Modicon M580

Modulo integrato BMENUA0100 OPC UA

Guida di installazione e configurazione

Traduzione delle istruzioni originali

06/2024

PHA83353.03

www.se.com

Informazioni di carattere legale

Le informazioni contenute nel presente documento contengono descrizioni generali, caratteristiche tecniche e/o raccomandazioni relative ai prodotti/soluzioni.

Il presente documento non è inteso come sostituto di uno studio dettagliato o piano schematico o sviluppo specifico del sito e operativo. Non deve essere utilizzato per determinare idoneità o affidabilità dei prodotti/soluzioni per applicazioni specifiche dell'utente. Spetta a ciascun utente eseguire o nominare un esperto professionista di sua scelta (integratore, specialista o simile) per eseguire un'analisi del rischio completa e appropriata, valutazione e test dei prodotti/soluzioni in relazione all'uso o all'applicazione specifica.

Schneider Electric si riserva il diritto di apportare modifiche o aggiornamenti relativi al presente documento o ai suoi contenuti o al formato in qualsiasi momento senza preavviso.

Nella misura in cui sia consentito dalla legge vigente, Schneider Electric e le sue consociate non si assumono alcuna responsabilità od obbligo per eventuali errori od omissioni nel contenuto informativo del presente materiale, o per qualsiasi utilizzo non previsto o improprio delle informazioni ivi contenute.

Sommario

Informazioni di sicurezza 7
Prima di iniziare 8
Avviamento e verifica 9
Funzionamento e regolazioni 10
Informazioni sul manuale 11
Caratteristiche del modulo BMENUA0100 17
Caratteristiche del modulo 17
Descrizione del modulo 19
LED del modulo 24
Standard e certificazioni 26
Standard e certificazioni 26
Modulo standard BMENUA0100 26
Compatibilità del firmware BMENUA0100 con EcoStruxure™ Control Expert 27
Descrizione funzionale di BMENUA0100 28
Impostazioni modalità operativa di sicurezza informatica 28
Servizi OPC UA 34
Caratteristiche operative del server OPC UA BMENUA0100 35
Server OPC UA 36
Servizi stack del server OPC UA BMENUA0100 38
Servizi di accesso ai dati dello stack del server OPC UA BMENUA0100 39
Servizi di sicurezza e rilevamento dello stack del server OPC UA BMENUA0100 41
Servizi di sottoscrizione e pubblicazione dello stack del server OPC UA BMENUA0100 43
Servizi di trasporto dello stack del server OPC UA BMENUA0100 47
Rilevamento variabili controller 48
Mappatura delle variabili del controller di Control Expert alle variabili logiche dei dati OPC UA 48
Hot Standby e ridondanza 53
Ridondanza del server OPC UA 53
Architetture supportate 61

Configurazioni supportate del modulo BMENUA0100 61
Rete di controllo isolata con controller M580 Hot Standby 64
Rete piana non isolata con M580 Hot Standby 66
Rete piana con più controller M580 standalone e singolo SCADA 69
Rete piana con più controller M580 standalone e SCADA ridondante 71
Rete piana con controller M580 Hot Standby e SCADA ridondante 73
Rete gerarchica con più controller M580 standalone collegati alla rete di controllo e SCADA ridondante 75
Rete gerarchica con più controller M580 Hot Standby e connessioni SCADA ridondanti 77
Messa in servizio e installazione 79
Elenco di controllo per la messa in servizio del modulo BMENUA0100 79
Messa in servizio del modulo BMENUA0100 80
Installazione del BMENUA0100 83
Configurazione 86
Configurazione delle impostazioni di sicurezza informatica di BMENUA0100 86
Presentazione delle pagine Web di BMENUA0100 86
Home page 91
Impostazioni 94
Gestione certificati 105
Controllo accesso 113
Gestione della configurazione 115
Configurazione del BMENUA0100 in Control Expert 117
Configurazione delle impostazioni dell'indirizzo IP 117
Configurazione della funzione orodatario sorgente 121
Gestione delle variabili orodatate all'origine 122
Configurazione del servizio di sincronizzazione dell'ora 126
Configurazione agente SNMP 129
Configurazione delle impostazioni del controller M580 per connessioni client - server OPC UA 132
Configurazione delle impostazioni di sicurezza del controller M580 133
Diagnostica 134
Diagnostica LED 134
Tipo di dati derivati (DDT) BMENUA0100 139

Configurazione della funzione elementare READ_DDT 144
Configurazione della funzione elementare READ_NUA_DDT 149
Diagnostica OPC UA 150
Syslog 154
Diagnostica Modbus 158
Diagnostica SNMP 159
Pagina Web Diagnostica OPC UA 160
Ottimizzazioni delle prestazioni del modulo BMENUA0100 162
Ottimizzazioni delle prestazioni del modulo BMENUA0100 162
Risoluzione dei problemi del modulo BMENUA0100 165
Aggiornamento del firmware 169
Strumento EcoStruxure™ Automation Device Maintenance 169
Appendici 171
Connessioni del controller 172
Connessioni da server OPC UA a controller 172
Architetture di inoltro del servizio (IP) 173
Architetture supportate dal servizio di inoltro (IP) 173
Architetture non supportate dal servizio di inoltro (IP) 176
Inoltro IP e comunicazione OPC UA 177
Impatto dell'inoltro IP sulle prestazioni 177
Inoltro IP e impatto di OPC UA sulle prestazioni 178
Script Windows IPsec 179
Script di configurazione di Windows Firewall IKE/IPsec 179
Impostazione di un'autorità di certificazione Windows 182
Passi preliminari 182
Cenni preliminari sull'installazione di Microsoft Windows Active Directory Certificate Server 183
Installazione di Active Directory Certificate Server (ADCS) 184
Applicazione del modello dell'Autorità di certificazione 206
Glossario 211
Indice 212

Informazioni di sicurezza

Informazioni importanti

Leggere attentamente queste istruzioni e osservare l'apparecchiatura per familiarizzare con i suoi componenti prima di procedere ad attività di installazione, uso, assistenza o manutenzione. I seguenti messaggi speciali possono comparire in diverse parti della documentazione oppure sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.

L'aggiunta di questo simbolo a un'etichetta di “Pericolo” o “Avvertimento” indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.

Questo simbolo indica un possibile pericolo. È utilizzato per segnalare all'utente potenziali rischi di lesioni personali. Rispettare i messaggi di sicurezza evidenziati da questo simbolo per evitare da lesioni o rischi all'incolumità personale.

⚠ PERICOLO

PERICOLO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ AVVERTIMENTO

AVVERTIMENTO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ ATTENZIONE

ATTENZIONE indica una situazione di potenziale rischio che, se non evitata, **può provocare** ferite minori o leggere.

AVVISO

Un ***AVVISO*** è utilizzato per affrontare delle prassi non connesse all'incolumità personale.

Nota

Manutenzione, riparazione, installazione e uso delle apparecchiature elettriche si devono affidare solo a personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall'uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, il funzionamento e l'installazione di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

Prima di iniziare

Non utilizzare questo prodotto su macchinari privi di sorveglianza attiva del punto di funzionamento. La mancanza di un sistema di sorveglianza attivo sul punto di funzionamento può presentare gravi rischi per l'incolumità dell'operatore macchina.

⚠ AVVERTIMENTO

APPARECCHIATURA NON PROTETTA

- Non utilizzare questo software e la relativa apparecchiatura di automazione su macchinari privi di protezione per le zone pericolose.
- Non avvicinarsi ai macchinari durante il funzionamento.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Questa apparecchiatura di automazione con il relativo software permette di controllare processi industriali di vario tipo. Il tipo o il modello di apparecchiatura di automazione adatto per ogni applicazione varia in funzione di una serie di fattori, quali la funzione di controllo richiesta, il grado di protezione necessario, i metodi di produzione, eventuali condizioni particolari, la regolamentazione in vigore, ecc. Per alcune applicazioni può essere necessario utilizzare più di un processore, ad esempio nel caso in cui occorra garantire la ridondanza dell'esecuzione del programma.

Solo l'utente, il costruttore della macchina o l'integratore del sistema sono a conoscenza delle condizioni e dei fattori che entrano in gioco durante l'installazione, la configurazione, il funzionamento e la manutenzione della macchina e possono quindi determinare l'apparecchiatura di automazione e i relativi interblocchi e sistemi di sicurezza appropriati. La scelta dell'apparecchiatura di controllo e di automazione e del relativo software per un'applicazione particolare deve essere effettuata dall'utente nel rispetto degli standard locali e nazionali e della regolamentazione vigente. Per informazioni in merito, vedere anche la guida National Safety Council's Accident Prevention Manual (che indica gli standard di riferimento per gli Stati Uniti d'America).

Per alcune applicazioni, ad esempio per le macchine confezionatrici, è necessario prevedere misure di protezione aggiuntive, come un sistema di sorveglianza attivo sul punto di funzionamento. Questa precauzione è necessaria quando le mani e altre parti del corpo dell'operatore possono raggiungere aree con ingranaggi in movimento o altre zone pericolose, con conseguente pericolo di infortuni gravi. I prodotti software da soli non possono proteggere l'operatore dagli infortuni. Per questo motivo, il software non può in alcun modo costituire un'alternativa al sistema di sorveglianza sul punto di funzionamento.

Accertarsi che siano stati installati i sistemi di sicurezza e gli asservimenti elettrici/meccanici opportuni per la protezione delle zone pericolose e verificare il loro corretto funzionamento prima di mettere in funzione l'apparecchiatura. Tutti i dispositivi di blocco e di sicurezza relativi alla sorveglianza del punto di funzionamento devono essere coordinati con l'apparecchiatura di automazione e la programmazione software.

NOTA: Il coordinamento dei dispositivi di sicurezza e degli asservimenti meccanici/elettrici per la protezione delle zone pericolose non rientra nelle funzioni della libreria dei blocchi funzione, del manuale utente o di altre implementazioni indicate in questa documentazione.

Avviamento e verifica

Prima di utilizzare regolarmente l'apparecchiatura elettrica di controllo e automazione dopo l'installazione, l'impianto deve essere sottoposto ad un test di avviamento da parte di personale qualificato per verificare il corretto funzionamento dell'apparecchiatura. È importante programmare e organizzare questo tipo di controllo, dedicando ad esso il tempo necessario per eseguire un test completo e soddisfacente.

⚠AVVERTIMENTO

RISCHI RELATIVI AL FUNZIONAMENTO DELL'APPARECCHIATURA

- Verificare che tutte le procedure di installazione e di configurazione siano state completate.
- Prima di effettuare test sul funzionamento, rimuovere tutti i blocchi o altri mezzi di fissaggio dei dispositivi utilizzati per il trasporto.
- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Eseguire tutti i test di avviamento raccomandati sulla documentazione dell'apparecchiatura. Conservare con cura la documentazione dell'apparecchiatura per riferimenti futuri.

Il software deve essere testato sia in ambiente simulato che in ambiente di funzionamento reale..

Verificare che il sistema completamente montato e configurato sia esente da cortocircuiti e punti a massa, ad eccezione dei punti di messa a terra previsti dalle normative locali (ad esempio, in conformità al National Electrical Code per gli USA). Nel caso in cui sia necessario effettuare un test sull'alta tensione, seguire le raccomandazioni contenute nella documentazione dell'apparecchiatura al fine di evitare danni accidentali all'apparecchiatura stessa.

Prima di mettere sotto tensione l'apparecchiatura:

- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.
- Chiudere lo sportello del cabinet dell'apparecchiatura.
- Rimuovere tutte le messa a terra temporanee dalle linee di alimentazione in arrivo.
- Eseguire tutti i test di avviamento raccomandati dal costruttore.

Funzionamento e regolazioni

Le precauzioni seguenti sono contenute nelle norme NEMA Standards Publication ICS 7.1-1995:

(In caso di divergenza o contraddizione tra una traduzione e l'originale inglese, prevale il testo originale in lingua inglese).

- Indipendentemente dalla qualità e della precisione del progetto nonché della costruzione dell'apparecchiatura o del tipo e della qualità dei componenti scelti, possono sussistere dei rischi se l'apparecchiatura non viene utilizzata correttamente.
- Eventuali regolazioni involontarie possono provocare il funzionamento non soddisfacente o non sicuro dell'apparecchiatura. Per effettuare le regolazioni funzionali, attenersi sempre alle istruzioni contenute nel manuale fornito dal costruttore. Il personale incaricato di queste regolazioni deve avere esperienza con le istruzioni fornite dal costruttore delle apparecchiature e con i macchinari utilizzati con l'apparecchiatura elettrica.
- All'operatore devono essere accessibili solo le regolazioni funzionali richieste dall'operatore stesso. L'accesso agli altri organi di controllo deve essere riservato, al fine di impedire modifiche non autorizzate ai valori che definiscono le caratteristiche di funzionamento delle apparecchiature.

Informazioni sul manuale

Ambito del documento

Questo manuale descrive le caratteristiche e l'uso del modulo di comunicazione Ethernet M580 BMENUA0100 con server OPC UA integrato.

NOTA: Le impostazioni di configurazione specifiche contenute in questa guida sono fornite solo a titolo esplicativo. Le impostazioni necessarie per la configurazione specifica dell'utente possono differire da quelle utilizzate negli esempi della presente guida.

Nota di validità

Il presente documento è valido per un sistema M580 quando utilizzato con EcoStruxure™ Control Expert versione 16.0 o versioni successive di supporto.

Le caratteristiche dei prodotti descritti in questo documento corrispondono a quelle disponibili su www.se.com. Nell'ambito della nostra strategia aziendale per un miglioramento costante, è possibile che il contenuto della documentazione venga revisionato nel tempo per migliorare la chiarezza e la precisione. Se si notano differenze tra le caratteristiche riportate in questo documento e quelle riportate su www.se.com, considerare www.se.com contenente le informazioni più recenti.

Documenti correlati

Titolo della documentazione	Codice prodotto
Modicon M580 Standalone, Guida di pianificazione del sistema per architetture di utilizzo frequente	HRB62666 (inglese), HRB65318 (francese), HRB65319 (tedesco), HRB65320 (italiano), HRB65321 (spagnolo), HRB65322 (cinese)
Modicon M580, Guida di pianificazione del sistema per topologie complesse	NHA58892 (inglese), NHA58893 (francese), NHA58894 (tedesco), NHA58895 (italiano), NHA58896 (spagnolo), NHA58897 (cinese)
Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente	NHA58880 (inglese), NHA58881 (francese), NHA58882 (tedesco), NHA58883 (italiano), NHA58884 (spagnolo), NHA58885 (cinese)
Modicon M580, M340 e X80 I/O, Piattaforme, standard e certificazioni	EIO0000002726 (inglese), EIO0000002727 (francese), EIO0000002728 (tedesco), EIO0000002730 (italiano), EIO0000002729 (spagnolo), EIO0000002731 (cinese)

Titolo della documentazione	Codice prodotto
M580 BMENOS0300 Modulo di switch opzionale di rete, Guida di installazione e configurazione	NHA89117 (ENG) NHA89119 (FRE) NHA89120 (GER) NHA89121 (ITA) NHA89122 (SPA) NHA89123 (CHS)
Modicon M580, Hardware, Manuale di riferimento	EIO0000001578 (inglese), EIO0000001579 (francese), EIO0000001580 (tedesco), EIO0000001582 (italiano), EIO0000001581 (spagnolo), EIO0000001583 (cinese)
Modicon M580, Moduli RIO, Guida di installazione e configurazione	EIO0000001584 (Inglese), EIO0000001585 (Francese), EIO0000001586 (Tedesco), EIO0000001587 (Italiano), EIO0000001588 (Spagnolo), EIO0000001589 (Cinese),
Modicon M580, Modifica della configurazione al volo (CCOTF) Guida utente	EIO0000001590 (inglese), EIO0000001591 (francese), EIO0000001592 (tedesco), EIO0000001594 (italiano), EIO0000001593 (spagnolo), EIO0000001595 (cinese)
Modicon X80, Moduli di I/O digitali, Guida utente	35012474 inglese), 35012475 (tedesco), 35012476 (francese), 35012477 (spagnolo), 35012478 (italiano), 35012479 (cinese)
Modicon X80, BMXEHC0200 Modulo di conteggio, Manuale dell'utente	35013355 inglese), 35013356 (tedesco), 35013357 (francese), 35013358 (spagnolo), 35013359 (italiano), 35013360 (cinese)
Messa a terra e compatibilità elettromagnetica dei sistemi PLC, Principi di base e misure, Manuale dell’utente	33002439 (ENG) 33002440 (FRE) 33002441 (GER) 33002442 (SPA) 33003702 (ITA) 33003703 (CHS)
EcoStruxure™ Control Expert, Struttura e linguaggi di programmazione, Manuale di riferimento	35006144 (inglese), 35006145 (francese), 35006146 (tedesco), 35013361 (italiano), 35006147 (spagnolo), 35013362 (cinese)
EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento	EIO0000002135 (inglese), EIO0000002136 (francese), EIO0000002137 (tedesco), EIO0000002138 (italiano), EIO0000002139 (spagnolo), EIO0000002140 (cinese)
EcoStruxure™ Control Expert, Modalità operative	33003101 (Inglese), 33003102 (Francese), 33003103 (Tedesco), 33003104 (Spagnolo), 33003696 (Italiano), 33003697 (Cinese)
EcoStruxure™ Control Expert, Manuale d'installazione	35014792 (Inglese), 35014793 (Francese), 35014794 (Tedesco), 35014795 (Spagnolo), 35014796 (Italiano), 35012191 (Cinese)

Titolo della documentazione	Codice prodotto
Web Designer for FactoryCast - Guida dell'utente	35016149 (inglese), 35016150 (francese), 35016151 (tedesco), 35016152 (italiano), 35016153 (spagnolo), 35016154 (cinese)
Cybersicurezza piattaforma controller Modicon, Manuale di riferimento	EIO0000001999 (ENG) EIO0000002001 (FRE) EIO0000002000 (GER) EIO0000002003 (SPA) EIO0000002002 (ITA) EIO0000002004 (CHS)

Per trovare i documenti online, visitare il centro download Schneider Electric (www.se.com/ww/en/download/).

Informazioni relative al prodotto

⚠PERICOLO

RISCHIO DI SCOSSA ELETTRICA, ESPLOSIONE O ARCO ELETTRICO

- Mettere fuori tensione tutte le apparecchiature, inclusi i dispositivi collegati, prima di rimuovere qualunque coperchio o sportello, o prima di installare/disinstallare accessori, hardware, cavi o fili, tranne che per le condizioni specificate nell'apposta Guida hardware per questa apparecchiatura.
- Per verificare che l'alimentazione sia isolata, usare sempre un rilevatore di tensione correttamente tarato.
- Prima di riattivare l'alimentazione dell'unità rimontare e fissare tutti i coperchi, i componenti hardware e i cavi e verificare la presenza di un buon collegamento di terra.
- Quando si utilizza questa apparecchiatura e qualunque prodotto associato, usare esclusivamente la tensione specificata.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

⚠AVVERTIMENTO

PERDITA DI CONTROLLO

- Eseguire una modalità FMEA (Perform a Failure Mode and Effects Analysis) o un'analisi dei rischi equivalente dell'applicazione e applicare i controlli di prevenzione e rilevazione prima dell'implementazione.
- Fornire uno stato di posizionamento di sicurezza per sequenze o eventi di controllo indesiderati.
- Fornire percorsi di controllo separati o ridondanti qualora richiesto.
- fornire i parametri appropriati, in particolare per i limiti.
- Esaminare le implicazioni dei ritardi di trasmissione e stabilire azioni di mitigazione.
- Esaminare le implicazioni delle interruzioni del collegamento di comunicazione e stabilire azioni di mitigazione.
- Fornire percorsi indipendenti per le funzioni di controllo (ad esempio, arresto di emergenza, condizioni di superamento limiti e condizioni di guasto) in base alla valutazione dei rischi effettuata e alle normative e regolamentazioni applicabili.
- Applicare le linee guida e le normative di sicurezza di prevenzione incidenti locali.
- Testare ogni implementazione di un sistema per il funzionamento adeguato prima di metterlo in servizio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Con questa apparecchiatura utilizzare esclusivamente il software approvato da Schneider Electric.
- Aggiornare il programma applicativo ogni volta che si cambia la configurazione dell'hardware fisico.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Terminologia derivata dagli standard

I termini tecnici, la terminologia, i simboli e le descrizioni corrispondenti nelle informazioni contenute nel presente documento, o che compaiono nei o sui prodotti stessi, derivano generalmente dai termini o dalle definizioni delle norme internazionali.

Nell'ambito dei sistemi di sicurezza funzionale, degli azionamenti e dell'automazione generale, tali espressioni possono includere, tra l'altro, termini quali *sicurezza*, *funzione di sicurezza*, *stato sicuro*, *guasto*, *reset guasto*, *malfunzionamento*, *errore*, *reset errore*, *messaggio di errore*, *pericoloso* e così via.

Queste norme comprendono, tra le altre:

Norma	Descrizione
IEC 61131-2:2007	Controller programmabili, parte 2: Requisiti per apparecchiature e test.
ISO 13849-1:2023	Sicurezza dei macchinari: Parti di sicurezza dei sistemi di controllo. Principi generali per la progettazione.
EN 61496-1:2020	Sicurezza dei macchinari: Electro-Sensitive Protective Equipment, dispositivo elettrosensibile di protezione. Parte 1: Requisiti generali e test
ISO 12100:2010	Sicurezza dei macchinari - Principi generali di progettazione - Valutazione e riduzione dei rischi
EN 60204-1:2006	Sicurezza dei macchinari - Equipaggiamento elettrico delle macchine - Parte 1: Requisiti generali
ISO 14119:2013	Sicurezza dei macchinari - Dispositivi di interblocco associati alle protezioni - Principi di progettazione e selezione
ISO 13850:2015	Sicurezza dei macchinari - Arresto di emergenza - Principi di progettazione
IEC 62061:2021	Sicurezza dei macchinari - Sicurezza funzionale dei sistemi di controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza
IEC 61508-1:2010	Sicurezza funzionale di sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti generali.
IEC 61508-2:2010	Sicurezza funzionale dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili.
IEC 61508-3:2010	Sicurezza funzionale dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti software.
IEC 61784-3:2021	Reti di comunicazione industriale - Profili - Parte 3: Bus di campo di sicurezza funzionale - Regole generali e definizioni dei profili.
2006/42/EC	Direttiva macchine
2014/30/EU	Direttiva compatibilità elettromagnetica
2014/35/EU	Direttiva bassa tensione

I termini utilizzati nel presente documento possono inoltre essere utilizzati indirettamente, in quanto provenienti da altri standard, quali:

Standard	Descrizione
Serie IEC 60034	Macchine elettriche rotative
Serie IEC 61800	Variatori di velocità elettrici regolabili
Serie IEC 61158	Comunicazioni dati digitali per misurazioni e controlli – Bus di campo per l'uso con i sistemi di controllo industriali

Infine, l'espressione *area di funzionamento* può essere utilizzata nel contesto di specifiche condizioni di pericolo e in questo caso ha lo stesso significato dei termini *area pericolosa* o *zona di pericolo* espressi nella *Direttiva macchine* (*2006/42/EC*) e *ISO 12100:2010*.

NOTA: Gli standard indicati in precedenza possono applicarsi o meno ai prodotti specifici citati nella presente documentazione. Per ulteriori informazioni relative ai singoli standard applicabili ai prodotti qui descritti, vedere le tabelle delle caratteristiche per tali codici di prodotti.

Marchi

Windows è un marchio registrato di Microsoft Corporation.

Informazioni sulla terminologia non inclusiva o insensibile

In quanto parte di un gruppo di aziende responsabili e inclusive, stiamo aggiornando la nostra comunicazione contenente terminologia non inclusiva. Fino al completamento di questo processo, tuttavia, potrebbero essere ancora presenti termini del settore standardizzati e ritenuti inappropriati dai nostri clienti.

Caratteristiche del modulo BMENUA0100

Introduzione

Questo capitolo descrive il modulo di comunicazione BMENUA0100 Ethernet con server OPC UA integrato.

Caratteristiche del modulo

Introduzione

Il modulo server OPC UA Modicon BMENUA0100 porta capacità OPC UA ad alte prestazioni nei sistemi di controllo Modicon M580.

OPC UA è una piattaforma di comunicazione aperta e sicura per le comunicazioni industriali, progettata per essere flessibile e scalabile dai sensori IoT a risorse vincolate nel campo ai server di livello aziendale presenti nel data center o nel cloud. Oltre al collegamento e allo spostamento dei dati, OPC UA definisce un modello informativo completo per pubblicare e gestire meta informazioni e contesto del sistema per semplificare integrazione di sistema e ingegneria dell'automazione.

Nella realizzazione di uno standard di comunicazione per attività industriali connesse moderne, OPC UA fornisce un collegamento comune tra prodotti collegati nei controller del campo e applicazioni e analisi aziendali. È progettato per la compatibilità con infrastrutture IT e di protezione come firewall, VPN e proxy. OPC UA è scalabile per ampiezza di banda e requisiti funzionali.

Caratteristiche

Il modulo BMENUA0100 include un server OPC UA e uno switch Ethernet integrato. È incluso nel **Catalogo hardware** di Control Expert nel gruppo del modulo di **Comunicazione**.

Il BMENUA0100 porta le seguenti funzionalità alla piattaforma Modicon M580:

Generale:

- Accesso diretto e ottimizzato al dizionario dati di Control Expert per la mappatura tra Control Expert e variabili OPC UA, pagina 48.
- Supporto per configurazioni Hot Standby tramite ridondanza, pagina 53 OPC UA.

- Compatibilità con i sistemi M580 di sicurezza come modulo non interferente di tipo 1 come definito da TÜV Rheinland.
- Comunicazioni backplane Ethernet senza interferenze.
- Client DHCP/FDR per il download di impostazioni di configurazione memorizzate (senza sicurezza informatica).
- Sincronizzazione di client e server, pagina 126 dell'ora NTP.
- Metodi di diagnostica multipli, inclusi LED, pagina 134, DDT, pagina 139, variabili ed elementi dati, pagina 150 OPC_UA, Syslog, pagina 154, Modbus, pagina 158, SNMP, pagina 159 e pagine Web sicure, pagina 160.
- Aggiornamento del firmware tramite Strumento EcoStruxure™ Automation Device Maintenance, pagina 169.
- Controllo di integrità del firmware.
- Memorizzazione protetta hardware.

Sicurezza informatica:

- Comunicazioni sicure tramite HTTPS, OPC UA (opzionale) e IPsec (opzionale).
- Sicurezza, pagina 94 OPC UA a livello di modulo configurabile tramite HTTPS.
- La possibilità di controllare il flusso di comunicazioni interno ed esterno abilitando e disabilitando i servizi di comunicazione, pagina 96.
- IPsec, pagina 101 basato su una chiave precondivisa (PSK) per la protezione di servizi come SNMPv1, Modbus/TCP, Syslog e NTPv4.

  NOTA: Il BMENUA0100 supporta IPsec modalità principale. Un canale IPsec può essere aperto dal server BMENUA0100 o da un client OPC UA remoto. Su un client PC, IPsec è supportato e convalidato su sistemi Windows 7, 10 e Windows server 2016.

Gestione dell'autenticazione:

- Controllo di accesso basato su ruolo (RBAC) e autenticazione utente, pagina 113 per HTTPS e client OPC UA.
- Certificati, pagina 105 per entità di applicazione client OPC UA.

Il modulo di comunicazione M580 contiene:

- Porta backplane Ethernet per comunicazione Ethernet su rack principale locale Ethernet.
- Porta backplane X bus per alimentazione a 24 Vcc e indirizzamento rack.
- Sincronizzazione di client e server dell'ora NTP, pagina 126.

Descrizione del modulo

Introduzione

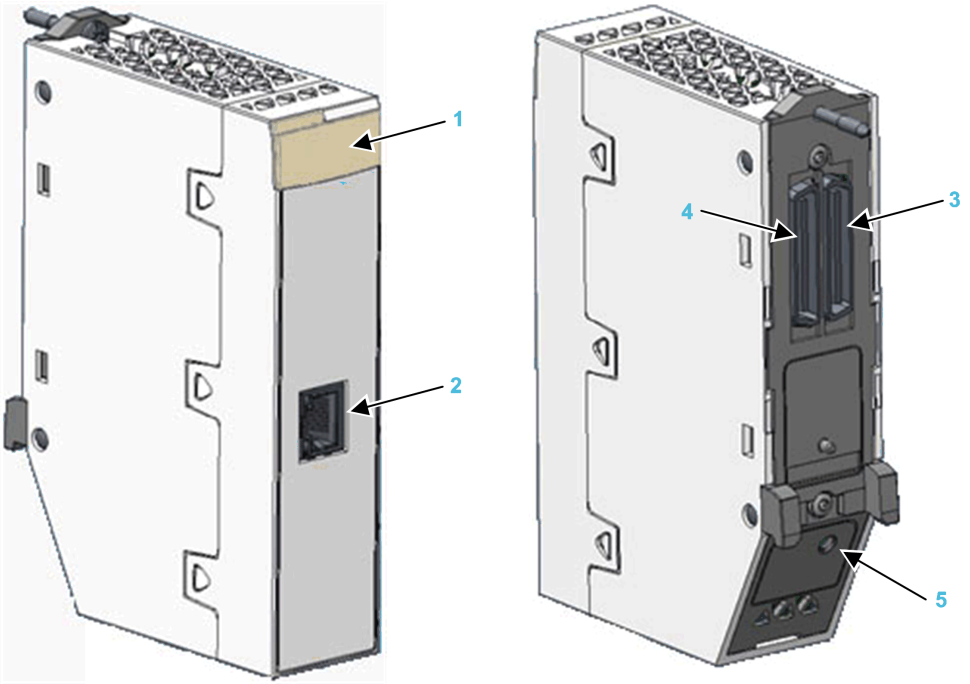
Schneider Electric offre due moduli di comunicazione Ethernet con un server OPC UA integrato per comunicazione con client OPC UA, compreso SCADA:

- Modulo BMENUA0100 per ambienti standard.
- Modulo BMENUA0100H per ambienti critici.

Il modulo può essere installato solo in uno slot Ethernet, su un rack Ethernet principale, locale. Consultare l'argomento *Configurazioni supportate del modulo BMENUA0100*, pagina 61 per una descrizione delle posizioni supportate del modulo, compreso il numero massimo di moduli BMENUA0100 che è possibile inserire in un rack.

Descrizione fisica

Questa figura mostra le caratteristiche esterne del modulo BMENUA0100:



1 Array di LED

2 Porta di controllo con LED di attività e collegamento Ethernet

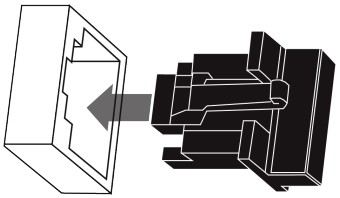
3 Porta backplane Ethernet

4 Porta backplane X Bus

5 Selettore a rotazione della modalità operativa di sicurezza informatica

Per informazioni sulla lettura dei LED del modulo, consultare l'argomento Diagnostica LED, pagina 134.

Se la porta di controllo Ethernet non è abilitata, utilizzare il fermo fornito con ogni modulo per impedire che nella porta di controllo entrino oggetti estranei:



Porte esterne

Il modulo BMENUA0100 include le seguenti porte esterne:

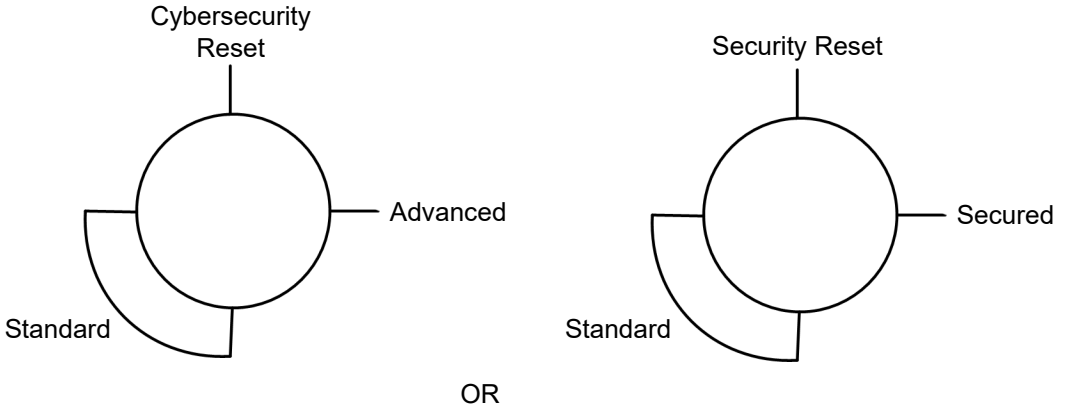
Porta	Descrizione
Porta di controllo	La porta di controllo è la porta singola posta sulla parte anteriore del modulo BMENUA0100. Le funzionalità comprendono: • La porta di controllo, quando è abilitata, costituisce l'interfaccia esclusiva per le comunicazioni OPC UA, tranne quando è configurato IPv6. ◦ Quando IPv6 è configurato, la porta backplane e la porta di controllo possono essere utilizzate per le comunicazioni OPC UA. ◦ Quando IPv6 non è configurato, è anche possibile collegare i client OPC UA situati sulla rete backplane tramite la porta di controllo di BMENUA0100 se nel computer che ospita il client OPC UA è stato definito/dichiarato un percorso. • Velocità operativa fino a 1 Gb/s. Quando si opera alla velocità di: ◦ 1 Gb/s, utilizzare solo cavi di rame a quattro paia intrecciati schermati CAT6. ◦ 10/100 Mb/s, utilizzare cavi di rame a quattro paia intrecciati schermati CAT5 o CAT6. • Doppio stack IP che supporta indirizzamento IP IPv4 (32 bit) e IPv6 (128 bit): ◦ IPv4 e IPv6 sono configurati per il modulo. ◦ La configurazione IPv6 può essere statica o dinamica (via SLAAC). ◦ L'impostazione predefinita, pagina 117 IPv4 è assegnata automaticamente in base all'indirizzo MAC del modulo, se non è configurato un indirizzo IP. • Accesso sicuro al server OPC UA tramite i protocolli IPv4 e IPv6. • Protocollo sicuro HTTPS (su IPv4) per aggiornamento del firmware, pagina 169 e configurazione della sicurezza informatica, pagina 86. • Supporto protocollo sicuro NTPv4. • Sicurezza IPsec fornita per servizi non sicuri, compresi SNMPv1, Modbus TCP e Syslog.
Porta backplane Ethernet	La porta backplane BMENUA0100 Ethernet supporta il protocollo IPv4 (32 bit). Quando la porta di controllo è disabilitata, la porta backplane può supportare le comunicazioni OPC UA; la porta backplane comprende le seguenti caratteristiche: • Velocità operativa fino a 100 Mb/s. • Connettività Modbus TCP IPv4 Ethernet con il controller: ◦ La porta backplane Ethernet è la porta esclusiva per la diagnostica Modbus. • Porta esclusiva per configurazione non di sicurezza informatica (IP, NTPv4, SNMPv1), tramite: ◦ Control Expert v14.1 e versioni successive di supporto ◦ Server FDR/DHCP • Se la porta di controllo è disabilitata, la porta backplane Ethernet fornisce accesso sicuro al server OPC UA tramite il protocollo IPv4 e supporta i servizi seguenti: ◦ Protocollo sicuro HTTPS per aggiornamento del firmware, pagina 169 e configurazione della sicurezza informatica, pagina 86. ◦ NTPv4, SNMPv1/v3 e Syslog.
Porta backplane X Bus	Il modulo BMENUA0100 utilizza la comunicazione backplane X Bus per: • Ricevere l'alimentazione 24 Vcc. • Rilevare l'indirizzo di rack e slot del modulo BMENUA0100. **NOTA:** Tramite la porta backplane X Bus del modulo BMENUA0100 non viene effettuata nessun'altra comunicazione.

Selettore a rotazione

Sul retro del modulo si trova un selettore a rotazione a quattro posizioni. Impostare questo selettore a rotazione per configurare una modalità per il controller

NOTA: Per maggiore comodità, è fornito un cacciavite in plastica, o equivalente, da utilizzare per cambiare la posizione del selettore a rotazione. Non utilizzare cacciaviti metallici

In base alla versione in uso del modulo, le posizioni del selettore a rotazione sono:



Le impostazioni sono:

- Modalità Advanced (RL 6 e successive) o Secured (precedente a RL 6), pagina 30
- Modalità Standard, pagina 30
- Cybersecurity Reset (RL 6 e successive) o Security Reset (precedente a RL 6), pagina 31

NOTA:

- Il selettore a rotazione non è accessibile quando si posiziona il modulo sul rack.
- In un sistema Hot Standby, verificare che le posizioni del selettore a rotazione del modulo BMENUA0100, nei rack principali locali primario e di standby, siano uguali. Il sistema non esegue automaticamente questa verifica.

Per informazioni su ciascuna impostazione della posizione del selettore a rotazione, consultare la descrizione delle modalità operative di sicurezza informatica, pagina 28.

LED del modulo

Display a LED

Un pannello di visualizzazione a 7 LED è posizionato sulla parte frontale del modulo BMENUA0100:

Le informazioni del display a LED sul modulo sono le seguenti:

LED	Descrive lo stato del modulo
RUN	Condizione di funzionamento.
ERR	Errori rilevati.
UACNX	Connessioni OPC UA.
BS	Porta backplane.
NS	Porta di controllo.
SEC	Condizione di sicurezza informatica.
BUSY	Stato del dizionario dati.

Consultare l'argomento Diagnostica LED, pagina 134 per informazioni su come utilizzare questi LED per diagnosticare lo stato del modulo BMENUA0100.

LED della porta di controllo

La porta di controllo, sulla parte anteriore del modulo, presenta due LED che descrivono lo stato del collegamento Ethernet sulla porta:

- Il LED ACT indica la presenza di attività Ethernet sulla porta.
- Il LED LNK indica l'esistenza di un collegamento Ethernet e la sua velocità.

Consultare l'argomento Diagnostica LED, pagina 138 per informazioni su come utilizzare i LED della porta di controllo per diagnosticare lo stato della porta di controllo del modulo BMENUA0100.

Standard e certificazioni

Panoramica

Questo capitolo descrive standard e certificazioni validi per il modulo di comunicazioni Ethernet BMENUA0100 con server OPC UA integrato.

Standard e certificazioni

Download

Fare clic sul collegamento corrispondente alla lingua preferita per scaricare gli standard e le certificazioni (formato PDF) validi per i moduli in questa linea di prodotti:

Titolo	Lingue
Modicon M580, M340 e X80 I/O, Piattaforme, standard e certificazioni	• Inglese: EIO0000002726 • Francese: EIO0000002727 • Tedesco: EIO0000002728 • Italiano: EIO0000002730 • Spagnolo: EIO0000002729 • Cinese: EIO0000002731

Modulo standard BMENUA0100

Requisiti normativi

Il modulo di comunicazione BMENUA0100 OPC UA Ethernet integrato è conforme ai seguenti standard normativi:

Marcatura	Requisito
OPC Unified Architecture	OPC UA V1.03: protocollo di comunicazione tra macchina e macchina OPC Unified Architecture.

Compatibilità del firmware BMENUA0100 con EcoStruxure™ Control Expert

Compatibilità

Le applicazioni create con il software EcoStruxure™ Control Expert sono compatibili con il firmware del modulo BMENUA0100 nel seguente modo:

Versione firmware del BMENUA0100	EcoStruxure™ Control Expert Versione software	
	14.0	**15.0 o successiva**
1.01	Pienamente compatibile	Solo le funzionalità precedenti della versione firmware 1.01 sono supportate dal software[1, 2, 3]
1.10	Pienamente compatibile	Pienamente compatibile

1. Se un modulo BMENUA0100 con versione firmware 1.01 riceve un'applicazione generata con EcoStruxure™ Control Expert V15 dove:
   - La **Frequenza di campionamento rapida** è **Attivata** (nella scheda IPConfig, pagina 118), questa impostazione non viene implementata.
   - IPv4 è disattivato per la porta di controllo; la porta di controllo del modulo viene configurata con l'indirizzo IPv4 visualizzato in grigio nella scheda **IPConfig** del modulo.

     NOTA: L'indirizzo IPv4 in grigio può essere l'indirizzo IPv4 di ingresso utente più recente o l'indirizzo IPv4 immesso automaticamente dal software EcoStruxure™ Control Expert (172.16.12.1) se non è stato immesso alcun indirizzo IPv4 in precedenza.
   - NTP, pagina 128 è stato configurato con un indirizzo IPv6, le pagine Web del modulo indicano erroneamente che NTP è operativo quando il servizio NTP in realtà non è operativo.

2. Se due moduli BMENUA0100 con versione firmware 1.01 sono configurati in un rack Hot Standby con EcoStruxure™ Control Expert V15, le limitazioni descritte nei punti precedenti si applicano anche a questi moduli.

3. Se SNMP è attivato in Control Expert, includere l'indirizzo IPv4 del gestore SNMP nella scheda SNMP del modulo, pagina 130 BMENUA0100 in modo che il gestore SNMP possa accedere al MIB SNMP.

NOTA: Le pagine Web visualizzate per il modulo BMENUA0100 dipendono dalla versione del firmware del modulo (ad esempio versione 1.01, 1.10 o 2.01).

Descrizione funzionale di BMENUA0100

Introduzione

Questo capitolo descrive le funzioni supportate del modulo di comunicazione BMENUA0100 Ethernet con server OPC UA integrato.

Impostazioni modalità operativa di sicurezza informatica

Introduzione

Il modulo BMENUA0100 può essere configurato per funzionare in modalità Advanced (o Secured) o Standard. Il selettore a rotazione a 4 posizioni sul retro del modulo determina la modalità operativa.

Le tre posizioni dei selettori a rotazione sono:

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

NOTA:

- La configurazione predefinita del modulo è la modalità Advanced (o Secured).
- È possibile visualizzare la posizione del selettore a rotazione nella pagina Home, pagina 91 delle pagine Web del modulo.

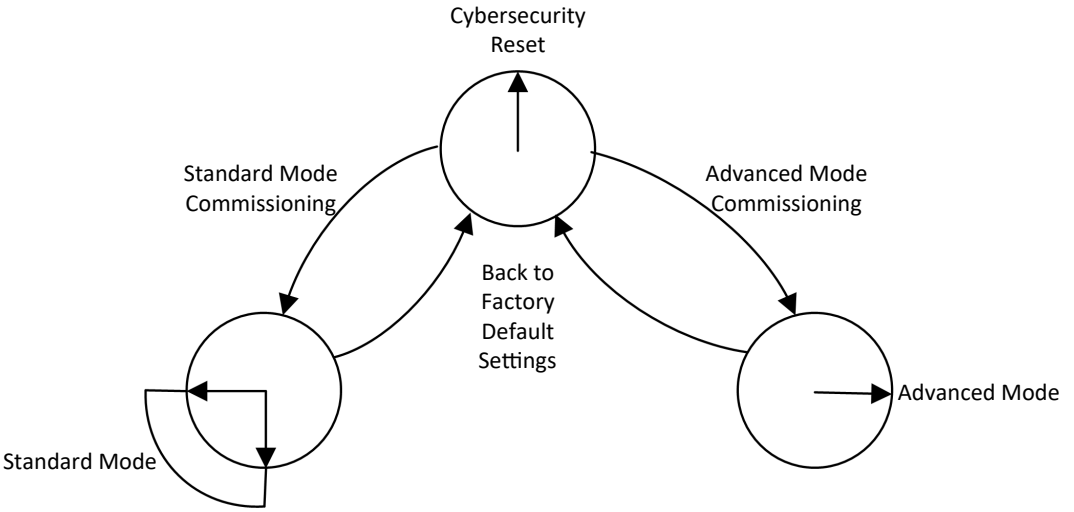
Poiché il selettore a rotazione non è accessibile mentre il modulo è sul rack, la posizione del commutatore può essere modificata solo quando il modulo viene spento e rimosso dal rack. Dopo aver selezionato una nuova posizione del selettore, il modulo può essere reinserito nel rack e acceso.

NOTA: utilizzare solo il piccolo cacciavite in plastica fornito con il modulo, pagina 23 per cambiare la posizione del selettore e configurare una modalità operativa di sicurezza informatica.

Modifica della modalità di funzionamento

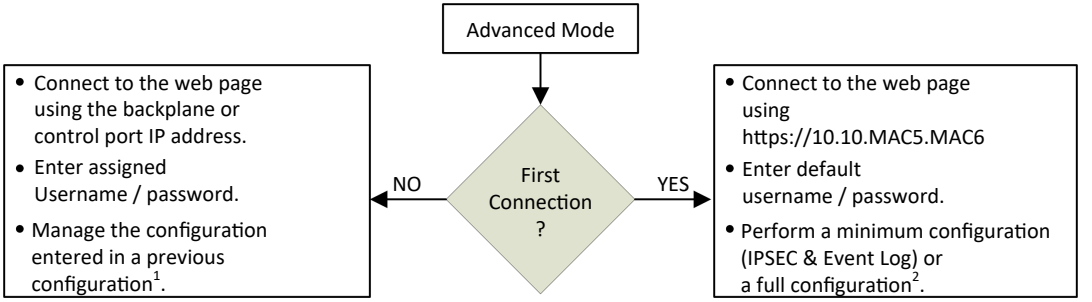
Ogni volta che si commuta la modalità operativa di sicurezza informatica dalla modalità Advanced (o Secured) alla modalità Standard, o dalla modalità Standard alla modalità Advanced (o Secured), eseguire un'operazione di Cybersecurity (o Security) Reset, pagina 82 prima di configurare la nuova modalità.

La posizione del selettore a rotazione determina lo stato operativo del modulo come segue:



Un nuovo modulo (con impostazione predefinita) o un modulo per cui è stato eseguito un **Cybersecurity (o Security) Reset**, può essere messo in servizio per il funzionamento in modalità Standard, pagina 82 o modalità Advanced (o Secured), pagina 80.

Il processo di configurazione del modulo per il funzionamento in modalità Advanced (o Secured) varia a seconda che ci si colleghi alle impostazioni di configurazione del modulo per la prima volta dopo aver eseguito un Cybersecurity (o Security) Reset:



1 Per informazioni sulla gestione della configurazione, vedere il capitolo sulla configurazione, pagina 86.

2 Per informazioni sull'esecuzione di una configurazione alla prima connessione, vedere la sezione Messa in servizio in modalità Advanced (o Secured), pagina 80.

Modalità Advanced (o Secured)

Quando si opera in modalità Advanced (o Secured), il modulo non avvia le comunicazioni di processo (sulla porta di controllo o sulla porta backplane) finché non sono state configurate le impostazioni di sicurezza informatica valide. Dopo aver configurato la modalità Advanced (o Secured), è possibile configurare le impostazioni di sicurezza informatica utilizzando le pagine Web del modulo, pagina 86, accessibili tramite il protocollo HTTPS sulle porte backplane o di controllo. In modalità Advanced (o Secured), il modulo supporta il livello di sicurezza informatica specificato nella configurazione di sicurezza informatica. Solo dopo aver configurato le impostazioni di sicurezza informatica, è possibile configurare le impostazioni di indirizzo IP, client NTP e agente SNMP, pagina 117 tramite il software di configurazione Control Expert.

Modalità Standard

Quando si opera in modalità Standard, le comunicazioni del modulo possono iniziare senza la necessità di una configurazione di sicurezza informatica. Le impostazioni di sicurezza informatica non sono necessarie e non possono essere configurate. È possibile configurare solo l'indirizzo IP e altre impostazioni disponibili in Control Expert.

Cybersecurity (o Security) Reset

Il comando **Cybersecurity (o Security) Reset** ripristina le impostazioni di configurazione predefinite. Vengono eliminate tutte le configurazioni di sicurezza informatica esistenti, i white list, i certificati e le impostazioni di controllo dell'accesso basato sui ruoli. Per completare l'operazione di Cybersecurity (o Security) Reset, spegnere e riaccendere il modulo BMENUA0100 o rimuoverlo fisicamente dal rack (che viene così spento), quindi reinserire il modulo nel rack (che viene così riacceso). Mentre il processo di ripristino delle impostazioni predefinite di fabbrica è in corso, il LED **RUN** lampeggia in verde. Al termine del processo, il LED **RUN** diventa verde fisso e i servizi sono disattivati.

Questa impostazione può essere effettuata mediante il selettore a rotazione o le pagine Web (quando si opera in modalità Advanced o Secured):

- Se impostato tramite selettore a rotazione: il modulo smette di funzionare finché non viene rimosso dal rack, il selettore a rotazione viene riposizionato su Advanced (o Secured) o Standard e il modulo viene nuovamente inserito nel rack. È necessario applicare le configurazioni necessarie.
- Con impostazione tramite le pagine Web: al termine del ciclo di spegnimento/riaccensione per portare il modulo (o sostituzione a caldo) in modalità Standard o Advanced (o Secured). È necessario configurare sicurezza informatica e l'indirizzo IP.

  NOTA: Dopo un Cybersecurity (or Security) Reset del modulo BMENUA0100, al modulo si applicano le seguenti condizioni:

  - Non viene mantenuto alcun certificato dispositivo.
  - Tutti i servizi sono disattivati ad eccezione del protocollo HTTPS, utilizzato per creare la configurazione della sicurezza informatica tramite la porta di controllo.
  - Vengono applicate le impostazioni predefinite, tra cui:
    - Impostazioni predefinite, pagina 31 di nome utente/password.
    - Impostazione predefinita dell'indirizzo IP 10.10.MAC5.MAC6, pagina 117.

  NOTA: Se gli ultimi due byte dell'indirizzo MAC (*MAC5.MAC6*) corrispondono a *0,0* nell'indirizzo predefinito, effettuare una connessione via cavo punto a punto tra il computer e il controller, il modulo di comunicazione o un altro modulo.

Combinazione nome utente/password predefinita

La combinazione nome utente/password predefinita dipende dall'impostazione della modalità operativa di sicurezza informatica:

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

NOTA: Il sistema chiede di modificare la password al primo utilizzo in modalità Advanced (o Secured). Verificare leggi e regolamentazioni locali per accertarsi che si tratti di un requisito.

Funzioni supportate dalle modalità operative Advanced (o Secured) e Standard

Le funzioni seguenti sono supportate dal modulo BMENUA0100 in modalità Advanced (o Secured) e Standard:

Modalità	**Modalità Standard**			**Modalità Advanced (o Secured)**		
Porta di controllo	**Disattiva**	**Attiva**		**Disattiva**	**Attiva**	
Porta Ethernet	**Backplane**	**Backplane**	**Porta di controllo**	**Backplane**	**Backplane**	**Porta di controllo**
OPC UA Comm	Sì	No	Sì	Sì	No	Sì
Impostazioni di sicurezza (4)	Nessuno	–	Nessuno	Nessuno, Firma, Firma e codifica (valore predefinito)	–	Nessuno, Firma, Firma e codifica (valore predefinito)
Autenticazione utente	Nessuna autenticazione (anonima)	–	Nessuna autenticazione (anonima)	Operatore, Tecnico, Nessuna autenticazione (anonimo)	–	Operatore, Tecnico, Nessuna autenticazione (anonimo)
SNMP V1	Sì (1, 2)	Sì (1, 2)	Sì (1, 2)	Sì (1)	Sì (1)	Sì (1)
SNMP V3	Sì (1, 2)	Sì (1, 2)	Sì (1, 2)	Sì (1)	Sì (1)	Sì (1)
NTP V4	Solo client (1)	Client (1), Server	Sì, solo client (1)	Solo client (1)	Client (1), Server	Sì, solo client (1)
Registro eventi	No	No	No	Sì	Sì	Sì
IPsec	No	No	No	No	No	Sì per Modbus, SNMP V1/V3, NTP V4 (3) e Syslog (IPsec attivato per impostazione predefinita)
Modifica configurazione Web CS (HTTPS)	No	No	No	Sì	Sì	Sì

Modalità	**Modalità Standard**			**Modalità Advanced (o Secured)**		
Porta di controllo	**Disattiva**	**Attiva**		**Disattiva**	**Attiva**	
Porta Ethernet	**Backplane**	**Backplane**	**Porta di controllo**	**Backplane**	**Backplane**	**Porta di controllo**
Autenticazione utente	–	–	–	Admin	Admin	Admin
Servizi di rete - Abilitazione/ disabilitazione server di comunicazione	Se supportata, sempre abilitata (vedere sopra)	Se supportata, sempre abilitata (vedere sopra)	Se supportata, sempre abilitata (vedere sopra)	Tutti i servizi sono configurabili (disattivato per impostazione predefinita)	Tutti i servizi sono configurabili (disattivato per impostazione predefinita)	Tutti i servizi sono configurabili (disattivato per impostazione predefinita)
Diagnostica Web (solo pagine Home e Diagnostica)	Sì	Sì	Sì	Sì	Sì	Sì
Autenticazione utente	Installatore (credenziali predefinite)	Installatore (credenziali predefinite)	Installatore (credenziali predefinite)	Admin, Operatore, Tecnico, Installatore	Admin, Operatore, Tecnico, Installatore	Admin, Operatore, Tecnico, Installatore
Aggiornamento firmware (HTTPS)	Sì	Sì	Sì	Sì	Sì	Sì, se HTTPS è abilitato
Autenticazione utente	Installatore (credenziali predefinite)	Installatore (credenziali predefinite)	Installatore (credenziali predefinite)	Installatore	Installatore	Installatore
Filtraggio: Inoltra tutto	–	–	(sempre abilitato)	–	–	Inoltra tutti i protocolli
Filtraggio: Protocollo di inoltro configurato	–	–	–	–	–	Inoltro dei protocolli configurati

Modalità	**Modalità Standard**			**Modalità Advanced (o Secured)**		
Porta di controllo	**Disattiva**	**Attiva**		**Disattiva**	**Attiva**	
Porta Ethernet	**Backplane**	**Backplane**	**Porta di controllo**	**Backplane**	**Backplane**	**Porta di controllo**
Filtraggio: Flussi di dati Control Expert a rete dispositivi (controller incluso) (FTP, EIP, Esplicito, Modbus, Ping) solo tramite IPv4[5]	–	–	Inoltro dei flussi dati Control Expert dalla rete di controllo alla rete di dispositivi (sempre abilitato)	–	–	Inoltro dei flussi dati Control Expert dalla rete di controllo alla rete di dispositivi (disattivato per impostazione predefinita)

1. Configurabile con Control Expert.
2. In modalità standard, la versione SNMP del modulo BMENUA0100 è impostata in Control Expert. Se SNMP è impostato a V3 e il modulo è configurato con:
   - Firmware versione 2 (BMENUA0100.2), utilizza SNMP V3 con livello di sicurezza senza autorizzazione né privacy.
   - Firmware precedente alla versione 2 (BMENUA0100), utilizza SNMP V1.

