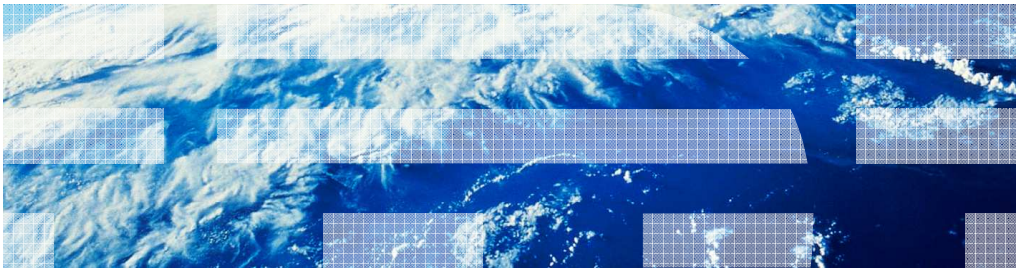
IBM WebSphere DataPower XC10 V2.0

Portal integration – session caching



WebSphere software

This presentation will discuss the IBM WebSphere DataPower XC10™ V2.0 and how it can be used for session caching for IBM WebSphere Portal Server V7.0.

Agenda

- Preparing for integration
  - Prerequisite software and firmware
  - Resources and access required
- Installation and configuration steps
  - Summary of installation and configuration steps
  - Installing the WebSphere eXtreme Scale client
  - Configuring “wps” application for caching
    - Settings for “wps” application
  - Configuring portlet for caching
    - Settings for portlet
  - Setting timeout.resume.session custom property
  - Adding the XC10 appliance certificate
  - Ensuring TLS security is disabled
- Testing portlet
- Summary

This presentation will discuss the prerequisite software products, product levels and firmware levels. You will see a summary of the access and resource requirements. Then you will see a summary of the installation and configuration steps. These steps include: installing the WebSphere eXtreme Scale client, configuring the wps application and portlet for caching, setting the necessary timeout value to allow the resumption of sessions, adding the DataPower XC10 appliance certificate to the WebSphere Portal Server installation, and ensuring that Transport Layer Security is disabled to assist in testing. Finally you will test the portlet and look in the DataPower XC10 administrative console to see the graph of the caching activity. This presentation then concludes with a summary of the topics.

Section

Preparing for integration

This section discusses the preparations for WebSphere Portal Server and DataPower XC10 appliance integration.

Prerequisite software and firmware

- IBM WebSphere Portal Server **(required level)**
  - Version 7.0.0.0 or newer
  - Version 6 levels are not supported for http session persistence by WebSphere eXtreme Scale client
- DataPower XC10 appliance and eXtreme Scale Client **(recommended levels)**
  - DataPower XC10 appliance firmware level V1.0.0.5 (fix pack 5)
  - WebSphere eXtreme Scale Client V7.1.0.2 (fix pack 2)

    Or
  - DataPower XC10 appliance firmware level V2
    - Install latest firmware updates, if any
  - WebSphere eXtreme Scale Client V7.1.0.3 or newer
    - Install latest software updates, if any

Here is a summary of the software levels and firmware levels required for integration to work properly.

WebSphere Portal Server must be V7.0.0.0 or newer, since older versions, including version 6, are not supported for http session persistence by the WebSphere eXtreme Scale client.

If you are running DataPower XC10 V1, then you should install the latest firmware level, which is currently V1.0.0.5, or fix pack 5. The recommended WebSphere eXtreme Scale client level for the WebSphere Portal Server is V7.1.0.2, or fix pack 2.

If you are running DataPower XC10 V2 or newer, you should install the latest firmware updates to V2, if any. Then you must install the latest WebSphere eXtreme Scale client, which currently is V7.1.0.3, or fix pack 3.

Resources and access required

- A working WebSphere Portal Server
  - Required level - V7.0.0.0 or newer
    - Suggestion: disable Transport Layer Security (TLS), if enabled, to simplify testing
  - An installed portlet that uses session persistence
- A working DataPower XC10 appliance
  - You must have login for the XC10 that provides authority for:
    - Session cache creation authority

You must begin testing with a working WebSphere Portal Server V7 environment. You should disable Transport Layer Security, if it is enabled, to simplify testing. You must have a portlet installed that uses session persistence.

