

Modicon M580

Módulo OPC UA integrado BMENUA0100

Guía de instalación y configuración

Traducción del manual original

04/2025

PHA83354.04

Información legal

La información proporcionada en este documento contiene descripciones generales, características técnicas o recomendaciones relacionadas con productos o soluciones.

Este documento no pretende sustituir a un estudio detallado o un plan de desarrollo o esquemático específico de operaciones o sitios. No debe usarse para determinar la adecuación o la fiabilidad de los productos o las soluciones para aplicaciones de usuario específicas. Es responsabilidad del usuario realizar o solicitar a un experto profesional (integrador, especificador, etc.) que realice análisis de riesgos, evaluación y pruebas adecuados y completos de los productos o las soluciones con respecto a la aplicación o el uso específicos de dichos productos o dichas soluciones.

La marca Schneider Electric y cualquier otra marca comercial de Schneider Electric SE y sus filiales mencionadas en este documento son propiedad de Schneider Electric SE o sus filiales. Todas las otras marcas pueden ser marcas comerciales de sus respectivos propietarios.

Este documento y su contenido están protegidos por las leyes de copyright aplicables, y se proporcionan exclusivamente a título informativo. Ninguna parte de este documento puede ser reproducida o transmitida de cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otro), para ningún propósito, sin el permiso previo por escrito de Schneider Electric.

Schneider Electric no otorga ningún derecho o licencia para el uso comercial del documento o su contenido, excepto por una licencia no exclusiva y personal para consultarla "tal cual".

Schneider Electric se reserva el derecho de realizar cambios o actualizaciones con respecto a o en el contenido de este documento o con respecto a o en el formato de dicho documento en cualquier momento sin previo aviso.

En la medida permitida por la ley aplicable, Schneider Electric y sus filiales no asumen ninguna responsabilidad u obligación por cualquier error u omisión en el contenido informativo de este documento o por el uso no previsto o el mal uso del contenido de dicho documento.

Tabla de contenido

Información de seguridad.....	7
Antes de empezar	8
Iniciar y probar	9
Funcionamiento y ajustes.....	10
Acerca del documento	11
Características del módulo BMENUA0100	19
Características del módulo	19
Descripción del módulo.....	21
LED del módulo.....	26
Normas y certificaciones.....	28
Normas y certificaciones	28
Normas del módulo BMENUA0100	28
Compatibilidad del firmware del módulo BMENUA0100 con EcoStruxure™	
Control Expert	29
Descripción de funciones de BMENUA0100.....	30
Ajustes de la modalidad de funcionamiento con ciberseguridad	30
Servicios OPC UA	36
Características de funcionamiento del servidor OPC UA del módulo BMENUA0100	37
Servidor OPC UA.....	38
Servicios de la pila del servidor OPC UA del módulo BMENUA0100	40
Servicios de acceso a datos de la pila del servidor OPC UA de BMENUA0100	41
Servicios de detección y seguridad de la pila del servidor OPC UA de BMENUA0100	43
Servicios de publicación y suscripción de la pila del servidor OPC UA de BMENUA0100	46
Servicios de transporte de la pila del servidor OPC UA de BMENUA0100	50
Detección de variables de controladores	50
Asignación de variables del controlador de Control Expert a variables lógicas de datos de OPC UA.....	50
Hot Standby y redundancia	55

Redundancia del servidor OPC UA	55
Arquitecturas compatibles.....	64
Configuraciones compatibles del módulo BMENUA0100	64
Red de control aislada con controladores Hot Standby M580	67
Red plana no aislada con M580 Hot Standby	69
Red plana con varios controlador independientes M580 y un solo SCADA.....	72
Red plana con varios controlador independientes M580 y SCADA redundantes.....	74
Red plana con controladores Hot Standby M580 y SCADA redundante	76
Red jerárquica con varios controladores independientes M580 conectados a la red de control y SCADA redundante.....	78
Red jerárquica con varios controladores Hot Standby M580 y conexiones SCADA redundantes	80
Puesta en marcha e instalación.....	82
Lista de comprobación para la puesta en marcha del módulo BMENUA0100.....	82
Puesta en marcha del módulo BMENUA0100	83
Instalación del módulo BMENUA0100.....	87
Configuración	89
Configuración de los ajustes de ciberseguridad de BMENUA0100	89
Introducción a las páginas web de BMENUA0100	89
Página de inicio	94
Configuración	97
Gestión de certificados	110
Control de acceso	119
Administración de la configuración	121
Configuración de BMENUA0100 en Control Expert	123
Configuración de la dirección IP	123
Configuración de las marcas de tiempo de origen.....	127
Gestión de variables con marcas de tiempo en origen	128
Configuración del servicio de hora de la red	133
Configuración del agente SNMP	136
Configuración de los ajustes del controlador M580 para las conexiones cliente/ servidor de OPC UA	140
Configuración de los ajustes de seguridad del controlador M580	140

Diagnóstico.....	141
Diagnóstico mediante indicadores LED	141
Tipo de datos derivados (DDT) del módulo BMENUA0100.....	146
Configuración de la función elemental READ_DDT	152
Configuración de la función elemental READ_NUA_DDT	157
Diagnóstico de OPC UA.....	159
Syslog	163
Diagnóstico Modbus	167
Diagnóstico SNMP	168
Página web de diagnóstico de OPC UA.....	169
Optimización del rendimiento de BMENUA0100	172
Optimización del rendimiento de BMENUA0100	172
Solución de problemas del módulo BMENUA0100	175
Actualización del firmware	179
Herramienta EcoStruxure™ Automation Device Maintenance	179
Apéndices	181
Conexiones del controlador.....	182
Conexiones del servidor OPC UA al controlador	182
Arquitecturas de reenvío de servicios (IP)	183
Arquitecturas compatibles con el reenvío de servicios (IP).....	184
Arquitecturas no compatibles con el reenvío de servicios (IP)	187
Reenvío de IP y comunicación OPC UA.....	188
Impacto del reenvío de IP en el rendimiento	188
Impacto del reenvío de IP y OPC UA en el rendimiento	189
Scripts de Windows IPsec.....	190
Scripts de configuración del cortafuegos de Windows IKE/IPsec	190
Configuración de una autoridad de certificación de Windows	193
Pasos preliminares	193
Vista general de instalación de servicios de certificados Active Directory de Microsoft Windows	194
Instalación de los Servicios de certificados de Active Directory (ADCS)	195
Aplicación de la plantilla de la autoridad de certificación	217
Glosario.....	221
Índice	222

Información de seguridad

Información importante

Lea atentamente estas instrucciones y observe el equipo para familiarizarse con el dispositivo antes de instalarlo, utilizarlo, revisarlo o realizar su mantenimiento. Los mensajes especiales que se ofrecen a continuación pueden aparecer a lo largo de la documentación o en el equipo para advertir de peligros potenciales, o para ofrecer información que aclara o simplifica los distintos procedimientos.



La inclusión de este icono en una etiqueta “Peligro” o “Advertencia” indica que existe un riesgo de descarga eléctrica, que puede provocar lesiones si no se siguen las instrucciones.



Éste es el icono de alerta de seguridad. Se utiliza para advertir de posibles riesgos de lesiones. Observe todos los mensajes que siguen a este icono para evitar posibles lesiones o incluso la muerte.

PELIGRO

PELIGRO indica una situación de peligro que, si no se evita, **provocará** lesiones graves o incluso la muerte.

ADVERTENCIA

ADVERTENCIA indica una situación de peligro que, si no se evita, **podría provocar** lesiones graves o incluso la muerte.

ATENCIÓN

ATENCIÓN indica una situación peligrosa que, si no se evita, **podría provocar** lesiones leves o moderadas.

AVISO

AVISO indica una situación potencialmente peligrosa que, si no se evita, **puede provocar** daños en el equipo.

Tenga en cuenta

La instalación, manejo, puesta en servicio y mantenimiento de equipos eléctricos deberán ser realizados sólo por personal cualificado. Schneider Electric no se hace responsable de ninguna de las consecuencias del uso de este material.

Una persona cualificada es aquella que cuenta con capacidad y conocimientos relativos a la construcción, el funcionamiento y la instalación de equipos eléctricos, y que ha sido formada en materia de seguridad para reconocer y evitar los riesgos que conllevan tales equipos.

Antes de empezar

No utilice este producto en maquinaria sin protección de punto de funcionamiento. La ausencia de protección de punto de funcionamiento en una máquina puede provocar lesiones graves al operador de dicha máquina.

 **ADVERTENCIA**

EQUIPO SIN PROTECCIÓN

- No utilice este software ni los equipos de automatización relacionados en equipos que no dispongan de protección de punto de funcionamiento.
- No introduzca las manos u otras partes del cuerpo dentro de la maquinaria mientras está en funcionamiento.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

Este equipo de automatización y el software relacionado se utilizan para controlar diversos procesos industriales. El tipo o modelo del equipo de automatización adecuado para cada uso varía en función de factores tales como las funciones de control necesarias, el grado de protección requerido, los métodos de producción, la existencia de condiciones poco habituales, las normativas gubernamentales, etc. En algunos usos, puede ser necesario más de un procesador, como en el caso de que se requiera redundancia de respaldo.

Solamente el usuario, el fabricante de la máquina o el integrador del sistema conocen las condiciones y los factores presentes durante la configuración, el funcionamiento y el mantenimiento de la máquina y, por consiguiente, pueden decidir el equipo asociado y las medidas de seguridad y los enclavamientos relacionados que se pueden utilizar de forma adecuada. Al seleccionar los equipos de automatización y control, así como el software relacionado para un uso determinado, el usuario deberá consultar los estándares y las normativas locales y nacionales aplicables. La publicación National Safety Council's

Accident Prevention Manual (que goza de un gran reconocimiento en los Estados Unidos de América) también proporciona gran cantidad de información de utilidad.

En algunas aplicaciones, como en el caso de la maquinaria de embalaje, debe proporcionarse protección adicional al operador, como la protección de punto de funcionamiento. Esta medida es necesaria si existe la posibilidad de que las manos y otras partes del cuerpo del operador puedan introducirse y quedar atrapadas en áreas o puntos peligrosos, lo que puede provocar lesiones graves. Los productos de software por sí solos no pueden proteger al operador frente a posibles lesiones. Por este motivo, el software no se puede sustituir por la protección de punto de funcionamiento ni puede realizar la función de esta.

Asegúrese de que las medidas de seguridad y los enclavamientos mecánicos/eléctricos relacionados con la protección de punto de funcionamiento se hayan instalado y estén operativos antes de que los equipos entren en funcionamiento. Todos los enclavamientos y las medidas de seguridad relacionados con la protección de punto de funcionamiento deben estar coordinados con la programación del software y los equipos de automatización relacionados.

NOTA: La coordinación de las medidas de seguridad y los enclavamientos mecánicos/eléctricos para la protección de punto de funcionamiento está fuera del ámbito de la biblioteca de bloques de funciones, la guía de usuario del sistema o de otras instalaciones mencionadas en esta documentación.

Iniciar y probar

Antes de utilizar los equipos eléctricos de control y automatización para su funcionamiento normal tras la instalación, es necesario que personal cualificado lleve a cabo una prueba de inicio del sistema para verificar que los equipos funcionan correctamente. Es importante realizar los preparativos para una comprobación de estas características y disponer de suficiente tiempo para llevar a cabo las pruebas de forma completa y correcta.

ADVERTENCIA

PELIGRO DE FUNCIONAMIENTO DEL EQUIPO

- Compruebe que se hayan seguido todos los procedimientos de instalación y configuración.
- Antes de realizar las pruebas de funcionamiento, retire de todos los dispositivos todos los bloqueos u otros medios de sujeción temporales utilizados para el transporte.
- Retire del equipo las herramientas, los medidores y el material de desecho que pueda haber.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

Realice todas las pruebas de inicio recomendadas en la documentación del equipo. Guarde la documentación del equipo para consultarla en el futuro.

Las pruebas del software deben realizarse tanto en un entorno simulado como en un entorno real.

Verifique que no existen cortocircuitos ni conexiones a tierra temporales en todo el sistema que no estén instalados según la normativa local (de conformidad con National Electrical Code de EE. UU., por ejemplo). Si fuera necesario realizar pruebas de tensión de alto potencial, siga las recomendaciones de la documentación del equipo para evitar dañar el equipo fortuitamente.

Antes de dar tensión al equipo:

- Retire del equipo las herramientas, los medidores y el material de desecho que pueda haber.
- Cierre la puerta de la carcasa del equipo.
- Retire todas las conexiones a tierra temporales de las líneas de alimentación de entrada.
- Realice todas las pruebas iniciales recomendadas por el fabricante.

Funcionamiento y ajustes

Las siguientes precauciones son de NEMA Standards Publication ICS 7.1-1995:

(En caso de divergencia o contradicción entre cualquier traducción y el original en inglés, prevalecerá el texto original en inglés).

- Aunque se ha extremado la precaución en el diseño y la fabricación del equipo o en la selección y las especificaciones de los componentes, existen riesgos que pueden aparecer si el equipo se utiliza de forma inadecuada.
- En algunas ocasiones puede desajustarse el equipo, lo que provocaría un funcionamiento incorrecto o poco seguro. Utilice siempre las instrucciones del fabricante como guía para realizar los ajustes de funcionamiento. El personal que tenga acceso a estos ajustes debe estar familiarizado con las instrucciones del fabricante del equipo y con la maquinaria utilizada para los equipos eléctricos.
- El operario solo debe tener acceso a los ajustes operativos que necesita. El acceso a los demás controles debe restringirse para evitar cambios no autorizados en las características de funcionamiento.

Acerca del documento

Alcance del documento

En este manual se describen las características y el uso del módulo de comunicación Ethernet M580 BMENUA0100 con servidor OPC UA integrado.

NOTA: Los parámetros de configuración específicos que contiene esta guía están concebidos para utilizarse solo con fines didácticos. Los parámetros necesarios para conseguir una configuración específica pueden ser distintos de los ejemplos presentados en esta guía.

Nota de validez

Este documento es válido para un sistema M580 cuando se utiliza con una versión 16.2 de EcoStruxure™ Control Expert o cualquier versión posterior compatible.

Las características de los productos descritos en este documento tienen como objetivo coincidir con las características disponibles en www.se.com. Como parte de nuestra estrategia corporativa de mejora constante, podemos revisar el contenido con el tiempo con el fin de elaborar documentos más claros y precisos. Si ve una diferencia entre las características de este documento y las características que aparecen en www.se.com, tenga en cuenta que www.se.com contiene la información más reciente.

Información relativa al producto

PELIGRO

PELIGRO DE DESCARGA ELÉCTRICA, EXPLOSIÓN O ARCO ELÉCTRICO

- Desconecte la alimentación de todos los equipos, incluidos los dispositivos conectados, antes de retirar cualquier cubierta o compuerta, o bien antes de instalar o retirar cualquier accesorio, hardware, cable o conductor salvo en las condiciones indicadas en la guía de hardware de este equipo.
- Utilice siempre un dispositivo de detección de tensión de capacidad adecuada para confirmar la ausencia de alimentación eléctrica cuando y donde se indique.
- Vuelva a montar y fijar todas las cubiertas, accesorios, elementos de hardware y cables del sistema y compruebe que haya una conexión a tierra adecuada antes de aplicar alimentación eléctrica a la unidad.
- Utilice solo la tensión especificada al operar este equipo y cualquier producto asociado.

Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.

⚠ ADVERTENCIA

PÉRDIDA DE CONTROL

- Realice un análisis de efecto o de modalidad de fallo (FMEA), o un análisis de riesgo equivalente, de su aplicación y aplique controles preventivos y de detección antes de la implementación.
- Proporcione un estado de recuperación para los eventos o las secuencias de control no deseados.
- Proporcione rutas de control separadas o redundantes donde se necesiten.
- Proporcione los parámetros adecuados, en especial respecto a límites.
- Revise las implicaciones de los retrasos en la transmisión y tome medidas para mitigarlos.
- Revise las implicaciones de las interrupciones del enlace de comunicación y tome medidas para mitigarlas.
- Proporcione rutas independientes para las funciones de control (por ejemplo, parada de emergencia, condiciones de superación de los límites y condiciones de error) de acuerdo con su evaluación de riesgos y con los códigos y normativas aplicables.
- Aplique las normas y directrices para la seguridad y la prevención de accidentes locales.
- Realice pruebas de todas las implementaciones de un sistema para verificar que funcione correctamente antes de ponerlas en servicio.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

⚠ ADVERTENCIA

FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

- Utilice solo software aprobado por Schneider Electric para este equipo.
- Actualice el programa de aplicación siempre que cambie la configuración de hardware física.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

Información general sobre ciberseguridad

En los últimos años, el creciente número de equipos y plantas de producción conectados a la red ha aumentado de la mano del potencial de las amenazas cibernéticas, como el acceso no autorizado, violaciones de datos e interrupciones operativas. Por lo tanto, es recomendable considerar todas las medidas de ciberseguridad posibles con el fin de ayudar a proteger los activos y los sistemas de dichas amenazas.

Para mantener sus productos de Schneider Electric seguros y protegidos, es conveniente que implemente las prácticas recomendadas de ciberseguridad que se indican en el documento [Cybersecurity Best Practices](#).

Schneider Electric proporciona información y asistencia adicionales:

- Suscríbase al [boletín de seguridad de Schneider Electric](#) .
- Consulta la página web de [Cybersecurity Support Portal](#) para:
 - Buscar notificaciones de seguridad.
 - Notificar vulnerabilidades e incidentes.
- Consulta la página web de [Schneider Electric Cybersecurity and Data Protection Posture](#) para:
 - Acceder a la perspectiva de ciberseguridad.
 - Obtener más información sobre la ciberseguridad en la academia de ciberseguridad.
 - Explorar los servicios de ciberseguridad de Schneider Electric.

Datos ambientales

Para obtener más información sobre el cumplimiento de los productos y el ambiente, consulte el [Environmental Data Program](#) de Schneider Electric.

Documentos relacionados

Título de la documentación	Número de referencia
Modicon M580 Autónomo, Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia	HRB62666 (inglés), HRB65318 (francés), HRB65319 (alemán), HRB65320 (italiano), HRB65321 (español), HRB65322 (chino)
Modicon M580, Guía de planificación del sistema para topologías complejas	NHA58892 (inglés), NHA58893 (francés), NHA58894 (alemán), NHA58895 (italiano), NHA58896 (español), NHA58897 (chino)

Título de la documentación	Número de referencia
Modicon M580 Hot Standby, Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia	NHA58880 (inglés), NHA58881 (francés), NHA58882 (alemán), NHA58883 (italiano), NHA58884 (español), NHA58885 (chino)
Modicon M580, M340 y X80 I/O: plataformas, normas y certificaciones	EIO0000002726 (inglés), EIO0000002727 (francés), EIO0000002728 (alemán), EIO0000002730 (italiano), EIO0000002729 (español), EIO0000002731 (chino)
M580 BMENOS0300 Conmutador de red opcional Guía de instalación y configuración	NHA89117 (ENG) NHA89119 (FRE) NHA89120 (GER) NHA89121 (ITA) NHA89122 (SPA) NHA89123 (CHS)
Modicon M580, Hardware, Manual de referencia	EIO0000001578 (inglés), EIO0000001579 (francés), EIO0000001580 (alemán), EIO0000001582 (italiano), EIO0000001581 (español), EIO0000001583 (chino)
Modicon M580, Módulos RIO, Guía de instalación y configuración	EIO0000001584 (inglés), EIO0000001585 (francés), EIO0000001586 (alemán), EIO0000001587 (italiano), EIO0000001588 (español), EIO0000001589 (chino)
Modicon M580, Cambio de configuración sobre la marcha, Manual del usuario	EIO0000001590 (inglés), EIO0000001591 (francés), EIO0000001592 (alemán), EIO0000001594 (italiano), EIO0000001593 (español), EIO0000001595 (chino)
Modicon X80, Módulos de entradas/salidas binarias, Manual de usuario	35012474 (inglés), 35012475 (alemán), 35012476 (francés), 35012477 (español), 35012478 (italiano), 35012479 (chino)
Modicon X80, Módulo de conteo BMXEHC0200, Manual del usuario	35013355 (inglés), 35013356 (alemán), 35013357 (francés), 35013358 (español), 35013359 (italiano), 35013360 (chino)
Manual de usuario de medidas y principios básicos de toma de tierra y compatibilidad electromagnética de sistemas PLC	33002439 (ENG) 33002440 (FRE) 33002441 (GER) 33002442 (SPA) 33003702 (ITA) 33003703 (CHS)
EcoStruxure™ Control Expert, Lenguajes y estructura del programa, Manual de referencia	35006144 (inglés), 35006145 (francés), 35006146 (alemán), 35013361 (italiano), 35006147 (español), 35013362 (chino)
EcoStruxure™ Control Expert, Palabras y bits de sistema, Manual de referencia	EIO0000002135 (inglés), EIO0000002136 (francés), EIO0000002137 (alemán), EIO0000002138 (italiano), EIO0000002139 (español), EIO0000002140 (chino)
EcoStruxure™ Control Expert, Modalidades de funcionamiento	33003101 (inglés), 33003102 (francés), 33003103 (alemán), 33003104 (español), 33003696 (italiano), 33003697 (chino)
EcoStruxure™ Control Expert, Manual de instalación	35014792 (inglés), 35014793 (francés), 35014794 (alemán), 35014795 (español), 35014796 (italiano), 35012191 (chino)

Título de la documentación	Número de referencia
Manual de usuario de Web Designer para FactoryCast	35016149 (inglés), 35016150 (francés), 35016151 (alemán), 35016152 (italiano), 35016153 (español), 35016154 (chino)
Ciberseguridad - Plataforma de controladores Modicon - Manual de referencia	EIO0000001999 (ENG) EIO0000002001 (FRE) EIO0000002000 (GER) EIO0000002003 (SPA) EIO0000002002 (ITA) EIO0000002004 (CHS)

Para consultar documentos en línea, visite el centro de descargas de Schneider Electric (www.se.com/ww/en/download/).

Normas y términos utilizados

Los términos técnicos, símbolos y las descripciones correspondientes de esta información o que aparecen en la parte interior o exterior de los propios productos se derivan, por lo general, de los términos y las definiciones de estándares internacionales.

En el área de sistemas de seguridad funcional, unidades y automatización general, se incluyen, pero sin limitarse a ellos, términos como *seguridad*, *función de seguridad*, *estado de seguridad*, *fallo*, *reinicio tras fallo*, *avería*, *funcionamiento incorrecto*, *error*, *mensaje de error*, *peligroso*, etc.

Entre estas normas se incluyen:

Norma	Descripción
IEC 61131-2:2007	Controladores programables, parte 2: Requisitos y ensayos de los equipos.
ISO 13849-1:2023	Seguridad de la maquinaria: Componentes de los sistemas de control relacionados con la seguridad. Principios generales del diseño.
EN 61496-1:2020	Seguridad de la maquinaria: Equipos de protección electrosensibles. Parte 1: Pruebas y requisitos generales.
ISO 12100:2010	Seguridad de las máquinas. Principios generales del diseño. Evaluación del riesgo y reducción del riesgo
EN 60204-1:2006	Seguridad de la maquinaria - Equipo eléctrico de las máquinas - Parte 1: Requisitos generales
ISO 14119:2013	Seguridad de la maquinaria. Dispositivos de bloqueo asociados con protecciones: principios de diseño y selección
ISO 13850:2015	Seguridad de la maquinaria. Parada de emergencia: principios de diseño

Norma	Descripción
IEC 62061:2021	Seguridad de la maquinaria. Seguridad funcional de sistemas de control eléctricos, electrónicos y electrónicos programables relacionados con la seguridad
IEC 61508-1:2010	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad: Requisitos generales.
IEC 61508-2:2010	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad: Requisitos para los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad.
IEC 61508-3:2010	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad: Requisitos de software.
IEC 61784-3:2021	Redes de comunicaciones industriales - Perfiles - Parte 3: Buses de campo de seguridad funcionales - Reglas generales y definiciones de perfiles.
2006/42/EC	Directiva de maquinaria
2014/30/EU	Directiva de compatibilidad electromagnética
2014/35/EU	Directiva de baja tensión

Además, los términos utilizados en este documento se pueden usar de manera tangencial porque se obtienen de otros estándares como:

Norma	Descripción
Serie IEC 60034	Máquinas eléctricas giratorias
Serie IEC 61800	Sistemas de variadores eléctricos de velocidad ajustable
Serie IEC 61158	Comunicación digital de datos para la medición y control: bus de campo para su uso en sistemas de control industriales

Por último, el término *zona de funcionamiento* se puede utilizar junto con la descripción de peligros específicos, y se define como tal para una *zona de peligro* o *zona peligrosa* en la *Directiva de maquinaria (2006/42/EC)* y *ISO 12100:2010*.

NOTA: Los estándares mencionados anteriormente podrían o no aplicarse a los productos específicos citados en la presente documentación. Para obtener más información en relación con los diferentes estándares aplicables a los productos descritos en este documento, consulte las tablas de características de las referencias de dichos productos.

Información sobre terminología no inclusiva o insensible

Como empresa responsable e inclusiva, Schneider Electric actualiza constantemente sus comunicaciones y productos que contienen terminología no inclusiva o insensible. Sin embargo, a pesar de estos esfuerzos, nuestro contenido aún puede contener términos que algunos clientes consideren inapropiados.

Marcas comerciales

Windows es una marca comercial registrada de Microsoft Corporation.

Características del módulo BMENUA0100

Introducción

En este capítulo se describe el módulo de comunicaciones Ethernet BMENUA0100 con servidor OPC UA integrado.

Características del módulo

Introducción

El módulo de servidor OPC UA BMENUA0100 Modicon proporciona capacidades OPC UA de alto rendimiento a los sistemas de controlador M580 Modicon.

OPC UA es una plataforma de comunicaciones abierta y fiable para las comunicaciones industriales, diseñada para ser flexible y escalable en entornos que van desde sensores IoT de recursos limitados in situ hasta servidores empresariales alojados en el centro de datos o la nube. Además de conectar y mover datos, OPC UA define un completo modelo de información para publicar y gestionar metainformación y contexto del sistema con el objetivo de simplificar la ingeniería de automatización y la integración de sistemas.

Al poner en práctica un estándar de comunicaciones para las operaciones industriales modernas y conectadas, OPC UA ofrece una conexión común entre productos conectados in situ, controladores, y aplicaciones y análisis empresariales. Está diseñado para ser compatible con infraestructuras de TI y seguridad, como cortafuegos, VPN y proxies. OPC UA se escala en lo referente a requisitos funcionales y ancho de banda.

Características

El módulo BMENUA0100 incluye un servidor OPC UA y un conmutador Ethernet integrado. Se incluye en el **Catálogo de hardware** de Control Expert, en el grupo del módulo **Comunicación**.

BMENUA0100 aporta las siguientes características a la plataforma M580 Modicon:

General:

- Acceso directo y optimizado al diccionario de datos de Control Expert para una asignación entre variables de Control Expert y variables OPC UA, página 50.

- Compatibilidad con configuraciones Hot Standby mediante redundancia, página 55 OPC UA.
- Compatibilidad con sistemas de seguridad M580 como un módulo sin interferencia de tipo 1, según la definición de TÜV Rheinland.
- Comunicaciones Ethernet de la placa de conexiones perfectas.
- Cliente DHCP/FDR para descargar los ajustes de configuración (sin ciberseguridad) almacenados.
- Sincronización horaria NTP de servidor, página 133 y cliente.
- Varios métodos de diagnóstico, entre los que se incluyen indicadores LED, página 141, DDT, página 146, variables y elementos de datos OPC-UA, página 159, Syslog, página 163, Modbus, página 167, SNMP, página 168 y páginas web seguras, página 169.
- Actualización del firmware mediante Herramienta EcoStruxure™ Automation Device Maintenance, página 179.
- Comprobación de la integridad del firmware.
- Almacenamiento protegido del hardware.

Ciberseguridad:

- Comunicaciones seguras mediante HTTPS, OPC UA (opcional) e IPsec (opcional).
- Seguridad, página 97 OPC UA a nivel de módulo configurable mediante HTTPS.
- La capacidad de controlar el flujo de comunicación entrante y saliente habilitando y deshabilitando servicios de comunicación, página 99.
- IPsec, página 106 basado en una clave precompartida (PSK) para proteger servicios como SNMPv1, Modbus/TCP, Syslog y NTPv4.

NOTA: El BMENUA0100 admite IPsec en la modalidad principal. Un canal IPsec pueden abrirlo el servidor BMENUA0100 o un cliente OPC UA remoto. En un cliente PC, IPsec es compatible y está validado en sistemas Windows 7 y 10 y Windows Server 2016.

Gestión de la autenticación:

- Control de acceso basado en rol (RBAC) y autenticación del usuario, página 119 para clientes HTTPS y OPC UA.
- Certificados, página 110 para entidades de aplicaciones cliente OPC UA.

Entre las características del módulo de comunicación M580 se incluyen:

- Puerto Ethernet de la placa de conexiones para la comunicación Ethernet mediante el bastidor Ethernet principal local.
- Puerto X Bus de la placa de conexiones para 24 V CC y direcciones del bastidor.
- Sincronización horaria NTP de servidor, página 133 y cliente.

Descripción del módulo

Introducción

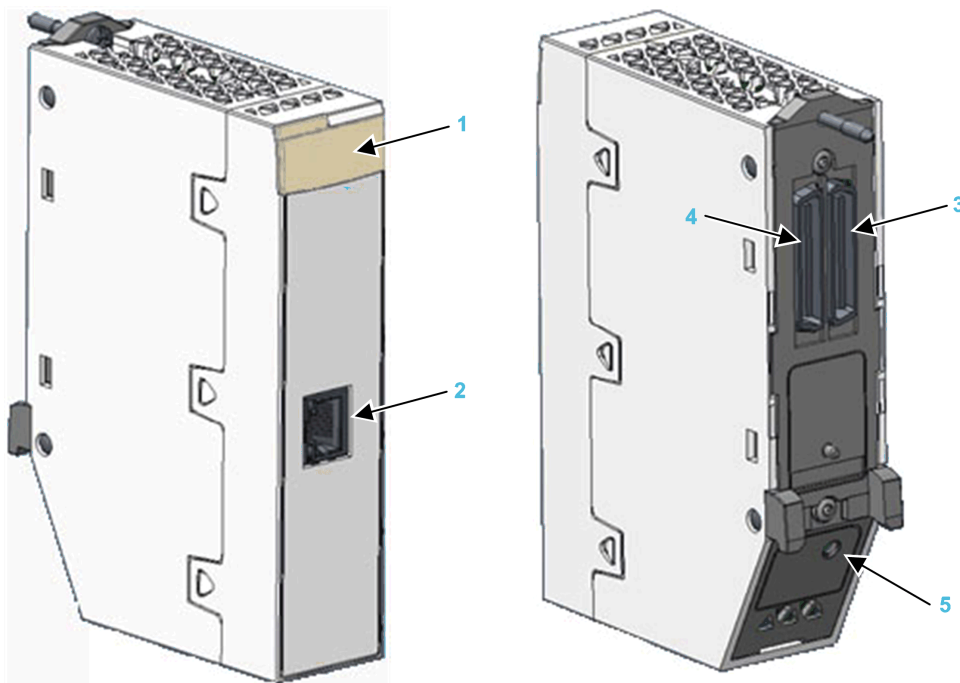
Schneider Electric ofrece dos módulos de comunicación Ethernet con un servidor OPC UA integrado para la comunicación con clientes OPC UA, incluido SCADA:

- Módulo BMENUA0100 para entornos estándar.
- Módulo BMENUA0100H para entornos difíciles.

El módulo solo se puede instalar en un slot Ethernet, en un bastidor Ethernet local principal. Consulte el tema *Configuraciones compatibles del módulo BMENUA0100*, página 64 si desea una descripción de las colocaciones compatibles del módulo, incluida la cantidad máxima de módulos BMENUA0100 que se pueden colocar en un bastidor.

Descripción física

En esta figura se muestran las funciones externas del módulo BMENUA0100:



1 Matriz de indicadores LED

2 Puerto de control con conexión Ethernet e indicadores LED de actividad

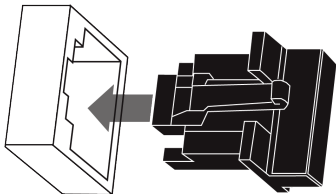
3 Puertos Ethernet de la placa de conexiones

4 Puerto X Bus de la placa de conexiones

5 Conmutador rotativo de modalidad de funcionamiento de ciberseguridad

Consulte el tema [Diagnóstico de los indicadores LED](#), página 141 si desea información sobre cómo leer los LED del módulo.

Si el puerto de control Ethernet no está habilitado, use el tapón incluido con cada módulo para contribuir a evitar que entre suciedad en el puerto de control:



Puertos externos

El módulo BMENUA0100 incluye los siguientes puertos externos:

Puerto	Descripción
Puerto de control	<p>El puerto de control es el único puerto situado en la parte delantera del módulo BMENUA0100. Sus características son, entre otras:</p> <ul style="list-style-type: none">• Cuando el puerto de control está habilitado, pasa a ser la interfaz exclusiva para las comunicaciones OPC UA, excepto si se ha configurado IPv6.<ul style="list-style-type: none">◦ Cuando se configura IPv6, se pueden utilizar tanto el puerto de la placa de conexiones como el puerto de control para las comunicaciones OPC UA.◦ Si no se ha configurado IPv6, puede conectar clientes OPC UA ubicados en la red de la placa de conexiones a través del puerto de control del módulo BMENUA0100 siempre que se haya definido o declarado una ruta en el ordenador que aloja el cliente OPC UA.• Velocidad de funcionamiento de hasta 1 Gb/s. Cuando funciona a la velocidad de:<ul style="list-style-type: none">◦ 1 Gb/s, use solo cables de cuatro pares trenzados blindados de cobre CAT6.◦ 10/100 Mb/s, use cables de cuatro pares trenzados blindados de cobre CAT5e o CAT6.• Doble pila IP compatible con direcciones IP IPv4 (32 bits) e IPv6 (128 bits):<ul style="list-style-type: none">◦ IPv4 e IPv6 están configurados para el módulo.◦ La configuración de IPv6 puede ser fija o dinámica (mediante SLAAC).◦ Si no hay ninguna dirección IP configurada, se asigna automáticamente el ajuste predeterminado, página 123 de IPv4 en función de la dirección MAC del módulo.• Acceso seguro al servidor OPC UA mediante protocolos IPv4 e IPv6.• Protocolo seguro HTTPS (mediante IPv4) para actualización de firmware, página 179 y configuración de ciberseguridad, página 89.• Compatibilidad con protocolo seguro NTPv4.• Seguridad facilitada por IPsec para servicios no seguros, como SNMPv1, Modbus TCP y Syslog.
Puerto Ethernet de la placa de conexiones	<p>El puerto de la placa de conexiones BMENUA0100 Ethernet es compatible con el protocolo IPv4 (32 bits). Cuando el puerto de control está deshabilitado, el puerto de la placa de conexiones puede admitir comunicaciones OPC UA. El puerto de la placa de conexiones presenta las siguientes características:</p> <ul style="list-style-type: none">• Velocidad de funcionamiento de hasta 100 Mb/s.• Conectividad Ethernet Modbus TCP IPv4 con el controlador:<ul style="list-style-type: none">◦ El puerto Ethernet de la placa de conexiones es el puerto exclusivo para el diagnóstico Modbus.• Puerto exclusivo para configuración sin ciberseguridad (IP, NTPv4, SNMPv1), mediante:<ul style="list-style-type: none">◦ Control Expert v14.1 y cualquier versión posterior compatible◦ Servidor FDR/DHCP• Si el puerto de control está deshabilitado, el puerto Ethernet de la placa de conexiones ofrece acceso seguro al servidor OPC UA a través del protocolo IPv4, y es compatible con los siguientes servicios:<ul style="list-style-type: none">◦ Protocolo seguro HTTPS para actualización de firmware, página 179 y configuración de ciberseguridad, página 89.◦ NTPv4, SNMPv1/v3 y Syslog.
Puerto X Bus de la placa de conexiones	<p>El módulo BMENUA0100 usa la comunicación X Bus de la placa de conexiones para:</p> <ul style="list-style-type: none">• Recibir 24 V CC de alimentación.• Detectar la dirección del bastidor y el slot del módulo BMENUA0100.

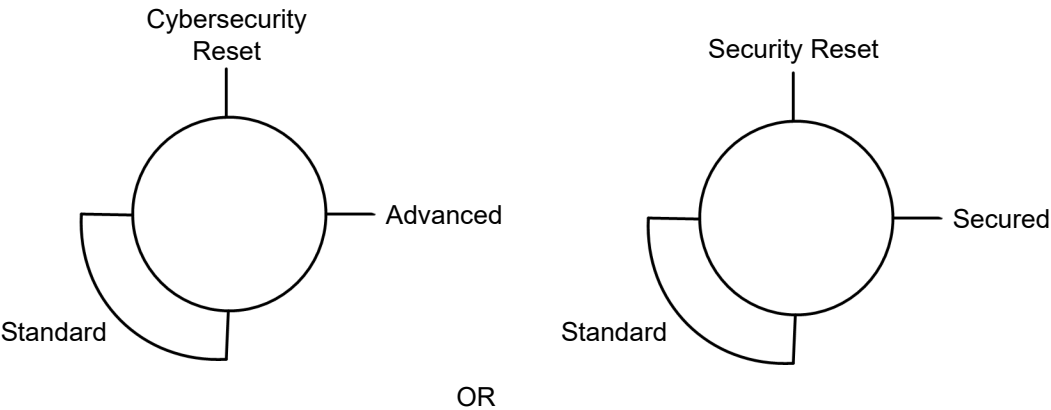
Puerto	Descripción
	NOTA: No se realiza ninguna otra comunicación a través del puerto X Bus de la placa de conexiones del módulo BMENUA0100.

Conmutador rotativo

Hay un conmutador rotativo de cuatro posiciones en la parte posterior del módulo. Ajuste este conmutador rotativo para configurar una modalidad para el controlador.

NOTA: Para su comodidad, se incluye un destornillador de plástico; utilícelo, o un equivalente, para cambiar la posición del conmutador rotativo. Evite utilizar destornilladores metálicos

En función de la versión del módulo, las posiciones del conmutador rotativo son:



Los ajustes son:

- Modo Advanced (RL 6 y posterior) o Secured (anterior a RL 6), página 32
- Modalidad Standard, página 32
- Cybersecurity Reset (RL 6 y posterior) o Security Reset (anterior a RL 6), página 33

NOTA:

- El conmutador rotativo no es accesible cuando el módulo está colocado en el bastidor.
- En un sistema Hot Standby, verifique que las posiciones del conmutador rotativo del módulo BMENUA0100 (en el bastidor primario y en el bastidor principal local en standby) sean las mismas. El sistema no realiza esta comprobación automáticamente.

Consulte la descripción de las modalidades de funcionamiento de ciberseguridad, página 30 si desea información sobre cada ajuste de la posición del conmutador rotativo.

LED del módulo

Pantalla de indicadores LED

El panel de visualización con 7 indicadores LED está ubicado en la parte frontal del módulo BMENUA0100:



Los LED muestran información sobre el módulo, como se indica a continuación:

Indicador LED	Describe el estado del módulo
RUN	Condición de funcionamiento.
ERR	Errores detectados.
UACNX	Conexiones OPC UA.
BS	Puerto de la placa de conexiones.
NS	Puerto de control.
SEC	Condición de ciberseguridad.
BUSY	Estado del diccionario de datos

Consulte el tema Diagnóstico de los indicadores LED, página 141 si desea información sobre cómo usar estos LED para diagnosticar el estado del módulo BMENUA0100.

LED del puerto de control

El puerto de control, en la parte frontal del módulo, presenta dos indicadores LED que describen el estado de la conexión Ethernet a través del puerto:



- El LED ACT indica la presencia de actividad Ethernet en el puerto.
- El LED LNK indica la existencia de una conexión Ethernet y la velocidad de la conexión.

Consulte el tema [Diagnóstico de los indicadores LED](#), página 145 si desea información sobre cómo usar los LED del puerto de control para diagnosticar el estado del puerto de control del módulo BMENUA0100.

Normas y certificaciones

Descripción general

En este capítulo se describen las normas y las certificaciones que se aplican al módulo de comunicaciones Ethernet BMENUA0100 con servidor OPC UA integrado.

Normas y certificaciones

Descarga

Haga clic en el enlace correspondiente al idioma que prefiera para descargar las normas y las certificaciones (formato PDF) aplicables a los módulos de esta línea de productos:

Título	Idiomas
Modicon M580, M340 y X80 I/O: plataformas, normas y certificaciones	<ul style="list-style-type: none">• Inglés: EIO00000002726• Francés: EIO00000002727• Alemán: EIO00000002728• Italiano: EIO00000002730• Español: EIO00000002729• Chino: EIO00000002731

Normas del módulo BMENUA0100

Requisitos oficiales

El módulo de comunicación BMENUA0100 OPC UA integrado Ethernet cumple con la siguiente norma oficial:

Marca	Requisito
	OPC UA V1.03: protocolo de comunicación entre máquinas OPC Unified Architecture.

Compatibilidad del firmware del módulo BMENUA0100 con EcoStruxure™ Control Expert

Compatibilidad

Las aplicaciones creadas con el software EcoStruxure™ Control Expert son compatibles con el firmware del módulo BMENUA0100 de la siguiente manera:

Versión del firmware del módulo BMENUA0100	Versión del software EcoStruxure™ Control Expert	
	14.0	15.0 o posterior
1,01	Totalmente compatible	El software solo admite las funciones heredadas de la versión del firmware 1.01 ^{1, 2, 3}
1,10	Totalmente compatible	Totalmente compatible
<div>1. Si un módulo BMENUA0100 con la versión del firmware 1.01 recibe una aplicación generada con EcoStruxure™ Control ExpertV15 y:</div> <ul style="list-style-type: none">• Velocidad de muestreo rápida está Activado (en la ficha IPConfig, página 124), esta configuración no se implementará.• IPv4 está desactivado para el puerto de control, el puerto de control del módulo se configura con la dirección IPv4 que aparece atenuada en la ficha IPConfig del módulo.<div>NOTA: La dirección IPv4 atenuada puede ser la dirección IPv4 que el usuario introdujo más recientemente, o bien la dirección IPv4 que el software EcoStruxure™ Control Expert introdujo automáticamente (172.16.12.1) si no se introdujo previamente ninguna dirección IPv4.</div>• NTP, página 135 se ha configurado con una dirección IPv6, las páginas web del módulo indicarán erróneamente que NTP está operativo cuando el servicio NTP en realidad no está funcionando. <div>2. Si se han configurado dos módulos BMENUA0100 con la versión 1.01 del firmware en un bastidor Hot Standby con EcoStruxure™ Control ExpertV15, las limitaciones descritas en los elementos anteriores también se aplican a estos módulos.</div> <div>3. Si SNMP está habilitado en Control Expert, incluya la dirección IPv4 del administrador SNMP en la ficha SNMP del módulo, página 137 BMENUA0100 para que el administrador SNMP pueda acceder a SNMP MIB.</div>		

NOTA: Las páginas web que se muestran para el módulo BMENUA0100 dependen de la versión del firmware del módulo (por ejemplo, la versión 1.01, 1.10 o 2.01).

Descripción de funciones de BMENUA0100

Introducción

En este capítulo se describen las funciones compatibles del módulo de comunicaciones Ethernet BMENUA0100 con servidor OPC UA integrado.

Ajustes de la modalidad de funcionamiento con ciberseguridad

Introducción

El módulo BMENUA0100 puede configurarse para funcionar en modalidad Advanced (o Secured) o Standard. El conmutador rotativo de 4 posiciones situado en la parte posterior del módulo determina la modalidad de funcionamiento.

Las tres posiciones del conmutador rotativo son:

- Modalidad Advanced (o Secured)
- Modalidad Standard
- Cybersecurity (o Security) Reset

NOTA:

- El valor predeterminado del módulo, es decir, la configuración lista para utilizarse, es la modalidad Advanced (o Secured).
- Para ver la posición del conmutador rotativo, vaya a la [página de inicio](#), [página 94](#) de las páginas web del módulo.

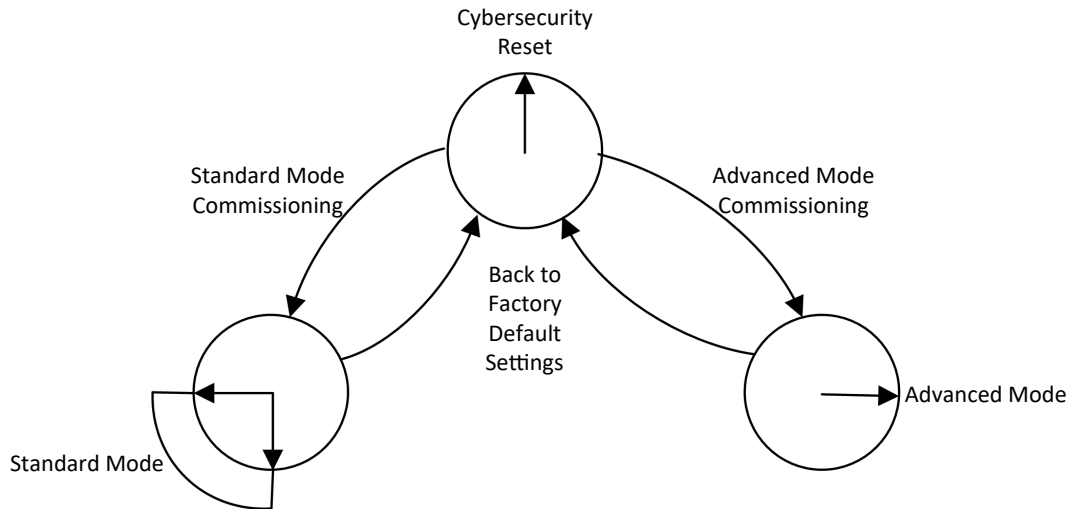
Como no se puede acceder al conmutador rotativo cuando el módulo se encuentra en el bastidor, solo se podrá cambiar la posición del conmutador cuando el módulo esté apagado y se haya extraído del bastidor. Después de seleccionar una nueva posición del conmutador, ya es posible volver a insertar el módulo en el bastidor y activar la alimentación.

NOTA: Utilice únicamente el [destornillador pequeño de plástico que se incluye con el módulo](#), [página 25](#) para cambiar la posición del conmutador y configurar una modalidad de funcionamiento de ciberseguridad.

Cambio de la modalidad de funcionamiento

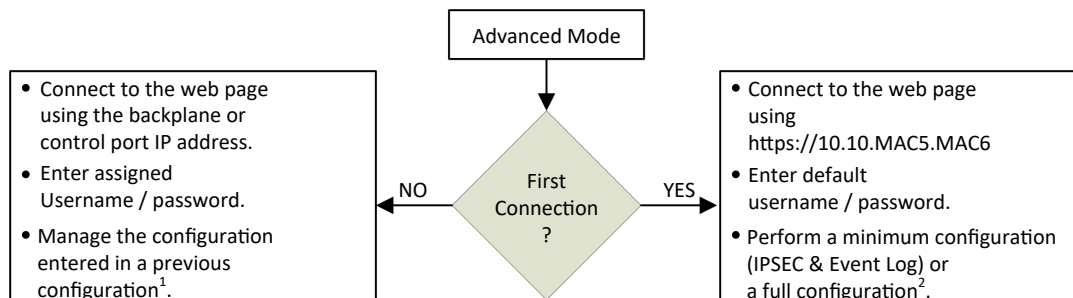
Cada vez que cambie la modalidad de funcionamiento de ciberseguridad de Advanced (o Secured) a Standard, o de Standard a Advanced (o Secured), realice una *operación Cybersecurity (o Security) Reset*, página 86 antes de configurar la nueva modalidad.

La posición del conmutador rotativo determina el estado de funcionamiento del módulo, de la manera siguiente:



Se puede poner en marcha un nuevo módulo (predeterminado de fábrica) o un módulo para el que se haya realizado un **Cybersecurity (o Security) Reset** las operaciones de modalidad Standard, página 85 o modalidad Advanced (o Secured), página 83.

El proceso de configuración del módulo para las operaciones de la modalidad Advanced (o Secured) varía en función de si se conecta por primera vez a los ajustes de configuración del módulo después de realizar un Cybersecurity (o Security) Reset:



1 Para obtener información sobre la gestión de la configuración, consulte el capítulo de configuración, página 89.

2 Para obtener información sobre cómo realizar una configuración con la primera conexión, consulte el tema Puesta en marcha en la modalidad Advanced (o Secured), página 83.

Modalidad Advanced (o Secured)

Cuando funcione en la modalidad Advanced (o Secured), el módulo no participará en las comunicaciones de procesos, ya sea a través del puerto de control o el puerto de la placa de conexiones, hasta que se hayan configurado los ajustes de ciberseguridad válidos. Una vez configurada la modalidad Advanced (o Secured), puede configurar los ajustes de ciberseguridad mediante las páginas web del módulo, página 89, a las que se accede a través del protocolo HTTPS y de los puertos de la placa de conexiones o de control. En la modalidad Advanced (o Secured), el módulo admite el nivel de ciberseguridad especificado en la configuración de ciberseguridad. Los ajustes de dirección IP, cliente NTP y agente SNMP, página 123 solo pueden configurarse mediante el software de configuración Control Expert una vez configurados los ajustes de ciberseguridad.

Modalidad Standard

Al funcionar en la modalidad Standard, las comunicaciones del módulo pueden comenzar sin necesidad de configurar la ciberseguridad. Los ajustes de ciberseguridad no son necesarios, por lo que no se pueden configurar. Solo se pueden configurar la dirección IP y otros ajustes disponibles en Control Expert.

Cybersecurity (o Security) Reset

El comando **Cybersecurity (o Security) Reset** permite restaurar los ajustes de configuración predeterminados de fábrica. Elimina cualquier configuración de ciberseguridad existente, listas blancas, certificados y ajustes de control de acceso basado en roles. Para completar el Cybersecurity (o Security) Reset, apague y encienda el módulo BMENUA0100 o extraiga físicamente el módulo del bastidor (con lo que se apagará) y, a continuación, vuelva a insertar el módulo en el bastidor (con lo que volverá a conectarse la alimentación). Mientras el proceso de restauración de los ajustes predeterminados de fábrica está en curso, el indicador LED **RUN** parpadea en verde. Una vez finalizado el proceso, el indicador LED **RUN** cambia a color verde fijo y los servicios se deshabilitan.

Este ajuste se puede realizar mediante el conmutador rotativo o las páginas web (cuando se funciona en la modalidad Advanced [o Secured]):

- Si se configura a través del conmutador rotativo: el módulo deja de funcionar hasta que se retira del bastidor, el conmutador rotativo se restablece en la posición Advanced (o Secured) o Standard y el módulo se vuelve a colocar en el bastidor. Será necesario aplicar las configuraciones necesarias.
- Si se configura a través de las páginas web: tras apagar y volver a encender el módulo (o intercambiarlo bajo tensión) en modalidad Standard o Advanced (o Secured). Es necesario configurar los ajustes de ciberseguridad y dirección IP.

NOTA: Después de un Cybersecurity (o Security) Reset del módulo BMENUA0100, se aplican las siguientes condiciones al módulo:

- No se conserva ningún certificado de dispositivo.
- Todos los servicios están deshabilitados excepto HTTPS, que se utiliza para crear la configuración de ciberseguridad a través del puerto de control.
- Se aplican los ajustes predeterminados de fábrica, incluidos:
 - Ajustes predeterminados, página 33 de nombre de usuario/contraseña.
 - Ajuste predeterminado de dirección IP de 10.10.MAC5.MAC6, página 123.

NOTA: Cuando los dos últimos octetos de la dirección MAC (*MAC5.MAC6*) corresponden a 0.0 en la dirección predeterminada, establezca una conexión de cables punto a punto entre el equipo y el controlador, módulo de comunicación u otro módulo.

Combinación predeterminada de nombre de usuario y contraseña

La combinación predeterminada de nombre de usuario y contraseña depende del ajuste de la modalidad de funcionamiento de ciberseguridad:

- Modalidad Advanced (o Secured): admin/password
- Modalidad Standard: installer / Inst@ller1

NOTA: Se le pedirá que modifique la contraseña la primera vez que la utilice en el modo Advanced (o Secured). Verifique las leyes y regulaciones locales para saber si esto es un requisito.

