Net.TCP Port Sharing

Windows Communication Foundation (WCF) provides a new TCP-based network protocol (net.tcp://) for high-performance communication. WCF also introduces a new system component, the Net.TCP Port Sharing Service that enables net.tcp ports to be shared across multiple user processes.

Background and Motivation

When the TCP/IP protocol was first introduced, only a small number of application protocols made use of it. TCP/IP used port numbers to differentiate between applications by assigning a unique 16-bit port number to each application protocol. For example, HTTP traffic today is standardized to use TCP port 80, SMTP uses TCP port 25, and FTP uses TCP ports 20 and 21. Other applications using TCP as a transport can choose another available port number, either by convention or through formal standardization.

Using port numbers to distinguish between applications had security problems. Firewalls are generally configured to block TCP traffic on all ports except for a few well-known entry points, so deploying an application that uses a non-standard port is often complicated or even impossible due to the presence of corporate and personal firewalls. Applications that can communicate over standard, well-known ports that are already permitted, reduce the external attack surface. Many network applications make use of the HTTP protocol because most firewalls are configured by default to allow traffic on TCP port 80.

The HTTP.SYS model in which traffic for many different HTTP applications is multiplexed onto a single TCP port has become standard on the Windows platform. This provides a common point of control for firewall administrators while allowing application developers to minimize the deployment cost of building new applications that can make use of the network.

The ability to share ports across multiple HTTP applications has long been a feature of Internet Information Services (IIS). However, it was only with the introduction of HTTP.SYS (the kernel-mode HTTP protocol listener) with IIS 6.0 that this infrastructure was fully generalized. In effect, HTTP.SYS allows arbitrary user processes to share the TCP ports dedicated to HTTP traffic. This capability allows many HTTP applications to coexist on the same physical machine in separate, isolated processes while sharing the network infrastructure required to send and receive traffic over TCP port 80. The Net.TCP Port Sharing Service enables the same type of port sharing for net.tcp applications.

Port Sharing Architecture

The Port Sharing architecture in WCF has three main components:

- A Worker Process: Any process communicating over net.tcp:// using shared ports.
- The WCF TCP transport: Implements the net.tcp:// protocol.
- The Net.TCP Port Sharing Service: Allows many worker processes to share the same TCP port.

The Net.TCP Port Sharing Service is a user-mode Windows service that accepts net.tcp:// connections on behalf of the worker processes that connect through it. When a socket connection arrives, the port sharing service inspects the incoming message stream to obtain its destination address. Based on this address, the port sharing service can route the data stream to the application that ultimately processes it.

When a WCF service that uses net.tcp:// port sharing opens, the WCF TCP transport infrastructure does not directly open a TCP socket in the application process. Instead, the transport infrastructure registers the service's base address Uniform Resource Identifier (URI) with the Net.TCP Port Sharing Service and waits for the port sharing service to listen for messages on its behalf. The port sharing service dispatches messages addressed to the application service as they arrive.

Installing Port Sharing

The Net.TCP Port Sharing Service is available on all operating systems that support WinFX, but the service is not enabled by default. As a security precaution, an administrator must manually enable the Net.TCP Port Sharing Service prior to first use. The Net.TCP Port Sharing Service exposes configuration options that allow you to manipulate several characteristics of the network sockets owned by the port sharing service. For more information, see How to: Enable the Net.TCP Port Sharing Service.

Using Net.tcp Port Sharing in an Application

The easiest way to use net.tcp:// port sharing in your WCF application is to expose a service using the NetTcpBinding and then to enable Net.TCP Port Sharing Service using the PortSharingEnabled property.

For more information about how to do this, see How to: Configure a Windows Communication Foundation Service to Use Port Sharing.

Security Implications of Port Sharing

Although the Net.TCP Port Sharing Service provides a layer of processing between applications and the network, applications that use port sharing should still be secured as if they were directly listening on the network. Specifically, applications that use port sharing should evaluate the process privileges under which they run. Consider running your application using the built-in Network Service account, which runs with the minimal set of process privileges required for network communication.

See Also

Configuring the Net.TCP Port Sharing Service
Hosting
How to: Configure a Windows Communication Foundation Service to Use Port Sharing
How to: Enable the Net.TCP Port Sharing Service

;