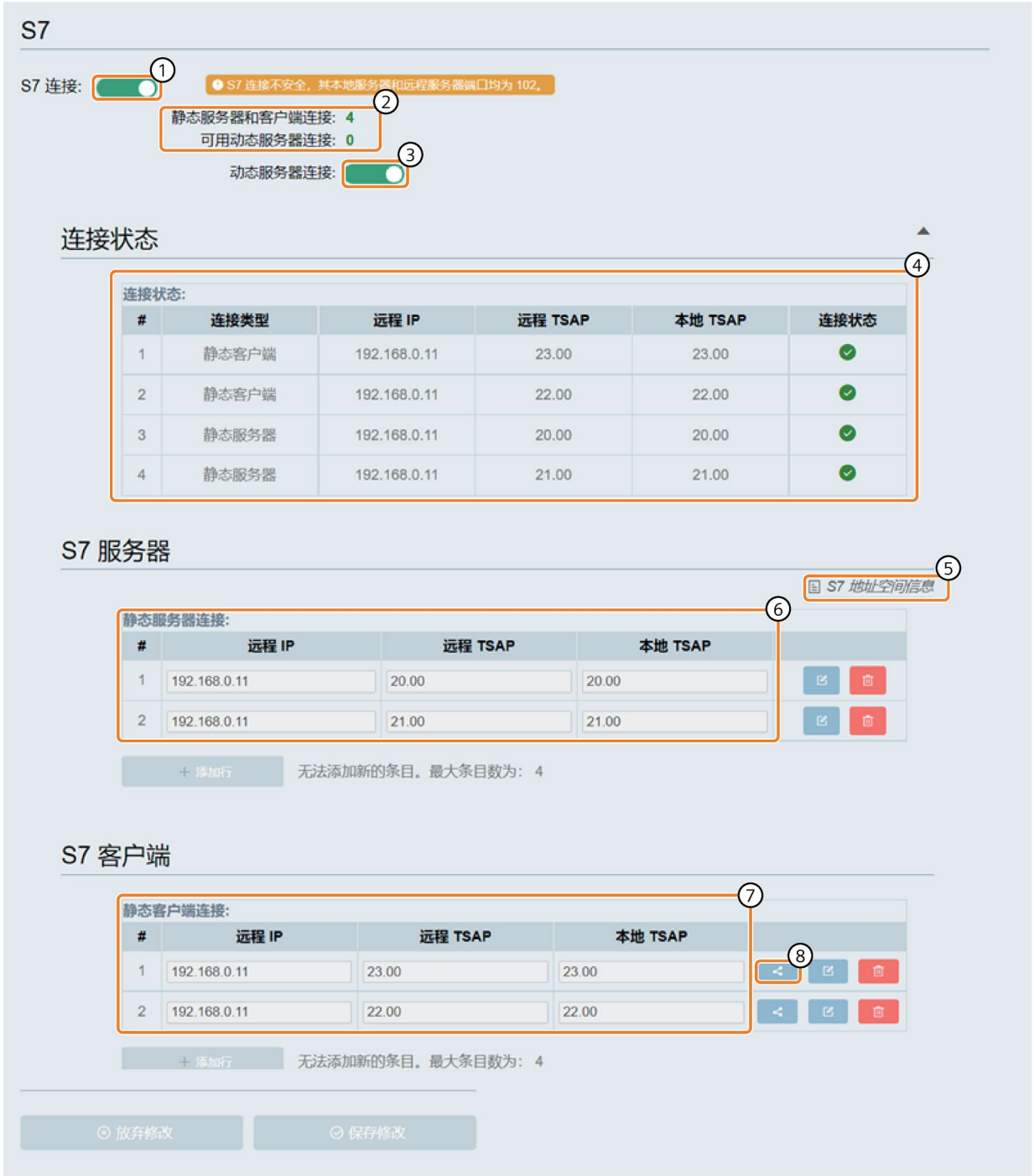
4.6.1 S7

此页面用于启用或禁用 S7 连接，以及检查和编辑 S7 连接。

SoftwareCIM 最多同时建立四个 S7 连接。如果 SoftwareCIM 既是 S7 服务器也是 S7 客户端，将共享连接。

说明

- 在远程设备 (LOGO! BM) 与 SoftwareCIM 之间设置 S7 通信时，确保在连接的远程设备 (LOGO! BM) 中启用 S7 连接和动态服务器连接。
- SGLAN 中的 SoftwareCIM 可配置为 S7 服务器或 S7 客户端。



① 启用或禁用 S7 连接。

注：S7 连接不安全。SoftwareCIM 充当 S7 服务器时，只能通过虚拟 LAN 适配器进行 S7 通信；SoftwareCIM 充当 S7 客户端时，可通过任何适配器进行 S7 通信。

② S7 连接摘要

③ 启用或禁用动态服务器连接

注：SoftwareCIM 最多同时建立四个 S7 连接。如果设置了静态连接，则动态服务器连接数 = 4 - 静态连接数

④ 当前 S7 连接状态

单击 展开连接列表或单击 折叠连接列表。

⑤ S7 地址空间信息页面的链接

⑥ SoftwareCIM 作为 S7 服务器运行时，在此配置其连接属性。
- 远程 IP：待连接的客户端的 IP 地址
- 本地 TSAP：SoftwareCIM 中的 TASP 是 00.01 到 FF.FF
- 远程 TSAP：要连接的客户端的 TSAP

⑦ SoftwareCIM 作为 S7 客户端运行时，在此配置其连接属性。
- 远程 IP：待连接的服务器的 IP 地址
- 远程 TSAP：要连接的服务器的 TSAP
- 本地 TSAP：SoftwareCIM 中的 TASP 是 00.01 到 FF.FF

⑧ SoftwareCIM 作为 S7 客户端运行时，单击打开相应连接的“数据传输表”(Data transfer table)。

配置数据传输表

SoftwareCIM 作为 S7 客户端运行时，需要配置连接的数据传输表：

1. 单击"添加行"(Add Row)。最多可以添加 16 行数据。
2. 单击 ②，选择 SoftwareCIM 的 UDM 地址类型。
3. 在 SoftwareCIM 的地址栏中输入一个地址 ③。
4. 单击 ④，选择数据传输方向。
5. 单击 ⑤，选择远程 S7 服务器的 S7 地址类型。
6. 输入远程 S7 服务器的 S7 起始地址 ⑥。
7. 输入需要传输的数据的长度 ⑦。

8. 要设置 SoftwareCIM 与服务器数据的同步时间间隔，启用"自定义间隔"(Customized Interval) 并输入指定的时间间隔 ⑧。

   默认的最小传输间隔为 80 ms。

9. 保存更改。

10. 单击 ⑨，关闭数据传输表。

数据传输限制

下表列出了客户端连接时的范围和本地地址限制。

读取和写入请求：

本地地址 (SoftwareCIM)		**远程地址（S7 兼容设备）**
地址类型	范围	地址类型
IB	0 到 511	IB、QB、MB、VB、数据块
QB	0 到 511	
MB	0 到 511	
VB	0 到 1023	
IW	0 到 510	IW、QW、MW、VW、数据块
QW	0 到 510	
MW	0 到 510	
VW	0 到 1022	
ID	0 到 508	ID、QD、MD、VD、数据块
QD	0 到 508	
MD	0 到 508	
VD	0 到 1020	

说明

地址类型是 UDM (页 8) 过程映像名称与数据类型的组合。例如，IB 表示存储器 I 中的字节。

值应遵循以下规则：本地地址 + 数据长度 ≤ 本地地址类型的最大值。

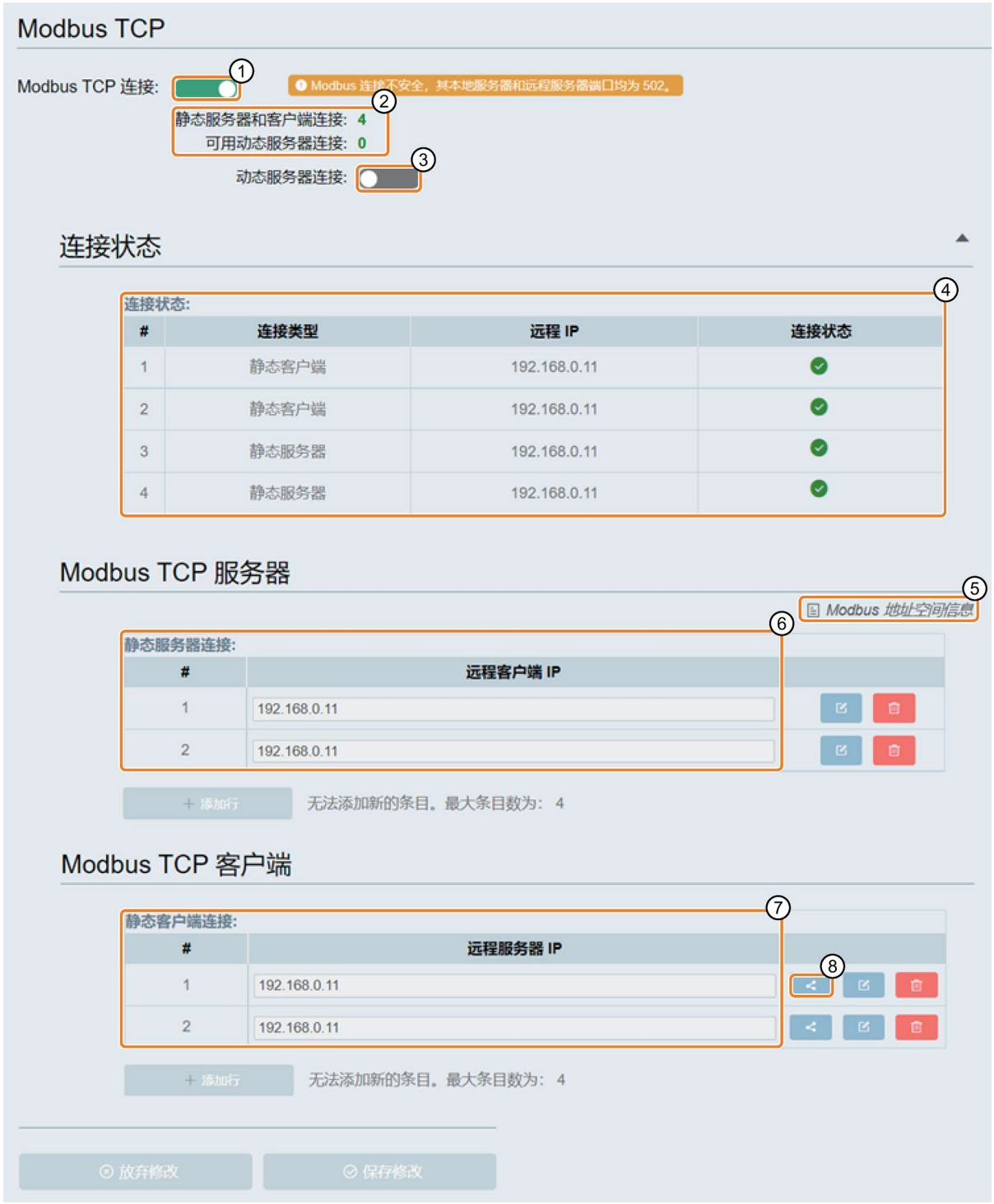
4.6.2 Modbus TCP

在此页面中，可启用或禁用 Modbus TCP 连接，配置 Modbus 通信的传输表，以及检查连接状态。

SoftwareCIM 最多可同时建立四个 Modbus TCP 连接。如果 SoftwareCIM 既是 Modbus TCP 服务器也是 Modbus TCP 客户端，将共享连接。

说明

- 在远程设备 (LOGO! BM) 与 SoftwareCIM 之间建立 Modbus TCP 通信时，确保连接的远程设备 (LOGO! BM) 中已启用 Modbus TCP 连接和 S7 动态服务器连接。
- SGLAN 中的 SoftwareCIM 可配置为 Modbus TCP 服务器或 Modbus TCP 客户端。


Modbus TCP
Modbus TCP 连接:
1
Modbus 连接不安全，其本地服务器和远程服务器端口均为 502。
2
静态服务器和客户端连接: 4
可用动态服务器连接: 0
3
动态服务器连接:
连接状态
4
连接状态:
连接类型 远程 IP 连接状态
1 静态客户端 192.168.0.11
2 静态客户端 192.168.0.11
3 静态服务器 192.168.0.11
4 静态服务器 192.168.0.11
Modbus TCP 服务器
5
Modbus 地址空间信息
6
静态服务器连接:
远程客户端 IP
1 192.168.0.11
2 192.168.0.11
+ 添加行
无法添加新的条目。最大条目数为: 4
Modbus TCP 客户端
7
静态客户端连接:
远程服务器 IP
8
1 192.168.0.11
2 192.168.0.11
+ 添加行
无法添加新的条目。最大条目数为: 4
放弃修改
保存修改