Funciones admitidas por las modalidades de funcionamiento Advanced (o Secured) y Standard

El módulo BMENUA0100 admite las siguientes funciones en las modalidades Advanced (o Secured) y Standard:

Modalidad	Modalidad Standard			Modalidad Advanced (o Secured)		
Puerto de control	Deshabilitar	Habilitar		Deshabilitar	Enable	
Puerto Ethernet	Placa de conexiones	Placa de conexio-nes	Puerto de control	Placa de conexiones	Placa de conexio-nes	Puerto de control
Comunicación OPC UA	Sí	No	Sí	Sí	No	Sí
Ajustes de seguridad ⁽⁴⁾	Ninguno	–	Ninguno	Ninguno, Firmar, Firmar y cifrar (valor predeterminado)	–	Ninguno, Firmar, Firmar y cifrar (valor predeterminado)
Autenticación de usuario	Sin autenticación (anónimo)	–	Sin autenticación (anónimo)	Operador, Ingeniero, Sin autenticación (anónimo)	–	Operador, Ingeniero, Sin autenticación (anónimo)
SNMP V1	Sí ^(1,2)	Sí ^(1,2)	Sí ^(1,2)	Sí ⁽¹⁾	Sí ⁽¹⁾	Sí ⁽¹⁾
SNMP V3	Sí ^(1,2)	Sí ^(1,2)	Sí ^(1,2)	Sí ⁽¹⁾	Sí ⁽¹⁾	Sí ⁽¹⁾
NTP V4	Solo cliente ⁽¹⁾	Cliente ⁽¹⁾ , servidor	Sí, solo cliente ⁽¹⁾	Solo cliente ⁽¹⁾	Cliente ⁽¹⁾ , servidor	Sí, solo cliente ⁽¹⁾
Registro de eventos	No	No	No	Sí	Sí	Sí
IPsec	No	No	No	No	No	Sí para Modbus, SNMP V1/V3, NTP V4 ⁽³⁾ y Syslog (IPsec habilitado de forma predeterminada)
Cambio de configuración de CS por web (HTTPS)	No	No	No	Sí	Sí	Sí

Modalidad		Modalidad Standard			Modalidad Advanced (o Secured)		
Puerto de control		Deshabilitar	Habilitar		Deshabilitar	Enable	
Puerto Ethernet		Placa de conexiones	Placa de conexiones	Puerto de control	Placa de conexiones	Placa de conexiones	Puerto de control
	Autenticación de usuario	—	—	—	Administrador	Administrador	Administrador
	Habilitación/deshabilitación del servidor de comunicaciones de servicios de red	Si se admite, siempre habilitado (consulte más arriba)	Si se admite, siempre habilitado (consulte más arriba)	Si se admite, siempre habilitado (consulte más arriba)	Todos los servicios son configurables (deshabilitado de forma predeterminada)	Todos los servicios son configurables (deshabilitado de forma predeterminada)	Todos los servicios son configurables (deshabilitado de forma predeterminada)
Diagnóstico web (solo páginas de inicio y diagnóstico)		Sí	Sí	Sí	Sí	Sí	Sí
	Autenticación de usuario	Instalador (credenciales predeterminadas)	Instalador (credenciales predeterminadas)	Instalador (credenciales predeterminadas)	Administrador, Operador, Ingeniero, Instalador	Administrador, Operador, Ingeniero, Instalador	Administrador, Operador, Ingeniero, Instalador
	Actualización del firmware (HTTPS)	Sí	Sí	Sí	Sí	Sí	Sí, si se ha habilitado HTTPS
	Autenticación de usuario	Instalador (credenciales predeterminadas)	Instalador (credenciales predeterminadas)	Instalador (credenciales predeterminadas)	Instalador	Instalador	Instalador
	Filtrado: Reenviar todo	—	—	(siempre habilitado)	—	—	Reenviar todos los protocolos
Filtrado: Protocolo de reenvío configurado		—	—	—	—	—	Reenvío de protocolos configurados

Modalidad	Modalidad Standard			Modalidad Advanced (o Secured)		
Puerto de control	Deshabilitar	Habilitar		Deshabilitar	Enable	
Puerto Ethernet	Placa de conexiones	Placa de conexiones	Puerto de control	Placa de conexiones	Placa de conexiones	Puerto de control
Filtrado: Flujos de datos de Control Expert a la red de dispositivos (incluido el controlador) (FTP, EIP, explícito, Modbus, Ping) solo a través de IPv4 ⁵	—	—	Reenvío de los flujos de datos de Control Expert de la red de control a la red de dispositivos (siempre habilitado)	—	—	Reenvío de los flujos de datos de Control Expert de la red de control a la red de dispositivos (deshabilitado de forma predeterminada)
<div><div>1. Se puede configurar con Control Expert.</div><div>2. En la modalidad estándar, la versión de SNMP del módulo BMENUA0100 se define en Control Expert. Si SNMP está ajustado en V3 y el módulo está configurado con:<ul style="list-style-type: none">La versión 2 del firmware (BMENUA0100.2), utiliza SNMP V3 con nivel de seguridad SinAutSinPriv.Una versión del firmware anterior a la versión 2 (BMENUA0100), utiliza SNMP V1.Para obtener más información, consulte el tema Configuración del agente SNMP en Control Expert y en las páginas web, página 137.</div><div>3. NTP V4 puede configurarse para transportarse fuera del túnel IPsec.</div><div>4. Para las modalidades de funcionamiento de ciberseguridad Standard y Advanced (o Secured), si Configuración de seguridad está ajustado en <i>Ninguno</i>, no habrá autenticación de usuario (es decir, el ajuste de OPC UA Tipos de token de identificador de usuarioOPC UA, página 108 se establece en <i>Anónimo</i>).</div><div>5. Para proporcionar acceso en línea al controlador o a la red de dispositivos de Control Expert, configure el PC (en el que está instalado Control Expert) con una dirección IP que se encuentre en la misma subred que el puerto de control del módulo BMENUA0100 y utilice la dirección IP del puerto de control del módulo BMENUA0100 como dirección IP de la pasarela del PC. En este caso, ninguna dirección IP del PC puede estar en la misma subred que el puerto de la placa de conexiones del módulo BMENUA0100.</div></div>						

Servicios OPC UA

Introducción

En esta sección se describen los servicios compatibles con el servidor OPC UA integrado en el módulo BMENUA0100.

Características de funcionamiento del servidor OPC UA del módulo BMENUA0100

Limitaciones

Máximo:

- El número de nodos que se pueden publicar en el espacio de direcciones de acceso a datos del servidor OPC UA del módulo BMENUA0100 es de 100 000 nodos.
- La cantidad de memoria que se puede asignar al servidor OPC UA del módulo BMENUA0100 es de 192 MB.

NOTA: Si se sobrepasa cualquiera de estos límites, el estado del espacio de direcciones del servidor pasará a *LimitsExceeded*.

NOTA: El tiempo necesario para establecer la suscripción de tiempo podría depender significativamente del número de elementos y el número de clientes conectados.

A continuación, se indican otras limitaciones, el contexto en el que se producen y sus consecuencias si se exceden:

Límite	Valor	Servicio OPCUA	Parámetro del servicio	Efectos
Recuento de sesiones acumuladas	10	CreateSession	(No aplicable)	Código de resultado del servicio <i>Incorrecto_DemasiadasSesiones</i>
Tiempo de espera mínimo de la sesión	30 s	CreateSession	Tiempo de espera de sesión solicitado	Tiempo de espera de sesión corregido
Tiempo de espera de sesión acumulado	3600 s	CreateSubscription	Tiempo de espera de sesión solicitado	Tiempo de espera de sesión corregido
Recuento máximo de suscripciones acumuladas	40	CreateSubscription	(No aplicable)	Código de resultado del servicio <i>Incorrecto_DemasiadasSuscripciones</i>
Intervalo de publicación mínimo	250 ms ¹ 20 ms ²	CreateSubscription	Intervalo de publicación solicitado	Intervalo de publicación corregido
Intervalo de publicación máximo	10 s	CreateSubscription	Intervalo de publicación solicitado	Intervalo de publicación corregido
Duración máxima de suscripción	300 s	CreateSubscription	Mín.(Intervalo de publicación solicitado, 3 600 000) * Recuento de duración solicitada	Recuento de duración corregido

Límite	Valor	Servicio OPCUA	Parámetro del servicio	Efectos
Número máximo de notificaciones por publicación	12 500	CreateSubscription	maxNotificationsPerPublish	Por lo tanto, la capacidad máxima de las notificaciones es de (1000 / Intervalo de publicación corregido) * 1000 notificaciones por segundo.
Intervalo de muestreo mínimo	125 ms ¹ 20 ms ²	CreateMonitoredItems	Parámetros de supervisión. Intervalo de muestreo	Intervalo de muestreo corregido
Tamaño máximo de la cola de mensajes	3	CreateMonitoredItems	Parámetros de supervisión. Tamaño de cola	Tamaño de cola corregido
Recuento máximo de elementos supervisados acumulados	50010 o 35010 ^{3, 4} 2010 ²	CreateMonitoredItems	(No aplicable)	Código de resultado del servicio <i>Incorrecto_DemasiadosElementosSupervisados</i>
Máximo de suscripciones por sesión	4	–	–	–
Número máximo de elementos supervisados por suscripción	25000	–	–	–
<div>1. Si el muestreo rápido está deshabilitado.</div> <div>2. Si el muestreo rápido está habilitado.</div> <div>3. Si el muestreo rápido está deshabilitado y el servidor se ha configurado con:<ul style="list-style-type: none">• un intervalo de muestreo de al menos 1 segundo y• un intervalo de publicación de al menos 1 segundo.</div> <div>4. Si la marca de tiempo de origen está habilitada y activada, página 127, el máximo es 35010. Si no está activada, el máximo es 50010.</div>				

Servidor OPC UA

Introducción

El principal objetivo del módulo de comunicación Ethernet BMENUA0100 es proporcionar un canal de comunicación OPC UA mediante Ethernet entre los controladores M580 y los clientes OPC UA. Los datos de la CPU M580 se asignan a variables del módulo BMENUA0100 y se ponen a disposición de los clientes OPC UA mediante una pila de

comunicación del servidor OPC UA integrada en el módulo BMENUA0100. Los clientes OPC UA se conectan a la pila del servidor OPC UA integrado mediante la dirección IP del puerto de control o el puerto de la placa de conexiones del módulo BMENUA0100, por lo que establecen una conexión entre cliente y servidor. El módulo BMENUA0100 puede manejar un máximo de diez (10) conexiones simultáneas de cliente OPC UA para la versión 1.1 del firmware (o tres [3] conexiones simultáneas de cliente OPC UA para la versión 1.0 del firmware).

NOTA: Los términos de cada conexión entre un cliente OPC UA y el servidor OPC UA integrado en el módulo BMENUA0100 los determina el cliente, que define los atributos de la conexión entre el cliente y el servidor.

La pila del servidor OPC UA integrada en el módulo BMENUA0100 está formada por funciones definidas por los siguientes términos:

- **Perfil:** una definición de la función, que comprende otros perfiles, facetas, grupos de conformidad y unidades de conformidad.
- **Faceta:** define una función parcial.
- **Grupo de conformidad:** una colección de unidades de conformidad.
- **Unidad de conformidad:** un servicio específico, como lectura, escritura, etc.

Perfil compatible con BMENUA0100

El módulo BMENUA0100 es compatible con el **perfil Embedded 2017 UA Server**. Tal como se establece en el sitio web de la OPC Foundation, este perfil “es un perfil con todas las funciones diseñado para dispositivos con más de 50 MB de memoria y un procesador más potente. Este perfil se basa en el perfil de servidor de dispositivos incorporados Micro. Las adiciones más importantes son: soporte para seguridad a través de políticas de seguridad y soporte para la faceta Standard DataChange Subscription Server. Este perfil también requiere que los servidores expongan todos los tipos OPC-UA que utiliza el servidor, incluidos sus componentes y sus supertipos.

Para obtener más información, consulte el sitio web de OPC Foundation en: <http://opcfoundation.org/UA-Profile/Server/EmbeddedUA2017>.

Facetas compatibles con BMENUA0100

El módulo BMENUA0100 admite las siguientes facetas:

- **Categoría de servidor > Facetas > Características principales:**
 - **Faceta del servidor Core 2017** (<http://opcfoundation.org/UA-Profile/Server/Core2017Facet>)

- **Categoría de servidor > Facetas > Acceso a datos:**
 - **Faceta del servidor ComplexType 2017** (<http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017>)
 - **Faceta del servidor Data Access** (<http://opcfoundation.org/UA-Profile/Server/DataAccess>)
 - **Faceta del servidor Embedded DataChange Subscription** (<http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription>)
- **Categoría de servidor > Facetas > Características genéricas:**
 - **Faceta del servidor Method** (<http://opcfoundation.org/UA-Profile/Server/Methods>)
- **Categoría de seguridad > Facetas > Política de seguridad:**
 - **Basic128RSA15** (<http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15>)
 - **Basic256** (<http://opcfoundation.org/UA/SecurityPolicy#Basic256>)
 - **Basic256Sha256** (<http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256>)
- **Categoría de transporte > Facetas > Cliente-servidor:**
 - **UA-TCP- UA-SC UA-Binary** (<http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary>)

En los siguientes temas se tratan los servicios, relacionados con las facetas a las que se ha hecho referencia, compatibles con el módulo BMENUA0100.

Servicios de la pila del servidor OPC UA del módulo BMENUA0100

Servicios OPC UA compatibles

La pila del servidor OPC UA del módulo BMENUA0100 es compatible con los siguientes conjuntos de servicios y servicios:

Service Set	Services
Attribute	<ul style="list-style-type: none">• Read• Write
Discovery	<ul style="list-style-type: none">• FindServers• GetEndpoints
MonitoredItem	<ul style="list-style-type: none">• CreateMonitoredItems• ModifyMonitoredItems• DeleteMonitoredItems• SetMonitoringMode

Service Set	Services
SecureChannel	<ul style="list-style-type: none">• OpenSecureChannel• CloseSecurechannel
Session	<ul style="list-style-type: none">• CreateSession• ActivateSession• CloseSession
Subscription	<ul style="list-style-type: none">• CreateSubscription• ModifySubscription• DeleteSubscription• SetPublishingMode• SetMonitoringMode• Publish• Republish
View	<ul style="list-style-type: none">• Browse• BrowseNext• TranslateBrowsePathToNodeIds• RegisterNodes• UnregisterNodes

NOTA: Para obtener una descripción de estos conjuntos de servicios y servicios, consulte el documento *Especificación de arquitectura unificada de OPC, 4.ª parte: servicios (versión 1.04)*.

Servicios de acceso a datos de la pila del servidor OPC UA de BMENUA0100

Servicios de acceso a datos compatibles

El acceso a datos mediante la pila del servidor OPC UA integrado del módulo BMENUA0100 se habilita gracias a su compatibilidad con las siguientes facetas y los servicios relacionados:

- Faceta Data Access Server
- Faceta de servidor ComplexType 2017
- Faceta Core 2017 Server

NOTA: En las descripciones de facetas que aparecen a continuación, la letra cursiva indica una traducción del material de OPC Foundation. Haga clic en los enlaces que aparecen a continuación y use *OPC Foundation Unified Architecture Profile Reporting Visualization Tool* para acceder a una descripción de cada faceta.

Faceta Core 2017 Server

Como se indica en el sitio web de OPC Foundation, la faceta Core 2017 Server “define la funcionalidad básica requerida para cualquier implementación de servidor UA. La funcionalidad básica incluye la capacidad de detectar terminales, establecer canales de comunicación seguros, crear sesiones, examinar el espacio de direcciones y leer o escribir en atributos de nodos. Los requisitos principales son: compatibilidad con una sola sesión, compatibilidad con el objeto de servidor y funcionalidades de servidor, todos los atributos obligatorios de nodos en el espacio de direcciones y autenticación con nombre de usuario y contraseña. Para ampliar las posibilidades de aplicación, se recomienda que los servidores admitan diversos perfiles de transporte y seguridad”.

Si desea una descripción completa de esta faceta, consulte <http://opcfoundation.org/UA-Profile/Server/Core2017Facet>.

La pila del servidor OPC UA integrado del módulo BMENUA0100 es compatible con las siguientes unidades de conformidad de la faceta Core 2017 Server:

- El conjunto de servicios View, incluye los siguientes grupos y servicios:
 - View Basic: incluye los servicios Browse y BrowseNext.
 - View TranslateBrowsePath: incluye el servicio TranslateBrowsePathsToNodeIds.
 - View Register Nodes: incluye los servicios RegisterNodes y UnregisterNodes como forma de optimizar el acceso a nodos de uso frecuente del espacio de direcciones OPC UA del servidor.
- El conjunto de servicios Attribute, incluye los siguientes grupos y servicios:
 - Attribute read: incluye el servicio Read, que permite leer uno o más atributos de uno o más nodos, incluida la compatibilidad con el parámetro IndexRange para leer un solo elemento o un intervalo de elementos cuando el valor del atributo es una matriz.
 - Attribute Write values: incluye el servicio Write Value, que permite escribir uno o más valores en uno o más atributos de uno o más nodos.
 - Attribute Write Index: incluye el servicio Write Index, que es compatible con IndexRange para escribir en un solo elemento o en un intervalo de elementos cuando el valor del atributo es una matriz y se permiten actualizaciones parciales de esta matriz.

Faceta Data Access Server

Como se indica en el sitio web de OPC Foundation, la faceta Data Access Server “especifica la compatibilidad con un modelo de información utilizado para proporcionar datos de automatización industrial. En este modelo se definen estructuras estándar para elementos de datos analógicos y binarios y su calidad de servicio. Esta faceta amplía la faceta Core Server, que incluye compatibilidad con el comportamiento básico del espacio de direcciones”.

Si desea una descripción completa de esta faceta, consulte <http://opcfoundation.org/UA-Profile/Server/DataAccess>.

Faceta de servidor ComplexType 2017

Como se indica en el sitio web de OPC Foundation, la faceta ComplexType 2017 Server “amplía la faceta Core Server para incluir variables con datos estructurados, es decir, datos compuestos por varios elementos, como pueda ser una estructura, y en los que los elementos individuales se exponen como variables de componentes. La compatibilidad de esta faceta requiere la implementación de tipos de datos estructurados y variables que utilicen estos tipos de datos. El conjunto de servicios Read, Write y Subscriptions será compatible con la codificación y decodificación de estos tipos de datos estructurados. De manera opcional, el servidor también puede admitir codificaciones alternativas, como una codificación XML cuando se utiliza actualmente el protocolo binario y viceversa”.

Si desea una descripción completa de esta faceta, consulte <http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017>.

Servicios de detección y seguridad de la pila del servidor OPC UA de BMENUA0100

Introducción

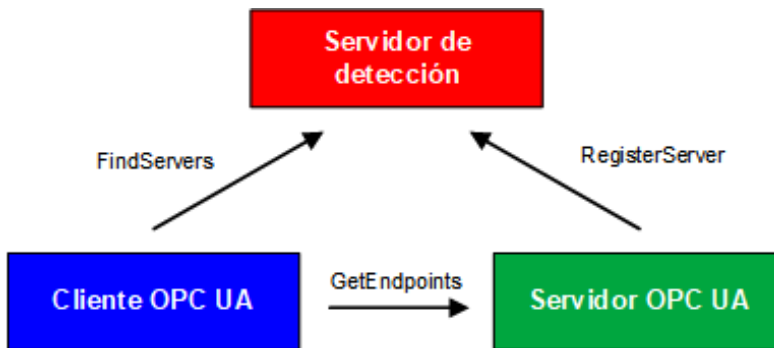
La pila del servidor OPC UA integrado del módulo BMENUA0100 admite servicios de detección y seguridad.

Para conectarse al servidor OPC UA del módulo BMENUA0100, el cliente OPC UA necesita información que describa el servidor, lo que incluye la dirección de red, el protocolo y la configuración de seguridad. OPC UA define un conjunto de características de detección que puede usar el cliente para obtener esta información.

La información necesaria para establecer una conexión entre un cliente OPC UA y un servidor OPC UA se almacena en un terminal. Un servidor OPC UA puede tener varios terminales, cada uno de los cuales contiene:

- URL del terminal (dirección de red y protocolo), por ejemplo:
 - Para IPv4: `opc.tcp://172.21.2.30:4840`, donde:
 - `opc.tcp` = protocolos
 - `172.21.2.30` = dirección IPv4
 - `4840` = número de puerto opcua-tcp configurado en Control Expert
 - Para IPv6: `opc.tcp://[2a01:cb05:431:f00:200:aff:fe02:a0a]:50000`, donde:
 - `opc.tcp` = protocolos
 - `[2a01:cb05:431:f00:200:aff:fe02:a0a]` = dirección IPv6
 - `50000` = número de puerto opcua-tcp configurado en Control Expert
- Política de seguridad (incluye un conjunto de algoritmos de seguridad y la longitud de la clave)
- Modalidad de seguridad de los mensajes (nivel de seguridad de los mensajes intercambiados)
- Tipo de token de usuario (tipos de autenticación del usuario compatibles con el servidor)

Puede haber uno o más servidores OPC UA. Si hay varios servidores, se puede usar un servidor de detección para proporcionar información sobre cada servidor. Pueden registrarse servidores individuales en el servidor de detección. Los clientes pueden pedir una lista de todos los servidores disponibles o de algunos de ellos al servidor de detección y usar el servicio `GetEndpoints` para adquirir información de conexión de un servidor individual.



El módulo BMENUA0100 es compatible con varios servicios de detección y seguridad, entre los que se incluyen:

- Conjunto de servicios Discovery
- Conjunto de servicios SecureChannel
- Conjunto de servicios Session

La decisión de habilitar o deshabilitar servicios depende de la política de ciberseguridad que decida implementar en el servidor.

Conjunto de servicios Discovery

La pila del servidor OPC UA de BMENUA0100 es compatible con el conjunto de servicios Discovery, que está incorporado en la *faceta Core 2017 Server*, página 42. Tal como se implementan en el módulo BMENUA0100, entre los servicios compatibles se incluyen:

- FindServers: tal como se implementa en la pila del servidor OPC UA del módulo BMENUA0100, este servicio busca los servidores solo en el servidor OPC UA local.
- GetEndpoints: devuelve los terminales compatibles con un servidor y la información de configuración necesaria para establecer un canal seguro y una sesión. Puede proporcionar una lista de devolución de terminales filtrada, en función de los perfiles.

Conjunto de servicios SecureChannel

La pila del servidor OPC UA de BMENUA0100 es compatible con el conjunto de servicios SecureChannel, que incluye los siguientes servicios:

- OpenSecureChannel: abre o renueva un canal seguro que proporciona confidencialidad e integridad para el intercambio de mensajes durante una sesión. Este servicio requiere que la pila del servidor OPC UA aplique los diferentes algoritmos de seguridad a los mensajes cuando se envían y reciben.
- CloseSecureChannel: termina un canal seguro.

Conjunto de servicios Session

La pila del servidor OPC UA de BMENUA0100 es compatible con el conjunto de servicios Session, que está incorporado en la *faceta Core 2017 Server*, página 42. Tal como se implementan en el módulo BMENUA0100, entre los servicios compatibles se incluyen:

- CreateSession: tras crear un canal seguro con el servicio OpenSecureChannel, el cliente usa este servicio para crear una sesión. El servidor devuelve dos valores que identifican de forma única la sesión:
 - Un ID de sesión, que se usa para identificar la sesión en los registros de auditoría y en el espacio de direcciones del servidor.
 - Un token de autenticación, que se usa para asociar una petición entrante con una sesión.
- ActivateSession: usado por el cliente para especificar la identidad del usuario asociado con la sesión. No se puede usar para cambiar el usuario de la sesión.
- CloseSession: termina una sesión.

NOTA: En los servicios CreateSession y ActivateSession, si la modalidad de seguridad = ninguna, entonces:

1. El certificado de la aplicación y el nonce son opcionales.
2. Las firmas son nulas o están vacías.

Servicios de publicación y suscripción de la pila del servidor OPC UA de BMENUA0100

Suscripciones

En lugar de leer información permanentemente mediante consultas, el protocolo OPC UA incluye la función Suscripción. Esta función permite a la pila OPC UA integrada en el módulo BMENUA0100 prestar servicios de publicación/suscripción, que se usan cuando el módulo se conecta a dispositivos remotos.

El cliente OPC UA puede suscribirse a uno o más nodos seleccionados y permitir que el servidor supervise estos elementos. Cuando se produce un evento de cambio, como un cambio de valor, el servidor notifica el cambio al cliente. Este mecanismo reduce significativamente la cantidad de datos transferidos y, por lo tanto, reduce significativamente el consumo de ancho de banda.

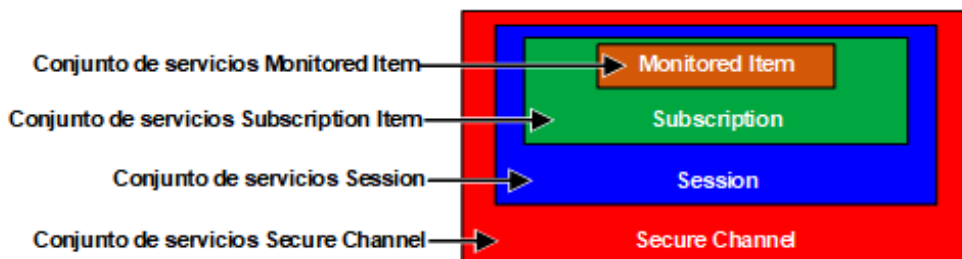
El cliente OPC UA puede suscribirse a los diferentes tipos de información que proporciona un servidor OPC UA. La suscripción agrupa estos diferentes tipos de datos, llamados elementos vigilados, para formar una sola colección de datos denominada notificación.

Una suscripción debe:

- Estar formada por un elemento vigilado como mínimo.
- Crearse en el contexto de una sesión, que se crea en el contexto de un canal seguro.

NOTA: La suscripción puede transferirse a otra sesión.

Los conjuntos de servicios que componen una suscripción de cliente se describen a continuación:



Suscripciones y desbordes

En algunos casos en los que existe un gran número de peticiones de suscripción, el servidor OPC UA intenta obtener datos del controlador en una cantidad superior a la que pueden gestionar el controlador o el módulo BMENUA0100 en el intervalo de publicación especificado. En este caso, el tiempo de ejecución de las peticiones de suscripción se ampliará automáticamente, y la siguiente ejecución de suscripción se pospondrá hasta que se puedan atender todas las peticiones.

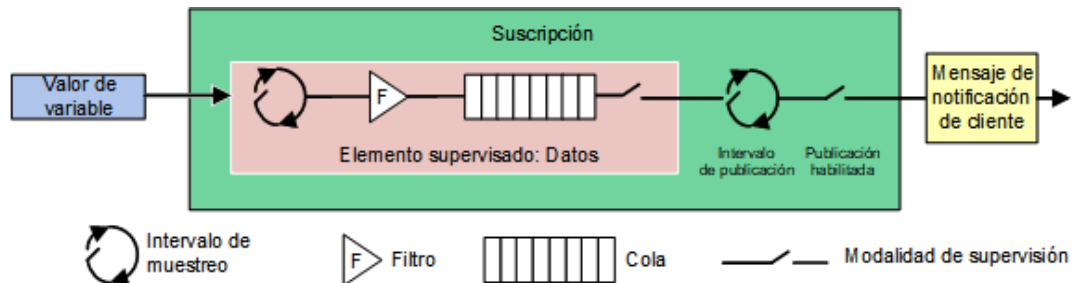
Al establecer un intervalo de publicación, tenga en cuenta el número de clientes y peticiones de cliente que el servidor debe gestionar. Al determinar el número de peticiones de cliente, compruebe que todos los clientes estén conectados en línea. En este sentido, tenga en cuenta que algunos clientes pueden tardar 2 minutos o más en conectarse en línea después de arrancarse.

NOTA: Establezca el intervalo de publicación en, como mínimo, el doble del intervalo de muestreo para evitar que falten cambios en los datos.

Eventos de cambio

Un cliente puede suscribirse a un evento de cambio de datos, que es desencadenado por un cambio del atributo de valor de una variable, como un elemento vigilado.

Los ajustes configurables de la suscripción, su secuencia y sus roles se describen a continuación:



Los tres ajustes siguientes determinan cómo se añaden a una suscripción los elementos vigilados:

- Intervalo de muestreo: el intervalo de tiempo de muestreo definido para cada elemento vigilado de la suscripción. Esta es la frecuencia con la que el servidor consulta el origen de datos para comprobar si hay cambios. Para un único elemento de variable, el intervalo de muestreo puede ser menor (es decir, más rápido) que el periodo transcurrido entre las notificaciones enviadas al cliente. En este caso, el servidor OPC UA puede poner en cola las muestras y publicar la cola completa. En casos extremos, el servidor revisará (es decir, ralentizará) el intervalo de muestreo para que el origen de datos no experimente la carga de colas excesiva que puede causar el propio muestreo.

NOTA: Si OPC UA puede poner en cola muestras de datos, el tamaño de la cola (es decir, el número máximo de valores que se pueden poner en cola) se puede configurar para cada elemento vigilado. Cuando los datos se entregan al cliente (se publican), la cola se vacía. En caso de desborde de la cola, se descartan los datos más antiguos y se sustituyen por datos nuevos.

- Filtro: una colección de varios criterios usados para identificar qué cambios o eventos de datos se comunican y cuáles se bloquean.
- Modalidad de vigilancia: usada para habilitar o deshabilitar el muestreo y la comunicación de datos.

Los dos ajustes siguientes se aplican a la propia suscripción:

- Intervalo de publicación: periodo tras el que las notificaciones recopiladas en las colas se entregan al cliente en un mensaje de notificación (respuesta de publicación). El cliente OPC UA debe confirmar que el servidor OPC UA ha recibido suficientes tokens de publicación (peticiones de publicación) para que, cuando haya transcurrido el intervalo de publicación y haya una notificación preparada para ser enviada, el servidor use dichos tokens y envíe los datos en una respuesta de publicación. Si no hay nada que comunicar (por ejemplo, no ha cambiado ningún valor), el servidor enviará al cliente una notificación KeepAlive, que es una publicación vacía, para indicar que el servidor sigue conectado.
- Publicación habilitada: habilita y deshabilita el envío del mensaje de notificación.

Faceta Embedded DataChange Subscription Server

Como se indica en el sitio web de la OPC Foundation, la faceta Embedded DataChange Subscription Server “especifica el nivel mínimo de compatibilidad para las notificaciones de cambio de datos dentro de las suscripciones. Incluye límites que minimizan el consumo de memoria y procesamiento necesarios para implementar la faceta. Esta faceta incluye funciones para crear, modificar y eliminar suscripciones, así como para añadir, modificar y eliminar elementos supervisados. Para cada sesión, como mínimo, los servidores admitirán una suscripción con un máximo de dos elementos. Además, es necesario admitir dos peticiones de publicación paralelas. Esta faceta está diseñada para una plataforma como la proporcionada por el perfil de servidor de dispositivos incorporados Micro, en la que la memoria es limitada y es necesario gestionarla”.

Si desea una descripción completa de esta faceta, consulte <http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription>.

Esta faceta admite los siguientes servicios :

- Conjunto de servicios Monitored Item
- Conjunto de servicios Subscription

Conjunto de servicios Monitored Item

El conjunto de servicios Monitored Item es compatible con los siguientes servicios:

NOTA: Si desea una descripción de estos conjuntos de servicios y estos servicios, consulte el documento *Especificaciones de OPC Unified Architecture, 4.ª parte: servicios (versión 1.04)*.

- CreateMonitoredItems: llamada asíncrona usada para crear uno o más elementos supervisados y añadirlos a una suscripción.
- ModifyMonitoredItems: una llamada asíncrona para modificar elementos vigilados. Este servicio se usa para modificar los elementos vigilados de una suscripción. El servidor aplica inmediatamente los cambios de los ajustes de los elementos vigilados.
- DeleteMonitoredItems: una llamada asíncrona para eliminar elementos vigilados. Este servicio se usa para quitar uno o más elementos vigilados de una suscripción. Cuando se elimina un elemento vigilado, también se eliminan las conexiones de elementos que ha desencadenado.
- SetMonitoringMode: una llamada asíncrona para definir la modalidad de vigilancia de una lista de elementos vigilados. Este servicio se usa para definir la modalidad de vigilancia de uno o más elementos vigilados de una suscripción. Si la modalidad se define como DESHABILITADA, se eliminan todas las notificaciones puestas en cola.

Conjunto de servicios Subscription

El conjunto de servicios Subscription es compatible con los siguientes servicios:

NOTA: Si desea una descripción de estos conjuntos de servicios y estos servicios, consulte el documento *Especificaciones de OPC Unified Architecture, 4.ª parte: servicios (versión 1.04)*.

- CreateSubscription: una llamada asíncrona para crear una suscripción.
- ModifySubscription: una llamada asíncrona para modificar una suscripción. El servidor aplica inmediatamente los cambios a la suscripción.
- DeleteSubscription: una llamada asíncrona para eliminar una o más suscripciones que pertenecen a la sesión de cliente. Una vez completado correctamente este servicio, se eliminan todos los elementos vigilados asociados con la suscripción.
- Publish: este servicio se usa con dos fines, que son confirmar la recepción de los mensajes de notificación de una o más suscripciones y solicitar al servidor que devuelva un mensaje de notificación o un mensaje KeepAlive.

- **Republish:** una llamada asíncrona de repetición de la publicación para recibir las notificaciones perdidas. Este servicio pide a la suscripción que vuelva a publicar un mensaje de notificación desde su cola de retransmisión. Si el servidor no tiene el mensaje pedido en su cola de retransmisión, devuelve una respuesta de error.
- **SetPublishingMode:** una llamada asíncrona para habilitar el envío de notificaciones en una o más suscripciones.

Servicios de transporte de la pila del servidor OPC UA de BMENUA0100

Compatibilidad con la faceta UA-TCP UA-SC UA-Binary

El módulo BMENUA0100 es compatible con la faceta de transporte UA-TCP UA-SC UA-Binary. (Si desea información adicional, consulte la descripción online en <http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary>).

Esta faceta de transporte define una combinación de protocolos de red, protocolos de seguridad y codificación de mensajes optimizada para consumir pocos recursos y ofrecer un alto rendimiento. Combina el protocolo de red TCP sencillo UA-TCP 1.0 con el protocolo de seguridad binario UA-SecureConversation 1.0 y la codificación de mensajes binaria UA-Binary 1.0.

Los datos que se transmiten del cliente OPC UA al servidor OPC UA integrado del módulo BMENUA0100 usan el protocolo TCP y se codifican de forma binaria de acuerdo con el formato de archivo binario OPC UA.

NOTA: El formato de archivo binario OPC UA sustituye a XML UA-Nodeset Schema, de OPC Foundation. Aumenta el rendimiento y reduce el consumo de memoria. No necesita analizador XML.

Detección de variables de controladores

Asignación de variables del controlador de Control Expert a variables lógicas de datos de OPC UA

Introducción

El servidor integrado OPC UA del módulo BMENUA0100 usa peticiones del diccionario de datos Unified Messaging Application Services (UMAS) para examinar y detectar las

variables de la aplicación del controlador M580. Tendrá que activar el diccionario de datos en los ajustes del proyecto de Control Expert.

NOTA:

- El módulo BMENUA0100 puede admitir un tamaño máximo de diccionario de datos de 100 000 variables.
- El tiempo necesario para cargar el diccionario de datos en el servidor OPC UA depende del número de elementos del diccionario de datos y del ajuste del periodo MAST, página 176.

Las variables recopiladas se traducen de la vista del modelo lógico de datos de Control Expert a la vista del modelo lógico de datos OPC UA con los servicios apropiados de la pila OPC UA. Un cliente OPC UA conectado al módulo BMENUA0100 (mediante su puerto de control o mediante su puerto de la placa de conexiones gracias al controlador o a un módulo de comunicación BMENOC0301 o BMENOC0311) puede recuperar esta colección de datos con los servicios de la faceta del servidor Data Access, página 42 compatibles con el perfil Embedded 2017 UA Server, página 39.

Carga previa del diccionario de datos para evitar interrupciones de la comunicación

Los cambios de la aplicación online realizados con Control Expert interrumpen temporalmente la comunicación servidor/cliente OPC UA mientras el servidor adquiere un diccionario de datos actualizado. Esta interrupción la causa la asignación incoherente de los datos del controlador mientras se actualiza el diccionario de datos. Durante el período de interrupción de la comunicación, el estado de los nodos monitoreados, según lo indicado por UA Expert, es erróneo (**error de comunicación incorrecta, comunicación incorrecta o tiempo de espera incorrecto**). Para evitar esta interrupción de las comunicaciones y sus consecuencias, puede configurarse un mecanismo de sincronización entre el módulo BMENUA0100 y el software de configuración de Control Expert basado en una carga previa del diccionario de datos actualizado.

NOTA: Los comandos OPC UA (READ/WRITE) no se tienen en cuenta cuando BMENUA0100 está ocupado adquiriendo el diccionario de datos.

Esta función se habilita en Control Expert en la ventana **Herramientas > Configuración del proyecto...**, en el área **General > Datos incorporados del PLC**, utilizando los ajustes **Cargar previamente si cambia la compilación y Tiempo de espera efectivo de cambios de compilación** (consulte EcoStruxure™ Control Expert, Modalidades de funcionamiento). Consulte la ayuda en línea de Control Expert si desea obtener información sobre cómo configurar esta característica.

Activación del diccionario de datos

Para activar el diccionario de datos en Control Expert:

Paso	Acción
1	En Control Expert, con el proyecto abierto, seleccione Herramientas > Ajustes del proyecto .
2	En la ventana Ajustes del proyecto , vaya a General > Datos incorporados del PLC y, a continuación, seleccione Diccionario de datos . NOTA: Si el proyecto de EcoStruxure™ Control Expert incluye un módulo BMENUA0100 y este ajuste no está seleccionado, se genera un error detectado durante la compilación de la aplicación.

Conversión de tipo de datos de variable

El módulo BMENUA0100 puede detectar y convertir en tipos de datos OPC UA los siguientes tipos de variables básicos compatibles con el modelo lógico de datos de Control Expert:

Tipo de datos elemental de Control Expert	Tipo de datos de 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
* Consulte la tabla que aparece a continuación, en la que se describe la conversión de los tipos de datos relacionados con la fecha.	

Para los datos de Control Expert de los tipos DATE, TIME, TOD y DT, los correspondientes tipos de datos OPC UA son los siguientes:

Tipo de datos elemental de Control Expert	Valor de ejemplo mostrado en Control Expert	Tipo de datos OPC UA	Valor correspondiente en el tipo de 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	Doble	4.29E-154
1. Los datos devueltos para los valores de fecha y hora son UATypeUInt64, que es la codificación interna de IEC 1131 DT en Control Expert (codificación decimal codificada en binario [BCD]).			

Variables detectables

Para las variables, el cliente OPC UA no accede directamente a una variable lógica de datos del controlador detectada. El cliente accede a la variable del controlador detectada mediante una variable lógica de datos OPC UA, que se encuentra en el módulo BMENUA0100 y está asignada a la variable del controlador subyacente. Dada la naturaleza de paso del acceso a la variable de datos, el proceso de petición de la adquisición no está optimizado, y el rendimiento de la adquisición del diccionario de datos no es representativo del rendimiento del controlador.

NOTA: El cliente OPC UA no puede acceder a referencias del tipo REF_TO a variables de la aplicación en el servidor OPC UA.

Entre los ejemplos de variables del controlador de Control Expert detectables por el servidor OPC UA en el módulo BMENUA0100 se incluyen:

- Variables estructuradas con subcampos: Variables de DDT y matriz.
- Las variables de unidad de programa son detectables como se indica a continuación:
 - El cliente OPC UA solo puede acceder a las variables de entrada/salida para el tipo BOOL.
 - El cliente OPC UA puede acceder a las variables de entrada y las variables de salida, excepto para los tipos REF_TO, ARRAY, String y Structure.

Además, las siguientes variables son detectables por el servidor OPC UA, que las asigna a variables de la aplicación y, a continuación, detecta las variables de la aplicación de dicha asignación:

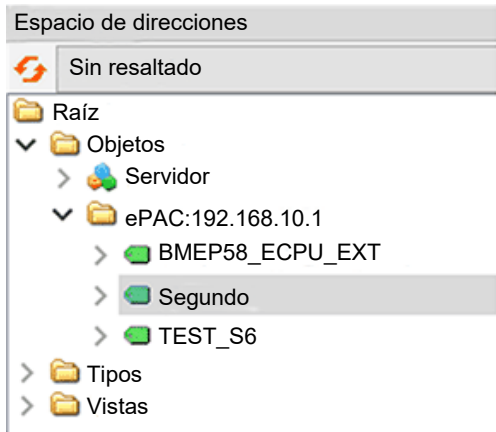
- Variables de E/S topológicas:
 - Entradas: %I, %IW, %ID, %IF.
 - Salidas: %Q, %QW, %QD, %QF.
- Variables ubicadas: %M, %MW, %MD, %MF.
- Variables de sistema: %S, %SW, %SD.

NOTA: La detección de la variable incluye una variable (o un símbolo) para un bit extraído (por ejemplo, MyBoolVar ubicada en %MW100.1).

Presentación de las variables detectadas en el cliente OPC UA

El servidor OPC UA del módulo BMENUA0100 puede organizar y mostrar gráficamente las variables del controlador detectadas. Es posible conectar una herramienta cliente OPC UA al módulo BMENUA0100 y ver una presentación de árbol de nodos de las variables del servidor OPC UA.

En el ejemplo que aparece a continuación, un cliente OPC UA (en este ejemplo, la herramienta cliente Unified Automation UaExpert) conectado al módulo BMENUA0100 puede ver las variables del controlador en sus ventanas de **Espacio de direcciones**. La dirección IP del controlador M580 está representada por el nodo ePAC:192.168.10.1. Sus nodos secundarios representan variables de aplicación de Control Expert:



En el ejemplo anterior, el primer subnodo, BMEP58_ECPU_EXT, representa los DDT del dispositivo para el controlador M580, del que se crea una instancia automáticamente cuando el controlador se añade a la aplicación Control Expert. Los nodos siguientes representan otros objetos añadidos a la aplicación.

Con la herramienta cliente OPC UA, el nodo TEST_S6 se arrastró y colocó en la ventana **Vista de acceso a datos**, en la que se muestran los detalles de la variable:

Vista de acceso a datos								
N.º	Servidor	ID de nodo	Nombre de visualización	Valor	Tipo de datos	Marca de tiempo de origen	Marca de tiempo de servidor	Código de estado
1	bmenua-server	NS2(String)0:Test_S6	TEST_S6	false	Booleano	10:43:54.830	10:43:54.830	Bueno
2	bmenua-server	NS0(Numeric)2258	CurrentTime	2019-08-12T08:43:54.733Z	Fecha y hora	10:43:54.733	10:43:54.830	Bueno

En este caso, el tipo de datos OPC UA de la variable es *Boolean* (lo que indica que el tipo de datos del controlador subyacente es BOOL) y su valor es *false*.

NOTA: El atributo **Marca de tiempo del servidor** de los nodos OPC UA se recibe del servidor OPC UA de BMENUA0100 en formato UTC (hora universal coordinada). Se muestra en hora local.

Lectura y escritura de las variables detectadas en el cliente OPC UA

Una etiqueta OPC UA de un cliente OPC UA (por ejemplo, un SCADA) que hace referencia a una variable de matriz permite al cliente leer o escribir todos los elementos de la matriz. Por ejemplo, la etiqueta "MyArray" declarada como ARRAY[0...31] OF INT.

Sin embargo, para que el cliente pueda leer o escribir solo un único elemento de una matriz, es necesario declarar una etiqueta específica que haga referencia a ese único elemento de destino de la matriz. Por ejemplo, "MyInt" declarado como INT en referencia a MyArray[2].

Hot Standby y redundancia

Redundancia del servidor OPC UA

Dos tipos de redundancia

El módulo BMENUA0100 admite los siguientes tipos de redundancia:

- Arquitectura Hot Standby, que describe los controladores redundantes.
- Redundancia de servidores OPC UA, que describe el uso de módulos redundantes BMENUA0100.

La redundancia de los servidores OPC UA, que gestionan los módulos BMENUA0100, sigue el estándar OPC UA "redundancia de servidores no transparente en modalidad de conmutación por error 'Warm'", tal y como define OPC Foundation.

Estos dos tipos de redundancia pueden combinarse. Se admiten los siguientes diseños:

- Un controlador independiente con dos módulos BMENUA0100.
- Dos controladores Hot Standby, cada uno de ellos con uno o dos módulos BMENUA0100.

Redundancia de OPC UA

En una arquitectura redundante de servidor no transparente OPC UA en modalidad de conmutación por error Warm, el cliente OPC UA establece sesiones y administra las

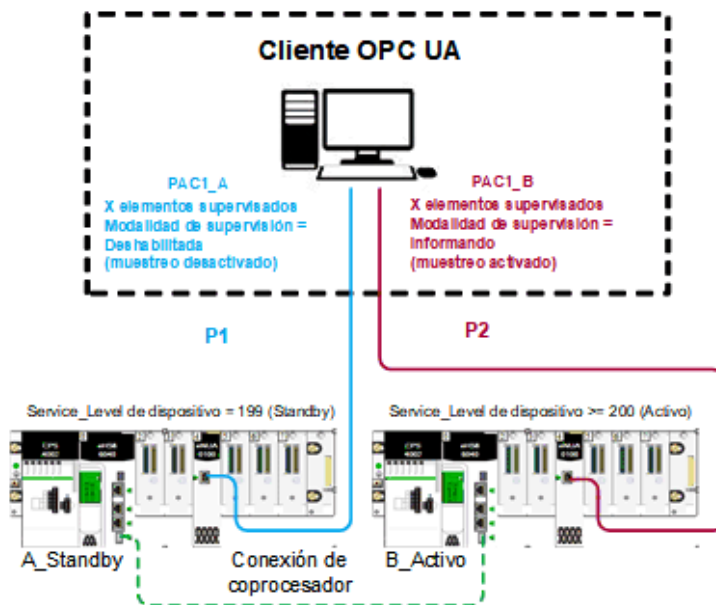
comunicaciones con servidores redundantes. Las sesiones que se establecerán incluyen: una sesión activa con el servidor primario y una sesión inactiva con el servidor secundario (o standby). El cliente necesita configurar estas dos sesiones para incluir los mismos elementos supervisados.

El cliente OPC UA comprueba el estado de los dos servidores a través de la variable `SERVICE_LEVEL` y cambia la comunicación al servidor cuyo estado funcional sea el más óptimo, en función del valor de esta variable.

El estándar OPC UA sostiene que la activación de las comunicaciones se realiza ajustando la *modalidad de supervisión* de las diferentes sesiones en el valor adecuado. La *modalidad de supervisión* de los servidores la controla el cliente OPC UA, mientras que el procedimiento para ajustarlo depende de la implementación del cliente. Para obtener más información sobre el ajuste de la *modalidad de supervisión*, consulte la documentación del cliente OPC UA.

Se trata de un principio general que se aplica a cualquier arquitectura, incluidas las arquitecturas Hot Standby.

En el siguiente diagrama se describe un cliente OPC UA conectado a un par de servidores OPC UA redundantes (cada uno integrado en un módulo BMENUA0100). El cliente ha designado como servidor activo el que tiene el valor de `SERVICE_LEVEL` más alto:



Hot Standby

En una configuración Hot Standby, se puede instalar un máximo de dos módulos BMENUA0100 en cada bastidor local principal Hot Standby. Cada módulo BMENUA0100 se configura con una sola dirección IP fija. Los módulos BMENUA0100 conservan sus respectivas direcciones IP y no intercambian direcciones IP en una conmutación o intercambio Hot Standby.

NOTA: En los sistemas Hot Standby, compruebe que los módulos BMENUA0100 de los controladores primario y Hot Standby:

- Estén configurados con ajustes de ciberseguridad, página 89 idénticos, y
- Tengan sus **conmutadores rotativos**, página 25 (ubicados en la parte trasera del módulo) colocados en la misma posición.
- Estén instalados en el mismo número de slot, página 65 en sus respectivos bastidores principales locales.

Si no se dan estas condiciones, el módulo no podrá recuperar la configuración establecida por Control Expert y almacenada en el controlador, y se iniciará en modalidad autónoma. El sistema no realiza estas comprobaciones automáticamente.

Los DDT del módulo BMENUA0100 incluyen la variable **SERVICE_LEVEL**, página 159, que facilita información al controlador sobre el estado del servidor OPC UA del módulo BMENUA0100. El cliente OPC UA es informado del estado del servidor OPC UA a través de la variable **SERVICE_LEVEL**, que está disponible como variable de OPC UA.

NOTA: Incluya la función elemental **READ_DDT** a fin de actualizar el DDT de cada módulo BMENUA0100. En una configuración Hot Standby, añada **READ_DDT** a una sección de código que se ejecute cuando el controlador esté en modalidad standby. Este diseño devuelve información de diagnóstico de BMENUA0100 que se puede intercambiar entre los controladores primario y Hot Standby. La aplicación puede usar esta información para realizar una comprobación de coherencia de los servicios compatibles y las configuraciones de ciberseguridad de los módulos BMENUA0100 en los controladores primario y Hot Standby.

Si el de **T_M_ECPU_HSBY** (consulte Modicon M580 Hot Standby, Guía de planificación del sistema, Arquitecturas de uso frecuente) del controlador Hot Standby y su elemento **CMD_SWAP** se ponen a disposición como variables de HMI en un sistema SCADA, la aplicación SCADA puede desencadenar un intercambio escribiendo en la variable OPC UA asignada apropiada del módulo BMENUA0100.

En un sistema Hot Standby, el módulo BMENUA0100 que administra las comunicaciones OPC UA con SCADA puede ser el ubicado en el bastidor local standby. Por este motivo, debe seleccionar el atributo **Intercambio en STBY** para todas las variables de la aplicación exploradas con el fin de garantizar la coherencia de los valores de las variables entre los controladores primario y Hot Standby.

Además, para mantener la coherencia, las aplicaciones de los dos controladores Hot Standby deben estar sincronizadas.

En casos raros (sobre todo, cuando el bit ECPU_HSBY_1.PLCX_ONLINE se define como FALSE manualmente o mediante programación), uno de los controladores de un sistema Hot Standby puede estar en la modalidad de espera. En esta modalidad, este controlador (el Hot Standby) no está sincronizado con el controlador primario y las variables leídas de este controlador son incorrectas. El estado de un controlador que responda puede vigilarse con los siguientes campos de los DDT de 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

Además, el sistema Hot Standby permite que los dos controladores funcionen al tiempo que se ejecutan diferentes aplicaciones. Para garantizar la coherencia de las variables entre los controladores primario y standby, el diseño de los datos de los 2 controladores debe ser coherente, como se muestra en el campo del DDT de T_M_ECPU_HSBY:

- T_M_ECPU_HSBY_1.DATA_LAYOUT_MISMATCH = FALSE

NOTA: Cuando configure la redundancia de OPC UA, compruebe mediante programación los DDT del módulo para confirmar que los servicios compatibles y las configuraciones de ciberseguridad de los módulos BMENUA0100 sean coherentes.

Compatibilidad de OPC UA con servidores, clientes y redes redundantes

Como se indica en las especificaciones de OPC Unified Architecture, 4.^a parte: Servicios, versión 1.04, "OPC UA la redundancia de servidores, clientes y redes. OPC UA proporciona las estructuras de datos y los servicios mediante los cuales se puede lograr la redundancia de manera estandarizada".

"La redundancia de servidores permite a los clientes disponer de múltiples fuentes de las cuales obtener los mismos datos. La redundancia de servidores se puede lograr de varias maneras, algunas de las cuales requieren la interacción del cliente, mientras que otras no la requieren. Los servidores redundantes podrían existir en sistemas sin redes o clientes redundantes. Los servidores redundantes también podrían coexistir en sistemas con redundancia de red y cliente".

"La redundancia de clientes permite que los clientes configurados de manera idéntica se comporten como si fueran clientes únicos; sin embargo, no todos los clientes obtienen datos en un momento determinado. Lo ideal es que no se pierda información cuando se produce una conmutación por error de cliente. Los clientes redundantes podrían existir en sistemas sin redes o servidores redundantes. Los clientes redundantes también podrían coexistir en sistemas con redundancia de red y servidor".

"La redundancia de red permite que un cliente y un servidor dispongan de varias rutas de comunicación para obtener los mismos datos. Las redes redundantes podrían existir en

sistemas sin servidores o clientes redundantes. Las redes redundantes también podrían coexistir en sistemas con redundancia de cliente y servidor. OPC UA 4.^a parte, sección 6.6.1”

Redundancia de servidores

Como se indica en las especificaciones de OPC Unified Architecture, 4.^a parte: Servicios, versión 1.04, “Hay dos modalidades generales de redundancia de servidores: transparente y no transparente”.

“En la redundancia transparente, la conmutación por error de las responsabilidades de un servidor a otro es transparente para el cliente. El cliente no sabe que se ha producido una conmutación por error, por lo que no tiene control sobre el comportamiento de dicha conmutación por error. Además, el cliente no necesita realizar ninguna acción para seguir enviando o recibiendo datos”.

