

SIEMENS

SIMATIC

SoftwareCIM

Instructions de service

<u>Sécurité</u>	1
<u>Introduction</u>	2
<u>Installation de SoftwareCIM</u>	3
<u>Configuration de SoftwareCIM</u>	4
<u>Mise à jour de SoftwareCIM</u>	5
<u>Dépannage de SoftwareCIM</u>	6
<u>Conseils et astuces</u>	7
<u>Exemple pratique</u>	8

Mentions légales

Signalétique d'avertissement

Ce manuel donne des consignes que vous devez respecter pour votre propre sécurité et pour éviter des dommages matériels. Les avertissements servant à votre sécurité personnelle sont accompagnés d'un triangle de danger, les avertissements concernant uniquement des dommages matériels sont dépourvus de ce triangle. Les avertissements sont représentés ci-après par ordre décroissant de niveau de risque.

 DANGER
signifie que la non-application des mesures de sécurité appropriées entraîne la mort ou des blessures graves.
 ATTENTION
signifie que la non-application des mesures de sécurité appropriées peut entraîner la mort ou des blessures graves.
 PRUDENCE
signifie que la non-application des mesures de sécurité appropriées peut entraîner des blessures légères.
IMPORTANT
signifie que la non-application des mesures de sécurité appropriées peut entraîner un dommage matériel.

En présence de plusieurs niveaux de risque, c'est toujours l'avertissement correspondant au niveau le plus élevé qui est reproduit. Si un avertissement avec triangle de danger prévient des risques de dommages corporels, le même avertissement peut aussi contenir un avis de mise en garde contre des dommages matériels.

Personnes qualifiées

L'appareil/le système décrit dans cette documentation ne doit être manipulé que par du **personnel qualifié** pour chaque tâche spécifique. La documentation relative à cette tâche doit être observée, en particulier les consignes de sécurité et avertissements. Les personnes qualifiées sont, en raison de leur formation et de leur expérience, en mesure de reconnaître les risques liés au maniement de ce produit / système et de les éviter.

Utilisation des produits Siemens conforme à leur destination

Tenez compte des points suivants:

 ATTENTION
Les produits Siemens ne doivent être utilisés que pour les cas d'application prévus dans le catalogue et dans la documentation technique correspondante. S'ils sont utilisés en liaison avec des produits et composants d'autres marques, ceux-ci doivent être recommandés ou agréés par Siemens. Le fonctionnement correct et sûr des produits suppose un transport, un entreposage, une mise en place, un montage, une mise en service, une utilisation et une maintenance dans les règles de l'art. Il faut respecter les conditions d'environnement admissibles ainsi que les indications dans les documentations afférentes.

Marques de fabrique

Toutes les désignations repérées par ® sont des marques déposées de Siemens Aktiengesellschaft. Les autres désignations dans ce document peuvent être des marques dont l'utilisation par des tiers à leurs propres fins peut enfreindre les droits de leurs propriétaires respectifs.

Exclusion de responsabilité

Nous avons vérifié la conformité du contenu du présent document avec le matériel et le logiciel qui y sont décrits. Ne pouvant toutefois exclure toute divergence, nous ne pouvons pas nous porter garants de la conformité intégrale. Si l'usage de ce manuel devait révéler des erreurs, nous en tiendrons compte et apporterons les corrections nécessaires dès la prochaine édition.

Sommaire

1	Sécurité.....	5
1.1	Notes relatives à la cybersécurité.....	5
1.2	Protection des données.....	5
1.3	Remarque concernant la sécurité	6
2	Introduction	7
2.1	Fonctions.....	7
2.2	Modèle de données universel.....	8
2.3	SGLAN	10
2.4	Compatibilité	10
3	Installation de SoftwareCIM	11
3.1	Installation de SoftwareCIM sur un PC local	11
3.2	Déploiement de SoftwareCIM sur le cloud	11
3.2.1	Déploiement sur AWS	12
3.2.2	Déploiement sur Alibaba	20
3.2.3	Dépannage de SoftwareCIM cloud deployment	28
4	Configuration de SoftwareCIM	29
4.1	Présentation de l'interface utilisateur.....	29
4.2	À propos de	32
4.3	Paramètres réseau	33
4.4	Paramètres SGLAN	34
4.4.1	Configuration du serveur SGLAN	34
4.4.2	Configuration du client SGLAN	35
4.5	Gestion des données.....	38
4.5.1	Variables.....	38
4.5.2	Associations de données	39
4.5.3	Surveillance en ligne.....	42
4.6	Paramètres des protocoles	43
4.6.1	S7.....	43
4.6.2	Modbus TCP.....	47
4.6.3	Modbus RTU	51
4.6.4	API RESTful	53
4.7	Paramètres de sécurité.....	56
4.7.1	Protocole	56
4.7.2	Certificats	57
4.7.2.1	Certificats détenus :	57
4.7.2.2	Certificat de confiance :	60

4.8	Paramètres système.....	62
4.8.1	Paramètres de l'heure	62
4.8.2	Changer le mot de passe.....	63
4.8.3	Réinitialisation du système.....	63
4.8.4	Gestion de la configuration système.....	64
5	Mise à jour de SoftwareCIM	65
5.1	Mise à jour en installant le pack de mise à jour	65
5.2	Mise à jour avec la configuration SoftwareCIM	65
6	Dépannage de SoftwareCIM.....	68
7	Conseils et astuces	70
7.1	Comment déployer manuellement SoftwareCIM sur AWS	70
7.2	Comment déployer manuellement SoftwareCIM sur Alibaba.....	79
8	Exemple pratique	84
8.1	Télécharger un programme à distance sur LOGO! BM	84
8.2	Échanger des données entre deux LOGO! BM	91
	Index.....	99

1.1 Notes relatives à la cybersécurité

Siemens commercialise des produits et solutions comprenant des fonctions de cybersécurité industrielle qui contribuent à une exploitation sûre des installations, systèmes, machines et réseaux.

Pour protéger les installations, systèmes, machines et réseaux des cybermenaces, il est recommandé de mettre en œuvre un concept de cybersécurité industrielle intégré (et continuellement mis à jour) qui corresponde à l'état actuel de la technique. Les produits et solutions de Siemens constituent une partie de ce concept.

Il incombe aux clients d'empêcher tout accès non autorisé à ses installations, systèmes, machines et réseaux. Ces systèmes, machines et composants doivent uniquement être connectés au réseau d'entreprise ou à Internet si et dans la mesure où cela est nécessaire et seulement si des mesures de protection adéquates (ex : pare-feu et/ou segmentation du réseau) ont été prises.

Pour plus d'informations sur les mesures de cybersécurité industrielle possibles, voir sous (<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>).

Les produits et solutions Siemens font l'objet de développements continus pour être encore plus sûrs. Siemens recommande vivement d'effectuer des mises à jour dès que celles-ci sont disponibles et d'utiliser la dernière version des produits. L'utilisation de versions qui ne sont plus prises en charge et la non-application des dernières mises à jour peut augmenter le risque de cybermenaces pour nos clients.

Pour être informé sur les mises à jour produit dès leur sortie, s'abonner au flux RSS Siemens Industrial Cybersecurity sur (<https://new.siemens.com/global/en/products/services/cert.html>) :

1.2 Protection des données

Siemens respecte les recommandations en matière de protection des données, en particulier les exigences de minimisation des données (respect de la vie privée dès la conception). Cela présente les implications suivantes pour ce produit : le produit ne traite pas / n'enregistre pas d'informations personnelles, mais uniquement des données fonctionnelles techniques (horodatages, par exemple). Si l'utilisateur associe ces données à d'autres données (par exemple, planification d'équipes) ou si l'utilisateur enregistre des informations personnelles sur le même support (disque dur, par exemple) et crée ainsi une référence personnelle dans le processus, c'est à lui d'assurer le respect des recommandations en matière de protection des données.

1.3 Remarque concernant la sécurité

Remarque

Remarques sur la protection des comptes d'administrateur

Un utilisateur avec des droits d'administrateur dispose de nombreuses options d'accès et de manipulation pour le système.

Par conséquent, assurez-vous qu'il existe des mesures de protection adéquates pour protéger les comptes d'administrateur afin d'empêcher les modifications non autorisées. Pour ce faire, utilisez des mots de passe sécurisés et un compte d'utilisateur standard pour le fonctionnement normal. D'autres mesures, telles que l'utilisation de stratégies de sécurité, doivent être appliquées selon les besoins.

Remarque

Pour protéger SoftwareCIM contre toute manipulation indésirable si votre PC devait faire l'objet d'attaques malveillantes via Internet, Siemens recommande vivement d'installer un outil de gestion de listes vertes sur le PC. Utilisez l'outil ensuite pour gérer le logiciel installé sur votre PC.

Respectez des consignes de sécurité suivantes pour éviter tout accès non autorisé au système.

Mot de passe

- Mettez à jour les mots de passe régulièrement pour renforcer la sécurité du système
- Utilisez uniquement des mots de passe forts
- Assurez-vous que les mots de passe sont protégés et inaccessibles aux personnes non autorisées.
- N'utilisez pas le même mot de passe pour plusieurs utilisateurs et systèmes.

Protocole

- Activez uniquement les protocoles requis par le système

Introduction

2.1 Fonctions

SoftwareCIM vous offre une meilleure solution de connexion réseau avec une fonctionnalité élargie.

Fonctions de base

SoftwareCIM prend en charge les fonctions suivantes :

- Modèle UDM (Universal Data Model)

Le modèle UDM fait office de centre de données pour SoftwareCIM et vous pouvez échanger des données via UDM à l'aide de protocoles pris en charge.

- SGLAN (Secured Global Local Area Network - réseau local global sécurisé)

Les appareils distribués dans le même SGLAN peuvent communiquer entre eux.

- Configuration de SoftwareCIM

Les configurations suivantes sont disponibles :

- Configurer LAN, WAN ou SGLAN sur SoftwareCIM
- Configurer les variables et associations de données
- Modifier et surveiller les variables
- Configurer les protocoles pris en charge
- Configurer les fonctions de sécurité comme la gestion des certificats
- Fonctions de maintenance telles que redémarrage du système ou réinitialisation aux paramètres d'usine

- Passerelle de protocole

Tous les appareils dans SGLAN peuvent communiquer avec SoftwareCIM au moyen d'un protocole S7/Modbus basé sur le modèle UDM (Universal Data Model).

Une application peut accéder aux données via l'API RESTful sur SoftwareCIM sur la base du modèle UDM.

- Gestion des données

Le SoftwareCIM peut exécuter une action lorsqu'un événement configuré est déclenché. Par exemple, une modification dans le modèle UDM.

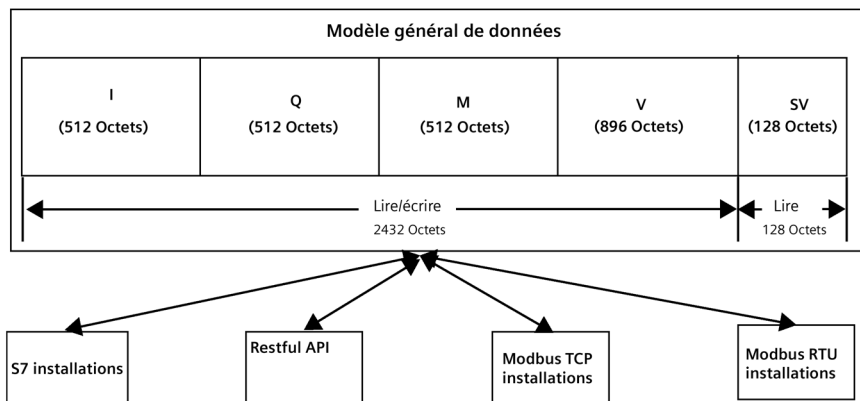
- Serveur de temps
 - SoftwareCIM peut faire office de serveur NTP pour fournir l'heure aux clients NTP.
 - SoftwareCIM peut activer/désactiver le mappage de l'heure sur UDM. Les clients SGLAN sans NTP peuvent obtenir l'heure via le multiprotocole ou l'API RESTful.
- Gestion des certificats
 - Certificat détenu : générer et sélectionner un certificat pour configurer un serveur web sécurisé et un serveur SGLAN ; SoftwareCIM prend également en charge le chargement de vos propres certificats de confiance afin de construire une stratégie de sécurité personnalisée.
 - Certificat approuvé : sélectionner le certificat pour configurer le client SGLAN.

2.2 Modèle de données universel

Le modèle de données universel (UDM) permet aux API compatibles de mapper leurs données de processus sur ce modèle même s'ils utilisent des protocoles de communication différents. Le modèle UDM fait office de centre de données pour SoftwareCIM et des protocoles différents peuvent échanger des données par le biais du modèle UDM.

Remarque

Le modèle UDM utilise le format "Little Endian" pour stocker les types de données à plusieurs octets.



Le modèle de données I, Q, M, V simule la mémoire image du processus dans un automate programmable.

Règle de nommage pour l'adresse UDM : type d'adresse + type de données court + adresse de début. Pas d'alignement sur les octets, par exemple VW3 correspond au mot constitué des octets 3 et 4 dans la zone V.

L'adresse UDM n'est pas sensible à la casse.

Type de données (type de données court)	Longueur	Plage de valeurs	I (512 octets)	Q (512 octets)	M (512 octets)	V (écriture : 896 octets ; lecture : 1024 octets)	
bool (x)	1 bit	0 ~ 1	0.0-511.7	0.0-511.7	0.0-511.7	0.0-895.7	0.0-1023.7
byte (b)	8 bits	0 ~ FF	0-511	0-511	0-511	0-895	0-1023
word (w)	16 bits	0 ~ FFFF	0-510	0-510	0-510	0-894	0-1022
double-word (dw)	32 bits	0 ~ FFFFFFFF	0-508	0-508	0-508	0-892	0-1020
long-word (lw)	64 bits	0 ~ FFFFFFFFFFFFFFFF	0-504	0-504	0-504	0-888	0-1016
short-int (si)	8 bits	-128 ~ 127	0-511	0-511	0-511	0-895	0-1023
int (i)	16 bits	-32768 ~ 32767	0-510	0-510	0-510	0-894	0-1022
double-int (di)	32 bits	-2147483648 ~ 2147483647	0-508	0-508	0-508	0-892	0-1020
long-int (li)	64 bits	-9223372036854775808 ~ 9223372036854775807	0-504	0-504	0-504	0-888	0-1016
real (r)	32 bits	-3.4E38 ~ +3.4E38	0-508	0-508	0-508	0-892	0-1020
long-real (lr)	64 bits	-1.797E308 ~ +1.797E308	0-504	0-504	0-504	0-888	0-1016
short-unsigned (su)	8 bits	0 ~ 255	0-511	0-511	0-511	0-895	0-1023
unsigned (u)	16 bits	0 ~ 65535	0-510	0-510	0-510	0-894	0-1022
double-unsigned (du)	32 bits	0 ~ 4294967295	0-508	0-508	0-508	0-892	0-1020
long-unsigned (lu)	64 bits	0 ~ 18446744073709551615	0-504	0-504	0-504	0-888	0-1016

Variable système

SV (pour "System Variable", variable système) permet de sauvegarder certaines données système, telles que l'heure, etc.

Élément	Type	Taille	Adresse	Plage	Unité	Commentaires	Exemple API RESTful
Temps							
Mémento valide	bool	1 bit	896.0	0 ou 1		Mémento valide pour la valeur de temps	/pi/rest/vx896.0
Horodatage UNIX	double unsigned	4 octets	897	0 ~ 4294967295	secondes	Heure actuelle, secondes depuis 1970-1-1 00:00:00 Unité : seconde	/pi/rest/vdu897
Année	unsigned	2 octets	901	1970 ~ 2106	années	Date actuelle, année	/pi/rest/vu901
Mois	short unsigned	1 octet	903	1 ~ 12	mois	Date actuelle, mois	/pi/rest/vsu903
Jour	short unsigned	1 octet	904	1 ~ 31	jours	Date actuelle, jour	/pi/rest/vsu904
Heures	short unsigned	1 octet	905	0 ~ 23	heures	Heure actuelle, heures	/pi/rest/vsu905

Élément	Type	Taille	Adresse	Plage	Unité	Commentaires	Exemple API RESTful
Minutes	short unsigned	1 octet	906	0 ~ 59	minutes	Heure actuelle, minutes	/pi/rest/vsu906
Secondes	short unsigned	1 octet	907	0 ~ 59	secondes	Heure actuelle, secondes	/pi/rest/vsu907

2.3 SGLAN

SGLAN (Secured Global Local Area Network - réseau local global sécurisé) vous permet de créer un réseau privé avec SoftwareCIM. SGLAN est la composante fondamentale de votre réseau privé. Les appareils du SGLAN peuvent communiquer entre eux en toute sécurité.

Rôles en SGLAN

Il existe deux rôles en SGLAN :

- **Serveur SGLAN** : le serveur SGLAN est le centre de commutation de données. Le serveur SGLAN est responsable de la transmission des données, de l'autorisation des demandes de liaison, du traitement des demandes de connexion et de déconnexion.

Remarque

Seul un appareil CIM ou SoftwareCIM peut fonctionner comme serveur SGLAN. Une fois SoftwareCIM déployé sur AWS ou Alibaba Cloud, le SoftwareCIM configuré comme serveur SGLAN peut connecter jusqu'à 500 clients SGLAN.

- **Client SGLAN** : tous les appareils dans SGLAN, y compris les clients SGLAN et les appareils du même réseau LAN avec des clients SGLAN peuvent communiquer entre eux. Le client SGLAN peut être un appareil CIM ou un SoftwareCIM.

Pour plus d'informations sur la configuration de SGLAN, voir Paramètres SGLAN (Page 34).

2.4 Compatibilité

Les systèmes d'exploitation suivants sont pris en charge :

- Windows 10 (64 bits) (21H2, 22H2)
- Windows 11 (22H2)

Installation de SoftwareCIM

3.1 Installation de SoftwareCIM sur un PC local

Procédez comme suit pour installer SoftwareCIM sur votre PC local :

1. Double-cliquez sur le programme d'installation "SoftwareCIMInstaller.exe".
2. Vérifiez les clauses de la licence et cliquez sur "Accepter" pour continuer.
3. Sélectionnez "Installer sur ce PC" et cliquez sur "Suivant".



4. Choisissez le chemin d'installation et cliquez sur "Suivant".
5. Chargez le fichier de certificat et le fichier de clé privée. Cliquez ensuite sur "Installer". Vous pouvez également cliquer sur "Ignorer" pour utiliser le certificat Siemens par défaut.
6. L'installation est terminée.

3.2 Déploiement de SoftwareCIM sur le cloud

Une fois le déploiement sur le cloud terminé, le SoftwareCIM est configuré par défaut comme serveur SGLAN. Le serveur SGLAN peut connecter jusqu'à 500 clients SGLAN. Si vous voulez configurer le SoftwareCIM déployé comme client SGLAN, vous pouvez modifier les réglages sur les pages de configuration de SoftwareCIM.

Les clouds suivants sont pris en charge pour le déploiement de SoftwareCIM :

- Déploiement sur AWS (Page 12)
- Déploiement sur Alibaba (Page 20)

Introduction au menu

Cliquez sur l'icône  pour ouvrir le menu de navigation. Le menu de navigation comprend l'entrée pour la page d'accueil, l'entrée pour la page de connexion au cloud, les informations sur la version du programme d'installation, le document d'aide et le fichier Lisezmoi OSS.

Cliquez sur l'icône  pour ouvrir le menu Langue.

3.2.1 Déploiement sur AWS

Conditions

Votre compte cloud AWS doit respecter les conditions minimales d'autorisation suivantes :

```
{
  "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": [
        "*"
      ]
    }
  ]
}
```

Pour plus d'informations sur les autorisations du compte cloud AWS, voir (https://docs.aws.amazon.com/fr_fr/AWSEC2/latest/UserGuide/dlm-access-control.html).

Pour modifier les autorisations du compte cloud AWS, voir (https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/id_users_change-permissions.html).

Pour créer un compte cloud AWS, voir (https://docs.aws.amazon.com/fr_fr/organizations/latest/userguide/orgs_manage_accounts_create.html).

Marche à suivre

Procédez comme suit pour déployer le SoftwareCIM sur le cloud AWS :

1. Double-cliquez sur le programme d'installation "SoftwareCIMInstaller.exe".
2. Vérifiez les clauses de la licence et cliquez sur "Accepter". Si vous cliquez "Annuler", le programme se termine.
3. Sélectionner "Déployer sur AWS Cloud", puis cliquez sur "Suivant".



4. Connectez-vous au cloud.
 - Saisissez l'"ID de clé d'accès".
 - Saisissez la "Clé d'accès secrète".
 - Saisissez le "Jeton de session" si vous vous connectez avec le compte d'identification temporaire d'AWS (TVM).

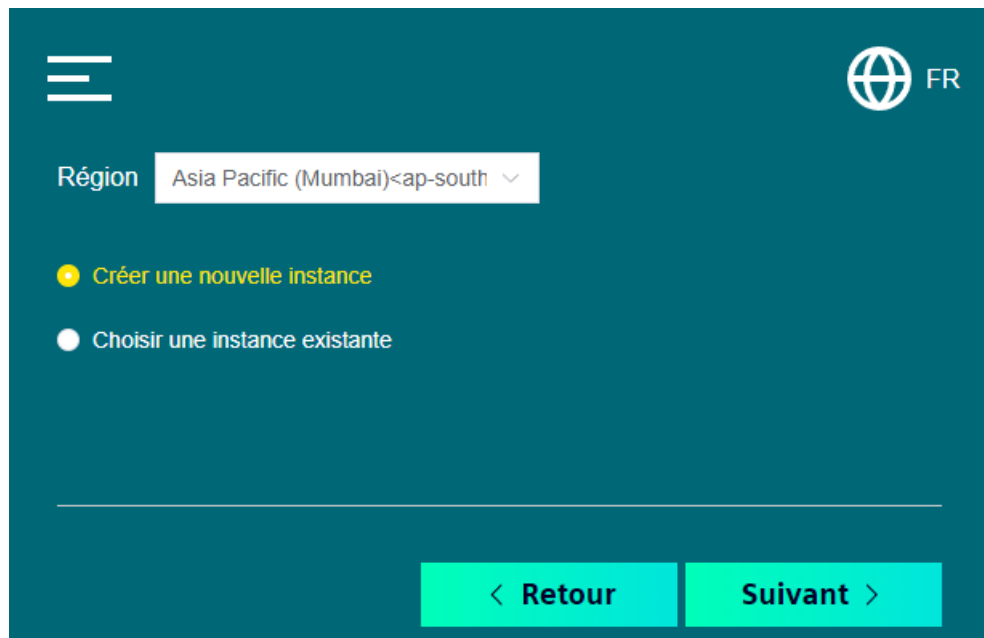
Cliquez sur le bouton "Suivant" pour continuer.