   Per ulteriori informazioni, vedere l'argomento Configurazione agente SNMP in Control Expert e le pagine Web, pagina 130.
3. È possibile configurare NTP V4 per il trasporto all'esterno del tunnel IPsec.
4. Per le modalità operative di sicurezza informatica Standard e Advanced (o Secured), se Impostazioni di sicurezza è impostato su *Nessuna*, non esiste autenticazione utente (ossia **Tipi token identificativo utente** Impostazione OPC UA, pagina 103 è impostata su *Anonimo*.)
5. Per consentire a Control Expert di accedere online al controller o alla rete di dispositivi, configurare il PC (su cui è installato Control Expert) con un indirizzo IP sulla stessa sottorete della porta di controllo del modulo BMENUA0100 e utilizzare l'indirizzo IP della porta di controllo del modulo BMENUA0100 come indirizzo IP del gateway del PC. In questo caso, nessun indirizzo IP del PC può essere sulla stessa sottorete della porta backplane del modulo BMENUA0100.

Servizi OPC UA

Introduzione

Questa sezione descrive i servizi supportati dal server OPC UA integrato nel modulo BMENUA0100.

Caratteristiche operative del server OPC UA BMENUA0100

Limitazioni

Il valore massimo:

- Il numero di nodi che possono essere pubblicati nello spazio indirizzo di accesso ai dati del server OPC UA BMENUA0100 è 100000 nodi.
- La quantità di memoria che può essere allocata al server OPC UA BMENUA0100 è 192 MB.

NOTA: se uno dei due limiti viene superato, lo stato dello spazio indirizzi del server passa allo stato *LimitiSuperati*.

NOTA: il tempo necessario per stabilire la sottoscrizione dell'ora può dipendere in modo significativo dal numero di elementi e dal numero di client collegati.

Altre limitazioni, il contesto in cui si verificano e le relative conseguenze in caso di superamento sono indicati di seguito:

Limite	Valore	Servizio OPCUA	Parametro di servizio	Effetti
Conteggio sessioni cumulative	10	*CreateSession*	(Non applicabile)	Codice risultato servizio *Errore_TroppeSessioni*
Timeout sessione minimo	30 s	*CreateSession*	Timeout sessione richiesto	Timeout sessione rivista
Timeout sessione cumulativa	3600 s	*CreateSubscription*	SessionTimeout richiesto	Timeout revisedSession
Numero massimo di sottoscrizioni cumulative	40	*CreateSubscription*	(Non applicabile)	Codice risultato servizio *Errore_TroppeSottoscrizioni*
Intervallo di pubblicazione minimo	250 ms[1] 20 ms[2]	*CreateSubscription*	Intervallo di pubblicazione richiesto	IntervalloPubblicazioneRivisto
Intervallo di pubblicazione massimo	10 s	*CreateSubscription*	Intervallo di pubblicazione richiesto	IntervalloPubblicazioneRivisto
Durata massima sottoscrizione	300 s	*CreateSubscription*	Min(Intervallo di pubblicazione richiesto, 3600000) * Conteggio del tempo di vita richiesto	Conteggio del tempo di vitaRivisto
Numero massimo di notifiche per	12500	*CreateSubscription*	maxNotifichePerPubblicazione	La capacità massima delle notifiche è quindi (1000/

Limite	Valore	Servizio OPCUA	Parametro di servizio	Effetti
pubblicazione				reviewPublishingInterval) * 1000 notifiche al secondo.
Intervallo di campionamento minimo	125 ms[1] 20 ms[2]	*CreateMonitoredtems*	MonitoraggioParametri. IntervalloCampionamento	Intervallo campionamento rivisto
Dimensioni massime coda messaggi	100	*CreateMonitoredtems*	MonitoraggioParametri. Dimensione coda	Dimensione coda rivista
Numero massimo di elementi monitorati cumulativi	50010 o 35010[3, 4] 2010[2]	*CreateMonitoredtems*	(Non applicabile)	Codice risultato servizio *Errore_ TroppiElementiMonitorati*
Numero massimo di sottoscrizioni per sessione	4	–	–	–
Numero massimo di elementi monitorati per sottoscrizione	25000	–	–	–

1. Se il campionamento rapido è disattivato.
2. Se il campionamento rapido è attivato.
3. Se il campionamento rapido è disattivato e il server è configurato con:
   - un intervallo di campionamento di almeno 1 secondo e
   - intervallo di pubblicazione di almeno 1 secondo.
4. Se Il timestamp di origine è abilitato e attivato, pagina 121, il massimo è 35010. Se non è attivato, il massimo è 50010.

Server OPC UA

Introduzione

Lo scopo principale del modulo di comunicazione Ethernet BMENUA0100 è fornire un canale di comunicazione OPC UA su Ethernet tra controller M580 e client OPC UA. I dati del controller M580 vengono assegnati a variabili nel modulo BMENUA0100 e resi disponibili per i client OPC UA tramite uno stack di comunicazione del server OPC UA integrato nel modulo BMENUA0100. I client OPC UA si collegano allo stack del server OPC

UA integrato utilizzando l'indirizzo IP della porta di controllo o backplane del modulo BMENUA0100, stabilendo così una connessione client server. Il modulo BMENUA0100 è in grado di gestire un massimo di dieci (10) connessioni client OPC UA simultanee per la versione firmware 1.1 (o tre (3) connessioni client OPC UA simultanee per la versione firmware 1.0).

NOTA: I termini di ogni connessione tra un client OPC UA e il server OPC UA integrato nel modulo BMENUA0100 sono determinati dal client, che imposta gli attributi della connessione tra il client e il server.

Lo stack del server OPC UA integrato nel modulo BMENUA0100 consiste di funzionalità definite dai termini seguenti:

- Profilo: una definizione di funzionalità che comprende altri profili, facet, gruppi di conformità e unità di conformità.
- Facet: definisce una funzionalità parziale.
- Gruppo di conformità: una raccolta di unità di conformità.
- Unità di conformità: un servizio specifico, ad esempio, lettura, scrittura e così via.

Profilo BMENUA0100 supportato

Il modulo BMENUA0100 supporta il **profilo Server UA 2017 integrato**. Come indicato nel sito Web OPC Foundation, questo profilo: è un profilo completo destinato a dispositivi con più di 50 MB di memoria e un processore più potente. Questo profilo si basa sul profilo server del dispositivo integrato Micro. Le aggiunte più importanti sono: supporto per la sicurezza tramite i criteri di sicurezza e supporto per il Facet server sottoscrizione DataChange standard. Questo profilo richiede inoltre che i server espongano tutti i tipi OPC-UA utilizzati dal server, inclusi i relativi componenti e i relativi super tipi."

Per ulteriori informazioni, consultare il sito Web di OPC Foundation all'indirizzo: http://opcfoundation.org/UA-Profile/Server/EmbeddedUA2017.

Facet BMENUA0100 supportati

Il modulo BMENUA0100 supporta i seguenti facet:

- **Categoria server > Facet > Caratteristiche principali**:
  - **Facet server Core 2017** (http://opcfoundation.org/UA-Profile/Server/Core2017Facet)

- **Categoria server > Facet > Accesso dati**:
  - **Facet server tipo complesso 2017** (http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017)
  - **Facet server accesso dati** (http://opcfoundation.org/UA-Profile/Server/DataAccess)
  - **Facet server sottoscrizione DataChange integrato** (http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription)
- **Categoria server > Facet > Funzionalità generiche**:
  - **Facet server di metodo** (http://opcfoundation.org/UA-Profile/Server/Methods)
- **Categoria sicurezza > Facet > Criteri di sicurezza**:
  - **Basic128RSA15** (http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15)
  - **Basic256** (http://opcfoundation.org/UA/SecurityPolicy#Basic256)
  - **Basic256Sha256** (http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256)
- **Categoria trasporto > Facet > Client-Server**:
  - **UA-TCP- UA-SC UA-Binary** (http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary)

Gli argomenti seguenti descrivono i servizi correlati ai facet indicati sopra, supportati dal modulo BMENUA0100.

Servizi stack del server OPC UA BMENUA0100

Servizi OPC UA supportati

Lo stack del server OPC UA del modulo BMENUA0100 supporta i seguenti servizi e set di servizi:

Set di servizi	Servizi
Attributo	• Lettura • Scrittura
Discovery	• FindServers • GetEndpoints
MonitoredItem	• CreateMonitoredItems • ModifyMonitoredItems • DeleteMonitoredItems • SetMonitoringMode
SecureChannel	• OpenSecureChannel • CloseSecurechannel

Set di servizi	Servizi
Sessione	• CreateSession • ActivateSession • CloseSession
Subscription	• CreateSubscription • ModifySubscription • DeleteSubscription • SetPublishingMode • SetMonitoringMode • Publish • Republish
View	• Browse • BrowseNext • TranslateBrowsePathToNodeIds • RegisterNodes • UnregisterNodes

NOTA: Per una descrizione di questi servizi e gruppi di servizi, vedere il documento *Specifica OPC Unified Architecture Parte 4: Servizi (Versione 1.04)*.

Servizi di accesso ai dati dello stack del server OPC UA BMENUA0100

Servizi di accesso ai dati supportati

L'accesso ai dati da parte dello stack del server OPC UA integrato del modulo BMENUA0100 è attivato dal supporto dei seguenti facet e servizi correlati:

- Facet server accesso dati
- Facet server tipo complesso 2017
- Facet server Core 2017

NOTA: nelle seguenti descrizioni dei facet, il testo in corsivo indica una citazione diretta del materiale di origine della OPC Foundation. Fare clic sui collegamenti di seguito e utilizzare lo *Strumento di visualizzazione reporting profilo architettura unificata di OPC Foundation* per accedere alla descrizione di ogni facet.

Facet server Core 2017

Come indicato nel sito Web di OPC Foundation, il Facet server Core 2017 "definisce la funzionalità di base richiesta per qualsiasi implementazione del server UA. La funzionalità principale include la possibilità di rilevare endpoint, stabilire canali di comunicazione sicuri, creare sessioni, esplorare lo spazio indirizzi e leggere e/o scrivere negli attributi dei nodi. I requisiti chiave sono: supporto per una singola sessione, supporto per server e oggetto capacità server, tutti gli attributi obbligatori per i nodi nello spazio indirizzi e autenticazione con nome utente e password. Per un'ampia applicabilità, è consigliabile che i server supportino più profili di trasporto e sicurezza."

Per una descrizione completa di questo facet, consultare http://opcfoundation.org/UA-Profile/Server/Core2017Facet.

Lo stack del server OPC UA integrato del modulo BMENUA0100 supporta le seguenti unità di conformità nel Facet server Core 2017:

- Set di servizi View, include i seguenti gruppi e servizi:
  - View Basic: include i servizi Browse e BrowseNext.
  - View TranslateBrowsePath: include il servizio Traduci seleziona percorsi su Id nodo.
  - View Register Nodes: include i servizi Registra nodi e Annulla reg. nodi come modo per ottimizzare l'accesso a nodi di utilizzo frequente nello Spazio indirizzo OPC UA del server.
- Set di servizi Attribute, include i seguenti gruppi e servizi:
  - Attribute read: include il servizio Read, che supporta la lettura di uno o più attributi di uno o più nodi, compreso il supporto del parametro IndexRange per leggere un singolo elemento o intervallo di elementi quando il valore dell'attributo è un array.
  - Attribute Write values: include il servizio Write Value, che supporta la scrittura di uno o più valori in uno o più attributi di uno o più nodi.
  - Attribute Write Index: include il servizio Write Index, che supporta IndexRange per scrivere in un singolo elemento o intervallo di elementi quando il valore dell'attributo è un array e per tale array sono consentiti aggiornamenti parziali.

Facet server accesso dati

Come indicato nel sito Web di OPC Foundation, il Facet server accesso dati "specifica il supporto per un modello informativo utilizzato per fornire dati di automazione industriale. Questo modello definisce le strutture standard per gli elementi dati analogici e digitali e la loro qualità del servizio. Questo Facet estende il Facet server Core che include il supporto del comportamento di base dello spazio indirizzi."

Per una descrizione completa di questo facet, consultare http://opcfoundation.org/UA-Profile/Server/DataAccess.

Facet server tipo complesso 2017

Come indicato nel sito Web di OPC Foundation, il Facet server ComplexType 2017 "estende il Facet server Core per includere variabili con dati strutturati, ossia dati composti da più elementi come una struttura e in cui i singoli elementi sono esposti come variabili componente. Il supporto di questo facet richiede l'implementazione di variabili e tipi di dati strutturati che utilizzano questi tipi di dati. Il set di servizi Lettura, Scrittura e Sottoscrizioni deve supportare la codifica e la decodifica di questi tipi di dati strutturati. Come opzione, il server può anche supportare codifiche alternative, come una codifica XML quando si utilizza il protocollo binario e viceversa."

Per una descrizione completa di questo facet, consultare http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017.

Servizi di sicurezza e rilevamento dello stack del server OPC UA BMENUA0100

Introduzione

Lo stack del server OPC UA integrato del modulo BMENUA0100 supporta i servizi di rilevamento e sicurezza.

Per collegarsi al server OPC UA nel modulo BMENUA0100, un client OPC UA richiede informazioni che descrivono il server, compresi i relativi indirizzo di rete, protocollo e impostazioni di sicurezza. OPC UA definisce un set di funzionalità di rilevamento utilizzabili da un client per ottenere tali dati.

Le informazioni necessarie per stabilire una connessione tra un client OPC UA e un server OPC UA vengono memorizzate in un endpoint. Un server OPC UA può possedere più endpoint, ciascuno contenente:

- URL dell'endpoint (protocollo e indirizzo di rete), ad esempio:
  - Per IPv4: opc.tcp://172.21.2.30:4840, dove:

    - opc.tcp = protocolli

    - 172.21.2.30 = indirizzo IPv4

    - 4840 = numero porta opcua-tcp configurato in Control Expert
  - Per IPv6: opc.tcp://[2a01:cb05:431:f00:200:aff:fe02:a0a]:50000, dove:

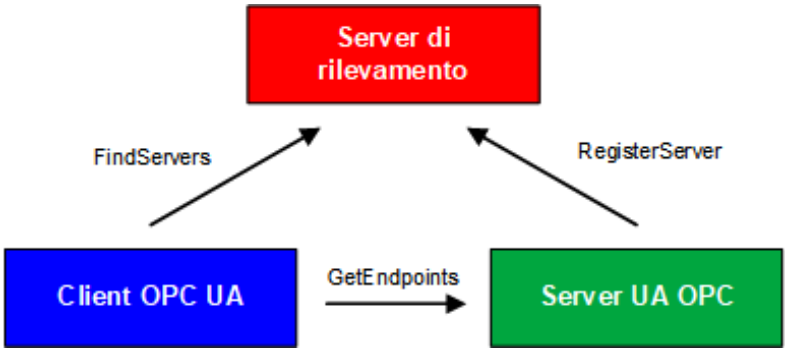
    - opc.tcp = protocolli

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

    - 50000 = numero porta opcua-tcp configurato in Control Expert

- Regolamentazione di sicurezza (comprendente un set di algoritmo di sicurezza e lunghezza chiave)
- Modalità di sicurezza messaggio (livello di sicurezza per i messaggi scambiati)
- Tipo token utente (tipi di autenticazione utente supportati dal server)

Possono esistere uno o più server OPC UA. Nel caso di più server, è possibile utilizzare un server di rilevamento per fornire informazioni relative a ciascun server. I singoli server possono registrarsi con il server di rilevamento. I client possono richiedere un elenco di alcuni dei server disponibili (o tutti) al server di rilevamento e utilizzare il servizio GetEndpoints per acquisire la connessione da un singolo server.



Il modulo BMENUA0100 supporta diversi servizi di rilevamento e sicurezza, tra cui:

- Set servizio Discovery
- Set servizio SecureChannel
- Set servizio Session

La decisione di attivare o disattivare i servizi dipende dal criterio di sicurezza informatica da implementare per il server.

Set servizio Discovery

Lo stack del server OPC UA BMENUA0100 supporta il Set servizio Discovery, incorporato nel Facet server Core 2017, pagina 40. Come implementato nel modulo BMENUA0100, i servizi supportati includono:

- FindServers: come implementato nello stack del server OPC UA del modulo BMENUA0100, questo servizio individua tutti i server solo sul server OPC UA locale.
- GetEndpoints: restituisce gli Endpoint supportati da un server e le informazioni di configurazione richieste per stabilire un SecureChannel e una Session. Può fornire un elenco di restituzione di Endpoint filtrati, basato su profili.

Set servizio SecureChannel

Lo stack del server OPC UA BMENUA0100 supporta il Set servizio SecureChannel, che include i seguenti servizi:

- OpenSecureChannel: apre o rinnova un SecureChannel che fornisce riservatezza e integrità per lo scambio di messaggi durante una sessione. Questo servizio richiede che lo stack del server OPC UA applichi i vari algoritmi di sicurezza ai messaggi inviati e ricevuti.
- CloseSecureChannel: termina un SecureChannel.

Set servizio Session

Lo stack del server OPC UA BMENUA0100 supporta il Set servizio Session, incorporato nel Facet server Core 2017, pagina 40. Come implementato nel modulo BMENUA0100, i servizi supportati includono:

- CreateSession: dopo aver creato un SecureChannel con il servizio OpenSecureChannel , un client utilizza questo servizio per creare una sessione. Il server restituisce due valori che identificano in modo univoco la sessione:
  - Un Id sessione, utilizzato per identificare la sessione nei registri di controllo e nello Spazio indirizzo del server.
  - Un Token di autenticazione, utilizzato per associare una richiesta in entrata a una sessione.
- ActivateSession: utilizzato dal client per specificare l'identità dell'utente associato alla sessione. Non può essere utilizzato per cambiare l'utente della sessione.
- CloseSession: termina una sessione.

  NOTA: per i servizi CreateSession e ActivateSession, se SecurityMode = Nessuna allora:

  1. Il Certificato applicazione e Nonce sono opzionali.
  2. Le firme sono nulle/vuote.

Servizi di sottoscrizione e pubblicazione dello stack del server OPC UA BMENUA0100

Sottoscrizioni

Invece di leggere in permanenza le informazioni tramite interrogazione, il protocollo OPC UA include la funzione Sottoscrizione. Questa funzione consente allo stack OPC UA

integrato nel modulo BMENUA0100 di fornire servizi di pubblicazione/sottoscrizione, utilizzati quando il modulo si collega ai dispositivi remoti.

Un client OPC UA può sottoscriversi a uno o più nodi selezionati e lasciare che il server monitori tali elementi. Quando si verifica un evento di cambiamento, ad esempio un cambiamento di valore, il server notifica il client del cambiamento. Questo meccanismo riduce notevolmente la quantità di dati trasferiti e rappresenta pertanto una riduzione significativa del consumo della larghezza di banda.

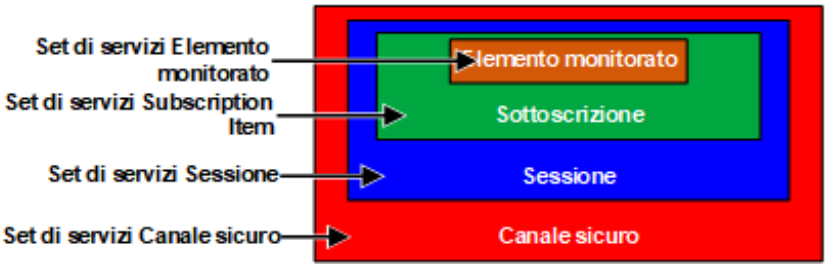
Un client OPC UA può sottoscrivere a più tipi di informazioni fornite da un server OPC UA. La sottoscrizione raggruppa insieme questi vari tipi di dati, denominati Elementi monitorati, per formare una singola raccolta di dati denominati Notifica.

Una sottoscrizione deve:

- Consistere di almeno un Elemento monitorato.
- Essere creata nel contesto di una sessione, creata nel contesto di un canale sicuro.

NOTA: la sottoscrizione può essere trasferita a un'altra sessione.

I set di servizi coinvolti in una sottoscrizione client sono descritti di seguito:



Sottoscrizioni e overrun

In alcuni casi, quando esiste un numero elevato di richieste di sottoscrizione, il server OPC UA tenta di ottenere dati dal controller in una quantità maggiore di quanto il controller o il modulo BMENUA0100 può gestire nell'intervallo di pubblicazione specificato. In questo caso, il tempo di esecuzione delle richieste di sottoscrizione verrà esteso automaticamente e la successiva esecuzione della sottoscrizione posticipata fino al completamento di tutte le richieste.

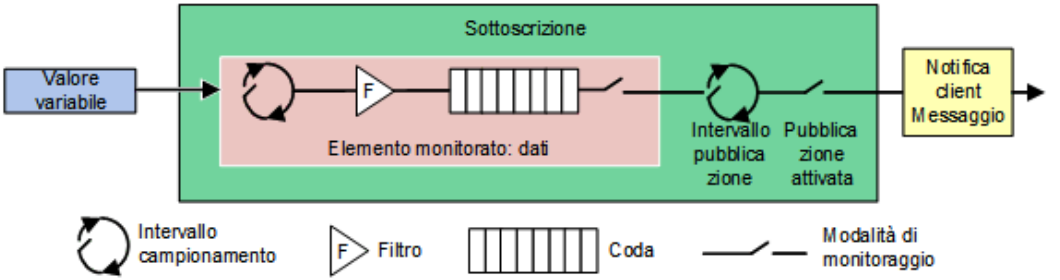
Quando si imposta un intervallo di pubblicazione, considerare il numero di client e richieste client che il server deve gestire. Quando si determina il numero di richieste client, verificare che tutti i client funzionino online. Per questo, tenere presente che per alcuni clienti possono essere necessari 2 minuti o più per essere online dopo l'avvio.

NOTA: Impostare l'intervallo di pubblicazione ad almeno il doppio dell'intervallo di campionamento per evitare modifiche ai dati mancanti.

Eventi di cambiamento

Un client può sottoscriversi a un evento di cambiamento dati, attivato da una modifica dell'attributo valore di una variabile, come un Elemento monitorato.

Le impostazioni configurabili della sottoscrizione, la loro sequenza e i ruoli sono descritti di seguito:



Le tre impostazioni seguenti determinano come gli Elementi monitorati vengono aggiunti a una sottoscrizione:

- Intervallo di campionamento: l'intervallo di tempo di campionamento impostato per ogni Elemento monitorato nella sottoscrizione. Si tratta della frequenza con cui il server verifica la presenza di eventuali cambiamenti nell'origine dati. Per un singolo elemento Variabile, l'Intervallo di campionamento può essere inferiore (ossia più veloce) del periodo tra le notifiche al client. In questo caso, il server OPC UA può accodare i campioni e pubblicare la coda completa. In casi estremi, il server rianalizza (ossia rallenta) l'Intervallo di campionamento in modo che sull'origine dati non si formi un carico di accodamento eccessivo provocato dal campionamento stesso.

  NOTA: Se l'accodamento OPC UA dei campioni di dati è supportato, la dimensione della coda (ossia, il numero massimo di valori che possono essere accodati) può essere configurata per ogni elemento monitorato. Quando vengono consegnati i dati (pubblicati) al client, la coda viene svuotata. In caso di overflow della coda, i dati meno recenti vengono eliminati e sostituiti dai nuovi dati.

- Filtro: una raccolta di diversi criteri utilizzati per identificare quali eventi o modifiche dei dati sono segnalati e quali bloccati.
- Modalità di monitoraggio: utilizzata per attivare o disattivare segnalazione e campionamento dati.

Le due impostazioni seguenti si applicano alla sottoscrizione stessa:

- Intervallo di pubblicazione: il periodo dopo cui le notifiche raccolte nelle code vengono consegnate al client in un messaggio di notifica (Pubblicazione risposta). Il client OPC UA deve confermare che il server OPC UA ha ricevuto sufficienti Token di pubblicazione (Richieste di pubblicazione), in modo che se l'intervallo di pubblicazione scade e una notifica è pronta per l'invio, il server utilizza tale token e invia i dati entro la Risposta di pubblicazione. Nel caso in cui non vi siano eventi da segnalare (ossia nessun valore modificato) il server invia una notifica KeepAlive al client, ossia una Pubblicazione vuota, per indicare che il server è ancora attivo.
- Pubblicazione attivata: attiva e disattiva l'invio del messaggio di notifica.

Facet server sottoscrizione DataChange integrato

Come indicato nel sito Web di OPC Foundation, il facet server sottoscrizione DataChange integrato "specifica il livello minimo di supporto per le notifiche di modifica dei dati all'interno delle sottoscrizioni. Include limiti che riducono al minimo il sovraccarico di memoria ed elaborazione necessario per l'implementazione del facet. Questo facet include la funzionalità per creare, modificare ed eliminare sottoscrizioni e per aggiungere, modificare e rimuovere elementi monitorati. Come minimo per ogni sessione, i server devono supportare una sottoscrizione con un massimo di due elementi. È inoltre necessario il supporto di due richieste di pubblicazione parallele. Questo facet è destinato a una piattaforma come quella fornita dal profilo server del dispositivo integrato Micro in cui la memoria è limitata e deve essere gestita.”

Per una descrizione completa di questo facet, consultare http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription.

Questo facet supporta i servizi seguenti:

- Set di servizi Monitored Item
- Set di servizi Subscription

Set di servizi Monitored Item

Il Set di servizi Monitored Item supporta i servizi seguenti:

NOTA: Per una descrizione di questi servizi e gruppi di servizi, vedere il documento *Specifica OPC Unified Architecture Parte 4: Servizi (Versione 1.04)*.

- CreateMonitoredItems: una chiamata asincrona utilizzata per creare e aggiungere uno o più MonitoredItem a una sottoscrizione.
- ModifyMonitoredItems: una chiamata asincrona per modificare gli elementi monitorati. Questo servizio consente di modificare gli elementi monitorati di una sottoscrizione. Le modifiche alle impostazioni MonitoredItem vengono applicate immediatamente dal server .

- DeleteMonitoredItems: una chiamata asincrona per eliminare gli elementi monitorati. Questo servizio consente di rimuovere uno o più elementi monitorati di una sottoscrizione. Quando si elimina un MonitoredItem , anche i relativi collegamenti all'elemento attivato vengono eliminati.
- SetMonitoringMode: una chiamata asincrona per impostare la modalità di monitoraggio per un elenco di elementi monitorati. Questo servizio consente di impostare la modalità di monitoraggio per uno o più elementi monitorati di una sottoscrizione. L'impostazione della modalità su DISATTIVA provoca l'eliminazione di tutte le notifiche accodate.

Set di servizi Subscription

Il Set di servizi Subscription supporta i servizi seguenti:

NOTA: Per una descrizione di questi servizi e gruppi di servizi, vedere il documento *Specifica OPC Unified Architecture Parte 4: Servizi (Versione 1.04)*.

- CreateSubscription: una chiamata asincrona per creare una sottoscrizione.
- ModifySubscription: una chiamata asincrona per modificare una sottoscrizione. Il server applica immediatamente le modifiche alla sottoscrizione.
- DeleteSubscription: una chiamata asincrona per eliminare una o più sottoscrizioni appartenenti alla sessione client. Il corretto completamento di questo servizio elimina tutti gli elementi monitorati associati alla sottoscrizione.
- Publish: questo servizio ha due scopi: riconoscere il ricevimento di messaggi di notifica per una o più sottoscrizioni e richiedere al server di restituire un messaggio di notifica o un messaggio keep-alive.
- Republish: una chiamata asincrona di ripubblicazione per ottenere le notifiche perse. Questo servizio richiede alla sottoscrizione di ripubblicare un messaggio di notifica dalla coda di ritrasmissione. Il server, se non ha il messaggio richiesto nella propria coda di ritrasmissione, restituisce una risposta di errore.
- SetPublishingMode: una chiamata asincrona per attivare l'invio di notifiche su una o più sottoscrizioni.

Servizi di trasporto dello stack del server OPC UA BMENUA0100

Supporto del Facet UA-TCP UA-SC UA-Binario

Il modulo BMENUA0100 supporta il facet di trasporto UA-TCP UA-SC UA-Binario. (Per ulteriori informazioni, consultare la documentazione in linea su http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary.)

Questo facet di trasporto definisce una combinazione di protocolli di rete, protocolli di sicurezza e codifica messaggi ottimizzati per alte prestazioni e basso consumo di risorse. Combina il semplice protocollo di rete -UA-TCP 1.0 basato su TCP con il protocollo di sicurezza binario UA-SecureConversation 1.0 e la codifica messaggi binaria UA-Binary 1.0.

I dati che passano tra un client OPC UA e il server OPC UA integrato del modulo BMENUA0100 utilizzano il protocollo TCP e la codifica binaria in conformità al formato di file binario OPC UA.

NOTA: Il formato di file binario OPC UA sostituisce lo schema XML UA-Nodeset della OPC Foundation. Migliora le prestazioni e il consumo di memoria. Non richiede un analizzatore XML.

Rilevamento variabili controller

Mappatura delle variabili del controller di Control Expert alle variabili logiche dei dati OPC UA

Introduzione

Il server OPC UA integrato nel modulo BMENUA0100 utilizza le richieste del dizionario dati Unified Messaging Application Services (UMAS) per cercare e rilevare le variabili dell'applicazione controller M580. È necessario attivare il dizionario dati nelle impostazioni di progetto di Control Expert.

NOTA:

- Il modulo BMENUA0100 può supportare una dimensione massima del dizionario dati di 100000 variabili.
- Il tempo richiesto per caricare il dizionario dati nel server OPC UA dipende dal numero di elementi del dizionario dati e dall'impostazione del periodo MAST, pagina 166.

Le variabili raccolte sono tradotte dalla vista modello logico dei dati di Control Expert nella vista modello logico dei dati OPC UA tramite i servizi appropriati dello stack OPC UA. Un client OPC UA collegato al modulo BMENUA0100 sulla porta di controllo o sulla porta backplane tramite il controller o un modulo di comunicazione BMENOC0301 o BMENOC0311 può recuperare questa raccolta di dati tramite i servizi del Facet server accesso dati, pagina 40 supportato dal Profilo server UA 2017 integrato, pagina 37.

Precaricamento del dizionario dati per evitare interruzioni della comunicazione

Una modifica dell'applicazione online effettuata con Control Expert interrompe temporaneamente la comunicazione server/client OPC UA mentre il server acquisisce un dizionario dati aggiornato. Questa interruzione è provocata dalla mappatura dei dati non coerenti del controller mentre si aggiorna il dizionario dati. Durante il periodo di interruzione della comunicazione, lo stato dei nodi monitorati, come indicato da UA Expert, è in errore (**bad communication error** o **bad no communication** o **bad timeout**). Per evitare l'interruzione delle comunicazioni e le conseguenze che ne derivano, è possibile definire un meccanismo di sincronizzazione tra il modulo BMENUA0100 e il software di configurazioneControl Expert, basato su un precaricamento del dizionario dati aggiornato.

Questa funzionalità è abilitata in Control Expert nella finestra **Strumenti > Impostazioni progetto...** nell'area **Generale > Dati integrati PLC** utilizzando le impostazioni (vedere EcoStruxure™ Control Expert, Modalità operative) **Precarica su Crea modifiche** e **Timeout modifiche creazione effettivo** . Per informazioni su come configurare questa funzionalità, consultare la guida in linea di Control Expert.

Attivazione del dizionario dati

Per attivare il dizionario dati in Control Expert:

Passo	Azione
1	In Control Expert, con il progetto aperto, selezionare **Strumenti > Impostazioni progetto**.
2	Nella finestra **Impostazioni progetto**, selezionare **Generale > Dati integrati PLC**, quindi **Dizionario dati**. **NOTA:** Se il progetto EcoStruxure™ Control Expert include un modulo BMENUA0100 e questa impostazione non è selezionata, viene generato un errore durante la compilazione dell'applicazione.

Conversione del tipo di dati variabile

Il modulo BMENUA0100 può rilevare e convertire nei tipi di dati OPC UA i seguenti tipi di variabile di base supportati dal modello logico dei dati di Control Expert:

Tipo di dati elementari di Control Expert	Tipo di dati OPC UA
BOOL	Booleano
EBOOL	Booleano
INT	Int16
DINT	Int32

Tipo di dati elementari di Control Expert	Tipo di dati OPC UA
UINT	UInt16
UDINT	UInt32
REAL	Float
BYTE	Byte
WORD	UInt16
DWORD	UInt32
DATE*	UInt32
TIME*	UInt32
TOD*	UInt32
DT*	Double
STRING	ByteString
* Vedere la tabella seguente per una descrizione della conversione del tipo di dati relativo alla data.	

Per i dati di tipo DATE, TIME, TOD, DT di Control Expert, i tipi di dati OPC UA corrispondenti sono i seguenti:

Tipo di dati elementari di Control Expert	Valore di esempio visualizzato in Control Expert	Tipo di dati OPC UA	Valore corrispondente nel tipo OPC UA
DATE	D#2017-05-17	UInt32	20170517 hex
TIME	T#07h44m01s100ms	UInt32	27841100
TOD	TOD#07:44:01	UInt32	07440100 hex
DT[1]	DT#2017-05-17-07:44:01	Double	4.29E-154
1. I dati restituiti per i valori di Data e ora sono UATypeUInt64, che è la codifica interna di IEC 1131 DT in Control Expert - codifica BCD (Binary Coded Decimal).			

Variabili rilevabili

Per le variabili, il client OPC UA non accede direttamente a una variabile logica rilevata dei dati del controller. Il client accede invece alla variabile rilevata del controller tramite una variabile logica dati OPC UA, esistente nel modulo BMENUA0100 e assegnata alla variabile del controller sottostante. A causa della natura passante dell'accesso alla variabile dati, il processo di richiesta di acquisizione non è ottimizzato e le prestazioni di acquisizione del dizionario dati non sono rappresentative delle prestazioni del controller.

NOTA: i riferimenti, del tipo REF_TO, alle variabili dell'applicazione nel server OPC UA non sono accessibili dal client OPC UA.

Esempi delle variabili del controller di Control Expert rilevabili dal server OPC UA nel modulo BMENUA0100 includono:

- Variabili strutturate con sottocampi: DDT e variabili array.
- le variabili dell'Unità programma sono rilevabili come indicato di seguito:
  - le variabili di I/O sono accessibili dal client OPC UA solo per il tipo BOOL;
  - le variabili di ingresso e le variabili di uscita sono accessibili dal client OPC UA, tranne per i tipi REF_TO, ARRAY, Stringa e Struttura.

Inoltre, le variabili seguenti sono rilevabili dal server OPC UA assegnandole alle variabili dell'applicazione, quindi rilevando le variabili dell'applicazione assegnate:

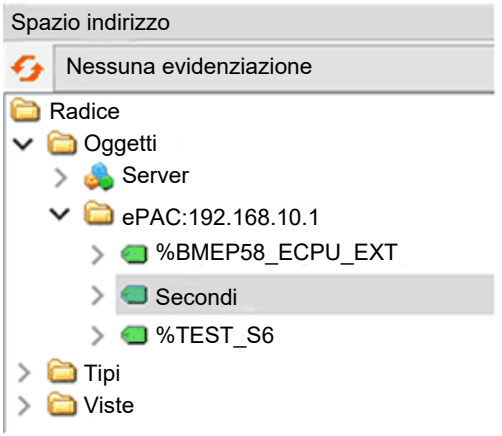
- variabili di I/O topologiche:
  - Ingressi: %I, %IW, %ID, %IF.
  - Uscite: %Q, %QW, %QD, %QF.
- Variabili identificate: %M, %MW, %MD, %MF.
- Variabili di sistema: %S, %SW, %SD.

NOTA: il rilevamento delle variabili comprende una variabile (o simbolo) per un bit estratto (ad esempio, MyBoolVar ubicato in %MW100.1).

Presentazione delle variabili rilevate nel client OPC UA

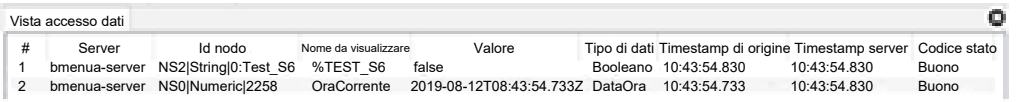
Il server OPC UA nel modulo BMENUA0100 può organizzare e visualizzare graficamente le variabili rilevate del controller. Uno strumento del client OPC UA può collegarsi al modulo BMENUA0100 e visualizzare una presentazione della struttura del nodo di variabili del server OPC UA.

Nell'esempio seguente, un client OPC UA (in questo esempio, lo strumento client Unified Automation UaExpert) collegato al modulo BMENUA0100 può visualizzare le variabili del controller neile relative finestre **Spazio indirizzo**. L'indirizzo IP del controller M580 è rappresentato dal nodo ePAC:192.168.10.1. I nodi secondari rappresentano le variabili dell'applicazione Control Expert:



Nell'esempio precedente, il primo sottonodo, BMEP58_ECPU_EXT, rappresenta il DDT dispositivo per il controller M580, istanziato automaticamente quando il controller è stato aggiunto all'applicazione Control Expert. I nodi successivi rappresentano altri oggetti aggiunti all'applicazione.

Mediante lo strumento client OPC UA, il nodo TEST_S6 è stato selezionato e trascinato nella finestra **Vista accesso dati**, dove vengono visualizzati i dettagli della variabile:


Vista accesso dati

#	Server	Id nodo	Nome da visualizzare	Valore	Tipo di dati	Timestamp di origine	Timestamp server	Codice stato
1	bmenua-server	NS2|String|0:Test_S6	%TEST_S6	false	Booleano	10:43:54.830	10:43:54.830	Buono
2	bmenua-server	NS0|Numeric|2258	OraCorrente	2019-08-12T08:43:54.733Z	DataOra	10:43:54.733	10:43:54.830	Buono

In questo caso, il tipo dati OPC UA della variabile è *Booleano* (per indicare che il tipo dati del controller sottostante è BOOL) e il suo valore è *false*.

> **NOTA:** l'attributo **Timestamp server** attributo dei nodi OPC UA viene ricevuto dal Server OPC UA BMENUA0100 in UTC (Universal Time Coordinated) e viene visualizzato nell'ora locale.

Lettura e scrittura di variabili rilevate nel client OPC UA

Un tag OPC UA in un client OPC UA (ad esempio uno SCADA) che fa riferimento a una variabile di array consente al client di leggere o scrivere tutti gli elementi dell'array. Ad esempio, il tag 'MyArray' dichiarato come ARRAY[0...31] OF INT.

Tuttavia, affinché il client possa leggere o scrivere solo un singolo elemento di un array, è necessario dichiarare un tag specifico che faccia riferimento al singolo elemento dell'array di destinazione. Ad esempio, 'MyInt' dichiarato come INT con riferimento a MyArray[2].

Hot Standby e ridondanza

Ridondanza del server OPC UA

Due tipi di ridondanza

Il modulo BMENUA0100 supporta i seguenti tipi di ridondanza:

- Architettura Hot Standby, che descrive i controller ridondanti.
- Ridondanza del server OPC UA, che descrive l'uso di moduli BMENUA0100 ridondanti.

La ridondanza dei server OPC UA, gestita dai moduli BMENUA0100, segue lo standard OPC UA "ridondanza del server non trasparente in modalità Warm failover" definito da OPC Foundation.

Questi due tipi di ridondanza possono essere combinati. Sono supportati i seguenti design:

- Un controller standalone, contenente due moduli BMENUA0100.
- Due controller Hot Standby, ciascuno contenente uno o due moduli BMENUA0100.

Ridondanza OPC UA

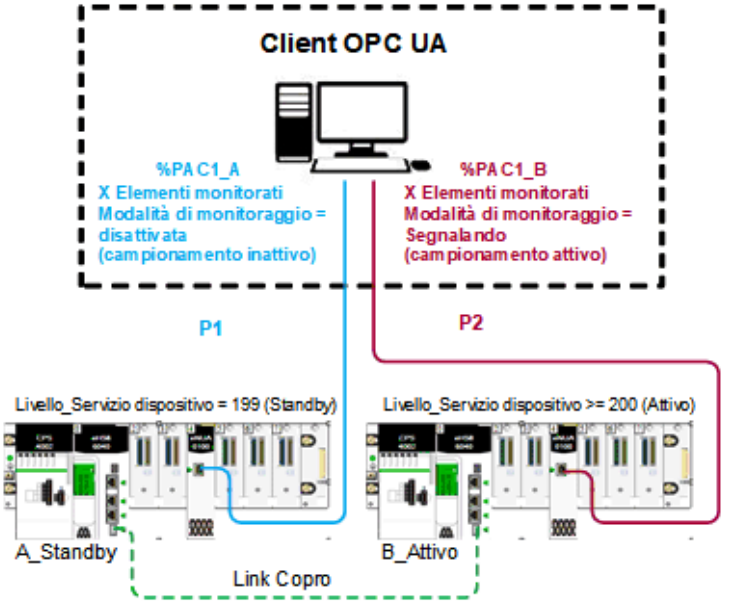
In un'architettura ridondante del server non trasparente OPC UA in modalità Warm failover, il client OPC UA stabilisce sessioni e gestisce le comunicazioni con server ridondanti. Le sessioni da stabilire includono: una sessione attiva con il server primario e una sessione inattiva con il server secondario (o di standby). Il client deve essere configurato per queste due sessioni per includere gli stessi elementi monitorati.

Il client OPC UA verifica lo stato dei due server tramite la variabile SERVICE_LEVEL e commuta la comunicazione con il server più sicuro, in base al valore di questa variabile.

Lo standard OPC UA sostiene che l'attivazione delle comunicazioni viene eseguita regolando la *Modalità di monitoraggio* delle varie sessioni al valore corretto. La *Modalità di monitoraggio* dei server è controllata dal client OPC UA e la procedura per regolarla dipende dall'implementazione del client. Per ulteriori informazioni sulla regolazione della *Modalità di monitoraggio*, vedere la documentazione del client OPC UA.

Questo è un principio generale e si applica a qualsiasi architettura, compresa un'architettura Hot Standby.

Lo schema seguente rappresenta un client OPC UA collegato a una coppia di server OPC UA ridondanti (ciascuno integrato in un modulo BMENUA0100). Il client ha designato come server attivo quello con il valore SERVICE_LEVEL più alto:



Hot Standby

In una configurazione Hot Standby, è possibile installare un massimo di due moduli BMENUA0100 in ogni rack locale principale Hot Standby. Ciascun modulo BMENUA0100 è configurato con un indirizzo IP univoco e statico. I moduli BMENUA0100 mantengono i rispettivi indirizzi IP e non li scambiano in caso di switchover o scambio Hot Standby.

NOTA: in un sistema Hot Standby, verificare che i moduli BMENUA0100 nei controller primario e di standby:

- siano configurati con identiche impostazioni di sicurezza informatica, pagina 86 e
- abbiano i relativi selettori a rotazione, pagina 23 (posti sul retro del modulo) impostati nella stessa posizione;
- siano installati nello stesso numero di slot, pagina 62 nei rispettivi rack principali locali.

Se queste condizioni non esistono, il modulo non può recuperare la configurazione impostata da Control Expert e memorizzata nel controller e si avvia in modalità standalone. Il sistema non esegue automaticamente questa verifica.

Il DDT del modulo BMENUA0100 include la variabile SERVICE_LEVEL, pagina 150, che fornisce informazioni al controller relative allo stato del server OPC UA nel modulo BMENUA0100. Il client OPC UA è informato dello stato del server OPC UA tramite la variabile SERVICE_LEVEL, disponibile come variabile OPC UA.

NOTA: includere la funzione elementare READ_DDT, allo scopo di aggiornare il DDT di ogni modulo BMENUA0100. In una configurazione Hot Standby, aggiungere READ_DDT a una sezione di codice eseguita quando il controller è in modalità standby. Questo design restituisce informazioni diagnostiche del BMENUA0100 che possono essere scambiate tra i controller primario e di standby. L'applicazione può utilizzare tali informazioni per eseguire una verifica di coerenza dei servizi supportati e delle configurazioni di sicurezza informatica per i moduli BMENUA0100 nei controller primario e di standby.

Se il controller Hot Standby T_M_ECPU_HSBY DDT (vedere Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente) e il relativo elemento CMD_SWAP sono resi disponibili come variabili HMI in un sistema SCADA, l'applicazione SCADA può attivare uno scambio scrivendo nella variabile OPC UA assegnata appropriata nel BMENUA0100.

In un sistema Hot Standby, il modulo BMENUA0100 che gestisce le comunicazioni OPC UA con SCADA può essere quello ubicato nel rack locale di standby. Per questo motivo, è necessario selezionare l'attributo **Scambio in STBY** per tutte le variabili dell'applicazione acquisite per fornire coerenza dei valori delle variabili tra i controller primario e di standby.

Inoltre, per mantenere la coerenza, le applicazioni nei due controller Hot Standby devono essere sincronizzate.

In rari casi (principalmente quando il bit ECPU_HSBY_1.PLCX_ONLINE è impostato su FALSE manualmente o da programma), uno dei controller in un sistema Hot Standby può essere in modalità di attesa. In tale modalità, questo controller (quello di standby) non è sincronizzato con il controller primario e le variabili lette da tale controller non sono precise. Lo stato di un controller in grado di rispondere può essere monitorato tramite i seguenti campi T_M_ECPU_HSBY DDT:

- 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

Inoltre, il sistema Hot Standby consente ai due controller di funzionare mentre eseguono applicazioni diverse. Per garantire la coerenza delle variabili tra i controller primario e di standby, il layout dei dati dei 2 controller deve essere coerente, come mostrato dal campo DDT T_M_ECPU_HSBY:

- T_M_ECPU_HSBY_1.DATA_LAYOUT_MISMATCH = FALSE

  NOTA: quando è configurata la ridondanza OPC UA, verificare da programma i DDT del modulo per confermare che i servizi supportati e le configurazioni di sicurezza informatica per i moduli BMENUA0100 siano coerenti.

Supporto OPC UA per server, client e reti ridondanti

Specifica OPC Unified Architecture Parte 4: Servizi, Versione 1.04, “OPC UA consente la ridondanza di server, client e reti. OPC UA fornisce le strutture dati e i servizi tramite i quali è possibile ottenere la ridondanza in modo standardizzato."

"La ridondanza del server consente ai client di disporre di più origini da cui ottenere gli stessi dati. La ridondanza dei server può essere ottenuta in diversi modi, alcuni dei quali richiedono l'interazione del client, altri non richiedono l'interazione di un client. I server ridondanti potrebbero esistere in sistemi senza reti o client ridondanti. I server ridondanti potrebbero inoltre coesistere nei sistemi con ridondanza di rete e client..."

“La ridondanza dei client consente ai client configurati in modo identico di comportarsi come se fossero singoli client, ma non tutti i client ottengono dati in un determinato momento. Idealmente non si dovrebbe verificare alcuna perdita di informazioni quando si verifica un failover del client. I client ridondanti potrebbero esistere in sistemi senza reti o server ridondanti. I client ridondanti potrebbero inoltre coesistere in sistemi con ridondanza di rete e server..."

"La ridondanza di rete consente a client e server di disporre di più percorsi di comunicazione per ottenere gli stessi dati. Nei sistemi senza server o client ridondanti potrebbero esistere reti ridondanti. Le reti ridondanti potrebbero inoltre coesistere in sistemi con ridondanza di client e server... OPC UA Parte 4, sezione 6.6.1."

Ridondanza dei server

Specifica OPC Unified Architecture Parte 4: Servizi, Versione 1.04, "Vi sono due modalità generiche di ridondanza dei server, trasparente e non trasparente."

“Nella ridondanza trasparente, il failover delle responsabilità del server da un server all'altro è trasparente per il client. Il client non è a conoscenza del fatto che si è verificato un failover e non ha alcun controllo sul comportamento di failover. Inoltre, il client non deve eseguire alcuna azione per continuare a inviare o ricevere dati.”

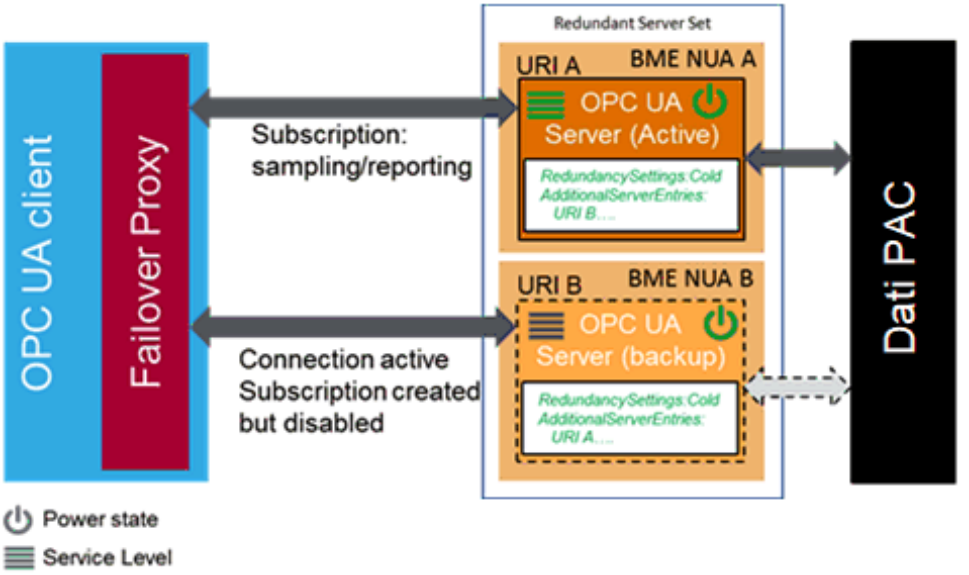
“Nella ridondanza non trasparente il failover da un server a un altro e le azioni per continuare a inviare o ricevere i dati vengono eseguite dal client. Il client deve essere a conoscenza del set di server ridondanti e deve eseguire le azioni richieste per usufruire della ridondanza del server.”

