M580

Module intégré OPC UA BMENUA0100

Guide d'installation et de configuration

Traduction de la notice originale

05/2022

PHA83351.03

www.se.com

Mentions légales

Table des matières

Consignes de sécurité

Informations importantes

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'appareil ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.

La présence de ce symbole sur une étiquette “Danger” ou “Avertissement” signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.

Ce symbole est le symbole d'alerte de sécurité. Il vous avertit d'un risque de blessures corporelles. Respectez scrupuleusement les consignes de sécurité associées à ce symbole pour éviter de vous blesser ou de mettre votre vie en danger.

⚠ DANGER

DANGER signale un risque qui, en cas de non-respect des consignes de sécurité, **provoque** la mort ou des blessures graves.

⚠ AVERTISSEMENT

AVERTISSEMENT signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** la mort ou des blessures graves.

⚠ ATTENTION

ATTENTION signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** des blessures légères ou moyennement graves.

AVIS

AVIS indique des pratiques n'entraînant pas de risques corporels.

Remarque Importante

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

Avant de commencer

N'utilisez pas ce produit sur les machines non pourvues de protection efficace du point de fonctionnement. L'absence de ce type de protection sur une machine présente un risque de blessures graves pour l'opérateur.

⚠ AVERTISSEMENT

EQUIPEMENT NON PROTEGE

- N'utilisez pas ce logiciel ni les automatismes associés sur des appareils non équipés de protection du point de fonctionnement.
- N'accédez pas aux machines pendant leur fonctionnement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cet automatisme et le logiciel associé permettent de commander des processus industriels divers. Le type ou le modèle d'automatisme approprié pour chaque application dépendra de facteurs tels que la fonction de commande requise, le degré de protection exigé, les méthodes de production, des conditions inhabituelles, la législation, etc. Dans certaines applications, plusieurs processeurs seront nécessaires, notamment lorsque la redondance de sauvegarde est requise.

Vous seul, en tant que constructeur de machine ou intégrateur de système, pouvez connaître toutes les conditions et facteurs présents lors de la configuration, de l'exploitation et de la maintenance de la machine, et êtes donc en mesure de déterminer les équipements automatisés, ainsi que les sécurités et verrouillages associés qui peuvent être utilisés correctement. Lors du choix de l'automatisme et du système de commande, ainsi que du logiciel associé pour une application particulière, vous devez respecter les normes et réglementations locales et nationales en vigueur. Le document National Safety Council's Accident Prevention Manual (reconnu aux Etats-Unis) fournit également de nombreuses informations utiles.

Dans certaines applications, telles que les machines d'emballage, une protection supplémentaire, comme celle du point de fonctionnement, doit être fournie pour l'opérateur. Elle est nécessaire si les mains ou d'autres parties du corps de l'opérateur peuvent entrer dans la zone de point de pincement ou d'autres zones dangereuses, risquant ainsi de provoquer des blessures graves. Les produits logiciels seuls, ne peuvent en aucun cas protéger les opérateurs contre d'éventuelles blessures. C'est pourquoi le logiciel ne doit pas remplacer la protection de point de fonctionnement ou s'y substituer.

Avant de mettre l'équipement en service, assurez-vous que les dispositifs de sécurité et de verrouillage mécaniques et/ou électriques appropriés liés à la protection du point de fonctionnement ont été installés et sont opérationnels. Tous les dispositifs de sécurité et de verrouillage liés à la protection du point de fonctionnement doivent être coordonnés avec la programmation des équipements et logiciels d'automatisation associés.

NOTE: La coordination des dispositifs de sécurité et de verrouillage mécaniques/électriques du point de fonctionnement n'entre pas dans le cadre de cette bibliothèque de blocs fonction, du Guide utilisateur système ou de toute autre mise en œuvre référencée dans la documentation.

Démarrage et test

Avant toute utilisation de l'équipement de commande électrique et des automatismes en vue d'un fonctionnement normal après installation, un technicien qualifié doit procéder à un test de démarrage afin de vérifier que l'équipement fonctionne correctement. Il est essentiel de planifier une telle vérification et d'accorder suffisamment de temps pour la réalisation de ce test dans sa totalité.

⚠AVERTISSEMENT

RISQUES INHERENTS AU FONCTIONNEMENT DE L'EQUIPEMENT

- Assurez-vous que toutes les procédures d'installation et de configuration ont été respectées.
- Avant de réaliser les tests de fonctionnement, retirez tous les blocs ou autres cales temporaires utilisés pour le transport de tous les dispositifs composant le système.
- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Effectuez tous les tests de démarrage recommandés dans la documentation de l'équipement. Conservez toute la documentation de l'équipement pour référence ultérieure.

Les tests logiciels doivent être réalisés à la fois en environnement simulé et réel

Vérifiez que le système entier est exempt de tout court-circuit et mise à la terre temporaire non installée conformément aux réglementations locales (conformément au National Electrical Code des Etats-Unis, par exemple). Si des tests diélectriques sont nécessaires, suivez les recommandations figurant dans la documentation de l'équipement afin d'éviter de l'endommager accidentellement.

Avant de mettre l'équipement sous tension :

- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.
- Fermez le capot du boîtier de l'équipement.
- Retirez toutes les mises à la terre temporaires des câbles d'alimentation entrants.
- Effectuez tous les tests de démarrage recommandés par le fabricant.

Fonctionnement et réglages

Les précautions suivantes sont extraites du document NEMA Standards Publication ICS 7.1-1995 (la version anglaise prévaut) :

- Malgré le soin apporté à la conception et à la fabrication de l'équipement ou au choix et à l'évaluation des composants, des risques subsistent en cas d'utilisation inappropriée de l'équipement.
- Il arrive parfois que l'équipement soit déréglé accidentellement, entraînant ainsi un fonctionnement non satisfaisant ou non sécurisé. Respectez toujours les instructions du fabricant pour effectuer les réglages fonctionnels. Les personnes ayant accès à ces réglages doivent connaître les instructions du fabricant de l'équipement et les machines utilisées avec l'équipement électrique.
- Seuls ces réglages fonctionnels, requis par l'opérateur, doivent lui être accessibles. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

A propos de ce manuel

Objectif du document

Ce guide présente les fonctionnalités et le fonctionnement du module de communication Ethernet M580 BMENUA0100 avec serveur OPC UA intégré.

NOTE: Les paramètres de configuration figurant dans le présent guide sont uniquement destinés à la formation. Ceux qui sont obligatoires pour votre propre configuration peuvent différer des exemples fournis.

Ce guide présente les fonctionnalités et le fonctionnement du module de communication Ethernet M580 BMENUA0100 avec serveur OPC UA intégré.

Champ d'application

Ce document s'applique à un système M580 utilisé avec EcoStruxure™ Control Expert 15.0 ou version ultérieure.

Les caractéristiques techniques des équipements décrits dans ce document sont également fournies en ligne. Pour accéder aux informations en ligne, allez sur la page d'accueil de Schneider Electric www.se.com/ww/en/download/.

Les caractéristiques présentées dans ce manuel devraient être identiques à celles fournies en ligne. Toutefois, en application de notre politique d'amélioration continue, nous pouvons être amenés à réviser le contenu du document afin de le rendre plus clair et plus précis. Si vous constatez une différence entre le manuel et les informations fournies en ligne, utilisez ces dernières en priorité.

Document(s) à consulter

Titre de la documentation	Numéro de référence
Modicon M580 Autonome - Guide de planification du système pour architectures courantes	HRB62666 (Anglais), HRB65318 (Français), HRB65319 (Allemand), HRB65320 (Italien), HRB65321 (Espagnol), HRB65322 (Chinois)
Modicon M580- Guide de planification du système pour topologies complexes	NHA58892 (Anglais), NHA58893 (Français), NHA58894 (Allemand), NHA58895 (Italien), NHA58896 (Espagnol), NHA58897 (Chinois)
Modicon M580 Guide de planification du système de redondance d'UC pour architectures courantes	NHA58880 (Anglais), NHA58881 (Français), NHA58882 (Allemand), NHA58883 (Italien), NHA58884 (Espagnol), NHA58885 (Chinois)
Modicon M580Plates-formes M340 et X80 I/O - Normes et certifications	EIO0000002726 (anglais), EIO0000002727 (français), EIO0000002728 (allemand),

Titre de la documentation	Numéro de référence
	EIO0000002730 (italien), EIO0000002729 (espagnol), EIO0000002731 (chinois)
M580 - BMENOS0300 - Module de sélection d'options de réseau - Guide d'installation et de configuration	NHA89117 (Anglais), NHA89119 (Français), NHA89120 (Allemand), NHA89121 (Italien), NHA89122 (Espagnol), NHA89123 (Chinois)
Modicon M580 - Manuel de référence du matériel	EIO0000001578 (Anglais), EIO0000001579 (Français), EIO0000001580 (Allemand), EIO0000001582 (Italien), EIO0000001581 (Espagnol), EIO0000001583 (Chinois)
Modicon M580 - Modules d'E/S distantes - Guide d'installation et de configuration	EIO0000001584 (Anglais), EIO0000001585 (Français), EIO0000001586 (Allemand), EIO0000001587 (Italien), EIO0000001588 (Espagnol), EIO0000001589 (Chinois),
Modicon M580 - Modification de la configuration en temps réel (CCOTF) - Guide utilisateur	EIO0000001590 (Anglais), EIO0000001591 (Français), EIO0000001592 (Allemand), EIO0000001594 (Italien), EIO0000001593 (Espagnol), EIO0000001595 (Chinois)
Modicon X80 - Modules d'E/S TOR - Manuel utilisateur	35012474 (Anglais), 35012475 (Allemand), 35012476 (Français), 35012477 (Espagnol), 35012478 (Italien), 35012479 (Chinois)
Modicon X80 - Module de comptage BMXEHC0200 - Guide utilisateur	35013355 (Anglais), 35013356 (Allemand), 35013357 (Français), 35013358 (Espagnol), 35013359 (Italien), 35013360 (Chinois)
Mise à la terre et compatibilité électromagnétique des systèmes automates - Principes et mesures de base - Manuel de l'utilisateur	33002439 (anglais), 33002440 (français), 33002441 (allemand), 33003702 (italien), 33002442 (espagnol), 33003703 (chinois)
EcoStruxure™ Control Expert - Langages de programmation et structure - Manuel de référence	35006144 (anglais), 35006145 (français), 35006146 (allemand), 35013361 (italien), 35006147 (espagnol), 35013362 (chinois)
EcoStruxure™ Control Expert - Bits et mots système - Manuel de référence	EIO0000002135 (Anglais), EIO0000002136 (Français), EIO0000002137 (Allemand), EIO0000002138 (Italien), EIO0000002139 (Espagnol), EIO0000002140 (Chinois)
EcoStruxure™ Control Expert - Modes de fonctionnement	33003101 (Anglais), 33003102 (Français), 33003103 (Allemand), 33003104 (Espagnol), 33003696 (Italien), 33003697 (Chinois)
EcoStruxure™ Control Expert - Manuel d'installation	35014792 (Anglais), 35014793 (Français), 35014794 (Allemand), 35014795 (Espagnol), 35014796 (Italien), 35012191 (Chinois)

Titre de la documentation	Numéro de référence
Web Designer pour FactoryCast - Manuel utilisateur	35016149 (anglais), 35016150 (français), 35016151 (allemand), 35016152 (italien), 35016153 (espagnol), 35016154 (chinois)
Cybersécurité des plates-formes automate Modicon - Manuel de référence	EIO0000001999 (Anglais), EIO0000002001 (Français), EIO0000002000 (Allemand), EIO0000002002 (Italien), EIO0000002003 (Espagnol), EIO0000002004 (Chinois)

Vous pouvez télécharger ces publications, le présent manuel et autres informations techniques depuis notre site web à l'adresse : www.se.com/en/download/.

Caractéristiques du module BMENUA0100

Introduction

Ce chapitre décrit le module de communications BMENUA0100 Ethernet avec serveur OPC UA.

Caractéristiques du module

Introduction

Le module BMENUA0100 Modicon avec serveur OPC UA associe les hautes performances de l'architecture OPC UA au système ePAC Modicon M580.

L'architecture OPC UA constitue une plateforme sécurisée, ouverte et fiable, destinée aux communications industrielles. Elle est flexible et évolutive, depuis les capteurs IoT aux ressources restreintes sur le terrain jusqu'aux serveurs d'entreprise hébergés dans le centre de données ou le Cloud. Outre la connexion aux données et leur transfert, le protocole OPC UA définit un modèle de données permettant la publication et la gestion des méta-données et du contexte des systèmes, pour simplifier l'intégration des systèmes et l'ingénierie de l'automatisation.

En établissant une norme de communication pour les opérations industrielles connectées, l'architecture OPC UA permet de relier les produits connectés sur le terrain, les contrôleurs d'automatisation et de périphérie, et les applications et outils d'analyse de l'entreprise. Elle est donc compatible avec les structures informatiques et de sécurité modernes telles que les pare-feu, les réseaux VPN et les proxies. L'architecture OPC UA s'adapte aux besoins fonctionnels et à la bande passante.

Fonctionnalités

Le module BMENUA0100 intègre un serveur OPC UA et un commutateur Ethernet. Il figure au **Catalogue matériel** de Control Expert dans le groupe de modules de **Communication**,

Le module BMENUA0100 exécute les fonctions suivantes pour la plateforme Modicon M580 :

Généralités :

- Accès direct et optimisé au dictionnaire de données Control Expert pour le mappage simple entre Control Expert et les variables OPC UA, page 45.

- Prise en charge des configurations à redondance d'UC via la redondance, page 49 OPC UA.
- Compatibilité avec les systèmes de sécurité M580 en tant que module non perturbateur de Type 1 tel que défini par TÜV Rheinland.
- Communications fluides par embase Ethernet.
- Client DHCP/FDR pour le téléchargement des paramètres de configuration stockés (non cybersécurité).
- Synchronisation entre client et serveur, page 124 NTP.
- Plusieurs méthodes de diagnostic : voyants, page 132, DDT, page 136, variables et éléments de données, page 148 OPC_UA, Syslog, page 152, Modbus, page 156, SNMP, page 157 et pages Web sécurisées, page 158.
- Mise à niveau du micrologiciel via Outil EcoStruxure™ Automation Device Maintenance, page 168.
- Vérification de l'intégrité du micrologiciel.
- Stockage sécurisé du matériel.

Cybersécurité:

- Communications sécurisées via HTTPS, OPC UA (en option), et IPSEC (en option).
- Sécurité, page 92 configurable OPC UA au niveau des modules via HTTPS.
- Capacité à contrôler le flux de communication entrant et sortant en activant et en désactivant des services de communication, page 94.
- IPSEC, page 100 basé sur une clé pré-partagée (PSK) pour sécuriser les services tels que SNMPv1, Modbus/TCP, Syslog et NTPv4.

  NOTE: Le BMENUA0100 prend en charge le mode IPSEC principal, non agressif. Une voie IPSEC peut être ouverte par le serveur BMENUA0100 ou un client OPC UA distant. Sur un client PC, IPSEC est pris en charge et validé sur les systèmes Windows 7, Windows 10 et Windows Server 2016.

Gestion de l'authentification :

- Contrôle d'accès basé sur des rôles (RBAC) et authentification des utilisateurs , page 111 pour les clients HTTPS et OPC UA.
- Certificats, page 103 pour entités d'application client OPC UA.

Principales caractéristiques du module de communication M580 :

- Client DHCP/FDR pour le téléchargement des paramètres de configuration stockés (non cybersécurité).
- Accès direct et optimisé au dictionnaire de données Control Expert pour le mappage des variables entre Control Expert et le serveur OPC UA, page 45.
- Port d'embase Ethernet pour les communications Ethernet sur le rack Ethernet principal local.
- Port d'embase X Bus pour l'alimentation 24 VCC et l'adressage de rack.

- Synchronisation entre client et serveur NTP, page 124.
- Compatibilité avec les configurations de redondance d'UC via la redondance OPC UA, page 49.
- Configuration de sécurité, module non perturbateur de Type 1 tel que défini par TÜV Rheinland.
- Différentes méthodes de diagnostic : voyants, page 132, DDT, page 136, variables et éléments de données OPC_UA, page 148, Syslog, page 152, Modbus, page 156, SNMP, page 127 et pages Web sécurisées, page 155.
- Mise à niveau du micrologiciel via l'outil EcoStruxure™ Maintenance Expert, page 168.
- Stockage sécurisé du matériel.
- Vérification d'intégrité du micrologiciel.

Description du module

Introduction

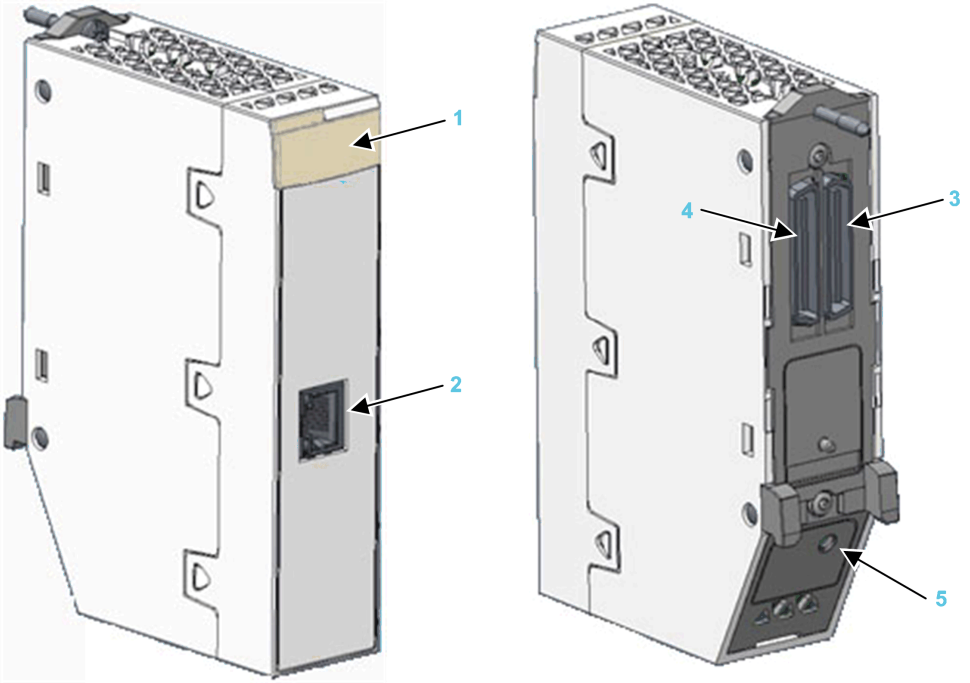
Schneider Electric propose deux modules de communication Ethernet avec serveur OPC UA intégré pour la communication avec les clients OPC UA, notamment SCADA :

- Module BMENUA0100 pour environnements standard.
- Module BMENUA0100H pour environnements difficiles.

Le module peut être installé uniquement dans un logement Ethernet, sur un rack Ethernet local principal. Consultez la rubrique *Configurations prises en charge pour le module BMENUA0100*, page 59 qui décrit les conditions d'installation des modules, notamment le nombre maximal de modules BMENUA0100 dans un rack.

Description physique

La figure ci-dessous montre les fonctionnalités externes du module BMENUA0100 :



1 Voyants

2 Port de contrôle avec liaison Ethernet et voyants d'activité

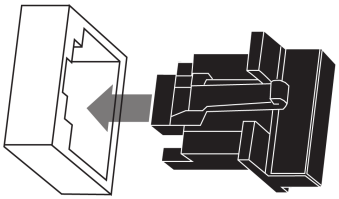
3 Port d'embase Ethernet

4 Port d'embase X Bus

5 Sélecteur rotatif du mode de fonctionnement de la cybersécurité

Consultez la rubrique Diagnostic des voyants, page 132 pour obtenir des informations sur les indications des voyants du module.

Si le port de contrôle Ethernet n'est pas activé, utilisez le bouchon fourni avec chaque module pour éviter la pénétration de saletés dans le port de contrôle :



Ports externes

Le module BMENUA0100 comporte les ports externes suivants :

Port	Description
Port de contrôle	Le port de contrôle est le port unique situé à l'avant du module BMENUA0100. Voici ses principales caractéristiques : • Lorsque le port de contrôle est activé, c'est l'interface exclusivement utilisée pour les communications OPC UA, sauf si IPv6 est configuré. ◦ Lorsque IPv6 est configuré, le port d'embase et le port de contrôle peuvent tous les deux être utilisés pour les communications OPC UA. ◦ Lorsque IPv6 n'est pas configuré, vous pouvez également connecter les clients OPC UA situés sur le réseau de l'embase via le port de contrôle du BMENUA0100 si un routage a été défini/déclaré sur l'ordinateur qui héberge le client OPC UA. • Vitesse de fonctionnement jusqu'à 1 Gb/s. Avec une vitesse de fonctionnement de : ◦ 1 Gb/s, utilisez uniquement des câbles à quatre paires torsadées en cuivre blindés CAT6. ◦ 10/100 Gb/s, utilisez des câbles à quatre paires torsadées en cuivre blindés CAT5e ou CAT6. • Double pile IP prenant en charge à la fois l'adressage IPv4 (32 bits) et IPv6 (128 bits) : ◦ Les types IPv4 et IPv6 sont tous deux configurés pour le module. ◦ La configuration de l'adressage IPv6 peut être statique ou dynamique (via SLAAC). ◦ La configuration IPv4 par défaut, page 116 est automatiquement attribuée en fonction de l'adresse MAC du module si aucune adresse IP n'est configurée. • Accès sécurisé au serveur OPC UA via les protocoles IPv4 et IPv6. • Protocole sécurisé HTTPS (sur IPv4) pour la mise à niveau du micrologiciel, page 168 et la configuration de la cybersécurité, page 84. • Prise en charge du protocole sécurisé NTPv4. • Sécurité fournie par IPsec pour les services non sécurisés, notamment SNMPv1, Modbus TCP, et Syslog.
Port d'embase Ethernet	Le port d'embase BMENUA0100 Ethernet prend en charge le protocole IPv4 (32 bits). Lorsque le port de contrôle est désactivé, le port d'embase peut prendre en charge les communications OPC UA. Le port d'embase présente les caractéristiques suivantes : • Vitesse de fonctionnement jusqu'à 100 Mb/s. • Connectivité Modbus TCP IPv4 Ethernet avec le processeur : ◦ Le port d'embase Ethernet est le port exclusivement utilisé pour les diagnostics Modbus. • Port exclusif pour la configuration sans cybersécurité (IP, NTPv4, SNMPv1), via : ◦ Control Expert v14.1 et versions ultérieures ◦ Serveur FDR/DHCP • Si le port de contrôle est désactivé, le port d'embase Ethernet fournit l'accès sécurisé au serveur OPC UA via le protocole IPv4 et prend en charge les services suivants : ◦ Protocole sécurisé HTTPS pour la mise à niveau du micrologiciel, page 168 et la configuration de la cybersécurité, page 84. ◦ NTPv4, SNMPv1 et Syslog.
Port d'embase X Bus	Le module BMENUA0100 utilise la communication de l'embase X Bus pour : • Recevoir l'alimentation 24 VCC. • Détecter le rack et l'adresse d'emplacement du module BMENUA0100.

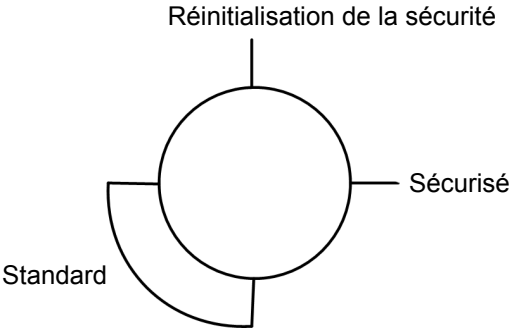
Port	Description
	NOTE: Aucune autre communication n'est établie via le port d'embase X Bus du module BMENUA0100.

Commutateur rotatif

Un commutateur rotatif à trois positions se trouve à l'arrière du module. Utilisez uniquement le petit tournevis en plastique fourni avec le module pour changer la position du commutateur et configurer le mode de fonctionnement de la cybersécurité pour le module.

AVIS
RISQUE DE FONCTIONNEMENT IMPRÉVU Utilisez uniquement le petit tournevis en plastique fourni avec le module pour changer la position du commutateur. L'utilisation d'un tournevis en métal peut endommager le commutateur et le rendre inutilisable. **Le non-respect de ces instructions peut provoquer des dommages matériels.**

Positions du commutateurs rotatif :



Paramètres :

- Mode Secured
- Mode standard
- Security Reset (réinitialisation de la sécurité)

NOTE:

- Le commutateur rotatif n'est pas accessible lorsque le module est placé sur le rack.
- Dans un système à redondance d'UC, vérifiez que la position du commutateur rotatif du module BMENUA0100 est identique dans les racks principaux locaux primaires et secondaires. Le système n'effectue pas automatiquement la vérification.

Consultez la description des modes de fonctionnement de la cybersécurité, page 25 pour obtenir des informations sur chaque position du commutateur rotatif.

Voyants du module

Affichage des voyants

Un panneau d'affichage à 7 voyants se trouve à l'avant du module BMENUA0100 :

Informations indiquées par les voyants du module :

Voyant	Indique l'état du module :
RUN	État de fonctionnement.
ERR	Erreurs détectées.
UACNX	Connexions OPC UA.
BS	Port d'embase.
NS	Port de contrôle.
SEC	État de la cybersécurité.
BUSY	État du dictionnaire de données

Consultez la rubrique Voyants de diagnostic, page 132 pour plus d'informations sur l'utilisation de ces voyants pour identifier l'état du module BMENUA0100.

Voyants du port de contrôle

Le port de contrôle situé à l'avant du module, présente deux voyants décrivant l'état de la liaison Ethernet sur le port :

- Le voyant ACT indique la présence d'activité Ethernet sur le port.
- Le voyant LNK indique la présence de la liaison Ethernet et sa vitesse.

Consultez la rubrique Voyants de diagnostic, page 135 pour plus d'informations sur l'utilisation de ces voyants pour identifier l'état du port de contrôle du module BMENUA0100.

Normes et certifications

Présentation

Ce chapitre décrit les normes et certifications qui s'appliquent au module de communications BMENUA0100 Ethernet avec serveur OPC UA intégré.

Normes et certifications

Télécharger

Cliquez sur le lien correspondant à votre langue favorite pour télécharger les normes et les certifications (format PDF) qui s'appliquent aux modules de cette gamme de produits :

Titre	Langues
Modicon M580Plates-formes M340 et X80 I/O - Normes et certifications	• Anglais : EIO0000002726 • Français : EIO0000002727 • Allemand : EIO0000002728 • Italien : EIO0000002730 • Espagnol : EIO0000002729 • Chinois : EIO0000002731

Norme du module BMENUA0100

Exigences gouvernementales

Le module de communication Ethernet OPC UA intégré BMENUA0100 est conforme à la norme officielle suivante :

Marquage	Exigence
OPC Unified Architecture	OPC UA V1.03 : Protocole de communication de machine à machine en architecture unifiée OPC.

Compatibilité du micrologiciel BMENUA0100 avec EcoStruxure™ Control Expert

Compatibilité

Les applications créées avec le logiciel EcoStruxure™ Control Expert sont compatibles avec le micrologiciel du module BMENUA0100 comme indiqué dans le tableau suivant :

Version du micrologiciel du module BMENUA0100	**Version du logiciel EcoStruxure™ Control Expert**	
	14.0	**15.0**
1.01	Totalement compatible	Seules les fonctions héritées de la version 1.01 sont prises en charge par le logiciel [1, 2, 3]
1.10	Totalement compatible	Totalement compatible

1. Si un module BMENUA0100 équipé du micrologiciel version 1.01 reçoit une application générée avec EcoStruxure™ Control Expert V15 où :
   - L'option **Taux d'échantillonnage rapide** est **activée** (dans l'onglet de configuration IP, page 116). Ce réglage ne sera pas mis en oeuvre.
   - IPv4 est désactivé pour le port de contrôle. Le port de contrôle du module sera configuré avec l'adresse IPv4 qui apparaît en grisé dans l'onglet **IPConfig** du module.

     NOTE: L'adresse IPv4 grisée peut être la dernière adresse IPv4 entrée par l'utilisateur ou l'adresse IPv4 entrée automatiquement par le logiciel EcoStruxure™ Control Expert (172.16.12.1) si aucune adresse IPv4 n'a été saisie entre-temps.
   - NTP, page 126 a été configuré avec une adresse IPv6. Les pages Web du module indiquent par erreur que NTP est opérationnel alors qu'il ne l'est pas.

2. Si deux modules BMENUA0100 avec micrologiciel de version 1.01 sont configurés dans un rack à redondance d'UC (Hot Standby) avec EcoStruxure™ Control Expert V15, les limitations décrites ci-dessus s'appliquent également à ces modules.

3. Si le protocole SNMP est activé dans Control Expert, incluez l'adresse IPv4 du gestionnaire SNMP dans l'onglet SNMP du module, page 127 BMENUA0100 pour que le gestionnaire SNMP puisse accéder à la base MIB SNMP.

NOTE: Les pages Web du BMENUA0100 seront les mêmes pour toutes les applications quelle que soit la référence de BMENUA0100 sélectionnée. Les pages Web affichées pour le module BMENUA0100 dépendent donc de la version de micrologiciel du module (1.01, 1.10 ou 2.01, par exemple) et non de la version du module (non BMENUA0100 ou BMENUA0100.2, par exemple).

Description fonctionnelle du BMENUA0100

Introduction

Ce chapitre décrit les fonctions prises en charge par le module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré.

Paramètres des modes de fonctionnement de la cybersécurité

Introduction

Cette section décrit les paramètres des modes de fonctionnement du module BMENUA0100.

Modes de fonctionnement de la cybersécurité

Introduction

Le module BMENUA0100 peut être configuré pour fonctionner en mode Secured ou Standard. Le sélecteur rotatif à 3 positions situé à l'arrière du module détermine le mode de fonctionnement.

Les trois positions du commutateur sont les suivantes :

- Mode Secured
- Mode Standard
- Security Reset (réinitialisation de la sécurité)

NOTE:

- La configuration par défaut du module est le mode Secured.
- Vous pouvez afficher la position actuelle du commutateur rotatif sur la page Web Accueil, page 89 du module.

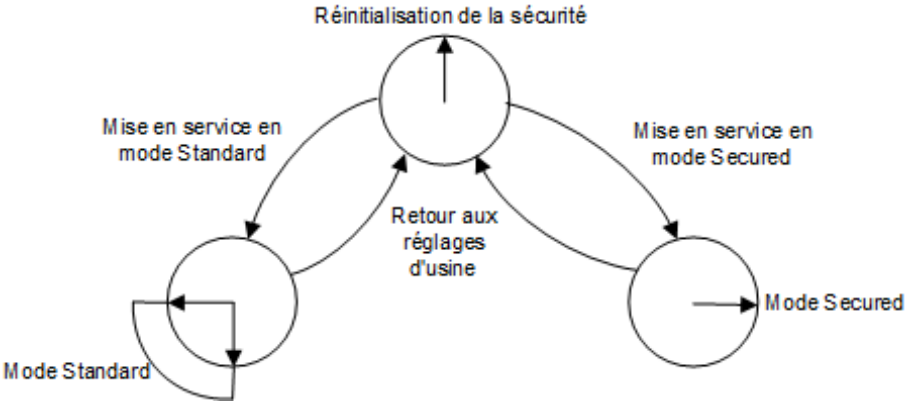
Comme le sélecteur rotatif n'est pas accessible lorsque le module est sur le rack, sa position ne peut être modifiée que lorsque le module est mis hors tension et retiré du rack. Une fois la nouvelle position sélectionnée, le module peut être réinséré dans le rack et mis sous tension.

NOTE: Utilisez uniquement le petit tournevis en plastique fourni avec le module, page 20 pour changer la position du commutateur et configurer un mode de fonctionnement de la cybersécurité.

Changement de mode de fonctionnement

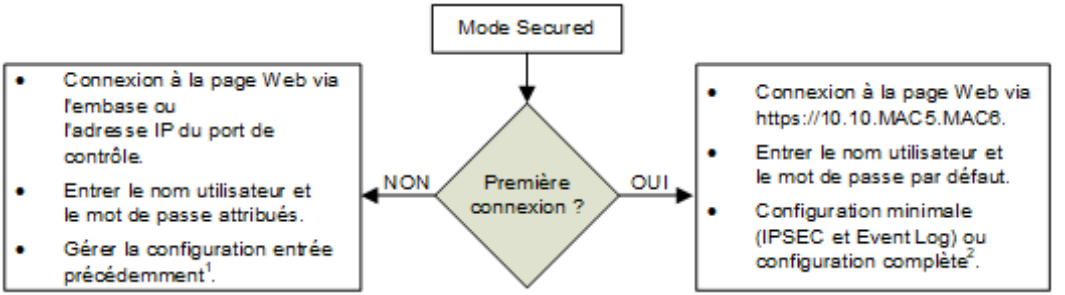
Chaque fois que vous basculez le mode de fonctionnement de la cybersécurité du mode Secured au mode Standard ou inversement, effectuez une opération Security Reset, page 80 avant de configurer le nouveau mode.

La position du commutateur rotatif détermine l'état de fonctionnement du module, comme suit :



Un module neuf (réglage d'usine par défaut) ou un module ayant subi une opération Security Reset peut être mis en service pour fonctionner en mode Standard, page 80 ou en mode Secured, page 78.

La procédure de configuration du module pour le mode Secured varie selon qu'il s'agit ou non de la première connexion aux paramètres de configuration du module après une réinitialisation de la sécurité :



1 Pour plus d'informations sur la gestion de la configuration, reportez-vous au chapitre Configuration, page 84.

2 Pour plus d'informations sur l'exécution d'une configuration lors de la première connexion, reportez-vous à la section Mise en service du mode Secured, page 78.

Mode Secured

En mode Secured, le module n'entre pas en communication de processus (via le port de contrôle ou le port d'embase) tant que des paramètres de cybersécurité valides n'ont pas été configurés. Une fois le mode Secured configuré, vous pouvez configurer les paramètres de cybersécurité à l'aide des pages Web du module, page 84, accessibles via le protocole HTTPS sur le port d'embase ou de contrôle. En mode Secured, le module prend en charge le niveau de cybersécurité spécifié dans la configuration de la cybersécurité. Ce n'est qu'une fois les paramètres de cybersécurité configurés que vous pouvez configurer les paramètres d'adresse IP, de client NTP et d'agent SNMP, page 115 à l'aide du logiciel de configuration Control Expert.

Mode Standard

En mode Standard, les communications du module peuvent commencer immédiatement. Les paramètres de cybersécurité ne sont pas nécessaires et ne peuvent pas être configurés. Seules l'adresse IP et d'autres paramètres disponibles dans Control Expert peuvent être configurés.

Security Reset

La commande **Security Reset** restaure les paramètres de configuration d'usine. Elle supprime toute configuration de cybersécurité, les listes blanches, les certificats et les

paramètres de contrôle d'accès basé sur les rôles. Pendant le processus de restauration des réglages par défaut d'usine, le voyant RUN clignote en vert. Une fois le processus terminé, le voyant RUN reste allumé en vert et tous les services sont désactivés. Pour parachever la réinitialisation de la sécurité, mettez le module BMENUA0100 hors tension puis sous tension ou retirez physiquement le module du rack (mise hors tension) puis réinsérez-le dans le rack (mise sous tension).

Ce réglage peut être effectué à l'aide du commutateur rotatif ou des pages Web (en mode Secured) :

- Si le commutateur rotatif est utilisé : le module cesse de fonctionner pendant qu'il retiré du rack et que le commutateur rotatif est réglé en position Secured ou Standard, puis fonctionne à nouveau quand il est réinséré. Des configurations doivent être appliquées.
- Si le réglage est effectué à l'aide des pages Web : à la fin du cycle d'alimentation (hors tension/sous tension) ou du remplacement à chaud du module en mode Standard ou Secured. Les paramètres de cybersécurité et d'adresse IP doivent être configurés.

  NOTE: Après une réinitialisation de la sécurité du module BMENUA0100, les conditions suivantes s'appliquent :

  - Aucun certificat d'équipement n'est conservé.
  - Tous les services sont désactivés, sauf HTTPS qui est utilisé pour créer la configuration de la cybersécurité via le port de contrôle.
  - Les réglages par défaut d'usine sont appliqués, notamment :
    - Nom d'utilisateur et mot de passe par défaut, page 28.
    - Adresse IP par défaut 10.10.MAC5.MAC6, page 115.

Combinaison nom d'utilisateur/mot de passe par défaut

La combinaison nom d'utilisateur/mot de passe par défaut dépend du mode de fonctionnement de la cybersécurité :

- Mode Secured : admin / password
- Mode Standard : installer / Inst@ller1

Fonctions prises en charge par les modes de fonctionnement Secured et Standard

Le module BMENUA0100 prend en charge les fonctions suivantes en mode Secured et Standard :

Mode de sécurité	**Mode Standard**			**Mode Secured**		
Port de contrôle	**Désactiver**	**Activer**		**Désactiver**	**Activer**	
Port Ethernet	**Embase**	**Embase**	**Port de contrôle**	**Embase**	**Embase**	**Port de contrôle**
Communication OPC UA	Oui	Non	Oui	Oui	Non	Oui
Paramètres de sécurité (4)	Aucun	–	Aucun	Aucun, signature, signature et cryptage (valeur par défaut)	–	Aucun, signature, signature et cryptage (valeur par défaut)
Authentification utilisateur	Pas d'authentification (anonyme)	–	Pas d'authentification (anonyme)	Opérateur, ingénieur, pas d'authentification (anonyme)	–	Opérateur, ingénieur, pas d'authentification (anonyme)
SNMP V1	Oui (1, 2)	Oui (1, 2)	Oui (1, 2)	Oui (1)	Oui (1)	Oui (1)
SNMP V3	Oui (1, 2)	Oui (1, 2)	Oui (1, 2)	Oui (1)	Oui (1)	Oui (1)
NTP V4	Client uniquement (1)	Client (1), serveur	Oui, client uniquement (1)	Client uniquement (1)	Client (1), serveur	Oui, client uniquement (1)
Journal d'événements	Non	Non	Non	Oui	Oui	Oui
IPSec	Non	Non	Non	Non	Non	Oui pour Modbus, SNMP V1/V3, NTP V4 (3) et Syslog (IPSec activé par défaut)
Changement de configuration CS Web (HTTPS)	Non	Non	Non	Oui	Oui	Oui
Authentification utilisateur	–	–	–	Admin	Admin	Admin
Activer/ Désactiver le serveur de comm de services réseau	Si pris en charge, toujours activé (voir ci-dessus)	Si pris en charge, toujours activé (voir ci-dessus)	Si pris en charge, toujours activé (voir ci-dessus)	Tous les services sont configurables (désactivés par défaut)	Tous les services sont configurables (désactivés par défaut)	Tous les services sont configurables (désactivés par défaut)
Diagnostic Web (pages Accueil et Diagnostic uniquement)	Oui	Oui	Oui	Oui	Oui	Oui

Mode de sécurité	**Mode Standard**			**Mode Secured**		
Port de contrôle	**Désactiver**	**Activer**		**Désactiver**	**Activer**	
Port Ethernet	**Embase**	**Embase**	**Port de contrôle**	**Embase**	**Embase**	**Port de contrôle**
Authentification utilisateur	Installateur (identifiants par défaut)	Installateur (identifiants par défaut)	Installateur (identifiants par défaut)	Administrateur, opérateur, ingénieur, installateur	Administrateur, opérateur, ingénieur, installateur	Administrateur, opérateur, ingénieur, installateur
Mise à niveau du micrologiciel (HTTPS)	Oui	Oui	Oui	Oui	Oui	Oui, si HTTPS est activé
Authentification utilisateur	Installateur (identifiants par défaut)	Installateur (identifiants par défaut)	Installateur (identifiants par défaut)	Installateur	Installateur	Installateur
Filtrage : Transférer tout	–	–	(toujours activé)	–	–	Transfert tous protocoles
Filtrage : Protocole de transfert configuré	–	–	–	–	–	Transfert des protocoles configurés

Mode de sécurité	**Mode Standard**			**Mode Secured**		
Port de contrôle	**Désactiver**	**Activer**		**Désactiver**	**Activer**	
Port Ethernet	**Embase**	**Embase**	**Port de contrôle**	**Embase**	**Embase**	**Port de contrôle**
Filtrage : Flux de données Control Expert vers le réseau d'équipements (y compris UC) (FTP, EIP, explicite, Modbus, Ping) via IPv4 uniquement[5]	–	–	Transfert des données Control Expert du réseau de contrôle vers le réseau d'équipe-ments (toujours activé)	–	–	Transfert des données Control Expert du réseau de contrôle au réseau d'équipements (désactivé par défaut)

1. Configurable avec Control Expert.
2. En mode standard, la version SNMP du module BMENUA0100 est définie dans Control Expert. Si SNMP est réglé sur V3 et que le module est configuré avec :
   - Micrologiciel version 2 (BMENUA0100.2) : SNMP V3 est utilisé avec le niveau de sécurité sans authentification et sans confidentialité.
   - Micrologiciel antérieur à la version 2 (BMENUA0100) : SNMP V1 est utilisé.

   Pour plus d'informations, reportez-vous à la section Configuration de l'agent SNMP dans Control Expert et les pages Web, page 128.
3. NTP V4 peut être configuré pour être transporté hors du tunnel IPSec.
4. Pour les modes de fonctionnement de la cybersécurité Standard et Secured, si les paramètres de sécurité sont définis sur *Aucun*, il n'y a pas d'authentification utilisateur (c'est-à-dire que le paramètre OPC UA, page 102 **Types de jeton d'identification d'utilisateur** est défini sur *Anonyme*).
5. Pour permettre à Control Expert d'accéder en ligne à la CPU ou au réseau d'équipements, configurez le PC (sur lequel Control Expert est installé) avec une adresse IP du même sous-réseau que le port de contrôle du BMENUA0100 et utilisez l'adresse IP du port de contrôle du module BMENUA0100 comme adresse IP de passerelle du PC. Dans ce cas, aucune adresse IP du PC ne peut se trouver sur le même sous-réseau que le port d'embase du module BMENUA0100.

Services OPC UA

Introduction

Cette section décrit les services pris en charge par le serveur OPC UA intégré au module BMENUA0100.

Caractéristiques de fonctionnement du serveur OPC UA intégré au module BMENUA0100

Limitations

Maxima :

- Nombre de noeuds pouvant être publiés dans l'espace d'adresses d'accès aux données du serveur OPC UA du BMENUA0100 : 100 000 noeuds.
- Quantité de mémoire pouvant être allouée au serveur OPC UA du BMENUA0100 : 192 Mo.

  NOTE: En cas de dépassement d'une de ces limites, l'espace d'adresse du serveur passe à l'état *LimitsExceeded*.

  NOTE: Le temps nécessaire à l'établissement d'une souscription horaire peut varier de manière très significative en fonction du nombre d'éléments et du nombre de clients connectés.

D'autres limitations sont décrites ci-après, avec le contexte où elles se produisent et les conséquences de leur dépassement :

Limite	Valeur	Service OPCUA	Paramètre du service	Effets
Nombre de sessions (cumul)	10	*Création de session*	(Non applicable)	Code de résultat du service *Bad_TooManySessions* (échec pour cause de nombre excessif de sessions)
Temporisation de session minimale	30 s	*Création de session*	Temporisation de session demandée	Temporisation de session révisée
Temporisation de session cumulée	3600 s	*Création de souscription*	Temporisation de session demandée	Temporisation de session révisée
Nombre maximum de souscriptions cumulé	40	*Création de souscription*	(Non applicable)	Code de résultat du service *Bad_TooManySubscriptions* (échec pour cause de nombre excessif de souscriptions)
Intervalle de publication minimum	250 ms[1] 20 ms[2]	*Création de souscription*	Intervalle de publication demandé	Intervalle de publication révisé
Intervalle de publication maximum	10 s	*Création de souscription*	Intervalle de publication demandé	Intervalle de publication révisé
Durée maximum de souscription	300 s	*Création de souscription*	Min(intervalle de publication demandé, 3600000) * durée de souscription demandée	Durée de souscription demandée

Limite	Valeur	Service OPCUA	Paramètre du service	Effets
Nombre maximum de notifications par publication	12500	*Création de souscription*	Nombre maximum de notifications par publication	Le nombre maximum de notifications par seconde est donc (1000 / intervalle de publication révisé) * 1000
Intervalle d'échantillonnage minimal	125 ms[1] 20 ms[2]	*Création d'éléments surveillés*	Surveillance de paramètres. Intervalle d'échantillonnage	Intervalle d'échantillonnage révisé
Taille maximale de la file d'attente des messages	100	*Création d'éléments surveillés*	Surveillance de paramètres. Taille de file d'attente	Taille de file d'attente révisée
Nombre maximal d'éléments surveillés (cumul)	50000[3] 2000[2]	*Création d'éléments surveillés*	(Non applicable)	Code de résultat du service *Bad_TooManyMonitoredItems* (échec pour cause de nombre excessif d'éléments surveillés)
Nombre maximum de souscriptions par session	4	–	–	–
Nombre maximum d'éléments surveillés par souscription	25000	–	–	–

1. Si l'option de surveillance rapide est désactivée.

2. Si l'option de surveillance rapide est activée.

3. Si l'option de surveillance rapide est désactivée et que le serveur est configuré avec :
   - un intervalle d'échantillonnage d'au moins 1 seconde et
   - un intervalle de publication d'au moins 1 seconde.

Serveur OPC UA

Introduction

L'objectif principal du module de communication Ethernet BMENUA0100 est de fournir une voie de communication OPC UA sur Ethernet entre des CPU M580 et des clients OPC UA. Les données de CPU M580 sont mappées sur des variables du module BMENUA0100, puis mises à la disposition des clients OPC UA via la pile de communication hautes performances du serveur OPC UA intégré au module BMENUA0100. Les clients OPC UA

se connectent à la pile du serveur OPC UA intégré via l'adresse IP du port de contrôle ou du port d'embase du module BMENUA0100, établissant ainsi une connexion client-serveur. Le module BMENUA0100 peut gérer jusqu'à dix (10) connexions client OPC UA simultanées pour la version 1.1 du micrologiciel (contre trois (3) connexions client OPC UA simultanées pour la version 1.0 du micrologiciel).

NOTE: Les conditions de chaque connexion entre un client OPC UA et le serveur OPC UA intégré au module BMENUA0100 sont déterminées par le client, lequel définit les attributs de la connexion entre client et serveur.

La pile du serveur OPC UA intégré au module BMENUA0100 contient des fonctionnalités définies par les termes suivants :

- Profil : définition des fonctionnalités incluant d'autres profils, facettes, groupes de conformité et unités de conformité.
- Facette : définition d'une fonctionnalité.
- Groupe de conformité : ensemble d'unités de conformité.
- Unité de conformité : service spécifique, par exemple : lecture, écriture, etc.

Profil pris en charge par BMENUA0100

Le module BMENUA0100 prend en charge le profil de **serveur UA 2017 intégré**. Comme indiqué sur le site Web OPC Foundation, ce profil "*est un profil complet conçu pour les équipements avec plus de 50 Mo de mémoire et un processeur plus puissant. Ce profil repose sur le profil de serveur d'équipements intégré Micro. Les principaux ajouts sont : prise en charge de la sécurité via les règles de sécurité et prise en charge de la facette de serveur de souscription aux modifications de données standard. Ce profil requiert également que les serveurs exposent tous les types OPC-UA utilisés par le serveur, y compris leurs composants et super-types.*" Pour plus d'informations, consultez le site Web OPC Foundation : http://opcfoundation.org/UA-Profile/Server/EmbeddedUA2017.

Facettes prises en charge par BMENUA0100

Le module BMENUA0100 prend en charge les facettes suivantes :

- **Catégorie de serveur > Facettes > Caractéristiques du serveur central** :
  - **Facette de serveur central 2017** (http://opcfoundation.org/UA-Profile/Server/Core2017Facet)

- **Catégorie de serveur > Facettes > Accès aux données** :
  - **Facette de serveur complexe 2017** (http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017)
  - **Facette de serveur d'accès aux données** (http://opcfoundation.org/UA-Profile/Server/DataAccess)
  - **Facette de serveur de souscription à modifications de données intégrée** (http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription)
- **Catégorie de serveur > Facettes > Fonctions générales**:
  - **Facette de serveur de méthodes** (http://opcfoundation.org/UA-Profile/Server/Methods)
- **Catégorie de sécurité > Facettes > Règles de sécurité**:
  - **Basic128RSA15** (http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15)
  - **Basic256** (http://opcfoundation.org/UA/SecurityPolicy#Basic256)
  - **Basic256Sha256** (http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256)
- **Catégorie de transport > Facettes > Client-Serveur**:
  - **UA-TCP- UA-SC UA-Binary** (http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary)

Les rubriques suivantes décrivent les services associés aux facettes référencées ci-dessus, prises en charge par ce module BMENUA0100.

Services de la pile du serveur OPC UA du BMENUA0100

Services OPC UA pris en charge

La pile du serveur OPC UA du module BMENUA0100 prend en charge les services et ensembles de services suivants :

Ensemble de services	Services
Attribute	• Lecture • Ecriture
Discovery	• FindServers • GetEndpoints
MonitoredItem	• CreateMonitoredItems • ModifyMonitoredItems • DeleteMonitoredItems • SetMonitoringMode
SecureChannel	• OpenSecureChannel

Ensemble de services	Services
	• CloseSecurechannel
Session	• CreateSession • ActivateSession • CloseSession
Subscription	• CreateSubscription • ModifySubscription • DeleteSubscription • SetPublishingMode • SetMonitoringMode • Publish • Republish
View	• Browse • BrowseNext • TranslateBrowsePathToNodeIds • RegisterNodes • UnregisterNodes

NOTE: Ces ensembles de services et services sont décrits dans le document *Spécifications de l'architecture unifiée OPC UA - Partie 4 : Services (version 1.04)*.