A dark blue form with three input fields. The first field is labeled '* ID de clé d'accès', the second '* Clé d'accès secrète', and the third 'Jeton de session'. At the bottom, there are two buttons: a red '< Retour' button and a grey 'Suivant >' button.

5. Sélectionnez "Région" pour l'instance.

- Si vous sélectionnez "Créer une nouvelle instance", cliquez sur le bouton "Suivant" pour passer à l'étape 6.
- Si vous sélectionnez "Choisir une instance existante", une table affiche toutes les instances en cours dans la région choisie. Si l'instance sélectionnée n'affiche aucun lien, cliquez sur le bouton "Suivant" pour passer à l'étape 7.
- Si l'instance sélectionnée affiche un lien, vous pouvez annuler le déploiement et accéder à SoftwareCIM à l'aide du lien.



A dark teal form. At the top left is a hamburger menu icon. At the top right is a globe icon with 'FR' next to it. Below the menu is a 'Région' label and a dropdown menu showing 'Asia Pacific (Mumbai)<ap-south >'. Below this are two radio button options: 'Créer une nouvelle instance' (selected) and 'Choisir une instance existante'. At the bottom, there are two red buttons: '< Retour' and 'Suivant >'.

6. Créez une instance.

- Saisissez un "Nom d'instance" ou utilisez le nom par défaut.
- Saisissez "Description" si besoin est.

Remarque

Limite de saisie pour le nom d'instance et la description

Vous pouvez faire glisser la souris sur le point d'interrogation pour plus de détails sur la limite de saisie pour "Nom d'instance" et "Description".

- Sélectionnez "Image de machine".
- Sélectionnez "Règle de groupe de sécurité".

Remarque

Sélection de la règle de groupe de sécurité

- SSH/22 : active l'accès au PC virtuel sur le cloud.
- SGLAN/8444 : active le SoftwareCIM déployé en tant que serveur SGLAN pour la connexion à des clients SGLAN.
- RDP/3389 : active la fonction de connexion Bureau à distance.
- HTTPS/443 : active l'accès aux pages de configuration du SoftwareCIM déployé à l'aide du navigateur web pris en charge.

Par défaut, toutes les règles de groupe de sécurité sont sélectionnées. Si vous désactivez une règle donnée, un message s'affiche pour rappeler que la fonction correspondante sera désactivée.

Les règles SSH/22 et SGLAN/8444 sont obligatoires. Si l'une ou l'autre est désactivée, vous ne pouvez pas poursuivre la configuration.

Vous pouvez également configurer ces règles sur la console AWS.

- Sélectionnez "Type d'instance".

Cliquez sur le bouton "Suivant" pour continuer.

Type d'instance	vCPUs	Architecture	Mémoire (Go)	Stockage (Go)	Type de stockage	Performance réseau	Prix à la demande (Windows)
t3.small	2	x86_64	2	--	--	Up to 5 Gigabit	0.04USD per Hour
c5.large	2	x86_64	4	--	--	Up to 10 Giga	0.18USD per Hour
c5.xlarge	4	x86_64	8	--	--	Up to 10 Giga	0.37USD per Hour

7. Chargez le certificat et le fichier de clé privée. Cliquez sur le bouton "Suivant" pour continuer.

Personnaliser le certificat

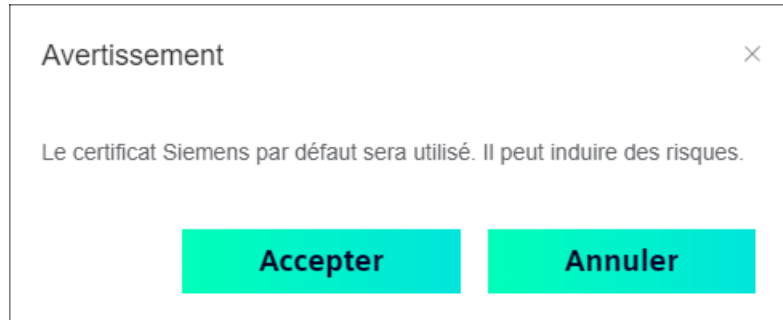
- Cette stratégie vous permet d'ajouter SoftwareCIM dans votre propre zone de confiance.
- Vous pouvez importer votre propre certificat et votre propre clé.
- Le type de paire de clés doit être : ecc256 / ecc384.

Certificat La taille de fichier ne peut pas dépasser 4000 octets.
Le type de paire de clés doit être ecc256 / ecc384.

Clé La taille de fichier ne peut pas dépasser 1000 octets.
Le type de paire de clés doit être ecc256 / ecc384.

< Retour Ignorer > Suivant >

Si vous cliquez sur "Ignorer", l'outil vous rappelle que le certificat Siemens par défaut sera utilisé.



Remarque

Pour des raisons de sécurité, Siemens vous recommande instamment de créer vos propres certificats, afin de créer votre zone de confiance personnelle.

8. Définissez un mot de passe en conséquence pour :

- Compte Windows : se connecter au PC virtuel sur le cloud.
- Compte SoftwareCIM : se connecter à SoftwareCIM. Le mot de passe peut être modifiée ultérieurement sur la page de configuration SoftwareCIM.
- Compte SGLAN : autoriser la connexion du client SGLAN au serveur SGLAN.

Si vous décidez de créer une nouvelle instance à l'étape 5, vous devez définir un mot de passe correspondant pour tous les comptes ci-dessus.

Si vous décidez d'utiliser une instance existante à l'étape 5, vous devez saisir le mot de passe correct du compte Windows pour vous connecter au PC virtuel sur le cloud. Vous devez ensuite saisir un mot de passe en conséquence pour le compte SoftwareCIM et le compte SGLAN.

Remarque

Le mot de passe par défaut du compte SGLAN est sglan.

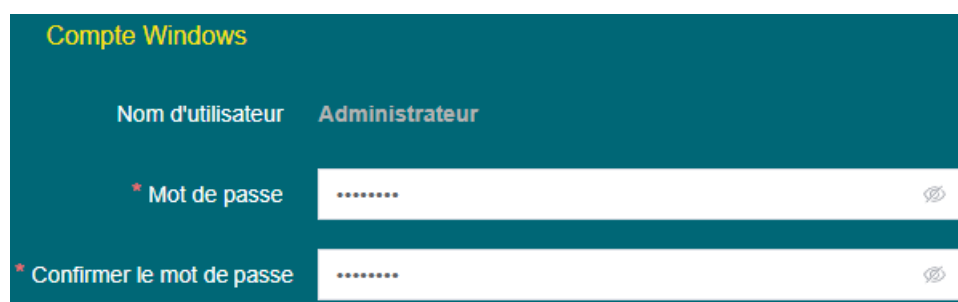
Le mot de passe par défaut du compte Windows est "Cim@1234".

Le mot de passe par défaut du compte SoftwareCIM est cim.

Remarque

Limite de saisie pour le mot de passe

Vous pouvez faire glisser la souris sur le point d'interrogation pour plus de détails sur la limite de saisie de tous les mots de passe.



Compte Windows

Nom d'utilisateur **Administrateur**

* Mot de passe [masked] ⓘ

* Confirmer le mot de passe [masked] ⓘ

9. Cliquez sur le bouton "Déployer".

La procédure prend généralement plus ou moins 10 minutes selon la région sélectionnée. Une fois qu'elle est terminée et si vous avez sélectionné la règle de groupe de sécurité HTTPS/443 à l'étape 6, la fenêtre affiche un QR code et des liens. Vous pouvez accéder aux pages de configuration de SoftwareCIM à l'aide du QR code ou de liens. Si vous n'avez pas sélectionné la règle de groupe de sécurité HTTPS/443, la fenêtre affiche uniquement l'IP publique de SoftwareCIM une fois le déploiement terminé.

Félicitations!
Veuillez enregistrer l'adresse IP ou le QR code pour une utilisation ultérieure en cas d'accès au SoftwareCIM déployé.



vous pouvez accéder au SoftwareCIM déployé en cliquant sur les liens ou en scannant le QR code. L'IP public est: 18.132.11.167

<https://18.132.11.167>

<https://ec2-18-132-11-167.eu-west-2.compute.amazonaws.com>

Remarques
1. Pour en savoir plus sur le déploiement de l'instance, voir <https://aws.amazon.com/console/>
2. Pour éviter une interruption de l'exploitation, assurez-vous que vous disposez de fonds suffisants sur votre compte.

3.2.2 Déploiement sur Alibaba

Conditions

Votre compte Alibaba Cloud doit respecter les conditions minimales d'autorisation suivantes :

```
{
  "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": "*"
  }
]
}

```

Pour modifier les autorisations de votre compte Alibaba Cloud, voir (<https://www.alibabacloud.com/help/en/resource-access-management/latest/grant-permissions-to-a-ram-role>).

Pour créer un compte Alibaba cloud, voir (<https://www.alibabacloud.com/help/en/analyticdb-for-mysql/getting-started/create-an-alibaba-cloud-account-2>).

Marche à suivre

Procédez comme suit pour déployer le SoftwareCIM sur Alibaba Cloud :

1. Double-cliquez sur le programme d'installation "SoftwareCIMInstaller.exe".
2. Vérifiez les clauses de la licence et cliquez sur "Accepter". Si vous cliquez "Annuler", le programme se termine.
3. Sélectionner "Déployer sur Alibaba Cloud", puis cliquez sur "Suivant".



4. Connectez-vous au cloud.
 - Saisissez l'"ID de clé d'accès".
 - Saisissez la "Clé d'accès secrète".
 - Saisissez le "Jeton de session" si vous vous connectez avec le compte d'identification temporaire (Temporary Credential Account, TVM) d'Alibaba.

Cliquez sur le bouton "Suivant" pour continuer.

A dark blue form with three input fields. The first field is labeled '* ID de clé d'accès', the second '* Clé d'accès secrète', and the third 'Jeton de session'. At the bottom, there are two buttons: a red '< Retour' button and a grey 'Suivant >' button.

* ID de clé d'accès

* Clé d'accès secrète

Jeton de session

< Retour Suivant >

5. Sélectionnez "Région" pour l'instance.

- Si vous sélectionnez "Créer une nouvelle instance", cliquez sur le bouton "Suivant" pour passer à l'étape 6.
- Si vous sélectionnez "Choisir une instance existante", une table affiche toutes les instances en cours dans la région choisie. Si l'instance sélectionnée n'affiche aucun lien, cliquez sur le bouton "Suivant" pour passer à l'étape 7.
- Si l'instance sélectionnée affiche un lien, vous pouvez annuler le déploiement et accéder à SoftwareCIM à l'aide du lien.

A dark teal form with a header containing a menu icon and a globe icon with 'FR'. Below the header is a 'Région' dropdown menu showing 'China (Chengdu)<cn-chengdu>'. There are two radio button options: 'Créer une nouvelle instance' (selected) and 'Choisir une instance existante'. At the bottom, there are two red buttons: '< Retour' and 'Suivant >'.

FR

Région China (Chengdu)<cn-chengdu> ▾

● Créer une nouvelle instance

● Choisir une instance existante

< Retour Suivant >

6. Créez une instance.

- Saisissez un "Nom d'instance" ou utilisez le nom par défaut.
- Saisissez "Description" si besoin est.

Remarque

Limite de saisie pour le nom d'instance et la description

Vous pouvez faire glisser la souris sur le point d'interrogation pour plus de détails sur la limite de saisie pour "Nom d'instance" et "Description".

- Sélectionnez "Image de machine".
- Sélectionnez "Règle de groupe de sécurité".

Remarque

Sélection de la règle de groupe de sécurité

- SSH/22 : active l'accès au PC virtuel sur le cloud.
- SGLAN/8444 : active le SoftwareCIM déployé en tant que serveur SGLAN pour la connexion à des clients SGLAN.
- RDP/3389 : active la fonction de connexion Bureau à distance.
- HTTPS/443 : active l'accès aux pages de configuration du SoftwareCIM déployé à l'aide du navigateur web pris en charge.

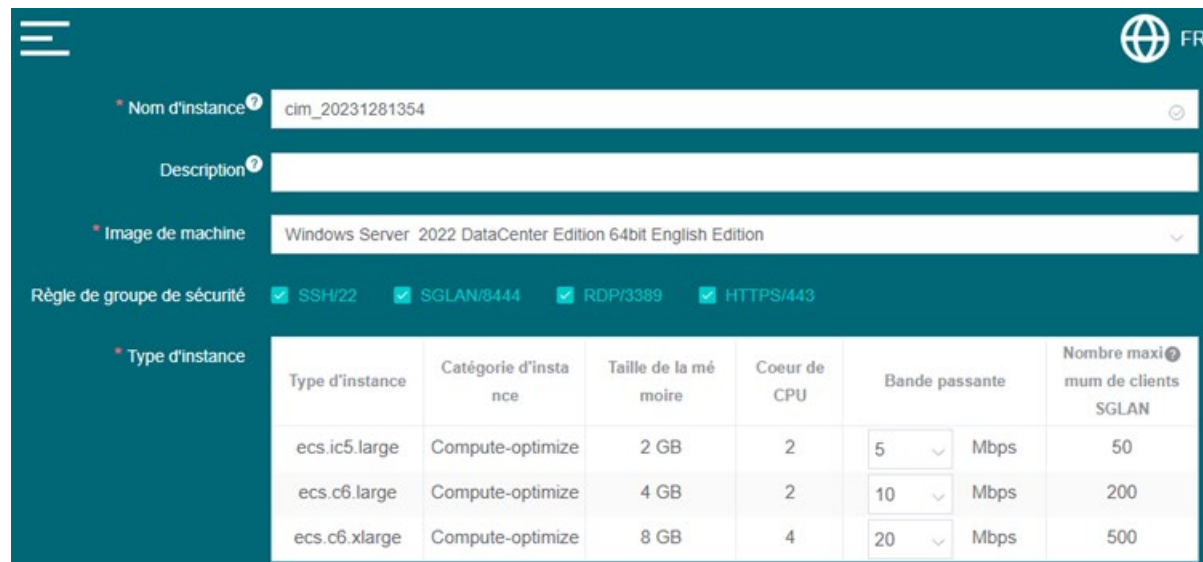
Par défaut, toutes les règles de groupe de sécurité sont sélectionnées. Si vous désactivez une règle donnée, un message s'affiche pour rappeler que la fonction correspondante sera désactivée.

Les règles SSH/22 et SGLAN/8444 sont obligatoires. Si l'une ou l'autre est désactivée, vous ne pouvez pas poursuivre la configuration.

Vous pouvez également configurer ces règles sur la console Alibaba.

- Sélectionnez "Type d'instance".

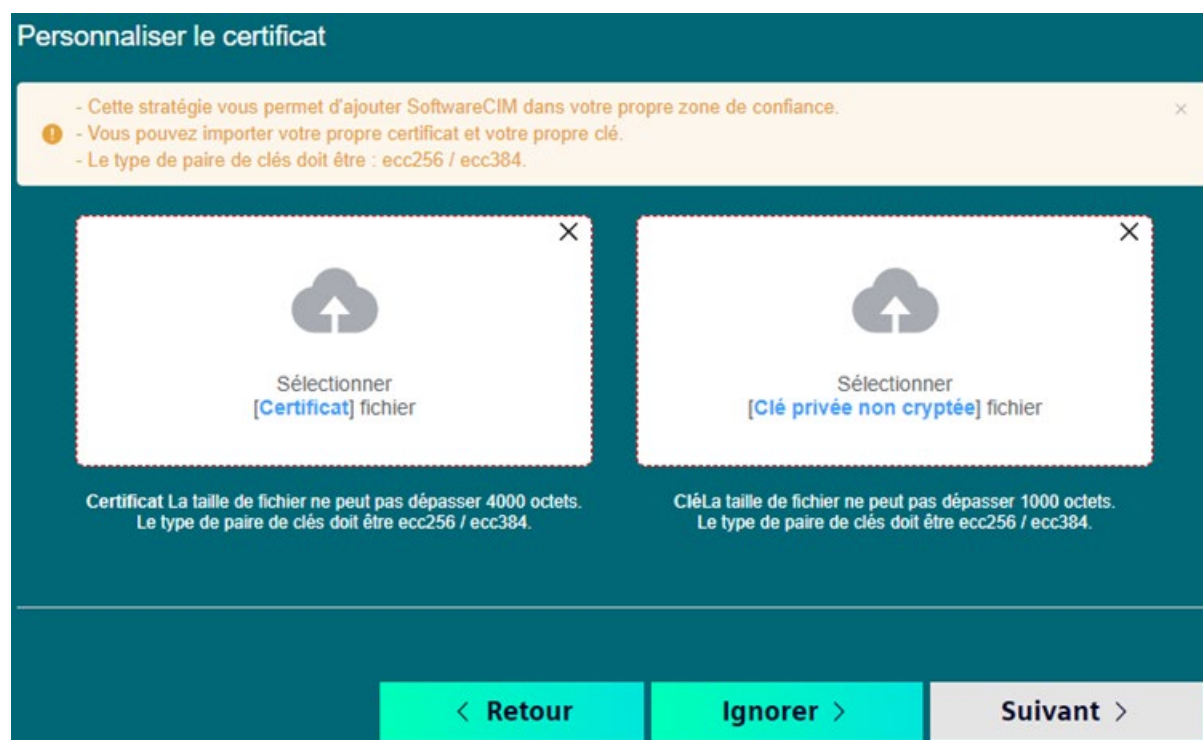
Cliquez sur le bouton "Suivant" pour continuer.



The screenshot shows a configuration page for a cloud instance. At the top, there's a header with a menu icon and 'FR'. Below it, the 'Nom d'instance' field is set to 'cim_20231281354'. The 'Description' field is empty. The 'Image de machine' dropdown is set to 'Windows Server 2022 DataCenter Edition 64bit English Edition'. Under 'Règle de groupe de sécurité', the checkboxes for SSH/22, SGLAN/8444, RDP/3389, and HTTPS/443 are all checked. The 'Type d'instance' section contains a table with three options:

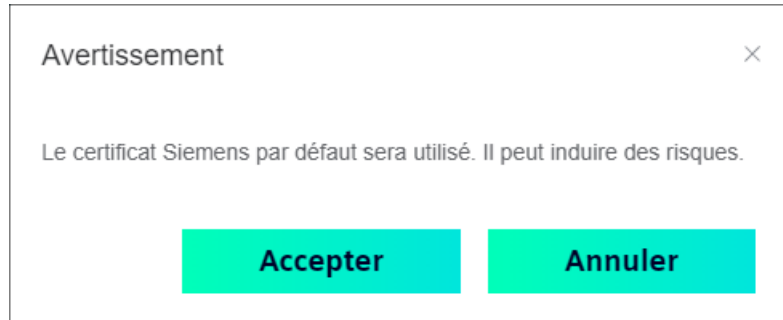
Type d'instance	Catégorie d'instance	Taille de la mémoire	Coeur de CPU	Bande passante	Nombre maximum de clients SGLAN
ecs.ic5.large	Compute-optimize	2 GB	2	5 Mbps	50
ecs.c6.large	Compute-optimize	4 GB	2	10 Mbps	200
ecs.c6.xlarge	Compute-optimize	8 GB	4	20 Mbps	500

7. Chargez le certificat et le fichier de clé privée. Cliquez sur le bouton "Suivant" pour continuer.



The screenshot shows the 'Personnaliser le certificat' step. At the top, there's a warning box with three points: 'Cette stratégie vous permet d'ajouter SoftwareCIM dans votre propre zone de confiance.', 'Vous pouvez importer votre propre certificat et votre propre clé.', and 'Le type de paire de clés doit être : ecc256 / ecc384.' Below this, there are two upload boxes. The left box is for the 'Certificat' (Certificate) and the right box is for the 'Clé privée non cryptée' (Unencrypted private key). Both boxes have a cloud icon with an upward arrow and the text 'Sélectionner [Certificat / Clé privée non cryptée] fichier'. Below each box, there's a note: 'Certificat La taille de fichier ne peut pas dépasser 4000 octets. Le type de paire de clés doit être ecc256 / ecc384.' and 'Clé La taille de fichier ne peut pas dépasser 1000 octets. Le type de paire de clés doit être ecc256 / ecc384.' At the bottom, there are three buttons: 'Retour', 'Ignorer', and 'Suivant'.

Si vous cliquez sur "Ignorer", l'outil vous rappelle que le certificat Siemens par défaut sera utilisé.



Remarque

Pour des raisons de sécurité, Siemens vous recommande instamment de créer vos propres certificats, afin de créer votre zone de confiance personnelle.

8. Définissez un mot de passe en conséquence pour :

- Compte Windows : se connecter au PC virtuel sur le cloud.
- Compte SoftwareCIM : se connecter à SoftwareCIM. Le mot de passe peut être modifiée ultérieurement sur la page de configuration SoftwareCIM.
- Compte SGLAN : autoriser la connexion du client SGLAN au serveur SGLAN.

Si vous décidez de créer une nouvelle instance à l'étape 5, vous devez définir un mot de passe correspondant pour tous les comptes ci-dessus.

Si vous décidez d'utiliser une instance existante à l'étape 5, vous devez saisir le mot de passe correct du compte Windows pour vous connecter au PC virtuel sur le cloud. Vous devez ensuite saisir un mot de passe en conséquence pour le compte SoftwareCIM et le compte SGLAN.

Remarque

Le mot de passe par défaut du compte SGLAN est sglan.

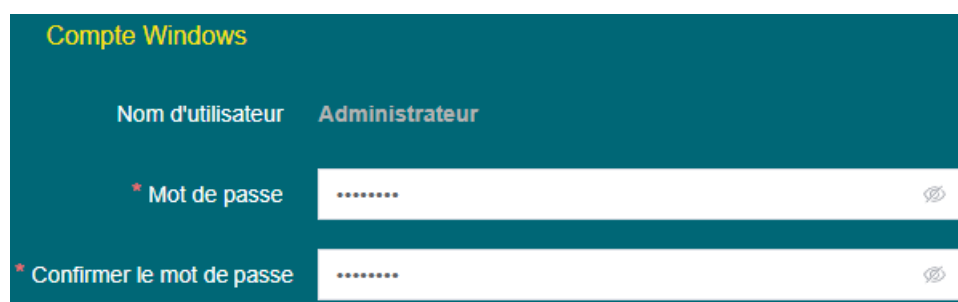
Le mot de passe par défaut du compte Windows est "Cim@1234".

Le mot de passe par défaut du compte SoftwareCIM est "cim".