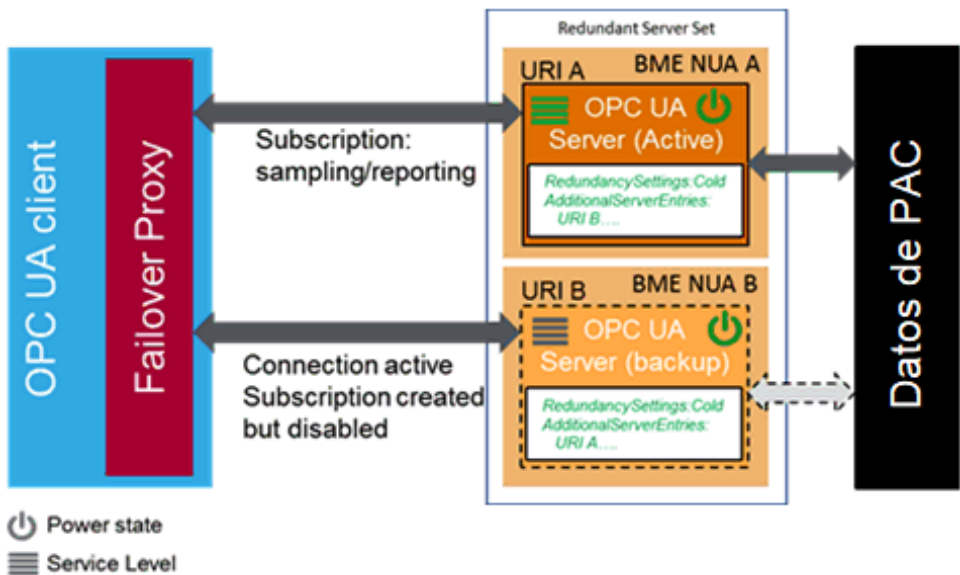
“En la redundancia no transparente, sin embargo, la conmutación por error de un servidor a otro y las acciones para seguir enviando o recibiendo datos las realiza el cliente. El cliente debe conocer el conjunto de servidores redundantes y realizar las acciones necesarias para beneficiarse de la redundancia del servidor”.

“El objeto ServerRedundancy indica la modalidad que admite el servidor. El ObjectType ServerRedundancyType y sus subtipos TransparentRedundancyType y NonTransparentRedundancyType proporcionan información sobre la modalidad de redundancia admitida. OPC UA 4.^a parte, sección 6.6.2.”

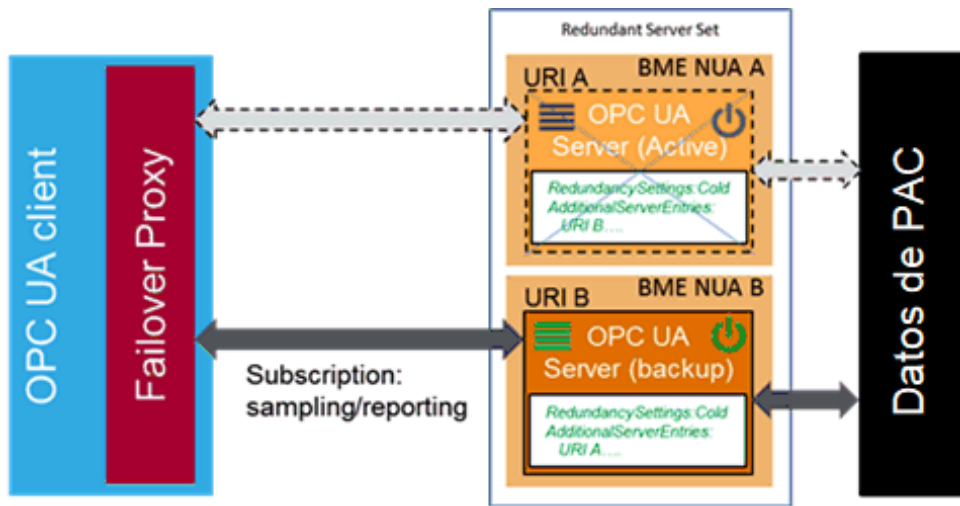
Como se ha indicado anteriormente, el servidor OPC UA del módulo BMENUA0100 es compatible con la redundancia de servidor no transparente en la modalidad de conmutación por error Warm.

Modalidad de conmutación por error Warm del servidor OPC UA

Como se indica en las especificaciones de OPC Unified Architecture, 4.^a parte: Servicios, versión 1.02, en la modalidad de conmutación por error Warm, “los servidores de reserva pueden estar activos, pero no pueden conectarse a puntos de datos reales”. Por lo tanto, solo un único servidor podrá consumir datos de la aplicación Control Expert. “La variable ServiceLevel ... indica la capacidad del servidor de proporcionar sus datos al cliente”. OPC UA, 4.^a parte, sección 6.6.2.4.4



Si se produce conmutación por error, es necesaria acción del cliente OPC UA; el servidor OPC UA integrado en BMENUA0100 se desactiva:



Comportamiento en la conmutación por error del cliente

Como se indica en las especificaciones de OPC Unified Architecture, 4.ª parte: Servicios, versión 1.04, "Cada servidor tiene una lista de URI del servidor para todos los servidores redundantes del conjunto de servidores redundantes".

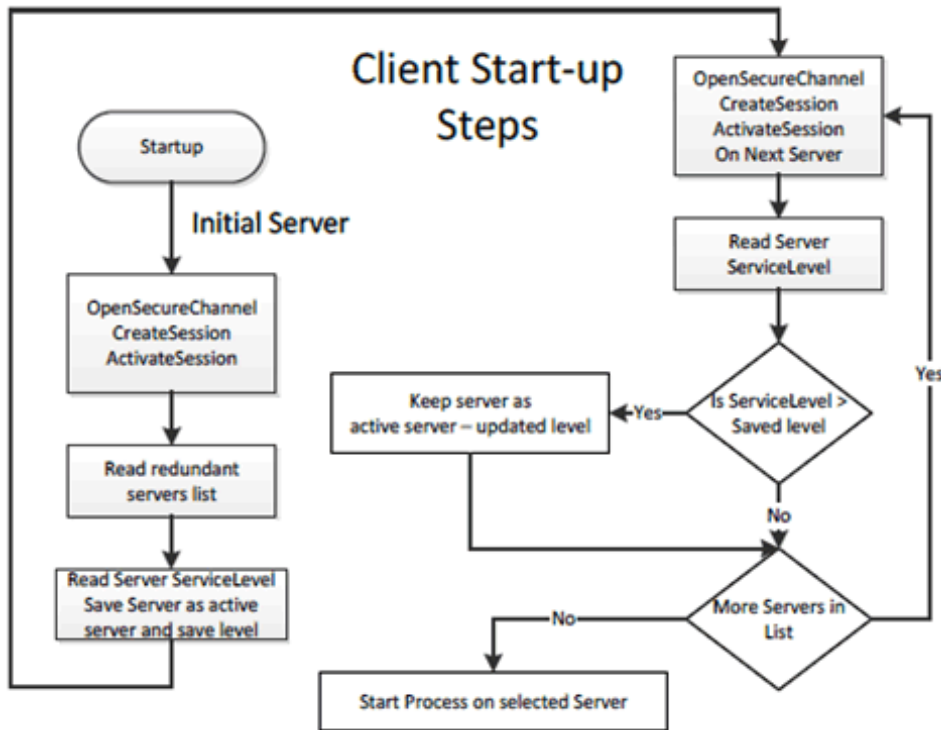
NOTA: Un conjunto de servidores redundantes es la colección de servidores OPC UA de la aplicación Control Expert configurados para proporcionar redundancia.

"La lista se proporciona junto con la modalidad de conmutación por error en el objeto ServerRedundancy. Para permitir que los clientes se conecten a todos los servidores de la lista, cada servidor de la lista debe proporcionar la descripción de la aplicación para todos los servidores del conjunto de servidores redundantes a través del servicio FindServers. El cliente necesita esta información para convertir los URI de servidor en la información necesaria para conectarse con los otros servidores del conjunto de servidores redundantes. Por lo tanto, un cliente necesita conectarse a uno solo de los servidores redundantes para encontrar los otros servidores según la información proporcionada. Uno de los clientes debe conservar la información sobre otros servidores del conjunto de servidores redundantes. OPC UA 4.ª parte, sección 6.6.2.4.5.1"

Entre las opciones del cliente en la modalidad de conmutación por error Warm se incluyen las siguientes:

- En la conexión inicial, además de las acciones en el servidor activo:
 - Conectarse a más de un servidor OPC UA.
 - Crear suscripciones y añadir elementos vigilados.
- En la conmutación por error:
 - Activar el muestreo en las suscripciones.
 - Activar la publicación.

“Los clientes que se comunican con un conjunto de servidores redundantes no transparentes necesitan algo de lógica adicional para poder gestionar los fallos de los servidores y para realizar la conmutación por error a otro servidor del conjunto de servidores redundantes. En la figura que aparece a continuación se ofrece una descripción general de los pasos que suele dar un cliente la primera vez que se conecta a un conjunto de servidores redundantes”.



“El servidor inicial se puede obtener mediante la detección estándar o a partir de una lista persistente de servidores del conjunto de servidores redundantes. Sin embargo, en cualquier caso, el cliente debe comprobar a qué servidor del conjunto de servidores debe conectarse. Las diferentes acciones dependerán de la modalidad de conmutación por error del servidor que proporcione el servidor y de la modalidad de conmutación por error que usará el cliente”.

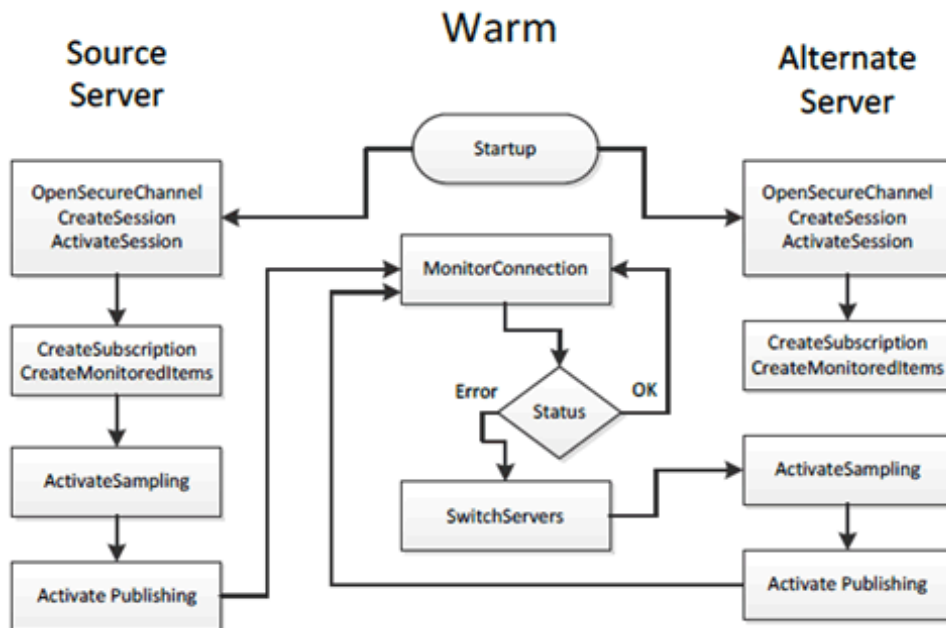
“Los clientes, una vez que se conectan a un servidor redundante, deben conocer las modalidades de conmutación por error que admite el servidor, ya que esta compatibilidad afecta a las opciones disponibles relacionadas con el comportamiento del cliente. Un cliente siempre puede tratar a un servidor mediante una modalidad de conmutación por error menor, es decir, en el caso de un servidor que proporciona redundancia Hot, un cliente puede conectarse y optar por tratarlo como si el servidor estuviera ejecutándose en modalidad de redundancia Warm o Cold. Esta elección dependerá del cliente. En el caso de la modalidad de conmutación por error HotAndMirrored, el cliente no utilizará la modalidad

de conmutación por error Hot o Warm, ya que generaría una carga innecesaria en los servidores. OPC UA 4.ª parte, sección 6.6.2.4.5.1”

Modalidad de conmutación por error Warm del cliente OPC UA

Como se indica en las especificaciones de OPC Unified Architecture, 4.ª parte: Servicios, versión 1.04, en el modo de conmutación por error Warm, “el cliente debe conectarse a uno o varios servidores en el conjunto de servidores redundantes principalmente para supervisar el nivel de servicio (ServiceLevel). Aunque un cliente puede conectar y crear suscripciones y elementos supervisados (MonitoredItems) en más de un servidor, el muestreo y la publicación solo pueden estar activos en un servidor. Sin embargo, el servidor activo devolverá los datos reales, mientras que los otros servidores del conjunto de servidores redundantes devolverán un error apropiado para los MonitoredItems en la respuesta de publicación como, por ejemplo, Bad_NoCommunication. El único servidor activo se puede encontrar leyendo la variable ServiceLevel de todos los servidores”.

“El servidor con el nivel de servicio más alto es el servidor activo. En el caso de la conmutación por error, el cliente activa el muestreo y la publicación en el servidor con el nivel de servicio más alto. En la figura 30, se muestran los pasos que un cliente realizaría al comunicarse con un servidor mediante la modalidad de conmutación por error Warm”.



OPC UA, 4.ª parte, sección 6.6.2.4.5.3

Arquitecturas compatibles

Introducción

En este capítulo se describen las arquitecturas topológicas compatibles con el módulo de comunicación Ethernet BMENUA0100 con servidor OPC UA integrado.

Configuraciones compatibles del módulo BMENUA0100

Colocación del módulo BMENUA0100

El módulo BMENUA0100 puede colocarse en un slot Ethernet en el bastidor principal local (es decir, en el mismo bastidor que el controlador) en las siguientes configuraciones:

- Como configuración independiente de M580.
- una configuración del controlador de seguridad autónomo M580.
- Como configuración Hot Standby de M580.
- una configuración del controlador de seguridad Hot Standby M580.

NOTA:

- El módulo BMENUA0100 puede usarse con todos los controladores M580.
- Si se crea un bucle de red, el módulo BMENUA0100 entra en el estado NOCONF (no configurado). Para evitar bucles y eventos relacionados, cuando utilice el puerto de control de BMENUA0100, divida físicamente la red del puerto de control y la red de la placa de conexiones del controlador (a través de la división de cableado) y no solo de forma lógica (a través de los ajustes de subred y máscara de subred).

⚠ ADVERTENCIA

FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

No conecte el puerto de control del módulo BMENUA0100 al puerto de servicio del controlador.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

Conexión mediante el protocolo HTTPS

Si su aplicación tiene problemas de conexión, consulte al servicio de asistencia de TI local para confirmar que la configuración de su red y las políticas de seguridad sean coherentes con el acceso de HTTPS (puerto 443) a la dirección IP del módulo BMENUA0100.

El módulo BMENUA0100 acepta las conexiones HTTPS con el protocolo de seguridad de la capa de transporte (TLS) v1.2 o posteriores. Por ejemplo, Windows 7 puede necesitar una actualización para permitir que TLS 1.2 actualice el firmware del BMENUA0100 o acceda a su sitio web.

Instalación del módulo BMENUA0100 en una red plana

En el caso de tener varios bastidores M580 conectados en una sola subred (es decir, una arquitectura de red plana) que incluyan módulos BMENUA0100 con el puerto de control deshabilitado, instale cada módulo BMENUA0100 en un número de slot diferente en su correspondiente bastidor (excepto en las configuraciones Hot Standby, en las que los módulos BMENUA0100 se instalan en el mismo número de slot). Como alternativa, use un enrutador para aislar los bastidores y, así, evitar posibles conflictos de dirección entre los módulos BMENUA0100.

Adición de prefijos a nombres de dispositivos (roles) en diseños de redes planas

Cuando una arquitectura incluye varios módulos BMENUA0100 que se comunican con otros dispositivos, como controladores M580 configuradas en una misma subred, utilice prefijos para el nombre de dispositivo (o rol) de todos los dispositivos, incluidos los controladores M580. Esta nomenclatura permite diferenciar los módulos BMENUA0100 entre los controladores M580 y determinar qué controlador está ubicado en qué bastidor. Esta nomenclatura también ayuda a eliminar la incertidumbre relacionada con el diseño de una red plana. Por ejemplo, sin prefijos únicos, un módulo BMENUA0100 no puede determinar con qué controlador M580 debe comunicarse para recuperar su propia configuración después de descargar una aplicación.

El prefijo del nombre del dispositivo se puede establecer en Control Expert en la ficha **Herramientas > Ajustes del proyecto > Configuración**.

Acceso al servidor OPC UA integrado de BMENUA0100

En las arquitecturas topológicas descritas en este capítulo, el puerto de la placa de conexiones Ethernet del módulo de comunicación BMENUA0100 y su puerto de control pueden utilizarse para proporcionar acceso al servidor OPC UA integrado en el módulo. Para obtener una descripción sobre cuándo se pueden utilizar estos puertos para acceder al servidor OPC UA integrado, consulte las descripciones del puerto de control y el puerto de la placa de conexiones Ethernet en el tema [Puertos externos](#), página 23.

Número máximo de módulos BMENUA0100 por configuración

El número máximo de módulos BMENUA0100 que se admiten en una configuración M580 es:

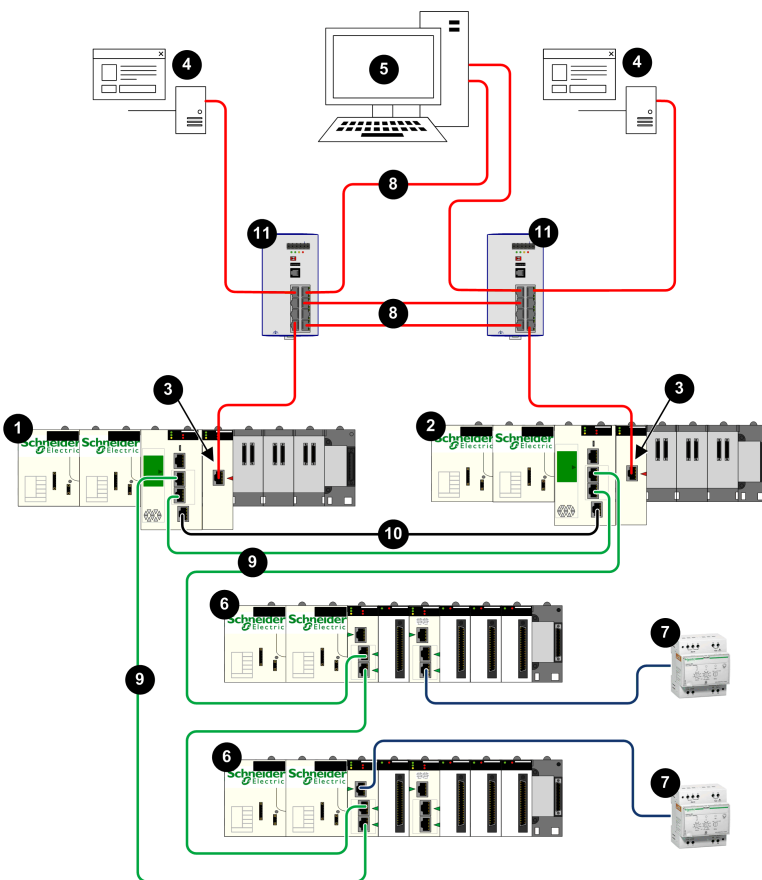
Tipo de configuración M580	Número máximo de módulos BMENUA0100
Independiente	Dos en el bastidor principal local para las configuraciones estándar y de seguridad independientes ¹ y Hot Standby ^{1,2} .
Controlador de seguridad	
Hot Standby	
Controlador de seguridad Hot Standby	
<div>1. Cuando dos módulos BMENUA0100 se utilizan en un rack principal:</div> <div><ul style="list-style-type: none">• El rendimiento de cada módulo será menor que si se hubiera usado un solo módulo.• Habilite el puerto de control en la configuración para los dos módulos.</div> <div>2. En las configuraciones Hot Standby, coloque los módulos BMENUA0100 en el mismo número de slot en los correspondientes bastidores principales locales.</div>	

Cambiar la configuración sobre la marcha (CCOTF)

El módulo BMENUA0100 no admite CCOTF.

Red de control aislada con controladores Hot Standby M580

Arquitectura



- 1** Controlador Hot Standby activo primario
- 2** Controlador Hot Standby activo estándar
- 3** Módulo de comunicaciones Ethernet BMENUA0100 con servidor OPC UA integrado
- 4** Cliente OPC UA (sistema SCADA)
- 5** Estación de trabajo de ingeniería con conexiones Ethernet duales
- 6** Estación Ethernet RIO X80
- 7** Equipo distribuido
- 8** Red de control
- 9** Anillo principal Ethernet RIO
- 10** Conexión de comunicación Hot Standby
- 11** Conmutador de anillo dual (DRS)

Descripción

Esta arquitectura proporciona conexiones redundantes a clientes OPC UA duales (sistemas SCADA). En esta arquitectura, la ciberseguridad puede estar habilitada o deshabilitada. La red de control (8) está aislada lógicamente de los dispositivos Ethernet que residen en el anillo principal Ethernet RIO (9), incluido el controlador, y de los dispositivos Ethernet distribuidos (7). Esto se consigue en la capa de red del modelo OSI mediante las direcciones IP.

El puerto de control BMENUA0100 (3), con sus pilas IPv6/IPv4 duales, permite la conectividad ascendente a la red de control. Cuando se comunica mediante IPv6, es compatible con la configuración automática de dirección sin estado (SLAAC) y con las direcciones IP fijas.

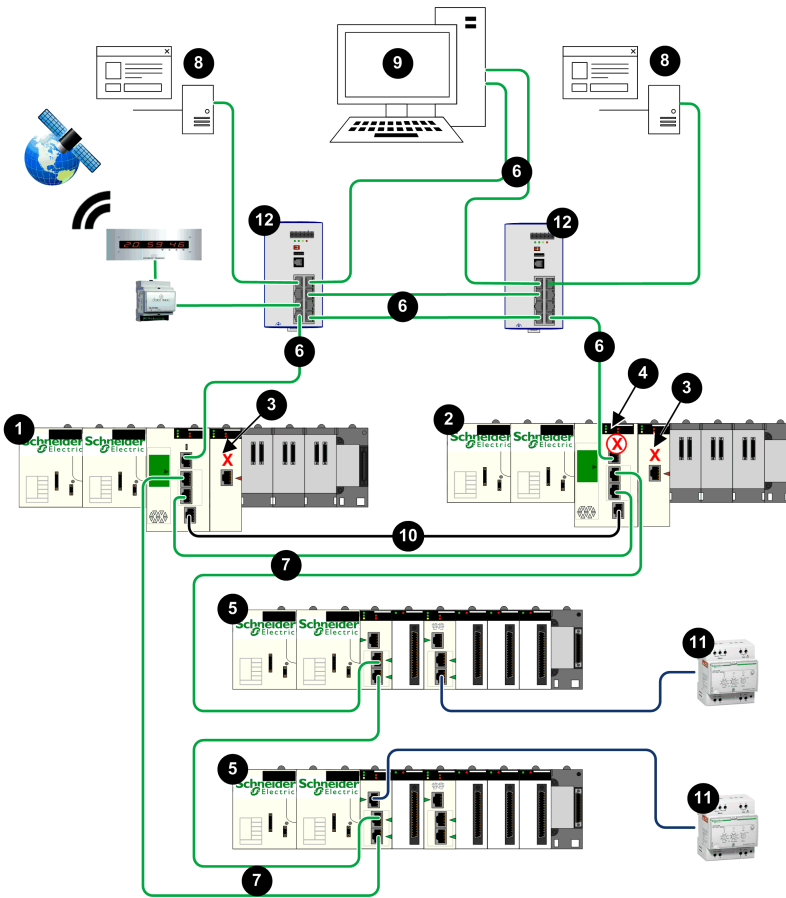
BMENUA0100 proporciona comunicación de par a par Modbus entre los dos controladores Hot Standby. Los puertos del controlador proporcionan conectividad descendente a los dispositivos Ethernet en el anillo principal Ethernet RIO.

Cada BMENUA0100 es un cliente de un servidor NTP que reside en la red de control. La conexión se establece mediante el puerto de control BMENUA0100. Los módulos BMENUA0100 funcionan también como servidores NTP para otros dispositivos en el anillo principal Ethernet RIO. En este diseño Hot Standby, el módulo BMENUA0100 configurado como actos "A" es el servidor NTP primario y el módulo BMENUA0100 configurado como actos "B" es el servidor NTP en standby. Así, se sincronizan la hora del controlador y la hora del módulo BMENUA0100.

BMENUA0100 es compatible con las marcas de tiempo de aplicación. En este proceso, los módulos con marcas de tiempo registran eventos en su búfer local. Estos eventos con marca de tiempo los consume la aplicación que se ejecuta en controlador, que convierte los datos del registro sin tratar y los almacena en un formato utilizable. Los registros con formato puede consumirlos una aplicación de supervisión, como un sistema SCADA.

Red plana no aislada con M580 Hot Standby

Arquitectura



- 1 Controlador Hot Standby activo primario
- 2 Controlador Hot Standby activo estándar
- 3 Módulo BMENUA0100 con puerto de control deshabilitado
- 4 Controlador en standby con bloqueo automático del puerto de servicio
- 5 Estación Ethernet RIO X80
- 6 Red de control
- 7 Anillo principal Ethernet RIO
- 8 Cliente OPC UA (sistema SCADA)
- 9 Estación de trabajo de ingeniería con conexiones Ethernet duales
- 10 Conexión de comunicación Hot Standby
- 11 Equipo distribuido
- 12 Conmutador de anillo dual (DRS)

Descripción

Esta arquitectura proporciona conexiones redundantes de controladores Hot Standby M580 a clientes OPC UA duales (sistemas SCADA). Su objetivo primario es proporcionar alta disponibilidad a los controladores Hot Standby. Por ese motivo, esta arquitectura presenta una red plana no aislada, que reúne la red de control y el anillo principal Ethernet RIO en una sola subred.

El puerto de control BMENUA0100 está deshabilitado. La comunicación Ethernet IPv4 con el módulo BMENUA0100 se proporciona mediante el puerto de la placa de conexiones. La comunicación ascendente de los controladores Hot Standby a los servidores SCADA se logra mediante el puerto de servicio del controlador primario. Los puertos del controlador proporcionan conectividad descendente a los dispositivos Ethernet en el anillo principal Ethernet RIO.

El puerto de servicio del controlador standby (4) se deshabilita, lo que se logra usando el software de configuración de Control Expert para seleccionar **Bloqueo automático del puerto de servicio en la CPU en standby** en la ficha **Puerto de servicio** de la configuración para las CPU primaria y en espera.

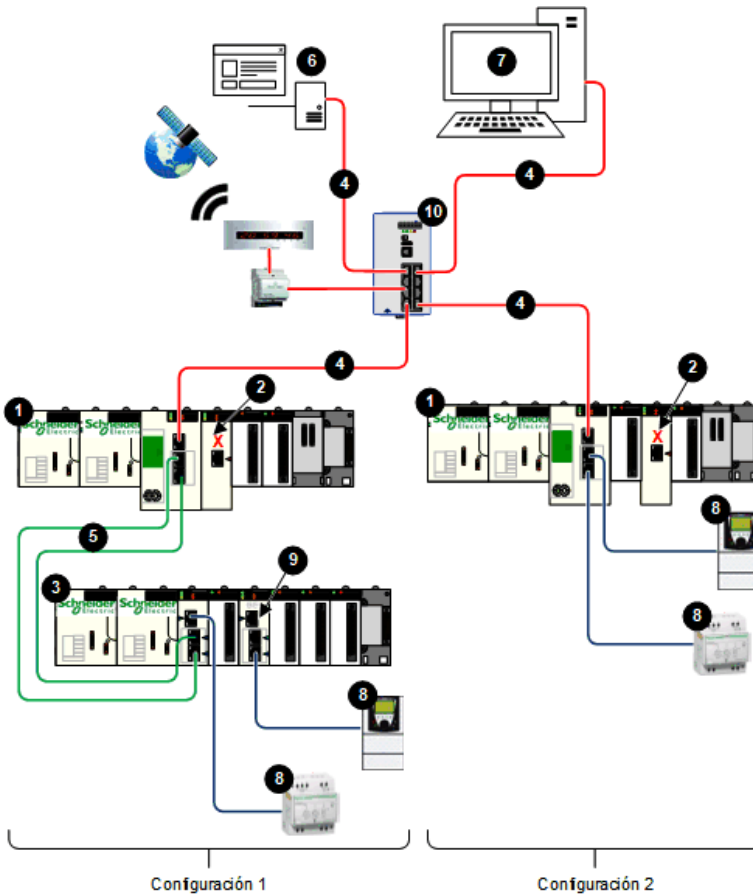
NOTA: El puerto de servicio del controlador standby se deshabilita para contribuir a prevenir la creación no intencionada de un bucle de comunicaciones Ethernet, donde la red de control y el anillo principal Ethernet RIO forman parte de la misma subred. Para obtener más información, consulte la *Guía de planificación del sistema M580 Hot Standby* y el tema Gestión de redes Ethernet planas con M580 Hot Standby (consulte *Modicon M580 Hot Standby, Guía de planificación del sistema, Arquitecturas de uso frecuente*).

En este diseño de red plana, todos los dispositivos, lo que incluye los controladores, los módulos BMECRA31310 y BMENUA0100, pueden ser clientes del mismo servidor NTP que reside en la red de control. Por ello, la hora del controlador se sincroniza con el módulo BMENUA0100.

BMENUA0100 es compatible con las marcas de tiempo de aplicación. En este proceso, los módulos con marcas de tiempo registran eventos en su búfer local. Estos eventos con marca de tiempo los consume la aplicación que se ejecuta en el controlador, que convierte los datos del registro sin tratar y los almacena en un formato utilizable. Los registros con formato puede consumirlos una aplicación de supervisión, como un sistema SCADA.

Red plana con varios controlador independientes M580 y un solo SCADA

Arquitectura



- 1** Controlador independiente
- 2** Módulo BMENUA0100 con puerto de control deshabilitado
- 3** Estación Ethernet RIO X80
- 4** Red de control
- 5** Anillo principal Ethernet RIO
- 6** Cliente OPC UA (sistema SCADA)
- 7** Estación de trabajo de ingeniería con una sola conexión Ethernet
- 8** Equipo distribuido
- 9** Conmutador del módulo BMENOS0300
- 10** Conmutador de anillo dual (DRS)

Descripción

Esta arquitectura proporciona una conexión a un solo cliente OPC UA (un sistema SCADA) desde varios controladores independientes M580. Es una arquitectura de costes optimizados que no requiere alta disponibilidad. Esta arquitectura presenta una red plana no aislada, que reúne la red de control y el anillo principal Ethernet RIO en una sola subred.

El puerto de control BMENUA0100 está deshabilitado para cada controlador independiente. La comunicación Ethernet IPv4 con el módulo BMENUA0100 se proporciona mediante el puerto de la placa de conexiones. La comunicación ascendente de cada controlador a cada servidor SCADA se logra mediante el puerto de servicio del controlador.

En la configuración 1, la conectividad descendente del controlador a la estación Ethernet RIO X80 (4) del controlador la proporcionan los puertos de red de dispositivos duales del controlador. El puerto de servicio del módulo BMECRA31310 y un conmutador BMENOS0300 (9) proporcionan más conectividad descendente al equipo Ethernet distribuido.

En la configuración 2, la conectividad descendente la proporcionan los puertos de red de dispositivos duales al equipo Ethernet distribuido.

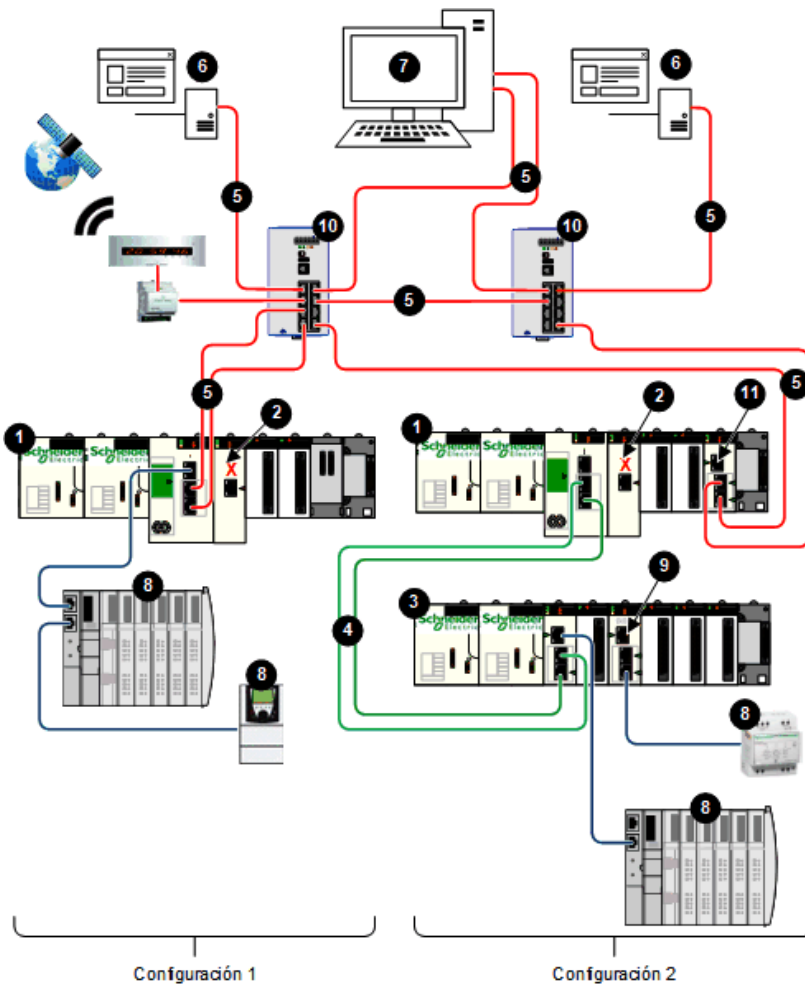
En este diseño de red plana, todos los dispositivos de red, lo que incluye los controladores, los módulos BMECRA31310 y el BMENUA0100, son clientes de un servidor NTP que reside en la red de control. Así, se sincronizan la hora del controlador y la hora del módulo BMENUA0100.

BMENUA0100 es compatible con las marcas de tiempo de aplicación. En este proceso, los módulos con marcas de tiempo registran eventos en su búfer local. Estos eventos con marca de tiempo los consume la aplicación que se ejecuta en controlador, que convierte los

datos del registro sin tratar y los almacena en un formato utilizable. Los registros con formato puede consumirlos una aplicación de supervisión, como un sistema SCADA.

Red plana con varios controlador independientes M580 y SCADA redundantes

Arquitectura



- 1** Controlador independiente
- 2** Módulo BMENUA0100 con puerto de control deshabilitado
- 3** Estación Ethernet RIO X80
- 4** Anillo principal Ethernet RIO
- 5** Red de control
- 6** Clientes OPC UA (sistemas SCADA)
- 7** Estación de trabajo de ingeniería con conexiones Ethernet duales
- 8** Equipo distribuido
- 9** Conmutador del módulo BMENOS0300
- 10** Conmutador de anillo dual (DRS)
- 11** Módulo BMENOS0300, BMENOC0301 o BMENOC0311

Descripción

Esta arquitectura proporciona alta disponibilidad de la red de control mediante conexiones redundantes entre clientes OPC UA (sistemas SCADA) y varios controladores independientes M580. Esta arquitectura presenta una red plana no aislada, que reúne la red de control y el anillo principal Ethernet RIO en una sola subred.

El puerto de control BMENUA0100 está deshabilitado para cada controlador independiente. La comunicación Ethernet IPv4 con el módulo BMENUA0100 se proporciona mediante el puerto de la placa de conexiones.

En la configuración 1, la comunicación ascendente a los servidores SCADA se logra mediante los puertos de red de dispositivos del controlador duales, usando el protocolo de redundancia RSTP para asignar roles a cada puerto con el objetivo de evitar bucles Ethernet lógicos. La conectividad descendente al equipo distribuido Ethernet la proporciona el puerto de servicio del controlador.

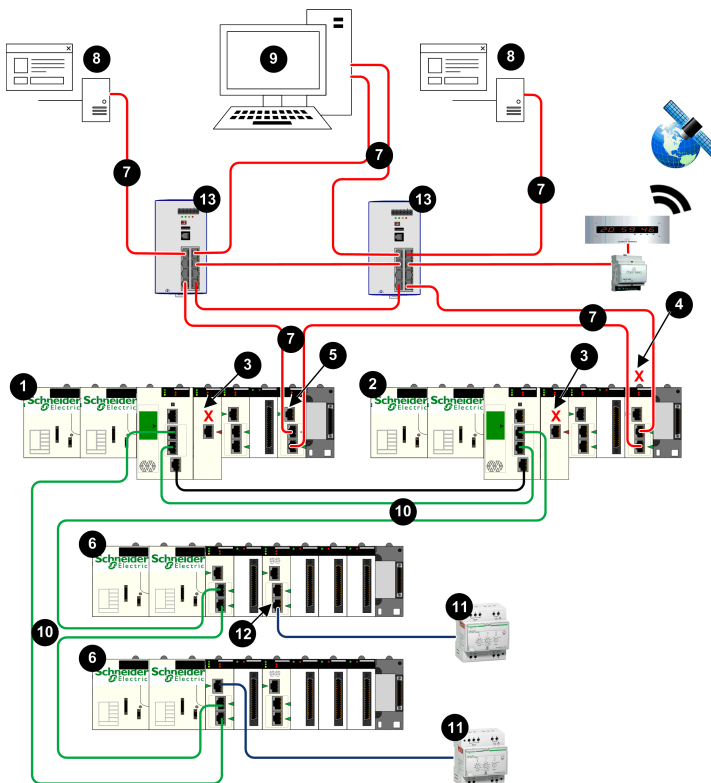
En la configuración 2, la conectividad ascendente a los servidores SCADA la proporcionan los puertos de red de dispositivos de un módulo BMENOS0300, BMENOC0301 o BMENOC0311. El protocolo de redundancia RSTP se usa para asignar roles a cada puerto con el objetivo de evitar bucles Ethernet lógicos. La conectividad descendente del controlador la proporcionan los puertos de red de dispositivos del controlador a la estación Ethernet de E/S remota X80. El puerto de servicio del módulo BMECRA31310 y un conmutador BMENOS0300 (9) proporcionan más conectividad descendente al equipo Ethernet distribuido.

En este diseño de red plana, todos los dispositivos de red, lo que incluye los controladores, los módulos BMECRA31310 y el BMENUA0100, son clientes de un servidor NTP que reside en la red de control. Así, se sincronizan la hora del controlador y la hora del módulo BMENUA0100.

BMENUA0100 es compatible con las marcas de tiempo de aplicación. En este proceso, los módulos con marcas de tiempo registran eventos en su búfer local. Estos eventos con marca de tiempo los consume la aplicación que se ejecuta en controlador, que convierte los datos del registro sin tratar y los almacena en un formato utilizable. Los registros con formato puede consumirlos una aplicación de supervisión, como un sistema SCADA.

Red plana con controladores Hot Standby M580 y SCADA redundante

Arquitectura



- 1** Controlador Hot Standby activo primario
- 2** Controlador Hot Standby activo estándar
- 3** Módulo BMENUA0100 con puerto de control deshabilitado
- 4** BMENOS0300, BMENOC0301 o BMENOC0311 con el puerto de la placa de conexiones deshabilitado
- 5** BMENOS0300, BMENOC0301 o BMENOC0311 con el puerto de la placa de conexiones habilitado
- 6** Estación Ethernet RIO X80
- 7** Red de control
- 8** Cliente OPC UA (sistema SCADA)
- 9** Estación de trabajo de ingeniería con conexiones Ethernet duales
- 10** Anillo principal Ethernet RIO
- 11** Equipo distribuido
- 12** Conmutador del módulo BMENOS0300
- 13** Conmutador de anillo dual (DRS)

Descripción

Esta arquitectura proporciona alta disponibilidad con conexiones redundantes que enlazan clientes OPC UA redundantes (sistemas SCADA) con controladores Hot Standby redundantes en una sola subred.

Cada controlador está conectado a SCADA mediante un módulo BMENOS0300, BMENOC0301 o BMENOC0311. Para evitar bucles Ethernet, se deshabilita el puerto de la placa de conexiones de uno de los módulos BMENOS0300, BMENOC0301 o BMENOC0311. En este ejemplo, el módulo del controlador en standby tiene el puerto de la placa de conexiones deshabilitado. También se usa el protocolo de redundancia RSTP para asignar roles a cada puerto con el objetivo de evitar bucles Ethernet lógicos.

El puerto de control BMENUA0100 está deshabilitado (3) para cada controlador independiente. La comunicación Ethernet IPv4 con el módulo BMENUA0100 se proporciona mediante el puerto de la placa de conexiones.

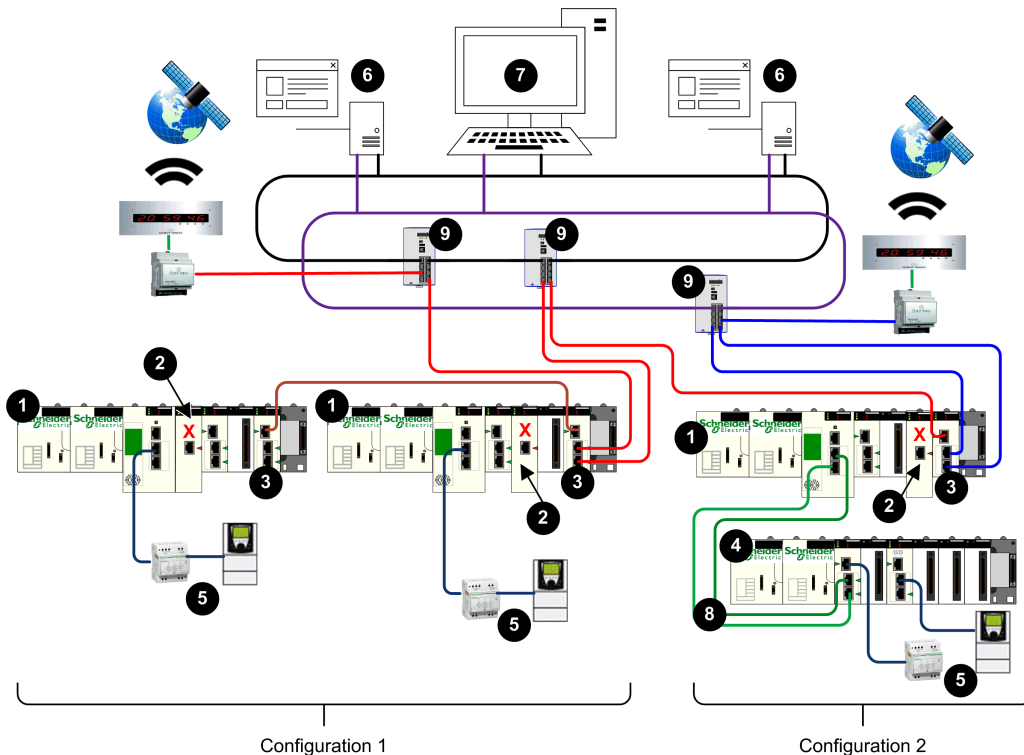
La conectividad descendente a las estaciones Ethernet RIO X80 la proporcionan los puertos de red de dispositivos del controlador. El puerto de servicio de CRA y un conmutador BMENOS0300 (12) proporcionan más conectividad descendente de las estaciones Ethernet RIO X80 al equipo Ethernet distribuido.

En este diseño de red plana, todos los dispositivos de red (lo que incluye el controlador Hot Stansby y el módulo BMENUA0100), son clientes NTP de un servidor NTP que reside en la red de control. Así, se sincronizan la hora del controlador y la hora del módulo BMENUA0100.

BMENUA0100 es compatible con las marcas de tiempo de aplicación. En este proceso, los módulos con marcas de tiempo registran eventos en su búfer local. Estos eventos con marca de tiempo los consume la aplicación que se ejecuta en el controlador, que convierte los datos del registro sin tratar y los almacena en un formato utilizable. Los registros con formato pueden consumirlos una aplicación de supervisión, como un sistema SCADA.

Red jerárquica con varios controladores independientes M580 conectados a la red de control y SCADA redundante

Arquitectura



- 1 Controlador independiente
- 2 Módulo BMENUA0100 con puerto de control deshabilitado
- 3 Módulo de comunicaciones Ethernet BMENOC0321
- 4 Estación Ethernet RIO X80
- 5 Equipo distribuido
- 6 Cliente OPC UA (sistema SCADA)
- 7 Estación de trabajo de ingeniería con conexiones Ethernet duales
- 8 Anillo principal Ethernet RIO
- 9 Conmutador de anillo dual (DRS)

Descripción

Esta arquitectura tiene una red jerárquica, que depende de módulos de comunicación BMENOC0321 para enrutar el tráfico de red entre subredes. La comunicación ascendente de los controladores a los clientes OPC UA (sistemas SCADA) se logra mediante los puertos de red de dispositivos duales del módulo BMENOC0321, usando el protocolo de redundancia RSTP para evitar bucles Ethernet lógicos.

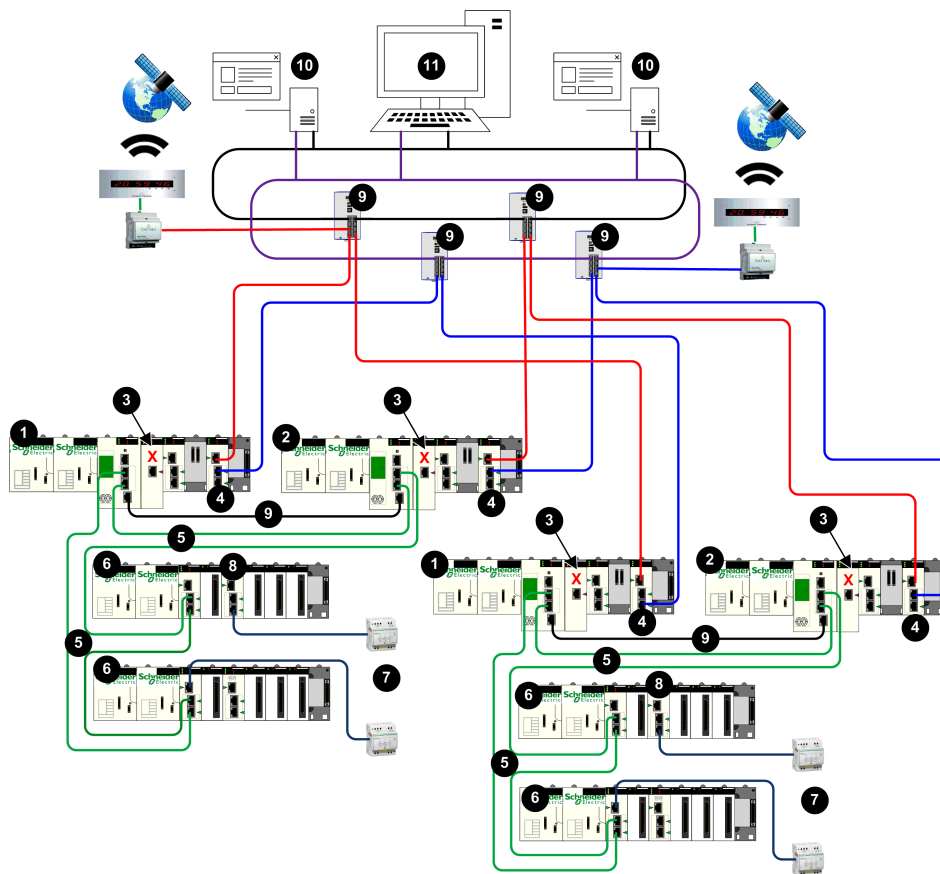
NOTA: Esta arquitectura requiere la configuración de rutas estáticas en el equipo de la red de control para redireccionar las diferentes subredes de los distintos controladores.

El puerto de control BMENUA0100 (2) está deshabilitado para cada controlador independiente. La comunicación Ethernet IPv4 con el módulo BMENUA0100 se proporciona mediante el puerto de la placa de conexiones.

La configuración 1 incluye dos controladores que residen en la misma subred. Esta configuración emplea el módulo BMENOC0321 para proporcionar comunicaciones ascendentes redundantes a los servidores SCADA redundantes. El módulo BMENOC0321 emplea el protocolo de redundancia RSTP para evitar bucles Ethernet lógicos. Los puertos de red de dispositivos duales de los dos controladores proporcionan comunicación descendente al equipo Ethernet distribuido.

La configuración 2 incluye un solo controlador, con estación Ethernet RIO X80. Este controlador usa el módulo BMENOC0321 para proporcionar comunicación ascendente a los servidores SCADA redundantes. BMENOC0321 logra esto usando dos subredes independientes. La comunicación descendente desde la estación Ethernet RIO X80 la proporcionan tanto el puerto de servicio del módulo BMECRA31310 como un BMENOS0300 cambiar a equipo Ethernet distribuido.

Arquitectura



- 1 Controlador Hot Standby activo primario
- 2 Controlador Hot Standby activo estándar
- 3 Módulo BMENUA0100 con puerto de control deshabilitado
- 4 Módulo de comunicaciones Ethernet BMENOC0321
- 5 Anillo principal Ethernet RIO
- 6 Estación Ethernet RIO X80
- 7 Equipo distribuido
- 8 Conmutador del módulo BMENOS0300
- 9 Conmutador de anillo dual (DRS)
- 10 Cliente OPC UA (sistema SCADA)
- 11 Estación de trabajo de ingeniería con conexiones Ethernet duales

Descripción

Esta arquitectura tiene una red jerárquica, que depende de módulos de comunicación BMENOC0321 (4) para enrutar el tráfico de red entre subredes. La comunicación ascendente de los controladores Hot Standby a los clientes OPC UA (sistemas SCADA) se logra mediante los puertos de red de dispositivos duales de los módulos BMENOC0321, usando el protocolo de redundancia RSTP para evitar bucles Ethernet lógicos.

NOTA: Esta arquitectura requiere la configuración de rutas estáticas en el equipo de la red de control para redireccionar las diferentes subredes de los distintos controladores.

El puerto de control BMENUA0100 (3) está deshabilitado para cada controlador. La comunicación Ethernet IPv4 con el módulo BMENUA0100 se proporciona mediante el puerto de la placa de conexiones.

Esta configuración emplea el módulo BMENOC0321 para proporcionar comunicaciones ascendentes redundantes mediante conexiones redundantes a los servidores SCADA redundantes. Los puertos de red de dispositivos duales de los controladores proporcionan comunicación descendente a las caídas de X80 Ethernet RIO. Se proporciona más comunicación descendente de la estación Ethernet RIO X80 al equipo Ethernet distribuido por parte del puerto de servicio de BMECRA31310 y un conmutador BMENOS0300 (8).

Puesta en marcha e instalación

Introducción

En este capítulo se describe cómo seleccionar una modalidad de funcionamiento e instalar el módulo de comunicaciones Ethernet BMENUA0100 con servidor OPC UA integrado.

Lista de comprobación para la puesta en marcha del módulo BMENUA0100

Lista de comprobación para la puesta en marcha

En el esquema siguiente se muestra una secuencia de las tareas que se deben seguir al poner en marcha e instalar un nuevo módulo BMENUA0100. En este ejemplo, se configura el módulo para que funcione en modalidad de PKI de autofirmado y CA con direcciones IPV6 SLAAC e IPV4:

1. Configure la aplicación, página 123 Control Expert.
2. Configure el enrutador/servidor SLAAC (para las direcciones IPV6 en modalidad SLAAC).
3. Seleccione las operaciones de modalidad Advanced (o Secured) para el módulo:

a.	Coloque el conmutador rotativo, página 25 de la parte posterior del módulo en la posición Modo Advanced (o Secured), página 32.
b.	Instale el módulo, página 88 en un slot Ethernet del bastidor.

4. Configure los ajustes de ciberseguridad mediante las páginas web, página 89 del módulo:

a.	Cree la configuración de ciberseguridad mediante la página web Configuración, página 97.
b.	Ajuste la modalidad de PKI en autofirmado y CA.
c.	Para los dispositivos cliente que no admitan PKI, cree una lista, página 117 Certificados de clientes de confianza .
d.	Aplique el archivo de configuración.

5. Lleve a cabo la inscripción manual de certificados, página 116:

a.	Genere una petición de firma de certificado (CSR).
b.	Envíe el certificado de la CA.
c.	Envíe el certificado del dispositivo.

6. Añada el certificado de la CA a los dispositivos cliente OPC UA.
7. Pruebe la comunicación entre el servidor y el cliente OPC UA.

Puesta en marcha del módulo BMENUA0100

Introducción

El módulo BMENUA0100 con servidor OPC UA integrado aparece en el catálogo de hardware de Control Expert como módulo de comunicaciones. Consume un canal de E/S.

Cuando un módulo BMENUA0100 sale de fábrica, su modalidad de funcionamiento de ciberseguridad predeterminada es la modalidad Advanced (o Secured). Para configurar el módulo nuevo para realizar operaciones de la modalidad Advanced (o Secured), siga el caso de [Puesta en marcha en la modalidad Advanced \(o Secured\)](#), página 32 expuesto a continuación.

