Environment Isolation in IBM PureApplication System

IBM Redbooks Solution Guide

In IBM® PureApplication™ System, applications run in the cloud as workloads that share system resources, such as CPU, memory, and networking. There are some deployments, however, where workloads must be *isolated* from each other.

Isolation is a key consideration for cloud computing. An application deployed into a cloud environment must be able to run independently from other applications in the cloud. Each application must have sufficient resources to process its workloads, move traffic along the network, and protect its data. Isolation of applications and data, by either physical separation or virtualization within the cloud, can prevent resource contention, satisfy security requirements, and ensure that a failure of one application will not cause the failure of other applications.

An ideal solution to implement such application and virtual systems isolation is to exploit the features of the IBM PureApplication System. This guide explains how isolation can be implemented to separate complete runtime environments, as illustrated in Figure 1.

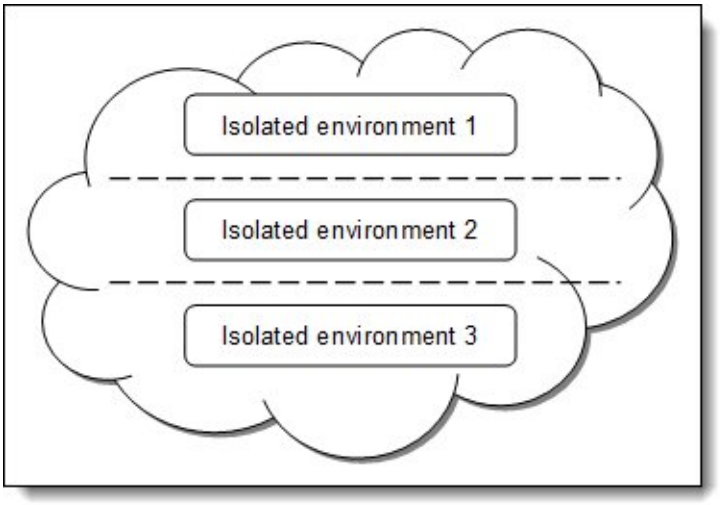

Figure 1. Isolated application environments in the cloud

Did you know?

IBM PureApplication System provides resource isolation and protection at multiple levels to address security and trust requirements. Built-in security controls provide computing node isolation, disk storage isolation, OS and virtual machine isolation, networking isolation, trust domain isolation, communication integrity and confidentiality protection, and fine-grained resource access control.

Business value

Using the isolation techniques that are incorporated in IBM PureApplication System can minimize business risks. Resource isolation offers increased security, performance, and application reliability.

For example, consider an enterprise that has an IBM PureApplication System in a cloud environment that is shared by different departments and their respective applications, such as marketing, human resources, and finance applications. To achieve the benefits of isolation, the enterprise might want to divide the computing resources into the following three sets or isolated resources:

- One set assigned to the marketing department
- One set assigned to the human resources department.
- One set assigned to the finance department.

When resource isolation techniques are implemented, if one virtual instance crashes, it does not affect applications for the other departments. The data can be isolated as well, such that it is not shared among the virtual instances. In addition, isolation accommodates varying levels of access control requirements.

Solution overview

An application development lifecycle normally requires separate runtime environments for development, testing, and production. These environments are usually isolated from one another so that activities in each environment do not interfere with the others. There might be further requirements within a company to isolate critical applications, or applications from different departments and lines of businesses. IBM PureApplication System supports the deployment of applications, known as pattern instances, into runtime environments. Such runtime environments consist of cloud groups and environment profiles. These cloud groups and environment profiles give IBM PureApplication System the means to create the separation that provides the necessary levels of isolation required for applications in different environments or lines of businesses.

To determine the proper way to set up cloud groups and environment profiles, you need to understand how these concepts apply in cloud computing, the key role they play in hardware resource virtualization, and how these features are implemented in IBM PureApplication System.

To address computing resource isolation requirements, IBM PureApplication System provides the capabilities to create cloud groups and environment profiles. The three cloud groups (development, testing, and production) provide physical isolation of the computing nodes of the three runtime environments. In addition, IP groups with distinct VLANs are used to provide virtual network isolation for each of the environments.