Services d'accès aux données de la pile serveur OPC UA du module BMENUA0100

Services d'accès aux données pris en charge

L'accès aux données par la pile serveur OPC UA intégré au module le module BMENUA0100 est possible par la prise en charge des facettes suivantes et services associés :

- Facette de serveur d'accès aux données (Data Access Server)
- Facette de serveur complexe 2017 (ComplexType Server)
- Facette de serveur central 2017 (Core Server)

NOTE: Dans les descriptions de facettes suivantes, le texte en italique est la traduction d'une citation du document source OPC Foundation . Cliquez sur les liens ci-dessous et utilisez l'outil de visualisation *OPC Foundation Unified Architecture Profile Reporting Visualization Tool* pour accéder à la description de chaque facette.

Facette de serveur central 2017 (Core Server)

La facette de serveur central 2017 *définit la fonctionnalité de base requise pour toute implémentation de serveur UA. La fonction de serveur central inclut la découverte des points terminaux, l'établissement de canaux de communication sécurisés, la création de sessions, l'accès à l'espace d'adresses et la lecture et/ou l'écriture des attributs des nœuds. Voici les principales conditions requises : prise en charge d'une seule session, prise en charge de l'objet de serveur et fonctionnalités du serveur, de tous les attributs obligatoires des noeuds dans l'espace d'adresses, et l'authentification par nom d'utilisateur et mot de passe. Pour une applicabilité étendue, les serveurs doivent prendre en charge plusieurs profils de transport et de sécurité.* Pour la description complète de cette facette, consultez http://opcfoundation.org/UA-Profile/Server/Core2017Facet.

La pile de serveur OPC UA intégré au module BMENUA0100 prend en charge les unités de conformité suivantes dans la facette de serveur central (Core Server 2017) :

- Ensemble de services View : inclut les groupes et services suivants :
  - View Basic : inclut les services de navigation Browse et BrowseNext.
  - View TranslateBrowsePath : inclut les services TranslateBrowsePathsToNodeIds.
  - View Register Nodes : inclut les services RegisterNodes et UnregisterNodes pour optimiser l'accès aux nœuds fréquemment utilisés dans l'espace d'adresses (AddressSpace) OPC UA du serveur.
- Ensemble de services Attribute : inclut les groupes et services suivants :
  - Attribute Read : inclut le service Read, qui prend en charge la lecture de un ou plusieurs attributs d'un ou plusieurs noeuds, notamment prend en charge le paramètre IndexRange pour lire un élément particulier ou une plage d'éléments lorsque la valeur de l'attribut est un tableau (array).
  - Attribute Write Values : inclut le service Write Value, qui prend en charge l'écriture d'une ou plusieurs valeurs sur un ou plusieurs attributs d'un ou plusieurs nœuds.
  - Attribute Write Index : inclut le service Write Index, qui prend en charge la plage d'index (IndexRange) pour l'écriture sur un élément ou une plage d'éléments si la valeur de l'attribut est un tableau et les mises à jour partielles sont autorisées pour ce tableau.

Facette de serveur d'accès aux données (Data Access Server)

La facette de serveur d'accès aux données *définit la prise en charge d'un modèle d'information utilisé pour fournir des données d'automatisation industrielle. Ce modèle définit les structures standard pour les éléments de données analogiques et TOR et leur qualité de service. Cette facette complète la facette de serveur central (Core Server) pour ajouter la prise en charge du fonctionnement de base de l'espace d'adresses.* Pour la description complète de cette facette, consultez http://opcfoundation.org/UA-Profile/Server/DataAccess.

Facette de serveur complexe 2017 (ComplexType Server)

La facette de serveur complexe 2017 *complète la facette de serveur central (Core Server) pour inclure des variables aux données structurées, c'est-à-dire des données constituées de plusieurs éléments tels qu'une structure et où les éléments sont présentés sous forme de variables de composant. La prise en charge de cette facette requiert l'implémentation de types de données structurés et de variables qui utilisent ces types de données. L'ensemble de services Read, Write et Subscriptions prend en charge le codage et le décodage de ces types de données structurés. Le serveur peut prendre en charge d'autres types de codage, tel que XML lorsque le protocole binaire est utilisé, et vice-versa.* Pour la description complète de cette facette, consultez http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017.

Services de sécurité et de découverte de la pile serveur OPC UA du module BMENUA0100

Introduction

La pile du serveur OPC UA intégré au module BMENUA0100 prend en charge à la fois des services de découverte et des services de sécurité.

Pour se connecter au serveur OPC UA sur le module BMENUA0100, un client OPC UA requiert des informations décrivant le serveur, notamment son adresse réseau, le protocole et les paramètres de sécurité. L'architecture OPC UA définit un ensemble de fonctionnalités de découverte que le client peut utiliser pour obtenir ces informations.

Les informations nécessaires à établir une connexion entre un client OPC UA et un serveur OPC UA sont stockées sur un point terminal. Un serveur OPC UA peut comporter plusieurs points terminaux, chacun contenant :

- URL de point terminal (adresse réseau et protocole), par exemple :
  - Pour IPv4 : opc.tcp://172.21.2.30:4840, où :

    - opc.tcp = protocoles

    - 172.21.2.30 = adresse IPv4

    - 4840 = numéro de port opcua-tcp configuré dans Control Expert
  - Pour IPv6 : opc.tcp://[2a01:cb05:431:f00:200:aff:fe02:a0a]:50000, où :

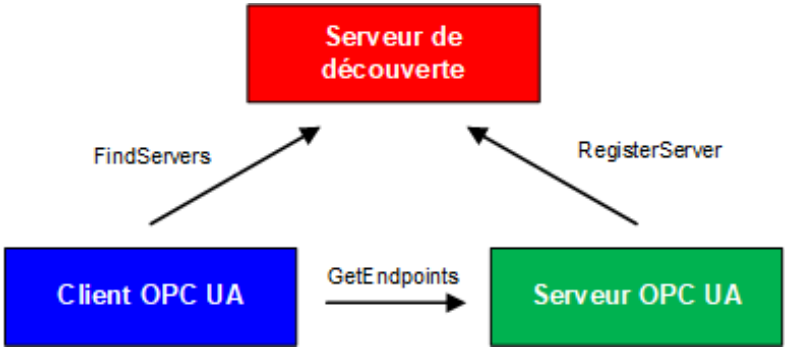
    - opc.tcp = protocoles

    - [2a01:cb05:431:f00:200:aff:fe02:a0a] = adresse IPv6

    - 50000 = numéro de port opcua-tcp configuré dans Control Expert
- Règles de sécurité (notamment ensemble d'algorithmes de sécurité et longueur de clé)
- Mode de sécurité des messages (niveau de sécurité pour les messages échangés)

- Type de jeton utilisateur (types d'authentification d'utilisateur pris en charge par le serveur)

Il peut y avoir un ou plusieurs serveurs OPC UA. Dans le cas de plusieurs serveurs, un serveur de découverte peut fournir les informations relatives à chacun des serveurs. Chaque serveur peut s'enregistrer auprès du serveur de découverte. Les clients peuvent demander au serveur de découverte une liste de serveurs disponibles (tous les serveurs ou une partie), et utiliser le service GetEndpoints pour obtenir les informations de connexion auprès de chaque serveur.



Le module BMENUA0100 prend en charge plusieurs services de découverte et services de sécurité, notamment :

- Ensemble de services Discovery
- Ensemble de services SecureChannel
- Ensemble de services Session

La décision d'activer ou de désactiver des services dépend de la règle de cybersécurité que vous choisissez d'implémenter pour le serveur.

Ensemble de services Discovery

La pile de serveur OPC UA du module BMENUA0100 prend en charge l'ensemble de services Discovery, qui est intégré à la facette de serveur central 2017, page 37. L'implémentation sur le module BMENUA0100 prend en charge les services suivants :

- FindServers : Dans l'implémentation sur la pile du serveur OPC UA du module BMENUA0100, ce service recherche tous les serveurs sur le serveur OPC UA local uniquement.
- GetEndpoints : Renvoie les points terminaux (Endpoints) pris en charge par un serveur et toutes les informations de configuration requises pour établir un canal sécurisé (SecureChannel) et une Session. Peut fournir une liste de retour des points terminaux, en fonction des profils.

Ensemble de services SecureChannel

La pile serveur OPC UA du module BMENUA0100 prend en charge l'ensemble de services SecureChannel, qui inclut les services suivants :

- OpenSecureChannel : Ouvre ou renouvelle un canal sécurisé (SecureChannel) qui fournit la confidentialité et l'intégrité de l'échange des messages pendant une session. Ce Service requiert que la pile du serveur OPC UA applique les divers algorithmes de sécurité aux messages lors de leur envoi et leur réception.
- CloseSecureChannel : Ferme un canal sécurisé.

Ensemble de services Session

La pile de serveur OPC UA du module BMENUA0100 prend en charge l'ensemble de services Session, qui est intégré à la facette de serveur central 2017, page 37. L'implémentation sur le module BMENUA0100 prend en charge les services suivants :

- CreateSession : Après la création d'un canal sécurisé avec le service OpenSecureChannel, un client utilise ce service pour créer une session. Le serveur renvoie deux valeurs qui identifient de façon unique la session :
  - Un ID de session, qui permet d'identifier la session dans les journaux d'audit et dans l'espace d'adresses du serveur.
  - Un jeton d'authentification (authenticationToken), qui permet d'associer une requête entrante à une session.
- ActivateSession : Utilisé par le client pour spécifier l'identité de l'utilisateur associé à la session. Ne peut pas être utilisé pour changer l'utilisateur de la session.
- CloseSession : Met fin à une session.

  NOTE: Pour les services CreateSession et ActivateSession, si SecurityMode = None, alors :

  1. Le certificat d'application et le nombre nonce sont facultatifs.
  2. Les signatures sont nulles ou vides.

Services de publication et de souscription de la pile serveur OPC UA du module BMENUA0100

Souscriptions

Au lieu d'une lecture continue des informations par interrogation, le protocole OPC UA inclut une fonction de souscription. Cette fonction permet à la pile hautes performances OPC UA

intégrée au module BMENUA0100 de fournir des services de publication/souscription qui sont utilisés lors de la connexion du module aux équipements distants.

Un client OPC UA peut s'inscrire à un ou plusieurs noeuds sélectionnés et laisser le serveur surveiller ces éléments. En cas d'événement de changement, par exemple un changement de valeur, le serveur informe le client du changement. Ce mécanisme réduit notablement la quantité de données transférées. Il s'ensuit une réduction de la consommation de bande passante et cette méthode est recommandée pour la lecture des informations d'un serveur OPC UA.

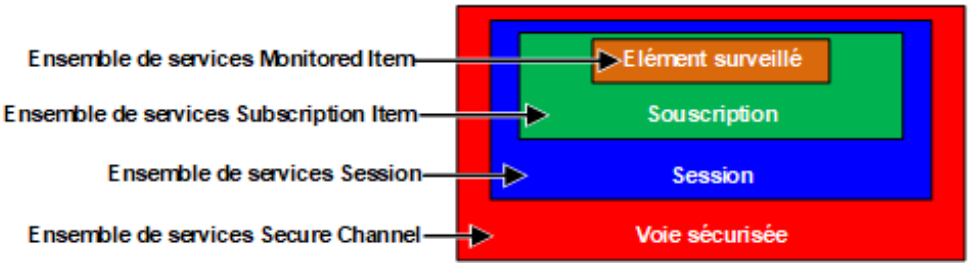
Un client OPC UA peut souscrire à un ou plusieurs types d'informations fournies par un serveur OPC UA. La souscription regroupe ces types de données, appelés éléments surveillés, pour constituer un ensemble de données appelées Notification.

Conditions requises pour une souscription :

- Elle doit inclure au moins un élément surveillé.
- Elle doit être créée dans le contexte d'une Session, laquelle est créée dans le contexte d'un canal sécurisé.

NOTE: La souscription peut être transférée à une autre session.

Les ensembles de services impliqués dans une souscription de client sont décrits ci-dessous :



Souscriptions et dépassements

Dans certains cas, lorsqu'il existe un grand nombre de demandes de souscription, le serveur OPC UA tente d'obtenir de la CPU une quantité de données supérieure à ce que la CPU ou le module BMENUA0100 peut traiter dans l'intervalle de publication spécifié. Dans ce cas, le temps d'exécution des demandes d'abonnement est automatiquement prolongé (et l'exécution de la souscription suivante reportée) jusqu'à ce que toutes les demandes soient traitées.

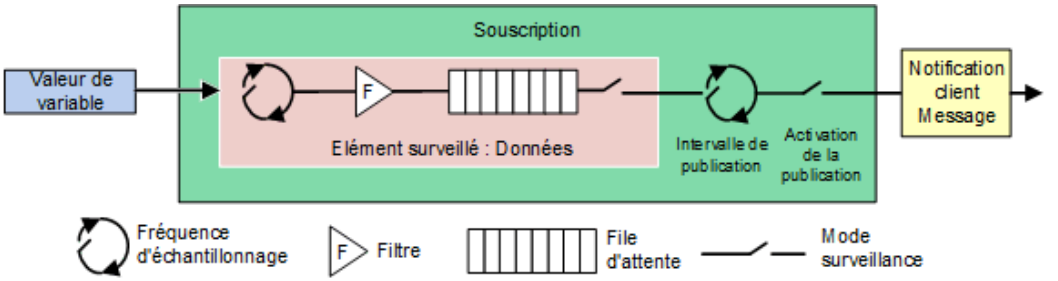
Lorsque vous définissez un intervalle de publication, tenez compte du nombre de clients et de requêtes client que le serveur doit gérer. Lorsque vous déterminez le nombre de requêtes client, vérifiez que tous les clients fonctionnent en ligne. A cet égard, notez que certains clients peuvent prendre 2 minutes ou plus pour se connecter après le démarrage.

NOTE: Un intervalle de publication égal à deux fois l'intervalle d'échantillonnage est recommandé.

Événements de changement

Un client peut s'inscrire à un événement de changement de données, qui est déclenché par un changement de la valeur de l'attribut d'une variable, en tant qu'élément surveillé.

Les paramètres configurables de la souscription, leur ordre et leurs rôles, sont décrits ci-dessous :



Les trois paramètres suivants déterminent comment les éléments surveillés sont ajoutés à une souscription :

- Intervalle d'échantillonnage : intervalle de temps d'échantillonnage défini pour chaque élément surveillé de la souscription. Il s'agit de la fréquence à laquelle le serveur vérifie si la source de données a été modifiée. Pour un élément de variable, l'intervalle d'échantillonnage peut être inférieur (plus rapide) que la période entre les notifications au client. Dans ce cas, le serveur OPC UA peut mettre en file d'attente les échantillons et publier la file complète. Dans des cas extrêmes, le serveur corrige (ralentit) l'intervalle d'échantillonnage pour que la source de données ne subisse pas de charge excessive en file d'attente pouvant être causée par l'échantillonnage.

  NOTE: Si la mise en file d'attente OPC UA des échantillons de données est prise en charge, la taille de la file d'attente (nombre maximal de valeurs à mettre en file d'attente) peut être configurée pour chaque élément surveillé (Monitored Item). Si les données sont fournies (publiées) au client, la file d'attente est vidée. En cas de débordement de la file d'attente, les données les plus anciennes sont supprimées et remplacées par les nouvelles données.

- Filtre : ensemble de critères appliqués pour identifier les événements ou changements de données à signaler, et lesquels doivent être bloqués.
- Mode de surveillance : permet d'activer ou de désactiver l'échantillonnage et les comptes-rendus.

Les deux paramètres suivants s'appliquent à la souscription :

- Intervalle de publication : Période au bout de laquelle les notifications collectées dans les files d'attente sont transmises au client dans un message de notification (réponse de publication). Le client OPC UA doit confirmer que le serveur OPC UA a reçu assez de jetons de publication (requêtes de publication), de sorte que si l'intervalle de publication est écoulé et qu'une notification est prête à être envoyée, le serveur utilise un jeton et envoie les données dans une réponse de publication. S'il n'y a rien à signaler (par exemple aucun changement de valeur) le serveur envoie une notification KeepAlive au client, qui est une publication vide indiquant que le serveur est actif.
- Activation publication : Active et désactive l'envoi du message de notification.

Facette de serveur de souscription à modifications de données (intégrée)

La facette de serveur de souscription à modifications de données intégrée *définit le niveau minimal de prise en charge des notifications de changement de données dans les souscriptions. Inclut les limites qui réduisent l'utilisation de mémoire et de temps système nécessaire pour implémenter la facette. Cette facette inclut des fonctions pour créer, modifier et supprimer des souscriptions et pour créer, modifier et supprimer des éléments surveillés. Pour chaque Session, les serveurs doivent prendre en charge au moins une souscription incluant jusqu'à deux éléments. De plus, la prise en charge de deux requêtes de publication parallèles est nécessaire. Cette facette est conçue pour une plateforme tel que celle que fournit le profil de serveur d'équipements intégré Micro où la mémoire est limitée et doit être gérée.* Pour la description complète de cette facette, consultez http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription.

Cette facette prend en charge les services suivants :

- Ensemble de services Monitored Item
- Ensemble de services Subscription

Ensemble de services Monitored Item

L'ensemble de services Monitored Item prend en charge les services suivants :

- CreateMonitoredItems : appel asynchrone qui permet de créer et d'ajouter un ou plusieurs éléments surveillés (MonitoredItems) à une souscription.
- ModifyMonitoredItems : appel asynchrone qui permet de modifier des éléments surveillés. Ce service permet de modifier les MonitoredItems d'une souscription. La modification des paramètres MonitoredItem doivent être appliqués immédiatement par le serveur. Ces modifications sont appliquées dès que possible.
- DeleteMonitoredItems : appel asynchrone qui permet de supprimer des éléments surveillés. Ce service permet de supprimer un ou plusieurs MonitoredItems d'une souscription. Si un MonitoredItem est supprimé, les liens déclenchés par l'élément sont également supprimés.

- SetMonitoringMode : appel asynchrone qui permet de définir le mode de surveillance d'une liste d'éléments surveillés. Ce service permet de définir le mode de surveillance d'un ou plusieurs MonitoredItems d'une souscription. La sélection du mode DISABLED entraîne la suppression de toutes les notification en file d'attente.

Ensemble de services Subscription

L'ensemble de services Subscription prend en charge les services suivants :

- CreateSubscription : appel asynchrone pour créer une souscription.
- ModifySubscription : appel asynchrone pour modifier une souscription. Le serveur applique immédiatement les modifications à la souscription, et les modifications sont appliquées dès que possible.
- DeleteSubscription: appel asynchrone pour supprimer une ou plusieurs souscriptions appartenant à la session client. L'exécution de ce service entraîne la suppression de tous les Monitored Items associés à la souscription.
- Publish : ce service est utilisé dans deux buts : acquitter la réception des NotificationMessages pour une ou plusieurs souscriptions, et demander au serveur de renvoyer un message de notification ou un message keep-alive.
- Republish : un appel asynchrone de republication pour obtenir les notifications perdues. Ce service demande à la souscription de republier un message de notification de la file d'attente de retransmission. Si le serveur n'a pas le message demandé dans sa file d'attente de retransmission, il renvoie une réponse d'erreur.
- SetPublishingMode : appel asynchrone pour activer l'envoi de notifications sur une ou plusieurs souscriptions.

Services de transport de la pile du serveur OPC UA BMENUA0100

Prise en charge de la facette UA-Binary UA-TCP UA-SC

Le module BMENUA0100 prend en charge la facette de transport UA-Binary UA-TCP UA-SC. (pour plus d'informations, consultez la description en ligne à l'adresse http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary.)

Cette facette de transport définit une combinaison de protocoles réseau, de protocoles de sécurité et de codage de message, optimisée pour la faible consommation de ressources et les hautes performances. Elle associe le protocole réseau TCP simple UA-TCP 1.0 au protocole de sécurité binaire UA-SecureConversation 1.0 et au codage de message binaire UA-Binary 1.0.

Les données qui circulent entre un client OPC UA et le serveur OPC UA intégré au module BMENUA0100 utilisent le protocole TCP et sont codées au format binaire conforme au format de fichier binaire OPC UA.

NOTE: Le format de fichier binaire OPC UA (Binary File Format) remplace le schéma XML UA-Nodeset Schema de OPC Foundation. Il améliore les performances et la consommation de mémoire. Il ne requiert pas d'analyseur XML.

Détection des variables du PAC

Mappage entre variables de PAC Control Expert et variables de logique de données OPC UA

Introduction

Le serveur OPC UA intégré au module BMENUA0100 utilise des requêtes du dictionnaire de données UMAS (Unified Messaging Application Services) pour chercher et détecter des variables d'application des PAC M580. Vous devez activer le dictionnaire de données dans les paramètres du projet dans Control Expert.

NOTE:

- Le module BMENUA0100 prend en charge une taille de dictionnaire de données maximale de 100 000 variables.
- Le temps nécessaire au chargement du dictionnaire de données dans le serveur OPC UA dépend du nombre d'éléments du dictionnaire de données et du réglage de la période MAST, page 165.

Toutes les variables collectées sont converties du modèle de logique de données Control Expert en modèle de logique de données OPC UA en utilisant les services de la pile OPC UA appropriés. Un client OPC UA connecté au module BMENUA0100 (sur son port de contrôle, ou sur son port d'embase via la CPU ou un module de communication BMENOC0301/11) peut récupérer cet ensemble de données en utilisant les services de la facette de serveur d'accès aux données, page 37 prise en charge par le profil de serveur UA 2017 intégré , page 34.

Préchargement du dictionnaire de données pour éviter l'interruption des communications

Une modification d'application en ligne effectuée avec Control Expert cause des interruptions temporaires de la communication serveur/client OPC UA lorsque le serveur récupère le dictionnaire de données mis à jour. Cette interruption est causée par un

mappage incohérent des données UC lors de la mise à jour du dictionnaire de données. Durant la période de perte de communication, l'état des nœuds surveillés devient BAD. Pour éviter cette interruption des opérations, un mécanisme de synchronisation peut être défini entre le module BMENUA0100 et le logiciel de configuration Control Expert, pour effectuer un préchargement du dictionnaire de données mis à jour.

Cette fonction est activée dans Control Expert, fenêtre **outils > Options du projet...**, zone **Général > Données intégrées de l'automate**, paramètres (voir ™EcoStruxure Control Expert, Modes de fonctionnement) **Préchargement après la génération** et **Délai de génération effectif**. Reportez-vous à ces rubriques dans l'aide en ligne de Control Expert pour plus d'informations sur la manière de configurer cette fonction.

Activation du dictionnaire de données

Pour activer le dictionnaire de données dans Control Expert :

Étape	Action
1	Dans Control Expert, le projet ouvert, sélectionnez **Outils > Paramètres du projet**.
2	Dans la fenêtre **Paramètres du projet**, accédez à **Général > Données intégrées de l'automate**, puis sélectionnez **Dictionnaire de données**. **NOTE:** Si le projet EcoStruxure™ Control Expert inclut un module BMENUA0100 et que cette option n'est pas sélectionnée, une erreur détectée est générée lors de la compilation de l'application.

Conversion des types de données de variables

Le module BMENUA0100 peut détecter et convertir en type de données OPC UA les types de variable élémentaires suivants pris en charge par le modèle de logique de données Control Expert :

Type de données élémentaire Control Expert	Type de données OPC UA
BOOL	Boolean
EBOOL	Boolean
INT	Int16
DINT	Int32
UINT	UInt16
UDINT	UInt32
REAL	Float
BYTE	Byte

Type de données élémentaire Control Expert	Type de données OPC UA
WORD	UInt16
DWORD	UInt32
DATE*	UInt32
TIME*	UInt32
TOD*	UInt32
DT*	Double
STRING	Tableau d'octets
* Consultez le tableau suivant qui décrit la conversion de types de données relatifs à la date.	

Pour les données Control Expert de types DATE, TIME, TOD, DT, les types de données OPC UA correspondants sont les suivants :

Type de données élémentaire Control Expert	Exemple de valeur affichée dans Control Expert	Type de données OPC UA	Valeur correspondante dans le type OPC UA
DATE	D#2017-05-17	UInt32	0x20170517
TIME	T#07h44m01s100ms	UInt32	27841100
TOD	TOD#07:44:01	UInt32	0x07440100
DT[1]	DT#2017-05-17-07:44:01	Double	4.29E-154
1. Les données renvoyées pour les valeurs de date et d'heure sont UATypeUInt64, qui est le codage interne du type IEC 1131 DT dans Control Expert - codage BCD (décimal codé binaire).			

Variables détectables

Pour toutes les variables, le client OPC UA n'accède pas directement à la variable de logique de données de PAC détectée. Le client accède à la variable de PAC détectée via une variable de logique de données OPC UA, qui est située dans le module BMENUA0100 et mappée à la variable de PAC sous-jacente. En raison de la nature transférable de l'accès aux variables de données, le processus de demande d'acquisition n'est pas optimisé, et les performances d'acquisition du dictionnaire de données ne sont pas représentatives des performances du PAC.

NOTE: Les références de type REF_TO aux variables d'application sur le serveur OPC UA ne sont pas accessibles par le client OPC UA.

Voici des exemples de variables de PAC Control Expert détectables par le serveur OPC UA sur le module BMENUA0100 :

- Variables structurées avec sous-champs : Variables de type DDT et tableau.

- Les variables d'unité de programme sont détectables comme suit :
  - Les variables d'entrée/sortie sont accessibles par le client OPC UA uniquement pour le type BOOL.
  - Les variables d'entrée et les variables de sortie sont accessibles par le client OPC UA, sauf les types REF_TO, ARRAY, String et Structure.

De plus, les variables suivantes sont détectables par me serveur OPC UA par mappage aux variables d'application, puis détection des variables d'application mappées :

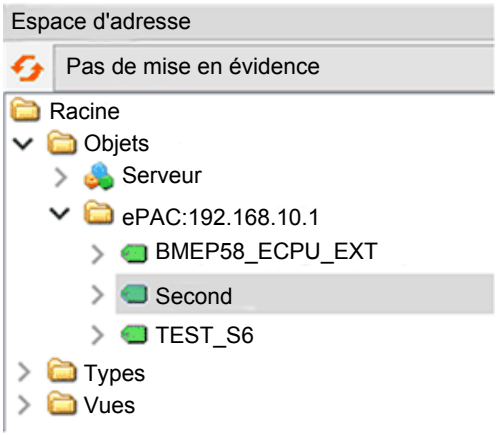
- Variables d'E/S topologiques :
  - Entrées : %I, %IW, %ID, %IF.
  - Sorties : %Q, %QW, %QD, %QF.
- Variables localisées : %M, %MW, %MD, %MF.
- Variables système : %S, %SW, %SD.

NOTE: La détection des variables inclut une variable (ou un symbole) pour un bit extrait (par exemple, MyBoolVar situé dans %MW100.1).

Présentation des variables détectées sur le client OPC UA

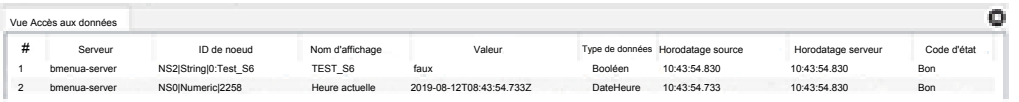
Le serveur OPC UA du module BMENUA0100 peut organiser et afficher sous forme graphique les variables de PAC détectées. Un outil client OPC UA peut se connecter au module BMENUA0100 et afficher une arborescence des variables du serveur OPC UA.

Dans l'exemple suivant, un client OPC UA (ici l'outil client Unified Automation UaExpert) connecté au module BMENUA0100 peut afficher les variables du PAC dans la fenêtre **Espace d'adresse**. L'adresse IP du PAC M580 est représentée par le noeud ePAC:192.168.10.1. Ses noeuds enfants représentent des variables d'application Control Expert :



Dans l'exemple ci-dessus, le premier sous-noeud, BMEP58_ECPU_EXT, représente le DDT d'équipement pour l'UC M580, qui a été automatiquement instancié lors de l'ajout de l'UC à l'application Control Expert. Les noeuds suivants représentent d'autres objets ajoutés à l'application.

En utilisant l'outil client OPC UA, le noeud TEST_S6 a été déplacé et déposé dans la vue **Accès aux données** de l'outil, où les informations de la variable s'affichent :


Vue Accès aux données

#	Serveur	ID de noeud	Nom d'affichage	Valeur	Type de données	Horodatage source	Horodatage serveur	Code d'état
1	bmenua-server	NS2|String|0:Test_S6	TEST_S6	faux	Booléen	10:43:54.830	10:43:54.830	Bon
2	bmenua-server	NS0|Numeric|2258	Heure actuelle	2019-08-12T08:43:54.733Z	DateHeure	10:43:54.733	10:43:54.830	Bon

Dans ce cas, le type de données OPC UA des variables est *Boolean* (ce qui indique que le type de données PAC sous-jacent est BOOL) et la valeur est *false*.

NOTE: L'attribut **Horodatage serveur** des noeuds OPC UA est reçu du serveur OPC UA du module BMENUA0100 au format UTC (Universal Time Coordinated). Il s'affiche pour l'utilisateur en temps réel. Les données ne sont pas horodatées sur leur source respective mais par le serveur OPC UA. Pour éviter les conflits de compatibilité avec certains clients OPC UA, l'horodatage à la source et l'horodatage du serveur sont configurés avec la même valeur d'horodatage serveur.

Lecture et écriture des variables détectées sur le client OPC UA

Une balise OPC UA sur un client OPC UA (par exemple SCADA) qui référence une variable de tableau permet au client de lire ou écrire tous les éléments du tableau. Par exemple la balise ‘MyArray’ déclarée comme ARRAY[0...31] OF INT.

Cependant, pour que le client puisse lire ou écrire un élément d'un tableau, il est nécessaire de déclarer une balise spécifique qui référence l'élément de tableau ciblé. Par exemple ‘MyInt’ déclarée comme INT référençant MyArray[2].

Redondance d'UC

Redondance de serveur OPC UA

Deux types de redondance

Le module BMENUA0100 prend en charge les types de redondance suivants :

- Architecture Hot Standby, qui décrit les UC redondantes.
- Redondance de serveur OPC UA, qui décrit l'utilisation de modules BMENUA0100 redondants.

La redondance de serveur OPC UA, qui est gérée par les modules BMENUA0100, est conforme à la norme OPC UA de *redondance de serveur non transparente en mode de basculement à chaud.*

Ces deux types de redondance peuvent être combinés. Les modèles suivants sont pris en charge :

- Un PAC autonome contenant deux modules BMENUA0100.
- Deux PAC à redondance d'UC (Hot Standby) contenant chacun un ou deux modules BMENUA0100.

Redondance OPC UA

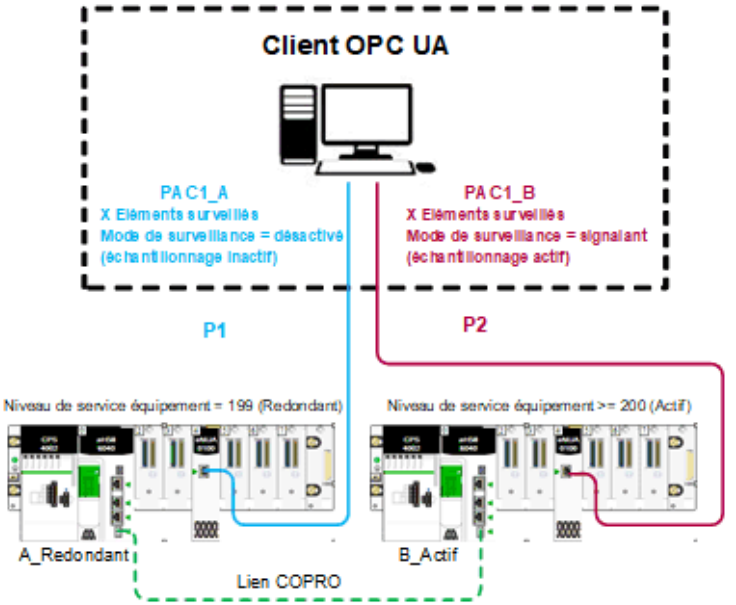
Dans une architecture OPC UA de redondance de serveur non transparente en mode de basculement à chaud, il incombe au client OPC UA d'établir les sessions et de gérer les communications avec les serveurs redondants. Les sessions à établir comprennent une session active avec le serveur primaire et une session inactive avec le serveur secondaire (redondant). Le client doit configurer ces deux sessions pour inclure les mêmes éléments surveillés.

Il incombe également au client OPC UA de vérifier l'état des deux serveurs via la variable SERVICE_LEVEL et de commuter la communication vers le serveur qui présente le meilleur état d'après la valeur de cette variable.

La norme OPC UA stipule que l'activation des communications s'effectue en réglant le *mode de surveillance* des différentes sessions sur la valeur correcte. Le *mode de surveillance* des serveurs est contrôlé par le client OPC UA et la procédure de réglage de ce mode dépend de l'implémentation du client. Pour plus d'informations sur le réglage du *mode de surveillance*, reportez-vous à la documentation du client.

Ce principe est général et s'applique à toute architecture, y compris à l'architecture de redondance d'UC (Hot Standby).

Le schéma suivant représente un client OPC UA connecté à une paire de serveurs OPC UA redondants (chacun étant intégré dans un module BMENUA0100). Le client a désigné comme serveur actif celui qui présente la valeur SERVICE_LEVEL la plus élevée :



Redondance d'UC

Dans une configuration de redondance d'UC (Hot Standby), deux (2) modules BMENUA0100 au maximum peuvent être installés dans chaque rack local principal Hot Standby. Chaque module BMENUA0100 est configuré avec une adresse IP statique unique. Les modules BMENUA0100 conservent leurs adresses IP respectives et n'échangent pas d'adresses IP lors d'un basculement ou d'une permutation Hot Standby.

NOTE: Sur un système redondant, vérifiez que les modules BMENUA0100 des PAC primaire et secondaire :

- sont configurés avec les mêmes paramètres de cybersécurité, page 84,
- ont leur sélecteur rotatif, page 20 (situé à l'arrière du module) sur la même position,
- sont installés dans le même numéro de logement, page 60 dans les racks principaux locaux respectifs.

Le système n'effectue pas automatiquement ces vérifications.

Le DDT du module BMENUA0100 inclut la variable SERVICE_LEVEL, page 148, qui fournit à la CPU des informations concernant l'état du serveur OPC UA dans le module

BMENUA0100. Le client OPC UA est informé de l'état du serveur OPC UA via la variable SERVICE_LEVEL, laquelle est disponible en tant que variable OPC UA.

NOTE: Incluez toujours la fonction élémentaire READ_DDT en vue de mettre à jour le DDT de chaque module BMENUA0100. Dans une configuration Hot Standby, ajoutez READ_DDT à une section de code qui s'exécute lorsque l'UC est en mode redondant. Cette conception envoie les informations de diagnostic de BMENUA0100 échangeables entre les UC primaire et secondaire. L'application peut utiliser ces informations pour exécuter une vérification de la cohérence des services et configurations de la cybersécurité pris en charge pour les modules BMENUA0100 des UC primaire et secondaire.

Si le DDT T_M_ECPU_HSBY (voir Modicon M580 - Système de redondance d'UC - Guide de planification du système pour les architectures courantes) de l'UC redondante et son élément CMD_SWAP sont rendus disponibles en tant que variables IHM dans un système SCADA, l'application SCADA peut déclencher une permutation en écrivant dans la variable OPC UA mappée appropriée dans le BMENUA0100.

Dans un système redondant, le module BMENUA0100 qui gère les communications OPC UA avec le système SCADA peut être celui qui est situé dans le rack local secondaire (redondant). C'est pourquoi vous devez sélectionner l'attribut **Echange sur l'automate redondant** pour toutes les variables d'application scrutées pour assurer la cohérence des valeurs des variables entre les PAC primaire et redondant.

De plus, pour maintenir la cohérence, les applications des deux PAC redondants doivent être synchronisées.

Dans de rares cas (principalement si le bit ECPU_HSBY_1.PLCX_ONLINE est défini sur false manuellement ou par programme), l'un des PAC du système redondant peut être en mode attente (Wait). Dans ce mode, ce PAC (secondaire) n'est pas synchronisé avec le PAC primaire et les variables lues par ce PAC sont inexactes. L'état du PAC de réponse peut être surveillé via les champs suivants du DDT du T_M_ECPU_HSBY :

- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.WAIT
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.RUN_PRIMARY
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.RUN_STANDBY
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.STOP

Le système redondant permet aux deux PAC de fonctionner durant l'exécution de différentes applications. Pour assurer la cohérence des variables entre les PAC primaire et redondant, la configuration des données des deux PAC doit être cohérente, comme indiqué par le champ DDT T_M_ECPU_HSBY :

- T_M_ECPU_HSBY_1.DATA_LAYOUT_MISMATCH = false

  NOTE: Lorsque la redondance OPC UA est configurée, il est recommandé de vérifier par programme les DDT des modules afin de s'assurer de la cohérence des services pris en charge et des configurations de cybersécurité entre les modules BMENUA0100.

NOTE: Dans les sections suivantes de cette rubrique, le contenu provient du document suivant :

OPC Unified Architecture Specification Part 4: Services, Release 1.04, abrégé ci-après en *OPC UA Part 4* suivi de la référence de la section. Le texte issu de ce document et traduit en français est en *italique*.

Prise en charge OPC UA pour serveurs, clients et réseaux redondants

OPC UA permet la redondance des serveurs, clients et réseaux. OPC UA fournit les structures de données et les services qui permettent de réaliser la redondance de façon standardisée.

La redondance des serveurs permet aux clients de disposer de plusieurs sources pour obtenir les mêmes données. La redondance des serveurs peut être obtenue de plusieurs façons, certaines nécessitent l'interaction du client, d'autres non. Les serveurs redondants peuvent être mis en place sur des systèmes sans redondance de réseaux ou de clients. Les serveurs redondants peuvent aussi coexister sur des systèmes avec redondance de réseaux et de clients...

La redondance de client permet à des clients configurés de façon identique de fonctionner comme un client unique, mais tous les clients n'obtiennent pas les données à un moment donné. En principe, il n'y a aucune perte d'information en cas de basculement de client. Les clients redondants peuvent être mis en place sur des systèmes sans redondance de réseaux ou de serveurs. Les clients redondants peuvent aussi coexister sur des systèmes avec redondance de réseaux et de serveurs...

La redondance de réseau permet à un client et un serveur de disposer de plusieurs chemins de communication pour obtenir les mêmes données. Les réseaux redondants peuvent être mis en place sur des systèmes sans redondance de serveurs ou de clients. Les réseaux redondants peuvent également coexister sur des systèmes avec redondance de client et de serveur... OPC UA Part 4, section 6.6.1.

Redondance de serveurs

Les deux principaux modes de redondance de serveurs sont : transparent et non transparent.

En redondance transparente, le basculement des responsabilités du serveur d'un serveur à l'autre est transparent pour le client. Le client ne détecte pas le basculement et n'a aucun contrôle sur le fonctionnement du basculement. De plus, le client n'a pas à effectuer des actions supplémentaires pour continuer à envoyer ou recevoir des données.

En mode non transparent, le basculement d'un serveur à l'autre et les actions pour continuer à envoyer et recevoir des données sont effectués par le client. Le client doit connaître le

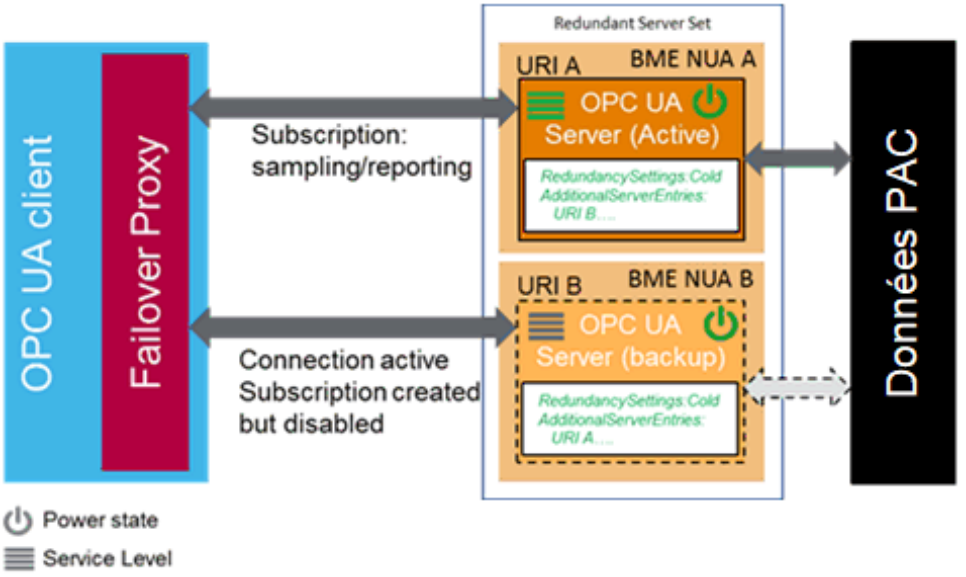
serveur redondant défini et doit effectuer les actions nécessaires pour bénéficier de la redondance de serveurs.

L'objet ServerRedundancy... indique le mode pris en charge par le serveur. Le type ServerRedundancyType et ses sous-types TransparentRedundancyType et NonTransparentRedundancyType ... fournissent des informations sur le mode de redondance pris en charge. OPC UA Part 4, section 6.6.2

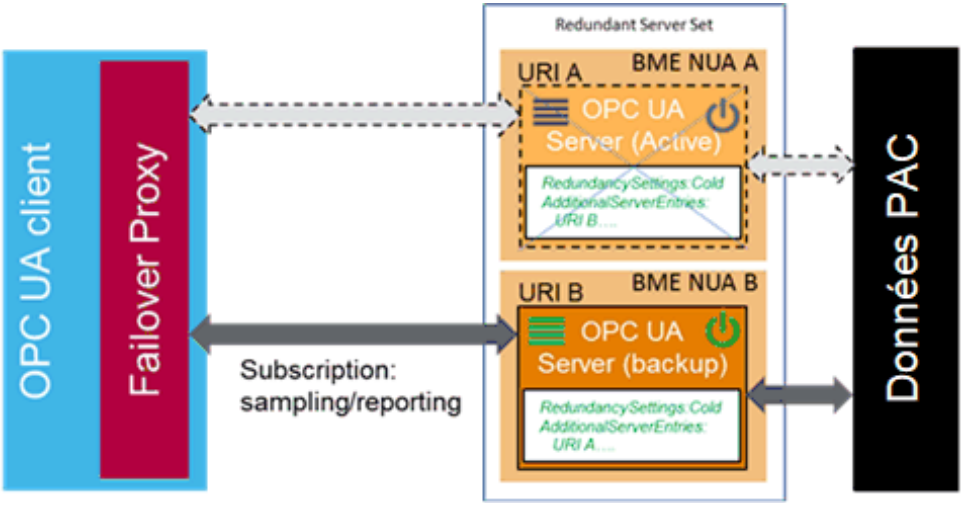
Comme indiqué ci-dessus, le serveur OPC UA intégré au module BMENUA0100 prend en charge la redondance de serveur non transparente en mode de basculement à chaud.

Mode de basculement à chaud du serveur OPC UA

En mode de basculement à chaud, *le ou les serveurs secondaires peuvent être actifs, mais ne peuvent pas se connecter aux points de donnés réels.* Par conséquent, un seul serveur peut consommer des données de l'application Control Expert. *La variable ServiceLevel ... indique la capacité du serveur à fournir ses données au client. OPC UA Part 4, section 6.6.2.4.4*



Lors d'un basculement, une action du client OPC UA est nécessaire, le serveur OPC UA intégré au BMENUA0100 devient inactif :



Fonctionnement du basculement du client

Chaque serveur gère une liste des identifiants URI (ServerUris) de tous les serveurs inclus dans l'ensemble de serveurs redondants (Redundant Server Set).

NOTE: Un ensemble Redundant Server Set inclut les serveurs OPC UA configurés pour assurer la redondance dans l'application Control Expert.

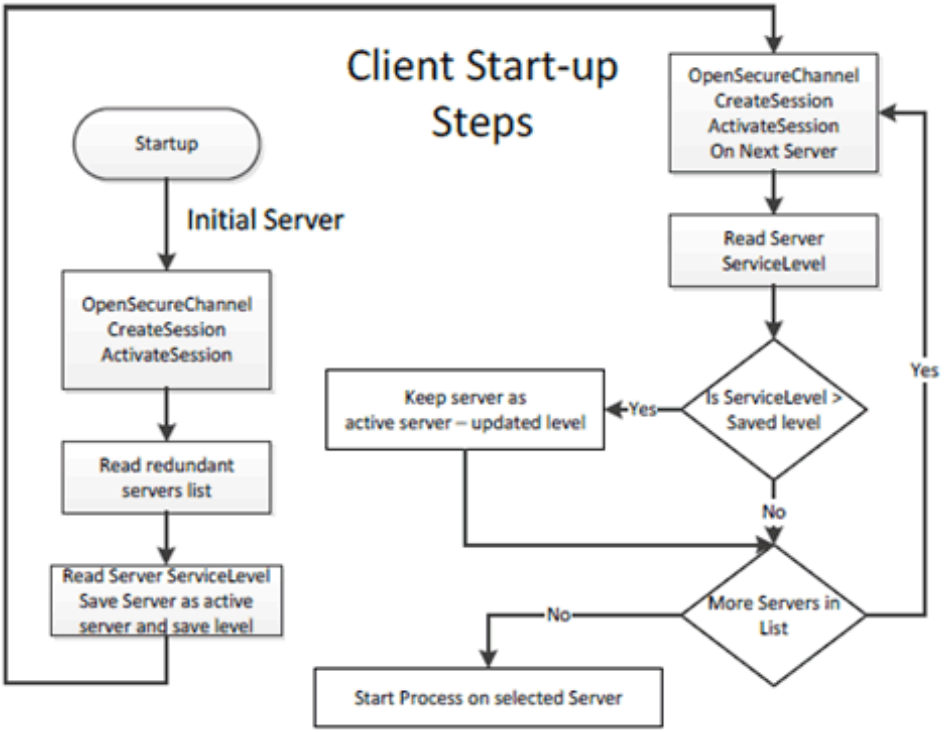
La liste est fournie avec le mode de basculement (Failover) dans l'objet ServerRedundancy. Pour permettre aux clients de se connecter à tous les serveurs de la liste, chaque serveur de la liste doit fournir la description de l'application (ApplicationDescription) pour tous les serveurs de l'ensemble Redundant Server Set via le service FindServers. Le client a besoin de ces informations pour convertir l'URI du serveur (ServerUri) en informations permettant la connexion aux autres serveurs de l'ensemble Redundant Server Set. Par conséquent, un client doit se connecter à un seul serveur redondant pour trouver les autres serveurs via les informations fournies. Un client doit conserver les informations sur les autres serveurs de l'ensemble Redundant Server Set. OPC UA Part 4, section 6.6.2.4.5.1

Exemples d'options du client en mode de basculement à chaud :

- Lors de la première connexion, en plus des actions sur le serveur actif :
  - Connexion à plusieurs serveurs OPC UA.
  - Création de souscriptions et ajout d'éléments surveillés (Monitored Item).

- Lors d'un basculement :
  - Activation de l'échantillonnage des souscriptions.
  - Activation de publication.

Les clients qui communiquent avec un ensemble de serveurs Redundant Server Set non transparent requièrent de la logique supplémentaire pour gérer les défaillances de serveur et enclencher le basculement sur un autre serveur de l'ensemble Redundant Server Set. La figure suivante *présente les étapes de la première connexion d'un client à un ensemble Redundant Server Set.*



Le serveur initial peut être déterminé via la fonction de découverte standard ou via une liste de serveurs dans l'ensemble Redundant Server Set. Dans tous les cas, le client a besoin de vérifier à quel serveur de l'ensemble il doit se connecter. Les actions particulières dépendent du mode de basculement fourni par le serveur et du mode de basculement utilisé par le client.

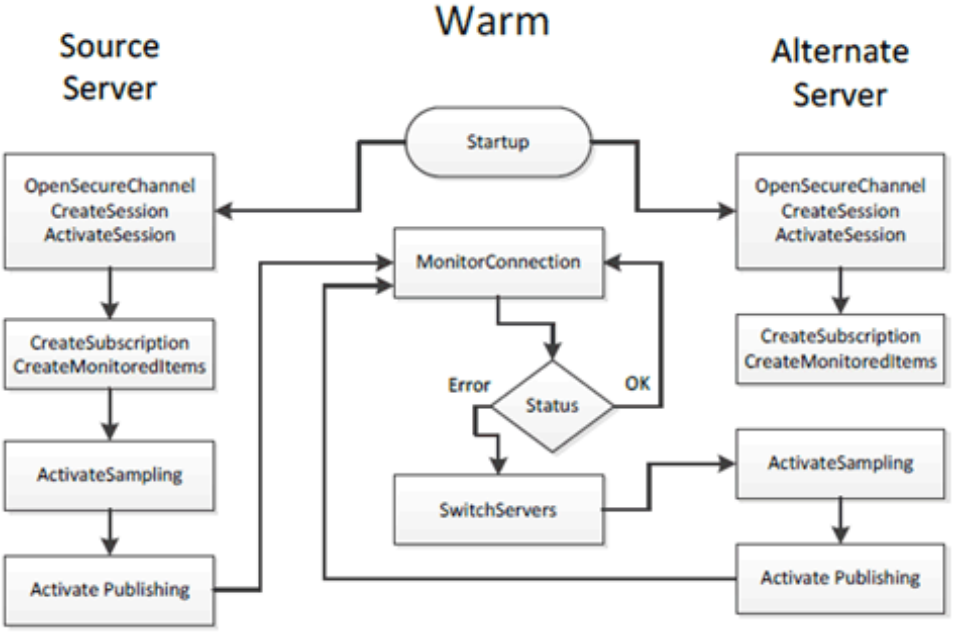
Une fois connecté à un serveur redondant, le client doit connaître les modes de basculement pris en charge par le serveur puisque cela détermine les options disponibles concernant le comportement du client. Un client peut toujours traiter avec un serveur en utilisant un mode de basculement inférieur (un client peut se connecter à un serveur qui fournit la redondance de type Hot Redundancy et choisir de le traiter comme s'il s'exécutait

en mode Warm Redundancy ou Cold Redundancy. Ce choix appartient au client. Dans le cas du mode de basculement HotAndMirrored, le client ne doit pas utiliser le mode de basculement Hot ou Warm car cela générerait une charge superflue sur les serveurs. OPC UA Part 4, section 6.6.2.4.5.1

Mode de basculement à chaud du client OPC UA

En mode de basculement à chaud (Warm), le client doit se connecter à un ou plusieurs serveurs de l'ensemble Redundant Server Set principalement pour surveiller le niveau de service (ServiceLevel). *Un client peut se connecter et créer des souscriptions et des éléments MonitoredItem sur plusieurs serveurs, mais les fonctions d'échantillonnage et de publication peuvent être actives sur un seul serveur.. Cependant, le serveur actif renvoie des données réelles, tandis que les autres serveurs de l'ensemble Redundant Server Set vont renvoyer une erreur correspondante pour les MonitoredItem dans la réponse de publication (Publish), par exemple Bad_NoCommunication. L'unique serveur actif peut être identifié par lecture de la variable ServiceLevel sur tous les serveurs.*

Le serveur ayant le plus haut niveau de service (ServiceLevel) est le serveur actif. Pour le basculement, le client active l'échantillonnage et la publication sur le serveur qui présente le plus haut niveau de service (ServiceLevel). La figure 30 représente les étapes effectuées par un client lors de la communication avec un serveur en utilisant le mode de basculement à chaud (Warm).



