Cloud Computing Infrastructure on IBM Power Systems

Getting started with ISDM

- Detailed cloud resource configuration instructions
- Detailed installation steps of ISDM
- Point and click deployment of AIX

Thierry Huché
Behzad Koohi
Thanh V. Lam
Paul Reynolds
Sean M. Swehla
Jez Wain

Redbooks

ibm.com/redbooks

International Technical Support Organization

Cloud Computing Infrastructure on IBM Power Systems: Getting Started with ISDM

May 2012

SG24-7983-00

Note: Before using this information and the product it supports, read the information in “Notices” on page xv.

First Edition (May 2012)

This edition applies to Version 7.2.2, of IBM Service Delivery Manager (CRFK7ML).

Contents

Figures

Tables

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

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.

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.

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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
Blue Gene®
CloudBurst®
DB2®
IBM®
Maximo®
Passport Advantage®
Power Systems™
POWER6®
POWER7®
PowerHA®
PowerVM®
POWER®
pSeries®
Redbooks®
Redbooks (logo) ®
Service Request Manager®
Systems Director VMControl™
Tivoli®
WebSphere®

The following terms are trademarks of other companies:

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Preface

Managing IT systems is hard. Virtualization brings numerous benefits to the datacenter and system administrators. However, it also creates a new set of choices. More choice implies more decisions and thus an increased management responsibility. Furthermore, the move towards cloud computing, with a service-based acquisition and delivery model, requires datacenter managers to take a holistic view of the resources that they manage and the actors who access the datacenter. IBM® Service Delivery Manager addresses this problem domain. Delivered as a set of appliances, it automates provisioning, deprovisioning, metering, and management of an IT platform and the services that it provides. It addresses the needs of both IT management and service users.

This IBM Redbooks® publication takes a hands-on approach to deploying IBM Service Delivery Manager Version 7.2.2 on an IBM Power platform. IBM Service Delivery Manager is a rich product with a great number of capabilities. The book covers these topics:

- Installation and configuration of the IBM Service Delivery Manager appliances
- Configuration of IBM Systems Director and VMControl for IBM Service Delivery Manager
- The administrative interface and Self Service Portal of Tivoli® Service Automation Manager
- An introduction to IBM Tivoli Monitoring
- An introduction to Tivoli Usage and Accounting Manager
- Managing IT resources, including server pools and image library
- Creating basic customers and projects
- Managing workload life-cycle
- Monitoring and metering of basic workloads

As an introductory book, we have deliberately kept the environment simple to facilitate understanding.

Managing IT systems is hard. IBM Service Delivery Manager makes it easier. The goal of this publication is to help you have a trouble-free deployment of IBM Service Delivery Manager.

The team who wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Thierry Huché is an IT Specialist at the Products and Solutions Support Center, Montpellier, France, working as an IBM Power Systems™ Benchmark Manager. He has been with IBM France for 22 years. He has more than 20 years of AIX® System Administration and Power Systems experience working in the pSeries® Benchmark Center and AIX support center in Paris. He is an IBM Certified pSeries AIX System Administrator. Thierry's areas of expertise include benchmarking, virtualization, performance tuning, networking, and high availability.

Behzad Koohi works in the ITS Server and Storage Pre-sales Technical Team in Toronto, Canada. He is an IT Architect and regularly assists customers with the design of IT solutions using IBM Power products. He has over 17 years of experience in AIX and Power Systems, including three years as an IBM client. He ha a bachelor of computer science degree from York University, Toronto. His areas of experience are System Management, PowerHA®, and IBM Power hardware.

Thanh V. Lam joined the IBM High Performance Supercomputer System Lab in 1988. He has been working in the areas of High Performance Computing applications enablement and Cluster System Test. He has a broad range of skills in parallel applications and job scheduling and system resource management on large-scale systems, including AIX, Linux, and Blue Gene®. Thanh is now an IT Management Consultant in IBM Systems Lab Services and Technical Training.

Paul Reynolds is a Technical Solution Architect for IBM Australia. Paul has worked in AIX system administration and on virtualization-based solutions for the past eight years. In 2006 he began supporting customers using PowerVM® and PowerHA solutions, and his areas of expertise are PowerVM and x86 virtualization. Paul previously worked in an Emerging Technologies team, where he focused on the cloud computing infrastructure. Paul is currently working as a Technical Solution Architect, where he is helping design solutions that enable clients to leverage IBM cloud computing solutions.

Sean M. Swehla is an Architect at the IBM Design Center in Poughkeepsie, NY. He began his IBM career in 2005 at the IBM Design Center. He left the Design Center for a time to contribute to Build Automation in High Performance Computing (HPC). Following that assignment, Sean participated in projects within the Linux Technology Center. He returned to the IBM Design Center in 2011, where he has been involved in various aspects of Cloud-related projects.

Jez Wain works for Group Bull in Grenoble in the French Alps. As part of the Bull-IBM cooperation, he worked on the AIX kernel, middleware, and PowerVM, including two previous Redbooks publications. He has recently been involved in research projects looking at reducing energy consumption in the datacenter. Before joining Bull, he worked on realtime airborne software and data acquisition systems.

The project that produced this publication was managed by:
Scott Vetter, PMP

Thanks to the following people for their contributions to this project:

David Bennin, **Richard Conway**
International Technical Support Organization, Poughkeepsie Center

Franklin R Almonte, Chema Rodriguez Barroso, Ezequiel Cervantes, Budi Darmawan,Tyrone Dechalus,Victor Estival,David Feisthammel, Guilherme Galoppini Felix, Amy C Freeman, Manish Garedia, Vasfi Gucer, Gary Hamilton, Thierry Huche, Rafal Kudlacik, Gary Louw, Mehboob Mithaiwala, Veronica Murillo, Heath Newburn, Soumyadeep Paul, Marcos Quezada, Marco Sebastiani, Michal Tabaj, Stephen Tremain, Pawel Wnek

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

`ibm.com/redbooks/residencies.html`

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@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

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Introduction

IBM Service Delivery Manager builds on the services provided by IBM Systems Director and VMControl to provide an off-the-shelf private cloud platform for infrastructure, platform, and software as service deployments. IBM Service Delivery Manager offers the following functions:

- Service automation
  - Orchestration of cloud operations: user portal, provisioning, virtual machine lifecycle management, multi-tenancy, and automation
  - Service catalog and templates
  - Trouble ticketing
- Monitoring and reporting
  - Physical and virtual resources
  - Servers, disks, and networks
  - Reporting and cost management
- Accounting and charge back
  - Metering and accounting for cloud services
  - Integration with billing systems
- Management
  - Energy and power
  - Physical and virtual servers, storage, and networks

1.1 Target audience

This publication describes the installation, configuration, and operation of IBM Service Delivery Manager. It does not cover any of the underlying technologies. We assume that you are familiar with IBM Systems Director and VMControl, Storage Control, NIM, and the HMC. Furthermore, we assume that IBM Systems Director and VMControl are already installed and configured with the NIM repository, a server system pool, and optionally a storage system pool.

1.2 IBM Service Delivery Manager and cloud computing

IBM Service Delivery Manager capabilities allow you to build a computing platform aligned with the cloud model. Figure 1-1 shows the major functional components of a cloud platform.

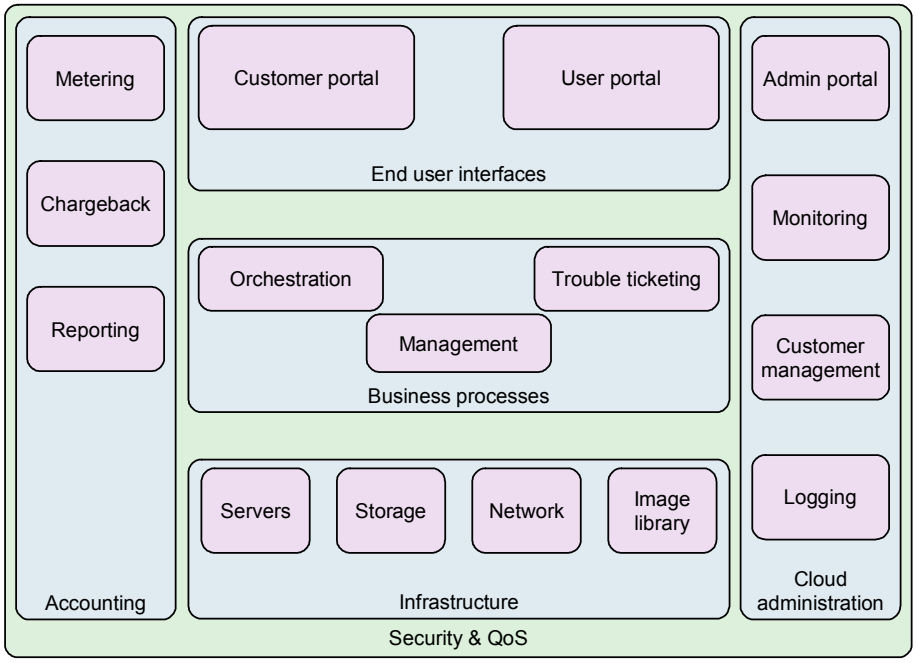

Figure 1-1 Cloud computing components

IBM Service Delivery Manager, coupled with IBM Systems Director and VMControl, provides an implementation for each of these. Figure 1-2 shows the process and resources involved in the creation and publication of a cloud service. After the need for a new service has been identified, the service designers and developers build it and publish it in the service catalog. Services might have tailorable options and customers might adapt the service to their specific environment. They then make it available to their projects and teams to be deployed, on demand, to the cloud infrastructure.

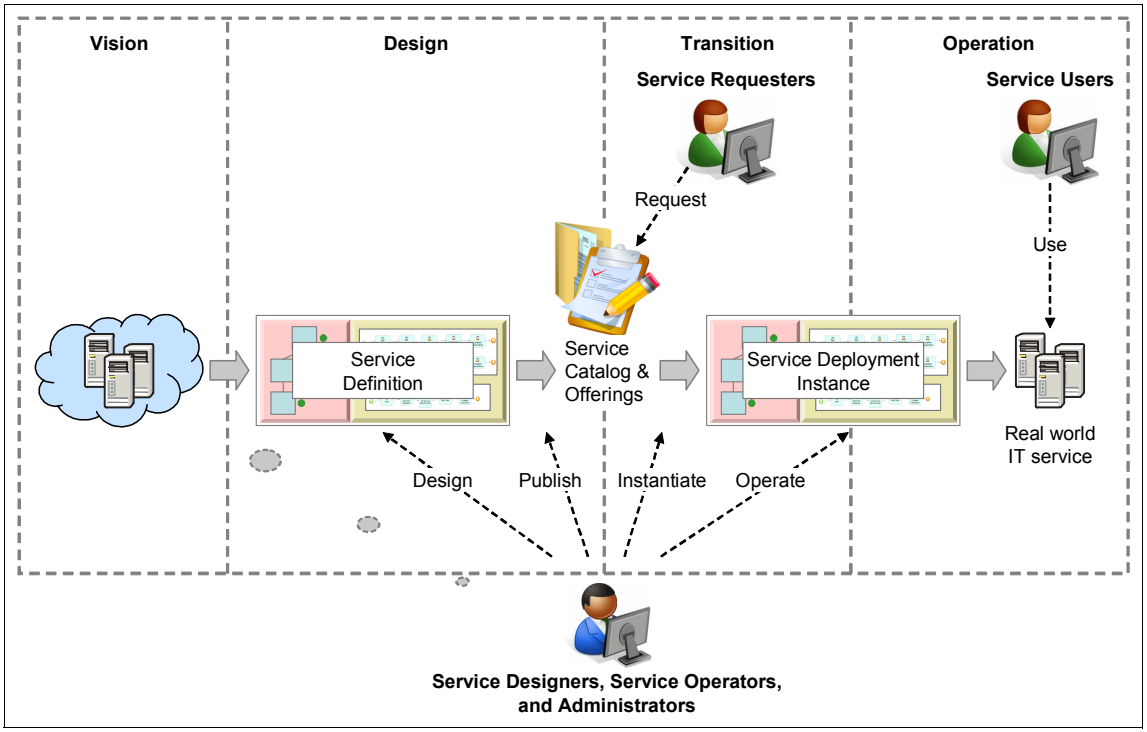

Figure 1-2 IBM Service Delivery Manager service workflow

1.3 IBM Service Delivery Manager components

IBM Service Delivery Manager is a software-only solution equivalent to the software stack that is preinstalled on IBM CloudBurst®. It is delivered as four software images that are deployed by IBM Systems Director on to the management server hardware. Each virtual image is dedicated to a specific service within the product:

TSAM appliance Self Service Portal, service catalog, and service automation.

ITM appliance Monitoring of the provisioned environment.

TUAM appliance Metering and accounting for cloud services. Billing integration.

HTTP appliance Central web server access point (URL redirection), file repository (NFS), and mail server.

IBM Service Delivery Manager has two mechanisms for working with the underlying PowerVM virtualization platform:

- Through the management console, either the Hardware Management Console (HMC) or the Integrated Virtualization Manager (IVM)
- Through IBM Systems Director and VMControl (IBM Systems Director manages the communication with the HMC.)

Because the later option offers the greatest flexibility, all the examples in this publication use IBM Service Delivery Manager running on top of IBM Systems Director and VMControl.

Figure 1-3 shows the server components of the management platform. In this diagram the IBM Service Delivery Manager appliances are shown in the center, underpinned by IBM Systems Director and VMControl. NIM is used by VMControl as the image repository. All operations performed on the hardware and LPARs are performed by the HMC on VMControl's behalf.

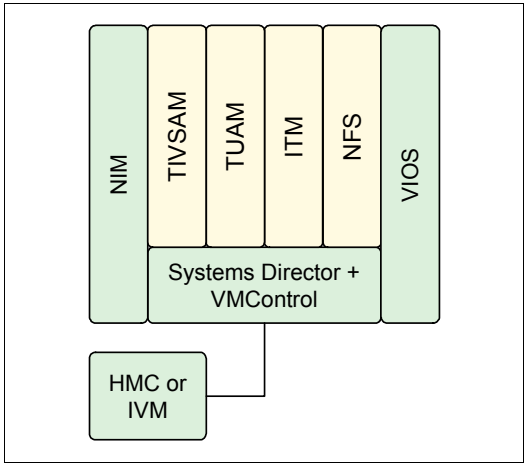

Figure 1-3 ISDM management platform components

1.4 TivSAM virtual appliance

The TivSAM virtual appliance orchestrates the activities of all the IBM Service Delivery Manager components. It is based on Tivoli's process automation engine (TPAe), implementing a data center model (DCM), workflows, and applications for automating the management of IT services.

Tivoli Service Automation Manager allows for automated provisioning, management, and deprovisioning of virtual servers, operating systems, middleware, and application software. Several virtualization (hypervisor) technologies are supported on IBM System x, System p, and System z.

The TivSAM virtual appliance comprises the components shown in Figure 1-4. On a Power Systems server, the LPAR runs AIX. At the time of writing it hosts these:

DB2®	Database: IBM DB2 Enterprise Server Edition V9.7 Fix Pack 3
WAS ND	WebSphere® Network Deployment V6.1.0.29
ITDS	LDAP directory server, Tivoli Directory Server V6.2.0.0
TPM	Tivoli Provisioning Manager Version V7.2.0 Fix Pack 1 and Tivoli Provisioning Manager for Images V7.1.1 Fix Pack 4
TSRM	Tivoli Service Request Manager®: Tivoli Service Request Manager V7.2.0.1 Fix Pack 2 Interim Fix 1 Advanced Workflow Designer and Tivoli Service Request Manager V7.3.0.0 Service Provider Support
TSAM	Tivoli Service Automation Manager V7.2.2 with interim fix HF0001 and Tivoli Service Automation Manager Extension for Usage and Accounting V1.0
HTTP	Web server: IBM HTTP Server V6.1.0.29

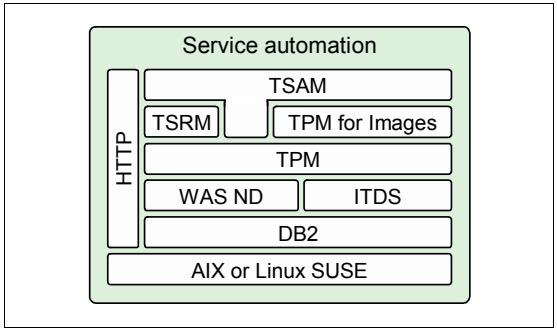

Figure 1-4 TivSAM appliance components

The operational relationship between each of these components is shown in Figure 1-5. In this figure CCMD is the configuration management database used by Tivoli Service Request Manager and Tivoli Service Automation Manager. The DCM is the data center model, a description of the cloud resources, required by Tivoli Provisioning Manager.

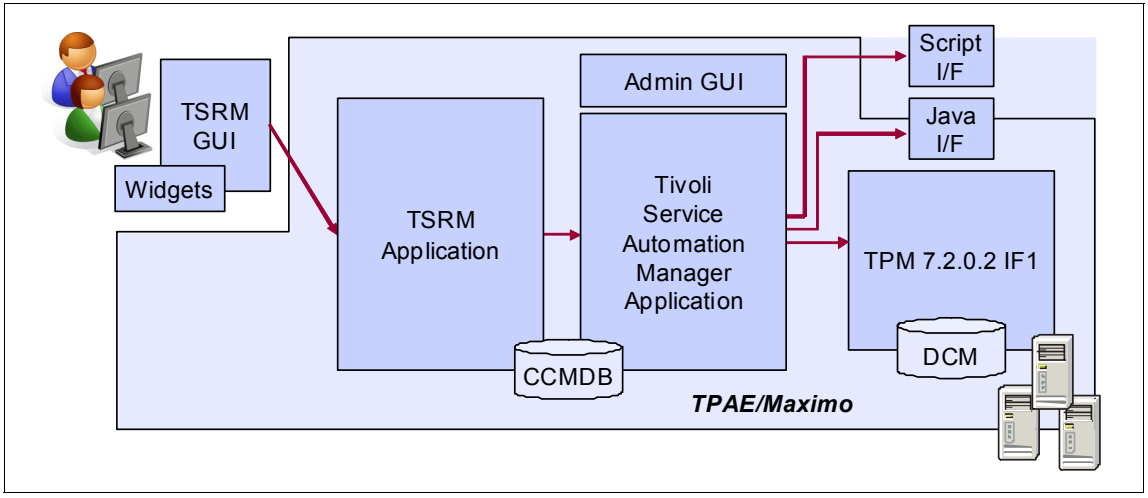

Figure 1-5 Tivoli Service Automation Manager request flow

Tivoli Service Automation Manager has a number of predefined services in the form of templates. These are customized to provide a customized service definition for a specific environment. A service definition captures real-world IT services in both its structure and process. It might be a simple, single-instance operating system or a complex, multitier service. Customized service definitions are made available for selection to one or more customers. The service definition can optionally undergo a review and approval cycle before being admitted into the service catalogue.

TivSAM user interfaces

Tivoli Service Automation Manager has two distinct user interfaces:

- A self-service interface through Tivoli Service Request Manager (SRM)
- An administrative interface through Tivoli's process automation engine (maximo). See Figure 1-5.

Self-service user interface

The self-service user interface is the interface seen by the users. It supports the user-initiated provisioning and management of services and virtual servers. It is a modern, easy-to-use, web interface.

The actions available from the self-service user interface include these:

- Create a virtual server and add it to a new or existing project.
- Install operating systems and applications to virtual servers from the image library.
- Save and restore virtual server images.
- Delete virtual servers.
- Cancel a project and free up projects resources.
- Start and stop virtual servers.
- Manage Tivoli Service Automation Manager application users.
- Manage users and teams.

This interface is described in detail in the “Using the Self-Service Virtual Management offerings” section of the *IBM Service Delivery Manager User's Guide*:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/topic/com.ibm.tsamee.doc/out/isdm.ug.book.pdf

Administrative user interface

The administrative user interface is the standard interface for the Tivoli's process automation engine, formerly known as Maximo®. It is the interface used by service and system administrators to install, upgrade, and configure the environment. The interface is described in detail in the *IBM Service Delivery Manager User’s Guide* and in the *Tivoli Service Automation Manager Installation and Administration Guide*:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/topic/com.ibm.tsam.doc/tsam.admin.book.pdf

1.5 IBM Tivoli Monitoring (ITM) appliance

IBM Service Delivery Manager includes the stand-alone software that monitors and manages system and network applications, power and energy usage, availability, and performance of your enterprise systems, and provides reporting for trending. It provides real-time and historical data through the Tivoli Enterprise Portal and the Tivoli Performance Analyzer interfaces.

The components of the IBM Tivoli Monitoring appliance are shown in Figure 1-6. On a Power Systems server, the LPAR runs AIX. At the time of writing it hosts these:

DB2	Database, IBM DB2 Enterprise Server Edition V9.7 Fix Pack 3
HTTP	Web server, IBM HTTP Server V7.0
TCR	Tivoli Common Reporting V1.3
TEMS	Tivoli Enterprise Monitoring Server V6.2.2 Fix Pack 4
TEPS	Tivoli Enterprise Portal Server V6.2.2 Fix Pack 4
VMAgent	From VMAgent to Power Systems agents - HMC Base Premium agent - IBM Tivoli Monitoring agent for System Director Base - CEC Base Agent
PA	Performance Analyzer (optional install)
TDW	Tivoli Data Warehouse database V6.2.2 Fix Pack 4

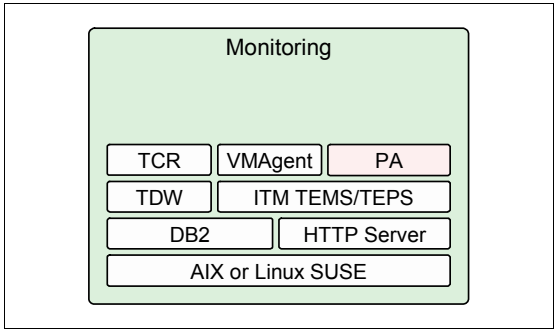

Figure 1-6 ITM appliance components

1.6 IBM Tivoli Usage and Accounting Manager (TUAM) appliance

Tivoli Usage and Accounting Manager helps you understand the costs incurred and revenues generated by your infrastructure. For example, you can track, allocate, and invoice based on criteria such as resource usage by department or user. It tracks service instance creation, modification, deletion, and the resources assigned (reserved) and consumed. The collected information can be periodically extracted and transformed in to common server resource (CSR) files.

Tivoli Usage and Accounting Manager retrieves these files and uses them to generate reports.

The components of the Tivoli Usage and Accounting appliance are shown in Figure 1-7. On a Power Systems server, the LPAR runs AIX. At the time of writing it hosts these:

DB2	Database, IBM DB2 Enterprise Server Edition V9.7 Fix Pack 3
TCR	Tivoli Common Reporting V2.1
TUAM	Tivoli Usage and Accounting Manager V7.3 Fix Pack 1

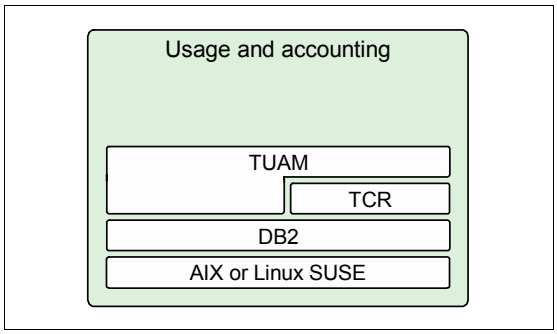

Figure 1-7 TUAM appliance components

See the *IBM Service Delivery Manager User's Guide* to learn about this component:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/topic/com.ibm.tsamee.doc/out/isdm.ug.book.pdf

1.7 NFS appliance

The NFS appliance hosts the auxiliary infrastructure required by IBM Service Delivery Manager. It provides a single point of contact for all IBM Service Delivery Manager components through URL redirection. It also provides e-mail forwarding of notifications and file servers, as shown in Figure 1-8 on page 11.

The NFS and SAMBA file repositories store the Tivoli Monitoring agent binaries. They are used by Tivoli Service Automation Manager when provisioning a virtual image.

The Postfix mail server supports the Tivoli Service Automation Manager notification system.

The virtual image is the single access point to Tivoli Usage and Accounting Manager, Tivoli Service Automation Manager Tivoli Provisioning Manager, Tivoli Common Reporting, and IBM Tivoli Monitoring user interfaces. This means that you can use its IP address and host name in a web browser to access the Tivoli Usage and Accounting Manager, Tivoli Service Automation Manager, Tivoli Provisioning Manager, Tivoli Common Reporting, and IBM Tivoli Monitoring user interfaces without needing to remember the specific virtual machines' addresses and host names.

The URL redirection mechanism relies on four HTTP server instances running on the NFS_appliance. A frontend HTTP server receives all incoming requests and, using rewrite rules, forwards them to one of three internal HTTP servers, each one specific to one of the other appliances:

- TivSAM
- TUAM
- ITM

These internal web servers have their own configuration files that route the request to the appropriate URL on the destination server. The request flow is shown in Figure 1-9 on page 12.

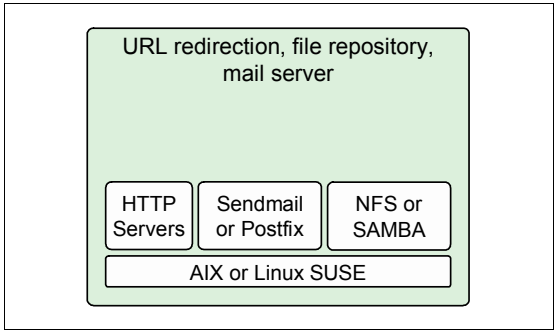

Figure 1-8 NFS appliance components

The front-end HTTP Server receives the requests from the external network. It redirects each of them to the HTTP server instance dedicated to the specific IBM Service Delivery Manager product machine by using a set of rewrite rules.

Each of these HTTP server instances then forwards the HTTP request to the real URL of the specific IBM Service Delivery Manager applications.

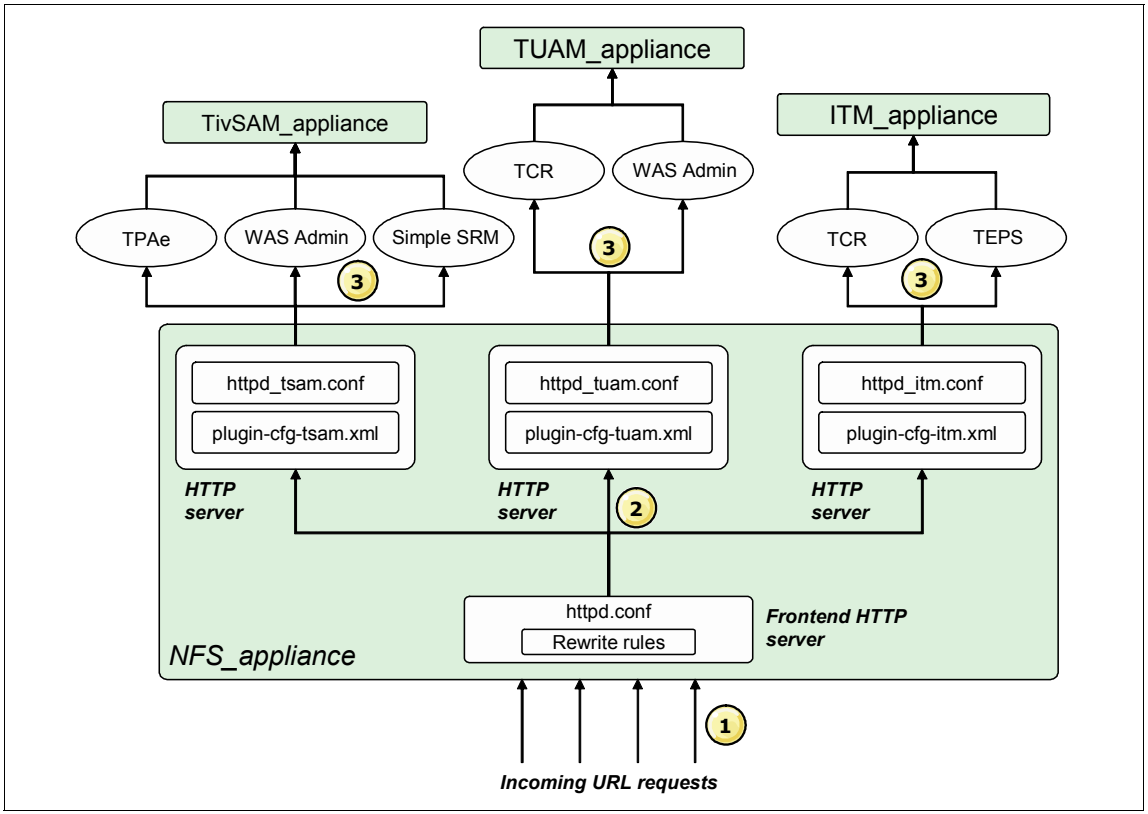

Figure 1-9 HTTP URL redirection within the NFS appliance

The URL redirection is a convenience mechanism. You can contact each appliance through its own web interface by directly addressing the server. However, the URL redirection mechanism allows you to place the web interfaces of the Tivoli Service Automation Manager, Tivoli Monitoring, and Tivoli Usage and Accounting appliances on a private network, thus hiding these services from users.

The URL rewrite rules are customized to your environment when setting up the stereo-cables with the **`vEngine.sh`** command, discussed in more detail in the following sections.

1.8 Connecting the appliances

After they are deployed, the four appliances that comprise IBM Service Delivery Manager find each other using a technology called *Service Connection Engine*, as shown in Figure 1-10. The Service Connection Engine is plugged in when running the **vEngine.sh** script. The complete installation, including the use of the **vEngine.sh** command, is discussed starting in Chapter 4, “ISDM installation” on page 65.

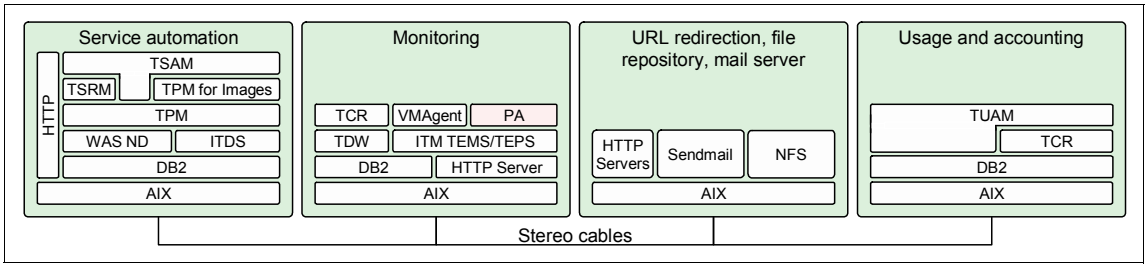

Figure 1-10 Connecting the appliances with Service Connection Engine

2

IBM Service Delivery Manager prerequisites

To deploy IBM Service Delivery Manager, your environment must meet certain minimum requirements. This chapter outlines the minimum system resources that you need, as well as the supporting software. This chapter also describes the specific resources and software versions used while writing this book.

2.1 Hardware prerequisites

The requirements for each of these components are outlined in this chapter, in addition to the specific configuration of the environment that we used when writing this publication.

2.1.1 Computer nodes

The computer nodes are the nodes on which Tivoli Service Automation Manager deploys the virtual images. The resources needed to support computer nodes vary depending on your specific workloads. For the list of hardware prerequisites, see the Tivoli Service Automation Manager *Installation and Administration Guide*:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?topic=%2Fcom.ibm.tsam.doc_7.2%2Ft_install_tsam_lpad.html

2.1.2 Management node

The management node is the system where you install IBM Service Delivery Manager. The following resource requirements are provided in the *IBM Service Delivery Manager Installation and Configuration Guide*. Table 2-1 shows the required resources for each virtual image, as well as the total resources required.

Table 2-1 Resources required for each of the virtual images on Power Systems

Virtual image	Number of cores[a]	Disk space (GB)	Memory (GB)
TIVSAM_image	4	130	16
ITM_image	2	40[b]	6
TUAM_image	1	30	4
NFS_image	1	22	2
TOTAL	8	230	28

a. IBM Service Delivery Manager requires POWER6® or POWER7® cores.

b. Additional disk space is required if you want to use the IBM Tivoli Monitoring data warehouse. For more information, see “Hardware prerequisites for IBM Tivoli Monitoring data warehouse” in the *IBM Service Delivery Manager Installation and Configuration Guide.*

2.1.3 Our configuration

The test systems used during the authoring of this publication were two IBM Power 750 Express machines, with the following specifications:

- 16 IBM POWER7 cores
- 128 GB RAM
- 2 x 69 GB 15K SAS drives
- 6 x 146 GB 15K SAS drives
- PowerVM Enterprise Edition

Our environment also included a DS4800 with 1.8 TB of storage provided by fourteen 146 GB disks and attached using an IBM 2005-B16 SAN switch.

2.2 Software prerequisites

In our configuration, IBM Service Delivery Manager uses PowerVM managed through IBM Systems Director VMControl™.

These software packages are required in support of VMControl:

- IBM Systems Director

  IBM Systems Director provides a single-point-of-control and simplifies the management of physical and virtual platform resources.

- IBM Systems Director VMControl Enterprise Edition

  IBM Systems Director VMControl provides life-cycle management for virtual machines in our Power Systems environment.

  As of this writing, the supported version is IBM Systems Director VMControl 2.3.1.2. For an updated list of IBM Systems Director VMControl requirements, access this URL:

  http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp?topic=/com.ibm.director.vim.helps.doc/fsd0_vim_main.html

  For the purposes of this document we used the IBM Systems Director VMControl, which was packaged with the IBM Service Delivery Manager eAssembly.

- Network Installation Manager (NIM)

  NIM provides the capability to manage and deploy software over the network to physical or virtual hardware. NIM can deploy base operating systems and software packages and is the mechanism by which VMControl deploys virtual appliances.

  For IBM Service Delivery Manager, NIM must run on AIX Version 6.1 Technology Level 6 (TL6) Service Pack 5 (SP5).

- Common Information Model (CIM)

  CIM is a standardized way to describe objects and their relationships. CIM is used to provide a common description of an environment to heterogeneous management products. The Storage Management Initiative - Specification (SMI-S) is a CIM-based standard for interacting with storage resources. In this environment, SMI-S CIM providers provide IBM Systems Director with an interface to our storage and SAN resources.

For the remainder of this publication we assume that these components are installed and properly configured in your environment. For more information about configuring these components in support of your IBM Service Delivery Manager deployment, refer to *Deploying Cloud Components on POWER*, SG24-8009:

http://www.redbooks.ibm.com/abstracts/sg248009.html?Open

In our configuration we used the following versions:

- IBM Systems Director 6.2.1.2
- IBM Systems Director VMControl 2.3.1.2
- LSI SMI-S Providers 10.10.6555
- Brocade SMIAgent 120.10.0

In addition, a few additional software packages will be required to complete the TIVSAM_image deployment. The following RPM packages must be installed to complete the activation of TIVSAM_image:

```
glib-1.2.10-2.aix4.3.ppc.rpm
gettext-0.10.40-8.aix5.2.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm
atk-1.12.3-2.aix5.2.ppc.rpm
bash-3.2-1.aix5.2.ppc.rpm
bash-doc-3.2-1.aix5.2.ppc.rpm
zlib-1.2.3-4.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm
libpng-1.2.32-2.aix5.2.ppc.rpm
```

```
pixman-0.12.0-2.aix5.2.ppc.rpm
xrender-0.9.1-2.aix5.2.ppc.rpm
cairo-1.8.6-1.aix5.2.ppc.rpm
curl-7.9.3-2.aix4.3.ppc.rpm
freetype-1.3.1-9.aix5.1.ppc.rpm
gdbm-1.8.3-5.aix5.2.ppc.rpm
readline-4.3-2.aix5.1.ppc.rpm
python-2.3.4-4.aix5.3.ppc.rpm
libtiff-3.8.2-1.aix5.2.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
xft-2.1.6-5.aix5.1.ppc.rpm
pango-1.14.5-2.aix5.2.ppc.rpm
xcursor-1.1.7-2.aix5.2.ppc.rpm
gtk2-2.10.6-1.aix5.2.ppc.rpm
unzip-5.51-1.aix5.1.ppc.rpm
wget-1.9.1-1.aix5.1.ppc.rpm
zip-2.3-3.aix4.3.ppc.rpm
perl-5.8.2-1.aix5.1.ppc.rpm
tar-1.14-2.aix5.1.ppc.rpm
procmail-3.21-1.aix4.3.ppc.rpm
```

IBM Service Delivery Manager launchpad

To use the launchpad to create an IBM Service Delivery Manager configuration, ensure that the system where the launchpad runs has one of the following operating systems installed:

- AIX 6.1
- Windows 7
- Windows 2008
- Windows Vista

Make sure that you use one of the following browsers:

- Internet Explorer 7
- Internet Explorer 8
- Firefox 3.0 or 3.5

3

Preparing IBM Service Delivery Manager for deployment

IBM Service Delivery Manager on Power Systems is distributed as electronic images and is available using IBM Passport Advantage®. The electronic images include everything required to set up and run a private cloud, including licensed copies of IBM Systems Director Standard Edition for Power Systems and IBM Systems Director VMControl Enterprise Edition. The license for IBM Systems Director and IBM Systems Director VMControl is only allowed to be used for IBM Systems Director VMcontrol.

Some of the downloaded images require further manual preparation before they can be used for deploying components of IBM Service Delivery Manager.

This chapter describes the included software in IBM Service Delivery Manager electronic distribution packages, how to prepare the electronic images deploying IBM Service Delivery Manager, and how to create the open virtualization format file using the launchpad tool.

3.1 Required software

IBM Service Delivery Manager for Power Systems version 7.2.2 is available for download from IBM Passport Advantage. The part number for IBM Service Delivery Manager for Power Systems Version 7.2.2 is CRFK7ML.

The entire IBM Service Delivery Manager for Power Systems Version 7.2.2 comprises 50 downloadable images with a total download size of 92.741 MB. Not all images are required to create an IBM Service Delivery Manager private cloud. Many of the images provide extra functionality to the private cloud.

The images that we downloaded to create our IBM Service Delivery Manager Power Systems private cloud are listed in Table 3-1.

Table 3-1 Downloaded Images

Part number	Description	File name	File size (MB)
CI25CML	IBM Service Delivery Manager for Power System V7.2.2, 1of 20, Installation Launchpad, for AIX	ISDM_for_Power_1of20_V722.tar	48
CI25EML	IBM Service Delivery Manager for Power V7.2.2, 3 of 20, IBM Tivoli Monitoring virtual image Part 1, for AIX	ISDM_Power_3of20_V722-ITM_part1.tar	4054
CI25FML	IBM Service Delivery Manager for Power V7.2.2, 4 of 20, IBM Tivoli Monitoring virtual image Part 2, for AIX	ISDM_Power_4of20_V722-ITM_part2.tar	4054
CI25GML	IBM Service Delivery Manager for Power V7.2.2, 5 of 20, IBM Tivoli Monitoring virtual image Part 3, for AIX, Multilingual	ISDM_Power_5of20_V722-ITM_part3.tar	1804
CI25HML	IBM Service Delivery Manager for Power V7.2.2, 6 of 20, IBM Tivoli Usage and Accounting Manager virtual image Part 1, for AIX	ISDM_Power_6of20_V722-TUAM_part1.tar	4054
CI25IML	IBM Service Delivery Manager for Power V7.2.2, 7 of 20, IBM Tivoli Usage and Accounting Manager virtual image Part 2, for AIX	ISDM_Power_7of20_V722-TUAM_part2.tar	4054
CI25JML	IBM Service Delivery Manager for Power V7.2.2, 8 of 20, IBM Tivoli Usage and Accounting Manager virtual image Part 3	ISDM_Power_8of20_V722-TUAM_part3.tar	4054
CI25KML	IBM Service Delivery Manager for Power V7.2.2, 9 of 20, IBM Tivoli Usage and Accounting Manager virtual image Part 4	ISDM_Power_9of20_V722-TUAM_part4.tar	1206

Part number	Description	File name	File size (MB)
CI25BML	IBM Service Delivery Manager for Power V7.2.2, 10 of 20, IBM HTTP Server and NFS virtual image Part 1	ISDM_Power_10of20_V722_NFS_part1.tar	4054
CI25LML	IBM Service Delivery Manager for Power V7.2.2, 11 of 20, IBM HTTP Server and NFS virtual image Part 2	ISDM_Power_11of20_V722_NFS_part2.tar	3493
CI25MML	IBM Service Delivery Manager for Power V7.2.2, 12 of 20, Tivoli Service Automation Manager virtual image Part 1	ISDM_Power_12of20_V722-TSAM_part1.tar	4054
CI25NML	IBM Service Delivery Manager for Power V7.2.2, 13 of 20, Tivoli Service Automation Manager virtual image Part 2	ISDM_Power_13of20_V722-TSAM_part2.tar	4054
CI25PML	IBM Service Delivery Manager for Power V7.2.2, 14 of 20, Tivoli Service Automation Manager virtual image Part 3	ISDM_Power_14of20_V722-TSAM_part3.tar	4054
CI25QML	IBM Service Delivery Manager for Power V7.2.2, 15 of 20, Tivoli Service Automation Manager virtual image Part 4	ISDM_Power_15of20_V722-TSAM_part4.tar	4054
CI25RML	IBM Service Delivery Manager for Power V7.2.2, 16 of 20, Tivoli Service Automation Manager virtual image Part 5	ISDM_Power_16of20_V722-TSAM_part5.tar	4054
CI25SML	IBM Service Delivery Manager for Power V7.2.2, 17 of 20, Tivoli Service Automation Manager virtual image Part 6	ISDM_Power_17of20_V722-TSAM_part6.tar	4054
CI25TML	IBM Service Delivery Manager for Power V7.2.2, 18 of 20, Tivoli Service Automation Manager virtual image Part 7	ISDM_Power_18of20_V722-TSAM_part7.tar	4054
CI25UML	IBM Service Delivery Manager for Power V7.2.2, 19 of 20, Tivoli Service Automation Manager virtual image Part 8	ISDM_Power_19of20_V722TSAM_part8.tar	4054
CI25VML	IBM Service Delivery Manager for Power V7.2.2, 20 of 20, Tivoli Service Automation Manager virtual image Part 9	ISDM_Power_20of20_V722-TSAM_part9.tar	334
CI2DGML	IBM System Director for AIX V6.2.1	System_Director_AIX_V6.2.1.tar	4377
CZVK0ML	IBM System Director VMControl Enterprise Edition V2.3.0 for ISDM V7.2.1	Sys_Dir_VMControl_Ent_Ed_V2.3.tar.gz	258

Note: IBM Systems Director for AIX 6.2.1 and IBM Systems Director VMControl Enterprise Edition V2.3.0 for ISDM V7.2.1 were downloaded and used to build the IBM Systems Director and IBM Systems Director VMControl infrastructure. The instructions for building the IBM Systems Director infrastructure can be found in *Deploying Cloud Components on POWER*, REDP-5711.

3.2 Preparing virtual images for deployment

To import the downloaded images into the hypervisor, two separate steps must be performed:

- The separate components that make up IBM Service Delivery Manager must be concatenated into a single file.

  The separate virtual images that make up IBM Service Delivery Manager are very large, for example, greater than 7 GB. They have been broken up into 4,054 MB files to make downloading easier and more manageable.

- An open virtualization format (OVF) file must be created.

  The OVF file contains information that is used during deployment of the virtual image to set the image's parameters, such as IP address, netmask, host name, passwords, and so on.

3.2.1 Concatenating the virtual images

After downloading the virtual images from Table 3-1 on page 22 onto our desktop, we copied the files to our AIX NIM server, nim.powercloud.ibm.com, using secure copy protocol. Logging in to our NIM server as root, we ran the following commands to concatenate, and we ran the **untar** command on the virtual image. The resulting virtual image is an AIX `mksysb` file.

To concatenate the virtual images and untar them on AIX, run the commands shown in Example 3-1 in the directory where the virtual images are stored.

Example 3-1 Commands to concatenate virtual images

```
cat ISDM_Power_?of2O_V722-ITM_part?.tar | gtar xvf -
cat ISDM_Power_?of2O_V722-TUAM_part?.tar | gtar xvf -
cat ISDM_Power_1?of2O_V722_NFS_part?.tar | gtar xvf -
cat ISDM_Power_*of2O_V722*SAM_part?.tar | gtar xvf -
```

Hint: GNU Tar is required to untar the virtual images. If using AIX, we recommend installing GNU Tar from the IBM AIX Toolbox website:

http://www.ibm.com/systems/p/os/aix/linux/toolbox/download.html

Hint: When concatenating on AIX, ensure that your ulimit for the particular shell session is set to unlimited using the **`ulimit unlimited`** command.

Hint: Ensure that you have enough free disk space to store all of the virtual images and the resulting `mksysb` file. The recommended minimum disk to perform the procedure is 130 GB.

The output from the commands in Example 3-1 on page 24 is four `mksysb` files:

- `isdmitm.mksysb`
- `isdmtuam.mksysb`
- `isdmnfs.mksysb`
- `isdmtivsam.mksysb`

3.2.2 Creating the OVF file

The easiest way to create the required OVF file is to use the *launchpad* application. This is supplied as part of the IBM Service Delivery Manager application bundle, part number CI25CML. The launchpad application is a graphical user interface (GUI) based application that runs on Windows Vista, Windows 7, Windows 2008, AIX Version 6.1, and AIX Version 7. The application prompts the user to complete information about each virtual image. When all of the answers have been completed, the application uses the inputted information to create an OVF file for each of the virtual images.

The launchpad tool requires multiple parameters. We recommend making a list of all of the required parameters before creating the OVF file.

Table 3-2 provides a list of the parameters that we used to complete the launchpad questions.

Table 3-2 OVF virtual image settings

Item	Value
Configuration name	isdm-power-722
Multicast IP address	228.1.2.3
Multicast Port Number	10283
Tivoli Service Automation Manager virtual image settings	

Item	Value
Hostname	tivsam
Domain	powercloud.ibm.com
IP Address	172.16.20.123
Netmask	255.255.252.0
Gateway	172.16.20.1
Primary DNS	172.16.20.7
Secondary DNS	172.16.20.7
root password	********
virtuser password	********
IBM Tivoli Monitoring virtual image settings	
Hostname	itm
Domain	powercloud.ibm.com
IP Address	172.16.20.124
Netmask	255.255.252.0
Gateway	172.16.20.1
Primary DNS	172.16.20.7
Secondary DNS	172.16.20.7
root password	********
virtuser password	********
Tivoli Usage and Accounting Manager virtual image settings	
Hostname	tuam
Domain	powercloud.ibm.com
IP Address	172.16.20.125
Netmask	255.255.252.0
Gateway	172.16.20.1
Primary DNS	172.16.20.7
Secondary DNS	

Item	Value
root password	********
virtuser password	********
IBM HTTP Server virtual image settings	
Hostname	nfs
Domain	powercloud.ibm.com
IP Address	172.16.20.126
Netmask	255.255.252.0
Gateway	172.16.20.1
Primary DNS	172.16.20.7
Secondary DNS	172.16.20.7
root password	********
virtuser password	********

Take note: All fields are compulsory to deploy the virtual appliance successfully using IBM Systems Director VMControl. We initially left the secondary DNS empty and experienced an **`NullPointerError`** error message when deploying the virtual images from IBM Systems Director VMControl. For more information see the following URL:

https://www-304.ibm.com/support/docview.wss?q1=vmcontrol&rs=0&uid=nas78a978b76a33e50fd862578620068931f&cs=utf-8&wv=1%EF%BE%83%EF%BE%A4%EF%BE%B8=en&loc=en_US&cc=us

The launchpad application is distributed as a `.tar` file. GNU tar is required to extract the files from the archive. An example of the command to extract the files can be found in Example 3-2.

Example 3-2 tar command to extract launchpad application

```
gtar -xvf ISDM_for_Power_1of20_V722.tar
```

The **gtar** command used to extract the files should produce the following files and folders in the directory where the `.tar` file was extracted, as can be seen in Example 3-3.

Example 3-3 Extracted launchpad files and folders

```
# ls -l
total 832
-rw-r--r--    1 root     system         1365 Sep 01 11:53 autorun.inf
drwxr-xr-x   38 root     system         8192 Sep 01 11:53 launchpad
-rw-r--r--    1 root     system       184320 Sep 01 11:53 launchpad.exe
-rw-r--r--    1 root     system         1609 Sep 01 11:53 launchpad.ini
-rwxr-xr-x    1 root     system         6002 Sep 01 11:53 launchpad.sh
-rw-r--r--    1 root     system       208896 Sep 01 11:53
launchpad64.exe
-rw-r--r--    1 root     system         1237 Sep 01 11:53
launchpad64.ini
drwxr-xr-x   12 root     system         4096 Sep 01 11:53 licenses
drwxr-xr-x    2 root     system          256 Sep 01 11:53
ovfConfigFiles
drwxr-xr-x    2 root     system          256 Sep 01 11:53 script
```

The extracted files in Example 3-3 list two important files for launching the launchpad application:

- `launchpad.exe`, the application launcher for Windows
- `launchpad.sh`, the application launcher for AIX

Here are the instructions for how to use the Windows launchpad application `launchpad.exe` to generate the OVF files for the virtual images:

1. Double-click the **`launchpad.exe`** file to start the launchpad application, as shown in Figure 3-1

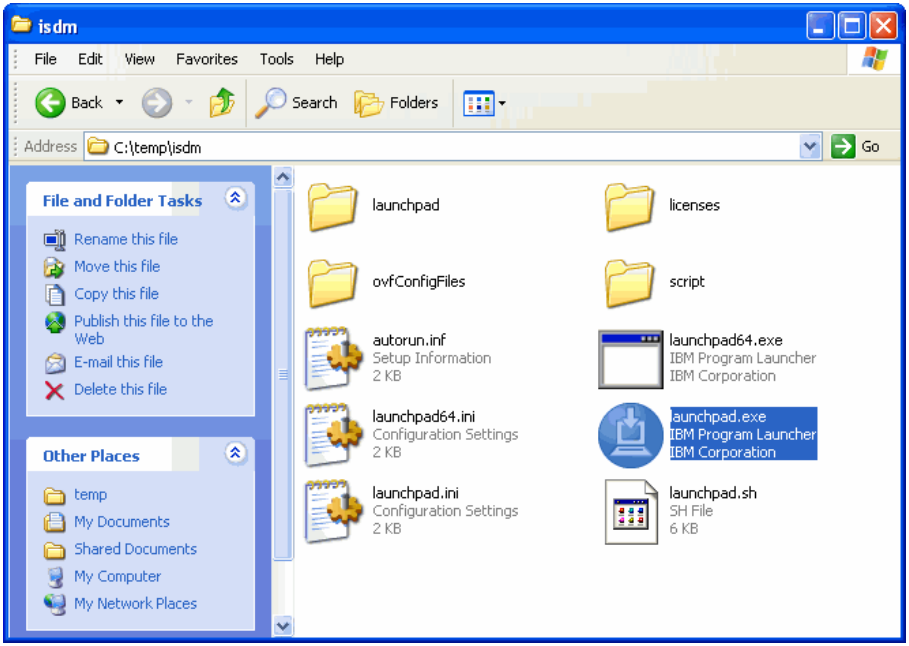

Figure 3-1 Start launchpad application on Windows

2. The launchpad application opens and displays the Welcome screen, as seen in Figure 3-2. The language settings for the GUI can be changed from the Welcome screen by using the drop-down panel in the upper right corner of the launchpad window. Select your preferred language, read the Welcome screen details, and click **Next** to continue.

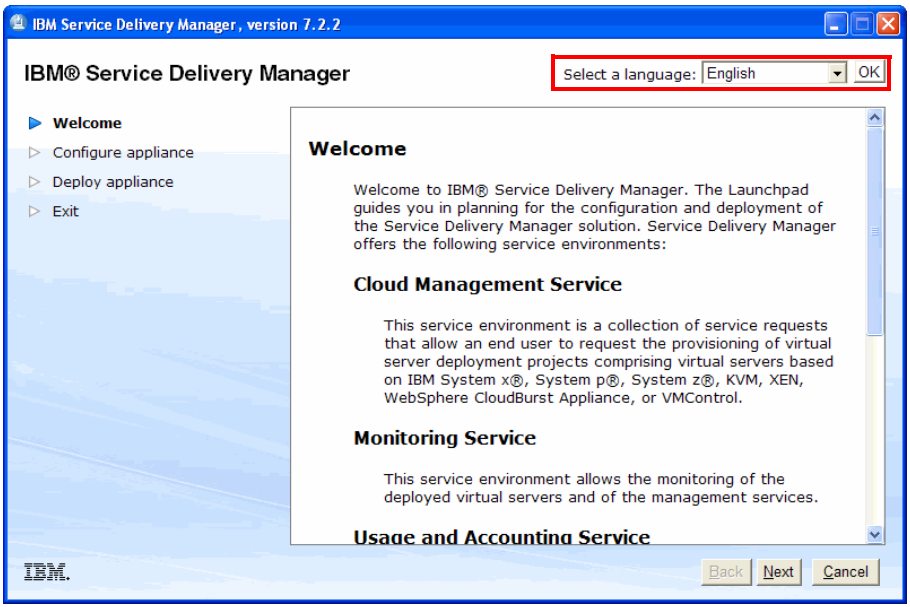

Figure 3-2 Launchpad Welcome panel

3. The Configure appliance screen is displayed, as seen in Figure 3-3. From this screen you can create a new configuration or open an existing configuration. Select **Create a new configuration** and enter the name of the new configuration in the Configuration name field. Click **Next** to continue.

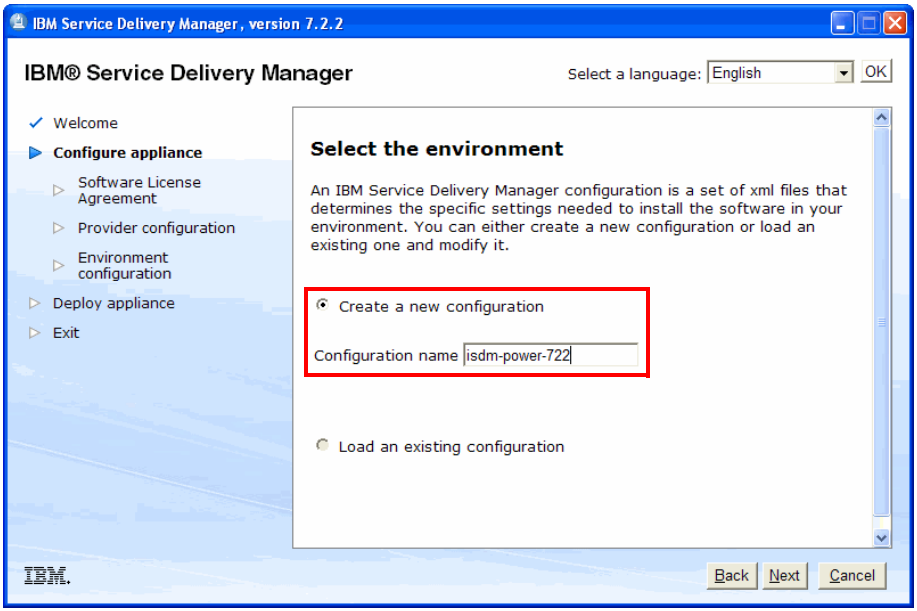

Figure 3-3 The Configure appliance panel

4. The software license agreement screen is displayed Figure 5 on page 33. Read through the license agreement. If you accept the license agreement, click the **I accept the terms in the license agreement** radio button and then click **Next** to continue.

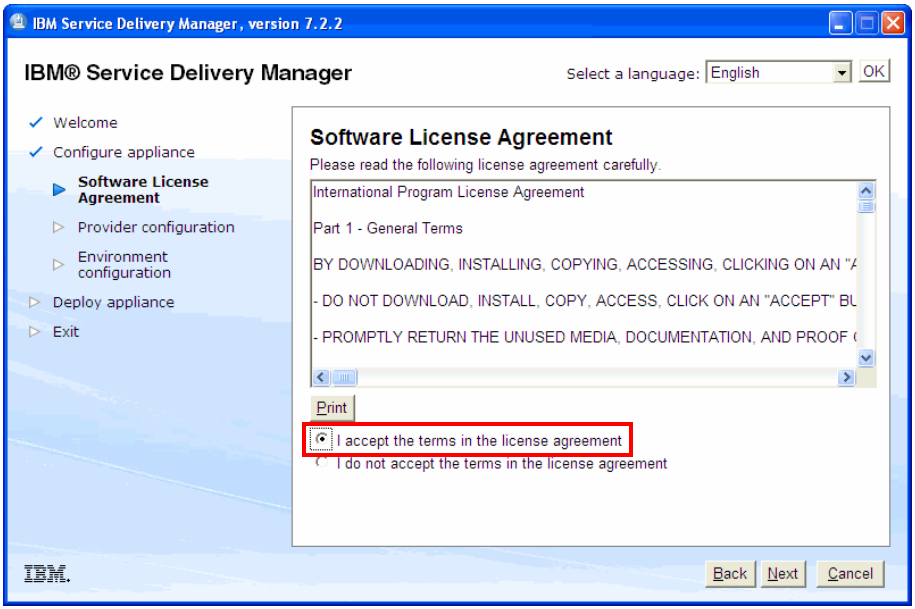

Figure 3-4 Accept the software license agreement panel

5. The Provider configuration screen is displayed, as shown in Figure 3-5. Use the Provider configuration information screen to enter the multicast IP address and port group information, which is required by the service connection engine to provide cross connectivity between the virtual images. Enter the multicast IP address and the service location protocol port number in the Listening/publishing port text field. Select the **Service Connection Engine automatic startup** check box to enable automatic starting of the Service Connection Engine. Click **Next** to continue.

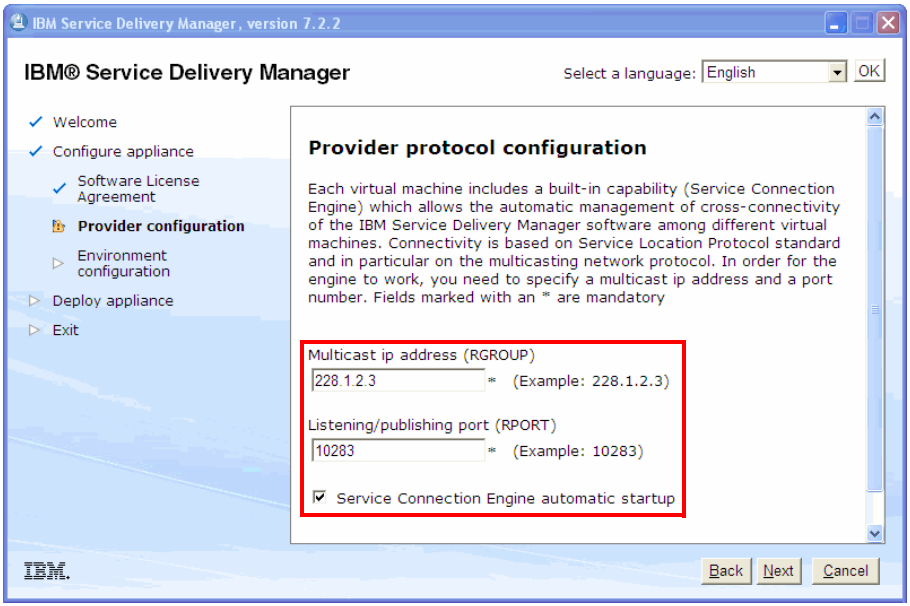

Figure 3-5 Provider configuration panel

6. The environment configuration screen is displayed, as shown in Figure 3-6. Use this screen to select the virtual images that need an OVF file configuration. Select the check boxes for **Monitoring** and **Usage and Accounting** virtual images. Click **Next** to continue.

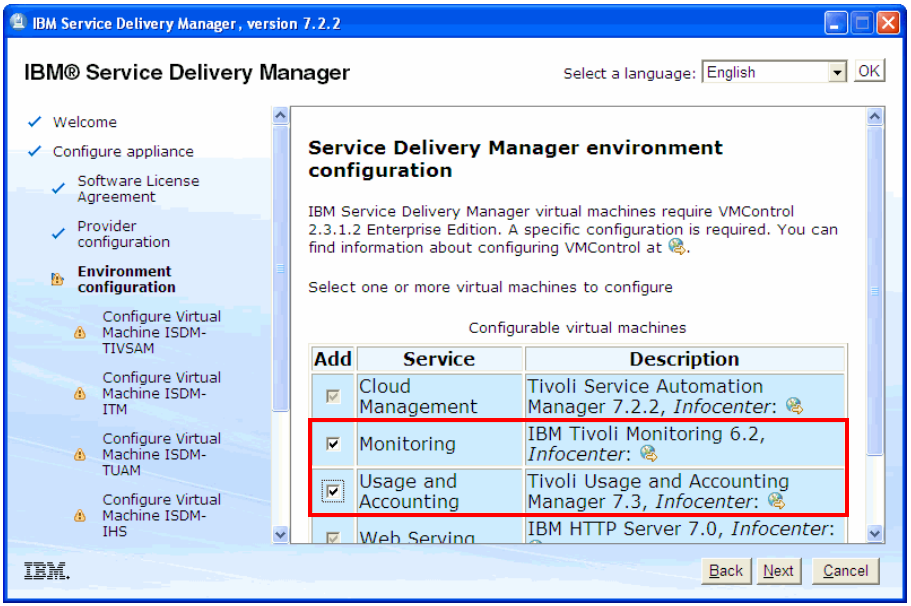

Figure 3-6 Environment configuration panel

7. The Configure Virtual Machine ISDM TIVSAM welcome screen is displayed, as shown in Figure 3-7. It contains the hardware requirements and the software stack that is going to be installed. Click **Next** to continue.

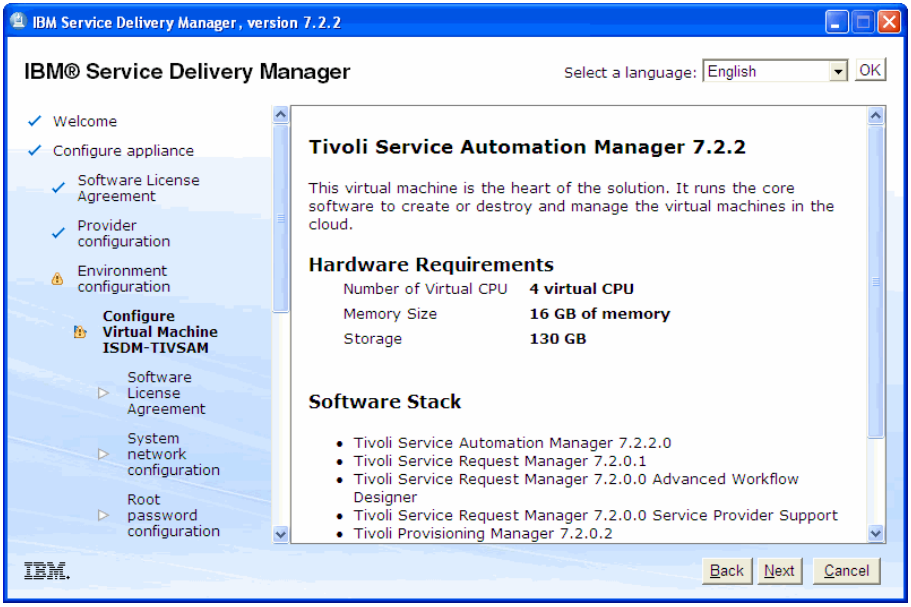

Figure 3-7 Configure virtual machine ISDM-TIVSAM welcome panel

8. The software license agreement for the Tivoli Service Automation Manager software stack is displayed, as shown in Figure 3-8. Read the software license agreement, and then select the **I accept the terms in the license agreement** radio button. Click **Next** to continue.

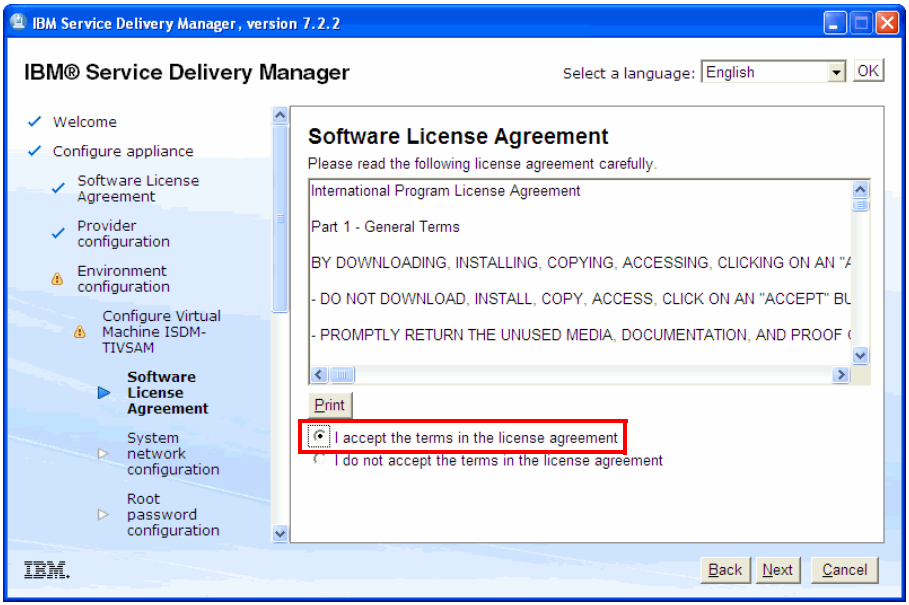

Figure 3-8 ISDM-TIVSAM software stack license agreement

9. The Tivoli Service Automation Manager system network configuration screen is displayed, as shown Figure 3-9. Use the network details that you created earlier in Table 3-2 on page 25 to complete the mandatory questions and the primary DNS details. Click **Next** to continue.

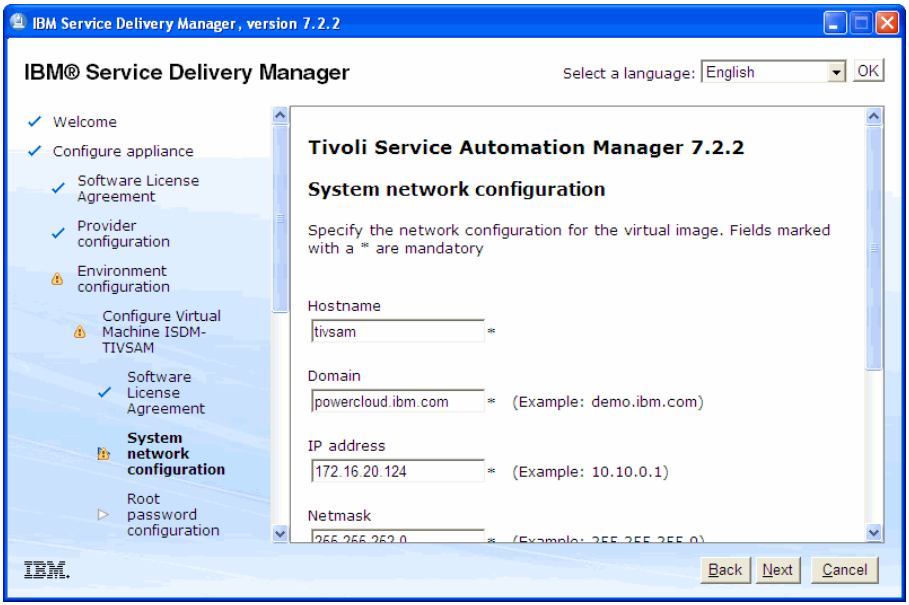

Figure 3-9 ISDM-TIVSAM network configuration

Reminder: All fields are compulsory to deploy the virtual appliance successfully using IBM Systems Director VMControl. We initially left the Secondary DNS field empty and experienced an `NullPointerError` error message when deploying the virtual images from IBM Systems Director VMControl. For further information refer to the following URL:

`https://www-304.ibm.com/support/docview.wss?q1=vmcontrol&rs=0&uid=nas78a978b76a33e50fd862578620068931f&cs=utf-8&wv=1%EF%BE%83%EF%BE%A4%EF%BE%B8=en&loc=en_US&cc=us`

10. The Root password configuration screen is displayed, as shown Figure 3-10. Enter the `root` password for the Tivoli Service Automation Manager virtual image in the password text fields. Click **Next** to continue.

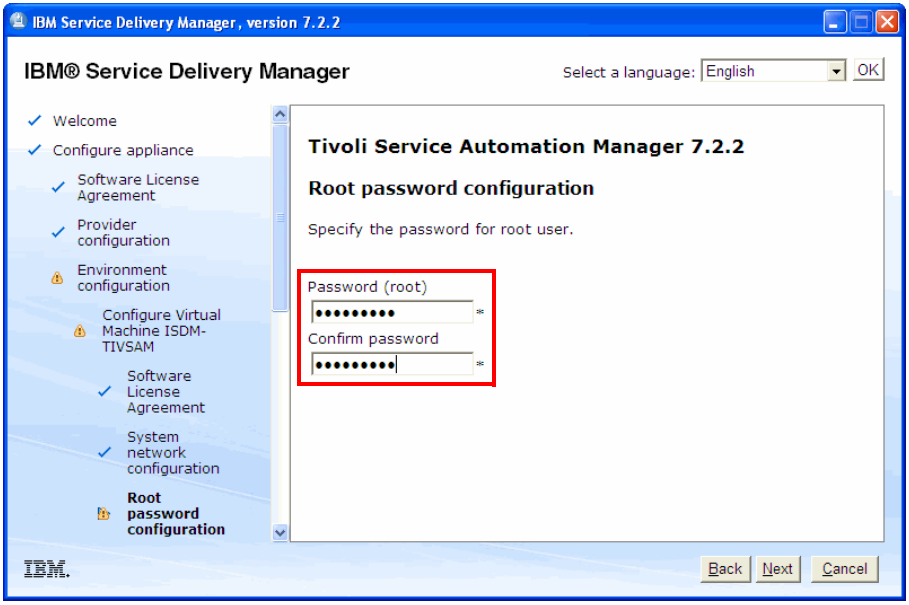

Figure 3-10 ISDM-TIVSAM root password configuration

11. The Virtuser password configuration screen is displayed, as shown in Figure 3-11. Enter the `virtuser` password for the Tivoli Service Automation Manager virtual image in the password text fields. Click **Next** to continue.

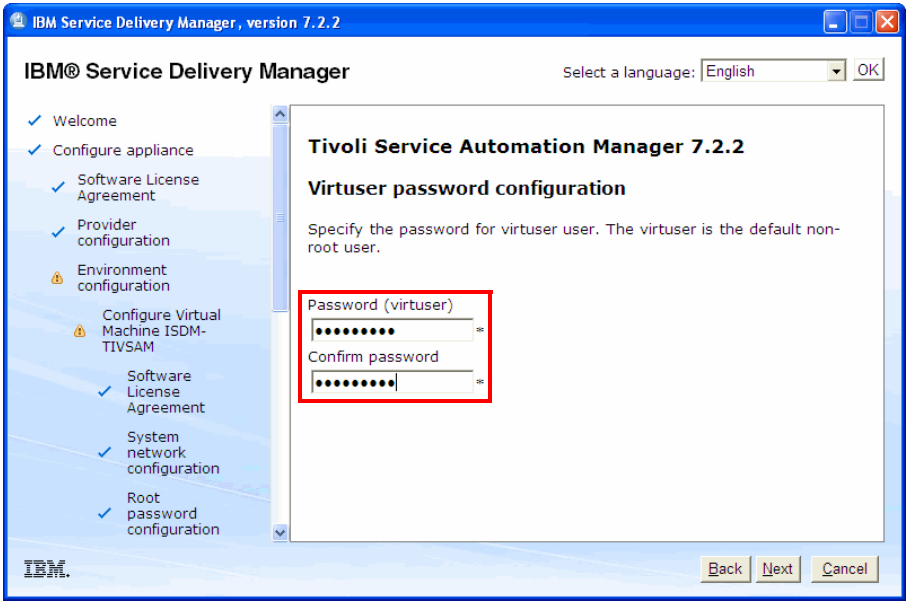

Figure 3-11 ISDM-TIVSAM virtuser password configuration

12. The Tivoli Service Automation Manager virtual image Configuration summary screen is displayed, as shown Figure 3-12. Read the summary information. If the summary information is correct, click **Next** to continue.

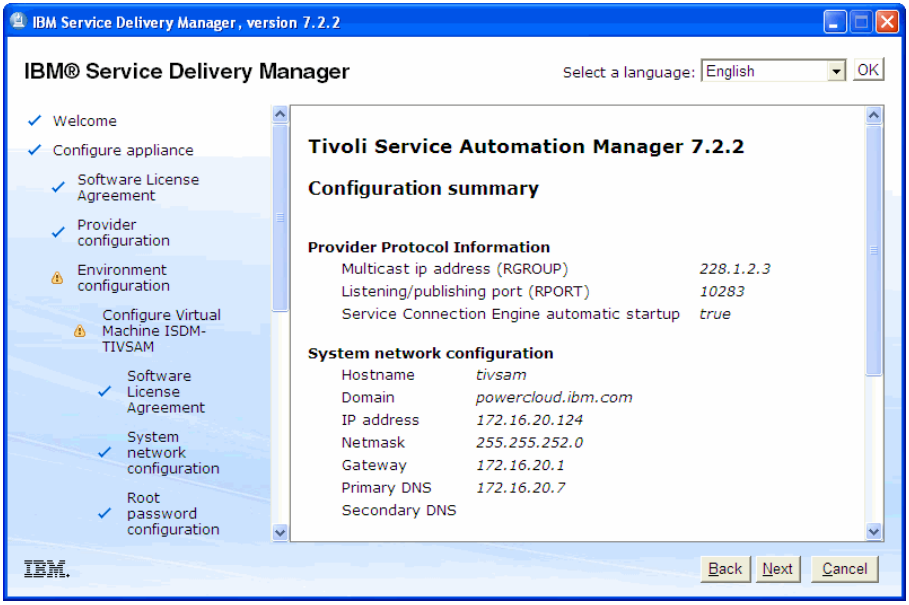

Figure 3-12 ISDM-TIVSAM configuration summary

13. The Configure Virtual Machine ISDM-ITM welcome screen is displayed, as shown in Figure 3-13. It contains the hardware requirements and the software stack that is going to be installed. Click **Next** to continue.