“L'oggetto ServerRedundancy ... indica la modalità supportata dal server. Il tipo di oggetto ServerRedundancyType e i relativi sottotipi TransparentRedundancyType e NonTransparentRedundancyType ... specificano le informazioni per la modalità di ridondanza supportata. OPC UA Parte 4, sezione 6.6.2"

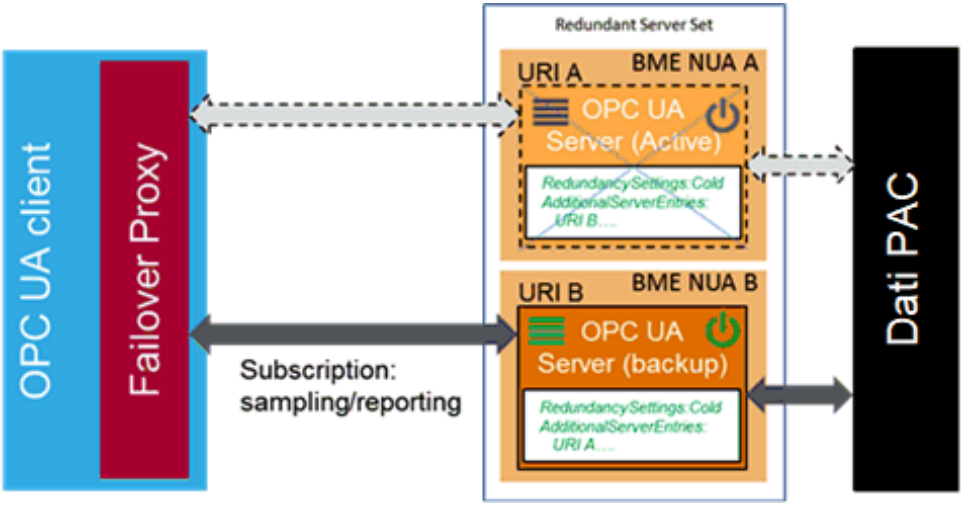
Come notato sopra, il server OPC UA nel BMENUA0100 supporta la ridondanza non trasparente del server in modalità Warm failover.

Modalità Warm failover del server OPC UA

Specifica OPC Unified Architecture Parte 4: Servizi, Versione 1.04, La modalità Warm failover si verifica quando i(l) server di backup può essere attivo ma non può collegarsi ai punti dati effettivi.” Perciò, solo un singolo server sarà in grado di consumare i dati dell'applicazione Control Expert. "La variabile ServiceLevel ... indica la capacità del server di fornire i propri dati al client." OPC UA Parte 4, sezione 6.6.2.4.4



Quando si verifica un failover, è necessario l'intervento del client OPC UA; il server OPC UA integrato in BMENUA0100 diventa inattivo:



Comportamento con failover del client

Specifica OPC Unified Architecture Parte 4: Servizi, Versione 1.04, "Ogni server mantiene un elenco di Uri server per tutti i server ridondanti nel Set di server ridondanti."

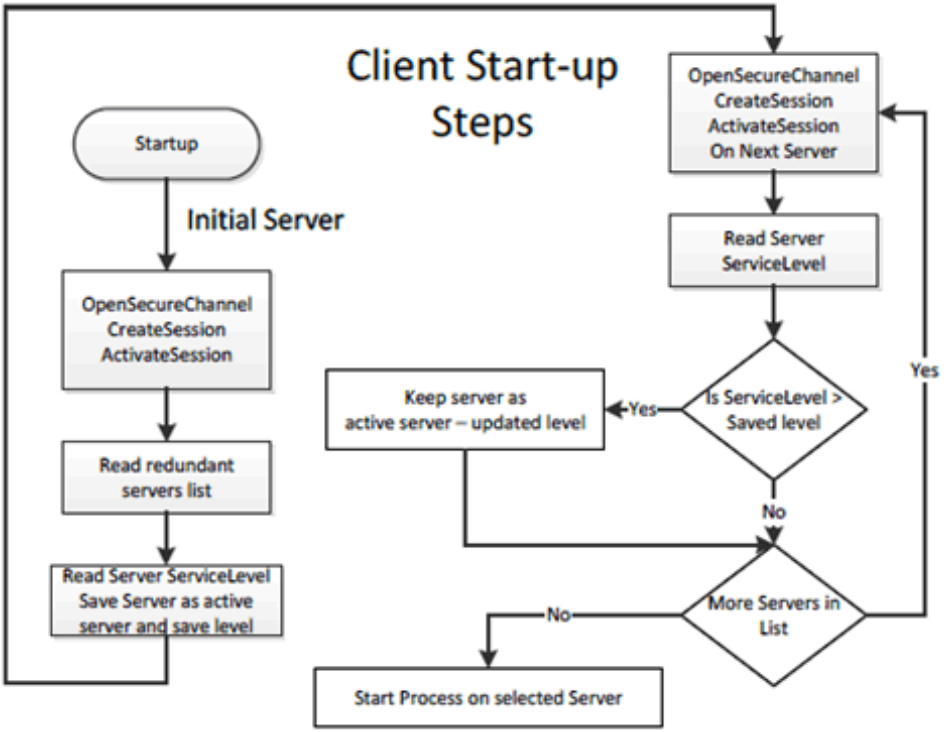
NOTA: un Set di server ridondanti è la raccolta di server OPC UA nell'applicazione Control Expert configurati per garantire la ridondanza.

“L'elenco viene fornito insieme alla modalità di failover nell'oggetto ServerRedundancy. Per consentire ai client di connettersi a tutti i server dell'elenco, ogni server dell'elenco deve fornire ApplicationDescription per tutti i server del set di server ridondanti tramite il servizio FindServers. Queste informazioni sono necessarie al client per convertire l'Uri server in informazioni necessarie per la connessione agli altri server nel Set di server ridondanti. Pertanto, un client deve connettersi solo a uno dei server ridondanti per trovare gli altri server in base alle informazioni fornite. Un client deve conservare le informazioni sugli altri server nel set di server ridondanti. OPC UA Parte 4, sezione 6.6.2.4.5.1"

Le opzioni per il client nella modalità Warm failover comprendono:

- Alla connessione iniziale, oltre alle azioni sul server attivo:
  - Connessione a più server OPC UA.
  - Creazione di sottoscrizioni e aggiunta di elementi monitorati.
- Al failover:
  - Attivazione di campionamento sulle sottoscrizioni.
  - Attivazione pubblicazione.

“I client che comunicano con un set di server ridondanti non trasparenti richiedono una logica aggiuntiva per poter gestire i guasti del server e il failover su un altro server nel set di server ridondanti. La figura seguente fornisce una panoramica dei passaggi che un client esegue in genere quando si collega per la prima volta a un Set di server ridondanti.”



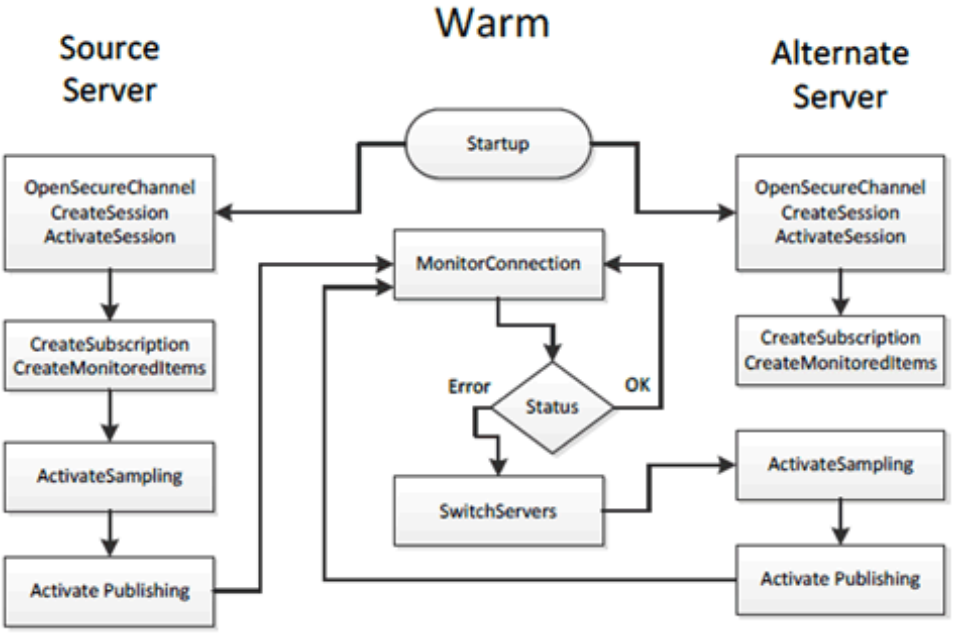
“Il server iniziale può essere ottenuto tramite rilevamento standard o da un elenco persistente di server nel Set di server ridondanti. In ogni caso, tuttavia, il client deve controllare a quale server nel set di server deve collegarsi. Le singole azioni dipendono dalla modalità di failover del server fornita dal server e dalla modalità di failover utilizzata dal client.”

“I client una volta connessi a un server ridondante devono essere consapevoli delle modalità di failover supportate da un server poiché questo supporto influisce sulle opzioni disponibili relative al comportamento del client. Un client può sempre trattare un server utilizzando una modalità di failover inferiore, ovvero per un server che fornisce ridondanza a caldo, un client può collegarsi e scegliere di trattarlo come se il server fosse in esecuzione in ridondanza a caldo o ridondanza a freddo. Questa scelta dipende dal client. In caso di modalità di failover HotAndMirrored, il client non deve utilizzare la modalità di failover a caldo o a freddo, in quanto genererebbe un carico non necessario sui server. OPC UA Parte 4, sezione 6.6.2.4.5.1"

Modalità Warm failover del client OPC UA

Specifica OPC Unified Architecture Parte 4: Servizi, Versione 1.04, In modalità Warm Failover, il client deve connettersi a uno o più server nel set di server ridondanti principalmente per monitorare il livello di servizio. Un client può connettersi e creare sottoscrizioni ed elementi monitorati (MonitoredItems) su più server, ma il campionamento e la pubblicazione possono essere attivi solo su un server. Tuttavia, il server attivo restituirà i dati effettivi, mentre gli altri server nel set di server ridondanti restituiranno un errore appropriato per gli elementi monitorati nella risposta di pubblicazione, ad esempio Bad_ NoCommunication. È possibile trovare un server attivo leggendo la variabile ServiceLevel da tutti i server."

"Il server con il livello di servizio più elevato è il server attivo. Per il failover, il client attiva il campionamento e la pubblicazione sul server con il livello di servizio più elevato. La Figura 30 illustra la procedura eseguita da un client per comunicare con un server utilizzando la modalità Warm Failover."



OPC UA Parte 4, sezione 6.6.2.4.5.3

Architetture supportate

Introduzione

Questo capitolo descrive le architetture topologiche supportate dal modulo di comunicazione Ethernet BMENUA0100 con server OPC UA integrato.

Configurazioni supportate del modulo BMENUA0100

Posizionamento del modulo BMENUA0100

Il modulo BMENUA0100 può essere posizionato in uno slot Ethernet sul rack principale locale (ossia nello stesso rack del controller) nelle configurazioni seguenti:

- una configurazione M580 standalone.
- una configurazione del controller di sicurezza M580 standalone.
- una configurazione M580 Hot Standby.
- una configurazione del controller di sicurezza M580 Hot Standby.

NOTA:

- Il modulo BMENUA0100 può essere utilizzato con tutti i controller M580.
- Nel caso in cui si venisse a creare un loop di rete, il modulo BMENUA0100 passa allo stato NOCONF (Non configurato). Per evitare loop ed eventi correlati, quando si utilizza la porta di controllo BMENUA0100, dividere fisicamente la rete della porta di controllo e la rete del backplane del controller (tramite suddivisione del cablaggio) e non solo logicamente (tramite le impostazioni di sottorete e subnet mask).

Connessione tramite il protocollo HTTPS

Se l'applicazione rileva problemi di connessione, rivolgersi al supporto IT locale per confermare che la configurazione di rete e i criteri di sicurezza siano coerenti con l'accesso HTTPS (porta 443) all'indirizzo IP del modulo BMENUA0100.

Il modulo BMENUA0100 accetta le connessioni HTTPS con protocollo TLS (transport layer security) v1.2 o successivo. Ad esempio, Windows 7 potrebbe richiedere un aggiornamento

per attivare TLS 1.2 per aggiornare il firmware del BMENUA0100 o accedere al proprio sito Web.

Installazione del modulo BMENUA0100 in una rete piana

Per più rack M580 collegati a una singola sottorete (ad esempio un'architettura di rete piana) che includono moduli BMENUA0100 con la porta di controllo disattivata, installare ciascun modulo BMENUA0100 in un diverso numero di slot nel rispettivo rack (tranne che per le configurazioni Hot Standby, dove i moduli BMENUA0100 sono installati nello stesso numero di slot). In alternativa, utilizzare un router per isolare i rack ed evitare potenziali conflitti di indirizzo con i moduli BMENUA0100.

Aggiunta di prefissi ai nomi dei dispositivi (ruolo) nelle progettazioni di reti piane

Se un'architettura comprende più moduli BMENUA0100 che comunicano con altri dispositivi, come i controller M580 configurati sulla stessa sottorete, utilizzare i prefissi per il nome dispositivo (o ruolo) dei dispositivi, compresi i controller M580. Questa convenzione di denominazione consente ai moduli BMENUA0100 di differenziare tra i controller M580 e determinare quale controller è posizionato su quale rack. Questa convenzione di denominazione contribuisce ad eliminare l'incertezza relativa a un progetto di rete piatta. Ad esempio, senza prefissi univoci, un modulo BMENUA0100 non può determinare con quale controller M580 deve comunicare per recuperare la propria configurazione dopo il download di un'applicazione.

Il prefisso del nome dispositivo può essere impostato in Control Expert nella scheda **Strumenti > Impostazioni progetto > Configurazione**.

Accesso al server OPC UA BMENUA0100 integrato

Nelle architetture topologiche descritte in questo capitolo, la porta backplane Ethernet del modulo di comunicazione BMENUA0100 e la porta di controllo possono essere utilizzate per fornire accesso al server OPC UA integrato nel modulo . Per una descrizione di quando queste porte possono essere utilizzate per accedere al server OPC UA integrato, consultare le descrizioni della porta di controllo e della porta backplane Ethernet nell'argomento Porte esterne, pagina 21.

Numero massimo di moduli BMENUA0100 per configurazione

Il numero massimo di moduli BMENUA0100 supportati in una configurazione M580 è:

Tipo di configurazione M580	**N. max di moduli BMENUA0100**
Autonomo	Due nel rack principale locale per le configurazioni standalone[1] e Hot Standby[1,2] standard e di sicurezza.
Controller di sicurezza	
Hot Standby	
Controller di sicurezza Hot Standby	

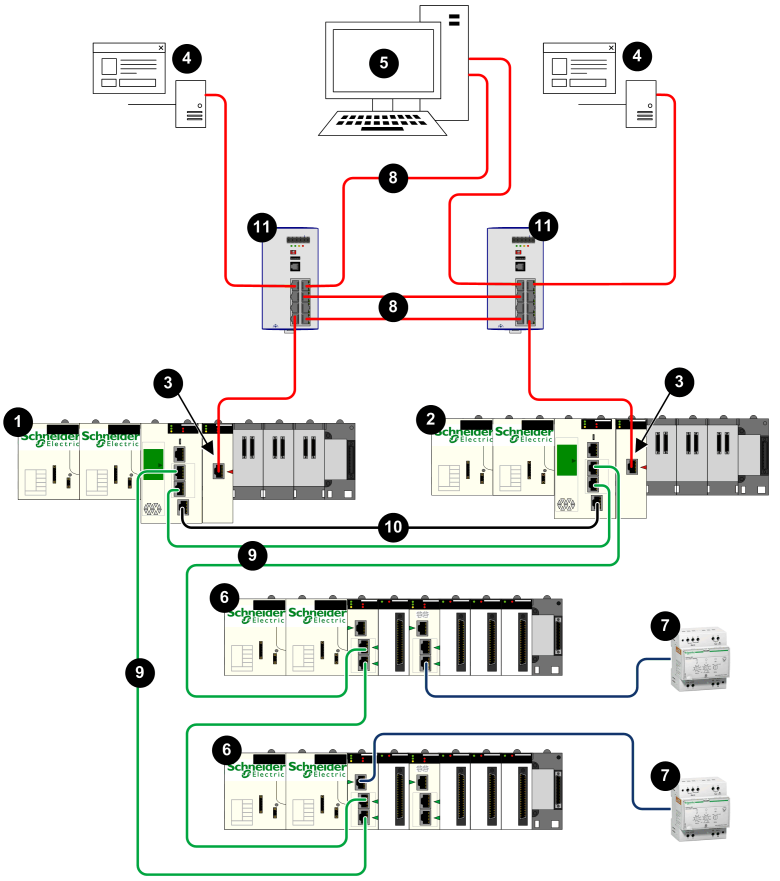
1. Quando si utilizzano due moduli BMENUA0100 in un rack principale:
   - Le prestazioni di ciascun modulo risulteranno inferiori rispetto all'uso di un solo modulo.
   - Attivare la porta di controllo nella configurazione per entrambi i moduli.
2. Nelle configurazioni Hot Standby, posizionare i moduli BMENUA0100 nello stesso numero di slot nei rispettivi rack principali locali.

Modifica della configurazione al volo (CCOTF)

Il modulo BMENUA0100 non supporta CCOTF.

Rete di controllo isolata con controller M580 Hot Standby

Architettura



1 Controller Hot Standby primario

2 Controller Hot Standby di standby

3 Moduli di comunicazione Ethernet BMENUA0100 con server OPC UA integrato

4 Client OPC UA (sistema SCADA)

5 Workstation tecnica con doppia connessione Ethernet

6 Derivazione RIO Ethernet X80

7 Apparecchiatura distribuita

8 Rete di controllo

9 Anello principale Ethernet RIO

10 Collegamento di comunicazione Hot Standby

11 Switch a doppio anello (DRS)

Descrizione

Questa architettura fornisce connessioni ridondanti a doppi client OPC UA (sistemi SCADA). In questa architettura, la sicurezza informatica può essere attivata o disattivata. La rete di controllo (8) è isolata logicamente dai dispositivi Ethernet che risiedono nell'anello principale RIO Ethernet (9), compreso il controller e i dispositivi Ethernet distribuiti (7), grazie al livello di Rete del modello OSI tramite indirizzamento IP.

La porta di controllo BMENUA0100 (3), con i due stack IPv6/IPv4, consente la connettività a monte alla rete di controllo. Quando si comunica tramite IPv6, supporta configurazione automatica dell'indirizzo stateless (SLAAC) e indirizzamento IP statico.

Il modulo BMENUA0100 fornisce comunicazione Modbus peer-to-peer tra i due controller Hot Standby. Le porte del controller forniscono connettività a valle ai dispositivi Ethernet sull'anello principale RIO Ethernet.

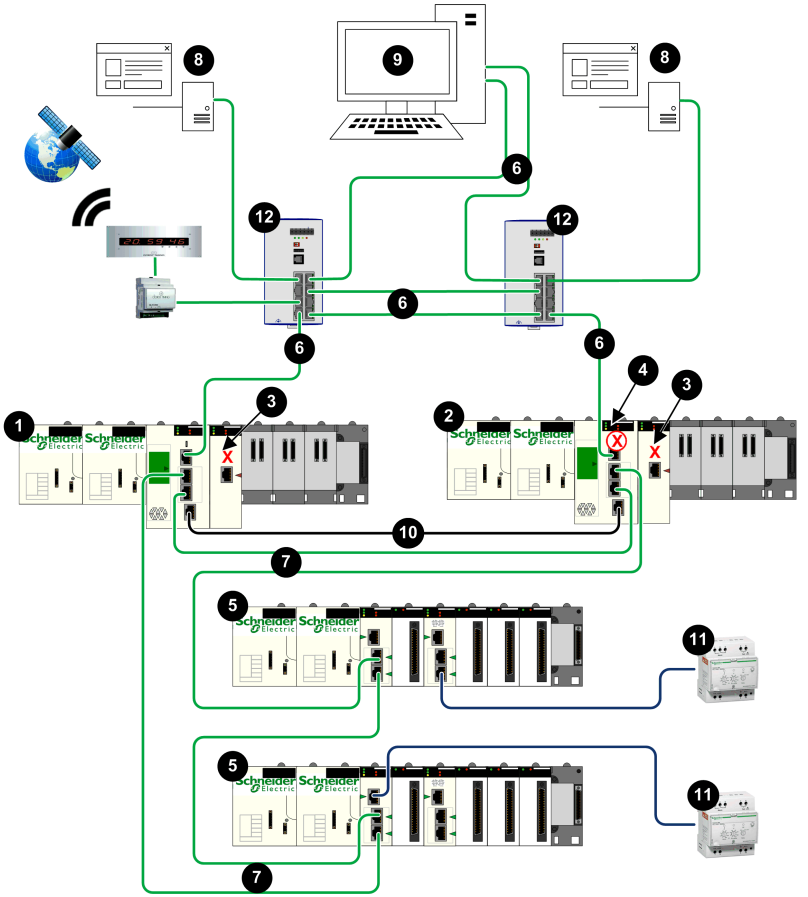
Ciascun BMENUA0100 è un client di un server NTP che risiede nella rete di controllo. La connessione è possibile tramite la porta di controllo BMENUA0100. I moduli BMENUA0100 fungono anche da server NTP per altri dispositivi nell'anello principale RIO Ethernet. In questo design Hot Standby, il modulo BMENUA0100 configurato come “A” funge da server NTP primario e il modulo BMENUA0100 configurato come “B” funge da server NTP di standby. In questo modo, l'ora del controller e l'ora del modulo BMENUA0100 è sincronizzata.

Il BMENUA0100 supporta indicazione di ora/data applicativa. In questo processo, i moduli di indicazione di ora/data registrano gli eventi nel loro buffer locale. Tali eventi con indicazione di data/ora sono consumati dall'applicazione in esecuzione nel controller, che converte i dati

di registrazione grezzi e li memorizza in un formato utilizzabile. Le registrazioni formattate possono essere quindi consumate da un'applicazione di supervisione, come un sistema SCADA.

Rete piana non isolata con M580 Hot Standby

Architettura



1 Controller Hot Standby primario

2 Controller Hot Standby di standby

3 BMENUA0100 con porta di controllo disattivata

4 Controller di standby con blocco automatico della porta service

5 Derivazione RIO Ethernet X80

6 Rete di controllo

7 Anello principale Ethernet RIO

8 Client OPC UA (sistema SCADA)

9 Workstation tecnica con doppia connessione Ethernet

10 Collegamento di comunicazione Hot Standby

11 Apparecchiatura distribuita

12 Switch a doppio anello (DRS)

Descrizione

Questa architettura fornisce connessioni ridondanti dai controller Hot Standby M580 ai client OPC UA doppi (sistemi SCADA). Lo scopo principale è fornire elevata disponibilità ai controller Hot Standby. Per tale motivo, questa architettura presenta una rete piana non isolata, che unisce insieme la rete di controllo e l'anello principale RIO Ethernet in una singola sottorete.

La porta di controllo di BMENUA0100 è disattivata. La comunicazione Ethernet IPv4 al modulo BMENUA0100 è fornita sulla porta backplane. La comunicazione a monte dai controller Hot Standby ai server SCADA avviene tramite la porta service del controller primario. Le porte del controller forniscono connettività a valle ai dispositivi Ethernet sull'anello principale RIO Ethernet.

La porta service del controller di standby (4) è disattivata tramite il software di configurazione Control Expert per selezionare **Blocco automatico della porta service sulla CPU di standby** nella scheda **ServicePort** della configurazione per i controller primario e di standby.

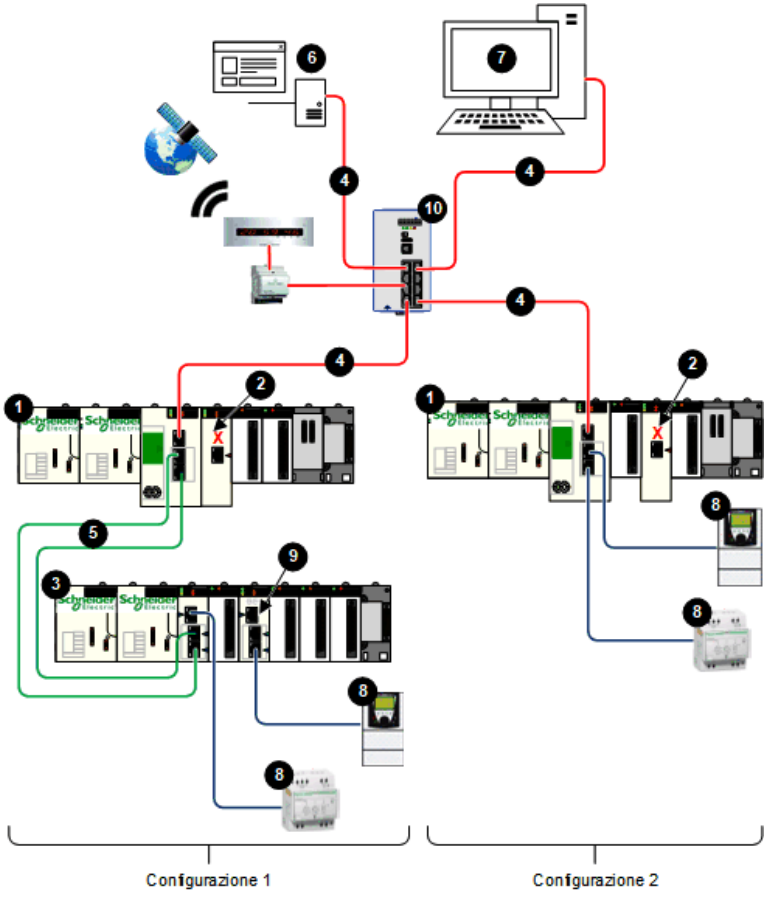
> **NOTA:** la porta service del controller di standby è disattivata per impedire la creazione imprevista di un loop di comunicazione Ethernet, dove la rete di controllo e l'anello principale RIO Ethernet sono parte della stessa sottorete. Vedere *M580 Hot Standby - Guida di pianificazione del sistema* e la sezione Gestione delle reti piane Ethernet con M580 Hot Standby (vedere *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente*) per ulteriori informazioni.

In questo design di rete piana, tutti i dispositivi, inclusi controller, moduli BMECRA31310 e il BMENUA0100 possono essere client dello stesso server NTP che risiede nella rete di controllo. L'ora del controller viene così sincronizzata con il modulo BMENUA0100.

Il BMENUA0100 supporta indicazione di ora/data applicativa. In questo processo, i moduli di indicazione di ora/data registrano gli eventi nel loro buffer locale. Tali eventi con indicazione di data/ora sono consumati dall'applicazione in esecuzione nel controller, che converte i dati di registrazione grezzi e li memorizza in un formato utilizzabile. Le registrazioni formattate possono essere quindi consumate da un'applicazione di supervisione, come un sistema SCADA.

Rete piana con più controller M580 standalone e singolo SCADA

Architettura



1 Controller standalone

2 BMENUA0100 con porta di controllo disattivata

3 Derivazione RIO Ethernet X80

4 Rete di controllo

5 Anello principale Ethernet RIO

6 Client OPC UA (sistema SCADA)

7 Workstation tecnica con connessione Ethernet singola

8 Apparecchiatura distribuita

9 Switch BMENOS0300

10 Switch a doppio anello (DRS)

Descrizione

Questa architettura fornisce una connessione a un singolo client OPC UA (un sistema SCADA) da più controller M580 standalone. Si tratta di un'architettura economica che non richiede elevata disponibilità. Questa architettura presenta una rete piana non isolata, che unisce insieme la rete di controllo e l'anello principale RIO Ethernet in una singola sottorete.

La porta di controllo BMENUA0100 è disattivata per ogni controller standalone. La comunicazione Ethernet IPv4 al modulo BMENUA0100 è fornita sulla porta backplane. La comunicazione a monte da ogni controller al singolo server SCADA avviene tramite la porta service del controller.

Nella configurazione 1, la connettività a valle dal controller alla derivazione RIO X80 Ethernet (4) dal controller è fornita dalle doppie porte di rete dispositivi del controller. Ulteriore connettività a valle è fornita dalla porta service del modulo BMECRA31310 e da uno switch BMENOS0300 (9) all'apparecchiatura Ethernet distribuita.

Nella configurazione 2, la connettività a valle è fornita dalle due porte di rete del dispositivo all'apparecchiatura Ethernet distribuita.

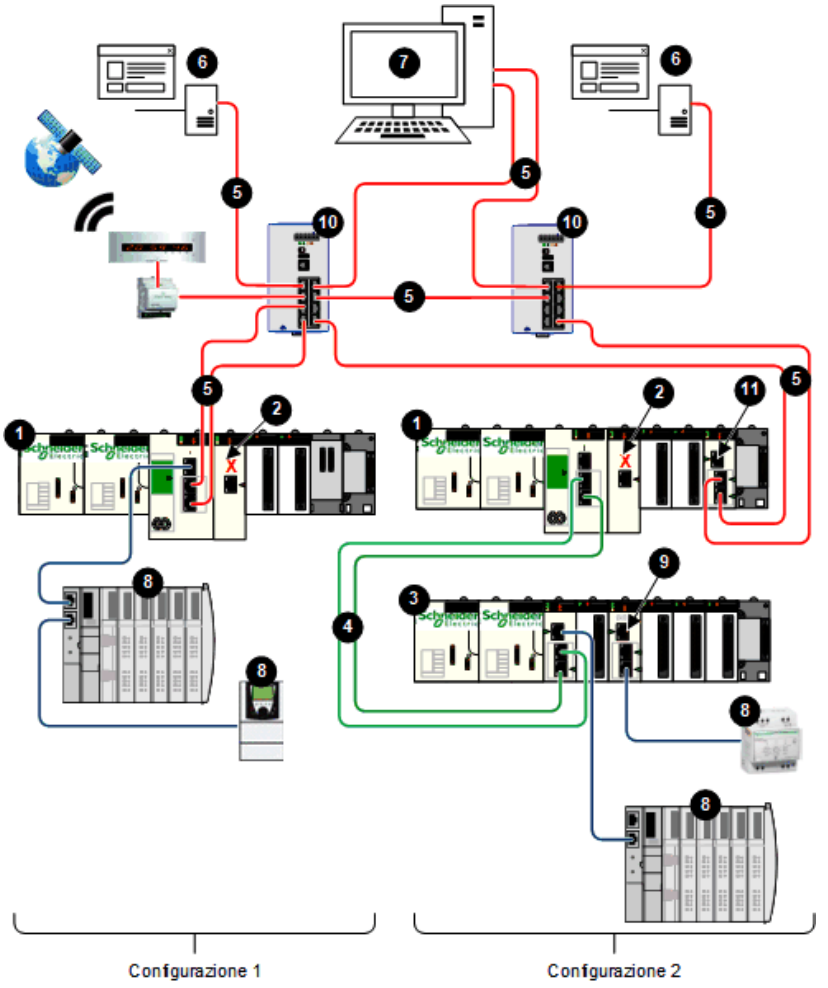
In questo design di rete piana, tutti i dispositivi di rete, inclusi controller, moduli BMECRA31310 e il BMENUA0100,sono client NTP di un server NTP che risiede nella rete di controllo. Di conseguenza, l'ora del controller e l'ora del modulo BMENUA0100 è sincronizzata.

Il BMENUA0100 supporta indicazione di ora/data applicativa. In questo processo, i moduli di indicazione di ora/data registrano gli eventi nel loro buffer locale. Tali eventi con indicazione di data/ora sono consumati dall'applicazione in esecuzione nel controller, che converte i dati di registrazione grezzi e li memorizza in un formato utilizzabile. Le registrazioni formattate

possono essere quindi consumate da un'applicazione di supervisione, come un sistema SCADA.

Rete piana con più controller M580 standalone e SCADA ridondante

Architettura



1 Controller standalone

2 BMENUA0100 con porta di controllo disattivata

3 Derivazione RIO Ethernet X80

4 Anello principale Ethernet RIO

5 Rete di controllo

6 Client OPC UA (sistemi SCADA)

7 Workstation tecnica con doppia connessione Ethernet

8 Apparecchiatura distribuita

9 Switch BMENOS0300

10 Switch a doppio anello (DRS)

11 Modulo BMENOS0300, BMENOC0301 oppure BMENOC0311

Descrizione

Questa architettura fornisce elevata disponibilità della rete di controllo, tramite connessioni ridondanti tra client OPC UA (sistemi SCADA) e più controller M580 standalone. Questa architettura presenta una rete piana non isolata, che unisce insieme la rete di controllo e l'anello principale RIO Ethernet in una singola sottorete.

La porta di controllo BMENUA0100 è disattivata per ogni controller standalone. La comunicazione Ethernet IPv4 al modulo BMENUA0100 è fornita sulla porta backplane.

Nella configurazione 1, la comunicazione a monte dei server SCADA avviene tramite doppie porte di rete dispositivi del controller, con il protocollo di ridondanza RSTP per assegnare ruoli a ogni porta per evitare loop Ethernet logici. La connettività a valle dell'apparecchiatura distribuita Ethernet è fornita dalla porta service del controller.

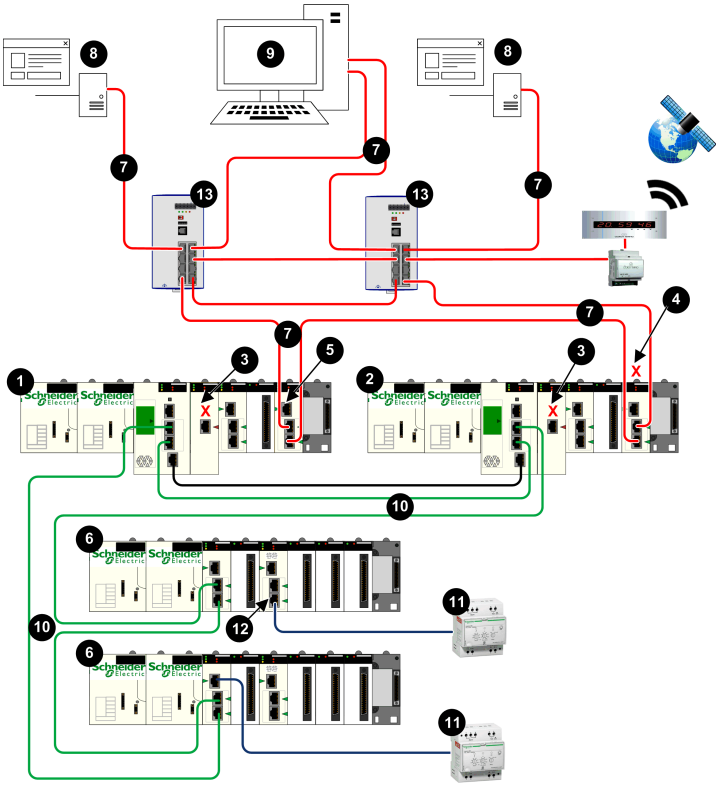
Nella configurazione 2, la connettività a monte dei server SCADA è fornita dalle porte di rete dispositivi di un modulo BMENOS0300, BMENOC0301 oppure BMENOC0311. Il protocollo di ridondanza RSTP consente di assegnare i ruoli a ogni porta per evitare loop Ethernet logici. La connettività a valle del controller è fornita dalle porte di rete dispositivi del controller alla derivazione di I/O remoti X80 Ethernet. Ulteriore connettività a valle è fornita dalla porta service del modulo BMECRA31310 e da uno switch BMENOS0300 (9) all'apparecchiatura Ethernet distribuita.

In questo design di rete piana, tutti i dispositivi di rete, inclusi controller, moduli BMECRA31310 e il BMENUA0100,sono client NTP di un server NTP che risiede nella rete di controllo. Di conseguenza, l'ora del controller e l'ora del modulo BMENUA0100 è sincronizzata.

Il BMENUA0100 supporta indicazione di ora/data applicativa. In questo processo, i moduli di indicazione di ora/data registrano gli eventi nel loro buffer locale. Tali eventi con indicazione di data/ora sono consumati dall'applicazione in esecuzione nel controller, che converte i dati di registrazione grezzi e li memorizza in un formato utilizzabile. Le registrazioni formattate possono essere quindi consumate da un'applicazione di supervisione, come un sistema SCADA.

Rete piana con controller M580 Hot Standby e SCADA ridondante

Architettura



1 Controller Hot Standby primario

2 Controller Hot Standby di standby

3 BMENUA0100 con porta di controllo disattivata

4 BMENOS0300, BMENOC0301 oppure BMENOC0311 con porta backplane disattivata

5 BMENOS0300, BMENOC0301 oppure BMENOC0311 con porta backplane attivata

6 Derivazione RIO Ethernet X80

7 Rete di controllo

8 Client OPC UA (sistema SCADA)

9 Workstation tecnica con doppia connessione Ethernet

10 Anello principale Ethernet RIO

11 Apparecchiatura distribuita

12 Switch BMENOS0300

13 Switch a doppio anello (DRS)

Descrizione

Questa architettura fornisce elevata disponibilità con connessioni ridondanti che collegano client OPC UA ridondanti (sistemi SCADA) a controller Hot Standby ridondanti in una singola sottorete.

Ciascun controller è collegato a SCADA tramite un modulo BMENOS0300, BMENOC0301 oppure BMENOC0311. Per evitare loop Ethernet, la porta backplane di uno dei moduli BMENOS0300, BMENOC0301 oppure BMENOC0311 è disattivato. In questo esempio, è il modulo nel controller di standby (4) ad avere una porta backplane disattivata. Inoltre, il protocollo di ridondanza RSTP consente di assegnare ruoli a ogni porta per evitare loop Ethernet logici.

La porta di controllo BMENUA0100 è disattivata (3) per ogni controller standalone. La comunicazione Ethernet IPv4 al modulo BMENUA0100 è fornita sulla porta backplane.

La connettività a valle delle derivazioni RIO X80 Ethernet è fornita dalle porte di rete dispositivi del controller. Ulteriore connettività a valle delle derivazioni RIO X80 Ethernet è fornita dalla porta service CRA e da uno switch (12) BMENOS0300 all'apparecchiatura Ethernet distribuita.

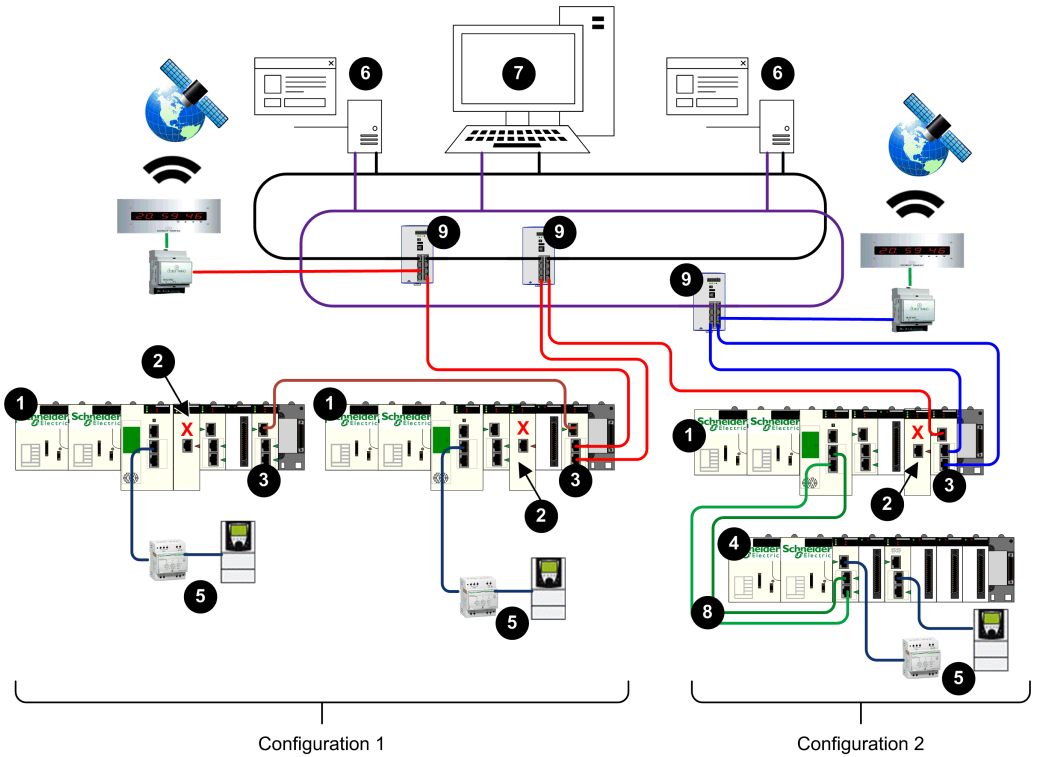
In questo design di rete piana, tutti i dispositivi di rete, compresi ciascun controller Hot Standby e modulo BMENUA0100, sono client NTP di un server NTP che risiede nella rete di

controllo. Di conseguenza, l'ora del controller e l'ora del modulo BMENUA0100 è sincronizzata.

Il BMENUA0100 supporta indicazione di ora/data applicativa. In questo processo, i moduli di indicazione di ora/data registrano gli eventi nel loro buffer locale. Tali eventi con indicazione di data/ora sono consumati dall'applicazione in esecuzione nel controller, che converte i dati di registrazione grezzi e li memorizza in un formato utilizzabile. Le registrazioni formattate possono essere quindi consumate da un'applicazione di supervisione, come un sistema SCADA.

Rete gerarchica con più controller M580 standalone collegati alla rete di controllo e SCADA ridondante

Architettura



1 Controller standalone

2 BMENUA0100 con porta di controllo disattivata

3 Modulo BMENOC0321 di comunicazione Ethernet

4 Derivazione RIO Ethernet X80

5 Apparecchiatura distribuita

6 Client OPC UA (sistema SCADA)

7 Workstation tecnica con doppia connessione Ethernet

8 Anello principale Ethernet RIO

9 Switch a doppio anello (DRS)

Descrizione

Questa architettura presenta una rete gerarchica, che si basa sui moduli di comunicazione BMENOC0321 per instradare il traffico di rete tra sottoreti. La comunicazione a monte dai controller ai client OPC UA (sistemi SCADA) è possibile tramite le doppie porte di rete dispositivi del modulo BMENOC0321, mediante il protocollo di ridondanza RSTP per evitare loop Ethernet logici.

> **NOTA:** Questa architettura richiede la configurazione di instradamenti statici nell'apparecchiatura delle rete di controllo per reindirizzare le varie sottoreti dei vari controller.

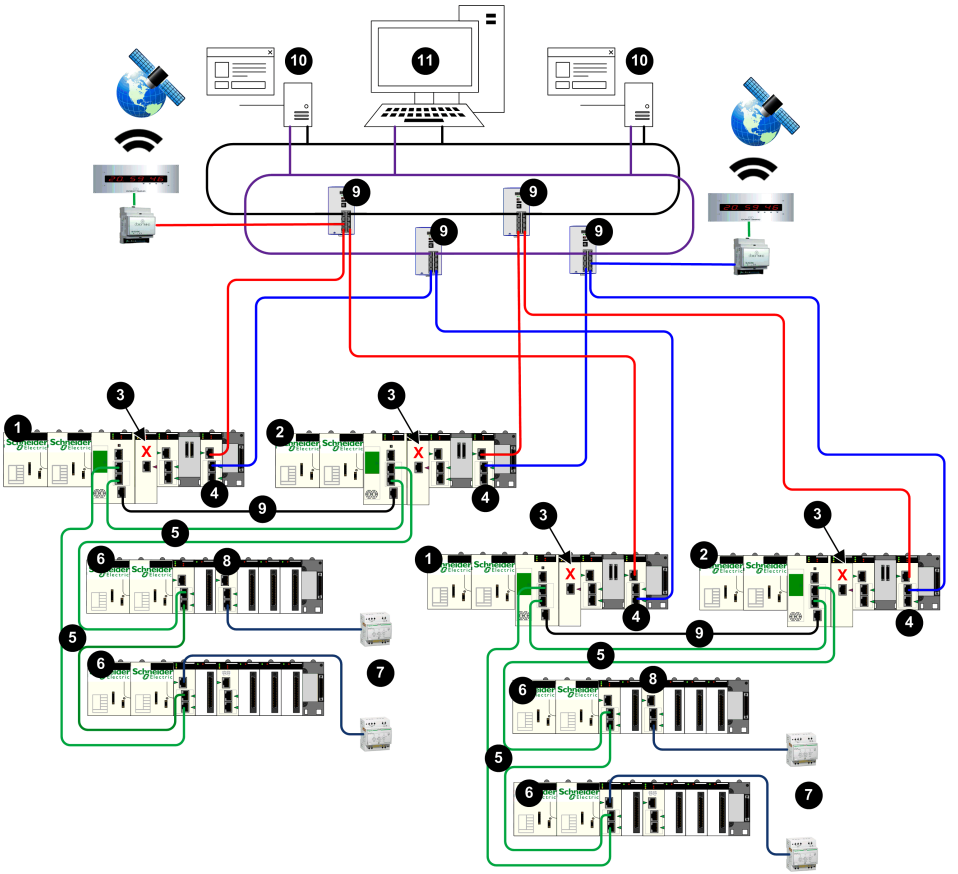
La porta di controllo BMENUA0100 (2) è disattivata per ogni controller standalone. La comunicazione Ethernet IPv4 al modulo BMENUA0100 è fornita sulla porta backplane.

La configurazione 1 comprende due controller che risiedono nella stessa sottorete. Questa configurazione impiega il modulo BMENOC0321 per fornire comunicazioni a monte ridondanti ai server SCADA ridondanti. Il modulo BMENOC0321 utilizza il protocollo di ridondanza RSTP per evitare loop Ethernet logici. Le doppie porte di rete dispositivi dei due controller forniscono comunicazione a valle all'apparecchiatura Ethernet distribuita.

La configurazione 2 comprende un singolo controller, con derivazione RIO X80 Ethernet. Questo controller utilizza il modulo BMENOC0321 per la comunicazione a monte ai server SCADA ridondanti. Il BMENOC0321 lo consente mediante due sottoreti indipendenti. La comunicazione a valle dalla derivazione RIO X80 Ethernet è fornita dalla porta service del modulo BMECRA31310 e da uno switch BMENOS0300 all'apparecchiatura Ethernet distribuita.

Rete gerarchica con più controller M580 Hot Standby e connessioni SCADA ridondanti

Architettura



1 Controller Hot Standby primario

2 Controller Hot Standby di standby

3 BMENUA0100 con porta di controllo disattivata

4 Modulo BMENOC0321 di comunicazione Ethernet

5 Anello principale Ethernet RIO

6 Derivazione RIO Ethernet X80

7 Apparecchiatura distribuita

8 Switch BMENOS0300

9 Switch a doppio anello (DRS)

10 Client OPC UA (sistema SCADA)

11 Workstation tecnica con doppia connessione Ethernet

Descrizione

Questa architettura presenta una rete gerarchica, che si basa sui moduli di comunicazione BMENOC0321 (4) per instradare il traffico di rete tra sottoreti. La comunicazione a monte dai controller Hot Standby ai client OPC UA (sistemi SCADA) è possibile tramite le doppie porte di rete dispositivi dei moduli BMENOC0321, mediante il protocollo di ridondanza RSTP per evitare loop Ethernet logici.

> **NOTA:** Questa architettura richiede la configurazione di instradamenti statici nell'apparecchiatura delle rete di controllo per reindirizzare le varie sottoreti dei vari controller.

La porta di controllo BMENUA0100 (3) è disattivata per ogni controller. La comunicazione Ethernet IPv4 al modulo BMENUA0100 è fornita sulla porta backplane.

Questa configurazione impiega il modulo BMENOC0321 per fornire comunicazioni a monte ridondanti ai server SCADA ridondanti. Le doppie porte di rete dispositivi dei controller forniscono comunicazione a valle alle derivazioni RIO X80 Ethernet. Ulteriore comunicazione a valle dalla derivazione RIO X80 Ethernet all'apparecchiatura Ethernet distribuita è fornita dalla porta service BMECRA31310 e da uno switch BMENOS0300 (8).

Messa in servizio e installazione

Introduzione

Questo capitolo descrive come selezionare una modalità operativa e installare il modulo di comunicazione Ethernet BMENUA0100 con server OPC UA integrato.

Elenco di controllo per la messa in servizio del modulo BMENUA0100

Elenco di controllo per la messa in servizio

La struttura seguente presenta una sequenza di attività da seguire durante la messa in servizio e l'installazione di un nuovo modulo BMENUA0100. Questo esempio configura il modulo in modo che funzioni in modalità PKI Autofirmato e CA con indirizzi IPV6 SLAAC e IPV4:

1. Configurare l'applicazione, pagina 117 Control Expert.
2. Configurare il router / server SLAAC (per IPV6 in modalità SLAAC).
3. Selezionare le operazioni in modalità Advanced (o Secured) per il modulo:

a.	Impostare il selettore a rotazione, pagina 23 sul retro del modulo nella posizione Modalità Advanced (o Secured), pagina 30.
b.	Installare il modulo, pagina 84 in uno slot Ethernet sul rack.

4. Configurare le impostazioni di sicurezza informatica tramite le pagine Web, pagina 86 del modulo:

a.	Creare la configurazione di sicurezza informatica tramite la pagina Web Impostazioni, pagina 94.
b.	Impostare la **Modalità PKI** su Autofirmato e CA.
c.	Per i dispositivi client che non supportano PKI, creare un elenco, pagina 111 di **certificati del client attendibili**.
g.	**Applicare** il file di configurazione.

5. Eseguire la registrazione manuale del certificato, pagina 110:

a.	Generare una richiesta di firma del certificato (CSR).
b.	Eseguire il push del certificato CA.
c.	Eseguire il push del certificato del dispositivo.

6. Aggiungere il certificato CA ai dispositivi client OPC UA.
7. Testare la comunicazione tra client e server OPC UA.

Messa in servizio del modulo BMENUA0100

Introduzione

Il modulo BMENUA0100 con server OPC UA integrato compare nel catalogo hardware di Control Expert come modulo di comunicazione. Consuma un canale di I/O.

Quando si aggiunge un nuovo modulo BMENUA0100, la modalità operativa di sicurezza informatica è impostata sulla modalità Advanced (o Secured) per impostazione predefinita. Per configurare il nuovo modulo per l'utilizzo in modalità Advanced (o Secured), seguire lo scenario per Messa in servizio della modalità Advanced (o Secured), pagina 30 di seguito.

Per cambiare la modalità operativa di sicurezza informatica di un modulo configurato in precedenza, includendo un nuovo modulo che si pensa di configurare per il funzionamento in modalità Standard, eseguire un'operazione di Cybersecurity Reset (o Security Reset), pagina 82 per il modulo. Dopo l'operazione di Cybersecurity Reset (o Security Reset), è possibile seguire lo scenario pe: Messa in servizio in modalità Advanced (o Secured), pagina 30 o Messa in servizio in modalità Standard, pagina 30.

Messa in servizio in modalità Advanced (o Secured)

La messa in servizio di un modulo BMENUA0100 per il funzionamento in modalità Advanced (o Secured) richiede il completamento di due processi di configurazione:

- Configurazione della sicurezza informatica tramite le pagine Web del modulo.
- Configurazione di indirizzo IP, client NTP e agente SNMP tramite lo strumento di configurazione Control Expert.

Solo un amministratore di sicurezza, che utilizza la combinazione predefinita di nome utente/password, pagina 31 della modalità Advanced (o Secured) può mettere in servizio il modulo in modalità Advanced (o Secured).

NOTA: Eseguire questi processi di configurazione nell'ordine seguente:

- Utilizzare Control Expert per configurare gli indirizzi IP di controllo e backplane.
- Utilizzare le pagine Web del modulo per configurare le impostazioni di sicurezza informatica.
- Utilizzare Control Expert per completare le configurazioni del client NTP e dell'agente SNMP.

NOTA: Per la messa in servizio in modalità Advanced (o Secured) con registrazione manuale, vedere la sezione Registrazione manuale, pagina 110.

La procedura seguente è prevista per un nuovo modulo non configurato in precedenza. Se si utilizza un modulo configurato in precedenza, eseguire un'operazione di Cybersecurity Reset (o Security Reset), pagina 82 prima di procedere con i passaggi seguenti.

Per mettere in servizio il modulo in modalità Advanced (o Secured):

1. Configurare le impostazioni dell'indirizzo IP:

a.	Aprire lo strumento di configurazione Control Expert.
b.	In Control Expert, creare un **nuovo progetto** aggiungere un modulo BMENUA0100 al progetto dal **Catalogo hardware**, quindi configurare le impostazioni dell'indirizzo IP, pagina 117.

