Modicon M580

Module intégré OPC UA BMENUA0100

Guide d'installation et de configuration

Traduction de la notice originale

06/2024

PHA83351.04

www.se.com

Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs.

Ce document et son contenu sont protégés par les lois sur la propriété intellectuelle applicables et sont fournis à titre d'information uniquement. Aucune partie de ce document ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), à quelque fin que ce soit, sans l'autorisation écrite préalable de Schneider Electric.

Schneider Electric n'accorde aucun droit ni aucune licence d'utilisation commerciale de ce document ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

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 :

(En cas de divergence ou de contradiction entre une traduction et l'original anglais, le texte original en anglais prévaudra.)

- 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.
- L’opérateur ne doit avoir accès qu’aux réglages fonctionnels dont il a besoin. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

À 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 servent uniquement à illustrer les procédures décrites. Votre propre configuration peut nécessiter des réglages différents de ceux fournis dans les exemples.

Champ d'application

Ce document s'applique à un système M580 utilisé avec EcoStruxure™ Control Expert 16.0 ou toute version de support ultérieure.

Les caractéristiques des produits décrits dans ce document sont censées correspondre aux caractéristiques disponibles sur www.se.com. Toutefois, en application de notre stratégie 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 les caractéristiques figurant dans ce document et celles fournies sur www.se.com, considérez que le site www.se.com contient les informations les plus récentes.

Document(s) à consulter

Titre de documentation	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), EIO0000002730 (italien), EIO0000002729 (espagnol), EIO0000002731 (chinois)

Titre de documentation	Référence
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) 33002442 (espagnol) 33003702 (italien) 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 documentation	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) EIO0000002003 (espagnol) EIO0000002002 (italien) EIO0000002004 (chinois)

Pour rechercher des documents en ligne, visitez le centre de téléchargement Schneider Electric (www.se.com/ww/en/download/).

Information spécifique au produit

⚠ DANGER

RISQUE DE CHOC ÉLECTRIQUE, D'EXPLOSION OU D'ARC ÉLECTRIQUE

- Coupez toutes les alimentations de tous les équipements, y compris les équipements connectés, avant de retirer les caches ou les portes d'accès, ou avant d'installer ou de retirer des accessoires, matériels, câbles ou fils, sauf dans les cas de figure spécifiquement indiqués dans le guide de référence du matériel approprié à cet équipement.
- Utilisez toujours un appareil de mesure de tension réglé correctement pour vous assurer que l'alimentation est coupée conformément aux indications.
- Remettez en place et fixez tous les caches de protection, accessoires, matériels, câbles et fils et vérifiez que l'appareil est bien relié à la terre avant de le remettre sous tension.
- Utilisez uniquement la tension spécifiée pour faire fonctionner cet équipement et tout autre produit associé.

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

⚠AVERTISSEMENT

PERTE DE CONTROLE

- Réalisez une analyse des modes de défaillance et de leurs effets (FMEA) ou une analyse de risques équivalente sur l'application et appliquez les contrôles de prévention et de détection appropriés avant la mise en œuvre.
- Prévoyez un état de repli pour les événements ou séquences de commande indésirables.
- Le cas échéant, prévoyez des chemins de commande séparés et redondants.
- Définissez les paramètres appropriés, notamment pour les limites.
- Examinez les conséquences des retards de transmission et prenez les mesures correctives nécessaires.
- Examinez les conséquences des interruptions de la liaison de communication et prenez des mesures correctives nécessaires.
- Prévoyez des chemins indépendants pour les fonctions de commande critiques (arrêt d'urgence, dépassement de limites, conditions d'erreur, etc.) en fonction de votre évaluation des risques ainsi que des réglementations et consignes applicables.
- Appliquez les réglementations et consignes locales en matière de sécurité et de prévention des accidents.
- Testez chaque mise en œuvre d'un système pour vérifier son bon fonctionnement avant de l'utiliser en environnement de production.

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

⚠AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- N'utilisez que le logiciel approuvé par Schneider Electric pour faire fonctionner cet équipement.
- Mettez à jour votre programme d'application chaque fois que vous modifiez la configuration matérielle physique.

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

Terminologie utilisée dans les normes

Les termes techniques, la terminologie, les symboles et les descriptions correspondantes employés dans ce manuel ou figurant sur les produits eux-mêmes proviennent généralement des normes internationales.

Dans le domaine des systèmes de sécurité fonctionnelle, des variateurs et de l'automatisme en général, il s'agit par exemple de termes tels que *sécurité*, *fonction de sécurité*, *état sécurisé*, *défaut*, *réinitialisation de défaut*, *dysfonctionnement*, *panne*, *erreur*, *message d'erreur*, *dangereux*, etc.

Ces normes incluent entre autres les éléments suivants :

Norme	Description
IEC 61131-2:2007	Automates programmables, partie 2 : Spécifications et essais des équipements.
ISO 13849-1:2023	Sécurité des machines : Composants liés à la sécurité dans les systèmes de commande. Principes généraux de conception
EN 61496-1:2020	Sécurité des machines : Equipement de protection électrosensible. Partie 1 : Exigences générales et tests.
ISO 12100:2010	Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque
EN 60204-1:2006	Sécurité des machines - Equipement électrique des machines - Partie 1 : exigences générales
ISO 14119:2013	Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix
ISO 13850:2015	Sécurité des machines - Fonction d'arrêt d'urgence - Principes de conception
IEC 62061:2021	Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmables relatifs à la sécurité
IEC 61508-1:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Exigences générales.
IEC 61508-2:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Exigences concernant la sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité.
IEC 61508-3:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Configuration logicielle requise.
IEC 61784-3:2021	Réseaux de communication industriels - Profils - Partie 3 : Bus de terrain liés à la sécurité fonctionnelle - Règles générales et définitions de profil.
2006/42/EC	Directive Machines

Norme	Description
2014/30/EU	Directive sur la compatibilité électromagnétique
2014/35/EU	Directive sur les basses tensions

De plus, des termes utilisés dans le présent document peuvent provenir d'autres normes telles que :

Norme	Description
Série IEC 60034	Machines électriques rotatives
Série IEC 61800	Entraînements électriques de puissance à vitesse variable
Série IEC 61158	Communications numériques pour les systèmes de mesure et de commande – Bus de terrain utilisés dans les systèmes de commande industriels

Enfin, le terme *zone de fonctionnement* peut être utilisé dans le contexte de la description de dangers spécifiques et a la même signification que *zone à risque* ou *zone dangereuse* dans la directive *Machines* (*2006/42/EC*) et *ISO 12100:2010*.

NOTE: Les normes susmentionnées peuvent s'appliquer ou pas aux produits cités dans la présente documentation. Pour plus d'informations sur chacune des normes applicables aux produits décrits dans le présent document, consultez les tableaux de caractéristiques de ces références de produit.

Les marques

Windows est une marque déposée de Microsoft Corporation.

Terminologie non inclusive ou non sensible

En tant que membre d'un groupe d'entreprises responsables et inclusives, nous actualisons continuellement nos communications contenant une terminologie non inclusive. Cependant, tant que nous n'aurons pas terminé ce processus, nos contenus risquent toujours de contenir des termes standardisés du secteur d'industrie qui pourraient être jugés inappropriés par nos clients.

Caractéristiques du module BMENUA0100

Introduction

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

Fonctionnalités du module

Introduction

Le module de serveur OPC UA Modicon BMENUA0100 offre des fonctionnalités OPC UA hautes performances aux systèmes de contrôleurs Modicon M580.

OPC UA est une plate-forme de communication sécurisée et ouverte destinée aux communications industrielles. Elle est conçue pour être flexible et évolutive, depuis les capteurs IoT aux ressources restreintes sur le terrain jusqu'aux serveurs d'entreprise hébergés dans le datacenter ou le cloud. Outre la connexion aux données et leur transfert, OPC UA définit un modèle d'informations complet permettant la publication et la gestion des méta-informations et du contexte système, dans le but de simplifier l'ingénierie de l'automatisation et l'intégration des systèmes.

En établissant une norme de communication pour les opérations industrielles modernes et connectées, OPC UA fournit un lien commun entre les produits connectés des contrôleurs de terrain et les applications et analyses de l'entreprise. Sa conception vise à réaliser la compatibilité avec les infrastructures informatiques et de sécurité telles que les systèmes de pare-feu, de réseau VPN et de proxy. Le modèle OPC UA s'adapte aux besoins fonctionnels et de bande passante.

Fonctionnalités

Le module BMENUA0100 comprend 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 apporte les fonctionnalités suivantes à la plateforme Modicon M580 :

Fonctionnalités générales :

- Accès direct et optimisé au dictionnaire de données Control Expert pour le mappage entre Control Expert et variables OPC UA, page 49.
- Prise en charge des configurations à redondance d'UC (Hot Standby) via la redondance, page 53 OPC UA.
- Compatibilité avec les systèmes M580 liés à la sécurité, en tant que module non perturbateur de type 1 conformément à 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 129 NTP.
- Plusieurs méthodes de diagnostic : voyants, page 137, DDT, page 142, variables et éléments de données, page 154 OPC_UA, Syslog, page 158, Modbus, page 162, SNMP, page 163 et pages Web sécurisées, page 164.
- Mise à niveau du micrologiciel via Outil EcoStruxure™ Automation Device Maintenance, page 174.
- 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 95 OPC UA au niveau des modules configurable via HTTPS.
- Capacité à contrôler les flux de communication entrant et sortant en activant et en désactivant des services de communication, page 97.
- IPsec, page 103 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 principal IPsec. 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 pour les systèmes Windows 7, 10 et Windows Server 2016.

Gestion de l'authentification :

- Contrôle d'accès basé sur des rôles (RBAC) et authentification des utilisateurs , page 115 pour les clients HTTPS et OPC UA.
- Certificats, page 107 pour entités d'application client OPC UA.

Principales fonctionnalités du module de communication M580 :

- 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 horaire entre client et serveur NTP, page 129.

Description du module

Introduction

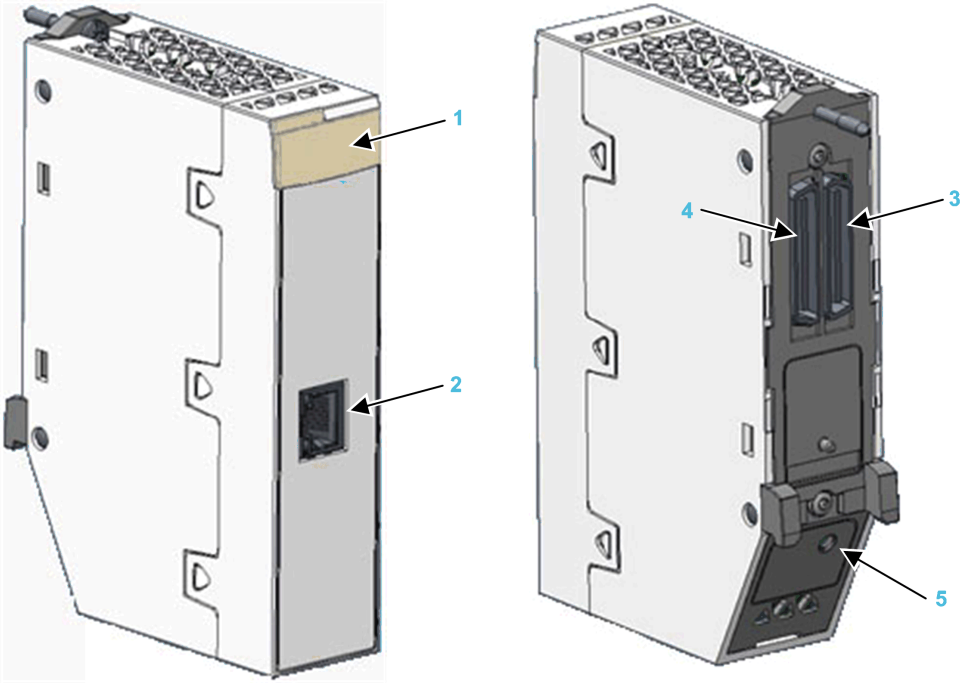
Schneider Electric propose deux modules de communication Ethernet avec serveur OPC UA intégré pour la communication avec les clients OPC UA, notamment SCADA :

- 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 62 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 voyants de liaison et d'activité Ethernet

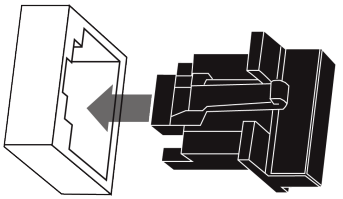
3 Port d'embase Ethernet

4 Port d'embase X Bus

5 Sélecteur rotatif du mode de fonctionnement de la cybersécurité

Consultez la rubrique Diagnostic des voyants, page 137 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 :

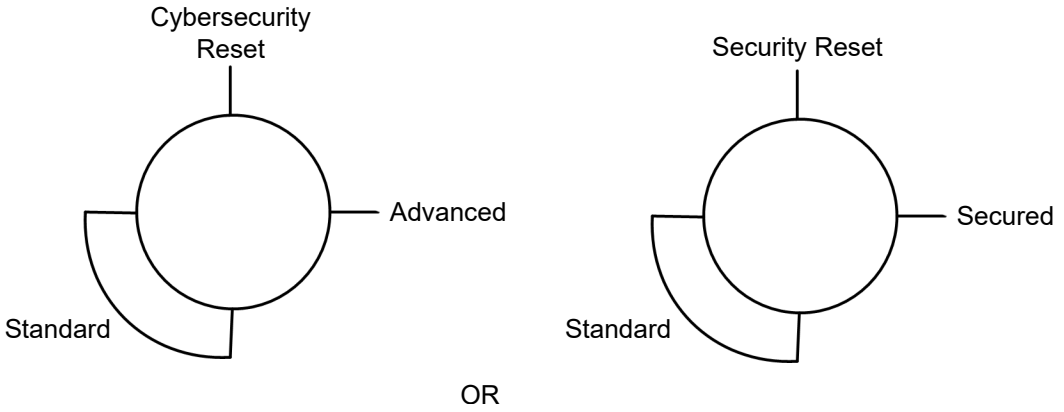
Port	Description
Port de contrôle	Le port de contrôle est le port unique situé à l'avant du module BMENUA0100. Voici ses principales caractéristiques : • Lorsque le port de contrôle est activé, c'est l'interface exclusivement utilisée pour les communications OPC UA, sauf si IPv6 est configuré. ◦ Lorsque 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 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 l'adressage IPv4 (32 bits) et IPv6 (128 bits) : ◦ Les types IPv4 et IPv6 sont tous les deux configurés pour le module. ◦ La configuration de l'adressage IPv6 peut être statique ou dynamique (via SLAAC). ◦ La configuration IPv4 par défaut, page 120 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 174 et la configuration de la cybersécurité, page 87. • 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 Ethernet du BMENUA0100 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 Ethernet Modbus TCP IPv4 vers le contrôleur : ◦ Le port d'embase Ethernet est exclusivement utilisé pour les diagnostics Modbus. • Port exclusif pour la configuration sans cybersécurité (IP, NTPv4, SNMPv1), via : ◦ Control Expert v14.1 et versions de prise en charge 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 174 et la configuration de la cybersécurité, page 87. ◦ NTPv4, SNMPv1/v3 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. **NOTE:** Aucune autre communication n'est établie via le port d'embase X Bus du module BMENUA0100.

Commutateur rotatif

Un commutateur rotatif à quatre positions est situé à l'arrière du module. Réglez ce commutateur rotatif pour configurer le mode du contrôleur

NOTE: Vous pouvez utiliser le tournevis en plastique fourni ou un outil équivalent pour changer la position du commutateur rotatif. Evitez d'utiliser des tournevis métalliques

Selon votre version du module, les positions du commutateur rotatif sont les suivantes :



Les réglages sont les suivants :

- Mode Advanced (RL 6 et versions ultérieures) ou Secured (versions antérieures à RL 6), page 30
- Mode Standard, page 30
- Mode Cybersecurity Reset (RL 6 et versions ultérieures) ou Security Reset (versions antérieures à RL 6), page 31

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 cette vérification.

Consultez la description des modes de fonctionnement de la cybersécurité, page 28 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	Etat de fonctionnement.
ERR	Erreurs détectées.
UACNX	Connexions OPC UA.
BS	Port d'embase.
NS	Port de contrôle.
SEC	Etat de la cybersécurité.
BUSY	Etat du dictionnaire de données

Consultez la rubrique Voyants de diagnostic, page 137 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 141 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 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 ou ultérieure**
1.01	Compatibilité totale	Seules les fonctions héritées de la version 1.01 sont prises en charge par le logiciel [1, 2, 3]
1.10	Compatibilité totale	Compatibilité totale

1. Si un module BMENUA0100 équipé du micrologiciel version 1.01 reçoit une application générée avec EcoStruxure™ Control Expert V15 où :
   - Le paramètre **Taux d'échantillonnage rapide** est **Activé** (dans l'onglet Configuration IP, page 121). Ce paramètre 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 131 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 132 BMENUA0100 pour que le gestionnaire SNMP puisse accéder à la base MIB SNMP.

NOTE: Les pages Web affichées pour le module BMENUA0100 dépendent de la version de micrologiciel du module (par exemple, version 1.01, 1.10 ou 2.01).

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.

Réglage du mode de fonctionnement de la cybersécurité

Introduction

Le module BMENUA0100 peut être configuré pour fonctionner en mode Advanced (ou Secured) ou en mode Standard. Le commutateur rotatif situé à l'arrière du module détermine le mode de fonctionnement.

Les trois positions du commutateur sont les suivantes :

- Mode Advanced (ou Secured)
- Mode Standard
- Cybersecurity (ou Security) Reset

NOTE:

- La configuration par défaut du module en usine est le mode Advanced (ou Secured).
- Vous pouvez afficher la position du commutateur rotatif dans les pages Web du module (il apparaît dans la page d'accueil, page 92).

Comme le sélecteur rotatif n'est pas accessible lorsque le module est inséré dans 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.

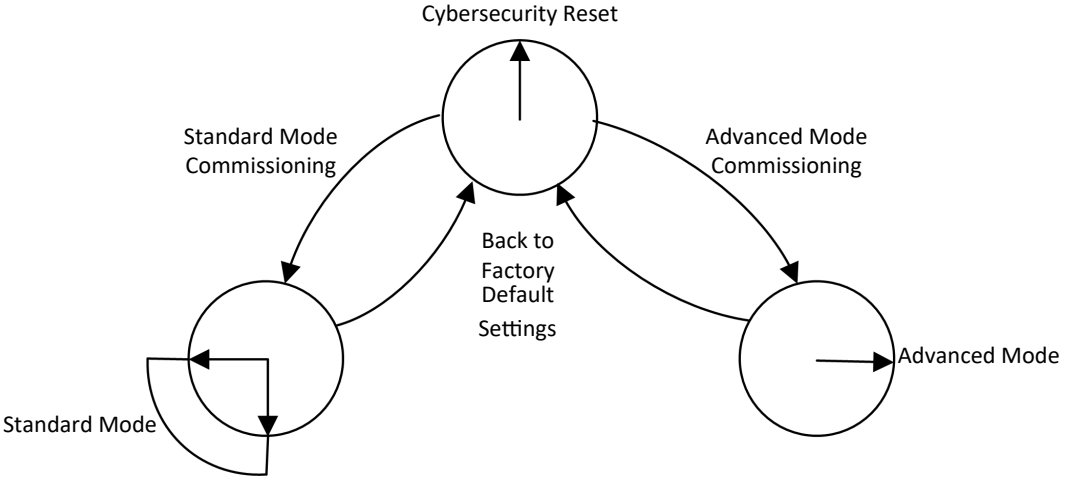
NOTE: Utilisez uniquement le petit tournevis en plastique fourni avec le module, page 23 pour changer la position du commutateur et configurer un mode de fonctionnement de la cybersécurité.

Changement de mode de fonctionnement

Un commutateur rotative à quatre positions est situé à l'arrière du module. Réglez ce commutateur.

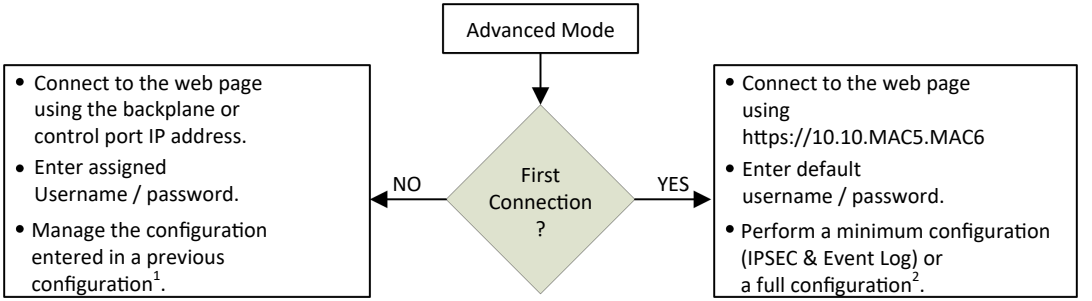
NOTE: Vous pouvez utiliser le tournevis en plastique fourni ou un outil équivalent pour changer la position du commutateur rotatif. Évitez d'utiliser des tournevis métalliques.

Selon votre version du module, les positions du commutateur rotatif sont les suivantes.



Un module neuf (avec les réglages par défaut d'usine) ou un module qui a subi une **Réinitialisation de la (cyber)sécurité** peut être mis en service pour fonctionner en mode Standard, page 83 ou en mode Advanced (ou Secured), page 81.

La procédure de configuration du module en mode de fonctionnement Advanced (ou Secured) varie selon qu'il s'agit ou non d'une première connexion aux paramètres de configuration du module après une réinitialisation de la cybersécurité (ou de la sécurité) :



1 Pour plus d'informations sur la gestion de configuration, reportez-vous au chapitre décrivant la configuration, page 87.

2 Pour plus d'informations sur la procédure de configuration lors d'une première connexion, reportez-vous à la section Mise en service en mode Advanced (ou Secured), page 81.

Mode Advanced (ou Secured)

En mode Advanced (ou 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 que le mode Advanced (ou Secured) est configuré, vous pouvez régler les paramètres de cybersécurité à l'aide des pages Web du module, page 87, accessibles via le protocole HTTPS sur les ports d'embase ou de contrôle. En mode Advanced (ou 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 119 à l'aide du logiciel de configuration Control Expert.

Mode Standard

Dans le mode Standard, les communications du module peuvent commencer sans configuration de cybersécurité préalable. Les paramètres de cybersécurité ne sont pas nécessaires et ne peuvent pas être configurés. Seuls l'adresse IP et d'autres paramètres disponibles dans Control Expert peuvent être configurés.

Cybersecurity (ou Security) Reset

La commande de **réinitialisation de la cybersécurité (ou de la sécurité)** restaure les paramètres de configuration par défaut définis en usine. Elle supprime toutes les configurations de cybersécurité, de listes autorisées, de certificats et de contrôle d'accès basé sur les rôles. Pour parachever l'opération de réinitialisation de la cybersécurité/sécurité, vous pouvez soit effectuer un cycle d'alimentation (hors/sous tension) du module BMENUA0100, soit retirer physiquement le module du rack (mise hors tension) et le réinsérer (mise sous tension). 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 fixement en vert et les services sont désactivés.

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

- Réglage à l'aide du commutateur rotatif : Le module cesse d'être fonctionnel pendant son extraction du rack, le réglage de son commutateur rotatif en position Advanced (ou Secured) ou Standard et sa réinsertion dans le rack. Certaines actions de configuration sont alors nécessaires.
- Réglage à l'aide des pages Web : A la fin du processus, procédez à un cycle hors/sous tension (ou un remplacement à chaud) du module en mode Standard ou Advanced (ou Secured). Les paramètres de cybersécurité et d'adresse IP doivent être configurés.

  NOTE: Après une réinitialisation de la cybersécurité (ou de la sécurité) du module BMENUA0100, ce dernier subit les conséquences suivantes :

  - 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 31.
    - Adresse IP par défaut 10.10.MAC5.MAC6, page 119.

  NOTE: Lorsque les deux derniers octets de l'adresse MAC (*MAC5.MAC6*) correspondent à *0.0* dans l'adresse par défaut, établissez une connexion câblée point à point entre votre ordinateur et le contrôleur, le module de communication ou un autre module.

Combinaison nom d'utilisateur/mot de passe par défaut

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

- Mode Advanced (ou Secured) : admin / password
- Mode Standard : installer / Inst@ller1

NOTE: Vous serez invité à modifier le mot de passe lors de la première utilisation en mode Advanced (ou Secured). Vérifiez que les lois et réglementations locales en vigueur l'exigent.

Fonctions prises en charge par les modes de fonctionnement Advanced (ou Secured) et Standard

Les fonctions suivantes sont prises en charge par le module BMENUA0100 dans les modes Advanced (ou Secured) et Standard

Mode	**Mode Standard**			**Mode Advanced (ou 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

Mode	**Mode Standard**			**Mode Advanced (ou Secured)**		
Port de contrôle	**Désactiver**	**Activer**		**Désactiver**	**Activer**	
Port Ethernet	**Embase**	**Embase**	**Port de contrôle**	**Embase**	**Embase**	**Port de contrôle**
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
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	Mode Standard			Mode Advanced (ou 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 (contrôleur inclus) (FTP, EIP explicite, Modbus, Ping) via IPv4 uniquement[5]	–	–	Transfert des flux de données Control Expert du réseau de contrôle vers le réseau d'équipements (toujours activé)	–	–	Transfert des flux de données Control Expert du réseau de contrôle vers le 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 133.
3. NTP V4 peut être configuré pour être transporté hors du tunnel IPsec.
4. Pour les modes de fonctionnement Standard et Advanced (ou Secured) de la cybersécurité, si les paramètres de sécurité sont réglés sur *Aucun*, il n'y a pas d'authentification des utilisateurs (le paramètre OPC UA, page 105 **Types de jeton d'identifiation d'utilisateur** est défini sur *Anonyme*).
5. Pour permettre à Control Expert d'accéder en ligne au contrôleur ou au réseau d'équipements, configurez le PC (sur lequel Control Expert est installé) avec une adresse IP appartenant au 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 dans 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	*CreateSession*	(Non applicable)	Code de résultat du service *Bad_TooManySessions* (échec pour cause de nombre excessif de sessions)
Temporisation de session minimale	30 s	*CreateSession*	Temporisation de session demandée	Temporisation de session révisée
Temporisation de session cumulée	3600 s	*CreateSubscription*	Temporisation de session demandée	Temporisation de session révisée
Nombre maximum de souscriptions cumulé	40	*CreateSubscription*	(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]	*CreateSubscription*	Intervalle de publication demandé	Intervalle de publication révisé
Intervalle de publication maximum	10 s	*CreateSubscription*	Intervalle de publication demandé	Intervalle de publication révisé
Durée maximum de souscription	300 s	*CreateSubscription*	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	*CreateSubscription*	Nombre maximum de notifications par publication	Le nombre maximum de notifications par seconde est donc (1000 / intervalle de publication révisé) * 1000
Intervalle d'échantillonnage minimum	125 ms[1] 20 ms[2]	*CreateMonitoredtems*	Paramètres de surveillance - Intervalle d'échantillonnage	Intervalle d'échantillonnage révisé
Taille maximale de la file d'attente des messages	100	*CreateMonitoredtems*	Paramètres de surveillance - Taille de file d'attente	Taille de file d'attente révisée
Nombre maximal d'éléments surveillés (cumul)	50010 ou 35010[3, 4] 2010[2]	*CreateMonitoredtems*	(Non applicable)	Code de résultat du service *Bad_TooManyMonitoredItems*
Nombre maximum de souscriptions par session	4	–	–	–
Nombre maximum d'éléments surveillés par abonnement	25000	–	–	–

1. Si l'échantillonnage rapide est désactivé.

2. Si l'échantillonnage rapide est activé.

3. Si l'échantillonnage rapide est désactivé 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.

4. Si l'horodatage source est permis et activé, page 123, le maximum est 35010. S'il n'est pas activé, le maximum est 50010.

Serveur OPC UA

Introduction

Le module de communication Ethernet BMENUA0100 a pour objectif principal de fournir une voie de communication OPC UA sur Ethernet entre des contrôleurs M580 et des clients OPC UA. Les données de contrôleur M580 sont mappées à des variables du module

BMENUA0100 et mises à la disposition des clients OPC UA via la pile de communication du serveur OPC UA intégré au module BMENUA0100. Les clients OPC UA se connectent à la pile du serveur OPC UA intégré en utilisant 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 de client OPC UA simultanées pour la version 1.1 du micrologiciel (contre trois (3) connexions de 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 de fonctionnalité comprenant d'autres profils, facettes, groupes de conformité et unités de conformité.
- Facette : définition d'une fonctionnalité partielle.
- 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 disposant de plus de 50 Mo de mémoire et d'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 à l'adresse : 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 centrales**:
  - **Facette de serveur central (Core Server) 2017** (http://opcfoundation.org/UA-Profile/Server/Core2017Facet)
- **Catégorie de serveur > Facettes > Accès aux données** :
  - **Facette de serveur complexe (ComplexType Server) 2017** (http://opcfoundation. org/UA-Profile/Server/ComplexTypes2017)
  - **Facette de serveur d'accès aux données (Data Access Server)** (http://opcfoundation.org/UA-Profile/Server/DataAccess)
  - **Facette de serveur d'abonnement aux 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 le 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 (Core Server) 2017

Comme indiqué sur le site Web OPC Foundation, la facette de serveur central 2017 "définit la fonctionnalité centrale 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, il est recommandé que les serveurs prennent en charge plusieurs profils de transport et de sécurité."

Vous trouverez une description complète de cette facette à l'adresse 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 afin d'optimiser l'accès aux noeuds utilisés de façon répétée dans l'espace d'adresses (AddressSpace) OPC UA des serveurs.
- 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)

Comme indiqué sur le site Web OPC Foundation, 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 étend la facette de serveur central (Core Server) comprenant la prise en charge du comportement de base de l'espace d'adresses (AddressSpace)."

Vous trouverez une description complète de cette facette à l'adresse http://opcfoundation.org/UA-Profile/Server/DataAccess.

Facette de serveur complexe 2017 (ComplexType Server)

Comme indiqué sur le site Web OPC Foundation, la facette de serveur complexe 2017 "complète la facette de serveur centrale (Core Server) pour inclure des variables aux données structurées, c'est-à-dire des données composées de plusieurs éléments tels qu'une structure et où les éléments individuels sont présentés en tant que 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. En option, le serveur peut prendre en charge d'autres codages, notamment XML lorsque le protocole binaire est actuellement utilisé et vice-versa."

Vous trouverez une description complète de cette facette à l'adresse 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

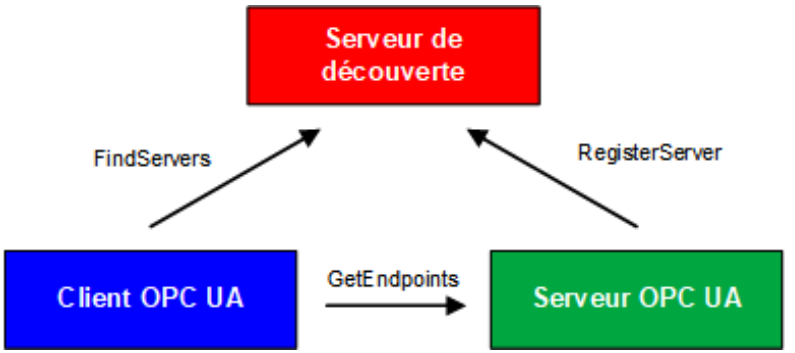
    - 4840 = numéro de port opcua-tcp configuré dans Control Expert
  - Pour IPv6 : opc.tcp://[2a01:cb05:431:f00:200:aff:fe02:a0a]:50000, où :

    - 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 40. L'implémentation sur le module BMENUA0100 prend en charge les services suivants :

- FindServers : Ce service implémenté dans la pile de serveur OPC UA du module BMENUA0100 recherche des serveurs sur le serveur OPC UA local uniquement.
- GetEndpoints : Renvoie les points de terminaison (Endpoints) pris en charge par un serveur et les informations de configuration requises pour établir un canal sécurisé (SecureChannel) et une Session. Peut fournir une liste de points de terminaison filtrée par profil.