① 启用或禁用 Modbus TCP 连接

注：Modbus TCP 连接不安全。SoftwareCIM 充当 Modbus TCP 服务器时，只能通过虚拟 LAN 适配器进行 Modbus TCP 通信；SoftwareCIM 充当 Modbus TCP 客户端时，可以通过任何适配器进行 Modbus TCP 通信。

② Modbus TCP 连接摘要

③ 启用或禁用动态服务器连接

注：SoftwareCIM 最多同时建立四个 Modbus TCP 连接。如果设置了一些静态连接，

动态服务器连接数 = 4 - 静态连接数

④ 当前 Modbus TCP 连接状态

⑤ Modbus TCP 地址空间信息页面的链接

⑥ 在此可配置服务器的属性。
- 远程 IP：待连接的客户端的 IP 地址

⑦ 在此可配置客户端的属性。
- 远程 IP：待连接的服务器的 IP 地址

⑧ SoftwareCIM 作为 Modbus TCP 客户端运行时，单击打开相应连接的“数据传输表”(Data transfer table)。

配置 Modbus TCP 数据传输

SoftwareCIM 作为 Modbus TCP 客户端运行时，需要配置连接的数据传输表：

1. 单击 ①，添加一个新行。
2. 单击 ②，选择 SoftwareCIM 的 UDM 地址类型。
3. 在 SoftwareCIM 的 UDM 起始地址字段中输入一个地址 ③。
4. 单击 ④，选择数据传输方向。
5. 单击 ⑤，选择远程 Modbus TCP 服务器的 Modbus 地址类型。
6. 输入远程 Modbus TCP 服务器的 Modbus 起始地址 ⑥。
7. 输入需要传输的数据的长度 ⑦。
8. 输入单元 ID ⑧。

9. 要设置 SoftwareCIM 与服务器数据的同步时间间隔，启用自定义间隔并输入指定的时间间隔⑨。

   默认的最小传输间隔为 80 ms。

10. 保存更改并关闭数据传输表。

数据传输限制

下表列出了客户端连接时的范围和本地地址限制。

本地地址 (SoftwareCIM)		**远程地址（Modbus TCP 兼容设备）**
地址类型	范围	地址类型
IB	0.0 到 511.7	线圈 离散输入 (DI)
QB	0.0 到 511.7	
MB	0.0 到 511.7	
VB	0.0 到 1023.7	
IW	0 到 510	保持性寄存器 (HR) 输入寄存器 (IR)
QW	0 到 510	
MW	0 到 510	
VW	0 到 1022	

说明

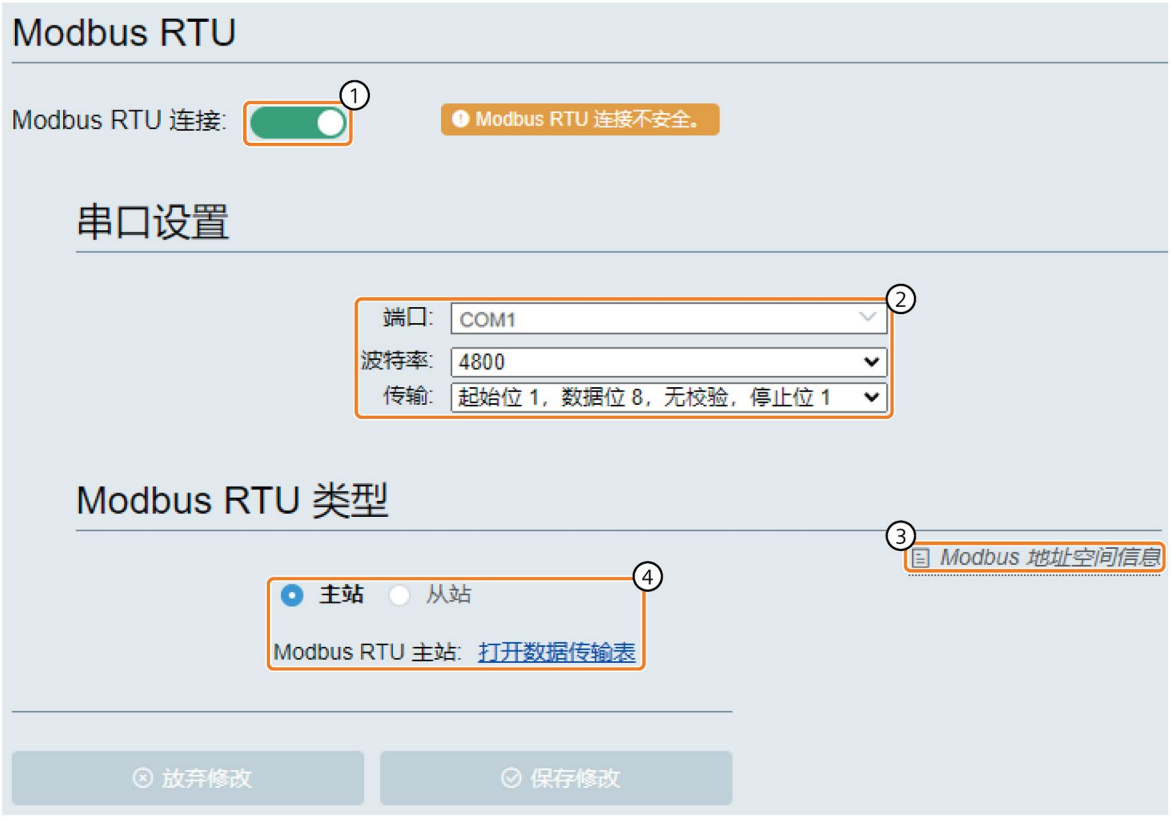
地址类型是 UDM (页 8) 过程映像名称与数据类型的组合。例如，IB 表示存储器 I 中的位。

值应遵循以下规则：本地地址 + 数据长度 ≤ 本地地址类型的最大值。

4.6.3 Modbus RTU

此页面用于启用、禁用和设置 Modbus RTU 连接。

SoftwareCIM 只能建立一个 Modbus RTU 连接，并充当 Modbus RTU 主站或 Modbus RTU 从站。



① 启用或禁用 Modbus RTU 连接

注：Modbus RTU 连接不安全。

② 在此，可配置串行端口的连接属性。

- “端口”(Port)：选择串行端口
- 波特率：设置传输速度
- 传输：串行端口设置

③ Modbus 地址空间信息页面的链接

④ 在此，可配置 Modbus RTU 类型

- 如果选择“主站”(Master)，则需要设置“数据传输表”(Data transfer table)。
- 如果选择“从站”(Slave)，则需要设置“Modbus RTU 从站 ID”(Modbus RTU Slave ID)。

  “Modbus RTU 从站 ID”(Modbus RTU Slave ID) 的范围：1 到 255。

设置数据传输表

SoftwareCIM 作为主站运行时，需要在连接的数据传输表中设置以下值：

1. 单击 ①，添加一个新行。
2. 单击 ②，选择 SoftwareCIM 的 UDM 地址类型。
3. 在 SoftwareCIM 的 UDM 起始地址字段中输入一个地址 ③。
4. 单击 ④，选择数据传输方向。
5. 单击 ⑤，选择远程 Modbus RTU 从站的 Modbus 地址类型。
6. 输入远程 Modbus RTU 从站的 Modbus 起始地址 ⑥。
7. 输入需要传输的数据的长度 ⑦。
8. 输入远程 Modbus RTU 从站的单元 ID（从站 ID/地址）⑧。
9. 要设置 SoftwareCIM 与服务器数据的同步时间间隔，选中该复选框并输入指定的时间间隔 ⑨。

   默认的最小传输间隔为 80 ms。
10. 保存更改并关闭数据传输表。

数据传输限制

下表列出了客户端连接时的范围和本地地址限制。

本地地址 (SoftwareCIM)		**远程地址（Modbus RTU 兼容设备）**
地址类型	范围	地址类型
IB	0.0 到 511.7	线圈 离散输入 (DI)
QB	0.0 到 511.7	
MB	0.0 到 511.7	
VB	0.0 到 1023.7	
IW	0 到 510	保持性寄存器 (HR) 输入寄存器 (IR)
QW	0 到 510	
MW	0 到 510	
VW	0 到 1022	

说明

地址类型是 UDM (页 8) 地址类型名称与数据类型的组合。例如，IB 表示存储器 I 中的位。

值应遵循以下规则：本地地址 + 数据长度 ≤ 本地地址类型的最大值。

4.6.4 RESTful API

对于熟悉该技术并希望使用自动化或编程接口与 SoftwareCIM 进行交互的用户，还可以使用 SoftwareCIM 提供的 REST 接口。

如果连接到 SoftwareCIM 的设备支持 RESTful，则可通过 RESTful API 在 UDM 上 get 或 put 数据。例如，可以通过 Swagger 用户界面访问 UDM 界面，其中包含类、方法和参数的详细说明。

URI 路径格式

```
https://[IP_address_for_cim]/pi/rest/[address_type][data_type_in_short][range]
```

支持的操作

- **get**
- **put**

  在范围内放入一组值时，使用“,”进行分隔。

参数

- **地址类型**：i、m、v、q
- **类型**：访问的数据类型。
- **&**：连接多个离散地址或范围或类型不同的地址
- **范围**：待读取或写入的地址类型中的范围。

  范围的格式：起始地址~结束地址。如果没有设置范围，SoftwareCIM 将设置地址类型的整个范围。

  - ~结束地址：如果没有设置起始地址，SoftwareCIM 将范围的开始视为起始地址。
  - 起始地址~：如果没有设置结束地址，SoftwareCIM 将范围的结束视为结束地址。
  - 地址：访问单个地址。

短数据类型	数据类型	长度	值范围	显示	示例
x	位	1 位	0~1	0 或 1	1
b	字节	8 位	0~FF	十六进制字符串	ab
w	字	16 位	0~FFFF	十六进制字符串	aabb
dw	双字	32 位	0~FFFFFFFF	十六进制字符串	aabbccdd
lw	长字	64 位	0~FFFFFFFFFFFFFFFF	十六进制字符串	aabbccddaabbccdd
su	无符号短整型	8 位	0~255	十进制	12
u	无符号	16 位	0~65535	十进制	1234
du	无符号双精度	32 位	0~4294967295	十进制	12345678
lu	无符号长整型	64 位	0~18446744073709551615	十进制	12345678
si	短整型	8 位	-128~127	十进制	-12
i	整型	16 位	-32768~32767	十进制	-1234
di	双整型	32 位	-2147483648~2147483647	十进制	-12345678
li	长整型	64 位	-9223372036854775808 至 9223372036854775807	十进制	-12345678
r [1]	实数	32 位	-3.4E38 ~ +3.4E38	十进制	1234.5678
lr [1]	长实数	64 位	-1.797E308 ~ +1.797E308	十进制	-1234.5678

1 REAL 和 LONG REAL 类型的有效位不能超过 6。

示例

在以下示例中，[address type][type][range] 部分可替换为其它允许的参数。

示例	描述
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3~8.7`	范围 I 中 [5.3, 8.7] 的所有位
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/i` `https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix`	范围 I 中的所有位
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3`	范围 I 中 5.3 的位
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3~8.7`	范围 I 中 [5.3, 8.7] 的所有位
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100`	范围 I 中 100 的字
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100~200`	范围 I 中 [100, 200] 的所有字
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100~`	范围 I 中 [100, range_end] 的所有字
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/qb100`	范围 Q 中 100 的字节
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/qr100`	范围 Q 中 100 的实数
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/qr~100`	范围 Q 中 [range start, 100] 的实数
`https://xxx.xxx.xxx.xxx:xxxx/pi/rest/ix0.0&qi12`	范围 I 中 0.0 的位和范围 Q 中 12 的位 [1]

1 从 `/pi/rest/` 开始，命令长度应在 500 个英文字符之内。

注：连接字错误将导致地址无法识别。

4.7 安全设置

4.7.1 协议

在此页面中，可检查和管理所有协议。通过切换开关，启用/禁用协议。系统默认禁用除 HTTPS 之外的其它所有协议。

启用 S7/Modbus TCP/Modbus RTU/NTP

启用某个协议时，会在相应的协议设置页面中恢复之前的协议配置。

说明

RESTful API 安全性较低。如果启用 RESTful API for SoftwareCIM，设备通过虚拟 LAN 适配器访问 SoftwareCIM 时不需要进行身份验证；只有设备通过选定的 WAN 适配器访问 SoftwareCIM 时才需要进行身份验证。

仅在需要时启用 RESTful API。

说明

NTP 连接不安全。SoftwareCIM 充当 NTP 服务器时，只能通过虚拟 LAN 适配器进行 NTP 通信。

禁用 S7/Modbus TCP/Modbus RTU/NTP

如果禁用协议，SoftwareCIM 将无法作为服务器或客户端。

4.7.2 证书

SoftwareCIM 可用于配置和维护证书。

- 自带证书：生成并选择证书用于设置安全 Web 服务器和 SGLAN 服务器的证书
- 受信任的证书：选择 SGLAN 客户端的证书

说明

出于安全原因，西门子强烈建议用户创建自定义证书来构建专属的信任区域。

4.7.2.1 已拥有的证书

为了安全访问 Web 配置和设置 SGLAN 服务器，SoftwareCIM 提供三种类型的证书解决方案。SoftwareCIM 内置证书是默认解决方案。

证书解决方案	源	大小限制（字节）
SoftwareCIM 内置证书	由 LOGO! 主模块进行签名	1024
SoftwareCIM 内部证书	由 SoftwareCIM 生成	1024
外部证书	由用户上传到 SoftwareCIM	4000

