Advanced: MQTT Modules in Redundant Ignition Environment

Prerequisites

Knowledge of Ignition and Module installation process: Cirrus Link Module Installation

Summary

The Inductive Automation platform and MQTT modules can be resilient to failures when configured to use redundancy. Redundant Ignition systems can be set up and configured to act as failover backups for primary/master Ignition instances. This tutorial will provide step by step instructions for installing a set of Ignition systems with redundancy on the host/primary Ignition instance as well as redundancy on the MQTT enabled edge nodes. For this tutorial we will show how to set up a total of six Ignition systems. These will be:

• Ignition Primary

An Ignition system running as master with MQTT Distributor and MQTT Engine installed. This is what remote Ignition systems will send data to in normal operation.

- Ignition Primary Backup
 - An Ignition system running as backup with MQTT Distributor and MQTT Engine installed. This is what remote Ignition systems will send data to when Ignition Primary fails.
- Ignition Edge 1

An gnition system running as master with MQTT Transmission installed. This will send data to Ignition Primary in normal operation. If Ignition Primary is in a failed state, this will send data to Ignition Primary Backup.

Ignition Edge 1 Backup

An Ignition system running as backup with MQTT Transmission installed. This will send data to Ignition Primary in the event that Ignition Edge 1 fails. If Ignition Primary is in a failed state and Ignition Edge 1 is in a failed state, this will send data to Ignition Primary Backup.

Ignition Edge 2

An Ignition system running as master with MQTT Transmission installed. This will send data to Ignition Primary in normal operation. If Ignition Primary is in a failed state, this will send data to Ignition Primary Backup.

- Ignition Edge 2 Backup
 - An Ignition system running as backup with MQTT Transmission installed. This will send data to Ignition Primary in the event that Ignition Edge 2 fails. If Ignition Primary is in a failed state and Ignition Edge 2 is in a failed state, this will send data to Ignition Primary Backup.

Additional Edge Nodes could be added to this infrastructure. It is also important to note that the Ignition Edge Nodes with MQTT Transmission could also be instances of Ignition Edge MQTT depending on your requirements (https://inductiveautomation.com/whats-new-ignition-edge). There are additional considerations when setting up a real world system using redundancy. These topics are not covered in this tutorial but should be taken into consideration.

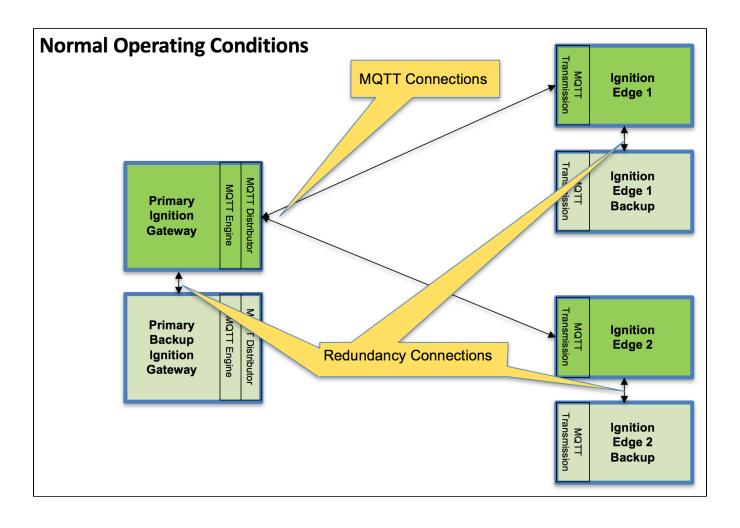
- Network paths
 - It may make sense to have edge nodes support multiple network paths to the MQTT servers. For example, Ethernet, cellular, and satellite could all exist as supported network paths on a single Edge gateway. This will help ensure additional reliability by supporting failover of networks.
- Primary Ignition and Primary Ignition backup placement
 - This tutorial was created by modeling this exact environment using Amazon AWS EC2 instances in the cloud. Reliability could be improved by putting Ignition Primary and Ignition Primary Backup in different AWS availability zones or even different AWS regions. This would allow the primary Ignition with MQTT Distributor and MQTT Engine to continue to operate even in the case of AWS failures. In the case of on premises installations of Ignition these could be placed in different physical locations and/or on secondary networks.
- MQTT Servers

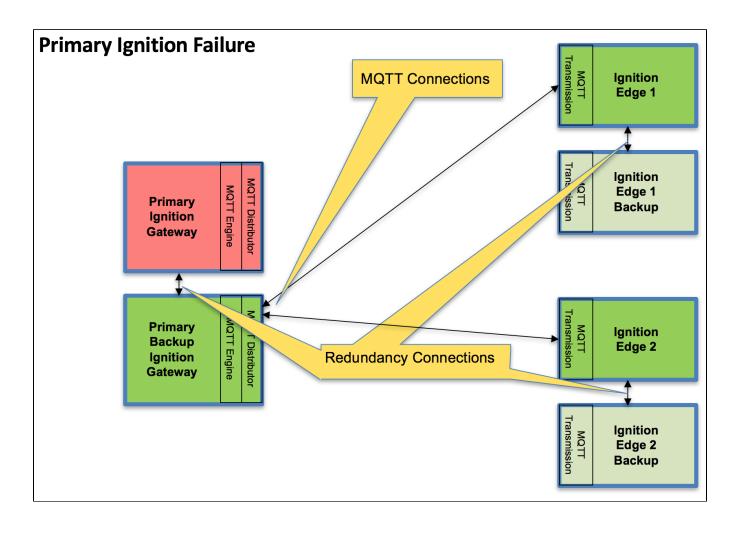
 Additional MQTT Servers can be added so MQTT connections from remote edge nodes remain established. Additional Chariot MQTT Servers can be used to make the system more robust (https://www.cirrus-link.com/iiot-mqtt-servers/).

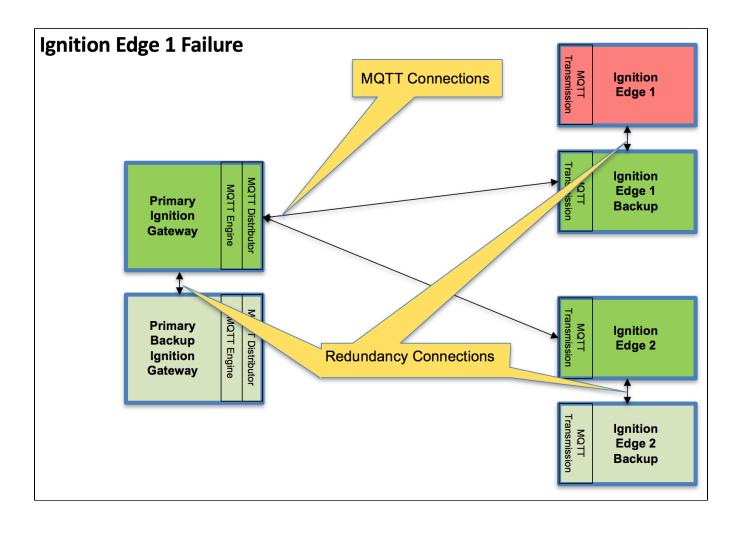
- History enablement in MQTT Transmission
 - MQTT Transmission supports caching of data in the case that it can not establish a connection to any of the configured MQTT Servers. Once a connection is reestablished, it will begin reporting and flush the stored historical values to prevent data loss in catastrophic failures.

