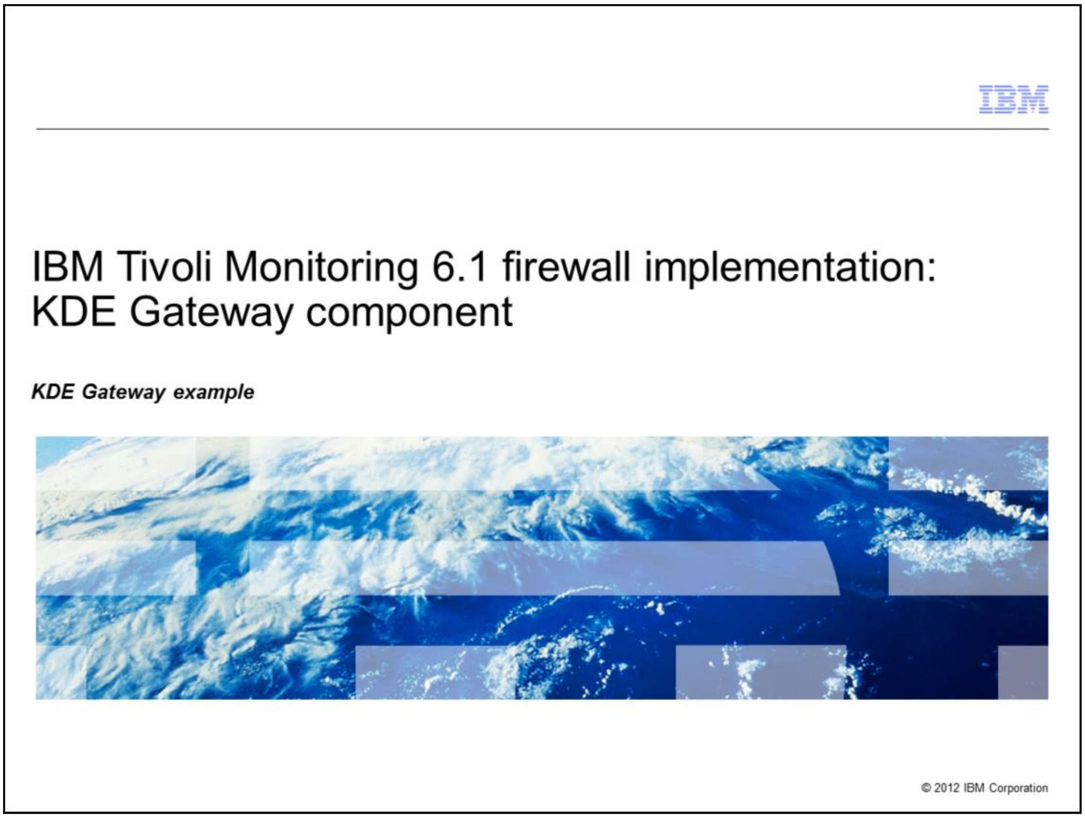
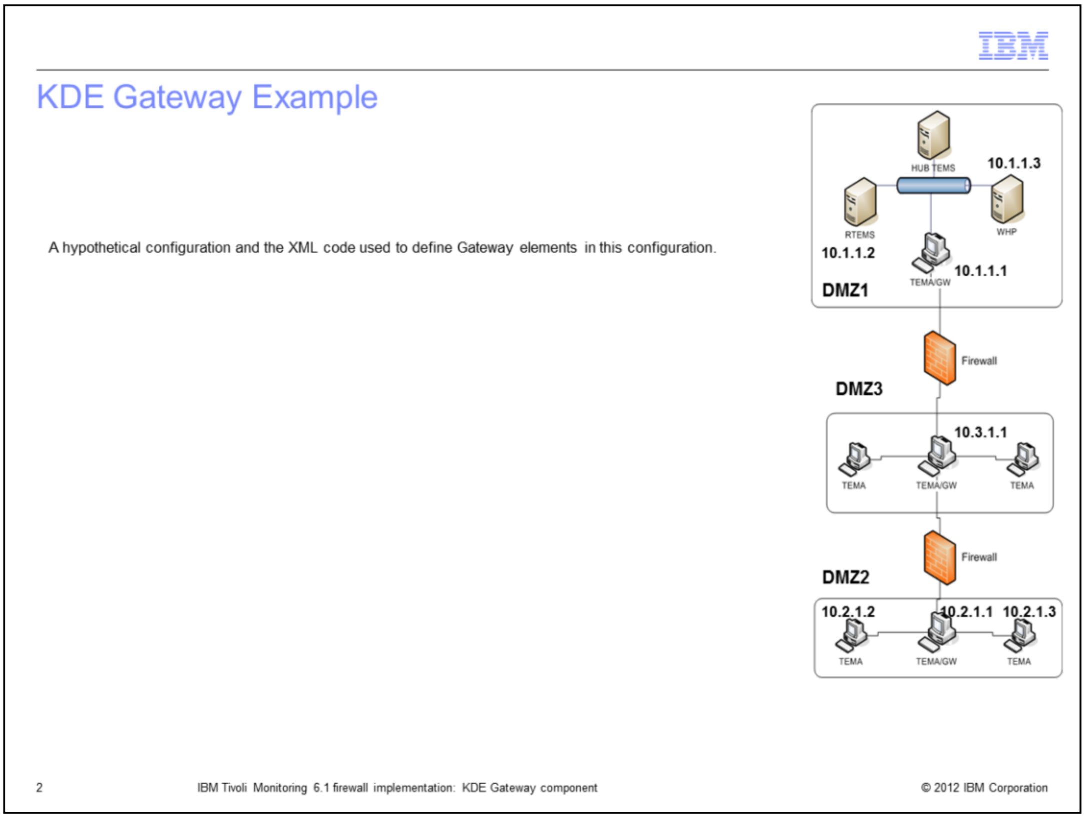