下载 SoftwareCIM 内置证书

SoftwareCIM 内置证书是在生产过程中创建的。

1. 通过选中内置证书旁的复选框来选择内置证书。
2. 单击“下载”(Download)，下载 LOGO Root CA。

获取 SoftwareCIM 内部证书

SoftwareCIM 可以为自己生成证书。

1. 通过选中 SoftwareCIM 内部证书旁的复选框来选择它。
2. 单击“生成”(Generate)，生成 SoftwareCIM CA。

3. 单击"下载"(Download)，下载 SoftwareCIM CA。
4. 单击"保存修改"(Save Changes) 保存更改；或单击"放弃修改"(Discard Changes) 放弃更改。

上传外部 CA

SoftwareCIM 允许用户向 SoftwareCIM 导入自定义 CA 和密钥。

1. 通过选中外部证书旁的复选框来选择外部证书。
2. 单击上传字段，选择自定义 CA 和密钥。

3. 单击“导入”(Import)，将 CA 和密钥导入 SoftwareCIM。
4. 单击“保存修改”(Save Changes) 保存更改；或单击“放弃修改”(Discard Changes) 放弃更改。

4.7.2.2 受信任的证书

要构建 SGLAN，需要在服务器和客户端中选择同一受信任证书。SoftwareCIM 内置证书是默认解决方案。

说明

确保导入 SoftwareCIM 中的证书在有效期内。

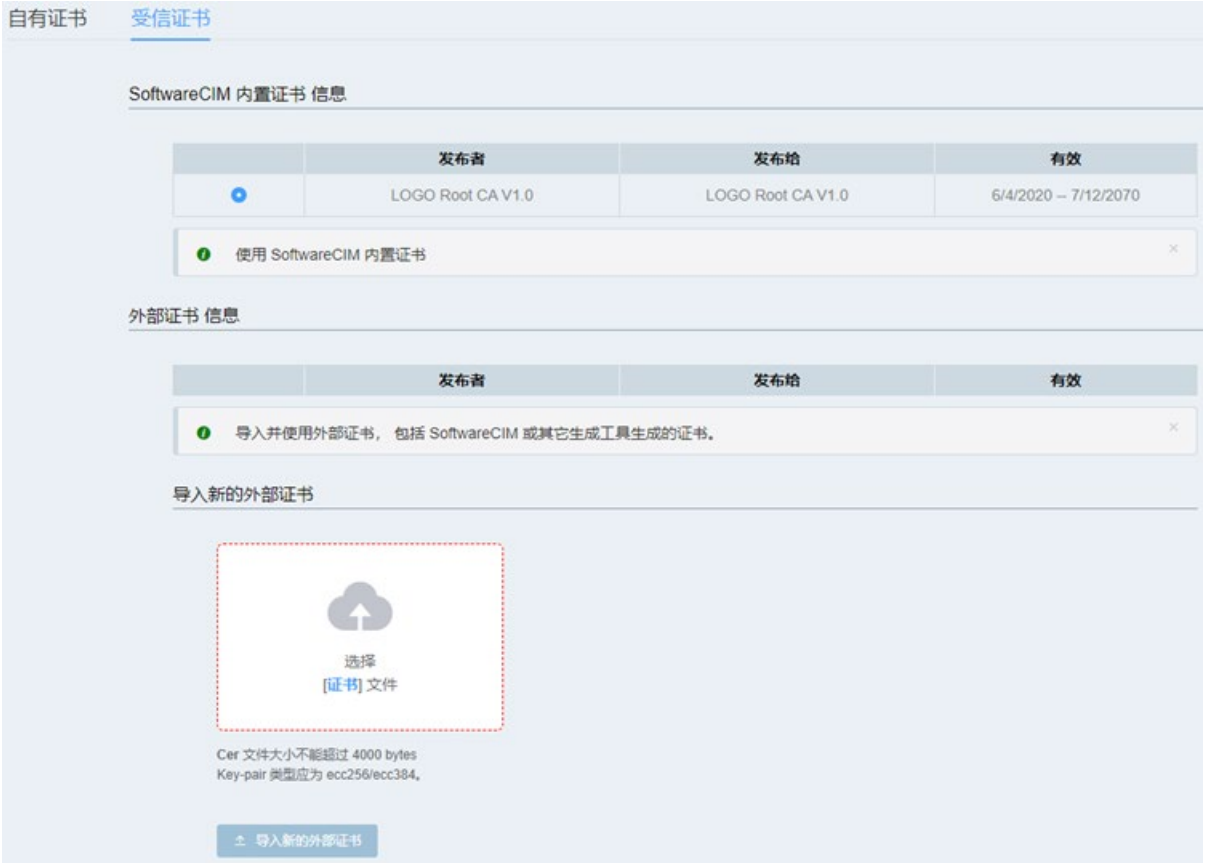
证书解决方案	源	大小限制（字节）
SoftwareCIM 内置证书	由 LOGO! 主模块进行签名	1024
外部证书	由用户上传到服务器和客户端 [1]	4000

[1] 外部证书包括由 SoftwareCIM 或其它生成工具创建的证书。

在 SoftwareCIM 中导入外部 CA

按如下方法将外部 CA 导入 SoftwareCIM：

1. 单击上传字段，选择自定义 CA。
2. 单击“导入新的外部证书”(Import New External Certificate) 将 CA 导入 SoftwareCIM。
3. 单击“保存修改”(Save Changes) 保存更改；或单击“放弃修改”(Discard Changes) 放弃更改。



4.8 系统设置

4.8.1 时间设置

在此页面中，可对 SoftwareCIM 执行以下操作。

- 检查当前时间和时区

  SoftwareCIM 时间和时区信息与 PC 系统时间同步。

- 启用/禁用 NTP 服务器
- 启用/禁用映射时间到 UDM

说明

如果 SoftwareCIM 时间超出证书定义的范围，SoftwareCIM 将生成新的证书。在证书生成过程中，页面可能会卡顿几秒钟。

4.8.2 修改密码

在此页面中，可更改 SoftwareCIM 的登录密码。

说明

如果没有更改密码，可以使用默认密码 cim 登录。

西门子强烈建议在首次登录 SoftwareCIM 后更改默认密码。

如果忘记密码，则需要卸载 SoftwareCIM，然后重新安装，之前的配置将丢失。重新安装后，可以使用默认密码登录 SoftwareCIM。

要更改密码，必须先输入现有密码，然后输入新密码，并再次输入新密码进行确认。密码最多可以包含 32 个字符。

4.8.3 系统重置

在此页面中，可重新启动 SoftwareCIM 服务或将 SoftwareCIM 配置重置为默认值。

重新启动

可以按“重启”(Restart) 按钮重启 SoftwareCIM 服务。

说明

SoftwareCIM 服务重启后，UDM 中的数据将被清除。

恢复为出厂设置

按下“恢复出厂设置”(Factory Reset) 按钮后，所有 SoftwareCIM 配置都会重置为默认值。

说明

恢复出厂设置前，通过路径“**系统设置 --> 系统配置管理**”(System Setting --> System Configuration Management)，备份配置数据。

恢复出厂设置后，内置证书 (页 63)仍保留。

4.8.4 系统配置管理

此功能用于导出当前的 SoftwareCIM 配置或将 SoftwareCIM 配置文件导入 SoftwareCIM 中。

说明

导出的配置文件只能用于 SoftwareCIM。

导出配置文件

1. 单击"导出配置文件"(Export Configure File) 按钮。
2. 要配置文件防止随意使用，需启用"通过密码保护文件"(Protect file with password) 并设置密码。

说明

将导出以下配置数据：

- IP 地址
- 密码
- 证书
- 密钥
- 时钟
- 网络

导入配置文件

1. 单击"导入配置文件"(Import Configure File) 按钮。
2. 导航到配置文件的保存文件夹，并选择该文件。
3. 如果配置文件受保护，则输入密码。

更新 SoftwareCIM

5

SoftwareCIM 可以通过以下方式进行更新：

- 通过安装更新包进行更新 (页 71)
- 通过 SoftwareCIM 配置进行更新 (页 72)

5.1 通过安装更新包进行更新

要通过安装更新包来更新 SoftwareCIM，请按以下步骤操作：

1. 从西门子网站 (http://www.siemens.com/)下载更新包。
2. 将更新包保存在安装 SoftwareCIM 的 PC 上。
3. 解压更新包。
4. 单击 .exe 文件开始更新。

如果要更新云端部署的 SoftwareCIM，可以使用远程桌面连接功能传输并安装更新包。

说明

出于安全原因，西门子建议通过安装更新包的方式更新 SoftwareCIM。

5.2 通过 SoftwareCIM 配置更新

可以选择通过 SoftwareCIM 配置来自动或手动更新 SoftwareCIM。

自动更新

配置自动更新后，要更新的 SoftwareCIM 将在某个时间点自动检查配置的更新源是否存在更高的版本。如果配置的更新源中存在更高版本的 SoftwareCIM，则将在指定的时间点自动更新 SoftwareCIM。

在配置 SoftwareCIM 的自动更新功能之前，应确保 SoftwareCIM 服务正在运行。

请按照以下步骤配置自动更新：

1. 在系统托盘图标菜单 (页 30)中单击“配置更新”(Configure Update)。
2. 启用自动更新。
3. 从“更新服务器”(Update Server) 下拉菜单中选择更新源。有两个更新源可供选择：
   - SGLAN 服务器

     当要更新的 SoftwareCIM 配置为 SGLAN 客户端并连接到作为 SGLAN 服务器的 SoftwareCIM 时，此更新源可用。

     说明

     SGLAN 服务器和 SGLAN 客户端的 IP 必须在同一子网中，更新才能成功。

     如果选择此更新源，请继续执行步骤 6。

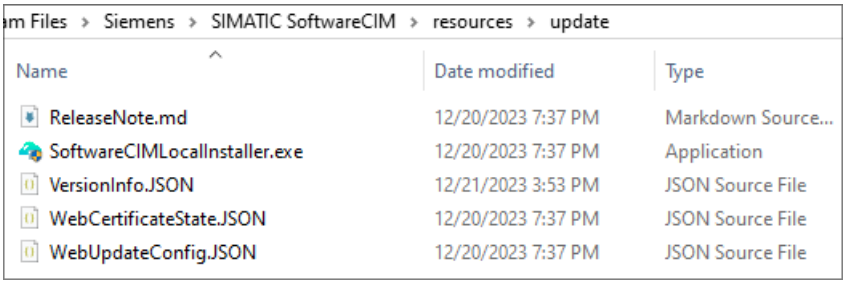
– 自定义更新服务器

  如果选择此更新源，请继续执行步骤 4。

4. 输入服务器地址。
5. 启用证书并上传信任证书。可以禁用证书并跳过此步骤。出于安全原因，西门子建议创建并上传自定义信任证书。
6. 单击"保存更改"(Save changes)。

如果要从自定义更新服务器更新 SoftwareCIM，除上述配置之外，还需要将更新文件复制到服务器中。在本地 PC 上安装最新版本的 SoftwareCIM 后，所需的更新文件位于安装文件夹内。更新文件存储在以下路径中："...SIMATIC SoftwareCIM -> resources -> update"。

下图显示了所有必需的更新文件示例：



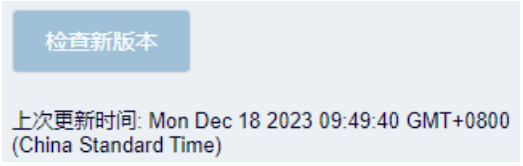
说明

请勿对更新文件进行任何更改；否则，更新将失败。

手动更新

在手动更新 SoftwareCIM 之前，需要执行上述步骤配置自动更新。然后执行以下步骤：

1. 在系统托盘图标菜单 (页 30)中单击“更新”(Update)。
2. 单击“检查新版本”(Check for new version)。



3. 如果从配置的更新源中检测到更高版本，可单击“更新”(Update) 来更新 SoftwareCIM。

SoftwareCIM 故障排除

6

本章介绍了确定故障位置和/或排除故障等信息。

问题	潜在原因	可采取的补救措施
无法访问 SoftwareCIM 服务	SGLAN 虚拟适配器已禁用或卸载。	在 PC 中启用 SGLAN 虚拟适配器。
无法通过 WAN IP 地址访问 SoftwareCIM	• 端口 443 被 PC 中的其它应用程序或服务占用 • SoftwareCIM 服务已停止 • Web 浏览器错误	• 检查 443 端口是否被占用 • 启动 SoftwareCIM 服务 • 清除 Web 浏览器缓存并重新启动浏览器
NTP 客户端时间与配置为 NTP 服务器的 SoftwareCIM 不同步	安装了 SoftwareCIM 的 PC 上的 NTP 服务未禁用。	在 PC 上禁用 NTP 服务。
Modbus RTU 通信失败	Modbus RTU 主站和 Modbus RTU 从站的串行端口模式不一致。	• 在 PC BIOS 中检查并配置 SoftwareCIM 的串行端口模式 • 在基于 Web 的配置页面中检查并配置 CIM 设备的串行端口模式
无法通过 Web 浏览器在云上访问 SoftwareCIM，并显示关于时钟时间错误的错误消息	Web 浏览器系统时间与云上的 Web 服务器时间不一致。	更改 Windows 系统时间，匹配云上 Web 服务器的系统时间。