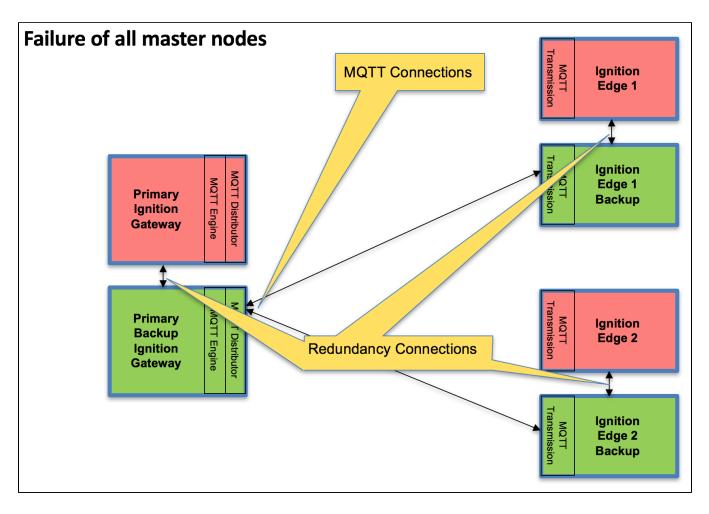
Upon completion of this tutorial you will have a functional system with redundancy/failover support for both remote edge nodes as well as the primary Ignition system that the remote edge nodes are reporting to.

Architecture









Tutorial

Step 1: Download and Install Ignition on Six Systems

Ignition is an Industrial Application Platform that can be used to create SCADA and HMI solutions. A fully functional Ignition system can be downloaded and run in trial mode.

Go to the Inductive Automation download page and download the desired Ignition installer for Windows, Linux or MacOS; https://inductiveautomation.com/downloads/archive.

Once the Ignition installer has been downloaded, follow the instructions provided by Inductive Automation to install and startup Ignition.

(Note: For this test infrastructure, MQTT Distributor will be installed as an Ignition module on both the Primary Ignition Gateway as well as the Primary Ignition Gateway Backup. Make sure to either turn off firewalls or at a minimum allow inbound connections to TCP/IP port 1883, as remote MQTT Clients will need to be able to establish a TCP/IP socket connection to these ports).

Step 2: Download and Install the Cirrus Link MQTT Modules

Go to the Inductive Automation download page again and scroll down to the Third Party modules section. Find the Cirrus Link modules section and download the MQTT Distributor, MQTT Engine, MQTT Transmission modules.

https://inductiveautomation.com/downloads/archive. For each of the Ignition instance, install the following MQTT Modules.

- Ignition Primary
- MQTT Distributor and MQTT Engine
- Ignition Primary Backup
- MQTT Distributor and MQTT Engine Ignition Edge 1
 - MQTT Transmission
- Ignition Edge 1 Backup
- MQTT Transmission
- Ignition Edge 2
- MQTT Transmission
 Ignition Edge 2 Backup
 - MQTT Transmission

Step 3: Configure the MQTT Modules

Once Ignition is installed, the MQTT Modules are installed, and everything is running we can configure the systems. Since we are going to have a backup for each master system, we only need to do most of the configuration for the master systems. Later, we can sync the configurations to the backups automatically. We'll start by configuring the modules and configure the redundancy settings in the next step.

- Ignition Primary MQTT Distributor
 - No modifications to the default parameters are required. However, it is important to make sure the Operation System allows inbound connections on port 1883 and there are no firewalls blocking inbound connections on this port from the remote edge nodes.
- Ignition Primary MQTT Engine
 - The only change from defaults is to set a Primary Host ID. MQTT uses Quality of Service (QOS) levels to ensure messages get delivered. However, this only ensures delivery between a single MQTT client and the MQTT server. In other words, it doesn't ensure delivery from one MQTT client to another MQTT client. Sparkplug introduces the notion of a Primary Host ID which is used to ensure client to client communications. The only requirement is that it match exactly on both the MQTT Engine and MQTT Transmission configurations.

	MQTT Engine Settings
	Servers Advanced Namespaces
	Advanced Settings
Set a Primary Host ID to some unique name.	Configuration
	Enabled @ Enable or Disable the MQTT Engine (default: true)
	Primary Host ID UNIQUE_NAME The Primary Host ID to allow connecting clients to ensure they remain connected to this application (optional)

Ignition Edge 1 and Ignition Edge 2 - MQTT Transmission (Configure the same on both Ignition instances)
 As with the MQTT Engine configuration, the Primary Host ID must be set on the General tab as shown below.

				un	a Primary Host ID to so ique name (matching the second	he
General	Servers Sets	Transmitters			TT Engine configuratio	on).
General Se	ettings					
Configuration						
Enabled	✓ Enable or disat	ole Mart Transmissio	on from connec	ting to the config	gured MQTT Servers	
Primary Host ID	UNIQUE_NAME					
	Primary Host ID o	f the backend applica	ation the MQTT	clients in MQTT	Transmission should rem	nain connected to (op
lete the existin	Primary Host ID o				Transmission should rem	nain connected to (op
lete the existir	ng default MQT		Server.		20 Changes	nain connected to (op
	ng default MQT	T Transmission	Server.	sav	20 Changes	nain connected to (op
QTT Transmis	ig default MQT	T Transmission	Server.	e the existing MC	20 Changes	nain connected to (op
QTT Transmis General Servers	ng default MQT sion Settings Sets Transm	T Transmission	a Server.	e the existing MC	20 Changes	nain connected to (op

 $^{\circ}~$ Create a new MQTT Server configuration by clicking the link below.

IQTT Tra	ansmissio	on Settings		Create a new MQTT definition	Server		
General	Servers	Sets Transmitte	ers	///			
✓ Success	fully deleted M	IQTT Server " Chariot	SC				
Name	URL	Server Type	Server Set	Username	Certificates	Connected	
No MTServe	rsRecord						

Configure MQTT Transmission to point to the Primary Ignition. Configure as shown below making sure to change the URL to reflect your network settings. For example, if you Ignition Primary is at 192.168.1.100 the MQTT Server URL would be: tcp://192.168.1.100:1883. Af ter setting the parameters as shown below. Click the 'Save Changes' button at the bottom.

MQTT Trans	smission Settings	Modify as needed to point to the
General	Servers Sets Transmitters	Primary Ignition URL
Edit MQT1	l Server	
Main		
Name	primary The friendly name of this M ⁹ Server	
URL	tcp://primary:1883 The URL of this MQTT Server. Should be of the	form tcp://mydomain.com:1883 or ssl://mydomain.com:8883
Server Type	MQTT Distributor The type of MQTT Server to connect to	
Server Set	Default The Server Set this MQTT Server is associated	with
Username	admin The username for this MQTT connection if req	uired by the MQTT Server (optional)
Change Password?	Check this box to change the existing passw	vord.
Password	The password for this MQTT connection if req	uired by the MQTT Server (optional)
Password	Re-type password for verification.	
Certificates	Browse No file selected.	
Show advance	ed properties	
		Save Changes

° Verify the MQTT Server has been created and is shown in the list of MQTT Servers as shown below.