IBM Tivoli Monitoring 6.1 firewall implementation: KDE Gateway component

KDE Gateway example

IBM Tivoli Monitoring 6.1 Firewall Implementation: KDE Gateway component

KDE Gateway example

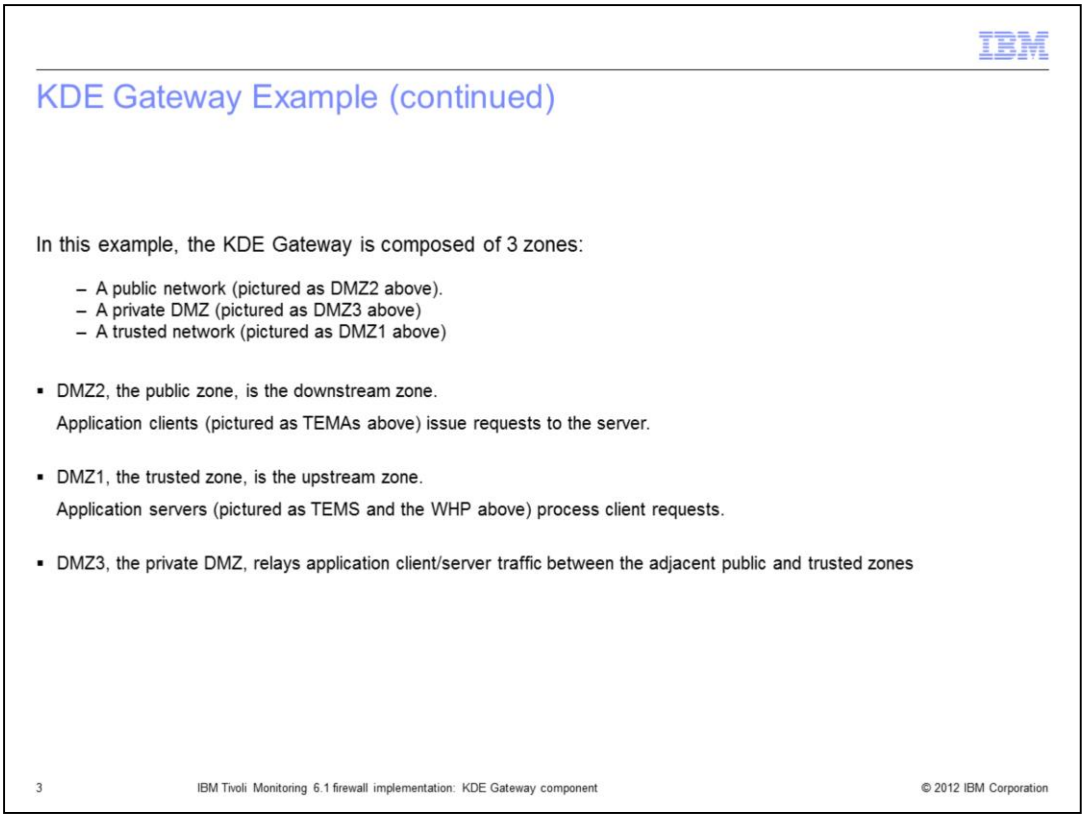


KDE Gateway Example

A hypothetical configuration and the XML code used to define Gateway elements in this configuration.

