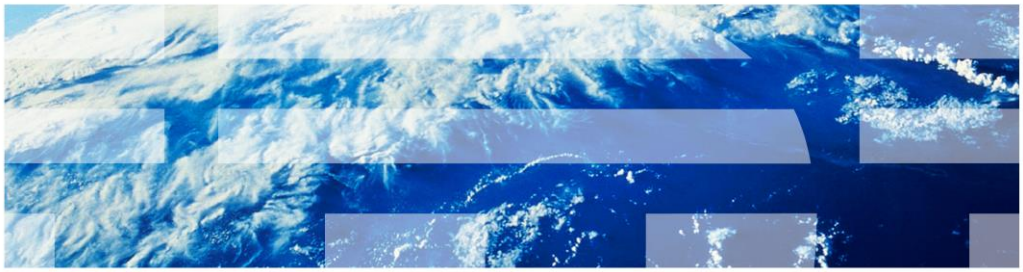
IBM Workload Deployer V3.1

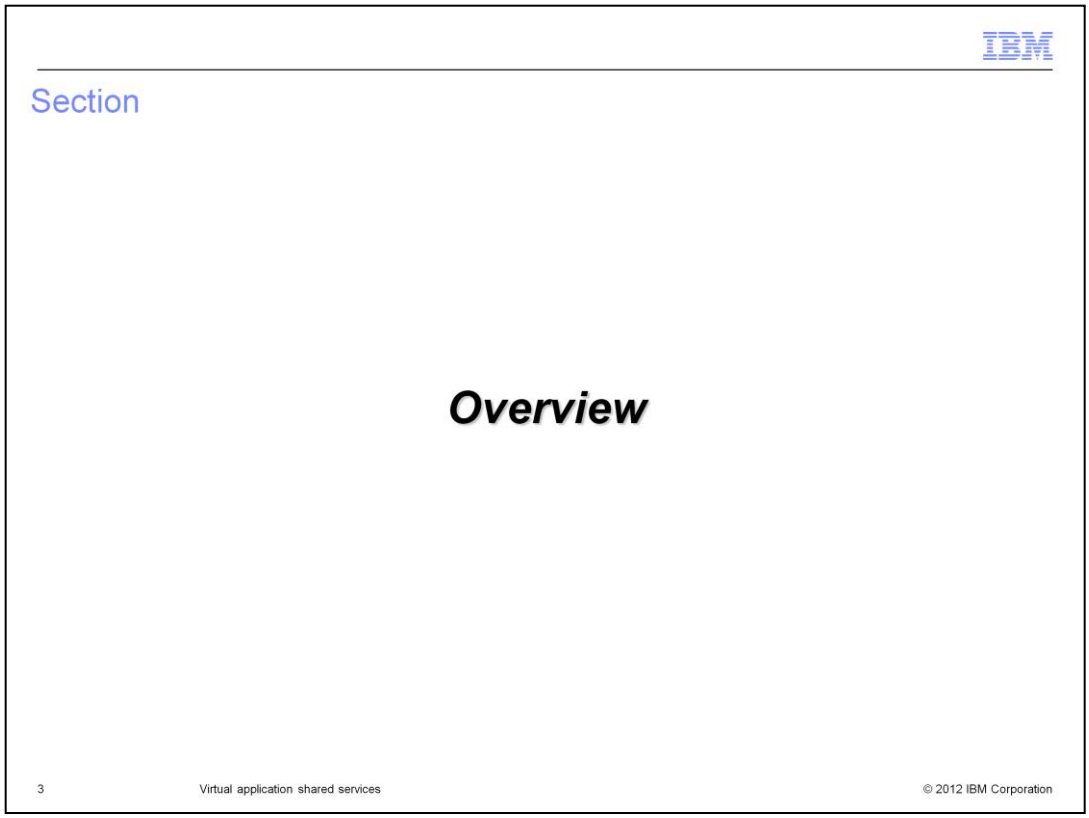
Virtual application shared services



This presentation covers virtual application shared services supplied with IBM Workload Deployer version 3.1.

Table of contents

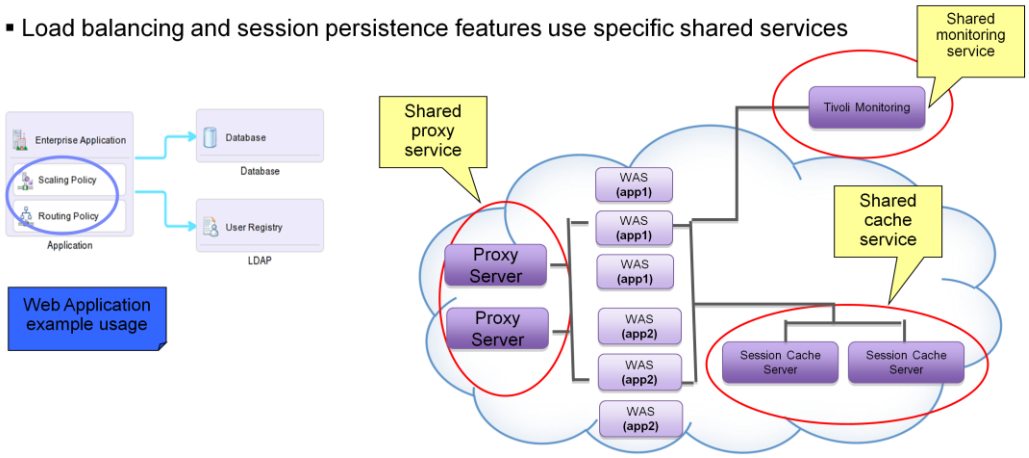
This presentation covers the shared cache and proxy services, then configuration for an external IBM Tivoli Monitoring server.



This section will give an overview of the IBM Workload Deployer shared services.

Overview

- Shared services reduce resource footprint
- Shared services shared by all deployed virtual applications
- Load balancing and session persistence features use specific shared services



4 Virtual application shared services

IBM Workload Deployer allows virtual applications to use a common, or shared, set of services to proxy HTTP requests, cache session data, and monitor components of the virtual application.

