Technical documentation

JACE Redundant Instruction Manuals

v1.5

powered by niagara framework®

Niagara JACE Redundant

Tridium, Inc.
3951 Westerre Parkway, Suite 350
Richmond, Virginia 23233
U.S.A.

Confidentiality

Trademark notice

Copyright and patent notice

Catalogue

Background

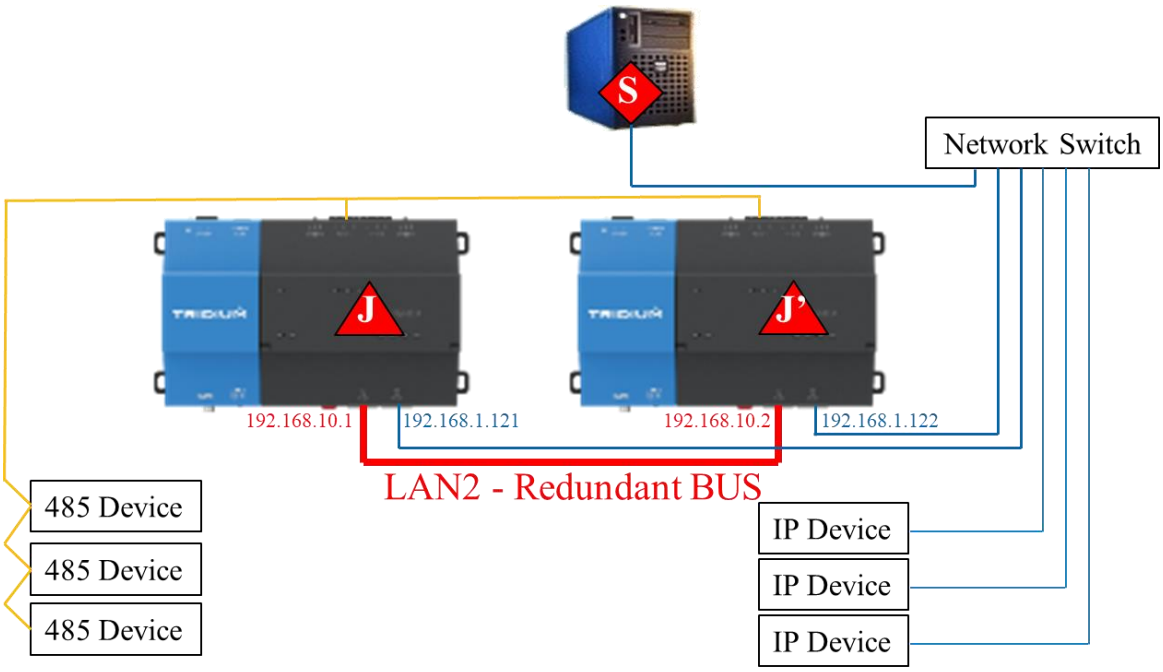
In the era of big data, the reliability and stability of data systems are important, especially in data centers, airport projects, and industrial projects. The goal of these project leaders is to ensure that the equipment can operate continuously under any circumstances, but each platform may encounter problems that cause downtime, such as hardware failures or software errors in the organization's internal deployment, which will result in loss of revenue and loss of customers or other consequences. The easiest way to deal with these failures is the redundancy technology, which allows administrators to achieve system reliability through backup, replication, and other measures to minimize the impact of failures on user services.

Niagara's application projects have many real-time requirements for the network, such as finance, securities, aviation, and some enterprise users. Their networks are not allowed to fail. Once the network fails, it will bring huge economic losses. Therefore, we should provide users with redundant networks. JACE is an important network device, which can realize redundancy of the network through backup and ensure the smooth flow of the network.

Network Architecture

JACE redundancy uses Primary&Secondary to implement redundant data communication. The Primary sends a data request message, then the Secondary can send data to the primary to respond to the request after receiving the correct message. The Primary can also directly send messages to modify the data on the Secondary to achieve bidirectional read and write.

The network architecture diagram of JACE redundancy is shown in the figure below. JACE J is the Primary, JACE J' is the Secondary, J and J' are mutually redundant. They have identical sites and identical connections, and the only difference between them is the IP address.



Under normal conditions, J is responsible for collecting data, communicating with S, and implementing control logic; J' obtains all the data of J through the redundant bus, and all the links of J' networks and proxy points are in the disabled state.

J and J' are directly connected through the second network port, which is called ‘redundant bus’. Both sides use the timing heartbeat to ensure that the partner site is online, and the recovery mechanism of J is realized through the heartbeat.

When the heartbeat between J' and J fails, the communication between S and J fails, but the communication between J' and S is ok, then J' will enable its all Networks and Links. Ultimately J' takes over J.

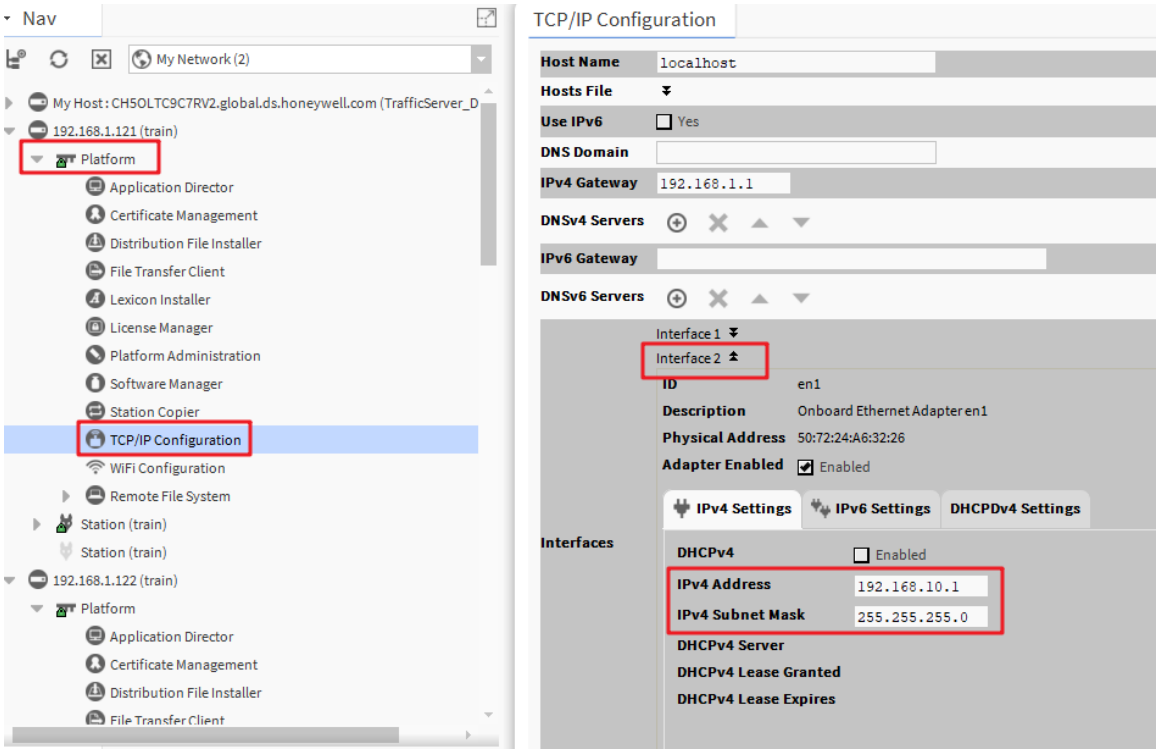
Configuration

The configuration of Primary and Secondary stations

- First copy the redundant-rt.jar to the modules in the Niagara installation;
- Require redundancy feature license;
- Launch Workbench and connect to the platforms of the Primary and Secondary stations respectively, then install the above redundancy modules for the Primary and Secondary stations through Software Manager;
- Restart the Primary and Secondary stations;

Configure LAN2 of two JACEs

Open TCP/IP Configuration under Platform, then click the drop-down arrow on the right side of Interface2 to enable and set the IPv4 address and subnet mask of LAN2.



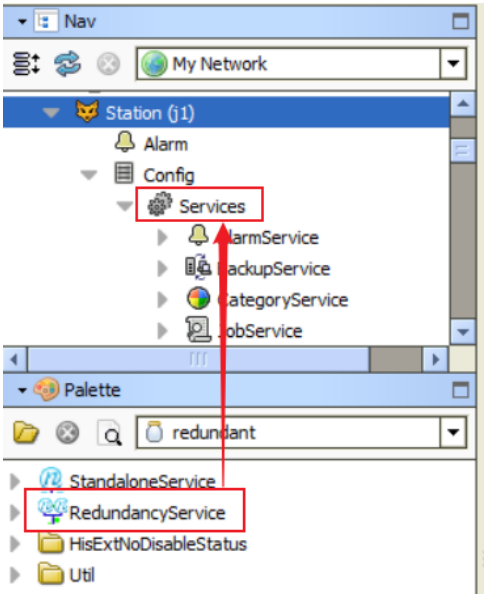
Note:

It is necessary to force the IP address of the LAN2 port of the primary and secondary stations to be in the same network segment. The last segment of the IP address of the LAN2 port of the primary station is 1, and the last segment of the IP address of the LAN2 port of the secondary station is 2. For example, the IP address of the primary station LAN2 is 192.168.10.1, and the IP address of the secondary station LAN2 is 192.168.10.2.