SGLAN 故障排除

连接状态	描述	潜在原因
连接错误	在 SGLAN 客户端与 SGLAN 服务器之间建立通信失败。	如果模式为 IPv4 或 IPv6： • IP 地址错误 • IP 地址不可访问 • SGLAN 客户端无法访问 Internet
登录失败	由于密码错误导致登录失败。	检查密码。
证书错误	证书校验失败。	• 信任证书不是 SGLAN 服务器专属的证书或信任证书 • 证书过期

系统状态故障排除

错误消息	潜在原因	可采取的补救措施
绑定服务器套接字失败	对应的端口被另一个进程占用。 SoftwareCIM 使用以下端口： • SGLAN 服务器：端口 8444 • S7 服务器：端口 102 • Modbus TCP 服务器：端口 502 • NTP 服务器：端口 123	针对 SoftwareCIM 功能，开启相应的端口。
获取 LAN 适配器的 IPv4 地址失败	• LAN 适配器已禁用 • LAN 适配器的配置无效 • LAN 适配器损坏	• 启用 LAN 适配器 • 使用静态 IPv4 地址配置 LAN 适配器 • 重新安装 SoftwareCIM
COM 端口配置失败	• COM 端口不可用 • 所选的配置选项不受支持	• 检查 COM 端口是否可用 • 使用其它配置选项重试

错误消息	潜在原因	可采取的补救措施
获取 WAN 适配器的 IPv6 地址失败	• 所选的 WAN 适配器已禁用 • 所选的 WAN 适配器不可用 • 所选 WAN 适配器没有有效的 IPv6 地址	• 启用所选 WAN 适配器 • 选择其它 WAN 适配器 • 确保主机可以通过所选的 WAN 适配器访问 Internet • 如果 IPv6 不可用，则使用 IPv4
获取 WAN 适配器的 IPv4 地址失败	• 所选的 WAN 适配器已禁用 • 所选的 WAN 适配器不可用 • 所选 WAN 适配器没有有效的 IPv4 地址	• 启用所选 WAN 适配器 • 选择其它 WAN 适配器 • 确保主机可以通过所选的 WAN 适配器访问 Internet

提示与技巧

7

7.1 如何在 AWS 上手动部署 SoftwareCIM

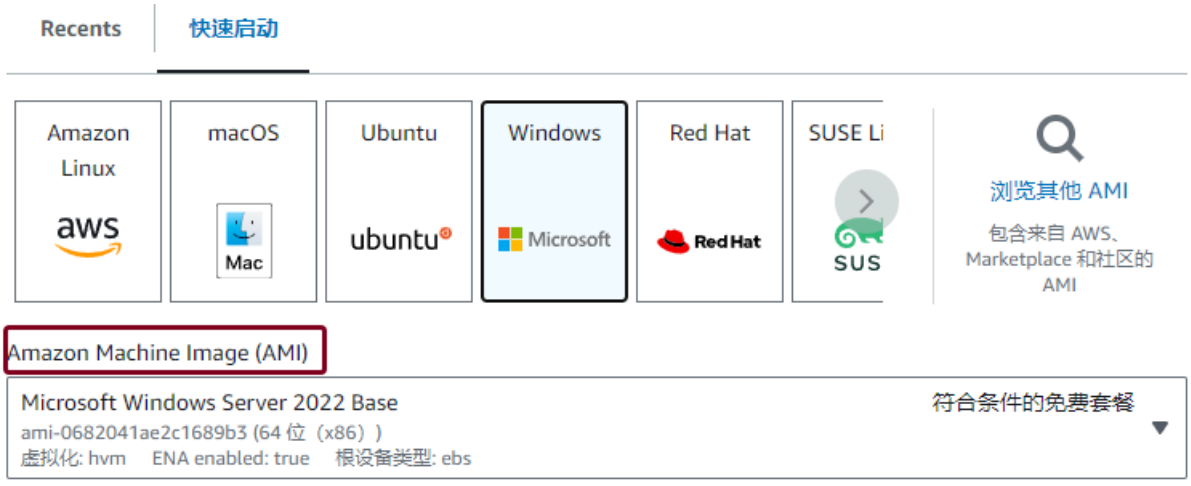
用户也可将 SoftwareCIM 手动部署到 AWS 云。AWS 帐户必须符合权限要求 (页 13)，才能成功部署。

要将 SoftwareCIM 手动部署到 AWS 云，请按照以下步骤操作：

创建 EC2 实例

1. 登录 AWS EC2 管理控制台。
2. 选择帐户旁的区域。通过此区域将 SoftwareCIM 部署到云中。
3. 单击“启动实例”(Launch instance)。

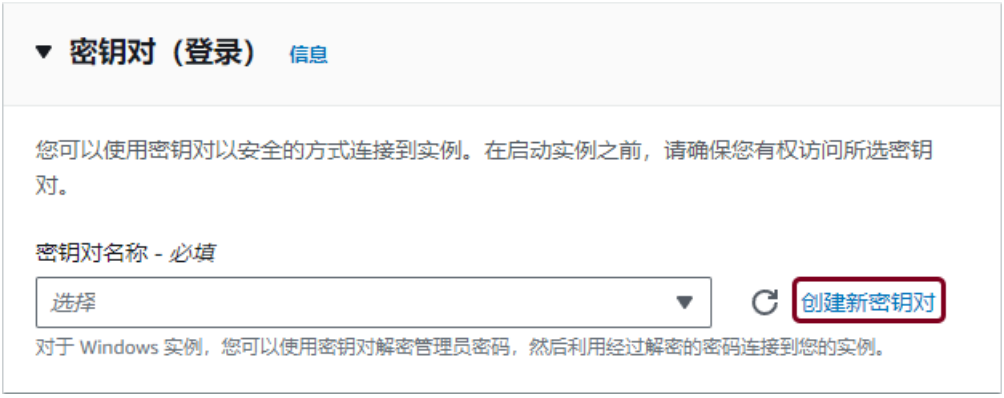
4. 在 Windows OS 中选择 Amazon Machine Image (AMI)。



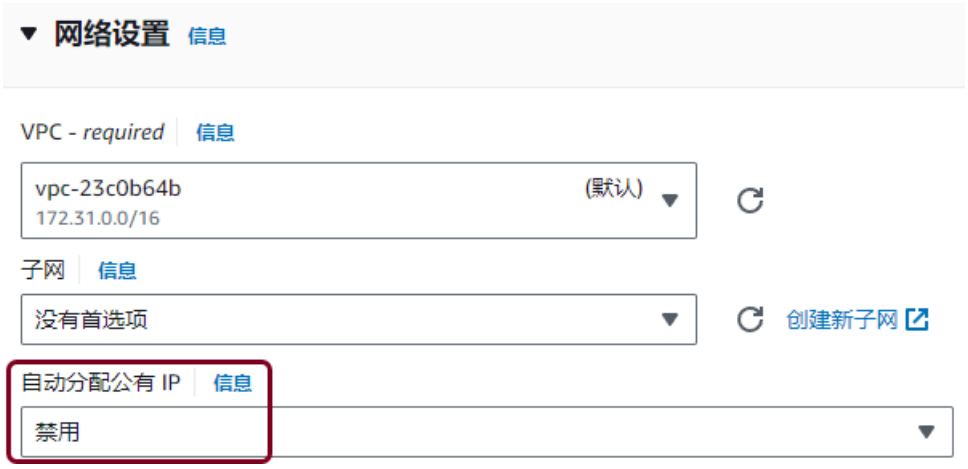
5. 选择 CPU 至少为 2 核、内存至少 2GB 的实例类型。

6. 创建新的密钥对。

   需要将生成的私钥存储在安全且可访问的位置，稍后在连接到实例时将使用该私钥。

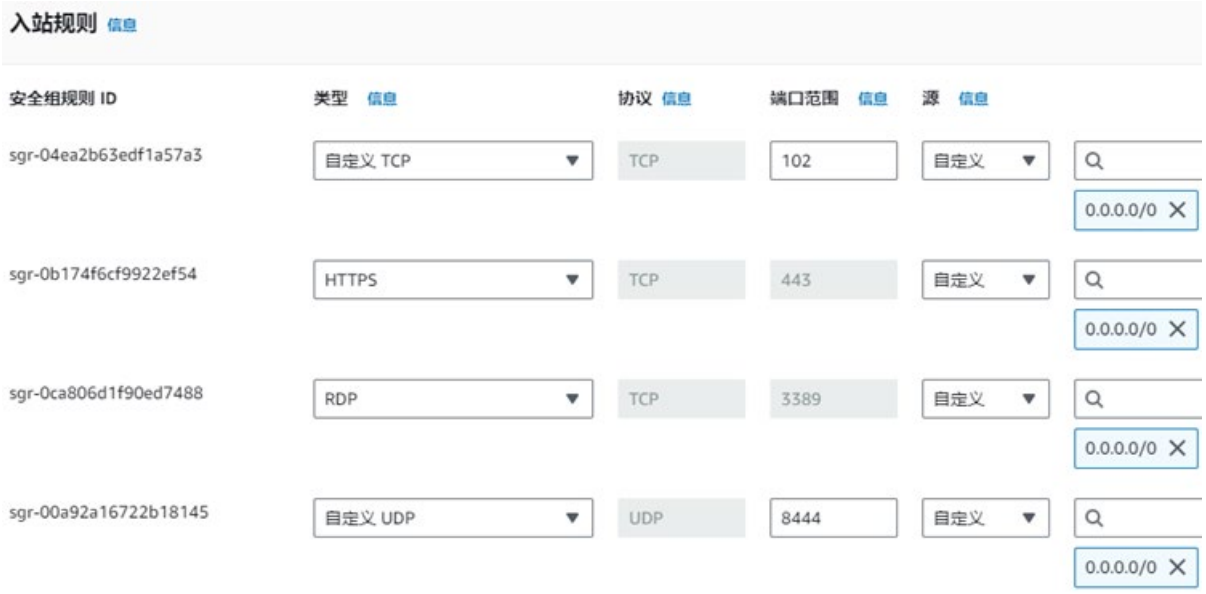


7. 配置网络设置。
   - 禁用自动分配的公共 IP。对于 SoftwareCIM，将使用弹性 IP。



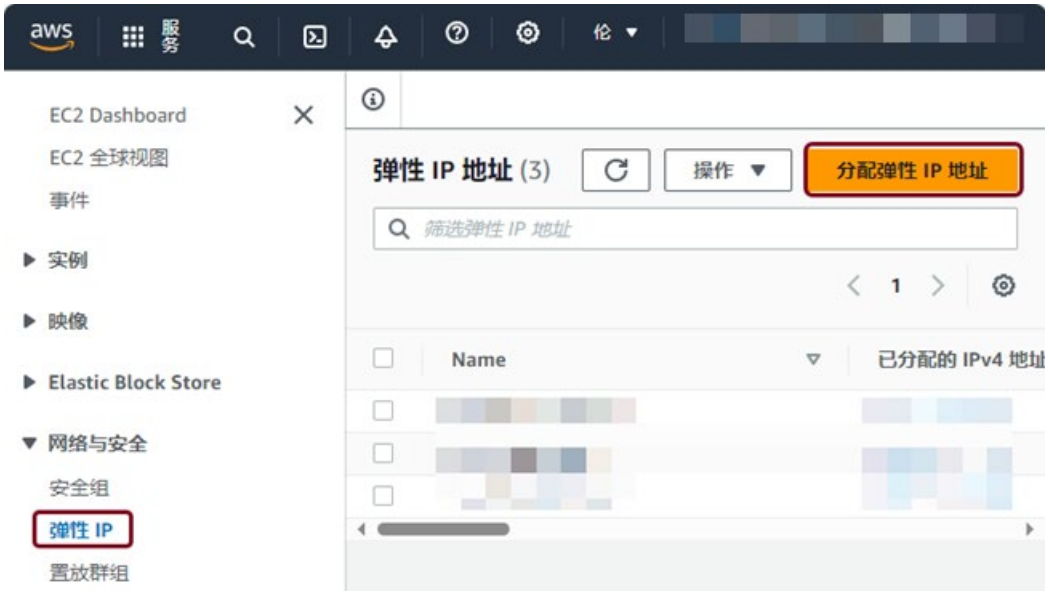
   - 创建安全组并添加安全组规则。安全组规则 HTTPS/端口 443、自定义 UDP/端口 8444 和自定义 TCP/端口 102 是必选项。RDP/端口 3389 和 ssh/端口 22 是可选项，便于连接到其它事务。