You must have access to a working DataPower XC10 appliance. You must have a login and password with the necessary authority to allow you to create the session cache you will need for WebSphere Portal Server. You will provide that user's credentials in the WebSphere eXtreme Scale client when you configure the cache settings in WebSphere Portal Server.

Section

Installation and configuration steps

This section will discuss the installation and configuration steps needed for integration.

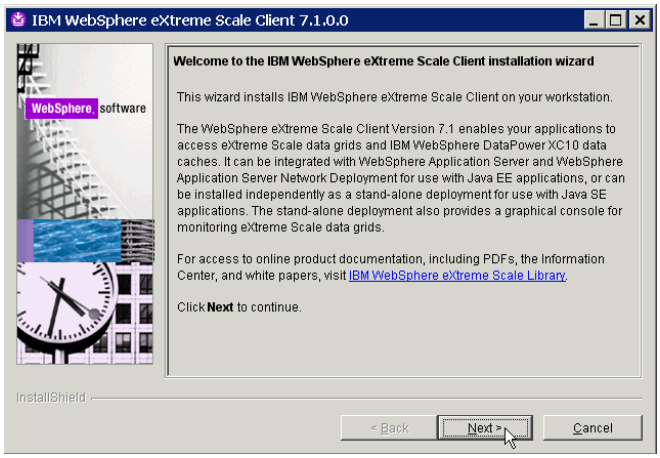
Summary of installation and configuration steps

- Install required level of WebSphere eXtreme Scale client
- Configure WebSphere Portal Server applications for caching
  - The “wps” application
    - Create session cache on XC10 appliance during configuration
  - A portlet you want to participate in http session caching
    - Use “pre-existing” session cache created for the “wps” application
- Set timeout.resume.session custom property in WebSphere Portal Server
- Add the appliance certificate to the WebSphere Portal Server configuration
- Test portlet and observe caching

The installation and configuration include these steps. First, you must install the required level of the WebSphere eXtreme Scale client. You then must provide the cache configuration settings for the “wps” application and the portlet of your choice within WebSphere Portal Server. This example shows the same session cache used for both the “wps” application and the portlet, but this is not required. Then you set the timout.resume.session custom property in WebSphere Portal Server. You must then add the DataPower XC10 appliance certificate to the WebSphere Portal Server configuration. Finally you test the portlet and observe the caching activity in the DataPower XC10 administrative console.

Installing the WebSphere eXtreme Scale client

- Stop all servers in cell
- Install WebSphere eXtreme Scale client
  - V7.1.0.2 if XC10 appliance is firmware level V1.0.0.5
  - V7.1.0.3 if XC10 appliance is firmware level V2
- Augment profiles
  - Dmgr profile
  - wp_portal profile
- Start Dmgr in the cell



8 Portal Integration

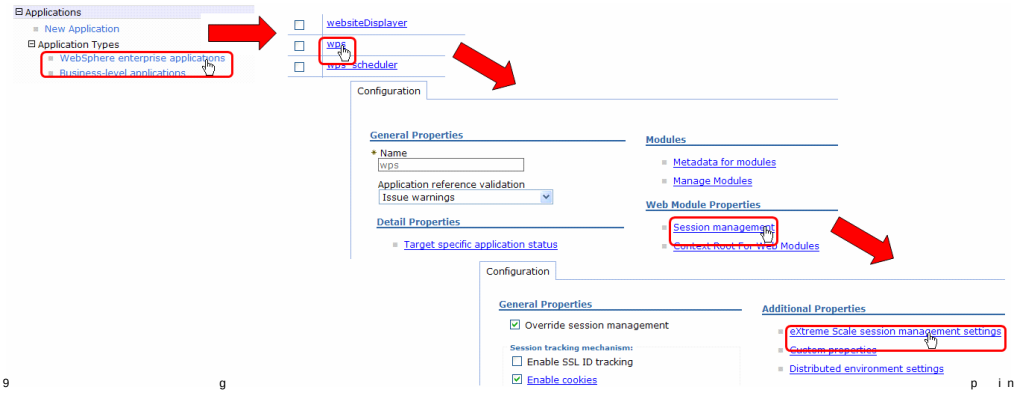
Before you install the WebSphere eXtreme Scale client, you must stop the WebSphere Portal Server. In this example, the portal server is part of a cluster. You must stop all processes in the cell cluster, starting with the WebSphere Portal Server, then the node agent, and finally the deployment manager.