Remarque

Limite de saisie pour le mot de passe

Vous pouvez faire glisser la souris sur le point d'interrogation pour plus de détails sur la limite de saisie de tous les mots de passe.



Compte Windows

Nom d'utilisateur	Administrateur
* Mot de passe	*****
* Confirmer le mot de passe	*****

9. Cliquez sur le bouton "Déployer".

La procédure prend généralement plus ou moins 10 minutes selon la région sélectionnée. Une fois qu'elle est terminée et si vous avez sélectionné la règle de groupe de sécurité HTTPS/443 à l'étape 6, la fenêtre affiche un QR code et un lien. Vous pouvez accéder aux pages de configuration de SoftwareCIM à l'aide du QR code ou du lien. Si vous n'avez pas sélectionné la règle de groupe de sécurité HTTPS/443, la fenêtre affiche uniquement l'IP public de SoftwareCIM une fois le déploiement terminé.

Félicitations!
Veuillez enregistrer l'adresse IP ou le QR code pour une utilisation ultérieure en cas d'accès au SoftwareCIM déployé.



vous pouvez accéder au SoftwareCIM déployé en cliquant sur les liens ou en scannant le QR code. L'IP public est: 18.132.11.167

<https://18.132.11.167>

Remarques
1. Pour en savoir plus sur le déploiement de l'instance, voir <https://ecs.console.aliyun.com/#/home>
2. Pour éviter une interruption de l'exploitation, assurez-vous que vous disposez de fonds suffisants sur votre compte.

3.2.3 Dépannage de SoftwareCIM cloud deployment

Ce chapitre vous donne des conseils sur la manière de localiser et de résoudre les problèmes.

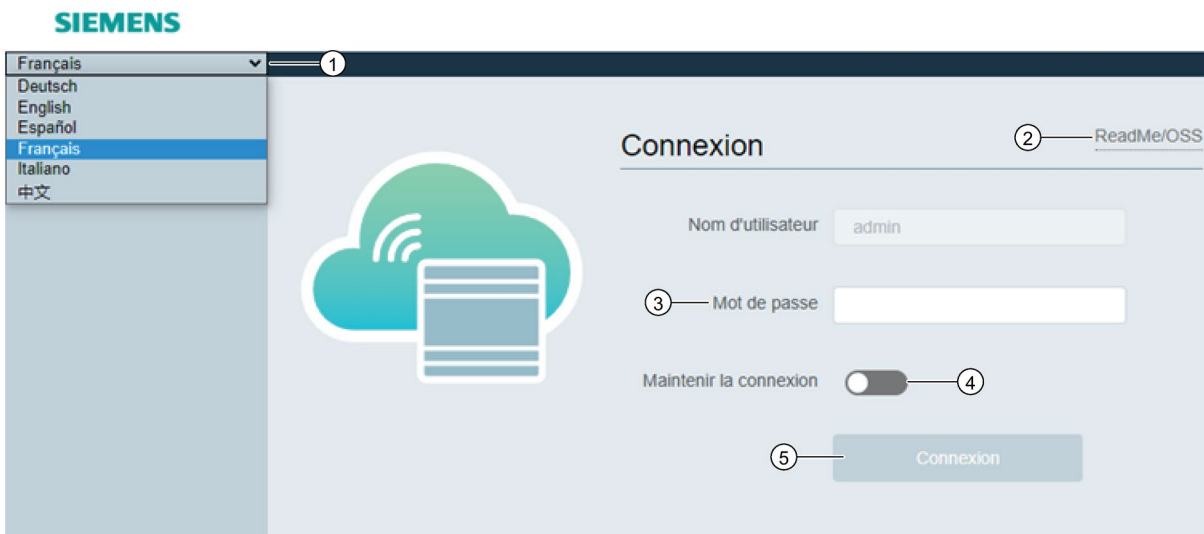
Diagnostic	Cause possible	Solution possible
Erreur inconnue	Erreur inconnue.	Quittez et exécutez à nouveau "SoftwareCIMInstaller.exe".
Échec de la connexion	Informations d'accès cloud incorrectes	Vérifiez l'ID de clé d'accès et la clé d'accès secrète.
Erreur réseau	Réseau instable pour connexion réseau interrompue	Vérifiez votre configuration réseau.
Autorisation refusée	Le compte cloud ne respecte pas les conditions d'autorisation.	Vérifiez et modifiez l'autorisation du compte cloud.
La vérification du certificat a échoué	- La taille du fichier de certificat dépasse la limite. - Le certificat n'est pas dans la période de validité	Renouvelez le certificat.
Échec de l'affectation EIP	Le nombre d'adresses IP Elastic dépasse la limite.	Supprimez les adresses IP Elastic inutilisées de la console du cloud.
Erreur de connexion au service SSH	Échec de la connexion à l'instance du service SSH	Vérifiez les points suivants : - l'instance est initialisée, - le compte cloud est verrouillé, - l'instance du service SSH est opérationnelle, - la connexion réseau est instable.

Configuration de SoftwareCIM

4.1 Présentation de l'interface utilisateur

Page de connexion

La page de connexion s'affiche comme suit :



- ① Sélectionnez la langue d'affichage appropriée si nécessaire.
- ② Consultez le fichier Lisezmoi OSS.
- ③ Saisissez le mot de passe.
- ④ Activez la fonction "Maintenir la connexion". Vous n'aurez plus à saisir le mot de passe à la prochaine connexion.
- ⑤ Se connecter à SoftwareCIM

Remarque

Le mot de passe de connexion par défaut est cim.

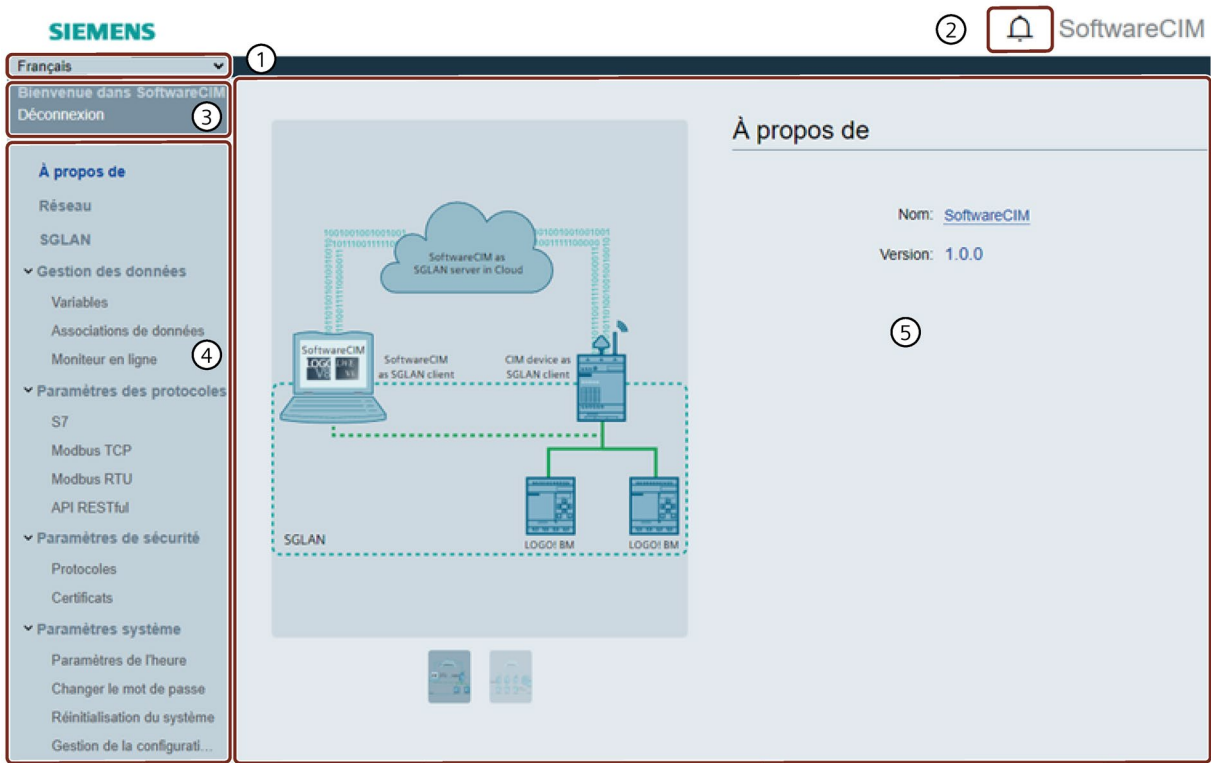
Pour des raisons de sécurité, Siemens vous recommande de remplacer le mot de passe par défaut par un mot de passe plus fort après la première connexion.

Remarque

"Maintenir la connexion" est désactivé par défaut. Si la fonction est activée, cette configuration expire après 30 jours.

Pages de configuration

Une fois connecté, vous voyez la page de configuration s'afficher comme suit :



- ① Affichage du menu de sélection de la langue
- ② Table d'état du système SoftwareCIM
- ③ Connexion/Déconnexion
- ④ Navigateur dans les pages de configuration
- ⑤ Informations détaillées d'une page Web spécifique

SoftwareCIM contient les pages de configuration suivantes :

Pages de configuration	Description
À propos de (Page 32)	Informations générales sur le SoftwareCIM
Réseau (Page 33)	Configurer LAN ou WAN
SGLAN (Page 34)	Définir le serveur SGLAN comme serveur ou client
Gestion des données (Page 38)	Édition des variables et associations
Paramètres des protocoles (Page 43)	Configuration des protocoles de communication
Paramètres de sécurité (Page 56)	Configuration de la stratégie de sécurité
Paramètres système (Page 62)	Configuration des paramètres système

État du système SoftwareCIM

Cliquez sur l'icône  pour afficher la table d'état du système SoftwareCIM. Vous pouvez vérifier tous les états des modules de fonction SoftwareCIM. En cas d'erreur sur un module de fonction, le message d'erreur s'affiche sur la table d'état du système. Pour comprendre la cause de l'erreur et savoir comment y remédier, voir la table de dépannage des états du système (Page 68) SoftwareCIM.

module	état	heure	message
Serveur S7	Désactivé	2023-12-06 09:59:05	
Client S7	Désactivé	2023-12-06 09:59:05	
Serveur NTP	Désactivé	2023-12-06 09:59:05	
Serveur Modbus TCP	Désactivé	2023-12-06 09:59:05	
Client Modbus TCP	Désactivé	2023-12-06 09:59:05	
Modbus RTU	Désactivé	2023-12-06 09:59:05	
SGLAN	Désactivé	2023-12-06 09:59:04	

Vue d'ensemble des éléments de navigation, de commande et d'affichage

Les pages de configuration utilisent les éléments suivants :

Icône	Fonction
	Éditer l'élément
	Supprimer l'élément
	Informations d'aide

Les pages de configuration comprennent les boutons suivants :

Icône	Fonction
	Ajouter une nouvelle ligne
	Enregistrer les modifications sur la page actuelle
	Rejeter les modifications sur la page actuelle

Menu icône barre système SoftwareCIM

Si SoftwareCIM est en cours d'exploitation, une icône d'application est visible sur la barre système. Un clic droit sur l'icône permet d'afficher le menu comme suit :

Ouvrez SoftwareCIM
Langue ▶
Actualiser
Configurer la mise à jour
Arrêter le service SoftwareCIM
Aide
Quitter

Commande de menu	Fonction
Ouvrez SoftwareCIM	Afficher la fenêtre SoftwareCIM
Langue	Sélectionner la langue d'affichage pour le menu icône de la barre système, les fenêtres Mise à jour et Configurer la mise à jour
Mise à jour (Page 65)	Rechercher si une nouvelle version de SoftwareCIM existe
Configurer la mise à jour (Page 65)	Configurer la mise à jour de SoftwareCIM
Arrêter/lancer le service SoftwareCIM	Arrête ou lance le service SoftwareCIM
Aide	Consulter le document d'aide
Quitter	Fermer la fenêtre SoftwareCIM et quitter la barre système

4.2 À propos de

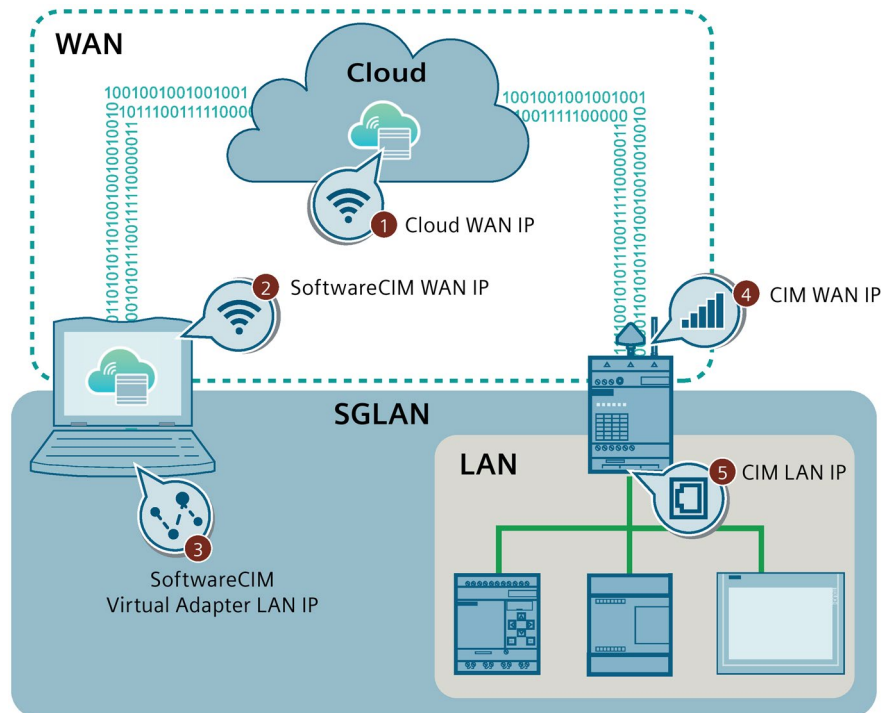
Cette page affiche les informations générales sur SoftwareCIM.

Élément d'affichage	Introduction
Nom	Affiche le nom du SoftwareCIM. Vous pouvez éditer le nom affiché en cliquant dessus
Version	Version de l'application bureau

4.3 Paramètres réseau

Les paramètres réseau permettent de configurer le LAN et le WAN.

Le schéma suivant montre le fonctionnement de LAN, WAN et SGLAN pour SoftwareCIM :



- | | |
|--|---|
| ① Cloud WAN IP | L'adresse IP publique du PC virtuel sur le cloud. |
| ② SoftwareCIM WAN IP | L'adresse IP du PC local sur lequel est installé SoftwareCIM. Cette adresse IP peut être utilisée pour accéder à Internet. |
| ③ IP du réseau LAN de l'adaptateur virtuel SoftwareCIM | L'adresse IP de l'adaptateur virtuel du PC local sur lequel est installé SoftCIM. Cette adresse IP peut être utilisée pour la communication SGLAN et pour accéder aux pages de configuration SoftwareCIM. |
| ④ IP WAN CIM | L'adresse IP de l'appareil CIM permettant d'accéder à Internet. |
| ⑤ IP du réseau local CIM | L'adresse IP de l'appareil CIM pour la communication SGLAN et pour accéder aux pages de configuration de l'appareil CIM. |

Si vous avez déployé SoftwareCIM sur le cloud AWS ou Alibaba à l'aide de l'application "SoftwareCIMInstaller.exe", l'IP WAN Cloud est configurée automatiquement lorsque vous activez l'accès à SoftwareCIM via WAN avec WAN -> Paramètres avancés. Si vous avez déployé SoftwareCIM manuellement sur le cloud sans l'application, vous devez demander une adresse IP Elastic et l'associer au PC virtuel sur le cloud. Vous pouvez ensuite configurer l'adresse IP Elastic sous Paramètres avancés. Une fois la configuration terminée, vous pouvez accéder au SoftwareCIM sur le cloud en utilisant l'IP WAN Cloud.

Remarque

L'adresse IP par défaut de SoftwareCIM est 192.168.0.81.

Remarque

La modification de l'interface WAN du SoftwareCIM affecte uniquement l'interface que le serveur écoute, mais pas l'interface de laquelle le client se déconnecte. L'interface à laquelle le client se connecte est toujours déterminée par le système d'exploitation.

4.4 Paramètres SGLAN

4.4.1 Configuration du serveur SGLAN

Cette page vous permet de configurer le SoftwareCIM comme serveur SGLAN.

Remarque

Afin d'éviter les attaques par saturation, Siemens vous recommande d'activer et de configurer le pare-feu sur le PC virtuel sur le cloud.

Conditions

- L'hôte pour installer SoftwareCIM est accessible via une adresse publique IPv4/IPv6

Configuration du serveur SGLAN

1. Activez "SoftwareCIM comme serveur SGLAN".
2. Sélectionnez le mode.

3. Définissez le "Mot de passe d'accès" et confirmez-le dans "Confirmer le mot de passe d'accès".

Remarque

Le mot de passe par défaut du serveur SGLAN est sglan.

4. Cliquez sur "Enregistrer les modifications".

Paramètres SGLAN

SoftwareCIM comme serveur SGLAN: ☒
SoftwareCIM comme client SGLAN: ☐

SoftwareCIM comme serveur SGLAN

Mode: IPv4

Mot de passe d'accès : 64/64

Confirmer le mot de passe 64/64

Serveur IP: 139.24.129.110

Statistiques

Octets envoyés	Octets reçus	Envoyer vitesse	Recevoir vitesse
0 Bytes	0 Bytes	0 B/S	0 B/S

État de la connexion du client

données de la liste de filtres

#	Name	IP du réseau local	LAN Mask	Status
Aucune donnée				

4.4.2 Configuration du client SGLAN

Cette page vous permet de configurer le SoftwareCIM comme client SGLAN.

Conditions

- Le PC sur lequel installer SoftwareCIM peut accéder à Internet via IPv4/IPv6

Connexion du client SGLAN au serveur SGLAN

Avant de connecter un client SGLAN au serveur SGLAN, vous devez obtenir le mode, l'adresse IP et le mot de passe d'accès du serveur SGLAN.

1. Activez "SoftwareCIM comme client SGLAN".
2. Sélectionnez "Mode hôte distant".
3. Saisissez l'adresse IP du serveur SGLAN sous "Hôte distant".

- Saisissez le mot de passe d'accès du serveur SGLAN sous "Mot de passe du serveur".

Remarque

Si vous avez activé le serveur SGLAN sans modifier le mot de passe, vous pouvez vous connecter au serveur SGLAN avec le mot de passe par défaut "sglan".

- Cliquez sur "Enregistrer les modifications".

Paramètres SGLAN

SoftwareCIM comme serveur SGLAN: ☐

SoftwareCIM comme client SGLAN: ☒

Serveur Liste de serveurs

Mode hôte distant: IPv6

Remote Host: 240E:476:F40:58F6:7044:27F8:6DAD:4234 37/64

Mot de passe du serveur: 64/64

Statistiques:

Nom	Statistiques des données SGLAN
Nom de serveur	CIM110 SGLAN Server
IP du réseau local du serveur	192.168.0.110
État	Connecté
Temps de connexion	00:06:31
Octets envoyés	2.218 MB
Octets reçus	2.328 MB
Envoyer vitesse	6.120 KB/S
Recevoir vitesse	6.696 KB/S

Rejeter les modifications Enregistrer les modifications

État de la connexion	Description
Déconnecté	Non connecté au SGLAN
Connexion en cours	Le client SGLAN se connecte au serveur SGLAN et configure SGLAN
Connecté	Le SGLAN est configuré et le client SGLAN est connecté au serveur SGLAN
Erreur de connexion	Impossible d'établir la communication entre le client SGLAN et le serveur SGLAN
Délai d'attente d'établissement de la communication dépassé	Délai d'attente d'établissement de la communication entre le client SGLAN et le serveur SGLAN dépassé
Échec de la connexion	Échec de la connexion en raison d'une erreur de mot de passe
Délai d'attente de connexion dépassé	Échec de la connexion dans une période valide
Rupture de connexion	Le SGLAN est déconnecté en raison d'une défaillance de longue durée de la communication réseau
Erreur de certificat	Échec de la vérification du certificat
Erreur générale	Erreur générale

Liste des serveurs

Vous pouvez ajouter à la liste les serveurs SGLAN que vous utilisez habituellement. La liste des serveurs permet de se connecter ou de se déconnecter rapidement au ou du serveur SGLAN.

Paramètres SGLAN

SoftwareCIM comme serveur SGLAN: ☐

SoftwareCIM comme client SGLAN: ☒

Serveur [Liste de serveurs](#)

🔍 données de la liste de filtres + Ajouter une ligne

	Mode hôte distant	Hôte distant	Description	État de la connexion	Action
1	IPv4	10.11.12.13	server3	Déconnecté	  
2	IPv6	240E:476:F42:D479:50CB:DC91:EEF8:AAAA	server4	Déconnecté	  

Créer un élément de serveur

1. Cliquez sur le bouton "Ajouter une ligne".
2. Saisissez les informations du serveur. Vous pouvez ajouter 64 éléments de serveur au maximum.

Description : description du serveur SGLAN

Mode hôte distant : mode hôte distant du serveur SGLAN

Hôte distant : adresse IP du serveur SGLAN

Mot de passe du serveur : mot de passe d'accès du serveur SGLAN

3. Cliquez sur "Enregistrer" pour confirmer les informations du serveur ou cliquez sur "Annuler" pour rejeter la configuration.
4. Répétez les étapes 1 à 3 pour ajouter tous les éléments de serveur nécessaires.

Connectez l'appareil.

Cliquez sur  pour connecter le serveur SGLAN

Modifier un élément de serveur

Cliquez sur , puis saisissez la nouvelle valeur dans le champ de l'élément de serveur correspondant que vous voulez modifier.

Supprimer un élément de serveur

Cliquez sur le bouton de suppression  en regard de l'élément de serveur que vous voulez supprimer.

4.5 Gestion des données

La gestion des données vous permet de gérer les variables et les associations de données et de surveiller les variables en ligne. Les noms des variables et des associations de données doivent être uniques.

4.5.1 Variables

Une variable est définie par son nom, le type de données, le type d'adresse et l'adresse. Ce chapitre montre comment créer et éditer des variables que vous utilisez pour stocker des valeurs dans SoftwareCIM. Vous pouvez créer des variables pour tous les types de données pris en charge par le modèle UDM.

Variables

#	Nom	Type de données	Type d'adresse	Adresse	Valeur	modValue	Modifier	
1	PAR	Int (I)	V	0	0		✓	 
2	Input1	Bool (x)	I	0.0	1		✓	 
3	output1	Bool (x)	Q	0.0	0		✓	 

+ Ajouter une ligne

Forcer toutes les valeurs

☐ Rejeter les modifications ☒ Enregistrer les modifications

Ajouter une variable

1. Cliquez sur le bouton "Ajouter une ligne". Vous pouvez ajouter 16 lignes au maximum.
2. Saisissez les paramètres de la variable.