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 40. 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 la session de façon unique :
  - 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 d'abonnement. Cette fonction permet à la pile OPC UA intégrée au module BMENUA0100 de fournir des services de publication/souscription d'abonnement qui sont utilisés lorsque le module se connecte aux équipements distants.

Un client OPC UA peut souscrire à un ou plusieurs noeuds sélectionnés et laisser le serveur surveiller ces éléments. En cas d'événement de modification (changement de valeur, par exemple), le serveur informe le client du changement. Ce mécanisme réduit considérablement la quantité de données transférées et représente donc une économie significative de la bande passante.

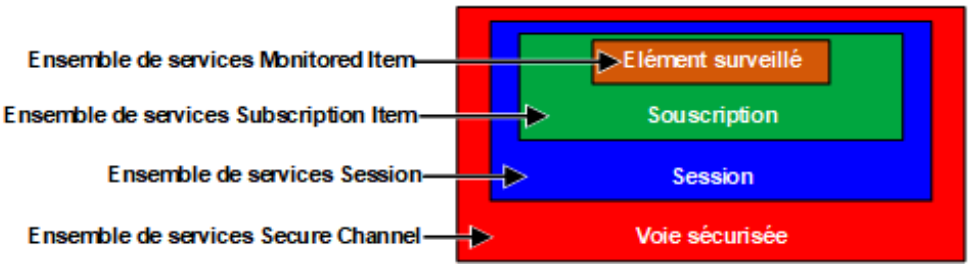
Un client OPC UA peut souscrire à un ou plusieurs types d'informations fournis par un serveur OPC UA. La souscription regroupe ces types de données, appelés éléments surveillés, pour constituer un ensemble de données appelées Notification.

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 :



Abonnements et dépassements

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

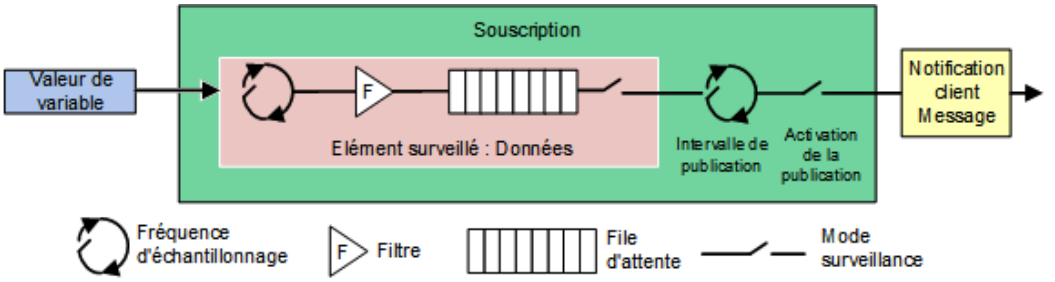
Lorsque vous définissez un intervalle de publication, tenez compte du nombre de clients et de requêtes client que le serveur doit gérer. Lorsque vous déterminez le nombre de requêtes client, vérifiez que tous les clients fonctionnent en ligne. A cet égard, notez que certains clients peuvent prendre 2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

NOTE: Définissez un intervalle de publication au moins égal à deux fois l'intervalle d'échantillonnage pour éviter de manquer des changements de données.

Evénements de changement

Un client peut souscrire 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 l'abonnement souscrit. Il s'agit de la fréquence à laquelle le serveur vérifie si la source de données a subi des modifications. Pour un élément de variable donné, l'intervalle d'échantillonnage peut être plus petit (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 données récentes.

- Filtre : ensemble de critères utilisés pour identifier les modifications de données ou les événements à signaler et à bloquer.
- Mode de surveillance : permet d'activer ou de désactiver l'échantillonnage des données et leur signalement.

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 d'abonnement aux modifications de données intégrée

Comme indiqué sur le site Web OPC Foundation, la facette de serveur d'abonnement aux modifications de données intégrée définit le niveau minimal de prise en charge des notifications de modification de données au sein des abonnements. Ce niveau comprend des 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 adaptée à une plate-forme telle que celle fournie par le profil de serveur d'équipements intégré Micro où la mémoire est limitée et doit être gérée.

Vous trouverez une description complète de cette facette à l'adresse 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 :

NOTE: Vous trouverez une description de ces services et ensembles de services dans la *Spécification OPC Unified Architecture, partie 4 : Services (édition 1.04)*.

- CreateMonitoredItems : Appel asynchrone qui permet de créer et d'ajouter un ou plusieurs éléments surveillés (MonitoredItems) à un abonnement.
- ModifyMonitoredItems : Appel asynchrone qui permet de modifier des éléments surveillés. Ce service est utilisé pour modifier les éléments surveillés d'un abonnement. Les modifications apportées aux paramètres MonitoredItem sont appliquées immédiatement par le serveur.
- 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 :

NOTE: Vous trouverez une description de ces services et ensembles de services dans la *Spécification OPC Unified Architecture, partie 4 : Services (édition 1.04)*.

- CreateSubscription : Appel asynchrone pour créer un abonnement.
- ModifySubscription : Appel asynchrone pour modifier un abonnement. Le serveur applique immédiatement les modifications à l'abonnement.
- DeleteSubscription : Appel asynchrone pour supprimer un ou plusieurs abonnements 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.

Découverte des variables du contrôleur

Mappage entre variables de contrôleur 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 rechercher et détecter les variables d'application du contrôleur 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 171.

Les variables collectées sont converties du modèle de logique de données de Control Expert dans le modèle de logique de données OPC UA à l'aide des services de pile OPC UA appropriés. Un client OPC UA connecté au module BMENUA0100 (sur son port de contrôle ou sur son port d'embase via le contrôleur ou un module de communication BMENOC0301 ou BMENOC0311) peut récupérer cet ensemble de données à l'aide des services de la facette de serveur d'accès aux données, page 40 prise en charge par le profil de serveur UA 2017 intégré, page 37.

Préchargement du dictionnaire de données pour éviter les interruptions de communication

Une modification d'application en ligne effectuée avec Control Expert interrompt temporairement la communication serveur/client OPC UA pendant que le serveur récupère un dictionnaire de données mis à jour. Cette interruption est due à un mappage incohérent des données du contrôleur lors de la mise à jour du dictionnaire de données. Tant que la communication est interrompue, l'état des noeuds surveillés (indiqué par UA Expert) est en erreur (**erreur de communication** ou **pas de communication** ou **dépassement de délai**). Pour éviter cette interruption des communications et ses conséquences, un mécanisme de synchronisation peut être mis en place entre le module BMENUA0100 et le logiciel de configuration Control Expert sur la base d'un préchargement du dictionnaire de données mis à jour.

Cette fonctionnalité est activée dans Control Expert sous **Outils > Options du projet...**, zone **Général > Données intégrées de l'automate**, à l'aide de **Préchargement lors de la génération** et **Délai de génération effectif** (voir EcoStruxure™ Control Expert, Modes de fonctionnement). Reportez-vous à l'aide en ligne de Control Expert pour plus d'informations sur la configuration de cette fonctionnalité.

Activation du dictionnaire de données

Pour activer le dictionnaire de données dans Control Expert :

Etape	Action
1	Dans Control Expert, le projet ouvert, sélectionnez **Outils > Paramètres du projet**.
2	Dans la fenêtre **Options 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
WORD	UInt16
DWORD	UInt32
DATE*	UInt32
TIME*	UInt32
TOD*	UInt32
DT*	Double
STRING	ByteString
* 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	20170517 hex
TIME	T#07h44m01s100ms	UInt32	27841100
TOD	TOD#07:44:01	UInt32	07440100 hex
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 les variables, le client OPC UA n'accède pas directement à une variable détectée de la logique de données du contrôleur. Le client accède à la variable de contrôleur détectée par le biais d'une variable de la logique de données OPC UA qui existe dans le module BMENUA0100 et qui est mappée à la variable de contrôleur sous-jacente. En raison de la nature indirecte 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 contrôleur.

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.

Exemples de variables de contrôleur Control Expert détectables par le serveur OPC UA du 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 :

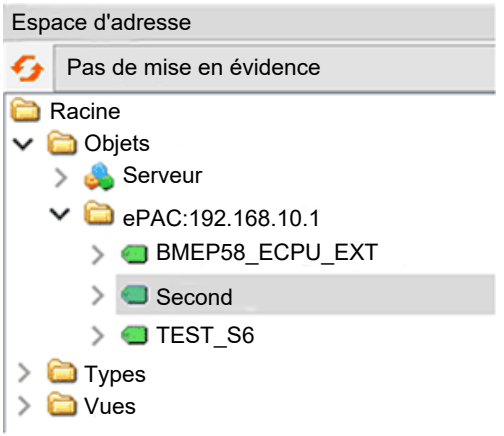
- Variables d'E/S topologiques :
  - Entrées : %I, %IW, %ID, %IF.
  - Sorties : %Q, %QW, %QD, %QF.
- Variables localisées : %M, %MW, %MD, %MF.
- Variables système : %S, %SW, %SD.

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

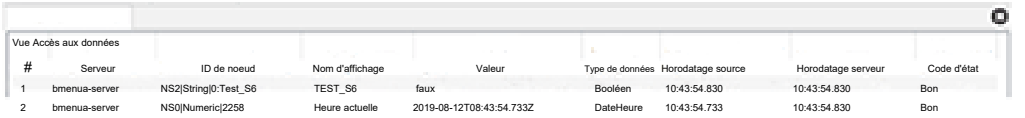
Le serveur OPC UA du module BMENUA0100 peut organiser et afficher sous forme graphique les variables de contrôleur détectées. Un outil client OPC UA peut se connecter au module BMENUA0100 et afficher une arborescence des variables du serveur OPC UA.

Dans l'exemple suivant, un client OPC UA (en l'occurrence, UaExpert) connecté au module BMENUA0100 peut afficher les variables du contrôleur dans les fenêtres **Espace d'adresse**. L'adresse IP du contrôleur 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 du contrôleur M580 qui est instancié automatiquement lors de l'ajout du contrôleur à l'application Control Expert. Les noeuds suivants représentent d'autres objets ajoutés à l'application.

A l'aide de l'outil client OPC UA, le noeud TEST_S6 a été déplacé et déposé dans la **vue d'accès aux données** de l'outil qui affiche les détails de la variable :


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 de la variable est *Boolean* (indiquant que le type de données de contrôleur sous-jacent est BOOL) et sa valeur est *false*.

NOTE: L'attribut d'**horodatage du serveur** des noeuds OPC UA est reçu depuis le serveur OPC UA du BMENUA0100 au format UTC (Universal Time Coordinated). Il est affiché en heure locale.

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 à redondance d'UC (Hot Standby), qui décrit des contrôleurs redondants.
- 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, suit le principe OPC UA de "redondance de serveur non transparente en mode de basculement à chaud" tel que défini par OPC Foundation.

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

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

Redondance OPC UA

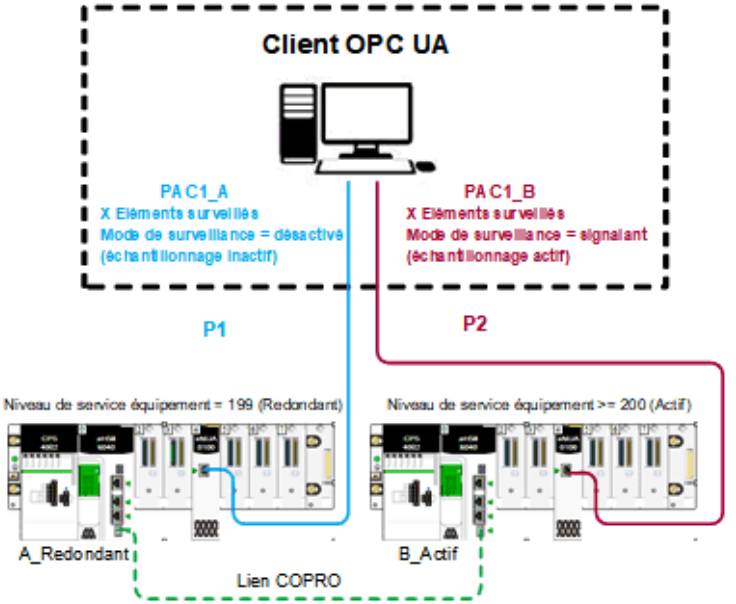
Dans une architecture à redondance de serveur OPC UA non transparente en mode de basculement à chaud, le client OPC UA établit les sessions et gère les communications avec les serveurs redondants. Les sessions à établir comprennent une session active avec le serveur primaire et une session inactive avec le serveur secondaire (redondant). Le client doit être configuré pour ces deux sessions de façon à inclure les mêmes éléments surveillés.

Le client OPC UA vérifie l'état des deux serveurs via la variable SERVICE_LEVEL et bascule 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 OPC UA.

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 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: Dans un système à redondance d'UC, vérifiez que les modules BMENUA0100 des contrôleurs primaire et redondant :

- sont configurés avec les mêmes paramètres de cybersécurité, page 87,
- ont leur sélecteur rotatif, page 23 (situé à l'arrière du module) sur la même position,
- sont installés dans le même numéro de logement, page 63 dans leur rack principal local respectif.

Si ces conditions ne sont pas remplies, le module ne peut pas récupérer sa configuration définie par Control Expert et stockée dans le contrôleur. Il va donc démarrer en mode autonome. Le système n'effectue pas automatiquement ces vérifications.

Le DDT du module BMENUA0100 inclut la variable SERVICE_LEVEL, page 154 qui fournit au contrôleur les 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 la fonction élémentaire READ_DDT en vue de mettre à jour le DDT de chaque module BMENUA0100. Dans une configuration à redondance d'UC (Hot Standby), ajoutez la fonction READ_DDT à une section de code qui s'exécute lorsque le contrôleur est en mode redondant. Cette conception renvoie les informations de diagnostic de BMENUA0100 qui peuvent être échangées entre les contrôleurs primaire et redondant. L'application peut utiliser ces informations pour vérifier la cohérence des services pris en charge et des configurations de la cybersécurité pour les modules BMENUA0100 des contrôleurs primaire et redondant.

Si le DDT T_M_ECPU_HSBY (voir Modicon M580 - Redondance d'UC - Guide de planification du système pour les architectures courantes) du contrôleur redondant 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 correcte dans le BMENUA0100.

Dans un système à redondance d'UC, 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 afin d'assurer la cohérence des valeurs des variables entre les contrôleurs primaire et redondant.

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

Dans quelques cas rares (principalement lorsque le bit ECPU_HSBY_1.PLCX_ONLINE est défini sur FALSE manuellement ou par programme), l'un des contrôleurs d'un système à redondance d'UC peut être en mode d'attente. Dans ce mode, le contrôleur (redondant) n'est pas synchronisé avec le contrôleur primaire et les variables qui y sont lues sont inexactes. L'état d'un contrôleur qui répond peut être surveillé via les champs suivant du DDT 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

Par ailleurs, le système à redondance d'UC permet aux deux contrôleur de fonctionner en exécutant des applications différentes. Pour assurer la cohérence des variables entre les contrôleurs primaire et redondant, la présentation des données des deux contrôleurs doit être cohérente, comme indiqué par le champ T_M_ECPU_HSBY du DDT :

- T_M_ECPU_HSBY_1.DATA_LAYOUT_MISMATCH = FALSE

  NOTE: Lorsque la redondance OPC UA est configurée, vérifiez par programme les DDT des modules pour vous assurer de la cohérence des services pris en charge et des configurations de cybersécurité entre les modules BMENUA0100.

Prise en charge de serveurs, clients et réseaux redondants dans OPC UA

Comme indiqué dans la partie 4 de la spécification OPC Unified Architecture : Services, édition 1.04 : OPC UA permet la redondance des serveurs, des clients et des réseaux. OPC UA fournit les structures de données et les services grâce auxquels la redondance peut être réalisée de manière 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 également coexister dans des systèmes avec redondance de réseaux et de clients...

La redondance des clients permet à des clients configurés de manière 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 également coexister dans 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 dans des systèmes avec redondance de clients et de serveurs... (OPC UA Partie 4, section 6.6.1.)

Redondance de serveurs

Comme indiqué dans la partie 4 de la spécification OPC Unified Architecture : Services, édition 1.04 : Les deux principaux modes de redondance de serveurs sont : transparent et non transparent.

En redondance transparente, le basculement des responsabilités de serveur d'un serveur à un 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.

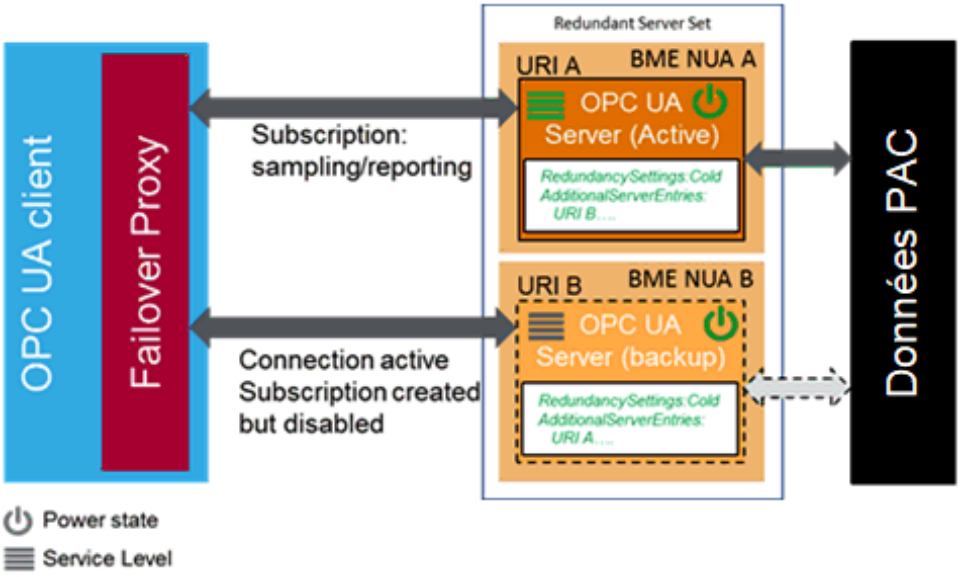
En mode non transparent, le basculement d'un serveur à un autre et les actions pour continuer à envoyer ou recevoir des données sont effectuées par le client. Le client doit connaître l'ensemble de serveurs redondants défini et doit effectuer les actions nécessaires pour bénéficier de la redondance de 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 Partie 4, section 6.6.2)

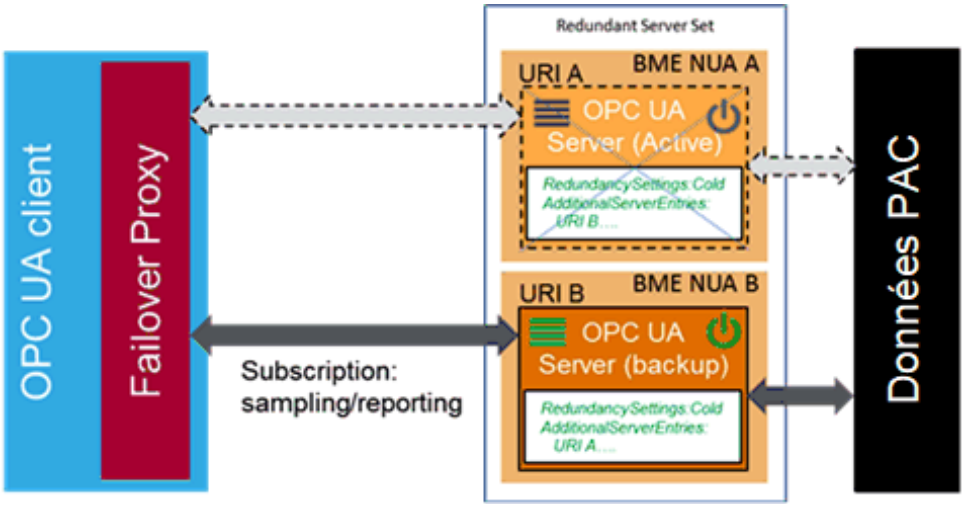
Comme indiqué ci-dessus, le serveur OPC UA intégré au module BMENUA0100 prend en charge la redondance de serveur non transparente en mode de basculement à chaud.

Mode de basculement à chaud des serveurs dans OPC UA

Comme indiqué dans la partie 4 de la spécification OPC Unified Architecture : Services, édition 1.04 : Dans le mode de basculement à chaud, le ou les serveurs de sauvegarde peuvent être actifs, mais ils ne peuvent pas se connecter aux points de données 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 Partie 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 :



Comportement du client lors d'un basculement

Comme indiqué dans la partie 4 de la spécification OPC Unified Architecture : Services, édition 1.04 : Chaque serveur gère une liste d'identifiants URI de tous les serveurs inclus dans l'ensemble de serveurs redondants défini (Redundant Server Set).

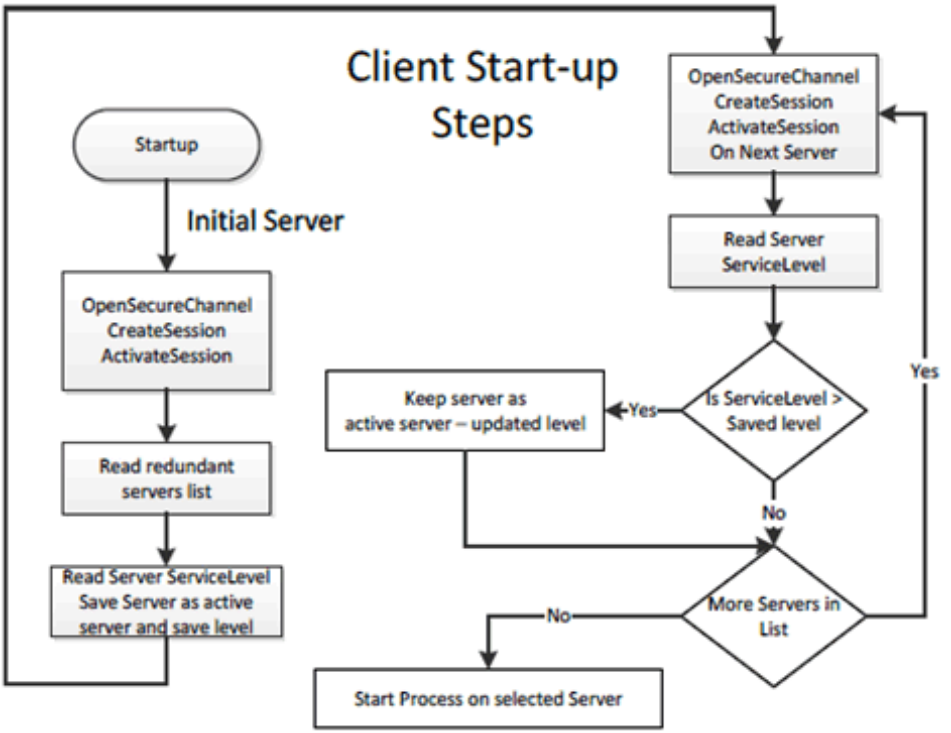
NOTE: Un ensemble Redundant Server Set inclut les serveurs OPC UA configurés pour assurer la redondance dans l'application Control Expert.

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 Partie 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 ruièrent 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 de Redundant Server Set.



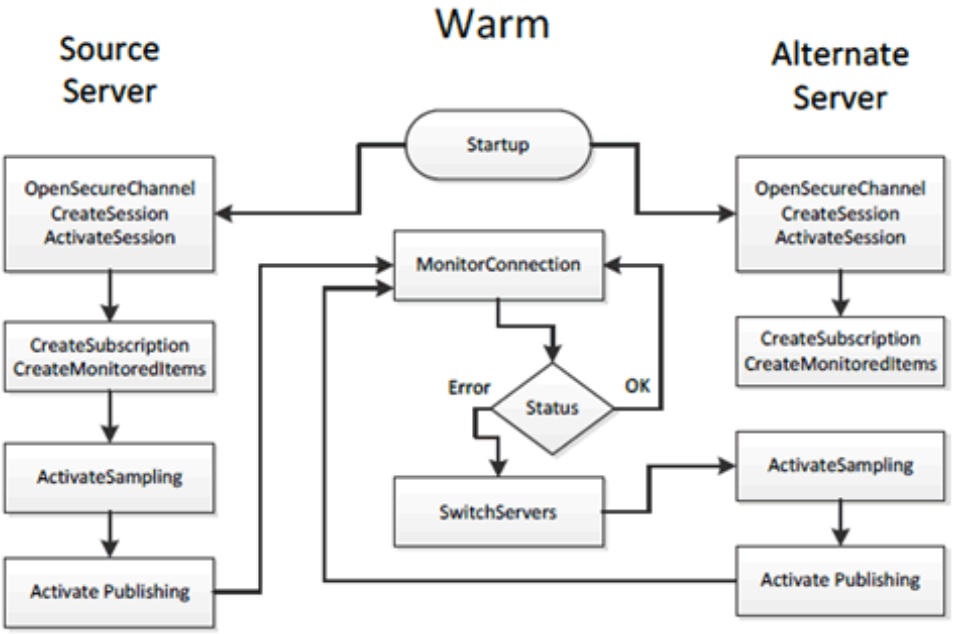
Le serveur initial peut être déterminé via la fonction de découverte standard ou via une liste de serveurs dans l'ensemble Redundant Server Set. Dans tous les cas, le client a besoin de vérifier à quel serveur de l'ensemble il doit se connecter. Les actions particulières dépendent du mode de basculement 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 Partie 4, section 6.6.2.4.5.1)

Mode de basculement à chaud du client OPC UA

Comme indiqué dans la partie 4 de la spécification OPC Unified Architecture : Services, édition 1.04 : 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 abonnements et des éléments surveillés (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 éléments MonitoredItem dans la réponse de publication (Publish), par exemple Bad_ NoCommunication. L'unique serveur actif peut être identifié par la 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 illustre les étapes effectuées par un client lors de la communication avec un serveur en utilisant le mode de basculement à chaud (Warm).



(OPC UA Partie 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 du rack principal local (c'est-à-dire dans le même rack que le contrôleur) dans les configurations suivantes :

- Configuration M580 autonome.
- Configuration M580 de contrôleur de sécurité autonome.
- Configuration M580 à redondance d'UC (Hot Standby)
- Configuration M580 de contrôleur de sécurité à redondance d'UC (Hot Standby).

NOTE:

- Le module BMENUA0100 peut être utilisé avec tous les contrôleurs 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 le réseau du port de contrôle et le réseau de l'embase du contrôleur de manière physique (via le câblage), pas seulement de manière logique (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 équipement 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) de version v1.2 ou ultérieure. Par exemple, Windows 7 peut nécessiter une mise à jour pour permettre à TLS 1.2 de mettre à niveau le micrologiciel du BMENUA0100 ou d'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). Vous pouvez également utiliser un routeur pour isoler les racks et éviter ainsi les conflits d'adresses potentiels 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 contrôleurs M580) configurés sur le même sous-réseau, utilisez des préfixes pour le nom d'équipement (ou de rôle) des équipements (y compris les contrôleurs M580). Cette convention de nom permet aux modules BMENUA0100 de différencier les contrôleurs M580 et de déterminer quel contrôleur est situé sur quel rack. Cette convention de nom contribue à éliminer l'incertitude liée à l'architecture de réseau plat. Par exemple, en l'absence de préfixes uniques, un module BMENUA0100 ne peut pas déterminer avec quel contrôleur 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 21.

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 dans le rack principal local pour les configurations standard et de sécurité autonome[1] et à redondance d'UC[1,2].
Contrôleur de sécurité	
Redondance d'UC	
Contrôleur de sécurité à redondance d'UC	

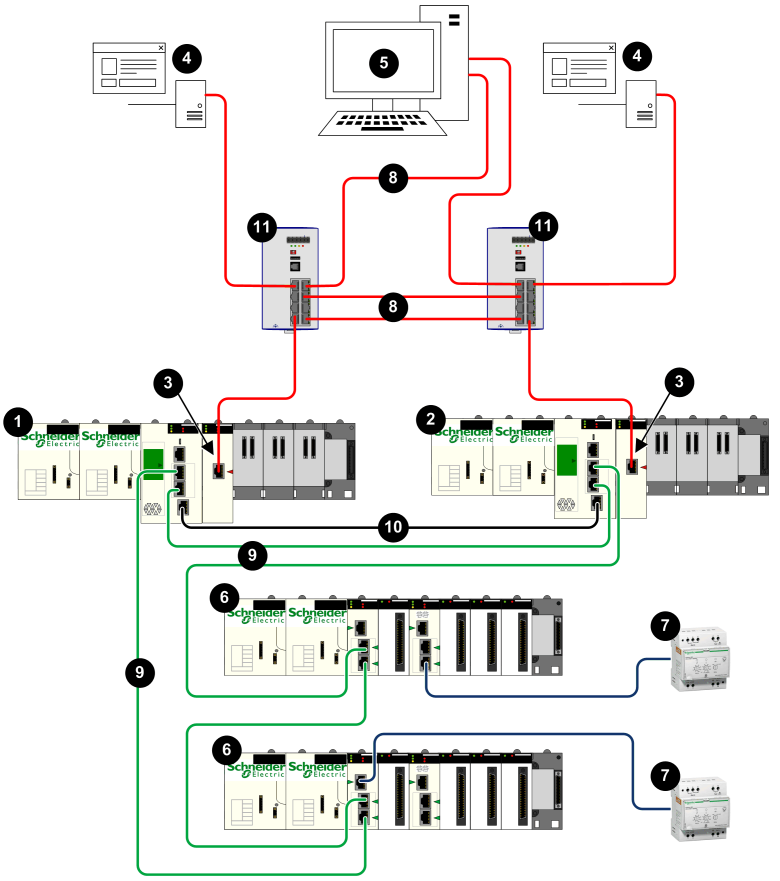
1. Quand deux modules BMENUA0100 sont utilisés dans un rack principal :
   - Les performances de chaque module seront plus lentes qu'avec l'utilisation d'un seul module.
   - Activez le port de contrôle dans la configuration des deux modules.
2. Dans les configurations à redondance d'UC, placez les modules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

Fonctionnalité CCOTF (Change Configuration On The Fly)

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

Réseau de contrôle isolé avec contrôleurs M580 à redondance d'UC

Architecture



1 Contrôleur à redondance d'UC primaire

2 Contrôleur à redondance d'UC redondant

3 Module de communication Ethernet BMENUA0100 à serveur OPC UA intégré

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 RIO Ethernet (9) (y compris le contrôleur) 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. En cas de communication via IPv6, les méthodes de configuration automatique d'adresse sans état (SLAAC) et d'adressage IP statique sont toutes les deux prises en charge.