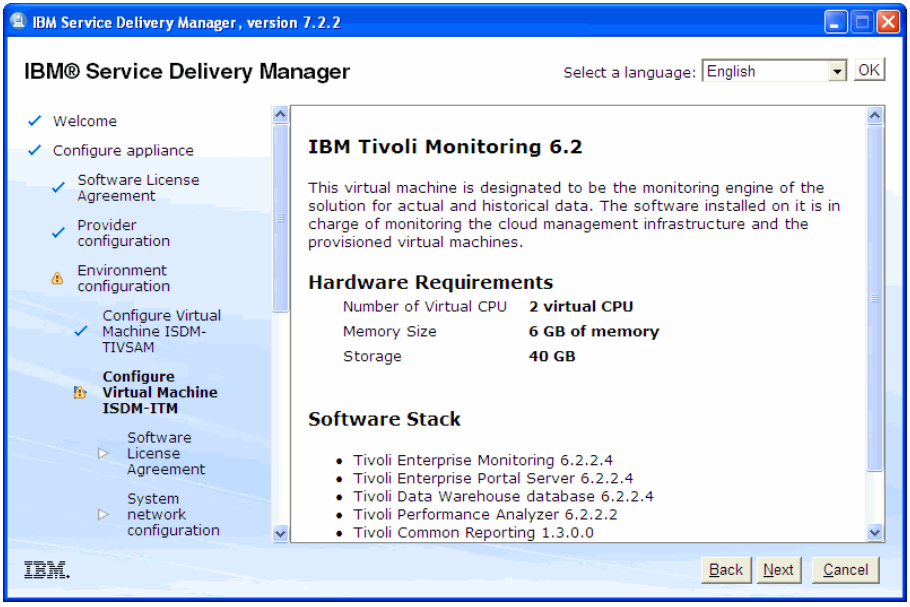

Figure 3-13 Configure virtual machine ISDM-ITM welcome panel

14. The software license agreement for the IBM Tivoli Monitoring software stack is displayed, as shown in Figure 3-14. Read the software license agreement, and then select the **I accept the terms in the license agreement** radio button. Click **Next** to continue.

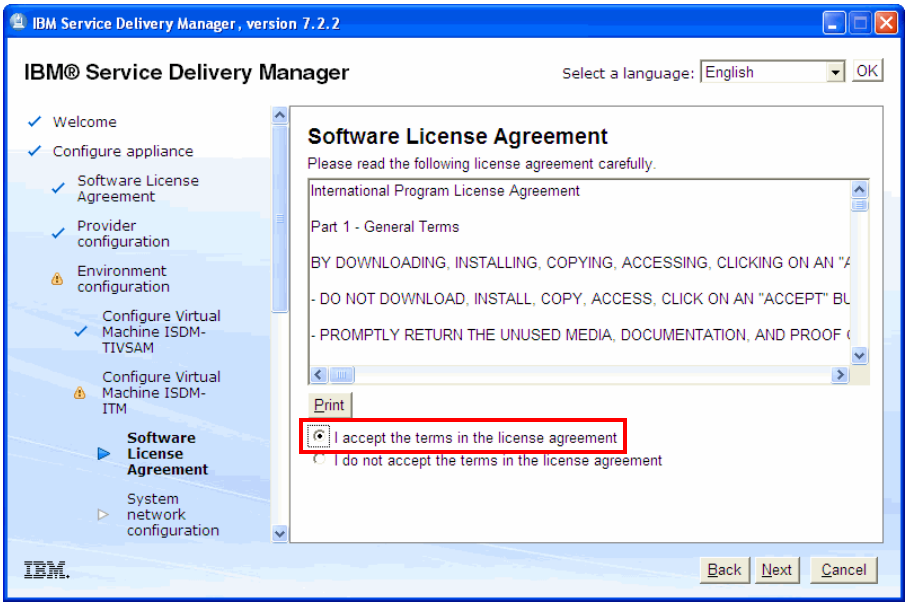

Figure 3-14 ISDM-ITM software stack license agreement

15. The IBM Tivoli Monitoring system network configuration screen is displayed, as shown Figure 3-15. Use the network details that you created earlier in Table 3-2 on page 25 to complete the mandatory questions and primary DNS details. Click **Next** to continue.

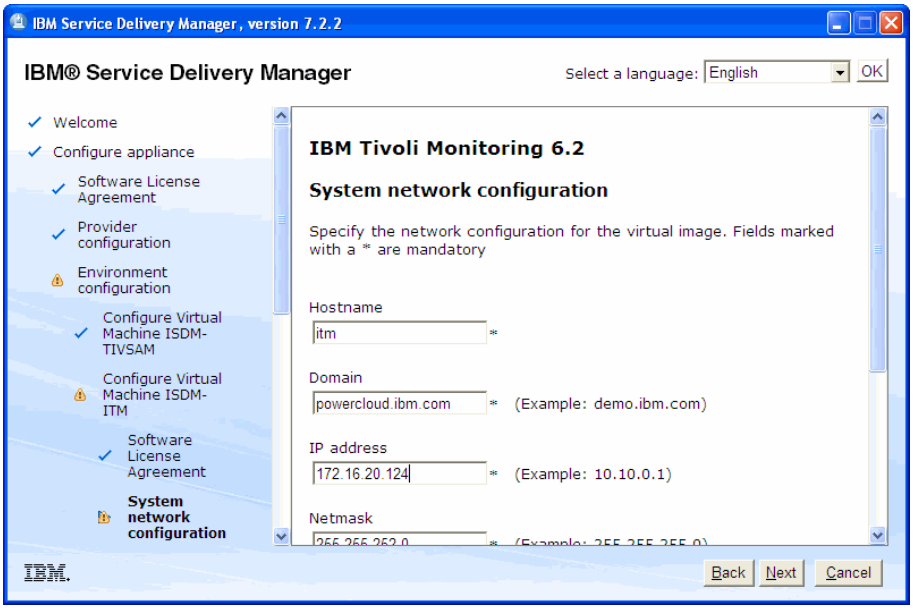

Figure 3-15 ISDM-ITM network configuration

16. The Root password configuration screen is displayed, as shown Figure 3-16. Enter the `root` password for the IBM Tivoli Monitoring virtual image in the password text fields. Click **Next** to continue.

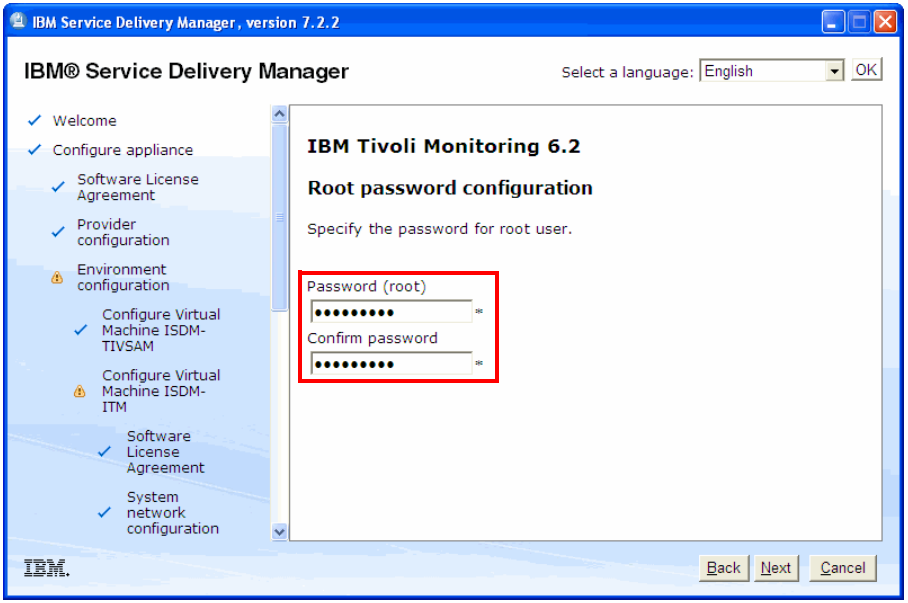

Figure 3-16 ISDM-ITM root password configuration

17. The Virtuser password configuration screen is displayed, as shown in Figure 3-17. Enter the `virtuser` password for the IBM Tivoli Monitoring virtual image in the password text fields. Click **Next** to continue.

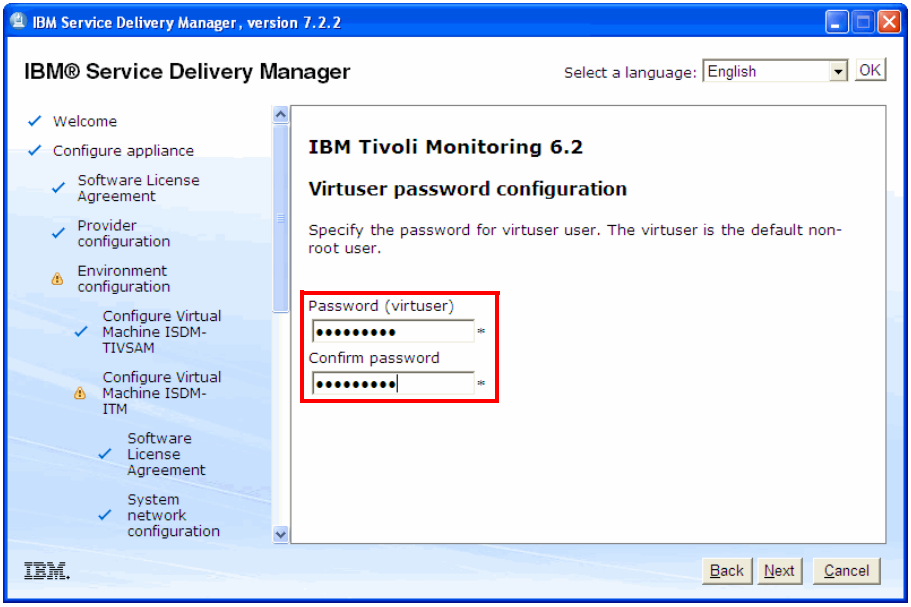

Figure 3-17 ISDM-ITM virtuser password configuration

18. The IBM Tivoli Monitoring virtual image configuration summary screen is displayed, as shown Figure 3-18. Read the summary information. If the summary information is correct, click **Next** to continue.

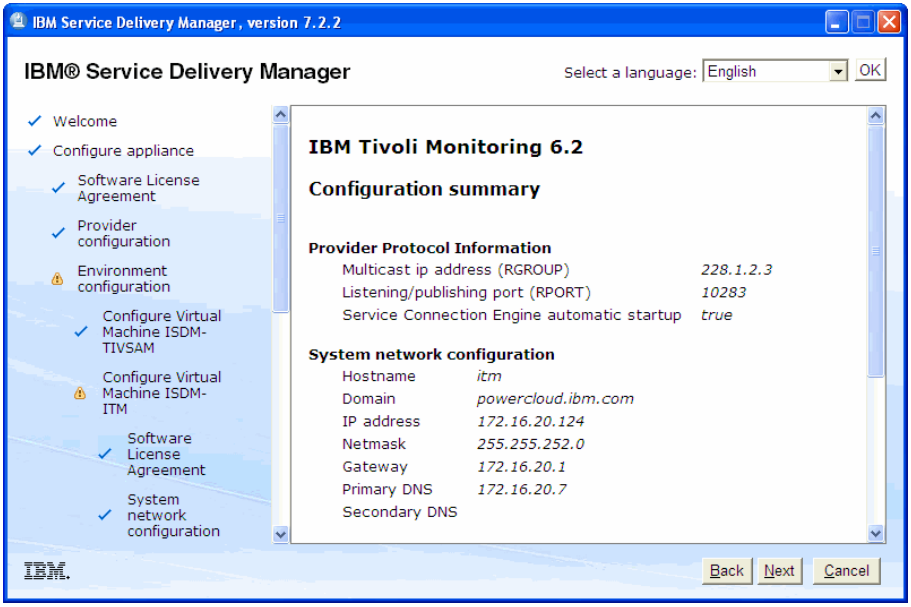

Figure 3-18 ISDM-ITM configuration summary

19. The Configure Virtual Machine ISDM-TUAM screen is displayed, as shown in Figure 3-19. It contains the hardware requirements and the software stack that is going to be installed. Click **Next** to continue.

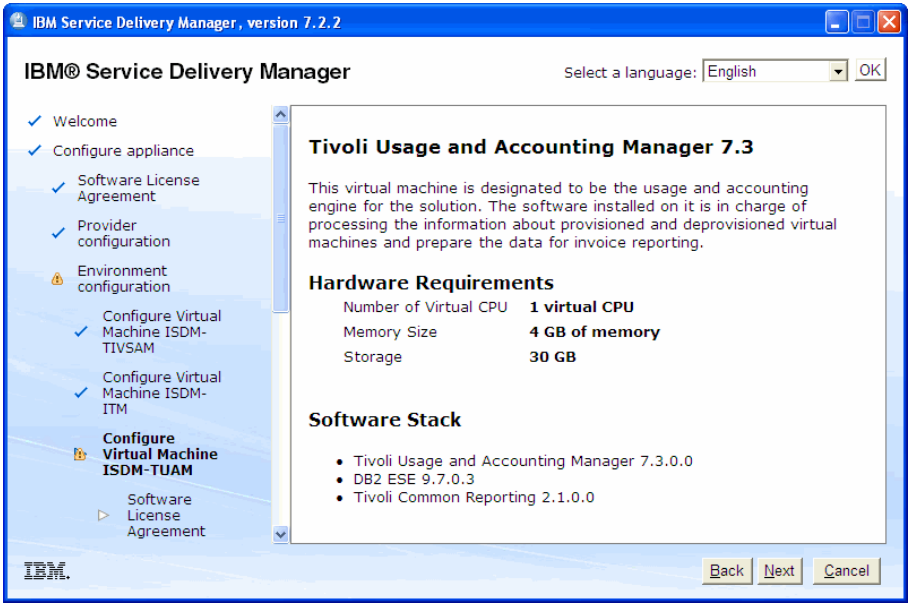

Figure 3-19 Configure virtual machine ISDM-TUAM welcome panel

20. The software license agreement for the Tivoli Usage and Accounting Manager software stack is displayed, as shown in Figure 3-20. Read the software license agreement, and then select the **I accept the terms in the license agreement** radio button. Click **Next** to continue.

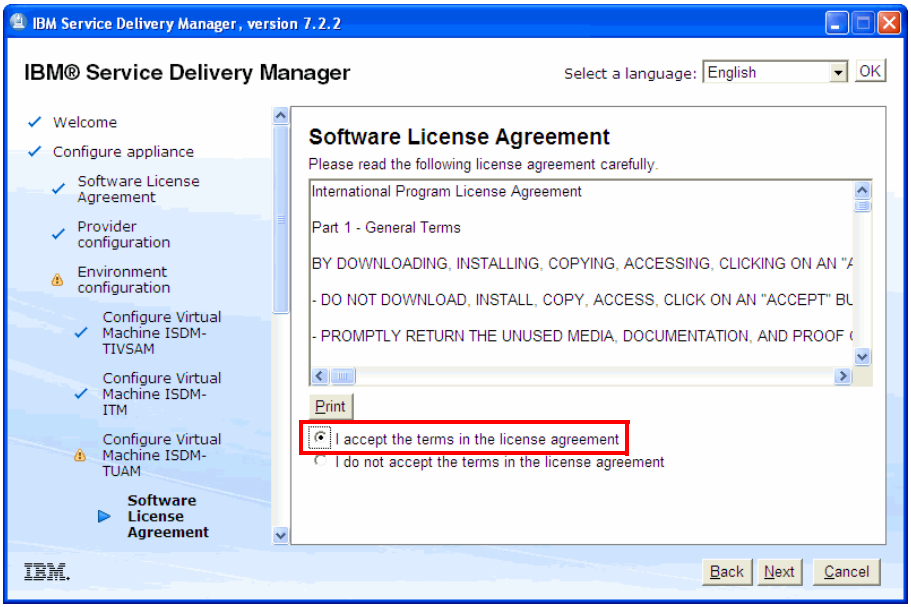

Figure 3-20 ISDM-TUAM software stack license agreement

21. The Tivoli Usage and Accounting Manager System network configuration screen is displayed, as shown Figure 3-21. Use the network details that you created earlier in Table 3-2 on page 25 to complete the mandatory questions and the primary DNS details. Click **Next** to continue.

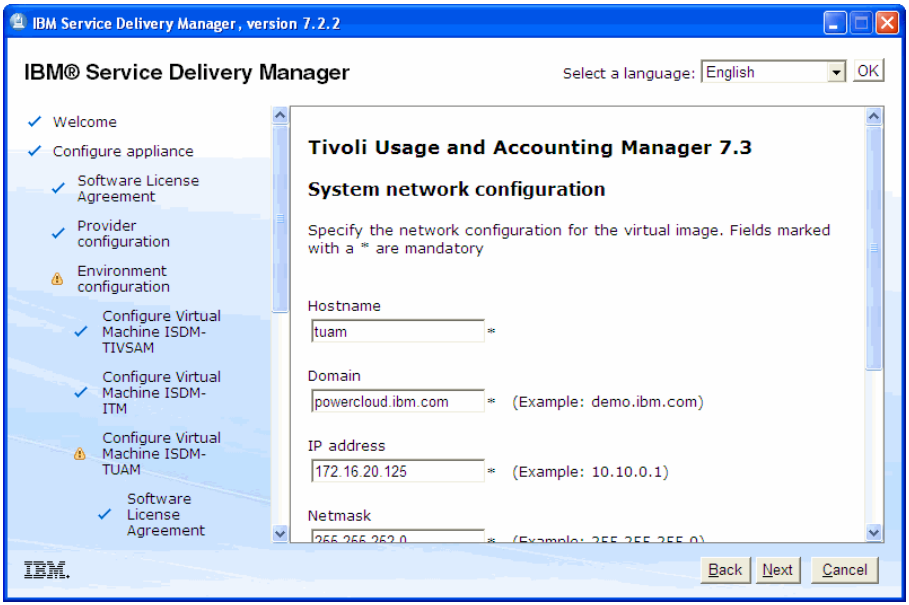

Figure 3-21 SDM-TUAM network configuration

22. The root password configuration screen is displayed, as shown Figure 3-22. Enter the `root` password for the Tivoli Usage and Accounting Manager virtual image in the password text fields. Click **Next** to continue.

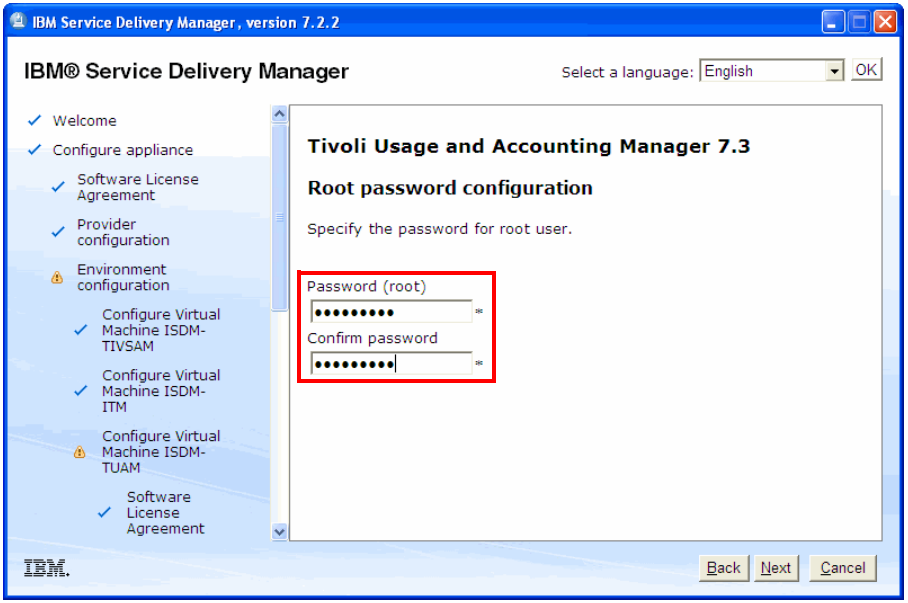

Figure 3-22 ISDM-TUAM root password configuration

23. The virtuser password configuration screen is displayed, as shown in Figure 3-23. Enter the `virtuser` password for the Tivoli Usage and Accounting Manager virtual image in the password text fields. Click **Next** to continue.

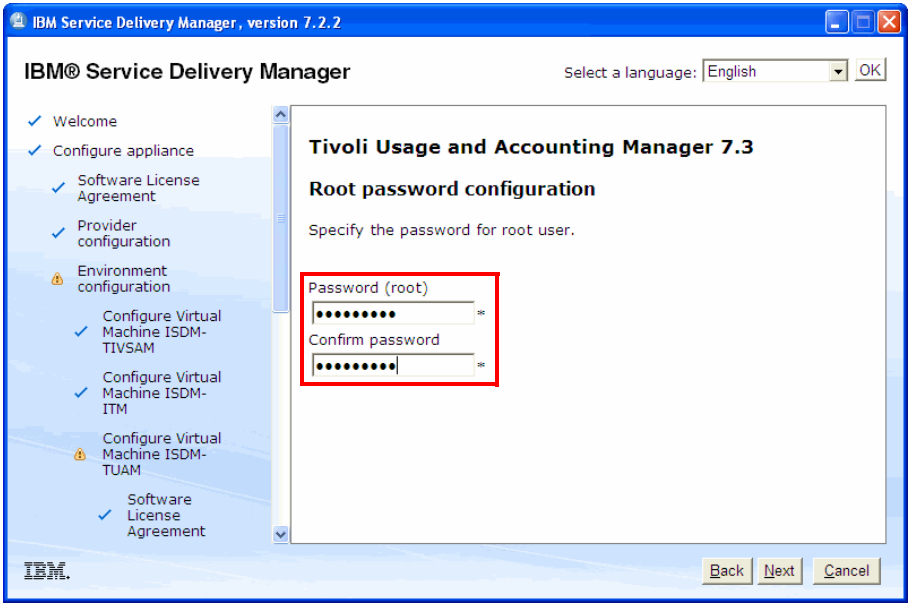

Figure 3-23 ISDM-TUAM virtuser password configuration

24. The Tivoli Usage and Accounting Manager virtual image configuration summary screen is displayed, as shown Figure 3-24. Read the summary information. If the summary information is correct, click **Next** to continue.

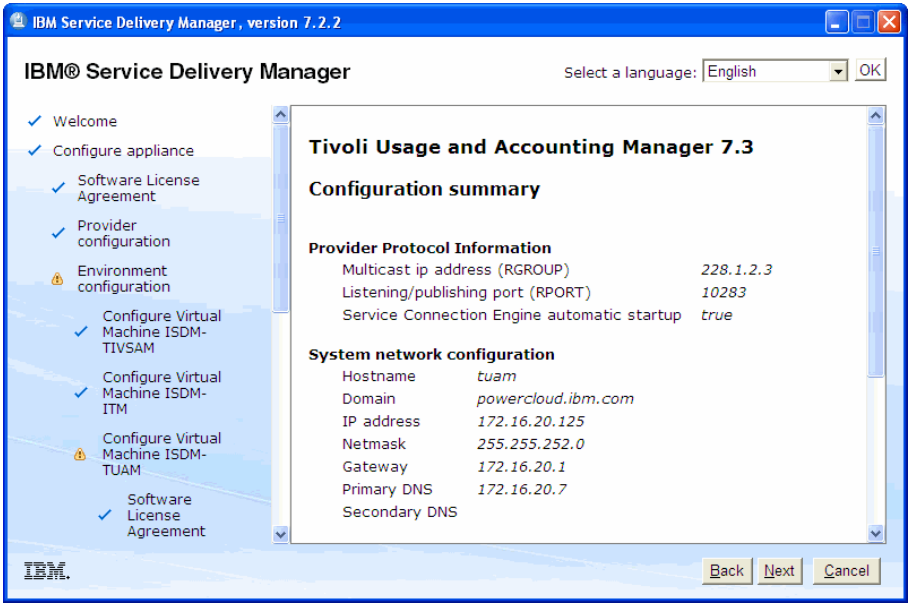

Figure 3-24 ISDM-TUAM configuration summary

25. The Configure Virtual Machine ISDM-IHS IBM HTTP Server welcome screen is displayed, as shown in Figure 3-25. This virtual image is often referred to as the NFS virtual image. It contains the hardware requirements and the software stack that is going to be installed. Click **Next** to continue.

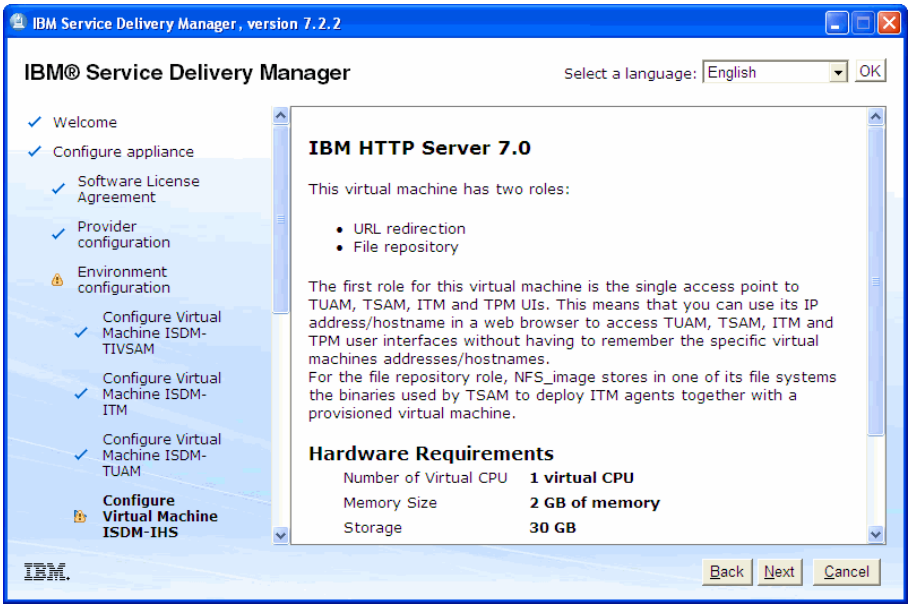

Figure 3-25 Configure virtual machine ISDM-IHS welcome panel

26. The Configure Virtual Machine IBM HTTP Server welcome screen is displayed, as shown in Figure 3-26. It contains the hardware requirements and the software stack that is going to be installed. Click **Next** to continue.

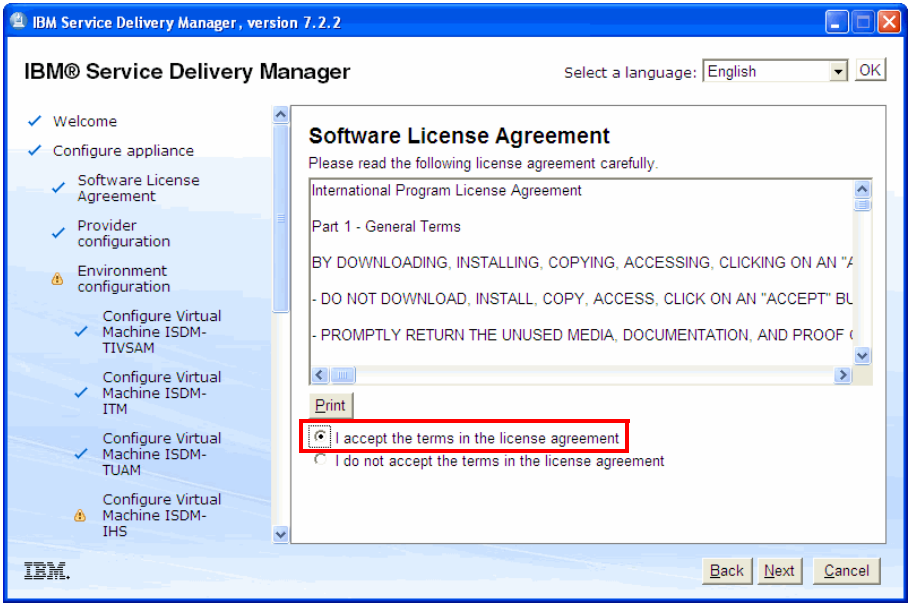

Figure 3-26 ISDM-IHS software stack license agreement

27. The IBM HTTP Server System network configuration screen is displayed, as shown Figure 3-27. Use the network details that you created earlier in Table 3-2 on page 25 to complete the mandatory questions and the primary DNS details. Click **Next** to continue.

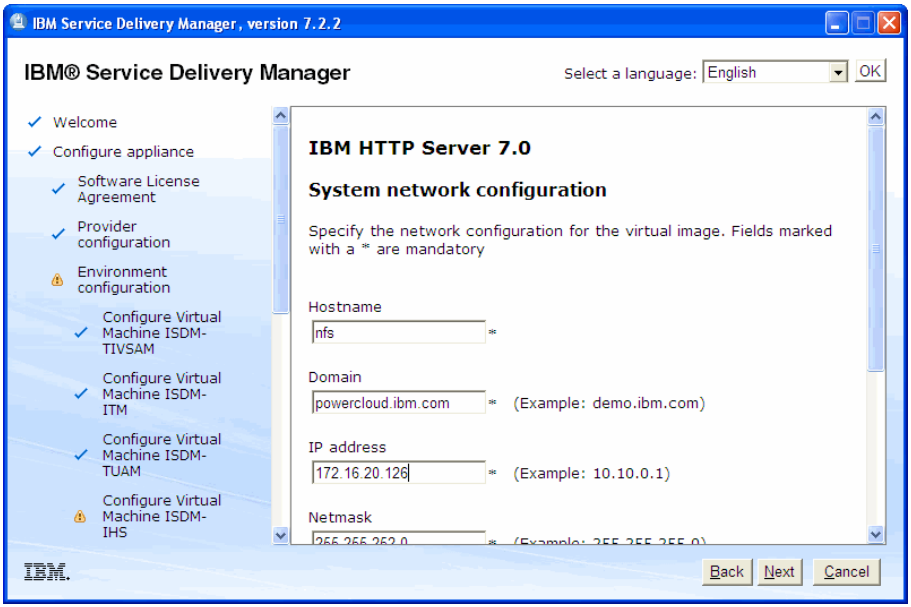

Figure 3-27 ISDM-IHS network configuration

28. The Root password configuration screen is displayed, as shown Figure 3-28. Enter the `root` password for the IBM HTTP Server virtual image in the password text fields. Click **Next** to continue.

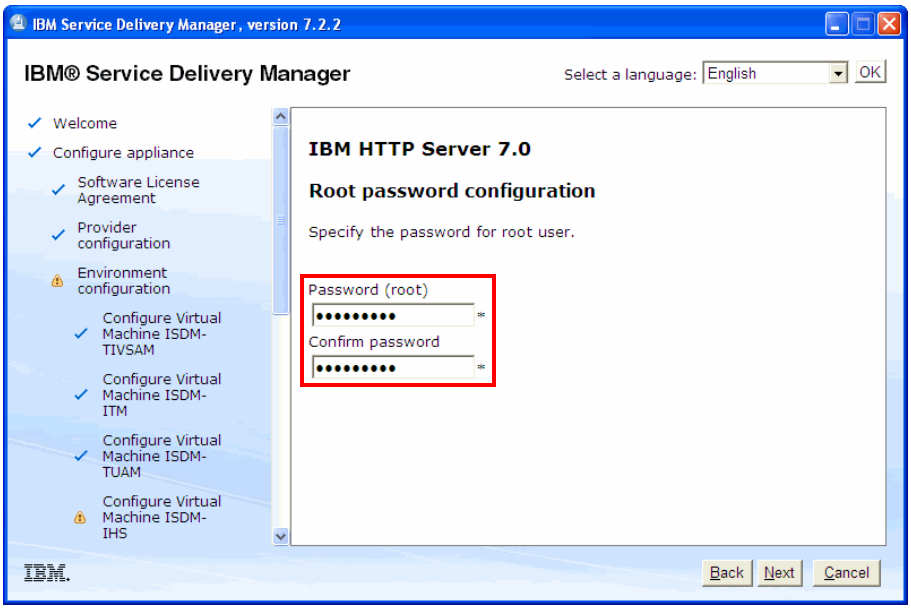

Figure 3-28 ISDM-IHS root password configuration

29. The Virtuser password configuration screen is displayed, as shown in Figure 3-29. Enter the `virtuser` password for the IBM HTTP Server virtual image in the password text fields. Click **Next** to continue.

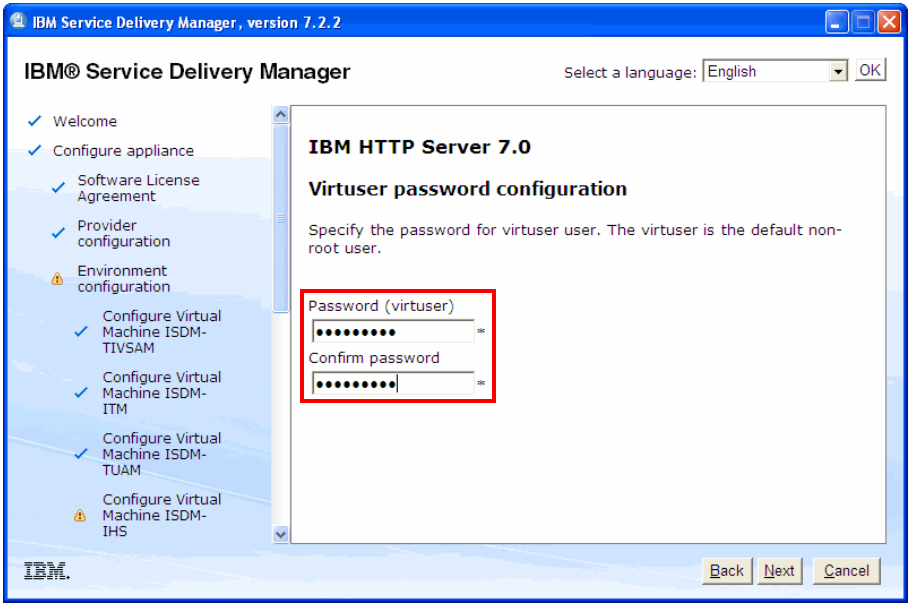

Figure 3-29 ISDM-IHS virtuser password configuration

30. The IBM HTTP Server virtual image configuration summary screen is displayed, as shown Figure 3-30. Read the summary information. If the summary information is correct, click **Next** to continue.

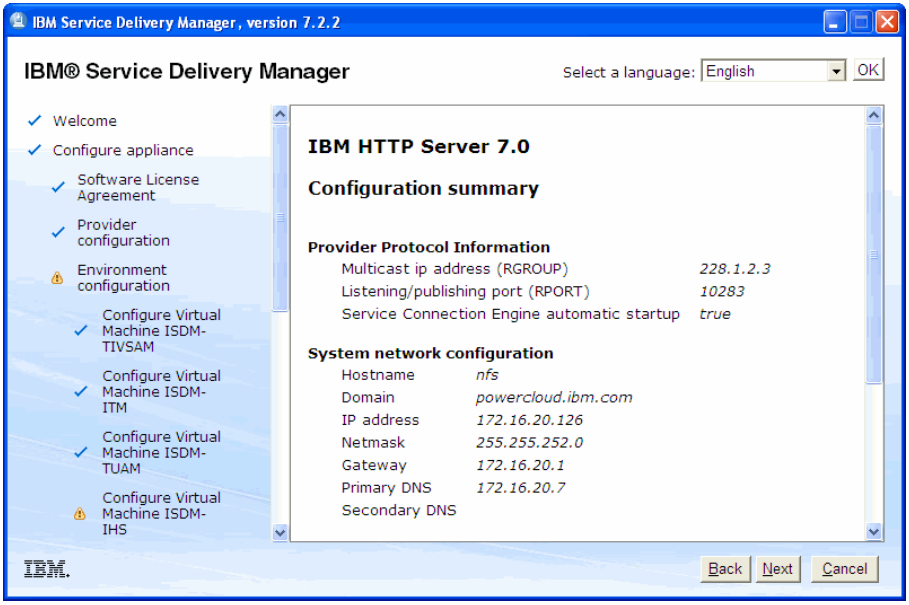

Figure 3-30 ISDM-IHS configuration summary

31. The Environment configuration summary screen is displayed, as shown in Figure 3-31. The environment configuration summary lists the file location of the OVF files on your local windows computer. Write down the location of the files for future reference. Click **Save and Continue** to continue.

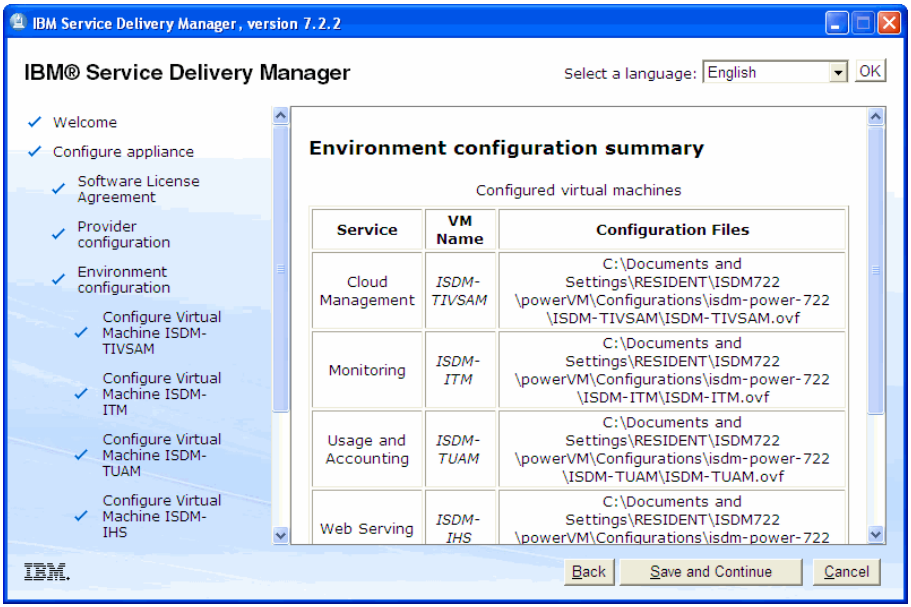

Figure 3-31 Environment configuration summary

32. The launchpad application saves the files to your local machine and displays a screen displaying the save progress for each OVF file, as seen in Figure 3-32.

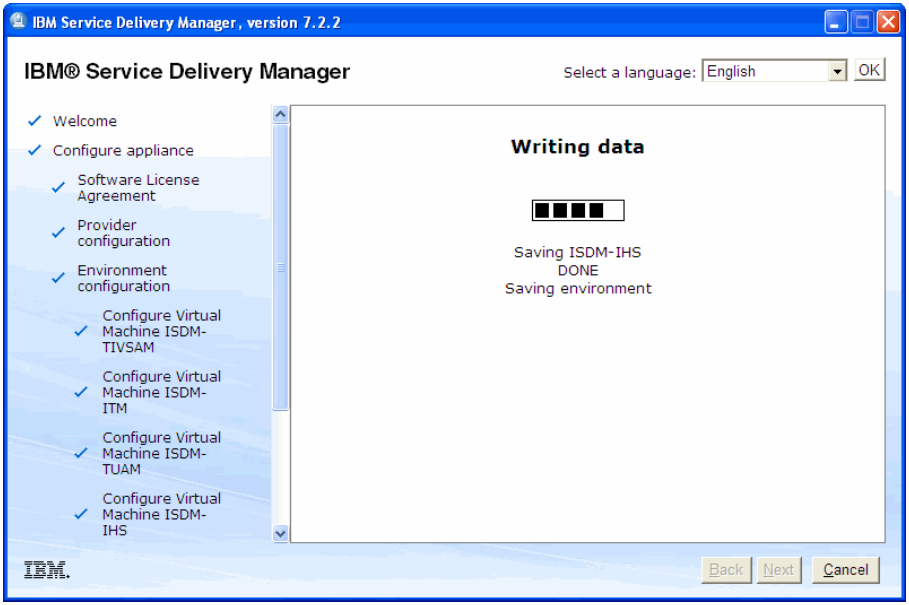

Figure 3-32 OVF saving progress window

33. The Deploy appliance screen is displayed, as shown in Figure 3-33. The Deploy appliance screen contains instructions for how to deploy the appliance in the PowerVM environment. Deploying an appliance is covered in the next chapter. Continue to click **Next** until the launchpad application closes, as seen in Figure 3-34 on page 62, Figure 3-35 on page 62, and Figure 3-36 on page 63.

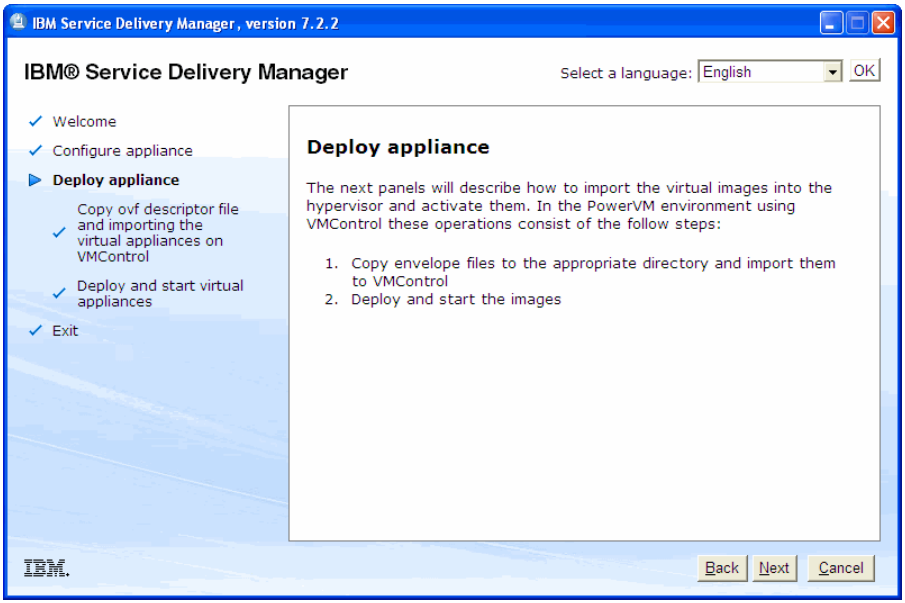

Figure 3-33 Instructions to deploy an appliance

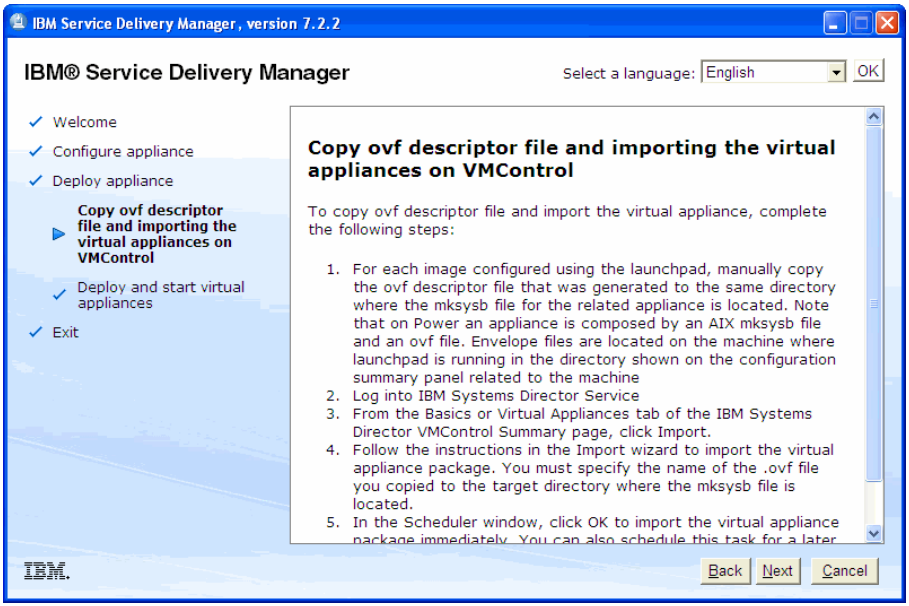

Figure 3-34 Copy the descriptor file and import the virtual image

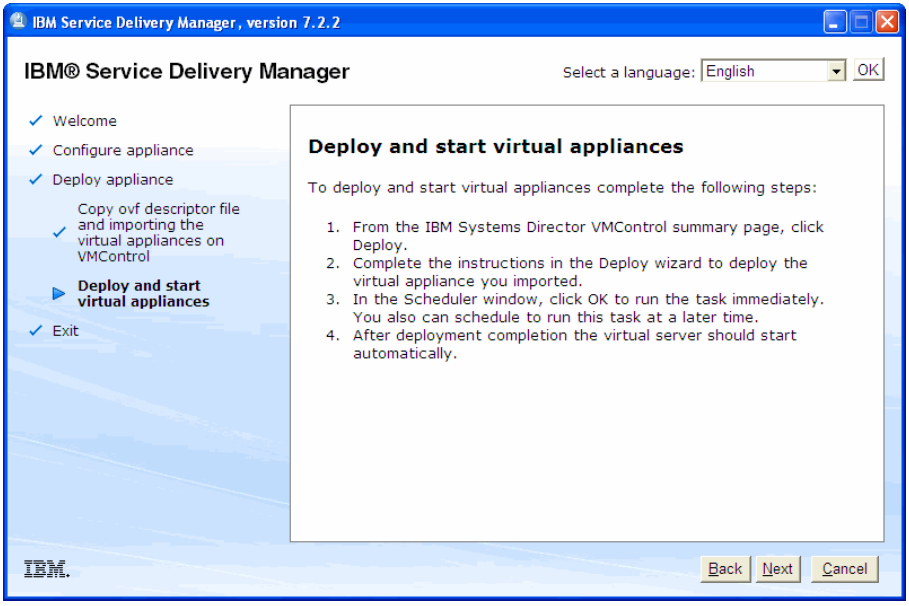

Figure 3-35 Deploy and start the virtual image

Figure 3-36 Quit the launchpad tool

Note: Although the above instructions were carried out on Windows, the AIX launchpad launcher uses exactly the same process.

3.2.3 Placing the virtual images on the IBM Director VMControl host

To complete the preparation of the virtual images, they need to be moved to the IBM Systems Director VMControl host. Using IBM Systems Director VMControl, the virtual images can then be imported and deployed to an IBM Power Systems server.

To import the virtual image successfully, the virtual image and the OVF file must be copied into the same directory on the IBM Systems Director VMControl server.

An example of the output can be seen in Example 3-4.

Example 3-4 Example of file listing of ISDM-related directories after the OVF and virtual image have been copied to the ISD VMControl host

```
# ls ./ISDM-TIVSAM
ISDM-TIVSAM.ovf     isdmtivsam.mksysb
# ls ./ISDM-ITM
ISDM-ITM.ovf     isdmitm.mksysb
# ls ./ISDM-TUAM
ISDM-TUAM.ovf     isdmtuam.mksysb
# ls ./ISDM-IHS
ISDM-IHS.ovf     isdmnfs.mksysb
```

4

ISDM installation

In the previous chapter, we prepared IBM Service Delivery Manager OVF files. In this chapter we describe the steps that we took to deploy IBM Service Delivery Manager OVF files on the Power Systems Management system and to configure and verify the ISDM software stack. The steps required the use of IBM System Director VMControl and AIX Network Installation Manager (NIM).

For detailed installation and configuration steps, see *IBM Systems Director VMControl Implementation Guide on IBM Power Systems*, SG24-7829*:*

http://www.redbooks.ibm.com/abstracts/sg247829.html

For details of an NIM setup in an AIX environment, see *NIM from A to Z in AIX 5L*, SG24-7296:

http://www.redbooks.ibm.com/abstracts/sg247296.html

4.1 Deploying ISDM server images using VMControl

In preparation for deploying an ISDM virtual image using VMControl, we completed the following tasks:

1. We configured NIM LPAR and tested NIM functionality by manually creating a regular LPAR through HMC, and we performed AIX operating system installation.
2. We configured Director LPAR, IBM Systems Director, and IBM Systems Director VMControl Enterprise Edition software.
3. SMI-S providers were configured to connect and manage SAN Switches and Storage.
4. IBM System Director ran a successful discovery, NIM Sub Agent was installed, switch and storage were discovered by IBM System Director through SMI-S.
5. In our configuration, we configured DS4500. A RAID Group was created and discovered by IBM System Director.
6. SAN switches were configured and discovered by IBM System Director.
7. Creating storage system pools is an optional step, and in our configuration we did not create one.
8. Server system pools were created in IBM System Director.
9. We identified Managed To and Managed From Hypervisor frames.
10. We reviewed the software and hardware requirements section of this publication.

4.1.1 OVF packages

All the OVF and `mksysb` files generated by the IBM Service Delivery Manager launchpad should be accessible from the Systems Director VMControl. You can copy these files to a local file system or an NFS mounted file system. Example 4-1 shows our directory structure.

Example 4-1 Directory structure

```
# cd /mnt/repository/OVF_packages
# ls -Rlrt
total 0
drwxr-xr-x    2 root     system          256 Oct 12 19:38 ISDM-TUAM
drwxr-xr-x    2 root     system          256 Oct 12 19:38 ISDM-TIVSAM
drwxr-xr-x    2 root     system          256 Oct 13 11:21 ISDM-NFS
drwxr-xr-x    2 root     system          256 Oct 13 11:24 ISDM-ITM
./ISDM-TUAM:
```

```
total 27379440
-rwxr--r--    1 root     system   14018252800 Sep  1 12:32 isdmtuam.mksysb
-rw-r-----    1 root     system        13768 Oct 12 19:38 ISDM-TUAM.ovf

./ISDM-TIVSAM:
total 67106344
-rwxr--r--    1 root     system   34358425600 Sep  1 05:45 isdmtivsam.mksysb
-rw-r-----    1 root     system        13784 Oct 12 19:38 ISDM-TIVSAM.ovf

./ISDM-NFS:
total 15457440
-rwxr--r--    1 root     system   7914188800 Sep  1 08:17 isdmnfs.mksysb
-rwxrwxrwx    1 root     system        13752 Oct 12 17:20 ISDM-IHS.ovf

./ISDM-ITM:
total 20300544
-rwxr--r--    1 root     system   10393856000 Sep  1 08:10 isdmitm.mksysb
-rw-r-----    1 root     system        13755 Oct 12 18:49 ISDM-ITM.ovf
```

An OVF file contains information about its associated `mksysb` file and other components that make up the OVF package.

4.1.2 Importing ISDM images in VMControl

You can deploy the OVF packages from the previous section. The packages are:

- NFS
- ITM
- TUAM
- TivSAM

Here we demonstrate the steps for deploying the NFS package. The other three packages can be deployed in the same way.

1. Log in to the IBM Systems Director as the administrator user:

   `https://172.16.20.129:8422/ibm/console/login.do?action=secure`

   Note: The IP address shown is your Director host URL port 8244.

   From the Systems Director Console in the navigate menu on the left side, expand the **System Configuration** menu and click **VMControl** to open the VMControl Enterprise Edition panel (Figure 4-1).

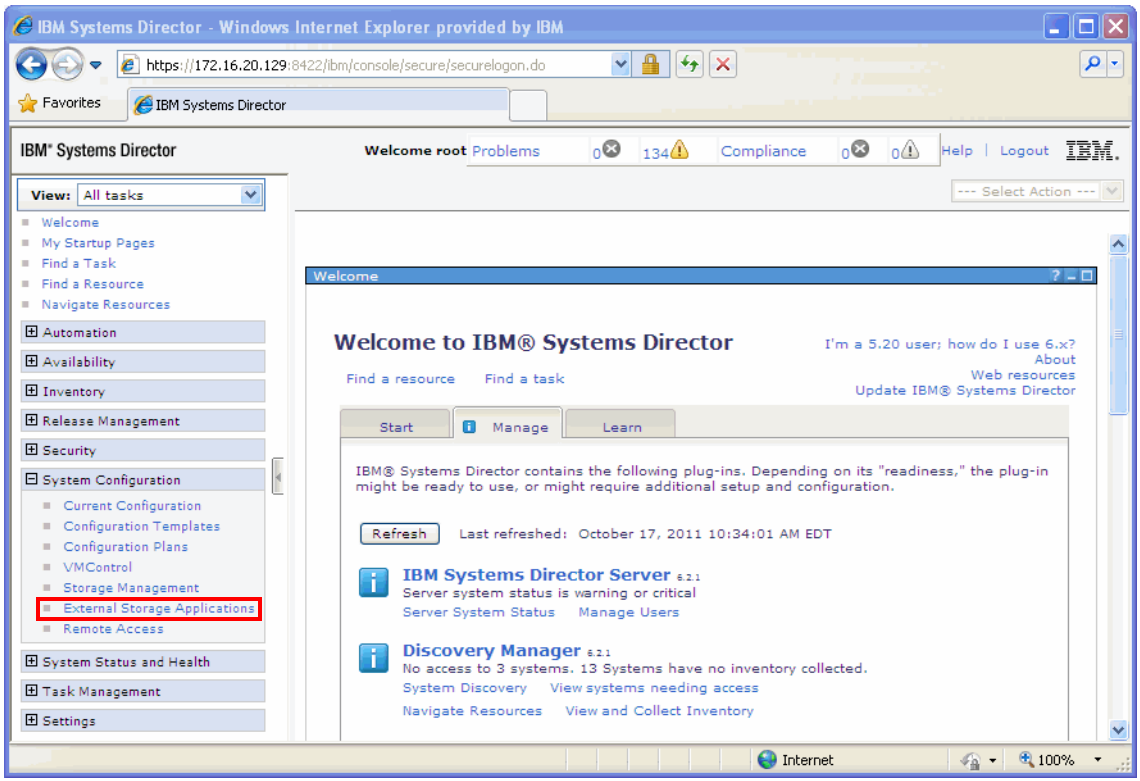

Figure 4-1 Open Systems Director VMControl

2. In the Basics tab, select **Import** under Virtualization Tasks, as shown in Figure 4-2.

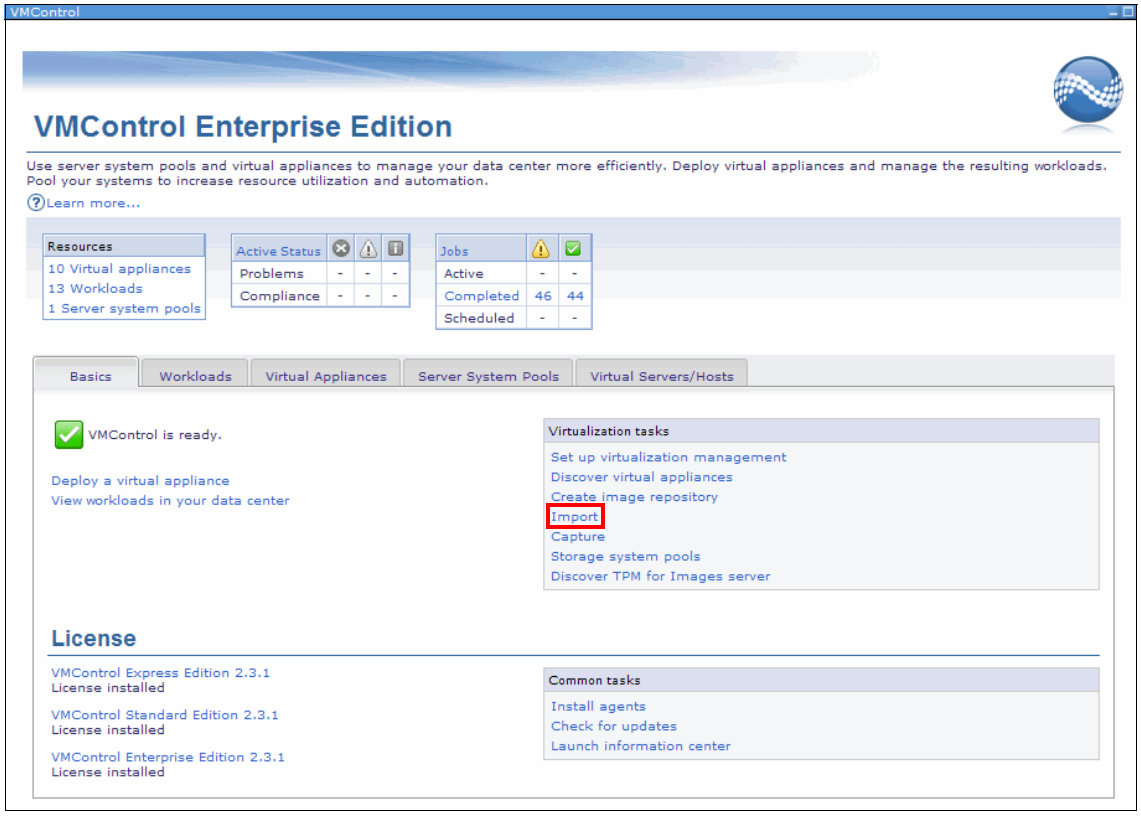

Figure 4-2 Selecting Import from Virtualization tasks

3. On the Import wizard Welcome panel, click **Next**, as in Figure 4-3.

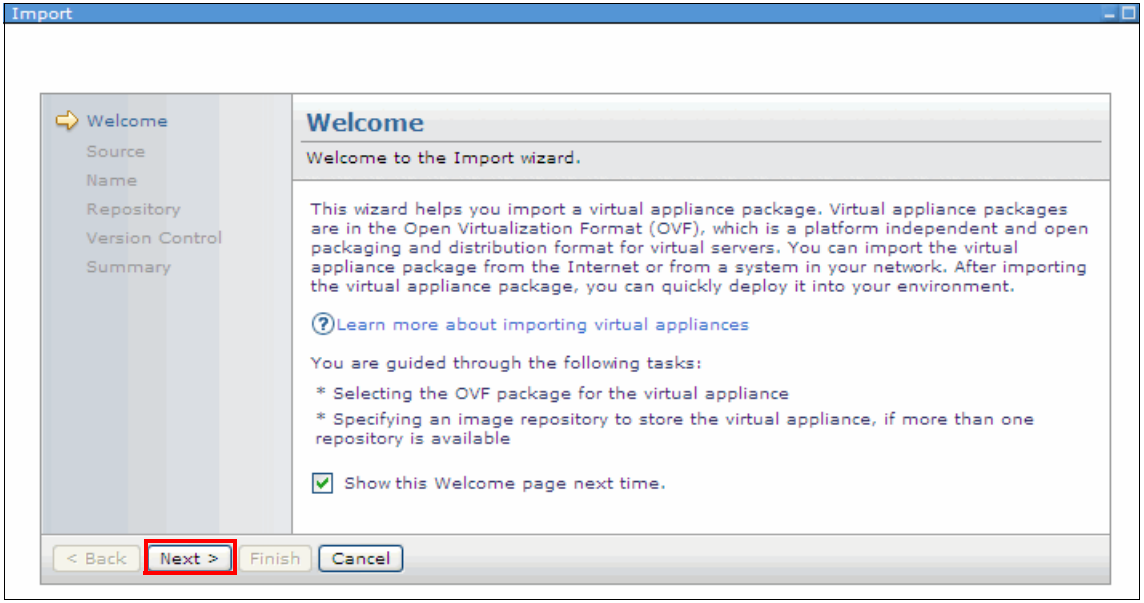

Figure 4-3 Import wizard Welcome panel

4. In the Source panel, enter the location of the OVF package, and then click **Next**, as in Figure 4-4.

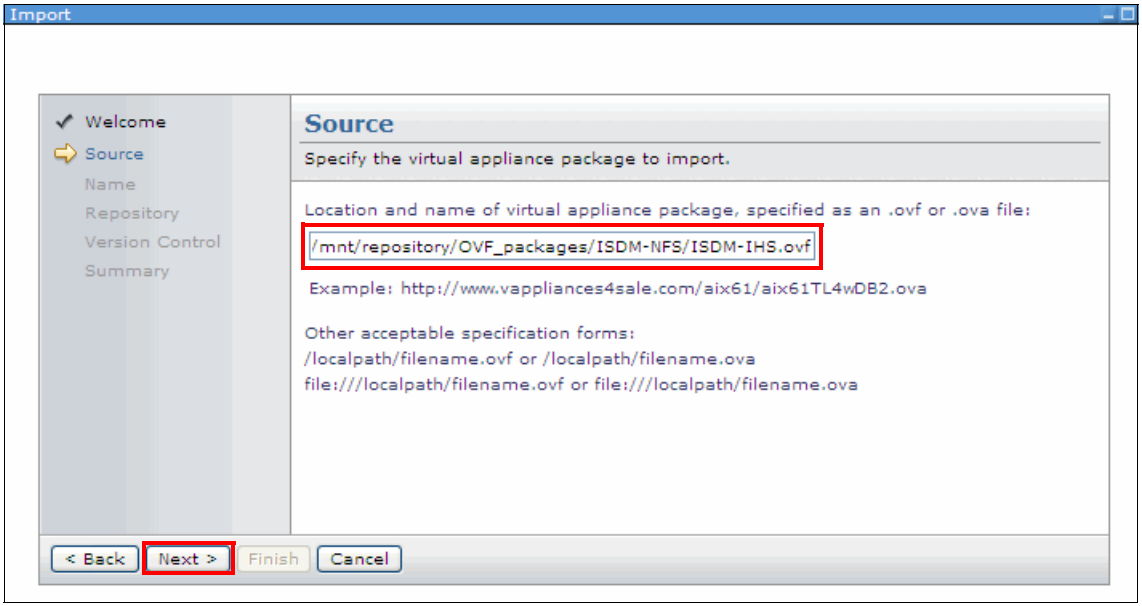

Figure 4-4 Entering OVF package location

5. In the Digital Signature panel, leave the check for Import without digital signature as the default. Click **Next**, as in Figure 4-5.

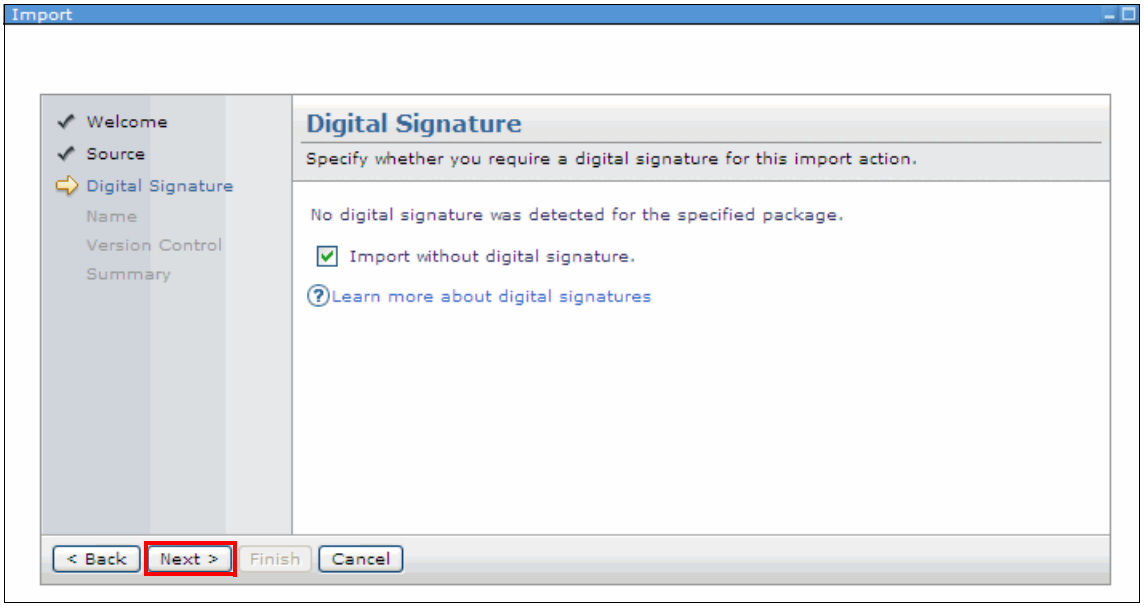

Figure 4-5 Digital Signature

6. In the Name panel, keep the text as is and click **Next**, as in Figure 4-6.

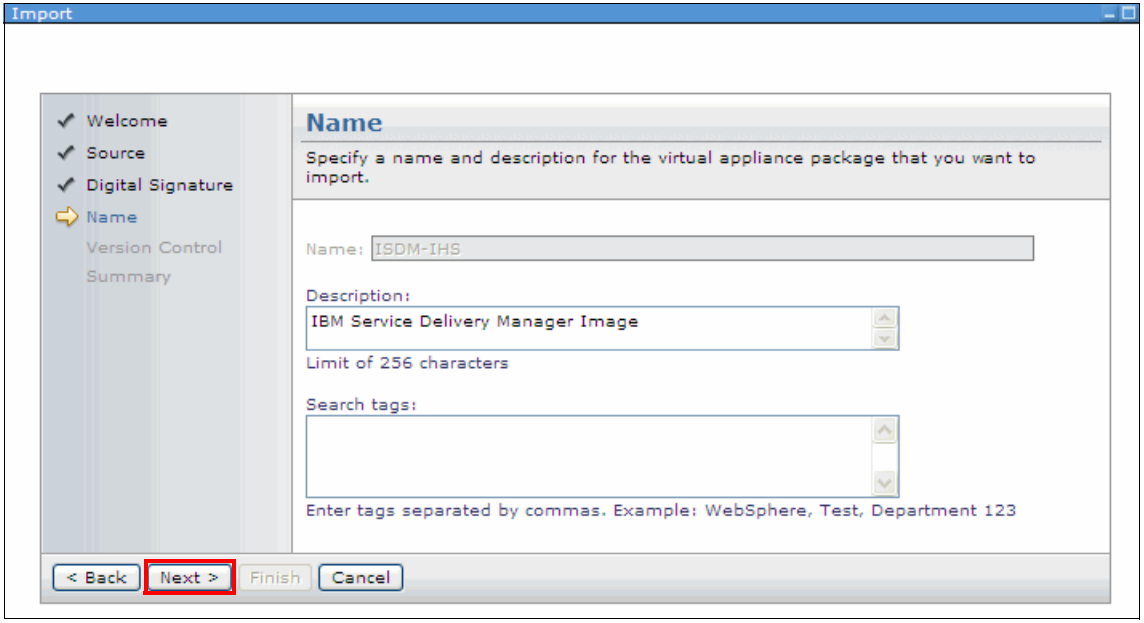

Figure 4-6 Specifying a name and descriptor

7. In the Version Control panel, select **Create a new version tree with the new virtual appliance as root** and click **Next**, as in Figure 4-7.

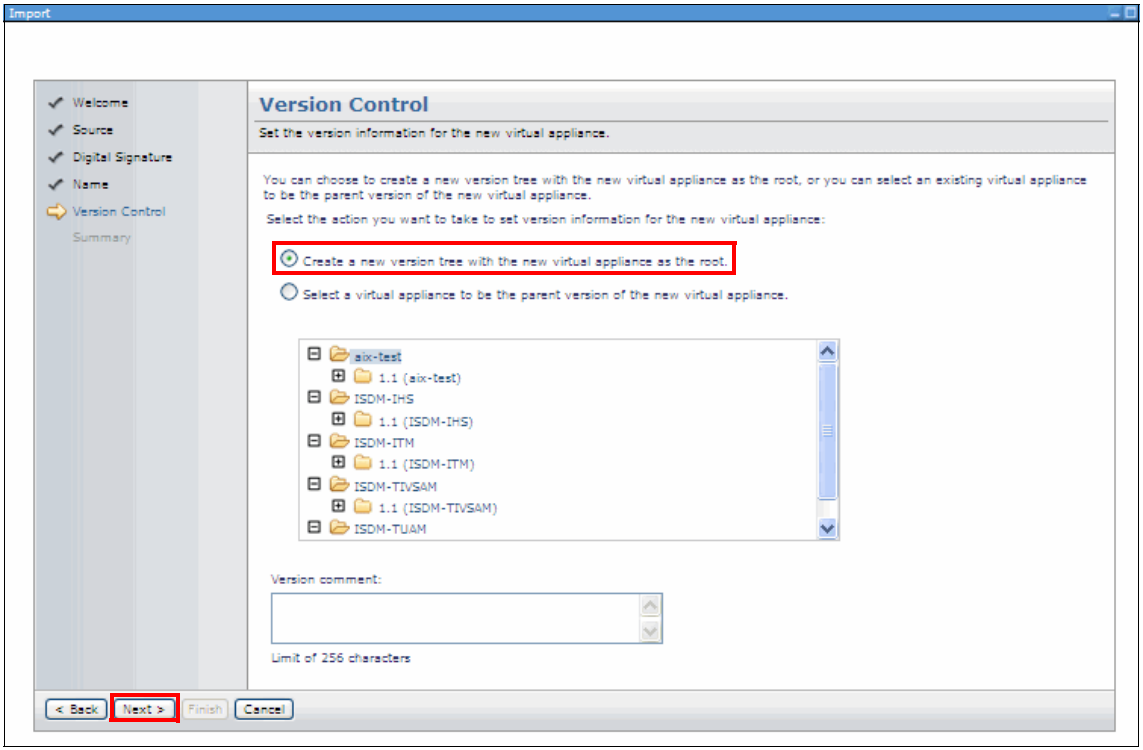

Figure 4-7 Selecting a new version tree

8. In the Summary panel, click **Finish**, as in Figure 4-8.

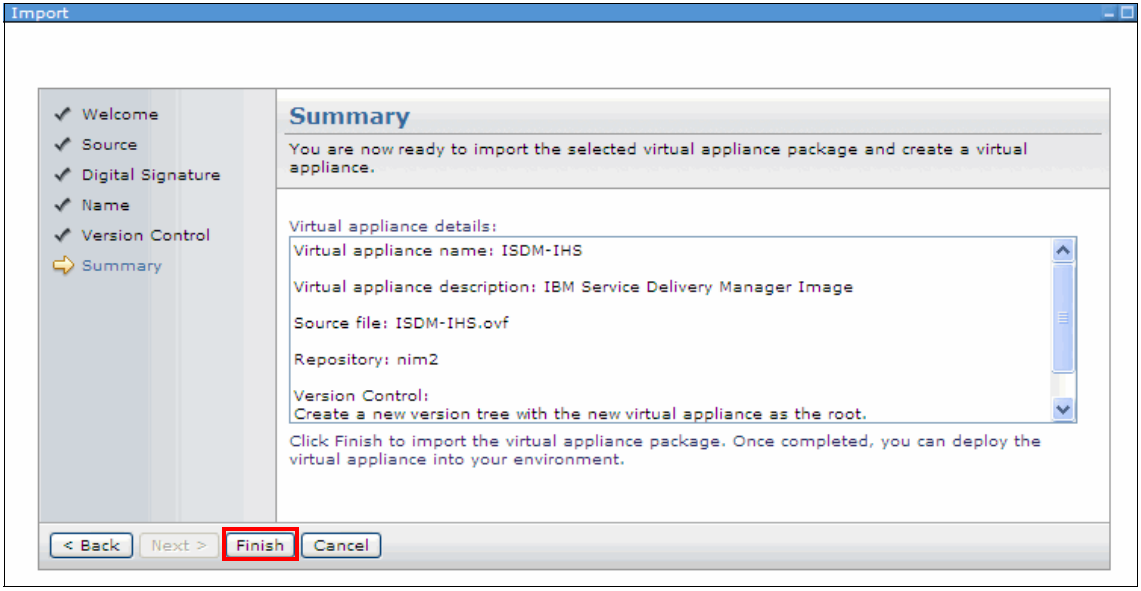

Figure 4-8 Summary for the import virtualization task

9. In the Task Launch Dialog, under the Schedule tab, a job is going to be created. Select **Run Now** and click **OK**, as in Figure 4-9.

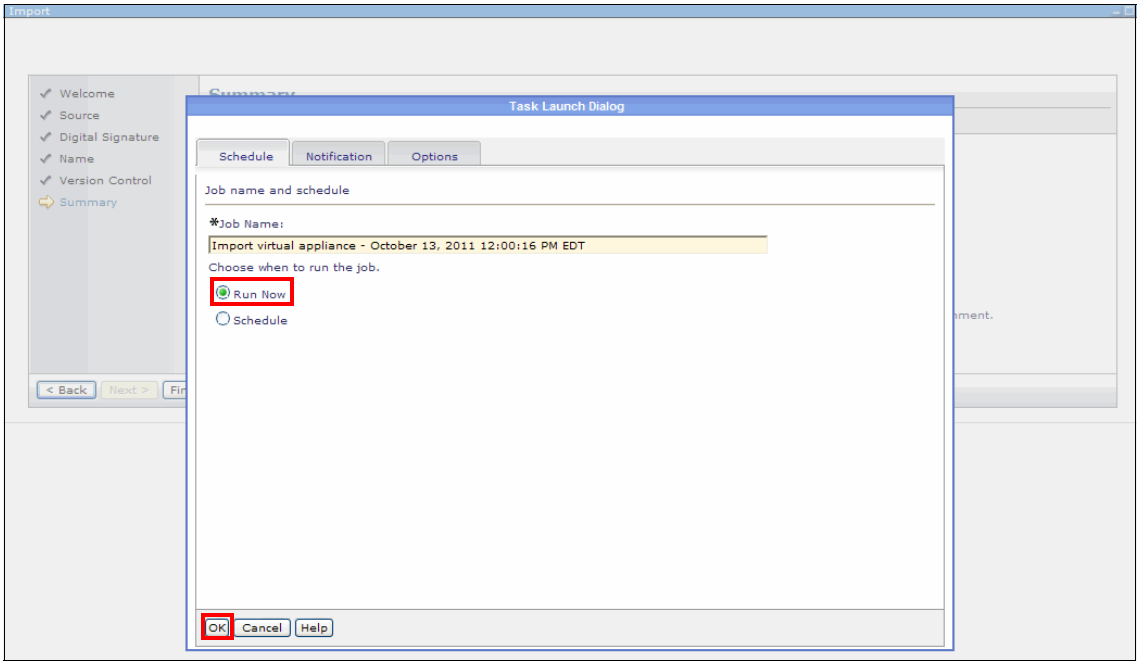

Figure 4-9 Submitting a job to import the OVF package

10. Import the ITM, TUAM, and TivSAM appliances by repeating steps 1 - 9 with the respective OVF packages.

4.1.3 Deploying A Virtual Appliance using VMControl

1. Log in to the IBM Systems Director portal:

   `https://172.16.20.129:8422/ibm/console/login.do?action=secure`

   In the navigation menus on the left side, expand the **System Configuration** menu, and then click **VMControl**.