When deployed, these services are shared amongst all virtual applications within a cloud group. Each cloud group must have its own instance of a shared service for it to be available.

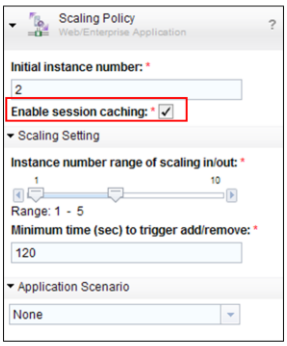
Virtual applications that enable a routing policy use the shared proxy service; those that “Enable session caching” in a scaling policy use the shared caching service. These shared services offer automatic failover, reduced resource footprint in the cloud and improved performance.

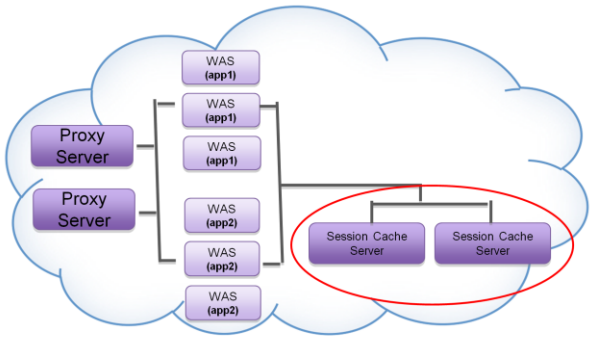
Shared caching service

This section covers the shared caching service.

Scaling policy (Web Application usage example)

- Session persistence backed by WebSphere® eXtreme Scale technology
  - Memory-to-memory





6 Virtual application shared services

By default, all HTTP session data in a virtual application is stored in memory in the individual application server instances. If an application server instance fails, the session data is lost. If your virtual application includes a scaling policy, you can enable session caching.

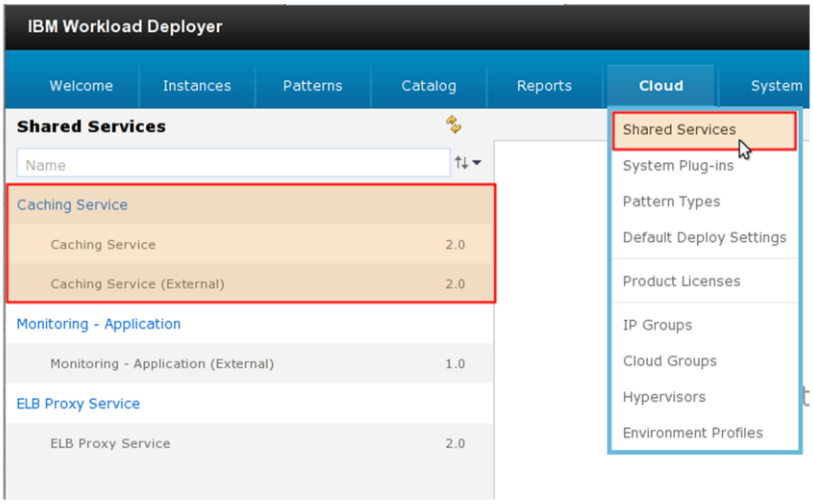
With session caching, session data is periodically replicated to a shared service that is backed by WebSphere eXtreme Scale technology. If an application server fails, requests can fail over to a peer application server which can retrieve the session data from the cache.

All virtual applications in a cloud group use the same shared cache service. The shared cache service is deployed as a set of virtual machines in the cloud bound as a single large cache. Session data sent to the shared cache is automatically replicated across the cache's virtual machines to ensure high availability of your data.

Using a shared caching service offers several benefits. It reduces the resource footprint by not requiring each virtual application to maintain its own memory and process overhead to share HTTP session data. Having the data available in a separate process allows sessions to seamlessly fail over to a new application server instance if necessary.

Shared cache

- Provides session persistence to all of your deployed virtual applications

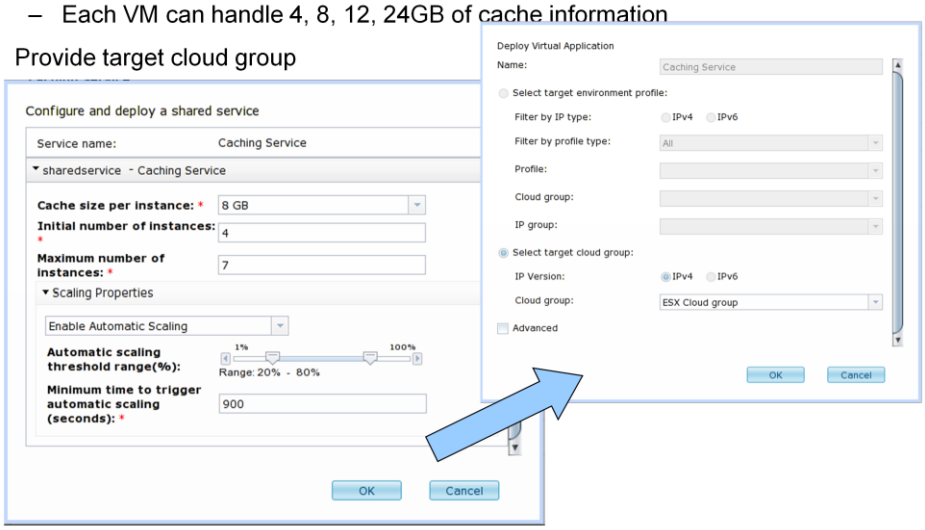


To enable the shared caching service navigate to Cloud > Shared Services and deploy the Caching Service. You must have administrator level permissions to deploy a shared service.

When you enable session persistence in a virtual application's scaling policy it will automatically configure your application to make use of the shared caching service. If a shared caching service is not deployed to the virtual application's target cloud group the virtual application will not deploy.