Para cambiar la modalidad de funcionamiento de la ciberseguridad de un módulo ya configurado, incluidos los módulos nuevos que pretenda configurar para realizar operaciones de la modalidad Standard, realice una operación de [Cybersecurity Reset \(o Security Reset\)](#), página 86 en el módulo. Tras la operación de [Cybersecurity Reset \(o Security Reset\)](#), puede seguir el caso de [la Puesta en marcha en la modalidad Advanced \(o Secured\)](#), página 32 o el de [la Puesta en marcha en la modalidad Standard](#), página 32.

Puesta en marcha en modalidad Advanced (o Secured)

Para poner en marcha un módulo BMENUA0100 con el objetivo de que funcione en la modalidad Advanced (o Secured), es necesario completar dos procesos de configuración:

- Configuración de la ciberseguridad, mediante las páginas web del módulo.
- Configuración de dirección IP, cliente NTP y agente SNMP, mediante la herramienta de configuración de Control Expert.

Solo un administrador de seguridad, usando la [combinación de nombre de usuario/contraseña predeterminada](#), página 33 de la modalidad Advanced (o Secured), puede poner en marcha el módulo en la modalidad Advanced (o Secured).

NOTA: Realice estos procesos de configuración en el siguiente orden:

- Utilice Control Expert para configurar las direcciones IP del panel de control y de la placa de conexiones.
- Utilice las páginas web del módulo para configurar los parámetros de ciberseguridad.
- Utilice Control Expert para completar la configuración del cliente NTP y del agente SNMP.

NOTA: Para la puesta en marcha en modalidad Advanced (o Secured) con inscripción manual, consulte el tema *Inscripción manual*, página 116.

El procedimiento que se indica a continuación se aplica a módulos nuevos aún no configurados. Si usa un módulo configurado anteriormente, realice una *operación de Cybersecurity Reset (o Security Reset)*, página 86 antes de continuar con los pasos que se indican a continuación.

Para poner en marcha el módulo en la modalidad de funcionamiento Advanced (o Secured):

1. Configure los parámetros de la dirección IP:

a.	Abra la herramienta de configuración de Control Expert.
b.	En Control Expert, cree un Nuevo proyecto , añada un módulo BMENUA0100 al proyecto desde el Catálogo de hardware y, a continuación, configure los ajustes de la dirección IP., página 123

2. Configure los ajustes de ciberseguridad:

a.	Con el módulo fuera del bastidor, use el destornillador de plástico incluido con el módulo, página 25 para colocar el conmutador rotativo en la posición Advanced (o Secured) .
b.	Instale, página 87 el módulo en un slot Ethernet del bastidor Ethernet principal local y apague y encienda el módulo.
c.	Utilice el navegador de Internet para conectar el PC de configuración al módulo mediante el puerto de control o el puerto de la placa de conexiones y, a continuación, desplácese hasta las páginas web del módulo en la dirección IP configurada.
d.	Si su navegador muestra un mensaje, página 91 que indica un posible riesgo de seguridad, lea el mensaje y, en caso de estar de acuerdo, establezca la conexión haciendo clic en Aceptar el riesgo y continuar (o un texto similar específico del navegador).
e.	En la página de inicio de sesión del usuario, introduzca la combinación de nombre de usuario/ contraseña predeterminada, página 33.
f.	Cambie y confirme la contraseña. Consulte el tema <i>Administración de usuarios</i> , página 119 para conocer los requisitos de la contraseña. Se muestra la <i>página</i> , página 94 Inicio del módulo.
g.	Desde la página Inicio , vaya a las páginas web del módulo y configure sus ajustes de ciberseguridad.

3. Configure los ajustes del cliente NTP y el agente SNMP:

a.	Abra la herramienta de configuración de Control Expert.
b.	En Control Expert, configure los parámetros del cliente NTP y el agente SNMP., página 123
c.	Una vez completada la configuración del proyecto de Control Expert, conéctese al controlador y transfiera el proyecto al controlador.

NOTA: Cuando la configuración se carga en el módulo BMENUA0100, el estado del módulo cambia de NO CONFIGURADO a CONFIGURADO. El indicador LED **SECURE**, página 145 indica si el módulo está o no configurado y si el servidor OPC UA está conectado a un cliente OPC UA.

Puesta en marcha en la modalidad Standard

En la modalidad Standard, no es necesaria configuración de ciberseguridad. Se configuran los ajustes de dirección IP, cliente NTP y agente SNMP mediante la herramienta de configuración de Control Expert. En la modalidad Standard, el módulo empieza a comunicarse cuando se coloca en el bastidor, se enciende el módulo y recibe una configuración válida de Control Expert.

Utilice la combinación predeterminada de nombre de usuario y contraseña, página 33 para poner en marcha el módulo en modalidad Standard.

Para poner en marcha el módulo en la modalidad Standard:

- 1. Con el módulo fuera del bastidor, use el destornillador de plástico incluido con el módulo, página 25 para colocar el conmutador rotativo en la posición **Standard**.
- 2. Coloque el módulo en un slot Ethernet del bastidor Ethernet principal local y apague y encienda el módulo.
- 3. Abra la herramienta de configuración de Control Expert.
- 4. En Control Expert, cree un **Nuevo proyecto**, añada un módulo BMENUA0100 al proyecto desde el **Catálogo de hardware** y, a continuación, configure los ajustes Dirección IP, página 123, Cliente NTP, página 133 y Señal SNMP, página 136.
- 5. Una vez completada la configuración del proyecto de Control Expert, conéctese al controlador y transfiera el proyecto al controlador.

NOTA: Cuando se funcione en la modalidad Standard, el LED **SECURE** estará apagado.

Operación de Cybersecurity Reset (o Security Reset)

En módulos configurados previamente o en módulos nuevos que desee configurar para realizar operaciones de ciberseguridad, ejecute una operación de Cybersecurity Reset (o Security Reset) antes de realizar la configuración de la ciberseguridad. Una operación de restablecimiento restaura los ajustes predeterminados de la ciberseguridad. Puede realizar un restablecimiento usando las páginas web del módulo o el conmutador rotativo situado en la parte trasera del módulo.

Páginas web: En módulos BMENUA0100 configurados para realizar operaciones de la modalidad Advanced (o Secured):

1. Vaya a la página web **Administración de la configuración > RESTABLECER**.
2. Haga clic en **Restablecer**.

NOTA: La operación de Cybersecurity Reset (o Security Reset) se ha completado cuando el LED **RUN** está encendido en verde de forma fija y el LED del puerto de control **NS** y el LED del puerto de la placa de conexiones **BS** están encendidos en rojo de forma fija.

3. Apague y encienda el módulo de una de las siguientes formas:
 - Apague el bastidor del módulo y, a continuación, enciéndalo.
 - Quite físicamente el módulo del bastidor y, a continuación, insértelo de nuevo.

Ya puede realizar la puesta en marcha en la modalidad Advanced (o Secured).

Conmutador rotativo: Para cualquier módulo BMENUA0100:

1. Con el módulo fuera del bastidor, use el destornillador de plástico incluido con el módulo, página 25 para colocar el conmutador rotativo en la posición **Cybersecurity Reset**.
2. Instale, página 87 el módulo en un slot Ethernet del bastidor Ethernet principal local y apague y encienda el módulo.

NOTA: Esto restaura los ajustes predeterminados del módulo, incluida la dirección IP predeterminada del puerto de control, página 123 de 10.10.MAC5.MAC6. Cuando los dos últimos octetos de la dirección MAC (**MAC5.MAC6**) corresponden a 0.0 en la dirección predeterminada, establezca una conexión de cables punto a punto entre el equipo y el controlador, módulo de comunicación u otro módulo.

Una vez completada la operación, el LED **RUN** está encendido en verde de forma fija y el LED del puerto de control **NS** y el LED del puerto de la placa de conexiones **BS** están encendidos en rojo de forma fija. Puede apagar el módulo, quitar el módulo del bastidor y realizar la puesta en marcha en la modalidad Advanced (o Secured), página 32 o la puesta en marcha en la modalidad Standard, página 32.

Instalación del módulo BMENUA0100

Introducción

Solo es posible instalar el módulo BMENUA0100 en un bastidor principal Ethernet local colocándolo en cualquier slot Ethernet no reservado para la fuente de alimentación o el controlador.

NOTA: Si su aplicación se basa en una versión de EcoStruxure Control Expert inferior a 15.3 e incluye varios controladores (que no son controladores Hot Standby), cada uno con un módulo BMENUA0100, instale los módulos de manera que el número de ranura de cada BMENUA0100 sea único. Por ejemplo, para una aplicación que incluya dos controladores, si se coloca un módulo BMENUA0100 del bastidor del controlador 1 en la ranura 4, coloque un módulo BMENUA0100 del bastidor del controlador 2 en una ranura que no sea la ranura 4.

Precauciones para la conexión a tierra

Siga todos los códigos y normativas de seguridad locales y nacionales.

PELIGRO

DESCARGA ELÉCTRICA

Utilice equipo de protección personal (EPI) cuando trabaje con cables blindados.

Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.

La placa de conexiones para su módulo es común con la placa de toma de tierra funcional (FE) y debe montarse y conectarse a una placa de conexiones conductora conectada a tierra.

ADVERTENCIA

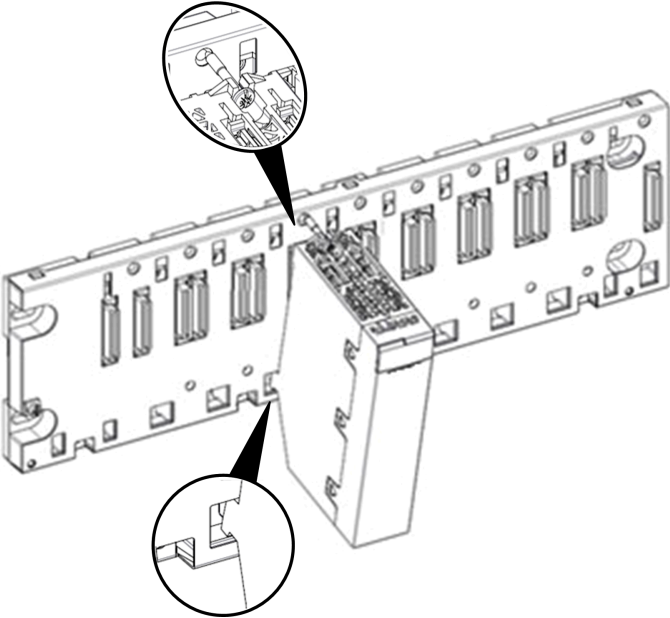
FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

Conecte la placa de conexiones a la toma de tierra funcional (FE) de la instalación.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

Instalación de un módulo BMENUA0100 en el bastidor

Un módulo BMENUA0100 requiere un solo slot Ethernet de bastidor. Puede instalar el módulo en cualquier ranura Ethernet no reservada para la fuente de alimentación o el controlador. Para instalar un módulo BMENUA0100 en un bastidor, siga estos pasos:

Paso	Acción	
1	Coloque los pins de posición que se encuentran en la parte posterior inferior del módulo en los slots correspondientes del bastidor.	
2	Inclinar el módulo hacia la parte superior del bastidor, de modo que coincida también con la parte posterior del bastidor. El módulo ahora está ahora debidamente colocado.	
3	Apriete el único tornillo de la parte superior del módulo para mantener el módulo en su sitio en el bastidor. Par de sujeción: De 0,4 a 1,5 N•m (de 0,30 a 1,10 lb-ft).	

Conexión a tierra de los módulos de E/S

Para obtener más información sobre la puesta a tierra, consulte el tema *Puesta a tierra del rack y el módulo de fuente de alimentación* en el documento *Manual de referencia de hardware para racks y fuentes de alimentación Modicon X80*.

Configuración

Introducción

En este capítulo se describe cómo configurar el módulo de comunicaciones Ethernet BMENUA0100 con servidor OPC UA integrado.

Configuración de los ajustes de ciberseguridad de BMENUA0100

Introducción

En esta sección se describe cómo usar las páginas web del módulo de comunicación Ethernet BMENUA0100 con servidor OPC UA. Use las páginas web para crear una configuración de ciberseguridad para el módulo y para ver datos de diagnóstico.

Introducción a las páginas web de BMENUA0100

Introducción

Use las páginas web del módulo BMENUA0100 para crear, gestionar y diagnosticar una configuración de ciberseguridad para el módulo, así como para ver datos de diagnóstico de OPC UA y eventos.

NOTA:

- Las páginas web del módulo BMENUA0100 admiten la comunicación HTTPS a través de los protocolos IPv4 e IPv6, página 124.
- Utilice solo versiones recientes de los navegadores de Internet para acceder a las páginas web. Algunos exploradores antiguos, como Internet Explorer v7 y versiones anteriores, no son compatibles.

NOTA: El navegador de Internet Chrome, versión 123.0.6312.123 (compilación oficial) (64 bits), se ha probado con las páginas web del módulo BMENUA0100.

Para que el módulo BMENUA0100 funcione en la modalidad Advanced (o Secured), se necesita una configuración de ciberseguridad, que debe realizarse antes de configurar con Control Expert, página 123 su dirección IP, su cliente NTP y sus ajustes SNMP. La configuración de ciberseguridad solo se puede configurar localmente para cada módulo

BMENUA0100 conectando un PC de configuración y ejecutando un navegador HTTPS para el módulo BMENUA0100:

- Puerto de control, si el puerto de control está habilitado.
- Puerto de la placa de conexiones (a través de un módulo BMENOC0301 o BMENOC0311, o el controlador) si el puerto de control está deshabilitado.

NOTA: Antes de comprobar la validez de los ajustes de ciberseguridad introducidos en las páginas web, el módulo BMENUA0100 establece primero los ajustes de dirección IP del puerto de control y el puerto de la placa de conexiones configurados en Control Expert, página 123.

Para que el módulo BMENUA0100 funcione en la modalidad Standard, los ajustes de ciberseguridad no son necesarios y no se pueden configurar.

NOTA:

- Si se usa un certificado autofirmado, algunos navegadores pueden indicar que la conexión entre el PC y el módulo es "No segura".
- Si los módulos BMENUA0100 funcionan en la modalidad Advanced (o Secured) en un sistema Hot Standby, compruebe que los ajustes de ciberseguridad del módulo BMENUA0100 en el controlador primario sean los mismos que los ajustes de ciberseguridad del módulo BMENUA0100 en el controlador Hot Standby. El sistema no realizará esta comprobación automáticamente.

La accesibilidad de las páginas web depende de la modalidad de funcionamiento de ciberseguridad:

Página web o grupo	Modalidad Advanced (o Secured)	Modalidad Standard
Home, página 94	✓	✓
Configuración (seguridad del dispositivo), página 97	✓	–
Administración de certificados, página 110	✓	–
Control de acceso, página 119	✓	–
Gestión de configuración, página 121	✓	–
Diagnóstico, página 169	✓	✓
✓: las páginas web son accesibles. –: las páginas web no son accesibles.		

Configuración inicial de los ajustes de ciberseguridad

Puede configurar los ajustes de ciberseguridad iniciales de un módulo BMENUA0100 que:

- Nunca se haya configurado y conserve su configuración predeterminada.

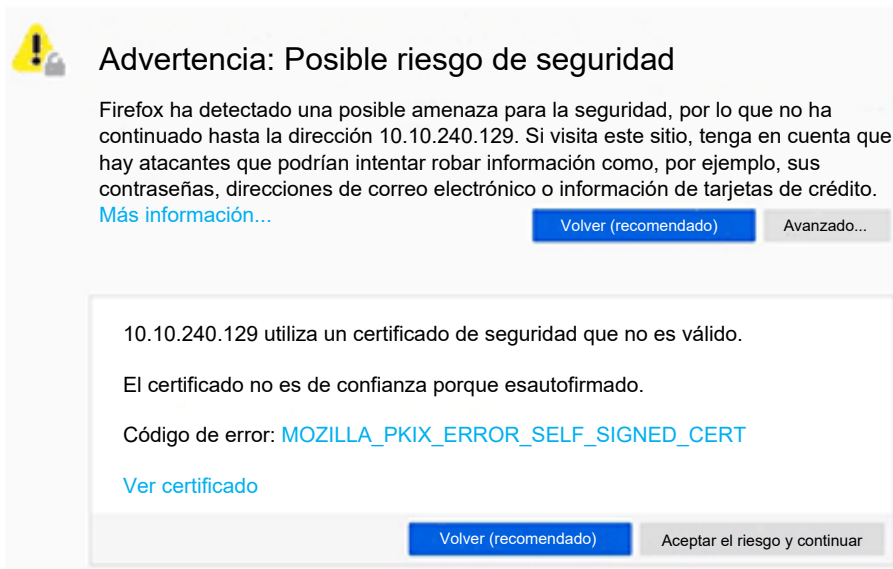
- Se haya configurado anteriormente, pero tenga su configuración predeterminada restaurada tras la ejecución del comando **Cybersecurity** (o **Security**) **Reset** , página 33.

Una vez configurados los ajustes de ciberseguridad de un módulo, cuando el módulo funciona en la modalidad **Advanced** (o **Secured**), también puede modificar los ajustes de ciberseguridad desde las páginas web.

Consulte en el **tema de puesta en marcha**, página 83 las instrucciones de aplicación de una configuración inicial al módulo.

Primer inicio de sesión en las páginas web

Cuando inicia sesión en un módulo BMENUA0100 sin configurar, aparece la pantalla siguiente (o una pantalla similar, según el navegador que esté utilizando):



A pesar de los términos utilizados en el mensaje, la conexión está protegida mediante HTTPS. Lea el mensaje y, si está de acuerdo, haga clic en **[Aceptar el riesgo y continuar]** (o un texto similar específico del navegador) para realizar el primer inicio de sesión.

NOTA: El mensaje anterior aparece porque el módulo aún no tiene una configuración válida y usa un certificado autofirmado.

Inicio de sesión en las páginas web

En el primer inicio de sesión, el administrador de seguridad introduce la combinación de nombre de usuario y contraseña, página 33 predeterminada. Inmediatamente después, se solicita al administrador que cambie la contraseña predeterminada.

Debe iniciar sesión cada vez que abra las páginas web del módulo BMENUA0100. Solo podrán acceder a las páginas web del módulo las personas que tengan asignada una cuenta de usuario válida, con una combinación válida de nombre de usuario y contraseña creada por un administrador de seguridad en la página web > **Control de acceso** Administración de usuarios Control de acceso, página 119.

En la página de inicio de sesión, seleccione un idioma en la lista desplegable y, a continuación, introduzca su **Nombre de usuario** y **Contraseña**.



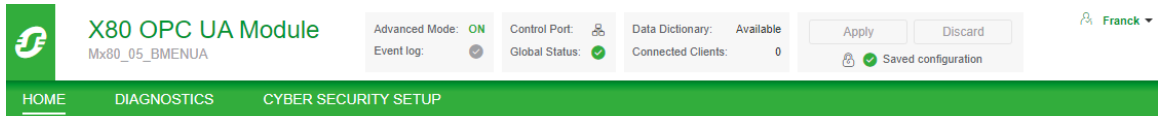
Se prohíbe el uso no autorizado del sistema, que quedará sujeto a sanciones penales o civiles. Esta aplicación está protegida por la ley de derechos de autor y por tratados internacionales. © 2019 Schneider Electric Industries SAS. Todos los derechos reservados.

NOTA: La modalidad de funcionamiento de la ciberseguridad del módulo la muestra el icono de candado de la parte superior derecha del cuadro de diálogo (indicado por la flecha roja, arriba). Si el candado está:

- Cerrado (como se muestra arriba): el módulo funciona en modalidad Advanced (o Secured), página 32.
- Abierto: el módulo funciona en modalidad Standard, página 32.

Banner de la página web

Cada página web presenta un banner en la parte superior:



El banner presenta la siguiente información sobre el módulo BMENUA0100:

- Modalidad Advanced (o Secured):
 - Encendido: el módulo funciona en Modalidad Advanced (o Secured), página 32.
 - Desactivado: el módulo funciona en modalidad Standard, página 32.
- Registro de eventos:
 - El servicio de registro de eventos está deshabilitado.
 - El servicio de registro de eventos está habilitado; se puede establecer conexión con el servidor de registro.
 - El servicio de registro de eventos está habilitado, pero no se puede establecer conexión con el servidor de registro.
 - El servicio de registro de eventos está habilitado, pero se ha detectado un error.
- Puerto de control:
 - El puerto de control está habilitado.
 - El puerto de control está deshabilitado.
- Estado global:
 - Todos los servicios están operativos.
 - Al menos un servicio no está operativo.
- Diccionario de datos:
 - Disponible: la función de diccionario de datos está disponible.
 - No disponible: la función de diccionario de datos no está disponible o no está habilitada.
- Clientes conectados: número de clientes OPC UA.

- Aplicar/rechazar configuración: indica el estado de la configuración de la página web de ciberseguridad del módulo en cuestión:
 -  Configuración sin cambios: la configuración de ciberseguridad no contiene ediciones pendientes o no válidas. Los botones **Aplicar** y **Rechazar** están deshabilitados.
 -  Configuración pendiente: uno o más cambios de la configuración de ciberseguridad aún no se han aplicado. Ambos: los comandos **Aplicar** y **Rechazar** están habilitados.
 -  Configuración no válida: la configuración de ciberseguridad está incompleta o es incorrecta. El botón **Aplicar** está deshabilitado; el botón **Rechazar** está habilitado. En este estado, la página web muestra, junto a cada elemento del menú afectado, un círculo rojo que contiene el número de ajustes de la configuración no válidos a los que se puede acceder desde esa ruta de acceso de menú. Cuando va a una página con un ajuste de la configuración no válido, la página muestra el ajuste de configuración no válido.

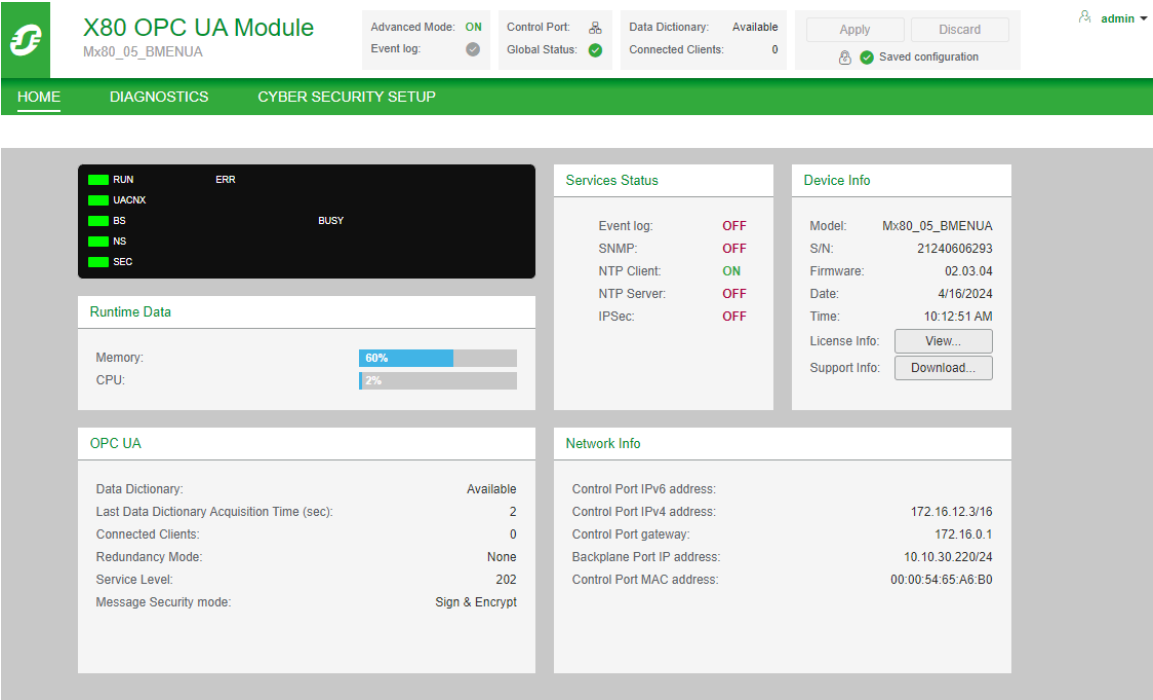
Ayuda de las páginas web

Muchas páginas web ofrecen ayuda contextual a nivel de parámetro. Para obtener ayuda sobre un parámetro o un campo específicos, coloque el cursor sobre el icono .

Página de inicio

Introducción a la página de inicio

Al iniciar sesión en las páginas web del módulo BMENUA0100, se abre la página **Inicio** de forma predeterminada. Si la configuración del módulo es válida, aparece la página siguiente:



Utilice la página **Inicio** para:

- Acceder al árbol de navegación, que contiene enlaces a las páginas web del módulo BMENUA0100. Cuando el módulo funciona en:
 - Modalidad Advanced (o Secured), página 32, los menús DIAGNÓSTICOS y CONFIGURACIÓN DE LOS AJUSTES DE CIBERSEGURIDAD se muestran y están accesibles para el administrador de seguridad.
 - Modalidad Standard, página 32, solo está accesible el menú DIAGNÓSTICOS.
- Mostrar el estado, página 141 de los LED del módulo, página 26.
- Mostrar colecciones de datos del módulo, como:
 - Datos en tiempo de ejecución, página 96
 - OPC UA, página 96
 - Estado de los servicios, página 96
 - Información de red, página 97
 - Información del dispositivo, página 97

NOTA: Cuando el conmutador rotativo de la parte trasera del módulo está colocado en la posición Cybersecurity (o Security) Reset, página 33, no puede haber comunicación con el módulo. Por eso, no se puede acceder a las páginas web (incluida la página **Inicio**).

Datos en tiempo de ejecución

El área **OPC UA** muestra:

- **Memoria:** Porcentaje de RAM interna utilizado por el servidor OPC UA (MEM_USED_PERCENT).
- **CPU:** Porcentaje de la capacidad de procesamiento de la CPU utilizado actualmente (CPU_USED_PERCENT).

NOTA: Los elementos descritos anteriormente están basados en elementos de los DDT, página 147 de T_BMENUA0100.

OPC UA

El área **Datos de ejecución** muestra:

- **Diccionario de datos:** Estado de disponibilidad del diccionario de datos (DATA_DICT).
- **Último tiempo de adquisición del diccionario de datos (s):** Duración de la última adquisición del diccionario de datos (DATA_DICT_ACQ_DURATION).
- **Clientes conectados:** Número de clientes OPC UA conectados (CONNECTED_CLIENTS).
- **Modalidad de redundancia:** Modalidad de conmutación por error compatible con un sistema Hot Standby (REDUNDANCY_MODE).
- **Nivel de servicio:** El estado del servidor OPC UA, en función de la calidad del servicio y los datos (SERVICE_LEVEL).

NOTA: Los cinco elementos descritos anteriormente están basados en elementos de los DDT, página 147 de T_BMENUA0100.

- **Modalidad de seguridad de mensajes:** Ajuste configurado en la página web de OPC UA, página 108: Ninguno, Firmar o Firmar y cifrar.

Estado de los servicios

El área **Estado de los servicios** muestra el estado (habilitado [Activado] o deshabilitado [Desactivado]) de los siguientes servicios, como se indica en los DDT, página 147:

- **Registro de eventos** (EVENT_LOG_SERVICE)
- **SNMP** (SNMP_SERVICE)
- **Cliente NTP** (NTP_CLIENT_SERVICE)
- **Servidor NTP** (NTP_SERVER_SERVICE)
- **IPSec** (IPSEC)

Para los módulos de versiones anteriores a la BMENUA0100.2.

- **Flujos de datos de Control Expert** (CONTROLIL_EXPERT_IP_FORWARDING)
- **Flujos de datos de CPU a CPU** (CPU_TO_CPU_IP_FORWARDING)

Información de red

En esta área se muestran los ajustes de configuración del módulo BMENUA0100 introducidos en **Control Expert**, página 123 y notificados en el DDT, página 147 de T_BMENUA0100, incluidos los siguientes:

- puerto de control (CONTROL_PORT_IPV6, CONTROL_PORT_IPV4 y CONTROL_PORT_GTW)
- puerto de la placa de conexiones (ETH_BKP_PORT_IPV4)
- dirección MAC del módulo (valor hexadecimal único asignado a cada módulo de forma predeterminada).

Información del dispositivo

Esta área muestra la referencia, el número de serie, la versión del firmware (FW_VERSION en los DDT, página 147 de T_BMENUA0100), la fecha y la hora del módulo BMENUA0100.

Haga clic en **Ver...** para ver la información de licencia.

Haga clic en **Descargar...** para ver el cuadro de diálogo **Descargar información de soporte**. Para obtener más información, consulte el tema **Control de acceso**, página 119.

Configuración

Configuración

En las páginas web del módulo BMENUA0100, comenzando en la página de **inicio**, seleccione **Configuración** para mostrar los enlaces a las siguientes páginas de configuración, donde podrá especificar los parámetros de seguridad del dispositivo:

- Política de cuenta de usuario, página 98
- Registros de eventos, página 99
- Servicios de red, página 99
- Reenvío de servicios, página 102
- IPsec, página 106
- SNMP, página 107

- OPC UA, página 108
- Banner de seguridad, página 110

A continuación se describen los parámetros configurables de cada nodo.

Use estos ajustes para configurar la seguridad del dispositivo para el módulo BMENUA0100. Después de cambiar la configuración, seleccione **Enviar** o **Cancelar**.

Política de cuenta de usuario

Utilice estos ajustes para configurar la política de cuenta de usuario:

Parámetro	Descripción
Tiempo máximo de inactividad de la sesión (minutos)	Período de tiempo de espera de sesión inactiva para las conexiones HTTPS. Si una conexión está inactiva durante este período, la sesión del usuario se cierra automáticamente. Valor predeterminado = 15 minutos. NOTA: No existe tiempo de espera del período de inactividad para las conexiones OPC UA.
Número máximo de intentos de inicio de sesión	El número de intentos de inicio de sesión fallidos permitidos. Valor predeterminado = 5 intentos. Cuando se alcanza el valor máximo configurado, la cuenta de usuario queda bloqueada.
Temporizador de intento de inicio de sesión (minutos)	Período máximo de tiempo para iniciar sesión. Valor predeterminado = 3 minutos.
Tiempo de bloqueo de la cuenta (minutos)	Período durante el cual no se pueden intentar otros inicios de sesión después de alcanzar el número máximo de intentos de inicio de sesión. Cuando vence este período, se desbloquea automáticamente la cuenta de usuario bloqueada. Valor predeterminado = 4 minutos.

NOTA: Esta configuración de la política de cuentas de usuario se aplica a los clientes OPC UA, página 177 a los que se ha asignado un nombre de usuario.

Registros de eventos

Utilice estos ajustes para configurar el cliente Syslog que reside en el módulo BMENUA0100. Los registros se almacenan localmente en el módulo y se intercambian con un servidor syslog, página 163 remoto:

Parámetro	Descripción
Activación del servicio	Enciende y apaga el servicio de cliente Syslog. Valor predeterminado = apagar.
Dirección IP del servidor Syslog	Dirección IPv4 o IPv6 del servidor Syslog remoto. NOTA: IPv6 está disponible para la versión del firmware 1.10 y posteriores del módulo BMENUA0100.
Puerto del servidor Syslog	Número de puerto utilizado por el servicio de cliente Syslog. Valor predeterminado = 601.

Activación de servicios de red

Estos servicios juntos constituyen un cortafuegos que permite o rechaza el paso de comunicaciones a través del módulo BMENUA0100. Utilice estos ajustes para habilitar o deshabilitar los siguientes servicios:

POLÍTICA GLOBAL:

Servicio	Descripción
Aplicar seguridad	Deshabilita los servicios de red, excepto IPsec.
Desbloquear seguridad	Habilita los servicios de red, excepto IPsec.

ACTIVACIÓN DE SERVICIOS DE RED: La configuración predeterminada para los siguientes servicios depende de la modalidad de funcionamiento de ciberseguridad (mod. func. CS), de la siguiente manera:

Servicio	Descripción	Valor predeterminado de mod. func. CS	
		Standard	Advanced (o Secured)
Agente SNMP	Habilita y deshabilita las comunicaciones del agente SNMP.	Activado	Deshabilitado
Servidor NTP	Habilita y deshabilita las comunicaciones del servidor NTP.	Activado	Desactivado
IPsec	Habilita y deshabilita las comunicaciones IPsec.	Desactivado	Habilitado ¹

Servicio	Descripción	Valor predeterminado de mod. func. CS	
		Standard	Advanced (o Secured)
Flujos de datos de controlador a controlador ^{2, 3}	Habilita y deshabilita las comunicaciones Modbus, pasando por el módulo BMENUA0100, entre los controladores M580. <i>Consulte Configuración de la comunicación para flujos de datos de controlador a controlador, página 102.</i>	Activado	Desactivado
Solo flujos de datos de Control Expert al controlador ^{2, 3}	Habilita y deshabilita las comunicaciones Modbus, EtherNet/IP, Ping, mensajes explícitos y FTP únicamente entre el software de configuración Control Expert y el controlador, pasando por el módulo BMENUA0100. <i>Consulte la sección Configuración de la comunicación para el flujo de datos de Control Expert, página 101.</i>	Activado	Desactivado
Flujos de datos de Control Expert a la red de dispositivos ^{2, 3}	Habilita y deshabilita las comunicaciones Modbus, EtherNet/IP, Ping, mensajes explícitos y FTP entre el software de configuración Control Expert y los dispositivos de red, incluido el controlador, pasando por el módulo BMENUA0100. <i>Consulte la sección Configuración de la comunicación para el flujo de datos de Control Expert, página 101.</i>	Activado	Desactivado
HTTPS en el puerto de control	Habilita y deshabilita las comunicaciones HTTPS a través del puerto de control. NOTA: Si HTTPS está deshabilitado y se aplica el cambio, no se podrá acceder a las páginas web a través del puerto de control. Para recuperar el acceso a las páginas web desde el puerto de control, restablezca la configuración de ciberseguridad.	Desactivado	Activado
<p>1. IPsec está habilitado sin reglas definidas. Es necesario configurar el servicio.</p> <p>2. Consulte el tema de solución de problemas <i>Activación de los servicios de red mediante una única conexión IPv6, página 178</i> para obtener información sobre el diseño de la configuración.</p> <p>3. Compatible únicamente con módulos de una versión anterior a BMENUA0100.2, como se indica en EcoStruxure Control Expert.</p>			

NOTA: Los servicios SNMP, NTP, Syslog y Modbus no son protocolos inherentemente seguros. Pasan a ser seguros cuando se encapsulan dentro de IPsec. No deshabilite IPsec si alguno de los servicios SNMP, NTP, Modbus o Syslog está habilitado.

Configuración de la comunicación para el software remoto que se ejecuta en los PC (no se utiliza el reenvío de NAT)

El software se dirige al dispositivo de destino (por ejemplo, el controlador M580) con la dirección IP del dispositivo de destino. Para respaldar esta comunicación, configure dos pasarelas predeterminadas, de la siguiente manera:

- En el PC host que ejecuta el software, con IPv4, configure una pasarela predeterminada del PC a la dirección IP del puerto de control del módulo BMENUA0100.
- En el dispositivo de destino (por ejemplo, el controlador M580), con IPv4, configure una pasarela predeterminada del dispositivo a la dirección IP del puerto de control del módulo BMENUA0100.
- En el PC host, añada una ruta con el siguiente comando:

```
route ADD <<destination=subnet of the target device>> MASK <<subnet  
mask of the target device>> <<gateway=BMENUA0100 module backplane  
port IP address>>
```

Para IPv4 en todas las versiones del firmware y para IPv6 en las versiones 1.10 y posteriores del firmware, las comunicaciones Modbus de la pantalla Conectar de Control Expert se dirigen a la dirección IP del puerto de control del módulo BMENUA0100. No se necesitan pasarelas para esta comunicación.

Configuración de la comunicación para flujos de datos de controlador a controlador

Las comunicaciones Modbus TCP/IP de controlador a controlador a través del módulo BMENUA0100 pueden utilizar la dirección del puerto de control IPv4 o IPv6 del módulo BMENUA0100, y no la dirección del controlador de destino.

NOTA:

- Para BMENUA0100, el reenvío de controlador a controlador está limitado al protocolo Modbus TCP/IP.
- El protocolo Modbus es el único protocolo compatible con la comunicación entre dispositivos.
- Las direcciones IPv4 admiten flujos de datos de controlador a controlador Modbus TCP/IP en las modalidades Advanced/Secured y Standard.
- Las direcciones IPv6 admiten flujos de datos de controlador a controlador Modbus TCP/IP para BMENUA0100 en la modalidad Advanced/Secured como se indica a continuación:
 - En las versiones de firmware 2.04 o superiores, si se define una regla de reenvío en la [página web Reenvío de servicios \(reenvío de IP\)](#), página 102 o si en **Reenviar todo** se selecciona **ACTIVADO**.
 - En las versiones de firmware 2.0x anteriores a 2.04, si se ha definido una regla de reenvío.

Si desea más información, consulte el tema [Funciones compatibles con las modalidades de funcionamiento Advanced \(o Secured\) y Standard](#), página 34.

Reenvío de servicios (reenvío de IP)

Los módulos BMENUA0100 con una versión 2.01 o posterior del firmware incluyen esta página web. Utilícela para configurar el reenvío de flujos de datos de unidifusión que pasan por el módulo entre la red de control y la red de dispositivos. En esta página web puede crear, editar o eliminar una lista de reglas de reenvío de IP para el módulo.

NOTA: La función de Reenvío de servicios (reenvío de IP) no admite las siguientes funciones:

- Flujos de datos de multidifusión.
- Mensajería implícita EtherNet/IP.

En consecuencia, este servicio no admite las siguientes tareas:

- Detección de dispositivos mediante la herramienta EcoStruxure Automation Device Maintenance (EADM) en modalidad de detección automática. Se admite la detección de dispositivos de EADM mediante la modalidad de detección manual (multidifusión).
- Reenvío de mensajes a los módulos de comunicación EtherNet/IP locales del controlador (mensajería implícita EtherNet/IP).

Características:

Las características principales de la función de reenvío de servicios/IP son:

- Capacidad para reenviar todos los flujos de datos ("Reenviar todo").
- Reenvío de IP de los protocolos más comunes utilizados en la arquitectura a través de plantillas predefinidas (por ejemplo: Modbus, HTTPS, SNMP, etc.)
- Creación y aplicación de plantillas de reenvío de IP personalizadas.
- Reenvío de NAT (Traducción de direcciones de red) de algunos protocolos al controlador local si la dirección IP @remote es el puerto de control IPv4 de BMENUA0100

NOTA: El reenvío de NAT se aplica a los siguientes protocolos: Modbus, Modbus sobre TLS, EtherNet/IP explícito, EIP explícito sobre TLS, EIP implícito, cliente OPC UA.

- La opción de utilizar o no utilizar IPsec para los protocolos reenviados por NAT. Consulte las directrices establecidas en las notas al final de la [sección de IPsec a continuación](#), página 106.

NOTA:

- Si hay varios módulos BMENUA0100 en un mismo bastidor, configure un solo BMENUA0100 con la función de reenvío.
- Los flujos de datos de multidifusión no se reenvían.
- Una actualización en línea de las reglas de reenvío de IP puede hacer que algunas comunicaciones activas se detengan.
- Para que el Reenvío de servicios (reenvío de IP) funcione, la red IP de destino debe ser diferente de la red IP de origen. Por ejemplo, no es posible ejecutar el reenvío de IP entre:
 - Una red IP de origen 192.168.x.x (máscara 255.255.0.0) y
 - Una red IP de destino 192.168.x.x (máscara 255.255.0.0).
- El valor del puerto de escucha OPC UA debe ser el mismo para todos los módulos BMENUA0100 que se comunican entre sí (por ejemplo, en el caso del reenvío de NAT de OPC UA entre varios módulos BMENUA0100).
- La activación del protocolo FTP abre un rango de puertos TCP, de 1024 a 65535. En consecuencia, también se pueden reenviar otros protocolos con puertos TCP en este rango. Habilite el reenvío del protocolo FTP solo temporalmente y cuando sea necesario.
 - La activación del protocolo TFTP como una regla personalizada provoca el mismo resultado que la activación del protocolo FTP. Habilite el reenvío del protocolo TFTP solo temporalmente y cuando sea necesario.

Consulte los siguientes temas para obtener más información sobre las arquitecturas de Reenvío de servicios (IP):

- [Arquitecturas compatibles con el reenvío de servicios \(IP\)](#), página 184
- [Arquitecturas no compatibles con el reenvío de servicios \(IP\)](#), página 187

Reenvío de IP y comunicación OPC UA

Tanto el reenvío de IP como OPC UA compiten por el ancho de banda de comunicación disponible del módulo BMENUA0100. Para obtener los resultados de las pruebas de rendimiento en los que se describen el impacto en el ancho de banda de la función de Reenvío de IP, las comunicaciones OPC UA, la configuración de confidencialidad y las reglas personalizadas, consulte el capítulo [Reenvío de IP y comunicación OPC UA](#), página 188.

Creación de reglas:

- Para documentar reglas predefinidas y reglas personalizadas, haga clic en **Nuevo reenvío** y complete los parámetros de definición de la regla en cuestión.

NOTA: Al seleccionar un nombre de servicio, el número de puerto y el protocolo se asignan automáticamente a sus valores predeterminados, que pueden editarse según se requiera.

- Para editar una regla existente, haga clic en el icono del lápiz y edite sus ajustes.

- Para eliminar una regla existente, haga clic en el icono del cubo de basura.

Ajuste **Reenviar todo** en **Desactivado** para aplicar las reglas enumeradas. Si ajusta **Reenviar todo** en **Activado**:

- Las reglas se suspenden y el módulo reenvía todos los protocolos.
- No puede configurar el reenvío para servicios individuales.
- Todos los servicios se reenviarán a través de IPsec si este último está habilitado.

Cada regla está definida por los siguientes campos:

Ajuste	Descripción
Nombre de servicio	<div>Los siguientes servicios están predefinidos:</div> <ul style="list-style-type: none">• Modbus• FTP• EIP explícito• ICMP• NTP/SNTP• SNMP• Captura SNMP• HTTPS• Modbus sobre TLS• EIP explícito sobre TLS• LDAP de inicio de TLS• Syslog• HTTP• Metadatos de DPWS• OPC UA (para clientes OPC UA)• DNP3• DNP3 sobre TLS• IEC 60870• IEC 60870 sobre TLS• EIP implícito <div>NOTA: Para OPC UA, el número de puerto es el puerto OPC UA configurado en Control Expert para el módulo BMENUA0100.</div>
Número de puerto ¹	Puerto asociado con el servicio.
Protocolo ¹	Protocolo asociado con el servicio.

Ajuste	Descripción
Uso de IPsec	<ul style="list-style-type: none">• TRUE : el protocolo se transporta por IPsec.• FALSE: el protocolo no se transporta por IPsec, aunque IPsec esté activado en la configuración. <p>Esta opción solo está disponible cuando IPsec está habilitado.</p> <p>NOTA:</p> <ul style="list-style-type: none">• No utilice IPsec para protocolos seguros de manera nativa (por ejemplo, Modbus sobre TLS, EIP explícito sobre TLS, DNP3 sobre TLS o EIP 60870 sobre TLS)• Utilice IPsec para protocolos seguros no de manera nativa (por ejemplo, Modbus, EIP explícito, cliente OPC UA o EIP IO)
Interfaz de entrada	<ul style="list-style-type: none">• Puerto de control: si se recibe la petición del cliente remoto en el puerto de control (por ejemplo: la solicitud Modbus TCP/IP procedente de Control Expert).• Puerto de la placa de conexiones: si la petición del cliente remoto se recibe en el puerto de la placa de conexiones (por ejemplo, la petición Modbus TCP procedente de un bloque de funciones del controlador).• Ambos: si la solicitud de cliente remoto se recibe en el puerto de la placa de conexiones y el de control (por ejemplo: la petición Modbus TCP/IP procedente de Control Expert y la petición Modbus TCP procedente de un bloque de funciones del controlador).
1. Se rellena automáticamente, aunque puede editarse, para nombres de servicio predefinidos.	

IPsec

Utilice IPsec para proteger la comunicación Ethernet IPv4.

NOTA: IPsec no es compatible con el direccionamiento IPv6.

Utilice estos parámetros para configurar un máximo de 8 canales IKE/IPsec sobre IPv4 para el módulo BMENUA0100. Si se configuran más de 4 conexiones IPsec, es posible que la conexión automática al controlador tras la transferencia a través del módulo BMENUA0100 no se realice correctamente. En ese caso, conecte el controlador manualmente.

Parámetro	Descripción
SERVICIO IPsec	<ul style="list-style-type: none">• Activado: Habilita el servicio IPsec. <p>NOTA: Como condición previa para habilitar el servicio IPsec, también debe habilitar el puerto de control en los ajustes de IPConfig, página 124.</p> <ul style="list-style-type: none">• Apagado: Deshabilita el servicio IPsec.
NTP autorizado fuera de IPsec	<ul style="list-style-type: none">• Sin seleccionar (deshabilitado): NTP solo se intercambia a través de IPsec.• Seleccionado (habilitado): NTP se intercambia a través de IPsec si se abre el canal IPsec y fuera de IPsec si no se abre el canal IPsec.
Nueva conexión	<p>Crea un nuevo canal IKE/IPsec y lo añade a la lista para su edición.</p> <p>NOTA: Se admite un máximo de 8 canales IKE/IPsec.</p>

Parámetro	Descripción
Para cada canal IKE/IPsec, configure los siguientes parámetros:	
Dirección IP remota	Dirección IPv4 del terminal de IPsec remoto. NOTA: Es necesario tener acceso al dispositivo remoto desde el puerto de control del módulo BMENUA0100 (y no desde el puerto de la placa de conexiones del módulo BMENUA0100).
Confidencialidad	<ul style="list-style-type: none">• Seleccionado: Se cifra la comunicación.• Sin seleccionar: Sin cifrado. NOTA: La confidencialidad se deshabilita si está habilitado <i>NTP sin IPsec</i> .
Tipo de cliente	Tipo de terminal IPsec remoto: Windows o Dispositivo. NOTA: El valor predeterminado es Windows. Verifique que el tipo de punto final configurado coincida con el cliente.
PSK	Clave precompartida de 32 caracteres hexadecimales, resultado de un número aleatorio generado por el módulo BMENUA0100. Puede copiarse y editarse en esta página web. NOTA: PSK se deshabilita si está habilitado <i>NTP sin IPsec</i> .

NOTA: Para configurar los parámetros del firewall de Windows, página 190, descargue el "script de Windows" del módulo BMENUA0100 por medio del comando **Descargar script** de cada dirección IP remota. Si se cambia la configuración de **Uso de IPsec** para algunos protocolos, el script de Windows deberá descargarse nuevamente desde el módulo BMENUA0100 y ejecutarse en Windows. Para obtener un ejemplo del script de Windows, consulte el tema **Scripts de Windows para IPsec**, página 190.

NOTA: Si configura 8 túneles IPsec, es posible que no pueda volver a conectarse automáticamente al controlador después de descargar una aplicación. En este caso, vuelva a conectarse manualmente al controlador después de la descarga.

NOTA: Si el servicio IPsec está activado (es decir, se establece en ON):

- El flujo de datos del servidor HTTPS local va fuera de IPsec.
- El flujo de datos de OPC UA local se lleva a cabo de forma predeterminada dentro de IPsec. Para llevar el flujo de datos de OPC UA local fuera de IPsec, se debe establecer una regla de reenvío de OPC UA con "Uso de IPsec = FALSE", aunque no haya necesidad de reenviar el flujo de datos de OPC UA.

SNMP

Utilice estos parámetros para configurar la versión SNMP y los ajustes relacionados.

NOTA: En la modalidad Advanced (o Secured), la versión de SNMP debe configurarse de la misma manera tanto en **Control Expert**, página 138 como en la página web de SNMP. Si estas configuraciones no son idénticas, el servicio SNMP no se inicia.

Parámetro	Descripción
Versión de SNMP	<ul style="list-style-type: none">v1v3
Nivel de seguridad	<p>Para SNMP v1 y v3:</p> <ul style="list-style-type: none">SinAutSinPriv: Comunicación sin autenticación o privacidad. NOTA: Para SNMP v1, se trata de la única configuración disponible. <p>Solo para SNMP v3:</p> <ul style="list-style-type: none">AutSinPriv: Comunicación con autenticación pero sin privacidad. El protocolo de autenticación es SHA (Secure Hash Algorithm, algoritmo hash seguro).AutPriv: Comunicación con autenticación y privacidad. Los protocolos utilizados son:<ul style="list-style-type: none">Autenticación: SHA.Privacidad: AES (Advanced Encryption Standard, estándar de cifrado avanzado).
Contraseña de autenticación	Si la autenticación está habilitada, introduzca una contraseña de autenticación que distinga entre mayúsculas y minúsculas. Puede tener de 8 a 12 caracteres y caracteres alfanuméricos (letras mayúsculas, minúsculas y números), tal como se indica en la información sobre herramientas de la página web.
Contraseña de privacidad	Si la privacidad está habilitada, introduzca una contraseña de privacidad que distinga entre mayúsculas y minúsculas. Debe tener 8 caracteres y puede incluir caracteres alfanuméricos (letras mayúsculas, minúsculas y números), tal como se indica en la información sobre herramientas de la página web.

OPC UA

Utilice estos ajustes para configurar la conexión del servidor OPC UA integrado en el módulo BMENUA0100:

Parámetro	Descripción
Modalidad de seguridad de mensajes	<ul style="list-style-type: none">Firmar y cifrar (valor predeterminado): A cada mensaje se le asigna una firma y se cifra.Firmar: Se aplica una firma a cada mensaje.Ninguno: No se aplica ninguna política de seguridad. Con esta opción, los dos campos siguientes están deshabilitados. <p>NOTA: Cuando se selecciona Ninguno, el Tipo de token de identificador de usuario del módulo BMENUA0100 se define como Anónimo. En este caso, también deberá ajustar el tipo de token de identificador de usuario del cliente OPC UA en Anónimo.</p>
Directiva de seguridad	<ul style="list-style-type: none">Basic256Sha256 (valor predeterminado): Define una directiva de seguridad para configuraciones con un conjunto de cifrado válido.Basic256: Define una directiva de seguridad para configuraciones con un conjunto de cifrado obsoleto. <p>NOTA: Esta opción no se utiliza a menos que sea necesaria para la interacción con el cliente remoto.</p> <ul style="list-style-type: none">Basic128Rsa15: Define una directiva de seguridad para configuraciones con un conjunto de cifrado obsoleto. <p>NOTA: Esta opción no se utiliza a menos que sea necesaria para la interacción con el cliente remoto.</p>
Tipos de token de identificador de usuario	<ul style="list-style-type: none">Anónimo: No hay información disponible sobre el usuario.Nombre de usuario (valor predeterminado): El usuario se identifica por medio del nombre de usuario y la contraseña.

NOTA: Los cambios en la configuración de la ciberseguridad de los ajustes del servidor OPC UA hacen que el servidor se reinicie y aplique los nuevos ajustes. En consecuencia, si existen una o varias sesiones de OPC UA al realizar cambios en la configuración, estas sesiones quedarán suspendidas. Cuando finalice el período de *Tiempo de espera de la sesión*, estas sesiones se cierran. El *Tiempo de espera de la sesión* forma parte de la configuración del cliente SCADA OPC UA.

NOTA: Cuando el ajuste **Modalidad de seguridad de mensajes** del servidor OPC UA se configura inicialmente en **Firmar y cifrar** o **Firmar** y un cliente OPC UA establece una conexión, si posteriormente establece el ajuste de **Modalidad de seguridad de mensajes** del servidor OPC UA en **Ninguno**, el cliente OPC UA (con su ajuste de **Modalidad de seguridad de mensajes** también configurado en **Ninguno**) no podrá establecer la conexión con el servidor.

Para restablecer una conexión:

1. Desconecte los clientes OPC UA.
2. Cambie la configuración de OPC UA en la página web del módulo BMENUA0100.
3. Espere mientras el indicador LED **BUSY** permanece encendido (amarillo) hasta que se apague (no se ilumine).
4. En los clientes OPC UA, cambie su configuración (**Modalidad de seguridad de mensajes**) por el mismo ajuste que el utilizado para el servidor OPC UA.
5. Vuelva a conectar los clientes OPC UA al servidor.

Banner de seguridad

Esta página contiene texto editable que se muestra cuando un usuario accede a las páginas web del módulo BMENUA0100:

Parámetro	Descripción
Texto del banner	Cadena de hasta 128 caracteres que se muestra a un usuario en la página de inicio de sesión. De forma predeterminada, se muestra el siguiente texto editable: "Se prohíbe el uso no autorizado del sistema, que quedará sujeto a sanciones penales o civiles".

Gestión de certificados

Gestión de certificados con y sin PKI

El módulo BMENUA0100 se basa en certificados para la autenticación. Para proporcionar ciberseguridad, cada entidad (incluidos los clientes OPC UA y el servidor OPC UA integrado en el módulo BMENUA0100) necesita gestionar una lista de confianza de los diferentes certificados de dispositivos/aplicaciones que se comunican con ella.

