Hybrid Connector Security

By Andrew Cook

CONTENTS

INTRODUCTION

Itron's Hybrid Connector is a solution whose only purpose is securely transmitting data from a customer premise to Itron's Cloud environment in Azure. Data never goes or is used anywhere else.

For this discussion, it is important to understand there are two (2) components of the Hybrid Connector:

1) On-premises Hybrid Service (OHS)

2) Hybrid Connector Proxy Service

Before Itron Analytics or other Itron Cloud Service applications can connect to your head end system or other data sources, an On-premises Hybrid Service (OHS) needs to be installed and configured. The OHS uses TLS 1.2 to facilitate quick and secure behind-the-scenes communication between customer data sources, such as OpenWay Operations Center Collection Manager, and Itron Cloud Platform services, such as Itron Analytics.

Installing and configuring an OHS is usually done by an administrator. It will require special knowledge of your on-premises servers and Server Administrator permissions.

This whitepaper doesn't provide step-by-step guidance on how to install and configure the gateway. For that, be sure to see your Itron Cloud Platform Services documentation. This is meant to provide you with an in-depth understanding of how the OHS/Itron Hybrid Connector (IHC) works and include details about how the OHS/IHC securely connects to your data source.

ON-PREMISES HYBRID SERVICE (OHS)

The OHS is a windows service that you install and configure on your network to access an on-premises data source, such as a head end (OWOC Collection Manager or ChoiceConnect, for example).

It acts as a bridge between the Itron Cloud environments and your on-premises data center by monitoring a specific tenant queue for messages on Azure Service Bus. Data transfer between the cloud and the OHS is secured through the Hybrid Connector Proxy Service and incorporates TLS 1.2, which uses Azure Service Bus to create a secure channel for each tenant between the cloud and your on-premises server through an outbound connection on the OHS. There are no inbound connections that you need to open on your on-premises firewall. Itron manages the Service Bus for you, so there are no additional costs or configuration steps required.

The closer the OHS is to the data source server, the faster the connection will be. If you can install the OHS on the same server as the data source (data collection head end server, for example), that is best to avoid network latency between the OHS and the on-premises server.

The security benefit to this is that your data source remains secured within your network and network security mechanism; data is only transferred through the secure channel used by the OHS.

OHS will access your data source using the following mechanisms:

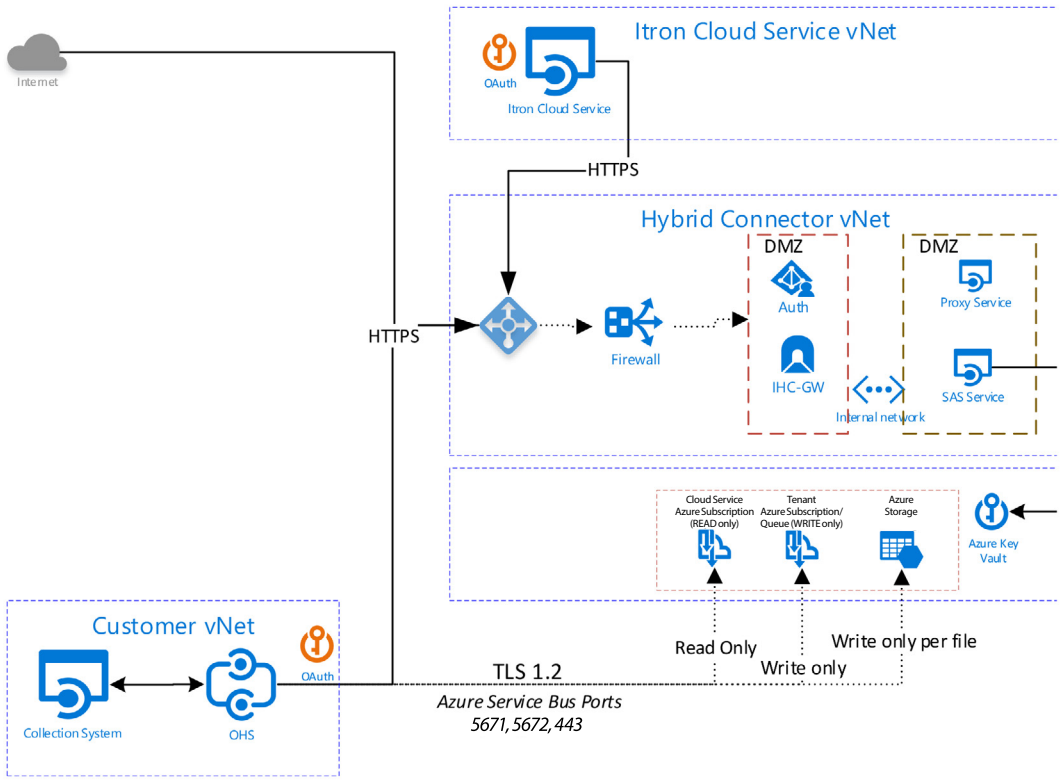
Data Feed: The data feed mechanism is used for subscribing to data streams published from an on-premises system using a proxy service. This is specifically used for requesting and receiving OWOC Collection Manager Interrogations for readings, events, exceptions, and alarms.