Shared cache deployment

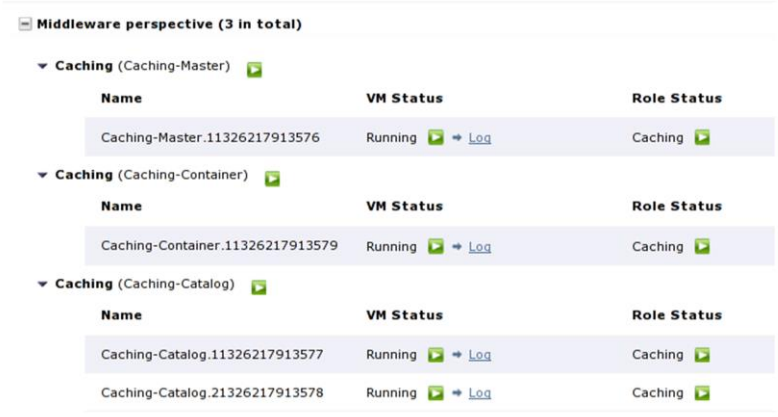
- Define the number of VMs
  - Share the responsibility of session persistence and provide failover
  - Each VM can handle 4, 8, 12, 24GB of cache information
- Provide target cloud group



Deploying the shared cache service requires that you specify the number of virtual machines and target cloud group to deploy into. The initial and maximum number of virtual machines determines how many VMs will share in the responsibility of session persistence and provide failover. Each VM can handle four to 24 gigabytes of cache information. The shared cache keeps two copies of each session stored in separate virtual machines for high availability, so some of the memory allocated per VM is used to store copies of data from other VMs.

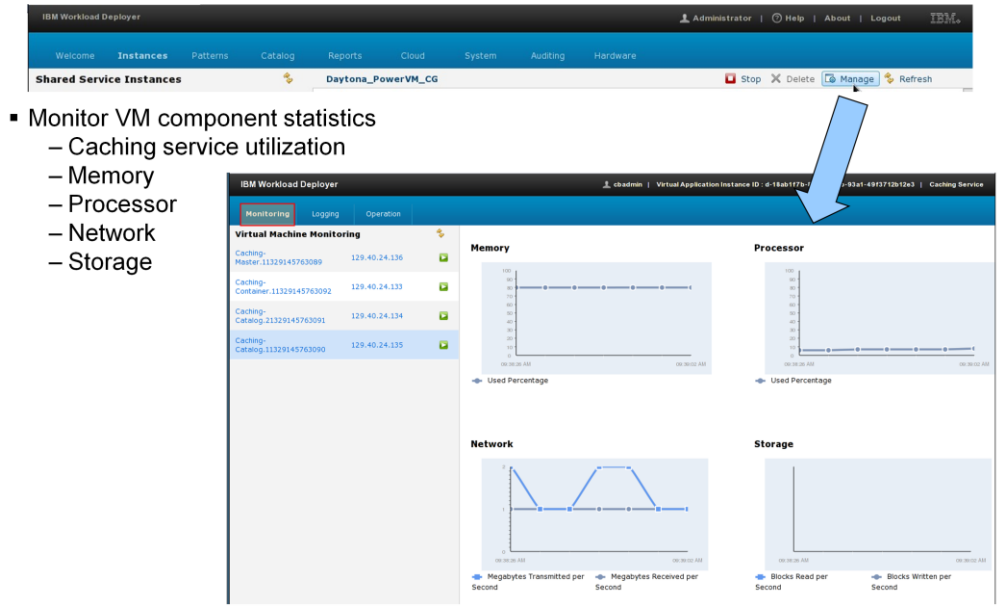
Shared cache instances

- Shared cache instances located under the Instances > Shared Services twisty



Shared cache virtual machine information is located under the Instances > Shared Services. Deploying a shared cache service will not create a separate instance under the Instances > Virtual Applications tab.

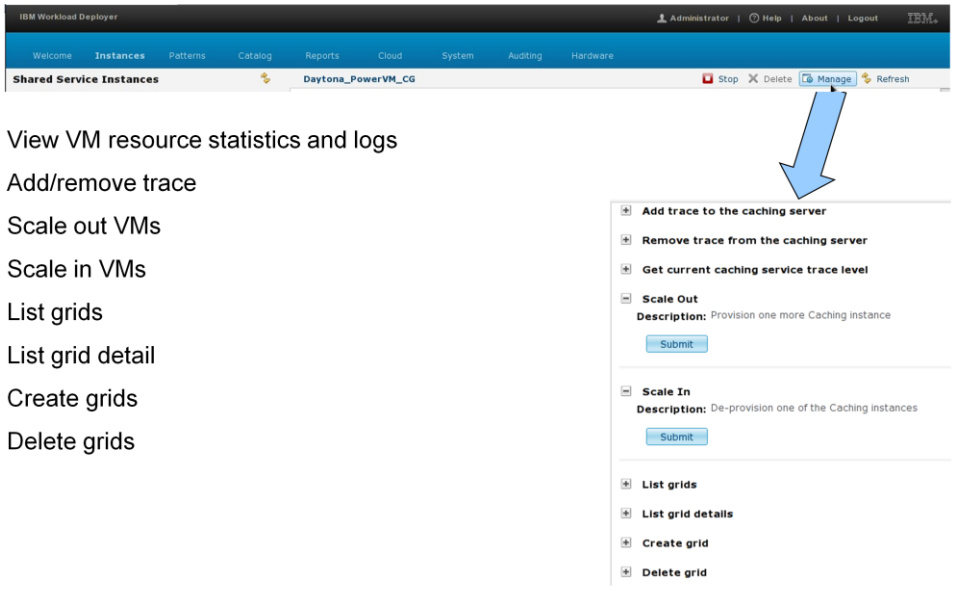
Shared cache log files



- Monitor VM component statistics
  - Caching service utilization
  - Memory
  - Processor
  - Network
  - Storage