8. 单击“启动实例”(Launch instance)。
9. 检查入站规则。

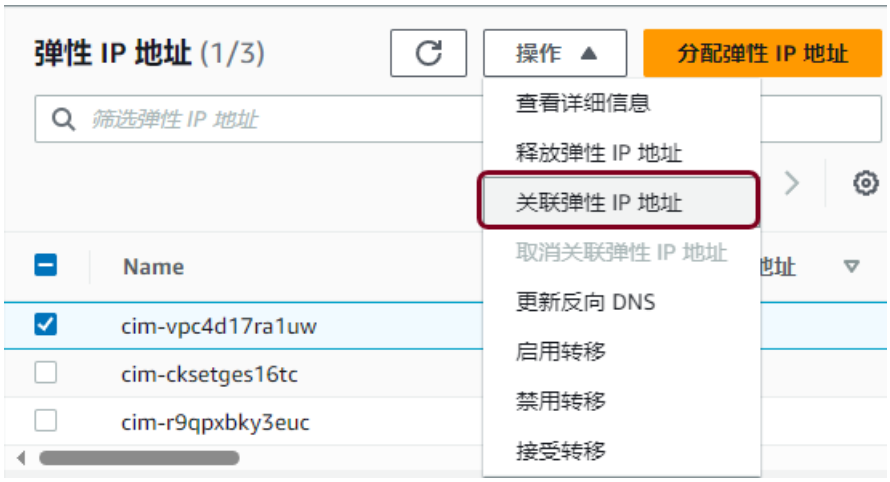


将弹性 IP 绑定到实例

1. 在 AWS EC2 管理控制台中导航到“网络与安全 -> 弹性 IP”(Network & Security -> Elastic IPs)。
2. 单击“分配弹性 IP 地址”(Allocate Elastic IP address)。



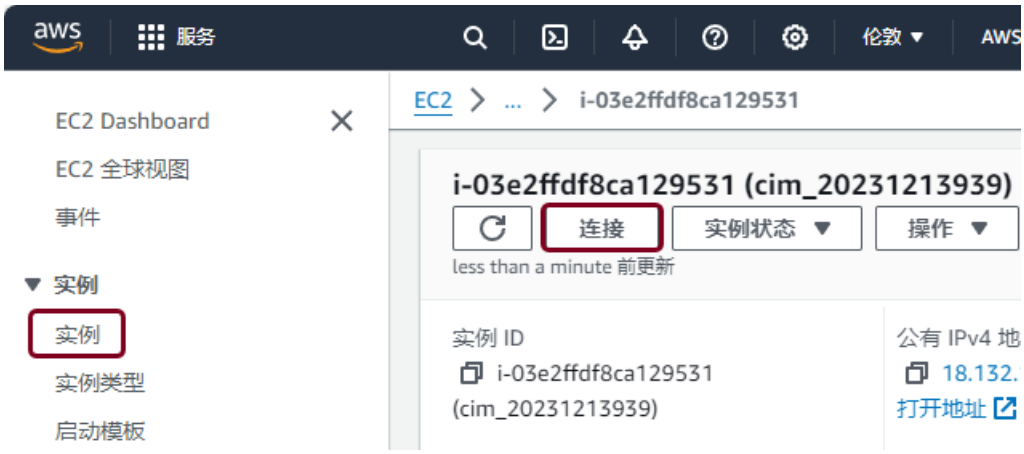
3. 在列表中选择之前创建的弹性 IP，然后在 Actions 菜单中单击“关联弹性 IP 地址”(Associate Elastic IP address)。



4. 选择在上述步骤中创建的实例，然后单击“关联”(Associate)。

登录 AWS 云上的虚拟 PC。

1. 返回之前创建的实例。单击“连接”(Connect)。



2. 单击“RDP 客户端”(RDP client) 并选择“使用 RDP 客户端进行连接”(Connect using RDP client)。单击“获取密码”(Get password)。

3. 上传在上述步骤中生成的私钥，然后单击“解密密码”(Decrypt password)。现在便已获得虚拟 Windows PC 登录密码。
4. 通过 RDP 登录 AWS 云上的虚拟 PC。

将 SoftwareCIM 部署到 AWS 云 - 方式 1

1. 将“SoftwareCIMInstaller.exe”从 Siemens 下载到本地 PC 上。
2. 通过 RDP，将安装程序发送到虚拟 PC 上。此过程可能需要一段时间。
3. 双击“SoftwareInstaller.exe”，在虚拟 PC 上安装 SoftwareCIM。
4. 登录 SoftwareCIM。
5. 在“网络设置”(Network Settings) 页面的“高级设置”(Advance Setting) 中，启用“通过 WAN 访问 SoftwareCIM”(Accessing SoftwareCIM via WAN)，并在“主机名”(Host Name) 中填入弹性 IP 地址。单击“保存更改”(Save changes)。

   现在，可使用弹性 IP 地址安全访问 SoftwareCIM。

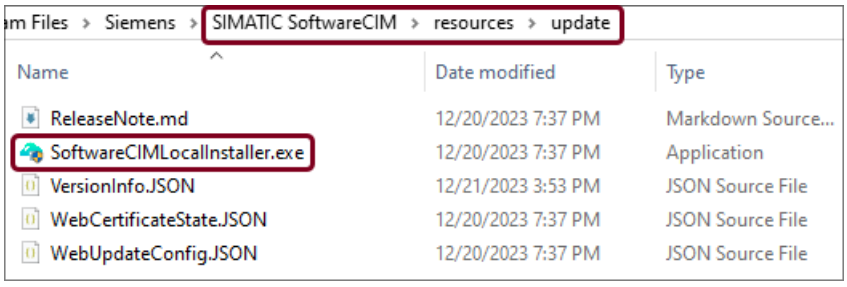
说明

仅当在“主机名”(Host Name) 中填入弹性 IP 时，所部署的 SoftwareCIM 才会配置为 SGLAN 服务器。

将 SoftwareCIM 部署到 AWS 云 - 方式 2

1. 运行“SoftwareCIMInstaller.exe”，将 SoftwareCIM 安装在本地 PC 上。
2. 安装成功后，打开 SoftwareCIM 安装文件夹。

3. “SoftwareCIMLocalInstaller.exe”位于“...SIMATIC SoftwareCIM -> resources -> update”路径中，并通过 RDP 发送到虚拟 PC 中。



4. 双击“SoftwareCIMLocalInstaller.exe”，在虚拟 PC 上安装 SoftwareCIM。
5. 登录 SoftwareCIM。
6. 在“网络设置”(Network Settings) 页面的“高级设置”(Advance Setting) 中，启用“通过 WAN 访问 SoftwareCIM”(Accessing SoftwareCIM via WAN)，并在“主机名”(Host Name) 中填入弹性 IP 地址。单击“保存更改”(Save changes)。

   现在，可使用弹性 IP 地址安全访问 SoftwareCIM。

说明

仅当在“主机名”(Host Name) 中填入弹性 IP 时，所部署的 SoftwareCIM 才会配置为 SGLAN 服务器。

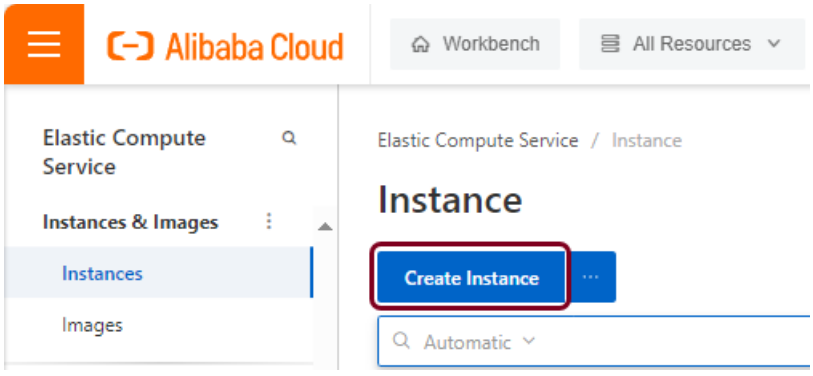
7.2 如何在 Alibaba 上手动部署 SoftwareCIM

此外，也可将 SoftwareCIM 手动部署到 Alibaba 云上。Alibaba 帐户必须符合权限要求 (页 21)，才能成功部署。

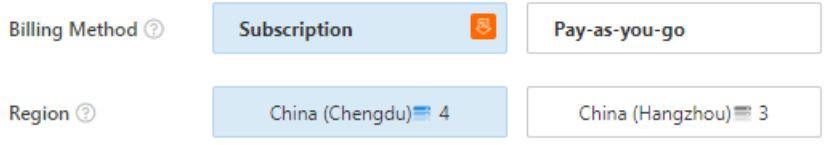
要将 SoftwareCIM 手动部署到 Alibaba 云，请按照以下步骤操作：

创建 ECS 实例

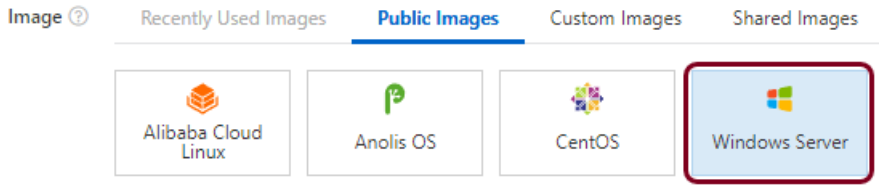
1. 登录 Alibaba ECS 控制台。
2. 单击“创建实例”(Create Instance)。



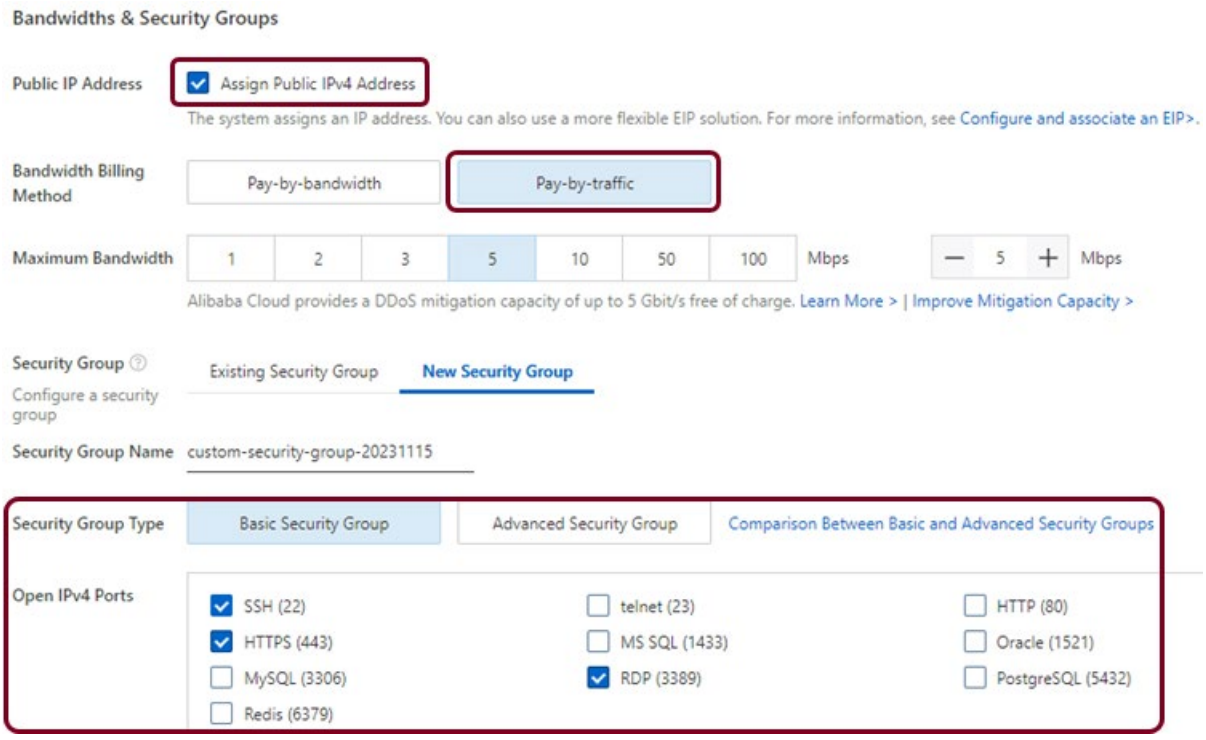
3. 选择“付费类型”(Billing Method) 和“地域”(Region)。