When all WebSphere Portal Server processes have stopped, you can begin the installation of the client. During the installation activities, you are prompted for permission to augment the profiles associated with WebSphere Portal Server. You must allow all profiles to be augmented. In the case of the cluster installation, the augmentation includes the deployment manager and any nodes that run the portal server.

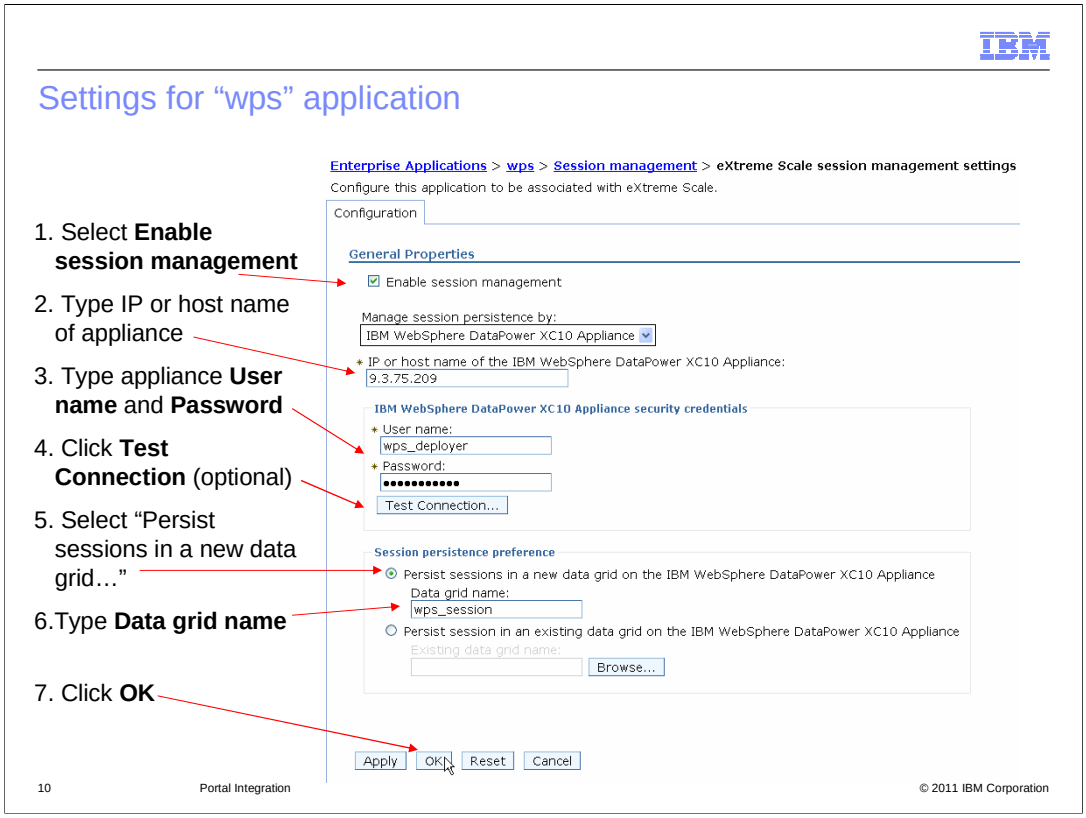
After the installation of the client completes successfully, start the deployment manager.