General	Servers Sets	Transmitters					
Successf	ully created new MQTT S	erver "primary"					
Name	URL	Server Type	Server Set	Username	Certificates	Connected	
	URL tcp://primary:1883	Server Type	Server Set Default	Username admin	Certificates	Connected 0 of 0	delete
Name primary					Certificates		delete

- · Repeat the process of creating a MQTT Server but instead point it to the Ignition Primary Backup MQTT Server. These are the parameters to use:
 - Name: primary-backup

 - URL: tcp://primary-backup:1883
 Change 'primary-backup' in the URL to reflect the network address of the Ignition Primary Backup server.
 - Server Type: MQTT Distributor
 - Server Set: Default
 - Username: admin
 - Password: changeme

0	When complete, verify both MQTT	Servers appear in the list as shown below.

MQTT Transmission Settings

General	Servers	Sets	Transmitters						
✓ Successful	lly created	new MQTT	Server "primary-b	ackup"					
Name	U	IRL		Server Type	Server Set	Username	Certificates	Connected	
primary	to	:p://primary:	1883	MQTT Distributor	Default	admin		0 of 0	delete edit
primary-back	Jp to	:p://primary-	backup:1883	MQTT Distributor	Default	admin		0 of 0	delete edit
 Create new I 	MQTT Serve	r							

° Finally, make sure to set up the same MQTT Transmission configuration in the Ignition Edge 2 instance.

Step 4: Configure Redundancy

The following configuration shows all of the redundancy settings that were used in setting this environment up using Amazon's AWS EC2 instances (virtual machines). The configuration will vary based on your network configuration. Additional Ignition redundancy resources can be found at the following links:

https://docs.inductiveautomation.com/display/DOC79/Setting+Up+Redundancy https://support.inductiveautomation.com/usermanuals/ignition/index.html?redundancy_settings.htm

- Ignition Primary
 - Select Redundancy on the left navigation bar. Then set the Mode to 'Master' and set the Standby Activity left to 'Warm' as shown below.

Igni	но номе	ես STATUS	¢ CONFIGURE	
Q Search	Trial Vei	rsion 1:26:34		friving our software. Have fun.
Select Redundancy on the left navigation bar Licensin Module Projects Redund Gateway NETWORK	Restore Redund g Redundanc ancy y Settings Mode	y Settings Master	twork Config eredundancy, and specif	uration y this node's role. There should be one ma
Gatewa Email S SECURITY Auditing Users, R Service	Standby Activ Level	How the node s	whould run when it is not c ing failover times.	urrently the active node. If cold , the noc
Security	S	out	tivity, in milliseconds, be	fore the backup assumes responsibility.

- Set up the Redundancy Network Settings. The settings here are specific to your network setup. On many LAN configurations none of these changes are required. What is shown below was the configuration for setting up all of these components in Amazon's AWS EC2 instances. The changes were:
 - Uncheck 'Auto-detect network interface'
 - Set the 'Network Bind Interface' to the public IP address of the Ignition Primary EC2 instance. On a LAN this would be the primary network interface address of the Ignition Primary machine.
 - Uncheck the 'Autodetect HTTP Address' tickbox.

Specify two explicit HTTP addresses for clients to use. These were the public IP addresses of the Ignition Primary and Ignition Primary Backup EC2 instances. On a LAN, these would be the primary network interface addresses of the Ignition Primary and Ignition Primary Backup machines. Also note the HTTP port is 8088 which is the default Ignition HTTP port.

	088/main/web/config/syste	ana courrounoy10					,	<u>م</u>	
Journal Notification	Network Setting	s							l
On-Call Rosters Schedules	Port	8750							
CS/GEM Equipment	Port	The TCP port used for redune (default: 8750)	ancy operations. Ma	ke sure that this port is not bloc	ked by a firewall.				
Equipment Module Settings Simulator User Manual	Auto-detect network interface?	If true, the system will a which interface to use. (default: true)	utomatically detect	which network interface to use. I	Nost commonly disable	d on systems with multiple netwo	ork cards, in order to explic	itly spe	
is History Realtime	Network Bind Interface	34.201.169.174 The IP address of the network	interface to use for	redundancy. Only used if "auto-	detect" is turned off.				
-UA SERVER ertificates evices	Autodetect HTTP Address	To specify an explicit HTTP (default: true)	address for clients t	o use, turn this off. Most users w	ill leave autodetect on.				
Settings		Address		HTTP Port		HTTPS Port			
		primary		8058		443	Re	move	
Servers		primary-backup		8088		443		move	
uick Client		Add New Address							
BILE	HTTP Addresses					[
Settings				80		443	Ad	3	
TERPRISE MINISTRATION									
gent Settings		If autodetect HTTP address is	false, clients will us	these addresses. Usually only r	ecessary in multi-hom	ed or port-forwarded redundancy	configurations		

° Set the Master Node Address. Note in the configuration below a hostname is being used. This should be the primary network interface address of the Ignition Primary Gateway.

	Set the Master Node Address
Ignition-primary - Ignition Gate ×	Θ
← → C ③ primary:8088/main/web/config/syste	am.redundancy?8 🖈 🛆 🖸 🗄
Whitelist	A list of (p addresses, or to accept connections from. Would normally only have one entry for the backup node, unless the backup machine connects through various (defuult)
Backup Node Se	ttings
Master Node Address	primary The address of the master Ignition system.
Ping Rate	1000 The time, in milliseconds, between messages from the backup to the master.
Reconnect Period	10000 How often, in milliseconds, to re-attempt connection when the backup node is not connected to the master. (default: 1000)
History Mode	Full Full Full Full Full, history will be stored normally, as it would be on the master system. If Fartial, history will be cached until the master is available again and the backup node is able to determine the exact time that the master was down.
	Save Changes
	(inductive

- Finally, click the 'Save Changes' button.
- Ignition Primary Backup
 Select Redundancy on the left navigation bar. Then set the Mode to 'Backup' and set the Standby Activity left to 'Warm' as shown below.

		А НОМЕ	M STATUS	¢ CONFIGURE	
	Q Search	Trial Versio	on 1:15:49	We're glad you're te	st driving our software. Have fun.
Select Redundancy on the left navigation bar	SYSTEM Overview Backup/Restore Licensing Modules Projects Redundancy Gateway Settings NETWORKING	Redundanc Redundancy Set	tings Backup		guration city this node's role. There should be one mas
	Gateway Network Email Settings SECURITY Auditing Users, Roles	Standby Activity Level		ould run when it is no ng failover times.	 t currently the active node. If cold , the node
	Service Security Security Zones DATABASES	Failover Timeout	10000 The time of inact (default: 10000)	ivity, in milliseconds,	before the backup assumes responsibility.

- Set up the Redundancy Network Settings. The settings here are specific to your network setup. On many LAN configurations none of these changes are required. What is shown below was the configuration for setting up all of these components in Amazon's AWS EC2 instances. The changes were:
 - Uncheck 'Auto-detect network interface'
 - . Set the 'Network Bind Interface' to the public IP address of the Ignition Primary Backup EC2 instance. On a LAN this would be the primary network interface address of the Ignition Primary Backup machine. Uncheck the 'Autodetect HTTP Address' tickbox.

 - Specify two explicit HTTP addresses for clients to use. These were the public IP addresses of the Ignition Primary and Ignition Primary Backup EC2 instances. On a LAN, these would be the primary network interface addresses of the Ignition Primary and Ignition Primary Backup machines. Also note the HTTP port is 8088 which is the default Ignition HTTP port.