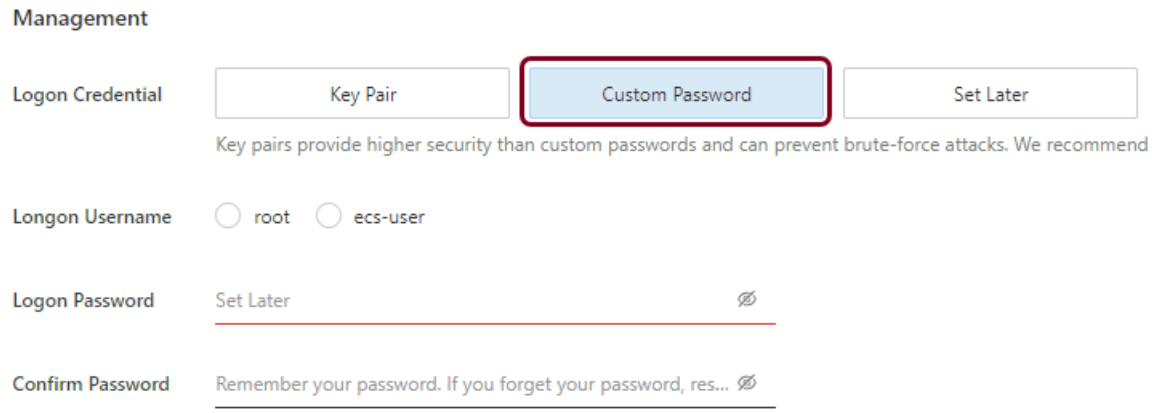
4. 根据需要配置实例。
5. 选择 Windows 服务器作为映像。



6. 配置带宽和安全组。“带宽计费模式”(Bandwidth Billing Method) 中必须选择“按使用流量”(Pay-by-traffic)，否则后续步骤将无法获取弹性 IP。



7. 配置虚拟 Windows PC 登录密码。

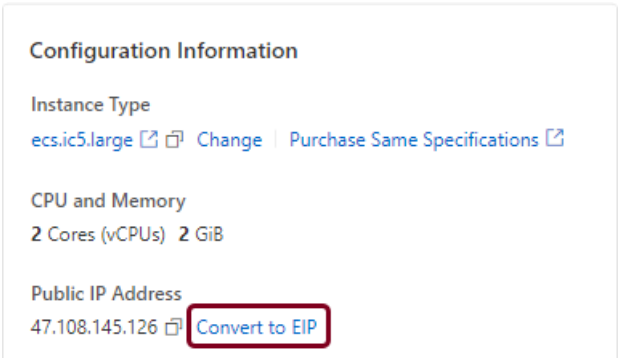


8. 单击“确认下单”(Create Order)。

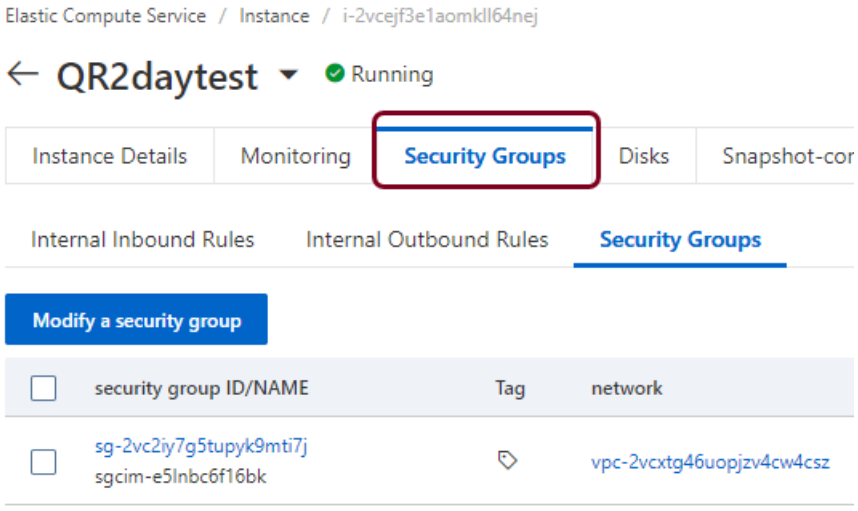
获取弹性 IP

1. 导航到 Alibaba ESC 控制台中的“实例”(Instance)。
2. 单击之前创建的实例。

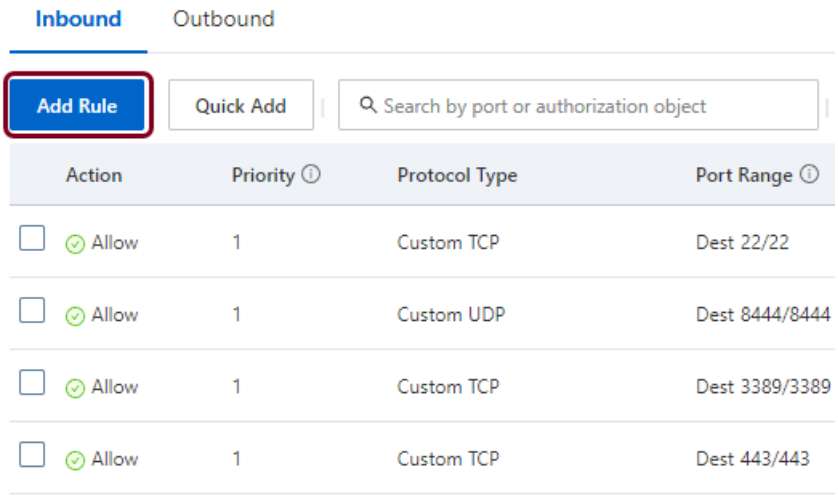
3. 单击“公共 IP 地址”(Public IP Address) 旁的“转换为 EIP”(Convert to EIP)。



4. 转到“安全组”(Security Groups) 并单击用户的安全组。



5. 单击“添加规则”(Add Rule)。添加安全组规则：自定义 UDP/端口 8444 和自定义 TCP/端口 443。



6. 现在，可通过 RDP 登录到 Alibaba 云上的虚拟 PC。

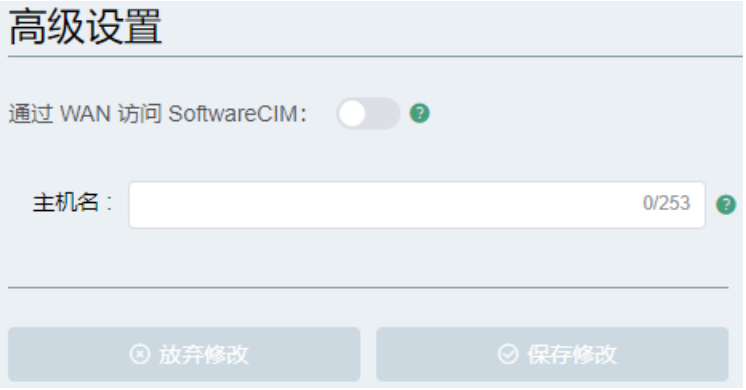
将 SoftwareCIM 部署到 Alibaba 云 - 方式 1

1. 将“SoftwareCIMInstaller.exe”从 Siemens 下载到本地 PC 上。
2. 通过 RDP，将安装程序发送到虚拟 PC 上。此过程可能需要一段时间。
3. 双击“SoftwareInstaller.exe”，在虚拟 PC 上安装 SoftwareCIM。
4. 登录 SoftwareCIM。
5. 在“网络设置”(Network Settings) 页面的“高级设置”(Advance Setting) 中，启用“通过 WAN 访问 SoftwareCIM”(Accessing SoftwareCIM via WAN)，并在“主机名”(Host Name) 中填入弹性 IP 地址。单击“保存更改”(Save changes)。

   现在，可使用弹性 IP 地址安全访问 SoftwareCIM。

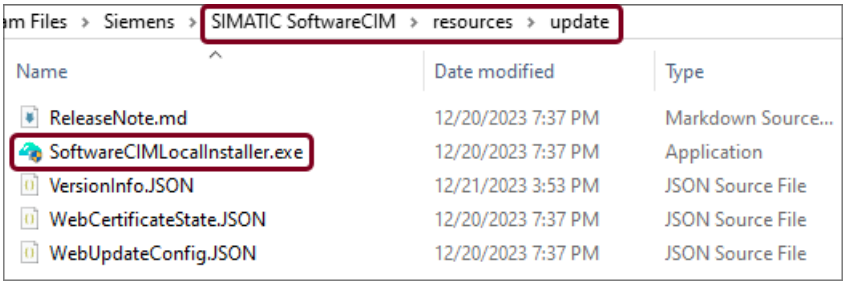
说明

仅当在“主机名”(Host Name) 中填入弹性 IP 时，所部署的 SoftwareCIM 才会配置为 SGLAN 服务器。



将 SoftwareCIM 部署到 Alibaba 云 - 方式 2

1. 运行“SoftwareCIMInstaller.exe”，将 SoftwareCIM 安装在本地 PC 上。
2. 安装成功后，打开 SoftwareCIM 安装文件夹。
3. “SoftwareCIMLocalInstaller.exe”位于“...SIMATIC SoftwareCIM -> resources -> update”路径中，并通过 RDP 发送到虚拟 PC 中。



4. 双击“SoftwareCIMLocalInstaller.exe”，在虚拟 PC 上安装 SoftwareCIM。
5. 登录 SoftwareCIM。
6. 在“网络设置”(Network Settings) 页面的“高级设置”(Advance Setting) 中，启用“通过 WAN 访问 SoftwareCIM”(Accessing SoftwareCIM via WAN)，并在“主机名”(Host Name) 中填入弹性 IP 地址。单击“保存更改”(Save changes)。

   现在，可使用弹性 IP 地址安全访问 SoftwareCIM。

说明

仅当在“主机名”(Host Name) 中填入弹性 IP 时，所部署的 SoftwareCIM 才会配置为 SGLAN 服务器。

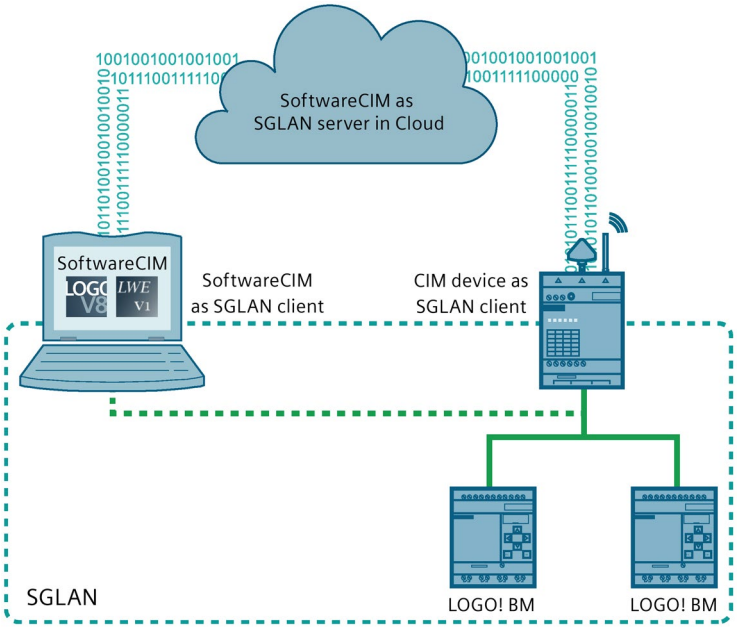
实例

8

8.1 将程序远程下载到 LOGO! BM

本实例展示了如何通过 SGLAN 将程序远程下载到 LOGO! BM。用户将了解如何将 SoftwareCIM 作为 SGLAN 服务器部署到 Alibaba 云，以及如何将 SGLAN 客户端连接到该 SGLAN 服务器。

下图演示了此类系统的运行方式：



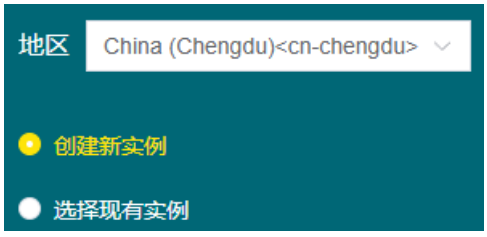
要求

- 要安装 SoftwareCIM 的 PC 必须满足以下要求：
  - 可以访问 Internet
  - 安有 Windows 10（64 位）（21H2、22H2）或 Windows 11 (22H2) 操作系统
- 有效的 Alibaba 云帐户
- SGLAN 中的所有设备和 SoftwareCIM 的 IP 位于同一子网，且不相互冲突
- 要配置为 SGLAN 客户端的 CIM 设备必须满足以下要求：
  - 具有 IoT 或 SIM 卡，可以访问 Interent，并具有 IPv4 地址