2. Configurare le impostazioni di sicurezza informatica:

a.	Con il modulo staccato dal rack, utilizzare il cacciavite in plastica fornito con il modulo, pagina 23 per impostare il selettore a rotazione sulla posizione **Advanced (o Secured)**.
b.	Installare, pagina 83 il modulo in uno slot Ethernet sul rack Ethernet principale locale, quindi spegnere e riaccendere l'alimentazione.
c.	Utilizzare il browser Internet per collegare il PC di configurazione al modulo, utilizzando la porta di controllo o la porta backplane e accedere alle pagine Web del modulo all'indirizzo IP configurato.
g.	Se il browser Internet visualizza un messaggio, pagina 88 che indica un potenziale rischio per la sicurezza, leggere il messaggio e, se si accetta, procedere per eseguire la connessione facendo clic su **Accetta il rischio e continua** (o messaggio simile, in base alla lingua specifica del browser).
e.	Nella pagina di accesso utente, immettere la combinazione di nome utente/password predefinita, pagina 31.
f.	Cambiare e confermare la password. Per i requisiti per la password, consultare l'argomento Gestione utente, pagina 113. Viene visualizzata la **Home** page, pagina 91 del modulo.
g.	Partendo dalla **Home** page, spostarsi sulle pagine Web del modulo e configurarne le impostazioni di sicurezza informatica.

3. Configurare le impostazioni di client NTP e agente SNMP:

a.	Aprire lo strumento di configurazione Control Expert.
b.	In Control Expert, configurare le impostazioni del client NTP e dell'agente SNMP., pagina 117
c.	Dopo aver completato la configurazione del progetto di Control Expert, collegarsi al controller e trasferirvi il progetto.

NOTA: quando la configurazione viene caricata nel modulo BMENUA0100, il relativo stato cambia da NON CONFIGURATO a CONFIGURATO. Il LED **SECURE**, pagina 138 indica se il modulo è configurato o meno e se il server OPC UA è collegato a un client OPC UA.

Messa in servizio in modalità Standard

Nella modalità Standard, non è richiesta la configurazione della sicurezza informatica. Le impostazioni di indirizzo IP, client NTP e agente SNMP vengono configurate utilizzando lo strumento di configurazione Control Expert. Nella modalità Standard, il modulo inizia a comunicare quando viene posto sul rack, si fornisce l'alimentazione e riceve una configurazione valida da Control Expert.

Utilizzare la combinazione predefinita di nome utente/password, pagina 31 per mettere in servizio il modulo in modalità Standard.

Per mettere in servizio il modulo in modalità Standard:

1. Con il modulo staccato dal rack, utilizzare il cacciavite in plastica fornito con il modulo, pagina 23 per impostare il selettore a rotazione sulla posizione **Standard**.
2. Posizionare il modulo in uno slot Ethernet sul rack Ethernet principale locale, quindi spegnere e riaccendere l'alimentazione.
3. Aprire lo strumento di configurazione Control Expert.
4. In Control Expert, creare un **nuovo progetto**, aggiungere un modulo BMENUA0100 al progetto dal **Catalogo hardware**, quindi configurare le impostazioni per Indirizzo IP, pagina 117, Client NTP, pagina 126 e Agente SNMP, pagina 129.
5. Dopo aver completato la configurazione del progetto di Control Expert, collegarsi al controller e trasferirvi il progetto.

   NOTA: quando si opera in modalità Standard, il LED **SECURE** è spento.

Operazione di Cybersecurity Reset (o Security Reset)

Per un modulo configurato in precedenza o per un nuovo modulo da configurare per il funzionamento in modalità di sicurezza informatica, eseguire un'operazione di

Cybersecurity Reset (o Security Reset) prima di procedere con la configurazione della sicurezza informatica. L'operazione di ripristino configura le impostazioni di sicurezza ai valori predefiniti. È possibile eseguire un ripristino tramite le pagine Web del modulo o il selettore a rotazione posto sul retro del modulo.

Pagine Web: per un modulo BMENUA0100 correntemente configurato per il funzionamento in modalità Advanced (o Secured):

1. Passare alla pagina Web **Gestione configurazione > RESET**.
2. Fare clic su **Reset**.

   NOTA: l'operazione di Cybersecurity Reset (o Security Reset) è completata quando il LED **RUN** è verde fisso ed entrambi i LED della porta di controllo **NS** e della porta backplane **BS** sono illuminati in rosso fisso.
3. Spegnere e riaccendere il modulo in uno dei modi seguenti:
   - Spegnere il rack del modulo, quindi riaccendere.
   - Estrarre fisicamente il modulo dal rack, quindi reinserirlo.

   A questo punto è possibile procedere con la messa in servizio in modalità Advanced (o Secured).

Selettore a rotazione: per qualsiasi modulo BMENUA0100:

1. Con il modulo staccato dal rack, utilizzare il cacciavite in plastica fornito con il modulo, pagina 23 per impostare il selettore a rotazione sulla posizione **Cybersecurity Reset**.
2. Installare, pagina 83 il modulo in uno slot Ethernet sul rack Ethernet principale locale, quindi spegnere e riaccendere l'alimentazione.

   NOTA: vengono così ripristinate le impostazioni predefinite del modulo, compreso l'indirizzo IP predefinito della porta di controllo, pagina 117 di 10.10.MAC5.MAC6. Se gli ultimi due byte dell'indirizzo MAC (*MAC5.MAC6*) corrispondono a *0,0* nell'indirizzo predefinito, effettuare una connessione via cavo punto a punto tra il computer e il controller, il modulo di comunicazione o un altro modulo.

   Al termine, il LED **RUN** è verde fisso ed entrambi i LED **NS** della porta di controllo e della porta backplane **BS** sono illuminati in rosso fisso. È possibile spegnere, rimuovere il modulo dal rack e procedere con la Messa in servizio in modalità Advanced (o Secured), pagina 30 o la Messa in servizio in modalità Standard, pagina 30.

Installazione del BMENUA0100

Introduzione

È possibile installare il modulo BMENUA0100 solo in un rack locale principale Ethernet posizionandolo in uno slot Ethernet non riservato per l'alimentatore o il controller.

NOTA: Se l'applicazione è basata su EcoStruxure Control Expert versione inferiore a 15.3 e se l'applicazione comprende più controller (che non sono controller Hot Standby) ciascuno con un modulo BMENUA0100, installare i moduli in modo che il numero di slot di ogni modulo BMENUA0100 sia univoco. Ad esempio, per un'applicazione che include due controller, se un modulo BMENUA0100 nel rack del controller 1 è posizionato nello slot 4, posizionare un modulo BMENUA0100 nel rack del controller 2 in uno slot diverso dallo slot 4.

Precauzioni sulla messa a terra

Seguire le normative e i codici locali e nazionali in materia di sicurezza.

⚠⚠ PERICOLO

RISCHIO DI SCARICHE ELETTRICHE

Quando si lavora con cavi schermati, indossare dispositivi di protezione individuale (DPI).

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

Il backplane per il modulo è in comune con il piano della messa a terra funzionale (FE) e deve essere montato e collegato a un backplane conduttivo con messa a terra.

⚠ AVVERTIMENTO

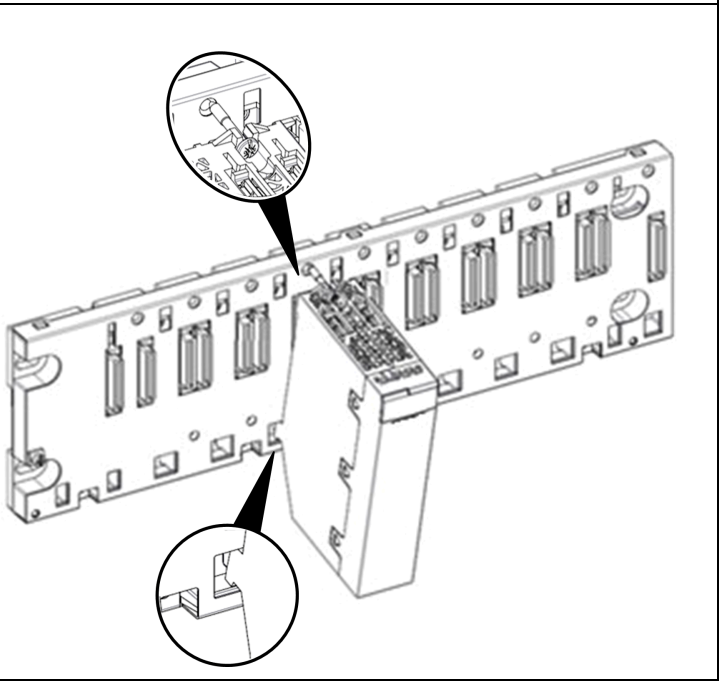
FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Collegare il backplane alla messa a terra funzionale (FE) dell'installazione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Installazione di un modulo BMENUA0100 nel rack

Un modulo BMENUA0100 richiede un singolo slot Ethernet del rack. È possibile installare il modulo in qualsiasi slot Ethernet non riservato per l'alimentatore o il controller. Seguire questa procedura per installare un modulo BMENUA0100 in un rack:

Passo	Azione	
1	Posizionare i pin di individuazione posti in basso nel retro del modulo negli slot corrispondenti sul rack.	
2	Ruotare il modulo verso la parte superiore del rack in modo che sia allineato alla parte posteriore del rack. A questo punto il modulo è in posizione.	
3	Serrare la singola vite di montaggio sul modulo per tenere il modulo in posizione nel rack. Coppia di serraggio: 0,4...1,5 N m (0.30...1.10 lbf-ft).	

Messa a terra dei moduli I/O

Per informazioni sulla messa a terra, consultare la sezione *Messa a terra del rack e del modulo alimentatore* nel documento *Modicon X80 Rack e alimentatori - Manuale di riferimento hardware*.

Configurazione

Introduzione

Questo capitolo descrive come configurare il modulo di comunicazione Ethernet BMENUA0100 con il server OPC UA integrato.

Configurazione delle impostazioni di sicurezza informatica di BMENUA0100

Introduzione

Questa sezione descrive come utilizzare le pagine Web del modulo di comunicazione Ethernet BMENUA0100 con server OPC UA. Utilizzare le pagine Web per creare una configurazione di sicurezza informatica per il modulo e visualizzare i dati di diagnostica.

Presentazione delle pagine Web di BMENUA0100

Introduzione

Utilizzare le pagine Web di BMENUA0100 per creare, gestire e diagnosticare una configurazione di sicurezza informatica per il modulo e visualizzare eventi e dati di diagnostica OPC UA.

NOTA:

- Le pagine Web del modulo BMENUA0100 supportano la comunicazione HTTPS sui protocolli IPv4 e IPv6, pagina 118.
- Per accedere alle pagine Web, utilizzare solo le versioni recenti dei browser Internet. Alcuni browser meno recenti, ad esempio Internet Explorer v7 e versioni precedenti, non sono supportati.

  NOTA: Il browser Internet Chrome, versione 123.0.6312.123 (build ufficiale) (64 bit) è stato testato con le pagine Web di BMENUA0100.

Per il funzionamento del modulo BMENUA0100 in modalità Advanced (o Secured), è richiesta una configurazione di sicurezza informatica da effettuare prima che le impostazioni di indirizzo IP, client NTP e SNMP possano essere configurate con Control Expert, pagina 117. È possibile definire una configurazione di sicurezza informatica solo localmente per

ciascun modulo BMENUA0100 collegando un PC di configurazione, eseguendo un browser HTTPS, al modulo BMENUA0100:

- Porta di controllo, la porta di controllo è attivata.
- Porta backplane (tramite un modulo BMENOC0301 o BMENOC0311 o il controller), se la porta di controllo è disattivata.

NOTA: Prima della verifica della validità delle impostazioni di sicurezza informatica immesse nelle pagine Web, il modulo BMENUA0100 configura innanzitutto le impostazioni dell'indirizzo IP per la porta di controllo e la porta backplane configurate in Control Expert, pagina 117.

Per il funzionamento del modulo BMENUA0100 in modalità Standard, le impostazioni di sicurezza informatica non sono richieste e non possono essere configurate.

NOTA:

- Quando si utilizza un certificato autofirmato, alcuni browser possono segnalare la connessione tra il PC e il modulo come “Non sicura”.
- Per il funzionamento dei moduli BMENUA0100 in modalità Advanced (o Secured) in un sistema Hot Standby, verificare che le impostazioni di sicurezza informatica per il modulo BMENUA0100 nel controller primario siano uguali alle impostazioni di sicurezza informatica per il modulo BMENUA0100 nel controller di standby. Il sistema non esegue automaticamente questa verifica.

L'accessibilità delle pagine Web dipende dalla modalità operativa di sicurezza informatica:

Pagina Web o gruppo	Modalità Advanced (o Secured)	Modalità Standard
Home, pagina 91	✓	✓
Impostazioni (sicurezza dispositivo), pagina 94	✓	–
Gestione certificati, pagina 105	✓	–
Controllo accesso, pagina 113	✓	–
Gestione configurazione, pagina 115	✓	–
Diagnostica, pagina 160	✓	✓
✓ : le pagine Web sono accessibili. – : le pagine Web non sono accessibili.		

Configurazione iniziale delle impostazioni di sicurezza informatica

È possibile configurare le impostazioni iniziali di sicurezza informatica per un modulo BMENUA0100 che:

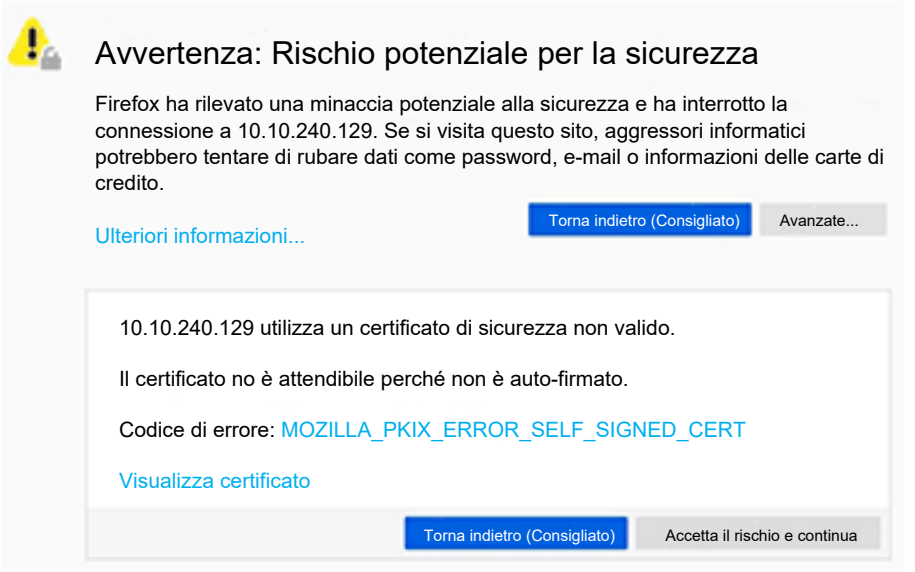
- non è mai stato configurato e conserva la configurazione predefinita iniziale;
- è stato configurato in precedenza, ma la configurazione predefinita è stata ripristinata eseguendo il comando di Cybersecurity (o Security) Reset, pagina 31.

Dopo aver configurato un modulo con le impostazioni di sicurezza informatica e il modulo funziona in modalità Advanced (o Secured), è inoltre possibile modificare le impostazioni di sicurezza informatica tramite le pagine Web.

Per le istruzioni su come applicare una configurazione iniziale al modulo, consultare la sezione sulla messa in servizio, pagina 80.

Primo accesso alle pagine Web

Quando si accede a un modulo BMENUA0100 non configurato, viene visualizzata la seguente schermata (o una schermata simile a seconda del browser in uso):



Malgrado i termini utilizzati nel messaggio, la connessione è protetta tramite HTTPS. Leggere il messaggio e, se si accetta, procedere con l'accesso iniziale facendo clic su **[Accetta il rischio e continua]** (o altro messaggio simile specifico del browser).

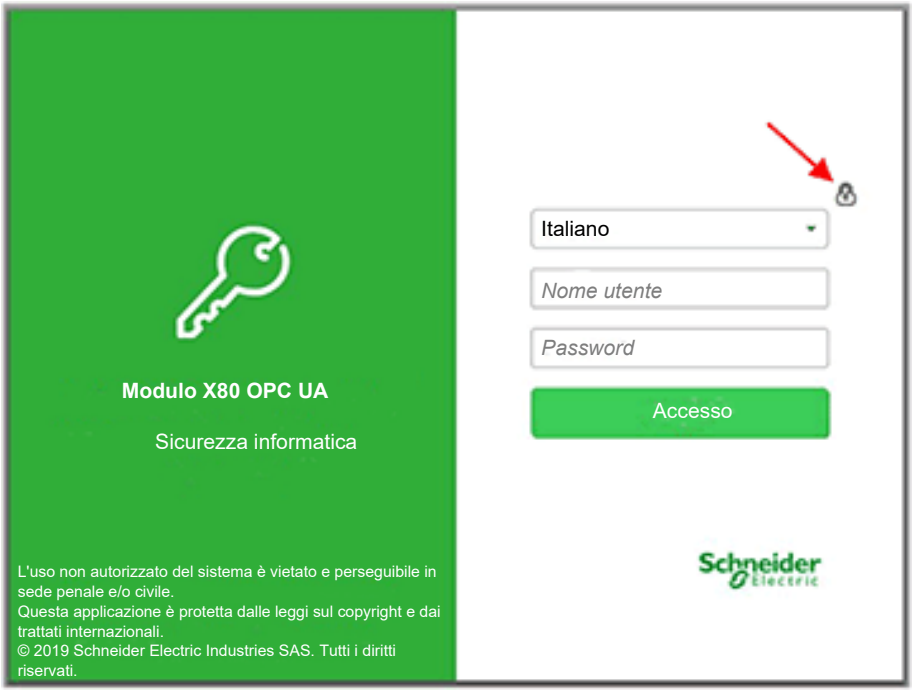
NOTA: il messaggio precedente viene visualizzato perché il modulo non contiene ancora una configurazione valida e utilizza un certificato autofirmato.

Accesso alle pagine Web

Al primo accesso, l'amministratore di sicurezza immette la combinazione predefinita di nome utente e password, pagina 31. Subito dopo, all'amministratore viene richiesto di cambiare la password predefinita.

È necessario accedere ogni volta che si aprono le pagine Web del modulo BMENUA0100. Solo gli utenti a cui è stato assegnato un account utente valido, con una combinazione valida di nome utente e password creata da un amministratore di sicurezza nella pagina Web **> Controllo accesso**Gestione utenteControllo accesso, pagina 113, possono accedere alle pagine Web del modulo.

Nella pagina di accesso, selezionare una lingua dall'elenco a discesa, quindi immettere il proprio **Nome utente** ela **Password**.

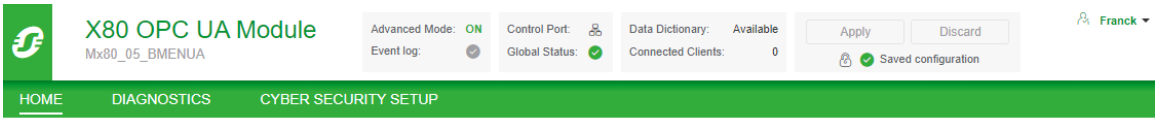


NOTA: la modalità operativa di sicurezza informatica del modulo viene visualizzata dall'icona del lucchetto nella parte superiore destra della finestra di dialogo (indicata dalla freccia rossa, sopra). Se il lucchetto è:

- Chiuso (come mostrato sopra): il modulo funziona in modalità Advanced (o Secured), pagina 30.
- Aperto: il modulo funziona in modalità Standard, pagina 30.

Banner pagina Web

Ogni pagina Web presenta un banner nella parte superiore:



Il banner presenta le informazioni seguenti sul modulo BMENUA0100:

- Modalità Advanced (o Secured):
  - ON: il modulo funziona in modalità Advanced (o Secured), pagina 30.
  - OFF: il modulo funziona in modalità Standard, pagina 30.
- Registro eventi:
  - Il servizio di registro Eventi è disattivato.
  - Il servizio di registro Eventi è attivato; il server di registro è raggiungibile.
  - Il servizio di registro Eventi è attivato, ma il server di registro non è raggiungibile.
  - Il servizio di registro Eventi è attivato, ma è stato rilevato un errore.
- Porta di controllo:
  - La porta di controllo è attivata.
  - La porta di controllo è disattivata.
- Stato globale:
  - Tutti i servizi sono operativi.
  - Almeno un servizio non è operativo.
- Dizionario dati:
  - Disponibile: la funzionalità del dizionario dati è disponibile.
  - Non disponibile: la funzionalità del dizionario dati non è disponibile o non è abilitata.
- Client collegati: il numero di client OPC UA collegati.

- Applica/Elimina configurazione: indica lo stato della configurazione della pagina Web di sicurezza informatica del modulo:
  - Configurazione non modificata: la configurazione della sicurezza informatica non contiene modifiche in sospeso o non valide. I pulsanti **Applica** e **Scarta** sono disattivati.
  - Configurazione in sospeso: una o più modifiche alla configurazione di sicurezza informatica non sono ancora state applicate. Entrambi i pulsanti **Applica** e **Scarta** sono attivati.
  - Configurazione non valida: la configurazione della sicurezza informatica è incompleta o errata. Il pulsante **Applica** è disattivato; il pulsante **Scarta** è attivato. In questo stato, la pagina Web visualizza, accanto a ogni voce di menu interessata, un cerchio rosso contenente il numero di impostazioni di configurazione non valide tramite tale percorso di menu. Quando ci si sposta su una pagina con un'impostazione di configurazione non valida, la pagina visualizza l'impostazione di configurazione non valida.

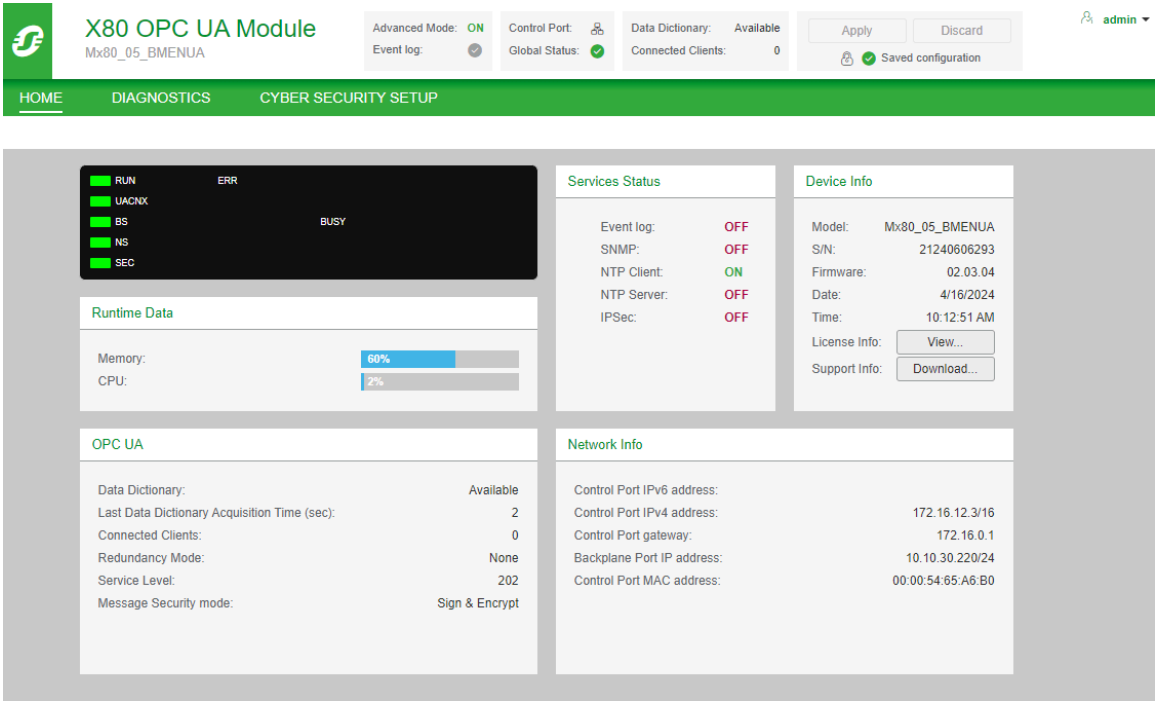
Guida della pagina Web

Molte pagine Web offrono una guida sensibile al contesto a livello di parametro. Per ottenere informazioni per un parametro o campo specifico, posizionare il puntatore del cursore sull'icona .

Home page

Introduzione alla home page

Quando si accede alle pagine Web di BMENUA0100, per impostazione predefinita si apre la **Home** page. Se il modulo ha una configurazione valida, viene visualizzata la seguente pagina:



Utilizzare la **Home** page per:

- Accedere alla struttura di navigazione, contenente i collegamenti alle pagine Web del modulo BMENUA0100. Quando il modulo opera in:
  - Modalità Advanced (o Secured), pagina 30, i menu DIAGNOSTICA e CONFIGURAZIONE SICUREZZA INFORMATICA sono visualizzati e accessibili per l'amministratore della sicurezza.
  - Modalità Standard, pagina 30, è accessibile solo il menu DIAGNOSTICA.
- Visualizzare lo stato, pagina 134 dei LED del modulo, pagina 24.
- Visualizzare le raccolte di dati per il modulo, compresi:
  - Dati di runtime, pagina 93
  - OPC UA, pagina 93
  - Stato servizi, pagina 93
  - Informazioni sulla rete, pagina 94
  - Informazioni sul dispositivo, pagina 94

NOTA: quando il selettore a rotazione sul retro del modulo è impostato sulla posizione Cybersecurity (o Security) Reset, pagina 31, non può esistere comunicazione con il modulo. Le pagine Web, quindi, compresa la **Home** page, non sono accessibili.

Dati di runtime

L'area **OPC UA** visualizza:

- **Memoria**: la percentuale di RAM interna utilizzata dal server OPC UA (MEM_USED_PERCENT).
- **CPU**: La percentuale di capacità di elaborazione della CPU correntemente utilizzata (CPU_USED_PERCENT).

NOTA: Le voci descritte sopra sono basate sugli elementi nel DDT, pagina 139 T_BMENUA0100.

OPC UA

L'area **Dati di runtime** visualizza:

- **Dizionario dati**: lo stato di disponibilità del dizionario dati (DATA_DICT).
- **Ora ultima acquisizione dizionario dati (sec)**: la durata dell'ultima acquisizione del dizionario dati (DATA_DICT_ACQ_DURATION).
- **Client connessi**: il numero di client OPC UA collegati (CONNECTED_CLIENTS).
- **Modalità di ridondanza** la modalità di failover supportata per un sistema Hot Standby (REDUNDANCY_MODE).
- **Livello di servizio**: la condizione del server OPC UA, basata su qualità di dati e servizio (SERVICE_LEVEL).

  NOTA: le cinque voci descritte sopra sono basate sugli elementi nel DDT, pagina 139 T_BMENUA0100.
- **Modalità Sicurezza messaggio**: l'impostazione configurata nella pagina Web OPC UA, pagina 103: Nessuno, Firma o Firma e codifica.

Stato servizi

L'area **Stato servizio** visualizza lo stato, attivato (ON) o disattivato (OFF), servizi seguenti come riportato nel DDT, pagina 139 T_BMENUA0100:

- **Registro eventi** (EVENT_LOG_SERVICE)
- **SNMP** (SNMP_SERVICE)
- **Client NTP** (NTP_CLIENT_SERVICE)
- **Server NTP** (NTP_SERVER_SERVICE)
- **IPSec** (IPSEC)

Per i moduli precedenti alla versione BMENUA0100.2.

- **Flussi dati Control Expert** (CONTROIL_EXPERT_IP_FORWARDING)

- **Flussi dati da CPU a CPU** (CPU_TO_CPU_IP_FORWARDING)

Informazioni sulla rete

Quest'area visualizza le impostazioni di configurazione per il modulo BMENUA0100 immesso in Control Expert, pagina 117 e riportato nel DDT, pagina 139 T_BMENUA0100, tra cui:

- porta di controllo (CONTROL_PORT_IPV6, CONTROL_PORT_IPV4 e CONTROL_PORT_GTW)
- porta backplane (ETH_BKP_PORT_IPV4)
- indirizzo MAC del modulo, un valore esadecimale univoco assegnato in fabbrica a ciascun modulo.

Informazioni sul dispositivo

Quest'area visualizza codice prodotto, numero di serie e versione del firmware (FW_VERSION nel DDT, pagina 139 T_BMENUA0100), data e ora per il modulo BMENUA0100.

Fare clic su **Visualizza...** per visualizzare le informazioni sulla licenza.

Fare clic su **Download...** per visualizzare la finestra di dialogo **Download informazioni supporto**. Per ulteriori informazioni, consultare la sezione Controllo accesso, pagina 113.

Impostazioni

Nelle pagine Web del modulo BMENUA0100, a partire dalla pagina **Home**, selezionare **Impostazioni** per visualizzare i collegamenti alle seguenti pagine di configurazione, in cui è possibile immettere le impostazioni di sicurezza del dispositivo:

- Policy account utente, pagina 95
- Registri eventi, pagina 95
- Servizi di rete, pagina 96
- Inoltro del servizio, pagina 98
- IPsec, pagina 101
- SNMP, pagina 102
- OPC UA, pagina 103
- Banner di sicurezza, pagina 105

I parametri configurabili per ogni nodo sono descritti di seguito.

Utilizzare queste impostazioni per configurare la sicurezza del dispositivo per il modulo BMENUA0100. Dopo aver modificato le impostazioni, selezionare **Invia** o **Annulla**.

Policy account utente

Utilizzare queste impostazioni per configurare i criteri dell'account utente:

Parametro	Descrizione
Inattività sessione max (minuti)	Periodo di timeout della sessione inattiva per le connessioni HTTPS. Se una connessione è inattiva per questo periodo, la sessione utente viene chiusa automaticamente. Impostazione predefinita = 15 minuti. **NOTA:** Non esiste un timeout del periodo di inattività per le connessioni OPC UA.
Tentativi di accesso max:	Numero di tentativi di accesso non riusciti consentiti. Impostazione predefinita = 5 tentativi. Quando si raggiunge il massimo configurato, l'account utente è bloccato.
Timer tentativi di accesso (minuti)	Il periodo di tempo massimo per l'accesso. Impostazione predefinita = 3 minuti.
Durata blocco account (minuti)	Periodo di tempo durante il quale non è possibile tentare ulteriori accessi dopo aver raggiunto il numero massimo di tentativi di accesso. Alla scadenza di questo periodo, un account utente bloccato viene sbloccato automaticamente. Impostazione predefinita = 4 minuti.

NOTA: queste impostazioni dei criteri dell'account utente si applicano ai client OPC UA, pagina 167 a cui è stato assegnato un nome utente.

Registri evento

Utilizzare queste impostazioni per configurare il client syslog che risiede nel modulo BMENUA0100. I registri sono memorizzati localmente nel modulo e scambiati con un server syslog, pagina 154 remoto:

Parametro	Descrizione
Attivazione servizio	Attiva e disattiva il servizio client syslog. Impostazione predefinita = disattivo.
Indirizzo IP server Syslog	Indirizzo IPv4 o IPv6 del server syslog remoto. **NOTA:** IPv6 è disponibile per la versione firmware 1.10 e successiva del modulo BMENUA0100.
Porta server Syslog	Il numero di porta utilizzato dal servizio client syslog. Valore predefinito = 601.

Attivazione servizi di rete

Questi servizi costituiscono un firewall che consente o nega il passaggio delle comunicazioni attraverso il modulo BMENUA0100. Utilizzare queste impostazioni per attivare o disattivare i servizi seguenti:

CRITERI GLOBALI:

Servizio	Descrizione
Sicurezza rinforzata	Disabilita i servizi di rete tranne IPsec.
Sblocca sicurezza	Abilita i servizi di rete tranne IPsec.

ATTIVAZIONE SERVIZI DI RETE: L'impostazione predefinita per i servizi seguenti dipende dalla modalità operativa di sicurezza informatica (CS Op Mode), come segue:

Servizio	Descrizione	CS Op Mode predefinita	
		Standard	Advanced (o Secured)
Agente SNMP	Attiva e disattiva le comunicazioni dell'agente SNMP.	Attivato	Disattivato
Server NTP	Attiva e disattiva le comunicazioni del server NTP.	Attivato	Disattivato
IPsec	Attiva e disattiva le comunicazioni IPsec.	Disattivato	Attivato[1]
Flussi dati da controller a controller[2, 3]	Attiva e disattiva le comunicazioni Modbus, passando attraverso il modulo BMENUA0100 tra i controller M580. Vedere *Configurazione della comunicazione per i flussi di dati da controller a controller*, pagina 98.	Attivato	Disattivato
Flussi di dati Control Expert solo nel controller[2, 3]	Attiva e disattiva le comunicazioni Modbus, EtherNet/IP, Ping, messaggistica esplicita e FTP, che passano per il modulo BMENUA0100, solo tra il software di configurazione Control Expert e il controller. Vedere *Configurazione della comunicazione per il flusso di dati Control Expert*, pagina 97.	Attivato	Disattivato
Flussi di dati Control Expert nella rete di dispositivi[2, 3]	Attiva e disattiva le comunicazioni Modbus, EtherNet/IP, Ping, messaggistica esplicita e FTP, che passano attraverso il modulo BMENUA0100, tra il software di configurazione Control Expert e i dispositivi di rete, compreso il controller. Vedere *Configurazione della comunicazione per il flusso di dati Control Expert*, pagina 97.	Attivato	Disattivato

Servizio	Descrizione	CS Op Mode predefinita	
		Standard	Advanced (o Secured)
HTTPS sulla porta di controllo	Attiva e disattiva le comunicazioni HTTPS sulla porta di controllo. **NOTA:** Se HTTPS è disattivato e la modifica applicata, non è possibile accedere alle pagine Web tramite la porta di controllo. Per ripristinare l'accesso alle pagine Web dalla porta di controllo, è possibile reimpostare la configurazione della sicurezza informatica.	Disattivato	Attivato
1. IPsec è abilitato senza regole definite. Il servizio deve essere configurato. 2. Per informazioni relative alla configurazione, vedere la sezione sulla risoluzione dei problemi Attivazione dei servizi di rete utilizzando solo una connessione IPv6, pagina 167. 3. Supportato solo dai moduli precedenti alla versione BMENUA0100.2, come indicato in EcoStruxure Control Expert.			

NOTA: i servizi SNMP, NTP, Syslog e Modbus non sono protocolli intrinsecamente sicuri. Vengono resi sicuri quando incapsulati in IPsec. Non disattivare IPsec se è attivato uno dei servizi SNMP, NTP, Modbus o Syslog.

Configurazione della comunicazione per il software remoto in esecuzione su PC (senza inoltro NAT)

Il software indirizza il dispositivo di destinazione (ad esempio, il controller M580) tramite l'indirizzo IP del dispositivo di destinazione. Per supportare questa comunicazione, impostare due gateway predefiniti, come segue:

- Sul PC host che esegue il software, con IPv4, impostare un gateway predefinito del PC sull'indirizzo IP della porta di controllo del modulo BMENUA0100.
- Sul dispositivo di destinazione (ad esempio il controller M580), con IPv4, impostare un gateway predefinito del dispositivo all'indirizzo IP della porta di controllo del modulo BMENUA0100.
- Sul PC host, aggiungere un instradamento con il comando seguente:

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

Per IPv4 in tutte le versioni firmware e per IPv6 nelle versioni firmware 1.10 e successive, le comunicazioni Modbus dalla schermata di connessione di Control Expert indirizzeranno l'indirizzo IP della porta di controllo BMENUA0100. I gateway non sono necessari per questa comunicazione.

Configurazione della comunicazione per i flussi di dati da controller a controller

Le comunicazioni Modbus TCP/IP da controller a controller tramite il modulo BMENUA0100 utilizzano l'indirizzo della porta di controllo IPv4 del modulo BMENUA0100 e non l'indirizzo del controller di destinazione.

NOTA:

- Per BMENUA0100, l'inoltro da controller a controller è limitato al protocollo Modbus TCP/IP.
- Il protocollo Modbus è l'unico che supporta la comunicazione tra dispositivi.
- Solo l'indirizzamento IPv4, e non IPv6, supporta i flussi di dati da controller Modbus TCP/IP a controller.

Inoltro del servizio (inoltro IP)

Questa pagina Web è inclusa in un modulo BMENUA0100 con versione firmware 2.01 o successiva. Utilizzarlo per configurare l'inoltro dei flussi di dati unicast che passano attraverso il modulo tra la rete di controllo e la rete di dispositivi. In questa pagina Web è possibile creare, modificare o rimuovere un elenco di regole di inoltro IP per il modulo .

NOTA: la funzionalità di inoltro del servizio (inoltro IP) non supporta le funzionalità seguenti

- Flussi di dati multicast.
- Messaggistica implicita EtherNet/IP.

Di conseguenza, questo servizio non supporta i task seguenti:

- Rilevamento dei dispositivi da parte dello strumento EcoStruxure Automation Device Maintenance (EADM) che funziona in modalità di rilevamento automatico. È supportato il rilevamento dispositivi EADM tramite la modalità di rilevamento manuale. (multicast).
- Inoltro dei messaggi ai moduli di comunicazione EtherNet/IP locali del controller (messaggistica implicita EtherNet/IP).

Caratteristiche:

Le caratteristiche principali della funzione di inoltro servizio/IP sono:

- Capacità di inoltrare tutti i flussi di dati ("Inoltra tutto").
- Inoltro IP dei protocolli più comuni utilizzati nell'architettura tramite modelli predefiniti (ad es. Modbus, HTTPS, SNMP, ...)
- Creazione e applicazione di modelli di inoltro IP personalizzati.

- Inoltro NAT (Network Address Translation) di alcuni protocolli al controller locale se l'indirizzo IP @remote è la porta di controllo IP V4 BMENUA0100

  NOTA: l'inoltro NAT si applica ai protocolli seguenti: Modbus, Modbus su TLS, EIP esplicito, EIP esplicito su TLS, EIP implicito, client OPC UA.

- La possibilità di utilizzare o meno IPsec per i protocolli inoltrati da NAT. Vedere le linee guida riportate nelle note alla fine della Sezione IPsec, di seguito, pagina 101.

NOTA:

- Se più moduli BMENUA0100 sono posizionati nello stesso rack, configurare solo un modulo BMENUA0100 con la funzione di inoltro.
- I flussi di dati multicast non vengono inoltrati.
- Un aggiornamento online delle regole di inoltro IP può causare l'interruzione di alcune comunicazioni in corso.
- Per il corretto inoltro del servizio (inoltro IP), la rete IP di destinazione deve essere diversa dalla rete IP di origine. Ad esempio, non è possibile eseguire l'inoltro IP tra:
  - Rete IP di origine 192.168.x.x (maschera 255.255.0.0) e
  - Rete IP di destinazione 192.168.x.x (maschera 255.255.0.0).
- Il valore della porta di ascolto OPC UA deve essere lo stesso per tutti i moduli BMENUA0100 che comunicano tra loro (ad esempio, nel caso di inoltro NAT OPC UA tra più moduli BMENUA0100.
- L'attivazione del protocollo FTP apre una serie di porte TCP, da 1024 a 65535. Di conseguenza, possono essere inoltrati anche altri protocolli con porte TCP in questo campo. Attivare l'inoltro del protocollo FTP solo temporaneamente e quando necessario.
  - L'attivazione del protocollo TFTP come regola personalizzata provoca lo stesso risultato dell'attivazione del protocollo FTP. Attivare l'inoltro del protocollo TFTP solo temporaneamente e quando necessario.

Per ulteriori informazioni sulle architetture di inoltro del servizio (IP), vedere i seguenti argomenti:

- Architetture supportate dal servizio di inoltro (IP), pagina 173
- Architetture non supportate dal servizio di inoltro (IP), pagina 176

Inoltro IP e comunicazione OPC UA

Inoltro IP e OPC UA sono in concorrenza per la larghezza di banda di comunicazione disponibile del modulo BMENUA0100. Per i risultati del test delle prestazioni che descrivono l'impatto dell'inoltro IP, delle comunicazioni OPC UA, delle impostazioni di riservatezza e delle regole personalizzate sulla larghezza di banda, vedere il capitolo Inoltro IP e comunicazione OPC UA, pagina 177.

Creazione di regole:

- Per documentare le regole predefinite e quelle personalizzate, fare clic su **Nuovo inoltro** e completare le impostazioni che definiscono tale regola.

  NOTA: quando si seleziona un nome di servizio, al numero di porta e al protocollo vengono assegnate automaticamente le impostazioni predefinite, modificabili in base alle esigenze.
- Per modificare una regola esistente, fare clic sull'icona della matita e modificarne le impostazioni.
- Per rimuovere una regola esistente, fare clic sull'icona del cestino.

Impostare **Inoltra tutto** su **OFF** per applicare le regole elencate. Se si imposta **Inoltra tutto** su **ON**:

- Le regole vengono sospese e il modulo inoltra tutti i protocolli;
- Non è possibile configurare l'inoltro per i singoli servizi e
- Tutti i servizi verranno inoltrati su IPsec, se IPsec è abilitato.

Ogni regola è definita dai campi seguenti:

Impostazione	Descrizione
Nome servizio	Sono predefiniti i servizi seguenti: • Modbus • FTP • EIP esplicito • ICMP • NTP / SNTP • SNMP • Trap SNMP • HTTPS • Modbus su TLS • EIP esplicito su TLS • LDAP avvia TLS • Syslog • HTTP • Metadati DPWS • OPC UA (per client OPC UA) • DNP3 • DNP3 su TLS • IEC 60870 • IEC 60870 su TLS • EIP implicito **NOTA:** per OPC UA, il numero di porta è la porta OPC UA impostata in Control Expert per il modulo BMENUA0100.
Numero porta[1]	La porta associata al servizio.

Impostazione	Descrizione
Protocollo[1]	Il protocollo associato al servizio.
Utilizzo di IPsec	• **TRUE**: il protocollo viene trasportato su IPsec. • **FALSE**: il protocollo non viene trasportato su IPsec, anche se IPsec è attivato nella configurazione. Questa selezione è disponibile solo quando IPsec è abilitato. **NOTA:** • **Non utilizzare** IPsec per protocolli protetti in modo nativo (ad esempio Modbus su TLS, EIP esplicito su TLS, DNP3 su TLS, EIP 60870 su TLS) • **Utilizzare** IPsec per protocolli non protetti in modo nativo (ad esempio Modbus, EIP esplicito, client OPC UA, EIP IO)
Interfaccia in ingresso	• **Porta di controllo**: se la richiesta client remota viene ricevuta sulla porta di controllo (ad esempio: richiesta Modbus TCP/IP da Control Expert). • **Porta backplane**: se la richiesta client remota viene ricevuta sulla porta backplane (ad esempio, richiesta Modbus TCP da un blocco funzione del controller). • **Entrambi**: se la richiesta del client remoto può essere ricevuta sulla porta di controllo e su quella backplane (ad esempio: richiesta Modbus TCP/IP da Control Expert e richiesta Modbus TCP da un blocco funzione del controller).
1. Compilazione automatica, ma modificabile, per un nome di servizi predefinito.	

IPsec

Utilizzare IPsec per proteggere la comunicazione Ethernet IPv4.

NOTA: IPsec non supporta l'indirizzamento IPv6.

Utilizzare queste impostazioni per configurare un massimo di 8 canali IKE / IPsec su IPv4 per il modulo BMENUA0100. Se sono configurati più di 4 collegamenti IPsec, la connessione automatica al controller dopo il trasferimento attraverso il BMENUA0100 potrebbe non riuscire. In questo caso, collegarsi al controller manualmente.

Parametro	Descrizione
SERVIZIO IPsec	• ON: abilita il servizio IPsec. **NOTA:** Come condizione preliminare per l'abilitazione del servizio IPsec, è inoltre necessario attivare la Porta di controllo nelle impostazioni IPConfig, pagina 118. • OFF: disabilita il servizio IPsec.
NTP autorizzato al di fuori di IPsec	• Deselezionato (disattivato): NTP viene scambiato solo tramite IPsec. • Selezionato (attivato): NTP viene scambiato tramite IPsec se il canale IPsec è aperto e al di fuori di IPsec se il canale IPsec non è aperto.

Parametro	Descrizione
Nuovo collegamento	Crea un nuovo canale IKE / IPsec e lo aggiunge all'elenco per la modifica. **NOTA:** sono supportati un massimo di 8 canali IKE / IPsec.
Per ogni canale IKE / IPsec, configurare le impostazioni seguenti:	
Indirizzo IP remoto	Indirizzo IPv4 dell'endpoint IPsec remoto. **NOTA:** il dispositivo remoto deve essere accessibile dalla porta di controllo BMENUA0100 (e non dalla porta backplane BMENUA0100).
Confidenzialità	• Selezionato: la comunicazione verrà crittografata. • Deselezionato: nessuna crittografia. **NOTA:** la confidenzialità è disabilitata se è attivato *NTP senza IPsec*.
Tipo di client	Tipo dell'endpoint IPsec remoto: Windows o Dispositivo. **NOTA:** l'impostazione predefinita è Windows. Verificare che il tipo di endpoint configurato corrisponda al client.
PSK	Una chiave precondivisa della lunghezza di 32 caratteri esadecimali è il risultato di un numero casuale generato dal modulo BMENUA0100. Può essere copiato e modificato in questa pagina Web. **NOTA:** PSK è disattivato se è attivato *NTP senza IPsec*.

NOTA: configurare le impostazioni del firewall Windows, pagina 179 scaricando lo "script Windows" da BMENUA0100 mediante il comando **Scarica script** per ogni indirizzo IP remoto. Se l'impostazione **Utilizzo IPsec** viene modificata per alcuni protocolli, lo script Windows deve essere nuovamente scaricato dal modulo BMENUA0100 ed eseguito su Windows. Per un esempio di script Windows, vedere l'argomento Script Windows IPsec, pagina 179.

NOTA: se sono configurati 8 tunnel IPsec, potrebbe non essere possibile ricollegarsi automaticamente al controller dopo il download di un'applicazione. In questo caso, ricollegarsi manualmente al controller dopo il download.

NOTA: Se il servizio IPsec è attivato (ovvero impostato su ON):

- Il flusso di dati del server HTTPS locale esce da IPsec.
- Il flusso di dati OPC UA locale viene trasportato per impostazione predefinita all'interno di IPsec. Per poter trasportare il flusso di dati OPC UA locale fuori da IPsec, è necessario impostare una regola di inoltro OPC UA con "Utilizzo IPsec = FALSE", anche se non è necessario inoltrare il flusso di dati OPC UA.

SNMP

Utilizzare queste impostazioni per configurare la versione SNMP e le relative impostazioni.

NOTA: in modalità Advanced (o Secured), la versione SNMP deve essere configurata in modo uguale in Control Expert, pagina 130 e nella pagina Web SNMP. Se queste impostazioni non sono uguali, il servizio SNMP non si avvia.

Parametro	Descrizione
Versione SNMP	• v1 • v3
Livello di sicurezza	Per SNMP v1 e v3: • senza autorizzazione né privacy: comunicazione senza autenticazione o privacy. **NOTA:** Per SNMP v1, questa è l'unica impostazione disponibile. Solo per SNMP v3: • autorizzazione senza privacy: comunicazione con autenticazione ma senza privacy. Il protocollo di autenticazione è SHA (Secure Hash Algorithm). • autorizzazione privacy: comunicazione con autenticazione e privacy. I protocolli utilizzati sono: ◦ Autenticazione: SHA. ◦ Privacy: AES (Advanced Encryption Standard).
Password di autenticazione	Se l'autenticazione è attivata, immettere una password di autenticazione che distingue tra maiuscole e minuscole. Può contenere da 8 a 12 caratteri e può includere caratteri alfanumerici (lettere maiuscole, lettere minuscole e numeri) come indicato nella descrizione comandi della pagina Web.
Password privacy	Se la privacy è attivata, immettere una password per la privacy che distingue tra maiuscole e minuscole. Deve contenere 8 caratteri e può includere caratteri alfanumerici (lettere maiuscole, lettere minuscole e numeri) come indicato nella descrizione comandi della pagina Web.

OPC UA

Utilizzare queste impostazioni per configurare la connessione per il server OPC UA integrato nel modulo BMENUA0100:

Parametro	Descrizione
Modalità Sicurezza messaggio	• Firma e codifica (predefinito): a ogni messaggio viene assegnata una firma ed è crittografato. • Firma: a ogni messaggio viene applicata una firma. • Nessuno: nessun criterio di sicurezza applicato. In questo caso, i due campi seguenti sono disattivati. **NOTA:** se si seleziona **Nessuno**, il **Tipo token identificativo utente** nel modulo BMENUA0100 è definito come **Anonimo**. In questo caso, occorre anche configurare il tipo di token identificativo utente nel client OPC UA su **Anonimo**.
Policy di sicurezza	• Basic256Sha256 (predefinito): definisce un criterio di sicurezza per le configurazioni con un gruppo di crittografia valido. • Basic256: definisce un criterio di sicurezza per le configurazioni con un gruppo di crittografia obsoleto. **NOTA:** questa selezione non viene utilizzata a meno che non sia necessario per l'interoperabilità con il client remoto. • Basic128Rsa15: definisce un criterio di sicurezza per le configurazioni con un gruppo di crittografia obsoleto. **NOTA:** questa selezione non viene utilizzata a meno che non sia necessario per l'interoperabilità con il client remoto.
Tipi di token identificativo utente	• Anonimo: nessuna informazione utente disponibile. • Nome utente (predefinito): l'utente è identificato da nome utente e password.

NOTA: le modifiche della configurazione di sicurezza informatica alle impostazioni del server OPC UA provocano il riavvio del server e l'applicazione delle nuove impostazioni. Di conseguenza, se una o più sessioni OPC UA esistono quando vengono apportate modifiche alla configurazione, queste sessioni vengono sospese. Alla scadenza del periodo *SessionTimeout*, queste sessioni vengono chiuse. *SessionTimeout* fa parte della configurazione del client OPC UA SCADA.

NOTA: quando l'impostazione **Modalità sicurezza messaggio** del server OPC UA è inizialmente configurata per **Firma e codifica** o **Firma** e un client OPC UA stabilisce una connessione, se successivamente si configura l'impostazione **Modalità sicurezza messaggio** del server OPC UA su **Nessuno**, un client OPC UA (con anche l'impostazione **Modalità sicurezza messaggio** configurata su **Nessuno**) non è in grado di stabilire una connessione al server.

Per ristabilire una connessione:

1. Scollegare i client OPC UA.
2. Modificare la configurazione OPC UA nella pagina Web di BMENUA0100.
3. Attendere che il LED **BUSY** sia acceso (giallo) e poi si spenga (non illuminato).
4. Per i client OPC UA, modificarne la configurazione (**Modalità sicurezza messaggio**) con la stessa impostazione utilizzata per il server OPC UA.
5. Ricollegare i client OPC UA al server.

Banner di sicurezza

Questa pagina contiene il testo modificabile visualizzato quando un utente accede alle pagine Web del modulo BMENUA0100:

Parametro	Descrizione
Testo banner	Stringa di massimo 128 caratteri visualizzata a un utente nella pagina di accesso. Per impostazione predefinita viene visualizzato il seguente testo modificabile: "L'uso non autorizzato del sistema è proibito e soggetto a sanzioni penali e/o civili."

Gestione certificati

Gestione dei certificati con e senza PKI

Il modulo BMENUA0100 si basa su certificati per l'autenticazione. Per garantire la sicurezza informatica, ogni entità (inclusi i client OPC UA e il server OPC UA integrato nel BMENUA0100) deve gestire un elenco di attendibilità di tutti i certificati di dispositivi/applicazioni che comunicano con esso.

Il metodo di gestione dei certificati dipende dalla progettazione del sistema, che può applicare o meno un'infrastruttura a chiave pubblica (PKI) con un'autorità di certificazione (CA).

Gestione certificato senza PKI:

utilizzare questo metodo di gestione dei certificati se il sistema non include una CA. Questo metodo di gestione è supportato dai moduli BMENUA0100 con firmware v1.0 e versioni successive. Gestire i certificati nella pagine Web **Gestione certificati** come indicato di seguito:

- Impostare la **Modalità PKI** su **Solo autofirmato**.
- Gestire l'**Elenco di certificati attendibili** utilizzando le funzioni **Aggiungi** ed **Elimina** per creare un elenco di client OPC UA autorizzati a comunicare con il modulo BMENUA0100.
- Esportare il certificato del modulo BMENUA0100 nei dispositivi client OPC UA tramite il comando **Download** nella pagina **Configurazione PKI > Certificato dispositivo**.

Gestione certificato con PKI:

utilizzare questo metodo di gestione dei certificati se il sistema include una CA. Questo metodo di gestione è supportato dai moduli BMENUA0100 con firmware v1.1 e versioni successive. Gestire i certificati nella pagine Web **Gestione certificati** come indicato di seguito:

- Impostare la **Modalità PKI** su:
  - **Solo CA**: se tutti i dispositivi client OPC UA installati supportano PKI.
  - **Autofirmato e CA**: se alcuni dei dispositivi client OPC UA installati non supportano PKI.
- Se la **Modalità PKI** è impostata su **Solo CA**:
  - Registrare manualmente , pagina 110 ogni modulo BMENUA0100 con la CA.
- Se la **Modalità PKI** è impostata su **Autofirmato e CA**:
  - Registrare manualmente , pagina 110 ogni modulo BMENUA0100 con la CA.
  - Gestire l'**Elenco di certificati attendibili** utilizzando le funzioni **Aggiungi** ed **Elimina** per creare un elenco di client OPC UA autorizzati a comunicare con il modulo BMENUA0100.