Journal Notification	Network Setting	15						
On-Call Rosters								
Schedules		8750						
	Port	The TCP port used for redund	dancy operations. Mak	e sure that this port is not block	ed by a firewall.			
		(default: 8750)						
Equipment								
Module Settings Simulator	Auto-detect		utomatically detect wi	hich network interface to use. M	lost commonly disable	d on systems with multiple netwo	ork cards, in order to ex	plicitly spe
User Manual	interface?	which interface to use. (default: true)						
		(denaurc trae)						
History	Network Bind Interface	54.211.69.177						
Realtime		The IP address of the network	k interface to use for re	dundancy. Only used if "auto-d	letect" is turned off.			
	Autodetect HTTP			use, turn this off. Most users wi				
Certificates	Address	(default: true)	address for clients to	use, turn this on. Most users wi	it leave autobetect on.			
Devices								
Settings		Address		HTTP Port		HTTPS Port		
		primary		8058		443		Remove
Servers		primary-backup		8088		443		Remove
Quick Client				8088		443		Remove
BILE	HTTP Addresses	Add New Address						
Settings				80		443		Add
ITERPRISE								

• Set the Master Node Address. Note in the configuration below a hostname is being used. This should be the primary network interface address of the Ignition Primary Gateway.

		Set the Master Node Address	
🔍 🔍 🚺 Ignition-primary - Ign	ition Gate ×	e	9
← → C () primary:8088/ma	ain/web/config/syste	m.redundancy?8 🖈 o 🖸 :	:
	Whitelist	A Bit of the addresses, on the accept connections from. Would normally only have one entry for the backup node, unless the backup machine connects through various mathematics.	
	Backup Node Set	tings	
	Master Node	primary	
	Address	The address of the master Ignition system.	
		1000	
	Ping Rate	The time, in milliseconds, between messages from the backup to the master. (default: 1000)	
		10000	
	Reconnect Period	Www often, in milliseconds, to re-attempt connection when the backup node is not connected to the master. (default: 10000)	
		Full	
	History Mode	How history is treated by the backup system. If Full, history will be stored normally, as it would be on the master system. If Partial, history will be cached until the master is available again and the backup node is able to determine the exact time that the master was down.	I
		Save Changes	
		(inductive	ľ

• Finally, click the 'Save Changes' button.

Ignition Edge 1

• Select Redundancy on the left navigation bar. Then set the Mode to 'Master' and set the Standby Activity left to 'Warm' as shown below.

Ignition	≜ номе	.la STATUS	¢ CONFIGURE
Q Search	Trial Versio	DN 1:26:34	We're glad you're test driving our software. Have fun.
SYSTEM Overview Backup/Restore Licensing Modules Projects	Redundancy Set		twork Configuration
Redundancy Gateway Settings NETWORKING	Mode	Master Enable or disab	• le redundancy, and specify this node's role. There should be one ma
Gateway Network Email Settings CURITY Auditing Users, Roles	Standby Activity Level		 v hould run when it is not currently the active node. If cold, the noc ing failover times.
rvice Security curity Zones BASES	Failover Timeout	10000 The time of inac (default: 10000)	tivity, in milliseconds, before the backup assumes responsibility.

- Set up the Redundancy Network Settings. The settings here are specific to your network setup. On many LAN configurations none of these changes are required. What is shown below was the configuration for setting up all of these components in Amazon's AWS EC2 instances. The changes were:
 - Uncheck 'Auto-detect network interface'
 - Set the 'Network Bind Interface' to the public IP address of the Ignition Edge 1 EC2 instance. On a LAN this would be the primary network interface address of the Ignition Edge 1 machine. Uncheck the 'Autodetect HTTP Address' tickbox.
 - .
 - . Specify two explicit HTTP addresses for clients to use. These were the public IP addresses of the Ignition Edge 1 and Ignition Edge 1 Backup EC2 instances. On a LAN, these would be the primary network interface addresses of the Ignition Edge 1 and Ignition Edge 1 Backup machines. Also note the HTTP port is 8088 which is the default Ignition HTTP port.

Journal Notification	Network Setting	zs						
Notification On-Call Rosters Schedules	Port	8750 The TCP port used for redundancy o						
ECS/GEM Equipment		(default: 8750)	iperations. Make	sure that this port is not blocked by	a nrewali.			
Equipment Module Settings Simulator User Manual	Auto-detect network interface?	If true, the system will automat which interface to use. (default: true)	tically detect whi	ch network interface to use. Most co	ommonly disabled	on systems with multiple netwo	ork cards, in order to e	xplicitly spe
IGS History Realtime	Network Bind Interface	52.54.221.215 The IP address of the network interf	ace to use for rec	lundancy. Only used if "auto-detect"	" is turned off.			
PC-UA SERVER Certificates Devices	Autodetect HTTP Address	To specify an explicit HTTP addres (default: true)	ss for clients to u	ise, turn this off. Most users will leav	re autodetect on.			
Settings		Address		HTTP Port		HTTPS Port		
		edge1		8088		443		Remove
Servers Quick Client		edge1-backup		8058		443		Remove
DBILE	HTTP Addresses	Add New Address						
Settings				80		443		Add
QUENTIAL FUNCTION								

° Set the Master Node Address. Note in the configuration below a hostname is being used. This should be the primary network interface address of the Ignition Edge 1 Gateway.

	Set the Master Node Address
e e 🔍 🔀 Ignition-edge1 - Ignition Gatev 🗙	е
← → C O edge1:8088/main/web/config/sys	(default:)
Backup Node Master Node Address	edge1 The address of the master ignition system.
Ping Rate	1000 The time, in milliseconds, between messages from the backup to the master. (defuult: 1000)
Reconnect Peri	d How often, in milliseconds, to re-attempt connection when the backup node is not connected to the master. (default: 10000)
History Mode	Full Full Full Full Full, bistory will be stored normally, as it would be on the master system. If Partial, history will be cached until the master is available again and the backup node is able to determine the exact time that the master was down.
	Save Changes
	Ignition by Inductive Automation Ignition by Inductive Automation. Copyright & 2003 2017. All rights resorved. Vew Roense

• Finally, click the 'Save Changes' button.

Ignition Edge 1 Backup

• Select Redundancy on the left navigation bar. Then set the Mode to 'Backup' and set the Standby Activity left to 'Warm' as shown below.

	Ignition.	А НОМЕ Ј	⊨ STATUS	¢ CONFIGURE	
	Q Search	Trial Versio	n 1:15:49	We're glad you're test d	riving our software. Have fun.
Select Redundancy on the left navigation bar	SYSTEM Overview Backup/Restore Licensing Modules Projects Redundancy Gateway Settings NETWORKING	Redundanc Redundancy Sett	ings Backup	etwork Configuration • • • • • • • • • • • • • • • • • •	
	Gateway Network Email Settings SECURITY Auditing Users, Roles	Standby Activity Level		▼ ould run when it is not cu ing failover times.	rrently the active node. If $\ \mbox{cold}$, the node
	Service Security Security Zones DATABASES	Failover Timeout	10000 The time of inac (default: 10000)	tivity, in milliseconds, bef	ore the backup assumes responsibility.