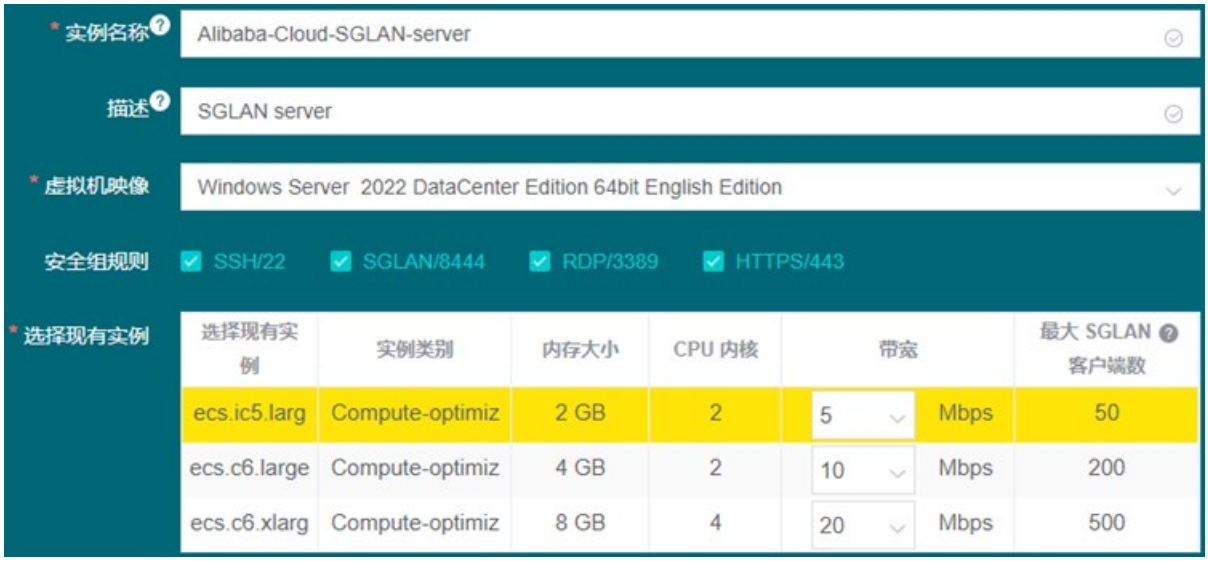
在 Alibaba 云上设置 SGLAN 服务器

1. 运行"SoftwareCIMInstaller.exe"，选择将 SoftwareCIM 部署到 Alibaba 云。
2. 输入"访问密钥 ID"(Access Key ID) 和"秘密访问密钥"(Secret Access Key)，以登录 Alibaba 云。单击"下一步"(Next)。

3. 选择"区域"(Region)。选择"创建新实例"(Create a new instance)。单击"下一步"(Next)。



4. 输入“实例名称”(Instance Name) 和“描述”(Description)；选择“虚拟机映像”(Machine Image)、“安全组规则”(Security Group Rule) 和“实例类型”(Instance Type)。单击“下一步”(Next)。

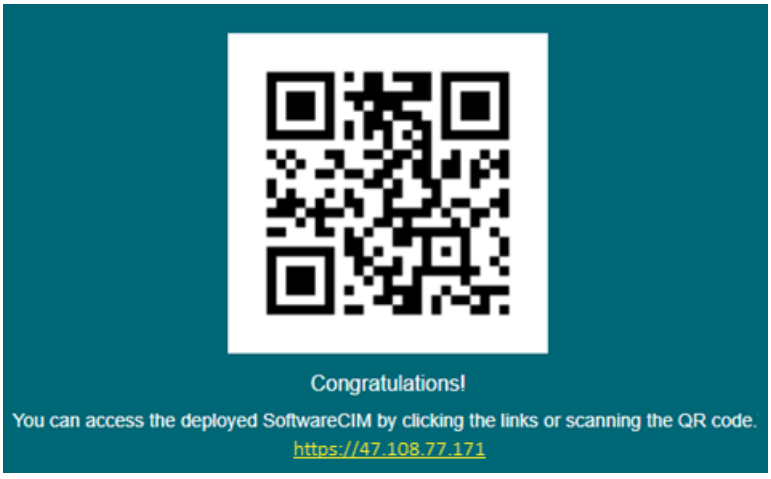


5. 单击“跳过”(Skip) 并接受使用默认的西门子证书。

6. 设置 Windows 帐户、SoftwareCIM 帐户和 SGLAN 帐户的密码。

7. 单击“部署”(Deploy) 开始部署。

部署成功后，窗口中显示一个二维码和一个链接。系统默认将部署的 SoftwareCIM 配置为 SGLAN 服务器。保存二维码或链接，以供以后使用。在这种情况下，SGLAN 服务器的公共 IP 是 47.108.77.171。保存公共 IP，将 SGLAN 客户端连接到 SGLAN 服务器时将使用此 IP。



在 PC 上将 SoftwareCIM 设置为 SGLAN 客户端

1. 在 PC 上运行“SoftwareCIMInstaller.exe”，并选择“安装到这台 PC”(Install on this PC)。
2. 在登录页面输入密码即可登录 SoftwareCIM。默认密码是 cim。
3. 转入 SGLAN 页面，启用“SoftwareCIM 作为 SGLAN 客户端”(SoftwareCIM as SGLAN Client)。
4. 在“远程主机模式”(Remote Host Mode) 中选择 IPv4。
5. 在“远程主机”(Remote Host) 中输入服务器的 IPv4 地址。IP 地址是 47.108.77.171。
6. 输入“服务器密码”(Server Password)。密码是将 SoftwareCIM 部署到云上时设置的 SGLAN 帐户密码。
7. 单击“保存更改”(Save changes)。

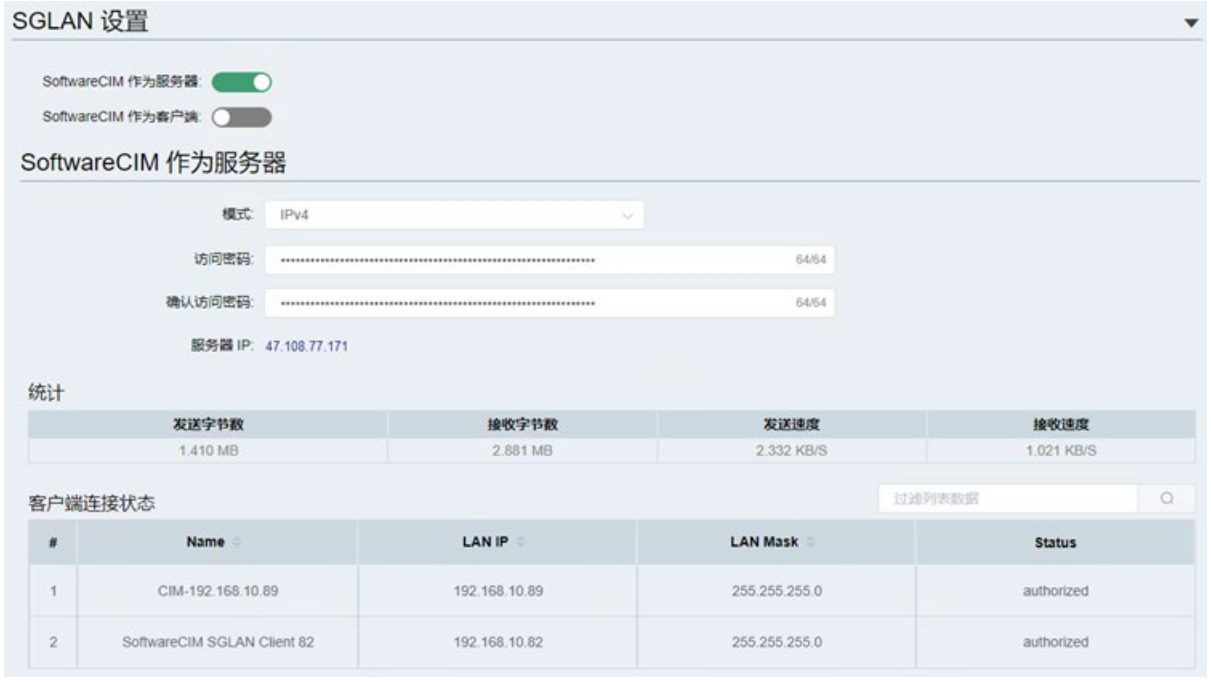
将 CIM 设备设置为 SGLAN 客户端

1. 访问 CIM 设备的基于 Web 的配置页面并登录。该配置页面与 SoftwareCIM 配置页面不同。
2. 检查蜂窝网络状态。
3. 转入 SGLAN 页面，启用“CIM 作为 SGLAN 客户端”(CIM as SGLAN Client)。

4. 在"远程主机模式"(Remote Host Mode) 中选择 IPv4。
5. 在"远程主机"(Remote Host) 中输入服务器的 IPv4 地址。IP 地址是 47.108.77.171。
6. 输入"服务器密码"(Server Password)。密码是将 SoftwareCIM 部署到云上时设置的 SGLAN 帐户密码。
7. 单击"保存更改"(Save changes)。

检查客户端与服务器的连接状态

1. 通过部署后保存的链接，转至 Alibaba 云上 SoftwareCIM 基于 Web 的配置平台。
2. 登录配置平台。
3. 转至 SGLAN 页面。可在此处查看 SGLAN 客户端连接状态。



将程序下载到 LOGO! BM

1. 在 PC 中输入 ping 命令，测试与远程 LOGO! BM 的连接。
2. 在安装有 LOGO!Soft Comfort 的 PC 上打开该程序，然后单击“下载”(Download)。

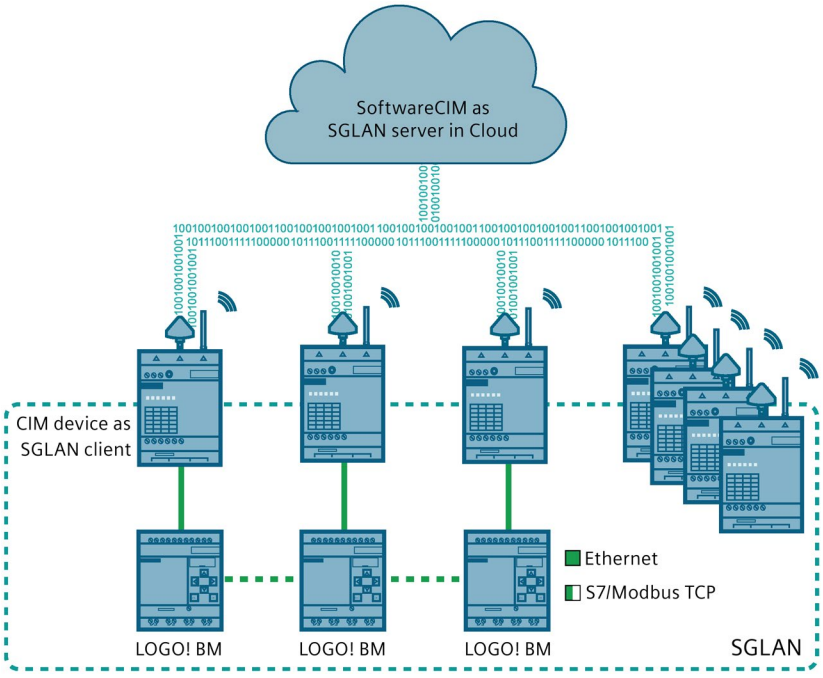
3. 将通信接口设为“SGLAN 虚拟适配器”(SGLAN Virtual Adapter)。

4. 在“可访问的 LOGO”(Accessible LOGO) 中选择目标 LOGO! BM，并单击“确定”(OK)。

8.2 在两个 LOGO! BM 之间交换数据

该实例展示了如何通过 SGLAN 在位置不同的两个 LOGO! BM 之间交换数据。

下图演示了此类系统的运行方式：



要求

- 有效的 AWS 云帐户
- SGLAN 中所有设备和 SoftwareCIM 的 IP 位于同一子网，且不相互冲突。
- 要配置为 SGLAN 客户端的 CIM 设备必须满足以下要求：
  - 具有 IoT 或 SIM 卡，可以访问 Interent，并具有 IPv4 地址

在 AWS 云上设置 SGLAN 服务器

1. 运行“SoftwareCIMInstaller.exe”，并选择将 SoftwareCIM 部署到 AWS 云。
2. 输入“访问密钥 ID”(Access Key ID) 和“秘密访问密钥”(Secret Access Key)，以登录 AWS 云。单击“下一步”(Next)。
3. 选择“区域”(Region)。选择“创建新实例”(Create a new instance)。单击“下一步”(Next)。
4. 输入“实例名称”(Instance Name) 和“描述”(Description)；选择“虚拟机映像”(Machine Image) 和“实例类型”(Instance Type)。单击“下一步”(Next)。

5. 单击“跳过”(Skip) 并接受使用默认的西门子证书。
6. 设置 Windows 帐户、SoftwareCIM 帐户和 SGLAN 帐户的密码。
7. 单击“部署”(Deploy) 开始部署。

部署成功后，窗口中显示一个二维码和两个链接。部署的 SoftwareCIM 默认配置为 SGLAN 服务器。保存二维码或链接，以供以后使用。在这种情况下，SGLAN 服务器的公共 IP 是 3.98.107.40。保存公共 IP，将 SGLAN 客户端连接到 SGLAN 服务器时将使用此 IP。