Aggiornamento dell'elenco dei certificati attendibili

Dopo la prima installazione di BMENUA0100 versione firmware 2.0 (BMENUA0100.2) o versione successiva, è necessario rimuovere i certificati aggiunti dall'**elenco dei certificati attendibili** nella pagina Web **Gestione certificati**. A tale scopo:

- Rimuovere manualmente questi certificati utilizzando il comando **Elimina** oppure
- Impostare il selettore a rotazione di sicurezza informatica alla posizione **Cybersecurity Reset**.

Dopo aver cancellato l'**elenco dei certificati attendibili**, è possibile ricompilarlo con certificati autofirmati o certificati rilasciati dalla CA.

Questa attività deve essere eseguita solo alla prima installazione del firmware versione 2.0 o successiva. Non è necessario ripetere la procedura per le installazioni successive di versioni firmware superiori.

NOTA: se non si cancella l'**elenco dei certificati attendibili**, come descritto in precedenza, le connessioni con i client OPC UA non possono essere stabilite o, se stabilite, verranno eliminate.

Panoramica autenticazione

Un client OPC UA o un modulo BMENUA0100 possono essere autenticati in tre modi:

- Per la versione firmware 1.0 e successive:
  - Certificato autofirmato (solo)
- Per la versione firmware 1.10 e successive:
  - Certificato PKI rilasciato solo da un'autorità di certificazione (CA) di terze parti
  - Certificato PKI rilasciato da una CA e un certificato autofirmato

Per fornire il livello richiesto di sicurezza informatica, ogni entità (client OPC UA BMENUA0100) deve gestire un elenco di attendibilità di tutti i certificati di dispositivi/applicazioni che comunicano con essa.

Per la versione firmware 1.10 e successive, il modulo BMENUA0100 crea un certificato autofirmato per:

- Configurazione delle impostazioni di sicurezza informatica tramite le pagine Web del modulo
- Diagnostica del modulo tramite le relative pagine Web
- Aggiornamento firmware
- Certificati di istanza dell'applicazione OPC UA per consentire ai client OPC UA di accedere al server OPC UA integrato nel modulo BMENUA0100.

Per la versione firmware 1.0, il modulo crea due certificati: un certificato HTTPS e un certificato OPC UA.

NOTA:

- Le date di scadenza dei certificati attendibili vengono eseguite in riferimento alle impostazioni interne di data e ora del modulo BMENUA0100. Per evitare incoerenze, utilizzare il servizio NTP per aggiornare le impostazioni di data e ora del modulo BMENUA0100 e verificare che il server NTP sia accessibile e disponga di impostazioni aggiornate di data e ora.
- Se si riceve un errore rilevato di *certificato errato per nome host non valido* durante il tentativo di connettere il client OPC UA al server BMENUA0100 in IPv6, la causa potrebbe essere un indirizzo IPv6 compresso (ad esempio un indirizzo IPv6 abbreviato). In questo caso verificare l'indirizzo IPv6 utilizzato e, se necessario, sostituirlo con un formato non compresso.
- Il modulo BMENUA0100 non gestisce automaticamente le date di scadenza dei certificati. È necessario gestire manualmente le date di scadenza del certificato.

Gestione dei certificati

Nelle pagine Web del modulo BMENUA0100, a partire dalla pagina **Home**, selezionare **Gestione certificati** per visualizzare i collegamenti alle seguenti pagine di gestione certificati dell'istanza di applicazione:

- Configurazione PKI, pagina 109
- Gestione elenco attendibili client, pagina 111
- Esportazione certificati dispositivo, pagina 112
- Registrazione manuale, pagina 110
- Certificati CA, pagina 112

Vedere le sezioni *Uso di GPO/LGPO*, pagina 166 e *Applicazione della gestione dei criteri di gruppo MMC*, pagina 167 per informazioni sugli strumenti di Windows™ utilizzabili per gestire i certificati.

Estensioni certificato

Per supportare la comunicazione con il modulo BMENUA0100, i certificati autofirmati e CA devono includere estensioni specifiche, come indicato di seguito:

Certificati autofirmati:

- UsoChiave (contrassegnato come critico):
  - FirmaDigitale
  - CifraturaChiave (nessun utilizzo per suite TLS basato su chiavi effimere come TLS_ECDHE_xxxx; uso per TLS_RSA_xxxx)
  - KeyCertSign: quando la chiave pubblica oggetto viene utilizzata per verificare le firme nei certificati di chiave pubblica (valore TRUE)
  - nonRepudiation (richiesto dallo standard OPC UA)
  - dataEncipherment (richiesto dallo standard OPC UA)
- Subject Alt Name: nel campo NAO è possibile specificare i seguenti valori: indirizzo IP V4/V6, URI
- Vincoli di base:
  - Campo cA: se la chiave pubblica certificata può essere utilizzata per verificare le firme dei certificati (Valore TRUE) e pathLenConstraint=0
- Identificatore chiave soggetto
  - mezzo per identificare i certificati che contengono un particolare hash SHA-1 a 160 bit pubblico del valore di BIT STRING subjectPublicKey (eccetto tag, lunghezza e numero di bit non utilizzati).
- Estensione uso chiave estesa:
  - id-kp-serverAuth se autenticazione server Web TLS
  - id-kp-clientAuth se autenticazione client Web TLS

Certificati CA:

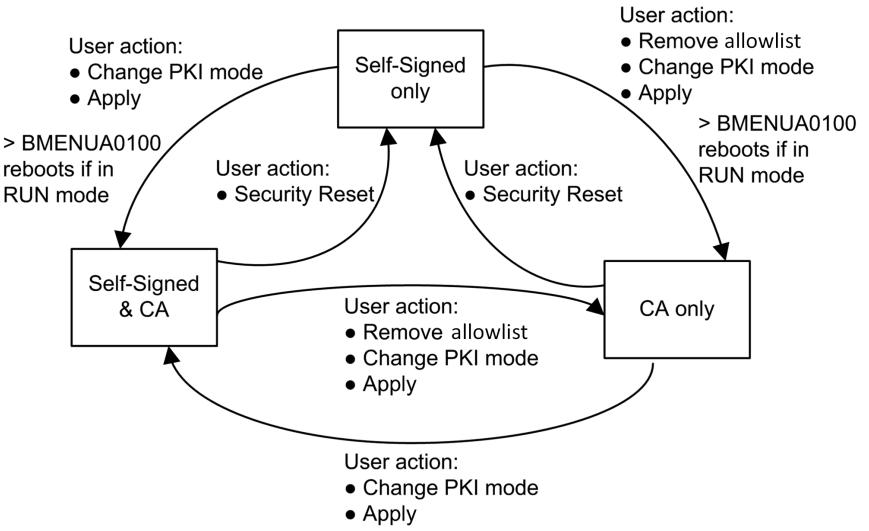
- UsoChiave (contrassegnato come critico):
  - FirmaDigitale
  - CifraturaChiave (nessun utilizzo per suite TLS basato su chiavi effimere come TLS_ECDHE_xxxx; uso per TLS_RSA_xxxx)
  - KeyCertSign: quando si utilizza la chiave pubblica oggetto per verificare le firme nei certificati di chiave pubblica (valore FALSE)
  - nonRepudiation (richiesto dallo standard OPC UA)
  - dataEncipherment (richiesto dallo standard OPC UA)
- Subject Alt Name: nel campo NAO è possibile specificare i seguenti valori: indirizzo IP V4/V6, URI
- Vincoli di base:
  - Campo cA: se la chiave pubblica certificata può essere utilizzata per verificare le firme dei certificati (valore FALSE)
- Estensione uso chiave estesa:
  - id-kp-serverAuth se autenticazione server Web TLS
  - id-kp-clientAuth se autenticazione client Web TLS
- Punti di distribuzione CRL
- Identificatore chiave di autorità
  - Identificazione della chiave pubblica corrispondente alla chiave privata utilizzata per firmare un certificato.

Configurazione PKI

Utilizzare la pagina **Configurazione PKI** per specificare i tipi di certificati accettati dal server OPC UA integrato nel modulo, tra cui:

Modalità PKI	**Descrizione**
Solo autofirmato	È necessario gestire solo i certificati nell'elenco dei **certificati client attendibili**.
Solo CA	Tutti i dispositivi di sistema richiedono certificati firmati da una CA.
Autofirmato e CA	I certificati sono gestiti come segue: • Il certificato per il modulo BMENUA0100 con versione firmware 1.10 e successive è rilasciato da una CA. • I certificati per i dispositivi client che supportano PKI sono rilasciati da una CA. • I certificati per i dispositivi client che non supportano PKI sono autofirmati.

Lo schema seguente illustra le azioni e gli eventi utente correlati alla modifica dell'impostazione della modalità PKI:



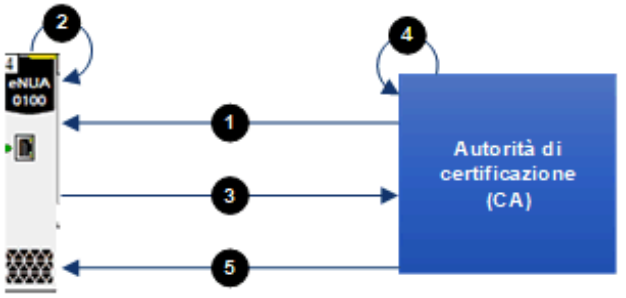
Registrazione manuale

Dopo aver configurato il modulo BMENUA0100 in Control Expert, è possibile utilizzare la pagina **Registrazione manuale** per ottenere (**get**) un file CSR da inviare a una CA. Dopo aver inviato il file CSR, è possibile estrarre il certificato CA corrispondente. In seguito, è possibile inserire (**Push**) questo certificato CA nel modulo BMENUA0100. Le operazioni combinate **Get** e **Push** registrano manualmente un certificato emesso da una CA di terze parti. Dopo aver spostato il certificato, il server OPC UA applica questo certificato allo scopo di firmare e crittografare la comunicazione con il client OPC UA.

NOTA: come condizione preliminare per eseguire la registrazione manuale:

- Verificare che il client NTP sia abilitato, pagina 127.
- Verificare che l'impostazione dell'ora per il modulo BMENUA0100 sia corretta.

Di seguito viene riportata una panoramica del processo di registrazione manuale dei certificati:



1 BMENUA0100 importa un certificato CA dall'autorità di certificazione (CA)

2 BMENUA0100 genera una richiesta di firma del certificato (CSR)

3 BMENUA0100 esporta la RSI nella CA

4 La CA esegue la CSR e genera un certificato

5 BMENUA0100 importa il certificato dalla CA

Vedere il video di Schneider Electric "How to work with PKI mode "Self-Signed & CA" on BMENUA0100 module?" (Come lavorare con la modalità PKI "Autofirmato e CA" sul modulo BMENUA0100?) all'indirizzo https://www.se.com/us/en/faqs/FAQ000191153/.

Gestione elenco attendibili client

Solo i client OPC UA che hanno fornito al modulo BMENUA0100 un certificato di istanza dell'applicazione possono comunicare con il server OPC UA integrato nel modulo. Il modulo implementa la gestione locale (basata su modulo) dei certificati dell'istanza dell'applicazione OPC UA, memorizzati in un elenco di attendibilità. Utilizzare i comandi delle pagine Web **Gestione certificati** per **aggiungere**, **scaricare** o **eliminare** un certificato.

NOTA: i certificati dell'elenco di attendibilità delle istanze dell'applicazione OPC UA sono codificati in ANSI CRT.

Per aggiungere un certificato all'elenco:

Passo	Azione
1	Scegliere **Aggiungi** dal menu di gestione elenco attendibili.
2	Fare clic su **Sfoglia**, quindi spostarsi e selezionare il certificato da aggiungere all'elenco.
3	Fare clic su **Invia** per aggiungere il certificato.
4	Fare clic su **Applica** per salvare la modifica alla configurazione.

Per rimuovere un certificato dall'elenco:

Passo	Azione
1	Nell'elenco attendibili, fare clic sul certificato da rimuovere
2	Selezionare **Elimina**.
3	Fare clic su **Sì** per rimuovere il certificato dall'elenco.
4	Fare clic su **Applica** per salvare la modifica alla configurazione.

Esportazione certificati dispositivo

È possibile esportare il certificato del modulo BMENUA0100 per HTTPS e OPC UA nella pagina **GESTIONE CERTIFICATI > CONFIGURAZIONE PKI** facendo clic sul pulsante **Download**

Certificati CA

Il certificato CA è un certificato a chiave pubblica che identifica l'autorità di certificazione (CA) in un'infrastruttura a chiave pubblica (PKI). Utilizzare la pagina **Certificati CA** per aggiungere i certificati CA nel dispositivo.

Per aggiungere un certificato dalla CA all'elenco Certificati CA:

Passo	Azione
1	Aprire le pagine Web del modulo e nella finestra di dialogo **Login** immettere: • nome utente • password Fare clic su **Login**.
2	Passare a **CONFIGURAZIONE SICUREZZA INFORMATICA > GESTIONE CERTIFICATI** per accedere alla scheda gestione certificati, quinfi selezionare **Certificati CA**.
3	Nell'elenco **CERTIFICATI ATTENDIBILI**, fare clic su **AGGIUNGI** per aggiungere il certificato CA all'elenco.
4	Applicare le modifiche alla configurazione della sicurezza informatica.

NOTA: è possibile aggiungere un massimo di dieci certificati CA.

Controllo accesso

Introduzione

Il modulo BMENUA0100 supporta l'autenticazione locale degli utenti basata sull'uso di combinazioni di nome utente/password per:

- configurazione delle impostazioni di sicurezza informatica del modulo tramite HTTPS
- download del firmware tramite HTTPS
- diagnostica della pagina Web del modulo tramite HTTPS

NOTA: solo un utente con ruolo di Amministratore di sicurezza può creare, modificare o eliminare gli account utente.

Le pagine Web del modulo BMENUA0100 contengono strumenti per la gestione degli account utente. Dalla pagina **Home**, fare clic su **Controllo di accesso** per visualizzare un elenco degli account utente OPC UA esistenti, inclusi i relativi ruoli e autorizzazioni. In questa pagina è possibile:

- Creare un account utente, pagina 114.
- Aggiornare il profilo, pagina 114 di un account utente esistente.
- Eliminare, pagina 115 un account utente.

Gestione utente

Il modulo BMENUA0100 fornisce controllo di accesso basato su ruolo (RBAC). A tutti gli account utente è assegnato un ruolo ed è consentita l'esecuzione delle sole attività associate a tale ruolo.

Sono supportati i seguenti ruoli e autorizzazioni:

Ruolo	**Autorizzazioni**			
	Configurazione sicurezza informatica (Cybersecurity)	**Aggiornamento del firmware**	**Accesso pagina Web diagnostica**	**Accesso protocollo OPC UA**
SECADM	Aggiornamento, Lettura, Scrittura	–	Lettura	–
OPERATORE	–	–	Lettura	Connessione
TECNICO	–	–	Lettura	Connessione
INSTALLATORE	–	Aggiornamento	Lettura	–

Ogni modulo BMENUA0100 supporta fino a 15 utenti contemporanei.

Non è possibile configurare ruoli personalizzati o set di autorizzazioni personalizzate. Non è possibile configurare elenchi di autorizzazione di controllo di accesso basati su indirizzo IP.

Creazione di un account utente

L'Amministratore di sicurezza può fare clic su **Nuovo utente**, quindi specificare i seguenti parametri per creare un nuovo account utente:

Parametro	Descrizione
Nome utente	L'ID dell'utente. L'utente deve inserirlo insieme alla password per accedere alle funzioni consentite.
Password Conferma password	La password dell'utente. La password non viene visualizzata in testo leggibile. Immettere questo valore due volte per confermarne la precisione. **NOTA:** le password devono contenere almeno 8 caratteri di cui almeno uno dei seguenti: • una lettera maiuscola (A...Z) • una lettera minuscola (a...z) • una cifra su base 10 (0...9) • un carattere speciale ~ ! @ $ % ^ & * _ + - = ` | \ ( ) [ ] : " ' < >
Ruoli	Selezionare il ruolo che definirà le autorizzazioni concesse all'utente: • Amministratore di sicurezza • Operatore • Tecnico • Installatore

Fare clic su **Applica modifiche** dopo aver configurato questi parametri per creare l'account utente.

Aggiornamento di un account utente

Per modificare le impostazioni di un account utente, un Amministratore di sicurezza può fare clic sull'icona di modifica (matita) per il profilo che si desidera modificare. Fare clic su **Applica modifiche** per salvare le modifiche. Viene visualizzata la stessa finestra di dialogo utilizzata per creare un account utente, che consente di aggiornare alcuni o tutti i parametri dell'account utente selezionato.

Eliminazione di un account utente

Per eliminare un account utente esistente, un Amministratore di sicurezza può fare clic con il pulsante destro del mouse sull'account utente nell'elenco e in **Elimina utente** fare clic su **OK**.

Gestione della configurazione

Introduzione

Per facilitare la configurazione del sistema, è possibile esportare le impostazioni di sicurezza informatica di un modulo BMENUA0100 configurato e importarle in un altro modulo. Nelle pagine Web del modulo BMENUA0100, dalla **Home** page, selezionare **Gestione della configurazione** per visualizzare i collegamenti alle seguenti pagine di gestione della configurazione della sicurezza informatica:

- ESPORTA, pagina 115
- IMPORTA, pagina 116
- RESET, pagina 116

NOTA: solo un amministratore di sicurezza, con il ruolo SECADM, può eseguire le attività di gestione della configurazione descritte in questa sezione.

Esportazione di una configurazione

Utilizzare la pagina **ESPORTA** per esportare il file di configurazione della sicurezza informatica del modulo BMENUA0100 locale. Il file di configurazione esportato è crittografato con la password assegnata in questa pagina. È possibile archiviare e riutilizzare un file di configurazione esportato.

Per esportare il file di configurazione della sicurezza informatica del modulo BMENUA0100 locale:

Passo	Descrizione
1	Nella pagina **ESPORTA**, assegnare al file di configurazione una **Password**. **NOTA:** La password deve contenere almeno 16 caratteri e rispettare le stesse regole utilizzate per la creazione delle password utente, pagina 114.
2	Reinserire la password assegnata nel campo **Conferma password**.
3	Fare clic su **Download**.

NOTA: Il file di configurazione viene prodotto con il nome: Mx80_xx_BMENUA.cfg, dove "xx" indica il numero di slot occupato dal modulo nel rack.

Importazione di una configurazione

Utilizzare la pagina **IMPORTA** per importare un file di configurazione di sicurezza informatica e applicarlo al modulo BMENUA0100 locale. Le impostazioni di sicurezza informatica applicate con questo comando sostituiscono quelle esistenti del modulo.

Per importare un file di configurazione di sicurezza informatica e applicarlo al modulo BMENUA0100 locale:

Passo	Descrizione
1	Nella pagina **IMPORTA**, fare clic sull'icona del file per aprire una finestra in cui è possibile selezionare un **Archivio di configurazione**.
2	Selezionare il file di configurazione che si desidera importare e fare clic su **OK**.
3	Nella pagina **IMPORTA**, immettere la **Password** del file di configurazione assegnata al file al momento dell'esportazione. **NOTA:** è possibile eventualmente selezionare **Salva** per applicare automaticamente la configurazione importata subito dopo averla caricata.
4	Fare clic su **Carica**. Si apre una finestra di dialogo che informa della chiusura della sessione. La configurazione è stata caricata sul server.
5	Fare clic su **Ricollega** per chiudere la finestra di dialogo e aprire la schermata di accesso, pagina 89.
6	Immettere nome utente e password dell'amministratore di sicurezza e fare clic su **Login**. Si apre la Home page. Se al passo 3 non è stato selezionato **Salva**, il banner indica l'esistenza di una configurazione in sospeso.
7	Nel banner, fare clic su **Applica**, quindi su **Sì** per confermare che si desidera applicare la configurazione in sospeso. La nuova configurazione viene applicata. **NOTA:** se in precedenza è stato selezionato **Salva** nella pagina **IMPORTA** (come indicato al passo 3 precedente) la configurazione viene applicata automaticamente e questo passo 7 viene eseguito automaticamente.

Ripristino di una configurazione

Fare clic su **Reset** nella pagina **RESET** per ripristinare le impostazioni di sicurezza informatica predefinite al modulo BMENUA0100 locale. Questa azione ha lo stesso effetto dell'impostazione del selettore a rotazione sulla posizione Cybersecurity (or Security) Reset, pagina 31. Dopo aver completato il reset, è necessario eseguire un riavvio del modulo.

Configurazione del BMENUA0100 in Control Expert

Introduzione

Questa sezione descrive come configurare le impostazioni dell'indirizzo IP, il client NTPv4 e l'agente SNMPv1 per il modulo di comunicazione BMENUA0100 Ethernet con il server OPC UA integrato.

Configurazione delle impostazioni dell'indirizzo IP

Introduzione

Il modulo di comunicazione Ethernet BMENUA0100 con server OPC UA integrato comprende due porte Ethernet:

- la porta di controllo posta sulla parte anteriore del modulo;
- una porta backplane che collega il modulo al backplane Ethernet del rack principale.

La porta di controllo può essere attivata o disattivata ed è attivata per impostazione predefinita. La porta backplane è sempre attivata.

Le impostazioni dell'indirizzo IP statico per la porta di controllo e la porta backplane possono essere configurate nella scheda **IPConfig** della finestra di dialogo di configurazione di BMENUA0100. Inoltre, è possibile assegnare dinamicamente le impostazioni dell'indirizzo IP alla porta di controllo tramite il metodo di configurazione automatica dell'indirizzo Stateless (SLAAC) di DHCP.

Quando si utilizza il modulo BMENUA0100 con un controller standalone, le impostazioni dell'indirizzo IP sono configurate per un modulo. Quando si utilizzano due istanze del modulo BMENUA0100 in un'architettura di controller Hot Standby (un modulo BMENUA0100 in ogni controller), la scheda di configurazione **IPConfig** di Control Expert contiene le impostazioni per due moduli (A e B). In un'architettura di controller Hot Standby, l'indirizzo IP di ogni modulo può essere in sottoreti diverse.

Supporto stack IPv4 e IPv6

È possibile configurare la porta di controllo in modo da supportare gli stack IP (ognuno dei quali consiste in una raccolta di protocolli di abilitazione Internet) come indicato di seguito:

- Stack IPv4: supporta solo l'indirizzamento a 32 bit. Un esempio di indirizzo IP IPv4 è: 192.168.1.2.

- Stack doppio IPv4/IPv6: supporta l'indirizzamento a 32 bit e a 128 bit. Quando sono configurati entrambi gli stack IPv4 e IPv6, la porta di controllo può ricevere e gestire pacchetti IPv4 e IPv6. Un esempio di indirizzo IPv6 a 128 bit è: 2001:0578:0123:4567:89AB:CDEF:0123:4567.

  NOTA:

  All'accensione iniziale (o dopo aver posizionato il selettore a rotazione del modulo su **Cybersecurity (o Security) Reset**, acceso, quindi riposizionato su **Modalità Advanced (o Secured)**, quindi riacceso), alla porta di controllo viene assegnato un indirizzo IPv4 predefinito 10.10.MAC5.MAC6, dove MAC5 è il valore decimale del 5° byte dell'indirizzo MAC del modulo e MAC6 è il valore decimale del 6° byte.

  Se gli ultimi due byte dell'indirizzo MAC (*MAC5.MAC6*) corrispondono a *0,0* nell'indirizzo predefinito, effettuare una connessione via cavo punto a punto tra il computer e il controller, il modulo di comunicazione o un altro modulo.

  L'indirizzo MAC del modulo è indicato sul lato anteriore.

IPv6 tramite la porta di controllo

La comunicazione IPv6 è supportata solo tramite la porta di controllo.

NOTA: Il flusso di Control Expert può essere configurato per essere instradato a un controller M580. Control Expert V15 e successivi può essere collegato a un controller M580 tramite l'indirizzo IPv6 BMENUA0100.

Configurazione degli indirizzi IP

Configurare l'indirizzamento IP in Control Expert, come indicato di seguito:

Passo	Azione
1	Nel **Browser di progetto**, espandere il nodo **Bus PLC** e aprire la finestra di dialogo di configurazione del modulo BMENUA0100.
2	Fare clic sulla scheda **IPConfig**.
3	Immettere le modifiche nei campi appropriati nella pagina di configurazione **IPConfig**. (La tabella seguente descrive i parametri della pagina di configurazione.)

Parametri configurabili

Configurare questi parametri di indirizzo IP per ciascun modulo di comunicazione BMENUA0100 nel progetto:

Parametro		Descrizione
Porta controllo		Attiva/disattiva la porta di controllo del modulo BMENUA0100. Quando impostata su: • Attivata: la porta di controllo è l'interfaccia esclusiva per la comunicazione IPv4 o IPv6 al server OPC UA integrato. • Disattivata (predefinito): la porta backplane Ethernet può supportare la comunicazione IPv4 con il server OPC UA.
Configurazione della porta di controllo IPv6		
	IPv6	Attiva/disattiva l'indirizzamento IPv6 per la porta di controllo quando la porta di controllo è abilitata. Impostazione predefinita = disattivato.
	Modalità	Identifica l'origine dell'indirizzo IPv6: • SLAAC: Indica che l'indirizzo IP IPv6 verrà servito alla porta di controllo da un server DHCP mediante il metodo SLAAC. • Statico (predefinito): attiva il campo IPv6@ per l'immissione di un indirizzo IPv6 statico.
	IPv6 @	Se si seleziona **Statico** come **Modalità**, sopra, immettere un indirizzo IPv6 valido per la porta di controllo. **NOTA:** • Il BMENUA0100 non è in grado di rilevare indirizzi IPv6 duplicati. Verificare con l'amministratore di rete per accertare che non vi siano indirizzi IPv6 duplicati nello stesso segmento di rete. • Il BMENUA0100 accetta, ma non può utilizzare, indirizzi IPv6 errati.
	Lunghezza prefisso sottorete	Impostata automaticamente per l'indirizzo IPv6 statico, che rappresenta il numero di bit dell'indirizzo IPv6 assegnato da SLAAC che definisce il prefisso di rete della sottorete. (predefinito = 64).
Configurazione della porta di controllo IPv4		

Parametro		Descrizione
	IPv4	Attiva/disattiva l'indirizzamento IP IPv4 per la porta di controllo quando la porta di controllo è abilitata. Valore predefinito = attivato.
	Modalità	Identifica l'origine dell'indirizzo IPv4: • Predefinito: il software assegna automaticamente un indirizzo IP. • Statico (predefinito): abilita i campi **IPv4 @**, **Subnet mask**, e **Gateway predefinito** per l'immissione di un indirizzo IP IPv4 statico per la porta di controllo.
	IPv4 @	Se la modalità selezionata è: • **Predefinito**: l'indirizzo IP viene assegnato automaticamente; i campi **IPv4 @**, **Subnet mask** e **Gateway predefinito** sono disattivati. • **Statico** Immettere un indirizzo IPv4 valido per la porta di controllo.
	Subnet mask	Se è selezionato **Statico** come **Modalità**, sopra, immettere una subnet mask IPv4 valida per la porta di controllo, che determina la porzione di rete dell'indirizzo IPv4.
	Gateway predefinito	Se è selezionato **Statico** come **Modalità**, sopra, immettere un indirizzo IPv4 valido per il gateway predefinito.
Porta backplane		
	IPv4 @	Immettere un indirizzo IPv4 valido per la porta backplane.
Orodatario sorgente		Vedere la sezione Configurazione della funzione orodatario sorgente, pagina 121.
Frequenza di campionamento rapida		Se selezionata, è possibile configurare il client OPC UA con un intervallo di campionamento minimo di 20 ms, che consente il monitoraggio di 2.000 elementi. Deselezionata per impostazione predefinita, il periodo di campionamento predefinito è 250 ms, che consente il monitoraggio dell'equivalente di 20.000 elementi di tipo INT. **NOTA:** una modifica di questa impostazione è effettiva solo dopo un download completo dell'applicazione.
Porta di ascolto TCP OPCUA		La porta TCP per la comunicazione OPCUA: • Per impostazione predefinita: preimpostata sulla porta 4840 • Altro valore: specificato dall'utente **NOTA:** il valore di questa porta deve essere lo stesso per tutti i moduli BMENUA0100 che comunicano tra loro (ad esempio, nel caso di inoltro NAT OPC UA tra più moduli BMENUA0100)

NOTA: quando si configura l'applicazione in Control Expert:

- La finestra **Rete Ethernet** (aperta tramite **Strumenti > Gestione rete Ethernet...**) visualizza le impostazioni per la porta backplane e la porta di controllo per il modulo BMENUA0100, comprese le informazioni per il server NTP, il gestore SNMP e, per un sistema Hot Standby, per il modulo standby BMENUA0100 (B).
- La pagina **Server indirizzi** del controller (aperta nel **Browser DTM** facendo doppio clic sul controller, quindi selezionando **Servizi > Server indirizzi**) visualizza l'indirizzo IP della porta backplane del modulo BMENUA0100. In una configurazione Hot Standby, la pagina **Server indirizzi** del controller visualizza l'indirizzo IP della porta backplane per entrambi i moduli BMENUA0100.

Configurazione della funzione orodatario sorgente

La funzione orodatario sorgente è supportata dalla versione firmware 2.01 (e successiva) del modulo BMENUA0100 (BMENUA0100.2) in Control Expert.

Per utilizzare la funzione orodatario sorgente in un'applicazione, è necessario abilitarla, quindi attivarla.

Dopo aver abilitato e attivato la funzione orodatario sorgente, il modulo BMENUA0100 inizia a interrogare i dispositivi quando è presente almeno un elemento monitorato con **Modalità di monitoraggio** impostata su **Campionamento** o **Segnalazione** nel client OPC UA.

NOTA: i valori vengono recuperati da un dispositivo orodatario all'origine solo per le variabili BOOL ed EBOOL che sono:

- configurate come ASTS (at-source-time-stamp) in Control Expert.
- monitorate da un client OPC UA come parte di una sottoscrizione OPC UA.

Se il nodo OPC UA non è stato aggiunto a una sottoscrizione e monitorato come parte di essa, il servizio di lettura sincrono OPC UA rileverà e segnalerà un errore.

Abilitazione orodatario sorgente

La funzione orodatario sorgente è abilitata nella finestra Impostazioni progetto. Selezionare **Generale > Tempo > Modalità orodatario** quindi **Sistema**.

NOTA: l'impostazione predefinita della **Modalità orodatario** è **Applicativa**. Se non si modifica l'impostazione predefinita a **Sistema**, l'errore rilevato viene visualizzato durante la creazione dell'applicazione.

Attivazione orodatario sorgente

Usare la scheda **IPConfig** della finestra di dialogo di configurazione BMENUA0100 per attivare e configurare la funzione orodatario.

Nella sezione **Orodatario sorgente**, configurare le impostazioni seguenti:

Impostazione	Descrizione
Activated	Attiva la funzione orodatario sorgente per l'applicazione.
Polling of buffer (ms)	La frequenza di interrogazione per le richieste di lettura evento gestite da BMENUA0100. L'intervallo di impostazioni valido è compreso tra 250 ms minimo e 5000 ms massimo in incrementi di 250 ms. **NOTA:** il numero massimo di variabili orodatate sorgente in Control Expert è 5000.

NOTA: Se il rack locale M580 include due moduli BMENUA0100, la funzione orodatario sorgente può essere utilizzata solo da un modulo. Vedere l'argomento Specifica del BMENUA0100 per gestire le variabili orodatate, pagina 125.

Gestione delle variabili orodatate all'origine

Utilizzo degli elementi dati OPC UA `#TSEventItemsReady` e `#TSEventSynchro`

È possibile utilizzare gli elementi dati specifici di OPC UA `#TSEventItemsReady` e `#TSEventSynchro` per cercare e impostare, rispettivamente, lo stato delle variabili orodatate all'origine.

NOTA: entrambi gli elementi dati sono significativi solo quando la funzione orodatario è abilitata in Control Expert e attivata per il modulo BMENUA0100 specifico.

BMENUA0100 tratta l'elemento dati `#TSEventSynchro` come nodo OPC UA booleano.

Impostando l'elemento `#TSEventSynchro` si invia un comando di sincronizzazione a tutti i dispositivi orodatati all'origine del controller M580. I valori restituiti al client OPC UA dai dispositivi inizializzano le variabili orodatate all'origine ai valori presenti.

Il BMENUA0100 risponde al client impostando l'elemento `#TSEventSynchro` con uno dei seguenti messaggi:

- `UA_EGOOD`: la richiesta di sincronizzazione è stata inviata correttamente a tutti i dispositivi di orodatazione.
- `UA_EBAD`: la richiesta di sincronizzazione non è riuscita perché l'orodatazione è disabilitata nel progetto Control Expert.

- `UA_EBADINVALIDSTATE`: la richiesta di sincronizzazione non è riuscita perché l'orodatazione è stata disattivata per il modulo BMENUA0100 dalla funzionalità % MW400, pagina 125.
- `UA_EBADINUSE`: la richiesta di sincronizzazione non è riuscita perché il modulo BMENUA0100 non è riuscito a riservare il buffer di orodatazione.
- `UA_EBADDISCONNECT`: la richiesta di sincronizzazione è scaduta e non è stato possibile scrivere i valori nell'intervallo di tempo specificato.

Per eseguire questa inizializzazione, utilizzare un client OPC UA, ad esempio UaExpert, per eseguire la sequenza di task seguente:

1. Monitorare l'elemento `#TSEventItemsReady` che indica che il modulo BMENUA0100 è pronto per gestire le variabili orodatate dei buffer del controller (inclusi controller M580, BMECRA31310, BMXERT1604), quindi attendere che il valore diventi 1 (TRUE).
2. Aggiungere elementi dati monitorati configurati come variabili orodatate all'origine a una o più sottoscrizioni.
3. Impostare il comando di scrittura `#TSEventSynchro` per aggiornare il valore di orodatazione all'origine di ogni elemento.

   NOTA:

   - BMENUA0100 legge tutte le variabili orodatate configurate nel controller. Se si verifica un evento (cambiamento di stato dell'elemento) su un elemento monitorato orodatato, tale elemento viene aggiornato. Un elemento, se non è monitorato, viene eliminato.
   - Impostare il filtro di modifica dati su **Stato/Valore/Timestamp**. In caso contrario, è possibile che diversi client OPC UA, ad esempio client che aggiornano i valori solo in caso di modifiche di stato/valore, visualizzino uno stato e un valore diversi per la stessa variabile.
   - Poiché BMENUA0100 aggiorna i valori periodicamente, è possibile che si verifichino più eventi dall'aggiornamento precedente. In tale caso, BMENUA0100 visualizza solo il valore più recente.
   - Poiché `#TSEventSynchro` viene inviato a più dispositivi di orodatazione, se un dispositivo singolo non risponde entro il periodo di tempo previsto, l'impostazione `#TSEventSynchro` restituisce la risposta `UA_EBADDISCONNECT` che indica il timeout del comando e il mancato completamento. Ciò vale anche se altri dispositivi rispondono correttamente.
   - Se la sottoscrizione viene modificata per contenere, ad esempio, una sola variabile per un dispositivo, l'esecuzione di `#TSEventSynchro` causa la perdita di valori restituiti in precedenza per le variabili e i dispositivi precedentemente sottoscritti.

Determinazione dei canali del controller M580 dedicati alla funzione orodatario

Per la comunicazione tra il BMENUA0100 e un controller M580, dove la funzione orodatario è abilitata in Control Expert, il 25% dei canali del controller sono dedicati a supportare la funzione di indicazione di data/ora. Rimane disponibile un massimo del 75% dei canali del controller per altre richieste di comunicazione.

Ad esempio, per il controller BMEP584040:

- N. max di canali 13
- Canali utilizzati per l'indicazione di data/ora: 3
- Canali utilizzati per non indicare data/ora: 10

Determinazione della capacità del BMENUA0100 di leggere variabili orodatate

Il numero di variabili orodatate che il BMENUA0100 può leggere per ciclo dipende da:

- Impostazione **Interrogazione del buffer** nella scheda **IPConfig** del modulo e
- Capacità del dispositivo all'origine, tra cui:
  - numero massimo di connessioni TCP e
  - numero massimo di variabili orodatate all'origine supportate.

La formula per determinare il numero massimo di variabili orodatate all'origine per un dispositivo è:

((Numero max di connessioni TCP) / (Numero di canali)) x (Numero max di variabili orodatate per ciclo)

Ad esempio:

- BMEP586040(C): 16 connessioni max, 4 canali, 82 variabili max:

  ((16 / 4) x 82 = 328 variabili totali

  Se **Polling del buffer** = 500 ms: 656 variabili al secondo.
- BMECRA31310: 1 connessione, 1 canale, 82 variabili max:

  1 x 82 = 82 variabili totali

  Se **Polling del buffer** = 500 ms: 164 variabili al secondo.
- BMXERT1604: 1 connessione, 1 canale, 20 variabili max:

  1 x 20 = 20 variabili totali

  Se **Polling del buffer** = 500 ms: 40 variabili al secondo.

Come specificare BMENUA0100 per gestire le variabili orodatate

Un rack principale M580 può contenere due moduli BMENUA0100. Tuttavia, le variabili orodatate nei moduli controller M580, BMECRA31310 e BMXERT1604 possono essere lette e gestite da un solo modulo BMENUA0100 alla volta. All'avvio, ciascun BMENUA0100 per impostazione predefinita tenta di riservare e bloccare l'accesso alle variabili orodatate.

In un rack con due moduli BMENUA0100, occorre specificare quello che leggerà e gestirà le variabili orodatate. Per specificare il BMENUA0100 che leggerà e gestirà le variabili, procedere come segue:

1. Nella scheda **IPConfig** dei due moduli BMENUA0100 per cui si desidera la funzione orodatario, selezionare **Attivato**.
2. Per il modulo BMENUA0100 per cui si desidera riservare il buffer di orodatazione, utilizzare il blocco `WRITE_VAR` per impostare la parola %MW400 a 2, che attiva la lettura e la gestione delle variabili orodatate per questo modulo.

   NOTA: l'impostazione %MW400 = 2 identifica il modulo BMENUA0100 che leggerà e gestirà le variabili quando due moduli BMENUA0100 hanno selezionato l'impostazione **Attivato**.
3. Per l'altro modulo BMENUA0100 per cui non si desidera riservare il buffer di orodatazione, utilizzare il blocco `WRITE_VAR` per impostare la parola %MW400 a 1, che disattiva la lettura e la gestione delle variabili orodatate per questi moduli.

   NOTA: è necessario eseguire questi passaggi dopo ogni modifica della modalità operativa, come accensione e spegnimento, caricamento dell'applicazione o esecuzione di un'inizializzazione.

Il BMENUA0100 specificato mantiene il controllo della lettura e della gestione delle variabili orodatate finché continuano a esistere entrambe le condizioni seguenti:

- Viene monitorata almeno una variabile orodatata.
- La BMENUA0100 **Modalità di monitoraggio** è impostata su **Segnalando** o **Campionamento**.

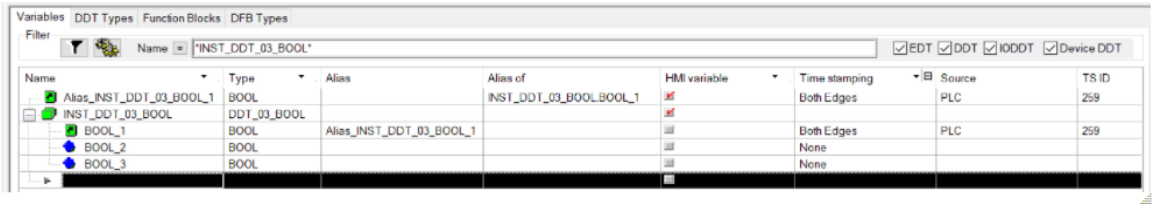
NOTA:

Quando l'impostazione **Attivato** è deselezionata, i valori delle variabili letti da BMENUA0100 sono i valori nella memoria del controller.

Quando l'impostazione **Attivato** è selezionata e %MW400 è stato impostato a 1, i valori delle variabili letti dal BMENUA0100 mantengono l'ultimo valore letto quando era riservato il buffer di orodatazione.

Monitoraggio delle variabili alias orodatate

BMENUA0100 riconosce le variabilli **Alias** BOOL o EBOOL orodatate create in Control Expert, ma non riconosce in modo simile alcuna variabile **Alias di** corrispondente. Di seguito è riportato un esempio di variabili **Alias** e **Alias di**:



Deve essere riconosciuto dal BMENUA0100, le variabili **Alias** devono essere integrate nel dizionario dati.

Le variabili **Alias** BOOL o EBOOL e le corrispondenti variabili **Alias di** condividono lo stesso indirizzo logico all'interno della memoria M580 e lo stesso EventID nel buffer orodatario M580. La funzione orodatario di origine è gestita solo sulla variabile **Alias** e non **Alias di**. In altre parole, è necessario sottoscrivere la variabile **Alias** (nodo OPC UA) nel client OPC UA per poter ricevere la funzione orodatario di origine dal dispositivo anziché dal modulo BMENUA0100.

Perché né la variabile **Alias di** BOOL o EBOOL è considerata orodatata all'origine dal firmware BMENUA0100, l'**Alias** deve essere integrato nel dizionario dati. In tale caso, occorre aggiungere la variabile **Alias** come elemento monitorato in una sottoscrizione OPC UA, per ottenere la funzione orodatario di origine impostata dal dispositivo.

Configurazione del servizio di sincronizzazione dell'ora

Introduzione

Il modulo di comunicazione BMENUA0100 Ethernet con server OPC UA integrato supporta la versione 4 del protocollo dell'ora di rete (NTP). Il servizio NTP sincronizza l'orologio nel modulo BMENUA0100 con l'orologio di un server dell'ora. Il valore sincronizzato è utilizzato per aggiornare l'orologio del modulo.

Sono supportati entrambi i protocolli IPv4 e IPv6.

NOTA:

- Se il server NTP risiede nel controller, il modulo BMENUA0100 può aggiornare le proprie impostazioni dell'ora senza introdurre ritardi.
- Quando si raggiunge un nuovo server NTP o è presente uno scostamento dell'ora in un server NTP, possono essere necessari fino a 5 minuti per aggiornare il modulo BMENUA0100. Il LED **ERR**, pagina 134 resta illuminato finché l'ora del BMENUA0100 non è sincronizzata con il server NTP.
- La configurazione manuale di una modifica dell'ora, immettendo un'ora futura, può scollegare i canali OPC UA esistenti. Se il client OPC UA esegue una riconnessione automatica al server OPC UA, verranno creati nuovi canali e verrà eseguita la riconnessione.

Attivazione e disattivazione del client NTP e del server NTP

Il modulo BMENUA0100 include un server NTP e un client NTP.

Client NTP:

Se l'indirizzo IP del server NTP primario o secondario è impostato a un valore diverso da 0.0.0.0, il client NTP è attivato. Se entrambe le impostazioni dell'indirizzo IP del server NTP primario e secondario sono vuote, oppure se sono impostate su 0.0.0.0 (IPv4) o su 0000:0000:0000:0000:0000:0000:0000:0000 (IPv6), il client NTP è disattivato.

NOTA: se l'indirizzo IP del **Server NTP primario** e del **Server NTP secondario** è impostato a 0.0.0.0, il modulo BMENUA0100 non può funzionare come client NTP o server NTP.

Server NTP:

Il server NTP è attivato, in base alla modalità operativa di sicurezza informatica:

- In modalità Advanced (o Secured), il server NTP è attivato se:
  - l'indirizzo IP del server NTP primario o secondario è impostato a un valore non nullo (ossia, impostato a un valore diverso da 0.0.0.0); e
  - il server NTP è impostato su attivato nelle impostazioni di configurazione della pagina Web, pagina 96 **Servizi di rete**.
- In modalità Standard, il server NTP è attivato se l'indirizzo IP del **Server NTP primario** o del **Server NTP secondario** è impostato a un valore non nullo (ossia, impostato su un valore diverso da 0.0.0.0).

  NOTA: Se il BMENUA0100 è configurato come client NTP sulla rete backplane (**Server NTP primario** o **Server NTP secondario**), il server NTP BMENUA0100 non può essere attivato per un altro dispositivo.

Se il server NTP e il client NTP sono entrambi attivati nel modulo BMENUA0100, il client NTP del modulo riceve le impostazioni dell'ora sulla propria porta di controllo da un server NTP remoto. Il server NTP del modulo inoltra queste impostazioni dell'ora sulla propria porta backplane ai client NTP.

NOTA: il modulo BMENUA0100 non può funzionare come server NTP sulla propria porta di controllo.

Interrogazione NTP

Il modulo BMENUA0100 gestisce in modo ottimale e dinamico il periodo di interrogazione NTP con il server NTP. Non sono necessarie ulteriori configurazioni.

Accensione

Per determinare un'ora di rete del sistema Ethernet, il sistema esegue i seguenti task all'accensione:

- Il modulo di comunicazione BMENUA0100 si accende.
- Il modulo di comunicazione BMENUA0100 ottiene l'ora dal server NTP.
- Per ottenere la massima accuratezza dell'ora il servizio richiede che le richieste siano inviate periodicamente. La configurazione del **Periodo di interrogazione** determina la precisione dell'ora.

Una volta ottenuta l'ora precisa, il servizio imposta lo stato nella diagnostica del servizio associata.

NOTA: Il modulo di comunicazione BMENUA0100 non mantiene l'ora. Al momento dell'accensione o durante un ciclo di spegnimento/riaccensione, il valore dell'orologio del modulo è 0, che equivale al 1° gennaio del 1980 - 00:00:00:00.

Configurazione del servizio

Configurare il servizio di sincronizzazione dell'ora della rete in Control Expert come indicato di seguito:

Passo	Azione
1	Nel **Browser di progetto**, espandere il nodo **Bus PLC** e aprire la finestra di dialogo di configurazione del modulo BMENUA0100.
2	Fare clic sulla scheda **NTP**.
3	Immettere le modifiche nei campi appropriati nella pagina di configurazione **Servizio di sincronizzazione dell'ora**. (La tabella seguente descrive i parametri della pagina di configurazione.)

Parametri configurabili

Configurare questi parametri di sincronizzazione dell'ora per ciascun modulo di comunicazione BMENUA0100 nel progetto:

Parametro		Descrizione
Configurazione server NTP IPv4		
	Server NTP primario (vedere Nota)	Immettere un indirizzo IPv4 o IPv6 valido per il server NTPv4 primario. **NOTA:** Per impostazione predefinita, impostare all'indirizzo IP principale del controller.

Parametro		Descrizione
	Server NTP secondario (vedere Nota)	Immettere un indirizzo IPv4 o IPv6 valido per il server NTPv4 secondario.

NOTA:

- Configurare l'indirizzo del server NTP raggiungibile dal modulo BMENUA0100. Se la porta di controllo è disattivata, immettere gli indirizzi IP del server NTP nella stessa sottorete della porta backplane.
- È possibile configurare un indirizzo IPV4 per il server NTP primario e un indirizzo IPV6 per il server NTP secondario (e viceversa), se entrambi gli indirizzi si trovano nello stesso dominio.
- Per le configurazioni Hot Standby, gli indirizzi del server NTP per **NUA(A)** e **NUA(B)** devono trovarsi nella stessa rete, ad esempio la rete accessibile tramite la porta backplane o la rete accessibile tramite la porta di controllo.

NOTA: Quando si opera in modalità Advanced (o Secured), verificare che il servizio NTP sia attivato nella sezione Attivazione dei servizi di rete, pagina 96 della pagina Web **Impostazioni**.

Configurazione agente SNMP

Informazioni sul protocollo SNMP

Tutte le versioni firmware del modulo BMENUA0100 supportano l'agente SNMP versione 1 (V1). La versione firmware 2 (e successiva) del modulo (BMENUA0100.2) supporta anche la versione 3 (V3) dell'agente SNMP.

NOTA: entrambe le versioni SNMP, V1 e V3, non sono supportate contemporaneamente.

Un agente SNMP è un componente software del servizio SNMP in esecuzione sul modulo BMENUA0100 per consentire l'accesso alle informazioni di diagnostica e di gestione del modulo. Per accedere a questi dati è possibile utilizzare il browser SNMP, il software di gestione di rete e altri strumenti.

Inoltre, l'agente SNMP può essere configurato con gli indirizzi IP di 1 o 2 dispositivi (in genere PC che eseguono il software di gestione di rete) come destinazione dei messaggi trap basati su evento. Tali messaggi informano il dispositivo di gestione di eventi come gli avvii a freddo e l'impossibilità di autenticare un dispositivo.

NOTA: La comunicazione con l'agente SNMP in esecuzione sul modulo BMENUA0100 può essere eseguita utilizzando l'indirizzamento IPv4 o IPv6.

Terminazione del servizio SNMP

Il servizio SNMP in esecuzione sul modulo BMENUA0100 viene terminato se:

- il modulo è in stato di ERRORE.

- il servizio SNMP è in stato di GUASTO.

Accesso alla scheda SNMP

Fare doppio clic sul modulo BMENUA0100 nella configurazione di Control Expert per accedere alla scheda **SNMP**.

L'agente SNMP può collegarsi e comunicare con 1 o 2 gestori SNMP. Il servizio SNMP comprende:

- controllo autenticazione eseguito dal modulo BMENUA0100 di qualsiasi gestore SNMP che invia richieste SNMP.
- gestione degli eventi o dei trap.

Configurazione agente SNMP in Control Expert e nelle pagine Web

I parametri SNMP comuni sono configurati in Control Expert. I parametri SNMP relativi alla sicurezza informatica sono configurati nelle pagine Web del modulo.

Se il selettore a rotazione di sicurezza informatica è impostato su:

- Modalità Advanced (o Secured): è possibile configurare l'agente SNMP nelle pagine Web di Control Expert e del modulo BMENUA0100.

  NOTA: in modalità Advanced (o Secured), la versione SNMP deve essere configurata in modo uguale in Control Expert e nella pagina Web SNMP, pagina 102. Se queste impostazioni non sono uguali, il servizio SNMP non si avvia.
- Modalità Standard: è possibile configurare l'agente SNMP solo in Control Expert.

  NOTA: se il modulo è configurato per SNMP V3 in Control Expert:

  - Il modulo BMENUA0100.2, dotato della versione firmware 2 o successiva, utilizza SNMP V3 con livello di sicurezza senza autorizzazione né privacy.
  - Il modulo BMENUA0100, con firmware precedente alla versione 2, gestisce SNMP V1.

Parametri SNMP

La scheda **SNMP** di Control Expert include i seguenti parametri. Se non diversamente indicato, i parametri si applicano a SNMP V1 e a V3.

NOTA: in modalità Advanced (o Secured), la versione SNMP deve essere configurata in modo uguale in Control Expert e nella pagina Web SNMP, pagina 102. Se queste impostazioni non sono uguali, il servizio SNMP non si avvia.

Campo	Parametro	Descrizione	Valore
Versione SNMP	SNMP V1	Selezionare questa opzione per utilizzare SNMP V1	selezionato/cancellato
	SNMP V3	Selezionare questa opzione per utilizzare SNMP V3	
Gestori indirizzo IP	Gestore indirizzo IP 1	L'indirizzo IPv4 del primo gestore SNMP a cui l'agente SNMP invia notifiche di trap.	Dipendente dal protocollo (IPv4)
	Gestore indirizzo IP 2	L'indirizzo IPv4 del secondo gestore SNMP a cui l'agente SNMP invia messaggi di trap.	
Agente	Posizione (SysLocation)	Posizione del dispositivo	31 caratteri (massimo)
	Contatto (SysContact)	Indicazione della persona da contattare per la manutenzione del dispositivo	
	Abilita gestore SNMP	*cancellato* (predefinito): è possibile modificare i parametri **Posizione** e **Contatto**. *selezionato*: non è possibile modificare i parametri **Posizione** e **Contatto**.	selezionato/cancellato
Nomi comunità (solo SNMP V1)	Set	Password richiesta dall'agente SNMP per la lettura di comandi da un gestore SNMP **NOTA:** Non esistono configurazioni predefinite. Se si utilizza un gestore SNMP, immettere lo stesso nome comunità utilizzato dal gestore SNMP.	15 caratteri (massimo)
	Get		
	Trap		
Sicurezza (solo SNMP V1)	Attiva trap **Errore di autenticazione**	*cancellato* (predefinito): non attivato. *selezionato*: abilitato. L'agente SNMP invia un messaggio trap al gestore SNMP se un gestore non autorizzato invia un comando **Get** o **Set** all'agente.	selezionato/cancellato
Nome utente SNMP (solo SNMP V3)		Il nome utente riconosciuto dal server SNMP.	stringa di 32 caratteri max ASCII / UTF8 nell'intervallo di codifica [33-122]

Trap supportati

Per impostazione predefinita, l'agente SNMP V1 del modulo BMENUA0100 supporta i trap seguenti:

- Linkup
- Linkdown

È supportato anche il trap di **Errore di autenticazione**, se attivato.