El método de administración de certificados depende del diseño de su sistema, que puede o no aplicar una infraestructura de clave pública (PKI) con una autoridad de certificación (CA).

Gestión de certificados sin PKI:

Utilice este método de gestión de certificados si el sistema no incluye una CA. Este método de gestión es compatible con los módulos BMENUA0100 con firmware v1.0 y posterior. Para gestionar certificados en las páginas web de **Gestión de certificados**:

- Ajuste la **Modalidad PKI** en **Sólo autofirmado**.
- Gestione la **lista de certificados de confianza** mediante las funciones **Añadir** y **Eliminar** para crear una lista de los clientes OPC UA autorizados para comunicarse con el módulo BMENUA0100.
- Exporte el certificado del módulo BMENUA0100 a dispositivos de cliente OPC UA mediante el comando **Descargar** en la página **Configuración PKI > Certificado de dispositivo**.

Gestión de certificados con PKI:

Utilice este método de gestión de certificados en el caso de que el sistema incluya una CA. Este método de gestión es compatible con los módulos BMENUA0100 con firmware v1.1 y posterior. Para gestionar certificados en las páginas web de **Gestión de certificados**:

- Ajuste la **Modalidad de PKI** en:
 - **Solo CA**: si todos los dispositivos cliente OPC UA instalados son compatibles con PKI.
 - **Autofirmado y CA**: si algunos de los dispositivos cliente OPC UA instalados no son compatibles con PKI.
- Si la **Modalidad de PKI** está configurada en **Solo CA**:
 - Inscriba manualmente, página 116 cada uno de los módulos BMENUA0100 en la CA.
- Si la **modalidad PKI** se establece en **Autofirmado y CA**:
 - Inscriba manualmente, página 116 cada uno de los módulos BMENUA0100 en la CA.
 - Gestione la **lista de certificados de confianza** mediante las funciones **Añadir** y **Eliminar** para crear una lista de los clientes OPC UA autorizados para comunicarse con el módulo BMENUA0100.

Actualización de la lista de confianza de certificados

Después de la primera instalación de la versión 2.0 o posterior del firmware del módulo BMENUA0100 (BMENUA0100.2), es necesario eliminar los certificados añadidos por el usuario de la **Lista de confianza de certificados** de la página web de **Gestión de certificados**. Para ello, puede hacer lo siguiente:

- Eliminar manualmente estos certificados mediante el comando **Eliminar** o
- Ajustar el conmutador rotativo de ciberseguridad a la posición **Cybersecurity Reset**.

Una vez que se borra la **Lista de confianza de certificados**, puede volver a llenarla con certificados autofirmados o emitidos por la CA.

Esta tarea solo debe realizarse durante la primera instalación de la versión 2.0 o posterior del firmware. No es necesario repetir el procedimiento en instalaciones posteriores de versiones posteriores del firmware.

NOTA: Si no borra la **lista de confianza de certificados**, tal como se describió anteriormente, no se podrán establecer conexiones con clientes OPC UA o, si se han establecido, se descartarán.

Vista general de la autenticación

Los clientes OPC UA o módulos BMENUA0100 pueden autenticarse de tres maneras:

- Para la versión del firmware 1.0 y posteriores:
 - Certificado autofirmado (solo)
- Para la versión del firmware 1.10 y posteriores:
 - Certificado de PKI emitido únicamente por una autoridad de certificación (CA) de terceros
 - Certificado de PKI emitido por una CA y certificado autofirmado

Para satisfacer el nivel requerido de ciberseguridad, cada entidad (cliente OPC UA, BMENUA0100) debe gestionar una lista de confianza de todos los certificados de dispositivos/aplicaciones que se comunican con ella.

Para la versión del firmware 1.10 y posteriores, el módulo BMENUA0100 crea un certificado autofirmado a fin de:

- Configuración de los ajustes de ciberseguridad a través de las páginas web del módulo
- Diagnóstico del módulo a través de sus páginas web
- Actualización del firmware
- Certificados de instancia de aplicación OPC UA para permitir a los clientes OPC UA acceder al servidor OPC UA integrado en el módulo BMENUA0100.

Con la versión 1.0 del firmware, el módulo crea dos certificados: un certificado HTTPS y otro OPC UA.

NOTA:

- Las fechas de caducidad de los certificados de confianza se generan en referencia a la configuración interna de fecha y hora del módulo BMENUA0100. Para evitar incoherencias, utilice el servicio NTP para actualizar los ajustes de fecha y hora del módulo BMENUA0100 y compruebe que el servidor NTP sea accesible y tenga una configuración de fecha y hora actualizada.
- Si recibe un error detectado *BadCertificateHostNameInvalid* al intentar conectar su cliente OPC UA al servidor BMENUA0100 en IPv6, puede deberse a una dirección IPv6 comprimida (es decir, una dirección IPv6 abreviada). En este caso, compruebe la dirección IPv6 que se utilizó y, si es necesario, sustitúyala utilizando un formato sin comprimir.
- El módulo BMENUA0100 no gestiona automáticamente las fechas de caducidad de los certificados. Debe gestionar las fechas de caducidad del certificado manualmente.

Gestión de certificados

En las páginas web del módulo BMENUA0100, en la página de **inicio**, seleccione **Gestión de certificados** para ver enlaces a las siguientes páginas de gestión de certificados de la instancia de aplicación:

- Configuración de PKI, página 115
- Gestión de listas de confianza de clientes, página 117
- Exportación de certificados de dispositivo, página 118
- Inscripción manual, página 116
- Certificados de CA, página 118

Consulte los temas *Uso de GPO/LGPO*, página 177 y *Aplicar la administración de directivas de grupo de MMC*, página 177 para obtener más información sobre las herramientas de Windows™ que puede utilizar para gestionar certificados.

Extensiones de certificado

Para admitir la comunicación con el módulo BMENUA0100, los certificados autofirmados y de CA deben incluir las siguientes extensiones específicas:

Certificados autofirmados:

- KeyUsage (marcado como crítico):
 - KeyEncipherment
 - KeyEncipherment (no se utiliza el conjunto TLS basado en claves efímeras como TLS_ECDHE_XXXX; uso para TLS_RSA_XXXX)
 - KeyCertSign: cuando se utiliza la clave pública de firmante para verificar las firmas en los certificados de clave pública (valor TRUE)
 - nonRepudiation (requerido por el estándar OPC UA)
 - dataEncipherment (requerido por el estándar OPC UA)
- Nombre alternativo del firmante: En el campo SAN se pueden especificar los siguientes valores: Dirección IPA V4/V6, URI
- Limitaciones básicas:
 - Campo cA: si la clave pública certificada puede usarse para verificar firmas de certificados (Valor TRUE) y pathLenConstraint = 0
- Identificador de clave de sujeto:
 - medios para identificar certificados que contienen un hash SHA-1 público específico de 160 bits del valor del subjectPublicKey BIT STRING (sin incluir la etiqueta, longitud y número de bits no utilizados).
- Extensión de uso de clave extendida:
 - id-kp-serverAuth en caso de autenticación de servidor web TLS
 - id-kp-clientAuth en caso de autenticación de cliente web TLS

Certificados de CA:

- KeyUsage (marcado como crítico):
 - KeyEncipherment
 - KeyEncipherment (no se utiliza el conjunto TLS basado en claves efímeras como TLS_ECDHE_XXXX; uso para TLS_RSA_XXXX)
 - KeyCertSign: cuando se utiliza la clave pública de firmante para verificar las firmas en los certificados de clave pública (valor FALSE)
 - nonRepudiation (requerido por el estándar OPC UA)
 - dataEncipherment (requerido por el estándar OPC UA)
- Nombre alternativo del firmante: En el campo SAN se pueden especificar los siguientes valores: Dirección IPA V4/V6, URI
- Limitaciones básicas:
 - Campo cA: si la clave pública certificada puede usarse para verificar firmas de certificados (Valor FALSE)

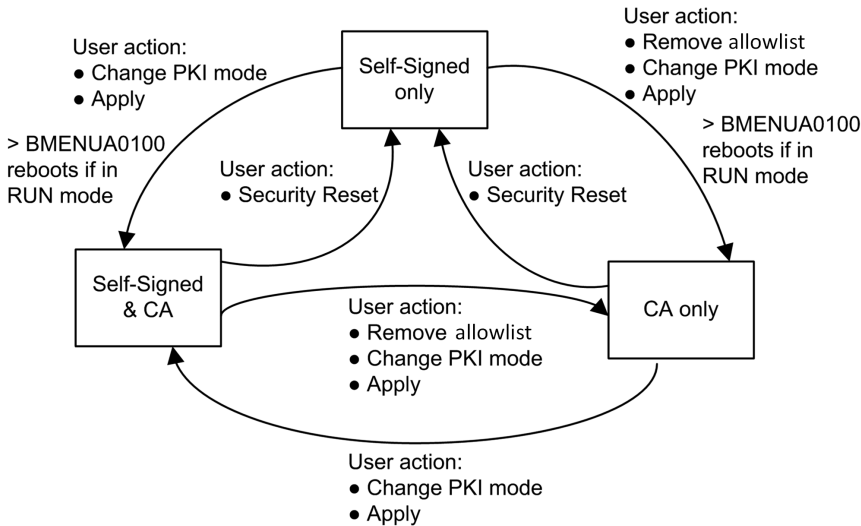
- Extensión de uso de clave extendida:
 - id-kp-serverAuth en caso de autenticación de servidor web TLS
 - id-kp-clientAuth en caso de autenticación de cliente web TLS
- Puntos de distribución de CRL
- Identificador de clave de autoridad:
 - Identificación de la clave pública correspondiente a la clave privada utilizada para firmar un certificado.

Configuración de PKI

Utilice la página **Configuración de PKI** para especificar los tipos de certificados aceptados por el servidor OPC UA integrado en el módulo, incluidos:

Modalidad de PKI	Descripción
Solo con autofirma	Solo se deben gestionar los certificados de la lista Certificado de cliente de confianza .
Solo CA	Todos los dispositivos del sistema necesitan certificados firmados por una CA.
Autofirmado y CA	Los certificados se gestionan de la siguiente manera: <ul style="list-style-type: none">• El certificado del módulo BMENUA0100 con la versión 1.10 y posterior del firmware lo emite una CA.• Los certificados para los dispositivos cliente compatibles con PKI los emite una CA.• Los certificados para los dispositivos cliente que no son compatibles con PKI son autofirmados.

En el siguiente diagrama se ilustran las acciones del usuario y los eventos relacionados con el cambio de la configuración de la modalidad de PKI:



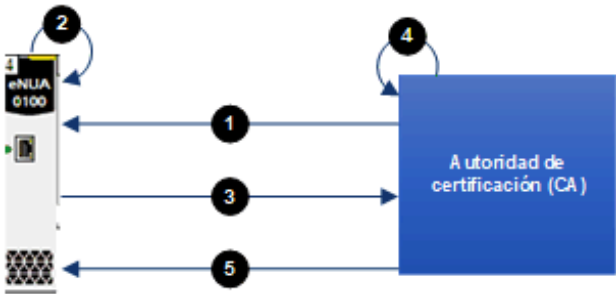
Inscripción manual

Después de configurar el módulo BMENUA0100 en Control Expert, puede utilizar la página **Inscripción manual** para **obtener** un archivo CSR que se enviará a una CA. Después de enviar el archivo CSR, puede extraer el certificado CA correspondiente. Por lo tanto, puede **ingresar** este Certificado CA en el módulo BMENUA0100. Las operaciones combinadas **obtener** e **ingresar** inscriben manualmente un certificado emitido por una CA de terceros. Una vez que se pulsa en el certificado, el servidor OPC UA aplica este certificado con el fin de firmar y cifrar su comunicación con el cliente OPC UA.

NOTA: Como condición previa para realizar la inscripción manual:

- Confirme que el cliente NTP esté habilitado, página 133.
- Verifique que el ajuste de hora para el módulo BMENUA0100 sea correcto.

A continuación se presenta una descripción general del proceso manual de inscripción de certificados:



- 1 El módulo BMENUA0100 importa un certificado de CA de la autoridad de certificación (CA)
- 2 El módulo BMENUA0100 genera una petición de firma de certificado (CSR)
- 3 El módulo BMENUA0100 exporta el CSR a la CA
- 4 La CA ejecuta el CSR y genera un certificado
- 5 El módulo BMENUA0100 importa el certificado de la CA

Consulte el vídeo de Schneider Electric "How to work with PKI mode "Self-Signed & CA" on BMENUA0100 module?" (¿Cómo trabajar con la modalidad de PKI "Solo autofirmado y CA" en el módulo BMENUA0100?) en <https://www.se.com/us/en/faqs/FAQ000191153/>.

Gestión de listas de confianza de clientes

Solo los clientes OPC UA que hayan proporcionado al módulo BMENUA0100 un certificado de instancia de aplicación pueden comunicarse con el servidor OPC UA integrado en el módulo. El módulo implementa la gestión local (basada en módulos) de los certificados de instancia de aplicación OPC UA, que se almacenan en una lista de confianza. Utilice los comandos de las páginas web de **Gestión de certificados** para **añadir**, **descargar** o **eliminar** un certificado.

NOTA: Los certificados de lista de confianza de instancias de aplicaciones OPC UA se codifican en ANSI CRT.

Para añadir un certificado a la lista:

Paso	Acción
1	En el menú de gestión de listas de confianza, haga clic en Añadir .
2	Haga clic en Examinar para desplazarse hasta el certificado que desea añadir a la lista y seleccionarlo.

Paso	Acción
3	Haga clic en Enviar para añadir el certificado.
4	Haga clic en Aplicar para guardar el cambio en la configuración.

Para eliminar un certificado de la lista:

Paso	Acción
1	En la lista de confianza, haga clic en el certificado que desea eliminar.
2	Seleccione Eliminar .
3	Haga clic en Sí para eliminar el certificado de la lista.
4	Haga clic en Aplicar para guardar el cambio en la configuración.

Exportación de certificados de dispositivo

Para exportar el certificado del módulo BMENUA0100 para HTTPS y OPC UA en la página **GESTIÓN DE CERTIFICADOS > CONFIGURACIÓN DE PKI** , haga clic en el botón **Descargar**.

Certificados de CA

El certificado CA es un certificado de clave pública que identifica a la autoridad de certificación (CA) en una infraestructura de clave pública (PKI). Utilice la página **Certificados de CA** para añadir los certificados de CA al dispositivo.

Para añadir un certificado de CA a la lista de certificados de CA:

Paso	Acción
1	Abra las páginas web del módulo y en el cuadro de diálogo Inicio de sesión , introduzca: <ul style="list-style-type: none">• username• password Haga clic en Inicio de sesión .
2	Desplácese hasta CONFIGURACIÓN DE LOS AJUSTES DE CIBERSEGURIDAD > GESTIÓN DE CERTIFICADOS para acceder a la ficha de gestión de certificados y, a continuación, seleccione Certificados de CA .
3	En la lista CERTIFICADOS DE CONFIANZA , haga clic en AÑADIR para añadir el certificado de CA a la lista.
4	Aplique los cambios a la configuración de ciberseguridad.

NOTA: Se puede añadir un máximo de diez certificados de CA.

Control de acceso

Introducción

El módulo BMENUA0100 permite la autenticación local de usuarios basada en el uso de combinaciones de nombre de usuario/contraseña para:

- Configuración de los ajustes de ciberseguridad del módulo mediante HTTPS
- Descarga de firmware mediante HTTPS
- Diagnósticos de páginas web del módulo mediante HTTPS

NOTA: Solo los usuarios con el rol de administrador de seguridad pueden crear, editar o eliminar cuentas de usuario.

Las páginas web de BMENUA0100 proporcionan herramientas para la administración de cuentas de usuario. En la página **Inicio**, haga clic en **Control de acceso** para ver una lista de las cuentas de usuario de OPC UA existentes en la que se incluyen sus roles y sus permisos. En esta página puede:

- Crear una cuenta de usuario, página 120.
- Actualizar el perfil, página 120 de una cuenta de usuario existente.
- Eliminar, página 121 una cuenta de usuario.

Administración de usuarios

El módulo BMENUA0100 proporciona control de acceso basado en rol (RBAC). Todas las cuentas de usuario tienen un rol asignado y solo pueden realizar las tareas asociadas con ese rol.

Se admiten los siguientes roles y permisos:

Función	Permisos			
	Configuración de ciberseguridad	Actualiza- ción del firmware	Acceso a la página web de diagnósticos	Acceso al protocolo OPC UA
SECADM	Actualizar, leer, eliminar	–	Leer	–
OPERADOR	–	–	Leer	Conectar
INGENIERO	–	–	Leer	Conectar
INSTALA- DOR	–	Actualizar	Leer	–

Cada módulo BMENUA0100 admite un máximo de 15 usuarios simultáneos.

No se pueden configurar roles personalizados ni conjuntos de permisos personalizados. No se pueden configurar listas de autorizaciones de control de acceso basadas en direcciones IP.

Crear una cuenta de usuario

Un administrador de seguridad puede hacer clic en **Nuevo usuario** y, a continuación, completar los siguientes parámetros para crear una nueva cuenta de usuario:

Parámetro	Descripción
Nombre de usuario	El ID de usuario. El usuario introducirá el nombre de usuario y la contraseña para acceder a las funciones permitidas.
Contraseña	La contraseña de usuario. La contraseña no se muestra en texto sin formato. Introduzca este valor dos veces para confirmar su precisión. NOTA: Cada contraseña debe tener una longitud mínima de 8 caracteres y contener al menos uno de los caracteres siguientes: <ul style="list-style-type: none">• un carácter alfabético en mayúsculas (A-Z)• un carácter alfabético en minúsculas (a-z)• Un número dígito (0...9)• Un carácter especial ~ ! @ \$ % ^ & * _ + - = ` \ () [] : " ' < >
Confirmar contraseña	
Roles	Seleccione el rol que definirá los permisos de ese usuario: <ul style="list-style-type: none">• Administrador de seguridad• Operador (Operator)• Ingeniero• Instalador

Haga clic en **Aplicar cambios** después de configurar estos parámetros para crear el nuevo usuario.

Actualizar una cuenta de usuario

Para editar los ajustes de una cuenta de usuario, el administrador de seguridad puede hacer clic en el icono de editar (lápiz) del perfil que desee editar. Haga clic en **Aplicar cambios** para guardar las ediciones. Se abre el mismo cuadro de diálogo utilizado para crear una cuenta de usuario, que permite actualizar algunos o todos los parámetros de cuenta de usuario seleccionados.

Eliminar una cuenta de usuario

Para eliminar una cuenta de usuario existente, el administrador de seguridad puede hacer clic con el botón derecho en ese usuario de la lista y, en **Eliminar usuario**, hacer clic en **Aceptar**.

Administración de la configuración

Introducción

Para facilitar la configuración del sistema, puede exportar los ajustes de ciberseguridad de un módulo BMENUA0100 configurado e importar esa configuración en otro módulo. En las páginas web del módulo BMENUA0100, en la página de **inicio**, seleccione **Administración de la configuración** para ver enlaces a las siguientes páginas de administración de la configuración de ciberseguridad:

- EXPORTAR, página 121
- IMPORTAR, página 122
- RESTABLECER, página 122

NOTA: Solo los administradores de seguridad con el rol SECADM pueden realizar las tareas de administración de la configuración descritas en este tema.

Exportar una configuración

Use la página **EXPORTAR** para exportar el archivo de configuración de ciberseguridad del módulo BMENUA0100 local. El archivo de configuración exportado se cifra con la contraseña asignada en esta página. Los archivos de configuración exportados se pueden almacenar y reutilizar.

Para exportar el archivo de configuración de ciberseguridad del módulo BMENUA0100 local:

Paso	Descripción
1	En la página EXPORTAR , asigne una Contraseña al archivo de configuración. NOTA: La contraseña debe tener 16 caracteres como mínimo, y se aplican las mismas reglas usadas en la creación de contraseñas de usuario, página 120.
2	Introduzca de nuevo en el campo Confirmar contraseña la contraseña asignada.
3	Haga clic en Descargar .

NOTA: El archivo de configuración se genera con el nombre: Mx80_xx_BMENUA.cfg, donde "xx" indica el número de slot que ocupa el módulo en el bastidor.

Importar una configuración

Use la página **IMPORTAR** para importar un archivo de configuración de ciberseguridad y aplicarlo al módulo BMENUA0100 local. Los ajustes de ciberseguridad aplicados con este comando sobrescriben los ajustes de ciberseguridad existentes en el módulo.

Para importar un archivo de configuración de ciberseguridad y aplicarlo al módulo BMENUA0100 local:

Paso	Descripción
1	En la página IMPORTAR , haga clic en el icono de archivo para abrir una ventana en la que puede seleccionar un Archivo de configuración .
2	Seleccione el archivo de configuración que desee importar y haga clic en Aceptar .
3	En el menú IMPORTAR , introduzca el archivo de configuración Contraseña asignado al archivo al exportarlo. NOTA: También puede seleccionar Guardar para aplicar automáticamente la configuración importada justo después de que se cargue.
4	Haga clic en Cargar . Se abrirá un cuadro de diálogo en el que se informará de que su sesión se ha cerrado. La configuración se ha cargado en el servidor.
5	Haga clic en Reconectar para cerrar el cuadro de diálogo y abrir la <u>pantalla de inicio de sesión</u> , página 92.
6	Introduzca su nombre de usuario y su contraseña de administrador de seguridad y haga clic en Iniciar sesión . Se abrirá la página de inicio. Si no seleccionó Guardar en el paso 3, el banner indicará que hay una configuración pendiente.
7	En el banner, haga clic en Aplicar y, a continuación, haga clic en Sí para confirmar que desea aplicar la configuración pendiente. Se aplicará la nueva configuración. NOTA: Si antes seleccionó Guardar en la página IMPORTAR (como se ha indicado anteriormente en el paso 3), la configuración se aplicará automáticamente y este paso 7 se realizará de forma automática.

Restablecer una configuración

Haga clic en **Restablecer** en la página **RESTABLECER** para restaurar los ajustes de ciberseguridad predeterminados del módulo BMENUA0100 local. Esta acción tiene el mismo efecto que colocar el conmutador rotativo en la posición *Cybersecurity* (o *Security*) Reset, página 33. Tras completar el restablecimiento, debe reiniciar el módulo.

Configuración de BMENUA0100 en Control Expert

Introducción

En esta sección se describe cómo configurar los ajustes de dirección IP, el cliente NTPv4 y el agente SNMPv1 para el módulo de comunicación Ethernet BMENUA0100 con servidor OPC UA integrado.

Configuración de la dirección IP

Introducción

El módulo de comunicaciones Ethernet BMENUA0100 con servidor OPC UA integrado incluye dos puertos Ethernet:

- El puerto de control situado en la parte delantera del módulo.
- Un puerto de la placa de conexiones que conecta el módulo a la placa de conexiones Ethernet del bastidor principal local.

El puerto de control se puede habilitar o deshabilitar, y está deshabilitado de forma predeterminada. El puerto de la placa de conexiones está siempre habilitado.

Los ajustes de dirección IP fija del puerto de control y el puerto de la placa de conexiones se pueden configurar en la ficha **IPConfig** del cuadro de diálogo de configuración del módulo BMENUA0100. Además, los ajustes de dirección IP se pueden asignar dinámicamente al puerto de control con el método Configuración automática de dirección sin estado (SLAAC) de DHCP.

Cuando el módulo BMENUA0100 se usa en un controlador independiente, los ajustes de dirección IP se configuran para un módulo. Cuando se usan dos instancias del módulo BMENUA0100 en una arquitectura de controlador Hot Standby (un módulo BMENUA0100 en cada controlador), la ficha de configuración **IPConfig** de Control Expert incluye ajustes para dos módulos (A y B). En una arquitectura controlador Hot Standby, la dirección IP de cada módulo puede estar en subredes diferentes.

Compatibilidad con pila IPv4 e IPv6

El puerto de control se puede configurar para ser compatible con pilas IP (cada una de las cuales consiste en una recopilación de protocolos de Internet) del modo siguiente:

- Pila IPv4: Solo admite direcciones de 32 bits. Un ejemplo de dirección IP IPv4 es: 192.168.1.2.

- Pila doble IPv4/IPv6: Admite direcciones de 32 y 128 bits. Cuando están configuradas las pilas IPv4 e IPv6, el puerto de control puede recibir y gestionar paquetes Ethernet IPv4 e IPv6. Un ejemplo de dirección IP de 128 bits IPv6 es:
2001:0578:0123:4567:89AB:CDEF:0123:4567.

NOTA:

En el primer arranque (o después de colocar el conmutador rotativo del módulo en **Cybersecurity (o Security) Reset**, encender el módulo, colocar el conmutador rotativo en **modalidad Advanced (o Secured)** y, a continuación, volver a encender el módulo), se asigna al puerto de control una dirección IPv4 predeterminada de 10.10.MAC5.MAC6, donde MAC5 es el valor decimal del quinto octeto de la dirección MAC del módulo y MAC6 es el valor decimal del sexto octeto.

Cuando los dos últimos octetos de la dirección MAC (*MAC5.MAC6*) corresponden a *0.0* en la dirección predeterminada, establezca una conexión de cables punto a punto entre el equipo y el controlador, módulo de comunicación u otro módulo.

La dirección MAC del módulo aparece en su cara delantera.

IPv6 a través del puerto de control

La comunicación IPv6 solo se admite a través del puerto de control.

NOTA: El flujo de Control Expert puede configurarse para que se enrute a un controlador M580. Control Expert V15 (o posterior) puede conectarse a un controlador M580 a través de la dirección IPv6 del módulo BMENUA0100.

Configuración de las direcciones IP

Configure las direcciones IP en Control Expert como se indica a continuación:

Paso	Acción
1	En el Explorador de proyectos , despliegue el nodo Bus PLC y abra el cuadro de diálogo de configuración del módulo BMENUA0100.
2	Haga clic en la ficha IPConfig .
3	Introduzca las modificaciones en los campos apropiados de la página de configuración IPConfig . (En la siguiente tabla se describen los parámetros de la página de configuración).

Parámetros configurables

Configure estos parámetros de la dirección IP para cada módulo de comunicaciones BMENUA0100 de su proyecto:

Parámetro		Descripción
Puerto de control		<p>Habilita/deshabilita el puerto de control del módulo BMENUA0100. Cuando se selecciona:</p> <ul style="list-style-type: none">Habilitado: el puerto de control es la interfaz exclusiva para la comunicación IPv4 o IPv6 con el servidor OPC UA integrado.Deshabilitado (valor predeterminado): el puerto Ethernet de la placa de conexiones admite la comunicación IPv4 con el servidor OPC UA.
Configuración del puerto de control IPv6		
	IPv6	Habilita/deshabilita las direcciones IP IPv6 para el puerto de control cuando el puerto de control está habilitado. Valor predeterminado = deshabilitado.
	Modo	<p>Identifica el origen de la dirección IPv6:</p> <ul style="list-style-type: none">SLAAC: indica que la dirección IP IPv6 la proporcionará al puerto de control un servidor DHCP mediante el método SLAAC.Fija (valor predeterminado): habilita el campo IPv6@ para introducir una dirección IP IPv6 fija.
	IPv6 @	<p>Si se selecciona Fija como Modalidad, introduzca una dirección IPv6 válida para el puerto de control.</p> <p>NOTA:</p> <ul style="list-style-type: none">BMENUA0100 no puede detectar direcciones IPv6 duplicadas. Consulte al administrador de su red para asegurarse de que no haya direcciones IPv6 duplicadas en el mismo segmento de red.El módulo BMENUA0100 aceptará direcciones IPv6 incorrectas, pero no podrá utilizarlas.
	Longitud del prefijo de subred	Se ajusta automáticamente para direcciones IPv6 fijas, y representa el número de bits de la dirección IPv6 asignada de SLAAC que definen el prefijo de subred (valor predeterminado = 64).
Configuración del puerto de control IPv4		

Parámetro		Descripción
	IPv4	Habilita/deshabilita las direcciones IP IPv4 para el puerto de control cuando el puerto de control está habilitado. Valor predeterminado = habilitado.
	Modo	Identifica el origen de la dirección IPv4: <ul style="list-style-type: none"> Valor predeterminado: El software asigna automáticamente una dirección IP. Fija (valor predeterminado): Habilita los campos IPv4 @, Máscara de subred y Pasarela predeterminada para introducir una dirección IP IPv4 estática para el puerto de control.
	IPv4 @	Si la modalidad seleccionada es: <ul style="list-style-type: none"> Valor predeterminado: La dirección IP se asigna automáticamente; los campos IPv4 @, Máscara de subred y Pasarela predeterminada están deshabilitados. Fija: Introduzca una dirección IPv4 válida para el puerto de control.
	Máscara de subred	Si se selecciona Fija como Modalidad , introduzca una máscara de subred IPv4 válida para el puerto de control, que determinará la parte de la red de la dirección IPv4.
	Pasarela predeterminada	Si se selecciona Fija como Modalidad , introduzca una dirección IPv6 válida para el puerto de control.
Puerto de la placa de conexiones		
	IPv4 @	Introduzca una dirección IPv4 válida para el puerto de la placa de conexiones.
Marca de tiempo en origen		Consulte el tema Configuración de las marcas de tiempo de origen , página 127.
Velocidad de muestreo rápida		Si se selecciona, puede configurar el cliente OPC UA con un intervalo de muestreo mínimo de 20 ms, que permite la supervisión de 2000 elementos. Si no se selecciona (valor predeterminado), el período de muestreo predeterminado es de 250 ms, lo que permite supervisar un valor equivalente a 20 000 elementos de tipo INT. NOTA: Los cambios en esta configuración solo se harán efectivos tras una descarga completa de la aplicación.
Puerto de escucha OPCUA TCP		El puerto TCP para la comunicación OPC UA: <ul style="list-style-type: none"> Valor predeterminado: preconfigurado en el puerto 4840 Otro valor: especificado por el usuario NOTA: El valor de este puerto debe ser el mismo para todos los módulos BMENUA0100 que se comunican entre sí (por ejemplo, en el caso del reenvío de NAT de OPC UA entre varios módulos BMENUA0100).

NOTA: Si se configura la aplicación en Control Expert:

- En la ventana **Red Ethernet** (que se abre seleccionando **Herramientas > Administrador de redes Ethernet...**) se muestran los ajustes del puerto de la placa de conexiones y del puerto de control del módulo BMENUA0100, incluida información del servidor NTP, el administrador SNMP y, en el caso de un sistema Hot Standby, el módulo standby BMENUA0100 (B).
- La página **Servidor de direcciones** del controlador (que se abre cuando va al **Explorador de DTM**, hace doble clic en el controlador y, a continuación, selecciona **Servicios > Servidor de direcciones**) muestra la dirección IP del puerto de la placa de conexiones del módulo BMENUA0100. En una configuración Hot Standby, la página **Servidor de direcciones** del controlador muestra la dirección IP del puerto de la placa de conexiones de los dos módulos BMENUA0100.

Configuración de las marcas de tiempo de origen

Las marcas de tiempo de origen son compatibles con la versión 2.01 (y posterior) del firmware del módulo BMENUA0100 (BMENUA0100.2) en Control Expert.

Para utilizar las marcas de tiempo de origen en una aplicación, debe habilitarlas y, luego, activarlas.

Una vez habilitadas y activadas, el módulo BMENUA0100 comienza a sondear los dispositivos cuando hay al menos un elemento supervisado con la **Modalidad de supervisión** configurada en **Muestreo** o **Informando** en el cliente OPC UA.

NOTA: Los valores se recuperan de un dispositivo de marcas de tiempo en origen solo para las variables BOOL y EBOOL que:

- Se han configurado con marcas de tiempo en origen (ASTS) en Control Expert.
- Se han supervisado por un cliente OPC UA como parte de la suscripción OPC UA.

Si el nodo OPC UA no se ha añadido a una suscripción (ni se ha supervisado como parte de ella), el servicio de lectura síncrona OPC UA detectará un error y lo notificará.

Habilitación de las marcas de tiempo de origen

Las marcas de tiempo de origen se habilitan en la ventana Ajustes del proyecto. Vaya a **General > Hora > Modalidad de marcas de tiempo** y, a continuación, seleccione **Sistema**.

NOTA: El ajuste predeterminado de la **Modalidad de marcas de tiempo** es **De aplicación**. Si no cambia el ajuste predeterminado por **Sistema**, se mostrará un error detectado cuando se compile la aplicación.

Activación de las marcas de tiempo de origen

Utilice la ficha **IPConfig** del cuadro de diálogo de configuración del módulo BMENUA0100 para activar y configurar las marcas de tiempo.

En la sección **Marcas de tiempo de origen**, configure los siguientes parámetros:

Ajuste	Descripción
Activado	Activa las marcas de tiempo de origen para la aplicación.
Sondeo de búfer (ms)	<p>Frecuencia de sondeo de las peticiones de lectura de eventos que gestiona el módulo BMENUA0100.</p> <p>El rango válido de ajustes va de 250 ms como mínimo a 5000 ms como máximo, en incrementos de 250 ms.</p> <p>NOTA: El número máximo de variables con marcas de tiempo de origen en Control Expert es de 5000.</p>

NOTA: Si el bastidor local de la unidad M580 incluye dos módulos BMENUA0100, las marcas de tiempo de origen solo podrá utilizarlas uno de los módulos. Consulte el tema *Especificación del módulo BMENUA0100 para gestionar variables con marcas de tiempo*, página 131.

Gestión de variables con marcas de tiempo en origen

Uso de elementos de datod OPC UA #TSEventItemsReady y #TSEventSynchro

Puede utilizar los elementos de datos específicos de OPC UA `#TSEventItemsReady` y `#TSEventSynchro` para examinar y establecer, respectivamente, el estado de las variables con marcas de tiempo en origen.

NOTA: Ambos elementos solo tienen sentido cuando las marcas de tiempo están habilitadas en Control Expert y activadas para el módulo BMENUA0100 en cuestión.

El módulo BMENUA0100 trata el elemento de datos `#TSEventSynchro` como un nodo OPC UA booleano.

Al establecer el elemento `#TSEventSynchro`, se envía un comando de sincronización a todos los dispositivos con marcas de tiempo en origen del controlador M580. Los valores devueltos al cliente OPC UA por los dispositivos inicializan las variables con marcas de tiempo en origen con sus valores actuales.

El módulo BMENUA0100 responde al cliente configurando el elemento `#TSEventSynchro` con uno de los mensajes siguientes:

- **UA_EGOOD:** la petición de sincronización se ha enviado correctamente a todos los dispositivos de marcas de tiempo.
- **UA_EBAD:** la petición de sincronización no se ha realizado correctamente porque las marcas de tiempo están deshabilitadas en el proyecto de Control Expert.
- **UA_EBADINVALIDSTATE:** la solicitud de sincronización no se ha realizado correctamente porque la función %MW400, página 131 desactivó las marcas de tiempo para el módulo BMENUA0100.
- **UA_EBADINUSE:** la petición de sincronización no se ha realizado correctamente porque el módulo BMENUA0100 no ha podido reservar el búfer de marcas de tiempo.
- **UA_EBADDISCONNECT:** se agotó el tiempo de espera de la petición de sincronización y no se pudieron escribir valores en el intervalo de tiempo especificado.

Para llevar a cabo esta inicialización, utilice un cliente OPC UA (por ejemplo, UaExpert) para realizar la siguiente secuencia de tareas:

1. Supervise el elemento `#TSEventItemsReady`, que indica que el módulo BMENUA0100 está listo para gestionar variables con marcas de tiempo de los búferes del ePAC (incluidos el controlador M580, BMECRA31310 y BMXERT1604) y, a continuación, espere a que su valor cambie a 1 (TRUE).
2. Añada elementos de datos supervisados configurados como variables con marcas de tiempo en origen a una o varias suscripciones.
3. Ajuste el comando de escritura `#TSEventSynchro` para actualizar el valor y la marca de tiempo de origen de cada elemento.

NOTA:

- El módulo BMENUA0100 lee todas las variables con marcas de tiempo configuradas en el controlador. Si se produce un evento (cambio de estado del elemento) en un elemento supervisado con marca de tiempo, se actualiza ese elemento. Si un elemento no se supervisa, se descarta.
- Establezca el filtro de cambio de datos en **Estado/Valor/Marca de tiempo**. De lo contrario, es posible que distintos clientes OPC UA (por ejemplo, clientes que actualizan valores únicamente con cambios de estado/valor) muestren un estado y un valor diferentes para la misma variable.
- Debido a que el módulo BMENUA0100 actualiza los valores periódicamente, es posible que se produzcan varios eventos desde la actualización anterior. En ese caso, el módulo BMENUA0100 solo muestra el valor más reciente.
- Debido a que `#TSEventSynchro` se envía a varios dispositivos con marcas de tiempo, si un dispositivo concreto no responde dentro del intervalo de tiempo esperado, el ajuste `#TSEventSynchro` devuelve la respuesta `UA_EBADDISCONNECT`, con la que se indica que el comando ha superado el tiempo de espera y no se ha ejecutado correctamente. Esto se aplica aunque haya otros dispositivos que responden correctamente.
- Si la suscripción se edita para incluir, por ejemplo, una única variable para un dispositivo, la ejecución de `#TSEventSynchro` hará que se pierdan los valores devueltos previamente para los dispositivos y variables suscritos anteriormente.

Determinación de los canales del controlador M580 dedicados a las marcas de tiempo

Para la comunicación entre el módulo BMENUA0100 y un controlador M580, para la que las marcas de tiempo están habilitadas en Control Expert, el 25 % de los canales del controlador están dedicados a admitir la función de marcas de tiempo. El 75 % de los canales del controlador, como máximo, permanecen disponibles para atender otras peticiones de comunicación.

Por ejemplo, para el controlador BMEP584040:

- Número máximo de canales: 13
- Canales utilizados para marcas de tiempo: 3
- Canales utilizados para tareas que no sean marcas de tiempo: 10

Determinación de la capacidad del módulo BMENUA0100 para leer variables con marcas de tiempo

El número de variables con marcas de tiempo que el módulo BMENUA0100 puede leer por ciclo depende de los siguientes factores:

- El ajuste **Sondeo de búfer** en la ficha **IP Config** del módulo y
- La capacidad del dispositivo de origen, incluidos:
 - El número máximo de conexiones TCP y
 - El número máximo de variables con marcas de tiempo en origen admitidas.

La fórmula para determinar el número máximo de variables con marcas de tiempo en origen para un dispositivo es:

$$((\text{Número máximo de conexiones TCP}) / (\text{Número de canales})) \times (\text{Número máximo de variables con marcas de tiempo por ciclo})$$

Por ejemplo:

- BMEP586040(C): 16 conexiones máx., 4 canales, 82 variables máx.:
 $(16 / 4) \times 82 = 328$ variables totales
Si **Sondeo del búfer** = 500 ms: 656 variables por segundo.
- BMECRA31310: 1 conexión, 1 canal, 82 variables máx.:
 $1 \times 82 = 82$ variables totales
Si **Sondeo del búfer** = 500 ms: 164 variables por segundo.
- BMXERT1604: 1 conexión, 1 canal, 20 variables máx.:
 $1 \times 20 = 20$ variables totales
Si **Sondeo del búfer** = 500 ms: 40 variables por segundo.

Especificación del módulo BMENUA0100 para gestionar variables con marcas de tiempo

Un bastidor principal M580 puede contener dos módulos BMENUA0100. Sin embargo, las variables con marcas de tiempo en los controladores M580, y los módulos BMECRA31310 y BMXERT1604 solo las puede leer y gestionar un único módulo BMENUA0100 a la vez. Durante el arranque, cada módulo BMENUA0100 intenta, de forma predeterminada, reservar y bloquear el acceso a las variables con marcas de tiempo.

En un bastidor con dos módulos BMENUA0100, es necesario especificar el que leerá y gestionará variables con marcas de tiempo. Para especificar el módulo BMENUA0100 que leerá y gestionará variables, siga estos pasos:

1. En la ficha **IPConfig** de los dos módulos BMENUA0100 en los que desea aplicar marcas de tiempo, seleccione **Activado**.
2. En el módulo BMENUA0100 para el que desea reservar el búfer de marcas de tiempo, utilice el bloque `WRITE_VAR` para establecer la palabra %MW400 en 2, con lo que se activa la lectura y la gestión de variables con marcas de tiempo para este módulo.
NOTA: Al establecer %MW400 = 2, se identifica el módulo BMENUA0100 que leerá y gestionará las variables cuando dos módulos BMENUA0100 tengan seleccionado el ajuste **Activado**.
3. En el otro módulo BMENUA0100 para el que no desea reservar el búfer de marcas de tiempo, utilice el bloque `WRITE_VAR` para establecer la palabra %MW400 en 1, con lo que se desactiva la lectura y la gestión de variables con marcas de tiempo para estos módulos.

NOTA: Debe realizar estos pasos después de cada cambio en la modalidad de funcionamiento, incluidos el apagado y encendido, la carga de la aplicación o la inicialización.

El módulo BMENUA0100 que especifique mantendrá el control de lectura y gestión de variables con marcas de tiempo siempre que se cumplan las dos condiciones siguientes:

- Se supervisa al menos una variable con marcas de tiempo.
- La **Modalidad de supervisión** del módulo BMENUA0100 se establece en **Informando** o **Muestreo**.

NOTA:

Cuando se deselecciona el ajuste **Activado**, los valores de las variables que ha leído el módulo BMENUA0100 corresponden a los valores de la memoria del controlador.

Si se selecciona el ajuste **Activado** y %MW400 se establece en 1, los valores de variables que ha leído el módulo BMENUA0100 conservan el último valor leído cuando se reservó el búfer de marcas de tiempo.

Supervisión de variables de alias con marcas de tiempo

El módulo BMENUA0100 reconoce las variables de **Alias** con marcas de tiempo **BOOL** o **EBOOL** creadas en Control Expert, pero no reconocerá ninguna otra variable de tipo **Alias** de correspondiente. A continuación se muestra un ejemplo de las variables de **Alias** y **Alias de**:

Variables DDT Types Function Blocks DFB Types								
Filter			Name INST_DDT_03_BOOL*			☒ EDT ☒ DDT ☒ IOODT ☒ Device DDT		
Name	Type	Alias	Alias of	HMI variable	Time stamping	Source	TS ID	
Alias_INST_DDT_03_BOOL_1	BOOL		INST_DDT_03_BOOL_1	☒	Both Edges	PLC	259	
INST_DDT_03_BOOL	DDT_03_BOOL			☒				
BOOL_1	BOOL	Alias_INST_DDT_03_BOOL_1		☐	Both Edges	PLC	259	
BOOL_2	BOOL			☐	None			
BOOL_3	BOOL			☐	None			

Para que el módulo BMENUA0100 las reconozca, las variables de **Alias** deben estar integradas en el diccionario de datos.

Las variables de **Alias** BOOL o EBOOL, y sus correspondientes variables de **Alias de**, comparten la misma dirección lógica en la memoria de M580 y el mismo EventID en el búfer de marcas de tiempo de M580. Las marcas de tiempo de origen se gestionan únicamente en el **Alias** y no en la variable **Alias de**. En otras palabras, es necesario suscribir la variable de **Alias** (nodo OPC UA) en el cliente OPC UA para poder recibir las marcas de tiempo de origen del dispositivo en lugar de hacerlo desde el módulo.

Dado que no se considera que el firmware BMENUA0100 aplique marcas de tiempo en origen a las variables **Alias de** BOOL ni EBOOL, el **Alias** debe estar integrado en el diccionario de datos. En tal caso, debe añadir la variable de **Alias** como elemento supervisado en una suscripción de OPC UA para alcanzar las marcas de tiempo de origen establecidas por el dispositivo.

Configuración del servicio de hora de la red

Introducción

El módulo de comunicaciones Ethernet BMENUA0100 con servidor OPC UA integrado es compatible con la versión 4 del protocolo de hora de la red (NTP). El servicio NTP sincroniza el reloj del módulo BMENUA0100 con el reloj de un servidor horario. El valor sincronizado se utiliza para actualizar el reloj del módulo.

Se admiten los protocolos IPv4 e IPv6.

NOTA:

- Si el servidor NTP reside en el controlador, el módulo BMENUA0100 puede actualizar sus ajustes horarios sin introducir retraso.
- Cuando se llega a un nuevo servidor NTP o si hay un offset de tiempo en un servidor NTP, pueden ser necesarios hasta 5 minutos para actualizar BMENUA0100. El LED **ERR**, página 141 permanece encendido hasta que la hora de BMENUA0100 se sincroniza con el servidor NTP.
- La configuración manual de un cambio de hora introduciendo una hora futura puede provocar que se desconecten los canales OPC UA existentes. Si el cliente OPC UA realiza una reconexión automática al servidor OPC UA, se crearán nuevos canales y se realizará la reconexión.

Habilitar y deshabilitar el cliente NTP y el servidor NTP

El módulo BMENUA0100 incluye un servidor NTP y un cliente NTP.

Cliente NTP:

Si la dirección IP del servidor NTP primario o secundario tiene un valor diferente de 0.0.0.0, el cliente NTP está habilitado. Si los ajustes de dirección IP del servidor NTP primario y secundario están vacíos o están establecidos en 0.0.0.0 (IPv4) o 0000:0000:0000:0000:0000:0000:0000:0000 (IPv6), el cliente NTP estará deshabilitado.

NOTA: Cuando los ajustes de la dirección IP **Servidor NTP primario** y **Servidor NTP secundario** son 0.0.0.0, el módulo BMENUA0100 no puede funcionar como cliente NTP o como servidor NTP.

Servidor NTP:

El servidor NTP está habilitado en función de la modalidad de funcionamiento de ciberseguridad:

- En la modalidad Advanced (o Secured), el servidor NTP está habilitado si:
 - El ajuste de la dirección IP del servidor NTP primario o secundario es un valor no nulo (es decir, un valor diferente de 0.0.0.0); y
 - el servidor NTP está habilitado en los ajustes de configuración de la página web **Servicios de red** *Activación de servicios de red*, página 99.
- En la modalidad Standard, el servidor NTP está habilitado si el ajuste de la dirección IP **Servidor NTP primario** o **Servidor NTP secundario** se establece en un valor no nulo (es decir, un valor diferente de 0.0.0.0).

NOTA: Si el módulo BMENUA0100 está configurado como cliente NTP en la red de plano posterior (**Servidor NTP primario** o **Servidor NTP secundario**), el servidor NTP del BMENUA0100 no puede habilitarse para otro dispositivo.

Cuando el servidor NTP y el cliente NTP están habilitados en el módulo BMENUA0100, el cliente NTP del módulo recibe ajustes horarios mediante su puerto de control desde un servidor NTP remoto. El servidor NTP del módulo reenvía estos ajustes horarios mediante su puerto de la placa de conexiones a los clientes NTP.

NOTA: El módulo BMENUA0100 no puede funcionar como servidor NTP mediante su puerto de control.

Consulta NTP

El módulo BMENUA0100 administra de forma óptima y dinámica el periodo de consulta NTP con el servidor NTP. No se requiere ningún tipo de configuración.

Arranque

Para establecer la hora de la red del sistema Ethernet correcta, el sistema lleva a cabo estas tareas durante el arranque:

- El módulo de comunicaciones BMENUA0100 se inicia.
- El módulo de comunicaciones BMENUA0100 obtiene la hora del servidor NTP.

- Este servicio requiere que las solicitudes se envíen periódicamente para obtener y mantener la hora correcta. La configuración del **Periodo de consulta** influye en la precisión de la hora.

Una vez que se ha recibido una hora correcta, el servicio establece el estado en el diagnóstico del servicio de hora asociado.

NOTA: El módulo de comunicaciones BMENUA0100 no conserva la hora. Si arranca o apaga y enciende el sistema, el valor del reloj del módulo será 0, que equivale al 1 de enero de 1980 a las 00:00:00:00.

Configuración del servicio

Configure el servicio de sincronización horaria de la red en Control Expert, como se indica a continuación:

Paso	Acción
1	En el Explorador de proyectos , despliegue el nodo Bus PLC y abra el cuadro de diálogo de configuración del módulo BMENUA0100.
2	Haga clic en la ficha NTP .
3	Introduzca los cambios en los campos apropiados de la página de configuración Servicio de hora de red . (En la siguiente tabla se describen los parámetros de la página de configuración).

Parámetros configurables

Configure estos parámetros de sincronización horaria para cada módulo de comunicaciones BMENUA0100 de su proyecto:

Parámetro		Descripción
Configuración de servidor NTP IPv4		
	Servidor NTP primario (consulte la nota)	Introduzca una dirección IPv4 o IPv6 válida para el servidor NTPv4 primario. NOTA: Ajuste la dirección IP principal del controlador de forma predeterminada.
	Servidor NTP secundario (consulte la nota)	Introduzca una dirección IPv4 o IPv6 válida para el servidor NTPv4 secundario.
NOTA: <ul style="list-style-type: none">• Configure la dirección del servidor NTP a la que podrá acceder el módulo BMENUA0100. Si el puerto de control está deshabilitado, introduzca direcciones IP del servidor NTP que estén en la misma subred que el puerto de la placa de conexiones.• Si ambas direcciones se encuentran en el mismo dominio, puede configurar una dirección IPV4 para el servidor NTP primario y una dirección IPV6 para el servidor NTP secundario (y viceversa).• En las configuraciones Hot Standby, las direcciones del servidor NTP para NUA(A) y NUA(B) deben estar en la misma red, por ejemplo, la red a la que se puede acceder a través del puerto de la placa de conexiones o la red a la que se puede acceder a través del puerto de control.		

NOTA: Cuando opere en modalidad Advanced (o Secured), compruebe que el servicio NTP esté habilitado en la sección **Activación de servicios de red**, página 99 de la página web **Configuración**.

Configuración del agente SNMP

Acerca de SNMP

Todas las versiones del firmware del módulo BMENUA0100 son compatibles con el agente SNMP versión 1 (V1). La versión 2 (y posterior) del firmware del módulo (BMENUA0100.2) también es compatible con la versión 3 (V3) del agente SNMP.

NOTA: Las versiones de SNMP V1 y V3 no son compatibles simultáneamente.

Un agente SNMP es un componente de software del servicio SNMP que se ejecuta en el módulo BMENUA0100 y proporciona acceso a información de diagnóstico y gestión del módulo. Puede utilizar navegadores SNMP, software de gestión de redes y otras herramientas para acceder a estos datos.

Además, el agente SNMP puede configurarse con las direcciones IP de 1 o 2 dispositivos (por lo general, PC que ejecutan software de gestión de redes) para que sean los destinos de mensajes de captura activados por eventos. Estos mensajes informan al dispositivo de gestión acerca de eventos como un arranque en frío o un error al no poder autenticar un dispositivo.

NOTA: La comunicación con el agente SNMP que se ejecuta en el módulo BMENUA0100 se puede establecer mediante direcciones IPv4 o IPv6.

Finalización del servicio SNMP

El servicio SNMP que se ejecuta en el módulo BMENUA0100 finaliza si:

- El módulo está en el estado ERROR.
- El servicio SNMP está en el estado FALLO.

Acceso a la ficha SNMP

Haga doble clic en el módulo BMENUA0100 de la configuración Control Expert para acceder a la ficha **SNMP**.

El agente SNMP puede conectarse y comunicarse con 1 o 2 administradores SNMP. El servicio SNMP incluye:

- Comprobación de autenticación mediante el módulo BMENUA0100 de cualquier administrador SNMP que envíe peticiones SNMP.
- Gestión de eventos o capturas.

Configuración del agente SNMP en Control Expert y en las páginas web

Los parámetros de SNMP comunes se configuran en Control Expert. Los parámetros de SNMP relacionados con la ciberseguridad se configuran en las páginas web del módulo.

Si el conmutador rotativo de ciberseguridad está ajustado en:

- Modalidad Advanced (o Secured): puede configurar el agente SNMP tanto en Control Expert como en las páginas web del módulo .

NOTA: En la modalidad Advanced (o Secured), la versión de SNMP debe configurarse de la misma manera tanto en Control Expert como en la [página web de SNMP](#), [página 107](#). Si estas configuraciones no son idénticas, el servicio SNMP no se inicia.

- Modalidad Standard: solo puede configurar el agente SNMP en Control Expert.

NOTA: Si el módulo está configurado para SNMP V3 en Control Expert:

- El módulo BMENUA0100.2, equipado con la versión 2 o posterior del firmware, funciona con SNMP V3 con el nivel de seguridad SinAutSinPriv.
- El módulo BMENUA0100, con una versión anterior a la versión 2 del firmware, funciona con SNMP V1.

Parámetros SNMP

La ficha Control Expert **SNMP** incluye los siguientes parámetros. A menos que se indique lo contrario, los parámetros se aplican a SNMP V1 y V3.

NOTA: En la modalidad Advanced (o Secured), la versión de SNMP debe configurarse de la misma manera tanto en Control Expert como en la [página web de SNMP](#), [página 107](#). Si estas configuraciones no son idénticas, el servicio SNMP no se inicia.