OPC UA Part 4, section 6.6.2.4.5.3

Architectures prises en charge

Introduction

Ce chapitre décrit les architectures prises en charge par le module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré.

Configurations de module BMENUA0100 prises en charge

Mise en place du module BMENUA0100

Le module BMENUA0100 peut être placé dans un logement Ethernet d'un rack principal local (c'est-à-dire dans le même rack que l'UC) dans les configurations suivantes :

- Configuration autonome M580.
- Configuration PAC de sécurité autonome M580.
- Configuration à redondance d'UC M580
- Configuration PAC de sécurité à redondance d'UC M580.

NOTE:

- Le module BMENUA0100 peut être utilisé avec toutes les UC M580.
- En cas de création de boucle réseau, le module BMENUA0100 passe à l'état NOCONF (Non configuré). Pour éviter les boucles et les événements associés, lorsque vous utilisez le port de contrôle du BMENUA0100, séparez physiquement le réseau du port de contrôle et le réseau de l'embase de l'UC (via le câblage), pas seulement logiquement (via les paramètres de sous-réseau et de masque de sous-réseau).

Connexion via le protocole HTTPS

Si votre application rencontre des problèmes de connexion, consultez votre équipe de support informatique locale pour vérifier que votre configuration réseau et vos stratégies de sécurité sont cohérentes avec l'accès HTTPS (port 443) à l'adresse IP du module BMENUA0100.

Le module BMENUA0100 accepte les connexions HTTPS avec le protocole TLS (Transport Layer Security) v1.2 ou ultérieure. Par exemple, Windows 7 peut nécessiter une mise à jour

pour activer TLS 1.2 pour la mise à niveau du micrologiciel de BMENUA0100 ou accéder à son site Web.

Installation du module BMENUA0100 sur un réseau plat

Pour plusieurs racks M580 connectés sur un seul sous-réseau (architecture de réseau plat) qui contiennent des modules BMENUA0100 avec port de contrôle désactivé, installez chaque module BMENUA0100 à un numéro d'emplacement différent dans son rack respectif (à l'exception des configurations de redondance d'UC où les modules BMENUA0100 sont installés au même numéro d'emplacement). De plus, il est fortement recommandé d'utiliser un routeur pour isoler les racks et ainsi éviter des conflits d'adresses entre les modules BMENUA0100.

Ajout de préfixes aux noms d'équipement (rôle) dans les architectures de réseau plat

Lorsqu'une architecture comprend plusieurs modules BMENUA0100 qui communiquent avec d'autres équipements (tels que des CPU M580) configurés sur le même sous-réseau, il est recommandé d'utiliser des préfixes pour le nom d'équipement (de rôle) de tous les équipements (y compris les CPU M580). Cette convention de dénomination permet aux modules BMENUA0100 de différencier les CPU M580 et de déterminer quelle CPU est située sur quel rack. Cette convention de dénomination contribue à éliminer l'incertitude liée à l'architecture de réseau plat. Par exemple, sans préfixes uniques, un module BMENUA0100 ne peut pas déterminer avec quelle CPU M580 il doit communiquer pour récupérer sa propre configuration après le téléchargement d'une application.

Le préfixe du nom d'équipement peut être défini dans Control Expert, dans l'onglet **Outils > Options du projet > Configuration**.

Accès au serveur OPC UA intégré au BMENUA0100

Dans les architectures topologiques décrites dans ce chapitre, le port d'embase Ethernet du module de communication BMENUA0100 et son port de contrôle peuvent être utilisés pour fournir l'accès au serveur OPC UA intégré au module. Pour savoir quand ces ports peuvent être utilisés pour accéder au serveur OPC UA intégré, reportez-vous aux descriptions du port de contrôle et du port d'embase Ethernet dans la section Ports externes, page 18.

Nombre maximal de modules BMENUA0100 par configuration

Le nombre maximum de modules BMENUA0100 pris en charge dans une configuration M580 est indiqué ci-après :

Type de configuration M580	**Nombre maximal de modules BMENUA0100**
Autonome	Deux (2) dans le rack principal local pour les configurations standard et de sécurité autonomes[1] et redondantes[1,2].
PAC de sécurité	
Redondante	
PAC de sécurité à redondance d'UC	

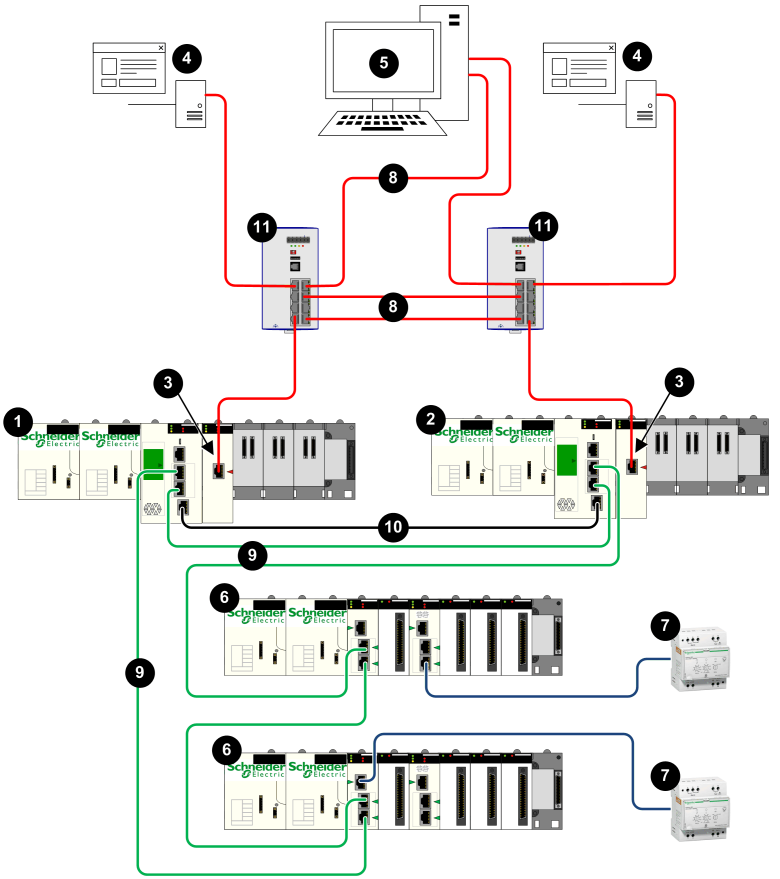
1. Lorsque deux (2) modules BMENUA0100 sont utilisés dans un rack principal :
   - Les performances de chaque module seront plus lentes qu'avec l'utilisation d'un seul module.
   - Activez le port de contrôle dans la configuration des deux modules.
2. Dans les conceptions redondantes, placez les modules BMENUA0100 aux mêmes numéros d'emplacement dans les racks principaux locaux respectifs.

CCOTF (Change Configuration On The Fly)

Le module BMENUA0100 ne prend pas en charge la fonction CCOTF.

Réseau de contrôle isolé avec des PAC à redondance d'UC M580

Architecture



1 PAC primaire

2 PAC redondant

3 Module de communication Ethernet à serveur OPC UA intégré BMENUA0100

4 Client OPC UA (système SCADA)

5 Poste de travail d'ingénierie avec deux connexions Ethernet

6 Stations d'E/S distantes Ethernet X80

7 Equipements distribués

8 Réseau de contrôle

9 Anneau principal d'E/S distantes Ethernet

10 Liaison de communication redondante

11 Commutateur double anneau (DRS)

Description

Cette architecture fournit des connexions redondantes aux clients OPC UA redondants (systèmes SCADA). La cybersécurité peut être activée ou désactivée dans cette architecture. Le réseau de contrôle (8) est logiquement isolé à la fois des équipements Ethernet situés dans l'anneau principal de la station RIO Ethernet (9), y compris l'UC, et des équipements Ethernet distribués (7). Ceci est mis en oeuvre sur la couche réseau du modèle OSI via l'adressage IP.

Le port de contrôle BMENUA0100 (3), avec deux piles IPv6/IPv4, permet la connectivité en amont au réseau de contrôle. Si la communication est établie via IPv6, elle prend en charge la configuration automatique de l'adresse sans état (SLAAC) et l'adressage IP statique.

Le BMENUA0100 fournit la communication Modbus d'égal à égal entre les deux UC redondantes. Les ports d'équipement des UC fournissent la connectivité en aval aux équipements Ethernet sur l'anneau principal RIO Ethernet.

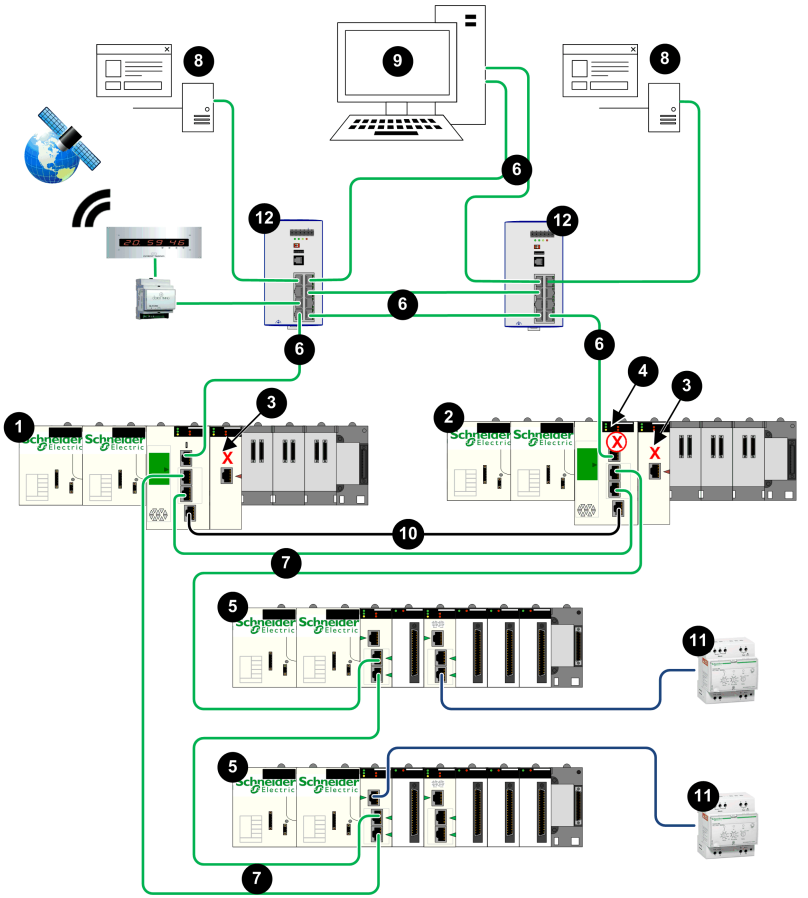
Chaque BMENUA0100 est client d'un serveur NTP situé dans le réseau de contrôle. La connexion est établie via le port de contrôle du module BMENUA0100. Les modules BMENUA0100 ont la fonction de serveur NTP pour les autres équipements dans l'anneau principal RIO Ethernet. Dans cette conception à redondance d'UC, le module BMENUA0100 configuré "A" est le serveur NTP primaire, et le module BMENUA0100 configuré "B" est le serveur NTP redondant. Ainsi, le temps UC et le temps du module BMENUA0100 sont synchronisés.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules à horodatage enregistrent les événements dans leur mémoire tampon locale. Ces

événements horodatés sont utilisés par l'application exécutée sur le PAC, qui convertit les données brutes et les stocke dans un format utilisable. Les enregistrements au bon format peuvent être utilisés par une application de supervision, par exemple un système SCADA.

Réseau plat (horizontal) non isolé avec redondance d'UC M580

Architecture



1 PAC primaire

2 PAC redondant

3 BMENUA0100 avec port de contrôle désactivé

4 UC redondante avec blocage automatique du port de service

5 Stations d'E/S distantes Ethernet X80

6 Réseau de contrôle

7 Anneau principal d'E/S distantes Ethernet

8 Client OPC UA (système SCADA)

9 Poste de travail d'ingénierie avec deux connexions Ethernet

10 Liaison de communication redondante

11 Equipements distribués

12 Commutateur double anneau (DRS)

Description

Cette architecture fournit des connexions redondantes depuis les UC redondantes M580 vers les clients OPC UA redondants (systèmes SCADA). L'objectif principal est de fournir la haute disponibilité aux PACs à redondance d'UC. Pour cette raison, cette architecture présente un réseau plat non isolé, qui relie ensemble le réseau de contrôle et l'anneau principal RIO Ethernet dans un même sous-réseau.

Le port de contrôle BMENUA0100 est désactivé. La communication Ethernet IPv4 au module BMENUA0100 est fournie via le port d'embase. La communication en amont entre les PACs à redondance d'UC et les serveurs SCADA est établie via le port de service de l'UC primaire. Les ports d'équipement des UC fournissent la connectivité en aval aux équipements Ethernet sur l'anneau principal RIO Ethernet.

Le port de service de l'UC (4) est automatiquement désactivé, en utilisant le logiciel de configuration Control Expert pour sélectionner **Blocage automatique du port de service avec un processeur hsby** dans l'onglet **Port de service** de la configuration des UC primaire et secondaire.

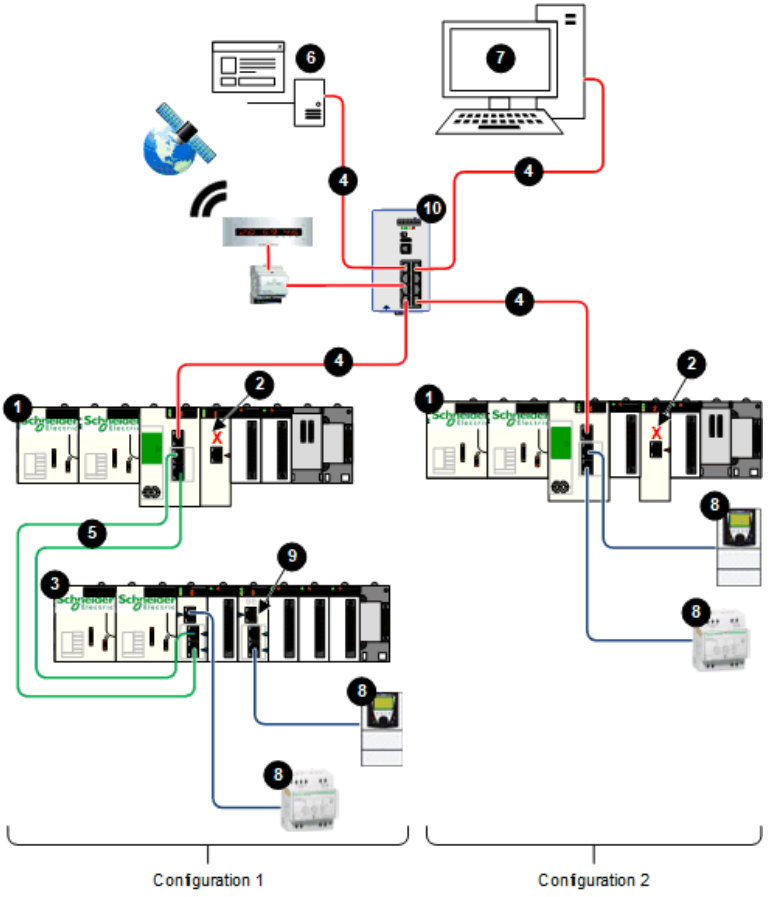
> **NOTE:** Le port de service de l'UC secondaire est désactivé pour empêcher la création indésirable d'une boucle de communications Ethernet, où le réseau de contrôle et l'anneau principal RIO Ethernet font partie du même sous-réseau. Pour plus d'informations, reportez-vous au *Guide de planification du système de redondance d'UC M580*, section Gestion des réseaux Ethernet plats avec redondance d'UC M580 (voir *Modicon M580 - Guide de planification du système de redondance d'UC pour architectures courantes*.

Dans cette conception de réseau, tous les équipements, notamment les UC, les CRA, et les BMENUA0100 peuvent être clients du même serveur NTP situé dans le réseau de contrôle. Ainsi, le temps des UC est synchronisé avec le module BMENUA0100.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules à horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont utilisés par l'application exécutée sur le PAC, qui convertit les données brutes et les stocke dans un format utilisable. Les enregistrements au bon format peuvent être utilisés par une application de supervision, par exemple un système SCADA.

Réseau plat avec plusieurs UC autonomes M580 et un seul système SCADA

Architecture



1 PAC autonome

2 BMENUA0100 avec port de contrôle désactivé

3 Stations d'E/S distantes Ethernet X80

4 Réseau de contrôle

5 Anneau principal d'E/S distantes Ethernet

6 Client OPC UA (système SCADA)

7 Poste de travail d'ingénierie avec une seule connexion Ethernet

8 Equipements distribués

9 Commutateur BMENOS0300

10 Commutateur double anneau (DRS)

Description

Cette architecture fournit une connexion à un client OPC UA (un système SCADA) à partir de plusieurs UC autonomes M580. Cette architecture à optimisation des coûts ne requiert pas la haute disponibilité. Cette architecture présente un réseau plat non isolé, qui relie ensemble le réseau de contrôle et l'anneau principal RIO Ethernet dans un même sous-réseau.

Le port de contrôle BMENUA0100 est désactivé pour chaque PAC autonome. La communication Ethernet IPv4 au module BMENUA0100 est fournie via le port d'embase. La communication en amont entre chaque PAC et le serveur SCADA unique est établie via le port de service de l'UC.

Dans la configuration 1, la connectivité en aval entre le PAC et la station RIO Ethernet X80 (4) est fournie par les deux ports de réseau d'équipements des UC. La connectivité en aval est fournie par le port de service CRA et un commutateur BMENOS0300 (9) à l'équipement Ethernet distribué.

Dans la configuration 2, la connectivité en aval est fournie par les deux ports de réseau d'équipements à l'équipement Ethernet distribué.

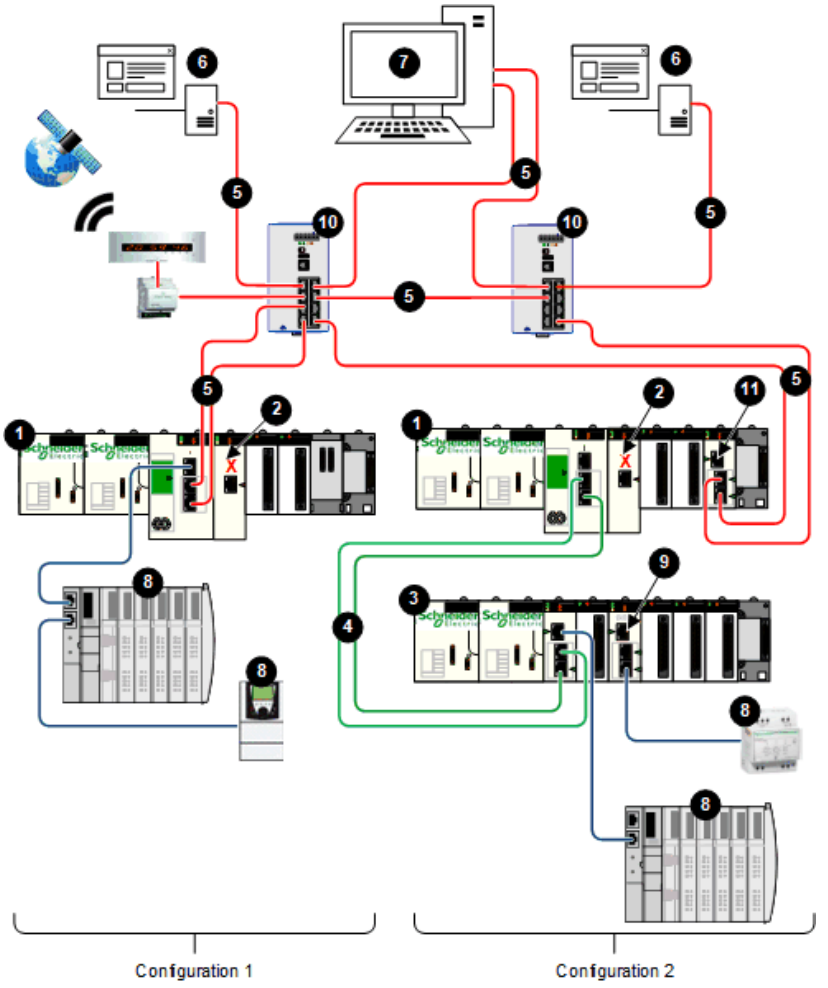
Dans cette conception de réseau plat, tous les équipements réseau (notamment les UC, les CRA, et les BMENUA0100) sont des clients NTP d'un serveur NTP situé dans le réseau de contrôle. Ainsi, le temps UC et le temps du module BMENUA0100 sont synchronisés.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules à horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont utilisés par l'application exécutée sur le PAC, qui convertit les

données brutes et les stocke dans un format utilisable. Les enregistrements au bon format peuvent être utilisés par une application de supervision, par exemple un système SCADA.

Réseau plat avec plusieurs UC autonomes M580 et serveurs SCADA redondants

Architecture



1 PAC autonome

2 BMENUA0100 avec port de contrôle désactivé

3 Stations d'E/S distantes Ethernet X80

4 Anneau principal d'E/S distantes Ethernet

5 Réseau de contrôle

6 Clients OPC UA (systèmes SCADA)

7 Poste de travail d'ingénierie avec deux connexions Ethernet

8 Equipements distribués

9 Commutateur BMENOS0300

10 Commutateur double anneau (DRS)

11 Module BMENOS0300 ou BMENOC0301/11

Description

Cette architecture fournit la haute disponibilité du réseau de contrôle, via les connexions redondantes entre les clients OPC UA (systèmes SCADA) et plusieurs UC autonomes M580. Cette architecture présente un réseau plat non isolé, qui relie ensemble le réseau de contrôle et l'anneau principal RIO Ethernet dans un même sous-réseau.

Le port de contrôle BMENUA0100 est désactivé pour chaque PAC autonome. La communication Ethernet IPv4 au module BMENUA0100 est fournie via le port d'embase.

Dans la configuration 1, la communication en amont aux serveurs SCADA est établie via les ports de réseau d'équipements des UC, en utilisant le protocole de redondance RSTP pour attribuer les rôles à chaque port et éviter les boucles Ethernet logiques. La connectivité en aval à l'équipement Ethernet distribué est établie par le port de service de l'UC.

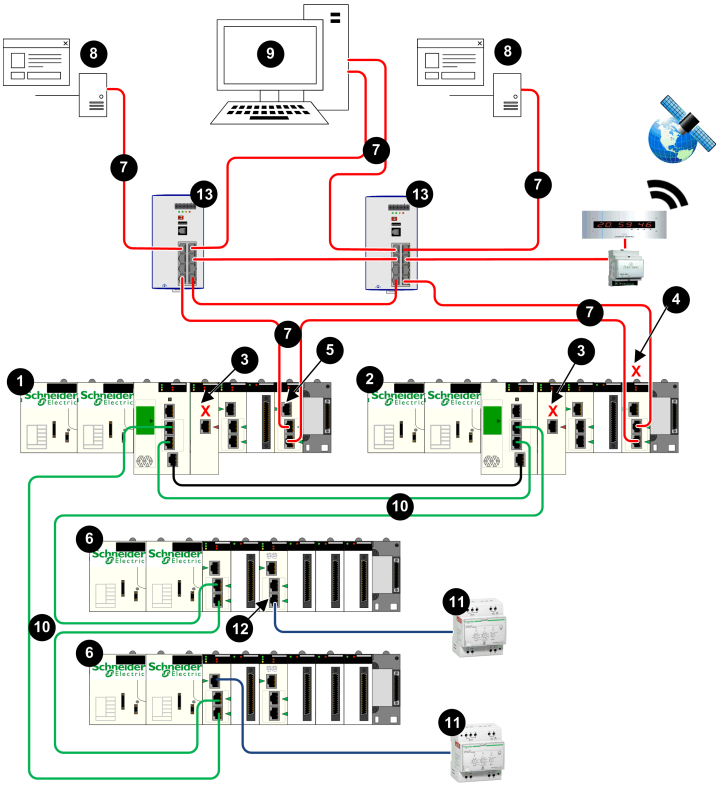
Dans la configuration 2, la connectivité en amont aux serveurs SCADA est fournie par les ports de réseau d'équipements d'un module BMENOS0300 ou BMENOC0301/11. Le protocole de redondance RSTP est utilisé pour attribuer les rôles à chaque port et éviter les boucles Ethernet logiques. La connectivité en aval entre le PAC et la station d'E/S distante Ethernet X80 est fournie par les ports du réseau d'équipements de l'UC. La connectivité en aval est fournie à la fois par le port de service CRA et un commutateur BMENOS0300 (9) à l'équipement Ethernet distribué.

Dans cette conception de réseau plat, tous les équipements réseau (notamment les UC, les CRA, et les BMENUA0100) sont des clients NTP d'un serveur NTP situé dans le réseau de contrôle. Ainsi, le temps UC et le temps du module BMENUA0100 sont synchronisés.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules à horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont utilisés par l'application exécutée sur le PAC, qui convertit les données brutes et les stocke dans un format utilisable. Les enregistrements au bon format peuvent être utilisés par une application de supervision, par exemple un système SCADA.

Réseau plat avec plusieurs UC redondances M580 et un système SCADA redondant

Architecture



1 PAC primaire

2 PAC redondant

3 BMENUA0100 avec port de contrôle désactivé

4 BMENOS0300 ou BMENOC0301/11 avec port d'embase désactivé

5 BMENOS0300 ou BMENOC0301/11 avec port d'embase activé

6 Stations d'E/S distantes Ethernet X80

7 Réseau de contrôle

8 Client OPC UA (système SCADA)

9 Poste de travail d'ingénierie avec deux connexions Ethernet

10 Anneau principal d'E/S distantes Ethernet

11 Equipements distribués

12 Commutateur BMENOS0300

13 Commutateur double anneau (DRS)

Description

Cette architecture fournit la haute disponibilité avec des connexions redondantes reliant les clients OPC UA redondants (systèmes SCADA) aux PACs redondants dans le même sous-réseau.

Chaque PAC est connecté à un système SCADA via un module BMENOS0300 ou BMENOC0301/11. Pour éviter la création indésirable de boucles Ethernet, le port d'embase du module BMENOS0300 ou BMENOC0301/11 est désactivé. Dans cet exemple, il s'agit du module du PAC autonome (4) avec port d'embase désactivé. En outre, le protocole de redondance RSTP est utilisé pour attribuer les rôles à chaque port et éviter les boucles Ethernet logiques.

Le port de contrôle BMENUA0100 est désactivé (3) pour chaque PAC autonome. La communication Ethernet IPv4 au module BMENUA0100 est fournie via le port d'embase.

La connectivité en aval aux stations RIO Ethernet X80 est fournie par les ports de service des UC. La connectivité en aval entre les stations RIO Ethernet X80 et l'équipement Ethernet distribué est fournie à la fois par le port de service CRA et un commutateur BMENOS0300 (12).

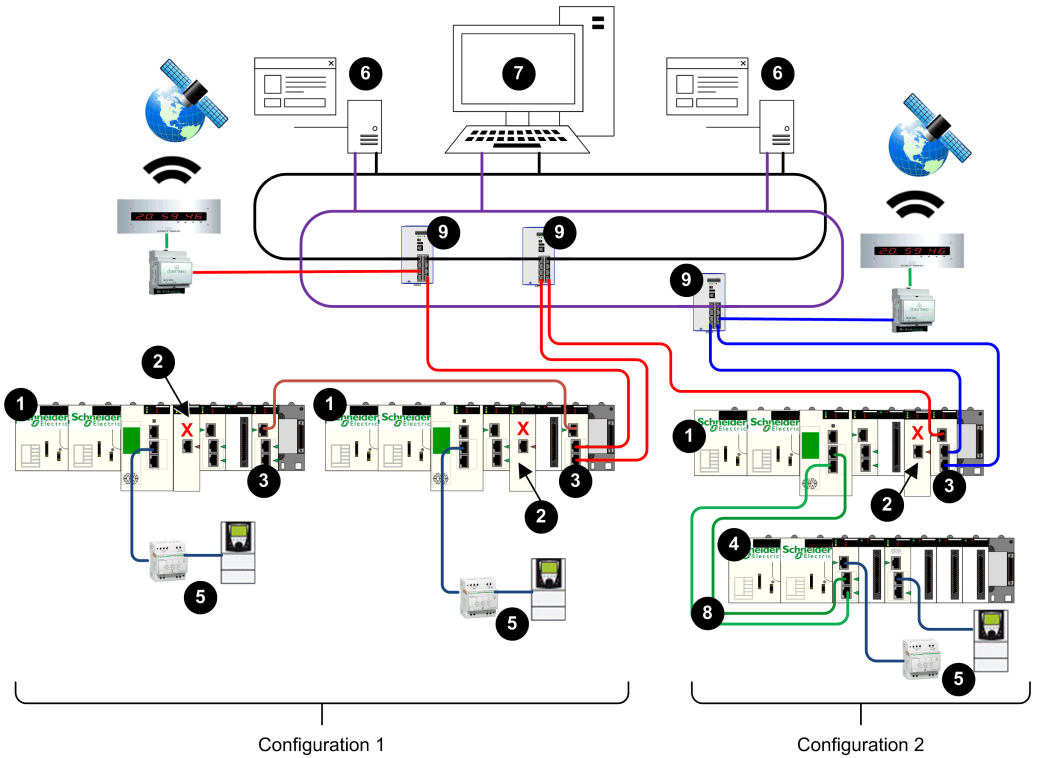
Dans cette conception de réseau plat, tous les équipements réseau (notamment chaque UC redondante et le module BMENUA0100) sont des clients NTP d'un serveur NTP situé dans

le réseau de contrôle. Ainsi, le temps UC et le temps du module BMENUA0100 sont synchronisés.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules à horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont utilisés par l'application exécutée sur le PAC, qui convertit les données brutes et les stocke dans un format utilisable. Les enregistrements au bon format peuvent être utilisés par une application de supervision, par exemple un système SCADA.

Réseau hiérarchique incluant plusieurs UC autonomes M580 connecté à un réseau de contrôle et un système SCADA redondant

Architecture



1 PAC autonome

2 BMENUA0100 avec port de contrôle désactivé

3 Module de communication Ethernet BMENOC0321

4 Stations d'E/S distantes Ethernet X80

5 Equipements distribués

6 Client OPC UA (système SCADA)

7 Poste de travail d'ingénierie avec deux connexions Ethernet

8 Anneau principal d'E/S distantes Ethernet

9 Commutateur double anneau (DRS)

Description

Cette architecture inclut un réseau hiérarchique, qui repose sur des modules de communication BMENOC0321 pour acheminer le trafic réseau entre les sous-réseaux. La communication en amont entre les PAC et les clients OPC UA (systèmes SCADA) est établie via les deux ports de réseau d'équipements du module BMENOC0321, en utilisant le protocole RSTP pour éviter les boucles Ethernet logiques.

NOTE: Cette architecture requiert la configuration de routes statiques sur l'équipement du réseau de contrôle pour rediriger les différents sous-réseaux de plusieurs PAC d'UC.

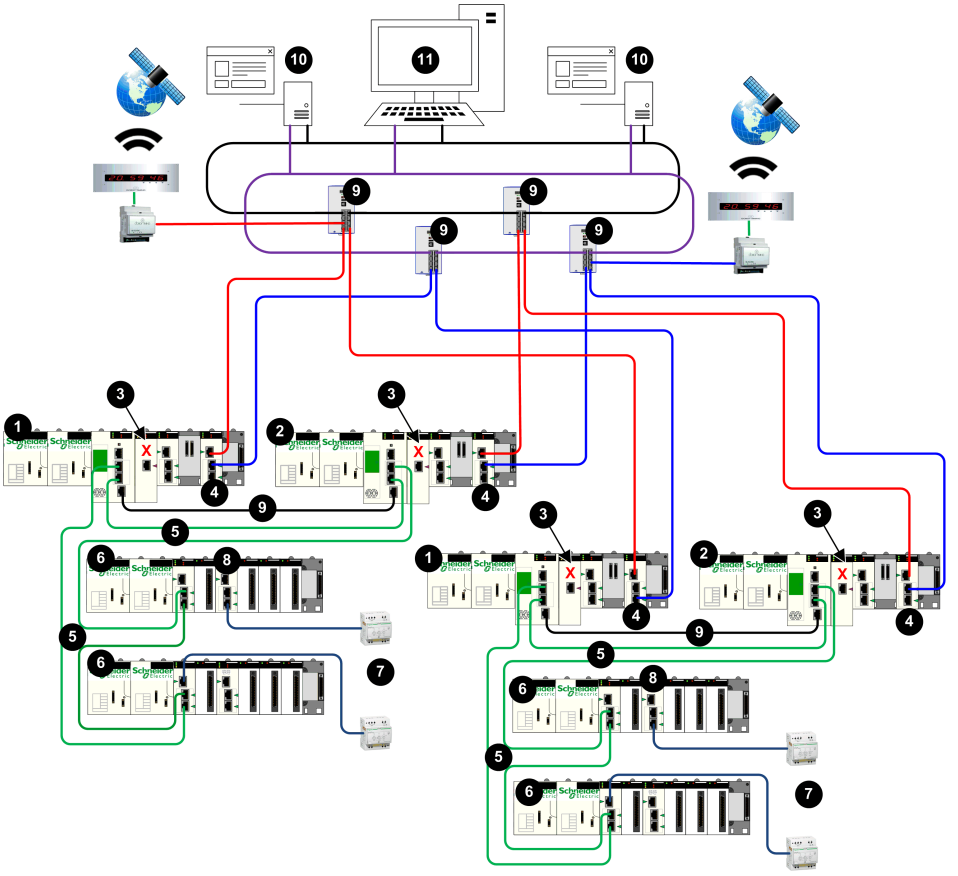
Le port de contrôle BMENUA0100 (2) est désactivé pour chaque PAC autonome. La communication Ethernet IPv4 au module BMENUA0100 est fournie via le port d'embase.

La configuration 1 inclut deux PACs situés dans le même sous-réseau. Dans cette configuration, le module BMENOC0321 fournit les communications en amont redondantes aux serveurs SCADA. Le module BMENOC0321 utilise le protocole de redondance RSTP pour éviter les boucles Ethernet logiques. Les deux ports de réseau d'équipements des deux UC fournissent la communication en aval à l'équipement Ethernet distribué.

La configuration 2 inclut un PAC, avec station RIO Ethernet X80. Ce PAC utilise le module BMENOC0321 pour la communication en amont aux serveurs SCADA redondants. Le BMENOC0321 réalise cela en utilisant deux sous-réseaux indépendants. La communication en aval entre la station RIO Ethernet X80 et l'équipement Ethernet distribué est fournie à la fois par le port de service CRA et un commutateur BMENOS0300.

Réseau hiérarchique avec plusieurs UC redondances M580 et des connexions SCADA redondantes

Architecture



1 PAC primaire

2 PAC redondant

3 BMENUA0100 avec port de contrôle désactivé

4 Module de communication Ethernet BMENOC0321

5 Anneau principal d'E/S distantes Ethernet

6 Stations d'E/S distantes Ethernet X80

7 Equipements distribués

8 Commutateur BMENOS0300

9 Commutateur double anneau (DRS)

10 Client OPC UA (système SCADA)

11 Poste de travail d'ingénierie avec deux connexions Ethernet

Description

Cette architecture inclut un réseau hiérarchique, qui repose sur des modules de communication BMENOC0321 (4) pour acheminer le trafic réseau entre les sous-réseaux. La communication en amont entre les PAC redondants et les clients OPC UA (systèmes SCADA) est établie via les deux ports de réseau d'équipements des modules BMENOC0321, en utilisant le protocole RSTP pour éviter les boucles Ethernet logiques.

NOTE: Cette architecture requiert la configuration de routes statiques sur l'équipement du réseau de contrôle pour rediriger les différents sous-réseaux de plusieurs PAC d'UC.

Le port de contrôle BMENUA0100 (3) est désactivé pour chaque PAC. La communication Ethernet IPv4 au module BMENUA0100 est fournie via le port d'embase.

Dans cette configuration, le module BMENOC0321 fournit les communications en amont redondantes aux serveurs SCADA via des connexions redondantes. Les deux ports de réseau d'équipements des UC fournissent la communication en aval aux stations RIO Ethernet X80. La communication en aval entre la station RIO Ethernet X80 et l'équipement Ethernet distribué est fournie à la fois par le port de service CRA et un commutateur BMENOS0300 (8).

Mise en service et installation

Introduction

Ce chapitre explique comment sélectionner un mode de fonctionnement et installer le module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré.

Liste de contrôle pour la mise en service du module BMENUA0100

Liste de contrôle pour la mise en service

Le schéma suivant présente une séquence de tâches à suivre lors de la mise en service et de l'installation d'un nouveau module BMENUA0100. Cet exemple configure le module pour qu'il fonctionne en mode PKI Auto-signature et CA avec les adresses IPV6 SLAAC et IPV4 :

1. Configurez l'application, page 115 Control Expert.
2. Configurez le routeur / serveur SLAAC (pour IPV6 en mode SLAAC).
3. Sélectionnez le mode sécurisé pour le module :

a. Réglez le commutateur rotatif, page 20 situé à l'arrière du module sur la position du mode de fonctionnement Secured, page 27.

b. Installez le module, page 82 dans un emplacement Ethernet du rack.

4. Configurez les paramètres de cybersécurité à l'aide des pages Web, page 84 du module :

a. Créez la configuration de la cybersécurité à l'aide de la page Web Paramètres, page 92.

b. Réglez le **mode PKI** sur Autosignature et CA.

c. Pour les équipements clients qui ne prennent pas en charge PKI, créez une liste blanche de **certificats client approuvés**, page 109.

d. **Appliquez** le fichier de configuration.

5. Effectuez l'inscription manuelle des certificats, page 109 :

a. Générez une demande de signature de certificat (CSR).

b. Insérez le certificat CA.

c. Insérez le certificat d'équipement.

6. Ajoutez le certificat CA aux équipements clients OPC UA.

7. Testez la communication entre le client et le serveur OPC UA.

Mise en service du module BMENUA0100

Introduction

Le module BMENUA0100 avec serveur OPC UA intégré figure dans le catalogue matériel de Control Expert en tant que module de communication. Il utilise une voie d'E/S.

Lors de l'arrivée d'un nouveau module BMENUA0100 de l'usine, le mode de fonctionnement défini par défaut pour la cybersécurité est le mode Secured. Pour configurer le nouveau module en mode Secured, suivez la procédure de Mise en service du mode Secured, page 27 indiquée ci-dessous.

Pour changer le mode de fonctionnement de la cybersécurité pour un module qui a déjà été configuré auparavant (ou pour configurer un module neuf en mode Standard), effectuez une opération Security Reset, page 80 sur le module. Après une opération Security Reset de la sécurité, vous pouvez suivre la procédure de Mise en service en mode Secured, page 27 ou de Mise en service en mode standard, page 27.

Mise en service en mode Secured

La mise en service d'un module BMENUA0100 pour un fonctionnement en mode Secured, requiert la réalisation de deux procédures de configuration :

- Configuration de la cybersécurité, en utilisant les pages Web du module.
- Configuration de l'adresse IP, du client NTP et de l'agent SNMP, en utilisant l'outil de configuration Control Expert.

Seul un Administrateur de la sécurité peut mettre en service un module en mode Secured, en utilisant le nom d'utilisateur et le mot de passe par défaut, page 28 du mode Secured.

NOTE: Effectuez ces les tâches de configuration suivantes dans l'ordre indiqué :

- Utilisez Control Expert pour configurer les adresses IP de contrôle et d'embase.
- Utilisez les pages Web du module pour configurer les paramètres de cybersécurité.
- Utilisez Control Expert pour terminer la configuration du client NTP et de l'agent SNMP.

NOTE: Pour la mise en service en mode Secured avec inscription manuelle, reportez-vous à la section Inscription manuelle, page 109.

La procédure suivante s'applique à un nouveau module qui n'a pas été configuré auparavant. Dans le cas d'un module qui a déjà été configuré, effectuez une opération Security Reset, page 80 avant de passer aux étapes suivantes.

Pour mettre en service le module en mode Secured :

1. Configurez les paramètres d'adresse IP :

a. Ouvrez l'outil de configuration Control Expert.

b. Dans Control Expert, créez un **Nouveau projet**, ajoutez un module BMENUA0100 au projet à partir du **Catalogue matériel**, puis configurez les paramètres d'adresse IP, page 115.

2. Configurez les paramètres de la cybersécurité :

a. Le module étant détaché du rack, utilisez le tournevis en plastique fourni, page 20 pour régler le commutateur rotatif sur la position **Secured**.

b. Installez, page 81 le module dans un logement Ethernet sur le rack Ethernet principal local et effectuez un cycle d'alimentation.

c. Utilisez votre navigateur Internet pour connecter votre PC de configuration au module à l'aide du port de contrôle ou du port d'embase, puis accédez aux pages Web du module à l'adresse IP configurée.

d. Si le navigateur Internet affiche un message, page 86 indiquant un risque de sécurité, effectuez la connexion en cliquant sur **Accepter les risques et continuer** (ou un message de ce type selon le navigateur et la langue).

e. Sur la page de connexion de l'utilisateur, entrez le nom d'utilisateur et le mot de passe par défaut, page 28.

f. Changez et confirmez le mot de passe. Consultez la rubrique Gestion des utilisateurs, page 111 pour connaître les conditions de création du mot de passe. La page, page 89 d'**accueil** du module s'affiche.

g. Depuis la page d'**accueil**, accédez aux pages Web du module et configurez les paramètres de la cybersécurité.

3. Configurez les paramètres du client NTP et de l'agent SNMP :

a. Ouvrez l'outil de configuration Control Expert.

b. Dans Control Expert, configurez les paramètres du client NTP et de l'agent SNMP, page 115.

c. Après la configuration du projet Control Expert, connectez-vous au PAC et transférez le projet au PAC.

NOTE: Après le chargement de la configuration sur le module BMENUA0100, l'état du module passe de l'état NON CONFIGURÉ à l'état CONFIGURÉ. Le voyant SECURE, page 135 indique si le module est configuré ou non configuré et si le serveur OPC UA est connecté à un client OPC UA.

Mise en service en mode standard

En mode standard, la configuration de la cybersécurité n'est pas requise. Il suffit de configurer l'adresse IP, le client NTP et l'agent SNMP en utilisant l'outil de configuration Control Expert. En mode standard, le module peut communiquer lorsqu'il est placé dans le rack, démarré et qu'il reçoit une configuration valide de Control Expert.

Utilisez le nom d'utilisateur et le mot de passe par défaut , page 28 Installer pour mettre en service le module en mode standard.

Pour mettre en service le module en mode standard :

1. Le module étant détaché du rack, utilisez le tournevis en plastique fourni avec le module, page 20 pour configurer le commutateur rotatif sur la position **Standard**.
2. Placez le module dans un logement Ethernet sur le rack Ethernet principal local et effectuez un cycle de démarrage.
3. Ouvrez l'outil de configuration Control Expert.
4. Dans Control Expert, créez un **Nouveau projet**, ajoutez un module BMENUA0100 au projet depuis le **Catalogue matériel**, puis configurez les paramètres d'adresse IP, page 115, de client NTP, page 124 et d'agent SNMP, page 127.
5. Après la configuration du projet Control Expert, connectez-vous au PAC et transférez le projet au PAC.

   NOTE: En mode de fonctionnement Standard, le voyant SECURE est éteint.

Opération Security Reset

Si le module a déjà été configuré auparavant, ou dans le cas d'un nouveau module à configurer en mode Standard pour la cybersécurité, réinitialisez la sécurité en exécutant l'opération Security Reset avant de configurer la cybersécurité. La réinitialisation remet les paramètres de la cybersécurité sur les valeurs par défaut d'usine. Vous pouvez effectuer une réinitialisation en utilisant les pages Web du module, ou le commutateur rotatif situé à l'arrière du module.

Pages Web : Pour un module BMENUA0100 actuellement configuré en mode Secured :

1. Accédez à la page Web **Gestion de la configuration > REINITIALISATION**.
2. Cliquez sur **Réinitialiser**.

   NOTE: L'opération Security Reset est terminée lorsque le voyant RUN est vert fixe, et que le voyant du port de contrôle NS et le voyant du port d'embase BS sont rouge fixe.

3. Effectuez un cycle de démarrage du module de l'une des façons suivantes :
   - Arrêtez et redémarrez le rack du module.
   - Retirez le module du rack, puis réinsérez-le.

   Vous pouvez ensuite effectuer la mise en service en mode Secured.

Commutateur rotatif : Pour tout module BMENUA0100 :

1. Le module étant détaché du rack, utilisez le tournevis en plastique fourni avec le module, page 20 pour régler le commutateur rotatif en position **Security Reset**.
2. Installez, page 81 le module dans un logement Ethernet sur le rack Ethernet principal local et effectuez un cycle de démarrage.

   NOTE: Cela restaure les paramètres par défaut du module, y compris l'adresse IP par défaut du port de contrôle, page 116 10.10.MAC5.MAC6.

   A la fin de l'opération, le voyant RUN est vert fixe, et le voyant du port de contrôle NS et le voyant du port d'embase BS sont rouge fixe. Vous pouvez couper l'alimentation et retirer le module du rack, puis effectuer la Mise en service en mode Secured, page 27 ou la Mise en service en mode Standard, page 27.

Installation du module BMENUA0100

Introduction

Vous ne pouvez installer le module BMENUA0100 que dans un rack Ethernet principal local et à un emplacement Ethernet qui n'est pas réservé à l'alimentation de sécurité ou à la CPU.

NOTE: Si votre application comprend plusieurs PAC (qui ne sont pas des paires de redondance) avec chacun un module BMENUA0100, faites en sorte que le numéro d'emplacement de chaque module BMENUA0100 soit unique. Par exemple, pour une application comprenant deux PAC, si un module BMENUA0100 est installé à l'emplacement 4 dans le rack PAC1, vous devrez installer le deuxième module BMENUA0100 dans le rack PAC2 à un emplacement de numéro différent de 4.

Précautions relatives à la mise à la terre

Chaque module BMENUA0100 est équipé de contacts de liaison à la terre.

Schneider Electric recommande l'utilisation d'une barre BMXXSP•••• pour protéger le rack contre les perturbations électromagnétiques.

Respectez toutes les normes et consignes de sécurité locales et nationales.

⚠⚠DANGER

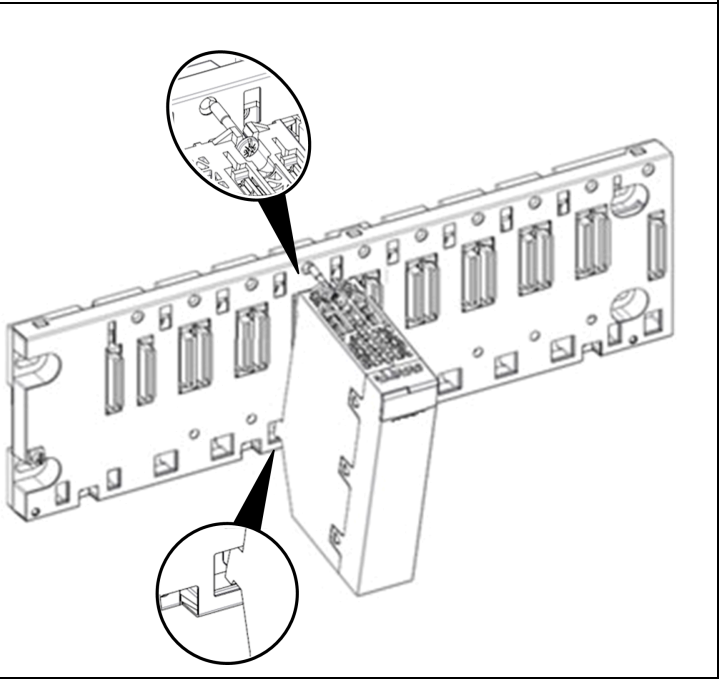
RISQUE D'ELECTROCUTION

Lorsqu'il est impossible de prouver que l'extrémité d'un câble blindé est reliée à la masse locale, ce câble doit être considéré comme dangereux et les équipements de protection individuelle (EPI) doivent être utilisés.