2 IBM Tivoli Monitoring 6.1 firewall implementation: KDE Gateway component © 2012 IBM Corporation

Here is a simple topology with the IP address reported in the screen capture.



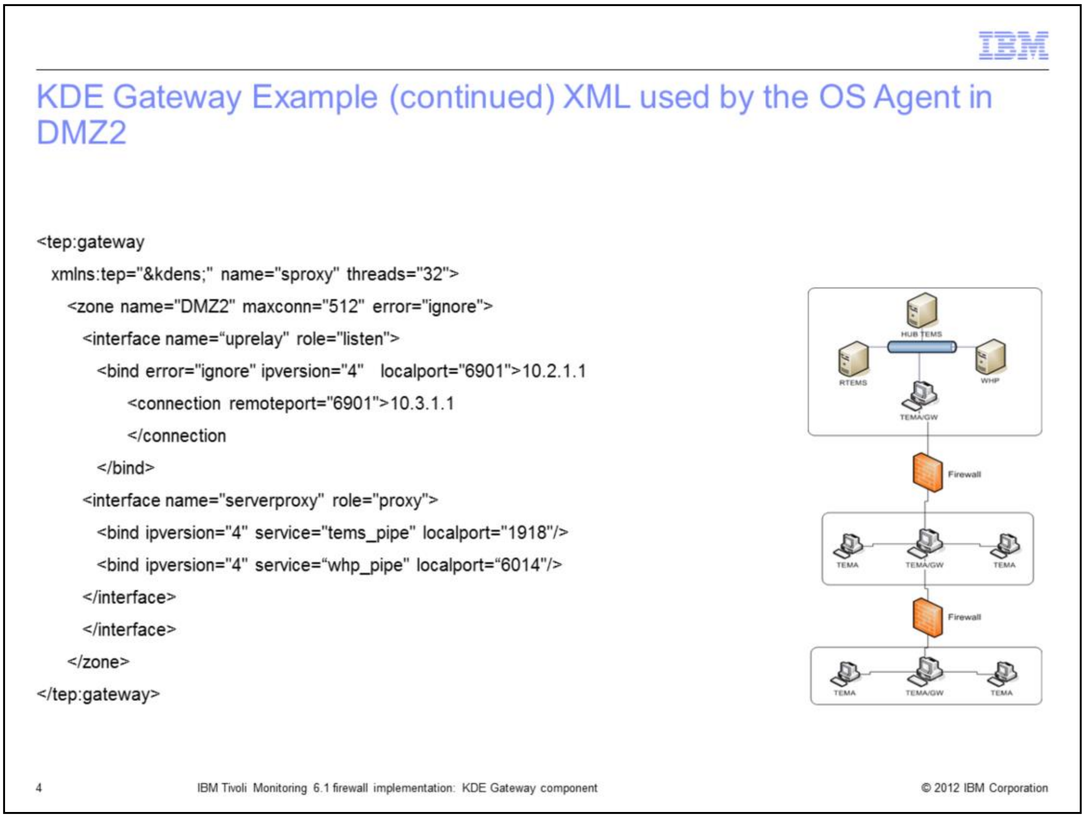
KDE Gateway Example (continued)

In this example, the KDE Gateway is composed of 3 zones:

- A public network (pictured as DMZ2 above).
- A private DMZ (pictured as DMZ3 above)
- A trusted network (pictured as DMZ1 above)

- DMZ2, the public zone, is the downstream zone.
  Application clients (pictured as TEMAs above) issue requests to the server.
- DMZ1, the trusted zone, is the upstream zone.
  Application servers (pictured as TEMS and the WHP above) process client requests.
- DMZ3, the private DMZ, relays application client/server traffic between the adjacent public and trusted zones

In this example, there are three zones, the public network (that is DMZ2), the private network (that is DMZ3) and the trusted network (that is DMZ1). In the downstream interface, the public zone, application clients (that is TEMAs for example) issue requests to the server (So requests to the TEMS or to the Warehouse Proxy). In the trusted zone, that is the upstream zone, the application servers will process the client requests and will provide the actual services. The DMZ3, the private DMZ, relays application client/server traffic between the adjacent public and trusted zones.