Campo	Parámetro	Descripción	Valor
Versión de SNMP	SNMP V1	Seleccione esta opción para utilizar SNMP V1.	seleccionado/borrado
	SNMP V3	Seleccione esta opción para utilizar SNMP V3.	
Direcciones IP de los administradores	Dirección IP del administrador 1	Dirección IPv4 del primer administrador SNMP al que el agente SNMP envía avisos de capturas.	Depende del protocolo (IPv4).
	Dirección IP del administrador 2	Dirección IPv4 del segundo administrador SNMP al que el agente SNMP envía mensajes de capturas.	
Agente	Ubicación (SysLocation)	ubicación del dispositivo	31 caracteres (máximo)
	Contacto (SysContact)	información sobre la persona de contacto para el mantenimiento del dispositivo	
	Habilitar administrador SNMP	<i>borrado</i> (predeterminado): Puede editar los parámetros Ubicación y Contacto . <i>seleccionado</i> : No puede editar los parámetros Ubicación y Contacto .	seleccionado/borrado
Nombres de comunidad (solo SNMP V1)	Set	Contraseña necesaria para que el agente SNMP pueda leer los comandos de un administrador SNMP NOTA: No hay ningún ajuste predeterminado. Si se utiliza un administrador SNMP, introduzca el mismo nombre de comunidad que el que utiliza el administrador SNMP.	15 caracteres (máximo)
	Get		
	Trap		

Campo	Parámetro	Descripción	Valor
Seguridad (solo SNMP V1)	Activar captura de Fallo de autenticación	<i>borrado</i> (predeterminado): no activado. <i>seleccionado</i> : Habilitado. El agente SNMP envía un mensaje de captura al administrador SNMP en el caso de que un administrador no autorizado envíe un comando Get o Set al agente.	seleccionado/borrado
Nombre de usuario SNMP (solo SNMP V3)		Nombre de usuario reconocido por el servidor SNMP.	Cadena de 32 caracteres máx. ASCII / UTF8 en el rango de codificación [33-122]

Capturas compatibles

De manera predeterminada, el agente SNMP V1 del módulo BMENUA0100 admite las siguientes capturas:

- Conexión activada
- Conexión desactivada

La captura de **Fallo de autenticación** también se admite si está activada.

Identificadores de objeto MIB-II SNMP

En el **Nombre de proveedor** Schneider Electric, el módulo BMENUA0100 presenta los siguientes valores de identificadores de objeto (OID):

Nombre del objeto	OID	Valor
SysDesc	1.3.6.1.2.1.1.1	Producto: módulo de comunicación BMENUA0100 - OPC UA. ID de firmware: 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, que representa la suma de $(2_{7-1} + 2_{4-1} + 2_{2-1})$ e indican compatibilidad de protocolos en las siguientes capas OSI: <ul style="list-style-type: none">• 7: capa de aplicación• 4: capa de transporte• 2: capa de conexión de datos
ifDesc	1.3.6.1.2.1.2.2.1.2	Este OID contiene información que describe la interfaz, lo que incluye el nombre del producto y el nombre del puerto.

Configuración de los ajustes del controlador M580 para las conexiones cliente/servidor de OPC UA

Introducción

En esta sección se describen los ajustes realizados en la configuración del controlador M580 para admitir conexiones entre el servidor OPC UA del módulo BMENUA0100 y un cliente OPC UA.

Configuración de los ajustes de seguridad del controlador M580

Configuración de servicios del controlador

Para admitir la comunicación entre el servidor OPC UA del módulo BMENUA0100 y un cliente OPC UA, habilite los ajustes siguientes en la ficha Seguridad del controlador M580:

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

Si ninguno de estos dos servicios está habilitado en el controlador, la comunicación OPC UA no funcionará correctamente.

Diagnóstico

Descripción general

En este capítulo se describen las herramientas de diagnóstico disponibles para el módulo de comunicación Ethernet BMENUA0100 con servidor OPC UA integrado.

Diagnóstico mediante indicadores LED

Diagnóstico mediante indicadores LED del panel de visualización

A continuación se presentan los diferentes estados de funcionamiento de los indicadores LED del panel de visualización, página 26 del módulo BMENUA0100.

NOTA: Se presenta por separado el estado del indicador LED **SECURE** para el estado configurado y no configurado del módulo, después de la presentación inicial.

Estado de funcionamiento		Indicadores LED						
		RUN (Ver-de)	UACNX (verde/ rojo)	ERR (Rojo)	BS (verde/ rojo)	NS LED (verde/ rojo)	BUSY (amari- llo)	SEC (verde/rojo)
Secuencia de encendido	1	Apaga-do	Encendido	Encen-dido	Verde apagado Rojo encendido	Verde apagado Rojo encendido	Apagado	Verde apagado Rojo encendido
	2 (todos los indicadores LED encendi-dos)	Encen-dido	Encendido	Encen-dido	Verde encendido Rojo encendido	Verde encendido Rojo encendido	Encendi-do	Verde encendido Rojo encendido
	3 (todos los indicadores LED apagados)	Apaga-do	Apagado	Apaga-do	Verde apagado Rojo apagado	Verde apagado Rojo apagado	Apagado	Verde apagado Rojo apagado
	4	Encen-dido	Apagado	Encen-dido	Verde apagado Rojo apagado	Verde apagado Rojo apagado	Apagado	Verde apagado Rojo apagado
	5 (prueba automáti-ca ¹)	Inter-miten-cia	Intermiten-te	Intermi-tencia	Verde intermitente Rojo apagado	Verde intermitente Rojo apagado	Intermi-tencia	Verde intermitente Rojo apagado
Sin configurar		Apaga-do	Apagado	Intermi-tencia	Parpadea en rojo si no está conectado a un puerto de placa de conexiones Ethernet. De lo contrario, parpadea en verde.	Apagado si no hay ningún cable enchufado y conectado a otro dispositivo alimentado. De lo contrario, parpadea en verde.	Apagado	Consulte los indicadores LED de ciberseguri-dad a continuación, página 145.

Estado de funcionamiento		Indicadores LED						
		RUN (Verde)	UACNX (verde/rojo)	ERR (Rojo)	BS (verde/rojo)	NS LED (verde/rojo)	BUSY (amarillo)	SEC (verde/rojo)
Configuración	Al detectar una dirección IPv4 duplicada en el puerto de la placa de conexiones	Intermitencia	Consulte la descripción del indicador LED UACNX a continuación, página 144	/	Verde apagado Rojo encendido	/	/	Consulte la descripción del indicador LED de estado de comunicación segura a continuación, página 145.
	Después de detectar una dirección IPv4 duplicada en el puerto de control	Intermitencia		/	/	Verde apagado Rojo encendido	/	
	Estado de RUN	Encendido		Apagado	Verde encendido Rojo apagado	Verde fijo si está conectado; apagado si está desconectado.	Encendido si la adquisición de diccionarios de datos está en curso; intermitente en caso de desborde del diccionario de datos; en cualquier otro caso, apagado	
Sin alimentación		Apagado	Apagado	Apagado	Verde apagado Rojo apagado	Verde apagado Rojo apagado	Apagado	Verde apagado Rojo apagado
Error detectado recuperable o configuración incoherente ²		/	/	Encendido	/	/	/	/

Estado de funcionamiento		Indicadores LED						
		RUN (Verde)	UACNX (verde/rojo)	ERR (Rojo)	BS (verde/rojo)	NS LED (verde/rojo)	BUSY (amarillo)	SEC (verde/rojo)
Error detectado no recuperable (el módulo se reiniciará)		Apagado	Apagado	Encendido	Verde apagado Rojo encendido	Verde apagado Rojo encendido	Apagado	Verde apagado Rojo encendido
Cybersecurity (o Security) Reset	En progreso	Intermitencia	OFF	Apagado	Verde apagado Rojo encendido	Verde apagado Rojo encendido	Encendido	Verde apagado Rojo apagado
	Completado	Encendido	Apagado	Apagado	Verde apagado Rojo encendido	Verde apagado Rojo encendido	Apagado	Verde apagado Rojo apagado
Falta Cybersecurity (o Security) Reset ³		Apagado	Apagado	Encendido	Verde apagado Rojo encendido	Verde apagado Rojo encendido	Apagado	Parpadeo rojo
Actualización del SO		Intermitencia	OFF	Apagado	Verde apagado Rojo encendido	Verde apagado Rojo encendido	Encendido	Verde apagado Rojo apagado
<div>1. La prueba automática se realiza rápidamente, por lo que el parpadeo del indicador LED no se puede detectar visualmente. NOTA: Si el módulo permanece en estado de prueba automática, compruebe el conmutador rotativo para confirmar que está en una posición válida.</div> <div>2. Consulte los códigos de error detectado SERVICES_STATUS del DDT de T_BMENUA0100, página 147.</div> <div>3. Este estado es el resultado de cambiar el conmutador rotativo de modalidad Standard a Advanced (o Secured,) o de Advanced (o Secured) a Standard, sin realizar un Cybersecurity (o Security) Reset, página 31 como paso intermedio. NOTA: En esta tabla, "/" indica cualquier estado.</div>								

Indicador LED UACNX cuando el módulo está en estado configurado

El color (rojo o verde) y el estado (parpadeo o fijo) describen el estado de las conexiones OPC UA:

Estado del diccionario de datos	Estado de la conexión del cliente OPC UA	
	No hay ningún cliente OPC UA conectado	Hay al menos 1 cliente OPC UA conectado
Diccionario de datos no disponible	Parpadeo rojo	Rojo fijo
Diccionario de datos disponible	Parpadeos en verde	Verde fijo

Indicador LED de estado de comunicaciones seguras con el módulo en estado configurado/no configurado

A continuación, se describen los estados del indicador LED **SECURE** cuando el módulo se encuentra en el estado configurado o no configurado:

Estado de LED	Descripción
Apagado	El módulo no funciona en modalidad de funcionamiento seguro (es decir, el conmutador rotativo no está ajustado en la posición segura).
Rojo	Se ha detectado un error crítico en las comunicaciones seguras. Por ejemplo, no hay ninguna configuración de seguridad presente, un certificado no es válido, ha caducado un certificado y las comunicaciones se han detenido, etc.
Verde	Comunicaciones seguras habilitadas y en ejecución sin errores detectados. Hay un cliente conectado al módulo y este último ha recibido una configuración de ciberseguridad válida. La sesión está abierta y el módulo está listo para responder a las peticiones del cliente.
Rojo intermitente	Comunicaciones seguras habilitadas y en ejecución, pero se ha detectado un error. Por ejemplo, un certificado ha caducado, pero la configuración autoriza la continuidad de las comunicaciones.
Verde intermitente	El módulo ha recibido una configuración de ciberseguridad válida y está listo para comunicarse con un cliente que iniciará una comunicación.

Diagnóstico mediante indicadores LED del puerto de control

Los indicadores LED del puerto de control, página 27 permiten diagnosticar el estado de las comunicaciones Ethernet a través del puerto de control:

Indi- cador LED	Estado	Descripción
ACT	Apagado	No se ha establecido ninguna conexión.
	Verde	Conexión establecida, sin actividad.
	Parpadeos en verde	Conexión establecida, actividad detectada.
LNK	Apagado	No se ha establecido ninguna conexión.
	Amarillo	Conexión establecida a una velocidad inferior a la capacidad máxima del módulo (10/100 Mbps).
	Verde	Conexión establecida a una velocidad equivalente a la capacidad máxima del módulo (1000 Mbps).

Tipo de datos derivados (DDT) del módulo BMENUA0100

Introducción

Cada módulo de comunicación Ethernet BMENUA0100 con servidor OPC UA integrado que agregue a su aplicación creará una instancia de una colección común de elementos de datos. Puede usar las herramientas presentadas en el software Control Expert para acceder a estos elementos de datos y diagnosticar el módulo.

NOTA:

- Los datos del DDT devueltos en respuesta a una petición Modbus no pueden exceder los 256 bytes de longitud.
- Dada la organización del diccionario de datos de Control Expert, las peticiones de datos almacenados en bits de palabras debe extraerlas el cliente solicitante.

Para acceder al contenido del DDT, se utiliza la función elemental `READ_DDT`, página 152 (EF) en el software Control Expert.

s

NOTA: Si el DDT del módulo no se puede leer por algún motivo (por ejemplo, si la dirección IP de la placa de conexiones no está configurada correctamente), puede realizar diagnósticos del módulo a través de los indicadores LED, página 141 del módulo.

Estructura del DDT de T_BMENUA0100

El DDT del módulo BMENUA0100 incluye los siguientes elementos:

Elemento	Tipo	Dirección	Descripción
DEVICE_NAME	STRING [16]	MW1...8	Nombre del módulo.
CONTROL_PORT_IPV6	STRING [44]	MW9...30	Puerto de control IPv6/longitud de prefijo de subred.
CONTROL_PORT_IPV4	STRING [18]	MW31...39	Puerto de control IPv4/longitud de prefijo de subred.
CONTROL_PORT_GTW	STRING [16]	MW40...47	Pasarela predeterminada del puerto de control.
ETH_BKP_PORT_IPV4	STRING [18]	MW48...56	Puerto de placa de conexiones IPv4/longitud de prefijo de subred.
ETH_STATUS	WORD	MW57	–
PORT_CONTROL_LINK	BOOL	MW57.0	<ul style="list-style-type: none">0: La conexión del puerto de control no está operativa.1: La conexión del puerto de control está operativa.
ETH_BKP_PORT_LINK	BOOL	MW57.1	<ul style="list-style-type: none">0: La conexión del puerto de la placa de conexiones no está operativa.1: La conexión del puerto de la placa de conexiones está operativa.
GLOBAL_STATUS	BOOL	MW57.2	<ul style="list-style-type: none">0: el módulo no está operativo.1: el módulo está operativo.
NETWORK_HEALTH	BOOL	MW57.3	<ul style="list-style-type: none">0: se ha detectado una condición de sobrecarga de red.1: la red funciona con normalidad.
Reserved	–	MW57.4...15	–
OPCUA_STATUS	T_OPCUA_STATUS	MW58...61	Consulte los detalles a continuación.

Elemento	Tipo	Dirección	Descripción
DATA_DICT	BYTE	MW58[0]	<ul style="list-style-type: none"> 1: No disponible. Causas posibles: <ul style="list-style-type: none"> La función de diccionario de datos no está disponible o no está habilitada en la aplicación Control Expert y no se puede integrar en el controlador. Hay una carga/un examen del diccionario de datos en curso en el servidor OPC UA. 2: Disponible, por ejemplo: <ul style="list-style-type: none"> El servidor OPC UA completó correctamente la carga/el examen del diccionario de datos. Puede haber una carga previa (de acuerdo con los ajustes del proyecto del diccionario de datos de Control Expert) en curso. 4: Ocupado. 8: Desborde del diccionario de datos.
DATA_DICT_ACQ_DURATION	BYTE	MW58[1]	Duración de la última adquisición (0...255 segundos). NOTA: Un valor de 255 indica una duración igual o mayor que 255 segundos.
CONNECTED_CLIENTS	BYTE	MW59[0]	Número de clientes OPC UA conectados.
DATA_DICT_PRELOAD_DURATION	BYTE	MW59[1]	Duración de la última carga previa del diccionario de datos (0...255 segundos). NOTA: Puede utilizar la información incluida en este elemento para ajustar y optimizar el ajuste Tiempo de espera efectivo de cambios de compilación en la ventana Herramientas > Ajustes del proyecto > General > Datos incorporados del PLC . Consulte la ayuda en línea de Control Expert para obtener información sobre cómo configurar este ajuste.
REDUNDANCY_MODE	BYTE	MW60[0]	<ul style="list-style-type: none"> 0: Ninguno 2: Modalidad de redundancia no transparente ("Warm"). 3: Modalidad de redundancia no transparente ("Hot").
SERVICE_LEVEL	BYTE	MW60[1]	Estado del servidor OPC UA, página 159, según los datos y la calidad del servicio.
Reserved	WORD	MW61	—
SERVICES_STATUS	T_SERVICES_STATUS	MW62...68	Consulte los detalles a continuación.

Elemento	Tipo	Dirección	Descripción
NTP_CLIENT_SERVICE	BYTE	MW62[0]	<p>Estado del cliente NTP:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bits 4...7: Código de error detectado: <ul style="list-style-type: none"> ◦ 1 = Hora no válida (hora nunca actualizada) ◦ 2 = recuperación de tiempo (el tiempo del servidor ha aumentado o disminuido en una compensación de al menos 1000 segundos. El módulo BMENUA0100 puede tardar hasta 5 minutos en volver a sincronizarse). ◦ 4 = el servidor NTP sigue siendo accesible, pero no sincroniza el cliente. Cuando el servidor NTP reanude sus operaciones, el error detectado se resolverá automáticamente. Este proceso puede tardar hasta 1024 segundos.
NTP_SERVER_SERVICE	BYTE	MW62[1]	<p>Estado del servidor NTP:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bits 4...7: Código de error detectado: solo en la modalidad Advanced (o Secured): <ul style="list-style-type: none"> ◦ 1 = Puerto de control no configurado ◦ 2 = Cliente NTP de placa de conexiones y servidor habilitado en páginas web
SNMP_SERVICE	BYTE	MW63[0]	<p>Estado del servidor SNMP:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bit 1 (SNMP V1): 0 = SNMP no configurado/1 = SNMP configurado • Bits 1 y 2: (SNMP V3): 00 = SNMP no configurado/11 = SNMP configurado • Bits 4...7: Código de error detectado: <ul style="list-style-type: none"> ◦ 1 = SNMP está habilitado en la modalidad Advanced (o Secured), pero no se ha definido ninguna dirección IP de SNMP en Control Expert (0.0.0.0)
Reserved	BYTE	MW63[1]	—
WEB_SERVER	BYTE	MW64[0]	<p>Estado del servidor web:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bits 4...7: Código de error detectado: <ul style="list-style-type: none"> ◦ 1 = Error detectado no recuperable

Elemento	Tipo	Dirección	Descripción
FW_UPGRADE	BYTE	MW64[1]	<p>Estado de actualización del firmware:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bits 4...7: Código de error detectado: <ul style="list-style-type: none"> ◦ 1 = paquete de firmware no válido ◦ 2 = La última actualización del firmware no se realizó correctamente (se gestionó como un error detectado no recuperable)
Reserved	BYTE	MW65[0]	—
Reserved	BYTE	MW65[1]	—
CONTROL_EXPERT_IP_FORWARDING	BYTE	MW66[0]	<p>Estado de reenvío de IP de Control Expert:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bits 4...7: Código de error detectado (solo en la modalidad Advanced [o Secured]): <ul style="list-style-type: none"> ◦ 1 = Puerto de control no configurado <p>NOTA: Para los módulos con versión de firmware 2.01 y posteriores, el valor de este elemento se fuerza a 0.</p>
CPU_TO_CPU_IP_FORWARDING	BYTE	MW66[1]	<p>Estado de reenvío de controlador al controlador:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bits 4...7: Código de error detectado (solo en la modalidad Advanced [o Secured]): <ul style="list-style-type: none"> ◦ 1 = Puerto de control no configurado <p>NOTA: Para los módulos con versión de firmware 2.01 y posteriores, el valor de este elemento se fuerza a 0.</p>
IPSEC	BYTE	MW67[0]	<p>Estado de IPsec:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bits 4...7: Código de error detectado (solo en la modalidad Advanced [o Secured]): <ul style="list-style-type: none"> ◦ 1 = Puerto de control no configurado
Reserved	BYTE	MW67[1]	—
EVENT_LOG_SERVICE	BYTE	MW68[0]	<p>Estado del servicio de registros de eventos:</p> <ul style="list-style-type: none"> • Bit 0: 0 = Inactivo/1 = Activo • Bits 4...7: Código de error detectado (solo en la modalidad Advanced [o Secured]): <ul style="list-style-type: none"> ◦ 1 = Error detectado en el registro de eventos de servicios ◦ 2 = Error detectado en la configuración del registro de eventos

Elemento	Tipo	Dirección	Descripción
LOG_SERVER_NOT_REACHABLE	BYTE	MW68[1]	Estado del servidor de registro: <ul style="list-style-type: none"> Bit 0: 0 = Confirmación recibida del servidor Syslog/1 = No se recibe confirmación del servidor Syslog
FW_VERSION	T_FW_VERSION	MW69...72	Versión del firmware del módulo. Consulte los detalles a continuación.
MAJOR_VERSION	WORD	MW69	Versión principal del firmware.
MINOR_VERSION	WORD	MW70	Versión secundaria del firmware.
INTERNAL_REVISION	WORD	MW71	Revisión interna del firmware.
Reserved	WORD	MW72	–
CONTROL_PORT_STATUS	BYTE	MW73[0]	Estado de IPv4 del puerto de control: <ul style="list-style-type: none"> Bit 0: 0 = Inactivo/1 = Activo Bits 4...7: Código de error detectado (solo en la modalidad Advanced [o Secured]): <ul style="list-style-type: none"> 1 = IP no válida 2 = IP duplicada
Reserved	BYTE	MW73[1]	–
IN_PACKETS_RATE	UINT	MW74	Número de paquetes recibidos por segundo en todas las interfaces Ethernet.
IN_ERROR_COUNT	UINT	MW75	Número de paquetes entrantes con errores detectados desde el último reinicio (módulo 65535).
OUT_PACKETS_RATE	UINT	MW76	Número de paquetes emitidos por segundo en todas las interfaces Ethernet.
OUT_ERROR_COUNT	UINT	MW77	Número de paquetes salientes con errores detectados desde el último reinicio (módulo 65535).
MEM_USED_PERCENT	BYTE	MW78[0]	Porcentaje de RAM interna utilizado por el servidor OPC UA.
CPU_USED_PERCENT	BYTE	MW78[1]	Porcentaje de procesador interno utilizado.
CYBERSECURITY_STATUS	T_CYBER_SECURITY_STATUS	MW79...80	Estado de ciberseguridad. Consulte los detalles a continuación.
SECURE_MODE	BYTE	MW79[0]	<ul style="list-style-type: none"> 0: El módulo funciona en modalidad Standard. 1: El módulo funciona en la modalidad Advanced (o Secured).

Elemento	Tipo	Dirección	Descripción
CYBERSECURITY_STATE	BYTE	MW79[1]	Estado de ciberseguridad: <ul style="list-style-type: none">• 0: Modalidad Advanced (o Secured) desactivada. (LED SECURE APAGADO)• 1: Comunicaciones seguras habilitadas y en ejecución sin errores detectados (LED SECURE VERDE)• 2: Preparado para comunicarse. (LED SECURE PARPADEA EN VERDE)• 3: Comunicación segura en funcionamiento con errores menores detectados (LED SECURE PARPADEA EN ROJO)• 4: Las comunicaciones seguras se han detenido debido a que se ha detectado un error crítico (LED SECURE ROJO)
IPSEC_CHANNELS	BYTE	MW80[0]	Número de canales IPsec abiertos.
Reserved	BYTE	MW80[1]	–

Configuración de la función elemental READ_DDT

Descripción general

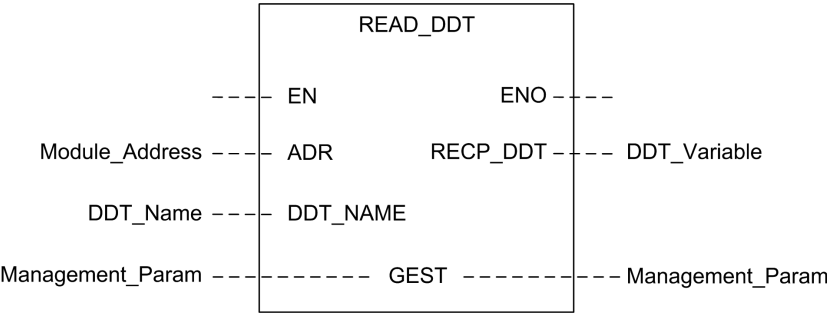
Utilice el bloque de funciones `READ_DDT` para configurar los mensajes de lectura del módulo de comunicación BMENUA0100.

Los parámetros `ADR`, `DDT_NAME` y `GEST` definen la operación.

Como parámetros adicionales se pueden configurar `EN` y `ENO`.

NOTA: Para obtener información sobre el uso de este bloque de funciones en un sistema de espera activa, consulte el tema Bloques de funciones de comunicación asíncrona (consulte *Guía del sistema de arquitecturas de uso frecuente Modicon M580 Hot Standby*).

Representación en el FBD



Parámetros de entrada

Parámetro	Tipo de datos	Descripción
EN	BOOL	Este parámetro es opcional. Si la entrada está establecida en uno, el bloque se activa, con lo que puede resolver el algoritmo de los bloques de funciones. Si la entrada está establecida en cero, el bloque se desactiva, con lo que no puede resolver el algoritmo del bloque de funciones.
ADR	Cualquier matriz de INT	Matriz que contiene la dirección de la entidad de destino de la operación de intercambio. La dirección es el resultado de la función ADDMX. (Por ejemplo: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) indica el módulo en la dirección IP 192.168.10.2, con UnitId 100 (servidor local del módulo), conectado al puerto Ethernet integrado.
DDT_NAME	STRING	Nombre del DDT que se debe leer: T_BMENUA0100

Parámetros de entrada/salida

La matriz GEST es local:

Parámetro	Tipo de datos	Descripción		
GEST	Matriz [0...3] de INT	Los parámetros de gestión, compuestos por cuatro palabras. Consulte el tema de ayuda de Control Expert <i>Estructura de los parámetros de gestión</i> (consulte <i>EcoStruxure™ Control Expert, Comunicación, Biblioteca de bloques</i>) para obtener más información sobre estos parámetros.		
		Palabra#	BYTE más significativo	BYTE menos significativo
		0	Número de intercambio	Bit de actividad: intervalo 0

Pará-me-tro	Tipo de datos	Descripción		
				Bit de cancelación: rango 1 Bit de confirmación inmediata: rango 2
		1	Informe de funcionamiento (consulte <i>EcoStruxure™ Control Expert, Comunicación, Biblioteca de bloques</i>)	Informe de comunicación (consulte <i>EcoStruxure™ Control Expert, Comunicación, Biblioteca de bloques</i>)
		2	Tiempo de espera (consulte <i>EcoStruxure™ Control Expert, Comunicación, Biblioteca de bloques</i>)	
		3	Longitud (consulte <i>EcoStruxure™ Control Expert, Comunicación, Biblioteca de bloques</i>)	

Parámetros de salida

Parámetro	Tipo de datos	Descripción
ENO	BOOL	Este parámetro es opcional. Al seleccionar esta salida, también se obtiene la entrada EN. La salida ENO se activa cuando se ejecuta correctamente el bloque de funciones.
RECP_DDT	Cualquiera	Búfer de recepción. Se puede utilizar una variable de DDT. Consulte en la descripción de los DDT de T_BMENUA0100, página 146 el contenido de estos DDT. El sistema escribe automáticamente el tamaño de los datos recibidos (en bytes) en la cuarta palabra de la tabla de gestión.

Bloque de funciones de comunicación asíncrona

En una aplicación Hot Standby y durante un evento de conmutación, el bloque de funciones de comunicación asíncrona READ_DDT no reanuda automáticamente el funcionamiento en el nuevo controlador primario, a menos que se configure específicamente, como se indica a continuación.

Siga el procedimiento siguiente para que los EFB de comunicación asíncrona puedan reanudar automáticamente el funcionamiento después de una conmutación:

- Programe la aplicación para que todas las instancias de las EFB no se intercambien con el controlador Standby. Para ello, deseccione el atributo **Intercambio en STBY** para la instancia de EFB.

Consideraciones a la hora de configurar la función

Cuando use la EF READ_DDT, tenga en cuenta lo siguiente:

- Si la aplicación incluye más de un BMENUA0100 en un bastidor, utilice instancias independientes de una matriz de palabras (WORD) para cada pin GEST. Cada bloque administra su propia matriz de palabras (WORD) de gestión.
- No tiene que especificar un valor para el parámetro de longitud en GEST[3] porque no hay datos que enviar. Al final de la operación (cuando el bit de actividad de GEST[0] se define como 0), la longitud se define con la longitud de los datos copiados en el parámetros de salida RECP_DDT si no se comunica ningún error detectado en GEST[1] o con un código de estado adicional. Consulte el tema de ayuda de Control Expert *Códigos de error de EFB con parámetro STATUS* (consulte *EcoStruxure™ Control Expert, Comunicación, Biblioteca de bloques*) para ver una descripción de estos valores de código de estado adicionales.
- Un valor de tiempo de espera de 0 indica que no hay tiempo de espera. En este caso, no se detectan los retrasos ni las pérdidas de comunicación que se produzcan durante la operación de intercambio. El parámetro RECP_DDT conserva su valor anterior. Para evitar esta situación, establezca el tiempo de espera en un valor distinto de cero.
- Si hay un informe de funcionamiento 16#01 (petición no procesada) o 16#02 (respuesta incorrecta) en la palabra GEST[1] de la tabla de gestión, puede comunicarse un código de estado adicional en el parámetro de longitud (GEST[3]). Los códigos de estado devueltos en este campo corresponden a un subintervalo de los posibles códigos del parámetro STATUS de los EFB de comunicación. Los valores posibles para READ_DDT son hex 30ss y hex 4001. Consulte el tema de ayuda de Control Expert *Códigos de error de EFB con parámetro STATUS* (consulte *EcoStruxure™ Control Expert, Comunicación, Biblioteca de bloques*) para ver una descripción de estos valores de código de estado adicionales.
- En función de los DDT especificados en el parámetro DDT_NAME, se realizan algunas comprobaciones de coherencia en los datos recibidos. Si se detecta una falta de coherencia, se establece el código 16#02 (respuesta incorrecta) en el byte de informe de funcionamiento (el byte más significativo de GEST[1]). Tenga en cuenta que el bloque no comprueba la validez del tipo de datos de la variable configurada como búfer de recepción (RECP_DDT). Compruebe que el tipo de datos de la variable conectada al parámetro RECP_DDT coincida con el tipo de datos recibido.

 **ADVERTENCIA**

FUNCIONAMIENTO INESPERADO DEL EQUIPO

- Compruebe que la variable de tipo DDT asociada al parámetro de salida RECP_DDT se corresponda con el tipo de datos escritos en el búfer de recepción.
- Compruebe que la dirección establecida en el parámetro ADR se corresponda con el módulo correcto, especialmente si hay varios módulos idénticos configurados en la misma red.

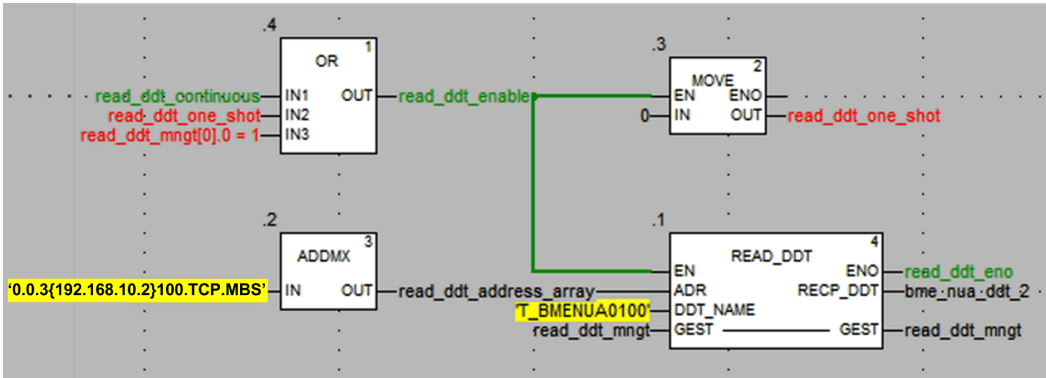
Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

Configuración de la función elemental READ_DDT

Para configurar la función elemental READ_DDT, siga estos pasos:

Paso	Acción
1	Establezca la dirección del dispositivo de destino en ADR (use un bloque ADDM para especificar esta dirección en un formato de cadena explícito).
2	Establezca el parámetro DDT_NAME con el nombre de los DDT que se deben leer.
3	Llame a la función READ_DDT para iniciar la comunicación (con el pin de entrada EN establecido en 1 si está configurado).
4	Vigile el bit de actividad (en el byte menos significativo del parámetro GEST[0]) hasta que se complete la comunicación (el sistema establece el bit de actividad en 0 cuando la comunicación ha finalizado). Ejecute esta función solamente una vez para no borrar los valores de estado. Por ejemplo, si establece el pin EN en 0 durante la operación, se llamaría de nuevo a la función.
5	Vea los parámetros del informe en GEST[1]. Si el informe indica 16#0000, el búfer RECP_DDT se ha llenado de datos recibidos. El tamaño de los datos recibidos (en bytes) se escribe en la cuarta palabra (GEST[3]) de la tabla de gestión.

Ejemplo de EF READ_DDT



En este ejemplo, la EF READ_DDT puede iniciarse:

- Continuamente, estableciendo la variable read_ddt_continuous.

NOTA: Si se detecta un error, los códigos del informe de la segunda palabra de la variable read_ddt_mngt no se pueden leer.

- Solo una vez, estableciendo la variable read_ddt_one_shot.

Configuración de la función elemental READ_NUA_DDT

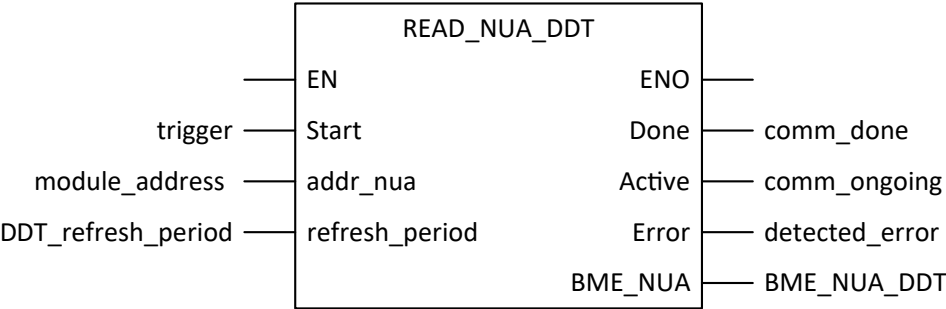
Utilice el bloque de funciones READ_NUA_DDT para acceder a la información de diagnóstico del módulo BMENUA0100.

Los parámetros de entrada Start, addr_nua y refresh_period definen la operación.

EN y ENO pueden configurarse como parámetros adicionales.

NOTA: Para obtener información sobre el uso de este bloque de funciones en un sistema de espera activa, consulte el tema Bloques de funciones de comunicación asíncrona (consulte *Guía del sistema de arquitecturas de uso frecuente Modicon M580 Hot Standby*).

Representación en el FBD



Parámetros de entrada

Parámetro	Tipo de datos	Descripción
EN	BOOL	Este parámetro es opcional. Si la entrada está establecida en uno, el bloque se activa, con lo que puede resolver el algoritmo de los bloques de funciones. Si la entrada está establecida en cero, el bloque se desactiva, con lo que ya no puede resolver el algoritmo de los bloques de funciones.
Iniciar	BOOL	La lectura del DDT de BMENUA0100 es continua.
addr_nua	string[32]	Dirección del módulo BMENUA0100 que se le proporciona a ADDMX() para la lectura. Cadena de longitud fija que contiene la dirección del módulo BMENUA0100 de destino. La dirección es el resultado de la función ADDMX. (Por ejemplo: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) indica el módulo en la dirección IP 192.168.10.2, con UnitId 100 (servidor local del módulo), conectado al puerto Ethernet integrado.
refresh_period	TIME	Período de actualización del DDT.

Parámetros de salida

Parámetro	Tipo de datos	Descripción
ENO	BOOL	Este parámetro es opcional. Al seleccionar esta salida también se obtiene la entrada EN. La salida ENO se activa al ejecutar correctamente el bloque de funciones.
Listo	BOOL	Comunicación finalizada.
Activo	BOOL	Comunicación en curso.

Parámetro	Tipo de datos	Descripción
Error	BOOL	Se detectó un error en el bloque de funciones de comunicación.
BME_NUA	T_BMENUA0100	DDT, página 146 del módulo BMENUA0100 que se puede utilizar tal cual.

Diagnóstico de OPC UA

Introducción

El módulo BMENUA0100 presenta variables del servidor OPC UA y elementos de datos específicos que se pueden usar para identificar la aplicación que se ejecuta en el módulo y para diagnosticar las operaciones del módulo.

Variable SERVICE_LEVEL de OPC UA

La variable SERVICE_LEVEL proporciona información a un cliente sobre el estado del controlador y el estado del servidor OPC UA. A la variable SERVICE_LEVEL se puede acceder directamente desde el árbol de nodos del servidor OPC UA. La variable SERVICE_LEVEL también está duplicada en el elemento OPCUA_STATUS.SERVICE_LEVEL de los DDT, página 147 del módulo BMENUA0100, y puede accederse a ella mediante programación ejecutando la función elemental READ_DDT, página 152 cuando el estado de la aplicación es RUN.

NOTA:

- En arquitecturas redundantes, el cliente OPC UA debe supervisar la variable SERVICE_LEVEL en los módulos BMENUA0100 primario y standby para gestionar el mecanismo de redundancia. Cuando el cliente detecta que el valor de SERVICE_LEVEL del módulo standby es mayor que el valor de SERVICE_LEVEL del módulo primario, el cliente debe activar una conmutación del módulo primario al módulo standby.
- SCADA debe supervisar SERVICE_LEVEL en todo momento durante el funcionamiento para garantizar el buen estado del servidor OPC UA.

Las siguientes variables de nivel de servicio se aplican a todas las versiones de firmware del módulo BMENUA0100, excepto en los casos indicados:

Valor de SERVICE_ LEVEL	Estado del controlador/servidor OPC UA	
	Firmware = V1.0	Firmware ≥ V1.1
0	BMENUA0100 está en fase de arranque. El estado del controlador es NOCONF o ERROR. Ejemplo de estado de ERROR: la tarea MAST está en estado HALT.	
1	El servidor OPC UA se ha iniciado. El examen de la lista del diccionario de datos está en curso.	
5	El examen del diccionario de datos se ha iniciado.	
10	Desborde del tamaño del diccionario de datos.	
20	El examen del tipo del diccionario de datos está en curso.	
50	El examen de la variable del diccionario de datos está en curso.	
100	El examen del diccionario de datos se ha completado. La lectura del estado del controlador está en curso. El espacio de direcciones se actualizará con el nuevo contenido del diccionario de datos.	
120 ¹	Controlador en estado STOP.	Controlador en estado STOP STANDBY o HALT STANDBY (solo controlador Hot Standby).
150 ¹	Controlador en estado WAIT STANDBY (solo controlador Hot Standby).	
199 ¹	Controlador en estado RUN STANDBY (solo controlador Hot Standby).	
202 ²	<No aplicable>	Solo Standalone_controller: controlador en estado STOP STANDALONE. Solo controlador Hot Standby: Cuando ambos controladores están en estado STOP o HALT, un módulo BMENUA0100 se declara como maestro con un nivel de servicio = 202. El espacio de dirección es correcto y puede utilizarse.
255	Controlador en RUN (o RUN PRIMARY para el controlador Hot Standby). El servidor OPC UA está completamente operativo	
1. No es necesario configurar este valor antes de que el servidor esté operativo. 2. Este nivel de servicio se aplica solo a las versiones de firmware V1.10 y posteriores del módulo BMENUA0100.		

NOTA: Cuanto mayor sea el tamaño del diccionario de datos, mayor será el tiempo de adquisición del diccionario de datos (es decir, el tiempo necesario para que el módulo examine y cargue el diccionario de datos). Durante la adquisición del diccionario de datos, SERVICE_LEVEL permanece en el valor 100 hasta que se completa la adquisición. Cuando se realiza un cambio de compilación en Control Expert que genera un nuevo diccionario de datos, el servidor OPC UA reinicia el proceso de examen del diccionario de datos. Durante este proceso, pueden detenerse las actualizaciones de los elementos supervisados, lo que provocará que los valores de los elementos supervisados se congelen en el valor de la actualización más reciente.

Variables del servidor OPC UA

Puede ver estas variables en línea con un dispositivo cliente OPC UA, como la herramienta UaExpert de Unified Automation. Vaya a **Estado del servidor > Información de compilación** en el árbol de nodos del servidor OPC UA para ver las siguientes variables del servidor OPC UA:

Variable	Descripción
BuildDate	La fecha de compilación de la aplicación en el controlador.
BuildNumber	El número de la compilación actual de la aplicación del controlador.
ManufacturerName	"Schneider Electric".
Nombre del producto	"BMENUA0100".
ProductUri	El identificador uniforme de recursos único asignado al módulo.
SoftwareVersion	La versión del firmware del módulo.

Elementos de datos específicos de OPC UA

El módulo BMENUA0100 admite los siguientes elementos de datos específicos. A estos elementos de datos se puede acceder mediante la pila del servidor OPC UA. Aunque son muy similares a los elementos de datos del controlador a los que se puede acceder mediante el software Control Expert, estos elementos de datos especiales no están conectados a símbolos del controlador y no se puede acceder a ellos mediante el software Control Expert:

Elemento de datos	Tipo de datos	Valor predeterminado	Descripción
#AddressSpaceState	INT16	0	El estado del espacio de direcciones, con su colección de objetos y nodos. Los valores posibles incluyen: 0. Vacío 1. Generado 2. Actualizando 3. Parcialmente generado (no existe ningún diccionario de datos en la aplicación o este presenta un desborde)
#ApplicationName	STRING	0	El nombre de la aplicación del controlador.
#ApplicationVersion	STRING	0	La versión de la aplicación del controlador.
#CurrentDataDictionaryItemsCount	INT32	0	Número de elementos del diccionario de datos que se han cargado en el servidor.
#CurrentMonitoredItemsCount	INT32	0	Número de elementos que supervisa el servidor.
#DeviceIdentity	STRING	0	El nombre de la referencia del controlador.
#PLCDataReady	BYTE	1	Supervisa el estado de carga del diccionario de datos del controlador: 1. El diccionario de datos del controlador no está disponible. Entre las posibles causas se incluyen las siguientes: <ul style="list-style-type: none"> La función de diccionario de datos no está disponible o no está habilitada en la aplicación Control Expert y no se puede integrar en el controlador. Hay una carga/un examen del diccionario de datos en curso en el servidor OPC UA. 2. El diccionario de datos del controlador está disponible, por ejemplo: <ul style="list-style-type: none"> El servidor OPC UA completó correctamente la carga/el examen del diccionario de datos. Puede haber una carga previa (de acuerdo con los ajustes del proyecto del diccionario de datos de Control Expert) en curso.
#PLCQualStatus	INT16	0	Supervisa el estado de comunicación de un controlador. Entre los valores (hexadecimales) posibles se incluyen los siguientes: <ul style="list-style-type: none"> 00C0 hex: La comunicación con el controlador es correcta.

Elemento de datos	Tipo de datos	Valor predeterminado	Descripción
			<ul style="list-style-type: none">• 0040 hex: No hay comunicación con el controlador durante un tiempo inferior al tiempo de espera del dispositivo (5 s).• 0 hex: el controlador no se ha identificado.
#TSEventItemsReady	BOOL	0	<p>Elemento de solo lectura que indica si en el origen se han explorado las variables con marca de tiempo y los dispositivos con marca de tiempo en el origen en la aplicación del controlador M580:</p> <ul style="list-style-type: none">• 0 = no examinado• 1 = examinado <p>NOTA: Este elemento solo tiene sentido cuando las marcas de tiempo están habilitadas en Control Expert y activadas para el módulo BMENUA0100 en cuestión.</p>
#TSEventSynchro	BOOL	0	<p>Elemento de lectura/escritura que, cuando se activa, envía un valor sincronizado a todos los dispositivos de marcas de tiempo de origen conectados al controlador M580 cada vez que se realiza una operación de escritura. El objetivo consiste en inicializar todos los elementos supervisados con marcas de tiempo con sus valores.</p> <ul style="list-style-type: none">• 0 = a la espera de activación• 1 = activado <p>NOTA:</p> <ul style="list-style-type: none">• El valor de este elemento aparecerá como 0. No se verá un valor de 1, ya que este solo existe momentáneamente y vuelve al valor de activación de 0 en espera.• Este elemento solo tiene sentido cuando las marcas de tiempo están habilitadas en Control Expert y activadas para el módulo BMENUA0100 en cuestión.

Syslog

Introducción

El módulo BMENUA0100 registra eventos en un búfer de diagnóstico local y, a continuación, envía un registro de estos eventos a un servidor Syslog remoto en el que se

almacenan y se ponen a disposición de los clientes Syslog. Para diagnosticar eventos anteriores, puede consultar los registros de eventos del servidor Syslog. Para los eventos en curso del módulo, puede usar las páginas web del módulo, página 166 con el fin de diagnosticar el estado del servicio Syslog y ver los eventos especificados en el búfer de diagnóstico.

El búfer local funciona como un búfer circular, en el que los eventos más recientes sobrescriben y sustituyen los eventos anteriores cuando el búfer está lleno.

El módulo almacena los eventos en la memoria volátil.

Los eventos registrados están relacionados con:

- Seguridad/autorización, página 165
 - o bien –
- Cambios importantes del sistema (registro de auditoría), página 166

El servicio Syslog se puede configurar en las páginas web, página 99 como parte de la configuración de ciberseguridad y, por lo tanto, solo puede estar activo cuando el módulo funciona en la modalidad Advanced (o Secured). Cuando el módulo funciona en la modalidad Standard, el servicio se desactiva.

El Syslog implementado en el módulo BMENUA0100 es compatible con IPv4 (versión del firmware 1.0 y posteriores) e IPv6 (versión del firmware 1.10 y posteriores).

NOTA: Syslog no es un protocolo nativamente seguro, sino que debe encapsularse en un canal seguro IPsec, página 106 mediante el puerto de control.

Estructura de mensajes de Syslog

El protocolo Syslog (RFC 5424) define cómo se intercambian los eventos entre el módulo y el servidor remoto. La estructura de mensajes de Syslog se expone a continuación:

Campo	Descripción				
PRI	Información del sitio y la gravedad (descripción ofrecida en las tablas siguientes).				
VERSION	Versión de la especificación del protocolo Syslog (Versión = 1 para RFC 5424).				
TIMESTAMP	<div>El formato de marca de tiempo se emite desde el RFC 3339 que utiliza el siguiente formato de fecha y hora de Internet ISO8601: YYY-MM-DDThh:mm:ss.nnnZ</div> <div>NOTA: -, T, :, . y Z son caracteres obligatorios y forman parte del campo de marca de tiempo. T y Z deben escribirse en mayúsculas. Z especifica que la hora es UTC.</div> <div>Descripción del contenido del campo de hora:</div> <table><tr><td>YYY</td><td>Year</td></tr><tr><td>MM</td><td>Month</td></tr></table>	YYY	Year	MM	Month
YYY	Year				
MM	Month				

Campo	Descripción	
	DD	Día
	hh	Hour
	mm	Minuto
	ss	Segundo
	nnn	Fracción de segundo en milisegundos (0 si no está disponible)
HOSTNAME	Identifica la máquina que envió originalmente el mensaje de Syslog: nombre de dominio completo (FQDN) o dirección IP estática IP de origen si FQDN no es compatible.	
APP-NAME	Identifica la aplicación que inicia el mensaje de Syslog. Contiene información que permite identificar la entidad que envía el mensaje (por ejemplo, subconjunto de referencia comercial).	
PROCID	Identifica el proceso, la entidad o el componente que envía el evento.	
MSGID	Identifica el tipo de mensaje con el que está relacionado el evento, por ejemplo HTTP FTP o Modbus.	
MESSAGE TEXT	<p>Este campo contiene información diversa:</p> <ul style="list-style-type: none">• Dirección del remitente: dirección IP de la entidad que genera el registro.• ID del interlocutor: ID del interlocutor si un elemento del mismo tipo (igual) está implicado en la operación (por ejemplo, el nombre de usuario para una operación de registro).• Dirección del interlocutor: dirección IP del interlocutor si en la operación hay un interlocutor.• Tipo: número único con el que se identifica un mensaje (se incluye la descripción en las tablas siguientes).• Comentario: cadena que describe el mensaje (se incluye la descripción en las tablas siguientes).	

Eventos relacionados con Seguridad/Autorización

- Error al abrir el canal seguro desde la pila OPC UA: por ejemplo, certificado no válido o certificado caducado.
- Sesiones de usuario correctas (inicio de sesión/contraseña) desde la pila OPC UA (inicio de sesión correcto)

NOTA: Si no hay conexión (modalidad Standard), el registro se deshabilita, por lo que no se crea un registro de la conexión correcta.

- Error en sesiones de usuario (inicio de sesión/contraseña) desde la pila OPC UA (inicio de sesión incorrecto)
NOTA: Si no hay conexión (modalidad Standard), el registro se deshabilita, por lo que no se crea un registro de la conexión incorrecta.
- Conexiones HTTPS correctas con o desde una herramienta (inicio de sesión correcto): por ejemplo, una conexión con el servidor web o una descarga de firmware mediante HTTPS.
- Error en conexiones HTTPS con o desde una herramienta: por ejemplo, inicio de sesión incorrecto al servidor web o descarga de firmware incorrecta mediante HTTPS.
- Desconexión correcta de sesión de usuario (cierre de sesión a petición) para HTTPS.
- Desconexión correcta de la sesión de usuario (cierre de sesión a petición) para OPC UA.
- Cierre de sesión automático: por ejemplo, en caso de que se supere el tiempo de espera de sesión inactiva para OPC UA o HTTPS.
- Error de comprobación de la integridad detectado: por ejemplo, error de firma digital detectado o error solo de integridad (hash) detectado.
- Cree un nuevo certificado.
- Quite los certificados locales. Con este fin, coloque el conmutador rotativo en la posición Cybersecurity (o Security) Reset para seleccionar esta modalidad de funcionamiento.
- Añada un nuevo certificado de cliente de la lista de autorizaciones del dispositivo.
- Elimine un certificado de cliente de la lista de autorizaciones del dispositivo.

Eventos relacionados con cambios importantes del sistema (registro de auditoría)

- Descarga de la configuración de ciberseguridad o de la aplicación en el dispositivo.
- Descarga de firmware en el dispositivo.
- Firma incorrecta de firmware que no se pudo descargar en el dispositivo.

Diagnósticos de páginas web de Syslog

Use las páginas web del módulo para diagnosticar el estado del servicio Syslog que se ejecuta en el módulo y para diagnosticar las partes especificadas del búfer de diagnóstico Syslog del módulo. También puede usar el elemento SERVICES_STATUS de los DDT, página 147 del módulo para ver el estado del servicio Syslog.

En el menú **Diagnósticos > Diagnósticos del registro de eventos**, use los siguientes comandos para ver el estado del servicio Syslog del módulo:

Parámetro	Descripción
Status	<ul style="list-style-type: none">Operativo: el módulo funciona en la modalidad Advanced (o Secured) y el servicio Syslog está habilitado.No operativo: el módulo funciona en la modalidad Advanced (o Secured), pero el servicio Syslog está deshabilitado.
Servidor de registro	<ul style="list-style-type: none">Accesible: se puede establecer una conexión con el servidor Syslog remoto.No accesible: no se puede establecer una conexión con el servidor Syslog remoto.

En el menú **Diagnóstico > Diagnóstico de registro de eventos**, en el menú **Búder de diagnóstico para leer**, introduzca la parte del búfer de diagnóstico que se va a leer.

Diagnóstico Modbus

Introducción

Puede usar los comandos del código de función Modbus para realizar diagnósticos en el módulo BMENUA0100. Los comandos Modbus solo pueden llegar al módulo por el puerto de la placa de conexiones. Modbus no es un protocolo inherentemente seguro, por lo que debe encapsular los comandos Modbus en IPsec.

En el módulo BMENUA0100 solo se admiten peticiones FC43/14 (identificación de dispositivo de lectura) y FC03 (para leer MW% de DDT).

Acceso a datos Modbus y modalidad de funcionamiento de ciberseguridad

- El método que podrá usar para acceder a los datos Modbus depende de la modalidad de funcionamiento de ciberseguridad. Si el módulo BMENUA0100 funciona en:
- Modalidad Standard: El módulo BMENUA0100 acepta el flujo de datos del cliente Modbus TCP/IP desde cualquier cliente que pueda acceder a la red Ethernet de la placa de conexiones. Utilice métodos de comunicación Modbus estándar, incluidos los bloques de funciones DATA_EXCH, MBP_MSTR, READ_VAR y WRITE_VAR, así como los comandos de Control Expert.

- Modalidad Advanced (o Secured): El módulo BMENUA0100 solo acepta el flujo de datos de cliente Modbus TCP/IP del controlador M580. Puede implementar el bloque DATA_EXCH en la aplicación. También se pueden utilizar los valores READ_VAR y WRITE_VAR.

NOTA: Para dirigirse al servidor Modbus en el módulo, se debe utilizar el UnitID 100. Consulte la documentación de su cliente Modbus para obtener información en la que se describe cómo establecer este valor. Por ejemplo, al utilizar el bloque DATA_EXCH, puede configurarse UnitId con ADDMX de la siguiente manera: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS), donde 192.168.168.10.2 es la dirección IP de la placa de conexiones del módulo BMENUA0100.