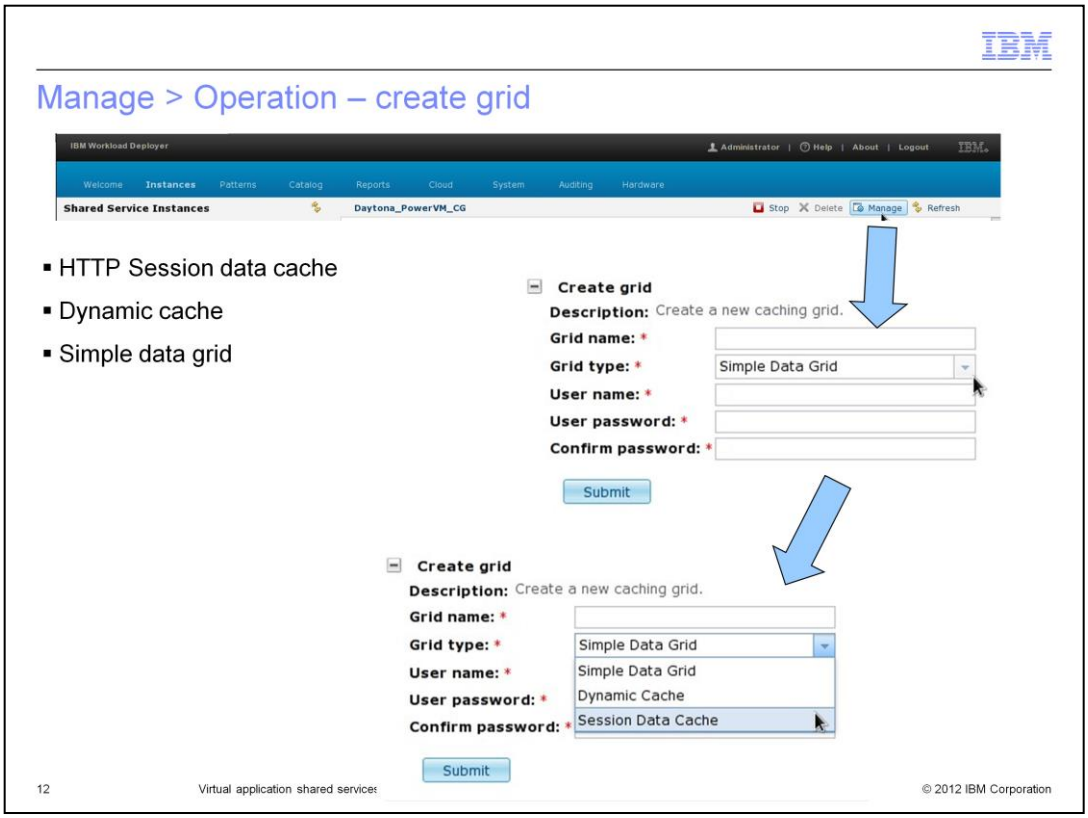
To monitor the VM details of your shared cache, click the Manage button located in the upper right corner of your Instances > Shared Services panel. The caching service management information will come up in a separate browser window displaying the default panel, Virtual Machine Monitoring. This view provides you with real-time statistics on processor, memory, disk and network. You can select Monitoring > Middleware to view caching service utilization.

Manage > Operation



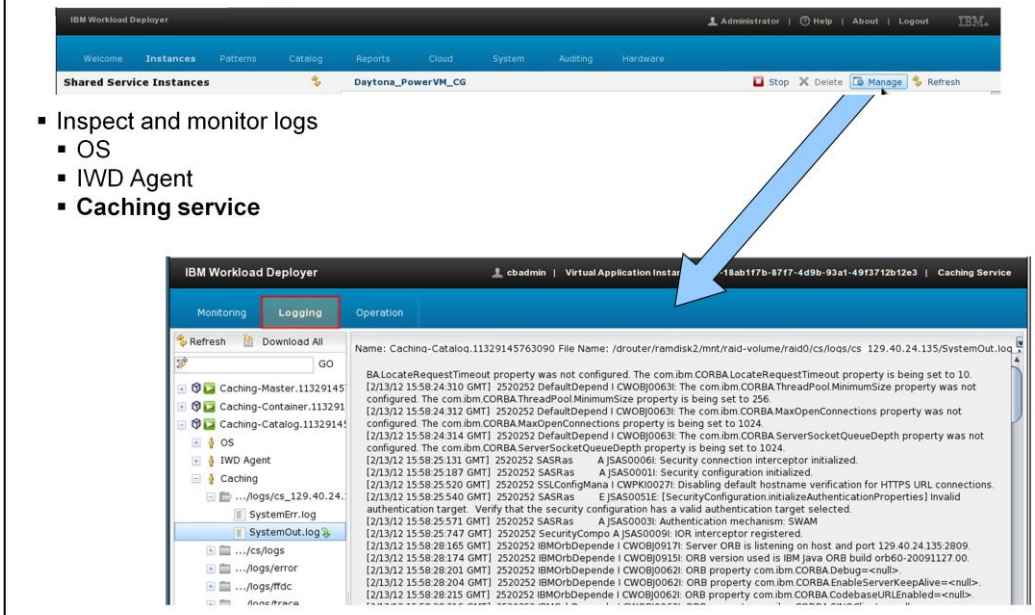
- View VM resource statistics and logs
- Add/remove trace
- Scale out VMs
- Scale in VMs
- List grids
- List grid detail
- Create grids
- Delete grids

The Manage > Operation panel allows you to perform post deployment operations on the caching service. From this panel you can change the trace level on the caching service, list the grids defined on the service, and get details for individual grids. You can also manually scale the number of active caching server VMs to accommodate changing workload demands.



When you deploy a virtual application that includes a scaling policy with session caching enabled, Workload Deployer will automatically create a grid to hold that application's session data. Each virtual application has a separate grid instance in the shared cache. An advanced feature on the Operation panel is the ability to manually create grids. You can then manually configure a *virtual system* to use this new grid. In addition to session data cache, you can also create dynamic data grids to hold WebSphere DynaCache data, or simple data cache to hold Java objects (accessed through the ObjectGrid API). These cache types are not directly supported by virtual applications.