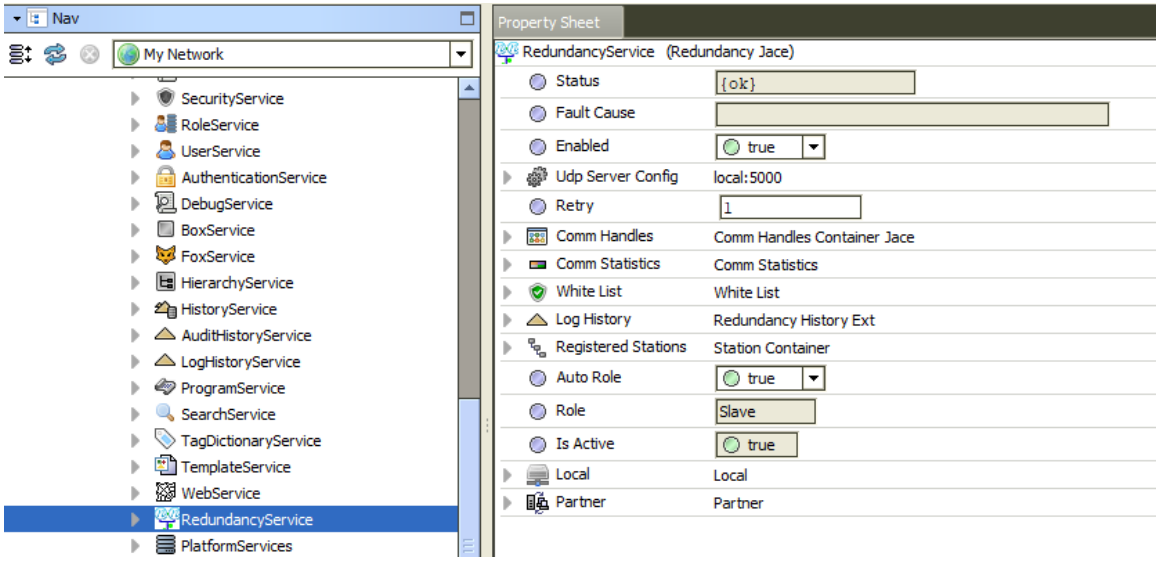
Two network cards of the same device cannot be in the same network segment.

Configure Redundant JACE Service

1. Select redundant in Palette and drag&drop RedundancyService to Services under Config.



2. Configure parameters related to RedundancyService.



Note: On JACE-8000, we suggest to configure only on the primary JACE station, and configure true for AutoRole of RedundancyService, configure true for Local.AutoGetIp, and configure true for Partner.AutoGetIp. After all configurations (including Network, Logics, Px pages, etc.) are processed, copy the primary station to the computer through station copier, and then copy the station to the secondary JACE station, to ensure the consistency of the station to the greatest extent.

Configure Supervisor

- First copy the redundant-rt.jar to the modules in the Niagara installation;
- Require redundancy feature license;
- Restart the Primary and Secondary stations;

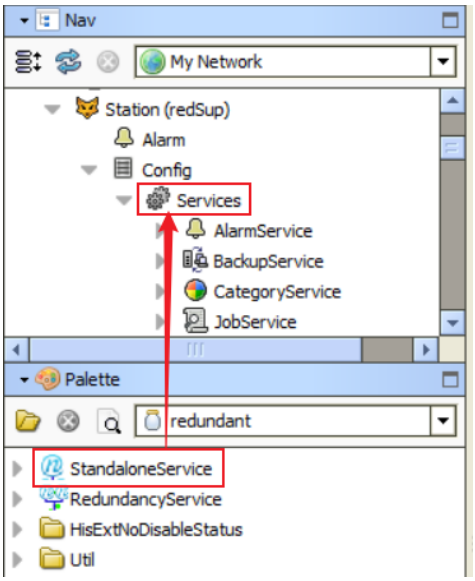
Configure connection between Supervisor and primary/secondary JACE

It is recommended to use unencrypted fox connections.

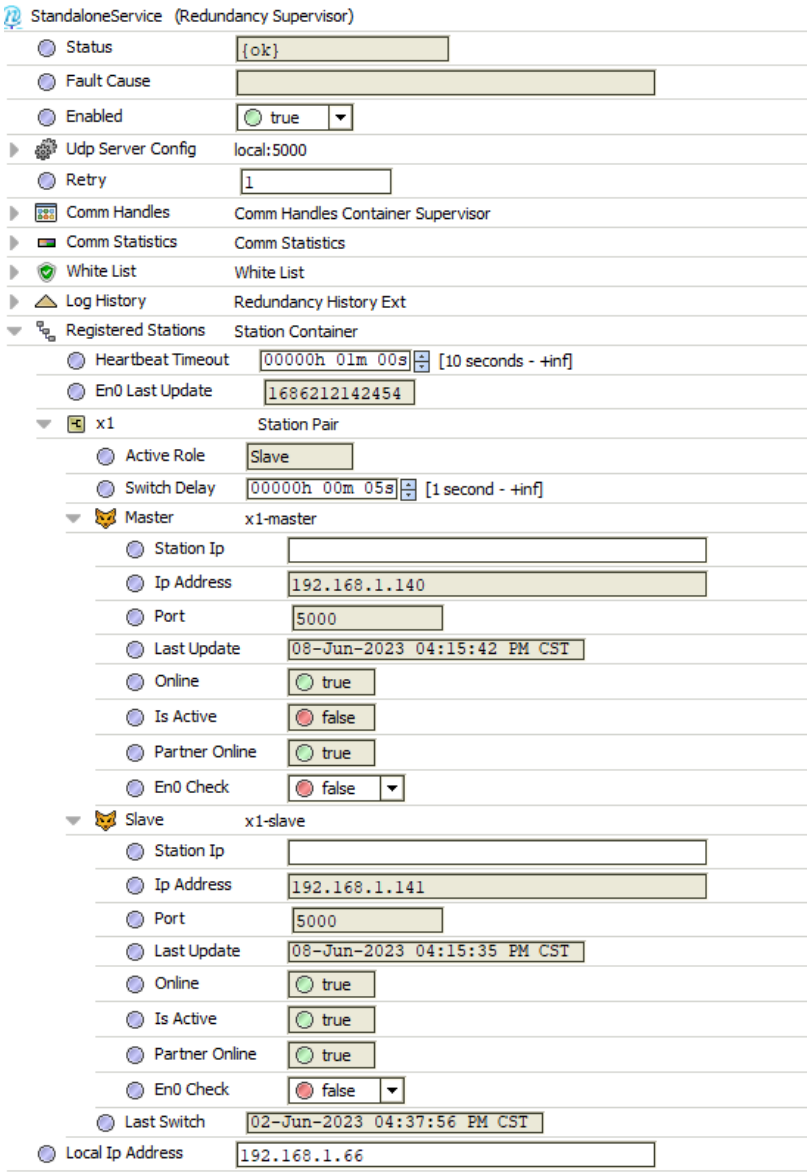
Refer to Appendix: Connection between Supervisor with primary or secondary JACE station

Configure Redundant Supervisor Service

1. Select the redundant palette and add the StandaloneService to the Config>Services.



2. Double-click on StandaloneService, you can see the following configuration information, where Jace Udp Port is set to 5000, Registered Stations automatically adds the primary and secondary JACE stations named x1 to the list and displays the status information of these JACE stations.



Configuration considerations

Before configuring, make sure:

1. The primary and secondary JACE stations should be completely consistent. After copying the primary station to the supervisor workbench user home, then copy it to the secondary through Station Copier to ensure the consistency of the primary and secondary JACE sites (see Appendix for the station duplication process);
2. The IP addresses of the primary and secondary JACE stations and the Supervisor station need to be pingable to each other. For example, the IP address of the LAN1 port of the primary station is 192.168.1.121, the IP address of the LAN1 port of the

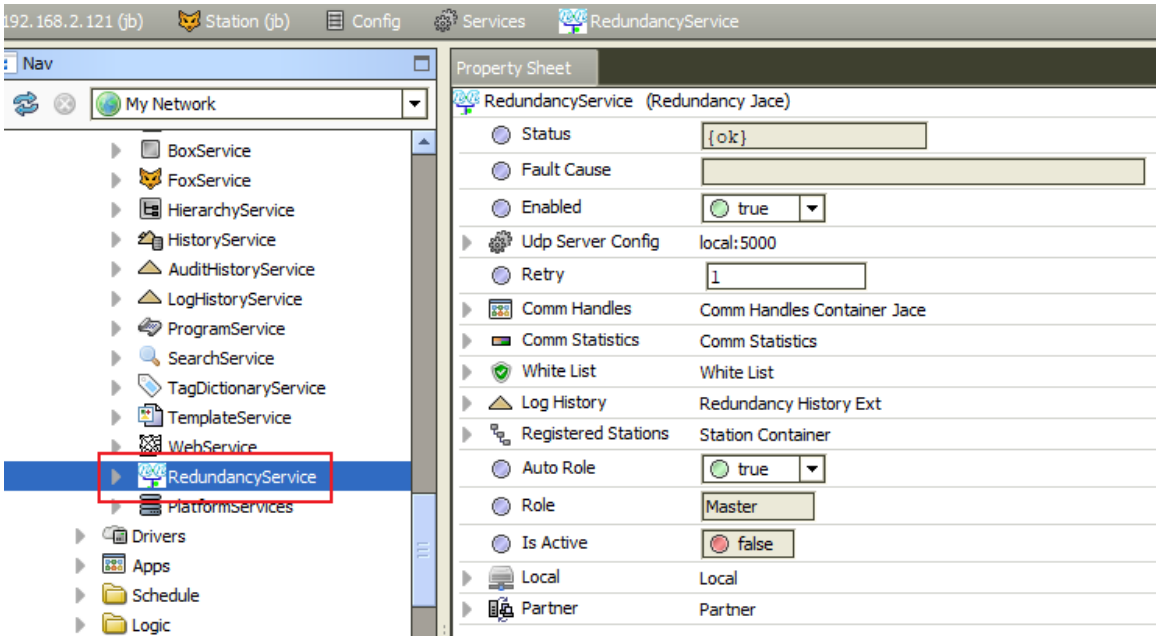
secondary station is 192.168.1.122, and the IP address of the local Supervisor station is 192.168.1.11;

3. When the primary and secondary JACE stations connect to the device through the BACnet MS/TP, the MAC address of the device cannot be 1. That is because the MAC address of the JACE where the primary station is located is 0, and the MAC address of the JACE where the secondary station is located is 1, and the MAC address of the device can be set to a number greater than or equal to 1, if the MAC address of the device is also 1, the repetition of the MAC address on the same bus will cause the secondary to drop frequently.
4. An NTP clock source is required, which is usually configured on the computer where the Supervisor station is located. The primary and secondary JACE stations should configure the NTP client service to ensure the primary and secondary station time synchronization;
5. Make sure that the UDP 5000 port of the computer firewall where the Supervisor station is located is to be opened (see Appendix 5.2 for details on firewall settings).
6. After the primary and secondary JACE stations are configured, both need to be restarted.