Identificatori oggetto MIB-II SNMP

In **Nome fornitore** Schneider Electric, il modulo BMENUA0100 presenta i seguenti valori dell'identificatore oggetto (OID):

Nome oggetto	OID	Valore
SysDesc	1.3.6.1.2.1.1.1	Prodotto: BMENUA0100 - Modulo di comunicazione OPC UA. ID 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, che rappresenta la somma di $(2)_{7-1}$ + $_{24-1}$ + 2_{2-1}) e indica il supporto di protocolli nei seguenti livelli OSI: • 7: livello applicazione • 4: livello trasporto • 2: livello collegamento dati
ifDesc	1.3.6.1.2.1.2.2.1.2	Questo OID contiene informazioni che descrivono l'interfaccia, compresi nome prodotto e nome porta.

Configurazione delle impostazioni del controller M580 per connessioni client - server OPC UA

Introduzione

Questa sezione descrive le impostazioni effettuate per la configurazione del controller M580 per supportare le connessioni tra il server OPC UA nel modulo BMENUA0100 e un client OPC UA.

Configurazione delle impostazioni di sicurezza del controller M580

Configurazione dei servizi del controller

Per supportare le comunicazioni tra il server OPC UA nel modulo BMENUA0100 e un client OPC UA, attivare le impostazioni seguenti nella scheda Sicurezza del controller M580:

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

Se entrambi questi servizi non sono attivati nel controller, le comunicazioni OPC UA non funzionano correttamente.

Diagnostica

Panoramica

Questo capitolo descrive gli strumenti di diagnostica disponibili per il modulo di comunicazione Ethernet BMENUA0100 con server OPC UA integrato.

Diagnostica LED

Diagnostica LED del pannello di visualizzazione

Di seguito sono descritti gli stati dei LED del pannello di visualizzazione, pagina 24 del modulo BMENUA0100 per i vari stati operativi del modulo.

NOTA: Lo stato del LED **SECURE** per lo stato configurato e non configurato del modulo viene presentato separatamente, di seguito, dopo la presentazione iniziale.

Stato operativo		**LED**						
		RUN (Verde)	**UACNX (Verde/ Rosso)**	**ERR (Rosso)**	**BS (Verde/ Rosso)**	**NS LED (verde/ rosso)**	**BUSY (Giallo)**	**SEC (Verde/ Rosso)**
Sequenza di accensione	1	Spento	Acceso	Acceso	Verde spento Rosso fisso	Verde spento Rosso fisso	Spento	Verde spento Rosso fisso
	2 (tutti i LED accesi)	Acceso	Acceso	Acceso	Verde fisso Rosso fisso	Verde fisso Rosso fisso	Acceso	Verde fisso Rosso fisso
	3 (tutti i LED spenti)	Spento	OFF	Spento	Verde spento Rosso spento	Verde spento Rosso spento	Spento	Verde spento Rosso spento
	4	Acceso	Spento	Acceso	Verde spento Rosso spento	Verde spento Rosso spento	Spento	Verde spento Rosso spento
	5 (Autotest[1])	Lampeggiante	Lampeggiante	Lampeggiante	Verde lampeggiante Rosso spento	Verde lampeggiante Rosso spento	Lampeggiante	Verde lampeggiante Rosso spento
Non configurata		Spento	Spento	Lampeggiante	Rosso lampeggiante se non collegato a una porta backplane Ethernet. Verde lampeggiante in caso contrario.	Spento se non è inserito alcun cavo e collegato a un altro dispositivo alimentato. Verde lampeggiante in caso contrario.	Spento	Vedere la sezione LED di sicurezza informatica di seguito, pagina 138.

Stato operativo		**LED**						
		RUN (Verde)	**UACNX** (Verde/ Rosso)	**ERR** (Rosso)	**BS** (Verde/ Rosso)	**NS** LED (verde/ rosso)	**BUSY** (Giallo)	**SEC** (Verde/ Rosso)
Configurato	Dopo aver rilevato un indirizzo IPv4 duplicato sulla porta backplane	Lampeggiante	Vedere la descrizione del LED **UACNX**, di seguito, pagina 137	/	Verde spento Rosso fisso	/	/	Vedere la descrizione del LED di stato della comunicazione sicura, di seguito, pagina 138.
	Dopo aver rilevato un indirizzo IPv4 duplicato sulla porta di controllo	Lampeggiante		/	/	Verde spento Rosso fisso	/	
	Stato RUN	Acceso		Spento	Verde fisso Rosso spento	Verde fisso se collegato; spento se scollegato.	Acceso se acquisizione dizionario dati in corso; Lampeggiante in caso di overflow del dizionario dati; altrimenti spento	
Alimentazione spenta		Spento	OFF	Spento	Verde spento Rosso spento	Verde spento Rosso spento	Spento	Verde spento Rosso spento
Rilevato errore ripristinabile o configurazione incoerente[2]		/	/	Acceso	/	/	/	/
Rilevato errore non ripristinabile (Il modulo verrà riavviato)		Spento	Spento	Acceso	Verde spento Rosso fisso	Verde spento Rosso fisso	Spento	Verde spento Rosso fisso

Stato operativo		LED						
		RUN (Verde)	**UACNX (Verde/ Rosso)**	**ERR (Rosso)**	**BS (Verde/ Rosso)**	**NS LED (verde/ rosso)**	**BUSY (Giallo)**	**SEC (Verde/ Rosso)**
Cybersecurity (o Security) Reset	In corso	Lampeggiante	OFF	Spento	Verde spento Rosso fisso	Verde spento Rosso fisso	Acceso	Verde spento Rosso spento
	Completa	Acceso	Spento	Spento	Verde spento Rosso fisso	Verde spento Rosso fisso	Spento	Verde spento Rosso spento
Cybersecurity (o Security) Reset mancante[3]		Spento	Spento	Acceso	Verde spento Rosso fisso	Verde spento Rosso fisso	Spento	Rosso lampeggiante
Aggiornamento SO		Lampeggiante	OFF	Spento	Verde spento Rosso fisso	Verde spento Rosso fisso	Acceso	Verde spento Rosso spento

1. L'autotest viene eseguito rapidamente e il LED lampeggiante non può essere rilevato visivamente.

   NOTA: Se il modulo rimane nello stato Autotest, verificare il selettore a rotazione per confermare che si trovi in una posizione valida.

2. Consultare i codici di errore SERVICES_STATUS rilevati nel DDT T_BMENUA0100, pagina 139.

3. Questo stato risulta dal passaggio del selettore a rotazione dalla modalità Standard alla modalità Advanced (o Secured) o dalla modalità Advanced (o Secured) alla modalità Standard senza eseguire un Cybersecurity (o Security) Reset, pagina 29 come passo intermedio.

   NOTA: In questa tabella, "/" indica qualsiasi stato.

LED UACNX quando il modulo è in stato configurato

Il colore (rosso o verde) e lo stato (lampeggiante o fisso) descrivono lo stato delle connessioni OPC UA:

Stato dizionario dati	Stato connessione client OPC UA	
	Nessun client OPC UA collegato	**Almeno 1 client OPC UA collegato**
Dizionario dati non disponibile	Rosso lampeggiante	Rosso fisso
Dizionario dati disponibile	Verde lampeggiante	Verde fisso

LED di stato comunicazioni sicure quando il modulo è configurato/non configurato

Gli stati del LED **SECURE**, quando il modulo è nello stato configurato o non configurato, sono descritti di seguito:

Stato del LED	Descrizione
Spento	Il modulo non funziona in modalità operativa sicura (ossia, il selettore a rotazione non è impostato in posizione di sicurezza).
ROSSO	È stato rilevato un errore critico di comunicazione sicura. Ad esempio, non è presente alcuna configurazione di sicurezza, un certificato non è valido, un certificato è scaduto, le comunicazioni sono interrotte e così via.
VERDE	Le comunicazioni sicure sono abilitate e in esecuzione senza errori rilevati. Un client è collegato al modulo e il modulo ha ricevuto una configurazione di sicurezza informatica valida. La sessione viene aperta e il modulo è pronto a rispondere alle richieste del client.
ROSSO LAMPEGGIANTE	Le comunicazioni sicure sono abilitate e in esecuzione, ma è stato rilevato un errore. Ad esempio, un certificato è scaduto ma la configurazione autorizza le comunicazioni a continuare.
VERDE LAMPEGGIANTE	Il modulo ha ricevuto una configurazione di sicurezza informatica valida ed è pronto a comunicare con un client che inizierà una comunicazione.

Diagnostica LED porta di controllo

I LED della porta di controllo, pagina 25 possono essere utilizzati per diagnosticare lo stato delle comunicazioni Ethernet sulla porta di controllo:

LED	Stato	Descrizione
il	Disattivato	Nessun collegamento stabilito.
	Verde	Collegamento stabilito, nessuna attività.
	Verde lampeggiante	Collegamento stabilito, attività rilevata.
LNK	Spento	Nessun collegamento stabilito.
	Giallo	Collegamento stabilito a una velocità inferiore alla capacità massima del modulo (10/100 Mbps).
	Verde	Collegamento stabilito a una velocità uguale alla capacità massima del modulo (1000 Mbps).

Tipo di dati derivati (DDT) BMENUA0100

Introduzione

Ogni modulo di comunicazione Ethernet BMENUA0100 con server OPC UA integrato che si aggiunge all'applicazione crea un'istanza comune di un insieme di elementi dati. È possibile utilizzare gli strumenti presentati nel software Control Expert per accedere a questi elementi dati ed eseguire la diagnostica del modulo.

NOTA:

- I dati DDT restituiti in risposta a una richiesta Modbus non possono superare i 256 byte di lunghezza.
- Data l'organizzazione del dizionario dati Control Expert, le richieste di dati memorizzati in bit di parole devono essere estratte dal client richiedente.

Il contenuto del DDT è accessibile mediante la funzione elementare READ_DDT, pagina 144 (EF) del software Control Expert.
s

NOTA: se il DDT del modulo non può essere letto per alcun motivo, ad esempio se l'indirizzo IP del backplane non è configurato correttamente, è possibile eseguire la diagnostica del modulo tramite i LED, pagina 134 del modulo.

Struttura DDT T_BMENUA0100

Il DDT BMENUA0100 include i seguenti elementi:

Elemento	Tipo	Indirizzo	Descrizione
DEVICE_NAME	STRING [16]	MW1...8	Il nome del modulo.
CONTROL_PORT_IPV6	STRING [44]	MW9...30	Porta di controllo IPv6 / lunghezza prefisso subnet.
CONTROL_PORT_IPV4	STRING [18]	MW31...39	Porta di controllo IPv4 / lunghezza prefisso subnet.
CONTROL_PORT_GTW	STRING [16]	MW40...47	Gateway predefinito porta di controllo.
ETH_BKP_PORT_IPV4	STRING [18]	MW48...56	Porta backplane IPv4 / lunghezza prefisso subnet.
ETH_STATUS	WORD	MW57	–
PORT_CONTROL_LINK	BOOL	MW57.0	• 0: Collegamento porta di controllo non operativo. • 1: Collegamento porta di controllo operativo.

Elemento	Tipo	Indirizzo	Descrizione
ETH_BKP_PORT_LINK	BOOL	MW57.1	• 0: Collegamento porta backplane non operativo. • 1: Collegamento porta backplane operativo.
GLOBAL_STATUS	BOOL	MW57.2	• 0: Modulo non operativo. • 1: Modulo operativo.
NETWORK_HEALTH	BOOL	MW57.3	• 0: È stata rilevata una condizione di sovraccarico di rete. • 1: La rete funziona normalmente.
Riservato	–	MW57.4...15	–
OPCUA_STATUS	T_OPCUA_STATUS	MW58...61	Vedere dettagli più avanti.
DATA_DICT	BYTE	MW58[0]	• 1: Non disponibile. Possibili cause: ◦ La funzionalità del dizionario dati non è disponibile o attivata nell'applicazione Control Expert e non può essere integrata nel controller. ◦ È in corso un'attività di caricamento/selezione nel dizionario dati nel server OPC UA. • 2: Disponibile, ad esempio: ◦ L'attività di caricamento/selezione nel dizionario dati del server OPC UA è stata completata correttamente. ◦ Potrebbe essere in corso un precaricamento (in conformità alle impostazioni di progetto del dizionario dati di Control Expert). • 4: Occupato. • 8: Overflow del dizionario dati.
DATA_DICT_ACQ_DURATION	BYTE	MW58[1]	Durata dell'ultima acquisizione (0...255 secondi). **NOTA:** il valore 255 indica un tempo di durata uguale o superiore a 255 secondi.
CONNECTED_CLIENTS	BYTE	MW59[0]	Numero di client OPC UA collegati.
DATA_DICT_PRELOAD_DURATION	BYTE	MW59[1]	Durata dell'ultimo precaricamento del dizionario dati (0...255 secondi). **NOTA:** è possibile utilizzare le informazioni contenute in questo elemento per regolare e ottimizzare l'impostazione del **timeout modifiche creazione effettiva** nella finestra di configurazione **Strumenti > Impostazioni progetto > Generale > Dati integrati PLC**. Per informazioni su come configurare questa impostazione, consultare la guida in linea di Control Expert.

Elemento	Tipo	Indirizzo	Descrizione
REDUNDANCY_MODE	BYTE	MW60[0]	• 0: Nessuno • 2: Modalità di ridondanza non trasparente ("calda").
SERVICE_LEVEL	BYTE	MW60[1]	Stato del server OPC UA, pagina 150, in base ai dati e alla qualità del servizio.
Riservato	WORD	MW61	–
SERVICES_STATUS	T_ SERVICES _STATUS	MW62...68	Vedere dettagli più avanti.
NTP_CLIENT_SERVICE	BYTE	MW62[0]	Stato client NTP: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato ◦ 1 = Ora non valida (ora non aggiornata) ◦ 2 = Tempo di recupero (il tempo del server è aumentato o diminuito di un offset di almeno 1000 secondi). Il modulo BMENUA0100 può richiedere fino a 5 minuti per essere risincronizzato). ◦ 4 = Il server NTP è ancora raggiungibile, ma non sincronizza il client. Quando il server NTP riprende le operazioni, l'errore rilevato viene risolto automaticamente. Questa operazione può richiedere fino a 1024 secondi.
NTP_SERVER_SERVICE	BYTE	MW62[1]	Stato server NTP: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato: solo modalità Advanced (o Secured): ◦ 1 = Porta di controllo non configurata ◦ 2 = Client NTP di backplane e server abilitato nelle pagine Web
SNMP_SERVICE	BYTE	MW63[0]	Stato server SNMP: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 1 (SNMP V1): 0 = SNMP non configurato / 1 = SNMP configurato • Bit 1 e 2: SNMP V3: 00 = SNMP non configurato / 11 = SNMP configurato • Bit 4...7: Codice di errore rilevato ◦ 1 = SNMP è attivato in modalità Advanced (o Secured) e nessun indirizzo IP SNMP è definito in Control Expert (0.0.0.0)
Riservato	BYTE	MW63[1]	–

Elemento	Tipo	Indirizzo	Descrizione
WEB_SERVER	BYTE	MW64[0]	Stato server Web: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato ◦ 1 = Errore non ripristinabile rilevato
FW_UPGRADE	BYTE	MW64[1]	Stato aggiornamento firmware: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato ◦ 1 = Pacchetto firmware non valido ◦ 2 = Ultimo aggiornamento del firmware non riuscito (gestito come errore rilevato non ripristinabile)
Riservato	BYTE	MW65[0]	–
Riservato	BYTE	MW65[1]	–
CONTROL_EXPERT_IP_ FORWARDING	BYTE	MW66[0]	Stato inoltro IP Control Expert: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato (solo modalità Advanced (o Secured)): ◦ 1 = Porta di controllo non configurata **NOTA:** Per i moduli con versione firmware 2.01 e successive, il valore di questo elemento è forzato a 0.
CPU_TO_CPU_IP_ FORWARDING	BYTE	MW66[1]	Stato di inoltro da controller a controller: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato (solo modalità Advanced (o Secured)): ◦ 1 = Porta di controllo non configurata **NOTA:** Per i moduli con versione firmware 2.01 e successive, il valore di questo elemento è forzato a 0.
IPSEC	BYTE	MW67[0]	Stato IPsec: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato (solo modalità Advanced (o Secured)): ◦ 1 = Porta di controllo non configurata
Riservato	BYTE	MW67[1]	–

Elemento	Tipo	Indirizzo	Descrizione
EVENT_LOG_SERVICE	BYTE	MW68[0]	Stato servizio registro eventi: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato (solo modalità Advanced (o Secured)): ◦ 1 = Errore rilevato registro eventi del servizio. ◦ 2 = Errore rilevato configurazione registro eventi
LOG_SERVER_NOT_ REACHABLE	BYTE	MW68[1]	Stato server di registrazione: • Bit 0: 0 = Riconoscimento ricevuto dal server syslog / 1 = Nessun riconoscimento ricevuto dal server syslog
FW_VERSION	T_FW_ VERSION	MW69...72	Versione del firmware del modulo. Vedere dettagli più avanti.
MAJOR_VERSION	WORD	MW69	Versione firmware principale.
MINOR_VERSION	WORD	MW70	Versione firmware secondaria.
INTERNAL_REVISION	WORD	MW71	Revisione interna del firmware.
Riservato	WORD	MW72	–
CONTROL_PORT_STATUS	BYTE	MW73[0]	Stato IPv4 porta di controllo: • Bit 0: 0 = Inattivo / 1 = Attivo • Bit 4...7: Codice di errore rilevato (solo modalità Advanced (o Secured)): ◦ 1 = IP non valido ◦ 2 = IP duplicato
Riservato	BYTE	MW73[1]	–
IN_PACKETS_RATE	UINT	MW74	Numero di pacchetti ricevuti al secondo su tutte le interfacce Ethernet.
IN_ERROR_COUNT	UINT	MW75	Numero di pacchetti in ingresso con errori rilevati dall'ultimo reset (modulo 65535).
OUT_PACKETS_RATE	UINT	MW76	Numero di pacchetti emessi al secondo su tutte le interfacce Ethernet.
OUT_ERROR_COUNT	UINT	MW77	Numero di pacchetti in uscita con errori rilevati dall'ultimo reset (modulo 65535).
MEM_USED_PERCENT	BYTE	MW78[0]	Percentuale di RAM interna utilizzata dal server OPC UA.
CPU_USED_PERCENT	BYTE	MW78[1]	Percentuale del processore interno utilizzata.
CYBERSECURITY_STATUS	T_CYBER SECURI-TY_ STATUS	MW79...80	Stato di sicurezza informatica. Vedere dettagli più avanti.

Elemento	Tipo	Indirizzo	Descrizione
SECURE_MODE	BYTE	MW79[0]	• 0: Il modulo funziona in modalità Standard. • 1: Il modulo funziona in modalità Advanced (o Secured).
CYBERSECURITY_STATE	BYTE	MW79[1]	Stato di sicurezza informatica: • 0: Modalità Advanced (o Secured) OFF: (LED **SECURE** SPENTO) • 1: Comunicazione protetta abilitata e in esecuzione senza errori rilevati. (LED **SECURE** VERDE) • 2: Pronto per la comunicazione. (LED **SECURE** VERDE LAMPEGGIANTE) • 3: Comunicazione sicura in esecuzione con errori secondari rilevati. (LED **SECURE** ROSSO LAMPEGGIANTE) • 4: Comunicazioni sicure interrotte a causa di un errore critico rilevato. (LED **SECURE** ROSSO)
IPSEC_CHANNELS	BYTE	MW80[0]	Il numero di canali IPsec aperti.
Riservato	BYTE	MW80[1]	–

Configurazione della funzione elementare READ_DDT

Panoramica

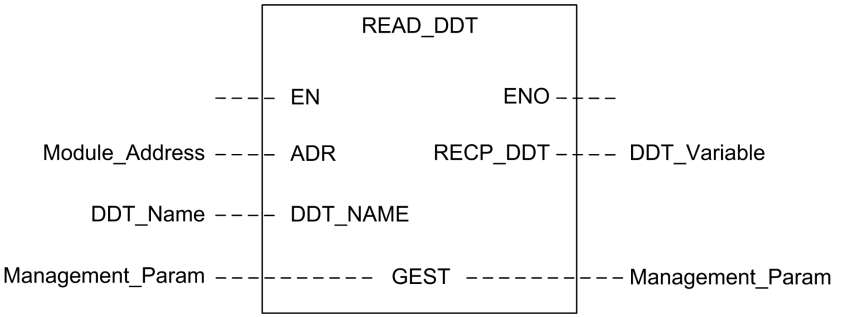
Utilizzare il blocco funzione `READ_DDT` per configurare i messaggi letti per il modulo di comunicazione BMENUA0100.

I parametri `ADR`, `DDT_NAME` e `GEST` definiscono l'operazione.

`EN` e `ENO` possono essere configurati come parametri aggiuntivi.

NOTA: Per informazioni sull'uso di questo blocco funzione in un sistema Hot Standby, consultare l'argomento Blocchi funzione di comunicazione asincrona (vedere *Modicon M580 Hot Standby - Architetture di utilizzo frequente - Guida di sistema*).

Rappresentazione FBD



Parametri di ingresso

Parametro	Tipo di dati	Descrizione
EN	BOOL	Questo parametro è facoltativo. Quando questo ingresso è impostato a uno, il blocco viene attivato e può risolvere l'algoritmo dei blocchi funzione. Quando questo ingresso è impostato a zero, il blocco viene disattivato e non risolve l'algoritmo del blocco funzione.
ADR	Qualsiasi array di INT	Array contenente l'entità di destinazione dell'operazione di scambio. L'indirizzo è il risultato della funzione ADDMX. (Ad esempio: ADDMX (0.0.3{192.168.10.2}100.TCP.MBS) indica il modulo all'indirizzo IP 192.168.10.2, con UnitId 100 (server locale del modulo), collegato alla porta Ethernet integrata.
DDT_NAME	STRING	Nome del DDT da leggere: T_BMENUA0100

Parametri di ingresso/uscita

L'array GEST è locale:

<table>
<tr><th>Parame-tro</th><th>Tipo di dati</th><th colspan="3">Descrizione</th></tr>
<tr><td rowspan="3">GEST</td><td rowspan="3">Array [0...3] of INT</td><td colspan="3">I parametri di gestione, costituiti da quattro parole. Vedere la sezione della guida di Control Expert Struttura dei parametri di gestione (vedere EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi) per ulteriori informazioni su questi parametri.</td></tr>
<tr><td>Paro-la#</td><td>BYTE più significativo</td><td>BYTE meno significativo</td></tr>
<tr><td>0</td><td>Numero di scambio</td><td>Bit di attività: rango 0</td></tr>
</table>

Parame-tro	Tipo di dati	Descrizione		
				Bit di annullamento: rango 1 Bit di riconoscimento immediato: rango 2
		1	Rapporto operazione (vedere *EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi*)	Rapporto comunicazione (vedere *EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi*)
		2	Timeout (vedere *EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi*)	
		3	Lunghezza (vedere *EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi*)	

Parametri di uscita

Parametro	Tipo di dati	Descrizione
ENO	BOOL	Questo parametro è facoltativo. Selezionando questa uscita si ottiene anche l'ingresso EN. L'uscita ENO viene attivata in caso di esecuzione corretta del blocco funzione.
RECP_DDT	Qualsiasi	Buffer di ricezione. È possibile utilizzare una variabile DDT. Per il contenuto di questo DDT, vedere la descrizione del DDT T_BMENUA0100, pagina 139. La dimensione dei dati ricevuti (in byte) viene scritta automaticamente dal sistema nella quarta parola della tabella di gestione.

Blocchi funzione per la comunicazione asincrona

In un'applicazione Hot Standby durante un evento di commutazione, il blocco funzione di comunicazione asincrona READ_DDT non riprende automaticamente il funzionamento sul nuovo controller primario, se non configurato specificamente, come indicato di seguito.

Utilizzare la procedura seguente per consentire agli EFB di comunicazione asincroni di riprendere automaticamente il funzionamento dopo una commutazione:

- Programmare l'applicazione in modo che non tutte le istanze degli EFB vengano scambiate con il controller di standby. A questo scopo, deselezionare l'attributo **Scambio su STBY** per l'istanza EFB.

Considerazioni quando si configura la funzione

Quando si utilizza la funzione elementare READ_DDT, considerare quanto segue:

- Se l'applicazione comprende più BMENUA0100 in un rack, utilizzare istanze separate di un array WORD per ogni pin GEST. Ogni blocco gestisce il proprio array WORD di gestione.
- Non è necessario specificare un valore per il parametro della lunghezza in GEST[3], in quanto non vi sono dati da inviare. Al termine dell'operazione (quando il bit di attività in GEST[0] è impostato a 0), la lunghezza viene impostata con la lunghezza dei dati copiati nel parametro di uscita RECP_DDT se non viene segnalato alcun errore rilevato in GEST[1] o con un codice di stato opzionale. Vedere la sezione della guida di Control Expert *Codici di errore degli EFB con parametro STATUS* (vedere *EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi*) per una descrizione di questi valori aggiuntivi del codice di stato.
- Un valore di timeout pari a 0 indica nessun timeout. In questo caso, una perdita o un ritardo di comunicazione che si verifica durante l'operazione di scambio non viene rilevato. Il parametro RECP_DDT mantiene il valore precedente. Per evitare questo scenario, impostare il timeout a un valore diverso da zero.
- In caso di report operazione 16#01 (Richiesta non elaborata) o 16#02 (Risposta errata) nella parola GEST[1] della tabella di gestione, un codice di stato aggiuntivo può essere segnalato nel parametro della lunghezza (GEST[3]). I codici di stato restituiti in questo campo corrispondono a un sottointervallo dei possibili codici del parametro STATUS degli EFB di comunicazione. I valori possibili per READ_DDT sono 30ss hex e 4001 hex. Vedere la sezione della guida di Control Expert *Codici di errore degli EFB con parametro STATUS* (vedere *EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi*) per una descrizione di questi valori aggiuntivi del codice di stato.
- In base al DDT specificato nel parametro DDT_NAME, sui dati ricevuti vengono eseguite alcune verifiche di coerenza. Se viene rilevata una mancata corrispondenza, viene impostato il codice 16#02 (Risposta errata) nel byte del report operazione (il byte più significativo di GEST[1]). Tenere presente che il blocco non verifica la validità del tipo di dati della variabile configurata come buffer di ricezione (RECP_DDT). Verificare che il tipo di dati della variabile collegata al parametro RECP_DDT corrisponda al tipo di dati ricevuti.

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Verificare che la variabile di tipo DDT associata al parametro di uscita RECP_DDT corrisponda al tipo di dati scritti nel buffer di ricezione.
- Verificare che l'indirizzo impostato nel parametro ADR corrisponda al modulo corretto, in particolare quando sono configurati più moduli identici nella stessa rete.

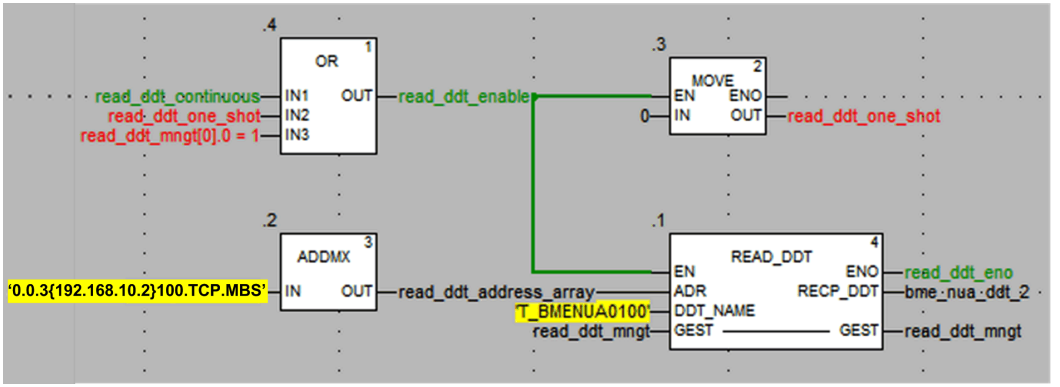
Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Configurazione della funzione elementare READ_DDT

Per configurare la funzione elementare READ_DDT, seguire questa procedura:

Passo	Azione
1	Impostare il dispositivo di destinazione in ADR (utilizzare un blocco ADDM per specificare questo indirizzo in formato stringa esplicito).
2	Impostare il parametro DDT_NAME con il nome del DDT da leggere.
3	Richiamare la funzione READ_DDT per avviare la comunicazione (con il pin di ingresso EN impostato a 1, se configurato).
4	Monitorare il bit di attività (nel byte meno significativo del parametro GEST[0]) fino al completamento della comunicazione (il bit di attività viene impostato a 0 dal sistema al termine della comunicazione). Eseguire la funzione solo una volta per evitare di cancellare i valori di stato. Ad esempio, impostando il pin EN a 0 durante il funzionamento si provoca il richiamo della funzione.
5	Visualizzare i parametri del report in GEST[1]. Se il report indica 16#0000, il buffer RECP_DDT contiene i dati ricevuti. La dimensione dei dati ricevuti (in byte) viene scritta nella quarta parola (GEST[3]) della tabella di gestione.

Esempio di EF READ_DDT EF



In questo esempio, è possibile avviare l'EF READ_DDT:

- Continuamente impostando la variabile read_ddt_continuous.

  NOTA: nel caso di un errore rilevato, non è possibile leggere i codici del report nella seconda parola della variabile read_ddt_mngt.

- Solo una volta, impostando la variabile read_ddt_one_shot.

Configurazione della funzione elementare READ_NUA_DDT

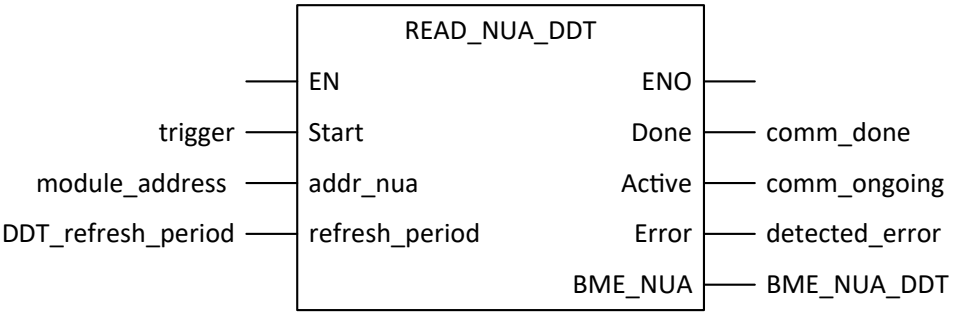
Utilizzare il blocco funzione `READ_NUA_DDT` per accedere alle informazioni di diagnostica del modulo BMENUA0100.

I parametri di ingresso `Start`, `addr_nua` e `refresh_period` definiscono l'operazione.

È possibile configurare EN ed ENO come parametri supplementari.

NOTA: per informazioni sull'uso di questo blocco funzione in un sistema Hot Standby, consultare l'argomento Blocchi funzione di comunicazione asincrona (vedere *Modicon M580 Hot Standby - Architetture di utilizzo frequente - Guida di sistema*).

Rappresentazione FBD



Parametri di ingresso

Parametro	Tipo di dati	Descrizione
EN	BOOL	Questo parametro è facoltativo. Quando questo ingresso è impostato a uno, il blocco viene attivato e può risolvere l'algoritmo dei blocchi funzione. Quando questo ingresso è impostato a zero, il blocco viene disattivato e non risolve l'algoritmo dei blocchi funzione.
Start	BOOL	La lettura del DDT BMENUA0100 è continua.

Parametro	Tipo di dati	Descrizione
addr_nua	string[32]	Indirizzo del modulo BMENUA0100 assegnato ad ADDMX() per la lettura. Stringa a lunghezza fissa contenente l'indirizzo della destinazione BMENUA0100. L'indirizzo è il risultato della funzione ADDMX. (Ad esempio: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) indica il modulo all'indirizzo IP 192.168.10.2, con UnitId 100 (server locale del modulo), collegato alla porta Ethernet integrata.
refresh_period	TIME	Periodo di aggiornamento del DDT.

Parametri d'uscita

Parametro	Tipo di dati	Descrizione
ENO	BOOL	Questo parametro è facoltativo. Quando si seleziona questa uscita, si ottiene anche l'ingresso EN. L'uscita ENO viene attivata a seguito della corretta esecuzione del blocco funzione.
Eseguito	BOOL	Comunicazione completata.
Attivo	BOOL	Comunicazione in corso.
Errore	BOOL	Errore rilevato sul blocco funzione di comunicazione.
BME_NUA	T_BMENUA0100	Il DDT, pagina 139 BMENUA0100 che può essere utilizzato così com'è.

Diagnostica OPC UA

Introduzione

Il modulo BMENUA0100 presenta le variabili del server OPC UA ed elementi dati specifici utilizzabili per identificare l'applicazione in esecuzione nel modulo e per diagnosticare il funzionamento del modulo.

Variabile OPC UA SERVICE_LEVEL

La variabile SERVICE_LEVEL fornisce informazioni a un client relative allo stato del controller e alla condizione del server OPC UA. La variabile SERVICE_LEVEL è accessibile direttamente nella struttura del nodo server OPC UA. La variabile SERVICE_LEVEL è inoltre duplicata nell'elemento OPCUA_STATUS.SERVICE_LEVEL del DDT, pagina 139 del

modulo BMENUA0100 e vi si può accedere da programma eseguendo la funzione elementare READ_DDT, pagina 144 quando l'applicazione è nello stato RUN.

NOTA: Nelle architetture ridondanti, il client OPC UA deve monitorare la variabile SERVICE_LEVEL nei moduli BMENUA0100 primario e di standby per gestire il meccanismo di ridondanza. Quando il client rileva che il valore SERVICE_LEVEL del modulo di standby è maggiore del valore SERVICE_LEVEL del modulo primario, il client deve attivare una commutazione dal modulo primario a quello di standby.

Le variabili seguenti del livello di servizio si applicano a tutte le versioni firmware del modulo BMENUA0100, ad eccezione di quanto indicato:

Valore SERVICE_LEVEL	**Stato del controller / server OPC UA**	
	Firmware = V1.0	**Firmware ≥ V1.1**
0	BMENUA0100 è in fase di avvio. Il controller è in stato NOCONF o ERROR. Esempio di stato ERROR: Il task MAST è in stato HALT.	
1	Il server OPC UA si è avviato. È in corso la ricerca nell'elenco del dizionario dati.	
5	La ricerca nel dizionario dati è avviata.	
10	Overflow dimensioni dizionario dati.	
20	È in corso la ricerca di tipo nel dizionario dati.	
50	È in corso la ricerca di variabili nel dizionario dati.	
100	La ricerca nel dizionario dati è completata. La lettura dello stato del controller è in corso. Lo spazio degli indirizzi verrà aggiornato con il nuovo contenuto del dizionario dati.	
120[1]	Controller in stato STOP.	Controller in stato STOP STANDBY o HALT STANDBY (solo controller Hot Standby).
150[1]	Controller in stato WAIT STANDBY (solo controller Hot Standby).	
199[1]	Controller in stato RUN STANDBY (solo controller Hot Standby).	
202[2]	<Non applicabile>	Solo controller standalone: controller in stato STOP STANDALONE. Solo controller Hot Standby: se entrambi i controller sono in stato STOP o HALT, un BMENUA0100 viene dichiarato come master con livello di servizio = 202. Lo spazio degli indirizzi è OK e utilizzabile.
255	Controller in RUN (o RUN PRIMARY per il controller Hot Standby). Il server OPC UA è operativo	

1. Questo valore non deve essere impostato prima che il server diventi operativo.

2. Questo livello di servizio si applica solo al firmware V1.10 e versioni successive di BMENUA0100.

NOTA: le dimensioni del dizionario dati sono proporzionali al tempo di acquisizione del dizionario (ossia, il tempo richiesto dal modulo per cercare e caricare il dizionario dati). Durante l'acquisizione del dizionario dati, SERVICE_LEVEL resta al valore 100 fino al completamento dell'acquisizione. Quando si esegue una modifica di creazione in Control Expert generando un nuovo dizionario dati, il server OPC UA riavvia la ricerca nel dizionario dati. Durante questo processo, gli aggiornamenti degli elementi correntemente monitorati possono essere interrotti, con i valori degli elementi monitorati bloccati al valore aggiornato più recente.

Variabili del server OPC UA

È possibile visualizzare queste variabili online mediante un dispositivo client OPC UA, come lo strumento UaExpert di Unified Automation. Selezionare il nodo server OPC UA **StatoServer > InfoBuild** per visualizzare le seguenti variabili del server OPC UA:

Variabile	Descrizione
BuildDate	La data di creazione dell'applicazione nel controller.
BuildNumber	Il numero di creazione dell'applicazione controller corrente.
ManufacturerName	“Schneider Electric”.
Nome prodotto	“BMENUA0100”.
ProductUri	L'Uniform Resource Identifier univoco assegnato al modulo.
SoftwareVersion	La versione del firmware del modulo.

Elementi dati OPC UA specifici

Il modulo BMENUA0100 supporta i seguenti elementi dati specifici. Tali elementi dati sono accessibili tramite lo stack del server OPC UA. Benché siano molto simili agli elementi dati del controller raggiungibili tramite il software Control Expert, questi elementi dati speciali non sono collegati ai simboli del controller e non sono raggiungibili tramite il software Control Expert:

Elemento dati	Tipo di dati	Valore predefinito	Descrizione
#AddressSpaceState	INT16	0	Stato dello spazio degli indirizzi, con la relativa raccolta di oggetti e nodi. I valori possibili sono: **0.** Vuoto **1.** Creato **2.** Aggiornamento **3.** Creazione parziale (nessun dizionario dati presente nell'applicazione oppure overflow del dizionario dati)
#ApplicationName	STRING	0	Il nome dell'applicazione del controller.
#ApplicationVersion	STRING	0	La versione dell'applicazione del controller.
#CurrentDataDictionaryItemsCount	INT32	0	Numero di elementi nel dizionario dati caricati nel server.
#CurrentMonitoredItemsCount	INT32	0	Numero di elementi monitorati dal server.
#DeviceIdentity	STRING	0	Il nome del riferimento del controller.
#PLCDatadicReady	BYTE	1	Monitora lo stato di caricamento del dizionario dati del controller: 1. Il dizionario dati del controller non è disponibile. Le spiegazioni possibili sono: • La funzionalità del dizionario dati non è disponibile o attivata nell'applicazione Control Expert e non può essere integrata nel controller. • È in corso un'attività di caricamento/selezione nel dizionario dati nel server OPC UA. 2. Il dizionario dati del controller è disponibile, ad esempio: • L'attività di caricamento/selezione nel dizionario dati del server OPC UA è stata completata correttamente. • Potrebbe essere in corso un precaricamento (in conformità alle impostazioni di progetto del dizionario dati di Control Expert).
#PLCQualStatus	INT16	0	Monitora lo stato della comunicazione di un controller. I possibili valori (hex) comprendono: • 00C0 hex: la comunicazione con il controller è corretta. • 0040 hex: nessuna comunicazione con il controller per un tempo inferiore al Timeout dispositivo (5s).

Elemento dati	Tipo di dati	Valore predefinito	Descrizione
			• 0 hex: il controller non è identificato.
#TSEventItemsReady	BOOL	0	Elemento di sola lettura che indica se nell'applicazione M580 econtroller sono state cercate variabili orodatate di origine e dispositivi orodatario di origine: • 0 = non selezionato • 1 = selezionato **NOTA:** Questa voce è significativa solo quando la funzione orodatario è abilitata in Control Expert e attivata per il modulo BMENUA0100 specifico.
#TSEventSynchro	BOOL	0	Elemento di lettura/scrittura che, quando attivato, invia un valore sincronizzato a tutti i dispositivi orodatario all'origine collegati al controller M580 ogni volta che viene eseguita un'operazione di scrittura. Lo scopo è inizializzare tutti gli elementi monitorati orodatati ai loro valori. • 0 = in attesa di attivazione • 1 = attivato **NOTA:** • Il valore di questo elemento apparirà come 0. Un valore 1 non verrà mai visto perché esiste solo momentaneamente e ritorna nuovamente al valore di attivazione in attesa di 0. • Questa voce è significativa solo quando la funzione orodatario è abilitata in Control Expert e attivata per il modulo BMENUA0100 specifico.

Syslog

Introduzione

Il modulo BMENUA0100 registra gli eventi in un buffer diagnostico locale, quindi invia un record di tali eventi a un server syslog remoto in cui vengono memorizzati e resi disponibili per i client syslog. Per la diagnostica degli eventi precedenti, è possibile interrogare i record eventi del server syslog. Per gli eventi correnti del modulo, è possibile utilizzare le pagine Web del modulo, pagina 157 per diagnosticare lo stato del servizio syslog e visualizzare gli eventi specificati nel buffer di diagnostica.

Il buffer locale funziona come un buffer circolare, dove gli eventi più recenti sovrascrivono e sostituiscono gli eventi meno recenti quando il buffer è pieno.

Il modulo memorizza gli eventi nella memoria volatile.

Gli eventi registrati si riferiscono a:

- Sicurezza/autorizzazione, pagina 156

  – oppure –

- Modifiche principali nel sistema (controllo registro), pagina 157

Il servizio syslog è configurabile nelle pagine Web, pagina 95 come parte della configurazione della sicurezza informatica e, pertanto, può essere attivo solo quando il modulo funziona in modalità Advanced (o Secured). Quando il modulo opera in modalità Standard, il servizio è disattivato.

Come implementato nel modulo BMENUA0100, syslog è supportato da IPv4 (versione firmware 1.0 e successive) e IPv6 (versione firmware 1.10 e successive).

NOTA: Syslog non è un protocollo sicuro in origine, ma deve essere incapsulato in un canale sicuro IPsec, pagina 101 sulla porta di controllo.

Struttura del messaggio Syslog

Il protocollo syslog, RFC 5424, definisce come si scambiano gli eventi tra il modulo e il server remoto. La struttura del messaggio syslog è indicata di seguito:

Campo	**Descrizione**
PRI	Informazioni sul servizio e sulla gravità (descrizione nelle tabelle seguenti).
VERSION	Versione delle specifiche del protocollo syslog (Versione = 1 per RFC 5424).
TIMESTAMP	Il formato orodatario è emesso da RFC 3339 che utilizza il seguente formato data e ora Internet ISO8601: YYY**-**MM**-**DD**T**hh**:**mm**:**ss**.**nnn**Z** **NOTA: -**, **T**, **:**, **.**, **Z** sono caratteri obbligatori e fanno parte del campo orodatario. **T** e **Z** devono essere scritti in maiuscolo. **Z** specifica che l'ora è UTC. Descrizione del contenuto del campo dell'ora:

YYY	Anno
MM	Mese
DD	Giorno
hh	Ora
mm	Minuti
ss	Secondi
nnn	Frazione di secondo in millisecondi (0 se non disponibile)

Campo	Descrizione
HOSTNAME	Identifica il computer che ha inviato originariamente il messaggio syslog: nome di dominio completo (FQDN) o indirizzo IP statico origine se FQDN non è supportato.
APP-NAME	Identifica l'applicazione che ha inizializzato il messaggio syslog. Contiene le informazioni che consentono di identificare l'entità che invia il messaggio (ad esempio, sottogruppo del modello commerciale).
PROCID	Identifica il processo, o entità o componente che invia l'evento.
MSGID	Identifica il tipo di messaggio a cui è associato l'evento, ad esempio HTTP, FTP, Modbus.
MESSAGE TEXT	Questo campo contiene diverse informazioni: • Indirizzo emittente: indirizzo IP dell'entità che genera il registro. • ID peer: ID peer se un peer è coinvolto nell'operazione (ad esempio, il nome utente per un'operazione di registrazione). • Indirizzo peer: indirizzo IP peer se un peer è coinvolto nell'operazione. • Tipo: numero univoco per identificare un messaggio (descrizione fornita nelle tabelle seguenti). • Commento: stringa che descrive il messaggio (descrizione fornita nelle tabelle seguenti).

Eventi correlati a sicurezza/autorizzazione

- Mancata apertura canale sicuro da stack OPC UA: ad esempio, certificato non valido, certificato scaduto.
- Sessioni utente riuscite (Login/Password) dallo stack OPC UA (login eseguito)

  NOTA: in caso di assenza di accesso (modalità Standard), il registro è disattivato quindi non viene creato alcun record della connessione effettuata.
- Sessioni utente non riuscite (Login/Password) dallo stack OPC UA (login non riuscito)

  NOTA: in caso di assenza di accesso (modalità Standard), il registro è disattivato quindi non viene creato alcun record della connessione non riuscita.
- Connessioni HTTPS riuscite a o da un tool (login eseguito): ad esempio, una connessione al server Web o un download del firmware tramite HTTPS.
- Accesso HTTPS non riuscito a/da un tool: ad esempio, una connessione non riuscita al server Web o un download del firmware non riuscito tramite HTTPS.
- Disconnessione sessione utente riuscita (logout a richiesta) per HTTPS.
- Disconnessione sessione utente riuscita (logout a richiesta) per OPC UA.
- Logout automatico: ad esempio, un timeout di inattività per OPC UA o HTTPS.
- Errore rilevato controllo integrità: ad esempio, un errore rilevato di firma digitale oppure un errore rilevato di sola integrità (hash).

- Creazione di un nuovo certificato.
- Rimozione di certificati locali. Questa azione è possibile tramite il selettore a rotazione per impostare la modalità operativa nella posizione di Cybersecurity (o Security) Reset.
- Aggiunta di un nuovo certificato del client dall'elenco autorizzati nel dispositivo.
- Rimozione di un certificato del client dall'elenco autorizzati nel dispositivo.

Eventi correlati a modifiche maggiori nel sistema (controllo registro)

- Download configurazione di sicurezza informatica o applicazione nel dispositivo.
- Download del firmware nel dispositivo.
- Firma non corrispondente per il firmware che non è stato possibile scaricare nel dispositivo.

Pagina Web di diagnostica Syslog

Utilizzare le pagine Web del modulo per la diagnostica dello stato del servizio syslog in esecuzione sul modulo e per diagnosticare parti specificate del buffer di diagnostica syslog del modulo. È inoltre possibile utilizzare l'elemento SERVICES_STATUS del DDT, pagina 139 del modulo per visualizzare lo stato del servizio syslog.

Nel menu **Diagnostica > Diagnostica registro eventi** utilizzare i comandi seguenti per visualizzare lo stato del servizio syslog del modulo:

Parametro	Descrizione
Stato	• Operativo: il modulo funziona in modalità Advanced (o Secured) e il servizio syslog è attivato. • Non operativo: il modulo funziona in modalità Advanced (o Secured) ma il servizio syslog è disattivato.
Server registro	• Raggiungibile: è possibile stabilire una connessione al server syslog remoto. • Non raggiungibile: non è possibile stabilire una connessione al server syslog remoto.

Nel menu **Diagnostica > Diagnostica registro eventi** nel campo **Buffer diag da leggere**, inserire la parte del buffer di diagnostica da leggere.

Diagnostica Modbus

Introduzione

È possibile utilizzare i comandi del codice funzione Modbus per eseguire la diagnostica del modulo BMENUA0100. I comandi Modbus possono raggiungere il modulo solo sulla relativa porta backplane. Poiché Modbus non è un protocollo intrinsecamente sicuro, è necessario incapsulare i comandi Modbus in IPsec.

Sul modulo BMENUA0100 sono supportate solo le richieste FC43/14 (Read Device Identification) e FC03 (lettura DDT MW%).

Accesso ai dati Modbus e modalità operativa di sicurezza informatica

Il metodo utilizzabile per accedere ai dati Modbus dipende dalla modalità operativa di sicurezza informatica. Se il modulo BMENUA0100 funziona in:

- Modalità standard: il modulo BMENUA0100 accetta il flusso dati client Modbus TCP/IP da qualsiasi client che può accedere alla rete Ethernet del backplane. Utilizzare i metodi di comunicazione Modbus standard, compresi i blocchi funzione DATA_EXCH, MBP_MSTR, READ_VAR e WRITE_VAR e i comandi Control Expert.
- Modalità Advanced (o Secured): il modulo BMENUA0100 accetta il flusso dati client Modbus TCP/IP solo dal controller M580. È possibile implementare il blocco DATA_EXCH nell'applicazione. È possibile utilizzare anche READ_VAR e WRITE_VAR.

  NOTA: per indirizzare il server Modbus nel modulo, è necessario utilizzare UnitID 100. Per informazioni su come impostare questo valore, consultare la documentazione del client Modbus. Ad esempio, quando si utilizza il blocco DATA_EXCH, UnitId può essere impostato con ADDMX come indicato di seguito: ADDMX (0.0.3{192.168.10.2}100.TCP.MBS) dove 192.168.168.10.2 è l'indirizzo IP backplane del modulo BMENUA0100.

43/14: Lettura di identificazione del dispositivo

I seguenti dati di identificazione dispositivo possono essere restituiti mediante il codice 43/ sottocodice 14 della funzione:

Categoria	ID oggetto	Nome oggetto	Tipo
Basic	00 hex	Nome fornitore	Stringa ASCII
	01 hex	Codice Prodotto	Stringa ASCII
	02 hex	Revisione maggiore minore	Stringa ASCII
Normale	03 hex	Url fornitore	Stringa ASCII
	04 hex	Nome prodotto	Stringa ASCII
	05 hex	Nome modello	Stringa ASCII
	06 hex	Nome applicazione utente	Stringa ASCII
	07 ...FF hex	Riservato	Stringa ASCII

Diagnostica SNMP

Introduzione

Quando l'agente SNMP è configurato, pagina 129, il modulo BMENUA0100 abilita la diagnostica SNMP nella rete Ethernet basata su TCP/IP tramite il supporto dei MIB seguenti:

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

MIB-II

MIB-II fornisce un gestore SNMP con una raccolta di variabili di gestione dispositivo. Leggendo queste variabili, un gestore SNMP può diagnosticare il funzionamento di un dispositivo specifico, ad esempio il BMENUA0100.

MIB LLDP

Il MIB LLDP contiene i dati raccolti dal funzionamento del protocollo di rilevamento livello relativo a identità, capacità e posizione sulla rete Ethernet. Utilizzando il MIB LLDP, un gestore SNMP può rilevare la topologia della rete e le capacità dei dispositivi di rete.

NOTA: La comunicazione SNMP dai dati MIB LLDP avviene esclusivamente sulla porta backplane.

Pagina Web Diagnostica OPC UA

Utilizzare la pagina Web **Diagnostica OPC UA** per visualizzare i dati dinamici che descrivono il funzionamento del server OPC UA integrato nel modulo BMENUA0100.

NOTA: la pagina Web **Diagnostica OPC UA** viene aggiornata ogni 5 secondi.

Dati di diagnostica

La pagina Web **Diagnostica OPC UA** visualizza i seguenti dati di sola lettura. Tenere presente che tutti i valori numerici sono in formato decimale:

Campo	Descrizione
Diagnostica del PLC	
EPAC	Indirizzo IP del controller.
Identità dispositivo	Codice prodotto del controller.
Versione dispositivo	Versione firmware del controller.
Stato dispositivo	Stato della connessione con il controller: **Buono**, **Cattivo**, **Incerto**, **Sconosciuto**, **Mancante**.
Timeout frame (in ms)	La lunghezza massima di tempo di attesa del server OPC UA di una risposta da un dispositivo dopo l'invio di una richiesta. Ad esempio, 1000.
Numero massimo di canali	Numero di connessioni aperte dal server OPC UA sul controller.
Canali utilizzati per non indicare data/ora	Numero di connessioni che trasportano i dati dell'applicazione.
Canali utilizzati per l'indicazione di data/ora	Numero di connessioni per l'indicazione di data/ora, pagina 124.
Lunghezza richiesta	Lunghezza della richiesta di comunicazione con il controller.
Nome applicazione (Dispositivo)	Nome progetto Control Expert.
Versione applicazione (dispositivo)	Checksum e firme applicazione.
Precaricamento dizionario dati	Disponibile o Non disponibile per l'applicazione nel controller.
Stato timestamp	Viene visualizzato lo stato dell'orodatario: • orodatario abilitato con accesso alle variabili orodatate nell'applicazione. • orodatatio è non abilitato, nessun accesso alle variabili orodatate.