Configuring “wps” for caching

- Log in to WebSphere Application server administrative console
- Configure wps application for caching
  - Navigate to **Applications > Application Types > WebSphere enterprise applications**
    - Click “wps” to select
    - Under “Web Module Properties”, click **Session management**
    - Under “Additional Properties”, click **eXtreme Scale session management settings**



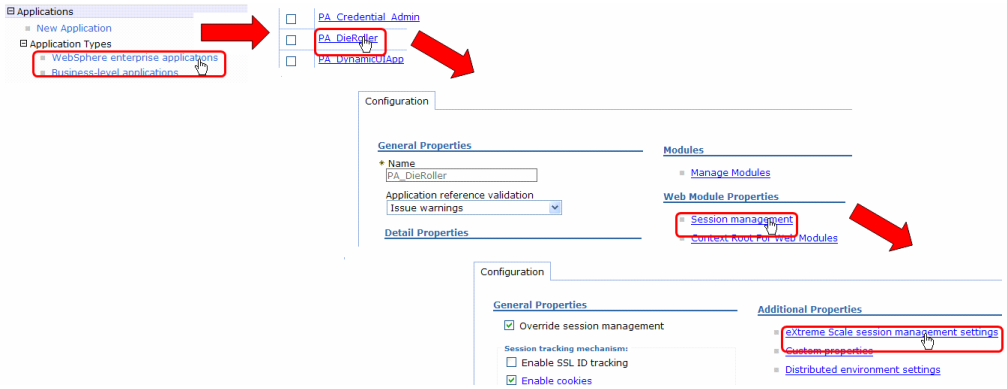
Here are the steps to configure the “wps” application for caching. First, expand **Applications**, then expand **Application Types**, and click **WebSphere enterprise applications**. This provides you with a list of enterprise applications. Find the entry for “wps” and click it. This brings you to a configuration page for the application. Under “Web Module Properties” click **Session management.** This brings you to the session management configuration page. Under “Additional Properties”, click **eXtreme Scale session management settings**. The settings page is shown on the next slide.



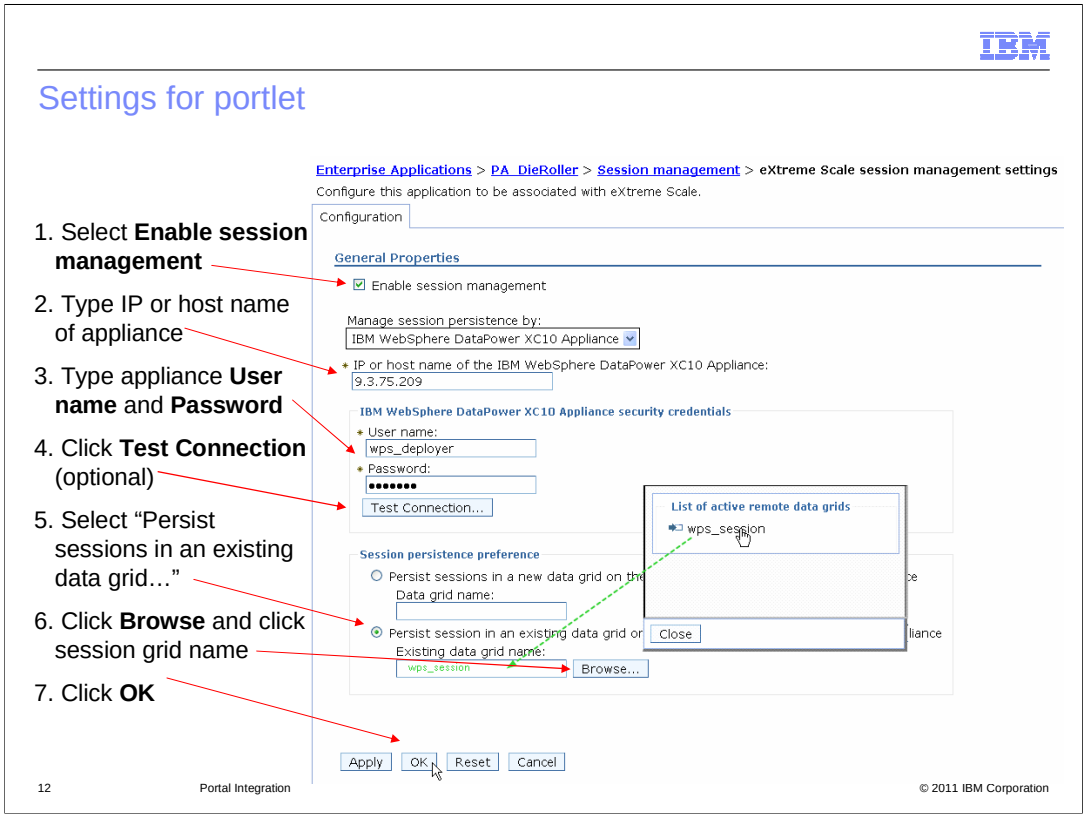
To set the properties for the “wps” application, perform these steps. Step 1 – check **Enable session management** check box. Step 2 – provide the IP address of host name for the DataPower XC10 appliance in the **IP or host name** field. Step 3 – type your user credentials in the **User name** and **Password** fields. This user must have cache creation authority in the DataPower XC10 appliance. Step 4 – (optional step) – click **Test Connection** to ensure you can connect to the appliance using the information you have supplied so far. Step 5 – select **Persist sessions in a new data grid.** Step 6 – type the grid name of your choice into the **Data grid name** field. Step 7 – click **OK.** You will later need to save the settings into the WebSphere Portal Server configuration.