Solution architecture

Cloud computing provides shared computing resources in a controlled way to application workloads, thus allowing these workloads to successfully run in parallel. There are three types of computing resources: computational (CPU and memory), storage, and networking. Cloud computing enables workloads to share all three. The following key concepts describe how cloud computing handles workloads and provides resources to applications:

- Resource isolation

  Prevents problems within applications deployed into the cloud environment from affecting other applications in the cloud with issues of resource contention. This is done by creating virtual barriers between cloud resources, allowing them to operate independently; problems in one application deployed in the cloud do not affect other isolated systems. The primary types of isolation are:

  - Computational isolation

    Groups of CPU and memory capacity are separated from each other. This type of isolation can be physical or virtual. Physical computational isolation provides dedicated hardware resources, whereas virtual computational isolation, or virtualized resources, creates groups of separate resources that might actually share the same hardware.

  - Network isolation

    Communication flows between computational resources by separate connections. The isolation can be physical or logical. Physical network isolation provides the resources to allow data to travel in parallel sets of network equipment, such as separate switches. Logical network isolation shares the same network equipment and bandwidth, but the data is routed separately by a different virtual local area network (VLAN).

- Resource sharing

  Common pools of resources, such as IP addresses, CPU, and memory are made available to systems deployed in the cloud. Each workload can acquire a different amount of resources, based on its requirements. Resource sharing is dynamic, meaning workloads acquire shared resources dynamically as needed. This configuration requires care and attention in planning and implementation because sharing resources can trigger workloads to consume excessive resources from any given pool, therefore starving the other workloads in the cloud environment.

- Resource allocation

  Resource allocation, or logical isolation, enables resource sharing, but requires setting boundaries on a workload by putting lower and upper limits on resource sharing. Allocation balances isolation and sharing, ensuring that a workload gets at least the minimum resources it needs to run properly. Moreover, it prevents workloads from consuming excessive amounts of a pooled resource. You can set allocation limits on any shared resource: CPU, memory, storage, bandwidth, and even software licenses.

The features and capabilities of IBM PureApplication System that enable it to provide resource sharing and isolation of workloads are:

- Compute nodes

  Compute nodes contain hardware components such as microprocessors, memory, network adapters, and storage adapters.

- IP groups

  IP Groups are logical groupings of one or more IP Addresses and networking information, such as DNS, subnet, VLAN, and so on. IP Groups, and by association IP addresses, are assigned to cloud groups. At least one IP group is needed to aggregate compute nodes into a cloud group. A cloud group can contain more than one IP Group. A virtual machine (VM), deployed into the IBM PureApplication System infrastructure, will be assigned its IP address. The addresses are assigned from the available pool of addresses defined in the IP group that has been associated with the cloud group used by the VM.

- Cloud groups

  A cloud group is a logical grouping of computing resources (Compute Nodes) to target your deployments in IBM PureApplication System. A cloud group requires one or more compute nodes and one or more IP groups. A pattern is deployed to a cloud group (using an environment profile). The pattern instance is composed of VMs. To deploy virtual machines into the IBM PureApplication System environment, you must associate these to cloud groups. Virtual machines are deployed on the compute nodes that are part of the chosen cloud group.

- Environment profile

  Environment profiles are policies for deploying patterns into cloud groups. They group together related deployment configurations, such as virtual machine names, IP address assignment, and cloud groups. Environment profiles also associate users and user groups with cloud groups. These profiles specify the cloud groups that each user or user groups can deploy patterns to. Finally, Environment profiles create the logical isolation of resources by allocating these resources.

- User group

  A user group is list of users in the same role. Through the use of environment profiles, IBM PureApplication System associates one or more user groups with cloud groups. This relationship enables users in the chosen user groups to deploy patterns into specific cloud groups.

Figure 2 shows the relationship between the various cloud resources within an IBM PureApplication System.