Components

Redundancy Service

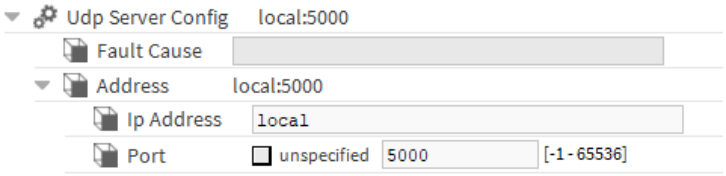
The following is an explanation of the relevant configuration of the Redundancy JACE Service in the Primary site:



Status: Show the status of the current JACE station;

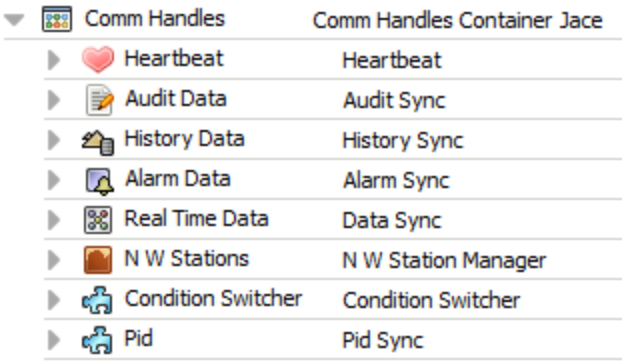
Enabled: Enable the service;

Udp Serve Config: Used to configure the IP address and port of the Udp server, just use the default value;

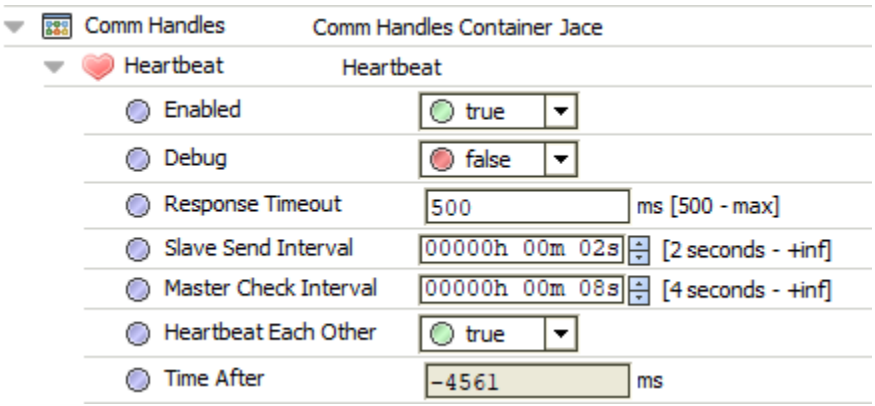


Retry: Configure the number of retries when communication fails

Comm Handles:



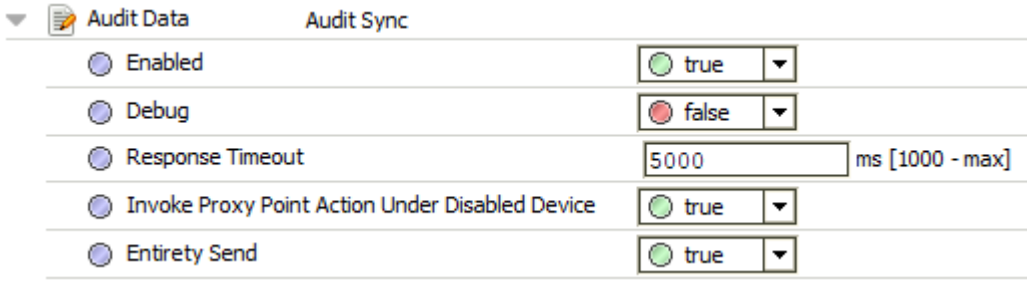
- **Heartbeat**: Set the relevant properties of the heartbeat



  - Enabled: Enable the functionality;
  - Debug: Print debugging information, used with DebugService configuration;
  - Response Timeout: Response timeout, in milliseconds;
  - Slave Send Interval: The time interval for sending the heartbeat command to Partner. The setting in the above figure indicates that the heartbeat command is sent every 2 seconds, and the minimum can be set to 2 seconds; if other messages are received within the configured time interval, such as real-time data synchronization, it is not necessary to send heartbeat;
  - Master Check Interval: The time interval for checking whether the Partner has sent data, which is set to 8 seconds in the figure, means checking whether the message sent by the Partner is received every 8 seconds, if not, the Partner is considered offline;
  - Heartbeat Each Other: Configure to send heartbeat messages to each other. It is recommended to set it to true. If it is false, only the standby JACE sends heartbeats to the active JACE;

- Time After: Displays the time difference with the partner site, a positive number indicates that the remote time is greater (later), and a negative number indicates that the remote time is smaller;

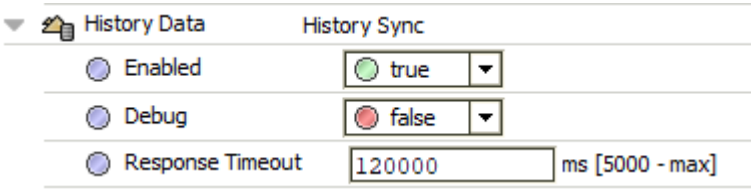
- **Audit Data**: Operation Synchronization



- Enabled: Enable the functionality;
- Debug: Print debugging information, used with DebugService configuration;
- Response Timeout: Response timeout, in milliseconds;
- Invoke Proxy Point Action Under Disabled Device: The Device of the standby JACE is in the Disabled state. If it is set to true, it means that the Action of the proxy point under the Disabled Device on the main JACE is also executed synchronously on the standby JACE.

  Note: some drivers may cause the point state to become Fault or Disabled;
- Entirety Send: When adding a complex component, whether it should be transmitted at one time as a whole or multiple times in layers, the default is one time transmission as a whole;

- **History Data**: The synchronization of historical data



When the station is started, the synchronization of historical data is performed. The process is as follows:

(1) Stop all active history extensions to prevent the station from recording historical data, resulting in the inability to insert old history;

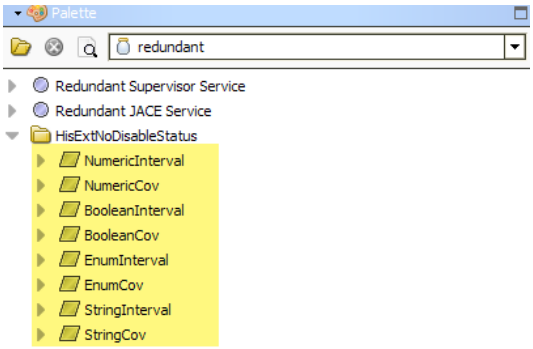
(2) Query the history of the partner station, send all the historical extensions' Ord and the time of the last history of the current station to the partner (the receiving process is too large, it may be sent multiple times), and query the number of historical extensions of the partner and the time of its history, when the partner's

historical data is newer, send back the partner's Ord and the last history of the time, and update to their own time;

(3) Obtain the history of the partner station, query each historical extension in turn, query the history database of the partner and send the historical data, and the current station will write the obtaining historical data into the local history database. If there is too many histories, multiple communication is required;

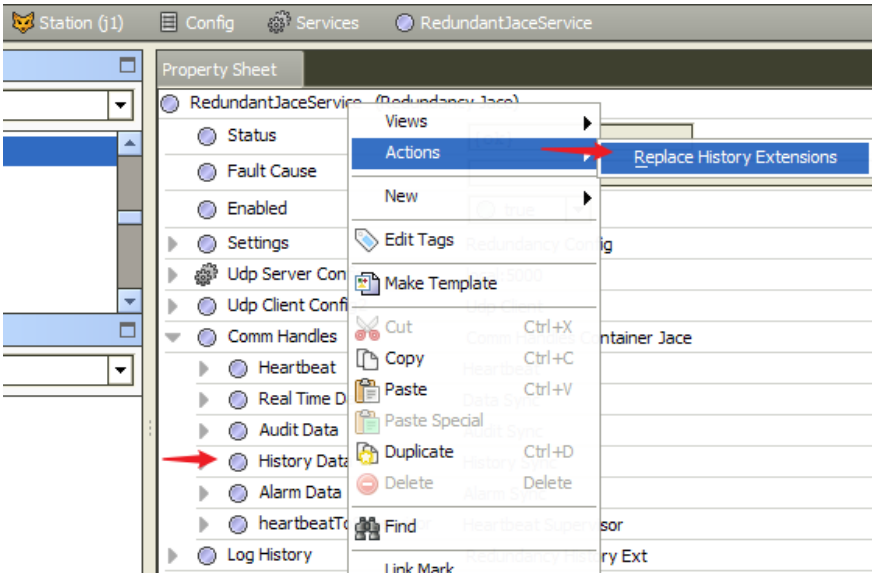
(4) Activate all historical extensions of the current station after updating the history database.