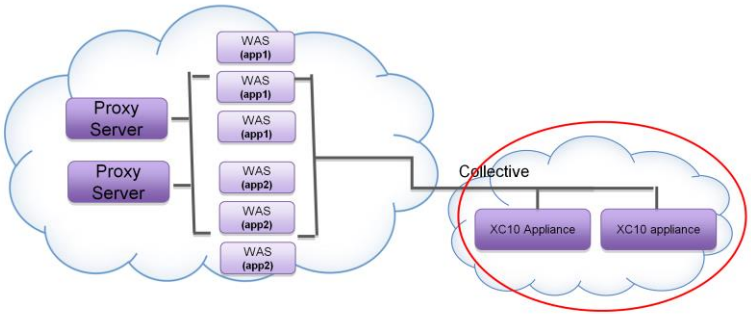
Shared cache log files



The Manage > Logging panel allows you to access logging information for each VM deployed as part of your shared caching service. You can also get the logs from the Log Viewer which is linked next to each virtual machine under Instances > Shared Services.

Caching appliance

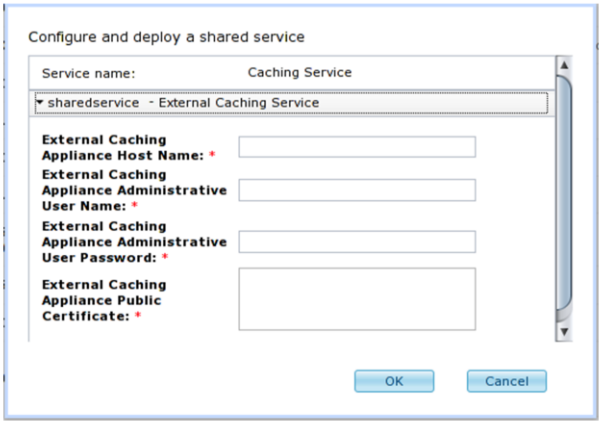
- Session persistence backed by WebSphere DataPower® XC10



In addition to the shared caching service, you can off-load session persistence to a shared service backed by an external WebSphere DataPower XC10 appliance. Since the DataPower XC10 is a separate appliance, you can configure multiple cloud groups to share the same DataPower XC10 collective. This allows you to use the large memory capacity and optimized hardware of the DataPower XC10 caching platform, reducing hypervisor resources used in your private cloud.

External caching service

- Provide connection information to XC10 collective

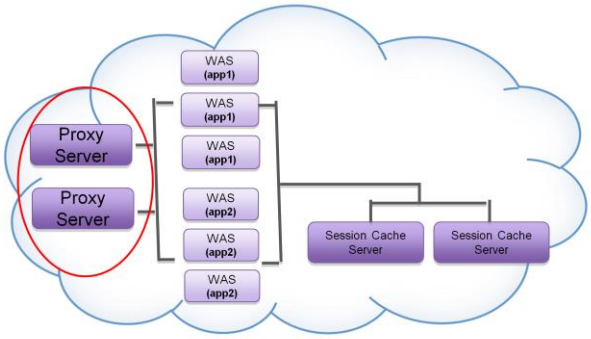


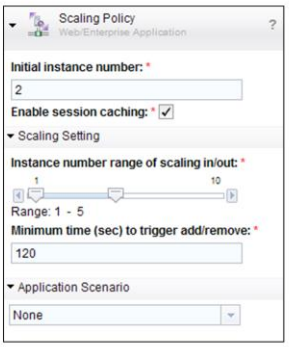
To configure an external caching service you must provide the host name or IP address of the DataPower XC10 appliance, a user ID and password with Administrative authority on that appliance, and the public certificate for the appliance. You can obtain the DataPower XC10's Public Certificate by using a browser to access the XC10 appliance and then export the appliance's public certificate as a base-64 encoded X.509 certificate.

This section covers the shared proxy service.

Scaling / Routing policies (Web Application usage example)

- Scaling and routing policies work together to provide an elastic load balanced solution





17 Virtual application shared services © 2012 IBM Corporation

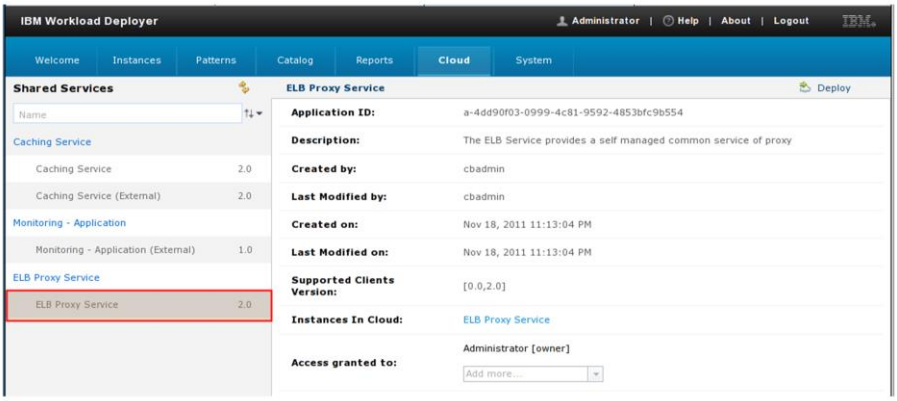
Including a routing policy in your virtual application automatically front ends your application with elastic load balancers (or ELBs). These ELBs are managed under a shared service called proxy service. The shared proxy service is shared by all virtual applications within a cloud group.

Using the shared proxy reduces the resource footprint in your cloud by not requiring each virtual application to have its own set of elastic load balancer VMs. You can enable multiple proxy servers for high availability.

The routing policy automatically configures the proxy server to route HTTP or HTTPS traffic to your application based on the virtual host name. The routing policy is normally used in conjunction with the scaling policy. If you enable a scaling policy you should also enable the routing policy so the shared proxy service can route requests to servers in the web application as they scale out or in.