设置 SGLAN 客户端

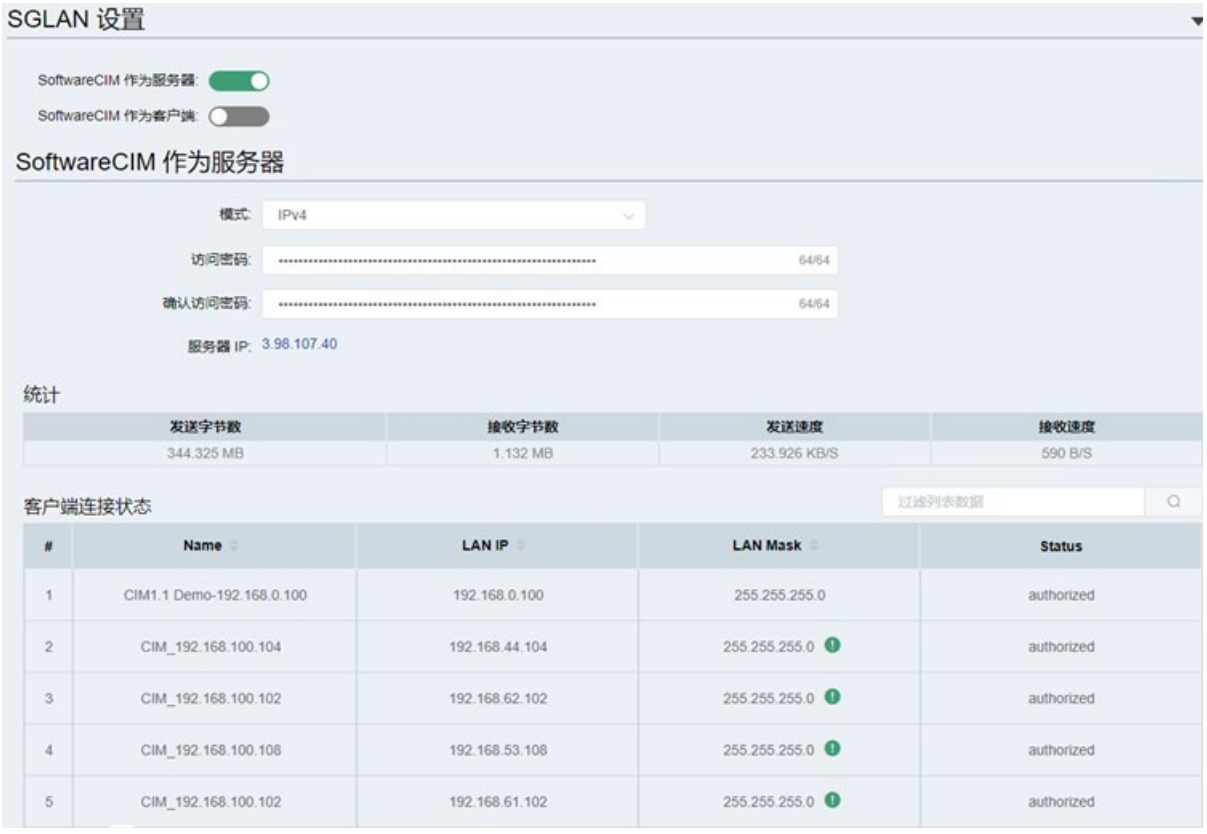
1. 访问 CIM 设备 1 的基于 Web 的配置页面并登录。该配置页面与 SoftwareCIM 配置页面不同。
2. 检查蜂窝网络状态。
3. 转入 SGLAN 页面，启用“CIM 作为 SGLAN 客户端”(CIM as SGLAN Client)。
4. 在“远程主机模式”(Remote Host Mode) 中选择 IPv4。
5. 在“远程主机”(Remote Host) 中输入服务器的 IPv4 地址。IP 地址是 3.98.107.40。

6. 输入“服务器密码”(Server Password)。密码是将 SoftwareCIM 部署到云时设置的 SGLAN 帐户密码。
7. 单击“保存更改”(Save changes)。

重复上述步骤，将 CIM 设备 2 设置为 SGLAN 客户端。

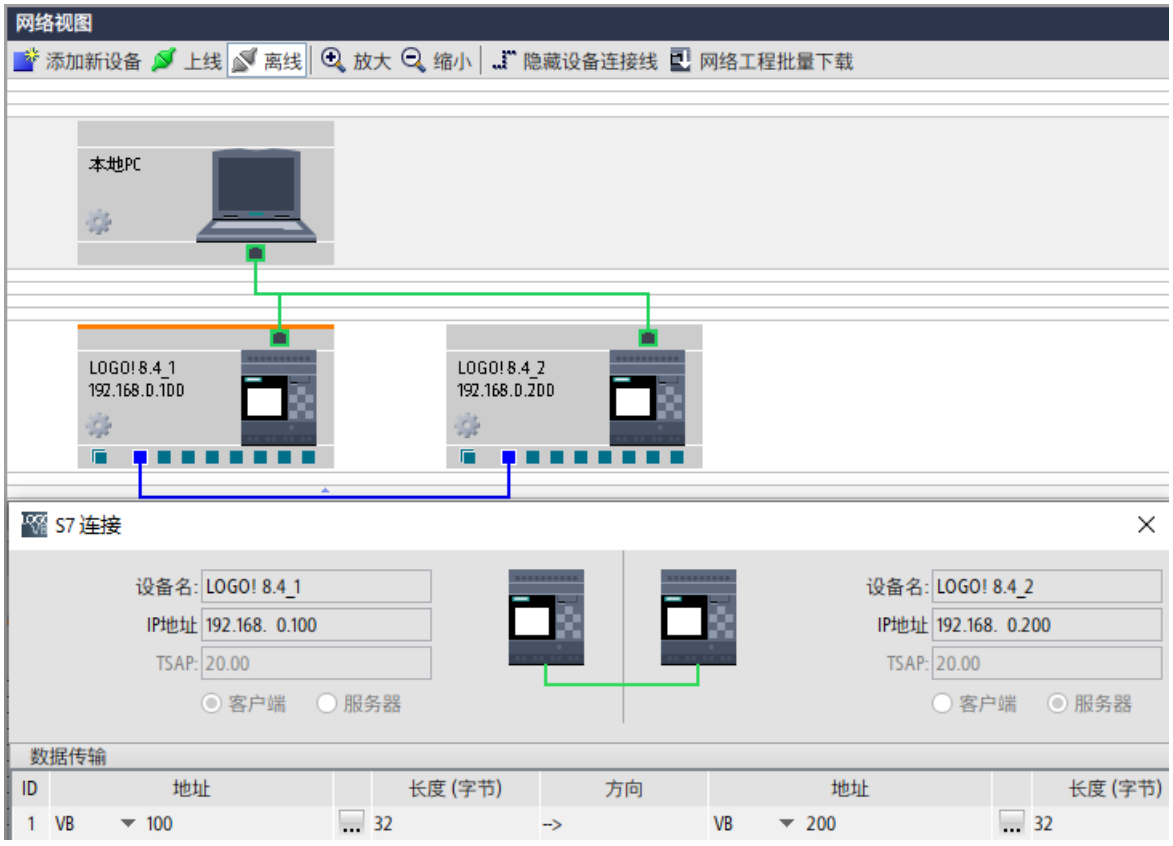
检查客户端与服务器的连接状态

1. 通过部署后保存的链接，转到 AWS 云上 SoftwareCIM 的基于 Web 的配置平台。
2. 登录配置平台。
3. 转至 SGLAN 页面。可在此处查看 SGLAN 客户端连接状态。



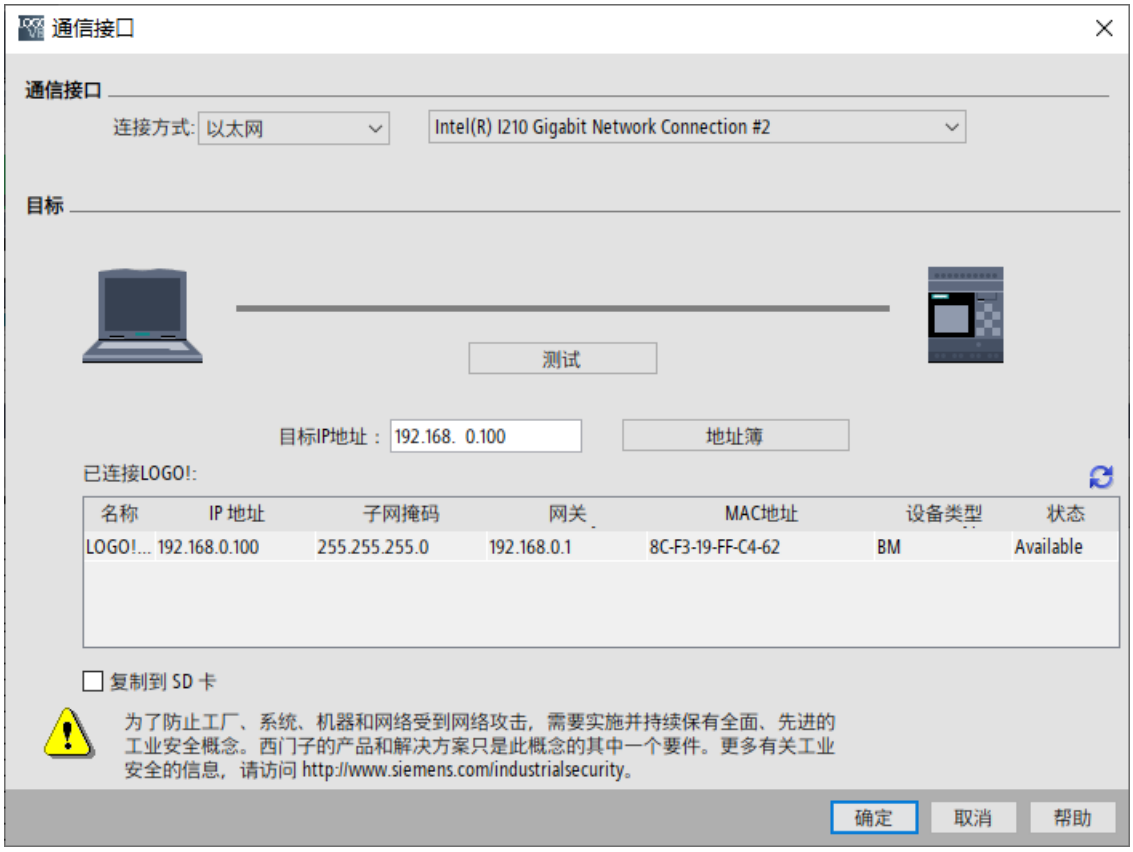
在两个 LOGO! BM 之间交换数据

1. 在 PC 1 上通过 LOGO!Soft Comfort 打开要下载的程序。
2. 设置通过 S7 连接进行数据传输。

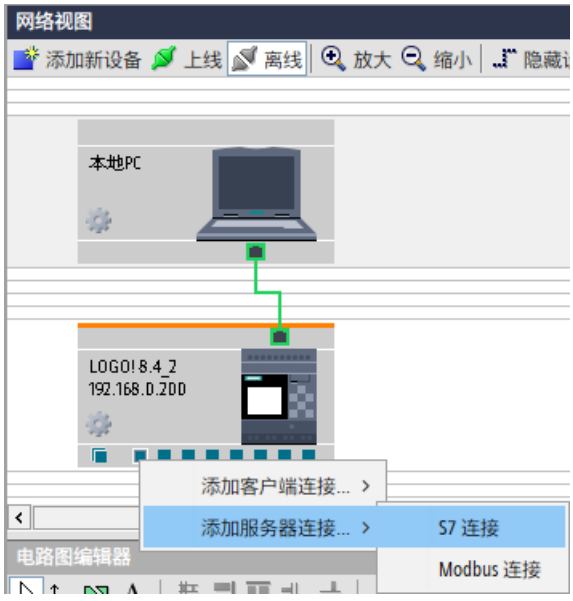


3. 单击“下载”(Download)，选择连接到 CIM 设备 1 的本地适配器作为接口。

4. 在“可访问的 LOGO”(Accessible LOGO) 中选择 LOGO! BM 1，单击“确定”(OK)。



5. 在 PC 2 上通过 LOGO!Soft Comfort 打开要下载的程序，添加服务器连接，并为 LOGO! BM 2 选择 S7 连接。



6. 在 S7 连接配置窗口中，选择“接受服务器端的所有连接请求”(Accept all connection request in server side)。然后单击“下载”(Download)。

7. 选择连接到 CIM 设备 2 的本地适配器作为接口。
8. 在“可访问的 LOGO”(Accessible LOGO) 中选择 LOGO! BM 2，单击“确定”(OK)。
9. 在 PC 1 上打开 LOGO!Soft Comfort，然后在“数据表”(Data Table) 中输入 LOGO! BM 地址的新值。

10. 在 PC 2 上打开 LOGO!Soft Comfort，检查数据是否传输到 LOGO! BM 2。

ID	地址	类型	数值	新值
1	VB200	有符号	+1	
2	VB201	有符号	+2	
3	VB202	有符号	+3	
4	VB203	有符号	+4	
5	VB204	有符号	+5	
6				

索引

H

P

B

J

T

M

D

S H