The data status of the secondary JACE changes briefly when the primary and secondary switchover occurs. And the status of disabled appears in a short time. You can use the redundancy history exts in the palette to avoid the problem. As shown in the following figure:



If the standard history extensions are configured in the station, you can perform batch update by invoking historyData's Action: 'Replace History Extensions'.

The results of the operation can be viewed in the Platform / Application Director view.



INFO [14:38:29 15-Feb-20 CST][redundancy.his] Replaced history extensions: 1
slot:/Drivers/ModbusTcpNetwork/Modbus%20Tcp%20Device1/points/Numeric%20Writable1/NumericInterval

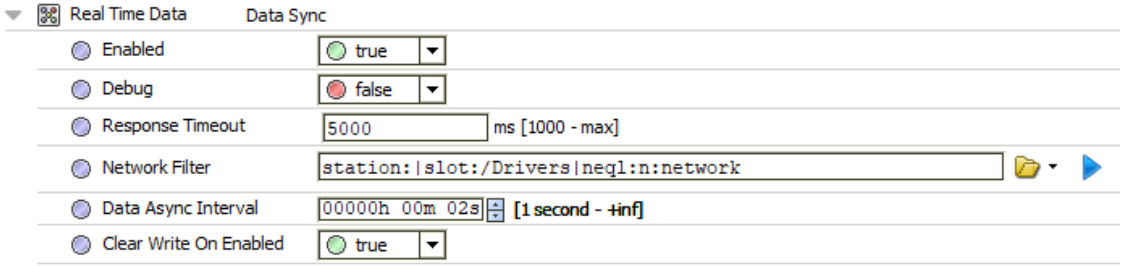
- **Alarm Data**: The synchronization of alarm data

  When the station starts up, it starts to perform the synchronization of alarm data. The process is as follows:

  (1) Query the alarm list of the partner station, send the time of the last alarm record of the current station, and query the last alarm time of the partner station and obtain the alarm uuid array of the partner station.

  (2) Obtain the alarm record of the specified time in the partner station and update the local alarm database of the current station.

- **Real Time Data**: Proxy Point Synchronization Configuration



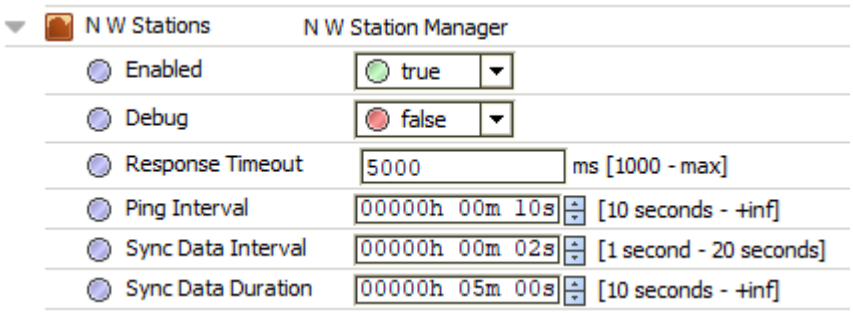
  - Network Filter: Used to filter the Network in which the proxy point that requires real-time data synchronization;
  - Data Async Interval: The time interval for data synchronization is set to 2 seconds in the figure, and the minimum can be set to 1 second;

- Clear Write On Enabled: If this attribute is set to true, the flag of the secondary will be cleared, that is, the Write On Enabled attribute of all its networks will be set to false. This is because the secondary sets all devices to disabled by default. When the data is synchronized, the write operation of the writable point under the secondary will fail, and the state of the point will become fault, resulting in a large number of write error messages. To avoid this, you need to set Clear Write On Enabled to true.

Note:

When the proxy point in the primary station does not update the data, the status of the proxy point in the secondary station is disabled. Only the proxy point's data in the primary station changes, and the corresponding proxy point in the secondary station updates the data, the status of the proxy point changes from disabled to ok at this time.

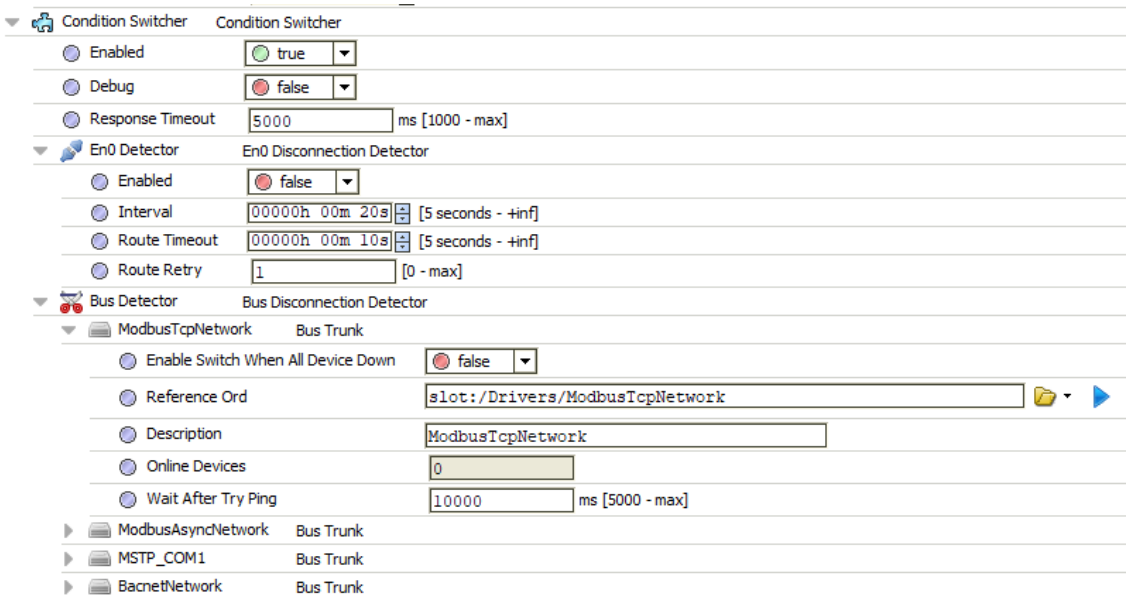
- **NW Stations**:



- Enabled: Enable the functionality;
- Debug: Whether to print debugging information, it needs to be used with DebugService configuration;
- Response Timeout: Response timeout, in milliseconds;
- Ping Interval: The interval for pinging the sites under NiagaraNetwork. Note that it is different from Station.ping, but the ping implemented by the redundancy function itself. You can get some information about the site and display it under RedundancyService/Registered Stations;
- Sync Data Interval: During the redundant site switching process, the IP of the station under NiagaraNetwork will be switched accordingly. This process may take a while, so set a Sync Data Duration. During this period, data synchronization will be performed at the Sync Data Interval cycle instead of NiagaraNetwork The proxy point synchronization;

- Sync Data Duration: See Sync Data Interval above;

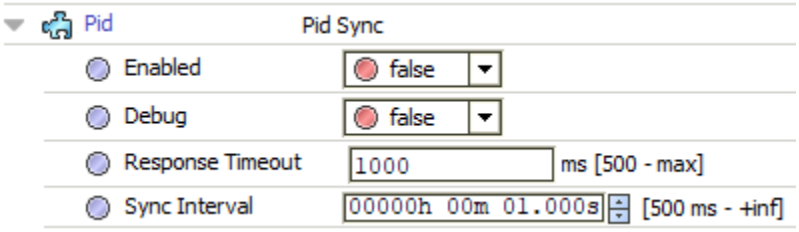
- **Condition Switcher**:



- Enabled: Set whether the functionality is enabled;
- Debug: Whether to print debugging information, it needs to be used with DebugService configuration;
- Response Timeout: Response timeout, in milliseconds;
- En0 Detector
  - Enabled: Whether to enable PRI network port detection;
  - Interval: Detection frequency;
  - Route Timeout: Reserved
  - Route Retry: Reserved
- Bus Detector: Detect all Networks in the Real Time Data configuration
  - Bus Trunk: Set Enable Switch When All Device Down to true to switch the point data under the corresponding Network from master to slave;
  - Enable Switch When All Device Down: Whether to monitor this bus;
  - Description: description, modification allowed;
  - Online Device: The current number of online devices on this bus;
  - Wait After Try Ping: Try to ping the device after all the devices are offline, and if all the devices are still in the down state after waiting for this time, it is judged that the bus is faulty;