Campo	Descrizione
Elenco dei dispositivi con orodatario sorgente configurato	Se è abilitato l'orodatario, viene visualizzato un elenco di dispositivi che indica per ogni dispositivo: • Numero di canali dedicati riservati per il polling dell'origine evento di orodatazione. • Tipo di dispositivo (BMECRA31310, controller, ecc.). • Indirizzo IPv4. • Prenotazione del buffer orodatario del dispositivo da parte del server OPC UA BMENUA0100 integrato: TRUE / FALSE.
Diagnostica OPC UA	
URL endpoint (IPV4)	Indirizzo IPv4 server OPC UA, nel formato: "opc.tcp://<indirizzo IPv4>:<numero porta>". Ad esempio: opc.tcp://192.168.2.142:4840
Frequenza di campionamento rapida	Indica se è selezionata l'impostazione della Frequenza di campionamento rapida, pagina 118: • TRUE = selezionato • FALSE = non selezionato
Numero di sessioni connesse	Numero totale di sessioni client supportate dal server OPC UA BMENUA0100 integrato.
Informazioni sulle sottoscrizioni:	Informazioni che descrivono le variabili monitorate dal server OPC UA incluse in una o più sottoscrizioni.
Numero di elementi monitorati dal nodo Server interno:	
Numero di elementi monitorati specifici:	
Numero di elementi monitorati non specifici:	
Numero di elementi monitorati orodatati con modalità di monitoraggio non disattivata:	
Numero totale di elementi monitorati:	
Numero corrente di timer	Il numero di intervalli di campionamento configurati per il server OPC UA BMENUA0100 integrato.
Elenco timer	Un elenco che descrive ogni intervallo di campionamento (ad esempio, il timer) monitorato dal server OPC UA BMENUA0100 integrato. Ogni voce indica: • L'intervallo di campionamento in ms. • Il numero di elementi monitorati. • Il numero di richieste generate durante l'esecuzione più recente.

Ottimizzazioni delle prestazioni del modulo BMENUA0100

Ottimizzazioni delle prestazioni del modulo BMENUA0100

Introduzione

Quando si ottimizzano le prestazioni del modulo BMENUA0100, tenere presente l'intero sistema. Prestare particolare attenzione all'efficienza delle comunicazione globale e al carico di lavoro nell'architettura di rete che include i moduli BMENUA0100. È in questo contesto che le ottimizzazioni delle prestazioni del client OPC UA influiscono anche sull'efficacia della comunicazione OPC UA.

Diverse impostazioni, a vari livelli dell'architettura, possono migliorare le prestazioni del sistema o rendere il sistema più stabile e robusto durante ciascuna delle fasi della modalità operativa (connessioni, ricerca, sottoscrizione, monitoraggio e così via).

NOTA:

- Aggiungere elementi in pacchetti di dimensione massima pari a 2000 elementi. L'intervallo di campionamento configurato è rilevante solo se maggiore o uguale al tempo di scansione del controller MAST.
- Impostare CallTimeout su un valore maggiore o uguale a 10 secondi nel client OPC UA.
- L'impostazione General.SecureChannelLifetime per la comunicazione con un client OPC UA è predefinita a 3.600.000 ms (1 ora). Utilizzare questa impostazione predefinita per evitare una riduzione delle prestazioni.
- Le prestazioni del sistema dipendono fortemente dalla configurazione (ad esempio, il numero di client collegati, il numero di variabili gestite e così via).
- Ad esempio, con 2000 elementi monitorati, la frequenza di aggiornamento può essere raggiunta entro 20 ms solo se i valori di un massimo di 500 elementi cambiano tra due iterazioni di pubblicazione consecutive.

Esempio di prestazioni

Un client OPC UA può monitorare fino a 20.000 elementi nella modalità di sicurezza informatica Standard.

Esempio basato su:

- BMEP584040 con un tempo di ciclo del task MAST a 20ms (carico della CPU inferiore all'80%).
- BMENUA0100 nella posizione Standard del selettore a rotazione (ossia nessuna comunicazione sicura, nessun canale IPsec).
- Il client OPC UA (UAExpert) inizia la comunicazione con la modalità di Sicurezza messaggio impostata su **Nessuna** e monitora 20.000 elementi facendo riferimento a variabili basate su un array di tipo 'INT' da un server OPC UA BMENUA0100. Tale server è configurato con Intervallo di pubblicazione a 1 secondo, Intervallo di campionamento a 1 secondo, Timeout sessione a 30 secondi.
- Nessun'altra comunicazione diversa da OPC UA.

Come regolare le prestazioni

Struttura di scambio dati

La memoria di applicazione dati del controller è organizzata in base alla definizione di applicazione dati in Control Expert. Più è strutturata la dichiarazione delle variabili, più il server BMENUA0100 genera richieste ottimizzate per l'accesso alle variabili e al dizionario dati in runtime.

Quindi, per le variabili a cui si accede dal client OPC UA:

- Utilizzare array o la struttura dati qualora possibile.
- Attivare l'opzione **Solo variabili HMI** in **Dati integrati PLC** delle **Impostazioni progetto** e impostare solo queste variabili con l'attributo **HMI** per ridurre le dimensioni del Dizionario dati.
- Nell'applicazione del controller di sicurezza, per ridurre la dimensione del dizionario dati, deselezionare l'opzione **Uso dello spazio dei nomi di processo** (in **Impostazioni progetto > Generale > Dati integrati PLC > Dizionario dati**.

Capacità di comunicazione del controller

La capacità del sistema di comunicazione dipende dal modello di controller M580 e da alcune impostazioni di configurazione. Il codice prodotto del controller determina:

- Le capacità prestazionali di elaborazione del controller a livello di sistema.
- Il numero di richieste per ciclo che possono essere elaborate, anche se configurabili dalla parola di sistema %SW90.
- Il numero massimo di canali disponibili per ciascun BMENUA0100 per stabilire le connessioni al controller M580, pagina 172.

Inoltre, minore è il tempo di ciclo MAST, maggiore è il numero di richieste di comunicazione che possono essere elaborate. Il livello prestazionale è perciò direttamente dipendente dal tempo di ciclo MAST.

Client OPC UA, configurazione e utilizzo

Il numero di variabili monitorate influisce sulle prestazioni. Le velocità di campionamento e gli intervalli di pubblicazione configurati per ciascun client OPC UA determinano il numero di richieste necessarie per animare le variabili. Ricordare che, quando più client OPC UA sono connessi allo stesso server OPC UA BMENUA0100, quando le velocità di campionamento e gli intervalli di pubblicazione sono diversi per ogni lato client OPC UA, questa configurazione genera più richieste.

Tutti i valori di timeout configurabili dal client OPC UA (Sfoglia, Connetti, Pubblica, Sessione, Watchdog…) devono essere regolati per ottimizzare e stabilizzare, per quanto possibile, il sistema globale. Come effetto collaterale, questi timeout possono influire sulle prestazioni del sistema.

In base alla modalità di Sicurezza messaggio (Nessuna, Firma, Firma e codifica), l'algoritmo per calcolare la firma e la crittografia richiede ulteriore tempo.

Comunicazioni da controller a controller e da Control Expert a controller

Ogni tunnel IPsec utilizzato per proteggere le comunicazioni diverse da OPC UA o HTTPS rallenta il traffico, in particolare quando l'impostazione è attivata **Confidenzialità**, generando così crittografia e decrittografia.

Come monitorare le prestazioni

È possibile monitorare le prestazioni in modi diversi.

Tramite Control Expert

Utilizzando Control Expert in modalità collegata, è possibile accedere al tempo di ciclo MAST effettivo e al carico del controller M580 per il sistema, per ogni task e per il totale di tutti i task leggendo le parole di sistema da %SW110 a %SW116. Inoltre, il DDDT del controller M580 e il DDT BMENUA0100 possono fornire varie informazioni di diagnostica collegate alle prestazioni di sistema del controller, come:

- Il livello di servizio del server OPC UA.
- Il numero di client OPC UA collegati.
- Stato, tempo di acquisizione e durata precaricamento del dizionario dati.
- Lo stato del servizio Ethernet.
- La condizione della rete.
- Lo stato della porta di controllo e della porta backplane.
- Il numero di pacchetti Ethernet al secondo.
- Il numero di pacchetti Ethernet contenenti errori rilevati.
- La percentuale di carico e memoria utilizzata della CPU BMENUA0100.
- Il numero di canali IPsec aperti.

Tramite il sito Web di BMENUA0100

La Home page e la pagina Diagnostica del sito Web di BMENUA0100 forniscono informazioni interessanti relative alle prestazioni dei server OPC UA. Alcune informazioni provengono dal DDT BMENUA0100 e altre sono fornite dal server OPC UA stesso:

- Numero di elementi monitorati.
- Numero di elementi specifici monitorati.
- I diversi intervalli di campionamento correntemente in esecuzione.
- Il numero di richieste generate per le animazioni.
- Overrun rilevati.
- Numero di client connessi.

Tramite il client OPC UA

Il client OPC UA può monitorare direttamente alcuni elementi specifici sotto il server OPC UA, ma anche la variabile ServiceLevel o alcuni sottocampi del DDT BMENUA0100 a richiesta tramite variabili dell'applicazione.

Altri servizi per la diagnostica

In un approccio più tecnico, l'agente SNMP e il server Syslog del modulo BMENUA0100 consentono di ottenere informazioni di diagnostica relative alle prestazioni dei server OPC UA.

Risoluzione dei problemi del modulo BMENUA0100

Introduzione

Questa sezione descrive i suggerimenti che è possibile utilizzare per migliorare il funzionamento del modulo BMENUA0100.

Impatto dell'uso di UaExpert come client OPC UA

Se si utilizza UaExpert come client OPC UA per leggere i valori dei dati, tenere presente che UaExpert incrementa il valore di *NumeroSottoscrizioniCorrenti* di 1 per ogni istanza di UAExpert.

NOTA: L'elemento *NumeroSottoscrizioniCorrenti* è correlato al server stesso e non deve essere scambiato per l'elemento relativo alla sessione *NumeroSottoscrizioniCorrenti*.

Tempo di acquisizione del dizionario dati e periodo MAST

Il tempo richiesto per caricare la raccolta di variabili nel dizionario dati dipende dal numero di elementi del dizionario dati e dal periodo MAST configurato. Per un'applicazione che richiede il server OPC UA nel modulo BMENUA0100 monitorizzi un numero che si avvicini al massimo di 100 000 elementi, sono stati osservati i seguenti risultati che possono essere istruttivi.

Per un'applicazione non di sicurezza con 99 000 elementi:

Periodo MAST	Tempo di acquisizione del dizionario dati osservato
20 ms	23 s
100 ms	46 s
200 ms	74 s

Per un'applicazione di sicurezza con 99 000 elementi:

Periodo MAST	Tempo di acquisizione del dizionario dati osservato
25 ms	15 s
200 ms	72 s

Configurazione delle sottoscrizioni con più di 30.000 elementi monitorati

Se si desidera creare una o più sottoscrizioni, che includono complessivamente più di 30.000 elementi monitorati, configurare ogni sottoscrizione nel client OPC UA rispettivo con un valore di **Conteggio del tempo di vita** di 300 secondi, che rappresenta il valore Durata massima sottoscrizione, pagina 35 che il server OPC UA del modulo BMENUA0100 può supportare.

Utilizzo di GPO / LGPO

Gestire i certificati su un PC host tramite uno dei seguenti strumenti disponibili nel sistema operativo Windows™:

- Oggetti Criteri di gruppo (GPO) per eseguire la gestione centralizzata delle impostazioni utente in un ambiente Active Directory centralizzato oppure
- Oggetti Criteri di gruppo locale (LGPO) per la gestione distribuita delle impostazioni utente per singoli PC.

In entrambi i casi, l'utilizzo di GPO o LGPO può contribuire a impedire l'accesso non autorizzato al PC e alle relative applicazioni. L'uso di GPO e LGPO disabilita l'accesso a Windows Microsoft Management Console (MMC) e supporta l'implementazione solo dell'elenco approvazioni configurato dal software.

Applicazione della Gestione Criteri di gruppo di MMC

Gestire i certificati utilizzando gli strumenti forniti da Microsoft Windows™ per evitare l'aggiunta di certificati non autorizzati al PC o la modifica di certificati autofirmati di un client OPC UA. In assenza di gestione, è possibile che qualcuno includa certificati non autorizzati all'elenco approvazioni di BMENUA0100 gestito dall'amministratore della sicurezza.

Questi strumenti includono i criteri di gestione dei criteri di gruppo applicati dall'oggetto Criteri di gruppo, un plug-in di Microsoft Management Console (MMC). Progettare i criteri in modo che disabilitino l'accesso a MMC Windows e consentano l'accesso solo alle voci dell'elenco approvazioni aggiunte correttamente dal software.

Blocco client OPC UA

Quando si collega un client OPC UA con un nome utente assegnato al server OPC UA integrato nel modulo BMENUA0100, vengono applicate le impostazioni dei criteri dell'account utente, pagina 95 del BMENUA0100. Ad esempio, se viene raggiunto o superato il numero **massimo di tentativi di accesso**, il client OPC UA non può accedere (**BadInternalError**) per il tempo impostato come **durata di blocco account**.

Attivazione dei servizi di rete utilizzando solo una connessione IPv6

Il modulo BMENUA0100 supporta solo l'uso di IPv6 per l'indirizzamento e la comunicazione IP. Se è attivato solo IPv6, pagina 117, i servizi di rete **Flussi dati da CPU a CPU** e **Flussi dati Control Expert nella rete di dispositivi** non sono disponibili. Questi servizi sono supportati solo da IPv4.

Tuttavia, è ancora possibile attivare queste funzionalità nella pagina Web **Impostazioni > Servizi di rete**. Se questi servizi sono attivati quando è attivato solo IPv6, questi servizi (**da CPU a CPU** e **CE nella rete di dispositivi**) appaiono come attivi nella pagina **Home** ma in realtà non sono attivati.

La comunicazione IPv6 supporta solo la funzione di filtraggio del flusso di dati **Flussi dati Control Expert solo a CPU**. In questo caso, con la sola comunicazione IPv6 attivata, la pagina **Home** mostra correttamente **CE solo a CPU** come attivo.

BOOL visti come BYTE nelle strutture dati del controller

Nel server OPC UA BMENUA0100, ogni elemento del DDT del controller è assegnato a un byte nel controller, anche se è definito come BOOL o EBOOL nel BMENUA0100. Tramite il protocollo OPC UA, un client può leggere o scrivere globalmente un membro BOOL o EBOOL di un'istanza BMENUA0100 nel DDT del controller, con un valore di byte valido diverso da 0 o 1 (ad esempio, 255). Progettare l'applicazione in modo da scrivere o leggere valori BOOL o EBOOL di solo 0 o 1, poiché solo questi valori sono validi nel BMENUA0100.

Aggiornamento del firmware

Strumento EcoStruxure™ Automation Device Maintenance

Presentazione dello strumento EcoStruxure™ Automation Device Maintenance

Utilizzare lo strumento EcoStruxure™ Automation Device Maintenance per aggiornare il firmware del modulo BMENUA0100. EcoStruxure™ Automation Device Maintenance è uno strumento basato sul Web che consente di:

- Rilevare manualmente uno o più moduli BMENUA0100 nel progetto in base agli indirizzi IP.
- Aggiornare alla versione del firmware più recente i moduli BMENUA0100 su Web.

Prima di aggiornare il firmware, è necessario:

- Collegarsi a BMENUA0100 nel ruolo di installatore.
- Scollegare i client (Web, OPC UA, altri controller) collegati al modulo.

Per informazioni su come installare e utilizzare lo strumento EcoStruxure™ Automation Device Maintenance, vedere la guida in linea (vedere *EcoStruxure Automation Device Maintenance, Strumento di aggiornamento firmware, Guida in linea*).

NOTA: lo strumento software Unity Loader™ di Schneider Electric non è utilizzabile per aggiornare il firmware del modulo BMENUA0100.

NOTA: dopo l'aggiornamento del firmware del modulo BMENUA0100 dalla versione 1.xx alla versione 2.xx quando BMENUA0100 è in modalità Standard, è necessario eseguire un'operazione di Security Reset, pagina 31 per ripristinare le impostazioni predefinite del modulo. Selezionare quindi una modalità operativa di sicurezza informatica, modalità Advanced (o Secured) o modalità Standard, per il modulo.

Download del firmware

È possibile eseguire il downgrade della versione firmware del modulo BMENUA0100, ad esempio dalla versione 1.1 alla versione 1.0. A questo scopo, dopo aver eseguito il downgrade della versione software mediante lo strumento EcoStruxure™ Automation Device Maintenance, eseguire un'operazione di Cybersecurity (o Security) Reset, pagina 31 per ripristinare le impostazioni predefinite del modulo. Selezionare quindi una modalità operativa di sicurezza informatica, modalità Advanced (o Secured) o modalità Standard, per il modulo.

Appendici

Contenuto della sezione

Connessioni del controller 172
Architetture di inoltro del servizio (IP)..... 173
Inoltro IP e comunicazione OPC UA 177
Script Windows IPsec..... 179
Impostazione di un'autorità di certificazione Windows 182

Connessioni del controller

Contenuto del capitolo

Connessioni da server OPC UA a controller 172

Connessioni da server OPC UA a controller

Connessioni aperte

Il numero di connessioni che possono essere aperte dal modulo BMENUA0100 con il controller M580 dipende dalla capacità del controller. Le prestazioni del modulo BMENUA0100 dipendono quindi dal tempo richiesto per eseguire il task MAST e dal controller selezionato. Il numero massimo di connessioni aperte da ciascun modulo BMENUA0100 con il controller M580 è il seguente:

Modello di controller	Numero massimo di connessioni aperte da ciascun 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

Architetture di inoltro del servizio (IP)

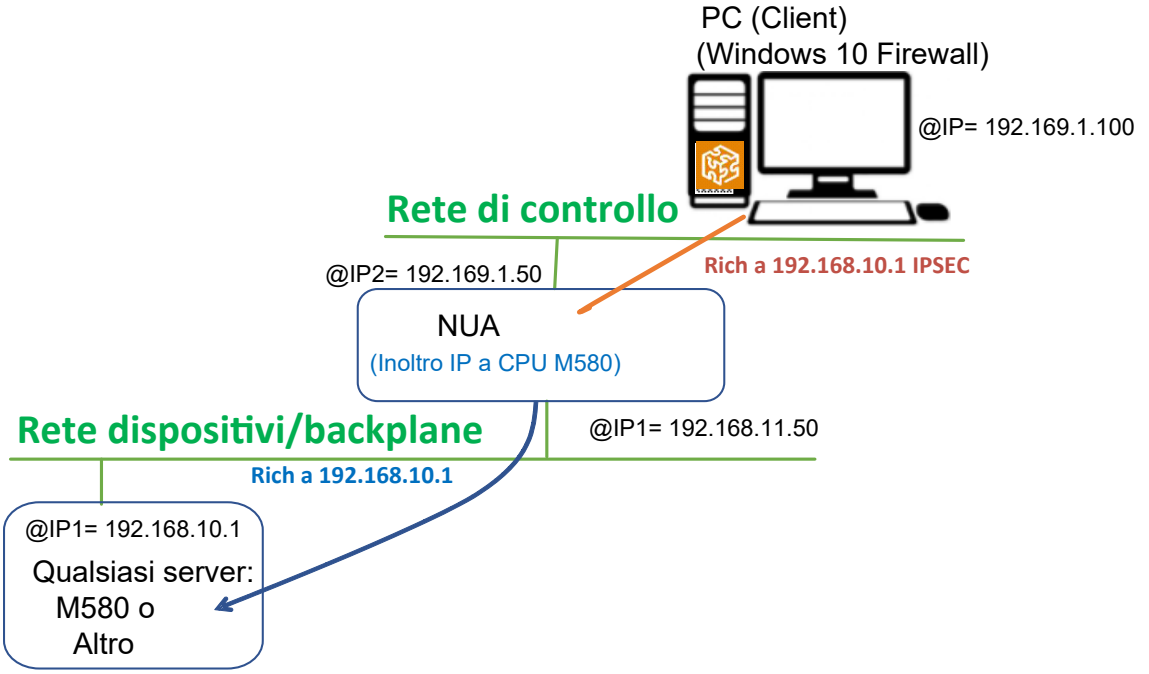
Contenuto del capitolo

Architetture supportate dal servizio di inoltro (IP) 173
Architetture non supportate dal servizio di inoltro (IP)..... 176

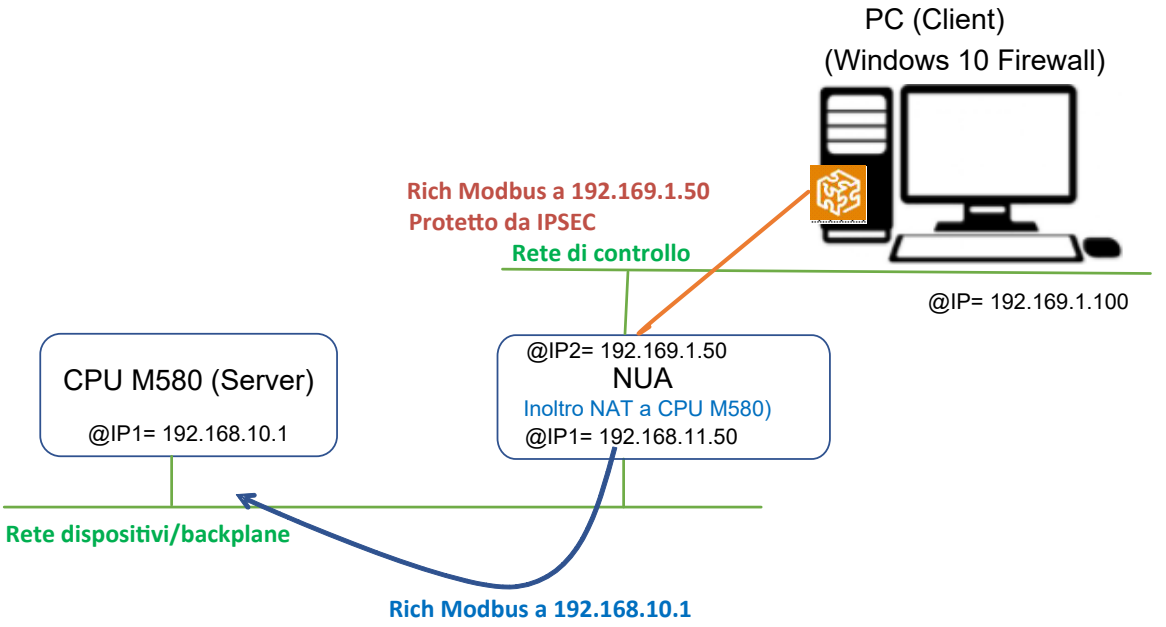
Questo capitolo presenta le architetture supportate e non supportate dalla funzione di inoltro del servizio (IP) del modulo BMENUA0100.

Architetture supportate dal servizio di inoltro (IP)

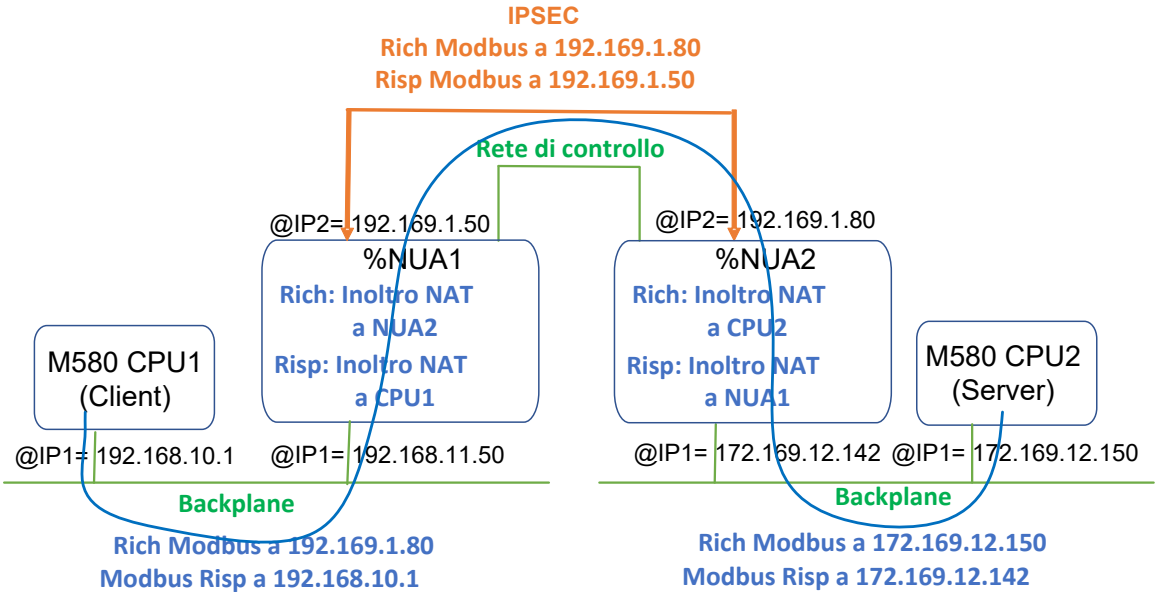
Inoltro IP da client Windows (rete di controllo) a qualsiasi client (rete backplane/dispositivo)



Inoltro NAT da client Windows (rete di controllo) a controller M580 (rete backplane/dispositivo)

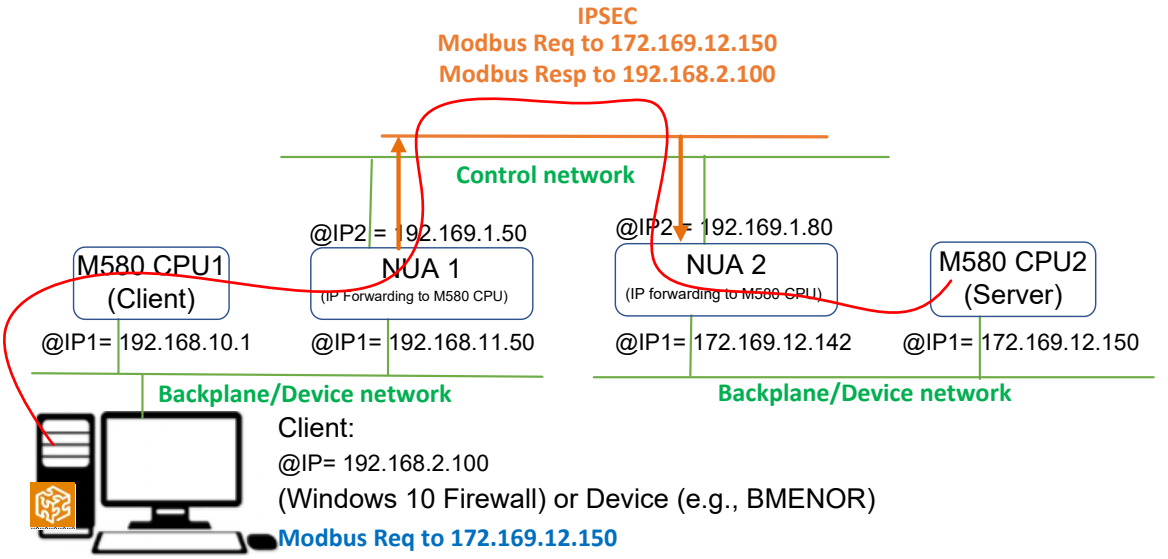


Inoltro NAT tra backplane per comunicazione da controller M580 a controller M580



Architetture non supportate dal servizio di inoltro (IP)

Inoltro IP tra backplane/reti di dispositivi



Inoltro IP e comunicazione OPC UA

Contenuto del capitolo

Impatto dell'inoltro IP sulle prestazioni 177
Inoltro IP e impatto di OPC UA sulle prestazioni 178

Inoltro IP e OPC UA sono in concorrenza per la larghezza di banda di comunicazione disponibile del modulo BMENUA0100. Questo capitolo contiene i risultati dei test delle prestazioni del modulo in cui viene utilizzato solo l'inoltro IP e quelle in cui vengono utilizzati l'inoltro IP e la comunicazione OPC UA.

Impatto dell'inoltro IP sulle prestazioni

Se è attivato solo l'inoltro IP e non la comunicazione OPC UA, l'impatto sulla larghezza di banda del modulo BMENUA0100 è il seguente:

IPsec	Riservatezza	Inoltro	Lunghezza frame (byte)	Larghezza di banda (kbyte/sec)
No	N/D	Inoltra tutto	1000	8800
No	N/D	Regola personalizzata	1000	10600
Sì	No	Inoltra tutto	1000	3400
Sì	No	Regola personalizzata	1000	4000
Sì	Sì	Inoltra tutto	1000	2600
Sì	Sì	Regola personalizzata	1000	2500

NOTA: questi valori sono presentati solo come esempio. Utilizzarli come stima dell'impatto dei diversi parametri (IPsec, Riservatezza, ecc.) sulle prestazioni. Le prestazioni effettive dipendono dall'infrastruttura specifica.

L'impatto sulla larghezza di banda viene visualizzato quando:

- È supportato solo il flusso di comunicazione di inoltro IP e non è incluso alcun flusso di comunicazione OPC UA.
- IPsec è utilizzato (IPsec = Sì) e non utilizzato (IPsec = No).
- I frame vengono firmati (Riservatezza = No) rispetto ai frame firmati e crittografati (Riservatezza = Sì) e viene utilizzato IPsec (in entrambi i casi).

- Le regole personalizzate per l'inoltro IP vengono applicate rispetto a Inoltra tutto.

  NOTA: La lunghezza dei frame incide solo leggermente sulle prestazioni globali.

Inoltro IP e impatto di OPC UA sulle prestazioni

Se sono attivati l'inoltro IP e la comunicazione OPC UA, l'impatto sulla larghezza di banda del modulo BMENUA0100 è il seguente:

Numero di elementi OPC UA monitorati per sottoscrizione	IPsec	Riservatezza	Inoltro	Larghezza di banda (kbyte/sec)
0	No	N/D	Regola personalizzata	10600
0	Sì	No	Regola personalizzata	4000
0	Sì	Sì	Regola personalizzata	2500
20000	No	N/D	Regola personalizzata	8800
20000	Sì	No	Regola personalizzata	2900
20000	Sì	Sì	Regola personalizzata	2000

NOTA: questi valori sono presentati solo come esempio. Utilizzarli come stima dell'impatto dei diversi parametri (IPsec, Riservatezza, ecc.) sulle prestazioni. Le prestazioni effettive dipendono dall'infrastruttura specifica.

L'impatto sulla larghezza di banda viene visualizzato quando:

- L'inoltro di tutti i pacchetti viene eseguito tramite la regola personalizzata (nessun Inoltra tutto).
- I flussi di comunicazione OPC UA non sono inclusi (numero di elementi OPC UA monitorati = 0) e inclusi (= 2000).

  NOTA: Il numero di elementi OPC UA monitorati ha un impatto limitato.

Script Windows IPsec

Contenuto del capitolo

Script di configurazione di Windows Firewall IKE/IPsec..... 179

Script di configurazione di Windows Firewall IKE/IPsec

Per eseguire IPsec su un PC che ospita il software di configurazione Control Expert o un client OPC UA (ad esempio SCADA), occorre aggiungere la configurazione di rete nel firewall host. Per ogni regola IPsec configurata nelle pagine Web, è possibile scaricare uno script associato (denominato IPSecWindowsConf.bat) utilizzando l'icona della ruota dentata. Eseguire questo script per impostare il firewall host nella configurazione.

- IKE/IPsec in modalità **trasporto** per i flussi dati locali al BMENUA0100.
- IKE/IPsec in modalità **tunnel** per i flussi di dati inoltrati al backplane Ethernet.
- Regole passthrough per HTTPS, OPCUA protetto e altri protocolli per cui **Utilizzo IPSEC** = FALSE.

Gli esempi seguenti presentano gli script di configurazione di Windows firewall con e senza confidenzialità IPsec.

In ciascun esempio di script, è necessario fornire i valori per le seguenti variabili:

- **`endpoint1`**: il valore dell'indirizzo IP remoto nella configurazione IPsec.
- **`endpoint2`**: indirizzo IP della porta di controllo BMENUA0100.
- **`Auth1psk`**: l'impostazione PSK nella configurazione IPsec.

Script di Windows Firewall con confidenzialità

NOTA: se la confidenzialità è attivata nella configurazione IPsec, utilizzare `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 di Windows Firewall senza confidenzialità