2. Under the Basics tab, select **Deploy a virtual appliance**, as in Figure 4-10.

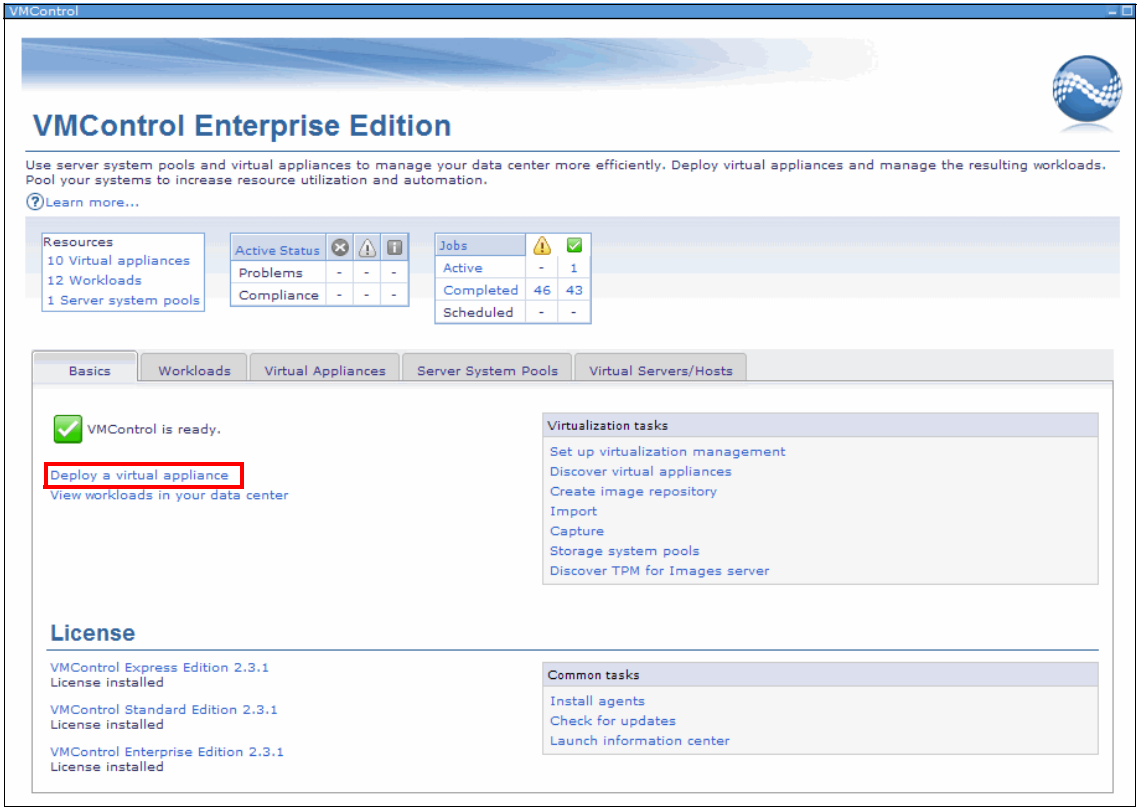

Figure 4-10 Deploying a virtual appliance

3. On the Deploy Virtual Appliance Welcome panel, click **Next**, as in Figure 4-11.

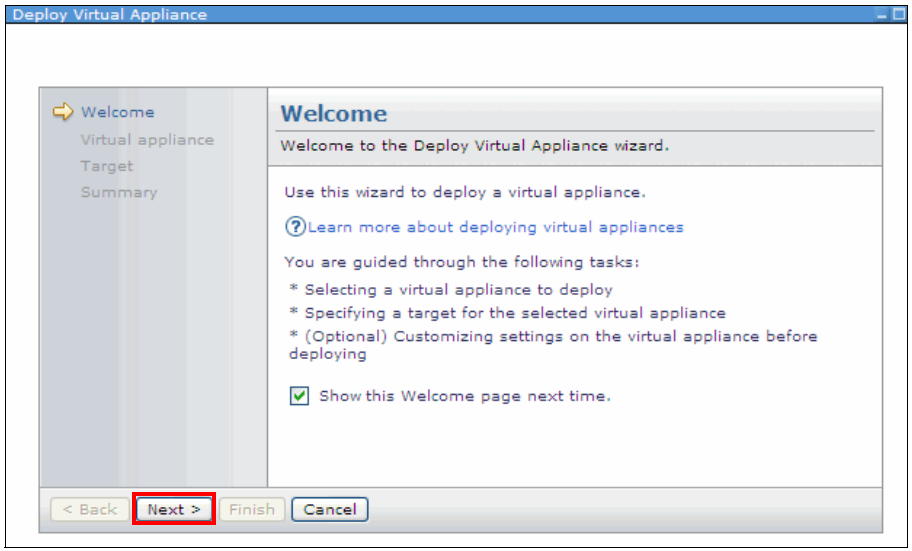

Figure 4-11 Deploy Virtual Appliance Welcome panel

4. On the Virtual Appliance panel, select the **ISDM-IHS** virtual appliance from the list and then click **Next**, as in Figure 4-12.

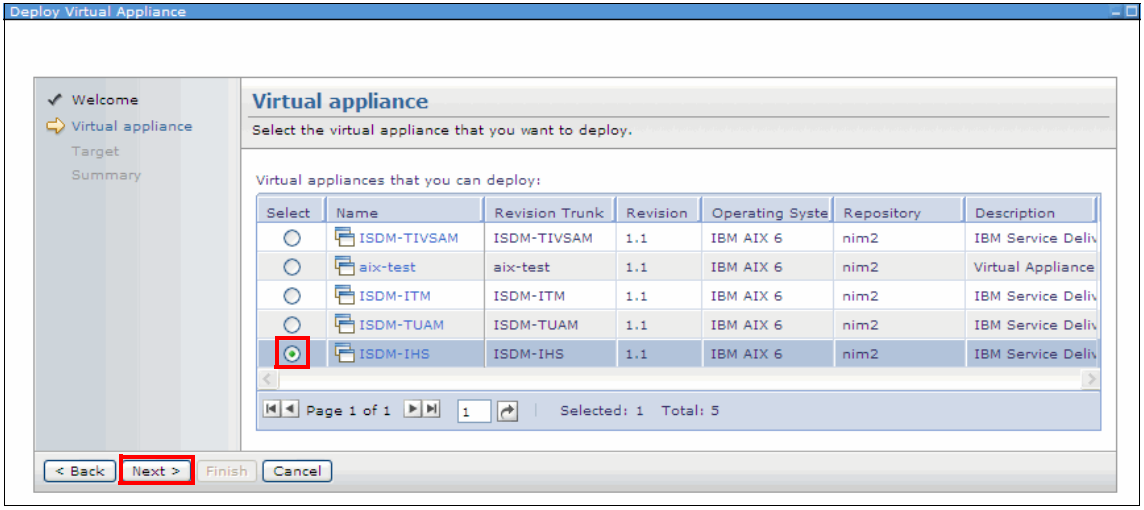

Figure 4-12 Selecting a virtual appliance from the list

5. On the Target panel, select **Deploy to a new virtual server on the following** and the target server frame from the list, and then click **Next**, as in Figure 4-13.

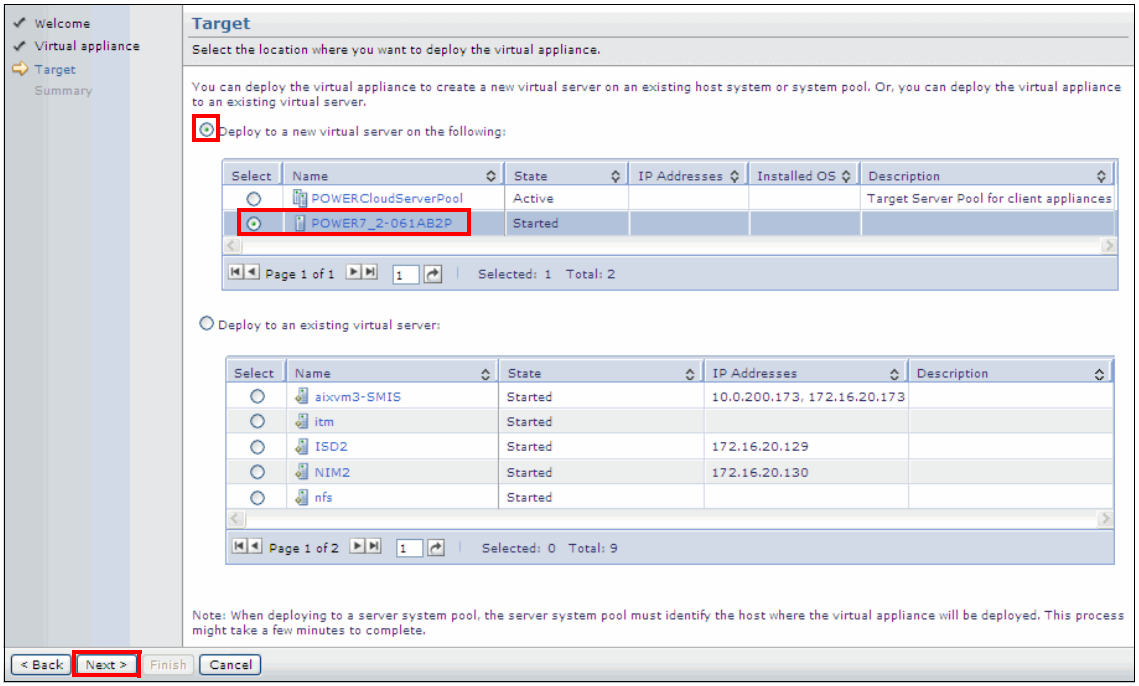

Figure 4-13 Selecting the server frame for deploying a new virtual appliance

6. On the Storage Mapping panel, select **vimRef1disk** from the list, then click **Assign to Storage Pool** if you want to use pool storage, or select **Assign to Storage Volume** if you want to use a specific device. See Figure 4-14.

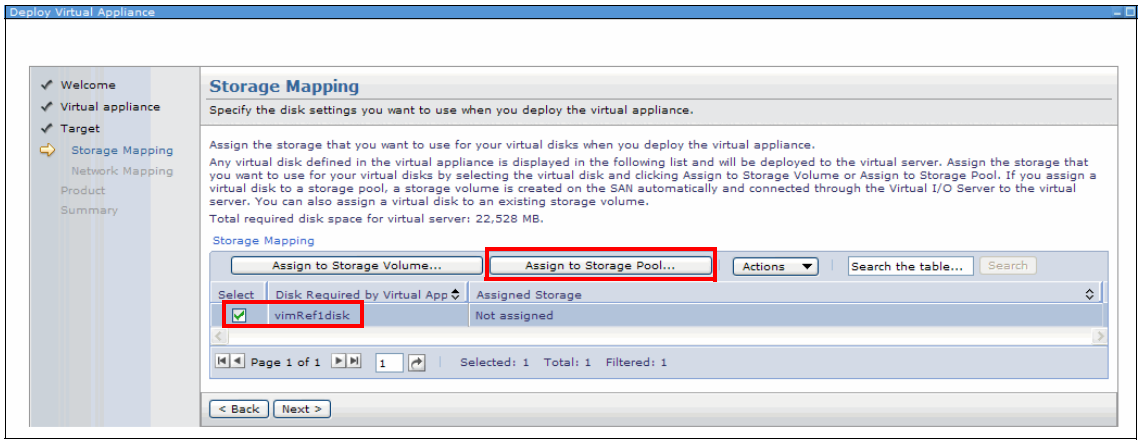

Figure 4-14 Mapping the new virtual appliance to storage

7. In the Assign to Storage Pool dialog, select the SAN Storage pool previously discovered, and then click **OK**, as in Figure 4-15. Back in the Storage Mapping panel, click **Next**.

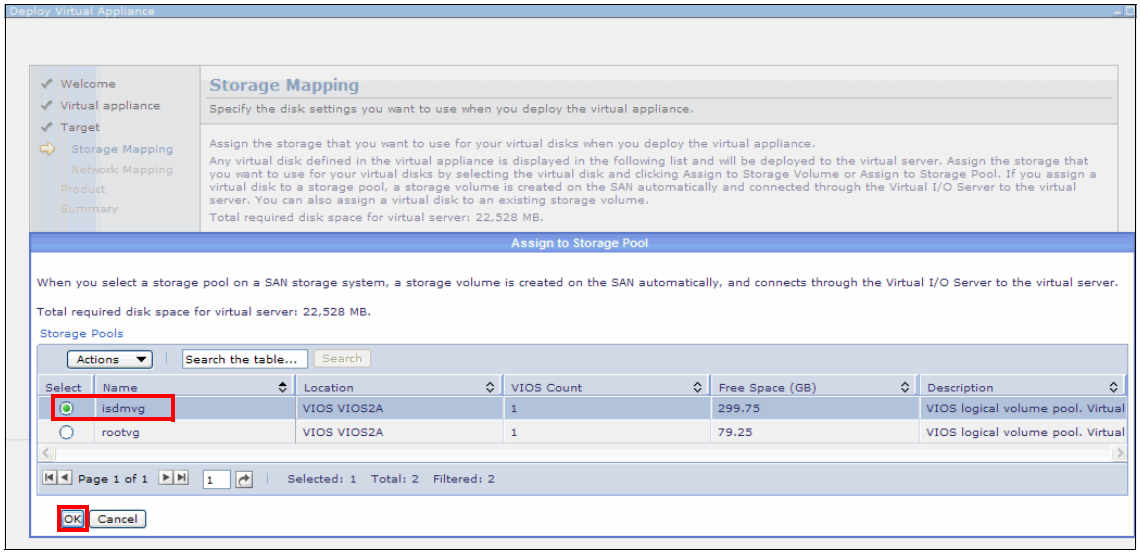

Figure 4-15 Assigning the new virtual appliance to a storage pool

8. On the Network Mapping panel, select the appropriate bridged virtual network and then click **Next**. In our example, we selected **VLAN 1 Bridged**, as in Figure 4-16.

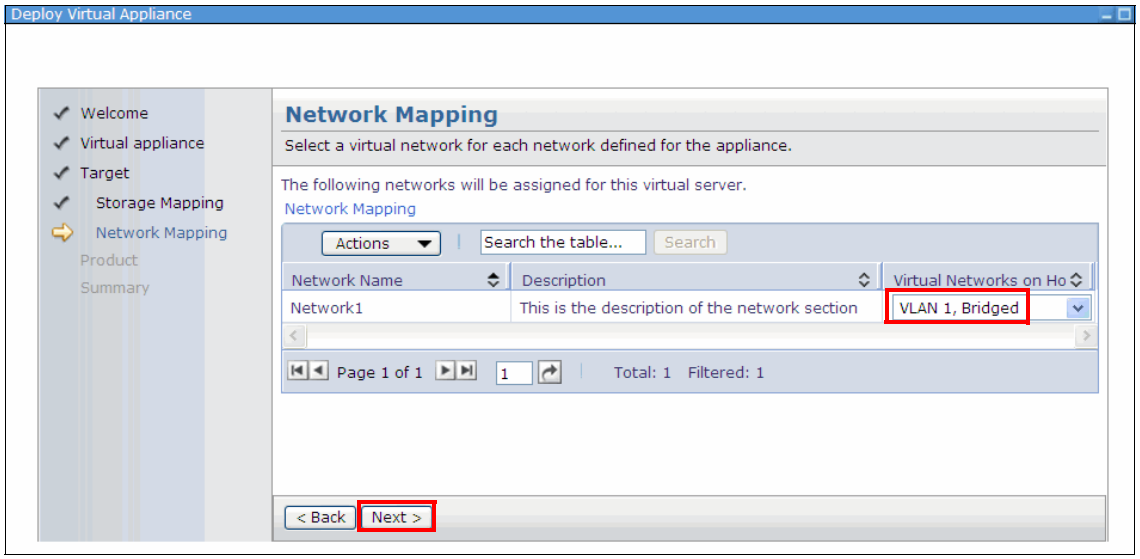

Figure 4-16 Mapping a Virtual Network to the virtual appliance

9. In the Product Summary panel, review the following settings:
   - System Network Configuration and NIM Configuration
   - License Acceptance
   - Default Locale Configuration
   - Root Password Configuration
   - User Password Configuration, WeSphere Application Server Hypervisor Edition Configuration, and Service Connection Engine Configuration

   If you need to make a correction, click **Back** until you reach the panel containing the wrong information. Make changes as described in the previous steps. When in this Product Summary panel again with all the correct information, click **Next**.

10. The final Summary panel shows the Deployment details:
    - Virtual appliance to deploy
    - Target server
    - Storage Mapping
    - Networks

Again, review the summarized information and click **Finish**, as in Figure 4-17, to set up the deployment schedule.

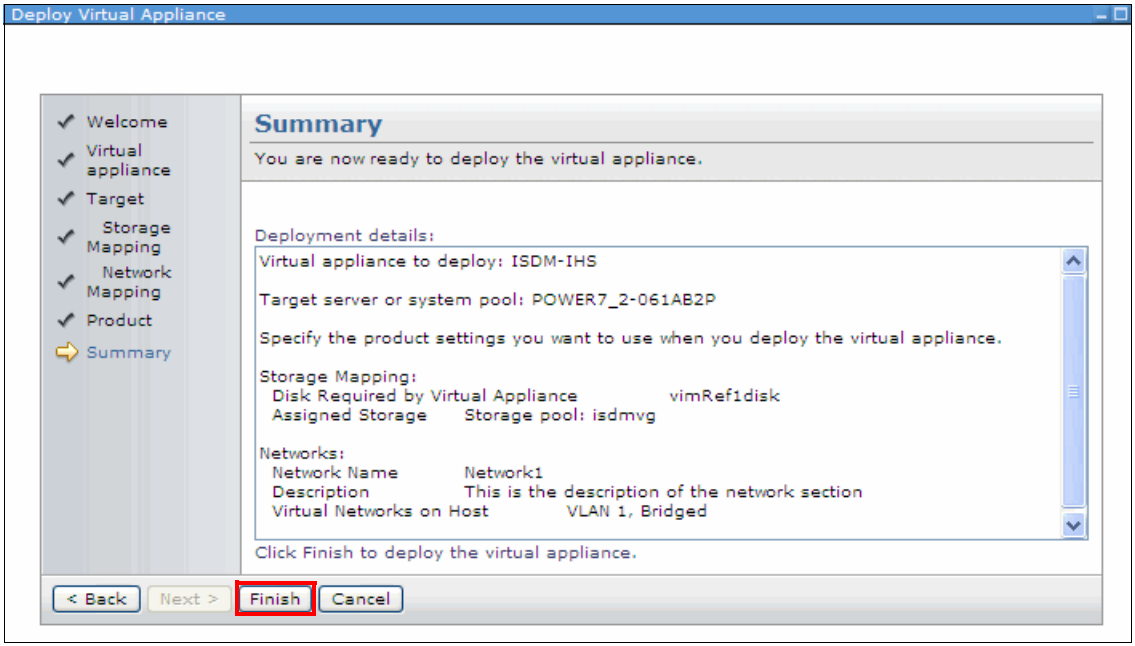

Figure 4-17 Deploy virtual appliance final summary

11. In the Task Launch Dialog, under the Schedule tab, select **Run Now** and click **OK**, as in Figure 4-18.

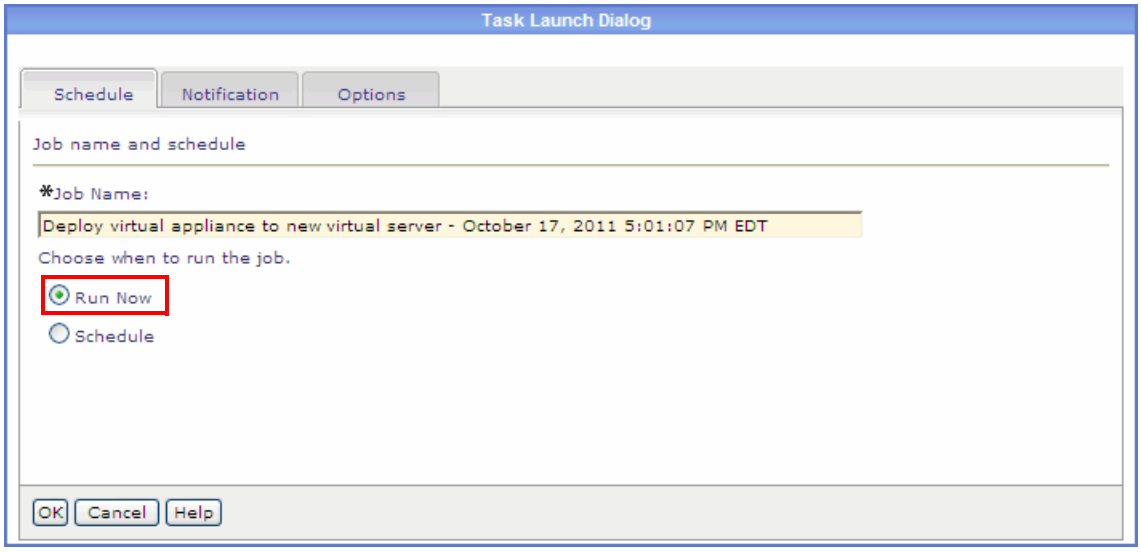

Figure 4-18 Running the virtual appliance deploying task

12. In the Active and Scheduled Jobs panel, you can select the task to view the detailed job steps in Running under the Logs tab (Figure 4-19).

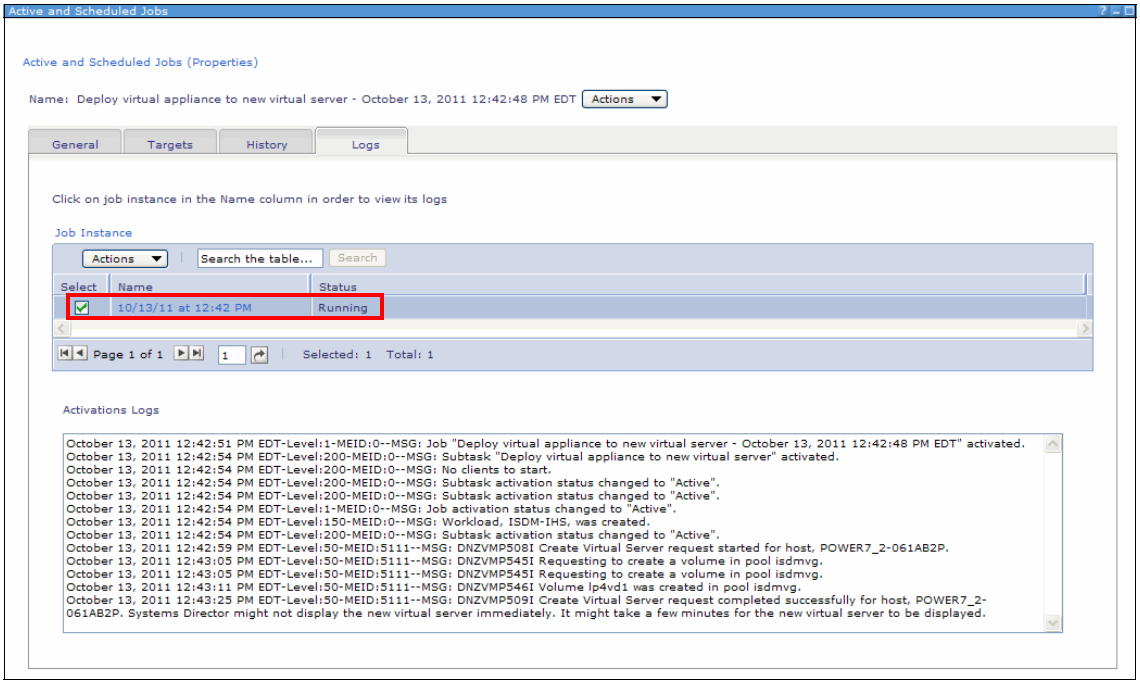

Figure 4-19 Virtual appliance deployment detailed job logs

13. During the deployment of the virtual appliance, you can see the installation progress in HMC. As Figure 4-20 shows, the virtual appliance named NFS is created.

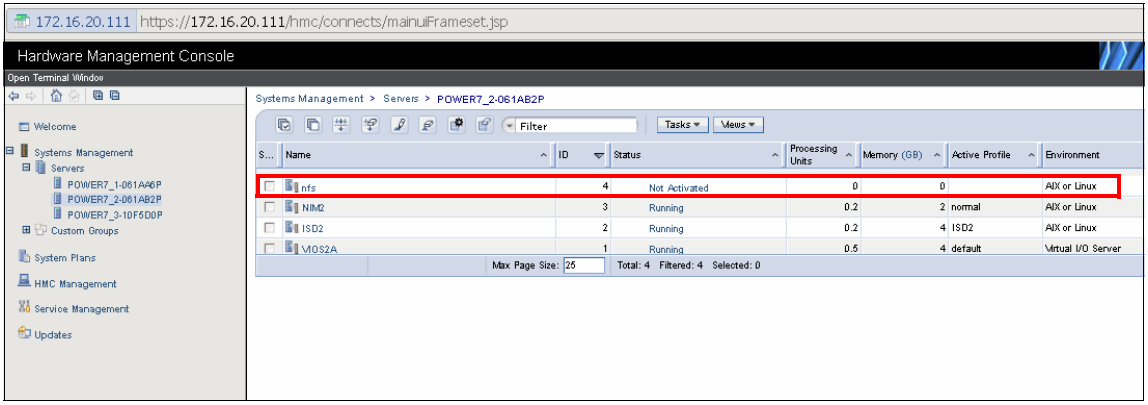

Figure 4-20 Virtual appliance deploying status in HMC

14. Follow steps 1 - 13 for deploying the ITM, TivSAM, and TUAM images.

4.2 Configuring and verifying the installation

After the ISDM virtual images are deployed, follow the procedures of configuring and verifying the installation in the *ISDM 7.2.2 Installation and Configuration Guide.* For the Power systems and AIX environment, follow these instructions:

- Complete the activation of TIVSAM.
- Configure the agent and services.
- Configure the cross connection.
- Synchronize the clocks of virtual images.
- Configure the NFS image as the email forwarder.

The verification software stacks procedures check these:

- The database manager installed with each virtual image is started and ready.
- The HTTP Server is installed with each virtual image and is working.
- ISDM virtual servers are integrated and working together.

4.2.1 Completing the activation of TIVSAM

After the TIVSAM appliance installation, the following log file indicates that some RPM packages required by Tivoli Provision Manager (TPM) are not installed:

`/var/log/10-13-2011-13-07-19_ConfigTSAM.sh.log`

The contents of the file are displayed in Example 4-2.

Example 4-2 ConfigTSAM.sh.log messages requiring additional RPMs

```
ConfigTSAM.sh Start -- logging into
/var/log/10-13-2011-13-07-19_ConfigTSAM.sh.log
Set Welcome Message
reconfigure: true
installPrereq: false
configureICB: false
No prereq to be installed
Starting TSAM reconfiguration ...
Checking if hostname is setted correctly into /etc/hosts file...
Checking if hostname is setted correctly into /etc/hosts file done.
ATTENTION: Some rpms required by TPM are not installed. Check logs
under /var/log directory.
Install all rpms required by TPM and restart activation.
These are the commands to restart activation:
/opt/IBM/AE/AS/ConfigTSAM.sh -reconfigure true
/opt/IBM/SC/vEngine.sh -run &
Restore Welcome Message
```

Obtaining and installing the RPMs

The *ISDM 7.2.2 Installation and Configuration Guide* provides a list of the required RPM packages, which can be downloaded from the following website:

http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/download.html

Figure 4-21 lists the RPM packages extracted from the *ISDM 7.2.2 Installation and Configuration Guide*.

```
glib-1.2.10-2.aix4.3.ppc.rpm
gettext-0.10.40-8.aix5.2.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm
atk-1.12.3-2.aix5.2.ppc.rpm
bash-3.2-1.aix5.2.ppc.rpm
bash-doc-3.2-1.aix5.2.ppc.rpm
zlib-1.2.3-4.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm
libpng-1.2.32-2.aix5.2.ppc.rpm
pixman-0.12.0-2.aix5.2.ppc.rpm
xrender-0.9.1-2.aix5.2.ppc.rpm
cairo-1.8.6-1.aix5.2.ppc.rpm
curl-7.9.3-2.aix4.3.ppc.rpm
freetype-1.3.1-9.aix5.1.ppc.rpm
gdbm-1.8.3-5.aix5.2.ppc.rpm
readline-4.3-2.aix5.1.ppc.rpm
python-2.3.4-4.aix5.3.ppc.rpm
libtiff-3.8.2-1.aix5.2.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
xft-2.1.6-5.aix5.1.ppc.rpm
pango-1.14.5-2.aix5.2.ppc.rpm
xcursor-1.1.7-2.aix5.2.ppc.rpm
gtk2-2.10.6-1.aix5.2.ppc.rpm
unzip-5.51-1.aix5.1.ppc.rpm
wget-1.9.1-1.aix5.1.ppc.rpm
zip-2.3-3.aix4.3.ppc.rpm
perl-5.8.2-1.aix5.1.ppc.rpm
tar-1.14-2.aix5.1.ppc.rpm
procmail-3.21-1.aix4.3.ppc.rpm
```

Figure 4-21 List of additional RPMs to be installed

Notes: The packages need to be installed in the order in which they are listed.

We found that the tcl, tk, and expect packages are already installed as LPPs in AIX. These packages are at later levels than the RPMs required in the list.

Install each RPM with the **rpm** command. For example:

```
# rpm -Uvh glib-1.2.10-2.aix4.3.ppc.rpm
glib ##################################################
```

The option flag -U requests rpm to upgrade the existing RPM. The previous version is removed automatically afer the install or upgrade has completed successfully.

To verify RPM installation, run the following script and check the output log in `/var/log/10-26-2011-13-11-52_checkTpmRpm.sh.log` for the required action:

```
/opt/IBM/AE/AS/checkTpmRpm.sh
```

Importing the VMControl certificate into TPM

The **importCert.sh** command allows you to import the IBM Director SSL certificate into the Tivoli Provisioning Manager truststore. Run this command on Tivoli Service Automation Manager to import the certificate of the director2 system into TPM (Example 4-3).

Example 4-3 Importing the certificate

```
# /opt/IBM/ISDM/bin/importCert.sh -host direcotr2 -serverstorepass
ibmpassw0rd -wasstorepass changeit -wasadmin wasadmin -adminpass
password

ibmjsse2.jks                                              100% 1242
1.2KB/s   00:00

Importing cbvsphere SSL certificate
Certificate stored in file </opt/IBM/ISDM/bin/../tmp/rui.crt>
Insert Director certificare alisas (default is vmcserver):

Certificate was added to keystore
[Storing cacerts]
Restarting TSAM server
Stopping the Software stack
-----------------------
Using Log directory /var/log/mwi
Using Timestamp 100212181554
Using DB2 Instance ctginst1 idsccmdb
Using LDAP DB2 Instance idsccmdb
Using LDAP Path /opt/IBM/ldap/V6.2
Using LDAP admin user cn=root
Using HTTP Server Path /usr/IBM/HTTPServer
Using Websphere Path /usr/IBM/WebSphere/AppServer

Stopping TPM...
```

```
Stopping HTTP Server...
Stopping LDAP Server...
Stopping DB2 instance...
Starting the Software stack
----------------------
Using Log directory /var/log/mwi
Using Timestamp 100212181554
Using DB2 Instances ctginst1 idsccmdb
Using LDAP DB2 Instance idsccmdb
Using LDAP Path /opt/IBM/ldap/V6.2
Using LDAP admin user cn=root
Using HTTP Server Path /usr/IBM/HTTPServer
Using WAS Path /usr/IBM/WebSphere/AppServer
Using TPM Path /opt/IBM/tivoli/tpm

Checking DB2...
NOT STARTED

OK

Starting DB2 instance...
Checking IBM Directory Server...
OK

IBM Direcory already started on port 389
Starting HTTP Server...
Starting WebSphere and TSAM ...

TSAM software stack restarted. Please check logs in /var/log/mwi with
time stamp 100212181554 for errors.
Done
```

You can check that the certificate has been imported by running the **keytool** command (Example 4-4).

Example 4-4 Using the keytool command to check the certificate

```
# cd /usr/IBM/WebSphere/AppServer/java/bin
# ./keytool -v -list -alias vmcserver -keystore
/usr/IBM/WebSphere/AppServer/java/jre/lib/security/cacerts -storepass
changeit
Alias name: vmcserver
Creation date: Feb 10, 2012
Entry type: trustedCertEntry
```

```
Owner: CN=director2, O=IBM, C=US
Issuer: CN=director2, O=IBM, C=US
Serial number: 4f0c10f4
Valid from: 1/10/12 11:20 AM until: 1/9/13 11:20 AM
Certificate fingerprints:
         MD5:  AF:D8:60:97:62:A5:4F:F0:8C:11:CA:FC:8A:A9:7E:3D
         SHA1:
5D:84:26:47:07:6C:15:F9:0D:06:BE:97:3C:48:AD:F0:24:C0:BE:D0
```

Reconfiguring TIVSAM

Run the following command to reconfigure TIVSAM:

```
# /opt/IBM/AE/AS/ConfigTSAM.sh -reconfigure true
```

Note: The first time that we ran the ConfigTSAM.sh script in our environment it failed due to host names used in DB2 configuration files in these:

- `/home/ctginst1/sqllib/db2nodes.cfg`
- `/home/db2inst1/sqllib/db2nodes.cfg`
- `/home/idsccmdb/sqllib/db2nodes.cfg`

We added the following aliases to the TivSAM host definition in `/etc/host` file:

- `icb-tivsam.icbvm.cloud.com`
- `tivsam.icbvm.cloud.com`

We also added `hosts=local,bind` to the `/etc/netsvc.conf` file:

```
# host tivsam
tivsam is 172.16.20.123, Aliases:   icb-tivsam.icbvm.cloud.com,
tivsam.icbvm.cloud.com
          tivsam.powercloud.ibm.com
#
```

Note: In our test environment, we added the host entry for ease of testing. We recommend using a properly configured DNS.

The second time that we ran the ConfigTSAM.sh script, it ran successfully and we were able to start up the TivSAM software stack manually.

4.2.2 Configuring the Service Connection Engine

The following configuration and verification procedures should be done on each ISDM server.

Verifying the Platform Agent

Stop and start the Platform Agent on each system using the **SRC** commands, as in Example 4-5.

Example 4-5 Stopping and starting the Platform Agent

```
# lssrc -s platform_agent
Subsystem         Group            PID          Status
 platform_agent                    3604628      active

# stopsrc -s platform_agent
0513-044 The platform_agent Subsystem was requested to stop.

# lssrc -s platform_agent
Subsystem         Group            PID          Status
 platform_agent                                 inoperative

# startsrc -s platform_agent
0513-059 The platform_agent Subsystem has been started. Subsystem PID
is 10551462.

# lssrc -s platform_agent
Subsystem         Group            PID          Status
 platform_agent                    10551462     active
```

Verifying the Service Location Protocol configuration

Verify the setting of the Service Location Protocol (SLP) in `/etc/slp.conf`. Add the following line under the `net.slp.useScopes` section:

```
net.slp.useScopes = isdm-power,default
```

Note: The Scope isdm-power matches with the environment property setting in `/opt/IBM/SC/conf/stereocable.properties`.

Stop and start the SLP process using the **slp_srvreg** command, as in Example 4-6, on all ISDM servers.

Example 4-6 Stopping and starting the SLP service

```
# slp_srvreg -k
# ps -ef | grep slp_srvreg | grep -v grep

# slp_srvreg -D
```

```
# ps -ef | grep slp_srvreg | grep -v grep
    root 10813506        1   0 15:16:28      -  0:00 slp_srvreg -D
```

Verifying the Service Connection Engine

View the Service Connection Engine configuration file:

```
/opt/IBM/SC/conf/stereocable.properties
```

Verify that the value of the rport and rgroup properties match the values in the TIVSAM OVF file. Figure 4-22 shows the contents of `stereocable.properties`.

```
#Passwords encrypted
#Mon Oct 17 23:17:10 CDT 2011
environment=isdm-power
scriptdir=/opt/IBM/SC/script
plugs=TSAM-NFS_PLUG,TSAM-ITM_TEPS_PLUG,TSAM-ITM_TEMS_PROV_PLUG,TSAM-
TUAM_PLUG,ITM_MGT_AGENT_PLUG
virtualsockets={itm \=>
[ITM_TEPS_SOCKET,ITM_TEMS_MGT_SOCKET,ITM_TEMS_PROV_SOCKET,ITM_TCR_SO
CKET] ; tuam \=> [TUAM_SOCKET]}
sockets=TSAM_SOCKET
rport=10283
rgroup=228.1.2.3
provider=slpAix
```

Figure 4-22 Setting values of rport and rgroup in stereocable.properties

The section “Sockets and plugs” in Appendix E of the *ISDM V7.2.2 Installation and Configuration Guide* contains descriptions of the Service Connection Engine plugs and sockets grouped by virtual image.

Configuring a cross connection

To check that the Service Connection Engine is active and running, run the following command:

```
# /opt/IBM/SC/vEngine.sh -status
CTJES0003I Loading the configuration.
CTJES0004I The configuration was loaded successfully.
CTJES0001I Running the operation: Getting the status of the engine.
CTJES0002I The operation was run successfully: Getting the status of
the engine.
CTJES0001I Running the operation: Event processing.
CTJES0002I The operation was run successfully: Cable processing.
Socket processed:
```

```
        TUAM_SOCKET: Success
Plug processed:
        ITM_MGT_AGENT_PLUG: Success
        TUAM-TSAM_PLUG: Waiting for TSAM_SOCKET
        TUAM-NFS_PLUG: Waiting for NFS_SOCKET
#
```

If the status is not `Success`, then we need to run the Service Connection service.

In the following example, Service Connection is in an error state:

```
# /opt/IBM/SC/vEngine.sh -status
CTJES0003I Loading the configuration.
CTJES0004I The configuration was loaded successfully.
CTJES0001I Running the operation: Getting the status of the engine.
CTJES0006E An error occurred while creating an RMI registry.
CTJES0007E The following operation failed: Getting the status of the
engine.
#
```

To activate the Service Engine, log in as root on the NFS, ITM, TivSAM, and TUAM servers and run the following two commands simultaneously:

```
#/opt/IBM/SC/vEngine.sh -reg
# /opt/IBM/SC/vEngine.sh -run
CTJES0003I Loading the configuration.
CTJES0004I The configuration was loaded successfully.
CTJES0001I Running the operation: Run the engine.
CTJES0001I Running the operation: Cable processing.
CTJES0005I Processing socket: ITM_TEMS_PROV_SOCKET.
CTJES0011I Publishing information.
CTJES0013I Sending the event: socket ITM_TEMS_PROV_SOCKET published.
CTJES0019I Processing the event with type:
STEREOCABLES_SOCKET_PUBLISHED.ITM_TEMS_PROV_SOCKET.
CTJES0020I The event was processed.
CTJES0006I The socket ITM_TEMS_PROV_SOCKET was processed successfully.
CTJES0005I Processing socket: ITM_TEPS_SOCKET.
CTJES0011I Publishing information.
CTJES0013I Sending the event: socket ITM_TEPS_SOCKET published.
CTJES0019I Processing the event with type:
STEREOCABLES_SOCKET_PUBLISHED.ITM_TEPS_SOCKET.
CTJES0020I The event was processed.
CTJES0006I The socket ITM_TEPS_SOCKET was processed successfully.
CTJES0005I Processing socket: ITM_TCR_SOCKET.
CTJES0011I Publishing information.
CTJES0013I Sending the event: socket ITM_TCR_SOCKET published.
```

```
CTJES0019I Processing the event with type:
STEREOCABLES_SOCKET_PUBLISHED.ITM_TCR_SOCKET.
CTJES0020I The event was processed.
CTJES0006I The socket ITM_TCR_SOCKET was processed successfully.
CTJES0005I Processing socket: ITM_TEMS_MGT_SOCKET.
CTJES0011I Publishing information.
CTJES0013I Sending the event: socket ITM_TEMS_MGT_SOCKET published.
CTJES0019I Processing the event with type:
STEREOCABLES_SOCKET_PUBLISHED.ITM_TEMS_MGT_SOCKET.
CTJES0020I The event was processed.
CTJES0006I The socket ITM_TEMS_MGT_SOCKET was processed successfully.
Socket processed:
        ITM_TEMS_PROV_SOCKET: Success
        ITM_TEPS_SOCKET: Success
        ITM_TCR_SOCKET: Success
        ITM_TEMS_MGT_SOCKET: Success
Plug processed:

CTJES0002I The operation was run successfully: Cable processing.
#
```

Note: vEngine.sh -run does not complete until all virtual images communicate and exchange information.

Note: Check the status of the TPM Deployment Engine by running the following command as **root**:

```
su - tioadmin -c "/opt/IBM/tivoli/tpm/tools/tioStatus.sh"
```

If it is not running, run the **tio.sh** command to start it:

```
su - tioadmin -c "/opt/IBM/tivoli/tpm/tools/tio.sh start tpm"
```

Check for errors in the log file:

```
/usr/ibm/tivoli/common/COP/logs/tio_start_service.log
```

4.2.3 Verifying the ISDM integration process

To check the functional integration among the virtual servers, log in to one of the ISDM virtual servers as **root** and issue the following command:

```
# /opt/IBM/SC/script/Cli.sh -list
```

The command output contains information about all the ISDM virtual servers. Due to the amount of information produced, you can redirect the command output to a file for further investigation. Look for the status of sockets and plugs to ensure that they are enabled or active.

4.2.4 Synchronizing the clocks of virtual machines

A time server must be up to synchronize the system clock across all virtual servers. In our configuration, we run the time server on the IBM Systems Director virtual machine. The rest of the ISDM virtual servers are NTP clients, which synchronize their clock to the time server.

On the NTP server machine

Verify that you have a suitable NTP server specified in the `/etc/ntp.conf` file using the **`vi`** editor. For example, the following line is a pseudo IP address that indicates that the time server is synchronized with itself at IP address 127.127.1.0:

```
server 127.127.1.0
```

Example 4-7 shows the content of the `/etc/ntp.conf` file on the NTP Time Server machine.

Example 4-7 Content of /etc/ntp.conf on the NTP Time Server machine

```
server 127.127.1.0
#broadcast client
driftfile /etc/ntp.drift
tracefile /etc/ntp.trace
```

From Example 4-7, the following line is commented out:

```
broadcast client.
```

After modifying the `/etc/ntp.conf` file, you need to stop and start the NTP daemon using the following commands:

```
# stopsrc -s xntpd
# startsrc -s xntpd
```

To check status of the ntp daemon, run this command:

```
# lssrc -s xntpd
Subsystem         Group            PID          Status
 xntpd            tcpip            5112012      active
```

On the NTP client machines

Verify that you have a server suitable for synchronization. In our configuration, the client is pointing to the Systems Director server as the Time Server. Example 4-8 shows the content of the `/etc/ntp.conf` file.

Example 4-8 Content of /etc/ntp.conf on an NTP client machine

```
#broadcast client
server director2
driftfile /etc/ntp.drift
tracefile /etc/ntp.trace
```

From Example 4-8, the time server is running on the server named director2. The line `broadcast client` is commented out.

Check the time offset between this client and the time server using this command:

```
# ntpdate -d director2 | grep offset
filter offset: 419.9948 419.9948 419.9948 419.9948
offset 419.994889
20 Oct 14:11:41 ntpdate[13828278]: step time server 172.16.20.129
offset 419.994889
```

Notes: Note the following information:

- The offset must be less than 1000 seconds for xntpd to synchronize. If the offset is greater than 1000 seconds, change the time manually on the client and run **`ntpdate -d`** again. Do not adjust the time backward on the time server.
- If **`ntpdate`** displays the following message, verify that **`xntpd`** is running on the server and that no firewalls are blocking port 123.

  ```
  no server suitable for synchronization found
  ```

- The NTP time server and its clients should be in the same time zone. In AIX, check the environment variable $TZ:

  ```
  echo $TZ
  ```

If you made any changes, stop and start the **`xntpd`** daemon:

```
# stopsrc -s xntpd
# startsrc -s xntpd
```

Verify that the client is synchronized with the time server using the **`lssrc`** command with option flag **`-ls`**:

```
# lssrc -ls xntpd
```

Note: The Sys peer field displays the IP address or name of your NTP time server. This process might take up to 12 minutes.

Starting ntp at reboot

On AIX, the `/etc/rc.tcpip` file contains the following line:

```
#start /usr/sbin/xntpd "$src_running"
```

If the line starts with the comment character #, remove it and save the file. NTP should start automatically at the next reboot.

Use the option flag -x with the **xntpd** command to specify small time adjustments. On the **start** command line in `/etc/rc.tcpip`, add **-x** at the end with double quotation marks around it:

```
start /usr/sbin/xntpd "$src_running" "-x"
```

4.2.5 Configuring ITM agents

Starting from ISDM 7.2.2, ITM agents for Power Systems include these:

- UNIX OS monitoring agent
- Monitoring agent for AIX Premium
- HMC Base Premium agent
- ITM agent for Systems Director Base
- CEC Base Agent

All of the agents are installed on the ITM server by default. Only the UNIX OS monitoring agent and the monitoring agent for AIX Premium are installed on the other ISDM virtual servers.

The monitoring agent for AIX Premium is configured automatically by the Service Connection Engine. On the ITM virtual server, the agent is started at image activation. On the other ISDM virtual servers, the agent is started when the Service Connection Engine completes integration with the ITM virtual server.

Configuring a monitoring data warehouse

We did not configure a data warehouse in our environment.

4.2.6 Configuring the NFS image as the email forwarder

This section describes how to configure sendmail in the AIX environment to forward or set up a mail server. In our environment, we only have a local mail

server running. If you have an external mail server, then you need to configure the relay host and domain.

Log in to the NFS virtual server as root. Follow these steps:

1. Back up the smtp configuration file if necessary.
2. Stop the sendmail daemon:

   ```
   # stopsrc -s sendmail
   ```

3. Edit the `/etc/mail/sendmail.cf` file as appropriate to configure the relay mail host and domain.
4. Start the sendmail daemon:

   ```
   # startsrc -s sendmail -a "-bd -q30n"
   ```

5. Verify that the sendmail server is listening on port 25 by using the **netstat** command:

   ```
   # netstat -an | grep LISTEN | grep 25
   tcp4       0      0  *.25                   *.* LISTEN
   ```

Log in to the TiVSAM virtual server as root. Follow these steps:

1. Back up the smtp configuration file (`/etc/sendmail.cf`).
2. Stop the sendmail daemon:

   ```
   # stopsrc -s sendmail
   ```

3. Edit the `/etc/mail/sendmail.cf` file to configure the relay mail host and domain, as shown in Example 4-9.

   Example 4-9 Sendmail configuration

   ```
   #Dj$w.Foo.COM
   Dj$w.powercloud.ibm.com
   # "Smart" relay host (may be null)
   DSnfs.powercloud.ibm.com
   ```

4. Start the sendmail daemon:

   ```
   # startsrc -s sendmail -a "-bd -q30n"
   ```

5. Log in to the TSAM Admin interface as maxadmin.
6. Go to **System Configuration** → **Platform Configuration** → **System Properties**.

7. In the Instance Properties section, click **New Row**. For the Value field, add the host name of the TivSAM server, as shown in Figure 4-23.

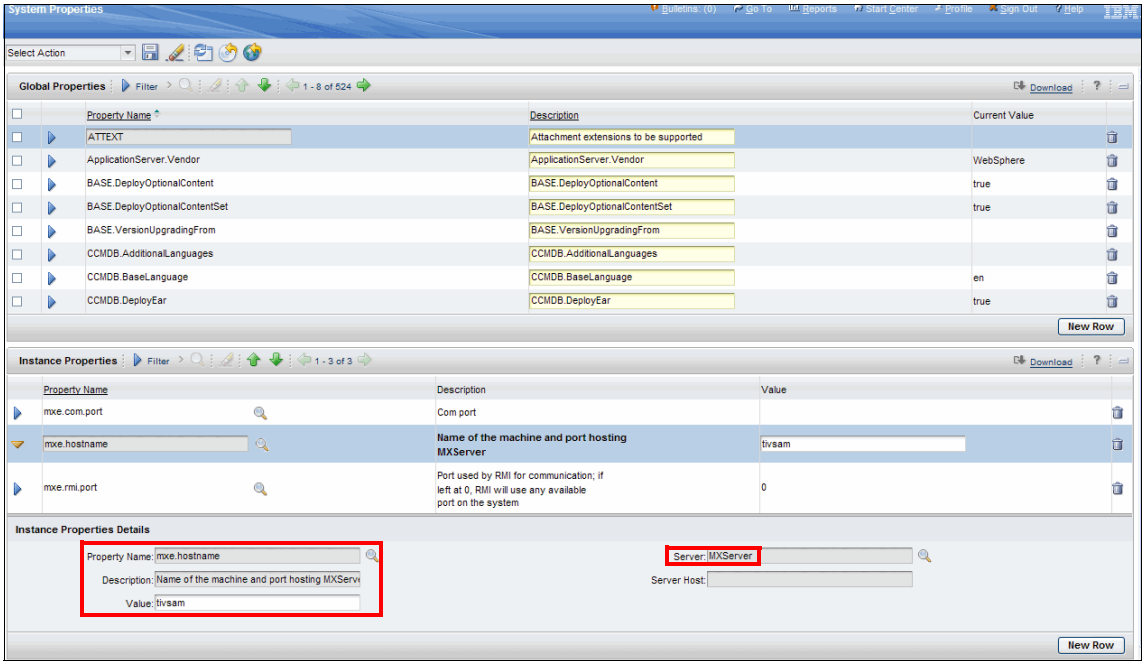

Figure 4-23 Adding new instance properties

8. For this change to take effect, we had to stop and start Tivoli Service Automation Manager using tio.sh.

9. To customize the content of the outgoing e-mail message, go to **Administration → Communication Templates**. Under List of templates, select **PMRDPNOTCHPW** as an example (Figure 4-24). This template is for the root password change of a running instance (LPAR) in a project. Upon completion of the root password change, an e-mail with the text shown in Figure 4-24 is sent out.

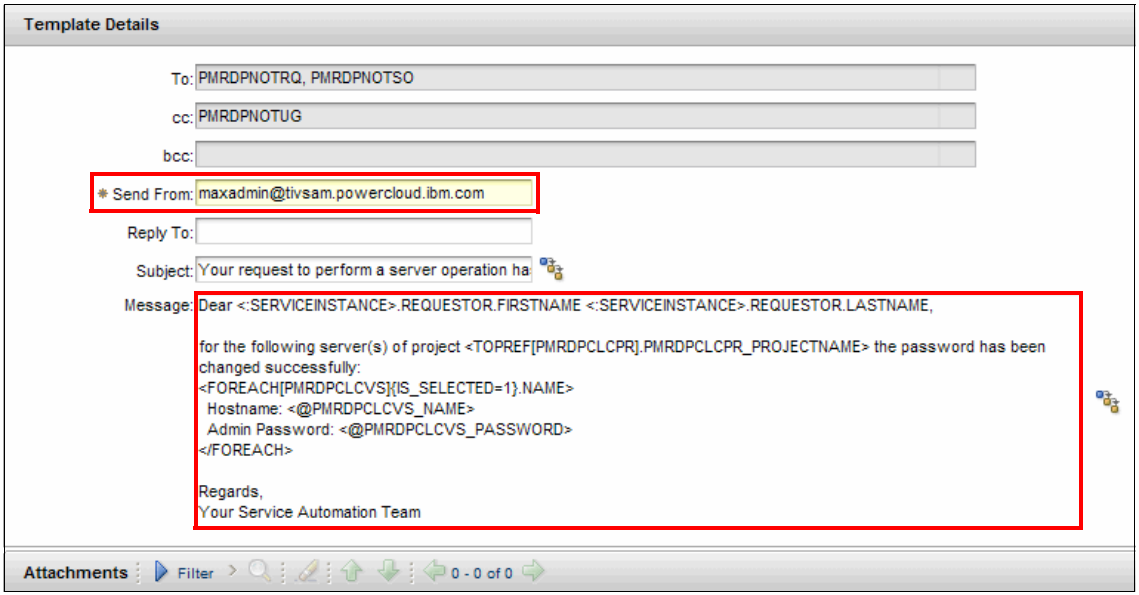

Figure 4-24 Communication Template Details

10. To test this password, change the email notification that you need to have a project deployed. At this step of the configuration, we are not ready to test this email notification. After we created the project, to change the root password, go to **Self Service UI → Request a New Service → Virtual Server Management → Modify Server → Reset Server Password**.

4.2.7 Verifying the software stack

Verify the status of the virtual images installation process based on the software stacks:

- IBM Tivoli Monitor (ITM)
- Network File system Server (NFS)
- Tivoli Services Automation Manager (TIVSAM)
- Tivoli Usage and Accounting Manager (TUAM)

There is no strict order for verifying the software stacks.

Verifying the ITM software stack

Log in to the ITM virtual machine as root. Switch to your DB2 administrator user ID to check the status of the database manager. Issue the **db2start** command:

```
$ su - db2inst1
$ db2start
```

See the status of the database manager, as in Figure 4-25.

Type the **exit** command to return to **root**. Issue the following command to see the status of the ITM products:

```
# /opt/IBM/ITM/bin/cinfo -r
```

The **cinfo** command output in Figure 4-25 shows ITM products running on the ITM host.

```
*                                                                              *
*                                                                              *
********************************************************************************
# su - db2inst1
$ db2start
10/13/2011 14:46:01     0   0   SQL1026N  The database manager is already active
.
SQL1026N  The database manager is already active.
$
# /opt/IBM/ITM/bin/cinfo -r

*********** Thu Oct 13 14:46:24 EDT 2011 *****************
User: root Groups: system bin sys security cron audit lp
Host name : itm  Installer Lvl:06.22.04.00
CandleHome: /opt/IBM/ITM
***********************************************************
Host   Prod  PID       Owner     Start     ID    ..Status
itm    kf    25886930  virtuser  13:42:20  None  ...running
itm    cq    27394138  virtuser  13:42:28  None  ...running
itm    ms    9568416   virtuser  13:42:48  TEMS  ...running
itm    pk    17563858  virtuser  13:43:19  None  ...running
itm    px    9371800   virtuser  13:43:34  None  ...running
itm    ux    21495950  virtuser  13:43:48  None  ...running
#
```

Figure 4-25 Database manager and ITM products running status

The ITM host also runs the HTTP Server processes, which can be found with the command shown in Example 4-10.

Example 4-10 Show the httpd processes

```
# ps -ef | grep httpd | grep -v grep
virtuser  5701752  6488144   0   Oct 13      -  0:00
/usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start

    root  6488144        1   0   Oct 13      -  0:00
/usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start

virtuser 20775116  6488144   0   Oct 13      -  0:00
/usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start

virtuser 21561368  6488144   0   Oct 13      -  0:05
/usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start
```

Since datawarehouse is not configured in our environment, server1 shows in stopped state:

```
# /opt/IBM/tivoli/tip/profiles/TIPProfile/bin/serverStatus.sh server1
ADMU0116I: Tool information is being logged in file

/opt/IBM/tivoli/tip/profiles/TIPProfile/logs/server1/serverStatus.log
ADMU0128I: Starting tool with the TIPProfile profile
ADMU0500I: Retrieving server status for server1
ADMU0509I: The Application Server "server1" cannot be reached. It
appears to be stopped.
```

Verifying the NFS software stack

Log in to the NFS virtual machine as root to check status of these:

- HTTP Server processes
- NFS processes
- Mail server

Use the **ps** command to check the number of HTTP Server processes. The following example shows 18 processes:

```
# ps -ef | grep httpd | grep -v grep | wc
18     270    2856
```

Use the **lssrc** command to check the status of the NFS and mail server processes. Their status should be active, as in following examples:

```
# lssrc -s nfsd
Subsystem         Group            PID          Status
 nfsd             nfs              3932300      active
# lssrc -s sendmail
Subsystem         Group            PID          Status
 sendmail         mail             10420364     active
```

Verifying the TIVSAM software stack

Log in to the TIVSAM virtual machine as root and switch to the user IDs to verify their setup with DB2 and LDAP. See Example 4-11

Example 4-11 Verifying user ID setup and DB2 or LDAP status

```
# su - dasusr1
$ db2admin start
SQL4409W  The DB2 Administration Server is already active.
$ exit
#
# su - ctginst1
$ db2start
10/18/2011 10:04:28     0   0   SQL1026N  The database manager is already active.
SQL1026N  The database manager is already active.
$ exit
#
# su - idsccmdb
$ db2start
10/18/2011 10:05:58     0   0   SQL1026N  The database manager is already active.
SQL1026N  The database manager is already active.
$ exit
#
# ps -ef | grep ibmdiradm | grep -v grep
idsccmdb  7733266        1   0 23:21:03      -  0:00
/opt/IBM/ldap/V6.2/sbin/64/ibmdiradm -I idsccmdb
#
# ps -ef | grep ibmslapd | grep -v grep
idsccmdb  7536796        1   0 00:51:46  pts/1  0:00 /opt/IBM/ldap/V6.2/sbin/64/ibmslapd
-I idsccmdb
```

Verifying the TUAM software stack

The TUAM server is installed with DB2 software. To check the status of the DB2 installation, log in to the TUAM server as root.

DB2 is installed and configured with a user ID *db2inst1*. The following commands ensure that the user is set up correctly and that DB2 has been started:

```
$ su - db2inst1
$ db2start
```

The **db2start** command displays the messages shown in Figure 4-26 indicating that the database manager is active.

```
$ db2start
10/13/2011 14:49:16     0   0   SQL1026N  The database manager is
already active.
SQL1026N  The database manager is already active.
```

Figure 4-26 Checking status of the database manager on TUAM

Type the command **exit** to return to *root* and verify the TIP server status with the following command:

```
# /opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/serverStatus.sh server1
-username virtuser -password <password>
```

Substitute <*password*> with your user password.

Figure 4-27 shows the messages displayed by **serverStatus.sh**. The application server is started.

```
# /opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/serverStatus.sh server1
-username virtuser -password <password>
ADMU0116I: Tool information is being logged in file

/opt/IBM/tivoli/tipv2/profiles/TIPProfile/logs/server1/serverStatus.log
ADMU0128I: Starting tool with the TIPProfile profile
ADMU0500I: Retrieving server status for server1
ADMU0508I: The Application Server "server1" is STARTED
```

Figure 4-27 Checking the application server status on TUAM

5

Configuring cloud components

Tivoli Service Automation Manager (TSAM) and Tivoli Provisioning Manager (TPM) need to know about the resources available to them before they can create and provision virtual servers. This information is provided through TPM's data model. Each data model describes a specific environment, known as a *cloud server pool*. This chapter describes the process of configuring the TPM data model.

5.1 Configuration

Tivoli Service Automation Manager and Tivoli Provisioning Manager need to know about the resources available to them before they can create and provision virtual servers. Each DCM defines a specific environment, known as a *cloud server pool*. For example, there might be a cloud server pool for systems managed by IBM Systems Director, another for systems managed directly by an HMC, and another for systems that use VMWare virtualization.

Note: Each cloud server pool has its own DCM.

The data center model is a collection of XML files, some of which are generic, others that are specific to the type of managed platform. It defines the following platform characteristics:

- Manager platforms
- Manager or virtualization type (HMC, VMControl, VMWare, KVM, to name a few)
- File repositories
- Resource pools
- Reservation parameters used for provisioning

You must create a cloud server pool and data center model within Tivoli Service Automation Manager for each virtualization technology used for provisioning cloud projects. The Tivoli Service Automation Manager includes the Cloud Server Pool Administration application to help you with the creation of cloud server pools and their associated data center model.

Perform these setup tasks:

- Connect IBM Service Delivery Manager to the virtualization environment (in our case, IBM Systems Director and VMControl).
- Configure the integration between the individual IBM Service Delivery Manager components.
- Discover the available physical and virtual resources, including servers, storage, networks, and images.
- Populate the image library.

The procedure described in this chapter is specific to VMControl.

Note: IBM Service Delivery Manager depends on a fully operational network. Before undertaking any installation task, ensure that all networks and, in particular, name resolution are correctly configured.

To establish the connection between IBM Service Delivery Manager and VMControl you must take these steps:

1. Import the VMControl SSL certificate into Tivoli Provisioning Manager.
2. Tailor the data center model description.
3. Import the data center model in to Tivoli Service Automation Manager.

5.2 Importing the VMControl SSL certificate in to TPM

For Tivoli Provisioning Manager to invoke operations on VMControl using HTTPS, you must import VMControl's SSL certificate into Tivoli Provisioning Manager's Java runtime truststore.

Procedure

Follow this procedure:

1. Log on to the AIX system upon which IBM Systems Director and VMControl are installed.
2. By default, VMControl's certificate is installed in the `ibmjsse2.jks` file in the `/opt/ibm/director/lwi/security/keystore/` directory. Copy this file to the TIVSAM_image.
3. Log on to the TivSAM_image as root.
4. Run the following commands to add the VMControl key to TPM:

```
cd /usr/IBM/WebSphere/AppServer/java

./jre/bin/keytool -export -alias lwiks -storepass ibmpassw0rd \
-file <ibmjsse2_path>/client.cer -keystore
<ibmjsse2_path/ibmjsse2.jks

./jre/bin/keytool -import -v -trustcacerts -alias lwiks \
-file <ibmjsse2_path>/client.cer -storepass changeit \
-keystore ./jre/lib/security/cacerts
```

Type `yes` when prompted to trust the certificate:

```
rm <ibmjsse2_path>/ibmjsse2.jks <ibmjsse2_path>/client.cer
```

Where <*ibmjsse2_path*> is the path to the directory in to which you copied the `ibmjsse2.jks` file in step .2 on page 107.

The passwords given in the above commands are the default ones. If you have changed them, then use your new ones.

5. Restart Tivoli Provisioning Manager so that it picks up the imported certificate.

5.3 Tailoring the data center model

Three files are used to describe the data center:

- `DCM_objects.xml`

  `DCM_objects.xml` describes the network configuration and the virtualization management platform (in our case, VMControl).

- `vrpool.properties`

  `vrpool.properties` provides the characteristics of the server resources available for a given Tivoli Service Automation Manager server pool.

- `NetworkTemplate.xml`

  `NetworkTemplate.xml` connects the network definitions in `DCM_objects.xml` to a given IBM Service Delivery Manager customer.

Figure 5-1 shows the functional architecture of the IBM Service Delivery Manager platform used for this publication. The configuration files presented in this section correspond to this setup.

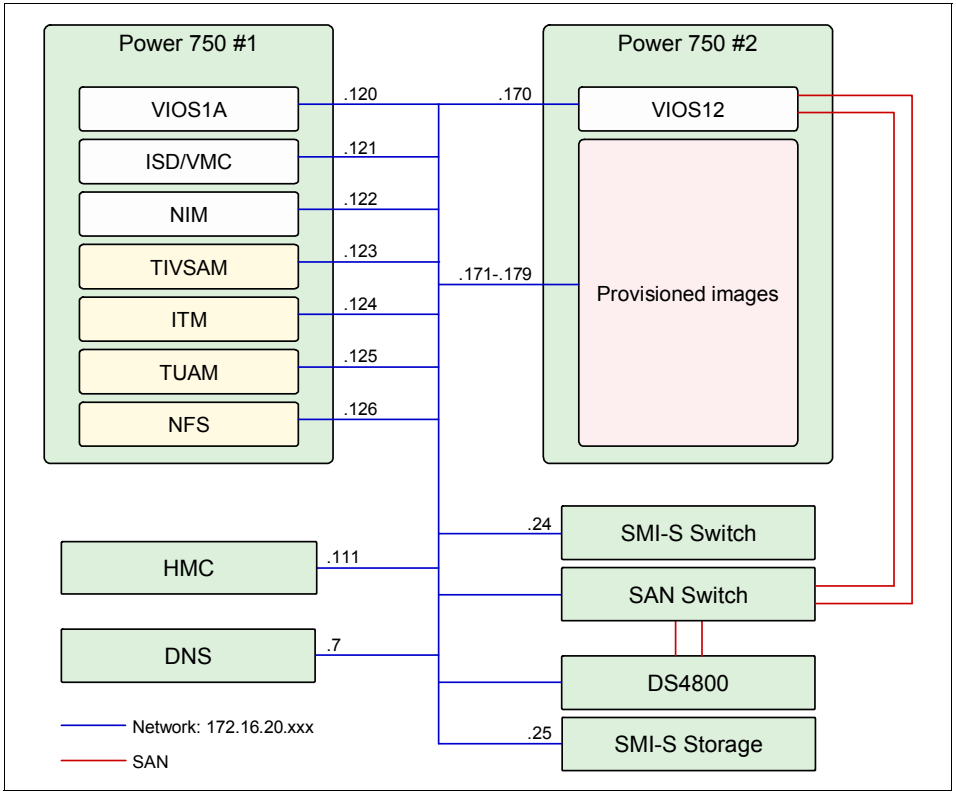

Figure 5-1 Functional architecture for the ISDM platform

5.3.1 DCM_objects.xml

On TIVSAM_image, from `/opt/IBM/ISDM/TSAMDefinitions/` copy the `DCM_objects.xml` file. This becomes your new data center model description file. This file specifies these:

- Network configuration, including subnetworks, virtual LANs (VLANS), routes, gateways, address ranges, and name resolution (DNS)
- Virtualization technology and the platform manager

Note: In earlier versions of IBM Service Delivery Manager, the datacenter model was described in several different files. In Version 7.2.2, the model is described in a single file. It is frequently referred to by its default name, `DCM_objects.xml`, but it can be given any legal filename.

Example 5-1 shows the `DCM_objects.xml` file for the publication environment. In this example, we use a single network definition.

Example 5-1 DCM_objects.xml file

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE datacenter SYSTEM "file:../xml/xmlimport.dtd">
<!--
 ********************************************************************
 * Licensed Materials - Property of IBM
 * (C) Copyright IBM Corp. 2010
 * All Rights Reserved
 * US Government Users Restricted Rights - Use, duplication or
 * disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
 ********************************************************************
-->

<datacenter>

<!-- Begin common definitions -->
  <kanaha-config>
    <dcm-object id="0" type="managedSystem" name="KANAHA">
      <!-- Limit to 5 maximum number of concurrent task from TSAM -->
      <property component="KANAHA" name="Cloud.HOST_TRANSACTION_NUMBER_LIMIT" value="5"/>
    </dcm-object>
  </kanaha-config>


<!-- Begin Subnet definitions -->
  <subnetwork address-space="DEFAULT"
                       name="POWERCloud Network VLAN1"
```

```
                  ipaddress="172.16.20.0"
                    netmask="255.255.252.0>

      <blocked-range from="172.16.20.0" to="172.16.20.170" />
      <blocked-range from="172.16.20.180" to="172.16.23.254" />

      <!-- Required Parameter. Has always to be set to true -->
      <property component="KANAHA" name="PMRDP.Net.Cloud" value="true"/>
      <!-- Defines the Gateway for this subnet -->
      <property component="KANAHA" name="PMRDP.Net.Gateway" value="172.16.20.1"/>

      <!-- Defines the VLAN id for this subnet.
           If external switch vlan tagging is active it is required to set this value to 0 -->
      <property component="KANAHA" name="PMRDP.Net.VLANID" value="1"/>

      <!-- Defines the broad cast address for this subnet -->
      <property component="KANAHA" name="PMRDP.Net.Broadcast" value="172.16.20.255"/>
      <property component="KANAHA" name="PMRDP.Net.DomainName" value="powercloud.ibm.com"/>

  </subnetwork>

<!-- End Subnet definitions -->
<!-- End common definitions -->

  <software-stack name="ODSDS_Pool_host_Stack"
                locale="en_US"
          description="ODSDS_auto-generated"
           stack-type="Declared">

    <software-resource-template name="Default Template"
              software-resource-type="PLACEHOLDER"
                   multiplicity-type="Zero_Or_More"
```

```
        software-configuration-type="Regular"
       is-selected="true" is-default="true"/>
  </software-stack>

  <spare-pool name="VMC Cloud Pool">
    <server-template name="ODSDS_Pool_host_Template" locale="en_US">
      <template-software-module software-module-name="ODSDS_Pool_host_Stack" />
    </server-template>

    <property component="KANAHA" name="cloud" value="true" />
    <property component="KANAHA" name="PMRDP.Net.SubnetPool_0" value="POWERCloud Network
VLAN1"/>
    <property component="KANAHA" name="PMRDP.Net.SubnetAliasesPool_0" value="Network 1"/>
    <!-- Definition of first network adapter as management network adapter-->
    <property component="KANAHA" name="PMRDP.Net.ManagementNIC" value="0"/>

    <!-- Definition of first network adapter as network adapter
         which is used in the hostname resolution -->
    <property component="KANAHA" name="PMRDP.Net.HostnameResolveNIC" value="0"/>

    <!-- Definition of the DNS servers list. Parameters are comma separated.-->
    <property component="KANAHA" name="PMRDP.Net.DNSServers" value="172.16.20.7"/>

     <!-- Definition of the DNS suffix list used for ip address resolvement.
          Parameters are comma separated -->
     <property component="KANAHA" name="PMRDP.Net.DNSSuffix" value="powercloud.ibm.com"/>
  </spare-pool>

  <server name="director2.powercloud.ibm.com" ignored-by-resource-broker="false" failed="true">
     <sap name="HTTPS" protocol-type="ipv4"
                       app-protocol="HTTPS"
                            context="NOCONTEXT"
                              port="8422"
                     auth-compulsory="false"
                               role ="host”>

       <credentials search-key="VMC" is-default="false">
         <password-credentials username="root" password="passw0rd" is-encrypted="false" />
       </credentials>
     </sap>
  </server>

</datacenter>
```

Following the xml headers, the outermost xml tag is <datacenter>. All datacenter model definitions occur within this scope.

Next comes the common definitions within the <kanaha-config> tag. These are the global settings. With larger configurations where you might have several deployments running at the same time, increase the number of concurrent tasks. For example:

```
<property component="KANAHA"
                name="Cloud.HOST_TRANSACTION_NUMBER_LIMIT" value="30"/>
```

Note: Previous versions of IBM Service Delivery Manager and Tivoli Service Automation Manager used a property called `Cloud.DUAL_NIC_MODE`. This has been deprecated by the `CPMRDP.Net.MultiNicSupport` property.

The sub-network definitions are next, defined within the `<subnetwork>` tag. You must include an xml paragraph for each subnet in your configuration. The `<subnetwork>` tag attributes are `name`, `ipaddress`, and `netmask`. The `name` attribute is referenced in the `<spare-pool>` paragraph in the same `DCM_objects.xml` file and also in the `Expression` paragraph in the `NetworkTemplate.xml` file. In Example 5-1 on page 110, the sub-network name is `POWERCloud Network VLAN1`.

Still within the `<subnetwork>` scope, the `<blocked-range>` property indicates which addresses are unavailable to Tivoli Service Automation Manager. As shown in Example 5-1 on page 110, you can specify more than one blocked range for each sub-network. In this example we use:

```
<blocked-range from="172.16.20.0" to="172.16.20.170" />
<blocked-range from="172.16.20.180" to="172.16.23.254" />
```

With this configuration, the addresses available for provisioned virtual servers are in the range 172.16.20.171 - 172.16.20.179.

`PMRDP.Net.Gateway`, `PMRDP.Net.VLANID`, `PMRDP.Net.Broadcast`, and `PMRDP.Net.DomainName` properties specify the network gateway, the VLAN ID, the broadcast address, and the network domain name, respectively.

If you have more than one network, for example, a management network and a customer network, then you will have a `<subnetwork>` xml paragraph for each.

The `<software-stack>` paragraph comes next. This describes the software stack that is associated with a resource pool. For VMControl resource pools this is usually just a placeholder. Its definition is required because the `<software-stack>` is a mandatory property of the `<spare-pool>` definition.

Note: If you have to re-import the `DCM_objects.xml` file, then you must comment out the `<software-stack>` paragraph using `<!--` and `-->`.

The `<spare-pool>` follows. Do not be misled by the name of this tag. There is nothing auxiliary about its contents. They describe the server resource pool to Tivoli Service Automation Manager and as such is mandatory.

The `<spare-pool>` paragraph must be modified such that the `name` attribute matches that given in the `vrpool.properties` file. The `PMRDP.Net.SubnetPool_0` property defines the first network adapter on the host and lists the existing

subnetwork names. It must match the subnetwork names specified in the first part of the DCM_objects.xml file. In Example 5-1 on page 110, only one sub-network is defined. Hence, there is only PMRDP.Net.SubnetPool_0 within the <spare-pool> paragraph. With additional sub-networks you will have PMRDP.Net.SubnetPool_1 and PMRDP.Net.SubnetPool_2, and so forth.

Note: In Tivoli Service Automation Manager 7.2.2 the network configuration has been changed and PMRDP.Net.SubnetPool_* properties are no longer used for this purpose.

The PMRDP.Net.ManagementNIC defines the management network through the reference to the suffix of the PMRDP.Net.SubnetPool_x property.

The PMRDP.Net.HostnameResolveNIC defines the network used to resolve the host name of an LPAR using a reverse DNS lookup. The value attribute references the suffix of the PMRDP.Net.SubnetPool_x property.

Note: PMRDP.Net.ManagementNIC and PMRDP.Net.HostnameResolveNIC properties both have value attributes (in our example, value="0"). This zero references the zero suffix of the PMRDP.Net.SubnetPool_0 property. It does *not* reference the AIX interface and adapter numbers, en0 and ent0.

The PMRDP.Net.DNSServers property gives the IP address of the DNS servers. If you have more than one server, they should be comma separated.

The PMRDP.Net.DNSSuffix property defines the domain name server suffixes. If you have more than one suffix, they should be comma separated.

The <server> paragraph describes the virtualization management environment. When using VMControl, the name attribute is the host name of the IBM Systems Director/VMControl server. The attribute must match that used in the imported certificate. If the certificate references the fully qualified name, then this field must also contain the fully qualified name. See 5.2, “Importing the VMControl SSL certificate in to TPM” on page 107. This name must also match that given for the name property in the vrpool.properties file.

The <sap> paragraph describes the service access point for the virtualization manager. Its content depends on the type of virtualization manager that you use (for example, VMControl, HMC, or VMWare). In this publication we use VMControl, so this describes how to connect to IBM Systems Director and VMControl.

5.3.2 vrpool.properties file

The `vrpool.properties` file contains references to one or more cloud server pools. The name of each pool must match that of the `name` attribute of the `<spare-pool>` paragraph in the `DCM_objects.xml` file.

In its simplest form, `vrpool.properties` references a single cloud pool, as shown in Example 5-2.

Example 5-2 vrpool.properties file for a VMControl-managed pool

```
#################################################################
# Licensed Materials - Property of IBM
# (C) Copyright IBM Corp. 2011
# All Rights Reserved
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#################################################################

5.name=VMC Cloud Pool
5.tpmHPType=PowerHMC
5.order=6
5.hypervisorHostName=director2
5.tpmPool=VMC Cloud Pool
5.maxVCPU=64
5.maxCPUUnits=40
5.maxMemMB=163840
```

The semantics of this file are as follows:

name The name of the cloud pool.

tpmHPType Stipulates the virtualization technology used for the pool. Legal values are:

LPAR	For HMC-managed PowerVM cloud pool
PowerHMC	For VMControl-managed PowerVM pool
VMWare	For VMWare ESX and ESXi
Xen	For Xen
KVM	For KVM
zVM	For zOS

order The order of the pool as presented in the Tivoli Service Automation Manager administrative (Maximo) interface. The order also relates to the number that prefixes each entry (the `5` in Example 5-2), with the subtlety that the

prefix starts at zero while the order attribute starts at one. The order does not have to be sequential.

hypervisorHostName The name of the management server. This must match the name attribute in the `<server>` paragraph of the `DCM_objects.xml` file.

tpmPool The pool name used by Tivoli Provisioning Manager. For VMControl, this is the same as that given in the name property on the first line.

maxVCPU Maximum number of virtual CPUs that any virtual server in this pool can contain.

maxCPUUnits A CPU unit is 1/10 of a full CPU. This value indicates the largest number of CPU units that can be allocated to a virtual server in this pool. If you are familiar with PowerVM, you might think of this as the largest entitlement.

maxMemMB The maximum amount of memory, in MB, allowed for any virtual server in this pool to contain.

Note: The attributes contained in the `vrpool.properties` file vary with the hypervisor technology used by the pool. Example 1-3 on page 11 shows the attributes for a cloud pool managed by VMControl.

Example 5-3 shows a richer `vrpool.properties` containing several different cloud pools.

Example 5-3 vrpool.properties file with multiple cloud pools

```
################################################################
# Licensed Materials - Property of IBM
# (C) Copyright IBM Corp. 2011
# All Rights Reserved
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
################################################################

0.name=VMware System x
0.tpmHPType=VMware
0.order=1
0.tpmPool=Esx Cloud Pool
0.hypervisorHostName=virtualcenter
0.fileRepositoryName=VMwareFileRepository
0.maxVCPU=4
0.maxCPUUnits=40
0.maxMemMB=8192
```

```
1.name=System p LPAR
1.tpmHPType=LPAR
1.order=2
1.tpmPool=Systemp Host Pool
1.maxVCPU=8
1.maxCPUUnits=40
1.maxMemMB=8192

2.name=System z pool
2.tpmHPType=zVM
2.order=3
2.tpmPool=System z pool
2.hypervisorHostName=mapserve
2.maxVCPU=4
2.maxCPUUnits=40
2.maxMemMB=8192

3.name=KVM Local Disk
3.tpmHPType=KVM
3.order=4
3.tpmPool=KVM Cloud Pool
3.maxVCPU=8
3.maxCPUUnits=40
3.maxMemMB=8192

4.name=Xen Local Disk
4.tpmHPType=Xen
4.order=5
4.tpmPool=Xen Cloud Pool
4.maxVCPU=8
4.maxCPUUnits=40
4.maxMemMB=8192

5.name=VMC Cloud Pool
5.tpmHPType=PowerHMC
5.order=6
5.tpmPool=VMC Cloud Pool
5.maxVCPU=64
5.maxCPUUnits=40
5.maxMemMB=8192
```

Backing up the Tivoli Service Automation Manager database

Make a backup of the Maximo database before making significant changes to the Tivoli Service Automation Manager configuration.

Procedure

Follow this procedure:

1. Log on to the TivSAM_image as root.
2. Switch to the tioadmin user:

   ```
   su - tioadmin
   ```

3. Change working directory to `TIO_HOME`:

   ```
   cd $TIO_HOME
   ```

4. Stop all WebSphere services:

   ```
   ./tools/tio.sh stop wasadmin password
   ```

5. Exit back to the root user:

   ```
   exit
   ```

6. Switch to the ctginst1 user:

   ```
   su - ctginst1
   ```

7. Create a directory to hold the backups:

   ```
   mkdir -p backups/clean
   ```

8. Ensure that no applications are connected to the database:

   ```
   db2 list applications
   ```

   The command produces no output.

9. Back up the database to the freshly created directory:

   ```
   db2 backup database maxdb71 to ./backups/clean compress
   ```

10. When the backup has completed, log out user ctginst1:

    ```
    exit
    ```

11. Switch to the tioadmin user:

    ```
    su - tioadmin
    ```

12. Start WebSphere services:

    ```
    $TIO_HOME/tools/tio.sh start wasadmin password.
    ```

    Wait for the MXServer and lightweight runtime to start.

13. Log out the tioadmin user:

    ```
    exit
    ```

Restoring a saved database

To restore a saved version, stop the WebSphere services, as shown in steps 1 on page 118 through 5 on page 118 of the backup procedure, then run the following command as root:

```
su - ctginst1 -c "db2 restore database maxdb71 from /backups/clean"
```

When this has completed, restart the WebSphere services, as shown in steps 11 on page 118 through 13 on page 118 of the backup procedure.

5.3.3 NetworkTemplate.xml

The cloud network configuration for IBM Service Delivery Manager defines the network that will be used on the provisioned virtual images. More than one network interface can be configured deployed virtual images. In our configuration we only configured a single network interface.

The cloud network configuration references some of the information previously created in the `DCM.xml` file in 5.1, “Configuration” on page 106. This information is then used to tell Tivoli Service Automation Manager the range of IP addresses that it can use when assigning an IP address to a cloud resource.

There are two steps required to define the cloud network configuration:

1. Identify and confirm the client networks that were specified when defining the cloud pool, as described in “DCM_objects.xml” on page 109.
2. Add the identified networks as a cloud network.

Identifying client networks

The client networks are defined in `DCM_objects.xml`. They are identified by the `name` attribute of the `subnetwork` tag in the xml file:

```
<!-- Begin Subnet definitions -->
  <subnetwork address-space="DEFAULT"
                       name="POWERCloud Network VLAN1"
                  ipaddress="172.16.20.0"
                    netmask="255.255.252.0>
```

In this example the name is. `POWERCloud Network VLAN1`.

Make a note of the names of all your subnetworks.

Adding a cloud network

To add the cloud network to Tivoli Server Automation Manager, perform the following steps:

1. The configuration of the network information is performed by uploading an `.xml` file into Tivoli Service Automation Manager. The `xml` template can be found in the following location on the Tivoli Service Automation Manager server:

   `/opt/IBM/ISDM/TSAMDefinitions/NetworkTemplate.xml`

   Copy the network template file to your personal computer and name it `MyCloudNetwork.xml`.

2. Open the example template in your home directory, `MyCloudNetwork.xml` in your preferred editor. Fill in the `xml` properties as appropriate. Example 5-4 is the `MyCloudNetwork.xml` file that we used for our implementation.

   Example 5-4 Example of MyCloudNetwork.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NetworkConfiguration
xmlns="http://www.ibm.com/xmlns/prod/ism/pmzhb/NetworkConfiguration"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/xmlns/prod/ism/pmzhb/NetworkConf
iguration PMZHB_NetworkConfiguration.xsd">
    <Version>1.0</Version>
    <NetworkSegments>
        <NetworkSegment>
            <Name>Management Segment</Name>
            <Type>Management</Type>
            <Subnets>
                <Name>POWERCloud Network VLAN1</Name>
                <Reference RefType="DCM">
                   <Expression>POWERCloud Network VLAN1</Expression>
                </Reference>
            </Subnets>
        </NetworkSegment>
    </NetworkSegments>
</NetworkConfiguration>
```

   The important properties that require changing are the `<Type>` markup tag and the `<Expression>` markup tag:

   – The `<Type>` tag can only contain the values of *Management*, *Customer*, *Storage*, and *Backup-Restore*. As the names imply, the values correspond to the type of network associated with that particular subnet.