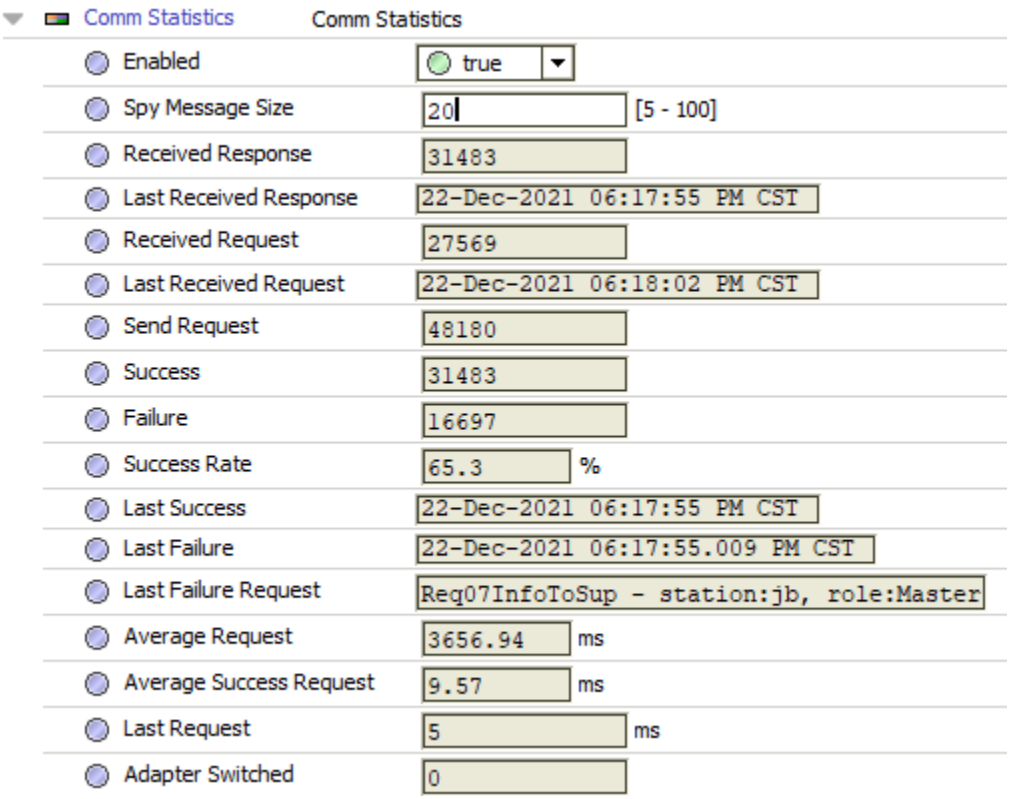
- **Pid**:

PID only processes the RdLoopPoint under the redundant module and does not perform synchronous processing on the LoopPoint under the kitControl. PID synchronization can ensure that the output jumps during the switching process:



- Enabled: Set whether the functionality is enabled;
- Debug: Whether to print debugging information, it needs to be used with DebugService configuration;
- Response Timeout: Response timeout, in milliseconds;
- Sync Interval: PID synchronization time;

- **Comm Statistics**: For statistical communication quality

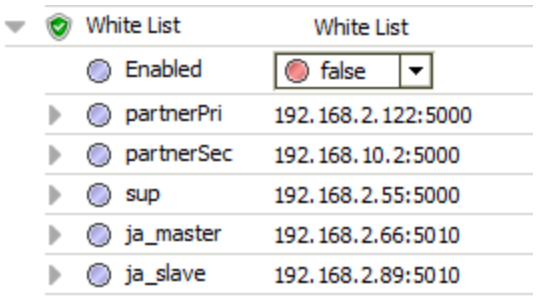


- Enabled: Set whether the functionality is enabled;
- Spy Message Size: Right-click Comm Statistics, select Spy Remote from the menu View, and four circular queues will be listed in it, namely RecentReceives (recently received messages), RecentSendRequests (recently sent requests),

RecentFailedSendRequests (recently failed requests), RecentSendMessages (recently Message sent without response), this attribute is used to configure the size of the ring queue, the latest data of the ring queue will replace the oldest piece of data;

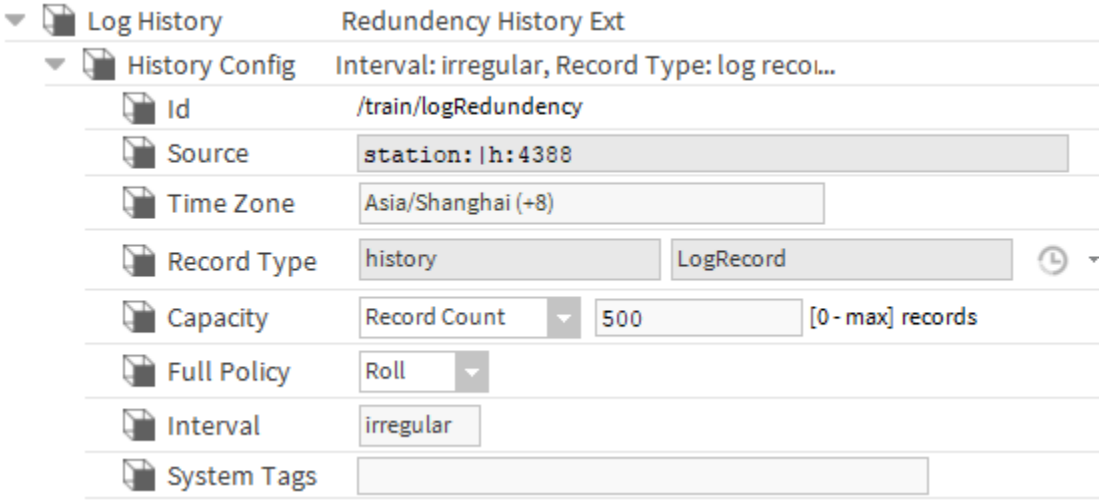
- Received Response: Responses Received;
- Last Received Response: The last time a reply was received;
- Received Request: Received request messages from other sites;
- Last Received Request: The last request message received from other sites;
- Send Request: Requests that are actively sent to other sites need to be answered by the other party;
- Success: The number of times the requests actively sent to other sites were successfully answered;
- Failure: The number of requests that were actively sent to other sites that were not answered correctly;
- Success Rate: The communication success rate, the communication success rate of the normal communication site should be close to 100%, only 65.3% in the above screenshot is because the configured site has not been online for a long time;
- Last Success: last successful time;
- Last Failure: last failure time;
- Last Failure Request: last failed message;
- Average Request: The average time it takes to send a request and wait for a response. If some sites are not online, the value will be significantly larger;
- Average Success Request: In a successful communication, the average time spent sending a request and waiting for a response;
- Last Request: The time-consuming time of the last communication request;
- Adapter Switched: When the redundant network card (SEC) communication fails, the data network card (PRI) will be used for redundant communication, and this value records the number of times such switching occurs;

- **White List**

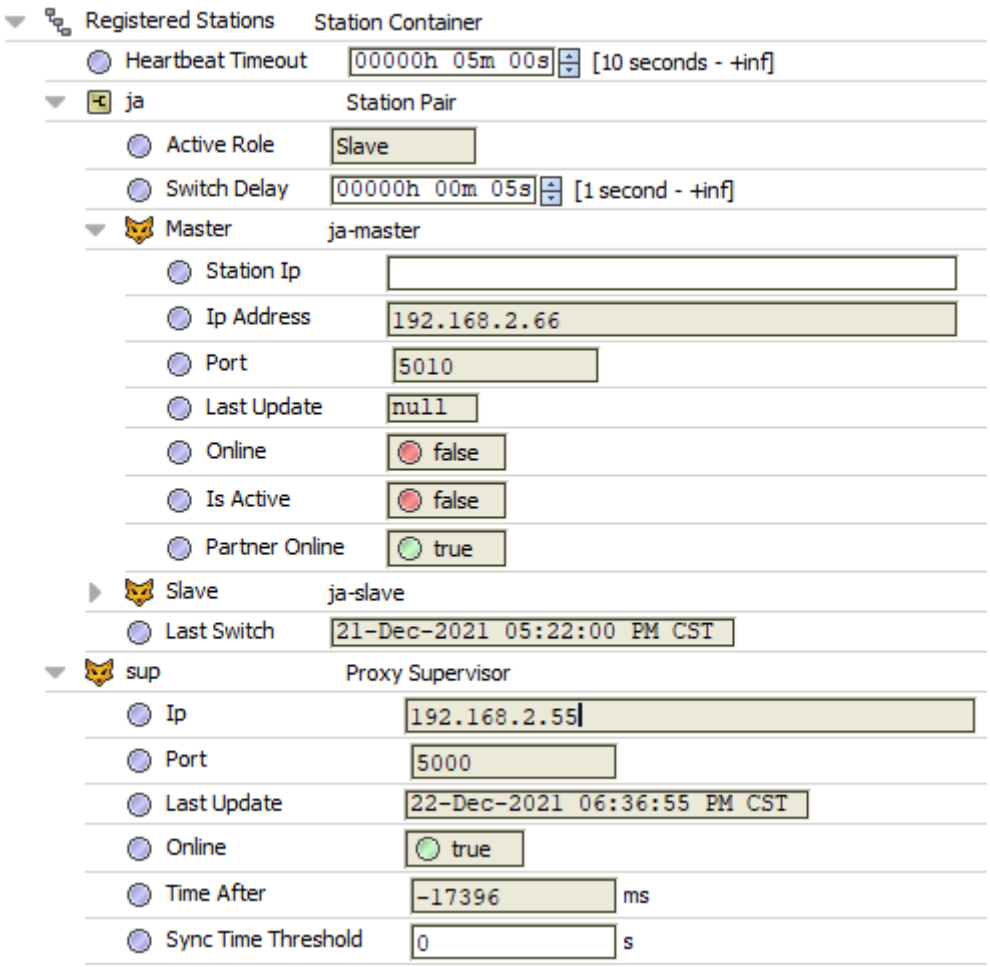


- Enabled: Whether to enable the whitelist; if the whitelist is enabled, the data sent from the IP address and port outside the whitelist will be completely ignored;

- **Log History**: Historical extension for recording redundant related operations



- **Registered Stations**



Used to store RedundancyService/commHandles/NWStations communicated sites, which are not Partner sites, but other redundant sites in the entire system, or independent sites with NiagaraNetwork proxy points