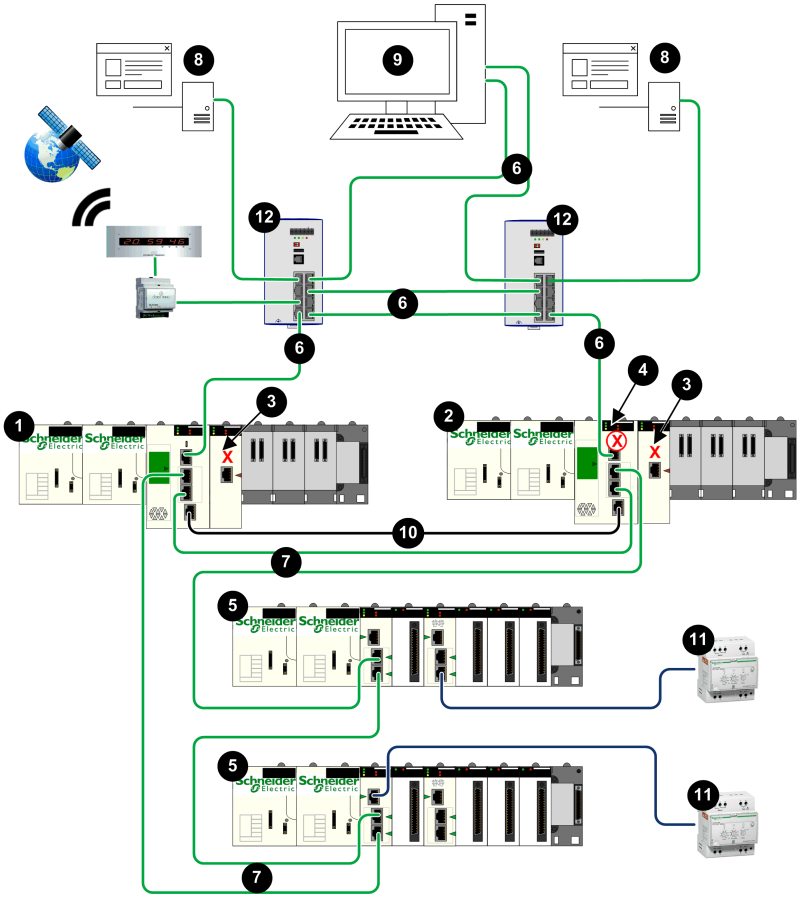
Le BMENUA0100 fournit la communication Modbus d'égal à égal entre les deux contrôleurs de redondance. Les ports du contrôleur assurent la connectivité aval avec les équipements Ethernet de l'anneau principal RIO Ethernet.

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 désigné par "A" est le serveur NTP primaire et le module BMENUA0100 désigné par "B" est le serveur NTP redondant. De cette manière, les horloges du contrôleur et du module BMENUA0100 sont synchronisées.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules d'horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont consommés par l'application exécutée dans le contrôleur, laquelle convertit les données d'enregistrement brutes et les stocke dans un format utilisable. Les enregistrements correctement formatés peuvent ensuite être utilisés par une application de supervision, par exemple un système SCADA.

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

Architecture



1 Contrôleur à redondance d'UC primaire
2 Contrôleur à redondance d'UC redondant
3 BMENUA0100 avec port de contrôle désactivé
4 Contrôleur redondant avec blocage automatique du port de service **5**
Station 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 entre des contrôleurs M580 à redondance d'UC et deux clients OPC UA (systèmes SCADA). Son objectif principal est de fournir la haute disponibilité aux contrôleurs 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 du BMENUA0100 est désactivé. La communication Ethernet IPv4 vers le module BMENUA0100 est fournie via le port d'embase. La communication amont entre les contrôleurs à redondance d'UC et les serveurs SCADA s'effectue via le port de service du contrôleur primaire. Les ports du contrôleur assurent la connectivité aval avec les équipements Ethernet de l'anneau principal RIO Ethernet.

Le port de service du contrôleur redondant (4) est désactivé via le logiciel de configuration Control Expert : option **Blocage automatique du port de service sur UC redondante** sélectionnée dans l'onglet **Port de service** de la configuration des deux contrôleurs primaire et redondant.

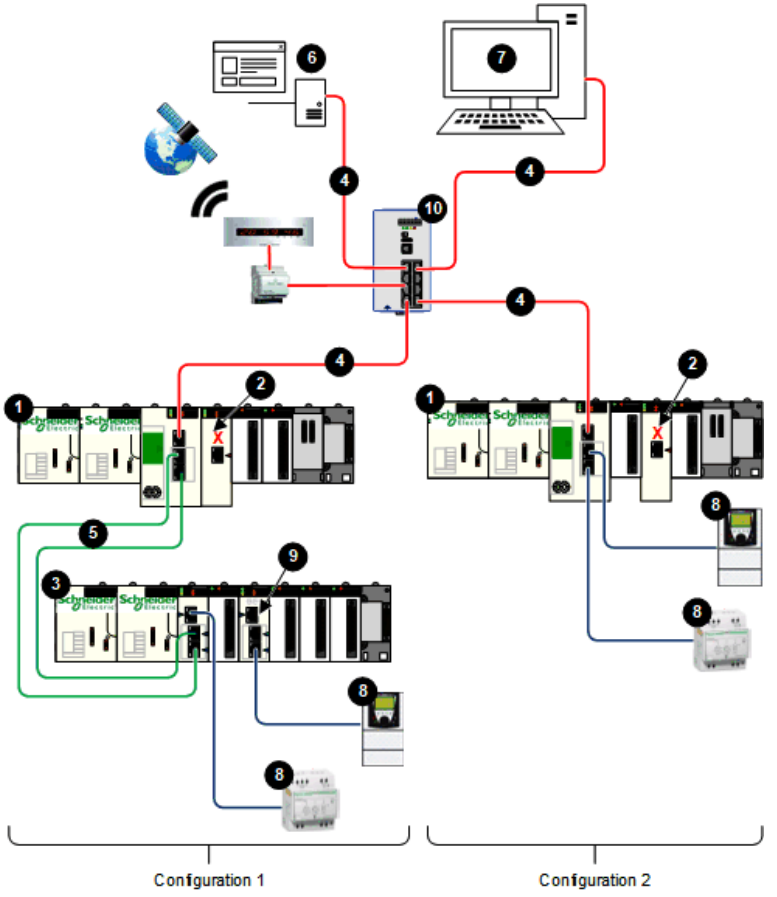
NOTE: Le port de service du contrôleur redondant (secondaire) est désactivé pour empêcher la création indésirable d'une boucle de communication Ethernet, où le réseau de contrôle et l'anneau principal RIO Ethernet font partie du même sous-réseau. Pour plus d'informations, reportez-vous au *Guide de planification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

Dans cette conception de réseau plat, tous les équipements (contrôleur, modules BMECRA31310 et module BMENUA0100 inclus) peuvent être clients du même serveur NTP situé dans le réseau de contrôle. L'horloge du contrôleur est donc synchronisée avec le module BMENUA0100.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules d'horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont consommés par l'application exécutée dans le contrôleur, laquelle convertit les données d'enregistrement brutes et les stocke dans un format utilisable. Les enregistrements correctement formatés peuvent ensuite être utilisés par une application de supervision, par exemple un système SCADA.

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

Architecture



1 Contrôleur autonome
2 BMENUA0100 avec port de contrôle désactivé
3 Station 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 seul client OPC UA (système SCADA) à partir de plusieurs contrôleurs M580 autonomes. Il s'agit d'une architecture à optimisation des coûts qui n'exige pas de 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 du BMENUA0100 est désactivé pour chaque contrôleur autonome. La communication Ethernet IPv4 vers le module BMENUA0100 est fournie via le port d'embase. La communication amont entre chaque contrôleur et l'unique serveur SCADA est établie via le port de service du contrôleur.

Dans la configuration 1, la connectivité aval entre le contrôleur et la station d'E/S distantes Ethernet X80 (4) est assurée par les deux ports de réseau d'équipements du contrôleur. Une connectivité aval est fournie entre le port de service du module BMECRA31310 et un commutateur BMENOS0300 (9) vers l'équipement Ethernet distribué.

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

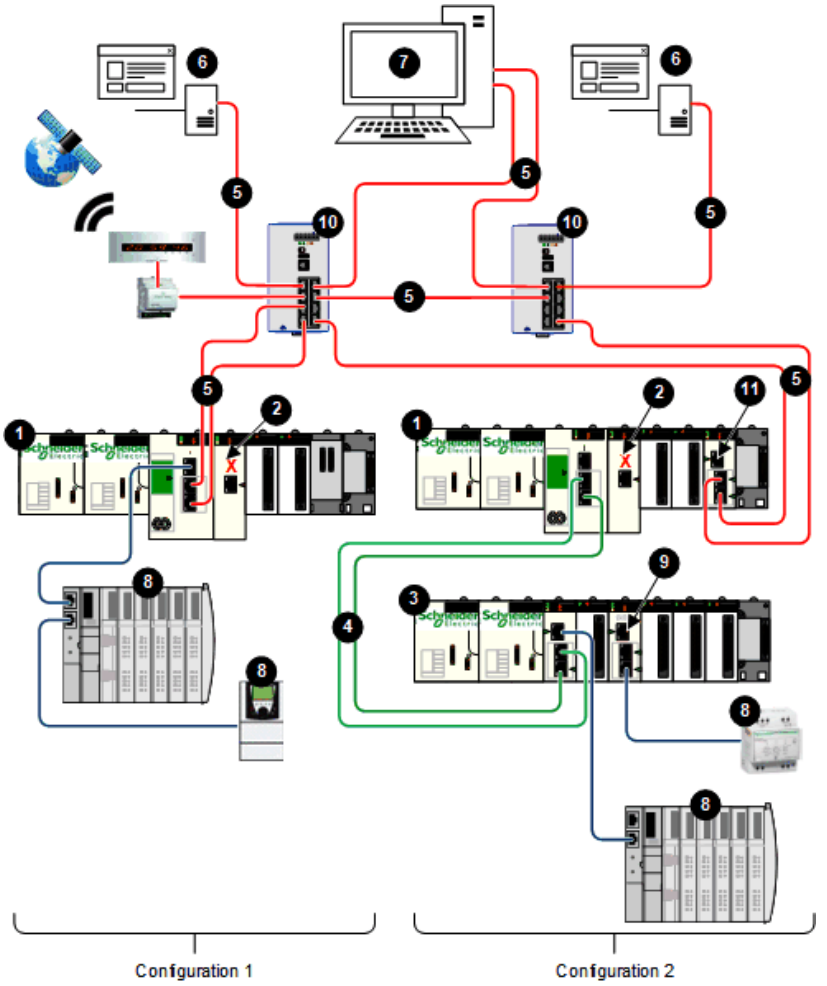
Dans cette conception de réseau plat, tous les équipements réseau (y compris le contrôleur, les modules BMECRA31310 et le BMENUA0100) sont des clients NTP d'un serveur NTP résidant dans le réseau de contrôle. Par conséquent, l'heure du contrôleur et l'heure du module BMENUA0100 sont synchronisées.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules d'horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont consommés par l'application exécutée dans le contrôleur,

laquelle convertit les données d'enregistrement brutes et les stocke dans un format utilisable. Les enregistrements correctement formatés peuvent ensuite être utilisés par une application de supervision, par exemple un système SCADA.

Réseau plat avec plusieurs contrôleurs M580 autonomes et SCADA redondant

Architecture



1 Contrôleur autonome
2 BMENUA0100 avec port de contrôle désactivé
3 Station 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, BMENOC0301 ou BMENOC0311

Description

Cette architecture assure une haute disponibilité du réseau de contrôle via des connexions redondantes entre les clients OPC UA (systèmes SCADA) et les contrôleurs 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 du BMENUA0100 est désactivé pour chaque contrôleur autonome. La communication Ethernet IPv4 vers le module BMENUA0100 est fournie via le port d'embase.

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

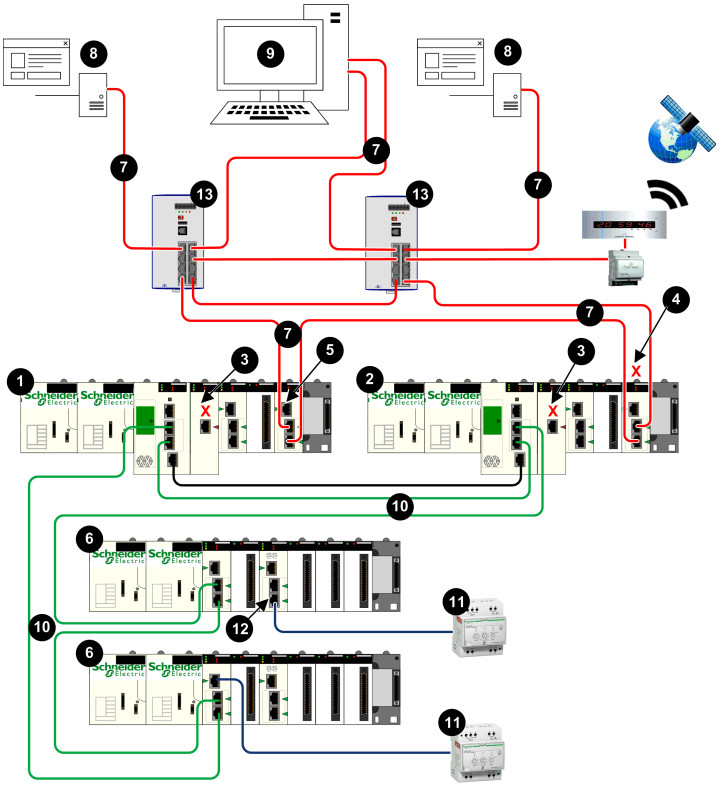
Dans la configuration 2, la connectivité amont vers les serveurs SCADA est fournie par les ports de réseau d'équipements d'un module BMENOS0300, BMENOC0301 ou BMENOC0311. Le protocole de redondance RSTP est utilisé pour attribuer des rôles à chaque port afin d'éviter les boucles Ethernet logiques. La connectivité en aval du contrôleur avec la station d'E/S distantes Ethernet X80 est assurée par les ports de réseau d'équipements du contrôleur. La connectivité aval vers les équipements Ethernet distribués est assurée par le port de service du module BMECRA31310 et un commutateur BMENOS0300 (9).

Dans cette conception de réseau plat, tous les équipements réseau (y compris le contrôleur, les modules BMECRA31310 et le BMENUA0100) sont des clients NTP d'un serveur NTP résidant dans le réseau de contrôle. Par conséquent, l'heure du contrôleur et l'heure du module BMENUA0100 sont synchronisées.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules d'horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont consommés par l'application exécutée dans le contrôleur, laquelle convertit les données d'enregistrement brutes et les stocke dans un format utilisable. Les enregistrements correctement formatés peuvent ensuite être utilisés par une application de supervision, par exemple un système SCADA.

Réseau plat avec redondance des contrôleurs M580 et du système SCADA

Architecture



1 Contrôleur à redondance d'UC primaire
2 Contrôleur à redondance d'UC redondant
3 BMENUA0100 avec port de contrôle désactivé
4 BMENOS0300, BMENOC0301 ou BMENOC0311 avec port d'embase désactivé
5 BMENOS0300, BMENOC0301 ou BMENOC0311 avec port d'embase activé
6 Station 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 des clients OPC UA redondants (systèmes SCADA) à des contrôleurs redondants dans un même sous-réseau.

Chaque contrôleur est connecté à SCADA via un module BMENOS0300, BMENOC0301 ou BMENOC0311. Pour éviter les boucles Ethernet, le port d'embase d'un des modules BMENOS0300, BMENOC0301 ou BMENOC0311 est désactivé. Dans cet exemple, le port d'embase est désactivé sur le module situé dans le contrôleur redondant (4). En outre, le protocole de redondance RSTP est utilisé pour attribuer des rôles à chaque port afin d'empêcher les boucles Ethernet logiques.

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

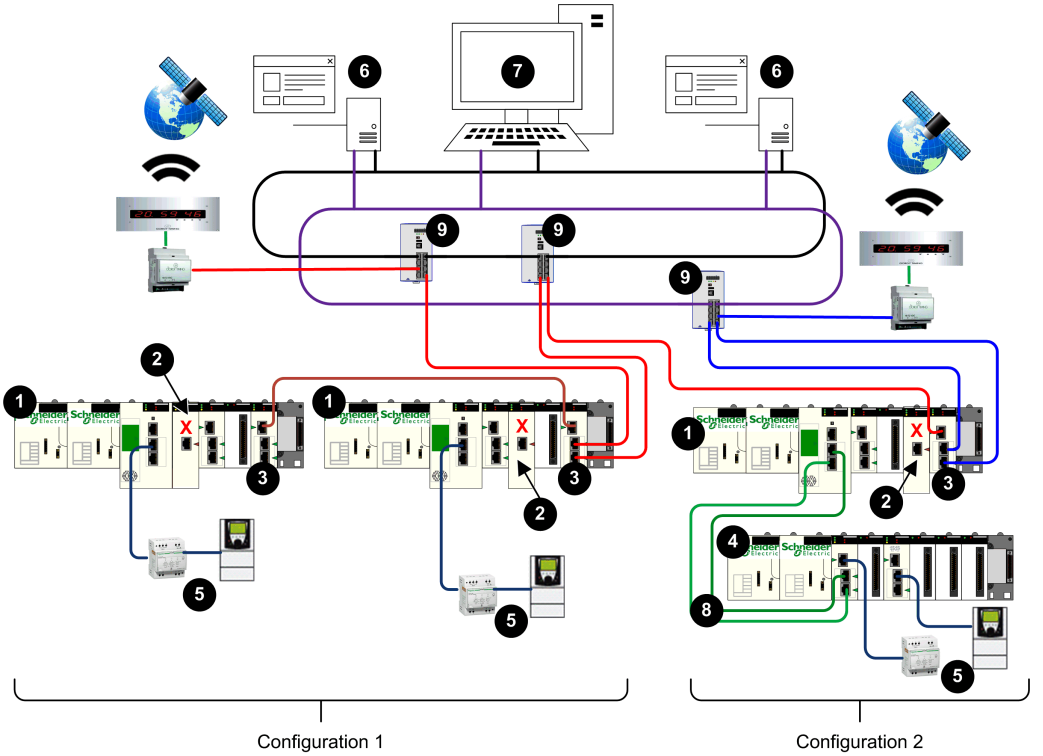
La connectivité aval aux stations d'E/S distantes (RIO) Ethernet X80 est fournie par les ports de réseau d'équipements des contrôleurs. La connectivité aval entre les stations RIO Ethernet X80 et l'équipement Ethernet distribué est fournie à la fois par le port de service du module CRA et un commutateur BMENOS0300 (12).

Dans cette conception de réseau plat, tous les équipements réseau (y compris chaque contrôleur à redondance d'UC et chaque module BMENUA0100) sont des clients NTP d'un serveur NTP qui réside dans le réseau de contrôle. Par conséquent, l'heure du contrôleur et l'heure du module BMENUA0100 sont synchronisées.

Le BMENUA0100 prend en charge l'horodatage applicatif. Dans ce processus, les modules d'horodatage enregistrent les événements dans leur mémoire tampon locale. Ces événements horodatés sont consommés par l'application exécutée dans le contrôleur, laquelle convertit les données d'enregistrement brutes et les stocke dans un format utilisable. Les enregistrements correctement formatés peuvent ensuite être utilisés par une application de supervision, par exemple un système SCADA.

Réseau hiérarchique avec plusieurs contrôleurs M580 autonomes connectés à un réseau de contrôle et un système SCADA redondant

Architecture



1 Contrôleur 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)

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 amont entre les contrôleurs et les clients OPC UA (systèmes SCADA) est établie via les deux ports de réseau d'équipements du module BMENOC0321 en utilisant le protocole de redondance RSTP pour éviter les boucles Ethernet logiques.

NOTE: Cette architecture nécessite la configuration de routes statiques dans l'équipement du réseau de contrôle pour rediriger les différents sous-réseaux des contrôleurs.

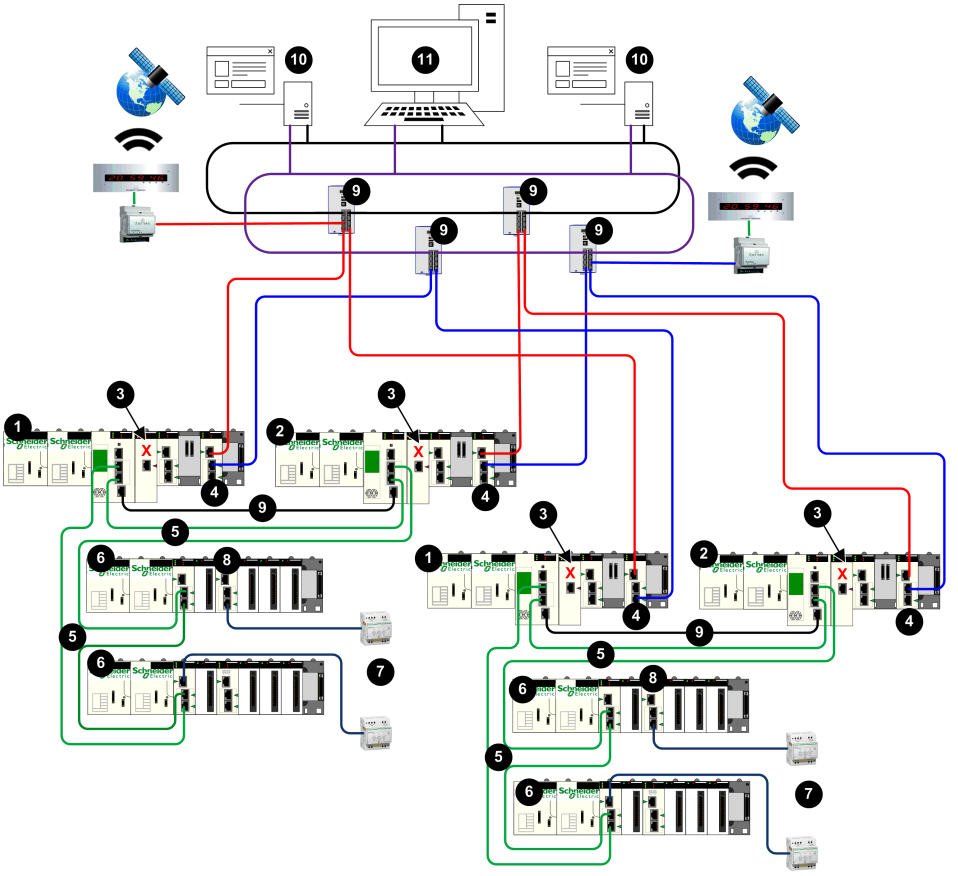
Le port de contrôle du BMENUA0100 (2) est désactivé pour chaque contrôleur autonome. La communication Ethernet IPv4 vers le module BMENUA0100 est fournie via le port d'embase.

La configuration 1 comprend deux contrôleurs qui résident dans le même sous-réseau. Dans cette configuration, le module BMENOC0321 assure les communications amont redondantes avec les serveurs SCADA redondants. Le module BMENOC0321 utilise le protocole de redondance RSTP pour éviter les boucles Ethernet logiques. Les deux ports de réseau d'équipement de chaque contrôleur assurent la communication aval avec les équipements Ethernet distribués.

La configuration 2 comprend un seul contrôleur avec une station RIO Ethernet X80. Ce contrôleur s'appuie sur le module BMENOC0321 pour la communication amont vers les serveurs SCADA redondants. Le BMENOC0321 utilise pour cela deux sous-réseaux indépendants. La communication aval depuis la station RIO Ethernet X80 vers des équipements Ethernet distribués est assurée à la fois par le port de service du module BMECRA31310 et un commutateur BMENOS0300.

Réseau hiérarchique avec plusieurs contrôleurs M580 de redondance d'UC et des connexions SCADA redondantes

Architecture



1 Contrôleur à redondance d'UC primaire

2 Contrôleur à redondance d'UC 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 amont entre les contrôleurs de redondance d'UC et les clients OPC UA (systèmes SCADA) est établie via les deux ports de réseau d'équipements des moodules BMENOC0321 en utilisant le protocole de redondance RSTP pour éviter les boucles Ethernet logiques.

> **NOTE:** Cette architecture nécessite la configuration de routes statiques dans l'équipement du réseau de contrôle pour rediriger les différents sous-réseaux des contrôleurs.

Le port de contrôle du BMENUA0100 (3) est désactivé pour chaque contrôleur. La communication Ethernet IPv4 vers le module BMENUA0100 est assurée via le port d'embase.

Dans cette configuration, le module BMENOC0321 fournit des communications amont redondantes via des connexions redondantes aux serveurs SCADA redondants. Les deux ports de réseau d'équipements des contrôleurs assurent la communication aval avec les stations d'E/S distantes (RIO) Ethernet X80. La communication aval entre la station RIO Ethernet X80 et l'équipement Ethernet distribué est assurée à la fois par le port de service du BMECRA31310 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 119 Control Expert.
2. Configurez le routeur / serveur SLAAC (pour IPV6 en mode SLAAC).
3. Sélectionnez le mode de fonctionnement Advanced (ou Secured) du module :

a.	Réglez le commutateur rotatif, page 23 à l'arrière du module sur le mode Advanced (ou Secured), page 30.
b.	Installez le module, page 86 dans un emplacement Ethernet du rack.

4. Configurez les paramètres de cybersécurité à l'aide des pages Web du module, page 87 :

a.	Créez la configuration de la cybersécurité à l'aide de la page Web Paramètres, page 95.
b.	Réglez le paramètre **Mode PKI** sur Auto-signature et CA.
c.	Pour les équipements clients qui ne prennent pas en charge PKI, créez une liste de **certificats client approuvés**, page 113.
d.	**Appliquez** le fichier de configuration.

5. Effectuez une inscription manuelle de certificat, page 113 :

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 seule voie d'E/S.

Lors de sa sortie d'usine, un module BMENUA0100 est réglé par défaut sur le mode de cybersécurité Advanced (ou Secured). Pour configurer un module neuf pour les opérations en mode Advanced (ou Secured), suivez le scénario Mise en service en mode Advanced (ou Secured), page 30 décrit ci-après.

Pour modifier le mode de fonctionnement de la cybersécurité pour un module qui a déjà été configuré auparavant (ou un module neuf que vous prévoyez de configurer pour le mode Standar), effectuez une opération de réinitialisation de la cybersécurité (ou sécurité), page 84 pour le module. Après l'opération de réinitialisation de la cybersécurité (ou de la sécurité), vous pouvez suivre le scénario Mise en service en mode Advanced (ou Secured), page 30 ou Mise en service en mode standard, page 30.

Mise en service en mode Advanced (ou Secured)

La mise en service d'un module BMENUA0100 pour qu'il fonctionne en mode Advanced (ou Secured) nécessite deux procédures de configuration :

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

Seul un administrateur de la sécurité peut mettre en service le module en mode Advanced (ou Secured) en utilisant la combinaison nom d'utilisateur / mot de passe par défaut, page 31 du mode Advanced (ou Secured).

NOTE: Effectuez 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 effectuer la configuration du client NTP et de l'agent SNMP.

NOTE: Pour la mise en service en mode Advanced (ou Secured) avec inscription manuelle, reportez-vous à la section Inscription manuelle, page 113.

La procédure suivante s'applique à un module neuf qui n'a jamais été configuré. Si vous utilisez un module qui a déjà été configuré, effectuez une Opération de réinitialisation de la cybersécurité (ou de la sécurité), page 84 avant de procéder aux étapes ci-après.

Pour mettre en service le module en mode Advanced (ou 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 119.

2. Configurez les paramètres de cybersécurité :

a.	Le module étant détaché du rack, utilisez le tournevis en plastique fourni avec le module, page 23 pour régler le commutateur rotatif sur la position **Advanced (ou Secured)**.
b.	Installez, page 85 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 89 indiquant un risque potentiel de sécurité, lisez le message et, si vous êtes d'accord, procédez à la connexion en cliquant sur **Accepter les risques et continuer** (ou un message similaire, 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 31.
f.	Changez et confirmez le mot de passe. Consultez la rubrique Gestion des utilisateurs, page 115 pour connaître les conditions de création du mot de passe. La page **Accueil**, page 92 du module s'affiche.
g.	A partir de la page d'accueil, accédez aux pages Web du module et configurez les paramètres de 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 119.
c.	Lorsque la configuration du projet Control Expert est terminée, connectez-vous au contrôleur et transférez le projet vers ce dernier.

NOTE: Une fois que la configuration est chargée sur le module BMENUA0100, celui-ci passe de l'état NON CONFIGURÉ à l'état CONFIGURÉ. Le voyant **SECURE**, page 141 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, aucune configuration de cybersécurité n'est requise. Les paramètres d'adresse IP, de client NTP et d'agent SNMP sont configurés à l'aide de l'outil de configuration Control Expert. En mode Standard, le module commence à communiquer lorsqu'il est inséré dans le rack et mis sous tension et qu'il reçoit une configuration valide de Control Expert.

Utilisez la combinaison nom d'utilisateur / mot de passe par défaut, page 31 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 dans la livraison, page 23 pour régler le commutateur rotatif sur la position **Standard**.
2. Placez le module dans un logement Ethernet du rack Ethernet principal local et effectuez un cycle d'alimentation.
3. Ouvrez l'outil de configuration Control Expert.
4. Dans Control Expert, créez un **Nouveau projet**, ajoutez au projet un module BMENUA0100 du **Catalogue matériel**, puis configurez les paramètres d'adresse IP, page 119, de client NTP, page 129 et d'agent SNMP, page 132.
5. Lorsque la configuration du projet Control Expert est terminée, connectez-vous au contrôleur et transférez le projet vers ce dernier.

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

Opération de réinitialisation de la cybersécurité (ou de la sécurité)

Dans le cas d'un module qui a déjà été configuré auparavant ou d'un module neuf que vous souhaitez configurer pour le mode de fonctionnement Cybersécurité, effectuez une opération de réinitialisation de la cybersécurité (ou de la sécurité) avant de procéder à la configuration de la cybersécurité. La réinitialisation restaure les valeurs par défaut d'usine des paramètres. Vous pouvez effectuer une réinitialisation à l'aide des pages Web du module ou du commutateur rotatif situé à l'arrière du module.

Pages Web : Module BMENUA0100 actuellement configuré pour le mode de fonctionnement Advanced (ou Secured) :

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

   NOTE: L'opération de réinitialisation de la cybersécurité (ou de la sécurité) est terminée lorsque le voyant **RUN** est allumé fixement en vert et que les voyants de port de contrôle **NS** et de port d'embase **BS** sont tous les deux allumés fixement en rouge.
3. Effectuez un cycle d'alimentation du module de l'une des façons suivantes :
   - Mettez le rack du module hors tension, puis à nouveau sous tension.
   - Retirez le module du rack puis réinsérez-le.

   Vous pouvez alors procéder à la mise en service en mode Advanced (ou Secured).

Commutateur rotatif : Tous modules BMENUA0100 :

1. Le module étant détaché du rack, utilisez le tournevis en plastique fourni dans la livraison, page 23 pour régler le commutateur rotatif sur la position **Cybersecurity Reset**.
2. Installez, page 85 le module dans un logement Ethernet sur le rack Ethernet principal local et effectuez un cycle d'alimentation.

   NOTE: Cette action restaure les réglages d'usine par défaut du module, notamment l'adresse IP par défaut 10.10.MAC5.MAC6 du port de contrôle, page 120. Lorsque les deux derniers octets de l'adresse MAC (*MAC5.MAC6*) correspondent à *0.0* dans l'adresse par défaut, établissez une connexion câblée point à point entre votre ordinateur et le contrôleur, le module de communication ou un autre module.