Request/Response: OHS can initiate service calls and return responses to interact with Service Oriented Architecture systems. This is specifically used to initiate a request for an Interactive Read, Ping, or Valve commands from OWOC Collection Manager or an On Demand Read from ChoiceConnect Fixed Network.

File Transfer: For file uploads from an on-premise data source, OHS detects new files that are placed into a shared folder, uploads them to a secure Azure Blob Storage Account using TLS 1.2, and then notifies and provides connection information to authorized Itron Cloud Services so they can process these files.

For file downloads from Itron Cloud services to on-premise, a service will send a notification to the proxy service of a file stored on a secure Azure Blob Storage Account to the OHS, which will then download the file to a configured folder using TLS 1.2.

HOW HYBRID CONNECTOR WORKS



HYBRID CONNECTOR PROXY SERVICE

The Itron Hybrid Connector (IHC) Proxy Service uses Azure Service Bus to manage requests between the Itron Cloud Service (such as Itron Analytics Integration Service) and the OHS on a secure channel for each tenant's on-premises data source.

Let's first look at what happens when an Itron Cloud Service interacts with a customer's on-premises head end, such as OWOC Collection Manager.

Data Feed

1. An Itron Cloud Service, such as the Itron Analytics Integration Service, subscribes to one or more specific data feeds being targeted, such as Interrogation Readings and Job Updates from OWOC Collection Manager.
2. When a subscriber posts a subscription, the proxy service will deliver this information to the OHS on a secure channel using TLS 1.2.
3. The OHS will store this information in its subscriber list and will use this list whenever data comes in for a specific data feed.
4. The OHS monitors the specific queues for on-premises system data feeds. When data is delivered to one of the queues, the OHS will receive the data and publish it to subscribers in its subscriber list for ingestion.

Request/Response

1. An Itron Cloud Service, such as the Itron Analytics Integration Service, serves a request to IHC and then request will be relayed to the OHS installed within the customer's on-premises network.
2. OHS sends the request to the on-premises data source (such as OWOC-CM).
3. The on-premises service responds back to OHS.
4. OHS then sends the response to the Cloud Service Bus Queue as a message for the requesting service to retrieve and process.

File Transfer

1. When the OHS is installed and started, a folder is created at the location specified by the OHS configuration files. This folder contains subfolders for each file type configured to be transferred to an Itron Cloud Service.
2. The OHS monitors all specifically configured folders within the shared root folder.
3. When a user or a process places a file in one of these directories, the OHS will send a message to proxy service.
4. The proxy service relays the message from IHC to notification service.

5. The notification service then sends notification any subscribed Itron Cloud Service that a new file has been detected and then uploads the file to Azure Blob Storage.
6. Once uploaded, the OHS will send a message to any subscribed Itron Cloud Service that a new file has been uploaded.
7. Itron Cloud Services will then be able to retrieve the file for processing from the notification.

LIST OF AVAILABLE DATA SOURCE TYPES

Data Source	Method
OWOC-CM Interrogation Readings (Web Service)	Data Feed
OWOC-CM Job Updates (Web Service)	Data Feed
OWOC-CM Exceptions (Web Service)	Data Feed
OWOC-CM Interactive Reads (WCF)	Request/Response
OWOC-CM Remote Disconnect (WCF)	Request/Response
ChoiceConnect Fixed Network On-Demand Reads (WCF)	Request/Response
Master Data Import (MDI) XML Files	File Transfer
Common Reading Format (CRF) XML Files	File Transfer
Common Event Format (CEF) XML Files	File Transfer
Distribution Equipment Hierarchy (DEH) XML Files	File Transfer
Weather CSV Files	File Transfer
AMM Tibco Interrogation Readings	Data Feed
AMM Tibco Alarms	Data Feed
AMM Tibco On-Demand Reads	Data Feed
SensorIQ High-Frequency Reads	Data Feed
SensorIQ Traps	Data Feed
Program-Based Configuration (PBC) XML Files	File Transfer
Wom - Various Files	File Transfer
Metering Exchange Protocol (CMEP) Files	File Transfer
SSN Files	File Transfer

AUTHENTICATION

For the OHS to connect to any Itron Cloud Service, each specific OHS instance and the subscribing Itron Cloud Service must be authenticated using Open Authentication (OAuth) 2.0 authentication tokens. Once authentication has been made, individual messages are not signed.