- Set up the Redundancy Network Settings. The settings here are specific to your network setup. On many LAN configurations none of these changes are required. What is shown below was the configuration for setting up all of these components in Amazon's AWS EC2 instances. The changes were:
 Uncheck 'Auto-detect network interface'

 - Set the 'Network Bind Interface' to the public IP address of the Ignition Edge 1 Backup EC2 instance. On a LAN this would be the primary network interface address of the Ignition Edge 1 Backup machine.
 - Uncheck the 'Autodetect HTTP Address' tickbox. .
 - Specify two explicit HTTP addresses for clients to use. These were the public IP addresses of the Ignition Edge 1 and Ignition Edge 1 Backup EC2 instances. On a LAN, these would be the primary network interface addresses of the Ignition Edge 1 and Ignition Edge 1 Backup machines. Also note the HTTP port is 8088 which is the default Ignition HTTP port.

cked by a firewall.
cked by a firewall.
cked by a firewall.
. Most commonly disabled on systems with multiple network cards, in order to explicitly sp
o-detect" is turned off.
will leave autodetect on.
HTTPS Port
443 Remove
443 Remove
443 Add
>

Set the Master Node Address. Note in the configuration below a hostname is being used. This should be the primary network interface address of the Ignition Edge 1 Gateway.

	Set the Master Node Address	
• • • 🕎 ignition-edge 1 - ignition Gate: x		6
← → C ① edge1-backup:8088/main/web/confi	g/system.redundancy	
	(default:)	
Backup Node Set	tings	
Master Node Address	edge1	
Address	The address of the master Ignition system.	
	1000	
Ping Rate	The time, in milliseconds, between messages from the backup to the master. (default 1000)	
	10000	
Reconnect Period	How often, in milliseconds, to re-attempt connection when the backup node is not connected to the master. (default: 10000)	
	Full *	
History Mode	How history is treated by the backup system. If Fall, history will be stored normally, as it would be on the master system. If Partial, history will be cached until the mast is available again and the backup node is able to determine the exact time that the master was down.	a
	Save Changes	
	gostori by inductive Automation. Copyright 6 2000 2017. All rights reserved. View Reserve	

• Finally, click the 'Save Changes' button.

Ignition Edge 2

 Select Redundancy on the left navigation bar. Then set the Mode to 'Master' and set the Standby Activity left to 'Warm' as shown below.

	Ignition.	🕈 НОМЕ	հ STATUS	CONFIGURE	
	Q Search	Trial Versio	DN 1:26:34	We're glad you're test	: driving our software. Have fun.
Select Redundancy on the left navigation bar	SYSTEM Overview Backup/Restore Licensing Modules Projects	Redundancy Set		twork Config	guration
	Redundancy Gateway Settings NETWORKING Gateway Network	Mode	Master Enable or disabl	▼ e redundancy, and spec	ify this node's role. There should be one ma
	Email Settings SECURITY Auditing Users, Roles	Standby Activity Level		 nould run when it is not ing failover times. 	currently the active node. If cold , the noc
	Service Security Security Zones DATABASES Connections	Failover Timeout	10000 The time of inac (default: 10000)	tivity, in milliseconds, b	efore the backup assumes responsibility.

- Set up the Redundancy Network Settings. The settings here are specific to your network setup. On many LAN configurations none of these changes are required. What is shown below was the configuration for setting up all of these components in Amazon's AWS EC2 instances. The changes were:
 - Uncheck 'Auto-detect network interface'
 - Set the 'Network Bind Interface' to the public IP address of the Ignition Edge 2 EC2 instance. On a LAN this would be the primary network interface address of the Ignition Edge 2 machine. Uncheck the 'Autodetect HTTP Address' tickbox. •

 - Specify two explicit HTTP addresses for clients to use. These were the public IP addresses of the Ignition Edge 2 and Ignition Edge 2 Backup EC2 instances. On a LAN, these would be the primary network interface addresses of the Ignition Edge 2 and Ignition Edge 2 Backup machines. Also note the HTTP port is 8088 which is the default Ignition HTTP port.

Journal								_
Notification	Network Setting							
On-Call Rosters								_
Schedules	Port	8750						
CS/GEM	POIL	The TCP port used for redundar	icy operations. M	lake sure that this port is not blo	cked by a firewall.			
Equipment		(default: 8750)						
Module Settings	Auto-detect							
Simulator	Auto-detect	which interface to use.	omatically detect	t which network interface to use.	Most commonly disabl	ed on systems with multiple netwo	irk cards, in order to explicitly s	.pe
User Manual	interface?	(default: true)						
GS								-
History	Network Bind	54.236.219.237						
Realtime	Interface	The IP address of the network i	nterface to use fo	r redundancy. Only used if "auto	-detect" is turned off.			
C-UA SERVER		-						
Certificates	Autodetect HTTP Address	To specify an explicit HTTP a (default: true)	ddress for clients	to use, turn this off. Most users w	will leave autodetect or	l.		
Devices	Hudress	(delabil: d'de)						
Settings		Address		HTTP Port		HTTPS Port		
		edge2		8058		443	Remov	
Servers								
Quick Client		edge2-backup		8088		443	Remov	e
BILE	HTTP Addresses	Add New Address						
Settings				80		443	Add	
OUENTIAL FUNCTION								
ÂRTS								
Settings						ned or port-forwarded redundancy		

• Set the Master Node Address. Note in the configuration below a hostname is being used. This should be the primary network interface address of the Ignition Edge 2 Gateway.

	Set the Master Node Address
Ignition-edge2 - Ignition Gates ×	θ
← → C O edge2:8088/main/web/confi	/system.redundancy?6 🖈 🖉 🖸 🗄
	(default:)
Backup N	ode Settings
Master Nor Address	
	The address of the master Ignition system.
Ping Rate	1000
Fing Rate	The time, in milliseconds, between messages from the backup to the master. (default: 1000)
	10000
Reconnect	Period How often, in milliseconds, to re-attempt connection when the backup node is not connected to the master. (default: 1000)
	Full v
History Mo	4e How history is treated by the backup system. If Full, history will be stored normally, as it would be on the master system. If Partial, history will be cached until the master is available again and the backup node is able to determine the exact time that the master was down.
	Save Changes
	Ignition by Inductive Automation. Copyright 6 2 and 2011 All rights reserved. Www Keenee

• Finally, click the 'Save Changes' button.

Ignition Edge 2 Backup

• Select Redundancy on the left navigation bar. Then set the Mode to 'Backup' and set the Standby Activity left to 'Warm' as shown below.

	Ignition.	А НОМЕ .	ha STATUS	¢ CONFIGURE
	Q Search	Trial Versio)N 1:15:49	We're glad you're test driving our software. Have fun.
ect Redundancy on the left navigation bar	SYSTEM Overview Backup/Restore Licensing Modules Projects	Redundance Redundancy Set		twork Configuration
	Redundancy Gateway Settings NETWORKING	Mode	Backup Enable or disable	redundancy, and specify this node's role. There should be one ma
	Gateway Network Email Settings SECURITY Auditing Users, Roles	Standby Activity Level		v ould run when it is not currently the active node. If cold , the node ing failover times.
	Users, Roles Service Security Security Zones	Failover Timeout	10000 The time of inact	ivity, in milliseconds, before the backup assumes responsibility.

- Set up the Redundancy Network Settings. The settings here are specific to your network setup. On many LAN configurations none of these changes are required. What is shown below was the configuration for setting up all of these components in Amazon's AWS EC2 instances. The changes were:

 - Uncheck 'Auto-detect network interface'
 Set the 'Network Bind Interface' to the public IP address of the Ignition Edge 2 Backup EC2 instance. On a LAN this would be the primary network interface address of the Ignition Edge 2 Backup machine.
 - Uncheck the 'Autodetect HTTP Address' tickbox.
 - . Specify two explicit HTTP addresses for clients to use. These were the public IP addresses of the Ignition Edge 2 and Ignition Edge 2 Backup EC2 instances. On a LAN, these would be the primary network interface addresses of the Ignition Edge 2 and Ignition Edge 2 Backup machines. Also note the HTTP port is 8088 which is the default Ignition HTTP port.