   – The `<Expression>` tag must contain the name of the data center model (DCM) network subnet. Here it corresponds to the subnetwork name in

DCM_objects.xml recorded in step “Identifying client networks” on page 119.

Note: The subnetwork template can contain more than one DCM network subnet. In our example we only used a single subnet.

5.4 Importing the datacenter model in to Tivoli Service Automation Manager

After you have edited the DCM_objects.xml, vrpool.properties, and NetworkTemplate.xml files, you must import them in to Tivoli Service Automation Manager.

5.4.1 Preparation

Perform the following steps to prepare for the data import:

1. Copy the DCM_objects.xml, vrpool.properties, and NetworkTemplate.xml files to your local machine.
2. Using a browser, connect to the TivSAM_image at the following URL:

   https://<TSAM>:9443/maximo
3. Log on as user maxadmin. The default password is password. You are presented with the Tivoli Service Automation Manager administration interface, also known as the Maximo interface.

5.4.2 Importing DCM_objects.xml

Take the following steps to import the objects:

1. Navigate to **Go To** → **Service Automation** → **Configuration** → **Cloud Server Pool Administration**, as shown in Figure 5-2.

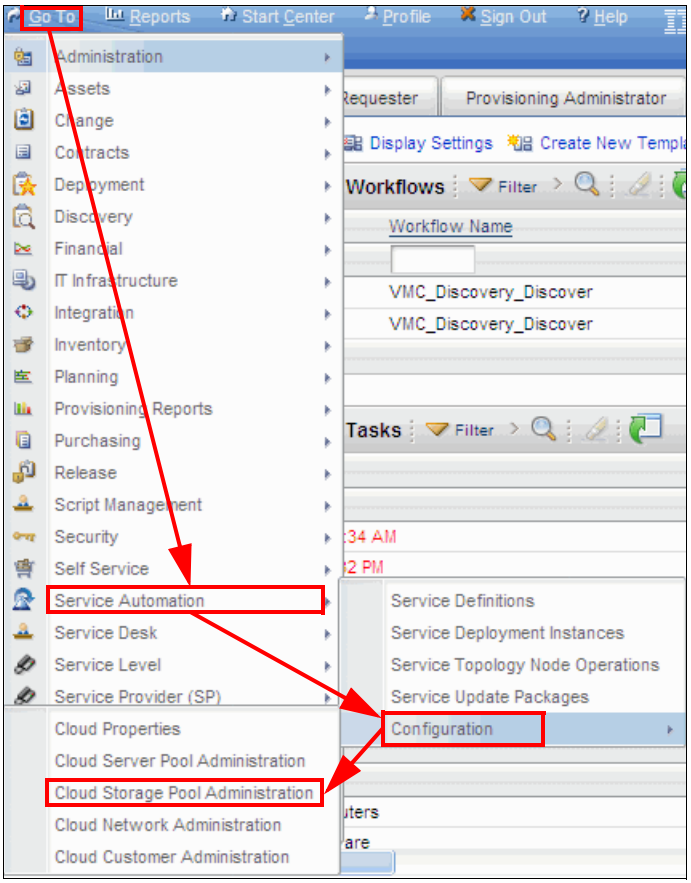

Figure 5-2 Navigating to Cloud Server Pool Administration

2. You are presented with the Cloud Server Pool Overview panel, shown in Figure 5-3. Click **Import DCM Objects** to be presented with a Select Input File pop-up, shown in Figure 5-4.

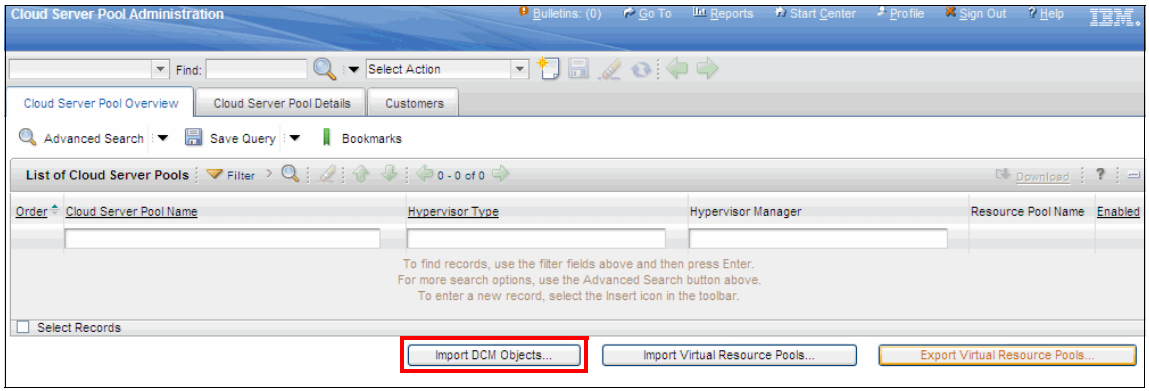

Figure 5-3 Cloud Server Pool Overview panel

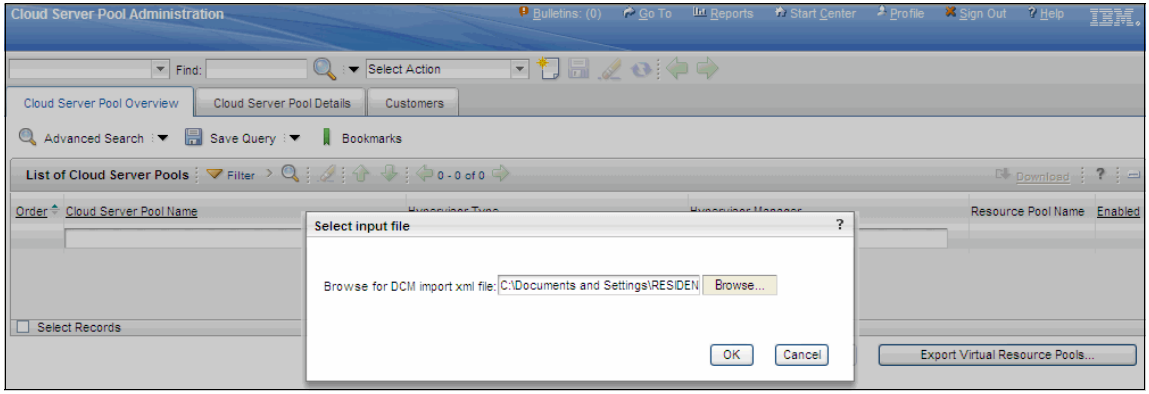

Figure 5-4 Select Input File pop-up

3. Click **Browse** and navigate to where you copied the `DCM_objects.xml` file in step 1 on page 121. Then click **OK**. A System Message pop-up confirms that the import has succeeded (Figure 5-5).

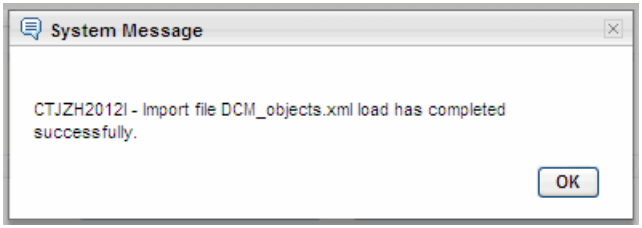

Figure 5-5 DCM_objects import confirmation pop-up

5.4.3 Importing vrpool.properties

Now import the cloud pool definition file, `vrpool.properties`, using this procedure:

1. In the Maximo Cloud Server Pool Overview panel, shown in Figure 5-6, click **Import Virtual Resource Pools**. In the Select Input File pop-up, navigate to where you saved the `vrpool.properties` file in step 1 on page 121. Click **OK** to import the file. A System Message pop-up indicates that the import has completed, as shown in Figure 5-7 on page 125.

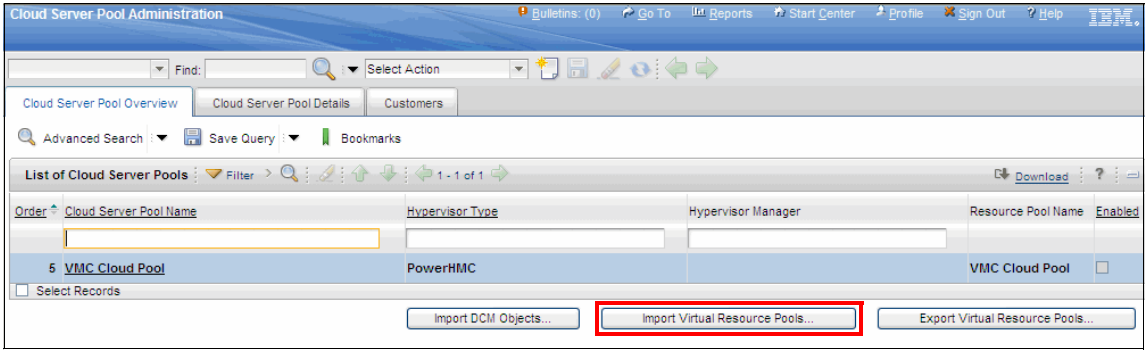

Figure 5-6 Cloud Server Pool Overview panel after importing the DCM objects

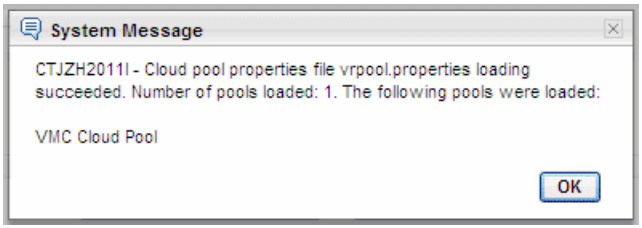

Figure 5-7 vrpool.properties import confirmation pop-up

Figure 5-8 shows the Cloud Server Pool Overview panel after importing the `vrpool.properties` file.

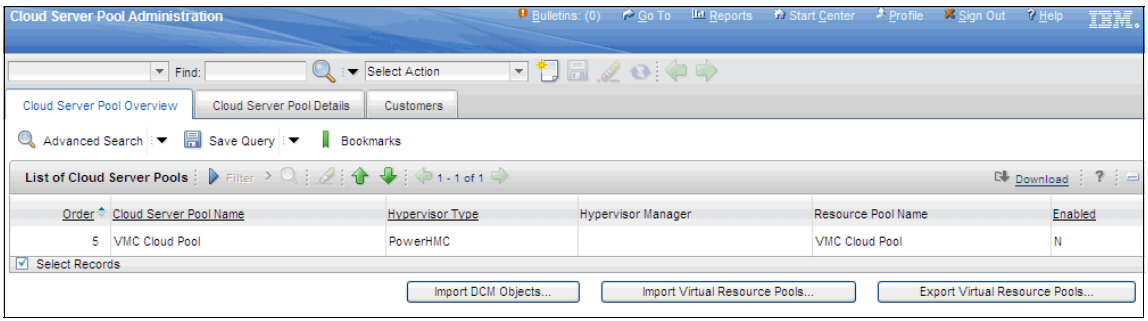

Figure 5-8 The Cloud Server Pool Overview panel after importing vrpool.properties

2. In the Cloud Pool Administration panel and Cloud Server Pool Overview tab there is a single section, List of Cloud Server Pools, shown in Figure 5-8. Ensure that the Select Records tick-box is *not* checked. To navigate to the Cloud Server Pool Details, either click the **Cloud Server Pool Details** tab or click the name of the server pool in the Cloud Server Pool Name column.

Scroll down to the Resource Configuration section and verify that the Resource Pool Name contains the correct pool name. See Figure 5-9. If it does not, click the chevron to the right of the text box, then click **Select Value** to choose your cloud pool.

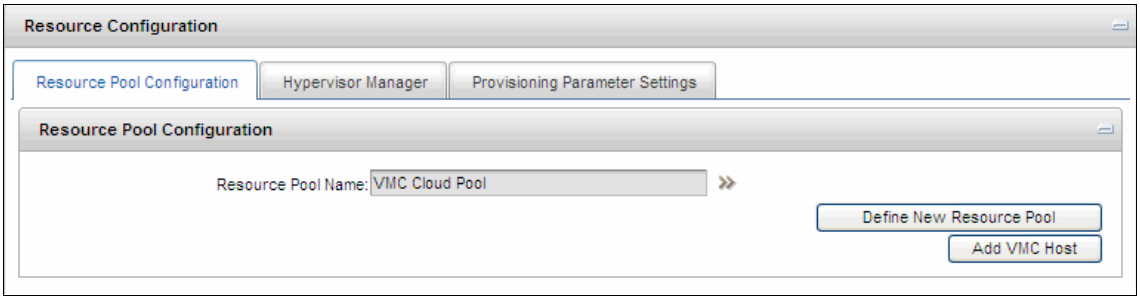

Figure 5-9 Cloud Server Pool Details: Resource Configuration

3. Verify that Tivoli Service Automation Manager knows about VMControl. If you provided the hypervisor manager name in the `vrpoo.properties` (hypervisorManagerName), you do not need to select the hypervisor manager, as shown in Figure 5-10.

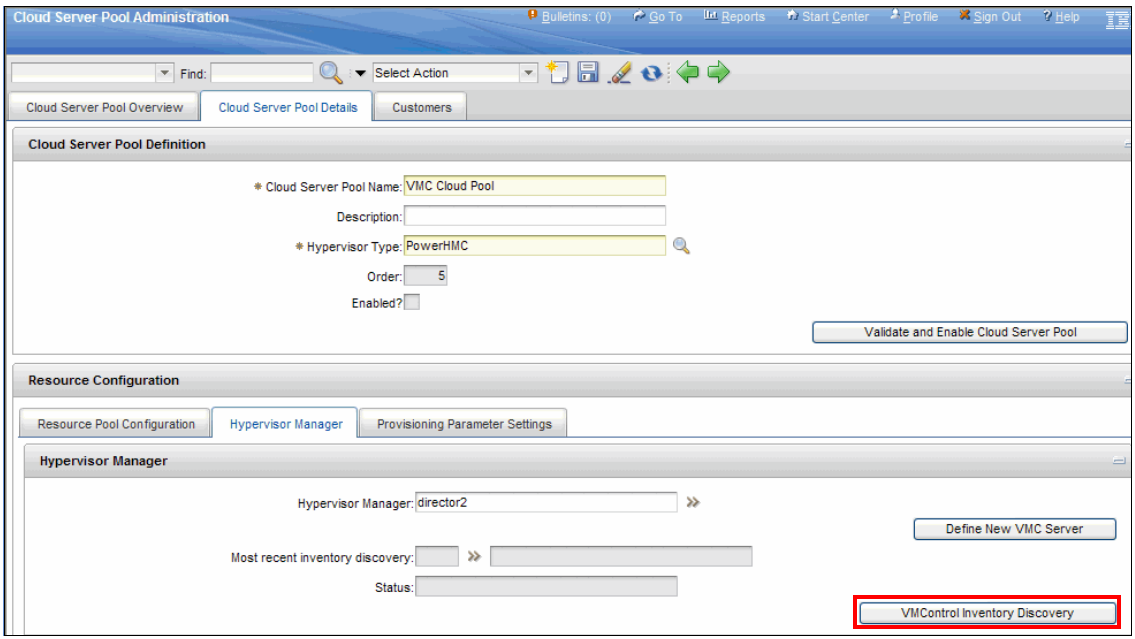

Figure 5-10 Selecting the hypervisor manager and collecting inventory

A system message appears, confirming the creation of the discovery workflow, as shown in Figure 5-11.

Figure 5-11 Workflow creation confirmation system message

Navigate back to the Start Center or click **Refresh**. You can see the progress of all your provisioning tasks, as shown in Figure 5-12.

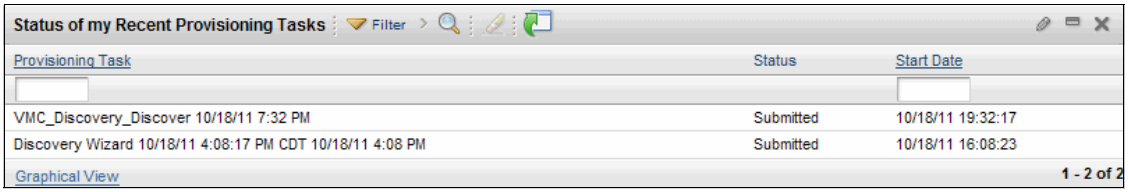

Figure 5-12 Provisioning tasks status on Start Center

Clicking the provisioning task allows you to track the workflow's progress, as shown in Figure 5-13.

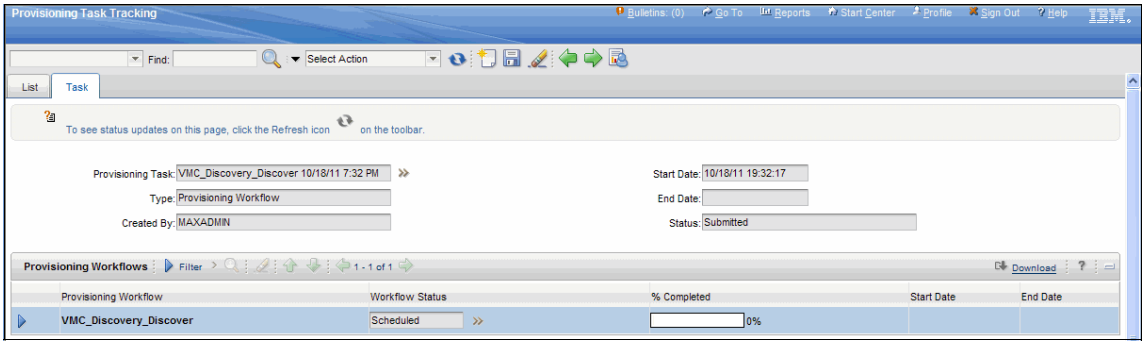

Figure 5-13 Provisioning Task Tracking panel

Alternatively, from the Start Center, click **Provisioning Workflow Status** in the Automation Development Applications section to obtain a list of provisioning tasks, as shown in Figure 5-14.

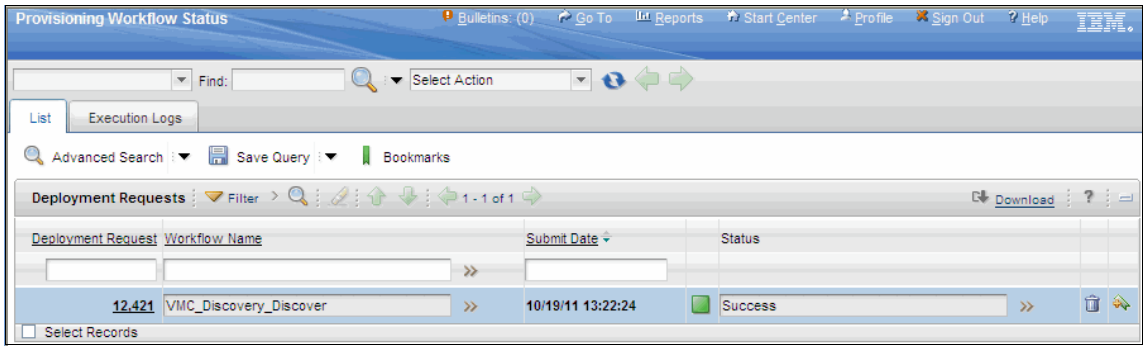

Figure 5-14 Provisioning Workflow Status panel

4. After discovery is complete, the next task is to specify which of the servers managed by VMControl will be part of this cloud pool. To do this, navigate back to Cloud Server Pool Administration using **Go To** → **Service Automation** → **Configuration** → **Cloud Server Pool Administration**, as shown in Figure 5-2 on page 122, and then click the **Cloud Server Pool Details** tab.

   Click **Add VMC Host** in the Resource Configuration section, also shown in Figure 5-9 on page 126. This presents you with the Add Host pop-up. Click **Select Value**, as shown in Figure 5-15.

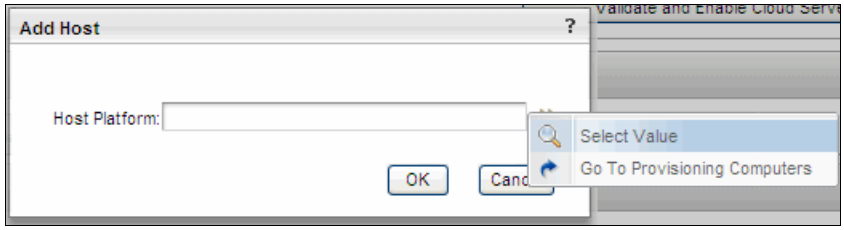

Figure 5-15 Add Host pop-up

This presents you with a list of available servers similar to that shown in Figure 5-16. If you have created a server system pool in VMControl, it will appear in the list. Click the one that you want to add to the cloud pool. In Figure 5-16, POWERCloudServerPool is a VMControl server system pool, and the POWER7-* entries are Power Systems. For this publication we chose the server system pool, as this simplifies the storage configuration.

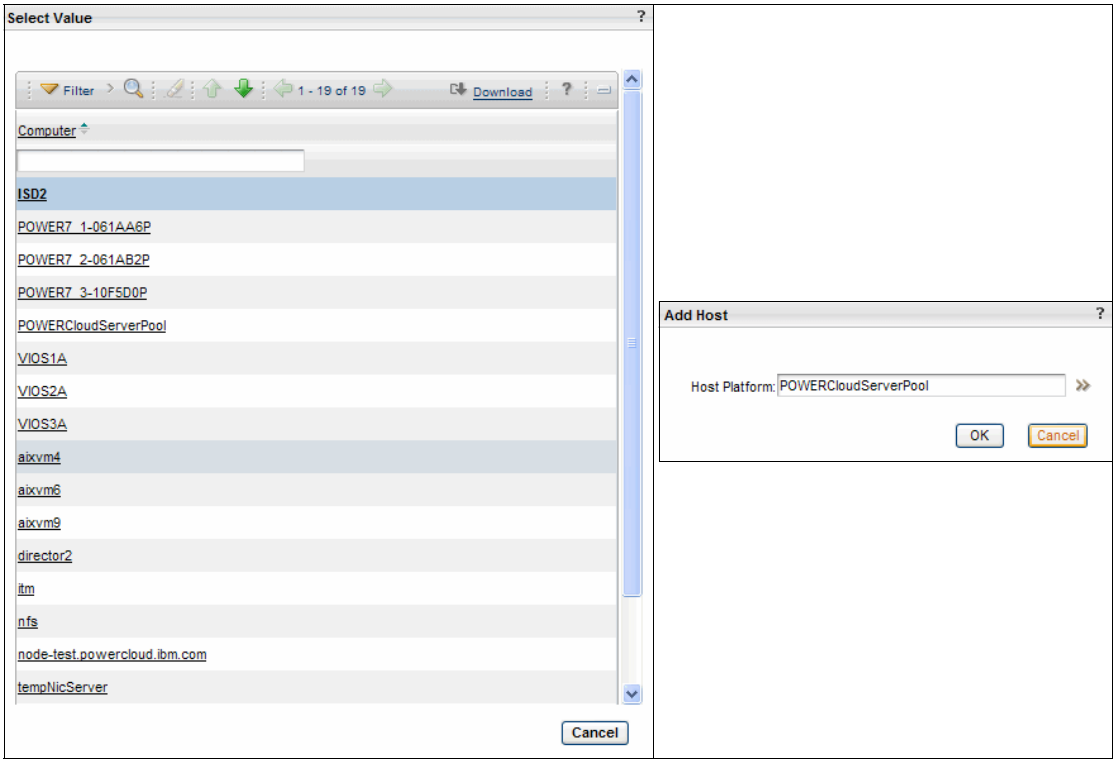

Figure 5-16 Server selection list

This fills out the Add Host pop-up, as shown in Figure 5-17. Click **OK**.

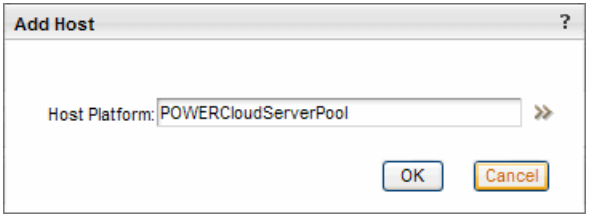

Figure 5-17 Filled out Add Host pop-up

Repeat this step for each server that you want to add to the pool.

5.4.4 Importing NetworkTemplate.xml

The following steps import the network template:

1. Navigate to **Go To** → **Service Automation** → **Configuration** → **Cloud Network Administration**, as shown in Figure 5-18.

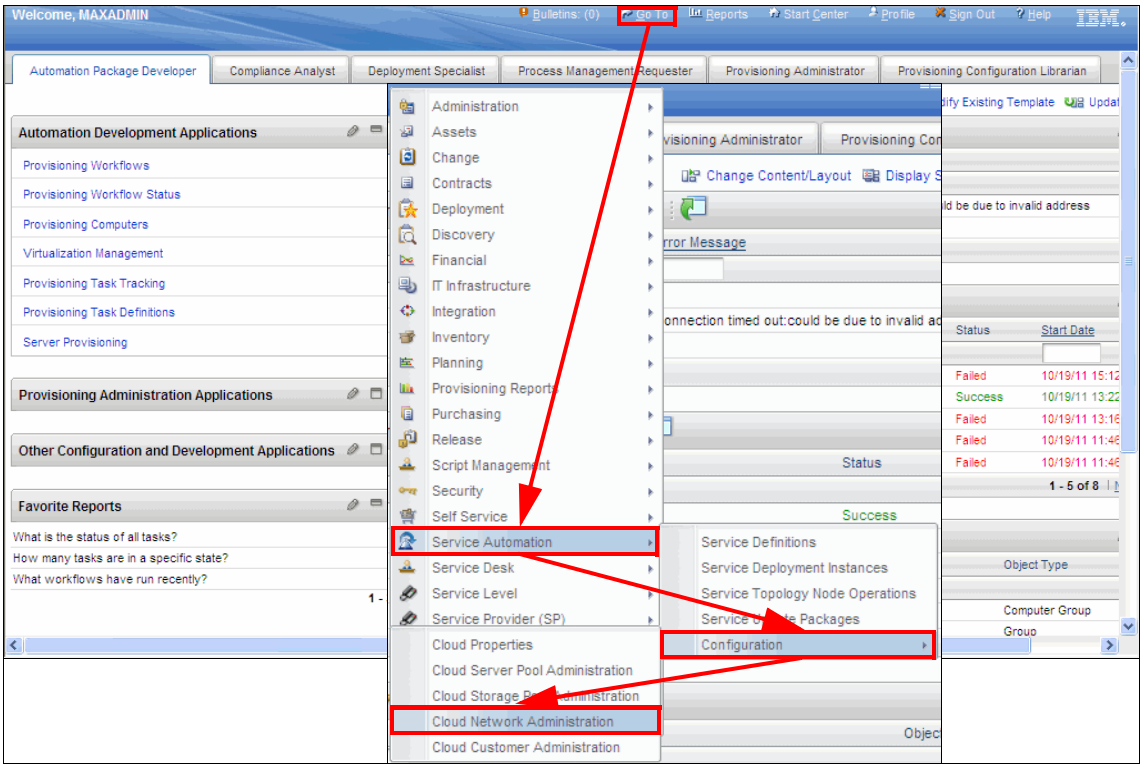

Figure 5-18 The cloud network administration interface

2. Click **Import Network template.xml**, as shown in Figure 5-19.

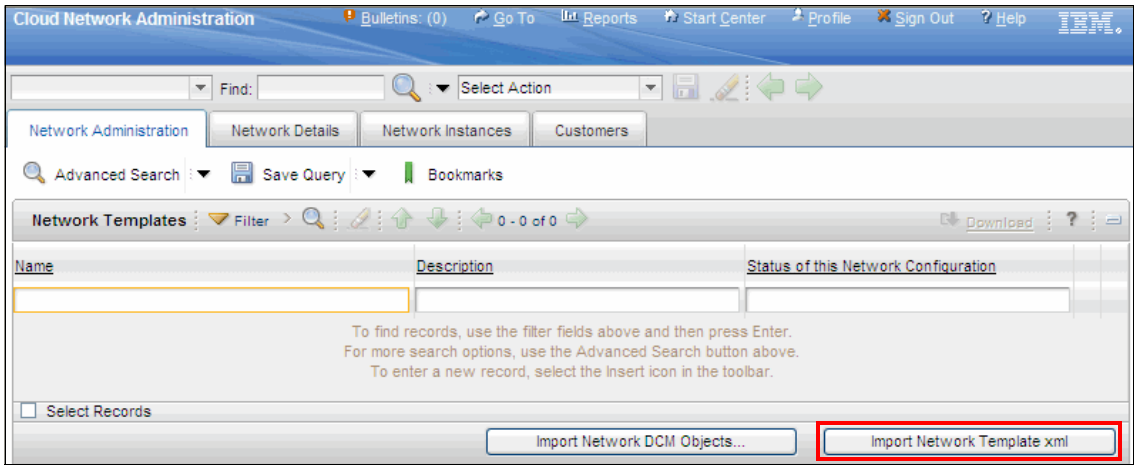

Figure 5-19 The Import Network template.xml button

3. Locate the `MyCloudNetwork.xml` file in your home directory and click I**mport**, as shown in Figure 5-20.

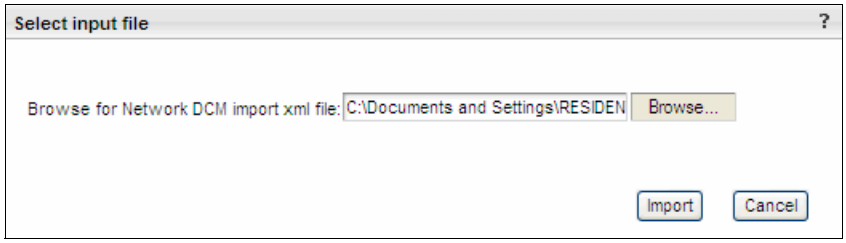

Figure 5-20 Importing the MyCloudNetwork.xml file

4. Click in the Name field and press Enter to list all network templates. Click the new imported template to view the network details, as shown in Figure 5-21.

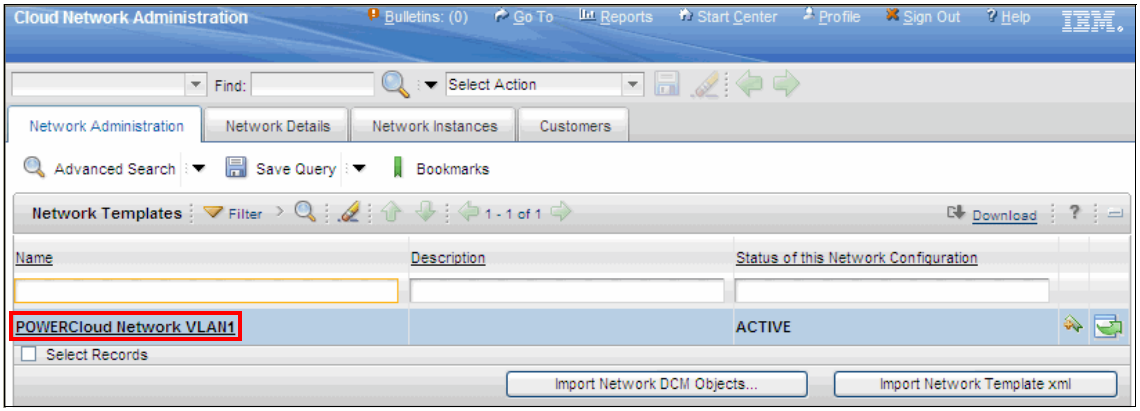

Figure 5-21 Click to view the network details

5. Click the magnifying glass icon next to the status of this network configuration property, as shown in Figure 5-22.

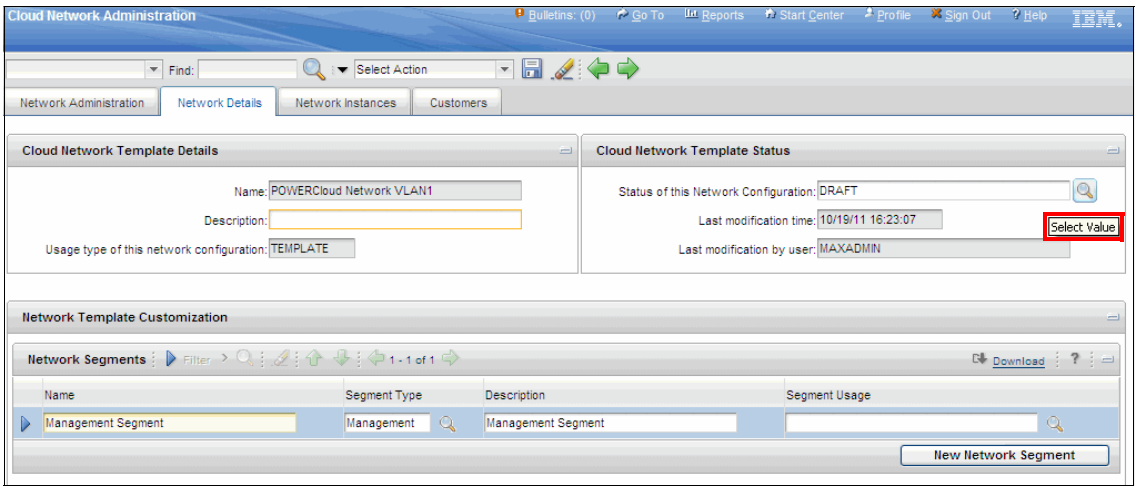

Figure 5-22 Network configuration status

6. From the newly opened status panel, click the **Active** value, as shown in Figure 5-23. This changes the template from draft to active status and makes the network available to the cloud.

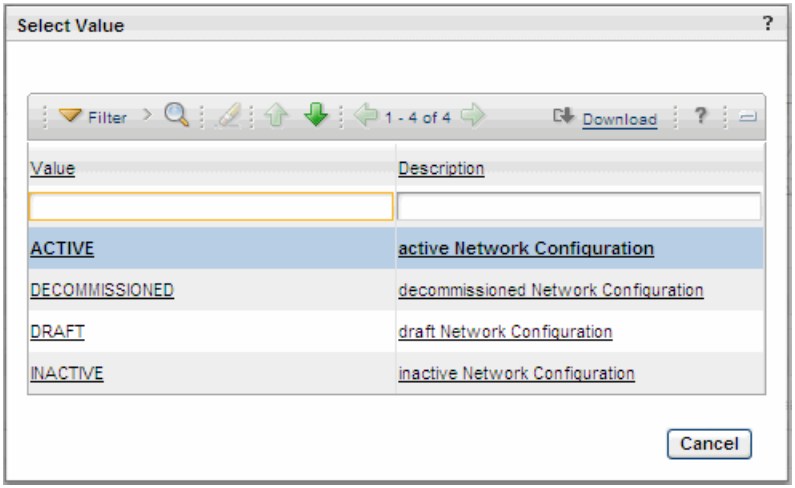

Figure 5-23 Change the network template status to active

7. Click **Save Network Configuration** to save the changes, as shown in Figure 5-24.

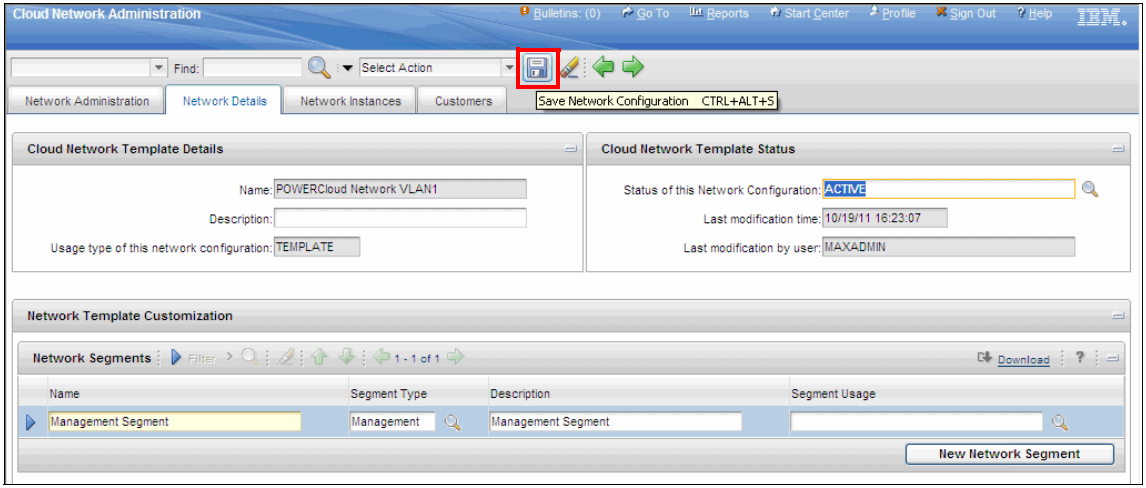

Figure 5-24 Save the template configuration

The network template is now ready to be assigned to a customer.

5.5 Validating the cloud server pool

You now validate and enable the pool. In the Cloud Server Pool Details tab of the Cloud Server Pool Administration application, click V**alidate and Enable**, as shown in Figure 5-25. You then see the validation confirmation pop-up shown in Figure 5-26.

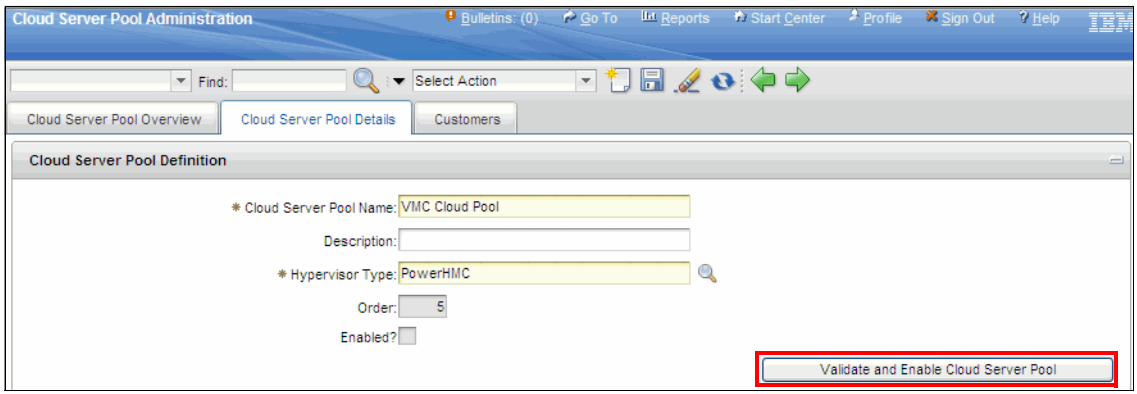

Figure 5-25 Validating and enabling the cloud server pool

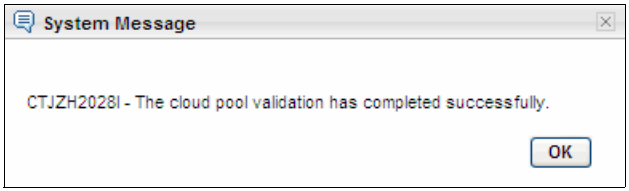

Figure 5-26 Cloud validation result

5.6 If you make a mistake

Re-importing the datacenter model files for a datacenter that is already defined within Tivoli Service Automation Manager can lead to erroneous configurations. If you made an error in one of your DCM files, then you have three options:

- If you have taken a backup of the Tivoli Service Automation Manager database prior to the import, then you can restore it as described in “Backing up the Tivoli Service Automation Manager database” on page 118.
- Delete the server pool and network definitions using Tivoli Service Automation administration interface (Maximo). Navigate to go to **Service Automation** → **Configuration** → **Cloud Server Pool Administration**. Click

the **Cloud Server Details** tab, then in the Select Action drop-down menu choose **Delete Cloud Server Pool**, as shown in Figure 5-27.

To delete the subnetworks, navigate to go to **IT Infrastructure** → **Provisioning Inventory** → **Subnetworks**. You are presented with the Subnetworks panel shown in Figure 5-28. Click on the red **X** to the right of the subnetwork that you want to delete.

Edit the `DCM_objects.xml` file to comment out the `<software-stack>` paragraph. Then re-import the datacenter model.

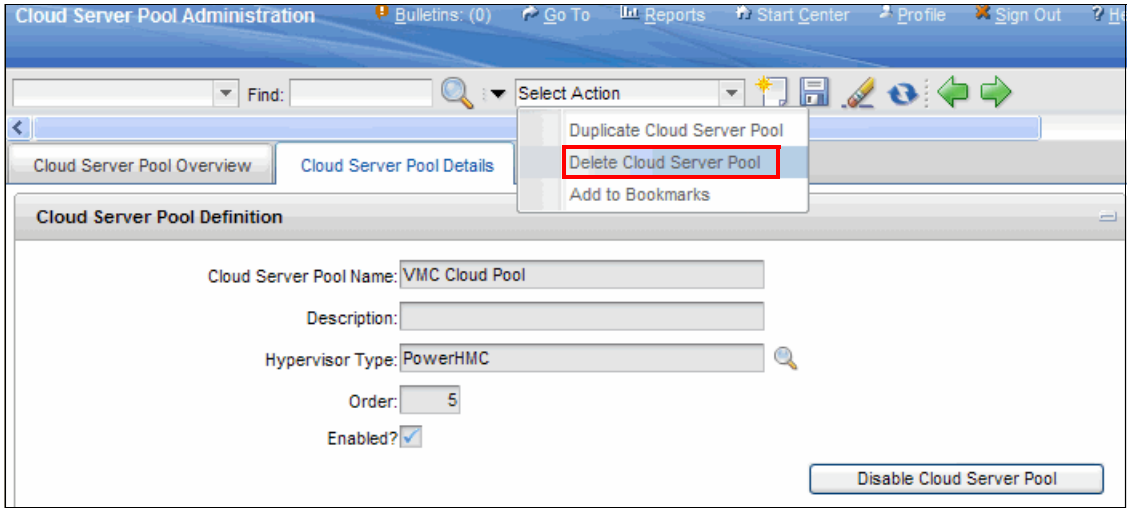

Figure 5-27 Deleting a cloud server pool

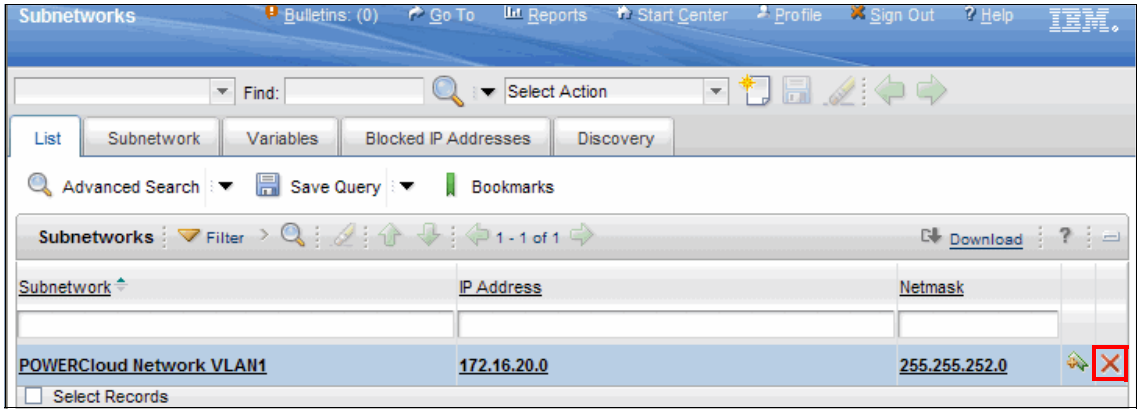

Figure 5-28 Deleting a subnetwork

- If the modifications are small, then you can make the changes directly through the Tivoli Service Automation Manager's administration interface.

6

Creating customers and assigning resources

After the IBM Service Delivery Manager servers have been deployed and the cloud environment is up and running, you can start creating the basic building blocks for providing cloud services. This chapter describes these topics:

- Creating a customer template from the Tivoli Service Automation Manager administration interfaces
- Assigning resources to the customer template
- Using the Tivoli Service Automation Manager Self Service Portal to create customers, users, and teams
- Checking the status of workflows

6.1 Overview

The ability to create and manage more than one customer is a new feature of IBM Service Delivery Manager 7.2.2. It is now possible to create different customers, each with his own separate set of cloud resources. The customers are totally isolated from each other.

Tivoli Service Automation Manager provides a default global customer called PMRDPCUST. The administrator can create a new customer and associate him with cloud resources in preparation for cloud services. Cloud customer administration is performed in the Tivoli Service Automation Manager administrative interface.

6.2 Administration interfaces and preparations

To perform cloud administration tasks, log in to the Tivoli Service Automation Manager administrative interface. To perform team and user tasks, log in to the Self Service Portal interface. Table 6-1 lists the interfaces and specific user IDs that we work with.

Table 6-1 Web interfaces for administrative or user tasks

Interface	URL	Default user ID	password
Tivoli Service Automation Manager administrative interface	`https://<nfs_imager>:9443/maximo`	maxadmin	password
Tivoli Service Automation Manager Self Service Portal	`https://<nfs image>:9443/SimpleSRM`	PMRDPCAUSR	maxadmin
Online Help	`http://<nfs_image>:9060/ibm/help`	none	none

Preparations for a new cloud customer

A customer is associated with resources such as hypervisors and storage. When a customer is created, a network definition is the only mandatory requirement. Other cloud resources can be added or removed from the customer after creation.

Network template

The Tivoli Service Automation Manager administrator creates network configurations, which are imported as network templates. When a customer is

created, these network templates are listed in the cloud network configuration tab. One or more networks can be assigned to a customer.

Cloud server pools

The Tivoli Service Automation Manager administrator creates cloud server pools for deploying virtual images. For a customer to provision images, they require a cloud server pool assigned to the customer. A list of available cloud server pools is presented to the customer at creation time.

Other resources

The following resources are optional at customer creation time. These resources can be assigned after the customer has been created:

- Cloud storage pool
- Master images
- Software modules

6.3 Creating customers

A customer is the highest category that is used for managing cloud environment resources. To create a specific customer with different currency and resources:

- Select an existing customer template that matches the requirements or create a new customer template.
- Use the TIVSAM self-service user interface to create the customer and select the appropriate customer template.

In practice, this customer contains account information for a company or a client that signs the cloud service contracts. You create a customer template to record specific information for this client. This information is retrieved automatically in customer accounting, service reports, and billing statements. For example:

- The client might speak a different language. The customer template provides many language options.
- They might use a different currency.
- Each client usually has a different website.
- You also want to record the customer starting date for billing purposes.
- From past billing activities, you can note the client credit rating.

Based on the customer template, the client administrators create teams and users for their projects.

6.3.1 Creating a customer template

A customer template represents a customer definition. When a Tivoli Service Automation Manager administrator creates a customer, it can be saved as a template. Customers can be created using the previously created customer template.

Creating and using a customer template is a good way to create multiple customers who share the same cloud resources.

In the following steps, we create a customer template for the customer CLOUDCUSTOMR. This customer uses the USD currency and has a network resource assigned to it:

1. Log in to the Tivoli Service Automation Manager administrative interface as a user with the cloud administrator role:

   `https://<nfs_image>:9443/maximo`

   Where *<nfs_image>* is the host name or IP address of your NFS virtual appliance.

2. From the Tivoli Service Automation Manager home page, click **Go To** → **Service Automation** → **Configuration** → **Cloud Customer Administration**. Figure 6-1 shows the look of those menus and the Cloud Customer Administration panel.

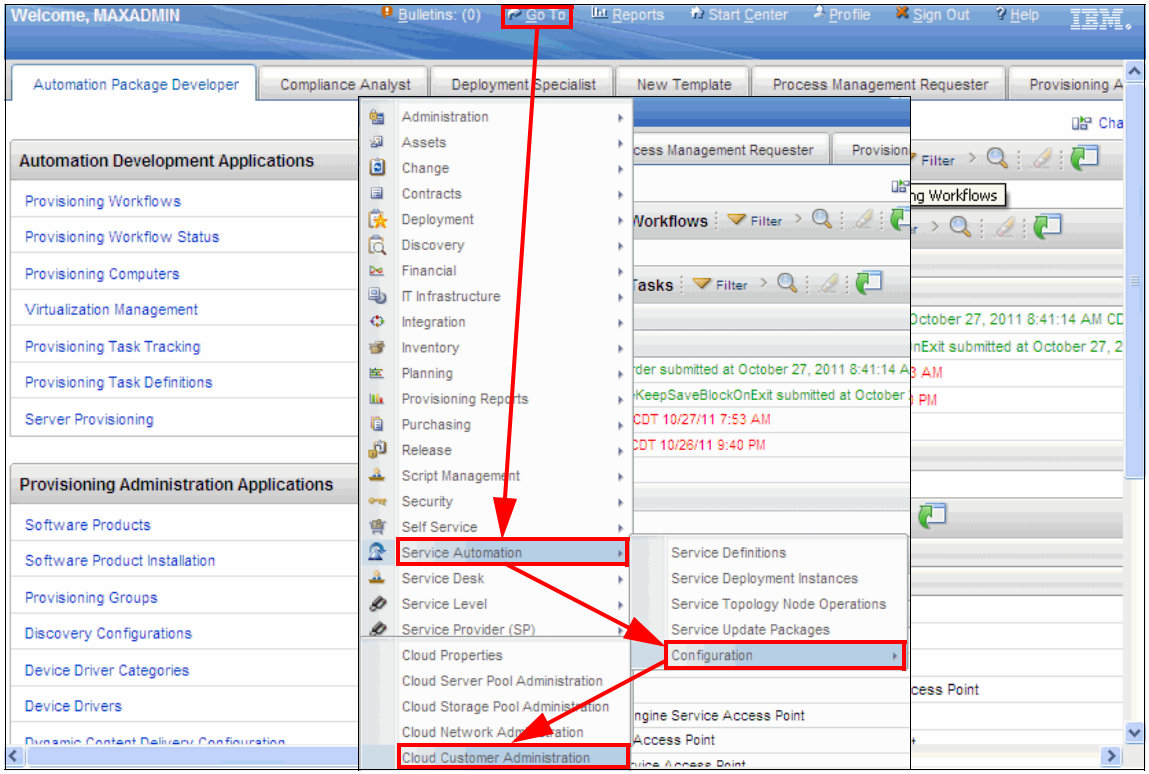

Figure 6-1 Menus leading to the Cloud Customer Administration panel

3. To create a new customer template, click the new customer icon on the tool bar, as shown in Figure 6-2.

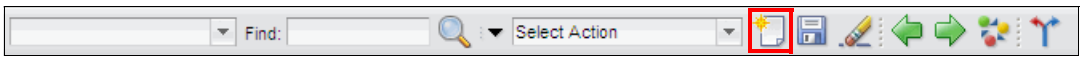

Figure 6-2 New customer icon

4. The new customer panel opens. The compulsory fields are *Customer and *Customer Currency. Click in the **Customer** text box and enter the name of your customer template. In our example we entered the name PCTemplate, as shown in Figure 6-3.

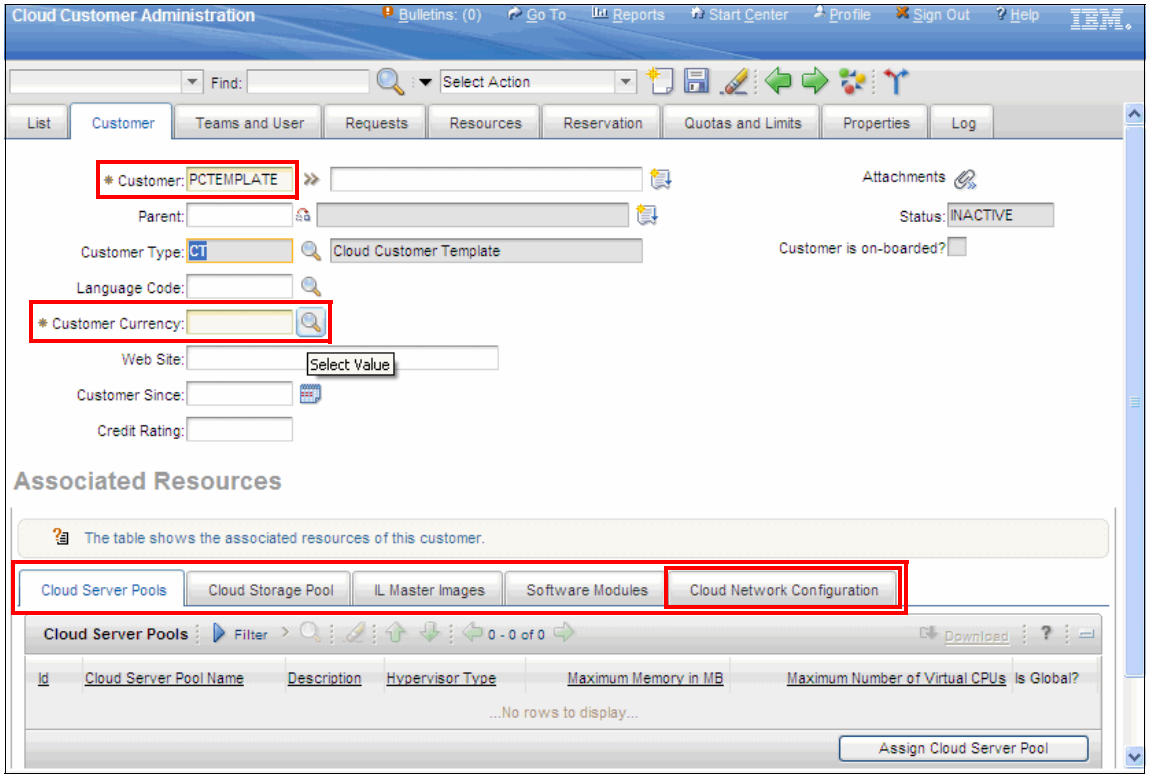

Figure 6-3 The new customer template panel

The Customer Type field is filled with the value CT for Cloud Customer Template by default. The value cannot be changed because we are creating a customer template.

Note: A customer template name can contain a maximum of 12 characters.

5. Select the currency of your choice by clicking the magnifying glass on the right side of the Customer Currency field, as shown in Figure 6-3 on page 142.

   The available currencies for IBM Service Delivery Manager are the US dollar and the Euro. More currencies can be added to IBM Service Delivery Manager, but they are out of scope for this publication. In our example we selected US dollars by clicking **USD** in the Select Value dialog (Figure 6-4).

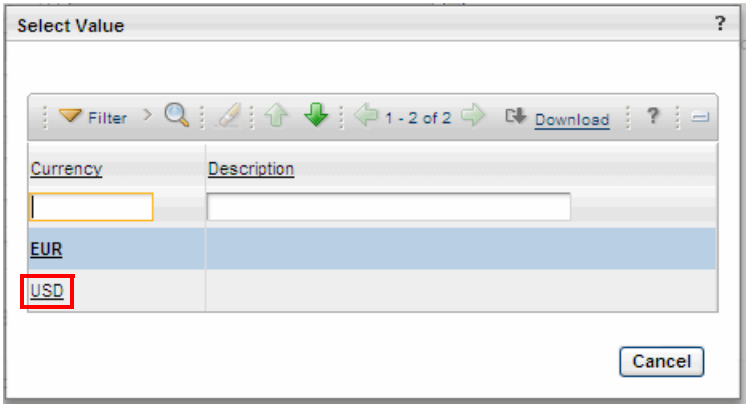

Figure 6-4 Customer information panel and the select value dialog box

6. To assign resources to the customer template, click the resource tabs at the bottom of the customer panel:
   - Cloud server pools: To assign cloud server pools to a customer, see 6.5.1, “Assigning a cloud server pool to a customer” on page 173.
   - Cloud storage pool.
   - Master images: To assign master images to a customer, see 6.5.2, “Assigning a virtual image to a customer” on page 178.
   - Software modules.
   - Cloud network configuration (covered in section).

   The tabs are highlighted as shown in Figure 6-3 on page 142. Each of the tabs is used to assign default resources to the customer template. These are basic resources for the customer at creation. After they are created, it is possible to customize a customer to provide additional resources and functionality at a later time.

   In our scenario we have not added any extra resources to our template. Cloud resources will be added to our customer when the customer is created.

7. To save the customer information, click the save customer icon on the tool bar, as shown in the Cloud Customer Administration panel in Figure 6-3 on page 142. You can see the tool bar icons in Figure 6-5. The customer is now saved in a template.

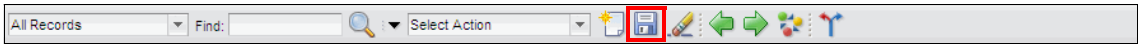

Figure 6-5 Save the customer template

8. The customer template is in an inactive state when first created. A Tivoli Service Automation Manager administrator needs to change the status of the template to active to make it available.

   To change the status of the customer template to active, click the change status icon on the tool bar, as shown in Figure 6-6.

Figure 6-6 Changing the customer status

9. This opens the change status dialog box. The new status field entry has a drop-down menu. Click the menu to select **Active**, then click **OK**, as shown in Figure 6-7.

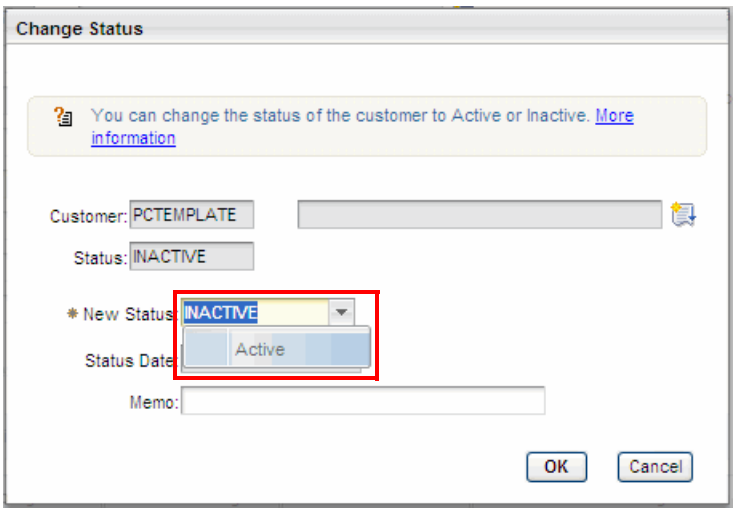

Figure 6-7 Change the state of the template

The customer template is now in active state and is ready for use by a customer, as shown in Figure 6-8.

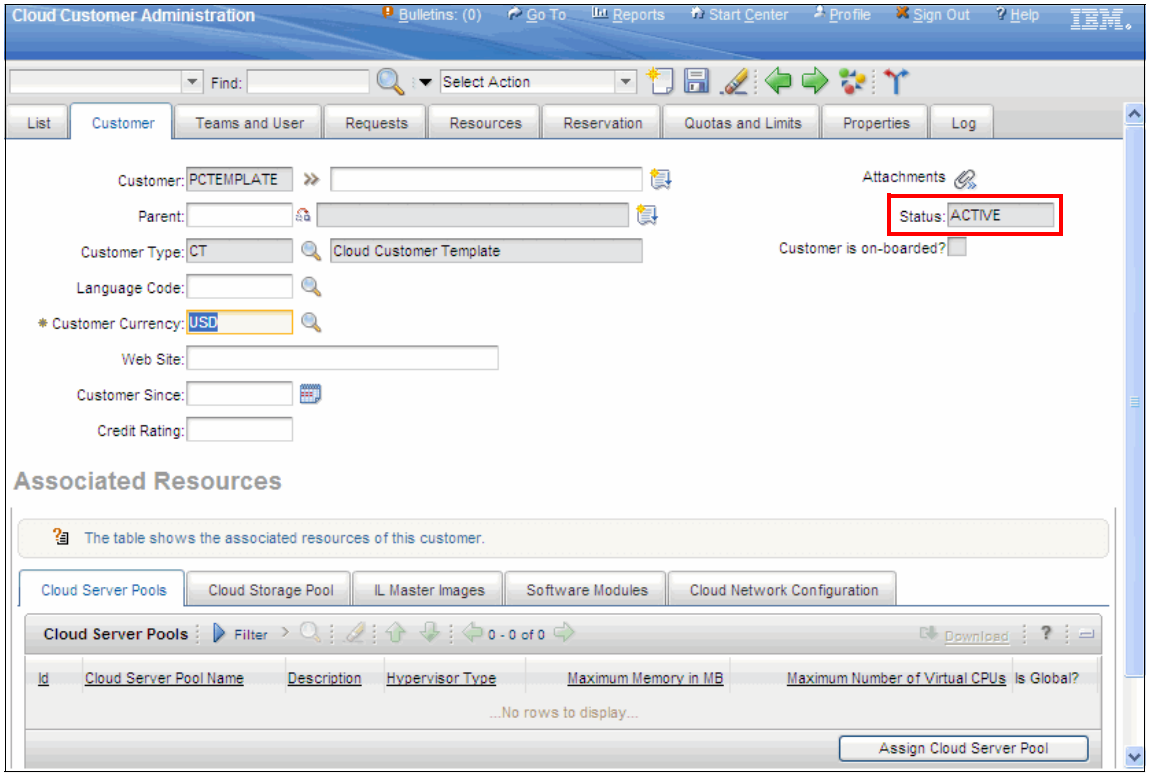

Figure 6-8 An active template

6.3.2 Modifying a customer template

Customer information can be changed or resources can be added or removed after the customer creation.

Note: Modifying a customer template might affect customers, teams, or users associated with this customer.

To modify the information of a customer, perform the following tasks:

1. From the Tivoli Service Automation Manager menu, click **Go To** → **Service Automation** → **Configuration** → **Cloud Customer Administration**, as previously shown in Figure 6-1 on page 141.
2. Press the Enter key on your keyboard to display all of the customers and customer templates.
3. Open the customer information by clicking the customer name in the list. In our example we selected the PCTemplate, as shown in Figure 6-9.

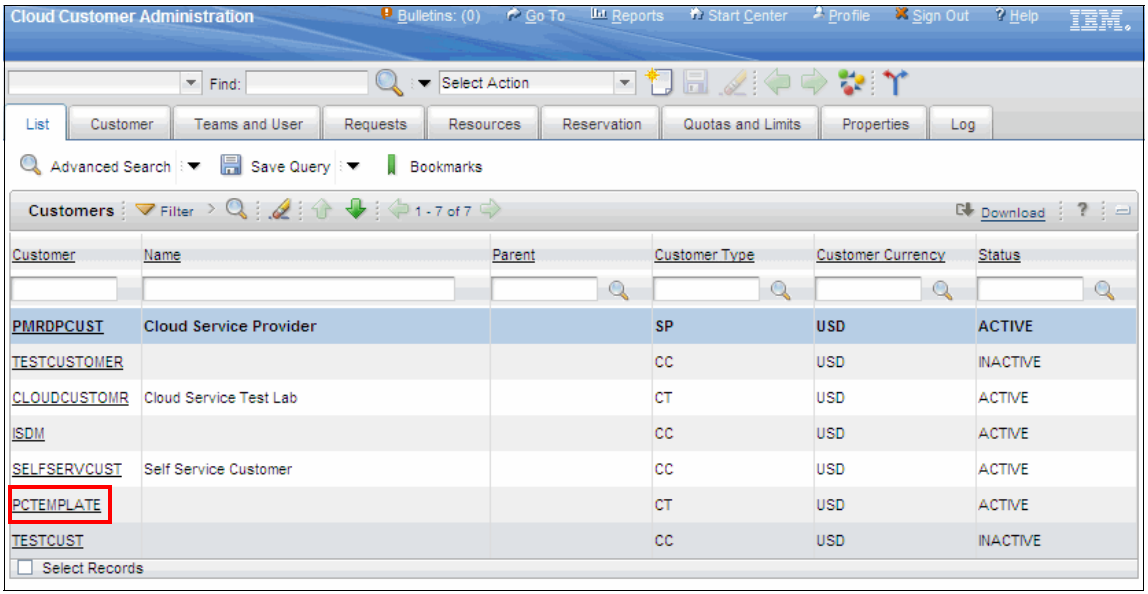

Figure 6-9 Clicking the customer name to display information

4. In the customer panel (Figure 6-10), add or remove resource objects. Then click the save customer icon on the tool bar, as shown in Figure 6-5 on page 144.

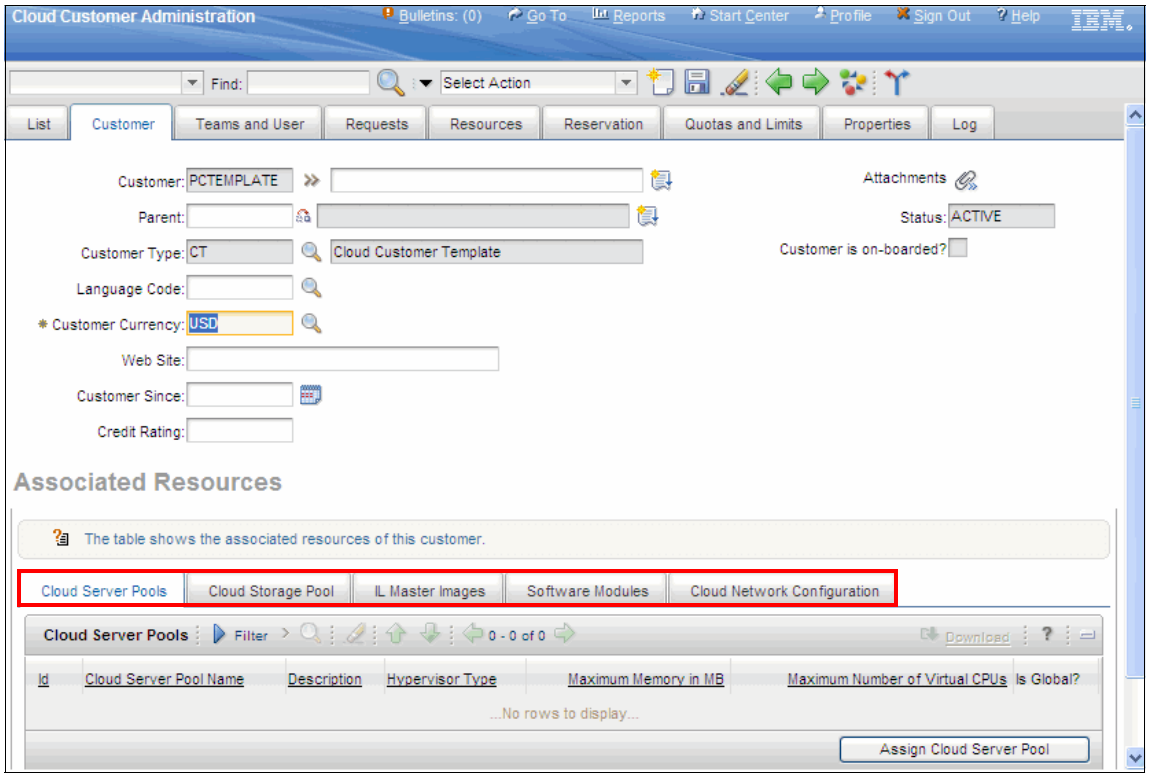

Figure 6-10 The customer information

6.3.3 Creating a customer

To create a customer in the cloud environment, perform the following tasks:

1. Log in to the Self Service Portal (`https://<nfs_image>/SimpleSRM`) as a user ID with the cloud administrative role. We used the default user ID PMRDPCAUSR, as shown in Figure 6-11. The default password for PMRDPCAUSR is maxadmin.