Nom : Un nom de variable peut contenir des lettres, des chiffres et des caractères spéciaux.

Type de données : type de données de la variable

Type d'adresse : type d'adresse de la variable

Adresse : adresse dans SoftwareCIM

3. Répétez les étapes 1 et 2 pour ajouter toutes les variables nécessaires.
4. Vous pouvez visualiser ou forcer la valeur de la variable.

Valeur : la valeur du paramètre

Forcer la valeur (modValue) : valeur modifiée du paramètre

Forcer : cliquez sur la coche pour forcer la valeur du paramètre

Forcer toutes les valeurs : cliquez sur "Forcer toutes les valeurs" pour modifier la valeur du paramètre en tant que modValue

Remarque

Si la variable est utilisée par un événement ou une action, elle ne peut pas être modifiée ni supprimée.

Modifier une variable

Cliquez sur , puis saisissez la nouvelle valeur dans le champ de la variable que vous voulez modifier.

Supprimer une variable

Cliquez sur le bouton Supprimer  pour supprimer la variable.

4.5.2 Associations de données

Cette page permet d'associer un événement à une action. Consultez Modèle de données universel (Page 8) pour plus d'informations.

Vous pouvez configurer l'événement de modification de variable et définir une action que le SoftwareCIM exécutera lorsque l'événement de liaison se produira.

Associations de données							
#	Nom	Type d'événement	Configuration de l'événement	Type d'action	Configuration de l'action	Activé	
1	Bind 1	Valeur m	Variable Variable :	Définir	Variable À Variable : 0	☒	 
2	Bind 2	Supérieur	Variable Supérieur à Variable : 0X20	Réduire	Variable Par Variable : 0X1	☒	 
3	Bind 3	Égal à	Variable Égal à Variable : 0X10	Augmenter	Variable Par Variable : 0X1	☒	 
4	Bind 4	Valeur de	Variable Variable :	Définir	Variable À Variable : 0X3	☒	 
5	Bind 5	Valeur de	Variable Variable :	Copier	Variable	☒	 
+ Ajouter une ligne							
☐ Rejeter les modifications ☒ Enregistrer les modifications							

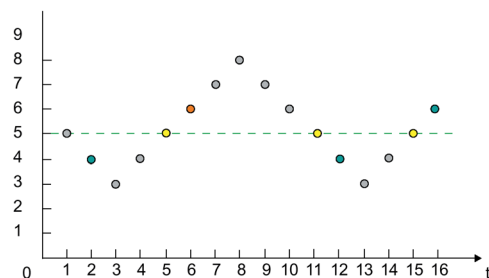
Associer des données

1. Cliquez sur "Ajouter une ligne" pour ajouter une nouvelle ligne.
2. Cliquez sur la liste déroulante "Type d'événement" pour choisir un événement.

	Événement	Source de l'événement	Restriction concernant la source
1	Transitions de 1 à 0	Variable	Type de données autorisé : bool
2	Transitions de 0 à 1		
3	Valeur modifiée		Type de données autorisé : tous les types de données UDM autorisés à l'exception de bool
4	Supérieur à		Type de données autorisé : tous les types de données UDM autorisés à l'exception de bool Remarque : le type et la plage de la valeur de référence doivent être les mêmes que ceux de la variable source de l'événement.
5	Égal à		
6	Inférieur à		

Remarque

L'événement "Supérieur à" est déclenché par un front montant et l'événement "Inférieur à" par un front descendant.



-  Aucun événement n'est déclenché.
-  L'événement "Supérieur à 5" est déclenché.
-  L'événement "Égal à 5" est déclenché.
-  L'événement "Inférieur à 5" est déclenché.

3. Configurez l'événement. Cliquez sur la liste déroulante "Variable" pour sélectionner une variable (Page 38).

Si aucune variable dans la liste ne répond à vos exigences, vous pouvez cliquer pour ajouter une variable.

 Ajouter une variable

bit_1

word_1

byte_1

4. Configurez le type d'action.

	Action	Source de l'action	Restriction concernant la cible	Remarque
1	Définir une nouvelle valeur	Variable	Type de données autorisé : tous les types de données UDM autorisés	
2	Copier la valeur de l'événement		Le type de variable de l'action doit être identique au type de variable de l'événement source d'où se fait la copie.	
3	Augmenter de la valeur		Type de données autorisé : tous les types de données UDM autorisés à l'exception de bool	- La valeur à ajouter ou soustraire doit être positive. - Lorsque la variable atteint la valeur maximale ou minimale de sa plage, elle n'est plus augmentée ni réduite.
4	Réduire de la valeur			

5. Configurez l'action. Vous devez sélectionner une variable dans la liste de variables et indiquer la nouvelle valeur.

6. Activez l'association.

Remarque

Si vous n'avez pas encore défini de variable, les événements et actions sélectionnables ne pourront pas tous être affichés.

Modifier une association de données

Cliquez sur l'icône  en regard de l'association de données que vous voulez modifier, puis modifiez la configuration.

Supprimer une association de données

Cliquez sur l'icône  en regard de l'association de données que vous voulez supprimer.

4.5.3 Surveillance en ligne

Dans le tableau de données UDM en ligne, vous pouvez surveiller les données UDM.

Moniteur en ligne							
	Plage	Type	Adresse	Valeur	ModValue	Modifier	
1	I	Bool(x)	0.0	1		☒	
2	Q	Bool(x)	0.0	0		☒	
3	M	Int (i)	0	100		☒	
+ Ajouter une ligne						Forcer toutes les valeurs	

Ajouter une variable en ligne

1. Cliquez sur le bouton "Ajouter une ligne". Vous pouvez ajouter 64 lignes au maximum.
2. Saisissez les paramètres de la variable.

Plage : type d'adresse UDM de la variable

Type : type de données de la variable

Adresse : adresse dans SoftwareCIM

Valeur : valeur de la variable dans l'adresse sélectionnée

ModValue : valeur modifiée de la variable dans l'adresse sélectionnée

Après avoir modifié la valeur de plusieurs lignes dans le champ ModValue, vous pouvez cliquer sur "Forcer toutes les valeurs" pour valider les modifications.

Forcer : Cliquez sur la coche pour forcer la valeur dans l'adresse sélectionnée

3. Répétez les étapes 1 et 2 pour ajouter toutes les variables nécessaires.

Supprimer une variable

Cliquez sur le bouton Supprimer  pour supprimer la variable.

4.6 Paramètres des protocoles

Cette page permet de configurer les protocoles suivants : S7, Modbus TCP, Modbus RTU, API RESTful.

4.6.1 S7

Cette page permet d'activer ou de désactiver les connexions S7, ainsi que de les vérifier et de les éditer.

SoftwareCIM prend en charge quatre connexions S7 simultanées au plus. SoftwareCIM partagera les connexions s'il agit en même temps comme serveur S7 et client S7.

Remarque

- Lorsque vous configurez une communication S7 entre un appareil distant (LOGO! BM) et SoftwareCIM, assurez-vous que la connexion S7 et la connexion serveur dynamique sont activées dans l'appareil distant connecté (LOGO! BM).
 - SoftwareCIM sur le SGLAN peut être configuré en tant que serveur S7 ou client S7.
-

S7

Connexion S7:

La connexion S7 n'est pas sécurisée, le port de serveur local et le port de serveur distant sont tous deux 102.

Connexions serveur et client statiques: 4

Connexions serveur dynamiques disponibles: 0

Connexion serveur dynamique:

État de la connexion

État de la connexion:

#	Type de connexion	Adresse IP distante	Adresse TSAP distante	Adresse TSAP locale	État de la connexion
1	Client statique	192.168.0.11	23.00	23.00	✓
2	Client statique	192.168.0.11	22.00	22.00	✓
3	Serveur statique	192.168.0.11	20.00	20.00	✓
4	Serveur statique	192.168.0.11	21.00	21.00	✓

S7 Serveur

Informations sur l'espace d'adressage S7

Connexions serveur statiques:

#	Adresse IP distante	Adresse TSAP distante	Adresse TSAP locale	
1	192.168.0.11	20.00	20.00	
2	192.168.0.11	21.00	21.00	

+ Ajouter une ligne

Impossible d'ajouter plus d'éléments. Le nombre maximum est : 4

S7 Client

Connexions client statiques:

#	Adresse IP distante	Adresse TSAP distante	Adresse TSAP locale	
1	192.168.0.11	23.00	23.00	
2	192.168.0.11	22.00	22.00	

+ Ajouter une ligne

Impossible d'ajouter plus d'éléments. Le nombre maximum est : 4

Rejeter les modifications

Enregistrer les modifications

①

Activez ou désactivez la connexion S7.
Remarque : la connexion S7 n'est pas sécurisée. Pour SoftwareCIM comme serveur S7, la communication S7 est possible uniquement via l'adaptateur LAN virtuel. Pour SoftwareCIM comme client S7, la communication S7 est possible via tout type d'adaptateur.

②

Récapitulatif des connexions S7

SoftwareCIM

Instructions de service, 01/2024

44

- ③ Activez ou désactivez la connexion serveur dynamique.
Remarque : SoftwareCIM prend en charge quatre connexions S7 simultanées au maximum. Si vous avez défini des liaisons statiques, le nombre de connexions serveur dynamiques sera égal à 4 moins le nombre de liaisons statiques.
- ④ État des connexions S7 actuelles
Cliquez sur ▼ pour développer la liste des connexions et sur ▲ pour la réduire.
- ⑤ Lien vers la page d'information sur l'espace d'adressage S7
- ⑥ Vous configurez ici les propriétés des connexions que SoftwareCIM utilise comme serveur S7.
 - Adresse IP distante : adresse IP du client auquel vous voulez vous connecter.
 - Adresse TSAP locale : l'adresse TASP dans SoftwareCIM est comprise entre 00.01 et FF.FF
 - Adresse TSAP distante : adresse TSAP du client auquel vous voulez vous connecter.
- ⑦ Vous configurez ici les propriétés des connexions que SoftwareCIM utilise comme client S7.
 - Adresse IP distante : adresse IP du serveur auquel vous voulez vous connecter.
 - Adresse TSAP distante : adresse TSAP du serveur auquel vous voulez vous connecter.
 - Adresse TSAP locale : l'adresse TASP dans SoftwareCIM est comprise entre 00.01 et FF.FF
- ⑧ Cliquez pour ouvrir la "table de transfert de données" de la connexion correspondante que SoftwareCIM utilise en agissant comme client S7.

Configuration de la table de transfert de données

Vous devez configurer la table de transfert de données pour les connexions que SoftwareCIM utilise en tant que client S7 :

1. Cliquez sur "Ajouter une ligne". Vous pouvez ajouter 16 lignes au maximum.
2. Cliquez sur ② pour choisir le type d'adresse UDM de SoftwareCIM.
3. Saisissez une adresse dans le champ d'adresse ③ de SoftwareCIM.
4. Cliquez sur ④ pour choisir le sens de transfert des données.
5. Cliquez sur ⑤ pour sélectionner le type d'adresse S7 du serveur S7 distant.
6. Saisissez l'adresse de début S7 ⑥ du serveur S7 distant.
7. Saisissez la longueur des données à transférer ⑦.

8. Pour définir à quel intervalle de temps SoftwareCIM synchronise les données avec le serveur, activez "Intervalle personnalisé" et saisissez l'intervalle de temps souhaité ⑧.

L'intervalle de transmission minimum par défaut est de 80 millisecondes.

9. Enregistrez vos modifications.

10. Cliquez sur ⑨ pour fermer la table de transfert de données.

Restrictions relatives au transfert de données

Le tableau ci-dessous présente les restrictions concernant la plage et l'adresse locale pour les connexions client.

Demandes de lecture et d'écriture :

adresse locale (SoftwareCIM)		Adresse distante (appareil compatible S7)
Type d'adresse	Plage	Type d'adresse
IB	0 à 511	IB, QB, MB, VB, bloc de données
QB	0 à 511	
MB	0 à 511	
VB	0 à 1023	
IW	0 à 510	IW, QW, MW, VW, bloc de données
QW	0 à 510	
MW	0 à 510	
VW	0 à 1022	
ID	0 à 508	ID, QD, MD, VD, bloc de données
QD	0 à 508	
MD	0 à 508	
VD	0 à 1020	

Remarque

Le type d'adresse est la combinaison du nom de la mémoire image du processus dans le modèle UDM (Page 8) et du type de données. Par exemple, "IB" signifie octet en mémoire I.

Les valeurs doivent suivre la règle : adresse locale + longueur de données ≤ valeur maximale du type d'adresse locale.

4.6.2 Modbus TCP

Cette page permet d'activer ou de désactiver les connexions Modbus TCP, de configurer la table de transfert de la communication Modbus, ainsi que de vérifier l'état des connexions.

SoftwareCIM prend en charge quatre connexions Modbus TCP simultanées au plus.

SoftwareCIM partagera les connexions s'il agit en même temps comme serveur Modbus TCP et client Modbus TCP.

Remarque

- Lorsque vous configurez une communication Modbus TCP entre un appareil distant (LOGO! BM) et SoftwareCIM, assurez-vous que la connexion Modbus TCP et la connexion serveur dynamique S7 sont activées dans l'appareil distant connecté (LOGO! BM).
 - SoftwareCIM sur le SGLAN peut être configuré en tant que serveur Modbus TCP ou client Modbus TCP.
-

Modbus TCP

Connexion Modbus TCP: ☒ ①

● La connexion Modbus TCP n'est pas sécurisée, le port de serveur local et le port de serveur distant sont tous deux 502.

Connexions serveur et client statiques: 4 ②
 Connexions serveur dynamiques disponibles: 0
 Connexion serveur dynamique: ☐ ③

État de la connexion

État de la connexion: ④

#	Type de connexion	Adresse IP distante	État de la connexion
1	Client statique	192.168.0.11	✓
2	Client statique	192.168.0.11	✓
3	Serveur statique	192.168.0.11	✓
4	Serveur statique	192.168.0.11	✓

Serveur Modbus TCP

⑤ Informations sur l'espace d'adressage Modbus

⑥ Connexions serveur statiques:

#	Adresse IP du client distant
1	192.168.0.11
2	192.168.0.11

+ Ajouter une ligne Impossible d'ajouter plus d'éléments. Le nombre maximum est : 4

Modbus TCP Client

Connexions client statiques: ⑦

#	Adresse IP du serveur distant
1	192.168.0.11
2	192.168.0.11

+ Ajouter une ligne Impossible d'ajouter plus d'éléments. Le nombre maximum est : 4

⑧

○ Rejeter les modifications ○ Enregistrer les modifications

- ① Activez ou désactivez la connexion Modbus TCP.
Remarque : la connexion Modbus TCP n'est pas sécurisée. Pour SoftwareCIM comme serveur Modbus TCP, la communication Modbus TCP est possible uniquement via l'adaptateur LAN virtuel. Pour SoftwareCIM comme client Modbus TCP, la communication Modbus TCP est possible via tout type d'adaptateur.
- ② Récapitulatif des connexions Modbus TCP

- ③ Activez ou désactivez la connexion serveur dynamique.
Remarque : SoftwareCIM prend en charge quatre connexions Modbus TCP simultanées au maximum. Si vous avez configuré des connexions statiques, le nombre de connexions serveur dynamiques sera égal à 4 moins le nombre de connexions statiques.
- ④ État des connexions Modbus TCP actuelles
- ⑤ Lien vers la page d'information sur l'espace d'adressage Modbus TCP
- ⑥ Vous configurez ici les propriétés du serveur.
 - Adresse IP distante : adresse IP du client auquel vous voulez vous connecter.
- ⑦ Vous configurez ici les propriétés du client.
 - Adresse IP distante : adresse IP du serveur auquel vous voulez vous connecter.
- ⑧ Cliquez ici pour ouvrir la "table de transfert de données" de la connexion correspondante que SoftwareCIM utilise en agissant comme client Modbus TCP.

Configuration du transfert de données Modbus TCP

Vous devez configurer la table de transfert de données pour les connexions que SoftwareCIM utilise en tant que client Modbus TCP :

Multiprotocole: Modbus TCP > Table de transfert de données
X

Table de transfert de données Connexion #1 Adresse IP du serveur distant [192.168.0.11]

#	Adresse de départ UDM	Sens	Adresse de départ Modbus	Longueur	ID d'unité	
1	IB ② 230.0 ③	← ④	Coil ⑤ 1 ⑥	16 ⑦	1 ⑧	✕
2	IB 230.0	→	Coil 417	16	1	✕
3	QB 230.0	←	Coil 1	16	1	✕
4	QB 230.0	→	Coil 433	16	1	✕
5	MB 380.0	←	Coil 1	16	1	✕
6	MB 380.0	→	Coil 449	16	1	✕
7	VB 380.0	←	Coil 1	16	1	✕
8	VB 380.0	→	Coil 465	16	1	✕
9	IW 240	←	HR 1	1	1	✕

+ Ajouter une ligne
Impossible d'ajouter plus d'éléments. Le nombre maximum est : 16

Intervalle personnalisé

Intervalle personnalisé: ☒

Heures: Minutes: Secondes: Millisecondes:

⌂ Rejeter les modifications
⌂ Enregistrer les modifications

1. Cliquez sur ① pour ajouter une nouvelle ligne.
2. Cliquez sur ② pour sélectionner le type d'adresse UDM de SoftwareCIM.
3. Saisissez une adresse dans le champ d'adresse de début UDM ③ de SoftwareCIM.
4. Cliquez sur ④ pour choisir le sens de transfert des données.
5. Cliquez sur ⑤ pour choisir le type d'adresse Modbus du serveur Modbus TCP distant.
6. Saisissez l'adresse de début ModBus ⑥ du serveur Modbus TCP distant.
7. Saisissez la longueur des données à transférer ⑦.
8. Saisissez l'ID d'unité ⑧.
9. Pour définir à quel intervalle de temps SoftwareCIM synchronise les données avec le serveur, activez l'intervalle personnalisé et saisissez l'intervalle de temps souhaité ⑨.
L'intervalle de transmission minimum par défaut est de 80 millisecondes.
10. Enregistrez vos modifications et fermez la table de transfert de données.

Restrictions relatives au transfert de données

Le tableau ci-dessous présente les restrictions concernant la plage et l'adresse locale pour les connexions client.

Adresse locale (SoftwareCIM)		Adresse distante (appareil compatible Modbus TCP)
Type d'adresse	Plage	Type d'adresse
IB	0.0 à 511.7	Bobine Entrée TOR (DI)
QB	0.0 à 511.7	
MB	0.0 à 511.7	
VB	0.0 à 1023.7	
IW	0 à 510	Registre de maintien (Holding Register, HR) Registre d'entrée (Input Register, IR)
QW	0 à 510	
MW	0 à 510	
VW	0 à 1022	

Remarque

Le type d'adresse est la combinaison du nom de la mémoire image du processus dans le modèle UDM (Page 8) et du type de données. Par exemple, "IB" signifie bit en mémoire I.

Les valeurs doivent suivre la règle : adresse locale + longueur de données ≤ valeur maximale du type d'adresse locale.

4.6.3 Modbus RTU

Cette page permet d'activer, de désactiver et de paramétrer la connexion Modbus RTU.

SoftwareCIM prend en charge une seule connexion Modbus RTU, soit en tant que maître Modbus RTU soit en tant qu'esclave Modbus RTU.

- ① Activez ou désactivez la connexion Modbus RTU.
Remarque : la connexion Modbus RTU n'est pas sécurisée.
- ② Vous configurez ici les propriétés des connexions du port série.
 - Port : sélectionnez le port série
 - Vitesse de transmission : définissez la vitesse de transfert
 - Transmission : configuration du port série
- ③ Lien vers la page d'information sur l'espace d'adressage Modbus
- ④ Vous configurez ici le type Modbus RTU.
 - Si vous sélectionnez "Maître", vous devrez configurer la "Table de transfert de données".
 - Si vous sélectionnez "Esclave", vous devrez configurer le Modbus RTU Esclave ID.
Plage pour l'ID d'esclave Modbus RTU : 1 à 255.

Configurer la table de transfert de données

Vous devez configurer les valeurs suivantes dans la table de transfert de données pour les connexions que SoftwareCIM utilise en tant que maître :

Multiprotocole: Modbus RTU > Table de transfert de données

Table de transfert de données

#	Adresse de départ UDM	Sens	Adresse de départ Modbus	Longueur	ID d'unité
1	VW ② 0 ③	HR ④	1 ⑥	1 ⑦	24 ⑧

+ Ajouter une ligne ①

Intervalle personnalisé

Intervalle personnalisé: ☒

Heures: 0 Minutes: 0 Secondes: 0 Millisecondes: 80 ⑨

⊙ Rejeter les modifications ⊙ Enregistrer les modifications

1. Cliquez sur ① pour ajouter une nouvelle ligne.
2. Cliquez sur ② pour choisir le type d'adresse UDM de SoftwareCIM.
3. Saisissez une adresse dans le champ d'adresse de début UDM ③ de SoftwareCIM.
4. Cliquez sur ④ pour choisir le sens de transfert des données.
5. Cliquez sur ⑤ pour sélectionner le type d'adresse Modbus de l'esclave Modbus RTU distant.
6. Saisissez l'adresse de début ModBus ⑥ de l'esclave Modbus RTU distant.
7. Saisissez la longueur des données à transférer ⑦.
8. Saisissez l'ID d'unité ⑧ de l'esclave Modbus RTU distant (ID/adresse d'esclave).
9. Pour définir l'intervalle de temps auquel le module CIM synchronise les données avec le serveur, activez l'option et saisissez l'intervalle de temps spécifié ⑨.
L'intervalle de transmission minimum par défaut est de 80 millisecondes.
10. Enregistrez vos modifications et fermez la table de transfert de données.

Restrictions relatives au transfert de données

Le tableau ci-dessous présente les restrictions concernant la plage et l'adresse locale pour les connexions client.

adresse locale (SoftwareCIM)		Adresse distante (appareil compatible Modbus RTU)
Type d'adresse	Plage	Type d'adresse
IB	0.0 à 511.7	Bobine Entrée TOR (DI)
QB	0.0 à 511.7	
MB	0.0 à 511.7	
VB	0.0 à 1023.7	
IW	0 à 510	Registre de maintien (Holding Register, HR)
QW	0 à 510	
MW	0 à 510	Registre d'entrée (Input Register, IR)
VW	0 à 1022	

Remarque

Le type d'adresse est la combinaison du nom de type d'adresse dans le modèle UDM (Page 8) et du type de données. Par exemple, "IB" signifie bit en mémoire I.