KDE Gateway Example (continued) XML used by the OS Agent in DMZ2

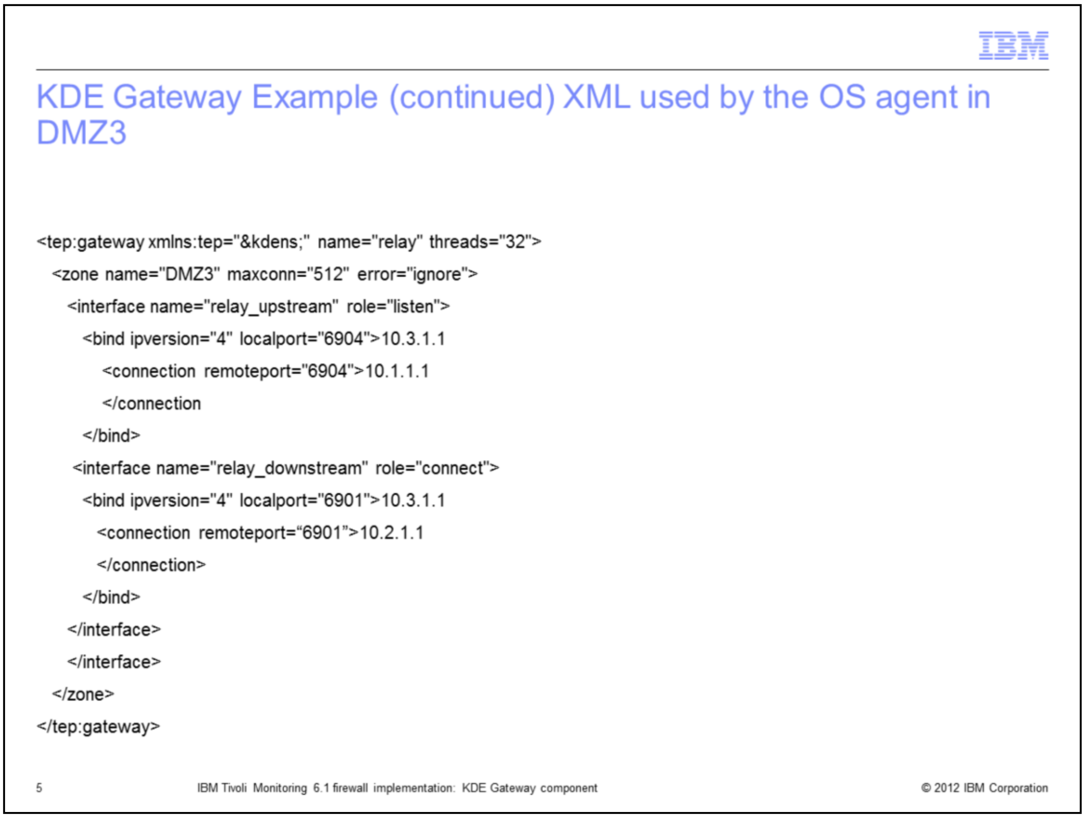
```
<tep:gateway
  xmlns:tep="&kdens;" name="sproxy" threads="32">
    <zone name="DMZ2" maxconn="512" error="ignore">
      <interface name=“uprelay" role="listen">
        <bind error="ignore" ipversion="4"   localport="6901">10.2.1.1
            <connection remoteport="6901">10.3.1.1
            </connection
        </bind>
      <interface name="serverproxy" role="proxy">
        <bind ipversion="4" service="tems_pipe" localport="1918"/>
        <bind ipversion="4" service=“whp_pipe" localport=“6014"/>
      </interface>
      </interface>
    </zone>
</tep:gateway>
```

4 IBM Tivoli Monitoring 6.1 firewall implementation: KDE Gateway component © 2012 IBM Corporation

The gateway topology is described starting from the downstream zone. Starting at DMZ2, first define the gateway that will be implemented in the TEMA with address 10.2.1.1. And it will connect to the TEMA in DMZ3 defined as gateway with IP address 10.3.1.1.