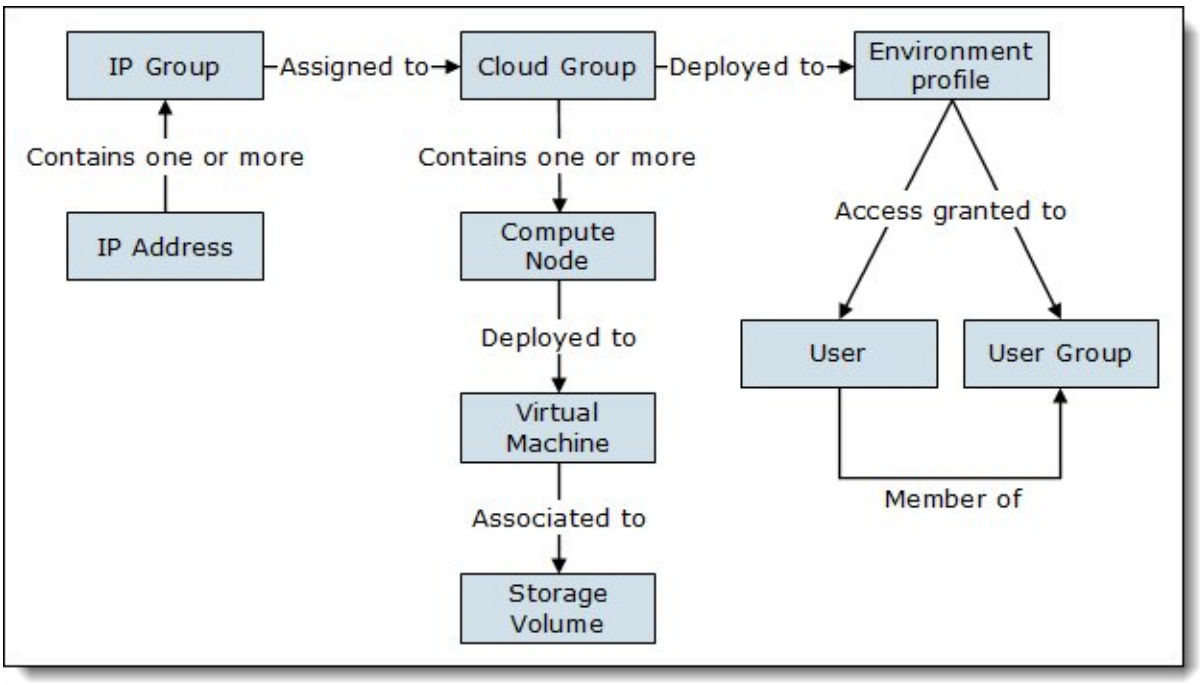

Figure 2. Cloud resources in an IBM PureApplication System

Usage scenario: Setting up several application environments

Companies normally separate environments according to application development lifecycle. The typical divisions are:

- **Development (DEV)**: An environment used for developing applications.
- **Testing (TEST)**: Used for testing applications.
- **Production (PROD)**: Used for running applications; this is the realm of business or end users.

Each of these environments typically runs on independent sets of hardware and networks to avoid cross-environment issues.

In this scenario, three cloud groups are created, one for each stage of the application development lifecycle. The following are configuration examples:

- A DEV cloud group with one compute node, giving developers 16 physical cores. Setting the cloud group type to *average* will give a 4 to 1 ratio of virtual CPUs, therefore giving developers 64 virtual CPUs.
- A TEST cloud group with two compute nodes and cloud group type *dedicated*, to mimic production.
- A PROD cloud group, with three compute nodes, and the cloud group type set to *dedicated*, because production applications are expected to be used heavily.

Each of these three cloud groups also needs at least one IP group with an otherwise unused VLAN ID to keep their network traffic separated.

Figure 3 shows the isolation of the three application environments that is proposed in this scenario.