43/14: lectura de identificación de dispositivo

Con el código de función 43/subcódigo 14 pueden devolverse los siguientes datos de identificación de dispositivo:

Categoría	ID de objeto	Nombre del objeto	Tipo
Básico	00 hex	Nombre de proveedor	Cadena ASCII
	01 hex	Código del producto	Cadena ASCII
	02 hex	Revisión principal/secundaria	Cadena ASCII
Normal	03 hex	URL del proveedor	Cadena ASCII
	04 hex	Nombre del producto	Cadena ASCII
	05 hex	Nombre del modelo	Cadena ASCII
	06 hex	Nombre de la aplicación de usuario	Cadena ASCII
	07 ...FF hex	Reserved	Cadena ASCII

Diagnóstico SNMP

Introducción

Cuando el agente SNMP está configurado, página 136, el módulo BMENUA0100 permite los diagnósticos SNMP en la red Ethernet basada en TCP/IP al admitir las MIB siguientes:

- MIB-II
- MIB Protocolo de detección de nivel de vínculo (LLDP)

MIB-II

MIB-II proporciona al administrador SNMP una colección de variables de administración de dispositivos. Al leer estas variables, el administrador SNMP puede diagnosticar el funcionamiento de un dispositivo específico, como BMENUA0100.

MIB LLDP

La MIB LLDP contiene datos recopilados mediante el uso del protocolo de detección de nivel de vínculo relativos a la identidad, las capacidades y la ubicación en la red Ethernet. Con la MIB LLDP, el administrador SNMP puede detectar la topología de la red y las capacidades de los dispositivos de red.

NOTA: La comunicación SNMP de los datos de la MIB LLDP se realiza exclusivamente mediante el puerto de la placa de conexiones.

Página web de diagnóstico de OPC UA

Use la página web **Diagnóstico de OPC UA** para ver datos dinámicos que describen el funcionamiento del servidor OPC UA integrado en el módulo BMENUA0100.

NOTA: La página web de **Diagnóstico de OPC UA** se actualiza cada 5 segundos.

Datos de diagnóstico

La página web **Diagnóstico de OPC UA** muestra los siguientes datos de solo lectura. Tenga en cuenta que todos los valores numéricos están en formato decimal:

Campo	Descripción
Diagnóstico de PLC	
EPAC	Dirección IP del controlador.
Identidad de dispositivo	Número de referencia del controlador.
Versión del dispositivo	Versión de firmware del controlador.
Device Status (Estado del dispositivo)	Estado de conexión con el controlador: Bueno, Malo, Incierto, Desconocido, Perdido.
Tiempo de espera de la trama (en ms)	Tiempo máximo durante el que el servidor OPC UA espera una respuesta de un dispositivo después de enviar una petición. Por ejemplo, 1000.

Campo	Descripción
Número máximo de canales	Número de conexiones abiertas por el servidor OPC UA en el controlador.
Canales utilizados para tareas que no sean marcas de tiempo	Número de conexiones que transportan datos de aplicación.
Canales utilizados para marcas de tiempo	Número de conexiones que transportan datos de marcas de tiempo, página 130.
Longitud de la petición	Longitud de la petición de comunicación con el controlador.
Nombre de la aplicación (dispositivo)	Nombre del proyecto de Control Expert.
Versión de la aplicación (dispositivo)	Suma de control y firmas de la aplicación.
Carga previa del diccionario de datos	Disponible o no disponible para la aplicación en el controlador.
Estado de marcas de tiempo	Se muestra el estado de las marcas de tiempo: <ul style="list-style-type: none">Las marcas de tiempo se habilitan con acceso a Variables con marca de tiempo en la aplicación.Las marcas de tiempo no se habilitan; no hay acceso a Variables con marca de tiempo.
Lista de dispositivos con marcas de tiempo de origen configuradas	Si las marcas de tiempo están habilitadas, se muestra una lista de dispositivos que indica lo siguiente para cada dispositivo: <ul style="list-style-type: none">Número de canales dedicados reservados para sondeo de origen de eventos con marca de tiempo.Tipo de dispositivo (BMECRA31310, controlador, etc.).Dirección IPv4.Reserva del búfer de marca de tiempo del dispositivo por parte del servidor integrado OPC UA del módulo BMENUA0100: TRUE/FALSE.
Diagnóstico de OPC UA	
URL del terminal (IPv4)	Dirección IPv4 del servidor OPC UA, con el formato: "opc.tcp://<dirección IPv4>:<número de puerto>". Por ejemplo: opc.tcp://192.168.2.142:4840
Velocidad de muestreo rápida	Indica si se selecciona el ajuste de la velocidad de muestreo rápida, página 124: <ul style="list-style-type: none">TRUE = seleccionadoFALSE = no seleccionado
Número de sesiones conectadas	Número total de sesiones de cliente admitidas por el servidor OPC UA integrado del módulo BMENUA0100.

Campo		Descripción
Información sobre suscripciones:		Información que describe las variables supervisadas por el servidor OPC UA que se incluyen en una o varias suscripciones.
	Número de elementos supervisados desde el nodo interno del servidor:	
	Número de elementos supervisados específicos:	
	Número de elementos supervisados no específicos:	
	Número de elementos supervisados con marca de tiempo con la modalidad de supervisión no deshabilitada:	
	Número total de elementos supervisados:	
Número actual de temporizadores		El número de intervalos de muestreo configurados para el servidor OPC UA integrado del BMENUA0100.
	Lista de temporizadores	Lista que describe cada uno de los intervalos de muestreo (es decir, temporizador) supervisados por el servidor OPC UA integrado del módulo BMENUA0100. Cada elemento indica: <ul style="list-style-type: none">• El intervalo de muestreo en ms.• El número de elementos supervisados.• El número de peticiones generadas durante la ejecución más reciente.

Optimización del rendimiento de BMENUA0100

Optimización del rendimiento de BMENUA0100

Introducción

Cuando optimice el rendimiento de BMENUA0100, tenga en cuenta todo el sistema. Preste especial atención a la eficiencia general de la comunicación y a la carga de trabajo de la arquitectura de red que incluye los módulos BMENUA0100. Es en este contexto en el que las optimizaciones del rendimiento del cliente OPC UA también influyen en la eficacia de la comunicación OPC UA.

Varios ajustes, a diferentes niveles de la arquitectura, pueden mejorar el rendimiento del sistema o hacer que su sistema sea más estable y robusto durante cada una de las fases de la modalidad de funcionamiento (conexiones, examen, suscripción, vigilancia, etc.).

NOTA:

- Añada elementos a paquetes con un tamaño máximo de 2000 elementos. El intervalo de muestreo configurado solo es relevante si es mayor o igual que el tiempo de exploración del controlador MAST.
- Ajuste CallTimeout en un valor mayor o igual que 10 segundos en el cliente OPC UA.
- El ajuste de General.SecureChannelLifetime para la comunicación con un cliente OPC UA está establecido de forma predeterminada en 3 600 000 ms (1 hora). Use esta configuración predeterminada para evitar disminuir el rendimiento.
- El rendimiento del sistema depende en gran medida de la configuración (por ejemplo, el número de clientes conectados, el número de variables gestionadas, etc.).
- Por ejemplo, con 2000 elementos supervisados, la velocidad de actualización solo se puede lograr en 20 ms si los valores de un máximo de 500 elementos cambian entre dos iteraciones de publicación consecutivas.

Ejemplo de rendimiento

Un cliente OPC UA puede vigilar hasta 20 000 elementos en la modalidad de ciberseguridad Standard.

Ejemplo basado en:

- BMEP584040 con un tiempo de ciclo de la tarea MAST de 20 ms (carga de la CPU de menos del 80 %).
- BMENUA0100 en posición Standard del conmutador rotativo (es decir, sin comunicación segura y sin canal IPsec).
- El cliente OPC UA (UAExpert) inicia la comunicación con la modalidad de seguridad de los mensajes configurada como **Ninguna** y vigila 20 000 elementos haciendo referencia a variables basadas en una matriz del tipo "INT" de un servidor OPC UA de BMENUA0100. Este servidor está configurado con un intervalo de publicación de 1 segundo, un intervalo de muestreo de 1 segundo y un tiempo de espera de sesión de 30 segundos.
- No existe más comunicación que la OPC UA.

Cómo ajustar el rendimiento

Estructura de datos de intercambio

La memoria de la aplicación de datos del controlador se organiza en función de la definición de la aplicación de datos de Control Expert. Cuanto más estructurada esté la declaración de variable, más optimizadas estarán las peticiones generadas por el servidor BMENUA0100 para acceder a las variables y al diccionario de datos en tiempo de ejecución.

Así, para las variables a las que accede el cliente OPC UA:

- Usar la estructura de datos o matrices siempre que sea posible.
- Habilitar la opción **Solo variable de HMI** en **Datos incorporador del PLC** en los **Ajustes del proyecto** y definir solo estas variables con el atributo **HMI** para reducir el tamaño del diccionario de datos.
- En la aplicación de seguridad del controlador, para reducir el tamaño del diccionario de datos, deseleccionar la opción **Uso del espacio de nombres de proceso** (en **Ajustes del proyecto > General > Datos incorporados del PLC > Diccionario de datos**).

Funcionalidades de comunicación del controlador

La capacidad del sistema de comunicación depende de la referencia del controlador M580 y de algunos ajustes de configuración. La referencia del controlador determina:

- Las capacidades de rendimiento del procesamiento del controlador en todo el sistema.
- El número de peticiones por ciclo que se pueden procesar, aunque pueda configurarlas la palabra del sistema %SW90.
- El número máximo de canales disponibles para cada BMENUA0100 con el fin de establecer conexiones con el controlador M580, página 182.

Además, cuanto menor sea el tiempo de ciclo de MAST, mayor será el número de peticiones de comunicación que se pueden procesar. Así, el nivel de rendimiento depende directamente del tiempo de ciclo de MAST.

Cliente OPC UA, configuración y uso

El número de variables vigiladas influye en el rendimiento. Las velocidades de muestreo y los intervalos de publicación configurados para cada cliente OPC UA determinan el número de peticiones necesarias para animar las variables. Recuerde que, cuando se conectan varios clientes OPC UA al mismo servidor OPC UA de BMENUA0100, si las velocidades de muestreo y los intervalos de publicación son diferentes en cada cliente OPC UA, esta configuración genera más peticiones.

Todos los valores de tiempo de espera configurables desde el cliente OPC UA (examen, conexión, publicación, sesión, watchdog...) deben ajustarse para optimizar y estabilizar (en la medida de lo posible) todo su sistema. Como efecto secundario, estos tiempos de espera pueden afectar al rendimiento del sistema.

En función de la modalidad de seguridad de los mensajes (Ninguna, Firmar, Firmar y cifrar), el algoritmo que calcula la firma y el cifrado necesita más tiempo.

Comunicaciones de controlador a controlador y Control Expert a controlador

Cada túnel IPsec usado para proteger comunicaciones diferentes de OPC UA o HTTPS ralentiza el tráfico, especialmente cuando se habilita el ajuste **Confidencialidad**, pues genera cifrado y descifrado.

Cómo vigilar el rendimiento

Existen varias formas de vigilar el rendimiento.

Con Control Expert

Con Control Expert en la modalidad de conexión, puede acceder al tiempo de ciclo de MAST efectivo y a la carga del controlador M580 del sistema para cada tarea y para el total de todas las tareas leyendo las palabras del sistema de %SW110 a %SW116. Además, los DDDT del controlador M580 y los DDT de BMENUA0100 pueden facilitar diferente información de diagnóstico relacionada con el rendimiento del sistema del controlador, como:

- El nivel de servicio del servidor OPC UA.
- El número de clientes OPC UA conectados.
- El estado, el tiempo de adquisición y la duración de la carga previa del diccionario de datos.
- El estado del servicio Ethernet.
- El estado de la red.
- El estado del puerto de control y el puerto de la placa de conexiones.
- El número de paquetes Ethernet por segundo.
- El número de paquetes Ethernet que contienen errores detectados.

- El porcentaje de carga de la CPU de BMENUA0100 y la memoria usada.
- Número de canales IPsec abiertos.

Con el sitio web de BMENUA0100

La página de inicio y la página de diagnóstico del sitio web de BMENUA0100 facilitan información interesante relacionada con el rendimiento de los servidores OPC UA. Alguna información procede de los DDT de BMENUA0100 y otra información la proporciona el propio servidor OPC UA:

- Número de elementos vigilados.
- Número de elementos específicos vigilados.
- Los diferentes intervalos de muestreo en ejecución en un momento dado.
- El número de peticiones generadas para las animaciones.
- Desbordes detectados.
- Número de clientes conectados.

Con el cliente OPC UA

El cliente OPC UA puede supervisar directamente algunos elementos específicos del servidor OPC UA, pero también la variable ServiceLevel o algunos subcampos de los DDT del módulo BMENUA0100 a petición mediante las variables de la aplicación.

Otros servicios de diagnóstico

En un enfoque más técnico, el agente SNMP y el servidor Syslog del módulo BMENUA0100 pueden ayudar a obtener otra información de diagnóstico relacionada con el rendimiento de los servidores OPC UA.

Solución de problemas del módulo BMENUA0100

Introducción

En este tema, se describen consejos que se pueden utilizar para mejorar el funcionamiento del módulo BMENUA0100.

Repercusiones del uso de UaExpert como cliente OPC UA

Si utiliza UaExpert como cliente OPC UA para leer valores de datos, tenga en cuenta que UaExpert incrementa el *recuento de suscripciones actual* por un valor de 1 para cada instancia de UAExpert.

NOTA: El *recuento de suscripciones actual* está relacionado con el propio servidor y no se debe confundir con el elemento relacionado de la sesión *Recuento de suscripciones actual*.

Periodo MAST y tiempo de adquisición del diccionario de datos

El tiempo necesario para cargar el conjunto de variables del diccionario de datos depende del número de elementos del diccionario de datos y del periodo MAST configurado. En el caso de una aplicación que requiera que el servidor OPC UA del módulo BMENUA0100 supervise un número que se acerca al máximo de 100 000 elementos, se han observado los siguientes resultados, que podrían resultar instructivos.

Para una aplicación no relacionada con la seguridad de 99 000 elementos:

Periodo MAST	Tiempo de adquisición del diccionario de datos observado
20 ms	23 s
100 ms	46 s
200 ms	74 s

Para una aplicación relacionada con la seguridad de 99 000 elementos:

Periodo MAST	Tiempo de adquisición del diccionario de datos observado
25 ms	15 s
200 ms	72 s

Configuración de suscripciones con más de 30 000 elementos supervisados

Si desea crear una o varias suscripciones que incluyen de forma colectiva más de 30 000 elementos supervisados, configure cada suscripción en el cliente OPC UA correspondiente

con un valor de **Contador de tiempo de vida** de 300 segundos, que representa el valor de **Duración máxima de suscripción**, página 37 que puede admitir el servidor OPC UA del módulo BMENUA0100.

Uso de GPO/LGPO

Gestione certificados en un PC host mediante una de las herramientas siguientes disponibles en el sistema operativo Windows™:

- Objetos de directiva de grupo (GPO) para realizar una administración centralizada de la configuración de usuario en un entorno de Active Directory centralizado, o bien
- Objetos de directiva de grupo local (LGPO) para la administración distribuida de la configuración de usuario para PC individuales.

En cualquier caso, el uso de GPO o LGPO puede evitar el acceso no autorizado al equipo y las aplicaciones. El uso de GPO y LGPO deshabilita el acceso a Microsoft Management Console (MMC) de Windows y solo admite la implementación de la lista de aprobadores configurada por el software.

Aplicación de la administración de directivas de grupo de MMC

Gestione certificados con las herramientas de Microsoft Windows™ para evitar que se añadan certificados no autorizados al PC o modifique certificados autofirmados de un cliente OPC UA. Si no se gestionan, alguien podría incluir certificados no autorizados en la lista de autorizaciones de BMENUA0100 gestionada por el administrador de seguridad.

Estas herramientas incluyen directivas de administración de directivas de grupo aplicadas por el objeto de directiva de grupo (GPO), un complemento de Microsoft Management Console (MMC). Diseñe sus directivas de modo que deshabiliten el acceso a la MMC de Windows y permitan el acceso únicamente a las entradas de configuración de la lista de autorizaciones que el software haya añadido correctamente.

Bloqueo del cliente OPC UA

Al conectar un cliente OPC UA que tiene un nombre de usuario asignado al servidor OPC UA integrado en el módulo BMENUA0100, se aplican los **ajustes de directiva de cuentas de usuario**, página 98 de BMENUA0100. Por ejemplo, si se alcanza o se excede el **Número máximo de intentos de iniciar sesión**, el cliente OPC UA no podrá iniciar sesión (**BadInternalError**) durante el tiempo establecido como **Tiempo de bloqueo de la cuenta**.

Activación de los servicios de red mediante una única conexión IPv6

El módulo BMENUA0100 solo admite el uso de IPv6 para la comunicación y el direccionamiento IP. Con solo IPv6 activado, [página 123](#), los servicios de red **Flujos de datos de CPU a CPU** y **Flujos de datos de Control Expert a la red de dispositivos** no estarán disponibles. Estos servicios solo son compatibles con IPv4.

Sin embargo, todavía es posible habilitar estas funciones en la página web **Configuración > Servicios de red**. Si estos servicios están habilitados cuando solo se activa IPv6, estos servicios (**CPU a CPU** y **CE a red de dispositivos**) aparecerán como activados en la página **Inicio**, pero en realidad no se activarán.

La comunicación IPv6 solo admite la función de filtrado de flujo de datos de **Flujos de datos de Control Expert a la CPU solamente**. En este caso, con solo la comunicación IPv6 activada, la página **Inicio** mostrará correctamente como activada la opción **De de CE a CPU solamente**.

Elementos BOOL considerados como BYTE en estructuras de datos de controlador

En el servidor OPC UA de BMENUA0100, cada elemento del DDT de controlador se asigna a un byte del controlador, incluso si se define como BOOL o EBOOL en el módulo BMENUA0100. Mediante el protocolo OPC UA, un cliente puede leer o escribir de forma global un miembro BOOL o EBOOL de una instancia de BMENUA0100 en el DDT del controlador con un valor de byte válido distinto de 0 o 1 (por ejemplo, 255). Diseñe la aplicación para que escriba o lea valores BOOL o EBOOL de únicamente 0 o 1, ya que solo estos valores son válidos en el módulo BMENUA0100.

Actualización del firmware

Herramienta EcoStruxure™ Automation Device Maintenance

Introducción a la herramienta EcoStruxure™ Automation Device Maintenance

Utilice la herramienta EcoStruxure™ Automation Device Maintenance para actualizar el firmware del módulo BMENUA0100. EcoStruxure™ Automation Device Maintenance es una herramienta web que permite:

- Detectar manualmente uno o varios módulos BMENUA0100 en el proyecto en función de las direcciones IP.
- Actualizar los módulos BMENUA0100 con la versión más reciente del firmware a través de Internet.

Antes de actualizar el firmware:

- Conéctese al BMENUA0100 en la función de instalador.
- Desconecte los clientes (web, OPC UA, otros controladores) conectados al módulo.

Para obtener información sobre cómo instalar y utilizar la herramienta EcoStruxure™ Automation Device Maintenance, consulte la ayuda en línea (consulte *EcoStruxure Automation Device Maintenance*, *Herramienta de actualización del firmware*, *Ayuda en línea*).

NOTA: La herramienta de software Unity Loader™ de Schneider Electric no se puede usar para actualizar el firmware del módulo BMENUA0100.

NOTA: Después de actualizar el firmware del módulo BMENUA0100 de la versión 1.xx a la versión 2.xx, si el BMENUA0100 se encuentra en modalidad Standard, debe realizar una operación de Security Reset, página 33 para restaurar la configuración predeterminada de fábrica del módulo. A continuación, seleccione una modalidad de funcionamiento de Cybersecurity (modalidad Advanced [o Secured] o Standard) para el módulo.

Cambiar a una versión anterior del firmware

Es posible volver a una versión anterior del firmware del módulo BMENUA0100, por ejemplo, de la versión 1.1 a la versión 1.0. Para ello, después de cambiar a una versión anterior del software con la herramienta EcoStruxure™ Automation Device Maintenance, realice una operación Cybersecurity (o Security) Reset, página 33 para restaurar los ajustes

predeterminados de fábrica del módulo. A continuación, seleccione una modalidad de funcionamiento de ciberseguridad (modalidad Advanced [o Secured] o Standard) para el módulo .

Apéndices

Contenido de esta parte

Conexiones del controlador	182
Arquitecturas de reenvío de servicios (IP)	183
Reenvío de IP y comunicación OPC UA	188
Scripts de Windows IPsec	190
Configuración de una autoridad de certificación de Windows	193

Conexiones del controlador

Contenido de este capítulo

Conexiones del servidor OPC UA al controlador.....

182

Conexiones del servidor OPC UA al controlador

Conexiones abiertas

El número de conexiones que puede abrir el módulo BMENUA0100 con el controlador M580 depende de la capacidad del controlador. Así, el rendimiento del módulo BMENUA0100 depende del tiempo necesario para realizar la tarea MAST y del controlador seleccionado. El número máximo de conexiones abiertas por cada módulo BMENUA0100 con el controlador M580 es el siguiente:

Modelo de controlador	Número máximo de conexiones abiertas por cada 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

Arquitecturas de reenvío de servicios (IP)

Contenido de este capítulo

Arquitecturas compatibles con el reenvío de servicios (IP)

Arquitecturas no compatibles con el reenvío de servicios (IP)

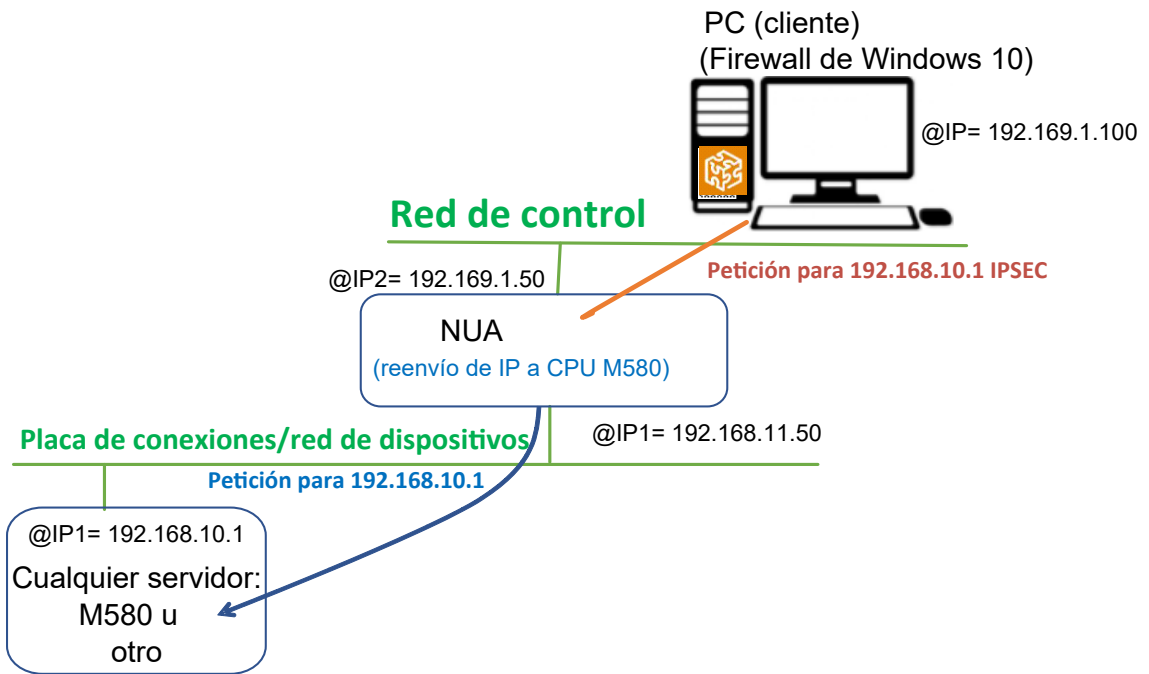
184

187

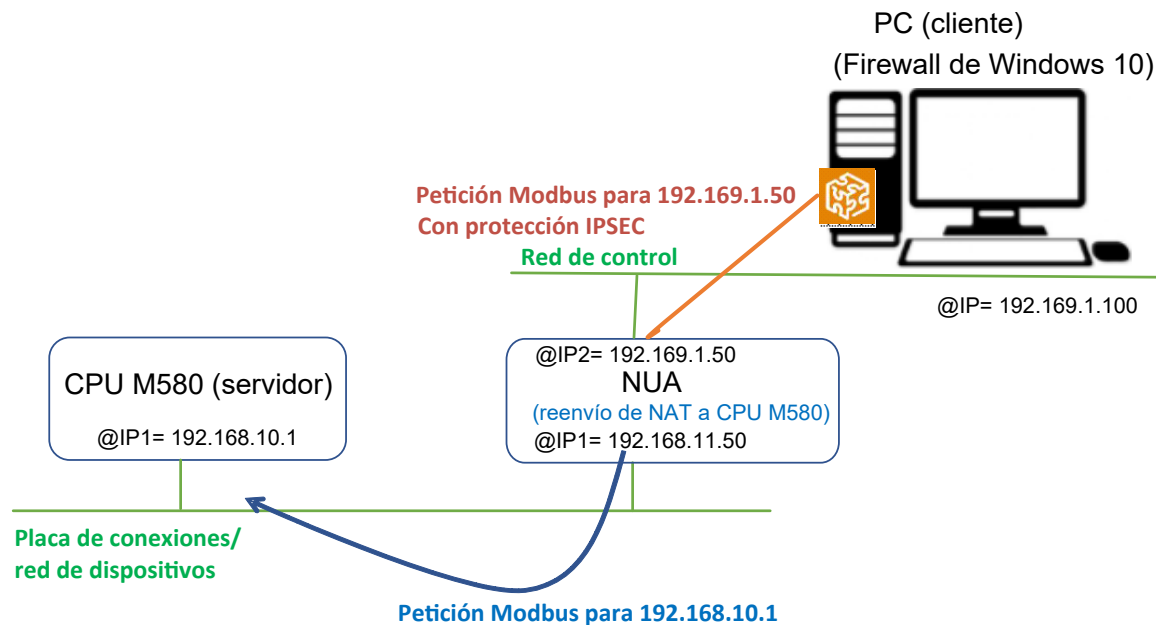
En este capítulo se presentan las arquitecturas compatibles y no compatibles con la función de reenvío de servicios (IP) del módulo BMENUA0100.

Arquitecturas compatibles con el reenvío de servicios (IP)

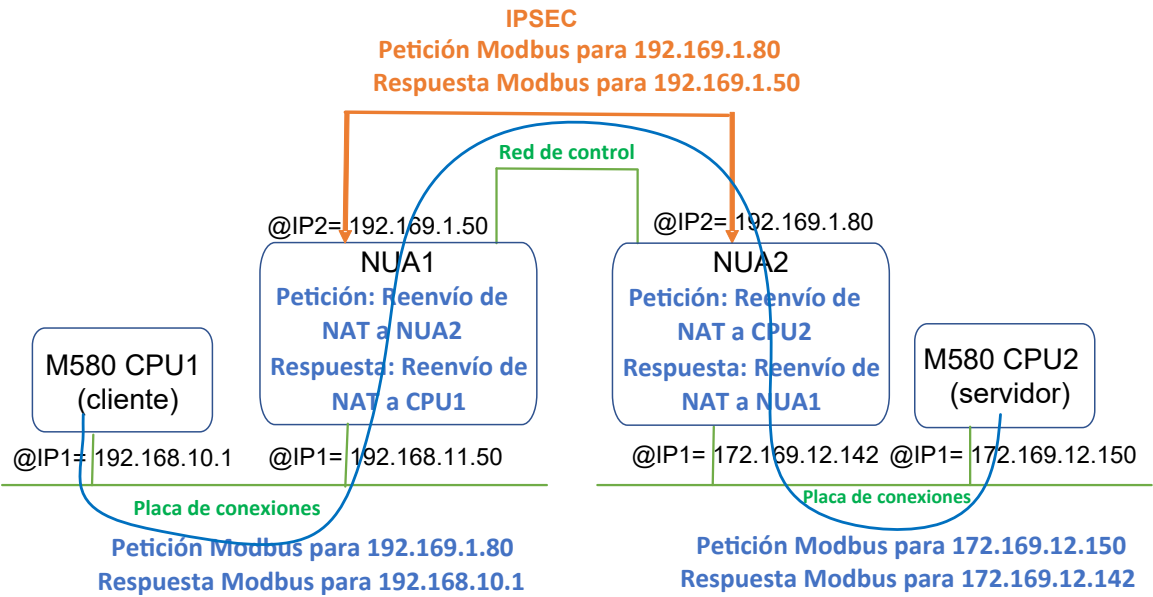
Reenvío de IP desde el cliente Windows (red de control) a cualquier cliente (red de dispositivos/placa de conexiones)



Reenvío de NAT desde el cliente Windows (red de control) al controlador M580 (red de dispositivos/placa de conexiones)

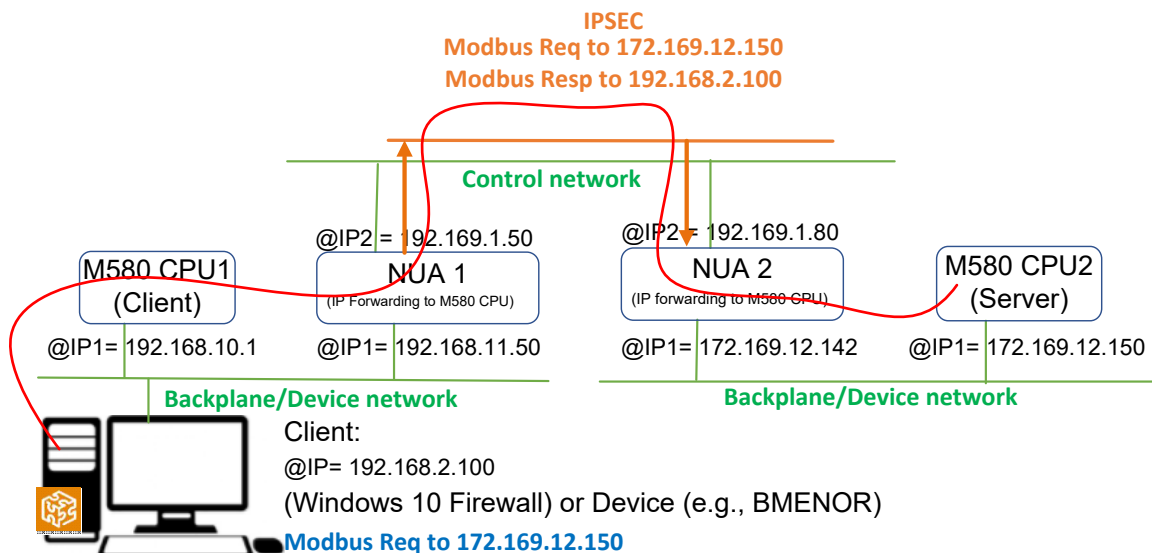


Reenvío de NAT entre placas de conexiones para la comunicación entre controladores M580



Arquitecturas no compatibles con el reenvío de servicios (IP)

Reenvío de IP entre placas de conexiones/redes de dispositivos



Reenvío de IP y comunicación OPC UA

Contenido de este capítulo

Impacto del reenvío de IP en el rendimiento..... 188

Impacto del reenvío de IP y OPC UA en el rendimiento..... 189

Tanto el reenvío de IP como OPC UA compiten por el ancho de banda de comunicación disponible del módulo BMENUA0100. En este capítulo se incluyen los resultados de las pruebas de rendimiento del módulo en las que solo se utiliza reenvío de IP o bien se utilizan reenvío de IP y comunicación OPC UA.

Impacto del reenvío de IP en el rendimiento

Cuando solo se activa el reenvío de IP (y no la comunicación OPC UA), el impacto en el ancho de banda del módulo BMENUA0100 es el siguiente:

IPsec	Confidencialidad	Forward (Hacia delante)	Trama de longitud (bytes)	Ancho de banda (Kbytes/s)
No	N/A	Reenviar todo	1000	8800
No	N/A	Regla personalizada	1000	10600
Sí	No	Reenviar todo	1000	3400
Sí	No	Regla personalizada	1000	4000
Sí	Sí	Reenviar todo	1000	2600
Sí	Sí	Regla personalizada	1000	2500

- NOTA:** Estos valores se presentan únicamente a modo de ejemplo. Utilícelos como una estimación del impacto de diferentes parámetros (IPsec, confidencialidad, etc.) en el rendimiento. El rendimiento real dependerá de su infraestructura concreta.
- El impacto en el ancho de banda se muestra cuando:
- Solo se admite el flujo de comunicación de reenvío de IP y no se incluye ningún flujo de comunicación OPC UA.
 - Se utiliza (IPsec = Sí) y no se utiliza (IPsec = No) IPsec.
 - Las tramas se firman (confidencialidad = No) frente a cuando las tramas se firman y cifran (confidencialidad = Sí) y se utiliza IPsec (en ambos casos).

- Se aplican reglas personalizadas para el reenvío de IP frente a la opción de reenviar todo.
- NOTA:** La longitud de las tramas solo posee un ligero impacto en el rendimiento global.

Impacto del reenvío de IP y OPC UA en el rendimiento

Cuando se activan el reenvío de IP y la comunicación OPC UA, el impacto en el ancho de banda del módulo BMENUA0100 es el siguiente:

Número de elementos OPC UA supervisados por suscripción	IPsec	Confidencialidad	Reenvío	Ancho de banda (Kbytes/s)
0	No	N/A	Regla personalizada	10600
0	Sí	No	Regla personalizada	4000
0	Sí	Sí	Regla personalizada	2500
20000	No	N/A	Regla personalizada	8800
20000	Sí	No	Regla personalizada	2900
20000	Sí	Sí	Regla personalizada	2000

- NOTA:** Estos valores se presentan únicamente a modo de ejemplo. Utilícelos como una estimación del impacto de diferentes parámetros (IPsec, confidencialidad, etc.) en el rendimiento. El rendimiento real dependerá de su infraestructura concreta.
- El impacto en el ancho de banda se muestra cuando:
- Todos los reenvíos de paquetes se realizan a través de la regla personalizada (sin reenvío de todo).
 - No se incluyen los flujos de comunicación OPC UA (número de elementos OPC UA supervisados = 0) y se incluyen (= 2000).
- NOTA:** El número de elementos supervisados de OPC UA tiene un impacto mínimo.

Scripts de Windows IPsec

Contenido de este capítulo

Scripts de configuración del cortafuegos de Windows IKE/
IPsec 190

Scripts de configuración del cortafuegos de Windows IKE/IPsec

Para ejecutar IPsec en un PC que aloje el software de configuración de Control Expert o un cliente OPC UA (por ejemplo, SCADA), debe añadir una configuración de red en el cortafuegos del host. Para cada regla IPsec configurada en las páginas web, se puede descargar un script asociado (denominado IPsecWindowsConf.bat) mediante el icono del engranaje. Ejecute este script para establecer la configuración del cortafuegos del host.

- IKE/IPsec en modalidad de **transporte** para los flujos de datos locales de BMENUA0100.
- IKE/IPsec en modalidad de **túnel** para los flujos de datos reenviados a la placa de conexiones Ethernet.
- Reglas de paso para HTTPS, OPCUA seguro y otros protocolos para los que **Uso de IPSEC = FALSE**.

En los ejemplos que se indican a continuación se presentan scripts de configuración del cortafuegos de Windows con y sin confidencialidad IPsec.

En cada ejemplo de script, debe proporcionar los valores para las siguientes variables:

- **endpoint1**: el valor de la dirección IP remota en la configuración IPsec.
- **endpoint2**: la dirección IP del puerto de control de BMENUA0100.
- **Auth1psk**: el ajuste de PSK en la configuración IPsec.

Script del cortafuegos de Windows con confidencialidad

NOTA: Si la confidencialidad está habilitada en la configuración IPsec, utilice
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 del cortafuegos de Windows sin confidencialidad