Next, define the gateway feature implemented in the TEMA in DMZ2. Define the upstream interface that is in listen on local port 6901 at address 10.2.1.1. And the remote port will be the same 6901 at address 10.3.1.1. Within the definition of the upstream interface, the downstream interface will be defined, which will in this case can have the role of proxy because this will accept the requests from the application clients.

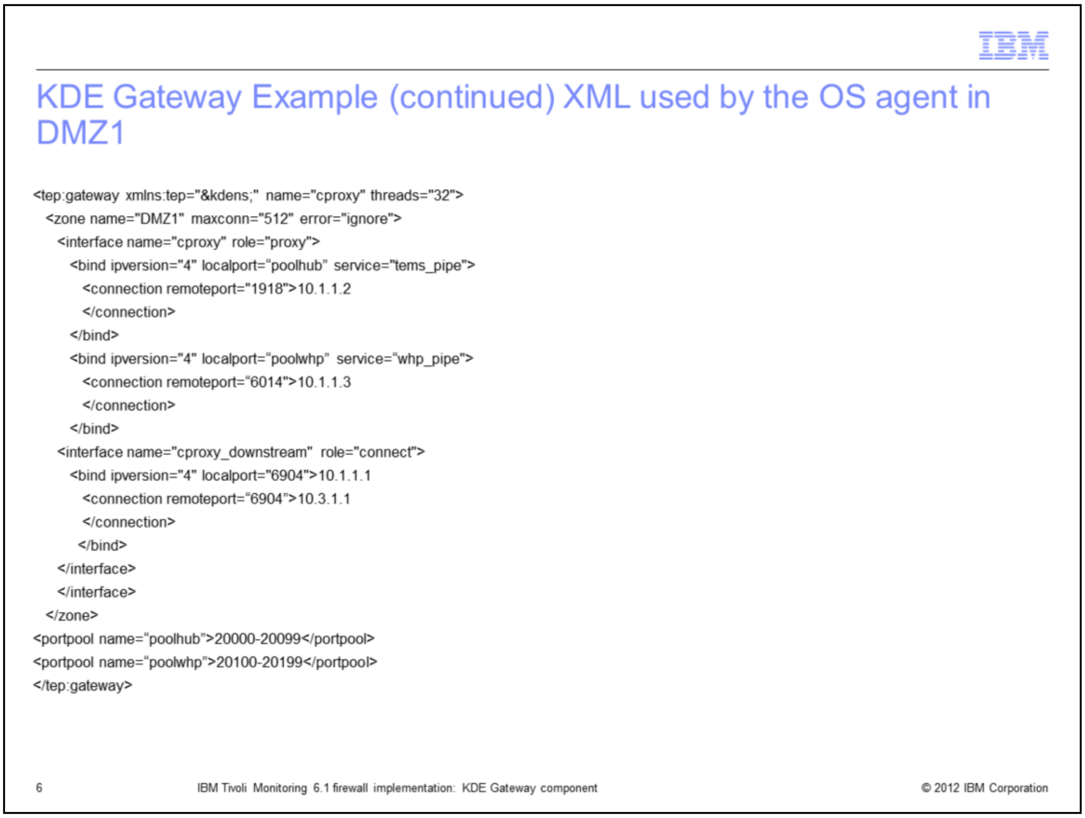
In this case two services are provided: The tems_pipe and the whp_pipe. The port also defines the application clients that have to use if they want to use those two services.



KDE Gateway Example (continued) XML used by the OS agent in DMZ3

```
<tep:gateway xmlns:tep="&kdens;" name="relay" threads="32">
  <zone name="DMZ3" maxconn="512" error="ignore">
    <interface name="relay_upstream" role="listen">
      <bind ipversion="4" localport="6904">10.3.1.1
         <connection remoteport="6904">10.1.1.1
         </connection
      </bind>
     <interface name="relay_downstream" role="connect">
      <bind ipversion="4" localport="6901">10.3.1.1
        <connection remoteport=“6901”>10.2.1.1
        </connection>
      </bind>
    </interface>
    </interface>
  </zone>
</tep:gateway>
```

The gateway implemented in the TEMA in the private zone, that is the one in the middle. In this case you see two interfaces defined: the listen one in the upstream interface and the connect one in the downstream interface.