   A la fin de l'opération, le voyant **RUN** est allumé fixement en vert et les voyants de port de contrôle **NS** et de port d'embase **BS** du module sont tous les deux allumés fixement en rouge. Vous pouvez couper l'alimentation, retirer le module du rack, puis passer à l'étape Mise en service en mode Advanced (ou Secured), page 30 ou Mise en service en mode Standard, page 30.

Installation du module BMENUA0100

Introduction

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

NOTE: Si votre application est basée sur une version d'EcoStruxure Control Expert antérieure à 15.3 et que votre application comprend plusieurs contrôleurs (qui ne sont pas des contrôleurs de redondance d'UC) contenant chacun un module BMENUA0100, installez ces modules de telle sorte que le numéro d'emplacement de chaque module BMENUA0100 soit unique. Par exemple, pour une application comprenant deux contrôleurs, si un module BMENUA0100 est à l'emplacement 4 dans le rack du contrôleur 1, le deuxième module BMENUA0100 doit être situé à un numéro d'emplacement différent de 4 dans le rack du contrôleur 2.

Précautions relatives à la mise à la terre

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

⚠⚠DANGER

CHOC ELECTRIQUE

Portez un équipement de protection individuelle (EPI) lorsque vous utilisez des câbles blindés.

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

L'embase de votre module est commune au plan de la terre fonctionnelle (FE) et doit être montée et connectée sur une embase conductrice reliée à la terre.

⚠AVERTISSEMENT

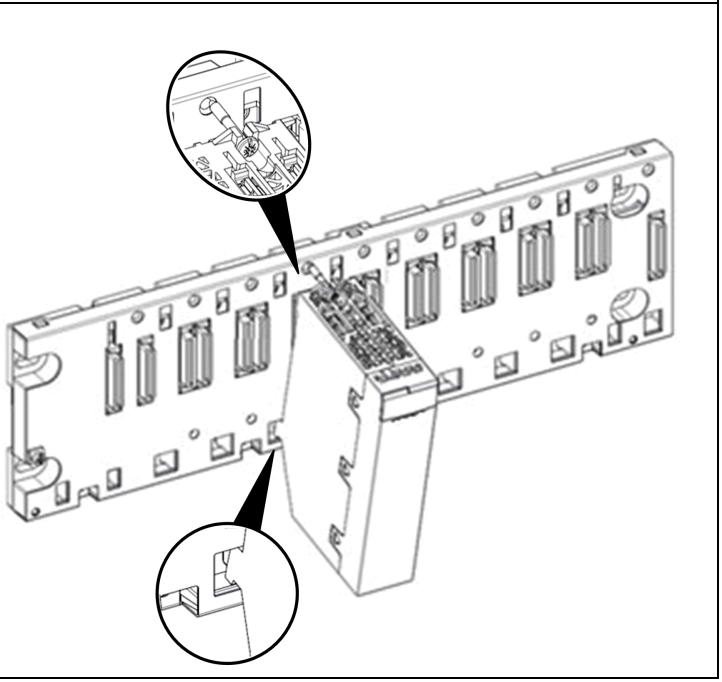
FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

Connectez l'embase à la terre fonctionnelle (FE) de votre installation.

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

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 au contrôleur. Procédez comme suit pour installer un module BMENUA0100 dans un rack :

Etape	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 rubrique *Mise à la terre du rack et du module d'alimentation* dans le document *Modicon X80 - Racks et alimentations - 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 121.
- Utilisez uniquement des versions récentes de navigateur Internet pour accéder aux pages Web. Certains navigateurs anciens tels que Internet Explorer v7 et les versions antérieures ne sont pas pris en charge.

  NOTE: Le navigateur Internet Chrome de version 123.0.6312.123 (officielle) (64 bits) a été testé avec les pages Web de BMENUA0100.

Pour que le module BMENUA0100 fonctionne en mode Advanced (ou Secured), une configuration de la cybersécurité est requise et doit être effectuée avant la configuration des paramètres d'adresse IP, de client NTP et d'agent SNMP dans Control Expert, page 119. La configuration de la cybersécurité ne peut être effectuée que localement, pour chaque

module BMENUA0100, en connectant un PC de configuration exécutant un navigateur HTTPS au module BMENUA0100 via son :

- Port de contrôle, s'il est activé.
- Port d'embase (via un module BMENOC0301 ou BMENOC0311 ou le contrôleur) 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 qui sont configurés dans Control Expert, page 119.

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

NOTE:

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

L'accès aux pages Web dépend du mode de fonctionnement de la cybersécurité :

Page Web ou Groupe	Mode Advanced (ou Secured)	Mode Standard
Accueil, page 92	✓	✓
Paramètres (sécurité de l'équipement), page 95	✓	–
Gestion des certificats, page 107	✓	–
Contrôle d'accès, page 115	✓	–
Gestion de la configuration, page 117	✓	–
Diagnostic, page 164	✓	✓
✓ : pages Web accessibles. – : pages Web inaccessibles.		

Configuration initiale des paramètres de cybersécurité

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

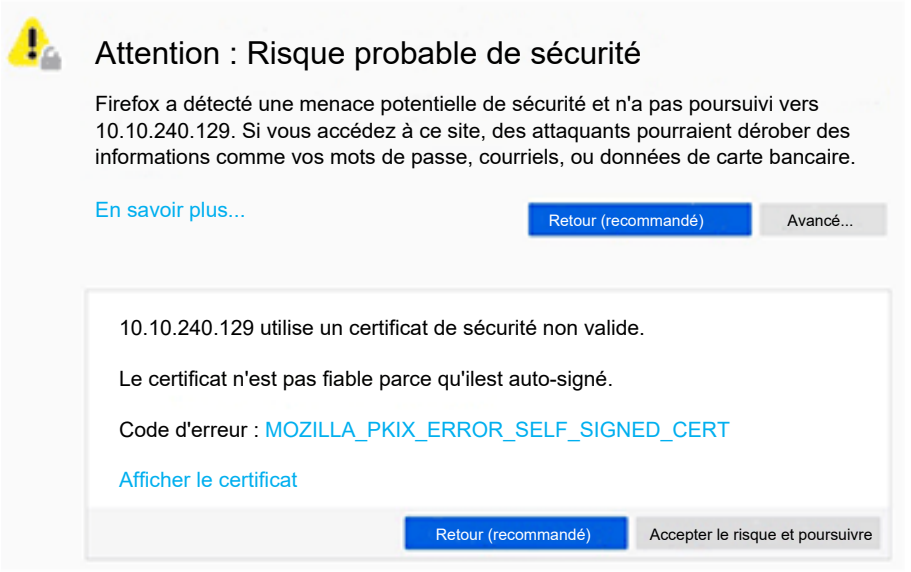
- Jamais configuré auparavant, et donc porteur de la configuration par défaut d'usine.
- Configuré auparavant, mais dont la configuration par défaut d'usine a été restaurée via la commande de réinitialisation de la cybersécurité (ou de la sécurité), page 31.

Une fois qu'un module a été configuré avec des paramètres de cybersécurité et qu'il fonctionne en mode Advanced (ou Secured), vous pouvez également modifier les paramètres de cybersécurité à l'aide des pages Web.

Consultez la rubrique Mise en service, page 81 pour savoir comment appliquer une configuration initiale au module.

Première connexion aux pages Web

Lorsque vous vous connectez à un module BMENUA0100 non configuré, l'écran suivant (ou un écran similaire selon le navigateur que vous utilisez) s'affiche :



En dépit des termes utilisés dans le message, la connexion est sécurisée via HTTPS. Lisez le message et, si vous êtes d'accord, procédez à l'ouverture de session initiale en cliquant sur **[Accepter les risques et continuer]** (ou message similaire, selon le navigateur).

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 la combinaison Nom d'utilisateur et mot de passe, page 31 définie par défaut. Immédiatement après, l'administrateur est invité à modifier le mot de passe par défaut.

Vous devez suivre la procédure de connexion 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 dans la page Web, page 115 **Contrôle d'accès > Gestion des utilisateurs**) peuvent accéder aux pages Web du module.

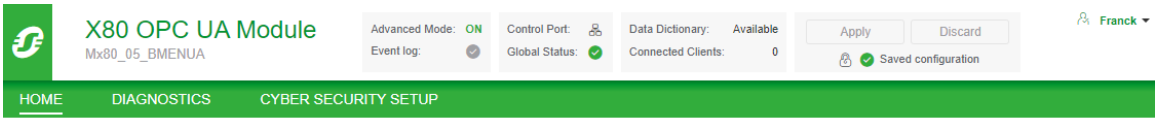
Dans la page de connexion, sélectionnez une langue dans la liste déroulante, puis entrez votre **Nom d'utilisateur** et votre **Mot de passe**.

NOTE: Le mode de fonctionnement de la cybersécurité du module est indiqué par l'icône de verrou en haut à droite de la boîte de dialogue (flèche rouge dans l'illustration ci-dessus). Si le verrou est :

- Fermé (comme dans l'illustration ci-dessus) : le module fonctionne en mode Advanced (ou Secured), page 30.
- Ouvert : le module fonctionne en mode Standard, page 30.

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 Advanced (ou Secured) :
  - ON : Le module fonctionne en mode Advanced (ou Secured), page 30.
  - OFF : Le module fonctionne en mode Standard, page 30.
- Journal d'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 n'est pas activée.
- Clients connectés : nombre de clients OPC UA connectés.

- Appliquer/Annuler la configuration : Indique l'état de la configuration 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 boutons **Appliquer** et **Annuler** sont désactivés.
  - Configuration en attente : Une ou plusieurs modifications de la configuration de cybersécurité n'ont pas encore été appliquées. Les boutons **Appliquer** et **Annuler** sont tous les deux activés.
  - Configuration non valide : La configuration de la cybersécurité est incomplète ou incorrecte. Le bouton **Appliquer** est désactivé ; le bouton **Annuler** est activé. Dans cet état, la page Web affiche, à côté de chaque option de menu concernée, 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, la page identifie ce paramètre.

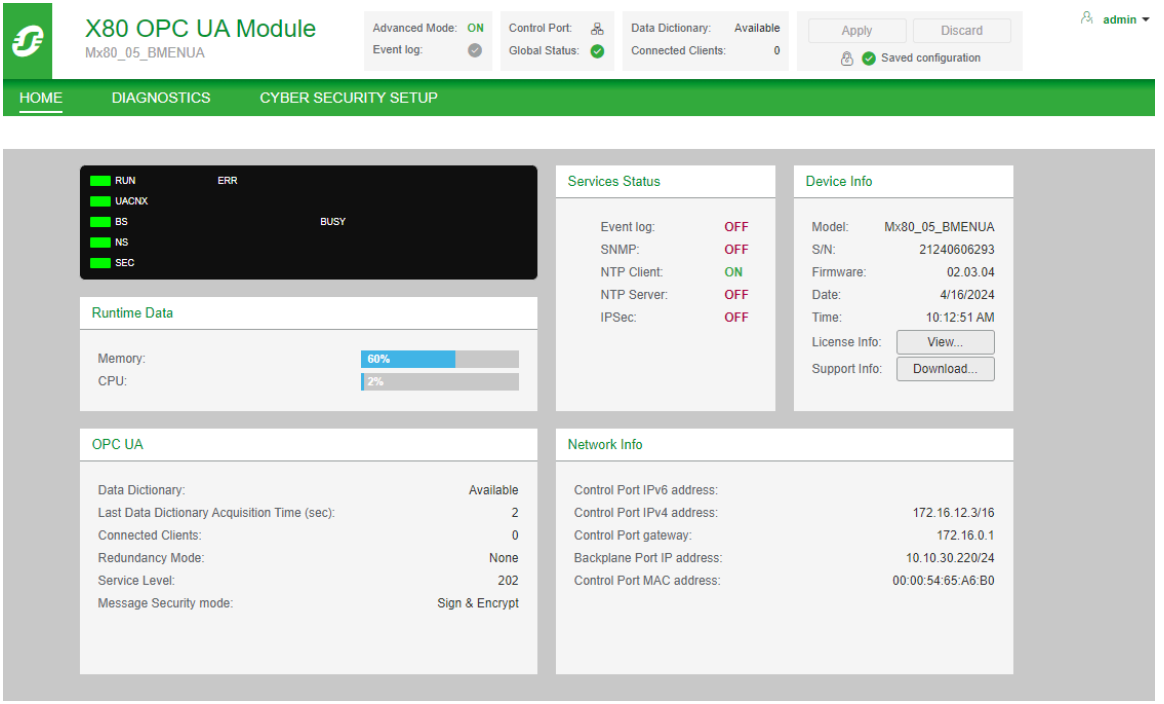
Aide des pages Web

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

Page d'accueil

Présentation de la page d'accueil

Lorsque vous vous connectez aux pages Web 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. Selon le mode de fonctionnement du module :
  - Mode Advanced (ou Secured), page 30 : les menus de diagnostics et de configuration de la cybersécurité s'affichent et sont accessibles à l'administrateur de la sécurité.
  - Mode Standard, page 30 : seul le menu DIAGNOSTICS est accessible.
- Affichage de l'état, page 137 des voyants du module, page 24.
- Affichage des données collectées concernant le module, notamment :
  - Données d'exécution, page 94
  - OPC UA, page 94
  - Etat des services, page 94
  - Infos sur le réseau, page 95
  - Infos sur les équipements, page 95

NOTE: Lorsque le commutateur rotatif à l'arrière du module est réglé sur Cybersecurity (/Security) Reset, page 31, aucune communication ne se produit avec le module. Par conséquent, les pages Web (y compris la page d'**Accueil**) ne sont pas accessibles.

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 142 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** : Etat d'intégrité du serveur OPC UA en fonction de la qualité des données et des services (SERVICE_LEVEL).

  NOTE: Les cinq éléments décrits ci-dessus sont basés sur les éléments du DDT, page 142 T_BMENUA0100.
- **Mode de sécurité des messages**: Paramètre configuré dans la page Web OPC UA, page 105 : 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 dans le DDT, page 142 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** (CONTROL_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 119 et indiqués dans le DDT, page 142 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 la référence, le numéro de série et la version de micrologiciel (FW_VERSION dans le DDT T_BMENUA0100) , page 142), la date et l'heure du module BMENUA0100.

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

Cliquez sur **Télécharger...** pour afficher la boîte de dialogue **Informations d'aide au téléchargement**. Consultez la rubrique Contrôle d'accès, page 115 pour plus d'informations.

Paramètres

Dans les pages Web du module BMENUA0100, à partir de la page **Acueil**, sélectionnez **Paramètres** pour afficher les liens vers les pages de configuration suivantes dans lesquelles vous pourrez entrer les paramètres de sécurité de l'équipement :

- Stratégie des comptes utilisateur, page 96
- Journaux d'événements, page 96
- Services réseau, page 97
- Transfert de service, page 99
- IPsec, page 103
- SNMP, page 104
- OPC UA, page 105

- Bannière de sécurité, page 107

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

Utilisez ces paramètres pour configurer la sécurité du module BMENUA0100. Après avoir modifié les 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 tentatives de connexion infructueuses autorisées. 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 172 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 158 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 pour les versions de micrologiciel 1.10 et ultérieures du module BMENUA0100.
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 :

STRATÉGIE GLOBALE :

Service	Description
Appliquer la sécurité	Désactive les services réseau sauf IPsec.
Déverrouiller la sécurité	Active les services réseau sauf IPsec.

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	Avanced (ou Secured)
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 entre contrôleurs[2, 3]	Active et désactive les communications Modbus transitant par le BMENUA0100 entre des contrôleurs M580. Consultez *Configuration de la communication pour les flux de données entre contrôleurs*, page 99.	Activé	Désactivé
Flux de données Control Expert vers un contrôleur uniquement[2, 3]	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 le contrôleur uniquement. Consultez *Configuration de la communication pour le flux de données Control Expert*, page 99.	Activé	Désactivé
Flux de données Control Expert vers le réseau d'équipements[2, 3]	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 le contrôleur. Consultez *Configuration de la communication pour le flux de données Control Expert*, page 99.	Activé	Désactivé

Service	Description	Mode CS par défaut	
		Standard	Avanced (ou Secured)
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 172.

3. Pris en charge uniquement par les modules antérieurs à la version BMENUA0100.2, comme indiqué dans EcoStruxure Control Expert.

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. Ne désactivez pas IPsec dès lors que l'un des services SNMP, NTP, Modbus et Syslog est activé.

Configuration de la communication pour un logiciel distant exécuté sur des PC (sans utilisation du transfert NAT)