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

Installation d'un module BMENUA0100 dans le rack

Un module BMENUA0100 a besoin d'un seul emplacement Ethernet dans un rack. Vous pouvez installer le module dans n'importe quel emplacement Ethernet non réservé à l'alimentation ou à la CPU. Procédez comme suit pour installer un module BMENUA0100 dans un rack :

Étape	Action	
1	Positionnez les ergots de guidage situés à l'arrière du module dans les emplacements correspondants du rack.	
2	Relevez le module pour le plaquer contre l'arrière du rack. Le module est en place.	
3	Serrez la vis de fixation sur la partie supérieure du module afin de maintenir le module en place sur le rack. Couple de serrage : 0,4 à 1,5 N•m (0,30 à 1,10 lbf-ft)	

Mise à la terre des modules d'E/S

Pour plus d'informations sur la mise à la terre, consultez la section *Mise à la terre du rack et du module d'alimentation* dans le document *Modicon X80 - Racks et modules d'alimentation - Manuel de référence du matériel*.

Configuration

Introduction

Ce chapitre explique comment configurer le module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré.

Configuration des paramètres de cybersécurité du BMENUA0100

Introduction

Cette section explique comment utiliser les pages Web du module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré. Les pages Web permettent de créer une configuration de cybersécurité pour le module et d'afficher les données de diagnostic.

Introduction aux pages Web de BMENUA0100

Introduction

Utilisez les pages Web du BMENUA0100 pour créer, gérer et diagnostiquer une configuration de cybersécurité pour le module et pour afficher les données de diagnostic OPC UA et d'événement.

NOTE: Les pages Web du module BMENUA0100 prennent en charge la communication HTTPS sur les protocoles IPv4 et IPv6, page 116.

Pour que le module BMENUA0100 fonctionne en mode Secured, une configuration de la cybersécurité est requise et doit être effectuée avant l'adresse IP, client NTP et les paramètres SNMP peuvent être configurés avec Control Expert, page 115. La configuration de la cybersécurité peut être effectuée uniquement localement pour chaque module BMENUA0100 en connectant un PC de configuration (en exécutant un navigateur HTTPS) au module BMENUA0100 :

- Port de contrôle, s'il est activé.
- Port d'embase (via un BMENOC0301/11 ou l'UC), si le port de contrôle est désactivé.

NOTE: Avant de vérifier la validité des paramètres de cybersécurité saisis dans les pages Web, le module BMENUA0100 définit les paramètres d'adresse IP du port de contrôle et du port d'embase configurés dans Control Expert, page 115.

Pour que le module BMENUA0100 fonctionne en mode Standard, les paramètres de la cybersécurité ne sont pas nécessaires et ne peuvent pas être configurés.

NOTE:

- Si vous utilisez un certificat auto-signé, certains navigateurs peuvent indiquer que la connexion entre le PC et le module n'est pas sécurisée.
- Pour les modules BMENUA0100 fonctionnant en mode Secured dans un système à redondance d'UC, vérifiez que les paramètres de cybersécurité du module BMENUA0100 du PAC primaire sont identiques à ceux du module BMENUA0100 du PAC redondant. Le système n'effectue pas automatiquement la vérification.

L'accès aux pages Web, en fonction du mode de fonctionnement de la cybersécurité :

Page Web ou Groupe	Mode Secured	Mode Standard
Accueil, page 89	✓	✓
Paramètres (sécurité de l'équipement), page 92	✓	–
Gestion des certificats, page 103	✓	–
Contrôle d'accès, page 111	✓	–
Gestion de la configuration, page 113	✓	–
Diagnostic, page 158	✓	✓
✓ : Pages Web accessibles. – : Pages Web inaccessibles.		

Configuration initiale des paramètres de cybersécurité

Vous pouvez configurer les paramètres de la cybersécurité d'un module BMENUA0100 :

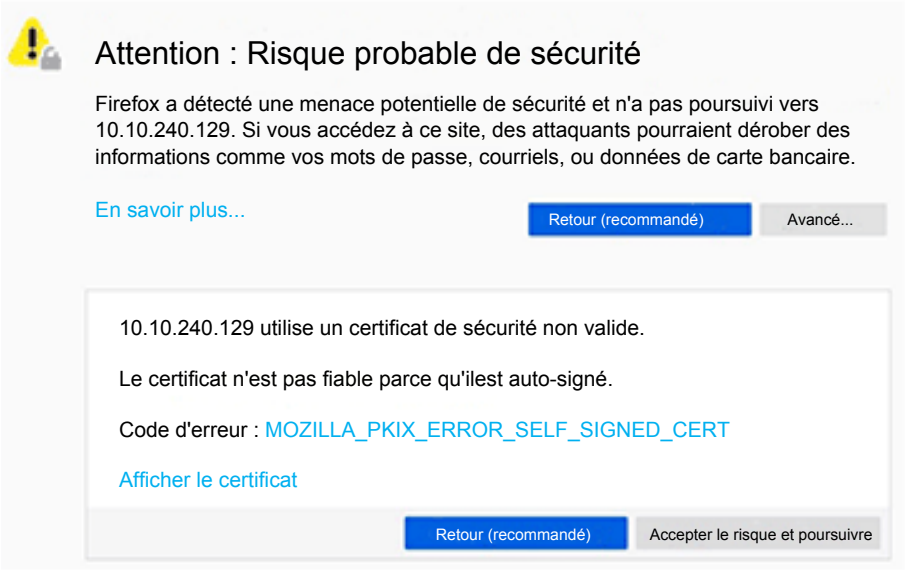
- Jamais configuré auparavant, configuré avec les valeurs par défaut initiale d'usine.
- Déjà configuré auparavant, mais restauré avec la configuration par défaut en exécutant la commande Security Reset, page 27.

Une fois le module configuré avec les paramètres de la cybersécurité, et fonctionnant en mode Secured, vous pouvez modifier également les paramètres de cybersécurité via les pages Web.

Consultez la rubrique Mise en service, page 78 pour savoir comment appliquer la configuration initiale au module.

D'abord connectez-vous aux pages Web

Si vous vous connectez à un module BMENUA0100 non configuré, l'écran suivant s'affiche :



En dépit de l'aspect du message, la connexion est sécurisée via HTTPS. Connectez-vous en cliquant sur le message de type **Accepter les risques et continuer** (ou autre message de ce type selon le navigateur et la langue).

NOTE: Le message ci-dessus s'affiche car le module ne contient pas encore de configuration valide et il utilise un certificat auto-signé.

Connexion aux pages Web

Lors de la première connexion, l'administrateur de la sécurité entre le Nom d'utilisateur et mot de passe, page 28 définis par défaut. Immédiatement après, l'administrateur doit modifier le mot de passe par défaut.

Vous devez vous connecter chaque fois que vous ouvrez des pages Web pour le module BMENUA0100. Seules les personnes ayant un compte utilisateur valide (nom d'utilisateur et mot de passe valides, créés par un administrateur de la sécurité sur la page Web, page 111 **Contrôle d'accès > Gestion des utilisateurs**) peuvent accéder aux pages Web d'un module.

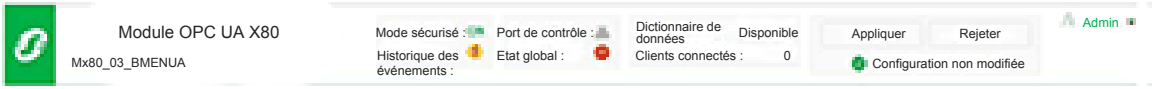
Sur la page de connexion, sélectionnez une langue dans la liste déroulante, entrez votre **Nom d'utilisateur** et votre **Mot de passe**.

NOTE: Le mode de fonctionnement de la cybersécurité du module s'affiche via une icône en forme de verrou en haut à droite de la boîte de dialogue (flèche rouge, au-dessus). Si le verrou est :

- Fermé (comme illustré ci-dessus) : le module fonctionne en mode Secured, page 27.
- Ouvert : le module fonctionne en mode Standard, page 27.

Bannière des pages Web

Chaque page Web comporte une bannière en haut de la page :



La bannière indique les informations suivantes relatives au module BMENUA0100 :

- Mode Secured :
  - Actif : le module fonctionne en mode Secured, page 27.
  - Inactif : le module fonctionne en mode Standard, page 27.
- Historique des événements :
  -  Le service de journalisation des événements est désactivé.
  -  Le service de journalisation des événements est activé, et le serveur de journalisation est joignable.
  -  Le service de journalisation des événements est activé, mais le serveur de journalisation n'est pas joignable.
  -  Le service de journalisation des événements est activé, mais une erreur a été détectée.
- Port de contrôle :
  -  Le port de contrôle est activé.
  -  Le port de contrôle est désactivé.
- Etat global :
  -  Tous les services sont opérationnels.
  -  Au moins un service n'est pas opérationnel.
- Dictionnaire de données :
  - Disponible : la fonctionnalité de dictionnaire de données est disponible.
  - Non disponible : la fonctionnalité de dictionnaire de données n'est pas disponible ou pas activée.
- Clients connectés : nombre de clients OPC UA actuellement connectés.

- Appliquer/Annuler la configuration : Indique l'état de la configuration actuelle de la page Web de cybersécurité du module :
  - Configuration non modifiée : La configuration de la cybersécurité ne contient aucune modification en cours ou non valide. Les commandes **Appliquer** et **Annuler** sont désactivées.
  - Configuration en attente : Une ou plusieurs modifications de la configuration de cybersécurité n'ont pas encore été appliquées. Les commandes **Appliquer** et **Annuler** sont activées.
  - Configuration non valide : La configuration de la cybersécurité est incomplète ou incorrecte. La commande **Appliquer** est désactivée, la commande **Annuler** est activée. Dans cet état, la page Web affiche, à côté de chaque élément de menu concerné, un cercle rouge contenant le nombre de paramètres de configuration non valides accessibles via le menu. Lorsque vous accédez à une page contenant un paramètre non valide, l'interface graphique identifie ce paramètre.

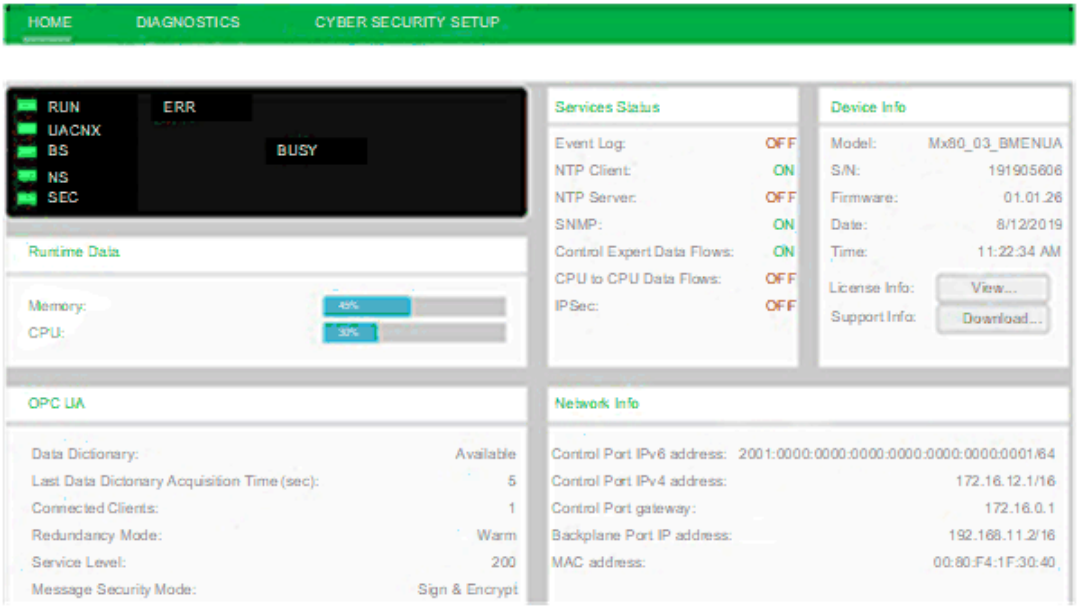
Aide des pages Web

De nombreuses pages Web permettent de consulter une aide contextuelle au niveau des paramètres. Pour obtenir de l'aide pour un paramètre particulier, ou un champ, placez le curseur sur l'icône .

Page d'accueil

Présentation de la page d'accueil

Lorsque vous vous connectez aux pages Web de BMENUA0100, la page **Accueil** s'ouvre par défaut. Si la configuration du module est valide, la page suivante apparaît :



Utilisez la page d'**Accueil** pour :

- Accéder à l'arborescence de navigation, qui contient des liens aux pages Web du module BMENUA0100. Si le module fonctionne en :
  - mode Secured, page 27, les menus DIAGNOSTICS et CYBER SECURITY SETUP s'affichent et sont accessibles pour l'administrateur de la sécurité.
  - mode Standard, page 27, seul le menu DIAGNOSTICS est accessible.
- Affichage de l'état, page 132 des voyants du module, page 21, notamment :
- Affichage d'ensembles de données du module, notamment :
  - Données d'exécution, page 90
  - OPC UA, page 91
  - Etat des services, page 91
  - Infos sur le réseau, page 92
  - Infos sur les équipements, page 92

NOTE: Si le commutateur rotatif à l'arrière du module est défini sur la position Security Reset, page 27, aucune communication n'est possible avec le module. Les pages Web ne sont donc pas accessibles, notamment la page d'**Accueil**.

Données d'exécution

La zone **OPC UA** affiche :

- **Mémoire** : Pourcentage de RAM interne utilisé par le serveur OPC UA (MEM_USED_PERCENT).
- **UC**: Pourcentage de la capacité de traitement de l'UC actuellement utilisé (CPU_USED_PERCENT).

NOTE: Les éléments décrits ci-dessus sont basés sur les éléments du DDT, page 136 T_BMENUA0100.

OPC UA

La zone **Données d'exécution** affiche :

- **Dictionnaire de données** : Etat de disponibilité du dictionnaire de données (DATA_DICT).
- **Durée de la dernière acquisition du dictionnaire de données (sec)** : Durée de la dernière acquisition du dictionnaire de données (DATA_DICT_ACQ_DURATION).
- **Clients connectés** : Nombre de clients OPC UA connectés (CONNECTED_CLIENTS).
- **Mode de redondance** : Mode de basculement pris en charge pour un système redondant (REDUNDANCY_MODE).
- **Niveau de service** : Niveau d'intégrité du serveur OPC UA, basé sur la qualité des données et des services (SERVICE_LEVEL).

  NOTE: Les cinq éléments décrits ci-dessus sont basés sur les éléments du DDT, page 136 T_BMENUA0100.
- **Mode de sécurité des messages** : Réglage configuré dans la page Web OPC UA, page 102 : Aucun, Signature ou Signature et cryptage.

Etat des services

La zone **Etat des services** affiche l'état (activé, ON, ou désactivé, OFF) des services suivants comme indiqué par le DDT, page 136 du T_BMENUA0100 :

- **Historique des événements** (EVENT_LOG_SERVICE)
- **SNMP** (SNMP_SERVICE)
- **Client NTP** (NTP_CLIENT_SERVICE)
- **Serveur NTP** (NTP_SERVER_SERVICE)
- **IPSEC** (IPSEC)

Pour les modules antérieurs à la version BMENUA0100.2.

- **Flux de données Control Expert** (CONTROIL_EXPERT_IP_FORWARDING)
- **Flux de données UC vers UC** (CPU_TO_CPU_IP_FORWARDING)

Infos sur le réseau

Cette zone affiche les paramètres de configuration du module BMENUA0100 entrés dans Control Expert, page 115 et indiqués dans le DDT, page 136 T_BMENUA0100, notamment :

- port de contrôle (CONTROL_PORT_IPV6, CONTROL_PORT_IPV4 et CONTROL_PORT_GTW)
- port d'embase (ETH_BKP_PORT_IPV4)
- adresse MAC du module, valeur hexadécimale unique attribuée à chaque module en usine.

Infos sur les équipements

Cette zone affiche le modèle, le numéro de série et la version de micrologiciel (FW_VERSION dans le DDT, page 136 T_BMENUA0100), la date et l'heure du module BMENUA0100.

Cliquez sur **Afficher...** pour afficher les informations de licence.

Cliquez sur **Télécharger...** pour afficher les informations de contact du support technique.

NOTE: Après avoir cliqué sur **Télécharger...**, vous serez invité à entrer votre mot de passe utilisateur, page 111 pour continuer.

Paramètres

Dans les pages Web du module BMENUA0100, en commençant par la page **Accueil**, sélectionnez **Paramètres** pour afficher les liens vers les pages de configuration suivantes où vous pouvez entrer les paramètres de sécurité de l'équipement :

- Stratégie des comptes utilisateur, page 93
- Journaux d'événements, page 93
- Services réseau, page 94
- Transfert de service, page 96
- IPSEC, page 100
- SNMP, page 101
- OPC UA, page 102
- Bannière de sécurité, page 103

Les paramètres configurables pour chaque noeud sont décrits ci-après.

Utilisez ces paramètres pour configurer la sécurité du module BMENUA0100. Après avoir modifié des paramètres, sélectionnez **Soumettre** ou **Annuler**.

Stratégie des comptes utilisateur

Utilisez ces paramètres pour configurer la stratégie des comptes utilisateur :

Paramètre	Description
Inactivité maximum de session (minutes)	Période de temporisation d'inactivité des sessions pour les connexions HTTPS. Si une connexion reste inactive pendant cette durée, la session utilisateur est automatiquement fermée. Valeur par défaut = 15 minutes. **NOTE:** Il n'existe aucune temporisation d'inactivité pour les connexions OPC UA.
Nombre maximum de tentatives de connexion	Nombre de fois où un utilisateur peut tenter de se connecter sans y réussir. Valeur par défaut = 5 tentatives. Lorsque le maximum configuré est atteint, le compte utilisateur est verrouillé.
Minuteur de tentative de connexion (minutes)	Temps maximum imparti pour se connecter. Valeur par défaut = 3 minutes.
Durée de verrouilalge du compte (minutes)	Période pendant laquelle aucune tentative de connexion supplémentaire ne peut être effectuée une fois le nombre maximum de tentatives atteint. A l'expiration de cette période, un compte utilisateur verrouillé est automatiquement déverrouillé. Valeur par défaut = 4 minutes

NOTE: Ces paramètres de stratégie de compte utilisateur s'appliquent aux clients OPC UA, page 166 auxquels un nom d'utilisateur a été attribué.

Journaux d'événements

Utilisez ces paramètres pour configurer le client Syslog qui réside dans le module BMENUA0100. Les journaux sont stockés localement dans le module et échangés avec un serveur Syslog, page 152 distant :

Paramètre	Description
Activation du service	Active/désactive le service client Syslog. Désactivé par défaut.
Adresse IP du serveur Syslog	Adresse IPv4 ou IPv6 du serveur Syslog distant. **NOTE:** IPv6 est disponible uniquement pour les versions 1.10 et supérieures du micrologiciel.
Port du serveur Syslog	Numéro de port utilisé par le service client Syslog. Valeur par défaut = 601.

Activation des services réseau

Ensemble, ces services constituent un pare-feu qui autorise ou refuse le passage des communications à travers le module BMENUA0100. Utilisez ces paramètres pour activer ou désactiver les services suivants :

STRATEGIE GLOBALE :

Service	Description
Appliquer la sécurité	Désactive tous les services réseau, sauf IPSec qui est activé.
Déverrouiller la sécurité	Active tous les services réseau, sauf IPSec qui est désactivé.

ACTIVATION DES SERVICES RESEAU : Le réglage par défaut des services suivants dépend du mode de fonctionnement de la cybersécurité (Mode CS), comme décrit ci-après :

Service	Description	Mode CS par défaut	
		Standard	Secure
Agent SNMP	Active et désactive les communications de l'agent SNMP.	Activé	Désactivé
Serveur NTP	Active et désactive les communications du serveur NTP.	Activé	Désactivé
IPSec	Active et désactive les communications IPSec.	Désactivé	Activé[1]
Flux de données de CPU à CPU[2, 3] (Voir la section *Configuration de la communication pour les flux de données* de CPU à CPU, page 96.)	Active et désactive les communications Modbus transitant par le module BMENUA0100 entre des CPU M580.	Activé	Désactivé
Flux de données Control Expert vers CPU uniquement[2, 3] (Voir la section *Configuration de la communication pour le flux de données Control Expert*, page 95.)	Active et désactive les communications Modbus, EtherNet/IP, Ping, de messagerie explicite et FTP transitant par le module BMENUA0100 entre le logiciel de configuration Control Expert et la CPU uniquement.	Activé	Désactivé
Flux de données Control Expert vers le réseau d'équipements [2, 3] (Voir la section *Configuration de la communication pour le flux de données Control Expert*, page 95.)	Active et désactive les communications Modbus, EtherNet/IP, Ping, de messagerie explicite et FTP transitant par le module BMENUA0100 entre le logiciel de configuration Control Expert et les équipements réseau, y compris la CPU.	Activé	Désactivé

Service	Description	Mode CS par défaut	
		Standard	Secure
HTTPS sur le port de contrôle	Active et désactive les communications HTTPS sur le port de contrôle. **NOTE:** Si HTTPS est désactivé et que la modification est appliquée, les pages Web ne sont pas accessibles via le port de contrôle. Pour récupérer l'accès aux pages Web à partir du port de contrôle, vous pouvez réinitialiser la configuration de cybersécurité.	Désactivé	Activé
1. IPSec est activé sans aucune règle définie. Le service doit être configuré. 2. Pour plus d'informations sur cette configuration, reportez-vous à la rubrique de dépannage Activation des services réseau à l'aide d'une connexion IPv6 uniquement, page 167. 3. Pris en charge uniquement par les modules antérieurs à la version BMENUA0100.2.			

NOTE: Les services SNMP, NTP, Syslog et Modbus ne sont pas des protocoles sécurisés par nature. Ils sont sécurisés lorsqu'ils sont encapsulés dans IPSEC. Il est recommandé de ne pas désactiver IPSEC dès lors que SNMP, NTP, Modbus ou Syslog est activé.

Configuration de la communication pour un logiciel distant exécuté sur des PC (transfert NAT non utilisé)

Le logiciel s'adresse à l'équipement cible (par exemple, la CPU M580) en utilisant l'adresse IP de ce dernier. Pour prendre en charge cette communication, configurez deux passerelles par défaut, comme suit :

- Sur le PC hôte exécutant le logiciel, à l'aide du protocole IPv4, configurez une passerelle PC par défaut vers l'adresse IP du port de contrôle du module BMENUA0100.
- Sur l'équipement cible (par exemple, la CPU M580), à l'aide d'IPv4, configurez une passerelle par défaut d'équipement vers l'adresse IP du port de contrôle du module BMENUA0100.
- Sur le PC hôte, ajoutez un routage avec la commande suivante :

```
route ADD <<destination=sous-réseau de l'équipement cible>> MASK
<<masque de sous-réseau de l'équipement cible>> <<passerelle=
adresse IP du port d'embase du module BMENUA0100>>
```

Pour IPv4 dans toutes les versions de micrologiciel et pour IPv6 dans les versions de micrologiciel 1.10 et ultérieures, les communications Modbus à partir de l'écran Control Expert Connexion s'adressent à l'adresse IP du port de contrôle du BMENUA0100. Cette communication ne nécessite aucune passerelle.

Configuration de la communication pour les flux de données de CPU à CPU

Les communications Modbus TCP/IP de CPU à CPU via le module BMENUA0100 utilisent l'adresse du port de contrôle IPv4 du module BMENUA0100 et non l'adresse de la CPU cible.

NOTE:

- Pour BMENUA0100 V1.x, le transfert de CPU à CPU est limité au protocole Modbus TCP/IP.
- Seul l'adressage IPv4 (et non IPv6) prend en charge les flux de données Modbus TCP/IP de CPU à CPU.

Transfert de service (transfert IP)

Un module BMENUA0100 équipé du micrologiciel version 2.01 ou supérieure inclut cette page Web. Utilisez-la pour configurer le transfert des flux de données de monodiffusion qui traversent le module entre le réseau de contrôle et le réseau d'équipements. Cette page Web permet de créer, modifier ou supprimer une liste de règles de transfert IP pour le module.

NOTE: La fonction de transfert de service (transfert IP) ne prend pas en charge les fonctions suivantes :

- Flux de données de multidiffusion.
- Messagerie implicite EtherNet/IP.

Par conséquent, les tâches suivantes ne sont pas prises en charge :

- Découverte d'équipements par l'outil EcoStruxure Automation Device Maintenance (EADM) fonctionnant en mode de découverte automatique. La découverte d'équipements par EADM en mode de détection manuel est prise en charge. (multidiffusion).
- Transfert de messages vers les esclaves locaux du PAC (messagerie implicite EtherNet/IP).

Fonctionnalités :

Les principales fonctionnalités de la fonction de transfert de service/ transfert IP sont les suivantes :

- Possibilité de transférer tous les flux de données ("Transférer tout").
- Transfert IP des protocoles les plus courants utilisés dans l'architecture via des modèles prédéfinis (par exemple : Modbus, HTTPS, SNMP, etc.)
- Création et application de modèles de transfert IP personnalisés.

- Transfert NAT (Network Address Translation) de certains protocoles vers la CPU locale si l'adresse IP distante est le port de contrôle IPv4 du BMENUA0100

  NOTE: Le transfert NAT s'applique aux protocoles suivants : Modbus, Modbus sur TLS, EIP explicite, EIP explicite sur TLS, EIP implicite, Client OPC UA.

- Option permettant d'utiliser ou non IPSEC pour les protocoles transférés par NAT. Reportez-vous aux recommandations figurant dans les remarques à la fin de la section IPSEC, ci-dessous, page 100.

NOTE:

- Si plusieurs modules BMENUA0100 sont placés dans le même rack, configurez un seul module BMENUA0100 avec la fonction de transfert.
- Les flux de données de multidiffusion ne sont pas transférés.
- Une mise à jour en ligne des règles de transfert IP peut interrompre certaines communications en cours et entraîner la perte de messages.
- Pour que le transfert de service (transfert IP) réussisse, le réseau IP cible doit être différent du réseau IP source. Par exemple, il n'est pas possible d'exécuter le transfert IP entre :
  - Réseau IP source 192.168.x.x (masque 255.255.0.0) et
  - Réseau IP cible 192.168.x.x (masque 255.255.0.0).
- La valeur du port d'écoute OPC UA doit être la même pour tous les modules BMENUA0100 communiquant entre eux (par exemple, dans le cas d'un transfert NAT OPC UA entre plusieurs modules BMENUA0100).
- L'activation du protocole FTP ouvre une plage de ports TCP allant de 1024 à 65535. Par conséquent, d'autres protocoles utilisant des ports TCP appartenant à cette plage peuvent également être transférés. Il est recommandé de n'activer le transfert du protocole FTP que temporairement, lorsque cela est indispensable.
  - L'activation du protocole TFTP comme règle personnalisée produit le même résultat que l'activation du protocole FTP. Il est recommandé de n'activer le transfert du protocole TFTP que temporairement, lorsque cela est indispensable.

Reportez-vous aux sections suivantes pour plus d'informations sur les architectures de transfert de service (transfert IP) :

- Transfert de service (IP) - Architectures prises en charge, page 172
- Transfert de service (IP) - Architectures non prises en charge, page 175

Transfert IP et communication OPC UA

Le transfert IP et la communication OPC UA sont en concurrence pour la bande passante de communication disponible du module BMENUA0100. Pour consulter les résultats des tests de performance décrivant l'impact du transfert IP, des communications OPC UA, des paramètres de confidentialité et des règles personnalisées sur la bande passante, reportez-vous au chapitre Transfert IP et communication OPC UA, page 176.

Création de règles :

- Pour documenter à la fois les règles prédéfinies et les règles personnalisées, cliquez sur **Nouveau transfert** et complétez les paramètres qui définissent cette règle.

  NOTE: Lorsque vous sélectionnez un nom de service, le numéro de port et le protocole reçoivent automatiquement leurs valeurs par défaut. Ces valeurs peuvent être modifiées si nécessaire.

- Pour modifier une règle existante, cliquez sur l'icône en forme de crayon et modifiez les paramètres.
- Pour supprimer une règle existante, cliquez sur l'icône en forme de bac à déchets.

Réglez **Transférer tout** sur **Désactivé** pour appliquer les règles répertoriées. Si vous réglez **Transférer tout** sur **Activé** :

- Les règles sont suspendues et le module transfère tous les protocoles ;
- Vous ne pouvez pas configurer le transfert pour des services individuels et
- Tous les services sont transférés via IPSec si IPSec est activé.

Chaque règle est définie par les champs suivants :

Réglage	Description
Nom du service	Les services suivants sont prédéfinis : • Modbus • FTP • EIP explicite • ICMP • NTP / SNTP • SNMP • Déroutement SNMP • HTTPS • Modbus sur TLS • EIP explicite sur TLS • TLS démarré par LDAP • Syslog • HTTP • Métadonnées DPWS • OPC UA (pour client OPC UA) • DNP3 • DNP3 sur TLS • IEC 60870 • IEC 60870 sur TLS • EIP implicite **NOTE:** Pour OPC UA, le numéro de port est le port OPC UA défini dans Control Expert pour le module BMENUA0100.
Numéro de port[1]	Port associé au service.
Protocole[1]	Protocole associé au service.
Utilisation IPSec	• **vrai** : le protocole est transporté via IPSec. • **faux** : le protocole n'est pas transporté via IPSec, même si IPSec est activé dans la configuration. Cette sélection n'est disponible que si IPSec est activé. **NOTE:** Recommandations : • **N'utilisez pas** IPSec pour les protocoles qui sont sécurisés par nature (tels que Modbus sur TLS, EIP explicite sur TLS, DNP3 sur TLS, EIP 60870 sur TLS) • **Utilisez** IPSEC pour les protocoles qui ne sont pas sécurisés par nature (tels que Modbus , EIP explicite, client OPC UA, EIP IO)

Réglage	Description
Interface entrante	• **Port de contrôle** : si la requête du client distant est reçue sur le port de contrôle (par exemple : requête Modbus TCP/IP en provenance de Control Expert). • **Port d'embase** : si la requête du client distant est reçue sur le port d'embase (par exemple : requête Modbus TCP en provenance d'un bloc fonction d'automate). • **Les deux** : si la requête du client distant peut être reçue à la fois sur le port de contrôle et le port d'embase (par exemple : requête Modbus TCP/IP en provenance de Control Expert + requête Modbus TCP en provenance d'un bloc fonction d'automate).
1. Complété automatiquement, mais modifiable, pour les noms de service prédéfinis.	

IPSEC

Utilisez IPSEC pour sécuriser la communication Ethernet IPv4.

NOTE: IPSEC ne prend pas en charge l'adressage IPv6.

Utilisez ces paramètres pour configurer un maximum de 8 voies IKE / IPSEC sur IPv4 pour le module BMENUA0100. Si plus de 4 liaisons IPSec sont configurées, la connexion automatique au PAC après le transfert via le BMENUA0100 peut échouer. Dans ce cas, connectez-vous manuellement au PAC.

Paramètre	Description
SERVICE IPSEC	• Activé : Active le service IPSec. • Désactivé : Désactive le service IPSec.
NTP autorisé en dehors de IPSEC	• Désélectionné (désactivé) : Les échanges NTP sont possibles uniquement via IPSEC. • Sélectionné (activé) : Les échanges NTP sont effectués via IPSEC si la voie IPSEC est ouverte, en dehors de IPSEC si la voie IPSEC n'est pas ouverte.
Nouvelle liaison	Crée une nouvelle voie IKE / IPSEC et l'ajoute à la liste pour modification. **NOTE:** 8 voies IKE/IPSec au maximum sont prises en charge.
Pour chaque voie IKE / IPSEC, configurez les paramètres suivants :	
Adresse IP distante	Adresse IPv4 du point de terminaison IPSEC distant. **NOTE:** L'équipement distant doit être accessible à partir du port de contrôle du BMENUA0100 (et non à partir du port d'embase du BMENUA0100).
Confidentialité	• Sélectionné : La communication sera cryptée. • Désélectionné : Pas de cryptage. **NOTE:** La confidentialité est désactivée si l'option *NTP sans IPSEC* est activée.

Paramètre	Description
Type de client	Type du point de terminaison IPSEC distant : Windows ou Equipement. **NOTE:** La valeur par défaut est Windows. Vérifiez que le type de point de terminaison configuré correspond au client réel.
PSK	Clé pré-partagée de 32 caractères hexadécimaux, résultat d'un nombre aléatoire généré par le module BMENUA0100. Copie et modification possibles dans cette page Web. **NOTE:** PSK est désactivé si l'option *NTP sans IPSEC* est activée.

NOTE: Configurez les paramètres de pare-feu Windows, page 178 en téléchargeant le "script Windows" à partir de BMENUA0100 à l'aide de la commande **Télécharger le script** pour chaque adresse IP distante. Si le réglage **Utilisation de IPSEC** est modifié pour certains protocoles, le script Windows doit être téléchargé à nouveau à partir du module BMENUA0100 et exécuté sur Windows. Pour consulter un exemple de script Windows, reportez-vous à la section Scripts Windows pour IPSEC, page 178.

NOTE: Si 8 tunnels IPSEC sont configurés, il peut s'avérer impossible de se reconnecter automatiquement au PAC après le téléchargement d'une application. Dans ce cas, reconnectez-vous manuellement au PAC après le téléchargement.

NOTE: Si IPSEC est activé, le flux de données du serveur HTTPS local sortira de IPSEC.

SNMP

Utilisez ces paramètres pour configurer la version SNMP et les réglages associés.

NOTE: En mode Secured, la version de SNMP doit être configurée de la même manière dans Control Expert, page 128 et dans la page Web SNMP. Si ces paramètres sont différents, le service SNMP ne démarre pas.

Paramètre	Description
Version de SNMP	• v1 • v3
Niveau de sécurité	Pour SNMP v1 et v3 : • NoAuthNoPriv : Communication sans authentification ni confidentialité. **NOTE:** Pour SNMP v1, il s'agit du seul réglage disponible. Pour SNMP v3 uniquement : • AuthNoPriv : Communication avec authentification mais sans confidentialité. Le protocole d'authentification est SHA (Secure Hash Algorithm).

Paramètre	Description
	• AuthPriv : Communication avec authentification et confidentialité. Les protocoles utilisés sont : ◦ Authentification : SHA. ◦ Confidentialité : AES (Advanced Encryption Standard).
Mot de passe d'authentification	Si l'authentification est activée, entrez un mot de passe d'authentification (sensible à la différence minuscule/majuscule). Il doit comprendre 8 à 12 caractères qui peuvent inclure des caractères alphanumériques (lettres majuscules et minuscules, chiffres), comme indiqué par l'info-bulle dans la page Web.
Mot de passe de confidentialité	Si la confidentialité est activée, entrez un mot de passe de confidentialité (sensible à la différence minuscule/majuscule). Il doit comprendre 8 caractères qui peuvent inclure des caractères alphanumériques (lettres majuscules et minuscules, chiffres), comme indiqué par l'info-bulle dans la page Web.

OPC UA

Utilisez ces paramètres pour configurer la connexion du serveur OPC UA intégré au module BMENUA0100 :

Paramètre	Description
Mode de sécurité des messages	• Signature et cryptage (par défaut) : Chaque message reçoit une signature et est crypté. • Signature : Une signature est appliquée à chaque message. • Aucun : Aucune stratégie de sécurité n'est appliquée. Dans ce cas, les deux champs suivants sont désactivés. **NOTE:** Lorsque l'option **Aucun** est sélectionnée, le **Type de jeton utilisateur** dans le module BMENUA0100 est défini sur **Anonyme**. Le cas échéant, vous devez également configurer le type de jeton d'identification utilisateur dans le client OPC UA sur **Anonyme**.
Stratégie de sécurité	• Basic256Sha256 (par défaut) : Définit une stratégie de sécurité pour les configurations avec une suite cryptographique valide. • Basic256 : Définit une stratégie de sécurité pour les configurations avec une suite cryptographique obsolète. **NOTE:** Cette sélection n'est utilisée que si elle est nécessaire à l'interopérabilité avec le client distant. • Basic128Rsa15 : Définit une stratégie de sécurité pour les configurations avec une suite cryptographique obsolète. **NOTE:** Cette sélection n'est utilisée que si elle est nécessaire à l'interopérabilité avec le client distant.
Types de jeton d'identification utilisateur	• Anonyme : Aucune information utilisateur n'est disponible. • Nom d'utilisateur (par défaut) : L'utilisateur est identifié par un nom d'utilisateur et un mot de passe.

NOTE: Les modifications apportées à la configuration de la cybersécurité du serveur OPC UA entraînent le redémarrage du serveur et l'application des nouveaux paramètres. Par conséquent, si une ou plusieurs sessions OPC UA existent lorsque des modifications de configuration sont effectuées, ces sessions sont suspendues. A l'expiration de la période *Timeout de session*, ces sessions sont finalement fermées. La valeur de *Timeout de session* fait partie de la configuration du client OPC UA SCADA.

NOTE: Lorsque le **Mode de sécurité des messages** du serveur OPC UA est initialement configuré pour **Signature et cruptage** ou **Signature** et qu'un client OPC UA établit une connexion, si vous définissez ensuite le **Mode de sécurité des messages** du serveur OPC UA sur **Aucun**, un client OPC UA (avec son paramètre **Mode de sécurité des messages** également défini sur **Aucun**) ne peut pas établir de connexion au serveur.

Pour établir à nouveau une connexion :

1. Déconnectez vos clients OPC UA actuels.
2. Modifiez la configuration OPC UA dans la page Web du BMENUA0100.
3. Attendez que le voyant BUSY (allumé en jaune) s'éteigne.
4. Pour les clients OPC UA, modifiez la configuration (**Mode de sécurité des messages**) en l'alignant sur celle utilisée pour le serveur OPC UA.
5. Reconnectez les clients OPC UA au serveur.

Bannière de sécurité

Cette page contient le texte modifiable qui s'affiche lorsqu'un utilisateur accède aux pages Web du module BMENUA0100 :

Paramètre	Description
Texte de la bannière	Chaîne de 128 caractères maximum adressée à l'utilisateur sur la page de connexion. Le texte (modifiable) suivant s'affiche par défaut : "L'utilisation non autorisée du système est interdite et soumise à des sanctions pénales et/ou civiles."

Gestion des certificats

Gestion des certificats avec et sans PKI

Le module BMENUA0100 s'appuie sur des certificats pour l'authentification. Pour assurer la cybersécurité, chaque entité (y compris les clients OPC UA et le serveur OPC UA intégré au BMENUA0100) doit gérer une liste de confiance de tous les certificats d'équipements/applications qui communiquent avec elle.

La méthode de gestion des certificats dépend de la conception de votre système, qui peut appliquer ou non une infrastructure de clé publique (PKI) avec une autorité de certification (CA).

Gestion des certificats sans PKI :

Utilisez cette méthode de gestion des certificats si votre système n'inclut pas d'autorité de certification. Cette méthode de gestion est prise en charge par les modules BMENUA0100 dotés du micrologiciel de version v1.0 ou supérieure. Gérez les certificats dans les pages Web **Gestion des certificats**, de la manière suivante :

- Réglez **Mode PKI** sur **Auto-signé uniquement**.
- Gérez la **liste de certificats approuvés** à l'aide des fonctions **Ajouter** et **Supprimer** pour créer une liste blanche des clients OPC UA autorisés à communiquer avec le module BMENUA0100.
- Exportez le certificat du module BMENUA0100 vers les équipements clients OPC UA à l'aide de la commande **Télécharger** de la page **Configuration desPKI > Certificat d'équipement**.

Gestion des certificats avec PKI :

Utilisez cette méthode de gestion des certificats si votre système inclut une autorité de certification (CA). Cette méthode de gestion est prise en charge par les modules BMENUA0100 dotés du micrologiciel de version v1.1 ou supérieure. Gérez les certificats dans les pages Web **Gestion des certificats**, de la manière suivante :

- Réglez **PKI mode** :
  - **CA uniquement** : si tous les équipements client OPC UA installés prennent en charge PKI.
  - **Auto-signé et CA** : si certains équipements client OPC UA installés ne prennent pas en charge PKI.
- Si **Mode PKI** est réglé sur **CA uniquement** :
  - Inscrivez manuellement, page 109 chaque module BMENUA0100 auprès de l'autorité de certification.
- Si **PKI mode** est réglé sur **Auto-signé et CA** :
  - Inscrivez manuellement, page 109 chaque module BMENUA0100 auprès de l'autorité de certification.
  - Gérez la **liste de certificats approuvés** à l'aide des fonctions **Ajouter** et **Supprimer** pour créer une liste blanche des clients OPC UA autorisés à communiquer avec le module BMENUA0100.

Mise à jour de la liste de certificats approuvés

Après la première installation du BMENUA0100 avec micrologiciel version 2.0 (BMENUA0100.2) ou supérieure, vous devez supprimer tous les certificats ajoutés par

l'utilisateur de la **Liste de certificats approuvés** dans la page Web **Gestion des certificats**. Les méthodes possibles sont les suivantes :

- Suppression manuelle des certificats concernés à l'aide de la commande **Supprimer** ou
- Réglage du commutateur rotatif de réglage de la cybersécurité sur la position **Security Reset** (réinitialisation de la sécurité).

Une fois la **liste de certificats approuvés** nettoyée, vous pouvez la réalimenter avec des certificats auto-signés ou émis par une autorité de certification.

Cette tâche doit être effectuée uniquement lors de la première installation du micrologiciel de version 2.0 ou supérieure. Il n'est pas nécessaire de répéter la procédure pour les installations suivantes de versions de micrologiciel supérieures.

NOTE: Si vous n'effacez pas la **Liste de certificats approuvés**, comme décrit ci-dessus, les connexions avec les clients OPC UA ne peuvent pas être établies ou, si elles sont établies, elles seront perdues.

Présentation de l'authentification

Un client OPC UA ou un module BMENUA0100 peut être authentifié de trois façons :

- Pour la version 1.0 ou supérieure du micrologiciel :
  - Certificat auto-signé (uniquement)
- Pour la version 1.10 ou supérieure du micrologiciel :
  - Certificat PKI émis par une autorité de certification tierce uniquement
  - Certificat PKI émis par une autorité de certification et un certificat auto-signé

Pour assurer le niveau de cybersécurité requis, chaque entité (client OPC UA, BMENUA0100) doit gérer une liste de confiance de tous les certificats d'équipements/applications qui communiquent avec elle.

Pour la version 1.10 ou supérieure du micrologiciel, le module BMENUA0100 crée un certificat auto-signé aux fins suivantes :

- Configuration des paramètres de cybersécurité via les pages Web du module
- Diagnostic du module via ses pages Web
- Mise à niveau du micrologiciel
- Certificats d'instance d'application OPC UA permettant aux clients OPC UA d'accéder au serveur OPC UA intégré au module BMENUA0100.

Pour la version 1.0 du micrologiciel, le module crée deux certificats : un certificat HTTPS et un certificat OPC UA.

NOTE:

- Les dates d'expiration des certificats approuvés sont définies par rapport aux paramètres internes de date et d'heure du module BMENUA0100. Pour éviter toute incohérence, utilisez le service NTP pour mettre à jour les paramètres de date et d'heure du module BMENUA0100 et vérifiez que le serveur NTP est accessible et qu'il a mis à jour les paramètres de date et d'heure.
- Si vous recevez un message d'erreur signalant un certificat incorrect en raison d'un nom d'hôte non valide lors d'une tentative de connexion de votre client OPC UA au serveur BMENUA0100 en IPv6, cela peut être dû à une adresse IPv6 compressée (raccourcie). Dans ce cas, vérifiez l'adresse IPv6 utilisée et, si nécessaire, remplacez-la par un format non compressé.
- Le module BMENUA0100 ne gère pas automatiquement les dates d'expiration des certificats. Vous devez gérer ces dates d'expiration manuellement.

Gestion des certificats

Dans les pages Web du module BMENUA0100, à partir de la page **Accueil**, sélectionnez **Gestion des certificats** pour afficher les liens vers les pages suivantes de gestion des certificats d'instance d'application :

- Configuration des PKI, page 108
- Gestion de liste de confiance de clients, page 109
- Exportation de certificats d'équipement, page 110
- Inscription manuelle, page 109
- Certificats CA, page 110

Consultez les sections *Utilisation des objets GPO/LGPO*, page 166 et *Application de la gestion des stratégies de groupe MMC*, page 166 pour plus d'informations sur les outils Windows™ que vous pouvez utiliser pour gérer les certificats.

Extensions de certificat

Pour prendre en charge la communication avec le module BMENUA0100, les certificats auto-signés et CA doivent inclure des extensions spécifiques, à savoir :

Certificats auto-signés :

- Utilisation des clés (marqué comme critique) :
  - Signature numérique
  - Chiffrement de clé (pas d'utilisation pour la suite TLS basée sur des clés éphémères telles que TLS_ECDHE_xxxx ; utilisation pour TLS_RSA_xxxx)
  - Signature des certificats de clé : lorsque la clé publique du sujet est utilisée pour vérifier les signatures sur les certificats de clé publique (valeur TRUE)
  - Non-répudiation (exigence de la norme OPC UA)
  - Chiffrement des données (exigence de la norme OPC UA)
- Autre nom du sujet : Ce champ accepte les valeurs suivantes : Adresse IP V4/V6, URI
- Contraintes de base :
  - le champ CA indique si la clé publique certifiée peut être utilisée pour vérifier les signatures de certificat (valeur TRUE) et la contrainte de longueur de chemin 0
- Identificateur de la clé du sujet :
  - moyen d'identifier les certificats qui contiennent un hachage public SHA-1 160 bits particulier de la valeur de la chaîne de bits de la clé publique du sujet (à l'exclusion de la balise, de la longueur et du nombre de bits inutilisés).
- Extension de l'utilisation améliorée des clés :
  - id-kp-serverAuth en cas d'authentification du serveur Web TLS
  - id-kp-clientAuth en cas d'authentification du client Web TLS

Certificats CA :

- Utilisation des clés (marqué comme critique) :
  - Signature numérique
  - Chiffrement de clé (pas d'utilisation pour la suite TLS basée sur des clés éphémères telles que TLS_ECDHE_xxxx ; utilisation pour TLS_RSA_xxxx)
  - Signature des certificats de clé : lorsque la clé publique du sujet est utilisée pour vérifier les signatures sur les certificats de clé publique (valeur FALSE)
  - Non-répudiation (exigence de la norme OPC UA)
  - Chiffrement des données (exigence de la norme OPC UA)
- Autre nom du sujet : Ce champ accepte les valeurs suivantes : Adresse IP V4/V6, URI
- Contraintes de base :
  - Champ CA : indique si la clé publique certifiée peut être utilisée pour vérifier les signatures de certificat (valeur FALSE)
- Extension de l'utilisation améliorée des clés :
  - id-kp-serverAuth en cas d'authentification du serveur Web TLS
  - id-kp-clientAuth en cas d'authentification du client Web TLS
- Points de distribution de liste de certificats de confiance

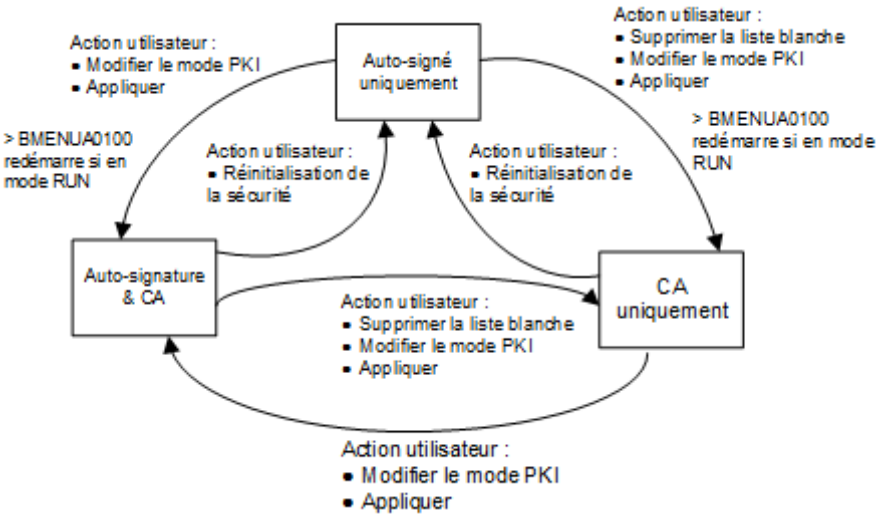
- Identificateur de clé de l'autorité :
  - Identification de la clé publique correspondant à la clé privée utilisée pour signer un certificat.

Configuration PKI

Utilisez la page **Configuration PKI** pour spécifier les types de certificats acceptés par le serveur OPC UA intégré au module, comme suit :

Mode PKI	Description
Auto-signé uniquement	Seuls les certificats de la liste **Certificats de client approuvés** ("liste blanche") ont à être gérés.
CA uniquement	Tous les équipements du système ont besoin de certificats signés par une autorité de certification.
Auto-signé et CA	Les certificats sont gérés comme suit : • Le certificat du module BMENUA0100 équipé du micrologiciel de version 1.10 ou supérieure est émis par une autorité de certification. • Les certificats des équipements clients qui prennent en charge PKI sont émis par une autorité de certification. • Les certificats des équipements clients qui ne prennent pas en charge PKI sont auto-signés.

Le schéma suivant illustre les actions utilisateur et les événements liés à la modification du réglage de mode PKI :



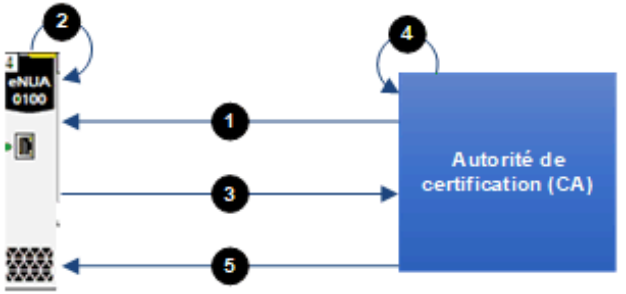
Inscription manuelle

Après avoir configuré le module BMENUA0100 dans Control Expert, vous pouvez utiliser la page **Inscription manuelle** pour obtenir un fichier CSR à soumettre à une autorité de certification. Après avoir envoyé le fichier CSR, vous pouvez extraire le certificat CA correspondant. Ensuite, vous pouvez insérer ce certificat CA dans le module BMENUA0100. Les opérations combinées d'obtention et d'insertion inscrivent manuellement un certificat émis par une autorité de certification tierce. Une fois le certificat inséré, le serveur OPC UA l'applique pour signer et crypter sa communication avec le client OPC UA.