Configuring portlet for caching

- Configure portlet for caching
  - Navigate to **Applications > Application Types > WebSphere enterprise applications**
    - Click “<portlet_name>” to select
    - Under “Web Module Properties”, click **Session management**
    - Under “Additional Properties”, click **eXtreme Scale session management settings**



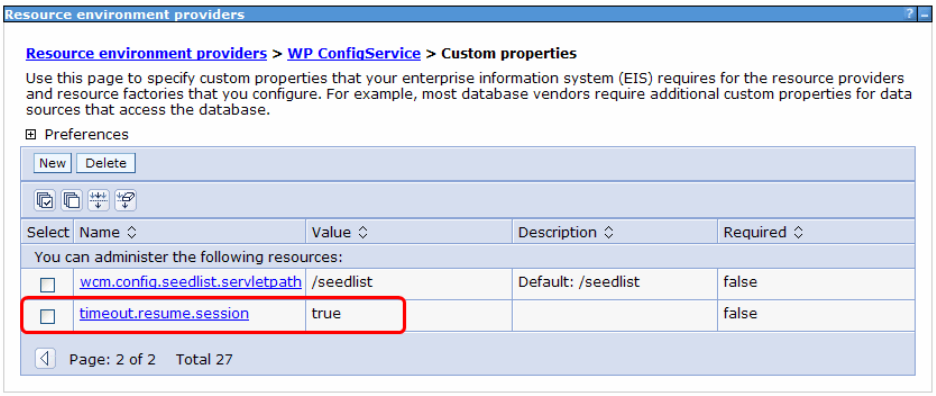
Here are the steps to configure your chosen portlet for caching. The example uses a portlet called “PA-DieRoller”. First, expand **Applications**, then expand **Application Types**, and click **WebSphere enterprise applications**. This provides you with a list of enterprise applications. Find the entry for your portlet and click it. This brings you to a configuration page for the application. Under “Web Module Properties” click **Session management.** This brings you to the session management configuration page. Under “Additional Properties”, click **eXtreme Scale session management settings**. The settings page is shown on the next slide.



To set the properties for the portlet application, perform these steps. Step 1 – check **Enable session management** check box. Step 2 – provide the IP address of host name for the DataPower XC10 appliance in the **IP or host name** field. Step 3 – type your user credentials in the **User name** and **Password** fields. Step 4 – (optional step) – click **Test Connection** to ensure you can connect to the appliance using the information you have supplied so far. Step 5 – select **Persist sessions in an existing data grid.** Step 6 – click **Browse** then select the previously-defined data grid name in the list provided in the pop-up window. This will populate the name into the **Existing data grid name** field. Step 7 – click **OK.** You will later need to save the settings into the WebSphere Portal Server configuration.