NOTA: se la confidenzialità non è attivata nella configurazione IPsec, utilizzare `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
```

Impostazione di un'autorità di certificazione Windows

Contenuto del capitolo

Passi preliminari 182
Cenni preliminari sull'installazione di Microsoft Windows Active Directory Certificate Server 183
Installazione di Active Directory Certificate Server (ADCS) 184
Applicazione del modello dell'Autorità di certificazione 206

In questo capitolo viene descritto come configurare un'Autorità di certificazione di Microsoft Windows™ da utilizzare in un sistema di autenticazione e autorizzazione utente a livello aziendale.

Passi preliminari

Di seguito vengono descritti gli elementi necessari e i passi preliminari da eseguire prima di installare il server dei certificati.

Elementi necessari

Sono necessari i seguenti elementi:

- Microsoft Windows™ Server Manager: è possibile scaricarlo dal sito Web Microsoft.
- Microsoft Windows Active Directory Certificate Server (ADCS): questo software commerciale è incluso come parte di Windows Server. Il modulo BMENUA0100 supporta le versioni server 2016 e 2019.
- Il file TemplatePackage.zip, che può essere scaricato da Schneider Electric.

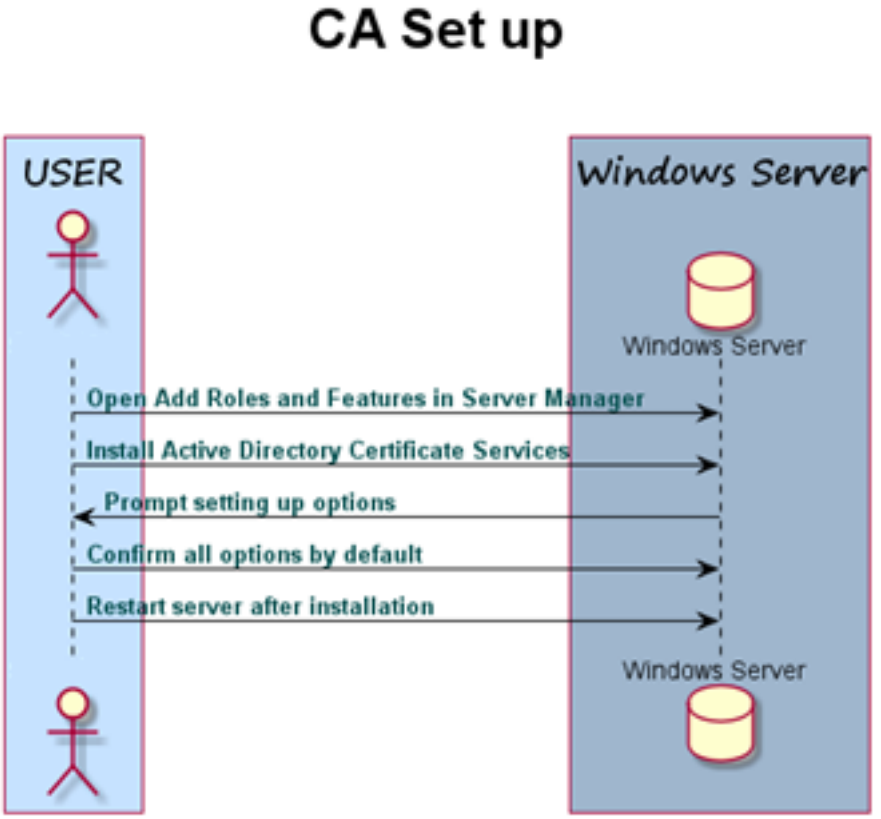
Installazioni software preliminari

Eseguire il file di installazione di Active Directory Certificate Server, quindi seguire i diversi passaggi richiesti per creare un account utente e una password.

Server Manager deve essere preinstallato sul PC host. In caso contrario, è possibile scaricarlo dal sito Web Microsoft.

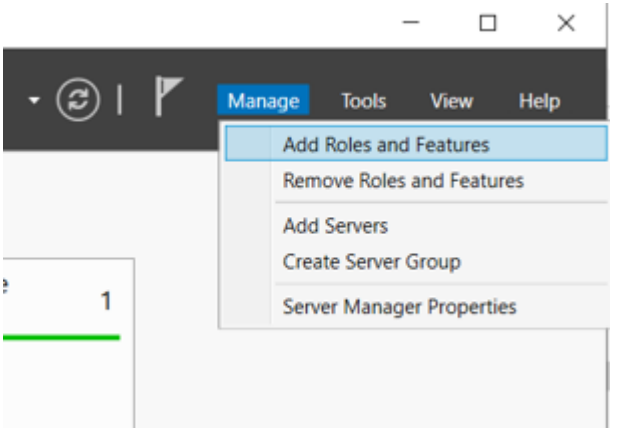
Cenni preliminari sull'installazione di Microsoft Windows Active Directory Certificate Server

Lo schema seguente presenta una panoramica del processo di configurazione dell'Autorità di certificazione (CA):

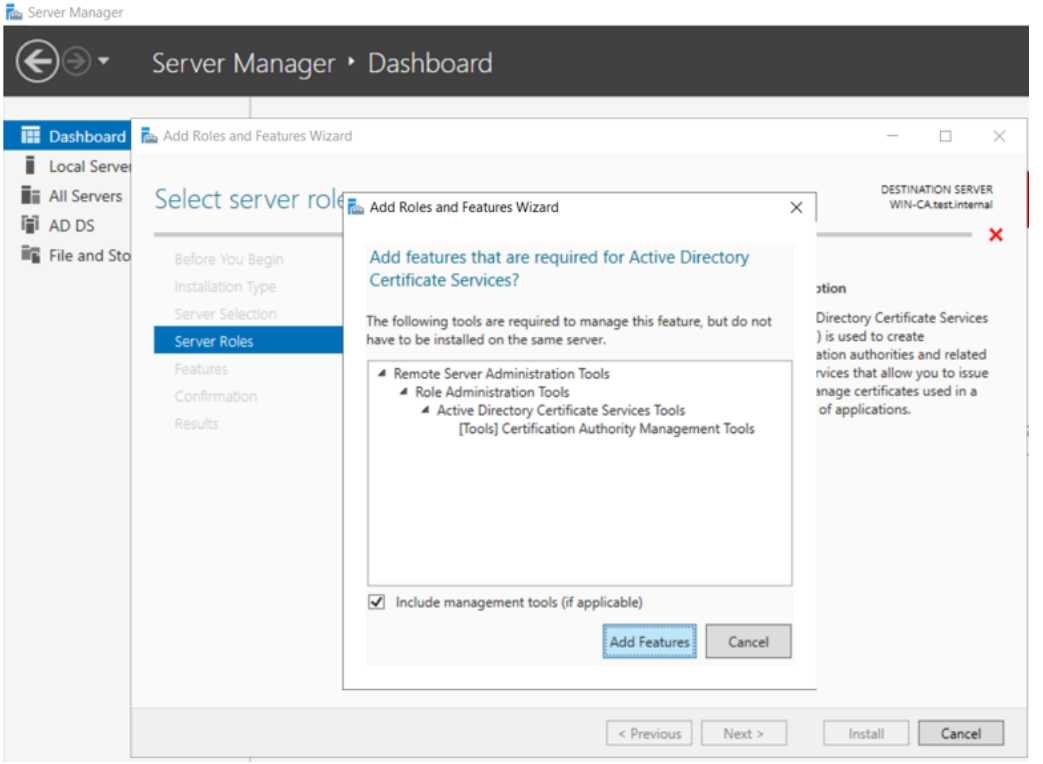


Installazione di Active Directory Certificate Server (ADCS)

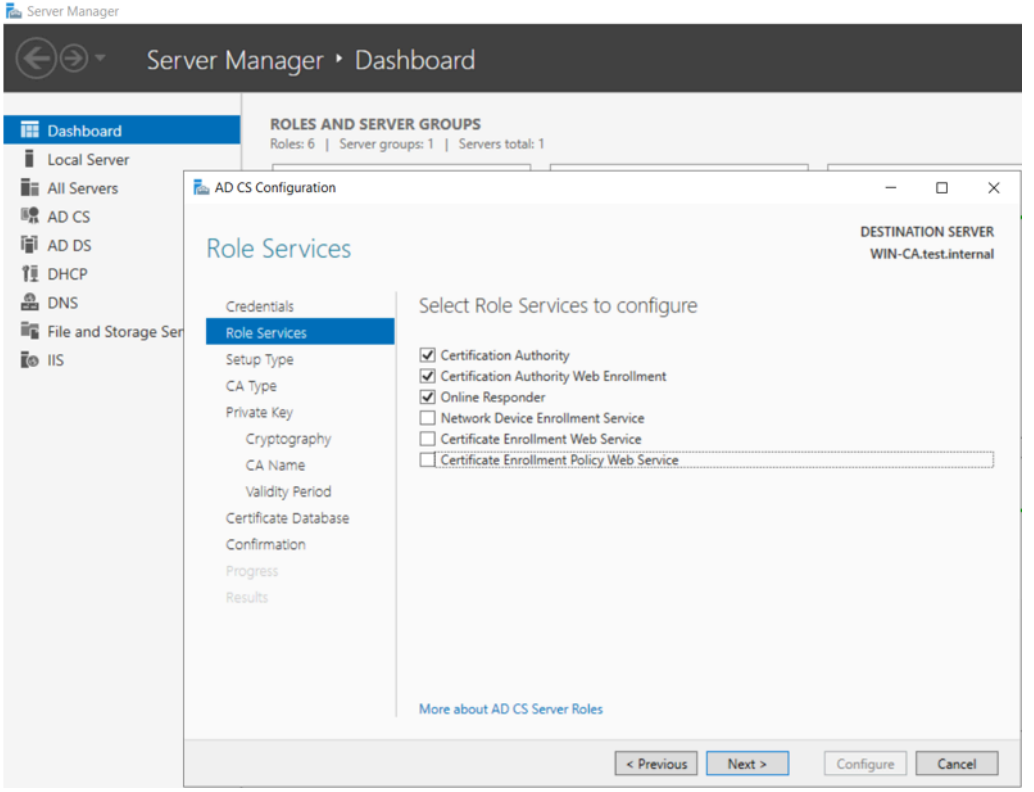
1. Avviare Microsoft Windows™ Server Manager e aprire il relativo dashboard.
2. Selezionare **Gestisci > Aggiungi ruoli e funzionalità**.



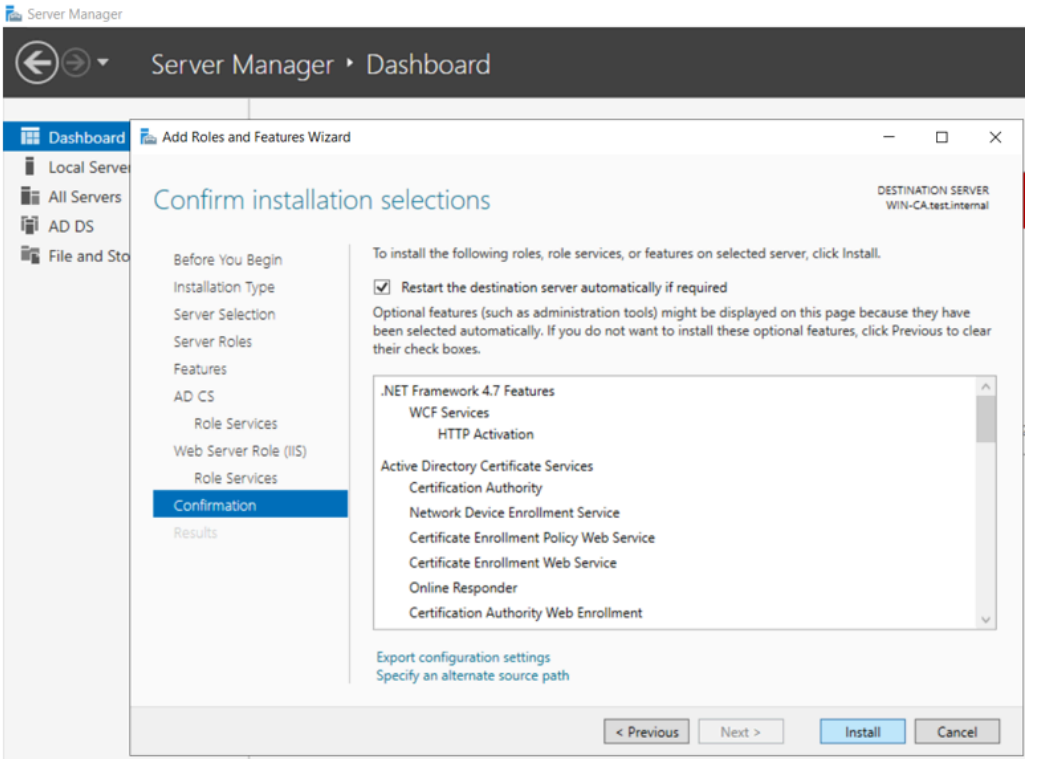
3. Aggiungere ruoli e funzionalità richiesti e includere gli strumenti di gestione:



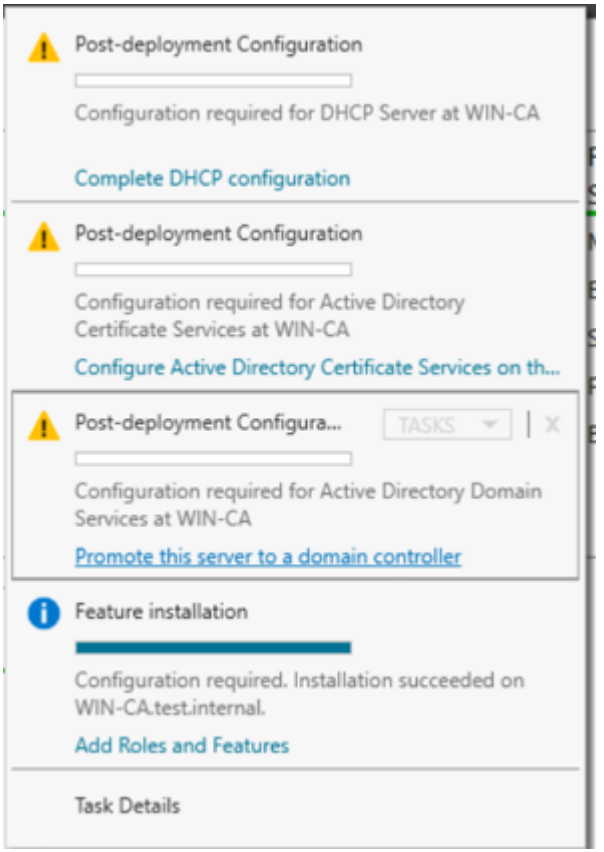
4. Selezionare i Servizi ruolo da configurare:



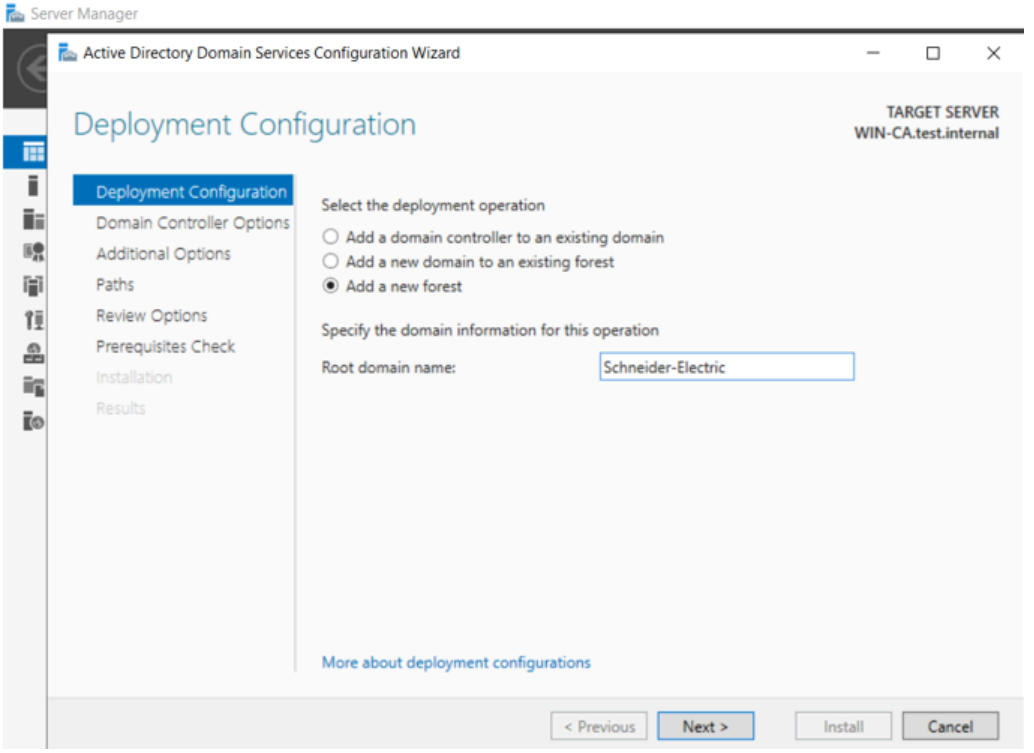
5. Confermare le selezioni di installazione:



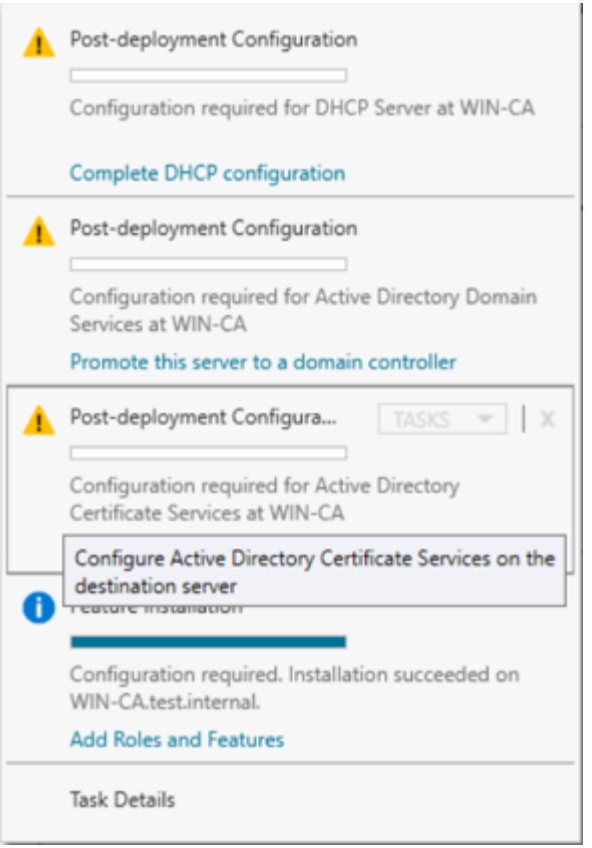
6. Fare clic su **Installa**. Server Manager visualizza l'avanzamento dell'installazione:



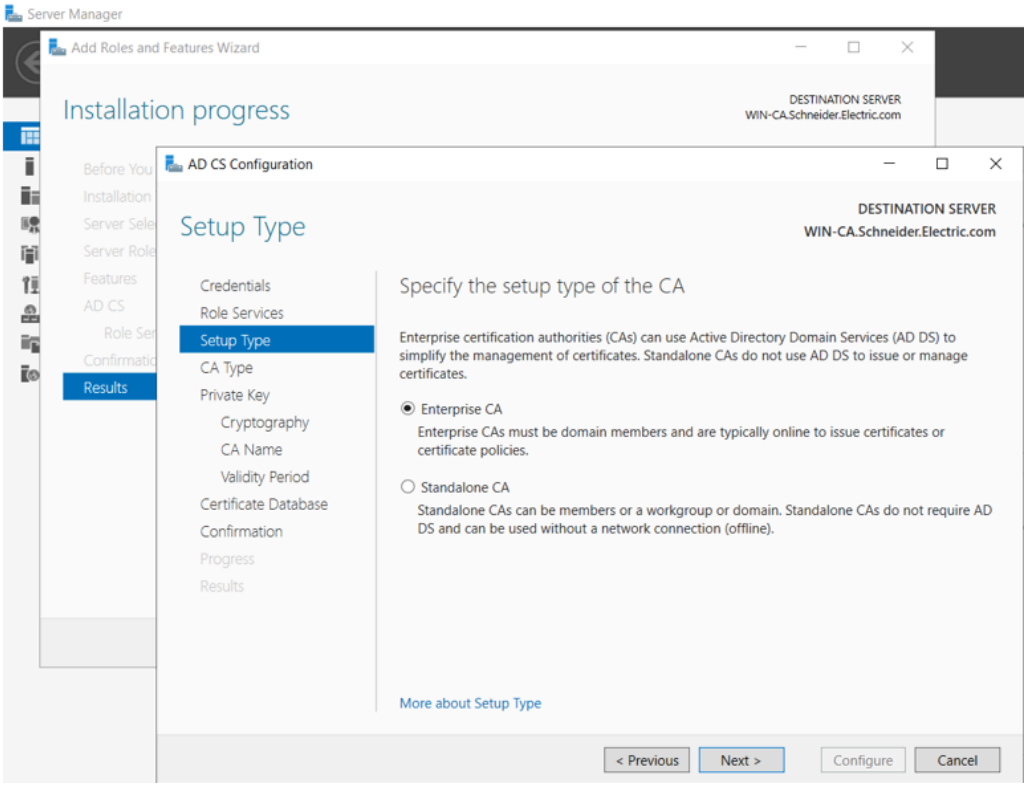
7. Selezionare l'operazione di distribuzione creando una nuova foresta o aggiungendo a una foresta esistente e specificare il dominio:



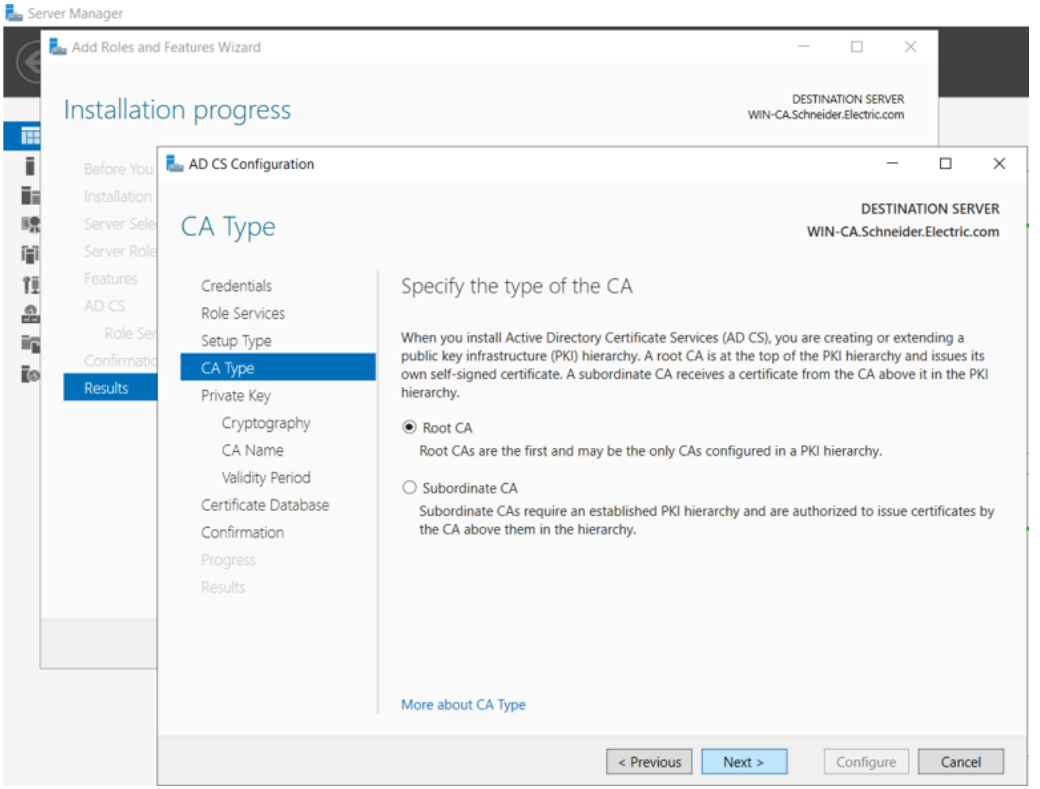
8. Server Manager visualizza le selezioni:



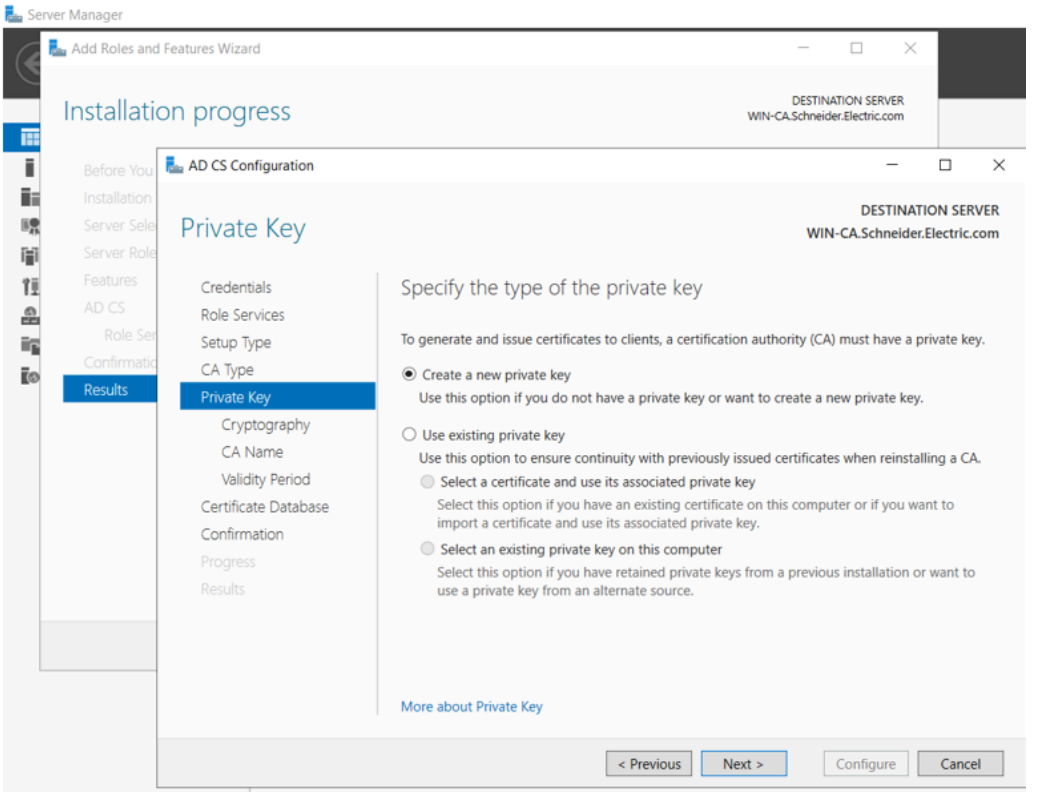
9. Specificare il tipo di CA da configurare:



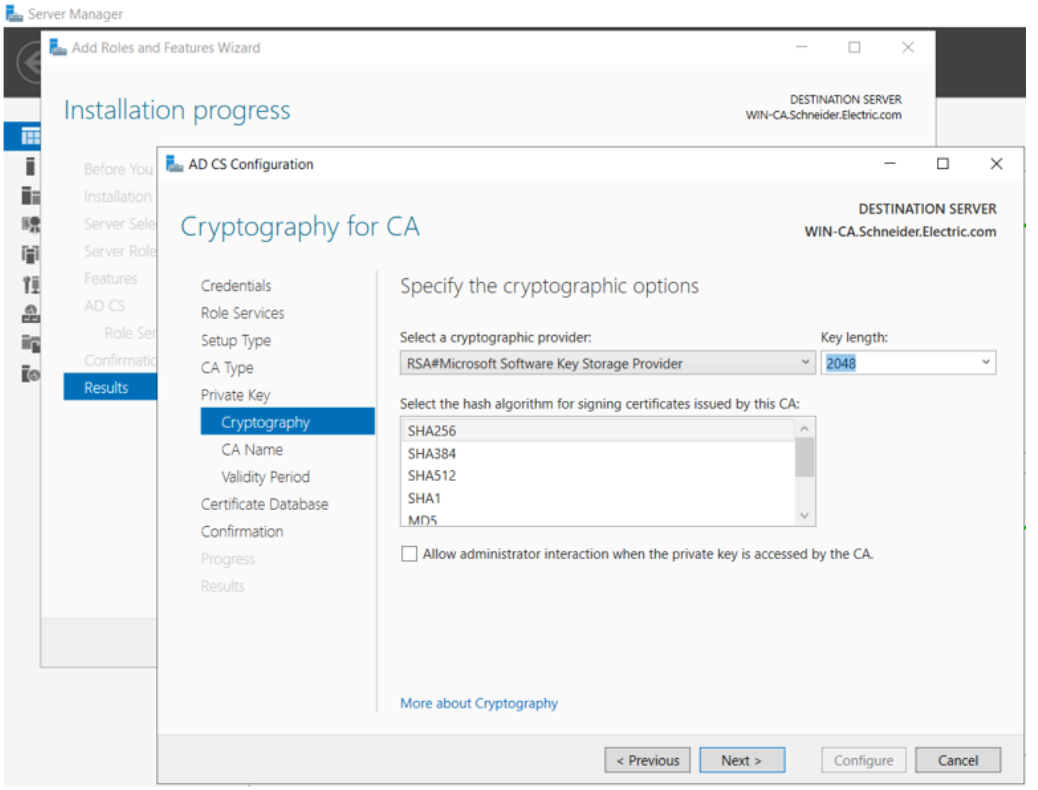
10. Specificare il tipo di CA:



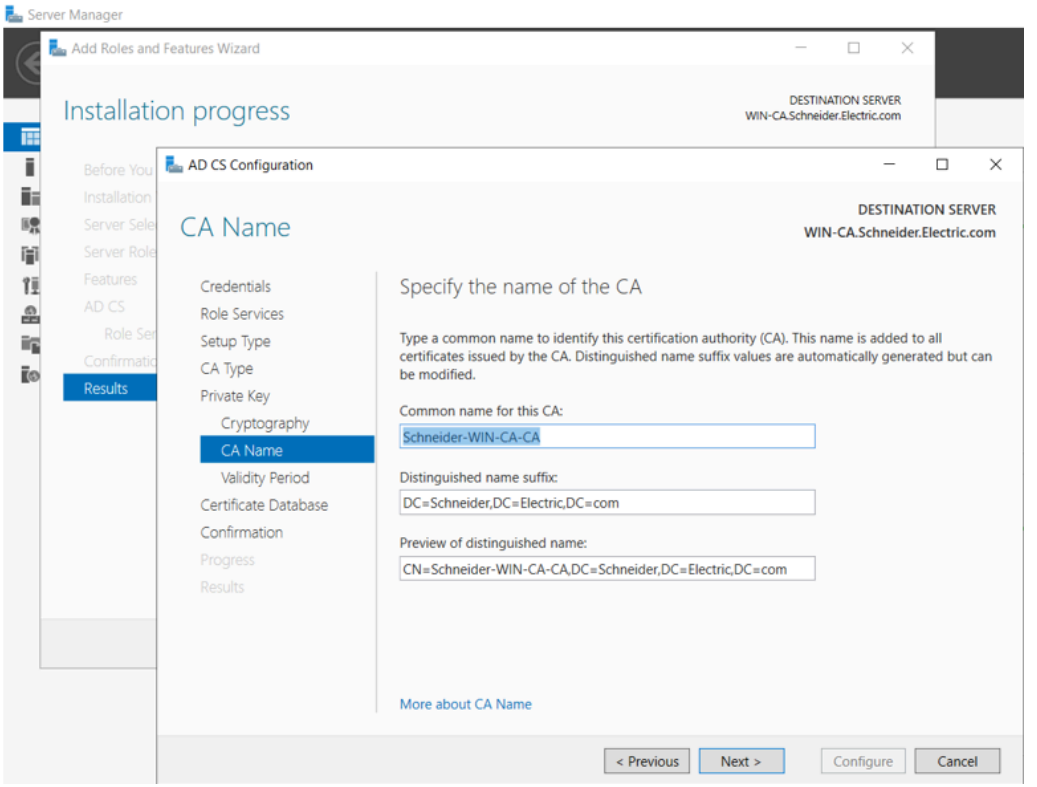
11. Specificare il tipo di chiave privata:



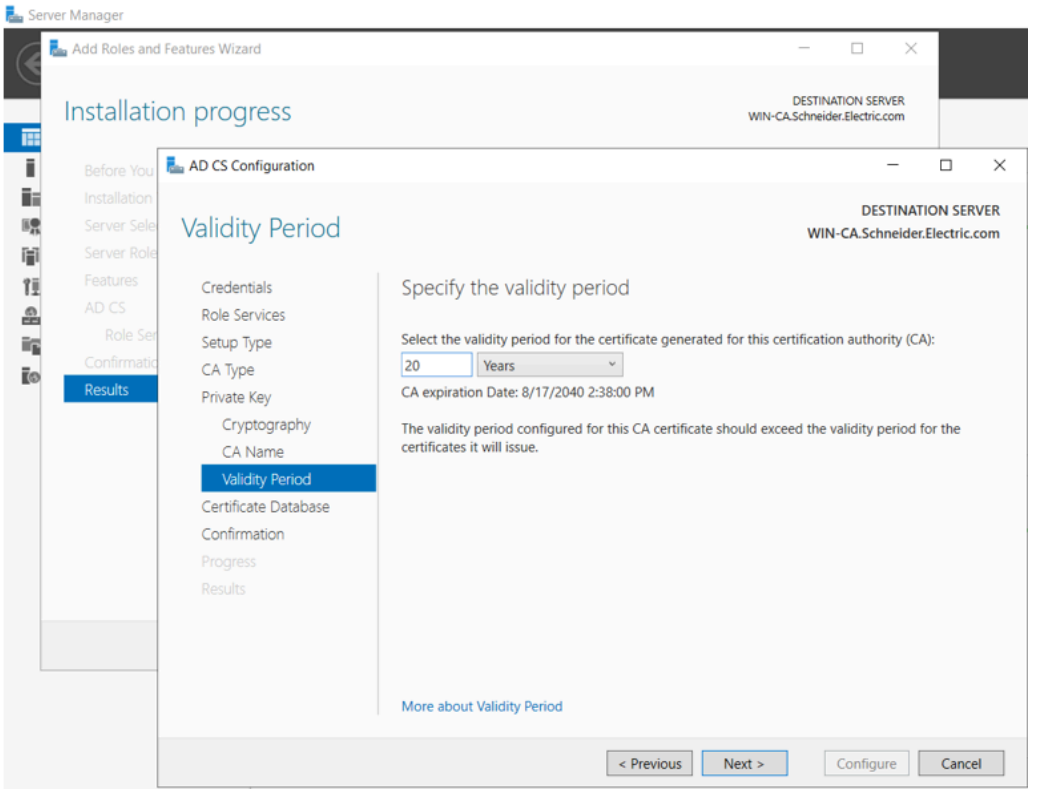
12. Specificare le selezioni di crittografia:



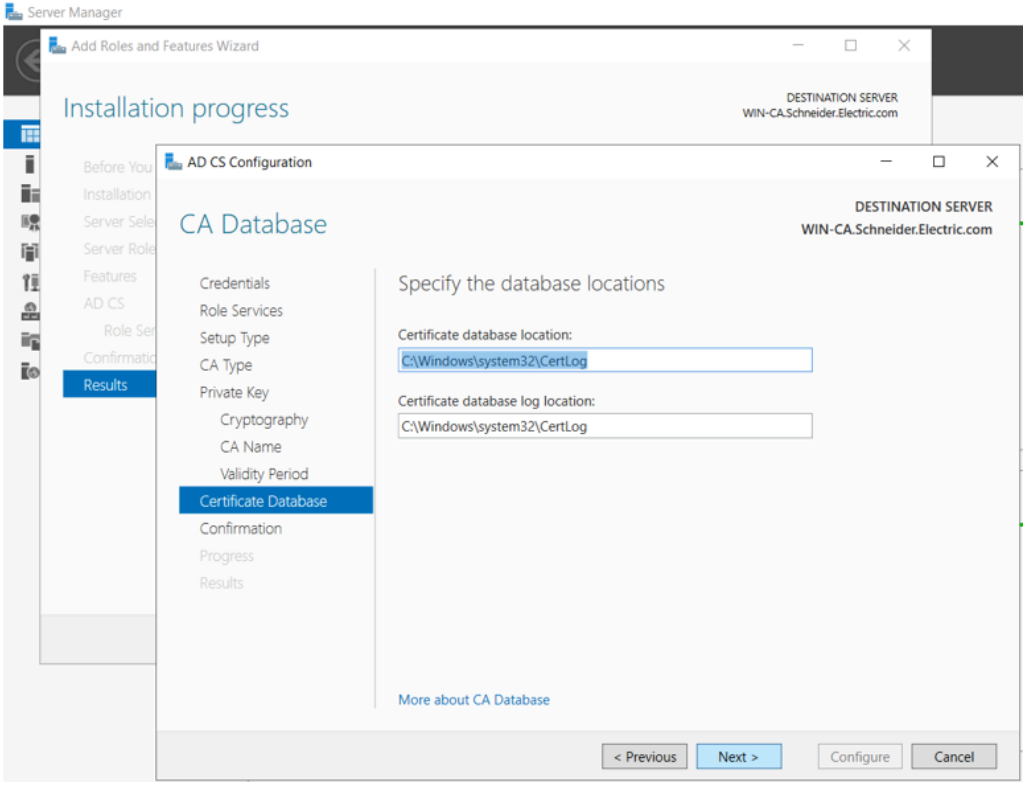
13. Specificare le selezioni di assegnazione dei nomi per la CA:



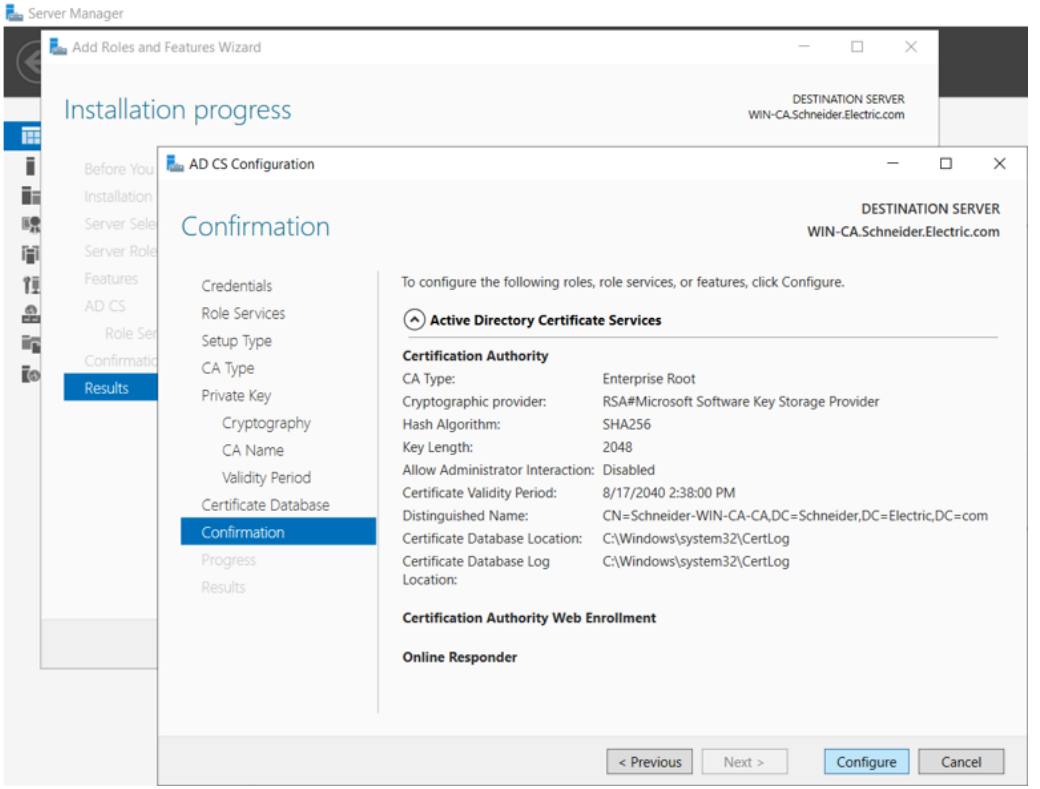
14. Specificare il periodo di validità. Il periodo di validità tipico di un certificato CA è di 5 anni:



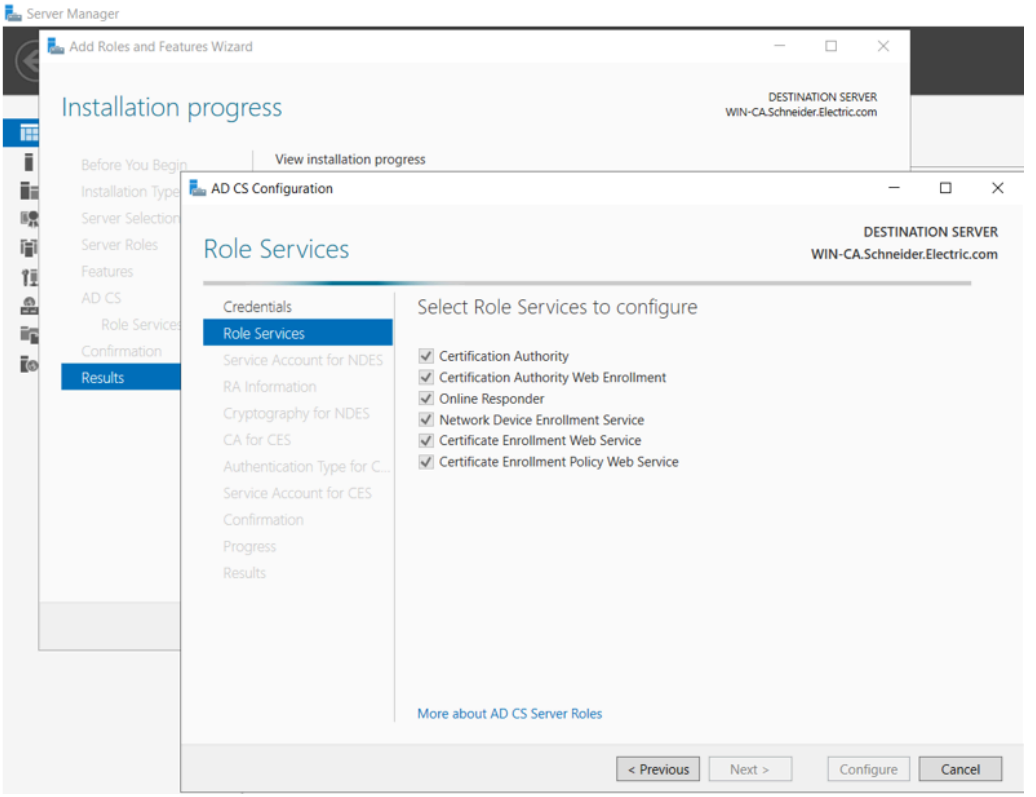
15. Specificare i percorsi del database di certificati e registro:



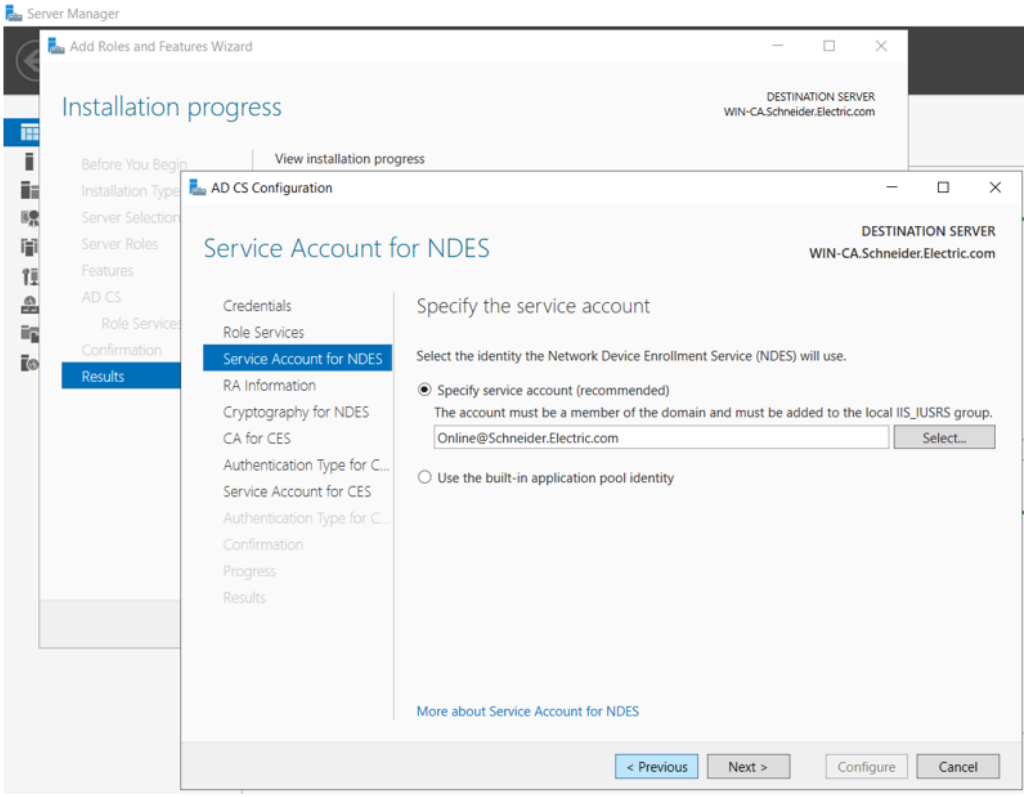
16. Confermare i Servizi certificati Active Directory selezionati e, se necessario, fare clic su **Configura**:



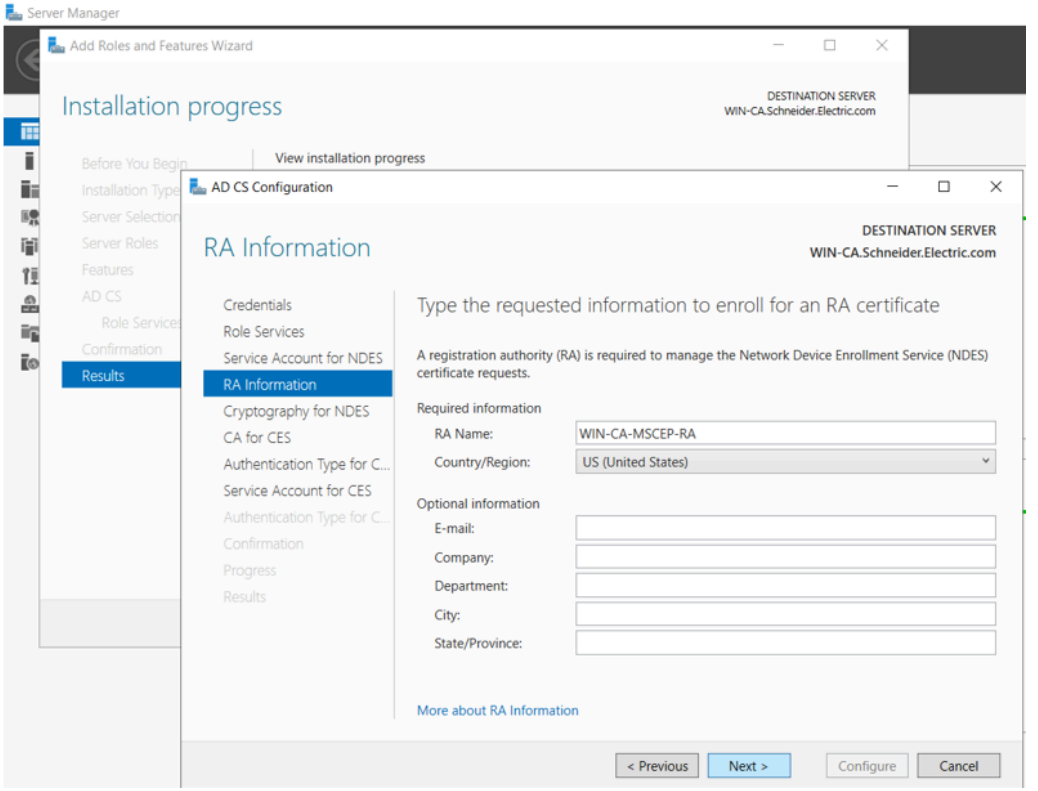
17. Selezionare i servizi ruolo da configurare:



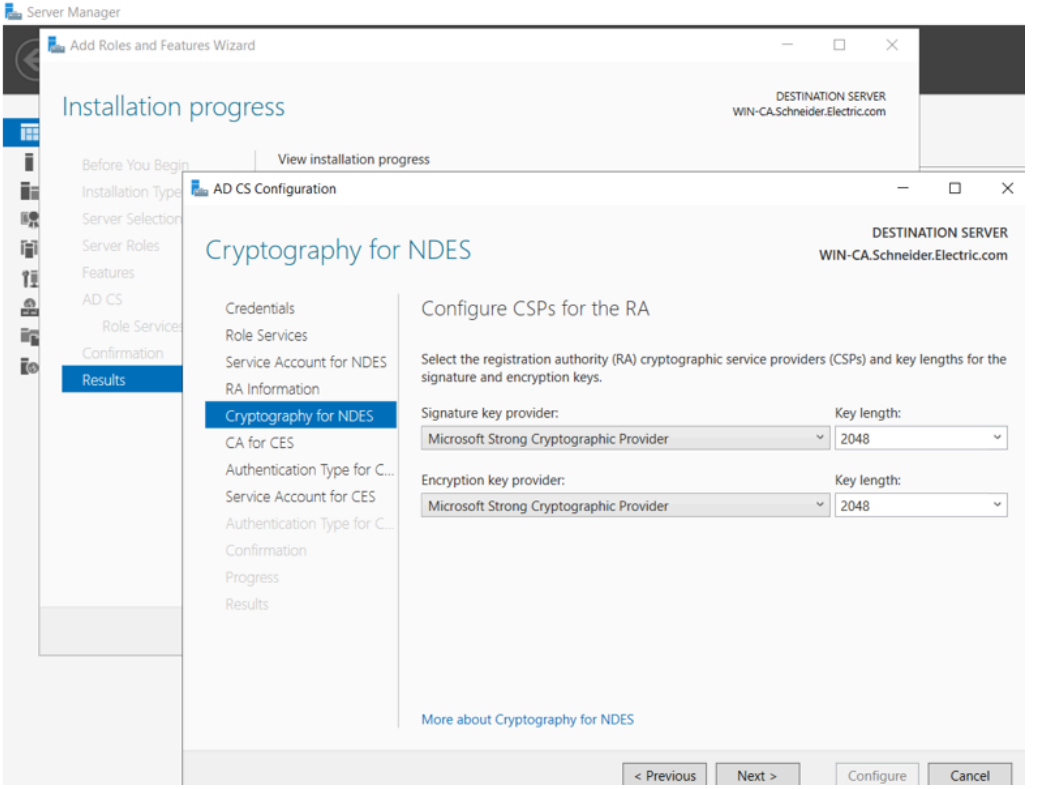
18. Specificare l'account del servizio:



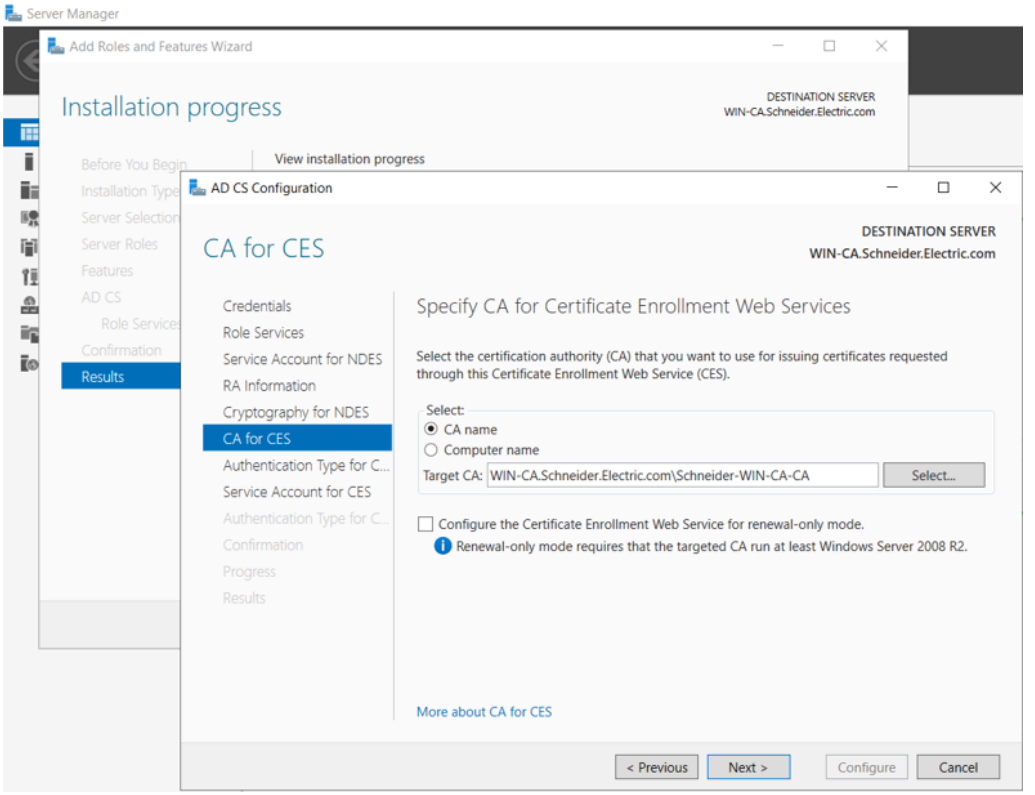
19. Immettere le informazioni da registrare per un certificato dell'Autorità di registrazione (RA):



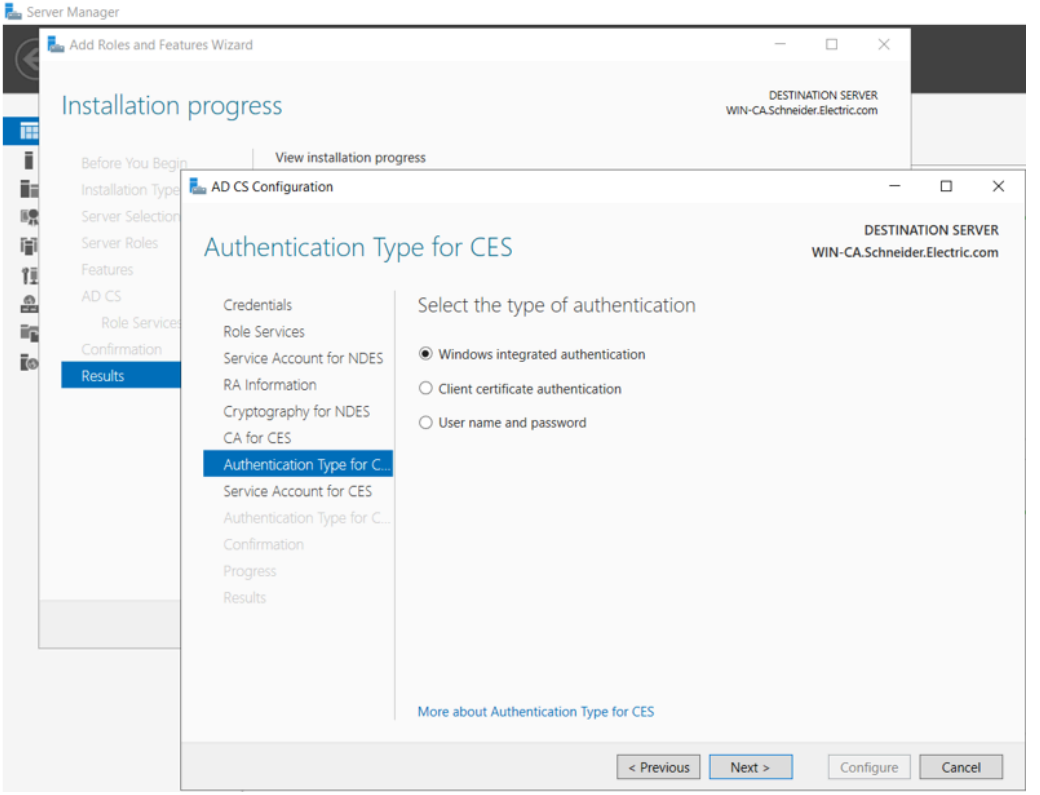
20. Selezionare le impostazioni di crittografia per l'RA:



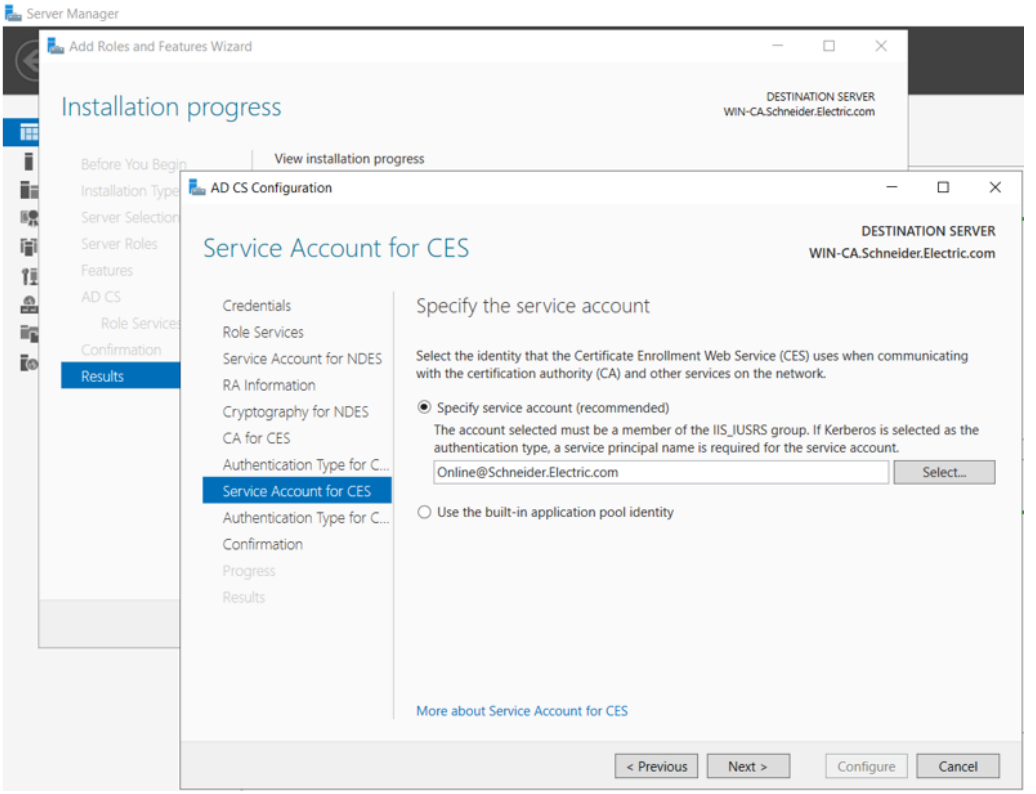
21. Specificare la CA per i servizi Web di registrazione certificati:



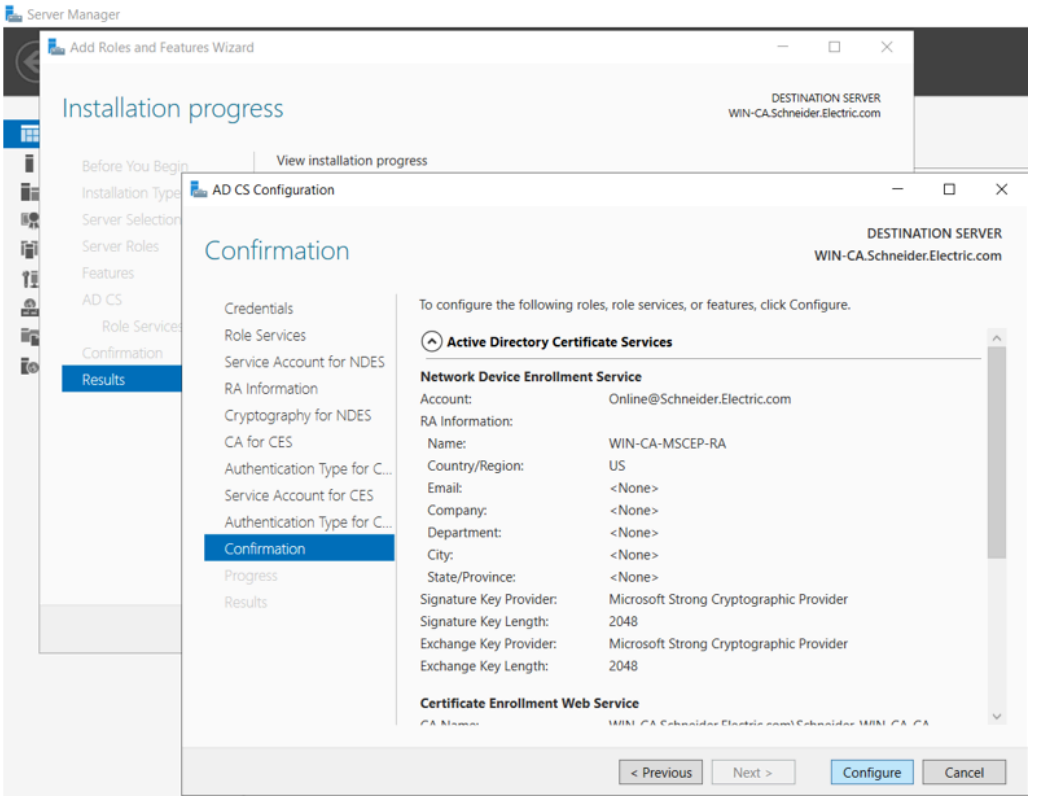
22. Selezionare un tipo di autenticazione:



23. Specificare l'account del servizio:



24. Confermare ruoli, servizi e funzionalità, quindi fare clic su **Configura**:



L'installazione di Active Directory Certificate Server è completata.

Applicazione del modello dell'Autorità di certificazione

L'ultima parte della configurazione di un'Autorità di certificazione di Microsoft Windows consiste nell'applicare il modello CA fornito da Schneider Electric.

Il modello e gli elementi di supporto sono contenuti nel file "TemplatePackage.zip" fornito da Schneider Electric.

Per applicare il certificato, seguire questa procedura:

1. Espandere il file "TemplatePackage.zip" e copiarne il contenuto (una cartella denominata "TemplatePackage" in un percorso diverso da C:\Windows\System32...

   Ad esempio, è possibile copiare questa cartella in "C:\Users\Administrator\Desktop\"

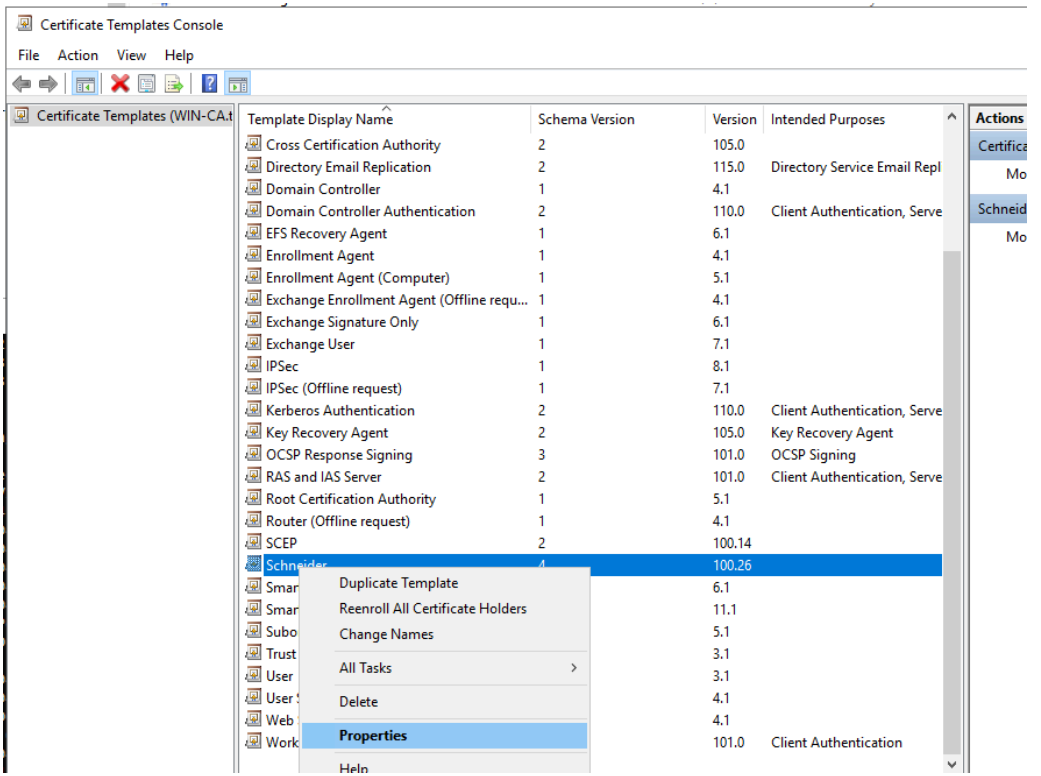
2. Avviare Microsoft Windows PowerShell (o un altro strumento di comando) come amministratore.
3. Passare alla cartella in cui è stata posizionata TemplatePackage, ad esempio:

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

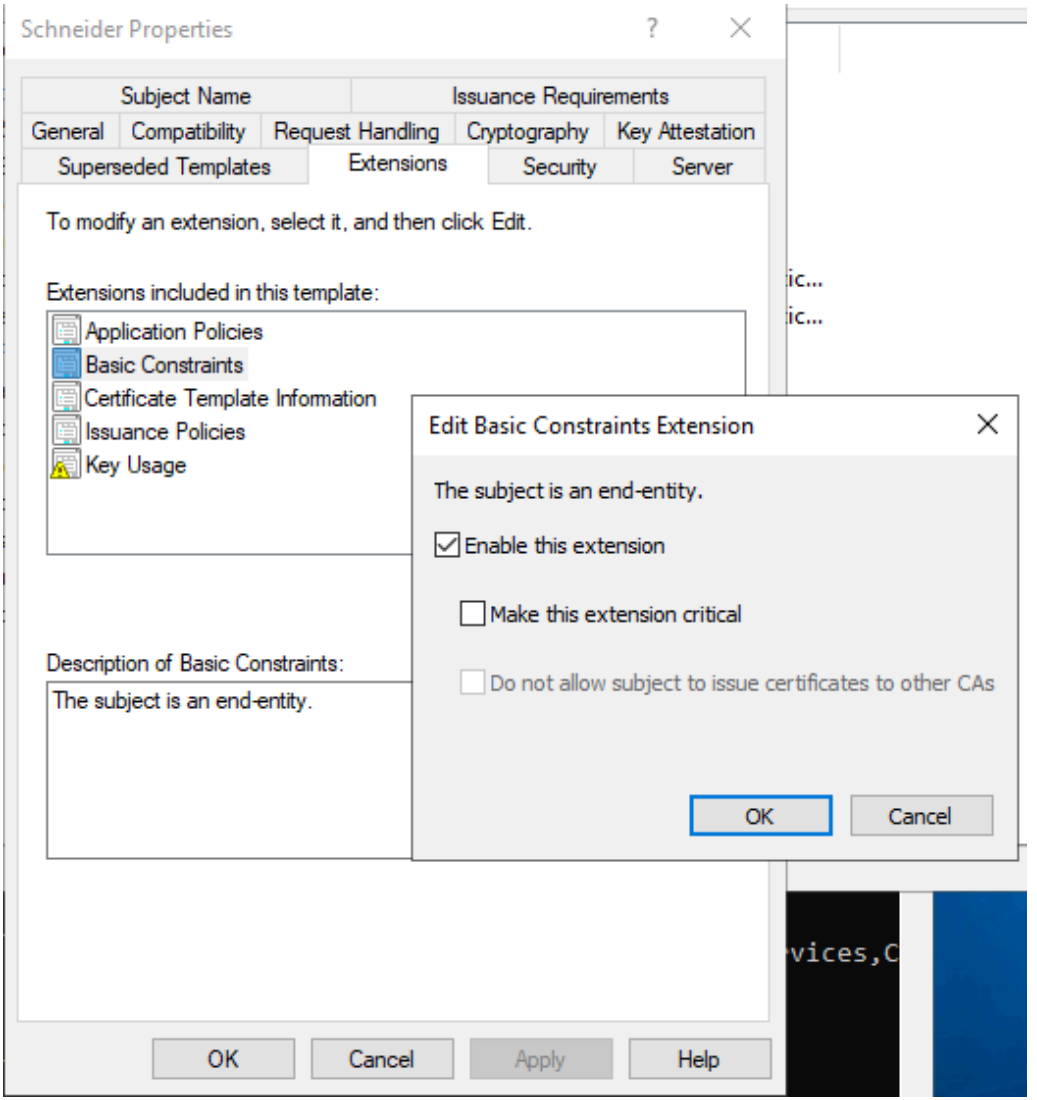
4. Eseguire il modello nella cartella TemplatePackage, come indicato di seguito:

   ```
   > .\ImportCertificateTemplate.ps1
   ```

5. Sul PC host, aprire la Console dei modelli di certificato, fare clic con il pulsante destro del mouse sul certificato Schneider, quindi selezionare **Proprietà**:



6. Nella finestra **Proprietà Schneider**, aprire la scheda **Estensioni**, fare doppio clic su **Limitazioni di base** e nella finestra di dialogo **Modifica estensione limitazioni di base** selezionare **Attiva l'estensione** e fare clic su **OK**:



Esecuzione della registrazione manuale

Per informazioni su come eseguire questa attività, vedere la sezione registrazione manuale dei certificati, pagina 110.

Fai clic sul link integrato in tale sezione per accedere a una presentazione video pratica.

Glossario

A

ambiente critico:

Resistenza a idrocarburi, oli industriali, detergenti e residui di saldatura. Umidità relativa fino a 100%, atmosfera salina, variazioni di temperatura significative, temperatura di funzionamento tra - 10°C e + 70°C o in installazioni mobili. Per i dispositivi rinforzati (H), l'umidità relativa arriva fino al 95% e la temperatura di funzionamento è compresa tra -25°C e + 70°C.

I

indirizzo IP:

Identificativo a 32 bit, formato da un indirizzo di rete e da un indirizzo host assegnato a un dispositivo collegato a una rete TCP/IP.

S

SNTP:

(*Simple network time protocol*) Vedere NTP.

T

trap:

Un trap è un evento generato da un agente SNMP che può indicare uno dei seguenti eventi:

- Una modifica avvenuta nello stato di un agente.
- Un dispositivo di gestione SNMP non autorizzato che ha tentato di recuperare dati da (o di modificare dati di) un agente SNMP.

Indice

A

architetture 61

B

BMENUA0100
  descrizione 19

C

CCOTF 63
certificazioni 26
compatibilità
  firmware del modulo e versioni software Control Expert 27
configurazione 86

D

DHCP-BOOTP
  M580, controller 133
diagnostica 134
  Modbus 158

F

firmware
  aggiornamento 169

H

HTTPS
  porta 443 61

I

inoltro IP 98

L

LED
  collegamento porta di controllo 25
  diagnostica 134
  Modulo 24
LED di stato sicurezza informatica 138

M

M580, controller
  configurazione sicurezza 132
messa in servizio 79–80
modalità operative 28

N

NTP
  configurazione 126
numero massimo di moduli per rack 63

P

pagine Web 86
porte 19
posizionamento del modulo
  rete piana 62

R

READ_DDT 144
rete piana
  posizionamento del modulo 62

S

selettore a rotazione 23
sincronizzazione dell'ora
  configurazione 126
SNMP, agente 129
standard 26

T

T_BMENUA0100 DDT 139

T_CYBERSECIURITY_STATUS DDT 143
T_FW_VERSION DDT 143
T_OPCUA_STATUS DDT 140
TFTP
  M580, controller 133
T_SERVICES_STATUS DDT 141

W

Web, pagine
  home page 91

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Poiché gli standard, le specifiche tecniche e la progettazione possono cambiare di tanto in tanto, si prega di chiedere conferma delle informazioni fornite nella presente pubblicazione.

PHA83353.03