NOTE: Condition préalable à l'inscription manuelle :

- Assurez-vous que le client NTP est activé, page 124.
- Vérifiez que le paramètre d'heure du module BMENUA0100 est l'heure réelle.

Vous trouverez ci-dessous une vue d'ensemble du processus d'inscription manuelle d'un certificat :



1 BMENUA0100 importe un certificat CA à partir de l'autorité de certification

2 BMENUA0100 génère une demande de signature de certificat (CSR)

3 BMENUA0100 exporte le fichier CSR vers l'autorité de certification

4 L'autorité de certification exécute la requête CSR et génère un certificat

5 BMENUA0100 importe le certificat émis par l'autorité de certification

Reportez-vous à la vidéo Schneider Electric illustrant l'utilisation du mode PKI "Auto-signé et CA" sur le module BMENUA0100, disponible sur https://www.se.com/us/en/faqs/FAQ000191153/.

Gestion de liste de confiance de clients

Seuls les clients OPC UA qui ont fourni un certificat d'instance d'application au module BMENUA0100 peuvent communiquer avec le serveur OPC UA intégré au module. Le module met en oeuvre une gestion locale (basée sur le module) des certificats d'instance

d'application OPC UA, lesquels sont stockés dans une liste de confiance. Utilisez les commandes des pages Web **Gestion des certificats** pour **Ajouter**, **Télécharger** ou **Supprimer** un certificat.

NOTE: Les certificats de la liste de confiance d'instances d'application OPC UA sont codés en ANSI CRT.

Pour ajouter un certificat à la liste :

Etape	Action
1	Dans le menu Gestion de la liste de confiance, cliquez sur **Ajouter**.
2	Cliquez sur **Parcourir**, puis naviguez jusqu'au certificat que vous souhaitez ajouter à la liste et sélectionnez-le.
3	Cliquez sur **Soumettre** pour ajouter le certificat.
4	Cliquez sur **Appliquer** pour enregistrer la modification dans la configuration.

Pour supprimer un certificat de la liste :

Étape	Action
1	Dans la liste de confiance, cliquez sur le certificat à supprimer
2	Sélectionnez **Supprimer**.
3	Cliquez sur **Oui** pour supprimer le certificat de la liste.
4	Cliquez sur **Appliquer** pour enregistrer la modification dans la configuration.

Exportation de certificats d'équipement

Vous pouvez exporter le certificat du module BMENUA0100 pour HTTPS et OPC UA sur la page **GESTION DES CERTIFICATS > CONFIGURATION PKI** en cliquant sur le bouton **Télécharger**

Certificats CA

Le certificat d'autorité de certification est un certificat de clé publique qui identifie l'autorité de certification (CA) dans une infrastructure de clé publique (PKI). Utilisez la page **Certificats CA** pour insérer le ou les certificats d'autorité de certification dans l'équipement.

Pour ajouter un certificat de l’autorité de certification à la liste de certificats CA :

Étape	Action
1	Ouvrez les pages Web du module et entrez les informations suivantes dans la boîte de dialogue **Connexion** : • nom d'utilisateur • mot de passe Cliquez sur **Connexion**.
2	Sélectionnez **CONFIGURATION DE LA CYBERSECURITE > GESTION DES CERTIFICATS** pour accéder à l'onglet gestion des certificats, puis sélectionnez **Certificats CA**.
3	Dans la liste **CERTIFICATS APPROUVÉS**, cliquez sur **AJOUTER** pour ajouter le certificat d'autorité de certification à la liste.
4	Appliquez les modifications à la configuration de cybersécurité.

NOTE: Vous pouvez ajouter jusqu'à dix (10) certificats CA.

Contrôle d'accès

Introduction

Le module BMENUA0100 prend en charge l'authentification des utilisateurs basée sur une combinaison nom d'utilisateur/mot de passe pour :

- Configuration des paramètres de cybersécurité via HTTPS
- Téléchargement de micrologiciel via HTTPS
- Diagnostics sur pages Web du module via HTTPS

NOTE: Seul un utilisateur ayant le rôle d'administrateur de la sécurité peut créer, modifier ou supprimer des comptes utilisateur.

Les pages Web BMENUA0100 fournissent des outils pour la gestion des utilisateurs. Sur la page d'**Accueil**, cliquez sur **Contrôle d'accès** pour afficher la liste des utilisateurs OPC UA existants ainsi que leurs rôles et autorisations. Dans cette page, vous pouvez :

- Ajouter un utilisateur, page 112.
- Mettre à jour le profil, page 113 d'un utilisateur existant.
- Supprimer, page 113 un utilisateur.

Gestion des utilisateurs

Le module BMENUA0100 fournit un contrôle d'accès basé sur des rôles (RBAC). Un rôle est attribué à chaque utilisateur, qui lui permet d'effectuer uniquement les tâches associées au rôle.

Les rôles et les autorisations ci-dessous sont pris en charge :

Rôle	Autorisations			
	Configuration de la cybersécurité	**Mise à niveau du firmware**	**Accès aux pages Web de diagnostic**	**Accès par protocole OPC UA**
SECADM	Mise à jour, Lecture, Suppression	–	Lecture	–
OPERATEUR	–	–	Lecture	Connexion
INGENIEUR	–	–	Lecture	Connexion
INSTALLA-TEUR	–	Mise à jour	Lecture	–

Chaque module BMENUA0100 prend en charge au maximum 15 serveurs simultanés.

Aucun ensemble de rôles personnalisés ou d'autorisations autorisées ne peut être configuré. Aucune liste blanche de contrôle d'accès par adresse IP ne peut être configurée.

Ajouter un utilisateur

Un administrateur de la sécurité peut cliquer sur **Nouvel utilisateur** puis configurer les paramètres suivants pour ajouter un nouvel utilisateur :

Paramètre	Description
Nom utilisateur	Identifiant de l'utilisateur. L'utilisateur saisit cette information avec le mot de passe pour accéder aux fonctions autorisées.
Mot de passe	Mot de passe de l'utilisateur. Comme le mot de passe ne s'affiche pas en texte clair, entrez cette valeur deux fois pour confirmer l'exactitude. **NOTE:** Chaque mot de passe doit contenir au moins 8 caractères, et au moins l'un des caractères suivants : • un caractère alphabétique en majuscule (A...Z) • un caractère alphabétique en minuscule (a...z) • un chiffre base 10 (0...9) • un caractère spécial ~ ! @ $ % ^ & * _ + - = ` | \ ( ) [ ] : " ' < >
Confirmation du mot de passe	
Rôles	Sélectionnez le rôle utilisateur, qui permet de définir les autorisations accordées à l'utilisateur : • Administrateur de la sécurité • Opérateur • Ingénieur • Installateur

Cliquez sur **Appliquer les modifications** après la configuration de ces paramètres pour créer le nouvel utilisateur.

Mise à jour de l'utilisateur

Pour modifier les paramètres d'un utilisateur existant, un administrateur de la sécurité peut cliquer sur l'icône de modification (crayon) pour le profil à modifier. Cliquez sur **Appliquer les modifications** pour enregistrer les modifications. La même boîte de dialogue que celle pour l'ajout d'un nouvel utilisateur s'ouvre, vos pouvez y mettre à jour la configuration des utilisateurs sélectionnés.

Suppression d'utilisateur

Pour supprimer un utilisateur existant, un administrateur de la sécurité peut cliquer avec le bouton droit sur l'utilisateur de la liste et dans **Suppression d'utilisateur** cliquer sur **OK**.

Gestion de la configuration

Introduction

Pour simplifier la configuration du système, vous pouvez exporter les paramètres de cybersécurité d'un module configuré BMENUA0100, et importer la configuration sur un autre module. Sur les pages Web du module BMENUA0100, sur la page d'**Accueil**, sélectionnez **Gestion de la configuration** pour afficher les liens d'accès aux pages suivantes de gestion de la configuration de la cybersécurité :

- EXPORTATION, page 113
- IMPORTATION, page 114
- REINITIALISATION, page 115

NOTE: Seul un administrateur de la sécurité, avec le rôle SECADM, peut effectuer les tâches de gestion de configuration décrites dans cette rubrique.

Exportation de configuration

Utilisez la page **EXPORTATION** pour exporter le fichier de configuration de la cybersécurité du module BMENUA0100 local. Le fichier de configuration exporté est chiffré avec le mot de passe attribué à cette page. Un fichier de configuration exporté peut être stocké et réutilisé.

Pour exporter le fichier de configuration de la cybersécurité du module BMENUA0100 local :

Etape	Description
1	Sur la page **EXPORTATION**, attribuez le fichier de configuration d'un **Mot de passe**. **NOTE:** Le mot de passe doit être au minimum de 16 caractères et s'applique aux mêmes règles utilisées dans la création des mots de passe de l'utilisateur, page 112.
2	Entrez à nouveau le mot de passe attribué dans le champ **Confirmation du mot de passe**.
3	Cliquez sur **Télécharger**.

NOTE: Le fichier de configuration est créé avec le nom suivant : Mx80_xx_BMENUA.cfg, où "xx" indique le numéro d'emplacement occupé par le module dans le rack.

Importation d'une configuration

Utilisez la page **IMPORTATION** pour importer le fichier de configuration de la cybersécurité et l'appliquer au module BMENUA0100 local. Les paramètres de cybersécurité appliqués en utilisant cette commande remplacent les paramètres de cybersécurité existants sur le module.

Pour importer un fichier de configuration de la cybersécurité et l'appliquer au module BMENUA0100 local.

Etape	Description
1	Sur la page **IMPORTATION**, cliquez sur l'icône du fichier pour ouvrir une fenêtre où vous pouvez sélectionner une **archive de configuration**.
2	Sélectionnez le fichier de configuration à importer, et cliquez sur **OK**.
3	Sur la page **IMPORTATION**, entrez le **mot de passe** du fichier de configuration (attribué au fichier lors de l'exportation). **NOTE:** Vous pouvez sélectionner **Enregistrer** pour appliquer automatiquement la configuration immédiatement importée après le chargement.
4	Cliquez sur **Charger**. Une boîte de dialogue s'ouvre pour vous informer que votre session a été fermée. La configuration a été chargée sur le serveur.
5	Cliquez sur **Reconnecter** pour fermer la boîte de dialogue et ouvrir l'écran de connexion, page 86.
6	Entrez votre nom d'utilisateur et le mot de passe d'administrateur de la sécurité, puis cliquez sur **Connexion**. La page Accueil s'affiche. Si vous n'avez pas sélectionné **Enregistrer** à l'étape 3, la bannière indique qu'une configuration est en cours.
7	Dans la bannière, cliquez sur **Appliquer**, puis cliquez sur **Oui** pour confirmer que vous souhaitez appliquer la configuration en cours. La nouvelle configuration est appliquée. **NOTE:** Si vous avez sélectionné **Enregistrer** sur la page **IMPORTATION** (comme indiqué dans l'étape 3 ci-dessus) la configuration est automatiquement appliquée, et cette étape 7 est automatiquement exécutée.

Réinitialisation de configuration

Cliquez sur **Réinitialiser** sur la page **REINITIALISATION** pour restaurer les paramètres d'usine de la cybersécurité sur le module BMENUA0100 local. Cette action a le même effet que la sélection avec le commutateur rotatif en position Security Reset, page 27.

Configuration du BMENUA0100 dans Control Expert

Introduction

Cette section explique comment configurer les paramètres d'adresse IP, de client NTPv4 et d'agent SNMPv1 pour le module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré.

Configuration des paramètres d'adresse IP

Introduction

Le module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré inclut deux ports Ethernet :

- Le port de contrôle situé à l'avant du module.
- Un port d'embase connectant le module à l'embase Ethernet du rack principal local.

Le port de contrôle peut être activé ou désactivé. Par défaut, il est désactivé. Le port d'embase est toujours activé.

Les paramètres d'adresse IP statique pour le port de contrôle et le port d'embase peuvent être configurés dans l'onglet **Configuration IP** de la boîte de dialogue de configuration du BMENUA0100. De plus, les paramètres de l'adresse IP peuvent être dynamiquement attribués au port de contrôle via la méthode DHCP appelée SLAAC (Stateless Address Auto-configuration).

Si le module BMENUA0100 est utilisé sur un PAC autonome, les paramètres de l'adresse IP sont configurés pour un seul module. Si deux instances du module BMENUA0100 sont actives dans une architecture PAC à redondance d'UC (un module BMENUA0100 dans chaque PAC), l'onglet **Configuration IP** de Control Expert affiche les paramètres pour deux modules (A et B). Dans une architecture PAC à redondance d'UC, l'adresse IP de chaque module peut se trouver dans différents sous-réseaux.

Prise en charge des piles IPv4 et IPv6

Le port de contrôle peut être configuré pour prendre en charge les piles IP (chacune est constituée d'une série de protocoles Internet) comme suit :

- Pile IPv4 : Prend en charge uniquement l'adressage 32 bits. Exemple d'adresse IPv4 : 192.168.1.2.
- Pile double IPv4/IPv6 : Prend en charge l'adressage 32 bits et 128 bits. Lorsque les deux piles IPv4 et IPv6 sont configurées, le port de contrôle peut recevoir et gérer des paquets Ethernet IPv4 et IPv6. Exemple d'adresse IPv6 128 bits : 2001:0578:0123:4567:89AB:CDEF:0123:4567.

  NOTE: A la mise sous tension initiale (ou après que le sélecteur rotatif a été réglé sur la position **Security Reset**, démarré, puis réglé en position **Secured** et redémarré), l'adresse IPv4 10.10.MAC5.MAC6 est attribuée au port de contrôle, où MAC5 est la valeur décimale du (5e octet de l'adresse MAC du module et MAC6 la valeur décimale du 6e octet. L'adresse MAC du module est indiquée sur la face avant.

IPv6 via le port de contrôle

La communication IPv6 n'est prise en charge que via le port de contrôle.

NOTE: Le flux Control Expert peut être configuré pour être routé vers un PAC M580. Control Expert V15 peut être connecté à un PAC M580 via l'adresse IPv6 du BMENUA0100.

Configuration des adresses IP

Configurez l'adressage IP dans Control Expert, comme suit :

Étape	Action
1	Dans le **Navigateur de projet** développez le noeud **BUS automate** et ouvrez la boîte de dialogue de configuration du module BMENUA0100.
2	Cliquez sur l'onglet **Configuration IP**.
3	Modifiez les champs appropriés dans la page **Configuration IP**. (Le tableau suivant décrit les paramètres de la page de configuration.)

Paramètres configurables

Configurez les paramètres de l'adresse IP pour chaque module de communication BMENUA0100 dans votre projet :

Paramètre		Description
Port de contrôle		Active/désactive le port de contrôle du module BMENUA0100. Si le paramètre est : • Activé : le port de contrôle est l'interface exclusive pour la communication IPv4 ou IPv6 avec le serveur OPC UA intégré. • Désactivé (par défaut) : le port d'embase Ethernet peut prendre en charge la communication IPv4 avec le serveur OPC UA.
Configuration du port de contrôle IPv6		
	IPv6	Active/désactive l'adressage IPv6 pour le port de contrôle lorsque celui-ci est activé. Par défaut = désactivé.
	Mode	Identifie la source de l'adresse IPv6 : • SLAAC : Indique que l'adresse IPv6 sera fournie au port de contrôle par un serveur DHCP à l'aide de la méthode SLAAC. • Statique (par défaut) : Active le champ IPv6@ pour la saisie d'une adresse IPv6 statique.
	IPv6 @	Si vous sélectionnez **Statique** dans **Mode**, entrez une adresse IPv6 valide pour le port de contrôle. **NOTE:** Le BMENUA0100 détecte des adresses IPv6 en double. Veuillez vérifier avec l'administrateur réseau qu'il n'y a pas d'adresses IPv6 en double dans le même segment du réseau.
	Longueur du préfixe du sous-réseau	Définie automatiquement pour l'adresse IPv6 statique, représente le nombre de bits de l'adresse IPv6 affectée par SLAAC qui définissent le préfixe du sous-réseau. (par défaut = 64).
Configuration du port de contrôle IPv4		
	IPv4	Active/désactive l'adressage IPv4 pour le port de contrôle lorsque celui-ci est activé. Par défaut = activé.
	Mode	Identifie la source de l'adresse IPv4 : • Par défaut : Une adresse IP est automatiquement attribuée par le logiciel. • Statique (par défaut) : Active les champs **IPv4 @**, **Masque de sous-réseau** et **Passerelle par défaut** pour la saisie d'une adresse IPv4 statique affectée au port de contrôle.
	IPv4 @	Si le mode sélectionné est : • **Par défaut** : L'adresse IP est automatiquement attribuée ; les champs **IPv4 @**, **Masque de sous-réseau** et **Passerelle par défaut** sont désactivés. • **Statique** : Entrez une adresse IPv4 valide pour le port de contrôle.

Paramètre		Description
	Masque sous-réseau	Si **Statique** est sélectionné pour le **Mode**, entrez un masque de sous-réseau IPv4 valide pour le port de contrôle, qui va déterminer le segment de réseau de l'adresse IPv4.
	Passerelle par défaut	Si vous sélectionnez **Statique** dans **Mode**, entrez une adresse IPv4 valide pour la passerelle par défaut.
Port d'embase		
	IPv4 @	Entrez une adresse IPv4 valide pour le port d'embase.
Horodatage source		Reportez-vous à la section Configuration de l'horodatage à la source, page 119.
Taux d'échantillonnage rapide		Lorsque cette option est sélectionnée, vous pouvez configurer le client OPC UA avec un intervalle d'échantillonnage minimum de 20 ms, ce qui permet de surveiller 2 000 éléments. Désélectionnée par défaut, la périodicité d'échantillonnage par défaut est de 250 ms, ce qui permet de surveiller l'équivalent de 20 000 éléments de type INT. **NOTE:** Une modification de ce paramètre n'est effective qu'après un téléchargement complet de l'application.
Port d'écoute OPCUA TCP		Port TCP pour la communication OPCUA : • Par défaut : prédéfini sur le port 4840 • Par une autre valeur : spécifié par l'utilisateur **NOTE:** La valeur de ce port doit être identique pour tous les modules BMENUA0100 communiquant ensemble (par exemple, dans le cas du transfert OPC UA NAT entre plusieurs modules BMENUA0100)

NOTE: Lors de la configuration de votre application dans Control Expert :

- La fenêtre **Réseau Ethernet** (ouverte via **Outils > Gestionnaire de réseau Ethernet...**) affiche les paramètres du port d'embase et du port de contrôle du module BMENUA0100, notamment les informations relatives au serveur NTP, au gestionnaire SNMP et, pour un système de redondance d'UC, au module BMENUA0100 redondant (B).
- La page **Serveur d'adresses** de la CPU (ouverte dans le **Navigateur de DTM** en cliquant deux fois sur la CPU, puis en sélectionnant **Services > Serveur d'adresses**) affiche l'adresse IP du port d'embase du module BMENUA0100. Dans une configuration à redondance d'UC, la page **Serveur d'adresses** de la CPU affiche l'adresse IP du port d'embase des deux modules BMENUA0100.

Configuration de l'horodatage à la source

L'horodatage à la source est pris en charge à partir de la version 2.01 du micrologiciel du module BMENUA0100 (BMENUA0100.2) dans Control Expert.

Pour utiliser l'horodatage à la source dans une application, vous devez l'autoriser puis l'activer.

Une fois que l'horodatage source est autorisé et activé, le module BMENUA0100 commence à interroger les équipements dès qu'il y a au moins un élément surveillé avec le **Mode de surveillance** défini sur **Echantillonnage** ou **Signalant** dans le client OPC UA.

Autorisation de l'horodatage à la source

Vous autorisez l'horodatage à la source dans la fenêtre Paramètres du projet. Accédez à **Général > Heure > Mode d'horodatage** et sélectionnez **Système**.

NOTE: Le **Mode d'horodatage** par défaut est **Applicatif**. Si vous ne modifiez pas le réglage par défaut en **Système**, une erreur détectée s'affiche lors de la génération de l'application.

Activation de l'horodatage à la source

Utilisez l'onglet **IPConfig** de la boîte de dialogue de configuration de BMENUA0100 pour activer et configurer l'horodatage.

Dans la section **Horodatage source**, effectuez les réglages suivants :

Paramètre	Description
Activé	Active l'horodatage à la source pour l'application.
Interrogation de la mémoire tampon (ms)	Fréquence d'interrogation pour les requêtes de lecture d'événement gérées par le BME NUA 0100. Plage de valeurs valides : • 250 ms (minimum) à • 5000 ms (maximum) par incréments de 250 ms. **NOTE:** Le nombre maximum de variables horodatées à la source dans Control Expert est de 5000.

NOTE: Si le rack local M580 comprend deux modules BMENUA0100, l'horodatage source ne peut être utilisé que par un seul module. Voir Paramétrage du module BMENUA0100 pour la gestion des variables horodatées, page 122.

Gestion des variables horodatées à la source

Utilisation des éléments de données OPC UA #TSEventItemsReady et #TSEventSynchro

Vous pouvez utiliser les éléments de données OPC UA `#TSEventItemsReady` et `#TSEventSynchro` pour parcourir et définir respectivement l'état des variables horodatées à la source.

NOTE: Ces éléments sont significatifs uniquement lorsque l'horodatage est autorisé dans Control Expert et activé pour le module BMENUA0100 concerné.

Le module BMENUA0100 traite l'élément `#TSEventSynchro` comme un noeud OPC UA booléen.

L'activation de `#TSEventSynchro` envoie une commande de synchronisation à tous les équipements horodatés à la source de l'ePAC M580. Les valeurs renvoyées par les équipements au client OPC UA initialisent les variables horodatées à la source avec leurs valeurs actuelles.

Le BMENUA0100 répond au client qui définit l'élément `#TSEventSynchro` avec l'un des messages suivants :

- `UA_EGOOD` : La requête de synchronisation a été correctement envoyée à tous les équipements d'horodatage.
- `UA_EBAD` : La requête de synchronisation a échoué car l'horodatage est désactivé dans le projet Control Expert.
- `UA_EBADINVALIDSTATE` : La requête de synchronisation a échoué car l'horodatage a été désactivé pour le module BMENUA0100 par la fonction %MW400, page 122.
- `UA_EBADINUSE` : La requête de synchronisation a échoué car le module BMENUA0100 n'a pas pu réserver de mémoire tampon d'horodatage.
- `UA_EBADDISCONNECT` : La requête de synchronisation n'a pas réussi à écrire les valeurs dans la période spécifiée et a été désactivée.

Pour effectuer cette initialisation, utilisez un client OPC UA (par exemple UaExpert) pour effectuer la séquence de tâches suivante :

1. Surveillez l'élément `#TSEventItemsReady` indiquant que le module BMENUA0100 est prêt à gérer les variables horodatées des tampons ePAC (y compris les modules M580 CPU, BMECRA, BMEERT), puis attendez que sa valeur passe à 1 (vrai).
2. Ajoutez des éléments de données surveillés configurés comme variables horodatées à la source à ZZun ou plusieurs abonnements.
3. Définissez la commande d'écriture `#TSEventSynchro` pour mettre à jour la valeur et l'horodatage à la source de chaque élément.

NOTE:

- Le BMENUA0100 lit toutes les variables horodatées configurées dans l'ePAC. Si un événement (changement d'état d'un élément) se produit sur un élément surveillé horodaté, cet élément est mis à jour. Si un élément n'est pas surveillé, il est ignoré.
- Il est recommandé de régler le filtre des modifications de données sur **Etat/Valeur/Horodatage**. Sinon, il pourrait arriver que différents clients OPC UA (par exemple des clients qui mettent à jour les valeurs uniquement en cas de changement d'état/de valeur) affichent un état et une valeur différents pour la même variable.
- Comme le module BMENUA0100 met à jour les valeurs périodiquement, il est possible que plusieurs événements se produisent entre deux mises à jour. Dans ce cas, le BMENUA0100 affiche uniquement la valeur la plus récente.
- `#TSEventSynchro` étant envoyé à plusieurs équipements d'horodatage, si un de ces équipements ne répond pas dans le délai imparti, `#TSEventSynchro` renvoie la réponse `UA_EBADDISCONNECT` indiquant que la commande a dépassé le délai sans aboutir, et cela même si plusieurs équipements répondent correctement.
- Si l'abonnement est modifié pour ne contenir (par exemple) qu'une seule variable pour un seul équipement, l'exécution de `#TSEventSynchro` entraîne la perte des valeurs renvoyées précédemment pour les équipements et variables faisant l'objet de l'abonnement précédent.

Détermination des voies d'UC M580 dédiées à l'horodatage

Pour la communication entre le BMENUA0100 et une CPU M580 où l'horodatage est activé dans Control Expert, 25 % des voies de la CPU sont dédiées à la prise en charge de la fonction d'horodatage. 75 % des voies de la CPU au maximum restent disponibles pour les autres requêtes de communication.

Par exemple, pour la CPU BMEP584040 :

- Nombre maximum de voies : 13
- Voies utilisées pour l'horodatage : 3
- Voies utilisées à d'autres fins : 10

Détermination de la capacité du BMENUA0100 à lire les variables horodatées

Le nombre de variables horodatées que le module BMENUA0100 peut lire par cycle dépend des éléments suivants :

- Réglage du paramètre **Interrogation de la mémoire tampon** dans l'onglet **Configuration IP** du module

- Capacité de l'équipement à la source, notamment :
  - Nombre maximum de connexions TCP,
  - Nombre maximum de variables horodatées à la source prises en charge.

La formule permettant de déterminer le nombre maximum de variables horodatées à la source pour un équipement donné est la suivante :

(Nbre max. de connexions TCP) / (Nbre de voies)) x (Nbre max. de variables horodatées par cycle)

Exemple :

- BMEP586040 : 16 connexions maximum, 4 voies, 82 variables maximum :

  (16 / 4) x 82 = 328 variables au total

  Si **Interrogation de la mémoire tampon** est réglé sur 500 ms : 656 variables par seconde.
- BMECRA : 1 connexion, 1 voie, 82 variables maximum :

  1 x 82 = 82 variables au total

  Si **Interrogation de la mémoire tampon** est réglé sur 500 ms : 164 variables par seconde.
- BMEERT : 1 connexion, 1 voie, 20 variables maximum :

  1 x 20 = 20 variables au total

  Si **Interrogation de la mémoire tampon** est réglé sur 500 ms : 40 variables par seconde.

Spécification du BMENUA0100 chargé de gérer les variables horodatées

Un rack M580 principal peut contenir deux modules BMENUA0100. Cependant, les variables horodatées des CPU M580 et des modules BMECRA et BMEERT ne peuvent être lues et gérées que par un seul module BMENUA0100 à la fois. Au démarrage, chaque BMENUA0100 tente par défaut de réserver et de verrouiller l'accès aux variables horodatées.

Dans un rack comprenant deux modules BMENUA0100, vous devez spécifier celui qui va lire et gérer les variables horodatées. Pour spécifier le BMENUA0100 qui va lire et gérer les variables, procédez comme suit :

1. Dans l'onglet **Configuration IP** des deux modules BMENUA0100 que vous souhaitez charger de l'horodatage, sélectionnez **Activé**.

2. Pour le module BMENUA0100 auquel vous souhaitez réserver le tampon d'horodatage, utilisez le bloc `WRITE_VAR` pour définir le mot %MW400 sur 2 et activer ainsi la lecture et la gestion des variables horodatées pour ce module.

   NOTE: Le réglage %MW400 = 2 identifie le module BMENUA0100 qui va lire et gérer les variables lorsque l'option **Activé** est sélectionnée pour deux modules BMENUA0100.

3. Pour l'autre module BMENUA0100 auquel vous ne souhaitez pas réserver de tampon d'horodatage, utilisez le bloc `WRITE_VAR` pour définir le mot %MW400 sur 1 et désactiver ainsi la lecture et la gestion des variables horodatées pour ce module.

   NOTE: Vous devez effectuer ces étapes après chaque changement de mode de fonctionnement, notamment la mise sous tension, le chargement de l'application ou l'exécution d'une initialisation.

Le BMENUA0100 que vous désignez conserve le contrôle de la lecture et de la gestion des variables horodatées tant que les deux conditions suivantes sont remplies :

- Au moins une variable horodatée est surveillée.
- Le **mode de surveillance** du BMENUA0100 est réglé sur **Signalant** ou sur **Echantillonnage**.

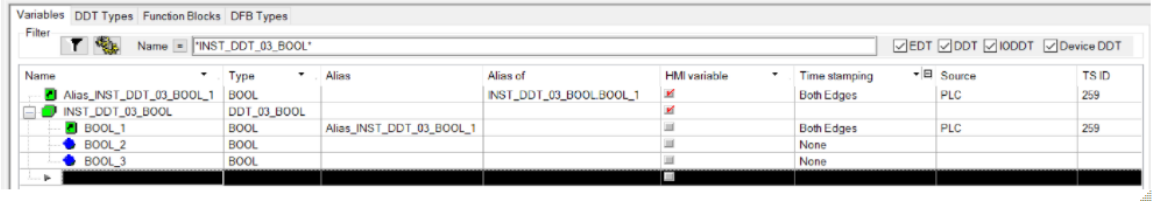
NOTE:

Lorsque le réglage **Activé** est désélectionné, les valeurs des variables lues par le BMENUA0100 sont celles stockées dans la mémoire ePAC.

Lorsque **Activé** est sélectionné et que %MW400 est réglé sur 1, les variables lues par le BMENUA0100 conservent la dernière valeur lue lorsque la mémoire tampon d'horodatage était réservée.

Surveillance des variables alias horodatées

Le BME NUA 0100 reconnaît les variables alias BOOL ou EBOOL horodatées qui sont créées dans Control Expert, mais il ne reconnaît pas de manière identique les variables "Alias de" correspondantes. Voici un exemple de variables Alias et "Alias de" :



Pour être reconnues par BME NUA 0100, les variables Alias doivent être intégrées dans le dictionnaire de données.

Les variables Alias BOOL ou EBOOL et leurs variables "Alias de" correspondantes partagent la même adresse logique dans la mémoire M580 et le même ID d'événement

dans le tampon d'horodatage M580. L'horodatage à la source est géré uniquement sur la variable Alias, pas sur la variable "Alias de". En d'autres termes, vous devez inscrire la variable Alias (noeud OPC UA) dans le client OPC UA pour pouvoir recevoir l'horodatage à la source depuis l'équipement au lieu du BME NUA 0100.

Comme aucune variable "Alias de" BOOL ou EBOOL n'est perçue comme étant horodatée à la source par le micrologiciel BME NUA 0100, l'alias doit être intégré dans le dictionnaire de données. Dans ce cas, vous devez ajouter la variable Alias en tant qu'élément surveillé dans un abonnement OPC UA pour réaliser l'horodatage à la source défini par l'équipement.

Configuration du service de temps réseau

Introduction

Le module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré prend en charge la version 4 du protocole NTP. Les services NTP synchronise l'horloge du module BMENUA0100 avec l'horloge d'un serveur temporel. La valeur synchronisée permet de mettre à jour l'horloge du module.

Les protocoles IPv4 et IPv6 sont tous les deux pris en charge.

NOTE:

- Si le serveur NTP se trouve sur la CPU, le module BMENUA0100 peut mettre à jour ses paramètres temporels sans générer de retard.
- Si un nouveau serveur NTP est contacté ou si un décalage temporel se produit sur un serveur NTP, la mise à jour de BMENUA0100 peut tarder 5 minutes. Le voyant ERR, page 132 reste allumé jusqu'à la synchronisation temporelle de BMENUA0100 avec le serveur NTP.
- La configuration manuelle d'un changement d'heure via la saisie d'une heure ultérieure peut déconnecter les voies OPC UA existantes. Si le client OPC UA effectue une reconnexion automatique au serveur OPC UA, de nouvelles voies sont créées et la reconnexion est effectuée.

Activation et désactivation du client NTP et du serveur NTP

Le module BMENUA0100 inclut à la fois un client NTP et un serveur NTP.

Client NTP :

Si l'adresse IP du serveur NTP primaire ou secondaire est définie sur une autre valeur que 0.0.0.0, le client NTP est activé. Si les paramètres d'adresse IP des serveurs NTP primaire et secondaire sont vides ou définis sur 0.0.0.0 (IPv4) ou 0000:000:000:000:000:000:000:000:000:0000 (IPv6), le client NTP est désactivé.

NOTE: Si l'adresse IP du **serveur NTP primaire** et du **serveur NTP secondaire** est définie sur 0.0.0.0, le module BMENUA0100 ne peut pas fonctionner comme client NTP ou serveur NTP.

Serveur NTP :

Le serveur NTP est activé, en fonction du mode de fonctionnement de la cybersécurité :

- En mode Secured, le serveur NTP est activé si :
  - L'adresse IP du serveur NTP primaire OU du serveur NTP secondaire est une valeur non nulle (valeur autre que 0.0.0.0), et
  - Le serveur NTP est activé dans les paramètres de configuration de la page web, page 94 **Services réseau**.
- En mode Standard, le serveur NTP est activé si l'adresse IP du **serveur NTP primaire** ou le **serveur NTP secondaire** est une valeur non nulle (autre que 0.0.0.0).

  NOTE: Si le BMENUA0100 est configuré en tant que client NTP d'un réseau d'embase (**serveur NTP primaire** ou **serveur NTP secondaire**), le serveur BMENUA0100 n'est activé dans aucun cas, même en l'absence de serveur NTP sur le réseau d'embase.

Si le serveur NTP et le client NTP sont activés sur le module BMENUA0100, le client NTP du module reçoit les paramètres de temps d'un serveur NTP distant via son port de contrôle. Le serveur NTP du module transfère ces paramètres de temps aux clients NTP via son port d'embase.

NOTE: Le module BMENUA0100 ne peut pas fonctionner comme serveur NTP via son port de contrôle.

Interrogation NTP

Le module BMENUA0100 gère de façon optimale et dynamique la période d'interrogation NTP sur le serveur NTP. Aucune configuration n'est nécessaire.

Mise sous tension

Pour définir l'heure exacte du réseau Ethernet, le système effectue les opérations suivantes lors de la mise sous tension :

- Le module de communication BMENUA0100 démarre.
- Le module de communication BMENUA0100 obtient l'heure fournie par le serveur NTP.
- Le service requiert l'envoi régulier de requêtes afin d'obtenir et de maintenir l'heure exacte. La configuration de la **Période d'interrogation** influence l'exactitude de l'heure.

Une fois une heure exacte reçue, le service définit l'état dans le diagnostic du service de temps associé.

Le module de communication BMENUA0100 ne gère pas l'heure. Lors du démarrage ou du redémarrage, la valeur de l'horloge du module est 0, ce qui correspond au 1er janvier 1980 à 00:00:00:00.

Configuration du service

Configurez le service de synchronisation du temps réseau dans Control Expert, comme suit :

Étape	Action
1	Dans le **Navigateur de projet** développez le noeud **BUS automate** et ouvrez la boîte de dialogue de configuration du module BMENUA0100.
2	Cliquez sur l'onglet **NTP**.
3	Modifiez les champs appropriés dans la page de configuration du **Service de temps réseau**. (Le tableau suivant décrit les paramètres de la page de configuration.)

Paramètres configurables

Configurez les paramètres de synchronisation temporelle pour chaque module de communication BMENUA0100 de votre projet :

Paramètre		Description
Configuration du serveur NTP IPv4		
	Serveur NTP primaire (voir la remarque)	Entrez une adresse IPv4 ou IPv6 valide pour le serveur NTPv4 primaire. **NOTE:** Configurez l'adresse IP principale par défaut de l'UC.
	Serveur NTP secondaire (voir la remarque)	Entrez une adresse IPv4 ou IPv6 valide pour le serveur NTPv4 secondaire.

NOTE:

- Configurez l'adresse du serveur NTP accessible par le module BMENUA0100. Si le port de contrôle est désactivé, entrez des adresses IP de serveur NTP qui se trouvent dans le même sous-réseau que le port d'embase.
- Vous pouvez configurer une adresse IPV4 pour le serveur NTP primaire et une adresse IPV6 pour le serveur NTP secondaire (et inversement), à condition que les deux adresses se trouvent dans le même domaine.
- Pour les configurations à redondance d'UC (Hot Standby), les adresses de serveur NTP pour **NUA(A)** et **NUA(B)** doivent se trouver dans le même réseau, par exemple le réseau accessible via le port d'embase ou le réseau accessible via le port de contrôle.

NOTE: En mode Secured, vérifiez que le service NTP est activé dans la section Activation des services réseau, page 94 de la page Web **Paramètres**.

Configuration d'un agent SNMP

A propos du protocole SNMP

Toutes les versions de micrologiciel du module BMENUA0100 prennent en charge l'agent SNMP version 1 (V1). La version 2 (ou ultérieure) du micrologiciel du module (BMENUA0100.2) prend également en charge la version 3 (V3) de l'agent SNMP.

NOTE: Les deux versions SNMP (V1 et V3) ne sont pas prises en charge simultanément.

Un agent SNMP est un composant logiciel du service SNMP qui s'exécute sur le module BMENUA0100 et permet d'accéder aux informations de diagnostic et de gestion du module. Vous pouvez utiliser des navigateurs SNMP, des logiciels de gestion de réseau et d'autres outils pour accéder à ces données.

En outre, l'agent SNMP peut être configuré avec les adresses IP de 1 ou 2 équipements (généralement des PC exécutant un logiciel de gestion de réseau) utilisées comme cibles des messages de déroutement (trap) fondés sur des événements. Ces messages communiquent à l'équipement de gestion les événements tels que les démarrages à froid et l'incapacité du logiciel d'authentifier un équipement.

NOTE: La communication avec l'agent SNMP exécuté sur le module BMENUA0100 peut utiliser l'adressage IPv4 ou IPv6.

Arrêt du service SNMP

Le service SNMP exécuté sur le module BMENUA0100 s'arrête si :

- Le module est à l'état ERREUR
- Le module est à l'état DEFAUT (FAULT).

Accès à l'onglet SNMP

Double-cliquez sur le module BMENUA0100 dans la configuration de Control Expert pour accéder à l'onglet **SNMP**.

L'agent SNMP peut se connecter et communiquer avec 1 ou 2 gestionnaires SNMP. Le service SNMP inclut :

- L'authentification, vérifiée par le module BMENUA0100, de tout gestionnaire SNMP qui envoie des requêtes SNMP.

- La gestion d'événements ou de déroutements (trap)

Configuration de l'agent SNMP dans Control Expert et les pages Web

Les paramètres SNMP courants sont configurés dans Control Expert. Les paramètres SNMP liés à la cybersécurité sont configurés dans les pages Web du module.

En fonction du réglage du sélecteur rotatif de cybersécurité :

- Mode Secured : vous pouvez configurer l'agent SNMP dans Control Expert et dans les pages Web du module BMENUA0100.

  NOTE: En mode Secured, la version de SNMP doit être configurée de la même manière dans Control Expert et dans la page Web SNMP, page 101. Si ces paramètres sont différents, le service SNMP ne démarre pas.

- Mode Standard : vous ne pouvez configurer l'agent SNMP que dans Control Expert.

  NOTE: Si le module est configuré pour SNMP V3 dans Control Expert :

  - Le module BMENUA0100.2 équipé du micrologiciel de version 2 ou supérieure utilise SNMP V3 avec le niveau de sécurité sans authentification et sans confidentialité.
  - Le module BMENUA0100 équipé d'un micrologiciel antérieur à la version 2 utilise SNMP V1.

Paramètres SNMP

L'onglet **SNMP** de Control Expert comprend les paramètres suivants. Sauf indication contraire, les paramètres s'appliquent à SNMP V1 et V3.

NOTE: En mode Secured, la version de SNMP doit être configurée de la même manière dans Control Expert et dans la page Web SNMP, page 101. Si ces paramètres sont différents, le service SNMP ne démarre pas.

Champ	Paramètre	Description	Valeur
Version de SNMP	SNMP V1	Sélectionnez cette option pour utiliser SNMP V1	case sélectionnée/ désélectionnée
	SNMP V3	Sélectionnez cette option pour utiliser SNMP V3	
Gestionnaires d'adresses IP	Gestionnaire d'adresses IP 1	Adresse IPv4 du premier gestionnaire SNMP auquel l'agent SNMP envoie les notifications de déroutement (trap).	Dépend du protocole (IPv4)

Champ	Paramètre	Description	Valeur
	Gestionnaire d'adresses IP 2	Adresse IPv4 du deuxième gestionnaire SNMP auquel l'agent SNMP envoie les messages de déroutement (trap).	
Agent	Emplacement (SysLocation)	emplacement de l'équipement	31 caractères maximum
	Contact (SysContact)	Informations sur la personne à contacter pour la maintenance de l'équipement	
	Activer le gestionnaire SNMP	option *désélectionnée* (par défaut) : Vous pouvez modifier les paramètres **Emplacement** et **Contact**. option *sélectionnée* : Vous ne pouvez pas modifier les paramètres **Emplacement** et **Contact**.	case sélectionnée/ désélectionnée
Noms de communautés (SNMP V1 uniquement)	Set	mot de passe requis par l'agent SNMP pour lire les commandes d'un gestionnaire SNMP **NOTE:** Il n'y a pas de valeur par défaut. Si un gestionnaire SNMP est utilisé, entrez le même nom de communauté que celui utilisé par le gestionnaire SNMP.	15 caractères (maximum)
	Get		
	Trap		
Sécurité (SNMP V1 uniquement)	Activer une interruption "Echec d'authentification"	*option désélectionnée* (par défaut) : Non activé. *option sélectionnée* : Activé. L'agent SNMP envoie un message de déroutement (trap) au gestionnaire SNMP si un gestionnaire non autorisé envoie une commande **Get** ou **Set** à l'agent.	case sélectionnée/ désélectionnée
Nom d'utilisateur SNMP (SNMP V3 uniquement)		Nom d'utilisateur reconnu par le serveur SNMP.	chaîne de 32 caractères ASCII / UTF8 maximum dans la plage de codage [33-122]

Déroutements (trap) pris en charge

Par défaut, l'agent SNMP V1 du module BMENUA0100 prend en charge les déroutements suivants :

- Liaison établie
- Liaison interrompue

Le déroutement (trap) d'échec d'authentification est également pris en charge, si activé.

Identifiants d'objets SNMP MIB-2

Dans la section **Nom du fournisseur** Schneider Electric, le module BMENUA0100 présente les valeurs suivantes pour l'identifiant d'objet (OID) :

Nom de l'objet	OID	Valeur
SysDesc	1.3.6.1.2.1.1.1	Produit : BMENUA0100 - Module de communication OPC UA. Identifiant du micrologiciel : xx.yy
SysObjectID	1.3.6.1.2.1.1.2	1.3.6.1.4.1.3833.1.7.255.53
SysName	1.3.6.1.2.1.1.5	BMENUA0100
SysServices	1.3.6.1.2.1.1.7	74 : représente la somme de (2**7-1 + 2**4-1 + 2**2-1) et indique la prise en charge des protocoles dans les couches OSI suivantes : • 7 : couche application • 4 : couche de transport • 2 : couche de liaison de données
ifDesc	1.3.6.1.2.1.2.2.1.2	Cet OID contient des informations décrivant l'interface, notamment le nom du produit et le nom de port.

Configuration des paramètres d'UC M580 pour les connexions client-serveur OPC UA

Introduction

Cette section décrit les paramètres de configuration de l'UC M580 concernés par la prise en charge des connexions entre le serveur OPC UA intégré au module BMENUA0100 et un client OPC UA.

Configuration des paramètres de sécurité de l'UC M580

Configuration des services de l'UC

Pour prendre en charge les communications entre le serveur OPC UA du module BMENUA0100 et un client OPC UA, activez les paramètres suivants dans l'onglet Sécurité de l'UC M580 :

- **TFTP**
- **DHCP / BOOTP**

Si ces services ne sont pas tous les deux activés dans l'UC, les communications OPC UA ne fonctionneront pas correctement.

Diagnostics

Présentation

Ce chapitre décrit les outils de diagnostic disponibles pour le module de communication Ethernet BMENUA0100 avec serveur OPC UA intégré.

Voyants de diagnostic

Panneau de voyants de diagnostic

Le panneau de voyants, page 21 du module BMENUA0100 est décrit ci-dessous pour les différents états de fonctionnement du module.

NOTE: L'état du voyant SECURE pour l'état configuré et non configuré du module est présenté séparément à la suite de la présentation initiale.

Etat de fonctionnement		**Voyant RUN (vert)**	**Voyant UACNX (vert/ rouge)**	**Voyant ERR (rouge)**	**Voyant d'embase BS (vert/ rouge)**	**Voyant du port de contrôle NS (vert/ rouge)**	**Voyant BUSY (jaune)**	**Voyant SECURE (vert/ rouge)**
Séquence de mise sous tension	1	Eteint	Allumé	Allumé	Vert éteint Rouge fixe	Vert éteint Rouge fixe	Eteint	Vert éteint Rouge fixe
	2 (tous les voyants sont allumés)	Allumé	Allumé	Allumé	Vert fixe Rouge fixe	Vert fixe Rouge fixe	Allumé	Vert fixe Rouge fixe
	3 (tous les voyants sont éteints)	Eteint	Eteint	Eteint	Vert éteint Rouge éteint	Vert éteint Rouge éteint	Eteint	Vert éteint Rouge éteint
	4	Allumé	Eteint	Allumé	Vert éteint Rouge éteint	Vert éteint Rouge éteint	Eteint	Vert éteint Rouge éteint
	5 (autotest[1])	Clignotant	Clignotant	Clignotant	Vert clignotant Rouge éteint	Vert clignotant Rouge éteint	Clignotant	Vert clignotant Rouge éteint

Etat de fonctionnement		**Voyant RUN (vert)**	**Voyant UACNX (vert/ rouge)**	**Voyant ERR (rouge)**	**Voyant d'embase BS (vert/ rouge)**	**Voyant du port de contrôle NS (vert/ rouge)**	**Voyant BUSY (jaune)**	**Voyant SECURE (vert/ rouge)**
Non configuré		Eteint	Eteint	Clignotant	Rouge clignotant si non connecté à un port d'embase Ethernet. Vert clignotant dans le cas contraire.	Eteint si aucun câble n'est branché et connecté à un autre appareil alimenté. Vert clignotant dans le cas contraire.	Eteint	Reportez-vous aux voyants de cybersécurité ci-dessous, page 135.
Configuré	Après détection d'une adresse IPv4 en double sur le port d'embase	Clignotant	Reportez-vous à la description du voyant UACNX ci-dessous, page 134	/	Vert éteint Rouge fixe	/	/	Reportez-vous à la description du voyant d'état de la communication sécurisée ci-dessous, page 135.
	Après détection d'une adresse IPv4 en double sur le port de contrôle	Clignotant		/	/	Vert éteint Rouge fixe	/	
	Etat RUN	Allumé		Eteint	Vert fixe Rouge éteint	Vert fixe si connecté ; éteint si aucun câble	Allumé fixe en cas d'acquisition du dictionnaire de données en cours ; clignotant en cas de débordement du dictionnaire de données ; éteint dans les autres cas	
Hors tension		Eteint	Eteint	Eteint	Vert éteint	Vert éteint	Eteint	Vert éteint

Etat de fonctionnement		Voyant RUN (vert)	Voyant UACNX (vert/ rouge)	Voyant ERR (rouge)	Voyant d'embase BS (vert/ rouge)	Voyant du port de contrôle NS (vert/ rouge)	Voyant BUSY (jaune)	Voyant SECURE (vert/ rouge)
					Rouge éteint	Rouge éteint		Rouge éteint
Erreur récupérable détectée ou configuration incohérente[2]		/	/	Allumé	/	/	/	/
Erreur non récupérable détectée (Le module va redémarrer)		Eteint	Eteint	Allumé	Vert éteint Rouge fixe	Vert éteint Rouge fixe	Eteint	Vert éteint Rouge fixe
Réinitialisation de la sécurité	En cours	Clignotant	Eteint	Eteint	Vert éteint Rouge fixe	Vert éteint Rouge fixe	Allumé	Vert éteint Rouge éteint
	Terminé	Allumé	Eteint	Eteint	Vert éteint Rouge fixe	Vert éteint Rouge fixe	Eteint	Vert éteint Rouge éteint
Réinitialisation de la sécurité manquante[3]		Eteint	Eteint	Allumé	Vert éteint Rouge fixe	Vert éteint Rouge fixe	Eteint	Rouge clignotant
Mise à jour du système d'exploitation		Clignotant	Eteint	Eteint	Vert éteint Rouge fixe	Vert éteint Rouge fixe	Allumé	Vert éteint Rouge éteint

1. L'autotest est exécuté rapidement et le clignotement du voyant est imperceptible.

NOTE: Si le module reste à l'état Autotest, vérifiez que le commutateur rotatif n'est pas cassé.

2. Consultez les codes d'erreur détectée SERVICES_STATUS dans le DDT T_BMENUA0100, page 136.

3. Cet état résulte du réglage du commutateur rotatif du mode Standard au mode Secured ou inversement sans passer par une réinitialisation de la sécurité, page 26.

NOTE: Dans ce tableau, "/" indique n'importe quel état.

Voyant UACNX lorsque le module est à l'état configuré

La couleur (rouge ou vert) et l'état (clignotant ou fixe) décrivent l'état des connexions OPC UA :

Etat du dictionnaire de données	Etat de connexion du client OPC UA	
	Aucun client OPC UA connecté	Au moins 1 client OPC UA connecté
Dictionnaire de données indisponible	Rouge clignotant	Rouge fixe
Dictionnaire de données disponible	Vert clignotant	Vert fixe

Voyant d'état des communications sécurisées lorsque le module est à l'état configuré/non configuré

Les états du voyant SECURE lorsque le module est dans l'état configuré ou non configuré sont décrits ci-dessous :

Etat du voyant	Description
Eteint	Le module ne fonctionne pas en mode sécurisé (le commutateur rotatif n'est pas réglé sur la position Secured).
ROUGE	Une erreur critique de la communication sécurisée est détectée. Par exemple, aucune configuration de sécurité n'est présente, un certificat n'est pas valide, un certificat a expiré et les communications se sont arrêtées, etc.
VERT	Les communications sécurisées sont activées et s'exécutent sans erreur détectée. Un client est connecté au module et celui-ci a reçu une configuration de cybersécurité valide. La session est ouverte et le module est prêt à répondre aux requêtes du client.
ROUGE CLIGNOTANT	Les communications sécurisées sont activées et s'exécutent mais une erreur a été détectée. Par exemple, un certificat a expiré mais la configuration autorise la poursuite des communications.
VERT CLIGNOTANT	Le module a reçu une configuration de cybersécurité valide et il est prêt à communiquer avec un client qui lancera une communication.