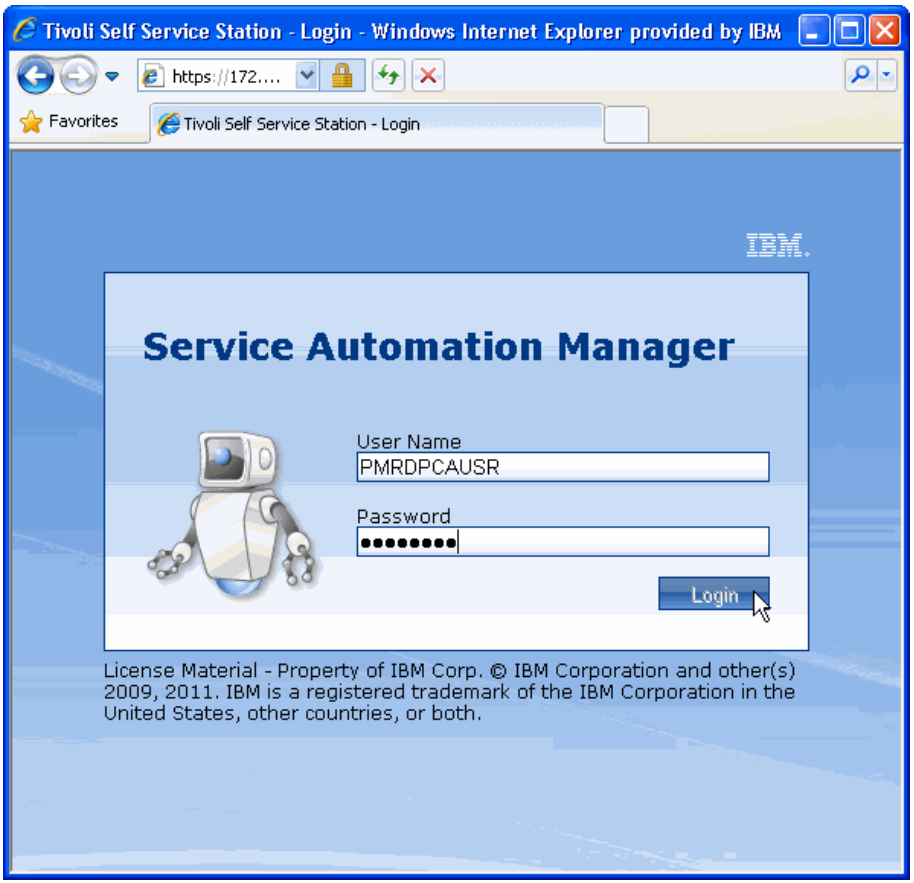

Figure 6-11 Self Service Portal login page

2. At the Self Service Portal home page, click **Request a New Service**, as shown in Figure 6-12.

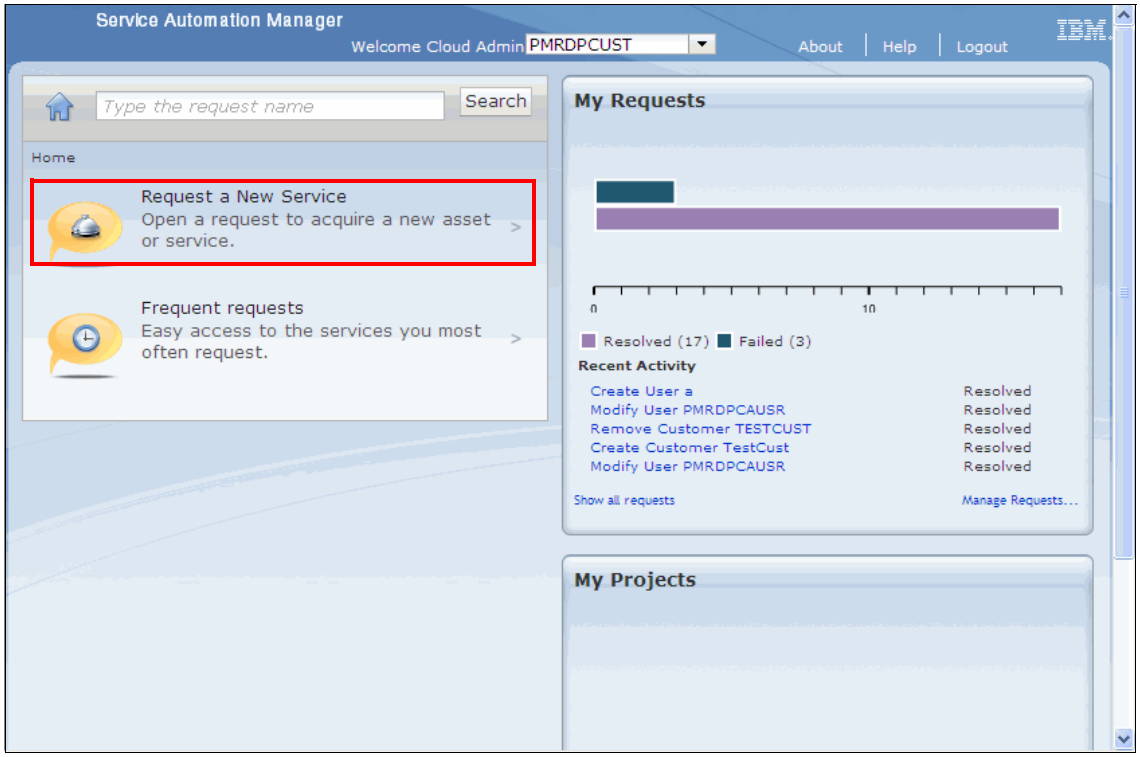

Figure 6-12 Request a new service

3. Click the **Virtual Server Management** icon, as shown in Figure 6-13.

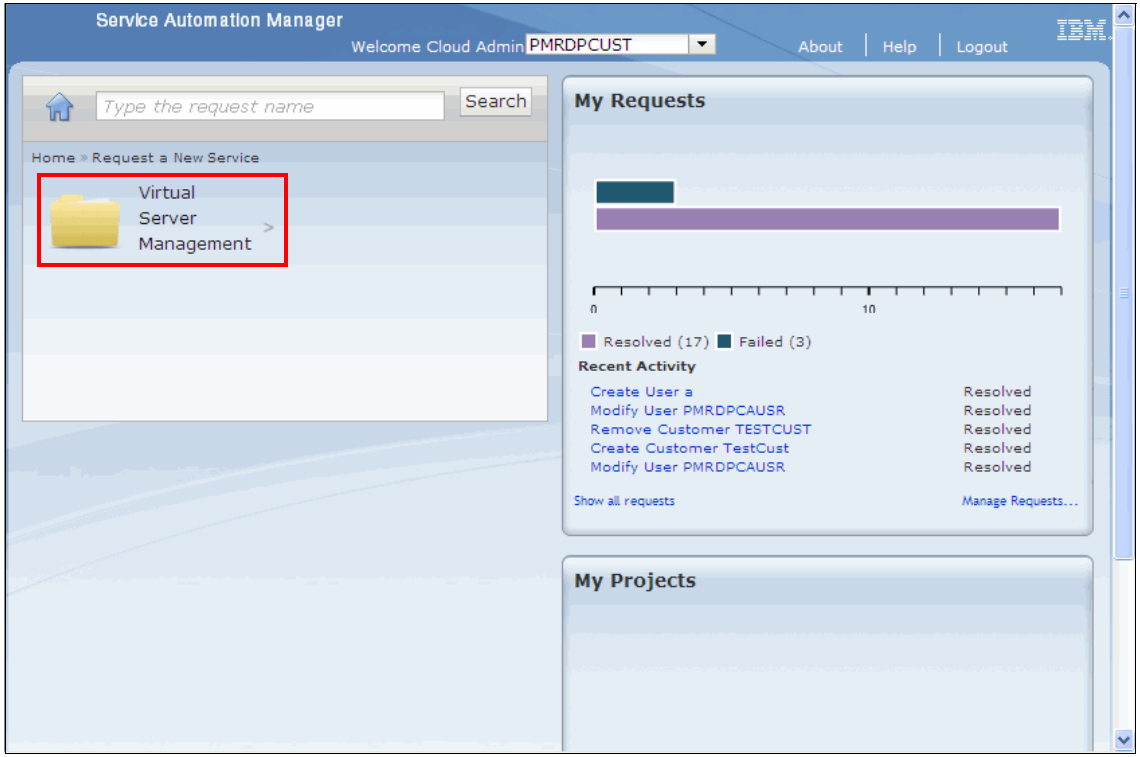

Figure 6-13 Managing virtual servers

4. Click the **Manage Customers** icon, as shown in Figure 6-14.

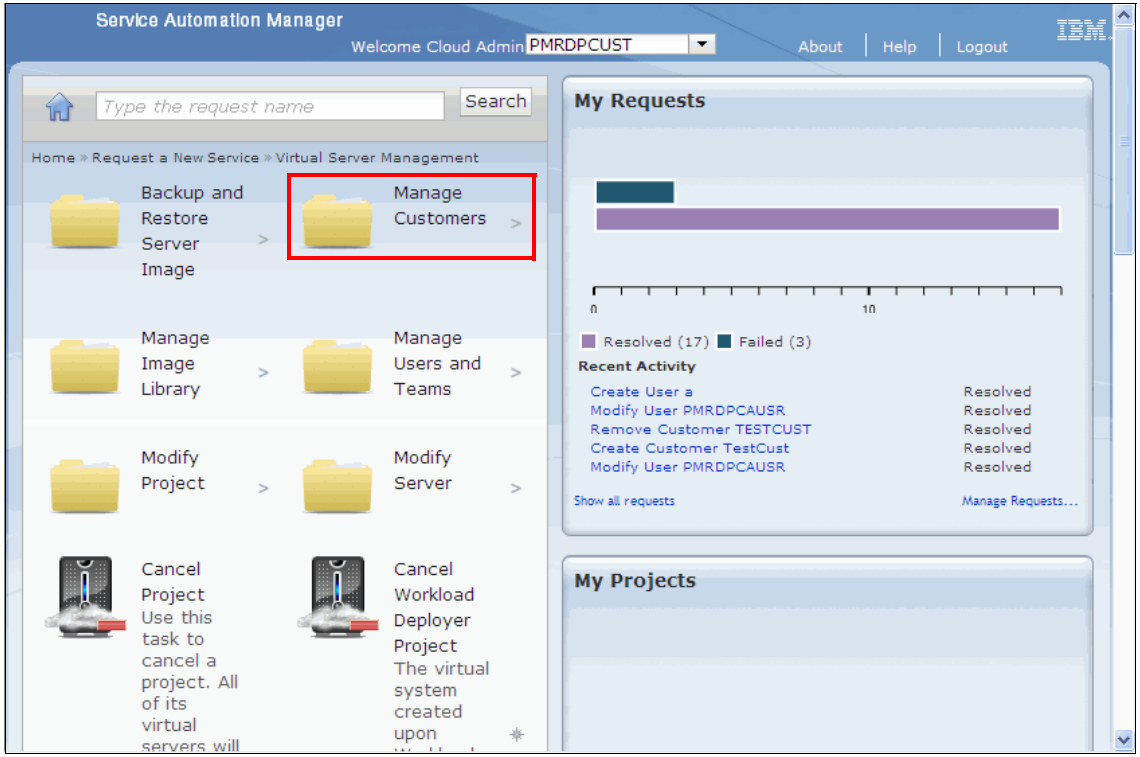

Figure 6-14 Manage Customers

5. Click **Create Customer**, as shown in Figure 6-15.

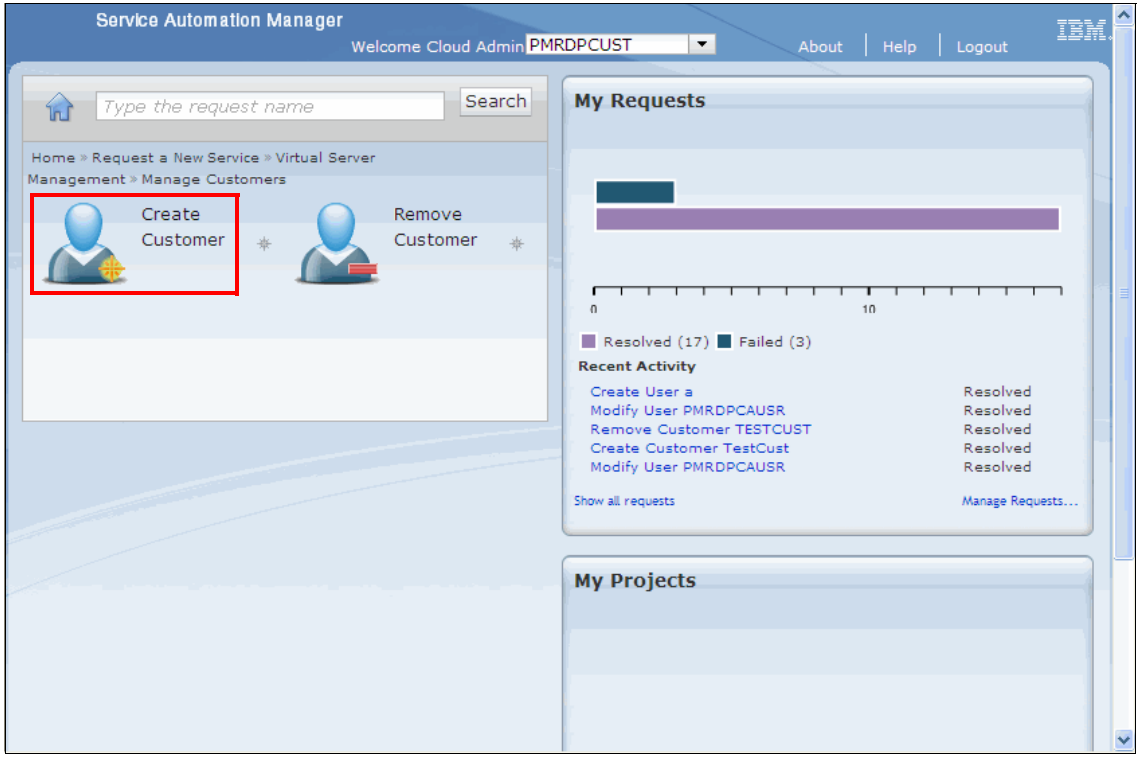

Figure 6-15 Create customer

6. The create customer dialog box opens. Enter a unique customer name. These are the fields to complete:

***Name**	The unique name of the customer
Customer Template	The customer template
***Network Configuration Template**	The network configuration for the customer
***Language**	The language for users of the customer
Description	A description of the customer

A field starting with an asterisk (*) is a compulsory field. If the Tivoli Service Automation Manager administrator has not created a customer template, the default template is available. Figure 6-16 shows an example of the create customer panel with completed fields. A field entry with a drop-down menu provides the available choices.

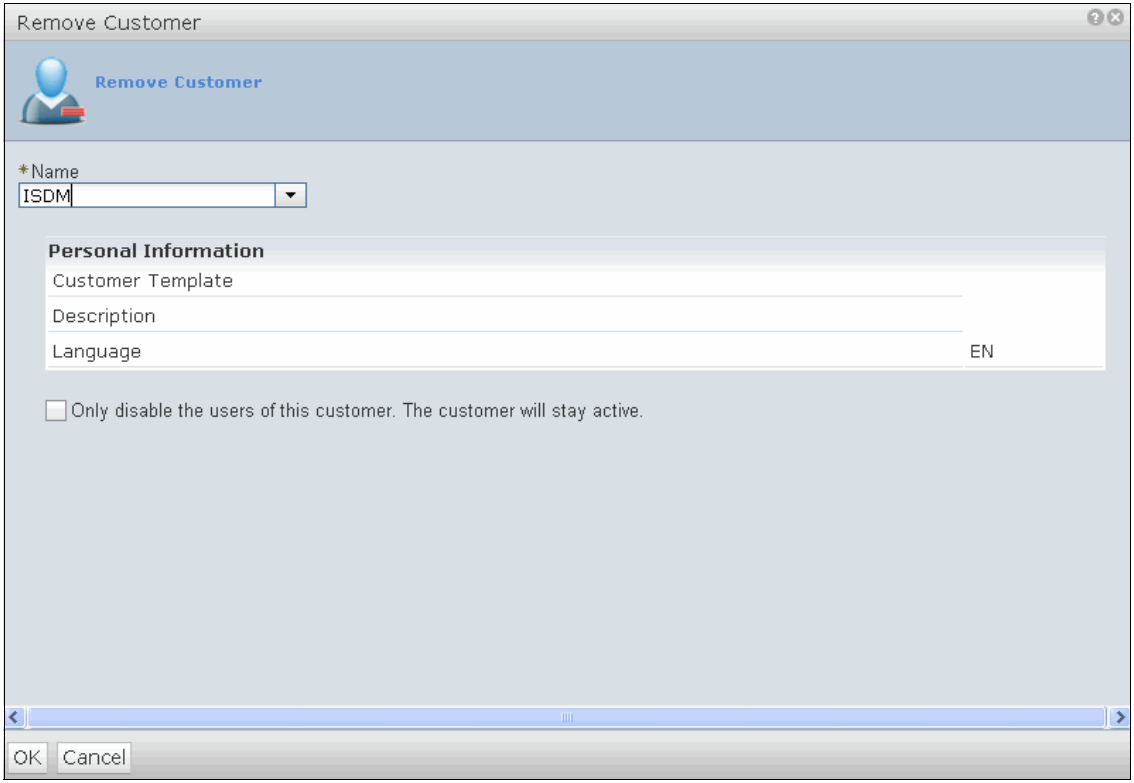

Figure 6-16 Self Service Portal create customer panel

These are the values that we used to create our customer:

Name	PowerCloud
Customer Template	CLOUDCUSTOMR
Network Configuration Template	POWERCloud Network VLAN1
Language	English

6.3.4 Removing customers

In practice, when a customer ends her service, the customer should be removed.

To remove a customer perform the following steps:

1. From the home page, follow the links **Request a New Service** → **Virtual Server Management** → **Manage Customers**.
2. Click **Remove Customer** icon, as shown in Figure 6-17.

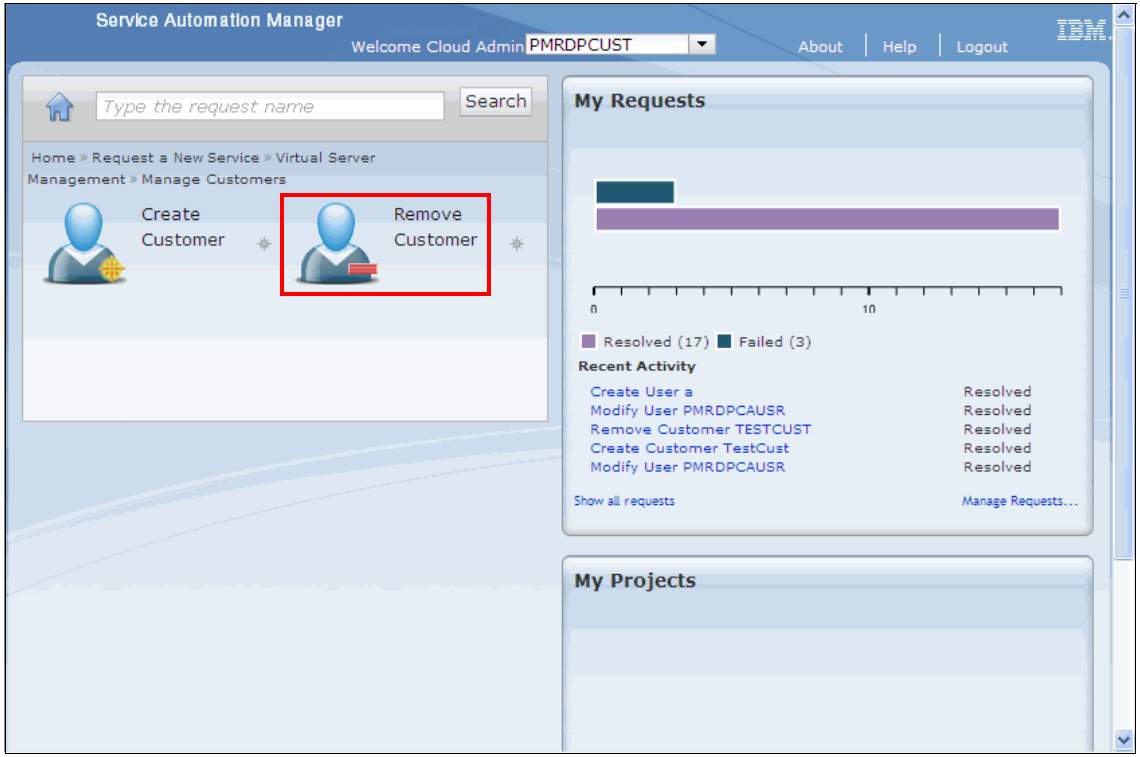

Figure 6-17 Selecting Remove Customer

3. The Remove Customer dialog displays, as shown in Figure 6-18. Click the drop-down menu to choose the name of the customer that you want to remove. Click **OK** to remove the customer.

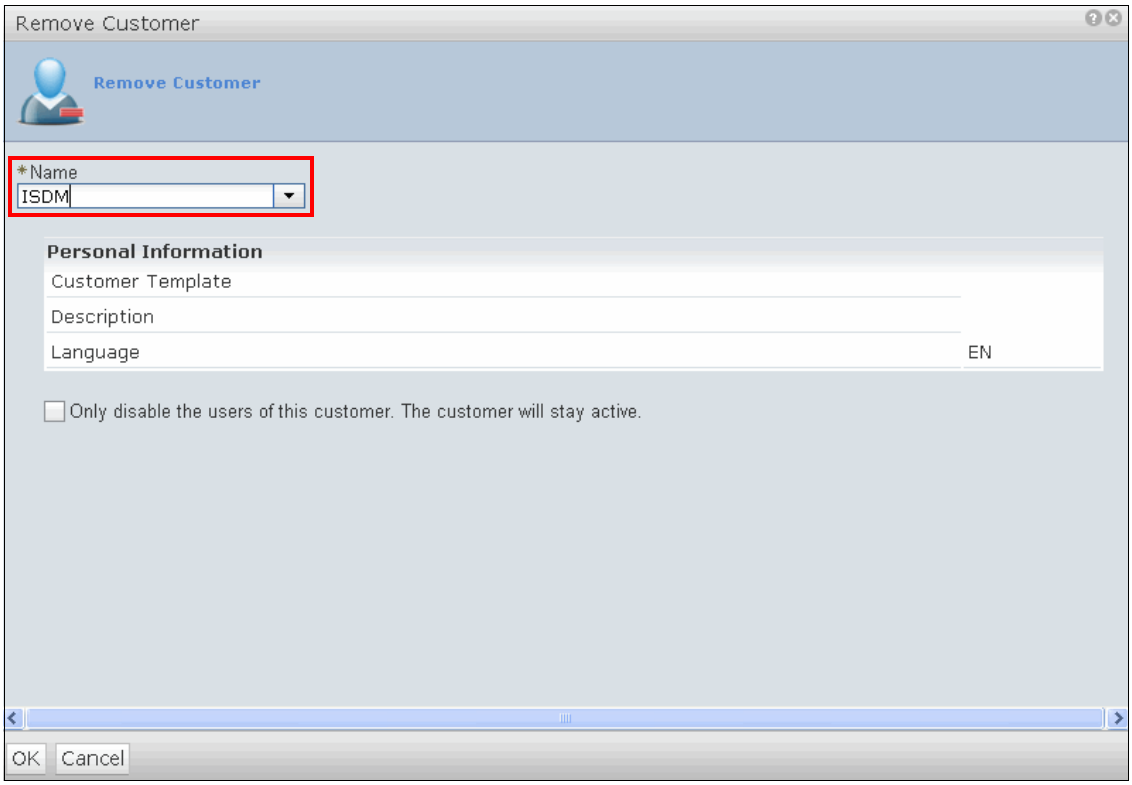

Figure 6-18 Removing a customer

The customer has been removed from IBM Service Delivery Manager. Any users and teams who were assigned to that customer are no longer able to use the resources assigned to that customer.

6.4 Creating teams and users

A team represents a group of users used to represent a project team. As an example, we create a team and two users. The team will be associated with a project that we create later.

6.4.1 Creating a team

Take these steps to create a team in the cloud environment:

1. Log in to the Self Service Portal (`https://<TSAM>/SimpleSRM`) as a user ID with the cloud administrative role, as shown in Figure 6-11 on page 148. We used the default user ID PMRDPCAUSR.
2. At the home page, click **Request a New Service** → **Virtual Server Management** icons.
3. Click the **Manage Users and Teams** icon, as shown in Figure 6-19.

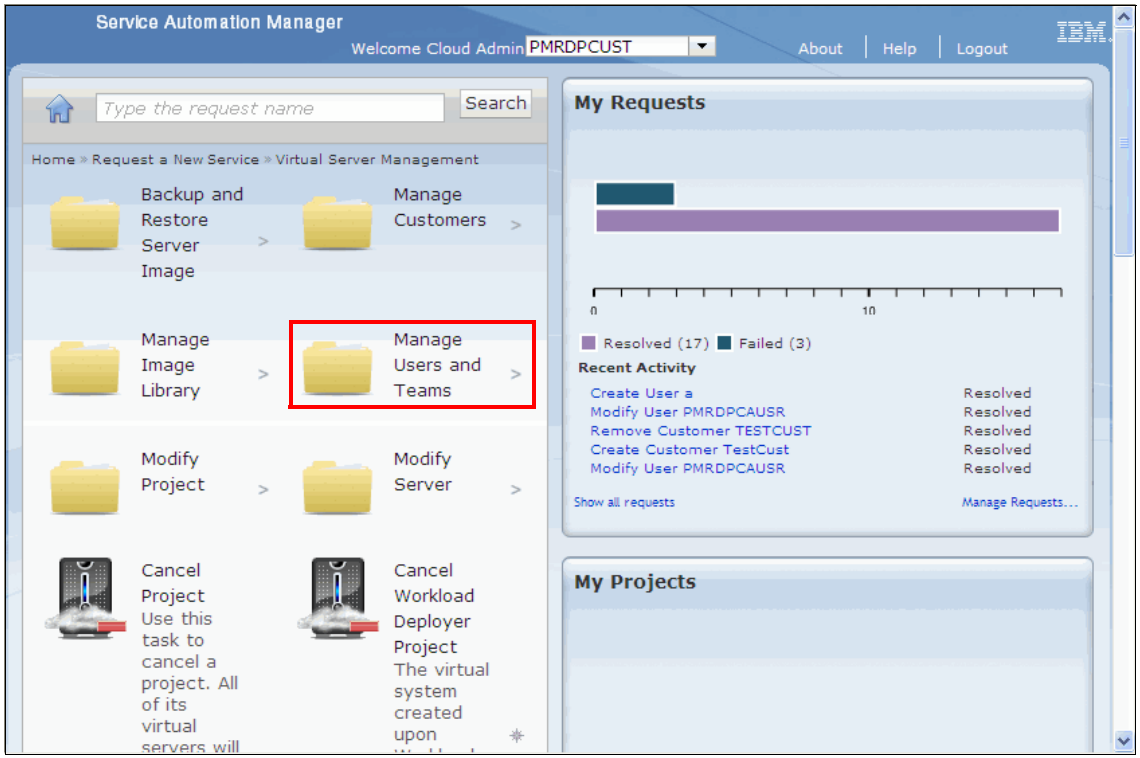

Figure 6-19 Manage users and teams

4. Click the **Create Team** icon, as shown in Figure 6-20.

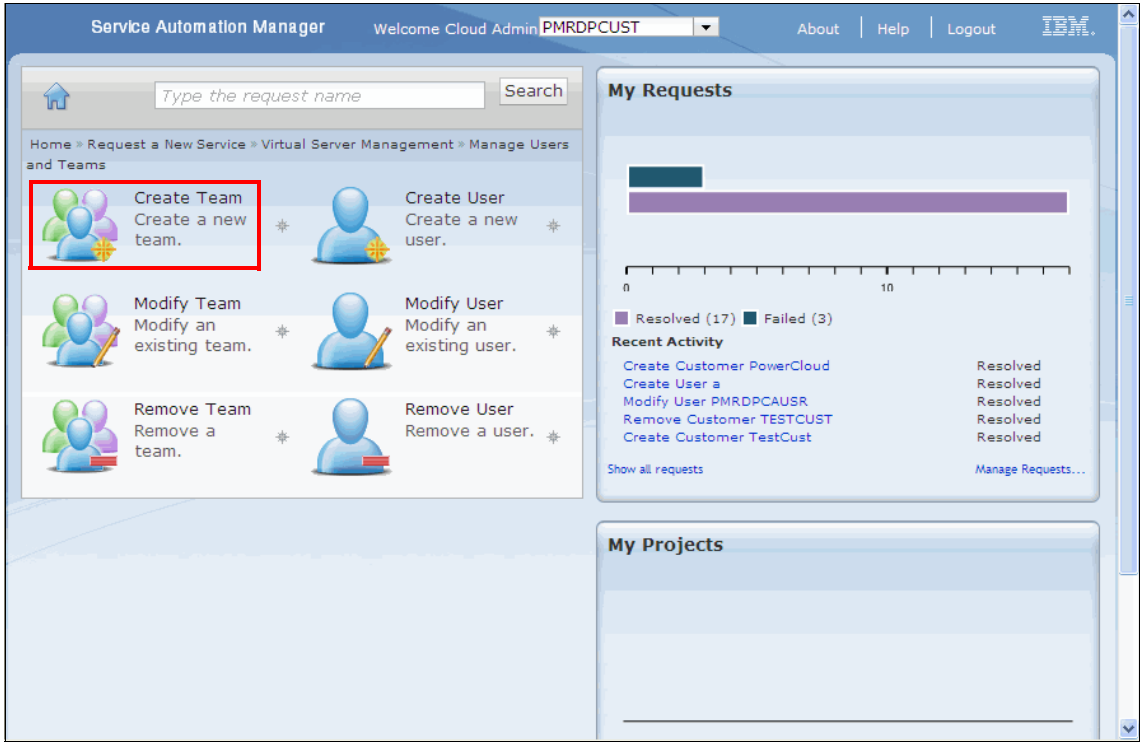

Figure 6-20 Create a team

5. The Create Team dialog displays, as shown in Figure 6-21. Give your team a unique name. Users can be added to the team by selecting the user and clicking the right arrow button in the dialog box to move the user from the Available Users list to the Selected Users list.

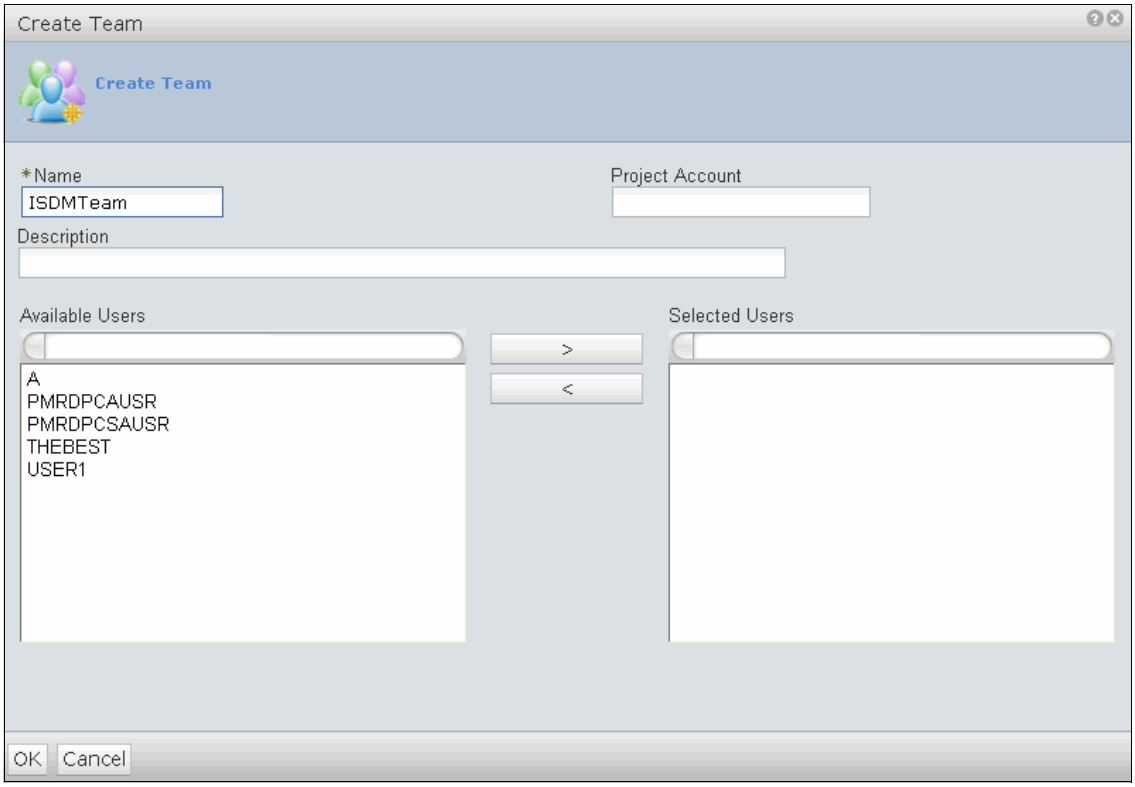

Figure 6-21 Enter team details

In our example we added a team named ISDMTeam, which current contains no users.

Notes: A team name must be unique and has a maximum of eight characters.

The Tivoli Usage and Accounting Manager reporting function requires each team in the self-service user interface to belong to a project account.

6. Check that the create team request has completed successfully by monitoring the resolved requests in the requests panel on the right side of the window, as shown in Figure 6-22. If the request does not display, click the **Show all requests** link in the lower left corner of the requests panel.

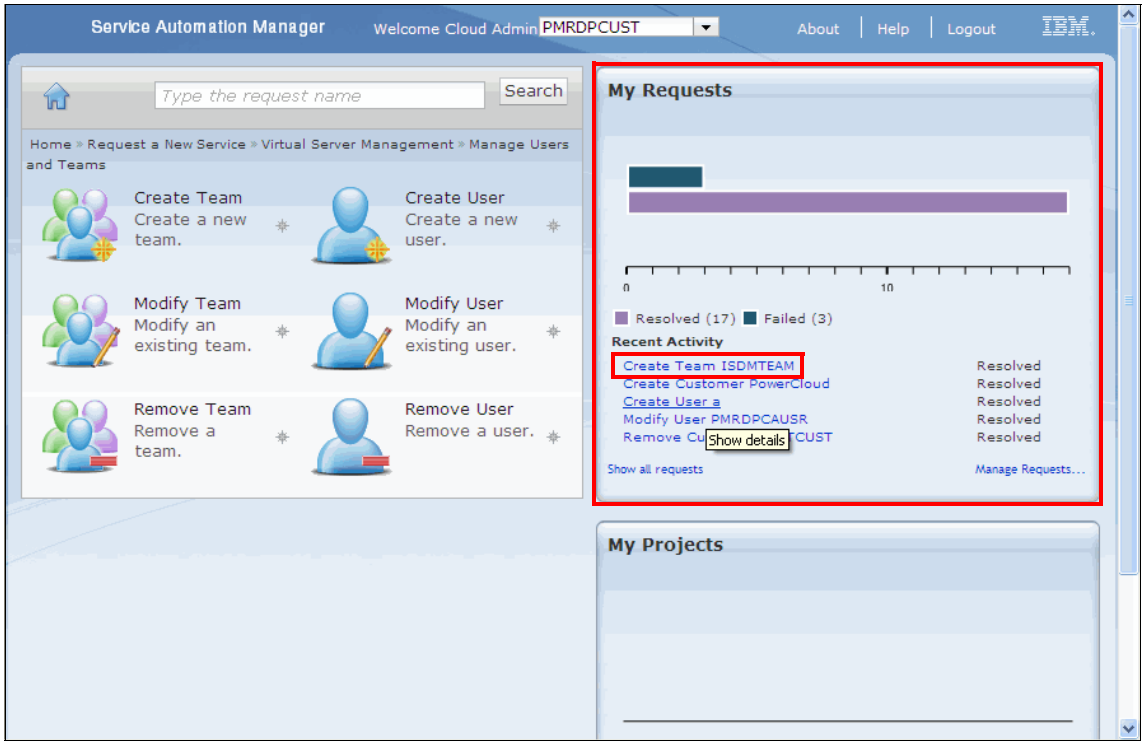

Figure 6-22 Check the requests panel for successful team creation

6.4.2 Modifying or removing teams

To modify the information of a team perform the following steps:

1. From the Self Service Portal home screen follow the icon path **Request a New Service** → **Virtual Server Management** → **Manage Users and Teams**.
2. Click **Modify Team**, as shown in Figure 6-23.

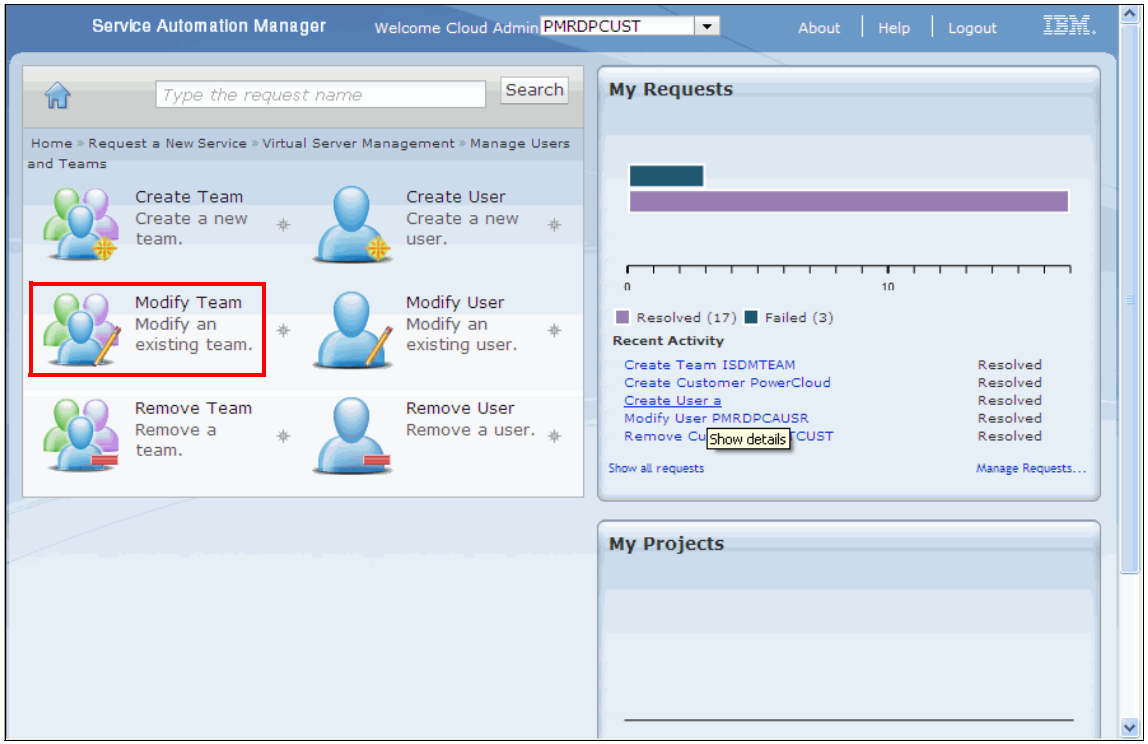

Figure 6-23 Manage team

3. The Modify Team dialog screen displays. Select a team from the pull-down menu to modify, and then click **OK**, as shown in Figure 6-24. In our example we selected the team created previously, called ISDMTeam.

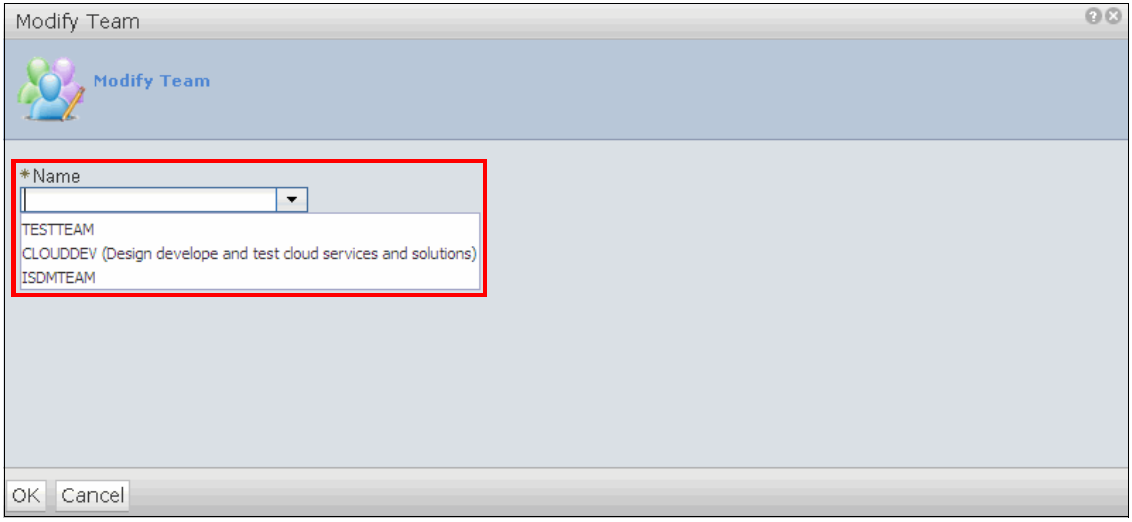

Figure 6-24 Modify team selection dialog panel

4. The team information is displayed. The team properties can be changed from this window. In our example we have added the user ISDMuser2 to the team by moving the user to the selected users. Click **OK**, as shown in Figure 6-25.

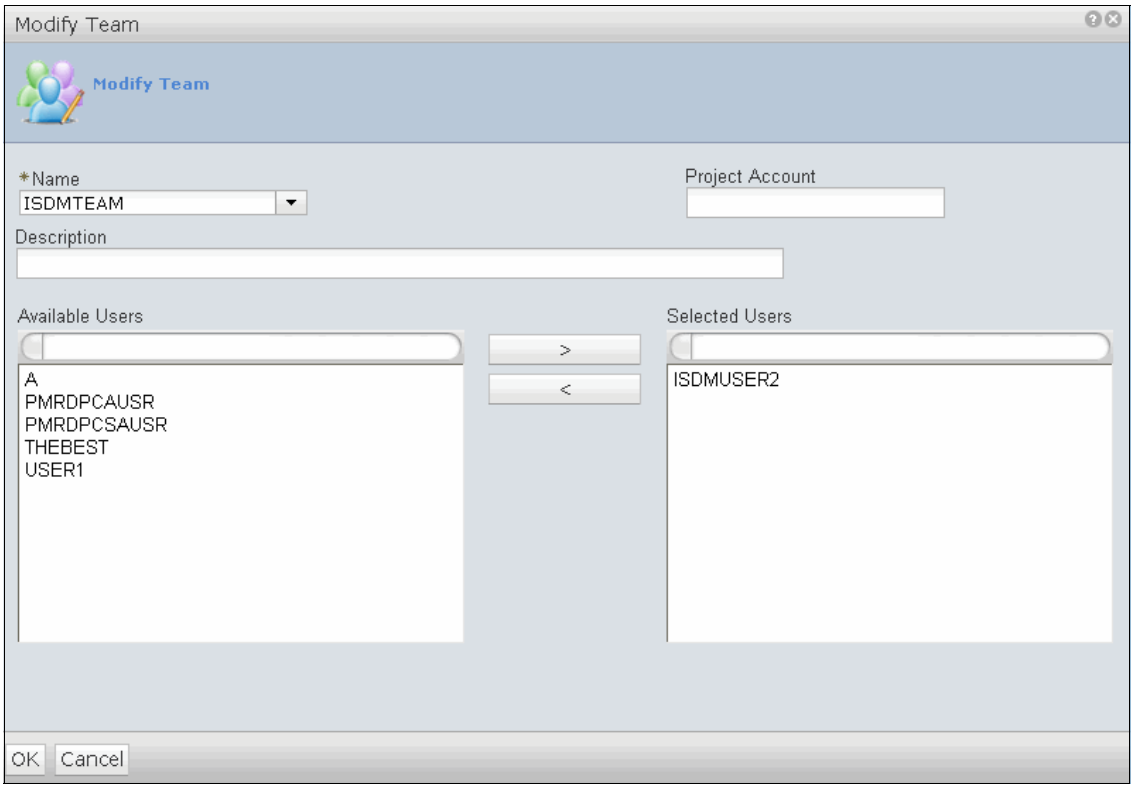

Figure 6-25 Modify the team

5. Check to ensure that the modify team request is resolved in the requests panel.

6.4.3 Removing a team

To remove a team perform the following steps:

1. From the Self Service Portal home screen follow the icon path **Request a New Service** → **Virtual Server Management** → **Manage Users and Teams**.
2. Click the **Remove Team** icon, as shown in Figure 6-26.

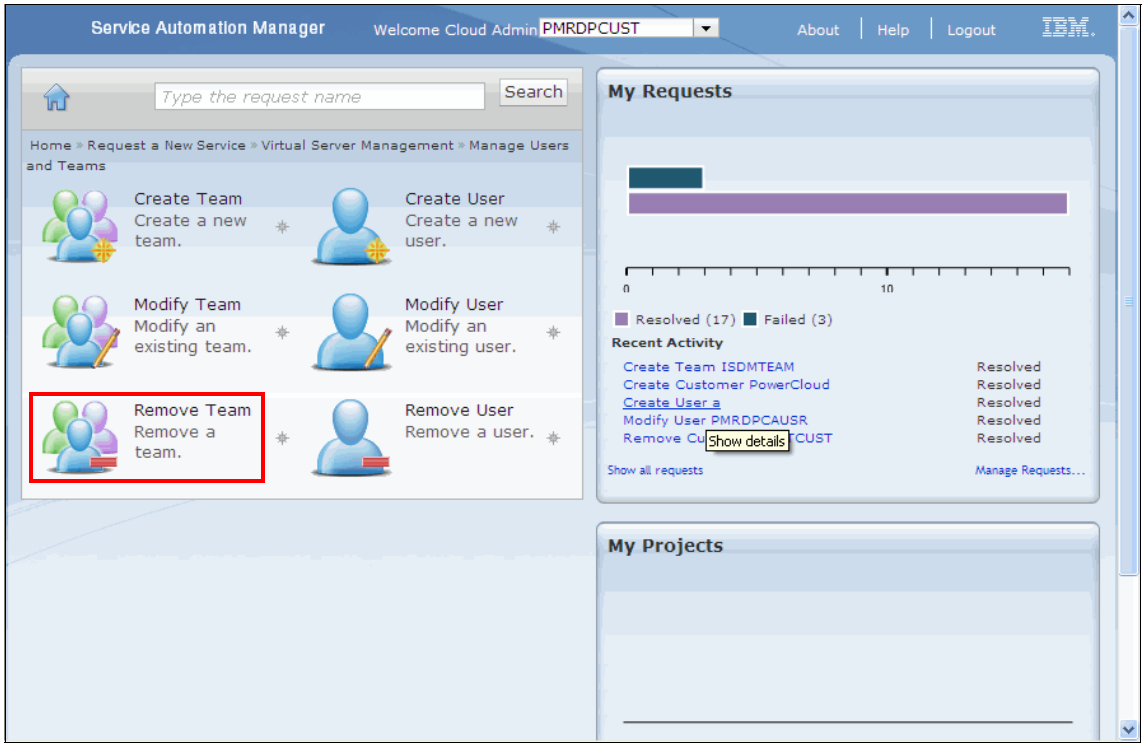

Figure 6-26 Remove user icon

3. The Remove Team dialog displays. Select the team to remove from the drop-down menu, and then click **OK**, as shown in Figure 6-27. In our example we remove ISDMtea2.

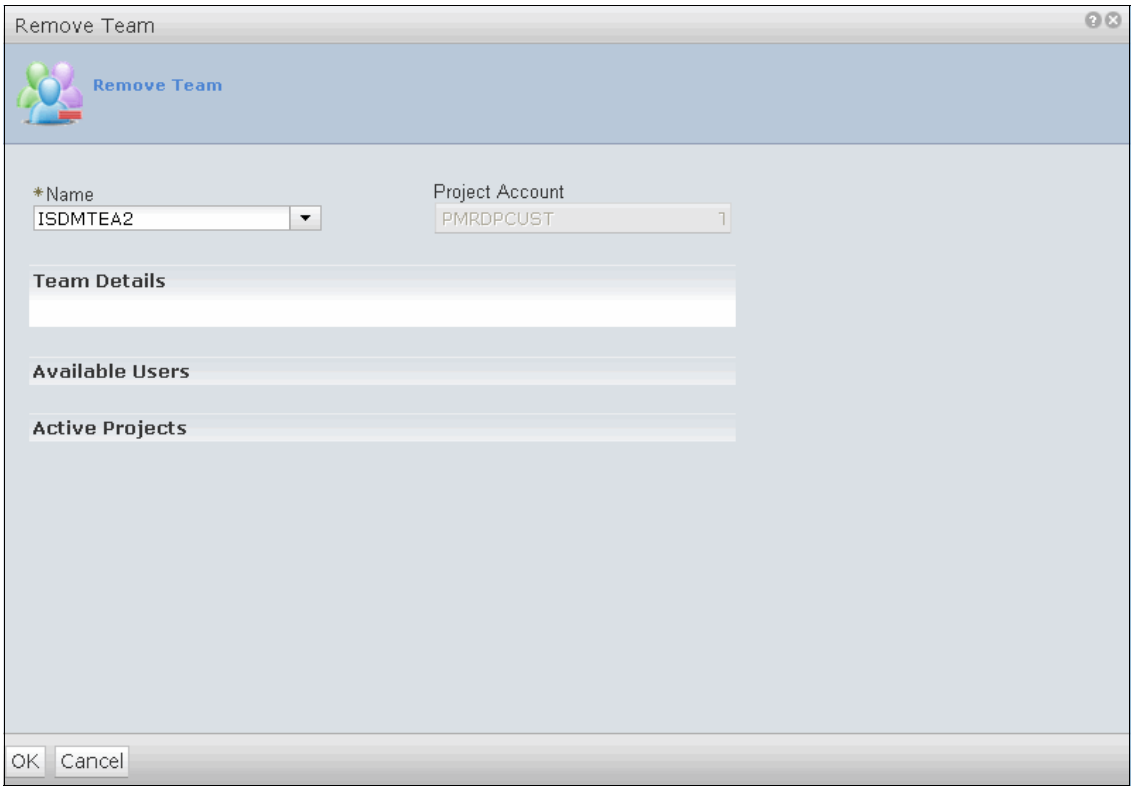

Figure 6-27 Remove Team dialog window

4. You are shown a confirmation message to confirm your remove action, as shown in Figure 6-28. Click **Yes** to confirm that you want to remove the team.

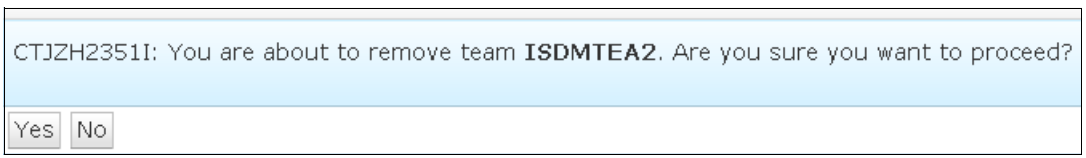

Figure 6-28 Confirm team removal

5. The ISDMtea2 team has now been removed. Check to ensure that the remove team request is resolved in the requests panel.

6.4.4 Creating users

A user is to identify a person who logs in to the Self Service Portal. A user is associated with a role. The role determines the ability that the user has to perform certain tasks in the Self Service Portal.

In one of the scenarios, we created two users. Each associates with a different customer-level policy. For the purpose of building the team that we just created, we need a team administrator user who has all the user privileges. This user should also have the Cloud Customer Level Policy for the PowerCloud customer. Because PowerCloud is the customer who we created for a specific client, this user can only access the resources limited to the PowerCloud.

Another user we created is the default customer PMRDPCUST. Only with this customer can the user have the Cloud Level Policy. This user can see resources outside of the PowerCloud. However, the role given to it limits its resources and capability.

Note: A user can be placed into one or more teams.

Creating a user

The administrator can create users from the Tivoli Service Automation Manager administration interface or the Self Service Portal interface. We chose to use the Self Service Portal in this section because it is simpler and easier for the client administrator. We use the default user ID at first to create the customer administrator ID. After that, all the administration tasks on the Self Service Portal should be done through the customer administrator ID:

1. Log in to the Self Service Portal as an administrative user. We used the PMRDPCAUSR user. Users can be created by a user who is a member of any of the following roles:
   - Cloud administrator
   - Cloud customer administrator
   - Security administrator
2. From the Self Service Portal home screen follow the icon path **Home** → **Request a New Service** → **Virtual Server Management** → **Manage Users and Teams**.

3. Click the **Create User** icon, as shown in Figure 6-29.

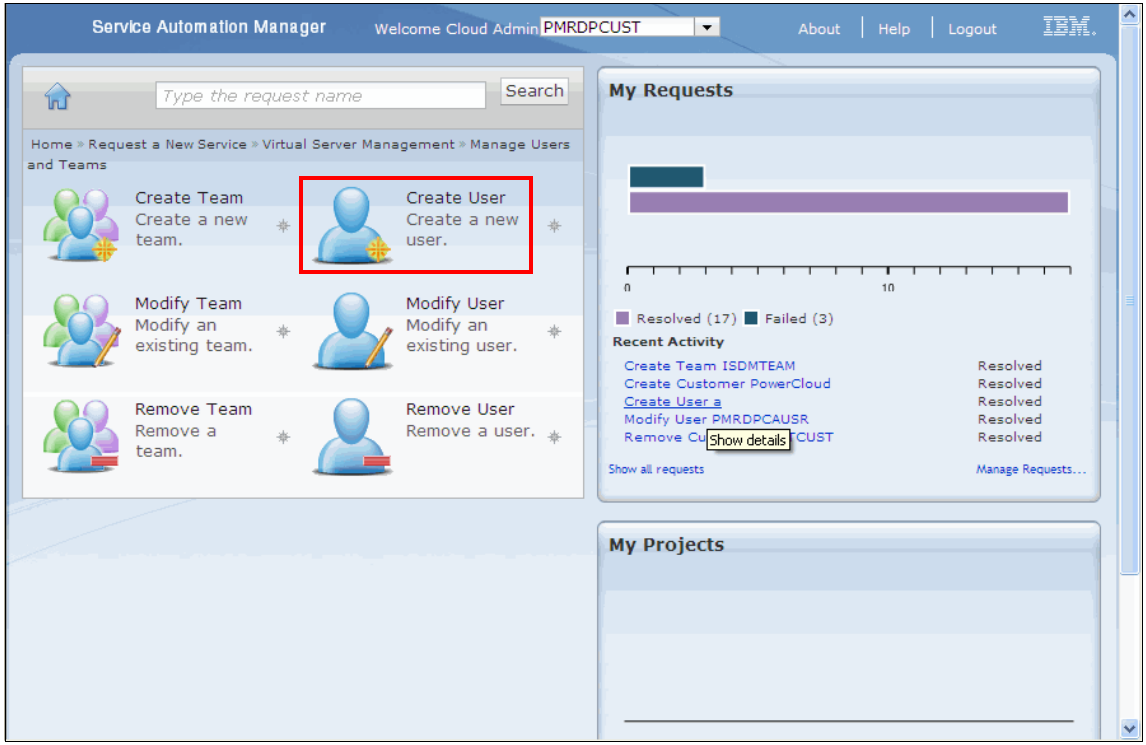

Figure 6-29 Create user icon

4. The Create User dialog screen displays. The first dialog screen contains the user information. Complete all fields on this screen as prompted and click **Next**, as shown in Figure 6-30. In our example we created a user called ISDMuser1.

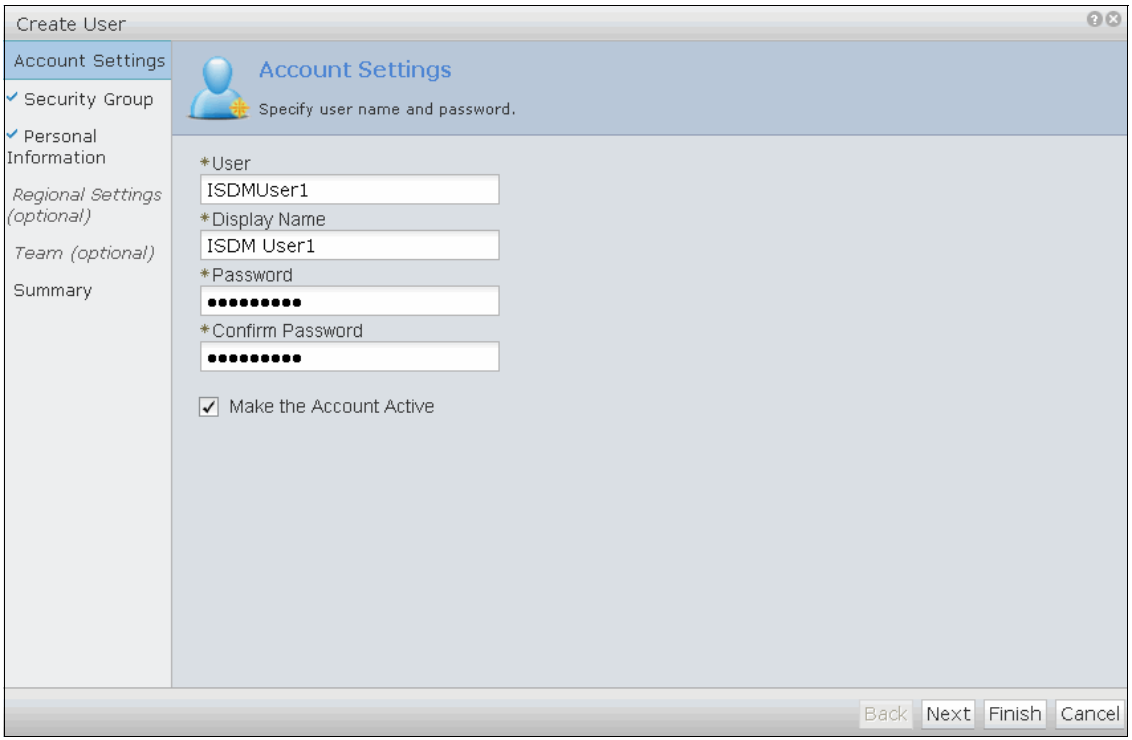

Figure 6-30 User information

Note: Each user ID must be unique and has a maximum of 30 characters.

5. The next dialog screen allows the user to be associated with roles. For detailed information about each role see this URL:

   http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?topic=%2Fcom.ibm.isdm_7.2.2.doc%2Fc_tsam_userroles.html

   Assign the appropriate role to your user by selecting the check box next to the user role and clicking **Next**, as shown in Figure 6-31. In our example we selected the Cloud Team Administrator role, as this role has the ability to place requests for provisioning servers.

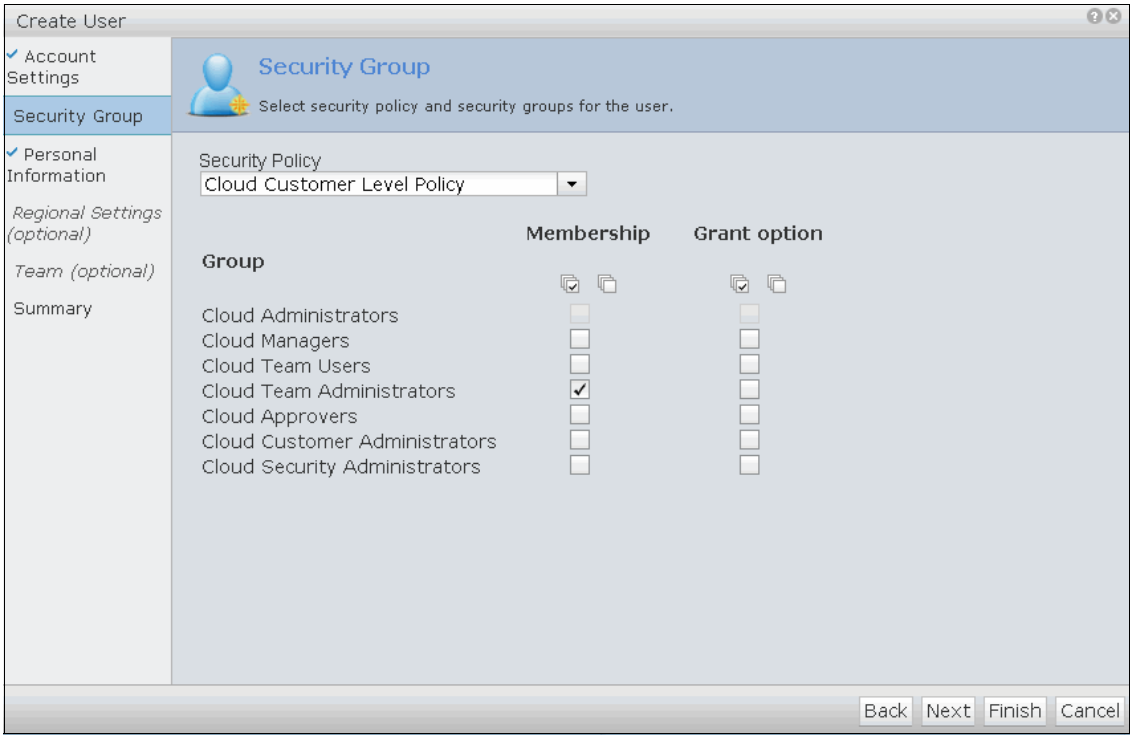

Figure 6-31 Assign user roles

6. Add the personal information for the user. Complete each field as appropriate and click **Next,** as shown in Figure 6-32.

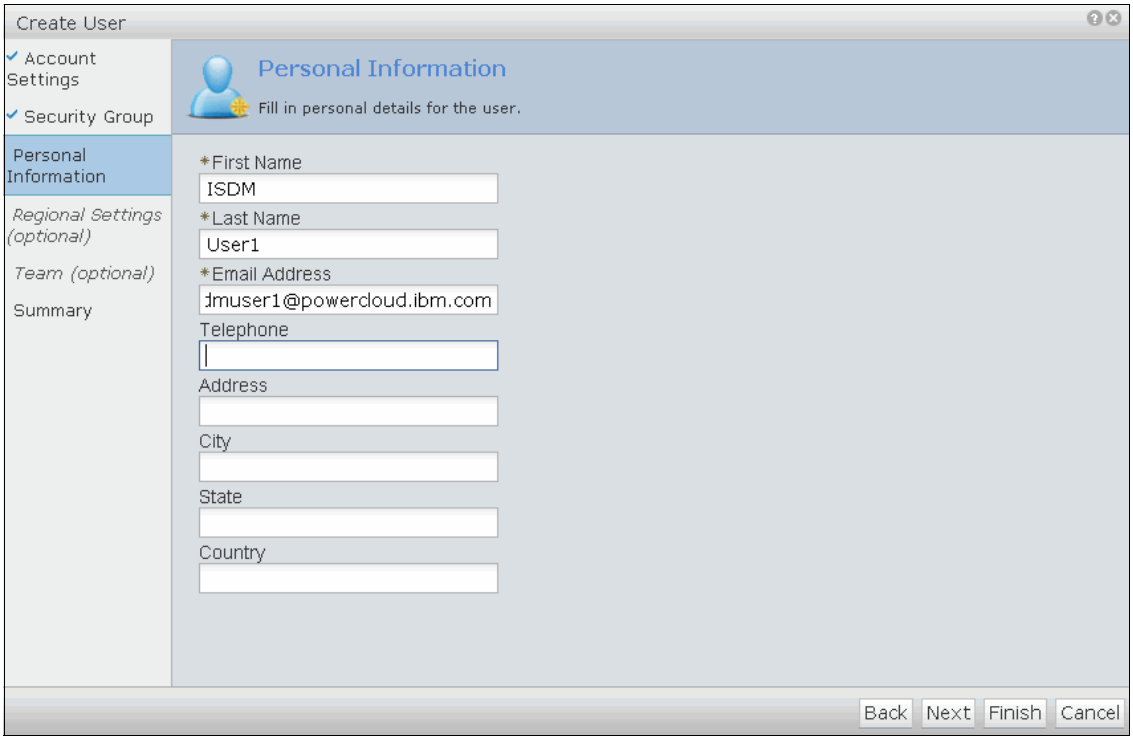

Figure 6-32 User personal information

7. Change the locale settings to the appropriate locale and click **Next**, as shown in Figure 6-33. In our example we selected English (United States).

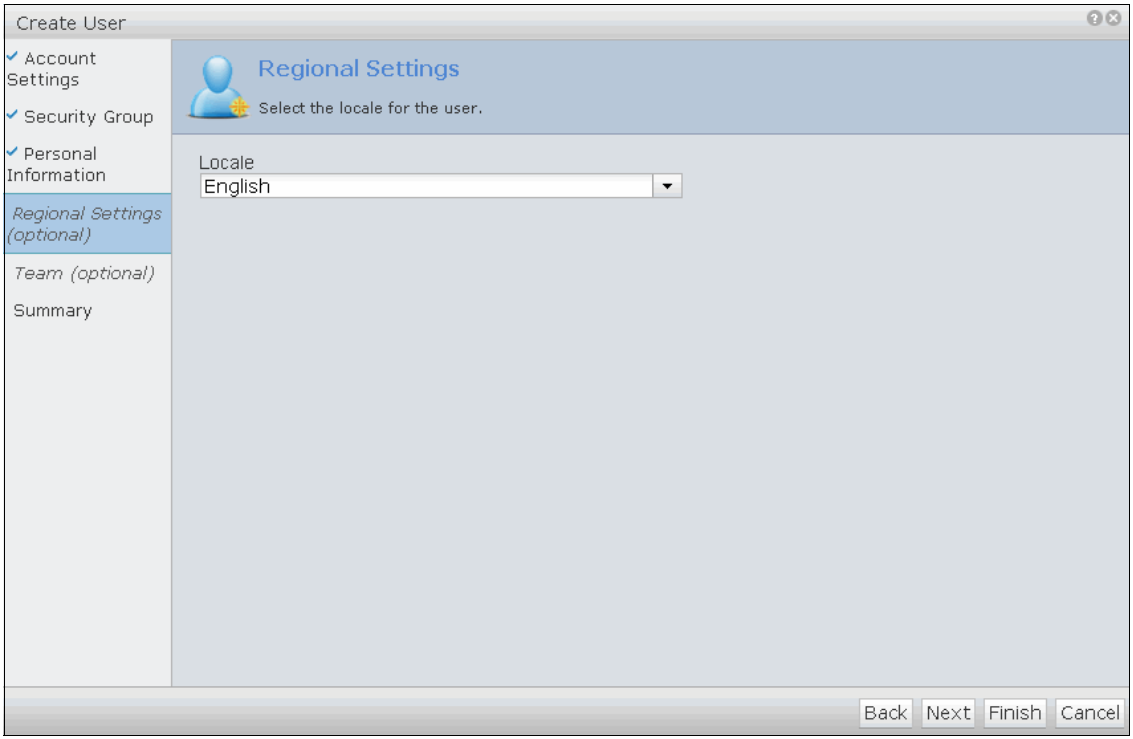

Figure 6-33 Set the locale settings for the user

8. Add the user to a team and click **Next**, as shown in Figure 6-34. In our example we added the user to team ISDMteam.

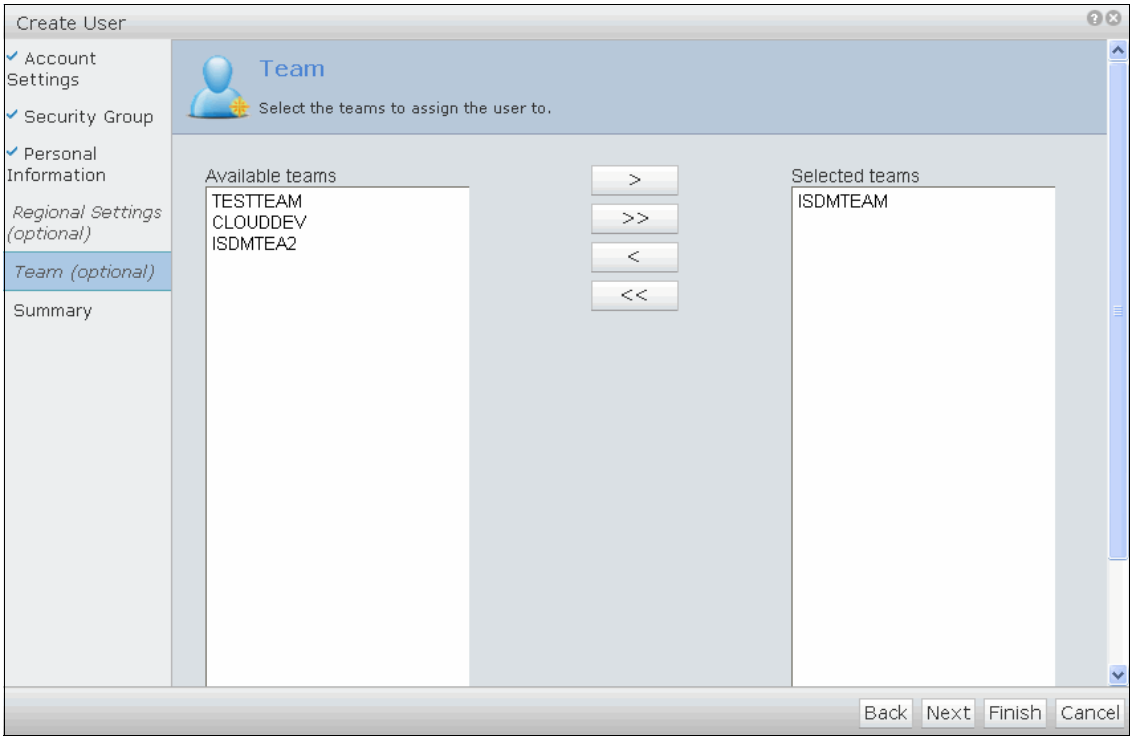

Figure 6-34 Add user to a team

9. Confirm that the user's details are correct and click **Finish**, as shown in Figure 6-35.

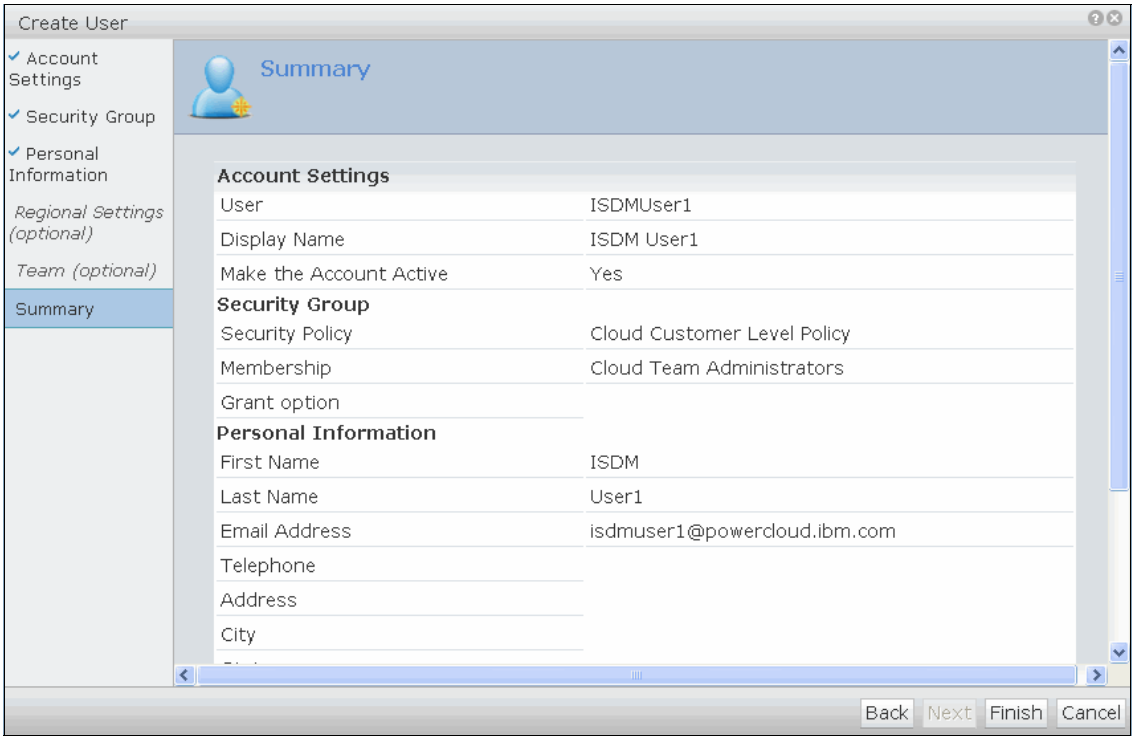

Figure 6-35 Confirm that the user details are correct

10. Check the **Create user** request in the Request panel to ensure that it is resolved.

6.4.5 Modifying a user

To modify the information of a user, follow the selection path **Home** → **Request a New Service** → **Virtual Server Management** → **Manage Users and Teams**. Click **Modify User** to display the Modify User dialog. Select a user from the pull-down menu to modify, and then click **OK**.

The user information is presented in sections similar to the steps in creating a user. Make the appropriate changes in the sections, then click **Finish** to display the Summary section. Click **Finish** again to complete the modification process.

6.4.6 Removing a user

To remove a user, follow a similar selection path. Click **Remove User** to display the Remove User dialog. Select a user from the pull-down menu to remove and then click **OK**. If you are sure that you want to remove the user, click **Yes** to respond to this warning message:

```
CTJZH2350I: You are about to remove user TESTUSER. Are you sure you
want to proceed?
```

6.5 Assigning cloud resources to a customer

Depending on the customer requirements or client contracts, the administrator can obtain resources and make them available for cloud services.

We work on the cloud pool resources to assign the following resources to the customer:

- Cloud server pools: The client gets the capability of provisioning virtual servers from the available pool of servers.
- Discovered virtual images, also referred to as master images: The image of choice can be deployed on a server in the provisioning process.

6.5.1 Assigning a cloud server pool to a customer

It is possible to assign multiple cloud server pools to multiple customers. Similarly, multiple customers can be assigned to multiple cloud server pools.

To assign the cloud server pool to a customer, perform the following steps:

1. Assign the network template log in to the Tivoli Service Automation Manager administrative interface, as the maxadmin user, as shown in step 1 on page 140.
2. From the menu on the top of the Tivoli Service Automation Manager administration screen select **Go To** → **Service Automation** → **Configuration** → **Cloud Customer Administration,** as shown in Figure 6-36.