- Heartbeat Timeout: If the station data is not received within this time period, the station is considered to be offline;
- Proxy Supervisor: Usually a stand-alone Supervisor site
  - IP: The IP address of the site obtained from the communication process;
  - Port: Redundant communication ports of the site obtained from the communication process;
  - Last Update: Last updated time;
  - Online: Is online;
  - Time After: Difference with the system time of this site, in milliseconds;
  - Sync Time Threshold: Synchronization time threshold, 0 means no time synchronization, when the value is not 0, if the absolute value of the time difference (Time After) is greater than this property. When adjusting the

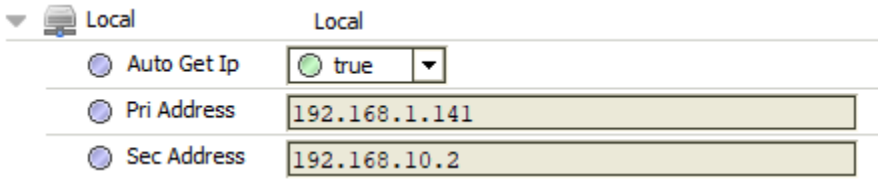
time, it is recommended not to set it too small (should be more than 10 seconds), otherwise it will lead to frequent time adjustments;

- En0 Check: Enable PRI network port detection;

- Station Pair: Pair of redundant sites with the same station name as the site under NiagaraNetwork
  - Active Role: Currently Active site;
  - Switch Delay: Delay time for switching the IP address of the Station under NiagaraNetwork;
  - Master: Primary station
    - Station Ip: If there is DNS, you can modify it
    - Ip Address: The IP address of the site obtained from the communication process;
    - Port: Redundant communication ports of the site obtained from the communication process;
    - Last Update: Last updated time;
    - Online: Is online;
    - Is Active: Indicate an active site
    - Partner Online: Whether the last obtained Partner is online or not. It is for reference only, its value has no meaning when it is not online;
    - En0 Check: Enable PRI network port detection;
  - Slave: Secondary station

    Refer to Master above

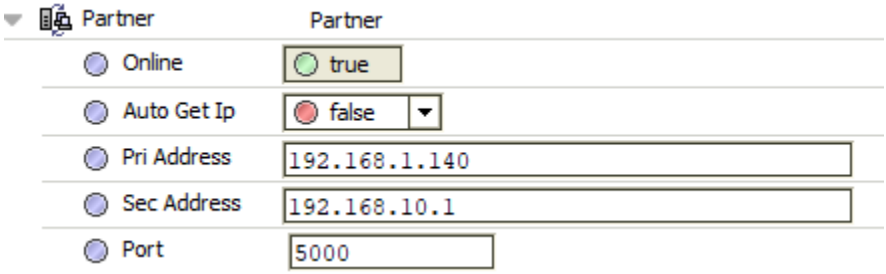
- **Auto Role**: Automatically match roles based on the IP address of LAN2 at startup;
- **Role**: Current station role;
- **Is Active**: Indicates whether the JACE station is Active, here true means that the data is actually collected, false means that it does not communicate with the device, and all data comes from Active JACE station;
- **Local**: Current station information



  - Auto Get Ip: Automatically configure the IP address of JACE, it is recommended to set it to true;

- Pri Address: IP of primary network card (PRI), used for data communication;
- Sec Address: IP of secondary network card (SEC), used for redundant communication;

- **Partner：**

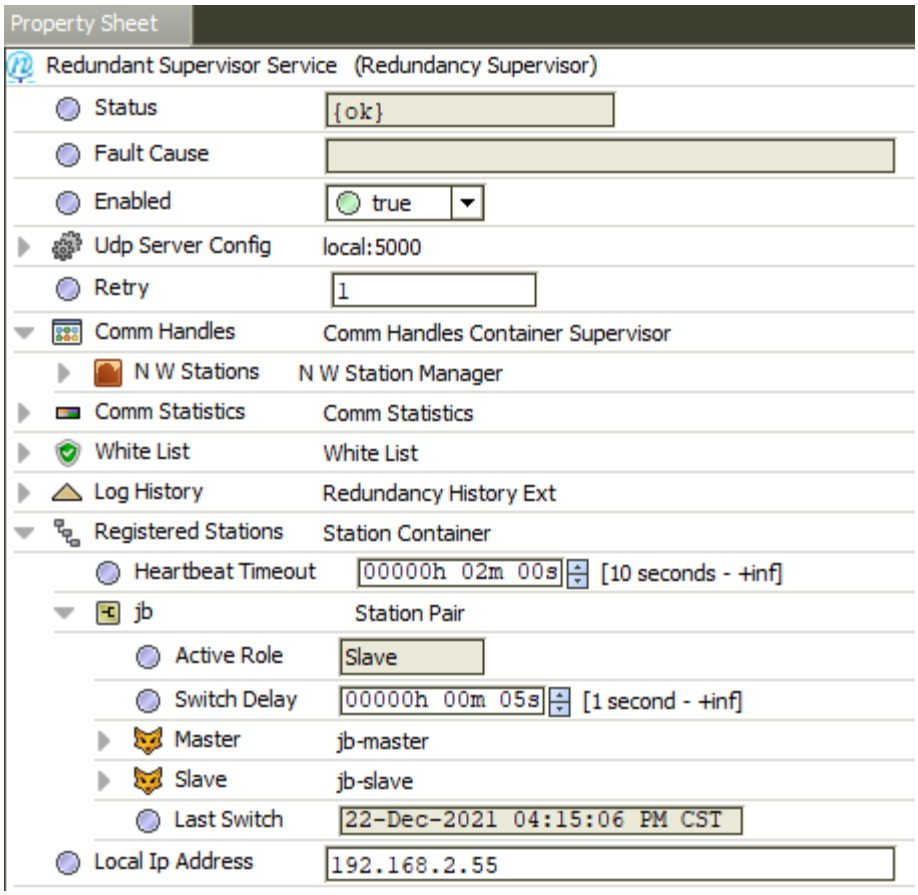


- Online: Show partner's online status;
- Auto Get Ip: Automatically configure the IP address of stations, it is recommended to set it to true;
- Pri Address: Set the primary station IP address;
- Sec Address: Set the secondary station IP address;
- Port: Set the partner's port;

Standalone Service

Standalone Service is a tailored version of RedundancyService. It is used in non-redundant stations, such as the Supervisor station in the aforementioned Network Architecture section. Its function is to manage the switching of stations under NiagaraNetwork.

Refer to RedundancyService.

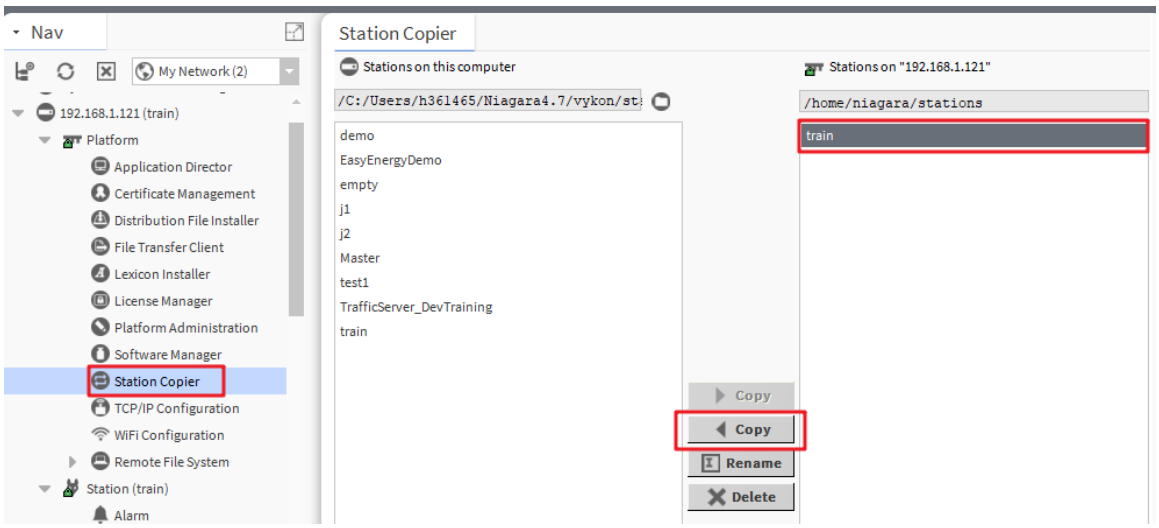

Property Sheet
Redundant Supervisor Service (Redundancy Supervisor)
Status
{ok}
Fault Cause
Enabled
true
Udp Server Config
local:5000
Retry
1
Comm Handles
Comm Handles Container Supervisor
N W Stations
N W Station Manager
Comm Statistics
Comm Statistics
White List
White List
Log History
Redundancy History Ext
Registered Stations
Station Container
Heartbeat Timeout
00000h 02m 00s
[10 seconds - +inf]
jb
Station Pair
Active Role
Slave
Switch Delay
00000h 00m 05s
[1 second - +inf]
Master
jb-master
Slave
jb-slave
Last Switch
22-Dec-2021 04:15:06 PM CST
Local Ip Address
192.168.2.55

Appendix

Station duplication

Copy primary station to local

Open the Station Copier tool under the Platform of the primary, select the station on the right, then click the Copy button on the left to keep the station name unchanged, you can copy the station to the local computer:



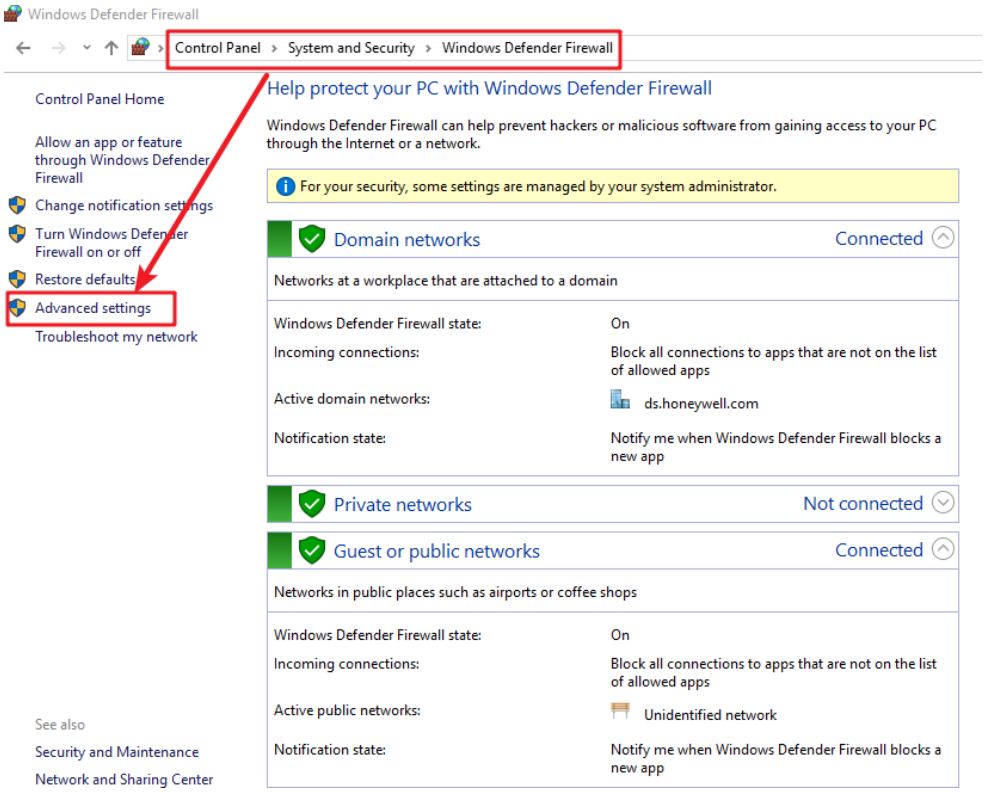
Copy local station to secondary

Open the Station Copier tool under the Platform of the secondary, select the station in the left side, and then click the Copy button to the right to copy the station to the secondary JACE. The station's name is unchanged while copying.

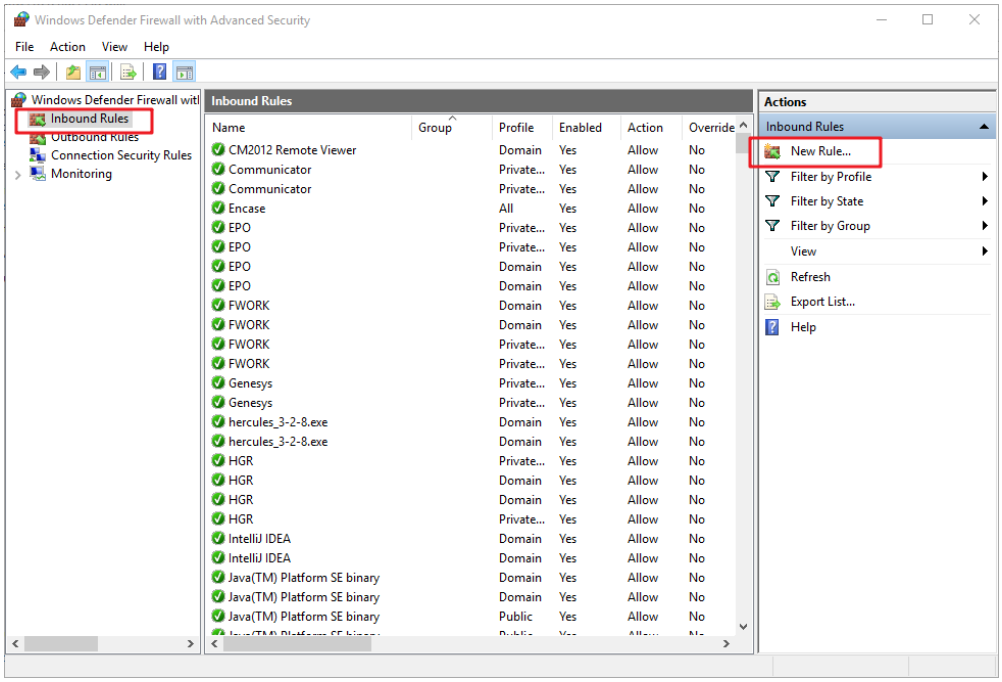
UDP 5000 port of the Firewall

1. Open the advanced settings of the Windows Firewall

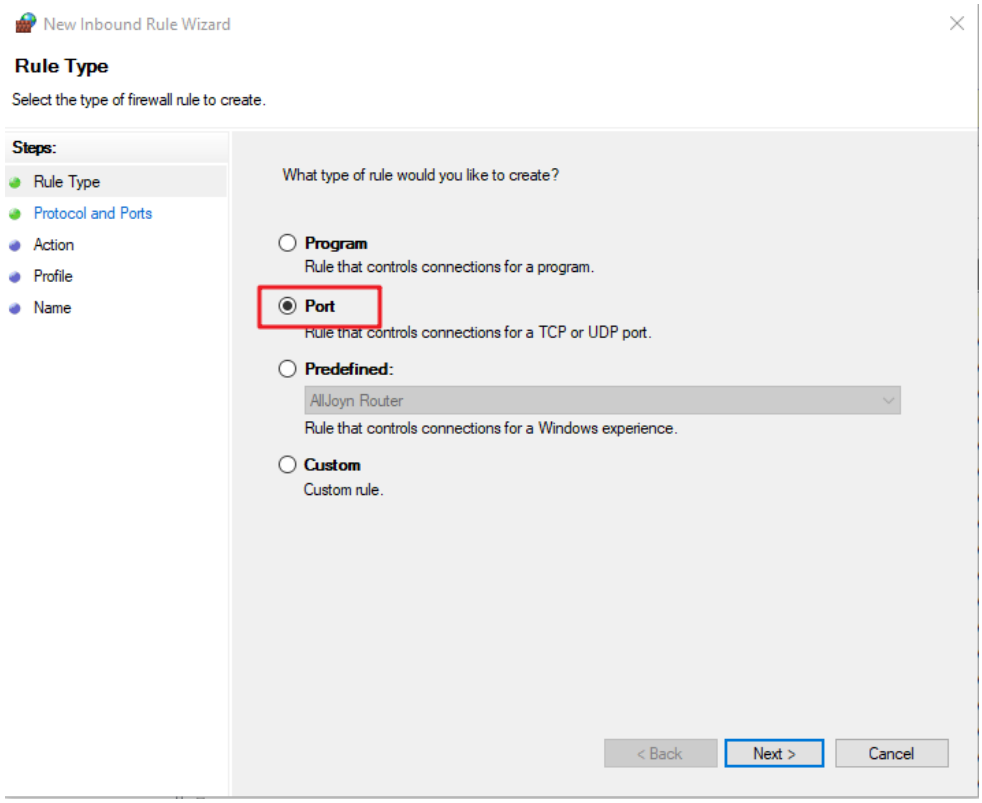
Control Panel->System and Security->Windows Defender Firewall->Advanced settings.



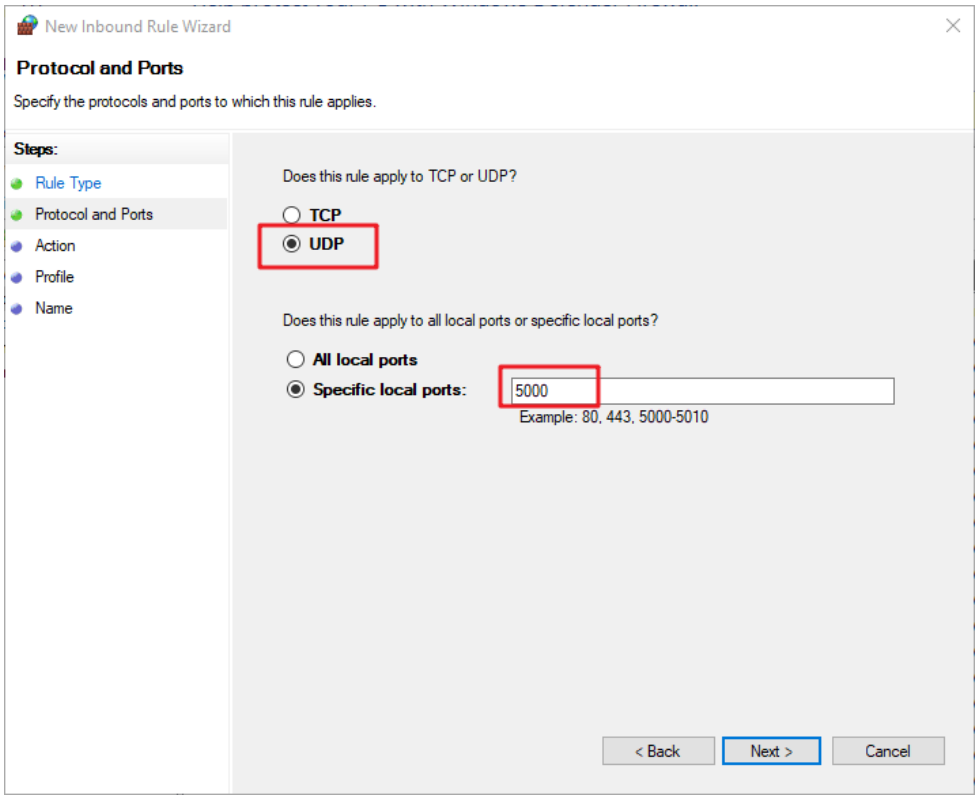
2. Choose Inbound Rules and click New Rule