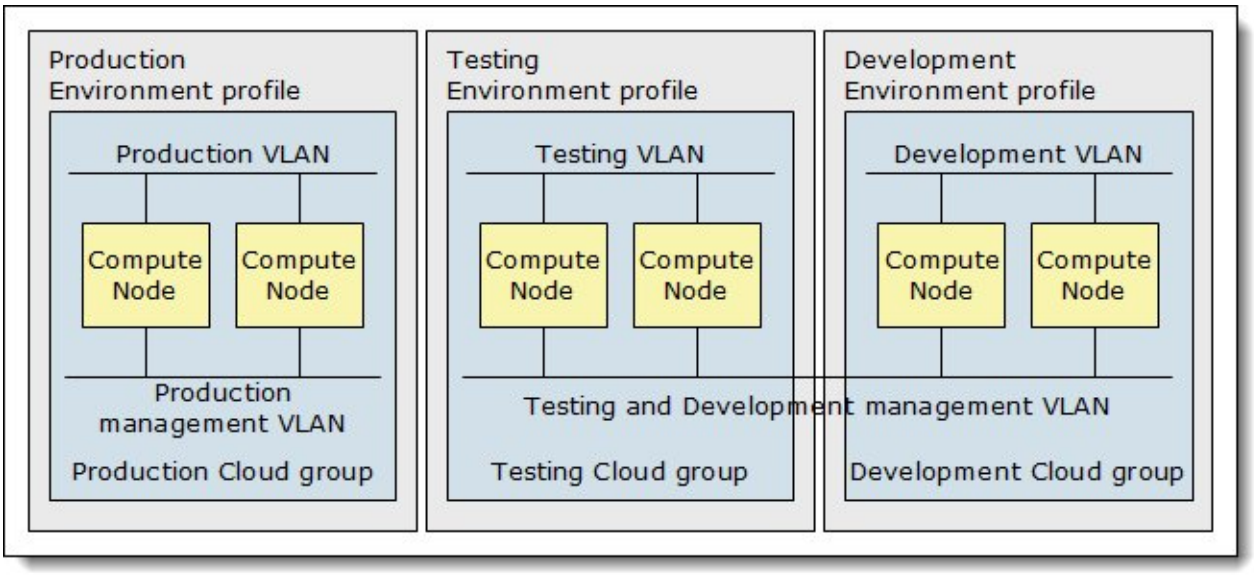

Figure 3. The proposed scenario with three isolated application environments

Three separate runtime environments are created for this scenario, with each one running its workloads in isolation. Because a runtime environment in PureApplication System is a cloud group, creating three separate runtime environments means that three cloud groups are needed. A cloud group consists of one or more compute nodes and at least one IP group. Compute nodes are hardware resources that are part of PureApplication System; we do not need to create them because they already exist within the system. IP groups, on the other hand, just represent configuration data, so we must create them. We also will create two environment profiles for deploying patterns. Before you start, ensure that the following hardware and network resources are available:

- **User**: There must be one with full permissions on the PureApplication System.
- **Compute nodes**: For this example, two compute nodes must be assigned for each environment. They need to be otherwise unassigned, that is, not part of another cloud group, so that you can assign them to your cloud groups.
- **Networks**: You will need three application VLANs, one for each set of isolated applications. VLANs can be defined on a single network, which creates logical isolation; or on separate enterprise networks, so that the network isolation will be not just logical but also physical. We assume that these networks are connected by their respective gateways. Greater network isolation can easily be achieved by reconfiguring the gateways or adding a firewall.

From the PureApplication System console, define each of the environments in the PureApplication System:

1. Create an IP group.

   Define one or more IP groups, with IP addresses and VLAN IDs that are assigned and provided by the network administrator.

2. Create a cloud group.

   Define a cloud group by assigning one or more compute nodes, the IP group created in the previous step, and a *management VLAN* ID. The management VLAN is used internally by the system, so it does not require IP addresses to be provided by an administrator; however, the administrator does

need to reserve each VLAN ID in the network. Unlike application VLANs, management VLANs do not need to be unique for each of these environments, as shown in Figure 3.

3. Create an environment profile.

   As noted in the Solution architecture section, the environment profile defines policies for how patterns are deployed to one or more cloud groups and how their instances run in the cloud group. The cloud group created in the previous step is added to the profile and the profile is then configured to use the IP group associated with the cloud group.

Figure 4 shows the configured environments.