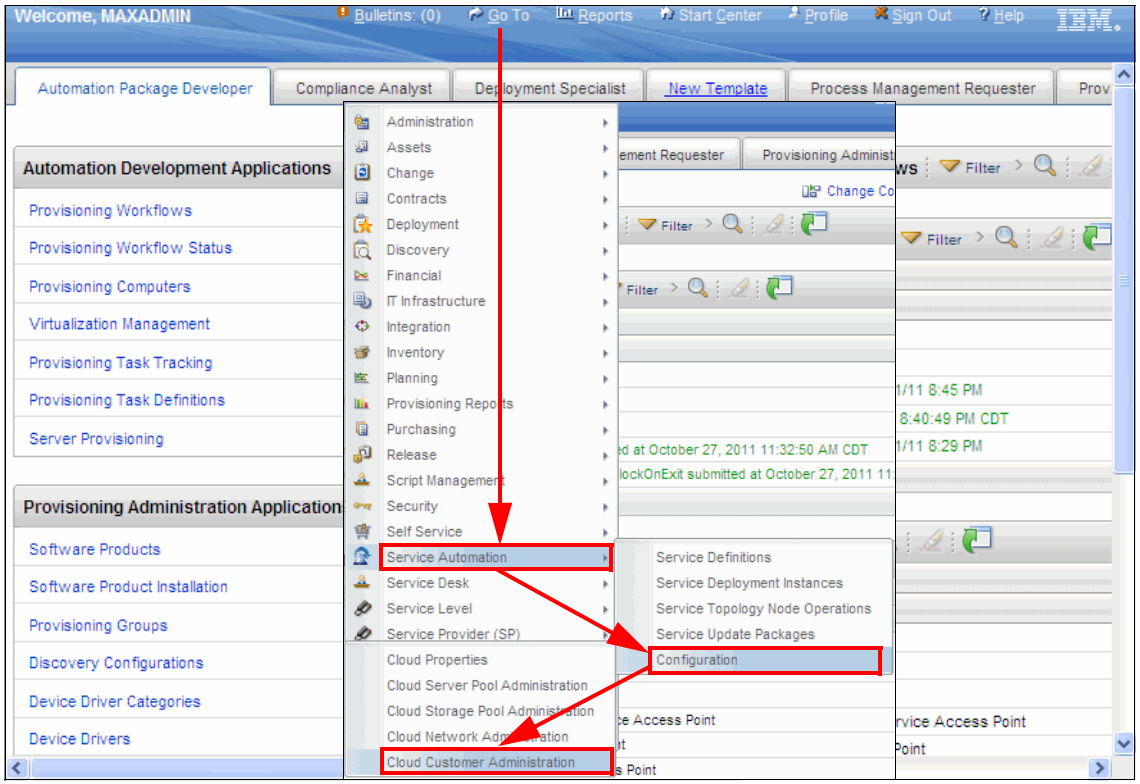

Figure 6-36 The cloud customer administration interface

3. Press Enter to display the list of customers. Select the customer **POWERCLOUD** that was previously created, as shown in Figure 6-37.

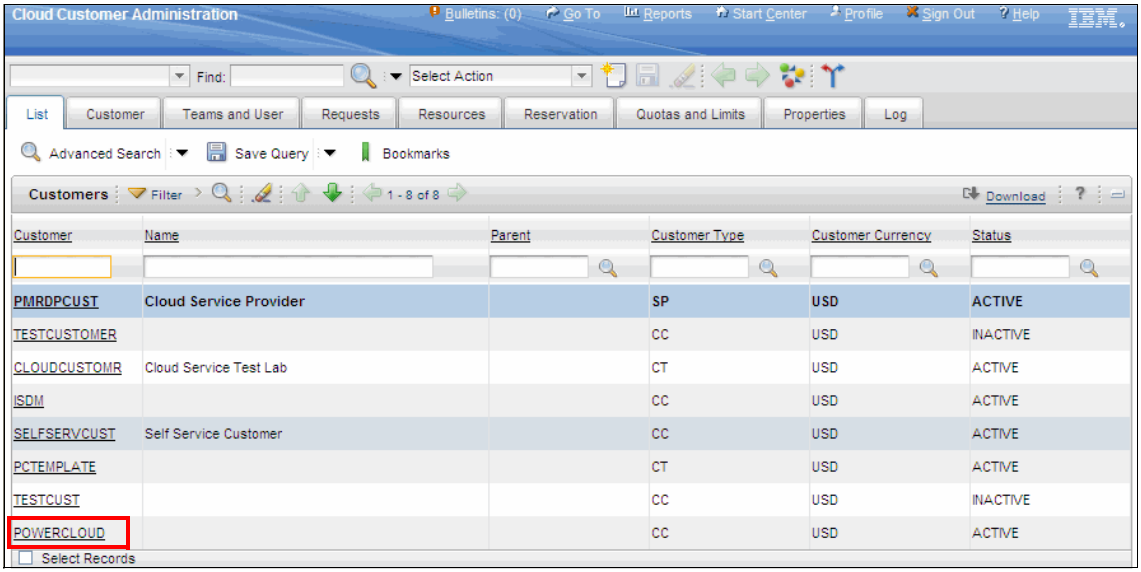

Figure 6-37 Select the POWERCLOUD customer

4. In the Associated Resources section of the screen click the **Cloud Server Pool** tab, as shown in Figure 6-38.

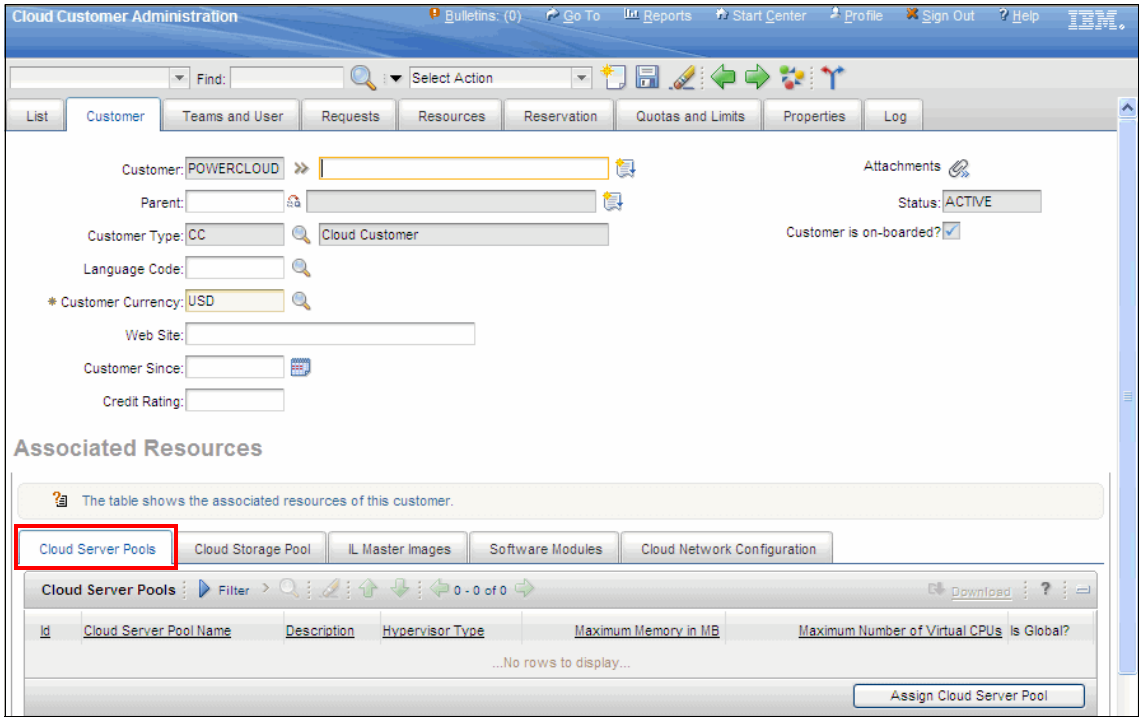

Figure 6-38 Find the Cloud Server Pool in the Associated Resources

5. Click **Assign Cloud Server Pool**, as shown in Figure 6-39.

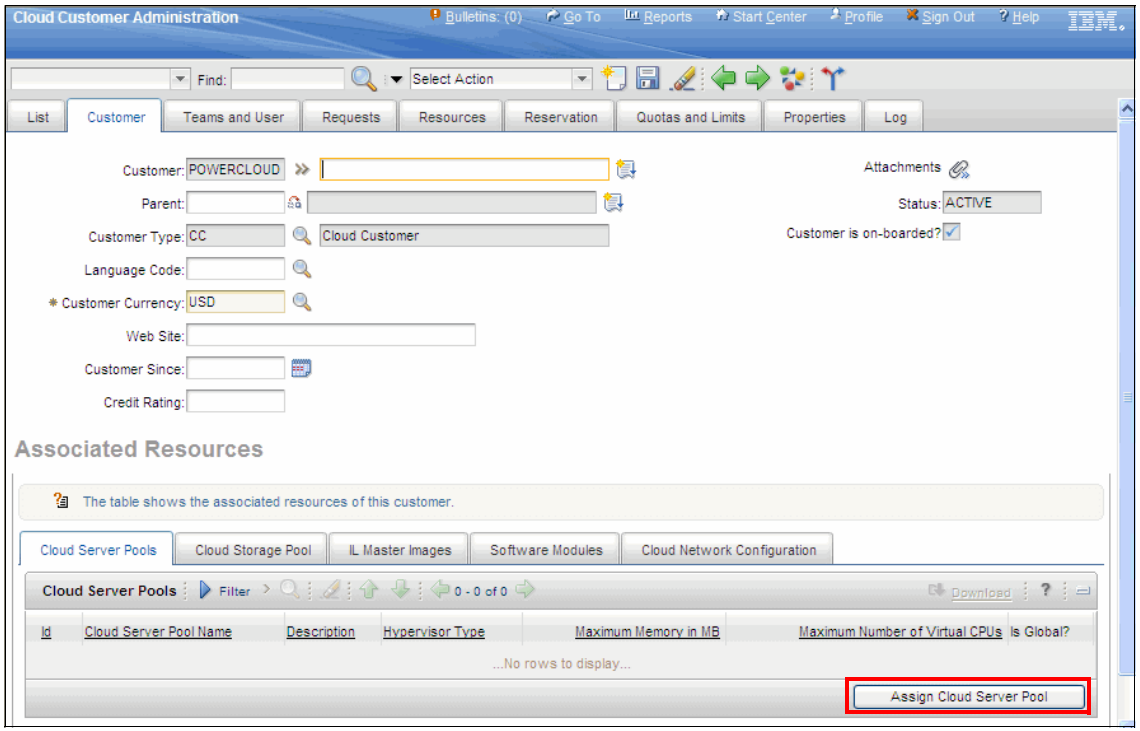

Figure 6-39 Click Assign Server Pool

6. From the Assign Cloud Server Pools to Customer screen that displays, select the check box next to the cloud server pool name **VMC Cloud Pool** that we created in 5.3.1, “DCM_objects.xml” on page 109. Click **Assign Cloud Server Pools**, as shown in Figure 6-40.

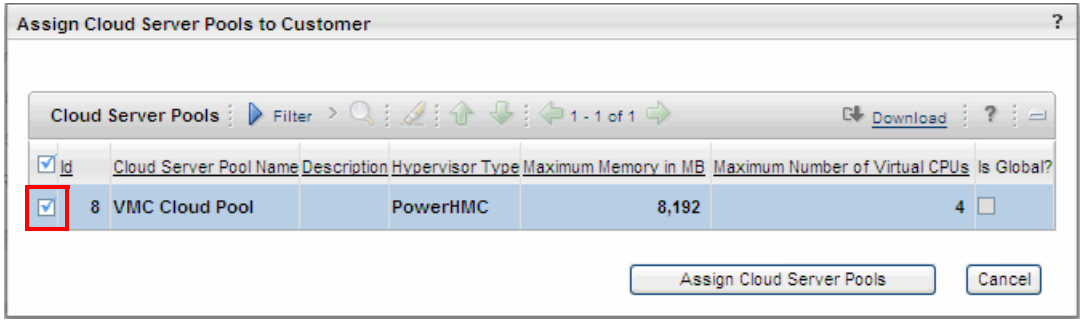

Figure 6-40 Assign cloud server pool

The cloud server pool, VMC Cloud Pool, has been assigned to the customer, PowerCloud.

6.5.2 Assigning a virtual image to a customer

A master image is a virtual appliance that was either imported to IBM Systems Director VMControl or captured by IBM Systems Director VMControl, which was discovered during the discovery phase when the cloud pool was defined.

It is possible to assign a virtual image to multiple customers and similarly assign multiple virtual images to one customer.

To add a virtual image to a customer perform the following steps:

1. Following on from step 6 on page 177, in the Associated Resources section of the screen click the **IL Master Images** tab, as shown in Figure 6-41.

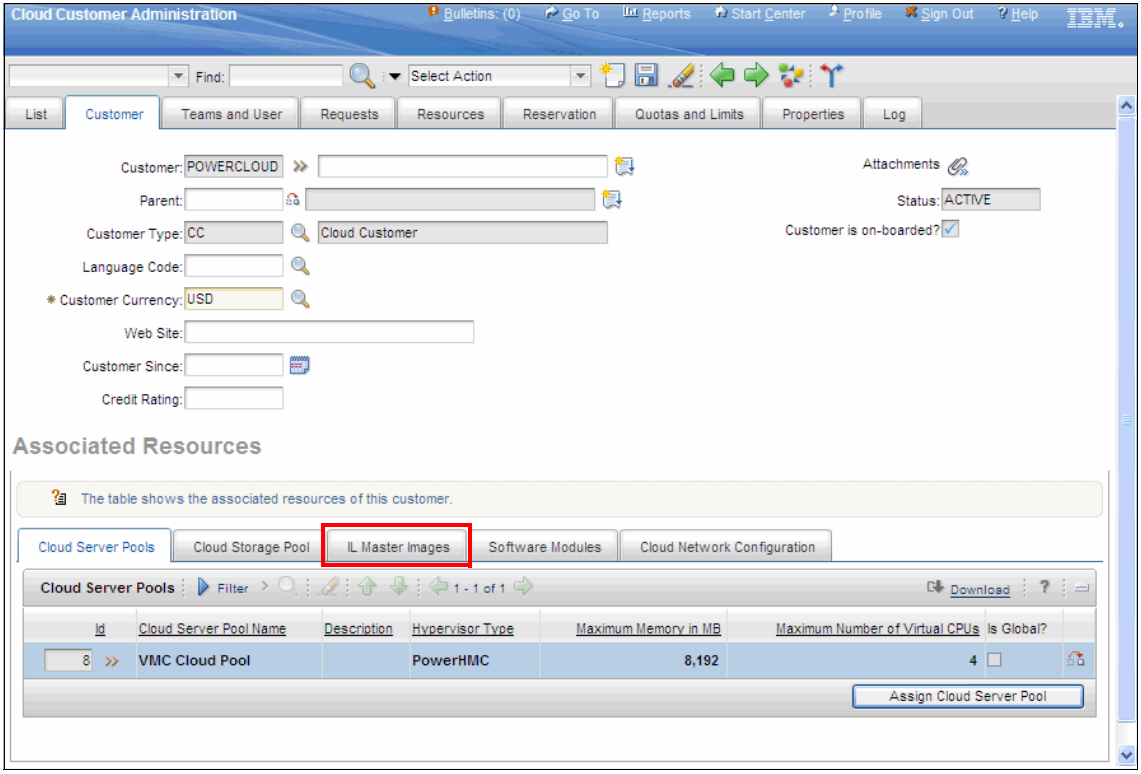

Figure 6-41 The IL Master Images tab

2. Click **Assign Master Image**, as shown in Figure 6-42.

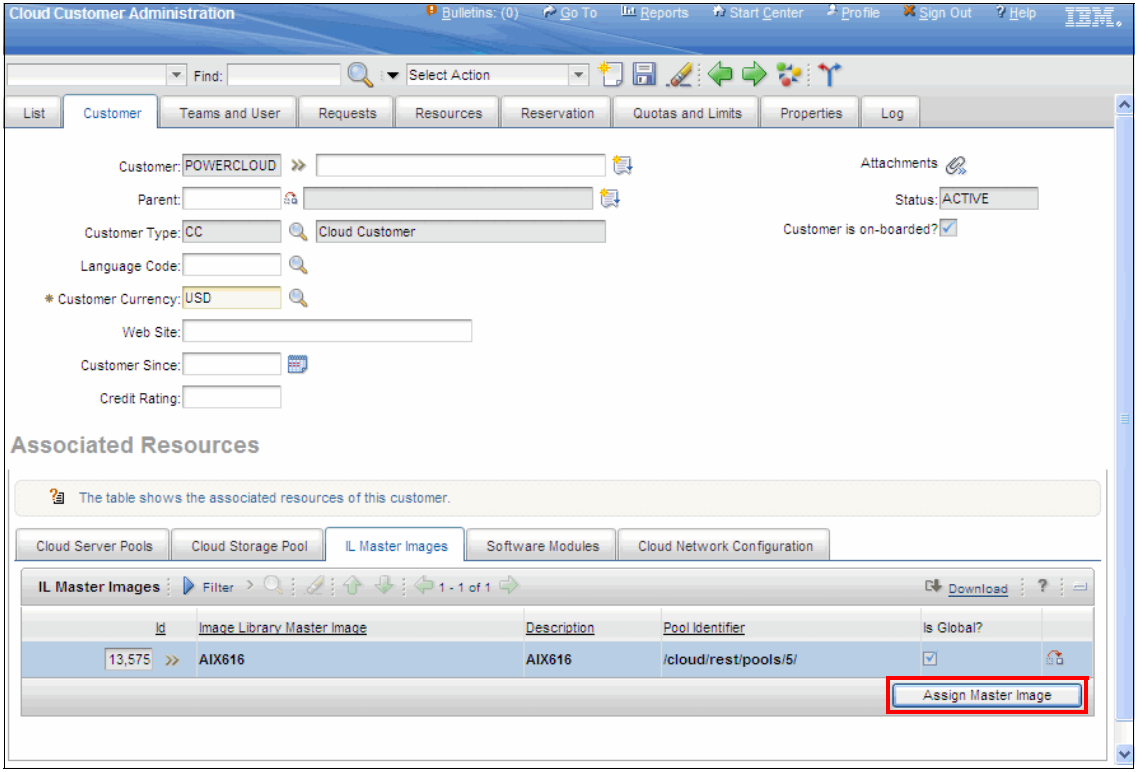

Figure 6-42 Assign Master Image

3. The Assign Master Images to Customer panel displays. Select the check box next to the virtual image that you want to assign and then click **Assign Master Image**. In our example we assigned Clean AIX 6.1 Install, as shown in Figure 6-43.

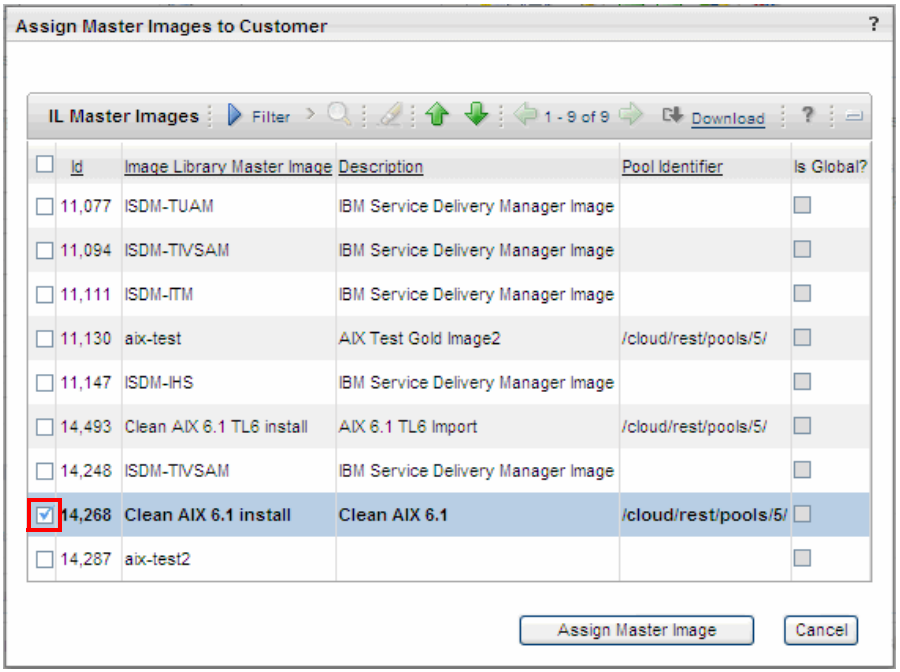

Figure 6-43 Assign master image to customer

The master image Clean AIX 6.1 Install has now been assigned to the customer and is available for users of customer PowerCloud to deploy on cloud pool VMC Cloud Pool.

6.6 Using workflows

Advanced Tivoli Service Automation Manager users can create workflows to automate processes. Workflows are effective ways of completing business tasks. Most commands in Tivoli Service Automation Manager have provisioning workflows assigned to them. When you run a Tivoli Service Automation Manager command from the command line or the web interface, the assigned workflow is invoked.

Workflows are used widely in IBM Service Delivery Manager with many processes and features. In this section, we only touch base on things that we are

able to do with this project in a limited amount of time. The key point about workflow is that when you run a provisioning task, it is submitted and scheduled to run immediately or at a later time. There are many other tasks in the global environment of automating services. Workflows are ways of organizing and managing these services.

Right from the Start Center, the administrator can see the status of recent provisioning tasks. For each task, a status indicates failed or success. The date and time of the task is also recorded. More information about the task is just a click away. See Figure 6-44 and 6.6.2, “An example of workflows” on page 187.

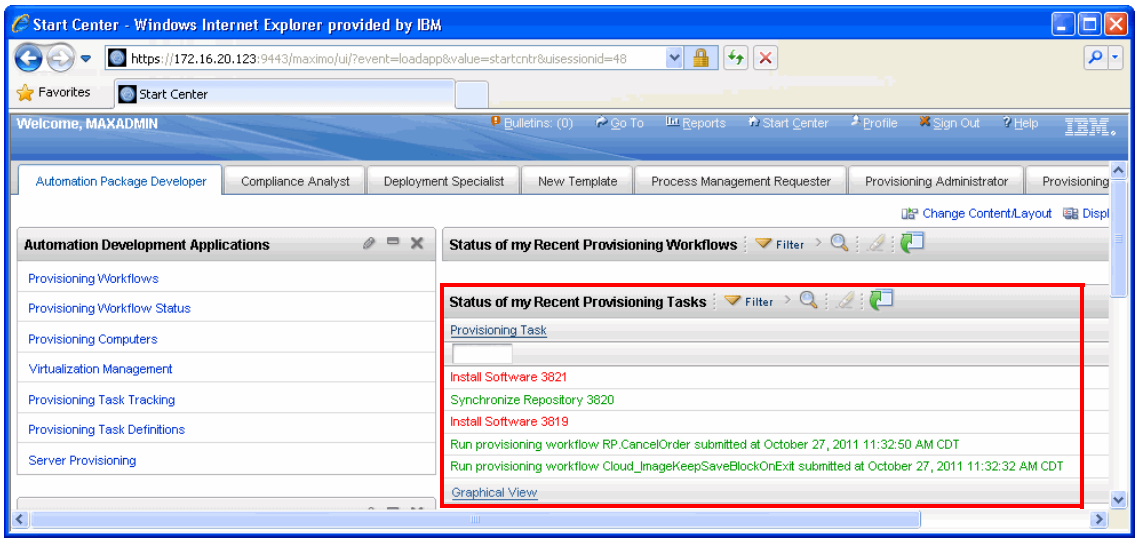

Figure 6-44 Provision workflow status

Also in the Start Center, we make use of the provisioning workflow status to check the provisioning results. Each of the workflows might contain many complicated tasks and other workflows. Following the status and other associated links related to the task helps tracking and debugging in case of failures. We discuss the detailed steps in 6.6.3, “Workflow process validation and administration” on page 189.

6.6.1 Workflow elements

If you are investigating a provisioning task and want to learn more about the workflow of that task, you are interested in parts of the application automation development. There are many other types of workflows besides provisioning tasks. You need to know what to look for. Understanding the basic elements of a workflow helps.

To work with workflow from the Tivoli Service Automation Management administration user interface, click **Start Center** to go to the home page. In the Automation Development Applications panel on the left, click **Provisioning Workflows**. The Provisioning Workflows panel contains the tool bar and three tabs:

- List
- Workflows
- Status

The content of each tab is described in detail in the following sections.

Workflow list

You can see all the workflows listed in alphabetical order. To list certain workflows, click **Filter** to open the search field. Type in a keyword, then press Enter. Figure 6-45 shows the list of workflows with Cloud in their name. You can navigate from one workflow to the next or skip to the next page using the green arrows.

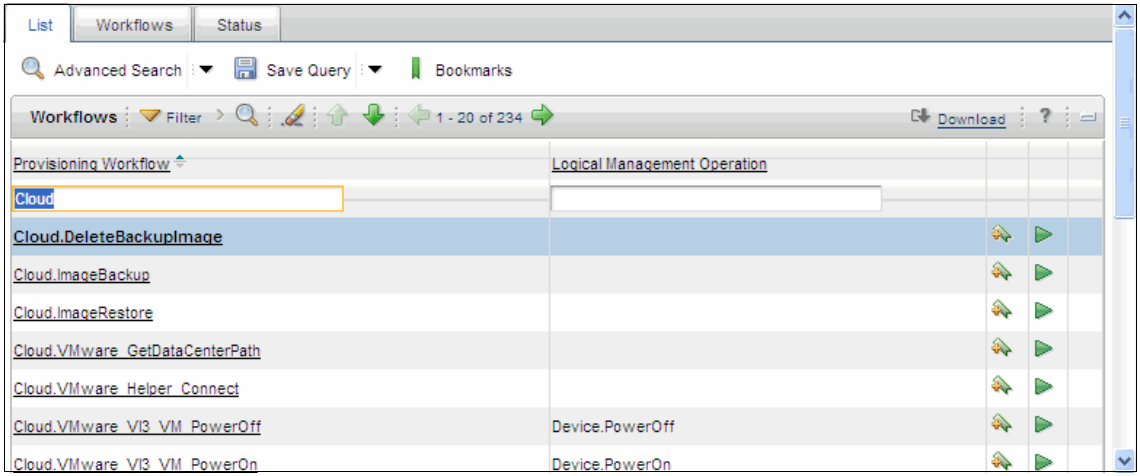

Figure 6-45 List of workflows with Cloud in their names

You can save the list of workflows into a local file by clicking the **Download** link. Choose the output file format between HTML or spreadsheet.

Workflow information

To see detailed information about a workflow, click the name of the workflow. Example 6-1 shows details of the AIX_Copy_File_from_Local workflow. The main parts of a workflow include these:

- @doc
- one or more @param
- workflow

Example 6-1 A workflow's detailed information

```
# ------------------------------------------------------------------
# Licensed Materials - Property of IBM
# 5724-F75
# (C) Copyright IBM Corp.  2003 - 2009
# All Rights Reserved
# US Government Users Restricted Rights -Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# ------------------------------------------------------------------

@doc Copies a script from $TIO_HOME/repository/AIX-Operating-System to the target server

@param Destination_Device_ID - DCM object ID of the target server
@param Destination_File - Name to call the script when copied
@param Destination_Path - Directory to copy to on target server
@param Source_File - Name of the script to copy
@param File_location  - Location of file (including file name) on target server

workflow AIX_Copy_File_from_Local(in Destination_Device_ID, in Destination_File, in
Destination_Path, out File_location, in Source_File) LocaleInsensitive
  var TC_ID

  #Grab tio.home.unix (set when deploymentengines start up) to set bin/repo dirs
  var tio_home_unix = Java[java.lang.System#getProperty("tio.home.unix")]
  var repo_src_dir = Jython(tio_home_unix + "/repository/AIX-Operating-System")

  java:com.thinkdynamics.kanaha.de.javaplugin.datacentermodel.FindDEDeviceId(TC_ID)

  #Device.Copy File
  Device.CopyFile(TC_ID, repo_src_dir, Source_File, Destination_Device_ID,
Destination_Path, Destination_File, "default", "default", "300")

  #Builds the fully qualified destination file name to return
  File_location = Jython[ "%s%s%s" % (Destination_Path,"/",Destination_File) ]
```

Workflow status

When workflows are requested or deployed, the Status tab contains the list of the requests and their status.

Communication template

As part of the application automation, tasks exchange messages and events with each other through e-mail. It is a good practice to standardize those messages so that they can be easily interpreted in programmatic ways. IBM Service Delivery Manager provides many such pre-formatted messages called communication templates.

Communication templates are used in sending notifications from workflows and escalation processes. A communication template has the form of an e-mail message. It can also be used in e-mail communications between applications or users.

Use the Communication Templates application to create or modify templates. Follow the selection path **Go To** → **Administration** → **Communication Templates**. The Communication Templates panel contains following tabs:

- List
- Communication Template
- Recipients
- Attachment Folders

On the List tab, click the pull-down menu on the left of the tool bar and select **All Records**. The templates are listed in alphabetical order. Use the navigation arrows to move from one template to the next or skip to the next page. Click the name of the template to view its contents. You can also change or add information in the fields and save.

To create a new template, click the New Communication Template icon in the tool bar. Enter template information in the blank fields, then click the Save Communication Template icon in the tool bar.

When viewing or modifying a template, you can also copy it to a new template and modify it. Click the **Selection Action** drop-down menu in the tool bar and select **Duplicate Template**. A new template is named with a number by default. Give it a meaningful name.

Three fields are required:

- Applies To
- Accessible From
- Send From

For the fields Applies To and Accessible From, click the magnifying glass on the right to see a list of values for selection. The Send From field requires an e-mail address.

A communication template can contain substitution variables that are replaced with the values from the database record before the status message is sent. An example of a communication template with substitution variables is shown in Example 6-2.

Example 6-2 Substitution variables in a communication template

```
Subject -- Status message
Message -- :FIRSTNAME :LASTNAME is the owner of this application.
```

At send time, :FIRSTNAME and :LASTNAME are replaced with the first name and last name values from the respective database columns, as in Example 6-3.

Example 6-3 Variables are substituted

```
Subject -- Status message
Message -- John Las is the owner of this application.
```

To see the name of the column, click the field and press Alt+F1. A Field Help dialog displays the Field name and Table.Column name with a brief help message. See Figure 6-46.

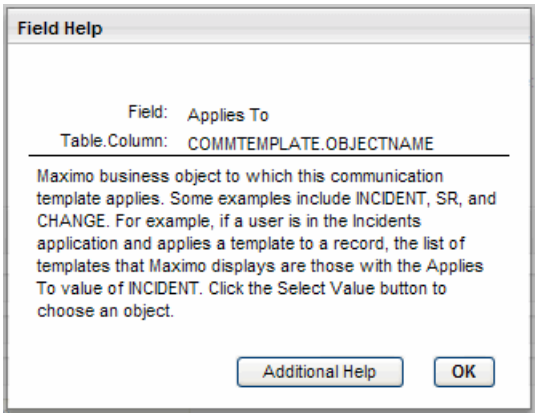

Figure 6-46 Field Help dialog shows Field and Table.Column names

To specify the e-mail recipients, click the **Recipients** tab. Four types of recipients are presented:

- Roles
- Persons
- Person Groups
- E-mails

You can enter information for one or more recipients, as in Figure 6-47. Click **Select Roles** to display a list of available roles for selection. Check the box to add this recipient in the To:, cc:, or bcc: field. You can add more recipients by clicking **New Row**. Similarly, enter information for Persons, Person Groups, and E-mails.

Note: If the recipient row is hidden, click the Show Table icon in the right-most location of the recipient row.

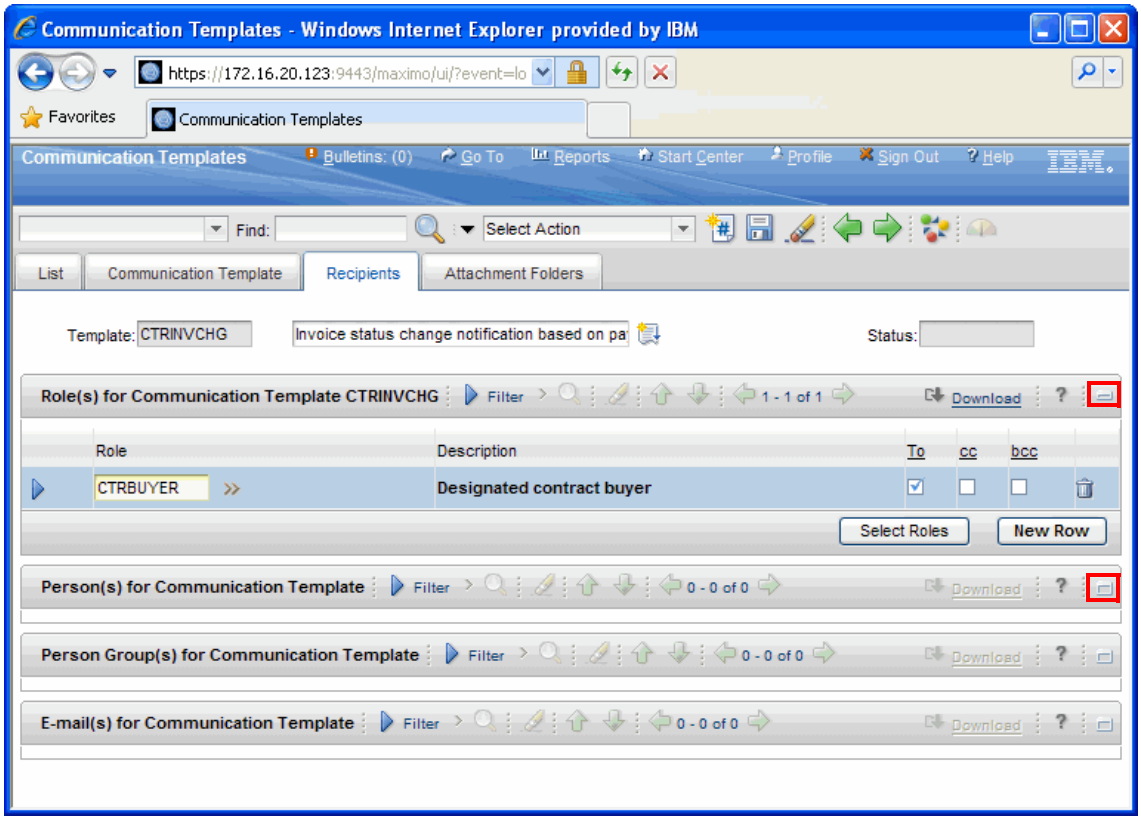

Figure 6-47 Enter recipients for the communication template

Click the **Attachment Folders** tab to specify a folder containing files for attachment.

6.6.2 An example of workflows

To see an example of workflows and notification, click **Start Center** at the top of the panel. The Status of my Recent Provisioning Tasks panel lists the Provisioning Tasks in start time order. Each task has one of the following statuses:

- In Progress
- Success
- Failed

See Figure 6-48.

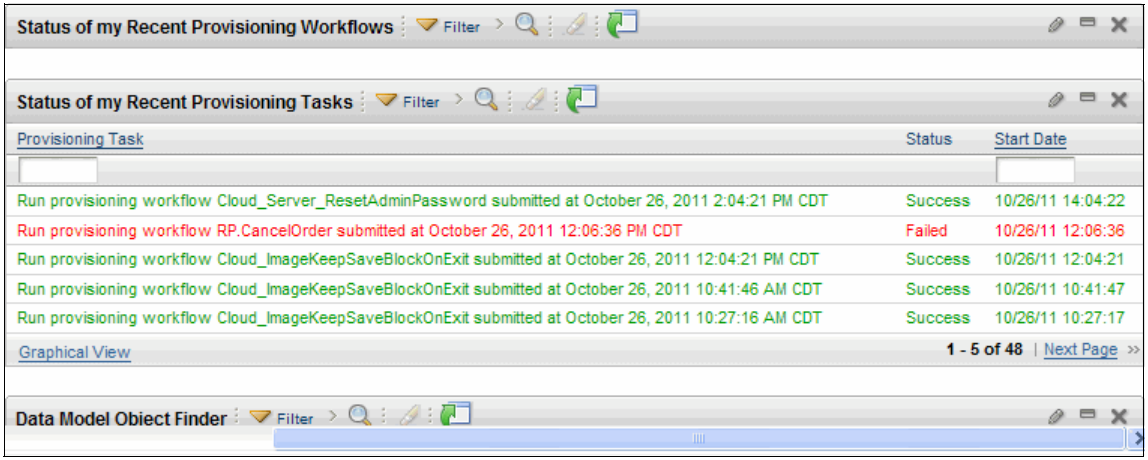

Figure 6-48 Status of recent provisioning tasks

Click one of the tasks to open the Provisioning Task Tracking panel. The Task tab presents detailed information about the task:

- Provisioning Workflows
- Notification
- Events

If there are recipients specified in the Notification section, the e-mail is sent to notify the task status.

To see more details of the workflow, click the View Details icon on the left of the workflow name. The detail information includes this:

- Workflow Parameters: A list of parameters and their values for this workflow.
- Targets: Containing different information depending on the task. The key here is the Provisioning Workflow Deployment Request ID. See Figure 6-49.

Provisioning Workflow Log

The Provisioning Workflow Log contains the workflow execution steps. A step can be an execution of another workflow. Click the View Details icon at the beginning of a step to see detailed information about the step.

Detailed information of a step includes this information:

- Parameter name and value
- The text message indicating that the step is executed

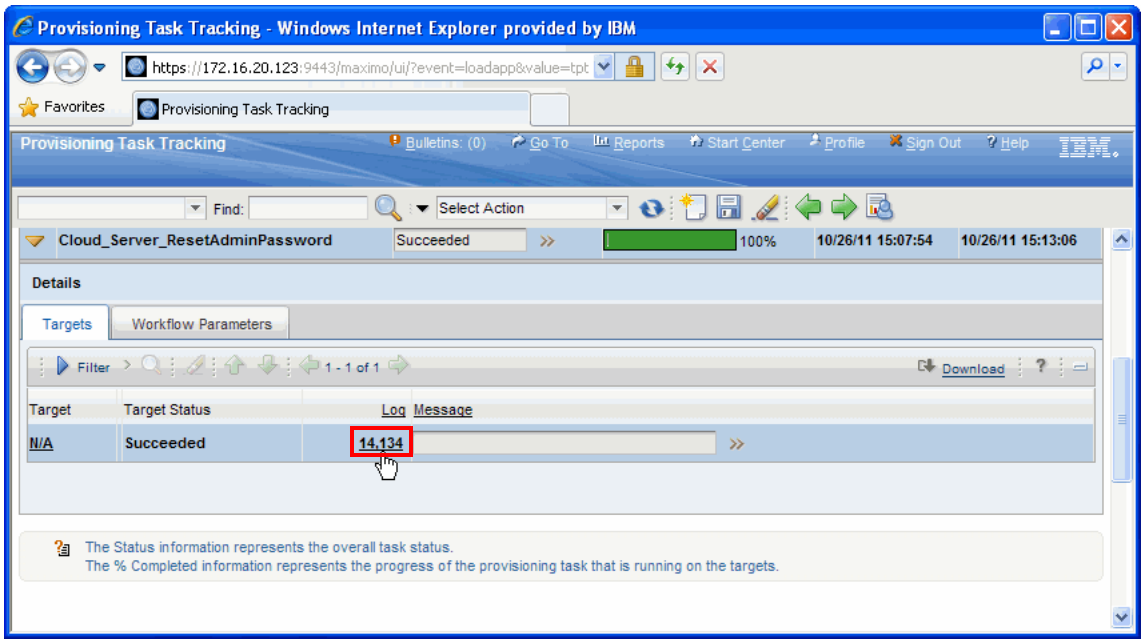

Figure 6-49 Provisioning Task Workflow Log

6.6.3 Workflow process validation and administration

To see the status of all provisioning workflows, click **Provisioning Workflow Status** in the Automation Development Applications panel in the Start Center. This panel has two tabs:

- List: Provisioning workflows are listed in order of deployment request IDs. The time order is most recent first. For each deployment request record, you can click the icon on the right to do the following actions:
  - See detailed error message if the request failed.
  - Delete the deployment request (not the workflow) if it is completed and there is no need to keep the record.
  - Save the record to a bookmark.

  See Figure 6-50.

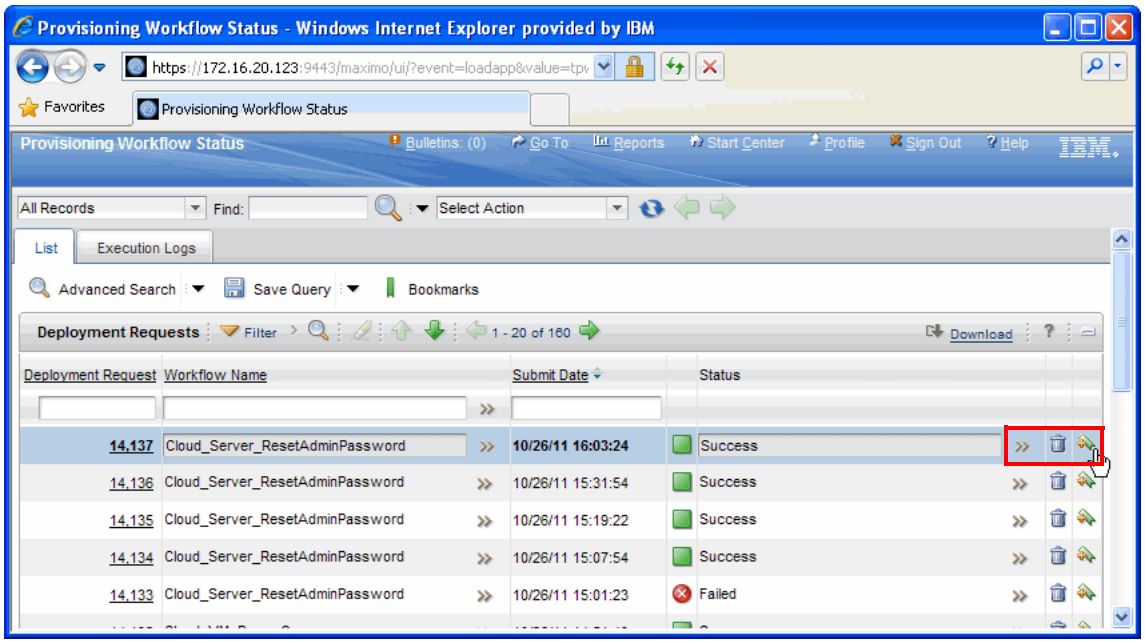

Figure 6-50 Deployment Request records

- Execution Logs: Detailed information about a selected workflow from the List tab. Clicking a deployment request ID on the List tab also opens up this panel. Details of a provisioning workflow status are discussed in “Provisioning Workflow Log” on page 188.

When validating the workflow processes, you can carry out the following actions on the selected workflow:

- Add to Bookmarks.
- Delete Workflow Execution.
- Stop Execution.
- Force Cancellation.
- Export.
- Run Workflow Again.

Click the **Select Action** pull-down menu in the tool bar to select one of the actions.

Adding a bookmark

Most List tabs list many items, one on each line. The Deployment Request Log is an example. The records are accumulated over a long period of time. If you find an item that you want to save for later use, adding the record to the bookmarks puts it in a different list.

You can list the bookmarked items by clicking the pull-down menu on the left of the tool bar and select **All Bookmarks**, as in Figure 6-51.

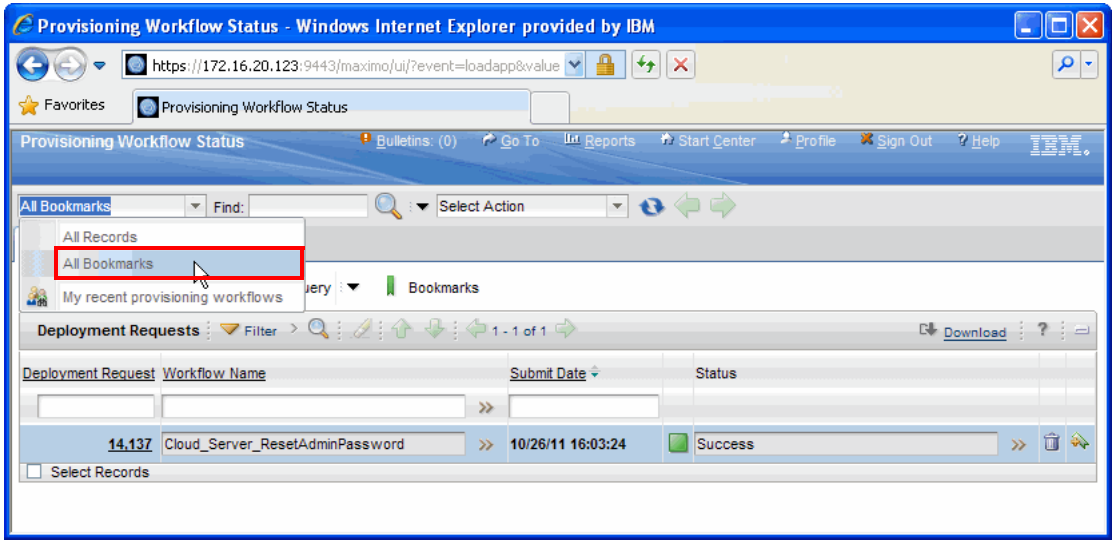

Figure 6-51 Selecting to list All Bookmarks

Deleting workflow execution

This action deletes the deployment request record (not the workflow execution), if you do not need to keep it. The action does prompt you for a confirmation message, as follows:

```
BMXAA4125E - Are you sure you want to delete this record?
```

Stopping execution

If a deployment request is in progress, you can select **Stop Execution** to stop it. You should know what the workflow does and the effects of stopping it.

Note: Stopping a workflow in the middle of an execution might result in unexpected outcomes. An alternative would be to wait for the workflow to finish, then check the Deployment Request Log.

You cannot stop a non-running workflow. The following message displays:

```
COPCOM700E - Cause:
COPJEE332E The system cannot cancel a finished deployment request
(deployment request ID 13200)
```

Forcing cancellation

This action is for a case in which a deployment stops unexpectedly. The document states that you can use this action to clean up all deployment requests that are still in progress.

Again, you cannot cancel a non-running workflow.

Exporting

When viewing a detailed execution log, you have the option of exporting the log data to an XML document for viewing in an XML editor or saving into a file. Figure 6-52 shows the saved XML file viewed in a browser. An XML editor provides more viewing and formatting options for better views of the log data.

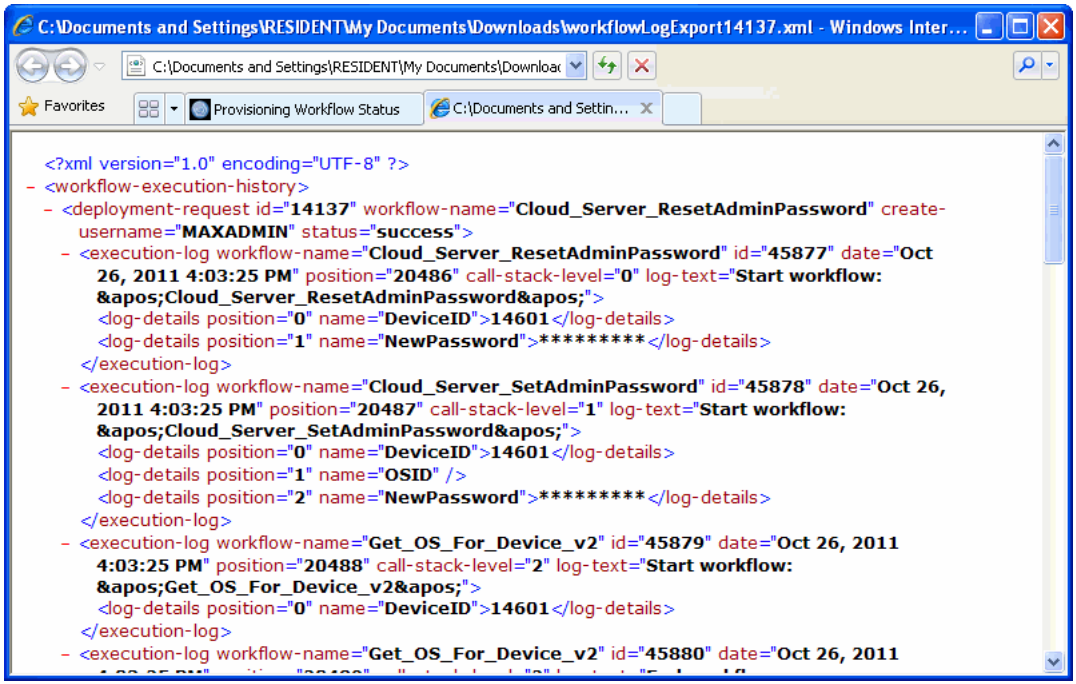

Figure 6-52 Deployment Log saved in XML

Running the workflow again

You select to do this if the workflow failed and needs to be run again. Some workflow can also be executed more than once without side effects. Know what the workflow does before selecting this action.

7

Projects: Putting it all together

Now that you have all the infrastructure components in place and configured, you are in a position to deploy an image to a server. This is done by creating a Tivoli Service Automation Manager project. A project is similar to a VMControl workload; it is a deployed virtual image. Creating a project automatically deploys the associated image to the server pool.

7.1 Tivoli Service Automation Manager projects

These are the steps to take to deploy an image:

1. Create a customer template.
2. Create a customer.
3. Create a user.
4. Create a team.
5. Collect inventory.
6. Assign the image to a team.
7. Create a project.

IBM Service Delivery Manager has default customers and users: PMRDPCUST and PMRDPCAUSR, respectively. These have authorization to create new customer templates, customers, users, and teams.

To deploy a service you must create a project. A project is an instance of a service deployment. This process is part of Tivoli Service Automation Manager's user-initiated provisioning and management of virtual servers. It is supported by the self-service interface.

A project is always associated with a team.

7.2 Collecting inventory

When the cloud pool is created (Chapter 5, "Configuring cloud components" on page 105), Tivoli Service Automation Manager automatically collects an inventory of the VMControl resources that constitute the pool, including the virtual appliances. If you create additional virtual images in VMControl, then you must collect inventory again so that Tivoli Service Automation Manager learns about them. Do this using the following steps:

1. Log on to the Tivoli Service Automation Manager's administrative interface at `https://<TSAM>:9443/maximo` as a user with cloud administration privileges, such as maxadmin.

2. Navigate to **Go to** → **IT Infrastructure** → **Image Library** → **Image Repositories**, as shown in Figure 7-1. You are presented with the panel shown in Figure 7-2.

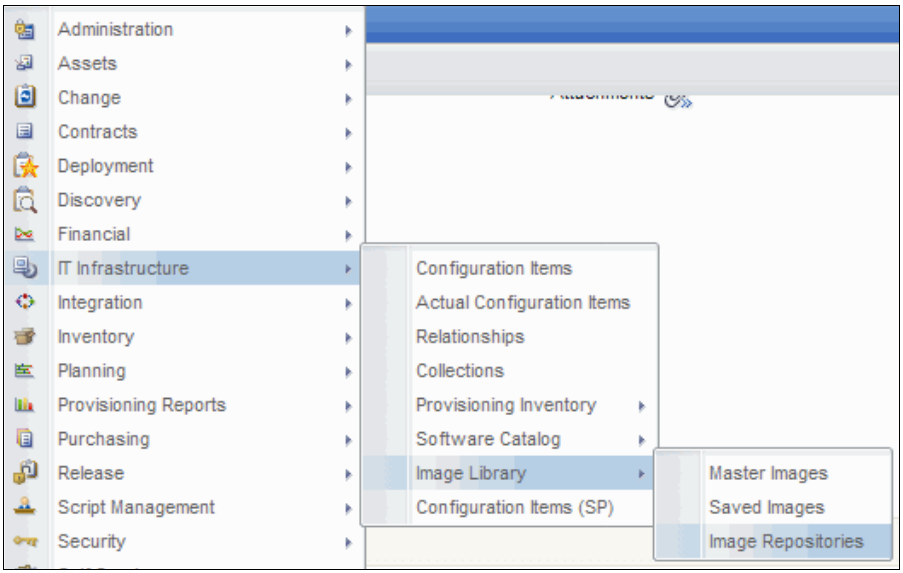

Figure 7-1 Navigating to Image Repositories

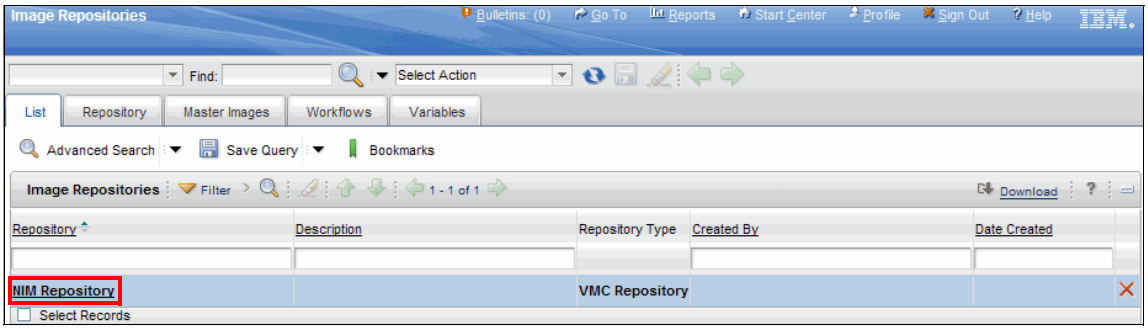

Figure 7-2 Image Repositories panel

3. Click **NIM Repository**, as indicated by the red box in Figure 7-2 on page 195, to display the image repository details, as shown in Figure 7-3, and click **Synchronize Repository**. This sets up the inventory collection task and presents you with a pop-up panel to run, as shown on the left in Figure 7-4. Clicking **OK** presents the pop-up shown on the right. If you want to monitor the task, click **Yes**, otherwise click **No**.

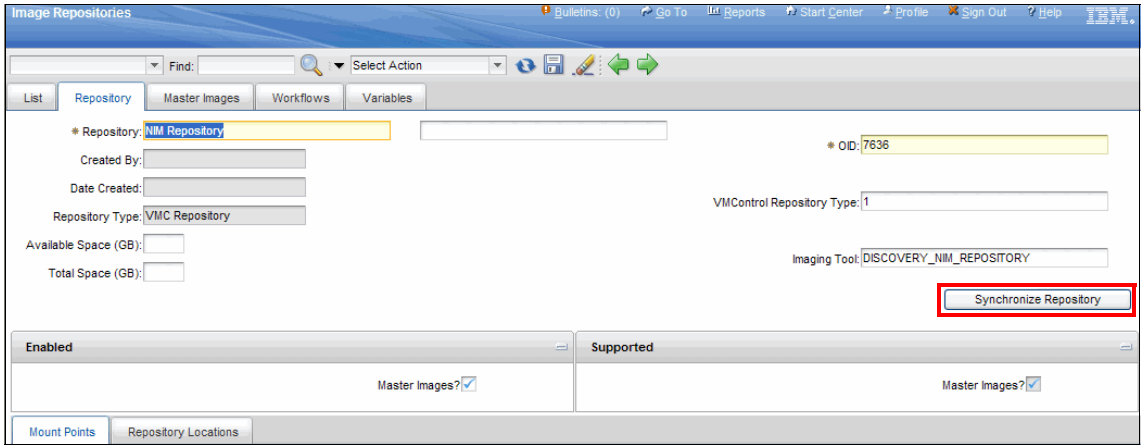

Figure 7-3 Image Repository details

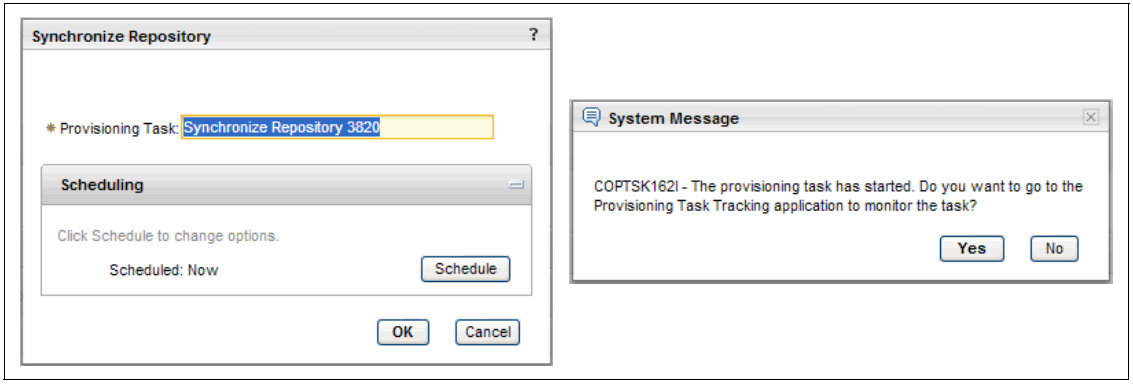

Figure 7-4 Synchronizing the image repository

When the task has completed, assign the discovered images to a customer, as described in the following section.

7.3 Assigning images to customers

After an image has been discovered by Tivoli Service Automation Manager, you must make it to one or more customers. You do this through Tivoli Service Automation Manager's administration interface. These are the steps to follow:

1. Log on to the Tivoli Service Automation Manager's administrative interface at `https://<TSAM>:9443/maximo` as a user with cloud administration privileges, such as maxadmin.
2. Navigate to **Go to** → **Service Automation** → **Configuration** → **Cloud Customer Administration**, as shown in Figure 7-5. You are presented with the panel shown in Figure 7-6 on page 198.

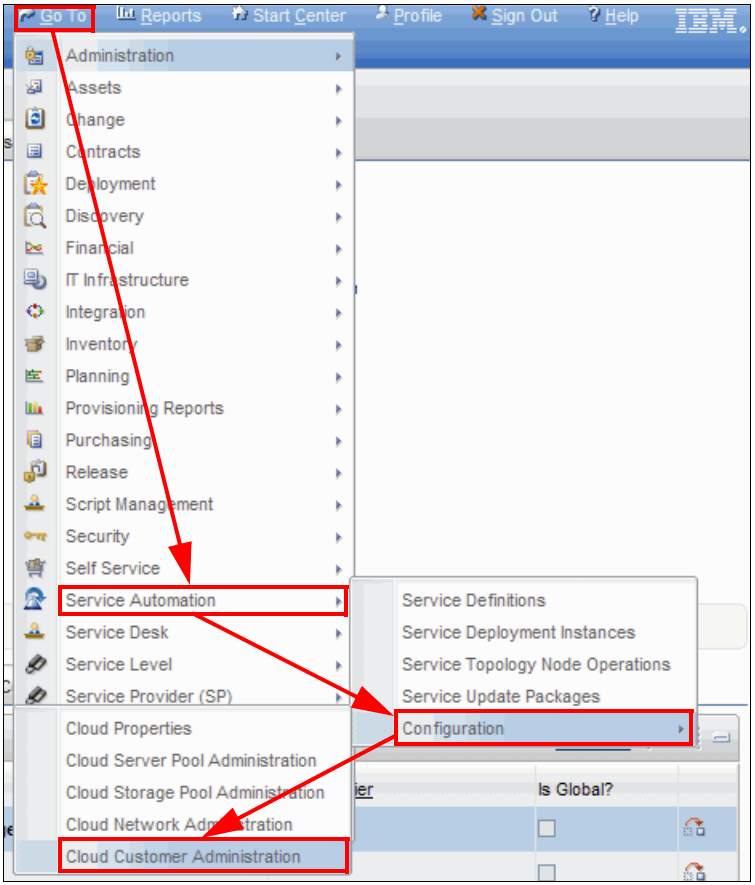

Figure 7-5 Navigation to Cloud Customer Administration

3. Enter the name of the customer to whom you want to assign the image in the Customer text field. In the example shown in Figure 7-6, this is `ISDM`. Press Enter to initiate a search.

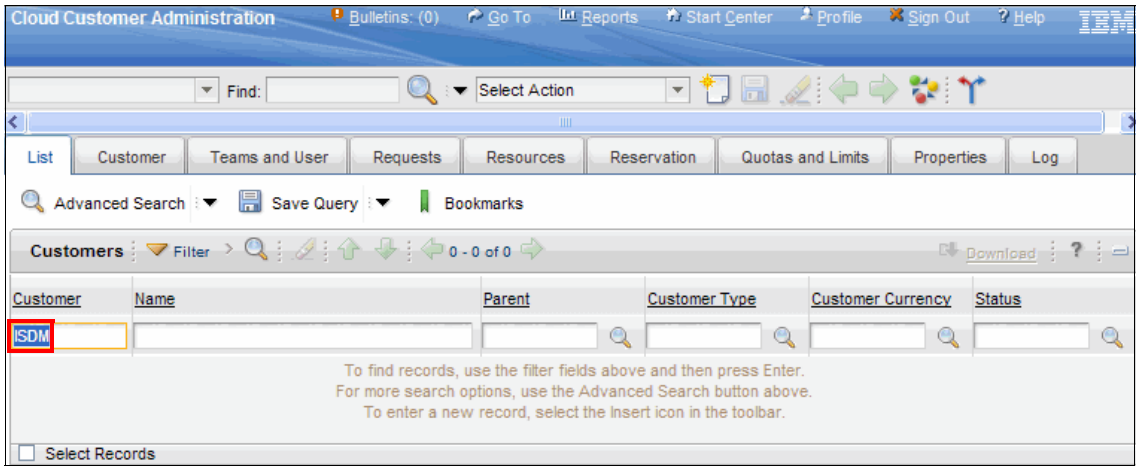

Figure 7-6 Cloud Customer Administration panel

The lower part of the panel updates with the results of your search, as shown in Figure 7-7.

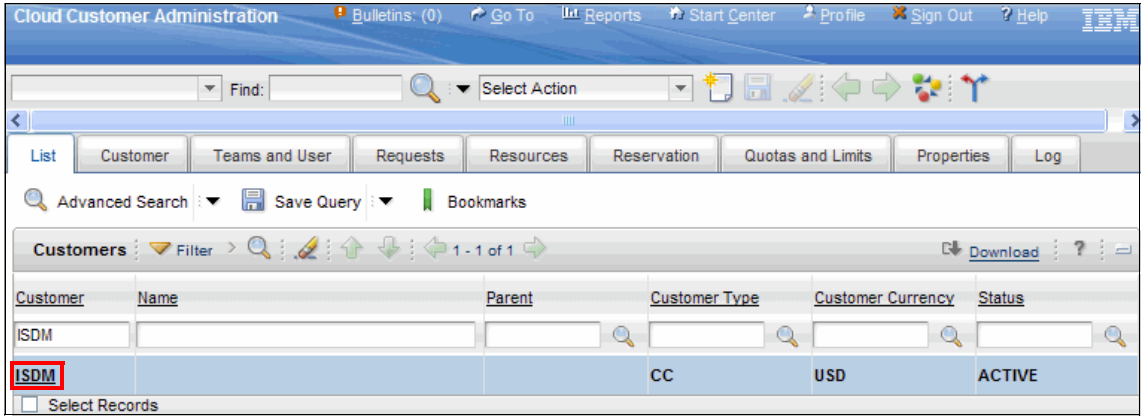

Figure 7-7 Customer search results

4. Click the name of the customer to whom you want to assign the image (ISDM in Figure 7-7 on page 198), to navigate to the Customer detail panel, shown in Figure 7-8.

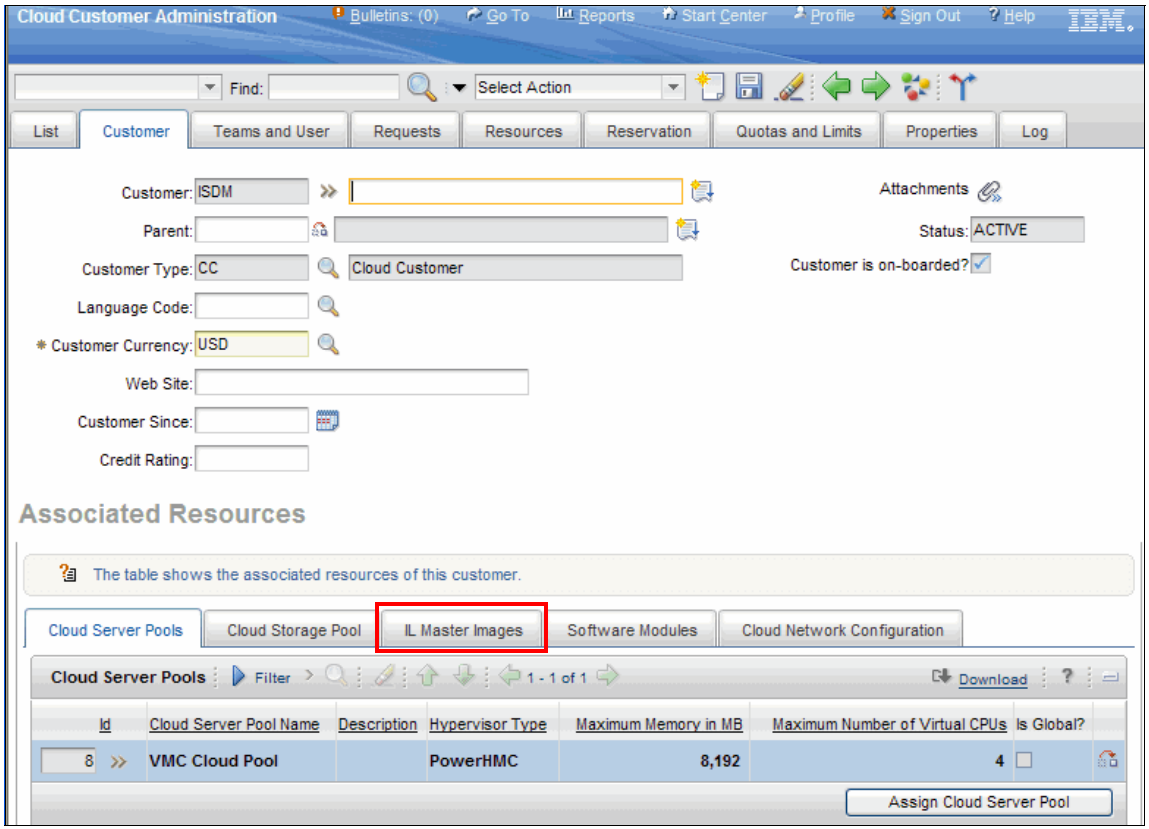

Figure 7-8 Customer detail tab

5. In the Associated Resources section, click the **IL Master Images** tab, highlighted in red in Figure 7-8 on page 199. You are presented with the panel listing all the images currently assigned to the customer, as shown in Figure 7-9.

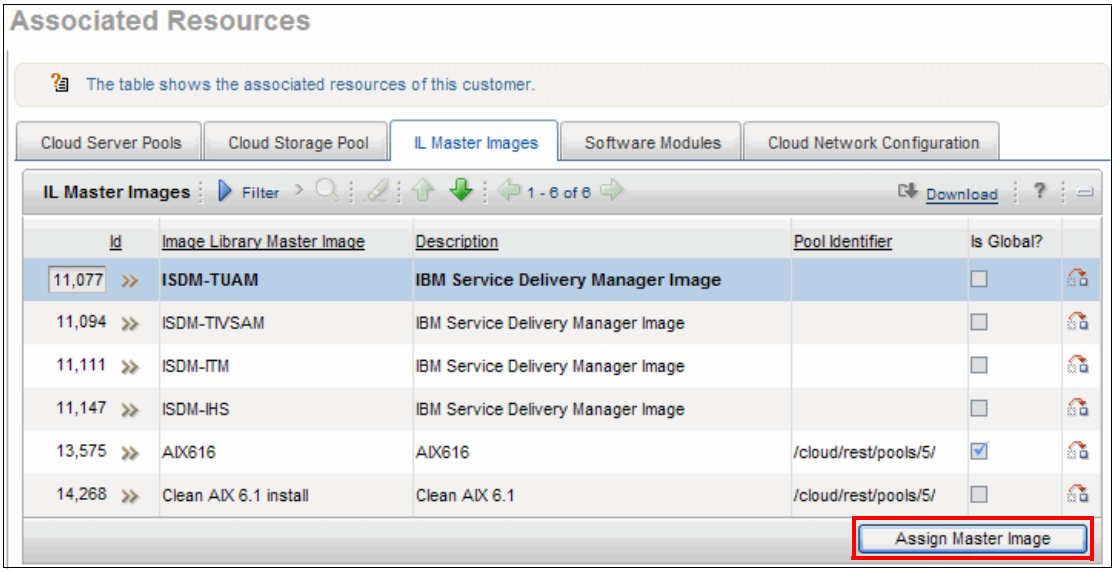

Figure 7-9 Customer's Master Images

6. Click **Assign Master Images** to add a new image to the customer. This brings up a list of images that can be assigned to the customer, as shown in Figure 7-10.

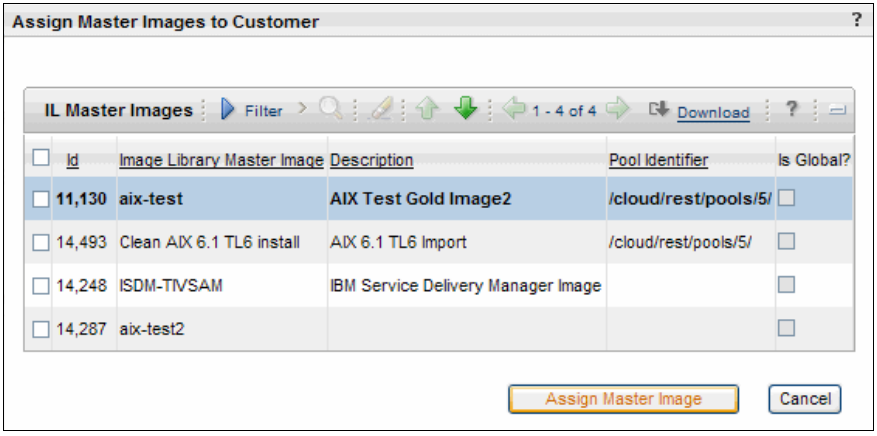

Figure 7-10 Assign Master Images to Customer

7. Select the images that you want to assign in the check boxes and click **Assign Master Image**. The table shown in Figure 7-9 on page 200 is updated with the newly assigned images.

> **Note:** If you want to make an image available to all customers, select the **Is Global** tick-box.

Now everything is in place. You can create a project that uses one of your images.

7.4 Creating a project

A project is an instance of a service deployment. When you create a process, the image with which it is associated is automatically deployed to the cloud pool.

Projects are created using the Self Service Portal of Tivoli Service Automation Manager. These are the steps to follow:

1. Log on to the Self Service Portal at `https://<TSAM>:9443/SimpleSRM` as a user with cloud or customer administration services, such as PMRDPCAUSR. You are presented with the self-service home page.
2. If you logged on as PMRDPCAUSR, then change roles to that of the customer for whom you want to create the project. This is done in the drop-down menu at the top of the home page, as shown in Figure 7-11.

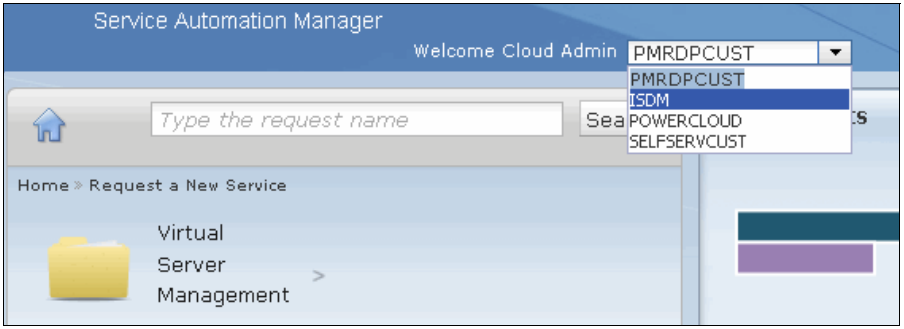

Figure 7-11 Changing customer in the self-service interface

3. Click the **Virtual Server Management** folder and scroll down to the cloud icon, **Create Project with POWER® LPAR Servers via IBM Systems Director VMControl**, shown in Figure 7-12.

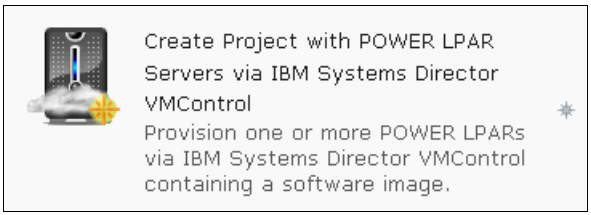

Figure 7-12 Create VMControl-based project

This launches the project creation wizard, shown in Figure 7-13. Complete the panel details with a project name, a project team, a project lifetime, and optionally a description. Click **Next**.

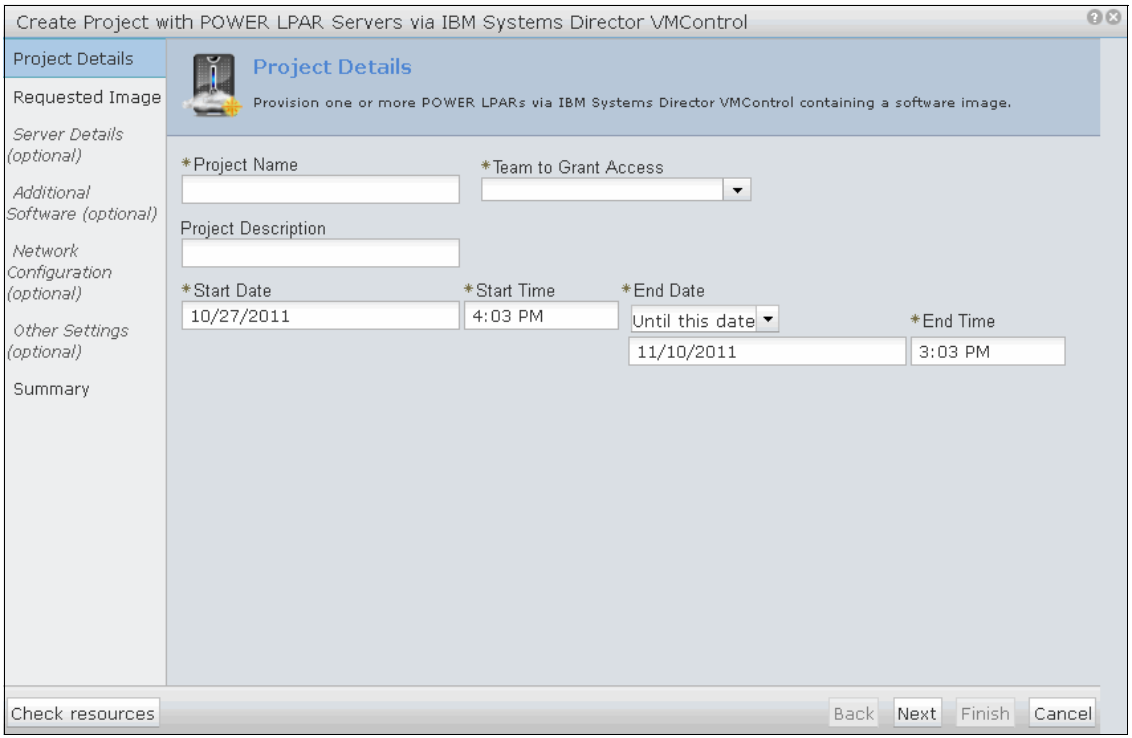

Figure 7-13 Project Details panel

4. You are presented with Requested Image panel of the wizard, shown in Figure 7-14.

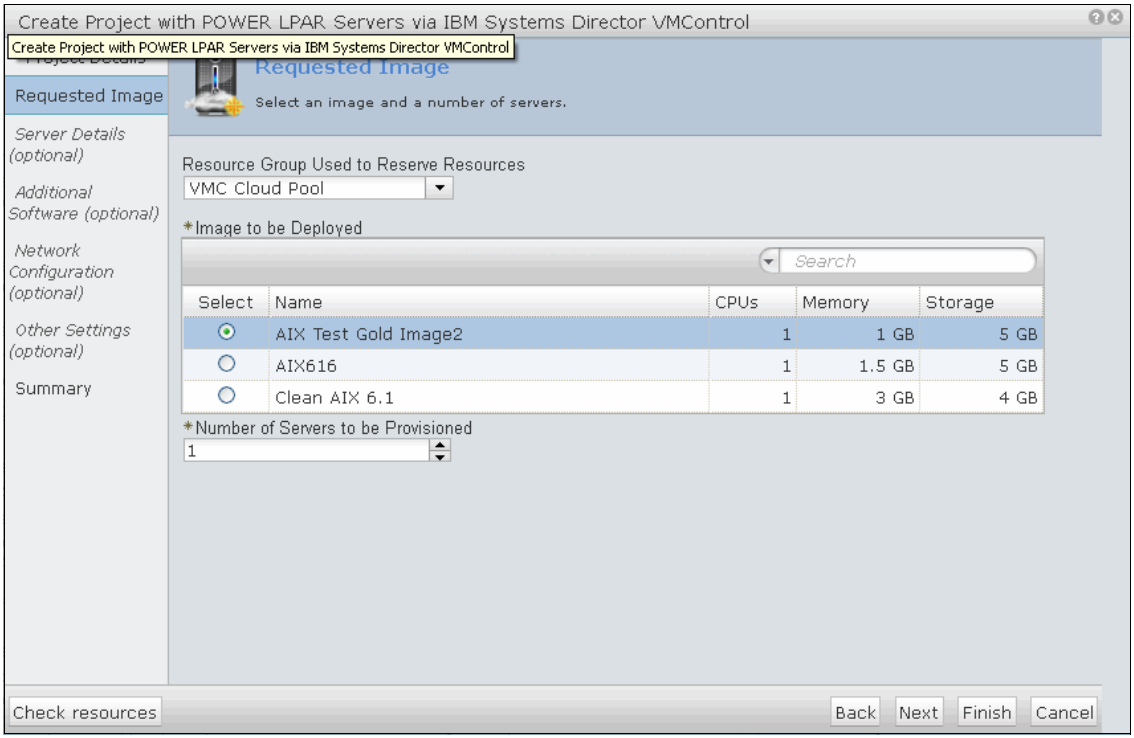

Figure 7-14 Requested Image panel

In the **Resource Group Used to Reserve Resources** drop-down menu, specify which server or VMControl server system pool the service will be deployed to.