Le logiciel s'adresse à l'équipement cible (contrôleur M580 par exemple) 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 (contrôleur M580 par exemple), à l'aide du protocole 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=subnet of the target device>> MASK <<subnet mask of the target device>> <<gateway=BMENUA0100 module backplane port IP address>>
```

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 Connexion de Control Expert 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 entre contrôleurs.

Les communications Modbus TCP/IP de contrôleur à contrôleur passant par le module BMENUA0100 utilisent l'adresse du port de contrôle IPv4 du module BMENUA0100 et non l'adresse du contrôleur cible.

NOTE:

- Pour BMENUA0100, le transfert de contrôleur à contrôleur est limité au protocole Modbus TCP/IP.
- Modbus est le seul protocole qui prend en charge la communication d'équipement à équipement.
- Seul l'adressage IPv4 (et non IPv6) prend en charge les flux de données Modbus TCP/IP de contrôleur à contrôleur.

Transfert de service (transfert IP)

Un module BMENUA0100 équipé du micrologiciel de version 2.01 ou ultérieure inclut cette page Web. Utilisez-la pour configurer le transfert des flux de données de monodiffusion qui

passent par ce 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 manuelle est prise en charge. (multidiffusion).
- Transfert de messages vers les modules de communication EtherNet/IP locaux du contrôleur (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 (Modbus, HTTPS, SNMP, etc.)
- Création et application de modèles de transfert IP personnalisés.
- Transfert NAT (Network Address Translation) de certains protocoles vers le contrôleur local si l'adresse IP distante est le port de contrôle IPv4 du module 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-après, page 103.

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 entraîner l'arrêt de certaines communications en cours.
- 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 compris dans cette plage peuvent également être transférés. N'activez 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. N'activez 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 178
- Transfert de service (IP) - Architectures non prises en charge, page 181

Transfert IP et communication OPC UA

Le transfert IP et 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 182.

Création de règles :

- Pour documenter à la fois les règles prédéfinies et les règles personnalisées, cliquez sur **Nouveau transfert** et renseignez 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 sur IPsec si IPsec est activé.

Chaque règle est définie par les champs suivants :

Paramètre	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.

Paramètre	Description
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:** • **Ne pas utiliser** IPsec pour les protocoles qui sont sécurisés par nature (par exemple Modbus sur TLS, EIP explicite sur TLS, DNP3 sur TLS, EIP 60870 sur TLS) • **Utiliser** IPsec pour les protocoles qui ne sont pas sécurisés par nature (par exemple Modbus , EIP explicite, client OPC UA, EIP IO)
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 de contrôleur). • **Les deux** : si la requête du client distant peut être reçue à la fois sur le port de contrôle et sur le port d'embase (par exemple, requête Modbus TCP/IP en provenance de Control Expert et requête Modbus TCP en provenance d'un bloc fonction de contrôleur).
1. Renseigné automatiquement, mais modifiable, pour un nom de service prédéfini.	

IPsec

Utilisez IPsec pour sécuriser la communication Ethernet IPv4.

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

Utilisez ces paramètres pour configurer au maximum 8 voies IKE/IPsec sur IPv4 pour le module BMENUA0100. Si plus de 4 liaisons IPsec sont configurées, la connexion automatique au contrôleur après le transfert via le BMENUA0100 risque d'échouer. Dans ce cas, connectez-vous manuellement au contrôleur.

Paramètre	Description
SERVICE IPsec	• Activé : Active le service IPsec. **NOTE:** Avant d'activer le service IPsec, vous devez activer le port de contrôle dans les paramètres de configuration IP, page 121. • Désactivé : Désactive le service IPsec.
NTP autorisé en dehors de IPsec	• Désélectionné (désactivé) : Les échanges NTP passent obligatoirement par IPsec. • Sélectionné (activé) : Les échanges NTP passent par IPsec si la voie IPsec est ouverte, en dehors de IPsec si la voie IPsec n'est pas ouverte.

Paramètre	Description
Nouvelle liaison	Crée un 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.
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.
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 184 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 IPsec** est modifié pour certains protocoles, le script Windows doit être téléchargé à nouveau à partir du module BMENUA0100 et exécuté sur Windows. Vous trouverez un exemple de script Windows dans la section Scripts Windows pour IPsec, page 184.

NOTE: Si 8 tunnels IPsec sont configurés, il peut s'avérer impossible de se reconnecter automatiquement au contrôleur après le téléchargement d'une application. Le cas échéant, reconnectez-vous manuellement au contrôleur après le téléchargement.

NOTE: Si le service IPsec est activé :

- Le flux de données du serveur HTTPS local passe en dehors de IPsec.
- Le flux de données OPC UA local est par défaut transporté à l'intérieur de IPsec. Pour transporter le flux de données OPC UA local en dehors de IPsec, une règle de transfert OPC UA avec "Utilisation IPsec = faux" doit être définie, même s'il n'est pas nécessaire de transférer le flux de données OPC UA.

SNMP

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

NOTE: En mode Advanced (ou Secured), la version de SNMP doit être configurée de la même manière dans Control Expert, page 133 et dans la page Web SNMP. Si ces réglages ne sont pas identiques, le service SNMP ne démarre pas.

Paramètre	Description
Version 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). • 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:** Quand le réglage **Aucun** est sélectionné, le **type de jeton d'identification 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 de chiffrement valide. • Basic256 : Définit une stratégie de sécurité pour les configurations avec une suite de chiffrement 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 de chiffrement 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 fermées. La valeur de *Timeout de session* fait partie de la configuration du client OPC UA SCADA.

NOTE: Lorsque le paramètre **Mode de sécurité des messages** du serveur OPC UA est initialement configuré sur **Signature et cryptage** ou **Signature** et qu'un client OPC UA établit une connexion, si vous configurez par la suite le **Mode de sécurité des messages** du serveur OPC UA sur **Aucun**, un client OPC UA (avec son **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.
2. Modifiez la configuration OPC UA dans la page Web du BMENUA0100.
3. Attendez que le voyant **BUSY** allumé en jaune s'éteigne.
4. En ce qui concerne les clients OPC UA, modifiez leur 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 équipés du micrologiciel de version v1.0 ou ultérieure. Procédez comme suit pour gérer les certificats dans les pages Web **Gestion des certificats** :

- 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 de 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 PKI > 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 équipés du micrologiciel de version v1.1 ou ultérieure. Procédez comme suit pour gérer les certificats dans les pages Web **Gestion des certificats** :

- Réglez le **Mode PKI** :
  - **CA uniquement** : si tous les équipements clients OPC UA installés prennent en charge PKI.
  - **Auto-signé et CA** : si certains équipements clients OPC UA installés ne prennent pas en charge PKI.
- Si **Mode PKI** est réglé sur **CA uniquement** :
  - Inscrivez manuellement, page 113 chaque module BMENUA0100 auprès de l'autorité de certification.
- Si **Mode PKI** est réglé sur **Auto-signé et CA** :
  - Inscrivez manuellement, page 113 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 de clients OPC UA autorisés à communiquer avec le module BMENUA0100.

Mise à jour de la liste de certificats approuvés

Après la première installation du micrologiciel BMENUA0100 de version 2.0 (BMENUA0100.2) ou une version ultérieure, vous devez supprimer 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 sélecteur rotatif de cybersécurité sur la position **Cybersecurity Reset** (réinitialisation de la cybersécurité).

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 ultérieure. Il n'est pas nécessaire de répéter la procédure pour les installations suivantes de versions ultérieures du micrologiciel.

NOTE: Si vous ne nettoyez 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 supprimées.

Présentation de l'authentification

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

- Pour les versions 1.0 et ultérieures du micrologiciel :
  - Certificat auto-signé (uniquement)
- Pour les versions 1.10 et ultérieures du micrologiciel :
  - Certificat PKI émis par une autorité de certification tierce uniquement
  - Certificat PKI émis par une autorité de certification et certificat auto-signé

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

Pour les versions de micrologiciel 1.10 et ultérieures, 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 date et d'heure du module BMENUA0100, et vérifiez que le serveur NTP est accessible et qu'il dispose de paramètres de date et d'heure à jour.
- Si vous recevez un message d'erreur détectée *BadCertificateHostnameInvalid* lors de la tentative de connexion de votre client OPC UA au serveur BMENUA0100 dans IPv6, le problème peut être causé par une adresse IPv6 compressée (c'est-à-dire abrégée). 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 manuellement les dates d'expiration des certificats.

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 PKI, page 112
- Gestion de liste de confiance de clients, page 113
- Exportation de certificats d'équipement, page 114
- Inscription manuelle, page 113
- Certificats CA, page 114

Consultez les sections *Utilisation des objets GPO/LGPO*, page 171 et *Application de la gestion des stratégies de groupe MMC*, page 172 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

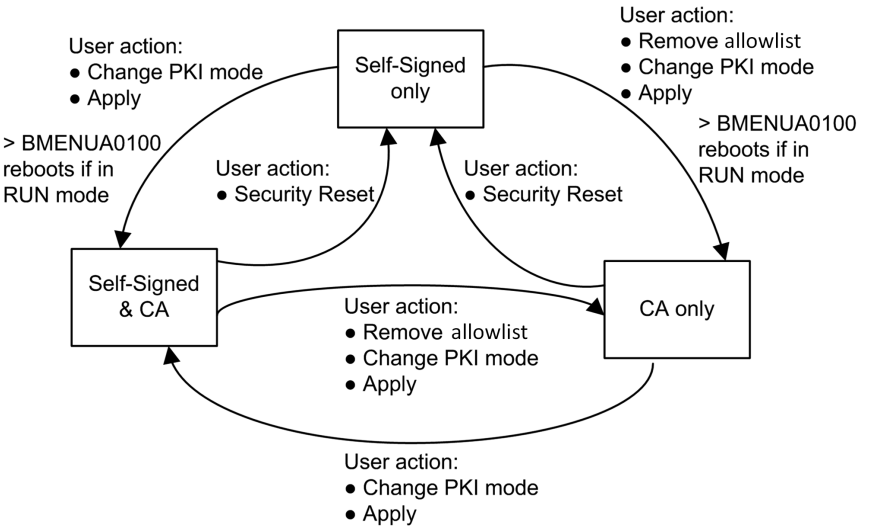
- Identificateur de clé de l'autorité :
  - Identification de la clé publique correspondant à la clé privée utilisée pour signer un certificat.

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** 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 ultérieure 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 :



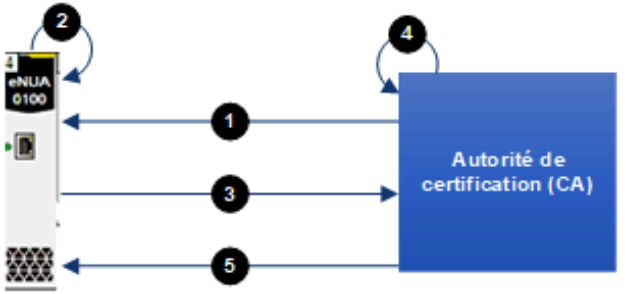
Inscription manuelle

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. Par la suite, vous pourrez **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 129.
- Vérifiez que le réglage d'heure du module BMENUA0100 est correct.

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, à l'adresse 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 apportée à la configuration.

Pour supprimer un certificat de la liste :

Etape	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 apportée à la configuration.

Exportation de certificats d'équipement

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

Certificats CA

Le certificat CA 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 ajouter 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 :

Etape	Action
1	Ouvrez les pages Web du module et entrez les informations suivante dans la fenêtre **Connexion** : • nom d'utilisateur • mot de passe Cliquez sur **Connexion**.
2	Sélectionnez **CONFIGURATION DE LA CYBERSECURITE > GESTION DES CERTIFICATS** pour accéder à l'onglet de 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 de BMENUA0100 fournissent des outils pour la gestion des comptes utilisateur. Dans la page **Accueil**, cliquez sur **Contrôle d'accès** pour afficher la liste des comptes utilisateur OPC UA existants ainsi que leurs rôles et autorisations. Dans cette page, vous pouvez :

- Créer un compte utilisateur, page 116.
- Mettre à jour le profil, page 117 d'un compte utilisateur existant.
- Supprimer, page 117 un compte utilisateur.

Gestion des utilisateurs

Le module BMENUA0100 fournit un contrôle d'accès basé sur les rôles (RBAC). Un rôle est attribué à chaque compte utilisateur et ce compte ne peut effectuer que les tâches associées à ce rôle.

Les rôles et les autorisations ci-après 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 utilisateurs simultanés.

Il n'est pas possible de configurer des rôles personnalisés ou des jeux d'autorisations personnalisés. Il n'est pas possible de configurer une liste autorisée de contrôle d'accès basée sur l'adresse IP.

Créer un compte utilisateur

Un administrateur de la sécurité peut cliquer sur **Nouvel utilisateur** puis renseigner les paramètres suivants pour créer un nouveau compte 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. Le mot de passe ne s'affiche pas en texte clair. Entrez cette valeur deux fois pour confirmer son exactitude. **NOTE:** Chaque mot de passe doit contenir au minimum 8 caractères dont au moins l'un des caractères suivants : • un caractère alphabétique en majuscule (A...Z) • un caractère alphabétique en minuscule (a...z) • un chiffre en base 10 (0 à 9) • un caractère spécial parmi ~ ! @ $ % ^ & * _ + - = ` | \ ( ) [ ] : " ' < >
Confirmation du mot de passe	
Rôles	Sélectionnez le rôle, lequel va définir les autorisations accordées à l'utilisateur : • Administrateur de la sécurité • Opérateur • Ingénieur • Installateur

Cliquez sur **Appliquer les modifications** après avoir configuré ces paramètres pour créer le compte utilisateur.

Mettre à jour un compte utilisateur

Pour modifier les paramètres d'un compte utilisateur, 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 utilisée pour créer un compte utilisateur s'ouvre, vous permettant de mettre à jour une partie ou la totalité des paramètres du compte utilisateur sélectionné.

Supprimer un compte utilisateur

Pour supprimer un compte utilisateur existant, un administrateur de la sécurité peut cliquer avec le bouton droit sur le compte utilisateur dans la liste puis, sous **Supprimer un 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. Dans les pages Web du module BMENUA0100, à partir de la page **Accueil**, sélectionnez **Gestion de la configuration** pour afficher les liens d'accès aux pages suivantes de gestion de la configuration de cybersécurité :

- EXPORTATION, page 117
- IMPORTATION, page 118
- REINITIALISATION, page 119

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

Exportation d'une 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 116.
2	Saisissez 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 à l'aide de cette commande remplacent les paramètres de cybersécurité existants du 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	Accédez au fichier de configuration à importer, sélectionnez-le, puis cliquez sur **OK**.
3	Dans la page **IMPORTATION**, entrez le **Mot de passe** du fichier de configuration (attribué 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 et vous informe 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 89.
6	Entrez votre nom d'utilisateur et votre 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 attente.
7	Dans la bannière, cliquez sur **Appliquer**, puis cliquez sur **Oui** pour confirmer que vous souhaitez appliquer la configuration en attente. La nouvelle configuration est appliquée. **NOTE:** Si vous avez sélectionné **Enregistrer** dans la page **IMPORTATION** (comme indiqué à l'étape 3 ci-dessus), la configuration est automatiquement appliquée et l'étape 7 est exécutée automatiquement.

Réinitialisation d'une configuration

Cliquez sur **Réinitialiser** dans la page **REINITIALISATION** pour restaurer les paramètres d'usine de la cybersécurité sur le module BMENUA0100 local. Cette action a le même effet que le réglage du commutateur rotatif sur la position Cybersecurity (ou Security) Reset, page 31. Une fois la réinitialisation terminée, vous devez redémarrer le module.

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).

Lorsque le module BMENUA0100 est utilisé avec un contrôleur autonome, les paramètres d'adresse IP sont configurés pour un seul module. Lorsque deux instances du module BMENUA0100 sont utilisées dans une architecture de contrôleur à redondance d'UC (un module BMENUA0100 dans chaque contrôleur), l'onglet **Configuration** de Control Expert affiche les paramètres pour deux modules (A et B). Dans une architecture de contrôleur à

redondance d'UC, l'adresse IP de chaque module peut appartenir à un sous-réseau différent.

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:

  Lors de la mise sous tension initiale du module (ou après un réglage du sélecteur rotatif sur **Cybersecurity (ou Security) Reset** suivi d'une mise sous tension, puis d'un réglage sur **Mode Advanced (ou Secured)**, puis d'une remise sous tension), le port de contrôle reçoit l'adresse IPv4 par défaut 10.10.MAC5.MAC6, où MAC5 est la valeur décimale du 5e octet de l'adresse MAC du module et MAC6 est la valeur décimale du 6e octet.

  Lorsque les deux derniers octets de l'adresse MAC (*MAC5.MAC6*) correspondent à *0.0* dans l'adresse par défaut, établissez une connexion câblée point à point entre votre ordinateur et le contrôleur, le module de communication ou un autre module.

  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 un routage vers un contrôleur M580. Control Expert V15 (ou version ultérieure) peut être connecté à un contrôleur M580 via l'adresse IPv6 du BMENUA0100.