Journal							
Notification	Network Setting						
On-Call Rosters Schedules		8750					
ECS/GEM	Port	The TCP port used for redun- (default: 8750)	dancy operations. M	lake sure that this port is not blo	icked by a firewall.		
Equipment Module Settings Simulator User Manual	Auto-detect network interface?	If true, the system will a which interface to use. (default: true)	utomatically detect	t which network interface to use	. Most commonly disab	led on systems with multiple netwo	ork cards, in order to explicitly spe
AGS History Realtime	Network Bind Interface	34.226.198.214 The IP address of the networ	k interface to use fo	r redundancy. Only used if "auto	o-detect" is turned off.		
PC-UA SERVER Certificates Devices	Autodetect HTTP Address	To specify an explicit HTT (default: true)	Paddress for clients	to use, turn this off. Most users	will leave autodetect or	ı.	
Settings		Address		HTTP Port		HTTPS Port	
		edge2		8088		443	Remove
Servers		edge2-backup		8088		443	Remove
Quick Client		Add New Address		0000		443	Kentove
	HTTP Addresses	Add New Address					
Settings				80		443	Add
EQUENTIAL FUNCTION							
Settings						med or port-forwarded redundancy	

° Set the Master Node Address. Note in the configuration below a hostname is being used. This should be the primary network interface address of the Ignition Edge 2 Gateway.

Set the Master Node Address					
Ignition-edge2 - Ignition Gater ×	θ				
← → C O edge2-backup:8088/main/web/confi					
	(default:)				
Backup Node Set	tings				
Master Node Address	edge2 The address of the master ignition system.				
Ping Rate	1000 The time, in milliseconds, between messages from the backup to the master. (default: 100)				
Reconnect Period	10000 How often, in millseconds, to re-attempt connection when the backup node is not connected to the master. (default: 1000)				
History Mode	Foll • • • • • • • • • • • • • • • • • •				
	Save Changes				
	ignition by inductive Automation. Copyright 2 202 3017 All rights reserved. View license				

• Finally, click the 'Save Changes' button.

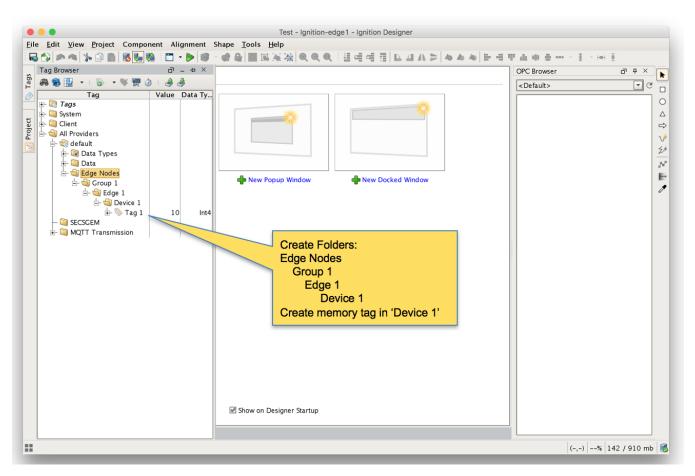
Step 5: Create some tags in Edge 1 and Edge 2

In this step we will use Ignition Designer in the Ignition Edge 1 and Edge 2 instances to create some tags. These tags will be used by MQTT Transmission and the Default Transmitter to push data to MQTT Distributor and MQTT Engine in the Ignition Primary instances.

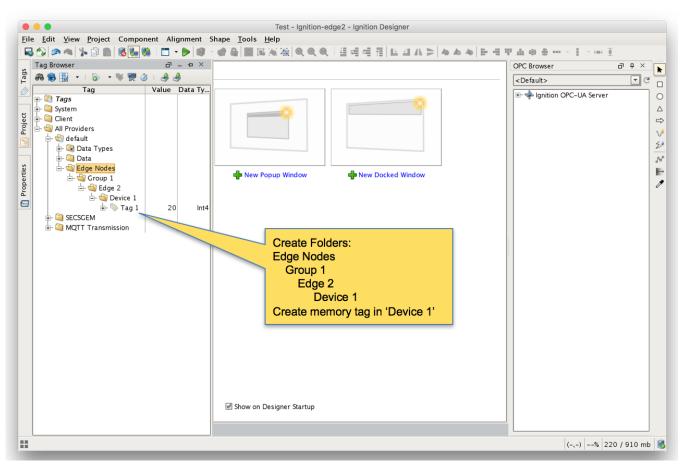
- Using Ignition Designer on Edge 1, do the following:

 - Create a new project called 'Test'.
 In the Tag Browser, confirm there is a folder called 'Edge Nodes'. If there is not, confirm MQTT Transmission is installed.
 - ° In the 'Edge Nodes' folder, create a folder called 'Group 1'.

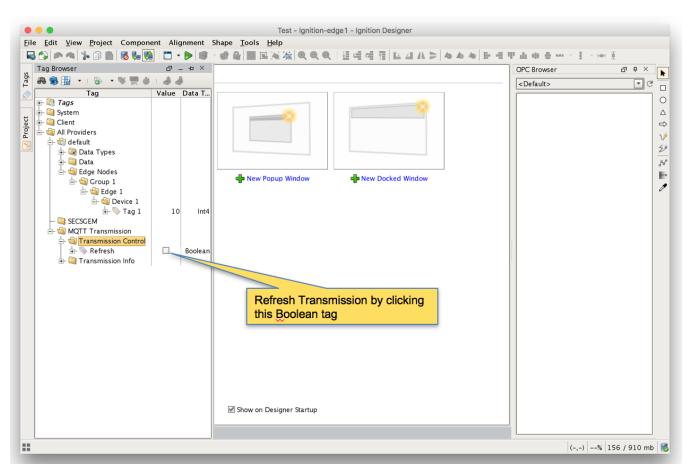
 - In the 'Edge 1' folder, create a folder called 'Edge 1'.
 In the 'Edge 1' folder, create a folder called 'Device 1'.
 - In the 'Device 1' folder, create a Tag called 'Tag 1'.
 - At the end, you should see something similar to what is shown below.



- Using Ignition Designer on Edge 2, do the following:
 - Create a new project called 'Test'.
 - In the Tag Browser, confirm there is a folder called 'Edge Nodes'. If there is not, confirm MQTT Transmission is installed.
 - In the 'Edge Nodes' folder, create a folder called 'Group 1'.
 - In the 'Group 1' folder, create a folder called 'Edge 2'.
 - ° In the 'Edge 2' folder, create a folder called 'Device 1'.
 - In the 'Device 1' folder, create a Tag called 'Tag 1'.
 - At the end, you should see something similar to what is shown below



• Finally, refresh the Transmission runtime. This is done by clicking the 'MQTT Transmission/Transmission Control/Refresh' Boolean tag.



° After clicking the Boolean tag you may need to 'Enable Read/Write Mode'

\bigcirc	Change to Read/Write Mode?
<u> </u>	
Cancel	Enable Read /Write Mode Write Once

Step 6: Force Sync of Backup Instances

The next step to to force the backup Ignition instances to receive their configurations from the master Ignition instances. This will happen automatically eventually but for expediency we're going to force the action.

Repeat the following steps for the following Ignition instances: Primary, Edge 1, and Edge 2
 Browse to the Status menu and then click in the Redundancy box as shown below.