Setting timeout.resume.session custom property

- Resources > Resource Environment > Resource Environment Providers > WP_ConfigService > Customer Properties
- Create new property called **timeout.resume.session** with value of **true**
  - Property setting prevents login requests
    - If number of sessions exceeds **sessionTableSize** on client (Portal server) side
      - Default setting for sessionTableSize is 2000
    - If an appliance fail-over occurs



The timeout.resume.session customer property must be set to cater for the situation when the number of portal sessions exceeds the session table size in the WebSphere Portal Server. If the session table size is about to be exceeded, a “least recently used” session is invalidated when the new session is added. When the application associated with the invalidated session becomes active again, the “timeout.resume.session = true” setting allows the session to be reconnected seamlessly to the DataPower XC10 appliance without requiring a login. The default setting for the session table size parameter is 2000.

The session identification also changes on an appliance failover. If the server where a session resides fails, the proxy re-routes the session to a new server. The objectgrid session provider on the new server creates a *new* session object (with a new ID) populated with all the data from the "old" session. In such a case, the “timeout.resume.session = true” setting allows for an appliance failover without requiring the portlet users to sign on again.

Adding the XC10 appliance certificate

- Even with Transport Layer Security disabled, you will need to apply the XC10 appliance certificate to the WebSphere Portal Server server or cell
- Navigate to Portal Server's binary or deployment manager binary and issue:

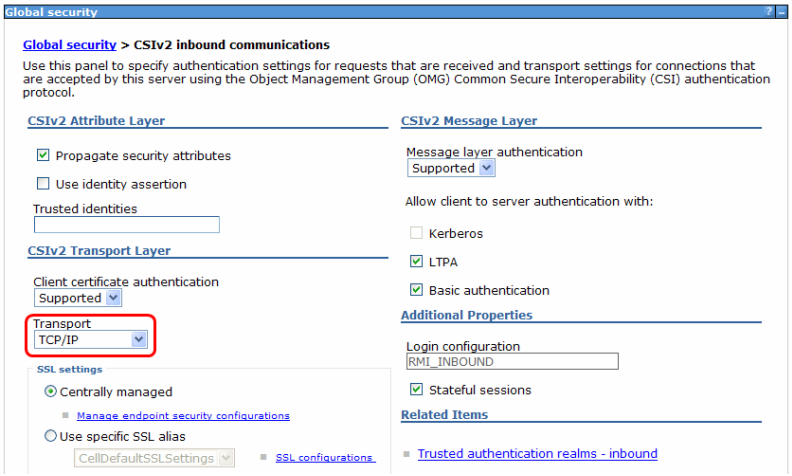
wsadmin.bat/sh –conntype SOAP –port <SOAP_PORT> -lang jython –user wpsadmin –password password –f addXC10PublicCert.py

- No connection is needed to DataPower XC10 in this case
  - Installation of the WebSphere eXtreme Scale client provided the default XC10 public certificate

You must install the DataPower XC10 appliance certificate into the default truststore for the WebSphere Portal Server or, if installed in a cluster configuration, for the cell. To do this, navigate to the server or to the deployment manager binary directory and issue the wsadmin command you see here. The **addXC10PublicCert** python script is invoked and adds the public certificate to the default trust store in the server or cell. The public certificate used for this operation was placed in the server's or deployment manager's properties directory when the eXtreme Scale Client was installed. Thus, no connection is needed to the DataPower XC10 appliance when adding this public certificate.

Ensuring TLS security is disabled in WebSphere Portal Server

- Navigate to **Security > Global security > RMI/IIOP security > CSIv2 inbound connections**
- Under “CSIv2 Transport Layer” ensure that Transport is set to **TCP/IP**
- This can be reset after testing if you plan to use Transport Layer Security



15 Portal Integration

Even though transport layer security is fully supported, to simplify testing of this scenario ensure it is turned off. In the administrative console, expand **Security,** then click **Global security**, expand **RMI/IIOP Security**, then click **CSIv2 inbound communications.** In the **Transport** pull-down menu, ensure that TCP/IP is specified. You can reset this later after you have ensured that caching is working for your portal server.