Configuration des adresses IP

Configurez l'adressage IP comme suit dans Control Expert :

Etape	Action
1	Dans le **Navigateur de projet**, développez le noeud **Bus automate** et ouvrez a 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	

Paramètre		Description
	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 l'option **Statique** est sélectionnée pour **Mode**, entrez une adresse IPv6 valide pour le port de contrôle. **NOTE:** • Le BMENUA0100 ne détecte pas les adresses IPv6 en double. Vérifiez auprès de votre administrateur réseau qu'il n'y a pas d'adresses IPv6 en double dans le même segment de réseau. • Le BMENUA0100 acceptera les adresses IPv6 incorrectes mais ne pourra pas les utiliser.
	Longueur du préfixe du sous-réseau	Définie automatiquement pour l'adresse IPv6 statique, cette valeur représentant le nombre de bits de l'adresse IPv6 affectée par SLAAC qui définissent le préfixe de 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 (option par défaut) : Active les champs **IPv4 @**, **Masque de sous réseau**, et **Passerelle par défaut** permettant de saisir une adresse IPv4 statique pour le 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.
	Masque de sous-réseau	Si **Statique** est sélectionné comme **Mode**, saisissez un masque de sous-réseau IPv4 valide pour le port de contrôle, qui va déterminer la partie réseau de l'adresse IPv4.
	Passerelle par défaut	Si **Statique** est sélectionné comme **Mode**, saisissez une adresse IPv4 valide pour la passerelle par défaut.
Port d'embase		

Paramètre	Description
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 123.
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 • 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, dans le cas d'un système de redondance d'UC, au module BMENUA0100 redondant (B).
- La page **Serveur d'adresses** du contrôleur (ouverte dans le **Navigateur de DTM** en double-cliquant sur le contrôleur 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** du contrôleur affiche l'adresse IP du port d'embase des deux modules BMENUA0100.

Configuration de l'horodatage à la source

L'horodatage source est pris en charge par la version 2.01 (et ultérieure) 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.

NOTE: Les valeurs sont extraites d'un équipement d'horodatage à la source uniquement pour les variables BOOL et EBOOL qui sont :

- configurées comme horodatées à la source (ASTS) dans Control Expert.
- surveillées par un client OPC UA dans le cadre d'un abonnement OPC UA.

Si le noeud OPC UA n'a pas été ajouté et n'est pas surveillé dans le cadre d'un abonnement, le service de lecture synchrone OPC UA détecte et signale une erreur.

Autorisation de l'horodatage à la source

L'horodatage à la source peut être autorisé dans la fenêtre Options 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 **Configuration IP** de la boîte de dialogue de configuration du BMENUA0100 pour activer et configurer l'horodatage.

Dans la section **Horodatage source**, configurez les paramètres suivants :

Paramètre	Description
Activé	Active l'horodatage source pour l'application.
Interrogation de la mémoire tampon (ms)	Fréquence d'interrogation des requêtes de lecture d'événement gérées par le BMENUA0100. La plage de valeurs valides va de 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 127.

Gestion des variables horodatées à la source

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

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

NOTE: Ces deux éléments de données ne sont pertinents que si l'horodatage est sélectionné dans Control Expert et activé pour le module BMENUA0100 concerné.

Le BMENUA0100 traite l'élément `#TSEventSynchro` en tant que noeud OPC UA booléen.

La définition de `#TSEventSynchro` envoie une commande de synchronisation à tous les équipements horodatés à la source du contrôleur M580. Les valeurs renvoyées par les équipements au client OPC UA initialisent les variables horodatées à la source à leurs valeurs actuelles.

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

- `UA_EGOOD` : La demande de synchronisation a été correctement envoyée à tous les équipements d'horodatage.
- `UA_EBAD` : La demande de synchronisation a échoué car l'horodatage est désactivé dans le projet Control Expert.
- `UA_EBADINVALIDSTATE` : La demande de synchronisation a échoué car l'horodatage a été désactivé pour le module BMENUA0100 par la fonction %MW400, page 127.
- `UA_EBADINUSE` : La demande de synchronisation a échoué car le module BMENUA0100 n'a pas pu réserver de mémoire tampon d'horodatage.
- `UA_EBADDISCONNECT` : La demande de synchronisation a expiré sans avoir pu écrire les valeurs dans la période spécifiée.

Pour réaliser cette initialisation, utilisez un client OPC UA (comme 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 de contrôleur (y compris le contrôleur M580, BMECRA31310, BMXERT1604), puis attendez que sa valeur passe à 1 (vrai).
2. Ajoutez des éléments de données surveillés, configurés comme variables horodatées à la source, à un 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 le contrôleur. 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.
- Définissez 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 équipement ne répond pas dans le délai imparti, le paramètre `#TSEventSynchro` renvoie la réponse `UA_EBADDISCONNECT` indiquant que la commande a dépassé le délai imparti sans aboutir, et cela même si d'autres équipements répondent correctement.
- Si l'abonnement est modifié pour ne contenir, par exemple, qu'une seule variable par équipement, l'exécution de `#TSEventSynchro` entraîne la perte des valeurs renvoyées précédemment pour les équipements et variables faisant l'objet de l'abonnement précédent.

Voies du contrôleur M580 dédiées à l'horodatage

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

Par exemple, pour le contrôleur 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 maximal de variables horodatées à la source prises en charge.

La formule permettant de déterminer le nombre maximal 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)

Par exemple :

- BMEP586040(C) : 16 connexions maximum, 4 voies, 82 variables maximum :

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

  Si **Interrogation de la mémoire tampon** = 500 ms : 656 variables par seconde.
- BMECRA31310 : 1 connexion, 1 voie, 82 variables maximum :

  1 x 82 = 82 variables au total

  Si **Interrogation de la mémoire tampon** = 500 ms : 164 variables par seconde.
- BMXERT1604 : 1 connexion, 1 voie, 20 variables maximum :

  1 x 20 = 20 variables au total

  Si **Interrogation de la mémoire tampon** = 500 ms : 40 variables par seconde.

Spécification du BMENUA0100 chargé de gérer les variables horodatées

Un rack M580 principal peut contenir deux modules BMENUA0100. Toutefois, les variables horodatées dans les contrôleurs M580 et les modules BMECRA31310 et BMXERT1604 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 chargé de réserver le tampon d'horodatage, utilisez le bloc `WRITE_VAR` pour définir le mot %MW400 sur 2, ce qui active 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 (non habilité à réserver la mémoire tampon d'horodatage), utilisez le bloc `WRITE_VAR` pour définir le mot %MW400 sur 1, ce qui désactive 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**.

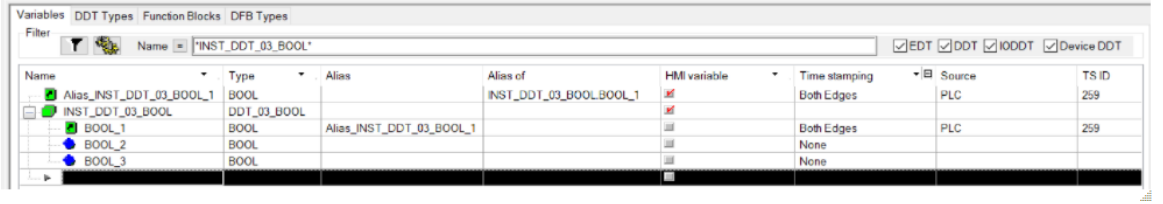
NOTE:

Lorsque l'option **Activé** est désélectionnée, les valeurs des variables lues par le BMENUA0100 sont celles présentes dans la mémoire du contrôleur.

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 BMENUA0100 reconnaît les variables **Alias** horodatées de type BOOL ou EBOOL créées dans Control Expert, mais pas les variables **Alias de** correspondantes. Un exemple de variables **Alias** et **Alias de** est présenté ci-après :



Pour être reconnues par le BMENUA0100, les variables **Alias** doivent être intégrées dans le dictionnaire de données.

Les variables **Alias** BOOL ou EBOOL et leurs variables **Alias de** associées 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 souscrire un abonnement à la variable **Alias** (noeud OPC UA) dans le client OPC UA pour pouvoir recevoir l'horodatage source depuis l'équipement et non depuis le module BMENUA0100.

Comme aucune des variables **Alias de** BOOL ou EBOOL n'est perçue comme étant horodatée à la source par le micrologiciel du BMENUA0100, la variable **Alias** doit être intégrée 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 de temps réseau (NTP). Le service 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 réside dans le contrôleur, 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 du BMENUA0100 peut prendre 5 minutes. Le voyant **ERR**, page 137 reste allumé jusqu'à ce que l'heure du BMENUA0100 soit synchronisée 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: Lorsque les paramètres d'adresse IP**Serveur NTP primaire** et **Serveur NTP secondaire** ont tous les deux la valeur 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 Advanced (ou 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 **Services réseau** , page 97.
- En mode Standard, 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).

  NOTE: Si le BMENUA0100 est configuré en tant que client NTP sur le réseau d'embase (**Serveur NTP primaire** ou **Serveur NTP secondaire**), le serveur NTP du BMENUA0100 ne peut pas être activé pour un autre équipement.

Si le serveur NTP et le client NTP sont tous les deux activés dans le module BMENUA0100, le client NTP du module reçoit les paramètres temporels 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 établir l'heure exacte du réseau Ethernet, le système effectue les tâches suivantes à 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.

NOTE: 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

Procédez comme suit pour configurer le service de synchronisation du temps réseau dans Control Expert :

Etape	Action
1	Dans le **Navigateur de projet**, développez le noeud **Bus automate** et ouvrez a 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:** Par défaut, elle a la valeur de l'adresse IP principale du contrôleur.
	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, 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: Si le mode de fonctionnement est Advanced (ou Secured), vérifiez que le service NTP est activé dans la section Activation des services réseau, page 97 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 de 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 d'un (1) ou de deux (2) équipements (généralement des PC exécutant un logiciel de gestion de réseau) utilisées comme destinataires des messages de trap fondés sur des événements. Ces messages informent l'équipement de gestion en cas d'événements tels que les démarrages à froid et l'impossibilité 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 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 Advanced (ou Secured) : vous pouvez configurer l'agent SNMP dans Control Expert et dans les pages Web du module BMENUA0100.

  NOTE: En mode Advanced (ou Secured), la version de SNMP doit être configurée de la même manière dans Control Expert, page 104 et dans la page Web SNMP. Si ces réglages ne sont pas identiques, 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 ultérieure 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 Advanced (ou Secured), la version de SNMP doit être configurée de la même manière dans Control Expert, page 104 et dans la page Web SNMP. Si ces réglages ne sont pas identiques, le service SNMP ne démarre pas.

Champ	Paramètre	Description	Valeur
Version de SNMP	SNMP V1	Sélectionnez cette option pour utiliser SNMP V1	sélectionné/désélectionné
	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)
	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	*désélectionné* (par défaut) : Vous pouvez modifier les paramètres **Emplacement** et **Contact**. *sélectionné* : Vous ne pouvez pas modifier les paramètres **Emplacement** et **Contact**.	sélectionné/désélectionné
Noms de communauté (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 le trap **Echec d'authentification**	*désélectionné* (par défaut) : Non activé. *sélectionné* : 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.	sélectionné/désélectionné
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) **Echec d'authentification** est également pris en charge s'il est activé.

Identifiants d'objet SNMP MIB-II

Sous le **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, soit la somme (2_{7-1} + $_{24-1}$ + 2_{2-1}) indiquant la prise en charge des protocoles dans les couches OSI suivantes : • 7 : couche d'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 de contrôleur M580 pour les connexions client-serveur OPC UA

Introduction

Cette section décrit les réglages effectués dans la configuration de contrôleur M580 pour 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 du contrôleur M580

Configuration des services du contrôleur

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 du contrôleur M580 :

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

Si ces services ne sont pas tous les deux activés dans le contrôleur, 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 24 du module BMENUA0100 est décrit ci-dessous pour les différents états de fonctionnement du module.

NOTE: L'état du voyant **SECURE** indiquant l'état configuré ou non configuré du module est illustré séparément à la suite de la présentation initiale.

Etat de fonctionnement		**Voyants**						
		RUN (vert)	**UACNX (vert/ rouge)**	**ERR (rouge)**	**BS (vert/ rouge)**	**NS (vert/rouge)**	**BUSY (jaune)**	**SEC (vert/ rouge)**
Séquence de mise sous tension	1	Eteint	Allumé	Allumé	Vert éteint Rouge allumé fixe	Vert éteint Rouge allumé fixe	Eteint	Vert éteint Rouge allumé fixe
	2 (tous les voyants sont allumés)	Allumé	Allumé	Allumé	Vert fixe Rouge allumé fixe	Vert allumé fixe Rouge allumé fixe	Allumé	Vert allumé fixe Rouge allumé 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
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 141.

Etat de fonctionnement		**Voyants**						
		RUN (vert)	**UACNX** (vert/ rouge)	**ERR** (rouge)	**BS** (vert/ rouge)	**NS** (vert/rouge)	**BUSY** (jaune)	**SEC** (vert/ rouge)
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 140	/	Vert éteint Rouge allumé fixe	/	/	Reportez-vous à la description du voyant d'état de la communication sécurisée ci-dessous, page 141.
	Après détection d'une adresse IPv4 en double sur le port de contrôle	Clignotant		/	/	Vert éteint Rouge allumé fixe	/	
	Etat RUN	Allumé		Eteint	Vert allumé fixe Rouge éteint	Vert allumé fixe si connecté ; éteint si déconnecté.	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 Rouge éteint	Vert éteint Rouge éteint	Eteint	Vert 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 allumé fixe	Vert éteint Rouge allumé fixe	Eteint	Vert éteint Rouge allumé fixe

Etat de fonctionnement		Voyants						
		RUN (vert)	**UACNX** (vert/ rouge)	**ERR** (rouge)	**BS** (vert/ rouge)	**NS** (vert/rouge)	**BUSY** (jaune)	**SEC** (vert/ rouge)
Cybersecurity (ou Security) Reset	En cours	Clignotant	Eteint	Eteint	Vert éteint Rouge allumé fixe	Vert éteint Rouge allumé fixe	Allumé	Vert éteint Rouge éteint
	Terminé	Allumé	Eteint	Eteint	Vert éteint Rouge allumé fixe	Vert éteint Rouge allumé fixe	Eteint	Vert éteint Rouge éteint
Réinitialisation de cybersécurité (ou de sécurité) manquante[3]		Eteint	Eteint	Allumé	Vert éteint Rouge allumé fixe	Vert éteint Rouge allumé fixe	Eteint	Rouge clignotant
Mise à jour du système d'exploitation		Clignotant	Eteint	Eteint	Vert éteint Rouge allumé fixe	Vert éteint Rouge allumé 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 sélecteur rotatif est dans une position valide.

2. Consultez les codes d'erreur détectée SERVICES_STATUS dans le DDT T_BMENUA0100, page 142.

3. Cet état résulte du changement de position du commutateur rotatif du mode Standard au mode Advanced (ou Secured) ou du mode Advanced (ou Secured) au mode Standard sans passer par l'étape de réinitialisation de la cybersécurité (ou de la sécurité), page 29.

NOTE: Dans ce tableau, "/" représente 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-après :

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 24 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.
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 147 du logiciel Control Expert.
s

NOTE: Si le DDT du module ne peut pas être lu pour une raison quelconque (par exemple, l'adresse IP de l'embase n'est pas correctement configurée), vous pouvez effectuer des diagnostics du module via ses voyants, page 137.

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
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	–

Elément	Type	Adresse	Description
PORT_CONTROL_LINK	BOOL	MW57.0	• 0 : La liaison du port de contrôle n'est pas opérationnelle. • 1 : La liaison du port de contrôle est opérationnelle.
ETH_BKP_PORT_LINK	BOOL	MW57.1	• 0 : La liaison du port d'embase n'est pas opérationnelle. • 1 : La liaison du port d'embase est opérationnelle.
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	Voir détails ci-dessous.
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 ne peut pas être intégrée dans le contrôleur. ◦ 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** configuration 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 • 2 : Mode de redondance non transparent ("Hot").
SERVICE_LEVEL	BYTE	MW60[1]	Intégrité du serveur OPC UA, page 154 en fonction de la qualité des données et des services.
Réservé	WORD	MW61	–