 Ignition-primar 	Status Menu y - gration Gu: x B8/main/web/status/		_	↔ I I I I I I I I I I I I I I I I I I I
Q Search SYSTEMS > Overview Performance Alarm Pipelines Gateway Scripts Modules	Trial Version 1:88:32 We're glad you're test driving our software. Have fur Systems Overview Architecture		Environment	Activate Ignition
Redundancy Reports SFCs Voice Alarming Tags Transaction Groups CONNECTIONS Databases Designers Designers Designers Gateway Network	NO Gateway Network Multiply the power of your Ignition Gateways by combining them into an enterprise ne	NACKUP	Process Id Operating System Java Version Local Time Available Disk Space Detected NICs Systems	10.0.0.38
Gateway Network Store & Forward OPC Connections	Multiply the power of your Ignition Gateways by combining them into an enterprise ne administration, monitoring, deployment, and commissioning process into one central	work. Streamline the location.		% CPU 104mb ctive, Connected

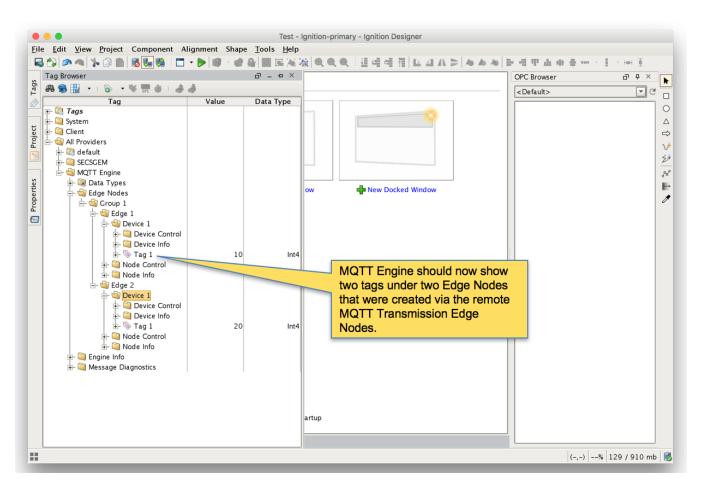
 Force the Re-sync via the button below. This will duplicate the master configuration to the backup Ignition instance it is connected to.

		Force the Re-Syno	;	
	ry - Ignifon Gai: x 88/main/web/status/sys.redundancy?6 A HOME <u>A STATUS</u> O CONFIGU	RE		☆ ♪ ♪ ♡ : USER MANUAL SUPPORT Ladmin Sign Out Launch Designer ✓
Q Search SYSTEMS Overview Performance	Trial Version 1:49:58 Were glad your systems Redundancy	re test driving our software. Have fun.		Activate Ignition
Alarm Pipelines Gateway Scripts Modules • Redundancy Reports SFCs Voice Alarming Tags Transaction Groups CONNECTIONS Databases	Role Master	PeerConnected	Redundancy perties Activity Level Synchronization Str. 4 Good Local Address Peer Address Force ite-Sync	
Databases Designers Devices Gateway Network Store & Forward OPC Connections	Statistics Data Throughput	Quet	ied Updates	

Repeat the above Re-sync steps on the Edge 1 and Edge 2 Ignition instances.

Step 7: Verify MQTT Engine is getting data from the MQTT Transmission Edge 1 and Edge 2

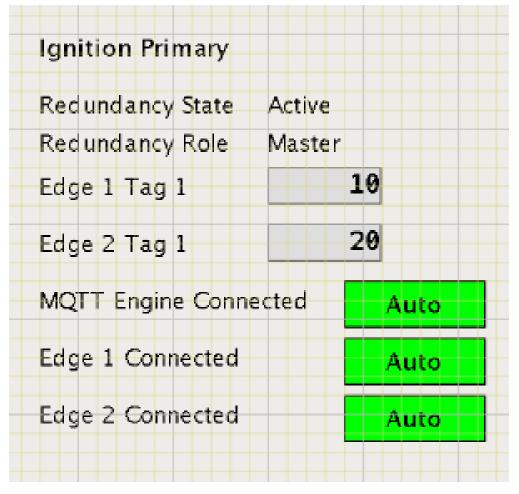
Open Ignition Designer on the Ignition Primary instance. Expand the MQTT Engine tag tree and validate the following tags are present. If they are present and not stale, they are properly connected.



Step 8: Test the Redundancy

In order to test the redundancy, we need to make a few simple dashboards. It is important to note that this can not be tested with Ignition Designer alone. Designer can not be opened from an Ignition backup instance since projects get replicated to the backup instances. So, to show everything working, we'll make some very rudimentary dashboards.

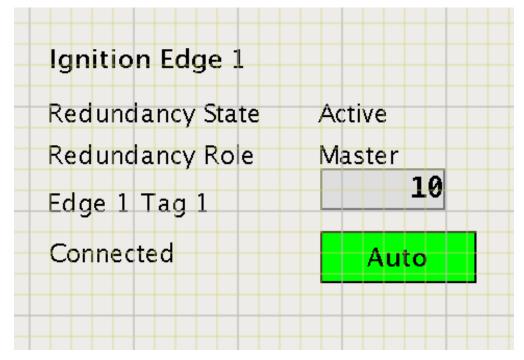
- Ignition Primary
 - Create the following widgets.
 - Label Ignition Primary
 - Label Redundancy State Label with Tag Path of "[MQTT Engine]/Engine Info/Redundancy State"
 - Label Redundancy Role Label with Tag Path of "[MQTT Engine]/Engine Info/Redundancy Role"
 - Label Edge 1 Tag 1 Label with Tag Path of "[MQTT Engine]/Edge Nodes/Group 1/Edge 1/Device 1/Tag 1"
 - Label Edge 2 Tag 1 Label with Tag Path of "[MQTT Engine]/Edge Nodes/Group 1/Edge 2/Device 1/Tag 1"
 - Label MQTT Engine Connected Multi-State Indicator with Tag Path of "[MQTT Engine]/Engine Info/MQTT Clients/Chariot SCADA/Online"
 - Label Edge 1 Connected Multi-State Indicator with Tag Path of "[MQTT Engine]/Edge Nodes/Group 1/Edge 1/Node Info /Online"
 - Label Edge 2 Connected Multi-State Indicator with Tag Path of "[MQTT Engine]/Edge Nodes/Group 1/Edge 2/Node Info /Online"
 - $^{\circ}\;$ When complete it should look similar to what is shown below



• Ignition Edge 1

• Create the following widgets

- Label Ignition Edge 1
- Label Redundancy State Label with Tag Path of "[MQTT Transmission]/Transmission Info/Redundancy State"
 Label Redundancy Role Label with Tag Path of "[MQTT Transmission]/Transmission Info/Redundancy Role"
- Label Edge 1 Tag 1 Label with Tag Path of "[default]/Edge Nodes/Group 1/Edge 1/Device 1/Tag 1"
- Label Connected Multi-State Indicator with Tag Path of "[MQTT Transmission]/Transmission Info/MQTT Clients/Group 1-Edge 1/Online"



Ignition Edge 2

- Create the following widgets
 - Label Ignition Edge 2

 - Label Redundancy State Label with Tag Path of "[MQTT Transmission]/Transmission Info/Redundancy State"
 Label Redundancy Role Label with Tag Path of "[MQTT Transmission]/Transmission Info/Redundancy Role"
 Label Edge 2 Tag 1 Label with Tag Path of "[default]/Edge Nodes/Group 1/Edge 2/Device 1/Tag 1"
 - Label Connected Multi-State Indicator with Tag Path of "[MQTT Transmission]/Transmission Info/MQTT Clients/Group 1-Edge 2/Online"

Ignition Edge 2	
Redundancy State Redundancy Role Edge 2 Tag 1	Active Master 20
Connected	Auto

- Once all three dashboards have been created, save and publish them and close the Ignition Designer windows.
- Now open each of the Ignition client 'Test' projects. With everything running you should see three windows similar to the following.