Shared proxy

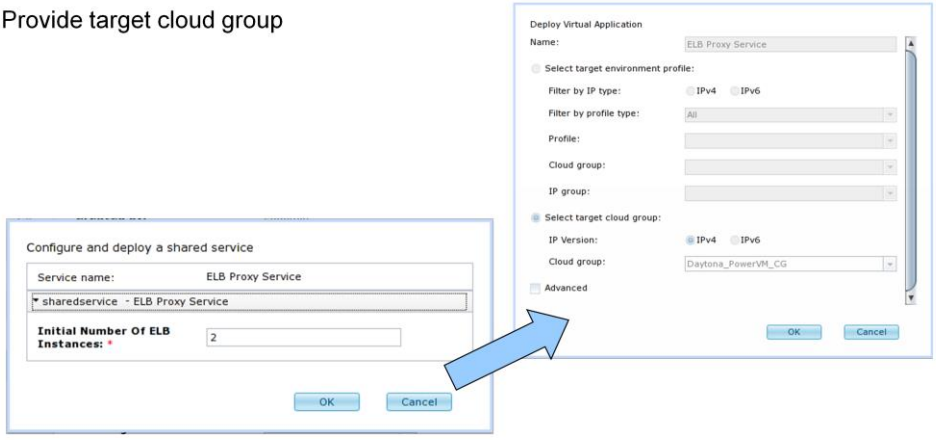
- Shared proxy is a shared service that provides elastic load balancing to all of your deployed virtual applications
  - Scaling policy should also be enabled



To enable the shared proxy service, navigate to Cloud > Shared Services and deploy the **ELB proxy service**. This service is used automatically by all virtual applications that include a scaling policy. If a virtual application includes a routing policy, an instance of the shared proxy service must be started within the same cloud group where you plan to deploy the virtual application. If a shared proxy service is not deployed to the target cloud group the virtual application will not deploy.

Shared proxy deployment

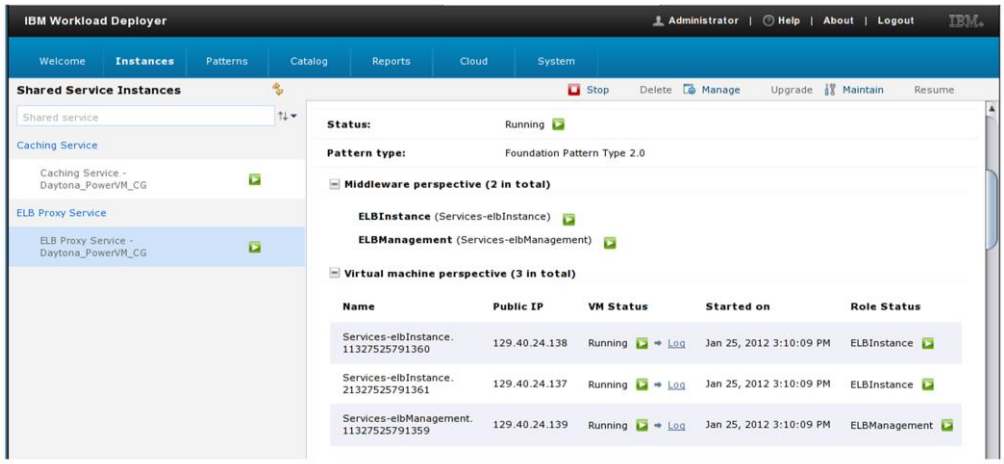
- Define the number of VMs
  - Share the responsibility of load balancing and provide failover
- Provide target cloud group



Deploying the shared proxy service requires that you specify the initial number of proxy instances and the target cloud group to deploy into. The initial number of instances determines how many virtual machines will share in the responsibility of load balancing and provide failover.

Shared proxy instances

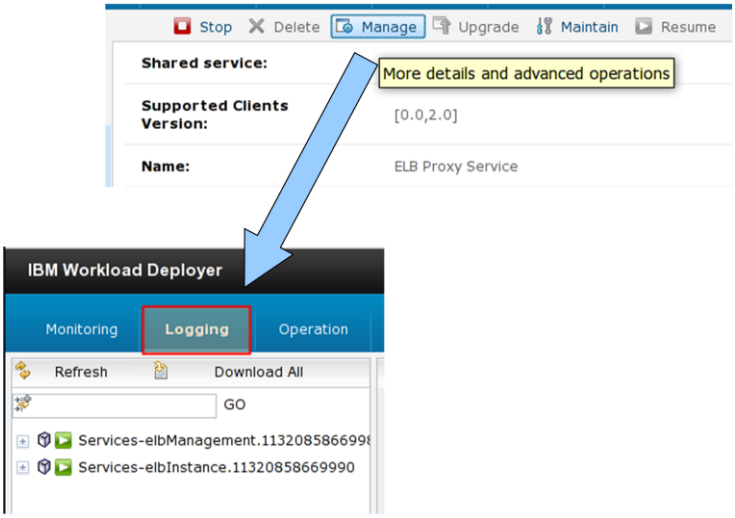
- Shared proxy instances located under the Virtual machines twisty



Shared proxy VM information is located under Instances > Shared Services. Deploying a shared proxy service will not create a separate instance under the Instances > Virtual Applications tab.

Shared proxy log files

- Inspect and monitor logs
  - OS
  - IWD Agent
  - **ELB Instance**



From Logging you can access logging information for each VM deployed as part of your virtual application. You can also get the logs from the Log Viewer which is linked next to each VM.

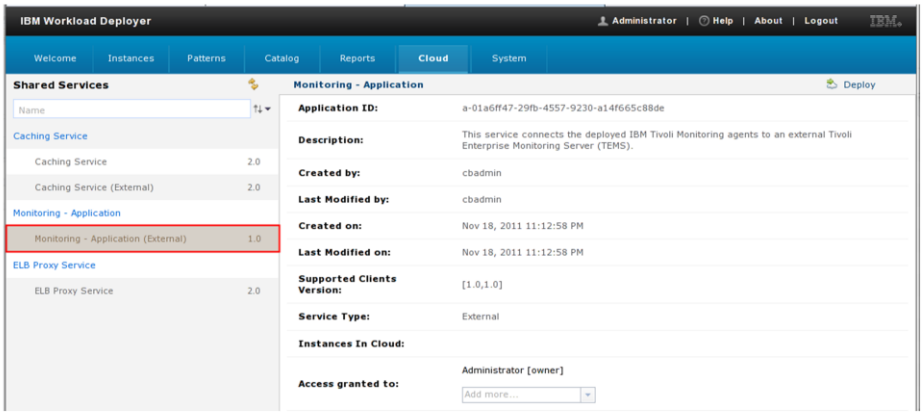
Section

IBM Tivoli Monitoring

This section covers the external monitoring service.