Voyants de diagnostic du port de contrôle

Les voyants du port de contrôle, page 22 permettent de diagnostiquer l'état des communications Ethernet sur le port de contrôle :

Voyant	Etat	Description
ACT	Eteint	Aucune liaison établie.
	Vert	Liaison établie, aucune activité.
	Vert clignotant	Liaison établie, activité détectée.

Voyant	Etat	Description
LNK	Eteint	Aucune liaison établie.
	Jaune	Liaison établie à une vitesse inférieure à la capacité maximale du module (10/100 Mbits/s).
	Vert	Liaison établie à une vitesse égale à la capacité maximale du module (1000 Mbits/s).

BMENUA0100 - Type de données dérivé (DDT)

Introduction

Chaque module de communication Ethernet BMENUA0100 à serveur OPC UA intégré que vous ajoutez à votre application instancie un ensemble commun d'éléments de données. Vous pouvez utiliser les outils présentés dans le logiciel Control Expert pour accéder à ces données et diagnostiquer le module.

NOTE:

- Les données DDT renvoyées en réponse à une requête Modbus ne peuvent pas dépasser 256 octets.
- Compte tenu de l'organisation du dictionnaire de données Control Expert, les requêtes de données stockées en bits de mots doivent être extraites par le client demandeur.

Le contenu du DDT est accessible à l'aide de la fonction élémentaire (EF) READ_DDT, page 141 du logiciel Control Expert.

NOTE: Si le DDT du module ne peut pas être lu pour une raison quelconque (par exemple, si l'adresse IP de l'embase n'est pas correctement configurée), vous pouvez dignostiquer le module via ses voyants, page 132.

Structure du DDT T_BMENUA0100

Le DDT BMENUA0100 comprend les éléments suivants :

Elément	Type	Adresse	Description
DEVICE_NAME	STRING [16]	MW1...8	Nom du module.
CONTROL_PORT_IPV6	STRING [44]	MW9...30	Adresse IPv6 du port de contrôle / longueur du préfixe de sous-réseau

Elément	Type	Adresse	Description
CONTROL_PORT_IPV4	STRING [18]	MW31...39	Adresse IPv4 du port de contrôle / longueur du préfixe de sous-réseau
CONTROL_PORT_GTW	STRING [16]	MW40...47	Passerelle par défaut du port de contrôle.
ETH_BKP_PORT_IPV4	STRING [18]	MW48...56	Adresse IPv4 du port d'embase / longueur du préfixe de sous réseau.
ETH_STATUS	WORD	MW57	–
PORT_CONTROL_LINK	BOOL	MW57.0	• 0 : Liaison du port de contrôle interrompue • 1 : Liaison du port de contrôle active.
ETH_BKP_PORT_LINK	BOOL	MW57.1	• 0 : Liaison du port d'embase interrompue. • 1 : Liaison du port d'embase active.
GLOBAL_STATUS	BOOL	MW57.2	• 0 : Le module n'est pas opérationnel. • 1 : Le module est opérationnel.
NETWORK_HEALTH	BOOL	MW57.3	• 0 : Une condition de surcharge réseau est détectée. • 1 : Le réseau fonctionne normalement.
Réservé	–	MW57.4...15	–
OPCUA_STATUS	T_OPCUA_ STATUS	MW58...61	–
DATA_DICT	BYTE	MW58[0]	• 1 : Non disponible. Causes possibles : ◦ La fonctionnalité de dictionnaire de données n'est pas disponible ou activée dans l'application Control Expert et elle ne peut pas être incorporée au PAC. ◦ Le chargement ou la consultation du dictionnaire de données est en cours sur le serveur OPC UA. • 2 : Disponible, par exemple : ◦ Le chargement ou la consultation du dictionnaire de données par le serveur OPC UA a réussi. ◦ Un pré-chargement (selon les paramètres de projet du dictionnaire de données Control Expert) peut être en cours. • 4 : Occupé. • 8 : Dépassement de capacité du dictionnaire de données.
DATA_DICT_ACQ_DURATION	BYTE	MW58[1]	Durée de la dernière acquisition (0 à 255 secondes). **NOTE:** La valeur 255 indique une durée supérieure ou égale à 255 secondes.
CONNECTED_CLIENTS	BYTE	MW59[0]	Nombre de clients OPC UA connectés.

Elément	Type	Adresse	Description
DATA_DICT_PRELOAD_ DURATION	BYTE	MW59[1]	Durée du dernier préchargement du dictionnaire de données (0 à 255 secondes). **NOTE:** Vous pouvez utiliser les informations contenues dans cet élément pour ajuster et optimiser le réglage **Délai de génération effectif** dans la fenêtre de configuration **Outils > Options du projet > Général > Données intégrées de l'automate**. Pour plus d'informations sur la configuration de ce paramètre, consultez l'aide en ligne de Control Expert.
REDUNDANCY_MODE	BYTE	MW60[0]	• 0 : Aucun (Transparent) • 2 : Mode de redondance non transparent ("Warm").
SERVICE_LEVEL	BYTE	MW60[1]	Intégrité du serveur OPC UA, page 148 en fonction de la qualité des données et des services.
Réservé	WORD	MW61	–
SERVICES_STATUS	T_ SERVI-CES_ STATUS	MW62...68	–
NTP_CLIENT_SERVICE	BYTE	MW62[0]	Etat du client NTP : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée : ◦ 1 = Heure non valide (heure jamais mise à jour) ◦ 2 = Rattrapage temporel (Le temps du serveur a augmenté ou diminué d'au moins 1000 secondes. La resynchronisation du module BMENUA0100 peut prendre jusqu'à 5 minutes.) ◦ 4 = L'horloge du serveur NTP a été perdue, mais le serveur NTP est toujours joignable. Vérifiez l'état et les paramètres du serveur NTP.
NTP_SERVER_SERVICE	BYTE	MW62[1]	Etat du serveur NTP : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée (mode sécurisé uniquement) : ◦ 1 = Port de contrôle non configuré ◦ 2 = Client NTP de l'embase et du serveur activé dans les pages Web
SNMP_SERVICE	BYTE	MW63[0]	Etat du serveur SNMP : • Bit 0 : 0 = Inactif / 1 = Actif

Elément	Type	Adresse	Description
			• Bits 4 à 7 : Code d'erreur détectée : ◦ 1 = SNMP est activé en mode Secured et aucune adresse IP SNMP n'est définie dans Control Expert (0.0.0.0)
Réservé	BYTE	MW63[1]	–
WEB_SERVER	BYTE	MW64[0]	Etat du serveur Web : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée : ◦ 1 = Erreur irrécupérable détectée
FW_UPGRADE	BYTE	MW64[1]	Etat de mise à niveau du micrologiciel : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée : ◦ 1 = Package de micrologiciel non valide ou en liste noire ◦ 2 = La dernière mise à jour du micrologiciel a échoué (gérée comme une erreur détectée irrécupérable)
Réservé	BYTE	MW65[0]	–
Réservé	BYTE	MW65[1]	–
CONTROL_EXPERT_IP_ FORWARDING	BYTE	MW66[0]	Etat du transfert IP de Control Expert : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée (mode Secured uniquement) : ◦ 1 = Port de contrôle non configuré **NOTE:** Pour les modules équipés du micrologiciel version 2.01 ou supérieure, la valeur de cet élément est forcée à 0.
CPU_TO_CPU_IP_ FORWARDING	BYTE	MW66[1]	Etat du transfert de CPU à CPU : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée (mode Secured uniquement) : ◦ 1 = Port de contrôle non configuré **NOTE:** Pour les modules équipés du micrologiciel version 2.01 ou supérieure, la valeur de cet élément est forcée à 0.
IPSEC	BYTE	MW67[0]	Etat IPSEC : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée (mode Secured uniquement) : ◦ 1 = Port de contrôle non configuré

Elément	Type	Adresse	Description
Réservé	BYTE	MW67[1]	–
EVENT_LOG_SERVICE	BYTE	MW68[0]	Etat du service de journalisation des événements : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée (mode Secured uniquement) : ◦ 1 = Erreur détectée dans le service de journalisation des événements ◦ 2 = Erreur détectée dans la configuration de la journalisation des événements
LOG_SERVER_NOT_ REACHABLE	BYTE	MW68[1]	Etat du serveur de journalisation : • Bit 0 : 0 = acquittement reçu du serveur syslog / 1 = Aucun acquittement reçu du serveur syslog
FW_VERSION	T_FW_ VERSION	MW69...72	Version de micrologiciel du module.
MAJOR_VERSION	WORD	MW69	Version majeure du micrologiciel.
MINOR_VERSION	WORD	MW70	Version mineure du micrologiciel.
INTERNAL_REVISION	WORD	MW71	Révision interne du micrologiciel.
Réservé	WORD	MW72	–
CONTROL_PORT_STATUS	BYTE	MW73[0]	Etat IPv4 du port de contrôle : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée (mode Secured uniquement) : ◦ 1 = IP non valide ◦ 2 = Adresse IP en double
Réservé	BYTE	MW73[1]	–
IN_PACKETS_RATE	UINT	MW74	Nombre de paquets reçus par seconde sur toutes les interfaces Ethernet.
IN_ERROR_COUNT	UINT	MW75	Nombre de paquets entrants comportant des erreurs détectées depuis la dernière réinitialisation (modulo 65535).
OUT_PACKETS_RATE	UINT	MW76	Nombre de paquets émis par seconde sur toutes les interfaces Ethernet.
OUT_ERROR_COUNT	UINT	MW77	Nombre de paquets sortants contenant des erreurs détectées depuis la dernière réinitialisation (modulo 65535).
MEM_USED_PERCENT	BYTE	MW78[0]	Pourcentage de RAM interne utilisé par le serveur OPC UA.
CPU_USED_PERCENT	BYTE	MW78[1]	Pourcentage de CPU interne utilisé.

Elément	Type	Adresse	Description
CYBERSECURITY_STATUS	T_CYBER SECURI-TY_ STATUS	MW79...80	Etat de la cybersécurité.
SECURE_MODE	BYTE	MW79[0]	• 0 : Le module fonctionne en mode Standard. • 1 : Le module fonctionne en mode Secured.
CYBERSECURITY_STATE	BYTE	MW79[1]	Etat de cybersécurité : • 0 : Mode Secured désactivé. (Voyant SECURE éteint) • 1 : Communications sécurisées activées et exécutées sans erreur détectée. (Voyant SECURE allumé vert) • 2 : Prêt à communiquer. (Voyant SECURE vert clignotant) • 3 : Communication sécurisée en cours avec erreurs détectées mineures. (Voyant SECURE rouge clignotant) • 4 : Communication sécurisée interrompue en raison d'une erreur critique détectée. (Voyant SECURE allumé en rouge fixe)
IPSEC_CHANNELS	BYTE	MW80[0]	Nombre de voiesIPSec ouvertes.
Réservé	BYTE	MW80[1]	–

Configuration de la fonction élémentaire READ_ DDT

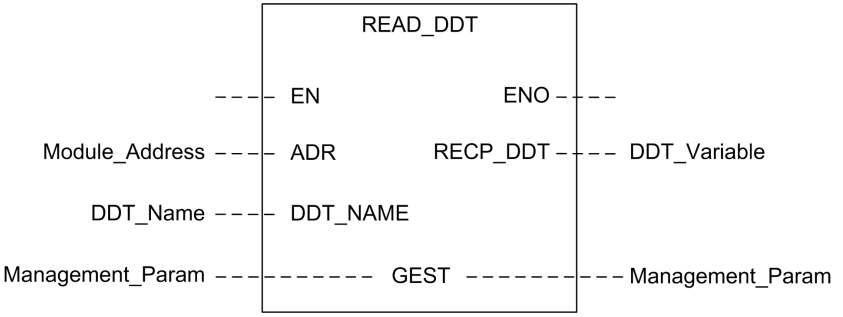
Présentation

Utilisez le bloc fonction `READ_DDT` pour configurer les messages pour le module de communication BMENUA0100.

Les paramètres `ADR`, `DDT_NAME` et `GEST` définissent l'opération.

`EN` et `ENO` peuvent être configurés en tant que paramètres supplémentaires.

Représentation en FBD



Paramètres d'entrée

Paramètre	Type de données	Description
EN	BOOL	Ce paramètre est facultatif. Lorsque la valeur un est associée à cette entrée, le bloc est activé et peut résoudre l'algorithme des blocs fonction. Lorsque la valeur zéro est associée à cette entrée, le bloc est désactivé et ne peut résoudre l'algorithme des blocs fonction.
ADR	Tout tableau de INT	Tableau contenant l'adresse de l'entité de destination de l'opération d'échange. L'adresse est le résultat de la fonction ADDMX. (Par exemple : ADDMX(0.0.3{192.168.10.2}100.TCP.MBS indique le module à l'adresse IP 192.168.10.2 correspondant à l'ID d'unité 100 (serveur local du module) et connecté au port Ethernet intégré.)
DDT_NAME	STRING	Nom du DDT à lire : T_BMENUA0100

Paramètres d'entrée/sortie

Le tableau GEST est local :

<table>
<tr><th>Para-mètre</th><th>Type de données</th><th colspan="3">Description</th></tr>
<tr><td rowspan="3">GEST</td><td rowspan="3">Array [0...3] of INT</td><td colspan="3">Paramètres de gestion, composés de quatre mots. Pour plus d'informations sur ces paramètres, consultez la rubrique d'aide de Control Expert Structure des paramètres de gestion (voir ™EcoStruxure Control Expert - Communication - Bibliothèque de blocs).</td></tr>
<tr><td>Mot#</td><td>Octet de poids fort</td><td>Octet de poids faible</td></tr>
<tr><td>0</td><td>Numéro de l'échange</td><td>Bit d'activité : rang 0
Bit d'annulation : rang 1</td></tr>
</table>

Para-mètre	Type de données	Description		
				Bit de données immédiat : rang 2
		1	Rapport d'opération (voir ™*EcoStruxure Control Expert - Communication - Bibliothèque de blocs*)	Rapport de communication (voir ™*EcoStruxure Control Expert - Communication - Bibliothèque de blocs*)
		2	Timeout (voir ™*EcoStruxure Control Expert - Communication - Bibliothèque de blocs*)	
		3	Longueur (voir ™*EcoStruxure Control Expert - Communication - Bibliothèque de blocs*)	

Paramètres de sortie

Paramètre	Type de données	Description
ENO	BOOL	Ce paramètre est facultatif. Lorsque vous sélectionnez cette sortie, vous obtenez également l'entrée EN. La sortie ENO est activée lorsque l'exécution du bloc fonction aboutit.
RECP_DDT	Quelconque	Mémoire tampon de réception. Une variable DDT peut être utilisée. Consultez la description du DDT de T_BMENUA0100, page 136 pour connaître le contenu de ce DDT. la taille des données reçues (en octets) est automatiquement écrite par le système dans le quatrième mot de la table de gestion.

Bloc fonction de communication asynchrone

Dans une application à redondance d'UC, pendant un événement de basculement, le bloc fonction de communication asynchrone READ_DDT ne recommence pas automatiquement à fonctionner sur le nouveau PAC primaire, sauf s'il est configuré de la manière spécifique décrite ci-après.

Procédez comme suit pour permettre aux EFB de communication asynchrone de fonctionner à nouveau automatiquement après un basculement :

- Programmez votre application afin que toutes les instances EFB ne soient pas échangées avec le PAC redondant. Pour cela, désélectionnez l'attribut **Echange sur l'automate redondant** de l'instance EFB.

Remarques relatives à la configuration de la fonction

Lors de l'utilisation de la fonction élémentaire (EF) READ_DDT, notez bien :

- Si votre application utilise plus d'un module BMENUA0100 dans un même rack, configurez une instance distincte de tableau d'éléments WORD pour chaque broche GEST. Chaque bloc gère son propre tableau de types WORD.
- Il n'est pas nécessaire de définir une valeur pour le paramètre de longueur dans GEST [3], car il n'y a aucune donnée à envoyer. A la fin de l'opération (lorsque le bit d'activité dans GEST[0] est défini sur 0), la longueur est définie avec la longueur des données copiées dans le paramètre de sortie RECP_DDT si aucune erreur détectée est signalée dans GEST[1] ou avec un code d'état supplémentaire. Reportez-vous à la rubrique d'aide de Control Expert *Codes d'erreur des EFB avec paramètre STATUS* (voir ™*EcoStruxure Control Expert - Communication - Bibliothèque de blocs*) pour une description de ces valeurs de code d'état supplémentaires.
- Si le délai est égal à 0 indique une période d'attente illimitée. Dans ce cas, le délai ou la perte de communication qui se produit durant l'opération d'échange n'est pas détecté. Durant cette période d'attente illimitée, le paramètre RECP_DDT conserve sa valeur précédente. Pour éviter ce scénario, définissez le délai à une valeur différente de zéro.
- En cas de rapport d'opération 16#01 (requête non traitée) ou 16#02 (réponse incorrecte) dans le mot GEST[1] du tableau de gestion, un code d'état supplémentaire peut être signalé dans le paramètre de longueur (GEST[3]). Les codes d'état renvoyés dans ce champ correspond à une sous-plage de codes STATUS possibles de EFB de communication. Les valeurs possibles pour READ_DDT sont 0x30ss et 0x4001. Reportez-vous à la rubrique d'aide de Control Expert *Codes d'erreur des EFB avec paramètre STATUS* (voir ™*EcoStruxure Control Expert - Communication - Bibliothèque de blocs*) pour une description de ces valeurs de code d'état supplémentaires.
- En fonction du DDT défini dans le paramètre DDT_NAME, certaines vérifications de cohérence sont exécutées sur les données reçues. En cas de détection de divergence, le code 16#02 (réponse incorrecte) est défini dans l'octet de rapport d'opération (octet de poids fort GEST[1]). Notez que le bloc ne vérifie pas la validité du type de données de la variable configurée comme mémoire tampon de réception (RECP_DDT). Vérifiez que le type de données de la variable liée au paramètre RECP_DDT correspond au type de données reçues.

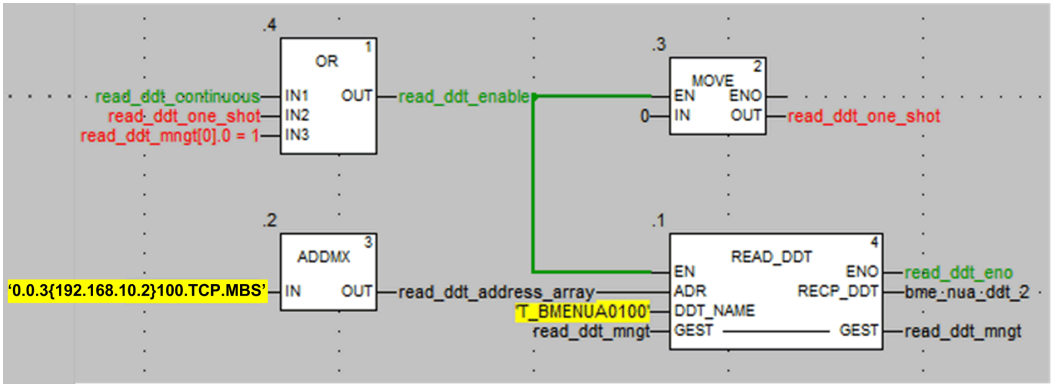
⚠ATTENTION
FONCTIONNEMENT IMPRÉVU DE L'APPLICATION • Vérifiez que la variable de type DDT associée au paramètre de sortie RECP_DDT correspond au type de données écrites dans la mémoire tampon de réception. • Vérifiez que l'adresse définie dans le paramètre ADR correspond au module approprié, en particulier si plusieurs modules identiques sont configurés sur le même réseau. **Le non-respect de ces instructions peut provoquer des blessures ou des dommages matériels.**

Configuration de la fonction élémentaire READ_DDT

Pour configurer la fonction élémentaire READ_DDT, suivez ces étapes :

Étape	Action
1	Définissez l'adresse de l'équipement de destination dans ADR (utilisez un bloc ADDM pour définir cette adresse dans un format de chaîne explicite).
2	Définissez le paramètre DDT_NAME avec le nom du DDT à lire.
3	Appelez la fonction READ_DDT pour lancer la communication (avec la broche d'entrée EN définie sur 1 si elle est configurée).
4	Surveillez ce bit d'activité (octet de poids faible du paramètre GEST[0]) jusqu'à la fin de la communication (le bit d'activité est défini sur 0 par le système lorsque la communication est terminée). Exécutez une seule fois cette fonction pour éviter d'effacer les valeurs d'état. Par exemple, si la broche EN est définie sur 0 durant l'opération, la fonction est appelée à nouveau.
5	Consultez les paramètres de rapport dans GEST[1]. Si le rapport indique 16#0000, alors la mémoire tampon RECP_DDT est remplie de données reçues. La taille des données reçues (en octets) est écrite dans le quatrième mot (GEST[3]) de la table de gestion.

Exemple de fonction élémentaire (EF) READ_DDT



Dans cet exemple, la fonction élémentaire READ_DDT peut être lancée :

- En continu, en définissant la variable read_ddt_continuous.

  NOTE: En cas de détection d'erreur, les codes de rapport dans le deuxième mot de la variable read_ddt_mngt ne peuvent pas être lu.

- Une seule fois, en définissant la variable read_ddt_one_shot.

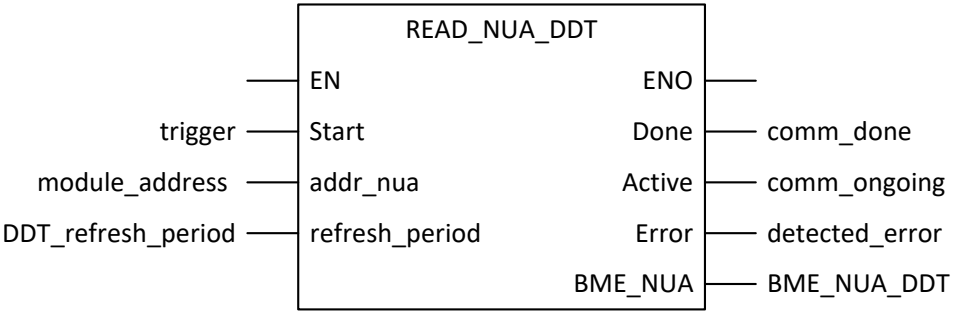
Configuration de la fonction élémentaire READ_NUA_DDT

Le bloc fonction `READ_NUA_DDT` permet d'accéder aux informations de diagnostic du module BMENUA0100.

Les paramètres d'entrée `Start`, `addr_nua` et `refresh_period` définissent l'opération.

EN et ENO peuvent être configurés comme paramètres supplémentaires.

Représentation en FBD



Paramètres d'entrée

Paramètre	Type de données	Description
EN	BOOL	Ce paramètre est facultatif. Lorsque la valeur un est associée à cette entrée, le bloc est activé et peut résoudre l'algorithme des blocs fonction. Lorsque la valeur zéro est associée à cette entrée, le bloc est désactivé et ne peut résoudre l'algorithme des blocs fonction.
Start	BOOL	La lecture du DDT BMENUA0100 est continue.
addr_nua	string[32]	Adresse du module BMENUA0100 transmise à ADDMX() pour lecture. Chaîne de longueur fixe contenant l'adresse du BMENUA0100 de destination. L'adresse est le résultat de la fonction ADDMX. (Par exemple : ADDMX(0.0.3{192.168.10.2}100.TCP.MBS indique le module à l'adresse IP 192.168.10.2 correspondant à l'ID d'unité 100 (serveur local du module) et connecté au port Ethernet intégré.)
refresh_period	TIME	Période d'actualisation du DDT.

Paramètres de sortie

Paramètre	Type de données	Description
ENO	BOOL	Ce paramètre est facultatif. Lorsque vous sélectionnez cette sortie, vous obtenez également l'entrée EN. La sortie ENO est activée lorsque l'exécution du bloc fonction aboutit.
Done	BOOL	La communication est terminée.
Active	BOOL	Communication en cours.

Paramètre	Type de données	Description
Error	BOOL	Erreur détectée sur le FB de communication.
BME_NUA	T_BMENUA0100	DDT, page 136 BMENUA0100 qui peut être utilisé tel quel.

Diagnostics OPC UA

Introduction

Le module BMENUA0100 présente à la fois des variables de serveur OPC UA et des éléments de données spécifiques qui peuvent être utilisés pour identifier l'application exécutée dans le module et pour diagnostiquer les opérations du module.

Variable OPC UA SERVICE_LEVEL

La variable SERVICE_LEVEL fournit à un client des informations relatives à l'état de la CPU et à l'intégrité du serveur OPC UA. La variable SERVICE_LEVEL est directement accessible dans l'arborescence du serveur OPC UA. La variable SERVICE_LEVEL est dupliquée dans l'élément OPCUA_STATUS.SERVICE_LEVEL du DDT, page 136 du module BMENUA0100, et elle est accessible par programme en exécutant la fonction élémentaire READ_DDT, page 141 lorsque l'application est à l'état RUN.

NOTE: Dans les architectures redondantes, le client OPC UA a besoin de surveiller la variable SERVICE_LEVEL des modules BMENUA0100 primaire et redondant pour gérer le mécanisme de redondance. Lorsque le client détecte que la valeur de SERVICE_LEVEL du module redondant est supérieure à celle du module primaire, le client doit déclencher un basculement du module primaire vers le module redondant.

Les variables de niveau de service suivantes s'appliquent à toutes les versions de micrologiciel du BMENUA0100, sauf indication contraire :

Valeur SERVICE_LEVEL	Etat de la CPU ou du serveur OPC UA	
	Micrologiciel = V1.0	Micrologiciel ≥ V1.1
0	BMENUA0100 est dans la phase d'amorçage. L'UC est à l'état NOCONF ou ERROR. Exemple d'état ERROR : La tâche MAST est à l'état HALT.	
1	Le serveur OPC UA a démarré. La consultation de la liste du dictionnaire de données est en cours.	
5	La consultation du dictionnaire de données a démarré.	

Valeur SERVICE_LEVEL	Etat de la CPU ou du serveur OPC UA	
	Micrologiciel = V1.0	**Micrologiciel ≥ V1.1**
10	Dépassement de la taille du dictionnaire de données.	
20	La consultation des types de dictionnaire de données est en cours.	
50	La consultation des variables du dictionnaire de données est en cours.	
100	La consultation du dictionnaire de données est terminée. La lecture de l'état de l'UC est en cours. L'espace d'adressage sera mis à jour avec le nouveau contenu du dictionnaire de données.	
120[1]	UC à l'état STOP.	UC à l'état STOP STANDBY ou HALT STANDBY (UC redondante uniquement).
150[1]	UC à l'état WAIT STANDBY (UC redondante uniquement).	
199[1]	UC à l'état RUN STANDBY (UC redondante uniquement).	
202[2]	<Non applicable>	Standalone_CPU uniquement : UC à l'état STOP STANDALONE. UC redondante uniquement: Lorsque les deux UC sont à l'état STOP ou HALT, un seul module BMENUA0100 est déclaré comme maître avec un niveau de service égal à 202. L'espace d'adressage est correct et utilisable.
255	UC à l'état RUN (ou RUN PRIMARY pour UC redondante). Le serveur OPC UA est totalement opérationnel	

1. Il n'est pas nécessaire de définir cette valeur avant que le serveur soit opérationnel.

2. Ce niveau de service ne s'applique qu'au micrologiciel BMENUA0100 de version V1.10 ou supérieure.

NOTE: Plus la taille du dictionnaire de données est élevée, plus le temps d'acquisition du dictionnaire de données est long (le temps nécessaire au module pour parcourir et charger le dictionnaire de données). Durant l'acquisition du dictionnaire de données, SERVICE_LEVEL reste à la valeur 100 jusqu'à la fin de l'acquisition. En cas de changement de build dans Control Expert qui génère un nouveau dictionnaire de données, le serveur OPC UA redémarre le processus de consultation du dictionnaire de données. Durant ce processus, les mises à jour des éléments en cours de surveillance peuvent être interrompues, avec des valeurs figées à leur plus récente mise à jour.

Variables de serveur OPC UA

Vous pouvez afficher ces variables en ligne en utilisant un équipement client OPC UA, par exemple l'outil UaExpert (Unified Automation). Dans l'arborescence du serveur OPC UA,

sélectionnez **Etat du serveur > Informations de génération** pour afficher les variables suivantes du serveur OPC UA :

Variable	Description
BuildDate	Date de compilation de l'application dans le PAC.
BuildNumber	Numéro de la compilation de l'application du PAC.
ManufacturerName	Toujours "Schneider Electric".
Nom du produit	Toujours "BMENUA0100".
ProductUri	Identifiant URI unique attribué au module.
SoftwareVersion	La version en cours du micrologiciel du module.

Elements de données spécifiques à OPC UA

Le module BMENUA0100 prend en charge les éléments de données spécifiques suivants : Ces éléments de données sont accessibles via la pile du serveur OPC UA. Même s'ils sont similaires aux éléments de données du PAC accessibles via le logiciel Control Expert, ces éléments de données spécifiques ne sont pas reliés aux symboles du PAC et ne sont pas accessibles via le logiciel Control Expert :

DataItem	Type de données	Valeur par défaut	Description
#AddressSpaceState	INT16	0	Etat de l'espace d'adressage, avec son ensemble d'objets et de noeuds. Les valeurs possibles sont les suivantes : **0.** Vide **1.** Généré **2.** Mise à jour en cours **3.** Généré partiellement (l'application ne contient aucun dictionnaire de données ou le débordement du dictionnaire de données)
#ApplicationName	STRING	0	Nom de l'application du PAC.
#ApplicationVersion	STRING	0	Version de l'application du PAC.
#CurrentDataDictionaryItemsCount	INT32	0	Nombre d'éléments du dictionnaire de données qui ont été chargés dans le serveur.
#CurrentMonitoredItemsCount	INT32	0	Nombre d'éléments actuellement surveillés par le serveur.
#DeviceIdentity	STRING	0	Référence de la CPU.

DataItem	Type de données	Valeur par défaut	Description
#PLCDatadicReady	BYTE	1	Surveillance de l'état de chargement du dictionnaire de données du PAC : 1. Le dictionnaire de données du PAC n'est pas disponible. Explications possibles : • La fonctionnalité de dictionnaire de données n'est pas disponible ou activée dans l'application Control Expert, elle ne peut être intégrée au PAC. • Le chargement ou la consultation du dictionnaire de données est en cours sur le serveur OPC UA. 2. Le dictionnaire de données du PAC est disponible, par exemple : • Le chargement ou la consultation du dictionnaire de données par le serveur OPC UA a réussi. • Un pré-chargement (selon les paramètres de projet du dictionnaire de données Control Expert) peut être en cours.
#PLCQualStatus	INT16	0	Surveillance de l'état de communication d'un PAC. Valeurs (hex) possibles : • 0x00C0 : La communication avec le PAC est correcte. • 0x0040 : Aucune communication avec le PAC pendant une durée inférieure à la temporisation de l'équipement (5 s). • 0x0 : Le PAC n'est pas identifié.

DataItem	Type de données	Valeur par défaut	Description
#TSEventItemsReady	BOOL	0	Elément en lecture seule qui indique si les variables horodatées à la source et les équipements d'horodatage à la source ont été explorés dans l'application ePAC M580 : • 0 = non exploré • 1 = exploré **NOTE:** Cet élément n'est pertinent que si l'horodatage est activé dans Control Expert et activé pour le module BMENUA0100 considéré.
#TSEventSynchro	BOOL	0	Elément en lecture-écriture qui, lorsqu'il est activé, envoie une valeur synchronisée à l'ensemble des équipements d'horodatage à la source connectés à l'ePAC M580, chaque fois qu'une opération d'écriture est effectuée. L'objectif est d'initialiser tous les éléments surveillés horodatés à leurs valeurs actuelles. • 0 = en attente d'activation • 1 = activé **NOTE:** • La valeur affichée sera toujours 0. La valeur 1 n'est jamais visible car elle n'existe que fugitivement et revient à la valeur 0 d'attente d'activation. • Cet élément n'est pertinent que si l'horodatage est activé dans Control Expert et activé pour le module BMENUA0100 considéré.

Syslog

Introduction

Le module BMENUA0100 consigne les événements dans la mémoire tampon locale de diagnostics, puis envoie les événements à un serveur syslog distant où ils sont stockés et mis à disposition des clients syslog. Pour diagnostiquer les événements plus anciens, vous pouvez interroger les événements enregistrés par le serveur syslog. Pour les événements en cours du module, vous pouvez utiliser les pages Web du module, page 155 pour diagnostiquer l'état du service syslog et afficher les événements spécifiques dans la mémoire tampon de diagnostic.

La mémoire tampon locale fonctionne de façon circulaire : les événements les plus récents remplacent les événements les plus anciens lorsque la mémoire tampon est remplie.

Le module stocke les événements dans la mémoire volatile.

Les événements journalisés concernent soit :

- Sécurité/Autorisation, page 154

  – ou –

- Modifications majeures sur le système (audit), page 155

Le service syslog est configurable sur les pages Web, page 93 dans le cadre de la configuration de la cybersécurité, par conséquent il peut être actif uniquement si le module fonctionne en mode Secured. Lorsque le module fonctionne en mode Standard, le service est désactivé.

Comme il est implémenté dans le module BMENUA0100, le service Syslog est pris en charge par IPv4 (version 1.0 ou supérieure du micrologiciel) et IPv6 (version 1.10 ou supérieure du micrologiciel).

NOTE: Syslog n'est pas un protocole sécurisé, il doit être encapsulé dans un canal IPSEC, page 100 sécurisé sur le port de contrôle.

Structure des messages Syslog

Le protocole syslog (RFC 5424) définit la manière dont les événements sont échangés entre le module et le serveur distant. La structure des messages syslog est définie ci-dessous :

Champ	Description
PRI	Informations sur la catégorie et la gravité (description fournie dans les tableaux suivants).
VERSION	Version de la spécification du protocole Syslog (Version = 1 pour RFC 5424).
TIMESTAMP	Le format d'horodatage est défini par la RFC 3339 qui recommande le format de date et d'heure Internet ISO8601 suivant : YYY-MM-DD**T**hh:mm:ss.nnn**Z** **NOTE: -**, **T**, **:**, **.** et **Z** sont des caractères obligatoires et font partie du champ TIMESTAMP. **T** et **Z** doivent figurer en majuscules. **Z** spécifie que l'heure est au format UTC. Description du contenu du champ d'horodatage :

YYY	Année
MM	Mois
DD	Jour
hh	Heure
mm	Mois
ss	Seconde
nnn	Fraction de seconde en milliseconde (0 si non disponible)

Champ	Description
HOSTNAME	Identifie la machine ayant envoyé le message Syslog : nom de domaine complet (FQDN) ou adresse IP statique source, si FQDN n'est pas pris en charge.
APP-NAME	Identifie l'application qui crée le message Syslog. Il contient des informations qui permettent d'identifier l'entité émettrice du message (par exemple, un sous-ensemble d'une référence commerciale).
PROCID	Identifie le processus, l'entité ou le composant qui envoie l'événement. Reçoit la valeur NILVALUE s'il n'est pas utilisé.
MSGID	Identifie le type de message auquel l'événement est lié, par exemple HTTP, FTP, Modbus. Reçoit la valeur NILVALUE s'il n'est pas utilisé.
MESSAGE TEXT	Ce champ contient plusieurs informations : • Adresse de l'émetteur : Adresse IP de l'entité qui génère le journal. • ID d'homologue : ID d'homologue si un homologue est impliqué dans l'opération (par exemple, nom d'utilisateur pour une opération de journalisation). Reçoit la valeur Null s'il n'est pas utilisé. • Adresse de l'homologue : Adresse IP de l'homologue si un homologue est impliqué dans l'opération. Reçoit la valeur Null s'il n'est pas utilisé. • Type : Numéro unique pour identifier un message (description fournie dans les tableaux suivants). • Commentaire : Chaîne décrivant le message (description fournie dans les tableaux suivants).

Evénements de type Sécurité/Autorisation

- Echec d'ouverture de canal sécurisé depuis la pile OPC UA : certificat non valide, certificat expiré...
- Sessions utilisateurs ouvertes (Nom d'utilisateur/Mot de passe) depuis la pile OPC UA (connexion réussie)

  NOTE: En l'absence de connexion (mode Standard), le journal est désactivé et donc aucune entrée consignant la réussite de la connexion n'est créée.
- Echecs de session utilisateur (Nom d'utilisateur/Mot de passe) depuis la pile OPC UA (échec de connexion)

  NOTE: En l'absence de connexion (mode Standard), le journal est désactivé, aucune entrée de consignation d'échec de connexion n'est créée.
- Connexions HTTPS établies avec ou par un outil (connexion réussie) : par exemple, une connexion au serveur Web ou téléchargement de micrologiciel via HTTPS.
- Echec de connexion HTTPS avec ou par un outil : par exemple, échec de connexion au serveur Web ou échec de téléchargement de micrologiciel via HTTPS.

- Fermeture de session utilisateur (déconnexion demandée) pour HTTPS.
- Fermeture de session utilisateur (déconnexion demandée) pour OPC UA.
- Déconnexion automatique : par exemple, expiration du délai d'inactivité pour OPC UA ou HTTPS.
- Détection d'erreur d'intégrité : par exemple, détection d'erreur de signature numérique ou uniquement erreur d'intégrité (hachage).
- Création de nouveau certificat.
- Suppression de certificats locaux. Cela est effectué avec le commutateur rotatif en sélectionnant le mode de fonctionnement Security Reset.
- Ajout d'un nouveau certificat client de la liste blanche sur l'équipement.
- Suppression d'un nouveau certificat client de la liste blanche sur l'équipement.

Evénements relatifs à modifications majeures sur le système (audit)

- Téléchargement de configuration de cybersécurité ou application sur l'équipement.
- Téléchargement de micrologiciel sur l'équipement.
- Divergence de signature du micrologiciel, dont le téléchargement a échoué sur l'équipement.

Diagnostic des pages Web Syslog

Utilisez les pages Web du module pour diagnostiquer l'état du service syslog exécuté sur le module, et diagnostiquer les zones spécifiques de la mémoire tampon de diagnostic syslog. Vous vous également utiliser l'élément SERVICES_STATUS du DDT, page 136 du module pour consulter l'état du service syslog.

Dans le menu **Diagnostics > Event log diagnostic**, utilisez les commandes suivantes pour consulter l'état du service du module :

Paramètre	Description
Statut	• Opérationnel : Lorsque le module fonctionne en mode Secured, et le service syslog est activé. • Non opérationnel : lorsque le module fonctionne en mode Secured, et le service syslog est désactivé.
Serveur de consignation	• Joignable : une connexion est établie avec le serveur syslog distant. • Non joignable : impossible d'établir la connexion avec le serveur syslog distant.

Dans le menu **Diagnostics > Diagnostic via le journal d'événements**, dans le champ **Mémoire tampon de diagnostic à lire**, entrez la zone de mémoire tampon à lire.

Diagnostics Modbus

Introduction

Vous pouvez utiliser les commandes de code fonction Modbus pour effectuer des diagnostics sur le module BMENUA0100. Le module peut recevoir les commandes Modbus uniquement via son port d'embase. Le protocole Modbus n'étant pas sécurisé, vous devez encapsuler les commandes Modbus dans IPSEC.

Seules les requêtes FC43/14 (lecture de l'identification de l'équipement) et FC03 (lecture de MW% DDT) sont prises en charge sur le module BMENUA0100.

Accès aux données Modbus et mode de fonctionnement de la cybersécurité

La méthode d'accès aux données Modbus dépend du mode de fonctionnement de la cybersécurité. Si le module BMENUA0100 fonctionne en :

- Mode Standard : Le module BMENUA0100 accepte le flux de données du client Modbus TCP/IP en provenance de tout client pouvant accéder au réseau Ethernet de l'embase. Utilisez les méthodes de communication Modbus standard, notamment les blocs fonction DATA_EXCH, MBP_MSTR, READ_VAR et WRITE_VAR et les commandes Control Expert.
- Mode Secured : Le module BMENUA0100 accepte le flux de données du client Modbus TCP/IP en provenance de la CPU M580 uniquement. Vous pouvez implémenter le bloc DATA_EXCH dans l'application. Les blocs fonction READ_VAR et WRITE_VAR peuvent également être utilisés.

  NOTE: Pour adresser le serveur Modbus dans le module, UnitID 100 doit être utilisé. Reportez-vous à la documentation de votre client Modbus pour plus d'informations sur la configuration de cette valeur. Par exemple, lorsque vous utilisez le bloc DATA_EXCH, UnitId peut être défini avec ADDMX comme suit : ADDMX(0.0.3{192.168.10.2}100.TCP.MBS), où 192.168.168.10.2 est l'adresse IP d'embase du module BMENUA0100.

43/14 : Lecture de l'identification de l'équipement

Les données d'identification d'équipements suivantes peuvent être obtenues avec le code 43 / sous-code 14 :

Catégorie	ID de l'objet	Nom de l'objet	Type
Basic	0x00	Nom du fournisseur	Chaîne ASCII
	0x01	Code produit	Chaîne ASCII
	0x02	Révision majeure/mineure	Chaîne ASCII
Regular	0x03	URL fournisseur	Chaîne ASCII
	0x04	Nom du produit	Chaîne ASCII
	0x05	Nom du modèle	Chaîne ASCII
	0x06	Nom de l'application utilisateur	Chaîne ASCII
	0x07...0xFF	Réservé	Chaîne ASCII

Diagnostics SNMP

Introduction

Lorsque l'agent SNMP est configuré, page 127, le module BMENUA0100 active les diagnostics SNMP dans le réseau Ethernet TCP/IP avec la prise en charge des bases MIB suivantes :

- MIB-II
- MIB LLDP (Link Layer Discovery Protocol)

MIB-II

MIB-II fournit un gestionnaire SNMP et un ensemble de variables de gestion d'équipements. La lecture de ces variables permet à un gestionnaire SNMP de diagnostiquer le fonctionnement d'un équipement spécifique, tel que BMENUA0100.

MIB LLDP

La base MIB LLDP contient des données collectées via le protocole de découverte de la couche de liaison relative à l'identité, les capacités et l'emplacement du réseau Ethernet. L'utilisation de la base MIB LLDP permet à un gestionnaire SNMP de détecter la topologie du réseau et les capacités des équipements du réseau.

NOTE: La communication SNMP des données MIB LLDP circule exclusivement via le port d'embase.

Page Web Diagnostics OPC UA

Utilisez la page Web **Diagnostics OPC UA** pour consulter les données dynamiques décrivant le fonctionnement du serveur OPC UA intégré au module BMENUA0100.

NOTE: La page Web **Diagnostics OPC UA** est actualisée toutes les 5 secondes.

Données de diagnostic

La page Web **Diagnostics OPC UA** affiche les données suivantes, accessibles en lecture seule. Notez que toutes les valeurs numériques sont au format décimal :

Champ	Description
Diagnostic automate	
EPAC	Adresse IP UC
Identité de l'équipement	Numéro de série de l'UC.
Version de l'équipement	Version du micrologiciel de l'UC.
Etat de l'équipement	Etat de la connexion avec l'UC : bon, mauvais, incertain, inconnu, manquant.
Délai d'attente (en ms)	Durée maximale pendant laquelle le serveur OPC UA attend une réponse de l'équipement après l'envoi d'une requête. Par exemple : 1000.
Nombre maximal de canaux	Nombre de connexions ouvertes par le serveur OPC UA sur l'UC.
Voies utilisées à d'autres fins que l'horodatage	Nombre de connexions transportant des données d'application.
Voies utilisées pour l'horodatage	Nombre de connexions transportant des données d'horodatage, page 121.
Longueur de requête	Longueur de la communication avec l'UC.
Nom de l'application (équipement)	Nom du projet Control Expert.

Champ	Description
Version de l'application (équipement)	Somme de contrôle (checksum) et signatures de l'application.
Préchargement du dictionnaire de données	Disponible ou non disponible pour l'application du PAC.
Etat d'horodatage	Affiche l'état de l'horodatage : • L'horodatage est activé avec accès aux variables horodatées dans l'application. • L'horodatage n'est PAS activé, AUCUN accès aux variables horodatées.
Liste des équipements avec horodatage à la source configuré	Si l'horodatage est activé, une liste d'équipements s'affiche et indique pour chaque équipement : • Nombre de voies dédiées réservées à l'interrogation de la source d'événements d'horodatage. • Type d'équipement (CRA, CPU, etc.). • Adresse IPv4. • Réservation du tampon d'horodatage d'équipement par le serveur OPC UA intégré au BMENUA0100 : vrai ou faux
Diagnostic OPC UA	
URL de point de terminaison (IPV4)	Adresse IPv4 du serveur OPC UA, dans le format suivant : "opc.tcp://<adresse IPv4>:<numéro de port>". Par exemple : opc.tcp://192.168.2.142:4840
Taux d'échantillonnage rapide	Indique si l'option Taux d'échantillonnage rapide est sélectionnée, page 116 : • True (vrai) = sélectionné • False (faux) = non sélectionné
Nombre de sessions connectées	Nombre total de sessions client prises en charge par le serveur OPC UA intégré au module BMENUA0100.
Informations de souscription :	Informations décrivant les variables surveillées par le serveur OPC UA qui sont incluses dans une ou plusieurs souscriptions.
Nombre d'éléments surveillés depuis le noeud Serveur interne :	
Nombre d'éléments surveillés spécifiques :	
Nombre d'éléments surveillés non spécifiques :	
Nombre d'éléments surveillés horodatés avec mode de surveillance non désactivé :	
Nombre total d'éléments surveillés :	

Champ	Description
Nombre actuel de temporisateurs	Nombre d'intervalles d'échantillonnage configurés pour le serveur OPC UA intégré au module BMENUA0100 :
Liste de temporisateurs	Liste décrivant chaque intervalle d'échantillonnage (temporisateur) surveillé par le serveur OPC UA intégré du BMENUA0100. Chaque élément indique : • L'intervalle d'échantillonnage en ms. • Le nombre d'éléments surveillés. • Le nombre de requêtes générées lors de la plus récente exécution.

Optimisation des performances du BMENUA0100

Optimisation des performances du BMENUA0100

Introduction

Lors de l'optimisation des performances de BMENUA0100, considérez le système dans son ensemble. Notamment, analysez l'efficacité globale des communications et la charge dans l'architecture réseau incluant les modules BMENUA0100. Dans ce contexte, l'optimisation des performances du client OPC UA influence également l'efficacité des communications OPC UA.

Plusieurs paramètres, à différents niveaux de l'architecture, peuvent améliorer les performances du système ou la stabilité du système et sa robustesse à chaque étape des modes de fonctionnement (connexions, navigation, souscription, surveillance, etc.).

NOTE:

- Schneider Electric recommande d'ajouter les éléments par paquets ne dépassant pas 2000 unités. L'intervalle d'échantillonnage configuré n'est pertinent que s'il est supérieur ou égal au temps de scrutation MAST du PAC.
- Schneider Electric recommande de définir CallTimeout sur une valeur supérieure ou égale à 10 secondes dans le client OPC UA.
- Le réglage de General.SecureChannelLifetime pour la communication avec un client OPC UA est défini par défaut sur 3 600 000 ms (1 heure). Schneider Electric recommande d'utiliser ce réglage par défaut, car une valeur très faible (par exemple, 30 secondes) peut avoir un impact négatif sur les performances.
- Les performances du système dépendent fortement de la configuration (nombre de clients connectés, nombre de variables gérées, etc.).
- Par exemple, avec 2000 éléments surveillés, la fréquence d'actualisation de 20 ms ne peut être atteinte que si 500 éléments au maximum changent de valeur entre deux publications consécutives.

Exemple de performances

Un client OPC UA peut surveiller jusqu'à 20 000 éléments en mode de cybersécurité Standard.

Exemple basé sur :

- BMEP584040 avec un temps de cycle de tâche MAST à 20 ms (charge UC inférieure à 80 %).
- BMENUA0100 avec sélecteur rotatif en position Standard (communication non sécurisée, pas de voie IPSec).
- Le client OPC UA (UAExpert) établit la communication avec le mode de sécurité des messages défini sur **Aucun** et surveille 20 000 éléments par rapport aux variables d'un tableau de types INT à partir du serveur OPC UA d'un module BMENUA0100. Ce serveur est configuré avec un intervalle de publication de 1 seconde, un intervalle d'échantillonnage de 1 seconde et une temporisation de session de 30 secondes.
- Aucune autre communication que OPC UA.

Comment régler les performances

Structure d'échange de données

La mémoire de l'application de données de l'UC est organisée en fonction de la définition de l'application de données dans Control Expert. Plus la déclaration de la variable est structurée, plus le serveur BMENUA0100 génère des requêtes optimisées pour l'accès aux variables et au dictionnaire de données durant l'exécution.

Pour les variables accessibles pour le client OPC UA, voici des recommandations :

- Utilisez des tableaux ou structure de données autant que possible.
- Activez l'option **Variable IHM uniquement** dans **Données intégrées de l'automate** (vue **Options du projet**) et définissez uniquement les variables avec l'attribut **IHM** pour réduire la taille du dictionnaire de données.
- Dans le processus de sécurité de l'UC, pour réduire la taille du dictionnaire de données, désélectionnez l'option **Utilisation de l'espace de nom de processus** dans **Options du projet > Général > Données intégrées de l'automate > Dictionnaire de données**.

Capacités de communication de l'UC

La capacité du système de communication dépend du modèle d'UC M580 et de certains paramètres de configuration. Le modèle d'UC détermine les aspects suivants :

- Performances de traitement UC sur le système.
- Nombre de requêtes par cycle pouvant être traitées, même si configurable par mot système %SW90.
- Nombre maximal de canaux disponibles pour chaque BMENUA0100 pour l'établissement de connexions à l'UC M580, page 170.