Each specific tenant (customer) must be authenticated for each transaction using the following information:

Item	Description
Client ID	Unique identifier of the Itron Cloud Service subscriber for a given Tenant. This is the Itron Azure DeveOps service and tenant that is requesting the integration. Similar to a user name.
Client Secret	Tenant specific “secret” that proves to the uthentication server that the OHS and subscribers are authorized to make requests. Similar to a password.
Client Scope	Similar to a role, tells the authorization service what the scope of functions the client is allowed.

This information is used to provide authentication for specific services to specific tenants using OHS and ensures secure communication between the on-premises data source and the Itron Cloud Service. Both are required or the request is rejected.

ROLE-BASED SECURITY

Once a subscriber or the OHS has been authenticated using the Client ID, Client Secret and Client Scope, the Hybrid Connector authorization service provides a token with a validity of one-hour duration access to the specific tenant data defined. This secures the IHC API by restricting access beyond the token validity, after which the token must be replenished. OHS connects to the IHC service bus and storage account using SAS tokens which will be rotated every ~30 minutes.

WINDOWS SERVICE ACCOUNT

In order to interact with on premise data sources, the OHS needs to be configured to run using a local administrator account for the Windows Service logon credential on the machine it is installed. It must have the rights of Log on as a service and the account should not be the same account used to access any Itron Cloud services. If the data source is on a different machine from where the OHS is installed, the account will also need domain access. The account should not be the same account used to access any Itron Cloud services.

PORTS AND DOMAINS

The OHS creates an outbound connection to Azure Service Bus using Transmission Control Protocol (TCP) and uses the Advanced Message Queuing Protocol (AMQP) with TLS 1.2 to send and receive messages using outbound port 5671, 5672 and 443. Firewall rules must allow these outbound connections.

Here is a listing of fully qualified domain names used by the gateway. These must be whitelisted by the network where the OHS is installed (US West reference shown below).

Component	Host	Port (Outbound Only)	Protocol	Required	Reason
Application insight for remote log analysis (public)	dc.applicationinsights.azure.com	443	HTTPS	Required	To send OHS and management services logs to application insight.
	dc.applicationinsights.microsoft.com				
	dc.services.visualstudio.com				
	westus2-1.in.applicationinsights.azure.com				
Azure service bus (public)	sb-usw-ihc-ps-prod.servicebus.windows.net	5671, 5672	AMQP (Default)	Required	To allow OHS to communicate with IHC-owned service bus.
		9350 - 9354	SBMP	Required	
		443	HTTPS	Required	
		80	HTTP	Optional	
Azure storage (public)	str1use1ihc1ps1prod.blob.core.windows.net	443	HTTPS, TLS	Required	To allow OHS to access IHC owned storage account to perform file upload/download and data transfer operations through blob.
Identity (Itron)	idenserver.itrontotal.com/connect/token	443	HTTPS	Required	OHS to access identity endpoint to fetch token for authenticate/authorize IHC services.
IHC.GW (Itron)	services.itrontotal.com/api	443	HTTPS	Required	Gateway endpoint to access IHC related backend services. (Notification, SAS & Proxy services).
Itron ADS URL (in case of OHS installation using release pipeline)	itron.visualstudio.com	443	HTTPS	Optional	Perform OHS installation through ADS release pipeline to the server/Virtual Machine.
	download.visualstudio.microsoft.com	443	HTTPS	Optional	To download installer package from blob while performing remote installation.
Monitor hub URL	k8s.itrontotal.com	443	HTTPS	Required	Required Access to Management service to perform Configuration and Health Check operations from On-Prem Hybrid Service UI.

SECURE COMMUNICATION WITH AZURE SERVICE BUS

OHS uses Transport Layer Security (TLS) 1.2 on Azure Service Bus to communicate with Itron Cloud Services. It automatically selects between the TCP or HTTPS modes based on an auto-detection mechanism that probes whether either connectivity option is available for the current network environment. If both are available, the system will choose TCP by default. No additional configuration is required to secure communication.

Itron

2111 North Molter Road
Liberty Lake, WA 99019 USA