IBM Tivoli Monitoring

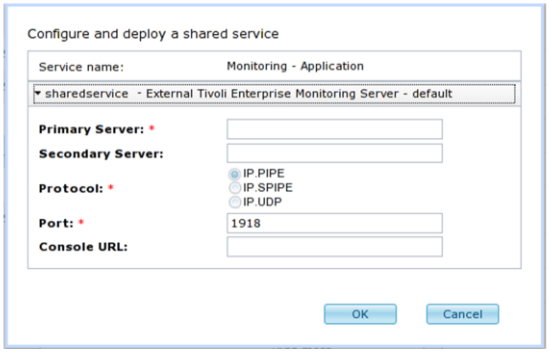
- External IBM Tivoli Monitoring server
- Monitoring Agent for IBM Workload Deployer



The Monitoring Agent for IBM Workload Deployer is automatically installed in all virtual machines in the virtual application when you deploy it to your cloud environment. This agent allows your virtual application to send status and performance statistics to an external IBM Tivoli Monitoring Server.

Deploying IBM Tivoli Monitoring

- Provide connection information to existing Tivoli Enterprise Monitoring Server
- At deployment, system plug-in will
  - configure TEMS settings in the VM
  - open firewall access to the TEMS



- Console URL
  - Webstart client: http://TEPS_hostname:15200/LICServletWeb/LICServlet.
  - Web client: http://TEPS_hostname:1920///cnp/kdh/lib/index.html,

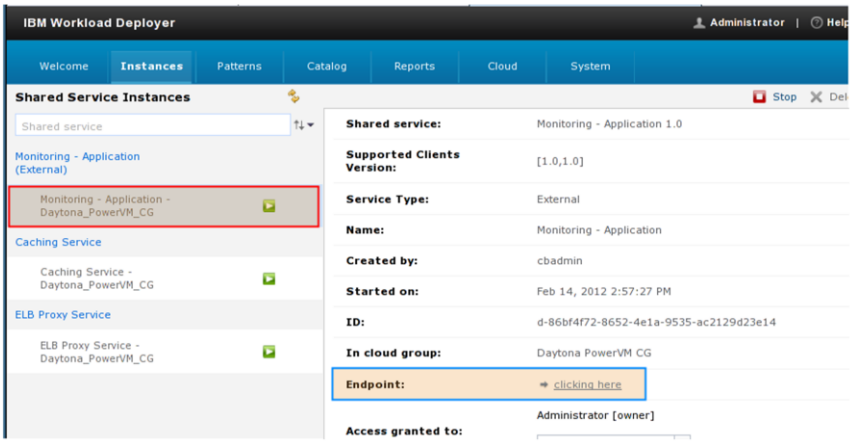
Deploying the monitoring service requires that you specify connection parameters for the external Tivoli Monitoring Server.

When created, the monitoring agents in deployed virtual applications are automatically connected to the defined instance of a Tivoli server using the supplied primary and failover Tivoli Enterprise Management server, protocol, and port.

You can optionally provide the URL for the Tivoli Enterprise Portal console to allow cloud administrators to easily launch the Tivoli Enterprise Console®

IBM Tivoli Monitoring status

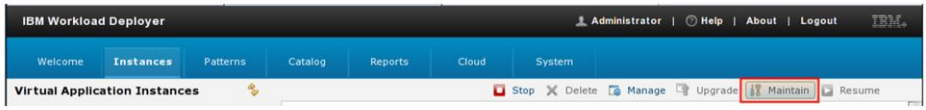
- Shared monitoring details located under the Instances > Shared Services twisty
- Does not create virtual machines



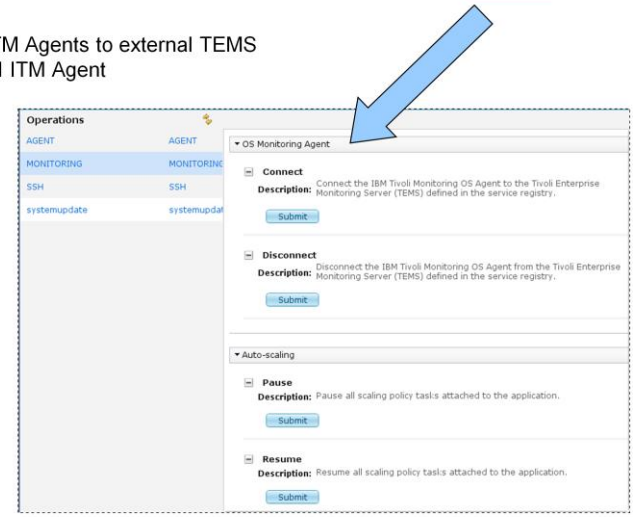
The shared monitoring service information is located under the Instances > Shared Services. Deploying a shared monitoring service does not create a virtual machine.

If you provided the URL for the Tivoli Enterprise Portal Webstart or web console at deployment, the service details will include the endpoint information that cloud administrators can use to launch the Tivoli Enterprise Console

Connecting to shared IBM Tivoli Monitoring



- Use Manage > Operation panel to
  - Manually connect deployed ITM Agents to external TEMS
  - Manually disconnect deployed ITM Agent