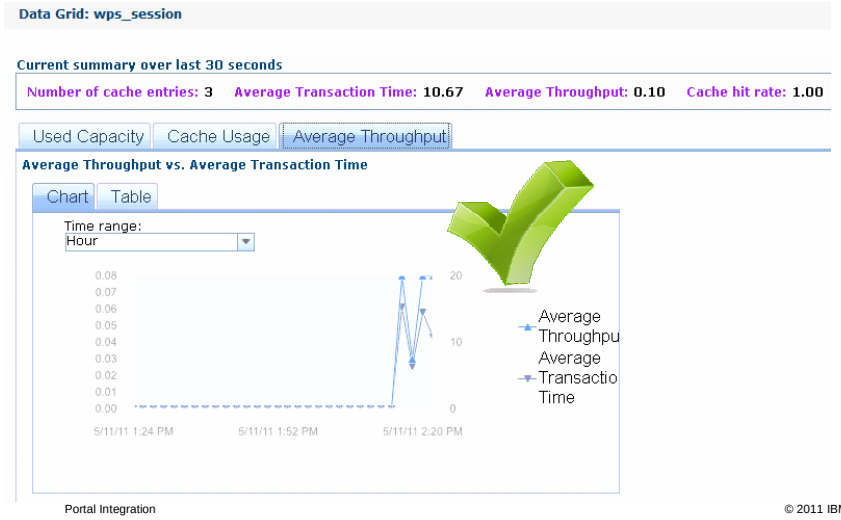
Restart the WebSphere Portal Server cell

- Stop and Start Dmgr in the cell
- Start the node agent in the cell
  - For WebSphere Portal Server cluster, the nodeagent must be started before WebSphere_Portal server will start
- Start WebSphere_Portal server

For a WebSphere Portal Cluster, stop and restart the deployment manager, then start the node agent. In a cluster environment, the node agent is required to be running before you can start the WebSphere Portal server. After the node agent is initialized, then start the WebSphere Portal Server.

Test portlet

- Invoke the portlet several times to cache data
- Login to the DataPower XC10 appliance and review the session grid
- Example: **Monitor > Individual Data Grid Overview** and click **<your_data_grid_name>**



Invoke the portlet you want to use for testing the session cache functionality. After several tests, login to the DataPower XC10 appliance and review the session grid. For example, navigate to **Monitor,** then click **Individual Data Grid Overview** and click your data grid name. Then use the graphical display to see the caching that occurred when you invoked the portlet.

Section

Summary

This section will summarize this presentation.

Summary

- Preparing for integration
  - Required software and firmware levels and resources
- Installation and configuration steps
  - Installing the WebSphere eXtreme Scale client
  - Configuring “wps” application for caching
    - Settings for “wps” application
  - Configuring portlet for caching
    - Settings for portlet
  - Setting timeout.resume.session custom property
  - Adding the XC10 appliance certificate
- Testing portlet

In summary, you saw the steps for integrating a portlet that uses session persistence with the DataPower XC10 appliance. Besides the necessary resources and software and firmware levels, you require the necessary access credentials to allow you to log in to the WebSphere Portal Server. You install the WebSphere eXtreme Scale client and then configure the necessary application portlets for caching. You define the timeout.resume.session custom property and add the DataPower XC10 appliance certificate to the WebSphere Portal Server truststore. Finally you test the portlet and use the DataPower XC10 appliance to review caching activity.

References

- Creating session persistence to a data grid
  http://publib.boulder.ibm.com/infocenter/wdpxc/v1r0/index.jsp?topic=/com.ibm.websphere.datapower.xc.doc/common/tsessionapp.html
- Configuring HTTP session manager with WebSphere Portal (link works after June 15, 2011)
  http://publib.boulder.ibm.com/infocenter/wdpxc/v2r0/topic/com.ibm.websphere.datapower.xc.doc/txshttpportal.html
- Redbook: Scalable, Integrated Solutions for Elastic Caching Using IBM WebSphere eXtreme Scale
  http://www.redbooks.ibm.com/redbooks/pdfs/sg247926.pdf

Here are some helpful resources. The first link is an article that describes in general how to configure session persistence to a data grid. The second link tells you specific details about how to configure the DataPower XC10 appliance for session persistence with WebSphere Portal Server. The third link references an IBM Red Book article which includes a chapter that discusses configuring WebSphere Portal Server to use session persistence with IBM WebSphere eXtreme Scale.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_XC10_Portal_Integration.ppt

This module is also available in PDF format at: ../XC10_Portal_Integration.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information