SERVICES_STATUS	T_ SERVI-CES_ STATUS	MW62...68	Voir détails ci-dessous.
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 horaire (l'heure du serveur a augmenté ou diminué d'au moins 1000 secondes. La synchronisation du module BMENUA0100 peut prendre jusqu'à 5 minutes.) ◦ 4 = Le serveur NTP est toujours accessible, mais il ne synchronise pas le client. Lorsque le serveur NTP reprend ses opérations, l'erreur détectée est résolue automatiquement. Cela peut prendre jusqu'à 1024 secondes.
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 Advanced (ou Secured) uniquement : ◦ 1 = Port de contrôle non configuré ◦ 2 = Client NTP de l'embase et du serveur activé dans les pages Web

Elément	Type	Adresse	Description
SNMP_SERVICE	BYTE	MW63[0]	Etat du serveur SNMP : • Bit 0 : 0 = Inactif / 1 = Actif • Bit 1 (SNMP V1) : 0 = SNMP non configuré / 1 = SNMP configuré • Bits 1 et 2 : (SNMP V3) : 00 = SNMP non configuré / 11 = SNMP configuré • Bits 4 à 7 : Code d'erreur détectée : ◦ 1 = SNMP est activé en mode Advanced (ou 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 ◦ 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 Advanced (ou Secured) uniquement) : ◦ 1 = Port de contrôle non configuré **NOTE:** Pour les modules équipés du micrologiciel de version 2.01 ou ultérieure, la valeur de cet élément est forcée à 0.
CPU_TO_CPU_IP_ FORWARDING	BYTE	MW66[1]	Etat du transfert contrôleur vers contrôleur : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée (mode Advanced (ou Secured) uniquement) : ◦ 1 = Port de contrôle non configuré **NOTE:** Pour les modules équipés du micrologiciel de version 2.01 ou ultérieure, la valeur de cet élément est forcée à 0.

Elément	Type	Adresse	Description
IPSEC	BYTE	MW67[0]	Etat IPsec : • Bit 0 : 0 = Inactif / 1 = Actif • Bits 4 à 7 : Code d'erreur détectée (mode Advanced (ou Secured) uniquement) : ◦ 1 = Port de contrôle non configuré
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 Advanced (ou 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. Voir détails ci-dessous.
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 Advanced (ou 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.

Elément	Type	Adresse	Description
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 d'utilisation du processeur interne.
CYBERSECURITY_STATUS	T_CYBER SECURI-TY_ STATUS	MW79...80	Etat de la cybersécurité. Voir détails ci-dessous.
SECURE_MODE	BYTE	MW79[0]	• 0 : Le module fonctionne en mode Standard. • 1 : Le module fonctionne en mode Advanced (ou Secured).
CYBERSECURITY_STATE	BYTE	MW79[1]	Etat de cybersécurité : • 0 : Mode Advanced (ou Secured) désactivé. (VOYANT **SECURE** ETEINT) • 1 : Communications sécurisées activées et exécutées sans erreur détectée. (VOYANT **SECURE** VERT) • 2 : Prêt à communiquer. (VOYANT **SECURE** VERT CLIGNOTANT) • 3 : Communication sécurisée en cours avec erreurs détectées mineures. (VOYANT **SECURE** VERT CLIGNOTANT) • 4 : Communication sécurisée interrompue en raison d'une erreur critique détectée. (VOYANT **SECURE** ROUGE)
IPSEC_CHANNELS	BYTE	MW80[0]	Nombre de canaux IPsec ouverts.
Réservé	BYTE	MW80[1]	–

Configuration de la fonction élémentaire READ_ DDT

Présentation

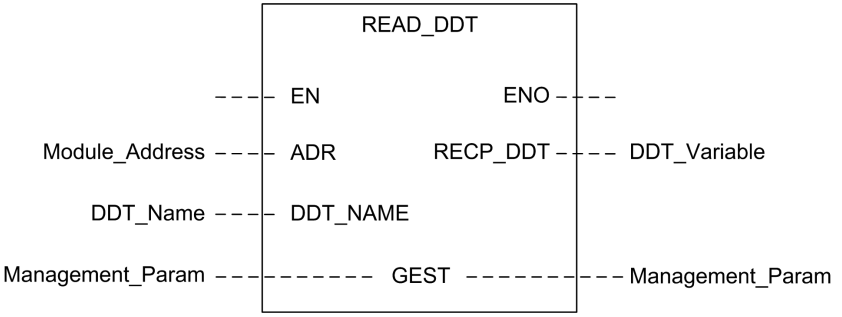
Utilisez le bloc fonction `READ_DDT` pour configurer les messages de lecture pour le module de communication BMENUA0100.

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

EN et ENO peuvent être configurés comme paramètres supplémentaires.

NOTE: Pour plus d'informations sur l'utilisation de ce bloc fonction dans un système de redondance d'UC (Hot Standby), reportez-vous à la rubrique Blocs fonction de communication asynchrone (voir *Modicon M580 - Redondance d'UC pour architectures courantes - Guide système*).

Représentation 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 pas résoudre l'algorithme des blocs fonction.
ADR	Tout tableau (Array) 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 que le module à l'adresse IP 192.168.10.2, avec UnitId 100 (serveur local du module), est 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="5">GEST</td><td rowspan="5">Array [0...3] of INT</td><td colspan="3">Paramètres de gestion, composés de quatre mots. Consultez la rubrique d'aide Control Expert Structure des paramètres de gestion (voir EcoStruxure™ Control Expert, Communication, Bibliothèque de blocs) pour plus d'informations sur ces paramètres.</td></tr>
<tr><td>N° de 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
Bit d'acquittement immédiat : rang 2</td></tr>
<tr><td>1</td><td>Rapport d'opération (voir EcoStruxure™ Control Expert, Communication, Bibliothèque de blocs)</td><td>Rapport de communication (voir EcoStruxure™ Control Expert, Communication, Bibliothèque de blocs)</td></tr>
<tr><td>2</td><td colspan="2">Timeout (voir EcoStruxure™ Control Expert, Communication, Bibliothèque de blocs)</td></tr>
<tr><td>3</td><td colspan="2">Longueur (voir EcoStruxure™ Control Expert, Communication, Bibliothèque de blocs)</td></tr>
</table>

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 réussit.
RECP_DDT	Quelconque	Mémoire tampon de réception. Une variable DDT peut être utilisée. Consultez la description du DDT de T_BMENUA0100, page 142 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, lors d'un basculement, le bloc fonction de communication asynchrone READ_DDT ne reprend pas automatiquement l'opération sur le nouveau contrôleur primaire, sauf s'il est configuré de la manière spécifique décrite ci-après :

Procédez comme suit pour permettre aux EFB de communication asynchrone de reprendre automatiquement leur opération après un basculement :

- Programmez votre application de sorte que toutes les instances EFB ne soient pas échangées avec le contrôleur 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 n'est signalée dans GEST[1] ou avec un code d'état supplémentaire. Consultez la rubrique d'aide Control Expert *Codes d'erreur des EFB avec paramètre STATUS* (voir *EcoStruxure™ Control Expert, Communication, Bibliothèque de blocs*) pour plus d'informations sur les valeurs de ces codes d'état supplémentaires.
- La valeur 0 de Timeout indique l'absence de temporisation. Dans ce cas, un retard ou une perte de communication survenant pendant l'opération d'échange n'est pas détecté (e). Le paramètre RECP_DDT conserve sa valeur précédente. Pour éviter ce scénario, définissez un timeout différent 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 des codes STATUS possibles des EFB de communication. Les valeurs possibles pour READ_DDT sont 30ss hex et 4001 hex. Consultez la rubrique d'aide Control Expert *Codes d'erreur des EFB avec paramètre STATUS* (voir *EcoStruxure™ Control Expert, Communication, Bibliothèque de blocs*) pour plus d'informations sur les valeurs de ces codes d'état supplémentaires.
- Selon le DDT spécifié dans le paramètre DDT_NAME, certaines vérifications de cohérence sont effectuées 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 tampon de réception (RECP_DDT). Vérifiez que le type de données de la variable liée au paramètre RECP_DDT correspond au type des données reçues.

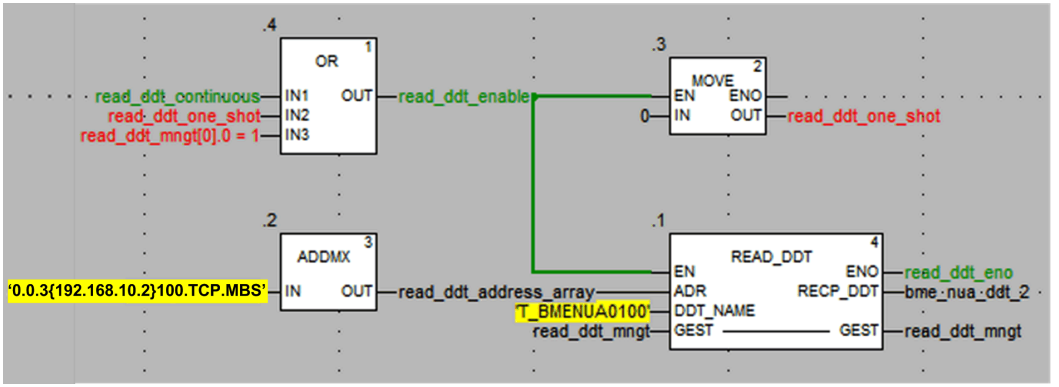
⚠AVERTISSEMENT
FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT • Vérifiez que la variable de type DDT associée au paramètre de sortie RECP_DDT correspond au type des données écrites dans le tampon de réception. • Vérifiez que l'adresse définie dans le paramètre ADR correspond au module approprié, en particulier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

Configuration de la fonction élémentaire READ_DDT

Pour configurer la fonction élémentaire READ_DDT, suivez ces étapes :

Etape	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

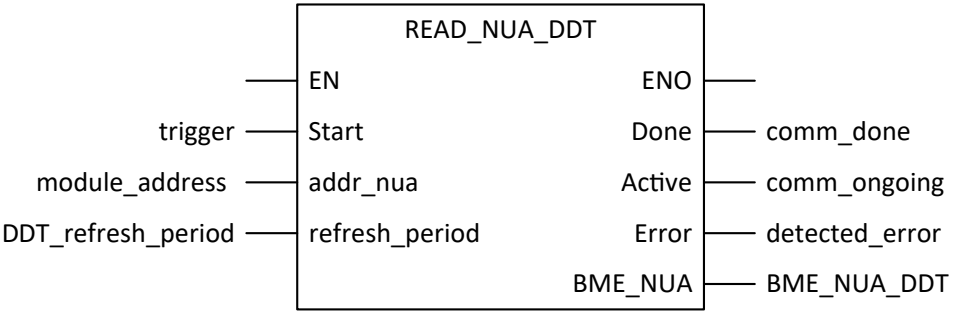
Le bloc fonction `READ_NUA_DDT` permet d'accéder aux informations de diagnostic du module BMENUA0100.

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

EN et ENO peuvent être configurés comme paramètres supplémentaires.

NOTE: Pour plus d'informations sur l'utilisation de ce bloc fonction dans un système de redondance d'UC (Hot Standby), reportez-vous à la rubrique Blocs fonction de communication asynchrone (voir *Modicon M580 - Redondance d'UC pour architectures courantes - Guide système*).

Représentation 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 résout pas l'algorithme des blocs fonction.
Démarrer	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 que le module à l'adresse IP 192.168.10.2, avec UnitId 100 (serveur local du module), est 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.
Terminé	BOOL	La communication est terminée.
Actif	BOOL	Communication en cours.

Paramètre	Type de données	Description
Erreur	BOOL	Erreur détectée sur le bloc fonction de communication.
BME_NUA	T_BMENUA0100	DDT, page 142 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 concernant l'état du contrôleur et 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 142 du module BMENUA0100, et elle est accessible par programme en exécutant la fonction élémentaire READ_DDT, page 147 lorsque l'application est à l'état RUN.

NOTE: Dans les architectures redondantes, le client OPC UA doit surveiller la variable SERVICE_LEVEL dans les modules BMENUA0100 primaire et redondant pour gérer le mécanisme de redondance. Lorsque le client détecte que la valeur SERVICE_LEVEL du module redondant est supérieure à la valeur SERVICE_LEVEL du module primaire, il 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 du contrôleur/serveur OPC UA	
	Micrologiciel = V1.0	Micrologiciel ≥ V1.1
0	BMENUA0100 est en phase d'amorçage. Le contrôleur 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 du contrôleur/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 du contrôleur est en cours. L'espace d'adressage sera mis à jour avec le nouveau contenu du dictionnaire de données.	
120[1]	Contrôleur à l'état STOP.	Contrôleur à l'état STOP STANDBY ou HALT STANDBY (contrôleur Hot Standby uniquement).
150[1]	Contrôleur à l'état WAIT STANDBY (contrôleur Hot Standby uniquement).	
199[1]	Contrôleur à l'état RUN STANDBY (contrôleur Hot Standby uniquement).	
202[2]	<Non applicable>	Contrôleur autonome seulement : contrôleur à l'état STOP STANDALONE. Contrôleur Hot Standby uniquement : Lorsque les deux contrôleurs 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	Contrôleur à l'état RUN (ou RUN PRIMARY pour un contrôleur Hot Standby). 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 s'applique uniquement au micrologiciel BMENUA0100 de version V1.10 ou ultérieure.		

NOTE: Plus la taille du dictionnaire de données est importante, plus le temps d'acquisition du dictionnaire de données est long (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. Au cours de ce processus, les mises à jour des éléments surveillés 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 génération de l'application dans le contrôleur.
BuildNumber	Numéro de génération de l'application actuelle du contrôleur.
ManufacturerName	"Schneider Electric".
ProductName	“BMENUA0100”.
ProductUri	Identifiant URI (Uniform Resource Identifier) unique attribué au module.
SoftwareVersion	Version du micrologiciel du module.

Eléments 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. Bien qu'ils ressemblent beaucoup aux éléments de données de contrôleur accessibles via le logiciel Control Expert, ces éléments de données spéciaux ne sont pas liés aux symboles du contrôleur et ne sont pas accessibles via le logiciel Control Expert :

Elément de données	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 débordement du dictionnaire de données)
#ApplicationName	STRING	0	Nom de l'application du contrôleur.
#ApplicationVersion	STRING	0	Version de l'application du contrôleur.
#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	Nom de la référence du contrôleur.

Elément de données	Type de données	Valeur par défaut	Description
#PLCDatadicReady	BYTE	1	Surveille l'état de chargement du dictionnaire de données du contrôleur : 1. Le dictionnaire de données du contrôleur n'est pas disponible. Explications possibles : • La fonctionnalité de dictionnaire de données n'est pas disponible ou activée dans l'application Control Expert et ne peut pas être intégrée dans le contrôleur. • Le chargement ou la consultation du dictionnaire de données est en cours sur le serveur OPC UA. 2. Le dictionnaire de données du contrôleur 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	Surveille l'état de communication d'un contrôleur. Valeurs (hex) possibles : • 00C0 hex : La communication avec le contrôleur est correcte. • 0040 hex : Aucune communication avec le contrôleur pendant une durée inférieure à la temporisation de l'équipement (5 s). • 0 hex : contrôleur non identifié.

Elément de données	Type de données	Valeur par défaut	Description
#TSEventItemsReady	BOOL	0	Elément en lecture seule qui indique si des variables horodatées à la source et des équipements d'horodatage à la source ont été explorés dans l'application du contrôleur 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 au contrôleur M580 chaque fois qu'une opération d'écriture est effectuée. L'objectif est d'initialiser tous les éléments surveillés horodatés à leurs valeurs. • 0 = en attente d'activation • 1 = activé **NOTE:** • La valeur affichée pour cet élément est 0. La valeur 1 n'apparaît pas car elle n'existe que momentanément et revient à la valeur d'activation en attente (0). • 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 une mémoire tampon locale de diagnostics, puis les envoie à un serveur Syslog distant où ils sont stockés et mis à disposition des clients Syslog. Pour diagnostiquer des événements anciens, vous pouvez interroger les enregistrements d'événements du serveur Syslog. En ce qui concerne les événements en cours, vous pouvez utiliser les pages Web du module, page 161 pour diagnostiquer l'état du service Syslog et afficher des événements spécifiques de 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 saturée.

Le module stocke les événements dans la mémoire volatile.

Les événements journalisés concernent soit :

- Sécurité/Autorisation, page 160

  – ou –

- Modifications majeures sur le système (audit), page 161

Le service Syslog est configurable dans les pages Web, page 96 dans le cadre de la configuration de la cybersécurité. Il ne peut donc être actif que si le module fonctionne en mode Advanced (ou Secured). Lorsque le module fonctionne en mode Standard, ce service est désactivé.

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

NOTE: Syslog n'étant pas un protocole sécurisé par nature, il doit être encapsulé dans un canal sécurisé IPsec, page 103 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 :

<table>
<tr><th>Champ</th><th>Description</th></tr>
<tr><td>PRI</td><td>Informations sur la catégorie et la gravité (description fournie dans les tableaux suivants).</td></tr>
<tr><td>VERSION</td><td>Version de la spécification du protocole Syslog (Version = 1 pour RFC 5424.).</td></tr>
<tr><td>TIMESTAMP</td><td>Le format d'horodatage provient de RFC 3339 qui utilise le format de date et d'heure Internet ISO8601 suivant : YYY-MM-DDThh:mm:ss.nnnZ
NOTE: -, T, :, . et Z sont des caractères obligatoires qui font partie du champ d'horodatage. T et Z doivent être écrits en majuscules. Z indique que l'heure est UTC.
Description du contenu du champ d'horodatage :
<table>
<tr><td>YYY</td><td>Année</td></tr>
<tr><td>MM</td><td>Mois</td></tr>
<tr><td>DD</td><td>Jour</td></tr>
<tr><td>hh</td><td>Heure</td></tr>
<tr><td>mm</td><td>Minute</td></tr>
</table>
</td></tr>
</table>

Champ	Description
	<table><tr><td>ss</td><td>Seconde</td></tr><tr><td>nnn</td><td>Fraction de seconde en milliseconde (0 si non disponible)</td></tr></table>
HOSTNAME	Identifie la machine qui a 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.
MSGID	Identifie le type de message auquel l'événement est lié, par exemple HTTP, FTP, Modbus.
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). • Adresse de l'homologue : Adresse IP de l'homologue si un homologue est impliqué dans l'opération. • 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 de l'ouverture de canal sécurisé depuis la pile OPC UA : certificat non valide, certificat expiré...
- Sessions utilisateur 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.
- Echec de sessions 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 consignant l'échec de connexion n'est créée.
- Connexions HTTPS établies vers ou depuis un outil (connexion réussie) : par exemple, connexion au serveur Web ou téléchargement de micrologiciel via HTTPS.
- Echec de connexion HTTPS vers ou depuis un outil : par exemple, échec de connexion au serveur Web ou échec d'un 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. Cette action est effectuée en positionnant le sélecteur rotatif de mode de fonctionnement sur Cybersecurity (ou Security) Reset.
- Ajout d'un nouveau certificat client de la liste approuvée dans l'équipement.
- Suppression d'un certificat client de la liste approuvée dans l'équipement.

Evénements relatifs à des modifications majeures dans le système (audit)

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

Diagnostic des pages Web Syslog

Utilisez les pages Web du module pour diagnostiquer l'état du service Syslog exécuté sur le module ainsi que des zones spécifiques de la mémoire tampon de diagnostic Syslog du module. Vous pouvez également utiliser l'élément SERVICES_STATUS du DDT, page 142 du module pour afficher l'état du service Syslog.

Dans le menu **Diagnostics > Diagnostic via le journal d'événements**, utilisez les commandes suivantes pour afficher l'état du service Syslog du module :

Paramètre	Description