Les valeurs doivent suivre la règle : adresse locale + longueur de données ≤ valeur maximale du type d'adresse locale.

4.6.4 API RESTful

SoftwareCIM fournit également une interface REST pour les utilisateurs qui connaissent cette technologie et qui veulent interagir avec SoftwareCIM au moyen d'une interface automatisée ou programmée.

Si l'appareil connecté à SoftwareCIM prend en charge RESTful, vous pouvez récupérer ou mettre des données sur l'UDM par le biais de l'API RESTful. Vous pouvez, par exemple, accéder à l'interface UDM via une interface utilisateur Swagger qui contient une description détaillée des classes, méthodes et paramètres.

Format de chemin URI

`https://[adresse_IP_pour_cim]/pi/rest/[type_d'adresse][type_de_données_court][plage]`

Actions prises en charge

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

Lorsque vous placez un ensemble de valeurs dans une plage, séparez-les par une virgule ",".

Paramètres

- **Type d'adresse** : i, m, v, q
- **Type** : type de données de l'accès
- **&** : connecter plusieurs adresses discrètes ou adresses avec une plage ou un type différent
- **Plage** : plage dans le type d'adresse que vous voulez lire ou écrire.

Format pour la plage : adresse de début~adresse de fin. Si la plage n'est pas définie, SoftwareCIM considère que vous avez besoin de toute la plage du type d'adresse.

- ~adresse de fin : si l'adresse de début n'est pas définie, SoftwareCIM considère que l'adresse de début est le début de la plage.
- adresse de début~ : si l'adresse de fin n'est pas définie, SoftwareCIM considère que l'adresse de fin est la fin de la plage.
- Une adresse : accès à une adresse unique

Type de données court	Type de données	Longueur	Plage de valeurs	Affichage	Exemple
x	bit	1 bit	0~1	0 ou 1	1
b	byte	8 bits	0~FF	chaîne hexadécimale	ab
w	word	16 bits	0~FFFF	chaîne hexadécimale	aabb
dw	double-word	32 bits	0~FFFFFFFF	chaîne hexadécimale	aabbccdd
lw	long-word	64 bits	0~FFFFFFFFFFFFFFFF	chaîne hexadécimale	aabbccddaabbccdd
su	short-unsigned	8 bits	0~255	décimal	12
u	unsigned	16 bits	0~65535	décimal	1234
du	double-unsigned	32 bits	0~4294967295	décimal	12345678
lu	long-unsigned	64 bits	0~18446744073709551615	décimal	12345678
si	short-int	8 bits	-128~127	décimal	-12
i	int	16 bits	-32768~32767	décimal	-1234
di	double-int	32 bits	-2147483648~2147483647	décimal	-12345678
li	long-int	64 bits	-9223372036854775808 ~ 9223372036854775807	décimal	-12345678
r ¹	real	32 bits	-3.4E38 ~ +3.4E38	décimal	1234.5678
lr ¹	long-real	64 bits	-1.797E308 ~ +1.797E308	décimal	-1234.5678

1 Le chiffre significatif pour les types REAL et LONG REAL ne peut pas dépasser 6.

Exemple

La partie [type d'adresse][type][plage] dans les exemples ci-dessous peut être remplacée par n'importe lequel des paramètres autorisés.

Exemple	Description
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3~8.7</code>	Tous les bits dans [5.3, 8.7] dans la plage I
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/i</code> <code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix</code>	Tous les bits dans la plage I
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3</code>	Un bit à 5.3 dans la plage I
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3~8.7</code>	Tous les bits dans [5.3, 8.7] dans la plage I
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100</code>	Un mot à 100 dans la plage I
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100~200</code>	Tous les mots dans [100, 200] dans la plage I
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100~</code>	Tous les mots dans [100, fin_de_plage] dans la plage I
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/qb100</code>	Un octet à 100 dans la plage Q
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/qr100</code>	Un réel à 100 dans la plage Q
<code>https://xxx.xxx.xxx.xxx:xxx/pi/rest/qr~100</code>	Un réel dans [début_de_plage, 100] dans la plage Q
<code>https://xxx.xxx.xxx.xxx:xxxx/pi/rest/ix0.0&qil12</code>	Un bit à 0.0 dans la plage I et un bit à 12 dans la plage Q ¹

- 1 À partir de /pi/rest/, la longueur de la commande doit être inférieure à 500 caractères anglais.

Remarque : un mauvais connecteur entraînera la non-reconnaissance des adresses.

4.7 Paramètres de sécurité

4.7.1 Protocole

Cette page permet de vérifier et de gérer tous les protocoles. Vous pouvez activer ou désactiver un protocole en basculant l'interrupteur. Tous les protocoles sont désactivés par défaut à l'exception de HTTPS.

Gestion des protocoles de communication

S7: ☐

Modbus TCP: ☐

Modbus RTU: ☐ Le port Modbus RTU doit être sélectionné.

NTP: ☐

RESTful API: ☐

HTTPS: ☒

Activer S7/Modbus TCP/Modbus RTU/NTP

Lorsque vous activez un protocole, la configuration de protocole précédente est récupérée dans la page de configuration des protocoles correspondante.

Remarque

L'API RESTful n'est pas sécurisée. Si vous activez l'API RESTful pour SoftwareCIM, l'authentification n'est pas nécessaire si l'appareil accède au SoftwareCIM via l'adaptateur LAN virtuel. Elle est requise si un appareil accède au SoftwareCIM via l'adaptateur WAN sélectionné.

N'activez l'API RESTful que lorsque c'est nécessaire.

Remarque

La connexion NTP n'est pas sécurisée. Pour SoftwareCIM comme serveur NTP, la communication NTP est possible uniquement via l'adaptateur LAN virtuel.

Désactiver S7/Modbus TCP/Modbus RTU/NTP

Si vous désactivez un protocole, SoftwareCIM ne peut fonctionner ni comme serveur, ni comme client.

4.7.2 Certificats

SoftwareCIM vous permet de configurer et de gérer vos certificats.

- Certificat détenu : génère et sélectionne un certificat pour configurer un serveur Web sécurisé et un serveur SGLAN
- Certificat approuvé : sélectionne un certificat pour configurer le client SGLAN

Remarque

Pour des raisons de sécurité, Siemens vous recommande instamment de créer vos propres certificats, afin de créer votre zone de confiance personnelle.

4.7.2.1 Certificats détenus :

SoftwareCIM fournit trois types de certificats pour accéder à la configuration web et configurer le serveur SGLAN en toute sécurité. Le certificat SoftwareCIM intégré est la solution par défaut.

Type de certificat	Source	Restriction de taille (octets)
Certificat SoftwareCIM intégré	Signé par le module LOGO! Base	1024
Certificat SoftwareCIM interne	Généré par SoftwareCIM	1024
Certificat externe	Chargé dans SoftwareCIM par vos soins	4000

Télécharger le certificat SoftwareCIM intégré

Le certificat SoftwareCIM intégré est créé pendant la production.

1. Sélectionnez "Certificat LOGO! intégré" en cliquant sur le bouton correspondant.
2. Cliquez sur "Télécharger" pour télécharger le certificat LOGO Root CA.

Certificats possédés

Certificat approuvé

☒ Certificat intégré dans SoftwareCIM

☐ Certificat SoftwareCIM interne

☐ Certificat externe

 **Certificat intégré dans SoftwareCIM:**

- Cette stratégie vous fournit une zone de confiance par défaut par LOGO! Root CA(trust root).
- La chaîne de certification intégrée est créée en mode de production.
- Si une CA racine est préinstallée sur votre PC, vous pouvez accéder à SoftwareCIM sans alerte de sécurité par défaut.

Certificat intégré dans SoftwareCIM Information

Émis par	Émis pour	Valide	Actions
LOGO Root CA V1.0	LOGO Root CA V1.0	6/4/2020 – 7/12/2070	Télécharger

Rejeter les modifications

Enregistrer les modifications

Obtenir le certificat SoftwareCIM interne

SoftwareCIM peut générer un certificat pour lui-même.

1. Sélectionnez le certificat SoftwareCIM interne en cochant la case en regard.
2. Cliquez sur "Générer" pour générer un certificat SoftwareCIM CA.

3. Cliquez sur "Télécharger" pour télécharger le certificat SoftwareCIM CA.
4. Cliquez sur "Enregistrer les modifications" pour enregistrer la modification ou sur "Rejeter les modifications" pour rejeter la modification.

Certificats possédés Certificat approuvé

☐ Certificat intégré dans SoftwareCIM
☒ **Certificat SoftwareCIM interne**
☐ Certificat externe

? **Certificat SoftwareCIM interne:**

- Cette stratégie vous permet de définir votre propre zone de confiance par SoftwareCIM.
- La CA(trust root) interne est changée chaque fois que vous déclenchez une nouvelle génération.
- Vous pouvez exporter la CA interne et la préinstaller sur le PC à des fins de validation.

Certificat SoftwareCIM interne

Émis par	Émis pour	Valide	Actions
LOGOICIM_7984B675	LOGOICIM_7984B675	12/13/2023 -- 11/30/2073	Télécharger







Charger le certificat externe

SoftwareCIM vous permet d'importer votre propre certificat et votre propre clé dans SoftwareCIM.

1. Sélectionnez "Certificat externe" en cliquant sur le bouton correspondant.
2. Cliquez sur le champ Charger pour sélectionner votre propre CA et votre clé.

- 3. Cliquez sur "Importer" pour importer le certificat et la clé dans SoftwareCIM.
- 4. Cliquez sur "Enregistrer les modifications" pour enregistrer la modification ou sur "Rejeter les modifications" pour rejeter la modification.

Certificats possédés

Certificat approuvé

Certificat intégré dans SoftwareCIM

Certificat SoftwareCIM interne

Certificat externe

Certificat externe:

- Cette stratégie aide l'utilisateur à ajouter SoftwareCIM dans sa propre zone de confiance.

- L'utilisateur peut importer sa propre CA et sa propre clé.

Certificat externe Information

Émis par

Émis pour

Valide

Importer un nouveau certificat externe

Sélectionner [Certificat] fichier

Cer

La taille du fichier ne doit pas dépasser 4000 bytes

Le type de paire de clés doit être ecc256 / ecc384.

Sélectionner [Clé privée non cryptée] fichier

Key

La taille du fichier ne doit pas dépasser 1000 bytes

Le type de paire de clés doit être ecc256 / ecc384.

Importer un nouveau certificat externe

Rejeter les modifications

Enregistrer les modifications

4.7.2.2 Certificat de confiance :

Pour créer le SGLAN, vous devez sélectionner le même certificat de confiance dans le serveur et le client. Le certificat SoftwareCIM intégré est la solution par défaut.

Remarque

Assurez-vous que le certificat que vous importez dans SoftwareCIM est en cours de validité.

Type de certificat	Source	Restriction de taille (octets)
Certificat SoftwareCIM intégré	Signé par le module LOGO! Base	1024
Certificat externe	Upload sur le serveur et le client par vos soins ¹	4000

¹ Le certificat externe inclut le certificat créé par SoftwareCIM ou un autre outil de génération.

60

SoftwareCIM
Instructions de service, 01/2024

Importer le certificat externe dans SoftwareCIM

Procédez comme suit pour importer un certificat externe dans SoftwareCIM.

1. Cliquez sur le champ Charger pour sélectionner votre CA.
2. Cliquez sur "Importer un nouveau certificat externe" pour importer le certificat dans SoftwareCIM.
3. Cliquez sur "Enregistrer les modifications" pour enregistrer la modification ou sur "Rejeter les modifications" pour rejeter la modification.

Certificats possédés

Certificat approuvé

Certificat intégré dans SoftwareCIM Information

	Émis par	Émis pour	Valide
	LOGO Root CA V1.0	LOGO Root CA V1.0	6/4/2020 – 7/12/2070

Utiliser le certificat intégré dans SoftwareCIM.

Certificat externe Information

	Émis par	Émis pour	Valide
Importez et utilisez un certificat externe, y compris le certificat créé par SoftwareCIM ou un autre outil de génération.			

Importer un nouveau certificat externe

Sélectionner
[Certificat] fichier

Cer La taille du fichier ne doit pas dépasser 4000 bytes
Le type de paire de clés doit être ecc256 / ecc384.

Importer un nouveau certificat externe

4.8 Paramètres système

4.8.1 Paramètres de l'heure

Cette page vous permet d'effectuer les opérations suivantes pour le SoftwareCIM.

- Vérifiez l'heure actuelle et le fuseau horaire

L'heure et le fuseau horaire de SoftwareCIM sont synchronisés sur l'horloge système du PC.

- Activez/désactivez le serveur NTP.
- Activez/désactivez le mappage de l'heure sur le modèle UDM.

Paramètres de l'heure

Heure actuelle: 2023-12-06 10:57:43

 Informations sur l'espace d'adressage d'heure

Fuseau horaire: (UTC+08: 00) Beijing, Chongqing, Hong Kong, Urumqi ▼

Activer le serveur NTP: ☐

Mapper l'heure sur UDM: ☐

 Rejeter les modifications

 Enregistrer les modifications

Remarque

Si l'heure de SoftwareCIM se situe hors de la plage définie par le certificat, SoftwareCIM générera un nouveau certificat. La page peut être figée pendant quelques secondes durant la génération du certificat.

4.8.2 Changer le mot de passe

Cette page permet de changer le mot de passe de connexion à SoftwareCIM.

Remarque

Si vous n'avez pas changé le mot de passe, vous pouvez vous connecter avec le mot de passe par défaut cim.

Siemens vous recommande vivement de changer le mot de passe par défaut après la première connexion au SoftwareCIM.

Si vous avez oublié le mot de passe, vous devez désinstaller et réinstaller SoftwareCIM, puis rejeter la configuration précédente. Après la réinstallation, vous pouvez vous connecter à SoftwareCIM à l'aide du mot de passe par défaut.

Pour changer le mot de passe, vous devez d'abord saisir le mot de passe actuel, puis saisir le nouveau mot de passe et le saisir une nouvelle fois pour confirmation. Le mot de passe ne doit pas avoir plus de 32 caractères.

4.8.3 Réinitialisation du système

Cette page permet de redémarrer le service SoftwareCIM ou de réinitialiser la configuration du SoftwareCIM aux paramètres d'usine.

Redémarrer

Vous pouvez cliquer sur le bouton "Redémarrer" pour redémarrer le service SoftwareCIM.

Remarque

Les données dans le modèle UDM sont effacées après un redémarrage du service SoftwareCIM.

Réinitialisation aux paramètres d'usine

Si vous appuyez sur le bouton "Réinitialisation aux paramètres d'usine", toute la configuration SoftwareCIM reprend les valeurs par défaut.

Remarque

Avant de procéder à la réinitialisation aux paramètres d'usine, créez une copie de sauvegarde des données de configuration à l'aide de **Paramètres système --> Gestion de la configuration système**.

Le certificat intégré (Page 57) est conservé après la réinitialisation aux paramètres d'usine.

4.8.4 Gestion de la configuration système

Cette fonction permet d'exporter la configuration SoftwareCIM actuelle ou d'importer un fichier de configuration SoftwareCIM dans SoftwareCIM.

Remarque

Le fichier de configuration exporté n'est utilisable que pour SoftwareCIM.

Exporter le fichier de configuration

1. Cliquez sur le bouton "Exporter le fichier de configuration".
2. Activez ou désactivez l'option "Protéger le fichier avec un mot de passe" et définissez le mot de passe si vous voulez protéger le fichier de configuration de tout usage intempestif.

Remarque

Les données de configuration suivantes ne sont pas exportées :

- Adresse IP
 - Mot de passe
 - Certificat
 - Clé
 - Horloge
 - Réseau
-

Importer le fichier de configuration

1. Cliquez sur le bouton "Importer le fichier de configuration".
2. Naviguez jusqu'au dossier où vous avez sauvegardé le fichier de configuration et sélectionnez-le.
3. Saisissez le mot de passe si le fichier de configuration est protégé.

Mise à jour de SoftwareCIM

SoftwareCIM peut être mis à jour à l'aide des méthodes suivantes :

- mise à jour en installant le pack de mise à jour (Page 65)
- mise à jour avec la configuration SoftwareCIM (Page 65)

5.1 Mise à jour en installant le pack de mise à jour

procédez comme suit pour mettre à jour SoftwareCIM en installant le pack de mise à jour :

1. Téléchargez le pack de mise à jour sur le site de Siemens (<http://www.siemens.com/>).
2. Enregistrez le pack de mise à jour sur le PC d'installation de SoftwareCIM.
3. Décompressez le fichier de pack de mise à jour.
4. Cliquez sur le fichier .exe pour lancer la mise à jour.

Pour mettre à jour le SoftwareCIM qui a été déployé sur le cloud, vous pouvez utiliser la fonction de connexion Bureau à distance pour transférer et installer le pack de mise à jour.

Remarque

Pour des raisons de sécurité, Siemens vous recommande de mettre à jour SoftwareCIM en installant le pack de mise à jour.

5.2 Mise à jour avec la configuration SoftwareCIM

Vous pouvez choisir de mettre à jour SoftwareCIM automatiquement ou manuellement avec la configuration SoftwareCIM.

Mise à jour automatique

Une fois la mise à jour automatique configurée, le SoftwareCIM à mettre à jour vérifiera automatiquement à l'heure donnée si la source de mise à jour configurée propose une version supérieure. Si la source de mise à jour configurée propose une version supérieure, le SoftwareCIM sera mis à jour automatiquement à l'heure donnée.

Avant de configurer la mise à jour automatique pour SoftwareCIM, assurez-vous que le service SoftwareCIM est en cours d'exécution.

Procédez comme suit pour configurer une mise à jour automatique :

1. Cliquez sur "Configurer la mise à jour" dans le menu icône de la barre système (Page 29).
2. Activez Mise à jour automatique.

3. Sélectionnez la source sur le menu déroulant de serveur de mise à jour. Deux sources de mise à jour sont disponibles :

- Serveur SGLAN

Cette source est opérationnelle si le SoftwareCIM à mettre à jour est configuré comme client SGLAN et s'il est connecté à un SoftwareCIM faisant office de serveur SGLAN.

Remarque

Pour que la mise à jour s'effectue correctement, les adresses IP du serveur SGLAN et du client SGLAN doivent se trouver dans le même sous-réseau.

Si vous choisissez cette source, passer à l'étape 6.

The screenshot shows a configuration window for the SGLAN server source. At the top, 'Mise à jour automatique' is toggled on. Below it, 'Serveur de mise à jour' is set to 'Serveur SGLAN'. An orange warning message states: 'Pour que la mise à jour réussisse, assurez-vous que le SoftwareCIM est dans le SGLAN.' At the bottom right is a button labeled 'Enregistrer les modifications'.

- Serveur de mise à jour personnalisé

Si vous choisissez cette source, passer à l'étape 4.

The screenshot shows a configuration window for the custom server source. 'Mise à jour automatique' is toggled on. 'Serveur de mise à jour' is set to 'Serveur de mise à jour pers'. Below, 'Adresse de serveur' is 'https://10.0.0.10'. 'Certificat' is toggled on. A dashed red box contains a cloud icon with an upward arrow and the text 'Sélectionner [Certificat] fichier'. An orange warning message states: 'Pour que la mise à jour réussisse, assurez-vous que le serveur de mise à jour personnalisé est accessible. Si le certificat est activé, veuillez charger un certificat de serveur valide.' At the bottom right is a button labeled 'Enregistrer les modifications'.

4. Entrez l'adresse du serveur.
5. Activez le certificat et téléchargez le certificat de confiance. Vous pouvez désactiver Certificat et passer cette étape. Pour des raisons de sécurité, Siemens vous recommande de créer et de télécharger votre propre certificat de confiance.
6. Cliquez sur "Enregistrer les modifications".

Si vous voulez mettre à jour votre SoftwareCIM depuis le serveur de mise à jour personnalisé, vous devez copier les fichiers de mise à jour sur le serveur en plus de la configuration ci-dessus. Vous trouverez les fichiers de mise à jour requis dans le dossier d'installation après avoir installé la dernière version du SoftwareCIM sur votre PC local. Les fichiers de mise à jour sont stockés dans le chemin : "...SIMATIC SoftwareCIM -> resources -> update".

L'image suivante est un exemple de tous les fichiers de mise à jour requis :

Files > Siemens > SIMATIC SoftwareCIM > resources > update		
Name	Date modified	Type
ReleaseNote.md	12/20/2023 7:37 PM	Markdown Source...
SoftwareCIMLocalInstaller.exe	12/20/2023 7:37 PM	Application
VersionInfo.JSON	12/21/2023 3:53 PM	JSON Source File
WebCertificateState.JSON	12/20/2023 7:37 PM	JSON Source File
WebUpdateConfig.JSON	12/20/2023 7:37 PM	JSON Source File

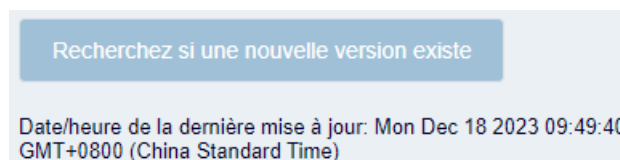
Remarque

N'apportez aucune modification aux fichiers de mise à jour. Si vous le faites, la mise à jour échouera.

Mise à jour manuelle

Avant la mise à jour manuelle de SoftwareCIM, configurez la mise à jour automatique comme indiqué plus haut. Procédez comme suit :

1. Cliquez sur "Actualiser" dans le menu icône de la barre système (Page 29).
2. Cliquez sur "Recherchez si une nouvelle version existe".



3. Si une version supérieure de la source de mise à jour configurée est détectée, cliquez sur "Actualiser" pour mettre à jour le SoftwareCIM.

Dépannage de SoftwareCIM

Ce chapitre vous donne des conseils sur la manière de détecter les problèmes et d'y remédier.

Problème	Cause possible	Solution possible
Impossible d'accéder au service SoftwareCIM	L'adaptateur virtuel SGLAN est inactif ou désinstallé.	Activez l'adaptateur virtuel SGLAN sur le PC.
Impossible d'accéder à SoftwareCIM via l'adresse IP WAN	- Le port 443 est occupé par une autre application ou un autre service sur le PC - Le service SoftwareCIM est arrêté - Erreur du navigateur web	- Vérifiez si le port 443 est occupé - Démarrez le service SoftwareCIM - Videz le cache et redémarrez le navigateur
Le temps du client NTP n'est pas synchronisé sur le SoftwareCIM configuré en tant que serveur NTP	Le service NTP du PC sur lequel est installé SoftwareCIM n'est pas désactivé.	Désactivez le service NTP sur le PC.
Échec de la communication Modbus RTU	Le mode port série du maître Modbus RTU et de l'esclave Modbus RTU n'est pas cohérent.	- Vérifiez et configurez le mode port série de SoftwareCIM dans le BIOS du PC - Vérifiez et configurez le mode port série de l'appareil CIM dans la page de configuration basée web
Impossible d'accéder au SoftwareCIM sur le cloud via le navigateur Web avec un message d'erreur indiquant une heure incorrecte	L'heure système du navigateur Web est incohérente avec l'heure du serveur Web sur le cloud.	Modifiez l'heure système Windows afin qu'elle corresponde à l'heure système du serveur Web sur le cloud.