NOTA: Si la confidencialidad no está habilitada en la configuración IPsec, utilice
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
```

Configuración de una autoridad de certificación de Windows

Contenido de este capítulo

Pasos preliminares	193
Vista general de instalación de servicios de certificados Active Directory de Microsoft Windows	194
Instalación de los Servicios de certificados de Active Directory (ADCS)	195
Aplicación de la plantilla de la autoridad de certificación.....	217

En este capítulo se describe cómo configurar una autoridad de certificación de Microsoft Windows™ a fin de utilizarlo en un sistema de autenticación y autorización de usuarios para toda la empresa.

Pasos preliminares

A continuación se describen los artículos que necesita y los pasos preliminares que debe seguir antes de instalar los servicios de certificados.

Artículos necesarios

- Necesitará los siguientes elementos:
- Microsoft Windows™ Server Manager: Puede descargarlo en el sitio web de Microsoft.
 - Servicios de certificados Active Directory (ADCS) de Microsoft Windows: Este software comercial se incluye como parte de Windows Server. El módulo BMENUA0100 es compatible con las versiones de Windows Server 2016 y 2019.
 - El archivo TemplatePackage.zip, que se puede descargar en Schneider Electric.

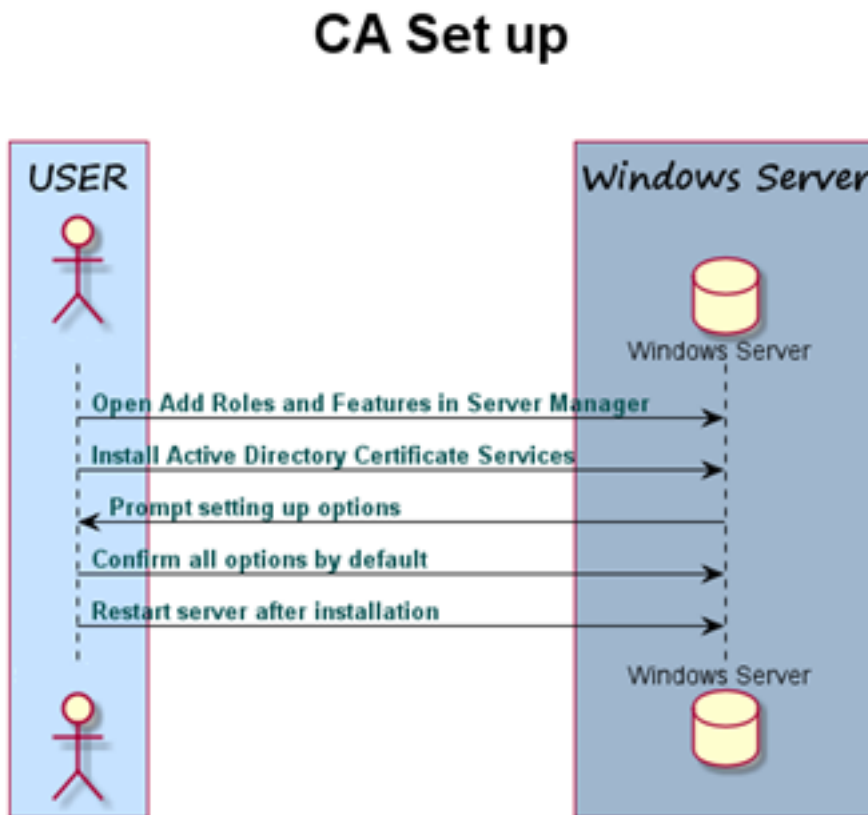
Instalaciones preliminares de software

Ejecute el archivo de instalación de Active Directory Certificate Server y, a continuación, siga los pasos indicados para crear una cuenta de usuario y una contraseña.

Server Manager debe estar preinstalado en su PC host. De lo contrario, puede descargarlo en el sitio web de Microsoft.

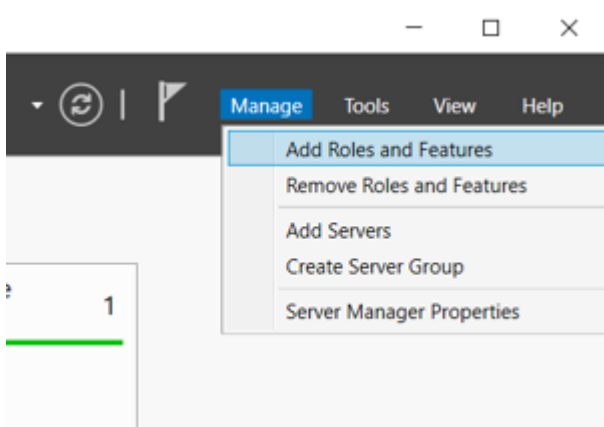
Vista general de instalación de servicios de certificados Active Directory de Microsoft Windows

En el diagrama siguiente se muestra un resumen del proceso de configuración de la autoridad de certificación (CA):

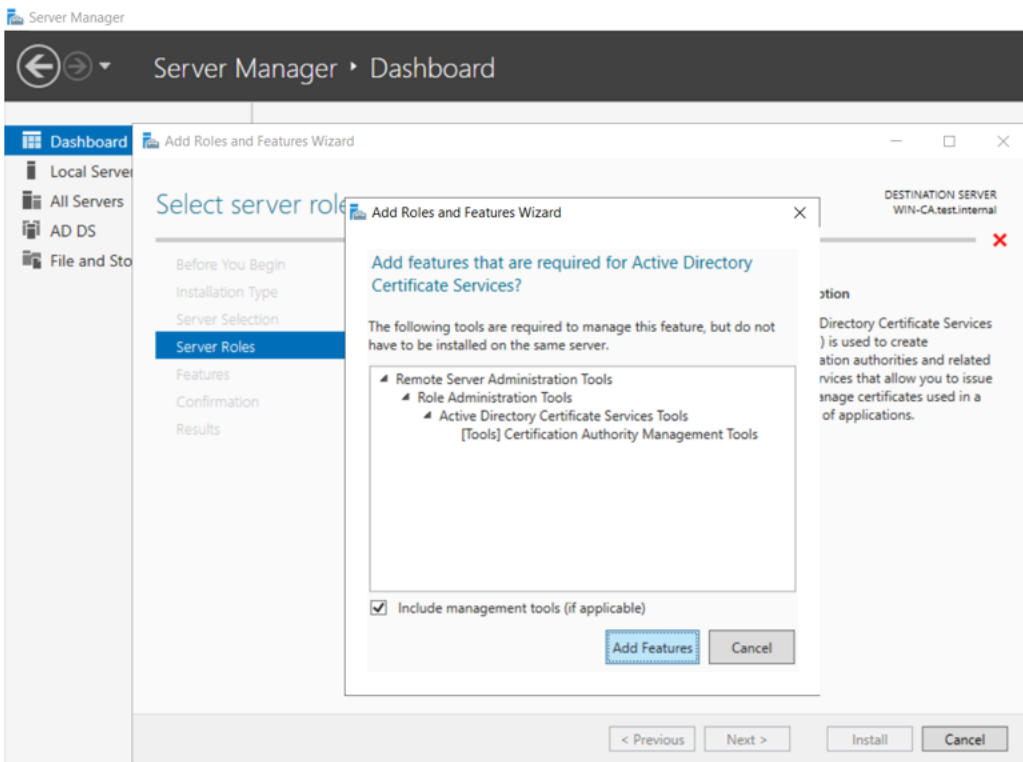


Instalación de los Servicios de certificados de Active Directory (ADCS)

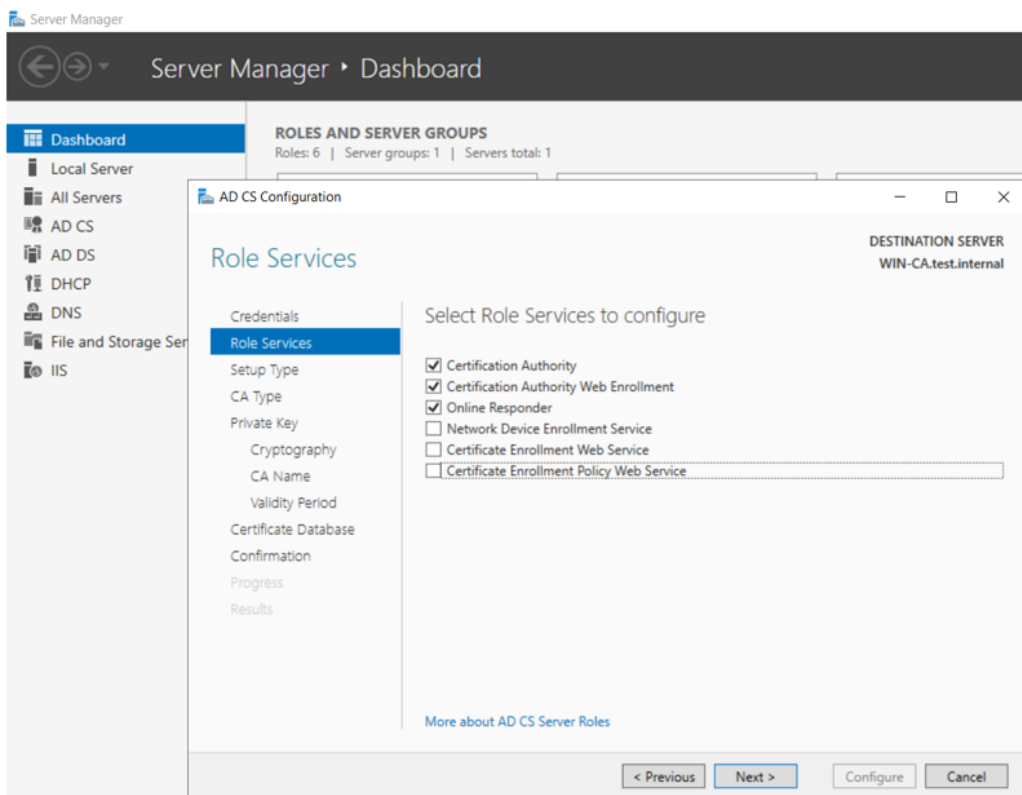
1. Inicie Microsoft Windows™ Server Manager y abra su escritorio.
2. Seleccione **Administrar > Agregar roles y características**.



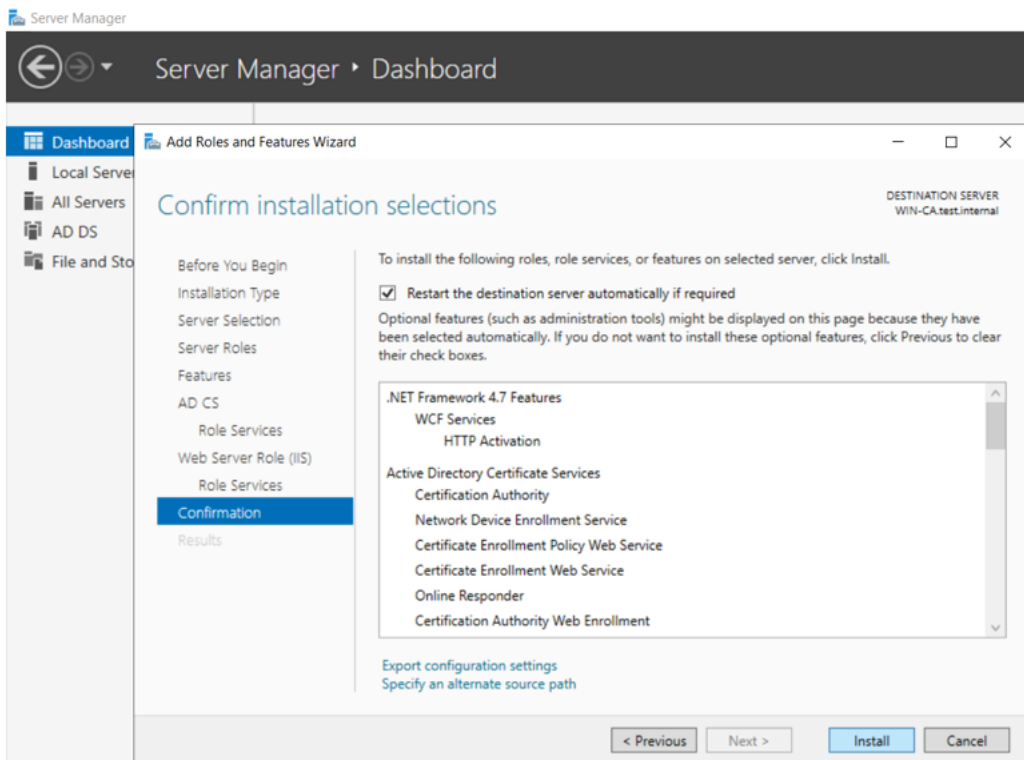
3. Añada los roles y características requeridos e incluya las herramientas de administración:



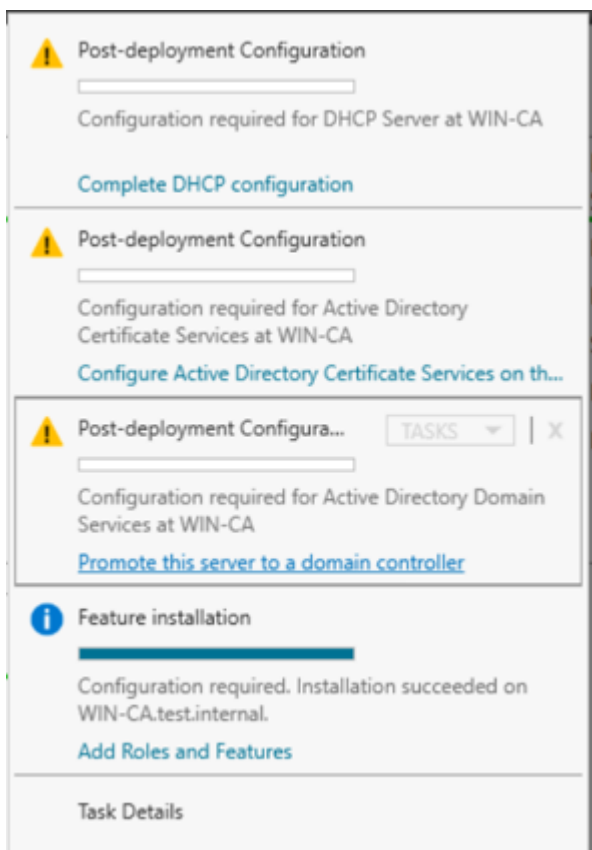
4. Seleccione los Servicios de rol que desea configurar:



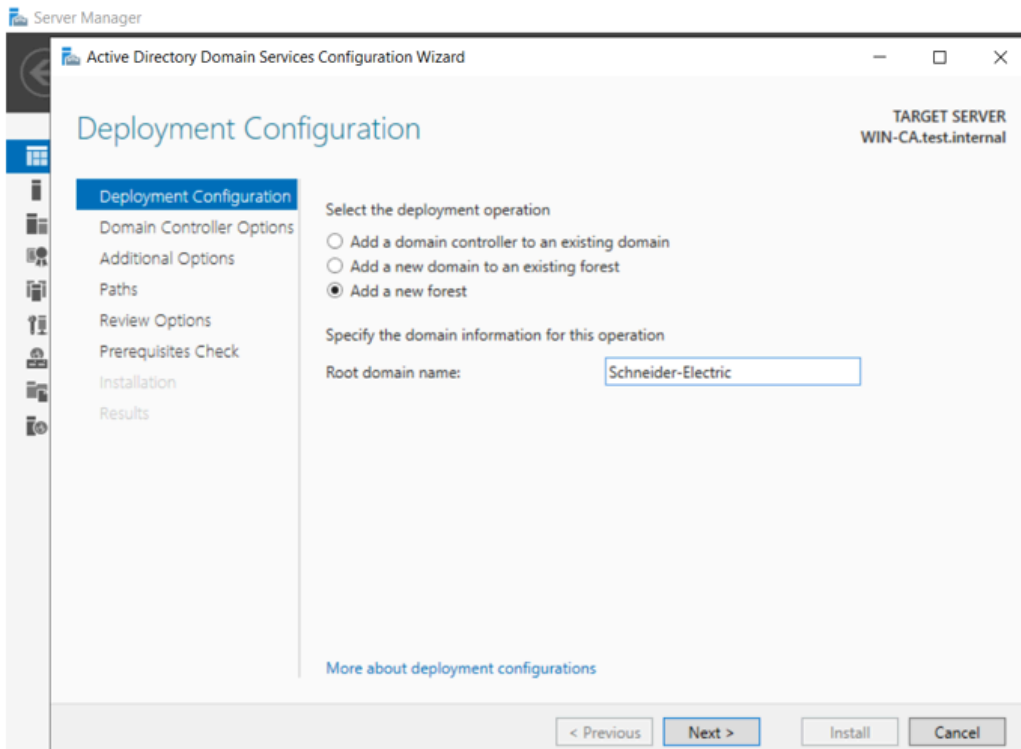
5. Confirme las opciones de instalación:



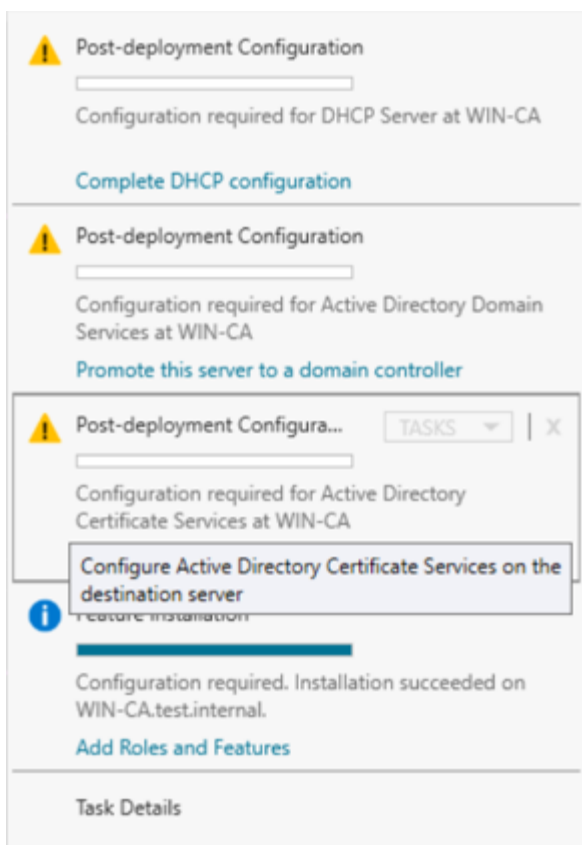
6. Haga clic en **Instalar**. Server Manager muestra el progreso de la instalación:



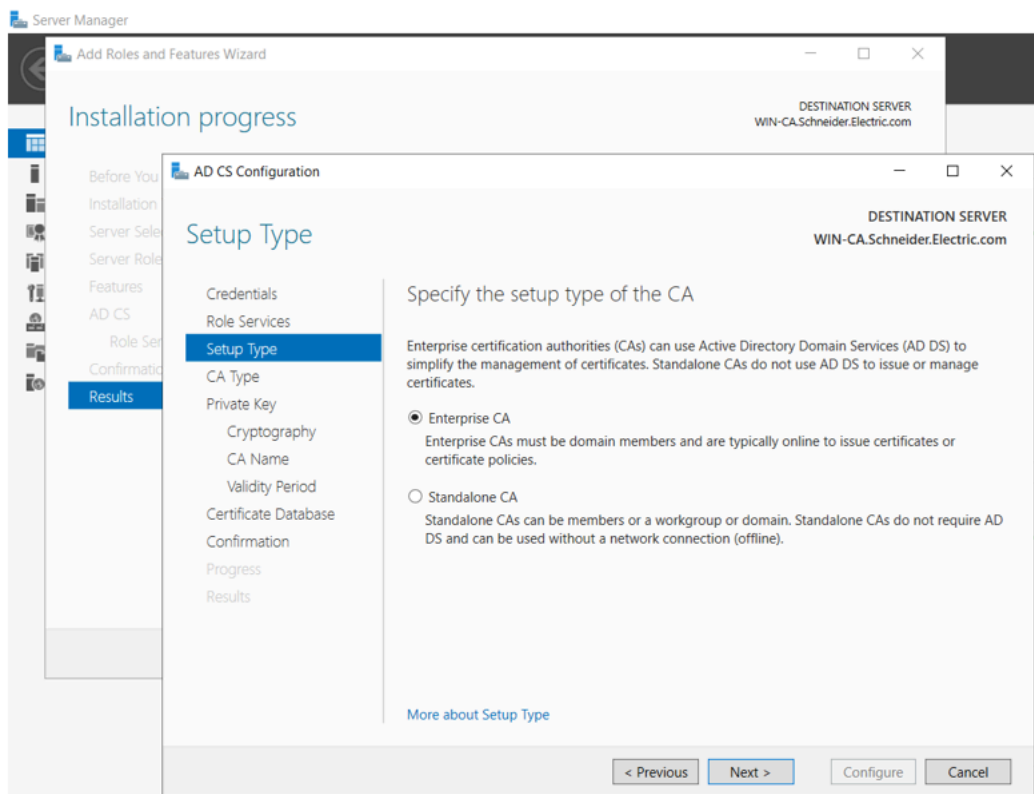
7. Seleccione la operación de implementación creando un nuevo bosque o añadiendo elementos a un bosque existente y especifique el dominio:



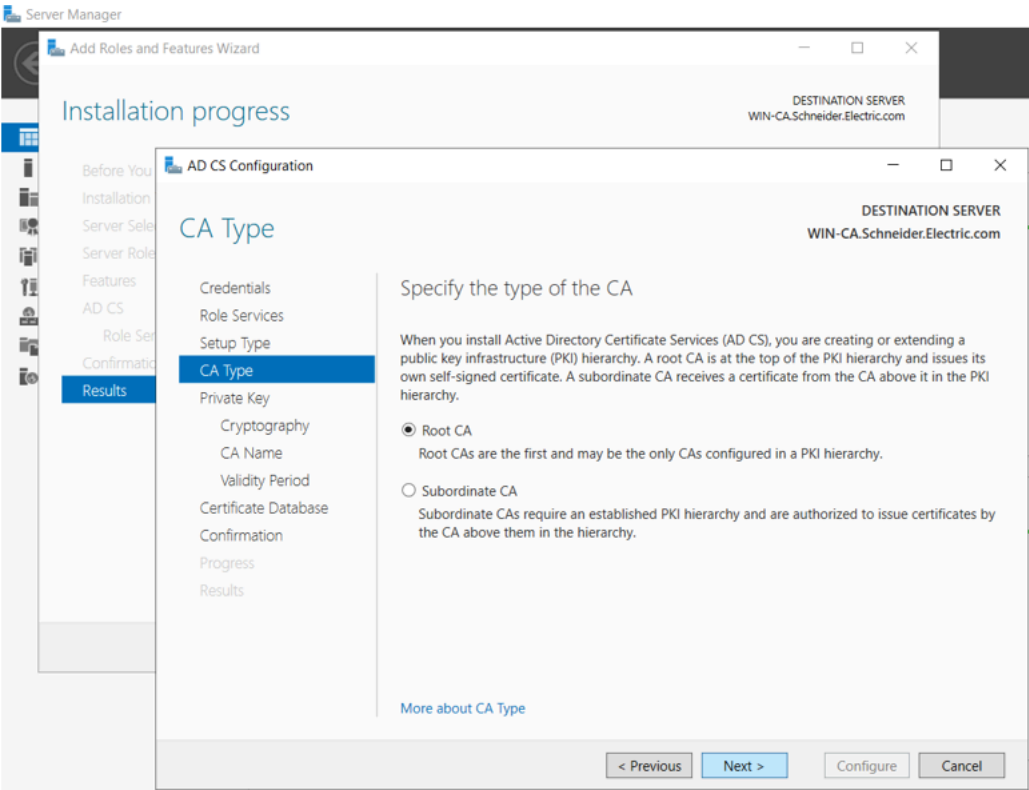
8. Server Manager muestra y configura las opciones:



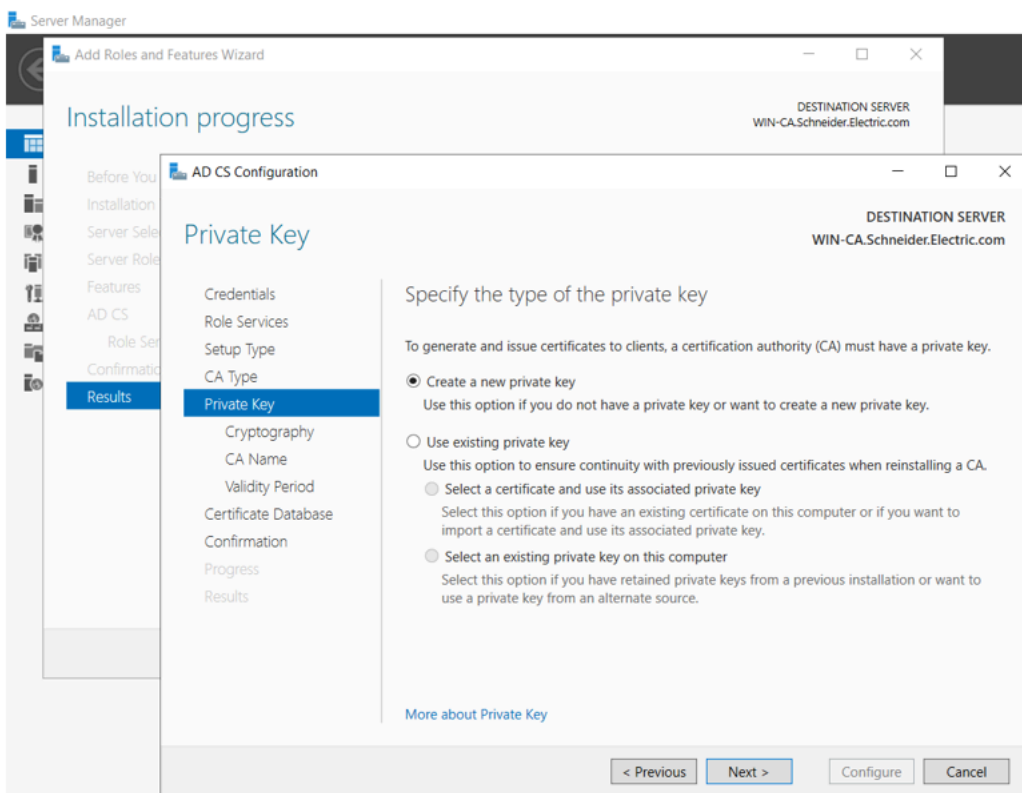
9. Especifique el tipo de CA que desea configurar:



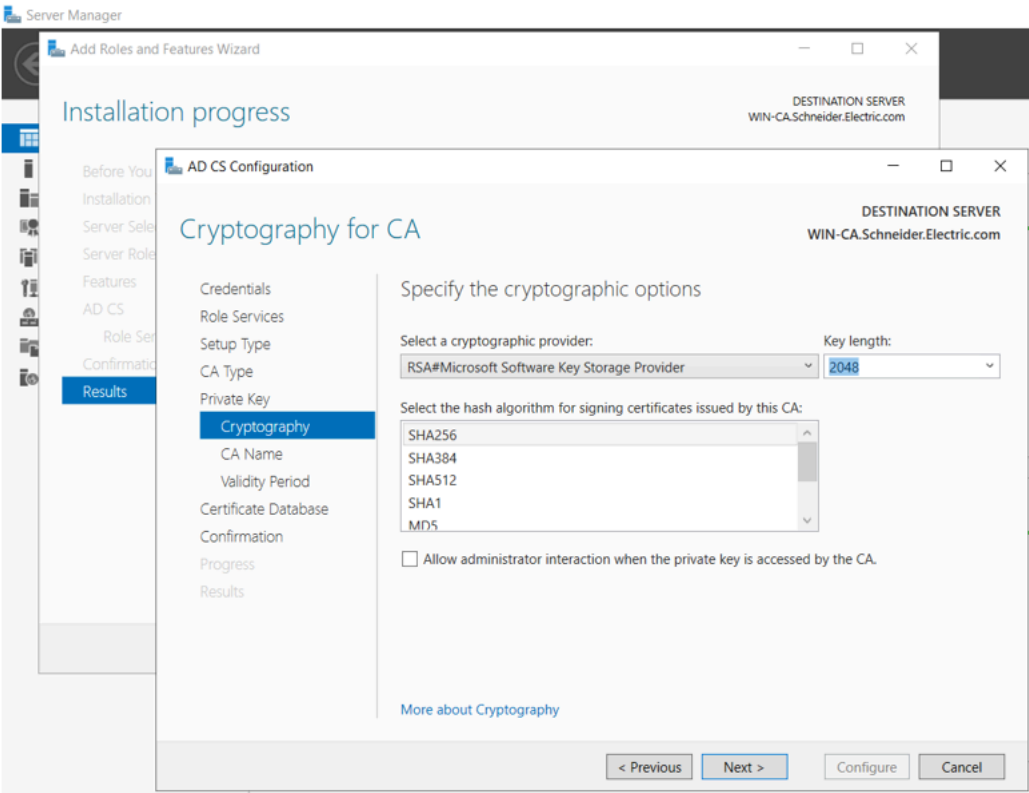
10. Especifique el tipo de CA:



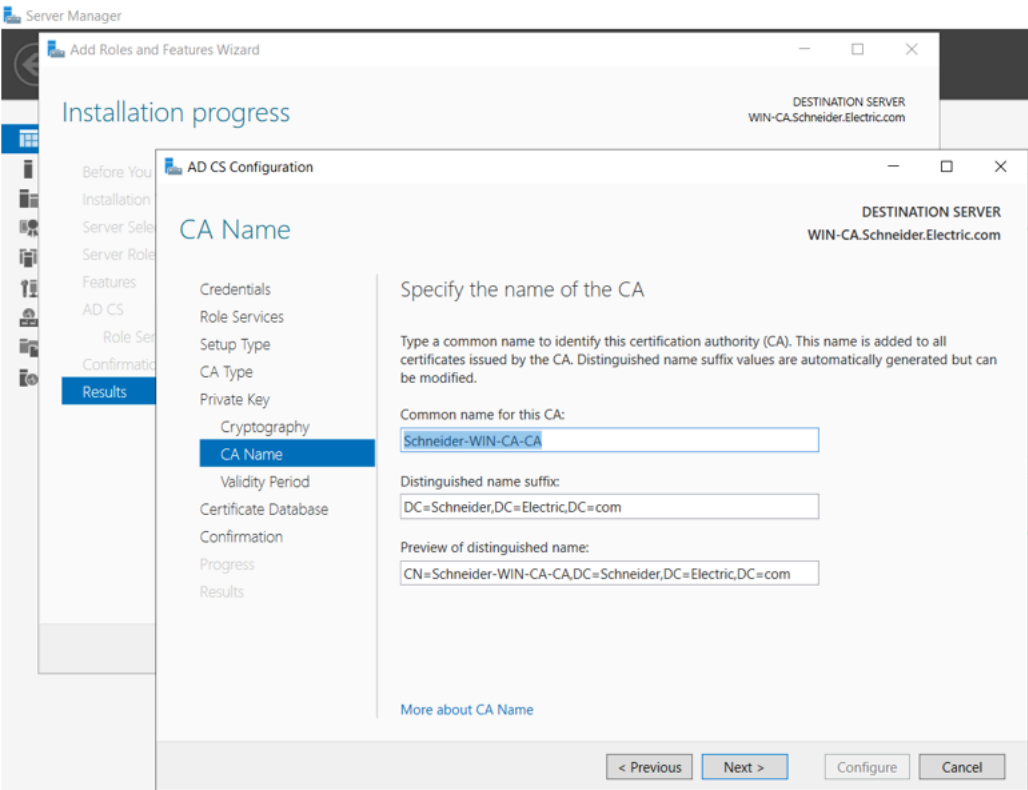
11. Especifique el tipo de clave privada:



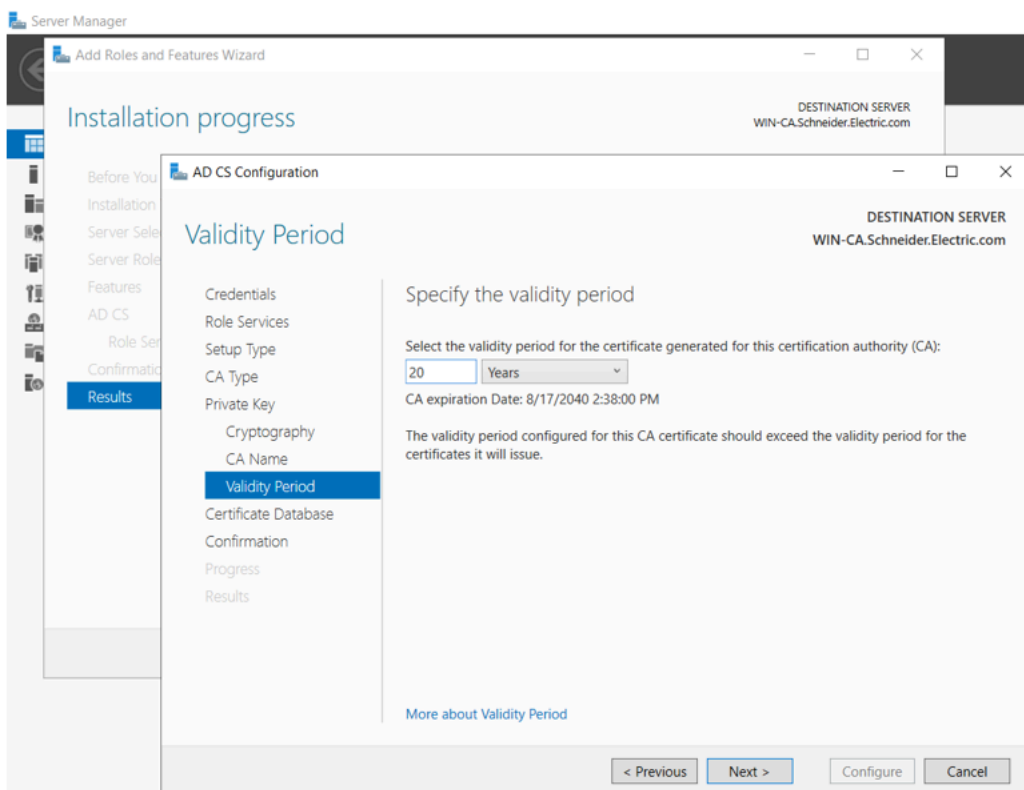
12. Especifique las opciones criptográficas:



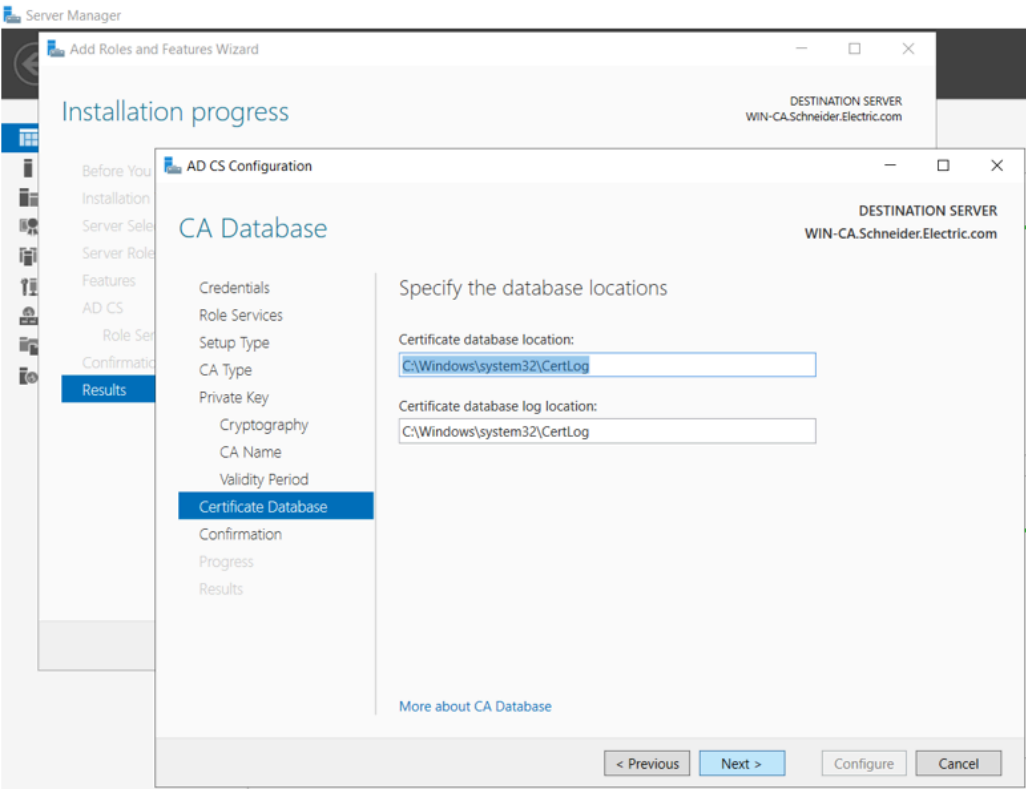
13. Especifique las opciones de denominación para la CA:



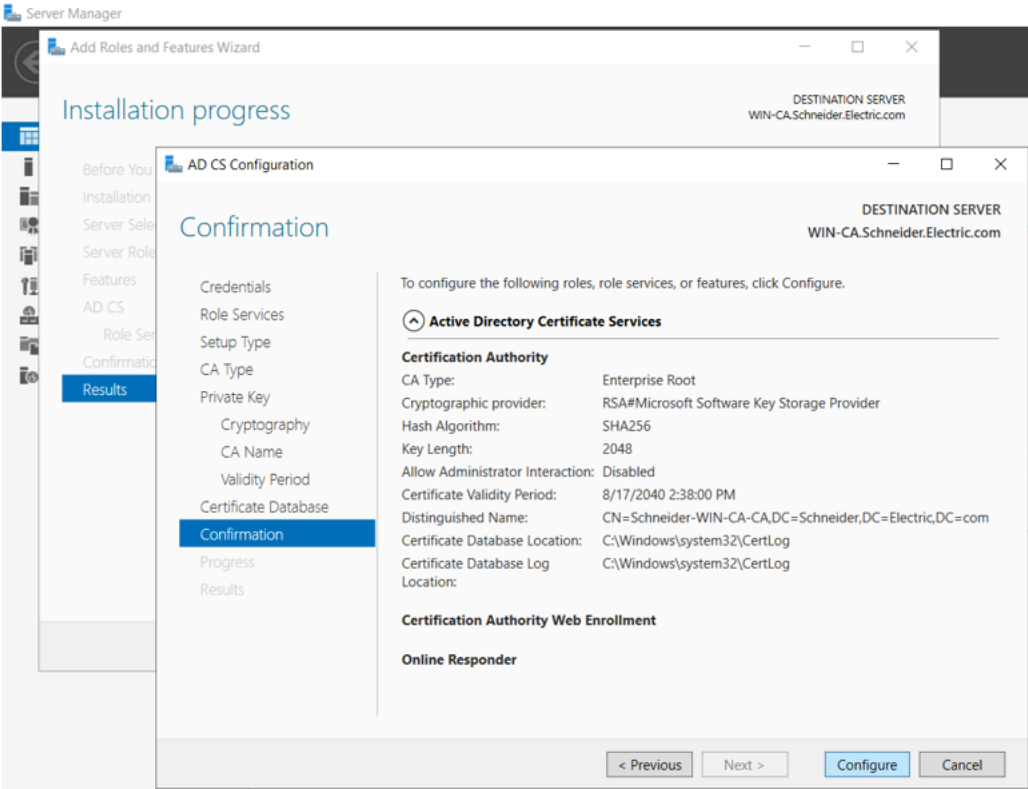
14. Especifique el período de validez. El período de validez típico de un certificado CA es de 5 años:



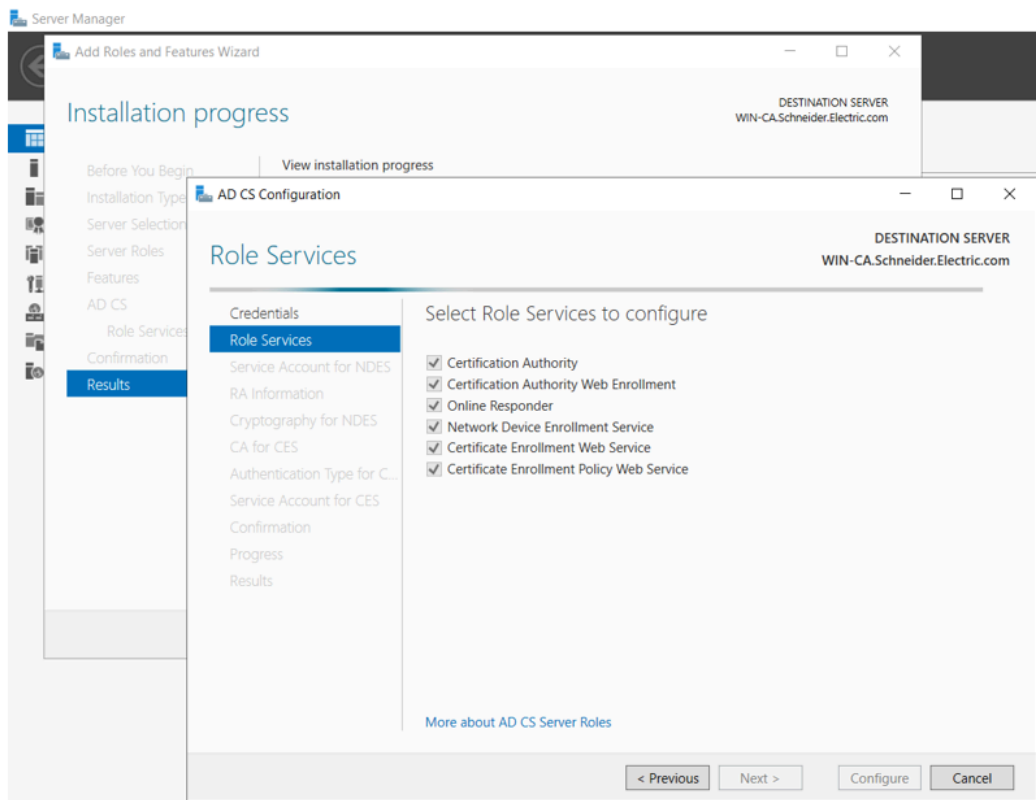
15. Especifique las ubicaciones de la base de datos de certificados y el registro:



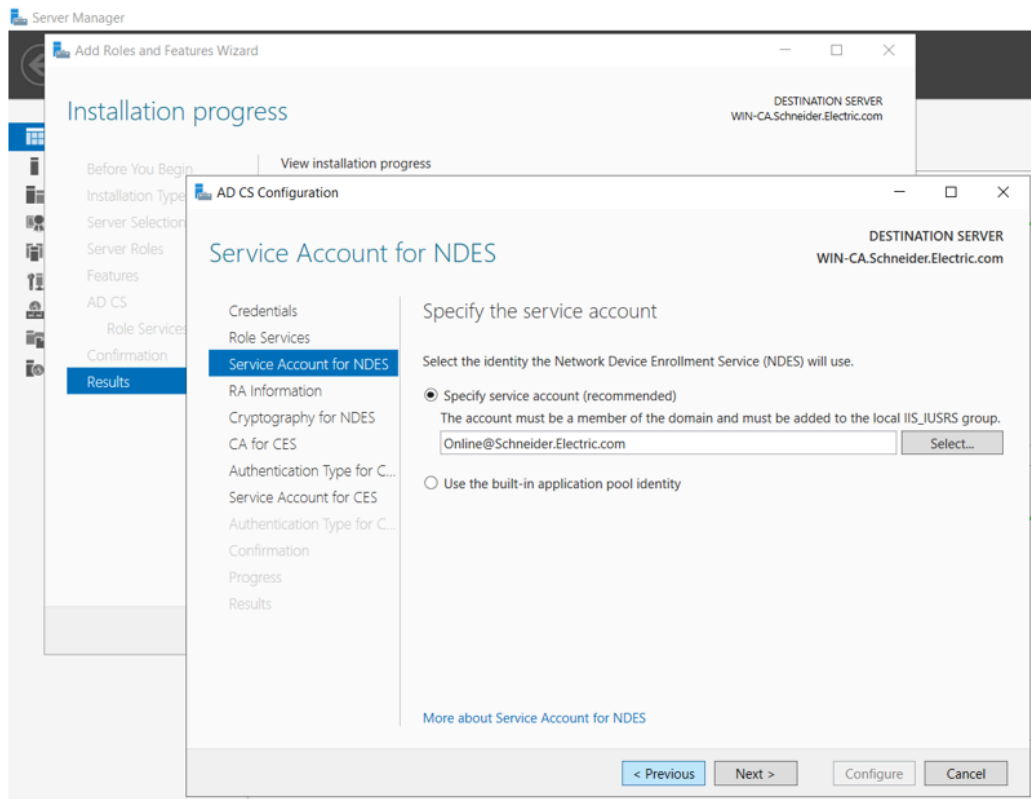
16. Confirme los servicios de certificados de Active Directory seleccionados y, si es correcto, haga clic en **Configurar**:



17. Seleccione los servicios de rol que desea configurar:



18. Especifique la cuenta de servicios:



19. Introduzca la información para inscribirse en un certificado de autoridad de registro (registration authority, RA):

Server Manager

Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-CA.Schneider.Electric.com

Before You Begin | View installation progress

Installation Type | AD CS Configuration

Server Selection

Server Roles

Features

AD CS

Role Services

Confirmation

Results

RA Information

Credentials

Role Services

Service Account for NDES

Cryptography for NDES

CA for CES

Authentication Type for C...

Service Account for CES

Authentication Type for C...

Confirmation

Progress

Results

RA Information

DESTINATION SERVER
WIN-CA.Schneider.Electric.com

Type the requested information to enroll for an RA certificate

A registration authority (RA) is required to manage the Network Device Enrollment Service (NDES) certificate requests.

Required information

RA Name: WIN-CA-MSCEP-RA

Country/Region: US (United States)

Optional information

E-mail:

Company:

Department:

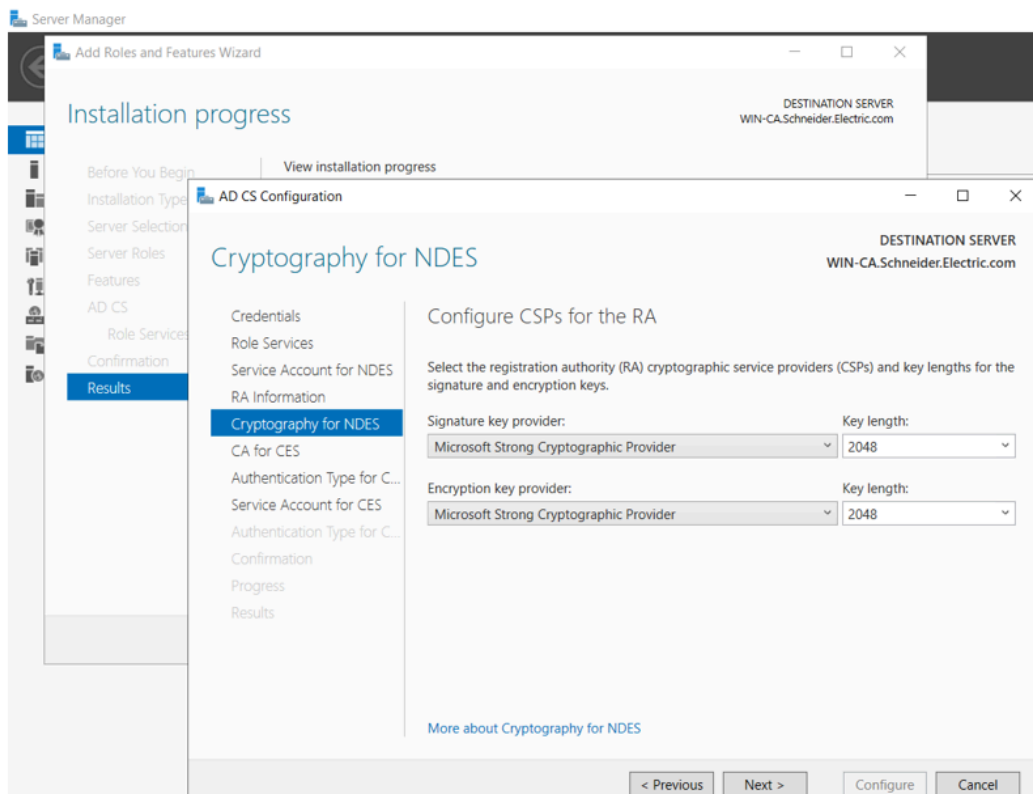
City:

State/Province:

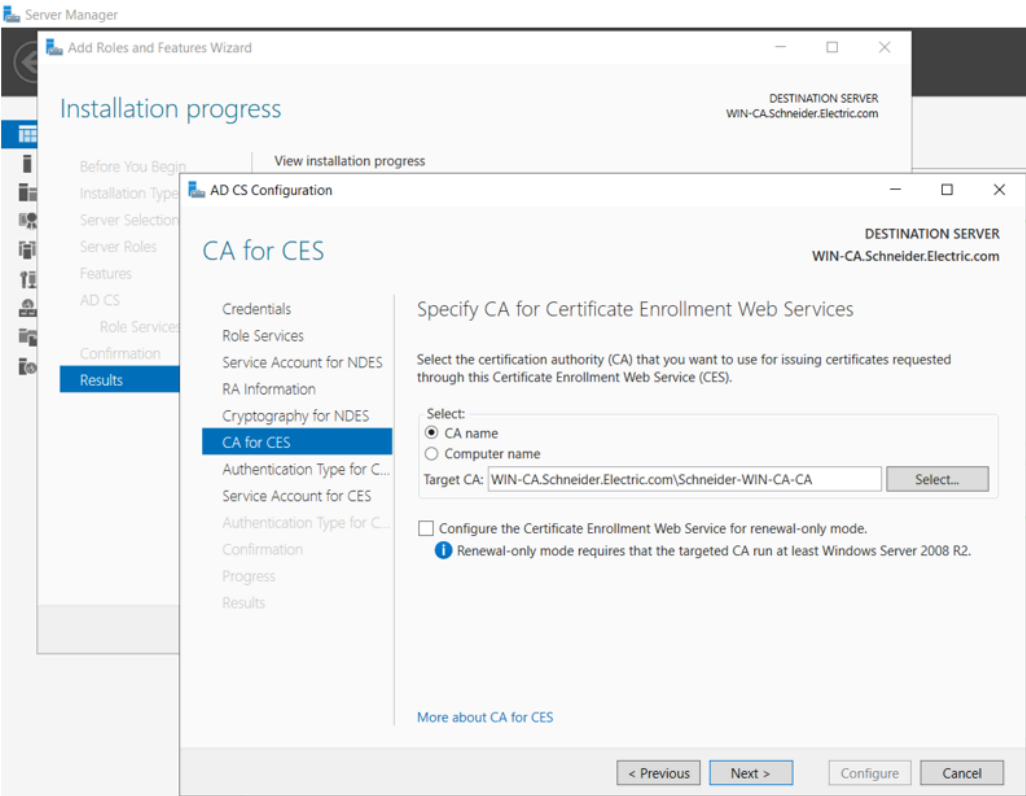
More about RA Information

< Previous Next > Configure Cancel

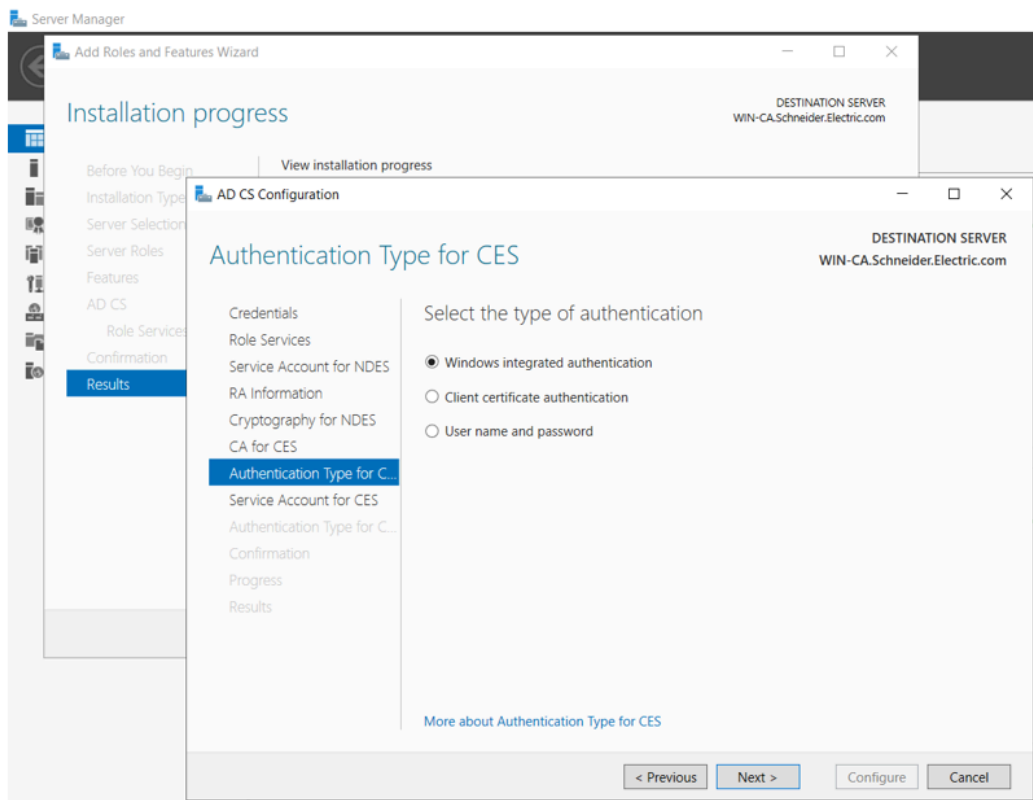
20. Seleccione la configuración de criptografía para la RA:



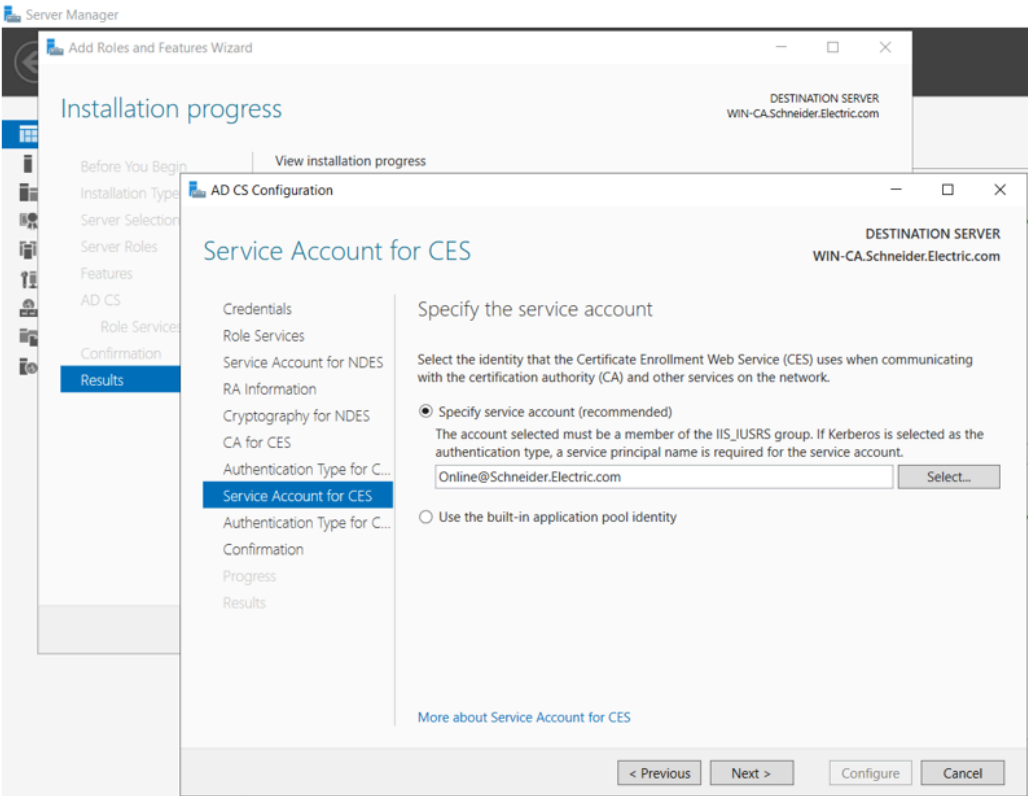
21. Especifique la CA para los servicios web de inscripción de certificados:



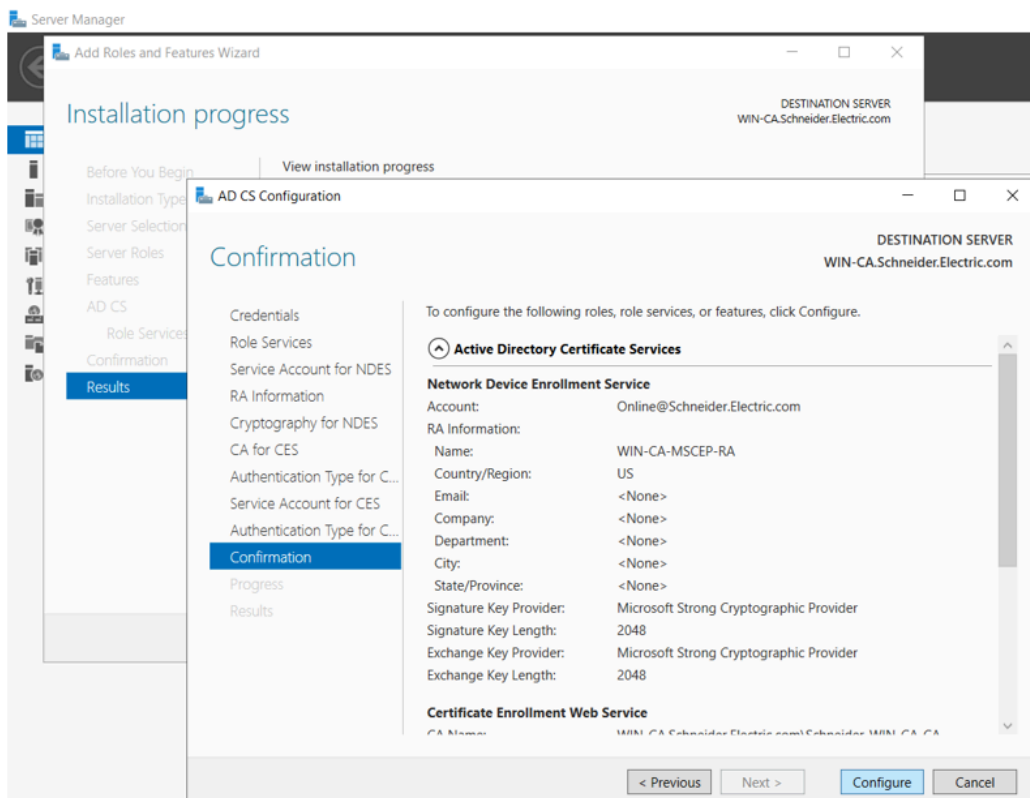
22. Seleccione un tipo de autenticación:



23. Especifique la cuenta de servicios:



24. Confirme los roles, los servicios y las características y, a continuación, haga clic en **Configurar**:



Al hacerlo, se completa la instalación de Active Directory Certificate Server.

Aplicación de la plantilla de la autoridad de certificación

La última parte de la configuración de una autoridad de certificación de Microsoft Windows consiste en aplicar la plantilla de CA proporcionada por Schneider Electric.

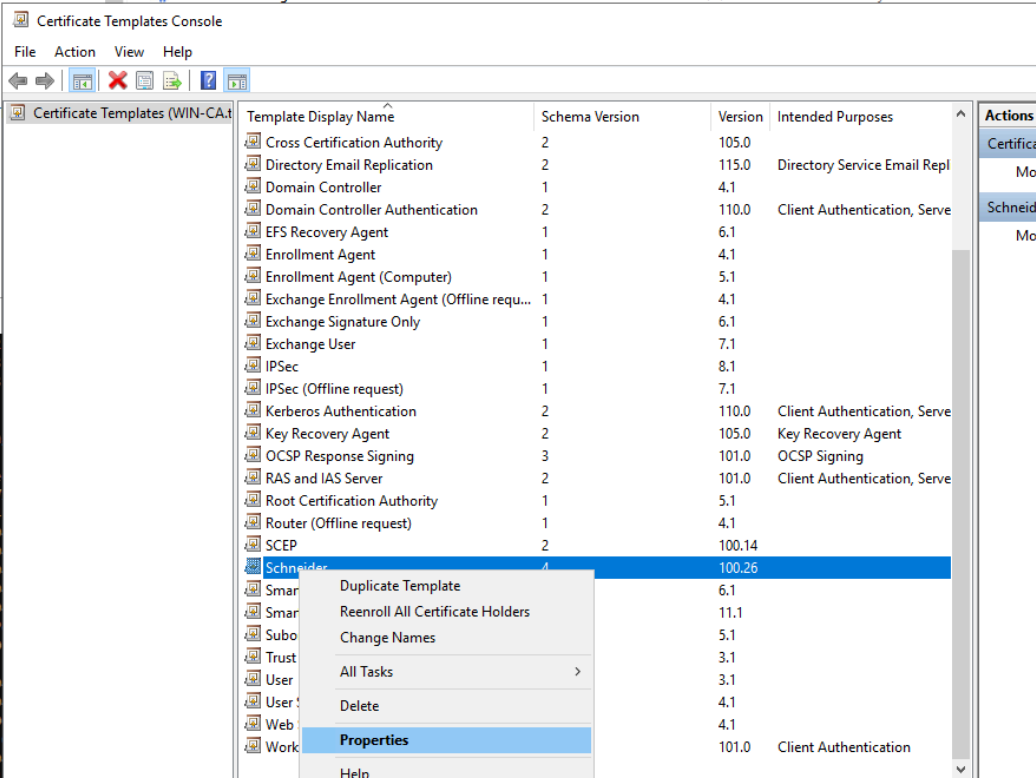
La plantilla y los elementos de apoyo se encuentran en el archivo "TemplatePackage.zip" proporcionado por Schneider Electric.

Para aplicar el certificado, siga estos pasos:

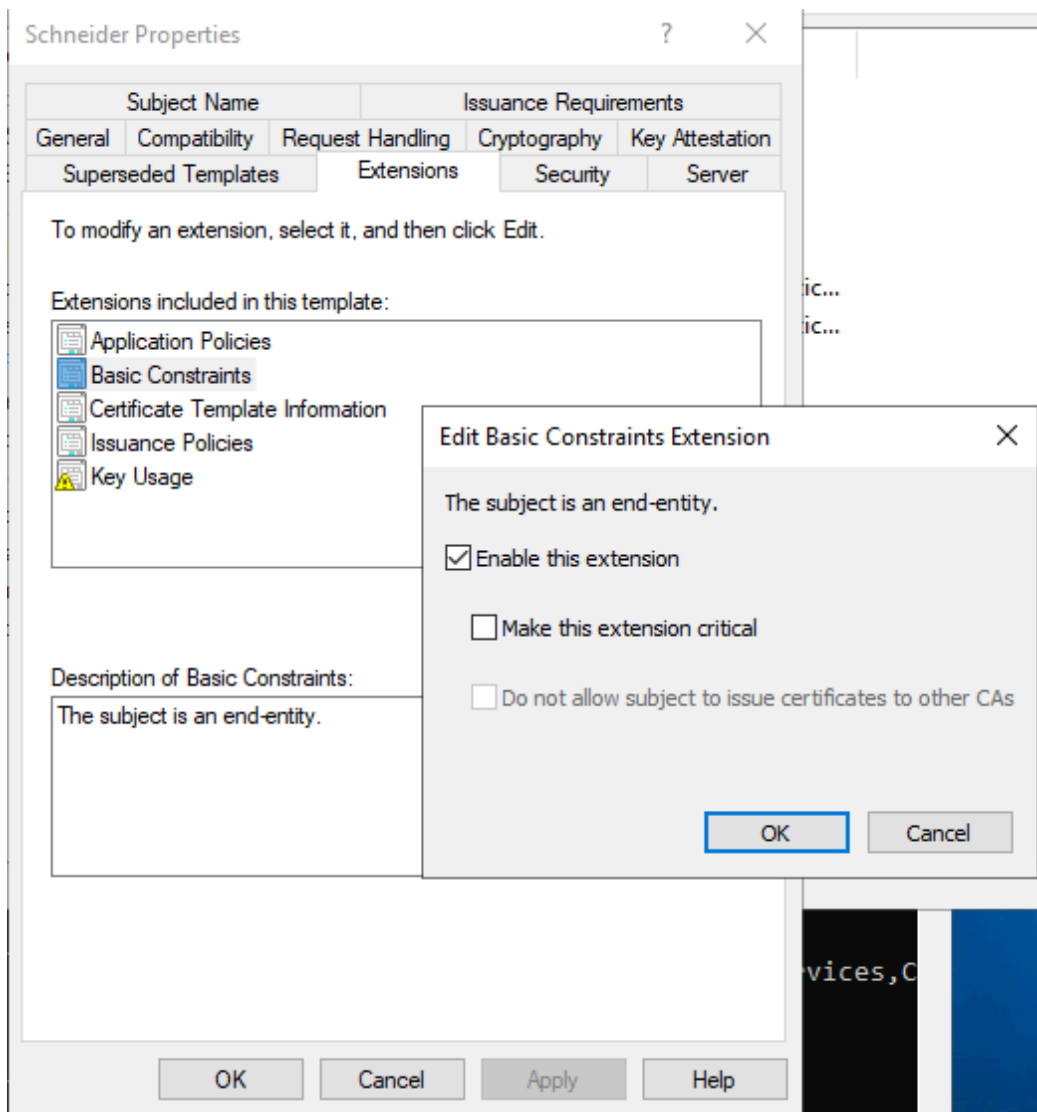
- Descomprima el archivo "TemplatePackage.zip" y copie su contenido (una carpeta denominada "TemplatePackage") en una ubicación que no sea C:\Windows\System32...
Por ejemplo, puede copiar esta carpeta en "C:\Usuarios\Administrador\Escritorio"
- Inicie Microsoft Windows PowerShell (u otra herramienta de comandos) como administrador.
- Desplácese hasta la carpeta donde colocó TemplatePackage, por ejemplo:

```
> cd C:\Users\Administrator\Desktop\TemplatePackage
```
- Ejecute la plantilla dentro de la carpeta TemplatePackage, de la siguiente manera:

```
> .\ImportCertificateTemplate.ps1
```
- En el PC host, abra la Consola de plantillas de certificado, haga clic con el botón derecho en el certificado de Schneider y, a continuación, seleccione **Propiedades**:



6. En la ventana **Propiedades de Schneider**, abra la ficha **Extensiones**, haga doble clic en **Restricciones básicas** y, en el cuadro de diálogo **Editar restricciones básicas**, seleccione **Habilitar esta extensión** y haga clic en **Aceptar**:



Realización de la inscripción manual

Consulte el tema [Inscripción manual de certificados](#), página 116 para obtener información sobre cómo realizar esta tarea.

Haga clic en el enlace incluido en ese tema para acceder a una presentación de vídeo sobre el procedimiento.

Glosario

C

captura:

Una captura es un evento dirigido por un agente SNMP que indica uno de estos eventos:

- Se ha producido una modificación en el estado de un agente.
- Un dispositivo administrador SNMP no autorizado ha intentado obtener datos de un agente SNMP (o modificar sus datos).

D

dirección IP:

Identificador de 32 bits (que incluye tanto una dirección de red como una dirección de host) asignado a un dispositivo conectado a una red TCP/IP.

E

entorno severo:

Resistencia a los hidrocarburos, aceites industriales, detergentes y virutas de soldadura. Humedad relativa de hasta el 100 %, ambiente salino, variaciones significativas de temperatura, temperatura de funcionamiento entre -10 °C y + 70 °C, o en instalaciones móviles. Para dispositivos endurecidos (H), la humedad relativa alcanza un máximo de 95 % y la temperatura de funcionamiento está entre -25 °C y + 70 °C.

S

SNTP:

(simple network time protocol, protocolo simple de hora de la red) Véase NTP.

Índice

A		F	
agente SNMP	136	firmware	
arquitecturas.....	64	actualizar	179
B		H	
BMENUA0100		HTTPS	
descripción.....	21	puerto 443.....	65
C		I	
CCOTF	66	indicador LED	
certificaciones.....	28	diagnóstico.....	141
colocación del módulo		indicador LED de estado de	
red plana.....	65	ciberseguridad	145
compatibilidad		indicadores LED	
firmware del módulo frente a versiones de		módulo.....	26
software de Control Expert.....	29	Indicadores LED	
configuración	89	conexión del puerto de control	27
conmutador rotativo	25	M	
Controlador M580		modalidades de funcionamiento	30
configuración de seguridad.....	140	N	
D		normas.....	28
DDT de T_BMENUA0100	147	NTP	
DDT de T_CYBERSECURITY_STATUS ...	151	configuración.....	133
DDT de T_FW_VERSION.....	151	número máximo de módulos por bastidor.....	66
DDT de T_OP_CUA_STATUS	147	P	
DDT de T_SERVICES_STATUS	148	páginas web	89
DHCP-BOOTP		página de inicio.....	94
Controladores M580	140	puertos.....	21
diagnóstico	141	puesta en marcha	82–83
Modbus.....	167	R	
E		READ_DDT	152
Estándares	28	red plana	
		colocación del módulo.....	65
		reenvío de IP	102

S

sincronización horaria
configurar..... 133

T

TFTP
Controlador M580 140

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Debido a que las normas, especificaciones y diseños cambian periódicamente,
solicite la confirmación de la información dada en esta publicación.

© 2025 Schneider Electric. Reservados todos los derechos.

PHA83354.04