En outre, plus le temps de cycle MAST est réduit, plus le nombre de requêtes de communication pouvant être traitées est élevé. Ainsi le niveau de performances dépend directement du temps de cycle MAST.

Client OPC UA, configuration et utilisation

Le nombre de variables surveillées a un impact sur les performances. Les fréquences d'échantillonnage et intervalles de publication configurés pour chaque client OPC UA détermine le nombre de requêtes nécessaires pour animer les variables. Notez que lorsque plusieurs clients OPC UA sont connectés au même serveur OPC UA BMENUA0100, si les fréquences d'échantillonnage et les intervalles de publication sont différentes pour chaque client OPC UA, cette configuration génère davantage de requêtes.

Toutes les valeurs de délai configurables du client OPC UA (navigation, connexion, publication, session, chien de garde…) doivent être réglées pour optimiser et stabiliser, autant que possible, l'ensemble du système. Ces délais peuvent à leur tour affecter les performances du système.

Selon le mode de sécurité des messages (mode de sécurité des messages : aucun, signature, signature et chiffrement), l'algorithme de traitement de la signature et du chiffrement requiert du temps supplémentaire.

Communications UC vers UC et Control Expert vers CPU

Chaque tunnel IPSec utilisé pour sécuriser les communications autres que OPC UA ou HTTPS ralentit le trafic, en particulier si la **Confidentialité** est activée, ce qui active le chiffrement et le déchiffrement.

Comment surveiller les performances

Vous pouvez surveiller les performances de plusieurs façons.

Avec Control Expert

En utilisant Control Expert en mode connecté, vous pouvez accéder au temps de cycle MAST effectif et à la charge de l'UC M580 sur le système, pour chaque tâche et pour la totalité des tâches par la lecture des mots système %SW110 à %SW116. De plus, le DDDT de l'UC M580 et le DDT de BMENUA0100 peuvent fournir différentes informations de diagnostic relatives aux performances du système du PAC, par exemple :

- Niveau de service du serveur OPC UA.
- Nombre de clients OPC UA connectés.
- Etat du dictionnaire de données, temps d'acquisition, durée de préchargement.
- Etat du service Ethernet.
- Intégrité du réseau.
- Etat du port de contrôle et du port d'embase.
- Nombre de paquets Ethernet par seconde.
- Nombre de paquets Ethernet contenant des erreurs détectées.

- Pourcentage de charge UC BMENUA0100 et de mémoire utilisée.
- Nombre de canaux IPSec ouverts.

Via le site Web BMENUA0100

La page d'accueil et la page de diagnostics du site Web BMENUA0100 fournissent des informations pertinentes relatives aux performances des serveurs OPC UA. Certaines informations sont issues du DDT de BMENUA0100, et d'autres informations sont fournies par le serveur OPC UA:

- Nombre d'éléments surveillés.
- Nombre d'éléments spécifiques surveillés.
- Les différents intervalles d'échantillonnage en cours d'exécution.
- Nombre de requêtes générées pour les animations en cours.
- Dépassements détectés.
- Nombre de clients connectés.

Via le client OPC UA

Le client OPC UA peut surveiller directement certains éléments spécifiques sous le serveur OPC UA, mais aussi la variable ServiceLevel ou certains sous-champs DDT de BMENUA0100 sur demande via les variables d'application.

Autres services de diagnostic

Selon une approche technique, l'agent SNMP et le serveur Syslog du module BMENUA0100 peut permettre d'obtenir d'autres informations de diagnostic liées aux performances des serveurs OPC UA.

Dépannage du module BMENUA0100

Introduction

Cette section fournit des conseils permettant d'exploiter le module BMENUA0100 de façon optimale.

Impact de l'utilisation de UaExpert comme client OPC UA

Si vous utilisez UaExpert comme client OPC UA pour lire les valeurs de données, notez que chaque instance de UaExpert incrémente le *nombre actuel de souscriptions* de 1 unité.

NOTE: L'élément *nombre actuel de souscriptions* est lié au serveur lui-même et ne doit pas être confondu avec le *nombre actuel de souscriptions* de niveau session

Temps d'acquisition du dictionnaire de données et période MAST

Le temps nécessaire au chargement de l'ensemble des variables du dictionnaire de données dépend du nombre d'éléments du dictionnaire de données et de la période MAST configurée. Pour une application qui nécessite que le serveur OPC UA intégré au module BMENUA0100 surveille un nombre d'éléments proche du maximum de 100000 (990000 en l'occurrence), les résultats suivants ont été observés et peuvent être instructifs.

Pour une application standard (non liée à la sécurité) :

Période MAST	Temps d'acquisition du dictionnaire de données observé
20 ms	23 s
100 ms	46 s
200 ms	74 s

Pour une application de sécurité :

Période MAST	Temps d'acquisition du dictionnaire de données observé
25 ms	15 s
200 ms	72 s

Configuration de souscriptions avec plus de 30 000 éléments surveillés

Si vous prévoyez de créer des souscriptions qui vont représenter au total plus de de 30 000 éléments surveillés, configurez chaque souscription dans le client OPC UA concerné avec une **Durée de vie** de 300 secondes, ce qui représente la durée de souscription maximum, page 32 maximum que le serveur OPC UA du module BMENUA0100 peut prendre en charge.

Utilisation d'objets GPO/LGPO

Schneider Electric recommande de gérer les certificats sur un PC hôte à l'aide de l'un des outils suivants fournis par le système d'exploitation Windows™ :

- Objets de stratégie de groupe (GPO - Group Policy Object) : pour centraliser la gestion des paramètres utilisateur dans un environnement Active Directory centralisé
- Objets de stratégie de groupe locaux (LGPO - Local Group Policy Object) : pour distribuer la gestion des paramètres utilisateur entre plusieurs PC.

Le recours aux GPO ou LGPO peut contribuer à empêcher l'accès non autorisé à votre PC et à ses applications, par exemple par un pirate qui cherche à injecter son propre certificat dans votre PC pour qu'il figure dans la liste blanche d'utilisateurs autorisés du BMENUA0100. L'utilisation de GPO et de LGPO désactive l'accès au service MMC (Microsoft Management Console) de Windows et prend en charge uniquement l'implémentation de la liste blanche configurée par le logiciel, ce qui interdit tout ajout de certificat auto-signé au serveur OPC UA par un pirate qui se fait passer pour un client OPC UA valide.

Application de la gestion de stratégies de groupe MMC

Schneider Electric recommande de gérer les certificats à l'aide des outils fournis par Microsoft Windows™ pour empêcher un intrus d'ajouter des certificats non autorisés au PC ou de modifier les certificats auto-signés d'un client OPC UA. A défaut, un intrus pourrait insérer des certificats non autorisés dans la liste blanche BMENUA0100 gérée par l'administrateur de la sécurité.

Ces outils incluent des règles de gestion de stratégie de groupe appliquées par GPO, un plug-in de Microsoft Management Console (MMC). Concevez vos stratégies de sorte qu'elles désactivent l'accès au service MMC de Windows et n'autorisent l'accès qu'aux entrées de la liste blanche qui ont été correctement ajoutées par le logiciel.

Verrouillage du client OPC UA

Lors de la connexion d'un client OPC UA ayant un nom d'utilisateur au serveur OPC UA intégré dans le BMENUA0100, les paramètres de stratégie de compte d'utilisateur, page 93 du BMENUA0100 sont appliqués. Par exemple, si le **Nombre maximum de tentatives de connexion** est atteint ou dépassé, le client OPC UA ne peut pas se connecter (**BadInternalError**) pendant la période définie comme **Durée de verrouillage du compte**.

Activation des services réseau à l'aide d'une connexion IPv6 uniquement

Le module BMENUA0100 prend en charge l'utilisation du seul protocole IPv6 pour l'adressage IP et la communication. Si seul IPv6 est activé, page 115, les services réseau **Flux de données UC vers UC** et **Flux de données Control Expert vers réseau d'équipements** ne sont pas disponibles. Ces services ne sont pris en charge que par IPv4.

Il reste toutefois possible d'activer ces fonctionnalités dans la page Web **Paramètres > Services réseau**. Si vous activez ces services (**UC vers UC** et **CE vers réseau d'équipements**) alors que seul IPv6 est activé, ils apparaîtront comme actifs (ON) dans la page **Accueil** mais ne le seront pas en réalité.

Seule la fonction de filtrage de flux de données **Flux de données Control Expert vers réseau d'équipements uniquement** est prise en charge par la communication IPv6. Dans ce cas, si seule la communication IPv6 est activée, la page **Accueil** affiche correctement **UC vers UC uniquement** comme étant activé.

Types BOOL considérés comme BYTE dans les structures de données de l'UC

Dans le serveur OPC UA du BMENUA0100, chaque élément du DDT ePAC est affecté à un octet dans l'UC, même s'il est défini comme BOOL ou EBOOL dans le BMENUA0100. Avec le protocole OPC UA, un client peut lire ou écrire globalement un membre BOOL ou EBOOL d'une instance BMENUA0100 dans le DDT de l'UC, avec une valeur d'octet valide autre que 0 ou 1 (par exemple, 255). Il est recommandé de concevoir l'application pour ne lire et écrire que les valeurs BOOL ou EBOOL égales à 0 ou 1, car seules ces valeurs sont valides dans le BMENUA0100.

Mise à niveau du firmware

Outil EcoStruxure™ Automation Device Maintenance

Présentation de l'outil EcoStruxure™ Automation Device Maintenance

Utilisez EcoStruxure™ Automation Device Maintenance pour mettre à niveau le micrologiciel du module BMENUA0100. EcoStruxure™ Automation Device Maintenance est un outil Web qui vous permet d'effectuer les tâches suivantes :

- Découvrir manuellement un ou plusieurs modules BMENUA0100 dans votre projet en fonction des adresses IP.
- Mettre à niveau la dernière version de micrologiciel sur les modules BMENUA0100 via le Web.

Pour plus d'informations sur l'installation et l'utilisation de l'outil EcoStruxure™ Automation Device Maintenance, reportez-vous à l'aide en ligne (voir *EcoStruxure Automation Device Maintenance, Outil de mise à niveau de micrologiciel, Aide en ligne*).

NOTE: L'outil logiciel Unity Loader™ de Schneider Electric ne peut pas être utilisé pour mettre à niveau le micrologiciel du module BMENUA0100. Vous ne pouvez pas connecter le logiciel Unity Loader au port de contrôle du module BMENUA0100 afin de télécharger des projets ou mettre à niveau le logiciel de la CPU ou du module.

Rétrogradation de micrologiciel

Il est possible de rétrograder la version du micrologiciel du module BMENUA0100, par exemple de la version 1.1 à la version 1.0. Après avoir rétrogradé le logiciel à l'aide de l'outil EcoStruxure™ Automation Device Maintenance, effectuez une opération Security Reset, page 27 pour restaurer la configuration d'usine du module. Sélectionnez ensuite un mode de fonctionnement de la cybersécurité (Secured ou Standard) pour le module.

Annexes

Contenu de cette partie

Connexions UC

Contenu de ce chapitre

Connexions entre serveur OPC UA et UC

Connexions ouvertes

Le nombre de connexions que le module BMENUA0100 peut ouvrir sur l'UC M580 dépend de la capacité de l'UC. Ainsi, les performances du module BMENUA0100 dépendent du temps nécessaire pour exécuter la tâche MAST et l'UC sélectionnée. Voici le nombre maximal de connexions ouvertes par chaque module BMENUA0100 avec l'UC M580 :

Modèle d'UC	Nombre maximal de connexions ouvertes par chaque BMENUA0100
	9
BMEP5820•0	9
BMEP5830•0	12
BMEP5840•0	15
BMEP585040	15
BMEP586040	18
BMEH582040	9
BMEH584040	15
BMEH586040	18

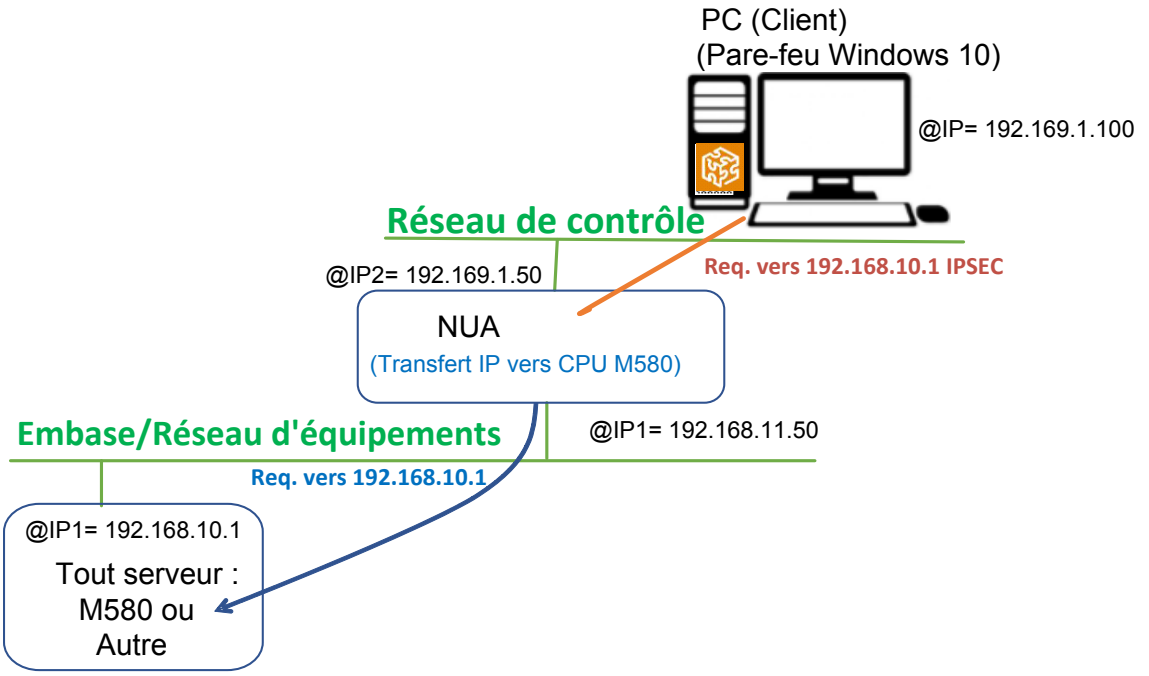
Architectures de transfert de service (IP)

Contenu de ce chapitre

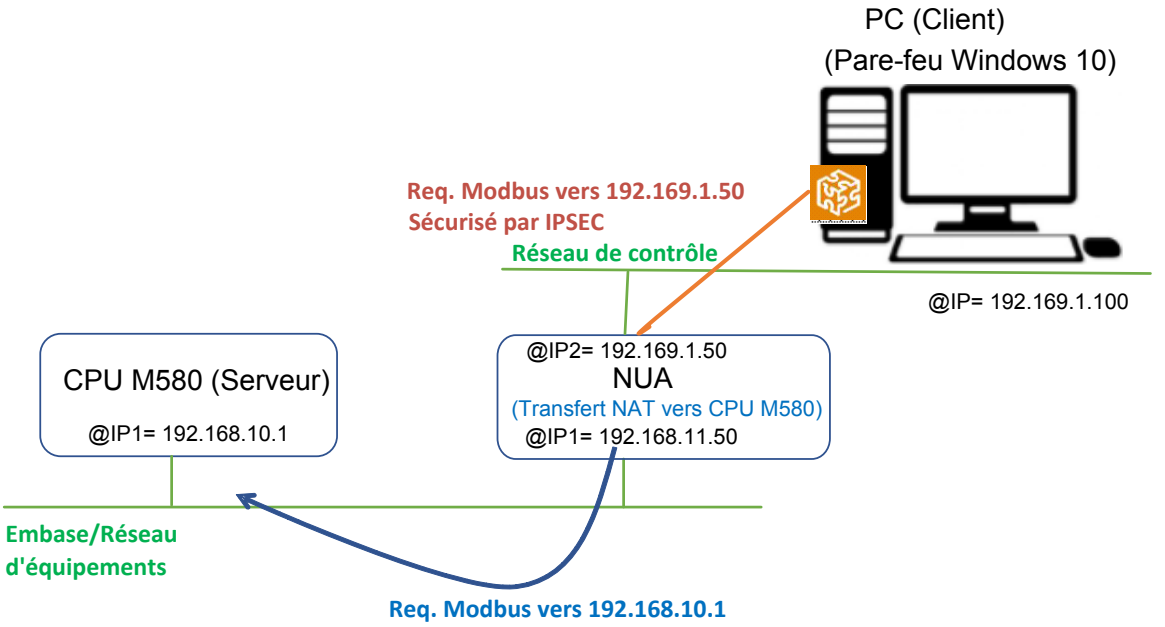
Ce chapitre présente les architectures prises en charge et non prises en charge par la fonction de transfert de service (IP) du module BMENUA0100.

Transfert de service (IP) - Architectures prises en charge

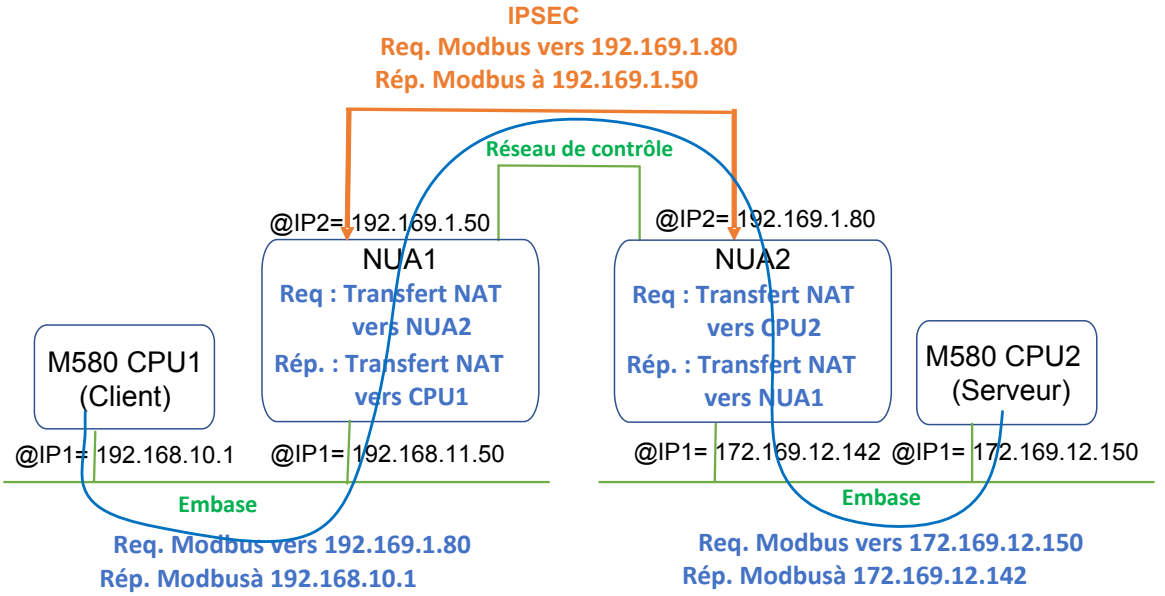
Transfert IP du client Windows (réseau de contrôle) vers n'importe quel client (embase/réseau d'équipements)



Transfert NAT du client Windows (réseau de contrôle) vers l'UC M580 (embase/réseau d'équipements)

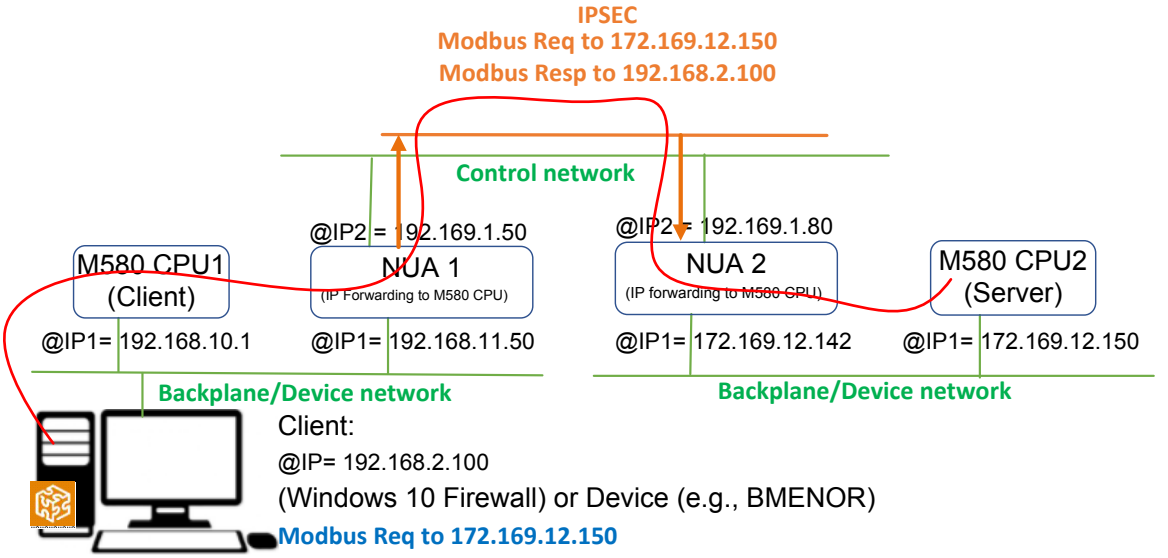


Transfert NAT entre embases pour la communication entre UC M580



Transfert de service (IP) - Architectures non prises en charge

Transfert IP entre embases/réseaux d'équipements



Transfert IP et communication OPC UA

Contenu de ce chapitre

Le transfert IP et la communication OPC UA sont en concurrence pour la bande passante de communication disponible du module BMENUA0100. Ce chapitre contient les résultats des tests de performances du module selon que le transfert IP seul est utilisé ou que la communication OPC UA est ajoutée.

Impact du transfert IP sur les performances

Lorsque seul le transfert IP est activé (à l'exclusion de la communication OPC UA), l'impact sur la bande passante du BMENUA0100 est le suivant :

IPSec	Confidentialité	Transfert	Longueur de trame (octets)	Bande passante (Ko/s)
Non	Sans objet	Transférer tout	1000	8800
Non	Sans objet	Règle personnalisée	1000	10600
Oui	Non	Transférer tout	1000	3400
Oui	Non	Règle personnalisée	1000	4000
Oui	Oui	Transférer tout	1000	2600
Oui	Oui	Règle personnalisée	1000	2500

NOTE: Ces valeurs sont indiquées à titre d'exemples uniquement. Utilisez-les pour estimer l'impact des différents paramètres (IPSEC, Confidentialité, etc.) sur les performances. Les performances réelles dépendent de l'infrastructure spécifique.

L'impact sur la bande passante s'affiche lorsque :

- Seul le flux de communication de transfert IP est pris en compte, aucun flux de communication OPC UA n'est inclus.
- IPSec est utilisé (IPSec = Oui) et inutilisé (IPSec = Non).
- Les trames sont signées (Confidentialité = Non) ou sont signées et cryptées (Confidentialité = Oui) et IPSEC est utilisé (dans les deux cas).

- Des règles personnalisées sont appliquées au transfert IP ou la commande Transférer tout est utilisée.

  NOTE: La longueur des trames n'a qu'un faible impact sur les performances globales.

Transfert IP et OPC UA - Impact sur les performances

Lorsque le transfert IP et la communication OPC UA sont tous les deux activés, l'impact sur la bande passante du module BMENUA0100 est le suivant :

Nombre d'éléments OPC UA surveillés par abonnement	IPSec	Confidentialité	Transfert	Bande passante (Ko/s)
0	Non	Sans objet	Règle personnalisée	10600
0	Oui	Non	Règle personnalisée	4000
0	Oui	Oui	Règle personnalisée	2500
20000	Non	Sans objet	Règle personnalisée	8800
20000	Oui	Non	Règle personnalisée	2900
20000	Oui	Oui	Règle personnalisée	2000

NOTE: Ces valeurs sont indiquées à titre d'exemples uniquement. Utilisez-les pour estimer l'impact des différents paramètres (IPSEC, Confidentialité, etc.) sur les performances. Les performances réelles dépendent de l'infrastructure spécifique.

L'impact sur la bande passante s'affiche lorsque :

- Toute l'activité de transfert de paquets est effectuée selon une règle personnalisée (pas de transfert global).
- Les flux de communication OPC UA sont exclus (nombre d'éléments OPC UA surveillés = 0) et inclus (= 2000).

  NOTE: Le nombre d'éléments OPC UA surveillés a un impact faible.

Scripts Windows IPSEC

Contenu de ce chapitre

Scripts de configuration de pare-feu Windows IKE/ IPSEC

Pour exécuter IPSEC sur un PC hébergeant le logiciel de configuration Control Expert ou un client OPC UA (par exemple, SCADA), vous devez ajouter une configuration réseau au pare-feu de l'hôte. Pour chaque règle IPSEC configurée dans les pages Web, un script associé (nommé IPSecWindowsConf.bat) peut être téléchargé à l'aide de l'icône en forme de roue dentée. Exécutez ce script pour définir le pare-feu de l'hôte dans la configuration appropriée.

- IKE/IPSEC en mode **transport** pour les flux de données locaux du BMENUA0100.
- IKE/IPSEC en mode **tunnel** pour les flux de données transférés à l'embase Ethernet.
- Règles de passage pour HTTPS, OPCUA sécurisé et d'autres protocoles pour lesquels l'option **Utilisation IPSEC** est désactivée.

Les exemples suivants présentent les scripts de configuration du pare-feu Windows avec ou sans la confidentialité IPSEC.

Dans chaque exemple de script, vous devez fournir les valeurs réelles pour les variables suivantes :

- **`endpoint1`** : valeur de l'adresse IP distante dans la configuration IPSEC.
- **`endpoint2`** : adresse IP du port de contrôle du BMENUA0100.
- **`Auth1psk`** : réglage PSK dans la configuration IPSEC.

Script de pare-feu Windows avec confidentialité

NOTE: Si la confidentialité est activée dans la configuration IPSEC, `qmsecmethods=esp:sha256-aes128`

```
netsh advfirewall reset

netsh advfirewall set global mainmode mmkeylifetime 2879min,0sess
```

```
netsh advfirewall set global mainmode mmsecmethods dhgroup14:aes128-
sha256,dhgroup2:aes128-sha256

netsh advfirewall consec delete rule name="IPSECtunnel"

netsh advfirewall consec delete rule name="IPSECtransport"

netsh advfirewall consec delete rule name="IPSECpassthroughOPCUA"

netsh advfirewall consec delete rule name="IPSECpassthroughHTTPS"

netsh advfirewall consec add rule name="IPSECtransport" endpoint1=
192.169.1.100 endpoint2=192.169.1.50 action=requireinrequireout
description="IPSECtransport" mode=transport enable=yes profile=public
type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
aes128+1440min

netsh advfirewall consec add rule name="IPSECpassthroughOPCUA"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughOPCUA" mode=transport
enable=yes profile=public type=static protocol=tcp port2=4840

netsh advfirewall consec add rule name="IPSECpassthroughHTTPS"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughHTTPS" mode=transport
enable=yes profile=public type=static protocol=tcp port2=443

netsh advfirewall consec add rule name="IPSECtunnel" endpoint1=
192.169.0.0/16 endpoint2=192.168.0.0/16 localtunnelendpoint=
192.169.1.100 remotetunnelendpoint=192.169.1.50 action=
requireinrequireout description="IPSECtunnel" mode=tunnel enable=yes
profile=public type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
aes128+1440min

netsh advfirewall consec show rule name=all verbose

pause
```

Script de pare-feu Windows sans confidentialité

NOTE: Si la confidentialité est activée dans la configuration IPSEC, `qmsecmethods=esp:sha256-None`

```
netsh advfirewall reset

netsh advfirewall set global mainmode mmkeylifetime 2879min,0sess
```

```
netsh advfirewall set global mainmode mmsecmethods dhgroup14:aes128-
sha256,dhgroup2:aes128-sha256

netsh advfirewall consec delete rule name="IPSECtunnel"

netsh advfirewall consec delete rule name="IPSECtransport"

netsh advfirewall consec delete rule name="IPSECpassthroughOPCUA"

netsh advfirewall consec delete rule name="IPSECpassthroughHTTPS"

netsh advfirewall consec add rule name="IPSECtransport" endpoint1=
192.169.1.100 endpoint2=192.169.1.50 action=requireinrequireout
description="IPSECtransport" mode=transport enable=yes profile=public
type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
None+1440min

netsh advfirewall consec add rule name="IPSECpassthroughOPCUA"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughOPCUA" mode=transport
enable=yes profile=public type=static protocol=tcp port2=4840

netsh advfirewall consec add rule name="IPSECpassthroughHTTPS"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughHTTPS" mode=transport
enable=yes profile=public type=static protocol=tcp port2=443

netsh advfirewall consec add rule name="IPSECtunnel" endpoint1=
192.169.0.0/16 endpoint2=192.168.0.0/16 localtunnelendpoint=
192.169.1.100 remotetunnelendpoint=192.169.1.50 action=
requireinrequireout description="IPSECtunnel" mode=tunnel enable=yes
profile=public type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
None+1440min

netsh advfirewall consec show rule name=all verbose

pause
```

Configuration d'une autorité de certification Windows

Contenu de ce chapitre

Ce chapitre explique comment configurer une autorité de certification Microsoft Windows™ en vue de l'utiliser dans un système d'authentification et d'autorisation des utilisateurs à l'échelle d'une entreprise.

Étapes préalables

Cette section décrit les outils dont vous avez besoin et les étapes préliminaires à suivre avant d'installer le serveur de certificats.

Outils nécessaires

Les éléments suivants vous seront nécessaires :

- Microsoft Windows™ Server Manager : Téléchargeable gratuitement à partir du site Web de Microsoft.
- Microsoft Windows Active Directory Certificate Server (ADCS) : Ce logiciel est inclus dans Windows Server. Vous devrez acheter une licence spécifique. Le module BMENUA0100 prend en charge les versions de serveur 2016 et 2019.
- Fichier TemplatePackage.zip, téléchargeable depuis le site de Schneider Electric.

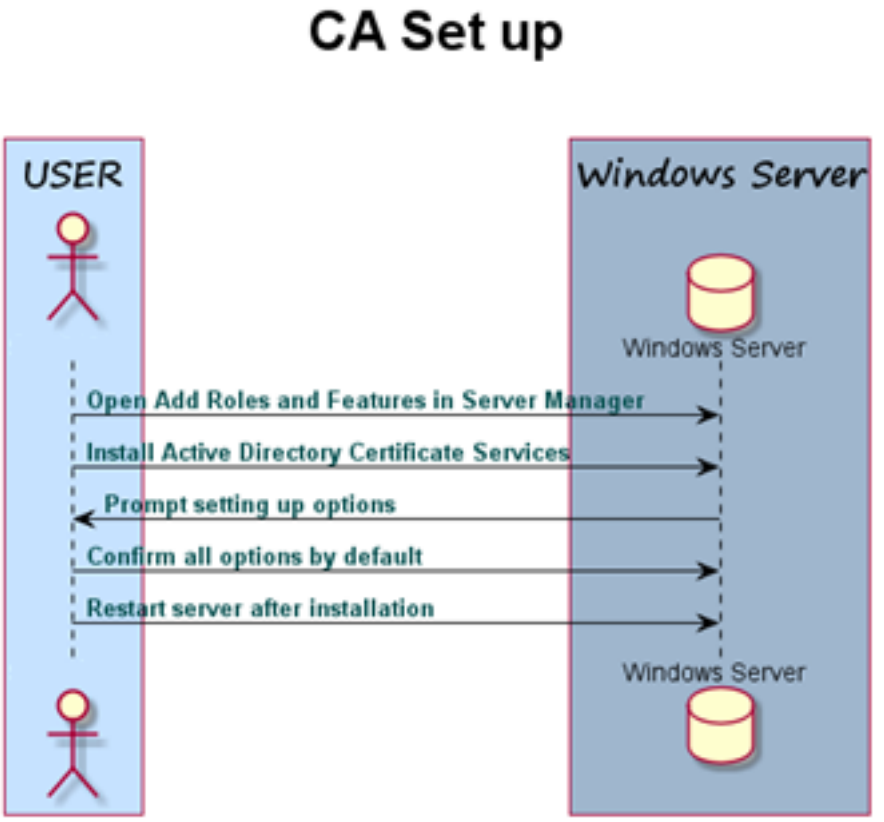
Installations de logiciel préalables

Exécutez le fichier d'installation ADCS et suivez les étapes décrites pour créer un utilisateur et un mot de passe.

Server Manager doit être préinstallé sur votre PC hôte. Si ce n'est pas le cas, vous pouvez le télécharger gratuitement à partir du site Web de Microsoft.

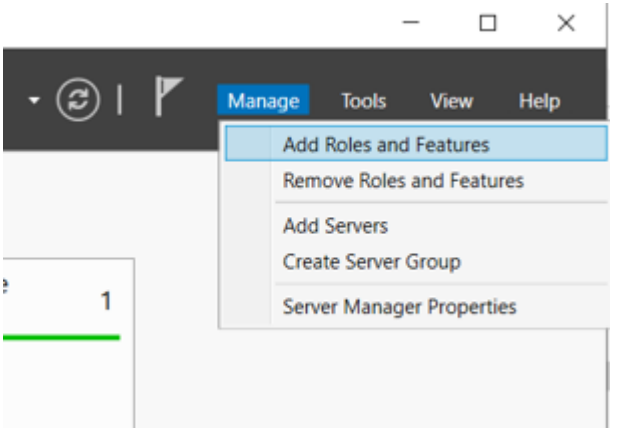
Installation de Microsoft Windows ADCS - Vue d'ensemble

L'illustration suivante présente le processus de configuration de l'autorité de certification (CA) :

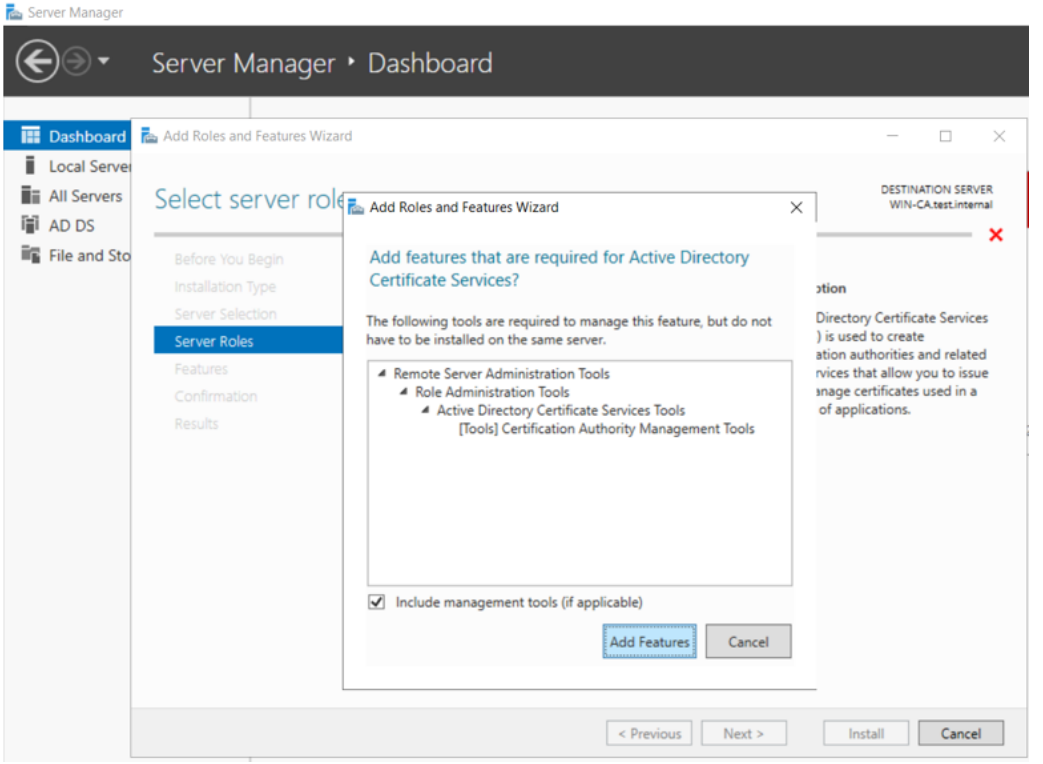


Installation du logiciel Active Directory Certificate Server (ADCS)

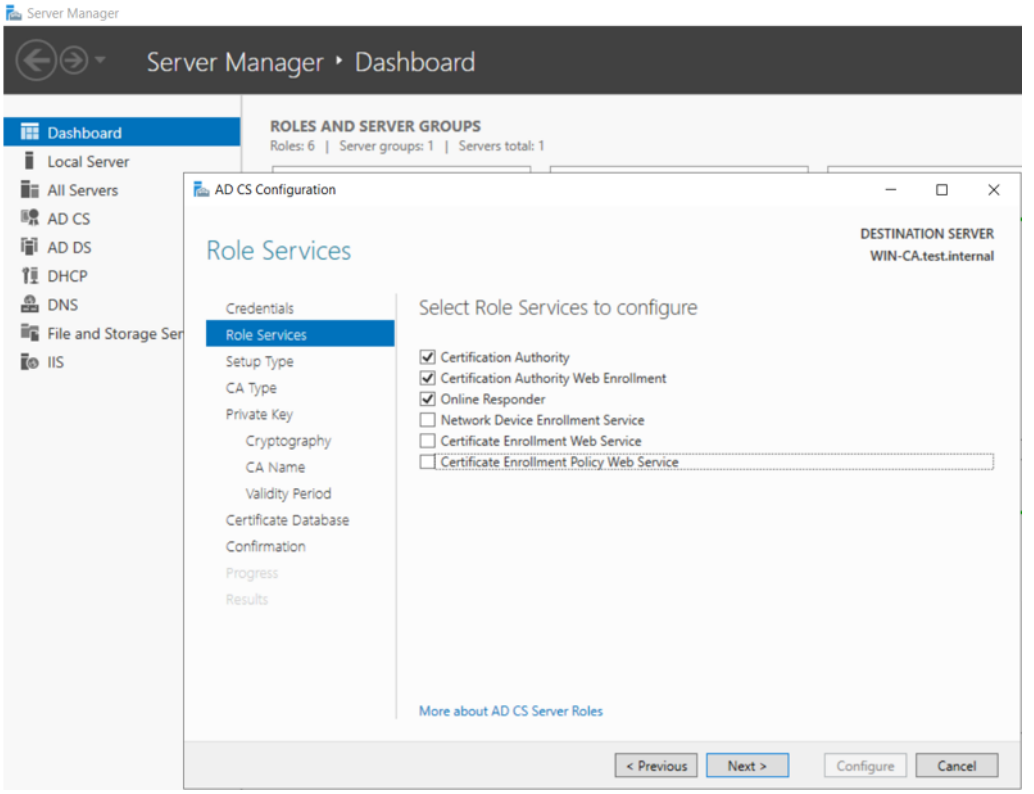
1. Lancez Microsoft Windows™ Server Manager et ouvrez le tableau de bord.
2. Sélectionnez **Gérer > Ajouter des rôles et des fonctionnalités**.



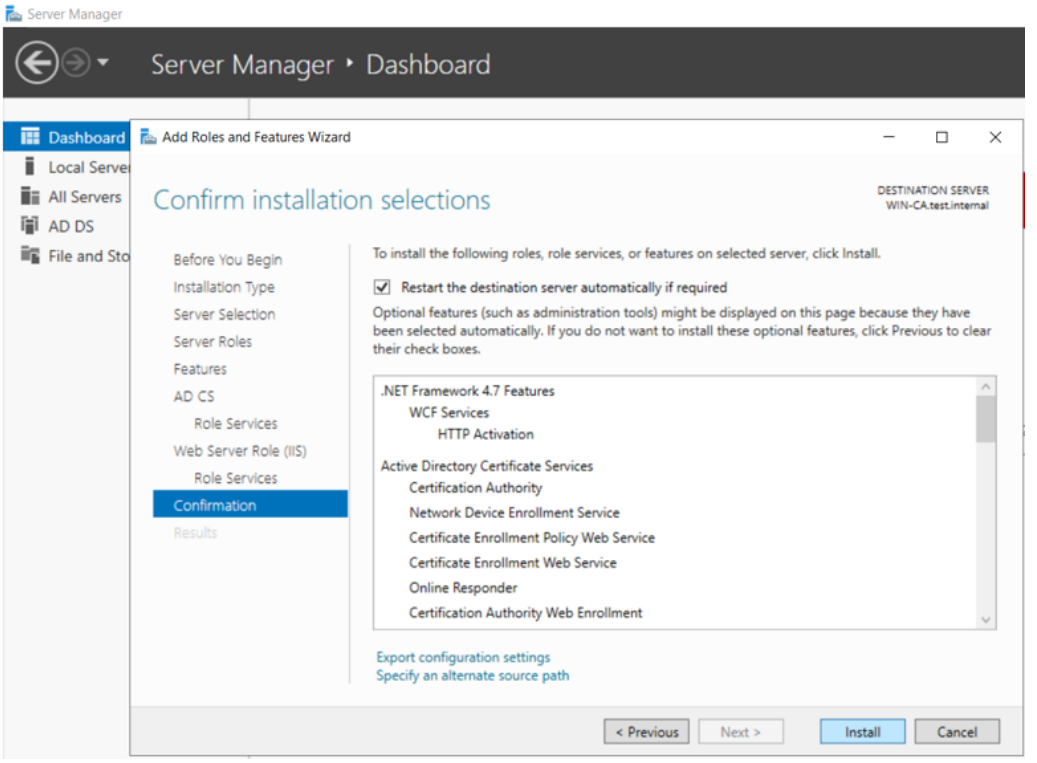
3. Ajoutez les rôles et les fonctions requis et incluez les outils de gestion :



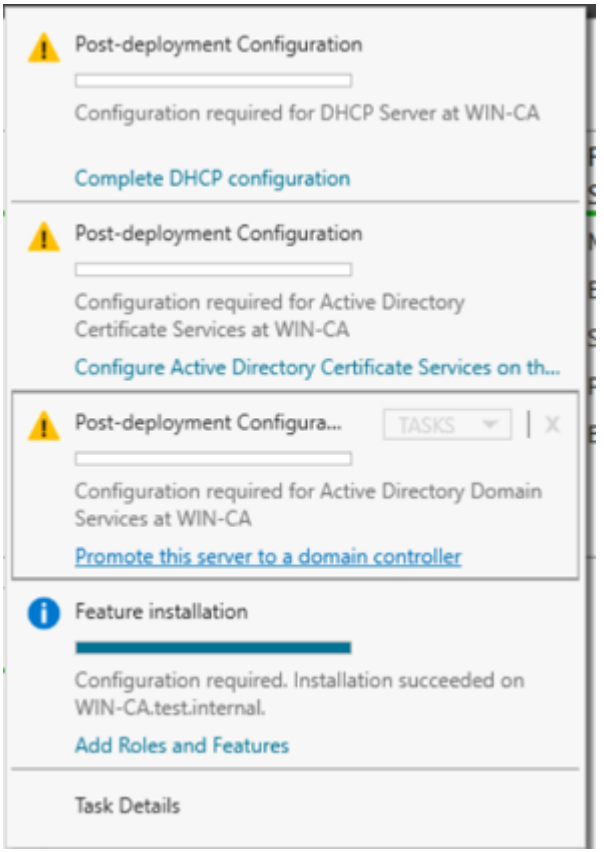
4. Sélectionnez les services de rôle à configurer :



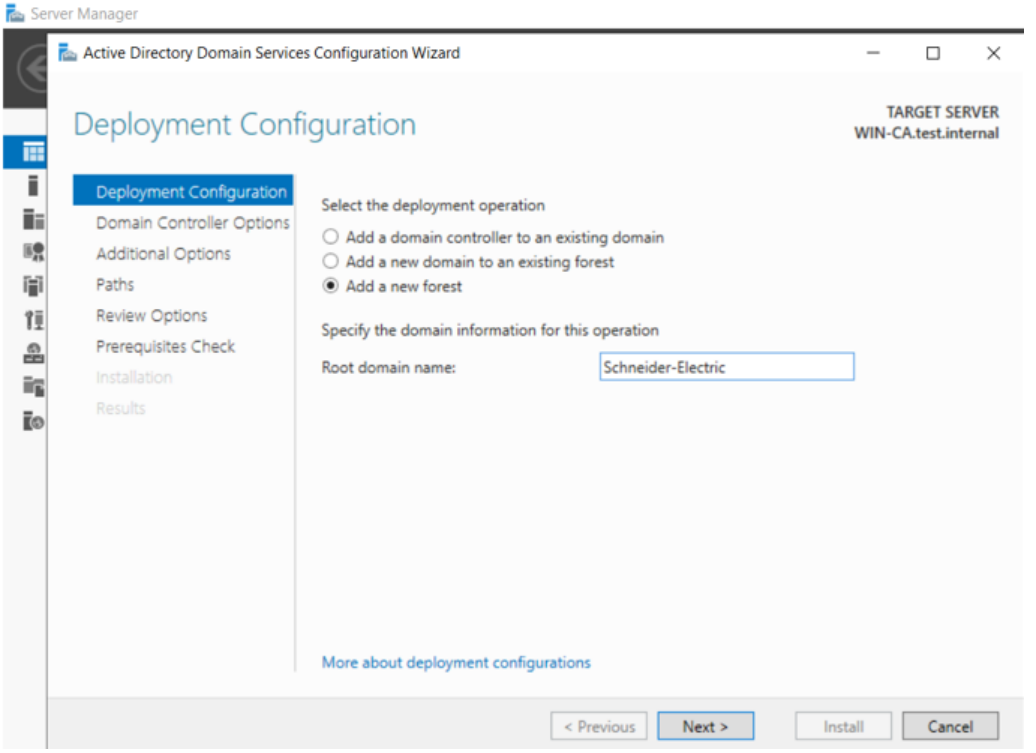
5. Confirmez les sélections d'installation :



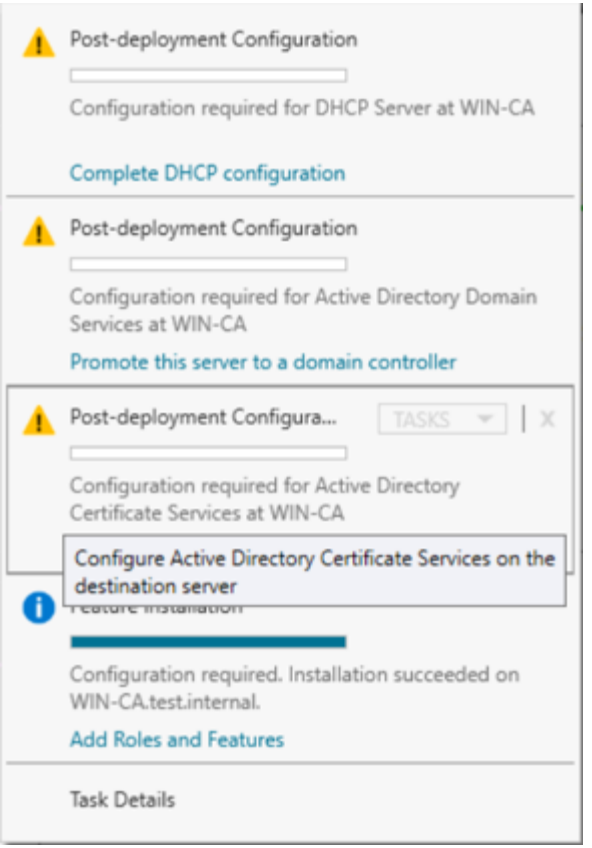
6. Cliquez sur **Installer**. Server Manager affiche la progression de l'installation :



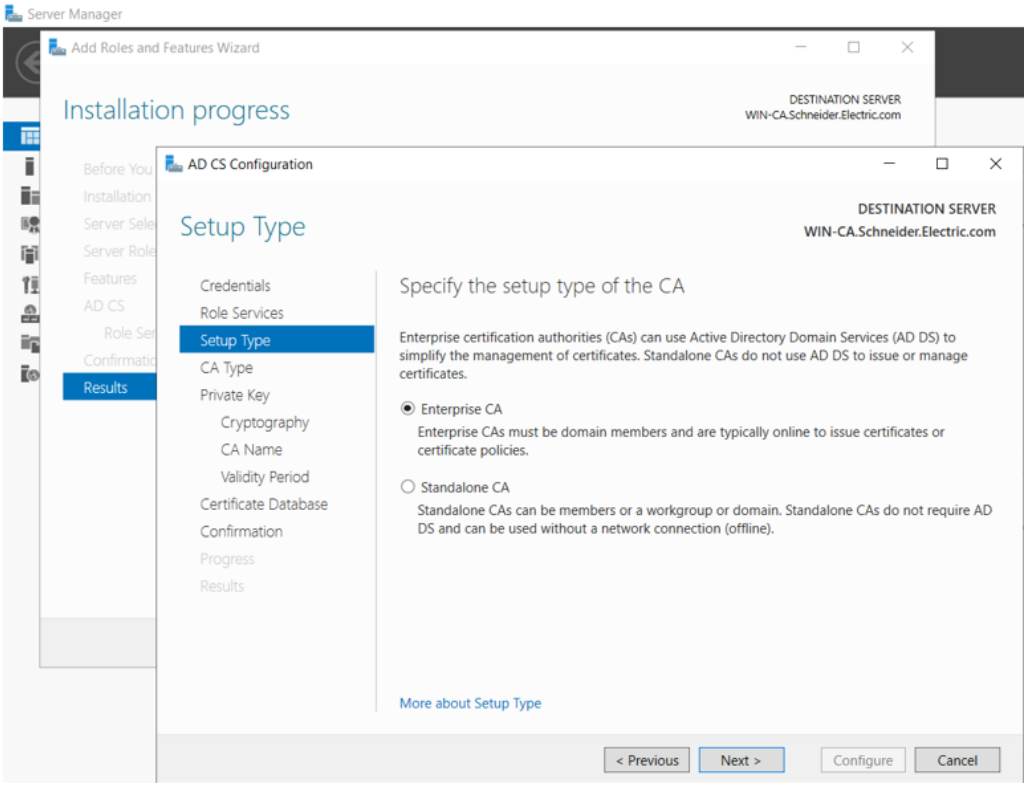
7. Sélectionnez l'opération de déploiement, en créant une nouvelle forêt ou en l'ajoutant à une forêt existante, et indiquez le domaine :