Dépannage de SGLAN

État de la connexion	Description	Cause possible
Erreur de connexion	Impossible d'établir la communication entre le client SGLAN et le serveur SGLAN.	Si le mode est IPv4 ou IPv6 : - L'adresse IP est erronée - L'adresse IP est inaccessible. - Le client SGLAN ne peut pas accéder à Internet
Échec de la connexion	Échec de la connexion en raison d'une erreur de mot de passe.	Vérifiez le mot de passe.
Erreur de certificat	Échec de la vérification du certificat.	- Le certificat de confiance n'est pas le certificat détenu ou n'est pas le certificat de confiance du serveur SGLAN - Le certificat expire

Dépannage de l'état du système

Message d'erreur	Cause possible	Solution possible
Impossible de connecter l'embase du serveur	Le port correspondant est occupé par un autre processus. SoftwareCIM utilise les ports suivants : • Serveur SGLAN : port 8444 • Serveur S7 : port 102 • Serveur Modbus TCP : port 502 • Serveur NTP : port 123	Libérez le port correspondant pour que SoftwareCIM fonctionne.
Impossible d'obtenir l'adresse IPv4 de l'adaptateur LAN	• L'adaptateur LAN est inactif • La configuration de l'adaptateur LAN est invalide • L'adaptateur LAN est endommagé	• Activez l'adaptateur LAN • Configurez l'adaptateur LAN en utilisant l'adresse IPv4 statique • Réinstallez SoftwareCIM
Impossible de configurer le port COM	• Le port COM est indisponible • L'option de configuration sélectionnée n'est pas prise en charge	• Vérifiez si le port COM est disponible • Réessayez avec d'autres options de configuration
Impossible d'obtenir l'adresse IPv6 de l'adaptateur WAN	• L'adaptateur WAN sélectionné est inactif • L'adaptateur WAN sélectionné est indisponible • L'adaptateur WAN sélectionné ne dispose d'aucune adresse Ipv6 valide	• Activez l'adaptateur WAN sélectionné • Sélectionnez un autre adaptateur WAN • Assurez-vous que l'hôte peut accéder à Internet via l'adaptateur WAN sélectionné • Utilisez IPv4 si IPv6 n'est pas disponible
Impossible d'obtenir l'adresse IPv4 de l'adaptateur WAN	• L'adaptateur WAN sélectionné est inactif • L'adaptateur WAN sélectionné est indisponible • L'adaptateur WAN sélectionné ne dispose d'aucune adresse IPv4 valide	• Activez l'adaptateur WAN sélectionné • Sélectionnez un autre adaptateur WAN • Assurez-vous que l'hôte peut accéder à Internet via l'adaptateur WAN sélectionné

Conseils et astuces

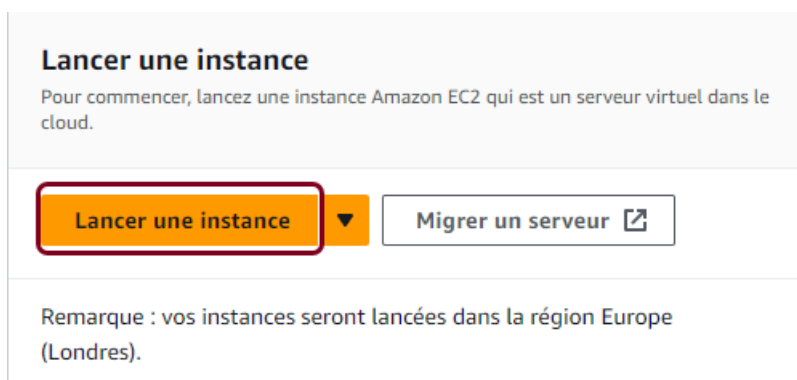
7.1 Comment déployer manuellement SoftwareCIM sur AWS

Vous pouvez également déployer le SoftwareCIM manuellement sur le cloud AWS. Pour que l'opération réussisse, assurez-vous que le compte AWS respecte les conditions d'autorisation (Page 12).

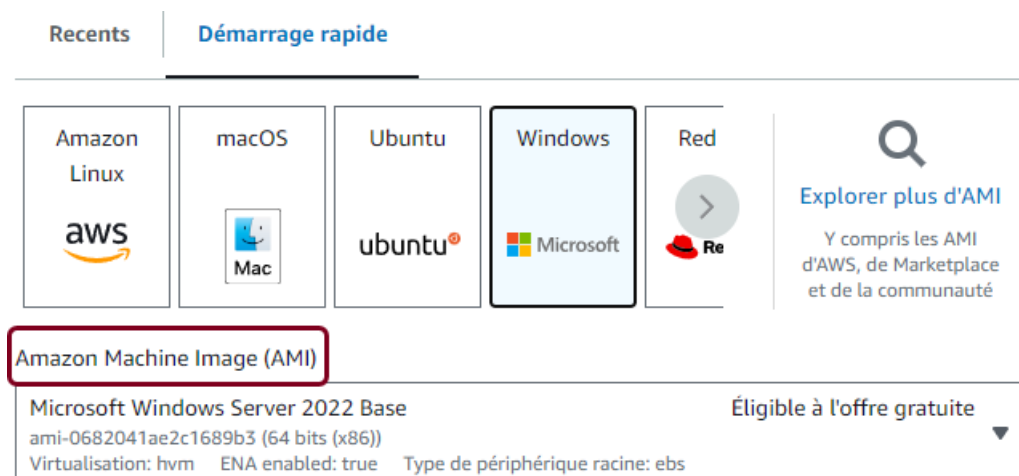
Procédez comme suit pour déployer manuellement SoftwareCIM sur le cloud AWS :

Création d'une instance EC2

1. Connectez-vous à la console de gestion AWS EC2.
2. Sélectionnez la région à proximité de l'affichage du compte. SoftwareCIM sera déployé sur le cloud de cette région.
3. Cliquez sur "Lancer l'instance".



4. Sélectionnez l'Amazon Machine Image (AMI) dans Windows OS.



5. Sélectionnez un type d'instance avec au moins une CPU double cœur et 2 Go de mémoire.

▼ **Type d'instance** [Informations](#) | [Get advice](#)

Type d'instance

t2.micro Éligible à l'offre gratuite

Famille: t2 1 vCPU 1 Gio Mémoire Génération actuelle: true

À la demande Windows base tarification: 0.0178 USD par heure

À la demande RHEL base tarification: 0.0732 USD par heure

À la demande SUSE base tarification: 0.0132 USD par heure

À la demande Linux base tarification: 0.0132 USD par heure

☐ Toutes les générations

[Comparer les types d'instance](#)

Des frais supplémentaires s'appliquent pour les AMI avec un logiciel préinstallé

6. Créez une nouvelle paire de clés.

Vous devez enregistrer la clé privée générée dans un endroit sûr et accessible, car elle vous servira ultérieurement à vous connecter à l'instance.

▼ **Paire de clés (connexion)** [Informations](#)

Vous pouvez utiliser une paire de clés pour vous connecter en toute sécurité à votre instance. Assurez-vous d'avoir accès à la paire de clés sélectionnée avant de lancer l'instance.

Nom de la paire de clés - *obligatoire*

Pour les instances Windows, vous utilisez une paire de clés pour déchiffrer le mot de passe administrateur. Vous utilisez ensuite le mot de passe déchiffré pour vous connecter à votre instance.

7. Configurez les paramètres réseau.

- Désactivez l'IP publique auto-attribuée. Une adresse IP Elastic sera utilisée pour SoftwareCIM.

▼ Paramètres réseau [Informations](#)

VPC - required [Informations](#)

vpc-23c0b64b
172.31.0.0/16

(par défaut) ▼

↻

Sous-réseau [Informations](#)

Aucune préférence ▼

↻

[Créer un nouveau sous-réseau](#) [↗](#)

Attribuer automatiquement l'adresse IP publique [Informations](#)

Désactiver ▼

- Créez un groupe de sécurité et ajoutez les règles de groupe de sécurité. Les règles de groupe de sécurité HTTPS/port 443, Custom UDP/port 8444 et Custom TCP/port 102 sont obligatoires. RDP/port 3389 et ssh/port 22 sont facultatives, elles simplifient la connexion à d'autres transactions.

7.1 Comment déployer manuellement SoftwareCIM sur AWS

Pare-feu (groupes de sécurité) Informations

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

☒ Créer un groupe de sécurité☐ Sélectionner un groupe de sécurité existant

Nom du groupe de sécurité - obligatoire

Ce groupe de sécurité sera ajouté à toutes les interfaces réseau. Le nom ne peut pas être modifié après la création du groupe de sécurité. La longueur maximale est de 255 caractères. Caractères valides : a-z, A-Z, 0-9, espaces et _ - : / () # , @ [] + = & ; { } ! \$ *

Description - obligatoire Informations

Règles entrantes des groupes de sécurité

▼ Security group rule 1 (TCP, 3389, 0.0.0.0/0) Supprimer

Type Informations	Protocole Informations	Plage de ports Informations
rdp	TCP	3389
Type de source Informations	Source Informations	Description - optional Informations
N'importe où	Ajouter une adresse CIDR, u 0.0.0.0/0 X	e.g. SSH for admin desktop

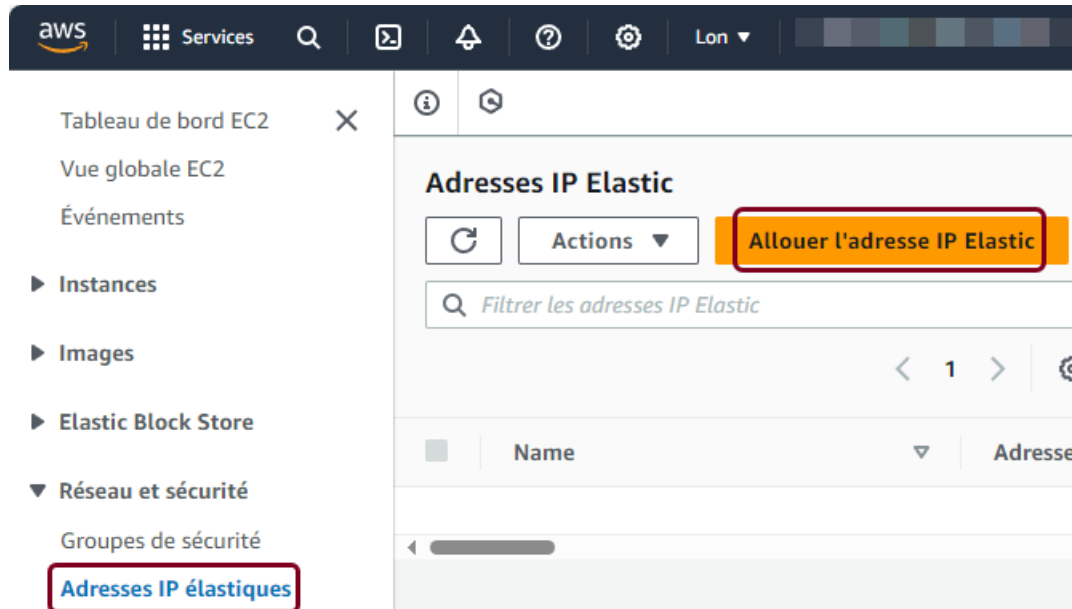
8. Cliquez sur "Lancer l'instance".

9. Vérifiez les règles d'entrée.

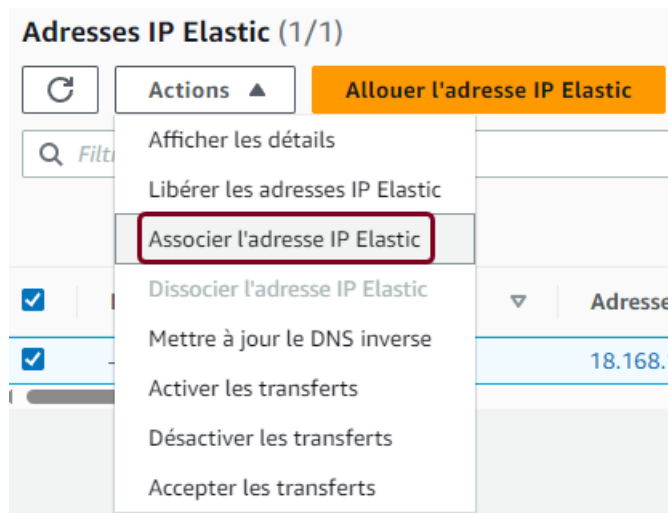
Règles entrantes Informations						
ID de règle de groupe de sécurité	Type Informations	Protocole Informations	Plage de ports Informations	Source Informations		
sgr-04ea2b63edf1a57a3	TCP personnalisé	TCP	102	Person...	Q	0.0.0.0/0 X
sgr-0b174f6cf9922ef54	HTTPS	TCP	443	Person...	Q	0.0.0.0/0 X
sgr-0ca806d1f90ed7488	RDP	TCP	3389	Person...	Q	0.0.0.0/0 X
sgr-00a92a16722b18145	UDP personnalisé	UDP	8444	Person...	Q	0.0.0.0/0 X

Association de l'adresses IP Elastic à l'instance

1. Allez à Réseau et sécurité -> Adresses IP Elastic dans la console de gestion AWS EC2.
2. Cliquez sur "Allouer l'adresse IP Elastic".



3. Sélectionnez l'adresse IP Elastic nouvellement créée sur la liste et cliquez sur "Associer l'adresse IP Elastic" dans le menu Actions.



4. Sélectionnez l'instance créée ci-dessus et cliquez sur "Associer".

Associer l'adresse IP Elastic Informations

Choisissez l'instance ou l'interface réseau à associer à cette adresse IP Elastic (18.168.130.252)

Adresse IP Elastic: 18.168.130.252

Type de ressource
Choisissez le type de ressource auquel l'adresse IP Elastic doit être associée.

☒ instance

☐ Interface réseau

instance

Adresse IP privée
L'adresse IP privée à laquelle associer l'adresse IP Elastic.

Réassociation
Spécifiez si l'adresse IP Elastic peut être réassociée à une autre ressource si elle est déjà associée à une ressource.

☐ Autoriser la réassociation de cette adresse IP Elastic

Annuler **Associer**

Connexion au PC virtuel sur le cloud AWS

1. Revenir à l'instance précédemment créée. Cliquez sur "Se connecter".

Tableau de bord EC2 X

Vue globale EC2

Événements

Console-to-Code [Aperçu](#)

▼ Instances

Instances

Types d'instances

EC2 > Instances > i-09c564bebe18fa272

Résumé de l'instance pour i-09c564bebe18fa272 (cim_longterm_1205) Informations

État de l'instance ▼ Actions ▼

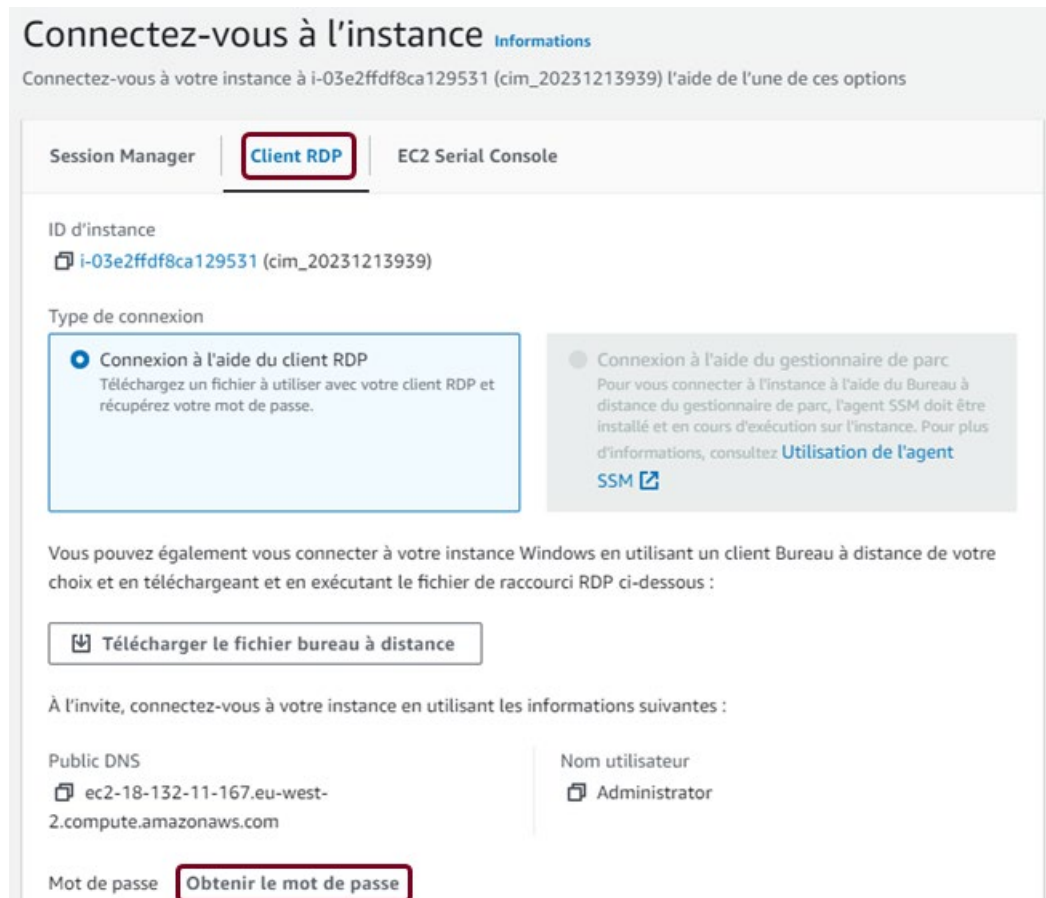
Mis à jour il y a less than a minute

ID d'instance
i-09c564bebe18fa272 (cim_longterm_1205)

Adresse IPv4 publique
adresse ouvert

7.1 Comment déployer manuellement SoftwareCIM sur AWS

2. Cliquez sur "Client RDP" et sélectionnez "Connexion à l'aide du client RDP". Cliquez sur "Obtenir le mot de passe".



3. Chargez la clé privée générée auparavant et cliquez sur "Déchiffrer le mot de passe". Vous obtenez ainsi le mot de passe de connexion au PC Windows virtuel.
4. Connectez-vous au PC virtuel sur le cloud AWS via RDP.

Déploiement de SoftwareCIM sur le cloud AWS - option 1

1. Chargez le programme "SoftwareCIMInstaller.exe" sur votre PC local depuis Siemens.
2. Envoyez le programme d'installation au PC virtuel via RDP. Ce processus peut prendre un certain temps.
3. Double-cliquez sur "SoftwareInstaller.exe" pour installer le SoftwareCIM sur le PC virtuel.

4. Connectez-vous à SoftwareCIM.
5. Activez "Accéder à SoftwareCIM via WAN" sous Paramètres avancés sur la page Paramètres réseau et entrez l'adresse IP Elastic dans le champ Nom d'hôte. Cliquez sur "Enregistrer les modifications".

Vous pouvez maintenant utiliser l'adresse IP Elastic pour accéder de manière sécurisée à SoftwareCIM.

Remarque

Le SoftwareCIM déployé est configuré en tant que serveur SGLAN uniquement si vous renseignez le champ Nom d'hôte avec l'adresse IP Elastic.

Accéder à SoftwareCIM via WAN : ☐ ?

Nom d'hôte : 0/253 ?

Déploiement de SoftwareCIM sur le cloud AWS - option 2

1. Exécutez "SoftwareCIMInstaller.exe" et installez SoftwareCIM sur votre PC local.
2. Une fois l'installation terminée, ouvrez le dossier d'installation de SoftwareCIM.
3. Recherchez "SoftwareCIMLocalInstaller.exe" dans le chemin "...SIMATIC SoftwareCIM -> resources -> update" et envoyez-le au PC virtuel via RDP.

Name			Date modified	Type
ReleaseNote.md			12/20/2023 7:37 PM	Markdown Source...
SoftwareCIMLocalInstaller.exe			12/20/2023 7:37 PM	Application
VersionInfo.JSON			12/21/2023 3:53 PM	JSON Source File
WebCertificateState.JSON			12/20/2023 7:37 PM	JSON Source File
WebUpdateConfig.JSON			12/20/2023 7:37 PM	JSON Source File

4. Double-cliquez sur "SoftwareCIMLocalInstaller.exe" pour installer SoftwareCIM sur le PC virtuel.

7.1 Comment déployer manuellement SoftwareCIM sur AWS

5. Connectez-vous à SoftwareCIM.
6. Activez "Accéder à SoftwareCIM via WAN" sous Paramètres avancés sur la page Paramètres réseau et entrez l'adresse IP Elastic dans le champ Nom d'hôte. Cliquez sur "Enregistrer les modifications".

Vous pouvez maintenant utiliser l'adresse IP Elastic pour accéder de manière sécurisée à SoftwareCIM.

Remarque

Le SoftwareCIM déployé est configuré en tant que serveur SGLAN uniquement si vous renseignez le champ Nom d'hôte avec l'adresse IP Elastic.

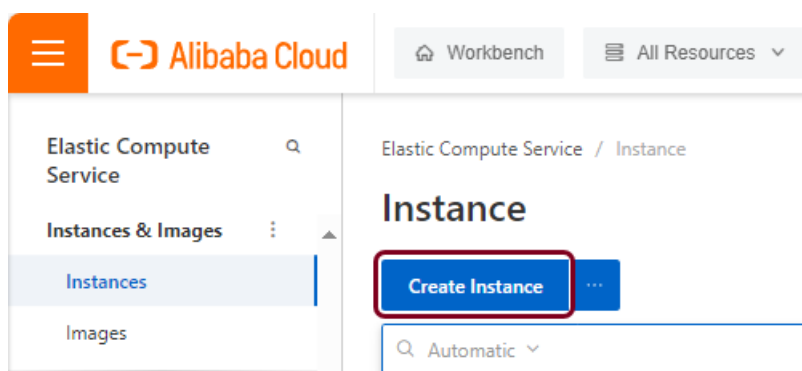
7.2 Comment déployer manuellement SoftwareCIM sur Alibaba

Vous pouvez également déployer le SoftwareCIM manuellement sur Alibaba Cloud. Pour que l'opération réussisse, assurez-vous que le compte Alibaba respecte les conditions d'autorisation (Page 20).