🗧 😑 🔹 Test - Main Window	Test - Main Window
<u>C</u> ommand Windows <u>H</u> elp	<u>C</u> ommand Windows <u>H</u> elp
Ignition Primary Redundancy State Active Redundancy Role Master Edge 1 Tag 1 10 Edge 2 Tag 1 20 MQTT Engine Connected Auto	Ignition Edge 1 Redundancy State Active Redundancy Role Master Edge 1 Tag 1 Connected Auto
Edge 1 Connected Auto	✓ Trial time remaining: 1:28:23
	C C Test - Main Window
	<u>C</u> ommand Windows <u>H</u> elp
	Ignition Edge 2 Redundancy State Active Redundancy Role Master Edge 2 Tag 1 20
▼ Trial time remaining: 1:28:16	Connected Auto

• At this point we can begin failing Ignition instances. From the Status Redundancy page we can use the 'Force Failover' button as shown below. Of course stopping the actual Ignition instance is another option.

		Click on the Force Failor Button	ver	
🗧 🔍 🚺 Ignition-primary	- Ignition Gate ×			Θ
\leftarrow \rightarrow C (1) primary:808	B/main/web/status/sys.redundancy?8			☆ 🛆 🖸 🗄
Ignition-primary Master				USER MANUAL SUPPORT
Ignition.	A HOME A STATUS & CONFIGURE			≗admin Sign Out
q Search	Trial Version 1:26:25 We're glad you're test			Activate Ignition
SYSTEMS Overview Performance Alarm Pipelines	systems Redundancy			Configuration
Gateway Scripts Modules	Role	Peer Connected	Redundancy Properties	
Redundancy Reports SFCs Voice Alarming Tags Transaction Groups CONNECTIONS	Master	Yes	Activity Level Active Synchronization Status Good Local Address 34.201.169.17 Peer Address 54.211.69.17 Force Re-Sync Force	Failover
Databases Designers Devices Gateway Network Store & Forward	Statistics			
OPC Connections	Data Throughput	Queued	Updates	

• Primary Ignition Failure: Failing the Ignition Primary instance will cause the following. • Ignition Primary will go down and be unreachable

- This results in all MQTT connections being lost.
 Ignition Primary Backup will come up and take the place of Ignition Primary
 MQTT Engine will reconnect on Ignition Primary

The MQTT Transmission instances will reconnect to the new MQTT Server (MQTT Distributor) running in Ignition Primary Backup
 This is all shown in the screenshot below of the Ignition projects. Note all connections are valid and the 'Redundancy Role' of Ignition Primary is now Backup.

Test - Main Window	💿 💿 💿 Test - Main Window
<u>C</u> ommand Windows <u>H</u> elp	<u>C</u> ommand Windows <u>H</u> elp
Ignition Primary Redundancy State Active Redundancy Role Backup Edge 1 Tag 1 10 Edge 2 Tag 1 20 MQTT Engine Connected Auto	Ignition Edge 1 Redundancy State Active Redundancy Role Master Edge 1 Tag 1 Connected <u>Auto</u>
Edge 1 Connected Auto	
Edge 2 Connected Auto	Trial time remaining: 1:12:23
	Test - Main Window
	Command Windows Help
	Ignition Edge 2 Redundancy State Active Redundancy Role Master Edge 2 Tag 1 20 Connected Auto
Trial time remaining: 1:51:37	Trial time remaining: 1:12:28

- Edge 1 Failure: Failing the Ignition Edge 1 instance will cause the following.
 Ignition Edge 1 will go down and be unreachable

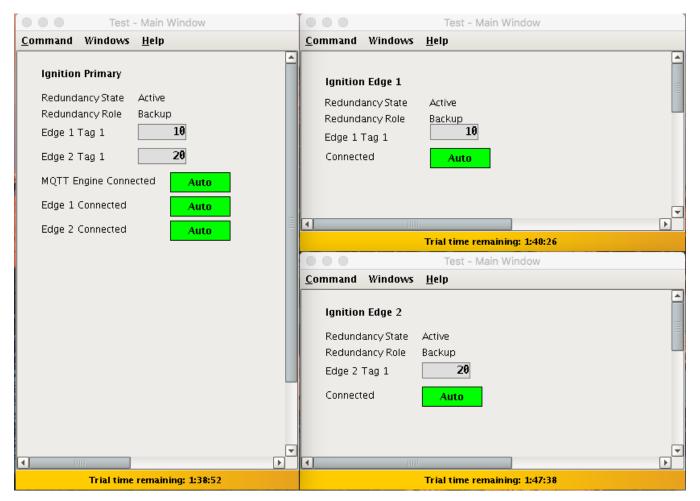
 This results in the MQTT Connection between Ignition Edge 1 and Ignition Primary being lost.
 Ignition Edge 1 Backup will come up and take the place of Ignition Edge 1.
 The MQTT Transmission instance on Ignition Edge 1 Backup will connect to the MQTT Server (MQTT Distributor) running in Ignition Primary

 Primary
 This is all shown in the screenshot below of the Ignition projects. Note all connections are valid and the 'Redundancy Role' of Ignition
 - Edge 1 is now Backup.

C C C Test	t - Main Window	000	Test - Main Window
<u>C</u> ommand Windows	s <u>H</u> elp	<u>C</u> ommand Windows	<u>H</u> elp
Ignition Primary Redundancy State Redundancy Role Edge 1 Tag 1 Edge 2 Tag 1 MQTT Engine Conr	Master 10 20 nected Auto	Ignition Edge 1 Redundancy State Redundancy Role Edge 1 Tag 1 Connected	Active Backup 10 Auto
Edge 1 Connected	Auto		
Edge 2 Connected	Auto		Trial time remaining: 1:45:04
		000	Test - Main Window
		Command Windows	Help
		Ignition Edge 2 Redundancy State Redundancy Role Edge 2 Tag 1 Connected	Active Master 20 Auto
	▼ 		
▲			

- Failure of all Master Nodes: Failing all master Ignition instances (Primary, Edge 1, and Edge 2) will cause the following.
 Ignition Primary, Edge 1, and Edge 2 will all go down and be unreachable

 This results in all MQTT connections being lost
 Ignition Primary Backup, Edge 1 Backup, and Edge 2 Backup will all come up and start their MQTT services.
 The new MQTT Transmission instances on Ignition Edge 1 Backup and Ignition Edge 2 Backup will connect to the new MQTT Server (MQTT Distributor) running in Ignition Primary Backup
 This is all shown in the screenshot below of the Ignition projects. Note all connections are valid and the 'Redundancy Role' of all instances is now Backup
 - instances is now Backup.



To summarize, this tutorial shows how Ignition and the MQTT Modules can be used to create a resilient infrastructure that is able to withstand failures of machines and network connections within the architecture. As noted earlier, this tutorial shows the basic requirements of configuring failover support with Ignition and the MQTT Modules. This can be further improved with additional advanced concepts. Feel free to contact sales@cirrus-link.com for more information.