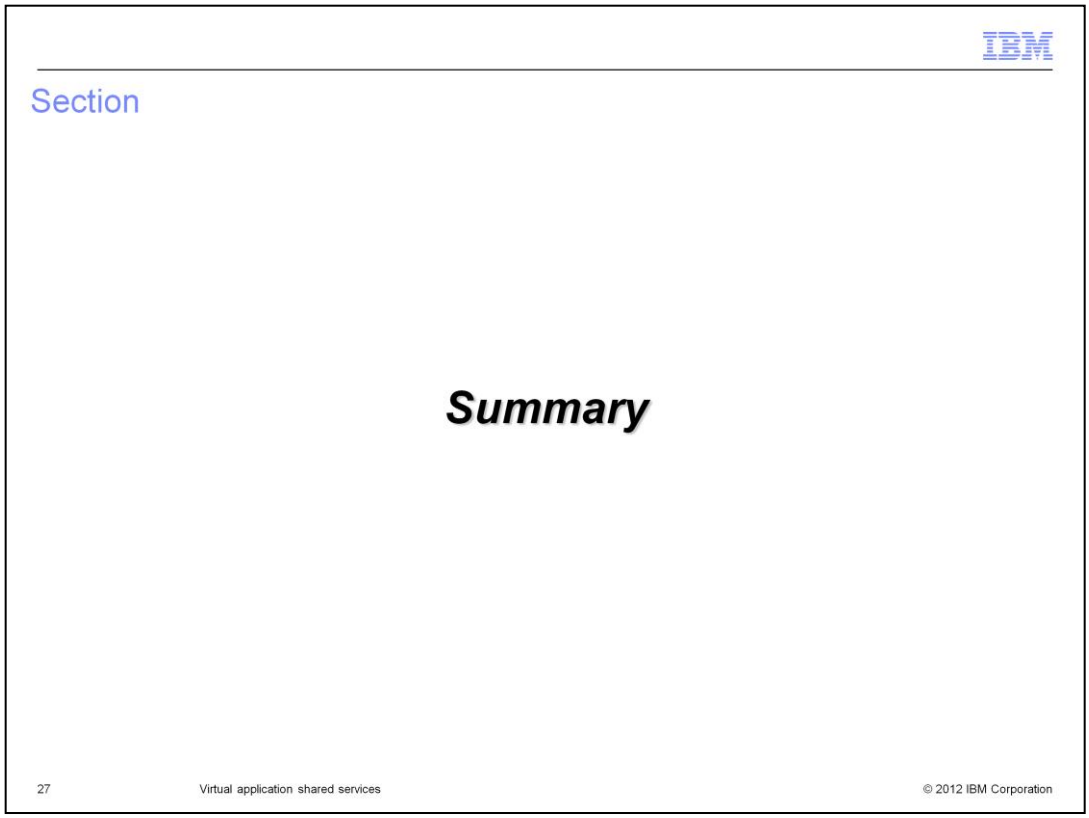


26 Virtual application shared services

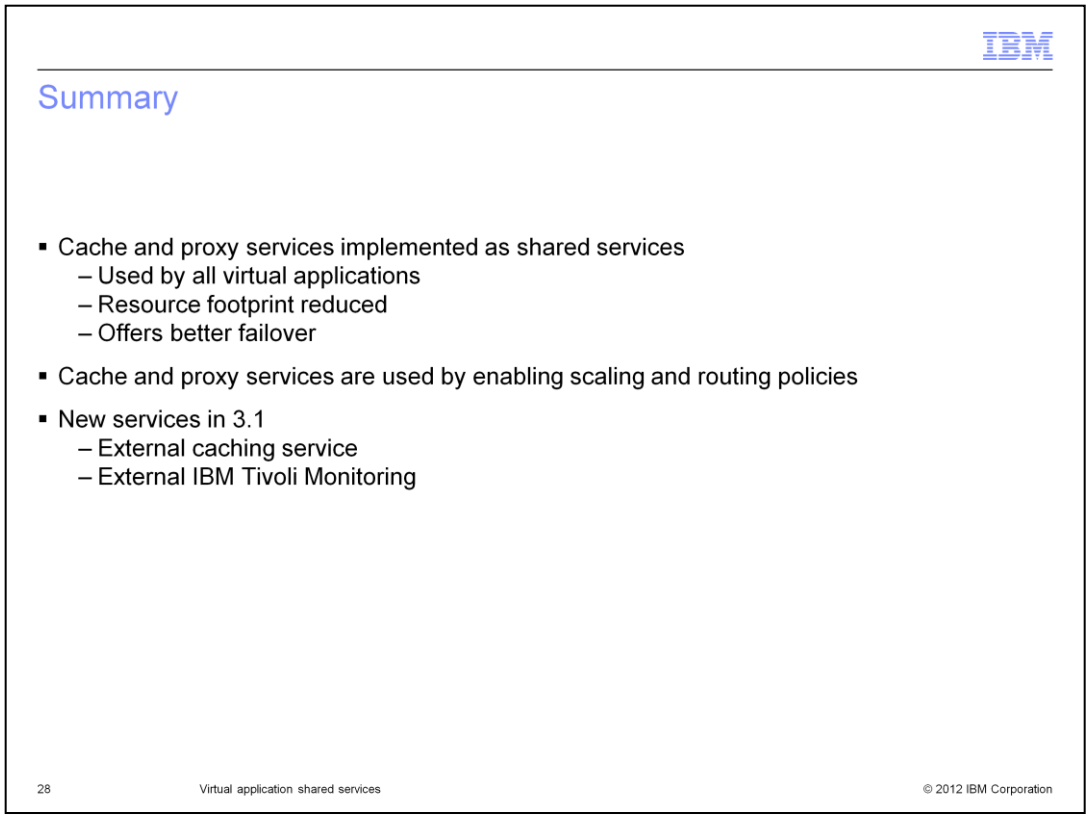
Virtual applications deployed after you deploy the monitoring service are automatically connected to the monitoring service. However you must explicitly connect any agents that already exist in the cloud to the monitoring service so they can connect to the Tivoli Enterprise Monitoring Server.

To connect a virtual system's Monitoring Agent for IBM Workload Deployer to the monitoring service, click **Instances > Virtual Applications** and select the deployment that you want to monitor. Click the Manage icon to open the virtual application's advanced operations in a new browser window. Click the Operation tab and select the Monitoring role from the Operation list.

Click connect on the OS Monitoring Agent panel to start sending data to the monitoring service, or disconnect to stop sending data to the monitoring service.



This section gives a brief summary.



The cache and proxy are implemented as a shared service used by all deployed virtual applications. This reduces resource footprint and offers better fail over. Both of these services are used in conjunction with the scaling and routing policies. IBM Workload Deployer V3.1 adds the ability to use a DataPower XC10 appliance as a shared caching service, and connection to an external IBM Tivoli Monitoring server.

Trademarks, disclaimer, and copyright information