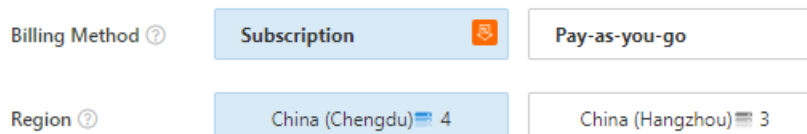
Procédez comme suit pour déployer manuellement SoftwareCIM sur le cloud Alibaba :

Création d'une instance ECS

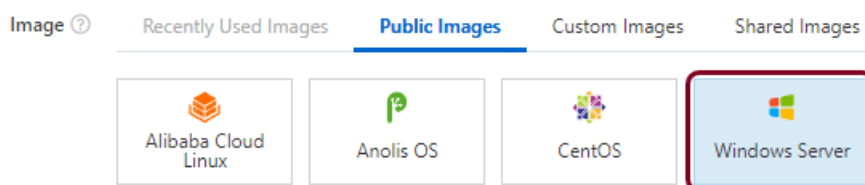
1. Connectez-vous à la console Alibaba ECS.
2. Cliquez sur "Create Instance".



3. Sélectionnez Billing Method et Region.



4. Configurez l'instance selon vos besoins.
5. Sélectionnez le serveur Windows comme image.



7.2 Comment déployer manuellement SoftwareCIM sur Alibaba

- Configurez la bande passante et les groupes de sécurité. Vous devez sélectionner Pay-by-traffic sous Bandwidth Billing Method, sinon vous ne pourrez pas obtenir d'adresse IP Elastic plus tard.

Bandwidths & Security Groups

Public IP Address ☒ Assign Public IPv4 Address
The system assigns an IP address. You can also use a more flexible EIP solution. For more information, see [Configure and associate an EIP](#).

Bandwidth Billing Method

Maximum Bandwidth Mbps Mbps
Alibaba Cloud provides a DDoS mitigation capacity of up to 5 Gbit/s free of charge. [Learn More >](#) | [Improve Mitigation Capacity >](#)

Security Group
Configure a security group

Security Group Name

Security Group Type [Comparison Between Basic and Advanced Security Groups](#)

Open IPv4 Ports

☒ SSH (22)	☐ telnet (23)	☐ HTTP (80)
☒ HTTPS (443)	☐ MS SQL (1433)	☐ Oracle (1521)
☐ MySQL (3306)	☒ RDP (3389)	☐ PostgreSQL (5432)
☐ Redis (6379)		

- Configurez le mot de passe de connexion au PC Windows virtuel.

Management

Logon Credential
Key pairs provide higher security than custom passwords and can prevent brute-force attacks. We recommend

Logon Username ☐ root ☐ ecs-user

Logon Password 

Confirm Password 

- Cliquez sur "Create Order".

Obtenir une adresse IP Elastic

- Allez à Instance sur la console Alibaba ESC.
- Cliquez sur l'instance précédemment créée.

3. Cliquez sur "Convert to EIP" à proximité de l'adresse IP publique.

Configuration Information

Instance Type
ecs.ic5.large [Change](#) | [Purchase Same Specifications](#)

CPU and Memory
2 Cores (vCPUs) 2 GiB

Public IP Address
47.108.145.126 [Convert to EIP](#)

4. Allez à Security Groups et cliquez sur votre groupe de sécurité.

Elastic Compute Service / Instance / i-2vcejf3e1aomkl64nej

← QR2daytest Running

Instance Details | Monitoring | **Security Groups** | Disks | Snapshot-cor

Internal Inbound Rules | Internal Outbound Rules | **Security Groups**

[Modify a security group](#)

☐	security group ID/NAME	Tag	network
☐	sg-2vc2iy7g5tupyk9mti7j sgcim-e5lnbc6f16bk		vpc-2vcxtg46uopjzv4cw4csz

5. Cliquez sur "Add Rule". Ajoutez une règle de groupe de sécurité : Custom UDP/port 8444 et Custom TCP/port 443.

Inbound | Outbound

[Add Rule](#) | Quick Add |

Action	Priority ①	Protocol Type	Port Range ①
☐ Allow	1	Custom TCP	Dest 22/22
☐ Allow	1	Custom UDP	Dest 8444/8444
☐ Allow	1	Custom TCP	Dest 3389/3389
☐ Allow	1	Custom TCP	Dest 443/443

6. Vous pouvez maintenant vous connecter au PC virtuel sur Alibaba Cloud via RDP.

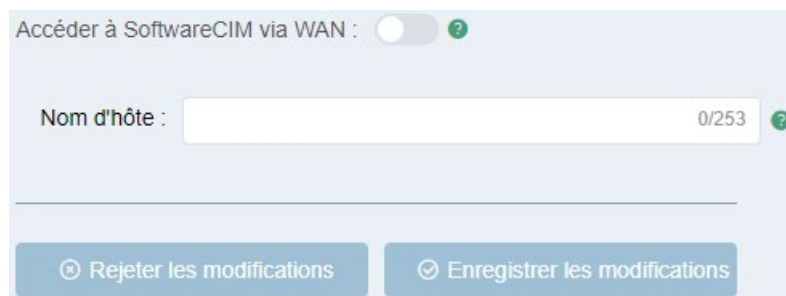
Déploiement de SoftwareCIM sur Alibaba Cloud - option 1

1. Chargez le programme "SoftwareCIMInstaller.exe" sur votre PC local depuis Siemens.
2. Envoyez le programme d'installation au PC virtuel via RDP. Ce processus peut prendre un certain temps.
3. Double-cliquez sur "SoftwareInstaller.exe" pour installer le SoftwareCIM sur le PC virtuel.
4. Connectez-vous à SoftwareCIM.
5. Activez "Accéder à SoftwareCIM via WAN" sous Paramètres avancés sur la page Paramètres réseau et entrez l'adresse IP Elastic dans le champ Nom d'hôte. Cliquez sur "Enregistrer les modifications".

Vous pouvez maintenant utiliser l'adresse IP Elastic pour accéder de manière sécurisée à SoftwareCIM.

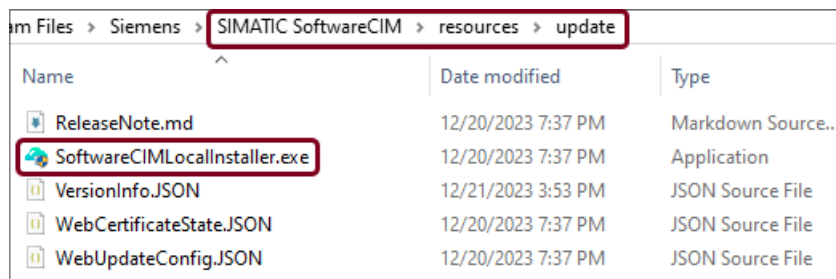
Remarque

Le SoftwareCIM déployé est configuré en tant que serveur SGLAN uniquement si vous renseignez le champ Nom d'hôte avec l'adresse IP Elastic.



Déploiement de SoftwareCIM sur Alibaba Cloud - option 2

1. Exécutez "SoftwareCIMInstaller.exe" et installez SoftwareCIM sur votre PC local.
2. Une fois l'installation terminée, ouvrez le dossier d'installation de SoftwareCIM.
3. Recherchez "SoftwareCIMLocalInstaller.exe" dans le chemin "...SIMATIC SoftwareCIM -> resources -> update" et envoyez-le au PC virtuel via RDP.



4. Double-cliquez sur "SoftwareCIMLocalInstaller.exe" pour installer SoftwareCIM sur le PC virtuel.

5. Connectez-vous à SoftwareCIM.
6. Activez "Accéder à SoftwareCIM via WAN" sous Paramètres avancés sur la page Paramètres réseau et entrez l'adresse IP Elastic dans le champ Nom d'hôte. Cliquez sur "Enregistrer les modifications".

Vous pouvez maintenant utiliser l'adresse IP Elastic pour accéder de manière sécurisée à SoftwareCIM.

Remarque

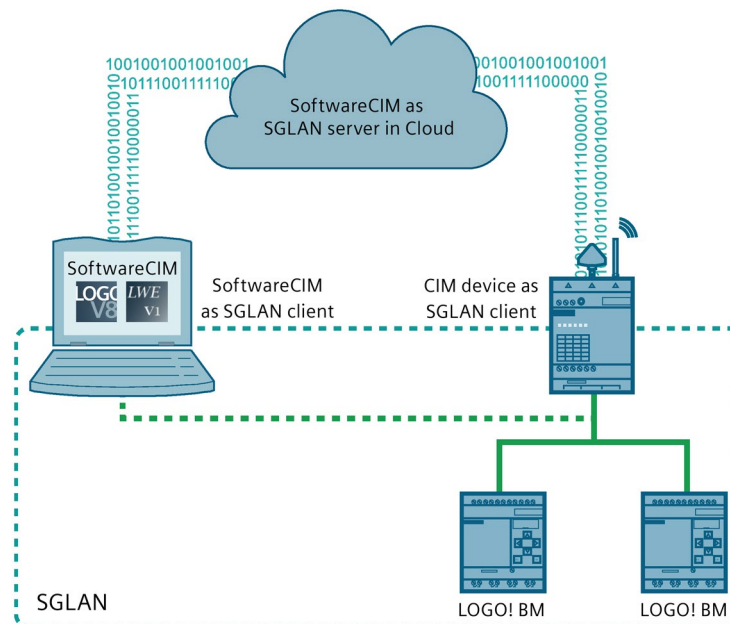
Le SoftwareCIM déployé est configuré en tant que serveur SGLAN uniquement si vous renseignez le champ Nom d'hôte avec l'adresse IP Elastic.

Exemple pratique

8.1 Télécharger un programme à distance sur LOGO! BM

Cet exemple pratique montre comment télécharger à distance un programme sur LOGO! BM via SGLAN. Vous apprendrez à déployer un SoftwareCIM sur Alibaba cloud comme serveur SGLAN et à connecter les clients SGLAN au serveur SGLAN.

Le schéma suivant montre le fonctionnement d'un tel système :



Conditions

- Le PC sur lequel SoftwareCIM doit être installé doit respecter les conditions suivantes :
 - dispose d'un accès Internet
 - avec le système d'exploitation Windows 10 (64 bit) (21H2, 22H2) ou Windows 11 (22H2)
- Un compte Alibaba Cloud valide
- Les adresses IP de tous les appareils et de SoftwareCIM sur SGLAN se trouvent dans le même sous-réseau et ne sont pas en conflit les unes avec les autres
- L'appareil CIM à configurer comme client SGLAN doit respecter les conditions suivantes :
 - disposer d'IoT ou d'une carte SIM avec un accès à Internet et d'une adresse IPv4

Configuration du serveur SGLAN sur Alibaba Cloud

1. Exécutez "SoftwareCIMInstaller.exe" et choisissez de déployer SoftwareCIM sur Alibaba Cloud.
2. Saisissez l'ID de clé d'accès et la clé d'accès secrète pour vous connecter à Alibaba Cloud. Cliquez sur "Suivant".

3. Sélectionnez Région Sélectionnez "Créer une nouvelle instance". Cliquez sur "Suivant".

4. Renseignez les champs Nom d'instance et Description. Sélectionnez Image de machine, Règle de groupe de sécurité et Type d'instance. Cliquez sur "Suivant".

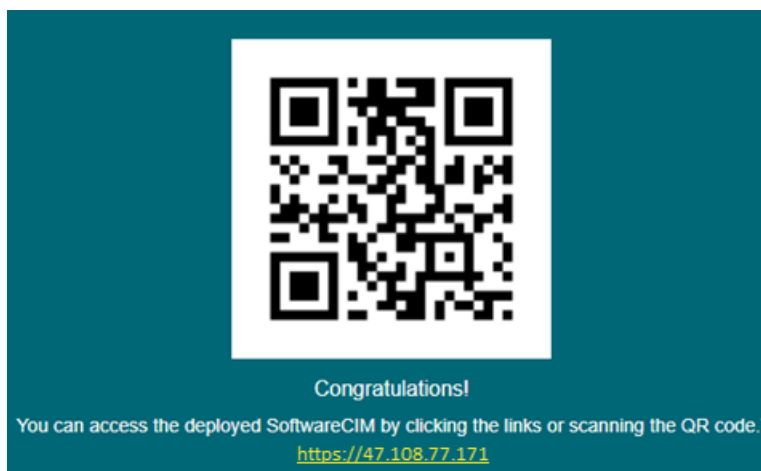
Type d'instance	Catégorie d'instance	Taille de la mémoire	Coeur de CPU	Bande passante	Nombre maximum de clients SGLAN
ecs.ic5.large	Compute-optimiz	2 GB	2	5 Mbps	50
ecs.c6.large	Compute-optimiz	4 GB	2	10 Mbps	200
ecs.c6.xlarge	Compute-optimiz	8 GB	4	20 Mbps	500

5. Cliquez sur "Ignorer" et acceptez le certificat Siemens par défaut.

8.1 Télécharger un programme à distance sur LOGO! BM

6. Définissez des mots de passe pour le compte Windows, le compte SoftwareCIM et le compte SGLAN.
7. Cliquez sur "Déployer" pour lancer le déploiement.

Une fois le déploiement terminé avec succès, vous voyez un QR code et un lien dans la fenêtre. Le SoftwareCIM déployé est configuré par défaut comme serveur SGLAN. Enregistrez le QR code ou le lien pour un usage ultérieur. Dans ce cas, l'IP publique du serveur SGLAN est 47.108.77.171. Enregistrez l'adresse IP publique, car elle servira pour connecter les clients SGLAN au serveur SGLAN.



Configuration de SoftwareCIM sur le PC comme client SGLAN

1. Exécutez "SoftwareCIMInstaller.exe" sur le PC et sélectionnez "Installer sur ce PC".
2. Entrez le mot de passe sur la page de connexion pour vous connecter à SoftwareCIM. Le mot de passe par défaut est cim.
3. Allez sur la page SGLAN et activez "SoftwareCIM comme client SGLAN".
4. Sélectionnez Mode hôte distant comme IPv4.
5. Saisissez l'adresse IPv4 du serveur pour "Hôte distant". L'adresse IP est 47.108.77.171.

6. Entrez le mot de passe du serveur. Ce mot de passe est celui du compte SGLAN que vous avez défini lors du déploiement de SoftwareCIM sur le cloud.
7. Cliquez sur "Enregistrer les modifications".

Paramètres SGLAN

SoftwareCIM comme serveur SGLAN: ☐

SoftwareCIM comme client SGLAN: ☒

Serveur Liste de serveurs

Mode hôte distant: IPv4

ⓘ Veuillez confirmer que le mode du serveur SGLAN est IPv4.

Remote Host: 47 . 107 . 77 . 171

Mot de passe du serveur: 64/64

Statistiques:

Nom	Statistiques des données SGLAN
Nom de serveur	Alibaba Cloud SGLAN Server
IP du réseau local du serveur	192.168.10.182
Server LAN Mask	255.255.255.0
État	Connecté
Temps de connexion	00:05:36
Octets envoyés	1.109 MB
Octets reçus	319.501 KB
Envoyer vitesse	974 B/S
Recevoir vitesse	1.527 KB/S

Configuration de l'appareil CIM comme client SGLAN

1. Accédez aux pages de configuration basées web de l'appareil CIM et connectez-vous. Vous pouvez constater que les pages de configuration sont différentes de celles de SoftwareCIM.
2. Vérifiez l'état cellulaire.
3. Allez sur la page SGLAN et activez "CIM comme client SGLAN".
4. Sélectionnez Mode hôte distant comme IPv4.
5. Saisissez l'adresse IPv4 du serveur pour "Hôte distant". L'adresse IP est 47.108.77.171.

8.1 Télécharger un programme à distance sur LOGO! BM

6. Entrez le mot de passe du serveur. Ce mot de passe est celui du compte SGLAN que vous avez défini lors du déploiement de SoftwareCIM sur le cloud.
7. Cliquez sur "Enregistrer les modifications".

Paramètres SGLAN

CIM comme serveur SGLAN: ☐

CIM comme client SGLAN: ☒

Serveur

Liste de serveurs

Mode hôte distant: IPv4

?

 Veuillez confirmer que le mode du serveur SGLAN est IPv4.

Remote Host:

47 . 108 . 77 . 171

Mot de passe du serveur:

..... 64/64

Statistiques:

Nom	Statistiques des données SGLAN
Nom de serveur	Alibaba Cloud SGLAN Server
IP du réseau local du serveur	192.168.10.182
État	Connecté ?
Temps de connexion	00:09:14
Octets envoyés	1.062 MB
Octets reçus	250.924 KB
Envoyer vitesse	2.988 KB/S
Recevoir vitesse	1.551 KB/S

Vérification de l'état de la connexion des clients au serveur

1. Allez sur la plateforme de configuration basée sur le web de SoftwareCIM sur Alibaba Cloud à l'aide du lien que vous avez enregistré après le déploiement.
2. Connectez-vous à la plateforme de configuration.
3. Allez à la page SGLAN. Vous pouvez vérifier l'état de la connexion au client SGLAN ici.

Paramètres SGLAN

SoftwareCIM comme serveur SGLAN: ☒

SoftwareCIM comme client SGLAN: ☐

SoftwareCIM comme serveur SGLAN

Mode:

Mot de passe d'accès :

Confirmer le mot de passe d'accès :

Serveur IP: 47.108.77.171

Statistiques

Octets envoyés	Octets reçus	Envoyer vitesse	Recevoir vitesse
1.336 MB	2.836 MB	4.090 KB/S	3.823 KB/S

État de la connexion du client

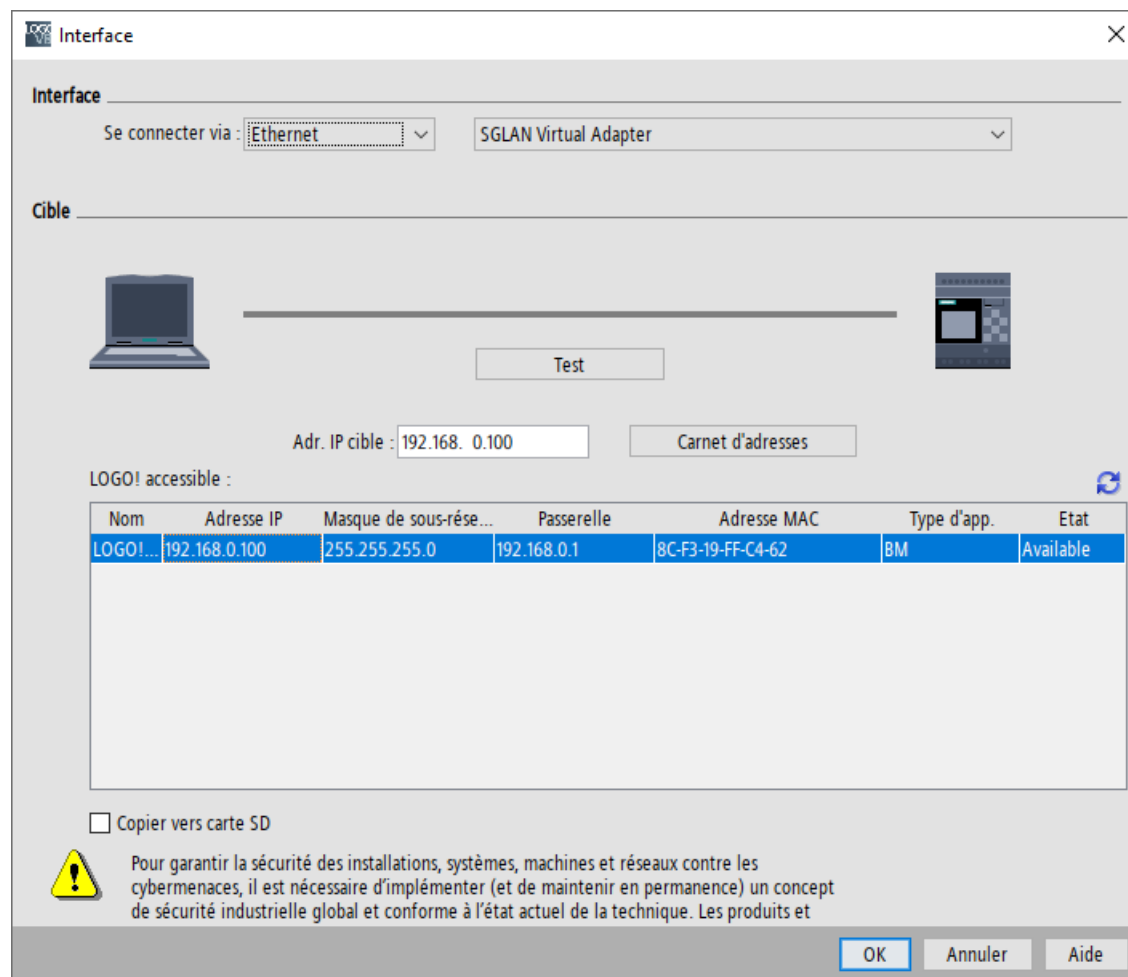
données de la liste de filtres

#	Name	IP du réseau local	LAN Mask	Status
1	CIM-192.168.10.89	192.168.10.89	255.255.255.0	authorized
2	SoftwareCIM SGLAN Client 82	192.168.10.82	255.255.255.0	authorized

Télécharger un programme sur LOGO! BM

1. Testez la connexion au LOGO! BM distant en entrant une commande ping sur le PC.
2. Ouvrez le programme sur le PC avec LOGO!Soft Comfort, puis cliquez sur "Télécharger".