Choose the image to be deployed from the Image to be Deployed table.

You can deploy multiple instances of the same images in a single project in the “Number of Servers to be Provisioned” field.

Note: When creating a project, you can only specify one image or service to be deployed. After the project has been created, you can modify its characteristics through the Manage Project panel to add additional images. In this way you can create a single project that contains images for different virtualization technologies.

If you do not want to make any modifications to the deployed image you can click **Finish**. Otherwise, click **Next**.

5. If you clicked **Next**, you are presented with the Server Details panel (shown in Figure 7-15), where you can change the resources allocated to the service within the limits given in the OVF file. For VMControl, these limits correspond to the minimum and maximum resource values in the partition profile.

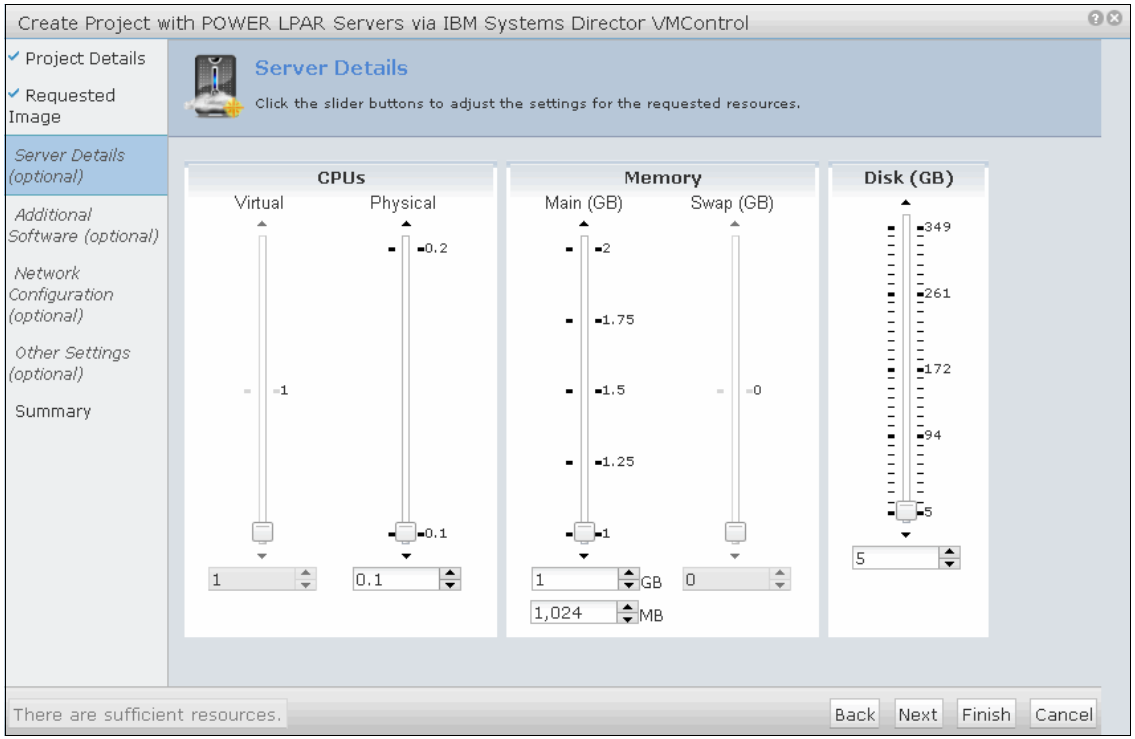

Figure 7-15 Server Details panel

Make the required changes, ensure that the message at the bottom of the panel shows `There are sufficient resources`, and click **Next**.

6. This takes you to the Additional Software panel (Figure 7-16). This allows you to customize the deployed image with additional software. Click **Next**.

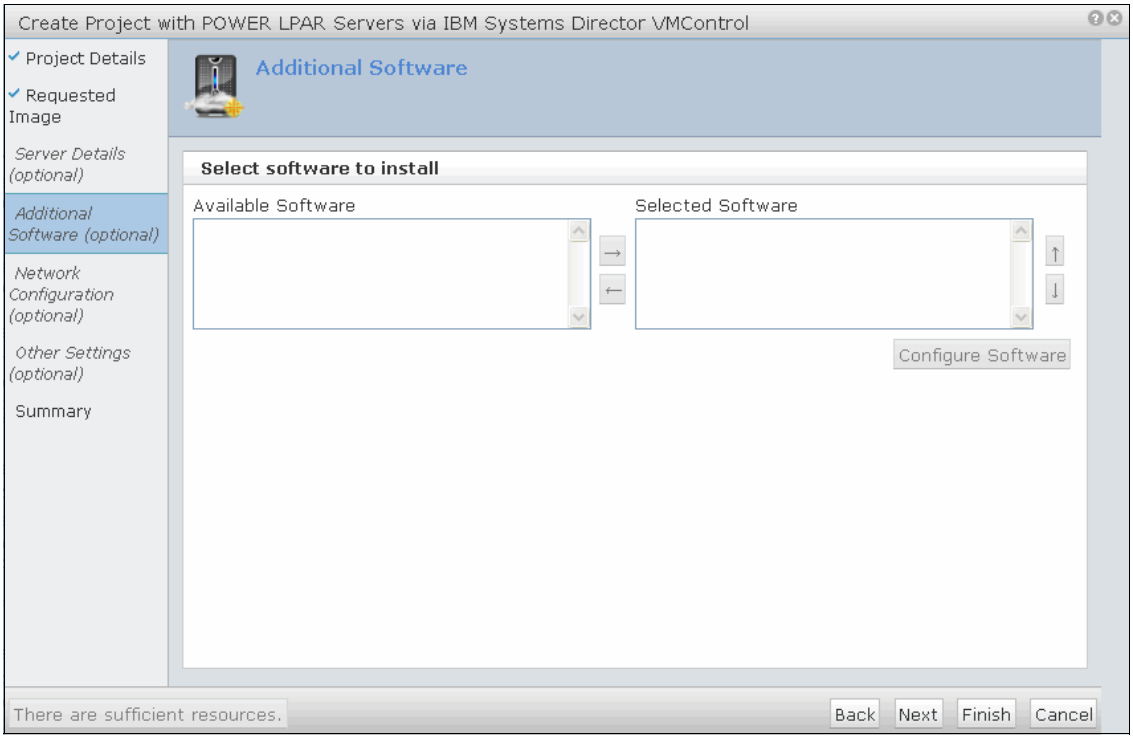

Figure 7-16 Additional Software panel

7. You are presented with the Network Configuration panel (Figure 7-17).

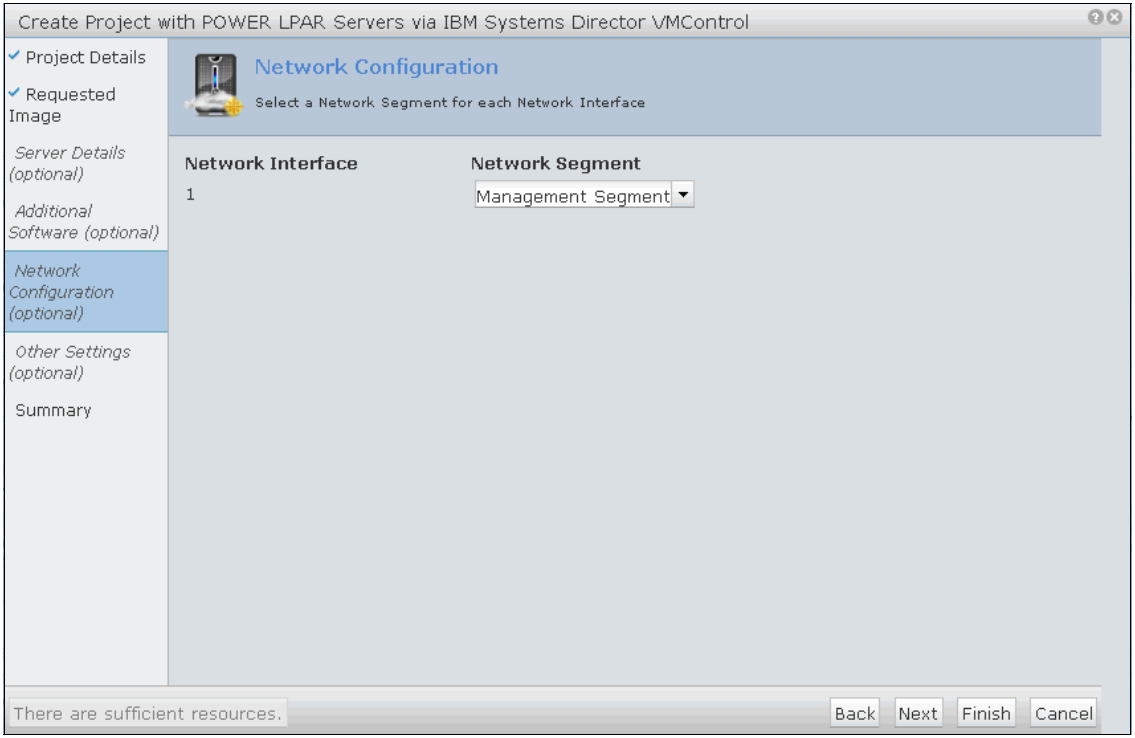

Figure 7-17 Network Configuration panel

Here you select the network that the service will use. The names correspond to those that you specified in `NetworkTemplate.xml` and from there links back to the subnetwork specification in `DCM_objects.xml` (in 5.3.1, “DCM_objects.xml” on page 109).

Choose the network that you want to use and click **Next**.

8. The next panel (Figure 7-18) gives you the option to install a monitoring agent in the project. If you have set IBM Tivoli Monitoring, then you can tick the box, which provides you with more details regarding the health and resource usage of the project. Otherwise, leave it blank. We have IBM Tivoli Monitoring up and running, so the box is ticked.

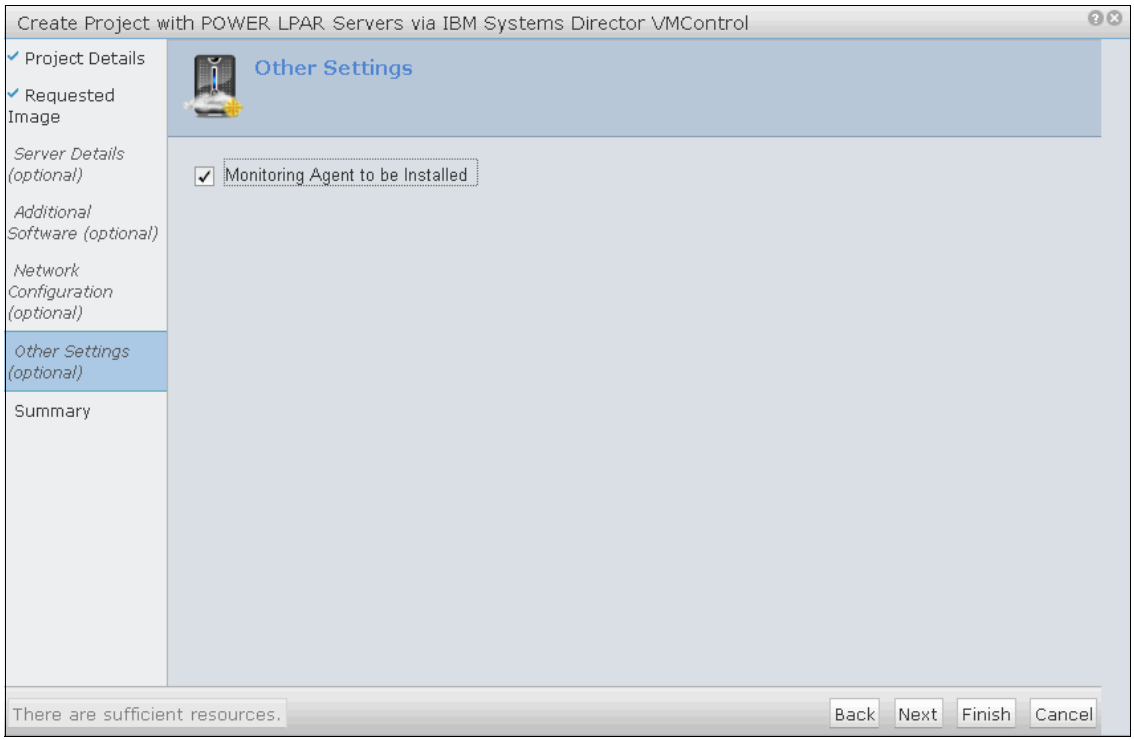

Figure 7-18 Other Settings panel

Note: The Additional Software panel is to install software components other than the monitoring agent.

Clicking **Next** takes you to the Summary panel (Figure 7-19). Check all the values. If you want to make changes you can click **Back** to the relevant step in the wizard. Otherwise, click **Finish**.

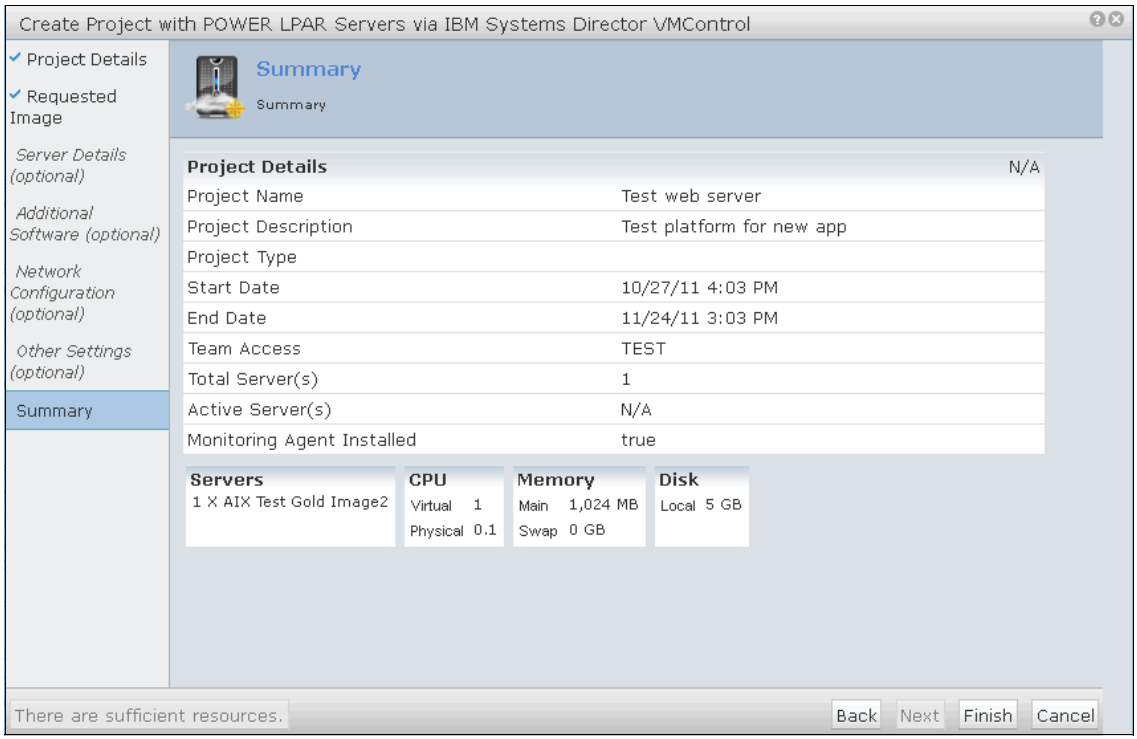

Figure 7-19 Summary panel

Clicking **Finish** launches the workflow to provision the image to the cloud pool and create the project. You are taken back to the Virtual Server Management panel of the Self Service Portal. In the My Requests pod you will see your newly created workflow in the new state, as shown in Figure 7-20.

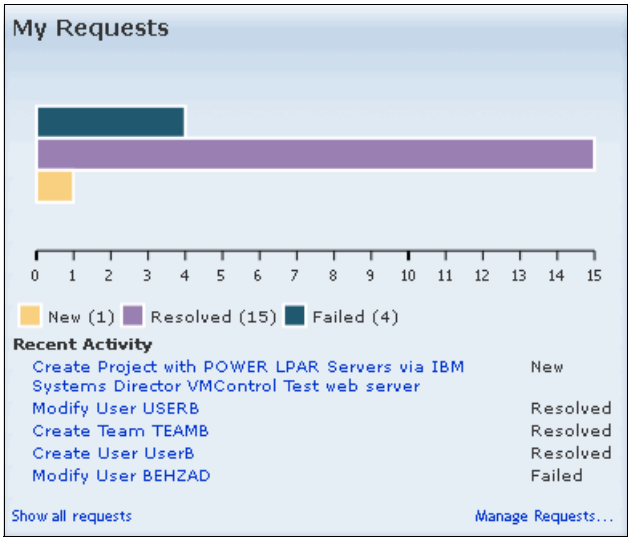

Figure 7-20 My Requests: New project

If approvals are configured for projects, shortly after appearing in the new state, the workflow will change to Waiting for approval, shown on the right in Figure 7-21, and the approval request will display in the My Approvals pod of the approver, shown on the right.

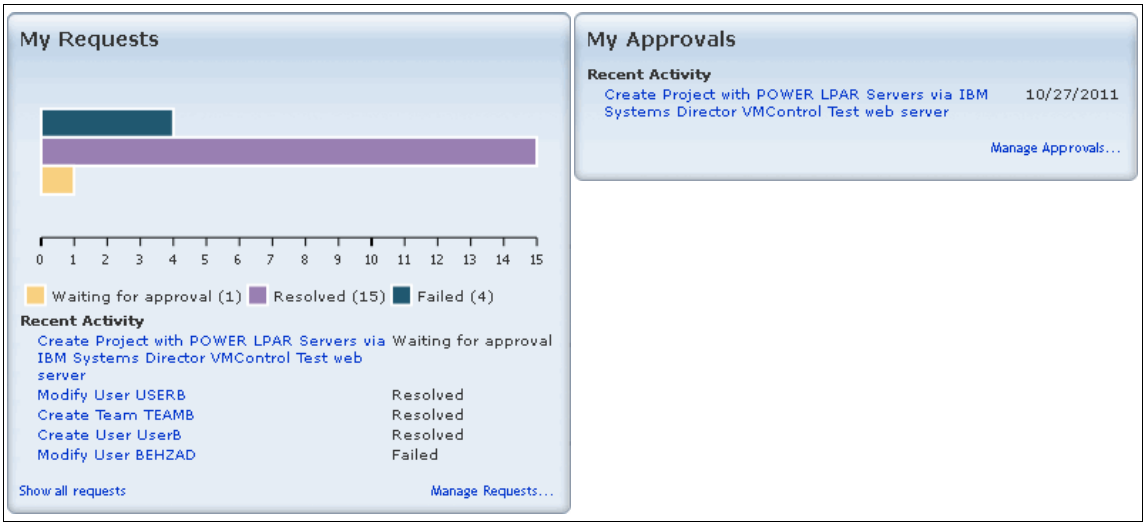

Figure 7-21 Waiting for approval

Clicking the **Manage Approvals** link displays the Manage Approvals pop-up, shown in Figure 7-22. Click the green tick to approve, or the no-entry sign to refuse.

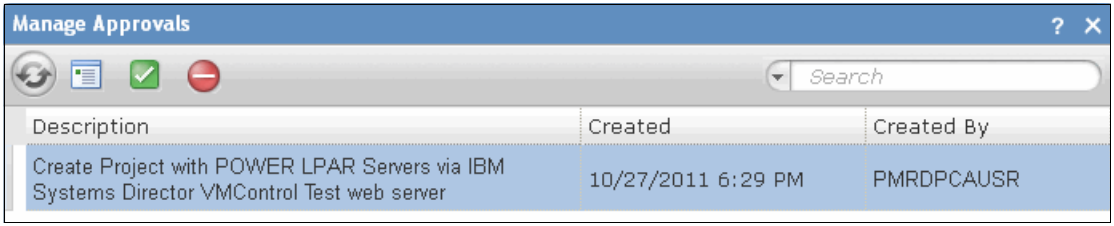

Figure 7-22 Manage Approvals

After it is approved and the service is deployed, your project displays in the My Projects pod and users can connect to it.

7.5 Installing additional software

Before you can install additional software modules on the provisioned virtual machines in the self-service user interface, you need to create software product definitions in Tivoli Provisioning Manager and then configure them.

In this section, you enable the IBM HTTP Server to be installed on virtual servers, as they are provisioned from the self-service user interface. You will use the IBM HTTP Server 6.1 software definition that comes with Tivoli Provisioning Manager. Before you can install the HTTP Server, you must define the target image in the software definition and expose this software product to the self-service user interface.

You need to be the Tivoli Service Automation Manager administrator (maxadmin) to perform this task:

1. Copy the IBM HTTP Server installation source **ihs.6100.aix.ppc32.tar** to the file repository `/repository/IBM_HTTP_Server/AIX` on the NFS server.
2. Log in to the Tivoli Service Automation Manager as maxadmin.

3. Click **Go To** → **IT Infrastructure** → **Software Catalog** → **Software Products** (Figure 7-23).

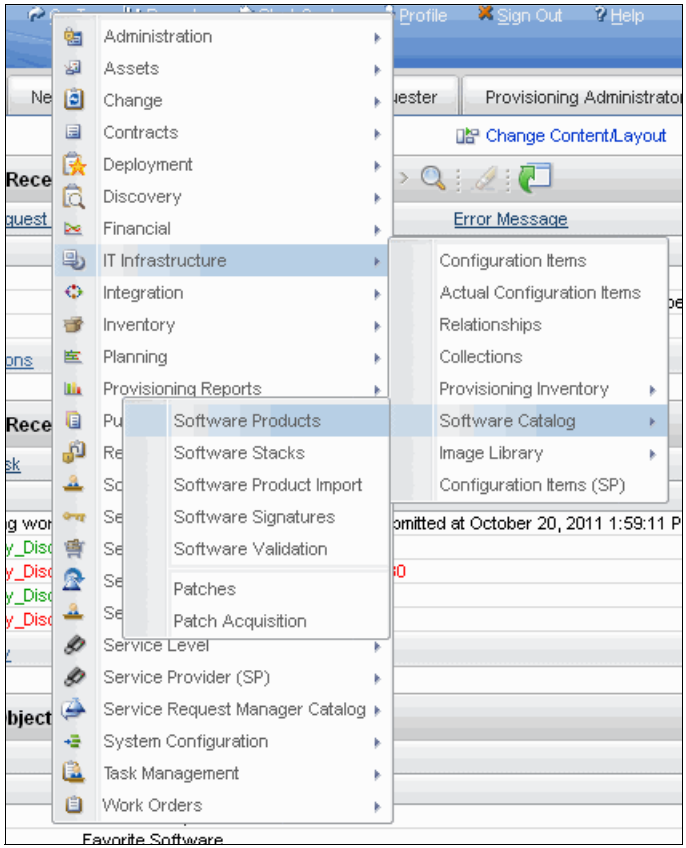

Figure 7-23 Software products tab

4. Filter the software definition name based on HTTP (Figure 7-24).

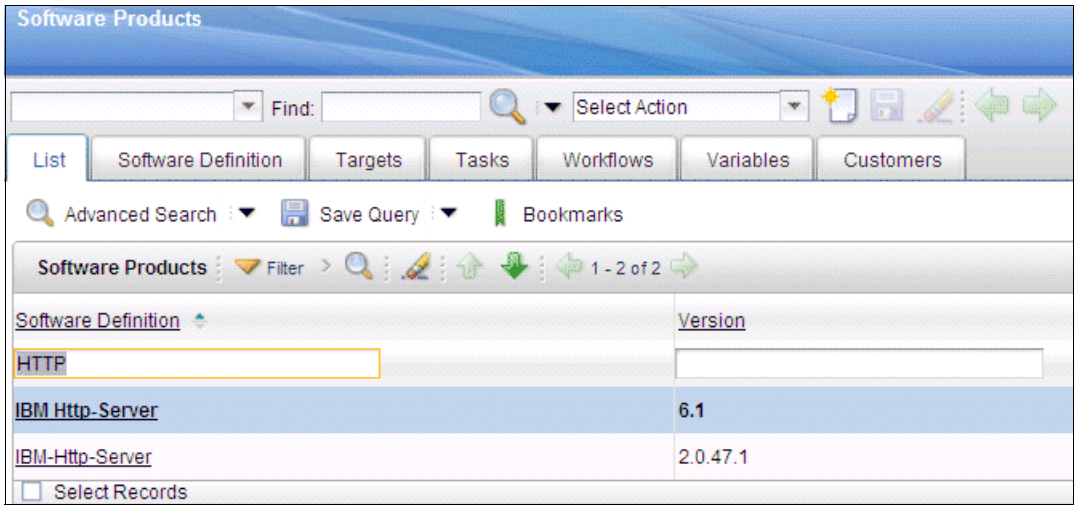

Figure 7-24 HTTP filter

5. Select the software definition **IBM Http-Server** (Version 6.1) from the list (Figure 7-25) and click **View Details** for the IBM HTTP Server for AIX installable.

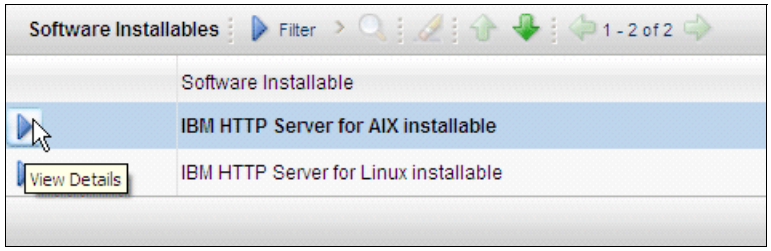

Figure 7-25 IBM Http-Server

6. Modify the following fields (Figure 7-26):
   - Package Path: `/IBM_HTTP_Server/AIX`
   - File: `ihs.6100.aix.ppc32.tar`
   - File Repository: `CloudFileRepository`

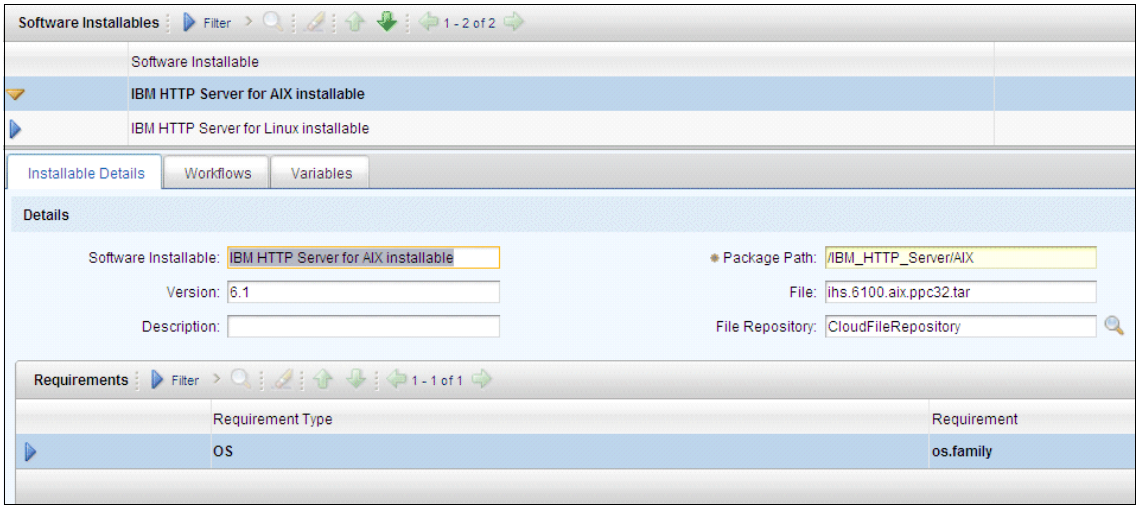

Figure 7-26 Fields to modify

7. Click the **Variables** tab for the software product definition. Click **New Row** to define a new variable (Figure 7-27). The variable exposetotivsam enables the software to be displayed on the self-service user interface and selected when provisioning a virtual server.

   Enter these values into the following fields:
   - Variable: `exposetotivsam`
   - Value: `1`

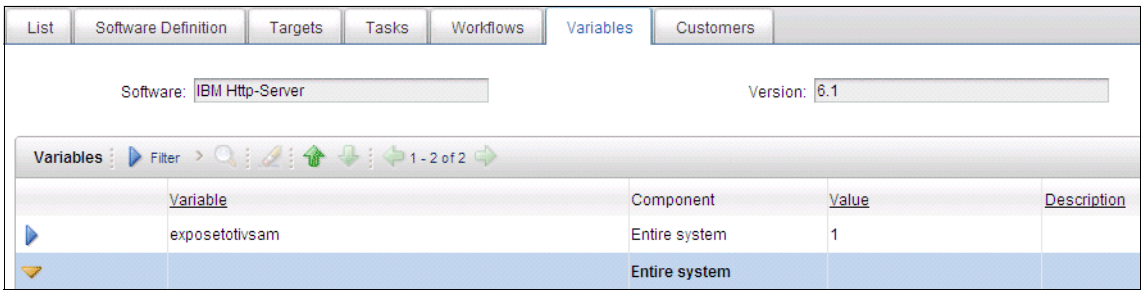

Figure 7-27 Entering a new row

8. Click **Save Software Product**.

9. Configure the OSDS_Pool_host_Stack software stack to include the **IBM Http-Server** Software. Click **Go To** → **IT Infrastructure** → **Software Catalog** → **Software Stacks** to display the list of known software stacks (Figure 7-28).

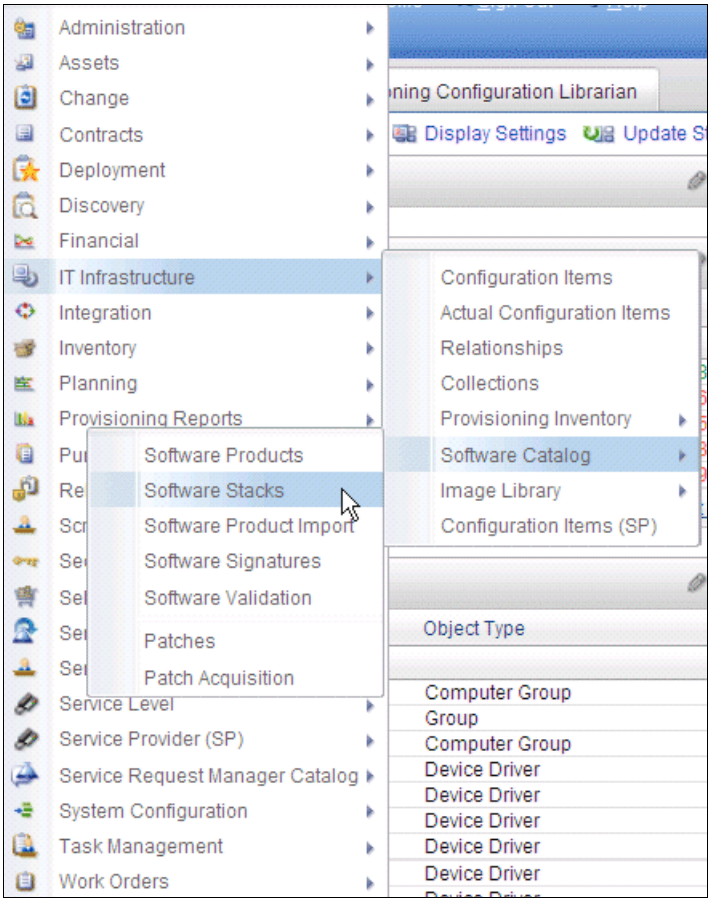

Figure 7-28 Configuring the software stacks

10. Select **OSDS_Pool_host_Stack** and click **Add Stack Entry** (Figure 7-29).

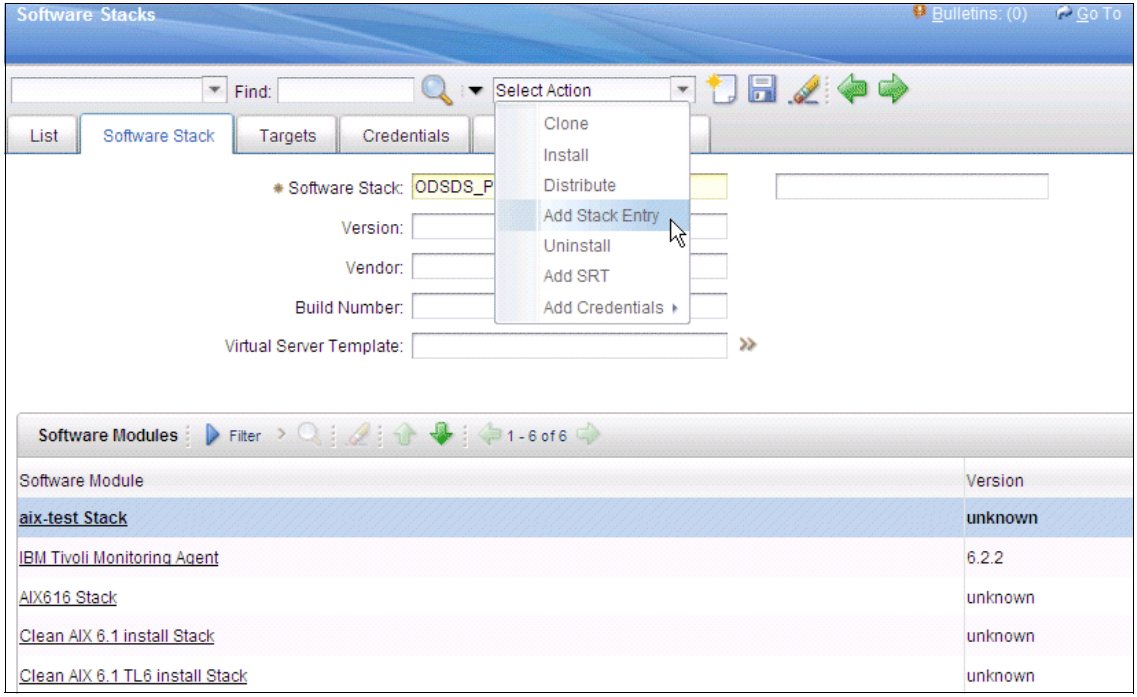

Figure 7-29 Adding a stack entry

11. Filter for a software definition based on HTTP, select **IBM Http-Server** (Version 6.1), and click **Submit** (Figure 7-30).

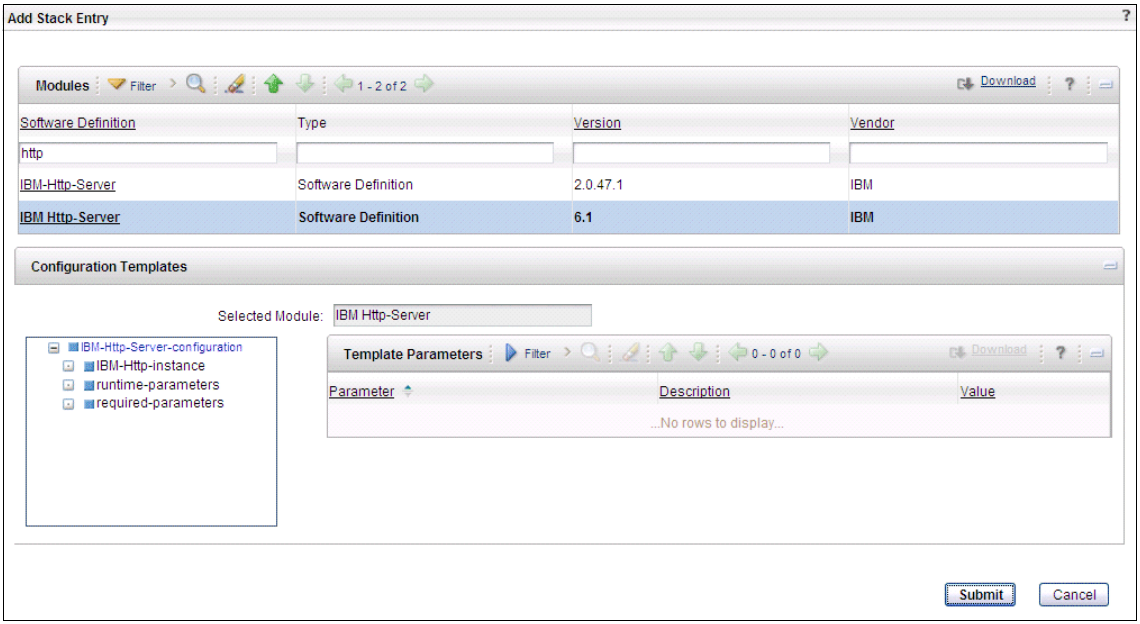

Figure 7-30 Filtering for the HTTP server

12. Assign the new software to a customer using the Cloud Customer Administration. Click **Go To** → **Service Automation** → **Configuration** → **Cloud Customer Administration** (Figure 7-31).

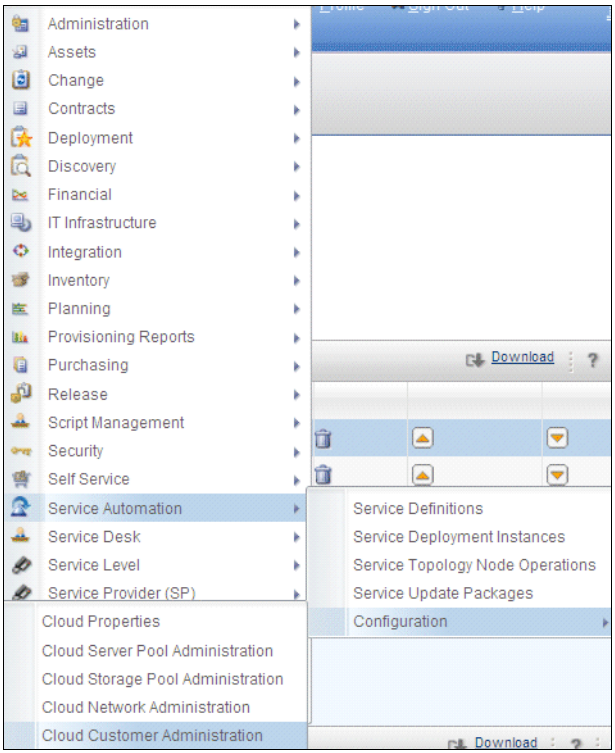

Figure 7-31 Configuring the cloud customer

13. Press the Enter key on your keyboard to display the list of customers. Select the **ISDM** customer (Figure 7-32).

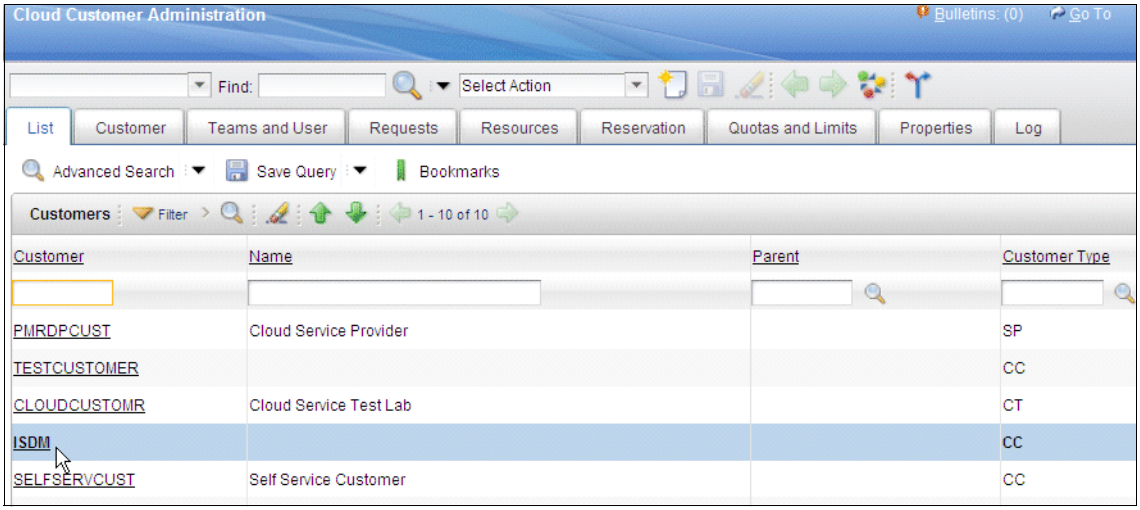

Figure 7-32 Selecting the customer

14. Select the **Software Modules** tab. Click **Assign Software Product** to add the software product (Figure 7-33).

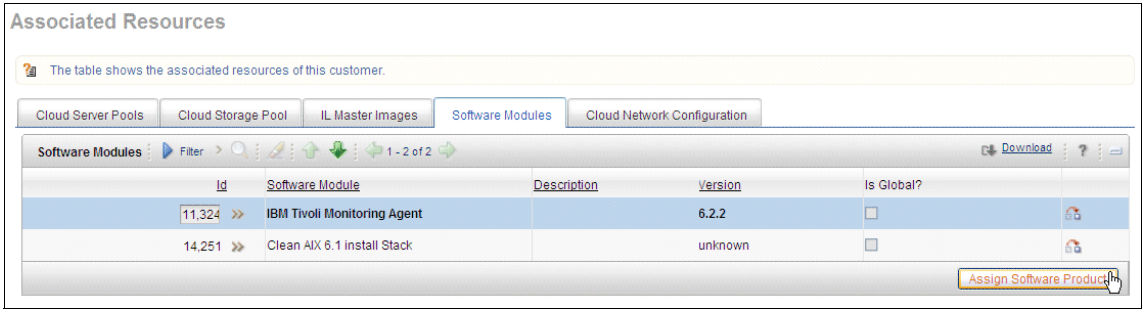

Figure 7-33 Assigning the software product

15. Select the **IBM Http-Server** check box and click **Assign Software Module** (Figure 7-34).

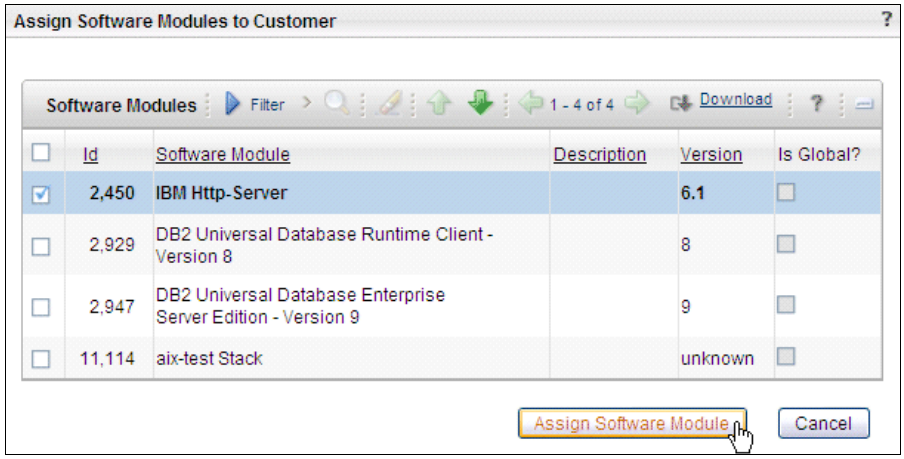

Figure 7-34 Connecting the software module and product

16. Verify that the IBM Http-Server Software is in the list, then click **Save Customer** (Figure 7-35).

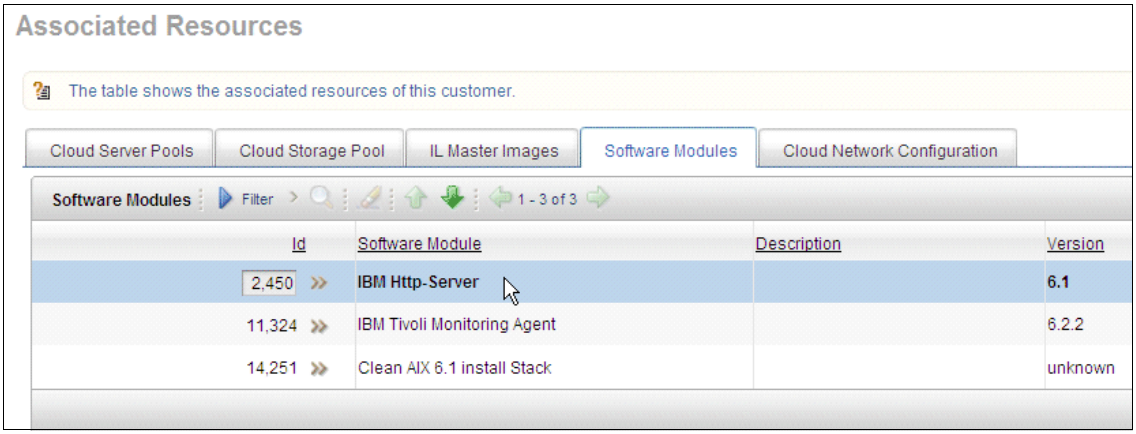

Figure 7-35 Saving the work

After you have defined the software product, you can install that software on a virtual machine using the self-service user interface.

7.6 Installing software on the server

After you have defined the software product, you can install that software on a virtual machine using the self-service user interface:

1. In the Home panel, click **Request a New Service** → **Virtual Server Management** → **Create Project with POWER LPAR Servers via IBM Systems Director VMControl** (Figure 7-36).
2. Complete the panel details with a project name, a project team, a project lifetime, and optionally a description, and then click **Next**.

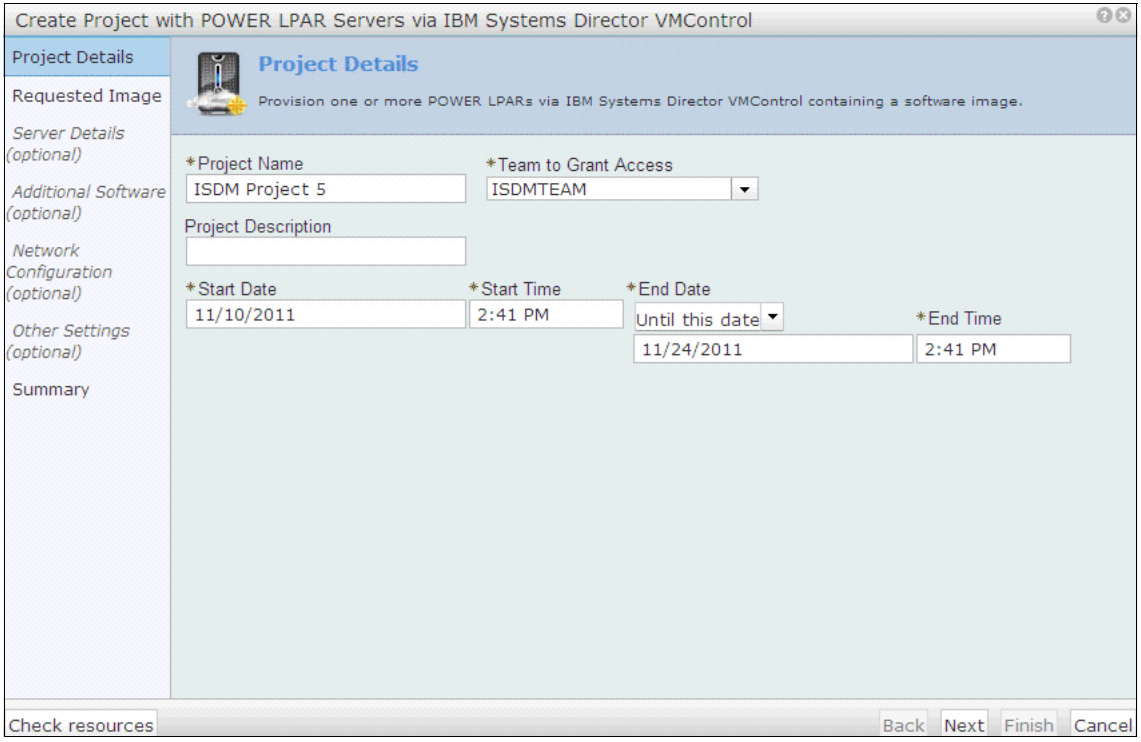

Figure 7-36 Requesting the image

3. Select **VMC Cloud Pool** for the resource group, select **Clean AIX 6.1** for the image to be deployed, and click **Next**.

4. Verify CPU, memory, and disk capacity (Figure 7-37), and then click **Next**.

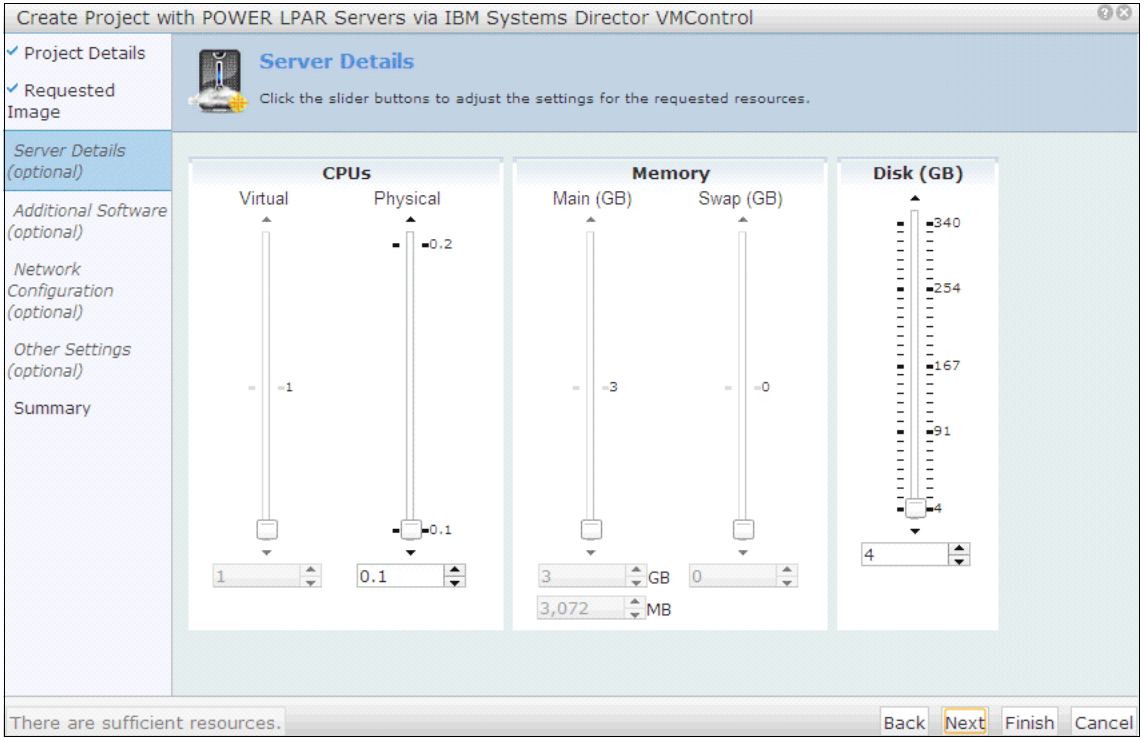

Figure 7-37 Setting the software requirements

5. Use the arrows to select the IBM Http-Server software to be installed on the provisioned servers. If the software item requirements can be fulfilled, its name will display in the Selected Software box (Figure 7-38). Click **Finish**.

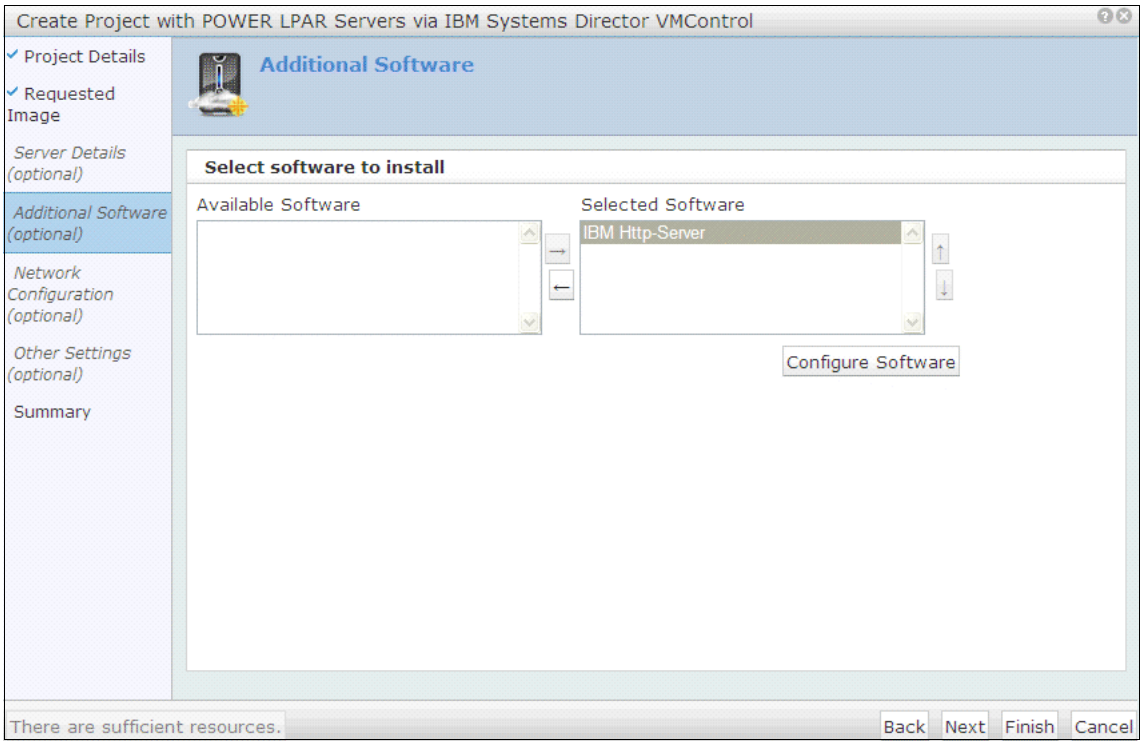

Figure 7-38 Finishing the deployment

8

Configuration of IBM Tivoli Monitoring agents

The IBM Tivoli Monitoring agent is used to gather statistics about LPAR resources and send the information to the IBM Tivoli Monitoring server. You can log on to the IBM Tivoli Monitoring Server and view a graphical representation of the partiton's statistics.

An explanation of how to use IBM Tivoli Monitoring can be found in *Deployment Guide Series: IBM Tivoli Monitoring 6.1*, SG24-7188.

8.1 Configuration of the IBM Tivoli Monitoring agent for deployment at provisioning time

By default the IBM Tivoli Monitoring agent is not deployed on virtual images deployed using IBM Service Delivery Manager. The IBM Tivoli Monitoring agent software stack needs to be configured in Tivoli Service Automation Manager so that it can be deployed at provisioning time.

To configure the IBM Tivoli Monitoring agent to be deployed at provisioning time, perform the following procedure:

1. Log in to the Tivoli Service Automation Manager administrative web interface as the maxadmin user.
2. From the menu on the top of the Tivoli Service Automation Manager administration screen select **Go To** → **IT Infrastructure** → **Software Catalog** → **Software Stacks**, as shown in Figure 8-1.

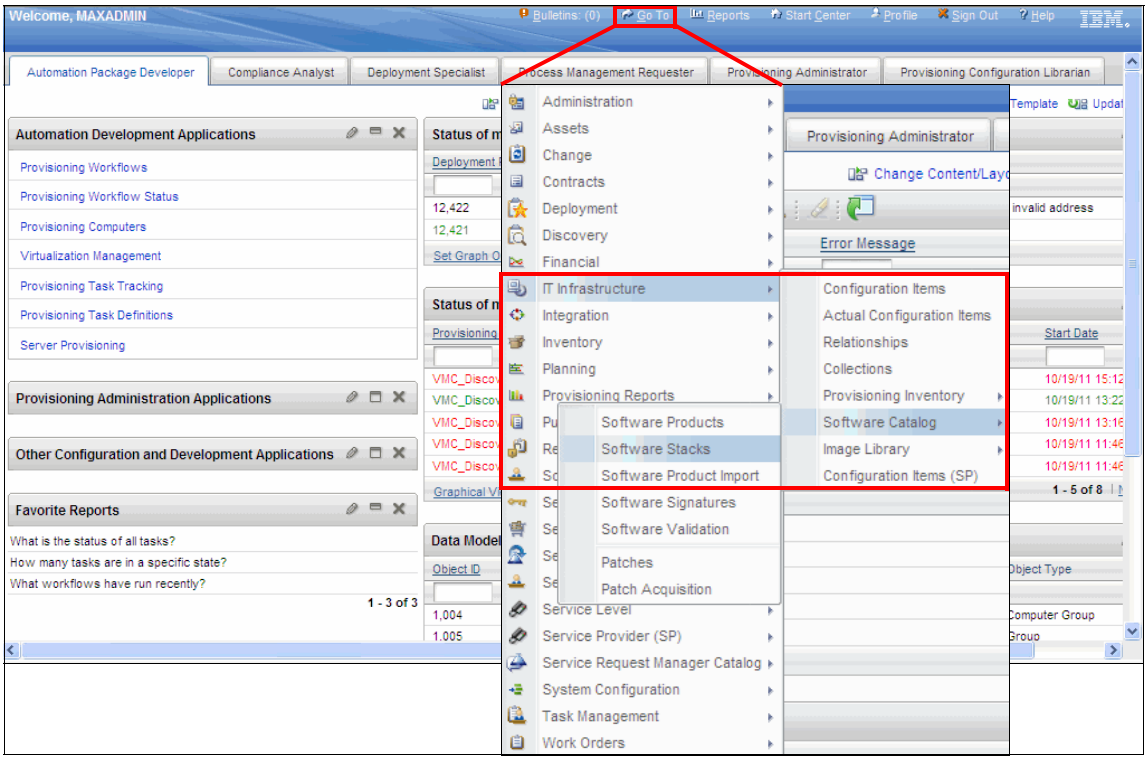

Figure 8-1 Open the software stacks interface

3. Click the software stack that was defined in your `DCM_objects.xml` file, which was imported in 5.3.1, “DCM_objects.xml” on page 109. In our example, we clicked our software stack named OSDS_Pool_host_Stack, as shown in Figure 8-2.

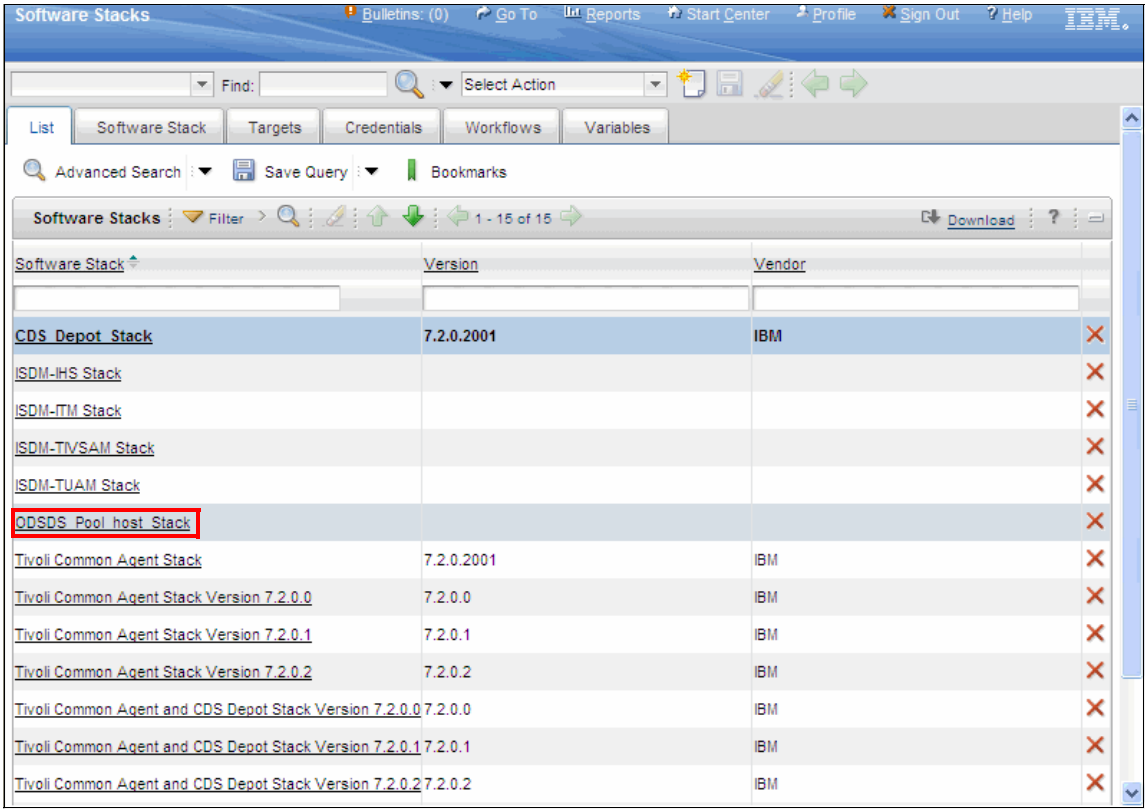

Figure 8-2 Select your software stack defined in DCM

4. The software stack screen opens. To add the IBM Tivoli Monitoring agent to the software stack click **Select Action** → **Add Stack Entry**, as shown in Figure 8-3.

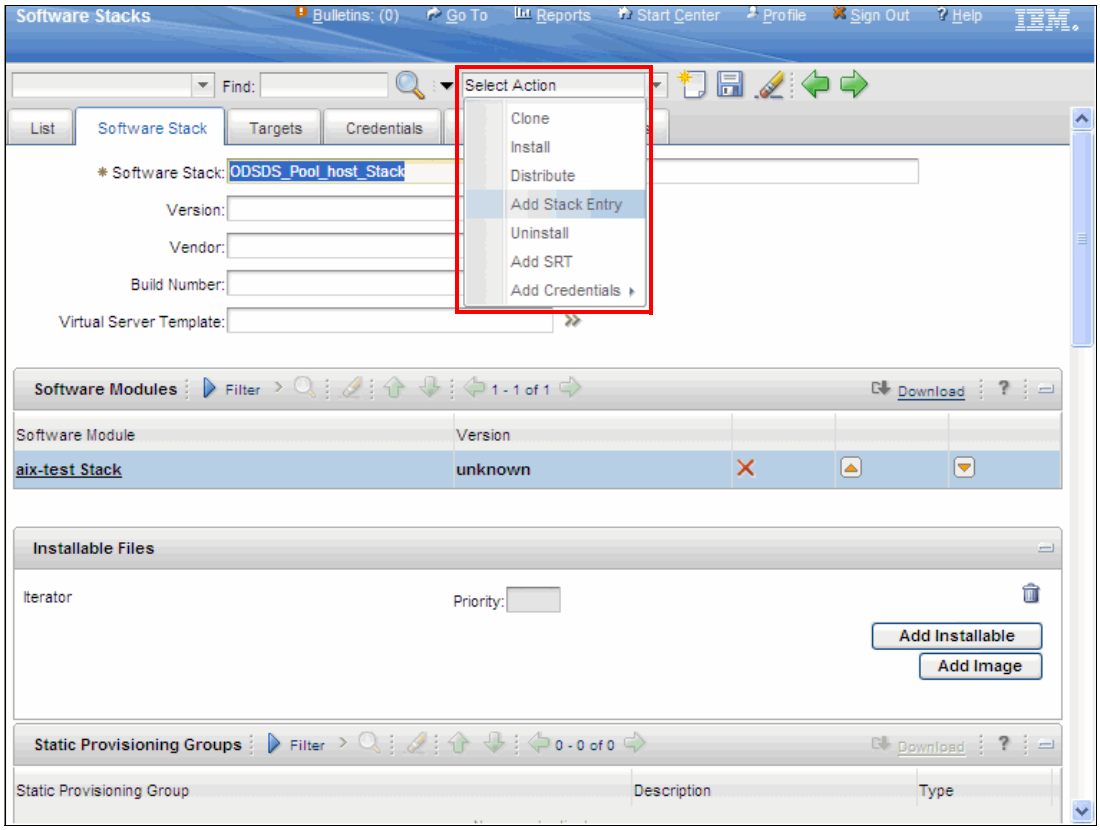

Figure 8-3 Add new software stack

5. On the software defining panel that opens, type `IBM Tivoli Monitoring Agent` into the Software Definition Edit field and press Enter, as shown in Figure 8-4.

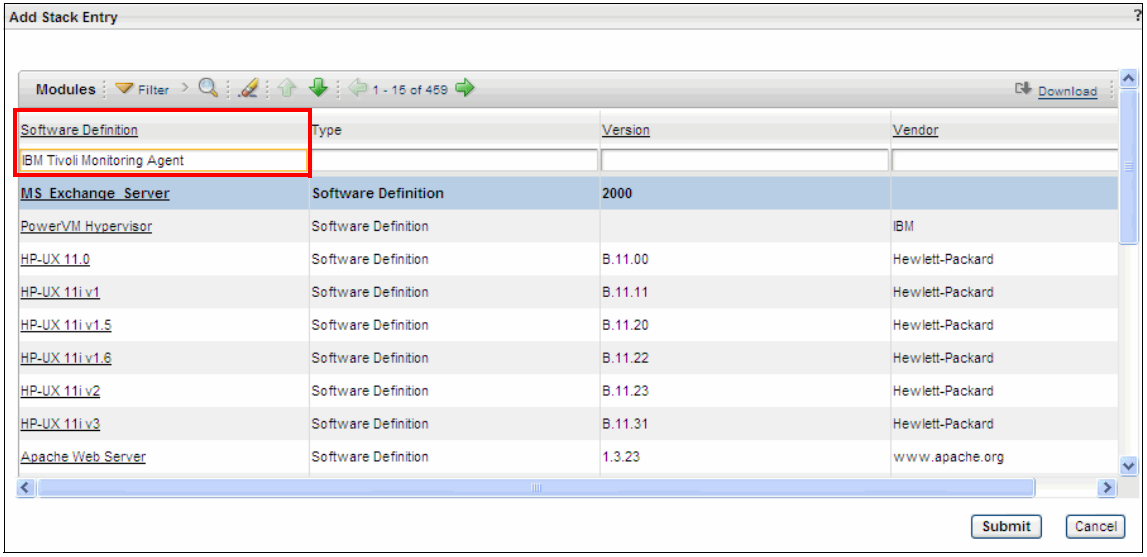

Figure 8-4 Find the ITM agent

6. Click **IBM Tivoli Monitoring Agent**, then click **Submit**, as shown in Figure 8-5. The IBM Tivoli Monitoring agent properties can also be checked from this screen.

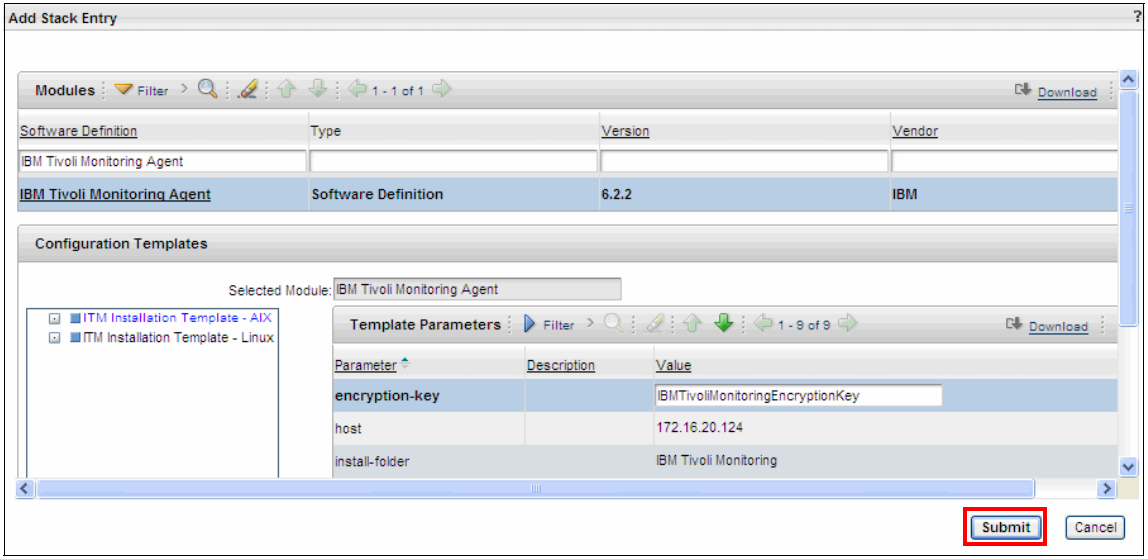

Figure 8-5 Select the ITM agent

Note: If you have difficulty finding the IBM Tivoli Monitoring Agent, ensure that your service connection engine configuration is correctly running. The IBM Tivoli Monitoring Agent is imported in Tivoli Service Automation Manager only when the service connection engine is configured correctly.

We were required to run the service connection engine three times before the IBM Tivoli Monitoring Agent appeared in the software stack. This feature has been noticed on different test systems, including VMware ISDM deployments.

If unsure, run the service connection engine.

7. Click the floppy disk save icon, to save the configuration, as shown in Figure 8-6.

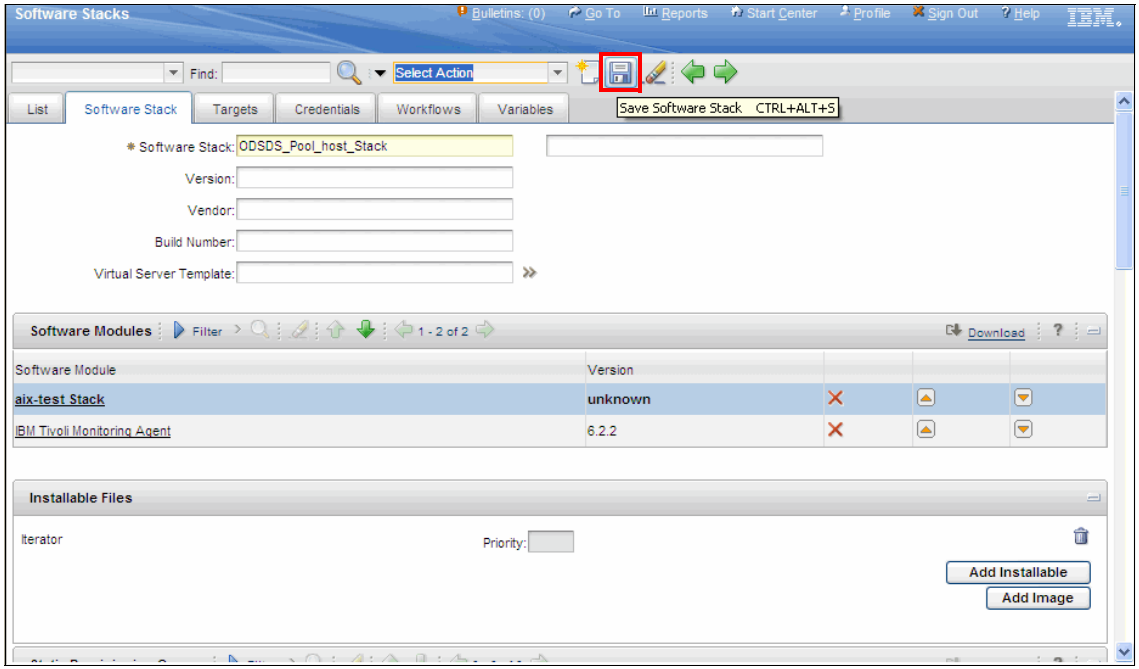

Figure 8-6 Save the configuration

The IBM Tivoli Monitoring agent has now been added to your software stack and is available for deployment at provisioning time. Any new servers that are deployed as part of a project using the Self Service Portal can now select to install the IBM Tivoli Monitoring agent. The IBM Tivoli Monitoring Agent is configured to connect to the IBM Service Delivery Manager IBM Tivoli Monitoring virtual image. It is possible to configure the agent to communicate with a different IBM Tivoli Monitoring server than the one that is delivered with IBM Service Delivery Manager.

Note: It is possible to import an IBM Tivoli Monitoring agent and configuration for a different existing IBM Tivoli Monitoring server which is already part of your existing IT management infrastructure. For the procedure for how to perform this task, refer to the IBM Tivoli Service Automation Manager information center:

`http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?topic=%2Fcom.ibm.tsam_7.2.2.doc%2Ft_config_itm_agent.html`

8.2 Configuring cloud resource IBM Tivoli Monitoring agents

It is possible to configure IBM Tivoli Monitoring agents on the Virtual I/O server, Hardware Management Console, and IBM Systems Director servers. Most of the IBM Tivoli Monitoring agents are already installed, except for the IBM Director Server the agents, which come as part of the IBM Systems Director Server software. All of the agents require configuration to report to the Tivoli Monitoring Server.