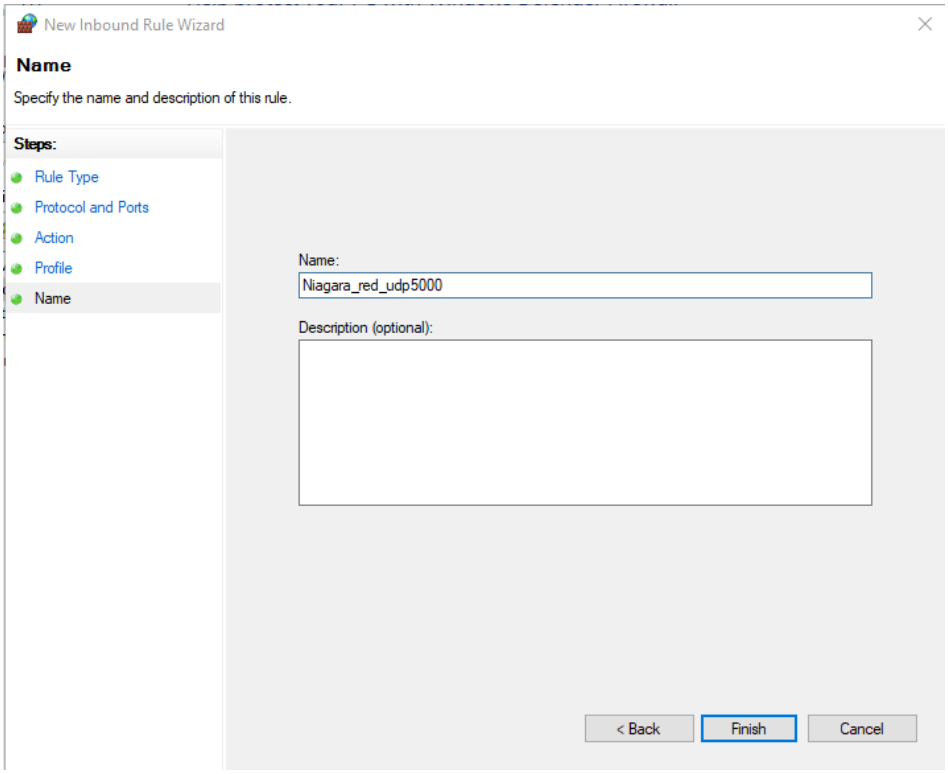
3. Set the Rule Type to Port



4. Apply the rule to UDP with port number 5000

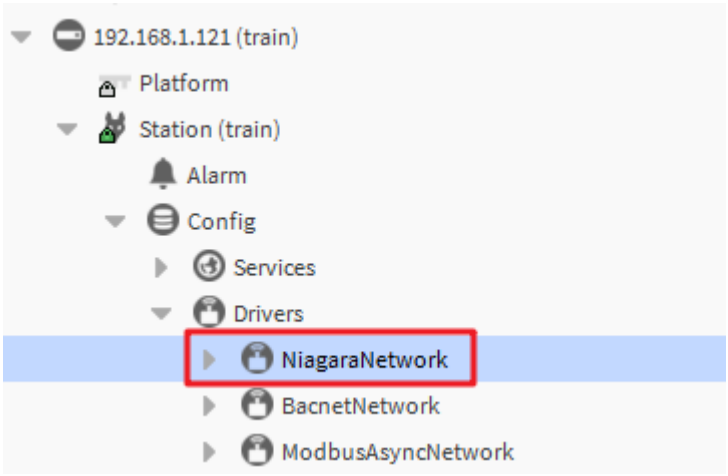


5. Continue to choose the next step until the rule is named and click Finish.

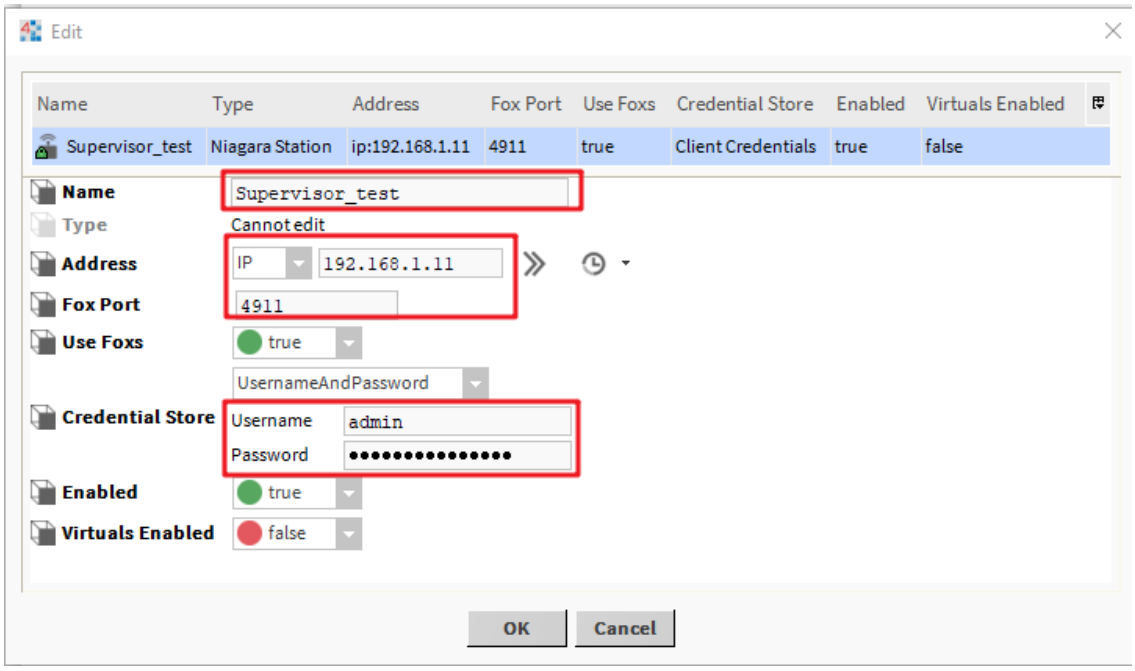


Connection between Supervisor with primary or secondary JACE station

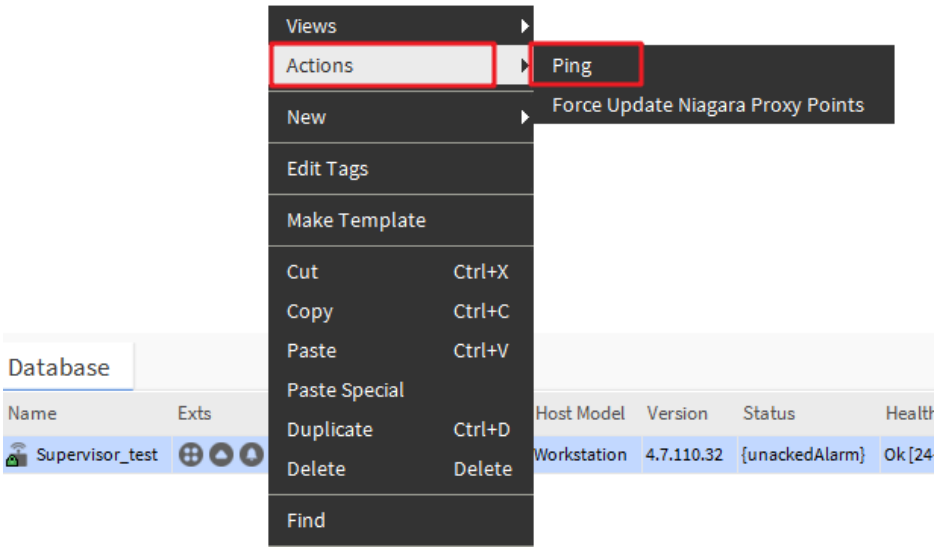
1. In the primary or secondary station, expand the Config->Drivers container, double-click NiagaraNetwork, and click the Discover button at the bottom of the Station Manager view to find the Supervisor station.



If the Supervisor station appears in the Discovered window, drag it to the Database window below. If you can't find it, you need to click the New button to add it, enter station name, IP address, port number of the Supervisor, username, and password. The station on JACE will use this user account to connect to the Supervisor station. Click OK to add it to the NiagaraNetwork in JACE.



2. Right click on the station in the Database window, select Actions -> Ping to establish a connection.



At this moment, the connection enters the Fault condition because the TLS security certificate provided by the remote station has not yet been approved. If the connection between the stations uses Foxs communication, and the CA signed certificate is not used, or the self-signed certificate configuration is not completed, the Foxs communication will become Fault immediately after the short ping, then the user needs to manually click to trust the certificate used by the communication.

Please refer to module://docNiagaraIT/doc/SecurityBestPractices-BFF3D9EB.html for mor information.

3. Open the Supervisor station, repeat the above 1-2 operations and use the same Station to connect the two master-slave sites in turn.

   During this process, because the Supervisor site needs to be connected to two primary and secondary sites with the same name, and the two sites with the same name cannot be added in the Database window of the Station Manager view, you can ping one of the sites successfully, double-click the site, and change the IP address to another site's IP, and execute the Ping command again.