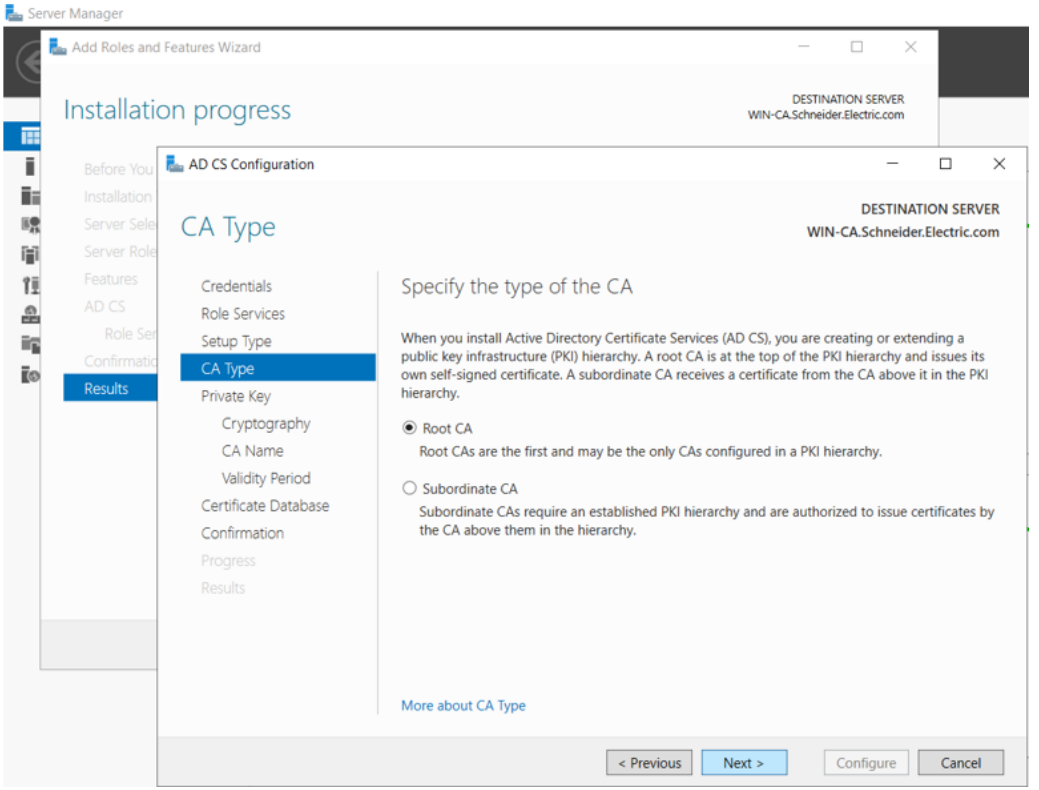
8. Server Manager affiche les sélections :



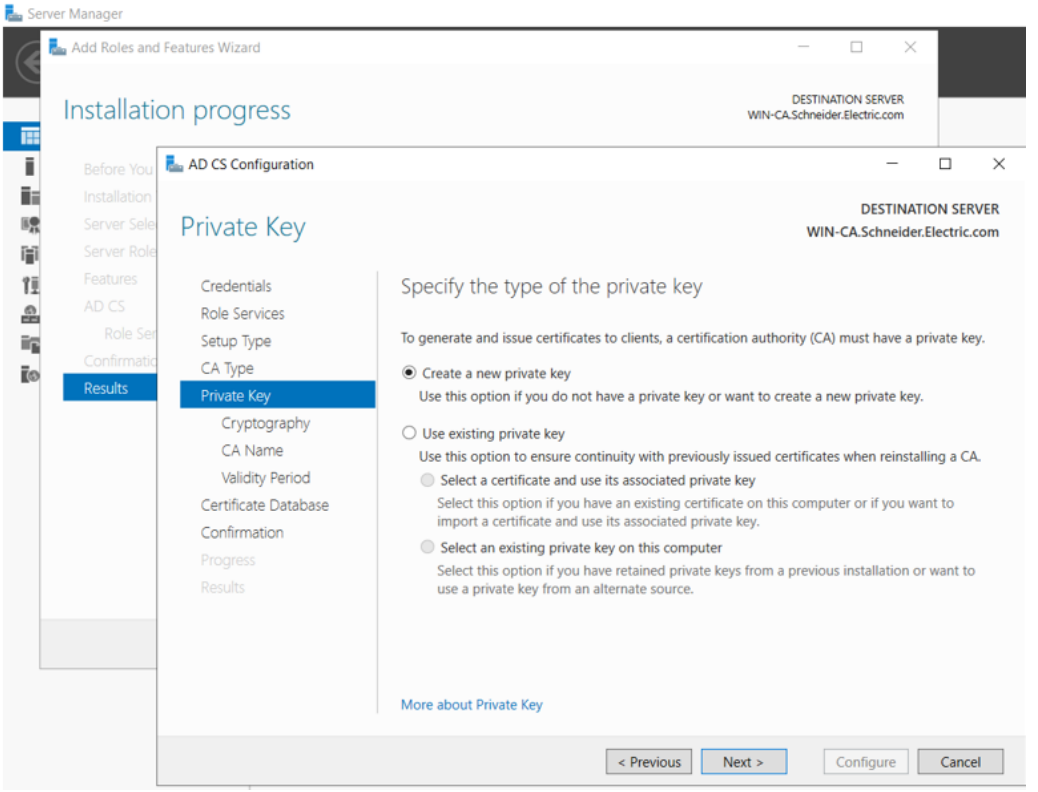
9. Spécifiez le type d'autorité de certification à configurer :



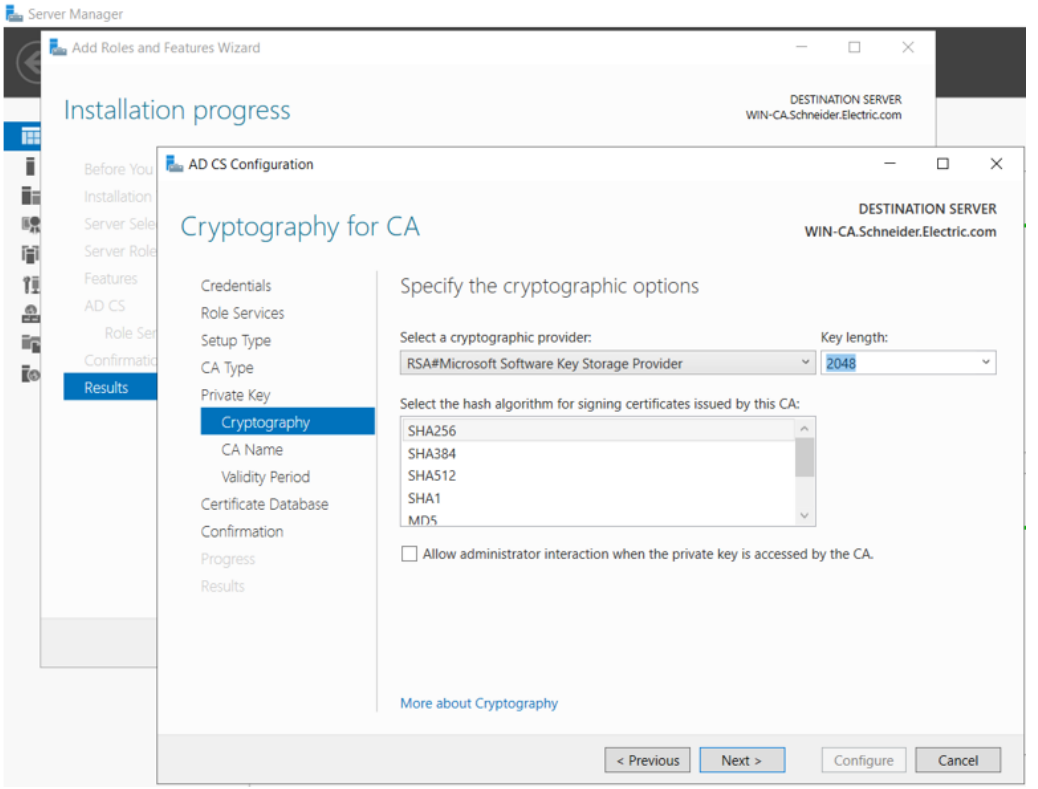
10. Spécifiez le type d'autorité de certification :



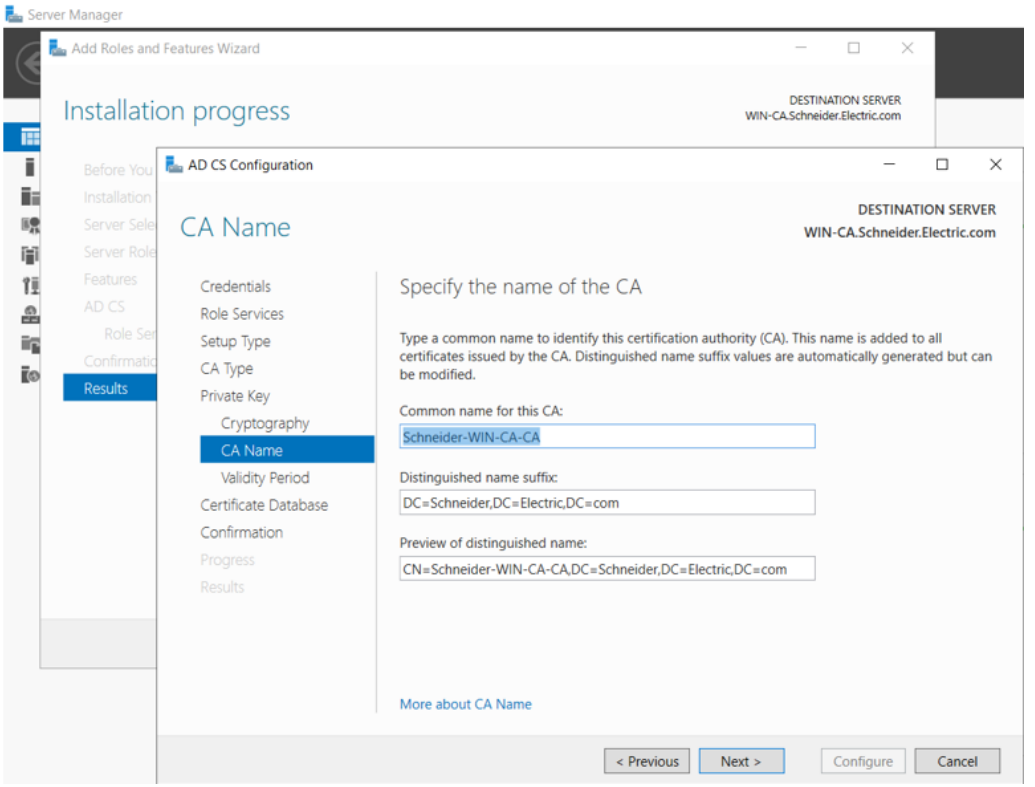
11. Spécifiez le type de clé privée :



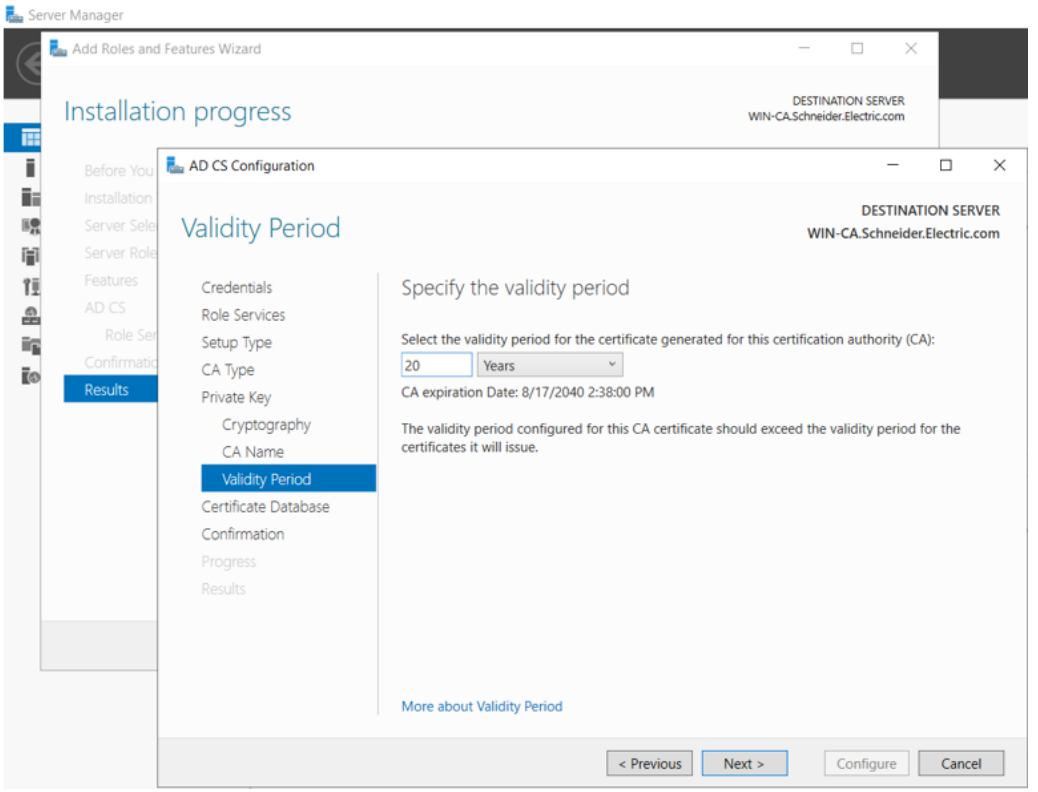
12. Sélectionnez les options de chiffrement :



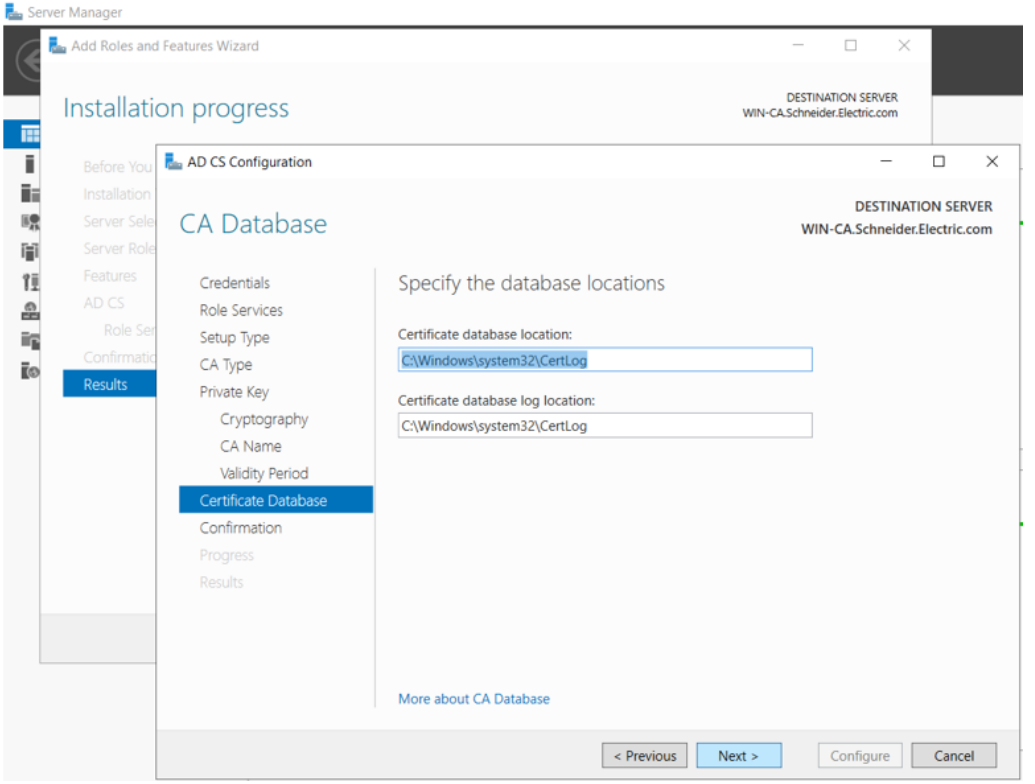
13. Spécifiez les options de dénomination pour l'autorité de certification :



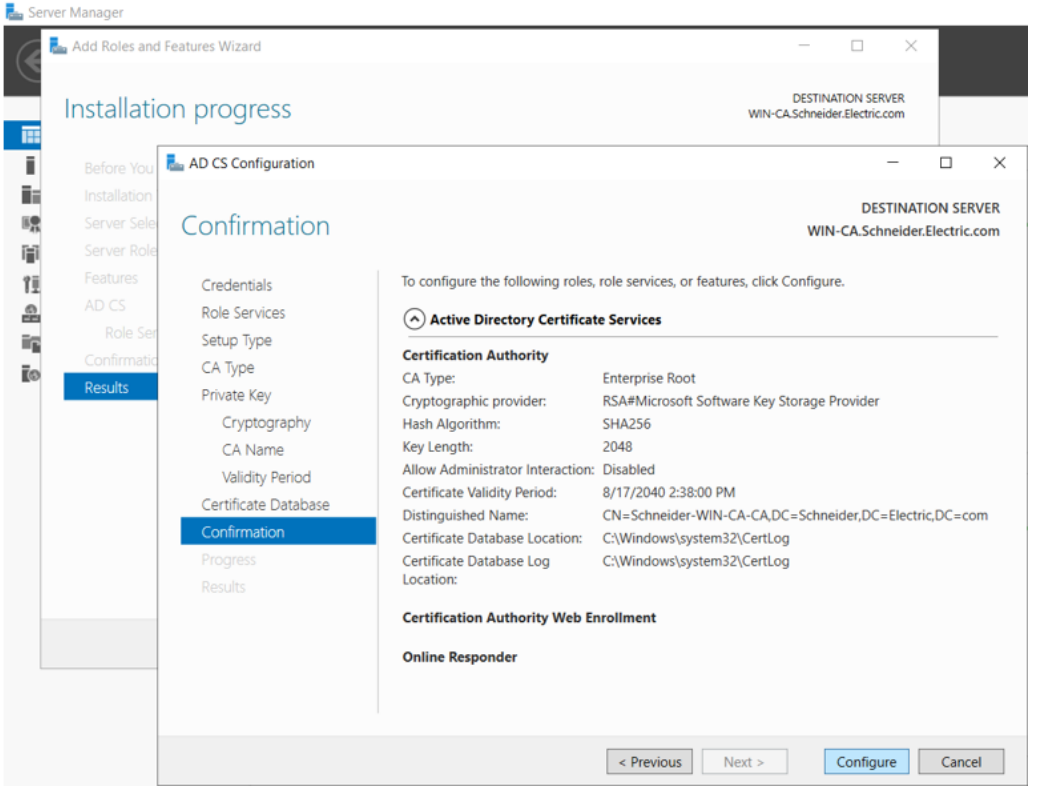
14. Indiquez la période de validité. La période de validité recommandée pour un certificat CA est de 5 ans :



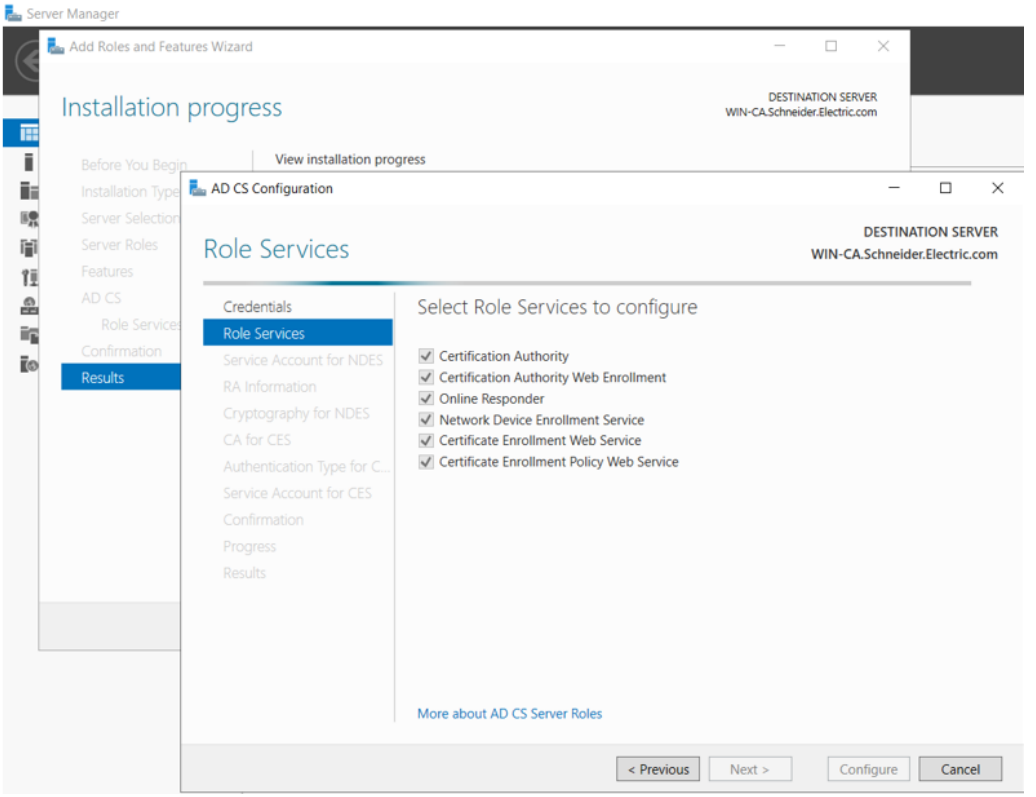
15. Indiquez les emplacements de la base de données des certificats et de l'historique :



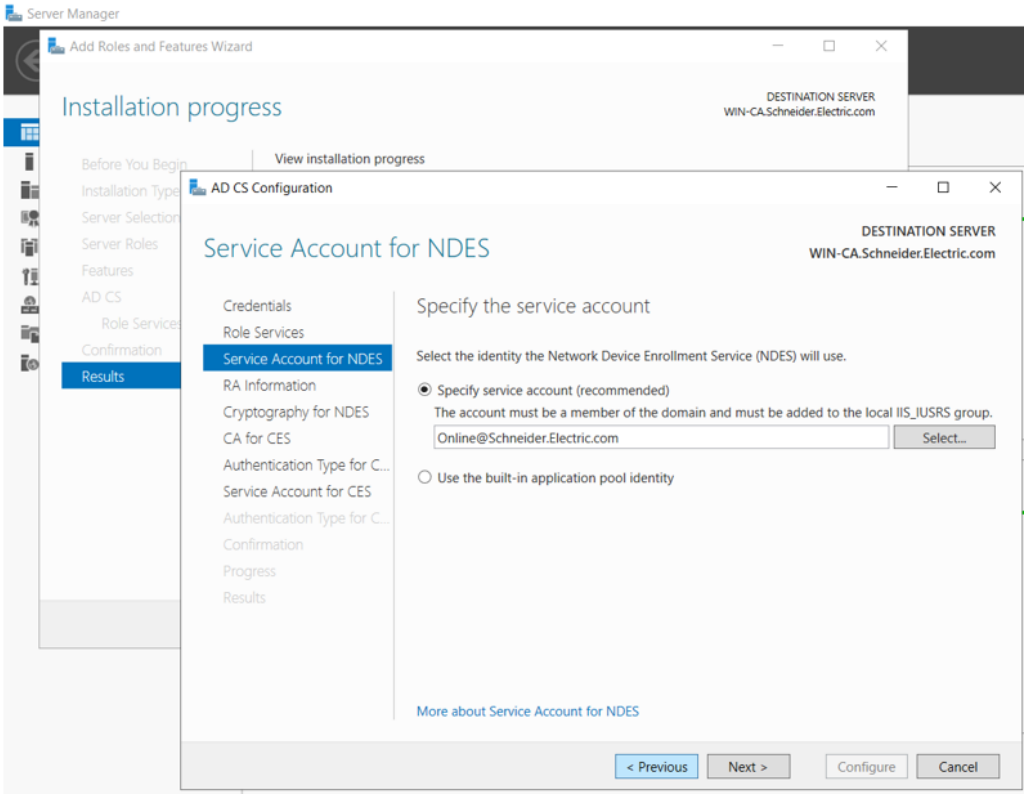
16. Confirmez les services ADCS sélectionnés et cliquez sur **Configurer** :



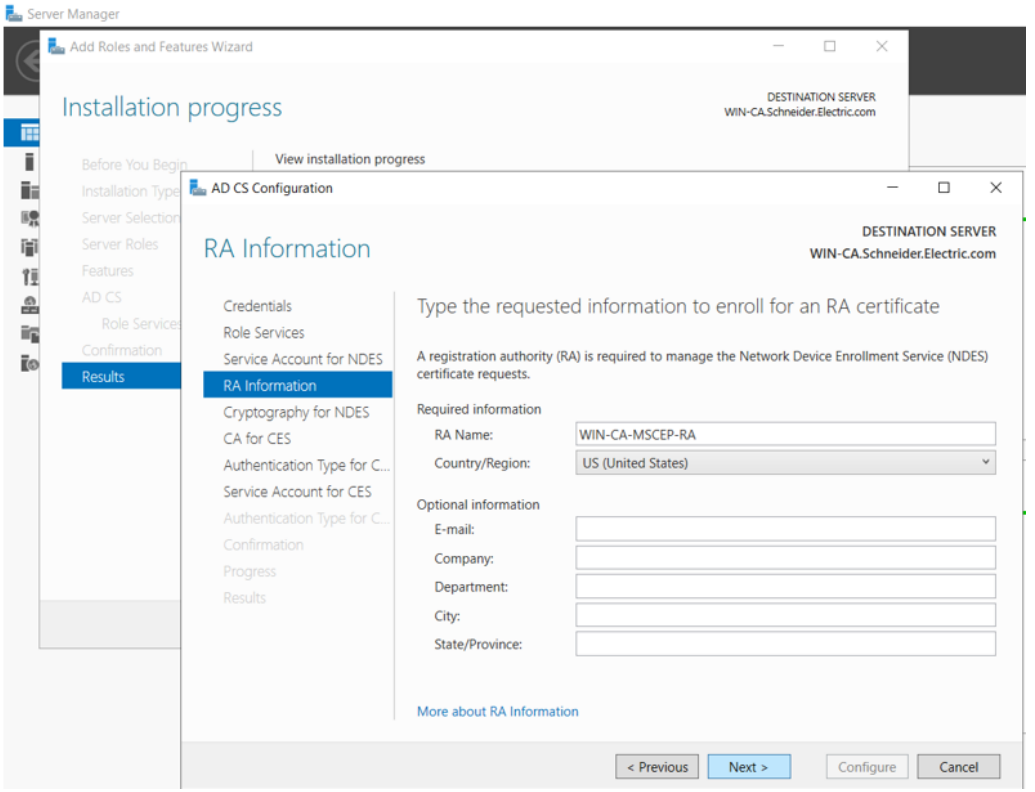
17. Sélectionnez les services de rôle à configurer :



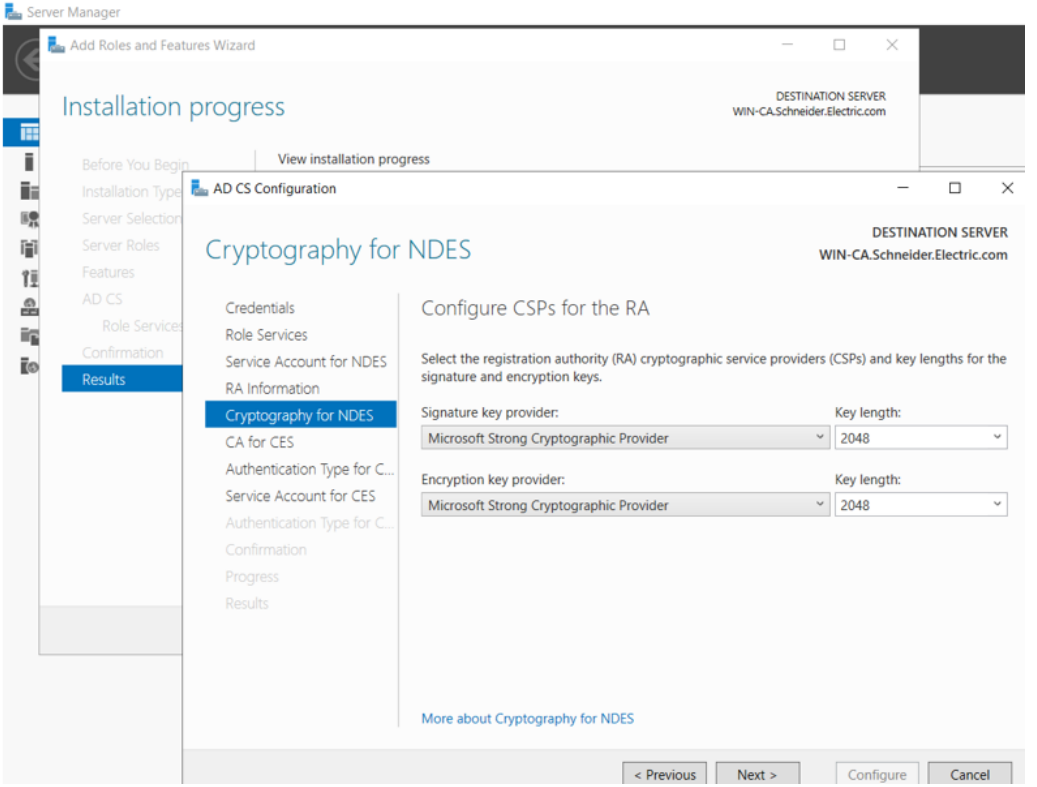
18. Indiquez le compte de service :



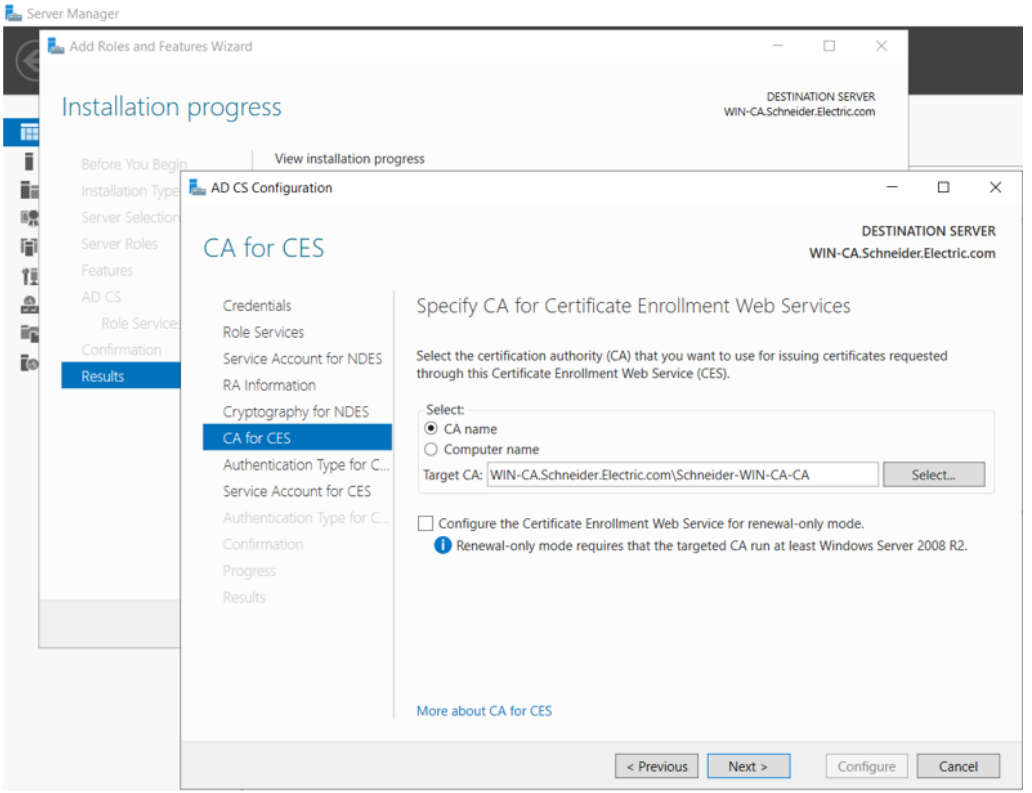
19. Entrez les informations pour adhérer à un certificat d'autorité d'inscription (RA) :



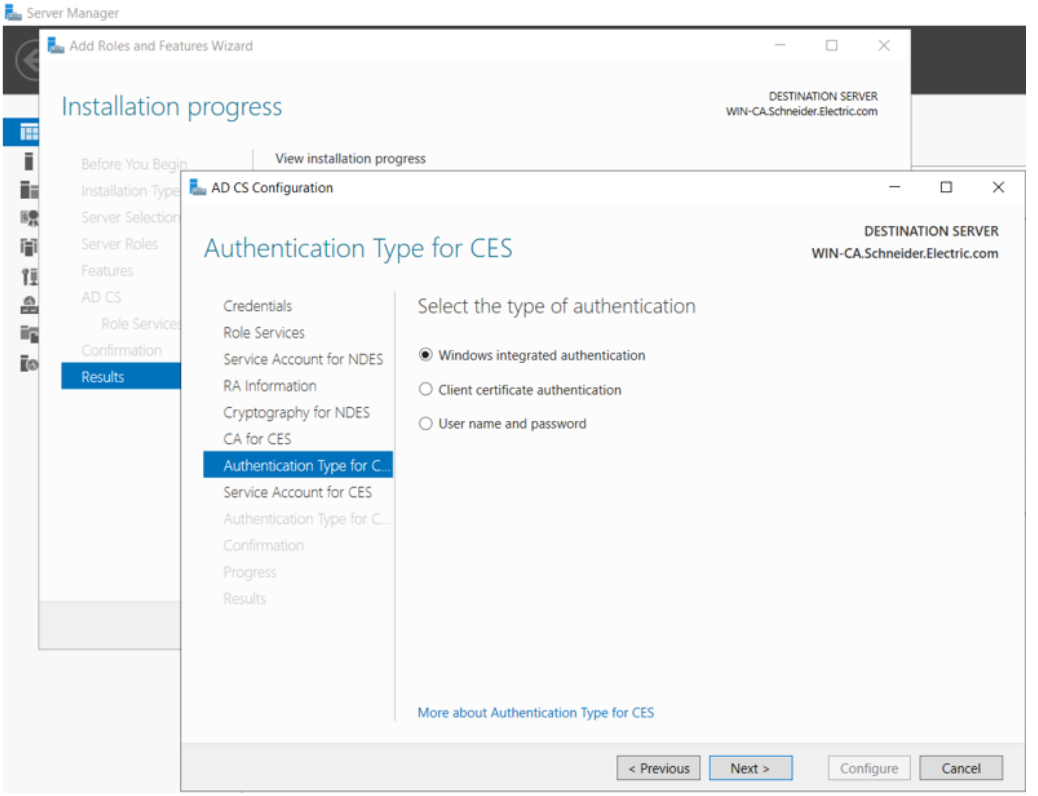
20. Sélectionnez les paramètres de chiffrement pour l'autorité d'inscription :



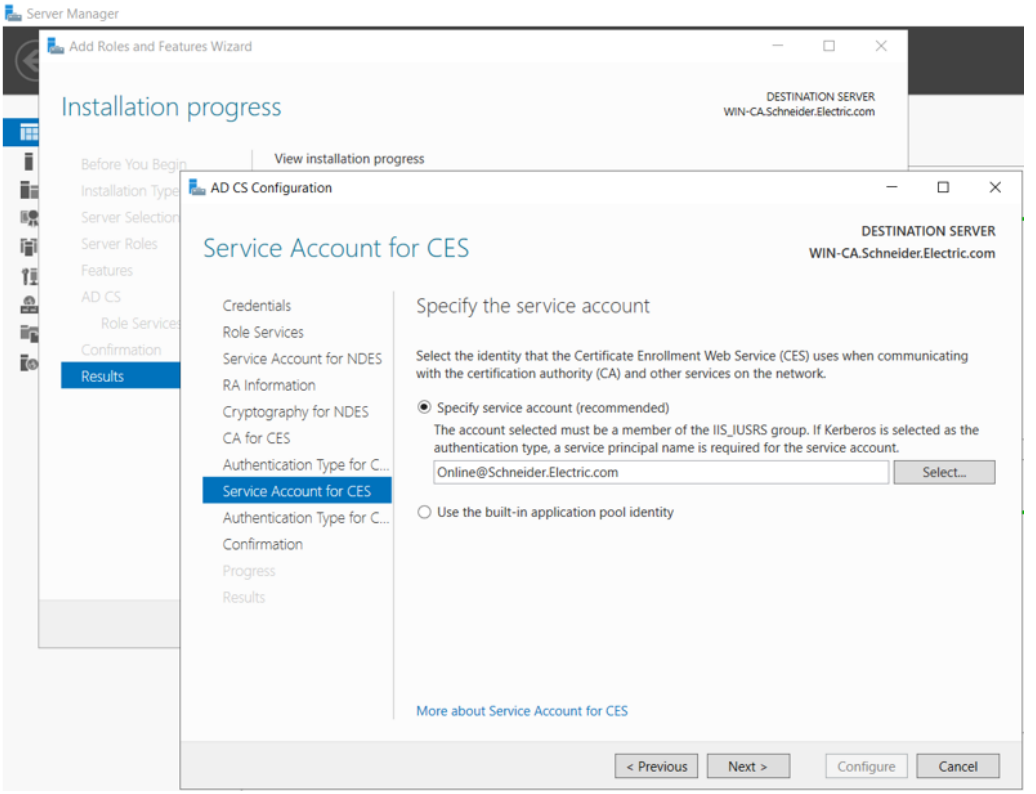
21. Spécifiez l'autorité de certification pour les services Web d'inscription de certificats :



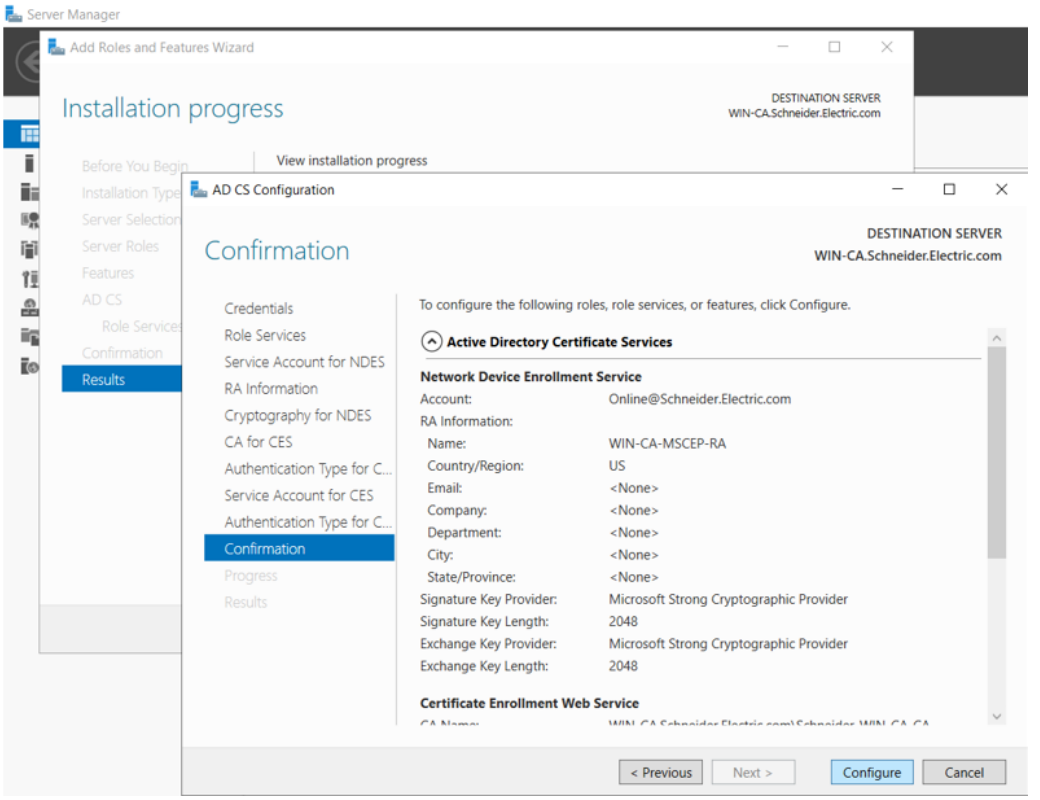
22. Sélectionnez un type d'authentification :



23. Indiquez le compte de service :



24. Confirmez les rôles, les services et les fonctionnalités, puis cliquez sur **Configurer** :



La configuration d'ADCS est terminée.

Application du modèle d'autorité de certification

La dernière partie de la configuration d'une autorité de certification (CA) Microsoft Windows consiste à appliquer le modèle CA fourni par Schneider Electric.

Ce modèle et les éléments de support sont contenus dans le fichier "TemplatePackage.zip" fourni par Schneider Electric.

Pour appliquer le certificat, procédez comme suit :

1. Décompressez le fichier "TemplatePackage.zip" et copiez son contenu (dossier nommé "TemplatePackage") à un emplacement autre que C:\Windows\System32...

   Par exemple, vous pouvez copier ce dossier dans "C:\Utilisateurs\Administrateur\Bureau\"

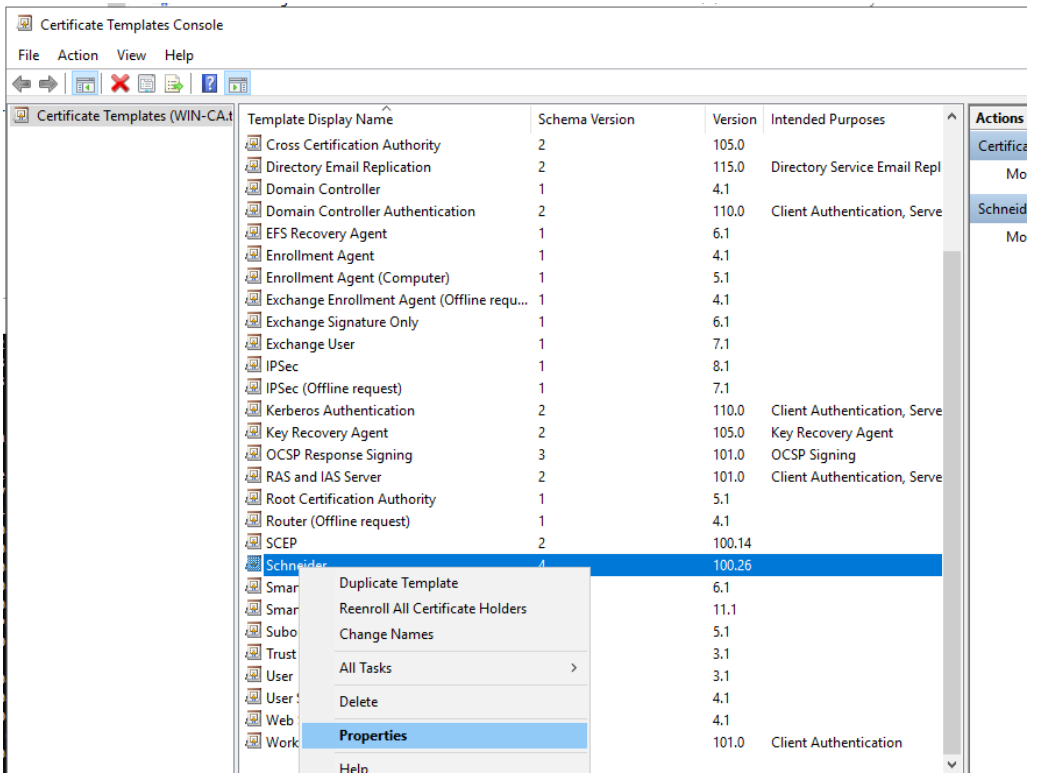
2. Démarrez Microsoft Windows PowerShell en tant qu'administrateur.
3. Dans PowerShell, accédez au dossier où vous avez placé TemplatePackage, par exemple :.

   ```
   > cd C:\Utilisateurs\Administrateur\Bureau\TemplatePackage
   ```

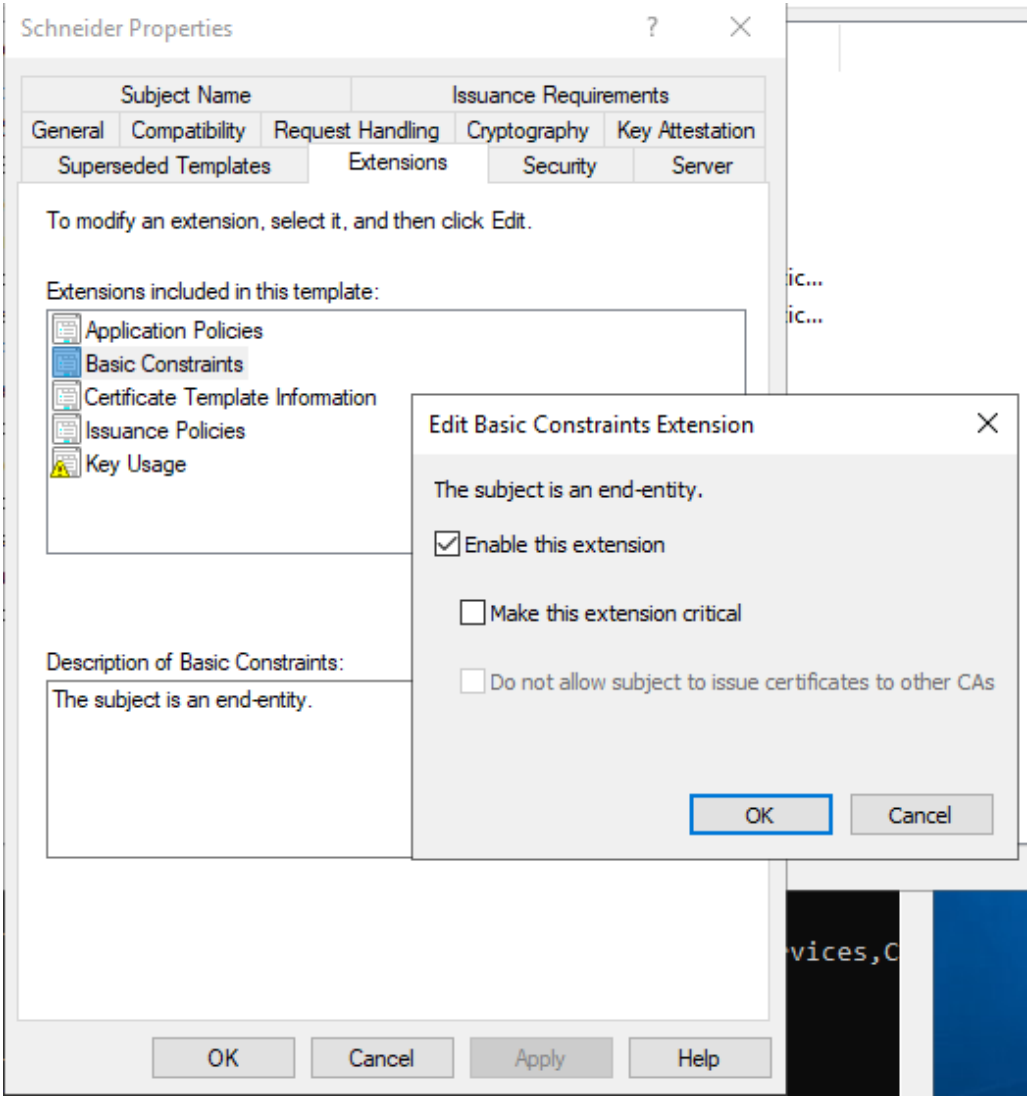
4. Dans PowerShell, exécutez le modèle depuis le dossier TemplatePackage, comme suit :

   ```
   > .\ImportCertificateTemplate.ps1
   ```

5. Sur le PC hôte, ouvrez la console Modèles de certificat, cliquez avec le bouton droit sur le certificat Schneider, puis sélectionnez **Propriétés** :



6. Dans la fenêtre **Propriétés Schneider**, ouvrez l'onglet **Extensions** et double-cliquez sur **Contraintes de base**. Dans la boîte de dialogue **Modifier les contraintes de base**, sélectionnez **Activer cette extension** et cliquez sur **OK** :



Procédure d'inscription manuelle

Reportez-vous à la section Inscription manuelle de certificats, page 109 pour plus d'informations sur la manière d'effectuer cette tâche.

Cliquez sur le lien fourni dans cette section pour accéder à une présentation vidéo de la procédure à suivre.

Glossaire

A

adresse IP:

Identificateur de 32 bits, constitué d'une adresse réseau et d'une adresse d'hôte, affecté à un équipement connecté à un réseau TCP/IP.

E

environnement difficile:

Résistance aux hydrocarbures, aux huiles industrielles, aux détergents et aux copeaux de brasure. Humidité relative pouvant atteindre 100 %, atmosphère saline, écarts de température importants, température de fonctionnement comprise entre -10 °C et +70 °C ou installations mobiles. Pour les équipements renforcés (H), l'humidité relative peut atteindre 95 % et la température de fonctionnement peut être comprise entre -25 °C et +70 °C.

S

SNTP:

Acronyme de *simple network time protocol* (protocole de temps réseau simple). Voir NTP.

T

Trap (déroutement):

Un déroutement est un événement dirigé par un agent SNMP qui indique l'un des événements suivants :

- L'état d'un agent a changé.
- Un équipement gestionnaire SNMP non autorisé a tenté d'obtenir (ou de modifier) des données d'un agent SMTP.

Index

V

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Les normes, spécifications et conceptions pouvant changer de temps à autre, veuillez demander la confirmation des informations figurant dans cette publication.

PHA83351.03