To configure the agents so that they will report to the IBM Tivoli Monitoring server, you will require the following information:

- Host name or IP address of the IBM Tivoli Monitoring Server
- Host name of the Hardware Management Console
- User name of a privileged Hardware Management Console user

Table 8-1 lists the variables that we used in our environment.

Table 8-1 List of variables we used in our implementation

Property	Value
ITM server hostname	`itm.powercloud.ibm.com`
HMC server hostname	`hmc.powercloud.ibm.com`
HMC user	`hscroot`

The Tivoli Monitoring Server host name was `itm.powercloud.ibm.com`.

8.2.1 Virtual I/O server agent configuration

The Virtual I/O server has two IBM Tivoli Monitoring agents installed by default:

- `ITM_premium`
- `ITM_cec`

These agents provide system information including I/O virtualization mappings and system utilization to the IBM Tivoli Monitoring Server.

There is a third monitoring agent installed, the IBM Systems Director agent. The IBM Systems Director agent is already configured to return performance data to the IBM Systems Director server. The agent views and tracks hardware information and monitors performance and use of critical components, such as processors, disks, and memory.

To configure the IBM Tivoli Monitoring agents on the Virtual I/O Server, perform the following tasks:

1. Log in to the Virtual I/O Server as the padmin user.
2. Run the **lssvc | grep ITM** command to list the ITM services, as shown in Example 8-1.

Example 8-1 List the ITM agents

```
$ lssvc | grep ITM
ITM_premium
ITM_cec
```

3. Configure the ITM_premium agent by running the following command:

```
cfgsvc ITM_premium -attr
MANAGING_SYSTEM=<hmc_username>@<hmchostname> HOSTNAME=<ITM hostname>
RESTART_ON_REBOOT=true
```

Where the variable *<ITM hostname>* is the host name or IP address of your IBM Tivoli Monitoring Server, variable *<hmc_username>* is the name of a privileged Hardware Management Console user, and variable *<hmchostname>* is the hostname or IP address of the hardware management console.

An example of the command and the output can be seen in Example 8-2.

Example 8-2 Configuration command of the ITM_preumium agent

```
$cfgsvc ITM_premium -attr
MANAGING_SYSTEM=hscroot@hmc.powercloud.ibm.com
HOSTNAME=itm.powercloud.ibm.com RESTART_ON_REBOOT=true
Agent configuration started...
Agent configuration completed...
```

4. Configure the ITM_premium agent by running the following command:

cfgsvc ITM_cec -attr MANAGING_SYSTEM=<*hmc_username*>@<***hmchostname***> **HOSTNAME**=<*ITM hostname*> **RESTART_ON_REBOOT=true**

Where the variable *<ITM hostname>* is the hostname or IP address of your IBM Tivoli Monitoring Server, variable *<hmc_username>* is the name of a privileged Hardware Management Console user, and variable *<hmchostname>* is the host name or IP address of the hardware management console.

An example of the command and the output can be seen in Example 8-3.

Example 8-3 Configuration of the ITM_cec agent on VIOS

```
$ cfgsvc ITM_cec -attr
MANAGING_SYSTEM=hscroot@hmc.powercloud.ibm.com
HOSTNAME=itm.powercloud.ibm.com RESTART_ON_REBOOT=true
Agent configuration started...
Agent configuration completed...
```

5. For the IBM Tivoli Manager agents to work correctly, and to ensure that no errors are produced when starting the agents, ssh keys need to be exchanged between the Hardware Management Console and the Virtual I/O Server. To do this perform the following steps:

   a. On the Virtual I/O Server as the padamin user run the following command to see the ssh key used by the IBM Tivoli Monitoring agents:

      ```
      cfgsvc ITM_premium -key
      ```

      An example of our configuration can be seen in Example 8-4.

      Example 8-4 Command to display ITM agent ssh public key

      ```
      $ cfgsvc -key ITM_premium
      ssh-rsa
      AAAAB3NzaC1yc2EAAAADAQABAAABAQClc3Up4bDEhyZqdOfh2H3Y+uznPrDBICBb/
      SLJ2zIIWaS+9DVO7inBECNaULo/jUifNwHwdlDPT/B2QOLu1F9G5Z4YaQq9glFqDK
      qH3v+BhBReU5hlqSRbUKnebml+klCTDJOSHjOcgfdjyRECyaWw2XdBrBtlE4xvLe2
      5QuhzO3gwjwiIuFAOr4rjAkgYUR7amTDkOXdh4x+sOt+UoUJhL5lbmDSpOVB6FTeP
      xrb/7wBntnNdjiwdRssUqdRsRonaF/iGB7cwO9T3o++rNKznrUKK3BgMiKIhPHVQP
      69DOyUMt/+bC5kzhDVv4FbgkjYjMquyOEoc3eJZFv29O22b root@VIOS1A
      ```

   b. Log on to your hmc as the hmc user specified in step 3 on page 233 and add the public ssh key using the following command:

      mkauthkeys -a '*<ssh-key>***'**

      The variable <*ssh-key*> is the output from the **cfgsvc -key ITM_premium** command. An example of the command we use can be seen in Example 8-5.

      Example 8-5 Command to add an ssh key to an hmc user

      ```
      hscroot@hmc:~> mkauthkeys --add 'ssh-rsa
      AAAAB3NzaC1yc2EAAAADAQABAAABAQClc3Up4bDEhyZqdOfh2H3Y+uznPrDBICBb/
      SLJ2zIIWaS+9DVO7inBECNaULo/jUifNwHwdlDPT/B2QOLu1F9G5Z4YaQq9glFqDK
      qH3v+BhBReU5hlqSRbUKnebml+klCTDJOSHjOcgfdjyRECyaWw2XdBrBtlE4xvLe2
      5QuhzO3gwjwiIuFAOr4rjAkgYUR7amTDkOXdh4x+sOt+UoUJhL5lbmDSpOVB6FTeP
      ```

```
xrb/7wBntnNdjiwdRssUqdRsRonaF/iGB7cwO9T3o++rNKznrUKK3BgMiKIhPHVQP
69DOyUMt/+bC5kzhDVv4FbgkjYjMquyOEoc3eJZFv29O22b root@VIOS1A'
```

c. Exit the Virtual I/O Server shell by running the **oem_setup_env** command. This ensures that we have a new shell as the root user.

d. Run the **ssh** command from the Virtual I/O Server as root and ssh to the Hardware Management Console. This caches the ssh key of the Hardware Management Console to the `/.root/known_hosts` file and prevents the agent from requesting to confirm authenticity each time that the agent is started. This step also confirms that the ssh key exchanging is working correctly between the two hosts, as there should be no prompting to enter a password. An example of the command that we performed is shown in Example 8-6.

Example 8-6 Caching of the ssh fingerprint key

```
# ssh hscroot@hmc.powercloud.ibm.com
The authenticity of host 'hmc.powercloud.ibm.com (172.16.20.111)'
can't be established.
RSA key fingerprint is
16:55:25:54:ed:68:63:c2:76:2f:60:e9:66:75:01:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'hmc.powercloud.ibm.com' (RSA) to the
list of known hosts.
Last login: Mon Oct 24 11:00:21 2011 from 172.16.20.120
hscroot@hmc:~>
```

e. Exit the root shell and return to the Virtual I/O Server shell by running the **exit** command.

6. Start the agents with the following commands:

```
startsvc ITM_premium
startsvc ITM_cec
```

An example of the commands that we used and the output is shown in Example 8-7.

Example 8-7 Commands to start the ITM agents on VIOS

```
$ startsvc ITM_premium
Starting Premium Monitoring Agent for VIOS ...
Premium Monitoring Agent for VIOS started
$ startsvc ITM_cec
Starting Base Monitoring Agent for CEC ...
Base Monitoring Agent for CEC started
```

7. Confirm that the IBM Tivoli Monitoring agents are reporting to the IBM Tivoli Monitoring server correctly by logging into the IBM Tivoli Monitoring server enterprise portal as the sysadmin user and confirming that the Virtual I/O Server hostname and the two agents can be seen in the UNIX folder from Tivoli Enterprise Portal, as shown in Figure 8-7.

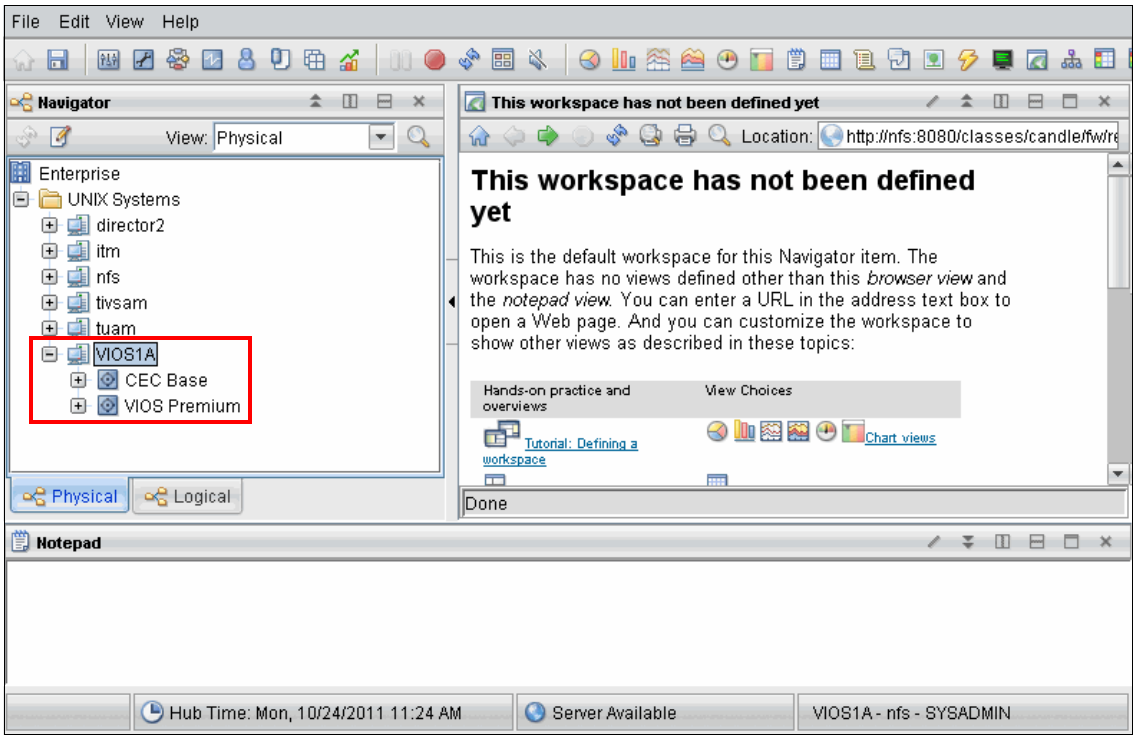

Figure 8-7 Confirm that the agents can be seen from the Tivoli Enterprise Portal

8.2.2 IBM Director Server agent configuration

Unlike the Virtual I/O Server agent, the IBM Director Server agents are not installed. The IBM Director Server should have two agents, the base UNIX monitoring agent and the IBM Director Server agent. It is possible to install the agents for the IBM Director Server either from the packages that come with IBM Service Delivery Manager (part numbers CZF82EN and CZL9GEN) or push out the agents from IBM Tivoli Monitoring Server.

It is our opinion that it is easier to perform a push style installation from the IBM Tivoli Monitoring Server. Thus, the manual installation of the monitoring agents is not covered in this publication.

To perform a push installation of the IBM Tivoli Monitoring agents for the IBM Systems Director server, perform the following steps:

1. Log in to the IBM Tivoli Monitoring server command shell.
2. Log in to the IBM Tivoli Monitoring application as a privileged user by running the following command:

   ```
   /opt/IBM/ITM/bin/tacmd login -s localhost -u <username> -p
   <password>
   ```

   In our example we logged in as the sysadmin user, as shown in Example 8-8. The default password for the sysadmin user is *password*.

   Example 8-8 Log in to ITM as sysadmin user

   ```
   # /opt/IBM/ITM/bin/tacmd login -s localhost -u sysadmin -p password
   Validating user...

   KUIC00007I: User sysadmin logged into server on
   https://localhost:3661.
   ```

3. Before the agents can be deployed they need to be added to the IBM Tivoli Monitoring repository.

   To add the base monitoring agent to the repository perform the following steps:

   a. Mount the repository directory from the NFS server instance that comes with IBM Service Delivery Manager. In our example we ran the following command:

      ```
      mount nfs:/repository /mnt
      ```

   b. Add the base agent to the repository by running the following command:

      ```
      /opt/IBM/ITM/bin/tacmd addBundles -i
      <mountpoint>/itmAgent622/unix -t ux
      ```

      In our example we ran the command shown in Example 8-9.

      Example 8-9 Adding the base operating system agent to the ITM repository

      ```
      # /opt/IBM/ITM/bin/tacmd addBundles -i /mnt/itmAgent622/unix -t
      ux -p aix523 aix526

       KUICAB023I: Are you sure you want to add the following bundles
      to the /opt/IBM/ITM/tables/TEMS/depot depot?

      Product Code : ux
      Deployable   : true
      Version      : 062201000
      ```

```
Description  : Monitoring Agent for UNIX OS
Host Type    : aix523
Host Version : aix523,aix533
Prerequisites: ci:062201000 ax:062201000 ui:062201000
jr:050900000 gs:074020000 la:010001000


Product Code : ux
Deployable   : true
Version      : 062201000
Description  : Monitoring Agent for UNIX OS
Host Type    : aix526
Host Version : aix526,aix536
Prerequisites: ci:062201000 ax:062201000 ui:062201000
jr:050900000 gs:074020000 la:010001000

 KUICAB024I: Enter Y for yes or N for no: Y

 KUICAB020I: Adding bundles to the /opt/IBM/ITM/tables/TEMS/depot
depot. The time required to complete this operation depends on
the number and size of the added bundles.

 KUICAB022I: The following bundles were successfully added to the
/opt/IBM/ITM/tables/TEMS/depot depot:


Product Code : ux
Deployable   : true
Version      : 062201000
Description  : Monitoring Agent for UNIX OS
Host Type    : aix523
Host Version : aix523,aix533
Prerequisites: ci:062201000 ax:062201000 ui:062201000
jr:050900000 gs:074020000 la:010001000


Product Code : ux
Deployable   : true
Version      : 062201000
Description  : Monitoring Agent for UNIX OS
Host Type    : aix526
Host Version : aix526,aix536
Prerequisites: ci:062201000 ax:062201000 ui:062201000
jr:050900000 gs:074020000 la:010001000
```

c. To add the IBM Systems Director monitoring agent to the repository, first download part number CZF82EN, IBM Tivoli Monitoring Agent for Systems Director base V6.2.2.2 Multiplatform, from IBM Partner Central. This part number is part of the IBM Service Delivery Manager packages. The filename for the downloaded file is `CZF82EN.tar.gz`. Copy it to the `/tmp` directory of IBM Tivoli Monitoring server.

d. Make a directory in the `/tmp` directory called `bundle`. Change to the `/tmp/bundle` directory gunzip and untar `CZF82EN.tar.gz`. Example 8-10 is an example of the commands we performed.

Example 8-10 Example of unzipping the ISD agent files

```
# cd /tmp
# mkdir bundles
# cd bundles
# gunzip CZF82EN.tar.gz | tar xvf -
```

e. Add the IBM Systems Director agent to the IBM Tivoli Monitoring repository by running the following command:

```
/opt/IBM/ITM/bin/tacmd addBundles -i /tmp/bundles/unix -t d9 -p
aix523
```

In our example we ran the command shown in Example 8-11.

Example 8-11 Add the ISD agent to the repository

```
# /opt/IBM/ITM/bin/tacmd addBundles -i /tmp/bundles/unix -t d9 -p
aix523 aix526

 KUICAB023I: Are you sure you want to add the following bundles
to the /opt/IBM/ITM/tables/TEMS/depot depot?


Product Code : d9
Deployable   : true
Version      : 062200000
Description  : Monitoring Agent for IBM Systems Director base
Host Type    : aix523
Host Version : aix523,aix533
Prerequisites: ci:062202000 la:010001000 jr:050900000
gs:074027000 ui:062202000 ax:062202000


Product Code : d9
Deployable   : true
Version      : 062200000
```

```
Description  : Monitoring Agent for IBM Systems Director base
Host Type    : aix526
Host Version : aix526,aix536
Prerequisites: ci:062202000 la:010001000 jr:050900000
gs:074027000 ui:062202000 ax:062202000

 KUICAB024I: Enter Y for yes or N for no: Y

 KUICAB020I: Adding bundles to the /opt/IBM/ITM/tables/TEMS/depot
depot. The time required to complete this operation depends on
the number and size of the added bundles.

 KUICAB022I: The following bundles were successfully added to the
/opt/IBM/ITM/tables/TEMS/depot depot:


Product Code : d9
Deployable   : true
Version      : 062200000
Description  : Monitoring Agent for IBM Systems Director base
Host Type    : aix523
Host Version : aix523,aix533
Prerequisites: ci:062202000 la:010001000 jr:050900000
gs:074027000 ui:062202000 ax:062202000


Product Code : d9
Deployable   : true
Version      : 062200000
Description  : Monitoring Agent for IBM Systems Director base
Host Type    : aix526
Host Version : aix526,aix536
Prerequisites: ci:062202000 la:010001000 jr:050900000
gs:074027000 ui:062202000 ax:062202000
```

The import of the agents into the IBM Tivoli Monitoring repository is complete.

4. To push out the base AIX monitoring agent run the following command:

   ```
   /opt/IBM/ITM/bin/tacmd createNode -h <hostname> -d /opt/IBM/ITM -u
   <username> -w <password>
   ```

We deployed our agent to the IBM Systems Director named director2.powercloud.ibm.com, as shown in Example 8-12.

Example 8-12 Deploy the ISD ITM agent

```
/opt/IBM/ITM/bin/tacmd createNode -h director2.powercloud.ibm.com -d
/opt/IBM/ITM -u root -w password
KUICCN022I: Request has been successfully queued to the deploy
controller. The transaction ID is 131922095617159700002583 9, use the
getDeployStatus CLI to view the status.
```

5. To view the progress status of the deployment use this command:

   ```
   /opt/IBM/ITM/bin/tacmd getDeployStatus
   ```

   In our example we used the command shown in Example 8-13.

Example 8-13 Checking the status of the ITM agent deployment

```
# /opt/IBM/ITM/bin/tacmd getDeployStatus -g
131922478015536700000887 0
Transaction ID : 131922478015536700000887 0
Command        : INSTALL
Status         : SUCCESS
Retries        : 0
TEMS Name      : TEMS
Target Hostname: director2.powercloud.ibm.com
Platform       : aix616
Product        : UX
Version        : 062201000
Error Message  : KDY2065I: The node creation operation was a
success.
```

6. To check communication between the IBM Tivoli Monitoring agent and the IBM Tivoli Monitoring Server, log into the IBM Tivoli Monitoring server enterprise web portal as the sysadmin user. Check the `UNIX` folder for the hostname of the IBM Systems Director Server and confirm that the base agent can be seen. An example of how the agent appears in the IBM Tivoli Monitoring in the enterprise web portal can be seen in Figure 8-8.

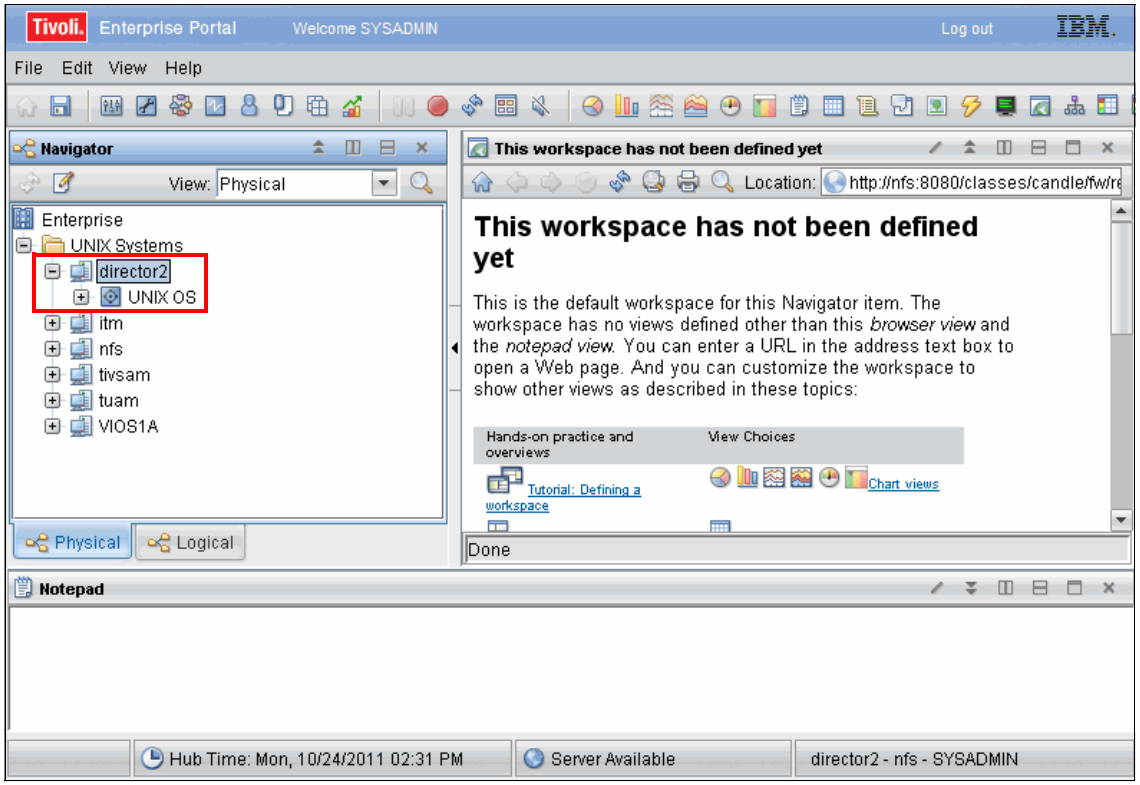

Figure 8-8 The ITM base UNIX agent as seen in the ITM web portal

7. Push out the IBM Systems Director Monitoring Agent by using this procedure:
   a. Identify the name of the director node by running this command:

      ```
      /opt/IBM/ITM/bin/tacmd listSystems -t UX
      ```

      An example of our output is shown in Example 8-14.

      Example 8-14 List of ITM nodes

      ```
      # /opt/IBM/ITM/bin/tacmd listSystems -t UX
      Managed System Name Product Code Version     Status
      nfs:KUX             UX           06.22.04.00 Y
      ```

```
tuam:KUX            UX          06.22.04.00 Y
director2:KUX       UX          06.22.01.00 Y
tivsam:KUX          UX          06.22.04.00 Y
itm:KUX             UX          06.22.04.00 Y
```

b. List the options that are available to IBM Systems Director Agent by running the following command:

```
/opt/IBM/ITM/bin/tacmd describeSystemType -t d9 -p aix526
```

8. To add the IBM Systems Director agent to the IBM Systems Director server run the following command:

```
/opt/IBM/ITM/bin/tacmd addSystem -t d9 -n <managed system name>
-p INSTANCE=<instance name>
KD9_CUSTOM_CONFIG.KD9_MSG_LOG_COUNT=<number of log messages>
KD9_CUSTOM_CONFIG.CDP_PURE_EVENT_CACHE_SIZE=<Number of events in
director>
KQZ_JAVA.JAVA_HOME=<path to java>
KQZ_JAVA.JAVA_TRACE_LEVEL=<"OFF", "ERROR", "WARN", "INFO",
"DEBUG_MIN", "DEBUG_MID", "DEBUG_MAX", "ALL">
KQZ_REST.KQZ_REST_USER=<director user>
KQZ_REST.KQZ_REST_PASSWORD=<director user password>
KQZ_REST.KQZ_REST_SERVER_NAME=<director hostname>
KQZ_REST.KQZ_REST_PORT_NUMBER=<rest port number>
KQZ_REST.KQZ_JMS_PORT_NUMBER=<jms port number>
KQZ_REST.KQZ_REST_CERTIFICATE_VALIDATION=<“TRUE” “FALSE”>
```

A rundown of the compulsory properties can be seen in Table 8-2.

Table 8-2 Compulsory IDS agent properties

Property	Description
INSTANCE	The name of the instance.
KD9_CUSTOM_CONFIG.KD9_MSG_LOG_COUNT	Specify the number of the most recent event history log messages to display.
KD9_CUSTOM_CONFIG.CDP_PURE_EVENT_CACHE_SIZE	The maximum number of real-time Director events that are stored in IBM Tivoli Monitoring at a given time.
KQZ_JAVA.JAVA_HOME	The path to where java is installed.
KQZ_JAVA.JAVA_TRACE_LEVEL	This parameter allows you to specify the trace level used by the Java providers.
KQZ_REST.KQZ_REST_USER	The Director server user.
KQZ_REST.KQZ_REST_PASSWORD	The Director server password.

Property	Description
KQZ_REST.KQZ_REST_SERVER_NAME	The host or IP address of the Director server.
KQZ_REST.KQZ_REST_PORT_NUMBER	The REST port number of the Director server.
KQZ_REST.KQZ_JMS_PORT_NUMBER	The JMS port number of the Director server.
KQZ_REST.KQZ_REST_CERTIFICATE_VALIDATION	Disabling certificate validation is potentially insecure.

In our example we ran the command shown in Example 8-15.

Example 8-15 Push IDS agent example

```
# /opt/IBM/ITM/bin/tacmd addSystem -t d9 -n director2:KUX -p
INSTANCE=director2 KD9_CUSTOM_CONFIG.KD9_MSG_LOG_COUNT=500
KD9_CUSTOM_CONFIG.CDP_PURE_EVENT_CACHE_SIZE=250
KQZ_JAVA.JAVA_HOME=/usr/java5 KQZ_JAVA.JAVA_TRACE_LEVEL=ERROR
KQZ_REST.KQZ_REST_USER=root KQZ_REST.KQZ_REST_PASSWORD=itsoadmin
KQZ_REST.KQZ_REST_SERVER_NAME=director2.powercloud.ibm.com
KQZ_REST.KQZ_REST_PORT_NUMBER=8422
KQZ_REST.KQZ_JMS_PORT_NUMBER=61616
KQZ_REST.KQZ_REST_CERTIFICATE_VALIDATION=false

KUICAR010I: The agent type d9 is being deployed.

KUICAR028I: The operation has been successfully queued for
deployment, the transaction id is 131948532731553200002831 7, use the
getDeployStatus CLI to view the status.
```

Note: Our IBM Director Server was installed and running using default values.

9. To view the progress status of the deployment use the following command:

   ```
   /opt/IBM/ITM/bin/tacmd getDeployStatus
   ```

   In our example we used the command shown in Example 8-16.

   Example 8-16 Checking the status of the ITM agent deployment

   ```
   # /opt/IBM/ITM/bin/tacmd getDeployStatus 131948532731553200002831 7
   Transaction ID : 131948532731553200002831 7
   Command        : CONFIGURE
   ```

```
Status          : SUCCESS
Retries         : 1
TEMS Name       : TEMS
Target Hostname: director2:KUX
Platform        : aix536
Product         : D9
Version         : 062200000
Error Message   : KDY0028I: Request completed successfully.
Deployment request was processed successfully and is now completed.
```

When the status shows a success, like the output in Example 8-16 on page 244, the IBM Director Server Agent has been deployed and configured successfully.

10. To check communication between the IBM Director Server monitoring agent and the IBM Tivoli Monitoring Server, log into the IBM Tivoli Monitoring server enterprise web portal as the sysadmin user. Check the `UNIX` folder for the hostname of the IBM Systems Director Server and confirm that the IBM Systems Director base agent can be seen. An example of how the agent appears in the IBM Tivoli Monitoring in the enterprise web portal can be seen in Figure 8-9.

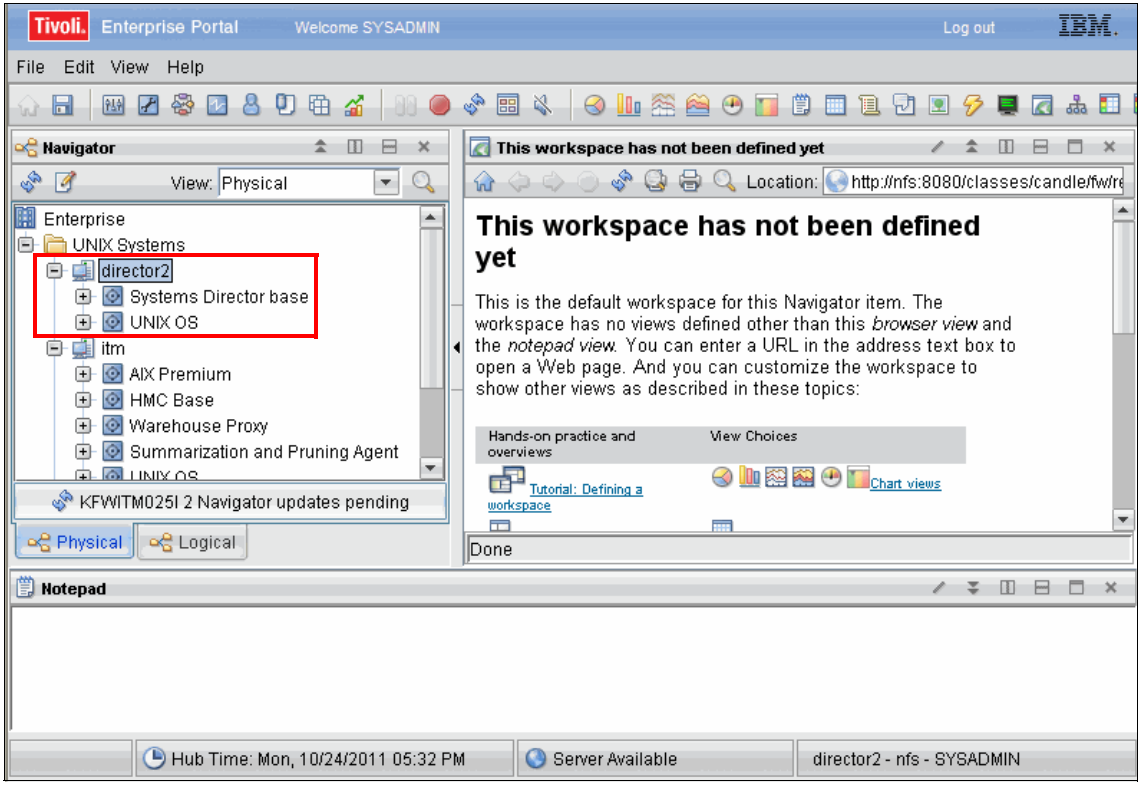

Figure 8-9 The ITM base UNIX agent as seen in the ITM web portal

8.2.3 Hardware Management Console configuration

The Hardware Management Console is a single IBM Tivoli Monitoring agent. Unlike most common agents, it is not installed on the host that it is monitoring. It is installed on a different host, which contains the connection details to communicate with the Hardware Management Console.

By default, the agent is already installed on the IBM Tivoli Monitoring virtual image of IBM Service Delivery Manager.

To configure the Hardware Management Console agent, perform these tasks:

1. Log in to the IBM Tivoli Monitoring server shell console as a privileged user. We used the root user.
2. Check to see whether the agent is running on the IBM Tivoli Monitoring server, as the agent cannot be configured if it is already running. To check which agents are running, run the following command:

   ```
   /opt/IBM/ITM/bin/cinfo -r
   ```

   The agent has a product code for the Hardware Management Console agent (that is, ph). An example of the command that we performed and its output is shown in Example 8-17.

   Example 8-17 Check to see which ITM agents are running

   ```
   # /opt/IBM/ITM/bin/cinfo -r

   *********** Wed Oct 19 10:29:48 EDT 2011 ******************
   User: root Groups: system bin sys security cron audit lp
   Host name : itm  Installer Lvl:06.22.04.00
   CandleHome: /opt/IBM/ITM
   ***********************************************************
   Host  Prod  PID       Owner     Start     ID    ..Status
   itm   kf    25886930  virtuser  Oct13     None  ...running
   itm   cq    27394138  virtuser  Oct13     None  ...running
   itm   ms    9568416   virtuser  Oct13     TEMS  ...running
   itm   pk    17563858  virtuser  Oct13     None  ...running
   itm   px    9371800   virtuser  Oct13     None  ...running
   itm   ux    21495950  virtuser  Oct13     None  ...running
   itm   hd    6684918   virtuser  15:56:35  None  ...running
   itm   sy    5243122   virtuser  15:56:54  None  ...running
   ```

3. Configure the Hardware Management Console agent by running this command:

   ```
   /opt/IBM/ITM/bin/itmcmd config -A ph
   ```

   The minimum information that you will need to configure the agent is listed in Table 8-3. All other information can be left blank for a default installation.

   Table 8-3 Minimum properties required to configure an HMC agent

Property	Description
Agent instance name	An instance name for the HMC agent. It is possible to monitor multiple HMC hosts from the same host that runs the HMC agent.

Property	Description
HMC hostname	The hostname of the HMC.
HMC username	The user used for connecting to the HMC.
ITM server hostname	The hostname of the ITM server.

An example of the configuration command that we ran can be seen in Example 8-18.

Example 8-18 HMC agent configuration

```
# /opt/IBM/ITM/bin/itmcmd config -A ph
Agent configuration started...
Enter instance name (default is: ): hmc1
Edit "Monitoring Agent for HMC Base" settings? [ 1=Yes, 2=No ] (default is:
1):
Edit 'HMC Information' settings? [ 1=Yes, 2=No ] (default is: 1):
HMC Hostname (default is: ): hmc.powercloud.ibm.com
HMC Username (default is: ): hscroot

Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 1):
TEMS Host Name (Default is: itm): itm

Network Protocol [ip, sna, ip.pipe or ip.spipe] (Default is: ip.pipe):
ip.pipe

     Now choose the next protocol number from one of these:
     - ip
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 2 (Default is: 0): 0
IP.PIPE Port Number (Default is: 1918): 1918
Enter name of KDC_PARTITION (Default is: null):

Configure connection for a secondary TEMS? [1=YES, 2=NO] (Default is: 2): 2
Enter Optional Primary Network Name or 0 for "none" (Default is: 0): 0

Agent configuration completed...
```

4. For the agent to work correctly and collect information from the Hardware Management Console, public and private ssh keys need to be set up between the agent that hosts the agent and the Hardware Management Console.

   To configure the ssh keys, perform the following steps:

   a. On the IBM Tivoli Monitoring Server create a pair of ssh public and private keys as the root user by running the following command:

      ```
      ssh-keygen -t rsa
      ```

      An example of the command that we used can be seen in Example 8-19.

      Example 8-19 Create ssh key

      ```
      # ssh-keygen -t rsa
      Generating public/private rsa key pair.
      Enter passphrase (empty for no passphrase):
      Enter same passphrase again:
      Your identification has been saved in /.ssh/id_rsa.
      Your public key has been saved in /.ssh/id_rsa.pub.
      The key fingerprint is:
      d0:a5:d6:15:82:4c:12:b4:d5:3b:b5:b6:ae:8b:d6:ff root@itm
      The key's randomart image is:
      +--[ RSA 2048]----+
      |     .++ooo o.   |
      |       =o+.o.    |
      |      o + .o .   |
      |       o  o o    |
      |        S  o .   |
      |           .     |
      |         . .     |
      |        ... .    |
      |       .. o+..E  |
      +-----------------+
      ```

      Note: For the Hardware Management Console agent to work correctly, the ssh key should not contain a passphrase.

   b. Print the ssh public key to the console by running the following command:

      ```
      cat ~/.ssh/id_rsa.pub
      ```

The output from this command needs to be used as input for a Hardware Management Console command. An example of the command that we ran can be seen in Example 8-20.

Example 8-20 The public ssh key

```
# cat ~/.ssh/id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC+qXHWtB6qPPzE7m56Z6iGmCwAFc/5/jdJo
MxIZp5c1UMLRpWMBZh2LjebvK3MotwmjGP4ddVM+6i8fOEUHMOIz3g/KgBtzE4z8u
Q3/bKxSObwXEFipPPMPzMAohilOUsC7ZjtavFGOC8BzqJovIMOmHBNxwhiN4wXz6F
HG4kJzab4hG29A4pp8MdBblM+EAXgXc3B8Q1pOIdJOvzBHxZ/x5TqevrF1JiLfcce
4eLrkjBEublEaFwXO7g/IwWBz3SCNcjb+3EqaGW1yfLoInCHREwxtIjVc97myGseE
hb9NsDxi/KXTL2Qqm+qM6bhOAvd1O5T5MBILPQxdCGc9e6V root@itm
```

c. Log on to your hmc shell console as the hmc user specified in step 3 on page 247 and add the public ssh key using the following command:

```
mkauthkeys -a '<ssh-key>'
```

The variable <*ssh-key*> is the output from the previous command, which displays the ssh public key. An example of the command that we use can be seen in Example 8-21.

Example 8-21 Add the public key to HMC

```
hscroot@hmc:~> mkauthkeys --add 'ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC+qXHWtB6qPPzE7m56Z6iGmCwAFc/5/jdJo
MxIZp5c1UMLRpWMBZh2LjebvK3MotwmjGP4ddVM+6i8fOEUHMOIz3g/KgBtzE4z8u
Q3/bKxSObwXEFipPPMPzMAohilOUsC7ZjtavFGOC8BzqJovIMOmHBNxwhiN4wXz6F
HG4kJzab4hG29A4pp8MdBblM+EAXgXc3B8Q1pOIdJOvzBHxZ/x5TqevrF1JiLfcce
4eLrkjBEublEaFwXO7g/IwWBz3SCNcjb+3EqaGW1yfLoInCHREwxtIjVc97myGseE
hb9NsDxi/KXTL2Qqm+qM6bhOAvd1O5T5MBILPQxdCGc9e6V root@itm'
```

d. Run the **ssh** command from the IBM Tivoli Monitoring server as root and ssh to the Hardware Management Console. This caches the ssh key of the Hardware Management Console to the `/.root/known_hosts` file and prevents the agent from requesting a confirmation of authenticity each time that the agent is started. This step also confirms that the ssh key exchanging is working correctly between the two hosts, as there should be no prompting to enter a password. An example of the command that we performed is shown in Example 8-22.

Example 8-22 Cache the ssh key

```
# ssh hscroot@hmc.powercloud.ibm.com
The authenticity of host 'hmc.powercloud.ibm.com (172.16.20.111)'
can't be established.
```

```
RSA key fingerprint is
16:55:25:54:ed:68:63:c2:76:2f:60:e9:66:75:01:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'hmc.powercloud.ibm.com,172.16.20.111'
(RSA) to the list of known hosts.
Last login: Tue Oct 15 09:27:01 2011 from 172.16.20.130
```

The communication pathway between the agent and the Hardware Management Console is now complete.

5. The Hardware Management Console monitoring agent can now be started. To start the agent use the following command:

   `/opt/IBM/ITM/bin/itmcmd agent -o <instance name> start ph`

   The variable <*instance name*> is the instance name that you specified in step 3 on page 247 when configuring the agent. An example of the command that we ran can be seen in Example 8-23.

   Example 8-23 Start the HMC agent

```
# /opt/IBM/ITM/bin/itmcmd agent -o hmc1 start ph

Starting Base Monitoring Agent for HMC ...
```

6. Confirm that the agent is running by using the **/opt/IBM/ITM/bin/cinfo -r** command. An example of the command that we ran can be seen in Example 8-24.

   Example 8-24 Confirm that the agent is started and running

```
# /opt/IBM/ITM/bin/cinfo -r

*********** Wed Oct 19 10:32:56 EDT 2011 ******************
User: root Groups: system bin sys security cron audit lp
Host name : itm  Installer Lvl:06.22.04.00
CandleHome: /opt/IBM/ITM
***********************************************************
Host  Prod  PID       Owner     Start     ID    ..Status
itm   kf    25886930  virtuser  Oct13     None  ...running
itm   cq    27394138  virtuser  Oct13     None  ...running
itm   ms    9568416   virtuser  Oct13     TEMS  ...running
itm   pk    17563858  virtuser  Oct13     None  ...running
itm   px    9371800   virtuser  Oct13     None  ...running
itm   ux    21495950  virtuser  Oct13     None  ...running
itm   hd    6684918   virtuser  15:56:35  None  ...running
```

```
itm    sy    5243122   virtuser  15:56:54  None   ...running
itm    ph    8061174   root      10:32:16  hmc1   ...running
```

7. Confirmthat the Hardware Management Console monitoring agent is reporting to the IBM Tivoli Monitoring server correctly by logging into the IBM Tivoli Monitoring server enterprise portal as the sysadmin user and checking that the IBM Tivoli Monitoring LPAR host name and the agent can be seen in the UNIX folder from Tivoli Enterprise Portal, as shown in Figure 8-10.

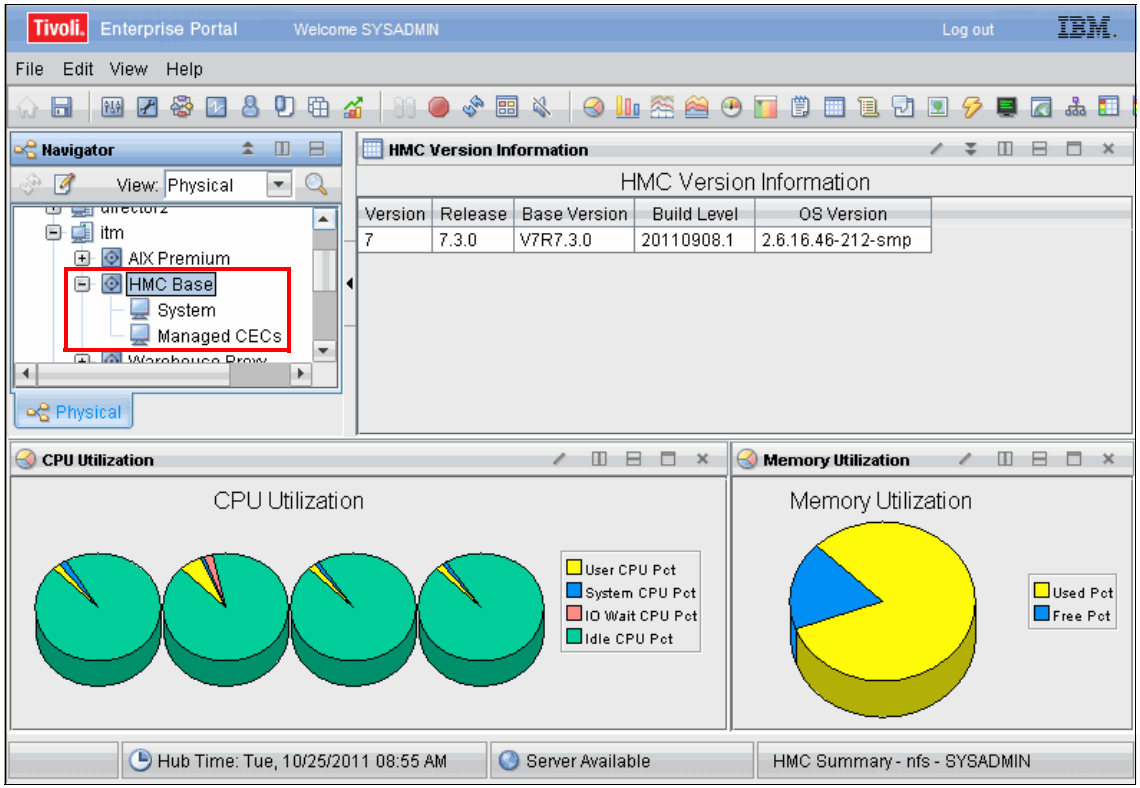

Figure 8-10 Confirm that the HMC agent can be seen in the ITM web console

9

Using Tivoli Usage and Accounting Manager

Tivoli Usage and Accounting Manager handles collecting, analyzing, and reporting on usage of computing resources, and billing based on costs of shared computing resources. This chapter discusses basic verification and reporting within Tivoli Usage and Accounting Manager in this environment. For more information about the capabilities of Tivoli Usage and Accounting Manager and how to use it, see *Tivoli Usage and Accounting Manager* in the IBM Tivoli Systems Management Information Center located at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.ituam.doc_7.3/welcome.htm

9.1 Verifying monitored resources

Before any reports can be generated, verify that Tivoli Service Automation Manager has provisioned at least one project, that reporting data has been generated, and that Tivoli Usage and Accounting Manager has properly imported the data:

1. Log in as maxadmin to the Tivoli Service Automation Manager administrative user interface at `https://<nfs server>/tivsam/admin`.
2. Navigate to **Go To** → **Service Automation** → **Service Deployment Instances**.
3. In the Status field, type either `Operational` or `Decommissioned` and press Enter.

   Note: At least one row should be returned by this filter. Check that the rows returned are related to the reporting period that you are interested in. If no rows related to the reporting period are present, it means that there have been no projects contributing to Tivoli Usage and Accounting Manager reports for the specified period. The reports will be empty.

4. Connect via SSH to the Tivoli Service Automation Manager server.
5. Verify that at least one non-zero length file related to your reporting period is present on the `TIVSAM_image` under `/var/IBM/TSAM/metering`, as shown in Example 9-1.

Example 9-1 Tivoli Service Automation Manager metering output (truncated)

```
# cd /var/IBM/TSAM/metering
# ls
RDPVS_5_20110810.txt  RDPVS_5_20110821.txt  RDPVS_5_20110901.txt
RDPVS_5_20110912.txt  RDPVS_5_20110923.txt  RDPVS_5_20111004.txt
RDPVS_5_20111015.txt
```

6. Verify that data has been properly imported into Tivoli Usage and Accounting Manager. To check this:
   a. Use a web browser to log on to `https://<nfs server>/tuam/tip`. In the login window, specify virtuser as the user ID. Click **Log in**.
   b. Expand **Task Management** → **Job Runner**, then click **Load Tracking**. Three rows are displayed for each day for which data has been uploaded.

9.2 Generating an invoice

After you have verified that Tivoli Usage and Accounting Manager has data from which to generate reports, generate an invoice to test the functionality:

1. Navigate to `http://<nfs server>/` and click **TUAM TIP**. This brings you to the Tivoli Integrated Portal, as you see in Figure 9-1.

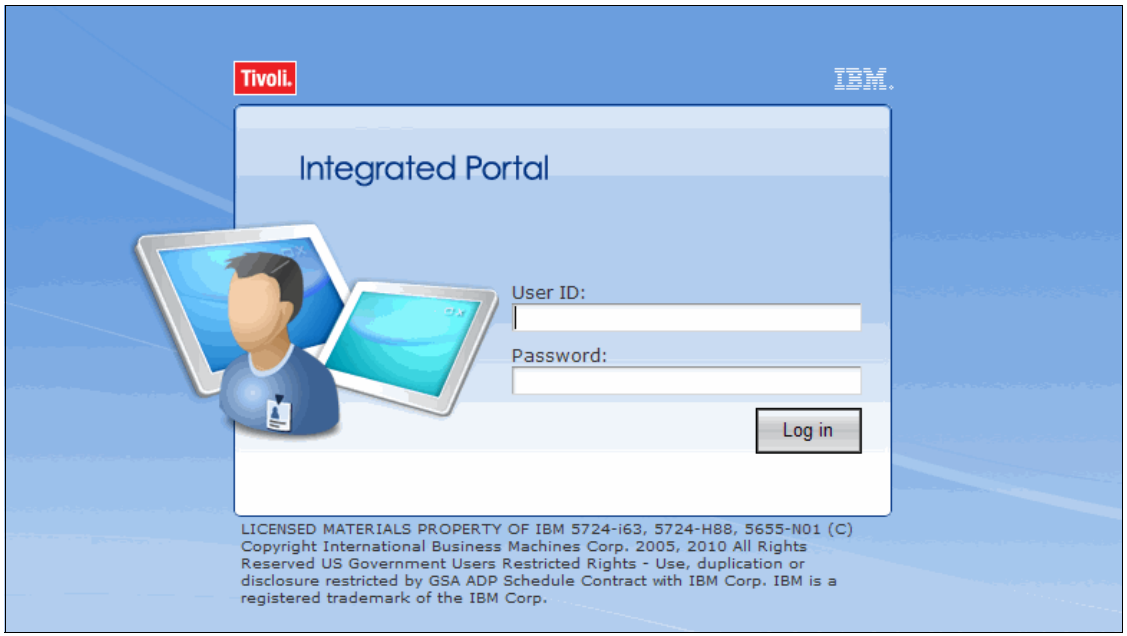

Figure 9-1 Tivoli Integrated Portal login panel

2. Log on to the Tivoli Usage and Accounting Manager server as virtuser. You will see the welcome screen, as shown in Figure 9-2.

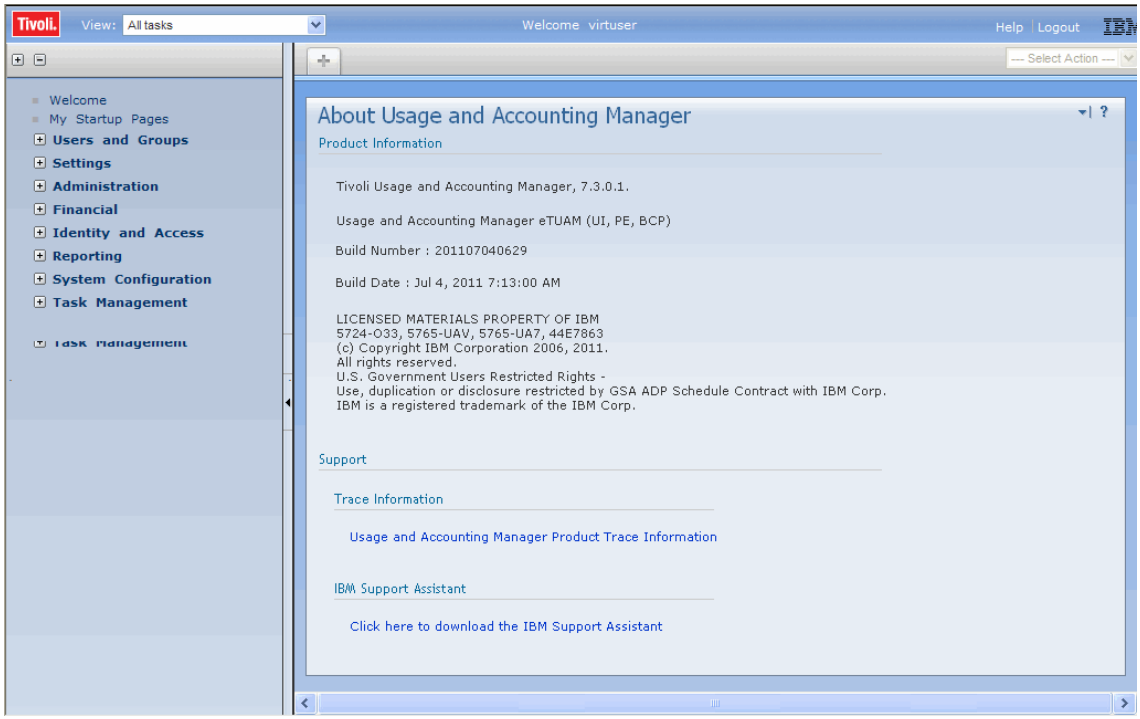

Figure 9-2 Tivoli Usage and Accounting Manager welcome panel

3. In the menu on the left side, click **Reporting** → **Common Reporting**. You will be presented with the dialog shown in Figure 9-3.

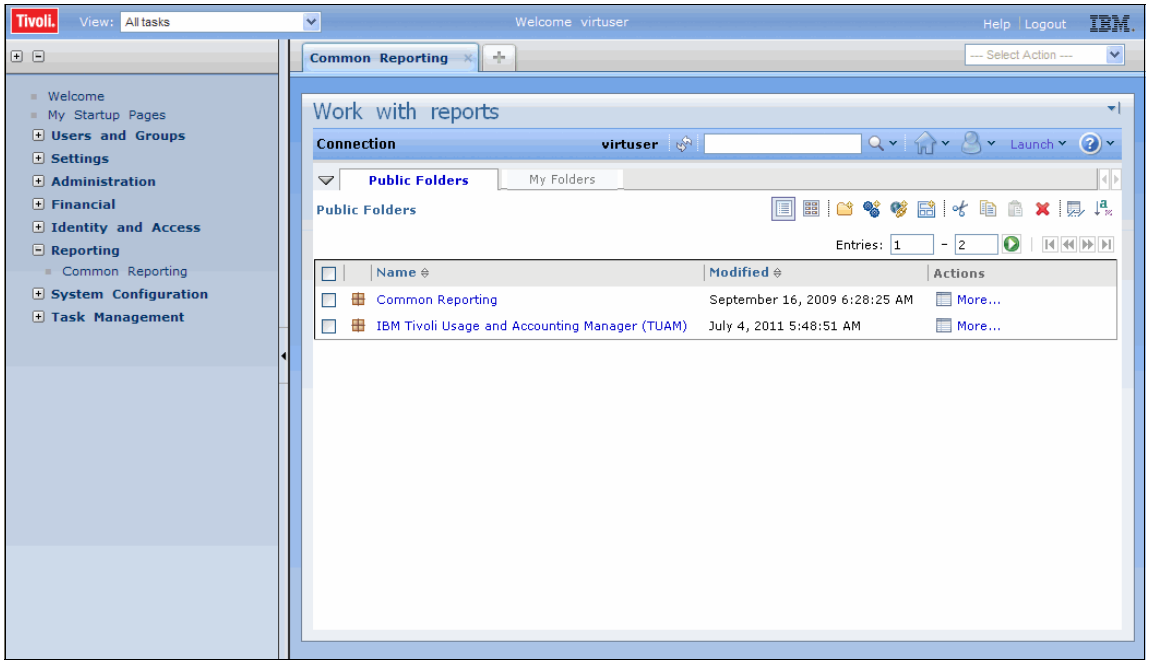

Figure 9-3 Common Reporting options

4. Click **IBM Tivoli Usage and Accounting Manager (TUAM)**. Figure 9-4 shows the default set of report folders.
5. Click **Account Reports**.

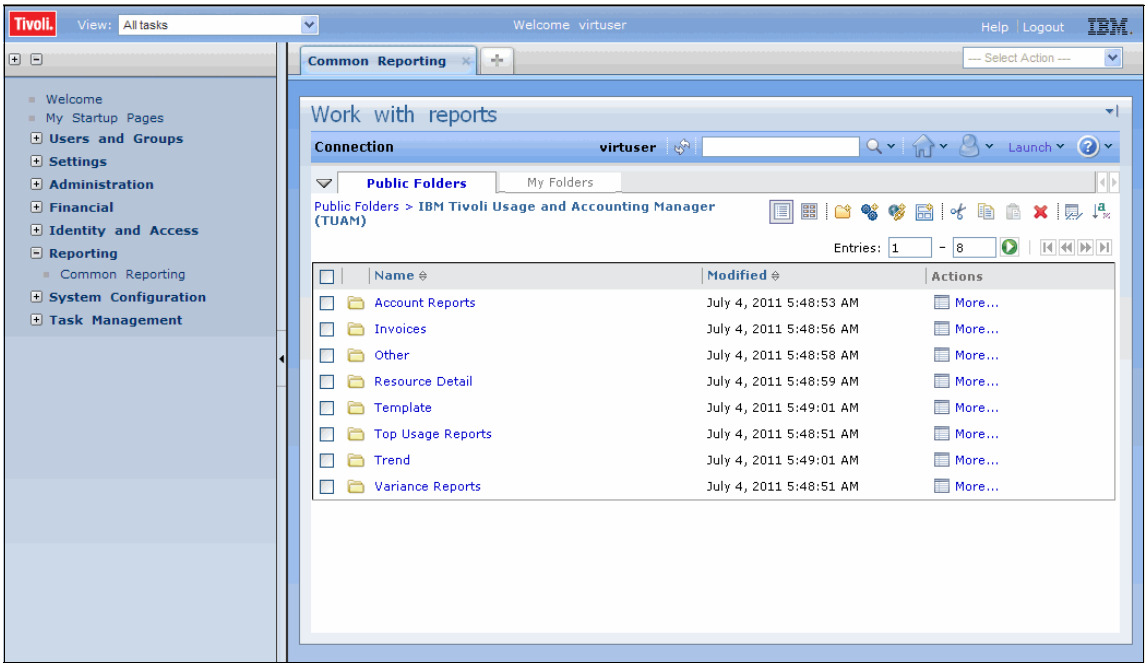

Figure 9-4 Tivoli Usage and Accounting Manager default report folders

6. The next dialog (shown in Figure 9-5) lists the type of invoice reports available by default. Select “**Invoice by Account Level**.

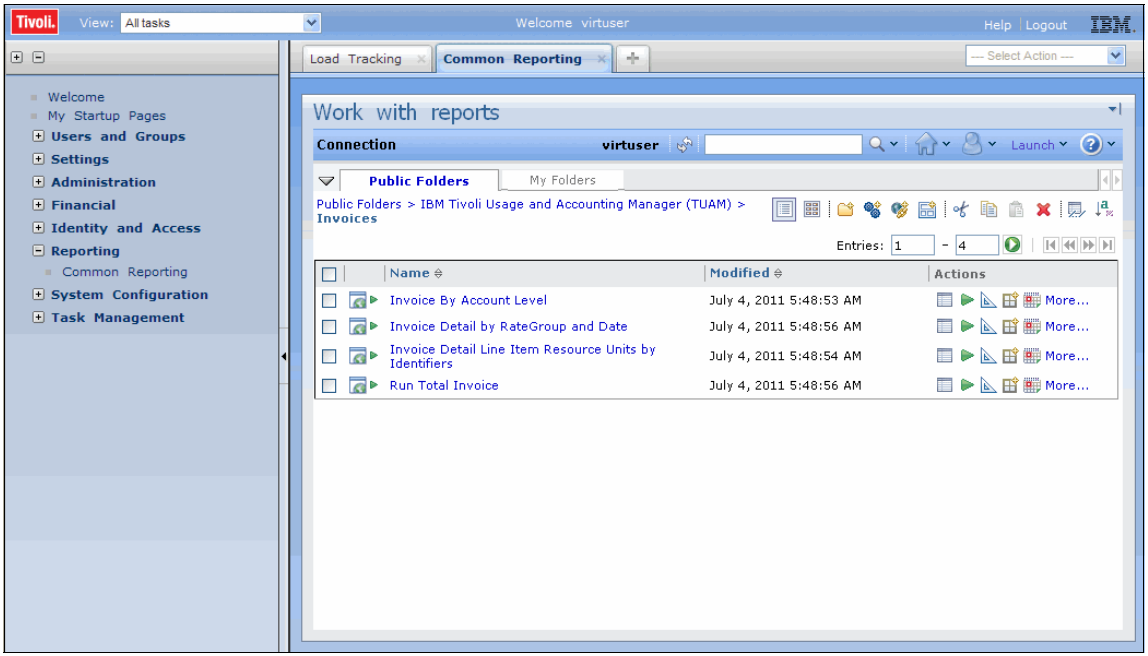

Figure 9-5 Reports available in Invoices

7. Figure 9-6 shows the options available for this report. The account structure reflects the chargeback hierarchy for the organization. Refer to the *Project account and the account code structure* in *IBM Service Delivery Manager User's Guide* for more details about the Account Structure. For now, simply select **CloudStandard**.

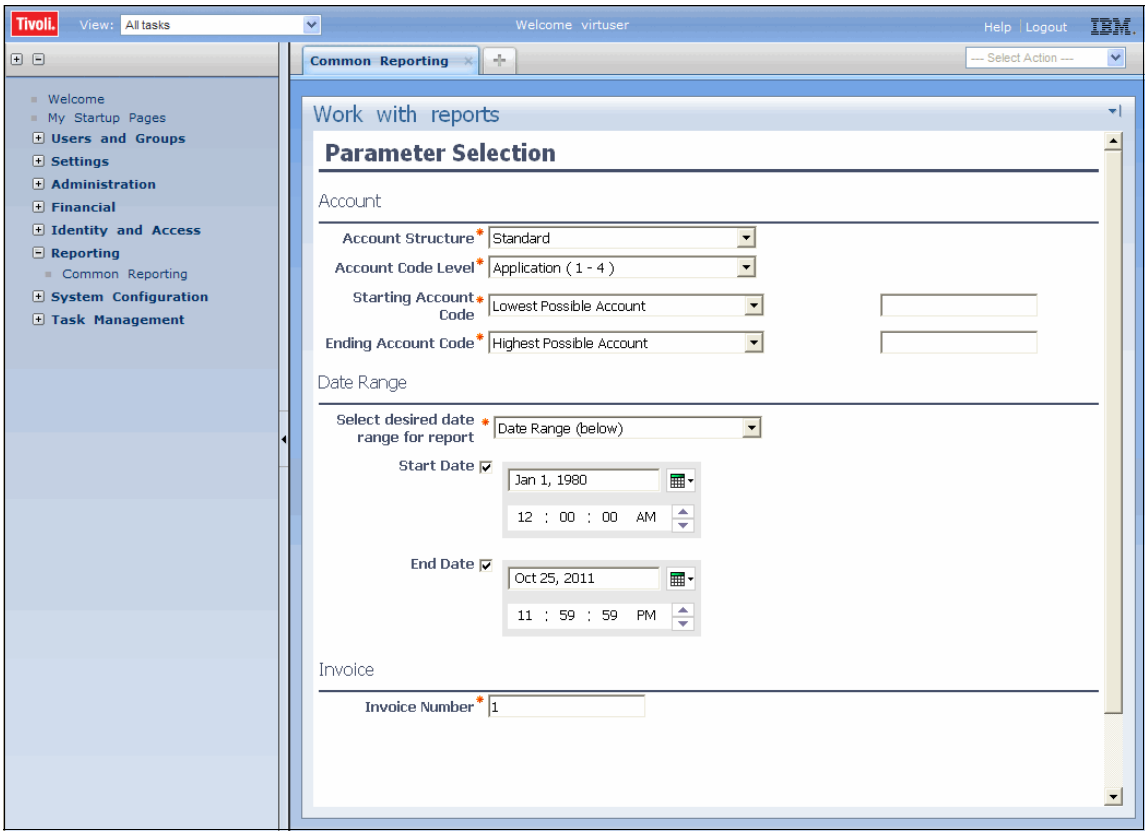

Figure 9-6 Parameter Selection for Invoice by Account Level

8. Leave the remaining options at their default values. Scroll to the bottom of the page and click **Finish**.

At this point you will see the generated invoice, as shown in Figure 9-7.

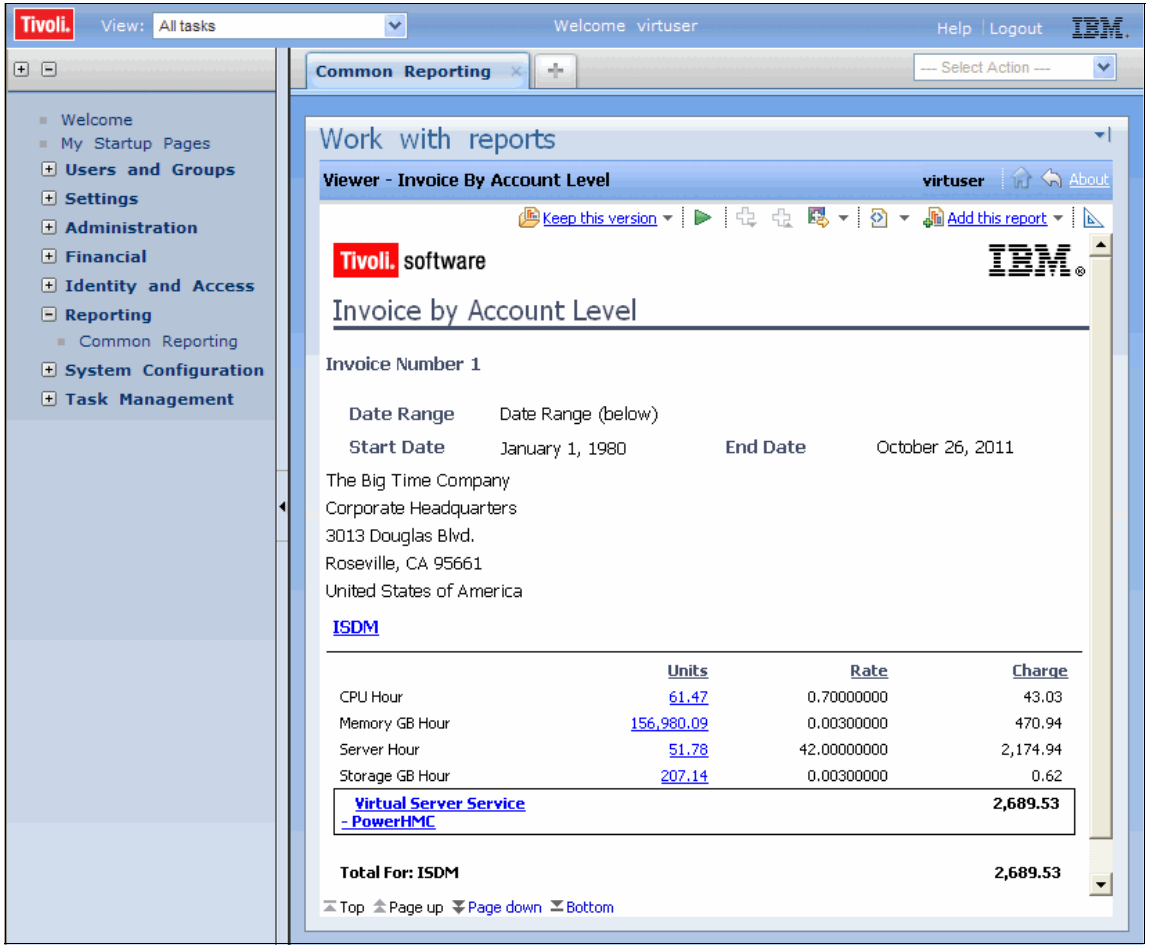

Figure 9-7 Sample invoice generated by Tivoli Usage and Accounting Manager

A

Configuration defaults

IBM Service Delivery Manager is preconfigured with a set of URLs and users. This appendix lists the default install-time values.

ISDM URLs

Table A-1 shows the URLs and default credentials that you use to access the individual components of IBM Service Delivery Manager. Table A-1 shows both redirected URLs through the NFS appliance and direct URLs to the specific host.

Table A-1 ISDM URL and credentials

Redirected URL	Direct UrL	User/ password	Function
http://<nfs>/	N/A	N/A	Central ISDM portal
https://<nfs>/SimpleSRM	https://<TSAM>:9443/ SimpleSRM	PMRDPCAUSR / maxadmin	Tivoli Service Automation Manager self-service interface
https://<nfs>/tivsam/admin	https://<TSAM>:9443/maximo	maxadmin / password	Tivoli Service Automation Manager/TPAe administrative interface
https://<nfs>/tivsam/wasadmin	https://<TSAM>:9043/ibm/console	wasadmin / password	WebSphere console on <tivsam>
http://<nfs>/itm/teps	http://<itm>:1920	sysadmin / password	ITM Service Index. Password set in ovf
http://NFS_image/itm/tcr	https://<itm>:16316/ibm/console	virtuser / <set in ovf>	Tivoli Common Reporting
http://<nfs>/ibm/console	http://<tuam>:11052/ibm/console	virtuser/ <set in ovf>	TUAM user interface
http://<nfs>/tuam/tip	https://<tuam>:17311/ibm/console	virtuser / <set in ovf>	Tivoli Integrated Portal (TIP): Tivoli Comon Reporting and Tivoli Usage and Accounting Manager
http://<nfs>/tuam/wasadmin	https://<tuam>:17316/ibm/console	virtuser / <set in ovf>	WebSphere Integrated Solutions Console

TivSAM default security configuration

The TivSAM appliance is preconfigured with default security and credentials. This section details the default values.

TivSAM appliance logins

Table A-2 lists the AIX user accounts created and used by IBM Service Delivery on the TivSAM appliance.

Table A-2 ISDM accounts on the TIVSAM appliance

User name/default password	Comment
root / <set in ovf>	Password set in OVF
ctginst1 / password	DB2 instance owner
dasusr1 / password	DB2 Admin Server
db2fenc1 / password	DB2 Fenced user, for instance, ctginst1
maximo / password	DB2
tioadmin / password	
wasadmin / password	WebSphere console admin user
maxadmin / password	TPM console admin
maxreg / password	
mxintadm / password	
PMSCADMUSER / maxadmin	
PMRDPCAUSER / maxadmin	Tivoli Service Automation Manager user for deploying images

TivSAM SSH passphrases

Table A-3 lists the pass phrases for SSH keystores on the TivSAM appliance.

Table A-3 SSH passphrases on the TIVSAM appliance

User name	Passphrase
root	
tioadmin	ssh4cloud

TivSAM certificates and keys

Table A-4 lists the certificates and keys on the TivSAM appliance. In the default configuration these keys are not protected by a passphrase.

Table A-4 ISSH certificates and keys on the TIVSAM appliance

Certificate / key	Comment
`/home/tioadmin/endpoint_keys`	To access VMs without a password.
`/home/tioadmin/.ssh/id_rsa`	Private key, used for provisioning.
`/home/tioadmin/.ssh/rsa.pub`	Public key, used for provisioning.
`https://<TSAM>:9043/ibm/console` **Security** > **SSL Certificates**	WAS certificate. Obtained from WAS admin console.

NFS default security configuration

The NFS appliance is preconfigured with default security and credentials. This section details the default values.

NFS appliance logins

Table A-2 on page 265 lists the AIX user accounts created and used by IBM Service Delivery on the NFS appliance.

Table A-5 ISDM accounts on the NFS appliance

User name	Passphrase
root / password	
virtuser / password	User provided by the VM

NFS certificates and keys

Table A-6 lists the certificates and keys and their respective passwords on the NFS appliance.

Table A-6 Issh certificates and keys on the NFS appliance

Certificate / key	Password	Comment
/opt/IBM/HTTPServer/etc/http_key.kdb		Keystore containing certificate to allow https connections
/opt/IBM/HTTPServer/etc/http_key.sth	password	Stash file
/opt/IBM/HTTPServer/Plugins/etc/plugin-tuam.kdb		Keystore containing TUAM certificate to allow URL redirection
/opt/IBM/HTTPServer/Plugins/etc/plugin-tuam.sth	password	Stash file
/opt/IBM/HTTPServer/Plugins/etc/plugin-key.kdb		Keystore containing Tivoli Service Automation Manager certificate to allow URL redirection
/opt/IBM/HTTPServer/Plugins/etc/plugin-key.sth	password	Stash file

ITM default security configuration

The IBM Tivoli Monitoring appliance is preconfigured with default security and credentials. This section details the default values.

ITM appliance logins

Table A-7 lists the AIX user accounts created and used by IBM Service Delivery on the ITM appliance.

Table A-7 ISDM accounts on the ITM appliance

User name/default password	Comment
root / password	
virtuser / password	VM user, owner of the ITM installation.
dasusr1 / password	DB2 Admin Server.
db2fenc1 / password	DB2 Fenced user for instance db2inst1.

User name/default password	Comment
db2inst1 / password	DB2 instance owner for instance db2inst1.
sysadmin / password	ITM default user. Used to log on to TEPS or access ITM command-line interface.
itmuser / password	ITM TEPS db user ID, owner of the tables created in DB2 for the ITM TEPS component.

Note: The db2inst1 and itmuser user IDs and passwords are contained in the TEPS configuration. If the passwords are changed, then the TEPS must be reconfigured with **`/opt/IBM/ITM/bin/itmcmd config -Acq`**.

Note: ITM's encryption key is ITMTivoliMonitoringEncryptionKey.

TUAM default security configuration

The Tivoli Usage and Accounting Manager appliance is preconfigured with default security and credentials. This section details the default values.

TUAM appliance logins

Table A-8 lists the AIX user accounts created and used by IBM Service Delivery on the TUAM appliance.

Table A-8 ISDM accounts on the ITM appliance

User name/default password	Comment
root / password	
virtuser / password	TUAM user for TUAM UI
db2inst1 / password	DB2 instance owner for instance db2inst1

TUAM certificates

Table A-9 shows the URL and path to obtain the TUAM's certificates.

Table A-9 Issh certificates and keys on the TUAM appliance

Certificate/key	Comment
https://<tuam>:11053/ibm/console **Security** > **SSL Certificates**	WAS certificate. Obtained from WAS admin console.

Abbreviations and acronyms

CSR	Common server resource
DCM	Data center model
GUI	Graphical user interface
HMC	Hardware Management Console
HPC	High Performance Computing
IBM	International Business Machines Corporation
ITM	IBM Tivoli Monitoring
ITSO	International Technical Support Organization
IVM	Integrated Virtualization Manager
Maximo	Manager administrative
NFS	Network File system Server
NIM	Network Installation Manager
OVF	Open virtualization format
SDMC	Systems Director Management Console
SLP	Service Location Protocol
SP5	Service Pack 5
SRM	Service Request Manager
TIP	Tivoli Integrated Portal
TIVSAM	Tivoli Services Automation Manager
TL6	Technology Level 6
TPAe	Tivoli Process Automation Engine
TPM	Tivoli Provisioning Manager
TSAM	Tivoli Service Automation Manager
TUAM	Tivoli Usage and Accounting Manager
VLANS	Virtual LANs

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topics in this document. Note that some publications referenced in this list might be available in softcopy only.

- *Deploying Cloud Components on POWER*, SG24-8009
- *IBM Systems Director VMControl Implementation Guide on IBM Power Systems*, SG24-7829
- *NIM from A to Z in AIX 5L*, SG24-7296

You can search for, view, download, or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- IBM Service Delivery Manager information center

  http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?topic=%2Fcom.ibm.tsamee.doc%2Ftsamee_welcome.html

- IBM Tivoli Service Automation Manager information center

  http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?topic=%2Fcom.ibm.tsamee.doc%2Ftsamee_welcome.html

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

D

S

T

U

V

W

X

Cloud Computing Infrastructure on IBM Power Systems: Getting Started with ISDM

Cloud Computing Infrastructure on IBM Power Systems

Getting started with ISDM

Detailed cloud resource configuration instructions

Detailed installation steps of ISDM

Point and click deployment of AIX

Managing IT systems is difficult. Virtualization brings numerous benefits to the datacenter and system administrators. However, it also creates a new set of choices. More choice implies more decisions, and thus an increased management responsibility. Furthermore, the move toward cloud computing, with a service-based acquisition and delivery model, requires that datacenter managers take a holistic view of the resources that they manage and the actors that access the data center.

IBM Service Delivery Manager addresses this problem domain. Delivered as a set of appliances, it automates provisioning, deprovisioning, metering, and management of an IT platform, and the services it provides. It addresses the needs of both IT management and service users.

This IBM Redbooks publication is intended for technical professionals who want to understand and deploy IBM ISDM Cloud on a Power platform.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7983-00 ISBN 0738436674