Etat	• Opérationnel : le module fonctionne en mode Advanced (ou Secured) et le service Syslog est activé. • Non opérationnel : le module fonctionne en mode Advanced (ou Secured) mais le service Syslog est désactivé.
Serveur de consignation	• Joignable : une connexion peut être établie avec le serveur Syslog distant. • Non joignable : impossible d'établir une connexion avec le serveur Syslog distant.

Dans le menu **Diagnostics > Diagnostic via le journal d'événements**, entrez dans le champ **Tampon de diagnostic à lire** la partie de la 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. Modbus n'étant pas un protocole sécurisé par nature, 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 Advanced (ou Secured) : Le module BMENUA0100 accepte le flux de données de client Modbus TCP/IP en provenance du contrôleur 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	00 hex	Nom du fournisseur	Chaîne ASCII
	01 hex	Code produit	Chaîne ASCII
	02 hex	Révision majeure/mineure	Chaîne ASCII
Normal	03 hex	URL fournisseur	Chaîne ASCII
	04 hex	Nom du produit	Chaîne ASCII
	05 hex	Nom du modèle	Chaîne ASCII
	06 hex	Nom de l'application utilisateur	Chaîne ASCII
	07 à FF hex	Réservé	Chaîne ASCII

Diagnostics SNMP

Introduction

Lorsque l'agent SNMP est configuré, page 132, 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 du contrôleur.
Identité de l'équipement	Référence du contrôleur.
Version de l'équipement	Version de micrologiciel du contrôleur.
Statut de l'équipement	Etat de la connexion avec le contrôleur : **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.

Champ	Description
Nombre maximum de voies	Nombre de connexions ouvertes par le serveur OPC UA sur le contrôleur.
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 126.
Longueur de requête	Longueur de la requête de communication avec le contrôleur.
Nom de l'application (équipement)	Nom du projet Control Expert.
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 contrôleur.
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, pas d'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 (BMECRA31310, contrôleur, etc.). • Adresse IPv4. • Réservation du tampon d'horodatage d'équipement par le serveur OPC UA intégré au BMENUA0100 : VRAI / 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 121 : • VRAI = sélectionné • FAUX = non sélectionné
Nombre de sessions connectées	Nombre total de sessions client prises en charge par le serveur OPC UA intégré au module BMENUA0100.

Champ	Description
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 :	
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, sa stabilité et sa robustesse dans chaque phase du mode de fonctionnement (connexions, navigation, abonnement, surveillance, etc.).

NOTE:

- Ajoutez des éléments sous forme de paquets de 2000 éléments maximum. L'intervalle d'échantillonnage configuré n'est pertinent que s'il est supérieur ou égal au temps de scrutation MAST du contrôleur.
- Définissez le paramètre CallTimeout sur une valeur supérieure ou égale à 10 secondes dans le client OPC UA.
- Le paramètre General.SecureChannelLifetime pour la communication avec un client OPC UA est réglé par défaut sur 3 600 000 ms (1 heure). Utilisez ce réglage par défaut pour éviter une réduction des 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 commutateur rotatif en position Standard (autrement dit : pas de communication sécurisée, pas de canal IPsec).
- Le client OPC UA (UAExpert) lance la communication avec le mode de sécurité des messages défini sur **Aucun** et il surveille 20 000 éléments par référence à des variables selon un tableau (array) de types "INT" provenant 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 d'application de données du contrôleur 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.

Ainsi, pour les variables auxquelles le client OPC UA accède :

- Utilisez autant que possible des tableaux (type Array) ou une structure de données.
- Activez l'option **Variable IHM uniquement** dans les **Données intégrées de l'automate** (**Options du projet**) et définissez uniquement les variables avec l'attribut **IHM** pour réduire la taille du dictionnaire de données.
- Dans l'application du contrôleur de sécurité, 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 du contrôleur

La capacité du système de communication dépend de la référence de contrôleur M580 et de certains paramètres de configuration. La référence du contrôleur détermine :

- Les performances de traitement à l'échelle du système.
- Le nombre de requêtes pouvant être traitées par cycle, même si ce paramètre est configurable via le mot système %SW90.
- Le nombre maximum de canaux dont dispose chaque BMENUA0100 pour établir des connexions au contrôleur M580, page 176.

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 (aucun, signature, signature et cryptage), l'algorithme de calcul de la signature et du cryptage prend du temps supplémentaire.

Communications entre contrôleurs et de Control Expert à contrôleur

Chaque tunnel IPsec utilisé pour sécuriser des communications autres que OPC UA ou HTTPS ralentit le trafic, en particulier lorsque le paramètre **Confidentialité** est activé car il génère de l'activité de cryptage et décryptage.

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 du contrôleur M580 à l'échelle du système, pour chaque tâche et pour la totalité des tâches, via la lecture des mots système %SW110 à %SW116. En outre, le DDT du contrôleur M580 et le DDT de BMENUA0100 peuvent fournir différentes informations de diagnostic liées aux performances système du contrôleur, à savoir :

- 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, d'autres informations sont fournies par le serveur OPC UA :

- Nombre d'éléments surveillés.
- Nombre d'éléments spécifiques surveillés.
- Différents intervalles d'échantillonnage en cours d'exécution.
- Nombre de requêtes générées pour les animations.
- 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 d'une unité le *nombre actuel d'abonnements*.

NOTE: Le *nombre actuel d'abonnements* est lié au serveur lui-même et ne doit pas être confondu avec le *nombre actuel d'abonnements* 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, les résultats suivants ont été observés et peuvent être instructifs.

Pour une application non liée à la sécurité avec 99000 éléments :

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 liée à la sécurité avec 99000 éléments :

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 abonnements qui vont représenter au total plus de de 30 000 éléments surveillés, configurez chaque abonnement dans le client OPC UA concerné avec une **durée de vie** de 300 secondes, ce qui représente la durée maximum d'abonnement, page 35 prise en charge par le serveur OPC UA du module BMENUA0100.

Utilisation d'objets GPO/LGPO

Gérez les certificats sur un PC hôte à l'aide d'un des outils suivants, disponibles dans le système d'exploitation Windows™ :

- Objets de stratégie de groupe (GPO - Group Policy Object) : pour gérer les 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.

L'utilisation d'objets GPO ou LGPO peut contribuer à empêcher les accès non autorisés à votre PC et à ses applications. L'utilisation des objets de stratégie de groupe GPO et LGPO désactive l'accès à la console MMC (Microsoft Management Console) Windows et prend en charge l'implémentation exclusive de la liste approuvée configurée par le logiciel.

Application de la gestion de stratégies de groupe MMC

Gérez les certificats à l'aide des outils fournis par Microsoft Windows™ pour empêcher l'ajout de certificats non autorisés au PC ou la modification de certificats auto-signés d'un client OPC UA. En l'absence d'une telle gestion, n'importe qui pourrait inclure des certificats non autorisés à la liste approuvée du BMENUA0100 gérée par l'administrateur de la sécurité.

Les outils en question 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 à la console MMC de Windows et n'autorisent l'accès qu'aux entrées de la liste approuvée qui ont été ajoutées selon les règles 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 utilisateur, page 96 du BMENUA0100 sont appliqués. Par exemple, si le nombre de **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. Avec seulement IPv6 activé, page 119, 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 les services **UC vers UC** et **Control Expert vers réseau d'équipements** sont activés alors que seul IPv6 est activé, ils apparaissent comme actifs (ON) dans la page **Accueil** alors qu'il ne le sont pas en réalité.

La communication IPv6 prend en charge uniquement la fonction de filtrage **Flux de données Control Expert vers UC**. Dans ce cas, si seule la communication IPv6 est activée, la page **Accueil** affiche correctement l'activation de l'option **CE vers UC uniquement**.

Types BOOL considérés comme types BYTE dans les structures de données du contrôleur

Dans le serveur OPC UA du BMENUA0100, chaque élément du DDT du contrôleur est affecté à un octet dans le contrôleur, même s'il est défini comme BOOL ou EBOOL dans le BMENUA0100. En utilisant le protocole OPC UA, un client peut globalement lire ou écrire un membre BOOL ou EBOOL d'une instance BMENUA0100 dans le DDT du contrôleur, avec une valeur d'octet valide autre que 0 ou 1 (par exemple, 255). Concevez votre application pour écrire ou lire uniquement les valeurs BOOL ou EBOOL 0 et 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 le micrologiciel des modules BMENUA0100 vers la plus récente version via le Web.

Avant de mettre à niveau le micrologiciel :

- Connectez-vous au BMENUA0100 dans le rôle d'installateur.
- Déconnectez les clients (Web, OPC UA, autres contrôleurs) connectés au module.

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.

NOTE: Après la mise à niveau du micrologiciel du module BMENUA0100 de la version 1.xx à la version 2.xx lorsque le BMENUA0100 est en mode Standard, vous devez effectuer une opération Security Reset, page 31 pour restaurer les paramètres par défaut du module. Sélectionnez ensuite le mode de fonctionnement de la cybersécurité Advanced (ou Secured) ou Standard pour le 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. Pour cela, après avoir rétrogradé le logiciel à l'aide de l'outil EcoStruxure™ Automation Device Maintenance, effectuez une opération Cybersecurity (ou Security) Reset, page 31 pour restaurer la configuration d'usine du module. Sélectionnez ensuite le mode de fonctionnement de la cybersécurité Advanced (ou Secured) ou Standard pour le module.

Annexes

Contenu de cette partie

Connexions de contrôleur

Contenu de ce chapitre

Connexions du serveur OPC UA au contrôleur

Connexions ouvertes

Le nombre de connexions que le module BMENUA0100 peut ouvrir vers le contrôleur M580 dépend de la capacité du contrôleur. Ainsi, les performances du module BMENUA0100 dépendent du temps nécessaire à l'exécution de la tâche MAST et du contrôleur sélectionné. Nombre maximal de connexions ouvertes par chaque module BMENUA0100 vers le contrôleur M580 :

Modèle de contrôleur	**Nombre maximum de connexions ouvertes par chaque BMENUA0100**
BMEP581020(H)	9
BMEP5820•0	9
BMEP5830•0	12
BMEP5840•0	15
BMEP585040	15
BMEP586040(C)	18
BMEH582040	9
BMEH584040(C)	15
BMEH586040	18

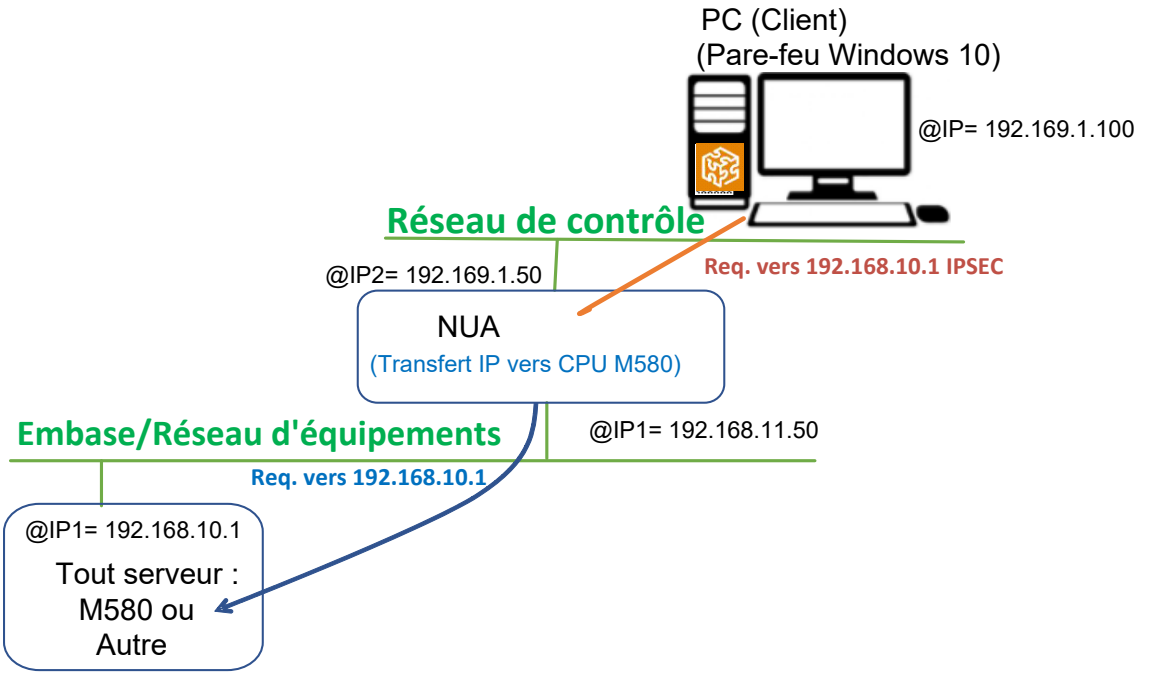
Architectures de transfert de service (IP)

Contenu de ce chapitre

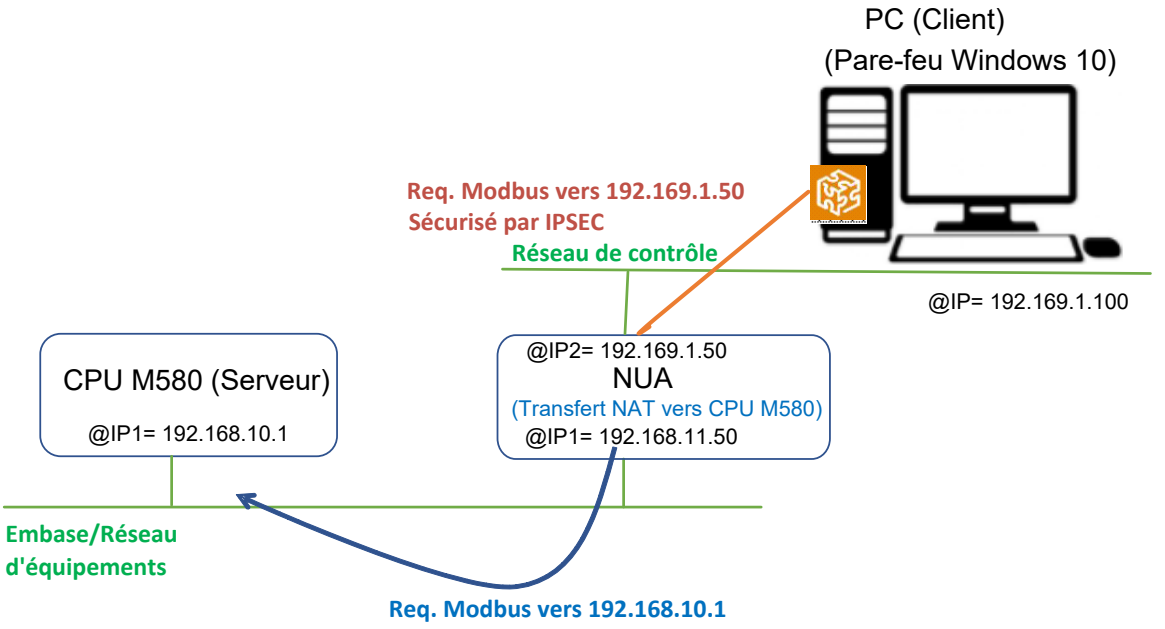
Ce chapitre présente les architectures prises en charge et non prises en charge par la fonction de transfert de service (IP) du module BMENUA0100.

Transfert de service (IP) - Architectures prises en charge

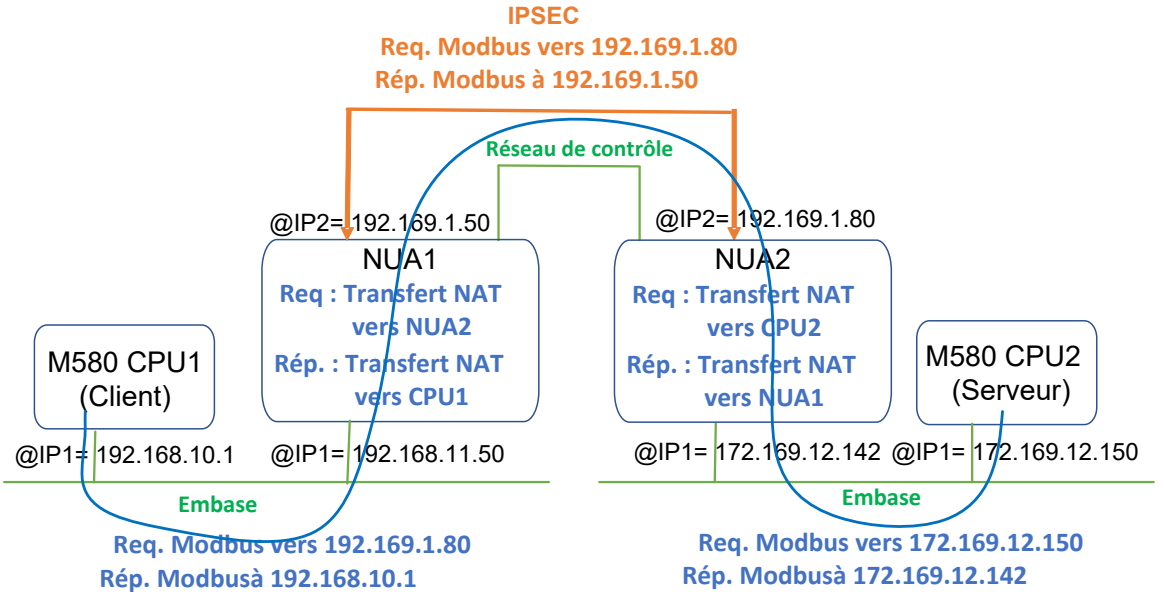
Transfert IP de client Windows (réseau de contrôle) vers n'importe quel client (embase/réseau d'équipements)



Transfert NAT de client Windows (réseau de contrôle) vers un contrôleur M580 (embase/réseau d'équipements)

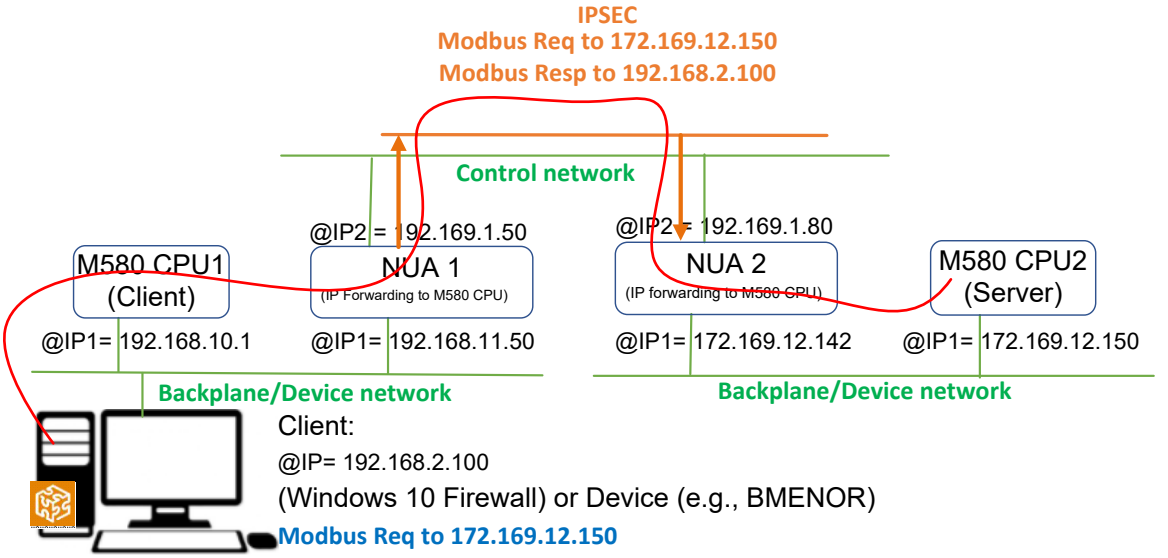


Transfert NAT entre embases pour la communication entre contrôleurs M580



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 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 y est ajoutée.

Impact du transfert IP sur les performances

Lorsque seul le transfert IP (à l'exclusion de la communication OPC UA) est activé, l'impact sur la bande passante du module BMENUA0100 est le suivant :

IPsec	Confidentialité	Transfert	Longueur de trame (octets)	Bande passante (Ko/s)
Non	N/A	Transférer tout	1000	8800
Non	N/A	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 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	N/A	Règle personnalisée	10600
0	Oui	Non	Règle personnalisée	4000
0	Oui	Oui	Règle personnalisée	2500
20000	Non	N/A	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 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 de roue dentée. Exécutez ce script pour définir le pare-feu d'hôte dans la configuration.

- 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 des scripts de configuration de pare-feu Windows avec et sans la confidentialité IPsec.

Dans chaque exemple de script, vous devez fournir des valeurs 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, utilisez `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 n'est pas activée dans la configuration IPsec, utilisez `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.

Etapes préliminaires

Cette section décrit les éléments dont vous avez besoin et les étapes préliminaires à suivre avant d'installer le serveur de certificats.

Eléments nécessaires

Les éléments suivants vous seront nécessaires :

- Microsoft Windows™ Server Manager : Téléchargeable à partir du site Web de Microsoft.
- Microsoft Windows Active Directory Certificate Server (ADCS) : Ce logiciel commercial est inclus dans Windows Server. Le module BMENUA0100 prend en charge les versions de serveur 2016 et 2019.
- Fichier TemplatePackage.zip, téléchargeable depuis le site de Schneider Electric.

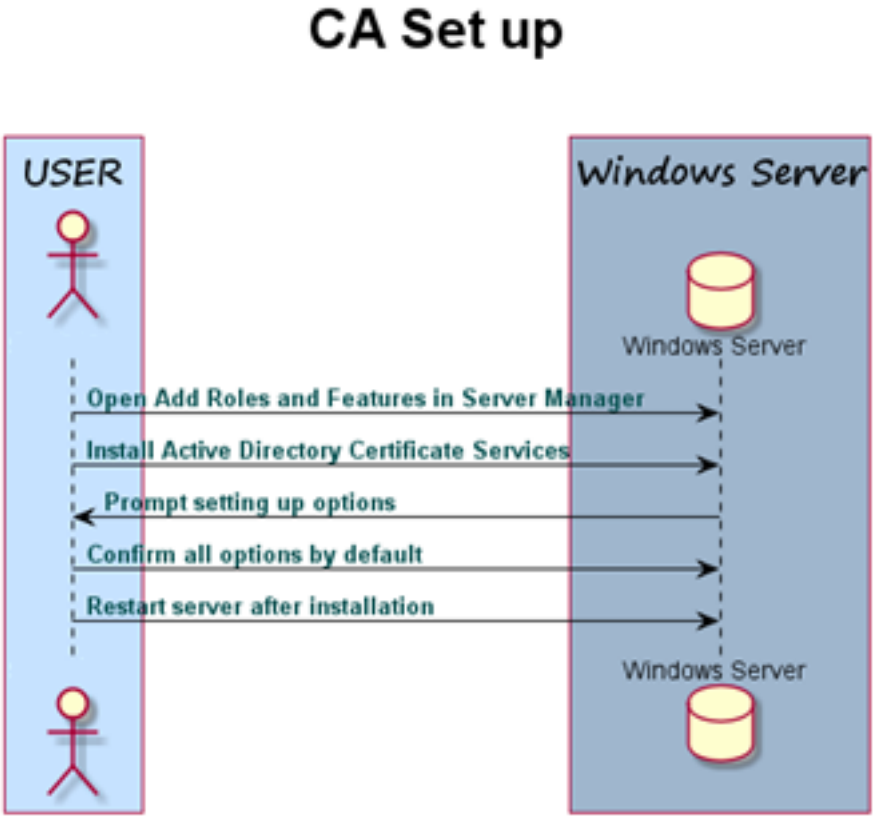
Installations de logiciel préalables

Exécutez le fichier d'installation d'ADCS, puis suivez les étapes décrites créer un compte 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 à partir du site Web de Microsoft.

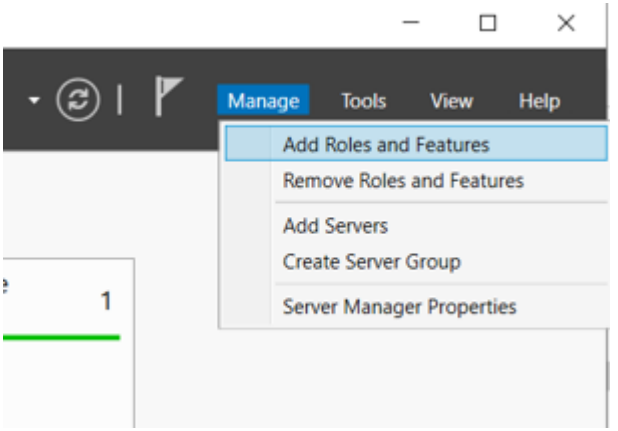
Installation du serveur de certificats Windows ADCS (Active Directory Certificate Server)

L'illustration suivante présente le processus de configuration de l'autorité de certification (CA) :

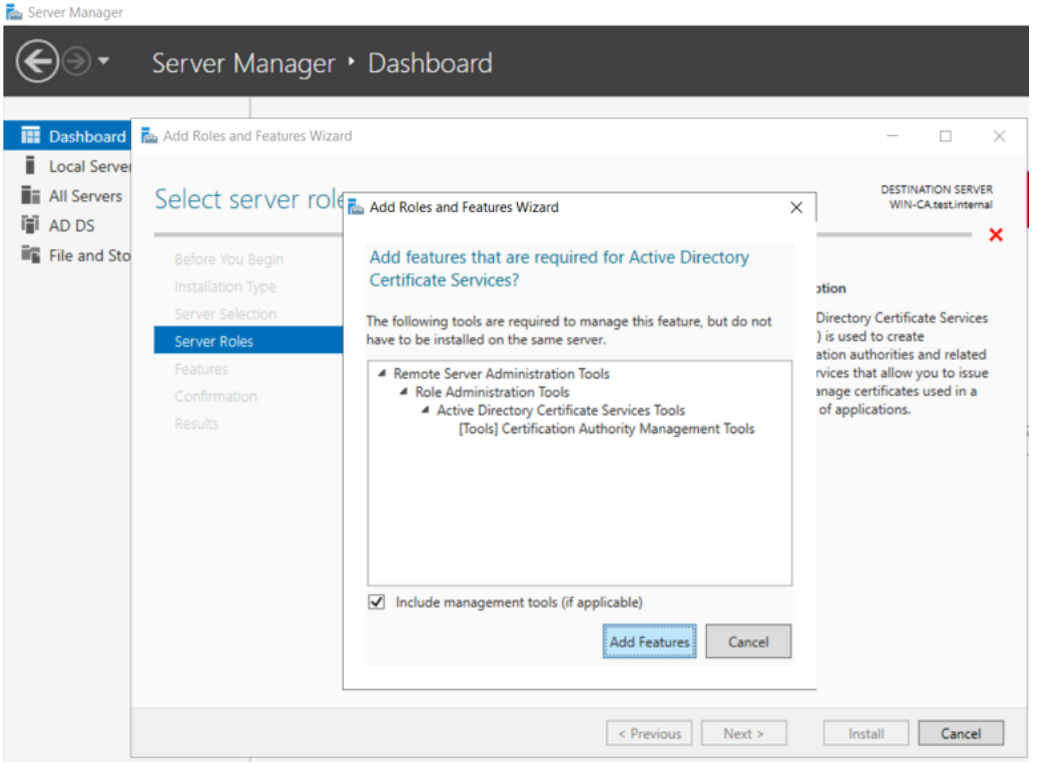


Installation du logiciel Active Directory Certificate Server (ADCS)

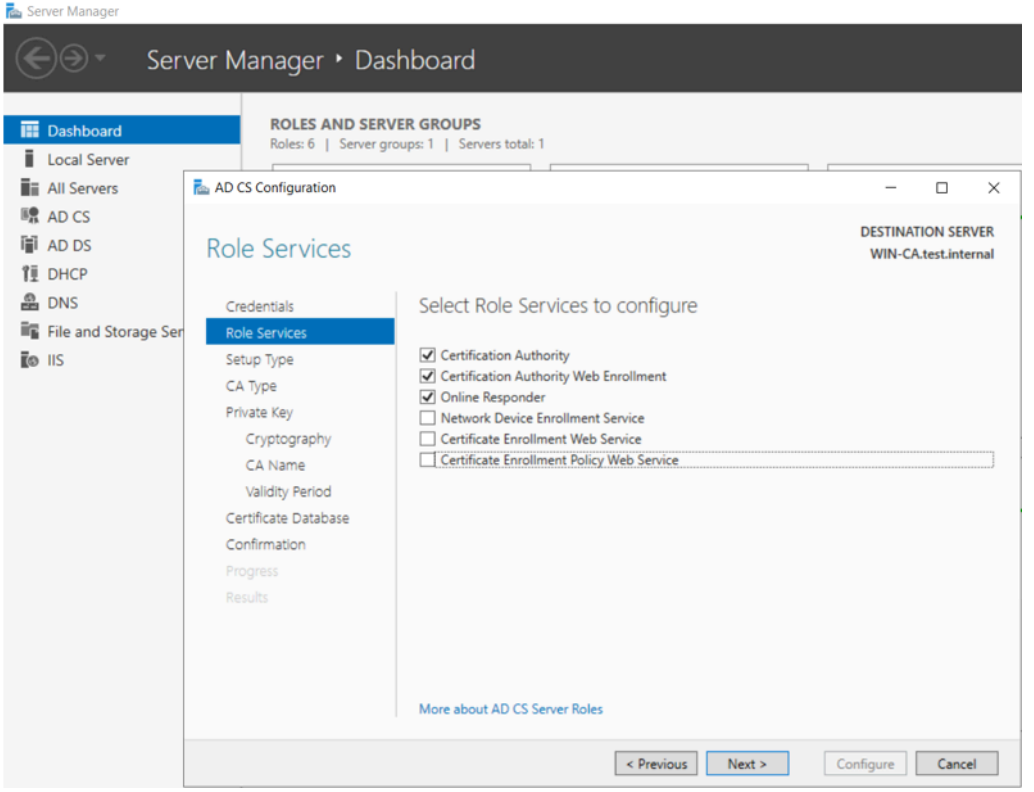
1. Lancez Microsoft Windows™ Server Manager et ouvrez le tableau de bord.
2. Sélectionnez **Gérer > Ajouter des rôles et des fonctionnalités**.



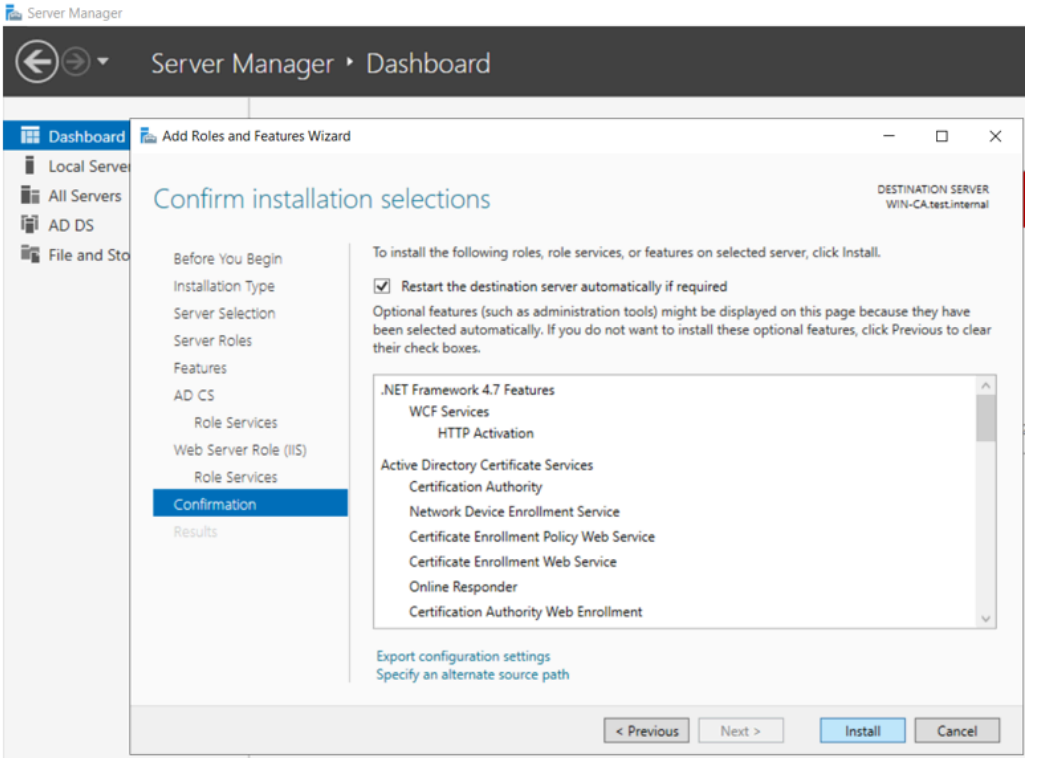
3. Ajoutez les rôles et les fonctionnalités requis et incluez les outils de gestion :



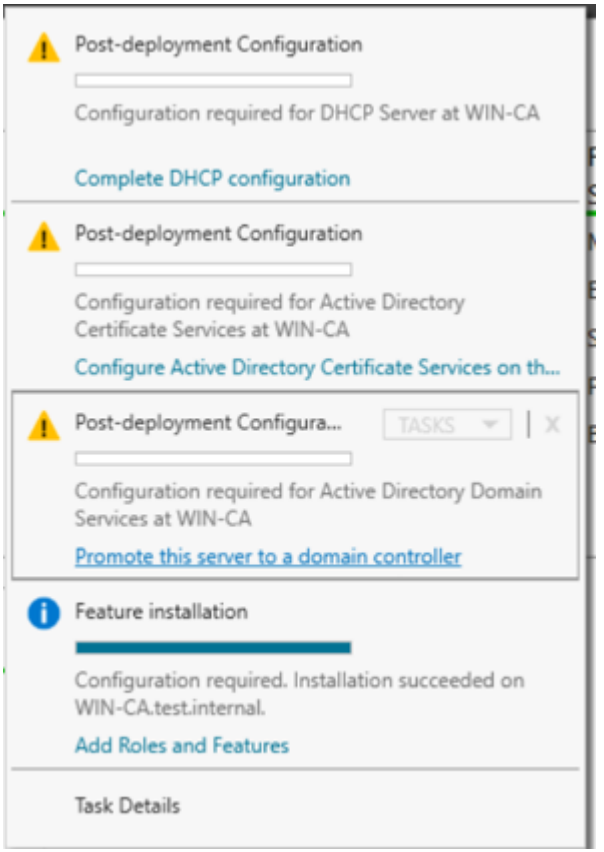
4. Sélectionnez les services de rôle à configurer :



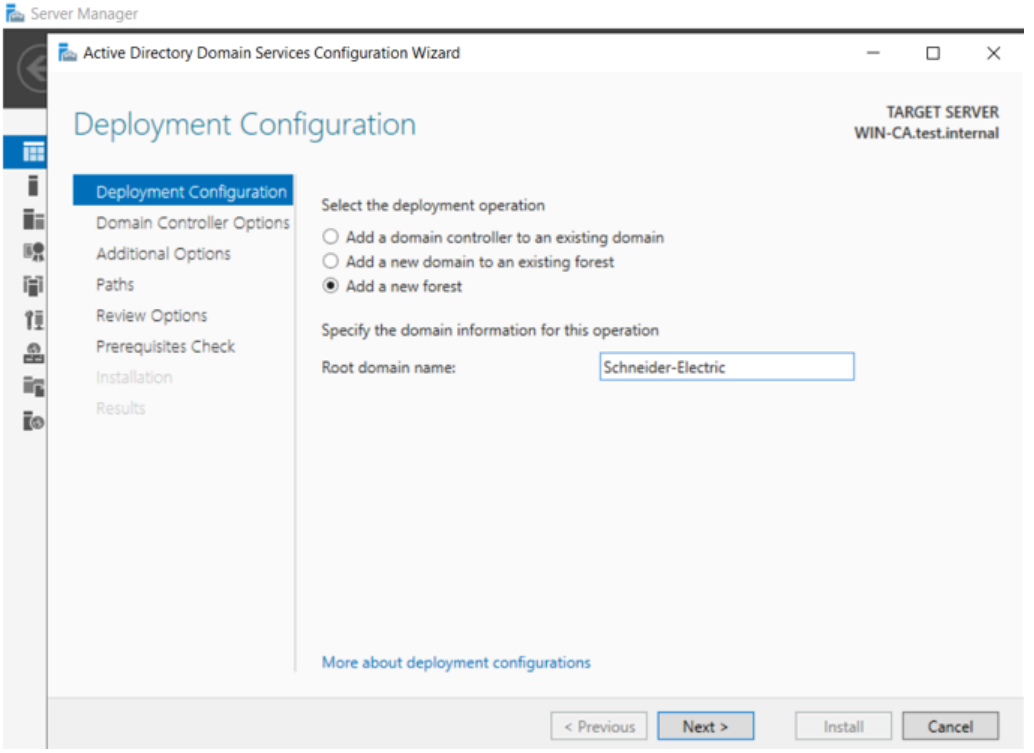
5. Confirmez les sélections d'installation :



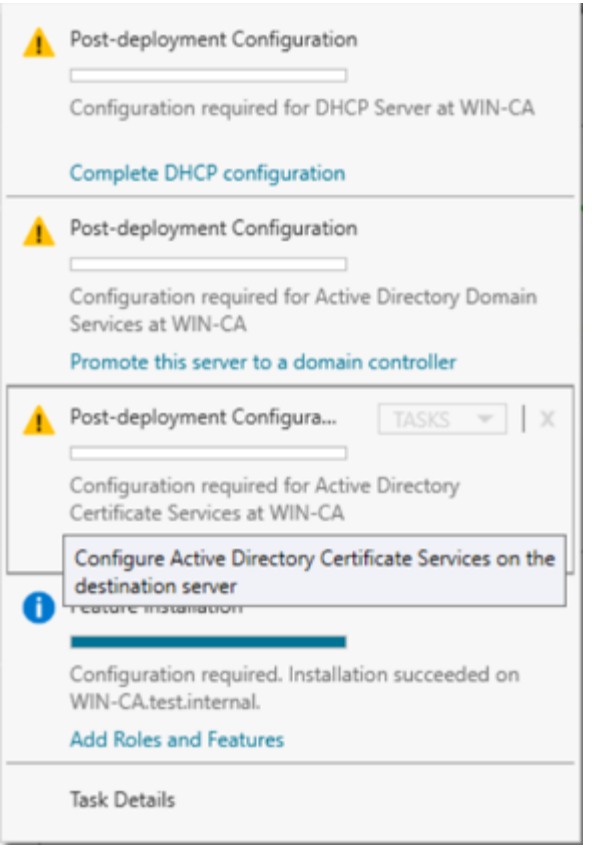
6. Cliquez sur **Installer**. Server Manager affiche la progression de l'installation :



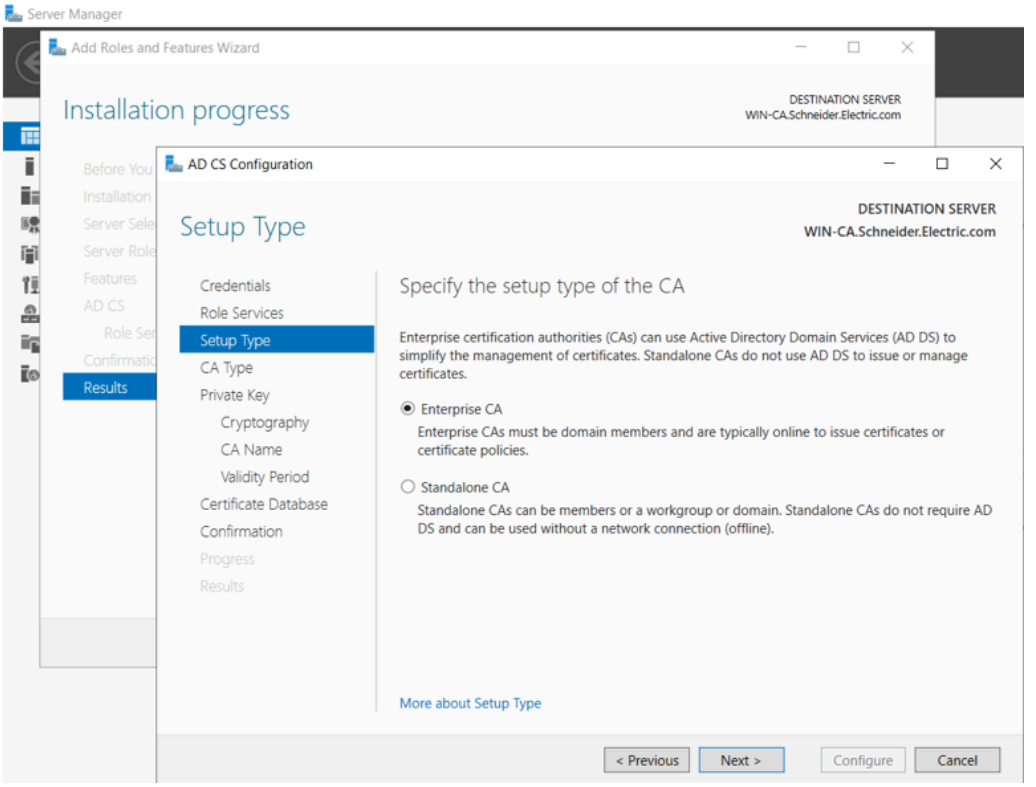
7. Sélectionnez l'opération de déploiement, en créant une nouvelle forêt ou en l'ajoutant à une forêt existante, et indiquez le domaine :



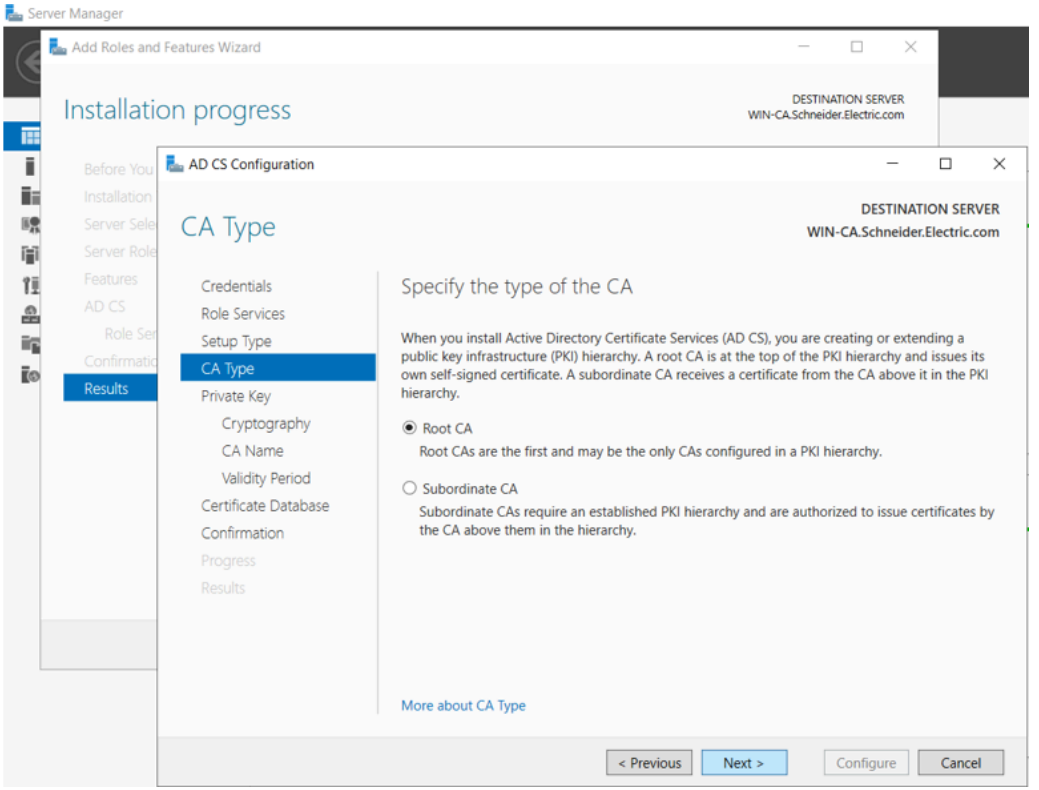
8. Server Manager affiche les sélections :



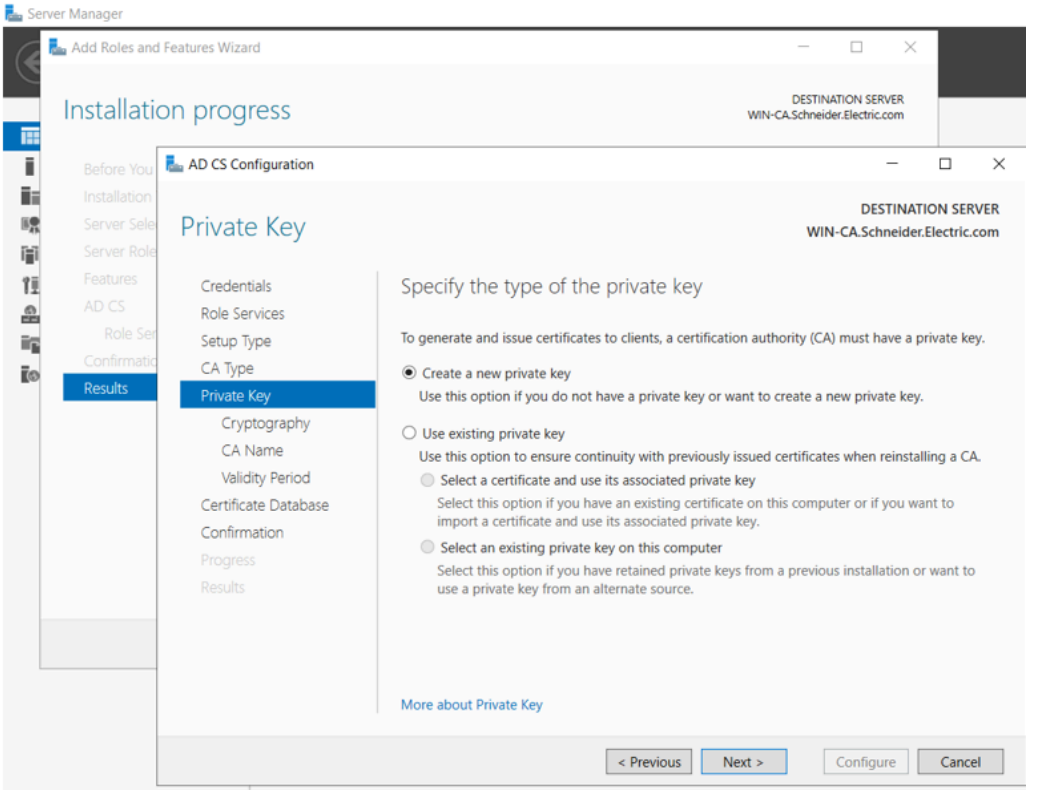
9. Spécifiez le type d'autorité de certification (CA) à configurer :



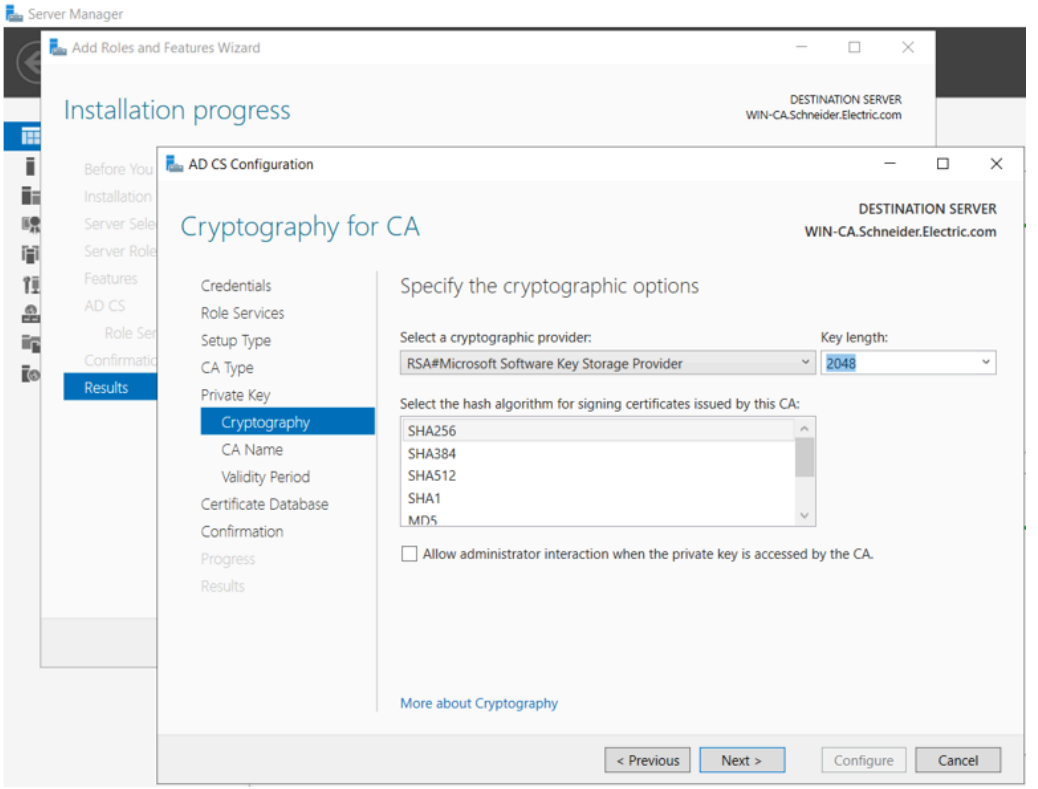
10. Spécifiez le type d'autorité de certification :



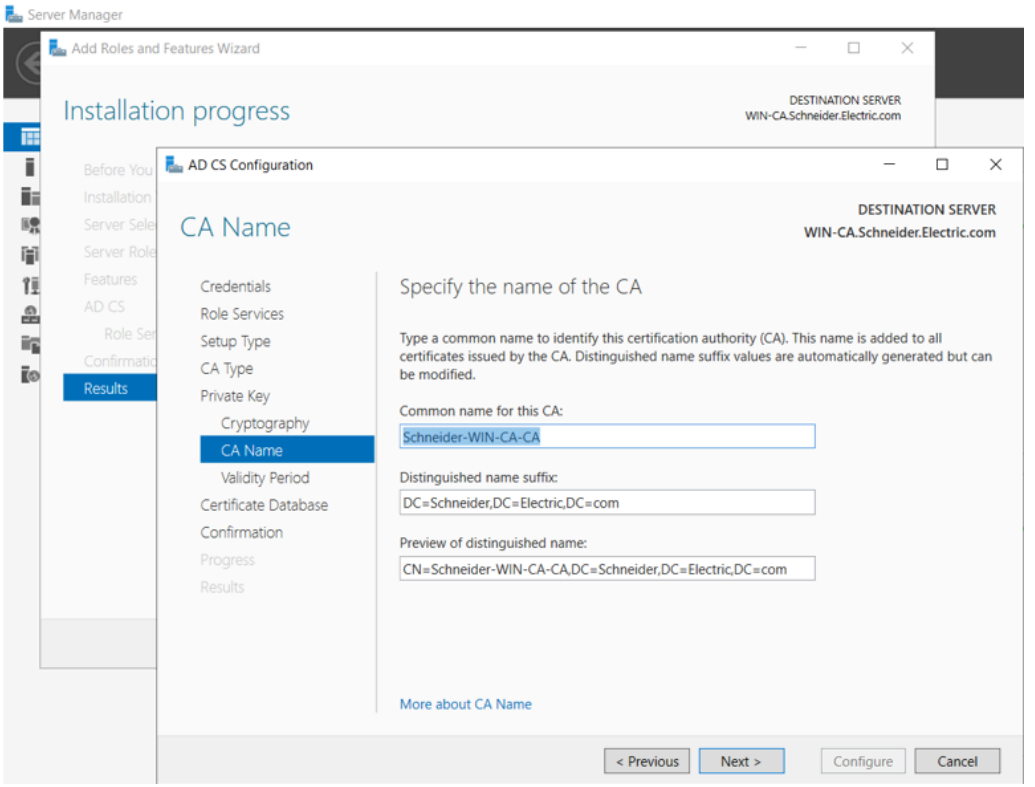
11. Spécifiez le type de clé privée :



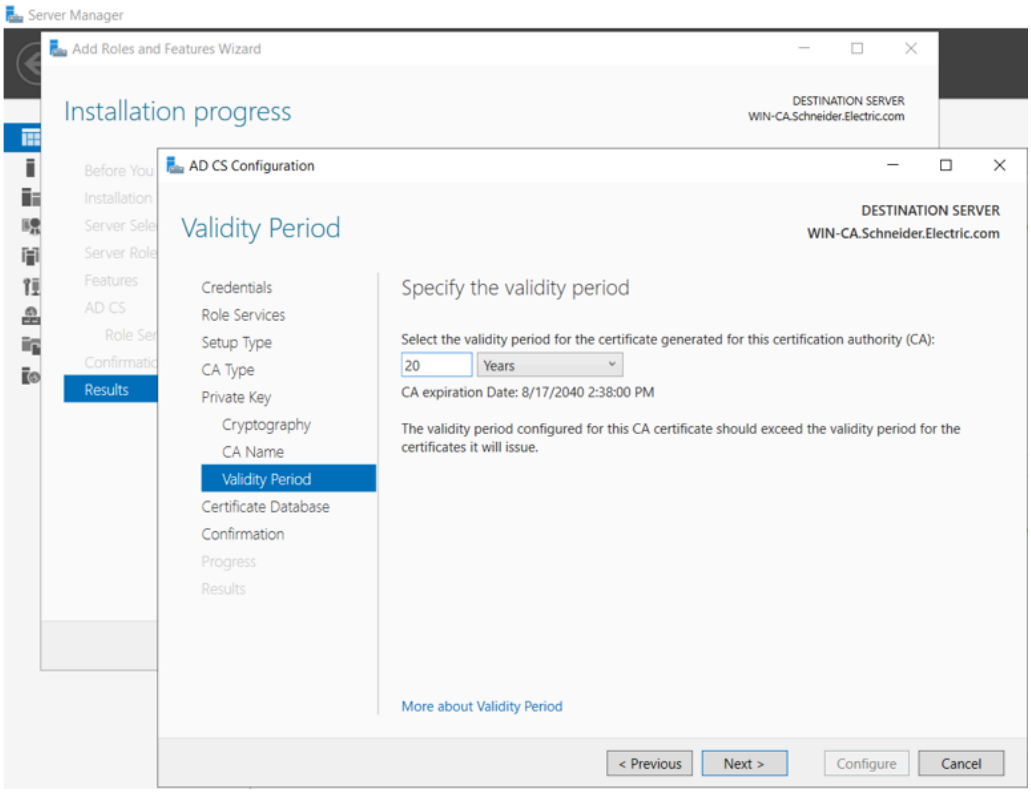
12. Sélectionnez les options de chiffrement :



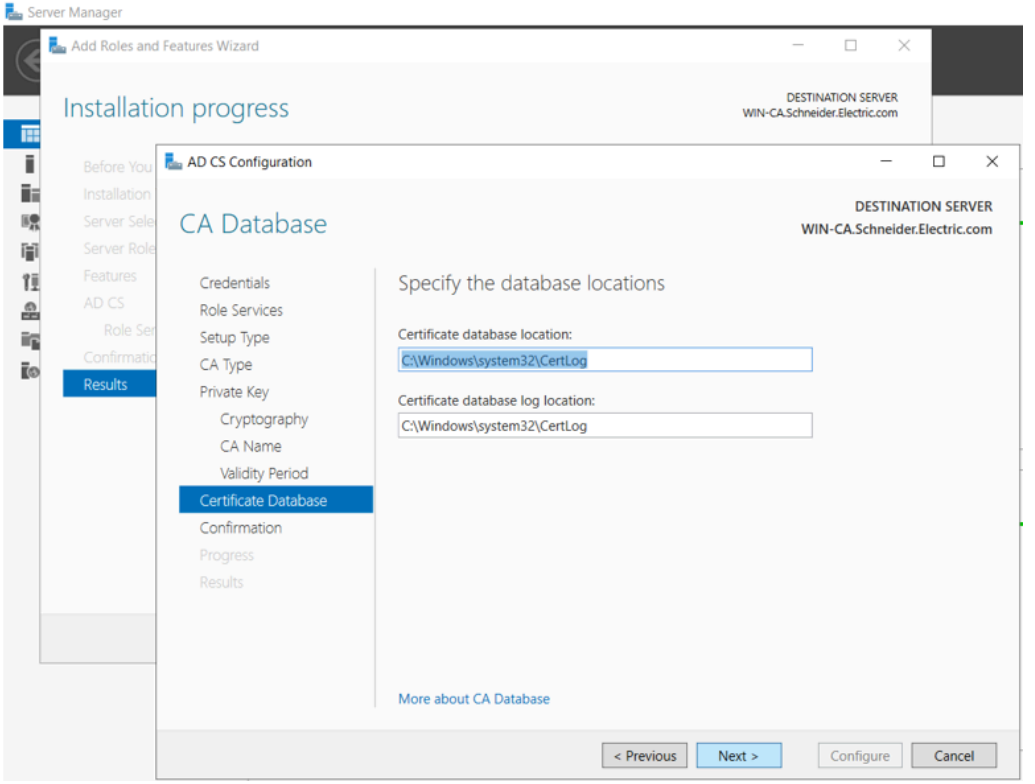
13. Spécifiez les options de dénomination pour l'autorité de certification :



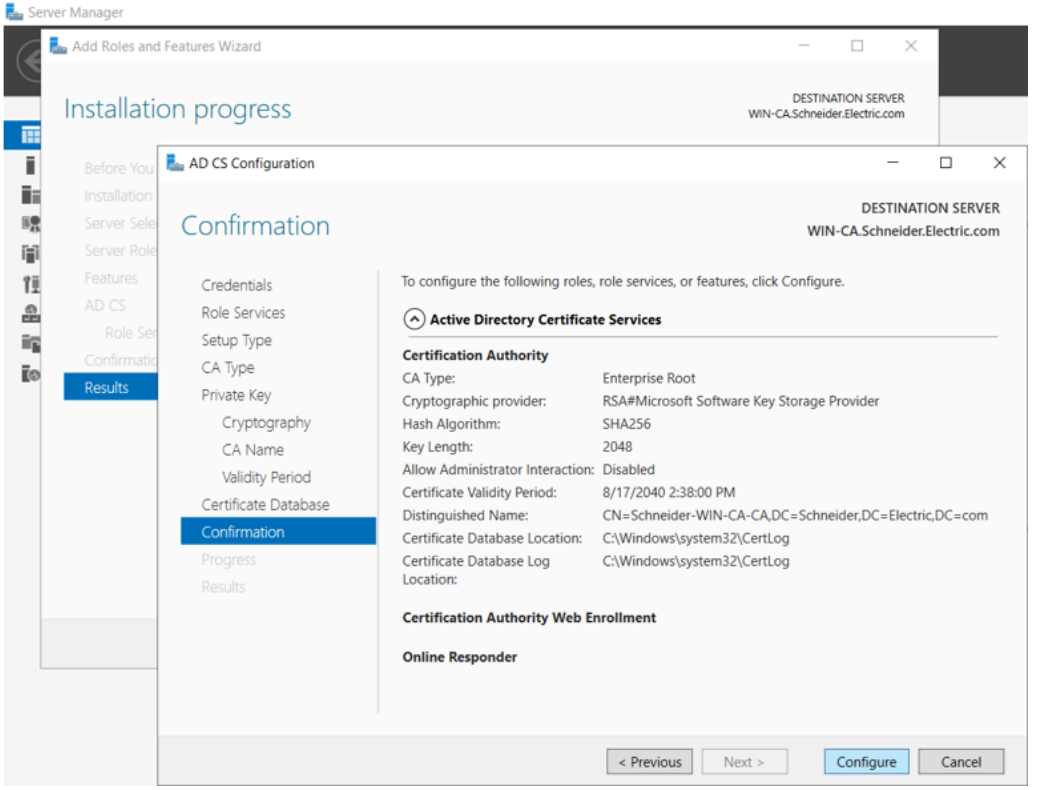
14. Indiquez la période de validité. La période de validité typique d'un certificat CA est de 5 ans :



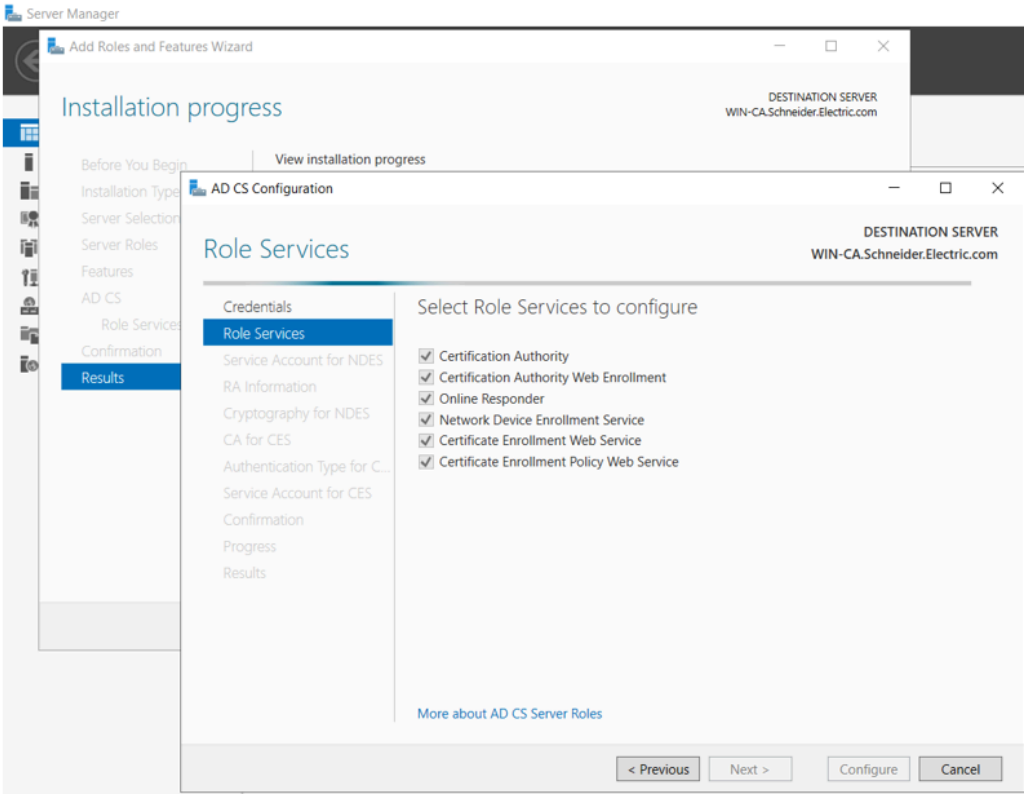
15. Indiquez les emplacements de la base de données des certificats et de l'historique :



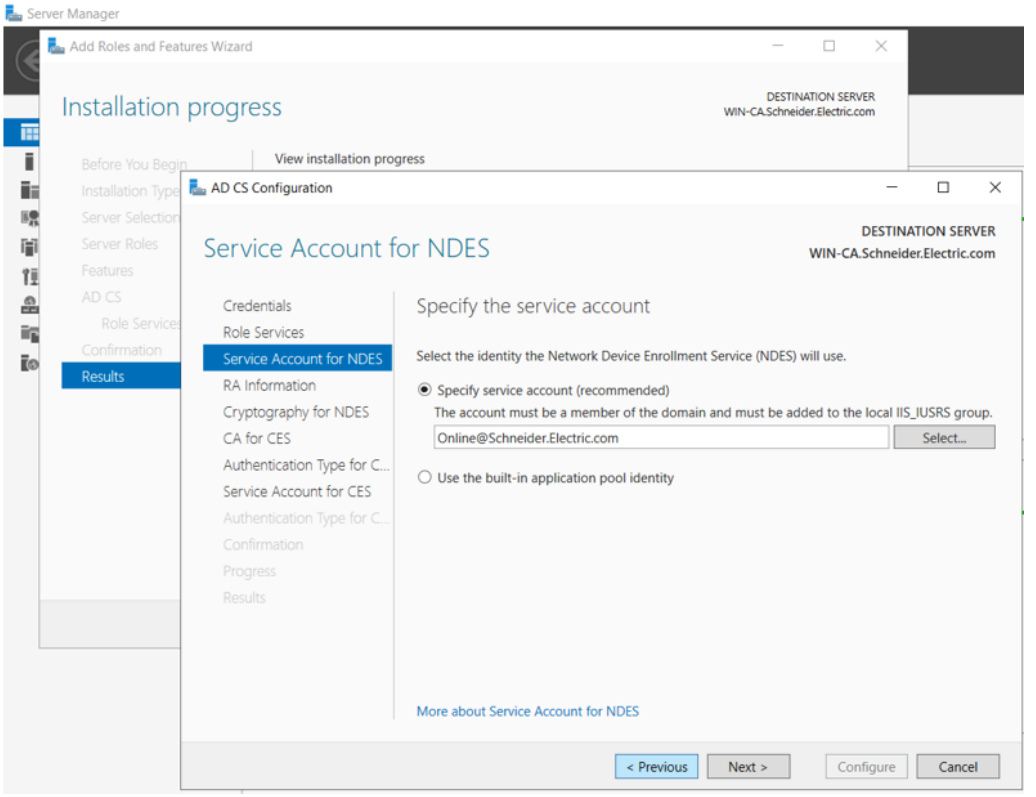
16. Confirmez les services ADCS sélectionnés et cliquez sur **Configurer** :



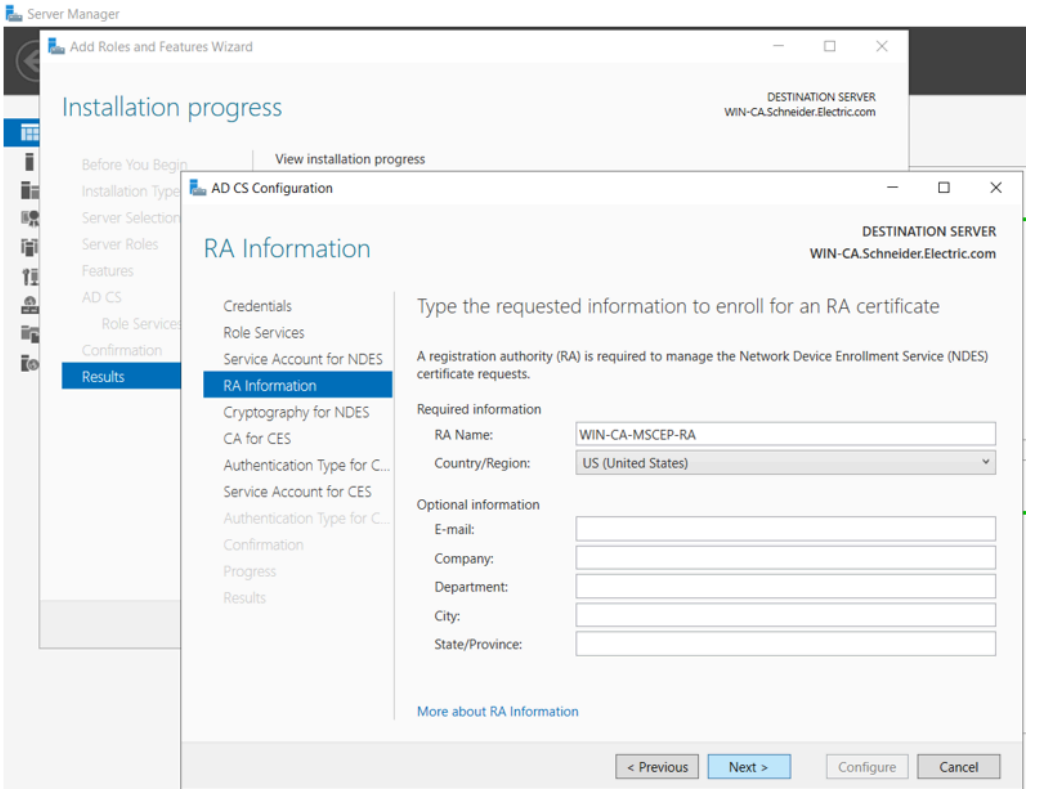
17. Sélectionnez les services de rôle à configurer :



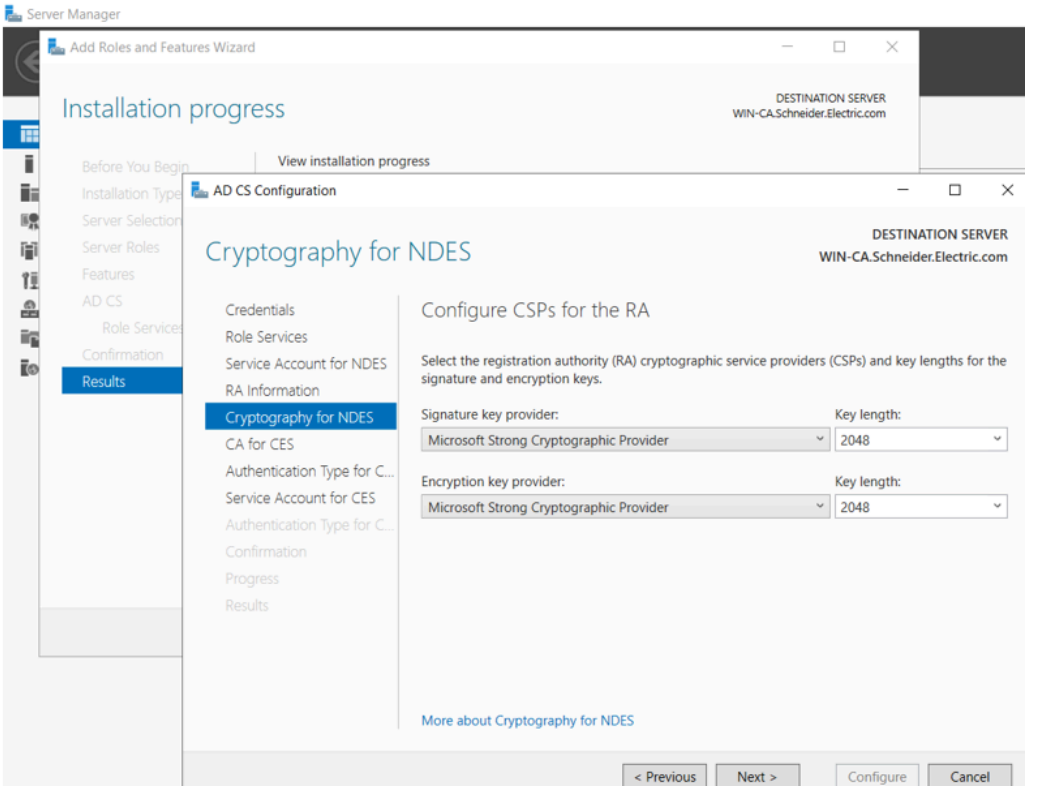
18. Indiquez le compte de service :



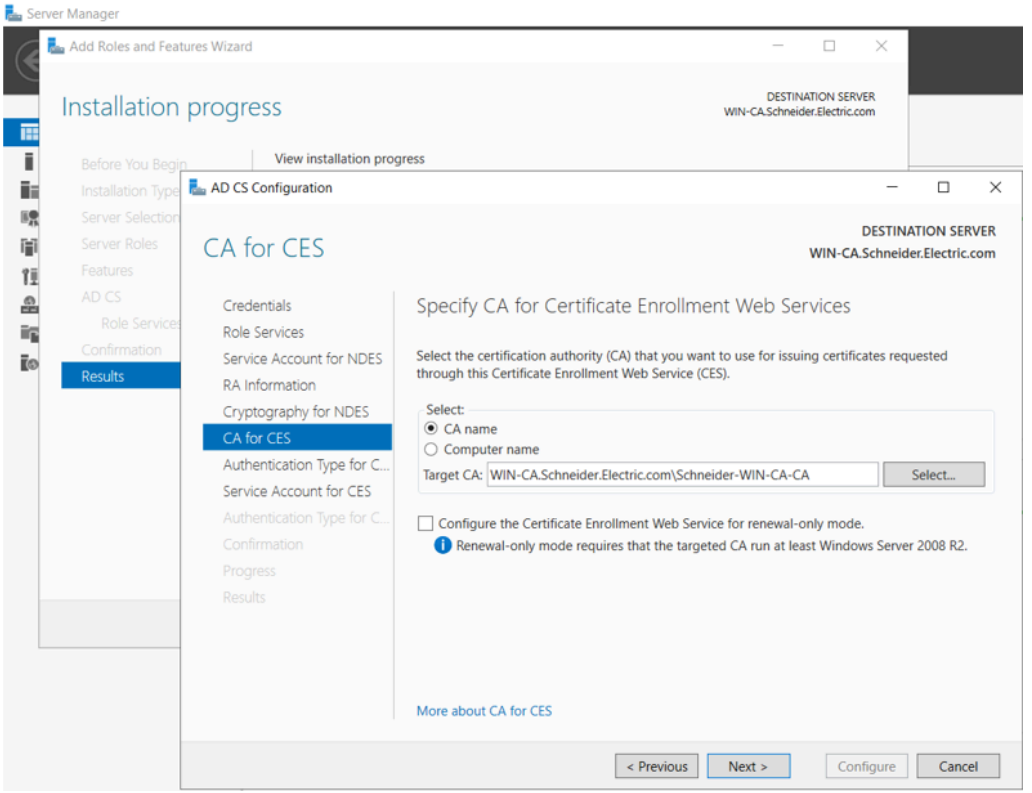
19. Entrez les informations pour adhérer à un certificat d'autorité d'inscription (RA) :



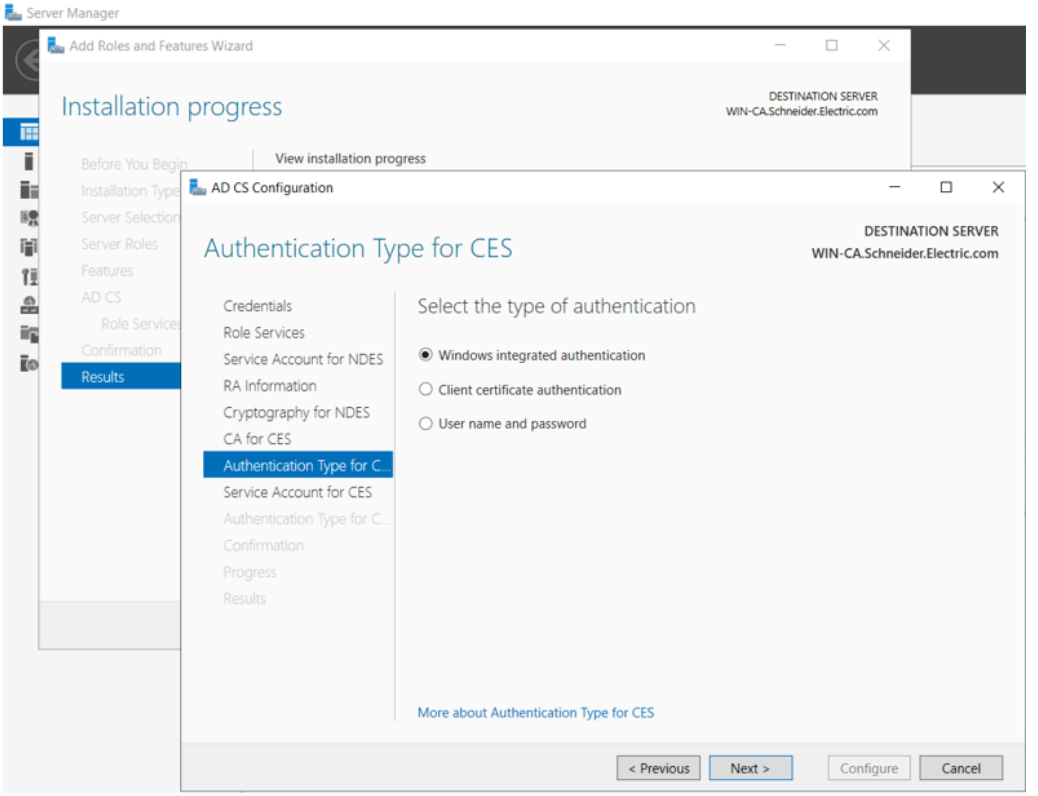
20. Sélectionnez les paramètres de chiffrement pour l'autorité d'inscription :



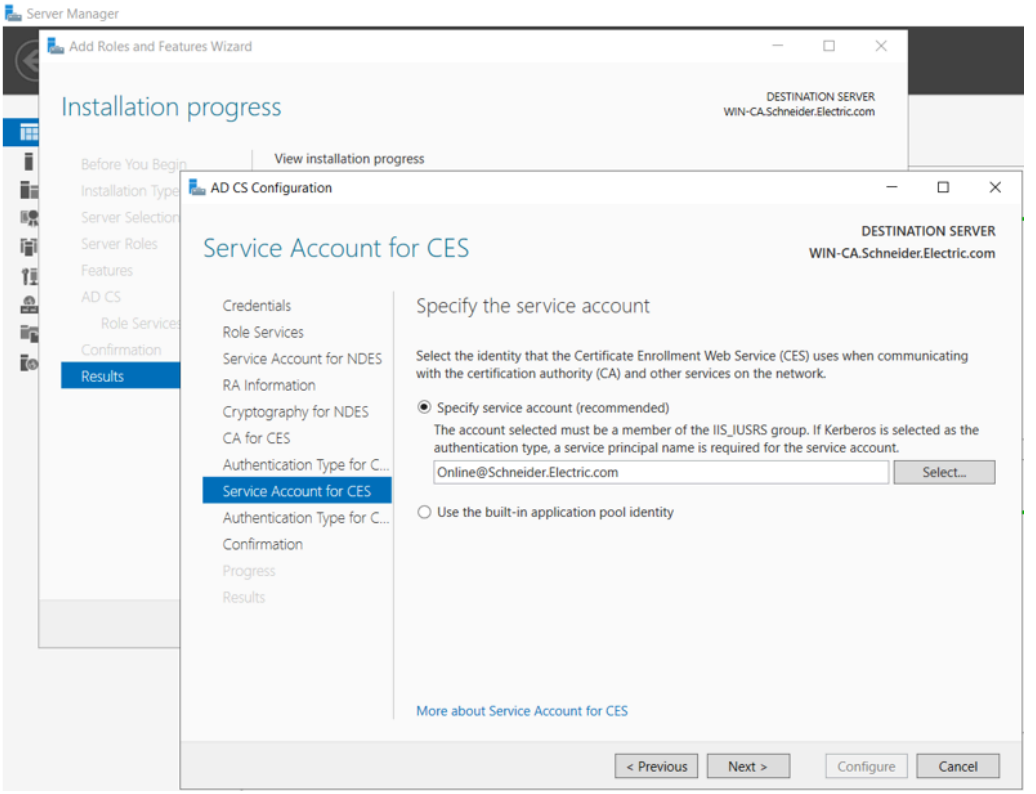
21. Spécifiez l'autorité de certification pour les services Web d'inscription de certificats :



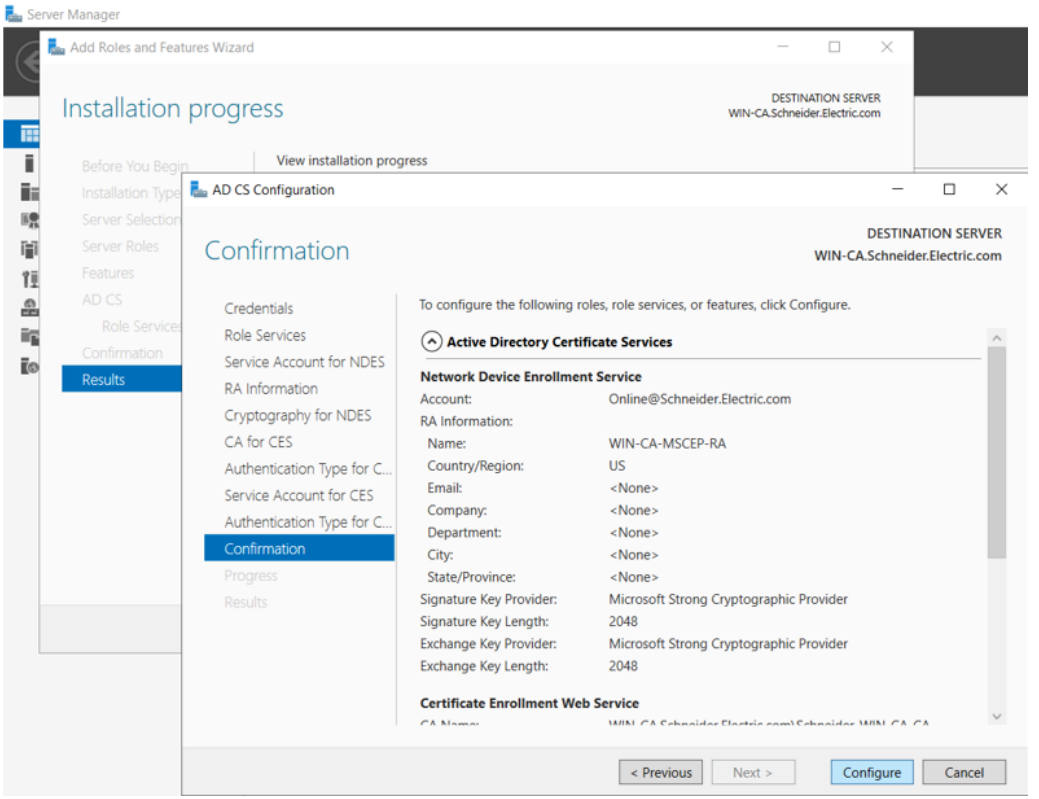
22. Sélectionnez un type d'authentification :



23. Indiquez le compte de service :



24. Confirmez les rôles, services et 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\"

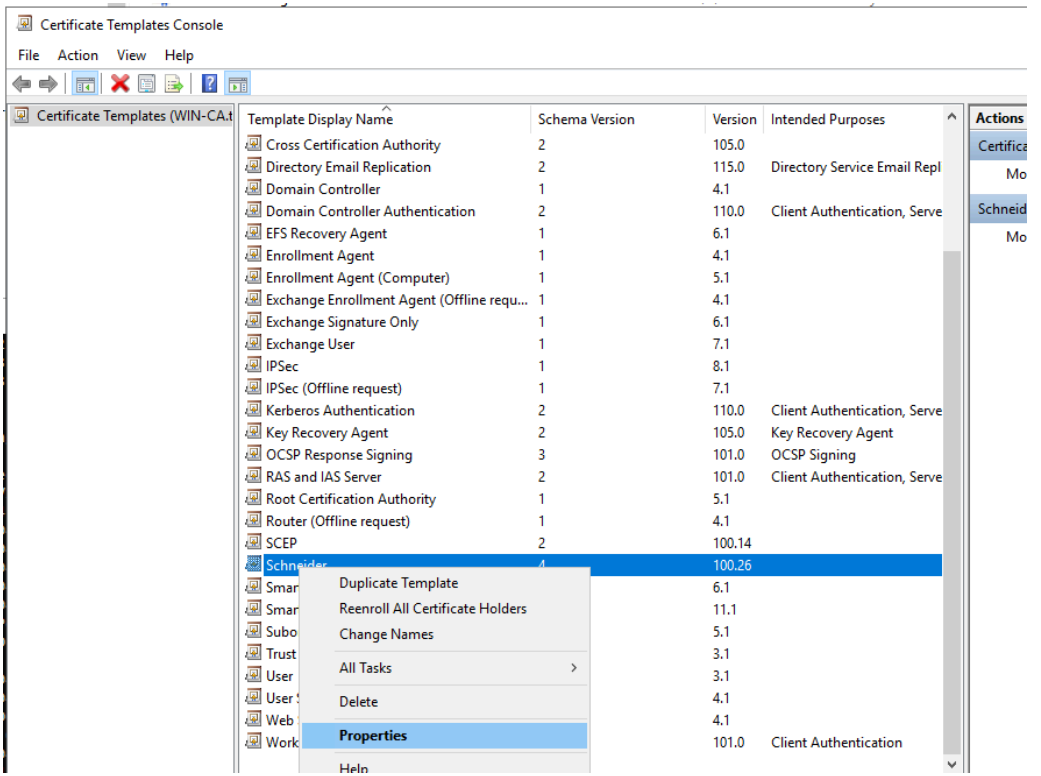
2. Démarrez Microsoft Windows PowerShell (ou un autre outil de commande) en tant qu'administrateur.
3. Accédez au dossier où vous avez placé TemplatePackage, par exemple :

   ```
   > cd C:\Users\Administrator\Desktop\TemplatePackage
   ```

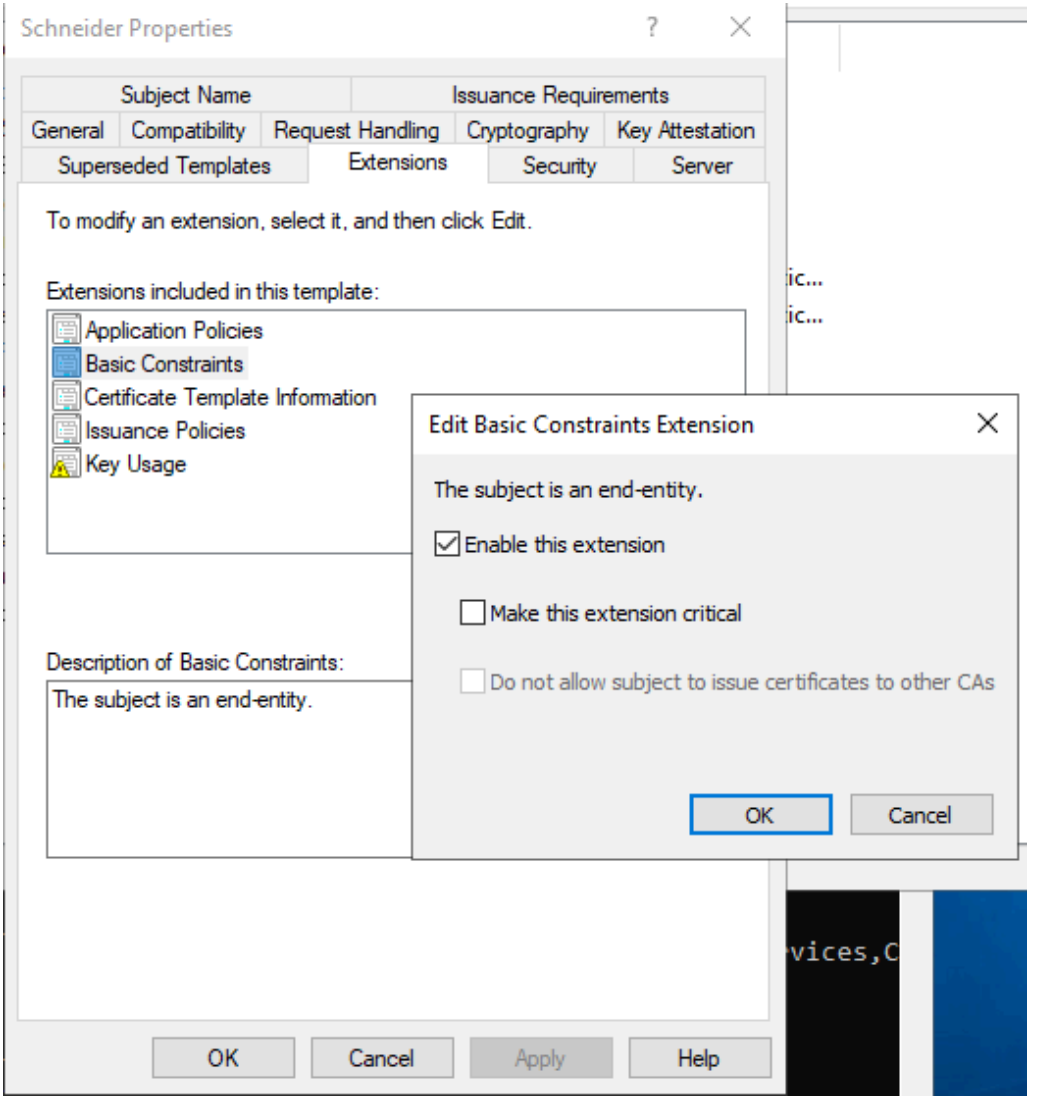
4. Exécutez le modèle dans le dossier TemplatePackage, comme suit :

   ```
   > .\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 113 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

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.

PHA83351.04