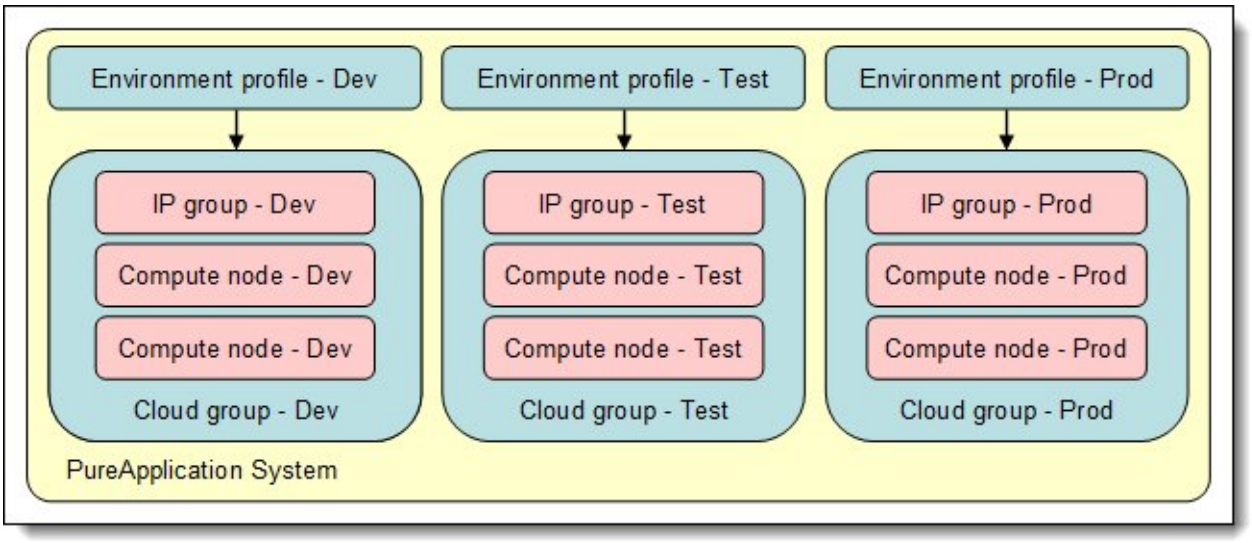

Figure 4. Environments configured in IBM PureApplication System

On completion of these steps, the system is ready for virtual pattern configuration and deployment of workloads.

Integration

IBM PureApplication System is an integrated hardware and software solution that provides an application-centric computing model in a cloud environment.

An application-centric system is an efficient way to manage complex applications and the tasks and processes that are invoked by the application. The entire system implements a diverse virtual computing environment, in which different resource configurations are automatically tailored to different application workloads. The application management capabilities of the PureApplication System platform make deployment of middleware and other application components quick, easy, and repeatable.

PureApplication System provides virtualized workloads and scalable infrastructure that is delivered in one integrated system:

- Virtualized system and application workloads, including:
  - Integrated middleware like IBM WebSphere® Application Server, web server, DB2®, and hypervisor images.
  - Elastic data.

- Application-centric workloads created using pattern types such as web application patterns, database application patterns, and topology patterns.

- Scalable infrastructure, including:
  - Optimized hardware tuned for running workloads.
  - Isolated networking for secure communications.
  - Server resiliency to prevent overload or failures.
  - Dynamic storage.

- Integrated delivery, including:
  - Factory assembled and wired system.
  - Tuned for maximum efficiency of data, storage, workload execution, and retrievability.
  - Simple approach to managing all integrated components and monitoring health of the system.
  - Single pane of glass management for administrator and application deployment.

For more information regarding product integration and the PureApplication System platform, follow the links in the "Related information" section.

Ordering information

Ordering information is shown in the following table.

Table 1. Ordering part numbers and feature codes

Program name	PID number	Charge unit description
IBM PureApplication System W1700	5725-846	Per appliance install

Related information

For more information, see the following documents:

- *Adopting IBM PureApplication System V1.0*, SG24-8113
  http://www.redbooks.ibm.com/abstracts/sg248113.html
- IBM PureApplication System product page
  http://www.ibm.com/ibm/puresystems/us/en/pf_pureapplication.html
- IBM Offering Information page (to search on announcement letters, sales manuals, or both):
  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  On this page, enter `PureApplication System`, select the information type, and then click **Search**. On the next page, narrow your search results by geography and language.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document was created or updated on May 2, 2013.

Send us your comments in one of the following ways:

- Use the online **Contact us** review form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

This document is available online at http://www.ibm.com/redbooks/abstracts/tips0959.html .

Trademarks