3. Définissez l'interface de communication sur "Adaptateur virtuel SGLAN".



Interface

Se connecter via : Ethernet SGLAN Virtual Adapter

Cible

Test

Adr. IP cible : 192.168. 0.100 Carnet d'adresses

LOGO! accessible :

Nom	Adresse IP	Masque de sous-rése...	Passerelle	Adresse MAC	Type d'app.	Etat
LOGO!...	192.168.0.100	255.255.255.0	192.168.0.1	8C-F3-19-FF-C4-62	BM	Available

☐ Copier vers carte SD

! Pour garantir la sécurité des installations, systèmes, machines et réseaux contre les cybermenaces, il est nécessaire d'implémenter (et de maintenir en permanence) un concept de sécurité industrielle global et conforme à l'état actuel de la technique. Les produits et

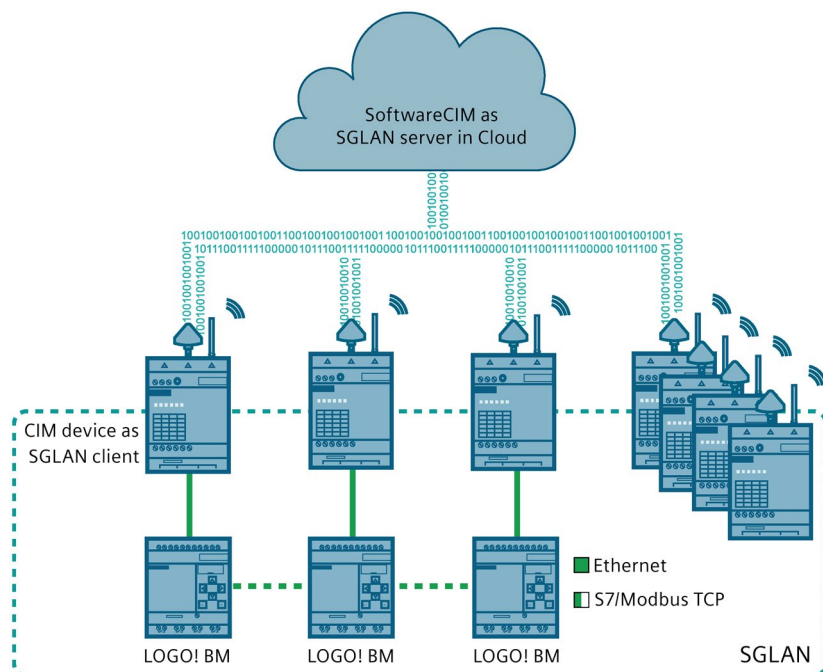
OK Annuler Aide

4. Sélectionnez le module LOGO! BM cible dans "LOGO accessible" et cliquez sur "OK".

8.2 Échanger des données entre deux LOGO! BM

Cet exemple pratique montre comment échanger des données entre deux LOGO! BM situés à des endroits différents via SGLAN.

Le schéma suivant montre le fonctionnement d'un tel système :



Conditions

- Un compte cloud AWS valide
- Les adresses IP de tous les appareils et de SoftwareCIM sur SGLAN se trouvent dans le même sous-réseau et ne sont pas en conflit les unes avec les autres
- Les appareils CIM à configurer comme clients SGLAN doivent respecter les conditions suivantes :
 - disposer d'IoT ou d'une carte SIM avec un accès à Internet et d'une adresse IPv4

Configuration du serveur SGLAN sur le cloud AWS

1. Exécutez "SoftwareCIMInstaller.exe" et choisissez de déployer SoftwareCIM sur le cloud AWS.
2. Saisissez l'ID de clé d'accès et la clé d'accès secrète pour vous connecter au cloud AWS. Cliquez sur "Suivant".
3. Sélectionnez Région Sélectionnez "Créer une nouvelle instance". Cliquez sur "Suivant".
4. Saisissez le nom d'instance et la description ; sélectionnez l'image de machine et le type d'instance. Cliquez sur "Suivant".
5. Cliquez sur "Ignorer" et acceptez le certificat Siemens par défaut.

6. Définissez des mots de passe pour le compte Windows, le compte SoftwareCIM et le compte SGLAN.
7. Cliquez sur "Déployer" pour lancer le déploiement.

Une fois le déploiement terminé avec succès, vous voyez un QR code et deux liens dans la fenêtre. Le SoftwareCIM déployé est configuré par défaut comme serveur SGLAN. Enregistrez le QR code ou les liens pour un usage ultérieur. Dans ce cas, l'IP publique du serveur SGLAN est 3.98.107.40. Enregistrez l'adresse IP publique, car elle servira pour connecter les clients SGLAN au serveur SGLAN.



Configuration de clients SGLAN

1. Accédez aux pages de configuration basées web de l'appareil CIM 1 et connectez-vous. Vous pouvez constater que les pages de configuration sont différentes de celles de SoftwareCIM.
2. Vérifiez l'état cellulaire.
3. Allez sur la page SGLAN et activez "CIM comme client SGLAN".
4. Sélectionnez Mode hôte distant comme IPv4.
5. Saisissez l'adresse IPv4 du serveur pour "Hôte distant". L'adresse IP est 3.98.107.40.

6. Entrez le mot de passe du serveur. Ce mot de passe est celui du compte SGLAN que vous avez défini lors du déploiement de SoftwareCIM sur le cloud.
7. Cliquez sur "Enregistrer les modifications".

Paramètres SGLAN

CIM comme serveur SGLAN: ☐

CIM comme client SGLAN: ☒

Serveur

Liste de serveurs

Mode hôte distant: IPv4

Remote Host:

3 . 98 . 107 . 40

Mot de passe du serveur:

64/64

Statistiques:

Nom	Statistiques des données SGLAN
Nom de serveur	AWS SGLAN Server
IP du réseau local du serveur	192.168.0.82
État	Connecté
Temps de connexion	00:33:54
Octets envoyés	1.943 MB
Octets reçus	430.261 KB
Envoyer vitesse	1.154 KB/S
Recevoir vitesse	1.719 KB/S

Répétez les étapes ci-dessus pour configurer l'appareil CIM 2 comme client SGLAN.

Vérification de l'état de la connexion des clients au serveur

1. Allez sur la plateforme de configuration basée sur le web de SoftwareCIM dans le cloud AWS à l'aide du lien que vous avez enregistré après le déploiement.
2. Connectez-vous à la plateforme de configuration.
3. Allez à la page SGLAN. Vous pouvez vérifier l'état de la connexion au client SGLAN ici.

Paramètres SGLAN

SoftwareCIM comme serveur SGLAN: ☒

SoftwareCIM comme client SGLAN: ☐

SoftwareCIM comme serveur SGLAN

Mode: IPv4

Mot de passe d'accès : 64/64

Confirmer le mot de passe d'accès : 64/64

Serveur IP: 3.98.107.40

Statistiques

Octets envoyés	Octets reçus	Envoyer vitesse	Recevoir vitesse
331.537 MB	1.089 MB	134.262 KB/S	342 B/S

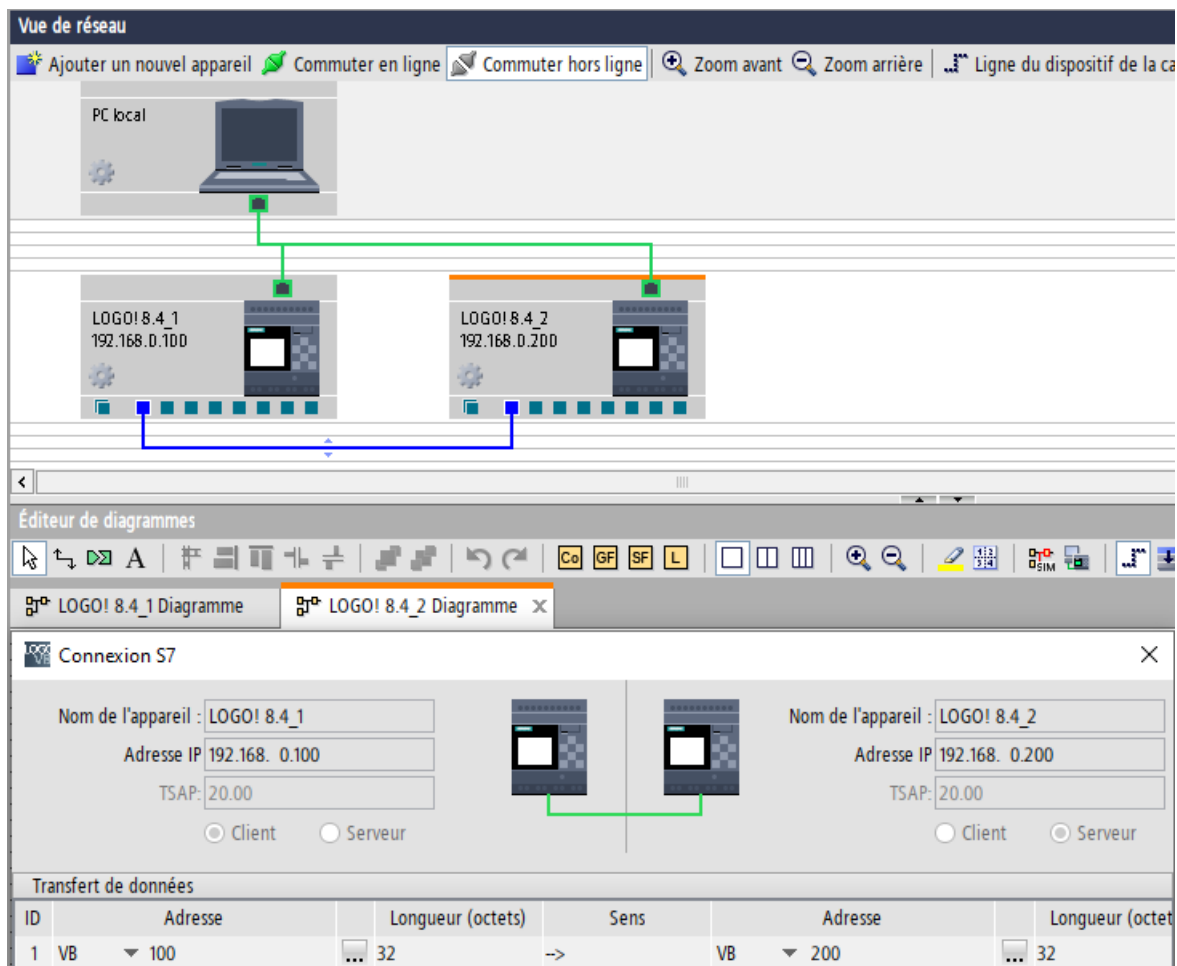
État de la connexion du client

données de la liste de filtres

#	Name	IP du réseau local	LAN Mask	Status
1	CIM1.1 Demo-192.168.0.100	192.168.0.100	255.255.255.0	authorized
2	CIM_192.168.100.104	192.168.44.104	255.255.255.0	authorized
3	CIM_192.168.100.102	192.168.62.102	255.255.255.0	authorized
4	CIM_192.168.100.108	192.168.53.108	255.255.255.0	authorized
5	CIM_192.168.100.102	192.168.61.102	255.255.255.0	authorized

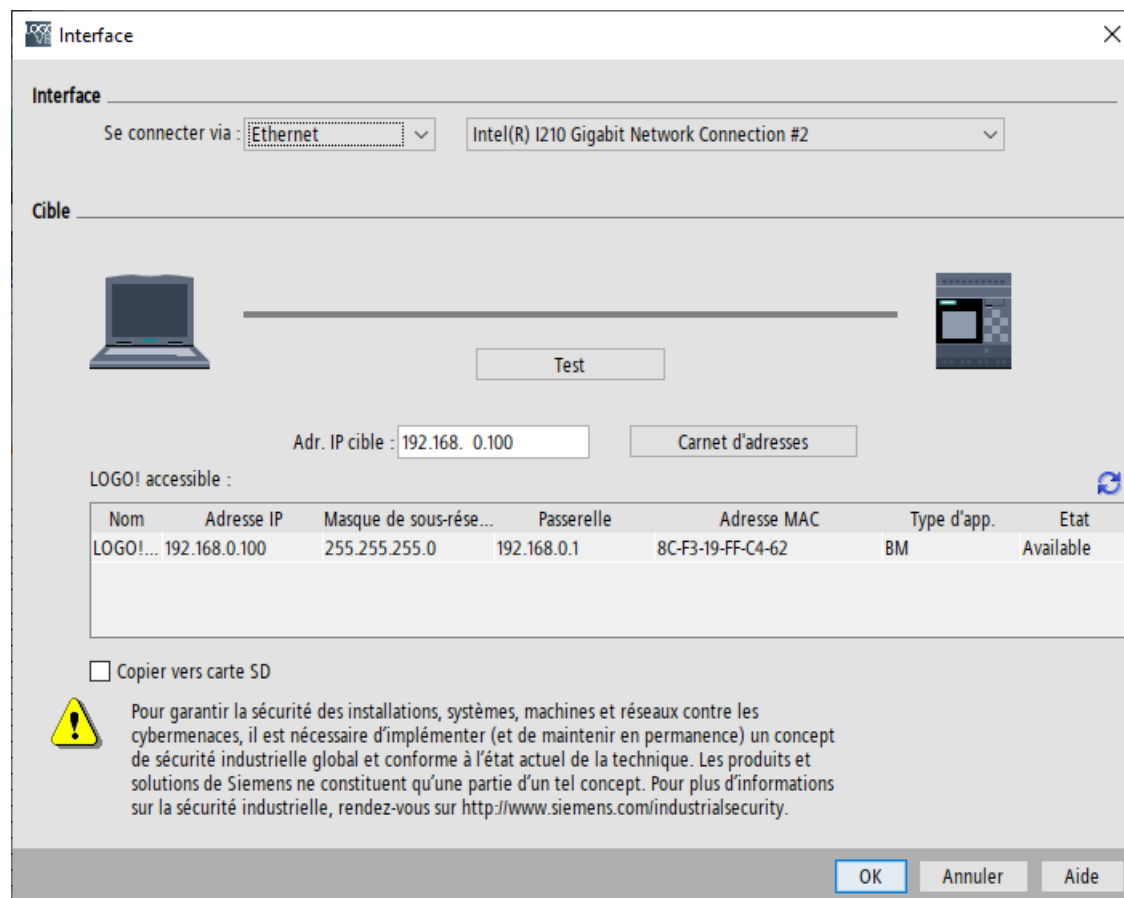
Échanger des données entre deux LOGO! BM

1. Ouvrez le programme à télécharger avec LOGO!Soft Comfort sur le PC 1.
2. Paramétrez le transfert de données dans la connexion S7.

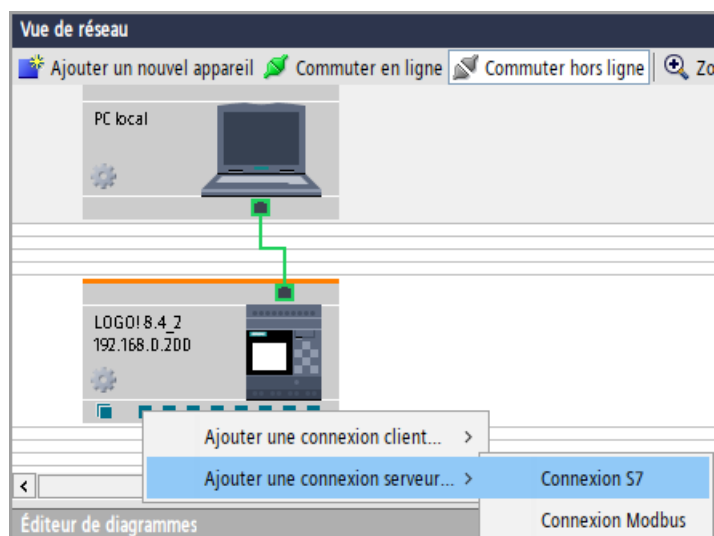


3. Cliquez sur "Télécharger" et sélectionnez l'adaptateur local connecté à l'appareil CIM 1 comme interface.

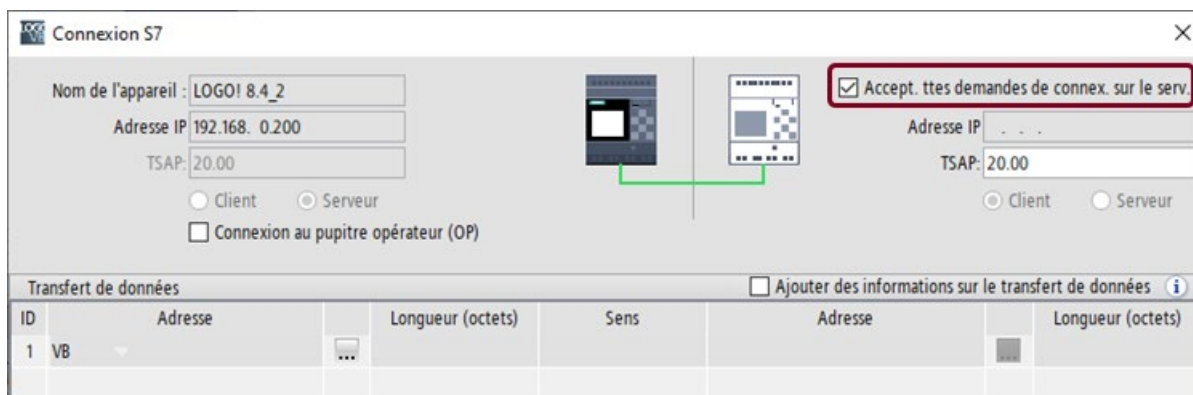
4. Sélectionnez le LOGO! BM 1 dans "LOGO! accessible" et cliquez sur "OK".



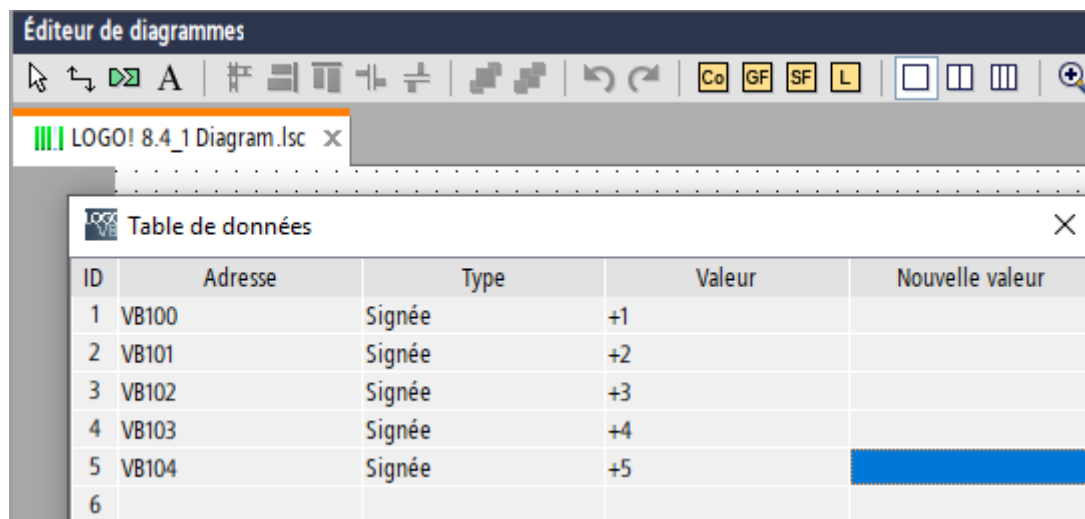
5. Ouvrez le programme à télécharger avec LOGO!Soft Comfort sur le PC 2, ajoutez la connexion serveur et sélectionnez la connexion S7 pour LOGO! BM 2.



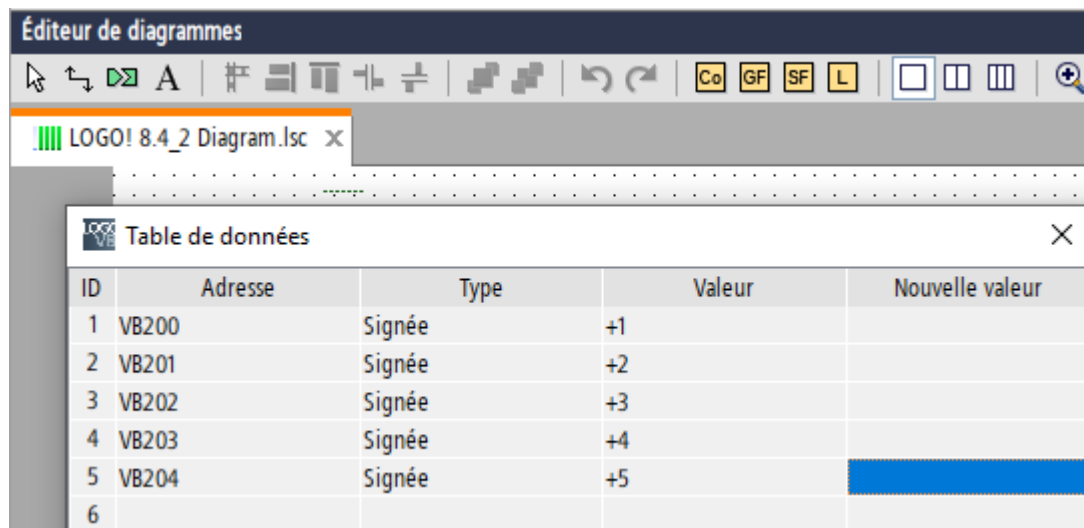
6. Sélectionnez "Accepter toutes les demandes de connexion sur le serveur" dans la fenêtre de configuration Connexion S7. Cliquez ensuite sur "Télécharger".



7. Sélectionnez l'adaptateur local connecté à l'appareil CIM 2 comme interface.
8. Sélectionnez le LOGO! BM 2 dans "LOGO! accessible" et cliquez sur "OK".
9. Ouvrez LOGO!Soft Comfort sur le PC 1 et saisissez de nouvelles valeurs pour l'adresse sur LOGO! BM dans la table de données.



10. Ouvrez LOGO!Soft Comfort sur le PC 2 et vérifiez que les données ont été transférées au LOGO! BM 2.



Index

A

API RESTful, 53

C

Certificat

 Certificat externe, 57, 60

 Certificat intégré, 57, 60

 Certificat SoftwareCIM interne, 57, 60

Compatibilité

 Système d'exploitation, 10

Configuration de SoftwareCIM

 À propos de, 32

 Paramètres réseau, 33

D

Dépannage, 28

 Dépannage de SGLAN, 68

 État du système, 69

Déploiement manuel, 70, 79

 Alibaba Cloud, 79

 Cloud AWS, 70

Déployer sur Alibaba, 21

Déployer sur AWS, 13

E

État du système, 31

Exemple pratique, 84, 91

G

Gestion des données

 Action, 39

 Associations de données, 39

 Variables, 39

Gestion des données

 Événement, 39

M

menu icône barre système, 32

Mettre à jour SoftwareCIM

 en installant le pack de mise à jour, 65

 mise à jour manuelle, 67

Mise à jour SoftwareCIM

 mise à jour automatique, 65

Modbus RTU, 51

Modbus TCP, 47

Modèle UDM (Universal Data Model), 8

Mot de passe, 63

P

Page de connexion, 11

Pages de configuration, 30

Paramètres de l'heure, 62

Paramètres réseau

 LAN, 33

 WAN, 33

R

Redémarrer, 63

Réinitialisation aux paramètres d'usine, 63

S

S7, 43

V

Variables, 38