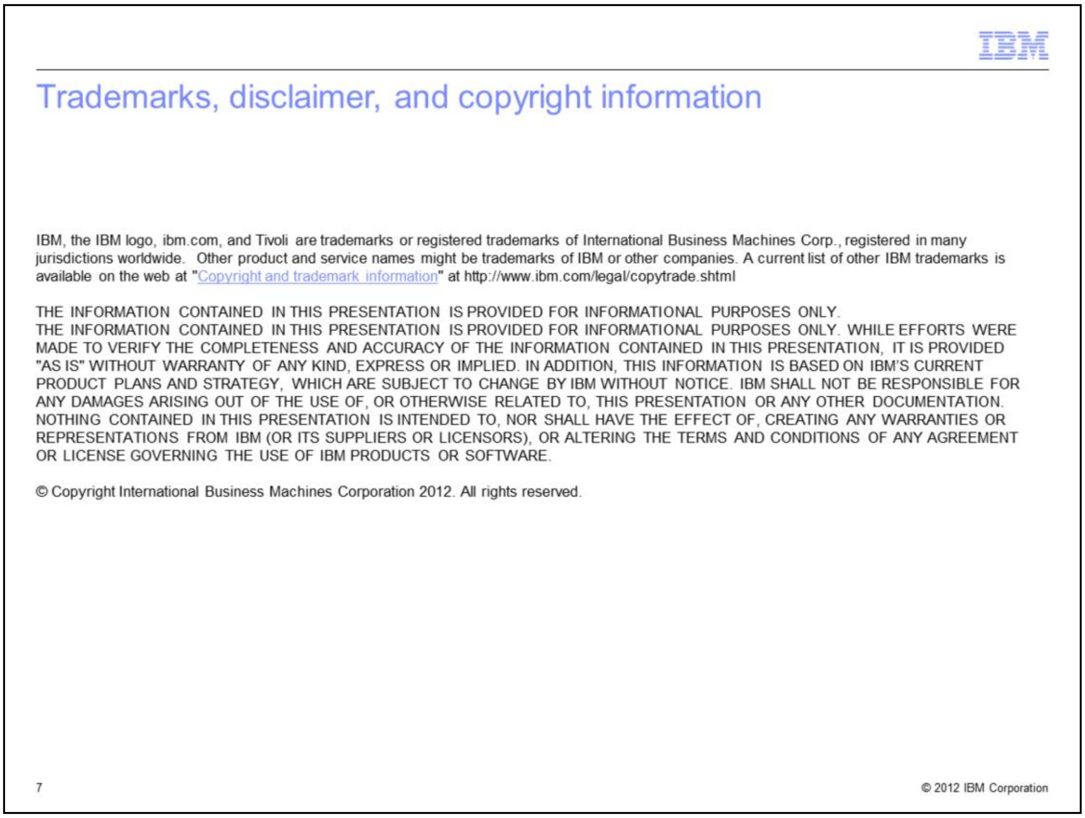


KDE Gateway Example (continued) XML used by the OS agent in DMZ1

```
<tep:gateway xmlns:tep="&kdens;" name="cproxy" threads="32">
  <zone name="DMZ1" maxconn="512" error="ignore">
    <interface name="cproxy" role="proxy">
      <bind ipversion="4" localport=“poolhub” service="tems_pipe">
        <connection remoteport="1918">10.1.1.2
        </connection>
      </bind>
      <bind ipversion="4" localport=“poolwhp” service=“whp_pipe">
        <connection remoteport=“6014">10.1.1.3
        </connection>
      </bind>
    <interface name="cproxy_downstream" role="connect">
      <bind ipversion="4" localport="6904">10.1.1.1
        <connection remoteport=“6904”>10.3.1.1
        </connection>
       </bind>
    </interface>
    </interface>
  </zone>
<portpool name=“poolhub”>20000-20099</portpool>
<portpool name=“poolwhp”>20100-20199</portpool>
</tep:gateway>
```

6 IBM Tivoli Monitoring 6.1 firewall implementation: KDE Gateway component © 2012 IBM Corporation

This will define the upstream interface in the trusted network. As shown, define the same service names as defined in the downstream interface, specifically in the server proxy. You have to be careful to use the same name here that you have used in the server proxy definition, and port.



Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.